invensys

NUCLEAR QUALIFIED PRODUCTS

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

TRICON APPLICATIONS IN NUCLEAR REACTOR PROTECTION SYSTEMS

COMPLIANCE WITH NRC INTERIM GUIDANCE ISG-2 & ISG-4

Document No.: NTX-SER-09-10

Revision: 2

Issue Date: January 5, 2011

TABLE OF CONTENTS

LIST OF FIGURES

Changes to NTX-SER-09-10 from Revision 1

Section	Description
2.0	Clarified role of Safety and Non-safety RXM chassis. Provided reference to new Appendix 2. Footnote 3 eliminated due to changes.
2.1	Provided reference to new Appendix 2 relative to I/O Bus.
5.0, Staff Position 17	Dropped final paragraph of Compliance Comments made redundant by new Appendix 2 on RXMs.
Appendix 2	New appendix to address operational details of V10 RXM Chassis.
--	Miscellaneous typo corrections

1.0 INTRODUCTION

The purpose of this attachment is to address the Invensys position in regard to NRC Interim Staff Guidance (ISG) ISG-02 (Reference 1) and ISG-04 (Reference 2) and other related regulatory standards and guidance.

The philosophy of Diversity and Defense-in-Depth (D3) analysis is a multi-layered approach to safe plant operation. It includes multiple physical boundaries between the fuel and environment, redundant paths and equipment to provide core cooling, and qualified control and monitoring systems for safe shutdown and long term cooling of the reactor, as defined in Nuclear Regulatory Commission (NRC) Branch Technical Position (BTP) 7-19 (Reference 6), with additional details and clarifications provided in ISG-02.

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 shipboard, power generation, and now with the endorsement of the NRC by Safety Evaluation Report (SER, Reference 8), dated December 12, 2001, nuclear power and processing plants subject to NRC licensing. The Invensys Tricon V10 Equipment Qualification Summary Report (EQSR, Reference 13) 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.

Applicable systems 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

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

To create a site-specific application, the licensee must identify differences between Tricon application guides and each unique application. It is expected that the licensee will add, delete,

modify, or confirm requirements to support the system licensing basis. It is also expected that the licensee will oversee the development and approval of:

- the functional requirements for the application;
- design-specific defense-in-depth and diversity approach (with license topical reports if Reactor Protection System (RPS) and/or Engineered Safety Features Actuation System (ESFAS));
- selection of Tricon power supplies, communication, and I/O modules;
- the quality control requirements for application software;
- system assembly and Factory Acceptance Testing;
- installation and Site Acceptance Testing; and
- NRC regulatory requirements and guidelines specific to the application.

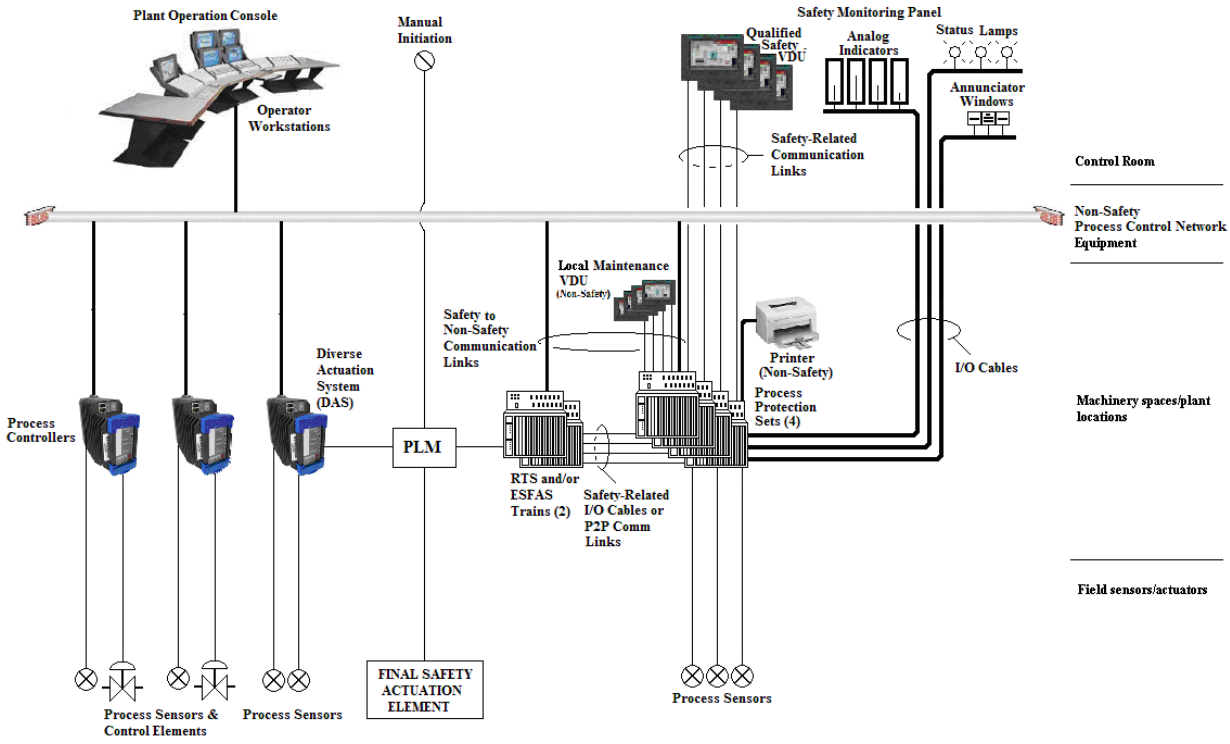


Figure 1. RPS-ESFAS Composite Architecture

While the Tricon 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 because of its many features. The figure is not proposed for any specific plant architecture, but is presented for discussion purposes of how

Tricons may be applied in reactor protection applications in compliance with regulatory requirements and endorsed industry standards.

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 components in separate cabinet(s), monitor critical plant process sensors. The Tricons 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 Tricons, or the Reactor Trip System (RTS), and the ESFAS 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[1] (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 are mounted in a remote Tricon chassis to provide physical separation and ensure electrical isolation.

The Tricon supports optional qualified Safety Visual Display Units[2] (SVDU) or Safety 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

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

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.

1.1 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
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	Safety 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 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, 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 position. Each logical slot provides two physical spaces for modules, one for the active module and the other for its optional hot-spare module.

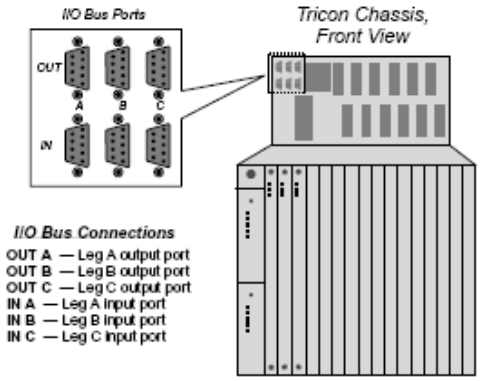


Figure 2. I/O Bus Ports

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 2 shows the arrangement of the connectors on the chassis.

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 associated regulatory issues described in ISG-04 are addressed in Appendix 2, "Additional Details on the Operation of the V10 Tricon Remote Extender Chassis."

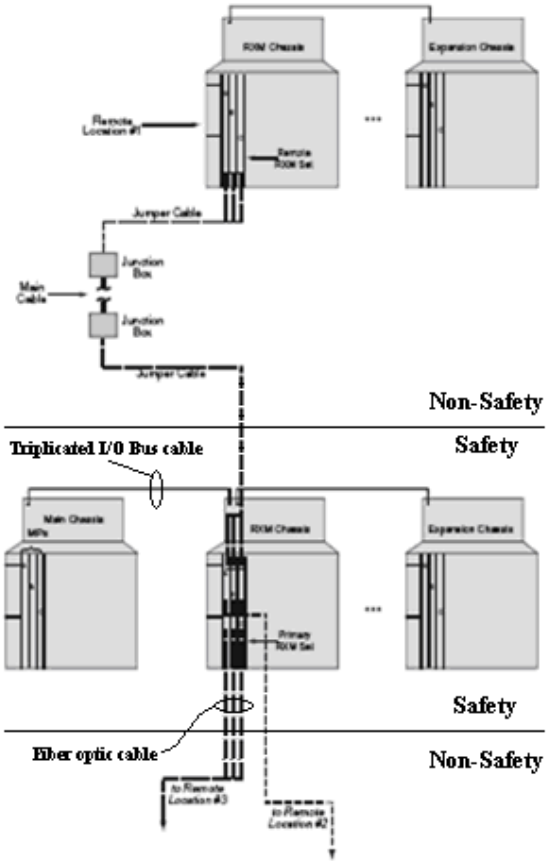


Figure 3. Safety-Related System with Non-Safety Remote Location

Figure 3 provides 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.

2.1 V10 Tricon System Bus Architecture

The V10 Tricon 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[3], as shown in Figure 4, 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

[3]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.

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 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 Communication Modules (TCMs) via the Communications Bus (COMBUS).

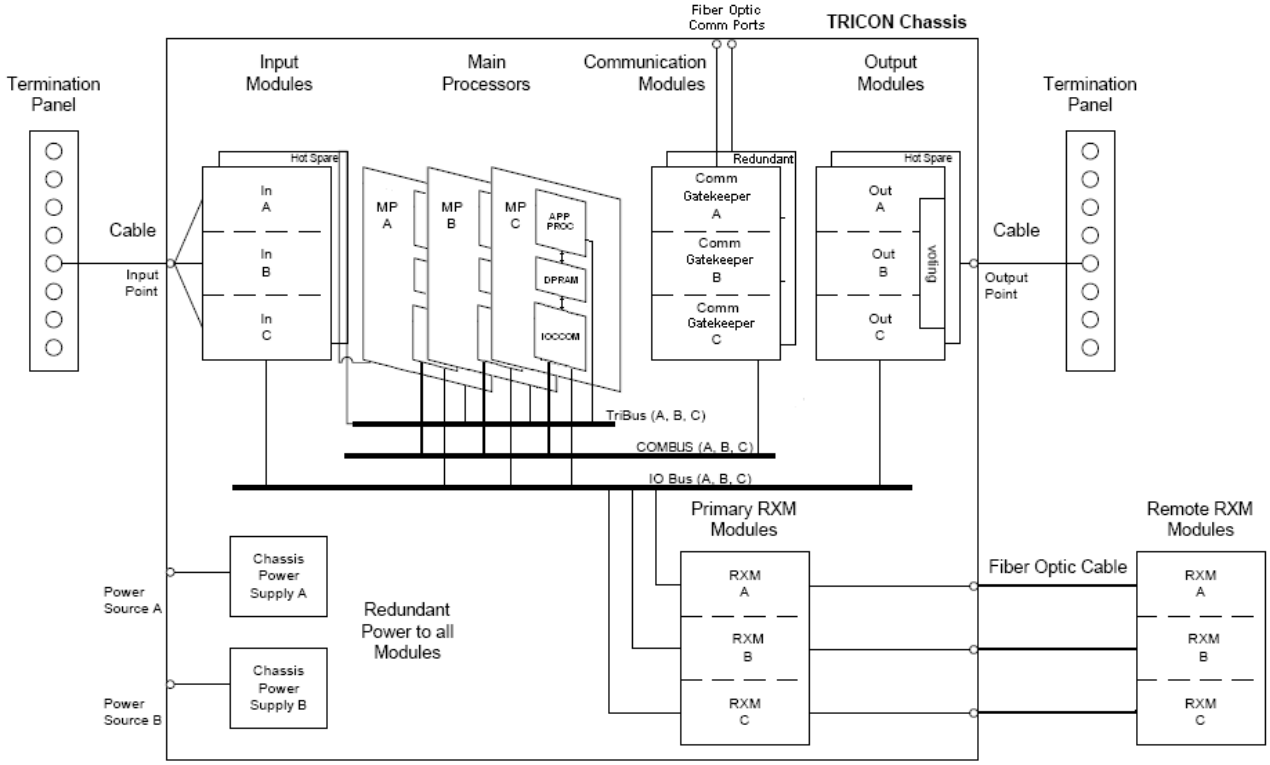


Figure 4. Simplified Block Diagram of the V10 Tricon System

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. From a programming perspective, the Tribus is inaccessible to the Application Engineer during development of the application program and to the user during run time. No changes can be made to the Tribus at run-time.

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[4] 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. However, legs on a spare I/O module only “listen” to IOCCOM requests to and responses from the active I/O module.

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

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 2). 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 3). The primary RXM chassis would be connected locally to the Main chassis via copper cables. For the remote RXM chassis, the triplicated I/O 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, and network communications are not transmitted via the multi-mode fiber optic cable.

The RXM modules provide immunity against electrostatic and electromagnetic interference. Since the RXM modules are connected with fiber optic cables, they may be used as Class 1E-to-non 1E isolation devices between a safety-related main chassis and a non safety-related expansion chassis.

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). The associated regulatory issues described in ISG-04 are addressed in Appendix 2, “Additional Details on the Operation of the V10 Tricon Remote Extender Chassis.”

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 at run-time. Therefore, TCM functionality is discussed in additional detail in the overall discussion of Tricon communications. Conformance of the Tricon communications features to ISG04 is treated extensively throughout the remainder of this document.

3.0 V10 TRICON 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 16). 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.

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 Foxboro 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 next section. The associated regulatory issues described in ISG-04 are addressed in Section 5.0, DI&C-ISG-04 "Highly-Integrated Control Rooms – Communications Issues".

3.1 Safety-to-Safety Communications

Typical safety-to-safety architectures will involve connections between safety-related Tricons or between Tricons and qualified safety-related VDUs (SVDUs). In the context of Figure 1, above, 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, depending 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.

3.2 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 5 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.

The essential feature of this configuration is the one-way-link (OWL) device between the safety-related Tricon controller and the Gateway computer. One example of an approved OWL device is the NetOptics Aggregator Tap (model number PA-CU) previously reviewed and accepted by NRC (Reference 9) 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. Again, 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.

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 highly 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.

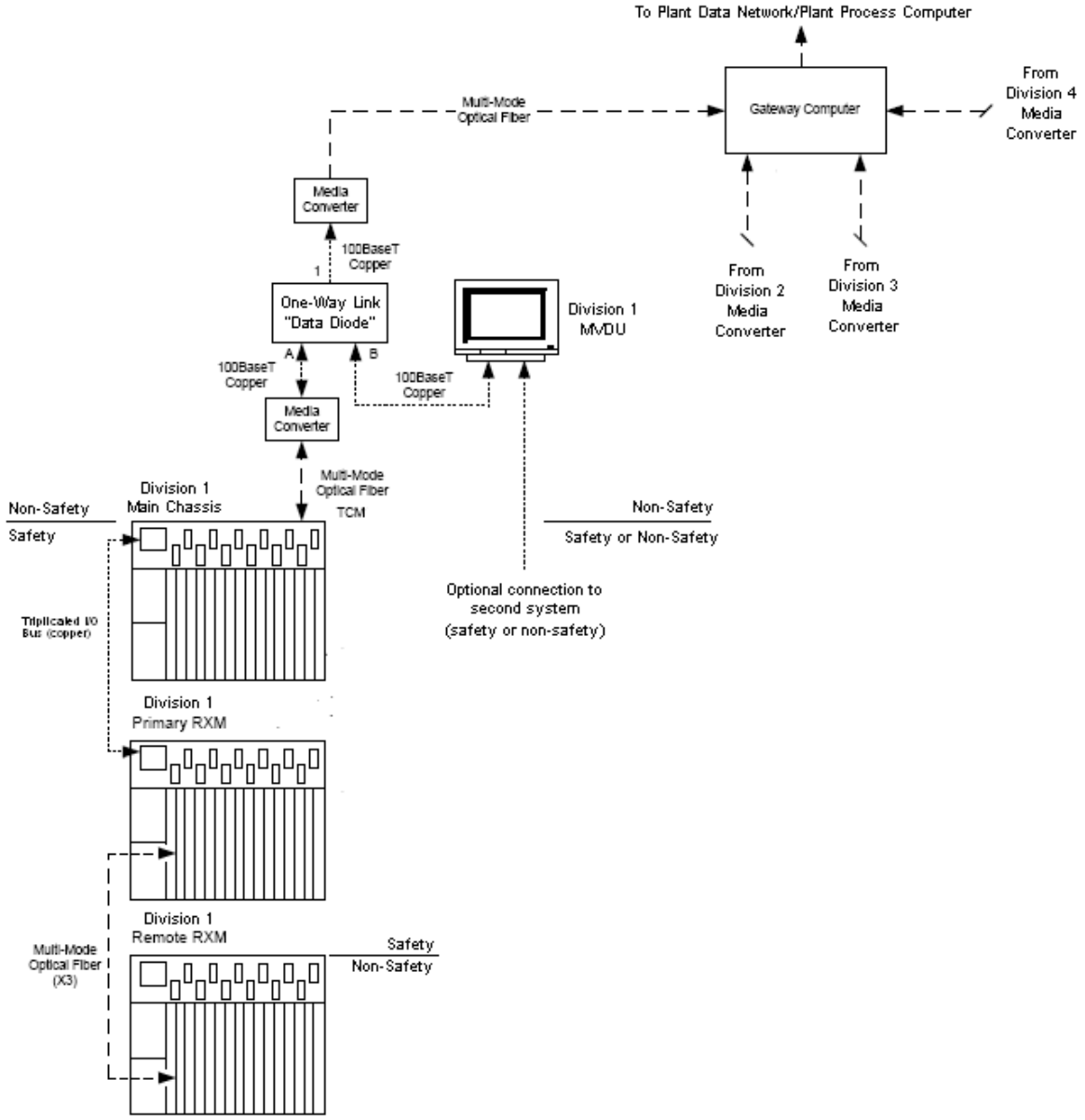


Figure 5. Safety-to-Nonsafety with MVDU and One-Way Link(s)

A potential variation on the configuration in Figure 5 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.

3.3 Hybrid Safety and Non-Safety 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 maintain traceability to the V10 Tricon nuclear qualification. Therefore any configuration in conflict with Invensys guidance would be the responsibility of the licensee/applicant.

4.0 DI&C-ISG-02 "DIVERSITY AND DEFENSE-IN-DEPTH ISSUES"

The following compares NRC ISG #2 position and Invensys compliance and comments in a point by point matrix.

NRC GUIDANCE – ISG-02	Deviation	INVENSYS COMPLIANCE & COMMENTS
#1 ADEQUATE DIVERSITY	None	Diversity is one aspect of D3 relied to mitigate the consequences of extremely unlikely Common Cause Failure (CCF) in RPS/ESFAS applications. Because a CCF is not a design basis event, the alternate shutdown means need only be adequately robust consistent with 10 CFR 50.62. Depending on the specific plant RPS/ESFAS application, Tricon based system designs make extensive use of advanced technology (i.e., equipment and design practices). These designs are significantly and functionally different from current operating plant analog practice, including the use of Tricons, microprocessor based operator indicators and displays, fiber optics, multiplexing, and different isolation techniques to achieve sufficient independence and redundancy. Upon support and approval by the licensee, Invensys conducts D3 analysis of new and replacement RPS/ESFAS applications in conformance with NUREG/CR-6303 (Reference 7), IEEE Std. 279-1971(Reference 10) or IEEE Standard 603-1991 (Reference 11), Reg. Guide 1.152 Rev. 2 (Reference 4) and BTP 7-19 (Reference 6). When included in the design, the DAS, composed of diverse hardware and software, independently monitors plant process parameters and automatically initiates protective actions. Given that it independently monitors all plant process parameters, the DCS may serve as the DAS. It utilizes hardware and software technology that is diverse from the Tricon and therefore not considered susceptible to the

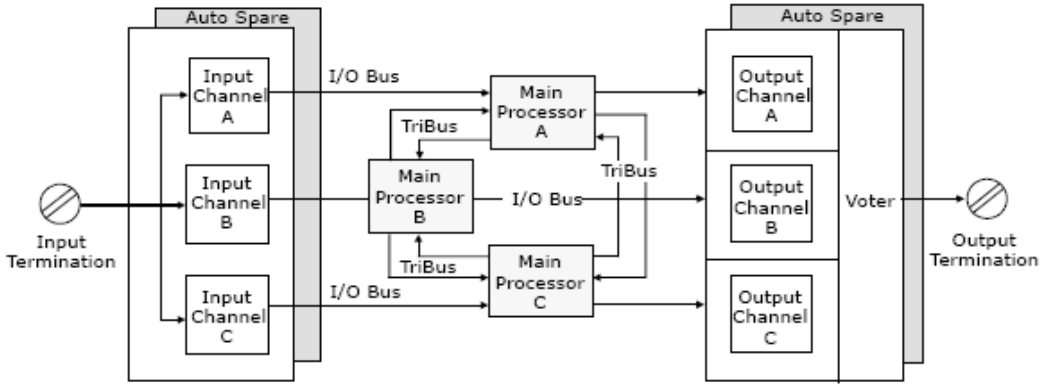
NRC GUIDANCE – ISG-02	Deviation	INVENSYS COMPLIANCE & COMMENTS
		same CCF. DAS designated components are configured and programmed to automatically initiate reactor shutdown and activate cooling equipment when accident conditions are sensed. The DCS also provides independent and diverse plant information displays in support of manual initiation. Another implementation may use a specifically designed DAS to actuate RPS/ESFAS equipment, provided it independently monitors plant process parameters, automatically initiates protective actions and is designed and manufactured in accordance with Generic Letter 85-06 "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related" (Reference 3).
#2 MANUAL OPERATOR ACTIONS	None	Upon support and approval by the licensee, Invensys conducts a human factors engineering (HFE) analysis to confirm that operators are able to observe and maintain safe plant parameters, and take action within an acceptable time, determined by following the realistic analysis described in BTP 7-19. For actions with limited margin, such as less than 30 minutes between time available and time required for operators to perform the protective actions, a higher level of analysis will be performed. Within the RPS/ESFAS architecture, independent displays are always available to the operator in the control room. Safety-related parameters are viewed at the "Safety Parameter Display Console" or other dedicated panel. Display technology may be conventional analog indicators and status lamps, controlled by Tricon analog and discrete output modules. Displays may be non-dedicated, nonsafety VDUs, which are configured and programmed to "read" plant process information from each Tricon using nonsafety-related communication media and protocols. Displays may also be microprocessor based Safety VDUs, which are configured and programmed to "read" plant process information from each Tricon using safety-related communication media and protocols.

NRC GUIDANCE – ISG-02	Deviation	INVENSYS COMPLIANCE & COMMENTS
		As illustrated in Figure 1, manual operator action is supported in all Invensys-designed RPS/ESFAS architectures. The operator may view plant process information at independent displays – Safety Parameter Display Console (analog or digital display) and the Plant Process Computer and/or DCS VDUs. Manual safety initiation is independent of both systems.
#3 BTP 7-19 POSITION 4 CHALLENGES **AND** **#4 EFFECTS OF COMMON CAUSE FAILURES.**	None	All replacement Invensys designed RPS/ESFAS architectures proposed for current operating reactors and all new reactors follow the guidelines of BTP 7-19. All support diverse automatic and manual initiation of safety functions at division level and at the individual component level.
#5 COMMON CAUSE FAILURE (CCF) APPLICABILITY	None	All Invensys proposed RPS/ESFAS conceptual designs are composed of multiple Tricons, which have been analyzed for CCF and a loss of protection. It is recommended to all nuclear owner/operators who select the Tricon for a partial or full RPS/ESFAS application, to perform a full BTP 7-19 analysis to defend both the diversity and defense-in-depth justification for the platform configuration chosen.
#6 ECHELONS OF DEFENSE	None	Invensys offers several conceptual RPS and ESFAS designs; all using the flexible Tricon in four protective channels, two RTS trains, and/or two ESFAS trains. Some architectures combine RTS and ESFAS functions into redundant trains. All configurations meet the analysis requirements of BTP 7-19, NUREG/CR-6303 and ISG-02.
#7 SINGLE FAILURE	None	The Tricon design achieves the requirements stated in General Design Criteria (GDC) 21 – single-fault tolerance and on-line repair. Fault

NRC GUIDANCE – ISG-02	Deviation	INVENSYS COMPLIANCE & COMMENTS
		tolerance is achieved by means of its Triple-Modular Redundant (TMR) architecture, from input modules through the main processors to the output modules. It provides error-free, uninterrupted control in the presence of either hard failures of components, or transient faults from internal or external sources. Extensive diagnostics continually evaluate system performance and when component fault/failure is discovered, system alarms are activated, capturing the attention of operators and technicians. A more detailed description of the system is provided in the Tricon Technical Product Guide (Reference 14), and the Tricon Planning and Installation Guide (Reference 15). Since the first safety system installation in the mid 1980s, the Tricons have provided safe and reliable operation in numerous safety critical applications. With more than 9,000 units currently in service, accumulating more than 500,000,000 operating hours, no Tricon has ever failed to operate on demand, either an actual demand or simulated during surveillance testing. However, Invensys understands there remains the very rare possibility of a software CCF. Since digital system CCFs are not classified as single failures, postulated digital CCFs are not assumed to be a single random failure in design basis evaluations, as stated in ISG 02, #7. Invensys recommends full design analysis following BTP 7-19 for partial or complete RPS/ESFAS upgrades or installations including best-estimate techniques to evaluate the effects of digital system CCFs coincident with design basis events.

5.0 DI&C-ISG-04 "HIGHLY-INTEGRATED CONTROL ROOMS – COMMUNICATIONS ISSUES"

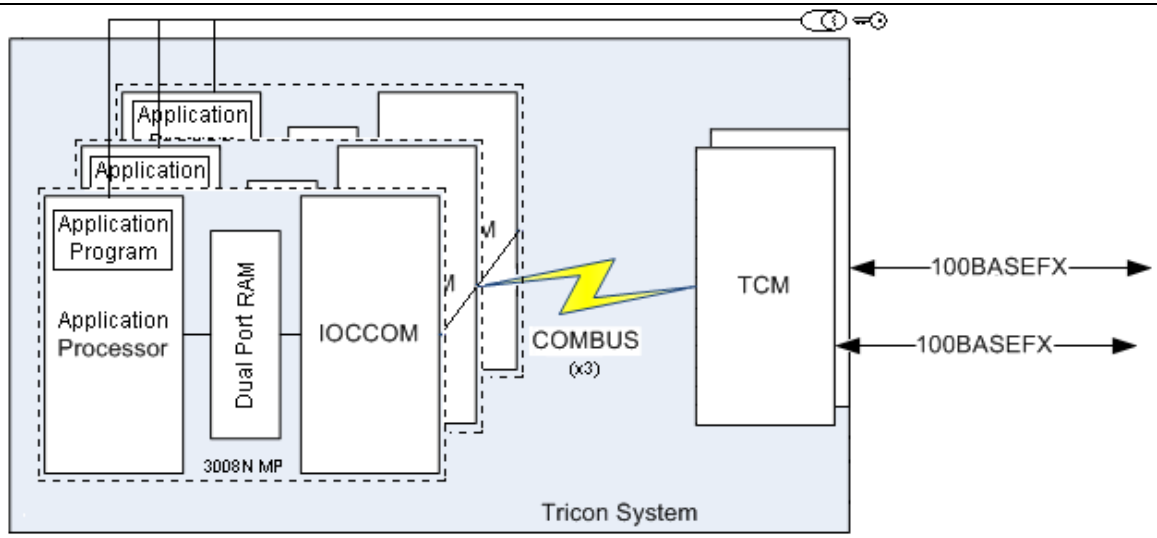
The following compares NRC DI&C-ISG-04 position and Invensys compliance and comments in a point by point matrix.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
#1 INTERDIVISIONAL COMMUNICATIONS		
STAFF POSITION 1 A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.	None	Architectures proposed in this position paper are composed of multiple divisions, and perhaps multiple channels within each division (a "Tricon-channel"). Each Tricon-channel monitors dedicated sensors allowing bistable logic within the Tricon to operate completely independent of other Tricon-channels/divisions. As shown in the figure below, the termination panels pass input signals from the field to an input module or pass signals generated by an output module directly to field wiring.  During each execution of the control application, each Tricon-channel independently verifies the: • Integrity of the data path between the 3008N Main Processors; • Proper voting of all input values; • Proper evaluation of the control application; and

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		• Calculated value of each output point. Each 3008N Main Processor (MP) module uses memory data comparison between itself and the other MPs to ensure that the control program executes correctly on each scan. Each MP transfers its input point data to the other two MPs via the TriBus during each scan. Each MP then votes the input data and provides voted data to the control program. The results of the control program (outputs), including all internal variables, are transferred by the TriBus. If a mis-compare is detected, special algorithms are used to isolate the faulting MP. The faulting MP enters the failsafe state and is ignored by the remaining MPs. Background diagnostics test MP memory and compare control program instructions and internal status. The integrity of the TriBus is continuously monitored and verified independently by each MP. All TriBus faults are detected within the scan associated with the TriBus transfer. Fault isolation hardware and firmware causes the MP with the faulting TriBus to enter the fail-safe state. Tricon I/O modules have their own processors, each of which is protected by an independent watchdog that verifies the timely execution of the I/O module firmware and diagnostics. If an I/O processor fails to execute correctly, the I/O processor enters the fail-safe state. The I/O bus transceiver and all outputs for the faulting Tricon-channel are disabled, leaving all outputs under control of the remaining healthy Tricon-channels. Furthermore, the integrity of the I/O bus is continuously monitored and verified independently by each Tricon-channel. A catastrophic bus fault results in the affected I/O module Tricon-channel reverting to the fail-safe state in less than 500 milliseconds (0.5 seconds), worst case. Digital output (DO) modules use output voter diagnostics (OVD). Under system control, each output point is commanded sequentially to both the energized and de-energized states. The forced state is maintained until the value is detected by the system or a time-out occurs (500 microseconds, typical case; 2 milliseconds, worst case). Using the integral OVD capability, each point can be independently verified for its ability to transition to either state. The OVD is executed in TMR mode, thus assuring nearly 100 percent fault coverage and fail-safe operation under all single-fault scenarios.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		Analog output (AO) modules use a combination of comparison and reference diagnostics. Under system control, each Tricon-channel is given control of the output sequentially using the Tricon's 2oo3 voting mechanism. Each Tricon-channel independently measures the actual state of an output value by comparing it with the commanded value. If the values do not match, a Tricon-channel switch is forced by voting another Tricon-channel. Each Tricon-channel also compares its measured values against internal references. Using these diagnostics, each Tricon-channel can be independently verified for its ability to control the analog output value, thus assuring nearly 100 percent fault coverage and fail-safe operation under all single-fault scenarios and most common multiple-fault scenarios. The above functions are self contained within each division Tricon. Safety system architectures that require voting among divisions, or have external systems that accept input from multiple divisions (e.g., Solid State Protection Systems) for voting trip signals would be site-specific. Methods for interdivisional data exchange include hardwired outputs from DO modules to DI modules, or data communication protocols Peer-to-Peer (P2P) and the Safety Application Protocol (SAP). The P2P and SAP are discussed in more detail below. In summary, these protocols validate uncorrupted message transmission between safety-related endpoints (Tricon to Tricon, Tricon to safety-related video display units) through the use of cyclic redundancy checks and/or hash algorithms depending upon the specific system architecture. Ultimately, requirements for safety system architectures involving interdivisional communications in which one division relies upon data from another division would be derived from Invensys customers and thus would warrant plant-specific reviews by the NRC staff.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 2 The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.	None	Depending on the licensee preferred architecture, bistable outputs are either communicated to other divisions, RTS and/or ESFAS via digital outputs wired to digital inputs, or via redundant P2P communications to support voting of bistable outputs (2-o-o-4, 2-o-o-3 or 1-o-o-2 taken twice). Failures or excessive delays in the redundant interdivisional communication results in 1-o-o-1 channel voting logic. Voting results control reactor shutdown, isolation, and heat removal equipment. Depending on the specific plant architecture, channel Tricons could receive read-only communication requests from the Plant Process Computer, the Plant Control Network or DCS, SVDUs, and/or 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 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 go through an approved OWL isolation device, and may utilize MODBUS TCP or the TSAA protocol. In terms of the communication pathway, as shown in the figure below, multiple layers of defense are designed into the Tricon, including the hardware, the software, and the Triconex communication protocols themselves.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		 The communication path includes the multi-mode fiber optic cable, the TCM, the triplicated Communication Bus (COMBUS), and the TMR 3008N MPs, which themselves contain the IOCCOM processor, dual-port RAM (DPRAM), and the embedded application processor that executes the control program. The TCM provides functional isolation by handling all the communications with external devices, and it has been qualified under the Invensys Appendix B program for nuclear applications. The fiber optic cable prevents propagation of electrical faults into the safety processors. In addition, the TCM has been designed for high-reliability and contributes to the overall reliability of the communication link through the use of Cyclic Redundancy Checks (CRCs), and testing has demonstrated that it will protect the safety core from network storms and other communication failures. Upon total loss of all TCMs, the safety core will continue to function. Furthermore, the Tricon has been tested by Wurldtech and it has been shown to be resilient against the communication faults listed in ISG-04 (see Invensys response to Staff Position 12).

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		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. Each 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 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. 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. 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. Another layer of protection is provided by the communication protocols at the Application Layer of the OSI protocol stack. The P2P and SAP protocols ensure end-to-end integrity of safety-critical messages. System architectures requiring data transfer between safety-related Tricons over a network would use the P2P protocol over an isolated, point-to-point network. Architectures requiring safety-critical data exchange with SVDUs would utilize the SAP. The SAP was developed to support third-party SVDUs.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		Both P2P and SAP operate at the Application Layer of the OSI protocol stack. The figure below shows conceptually how SAP messages move between a SVDU and safety-related Tricon. (P2P follows the same principle.) 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 do not rely upon the TCM(s) or IOCCOM for message integrity. 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. Certain integrity features are built into the protocols, such as message acknowledgement and negative acknowledgement (ACK/NAK). 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.

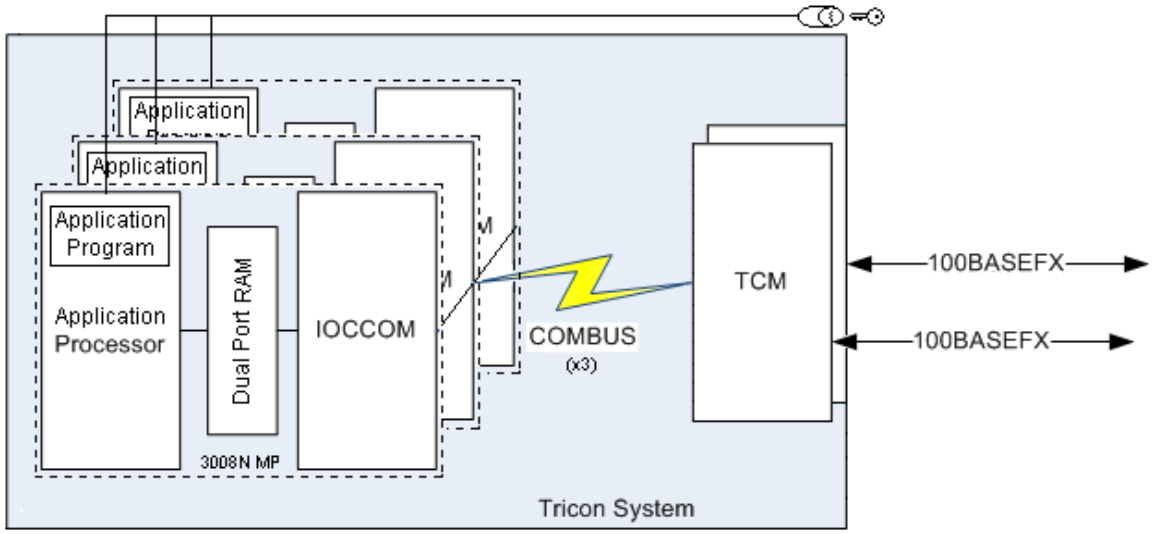
NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		a, b **SAP End-to-End Integrity** Invensys document "Safety Considerations Guide for v9-v10 Systems" (Safety Considerations Guide, Reference 17) contains guidance for the application engineer on implementing safety-related P2P communication networks. It should be noted that 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. P2P applications use a specific SEND function block to send data to a matching RECEIVE function block in another application. Each SEND function block has a parameter that identifies the RECEIVE function block to which it sends data. Each RECEIVE function block has a parameter that identifies the SEND function block from which it receives data. For added reliability, redundant P2P connections could be utilized, though this is not required. If multiple TCM modules are installed, all P2P paths are used simultaneously to exchange data, where the

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		failure of one path will not affect P2P communication on the other paths. The TR_PEER_STATUS function block is used to monitor the P2P paths, with path status being updated every 30 seconds. The TR_PORT_STATUS function block is used to determine whether the TCM ports are receiving P2P data. A non-safety computer will be used to upgrade module firmware and/or reprogram the application program installed on the Tricon controller(s). During these activities the Tricon keyswitch functions to take the Tricon out of service and place it into PROGRAM mode. The Tricon keyswitch is a physical interlock that controls the mode of the MPs. It prevents the TCM from accepting "write" messages when placed in the RUN position. The position of the keyswitch is continuously monitored by the TMR MPs, with the MPs voting on the detected position of the keyswitch. An annunciator window is activated in the control room when not in the RUN position. Multiple failures would be necessary in order to inadvertently allow software programming or changes to critical data values. See Invensys response to Staff Position 10 for additional details on the Tricon keyswitch.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 3 A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the	None	The design features of the Tricon allow for connections between safety-related Tricon controllers using the P2P protocol, between a safety-related Tricon controller(s) and a SVDU(s) using the Safety Application Protocol (SAP), or between safety-related Tricon controllers and non-safety devices (MVDUs, non-safety Tricon controllers, etc.). Interdivisional connectivity using hardwired digital output (DO) to Digital Input (DI) connections would be done presumably in accordance with the design basis of the plant (i.e., the new architecture based on the Tricon is the same as the original architecture), and thus would not present new technical or regulatory issues aside from any new failure modes arising as a result of using digital technology. Interdivisional communications between safety-related Tricon controllers using the P2P protocol would require specific analysis and design activities to address the technical issues arising from safety-critical communications via point-to-point network. Invensys response to Staff Positions 1 and 2 describe the generic Tricon platform design features that protect against external influences and communication errors. Issues specific to a particular application include a timing analysis of the interdivisional communication pathways to validate that required trip response times can be met, and analysis of P2P redundancy requirements and associated logic to mitigate loss of safety-critical data transmission. Additional guidance on safety-related communications is provided to the application engineer in the Safety Considerations Guide. Interdivisional communications between safety-related Tricon controllers and a SVDU or a network of SVDUs would require specific analysis and design activities to address the technical issues arising from safety-critical communications via the SAP. Invensys response to Staff Positions 1 and 2 describe the generic Tricon platform design features that protect against external influences and communication errors. Issues specific to a particular application include a timing analysis of the interdivisional communication pathways to validate that operator response times credited during an accident can be met, and analysis of SAP/SVDU redundancy requirements and associated logic to mitigate loss of safety-critical operator commands and display data. Additional guidance on safety-related communications is provided to the application engineer in the Safety Considerations Guide.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside		Interdivisional communication between a safety-related Tricon controller and a non-safety device is discussed in Section 3.2, Safety-to-Nonsafety Communications. Figure 4 presents one example of interdivisional communications with a Gateway computer via an OWL device to support plant operations and a MVDU to support maintenance activities, such as periodic maintenance, instrument loop testing, troubleshooting, etc. Under operating plant conditions the MVDU would simply display plant parameters, perhaps including division diagnostic information. Access to features beyond displaying data would be under strict administrative and physical controls. During plant outages, for example, the MVDU would be used for injecting test values and modifying trip setpoints. These activities would be performed 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. Such procedures would require manipulation of the Tricon keyswitch, discussed in Invensys response to Staff Position 2, as well as the hardware switch specific to a given instrument loop under test. In addition to the procedural and hardware controls, the application software would utilize, in the case of setpoint changes while the Tricon is in RUN mode, the safety-critical Tricon library functions “GATENB” and “GATDIS”. Upon placing the instrument-loop-specific switch in the “Open Access” position, the Tricon would activate the pre-programmed “GATENB” and “GATDIS” functions to open a data window of limited range and duration. Prior to updating the setpoint in the Tricon control program, the new value would be staged on the MVDU screen for acknowledgement. After the changes have been made and the maintenance technician has placed the switch in “Closed Access” position, or if the time duration has passed, the data window would be closed to prevent further changes. The MVDU interface would also have protective measures built in, such as password-protected log-on, role-based security features to ensure only authorized individuals change parameter setpoints, etc. Appendix 1, Non-Safety to Safety Communication Recommendation, discusses the use of the MVDU and “GATENB/GATDIS”. With regard to features that enhance the safety function and on-line monitoring, Invensys response to Staff Position 1 summarizes diagnostic features built into the Tricon. These diagnostics are not

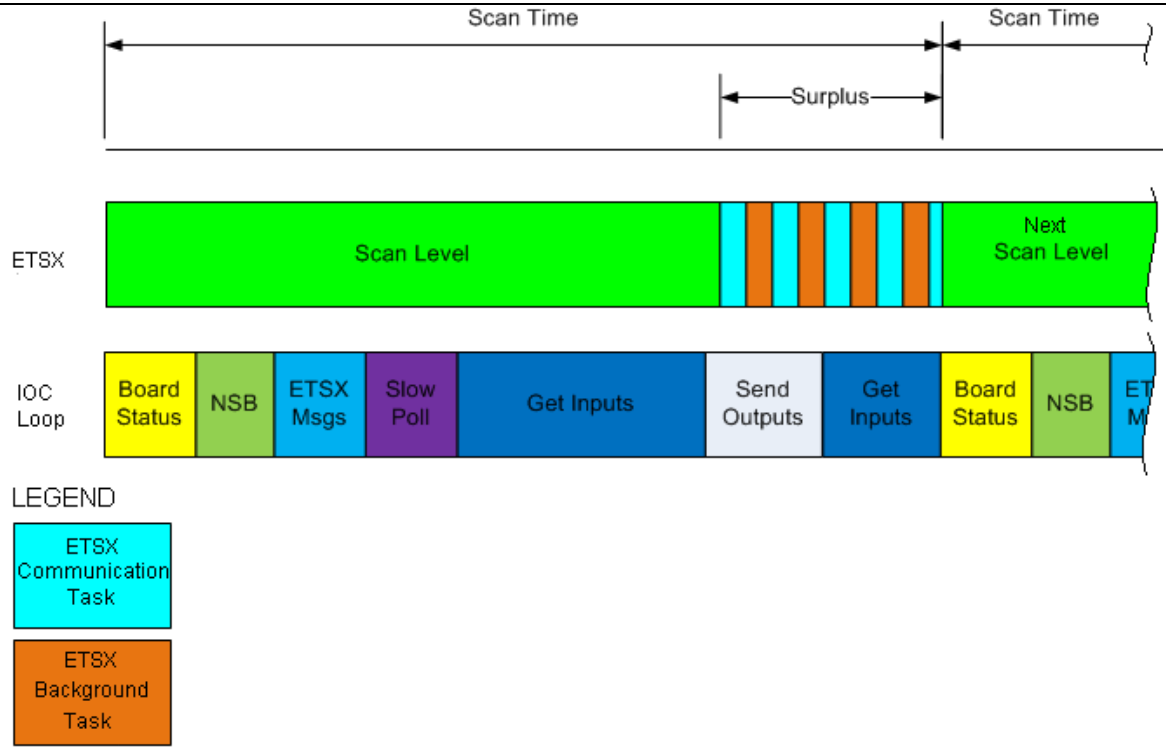
NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.		dependent upon external inputs, and contribute to the Tricon's exceptional reliability and availability. Any application software functions related to on-line monitoring would be plant-specific and would require additional NRC scrutiny if intended for safety-related use.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 4 The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-	None	As described in the EQSR, all Tricon communication with external devices is conducted and supervised by one or more separate Tricon Communication Modules (TCMs). As described, the TCMs operate asynchronously, sharing information only at end of the application processor scan. When the host device requests data, the communication processor forwards the data from the application processor received at the previous end of scan. When a host device writes data, the communication processor passes the data to the application processor at next end of scan exchange. A simplified view of the Tricon system is shown in the figure below.  The TCM provides functional isolation by handling all the communications with external devices, and it has been qualified under the Invensys Appendix B program for nuclear applications. The fiber optic cable prevents propagation of electrical faults into the safety processors. In addition, the TCM has been designed for high reliability and contributes to the overall reliability of the

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the		communication link through the use of Cyclic Redundancy Checks (CRCs). 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). The internal communication path includes the TCM, the triplicated Communication Bus (COMBUS), and the TMR 3008N MPs, which themselves contain the IOCCOM processor, dual-port RAM (DPRAM), and the embedded application processors that execute the control program. Valid messages received by the TCM are triplicated for transmission on the COMBUS to the IOCCOM, which is running at its own scan rate without the use of interrupts. The IOCCOM retrieves data from the DPRAM to send to either the I/O modules or the TCM, or deposits I/O data or communications (COM) messages into the DPRAM for use by the embedded application processor. Separate queues are provided in the IOCCOM for I/O Bus and COM messages. To ensure adequate execution time for safety-related I/O, the IOCCOM executes COM messages with the TCM only while waiting for I/O responses. The IOCCOM checks the link-level format and the CRC of all messages from the TCM. If the IOCCOM determines that the message is valid and correct, the data is placed into DPRAM. Both 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. As with the IOCCOM, the DPRAM provides separate memory areas and queues for communication messages and I/O data. These "bins" are separated according to input, output, read-only, read-write, and data type (i.e., Boolean, Reals, Integers). The DPRAM includes extensive memory protection via parity checks, CRCs, checksum, and other mechanisms. 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. Conversely, the TCM votes on the messages from

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.		the three 3008N MPs and sends a single copy to an external device if two out of three agree. The embedded application processor, IOCCOM, and TCM each runs its own scan loop (see figure below). The embedded application processor and IOCCOM are synchronized to facilitate exchange of data through the DPRAM. The main scan loop ("ETSX") of the embedded application processor consists of three tasks: 1) Scan Task, 2) Communication Task, and 3) Background Task. The Scan Task sequence is essentially: Input data from DPRAM and vote → Process control program → Send outputs to DPRAM. The Communication Task is run after the Scan Task during the "Scan Surplus" period. The embedded application processor and the IOCCOM scan loops are synchronized such that during the Communication Task the IOCCOM deposits I/O and communications messages into the DPRAM for use by the embedded application processor at the beginning of the next Scan Task. The IOCCOM scan loop ("IOC loop") gives priority to I/O data exchanges. During the IOC loop when the IOCCOM is waiting for responses from the I/O modules, scan time is allotted for COM messaging via the COMBUS.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS



In summary, the combination of prioritizing execution of the control program and I/O data exchange over communications messaging, layers of integrity checks, interface through the DPRAM, and reliable TCM design provide reasonable assurance that communications from devices external to the Tricon cannot delay or corrupt the safety function.

See Invensys response to Staff Position 3 regarding application programming of safety-related protocols P2P and SAP to ensure process timing requirements are met.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 5 The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.	None	Invensys response to Staff Position 1 explains that Tricon controllers are qualified TMR systems and are not dependent upon interdivisional communications or external systems to perform the safety function. For those system architectures involving safety-critical network communications between Tricon controllers, an analysis of the safety process (e.g., the plant safety analysis) will be necessary to ensure that the point-to-point data exchange meets the timing requirements of the safety process. The analysis will require consideration of the Tricon controller scan loop, as well as the point-to-point network delays. Invensys response to Staff Position 4 describes the scan loop for the Tricon controller. To summarize, the TMR 3008N MPs and TCM exchange messages asynchronously over the triplicated COMBUS. On board each 3008N MP, the embedded application processor and IOCCOM processor exchange data via a 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. Data is deposited into DPRAM at the end of the embedded application processor Scan Task, which the IOCCOM processor retrieves during its own scan loop (synchronized with the embedded application processor scan loop). During surplus scan time the Communication Task is run and the embedded application processor retrieves messages from the DPRAM in preparation for the next Scan Task. Priority is given to the control program and I/O data exchanges, with communication message exchanges with the TCM via the COMBUS occurring between scans. In general, because all data is exchanged at each End-of-Scan, communication message exchanges may require multiple scans to satisfy a host device (such as a Tricon, SVDU, or other device on the DCS) read or write communication function. Additional time (at least two scan loops) is required for a sending Tricon controller to get an acknowledgment from the receiving Tricon controller that the message has been acted on. In fact most messages from an external host require voting by the TMR 3008N MPs, thus typical message response times require three or more scans to complete – one scan to send and two scans for the response. Exceptions to this are MODBUS and TSAA "read" requests. Typically MODBUS or TSAA requests would come from a DCS device, Operator Display VDU, or MVDU for data display or diagnostics. These are not safety

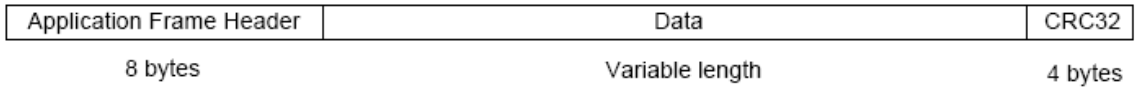
NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		critical and pose no threat to the safety function. (See Invensys response to Staff Position 7.) The Invensys protocols used for safety-critical communications, P2P and SAP, are briefly discussed in previous sections of this position paper, as well as in Invensys responses to Staff Positions 1 and 2. The SAP and P2P protocols are responsible for the end-to-end integrity of safety-critical communications, and thus will be implemented by the application engineer during plant-specific application software development. Because of the additional functions these protocols specify at the Application Layer to protect communications, P2P and SAP will place a burden on the application processor and therefore extend the Tricon controller scan time. Invensys documents, such as the Safety Considerations Guide, the "Communication Guide for Tricon v9-v10 Systems" (Communication Guide, Reference 18), and the "TriStation 1131 Developer's Guide" (Reference 19) provide guidance on proper configuration of these protocols. Using P2P as an example, the guidance covers: 1) P2P port configuration – a single TCM can support multiple connections, both network and serial connections. The guidance explains how to set up the network port for P2P communications. 2) Memory allocation – P2P requires a SEND function block at the sending node and a RECEIVE function block at the receiving end. Total transfer time between two P2P nodes is partially determined by the P2P memory requirement calculation of: 1) total bytes sent by the sending Tricon controller; and 2) total bytes received by the receiving Tricon controller. This calculation feeds into the overall transfer time calculation. 3) Point-to-point transfer time – The guidance includes a method to calculate the estimated time required for transferring P2P data between endpoints (including receiving-node acknowledgement). The calculation is based on: 1) total bytes sent and received (determined in item 2, above); 2) COMBUS transfer time; 3) the number of P2P SEND and RECEIVE function blocks in an application; and 4) both the sending and receiving Tricons' scan time. The calculation takes into account whether multiple scan loops are required for all communications (P2P, SAP, MODBUS, etc.). Consideration is also given to the number of

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		Tricon controllers on the P2P network (if more than two). 4) Discussion of restrictions and limitations to ensure appropriate use of P2P in safety-related applications. For example, the Tricon controller is limited to a maximum number of P2P "reads" and P2P "writes" within a given scan, which limits the application processor burden. Guidance on the SAP will be similar for safety-critical communications between Tricon controllers and SVDUs. Transfer times will be used in the safety analysis to ensure safety-critical timing requirements are met by the P2P and SAP communications. The Tricon continuously monitors system health and performance, activating an alarm should scan time exceed the predicted performance. Should P2P or SAP communications be included in an application program, thorough program operational testing will be conducted to determine the longest scan-time duration. Application development will be performed in accordance with the Invensys Appendix B quality program and the approved Nuclear System Integration Program Manual (NSIPM, Reference 20).

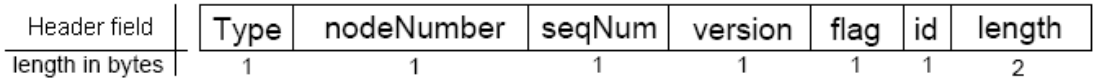
NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 6 The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	None	For the Tricon controller, the 3008N MP acts as the safety function processor in a Triple-Modular-Redundant configuration. Invensys response to Staff Position 1 explains that Tricon controllers are qualified TMR systems and are not dependent upon interdivisional communications or external systems to perform the safety function. This would include interrupts from external systems. The TMR 3008N MP application processors are isolated from data communications by the TCM. One or more TCM(s) act as the communication processor(s) to handle all communication protocol requirements, i.e. handshaking, start, stop bits, etc. Invensys responses to Staff Positions 2 and 4 describe in detail the electrical and functional isolation provided by the TCM, reliable design of the TCM, and the several engineered layers of protection against communication failures. The engineered safety and reliability features of the Tricon provide reasonable assurance that communication failures will not adversely impact the safety function.
STAFF POSITION 7 Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function	None	All host communications are limited to Tricon-compatible protocols, briefly discussed in Section 3.0, V10 Tricon Communications. Each protocol is well-defined and -ordered, e.g. number of start and stop bits, timing, data frame format, number of data fields and check sum or Cyclic Redundancy Check (CRC) field. Should an error occur, the communication processor rejects the message. Message length may vary, however, as a host device may request a different number of data points within each request. MODBUS TCP: The MODBUS TCP protocol functions at the Application Layer of the OSI protocol stack. MODBUS is an industry-standard master/slave protocol that is defined in the open literature. Because of its extensive use for energy management, transfer line control, pipeline monitoring, and other industrial processes protocols, Invensys has implemented a standard Tricon library containing function blocks that the application engineer can use for non-safety MODBUS communications with a Tricon controller. MODBUS has a pre-defined message format, though message lengths vary depending on Function Code, as shown in the figure below.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.		**RTU Mode** Bytes 1 2 3 4 5 6 7 8 Station Address | Function Code | Data | Data | CRC **ASCII Mode** Bytes 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 : | Station Address | Function Code | Data | Data | LRC | CR | LF **MODBUS message formats for RTU and ASCII modes** More information on MODBUS can be found in the open literature, as well as the Invensys Communication Guide. See Invensys response to Staff Position 9 regarding how variables are organized on the Tricon controller and accessed by external hosts using MODBUS aliases. TSAA: Tricon System Application Access (TSAA) is an Invensys protocol that also functions at the Application Layer of the OSI protocol stack. However, it is transparent to the Tricon application engineer and system user/operator, as it does not require Tricon application programming. It is primarily used by external devices to request Tricon system variables or for retrieval of Tricon data points by HMIs/VDUs. It is not intended for safety-critical data communications, and thus does not impact the safety function upon failure. The TSAA protocol has a predefined message format, as show in the figure below. Message length is dependent upon the Type field, which determines the data contained in the (variable length) Data field.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS



TSAA frame format



TSAA Application Frame Header format

The following fields are contained in the Application Frame Header:

- Type: Determines the TSAA message type, such as read/write request, read/write acknowledgement, system status request/acknowledgement, etc.
- nodeNumber: Contains the node address of the destination (receiving) Tricon controller
- seqNumber: Identifies the number of the message in a multiple-message response. This field can help determine if there are missing messages.
- version: The version field identifies the version number of the protocol used by the sender, set to 0 for Tricon controllers.
- flag: The flag field is a bit field that indicates the position of the frame in a multi-frame message (first, middle, last frame), or that the message is a single frame.
- id: A number assigned to a request and its associated response. If a client makes periodic requests of the same message type and wants to associate them with the responses, this field is used to assign an identifier. The request and response use the same identifier.
- length: The length of the frame in bytes, excluding the CRC32 field.

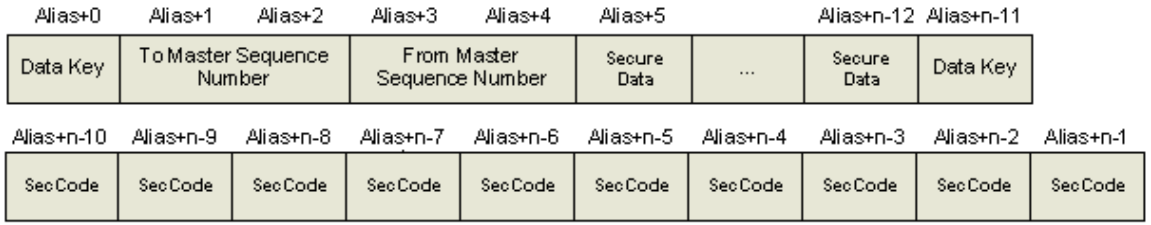
NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		Data: Variable-length data, depending on Type field. See response to Staff Position 9 regarding how variables are organized on the Tricon controller and accessed by external hosts. CRC32: The 32-bit CRC of the TSAA message frame. NOTE: Because of how variables are organized in the Tricon controller's memory, MODBUS and TSAA reads require less overhead to complete. These read requests can generally be completed within a single scan loop of the responding Tricon controller. See Invensys response to Staff Position 9 regarding how variables are organized on the Tricon controller and accessed by external hosts. a, b

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS

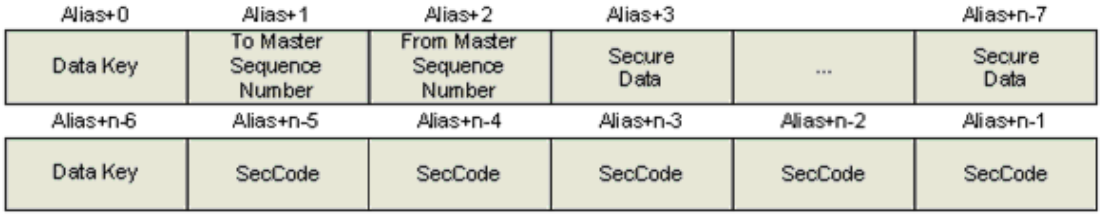
a, b

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		a, b SAP: The SAP functions at the Application Layer of the OSI protocol stack. The application engineer will use safety-related Tricon library function blocks to implement SAP communications between safety-related Tricon controllers and SVDUs. SAP uses a NIST-published cryptographic algorithm to ensure the end-to-end integrity of safety-critical data embedded in either MODBUS or TSAA messages. The figure below depicts the message format for MODBUS and TSAA with embedded SAP payloads.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS



MODBUS - SAP payload



TSAA - SAP payload

Data Key: Indicates the start and end of protected data in the payload, and provides identification of the data. The Data Key will be checked for the correct value to ensure the data is valid. The Data Key will be unique for each Modbus Safety Message. Configured by the application engineer during application programming with the SAP function block library.

To/From Master Sequence Number: There is a sequence number for each direction of data transmission to and from the master. The sequence numbers are incremented each time a message is sent. The sequence numbers are used for detection of missed, late, or duplicated messages. The sequence numbers are also used to detect loss of communication. Any discrepancies during the compare will result in the message being discarded.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		SecureData: These fields contain the safety-critical data; The amount of secure data to be transferred is dependent upon the Function Code (MODBUS) or the Type (TSAA) field. See the description of the applicable protocol for an explanation of those fields. SecCode: The value calculated using the NIST-published cryptographic algorithm to ensure end-to-end integrity of the message – any change to the message will, with a very high probability, result in a mismatch at the receiving node. The calculation is done across the message including the Data Key, To and From Master Sequence Numbers, and SecureData. If the calculated SecCode at the receiving node does not match the SecCode in the message, the message will be discarded. The end-to-end integrity calculation of the SAP provides reasonable assurance that errors in the safety-critical communications will not adversely affect the safety function. Each application processor responds and replies only when all data is correct. See Invensys response to Staff Position 12 on how P2P and SAP provide mitigation of the various communication errors. It should be noted that for P2P and SAP in particular that the checks performed by the TCM and the lower layers of the OSI protocol stack are not credited in the safety analysis. These additional checks do, however, provide additional communications reliability, and are considered relevant to diversity-and-defense-in-depth analyses.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 8 Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	None	As discussed above in Invensys response to Staff Position 2, data communications with non-safety systems are supervised by the Tricon communication processor (TCM). The non-safety system may request any data points and the TCM will reply if the request is valid and error free. Data "writes" from the non-safety system to the Tricon are only accepted if: • The data is valid and error free; • The main chassis keyswitch is in correct position; and • The specific memory tag name attribute is configured as 'writeable'. Note that governing site-specific administrative and physical access controls are followed during activities requiring writes to Tricon controllers (such as during maintenance outages). The majority of cases would not require data "write" requests during normal (i.e., at power) operations. Activities or applications requiring "write" requests at power would be governed by site-specific procedural controls and would require further NRC review and approval. Interdivisional communication is discussed in Invensys response to Staff Positions 1 and 2, specifically how the Tricon controller design features provide reasonable assurance that the safety function will not be adversely impacted by failures of external devices/systems. With regard to communications between safety divisions, whether between Tricons or with SVDUs in other divisions, these would be done via proprietary P2P or SAP networks. P2P messages are limited in length and number so as not to overburden either transmitting or receiving Tricon. Predetermined matching message blocks must be programmed in both the sending and receiving Tricons. Each message contains sending and receiving identification, fixed number of data fields, fixed data type, and extending error check coding. The SAP ensures end-to-end integrity using a NIST-published cryptographic algorithm, predetermined matching message blocks, sending and receiving node identification, fixed number of data fields, and fixed data type. Flexibility is provided, as the SAP can be used with third-party SVDUs with the use of an application programming interface (API). Application programming of the P2P and the SAP communications links will be done in accordance with Invensys Appendix B quality procedures and the approved Invensys NSIPM. See Appendix 1 on Invensys guidance on non-safety to safety system communications.

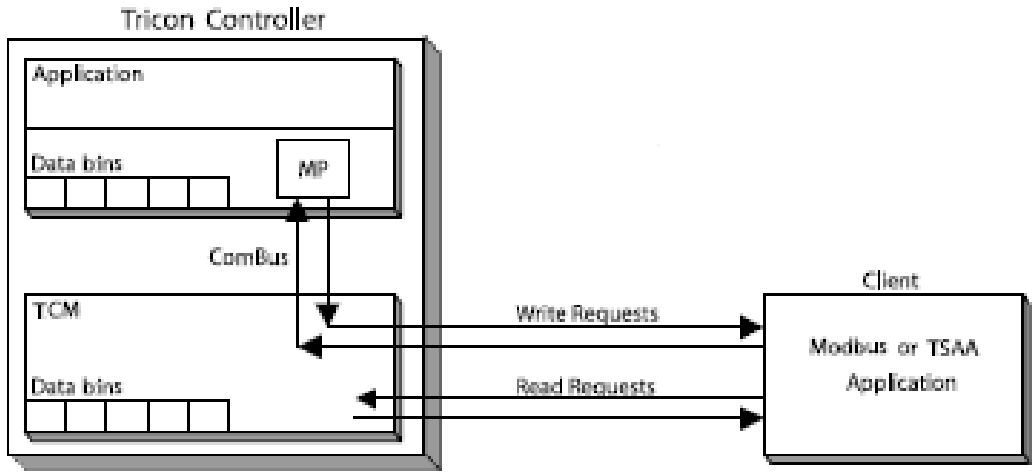
NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 9 Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.	None	Tricon received data is stored in fixed aliased memory locations, which are utilized by the application processor when computing application logic. Input data is segregated from output data within memory, as discussed below. All communication messages, via host (including SVDU using the SAP) or P2P, are conducted by, and stored in separate communication processors. Data is exchanged with the application processors at the end of each application program scan. Invensys response to Staff Positions 4 and 5 discuss the separate Tricon communications processor (i.e., the TCM) and details on the Tricon controller scan loop. To be accessed by external hosts, a variable must have a unique identifying integer value known as its *alias*. The TriStation 1131 application programming tool automatically assigns aliases to input, output, and system variables. The application engineer assigns aliases to memory variables, which will be done using Invensys or customer software programming guidelines. If an alias is not assigned, a variable cannot be accessed by an external host. An alias is a five-digit number that the Tricon controller uses in place of a variable name when communicating with an external host. The first digit, which is the most significant, is the MODBUS message type. There are four message types: 0 — Read/Write Discrete 1 — Read Only Discrete 3 — Read Only Register 4 — Read/Write Register The last four digits of the alias number define its hardware address in the Tricon controller and can have any value between 1 and 9999. Each type of Tricon data, such as analog inputs, is assigned an appropriate MODBUS message type and a range of points. Aliases are organized into multiple *bins*. Aliases of the same bin share certain similar properties, such as access mode (read/write), class (input, memory, output), and data type (boolean – BOOL, double integer – DINT, real – REAL). The following table shows how similar aliases are grouped into bins in the Tricon controller:

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS

Bin	Data Type	Variable Type	Message Type	Tricon Range	Bin Size
0	BOOL	Output	Read/Write	00001 - 02000	2048
1	BOOL	Memory	Read/Write	02001 - 04000	2016
2	BOOL	Input	Read	10001 - 12000	4096
3	BOOL	Memory	Read	12001 - 14000	2016
4	DINT	Input	Read	30001 - 31000	1024
5	DINT	Memory	Read	31001 - 32000	1000
6	REAL	Input	Read	32001 - 32120	120
7	REAL	Memory	Read	33001 - 34000	1000
8	BOOL	System status	Read	14001 - 19999	5999
9	DINT	System status	Read	39631 - 39999	369
10	DINT	Output	Read/Write	40001 - 40250	512
11	DINT	Memory	Read/Write	40251 - 41000	750
12	REAL	Memory	Read/Write	41001 - 42000	1000
13	Not applicable (Number of bins)				

There are 13 bins numbered 0 through 12, each containing a specific range of contiguous aliases. System configuration determines the number of data points in a bin. For example, bin 0 has a defined range of aliases from 1 through 2000. If the highest alias assigned by the application engineer in bin 0 is x ($1 \leq x \leq 2000$), the bin contains x data points (from 1 through x). This does not necessarily mean that all aliases from 1 through x have been assigned (it is common to leave unassigned aliases for expansion), but it does mean that when an external host reads the data points using bin addressing, the TRICON sends x data points.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		The figure shows the path of information flow for both Read requests and Write requests:



Message Flow Between Tricon Controller and Client

These actions occur with TSAA and MODBUS messages:

Read requests – these are directly processed by the TCM. The communication module returns data from bins which mirror the bins stored on the 3008N MPs. This data is updated by the 3008N MPs via the COMBUS at the end of each scan, during the period referred to as the scan surplus.

P2P, SAP, and Write requests – these pass through the TCM and are processed by the TMR 3008N MPs. The 3008N MPs are running the application program, and must vote these message types before processing them. For write requests, if the data items are aliased read/write variables and remote access is enabled, the 3008N MPs update data in their bins and communicate the updates to the application running on the controller and to the TCM. After voting the input from

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		the TMR 3008N MPs, the TCM then responds with a success or failure message to the client. For P2P and SAP, the Application Layer integrity checks are done prior to acting on any message from an external client, whether SVDU or peer Tricon controller. It should be noted that for safety-related applications, write requests will not be implemented with TSAA or MODBUS protocols under normal operating conditions. There will be cases where the control program may require upgrades, or instrument loop testing may result in setpoint changes. These cases will be plant-specific and thus handled under site procedural and physical access control. See Invensys response to Staff Position 10.

<table>
<tr><th>NRC GUIDANCE – ISG-04</th><th>Deviation</th><th>INVENSYS COMPLIANCE & COMMENTS</th></tr>
<tr><td>STAFF POSITION 10
Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction</td><td>None</td><td>There are several layers of protection to prevent inadvertent application program changes. These include the Tricon keyswitch, as well as P2P and SAP end-to-end integrity checks in the application program. Though non-safety related, additional reliability gains are realized by the TCM design itself (reliable design) and configuration features to prevent access from unknown network nodes. Additional protection is provided by features in the TriStation 1131 programming interface, including password access.

The Tricon keyswitch is a physical interlock that controls the mode of the 3008N MPs. It prevents the 3008N MPs from accepting “write” messages when placed in the RUN position. 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:

<table>
<tr><th rowspan="2">Position</th><th colspan="2">Value</th></tr>
<tr><th>Decimal</th><th>Binary</th></tr>
<tr><td>Stop</td><td>0</td><td>00</td></tr>
<tr><td>Program</td><td>1</td><td>01</td></tr>
<tr><td>Run</td><td>2</td><td>10</td></tr>
<tr><td>Remote</td><td>3</td><td>11</td></tr>
</table>

The keyswitch position is voted between the three 3008N MPs and the voted value is used to perform key switch functions. The application program has access to the voted keyswitch position through specialized function blocks. The application can be programmed to perform any required action on a change of the keyswitch position. For example, the application could annunciate an alarm if the keyswitch position is taken out of RUN mode.

The keyswitch design mitigates against any single hardware fault. If one of the gangs on the switch goes bad or an input to a 3008N MP fails (e.g., a single bit flip), the error would affect only the 3008N MP that is attached to the failed gang. The other two 3008N MPs would continue to receive good inputs values and out vote the 3008N MP with the bad input. This protects against</td></tr>
</table>

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not		any single fault in the physical keyswitch or on the 3008N MP. The Tricon design supports on-line changes to the application program, but only within rigid restrictions. To modify the program, the programmer must have access to the current program version loaded on the programming terminal, TriStation 1131 (TS1131). To access the program, the programmer must enter the correct password. Once the program is modified and compiled, the TS1131 terminal must be physically connected to the Tricon and the keyswitch rotated to the PROGRAM position. Using the programming terminal, the programmer opens communications with the Tricon and downloads the program. Once downloaded the Tricon automatically changes the program version number. An alarm is activated when the version number changes and the version number is visible on several control room VDUs, if so equipped. Several administrative and programming techniques prevent unauthorized on-line program alterations. The programmer must obtain cabinet and chassis keys to physically gain access to the Tricon. Licensees may wish to set control room annunciator alarms when the cabinet door and/or chassis key position is rotated out of the normal position. The programmer must gain access to the current program and password before the program may be altered, compiled and downloaded. It is anticipated that administrative procedures will restrict on-line program changes by taking the channel off-line, remove the loop from service, or place the trip in bypass before physically connecting the programming terminal to the safety channel and rotating the Main Chassis keyswitch to the PROGRAM position. Some licensees may wish to enforce this requirement by programming the Tricon to initiate program halt when the keyswitch is rotated to the PROGRAM position.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 11 Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.	None	P2P and SAP communications will be utilized for safety-critical communications. Tricon P2P and SAP messages support data exchange only. There are no "flow of control" message functions in the P2P protocol. There are no "flow of control" message functions in the SAP protocol. During normal operations, the Tricon keyswitch will be in the RUN position. Section 3.2, Safety-to-Nonsafety Communications, and Invensys responses to Staff Positions 2 and 3 discuss safety-to-nonsafety system architectures, including reprogramming of Tricon application programs. As explained in these previous responses, several layers of protection are provided in the Tricon design to prevent failures end errors from impacting the safety function. The primary protection is that the Tricon keyswitch must be in PROGRAM mode before reprogramming of the application program can occur. All "write" messages are ignored by the Tricon controller. From Invensys responses to Staff Positions 7 and 10, the Tricon keyswitch design protects against single failures to prevent inadvertent mode changes (e.g., inadvertent mode changes from RUN to PROGRAM). Invensys response to Staff Position 1 explains that Tricon controllers are qualified TMR systems and are not dependent upon interdivisional communications or external systems to perform the safety function. With the keyswitch in RUN, each Tricon is independent of other channels/divisions. As stated in the response to Staff Position 1, any architecture in which one division relies upon data from another division would be site-specific and thus would warrant plant-specific reviews by the NRC staff. Invensys responses to Staff Positions 2 and 4 describe in detail the electrical and functional isolation provided by the TCM, reliable design of the TCM, and the several engineered layers of protection against communication failures. Other layers of protection will be provided by site-specific administrative and physical access controls. For example, annunciation of alarms occurs when the access door on the Tricon rack is opened and when the Tricon keyswitch is taken out of RUN mode. Additional examples of site-specific administrative controls include procedural controls on keys to open the Tricon rack door; and administrative controls of when, how, and by whom reprogramming will be performed.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		Therefore, the lack of "flow of control" capability within P2P and SAP combined with the many engineered safety and reliability features of the Tricon provide reasonable assurance that communication failures will not adversely impact the safety function. Furthermore, site-specific administrative and physical access controls described above would provide additional layers of protection against inadvertent and unauthorized changes to the application program.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 12 Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following: • Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise. • Messages may be	None	Invensys responses to Staff Positions 2 and 4 describe in detail the electrical and functional isolation provided by the TCM, reliable design of the TCM, and the several engineered layers of protection against communication failures. Invensys response to Staff Position 6 explains that the TCM handles all external communications, and thus isolates the TMR 3008N MPs from communications. Invensys response to Staff Position 7 describes in detail the Tricon communication protocols, including the end-to-end integrity checks performed by P2P and SAP. The design and operation of the Tricon prevents any communication fault altering the application program or its performance. All data "writes" must be in proper format, have the proper address and be within a given alias range. Testing was performed by an independent third-party to validate the robustness of the Tricon against communication failures. Tricon security testing was performed using the Achilles Test System from Wurldtech. The V10.5 Tricon was awarded Achilles Level 1 certification. To achieve Level 1 certification the Tricon under test must pass tests designed to verify the robustness of the TCM to various communication failures, such as proper handling of rogue and invalid protocol packets, and continued operation under network storm conditions without adverse impact on the TMR 3008N MP control algorithm. Ethernet, ARP, IP, ICMP, TCP, and UDP protocols were tested. The test configuration included monitoring of digital output (DO) signals to confirm that the Tricon application program running on the TMR 3008N MPs was unperturbed. Testing validated that the TCM will discard rogue, invalid, and excessive Ethernet packets (such as during data storms), thereby ensuring the operation of the TMR 3008N MPs was unperturbed during communication failures. The results of the Wurldtech testing validated the added reliability the TCM provides to the communication link. For safety-related communications, credit is not taken for the reliability gains provided by the TCM. Instead, the end-to-end integrity of safety-related communications is provided by P2P and SAP, as discussed in previous responses in this position paper. All P2P and SAP communications are further enhanced to mitigate communication faults, including, but not limited to, the following:

<table>
<tr><th>NRC GUIDANCE – ISG-04</th><th>Deviation</th><th>INVENSYS COMPLIANCE & COMMENTS</th></tr>
<tr><td>repeated at an incorrect point in time.
• Messages may be sent in the incorrect sequence.
• Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
• Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
• Messages may be inserted into the communication medium from unexpected or unknown sources.</td><td></td><td>
<table>
<tr><td>Fault</td><td>Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.</td></tr>
<tr><td>Mitigation</td><td>Mitigated through: application-generated 32-bit CRC; sequence numbers; the SAP Data Key; the SAP NIST-published cryptographic algorithm for message integrity check; requests for resend of the message; limits on acceptable delay; and maximum number of errors before declaring loss of communication.</td></tr>
<tr><td>Fault</td><td>Messages may be repeated at an incorrect point in time, due to errors, faults, or interference.</td></tr>
<tr><td>Mitigation</td><td>Mitigated through: tracking message identification numbers and sequence numbers, and deleting such unintended repeats; and use of multiple transmissions to increase the probability that message corruption would be detected.</td></tr>
<tr><td>Fault</td><td>Messages may arrive out of order, in that message store and forward may send later messages before successfully transmitting older messages.</td></tr>
<tr><td>Mitigation</td><td>Mitigated with the use of message sequence numbers and through software design.</td></tr>
<tr><td>Fault</td><td>Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.</td></tr>
<tr><td>Mitigation</td><td>Mitigated through unique message identification, sequence numbers, and ability to request missing data.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>NRC GUIDANCE – ISG-04</th><th>Deviation</th><th>INVENSYS COMPLIANCE & COMMENTS</th></tr>
<tr><td>• Messages may be sent to the wrong destination, which could treat the message as a valid message.
• Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
• Messages may contain data that is outside the expected range.
• Messages may appear valid, but data may be placed in incorrect locations within the message.
• Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
• Message headers or addresses may be corrupted.</td><td></td><td>
<table>
<tr><td>Fault</td><td>Messages may be delayed beyond their permitted arrival time window, such as errors in the transmission medium.</td></tr>
<tr><td>Mitigation</td><td>Mitigated through sequence numbers, repetition, and use of the lost-message mechanisms.</td></tr>
<tr><td>Fault</td><td>Messages may be inserted into the communication medium from unexpected or unknown sources.</td></tr>
<tr><td>Mitigation</td><td>Mitigated by source and destination identifiers in all messages, sequence numbers, and discarding messages that are not intended for the receiver.</td></tr>
<tr><td>Fault</td><td>Messages may be sent to the wrong destination, which could treat the message as a valid message.</td></tr>
<tr><td>Mitigation</td><td>Mitigated through: unique message identification; checking of source and destination identifiers in all messages; SAP Data Key; and ability to request missing data.</td></tr>
<tr><td>Fault</td><td>Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.</td></tr>
<tr><td>Mitigation</td><td>Mitigated through: application-generated 32-bit CRC; fixed message format; deleting messages longer than expected; and requests for resend of the message.</td></tr>
<tr><td>Fault</td><td>Messages may contain data that is outside the expected range.</td></tr>
<tr><td>Mitigation</td><td>Mitigated through application checks of data before use.</td></tr>
</table>
</td></tr>
</table>

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
		Fault	Messages may appear valid, but data may be placed in incorrect locations within the message.
		Mitigation	Mitigated through fixed message format, with all data sent in each message, and sent on a periodic interval.
		Fault	Messages may occur at a high rate that degrades or causes the system to fail.
		Mitigation	Tricon application program configuration places an upper limit on send and receive messages in one scan. Supplemental testing by Wurldtech Technologies verified robustness against this type of failure (see below).
		Fault	Message headers or addresses may be corrupted.
		Mitigation	Mitigated through application-generated 32-bit CRC; requests for resend of the message. Supplemental testing by Wurldtech Technologies verified robustness against this type of failure (see below).

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 13 Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original message exactly or to designate the message	None	Invensys response to Staff Position 1 explains that each Tricon is self-contained and not dependent upon communications with external devices to perform the safety function. Architectures involving vital communications between channels or divisions, such as for voting trip decisions, are supported using the P2P and SAP safety-related communication protocols, as explained in Invensys responses to Staff Positions 2, 4, and 7. However, such architectures would be site-specific, and in accordance with the site licensing basis. If interdivisional communications with P2P or SAP were specified, a safety analysis to validate timing constraints would be necessary. Figure 1 in Section 1.0, Introduction, depicts one possible configuration with vital communications between safety Tricon controllers, as well as safety-Tricon to SVDU communications. For the shown configuration, both P2P and SAP communication protocols would be utilized. The Tricon P2P communication protocol supports applications where Process Protection division Tricons pass process trip values and status to the RTS and ESFAS Tricons for voting and safety equipment actuation. Both the transmitting and receiving Tricon would validate all messages, employing message sequence numbers, connection authentication, and data integrity assurance algorithms to compensate for potential message corruption, unintended repetition, incorrect sequences, loss of message, unacceptable delay, unexpected message, and addressing errors. (See reply to Staff Position 12) In the example, each division Tricon would be programmed to periodically send time stamped test messages to RTS Tricons, which would return a feedback message. Should the transmitted or feedback message be lost, corrupted, incorrectly addressed, or significantly delayed, an alarm would be activated. Additionally, the RTS Tricons would be programmed to set/clear associated voter inputs upon loss of communications from division Tricons. The SAP communications would be utilized between the Tricons and the SVDUs within a division. As explained in previous responses, the SAP would provide similar end-to-end integrity checks of the communication links between the SVDUs and the associated division Tricons. See Appendix 1 for more detailed discussion of vital communications between safety Tricon controllers.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
as unrecoverable. None of this activity should affect the operation of the safety-function processor.		All communication functionality is extensively tested in accordance with Invensys Engineering Department Manual. Safety-Related applications involving vital communications between safety Tricon controllers or between safety Tricon controllers and SVDUs will be designed and tested in accordance with the approved NSIPM. See Invensys response to Staff Position 12 regarding testing of the Tricon.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 14 Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	None	The Tricon supports point-to-point and routed network communication protocol and media, copper and fiber optics. Both support redundant communication links.
STAFF POSITION 15 Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	None	In those protective system designs that utilize P2P and/or SAP communications to pass process trip values and status to other safety-related Tricon controllers or SVDUs (as depicted in Figure 1, this would be communications links with the RTS and ESFAS Tricons and the SVDUs) for voting and safety equipment actuation, each Tricon is programmed to pass all values each scan, whether the values have changed or not. As explained in Invensys response to Staff Position 2, the application engineer will utilize safety-related function blocks to monitor the vital communication links and take appropriate action as required by the particular safety process. Application programs will be developed and tested in accordance with the approved NSIPM.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 16 Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power	None	Invensys responses to Staff Positions 1 and 2 describe the independence of Tricon controllers from external devices, and the engineered layers of protection against communication failures. The TCM has been qualified under Invensys Appendix B program, and it provides functional and electrical isolation for the TMR 3008N MP safety processors. In those protective system designs that utilize P2P and SAP communications, end-to-end integrity checking of safety-related communications links is provided through the use of validation bits and timing within the message, so that the receiving Tricon or SVDU, as appropriate, is "aware" that the messages are current and not static. If the messages are detected to be static, lost, or significantly delayed, the receiving Tricon/SVDU activates an alarm. In the case of a receiving safety-related Tricon, it will assume the "fail-safe" status of the transmitting Tricon.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 17 Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.	None	As explained in previous Invensys responses, the TCM has been qualified under the Invensys Appendix B program to provide electrical isolation in accordance with EPRI TR-107330 and Regulatory Guide 1.180 Rev. 1. The qualified version utilizes fiber optic network ports for P2P, SAP, MODBUS TCP, and TSAA communications. In those protective system designs that utilize P2P and SAP communications, only fiber optic cables precisely designed for the anticipated conditions specified in EPRI TR-107330 (Reference 12) and Reg. Guide 1.180 Rev. 1 (Reference 5) are utilized in protective system applications. However, the qualification of the V10 Tricon does not include the fiber optic cables. The licensee would be responsible for providing fiber optic cables qualified for the environment in which they will be used, in accordance with 10 CFR 50.49 as applicable. Further discussion on the V10 Tricon qualification program, which includes qualification of the TCM, follows. The V10 Tricon has been qualified on a generic basis to provide utilities and other users with a platform that has been shown to comply with the applicable requirements for digital safety systems. Where appropriate, compliance with the applicable requirements is defined in terms of a "qualification envelope." This envelope defines the range of conditions within which the V10 Tricon meets the acceptance criteria. In applying the V10 Tricon system to a specific safety-related application, the user must confirm that the qualification envelope bounds the plant-specific requirements. Test results are summarized in the EQSR. Additional guidance in the form of qualification limitations on the use of the V10 Tricon system in safety-related applications is provided in the EQSR Appendix B - Application Guide. The generic qualification of the V10 Tricon encompasses both the hardware and the software used in the system. The hardware includes termination assemblies, signal conditioners, chassis, power supplies, main processor modules, communication modules, input/output modules, termination assemblies, signal conditioners and interconnecting cables. The V10 Tricon Nuclear Qualification Project was initiated to qualify the V10 Tricon in accordance with the EPRI TR-107330 requirements. The major activities completed as part of this project include the following:

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		• Identifying the specific PLC modules and supporting devices to be qualified. The Tricon hardware included in the qualification envelope was integrated into a complete test system intended to demonstrate capabilities typical of various nuclear safety systems. • Specifying the set of qualification tests to be performed on the test system, including defining a set of Operability and Prudency tests to be performed at suitable times in the qualification process. Operability and Prudency tests are required to determine the baseline system performance and to demonstrate satisfactory system operation under the stresses applied during qualification testing. • Performing the qualification tests and documenting the results. • Performing other technical evaluations as needed to demonstrate compliance with regulatory requirements and other technical requirements in EPRI TR-107330. These include evaluations of the embedded operating system and programming software, evaluation of new hardware modules (MP 3008, NGAID 3721, NGDO 3625, and TCM), a failure modes and effects analysis evaluating the effects of component failures on Tricon operation, an assessment of the accuracy specifications for the Tricon system for use in calculating instrument measurement uncertainties and establishing critical control setpoints. Qualification testing included the following: • Radiation Exposure testing to demonstrate the ability of the V10 Tricon to operate properly after being exposed to radiation. The operability tests and prudency tests were performed immediately after to demonstrate proper operation of the system. • Environmental testing to demonstrate the ability of the V10 Tricon to operate properly under the extremes of temperature and humidity. The operability test was performed at the high and low temperature and humidity conditions and also immediately after the environmental test (at ambient conditions) to demonstrate proper system operation. The prudency test was also performed at the high temperature conditions. • Seismic testing to demonstrate the ability of the V10 Tricon to operate properly during and after design basis seismic events, and therefore demonstrate the suitability of the device for qualification as Seismic Category I equipment. The operability tests were performed

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		immediately after the seismic test to demonstrate continued proper operation of the system. • Electromagnetic interference (EMI) and radio frequency interference (RFI) testing to demonstrate the suitability of the V10 Tricon for qualification as a safety-related device with respect to EMI/RFI emissions and susceptibility. • Electrical Fast Transient (EFT) testing to demonstrate the suitability of the V10 Tricon for qualification as a safety-related device with respect to susceptibility to repetitive electrical fast transients on the power and signal input/output leads. • Surge Withstand testing to demonstrate the suitability of the Tricon for qualification as a safety-related device with respect to AC power and signal line electrical surge withstand capability. • Electrostatic Discharge (ESD) testing to demonstrate the suitability of the V10 Tricon for qualification as a safety-related device with respect to immunity to electrostatic discharge exposure • Class 1E-to-non 1E electrical isolation testing to demonstrate the suitability of the V10 Tricon for qualification as a safety-related, Class 1E device with respect to providing electrical isolation at Non-1E field connections. After the qualification tests, the following performance proof tests were done: • Operability test as described above. • Prudency test as described above. Individual test reports contain the full discussion of the detailed qualification envelope defined by the test results. These reports have been provided to NRC to support the V10 Tricon safety evaluation. Below is a summary of the test results applicable to vital communications via the TCM. 1) The Radiation Exposure Test results demonstrate that the V10 Tricon will not experience failures due to normal and abnormal service conditions of gamma radiation exposure. 2) The environmental test results demonstrate that the V10 Tricon will not experience failures due to abnormal service conditions of temperature and humidity.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		3) The seismic test results demonstrate that the V10 Tricon platform is suitable for qualification as Category 1 seismic equipment. 4) EMI/RFI tests were performed in accordance with the requirements and methodologies of NRC RG 1.180, Rev. 1. Specifically: • The V10 Tricon fully complies with the allowable equipment radiated emissions levels defined in NRC RG 1.180, Rev. 1 for MIL-STD-461E, RE101 and RE102 testing. • The following V10 Tricon components do not fully comply with the allowable equipment conducted emissions levels defined in NRC RG 1.180, Rev. 1 for MIL-STD-461E, CE101 and CE102 testing: i. 120 VAC Chassis Power Supply ii. 230 VAC Chassis Power Supply • The V10 Tricon under test did not exhibit any anomalous behavior during the EMI/RFI susceptibility tests. The 3008 MPs continued to function correctly throughout testing. The transfer of input and output data was not interrupted. There were no interruptions or inconsistencies in the operation of the system or the software. i. The V10 Tricon 3008 MPs, chassis power supply, RXMs, and TCMs fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1 for all of the EMI/RFI susceptibility tests. ii. The V10 Tricon discrete Digital Output Module 3601T (115 VAC) with ETA 9663-610N does not fully comply with the minimum susceptibility thresholds required by NRC RG 1.180, Rev. 1, IEC 61000-4-6 Conducted Susceptibility Testing (150 kHz to 80 MHz). 5) The EFT Test results demonstrate that the V10 Tricon will not experience operational failures or susceptibilities due to exposure to repetitive electrical fast transients on the power and signal input/output leads. 6) The Surge Withstand Test results demonstrate that the V10 Tricon will not experience operational failures or susceptibilities that could result in a loss of the ability to generate a trip due to exposure to Ring Wave and Combination Wave electrical surges to the components listed above.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		7) The ESD Test results demonstrate that the V10 Tricon will not experience operational failures or susceptibilities due to exposure to electrostatic discharges to the components listed above. The main processors continued to function. The transfer of I/O was not interrupted. The TCM P2P and MODBUS communication links continued to operate correctly. 8) The TUT met all applicable performance requirements during and after application of the Class 1E to Non-1E isolation test voltages. Furthermore: • The isolation test results (together with the Prudency Test communication port fault tests) demonstrate that the Tricon Model 4352A TCM Module MODBUS serial communication ports provide adequate electrical isolation per IEEE 384-1981 between the safety related portions of the V10 Tricon and connected non-safety related communication circuits. • The Class 1E to Non-1E Isolation Test results demonstrates that the V10 Tricon relay output module Model 3636T provides adequate electrical isolation per IEEE 384-1981 between the safety related portions of the V10 Tricon and connected non-safety related field circuits. • The V10 Tricon Model 4201 Remote RXM fiber optic module is considered an acceptable Class 1E to Non-1E isolation device by design, and was not tested by the procedure. The fiber optic cables are incapable of transmitting electrical faults from the remote Non-1E RXM module to the primary RXM module (which would be installed in the safety related Tricon chassis), and therefore meet IEEE 384-1981 electrical isolation requirements. See below for further discussion on system architectures utilizing the RXM chassis. As stated above, when applying the V10 Tricon system to a specific safety-related application, the user must confirm that the qualification envelope bounds the plant-specific requirements. Additional guidance in the form of qualification limitations on the use of the V10 Tricon system in safety-related applications is provided in the EQSR Appendix B - Application Guide. The guidance includes mitigation of the identified susceptibilities. Guidance is also provided in the Invensys Planning and Installation Guide.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 18 Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	None	The Tricon Communication Module (TCM) handles all protocol, start/stop bits, handshaking, etc. tasks. The MP is neither burdened nor interrupted. Communication errors and malfunctions do not interfere with the execution of the safety function. Exchange of data between the communication processors and MPs occur once each MP scan cycle. Because all the communication with external devices, systems, and hosts is performed by and localized in the TCM, the 3008N MPs are alleviated of unneeded communications functionality and attendant complications due to complexity. Also, as discussed in Invensys response to Staff Position 10, the Tricon architecture ensures that the keyswitch in conjunction with the system software prevents changes to the application program and setpoints. This mitigates any deficiencies in the TCM with regard to performance deficits posed by unneeded functionality.
STAFF POSITION 19 If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications	None	In those protective system designs that utilize P2P and SAP communications, the data rate capacity of the TCM and cabling far exceed the 3008N MP ability to initiate and receive data. Tricons validate all data exchange between safety divisions for correctness and timeliness, setting of alarms, and assuming fail-safe state upon failure. Factors which affect performance include: COMBUS speed; the amount of aliased data and scan time; network speed and loading; and the particular communication protocol being used. The COMBUS speed determines the speed at which data is communicated between the 3008N MPs and TCMs. If the amount of aliased data updated by the 3008N MPs is too large for a single scan, it may take several scans to update the aliased data stored in the TCMs. Network communication speeds with the TCM is 100 megabits-per-second, which means that it is highly likely that data transfer between the TCM and client will not be affected by the physical network. For TSAA and MODBUS communications, “read” requests are typically processed in 10 to 50 milliseconds because the TCM responds with data from its bins, without communicating with the 3008N MPs (see Invensys response to Staff Position 9). TSAA and MODBUS “write” requests depend on scan time because the request must be communicated to and from the 3008N MPs.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.		Similarly, P2P and SAP depend on scan time because these are configured in the application program that is executed by the TMR 3008N MPs. These protocols are Application Layer protocols (see Invensys response to Staff Position 7) utilized for safety-critical communications for the added end-to-end integrity checks built into them. Because they function at the Application Layer, the 3008N MPs are involved in each message exchange. Also, the added layer of protection (see Invensys responses to Staff Positions 5 and 7) requires more 3008N MP resources for message-integrity calculations. In the context of safety-related applications, their relative simplicity naturally limits the number of application variables exchanged via P2P and SAP. The TCM is capable of 100 megabits-per-second transmission rate, which far exceeds the needs of typical safety systems. In the event that the 3008N MPs are excessively burdened with data requests, the Tricon continuously monitors system health and performance, activating an alarm should scan time exceed the predicted performance. Invensys documents provide guidance to the application engineer for configuring P2P and SAP communications links. As an example, Invensys response to Staff Position 5 provides a summary of the transfer time calculation for P2P messages. The Safety Considerations Guide discusses the transfer time calculation in detail. Transfer time calculations will be used to determine whether safety-critical timing requirements in the plant-specific safety analysis are met by the P2P and SAP communications. Should P2P or SAP communications be included in an application program, thorough program operational testing will be conducted to determine the longest scan-time duration. Application development will be performed in accordance with Invensys Appendix B quality program and the approved NSIPM. For those applications utilizing P2P and/or SAP, factory acceptance testing, within Invensys scope of supply, will identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. In addition, communications throughput thresholds and system sensitivity to communications throughput issues will be confirmed by testing.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 20 The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.	None	"Response time" is generally defined as the total time elapsed from initiation of a change in process control signal at one end of an instrumentation loop (the detector or sensor) until the end-of-loop actuated device reaches its final desired position. This term is generally utilized to describe protection function response (i.e., those required by the Technical Specifications where the actuation occurs at a given predetermined setpoint), but it can also be applied to any instrument and control process loop where a field component is required to actuate or otherwise achieve a known position in response to a change in a measured process. Safety system response time is dependent upon the specific plant process and safety system architecture. The plant safety analysis determines the response time required to prevent exceeding a safety limit. The Tricon processor is only one contributor to the overall response time computation, and this variable is referred to as the "throughput" of the Tricon processor. Throughput is generally referred to as the time required for processing a change in any signal or variable from the input screws to output screws of the Tricon cabinet. Throughput is dependent upon a number of factors, such as the number of variables scanned, size and complexity of the application program, when a change in a signal or variable is detected, etc. For those safety system architectures utilizing P2P communications (e.g., voting trip decisions), the number of P2P variables being transmitted/received would also affect throughput. Invensys response to Staff Position 5 discusses the calculation of P2P transmission time. Scan time is the rate at which the application program is run. As a general rule, the Tricon controller scan time is set at least two times faster than the throughput to meet the required response time. Certain plant applications may set scan time based on the actual processor time required to scan all the inputs and process the application program, plus a margin. (It should be noted that when the actual scan time as measured by the firmware exceeds the maximum scan time value, an alarm is triggered.) Because the number of factors involved, throughput cannot be exactly predicted for any given configuration. Therefore, conservative estimates for the various factors will be used to calculate the Tricon controller throughput. For example, since throughput is the time required for processing a change in a variable, and this change can occur late during any given scan, to

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		conservatively estimate throughput a variable change is assumed to occur at the very end of a scan. When a change occurs at the very end of a scan period, the actual change in a given variable would not be detected, voted, and sent to the output of the processor until the end of the next scan. This makes the worst possible throughput just slightly less than two scan periods. For the total response time of any given loop, this throughput is then added to the sensor response time and the actuation device response time to verify that the total loop response time satisfies the safety analysis requirements. Margin accounting for transfer time will be added for architectures utilizing safety-critical P2P communications. Also, margin will be added, as appropriate, for data error rates affecting transfer time (e.g., delays due to re-transmission). An example calculation of throughput can be found in "Maximum Response Time Calculations" (Reference 22) used for the V10 Tricon qualification project. Values for some of the parameters included in the calculation would be different for specific plant configuration, such as application program Scan Time and Surplus Time. Additionally, as explained in previous responses, the number of, for example, P2P SEND-RECEIVE pairs would affect throughput. Actual scan time, throughput, and data error rates will be measured and recorded during the plant-specific Factory Acceptance Tests (FATs).
#2 COMMAND PRIORITIZATION	None	As illustrated in Figure 1, all Invensys-designed reactor protection systems include a DAS, as well as manual actuation in the architectural design and operational functionality, based on the results of the plant specific BTP 7-19 plant specific analysis. The architecture includes the placement of a safety-related Priority Logic Module (PLM) connected between all actuation logic and final safety element (circuit breaker, motor, valve, etc.) Invensys-designed or other third-party PLMs are not included in the safety evaluation of the V10.5 Tricon.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 1 A priority module is a safety related device or software function. A priority module must meet all of the 10 C.F.R. Part 50, Appendix A and B requirements (design, qualification, quality, etc.) applicable to safety-related devices or software.	None	Invensys installs safety qualified physical devices in accordance with all requirements of 10CFR50 Appendix A and B. Technology may be qualified discrete devices (i.e. relays, switches, solid state), digital computer-based devices, or qualified FPGA-based devices.
STAFF POSITION 2 Priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met.	None	PLM devices will be completely independent of Tricons, DAS logic, and manual initiation. No failure within the Tricon, DAS, or manual equipment will prevent the PLM from correctly arbitrating the protective action.
STAFF POSITION 3	None	The PLM design is typically such that required functions are allocated and assigned to the Tricon,

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state."), and which do not directly support any safety function, have lower priority and may be overridden by other commands. In some cases, such as a containment isolation valve in an auxiliary feedwater line, there is no universal "safe state:" the valve must be		DAS, and to the operator-controlled manual devices based on the results of the plant-specific BTP 7-19 analysis. Generally, a PLM will allow any one of the three inputs to initiate protective action. For example, a RTS Tricon, the DAS, or manual input has unhindered ability to trip the Reactor Trip Breakers or initiate ESFAS equipment. It is anticipated that resetting the protective action will only be accomplished manually (i.e., operator action) or in some situations by the DCS, but only if the cause of the Tricon trip initiation has cleared. Other PLM applications will enforce a hierarchy of safety initiators, with manual having highest priority and the DAS the lowest.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
open under some circumstances and closed under others. The relative priority to be applied to commands from a diverse actuation system, for example, is not obvious in such a case. This is a system operation issue, and priorities should be assigned on the basis of considerations relating to plant system design or other criteria unrelated to the use of digital systems. This issue is outside the scope of this ISG. The reasoning behind the proposed priority ranking should be explained in detail. The reviewer should refer the proposed priority ranking and the explanation to appropriate systems experts for review. The priority module itself should be shown to apply the commands correctly in order of their priority		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
rankings, and should meet all other applicable guidance. It should be shown that the unavailability or spurious operation of the actuated device is accounted for in, or bounded by, the plant safety analysis.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 4 A priority module may control one or more components. If a priority module controls more than one component, then all of these provisions apply to each of the actuated components.	None	The PLM will control only one safety-related component. If the PLM technology implemented will control more than one component, the actuated components will be made compliant to all of the provisions in this ISG.
STAFF POSITION 5 Communication isolation for each priority module should be as described in the guidance for interdivisional communications.	None	For PLM technology that supports digital communications, the conformance of the specific device to applicable regulatory requirements and guidance, such as ISG-04, will be reviewed. Implementations using PLM technology will be plant specific.
STAFF POSITION 6 Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Standard 7-4.3.2-2003 (with comments). This includes	None	Invensys white paper NTX-SER-09-06, Triconex Development Processes for Programmable Logic Devices in Nuclear-Qualified Products (Reference 21), describes commitments to developing programmable logic devices, such as a PLM, under a software development lifecycle in accordance with the Invensys 10 CFR 50 Appendix B quality program, to include V&V activities that conform to IEEE Standard 1012. This includes handling the tools used in developing programmable logic devices in accordance with the established program conforming to IEEE Standard 1012. Any Invensys programming terminal(s) used in the configuration and programming of a PLM will be reviewed for compliance with the applicable regulatory requirements and guidance, including Regulatory Guide 1.152 and ISG-04. Implementations using PLM technology will be plant

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs), programmable gate arrays, or other such devices. Section 5.3.2 of IEEE 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the		specific.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 7 Any software program that is used in support of the safety function within a priority module is safety-related software. All requirements that apply to safety-related software also apply to prioritization module software. Nonvolatile memory (such as burned-in or reprogrammable gate arrays or random-access memory) should be changeable only through removal and replacement of the memory device. Design provisions should ensure that static memory and programmable logic cannot be altered while installed in the module. The contents and configuration of field programmable memory should be considered to be software, and should be developed, maintained, and controlled accordingly.	None	Any software developed by Invensys for use on a safety-related PLM will be developed, maintained, and controlled in accordance with 10 CFR 50 Appendix B. The selected PLM technology may utilize FPGA technology. Depending upon the selected PLM technology, the logic may or may not be alterable while the FPGA is installed in the module. Regardless, logic within the FPGA will be considered to be software, and therefore will be developed, maintained, and controlled in accordance with 10CFR50 Appendix B.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 8 To minimize the probability of failures due to common software, the priority module design should be fully tested (This refers to proof-of-design testing, not to individual testing of each module and not to surveillance testing.). If the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Testing should include the application of every possible combination of inputs and the evaluation of all of the outputs that result from each combination of inputs. If a module includes state-based logic (that is, if the response to a particular set of inputs depends upon past conditions), then all	None	Selected PLM technology will be developed, maintained, qualified, and controlled in accordance with 10 CFR 50 Appendix B. CCF concerns will be addressed as deemed appropriate to the PLM technology selected and the plant-specific implementation.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
possible sequences of input sets should also be tested. If testing of all possible sequences of input sets is not considered practical by an applicant, then the applicant should identify the testing that is excluded and justify that exclusion. The applicant should show that the testing planned or performed provides adequate assurance of proper operation under all conditions and sequences of conditions. Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from the "all possible combinations" criterion. For example, a priority module may include logic executed in a		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the "all possible combinations" testing.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 9 Automatic testing within a priority module, whether initiated from within the module or triggered from outside, and including failure of automatic testing features, should not inhibit the safety function of the module in any way. Failure of automatic testing software could constitute common-cause failure if it were to result in the disabling of the module safety function.	None	CCF concerns will be addressed as deemed appropriate to the PLM technology selected and the plant-specific implementation.
STAFF POSITION 10 The priority module must ensure that the completion of a protective action as required by IEEE Standard 603 is not interrupted by commands, conditions, or failures outside the module's own safety division.	None	Protective action inputs to the selected PLM technology will have the capability to initiate safety actuation, but not to halt the actuation. Once initiated, the protective action will continue to completion, unless reset by manual operation external of the PLM circuitry.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
#3 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS	None	A fully integrated Invensys nuclear plant non-safety DCS and safety system supports multiple operator workstations. The specific plant requirements determine the number, type and locations. Invensys safety system architectures fully comply with current NRC regulations, based on the NRC SER (Reference 8). The DCS is used to support the operator task of monitoring, recording and logging process variables and manipulating process equipment within the plant. The DCS provides significant automation features, which allow the operator to focus on abnormal situations, rather than normal operations. Typically all safety-related parameters within the Tricons are read by the DCS and are monitored and logged by the DCS.
#3 STAFF POSITION		
STAFF POSITION 3.1.1 **Non-safety stations receiving information from one or more safety divisions:** All communications with safety-related equipment should conform to the guidelines for interdivisional communications.	None	Typically all process data within each Tricon safety division is read by the non-safety DCS and/or plant computer, and/or maintenance VDUs, which complies with interdivisional communications guidelines. With the Main Chassis keyswitch in the RUN position, non-safety devices are granted "read only" access to Tricon data. The communication processor rejects all "write" messages from non-safety devices. Non-safety communications are segregated by communication processors and media. No electrical fault, software error in the non-safety VDU, non-safety DCS and/or plant computer or printer will effect the operation of the Main Processors.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 3.1.2 **Safety-related stations receiving information from other divisions (safety or nonsafety):** All communications with equipment outside the station's own safety division, whether that equipment is safety-related or not, should conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself.	None	All P2P, safety-related and non-safety VDU communications comply with interdivisional communications guidelines. It is anticipated that licensees may need to view and maintain data variables within Tricon based reactor protection systems. Appendix 1, "Non-Safety to Safety Communication Recommendation," provides Invensys guidance on the use of non-safety MVDU and DCS digital communication with Tricons.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 3.1.3 **Non-safety stations controlling the operation of safety-related equipment:** Nonsafety stations may control…the operation of safety-related equipment, provided the following restrictions are enforced: • The nonsafety station should access safety-related plant equipment only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules. • A nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is	None	It is anticipated that the selected PLM technology will support actuation of safety-related plant equipment via safety channel Tricons, non-safety workstations (DAS, DCS or dedicated VDU), and manual control devices. The Invensys protective system architecture precludes the non-safety workstation from preventing the Tricons initiating safety equipment actuation. No error or malfunction within the non-safety equipment will interrupt Tricon initiated protective action. The PLM design will accept safety initiation from any of the three inputs – Tricon, DCS, and manual. The Tricon does not have the capacity to self-reset the protective action. The operator must participate in the reset action and then only if the trip conditions are cleared and the Tricon logic is reset.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
performing its safety function. This provision should be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment. In addition: ➢ The nonsafety station should be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable. ➢ The nonsafety station should not be able to suppress any safety function. (If the safety system itself		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
protection from inappropriate or accidental reset.) ➢ The nonsafety station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 3.1.4 **Safety-related stations controlling the operation of equipment in other safety-related divisions:** Safety-related stations controlling (see note above) the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that control the operation of safety-related equipment. • A control station should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules.	None	It is anticipated that the selected PLM technology will support actuation of safety-related plant equipment via safety channel Tricons, safety workstations, and manual control devices. The Invensys protective system architecture will preclude the safety workstation from preventing the Tricons initiating safety equipment actuation. No error or malfunction within the safety workstation will interrupt Tricon initiated protective action. It is anticipated that the selected PLM design will accept safety initiation from any of the three inputs – Tricon, DAS, and manual. The safety-related workstation will not have the capacity to suppress any safety function. Once initiated by the Tricon, the safety actuation may not be reset until completion of the function and operation is restored to a safe operating envelope. The Tricon does not have the capacity to self-reset the protective action. The operator must participate in the reset action and then only if the trip conditions are cleared and the Tricon logic is reset.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
• A station must not influence the operation of safety-related equipment outside its own division when that equipment is performing its safety function. This provision should be implemented within the affected (target) safety-related system, and should be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member. In addition: ➢ The extra-divisional (that is, "outside the division") control station should be able to bypass a safety function		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
only when the affected division itself determined that such action would be acceptable. ➢ The extra-divisional station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.) ➢ The extra-divisional station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 3.1.5 **Malfunctions and Spurious Actuations:** The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, as set forth in 10 C.F.R. § 50.34 and 50.59, include but are not limited to the following: • Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station.	None	Malfunctions of the DCS, workstations, and protective system processors will be evaluated against the assumptions of the plant safety analysis. Failure of the safety and non-safety control and display stations has no effect on the control processors. Failure of a single control processor in the DCS has no effect on control or safety-related functions. A CCF of software in the DCS or Tricons may cause a loss of protection in that system, or a spurious activation of some or all safety equipment. Operator initiation of commands to the DCS and safety-related consoles is a two-step process to minimize spurious actuations. The operator selects the component to be manipulated, sets the command state, and confirms the desired action. DCS control and Tricon processors block erroneous communication commands from the non-safety and safety workstations. Safety-related control and display workstations will be qualified to operate in adverse environments as specified in EPRI TR-107330. Safety-related workstations will be qualified to operate in adverse electrical environments as specified in EPRI TR-107330. The selected DCS technology will support the “operator workstation disable” function. Failure of one or more operator workstations, safety or non-safety, has no affect on Tricon operation.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
• Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor. • Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed. • No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. For example: When the operator requests any safety function or other important function, the system should respond "do you want to proceed?" The operator should then be required to respond "Yes" or "No" to cause the system to execute the function. Other		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors. • Each control processor or its associated communication processor should detect and block commands that do not pass the communication error checks. • Multidivisional control		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may warrant the inclusion of additional qualification criteria or measures in addition to those described herein. • Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses. • The design should have provision for an "operator workstation disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
control room, etc., that might restore functionality to the control room operator stations and result in spurious actuations. • Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 3.2 **Human Factors Considerations**	None	Depending on the control and safety system architecture implemented, safety VDUs may or may not be required. Non-safety VDUs may be acceptable, provided Invensys-recommended restrictions are enforced. Upon support and approval by the licensee, Invensys shall commission an HFE analysis to establish the number and type of VDUs in the control room. The analysis will be in accordance with accepted human factors principles, such as those in Rev.2 of NUREG 0711. HFE findings will be resolved in an appropriate manner. Safety-related Tricons typically have safety-related controls and indications and/or displays. Depending upon licensee needs, controls and displays may be individual analog indicators, switches, lamps and annunciators, or VDUs displaying the same in graphical format. Regardless of licensee requirements, safety-related devices with safety-related software will be dedicated to specific safety divisions. The Tricon supports the use of non-safety displays of safety-applications. Non-safety VDUs are optional, however. They are never considered essential for safe plant operations. See Section 3.0, V10 Tricon Communications, and Invensys responses to the applicable Staff Positions in ISG-04 – #1 Interdivisional Communications. Additional safety-related VDUs, switches, indicators are provided to support operator initiated safety action. Typically, all required safety parameters are monitored via safety-related VDUs and/or indicators. Operator initiated safety actions may be via panel switches and/or the safety-related VDUs. Non-safety VDUs may also be used to monitor, record, and log safety-related variables. The typical Invensys architecture does not support the use of non-safety VDUs to initiate safety actions. Such architectures will be plant-specific and thus warrant additional regulatory scrutiny during the NRC safety evaluation.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 3.3 **Diversity and Defense-in-Depth (D3) Considerations**	None	The number, type, location and screen formats are included in the D3 analysis to minimize the potential for operator error.

6.0 REFERENCES

1) United States Nuclear Regulatory Commission Digital Instrumentation and Controls Task Working Group #2, "Diversity and Defense-in-Depth Issues Interim Staff Guidance," Rev. 2.

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

3) United States Nuclear Regulatory Commission Generic Letter 85-06, Quality Assurance Guidance For ATWS Equipment That Is Not Safety-Related

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

5) Reg. Guide 1.180 Rev. 1, "Guidelines For Evaluating Electromagnetic And Radio-Frequency Interference In Safety-Related Instrumentation And Control Systems"

6) NUREG-0800 BTP 7-19 "Guidance For Evaluation Of Diversity And Defense-In-Depth In Digital Computer-Based Instrumentation And Control Systems"

7) NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems."

8) 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.

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

10) IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations."

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

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

13) 9600164-545, Tricon V10 Equipment Qualification Summary Report, Rev. 2 (October 2008).

14) Technical Product Guide for Tricon v10 Systems, September 2008.

15) Planning and Installation Guide for Tricon v9–v10 Systems, February 2009.

16) 9100089-001, Tricon V9/10 Failure Modes and Effects Analysis with Criticality Analysis," Version 1.0, July 2006.

17) 9720097-007, Safety Considerations Guide for v9-v10 Systems, September 2009

18) 9720088-008, Communications Guide for Tricon v9-v10 Systems, February 2009.

19) 9700100-004, TriStation 1131 Developer's Guide, March 2007.

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

21) NTX-SER-09-06, Triconex Development Processes for Programmable Logic Devices in Nuclear-Qualified Products, April 2010.

22) 9600164-731, Maximum Response Time Calculations, December 2005.

APPENDIX 1

Non-Safety to Safety Communication Recommendation

1.0 INTRODUCTION

It is anticipated that Nuclear Power Plant (NPP) licensees may need to view and maintain data variables within Tricon based Reactor Protection Systems (RPS) and Engineered Safety Features Actuation Systems (ESFAS) applications. NRC Interim Staff Guidance (ISG) #4 – Staff Position 1 accepts bidirectional communications between safety divisions and between safety and non-safety equipment provided certain restrictions are enforced. The restrictions ensure no adverse impact on RPS and ESFAS functionality. This document provides Invensys guidance on the use of non-safety Maintenance Visual Display Units (MVDU) and Digital Control System (DCS) digital communication with Tricons in reactor protection system applications.

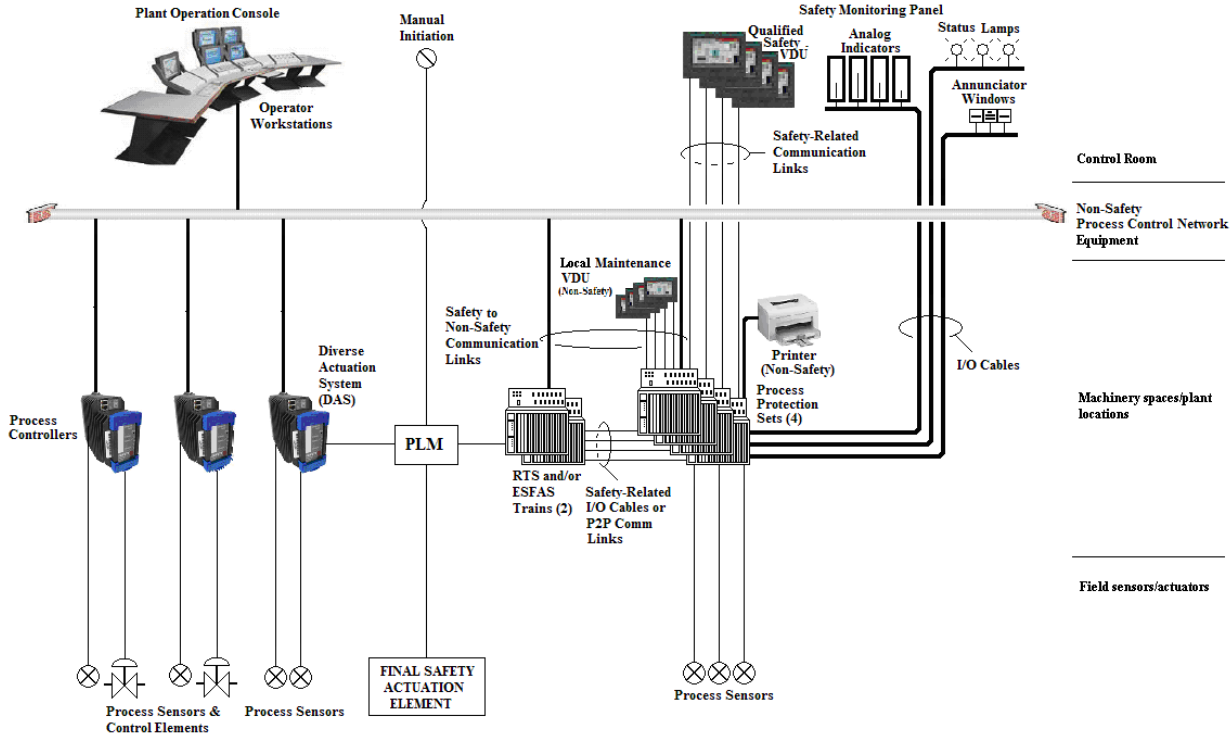


Figure 1. RPS-ESFAS Composite Architecture

2.0 RPS/ESFAS APPLICATION OVERVIEW

As shown in Figure 1, traditional Invensys safety system architectures are composed of four Process Protection Sets (PPS), channels or divisions. Each is self sufficient and its functionality is not dependent upon any information originating or resource residing outside its own safety division. Each channel monitors dedicated sensors allowing bistable logic within the Tricon to operate completely independent of other channels. Depending on the specific plant architecture, channel bistable output status is communicated to two Reactor Trip System (RTS) and ESFAS trains via Digital Outputs (DO) wired to Digital Inputs (DI); or via Peer-to-Peer (P2P) communication links. Some plant architectures combine RTS and ESFAS functionality into two Tricon trains. Other licensees prefer to distribute RTS functionality into the four channels.

3.0 TRICON COMMUNICATION FEATURES

Tricons support safe and reliable data communication links, connecting non-safety VDUs and Tricons, provided the user incorporates recommended physical interlocks and configuration guidelines. Each Tricon receives "read" communication requests through digital communication interfaces, which are separate from the Main Processors (MP). All host communications are limited to Tricon approved protocols. Each protocol is well defined and ordered, e.g. number of start and stop bits, timing, data frame format, number of data fields and check sum or CRC field. The Tricon Communication Module (TCM) handles all protocol, start/stop bits, handshaking, etc. tasks. The MP is neither burdened nor interrupted. Communication errors and malfunctions do not interfere with the execution of the safety function. Exchange of data between the communication processors and MPs occur once each MP scan cycle. Each channel may also receive "write" messages from division dedicated safety and non-safety VDUs.

Data communications with non-safety systems are supervised by the TCM. The non-safety system may request any data point and the TCM will reply if the request is valid and error free. Data writes from the non-safety system to the Tricon will only be accepted if valid, error free, keyswitches are in correct position and the memory tag name attribute is configured as 'writeable'.

The position of the Tricon Main Chassis keyswitch (physical interlock) prevents the communication module from accepting "write" messages. The position of the keyswitch is continuously monitored by the Tricon, which may enable an alarm when out of position. Additionally, all critical data values, e.g. trip setpoints, are declared as constants, which may only be changed by compiling and downloading a modified program. Invensys recommends that the Tricon Main Chassis keyswitch remain in the RUN position at all times, excepting the need to change program coding.

4.0 NON-SAFETY VDU COMMUNICATION TO TRICON EXAMPLE

As shown in Figure 1, Maintenance VDUs (MVDU) and TriStation 1131 (TS1131) may be safely utilized within the reactor protection system architecture. Although classified as non-safety devices, TS1131 and the MVDU may be used by maintenance and engineering personnel to view and change algorithmic constants utilized in RPS/ESFAS applications. It is anticipated that MVDUs will be mounted near the Tricon, out of view of the control room operator. TS1131 is an application on a laptop computer. Both the MVDU and TS1131 are connected point-to-point to the TCM and not networked.

For those licensees wishing to modify a limited set of variables via a non-safety or safety-related VDU, the Tricon supports a limited access function to enable the VDU to write to those internal tags with the "write" attribute set, even when the Main Chassis key remains in the RUN position. It is anticipated that the licensee will specify that the MVDU display all "read-only" and "writable" tags on one or more screens.

Should a technician wish to change the tag name data, it is anticipated that under administrative procedures, they will be required to inform and gain permission from the control room operator prior to entering the change. Plant administrative controls require the control room operator issue a unique key which fits a panel board or console keyswitch.

The keyswitch is wired to a Tricon digital input (DI). The Tricon continually monitors the status of the DI and upon detecting that point "ON", it illuminates a status lamp and/or an annunciator window in the control room, informing the operator that a change is in progress and that the channel is in bypass mode. Upon the switch being placed in the "Open Access" position, the Tricon activates the pre-programmed "GATENB" and "GATDIS" functions to open a data window of limited range and duration.

The technician, utilizing the MVDU touch screen or keyboard, would log into the maintenance terminal that has been configured with a role-based password log-on scheme. This means that access privileges would be dependent upon log on credentials so that only authorized and trained individuals are allowed to perform certain activities. Role-based access allows locking out certain MVDU screen functions or preventing reaching certain screens, for example, when not in maintenance mode. Therefore, depending on site needs, operators, technicians, and roving watchstanders would all have different access privileges. After logging on with the correct password, the technician enters the pre-approved data and strikes the "Enter" button, whereupon the MVDU writes the data to the Tricon, immediately reading it back and displaying the data as "staged". Once the technician concurs that the "staged" data is the same as the approved data entry sheet, they press the touch screen or keyboard to confirm entry. The Tricon program will then move the "staged" data to the tag name variable, which is used in program logic.

Upon returning the panel/console keyswitch to "Access Closed" position, disabling the gated access function, the Tricon initiates print commands to a dedicated printer which prints all programmed variables. The technician then confers with the control room operator to show that all approved changes were accomplished, and that the data access window is closed.

Should the operator fail to return the switch to "Access Closed" position within a pre-set time, the Tricon automatically closes the data access window and prints all programmed pre-formatted variables. The annunciator window and status lamps will not extinguish until the keyswitch is returned to normal, however.

5.0 SECURITY SUMMARY

Changing a limited set of variables within a protection system application may be safely accomplished through a combination of administrative controls, technician training and observation, physical interlocks and controls, and Tricon security features.

(1) Administrative control includes the development of authorized data change list and the approval by the control room operator to make the change.

(2) Depending on licensee policy, control room operator approval may include issuing a cabinet and/or panel switch key.

(3) Upon insertion of the key and rotation to "Open Access", an alarm and/or status lamp is illuminated in the control room, alerting the operator of a pending change.

(4) Configuration of the Tricon limits access to a small set of variables, which may be changed.

(5) The technician logs into the MVDU with the proper access credentials (e.g., technician password).

(6) Entering change data is a two-step process. The technician is trained to select the target variable, enter the change, observe the pending change on screen, and then confirm the change.

(7) Upon rotating the key to the normal "Close Access" position, the Tricon sends a list of all "writable" variables to the printer. The printer communication protocol is different from the non-safety VDU communications. Should the technician fail to enter the data in the allotted time, or fail to return the key to the "Close Access" position, the Tricon will automatically close access and print the list.

(8) The technician reports to the control room operator when the task is complete, showing that all changes were accomplished in accordance with the authorized work order.

APPENDIX 2

Additional Details on the Operation of the V10 Tricon Remote Extender Chassis

1.0 INTRODUCTION

NTX-SER-09-10 Sections 2, *V10 Tricon Chassis Configurations*, and 3.2, *V10 Tricon Communications – Safety-to-Nonsafety Communications*, propose safety-to-nonsafety V10 Tricon architectures utilizing non-safety Remote Extender Chassis (RXMs). Figure 1, below, taken from Section 2 for convenience, shows a safety-related Main Chassis connected to a safety-related Primary RXM Chassis, which is, in turn, connected to a non-safety Remote RXM Chassis. This appendix provides clarification on how the configuration depicted in the figure meets ISG-04. Specifically, it clarifies the communications isolation provided by the safety-related Primary RXM, and the impact on the safety function upon worst-case failure of the non-safety RXM chassis and/or input/output (I/O) module in the non-safety RXM chassis.

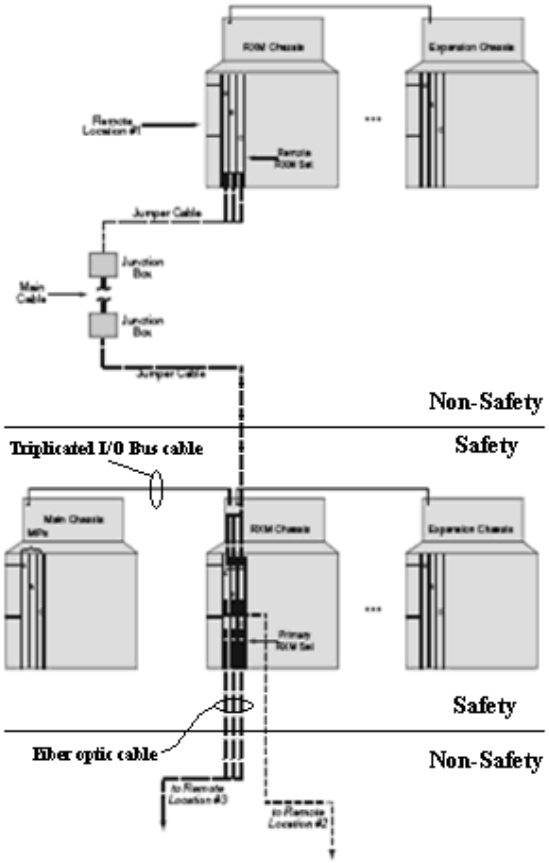


Figure 1. Safety-Related System with Non-Safety Remote Location (Figure 3 in Section 2)

Conclusions from the V9 Tricon safety evaluation that are relevant to the V10 Tricon are highlighted, and discussion is provided on the compliance of the V10 Tricon to the applicable regulatory requirements. The following sections build upon technical information in NTX-SER-09-10 Section 2.1. Additional technical details are provided as necessary.

2.0 PRECEDENCE

The RXM technology was reviewed during the V9 Tricon safety evaluation. The relevant excerpts from the V9 Tricon safety evaluation report (SER), ADAMS Accession Number ML013470433, are as follows (emphasis added):

> "2.1.1.3 Remote Extender Chassis
>
> "The remote extender chassis are similar to the expansion chassis, but are used for remote locations (up to several miles away), rather than locally. As such, each remote extender chassis has remote extender modules (RXMs) that serve as repeaters or extenders of the Tricon PLC I/O bus to allow communications with the main chassis and expansion chassis. The RXMs are single-mode fiber optic modules that allow the expansion chassis to be located up to 7.5 miles away from the main chassis. Each RXM module has separate transmit and receive cabling ports, requiring two unidirectional fiber optic cables (one to transmit and one to receive), for each module. Since the RXM modules are connected by fiber optic cables and not electrical cables, they provide ground loop isolation and immunity against electrostatic and electromagnetic interference, *and they can be used as 1E-to-non-1E isolators between a safety-related main chassis and a non safety-related expansion chassis*. The Tricon PLC remote extender chassis uses the same type of power supplies as the main chassis, and has the same dual and redundant power bus arrangement.
>
> "4.1.3.8 Class 1E to Non-1E Isolation Testing
>
> "During electrical isolation testing, the Tricon PLC test system was mounted in open instrument racks. No additional electrical protection devices were used on the I/O interfaces. At least one point on each I/O module was monitored for proper operation, and the communications modules were exercised through interfaces with external monitoring devices. Operability and prudency testing was performed following electrical isolation testing to demonstrate acceptable operation.
>
> "*The Tricon PLC test system used a fiber optic link to connect two of the expansion chassis to the system's main chassis. Triconex has demonstrated by analysis that the fiber optic cables provide electrical isolation between the main chassis and the fiber optically linked expansion chassis*. The basis for this conclusion is that since the fiber optic cables do not conduct electricity, they are incapable of transmitting electrical faults. In addition, the operability and prudency testing demonstrated that faults and failures of the fiber optic link do not degrade operation of the main chassis hardware…

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

The staff goes on to state in the V9 SER that the licensee must ensure the test voltages envelope the worst-case voltages at the site.

Since the time the V9 SER was issued in 2001, the RXM firmware has not been changed. As stated in the V9 SER, pages 18 and 22 show the firmware version number as 3310. This is the same version used for the V10 Tricon RXM modules. The differences between the RXM technology the staff approved for V9 and RXM technology of the V10 lie in the hardware – the NRC-approved V9 RXM modules utilize single-mode fiber optic cables, whereas the V10 RXM modules utilize multi-mode fiber optic cables.

3.0 REGULATORY CONSIDERATIONS

IEEE Standard 603-1991 Clause 5.6, Independence, contains requirements to protect the safety system against the effects of design basis events and failures such that the safety system will perform its safety function when demanded. Specifically, IEEE Standard 603-1991 contains requirements for independence between:

- Redundant portions of a safety system;
- Safety systems and effects of design basis events;
- Safety systems and other systems, to include interconnected equipment, equipment in proximity to the safety systems, and the effects of single failures.

With regard to safety-related digital systems utilizing software, IEEE Standard 7-4.3.2-2003, which was endorsed by the staff in Regulatory Guide 1.152, Revision 2, contains additional guidance on independence, specifically:

- Data communication between safety channels and between safety and non-safety systems; and
- Adequate barriers between safety and non-safety software on the same computer.

In the Standard Review Plan, NUREG-0800, Chapter 7, Appendix 7.1-C, the staff divided the independence requirements contained in IEEE Standard 603-1991 into three distinct facets, and identified review criteria for determining conformance:

(1) Physical Independence;

(2) Electrical Independence; and

(3) Communications Independence.

In Appendix 7.1-D, the staff provided further clarification of adequate software barriers and data communications independence.

The subsequent sections explain how the proposed architecture in Figure 1, above, meets the independence requirements in IEEE Standard 603-1991 (i.e., Physical, Electrical, and Communications Independence), as well as describe software barriers inherent in the V10 Tricon RXM technology.

3.1 Physical Independence

The V10 Tricon comprises a Main Chassis, and, depending on how many I/O points are needed, an Expansion Chassis. If distances between the Main Chassis and the Expansion Chassis exceed the capability of the standard 9000-series copper cable, then a remote expansion chassis, or RXM Chassis, will be utilized. NTX-SER-09-10 Section 2.0 gives more detail on the various V10 Tricon chassis.

In Figure 1, a safety-related Main, RXM, and Expansion Chassis are shown. Connected to the safety-related RXM Chassis via fiber-optic cables are a non-safety-related RXM and Expansion Chassis (connected via a 9000-series copper cable). In accordance with IEEE Standard 603-1991 and guidance in Chapter 7 of the SRP, the requirements for physical independence are satisfied by physical separation of safety- and nonsafety-related equipment in their respective chassis, as well as by distance. By definition, the RXM Chassis is utilized when the remote I/O is separated from the Main Chassis at a distance exceeding the capability of the 9000-series

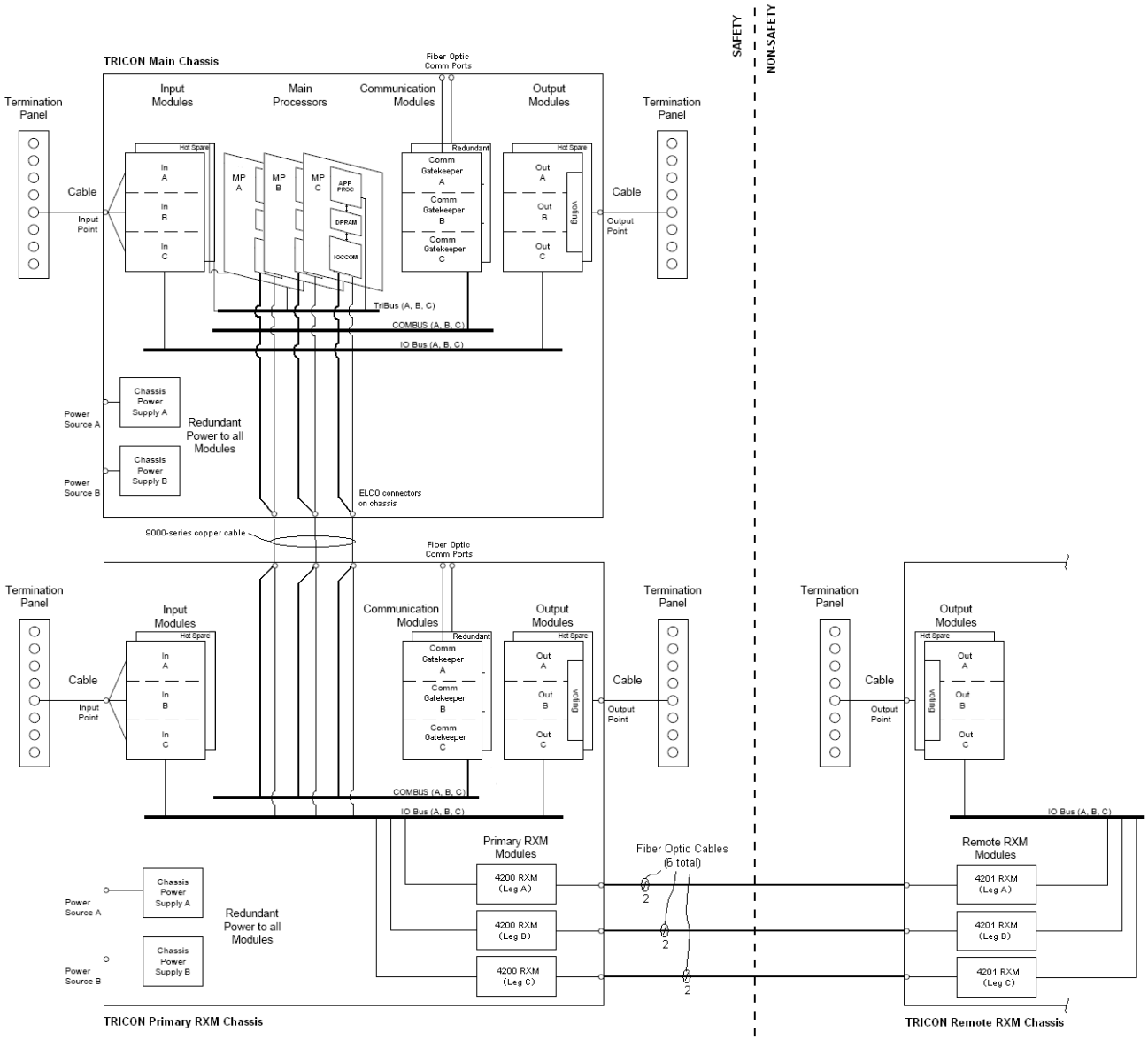


Figure 2. System Block Diagram: Safety-Related Main and Primary RXM with Non-Safety Remote RXM

copper cable (greater than 100 feet). Therefore, the non-safety remote RXM Chassis would typically be located at a distance that would ensure compliance with the physical separation requirements of IEEE Standard 603. The Primary RXM would always be safety-related to maintain traceability to the V10 Tricon nuclear qualification, thus the Primary RXM and Main Chassis would not be subject to the separation criteria.

Figure 2, a more detailed version of Figure 4 in NTX-SER-09-10 Section 2.1, shows the V10 Tricon system bus architecture for the case under consideration, i.e., safety-related Main and Primary RXM Chassis and nonsafety-related Remote RXM Chassis. The safety-to-nonsafety demarcation is represented by the vertical dashed line: on the left side are the safety-related Main Chassis and Primary RXM Chassis; on the right side is the non-safety Remote RXM Chassis. It is physically possible to have multiple Remote RXM Chassis connected to a single Primary RXM, or multiple Primary RXM Chassis connected to a single Main Chassis (up to a maximum of 14 expansion chassis). For simplicity, Figure 2 shows a single safety-related Primary RXM Chassis connected to a single non-safety Remote RXM Chassis. (It should be noted that a "primary" RXM Chassis and a "remote" RXM Chassis are physically the same, with the difference being where in the chain a given chassis is located.)

The Primary RXM Chassis is connected to the Main Chassis using a 9000-series copper cable. If a TCM is in the Primary RXM Chassis, then a 9001 copper cable connects the Primary and Main Chassis, otherwise a 9000 copper cable is used. The 9001 copper cable contains the extra wiring for transmitting network communications between the Primary RXM Chassis and the Main Chassis. Because the RXM 4200-series modules extend only the system internal I/O Bus, a TCM cannot be used in any Remote RXM Chassis.

The above Figure 2 provides a clearer picture of the physical separation between the safety and non-safety portions of the proposed architecture.

3.2 Independence between Redundant Portions of a Safety System

The V10 Tricon is a triple-modular-redundant system. Therefore, for the configuration in Figure 2, the safety-related Primary RXM Chassis will have three 4200 RXM modules with fiber optic connections to the non-safety 4201 RXM modules in the non-safety Remote RXM Chassis, with one 4200-4201 RXM module pair for each leg of the I/O Bus (Legs A, B, and C). Each 4200-4201 RXM module pair requires two multi-mode fiber optic cables (one for transmitting and one for receiving I/O Bus data), for a total of six fiber optic cables between RXM Chassis. A 4200 RXM module can support connections to three 4201 RXM modules, which means a Primary RXM Chassis can support fiber optic connections with up to three Remote RXM Chassis. The fiber optic connections provide ground loop isolation and immunity against electrostatic and electromagnetic interference, and the Invensys V10 Equipment Qualification Program has qualified the 4200-series RXM modules for safety related use, as documented in Invensys report 9600164-545, "Equipment Qualification Summary Report (EQSR)."

For nuclear applications, often redundant channels and trains are required to meet stringent nuclear safety requirements. For example, reactor protection systems may comprise four

redundant trains, Train A, B, C, and D, with two-out-of-four voting. When composed of V10 Tricon controllers, there would effectively be twelve separate processing legs, three in each Train that would then vote amongst each other to obtain the two-out-of-four trip logic. The independence requirements for redundant portions of a safety system apply at the Train level, meaning Train A, B, C, and D are required to be isolated and independent from each other. Though internal to the V10 Tricon each leg is isolated from the other two, this is not governed by the overarching independence requirement.

This particular aspect of independence is applicable to plant-specific implementations of the V10 Tricon, as explained in NTX-SER-09-10 Section 5.0 in greater detail.

3.3 Electrical Independence

Each Tricon chassis type has dual-redundant power supplies. For the configuration shown in Figure 2, the safety-related Main and Primary RXM Chassis would be powered from safety-related power sources A and B, and the nonsafety-related remote RXM Chassis (though not explicitly shown) would be powered from nonsafety power sources. The Tricon can accept either AC or DC power sources. The actual configuration would be plant-specific, and would thus be the responsibility of the Licensee. However, the V10 Tricon in its various configurations satisfies the requirements for electrical independence.

If a particular Licensee implementation requires sharing of data between redundant trains, appropriate isolation would be utilized (e.g., safety-related opto-isolators). However, train-level configurations utilizing the Tricon are plant-specific and thus the responsibility of the Licensee. NTX-SER-09-10 Section 5.0 discusses interdivisional communications in greater detail.

a, b

Figure 3. Relationship between RXM modules and the System (one leg shown)

3.4 Communications Independence

Figure 3 shows the relationship between the RXM modules and the system for a *single leg* of I/O (Leg A, B, or C). The demarcation between safety and non-safety equipment is the dashed line; above the line is the safety-related Primary RXM Chassis with the safety-related portion of the I/O Bus shown by the block "Primary I/O Bus" in the upper-left portion of the figure. This represents the Primary RXM Chassis backplane I/O bus that would transfer data to/from I/O modules inserted into the safety-related Primary RXM Chassis. Recall that the Primary I/O Bus is connected to the Main Chassis via the 9000-series copper cable (shown in Figure 2) at the Primary RXM Chassis panel connectors. Ultimately this goes to the IOCCOM processors on the associated 3008N MPs (Legs A, B, and C).

Each RXM module extends one leg of the triplicated I/O Bus by operating as an active repeater of the I/O Bus messages. Each RXM module is connected to one leg, with three RXM modules installed to assure continued operation in the event of any failure of a single leg. The data on the

I/O Bus is repeated onto the extended (fiber optic) I/O bus on a per-leg basis. Each leg operates completely independently of the others. Those messages that are intended for a specific RXM on a given leg will be responded to by the addressed RXM. These messages will also be relayed to all portions of the system *within the leg*, but will be ignored by all other modules. It should be noted that, as depicted in Figure 2, the I/O Bus is separated into command and response busses to eliminate erroneous messaging/interaction between I/O modules. All I/O Bus interactions are between the IOCCOM master and an I/O module slave within the same leg.

a, b

a, b

3.5 Software Barriers

The RXM modules utilize firmware in the master and slave CPUs, and the HDL for the PAL-based communication multiplexer. The firmware and HDL netlist are loaded onto the RXM module at the time of manufacture, and subsequently tested at the board level prior to installation into an integrated system. The safety-related RXM modules (in this case the safety-related Primary 4200 RXM modules) are dedicated in accordance with the Invensys Appendix B program for use in safety-related applications. Invensys document NTX-SER-10-14, "Tricon V10 Conformance to Regulatory Guide 1.152," describes the manufacturing process for Tricon modules. The 4200 and 4201 RXM modules have been qualified by Invensys for use in nuclear safety-related applications, as documented in the EQSR. The firmware (Revision 3310) has previously been approved by the NRC for safety-related use in nuclear power plants in the V9 SER, as explained previously. For the configuration shown in Figure 2, above, the 4200 RXM modules in the Primary RXM would be safety-related, while the 4201 RXM modules in the Remote RXM would be nonsafety-related. Because the firmware is loaded onto individual RXM modules, the barrier in this case is physical separation. The firmware is executing on separate safety and non-safety processors on separate RXM modules, thereby satisfying the barrier requirement.

The same is true of the firmware for the embedded IOCCOM processors on the safety-related 3008N MP modules. The firmware for the IOCCOM is distinctly different from the RXM firmware, and is loaded onto a physically separate 3008N MP module. The IOCCOM, as described in Section 2.1, provides an additional communication barrier (see that discussion for additional detail on the IOCCOM and I/O Bus operation). Essentially, the IOCCOM issues command messages (originating from the embedded application processor on the 3008N MP) to the I/O modules, and any responses that do not meet format requirements and timing requirements are rejected (e.g., CRC, data type, message length, sequence number). This ensures that any expected I/O module responses that are corrupted during a valid command-response exchange will be detected and subsequently ignored. Also, if the IOCCOM receives a response message from an unrecognized I/O module, the message is ignored. The combination of physical separation between the safety-related IOCCOM firmware and nonsafety-related Remote RXM module firmware and communication isolation provided by the IOCCOM satisfies the independence requirements.

A third barrier is established in the application program executing on the embedded 3008N MP through strict adherence to Invensys guidance and procedures. Invensys document NTX-SER-09-21, Nuclear System Integration Program Manual, (NSIPM) governs the development process[1] for nuclear safety-related systems starting at the conceptual phase through testing phase and into delivery. Invensys documents 9700097-007, Safety Considerations Guide for Tricon V9-V10 Systems, and 7286-545 -1, V10 Tricon Application Guide, Appendix B, both contain guidance to the application engineer on programming of fault-handling algorithms for I/O faults. Specialized Tricon library function blocks are available specifically for ensuring proper operation of safety-critical I/O. The Application Guide also contains guidance for the application engineer on proper handling of both safety-critical and non-safety critical I/O in application programs.

For configurations utilizing nonsafety Remote RXM Chassis, such as that shown in Figure 2, the safety function will not depend upon the non-safety I/O points, because the safety-related application program functions that handle the non-safety I/O residing on the non-safety RXM Chassis and modules would be developed, tested, and maintained equivalent to safety-related functions, consistent with IEEE Std 603 and 7-4.3.2, and in conformance with guidance from the staff. Adhering to Invensys procedures and application guidance during development of application code for nuclear safety-related systems and following the NSIPM process will ensure the application program will be designed, implemented, tested, and maintained in accordance with NRC requirements for safety-related software in nuclear power plants.

[1] The Invensys Quality Assurance (QA) Program and implementing procedures have been assessed by several organizations, such as the NRC (during the V9 safety evaluation and subsequent inspections, the latest of which was 2008), and audits by NUPIC, Florida Power & Light, Bechtel National, and other nuclear customers. These audits continue to demonstrate that the Invensys Tricon development process and QA program satisfy the requirements of 10 CFR Part 50 Appendix B and BTP 7-14.

4.0 SUMMARY DESCRIPTION OF THE I/O BUS

There are three 3008N MPs in the system and three legs in each I/O module. There are three independent I/O buses that connect each 3008N MP with one leg of an I/O Module. The I/O bus implements a serial master-slave protocol where the master (IOCCOM processor on the 3008N MP module) polls the slave (a leg in an I/O module). The I/O Bus is a closed system that is configured at design time. Messages are single threaded, which means a response message from an I/O module for a given command message from the IOCCOM must be received or timed out *before* the next command message is issued. Commands from the IOCCOM processor are addressed to a specific I/O module or may be broadcast to all I/O modules. An I/O Module's leg must respond only to messages that are addressed to it. However, a spare module's leg may listen to command messages and responses from its active partner but it will not respond.

a, b

a, b

5.0 FAILURE MODES AND EFFECTS ANALYSIS

A Failure Modes and Effects Analysis (FMEA) was performed on the V10 Tricon system in accordance with the applicable requirements of EPRI TR-107330 Section 6.4.1. In general, the techniques of ANSI/IEEE Std. 352-1987 were used in the analysis. The results of the FMEA are documented in Invensys document 9600164-531, "Failure Modes and Effects Analysis for the Tricon Version 10.2 Programmable Logic Controller." The FMEA addressed failures of major components and at the module level. The approach was appropriate because sub-components in the Tricon modules are triple-redundant, and no single failure of an individual subcomponent can impact the ability of the Tricon to perform its safety-related functions, where *safety-related function* was defined as the ability of the safety system to perform a safe shutdown function. In addition, the Tricon self-diagnostic features have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the diagnostics detect all possible single failures within each module.

The FMEA tabulation in Table 3 is an extension of the FMEA in 9600164-531 that postulates credible failures of the non-safety Remote RXM Chassis as shown in Figure 2. The approach identified the mechanisms that could cause the failure modes, and evaluated the consequences of the failures on the operation of the safety-related portion of the configuration (i.e., safety-related 3008N MPs and Primary RXM chassis and I/O modules). Because of the architecture of the Tricon, failure mechanisms that affect a single leg of the triple redundant system generally have no effect on system operation. Therefore, the FMEA considered (1) failure mechanisms that are recognized as being highly unlikely but that could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures). Multiple-failure scenarios include failures of all three non-safety Remote RXM modules due to software common mode failure, loss of all power, fire, floods, or missiles. These types of multiple-failure scenarios are recognized as being very unlikely, but are included to describe system behavior in the presence of severe failures and to provide guidance for application design.

Scenarios involving credible failures of non-safety I/O modules in the Remote RXM Chassis were not specifically assessed because:

- The safety-related application program executing on the 3008N MPs would be developed and tested using a process for developing safety-related software under an approved Appendix B program to ensure loss of non-safety I/O process data would not cause loss of safety function;
- Hardware single failure of non-safety remote RXM Chassis and I/O modules and related hardware (e.g., termination panels in the cabinet) would be detected and alarmed; a review of the overall FMEA for the V10 Tricon in 9600164-531 confirms this; and
- Catastrophic failures of the non-safety I/O modules are bounded by the various scenarios in Table 3; for example, in accordance with EPRI TR-107330, Section 4.6.4, the maximum credible voltage transient (up to 600Vac and 250Vdc) on the input of a non-safety remote I/O module could lead to an open I/O bus in the non-safety Remote RXM Chassis, which is one of the scenarios analyzed in Table 3.

The tabulation provides the following data for each failure:

- Affected Components
- Failure Mode
- Failure Mechanism
- Effect on the safety-related Tricon Inputs and Outputs
- Effect on operability of the safety-related Main and Primary Remote RXM Chassis

FMEA Table 3 addresses hardware failures and software failures. Section 6 contains the conformance matrix describing RXM conformance to DI&C-ISG-04, including failure modes postulated in Staff Position 12. Figures 1, 2, and 3 are essential to the context of the compliance table in Section 6.0 this Appendix.

Table 3. Failure Modes and Effects Analysis for Tricon V10.2 TMR Programmable Logic Controller – Cable and Non-Safety Remote RXM Module and Chassis Failures

Affected Components	Failure Mode	Failure Mechanisms	Effect on PLC Inputs and Outputs	Effect on PLC Operability
NON-SAFETY REMOTE RXM MODULE-RELATED FAILURES				
1) Model 4201-3; Non-Safety Remote Extender Module (RXM), Multimode Fiber Optics (set of 3 modules)	Loss of all three non-safety RXM modules	Fire; flood; missiles; Software common mode failure	Input signals in affected non-safety RXM chassis will not be read. Non-safety analog and digital outputs fail low.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of non-safety I/O function in the failed non-safety Remote RXM chassis as noted, and all downstream non-safety chassis assemblies. Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM communications fault.
2) Model 4201-3; Non-Safety Remote Extender Module (RXM), Multimode Fiber Optics (set of 3 modules)	Loss of one or two non-safety RXM modules	Electronics or software failure	None	Safety-Related Main and Primary RXM Chassis continue to operate via intact non-safety Remote RXM module(s). Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM module fault.
NON-SAFETY REMOTE RXM CHASSIS POWER SUPPLY-RELATED FAILURES				
1) Non-Safety RXM Chassis power supply: Model 8310 – 120Vac/Vdc Model 8311 – 24Vdc Model 8312 – 230Vac	Loss of one non-safety power supply output	Electronic component or fuse failure	None	Safety-Related Main and Primary RXM Chassis continue operation. Non-Safety Remote RXM Chassis continues to operate via the redundant non-safety Remote RXM Chassis power supply. Safety-Related 3008N MP diagnostics will detect and flag board fault on the non-safety Remote RXM Chassis power supply. Fault alarm via safety-related Main Chassis Power Module alarm circuit.

2) Non-Safety RXM Chassis power supply: Model 8310 – 120Vac/Vdc Model 8311 – 24Vdc Model 8312 – 230Vac	Non-Safety power supply outputs fail (both non-safety power supplies fail)	Electronic component or fuse failure	All outputs fail low on all modules in affected non-safety Remote RXM Chassis.	Safety-Related Main and Primary RXM Chassis continue operation. Safety-Related 3008N MP diagnostics will detect and flag board fault in the non-safety Remote RXM Chassis. Fault alarm via safety-related Main Chassis Power Module alarm circuit.
NON-SAFETY REMOTE RXM CHASSIS-RELATED FAILURES				
1) Non-Safety Remote RXM Chassis power supply rails	Both rails fail open or short to ground	Electrical power transient; fire; flood; missiles	Non-Safety input signals will not be read. Non-Safety analog and digital outputs fail low for shorted rails, and fail low at and past the failure points for open rails.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of non-safety I/O function in the failed non-safety Remote RXM Chassis as noted, and all downstream non-safety chassis assemblies. Safety-Related 3008N MP diagnostics will detect and flag power rail fault in the non-safety Remote RXM Chassis. Fault alarm via safety-related Main Chassis Power Module alarm circuit.
2) Non-Safety Remote RXM Chassis power supply rails	One rail fails open or shorts to ground	Electrical power transient and/or Motherboard insulation failure	None	Safety-Related Main and Primary RXM Chassis continue operation. Non-Safety Remote RXM Chassis continues operation via the redundant non-safety Remote RXM Chassis power supply. Safety-Related 3008N MP diagnostics will detect and flag power rail fault in the non-safety Remote RXM Chassis. Fault alarm via the safety-related Main Chassis Power Module alarm circuit.

3) Non-Safety Remote RXM Chassis I/O Bus	All buses open or short to ground	Electrical power transient; fire; flood; missiles	Non-Safety input signals will not be read. Non-Safety analog and digital outputs fail low for shorted rails, and fail low at and past the failure points for open rails.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of non-safety I/O function in the failed non-safety Remote RXM Chassis as noted, and all downstream non-safety chassis assemblies. Safety-Related 3008N MP diagnostics will detect and flag power rail fault in the non-safety Remote RXM Chassis. Fault alarm via safety-related Main Chassis Power Module alarm circuit.
4) Non-Safety Remote RXM Chassis I/O Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	None	Safety-Related Main and Primary RXM Chassis continue to operate via intact I/O bus(es). Safety-Related 3008N MP diagnostics will detect and flag I/O bus fault.
PLC CABLE-RELATED FAILURES				
3) Model 4200-3 to Model 4201-3; Safety-Related Primary RXM to Non-Safety Remote RXM, Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of all three RXM transmit or receive cables	Fire; flood; missiles	Input signals in affected non-safety Remote RXM Chassis will not be read. Analog and digital outputs fail low.	Safety-Related Main and Primary RXM Chassis continue to operate, with loss of I/O function in the failed non-safety Remote RXM Chassis as noted. Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM communications fault.
4) Model 4200-3 to Model 4201-3; Safety-Related Primary RXM to Non-Safety Remote RXM, Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of one or two RXM transmit or receive cables	Fire or cable cut	None	Safety-Related Main and Primary RXM Chassis continue to operate via intact RXM fiber optic cable(s). Safety-Related 3008N MP diagnostics will detect and flag non-safety Remote RXM communications fault.

6.0 RXM CONFORMATION MATRIX FOR DI&C-ISG-04 "HIGHLY-INTEGRATED CONTROL ROOMS – COMMUNICATIONS ISSUES"

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
#1 INTERDIVISIONAL COMMUNICATIONS		
STAFF POSITION 1 A safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function. This is a fundamental consequence of the independence requirements of IEEE603. It is recognized that division voting logic must receive inputs from multiple safety divisions.	None	For configurations involving safety-related Primary RXM Chassis and nonsafety Remote RXM Chassis, the independence requirements of IEEE Standard 603 are satisfied through inherent design characteristics as well as administrative controls. **Physical independence**. The safety-related Primary RXM Chassis is physically separate from the non-safety Remote RXM Chassis. Multi-mode fiber optic cables connect the safety-related 4200 Primary RXM modules to the nonsafety 4201 Remote RXM modules. The combination of physically separate chassis as well as distance between chassis satisfies this criterion. **Electrical independence**. The RXM Chassis utilizes dual-redundant power modules, with the capability to utilize both AC and DC site electrical power sources to the chassis. Each RXM Chassis would have its own pair of redundant power modules, with safety-related RXM Chassis powered from site vital electrical power sources, and the nonsafety RXM Chassis powered from non-vital sources. The safety-related Primary RXM Chassis would have redundant, qualified power modules. Additionally, the multi-mode fiber optic cable interconnection between the safety-related Primary RXM Chassis and nonsafety Remote RXM Chassis provide ground loop isolation and immunity against electrostatic and electromagnetic interference. This combination of redundant, separate chassis power modules, site electrical sources, and RXM Chassis interconnection with fiber-optic cables meets the requirements for electrical independence. **Communications independence**. The safety-related Primary RXM 4200 modules provide a gatekeeper function to ensure communication failures on the non-safety Remote RXM do not propagate to the safety-related portion of the

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		I/O bus. The master-slave CPUs on safety-related Primary RXM modules monitor data messages and enable data transfer to and from the non-safety RXM modules only for valid command messages to the downstream non-safety I/O modules. Another layer of protection is provided by the embedded IOCCOM processor on the safety-related 3008N Main Processor module during a valid command-response sequence between the IOCCOM and a non-safety I/O module. The IOCCOM checks for erroneous (including invalid and unexpected) and corrupted messages, and will time-out the sequence when a packet is delayed and/or missing. The combination of the IOCCOM and the gatekeeper function in the safety-related Primary RXM modules meet the requirements for communications isolation. **Software barriers**. The various firmware in the RXM Chassis is loaded into separate and distinct programmable devices (e.g., Programmable Array Logic and embedded processors). Furthermore, the safety-related Primary RXM modules are physically separate from the nonsafety Remote RXM modules, thus a physical barrier separates safety-related firmware from nonsafety firmware. With regard to the application program executing on the embedded application processor on the safety-related 3008N, Invensys commits to designing the plant-specific application safety functions such that they will not depend upon the non-safety I/O points, and to develop, test, and maintain them equivalent to safety-related functions, consistent with IEEE Std 603 and 7-4.3.2, and in conformance with guidance from the staff. Adhering to Invensys procedures and application guidance during development of application code for nuclear safety-related systems will ensure the application program will be designed, implemented, tested, and maintained in accordance with NRC requirements for safety-related software in nuclear power plants.
STAFF POSITION 2 The safety function of each safety channel should be protected from adverse influence from outside the division of which that channel is a member. Information	None	Invensys response to Staff Position addresses all of the concerns in this Staff Position. Physical separation is inherent in the design of the RXM Chassis. The purpose of the RXM Chassis is to extend the system I/O bus to locations at distances

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
and signals originating outside the division must not be able to inhibit or delay the safety function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation, malfunction, design error, communication error, or software error or corruption existing or originating outside the division.		farther than the standard 9000-series copper cables can handle. Therefore, a nonsafety Remote RXM Chassis would be physically separated from the safety-related Main and Primary RXM Chassis in accordance with IEEE Standard 603. There will be no data exchange between RXM Chassis in different safety divisions or trains. Interdivisional communications may be utilized with hardwired I/O and/or Tricon Communication Modules (see NTX-SER-09-10 Section 5.0). Because the V10 Tricon is not dependent upon data from other safety divisions or trains, this would be a plant-specific configuration that would warrant further NRC review. The Primary RXM module gatekeeper function (the master CPU) protects the safety-related segment of the I/O Bus. The master-slave CPUs on safety-related Primary RXM modules monitor data messages and enable data transfer to and from the non-safety RXM modules only for valid command messages to the downstream non-safety I/O modules. Another layer of protection is provided by the embedded IOCCOM processor on the safety-related 3008N MP module during a valid command-response sequence between the IOCCOM and a non-safety I/O module. The IOCCOM checks for erroneous (including invalid and unexpected) and corrupted messages, and will time-out the sequence when a packet is delayed and/or missing. Invensys commits to designing the plant-specific application safety functions such that they will not depend upon the non-safety I/O points, and to develop, test, and maintain them equivalent to safety-related functions, consistent with IEEE Std 603 and 7-4.3.2, and in conformance with guidance from the staff. Adhering to Invensys procedures and application guidance during development of application code for nuclear safety-related systems will ensure the application program will be designed, implemented, tested, and maintained in accordance with NRC requirements for safety-related software in nuclear

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		power plants.
STAFF POSITION 3 A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety functions, and should not be executed within the safety system. Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be	None	There will be no data exchange between RXM Chassis in different safety divisions or trains. Interdivisional communications may be utilized with hardwired I/O and/or Tricon Communication Modules (see NTX-SER-09-10 Section 5.0). Because the V10 Tricon is not dependent upon data from other safety divisions or trains, this would be a plant-specific configuration that would warrant further NRC review. IEEE Standard 603 allows safety and nonsafety functions to reside on the same computer and use the same resources as long as sufficient barriers are utilized to ensure the nonsafety function cannot impair the safety function. If barriers cannot be established, then the nonsafety software functions must be developed in accordance with IEEE Standard 7-4.3.2. Barriers identified by Invensys include: 1) Physical separation of safety-related and nonsafety firmware in the V10 Tricon, 2) Special software function blocks for safety-related I/O in the standard TS1131 function-block library, and 3) Commitments to design, implement, test, and maintain the application program in accordance with NRC requirements for safety-related software in nuclear power plants through implementation of NTX-SER-09-21, the NSIPM.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.		
STAFF POSITION 4 The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function	None	The RXM module contains two on-board microprocessors (CPUs) in a master-slave configuration. The master CPU monitors all messages coming from, and is directly polled by, the safety-related 3008N MP. The master CPU is responsible for the on-board diagnostics. It monitors the I/O bus for messages intended for the RXM, and provides the required responses. The slave CPU monitors all messages coming from the I/O modules (i.e., response messages). The slave CPU provides updated information to the master CPU regarding active I/O modules in its downstream path (e.g., in the nonsafety RXM Chassis). Any errors the slave CPU detects are also passed to the master CPU. Together the master and slave CPUs enable/disable the communication multiplexer on the RXM module. In normal mode, whenever the master CPU detects that the chassis number embedded in a valid command from the safety-related 3008N MP is addressed to an I/O module in its downstream leg, it will enable the communication multiplexer. Otherwise, it will be disabled. Therefore, noise and erroneous messages received by the Primary RXM while the communication multiplexer is disabled will not be passed to the safety-related IOCCOM on the safety-related 3008N MP. Consequently, the chance of faults and/or noise from the non-safety Remote RXM and non-safety I/O modules affecting the normal operation of the safety-related 3008N MP is reduced.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.		The I/O Bus is composed of separate command and response buses. Commands from the safety-related IOCCOM on the safety-related 3008N MP are sent over a separate path than the responses from the I/O modules. This separation of commands and responses at the hardware level ensures that I/O modules (I/O Bus slaves) respond only to valid commands from the IOCCOM via the safety-related Primary RXM. NTX-SER-09-10 Section 5.0 contains additional details on the IOCCOM, dual-port RAM (DPRAM), and the embedded application processors on the 3008N MP modules.
STAFF POSITION 5 The cycle time for the safety function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.	None	In NTX-SER-09-10 Section 5.0, the Invensys response to Staff Position 4 describes the scan loop for the Tricon controller. To summarize, on board each 3008N MP, the embedded application processor and IOCCOM processor exchange data via a 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. Data is deposited into DPRAM at the end of the embedded application processor Scan Task, which the IOCCOM processor retrieves during its own scan loop. During surplus scan time the Communication Task is run and the embedded application processor retrieves messages from the DPRAM in preparation for the next Scan Task. Priority is given to the control program and I/O data exchanges, with communication message exchanges occurring between scans. The Tricon continuously monitors system health and performance, activating an alarm should scan time exceed the predicted performance. Invensys document 9600164-731, Maximum Response Time Calculation, provides formulas to estimate the maximum response time for the various I/O

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		module types. The application engineer will utilize the formulas and built-in features in the development of the safety-related application program. Also, thorough program operational testing will be conducted to determine the longest scan-time duration. Application code for nuclear safety-related systems will be designed, implemented, tested, and maintained in accordance with the Invensys Appendix B quality program and NRC requirements for safety-related software in nuclear power plants.
STAFF POSITION 6 The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	None	For the Tricon controller, the 3008N MP acts as the safety function processor in a Triple-Modular-Redundant configuration. The Tricon controllers are qualified TMR systems and are not dependent upon interdivisional communications or external systems to perform the safety function. This would include interrupts from external systems. The TMR 3008N MP application processors are isolated from nonsafety I/O data communications by the combination of the DPRAM, the IOCCOM, and the safety-related Primary RXM. There is no handshaking on the I/O bus, and any changes are considered a hardware change.
STAFF POSITION 7 Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety logic executed by the safety function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the	None	There are three 3008N MPs in the system and three legs in each I/O module. There are three independent I/O buses that connect each 3008N MP with one leg of an I/O Module. The I/O bus implements a serial master-slave protocol where the master (IOCCOM processor on the 3008N MP module) polls the slave (a leg in an I/O module). The I/O Bus is a closed system that is configured at design time. Messages are single threaded, which means a response message from an I/O module for a given command message from the IOCCOM must be received or timed out *before* the next command message is issued. Commands from the IOCCOM processor are addressed to a specific I/O module or may be broadcast to all I/O modules. An I/O Module's leg must respond only to messages that are addressed to it.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.		The communication between the 3008N MP and the I/O module uses a serial, asynchronous, RS485 master/slave protocol at 375 Kbps. The RS485 frame contains eleven bits, including a start bit. Multiple frames comprise a single command message from the 3008N MP to the I/O module. The format of I/O message commands is fixed. Depending on the command message, the command data can be up to 255 eight-bit elements. When the master CPU on the RXM module receives a command message with a valid chassis number (that is, in its downstream leg), then it will enable the communication multiplexer. When the addressed I/O module receives a properly formatted, valid command message (chassis number, leg number, and slot number, correct CRC) then the I/O module will send a corresponding response message also with a fixed format for the response message type. Therefore, for every command message, there is an expected corresponding response message. The slave CPU on the RXM module updates a local "chassis map" and sends it to the master CPU along with any error codes contained in response messages. The IOCCOM processor performs a validity check before processing the response message (i.e., forwarding the I/O response data to the DPRAM on the 3008N MP for the embedded application processor to retrieve). Corrupted and improperly addressed messages will be ignored by the IOCCOM and I/O modules.
STAFF POSITION 8 Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.	None	There will be no data exchange between RXM Chassis in different safety divisions or trains. Interdivisional communications may be utilized with hardwired I/O and/or Tricon Communication Modules (see NTX-SER-09-10 Section 5.0). Because the V10 Tricon is not dependent upon data from other safety divisions or trains, this would be a plant-specific configuration that would warrant further NRC review. The TMR 3008N MP application processors are isolated from nonsafety I/O data communications by the combination of the DPRAM, the IOCCOM, and

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		the safety-related Primary RXM, as discussed in Invensys responses to other Staff Positions. The I/O Bus is a closed system that is configured at design time. Messages are single threaded, which means a response message from an I/O module for a given command message from the IOCCOM must be received or timed out *before* the next command message is issued. Commands from the IOCCOM processor are addressed to a specific I/O module or may be broadcast to all I/O modules. An I/O Module's leg must respond only to messages that are addressed to it. There is no handshaking on the I/O bus. The communication between the 3008N MP and the I/O module uses a serial, asynchronous, RS485 master/slave protocol at 375 Kbps. The RS485 frame contains eleven bits, including a start bit. The format of I/O messages is fixed. The above design characteristics ensure the I/O messages between the safety-related 3008N MP and non-safety I/O modules (via the safety-related Primary RXM and nonsafety Remote RXM) are processed in a deterministic manner, with the characteristics of predictability, repeatability, bounded in time, and robustness. The inherent design characteristics as well as the built-in diagnostics ensure any failures of the non-safety Remote RXM Chassis, whether the Remote RXM modules or nonsafety I/O modules, will not adversely impact the safety function of the safety-related Main and Primary RXM Chassis. As stated in Invensys response to Staff Position 2, Invensys commits to designing the plant-specific application safety functions such that they will not depend upon the non-safety I/O points, and to develop, test, and maintain them equivalent to safety-related functions, consistent with IEEE Std 603 and 7-4.3.2, and in conformance with guidance from the staff. Adhering to Invensys procedures and application guidance during development of application code for nuclear safety-related systems will ensure the application program will be designed, implemented, tested, and maintained in accordance with NRC

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		requirements for safety-related software in nuclear power plants.
STAFF POSITION 9 Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.	None	The safety-related 3008N MP contains an application processor, DPRAM, and the IOCCOM processor. The application processor executes the safety-related application program. The IOCCOM handles interactions with the I/O subsystem via the I/O Bus, utilizing dedicated memory locations for I/O data. Both the application processor and IOCCOM exchange data through the DPRAM. The DPRAM provides separate memory areas and queues for communication messages and I/O data. The memory locations dedicated to I/O data are separated according to physical inputs from and physical outputs to I/O modules, as well as input and output message queues for status messages to and from I/O modules. The DPRAM includes extensive memory protection via parity checks, CRCs, checksum, and other mechanisms. The I/O subsystem is plant-specific, but could include safety-related and nonsafety RXM Chassis, each containing numerous possible combinations of I/O modules. The I/O subsystem is configured at design time, thus there is no dynamic allocation of memory during run time. The allocation of memory is determined at compile time, is dependent upon I/O subsystem configuration, and is independent of the application program executing on the safety-related application processor.
STAFF POSITION 10 Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme	None	There are several layers of protection to prevent inadvertent application program changes. These include the Tricon keyswitch, access-control features in the TriStation 1131 programming interface, including password access, and site-specific administrative controls. NTX-SER-09-10 Section 5.0 discusses these safeguards in more detail. As explained in Invensys response to Staff Position 9, the I/O subsystem, which includes the RXM Chassis, cannot be modified during run time. There is no interface with the operator or TS1131 user that would allow modification of the RXM module firmware during run time. Modification or update of RXM

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.		module firmware requires: 1) Removal of the RXM module from the RXM Chassis 2) Special tools to interface directly with the single RXM module; Invensys neither provides nor sells these tools to its customers. Invensys document NTX-SER-10-14, Tricon V10 Conformance to Regulatory Guide 1.152, describes the physical protection of the embedded firmware and the process that must be followed to update it. Any modifications to the I/O subsystem configuration, such as adding or deleting an I/O module(s) or changing to a different model I/O module, would be a significant hardware change to theTricon system and could not be performed on line and without a "Download All" command from TS1131. In addition to the above hardware-level changes, several administrative techniques would be utilized at the Licensee's facility to prevent unauthorized alterations. The programmer must obtain cabinet and chassis keys to physically gain access to the Tricon. Licensees may wish to set control room annunciator alarms when the cabinet door and/or chassis key position is rotated out of the normal position. Also, administrative control over the TS1131 engineering workstation under an approved program for handling maintenance and test equipment.
STAFF POSITION 11 Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its	None	The RXM Chassis provides no means to send software instructions to the safety-related 3008N MP. As explained in other Invensys responses, the RXM Chassis provides the capability to handle I/O at remote locations. The I/O Bus protocol is a single-threaded command-response serial protocol for transferring I/O data as well as I/O module status. Software commands allowing remote control of the safety-related 3008N MP from the RXM Chassis is not possible. Firmware changes are performed while the RXM modules are removed from the chassis. Any modifications to the I/O subsystem configuration, such as

<table>
<tr><th>NRC GUIDANCE – ISG-04</th><th>Deviation</th><th>INVENSYS COMPLIANCE & COMMENTS</th></tr>
<tr><td>division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.</td><td></td><td>adding or deleting an I/O module(s) or changing to a different model I/O module, would be a significant hardware change to theTricon system and could not be performed on line and without a “Download All” command from TS1131.

Finally, there will be no data exchange between RXM Chassis in different safety divisions or trains.</td></tr>
<tr><td>STAFF POSITION 12

Communication faults should not adversely affect the performance of required safety functions in any way. Faults, including communication faults, originating in nonsafety equipment, do not constitute “single failures” as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:

• Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.

• Messages may be repeated at an incorrect point in time.

• Messages may be sent in the incorrect sequence.

• Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.

• Messages may be delayed beyond their permitted</td><td>None</td><td>Invensys responses to other Staff Positions (e.g., 1, 2, 3, and 4) describe the physical, electrical, and functional isolation provided in the design of the V10 Tricon I/O subsystem, as well as the several engineered layers of protection against communication failures. Invensys responses to Staff Positions 10 and 11 explain that I/O subsystem firmware alterations and upgrades to a particular configuration are hardware changes that cannot be modified at run time, and must be done with special tools unavailable outside Invensys. Therefore, the design and operation of the Tricon prevents any communication fault from altering the application program or its performance, including, but not limited to, the following:

<table>
<tr><td>Fault</td><td>Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.</td></tr>
<tr><td>Mitigation</td><td>The I/O Bus is a closed system bus utilizing a single-threaded, master-slave serial protocol. A given command message has an expected response message, both of fixed format (though data length can vary depending on the command code). The following are checked at the IOCCOM bus master and I/O module</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>NRC GUIDANCE – ISG-04</th><th>Deviation</th><th colspan="2">INVENSYS COMPLIANCE & COMMENTS</th></tr>
<tr><td>arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.
• Messages may be inserted into the communication medium from unexpected or unknown sources.
• Messages may be sent to the wrong destination, which could treat the message as a valid message.
• Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
• Messages may contain data that is outside the expected range.
• Messages may appear valid, but data may be placed in incorrect locations within the message.
• Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).
• Message headers or addresses may be corrupted.</td><td></td><td colspan="2"><table>
<tr><td></td><td>bus slave: valid command code; valid address (Chassis number, Leg, and Position (slot number)); valid message length; correct 16-bit CRC. If any of these checks indicate an error, the message is ignored. If the Primary RXM (master CPU) does not recognize the chassis number in the command message, it does not enable the communication multiplexer (PAL device). Because the I/O Bus protocol is single-threaded, the thread would time out (that is, the IOCCOM would not see a response from the I/O module due to time-out).
The Tricon is a triple-modular-redundant system, therefore the other two legs will vote out the leg with the faulted I/O.</td></tr>
<tr><td>Fault</td><td>Messages may be repeated at an incorrect point in time, due to errors, faults, or interference.</td></tr>
<tr><td>Mitigation</td><td>The I/O Bus is a closed system utilizing a single-threaded, master-slave serial protocol. Communications are initiated by the IOCCOM master. The safety-related Primary RXM (master CPU) will enable transmission to the downstream I/O module upon recognizing a valid address in the command message. The fiber optic cables are resilient against EMI/RFI. An I/O module responds only to those messages addressed to it. If a fault occurs such that a given response message from the non-safety I/O module is duplicated without being corrupted, then the message will be rejected by the IOCCOM because of incorrect length and CRC. Time out of the communication thread prevents delayed duplicate</td></tr>
</table></td></tr>
</table>

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			messages from reaching the IOCCOM because the Primary RXM will disable the communication multiplexer (PAL device). The Tricon is a triple-modular-redundant system, therefore the other two legs will vote out the leg with the faulted I/O.
		Fault	Messages may arrive out of order, in that message store and forward may send later messages before successfully transmitting older messages.
		Mitigation	The I/O Bus protocol is single-threaded by design, which means one command message is sent from the IOCCOM and no other until a valid response is received or the thread times out. There is no credible fault that can cause messages to be received out of order.
		Fault	Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.
		Mitigation	The I/O Bus protocol is single-threaded by design, which means one command message is sent from the IOCCOM and no other until a valid response from the non-safety I/O module is received or the thread times out. If a message is lost, a resend request may be issued by the IOCCOM to the non-safety I/O module. However, the non-safety I/O by definition is not required for the safety function. Lost messages and

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			acknowledgements will not impact the functioning of the safety-related application. The application code will be developed in accordance with Invensys guidance previously mentioned such that lost messages from the non-safety RXM and non-safety I/O will be handled appropriately. The safety-related application code will be designed, implemented, and tested in accordance with NTX-SER-09-21, the NSIPM.
		Fault	Messages may be delayed beyond their permitted arrival time window, such as errors in the transmission medium.
		Mitigation	The I/O Bus protocol is single-threaded by design, which means one command message is sent from the safety-related IOCCOM and no other until a valid response from the non-safety I/O module is received or the thread times out. When the safety-related Primary RXM Chassis receives a command message with a valid address and CRC, it will forward the message to the downstream nonsafety I/O module. If a corruption occurs, the safety-related IOCCOM will resend the request. If the addressed non-safety I/O module verifies the command message is valid and uncorrupted, the I/O module will respond. If at that point the nonsafety I/O module fails and begins to babble, it will corrupt that leg (*A*, *B*, or *C*) of the nonsafety response bus in the nonsafety RXM Chassis only (i.e., the other two legs remain operational). The two operational legs will vote out the corrupted leg. When the IOCCOM sends a command message to an

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			I/O module not downstream of the safety-related Primary RXM, the safety-related Primary RXM disables the communication multiplexer and prevents the corrupted nonsafety segment of the I/O Bus from propagating to the safety-related segment. If a message is lost, a resend request may be issued by the IOCCOM to the non-safety I/O module during the next fetch of I/O input data. However, the non-safety I/O by definition is not required for the safety function. Delayed messages and acknowledgements will not impact the functioning of the safety-related application. The application code will be developed in accordance with Invensys guidance such that lost messages from the non-safety RXM and non-safety I/O will be handled appropriately. The safety-related application code will be designed, implemented, and tested in accordance with NTX-SER-09-21, the NSIPM.
		Fault	Messages may be inserted into the communication medium from unexpected or unknown sources.
		Mitigation	The I/O Bus is a closed system utilizing a single-threaded, master-slave serial protocol. In order to inject a message onto the I/O Bus, physical access is required to insert a RXM or I/O module into the system. Before a RXM Chassis or I/O module will go active, the hardware configuration must first be modified and downloaded to the Tricon controller(s) using TriStation 1131. Any messages sent by a RXM or I/O module not

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			configured in the application program will be ignored by the safety-related IOCCOM. Physical access to the system is a licensee-specific issue, but minimum requirements should include an alarm on the cabinet door, controls over M&TE with the TriStation 1131 installed, material controls over spare Tricon equipment, and Quality Controls over the supply chain for nuclear-grade equipment and parts.
		Fault	Messages may be sent to the wrong destination, which could treat the message as a valid message.
		Mitigation	The I/O Bus is a closed system bus utilizing a single-threaded, master-slave serial protocol. With regard to message addressing, the following are checked at the safety-related IOCCOM bus master and I/O module bus slave: valid Chassis Number; valid Leg Number; and valid Position (or slot) Number. In addition, the message is checked for a correct CRC. If any of these checks indicate an error, the message is ignored. The I/O command bus and I/O response bus are separate communication paths which prevents any I/O bus slave from sending commands to any other I/O module bus slaves. Therefore, the only case requiring consideration is command messages sent to the wrong destination. If the safety-related Primary RXM (master CPU) does not recognize the chassis number in the command message, it does not enable the communication multiplexer. If the Primary RXM recognizes the incorrect address as being in its downstream path, the

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			command message will be passed. All downstream non-safety I/O modules will respond only to command messages addressed to them and ignore all other command messages. If the incorrect address somehow corresponds to a downstream non-safety I/O module, the I/O module will also check for correct message length, and a valid command code. If there are no errors, the non-safety I/O module will respond appropriately. The Tricon is a triple-modular-redundant system, therefore the other two legs will vote out the leg with the faulted I/O.
		Fault	Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.
		Mitigation	The I/O Bus is a closed system bus utilizing a single-threaded, master-slave serial protocol. A given command message has an expected response message, and both are of fixed format (though data length can vary depending on the command code). The following are checked at the IOCCOM bus master and I/O module bus slave: valid command code; valid address (Chassis Number, Leg Number, and Position (or slot) Number); and correct CRC. If any of these checks indicate an error, the message is ignored. The message length is also checked. If the actual message is longer than expected, a bad CRC will be detected. The safety-related IOCCOM ignores all bytes of the message that are beyond the defined maximum length of the I/O Bus

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			protocol.
		Fault	Messages may contain data that is outside the expected range.
		Mitigation	Mitigated in the safety-related application program utilizing range checks of data before use. This can be done by using the data quality bit that is associated with each input and output data point (e.g., range checking of analog inputs). The data quality bit can be accessed in the safety-related application program using a standard Tricon library function block, TR_STATUS. If the data quality is not valid, the application program can therefore be designed to take appropriate action commensurate with the safety impact. For the non-safety I/O data, most likely an alarm would be set. (However, for analog outputs the default action is to set the output to the safe value of zero.) The application code will be developed in accordance with Invensys guidance such that lost messages from the non-safety RXM and non-safety I/O will be handled appropriately. The safety-related application code will be designed, implemented, and tested in accordance with NTX-SER-09-21, the NSIPM.
		Fault	Messages may appear valid, but data may be placed in incorrect locations within the message.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			Mitigated through fixed message format, with all data sent in each message, and sent on a periodic interval. The I/O Bus is a closed system bus utilizing a single-threaded, master-slave serial protocol. A given command message has an expected response message, and both are of fixed format (though data length can vary depending on the command code). A message containing transposed fields could appear valid if it had a correct CRC. However, the following are checked at the IOCCOM bus master and I/O module bus slave: valid command code; and valid address (Chassis Number, Leg Number, and Position (or slot) Number). If any of these checks indicate an error, the message is ignored.
		Mitigation	If the safety-related Primary RXM (master CPU) does not recognize the chassis number in the command message, it does not enable the communication multiplexer. Because the I/O Bus protocol is single-threaded, the thread would time out (that is, the IOCCOM would not see a response from the I/O module due to time-out). If the CRC and address were valid, but the message and data length fields do not match the actual message length, then it will either be recognized as a bad CRC (actual message too long) or a timeout will occur (actual message too short). The Tricon is a triple-modular-redundant system. Therefore if the data field were transposed with some other field, the other two legs will vote out the leg with

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
			the faulty data.
		Fault	Messages may occur at a high rate that degrades or causes the system to fail.
		Mitigation	The I/O Bus protocol is single-threaded master-slave serial protocol based on RS485. By design one command message is sent from the safety-related IOCCOM and no other until a valid response from the non-safety I/O module is received or the thread times out. Also, the safety-related IOCCOM polls a given I/O module at most once every 10 milliseconds. Therefore, data rates are strictly defined and controlled. The event of concern is if the nonsafety I/O module were to transmit longer than its allotted time, called "babble" (perhaps analogous to a datastorm event on a network). If the non-safety I/O module were to fail (babble) when responding to a valid command message, the safety-related IOCCOM would interpret the data stream as a longer-than-expected message and ignore the response. Next, the communication thread would time out and the safety-related Primary RXM would deactivate the communication multiplexer and prevent the babbling nonsafety I/O module from impairing the safety-related IOCCOM. Therefore, the safety-related portion of the affected leg would not be adversely impacted by the babbling of the non-safety I/O module.

<table>
<tr><th>NRC GUIDANCE – ISG-04</th><th>Deviation</th><th>INVENSYS COMPLIANCE & COMMENTS</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Fault</td><td>Message headers or addresses may be corrupted.</td></tr>
<tr><td>Mitigation</td><td>Check for valid command code; check for valid address (Chassis number, Leg, and Position (slot number)) in the message; check for correct 16-bit CRC. If any of these checks indicate an error, the message is ignored.

If the safety-related Primary RXM does not recognize the chassis number in the command, it does not enable the communication multiplexer. Because the I/O Bus protocol is single-threaded, the thread would time out (that is, the safety-related IOCCOM would not see a response from the I/O module due to time-out).

The Tricon is a triple-modular-redundant system, therefore the other two legs will vote out the leg with the faulted I/O.</td></tr>
</table>
</td></tr>
<tr><td>STAFF POSITION 13

Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always reconstruct the original</td><td>None</td><td>There will be no data exchange between RXM Chassis in different safety divisions or trains. Additionally, nonsafety Remote RXM Chassis will not be utilized for vital communications.</td></tr>
</table>

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.		
STAFF POSITION 14 Vital communications should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, "point-to-point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.	None	There will be no data exchange between RXM Chassis in different safety divisions or trains. Additionally, nonsafety Remote RXM Chassis will not be utilized for vital communications.
STAFF POSITION 15 Communication for safety functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.	None	NTX-SER-09-10 Section 5.0 discusses the Tricon scan cycle in detail. In summary, at least once every Scan Task the I/O input data is retrieved and I/O puts are sent to the I/O modules. As discussed previously (e.g., Invensys response to Staff Position 7), the I/O Bus message formats are fixed (though data length can vary depending upon the valid command-response sequence).
STAFF POSITION 16 Network connectivity, liveness, and real-time properties essential to the safety application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and	None	The I/O Bus is an internal system bus based on RS485. The I/O Bus protocol is single-threaded master-slave serial protocol. By design one command message is sent from the safety-related IOCCOM and no other until a valid response from the non-safety I/O module is received or the thread times out. Also, every Scan Task, the safety-related IOCCOM polls a given I/O module at most once every 10 milliseconds. The issues with communication networks do not apply to the RXM modules.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)		
STAFF POSITION 17 Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.	None	The Tricon, including RXM Chassis and 4200-series modules, has been qualified under the Invensys Appendix B program in accordance with EPRI TR-107330 and Regulatory Guide 1.180 Rev. 1. However, the qualification of the V10 Tricon does not include the fiber optic cables. The licensee would be responsible for providing fiber optic cables qualified for the environment in which they will be used, in accordance with 10 CFR 50.49 as applicable. Nonsafety Remote RXM Chassis will not be utilized for vital communications.
STAFF POSITION 18 Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	None	The I/O Bus is an internal system bus based on RS485. The I/O Bus protocol is single-threaded master-slave serial protocol. By design one command message is sent from the safety-related IOCCOM and no other until a valid response from the non-safety I/O module is received or the thread times out. Also, every Scan Task, the safety-related IOCCOM polls a given I/O module at most once every 10 milliseconds. The RXM modules are relatively simple modules, because they simply act as I/O Bus repeaters with gatekeeper functionality implemented on the 80C50 family of processors. A Failure Modes and Effects Analysis (FMEA) was performed on the V10 Tricon system in accordance with the applicable requirements of EPRI TR-107330 Section 6.4.1. In general, the techniques of ANSI/IEEE Std. 352-1987 were used in the analysis. The results of the FMEA are documented in Invensys document 9600164-531, "Failure Modes and Effects Analysis for the Tricon Version 10.2 Programmable Logic Controller." The FMEA addressed

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		failures of major components and at the module level. The approach was appropriate because sub-components in the Tricon modules are triple-redundant, and no single failure of an individual subcomponent can impact the ability of the Tricon to perform its safety-related functions, where *safety-related function* was defined as the ability of the safety system to perform a safe shutdown function. In addition, the Tricon self-diagnostic features have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the diagnostics detect all possible single failures within each module. See also the FMEA tabulation in Table 3 of this Appendix, which is an extension of the FMEA in 9600164-531 that postulates credible failures of the non-safety Remote RXM Chassis. The approach identified the mechanisms that could cause the failure modes, and evaluated the consequences of the failures on the operation of the safety-related portion of the configuration (i.e., safety-related 3008N MPs and Primary RXM chassis and I/O modules). Because of the architecture of the Tricon, failure mechanisms that affect a single leg of the triple redundant system generally have no effect on system operation. Therefore, the FMEA considered (1) failure mechanisms that are recognized as being highly unlikely but that could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures). Multiple-failure scenarios include failures of all three non-safety Remote RXM modules due to software common mode failure, loss of all power, fire, floods, or missiles. These types of multiple-failure scenarios are recognized as being very unlikely, but are included to describe system behavior in the presence of severe failures and to provide guidance for application design.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
STAFF POSITION 19 If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing.	None	Congestion is not a concern, because the I/O Bus is a closed system utilizing a single-threaded master-slave serial protocol based on RS485. By design one command message is sent from the safety-related IOCCOM and no other until a valid response from the non-safety I/O module is received or the thread times out. Also, the safety-related IOCCOM polls a given I/O module at most once every 10 milliseconds. Therefore, data rates are strictly defined and controlled. See Invensys response to Staff Position 20 regarding response time.
STAFF POSITION 20 The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.	None	"Response time" is generally defined as the total time elapsed from initiation of a change in process control signal at one end of an instrumentation loop (the detector or sensor) until the end-of-loop actuated device reaches its final desired position. This term is generally utilized to describe protection function response (i.e., those required by the Technical Specifications where the actuation occurs at a given predetermined setpoint), but it can also be applied to any instrument and control process loop where a field component is required to actuate or otherwise achieve a known position in response to a change in a measured process. Safety system response time is dependent upon the specific plant process and safety system architecture. The plant safety analysis determines the response time required to prevent exceeding a safety limit. The Tricon processor is only one contributor to the overall response time computation, and this variable is referred to as the "throughput" of the Tricon processor. Throughput is generally referred to as the time required for processing a change in any signal or variable from the input screws to output screws of the Tricon cabinet. Throughput is dependent upon a number of factors, such as the number of variables scanned, size and complexity of the application program, when a change in a signal or variable is detected, etc. Scan time is the rate at which the application program is run. As a general rule,

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		the Tricon controller scan time is set at least two times faster than the throughput to meet the required response time. Certain plant applications may set scan time based on the actual processor time required to scan all the inputs and process the application program, plus a margin. (It should be noted that when the actual scan time as measured by the firmware exceeds the maximum scan time value, an alarm is triggered.) Because the number of factors involved, throughput cannot be exactly predicted for any given configuration. Therefore, conservative estimates for the various factors will be used to calculate the Tricon controller throughput. For example, since throughput is the time required for processing a change in a variable, and this change can occur late during any given scan, to conservatively estimate throughput a variable change is assumed to occur at the very end of a scan. When a change occurs at the very end of a scan period, the actual change in a given variable would not be detected, voted, and sent to the output of the processor until the end of the next scan. This makes the worst possible throughput just slightly less than two scan periods. For the total response time of any given loop, this throughput is then added to the sensor response time and the actuation device response time to verify that the total loop response time satisfies the safety analysis requirements. An example calculation of throughput can be found in "Maximum Response Time Calculations" (Reference 22) used for the V10 Tricon qualification project. Values for some of the parameters included in the calculation would be different for specific plant configuration, such as application program Scan Time and Surplus Time. Actual scan time, throughput, and data error rates will be measured and recorded during the plant-specific Factory Acceptance Tests (FATs).