invensys
Operations Management

invensys
Triconex

Project:	**PG&E PROCESS PROTECTION SYSTEM REPLACEMENT**
Purchase Order No.:	3500897372
Project Sales Order:	993754

PACIFIC GAS & ELECTRIC COMPANY

NUCLEAR SAFETY-RELATED PROCESS PROTECTION SYSTEM REPLACEMENT DIABLO CANYON POWER PLANT

DI&C-ISG-04 CONFORMANCE REPORT

Document No. 993754-1-912 (-NP)

Revision 0

September 6, 2011

Non -Proprietary copy per 10CFR2.390
- Areas of Invensys Operations Management proprietary information, marked as [P], have been redacted based on 10CFR2.390(a)(4).

	Name	Signature	Title
Author:	**G. McDonald**		**Application Engineer**
Reviewer	**K. Harris**		**Project Engineer**
Approvals:	**R. Shaffer**		**Project Manager**

Document Change History			
Revision	**Date**	**Change**	**Author**
0	09/06/11	Initial issue.	G. McDonald

Table of Contents

LIST OF FIGURES

1.0 INTRODUCTION

The purpose of this document is to address the Diablo Canyon Power Plant (DCPP) Process Protection System (PPS) Replacement System conformance to NRC Interim Staff Guidance (ISG) ISG-04, Highly Integrated Control Rooms – Communication Issues (Reference 2), and other related regulatory standards and guidance.

This document describes compliance of the replacement system for the DCPP Eagle 21 Process Protection System with ISG-04. The project replaces the Westinghouse Eagle 21 protection sets currently housed in Protection Racks 1 – 16 in the Cable Spreading Room with V10 Tricon equipment. The scope of the replacement concept is illustrated by the shaded area in Figure 1 below. Section 2.0 provides an overview of the changes being made to the PPS including the communication architecture.

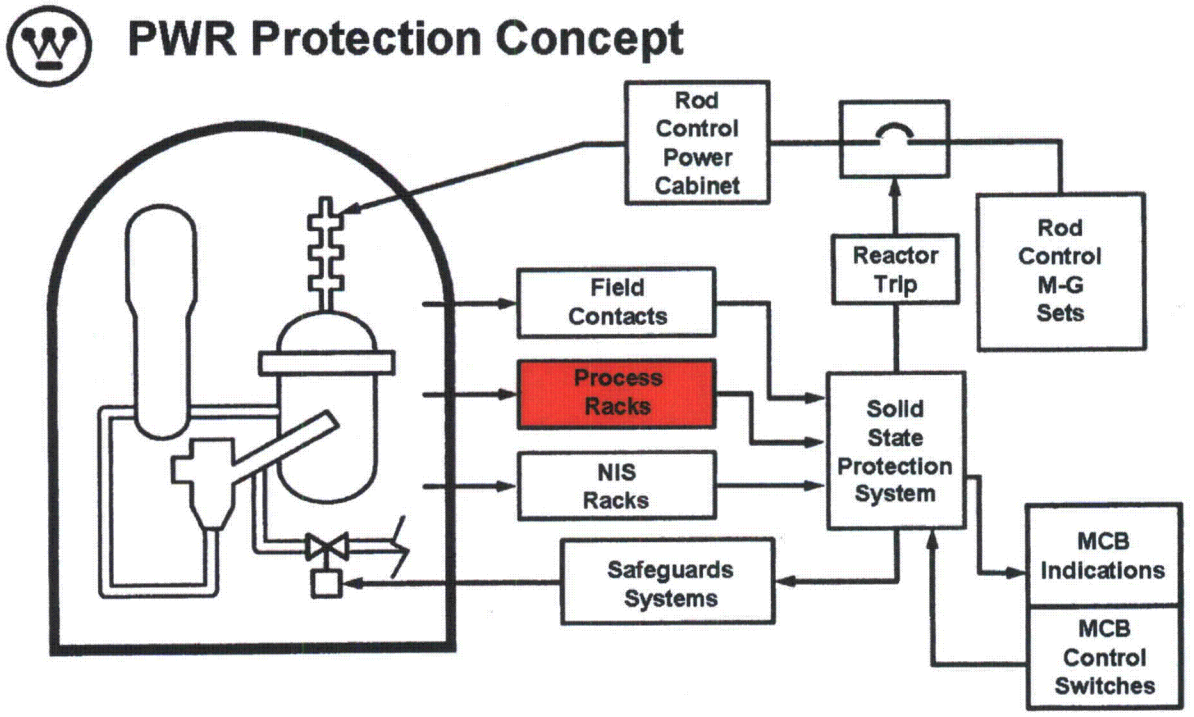


Figure 1. Westinghouse PWR Protection Scheme

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 nuclear power and processing plants. The Invensys Tricon V10 Topical Report 7286-545-1 (Reference 6) demonstrates that the Tricon is sufficiently robust, and the quality of manufacturing hardware and operating software is sufficient for use in Nuclear Power Plant (NPP) and nuclear facility safety-related systems.

Section 3.0 of this document provides a description of the Tricon Platform chassis configuration and bus architecture. Section 4.0 discusses the Tricon communication interfaces in the PPS Replacement System. Section 5.0 documents the conformance of the PPS Replacement System to NRC Interim Staff Guidance ISG-04.

1.1 Abbreviations and Acronyms

ACK	Acknowledge (e.g., during network communication handshaking)
AI	Analog Input
ALS	Advanced Logic System
AO	Analog Output
ATWS	Anticipated Transient Without Scram
BTP	Branch Technical Position
CFR	Code of Federal Regulations
COM	Communication(s)
COMBUS	Communications Bus
CRC	Cyclic Redundancy Check
D3	Diversity and Defense in Depth
DCPP	Diablo Canyon Power Plant
DAS	Diverse Actuation System
DCS	Distributed Control System
DI	Digital Input
DI&C	Digital Instrumentation and Controls
DO	Digital Output
DPRAM	Dual-Port Random Access Memory
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ESFAS	Engineering Safety Features Actuation System
ETSX	Enhanced Tricon System Executive
EXP	Tricon Expansion Chassis
FAT	Factory Acceptance Test
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
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input / Output
IOCCOM	I/O Controller/Communications Controller
IP	Internet Protocol
ISG	Interim Staff Guidance
KHz	Kilohertz
MAS	Main Annunciator System

MHz	Megahertz
MP	3008N Main Processor
MVDU	Maintenance Video Display Unit (Maintenance Workstation)
NGAI	Next-Generation I/O module – Analog Input (Differential)
NGDO	Next-Generation I/O module – Digital Output
NPP	Nuclear Power Plant
NRC	U.S. Nuclear Regulatory Commission
NSIPM	Invensys Nuclear Systems Integration Program Manual
NUREG	Nuclear Regulatory
OSI	Open Systems Interconnect
OOS	Out of Service
P2P	Peer-to-Peer
PG&E	Pacific Gas & Electric
PLC	Programmable Logic Controller
PLM	Priority Logic Module
PPC	Plant Process Computer
PPS	Process Protection System
RFI	Radio-Frequency Interference
RG	Regulatory Guide
RPS	Reactor Protection System
RTS	Reactor Trip System
RXM	Remote Expansion Chassis
SAP	Safety Application Protocol
SCRAM	Super-Critical Reactor Axe Man (emergency shutdown of a nuclear reactor)
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

1.2 Definitions

Channel
An arrangement of components, modules, and software as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single action signals are combined.

Module
Any assembly of interconnected components that constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics that permit it to be tested as a unit. A module can be a card or other subassembly of a larger device, provided it meets the requirements of this definition.

Components
Items from which the system is assembled (such as resistors, capacitors, wires, connectors, transistors, tubes, switches, and springs).

Protection Set
A protection set is a physical grouping of process channels with the same Class-1 electrical channel designation (I, II, III, or IV). Each of the four redundant protection sets is provided with separate and independent power feeds and process instrumentation transmitters. Thus, each of the four redundant protection sets is physically and electrically independent of the other sets.

Diversity and Defense-In-Depth (D&D-in-D or D3)
Requirement imposed on the Protection System design to ensure that required protective actions will occur to protect against Anticipated Operational Occurrences and Design Basis Accidents (as described in the FSARU) concurrent with a common cause failure (usually assumed to be software) that disables one or more echelons of defense.

Single Failure
Any single event that results in a loss of function of a component or components of a system. Multiple failures resulting from a single event shall be treated as a single failure.

2.0 PROCESS PROTECTION SYSTEM REPLACEMENT SCOPE

2.1 Existing System

The Process Protection System (PPS) monitors plant parameters, compares them against setpoints and provides signals to the Solid State Protection System (SSPS) if the setpoints are exceeded. The SSPS evaluates the signals and performs Reactor Trip System (RTS) and Engineered Safety Feature Actuation (ESFAS) functions to mitigate the event that is in progress. There are four separate PPS rack sets. Separation of redundant process channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and process protection racks to the two redundant trains in the SSPS logic racks. Redundant process channels are separated by locating the electronics in different PPS rack sets.

The Westinghouse Eagle 21 PPS comprises Protection Racks 1-16. The functional relationship of Eagle 21 with the other components of the overall Reactor Protection System (RPS) is illustrated in Figure 2 below.

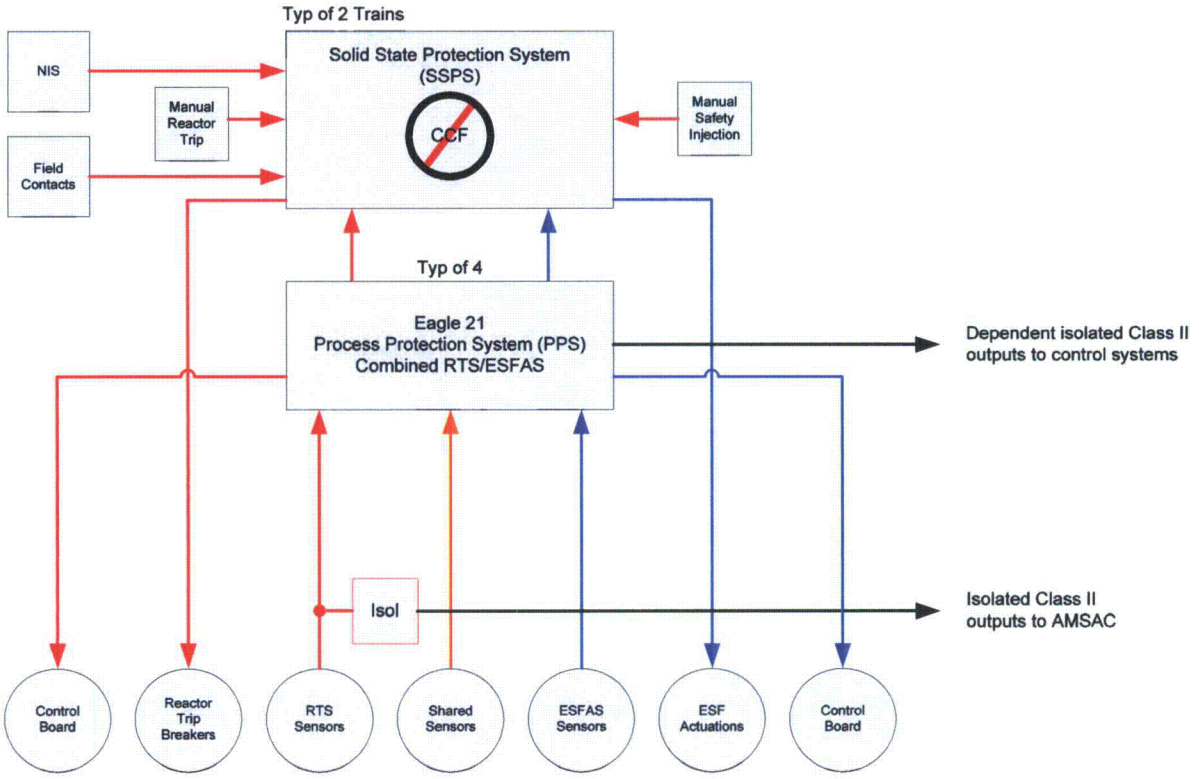


Figure 2. Existing DCPP Reactor Protection System with Eagle 21

2.2 Replacement System

The project replaces the Westinghouse Eagle 21 protection sets currently housed in Protection Racks 1 – 16. Figure 3 shows the Replacement PPS system.

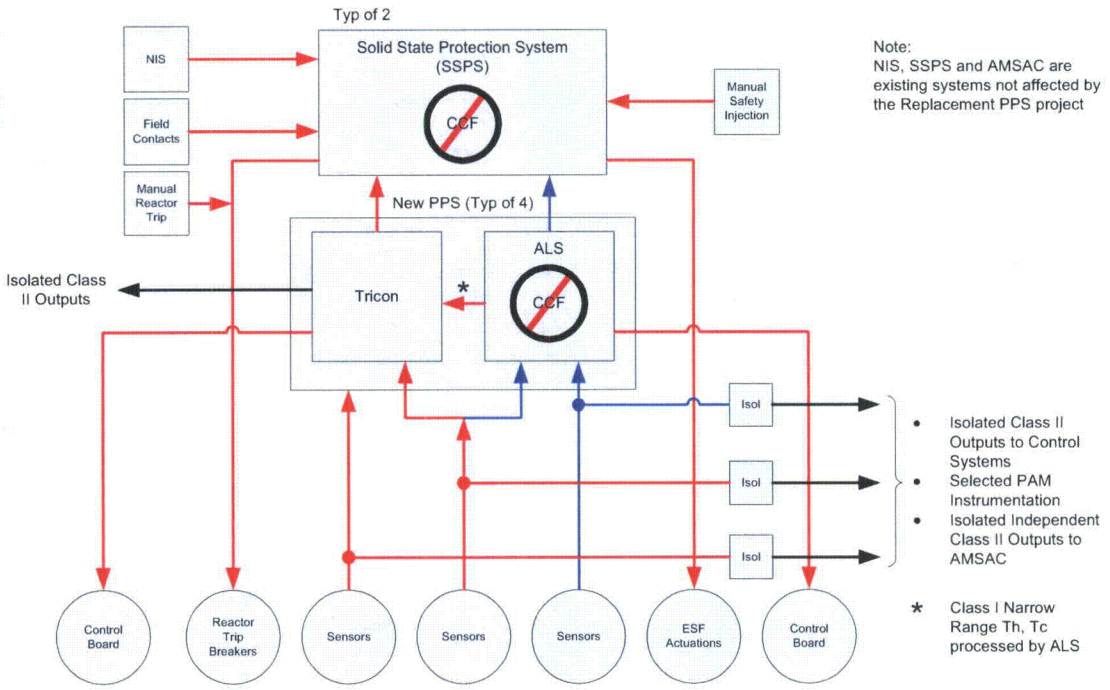
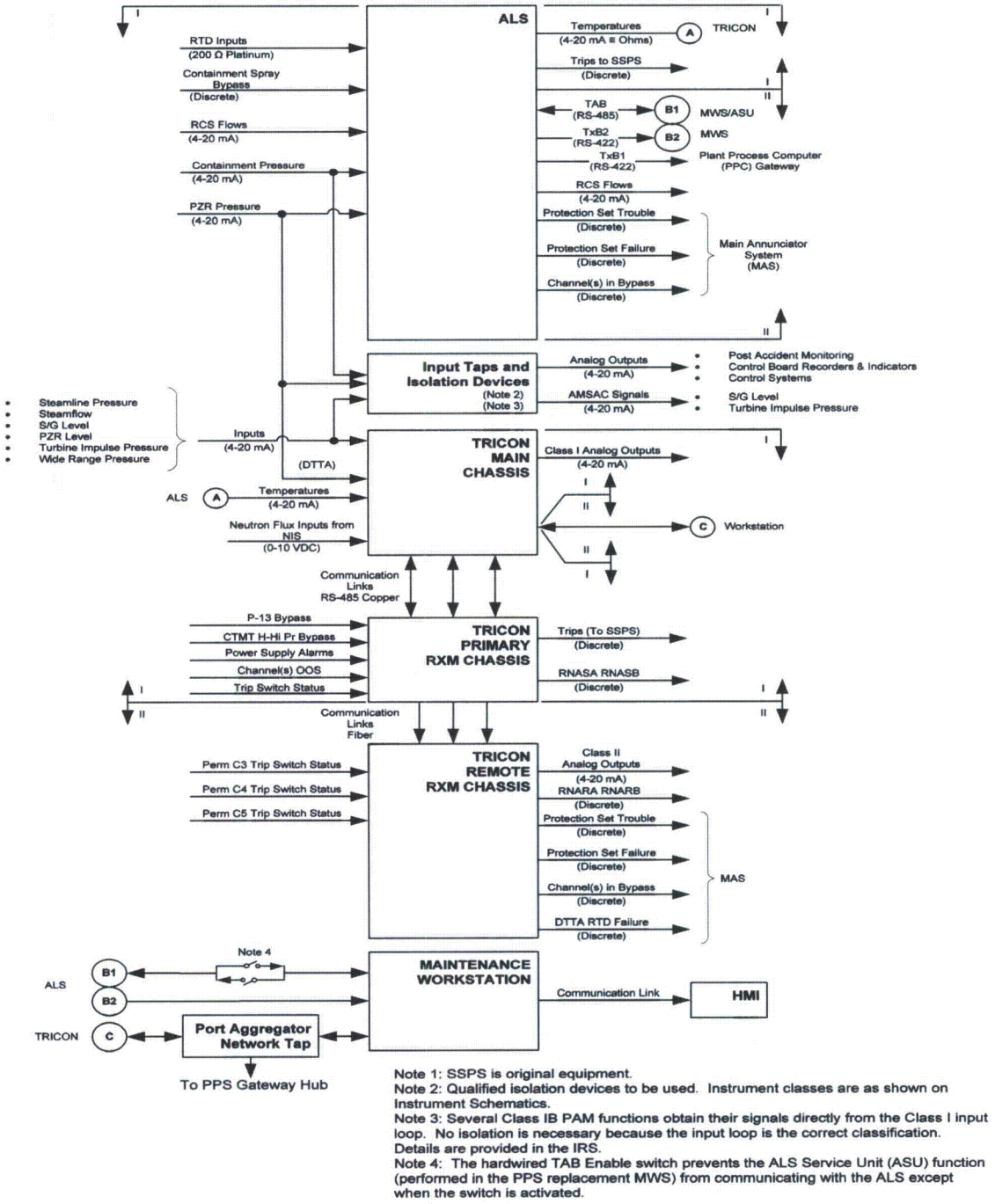


Figure 3. Process Protection System Replacement

Replacement PPS protective functions are implemented in four (4) redundant protection sets, each using a software-based Invensys Operations Management Tricon system to mitigate events where existing diverse and independent automatic mitigating functions are available per the Eagle 21 Diversity Report. For the events where existing analyses credit manual mitigative action, automatic protective functions are performed in a diverse Class 1E CS Innovations, LLC, Advanced Logic System (ALS). The Diversity and Defense in Depth analysis for the Replacement PPS is documented in PG&E Topical Report "Process Protection System Replacement Diversity & Defense-in-Depth Assessment" (Reference 12), which has been approved by the NRC (Reference 18).

Figure 4 shows the PPS Replacement Architecture with Tricon and ALS hardware, typical of each protection set.



Note 1: SSPS is original equipment.
Note 2: Qualified isolation devices to be used. Instrument classes are as shown on Instrument Schematics.
Note 3: Several Class IB PAM functions obtain their signals directly from the Class I input loop. No isolation is necessary because the input loop is the correct classification. Details are provided in the IRS.
Note 4: The hardwired TAB Enable switch prevents the ALS Service Unit (ASU) function (performed in the PPS replacement MWS) from communicating with the ALS except when the switch is activated.

Figure 4. PPS Replacement Architecture

Figure 4 illustrates a communications architecture that is consistent with NRC DI&C-ISG-04 (ISG-04), Staff Position 1, Interdivisional Communications.

The safety system architecture is composed of four protection sets (I-IV). Each is self sufficient and its functionality is not dependent upon any information originating or resource residing outside its own protection set. A small subset of plant process parameters is monitored by diverse safety related systems and provides signals to the SSPS to automatically halt the fission process and initiate cooling of the reactor during anticipated accident scenarios.

The four independent protection sets, each composed of Tricon components in separate cabinets, monitor critical plant process sensors. The Tricons convert the signals to engineering units; compare against specified setpoints (bistable function); and set/clear discrete memory variables depending on results of the comparisons. The results are sent to the SSPS for voting and safety action, as appropriate.

The Tricon supports an interface with non-safety Maintenance Workstations (MWS), which allows maintenance technicians to view plant variables and Tricon diagnostics during periodic functional surveillance testing. The Maintenance Workstation enables maintenance technicians and engineering personnel to set and/or change addressable tag names 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 are used during these maintenance activities.

All Tricons support the broadcast of all critical parameters within memory, via non-safety communication links, to be displayed and logged at the non-safety Maintenance Workstations.

ISG-04 defines interdivisional communications as communications among different safety divisions or between a safety division and a non-safety entity (such as the maintenance HMI unit). Bidirectional communications among safety divisions and between safety and non-safety equipment is acceptable provided certain restrictions are enforced to ensure that there is no adverse impact on safety system functions.

The proposed PPS Replacement System architecture does not allow communications among protection sets I to IV.

The Tricon is isolated from the Class 2 MWS by the qualified Class 1 Tricon Communications Module (TCM). The fiber optic cable electrically isolates the Tricons from external Class 2 devices. An additional data isolation device such as a NetOptics port aggregator network tap permits two-way communications between the Maintenance Workstation belonging to a specific protection set and the Tricon in that protection set, and ensures only one-way communication to the PPC Gateway, as shown in Figure 4.

When used with function block logic, the proposed architecture ensures that bidirectional communications between a safety division and non-safety equipment adhere to provisions of ISG-04 (i.e., Staff Position 1). These items are covered in section 5.0.

The Westinghouse ALS conformance to ISG-04 is documented in a separate PG&E report.

3.0 TRICON CHASSIS CONFIGURATIONS

For the PPS Replacement System, a V10 Tricon (protection set) is composed of a safety-related Main Chassis and two Remote Expansion (RXM) Chassis; a safety-related Primary RXM (4200) and a non-safety Remote RXM (4201). 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. The TCM is located in this chassis. Each logical slot provides two physical spaces for modules, one for the active module and the other for its optional hot-spare module.

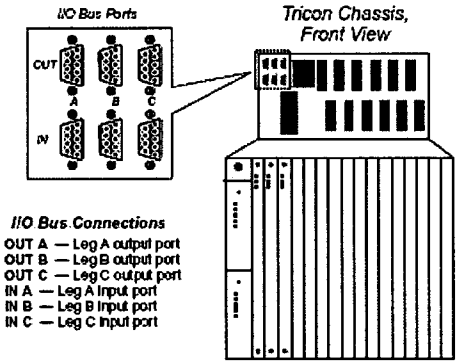


Figure 5. I/O Bus Ports

The RXM chassis is used to maintain electrical and communication isolation between the safety & non-safety parts of the system. 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. The next RXM chassis, called the "remote" RXM, is connected to the primary RXM using three RXM 4200-series modules.

The 4200 (Primary) and 4201 (Remote) RXM modules convert the system I/O Bus to multi-mode fiber optic cable. Network communications are not routed through the RXM modules. As discussed in the Triconex Topical Report 7286-545-1 (Reference 6), the 4200 RXM modules are qualified electrical isolation devices. This maintains isolation between the safety-related Main and Primary RXM chassis, and a non-safety remote RXM chassis. The application software executed in the safety-related Main Chassis (i.e., the 3008N MPs mounted in the Main Chassis) is developed and tested in accordance with NRC regulatory requirements for safety-related software as described in the Tricon Topical Report (Reference 6). By design, the non-safety remote RXM chassis does not have any safety-related I/O assigned to it. Furthermore, there are no I/O hardware or software failures that could occur in the non-safety remote RXM chassis that would prevent the safety function in the safety-related Main Chassis and primary RXM. See Invensys document NTX-SER-09-10 (Reference 9) for further discussion of the RXM communications.

3.1 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[1], as shown in Figure 6, below. A separate 3008N MP module controls each leg of the Tricon, shown in the figure as "MP A", "MP B", and "MP C". The three 3008N MP modules communicate with each other via the Tribus. Tribus is a high-speed, fault-tolerant communication path between the MPs primarily used for voting.

A 3008N MP consists of two processor sections, the application processor section and the I/O and communications (IOCCOM) processor section. Each application processor communicates with its IOCCOM processor via a dual-port RAM (DPRAM). The application processor 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 TCMs via the Communications Bus (COMBUS). Conformance of the V10 Tricon protection set Architecture to ISG-04 is addressed extensively in the following sections of this document.

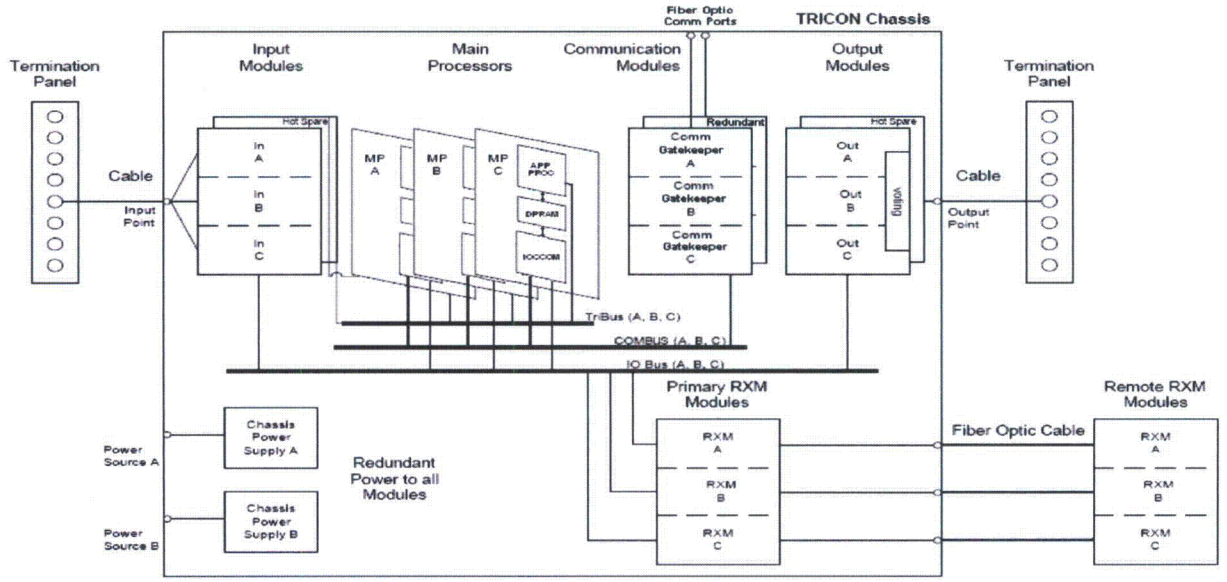


Figure 6. Simplified Block Diagram of the V10 Tricon System

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

[1]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 are triplicated through the respective Gatekeeper circuits and sent separately to each 3008N MP.

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. Further discussion of the Tribus can be found in Invensys Document NTX-SER 09-10 (Reference 9).

I/O Bus. The I/O Bus is the low-level RS485[2] 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 IOCCOM detects, verifies, processes, and passes the pending commands/output to the I/O modules. Further discussion of the I/O Bus can be found in Invensys Document NTX-SER 09-10 (Reference 9).

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 1131 and downloaded. Otherwise the new TCM would never reach the ACTIVE state, and the 3008N MPs would 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 ISG-04 is treated extensively throughout the next sections of this document.

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

4.0 V10 TRICON COMMUNICATIONS

The flexibility of the Tricon allows for transmission of both safety-related and non-safety-related data. For this application, 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 do 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 7). 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 Triconex Topical Report 7286-545-1 (Reference 6).

The following Communications Protocol supported by the TCM is included in the design for the Diablo Canyon PPS replacement:

- Triconex System Access Application (TSAA) protocol. The TSAA protocol allows client/server communication between the Triconex controller and the Maintenance Workstation. This non-safety communication is the only communication protocol being implemented in the Tricon for the Diablo Canyon PPS Replacement System.

Other communications protocols available via the TCM but not currently included in the PPS design are detailed in Invensys Document NTX-SER 09-10 "Compliance with NRC ISG-2 & ISG-4" (Reference 9), section 3.0.

The design of this application does not incorporate Safety-to-Safety Communications.

NRC Interim Staff Guidance (ISG) #4 – Staff Position 1 accepts bidirectional communications between safety and non-safety equipment provided certain restrictions are enforced. In the PPS Replacement System application there are two safety–to-nonsafety interfaces. One uses the TCM to communicate on a network that includes the Port Aggregator and the Maintenance Workstation. The other uses the RXM modules with their fiber link to communicate between the safety Tricon Primary RXM chassis and the non-safety Remote RXM chassis.

4.1 TCM Safety-to-Nonsafety Communications

Interactions between safety and non-safety systems, such as the safety related Tricon and the Maintenance Workstation, are supported by the Tricon TCM for normal operations. A non-safety Maintenance Workstation is used to view plant variables and Tricon diagnostics during periodic functional surveillance testing. The workstation allows maintenance technicians and engineering personnel, in accordance with PG&E administrative (procedural) and physical-access controls, to set and/or change addressable tag names while the channel and protection loops are in bypass mode. Additionally, Tricon controllers support the transmission of all critical parameters within memory via non-safety communication links for display and logging at the non-safety Maintenance Workstations. Note that for the PPS Replacement System: 1) there is

one Maintenance Workstation per protection set, and 2) there are no communications or transfer of data between protection sets or between their associated Maintenance Workstations. Each Maintenance Workstation communicates with its own protection set as described below.

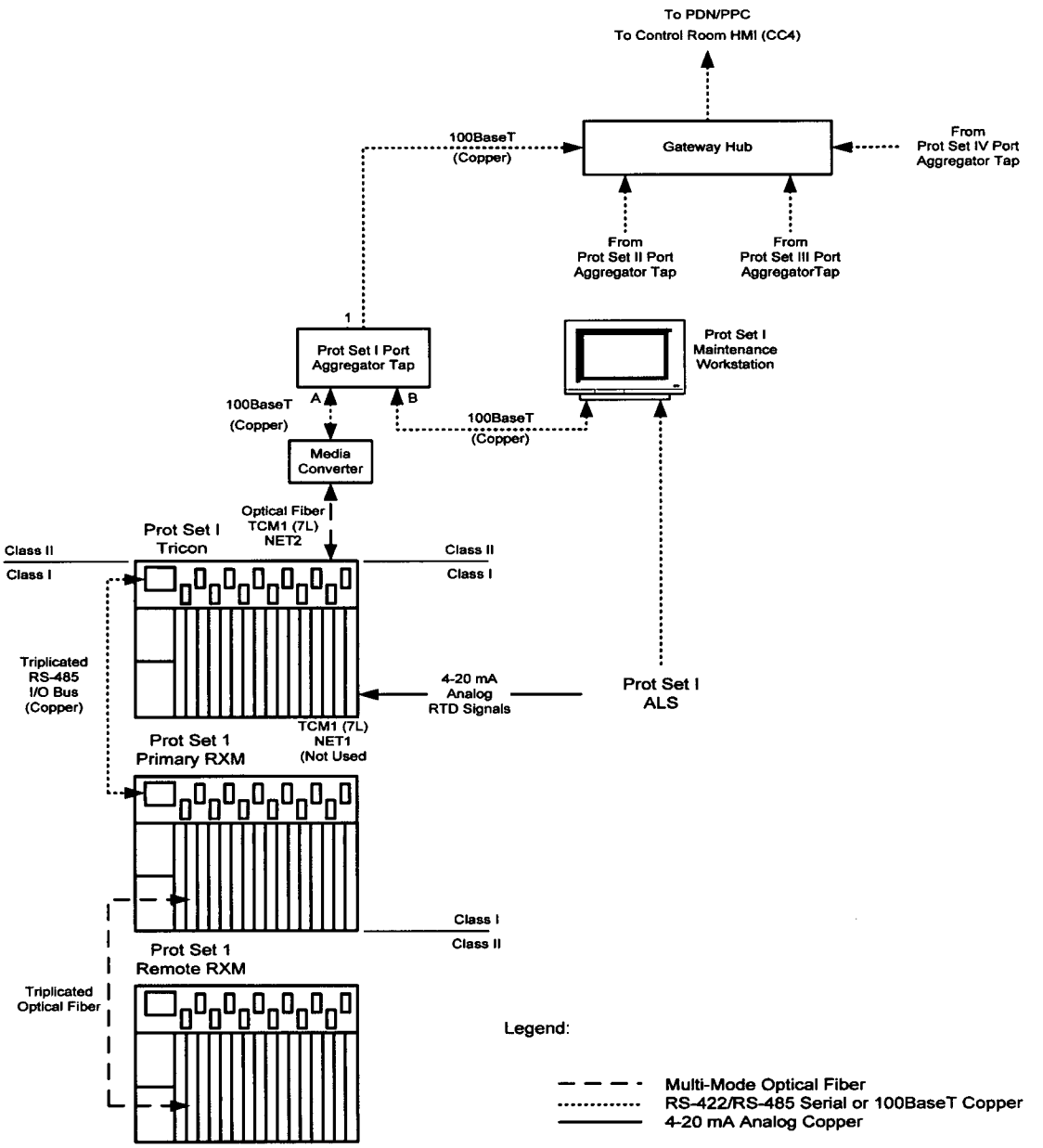


Figure 7. Safety-to-Nonsafety (Class 1E - to - Class 2) with Maintenance Workstation

Figure 7 presents the PPS Replacement System configuration to support maintenance personnel and control room operators. None of the non-safety-related data pathways would be used during accidents, nor would failures of any of the devices adversely impact the safety function of the safety-related Tricon equipment.

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 is a qualified safety related isolation device. This provides assurance that the safety function performed by the safety-related Tricon would not be impacted by any failure of the Maintenance Workstation.

P

P

4.2 Remote RXM Safety-to-Nonsafety Communications

The communication between the Primary RXM and the Remote RXM is accomplished using three Fiber Optic Cables and six RXM modules all residing on and consisting of the Tricon I/O bus. The bus is triply redundant and fault tolerant and thus ensures that a failure of the non-safety chassis does not interfere with the safety function on the safety side of the V10 Tricon protection set. The fiber optic cables provide both physical and electrical isolation. For more information on this part of the architecture refer to NTX-SER-09-10 (Reference 9), Appendix 2.

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

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

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
#1 INTERDIVISIONAL COMMUNICATIONS		
As used in this document, interdivisional communications includes transmission of data and information among components in different electrical safety divisions and communications between a safety division and equipment that is not safety-related. It does not include communications within a single division. Interdivisional communications may be bidirectional or unidirectional.	N/A	Information only
STAFF POSITION Bidirectional communications among safety divisions and between safety and nonsafety equipment is acceptable provided certain restrictions are enforced to ensure that there will be no adverse impact on safety systems. Systems which include communications among safety divisions and/or bidirectional communications between a safety division and nonsafety equipment should adhere to the guidance described in the remainder of this section. Adherence to each point should be demonstrated by the applicant and verified by the reviewer. This verification should include detailed review of the system configuration and software specifications, and may also involve a review of selected software code.	None	As the PPS Replacement System will have bidirectional communication between a safety division and nonsafety equipment, adherence to the following 20 Points shall be demonstrated and verified.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS	
Point 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	Further technical detail on the V10 Tricon, including RXM isolation functions, can be found in the corresponding staff position in NTX-SER-09-10 (Reference 9).	P
Point 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		P

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		P

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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	None	P

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
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.		P

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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 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.	None	As described in the Triconex Topical Report, document 7286-545-1 (Reference 6), all Tricon communication with external devices is conducted and supervised by Tricon Communication Modules (TCMs). The TCMs operate asynchronously, sharing information only at end of the application processor scan. The TCM and the application processor are bridged with Dual Port RAM (DPRAM). When the host device requests data, the communication processor forwards the data from the application processor received at end of the previous scan. When a host device writes data, the communication processor passes the data to the application processor at next end of scan exchange. If there are any remaining communications tasks to be performed they are communicated in the next scan cycle(s). The hardware is designed, qualified, and fabricated in accordance with 10 CFR Part 50, Appendix A and B. Each RXM 4200-series 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 are responded to by the addressed RXM. These messages are also relayed to all portions of the system *within the leg*, but are ignored by all other modules. It should be noted that the I/O Bus is separated into command and response busses to eliminate erroneous messaging and 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. See Invensys document NTX-SER-09-10 (Reference 9) for additional technical details on the operation of the I/O Bus and RXM chassis.

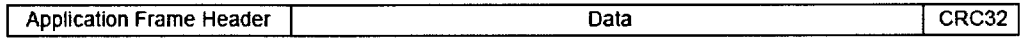
NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
The safety function circuits and program logic should ensure that the safety function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.		

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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	P To summarize the scan loop, 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 read or write communication function. TSAA "read" requests come from the Maintenance Workstation for data display or diagnostics. These are not safety critical and pose no threat to the safety function during normal operations. TSAA "write" requests are normally performed during plant outages when the process is shut down. The Tricon continuously monitors system health and performance, activating an alarm should scan time exceed the predicted performance. The PPS Tricon application program contains provisions for scan time performance per the application programming guidance in Appendix B of the Triconex Topical Report 7286-545-1 (Reference 6). Invensys documents provide formulas to estimate the maximum response time for the various I/O module types. The Invensys project application engineer utilizes the formulas and built-in features in the development of the safety-related application program.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		P

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 6 The safety function processor should perform no communication handshaking and should not accept interrupts from outside its own safety division.	None	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. Further information can be found in NTX-SER-09-10 (Reference 9).
Point 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 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.	None	All host communications are limited to Tricon-compatible protocols, briefly discussed in Section 4.0, 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. 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 are ignored by the IOCCOM and I/O modules. 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 used by external devices to request Tricon system variables or for retrieval of Tricon data points. It is not intended for safety-critical data communications, and thus does not impact the safety function upon failure. However, during application programming it is important to ensure that the necessary I/O tag names are identified and properly formatted for use by the Maintenance Workstation. Invensys document 993754-1-907, PPS Replacement Project Coding Guidelines, provides guidance on the I/O tag name database. 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

Header field	Type	nodeNumber	seqNum	version	flag	id	length
length in bytes	1	1	1	1	1	1	2

TSAA Application Frame Header format

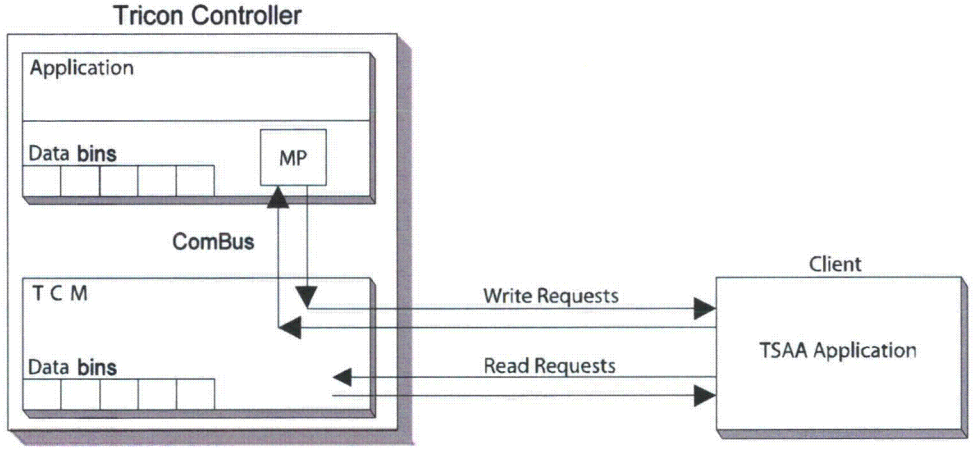
The following fields are contained in the Application Frame Header:

- 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.

Data: Variable-length data, depending on Type field. See response to Point 9 regarding how variables are organized on the Tricon controller and accessed by external hosts.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		CRC32: The 32-bit CRC of the TSAA message frame. The MODBUS TCP, P2P, and SAP protocols are not used. Further information can be found in the corresponding staff position in NTX-SER-09-10 (Reference 9).

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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	Data exchange between redundant safety divisions is not performed in the DCPP architecture. As discussed above in Point 2, data communications with non-safety systems in the same safety division (i.e., protection set) are handled by the TCM. The non-safety system may request any data points, and the TCM replies 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 the Tricon (such as during maintenance outages). Activities or applications requiring "write" requests at power are governed by DCPP site-specific procedural controls. As discussed in Invensys responses to other Points, 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. The design characteristics of the Tricon 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 that any failures of the non-safety Remote RXM Chassis, whether the Remote RXM modules or nonsafety I/O modules, do not adversely impact the safety function of the safety-related Main and Primary RXM Chassis. The PPS Replacement application design is such the safety functions do not depend upon the non-safety I/O points. The Project Management Plan, 993754-1-905, and the Software Development Plan, 993754-1-906, describe the application code development activities. The independent verification and validation activities are defined in the project Software Verification and Validation Plan, 993754-1-802.
Point 9 Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with	None	Tricon received data is stored in fixed aliased memory locations, which are utilized by the application processor when executing application logic. Input data is segregated from output data within memory. All communication messages are conducted by and stored in separate communication processors. Data is exchanged with the application processors at the end of each application program scan.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
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.		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 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 messages: **Read requests** – these are directly processed by the TCM. The communication module returns data from "bins" which mirror the bins stored on the safety-related 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." **Write requests** – these pass through the TCM and are processed by the safety-related 3008N MPs. The 3008N MPs are running the application program, and must vote these message types before

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		processing them. For write requests, if the data items are aliased read/write variables and remote access is enabled, the safety-related 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 the safety-related 3008N MPs, the TCM then responds with a success or failure message to the client. For the DCPP safety-related application, write requests are implemented with the TSAA protocol when the channel is placed out of service with the hardware OOS switch. These are cases where the control program requires upgrades, or instrument loop testing may require setpoint changes. These functions are handled under DCPP site procedural and physical access control. 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. Further information can be found in NTX-SER-09-10 (Reference 9).

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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 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	None	There are several layers of protection to prevent inadvertent application program changes. These include the Tricon keyswitch. 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: **Position** / **Value** (Decimal / Binary) Stop: 0 / 00 Program: 1 / 01 Run: 2 / 10 Remote: 3 / 11 The keyswitch position is voted between the three 3008N MPs and the voted value is used to perform 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 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

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.		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. P 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 the Tricon system and could not be performed on line and without a "Download All" command from TS1131.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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	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 when not in PROGRAM or when GATEDIS is active. See response to Point 3. 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 safety divisions (protection sets). With OOS in "Access Closed/Off," no external "writes" from the Maintenance Workstation are allowed. Invensys responses to Points 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 many engineered safety and reliability features of the Tricon provide reasonable assurance that communication failures do not adversely impact the safety function. Furthermore, site-specific administrative and physical access controls provide additional layers of protection against inadvertent and unauthorized changes to the application program.
Point 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.	None	The DCPP replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function, thereby ensuring that interdivisional communication faults will not occur. Responses to Staff Positions 2 and 4 in NTX-SER-09-10 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 safety-related 3008N MPs from communications. See NTX-SER-09-10 for additional details. 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

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
• 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. • 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.		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 discards 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. Further information on potential communication faults and mitigation can be found in NTX-SER-09-10 (Reference 9).

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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 as unrecoverable. None of this activity should affect the operation of the safety-function processor.	None	The PPS Replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function. Further platform specific information can be found in NTX-SER-09-10 (Reference 9).
Point 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 PPS Replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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	The Tricon is programmed to pass all values each scan, whether the values have changed or not. NTX-SER-09-10 Section 5.0 discusses the Tricon scan cycle in detail.
Point 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 Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)	None	The PPS Replacement architecture does not depend on any information or resource originating or residing outside its own safety division to accomplish its safety function. Invensys responses to Points 1 and 2 describe the independence of Tricon controllers from external devices and the engineered layers of protection against communication failures.
Point 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	None	The qualification of the V10 Tricon does not include the fiber optic cables. Since the TCM and the Remote RXM link do not constitute vital or safety links, the gradual degradation requirement does not apply. However, it has been established that the fiber optic cable meets electrical isolation requirements. It is possible to have a safety-related Primary RXM connected to a nonsafety-related Remote RXM chassis via triplicated multi-mode fiber optic cables between the 4200/4201 RXM Modules. No network communications are routed through the RXM Modules. As discussed in the V10 Tricon Topical Report (Reference 6), the 4200 and 4201 RXM Modules are qualified electrical isolation devices, because the fiber optic cable is incapable of propagating electrical faults between the RXM chassis. Therefore they meet the requirements of IEEE 384-1981 electrical isolation

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.		requirements for 1E-to-non1E isolation devices. The non-safety Remote RXM chassis does not have any safety-related I/O assigned to it. Furthermore, there are no I/O hardware or software failures that could occur in the non-safety Remote RXM chassis that would impact the functioning of the safety-related Main Chassis and Primary RXM. The Tricon, including RXM Chassis and 4200-series modules, has been qualified under the Invensys Appendix B program in accordance with EPRI TR-107330 (Reference 5) and Regulatory Guide 1.180 Rev. 1 (Reference 3). Further information can be found in NTX-SER-09-10 (Reference 9).

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 18 Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.	None	The 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 Point 10, the Tricon architecture ensures that the keyswitch, OOS switches, and programmed features in the PPS application program prevent changes to the application program and setpoints. This mitigates any deficiencies in the TCM with regard to performance deficits posed by unneeded functionality. A Failure Modes and Effects Analysis (FMEA) was performed on the V10 Tricon system in accordance with the applicable requirements of EPRI TR-107330 (Reference 5) Section 6.4.1. The results of the FMEA are documented in Invensys document 9600164-531 (Reference 11), The FMEA addressed failures of major components and at the module level. Document NTX-SER-09-10 Appendix 2 (Reference 9) included a FMEA tabulation which is an extension of the FMEA in 9600164-531 that postulates credible failures of the non-safety Remote RXM Chassis. The approach 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. Application programs for the DCPP Process Protection System are developed in accordance with programming guidance contained in Appendix B to the V10 Tricon Topical Report, 7286-545-1, and the NPSIM (Reference 8). Software development guidelines address good coding practices, including avoiding unused functionality and program complexity. The Project Plan, 993754-1-905, and the Software Development Plan, 993754-1-908, describe the application code development activities. The independent verification and validation activities are defined in the project Software Verification and Validation Plan, 993754-1-802.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
Point 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	The data rate capacity of the TCM and cabling far exceed the 3008N MP ability to initiate and receive non-vital data. 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 unlikely that data transfer between the TCM and client could be affected by the physical network. For TSAA 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 Point 9). TSAA "write" requests depend on scan time because the request must be communicated to and from the 3008N MPs. 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. See also Invensys response to Point 20 regarding response time. For the RXMs, 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. Further information can be found in NTX-SER-09-10 (Reference 9).
Point 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 the detector or sensor until the 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.

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
		The Tricon processor is only one contributor to the overall response time computation, and this variable for the PPS Replacement System is referred to as the "throughput" of the Tricon processor. Throughput in this case is 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, 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 are used to calculate the Tricon protection set 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 10) used for the V10 Tricon qualification project. A similar method will be followed for the PPS Replacement Project to determine the maximum allowable scan time for each protection set. Actual scan time, throughput, and data error rates are measured and recorded during the DCPP PPS Factory Acceptance Tests (FATs) in the System Response Time Confirmation Report, 993754-1-818 (Reference 14). The report is submitted as part of PPS Replacement Project Phase 2 deliverables. Further information can be found in NTX-SER-09-10 (Reference 9).

NRC GUIDANCE – ISG-04	Deviation	INVENSYS COMPLIANCE & COMMENTS
#2 COMMAND PRIORITIZATION	None	Not applicable to the DCPP Replacement Architecture.
#3 MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS	None	Not applicable to the DCPP Replacement Architecture.

6.0 REFERENCES

1) NRC Interim Staff Guidance (ISG) ISG-06, Task Working Group #6, "Licensing Process," Rev. 1.
2) NRC Interim Staff Guidance (ISG) ISG-04, Task Working Group #4, "Highly-Integrated Control Rooms—Communications Issues (HICRc)," Rev. 1.
3) Reg. Guide 1.180 Rev. 1, "Guidelines For Evaluating Electromagnetic And Radio-Frequency Interference In Safety-Related Instrumentation And Control Systems"
4) IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
5) EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants."
6) 7286-545-1, Triconex Topical Report, Rev. 4 (December 2010).
7) 9100089-001, Tricon V9/10 Failure Modes and Effects Analysis with Criticality Analysis," Version 1.0, July 2006.
8) NTX-SER-09-21, Nuclear System Integration Program Manual, Revision 1, April 2010.
9) NTX-SER-09-10, Tricon applications in Nuclear Reactor Protection Systems – Compliance with NRC ISG-2 & ISG-4, Revision 2, January 2011.
10) 9600164-731, Maximum Response Time Calculations, December 2005.
11) 9600164-531, Rev 0, "Failure Modes and Effects Analysis for the Tricon Version 10.2 Programmable Logic Controller."
12) PG&E Topical Report, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment."
13) PG&E Process Protection System Replacement Conceptual Design Document.
14) 993754-1-818, PPS Replacement Project System Response Time Confirmation Report.
15) 993754-1-905, PPS Replacement Project Project Management Plan.
16) 993754-1-802, PPS Replacement Project Software Verification and Validation Plan.
17) 993754-1-906, PPS Replacement Project Software Development Plan.
18) Diablo Canyon Power Plant, Units 1 and 2 – Safety Evaluation for Topical Report, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment," April 19, 2011 (ML110480845)