

| | |
|----------------------|--|
| 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

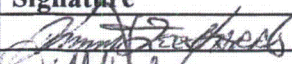
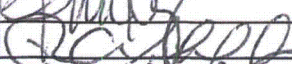

SYSTEM ARCHITECTURE DESCRIPTION (SAD)

Document No. 993754-1-914 (-NP)

Revision 0

October 20, 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: | K. Harris |  | Project Engineer |
| Review: | J. McKay |  | Application Engineer |
| Approval: | R. Shaffer |  | Project Manager |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 2 of 41 | Date: | 10/20/2011 |

| Document Change History | | | |
|-------------------------|------------|----------------|-----------|
| Revision | Date | Change | Author |
| 0 | 10/20/2011 | Initial issue. | K. Harris |
| | | | |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 3 of 41 | Date: | 10/20/2011 |

Table of Contents

| | |
|--|-----------|
| List of Tables | 5 |
| List of Figures..... | 6 |
| 1.0 Introduction | 7 |
| 1.1. PG&E PPS Architecture..... | 7 |
| 1.2. Acronyms | 12 |
| 1.3. References | 14 |
| 1.3.1. PG&E Documents..... | 14 |
| 1.3.2. NRC Documents | 14 |
| 1.3.3. Industry Documents | 14 |
| 1.3.4. Invensys Operations Management Documents | 14 |
| 2.0 V10 Tricon System | 15 |
| 2.1. TMR Architecture | 15 |
| 2.2. TRICON Fault Tolerance | 18 |
| 2.3. Safety System and Non-Safety System Independence | 19 |
| 2.4. Safety-to-Non-Safety Communications | 19 |
| 2.5. PPS Replacement System Hardware Configuration..... | 20 |
| 2.6. Field Signals..... | 22 |
| 2.7. Out-of-Service Switches..... | 22 |
| 2.8. Trip Switches..... | 23 |
| 2.9. Bypass Switches..... | 23 |
| 3.0 Hardware I/O Architecture..... | 24 |
| 4.0 Tricon Field Termination | 29 |
| 4.1. External Termination Assemblies (ETA)..... | 29 |
| 5.0 Tricon I/O and Communication Sub-Systems..... | 30 |
| 6.0 Input and Output Digital and Analog Signal Assignments..... | 31 |
| 7.0 Safety-Related Operating System Software Description..... | 32 |
| 7.1. Main Processor Module Software | 32 |
| 7.2. ETSX Operating Environment Software..... | 32 |
| 7.3. I/O Controller Software..... | 33 |
| 7.4. I/O Module Software..... | 33 |
| 7.5. Software Protective Functions (TS1131 Application Software) | 34 |
| 7.5.3. Wide Range Reactor Coolant Temperature..... | 37 |
| 7.5.4. Pressurizer Vapor Temperature..... | 38 |
| 7.5.5. Wide Range Reactor Coolant Pressure | 38 |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 4 of 41 | Date: | 10/20/2011 |

| | | |
|---------|---|----|
| 7.5.6. | Delta Temperature – Temperature Average (DTTA)..... | 38 |
| 7.5.7. | Steam Generator Narrow Range Level | 39 |
| 7.5.8. | Steamline Break Protection | 40 |
| 7.5.9. | Steamflow | 40 |
| 7.5.10. | Pressurizer Level..... | 41 |
| 7.5.11. | Turbine Impulse Chamber Pressure | 41 |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 5 of 41 | Date: | 10/20/2011 |

List of Tables

| | |
|---|----|
| Table 1. V10 Tricon PPS Protection Set Channel Functions..... | 10 |
| Table 2. Protection Set I I/O Configuration..... | 25 |
| Table 3. Protection Set II I/O Configuration | 26 |
| Table 4. Protection Set III I/O Configuration | 27 |
| Table 5 Protection Set IV I/O Configuration..... | 28 |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 6 of 41 | Date: | 10/20/2011 |

List of Figures

| | |
|---|----|
| Figure 1. Westinghouse PWR Reactor Protection Concept..... | 7 |
| Figure 2. Tricon Protection Set Architecture for the PPS Replacement System | 9 |
| Figure 3. TMR Architecture of the Tricon PLC System | 15 |
| Figure 4. Main Chassis (Typical)..... | 16 |
| Figure 5. Tricon Bus Systems and Power Distribution..... | 17 |
| Figure 6. Safety Related Main and Primary with Non-Safety related remote RXM..... | 21 |
| Figure 7 Software Architecture Of V10 Tricon TSAP | 35 |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 7 of 41 | Date: | 10/20/2011 |

1.0 Introduction

1.1 PG&E PPS Architecture

The Pacific Gas & Electric (PG&E) Diablo Canyon Power Plant (DCPP) Process Protection System (PPS) Replacement Project upgrades the existing Westinghouse Eagle 21 safety system. The scope of the equipment replacement is shown in the red box in Figure 1, below. The red box represents the Process Protection racks that contain the safety-related equipment.

The PPS monitors plant parameters, compares them against setpoints and provides signals to the Solid State Protection System (SSPS) if setpoints are exceeded. The SSPS evaluates the signals and performs Reactor Trip System (RTS) and Engineered Safety Feature Actuation System (ESFAS) functions to mitigate the event that is in progress. The SSPS, RTS, and ESFAS functions are not within the scope of the PPS Replacement Project.

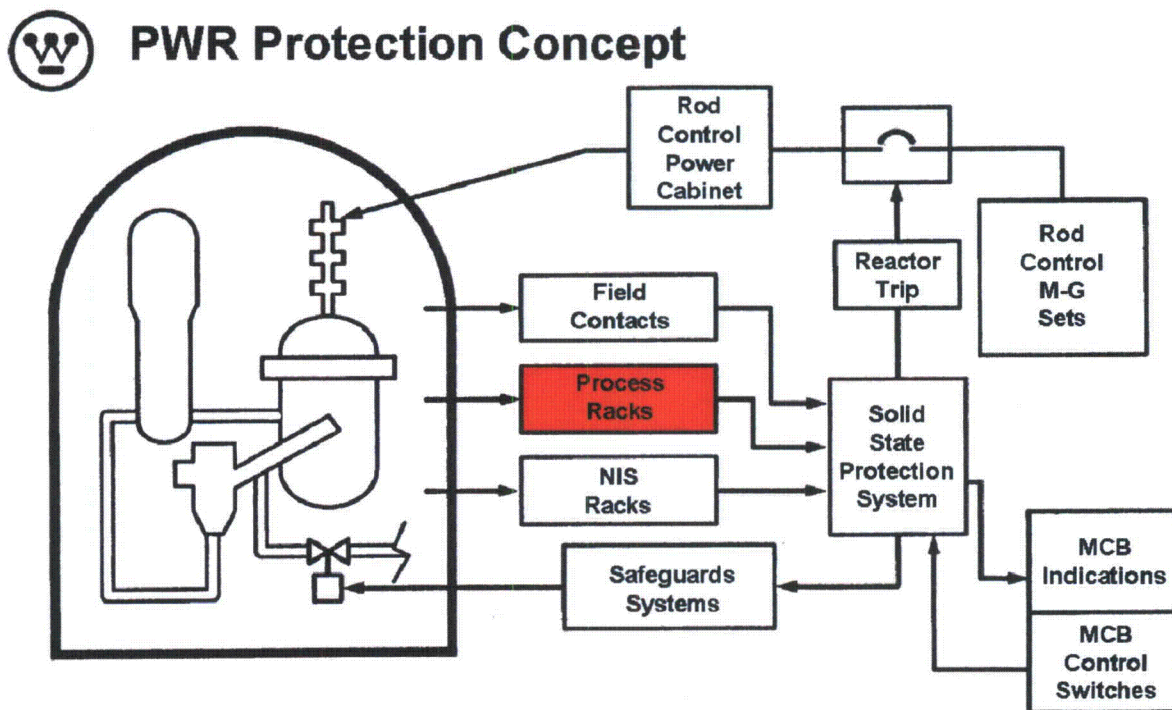


Figure 1. Westinghouse PWR Reactor Protection Concept

The PPS comprises four Protection Sets in sixteen racks. Separation of redundant process channels begins at the process sensors and is maintained in the field wiring, containment penetrations, and Protection Sets to the two redundant trains in the SSPS logic racks. Redundant process channels are separated by locating the electronics in different Protection Sets.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 8 of 41 | Date: | 10/20/2011 |

As shown in Figure 2, the replacement Protection Sets (I thru IV) each comprise the V10 Tricon, the Westinghouse Advanced Logic System (ALS) platform, the Maintenance Workstation (MWS), and various interface devices, such as the NetOptics Network Aggregator Tap and instrument loop isolators. The ALS is not within Invensys Operations Management scope of supply. However, the ALS converts sensor inputs to a signal type compatible with the V10 Tricon hardware. Specifically, the ALS processes resistance temperature detector (RTD) inputs and converts them to 4-20 milliamp signals. This conversion is necessary to satisfy Diablo Canyon Power Plant loop accuracy requirements. See the Functional Requirements Specification [Ref.1.3.1.3] for additional information.

The V10 Tricon portion of the PPS Replacement System comprises three V10 Tricon chassis per Protection Set: one safety-related Main Chassis, one safety-related Remote Expansion Chassis (RXM), and one nonsafety-related RXM chassis, see Figure 2. The Network Aggregator Tap, which is intended as an isolation device between the Tricon and the nonsafety plant network, is provided by PG&E to Invensys Operations Management for factory acceptance testing. The media converter between the Tricon Main Chassis and the Network Aggregator Tap, to be provided by PG&E, is necessary to convert the fiberoptic medium at the output of the Tricon Communication Module (TCM) to copper medium at the input of the Network Aggregator Tap.

The MWS is a nonsafety device developed separately from the PPS Replacement Project under a separate PG&E Purchase Order, budget, and staff. Development of the MWS is handled under a different project plan and by a separate project team. However, the MWS is part of the factory acceptance test of the V10 Tricon Protection Sets, as discussed in the Validation Test Plan, 993754-1-813 [Ref. 1.3.4.15]. The technical requirements for the Tricon-to-MWS interface are provided in PG&E Interface Requirements Specification [Ref. 1.3.1.4].

The functions required in each V10 Tricon Protection Set are listed in Table 1 below. See the Functional Requirements Specification [Ref. 1.3.1.3] for additional details on the protection functions and their design bases. As can be seen in Table 1, all PPS Protection Sets do not have the same channel safety functions. This difference among Protection Sets influences the PPS Replacement Project approach to hardware and software development, and independent verification and validation. The Conceptual Design Document [Ref. 1.3.1.2] and Functional Requirements Specification [Ref. 1.3.1.3] have additional detail on the hardware configuration of the PPS.

The four Protection Sets have different hardware and software requirements. The Main Chassis in each Protection Set executes the TriStation 1131 application code (the PT2 file), therefore the PPS requires four application programs (four PT2 files). The application programs are developed as nuclear safety-related Software Integrity Level 4 (SIL4) software per IEEE Standard 1012 1998 [Ref. 1.3.3.1] in accordance with the Project Management Plan (PMP), 993754-1-905 [Ref. 1.3.4.14].

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 9 of 41 | Date: | 10/20/2011 |

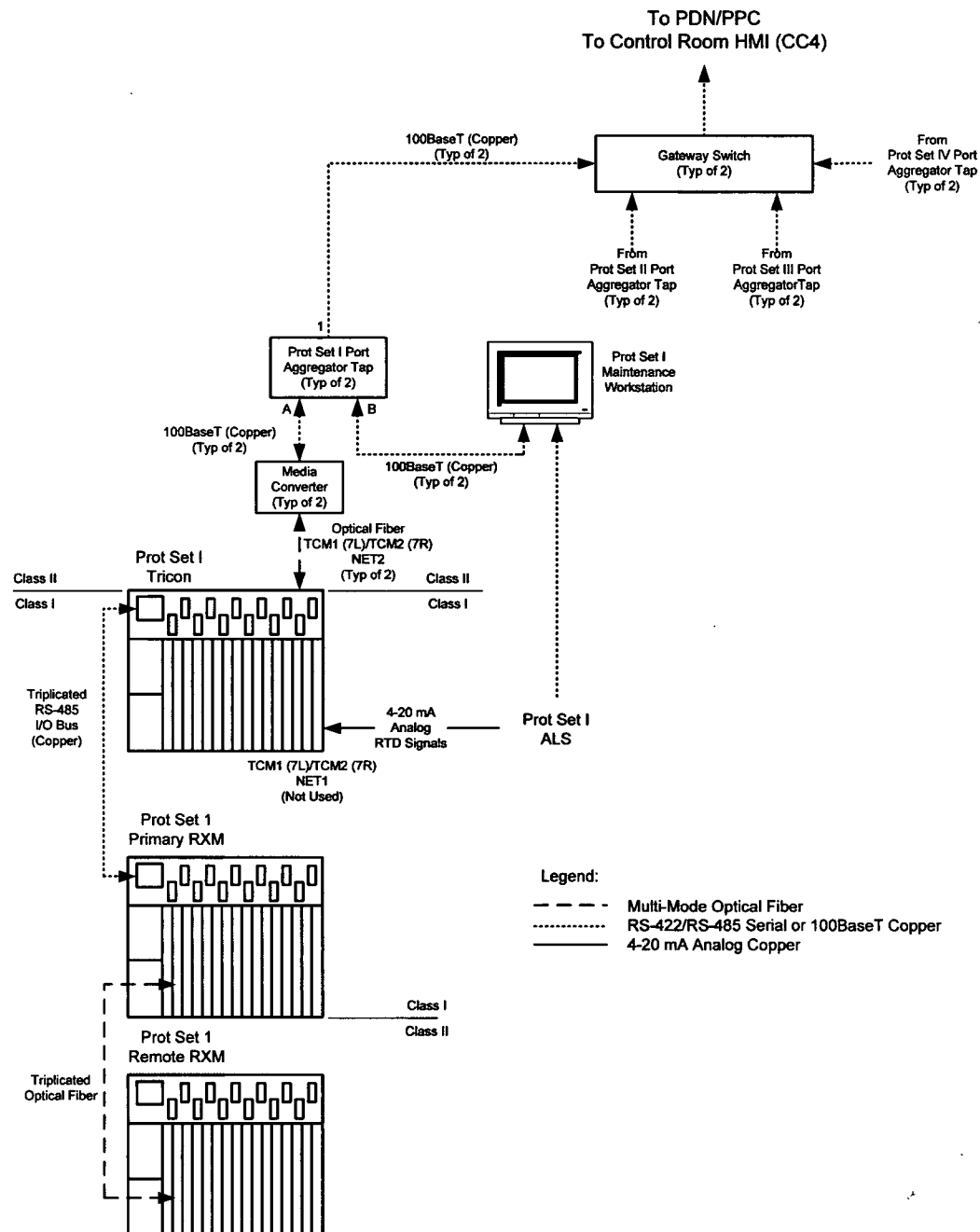


Figure 2. Tricon Protection Set Architecture for the PPS Replacement System

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 10 of 41 | Date: | 10/20/2011 |

Table 1. V10 Tricon PPS Protection Set Channel Functions

| Channel(s) | Purpose | Protection Set | | | |
|--|---|----------------|----|-----|----|
| Function | | I | II | III | IV |
| Wide Range Reactor Coolant Temperature Channels | | | | | |
| Input to Low Temperature Overpressure Protection System (LTOPS) | Provides protection against over-pressurization at low plant temperature | X | X | | |
| Wide Range Reactor Coolant Pressure Channels | | | | | |
| Input to LTOPS | Provides protection against over-pressurization at low plant temperature | | | X | X |
| Input to Residual Heat Removal (RHR) valve interlock circuit | Provides protection against improper operation of RHR isolation valves | | | X | X |
| Delta-T / Tavg (DTTA) Channels | | | | | |
| Overtemperature Delta-T (OTDT) Reactor Trip | Provides DNB protection | X | X | X | X |
| Overpower Delta-T (OPDT) Reactor Trip | Provides protection against excessive power (fuel rod rating protection) | X | X | X | X |
| Low-Low Tavg P-12 | Blocks steam dump to prevent undesired cooldown | X | X | X | X |
| Low Tavg Feedwater Isolation | Prevents excessive cooling after trip to maintain shutdown margin | X | X | X | X |
| Pressurizer Level Channels | | | | | |
| Pressurizer High Water Level Reactor Trip | <ul style="list-style-type: none">Provides backup protection to the Pressurizer High Pressure Reactor Trip, andPrevents the pressurizer from becoming water solid during low-power and -power rod withdrawal accidents | X | X | X | |
| Pressurizer Vapor Temperature Channel | | | | | |
| Pressurizer Vapor Space Temperature Low | RHR valve V-8701 interlock circuit input | | | | X |
| Steam Generator Steam Flow Channel | | | | | |
| Steam Flow Indication | Provide safety-related outputs for post-accident monitoring (S/G 1 thru 4) | X | X | | |
| Steamline Break Protection Channels | | | | | |
| Steamline Pressure Low SI and Steamline Isolation | <ul style="list-style-type: none">Initiate the automatic starting of boron injection and decay heat removal systems andProvide protection against steamline break accidents | X | X | X | X |
| Steamline Pressure High Negative Rate Steamline Isolation | Provide protection in the case of a steamline break when Pressurizer Pressure is less than the P-11 setpoint and Low Steamline Pressure SI is blocked | X | X | X | X |
| Steam Generator Narrow Range Level Channels | | | | | |
| Steam Generator (S/G) High-High Level Turbine Trip and Feedwater Isolation (P-14, S/G High Level Permissive) | Provides protection against S/G overfill and damage to the main steamlines or main turbine | X | X | X | X |
| S/G Low-Low Level Reactor Trip and Auxiliary Feedwater (AFW) Pump Start | Protects the reactor from loss of heat sink in the event of loss of feedwater to one or more S/Gs or a major feedwater line rupture | X | X | X | X |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 11 of 41 | Date: | 10/20/2011 |

| Channel(s) | Purpose | Protection Set | | | |
|---|---|----------------|----|-----|----|
| Function | | I | II | III | IV |
| Turbine Impulse Chamber Pressure Channels | | | | | |
| Turbine Impulse Chamber Pressure High to P-13 Interlock | <ul style="list-style-type: none">• Provide an input to P-7 indicative of low turbine power when less than the setpoint• P-7 permissive disables selected Reactor Trip signals at low power levels | X | X | | |
| Turbine Impulse Chamber Pressure Low Interlock C-5 | <ul style="list-style-type: none">• Blocks control rod withdrawal• The purpose of the C-5 interlock is to prevent automatic outward rod motion when power is less than the design limit for the Rod Control System | X | X | | |

A separate 3008N MP module controls each leg of the Tricon, shown in Figure 3, simplified Tricon block diagram, 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 processor section. Each application processor communicates with its I/O Controller/Communication Controller (IOCCOM) processor via a dual-port RAM (DPRAM). The application processor executes the Tricon System Executive (ET SX) 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).

Section 2.0 describes the Tricon V10 Triple Modular Redundant (TMR) architecture as utilized for the PG&E PPS Replacement Project. Section 3.0 describes the input/output (I/O) module configuration for the PPS Replacement Project and Section 4.0 describes the External Field Termination panels to be utilized for the project for all digital and analog field inputs and outputs. Section 5.0 and 6.0 describe the communication and I/O signals setup for Protections Sets I through IV.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 12 of 41 | Date: | 10/20/2011 |

1.2. Acronyms

| | |
|--------|---|
| AI | Analog Input |
| ALS | Advanced Logic System |
| AO | Analog Output |
| COMBUS | Communication Bus |
| CRC | Cyclic Redundancy Check |
| DCRO | Dry Contact Relay Output |
| DCS | Distributed Control System |
| DI | Digital Input. |
| DO | Digital Output. |
| DPRAM | Dual-Port RAM |
| ELCO | Brand name for standard rack & panel connector. |
| ESD | Electrostatic discharge |
| ESFAS | Engineered Safety Features Actuation System |
| ETA | External Termination Assembly |
| ETSX | Tricon System Executive |
| FTP | Field Termination Panel |
| IEC | International Electrotechnical Commission |
| I/O | Input/Output |
| IOCCOM | Input/Output Controller-Communications Controller |
| MAS | Main Annunciator System |
| MCR | Main Control Room |
| MP | Main Processor. |
| MWS | Maintenance Workstation |
| OOS | Out-of-Service |
| OVD | Output Voter Diagnostics |
| PCB | Printed Circuit Board |
| PG&E | Pacific Gas and Electric |
| PLC | Programmable Logic Controller |
| PMP | Project Management Plan |
| PPS | Process Protection System |
| RTOS | Real Time Operating System |
| RTD | Resistance Temperature Detector |
| RXM | Remote Expansion Chassis |
| RTS | Reactor Trip System |
| SIL | Software Integrity Level |
| SIS | Safety Instrumented System |
| SOE | Sequence of Events |
| SSPS | Solid State Protection System |
| TCM | Tricon Communications Module |
| TMR | Triple Modular Redundant |
| TSAP | TriStation Application Program |

i n v e n s y sTM

Operations Management

i n v e n s y sTM

Triconex

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 13 of 41 | Date: | 10/20/2011 |

TS1131
VDU

TriStation 1131.
Visual Display Units

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 14 of 41 | Date: | 10/20/2011 |

1.3. References

1.3.1. PG&E Documents

- 1.3.1.1. PG&E Purchase Order 3500897372.
- 1.3.1.2. PG&E Process Protection System Replacement Conceptual Design Document.
- 1.3.1.3. PG&E Functional Requirements Specification, 08-0015-SP-001.
- 1.3.1.4. PG&E Process Protection System Replacement Interface Requirements Specification.
- 1.3.1.5. PG&E DCPD PPS Controller Transfer Functions Design Input Specification; Spec. No.10115-J-NPG.

1.3.2. NRC Documents

- 1.3.2.1. DI&C-ISG-04, Digital Instrumentation and Controls Task Working Group #4: Highly-Integrated Control Rooms – Communications Issues Interim Staff Guidance, U.S. Nuclear Regulatory Commission.
- 1.3.2.2. DI&C-ISG-06, Digital Instrumentation and Controls Task Working Group #6: Licensing Process Interim Staff Guidance, U.S. Nuclear Regulatory Commission.
- 1.3.2.3. Title 10 of the Code of Federal Regulations, Part 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.
- 1.3.2.4. Regulatory Guide 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants, U.S. Nuclear Regulatory Commission.

1.3.3. Industry Documents

- 1.3.3.1. IEEE Standard 1012-1998, IEEE Standard for Software Verification and Validation.
- 1.3.3.2. NQA-1-1994, Quality Assurance Requirements for Nuclear Facility Applications.

1.3.4. Inven·sys Operations Management Documents

- 1.3.4.1. NSIPM, Nuclear Systems Integration Program Manual, NTX-SER-09-21.
- 1.3.4.2. IOM-Q2, Inven·sys Operations Management Nuclear Quality Assurance Manual.
- 1.3.4.3. V10 Tricon Topical Report, 7286-1-545, Inven·sys Operations Management (ADAMS Accession Number ML110140443).
- 1.3.4.4. Project Procedures Manual, Inven·sys Operations Management.
- 1.3.4.5. Manufacturing Department Manual, Inven·sys Operations Management.
- 1.3.4.6. NTX-SER-10-14, V10 Tricon Conformance to Regulatory Guide 1.152.
- 1.3.4.7. Tricon Planning and Installation Guide for Tricon v9-V10 Systems, 9700077-13.
- 1.3.4.8. Communication Guide for Tricon v9-V10, 9700088-008.
- 1.3.4.9. Field Termination Guide for Tricon v9-V10, 9700052-019.
- 1.3.4.10. Safety Considerations Guide for Tricon v9-v10 Systems, 9720097-008.
- 1.3.4.11. TriStation 1131 Developers Guide, 9720100-01x.
- 1.3.4.12. Compliance with NRC Interim Guidance ISG-2 & ISG-4, NTX-SER-09-10.
- 1.3.4.13. Equipment Qualification Summary Report, 96000164-545.
- 1.3.4.14. Project Management Plan, 993754-1-905
- 1.3.4.15. Validation Test Plan, 993754-1-813

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 15 of 41 | Date: | 10/20/2011 |

2.0 V10 Tricon System

This section describes the V10 Tricon overall system architecture as applied to the PG&E process protection systems and includes architecture drawings and fault tolerance descriptions.

2.1. TMR 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, as shown in Figure 3.

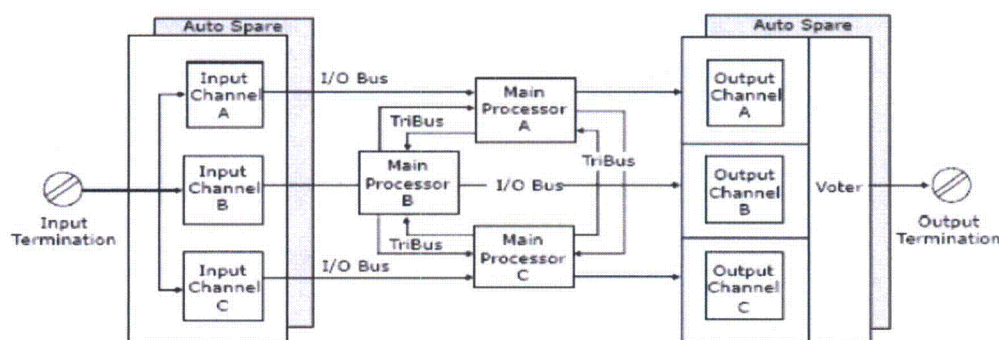


Figure 3. TMR Architecture of the Tricon PLC System

The V10 Tricon provides fault tolerance through a Triple Modular Redundant (TMR) architecture. The controller consists of three identical system channels, except for the Power Modules which are dual-redundant. Each channel independently executes the control program (also referred to as the TriStation Application Program) in parallel with the other two channels. Hardware voting mechanisms qualify and verify all digital inputs and outputs from the field; analog inputs are subject to a mid-value selection process.

Because each channel is isolated from the others, no single-point failure in any channel can pass to another. If a hardware failure occurs in one channel, the faulty channel is overridden by the other channels. Repairs consist of removing and replacing the module containing the faulty channel while the V10 Tricon is online and without process interruption. The controller then continues in full TMR operation.

Extensive diagnostics on each channel, module, and functional circuit immediately detect and report operational faults by means of indicators or alarms. The diagnostics also store information about faults in system variables. If faults are detected, the operator can use the diagnostic information to modify control actions or direct maintenance procedures.

Tricon Input/Output 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

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 16 of 41 | Date: | 10/20/2011 |

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. See the V10 Tricon Topical report [Ref. 1.3.4.3] for additional information.

Each V10 Tricon Protection Set includes a main chassis, illustrated in Figure 4, and a Primary remote extender chassis (Primary RXM) and a non-safety related remote extender chassis (Remote RXM).

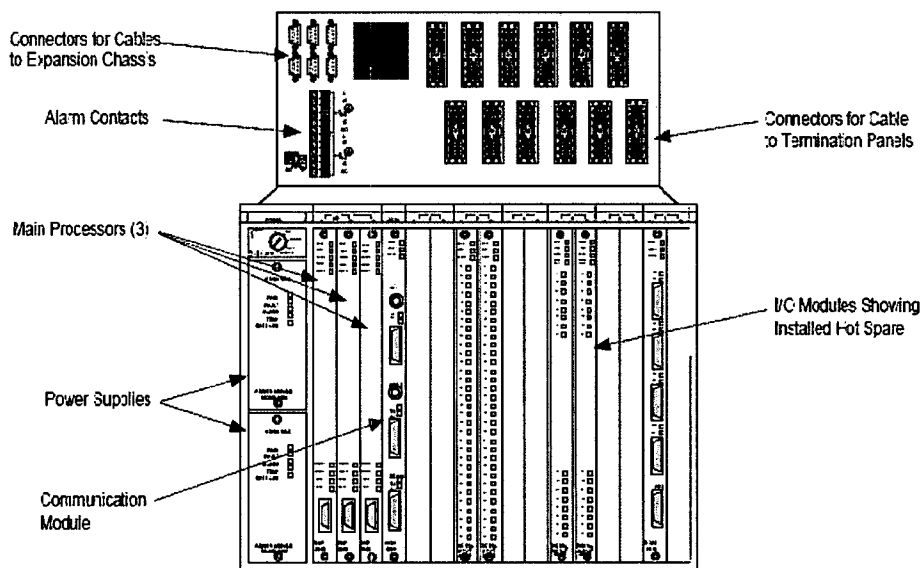


Figure 4. Main Chassis (Typical)

Figure 5, Tricon Bus Systems and Power Distribution depicts the three triplicated bus systems which are etched on the Main Chassis backplane: TriBus, I/O bus, and Communication bus.

The TriBus consists of three independent serial links that synchronize the Main Processors at the beginning of a scan, and performs either of these functions:

- Transfers I/O, diagnostic, and communication data.
- Compares data and flag disagreements of output or memory data from the previous scan.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 17 of 41 | Date: | 10/20/2011 |

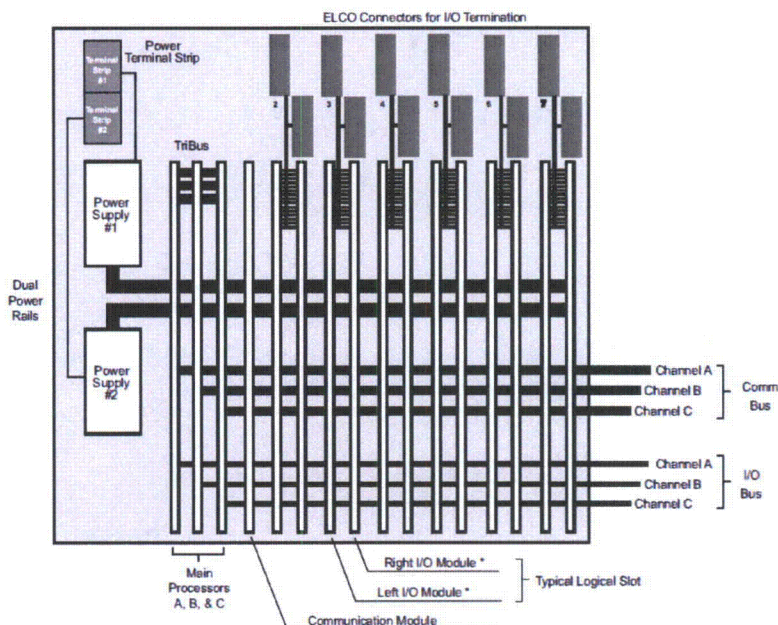


Figure 5. Tricon Bus Systems and Power Distribution

The triplicated I/O bus transfers data between the I/O modules and the Main Processors at 375 kilobits per second. The I/O bus is carried along the bottom of the backplane. Each channel of the I/O bus runs between one Main Processor and the corresponding channels on the I/O module. The I/O bus extends between chassis using a set of three I/O bus cables.

Each I/O module transfers signals to or from the field through its associated external termination assembly. Two positions in the chassis tie together as one logical slot. Termination cables are tied to panel connectors at the top of the backplane. Each connection extends from the termination assembly to both active and hot-spare I/O modules, which means both the active module and the hot-spare module receive the same information from the external termination wiring.

The Communication Bus runs between the Main Processors and the communication modules at 2 megabits per second.

Power for the chassis is distributed across two independent power rails and down the center of the backplane. Each module in the chassis draws power from both power rails through dual power regulators. There are four sets of power regulators on each input and output board: one set for each channel (A, B, and C) and one set for the status indicators.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 18 of 41 | Date: | 10/20/2011 |

2.2. TRICON Fault Tolerance

Fault tolerance, the most important capability of the V10 Tricon, is the ability to detect transient and steady-state error conditions and to take appropriate corrective action online. With fault tolerance, there is an increase in safety and an increase in the availability of the controller and the process being controlled.

Each Tricon-channel monitors dedicated sensors allowing bistable logic within the Tricon to operate completely independent of other Tricon-channels/divisions. As shown in Figure 6 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
- 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 faulted MP. The faulted 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.

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.

The primary RXM chassis will 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.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 19 of 41 | Date: | 10/20/2011 |

The RXM modules provide immunity against electrostatic and electromagnetic interference. Since the RXM modules are connected with fiber optic cables, they are 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 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.

2.3. Safety System and Non-Safety System Independence

For the configuration shown in Figure 6 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 the Primary and 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)" [Ref. 1.3.4.13].

The Primary RXM Chassis is connected to the Main Chassis using a 9000-series copper cable.

2.4. Safety-to-Non-Safety Communications

Interactions between safety and non-safety systems, such as the safety related Tricon and the MWS, are supported by the Tricon TCM for normal operations. Figure 2 shows data isolation between the Tricon and the non-safety MWS. The Tricon is isolated from the MWS by the TCM. The TCM provides data isolation and communication by fiberoptic media, also providing electrical isolation. The MWS is used to view plant variables and Tricon diagnostics during periodic functional surveillance testing. The workstation allows maintenance technicians and

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 20 of 41 | Date: | 10/20/2011 |

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 physically Out of Service and procedurally in bypass or trip. 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 MWSs. Note that for the PPS Replacement System: 1) there is one MWS per protection set, and 2) there are no communications or transfer of data between Protection Sets or between their associated MWSs. Each MWS communicates only with its own Protection Set.

2.5. PPS Replacement System Hardware Configuration

Two power supply modules 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 supply modules. The remainder of the chassis is divided into six logical slots for I/O and communication modules. Each logical slot provides two physical spaces for modules, one for the active module and the other for its optional hot-spare module. The Main Chassis includes one dedicated COM slot with no hot-spare position.

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 designated the “primary” RXM, is connected to the Main Chassis with the triplicated I/O bus cables. Subsequent RXM chassis, designated 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.

Figure 6 shows the V10 Tricon system bus architecture for the PG&E PPS, i.e., safety-related Main and Primary RXM Chassis and non-safety-related Remote RXM Chassis. The safety-to-non-safety 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. In accordance with PG&E Interface Requirements Specification [Ref. 1.3.1.4], Figure 6 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.)

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 21 of 41 | Date: | 10/20/2011 |

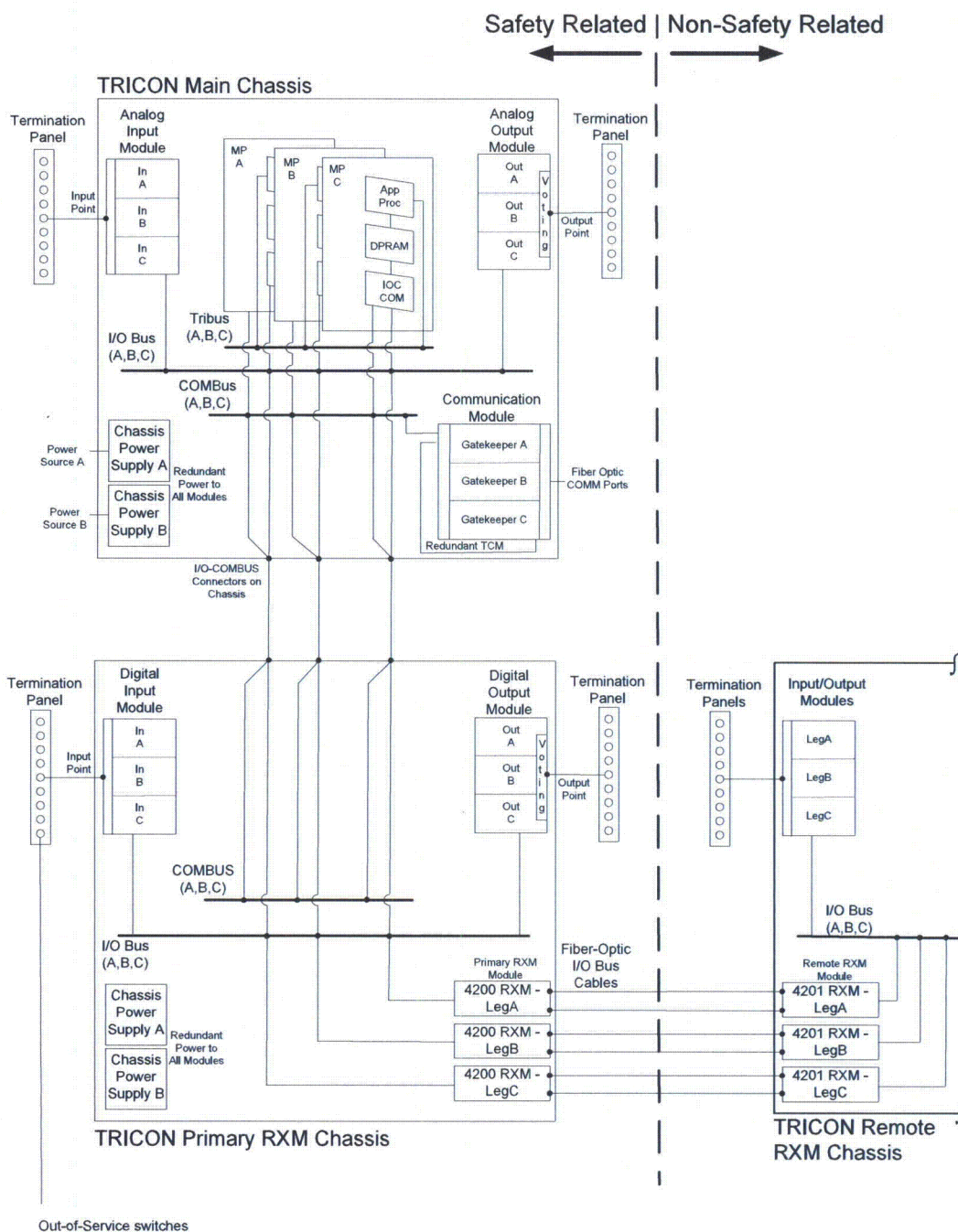


Figure 6. Safety Related Main and Primary with Non-Safety related remote RXM.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-I-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 22 of 41 | Date: | 10/20/2011 |

2.6. Field Signals

Each I/O module transfers signals to or from the field through its associated external termination assembly. Two positions in the chassis tie together as one logical slot. The first position holds the active I/O module and the second position is available for a hot-spare I/O module. This spare slot will be used to install a replacement for a failed module. Hot-spare modules will not be installed in the PPS Replacement System. Termination cables are connected to the top of the backplane. Each connection extends from the termination assembly to both positions in the logical slot.

Every digital input (DI) module houses the circuitry for three identical channels (A, B, and C). Although the channels reside on the same module, they are completely isolated from each other and operate independently. A fault on one channel cannot pass to another. In addition, each channel contains an 8-bit microprocessor called the I/O communication processor, which handles communication with its corresponding Main Processor.

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.

2.7. Out-of-Service Switches

Out-of Service (OOS) switches will be supplied by PG&E. When an OOS switch is activated, the V10 Tricon application program allows the associated instrument channel to be taken out of service while maintaining the remainder of the safety division operable (see Section 7.5.2). Operation of the hardware switch alone will not place the channel out of service. Out-of-Service confirmation is also required at the MWS to place the function out of service. When out of service a limited selection of parameters (such as tunable constants) may be modified. Features to limit inadvertent modification include, but are not limited to:

- While multiple safety functions can be simultaneously placed OOS, only one safety function can be modified at a time.
- Approved procedures and administrative controls are required to perform testing and updates.
- The parameter values to be updated are limited by the software application to predetermined ranges (see Section 7.5.2).
- The MWS software application will request operator confirmation that the parameter update process is complete prior to saving the new parameter values.
- Each OOS switch will be mechanically protected from accidental operation and access will be limited by installation in a locked Protection Cabinet.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 23 of 41 | Date: | 10/20/2011 |

Signals are provided to the Main Annunciator System if the external Out-of-Service switches are activated to indicate the condition in the control room.

2.8. Trip Switches

External trip switches are to be supplied by PG&E on PPS trip and actuation outputs to SSPS. The switches may also be used to trip or actuate the channel manually if needed (Ref.1.3.1.2, Section 1.2).

Activation of the external trip switches is indicated in the control room through the SSPS partial trip indicators.

2.9. Bypass Switches

Software Bypass Switches at the MWS are provided to allow testing and maintenance access to the Protective Function while the remainder of the Protection Set continues to operate normally. Placing a Protective Function into “Bypass” will remove it from the trip voting algorithm to allow maintenance, test, or parameter updates to that function.

A hardware bypass switch is provided by PG&E for the Turbine Impulse Chamber Pressure High to P-13interlock. Other Protective Functions are bypassed through the use of a software bypass switch initiated through the MWS. All bypass switches will bypass their channel outputs when selected, regardless of the associated comparator state.

Indication of a bypass condition is provided to the Main Annunciator System in the control room if a Bypass Switch is in the bypass position.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 24 of 41 | Date: | 10/20/2011 |

3.0 Hardware I/O Architecture

This Section provides the input and output module configuration for the four PG&E Protection Sets.

As described in Section 2.0, the PPS Replacement system is composed of a Main Chassis, a Safety Related Primary RXM, and a Non-Safety Remote RXM. I/O configuration for the four Protection Sets is summarized in Table 2 through Table 5 for Protection Sets I through IV.

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. The Primary RXM Chassis is connected to the Main Chassis using a 9000-series copper cable.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 25 of 41 | Date: | 10/20/2011 |

Table 2. Protection Set I I/O Configuration

| Safety / Non-Safety | Chassis | | Analog/ Digital | | Module | | Slot | No. of Active Points |
|---------------------|-------------|----|-----------------|---------|------------|---------------|--------------|------------------------|
| SAFETY | Main | | AI | 3703EN | | | | |
| | Main | | AI | 3721N | | | | |
| | Main | | AI | 3721N | | | | |
| | Main | | AO | 3805HN | | | | |
| | Main | | AO | 3805HN | | | | |
| | Primary RXM | | DI | 3503EN2 | | | | |
| | Primary RXM | | DI | 3501TN2 | | | | |
| | Primary RXM | | DO | 3601TN | | | | |
| | Primary RXM | | DO | 3601TN | | | | |
| NON-SAFETY | Remote RXM | | AO | 3805E | | | | |
| | Remote RXM | | DI | 3501E | | | | |
| | Remote RXM | | DO | 3636T | | | | |
| | AI | AO | DI | DO | Total Main | Total Primary | Total Remote | Total Protection Set I |
| Total I/O Points | | | | | | | | |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 26 of 41 | Date: | 10/20/2011 |

Table 3. Protection Set II I/O Configuration

| Safety / Non-Safety | Chassis | | | | Analog/ Digital | Module | Slot | No. of Active Points |
|---------------------|-------------|----|----|----|-----------------|---------------|--------------|-------------------------|
| SAFETY | Main | | | | AI | 3703EN | | |
| | Main | | | | AI | 3721N | | |
| | Main | | | | AI | 3721N | | |
| | Main | | | | AO | 3805HN | | |
| | Main | | | | AO | 3805HN | | |
| | Primary RXM | | | | DI | 3503EN2 | | |
| | Primary RXM | | | | DI | 3501TN2 | | |
| | Primary RXM | | | | DO | 3601TN | | |
| | Primary RXM | | | | DO | 3601TN | | |
| NON-SAFETY | Remote RXM | | | | AO | 3805E | | |
| | Remote RXM | | | | DI | 3501E | | |
| | Remote RXM | | | | DO | 3636T | | |
| | | | | | | | | |
| | AI | AO | DI | DO | Total Main | Total Primary | Total Remote | Total Protection Set II |
| Total I/O Points | | | | | | | | |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 27 of 41 | Date: | 10/20/2011 |

Table 4. Protection Set III I/O Configuration

| Safety / Non-Safety | Chassis | | Analog/ Digital | Module | | Slot | No. of Active Points | |
|------------------------|-------------|----|--------------------|---------|---------------|------------------|----------------------------|--------------------------------|
| SAFETY | Main | | AI | 3703EN | | | | |
| | Main | | AI | 3721N | | | | |
| | Main | | AI | 3721N | | | | |
| | Primary RXM | | DI | 3503EN2 | | | | |
| | Primary RXM | | DI | 3501TN2 | | | | |
| | Primary RXM | | DO | 3601TN | | | | |
| | Primary RXM | | DO | 3601TN | | | | |
| NON-SAFETY | Remote RXM | | AO | 3805E | | | | |
| | Remote RXM | | DI | 3501E | | | | |
| | Remote RXM | | DO | 3636T | | | | |
| | AI | AO | DI | DO | Total Main | Total Primary | Total Remote | Total Protection Set III |
| Total I/O Points | | | | | | | | |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 28 of 41 | Date: | 10/20/2011 |

Table 5 Protection Set IV I/O Configuration

| Safety / Non-Safety | Chassis | | Analog/ Digital | | Module | | Slot | No. of Active Points |
|---------------------|-------------|----|--------------------|----|---------------|------------------|-----------------|-------------------------------|
| SAFETY | Main | | AI | | 3703EN | | | |
| | Main | | AI | | 3721N | | | |
| | Main | | AI | | 3721N | | | |
| | Primary RXM | | DI | | 3503EN2 | | | |
| | Primary RXM | | DI | | 3501TN2 | | | |
| | Primary RXM | | DO | | 3601TN | | | |
| | Primary RXM | | DO | | 3601TN | | | |
| NON-SAFETY | Remote RXM | | AO | | 3805E | | | |
| | Remote RXM | | DI | | 3501E | | | |
| | Remote RXM | | DO | | 3636T | | | |
| | | | | | | | | |
| | AI | AO | DI | DO | Total Main | Total Primary | Total Remote | Total Protection Set IV |
| Total I/O Points | | | | | | | | |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 29 of 41 | Date: | 10/20/2011 |

4.0 Tricon Field Termination

V10 Tricon analog and digital input and output modules are connected to field instrumentation and control devices via the External Termination Assembly (ETA) panels.

4.1 External Termination Assemblies (ETA)

An External Termination Assembly (ETA) is an electrically-passive printed circuit board (PCB) to which field wiring is attached. A panel connector, terminal blocks, and optional components are mounted to the PCB and enclosed in a DIN-rail compatible plastic housing. A termination panel and associated cable pass input signals from the field directly to an input module, or pass output signals from an output module directly to field wiring. This arrangement permits the removal or replacement of I/O modules without disturbing field wiring.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 30 of 41 | Date: | 10/20/2011 |

5.0 Tricon I/O and Communication Sub-Systems

The V10 Tricon system has four separate bus structures;

- the Tribus;
- the communications bus;
- the I/O bus; and
- the bus internal to each of the main processor modules.

Each of these bus structures is triplicated.

The Tribus interconnects the three MP modules with each other, and is used for data transfer, voting, and program loading. The communications bus connects the MP modules with the Tricon Communications Modules. The I/O bus connects the MP modules to the I/O modules within the Main Chassis and the RXM Chassis. The internal bus in each MP module interconnects the application processors with the IOCCOM processors via the dual-port RAM. The internal bus also interconnects flash memory, non-volatile random access memory (NVRAM), dynamic random access memory (DRAM), and Tribus . Communication between the IOCCOM and the I/O modules is by way of the triple redundant I/O Bus. The I/O bus implements a serial, asynchronous RS485 Master/Slave protocol or “polling” protocol. Refer to. Triconex Topical Report, Section 1.2 [Ref. 1.3.4.3], for additional details on the internal bus architecture of the V10 Tricon.

The triple-redundant Main Processor sub-system retrieves the input signals from the I/O sub-system via the triple-redundant I/O Bus (i.e., legs A, B and C), executes the TriStation Application Program (TSAP) and sends outputs to the appropriate analog or digital output module. The three Main Processors communicate with each other via Tribus.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 31 of 41 | Date: | 10/20/2011 |

6.0 Input and Output Digital and Analog Signal Assignments

Input/output signals and their physical slot configuration is provided in Tables 2 through 5 for Protection Sets I through IV. Safety-Related Analog signals are primarily assigned to the safety-related Main Chassis for each Protection Set, and safety-related digital signals are primarily assigned to the safety-related Primary RXM chassis. Signals assigned to the non-safety related Remote RXM chassis are noted separately in the I/O tables.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 32 of 41 | Date: | 10/20/2011 |

7.0 Safety-Related Operating System Software Description

The Tricon Protection Set safety firmware resides on the triplicated Main Processors (MP) in the main chassis of each system. In addition to this safety firmware, the application-specific TriStation Application Program (TSAP) code is loaded onto the MPs. This software code is written using the TriStation 1131 Developer's Workbench, which allows the safety application to be written in either a structured-text format, Function Block Diagram format, or a combination of both. Individual programs in the TriStation project are written to address specific needs of the application project. Variable tagnames are created which can be accessed across programs in the project, or in specific cases accessed from external devices via the TCM. The Function Block Diagram format is a graphical interface which uses a standard, pre-approved library of functions. Using the standard library a programmer can create custom functions for repeated use, changing only the inputs and destinations of the outputs to that function.

The Tricon TSAP developed for the DCPD also contains application code enabling maintenance personnel to access or modify certain parameters of the TSAP while it is running without affecting the safety functions provided by the Tricon. Qualified personnel can open a small and pre-determined window of writable tag names in the Tricon by performing a series of actions designed to take a protective function out of service while maintenance is performed. This maintenance includes alarm testing, setpoint and tuning constant modification, and output testing. Any changes to parameters which affect the running safety system after it is returned to service must be acknowledged by the maintenance personnel initiating the changes before taking effect.

7.1 Main Processor Module Software

Each V10 Tricon system has three MP boards, each of which contains a separate copy of identical software. Each main processor board contains two microprocessors, the application processor and the Input/Output Control and Communication (IOCCOM) processor. Each of these 32-bit microprocessors are safety-related. The application processor runs both the ETSX operating environment software and the plant-specific application software. The IOCCOM can be thought of as two separate processes running in the same processor. The IOC process manages the I/O bus, and the COM runs communications related (COM) software, controlling the external communications bus functions of the Tricon Protection Set system.

7.2 ETSX Operating Environment Software

The application processor on the Model 3008N module is responsible for performing built-in self-diagnostics, managing the triple-redundancy features, and executing the application software. The operating system executes a sequence of steps in four main blocks, known as Power Up, Background, Scan Level, and Loader. A detailed description of the operating system is provided in document number 7286-1-545, V10 Tricon Topical Report [Ref.1.3.4.3]. The four main blocks perform the following:

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 33 of 41 | Date: | 10/20/2011 |

- Power Up performs memory, clock, and Tribus communication tests. These functions are only performed when the system is powered up or reset, and are not performed during normal operation.
- Background performs runtime diagnostic and fault analysis functions, including microprocessor checks, verification of constants stored in RAM, checks of the I/O and communication bus interfaces, checksum checks on the application programs, and Tribus fault analysis tests.
- Scan Level obtains and votes on input data, executes the application programs, and generates outputs at the scan cycle interval set by the application programs. The input data validation checks described above are completed during this step.
- Loader processes any TriStation messages when the key switch on the main chassis is in the "remote" position.

7.3. I/O Controller Software

The IOCCOM on the Model 3008N main processor module uses firmware that provides the interface between the main processor and the system I/O modules via the I/O bus. The IOCCOM interchanges data with the MP using the dual-port RAM data structures based on the I/O module configuration.

7.4. I/O Module Software

The V10 Tricon input modules are responsible for receiving sensor data from the attached instrumentation, manipulating the data as required, and passing the data to the IOCCOM via the I/O bus. The output modules receive data from the IOCCOM via the I/O bus, convert it as required, and pass it on to the connected output devices.

On each I/O module the firmware is replicated on each of the three legs, for use by the three leg-specific microprocessors, which exchange diagnostic data but not field data. The application software resides on the MP and not the I/O Module. The I/O modules do not contain plant-specific application software; however, an I/O module can be dedicated to a specific use in a plant-specific system by setting parameters within the system configuration and application code running on the MP. The firmware of the output modules continuously reads the output data provided by the main processor and updates the output registers of its own leg.

In both the input and output modules, the firmware is responsible for performing self diagnostics and handling communication with the main processor via each leg's individual I/O bus. This bus is a serial bus, and the I/O modules operate as slaves responding to requests from the master main processor board. The I/O data is continuously updated using an infinite loop that also runs diagnostics.

All I/O modules have both software and hardware watchdog timers to monitor and verify bus and module activity.

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 34 of 41 | Date: | 10/20/2011 |

7.5. Software Protective Functions (TS1131 Application Software)

The Tricon TSAP is designed to continuously provide safety protective functions while allowing maintenance and testing to be performed on a subset of these functions. Maintenance and updates can be performed while the rest of the Protection Set is under power and providing safety processing.

i n v e n s y sTM

Operations Management

i n v e n s y sTM

Triconex

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 35 of 41 | Date: | 10/20/2011 |

P

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 36 of 41 | Date: | 10/20/2011 |

7.5.1. Tricon System Diagnostics

The Tricon system is constantly performing internal diagnostics to ensure the validity and consistency of system integrity and programmed functions. Failures of these diagnostics are reported to external interfaces via the Trouble and Failure Alarms. Extra details on the individual drivers of these alarms can be accessed via the MWS.

P

7.5.2. Online Maintenance and Test

The Tricon PPS has been designed to allow online test and maintenance while the plant and Protection Sets are under power and functioning. Specific subfunctions of the Protective Functions can be removed from service to allow updating of plant operating parameters such as setpoints or tuning constants. Output value ranges can be tested, trip and bypass signals simulated and reported, and testmode alarms set to check MCR indicators are properly set. Any altered parameters for a function set to Out-of-Service (OOS) will have no influence on the protective function or Tricon PPS until the changes are acknowledged and the function returned to service by personnel with sufficient access privileges.

Online Maintenance and Test is available by using the OOS switch. In addition to the OOS hardware switch, authorized maintenance personnel must acknowledge the OOS status of the protective function before any online maintenance or test may be performed. Taking a protective function out of service will not affect the other safety functions of the Tricon, and thus maintenance and testing can be performed while the plant is at power. While multiple safety functions can be simultaneously placed out of service, only one protective function may be modified at a time.

P

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 37 of 41 | Date: | 10/20/2011 |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 38 of 41 | Date: | 10/20/2011 |

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 39 of 41 | Date: | 10/20/2011 |

i n v e n s y sTM

Operations Management

i n v e n s y s

Triconex

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 40 of 41 | Date: | 10/20/2011 |

P

| | | | | | |
|------------------|--------------|---------------|-------------------------------------|--------------|------------|
| Document: | 993754-1-914 | Title: | PPS System Architecture Description | | |
| Revision: | 0 | Page: | 41 of 41 | Date: | 10/20/2011 |