invensys
Operations Management

invensys
Triconex

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

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).

PACIFIC GAS & ELECTRIC COMPANY

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

FAILURE MODES AND EFFECTS ANALYSIS

Document No. 993754-1-811 (-NP)

Revision 1

February 21, 2014

	Name	Signature	Title
Author:	**D. Hoag**	David Alan Hoag	**Application Engineer**
Reviewer:	**G. McDonald**	Gayle R. McDonald	**IRE**
Approvals:	**D. Head**		**Project Manager**

Document Change History			
Revision	**Date**	**Change**	**Author**
0	10/31/2013	Initial Release	D. Hoag
1	02/21/2014	Revised to incorporate PG&E comments and reflect the IFS/FRS rev 9 changes.	D. Hoag

Table of Contents

LIST OF FIGURES **5**

LIST OF TABLES **6**

1. INTRODUCTION **7**

1.1 PURPOSE OF ANALYSIS 7
1.2 OBJECTIVE OF ANALYSIS 7
1.3 SCOPE OF ANALYSIS 7
1.4 METHOD OF ANALYSIS 7
1.5 ANALYSIS GUIDELINES 8

2 DEFINITIONS AND ACRONYMS **12**

2.1 DEFINITIONS 12
2.2 ACRONYMS 15

3 RELATED DOCUMENTS AND REFERENCES **16**

3.1 STANDARDS 16
3.2 INVENSYS PROJECT DOCUMENTS 16
3.3 INVENSYS DOCUMENTS 16
3.4 PACIFIC GAS AND ELECTRIC DOCUMENTS 16

4 SYSTEM AND DIAGNOSTIC OVERVIEW **17**

4.1 PROCESS PROTECTION SYSTEM (PPS) OVERVIEW 17
4.2 PLC MODULE DIAGNOSTIC DESCRIPTION 23
4.2.1 Input Modules *23*
4.2.2 Output Modules *25*
4.2.3 Main Processor Module *28*
4.2.4 Communications Module *30*
4.2.5 RXM Modules *31*
4.2.6 Tricon Chassis Assemblies *31*
4.2.7 Power Supply Modules *39*
4.2.8 Tricon Termination Panels *40*

5 DETAILED ANALYSIS **41**

5.1 TRICON HARDWARE ANALYSIS 41
5.2 KEY SWITCH ANALYSIS 42
5.3 BUYOUT ANALYSIS 44
5.4 TSAP TIMING ANALYSIS 44
5.4.1 Calculated TSAP Scan Time *44*
5.4.2 Failures Not Affecting Response Time *45*
5.5 SIGNAL LOADING 45

5.6 NON-DETECTABLE FAULTS 45
5.6.1 Drift 45
5.6.2 Stuck-At 47
5.6.3 Digital Input Points - Normally Off 47
5.6.4 Digital Output Points - Same Commanded State 48

6 SUMMARY AND CONCLUSIONS 49

6.1 ANALYSIS SUMMARY 49
6.2 DISCUSSION 49
6.3 RECOMMENDATIONS 50
6.4 CONCLUSIONS 50

APPENDIX A – FMEA; PPS TRICON (SAFETY RELATED COMPONENTS) 52

APPENDIX B – FMEA; PPS TRICON (NON-SAFETY RELATED COMPONENTS) 76

APPENDIX C – FMEA; SAFETY-RELATED SOFTWARE 84

APPENDIX D – FMEA; INPUT SIGNAL LOADING 85

APPENDIX E – FMEA; PPS BUYOUT COMPONENTS 88

List of Figures

Figure 1. Westinghouse PWR Reactor Protection Concept 17
Figure 2. Tricon Protection Set Architecture for the PPS Replacement System 19
Figure 3. Key Switch - TMR Gang Connections 32
Figure 4. Key Switch - Logic Flow 34
Figure 5. Key Switch - Disabling STOP from TriStation 35
Figure 6. Key Switch - Positions to Allow Client Access 36
Figure 7. Key Switch - Firmware in the Tricon MP 37

List of Tables

Table 1. Failure State Categories 9
Table 2. Failure State Categories – Further Clarification 10
Table 3. V10 Tricon PPS Protection Set Channel Functions 20
Table 4. Required Key Switch Settings for Command Categories 33
Table 5. 30-Month Drift Uncertainty for Analog Modules 46
Table 6. 30-Month Normally Off Proof Test Input Point List 47
Table 7. 30-Month Proof Test Output Point List 48

1. Introduction

Failure Modes and Effects Analysis (FMEA) is a systematic procedure for identifying the modes of failure and for evaluating their consequences. The essential function of an FMEA is to consider each major part of the system, how it may fail (the mode of failure), and what the effect of the failure on the system would be (the failure effect).

1.1 Purpose of Analysis

EPRI TR-107330 [Reference 3.1.2] defines the requirements for qualifying commercially available programmable logic controllers (PLCs) for safety-related nuclear power plant applications. The guidelines [Reference 3.1.2] require the performance of a FMEA to evaluate the effects of failures of components in the modules on PLC performance.

This FMEA will:

- Evaluate the effects and the sequences of events caused by each identified failure mode, from whatever cause, at various levels of the system's functional hierarchy;
- Determine the significance or criticality of each failure mode as to the system's correct function or performance and the impact on the reliability and/or safety of the controlled process;
- Classify identified failures according to whether the failures can be detected, diagnosed, or tested.
- Identify whether items may be replaced, compensated for, or whether operating provisions (repair, maintenance and logistics, etc.) provide other relevant characteristics.

1.2 Objective of Analysis

Invensys Operations Management is implementing the Tricon on the Process Protection System (PPS) replacement for the Diablo Canyon Power Plant PPS Replacement Project. This report documents the methodology and results of the FMEA performed on the Tricon portion of the PPS.

1.3 Scope of Analysis

The scope of this FMEA is limited to the analysis of the components of the PPS (refer to Section 4.1 for the PPS overview). These components include:

1. Tricon
2. Inputs
3. Outputs
4. Associated equipment
5. Software
6. Input Module Signal Loading
7. Critical timing requirements

The FMEA of the Associated Equipment addresses the impact of Class I component failures on the PPS.

1.4 Method of Analysis

This FMEA is performed in accordance with the applicable requirements of EPRI TR-107330 Section 6.4.1, "FMEA" [Reference 3.1.2]. In general, the techniques of Sections 4.1, 4.4, 4.5 and Appendix A of ANSI/IEEE Std. 352-1987 [Reference 3.1.1], have been used in this analysis. These techniques include

definition of functional areas of PLC operation, as described in Section 4.1 of this document. The effect of both single failures and common mode failures on each functional area were then analyzed, as detailed in Section 5, appendices A through E, and summarized in Section 6 of this document.

The FMEA data for the Tricon platform of the PPS Replacement is based on the Test Specimen configuration analyzed in Invensys document 9600164-531, "FMEA for Tricon V10.2 PLC" [Reference 3.3.4]. The Tricon V10.5.3 system continues to be represented by the V10.2 FMEA, as none of the subsequent software upgrades have impacted the baseline FMEA. The Tricon FMEA document [Reference 3.3.4] is referenced in 7286-545-1-A Rev 4, "NRC Approved Triconex Topical Report" [Reference 3.3.2]. The Test Specimen included one Tricon Main Chassis, two RXM Chassis and one Expansion Chassis. The Test Specimen configuration was established to simulate a single channel/train of a typical nuclear power plant safety-related protection system installation. These references form a baseline reference set to which PPS Replacement specifics are applied to generate a project specific FMEA relevant to the PPS Replacement.

Specific hardware configurations, application programs, supporting drawings and documents are identified in the System Architecture Description for PPS Replacement [Reference 3.2.2].

1.5 Analysis Guidelines

In this analysis, a safety related function is defined as the ability of the safety system to perform a safety shutdown function. In addition, the Tricon self-diagnostic features, described in Section 4.2 and Appendix A, and summarized in Section 6.1 of this report, have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the diagnostics detect all possible single failures within each module.

Because all single, internal failures are detected and alarmed, this FMEA focuses on credible failure modes of major components and modules in the PPS. The components considered include the following:

1. Power Supplies (including chassis power supplies and I/O loop power supplies)
2. Tricon Chassis (including internal power, communication buses, and key switch)
3. Main Processors and Communications Modules
4. Tricon I/O Modules
5. Termination Panels
6. Tricon Cables
7. Application Software
8. Input Module Signal Loading
9. Critical timing requirements

Figure 2 (in Section 4 of this document) is a simplified block diagram of the PPS Tricon equipment showing the arrangement of the major components. The approach used in this FMEA is to postulate credible failures of these components, identify the mechanisms that could cause these failure modes, and evaluate the consequences of these failures on the operation of the Tricon system. Because of the internal architecture of the Tricon, failure mechanisms that affect a single leg of the triple redundant system generally have no effect on system operation.

In order to identify the effect of failures on system operation (i.e., to prioritize types of failures), Section 4.2.3.5.C of Reference 3.1.2 recommends the following categories (C1 – C4) of failure states be identified as a part of the FMEA for PLCs with internal redundancy:

C1 - States that result from one or more failures where the PLC remains operable as well as states where it is not operable

C2 - States where undetected failures have occurred

C3 - States where a failure in a single element has caused the PLC to fail

C4 - States where failures reduce the effectiveness of self-diagnostics

Reference 3.1.2 also recommends identification of failures detected by the system diagnostics, and those that will only be detected by surveillance testing. For this FMEA, the failure categories specified by Reference 3.1.2 are modified to be more applicable to the Tricon system. The categories used in this FMEA are defined in Table 1, as follows:

P

The failure state categories of Table 1 are further clarified in Table 2, as follows:

P

For this FMEA, multiple failures are considered to include scenarios such as failure of all three Main Processors 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 catastrophic failures and to provide guidance for application design.

The FMEA tabulation in appendices A through E of this report includes a column that documents the appropriate failure category assignment for each postulated PLC failure mode. The tabulation in appendices A through E provides the following data for each type of failure, as required by the guidance of Reference 3.1.2:

a) Affected Components
b) Failure Mode
c) Failure Mechanism
d) Failure Category
e) Effect on PLC Inputs and Outputs
f) Effect on PLC Operability

Section 4.2 of this report provides a description of the PLC diagnostics that aid in detection of postulated failures.

2 Definitions and Acronyms

This section provides a list of abbreviations and definitions used in this document.

2.1 Definitions

Term	Definition
Commercial-Grade Dedication	Commercial-grade dedication is a process by which a commercial-grade item (CGI) is designated for use as a basic component. This acceptance process is undertaken to provide reasonable assurance that a CGI to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program. This assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses by the purchaser or third-party dedicating entity.
Diablo PPS	Diablo Canyon Power Plant Process Protection System.
Error	(1) The difference between a computed, observed, or measured value or condition, and the true, specified, or theoretically correct value or condition. For example, a difference of 30 meters between a computed result and the correct result. (2) An incorrect step, process, or data definition. For example, an incorrect instruction in a computer program. (3) An incorrect result. For example, a computed result of 12 when the correct result is 10. (4) A human action that produces an incorrect result. For example, an incorrect action on the part of a programmer or operator.
Failure	The inability of a system or component to perform its required functions within specified performance requirements. NOTE - The fault tolerance discipline distinguishes between a human action (a mistake), its manifestation (a hardware or software fault), the result of the fault (a failure), and the amount by which the result is incorrect (the error).
Failure Cause and/or Mechanism	Defects in requirements, design, process, quality control, handling or part application, which are the underlying cause or sequence of causes that initiate a process (mechanism) that leads to a failure mode over a certain time. A failure mode may have more causes. For example; fatigue or corrosion of a beam or contact is a failure mechanism and not a failure mode. The related failure mode (state) under analysis could be a "full fracture of structural beam" or for example "a open electrical contact". The initial Cause might have been "Improper application of corrosion protection layer (paint)" and /or "(abnormal) vibration input from another failed system".

Term	Definition
Failure Effect	Immediate consequences of a failure on operation, function or functionality, or status of some item.
Failure Mode	The manner or way by which a failure is observed in terms of failure of the part function under investigation; it may generally describe the way the failure occurs. It shall at least clearly describe a (end) failure state of the item/function under consideration as result of the failure mechanism (cause of the failure mode). For example; a fractured axle or an open electrical contact can be a failure mode.
Fault	(1) A defect in a hardware device or component; for example, a short circuit or broken wire. (2) An incorrect step, process, or data definition in a computer program. NOTE - This definition is used primarily by the fault tolerance discipline. In common usage, the terms “error” and “bug” are used to express this meaning.
Fault Tolerance	The ability to continue operating safely in the presence of a detected fault.
Integrity Level	A denotation of a range of values of a property of an item necessary to maintain system risks within acceptable limits. For items that perform mitigating functions, the property is the reliability with which the item must perform the mitigating function. For items whose failure can lead to a threat, the property is the limit on the frequency of that failure.
Maximum Allowable Scan Time	The allocated throughput time for the V10 Tricon portion not exceeding 200 milliseconds for any protective function.
Operability	A system, subsystem, train, component, or device shall be OPERABLE or have OPERABILITY when it is capable of performing its specified safety function(s) and when all necessary attendant instrumentation, controls, normal or emergency electrical power, cooling and seal water, lubrication, and other auxiliary equipment that are required for the system, subsystem, train, component, or device to perform its specified safety function(s) are also capable of performing their related support function(s).
Output Voter Diagnostics	Every Digital Output Module executes a specific type of Output Voter Diagnostics (OVD) for every point. This safety feature allows unrestricted operation under a variety of multiple-fault scenarios. In general, during OVD execution the commanded state of each point is momentarily reversed on one of the output drivers, one after another. Loopback on the module allows each microprocessor to read the output value for the point to determine whether a latent fault exists within the output circuit. (For devices that cannot tolerate a signal transition of any length, OVD on both AC and DC voltage Digital Output Modules can be disabled.)
PFDavg	Probability of Failure on Demand, average

Term	Definition
PPS Replacement	See Diablo PPS.
Response Time	The time from a physical input change to a physical output change.
Scan Time	The requested number of milliseconds for a scan (execution of the application) on the controller. The number is requested before an application is built. After the application is built and downloaded, the controller determines an actual scan time range and uses the specified scan time if it falls within these limits.
Safety Integrity Level (SIL)	SIL is a measurement of performance required for a Safety Instrumented Function.

2.2 Acronyms

Acronym	Definition
ANSI	American National Standards Institute
CGD	Commercial-Grade Dedication
CGI	Commercial-Grade Item
EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
ESF	Engineered Safety Feature
FMEA	Failure Modes and Effects Analysis
I/O	Input/output
IEEE	Institute of Electrical and Electronics Engineers
IRE	Independent Review Engineer
MAS	Main Annunciator System
MWS	Maintenance Work Station
ND	Nuclear Delivery
NRC	U.S. Nuclear Regulatory Commission
OOS	Out Of Service
OVD	Output Voter Diagnostics
PFD	Probability of Failure on Demand
PG&E	Pacific Gas and Electric
PPM	Project Procedures Manual
PPS	Process Protection System
PWR	Pressurized Water reactor
QA	Quality Assurance
RFI	Radio-Frequency Interference
RXM	Remote Extender Module
SER	Safety Evaluation Report
SIL	Safety Integrity Level
TSAP	TriStation Application Project

3 Related Documents and References

The following material was utilized in the development and support of this FMEA:

3.1 Standards

3.1.1 ANSI/IEEE Std. 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety System."

3.1.2 EPRI Report TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," Final Report, dated February 1, 1998.

3.1.3 IEEE Std. 379-2000, "IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class IE Systems".

3.2 Invensys Project Documents

3.2.1 993754-1-817, "Maximum TSAP Scan Time," Revision 1, dated April 9, 2012.

3.2.2 993754-1-914, "System Architecture Description," Revision 1, dated January 31, 2014.

3.3 Invensys Documents

3.3.1 Invensys Operations Management PPM, "Project Procedure Manual", Section PPM 2.03 - Project System Failure Modes and Effects Analysis, Revision 001, dated May 25, 2012.

3.3.2 7286-545-1-A Rev 4, "Triconex Approved Topical Report – Nuclear Qualification of v10 Tricon Triple Modular Redundant (TMR) PLC System – NRC Approved Version (TAC No. ME2435)," Revision 4, Issue Date: May 15, 2012.

3.3.3 9600164-527, "EMI / RFI Test Report" Revision 3, dated February, 2012.

3.3.4 9600164-531, "Failure Modes and Effects Analysis (FMEA) for the Tricon Version 10.2 Programmable Logic Controller," Rev. 1.2, dated August 3, 2012.

3.3.5 9600164-532, "Reliability/Availability Study for the Tricon Version 10 Programmable Logic Controller," Rev. 0, dated May 23, 2007.

3.3.6 9600164-732, "Reliability/Availability Spreadsheet for Tricon Version 10.2 PLC Operating under Normal Conditions," dated March 2, 2007.

3.3.7 9700077-018, "Tricon v9-v10 Planning and Installation Guide," July 2013.

3.3.8 9791007-025, "Technical Product Guide Tricon v10 Systems," July 2013.

3.3.9 9600460-001, "Tricon I/O Accuracy Including Drift Over Time for V10 Nuclear-Qualified Products," December 19, 2011.

3.3.10 9100069-001, "Tricon V9 ETP Design Specification," Revision 1.2, January 2006.

3.3.11 993754-1-916, "V10 Tricon Reference Design Change Analysis," Revision 0, March 19, 2012.

3.4 Pacific Gas and Electric Documents

3.4.1 993754-35R "PPS Document Transmittal" [DCPP operational data and initial tunable parameter settings; 4 attachments], dated December 13, 2012.

3.4.2 10115-J-NPG, "Process Protection System Controller Transfer Functions Design Input Specification," Revision 4, Issue Date: November 13, 2013.

4 System and Diagnostic Overview

4.1 Process Protection System (PPS) Overview

The Pacific Gas & Electric (PG&E) Diablo Canyon Power Plant (DCPP) PPS Replacement Project upgrades the existing Westinghouse Eagle 21 safety system. The scope of the equipment replacement is shown in the Process Racks box in Figure 1, below, which contains safety and non-safety Tricon and ALS.

The PPS monitors plant parameters, compares them against set points and provides signals to the Solid State Protection System (SSPS) if set points 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.

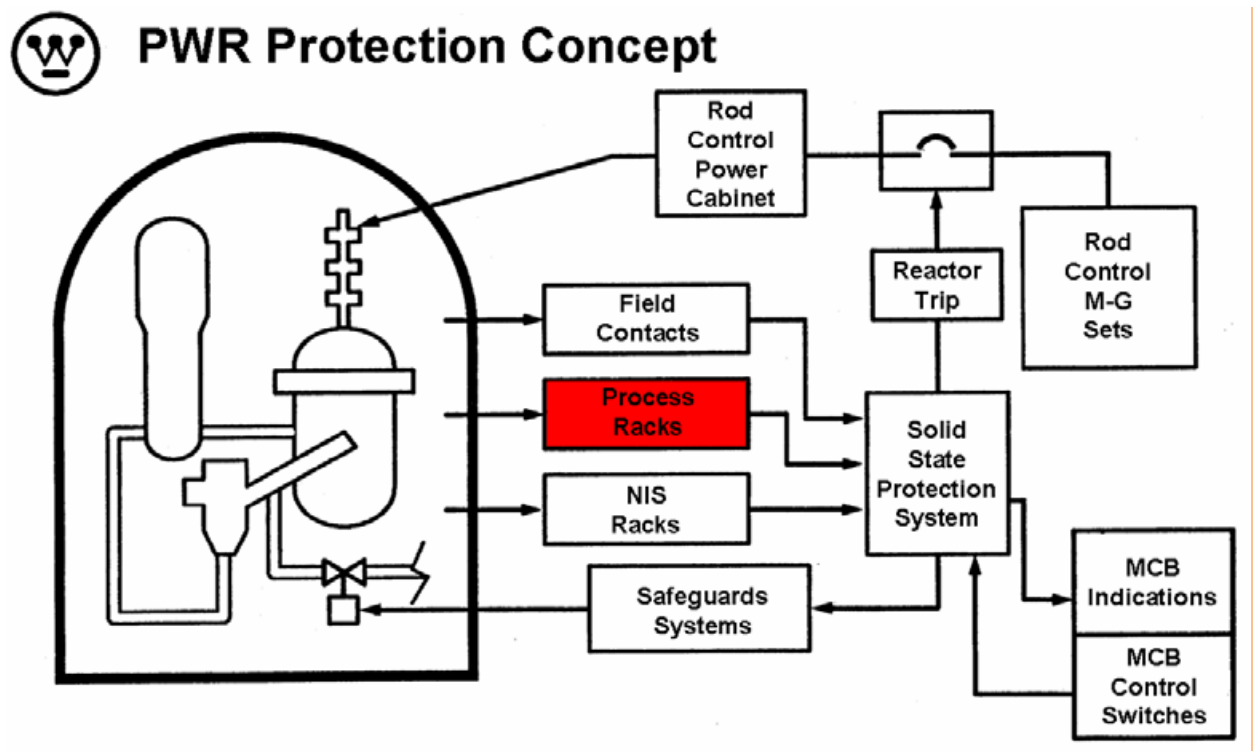


Figure 1. Westinghouse PWR Reactor Protection Concept

The PPS is composed of 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.

As shown in Figure 2, the replacement Protection Sets (I thru IV) each comprise the V10 Tricon, the Westinghouse Advanced Logic System (ALS) platform, separate Maintenance Workstations (MWS) for each Tricon and ALS system, 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.

The V10 Tricon portion of the PPS Replacement System is comprised of three V10 Tricon chassis per Protection Set: one safety-related Main Chassis, one safety-related Remote Expansion Chassis (RXM), and one non-safety related RXM chassis, see Figure 2. The Network Aggregator Tap, which is intended as a communications isolation device between the Tricon and the non-safety 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 fiber optic 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 non-safety 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. The MWS is used as a tool to perform testing.

The functions required in each V10 Tricon Protection Set are listed in Table 3 below. As can be seen in Table 3, 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 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.

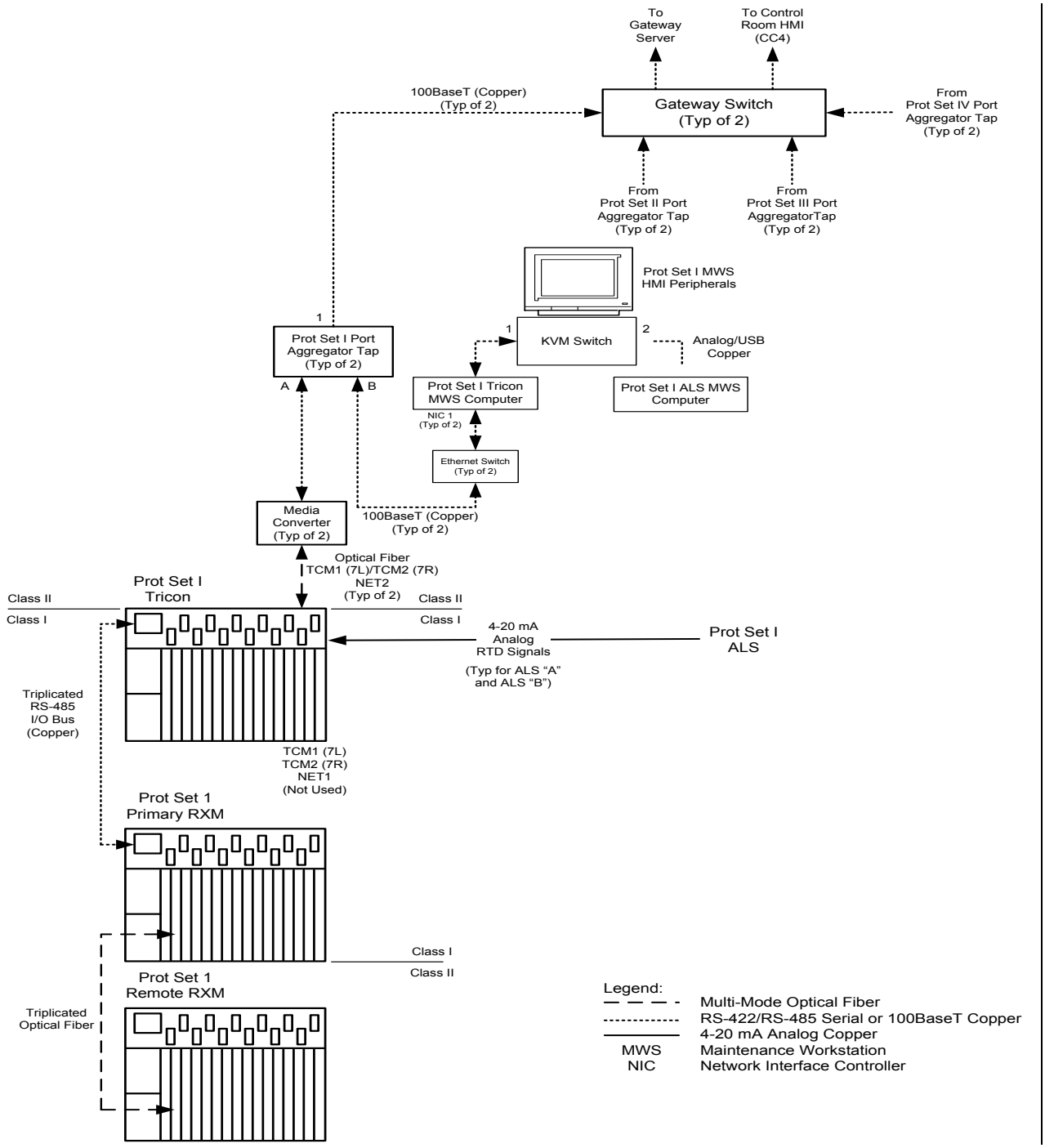


Figure 2. Tricon Protection Set Architecture for the PPS Replacement System

Table 3. V10 Tricon PPS Protection Set Channel Functions

Channel(s) Function	Purpose	Protection Set 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					
Over Temperature 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 cool down.	X	X	X	X
Low Tavg Feed Water Isolation	• Prevents excessive cooling after trip to maintain shutdown margin.	X	X	X	X
Pressurizer Level Channels					
Pressurizer High Water Level Reactor Trip	• Provides backup protection to the Pressurizer High Pressure Reactor Trip. • Prevents the Pressurizer from becoming water solid during low-worth 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		
Steam line Break Protection Channels					
Steam line Pressure Low SI and Steam line Isolation	• Initiate the automatic starting of boron injection and decay heat removal systems. • Provide protection against steam line break accidents.	X	X	X	X
Steam line Pressure High Negative Rate Steam line Isolation	• Provide protection in the case of a steam line break when Pressurizer Pressure is less than the P-11 set point and Low Steam line 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 steam lines or main turbine.	X	X	X	X
S/G Low-Low Level Reactor Trip and Auxiliary Feed water (AFW) Pump Start	• Protects the reactor from loss of heat sink in the event of loss of feed water to one or more S/Gs or a major feed water line rupture.	X	X	X	X
Turbine Impulse Chamber Pressure Channels					
Turbine Impulse Chamber Pressure High to P-13 Interlock	• Provide an input to P-7 indicative of low turbine power when less than the set point. • P-7 permissive disables selected Reactor Trip signals at low power levels.	X	X		
Turbine Impulse Chamber Pressure Low Interlock C-5	• Blocks control rod withdrawal by preventing automatic outward rod motion when power is less than the design limit for the Rod Control System.	X			

The Tricon uses a fault-tolerant triple modular redundant (TMR) architecture. The system design identifies and compensates for failed system elements, which facilitates its use in critical and safety-related process applications. The Tricon self-diagnostics features, described in Reference 3.3.4, have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the online diagnostics will detect a very high percentage of failures within each module. The diagnostic coverage for the Main Processors and the common processing circuitry on the I/O modules are in the 95 to 99% range. The diagnostic coverage for the I/O point circuitry on the I/O modules for the Tricon platform is 99% [Reference 3.3.5]. The Reliability Analysis Report (document number 993754-1-819) provides additional analysis of the diagnostic coverage specific to the PPS Replacement application.

Invensys has qualified specific Tricon v10 products for use in 1E (safety-related) applications in nuclear power plants in accordance with EPRI Report TR-107330, "Generic Requirements Specification for Qualifying Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants." EMC testing was performed in accordance with USNRC Regulatory Guide 1.180, Revision 1, "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems."

All of the information (specifications, simplified schematics, installation guidelines, and so on) for standard equipment also applies to nuclear equipment.

The Tricon system design information presented in Reference 3.3.4 includes recommendations for periodic off-line testing of field inputs and outputs. These recommendations establish general surveillance techniques and surveillance intervals intended to maintain the high reliability of the overall control system.

The Invensys Operations Management (Invensys) scope of components includes the analog and digital input/output modules, the field termination assemblies as the signals enter and exit the Tricon, power supplies, Main Processors, chassis assemblies, cables, and communication modules.

In particular:

Main Processor Modules

1. 3008N Main Processor

V10 Tricon Chassis

2. 8110N2 Tricon Main Chassis - High Density
3. 8112N Tricon RXM Chassis - High Density
4. 8112 Tricon RXM Chassis - High Density

RXM I/O Expansion Modules

5. 4200N Primary RXM 3-1 Fiber Optic Set
6. 4201 Secondary RXM 3-1 Fiber Optic Set

Power Modules

7. 8310N2 High Density Power Module, 120 VAC
8. 8310 High Density Power Module, 120 VAC

Cables

9. 9000NJ I/O-COMM Bus Cables

Communication Module

10. 4352AN TCM - Tricon Communication Module, Fiber Optic A

Digital Input Modules

11. 3501TN2 EDI - Enhanced Digital Input, 115 VAC/VDC, 32 pts, TMR Opto-isolated
12. 3503EN2 EDI - Enhanced Digital Input, 24 VAC/VDC, 32 pts, Commoned, Self-Test
13. 3501E EDI - Enhanced Digital Input, 115 VAC/VDC, 32 pts, TMR Opto-isolated (NS)

Digital Output Modules

14. 3601TN EDO - Enhanced Digital Output, 115 VAC, 16 pts, opto-isolated

Relay Output Module

15. 3636T RO – Relay Output (non-triplicated), Normally Open, 32 pts (NS)

Analog Input Modules

16. 3703EN EAI - Enhanced Analog Input, 0 –5VDC or 0 – 10VDC, isolated 16 pts
17. 3721N NGAI - Analog Input Module, ; 0–5 VDC or –5 to +5 VDC, 32 pts

Analog Output Modules

18. 3805HN EAO - Enhanced Analog Output, 4-20 mA, 8 points
19. 3805E EAO - Enhanced Analog Output, 4-20 mA, 8 points (NS)

Termination Panels

20. 9561-810NJ Termination Panel for 3501TN2 EDI Module, 115 VAC/VDC
21. 9563-810NJ Termination Panel for 3503EN2 EDI Module, 24VAC/VDC
22. 9663-610NJ Termination Panel for 3601TN EDO Module 115VAC
23. 9783-110NJ Termination Panel for 3703EN EAI Module 0-5VDC/0-10VDC
24. 9792-610NJ Termination Panel for 3721N NGAI Module 0-5VDC/-5 to +5VDC
25. 9860-610NJ Termination Panel for 3805HN EAO Module 4-20 mA
26. 9561-810F Termination Panel for 3501E EDI Module, 115VAC/VDC (NS)
27. 9853-610F Termination Panel for 3805E EAO Module 4-20 mA (NS)
28. 9668-110F Termination Panel for 3636T RO Module (NS)

4.2 PLC Module Diagnostic Description

This section provides a basic description of the Tricon processor, communications and input/output module operation and diagnostic functions. This description of the diagnostic operations is provided to augment the FMEA tabulation provided in appendices A through E. A more detailed description of this information is presented in References 3.3.4 and 3.3.5.

4.2.1 Input Modules

All triple modular redundant (TMR) input modules contain three separate, independent processing systems, referred to as legs, for signal processing (Input Legs A, B, and C). The legs receive signals from common field input termination points. The microprocessor in each leg continually polls the input points, and constantly updates a private input data table in each leg's local memory. Any signal conditioning, isolation, or processing required for each leg is also performed independently. The input modules possess sufficient leg-to-leg isolation and independence so that a component failure in one leg will not affect the signal processing in the other two legs.

4.2.1.1 Digital Input Modules

This discussion is applicable to the following digital input (DI) modules:

- Model 3501TN2 115 Vac/Vdc Opto-isolated, non-commoned (32 points)
- Model 3501E 115 Vac/Vdc Opto-isolated, non-commoned (32 points)
- Model 3503EN2 24 Vac/Vdc Commoned in groups of 8, Self Test (32 points)

Each DI module contains the circuitry for three identical legs. The three legs are completely isolated from each other and operate independently, so a fault on one leg cannot pass to another. There is an 8-bit microprocessor, called the I/O communication processor on each Main Processor Module to control communication with all I/O modules on a specific leg.

The three input legs independently measure each input signal, determine the respective state of each input signal, and place the values into input tables A, B, and C. Each input table is regularly interrogated over the leg-specific I/O busses by the I/O communication processor located on the corresponding Main Processor module. For TMR digital modules, all critical signal paths are triplicated. Each leg conditions signals independently and provides optical isolation between the field and the Tricon.

Each DI module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module Fault Indicator, which in turn activates the chassis alarm signal. The module is designed to operate correctly in the presence of a single fault and may continue to operate properly with some multiple faults.

The diagnostic routine for the Model 3501TN2 DI Module compares the input table data for the three legs. Any data discrepancies are reported to the respective Main Processor Modules, which maintain diagnostic information in local memory. The Main Processor Module fault analyzer routines determine whether a fault exists on a particular module at the end of each scan. One-time or short term differences that result from sample timing variations are distinguished from a pattern of differing data. Should a Main Processor Module diagnose a faulty leg, a fault indicator will be illuminated on that particular input module.

Failed optical isolation or signal processing/conditioning components could inhibit the ability of a module to communicate field input state transitions to the Main Processor Modules. Therefore, when a DI module is used to monitor field inputs signals that remain in one state for long periods of time, the field points should be toggled from the normal operational state to the opposite state within twenty-four months. Input signal toggling will test the module's ability to transition to the opposite state in order to diagnose problems such as "Stuck On" / "Stuck Off" signals due to failed or faulted leg components. Since normal opto-isolator failures are random and detectable due to the TMR sampling of inputs, only a single failure per input is likely. Even with stuck on faults on a single input leg, the other two input legs would vote out the failed opto-isolator.

The Model 3503EN2 DI modules extend fault coverage by self-diagnosing "Stuck On" leg signals. The DI modules are designed to monitor field signals that remain in the "On" state for long periods of time. The extended diagnostics verify the leg can process a transition to the "Off" commanded state.

The DI modules contain loopback circuitry in each leg that momentarily drives the input signal for the leg under test to the "logical zero" or "low" state. This test, which is continually rotated among the three legs, verifies proper operation of leg optical isolation and/or signal processing/conditioning circuitry. Should a leg fail the test, the module fault indicator will be illuminated. However, if these modules monitor normally off points, the field point must be toggled from the "Off" state to the "On" state.

The DI module diagnostics are specified to operate as follows:

Module	Minimum Input Toggle Rate	Maximum Input Toggle Rate
Model 3501TN2	Every 24 months	Every 100 msec
Model 3501E	Every 24 months	Every 100 msec
Model 3503EN2	On-state: Not required Off-state: Every 24 months	Every 100 msec

4.2.1.2 Analog Input Modules

This discussion is applicable to the following analog input (AI) modules:

- Model 3703EN 0-5/0-10 Vdc Differential, Isolated (16 points)
- Model 3721N 0-5/-5 to +5 Vdc Differential, DC Coupled (32 points)

Each of the three AI legs asynchronously measure the input signal and place the results into an input table of values, which is passed to its associated Main Processor module using the corresponding I/O bus. The input table in each Main Processor module is transferred to its neighbor across the TRIBUS. The median value is selected by each Main Processor (in a duplex mode, the average value is used), and the input table in each Main Processor is corrected accordingly. Signals outside an internally specified error band in this median signal selection process will be alarmed by the Main Processor on the input module. Each AI module leg is automatically calibrated using multiple reference voltages read through the multiplexer, which determine the gain and bias required to adjust the readings of the A/D converter. Several drift over time components can affect the automatically calibrated level and cannot be calibrated out (Reference 3.3.9).

Each AI module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module Fault Indicator, which in turn activates the chassis alarm signal. The module is designed to operate correctly in the presence of a single fault, and may continue to operate properly with some multiple faults.

The extent of the diagnostic routine for the Model 3721N AI modules includes automatic or self-calibration of the A/D converters in each of the three legs. The microprocessors on each leg test for known or expected signal values within a certain tolerance. If the signals reaching the leg microprocessors are within the allowed tolerance, the leg will self-calibrate its A/D converter to null out any undesirable offsets or gains. A leg in violation of the allowed tolerance will be flagged by illumination of a module Fault LED.

The Model 3703EN AI module performs cross comparison of input table data across the three legs, within the module. The microprocessors in each leg compare the respective input table data with the neighbor legs, with out-of-tolerance data reported to respective Main Processor Modules. The Main Processor Module fault analyzer routines diagnose faulty input module legs at the end of each scan. One-time and short-term differences that result from sample timing variations are distinguished from a pattern of differing data. Should a Main Processor Module diagnose a faulty leg on a particular module, it will signal the input module to illuminate its Fault LED.

The AI module diagnostics are specified to operate as follows:

Module	Minimum Input Change	Input Change Sample Period	Minimum Period of Mis-compares
Model 3703EN	0.5% of full scale	1 scan or 50 msec, whichever is greater	256 samples
Model 3721N	0.25% of full scale	20 ms	25 samples

For a single input reading, a leg-to-leg deviation may result if the measured values of the three legs differ by the minimum input change specified. If the deviations continue for the specified minimum period, an input fault may be declared.

4.2.2 Output Modules

4.2.2.1 Digital Output Modules

This discussion is applicable to the following digital output (DO) modules:

- Model 3601TN 115 Vac Opto-isolated, Non-commoned (16 points)

Every DO module contains three identical and isolated legs. Each leg includes an I/O microprocessor that receives its output table from the Main Processor's I/O communication processor associated with that leg. All of the DO modules use special quadruplicated output circuitry that votes on the individual output signals. This voter circuitry is based on parallel-series paths that pass power if the driver for legs A and B, or legs B and C, or legs A and C command them to close (i.e., 2-out-of-3 vote).

A single switch failure will not affect the logic, which is optimized for de-energize-to-trip applications. The switches are opened and closed on command by the Output Switch Drive circuitry. Power will be

passed to the load if the commanded state of Channels A and B, or Channels A and C, or Channels B and C feeding the Switch Drive Circuitry are "On" or energized, completing the path between the voltage source and the load. Any single leg failure, any single switch failure, or corrupted signal from a Main Processor Module will be compensated for or filtered out by the Voter Logic at the output module level.

All DO modules contain diagnostic routines called "Output Voter Diagnostics" (OVD) designed to detect failures in the four switches managing the field load terminal state. The routine consists of three basic steps.

In Step One, the "Commanded State" of each leg is compared to the "Actual State" of the field load terminal, to identify problems such as blown fuses and/or bad loopback detectors. The next two steps will not occur unless the module passes the first test.

In Step Two, the "Commanded State" of one of the three legs feeding the Output Switch Drive Circuitry is momentarily reversed, resulting in an indication of a switch failure. For this test, no output change will occur unless a switch has failed. If the leg was toggled from the "On" state to the "Off" state, a state change or "glitch" at the load is an indication of a switch stuck in the "Off" state. If the leg was toggled from the "Off" state to the "On" state, a glitch at the load is an indication of a switch stuck in the "On" state. The test is continuously rotated among the three legs.

In Step Three, the "Commanded States" of two of the three legs feeding the Output Switch Drive Circuitry are simultaneously toggled. A glitch at the field load is an indication of healthy circuitry. No glitch at the output is an indication of internal switch failure. The glitch at the field load during diagnostic routine execution is guaranteed to be less than 2.0 milliseconds and is transparent to most electromechanical field devices. If the "Commanded States" of the two legs are toggled from the "On" state to the "Off" state, the absence of a glitch at the load is an indication of a switch stuck in the "On" state.

If the "Commanded States" of the two legs are toggled from the "Off" state to the "On" state, the absence of a glitch at the load is an indication of a switch stuck in the "Off" state. The test is continually rotated for the three possible leg combinations.

Failure of any test within the three steps will result in the illumination of the fault LED on the output module. The modules additionally compare output table data across the three legs, with any discrepancies reported back to respective Main Processor Modules. The Main Processor Module fault analyzer routine diagnoses failed legs on output modules at the end of each scan, with a faulty output module annunciated by the system. The modules are specifically designed for applications that hold points in one state for long periods of time. The routine guarantees full fault coverage even if the commanded state at the field terminals never change.

The Model 3601TN DO modules execute Steps 1 and 2 of the OVD routine. The modules do not attempt Step 3 due to the use of triacs instead of transistors for the series-parallel switch configuration driving the load. The triacs would cause a glitch duration of approximately 8.33 milliseconds for a 60 Hz load, which would not be transparent to most electromechanical field devices. A faulty switch will cause the output to transition to the opposite state for a maximum of one half an AC cycle during Step Two of the OVD routine. However, the module cannot self-diagnose "Stuck On" switches if the "Commanded State" of a leg is "On," or "Stuck Off" switches if the "Commanded State" of a leg is "Off". Therefore, it is recommended that the field points should be toggled from the normal state to the opposite state and leg output tested accordingly once every 24 months to guarantee the health of the circuitry.

The DO module diagnostics are specified to operate as follows:

Module	Minimum Output Toggle Rate	Maximum Output Toggle Rate
Model 3601TN	Every 24 months	Every 100 msec plus one scan

4.2.2.2 Relay Output Module

This discussion is applicable to the following relay output (RO) module:

- Model 3636T Relay Output, Non-triplicated, Normally Open, 32 points

This module may be used in both nuclear safety-related and non-safety related systems and is qualified as a Class 1E to non-1E isolation device; configured in the PPS Replacement as a non-safety related module.

The RO modules have three legs that receive signals from respective Main Processor Modules. The three leg signal sets are voted and the voted signals are used to drive the 32 individual output relays. Each output contains loopback circuits that verify the operation of each relay independent of the load. Ongoing diagnostics test the operational status of the module. Failure of any diagnostic activates a Fault indicator on the module, which in turn activates the chassis alarm.

4.2.2.3 Analog Output Module

This discussion is applicable to the following Analog Output (AO) module:

- Model 3805HN 4-20ma Current Loop, DC Coupled (8 points)
- Model 3805E 4-20ma Current Loop, DC Coupled (8 points)

AO modules contain three separate and isolated legs, with each leg equipped with a D/A converter. One of the legs is selected to drive the analog output, and the output is continuously checked for correctness by loopback inputs on each point which are read by all three microprocessors. Each module in the system receives three tables of output values from the Main Processor Modules. All three legs drive current to leg-specific switches. Two of the switches are normally positioned to shunt the leg's output current to ground. Only one output leg switch will be set to drive current to the load.

Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module Fault Indicator, which in turn activates the chassis alarm signal. The module is designed to operate correctly in the presence of a single fault and may continue to operate properly with some multiple faults.

The health of each leg is verified by monitoring output current via a voltage loopback circuit. Each leg monitors the health of neighboring legs, by comparing output current signal values, and ensuring the leg driving the load is supplying the correct signal value. Each AO voltage loopback is automatically calibrated using multiple reference voltages read through the multiplexer, which determine the gain and bias required to adjust the readings of the A/D converter. Several drift over time components can affect the automatically calibrated level and cannot themselves be calibrated out (Reference: 3.3.9). Two out of three legs must vote a leg healthy before it is allowed to drive the load. The leg driving the load is rotated every 10 seconds between the healthy legs in a predetermined direction. Each leg tracks which leg is

currently driving the load and which leg is next in the rotation, to allow each leg to vote on the health of the next leg up in the rotation. A leg must diagnose itself as healthy or it will be skipped in the rotation, and will also be unable to vote on the health of neighboring legs.

If a faulted leg is not currently selected to drive the load when the process outputs are updated, then any single leg failure or corrupted signal from a Main Processor Module will be compensated for or filtered out by the Voter Logic at the output module level.

If a faulted leg is currently driving the load, then the output modules receive updated process outputs as soon as the faulted signal reaches the field load. However, at the same time the AO module will go through the process of voting on the health of the faulted leg. The module will diagnose the faulty signal and select a healthy leg to drive the load. The AO module is guaranteed to correct the faulted output signal within 20 ms, which is transparent to most electromechanical devices due to the capacitance of the system.

4.2.3 Main Processor Module

4.2.3.1 3008N MP

This discussion is applicable to the following Main Processor Module:

- Model 3008N Enhanced Tricon Main Processor

A Tricon system utilizes three Main Processor Modules to control three separate legs of the system. Each Main Processor Module operates independently with no shared clocks, power regulators, or circuitry. In Model 3008N, each module owns and controls one of the three signal processing legs in the system, and each contains two 32-bit processors. One of the 32-bit processors is (1) a dedicated, leg-specific I/O communication (IOC) microprocessor that processes all I/O with the system I/O modules, and (2) a dedicated, leg-specific processor manages interfaces with all Communication Modules in the system.

For Model 3008N, the 32-bit primary processor manages execution of the control program and all system diagnostics at the Main Processor Module level. Between both 32-bit processors is a dedicated dual port RAM allowing for direct memory access data exchanges.

The IOC processors constantly poll respective legs for all the input and output modules in the system. They continually update an input data table in shared memory on the Main Processor module with data downloaded from the leg-specific input data tables from each input module. Communication of data between the Main Processor Modules and the input and output modules is accomplished over the triplicated I/O data bus using a master-slave communication protocol. The system uses cyclic redundancy code (CRC) to ensure the health of data transmitted between modules. Should a Main Processor Module lose communication with its respective leg on any of the input modules in the system or the CRC reveals that the data has been corrupted, the system will retry the data transmission up to three times. If unsuccessful, input tables at the Main Processor Module level will be constructed with data in the de-energized state. Errors such as an open circuited data bus, short circuited data bus, or data corrupted while in transit will force the input table entries to the de-energized state.

At the beginning of each scan, each primary processor takes a snapshot of the input data table in shared memory, and transmits the snap shots to the other Main Processor Modules over the TRIBUS. Each Module independently forms a voted input table based on respective input data points across the three

snapshot data tables. If a Main Processor Module receives corrupted data or loses communication with a neighbor, the local table representing that respective leg data will default to the de-energized state.

For digital inputs, the voted input table is formed by a 2 out of 3 majority vote on respective inputs across the three data tables. The Voting scheme is designed for de- energize to trip applications, always defaulting to the de-energized state unless voted otherwise. Any single leg failure or corrupted signal feeding a Main Processor Module will be corrected or compensated for at the Main Processor Module level when the voted data table is formed.

A mid-value selection algorithm chooses an analog input signal representation in the voted input table. The algorithm selects the median of the three signal values representing a particular input point for representation in the voted input tables. Any single leg failure or corrupted signal feeding a Main Processor Module will be compensated for at the Main Processor Module level when the voted data table is formed. If an analog input value on one leg has a significant deviation from the other leg inputs, the point will be alarmed and the Main Processors will use the average value of the two analog inputs on the other two legs.

The primary processors on the Main Processor Modules execute the application program in parallel on the voted input table data and produce an output table of values in shared memory. The voting schemes explained above for analog and digital data ensure the process control programs are executed on the same or equal input data value representations. The IOC processors generate smaller output tables, each corresponding to an individual output module in the system. Each small table is transmitted to the appropriate leg to the corresponding output module over the I/O data bus.

The transmission of data between the Main Processor Modules and the output modules is performed over the I/O data bus using a master-slave communication protocol. The system uses cyclic redundancy code (CRC) to ensure the health of data transmitted between modules. If the CRC reveals that the data has been corrupted, the system will retry the data transmission up to three times. If unsuccessful, that respective leg data table at the output module level will default to the de-energized state. Watchdog timers on each output module leg ensure communication has been maintained with its respective Main Processor Module with a certain timeout period. If communication has not been established or has been lost, the respective leg data table will default to the de-energized state to protect against open or short-circuited data bus connection between modules.

Diagnostics at the Main Processor Module level validate the health of its circuitry as well as make decisions about the health of each I/O module and communication module in the system. The modules compare memory, basic processor instructions and operating modes, verify communication between shared memory and the IOC processor, verify communication between the IOC and the I/O modules, and verify the TriClock/TriTime and TRIBUS interfaces.

At the beginning of each scan, the Main Processor Modules transmit/receive copies of the previous scan Output Tables to/from neighbors over the TRIBUS. At the end of the scan, the modules vote on the previous scan output data to diagnose any faults. Extensive diagnostics validate the health of each Main Processor as well as each I/O module and communication channel. Transient faults are recorded and masked by the hardware majority-voting circuit. Persistent faults are diagnosed, and the faulted module can be replaced or operated in a fault-tolerant manner until replacement. The Main Processor Modules also process diagnostic data recorded locally and data received from the input module level diagnostics in

order to make decisions about the health of the input modules in the system. All discrepancies are flagged and used by the built in fault analyzer routine to diagnose latent faults.

The Main Processor diagnostics perform the following:

- Verification of fixed-program memory
- Verification of the static portion of RAM
- Testing of all basic floating-point processor instructions
- Verification of the shared memory interface with each I/O communication processor and communication channel
- Verification of handshake signals and interrupt signals between the CPU, each I/O communication processor and communication channel
- Checking of each I/O communication processor and communication channel microprocessor, ROM, shared memory access and loopback of RS-485 transceivers
- Verification of the TriClock/TriTime interface
- Verification of the TRIBUS interface

4.2.4 Communications Module

4.2.4.1 TCM Module

This discussion is applicable to the following Communications Module:

- Model 4352AN Tricon Communication Module (TCM), Fiber

TCM Model 4352A is compatible with only Tricon V10.1 systems and later. Each TCM contains two fiber-optic network ports (MTRJ connectors with 62.5/125 um fiber cables) – NET 1 and NET 2. It has a communication speed of 100 Mbps. Serial ports have speeds of up to 115.2 Kbps per port, aggregate data rate of 460.8 Kbps for all four ports. A single Tricon system supports a maximum of four TCMs, which must reside in two logical slots. Each Tricon system supports a total of sixteen Modbus masters or slaves – this total includes network and serial ports. The hot-spare feature is not available for the TCM, though you can replace a faulty TCM while the controller is online.

The TCM communicates with all three Main Processors over three separate communication busses, one to each Main Processor. The TCM module has a dedicated communication port for each communication buss. Hence the TCM will continue to communicate with the Main Processors upon the failure of a Main Processor or a communication port.

Two TCMs are placed in one logical slot of the Tricon controller chassis, but they function independently, not as hot-spare modules. A faulty TCM module can be replaced while the controller is online. In TMR mode, the presence of any fault on a MP will not affect the operation of the TCM, except the normal TMR to Dual mode transition (i.e. correctly receive and process the data from the remaining good MPs. In Dual mode, the presence of any fault on a MP should not affect the operation on the TCM, except the normal Dual to Single mode transition. If data integrity cannot be assured, the TCM should enter the fail-safe state for all communication ports. The fail-safe state is defined as follows: Disable all process communications except debug information. In Single mode, the presence of any single critical fault on a MP will cause the system to enter a fail-safe state. In Zero mode, the TCM terminates all except diagnostic / debug communications.

4.2.5 RXM Modules

This discussion is applicable to the following Remote Extender Modules:

- Model 4200N Primary RXM, Multi-mode Fiber Optics (set of 3 modules)
- Model 4201 Remote RXM, Multi-mode Fiber Optics (set of 3 modules)

The RXM Multi-mode Fiber Optics modules allow I/O modules to be located several kilometers away from the Main Chassis. The RXM consists of three identical modules, serving as repeaters / extenders of the Tricon I/O bus, that also provide ground loop isolation. Each RXM module has single channel transmit and receive cabling ports. A Primary RXM module set is connected to the Remote RXM module set housed in a remote chassis. The RXM sets are available for fiber optic cables with a communication rate of 375 Kbits/s. These sets provide maximum immunity against electrostatic and electromagnetic interference, and support configurations with optical modems and fiber optic point-to-point cabling. The interfacing cabling is unidirectional for each channel. One cable carries data transmitted from the Primary RXM to the Remote RXM. The second cable carries data received by the Primary RXM from the Remote RXM.

4.2.6 Tricon Chassis Assemblies

Diablo Canyon Power Plant's PPS system consists of one Main Chassis and two additional chassis per protection set. The Tricon Main Chassis can support the following modules:

- Two Power Modules
- Three Main Processors
- Communications Modules (TCM)
- I/O Modules

The Tricon RXM Chassis can support the following modules:

- Two Power Modules
- Three RXM modules
- I/O Modules

A Tricon controller contains three Main Processor modules. Each Main Processor controls a separate channel of the system and operates in parallel with the other Main Processors. A dedicated I/O processor on each Main Processor manages the data exchanged between the Main Processor and the I/O modules. A triplicated I/O bus, located on the chassis backplane, extends from chassis to chassis by means of I/O bus cables.

This triplicated I/O bus system is etched on the chassis backplane. It transfers data between the I/O modules and the Main Processors at 375 Kbits/s. 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.

A master-slave protocol is used for communication on the I/O bus. The IOC microprocessor is the master and controls the I/O messages on the bus. I/O modules only transmit messages upon request from the IOC microprocessor. All messages contain a 16-bit CRC to ensure the messages have not been corrupted. All legs on the I/O modules periodically check their transmitter to make sure their transmitter is not in a "Stuck On" state. If the transmitter is in the "Stuck On" state, the module fault LED is turned on and the fault condition is sent to the Main Processor.

4.2.6.1 Key Switch

A key switch on the main chassis selects the Tricon mode. Each key "position" forces a "mode" within the Tricon that defines operational configurations, limitations, and overrides.

The key switch is implemented by a three-gang, four-position switch. Each of the gangs is connected to one of the Main Processors, as depicted in the following figure:

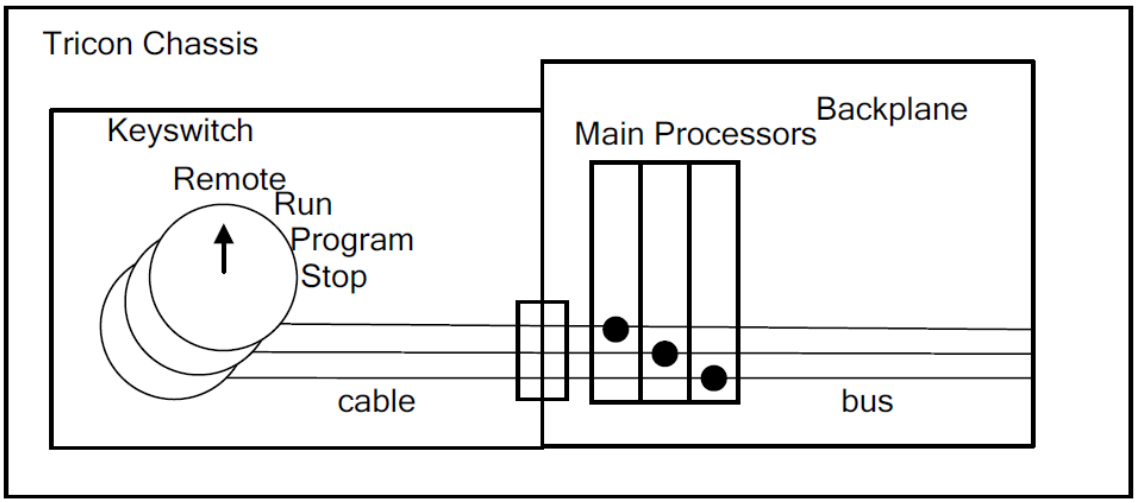


Figure 3. Key Switch - TMR Gang Connections

4.2.6.1.1 Key Switch Operation

The values are read by each of the Main Processors as a two bit value:

Position	Value
Stop	0
Program	1
Run	2
Remote	3

The key switch position is voted between the three Main Processors and the voted value is used to perform key switch functions. The application has access to the voted key switch position and can perform a specified action depending on the key switch's position. The PPS Replacement application turns on an annunciator when the key switch position is not in RUN.

The key switch design mitigates any single hardware fault. If one of the gangs on the switch goes bad or the inputs on the Main Processor, it only affects the Main Processor that is attached to that gang. The other two Main Processors will continue to receive good input values and out vote the Main Processor

with the bad input. This protects against any single fault in the physical key switch or on the Main Processor.

The Main Processor is responsible for handling requests from external clients through the TCM. The handler inside the Main Processor validates that the key switch is in the correct position before executing a request from the client.

Table 4 shows the required key switch setting for the different categories of commands:

Table 4. Required Key Switch Settings for Command Categories

Command Category	Required Key Switch Setting
Application Changes	Program
Writes of Point Values	Remote or Program
Reads of Point Values	Any
Disabling of Points	Program
Read of Maintenance Information	Any
Control OVD on a Module	Program
Clear Faults	Any
Set and Adjust Clock Calendar	Any

The Main Processor checks whether the key switch is in the correct position before processing any request, as depicted in the following figure:

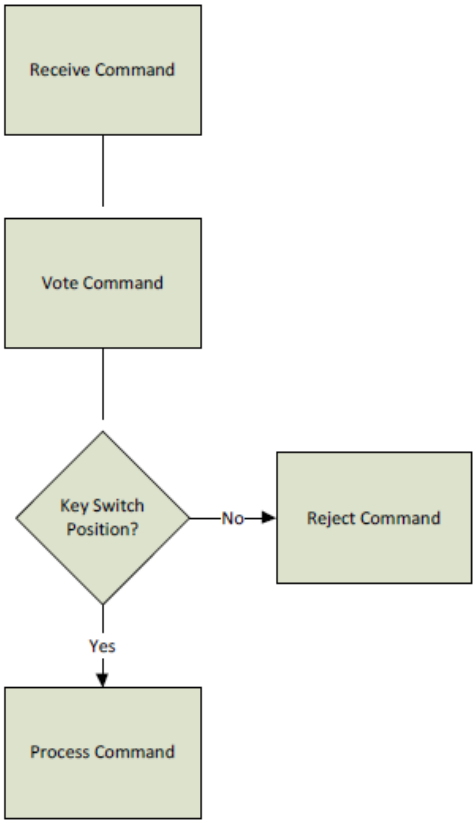


Figure 4. Key Switch - Logic Flow

The implementation in the Main Processor firmware prevents any request from being executed when the key switch is not in the correct position. Below is an example of the code for halting the execution of the application:

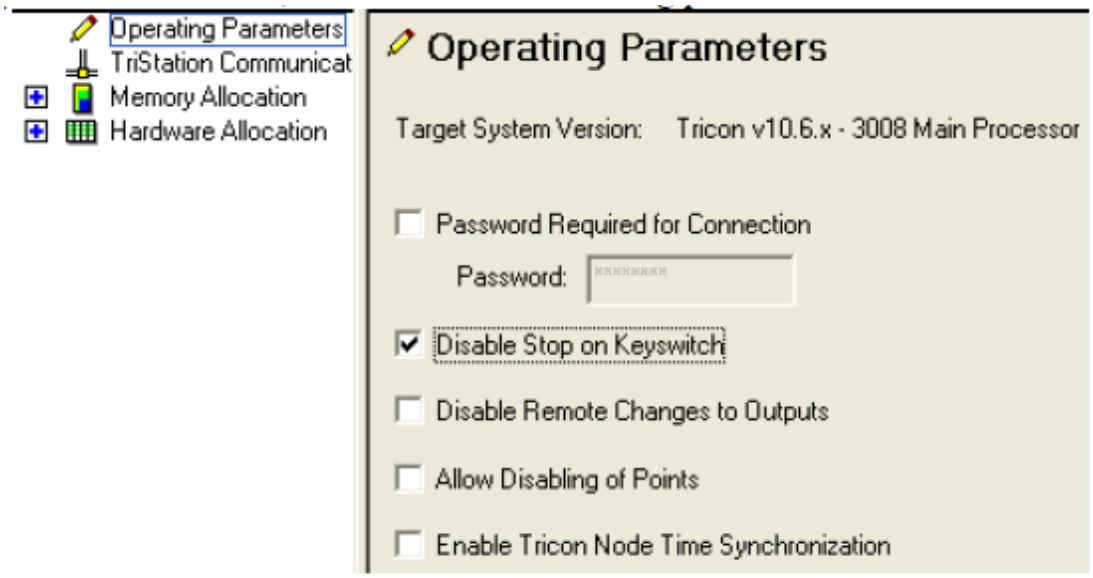
```
GLOBAL void
haltProgram (int connNum)
{
	/*
	* Make sure the key switch is in a position that allows this command.
	*/
	if (!KEY_PROGRAM) {
		reject (WRONG_KEY_SETTING, connNum);
		return;
	}
	my_diagbuf.rll_status.cpRunState = CP_HALTED;	/* Note that we are halted. */
	respond (PROGRAM_HALTED, connNum);		/* Respond to the TRISTATION */
	return;
}
```

Every request has an appropriate check for the key switch position at the beginning of the function.

The TSAP reads the position of the key switch every scan. If the key switch is not in the RUN position, the TSAP annunciates an alarm.

The STOP position of the key switch stops reading inputs, forces non-retentive digital and analog outputs to 0, and halts the control program. Retentive outputs remain at the value they had before the key switch was turned to STOP.

TriStation may be used to prevent the application from halting when the key switch is turned to STOP. A property named "Disable Stop on Key switch" determines whether the STOP position is disabled, as shown by a portion of a TriStation screen shot in the following figure:



TriStation > Controller tree > Configuration > Operating Parameters

Figure 5. Key Switch - Disabling STOP from TriStation

If the property is checked, setting the key switch to STOP does not halt the application. If cleared, then setting the key switch to STOP does halt the application. For the PPS Replacement application, the property is checked so that the key switch to STOP will not halt the application.

4.2.6.1.2 Software Affected by the Key Switch

The key switch affects the firmware and application program running in the safety controller, commands from TriStation software, and access by client software on the network:

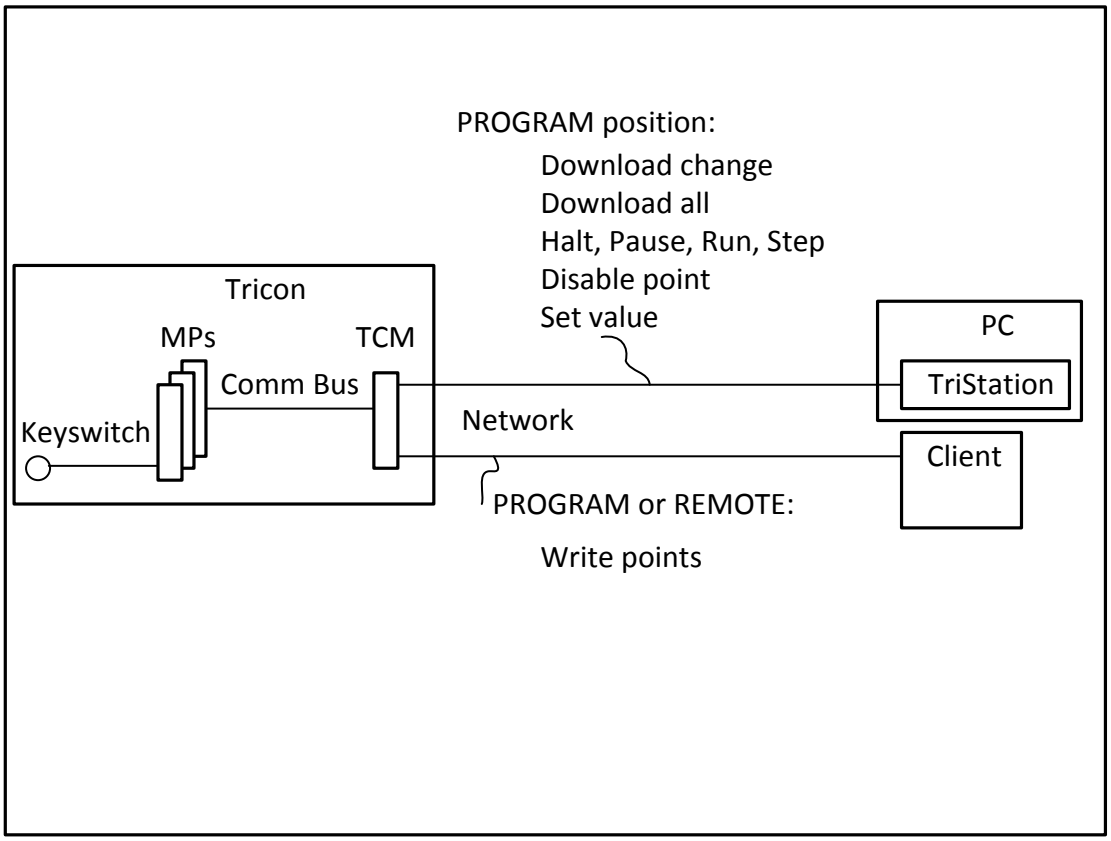


Figure 6. Key Switch - Positions to Allow Client Access

The key switch must be in the PROGRAM position to accept commands from TriStation that can modify the application running in the controller. The key switch must be in PROGRAM position or REMOTE position to allow writing of points by a network client.

The software running on each Tricon Main Processor includes the system executive firmware and the application program, as shown in the following figure:

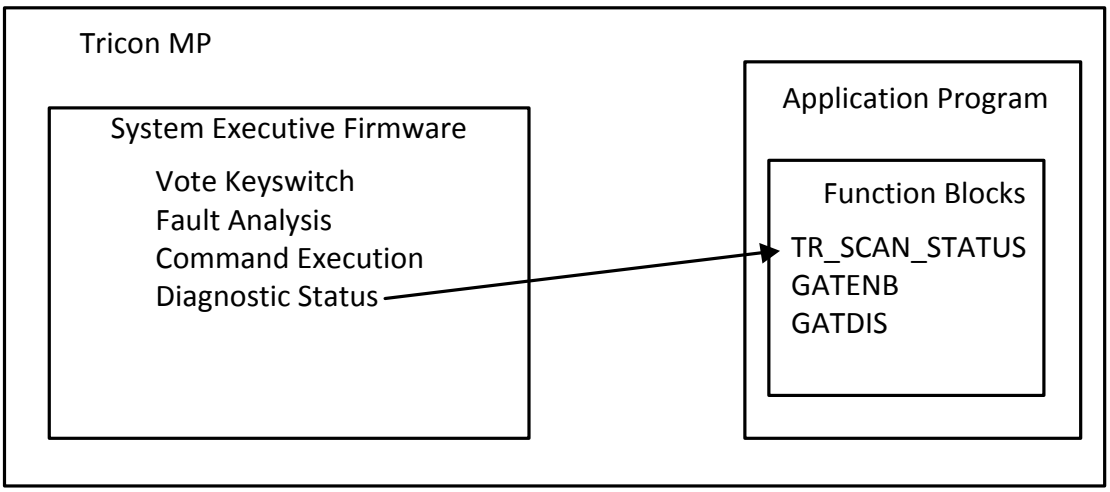


Figure 7. Key Switch - Firmware in the Tricon MP

The firmware includes key switch voting, fault analysis, command execution, and a diagnostic status structure. The application can call function blocks affected by the key switch.

- **Vote Key Switch:** Key switch voting starts when the key switch values have stopped changing for three seconds. If all voting legs agree on one value, then the voted value is the agreed value. For a single failure, if one leg disagrees, that leg is reset, failed, and taken out of the voting. For multiple failures, if all voting legs mismatch, then an error message is logged without reset, and the voted value is 0 (STOP). When the voted value changes to STOP, if key stop is enabled, then halt, else just log the change.
- **Fault Analysis:** Resets the Main Processor for a single failure, logs key switch errors, and logs changes in key switch position.
- **Command Execution:** The firmware executes commands depending on the voted position of the key switch, as explained in the previous clause "Key switch Operation."
- **Diagnostic Status:** Diagnostic status is a structure with a key switch member that holds the voted key switch position. The key switch member is a system variable that can be read by a network client or by a TR_SCAN_STATUS function block in the application program.

An application can call any of the following three function blocks: TR_SCAN_STATUS, GATENB, and GATDIS, which provide the following functions:

- **TR_SCAN_STATUS:** The KEYSWITCH output provides the key switch position.
- **GATENB:** Can be used to temporarily allow writes to specified points even when the key switch is in the RUN position.
- **GATDIS:** Can be used to temporarily allow writes to specified points even when the key switch is in the RUN position.

For the PPS Replacement application, the GATENB and GATDIS functions are utilized to allow setpoint and tunable parameter changes from the MWS.

4.2.6.1.3 Key Switch Tests

The PPS Replacement application will be able to test the enable and disable of commands by the key switch.

The application includes the following tests:

- Stopping and starting the application – turning active LEDs on and off
- Ability to disable points.
- Disable of the STOP position of the key switch.
- RUN mode inhibits the ability to:
    - Disable variables
    - Change variable values
    - Download change
    - Halt
    - Download All
    - Change clock/calendar
    - Other commands in the command menu
- REMOTE mode inhibits similar to RUN mode
- Operation of the GATENB and GATDIS function blocks.
- Test the KEYSWITCH output of the TR_SCAN_STATUS function block.

4.2.7 Power Supply Modules

This discussion is applicable to the following Power Supply Modules:

- Model 8310N2 120 Vac/Vdc – 175-Watt Power Module
- Model 8310 120 Vac/Vdc – 175-Watt Power Module

The Power Supply modules possess built in diagnostic circuitry to check for out-of-range voltages and/or over temperature conditions. Indicator LEDs on the front face of each power module provide module status as follows:

Indicator	Color	Description
PASS	Green	Input Power is OK
FAULT	Red	Power Module is not OK
ALARM	Red	Chassis Alarm Condition
TEMP	Yellow	Over-temperature Condition
BATT LOW	Yellow	Battery Low Condition

The chassis backplane provides terminal strip interfaces for power and alarm connections. The alarm feature operates independently for each power module. The alarm contacts on both main chassis power modules are actuated on the following states:

- System configuration does not match the control-program configuration
- A digital output module experiences a Load / Fuse error
- A module is missing somewhere in the system
- A Main Processor or I/O module in the main chassis fails
- An I/O module in an expansion chassis fails
- A Main Processor detects a system fault
- The inter-chassis I/O bus cables are incorrectly installed (i.e. cross connected)

The alarm contact on at least one Main Chassis power module is actuated when the following power conditions exist:

- A power module fails
- Primary power to a power module is lost
- A power module has a low battery or over temperature condition

The alarm contacts on at least one power module of an expansion chassis actuates when the following conditions exist:

- A power module fails
- Primary power to a power module is lost
- A power module has a over temperature condition

The alarm contacts on both power modules of an expansion chassis actuate when an I/O module fails.

Each Tricon chassis houses two Power Modules containing independent power supplies arranged in a dual redundant configuration.

Dual independent power rails are etched on the back plane of each chassis in a Tricon system. Both power rails feed each of the three legs on each I/O module and each Main Processor Module residing within the

chassis through dual independent voltage regulators. Each power rail is fed from one of the two Power Supply Modules residing in the chassis. Under normal circumstances, each of the three legs on each I/O module and each Main Processor Module draw power from both power supplies through the dual power rails and the dual power regulators. If one of the power supplies or its supporting power line fails, the other power supply will increase its power output to support the requirements of all modules in the chassis. A short on a voltage rail disables the power regulators for that leg rather than affecting the power bus.

Each Power Supply Module is capable of supporting all the power requirements for all the modules in the chassis within which it resides. All models of power modules are protected against reverse connection of the DC inputs.

The Tricon also has dual redundant batteries located on the Main Chassis backplane. If a total power failure occurs, these lithium batteries can maintain data and programs on the Main Processor modules for a cumulative period of six months. When less than 30 days of battery life remains the system will generate an alarm.

4.2.8 Tricon Termination Panels

The termination panels are printed circuit boards utilized to facilitate landing of field wiring. This panel contains terminal blocks, resistors, fuses and blown fuse indicators. The standard panels are configured for specific applications (e.g., digital input, analog input).

Each termination panel is packaged with a matched interface cable that connects between the termination panel and the Tricon backplane.

5 Detailed Analysis

5.1 Tricon Hardware Analysis

The FMEA tabulation is provided in Appendix A through Appendix E. As shown, failure modes that can prevent the Tricon system from performing its function are detected by proper application-specific design, the built-in on-line system diagnostics, or by periodic off-line testing.

The general effect of failures in C1a and C1b category are single failures detected by the Tricon on-line diagnostics that do not affect PLC operability and I/O capability, as detailed in the Appendices. PPS Replacement application-specific design features monitor the Tricon diagnostic alarms and annunciate these types of failures in a timely manner.

Category C2 includes single and multiple failures, not detected by PLC diagnostics, which do not affect PLC operability. It can be classified as follows:

a) Failures that would be detected by periodic off-line testing in accordance with the manufacturer's standard recommendations;
b) Failures associated with PLC functions not used for safety-related functions; and
c) Failures that can be detected by application-specific design considerations (e.g., monitoring for loss of external communications links, loss of loop power supplies, failures in termination cables and termination panels). The PPS Replacement employs application-specific design features to detect the loss of external communications links, loss of loop power supplies, and indications of failures in termination cables and termination panels.

Category C3a includes single failure conditions where the PLC is unable to perform all of its safety functions. These failures are generally related to loss of a single I/O point or the I/O points on a single termination panel. Loss of a non-redundant loop power supply, I/O point fuse failures, termination panel, or termination cable failures are also Category C3a failures. The majority of these failures would be detected by the PLC on-line diagnostics, as described in Section 4.0. Four items, identified with the combination of failure categories C2 and C3a, are not detected by the PLC. These types of failures can be detected by either by periodic channel checks and surveillance testing, or by application-specific design features. In the PPS Replacement, these four failures (identified in Appendix A) are summarized as follows:

Failure Type	Failure Mode	Effect on PLC I/O	Detection Methodology
Chassis to Term Panel Cable For 3501TN2, 3503EN2 (See Appendix A, PLC Cable-Related Failures #6)	Open circuit or short circuit to ground	Affected digital inputs will fail LOW	Detected by Critical_IO function block in TSAP; generates an alarm.
Chassis to Term Panel Cable For 3501TN2, 3503EN2 (See Appendix A, PLC Cable-Related Failures #7)	Short circuit across DI point	Affected digital inputs will fail HIGH	Detected by Critical_IO function block in TSAP; generates an alarm.

Failure Type	Failure Mode	Effect on PLC I/O	Detection Methodology
Chassis to Term Panel Cable Model 3601TN; 115 Vac (See Appendix A, PLC Cable-Related Failures #9)	Open circuit	PLC digital inputs will not be affected, but field devices will fail LOW	Detected by Critical_IO function block in TSAP; generates an alarm.
Term Panel For 3501TN2, 3503EN2 (See Appendix A, PLC Termination Panel-Related Failures #2)	Short circuit across DI point	Affected digital inputs will fail HIGH	Detected by Critical_IO function block in TSAP; generates an alarm.

The next failure category defined in Section 1.5 is Category C3b, which includes multiple failure conditions where the PLC is unable to perform all of its safety functions. These failures include the effects of fire, flooding and missiles, which are minimized by applying standard industry design practices in the PPS Replacement application and are considered low-probability events. The remaining failures are either common cause hardware failures or common cause software errors. These types of multiple failure scenarios are typically considered to be a small percentage of the total failures. Common cause failures are minimized in the PPS Replacement through an architecture of 4 Protection Sets, where each Protection Set is electrically and physically separate from the others, unable to communicate with any other Protection Set, and provides overlapping safety coverage.

Finally, failure categories defined in Section 1.5 are Category C4a and C4b, which include single or multiple failure conditions where the PLC self-diagnostic capability is reduced, but the PLC remains operable. These failures all fall in the category of single or double failures of triple redundant components, such as Main Processor modules, I/O modules, I/O Bus links, TRIBUS links, or RXM modules. Most failures that reduce the on-line diagnostic capabilities are detected and hence are repaired quickly using the on-line repair capability of the Tricon system. The items that cannot be repaired on-line (i.e., chassis, I/O bus, TRIBUS links) have very low failure rates that can typically be ignored.

The Tricon system design information presented in References 3.3.7 and 3.3.8 includes recommendations for periodic off-line testing of field inputs and outputs. These recommendations establish general surveillance techniques and surveillance intervals intended to maintain the high reliability of the overall control system. It is strongly recommended that nuclear plant safety-related applications incorporate the specified methods and frequencies of Reference 3.3.7, 3.3.8 and 3.3.9 to maximize system reliability and operability. To ensure that the high reliability of the overall control system is maintained, Invensys recommends that off-line periodic proof testing of field inputs and outputs be performed at least every 30 months of continuous operation (24 month refueling cycle plus a 25% extension as allowed in the technical specifications).

5.2 Key Switch Analysis

As described in Section 4.2.6.1 of this document, there are several layers of protection to prevent inadvertent application program changes. These include the Tricon key switch, as well as communication protocol end-to-end integrity checks in the application program. Additional protection is provided by features in the TriStation 1131 programming interface, including password access.

The Tricon key switch 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 key switch is implemented by a three-gang, four-position switch. Each of the gangs is connected to one of the 3008N MPs.

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

The key switch design mitigates 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 data and out vote the 3008N MP with the bad input. This protects against any single fault in the physical key switch or on the 3008N MP from disabling the entire Tricon.

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 key switch rotated to the PROGRAM position. Using the programming terminal, the programmer opens communications with the Tricon and downloads the program. Once downloaded the Tricon automatically changes the program version number.

5.3 Buyout Analysis

Appendix E, the FMEA for PPS buyout components, shows that the failure modes of the buyout components have little or no effect on the Tricon operability. At worst, the Tricon might indicate the loss of one of two redundant power supplies, problems with unused points, or other cascading common cause faults like loss of a power strip, breaker, or fuse.

5.4 TSAP Timing Analysis

P

5.4.2 Failures Not Affecting Response Time

1. ***Out of Service (OOS) Switch Failure:***
   The OOS switches are a request toggle. OOS requires additional operator confirmation, so failure of any OOS switch initiates no additional TSAP logic.
2. ***Bypass Switch Failure:***
   The Bypass switch overrides the Tricon output and works with the Tricon de-energized. Bypass requires additional operator confirmation, so failure of any Bypass switch initiates no additional TSAP logic.
3. ***Hardware Failures:***
   The evaluation of the PPS Replacement system has determined that potentially degraded hardware conditions affecting response time will not impact TSAP response time, or will be detected by internal Tricon platform performance calibrations and functional checks, as well as surveillance testing within the TSAP logic.

5.5 Signal Loading

Appendix D contains the tabulated safety critical inputs for each protection system. Analysis was performed to determine whether the inputs have been appropriately assigned to ensure that a single failure of an input module or Protection Set would not render a safety-related function of a particular parameter inoperable. Appendix D provides application specific analysis of the PPS Replacement, as opposed to the generic hardware/software analysis presented in the other attachments.

Analysis in Appendix D shows that the input signal loading assignment provides diversity and defense-in-depth for the PPS safety function inputs. This is accomplished by ensuring that each process variable parameter is covered by at least two independent Protection Sets, and that each Protection Set has its own set of independent inputs.

Two signals (TE-454 and PT-505) have coverage by only a single Protection Set. By design, these two signals do not have a redundancy requirement, but are included in the analysis for completeness.

5.6 Non-detectable Faults

5.6.1 Drift

The Tricon will maintain its rated reference accuracy specifications over extended periods. As stated in the Tricon FMEA (Reference 3.3.4), failure of components affecting the rated reference accuracy are detected, the system will generate an alarm, and the faulted module will be indicated. Response to the alarm would require replacement of the faulted module, because field adjustments or calibrations of the Tricon are not possible. The Tricon TMR architecture allows continuous cross comparisons between the triplicated values. The effects of calibrated accuracy including drift over time, hysteresis and non-linearity, and repeatability are applicable to the Tricon system and I/O modules, and their error contributions are specified in the Tricon I/O Accuracy document (Reference 3.3.9). The effects of temperature sensitivity, power supply variations, arithmetic operations errors, vibration, radiation, and relative humidity are not applicable to the Tricon system and I/O modules, thus their error contribution is zero.

5.6.1.1 Accuracy Drift in Analog Modules

The Tricon analog I/O modules have an auto-calibration feature which maintains the module accuracy rating. Over time the accuracy of the reference used to perform the auto-calibration can experience accuracy drift.

P

To ensure that specified accuracy is maintained Invensys recommends that the analog I/O modules be periodically proof tested at least every 30 months of continuous operation.

Calculations, using vendor supplied data for the electronic components, demonstrate that time related "drift" of the subject analog modules will meet the Invensys specified accuracy, with a 95% confidence and 95% probability, over the first 30 month interval (24 month refueling cycle plus a 25% extension as allowed in the technical specifications). Additional assurance is provided by testing performed by Invensys, prior to shipment, to ensure that each module meets the specifications. Therefore it is concluded that drift over time does not present a failure to comply with the published specifications in the first 30 month interval.

Over the long term, however, since the PPS Replacement modules cannot be adjusted, an unquantifiable possibility exists that a module, at the limits of its specified accuracy during surveillance testing, may subsequently, over the next 30 months drift slightly outside of the specified accuracy. In order to ensure a conservative margin, PG&E should publish a drift specification so that this possibility may be taken into account.

5.6.1.1.1 Actions Recommended to Resolve Drift Issue

1. PG&E should include an allowance for drift in their analysis of the loop performance for the PPS Replacement safety system. Suggested allowances are presented in last column of Table 5.
2. PG&E should continue to perform periodic testing at intervals of no less than 30 months and replace modules which fail to meet the published accuracy.

5.6.1.2 Accuracy Drift in System Timing

System timing can also drift over time. However, based on the detailed analysis of parameters that might impact system timing, it is concluded that the drift over time is negligible and therefore no proof test is needed on the time base of the Main Processors (Reference 3.3.9).

5.6.2 Stuck-At

The Analog Input modules (Model 3703EN and Model 3721N) detect Stuck-High and Stuck-Low input legs. Stuck-At legs, which are most likely to occur where input values remain within miscompare limits for extended periods of time, are detected by automatic leg calibration within the Analog Input modules. Each AI module leg is automatically calibrated using multiple reference voltages read through the multiplexer by the microprocessor, which determines the gain and bias required to adjust the readings of the A/D converter. The microprocessors in each leg compare the respective input table data with the neighbor legs, with out-of-tolerance data reported to respective Main Processor modules. The Main Processor module fault analyzer routines diagnose faulty input module legs at the end of each scan. One-time and short-term differences that result from sample timing variations are distinguished from a pattern of differing data. Should a Main Processor module diagnose a faulty leg on a particular module, it will signal the input module to illuminate its Fault LED.

To ensure that specified tolerances are maintained over time, Invensys recommends that the analog I/O modules be periodically proof tested at least every 30 months of continuous operation.

5.6.3 Digital Input Points - Normally Off

The Tricon Digital Input modules contain loopback circuitry in each leg that momentarily drives the input signal for the leg under test to the “logical zero” or “low” state. This test, which is continually rotated among the three legs, verifies proper operation of leg optical isolation and/or signal processing and conditioning circuitry. Should a leg fail the test, the module fault indicator will be illuminated. However, if these modules monitor normally off points, the field point must be toggled from the “Off” state to the “On” state at periodic intervals. To ensure the proper operation of leg optical isolation and/or signal processing/conditioning circuitry, Invensys recommends that any normally off field points connected to Tricon Digital Input modules should be periodically proof tested at least every 30 months of continuous operation.

The following normally off input points in Table 6 should be proof tested at a minimum of 30-month intervals of continuous operation.

Table 6. 30-Month Normally Off Proof Test Input Point List

Protection Set	Tagname	- Switch Status: Bypass/Trip Switches - Instrument Tag and Channel Function	Normal State
1	PC505A_BYP	PC-505A_Byp Turbine Impulse Pressure High to P13 (Bypass Switch)	OFF
1	PS505C_TRIP	PS/505C PC-505C Trip Status (Turb Impulse Press PT-505)	OFF
1	TS411D_TRIP	TS/411D TC-411D Trip Status (DTTA Loop 1)	OFF
1	TS411H_TRIP	TS/411H TC-411H Trip Status (DTTA Loop 1)	OFF
2	PC506A_BYP	PC-506A_Byp Turbine Impulse Pressure High to P13 Bypass Switch	OFF

Protection Set	Tagname	- Switch Status: Bypass/Trip Switches - Instrument Tag and Channel Function	Normal State
2	TS421D_TRIP	TS/421D TC-421D Trip Status (DTTA Loop 2)	OFF
2	TS421H_TRIP	TS/421H TC-421H Trip Status (DTTA Loop 2)	OFF
3	TS431D_TRIP	TS/431D TC-431D Trip Status (DTTA Loop 3)	OFF
3	TS431H_TRIP	TS/431H TC-431H Trip Status (DTTA Loop 3)	OFF
4	TS441D_TRIP	TS/441D TC-441D Trip Status (DTTA Loop 4)	OFF
4	TS441H_TRIP	TS/441H TC-441H Trip Status (DTTA Loop 4)	OFF

While the input points associated with the Bypass and Out of Service (OOS) switches are maintenance-related, the Bypass and OOS input points are normally-off points and should also be proof tested at a minimum of 30-month intervals of continuous operation.

5.6.4 Digital Output Points - Same Commanded State

The Model 3601TN DO modules execute self diagnostics of the switches in such a way as to be transparent to most electromechanical field devices. A faulty switch will cause the output to transition to the opposite state for a maximum of one half an AC cycle during the OVD routine. However, the module cannot self-diagnose “Stuck On” switches if the “Commanded State” of a leg is “On,” or “Stuck Off” switches if the “Commanded State” of a leg is “Off”. Therefore, it is recommended that the field points be toggled from the normal state to the opposite state and leg output tested accordingly once every 30 months to guarantee the health of the circuitry.

All Digital Output field points should be proof tested at a minimum of 30-month intervals of continuous operation. The following normally off output points in Table 7 should be proof tested at a minimum of 30-month intervals of continuous operation.

Table 7. 30-Month Proof Test Output Point List

Protection Set	Point	- Bi-stable Partial Trip Outputs - Function Description	Normal State
1	TC-423A	Loop 2 Cold Leg Temp Low LTOPS	OFF
2	TC-433A	Loop 3 Cold Leg Temp Low LTOPS	OFF
3	PC-403A	Loop 4 Wide Range Pressure Low to RHR V-8702 Open Circuit	OFF
3	PC-403D	Loop 4 Wide Range Pressure High to LTOPS	OFF
4	PC-405A	Loop 4 Wide Range Pressure Low to RHR V-8701 Open Circuit	OFF
4	PC-405D	Loop 4 Wide Range Pressure High to LTOPS	OFF

6 Summary and Conclusions

6.1 Analysis Summary

As stated in Section 4.0 of this report, the Tricon utilizes a fault-tolerant triple modular redundant architecture. This system design identifies and compensates for failed system elements. The Tricon self-diagnostic features have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate the diagnostic coverage of single failures within each module.

Per Reference 3.3.2, the NRC has reviewed the FMEA qualification documentation from Invensys as part of the Tricon V10 safety evaluation. The results of the FMEA showed that, in general, failure modes that could prevent a Tricon PLC system from performing its safety-related functions are detected by the built-in system diagnostics or by periodic testing. The staff concluded that the FMEA shows that the Tricon PLC system is suitable for use in safety-related applications in nuclear power plants.

As stated in Section 4.0 of this report, the Tricon utilizes a fault-tolerant triple modular redundant architecture. This system design identifies and compensates for failed system elements, which facilitates its use in critical and safety-related process applications. The Tricon self-diagnostic features summarized in Section 4.0 of this report have been specifically designed to detect and alarm failures of sub-components within each module. Extensive testing has been performed on each module to validate that the on-line diagnostics will detect a very high percentage of the failures within each module. The diagnostic coverage for the Main Processors and the common processing circuitry on the I/O modules are in the 95 to 99% range. The diagnostic coverage of the I/O point circuitry on the I/O modules is 99%. Reference 3.3.5 shows the diagnostic coverage of the Tricon Main Processors and I/O modules.

On the Tricon, all safety-related operating software (.pt2 file) exists permanently in electronically erasable programmable read only memory and is considered as firmware. This software performs built-in self-diagnostics, manages the TMR features, and executes the application software.

As summarized in Reference 3.3.5, the Tricon PLC exceeds EPRI requirements (Reference 3.1.2) for both Safety and Overall Availability. The Reliability Analysis Report (document number 993754-1-819) provides additional analysis of the diagnostic coverage specific to the PPS Replacement application.

6.2 Discussion

The NRC reviewed the historical data available on the use of the Tricon PLC system in commercial and foreign nuclear applications and concluded the following in the Triconex Approved Topical Report 7286-545-1A, "Qualification Summary Report" (TAC No. ME2435):

> *"The Tricon, with its TMR architecture, is resilient against single failures and operating experience has shown it is highly reliable (more than 9,000 units in operation and over 500,000,000 hours without failure to perform on demand). Invensys understands there remains the very rare possibility of a software common cause failure (CCF). Since digital system CCFs are not classified as single failures, postulated digital CCFs are not assumed to be a single random failure in design basis evaluations. The two design attributes sufficient to eliminate consideration of common cause failure – diversity and testability – would not be satisfied by the proposed architecture. Therefore, a diverse actuation system (DAS) would be required." [7286-545-1A; Appendix B, page 21]*

> *"The NRC staff reviewed these CGD activities and based on the review of the associated development history, operating experience, life cycle design output documentation, and testing and review activities, the NRC staff finds the dedication evidence for the PDS of the Tricon V10 platform to be acceptable for demonstrating built-in quality. In addition, the NRC staff determined that the Invensys QA processes for software maintenance provides reasonable assurance that the quality characteristics of the PDS can be preserved. Consequently, the NRC staff concludes that the Tricon V10 hardware and software is of sufficient quality to satisfy Clause 5.3 and is suitable for use in SR applications." [7286-545-1A; page 116]*

Analysis indicates that the Tricon analog IO modules have accuracy margin issues after 30 months of continuous operation. Proof testing of the analog modules is required after no more than 30 months of continuous operation to detect common cause drift.

Analysis of the timing drift indicates that there is no proof test that needs to be done on the time base of the Main Processor.

The computational analysis performed in Reference 3.2.1 calculates a worst-case Scan Time for the PPS Replacement application code well within the Scan Time range to satisfy the 200 ms worst case response time requirement for the PPS Replacement. Because the TSAP follows TS1131 design and coding guidelines, executes within the allowable scan time, and is triply redundant within the Tricon, there are no internal (software) or external (hardware) failures that can impact the Tricon response time to any event.

6.3 Recommendations

Based on the FMEA results, there are no recommendations resulting from the analysis that would require design changes, new or modified diagnostics, or custom installation instructions.

6.4 Conclusions

The FMEA tabulation provided in Appendix A of this report has reviewed possible failures of the Tricon PLC system components, identified the mechanisms that could cause those failures and evaluated the consequences of those failures on the operation of the Tricon PLC system. Because of the TMR architecture of the Tricon PLC system, failure mechanisms that affect a single leg of the triple redundant system generally have no effect on the PPS operation and provide the capability of the operator to retrieve all Tricon indications in the Main Annunciator System (MAS). As shown, failure modes that can prevent the Tricon system from performing its safety-related functions are detected by proper design, the built-in system diagnostics, or by periodic testing. There are no failure-modes associated with safety-related functions for the PPS that are undetectable after application of all of the above methodologies.

Based on this analysis, there are no requirements for any hardware or software design changes, new or modified diagnostics, or maintenance issues with the existing Tricon PLC system for use in the PG&E PPS Replacement for the Diablo Canyon Power Plant. Since the PPS consists of four independent redundant Protection Sets, with a minimum of two independent Protection Sets monitoring all critical PPS Protection Set Channel functions, no single failure will defeat the overall function of the PPS. Furthermore, operational failure of one channel will leave the redundant PPS channel available to the operator. Therefore, this FMEA concludes that the Tricon PLC system is suitable for use in its intended application as PPS replacement.

The following appendices contain supporting information for this FMEA.

Appendix A - FMEA for PPS Tricon (Safety Related Components)
Appendix B - FMEA for PPS Tricon (Non-Safety Related Components)
Appendix C - FMEA for Safety Related Software
Appendix D - FMEA for Input Module Signal Loading
Appendix E - FMEA for PPS Buyout Components

Appendix A – FMEA; PPS Tricon (Safety Related Components)

NOTE: **Failure Category Column**

The Failure Category column in the FMEA Table shows the primary failure categories. For example nearly all single failures on the Tricon modules are in the C1a and C1b category since the diagnostic coverage is in the 95 to 99% range. The C2a and C2b categories represent the small percentage of failures that are not detected by self-diagnostics and require additional levels of protection.

Power and Termination

The FMEA assumes that all loop power supplies are redundant (two power supplies). The FMEA also includes the termination panels and termination cables. These panels and cables have many single points of failure and these failures are typically considered as a part of the connected I/O device. In many cases they are neglected since the panel and cable failure rates are very low compared to the failure rate of the connected I/O device (Reference 3.3.4).

Tricon Platform FMEA Qualification

As of the date of this document, the Tricon V10.5.3 is the most current nuclear qualified product, subsequent to two maintenance releases (V10.5.2 and V10.5.3) since V10.5.1 (the version upon which the NRC based its Tricon V10 SER for generic nuclear industry approval). The V10 Tricon Reference Design Change Analysis, Revision 0 [Reference 3.3.11] identifies and characterizes the platform changes that have occurred since V10.5.1 and evaluates the significance of the changes as they relate to documents under review for the PPS Replacement System.

Qualification of Tricon V10.5.1 was by analysis based on the Tricon V10.2.1 tests. Tricon V10.5.1 essentially represents the further evolutionary upgrades and bug fixes made to platform software since V10.2.1 was released. Qualification evaluations have determined that the routine product upgrades have not altered the critical characteristics of the product, i.e., current modules have the same (or better) functional and environmental characteristics as the Tricon V10.2.1 Test Specimen FMEA provided in the Triconex Topical Report 7286-545-1-A, revision 4 [Reference 3.3.2].

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
CONTROL AND COMMUNICATIONS MODULE-RELATED FAILURES					
1. Main Chassis Processor Module: Model 3008N; Enhanced Tricon Main Processor, 16 Mbytes DRAM	Loss of all three processor modules	Fire; flood; missiles; software common mode failure	C3b	Input signals will not be read. Analog and digital outputs fail low.	Fails to operate
2. Main Chassis Processor Module: Model 3008N; Enhanced Tricon Main Processor, 16 Mbytes DRAM	Loss of one or two processor modules	Electronics or software failure	C1a, C1b, C4a, C4b	None	Continues to operate via intact processor module(s). Main processor diagnostics will detect and flag processor fault.
3. Main Chassis Communications Module: Model 4352AN, Tricon Communication Module (TCM)	Failure of module to transmit or receive data on all three legs	Electronics or software failure	C1a, C1b	No safety related data is being transmitted. No impact on safety functions.	Continues to operate. Communications to external network devices is interrupted. Main processor diagnostics will detect and flag communications fault upon loss of communications with MWS. A faulty TCM module can be replaced while the controller is online.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
4. Main Chassis Communications Module: Model 4352AN, Tricon Communication Module (TCM)	Failure of module to communicate with one or two of the Main Processors.	Electronics or software failure	C1a, C1b	None	Third leg will still communicate with the MP.
5. RXM Chassis Primary RXM (Remote Extender Module); Model 4200N; Multi-mode Fiber Optics (set of 3 modules)	Loss of all three RXM modules	Fire; flood; missiles; software common mode failure	C3b	Input signals in affected downstream RXM chassis will not be read. Downstream analog and digital outputs fail low. No effect on safety system.	Continues to operate, with loss of I/O function in all downstream chassis assemblies. Main processor diagnostics will detect and flag RXM communications fault.
6. RXM Chassis Primary RXM (Remote Extender Module); Model 4200N; Multi-mode Fiber Optics (set of 3 modules)	Loss of one or two RXM modules	Electronics or software failure	C1a, C1b, C4a, C4b	None	Continues to operate via intact RXM module(s). Main processor diagnostics will detect and flag RXM module fault.
PLC I/O MODULE-RELATED FAILURES					
1. Digital input modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Input point(s) stuck OFF on one leg.	Electronic component or multiple components on different points.	C1a, C1b; C2a, C2b if point is normally OFF	None	Continues operation. Condition will be detected for all DI modules except Model 3501TN2 if the point is normally OFF. Model 3501TN2 does not include Stuck Off diagnostic capability. Non-detectable fault.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
2. Digital input modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Input point(s) stuck OFF on multiple legs.	Multiple electronic component failures on same point or fuse failure	C1a, C1b, C3b,and C2a, C2b if point is normally OFF	Affected digital input(s) will fail low	Continues operation. Condition will be detected for all DI modules except Model 3501TN2 if the point is normally OFF. Model 3501TN2 does not include Stuck Off diagnostic capability. Non-detectable fault.
3. Digital input modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Input point(s) stuck ON for one leg	Electronic component failure or multiple component failures on different points.	C1a, C1b for 3503EN2; C2a, C2b only for 3501TN2 if point is normally ON.	None	Continues operation. Condition will be detected for all DI modules except Model 3501TN2 if the point is normally ON. Model 3501TN2 does not include Stuck On diagnostic capability. Non-detectable fault.
4. Digital input modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Input point(s) stuck ON for multiple legs	Multiple electronic component failures on same point or fuse failure	C1a, C1b, C3b for 3503EN2; C2a, C2b only for 3501TN2 if point is normally ON	Affected digital input(s) will fail high.	Continues operation. Unable to correctly determine the state of the affected point(s). Condition will be detected for all DI modules except Model 3501TN2 if the point is normally ON. Model 3501TN2 does not include Stuck On diagnostic capability. Non-detectable fault.
5. Digital input modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Common processing failure on one or two legs.	Electronic component failure(s)	C1a, C1b	None	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
6. Digital input modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Common processing failure on all three legs.	Electronic component failures on all legs or comm. Software failure	C3b	Affected digital inputs will not be read.	Treats all affected input points as OFF. Main processor diagnostics will detect and flag board fault(s). Fault alarm via Main Chassis Power Module alarm circuit.
7. Digital output modules: Model 3601TN; 115 Vac	Output point fails high or low on one leg	Electronic component failure	C1a, C1b	None	Continues operation. DO module OVD diagnostics will detect the fault on all modules except for the 3601TN if the output point is not being toggled periodically.
8. Digital output modules: Model 3601TN; 115 Vac	Output point fails high or low on multiple legs	Multiple electronic component failures or fuse failure	C3b	Affected digital outputs will fail to the corresponding output state, or will go OFF if fuse fault.	Continues operation. Unable to control the affected output point(s). Condition will be detected by DO module field voltage detection circuit, which will activate the LOAD/FUSE alarm since the commanded DO state will not match the detected field voltage; or if fails to current state, will be detected during the OVD diagnostics, except on the 3601TN.
9. Digital output modules: Model 3601TN; 115 Vac	Common processing failure on one or two legs	Electronic component failure(s)	C1a, C1b	None	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
10. Digital output modules: Model 3601TN; 115 Vac	Common processing failure on all legs	Multiple electronics failures or comm. Software failure	C3b	Affected output points will go OFF.	Unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
11. Analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Input point fails high or low on single leg	Electronic component failure	C1a, C1b	None	Continues operation. Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.
12. Analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Input point fails high or low on multiple legs	Multiple electronic component failures or fuse failure	C3b	Affected analog inputs will fail to the corresponding input state, or will go downscale if fuse fault.	Unable to correctly determine the value of the affected point(s). Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.
13. Analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Common processing failure on one or two legs	Electronic component failure(s)	C1a, C1b	None	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
14. Analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Common processing failure on all legs	Multiple electronics failures or comm. software failure	C3b	Affected input points will go downscale.	Treats all affected input points as downscale. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
15. Analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Module accuracy out of specification on multiple legs.	Components of the self-calibration voltage-reference circuits for all legs drift over time.	C2b	Affected inputs could potentially be outside of the published accuracy.	Continues operation. Minimum proof test interval is once every 30 months to detect common cause drift.
16. Analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Module accuracy out of specification on a single leg.	Components of the self-calibration voltage-reference circuits for all legs drift over time.	C1a, C2a	Affected inputs could potentially be outside of the published accuracy.	Continues operation. Significant deviations are detected and alarmed.
17. Analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Input signal fails on a single leg.	Detected Stuck-At leg(s) voted out by Main Processor.	C1a	None.	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
18. Analog output module: Model 3805HN; 4-20ma	Output signal fails high or low on one or two legs.	Electronic component failure(s)	C1a, C1b	None	Continues operation. Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's Fault Indicator, which in turn activates the chassis alarm signal.
19. Analog output module: Model 3805HN; 4-20ma	Output signal fails high or low on all three legs.	Multiple electronic component failures or firmware failure	C3b	Affected analog outputs will fail to unknown value.	Unable to control the affected output points. Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's Fault Indicator, which in turn activates the chassis alarm signal. Failure of all three legs for a given output will activate the Load Indicator, and output will not be driven.
20. Analog output module: Model 3805HN; 4-20ma	Common processing failure on one or two legs.	Electronic component failure(s)	C1a, C1b	None	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
21. Analog output module: Model 3805HN; 4-20ma	Common processing failure on all three legs.	Multiple module electronics failure or comm. software failure	C3b	Affected analog outputs will fail downscale.	Unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
22. Analog output module: Model 3805HN; 4-20ma	Module accuracy out of specification on multiple legs.	Components of the self-calibration voltage-reference circuits for all legs drift over time.	C3b	Affected outputs could potentially be outside of the published accuracy.	Continues operation. Minimum proof test interval is once every 30 months to detect common cause drift.
23. Analog output module: Model 3805HN; 4-20ma	Module accuracy out of specification on a single leg.	Components of the self-calibration voltage-reference circuits for all legs drift over time.	C1a, C2a	Affected outputs could potentially be outside of the published accuracy.	Continues operation. Significant deviations are detected and alarmed.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
POWER SUPPLY-RELATED FAILURES					
1. All chassis power supplies	Loss of all input power	Loss of inverter power	C3b	Input signals will not be read. Analog and digital outputs fail low.	Fails to operate
2. All chassis power supplies:	Power supply output fails high	Electronic component or fuse failure	N/A	None	Continues operation. The three terminal linear regulators are thermally protected, and the power supplies are over voltage-limited. Failure modes initiated by overvoltage conditions are therefore inapplicable.
3. Main Chassis power supply: Model 8310N; 120Vac/Vdc	Loss of one power supply output	Electronic component or fuse failure	C1a, C1b	None	Continues operation via redundant main chassis power supply. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
4. Main Chassis power supply: Model 8310N; 120Vac/Vdc	Power supply outputs fail (both power supplies fail)	Electronic component or fuse failure	C3b	Main processors fail and all analog and digital outputs fail low	Fails to operate.
5. RXM Chassis power supply: Model 8310N; 120Vac/Vdc	Loss of one power supply output	Electronic component or fuse failure	C1a, C1b	None	Continues operation via redundant RXM chassis power supply. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
6. RXM Chassis power supply: Model 8310N; 120Vac/Vdc	Power supply outputs fail (both power supplies fail)	Electronic component or fuse failure	C3b	All outputs fail low on all modules in affected chassis.	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
7. Loop power supply for digital inputs: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Power supply output voltage fails low (both power supplies fail)	Fire; flood; missile	C3b	Affected digital inputs will fail low	Continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) DI point failures triggered alarms associated with measured parameters; or (c) by periodic channel checks or surveillance testing. DI point could also be wired as a power failure alarm to provide detection (application-specific).
8. Loop power supply for digital inputs: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24	Power supply output voltage fails low (both power supplies fail)	Electronic component or fuse failure	C1a, C1b, C2a, C2b	None	Continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) by periodic channel checks or surveillance testing. DI point could also be wired as a power failure alarm to provide detection (application-specific).
9. Loop power supply for digital inputs: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Power supply output voltage fails high	Electronic component or fuse failure; fire; flood; missile	C3a, C3b	Affected digital inputs may fail low: provided failure voltage is high enough to burn out affected DI points	Continues operation. Main processor diagnostics will detect and flag board fault for modules with SAO/SAZ fault detection on the inputs. Fault alarm via Main Chassis Power Module alarm circuit. Application specific monitoring required to detect and alarm the failure for remaining modules.
10. Loop power supply for digital outputs: Model 3601TN; 115 Vac	Power supply output voltage fails low (both DC power supplies fail)	Electronic component or fuse failure	C3b	Affected digital outputs will fail low	Continues operation. Condition will be detected by the output voter diagnostics on the affected DO module, and by the DO module's field voltage detection circuit, which will activate the LOAD/FUSE alarm since the commanded DO state will not match the detected field voltage.
11. Loop power supply for digital outputs: Model 3601TN; 115 Vac	Power supply output voltage fails low (One power supply fails)	Electronic component or fuse failure	C1a, C1b, C2a, C2b	None	Continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) by periodic channel checks or surveillance testing. DI point could also be wired as a power failure alarm to provide detection (application-specific).

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
12. Loop power supply for digital outputs: Model 3601TN; 115 Vac	Power supply output voltage fails high	Electronic component failure	C3a, C3b	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
13. Loop power supply for analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Power supply output voltage fails low (both power supplies fail)	Electronic component or fuse failure	C3b	Affected analog inputs will fail low (downscale)	Continues operation. Low range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.
14. Loop power supply for analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Power supply output voltage fails low (one power supply fails)	Electronic component or fuse failure	C1a, C1b, C2a, C2b	None	Continues operation. Low range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.
15. Loop power supply for analog input modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Power supply output voltage fails high	Electronic component failure	C3a, C3b	Affected analog inputs may fail low (downscale); assuming failure voltage is high enough to burn out affected AI points	Continues operation. Low range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.
16. Loop power supply for analog output module: Model 3805HN; 4-20ma	Power supply output voltage fails low (both power supplies fail)	Electronic component or fuse failure	C3b	Affected analog outputs will fail low (downscale)	Continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Fault Indicator, which in turn activates the chassis alarm signal.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
17. Loop power supply for analog output module: Model 3805HN; 4-20ma	Power supply output voltage fails low (one power supply fails)	Electronic component or fuse failure	C1a, C1b, C2a, C2b	None	Continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Fault Indicator, which in turn activates the chassis alarm signal.
18. Loop power supply for analog output module: Model 3805HN; 4-20ma	Power supply output voltage fails high	Electronic component failure	C3a, C3b	Affected analog outputs may fail low (downscale); assuming failure voltage is high enough to burn out affected AO points	Continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Fault Indicator, which in turn activates the chassis alarm signal.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
PLC CHASSIS-RELATED FAILURES					
1. Main Chassis System Control Key Switch	Single failure affecting one leg that disagrees with the other legs	Short, open	C1a	No effect on inputs or outputs, which are voted by the two good legs. The fail LED is turned on for the failed leg.	PLC continues to operate with two good legs.
2. Main Chassis System Control Key Switch	Multiple failures that cause all three legs to mismatch (with key stop disabled)	Electrical power transient; fire; flood; missiles	C1b	The voted key switch changes to STOP, but the application program does not halt because key stop is disabled.	PLC continues to operate with some degraded capability, but still able to perform its safety function. Degraded capability – if the key switch was in REMOTE position, the change to STOP would inhibit remote access. If the key switch was in PROGRAM position, the change to STOP would inhibit programming changes.
3. Main Chassis System Control Key Switch	Multiple failures that cause all three legs to mismatch (with key stop enabled)	Electrical power transient; fire; flood; missiles	C3b	The voted key switch changes to STOP.	The application program halts with outputs turned off.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
4. Main Chassis System Control Key Switch	Multiple failures that cause multiple legs to fail the same way	Loose connector, Electrical power transient; fire; flood; missiles	C1b	The voted key switch changes to: REMOTE, RUN, PROGRAM, or STOP.	PLC can continue to operate with degraded capability, depending on the change to the voted key switch value: REMOTE to other: could lose write access permission. Other to REMOTE: could permit unwanted write access to points. Other to STOP: depends on configuration of key stop disable - could halt the application. Other to PROGRAM: could permit unwanted programming changes PROGRAM to other: could inhibit programming changes. STOP to RUN: unexpected start of the application program.
5. Main Chassis Power Supply Rails	Both rails fail open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals will not be read. Analog and digital outputs fail low.	PLC fails to operate. All analog, digital and relay outputs turn off.
6. Main Chassis Power Supply Rails	One rail fails open or shorts to ground	Electrical power transient and/or motherboard insulation failure	C1a, C1b	None	PLC continues operation via redundant main chassis power supply. Main processor diagnostics will detect and flag power rail fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
7. Main Chassis TRIBUS Serial Links	All three links open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals will not be read. Analog and digital outputs fail low.	PLC fails to operate
8. Main Chassis TRIBUS Serial Links	One or two links open or short to ground.	Electrical power transient and/or motherboard insulation failure	C1a, C1b, C4a, C4b	None	PLC continues to operate via intact TRIBUS. Main processor diagnostics will detect and flag TRIBUS link fault.
9. Main Chassis I/O Bus	All three buses open or short to ground	Electrical power transient; fire; flood; missiles	C3b	I/O signals downstream of an open bus will not be read. I/O signals will not be read for a shorted bus condition. Analog and digital outputs fail low at and past an open bus.	PLC microprocessors continue to operate, with I/O limitations as noted. Main processor diagnostics will detect and flag I/O bus fault.
10. Main Chassis I/O Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	C1a, C1b, C4a, C4b	None	PLC continues to operate via intact I/O bus(es). Main processor diagnostics will detect and flag I/O bus fault.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
11. Main Chassis Communications Bus	All buses open or short to ground	Electrical power transient; fire; flood; missiles	C4a, C4b	None	PLC continues to operate as a standalone device. Communications to external terminals is interrupted. Main processor diagnostics will detect and flag communications bus fault. Would require logic in the external system to detect and alarm this failure (application-specific).
12. Main Chassis Communications Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	C1a, C1b, C4a, C4b	None	PLC continues to operate. Communications to external devices continues via intact communications bus(es). Main processor diagnostics will detect and flag communications bus fault.
13. Main Chassis Communications Bus	Communication from one MP to the two others differs at the two other MPs	Failure of receiver at one receiving MP	C1a, C1b, C4a, C4b	None	Voted out and alarmed.
14. Main Chassis Battery Pack	Output voltage fails low	Battery aging or short circuit	C1a, C1b	None	PLC continues to operate, unless failure is concurrent with loss of all input power. Battery failure concurrent with all power failure will result in loss of main program memory from SRAM. Main processor diagnostics will detect and flag low battery voltage prior to failure.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
15. RXM Chassis Power Supply Rails	Both rails fail open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals will not be read. Analog and digital outputs fail low for shorted rails, and fail low at and past the failure points for open rails.	PLC continues to operate, with loss of I/O function in the failed RXM chassis as noted, and all downstream chassis assemblies. Main processor diagnostics will detect and flag power rail fault. Fault alarm via Main Chassis Power Module alarm circuit.
16. RXM Chassis Power Supply Rails	One rail fails open or shorts to ground	Electrical power transient and/or motherboard insulation failure	C1a, C1b	None	PLC continues operation via redundant RXM chassis power supply. Main processor diagnostics will detect and flag power rail fault. Fault alarm via Main Chassis Power Module alarm circuit.
17. RXM Chassis I/O Bus	All buses open or short to ground	Electrical power transient; fire; flood; missiles	C3b	Input signals downstream of an open bus will not be read. Input signals will not be read for a shorted bus condition. Analog and digital outputs fail low.	PLC microprocessors continue to operate, with I/O limitations in the specific RXM chassis as noted, and all downstream chassis assemblies. Main processor diagnostics will detect and flag I/O bus fault.
18. RXM Chassis I/O Bus	One or two buses open or short to ground	Electrical power transient and/or motherboard insulation failure	C1a, C1b, C4a, C4b	None	PLC continues to operate via intact I/O bus(es). Main processor diagnostics will detect and flag I/O bus fault.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
PLC CABLE-RELATED FAILURES					
1. Main Chassis-to-RXM Chassis I/O Expansion Cables (set of 3 cables)	Open circuit, short circuit or hot short in all three cables	Fault in adjacent power cable; fire; flood; missiles	C3b	Input signals downstream of the faulted cables will not be read. Analog and digital outputs fail low.	PLC microprocessors continue to operate, with I/O limitations downstream of the I/O Expansion cable fault as noted. Main processor diagnostics will detect and flag I/O cable fault.
2. Main Chassis-to-RXM Chassis I/O Expansion Cables (set of 3 cables)	Open circuit, short circuit or hot short in one or two cables	Fault in adjacent power cable; cable cut	C1a, C1b, C4a, C4b	None	PLC continues to operate via intact I/O cable(s). Main processor diagnostics will detect and flag I/O cable fault.
3. Main Chassis Communications Module: Model 4352AN, Tricon Communication Module (TCM) – network cable	Open circuit, short circuit or hot short in cable	Fault in adjacent power cable; cable cut	C1a, C1b, C2a, C2b	None	PLC continues to operate. Communications to external network devices is interrupted. Main processor diagnostics will detect and flag communications fault. Requires application-specific alarming in the external system.
4. Primary RXM (4200N) to Remote RXM (4201) Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of all three RXM transmit or receive cables	Fire; flood, missiles	C3b	Input signals in affected RXM chassis will not be read. Analog and digital outputs fail low.	PLC continues to operate, with loss of I/O function in the failed RXM chassis as noted. Main processor diagnostics will detect and flag RXM communications fault.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
5. Primary RXM (4200N) to Remote RXM (4201) Multi-mode Fiber Optics (set of 6 fiber optic cables)	Loss of one or two RXM transmit or receive cables	Fire or cable cut	C1a, C1b, C4a, C4b	None	PLC continues to operate via intact RXM cable(s). Main processor diagnostics will detect and flag RXM communications fault.
6. Chassis to Term Panel Cable For Digital Input Modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Open circuit or short circuit to ground	Fault in adjacent power cable; cable cut; fire; flood; missiles	C2a, C2b, C3a	Affected digital inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing.
7. Chassis to Term Panel Cable For Digital Input Modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Short circuit across DI point	Fire or cable cut; term panel short	C2a, C2b, C3a	Affected digital inputs will fail high	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing; or (c) a single DI point has been used to indicate supply of external power as an application specific alarm.
8. Chassis to Term Panel Cable For Digital Input Modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital inputs may fail low; provided failure voltage is high enough to burn out affected DI points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
9. Chassis to Term Panel Cable For Digital Output Modules: Model 3601TN; 115 Vac	Open circuit	Fault in adjacent power cable; cable cut; fire; flood; missiles	C2a, C2b, C3a	PLC digital outputs will not be affected, but field devices will fail low	PLC continues operation. Condition will not be detected unless: (a) DO point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
10. Chassis to Term Panel Cable For Digital Output Modules: Model 3601TN; 115 Vac	Short circuit to ground	Fault in adjacent power cable; fire; flood; missiles	C3a	Affected digital outputs will fail low	PLC continues operation. Condition will be detected by DO module field voltage detection circuit, which will activate the LOAD/FUSE alarm since the commanded DO state will not match the detected field voltage.
11. Chassis to Term Panel Cable For Digital Output Modules: Model 3601TN; 115 Vac	Hot short	Fault in adjacent power cable	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
12. Chassis to Term Panel Cable For Analog Input Modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Open circuit or short circuit to ground	Fault in adjacent power cable; cable cut; fire; flood; missiles	C3a	Affected analog inputs will fail low (downscale)	PLC continues operation. Low range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.
13. Chassis to Term Panel Cable For Analog Input Modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected analog inputs may fail low (downscale); assuming failure voltage is high enough to burn out affected AI points	PLC continues operation. Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
14. Chassis to Term Panel Cable For Analog Output Module: Model 3805HN; 4-20ma	Open circuit	Fault in adjacent power cable; cable cut; fire; flood; missiles	C3a	Affected analog output end devices will fail low (downscale)	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Load Indicator, which in turn activates the chassis alarm signal.
15. Chassis to Term Panel Cable For Analog Output Module: Model 3805HN; 4-20ma	Short circuit to ground or hot short	Fault in adjacent power cable; fire; flood; missiles	C3a	Affected analog outputs will fail downscale for a short circuit, and may fail low for a hot short; assuming failure voltage is high enough to burn out affected AO points	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each channel. Failure of any diagnostic on any channel activates the module's Fault Indicator, which in turn activates the chassis alarm signal.
TERMINATION PANEL-RELATED FAILURES					
1. Term Panel For Digital Input Modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Open circuit or short circuit to ground	Fire; flood; missiles; term panel fuse failure or short	C2a, C2b, C3b	Affected digital inputs will fail low	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing.
2. Term Panel For Digital Input Modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Short circuit across DI point	Fire or cable cut; term panel short	C2a, C2b, C3a	Affected digital inputs will fail high	PLC continues operation. Condition will not be detected unless: (a) DI point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
3. Term Panel For Digital Input Modules: Model 3501TN2; 115 Vac/Vdc Model 3503EN2; 24 Vac/Vdc	Hot short	Fault in adjacent power cable	C3a	Affected digital inputs may fail low; provided failure voltage is high enough to burn out affected DI points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
4. Term Panel For Digital Output Modules: Model 3601TN; 115 Vac	Open circuit	Fire; flood; missiles; term panel fuse failure	C2a, C2b, C3b	PLC digital outputs will not be affected, but field devices will fail low	PLC continues operation. Condition will not be detected unless: (a) DO point failures triggered alarms associated with measured parameters; or (b) by periodic channel checks or surveillance testing.
5. Term Panel For Digital Output Modules: Model 3601TN; 115 Vac	Short circuit to ground	Fire; flood; missiles or cable fault; term panel short	C3a, C3b	Affected digital outputs will fail low	PLC continues operation. Condition will be detected by DO module field voltage detection circuit, which will activate the LOAD/FUSE alarm since the commanded DO state will not match the detected field voltage; or by the OVD diagnostic if the failed state matches the current demanded state.
6. Term Panel For Digital Output Modules: Model 3601TN; 115 Vac	Hot short	Fault in adjacent power cable	C3a	Affected digital outputs may fail low; assuming failure voltage is high enough to burn out affected DO points	PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
7. Term Panel For Analog Input Modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Open circuit or short circuit to ground	Fire; flood; missiles; term panel fuse failure or short	C3a, C3b	Affected analog inputs will fail low (downscale)	PLC continues operation. Low range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.

APPENDIX A: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
8. Term Panel For Analog Input Modules: Model 3703EN; 0-5, 0-10 Vdc Model 3721N; 0-5/-5 to +5 Vdc	Hot short	Fault in adjacent power cable	C3a	Affected analog inputs may fail high or low (downscale); assuming failure voltage is high enough to burn out affected AI points	PLC continues operation. Low or high range diagnostic monitoring alarm (channel violation of allowed tolerance) resulting in board fault alarm. Main processor diagnostics will detect and flag board fault via Main Chassis Power Module alarm circuit.
9. Term Panel For Analog Output Modules: Model 3805HN; 4-20ma	Open circuit	Fire; flood; missiles; term panel fuse failure or short	C3a, C3b	Affected analog output end devices will fail low (downscale)	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's Load Indicator, which in turn activates the chassis alarm signal.
10. Term Panel For Analog Output Modules: Model 3805HN; 4-20ma	Short circuit to ground or hot short	Fault in adjacent power cable	C3a	Affected analog outputs will fail downscale for a short circuit, and may fail low for a hot short; assuming failure voltage is high enough to burn out affected AO points	PLC continues operation. Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's Fault Indicator, which in turn activates the chassis alarm signal.

Appendix B – FMEA; PPS Tricon (Non-Safety Related Components)

NOTE: Failure Category Column

The Failure Category column in the FMEA Table shows the primary failure categories. For example nearly all single failures on the Tricon modules are in the C1a and C1b category since the diagnostic coverage is in the 95 to 99% range. The C2a and C2b categories represent the small percentage of failures that are not detected by self-diagnostics and require additional levels of protection.

Power and Termination

The FMEA assumes that all loop power supplies are redundant (two power supplies). The FMEA also includes the termination panels and termination cables. These panels and cables have many single points of failure and these failures are typically considered as a part of the connected I/O device. In many cases they are neglected since the panel and cable failure rates are very low compared to the failure rate of the connected I/O device (Reference 3.3.4).

Tricon Platform FMEA Qualification

As of the date of this document, the Tricon V10.5.3 is the most current nuclear qualified product, subsequent to two maintenance releases (V10.5.2 and V10.5.3) since V10.5.1 (the version upon which the NRC based its Tricon V10 SER for generic nuclear industry approval). The V10 Tricon Reference Design Change Analysis, Revision 0 [Reference 3.3.11] identifies and characterizes the platform changes that have occurred since V10.5.1 and evaluates the significance of the changes as they relate to documents under review for the PPS Replacement System.

Qualification of Tricon V10.5.1 was by analysis based on the Tricon V10.2.1 tests. Tricon V10.5.1 essentially represents the further evolutionary upgrades and bug fixes made to platform software since V10.2.1 was released. Qualification evaluations have determined that the routine product upgrades have not altered the critical characteristics of the product, i.e., current modules have the same (or better) functional and environmental characteristics as the Tricon V10.2.1 Test Specimen FMEA provided in the Triconex Topical Report 7286-545-1-A, revision 4 [Reference 3.3.2].

APPENDIX B: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Non-Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
1. Remote RXM Chassis Model 4201; Remote Extender Module (RXM), Multi- mode Fiber Optics (set of 3 modules)	Loss of all three RXM modules	Fire; flood; missiles; software common mode failure	C3b	Input signals in affected RXM chassis will not be read. Analog and digital outputs fail low.	Continues to operate, with loss of I/O function in the failed Remote RXM chassis, and all downstream chassis assemblies (if any). Main processor diagnostics will detect and flag RXM communications fault. Non-safety trip outputs go to OFF: - OTTR/OPTR Trip
2. Remote RXM Chassis Model 4201; Remote Extender Module (RXM), Multi- mode Fiber Optics (set of 3 modules)	Loss of one or two RXM modules	Electronics or softwar e failure	C1a, C1b, C4a, C4b	None	Continues to operate via intact RXM module(s). Main processor diagnostics will detect and flag RXM module fault.
3. Digital input modules: Model 3501E; 115 Vac/Vdc	Input point(s) stuck OFF on one leg.	Electronic component or multiple components on different points.	C1a, C1b; C2a, C2b if point is normally OFF	None	Continues operation. Condition will be detected for all DI modules except Model 3501E if the point is normally OFF, which does not include Stuck Off diagnostic capability. Non-detectable fault.
4. Digital input modules: Model 3501E; 115 Vac/Vdc	Input point(s) stuck OFF on multiple legs.	Multiple electronic component failures on same point or fuse failure	C1a, C1b, C3b,and C2a, C2b if point is normally OFF	Affected digital input(s) will fail low	Continues operation. Condition will be detected for all DI modules except Model 3501E if the point is normally OFF, which does not include Stuck Off diagnostic capability. Non-detectable fault.

APPENDIX B: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Non-Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
5. Digital input modules: Model 3501E; 115 Vac/Vdc	Input point(s) stuck ON for one leg	Electronic component failure or multiple component failures on different points.	C1a, C1b; C2a, C2b only for 3501E if point is normally ON.	None	Continues operation. Condition will be detected for all DI modules except Model 3501E if the point is normally ON, which does not include Stuck On diagnostic capability. Non-detectable fault.
6. Digital input modules: Model 3501E; 115 Vac/Vdc	Input point(s) stuck ON for multiple legs	Multiple electronic component failures on same point or fuse failure	C1a, C1b,, C3b C2a, C2b only for 3501E if point is normally ON.	Affected digital input(s) will fail high.	Unable to correctly determine the state of the affected point(s). Condition will be detected for all DI modules except Model 3501E if the point is normally ON, which does not include Stuck On diagnostic capability.
7. Digital input modules: Model 3501E; 115 Vac/Vdc	Common processing failure on one or two legs.	Electronic component failure(s)	C1a, C1b	None	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
8. Digital input modules: Model 3501E; 115 Vac/Vdc	Common processing failure on all three legs.	Electronic component failures on all legs or comm. Software failure	C3b	Affected digital inputs will not be read.	Treats all affected input points as OFF. Main processor diagnostics will detect and flag board fault(s). Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX B: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Non-Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
9. Analog output module: Model 3805E; 4-20ma	Output signal fails high or low on one or two legs.	Electronic component failure(s)	C1a, C1b	None	Continues operation. Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's Fault Indicator, which in turn activates the chassis alarm signal. Failure of all three legs for a given output will activate the Load Indicator, and output will not be driven.
10. Analog output module: Model 3805E; 4-20ma	Output signal fails high or low on all three legs.	Multiple electronic component failures or firmware failure	C3b	Affected analog outputs will fail to unknown value.	Unable to control the affected output points. Each analog output module sustains complete ongoing diagnostics for each leg. Failure of any diagnostic on any leg activates the module's Fault Indicator, which in turn activates the chassis alarm signal.
11. Analog output module: Model 3805E; 4-20ma	Common processing failure on one or two legs.	Electronic component failure(s)	C1a, C1b	None	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.
12. Analog output module: Model 3805E; 4-20ma	Common processing failure on all three legs.	Multiple module electronics failure or comm. software failure	C3b	Affected analog outputs will fail downscale.	Unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX B: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Non-Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
13. Analog output module: Model 3805E; 4-20ma	Module accuracy out of specification on multiple legs.	Components of the self-calibration voltage-reference circuits for all legs drift over time.	C3b	Affected outputs could potentially be outside of the published accuracy.	Continues operation. Minimum proof test interval is once every 30 months to detect common cause drift.
14. Analog output module: Model 3805E; 4-20ma	Module accuracy out of specification on a single leg.	Components of the self-calibration voltage-reference circuits for all legs drift over	C1a, C2a	Affected outputs could potentially be outside of the published accuracy.	Continues operation. Significant deviations are detected and alarmed.
15. Relay output module: Model 3636T; Relay Output	Relay output fails open or closed	Electronic component or fuse failure	C1a, C1b, C2a, C2b	If relay contact or fuse, affected field loads from relay outputs will fail to the corresponding output state. If internal fault, no effect on output.	Unable to control affected output points, if contact or fuse fault. Relay contact or fuse faults will not be detected. All internal faults will be detected by RO diagnostics and alarmed.
16. Relay output module: Model 3636T; Relay Output	Common processing failure on one or two legs	Electronic component failure(s)	C1a, C1b,C2a, C2b	None	Continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit.

APPENDIX B: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Non-Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
17. Relay output module: Model 3636T; Relay Output	Common processing failure on all three legs.	Module electronics failure or comm. software failure	C1a, C1b, C2a, C2b, C3b	Affected relay outputs will be OPEN.	Unable to control the affected output points. Main processor diagnostics will detect and flag board fault. Relay contact or fuse faults will not be detected. Fault alarm via Main Chassis Power Module alarm circuit.
18. Loop power supply for relay output module: Model 3636T; Relay Output	Power supply output voltage fails low	Electronic component or fuse failure	C2a, C2b	Affected field loads from relay outputs will fail to the de-energized state	Continues operation. Condition will not be detected unless: (a) power supply failure was alarmed, or (b) RO point failures triggered alarms associated with controlled parameters; or (c) by periodic channel checks or surveillance testing.
19. Loop power supply for relay output module: Model 3636T; Relay Output	Power supply output voltage fails high	Electronic component failure	C2a, C2b	Affected field loads from relay outputs may fail to the de-energized state; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Relay contacts may flash over if failure voltage exceeds maximum specified voltage.
20. Term Panel For Relay Output Modules: Model 3636T; Relay Output	Open circuit or short circuit to ground	Fire; flood; missiles; term panel fuse failure or short	C2a, C2b	Affected field loads from relay outputs will fail to the de-energized state	PLC continues operation. Condition will not be detected unless: (a) RO point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing.

APPENDIX B: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Non-Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
21. Term Panel For Relay Output Modules: Model 3636T; Relay Output	Hot short	Fault in adjacent power cable	C2a, C2b	Affected field loads from relay outputs may fail to the de-energized state; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Relay contacts may flash over if failure voltage exceeds maximum specified voltage.
22. Chassis to Term Panel Cable For Relay Output Module: Model 3636T; Relay Output	Open circuit or short circuit to ground	Fault in adjacent power cable; cable cut; fire; flood; missiles	C2a, C2b	Affected field loads from relay outputs will fail to the de-energized state	PLC continues operation. Condition will not be detected unless: (a) RO point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing.

APPENDIX B: FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.x TMR PLC (Non-Safety Related Components)

Affected Components	Failure Mode	Failure Mechanism	Failure Category	Effect on PLC Inputs and Outputs	Effect on PLC Operability
23. Chassis to Term Panel Cable For Relay Output Module: Model 3636T; Relay Output	Hot short	Fault in adjacent power cable	C2a, C2b	Affected field loads from relay outputs may fail to the de-energized state; assuming failure voltage is high enough to burn out field devices (application-specific failure).	PLC continues operation. Relay contacts may flash over if failure voltage exceeds maximum specified voltage.

Appendix C – FMEA; Safety-Related Software

APPENDIX C - FMEA FOR SAFETY-RELATED SOFTWARE			
Affected Software	**Failure Mode/ Detectable or Undetectable**	**Failure Mechanism**	**Effect on Tricon System/Barriers to Overcome to Achieve Failure**
1. Application software	One or more functions fails to execute/ Detectable	Intentional or unintentional change to software	Effects could be from minimal to complete shutdown of system to safe state. For this event to occur, a person with knowledge of the Tricon and TriStation 1131 would need to: b) build and compile new application program with all errors resolved, c) physically connect PC to Tricon; which should be administratively prohibited while system is operational, d) perform download procedures, e) direct Tricon to run new application. Redundant PPS channels are unaffected.
2. Application software	Random bit change/Detectable	Cosmic radiation, inadvertent moisture addition, etc.	None. The nature of a failure of this type would only appear on one of the three MPs at a time. Any change to program, input or output data would be voted as bad at any number of points based on triple redundancy architecture. Redundant PPS legs are unaffected.
3. Application software	Erroneous data and I/O outputs/Detectable	One or more functions not programmed correctly	Effect could be from minimal to complete shutdown of system to a safe state depending on error. For this event to occur, the error or omission would have to go undetected from design review, design verification, emulator testing, verification and validation. Redundant PPS channels are unaffected.
4. Application software	Erroneous data and I/O outputs/Undetectable	Undetected program bug	Tricon will operate erratically. Redundant PPS channels are unaffected.
5. Connection to external networks or software.	Extraneous message or virus is introduced/Detectable	Inadvertent connection to a network or outside software.	Tricon will operate as normal. Tricon will reject any message that does not pass error checking algorithms, handshake checks, or unexpected protocols. Additionally, access through ports or drives should be controlled through one or more means of administrative controls, physical blocking, or software disabling. Redundant PPS channels are unaffected.

Appendix D – FMEA; Input Signal Loading

APPENDIX D – FMEA FOR INPUT SIGNAL LOADING					
Process Variable Parameter	**Protection Set I**	**Protection Set II**	**Protection Set III**	**Protection Set IV**	**Loading Analysis**
1. DTTA Upper Neutron Flux	NE-41A Loop 1	NE-42A Loop 2	NE-43A Loop 3	NE-44A Loop 4	Redundant upper flux in each Protection Set.
2. DTTA Lower Neutron Flux	NE-41B Loop 1	NE-42B Loop 2	NE-43B Loop 3	NE-44B Loop 4	Redundant lower flux in each Protection Set.
3. Wide Range Reactor Coolant Temperature Channels Hot/Cold Legs	TE-413A Loop 1 TE-413B Loop 1	TE-433A Loop 3 TE-433B Loop 3			All four loops are input into the Protection Sets – Loops 1 & 2 into PS1; Loops 3 & 4 into PS2. The T_{hot} & T_{cold} for each loop enter on same AI module.
4. Wide Range Reactor Coolant Temperature Channels Hot/Cold Legs	TE-423A Loop 2 TE-443B Loop 2	TE-443B Loop 4 TE-443A Loop 4			All four loops are input into the Protection Sets – Loops 1 & 2 into PS1; Loops 3 & 4 into PS2. The T_{hot} & T_{cold} for each loop enter on same AI module.
5. DTTA Pressurizer Pressure	PT-455 Loop 1	PT-456 Loop 2	PT-457 Loop 3	PT-474 Loop 4	Redundant pressurizer pressure in each Protection Set.
6. DTTA Thot	TE-410A Loop 1 T_{hot-1A} TE-411A Loop 1 T_{hot-2A} TE-412A Loop 1 T_{hot-3A} TE-410C Loop 1 T_{hot-1B} TE-411C Loop 1 T_{hot-2B} TE-412C Loop 1 T_{hot-3B}	TE-420A Loop 2 T_{hot-1A} TE-421A Loop 2 T_{hot-2A} TE-422A Loop 2 T_{hot-3A} TE-420C Loop 2 T_{hot-1B} TE-421C Loop 2 T_{hot-2B} TE-422C Loop 2 T_{hot-3B}	TE-430A Loop 3 T_{hot-1A} TE-431A Loop 3 T_{hot-2A} TE-432A Loop 3 T_{hot-3A} TE-430C Loop 3 T_{hot-1B} TE-431C Loop 3 T_{hot-2B} TE-432C Loop 3 T_{hot-3B}	TE-440A Loop 4 T_{hot-1A} TE-441A Loop 4 T_{hot-2A} TE-442A Loop 4 T_{hot-3A} TE-440C Loop 4 T_{hot-1B} TE-441C Loop 4 T_{hot-2B} TE-442C Loop 4 T_{hot-3B}	Multiple T_{hot} inputs from a single loop on two different AI modules in each Protection Set. Each Protection Set has inputs from the corresponding loop number.

APPENDIX D – FMEA FOR INPUT SIGNAL LOADING

Process Variable Parameter	Protection Set I	Protection Set II	Protection Set III	Protection Set IV	Loading Analysis
7. DTTA Tcold	TE-410B Loop 1 T_{cold-1} TE-411B Loop 1 T_{cold-2}	TE-420B Loop 2 T_{cold-1} TE-421B Loop 2 T_{cold-2}	TE-430B Loop 3 T_{cold-1} TE-431B Loop 3 T_{cold-2}	TE-440B Loop 4 T_{cold-1} TE-441B Loop 4 T_{cold-2}	Multiple T_{cold} inputs from a single loop on two different AI modules in each Protection Set. Each Protection Set has inputs from the corresponding loop number.
8. Wide Range Reactor Coolant Pressure Channels			PT-403 Loop 4	PT-405 Loop 3	Reactor coolant pressure from two different loops input to two Protection Sets.
9. Wide Range Reactor Coolant Pressure Channels Input to Residual Heat Removal (RHR) valve interlock circuit			PT-403A Loop 4	PT-405A Loop 4	Redundant loops in two Protection sets.
10. Pressurizer High Water Level Reactor Trip	LT-459	LT-460	LT-461		Pressurizer High Water Level is redundant in Protection Sets I, II & III.
11. Pressurizer Vapor Space Temperature Low				TE-454	This interlock augments the loop 4 wide range pressure parameter (PT-405A) for Residual Heat Removal (RHR) cold leg isolation valve V-8701. Redundancy is not required.
12. Steam Flow	FT-512 Loop 1 FT-522 Loop 2 FT-532 Loop 3 FT-542 Loop 4	FT-513 Loop 1 FT-523 Loop 2 FT-533 Loop 3 FT-543 Loop 4			Each of the 4 loops is redundant in Protection Sets 1 & 2.

APPENDIX D – FMEA FOR INPUT SIGNAL LOADING

Process Variable Parameter	Protection Set I	Protection Set II	Protection Set III	Protection Set IV	Loading Analysis
13. Steam Line Pressure	PT-514 Loop 1 PT-524 Loop 2 PT-534 Loop 3 PT-544 Loop 4	PT-515 Loop 1 PT-525 Loop 2 PT-535 Loop 3 PT-545 Loop 4	PT-526 Loop 2 PT-536 Loop 3	PT-516 Loop 1 PT-546 Loop 4	Each of the 4 loops is input to at least 3 Protection Sets.
14. Steam Generator Narrow Range Level Channels S/G Low-Low Level Reactor Trip and Auxiliary Feedwater (AFW) Pump Start	LT-529 S/G 2 LT-539 S/G 3	LT-519 S/G 1 LT-549 S/G 4	LT-518 S/G 1 LT-528 S/G 2 LT-538 S/G 3 LT-548 S/G 4	LT-517 S/G 1 LT-527 S/G 2 LT-537 S/G 3 LT-547 S/G 4	Each of the 4 loops is input to 3 Protection Sets.
15. Turbine Impulse Power Low C-5 Interlock	PT-505				Turbine Impulse Power Low C-5 Interlock is to prevent automatic outward rod motion when power is less than the design limit for the Rod Control System.
16. Turbine Impulse Chamber Pressure High P-13 Interlock	PT-505	PT-506			Turbine Impulse Chamber Pressure High P-13 Interlock is to provide an input to P-7 indicative of low turbine power when less than the setpoint.

Appendix E – FMEA; PPS Buyout Components

APPENDIX E - FMEA FOR PPS BUYOUT COMPONENTS					
Affected Components	**Failure Mode/ Detectable or Undetectable**	**Failure Mechanism**	**Failure Category**	**Effect on Tricon Inputs and Outputs/Effect on PPS**	**Effect on Tricon Operability**
1. 24 VDC Loop Power Supply for Digital I/O field loops (3503EN2) Kepco; HSF-24-4.5PFC	Loss of one power supply output/ Detectable	Power or electronics failure	N/A	None/None	Tricon continues to operate through redundant Kepco power supply feed. “PS X Trouble” alarm is generated by loss of one instrument power supply.
2. 24 VDC Loop Power Supply for Digital I/O field loops (3503EN2) Kepco; HSF-24-4.5PFC	Power Supply output Fails High or low/ Detectable	Electronic component or fuse failure	N/A	None/None	Tricon continues to operate through redundant Kepco power supply feed. “PS X Trouble” alarm is generated by loss of one instrument power supply.
3. 48 VDC Loop Power Supply for Analog I/O field loops (3721N) Kepco; HSF-48-3.3PFC	Loss of one power supply output/ Detectable	Power or electronics failure	N/A	None/None	Tricon continues to operate through redundant Kepco power supply feed. “PS X Trouble” alarm is generated by loss of one instrument power supply.
4. 48 VDC Loop Power Supply for Analog I/O field loops (3721N) Kepco; HSF-48-3.3PFC	Power Supply output Fails High or low/ Detectable	Electronic component or fuse failure	N/A	None/None	Tricon continues to operate through redundant Kepco power supply feed. “PS X Trouble” alarm is generated by loss of one instrument power supply.

APPENDIX E - FMEA FOR PPS BUYOUT COMPONENTS

Affected Components	Failure Mode/ Detectable or Undetectable	Failure Mechanism	Failure Category	Effect on Tricon Inputs and Outputs/Effect on PPS	Effect on Tricon Operability
5. Analog Input Terminator -- For 3721N AI Module -- Triconex; 4000220-001N	Errors on unused Analog Input points	Manufacturing error, bent connector pin(s)	N/A	None/None	Tricon continues to operate. Analog errors for unused points are reported, as applicable.
6. Media Converter Garrettcom; 14EH-ST-9VDC	Complete loss of data throughput/ Detectable	Media Converter power supply failure	N/A	None/None Note: If loss occurs during Maintenance Mode, Points will remain in previously selected states (bypass, OOS).	Tricon continues to operate. Communication error reported.
7. Media Converter Garrettcom; 14EH-ST-9VDC	Complete loss of data throughput/ Detectable	Cable problem; broken or disconnected	N/A	None/None Note: If loss occurs during Maintenance Mode, Points will remain in previously selected states (bypass, OOS).	Tricon continues to operate. Communication error reported.
8. Media Converter Garrettcom; 14EH-ST-9VDC	Data loss, garbled data, data collisions/ Detectable	Component or firmware errors, or configuration setup error	N/A	None/None Note: If loss occurs during Maintenance Mode, Points will remain in previously selected states (bypass, OOS).	Tricon continues to operate. Communication error reported.