

Project: **TRICON v10 NUCLEAR QUALIFICATION PROJECT**

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

**FAILURE MODES AND EFFECTS ANALYSIS (FMEA)
 FOR THE TRICON VERSION 10.2
 PROGRAMMABLE LOGIC CONTROLLER**

Document No: 9600164-531

Revision 0

May 23, 2007

| | Name | Signature | Title |
|--------------|--------------------|---------------------------|-----------------------------|
| Author: | Wolfgang Sinocruz | <i>Wolfgang Sinocruz</i> | Hardware Engineer |
| Contributor: | Anton Frederickson | <i>Anton Frederickson</i> | R&D Engineer |
| Reviewer: | Aad Faber | <i>Aad Faber</i> | Independent Review Engineer |
| | Frank Kloer | <i>Frank Kloer</i> | Project Engineer |
| | Ted Porfilio | <i>Ted Porfilio</i> | Project QA Engineer |
| Approvals: | Naresh Desai | <i>Naresh Desai</i> | Product Manager |

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 2 of 61 | Date: | 05/23/07 |

Revision History

| Revision | Date | Change | Author |
|-----------------|-------------|---------------|-------------------|
| 0 | 5/23/2007 | Initial Issue | Wolfgang Sinocruz |
| | | | |

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 3 of 61 | Date: | 05/23/07 |

TABLE OF CONTENTS

| | <u>Page Number</u> |
|---|--------------------|
| 1.0 PURPOSE | 4 |
| 2.0 OBJECTIVE | 4 |
| 3.0 SCOPE | 4 |
| 4.0 METHOD OF ANALYSIS | 5 |
| 5.0 REFERENCES | 9 |
| 6.0 PLC MODULE DIAGNOSTIC DESCRIPTION | 9 |
| 7.0 FMEA SUMMARY AND CONCLUSIONS | 27 |
| 8.0 FAILURE MODES AND EFFECTS ANALYSIS | 30 |

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 4 of 61 | Date: | 05/23/07 |

1.0 PURPOSE

EPRI TR-107330 “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants” (Reference 5.1) defines the requirements for qualifying commercially available programmable logic controllers (PLCs) for safety-related nuclear power plant applications. The Reference 5.1 guidelines require the performance of a Failure Modes and Effects Analysis (FMEA) to evaluate the effects of failures of components in the PLC modules on PLC performance.

The Triconex Corporation is qualifying the commercial grade TRICON VERSION 10.2 Triple Modular Redundant (TMR) Programmable Logic Controller for safety-related nuclear power plant applications. This report documents the methodology and results of the FMEA performed for the generic qualification of the TRICON VERSION 10.2 TMR PLC.

2.0 OBJECTIVE

The objective of this report is to document the methodology and results of the generic FMEA for the TRICON VERSION 10.2 TMR PLC. The FMEA is performed in accordance with the applicable guidelines of Reference 5.1, Section 6.4.1, “FMEA”.

3.0 SCOPE

- 3.1 This analysis is prepared as a part of the TRICON Nuclear Qualification Program as defined in Reference 5.2.
- 3.2 The system analyzed by the FMEA is identical to the Test Specimen configuration that was used in the Qualification Test Program. The Test Specimen includes 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. Specific hardware configurations, application programs, supporting drawings and documents are identified in the Master Configuration List (Reference 5.3).

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 5 of 61 | Date: | 05/23/07 |

3.3 The intent of the FMEA is to identify potential failure states of a typical TRICON PLC in a single train system and to provide data for use in the application-specific FMEA for a particular system. This analysis does not address failure modes associated with application of multiple PLC systems in redundant safety trains. Although application-specific mitigating design features are described for certain failures, this analysis should not be considered as a bounding analysis applicable to actual safety-related applications and installations.

3.4 The Model 8107 Seismic Balance Module used in the qualification test specimen is passive in nature and provides no operational functionality. This module is therefore not included in the scope of the FMEA.

4.0 METHOD OF ANALYSIS

The subject FMEA is performed in accordance with the applicable requirements of EPRI TR-107330 Section 6.4.1, “FMEA” (Reference 5.1). In general, the techniques of Appendix A and Sections 4.1, 4.4, and 4.5 of ANSI/IEEE Std. 352-1987 (Reference 5.4), have been used in this analysis. These techniques included definition of functional areas of PLC operation, as described later in this section. The effect of both single failures and common mode failures on each functional area were then analyzed, as summarized in Section 8.0.

This FMEA is performed using a macroscopic approach, addressing failures on a major component and module level. This approach is appropriate because sub-components in the TRICON modules are triple redundant, and no single failure of an individual sub-component would impact the ability of the PLC to perform its safety related functions. In this analysis, a safety related function is defined as the ability of the safety system to perform a safety shut down function. In addition, the TRICON self-diagnostic features, described in References 5.5 and 5.6 and summarized in Section 6.0 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 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 a typical TRICON PLC system. The components considered include the following:

- a) Power Supplies (including chassis power supplies and I/O loop power supplies)
- b) PLC Chassis (including internal power and communication buses)
- c) Main Processors and Communications Modules
- d) PLC Cables

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 6 of 61 | Date: | 05/23/07 |

- e) PLC I/O Modules
- f) Termination Panels

Figure 1 is a simplified block diagram of a typical TRICON chassis showing the arrangement of these 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 architecture of the TRICON, failure mechanisms that affect a single leg of the triple redundant system generally have no effect on system operation. Therefore, this FMEA considers (1) failure mechanisms that are recognized as being highly unlikely but that could affect multiple components, and (2) the coincident occurrence of otherwise single failures (i.e., multiple failures).

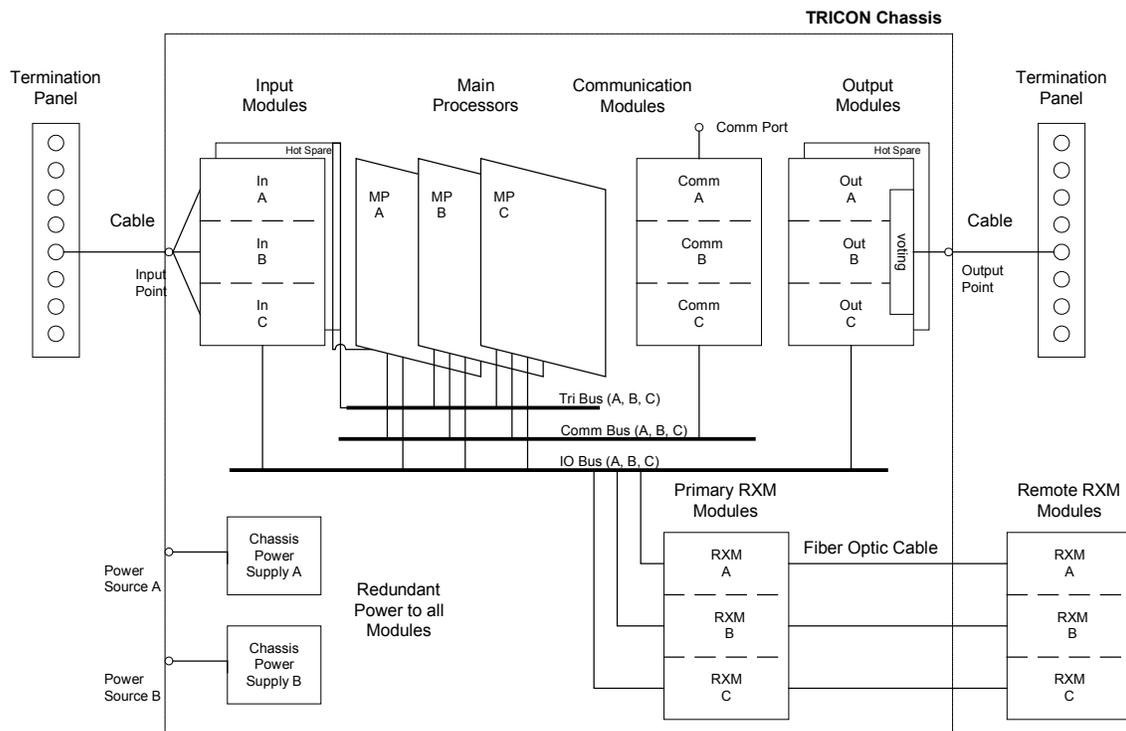


Figure 1. Simplified Block Diagram of Typical TRICON System

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 5.1 recommends the following categories of failure states be identified as a part of the FMEA for redundant PLCs:

- 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.

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 7 of 61 | Date: | 05/23/07 |

- 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 5.1 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 5.1 are modified to be more applicable to the TRICON system. The categories used in this FMEA are as follows:

a

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 8 of 61 | Date: | 05/23/07 |

a

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 severe failures and to provide guidance for application design.

The FMEA tabulation in Section 8.0 of this report includes a column that documents the appropriate failure category assignment for each postulated PLC failure mode. The tabulation in Section 8.0 provides the following data for each type of failure, as required by the guidance of Reference 5.1:

- a) Affected Components

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 9 of 61 | Date: | 05/23/07 |

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

Section 6.0 of this report provides a description of the PLC diagnostics that aid in detection of postulated failures.

5.0 REFERENCES

- 5.1 EPRI Report TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants”, Final Report dated December 1996
- 5.2 Triconex Document 9600164-500, Master Test Plan
- 5.3 Triconex Document 9600164-540, Master Configuration List
- 5.4 ANSI/IEEE Std. 352-1987, “IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems”
- 5.5 Triconex Part No. 9720077-007, TRICON Planning and Installation Guide, August 2006.
- 5.6 Triconex Part No. 9791007-013, TRICON Technical Products Guide, Version 10.2, August 2006.
- 5.7 Triconex Part No. 9100069-001, TRICON V9 ETP Design Specification, Revision 1.2, January 2006.
- 5.8 Triconex Part No. 9600164-532, Reliability/ Availability Study for the TRICON VERSION 10.2 PLC, March 2, 2007.
- 5.9 Triconex Part No. 9600164-732, Reliability/ Availability Spreadsheet for TRICON VERSION 10.2 PLC Operating Under Normal Conditions, March 2, 2007.

6.0 PLC MODULE DIAGNOSTIC DESCRIPTION

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 10 of 61 | Date: | 05/23/07 |

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 Section 8.0. A more detailed description of this information is presented in References 5.5 and 5.6.

6.1 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.

6.1.1 DIGITAL INPUT MODULES

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

- Model 3501T; 115 Vac/Vdc Opto-isolated, non-commoned (32 points)
- Model 3502E; 48 Vac/Vdc Commoned in groups of 8, Self Test (32 points)
- Model 3503E; 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

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 11 of 61 | Date: | 05/23/07 |

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 3501T 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 every three to six 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 3502E and 3503E 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 drive 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, as defined in Reference 5.5:

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 12 of 61 | Date: | 05/23/07 |

| Module | Minimum Input Toggle Rate | Maximum Input Toggle Rate |
|-------------|--|---------------------------|
| Model 3501T | Every 24 months | Every 100 msec |
| Model 3502E | On-state: Not required Off-state: Every 24 months | Every 100 msec |
| Model 3503E | On-state: Not required Off-state: Every 24 months | Every 100 msec |

The maximum input toggle rate enables proper operation of I/O diagnostics and detection of all normally detectable faults. The minimum toggle rate provides fault coverage of normally undetectable faults within 4 % of the calculated Mean Time Between Failure (MTBF) of one of the input circuits on the digital input module.

6.1.2 PULSE INPUT MODULE

This discussion is applicable to the following pulse input (PI) module:

Model 3511; Pulse Input, AC Coupled, fast update (8 points)

For the PI module, the extent of the diagnostic routine is the comparison across the three legs of the respective signal values.

Any leg signal value outside a set tolerance with the signal values in neighboring legs is reported to its respective Main Processor Module. The Main Processor Module fault analyzer routines determine whether a fault exists on a particular module at the end of each scan. One-time 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 pulse input module to illuminate its fault LED.

The PI module diagnostics are specified to operate as follows, as defined in Reference 5.5:

| Module | Minimum Input Change | Input Change Sample Period | Minimum Period of Mis-compares |
|------------|----------------------|--|--------------------------------|
| Model 3511 | 0.5% of full scale | 1 scan or 210 msec, whichever is greater | 10 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.

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 13 of 61 | Date: | 05/23/07 |

6.1.3 ANALOG INPUT MODULES

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

Model 3701; 0-10 Vdc Differential, DC Coupled (32 points)

Model 3703E; 0-5/0-10 Vdc Differential, Isolated (16 points)

Model 3721; 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.

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 3701 and Model 3721 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 3703E AI module built on the diagnostic routine of the 3701 input modules by 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.

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 14 of 61 | Date: | 05/23/07 |

The AI module diagnostics are specified to operate as follows, as defined in Reference 5.5:

| Module | Minimum Input Change | Input Change Sample Period | Minimum Period of Mis-compares |
|-------------|----------------------|--|--------------------------------|
| Model 3701 | 2% of full scale | 1 s can or 200 m sec, whichever is greater | 40 samples |
| Model 3703E | 0.5% of full scale | 1 s can or 50 m sec, whichever is greater | 256 samples |
| Model 3721 | 2% of full scale | 10 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.

6.1.4 THERMOCOUPLE INPUT MODULE

Sensing of each thermocouple input is performed in a manner that prevents a single failure on one channel from affecting another channel. Each module performs complete ongoing diagnostics on each channel.

The diagnostic routine for the Thermocouple Input (TC) modules consists of the automatic or self-calibration of each leg using internal-precision reference voltages. The microprocessors on each leg test for known or expected signal values within a certain tolerance. If the leg microprocessors receive signals within the allowed tolerance, the leg will self-calibrate its A/D converter to null out any undesirable offsets or gains. The module will flag any out of tolerance signal received.

The thermocouple input modules also perform automatic cold or reference junction temperature compensation. Solid-state temperature sensors on the termination panel produce a current for each leg that is proportional to the temperature at the field contact terminals. Each leg in turn adds the reference or cold junction temperature from the measured temperature signal.

The input diagnostic fault coverage is as follows:

| Module | Minimum Input Change | Input Change Sample Period | Minimum Period of Miss-compares |
|-------------|----------------------|----------------------------|---------------------------------|
| Model 3708E | 0.5% of full scale | 50 ms | 256 samples |
| | | | |

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 15 of 61 | Date: | 05/23/07 |

6.2 OUTPUT MODULES

6.2.1 DIGITAL OUTPUT MODULES

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

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

Model 3603T; 120 Vdc Opto-isolated, Commoned (16 points)

Model 3607E; 48 Vdc Opto-isolated, Non-commoned (16 points)

Model 3625; 24 Vdc Commoned (32 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.

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 16 of 61 | Date: | 05/23/07 |

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.

The Models 3603T and 3607E DO modules execute the three phases of the OVD routine described above. Voltage loop-back circuits allow the modules to self-diagnose latent faults within the output voter circuitry.

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 3601T 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, to ensure 100% fault coverage, the field points should be toggled from the normal state to the opposite state and leg output tested accordingly once every three to six months to guarantee the health of the circuitry.

The Model 3625 DO module OVD has two parts. For the normal routine, OVD collects 4 samples with no FET switches modified followed by 4 samples with a single FET switch modified followed by 4 samples with the FET switch returned to it’s commanded

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 17 of 61 | Date: | 05/23/07 |

state. . If no change in the data samples is detected as a result of the single FET switch modification software will resort to the Glitch diagnostic to determine proper operation of the FET switch. During a Glitch cycle the first 8 samples are collected the same as a Normal cycle. The next three samples are collected with the analog feedback is set to low gain voltage, the ninth sample is taken to establish a pre Glitch data point after which the state of the appropriate FET switches are modified to cause the output to change state.

The DO module diagnostics are specified to operate as follows, as defined in Reference 5.5:

| Module | Minimum Output Toggle Rate | Maximum Output Toggle Rate |
|-------------|----------------------------|------------------------------|
| Model 3601T | Every 24 months | Every 100 msec plus one scan |
| Model 3603T | Not applicable | Every 100 msec plus one scan |
| Model 3607E | Not applicable | Every 100 msec plus one scan |
| Model 3625 | Not applicable | Every 30 msec |

The maximum output toggle rate enables proper operation of I/O diagnostics and detection of all normally detectable faults. The minimum toggle rate provides fault coverage of normally undetectable faults within 5 % of the calculated Mean Time Between Failure (MTBF) of one of the switches on the digital output module.

6.2.2 SUPERVISED DIGITAL OUTPUT MODULES

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

Model 3623T; 120 Vac Opto-isolated, Commoned, Supervised (16 points)

Model 3625; 24 Vdc Commoned, Supervised (32 points)

The Model 3623T SDO module performs all three steps of the OVD routine, as discussed in the previous Section 6.2.1. However, these modules extend Step One of the routine to include fault coverage of the field load device. In addition to voltage loopback circuitry, the SDO modules contain additional current loopback circuitry allowing each leg to measure the current flowing to the load.

The current loopback circuitry allows the SDO modules to self-diagnose possible open or short circuit conditions at the field load terminals. The modules perform continuous continuity checks of the field load by verifying that when energized, current is actually

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 18 of 61 | Date: | 05/23/07 |

flowing and the current is below a certain threshold value. The module annunciates any faulty switch or loss of field load. The modules are designed to provide complete fault coverage for both energize-to-trip and de-energize-to-trip applications.

The Model 3625 has a Supervisory portion of the OVD. During a Supervisory cycle if the point is not commanded ON the FET switches are turned ON and the appropriate gain is set. The data stored for the first eight samples represent the field point current. Measurement mode the mode is switched to low gain voltage and the 9th sample is stored then the FET switches are set to back to the commanded state.

The SDO module diagnostics are specified to operate as follows, as defined in Reference 5.5:

| Module | Minimum Output Toggle Rate | Maximum Output Toggle Rate |
|-------------|----------------------------|----------------------------|
| Model 3623T | Not applicable | Every 100 msec |
| Model 3625 | Not applicable | Every 30 msec |

6.2.3 RELAY OUTPUT MODULE

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

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

RO modules are designed for use on non-critical points that are not compatible with “high-side” solid-state output switches. The modules do not possess the series-parallel switch configuration, designed to accommodate single switch failure without affecting the signal driving the load. Therefore, the RO module is not single fault tolerant, and is not intended for use in critical safety-related applications. This module may be used to provide contact inputs to a non-safety annunciator system and is qualified as a 1E to non-1E isolator.

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 verifies 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.

6.2.4 ANALOG OUTPUT MODULE

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 19 of 61 | Date: | 05/23/07 |

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

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. 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.

6.3 MAIN PROCESSOR MODULE

This discussion is applicable to the following Main Processor Module:

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 20 of 61 | Date: | 05/23/07 |

Model 3008; Enhanced TRICON Main Processor, 16 Mbytes DRAM

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 3008, 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 3008, 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 snapshots 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

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 21 of 61 | Date: | 05/23/07 |

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

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 22 of 61 | Date: | 05/23/07 |

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

6.4 COMMUNICATIONS MODULE

6.4.1 TCM MODULE

This discussion is applicable to the following Communications Module:

Model 4352A; 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. TCM communication protocols include: TriStation, Modbus, Modbus TCP, TCP/IP, SNMP, TSAA, Trimble GPS, Peer-to-Peer, Triconex Time Synchronization, and Jet Direct.

The TCM communicates with all three Main Processors over three separate communication busses, one to each Main Processor. The TCM module has a dedicated

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 23 of 61 | Date: | 05/23/07 |

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.

The TCM can be used to transmit safety relevant data, provided the receiving Main Processors check for proper validity of the message and check to make sure the messages are being received at the require update rate. If the received data is not valid, delayed or not received then the data should be set to the Fail Safe state.

Two TCMs can be 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 can not 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.

6.4.2 RXM MODULES

This discussion is applicable to the following Remote Extender Modules:

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

Model 4201-3; 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.

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 24 of 61 | Date: | 05/23/07 |

6.5 TRICON CHASSIS ASSEMBLIES

A TRICON system consists of one Main Chassis and up to fourteen additional chassis. The TRICON Main Chassis can support the following modules:

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

The TRICON Expansion Chassis can support the following modules:

- Two Power Modules
- Communications Modules (in expansion chassis #2 only)
- 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”

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 25 of 61 | Date: | 05/23/07 |

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.

6.6 POWER SUPPLY MODULES

This discussion is applicable to the following Power Supply Modules:

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

Model 8311; 24 Vdc – 175-Watt Power Module

Model 8312; 230 Vac – 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:

| <u>Indicator</u> | <u>Color</u> | <u>Description</u> |
|------------------|--------------|----------------------------|
| 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:

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 26 of 61 | Date: | 05/23/07 |

- 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.

6.7 TRICON TERMINATION PANELS

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 27 of 61 | Date: | 05/23/07 |

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, etc.). The thermocouple input termination panel provides cold-junction temperature sensors and can be ordered with upscale, downscale, or programmable burnout detection.

ATEX/Nuclear EMC ETPs will share the following mechanical design features (Reference 5.7):

- Two Protective Earth terminals, such as the Phoenix Contact 1704033), will be rated for:
- 24-14 AWG wire
- 20A minimum
- 200V minimum
- Horizontal entry
- Located on each end of ETP in such a manner as to minimize connection length to DIN rail mounted PE terminal blocks

ETPs that must meet the nuclear EMC requirements will share the following common design attributes (Reference 5.7):

- All ETP field I/O signals shall have capacitive filtering upon entering the ETP to Chassis Ground. This capacitance shall be nominally 0.001 μ F.
- All single ended type I/O signals shall have a series ferrite and shunt capacitor to field ground.
- All differential type I/O signals shall have a series ferrite and differential shunt capacitor.
- Chassis and field ground shall have 800V_{DC} Isolation.

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

7.0 FMEA SUMMARY AND CONCLUSIONS

The failure modes and effects analysis (FMEA) tabulation is provided in Section 8.0 of this report. As shown, failure modes that can prevent the TRICON system from performing its function are detected by proper application-specific design, the built-in,

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 28 of 61 | Date: | 05/23/07 |

on-line system diagnostics or by periodic off-line testing. Provided the results of this FMEA are applied to specific control system designs, the percentage of undetectable failures associated with safety-related functions will be very low (from Reference 5.9, it is typically less than 1%).

The general effect of failures in C1a & 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 Section 8.0 tabulation. Application-specific design features should be implemented to monitor the TRICON diagnostic alarms so that these failures can be annunciated and repaired in a timely manner (from Reference 5.8, the Mean Time to Repair Online is within 24 hours).

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 as described in the preceding sections.
- b) Failures associated with PLC functions not intended for safety-related applications (e.g., relay outputs).
- c) Failures that could 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).

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 6.0. Only five items, identified with the combination of failure categories C2 and C3a, are not detected by the PLC. These can be detected by either application-specific design features or by periodic channel checks and surveillance testing.

The next failure category defined by Section 4.0 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 specific system applications and are considered low-probability events. The remaining failures are either common cause hardware failures or software errors. These types of multiple failure scenarios are typically considered to be a small percentage of the total failures. The reliability analysis referenced in Section 5.8 uses a common cause Beta factor of 1 %. This Beta factor is typical of the factor used in process industry safety systems.

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 29 of 61 | Date: | 05/23/07 |

The final failure category defined by Section 4.0 is Category C4a & C4b, which includes 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.

With the TRICON system, the Safe Undetected Failure Rate, on average account for about 0.7% of the Total Failure Rate. The Dangerous Undetected Failure Rate, on average account for about 0.5% of the Total Failure Rate. The undetected failure rate data is very small as a result of TRICON’s high Diagnostic Coverage, which is around 95% and above. This coverage enabled the majority of system failures to fall in the safe category. The Safe Failure Fraction average is about 99%. Furthermore, because of the TRICON’s TMR architecture, it will need to have two undetected failures to get to the final fail-to-function state. (Refer to the Fail-to-Function Markov Model in the Reliability/ Availability Study document (See Section 5.8)). Any detected failure will be fixed at a given on-line repair rate (24 hours in the reliability/ availability study). This allows for the system to run in applications that require PFDavg in the range 10^{-4} to 10^{-3} .

The Safety Availability of the TRICON-UNDER-TEST MODULE configuration (Reference 5.1) is over 99.99% and exceeds the EPRI requirement of 99%. The Overall Availability of the TRICON-UNDER-TEST MODULE configuration is also over 99.99% and also exceeds the EPRI requirement of 99 %.

As stated in Section 4.0 of this report, the PLC 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, described in References 5.5 and 5.6 and summarized in Section 6.0 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 coverages 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 5.8 shows the failure rates and diagnostic coverages of the TRICON Main Processors and I/O modules.

The TRICON system design information presented in References 5.5 and 5.6 includes recommendations for periodic off-line testing of field inputs and outputs. These

| | | | | | |
|------------------|--------------|---------------|---|--------------|----------|
| Document: | 96000164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 30 of 61 | Date: | 05/23/07 |

recommendations establish general surveillance techniques and surveillance intervals intended to maintain the high reliability of the overall control system. It is strongly recommended that specific nuclear plant safety-related applications incorporate the specified methods and frequencies of Reference 5.5 and 5.6 to maximize system reliability and operability.

8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR THE TRICON V10.2

It should be noted that 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. Hence the C2a and C2b categories are not shown since the percent of undetected failures is so small.

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.

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 31 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|---|-------------------------|--|---|
| 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 3008; 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. | PLC fails to operate |
| 2) Main Chassis Processor Module: Model 3008; Enhanced TRICON Main Processor, 16 Mbytes DRAM | Loss of one or two processor modules | Electronics or software failure | C1a, C1b, C4a, C4b | None | PLC continues to operate via intact processor module(s). Main processor diagnostics will detect and flag processor fault. See Sec. 6.3. |
| 3) Main Chassis Communications Module: Model 4352A, TRICON Communication Module (TCM) | Failure of module to transmit or receive data on all three legs | Electronics or software failure | C1a, C1b | If safety related data is being transmitted, the receiving Main Processor will assume the data should be set to the fail safe state and put devices dependent on the data into a safe state. | PLC continues to operate. Communications to external network devices is interrupted. Main processor diagnostics will detect and flag communications fault if application software is so designed. Requires application-specific alarming in the external system. See Sec. 6.4.1. A faulty TCM module can be replaced while the controller is online. |
| 4) Main Chassis Communications Module: Model 4352A, TRICON Communication Module (TCM) | Failure of com module to communicate with one or two of the Main Processor.. | Electronics or software failure | C1a, C1b | None | Third leg will still communicate with the MP. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 32 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--------------------------------|---|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| CONTROL AND COMMUNICATIONS MODULE-RELATED FAILURES (CONTINUED) | | | | | |
| 5) Model 4200-3; Primary 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. | 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 RXM communications fault. See Sec. 6.4.2. |
| 6) Model 4200-3; Primary Remote Extender Module (RXM), Multi-mode Fiber Optics (set of 3 modules) | Loss of one or two RXM modules | Electronics or software failure | C1a, C1b, C4a, C4b | None | PLC continues to operate via intact RXM module(s). Main processor diagnostics will detect and flag RXM module fault. See Sec. 6.4.2. |
| 7) Model 4201-3; 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. | 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 RXM communications fault. See Sec. 6.4.2. |
| 8) Model 4201-3; Remote Extender Module (RXM), Multi-mode Fiber Optics (set of 3 modules) | Loss of one or two RXM modules | Electronics or software failure | C1a, C1b, C4a, C4b | None | PLC continues to operate via intact RXM module(s). Main processor diagnostics will detect and flag RXM module fault. See Sec. 6.4.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 33 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|---|--|--|---|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC I/O MODULE-RELATED FAILURES | | | | | |
| 1) Digital input modules: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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 | PLC continues operation. If point is normally OFF, then condition will only be detected for Model 3504E DI module, which includes Stuck Off diagnostic capability. See Sec. 6.1.1. |
| 2) Digital input modules: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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 | PLC unable to correctly determine the state of the affected point(s). If point is normally OFF, then condition will only be detected for Model 3504E DI module, which includes Stuck Off diagnostic capability. See Sec. 6.1.1. |
| 3) Digital input modules: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 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 3501T if point is normally ON. | None | PLC 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. See Sec. 6.1.1. |
| 4) Digital input modules: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 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 3501T if point is normally ON. | Affected digital input(s) will fail high. | PLC 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. See Sec. 6.1.1. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 34 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|---|---|---|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC I/O MODULE-RELATED FAILURES (CONTINUED) | | | | | |
| 5) Digital input modules: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc | Common processing failure on one or two legs. | Electronic component failure(s) | C1a, C1b | None | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.1. |
| 6) Digital input modules: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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. | PLC will treat 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. See Sec. 6.1.1. |
| 7) Digital output modules: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | Output point fails high or low on one leg | Electronic component failure | C1a, C1b | None | PLC continues operation. DO module OVD diagnostics will detect the fault on all modules except for the 3601E if the output point is not being toggled periodically. See Sec. 6.2.1. |
| 8) Digital output modules: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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. | PLC 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 3601E. See Sec. 6.2.1. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 35 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|---|-------------------------|---|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC I/O MODULE-RELATED FAILURES (CONTINUED) | | | | | |
| 9) Digital output modules: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | Common processing failure on one or two legs | Electronic component failure(s) | C1a, C1b | None | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.1. |
| 10) Digital output modules: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | Common processing failure on all legs | Multiple electronics failures or comm. software failure | C3b | Affected output points will go OFF. | PLC 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. See Sec. 6.2.1. |
| 11) Supervised digital output modules: Model 3623T; 120 Vac Model 3625; 24 Vdc | Output point fails high or low on one leg. | Electronic component failure | C1a, C1b | None | PLC continues operation. SDO module OVD diagnostics will detect the fault . See Sec. 6.2.2. |
| 12) Supervised digital output modules: Model 3623T; 120 Vac Model 3625; 24 Vdc | 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. | PLC unable to control the affected output point(s). Condition will be detected by SDO OVD diagnostics. Module, Load or Power alarm will be asserted based upon specific fault scenario. See Sec. 6.2.2. |
| 13) Supervised digital output modules: Model 3623T; 120 Vac Model 3625; 24 Vdc | Common processing failure on one or two legs | Electronic component failure(s) | C1a, C1b | None | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 36 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|---|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC I/O MODULE-RELATED FAILURES (CONTINUED) | | | | | |
| 14) Supervised digital output modules: Model 3623T; 120 Vac Model 3625; 24 Vdc | Common processing failure on all legs | Multiple electronics failures or comm. software failure | C3b | Affected output points will go OFF. | PLC 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. See Sec. 6.2.2. |
| 15) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | Input point fails high or low on single leg | Electronic component failure | C1a, C1b | None | 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. See Sec. 6.1.3 |
| 16) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | 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. | PLC 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. See Sec. 6.1.3 |
| 17) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | Common processing failure on one or two legs | Electronic component failure(s) | C1a, C1b | None | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.3. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 37 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|--|-------------------------|---|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC I/O MODULE-RELATED FAILURES (CONTINUED) | | | | | |
| 18) Analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | Common processing failure on all legs | Multiple electronics failures or comm. software failure | C3b | Affected input points will go downscale. | PLC will treat all affected input points as downscale. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.3. |
| 19) 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 | 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. Failure of all three legs for a given output will activate the Load Indicator, and output will not be driven. See Sec. 6.2.4. |
| 20) 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. | PLC 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. See Sec. 6.2.4. |
| 21) Analog output module: Model 3805E; 4-20ma | Common processing failure on one or two legs | Electronic component failure(s) | C1a, C1b | None | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.4. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 38 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|---|-------------------------|--|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC I/O MODULE-RELATED FAILURES (CONTINUED) | | | | | |
| 22) 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. | PLC 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. See Sec. 6.2.4. |
| 23) 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. | PLC 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. Module not intended for safety-related applications. See Sec. 6.2.3. |
| 24) Relay output module: Model 3636T; Relay Output | Common processing failure on one or two legs | Electronic component failure(s) | C1a, C1b, C2a, C2b | None | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. Module not intended for safety-related applications. See Sec. 6.2.3. |
| 25) 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. | PLC 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. Module not intended for safety-related applications. See Sec. 6.2.3. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 39 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|---|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC I/O MODULE-RELATED FAILURES (CONTINUED) | | | | | |
| 26) Pulse input module: Model 3511; 8 pulse input | Input point fails high or low on single leg | Electronic component failure | C1a, C1b | None | 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. See Sec. 6.1.2 |
| 27) Pulse input module: Model 3511; 8 pulse input | Input point fails high or low on multiple legs | Multiple electronic component failures | C3b | Affected inputs will fail to the corresponding input state. | PLC 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. See Sec. 6.1.2 |
| 28) Pulse input module: Model 3511; 8 pulse input | Common processing failure on one or two legs | Electronic component failure(s) | C1a, C1b | None | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.2. |
| 29) Pulse input module: Model 3511; 8 pulse input | Common processing failure on all legs | Multiple electronics failures or comm. software failure | C3b | Affected input points will go downscale. | PLC will treat all affected input points as downscale. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.1.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 40 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--------------------------------------|-------------------------|--|---|
| 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 | Facility blackout | C3b | Input signals will not be read. Analog and digital outputs fail low. | PLC fails to operate |
| 2) All chassis power supplies: | Power supply output fails high | Electronic component or fuse failure | N/A | None | PLC 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. See Sec. 6.6. |
| 3) Main Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac | Loss of one power supply output | Electronic component or fuse failure | C1a, C1b | None | PLC 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. See Sec. 6.6. |
| 4) Main Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac | 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 | PLC fails to operate. |
| 5) RXM or Expansion Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac | Loss of one power supply output | Electronic component or fuse failure | C1a, C1b | None | PLC continues operation via redundant RXM/Expansion chassis power supply. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.6. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 41 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--------------------------------------|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| POWER SUPPLY-RELATED FAILURES (CONTINUED) | | | | | |
| 6) RXM or Expansion Chassis power supply: Model 8310; 120Vac/Vdc Model 8311; 24Vdc Model 8312; 230Vac | Power supply outputs fail (both power supplies fail) | Electronic component or fuse failure | C3b | All outputs fail low on all modules in affected chassis. | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.6 |
| 7) Loop power supply for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc | power supply output voltage fails low (both power supplies fail) | Fire; flood; missile | C3b | Affected digital inputs will fail low | PLC 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). See Sec. 6.1.1. |
| 8) Loop power supply for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 24 Vac/Vdc | power supply output voltage fails low (one power supply fails) | Electronic component or fuse failure | C1a, C1b, C2a, C2b | None | PLC 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). See Sec. 6.1.1. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 42 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|---|---|--|-------------------------|--|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| POWER SUPPLY-RELATED FAILURES (CONTINUED) | | | | | |
| 9) Loop power supply for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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 | PLC 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. See Sec. 6.1.1. |
| 10) Loop power supply for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | Power supply output voltage fails low (both DC power supplies fail) | Electronic component or fuse failure | C3b | Affected digital outputs will fail low | PLC 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. See Sec. 6.2.1. |
| 11) Loop power supply for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | Power supply output voltage fails low (One power supply fails) | Electronic component or fuse failure | C1a, C1b, C2a, C2b | None | PLC 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). See Sec. 6.1.1. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 43 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|---|--|--------------------------------------|-------------------------|---|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| POWER SUPPLY-RELATED FAILURES (CONTINUED) | | | | | |
| 12) Loop power supply for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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 | PLC continues operation. Main processor diagnostics will detect and flag board fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.1. |
| 13) Loop power supply for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | Power supply output voltage fails low (both power supplies fail) | Electronic component or fuse failure | C3b | Affected digital outputs will fail low | PLC continues operation. Loss of power will be detected by SDO circuitry, which will generate a Power Alarm and/or a Load Alarm. See Sec. 6.2.2. |
| 14) Loop power supply for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | Power supply output voltage fails low (one power supply fails) | Electronic component or fuse failure | C1a, C1b, C2a, C2b | None | PLC 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). See Sec. 6.1.1. |
| 15) Loop power supply for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | 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 | PLC continues operation. Loss of power will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 44 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--------------------------------------|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| POWER SUPPLY-RELATED FAILURES (CONTINUED) | | | | | |
| 16) Loop power supply for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | Power supply output voltage fails low (both power supplies fail) | Electronic component or fuse failure | 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. See Sec. 6.1.3. |
| 17) Loop power supply for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | Power supply output voltage fails low (one power supply fails) | Electronic component or fuse failure | C1a, C1b, C2a, C2b | None | 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. See Sec. 6.1.3. |
| 18) Loop power supply for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | 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 | 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. See Sec. 6.1.3. |
| 19) Loop power supply for analog output module: Model 3805E; 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) | 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. See Sec. 6.2.4. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 45 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--------------------------------------|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| POWER SUPPLY-RELATED FAILURES (CONTINUED) | | | | | |
| 20) Loop power supply for analog output module: Model 3805E; 4-20ma | Power supply output voltage fails low (one power supply fails) | Electronic component or fuse failure | C1a, C1b, C2a, C2b | None | 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. See Sec. 6.2.4. |
| 21) Loop power supply for analog output module: Model 3805E; 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 | 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. See Sec. 6.2.4. |
| 22 Loop power supply for relay output module: Model 3636T; Relay Output The Relay Output Module is not used for safety applications. I believe it should be removed from FMEA. | 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 | PLC 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. Module not intended for safety-related applications. See Sec. 6.2.3. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 46 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--------------------------------------|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| POWER SUPPLY-RELATED FAILURES (CONTINUED) | | | | | |
| 23) 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 | PLC 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. Module not intended for safety-related applications. See Sec. 6.2.3. |
| 24) 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. Module not intended for safety-related applications. See Sec. 6.2.3. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 47 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|--|-------------------------|--|---|
| 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 keyswitch | Switch shorts or is closed to “STOP” position | Electrical power transient; fire; flood; missiles | C3b | Input signals will not be read. Analog and digital outputs fail low. | PLC fails to operate. STOP position shall be software-disabled per the Software Qualification Report. Multiple wafer switch, with switch state voted in MP. Credible single failures will be voted out. |
| 2) 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. |
| 3) 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. See Sec. 6.6. |
| 4) 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 |
| 5) 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. See Sec. 6.3. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 48 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--|-------------------------|--|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CHASSIS-RELATED FAILURES CONTINUED) | | | | | |
| 6) 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. See Sec. 6.3. |
| 7) 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. See Sec. 6.3. |
| 8) 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). See Sec. 6.3. |
| 9) 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. See Sec. 6.3. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 49 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CHASSIS-RELATED FAILURES (CONTINUED) | | | | | |
| 10 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. See Sec. 6.3. |
| 11) 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. See Sec. 6.6. |
| 12) RXM or Expansion 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 or Expansion 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. See Sec. 6.6 |
| 13) RXM or Expansion 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/Expansion chassis power supply. Main processor diagnostics will detect and flag power rail fault. Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.6. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 50 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|--|--|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CHASSIS-RELATED FAILURES CONTINUED) | | | | | |
| 14) RXM or Expansion 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 or Expansion chassis as noted, and all downstream chassis assemblies. Main processor diagnostics will detect and flag I/O bus fault. See Sec. 6.4.2. |
| 15) RXM or Expansion 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. See Sec. 6.4.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 51 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|--|-------------------------|---|--|
| 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. See Sec. 6.4.2. |
| 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. See Sec. 6.4.2. |
| 3 RXM Chassis-to-Expansion 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. See Sec. 6.4.2. |
| 4) RXM Chassis-to-Expansion 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. See Sec. 6.4.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 52 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|---|-------------------------|--|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CABLE-RELATED FAILURES (CONTINUED) | | | | | |
| 5) Main Chassis Communications Module: Model 4352A, 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. See Sec. 6.4.1. |
| 6) Model 4200-3; Primary Remote Extender Module (RXM) to Model 4201-3; Remote Extender Module, 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. See Sec. 6.4.2. |
| 7) Model 4200-3; Primary Remote Extender Module (RXM) to Model 4201-3; Remote Extender Module, 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. See Sec. 6.4.2. |
| 8) Chassis to termination cable for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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. See Sec. 6.1.1. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 53 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|-------------------------------|---|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CABLE-RELATED FAILURES (CONTINUED) | | | | | |
| 9) Chassis to termination cable for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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. See Sec. 6.1.1. |
| 10) Chassis to termination cable for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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. See Sec. 6.1.1. |
| 11) Chassis to termination cable for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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. See Sec. 6.2.1. |
| 12) Chassis to termination cable for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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. See Sec. 6.2.1. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 54 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|-------------------------|---|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CABLE-RELATED FAILURES (CONTINUED) | | | | | |
| 13) Chassis to termination cable for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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. See Sec. 6.2.1. |
| 14) Chassis to termination cable for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | Open circuit | Fault in adjacent power cable; cable cut; fire; flood; missiles | C3a | PLC digital outputs will not be affected, but field devices will fail low | PLC continues operation. Loss of field loops will be detected by SDO circuitry, which will generate a Power Alarm and/or a Load Alarm. See Sec. 6.2.2. |
| 15) Chassis to termination cable for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | Short circuit to ground | Fault in adjacent power cable; fire; flood; missiles | C3a | Affected digital outputs will fail low | PLC continues operation. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2. |
| 16) Chassis to termination cable for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | 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. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 55 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|---|---|---|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CABLE-RELATED FAILURES (CONTINUED) | | | | | |
| 17) Chassis to termination cable for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | 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. See Sec. 6.1.3. |
| 18) Chassis to termination cable for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | 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. See Sec. 6.1.3. |
| 19) Chassis to termination cable for analog output module: Model 3805E; 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. See Sec. 6.2.4. |
| 20) Chassis to termination cable for analog output module: Model 3805E; 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. See Sec. 6.2.4. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 56 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|---|-------------------------|---|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CABLE-RELATED FAILURES (CONTINUED) | | | | | |
| 21) Chassis to termination 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. Module not intended for safety-related applications. See Sec. 6.2.3. |
| 22) Chassis to termination 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. Module not intended for safety-related applications. See Sec. 6.2.3. |
| 23) Chassis to termination cable for pulse input module: Model 3510; 8 pulse input Model 3511; 8 pulse input | Open circuit or short circuit to ground | Fault in adjacent power cable; cable cut; fire; flood; missiles | C3a | Affected pulse inputs will fail low | PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2. |
| 24) Chassis to termination cable for pulse input module: Model 3511; 8 pulse input | Hot short | Fault in adjacent power cable | C3a | Affected pulse inputs may fail low; assuming failure voltage is high enough to burn out field devices (application-specific failure). | PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2. |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 57 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|---|-------------------------|--|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| PLC CABLE-RELATED FAILURES (CONTINUED) | | | | | |
| 25) Combined I/O bus of various chassis – Expansion to Expansion, Main to Expansion, Main to RXM, RXM to Expansion | Open/short on all three busses | Fault in adjacent power cable; cable cut; fire; flood; missiles | C1a, C1b, C3b | Unable to transmit signals to the I/O modules on faulted busses. | Set the outputs to fail safe mode. |
| TERMINATION PANEL-RELATED FAILURES | | | | | |
| 1) Termination panel for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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. See Sec. 6.1.1. |
| 2 Termination panel for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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. See Sec. 6.1.1. |
| 3) Termination panel for digital inputs: Model 3501T; 115 Vac/Vdc Model 3502E; 48 Vac/Vdc Model 3503E; 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. See Sec. 6.1.1. |
| TERMINATION PANEL-RELATED FAILURES (CONTINUED) | | | | | |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 58 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|-------------------------|--|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| 4) Termination panel for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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. See Sec. 6.2.1. |
| 5) Termination panel for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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. See Sec. 6.2.1. |
| 6) Termination panel for digital outputs: Model 3601T; 115 Vac Model 3603T; 120 Vdc Model 3607E; 48 Vdc Model 3625; 24 Vdc | 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. See Sec. 6.2.1. |
| 7) Termination panel for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | Open circuit | Fire; flood; missiles; term panel fuse failure | C3a, C3b | PLC digital outputs will not be affected, but field devices will fail low | PLC continues operation. Loss of field loops will be detected by SDO circuitry, which will generate a Power Alarm and/or a Load Alarm. See Sec. 6.2.2. |
| TERMINATION PANEL-RELATED FAILURES (CONTINUED) | | | | | |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 59 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|---|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| 8) Termination panel for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | Short circuit to ground | Fire; flood; missiles or cable fault; term panel short | C3a, C3b | Affected digital outputs will fail low | PLC continues operation. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2. |
| 9) Termination panel for supervised digital outputs: Model 3623T; 120 Vac Model 3625; 24 Vdc | 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. Fault will be detected by SDO circuitry, which will generate a Fault alarm via Main Chassis Power Module alarm circuit. See Sec. 6.2.2. |
| 10) Termination panel for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | 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. See Sec. 6.1.3. |
| 11) Termination panel for analog input modules: Model 3701; 0-10 Vdc Model 3703E; 0-5, 0-10 Vdc Model 3704E; 0-5, 0-10 Vdc Model 3721; 0-5/-5 to +5 Vdc Model 3708E, Thermocouple | 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. See Sec. 6.1.3. |
| TERMINATION PANEL-RELATED FAILURES (CONTINUED) | | | | | |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 60 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|---|-------------------------|---|---|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| 12 Termination panel for analog output module: Model 3805E; 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. See Sec. 6.2.4. |
| 13) Termination panel for analog output module: Model 3805E; 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. See Sec. 6.2.4. |
| 14) Termination panel for relay output module: 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. Module not intended for safety-related applications. See Sec. 6.2.3. |
| 15) Termination panel 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. Module not intended for safety-related applications. See Sec. 6.2.3. |
| TERMINATION PANEL-RELATED FAILURES (CONTINUED) | | | | | |

| | | | | | |
|------------------|-------------|---------------|---|--------------|----------|
| Document: | 9600164-531 | Title: | FAILURE MODES AND EFFECTS ANALYSIS | | |
| Revision: | 0 | Page: | 61 of 61 | Date: | 05/23/07 |

| SECTION 8.0 FAILURE MODES AND EFFECTS ANALYSIS FOR TRICON V10.2 TMR PROGRAMMABLE LOGIC CONTROLLER | | | | | |
|--|---|-------------------------------|-------------------------|---|--|
| Affected Components | Failure Mode | Failure Mechanism | Failure Category | Effect on PLC Inputs and Outputs | Effect on PLC Operability |
| 16) Termination panel for pulse input module: Model 3511; 8 pulse input | Open circuit or short circuit to ground | Fire; flood; missiles | C2a, C2b, C3b | Affected pulse inputs will fail low | PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2. |
| 17) Termination panel for pulse input module: Model 3511; 8 pulse input | Hot short | Fault in adjacent power cable | C2a, C2b, C3a | Affected pulse inputs may fail low; assuming failure voltage is high enough to burn out field devices (application-specific failure). | PLC continues operation. Condition will not be detected unless: (a) PI point failures triggered alarms associated with controlled parameters; or (b) by periodic channel checks or surveillance testing. See Sec. 6.1.2. |