invensys™
TRICONEX®

TRICONEX PRODUCTS – INVENSYS PROCESS SYSTEMS

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 TCXNRC-09-01, Affidavit, Section 4.)

RELIABILITY / AVAILABILITY STUDY FOR THE TRICON VERSION 10 PROGRAMMABLE LOGIC CONTROLLER

9600164-532

Revision 0

May 23, 2007

	Name	Signature	Title
Author:	Wolfgang Sinocruz	Wolfgang Sinocruz	Hardware Engineer
Contributor:	Anton Frederickson	Anton Frederickson	R&D Engineer
Reviewer:	Les Powers	Les Powers	Independent Review Engineer
	Frank Kloer		Project Engineer
	Ted Porfilio		Project QA Engineer
Approvals:	Naresh Desai		Product Manager

Revision History

Revision	Date	Description	Author
0	05/23/07	Initial issue.	Wolfgang Sinocruz

Table of Contents

1. Purpose

The purpose of this calculation is to document a reliability/availability study of the TRICON VERSION 10 PLC controller for use in nuclear safety-related applications. The reliability study is performed to meet the requirements of Section 4.2.3 of Reference 1.

2. Results

A TRICON VERSION 10 PLC using a combination of modules specified in Reference 1 is analyzed for reliability and availability using Markov models of the system. For a one-year periodic test interval, the mean time to failure due to a spurious trip (MTTFspurious) is 310.2 years resulting in an overall availability of 99.9991%. For the same test interval, the average probability of failure on demand (PFDavg) is 6.577 x 10^{-6} resulting in a Safety Availability of 99.9993%. Detailed results for different periodic test intervals are presented in Tables 4-2 and 4-4. Both the Overall and the Safety Availabilities determined for the TRICON TMR PLC are greater than the recommended Goal of 99% per Reference 1.

Appendix C examines the reliability of the TRICON TMR PLC for a two-week period in a post accident environment. In the post accident period, the overall availability is 99.9506%, and the safety availability is 99.9982%. As before, both of these results exceed the recommended goal of 99% as stated in Reference 1.

3. Approach

The TRICON TMR PLC is a programmable logic controller that can accept input signals, make appropriate decisions with a main processor, and send output signals. The input and output signals can be analog or discrete digital. The PLC is modular, meaning that each of the functions are performed by various types of cards which are plugged into the main chassis of the system. Consequently, one TRICON TMR PLC can have any number of configurations. Each module of the TRICON TMR PLC has at least 3-2-0 redundancy meaning that one channel can be lost and the module still functions properly.

The TRICON TMR PLC can be used to replace analog reactor protection or engineered safety features actuation systems in nuclear power plants. The input modules can accept input from current plant wiring, the main processor would replace the current analog and discrete logic circuits, and the output modules can generate signals comparable to the current relays. Because these systems are critical to the safe operation of the reactor, the replacement digital PLC must have a high degree of reliability and availability.

EPRI TR-107330 (Reference 1) has been written to specify generic requirements for qualifying

PLCs for safety-related applications in nuclear plants. This calculation addresses the requirements specified in Section 4.2.3 of Reference 1 regarding the reliability and availability requirements for PLCs.

For all nuclear plant applications, one TRICON TMR PLC is used for each channel of a safety system. Losing two redundant legs inside the triple redundant TRICON does not necessarily lead to a system failure. Therefore, the reliability evaluations performed in this calculation assuming the TRICON TMR PLC only has 3-2-0 redundancy are very conservative for the actual applications in nuclear plant safety systems. It should also be noted that this calculation does not address software common cause failures.

3.1.System Configuration Analyzed

Per the Master Configuration List in Reference 7, the system in the following table is representative of the full range of components of the PLC. The TRICON TMR PLC modules used to comply with the EPRI guidelines are also shown in the table. For cases where more than one type of TRICON module meets the EPRI component type, the TRICON module with the highest failure rate is chosen for evaluation. An additional analog type module was added to show the differences between the pulse input module and the other analog module types.

Table 3-1. TRICON Modules

EPRI Section	Component Type	Range of TRICON Modules
4.2.3.2.A	3 Discrete Input Modules	3501T, 3502E, 3503E
4.2.3.2.B	3 Analog Input Modules	3511 (pulse input), 3701, 3703E, 3721, 3708E (thermocouple)
4.2.3.2.C	1 Analog Output Module	3805E
4.2.3.2.D	3 Discrete Output Modules	3601T, 3603T, 3607E, 3623T, 3625
	1 Relay Output Module	Not included in TRICON TMR for safety applications
4.2.3.2.E	1 High-level Language Module	Included in main processor
4.2.3.2.F	Support Module	(Note 1)
4.2.3.2.G	Ancillary Devices	Not required for TRICON TMR
4.2.3.2.H	Main Processor (3 required)	3008
4.2.3.2.1	Power Supply	8310, 8311, 8312
4,2.3.2.J	4 Chassis	Main, Expansion , and 2 RXM Chassis
4.2.3.2.K	Interconnect Devices	Not required for TRICON TMR
4.2.3.2.L	Modules necessary for redundancy	Not required for TRICON TMR

4.2.3.2.M	Ringback signals	Included in Input/Output Modules

Note 1: Support modules are not necessary for normal operation of the TRICON TMR. A communication module is required to reconfigure the system.

3.2. Markov Model for Safe Failures

Both the availability and the safety availability can be determined from a Markov model of the TRICON TMR PLC in the configuration described above. A Markov model uses a state diagram of various failure states of the system. From this model, the probability to be in any one state at a given time can be predicted. Using the combined probabilities of various failed states the mean time to failure due to a spurious trip (MTTF) and the probability of failure on demand (PFD) can be calculated for the system. These quantities are directly related to the availability and the safety availability.

Failures can be generally classified into two categories: safe and dangerous. Safe failures are failures that result in the safety system failing into a safe configuration. For example, most safety systems including the TRICON TMR are designed to actuate upon complete failure of both power supplies. Dangerous failures are failures that result in the system failing to perform its intended safety function. Each category of failure can be further classified into dangerous detected and undetected failures. Detected failures can be repaired on-line. Undetected failures are only detected and repaired during off-line periodic testing.

3.2.1. *Model Description for Safe Failures*

The Markov model for a safe spurious trip is shown in Figure 3-1. Note that this figure is developed using the methodology described in Reference 5.

The TRICON TMR is a fail safe PLC with triplicated inputs (3-2-0), triple redundant main processor with communication, and a quad output voter. As required by Reference 1, the Markov model includes the main processor, a digital input module, an analog input module, a digital output module, and an analog output module. Along with each input/output microprocessor, the Markov model includes each input/output circuit. Also included is the dual power supply.

The first state in the Markov model is the system operating normally with no failures. The intermediate states are when one channel of the various modules fail. The last state is when a second failure causes the system to trip spuriously. The probability of moving from one state to another (i.e., probability of failure or repair) are shown by the arrows. Note that constant failure and repair rates are assumed. Also time steps are assumed to be short so that the probability function can be estimated as shown below:

$$P(t) = 1 - e^{-\lambda t} \quad \approx \quad \lambda t$$

Each intermediate failure state is described below. All equations and transition coefficients are taken from the fail safe Markov model for a triplicated PLC with a quad output voter developed in Draft 12 of ISA SP.84.02 (see Reference 5).

States 1 and 2 - Digita1 Input

Each digital input model is triplicated with 3-2-0 capability. Each module consists of three triplicated legs. State 1 is the safe failure of one of the digital input microprocessor modules. State 2 is the safe failure of one of the digital input circuits to an input module. The transitions from the initial state to the intermediate states representing an initial failure of one of three input micro processors or input circuits are given by:

$$\boldsymbol{\lambda 1} = 3*n*\text{FR\_IP\_S}$$
$$\boldsymbol{\lambda 2} = 3*n*nic*\text{FR\_IC\_S}$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{1E}$$
$$\mu_{2E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\boldsymbol{\theta 1} = 2*(\text{FR\_MP\_S} + \text{FR\_I\_S})$$
$$\boldsymbol{\theta 2} = 2*(\text{FR\_MP\_S} + \text{FR\_IP\_S} + \text{FR\_IC\_S})$$

States 3 and 4 – High Density Digita1 Input

Each high density digital input model is triplicated with 3-2-0 capability. Each module consists of three triplicated legs. State 3 is the safe failure of one of the digital input microprocessor modules. State 4 is the safe failure of one of the digital input circuits to an input module. The transitions from the initial state to the intermediate states representing an initial failure of one of three input micro processors or input circuits are given by:

$$\boldsymbol{\lambda 3} = 3*nhd*\text{FR\_HDIP\_S}$$
$$\boldsymbol{\lambda 4} = 3*nhd*nhdic*\text{FR\_HDIC\_S}$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{3E}$$
$$\mu_{4E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\theta 3 = 2*(FR\_MP\_S + FR\_HDI\_S)$$
$$\theta 4 = 2*(FR\_MP\_S + FR\_HDIP\_S + FR\_HDIC\_S)$$

States 5 and 6 - Analog Input

Each analog input model is triplicated with 3-2-0 capability. Each module consists of three triplicated legs. State 5 is the safe failure of one of the analog input microprocessor modules. State 6 is the safe failure of one of the analog input circuits to an input module. The transitions from the initial state to the intermediate states representing an initial failure of one of three input micro processors or input circuits are given by:

$$\lambda 5 = 3*na*FR\_AIP\_S$$
$$\lambda 6 = 3*na*nic*FR\_AIC\_S$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{5E}$$
$$\mu_{6E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\theta 5 = 2*(FR\_MP\_S + FR\_AI\_S)$$
$$\theta 6 = 2*(FR\_MP\_S + FR\_AIP\_S + FR\_AIC\_S)$$

States 7 and 8 – High Density Analog Input

Each high density analog input model is triplicated with 3-2-0 capability. Each module consists of three triplicated legs. State 7 is the safe failure of one of the analog input microprocessor modules. State 8 is the safe failure of one of the analog input circuits to an input module. The transitions from the initial state to the intermediate states representing an initial failure of one of three input microprocessors or input circuits are given by:

$$\lambda\mathbf{7} = 3*\text{nahd}*\text{FR\_HDAIP\_S}$$

$$\lambda\mathbf{8} = 3*\text{nahd}*\text{nhdic}*\text{FR\_HDAIC\_S}$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{7E}$$

$$\mu_{8E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\theta\mathbf{7} = 2*(\text{FR\_MP\_S} + \text{FR\_HDAI\_S})$$

$$\theta\mathbf{8} = 2*(\text{FR\_MP\_S} + \text{FR\_HDAIP\_S} + \text{FR\_HDAIC\_S})$$

States 9 and 10 – 16 point Isolated Analog Input

Each isolated analog input model is triplicated with 3-2-0 capability. Each module consists of three triplicated legs. State 9 is the safe failure of one of the analog input microprocessor modules. State 10 is the safe failure of one of the analog input circuits to an input module. The transitions from the initial state to the intermediate states representing an initial failure of one of three input microprocessors or input circuits are given by:

$$\lambda\mathbf{9} = 3*\text{niai}*\text{FR\_IAIP\_S}$$

$$\lambda\mathbf{10} = 3*\text{niai}*\text{niaic}*\text{FR\_IAIC\_S}$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{9E}$$

$$\mu_{10E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\theta\mathbf{9} = 2*(\text{FR\_MP\_S} + \text{FR\_IAI\_S})$$

$$\theta\mathbf{10} = 2*(\text{FR\_MP\_S} + \text{FR\_IAIP\_S} + \text{FR\_IAIC\_S})$$

States 11 - Analog Output

Each analog output module is triplicated with 3-2-1-0 capability. Each analog output leg can vote to drive 3 analog output devices for each analog output point. Hence three safe failures of the analog output devices must occur before an analog output point has a safe failure. Since the probability of safe failure for an analog output point is third order (~ λ^3), its effect on the mean time to failure can be neglected. Hence only the safe failure of the analog output microprocessors affects the safe failure of the module.

$$\mathbf{\lambda 11} = 3*ma*FR\_AOP\_S$$

$$\mathbf{\theta 11} = 2*(FR\_MP\_S + FR\_AOP\_S)$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure is given by:

$$\mu_{11E}$$

States 12 – Not used

States 13 and 14 – 24 VDC Digital Output

Each 24 VDC digital output module has a triplicated output processor with a quad voter output circuit. State 13 is the safe failure of one of the digital output microprocessor modules. State 14 is the safe failure of one of the digital output circuits. The transitions from the initial state to the intermediate states are given by:

$$\mathbf{\lambda 13} = 3*m*FR\_OP\_S$$

$$\mathbf{\lambda 14} = 4*m*nhdoc*FR\_OC\_S$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{13E}$$

$$\mu_{14E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\mathbf{\theta 13} = 2*(FR\_MP\_S + FR\_OP\_S) + 5/3*nhdoc*FR\_OC\_S$$

$$\mathbf{\theta 14} = 5/4*(FR\_MP\_S + FR\_OP\_S) + FR\_OC\_S$$

States 15 and 16 – 115 VAC Digital Output

Each 115 VAC digital output module has a triplicated output processor with a quad voter output circuit. State 15 is the safe failure of one of the digital output microprocessor modules. State 16 is the safe failure of one of the digital output circuits. The transitions from the initial state to the intermediate states are given by:

$$\boldsymbol{\lambda 15} = 3*\mathrm{mhv}*\mathrm{FR\_HVOP\_S}$$

$$\boldsymbol{\lambda 16} = 4*\mathrm{mhv}*\mathrm{noc}*\mathrm{FR\_HVOC\_S}$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{15E}$$

$$\mu_{16E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\boldsymbol{\theta 15} = 2*(\mathrm{FR\_MP\_S} + \mathrm{FR\_HVOP\_S}) + 5/3*\mathrm{noc}*\mathrm{FR\_HVOC\_S}$$

$$\boldsymbol{\theta 16} = 5/4*(\mathrm{FR\_MP\_S} + \mathrm{FR\_HVOP\_S}) + \mathrm{FR\_HVOC\_S}$$

States 17 – Main Processor

There are triple redundant main processors. State 17 is the safe failure of one of the three main processors. The transition from the initial state to the intermediate state is given by:

$$\boldsymbol{\lambda 17} = 3*\mathrm{FR\_MP\_S}$$

The transition from the intermediate state to the initial state representing the repair of the initial failure is given by:

$$\mu_{17E}$$

The transition from the intermediate state to a spurious trip representing a safe failure of any one of the circuits in the other two channels is:

$$\boldsymbol{\theta 17} = 2*(FR\_MP\_S + n*FR\_I\_S + nhd*FR\_HDI\_S + na*FR\_AI\_S + nahd*FR\_HDAI\_S + niai*FR\_IAI\_S + ma*FR\_AOP\_S + m*FR\_O\_S + mhv*FR\_HVO\_S + np*FR\_PI\_S)$$

State 18 – Power Supply

State 18 is the safe failure of one of the dual power supplies in a channel. The transition from the initial state to the intermediate state is given by:

$$\boldsymbol{\lambda 18} = 2*l*FR\_PS\_S$$

The transition from the intermediate state to the initial state representing the repair of the initial failure is given by:

$$\mu_{18E}$$

The transition from the intermediate state to a spurious trip representing safe failure of the remaining power supply in the channel is given by:

$$\boldsymbol{\theta 18} = FR\_PS\_S$$

States 19 and 20 - Pulse Input

The transitions from the initial state to the intermediate states representing an initial safe failure of one of three input micro processors or input circuits are given by:

$$\boldsymbol{\lambda 19} = 3*np*FR\_PIP\_S$$
$$\boldsymbol{\lambda 20} = 3*np*npc*FR\_PIC\_S$$

The transitions from the intermediate state to the initial state representing the repair of the initial failure are given by:

$$\mu_{19E}$$
$$\mu_{20E}$$

The transitions from the intermediate state to a spurious trip representing a safe failure in one of the two remaining input channels or main processors are given by:

$$\boldsymbol{\theta 19} = 2*(\mathrm{FR\_MP\_S} + \mathrm{FR\_PI\_S})$$

$$\boldsymbol{\theta 20} = 2*(\mathrm{FR\_MP\_S} + \mathrm{FR\_PIP\_S} + \mathrm{FR\_PIC\_S})$$

Effects of Common Cause Failures

The effects of dual or triple mode safe failure is modeled directly as a transition from the initial state to the spurious trip state. The common cause safe failure transition is given by:

$$\begin{aligned}
\boldsymbol{\lambda 21} = {} & 3*\mathrm{Beta}*(\mathrm{FR\_MP\_S} + n*\mathrm{FR\_I\_S} + nhd*\mathrm{FR\_HDI\_S} + na*\mathrm{FR\_AI\_S} \\
& + nahd*\mathrm{FR\_HDAI\_S} + niai*\mathrm{FR\_IAI\_S} + ma*\mathrm{FR\_AOP\_S} + m*\mathrm{FR\_O\_S} \\
& + mhv*\mathrm{FR\_HVO\_S} + np*\mathrm{FR\_PI\_S}) \\
& + 3*\mathrm{Beta}*\mathrm{ccf3legs}*(\mathrm{FR\_MP\_DD} + n*(\mathrm{FR\_I\_DD}) + nhd*(\mathrm{FR\_HDI\_DD}) \\
& + na*(\mathrm{FR\_AI\_DD}) + nahd*(\mathrm{FR\_HDAI\_DD}) + niai*(\mathrm{FR\_IAI\_DD}) \\
& + m*(\mathrm{FR\_O\_DD}) + mhv*(\mathrm{FR\_HVO\_DD}) + np*(\mathrm{FR\_PI\_DD}) \\
& + ma*(\mathrm{FR\_AOP\_DD})) \\
& + 2*\mathrm{Beta}*l*\mathrm{FR\_PS\_S}
\end{aligned}$$

Note that since the Tricon has three legs, the ccf3legs factor considers the situation where a single failure can commonly affect all three legs of the module.

Where:

Symbol	Description
l	Number of Redundant Power Supply Modules (= Number of Chassis)
m	Number of NG 24 VDC Digital Output Modules
ma	Number of Analog Output Modules
mhv	Number of 115 VAC Digital Output Modules
n	Number of 24 VDC Digital Input Modules
nhd	Number of High Density Digital Input Modules
na	Number of NG Diff. Analog Input Modules
nahd	Number of NG High Density Analog Input Modules
niai	Number of Isolated Analog Input Modules
np	Number of Pulse Input Modules

Symbol	Description
nic	Number of Input Points on Digital Input and Analog Input Modules (32 points)
nhdic	Number of Input Points on High Density Modules (64 points)
niaic	Number of Input Points on Isolated Analog Input Modules (16 points)
noc	Number of Output Points on 115 VAC Digital Output Modules (16 points)
nhdoc	Number of Output Points on NG 24 VDC Digital Output Modules (16 points)
npc	Number of Input Points on Pulse Input Module (8 points)
FR_AI	Failure Rate of an Analog Input Module Leg
FR_AI_DU	Dangerous Undetected Failure Rate of an Analog Input Module Leg
FR_AI_SU	Safe Undetected Failure Rate of an Analog Input Module Leg
FR_AI_S	Safe Failure Rate of an Analog Input Module Leg
FR_AIP_S	Safe Failure Rate of an Analog Input Module Common Processing Circuit
FR_AIC_S	Safe Failure Rate of an Analog Input Circuit
FR_AOP	Failure Rate of an Analog Output Module Leg
FR_AOP_DU	Dangerous Undetected Failure Rate of an Analog Output Module Leg
FR_AOP_SU	Safe Undetected Failure Rate of an Analog Output Module Leg
FR_AOP_S	Safe Failure Rate of an Analog Output Module Common Processing Circuit
FR_HDAI	Failure Rate of a High Density Analog Input Module Leg
FR_HDAI_DU	Dangerous Undetected Failure Rate of a High Density Analog Input Module Leg
FR_HDAI_SU	Safe Undetected Failure Rate of a High Density Analog Input Module Leg
FR_HDAI_S	Safe Failure Rate of a High Density Analog Input Module Leg
FR_HDAIP_S	Safe Failure Rate of a High Density Analog Input Module Common Processing Circuit
FR_HDAIC_S	Safe Failure Rate of a High Density Analog Input Circuit
FR_HDI	Failure Rate of a High Density Digital Input Module Leg
FR_HDI_DU	Dangerous Undetected Failure Rate of a High Density Digital Input Module Leg
FR_HDI_SU	Safe Undetected Failure Rate of a High Density Digital Input Module Leg
FR_HDI_S	Safe Failure Rate of a High Density Digital Input Module Leg
FR_HDIP_S	Safe Failure Rate of a High Density Digital Input Module Common Processing Circuit
FR_HDIC_S	Safe Failure Rate of a High Density Digital Input Circuit
FR_HVO	Failure Rate of a 115 VAC Digital Output Module Leg
FR_HVO_DU	Dangerous Undetected Failure Rate of a 115 VAC Digital Output Module Leg

Symbol	**Description**
FR_HVO_SU	Safe Undetected Failure Rate of a 115 VAC Digital Output Module Leg
FR_HVO_S	Safe Failure Rate of a 115 VAC Digital Output Module Leg
FR_HVOP_S	Safe Failure Rate of a 115 VAC Digital Output Module Common Processing Circuit
FR_HVOC_S	Safe Failure Rate of a 115 VAC Digital Output Switch
FR_IAI	Failure Rate of an Isolated Analog Input Module Leg
FR_IAI_DU	Dangerous Undetected Failure Rate of an Isolated Analog Input Module Leg
FR_IAI_SU	Safe Undetected Failure Rate of an Isolated Analog Input Module Leg
FR_IAI_S	Safe Failure Rate of an Isolated Analog Input Module Leg
FR_IAIP_S	Safe Failure Rate of an Isolated Analog Input Module Common Processing Circuit
FR_IAIC_S	Safe Failure Rate of an Isolated Analog Input Circuit
FR_I_DU	Dangerous Undetected Failure Rate of a 24 VDC Input Module Leg
FR_I_SU	Safe Undetected Failure Rate of a 24 VDC Input Module Leg
FR_I_S	Safe Failure Rate of a 24 VDC Input Module Leg
FR_IP_S	Safe Failure Rate of a 24 VDC Input Module Common Processing Circuit
FR_I	Failure Rate of a 24 VDC Input Module Leg
FR_IC_ S	Safe Failure Rate of a 24 VDC Input Circuit
FR_MP	Failure Rate of a Main Processor
FR_MP_S	Safe Failure Rate of a Main Processor
FR_MP_SU	Safe Undetected Failure Rate of a Main Processor
FR_MP_DU	Dangerous Undetected Failure Rate of a Main Processor
FR_O	Failure Rate of a 24 VDC Digital Output Module Leg
FR_O_DU	Dangerous Undetected Failure Rate of a 24 VDC Digital Output Module Leg
FR_O_SU	Safe Undetected Failure Rate of a 24 VDC Digital Output Module Leg
FR_O_S	Safe Failure Rate of a 24 VDC Digital Output Module Leg
FR_OP_S	Safe Failure Rate of a 24 VDC Digital Output Module Common Processing Circuit
FR_OC_S	Safe Failure Rate of a 24 VDC Digital Output Switch
FR_PS_S	Safe Failure Rate of a Power Supply
FR_PI	Failure Rate of an Pulse Input Module Leg
FR_PI_DU	Dangerous Undetected Failure Rate of an Pulse Input Module Leg
FR_PI_SU	Safe Undetected Failure Rate of an Pulse Input Module Leg
FR_PI_S	Safe Failure Rate of an Pulse Input Module Leg

Symbol	Description
FR_PIP_S	Safe Failure Rate of an Pulse Input Module Common Processing Circuit
FR_PIC_S	Safe Failure Rate of an Pulse Input Circuit
Beta	Common Cause Factor (0.01 or 1%)
ccf3legs	Common Cause Factor affecting all three legs of module (0.5)

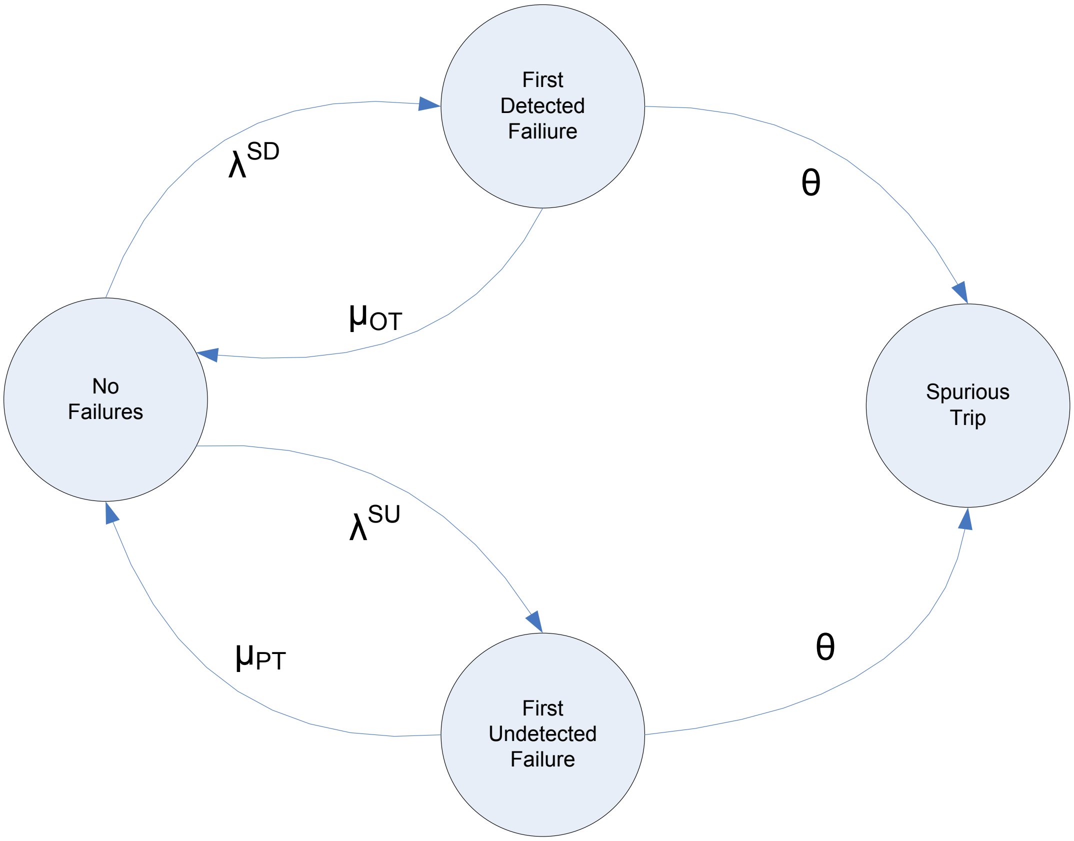
3.2.2. Solution Technique for Safe Failure Markov Model

The effective repair rate includes the repair for detected and undetected safe failures. Detected safe failures can be repaired on-line at a much faster rate. Undetected safe failures can only be repaired after the system is taken off-line for periodic testing. The effective repair rate is determined below. The safe failure rate can be broken down as:

$$\lambda^{S} = C^{S}\,\lambda^{SD} + (1 - C^{S})\,\lambda^{SU}$$

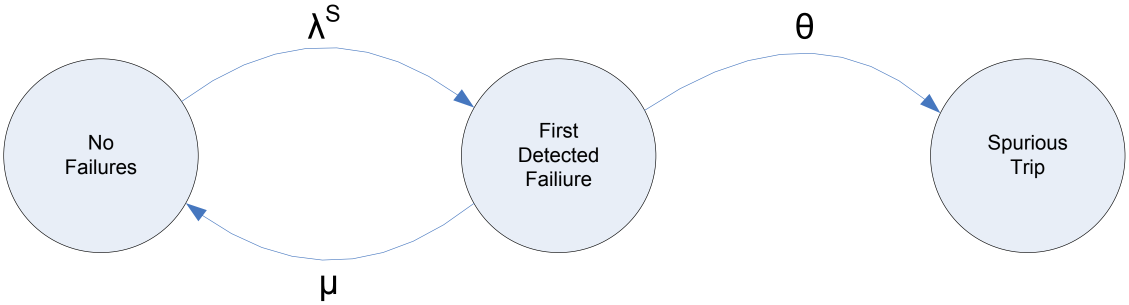
Where:
λ^{S} = Safe failure rate of a component
λ^{SD} = Safe detected failure rate of a component
λ^{SU} = Safe undetected failure rate of a component
C^{S} = Fraction of safe failures detected by diagnostic coverage

The generalized Markov model for safe failures is shown on the following page:



Where:
θ = Failure rate from the intermediate state to the spurious trip state
μ_{ot} = Repair rate when detected due to on-line testing
μ_{pt} = Repair rate for off-line periodic testing

This model can be simplified to the following by determining the effective repair rate.



Where: μ = Effective on-line repair rate

The effective repair rate can be determined by equating the MTTF for each model. After algebraic manipulation, the MTTF's can be shown to be equal if:

$$1 / (\mu + \theta) = C^S / (\mu_{ot} + \theta) + (1 - C^S) / (\mu_{pt} + \theta)$$

Solving for the effective repair rate yields:

$$\mu = [(1 - C^S)\, \theta\, \mu_{pt} + C^S\, \theta\, \mu_{ot} + \mu_{pt}\, \mu_{ot}] / [C^S\, \theta\, \mu_{pt} + (1 - C^S)\, \mu_{ot} + \theta]$$

The MTTF can be determined from the Markov model by integrating the probability for the time that the system is in a non-failed state. States 1 through 20 are the non-failed states.

A closed form solution to this model exists. From Reference *5,* the MTTF is given below.
Note that this solution has been verified using alternative techniques outlined in
Reference 4.

$$MTTFspurious = \frac{1 + \sum_{i=1}^{n} \frac{\lambda_i}{\mu_i + \theta_i}}{\sum_{i=1}^{n} \frac{\lambda_i \theta_i}{\mu_i + \theta_i} + \lambda_{21}}$$

Where **λ_i** is the first subsystem failure to an intermediate (derated) state, **θ_i** is the failure rate from the derated state i to the fail safe state, **μ_i** is the effective repair rate of subsystems in the derated state.

The availability is defined as the ratio of system up-time to total time. The availability is given by:

$$A = [MTTF / (MTTF + MTTR)] (100\%)$$

Where:
A = System availability
MTTF = Mean time to failure
MTTR = Mean time to repair

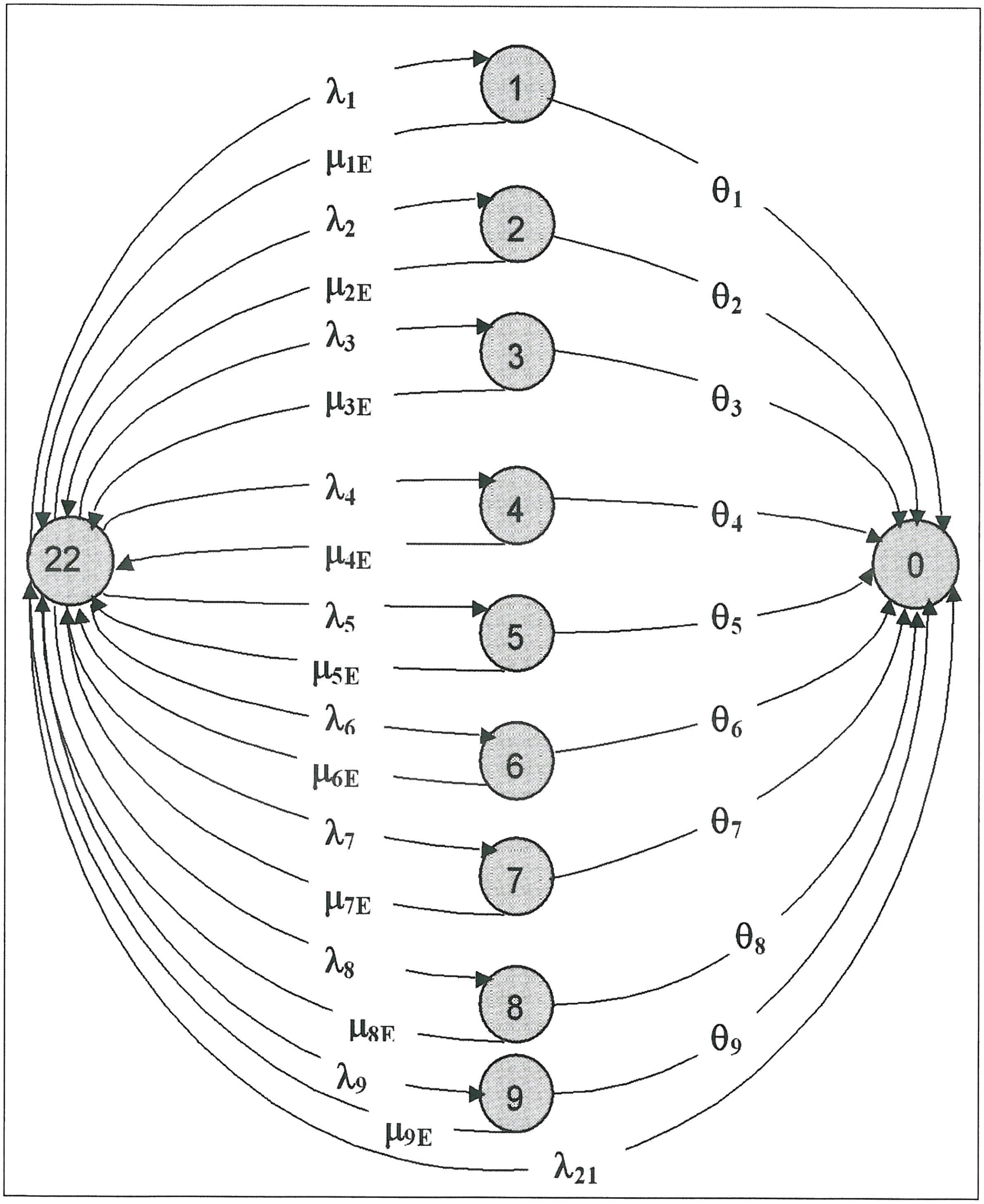


Figure 3-1 (Part 1). Fail Safe Markov Model

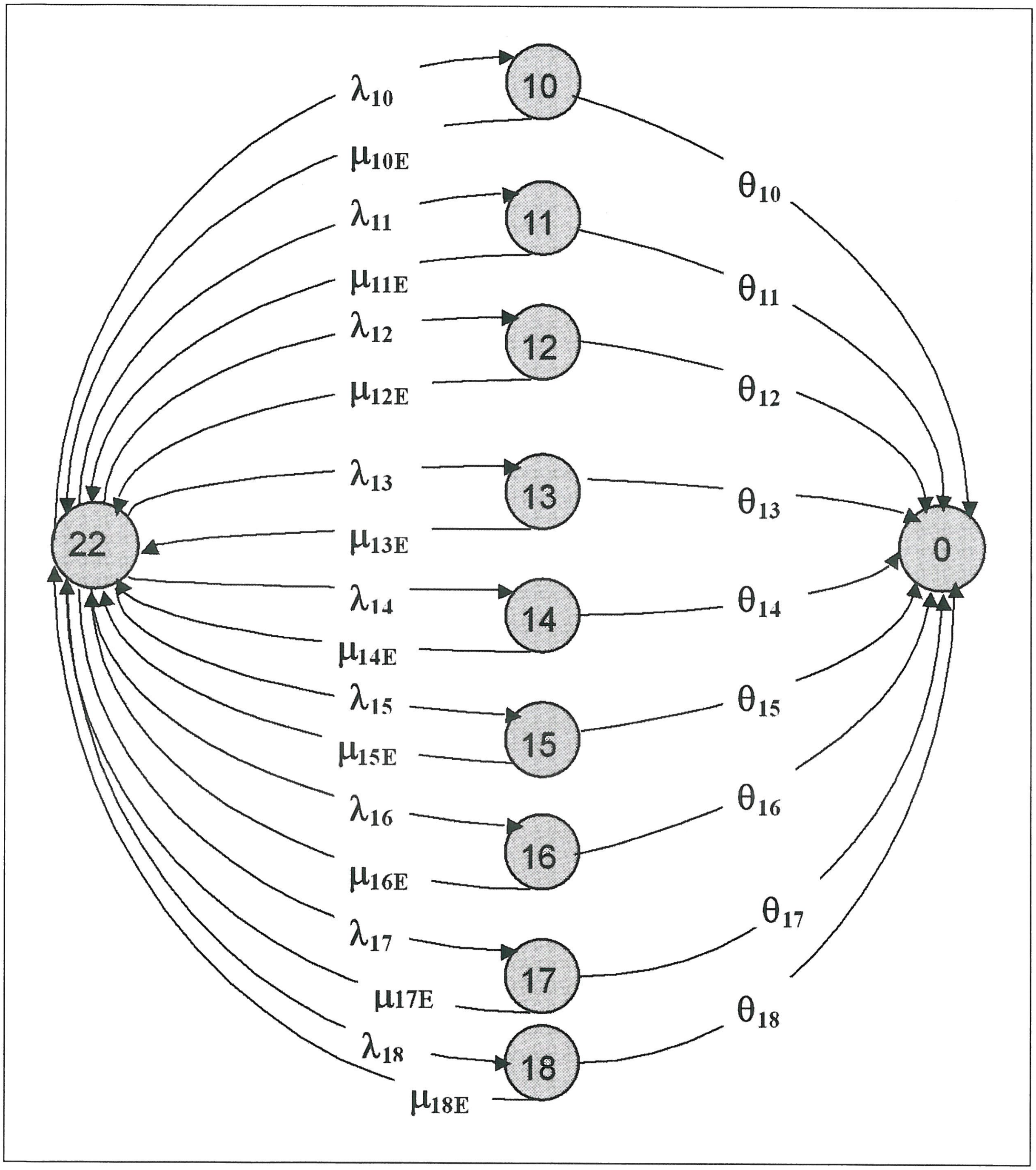


Figure 3-1 (Part 2). Fail Safe Markov Model

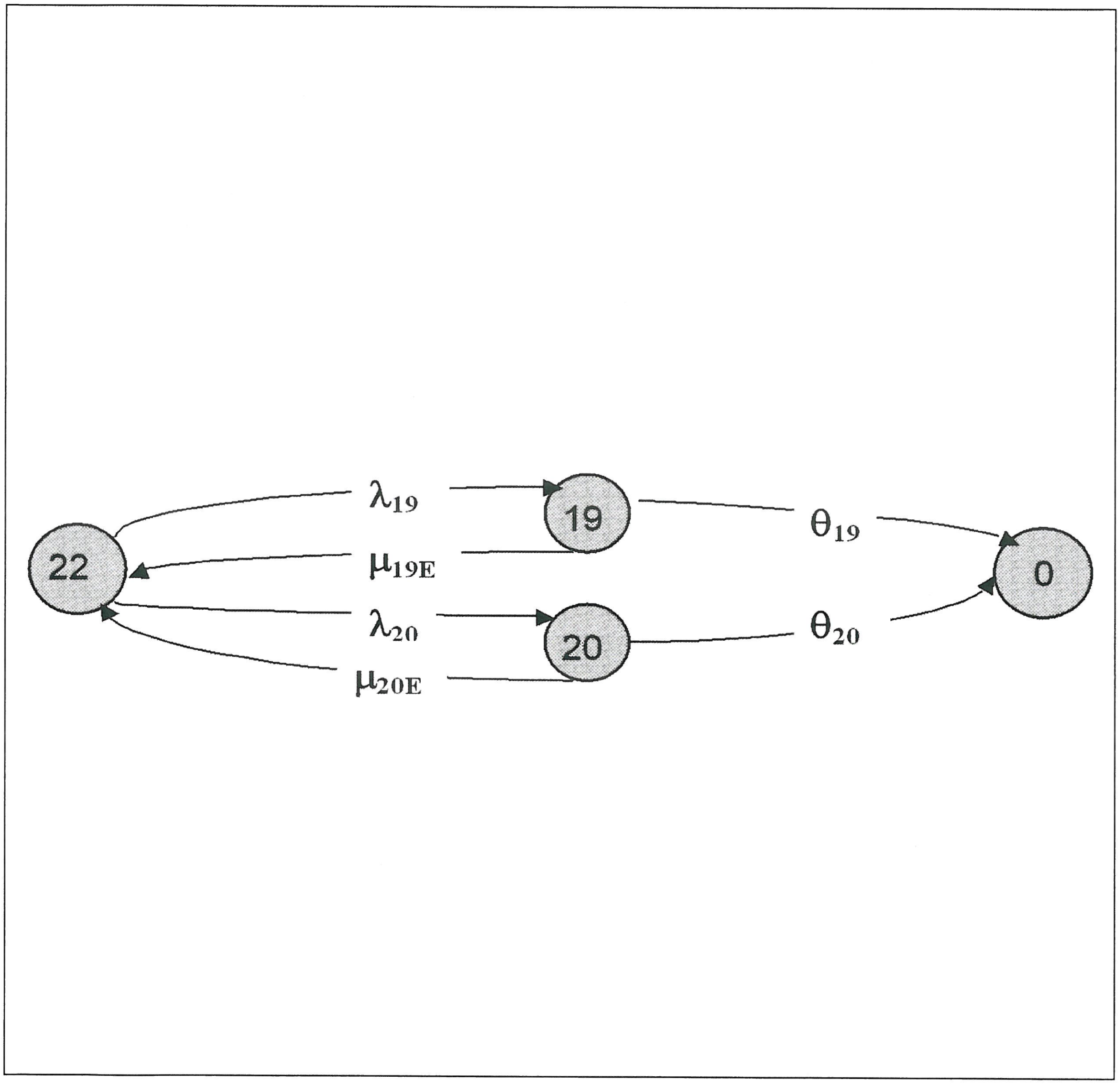


Figure 3-1 (Part 3). Fail Safe Markov Model

3.3. Fail-to-Function Markov Model

3.3.1. Model Description

The fail-to-function Markov model is shown in Figure 3-2. Note that this figure is developed using the methodology described in Reference *5.* The TRICON PLC is a fail safe PLC with triplicated inputs (3-2-0), triple redundant main processor with communication, and a quad output voter. As required by Reference 1, the Markov model includes the main processor, a digital input module, an analog input module, a digital output module, and an analog output module. Along with each input/output microprocessor, the Markov model includes each input/output circuit. Also included is the dual power supply.

The first state in the Markov model is the system operating normally with no failures. The system fails to function after two of the three channels have dangerous undetected failures. The intermediate states occur after one dangerous undetected failure and after a subsequent dangerous detected failure. The probability of moving from one state to another (i.e., probability of failure or repair) are shown by the arrows. Constant failure and repair rates are assumed. The first dangerous detected failure is not modeled because the repair rate is significantly greater than the chance of a second undetected failure occurring while the system is in that state.

Each intermediate failure state is described below. All equations and transition coefficients are taken from the fail to function Markov model for a triplicated PLC with a quad output voter developed in Draft 12 of ISA SP.84.02 (see Reference *5).*

States 2, 3, 23, and 24 – Digital Input

Each digital input model is internally triplicated with 3-2-0 capability. State 2 is the first dangerous undetected failure of a digital input microprocessor module, and state 3 is the first dangerous undetected failure of a digital input circuit to an input module. States 23 and 24 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of three input microprocessors or input circuits are given by:

$$\boldsymbol{\lambda 12} = 3 * \mathrm{nsf} * \mathrm{FR\_IP\_DU}$$

$$\boldsymbol{\lambda 13} = 3 * \mathrm{nsf} * \mathrm{nic} * \mathrm{FR\_IC\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure its subsequent repair are given by:

$$\boldsymbol{\lambda 223} = 2 * (\mathrm{FR\_MP\_DD} + \mathrm{FR\_I\_DD})$$

$$\boldsymbol{\lambda 324} = 2*(FR\_MP\_DD + FR\_IP\_DD + FR\_IC\_DD)$$

$$\boldsymbol{\lambda 232} = MU\_OT$$

$$\boldsymbol{\lambda 243} = MU\_OT$$

The transitions from the first dangerous undetected failure to the system failing to function are given by:

$$\boldsymbol{\lambda 244} = 2* (FR\_MP\_DU + FR\_I\_DU)$$

$$\boldsymbol{\lambda 344} = 2*(FR\_MP\_DU + FR\_IP\_DU + FR\_IC\_DU)$$

States 4, 5, 25, and 26 – Analog Input

Each analog input model is internally triplicated with 3-2-0 capability. State 4 is the first dangerous undetected failure of an analog input microprocessor module, and state *5* is the first dangerous undetected failure of an analog input circuit. States 25 and 26 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of input microprocessors or input circuits are given by:

$$\boldsymbol{\lambda 14} = 3*nasf*FR\_AIP\_DU$$

$$\boldsymbol{\lambda 15} = 3*nasf*nic*FR\_AIC\_DU$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure and its subsequent repair are given by:

$$\boldsymbol{\lambda 425} = 2*(FR\_MP\_DD + FR\_AI\_DD)$$

$$\boldsymbol{\lambda 526} = 2*(FR\_MP\_DD + FR\_AIP\_DD + FR\_AIC\_DD)$$

$$\boldsymbol{\lambda 254} = MU\_OT$$

$$\boldsymbol{\lambda 265} = MU\_OT$$

The transitions from the first dangerous undetected failure to the system failing to function are given by:

$$\boldsymbol{\lambda 444} = 2*(FR\_MP\_DU + FR\_AI\_DU)$$

$$\boldsymbol{\lambda 544} = 2*(FR\_MP\_DU + FR\_AIP\_DU + FR\_AIC\_DU)$$

States 6, 7, 27, and 28 – 16 point Analog Input

State 6 is the first dangerous undetected failure of an analog input microprocessor module, and state 7 is the first dangerous undetected failure of an analog input circuit. States 27 and 28 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of input microprocessors or input circuits are given by:

$$\boldsymbol{\lambda 16} = 3*\mathrm{niaisf}*\mathrm{FR\_IAIP\_DU}$$
$$\boldsymbol{\lambda 17} = 3*\mathrm{niaisf}*\mathrm{niaic}*\mathrm{FR\_IAIC\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure and its subsequent repair are given by:

$$\boldsymbol{\lambda 627} = 2*(\mathrm{FR\_MP\_DD} + \mathrm{FR\_IAI\_DD})$$
$$\boldsymbol{\lambda 728} = 2*(\mathrm{FR\_MP\_DD} + \mathrm{FR\_IAIP\_DD} + \mathrm{FR\_IAIC\_DD})$$
$$\boldsymbol{\lambda 276} = \mathrm{MU\_OT}$$
$$\boldsymbol{\lambda 287} = \mathrm{MU\_OT}$$

The transitions from the first dangerous undetected failure to the system failing to function are given by:

$$\boldsymbol{\lambda 644} = 2*(\mathrm{FR\_MP\_DU} + \mathrm{FR\_IAI\_DU})$$
$$\boldsymbol{\lambda 744} = 2*(\mathrm{FR\_MP\_DU} + \mathrm{FR\_IAIP\_DU} + \mathrm{FR\_IAIC\_DU})$$

States 8, 9, 29, and 30 – Analog Output

Per Reference 8, each analog output module has triplicated analog output circuitry that operates in 3-2-1-0 modes. Hence the triplicated output circuitry requires three faults before a failure condition is reached. Since the probability of failure for the output circuitry is third order ($\sim \lambda^3$), its effect on the mean time to failure can be neglected. The transitions are:

$$\boldsymbol{\lambda 18} = 3*\mathrm{masf}*\mathrm{FR\_AOP\_DU}$$
$$\boldsymbol{\lambda 19} = 0$$

$$\boldsymbol{\lambda 829} = 2*(\mathrm{FR\_MP\_DD} + \mathrm{FR\_AO\_DD})$$
$$\boldsymbol{\lambda 930} = 0$$
$$\boldsymbol{\lambda 298} = \mathrm{MU\_OT}$$
$$\boldsymbol{\lambda 309} = 0$$

$$\boldsymbol{\lambda 844} = 2*(\mathrm{FR\_MP\_DU} + \mathrm{FR\_AO\_DU})$$

$$\boldsymbol{\lambda 944} = 0$$

State 10 and 31 – Main Processor

There are triple redundant main processors. State 10 is the dangerous undetected failure of one of the three main processors. The transition from the initial state to the intermediate states representing the initial failure of one of three main processors is given by:

$$\boldsymbol{\lambda 110} = 3*\mathrm{FR\_MP\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure and its subsequent repair are given by:

$$\boldsymbol{\lambda 1031} = 2*(\mathrm{FR\_MP\_DD} + \mathrm{nsf}*\mathrm{FR\_I\_DD} + \mathrm{nasf}*\mathrm{FR\_AI\_DD} + \mathrm{niaisf}*\mathrm{FR\_IAI\_DD} + \mathrm{masf}*\mathrm{FR\_AO\_DD} + \mathrm{msf}*\mathrm{FR\_O\_DD} + \mathrm{mhvsf}*\mathrm{FR\_HVO\_DD} + \mathrm{nhdsf}*\mathrm{FR\_HDI\_DD} + \mathrm{nahdsf}*\mathrm{FR\_HDAI\_DD})$$

$$\boldsymbol{\lambda 3110} = \mathrm{MU\_OT}$$

The transition from the first dangerous undetected failure to the system failing to function is given by:

$$\boldsymbol{\lambda 1044} = 2*(\mathrm{FR\_MP\_DU} + \mathrm{nsf}*\mathrm{FR\_I\_DU} + \mathrm{nasf}*\mathrm{FR\_AI\_DU} + \mathrm{niaisf}*\mathrm{FR\_IAI\_DU} + \mathrm{masf}*\mathrm{FR\_AO\_DU} + \mathrm{msf}*\mathrm{FR\_O\_DU} + \mathrm{mhvsf}*\mathrm{FR\_HVO\_DU} + \mathrm{nhdsf}*\mathrm{FR\_HDI\_DU} + \mathrm{nahdsf}*\mathrm{FR\_HDAI\_DU})$$

States 11, 12, 32, and 33 – 24 VDC Digital Output

Each 24 VDC digital output module has a triplicated output processor with a quad voter output circuit. State 11 is the first dangerous undetected failure of a digital output microprocessor module, and state 12 is the first dangerous undetected failure of a digital output circuit. States 32 and 33 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of three output microprocessors or output circuits are given by:

$$\boldsymbol{\lambda 111} = 3*\mathrm{msf}*\mathrm{FR\_OP\_DU}$$

$$\boldsymbol{\lambda 112} = 4*\mathrm{msf}*\mathrm{nhdoc}*\mathrm{FR\_OC\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure and its subsequent repair are given by:

$$\boldsymbol{\lambda 1132} = 2\ast(\mathrm{FR\_MP\_DD} + \mathrm{FR\_O\_DD})$$

$$\boldsymbol{\lambda 1233} = 2\ast(\mathrm{FR\_MP\_DD} + \mathrm{FR\_OP\_DD} + \mathrm{FR\_OC\_DD})$$

$$\boldsymbol{\lambda 3211} = \mathrm{MU\_OT}$$

$$\boldsymbol{\lambda 3312} = \mathrm{MU\_OT}$$

The transitions from the first dangerous undetected failure to the system failing to function are given by:

$$\boldsymbol{\lambda 1144} = 2\ast(\mathrm{FR\_MP\_DU} + \mathrm{FR\_O\_DU})$$

$$\boldsymbol{\lambda 1244} = 2\ast(\mathrm{FR\_MP\_DU} + \mathrm{FR\_OP\_DU} + \mathrm{FR\_OC\_DU})$$

States 13, 14, 34, and 35 - 115 VAC Digital Output

Each 115 VAC digital output module has a triplicated output processor with a quad voter output circuit. State 13 is the first dangerous undetected failure of a digital output microprocessor module, and state 14 is the first dangerous undetected failure of a digital output circuit. States 34 and 35 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of three output microprocessors or output circuits are given by:

$$\boldsymbol{\lambda 113} = 3\ast \mathrm{mhvsf}\ast \mathrm{FR\_HVOP\_DU}$$

$$\boldsymbol{\lambda 114} = 4\ast \mathrm{mhvsf}\ast \mathrm{noc}\ast \mathrm{FR\_HVOC\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure and its subsequent repair are given by:

$$\boldsymbol{\lambda 1334} = 2\ast(\mathrm{FR\_MP\_DD} + \mathrm{FR\_HVO\_DD})$$

$$\boldsymbol{\lambda 1435} = 2\ast(\mathrm{FR\_MP\_DD} + \mathrm{FR\_HVOP\_DD} + \mathrm{FR\_HVOC\_DD})$$

$$\boldsymbol{\lambda 3413} = \mathrm{MU\_OT}$$

$$\boldsymbol{\lambda 3514} = \mathrm{MU\_OT}$$

The transitions from the first dangerous undetected failure to the system failing to function are given by:

$$\boldsymbol{\lambda 1344} = 2\ast(\mathrm{FR\_MP\_DU} + \mathrm{FR\_HVO\_DU})$$

$$\boldsymbol{\lambda 1444} = 2*(\mathrm{FR\_MP\_DU} + \mathrm{FR\_HVOP\_DU} + \mathrm{FR\_HVOC\_DU})$$

States 15, 16, 36, and 37 – High Density Digital Input

Each high density digital input model is internally triplicated with 3-2-0 capability. State 15 is the first dangerous undetected failure of a digital input microprocessor module, and state 16 is the first dangerous undetected failure of a digital input circuit. States 36 and 37 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of three input microprocessors or input circuits are given by:

$$\boldsymbol{\lambda 115} = 3*\mathrm{nhdsf}*\mathrm{FR\_HDIP\_DU}$$
$$\boldsymbol{\lambda 116} = 3*\mathrm{nhdsf}*\mathrm{nhdic}*\mathrm{FR\_HDIC\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure its subsequent repair are given by:

$$\boldsymbol{\lambda 1536} = 2*\ (\mathrm{FR\_MP\_DD} + \mathrm{FR\_HDI\_DD})$$
$$\boldsymbol{\lambda 1637} = 2*(\mathrm{FR\_MP\_DD} + \mathrm{FR\_HDIP\_DD} + \mathrm{FR\_HDIC\_DD})$$
$$\boldsymbol{\lambda 3615} = \mathrm{MU\_OT}$$
$$\boldsymbol{\lambda 3716} = \mathrm{MU\_OT}$$

The transitions from the first dangerous failure to the system failing to function are given by:

$$\boldsymbol{\lambda 1544} = 2*\ (\mathrm{FR\_MP\_DU} + \mathrm{FR\_HDI\_DU})$$
$$\boldsymbol{\lambda 1644} = 2*(\mathrm{FR\_MP\_DU} + \mathrm{FR\_HDIP\_DU} + \mathrm{FR\_HDIC\_DU})$$

States 17, 18, 38, and 39 – High Density Analog Input

Each high density analog input model is internally triplicated with 3-2-0 capability. State 17 is the first dangerous undetected failure of an analog input microprocessor module, and state *18* is the first dangerous undetected failure of an analog input circuit t. States 38 and 39 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of input microprocessors or input circuits are given by:

$$\boldsymbol{\lambda 117} = 3*\text{nahdsf}*\text{FR\_HDAIP\_DU}$$
$$\boldsymbol{\lambda 118} = 3*\text{nahdsf}*\text{nhdic}*\text{FR\_HDAIC\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure and its subsequent repair are given by:

$$\boldsymbol{\lambda 1738} = 2*(\text{FR\_MP\_DD} + \text{FR\_HDAI\_DD})$$
$$\boldsymbol{\lambda 1839} = 2*(\text{FR\_MP\_DD} + \text{FR\_HDAIP\_DD} + \text{FR\_HDAIC\_DD})$$
$$\boldsymbol{\lambda 3817} = \text{MU\_OT}$$
$$\boldsymbol{\lambda 3918} = \text{MU\_OT}$$

The transitions from the first dangerous failure to the system failing to function are given by:

$$\boldsymbol{\lambda 1744} = 2*(\text{FR\_MP\_DU} + \text{FR\_HDAI\_DU})$$
$$\boldsymbol{\lambda 1844} = 2*(\text{FR\_MP\_DU} + \text{FR\_HDAIP\_DU} + \text{FR\_HDAIC\_DU})$$

States 19, 20, 40, and 41 – Pulse Input

State 19 is the first dangerous undetected failure of a digital input microprocessor module, and state 20 is the first dangerous undetected failure of a digital input circuit. States 40 and 41 are the corresponding states after a second dangerous detected failure occurs. The transitions from the initial state to the intermediate states representing the initial failure of one of three input microprocessors or input circuits are given by:

$$\boldsymbol{\lambda 119} = 2*\text{npsf}*\text{FR\_PIP\_DU}$$
$$\boldsymbol{\lambda 120} = 2*\text{npsf}*\text{npc}*\text{FR\_PIC\_DU}$$

The transitions from the first failed state to the intermediate state for a dangerous detected failure its subsequent repair are given by:

$$\boldsymbol{\lambda 1940} = 2*(\text{FR\_MP\_DD} + \text{FR\_PI\_DD})$$
$$\boldsymbol{\lambda 2041} = 2*(\text{FR\_MP\_DD} + \text{FR\_PIP\_DD} + \text{FR\_PIC\_DD})$$
$$\boldsymbol{\lambda 4019} = \text{MU\_OT}$$
$$\boldsymbol{\lambda 4120} = \text{MU\_OT}$$

The transitions from the first dangerous failure to the system failing to function are given by:

$$\boldsymbol{\lambda 1944} = 2*(\text{FR\_MP\_DU} + \text{FR\_PI\_DU})$$

$$\boldsymbol{\lambda 2044} = 2*(\text{FR\_MP\_DU} + \text{FR\_PIP\_DU} + \text{FR\_PIC\_DU})$$

States 21 and 22 – Not used

These are reserved for addition of an I/O module.

Effects of Common Cause Failures

The common cause failure transition is given by:

$$\begin{aligned}\boldsymbol{\lambda 144} = 3*\text{Beta}*\ \text{ccf3legs} * (&\text{FR\_MP\_DU} + \text{nsf}*\text{FR\_I\_DU} + \text{nhdsf}*\text{FR\_HDI\_DU} + \text{nasf}*\text{FR\_AI\_DU} + \\ &\text{nahdsf}*\text{FR\_HDAI\_DU} + \text{niaisf}*\text{FR\_IAI\_DU} + \text{masf}*\text{FR\_AO\_DU} \\ &+ \text{msf}*\text{FR\_O\_DU} + \text{mhvsf}*\text{FR\_HVO\_DU} + \text{npsf}*\text{FR\_PI\_DU})\end{aligned}$$

Where,

Symbol	Description
msf	Number of NG 24 VDC Digital Output Modules for Typical Safety Function
masf	Number of Analog Output Modules for Typical Safety Function
mhvsf	Number of 115 VAC Digital Output Modules for Typical Safety Function
nsf	Number of 24 VDC Digital Input Modules for Typical Safety Function
nhdsf	Number of High Density Digital Input Modules for Typical Safety Function
nasf	Number of NG Diff. Analog Input Modules for Typical Safety Function
nahdsf	Number of NG High Density Analog Input Modules for Typical Safety Function
niaisf	Number of Isolated Analog Input Modules for Typical Safety Function
npsf	Number of Pulse Input Modules for Typical Safety Function
nic	Number of Input Points on Digital Input and Analog Input Modules (32 points)
nhdic	Number of Input Points on High Density DI and AI Modules (64 points)

Symbol	**Description**
niaic	Number of Input Points on Isolated Analog Input Modules (16 points)
noc	Number of Output Points on 115 VAC Digital Output Modules (16 points)
nhdoc	Number of Output Points on NG 24 VDC Digital Output Modules (32 points)
npc	Number of Pulse Input Points on Pulse Input Modules (8 points)
FR_AI	Failure Rate of an NG Diff. Analog Input Module Leg
FR_AI_DU	Dangerous Undetected Failure Rate of an Analog Input Module Leg
FR_AI_DD	Dangerous Detected Failure Rate of an Analog Input Module Leg
FR_AIP	Failure Rate of an Analog Input Module Common Processing Circuit
FR_AIP_DU	Dangerous Undetected Failure Rate of an Analog Input Module Common Processing Circuit
FR_AIC	Failure Rate of an Analog Input Circuit
FR_AIC_DU	Dangerous Undetected Failure Rate of an Analog Input Circuit
FR_AOP	Failure Rate of an Analog Output Module Common Processing Circuit
FR_AOP_DD	Dangerous Detected Failure Rate of an Analog Output Module Common Processing Circuit
FR_AOP_DU	Dangerous Undetected Failure Rate of an Analog Output Module Common Processing Circuit
FR_HDAI	Failure Rate of a High Density Analog Input Module Leg
FR_HDAI_DU	Dangerous Undetected Failure Rate of a High Density Analog Input Module Leg
FR_HDAI_DD	Dangerous Detected Failure Rate of a High Density Analog Input Module Leg
FR_HDAIP	Failure Rate of a High Density Analog Input Module Common Processing Circuit
FR_HDAIP_DU	Dangerous Undetected Failure Rate of a High Density Analog Input Module Common Processing Circuit
FR_HDAIC	Failure Rate of a High Density Analog Input Circuit
FR_HDAIC_DD	Dangerous Undetected Failure Rate of a High Density Analog Input Circuit
FR_HDI	Failure Rate of a High Density Digital Input Module Leg
FR_HDI_DU	Dangerous Undetected Failure Rate of a High Density Digital Input Module Leg
FR_HDI_DD	Dangerous Detected Failure Rate of a High Density Digital Input Module Leg
FR_HDIP	Failure Rate of a High Density Digital Input Module Common Processing

Symbol	Description
	Circuit
FR_HDIP_DU	Dangerous Undetected Failure Rate of a High Density Digital Input Module Common Processing Circuit
FR_HDIC	Failure Rate of a High Density Digital Input Circuit
FR_HDIC_DU	Dangerous Undetected Failure Rate of a High Density Digital Input Circuit
FR_HVO	Failure Rate of a 115 VAC Digital Output Module Leg
FR_HVO_DU	Dangerous Undetected Failure Rate of a 115 VAC Digital Output Module Leg
FR_HVO_DD	Dangerous Detected Failure Rate of a 115 VAC Digital Output Module Leg
FR_HVOP	Failure Rate of a 115 VAC Digital Output Module Common Processing Circuit
FR_HVOP_DU	Dangerous Undetected Failure Rate of a 115 VAC Digital Output Module Common Processing Circuit
FR_HVOC	Failure Rate of a 115 VAC Digital Output Switch
FR_HVOC_DU	Dangerous Undetected Failure Rate of a 115 VAC Digital Output Switch
FR_IAI	Failure Rate of an Isolated Analog Input Module Leg
FR_IAI_DU	Dangerous Undetected Failure Rate of an Isolated Analog Input Module Leg
FR_IAI_DD	Dangerous Detected Failure Rate of an Isolated Analog Input Module Leg
FR_IAIP	Failure Rate of an Isolated Analog Input Module Common Processing Circuit
FR_IAIP_DU	Dangerous Undetected Failure Rate of an Isolated Analog Input Module Common Processing Circuit
FR_IAIC	Failure Rate of an Isolated Analog Input Module Input Circuit
FR_IAIC_DU	Dangerous Undetected Failure Rate of an Isolated Analog Input Circuit
FR_I	Failure Rate of a 24 VDC Input Module Leg
FR_I_DU	Dangerous Undetected Failure Rate of a 24 VDC Input Module Leg
FR_I_DD	Dangerous Detected Failure Rate of a 24 VDC Input Module Leg
FR_IP	Failure Rate of a 24 VDC Input Module Common Processing Circuit
FR_IP_DU	Dangerous Undetected Failure Rate of a 24 VDC Input Module Common Processing Circuit
FR_IC	Failure Rate of a 24 VDC Input Circuit
FR_IC_ DU	Dangerous Undetected Failure Rate of a 24 VDC Input Circuit
FR_MP	Failure Rate of a Main Processor
FR_MP_DD	Dangerous Detected Failure Rate of a Main Processor

Symbol	Description
FR_MP_DU	Dangerous Undetected Failure Rate of a Main Processor
FR_O	Failure Rate of a NG 24 VDC Digital Output Module Leg
FR_O_DU	Dangerous Undetected Failure Rate of a NG 24 VDC Digital Output Module Leg
FR_O_DD	Dangerous Detected Failure Rate of a NG 24 VDC Digital Output Module Leg
FR_OP	Failure Rate of a NG 24 VDC Digital Output Module Common Processing Circuit
FR_OP_DU	Dangerous Undetected Failure Rate of a NG 24 VDC Digital Output Module Common Processing Circuit
FR_OC	Failure Rate of a NG 24 VDC Digital Output Switch
FR_OC_DU	Dangerous Undetected Failure Rate of a NG 24 VDC Digital Output Switch
FR_PI	Failure Rate of a Pulse Input Module Leg
FR_PI_DU	Dangerous Undetected Failure Rate of a Pulse Input Module Leg
FR_PI_DD	Dangerous Detected Failure Rate of a Pulse Input Module Leg
FR_PIP	Failure Rate of a Pulse Input Module Common Processing Circuit
FR_PIP_DU	Dangerous Undetected Failure Rate of a Pulse Input Module Common Processing Circuit
FR_PIC	Failure Rate of a Pulse Input Circuit
FR_PIC_ DU	Dangerous Undetected Failure Rate of a Pulse Input Circuit
Beta	Common Cause Factor (0.01 or 1%)
ccf3legs	Common Cause Factor affecting all three legs of module (0.5)

3.4.Solution Techniques for Fail-to-Function Markov Model

The effective repair rate includes the repair for detected and undetected dangerous failures. Dangerous detected failures can be repaired on-line at a much faster rate. Dangerous undetected failures can only be repaired after the system is taken off-line for periodic testing. The effective repair rate is determined below. The safe failure rate can be broken down as:

$$\lambda^{D} = C^{D}\,\lambda^{DD} + (1 - C^{D})\,\lambda^{DU}$$

Where:
λ^{D} = Dangerous failure rate of a component
λ^{DD} = Dangerous detected failure rate of a component
λ^{DU} = Dangerous undetected failure rate of a component
C^{D} = Fraction of dangerous failures detected by diagnostic coverage

From Reference *5,* the Markov model can be solved using the method of differential equations. Note that a similar technique is described in Reference 4. A 44 x 44 transition matrix can be formed with each of the transition coefficients determined previously.

The probability of failure on demand at a given time can be determined by summing the probabilities of being in a failed state (states 23 through 44) at a given time. The average probability of failure on demand can be determined by averaging the sum over the periodic test interval.

$$PFDavg = (1 / PTI) \int_{0}^{PTI} [\sum_{i=23}^{44} P_i(t)]\, dt$$

Where:
PFDavg = Average probability of failure on demand
PTI = Periodic test interval

The average probability of failure on demand can be determined using these equations and evaluating the integral between zero and the periodic test interval. The safety availability can be determined from the average probability of failure by:

SA = (1-PFDavg) (100%)
Where:

SA = Safety Availability

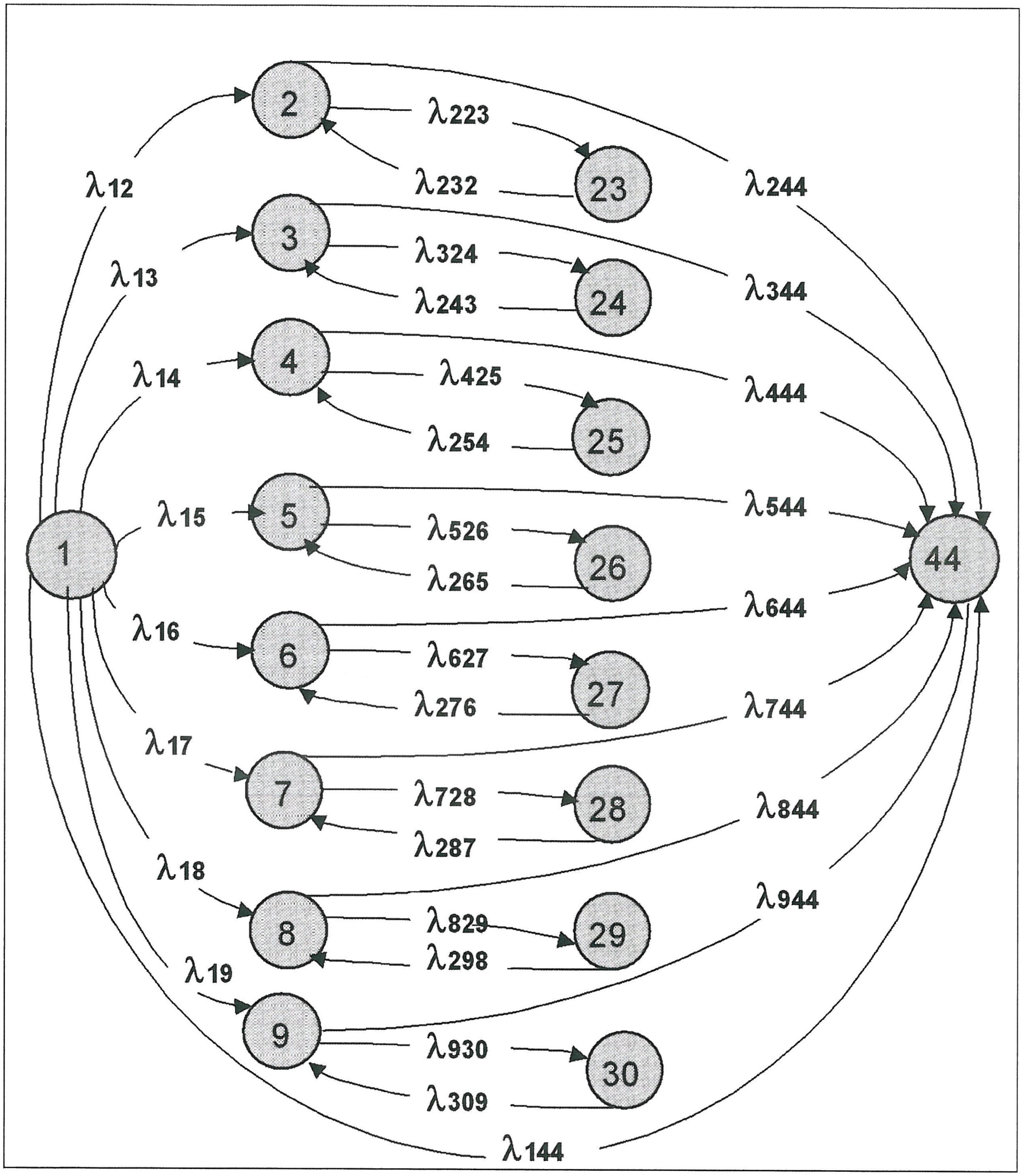


Figure 3-2 (part 1). Fail to Function Markov Model

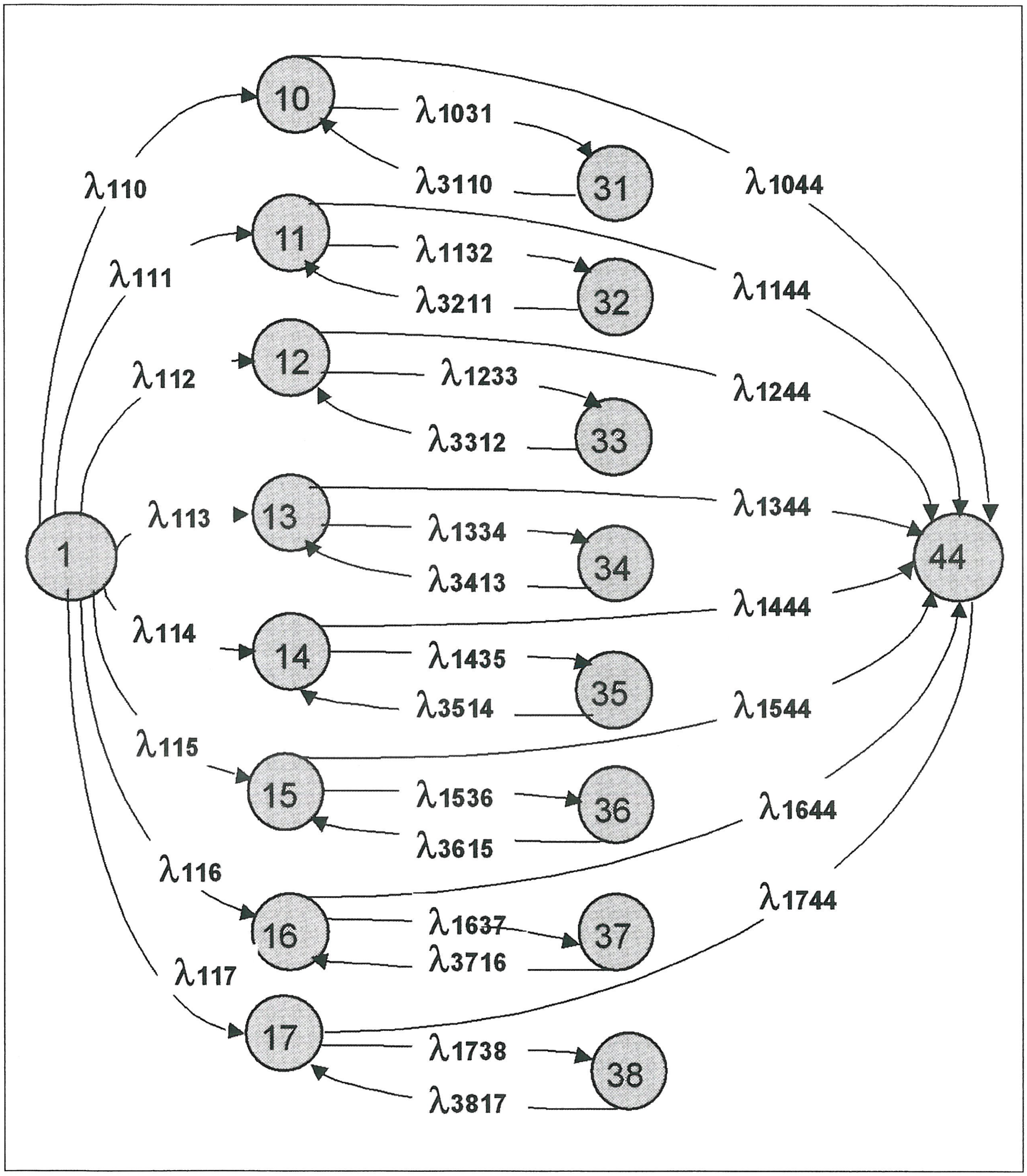


Figure 3-2 (part 2). Fail to Function Markov Model

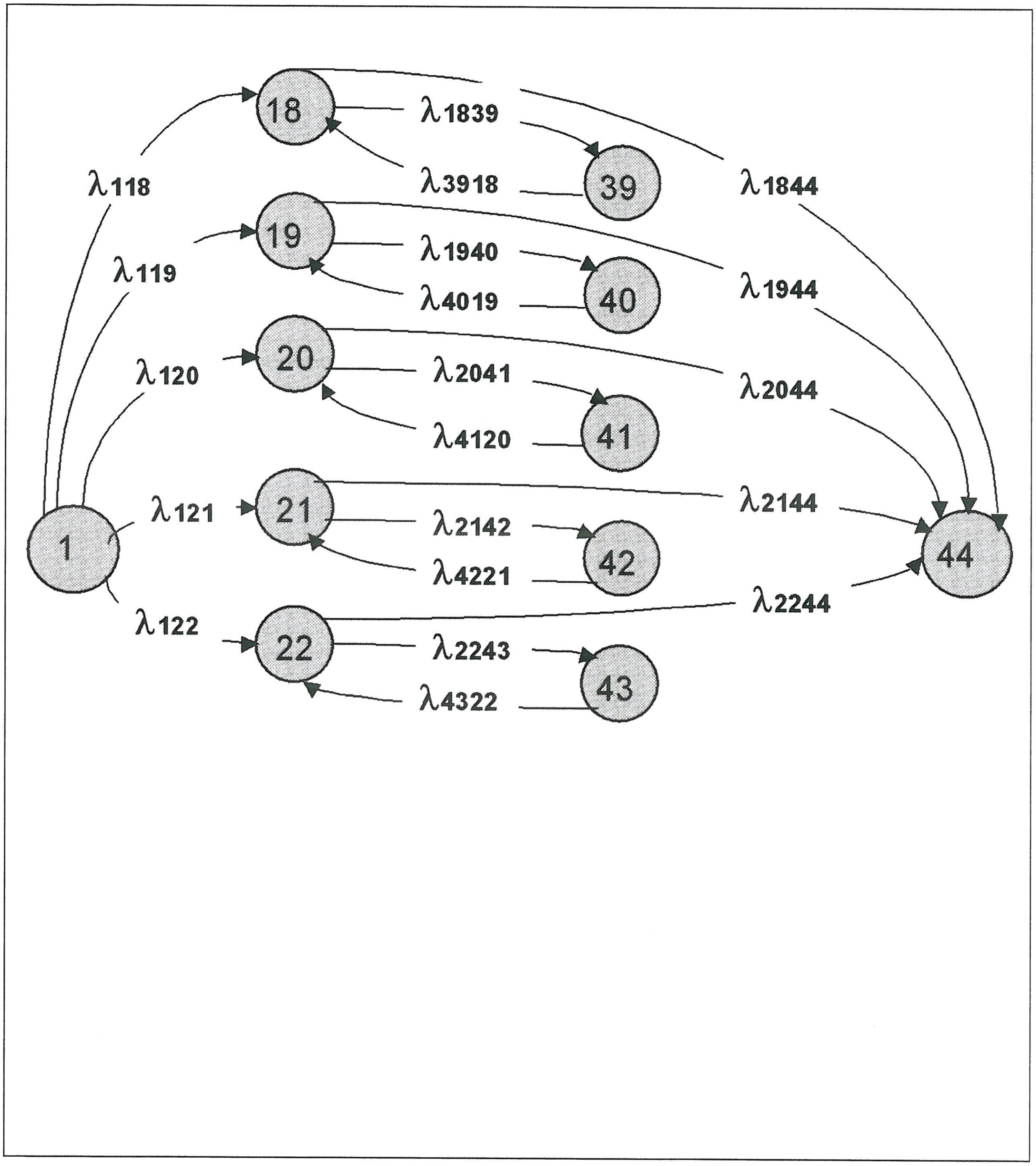


Figure 3-2 (part 3). Fail to Function Markov Model

4. CALCULATION INPUTS AND RESULTS

4.1.Safe Failure Markov Model Input Data and Results

The following table provides the inputs used in the Markov Model for safe failures.

Table 4-1. Inputs to Safe Failure Markov Model

Number of 32 point Digital Input Modules (n) [3501T, 3502E, 3503E]	**3**
Number of 64 point HD Digital Input Modules (nhd)	**0**
Number of 32 point NG Diff. Analog Input Modules (na) [3721]	**1**
Number of 64 point NG HD Analog Input Modules (nahd)	**0**
Number of 16 point IAI/ITC Modules (niai) [3703E]	**1**
Number of 32 point NG 24 VDC Digital Output Modules (m) [3625]	**2**
Number of 16 point 115 VAC Digital Output Modules (mhv) [3601E]	**1**
Number of 8 point Analog Output Modules (ma) [3805E]	**1**
Number of 8 point Pulse Input Modules (np) [3511]	**1**
Total Number of Chassis (Main, Exp. & RXM) (I) [[8310, 8311, 8312]	**4**
Mean Time to Repair- Online (MTTRot)	**24 Hours**
Periodic Offline Test Interval (TI) – Varies from 6 to 30 Months	**4380 to 21900 Hours**
Common Cause - Beta Factor (Beta)	**1.0%**

The failure rate data for each module is contained in Appendix A. The data also includes the ratio of safe to dangerous failures, and the diagnostic coverage for each module.

Appendix B contains the detailed calculations solving both Markov models for the safety availability and the overall availability of the TRICON VERSION 10. The results of the calculations are contained in the following tables.

Table 4-2. Results of Safe Failure Markov Calculations

MTTFspurious and Overall Availability
TRICON-UNDER-TEST MODULE CONFIGURATION

Periodic Test Interval TI - Months	Mean Time to Repair Failures Detected On-line MTTRot - Hours	Mean Time to Failure Due to a Spurious Trip MTTFspurious		Overall Availability
		Hours	Years	
6	24	1,929,410	220.3	99.9988%
12	24	1,908,027	217.8	99.9987%
18	24	1,887,857	215.5	99.9987%
24	24	1,868,780	213.3	99.9987%
30	24	1,850,696	211.3	99.9987%

Note 1: Per Section 4.2.3.3.B of Reference 1, Overall Availability calculations are performed for each of the periodic test intervals (TI).

Note 2: Per Section 4.2.3.3.C of Reference 1, MTTRot, the mean time to repair a failure dangerous detected online is equal to one day.

4.2. Fail to Function Markov Model Input Data and Results

The following table provides the inputs used in the Markov Model for fail to function failures.

Table 4-3. Inputs for Fail to Function Markov Calculations

Number of 32 point Digital Input Modules (nsf)) [3501T, 3502E, 3503E]	**1**
Number of 64 point HD Digital Input Modules (nhdsf)	**0**
Number of 32 point NG Diff. Analog Input Modules (nasf) [3721]	**1**
Number of 64 point NG HD Analog Input Modules (nahdsf)	**0**
Number of 16 point IAI/ITC Modules (niaisf) [3703E]	**0**
Number of 32 point NG 24 VDC Digital Output Modules (msf) [3625]	**1**
Number of 16 point 115 VAC Digital Output Modules (mhvsf) [3601E]	**0**
Number of 8 point Analog Output Modules (masf) [3805E]	**0**
Number of 8 point Pulse Input Modules (npsf) [3511]	**0**
Mean Time to Repair- Online (MTTRot)	**24 Hours**
Periodic Offline Test Interval (TI) – Varies from 6 months to 30 months	**4380 to 21900 Hours**
Common Cause - Beta Factor	**1.0%**

Table 4-4. Results of Fail to Function Markov Calculations

PFDavg and Safety Availability			
TRICON-UNDER-TEST MODULE CONFIGURATION			
Periodic Test Interval TI - Months	Mean Time to Repair Failures Dangerous detected On-line MTTRot - Hours	Average Probability of Failure on Demand PFDavg	Safety Availability
6	24	3.179E-06	99.9997%
12	24	6.577E-06	99.9993%
18	24	1.019E-05	99.9990%
24	24	1.403E-05	99.9986%
30	24	1.809E-05	99.9982%

Note 3: Per Section 4.2.3.3.B of Reference 1, Safety Availability calculations are performed for each of the periodic test intervals (TI).

5. REFERENCES

1. EPRI Report TR-107330, “Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants,” December 1996.

2. ANSI/IEEE Std 352-1987, “IEEE Guidelines for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.”

3. MIL-HDBK-217F, “Military Handbook, Reliability Prediction of Electronic Equipment,” 2 December 1991.

4. Goble, W. Control Systems Safety Evaluation and Reliability, 2nd Edition. Research Triangle Park, NC: Instrument Society of America, 1998.

5. Triconex Memorandum from T. Fredrickson to M. Albers (MPR), “Markov Models for the TRICON Controller,” dated September 13, 1999 (Attachments include Draft 12 of ISA SP.84.02)

6. Triconex Document 9600164-540, Master Configuration List

7. Triconex Part Number 9600164-732, Reliability/ Availability Spreadsheet for TRICON VERSION 10.2 PLC Operating Under Normal Conditions. File Name: TRICONV10.2_0906_Nuclear.xls.

8. Triconex Part Number 9600164-733, Reliability/ Availability Spreadsheet for TRICON VERSION 10.2 PLC Operating Under Post Accident Conditions. File Name: TRICONV10.2_0906_Nuclear_Post_Accident.xls.

a

Appendix A - FAILURE RATE DATA FOR THE TRICON TMR MODULES

a

Appendix B - SOLUTIONS OF THE MARKOV MODELS

B.1 Purpose

The purpose of this appendix is to show the results of the Safe Failure and Fail to Function Markov Model calculations. The solution techniques are presented in Section 3 of the main body of the calculation. Inputs to the Markov Model calculations are shown in Section 4 and Appendix A.

B.2 Safe Failure Markov Model Calculation Results

The results of the Safe Failure Markov Model calculations are shown on the following pages. Calculations are shown for five different values of the Periodic Off-line Test Interval (6, 12,18, 24 and 30 Months).

a

a

a

a

a

a

a

B.3 Fail to Function Markov Model Calculation Results

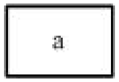
The results of the Fail to Function Markov Model calculations are shown on the following pages. Calculations are shown for five different values of the Periodic Off-line Test Interval (6, 12,18,24,and 30 Months).

a

a

a

a


a

a

a

a

a

Appendix C - POST LOCA AVAILABILITY

C.1 Purpose

The purpose of this appendix is to calculate the safety availability and overall availability of the TRICON VERSION 10 during a two-week period after an accident.

C.2 Results

For a two-week post accident period, the overall availability is 99.95 %, and the safety availability is 99.99%. Both of these values are greater than the recommended goal of 99% per Reference 1.

C.3 Calculations

Post accident environmental conditions are more severe than the usual operating conditions of the TRICON VERSION 10. Per Section 4.3.6.2.A of Reference 1, the following environmental conditions should be considered for a two week post accident period.

50°C Ambient Temperature
95% Relative Humidity

The failure rates for each component are provided in Appendix A. These failure rates are calculated in Reference 7 using the methodology presented in Reference 3. The failure rate calculations use an ambient temperature of 30°C and a benign ground environment. For integrated silicon microcircuits, the failure rate is determined using the following formula:

$$\lambda = (C_1 \pi_T + C_2 \pi_E) \pi_Q \pi_L$$

Where:

λ	=	Failure rate in failures per million hours
C_1	=	Die complexity failure rate
π_T	=	Temperature factor
C_2	=	Package failure rate
π_E	=	Environmental factor
π_Q	=	Quality factor
π_L	=	Learning factor

Per Reference 3, only the factors π_T and π_E are affected by more severe operating environments; all other factors in this equation remain constant. When the ambient temperature of silicon microcircuits is increased from 30°C to 50°C , π_T increases by a factor of 5. Changing the environment from benign (ground) to mobile (ground) or naval (sheltered) increases π_E by a factor of 8.

From examining the above equation, it is obviously conservative to combine these two factors to determine a maximum possible increase in failure rate. The maximum increase in failure rate is 40. From further examination of Reference 3, the calculated increase in failure rate for microcircuits due to post accident environmental effects bounds the same increase determined for all other types of electronic components found in the TRICON TMR controller.

The overall availability and safety availability for the post accident environment are calculated in the following tables using the same methods outlined in previous sections. All failure rates are conservatively increased by a factor of 40 to account for the higher temperature and more severe environmental conditions present during post accident conditions. The on-line repair rate of 24 hours is unchanged from before. Note that the effective off-line repair rate assumes the undangerous detected failures cannot be repaired for at least the two-week post accident period. As required by Section 4.2.3.3.F of Reference 1, the availability is calculated for the entire two week period. The results of the calculations are shown in the tables in Section C.6.

a

C.4 Post Accident Failure Rate Data

C.5 Post Accident Configuration Data

The TRICON configuration data is the same as shown in Section 4 (See Tables 4-1 and 4-3) except for TI. The periodic offline test interval (TI) is set to two weeks (336 hours).

C.6 Post Accident Markov Model Calculation Results

The Results for Fail Safe and Fail to Function Results are shown on the following pages. The calculations were performed using the EXCEL spreadsheet listed in Reference 8.

a

a