TRICONEX

Triconex Corporation

15091 Bake Parkway
Irvine, California 92618
United States of America

Telephone +1 949 699 2100
Facsimile +1 949 768 6601
http://www.triconex.com

November 15, 2000

Document Control Desk
United States Nuclear Regulatory Commission
Washington, DC 20555

Subject: Nuclear 1E Qualification of the TRICON TMR Programmable Logic Controller (PLC) – Revised Project Proprietary Documents

Reference: 1. Letter, T. Martel (Triconex) to NRC, September 29, 2000, subject; Nuclear Qualification of the TRICON TMR PLC – Additional Project Qualification Document Submittals

2. Project Number 709

Gentlemen:

In the referenced letter, Triconex submitted 3 proprietary documents for the NRC's review in connection with our TRICON 1E Qualification Project, as listed below. These documents were accompanied by a request for withholding from public disclosure per 10CFR2.790 and the required affidavit.

1.	Reliability/Availability Study	7286-531	Rev 0
2.	Certificate of Conformance	7286-542	Rev 0
3.	Master Configuration List	7286-540	Rev 22

Non-proprietary versions of these documents were not provided at the time. Also, the proprietary portions of these documents were not specifically identified as requested by the staff. To resolve these documentation concerns, we are enclosing revised copies of the documents listed above, marked up as requested to show areas of proprietary information (please note that content has not changed). Also provided are non-proprietary versions of these documents for the public record with proprietary areas deleted.

These enclosed documents replace and supersede earlier versions provided. As indicated in the September 29, 2000 letter, the enclosed documents are considered proprietary where so marked and should be withheld from public disclosure per 10CFR2.790. The affidavit provided in the September 29, 2000 letter still applies to these documents.

D062

If you have any questions regarding the enclosed documents, please contact me at (281) 360-6401 or Mr. Michael Phillips at (949) 699-2111.

Sincerely,

J. Troy Martel, P.E.

J. Troy Martel, P. E.
Triconex Nuclear Qualification Project Director

Enclosures
cc: L. Raynard Wharton, NRC (w/o attachments)
P. Loeser, NRC (w/o attachments)

TRICONEX DOCUMENTS

NON-PROPRIETARY VERSIONS

1. Reliability/Availability Study	7286-531	Rev 0
2. Certificate of Conformance	7286-542	Rev 0
3. Master Configuration List	7286-540	Rev 22

TRICONEX

Project:	NUCLEAR QUALIFICATION OF TRICON PLC SYSTEM
Purchase Order No.:	ST – 401734
Project Sales Order:	7286

RELIABILITY/AVAILABILITY STUDY FOR TRICON PLC CONTROLLER

Document No.: 7286-531

Revision 0

January 14, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Author:	Craig Swanner		Project Engineer
Approvals:	Mitchell Albers	Mitchell Albers	Project Manager
	Troy Martel	Troy Martel	Triconex Project Director
	Aad Faber		Director, Product Assurance

TRICONEX

Document:	7286-531	**Title:**	**Reliability/Availability Study for Tricon PLC Controller**		
Revision:	0	**Page:**	2 of 3	**Date:**	01/14/00

Document Change History			
Revision	**Date**	**Change**	**Author**
0	01/14/00	Initial issue.	Craig Swanner

TRICONEX

Document:	7286-531	**Title:**	**Reliability/Availability Study for Tricon PLC Controller**		
Revision:	0	**Page:**	3 of 3	**Date:**	01/14/00

SEE ATTACHED

MPR ASSOCIATES CALCULATION

No. 426-001-CBS-01, Revision 1

Pages: 1 through 27
A-1 through A-2
B-1 through B-7
C-1 through C-5

MPR

MPR Associates, Inc.
320 King Street
Alexandria, VA 22314

CALCULATION TITLE PAGE

Client	Triconex Corporation	Page 1 of 27 + Appendices
Project	Tricon PLC Qualification	Task No. 426-9901-001-0
Title	Reliability Study for Tricon PLC Controller	Calculation No. 426-001-CBS-01

Preparer/Date	Checker/Date	Reviewer/Approver Date	Rev. No.
10/7/99	10-8-99	10-12-1999	0
1/10/00	1/10/00	1/10/00	1

QUALITY ASSURANCE DOCUMENT

This document has been prepared, checked, and reviewed in accordance with the Quality Assurance requirements of 10CFR50 Appendix B, as specified in the MPR Quality Assurance Manual.

MPR

MPR Associates, Inc.
320 King Street
Alexandria, VA 22314

RECORD OF REVISIONS

Calculation No.	Prepared By	Checked By	Page 2
426-001-CBS-01			

Revision	Description
0	Initial Issue
1	Revised to address minor comments from Triconex. Revisions are indicated by a bar in the right margin. Only page 25 is affected.

1. PURPOSE

The purpose of this calculation is to document a reliability/availability study of the Tricon 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 TMR PLC using a combination of modules specified in Reference 1 is analyzed for reliability and availability using a Markov model of the system. For a one year periodic test interval, the mean time to failure due to a spurious trip (MTTF) is 231.4 years resulting in an overall availability of 99.9988%. For the same test interval, the average probability of failure on demand (PFDavg) is 4.686×10^{-5} resulting in a safety availability of 99.9953%. Detailed results for different periodic test intervals are presented in Tables 4-2 and 4-3. 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 99.7121%, and the safety availability is 99.9377%. As before, both of these results exceed the recommended goal of 99% 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 Section 4.2.3.2 of Reference 1, the system in the following table is representative of the full range of components of the PLC. The Tricon TMR PLC module used to comply with the EPRI guidelines is 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.

Table 3-1. **Tricon Modules**

EPRI Section	Component Type	Range of Tricon Modules
4.2.3.2.A	3 Discrete Input Modules	3501E, 3502E, 3503E, 3504E, 3505E, 3510 (pulse input)
4.2.3.2.B	2 Analog Input Modules	3700A, 3701, 3703E, 3704E, 3706A 3708E
4.2.3.2.C	1 Analog Output Module	3805E
4.2.3.2.D	3 Discrete Output Modules	3601E, 3603E, 3604E, 3607E, 3611E, 3623, 3624
	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)	3006
4.2.3.2.I	Power Supply	8310, 8311, 8312
4.2.3.2.J	Chassis	Included in power supply
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

Notes:

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 classifed into 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:

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

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 2 and 3— Digital Input

Each digital input model is triplicated with 3-2-0 capability. Each module consists of three triplicated legs. State 2 is the failure of one of the digital input microprocessor modules. State 3 is the 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:

$$k_{1,2} = 3\, n_d\, \lambda^S{}_{ipd}$$
$$k_{1,3} = 3\, n_d\, n_{icd}\, \lambda^S{}_{icd}$$

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

$$k_{2,1} = \mu_{ipd}$$
$$k_{3,1} = \mu_{icd}$$

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

$$k_{2,12} = 2\,(\lambda^S{}_{mp} + \lambda^S{}_{ipd} + n_{icd}\, \lambda^S{}_{icd})$$
$$k_{3,12} = 2\,(\lambda^S{}_{mp} + \lambda^S{}_{ipd} + \lambda^S{}_{icd})$$

Where:

$k_{i,j}$ = Probability of transition from the i^{th} to the j^{th} state
n_d = Number of digital input modules
n_{icd} = Number of input circuits for each digital input module
$\lambda^S{}_{ipd}$ = Safe failure rate for digital input microprocessor
$\lambda^S{}_{icd}$ = Safe failure rate for digital input circuits
$\lambda^S{}_{mp}$ = Safe failure rate for main processor
μ_{ipd} = Effective repair rate of digital input microprocessor
μ_{icd} = Effective repair rate of digital input circuit

States 4 and 5—Analog Input

Each analog input model is triplicated with 3-2-0 capability. Each module consists of three triplicated legs. State 4 is the failure of one of the analog input microprocessor modules. State 5 is the 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:

$$\begin{aligned} k_{1,4} &= 3\, n_a\, \lambda^S{}_{ipa} \\ k_{1,5} &= 3\, n_a\, n_{ica}\, \lambda^S{}_{ica} \end{aligned}$$

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

$$\begin{aligned} k_{4,1} &= \mu_{ipa} \\ k_{5,1} &= \mu_{ica} \end{aligned}$$

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

$$\begin{aligned} k_{4,12} &= 2\,(\lambda^S{}_{mp} + \lambda^S{}_{ipa} + n_{ica}\, \lambda^S{}_{ica}) \\ k_{5,12} &= 2\,(\lambda^S{}_{mp} + \lambda^S{}_{ipa} + \lambda^S{}_{ica}) \end{aligned}$$

Where:

n_a = Number of analog input modules
n_{ica} = Number of input circuits for each analog input module
$\lambda^S{}_{ipa}$ = Safe failure rate for analog input microprocessor
$\lambda^S{}_{ica}$ = Safe failure rate for analog input circuits
μ_{ipa} = Effective repair rate of analog input microprocessor
μ_{ica} = Effective repair rate of analog input circuit

States 6 and 7— Digital Output

Each digital output module has a triplicated output processor with a quad voter output circuit. State 6 is the failure of one of the inputs into the digital output microprocessor modules. State 7 is the failure of one of the digital output circuits. The transitions from the initial state to the intermediate states are given by:

$$k_{1,6} = 3\, m_d\, \lambda^{S}_{opd}$$
$$k_{1,7} = 4\, m_d\, n_{ocd}\, \lambda^{S}_{ocd}$$

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

$$k_{6,1} = \mu_{opd}$$
$$k_{7,1} = \mu_{ocd}$$

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

$$k_{6,12} = 2\,(\lambda^{S}_{mp} + \lambda^{S}_{opd}) + (5\,/\,3)\, n_{ocd}\, \lambda^{S}_{ocd}$$
$$k_{7,12} = (5\,/\,4)\,(\lambda^{S}_{mp} + \lambda^{S}_{opd}) + \lambda^{S}_{ocd}$$

Where:

m_d	=	Number of digital output modules
n_{ocd}	=	Number of output circuits for each digital output module
λ^{S}_{opd}	=	Safe failure rate for digital output microprocessor
λ^{S}_{ocd}	=	Safe failure rate for digital output circuits
μ_{opd}	=	Effective repair rate of digital output microprocessor
μ_{ocd}	=	Effective repair rate of digital output circuit

States 8 and 9— Analog Output

Per Reference 8, each analog output module is triplicated for 3-2-1-0 capability meaning the triplicated input from the main processor requires three faults before a failure condition is reached. Since the probability of failure for the module is third order ($\sim\lambda^3$), its effect on the mean time to failure can be neglected. The transitions are:

$$k_{1,8} = 0$$
$$k_{1,9} = 0$$
$$k_{8,12} = 0$$
$$k_{9,12} = 0$$

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

$$k_{8,1} = \mu_{opa}$$
$$k_{9,1} = \mu_{oca}$$

Where:

μ_{opa} = Effective repair rate of analog output microprocessor
μ_{oca} = Effective repair rate of analog output circuit

State 10— Main Processor

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

$$k_{1,10} = 3\,\lambda^S{}_{mp}$$

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

$$k_{10,1} = \mu_{mp}$$

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

$$k_{10,12} = 2\,(\lambda^S{}_{mp} + n_d\,\lambda^S{}_{ipd} + n_d\,n_{icd}\,\lambda^S{}_{icd} + n_a\,\lambda^S{}_{ipa} + n_a\,n_{ica}\,\lambda^S{}_{ica} + m_d\,\lambda^S{}_{opd} + m_d\,n_{ocd}\,\lambda^S{}_{ocd})$$

Where:

μ_{mp} = Effective repair rate of main processor

State 11— Power Supply

State 11 is the failure of one of the dual power supplies in a channel. The transition from the initial state to the intermediate state is given by:

$$k_{1,11} = 2\,l\,\lambda^{S}_{ps}$$

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

$$k_{11,1} = \mu_{ps}$$

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

$$k_{11,12} = \lambda^{S}_{ps}$$

Where:

l = Number of power supplies per channel
λ^{S}_{ps} = Safe failure rate for power supply
μ_{ps} = Effective repair rate of power supply

Effects of Common Cause Failures

The effects of dual or triple mode failure is modeled directly as a transition from the initial state to the spurious trip state. The common cause failure includes two factors. The first factor (p_3) is for the chance of the remaining two channels failing after the first channel fails. Three safe failures or three dangerous detected failures of any channel would cause a spurious trip. The second factor (p_2) is for the chance of a second channel failing after the first fails. Two safe undetected failures could cause a spurious trip. Since no clear software model exists, the software contribution to common cause failure is not modeled or included. The common cause failure transition is given by:

$$
\begin{aligned}
k_{1,12} \quad = \quad & 3\, p_3\, [\lambda_{mp} - \lambda^{DU}{}_{mp} + n_d\, (\lambda_{ipd} - \lambda^{DU}{}_{ipd} + n_{icd}\, \lambda_{icd} - n_{icd}\, \lambda^{DU}{}_{icd}) + \\
& n_a\, (\lambda_{ipa} - \lambda^{DU}{}_{ipa} + n_{ica}\, \lambda_{ica} - n_{ica}\, \lambda^{DU}{}_{ica}) + \\
& m_d\, (\lambda_{opd} - \lambda^{DU}{}_{opd} + n_{ocd}\, \lambda_{ocd} - n_{ocd}\, \lambda^{DU}{}_{ocd}) + \\
& 3\, p_2\, [\lambda^{SU}{}_{mp} + n_d\, (\lambda^{SU}{}_{ipd} + n_{icd}\, \lambda^{SU}{}_{ipd}) + n_a\, (\lambda^{SU}{}_{ipa} + n_{icd}\, \lambda^{SU}{}_{ipa}) + \\
& m_d\, (\lambda^{SU}{}_{opd} + n_{ocd}\, \lambda^{SU}{}_{opd})] + 2\, p_2\, l\, \lambda_{ps}
\end{aligned}
$$

Where:

p_2 = Fraction of single module or circuit failures that result in the failure of an additional module or circuit performing the same function as the original failure

p_3 = Fraction of single module or circuit failures that result in the failure of two additional modules or circuits performing the same function as the original failure

λ_{mp} = Total failure rate of main processor

$\lambda^{DU}{}_{mp}$ = Dangerous undetected failure rate of main processor

$\lambda^{SU}{}_{mp}$ = Safe undetected failure rate of main processor

λ_{ipd} = Total failure rate of digital input microprocessor

$\lambda^{DU}{}_{ipd}$ = Dangerous undetected failure rate of analog input microprocessor

$\lambda^{SU}{}_{ipd}$ = Safe undetected failure rate of analog input microprocessor

λ_{icd} = Total failure rate of digital input circuit

$\lambda^{DU}{}_{icd}$ = Dangerous undetected failure rate of analog input circuit

$\lambda^{SU}{}_{icd}$ = Safe undetected failure rate of analog input circuit

λ_{ipa} = Total failure rate of analog input microprocessor

$\lambda^{DU}{}_{ipa}$ = Dangerous undetected failure rate of analog input microprocessor

$\lambda^{SU}{}_{ipa}$ = Safe undetected failure rate of analog input microprocessor

λ_{ica} = Total failure rate of analog input circuit

$\lambda^{DU}{}_{ica}$ = Dangerous undetected failure rate of analog input circuit

$\lambda^{SU}{}_{ica}$ = Safe undetected failure rate of analog input circuit

λ_{opd} = Total failure rate of digital output microprocessor

$\lambda^{DU}{}_{opd}$ = Dangerous undetected failure rate of digital output microprocessor

$\lambda^{SU}{}_{opd}$ = Safe undetected failure rate of digital output microprocessor

λ_{ocd} = Total failure rate of digital output circuit

$\lambda^{DU}{}_{ocd}$ = Dangerous undetected failure rate of digital output circuit

$\lambda^{SU}{}_{ocd}$ = Safe undetected failure rate of digital output circuit

λ_{ps} = Total failure rate of power supply

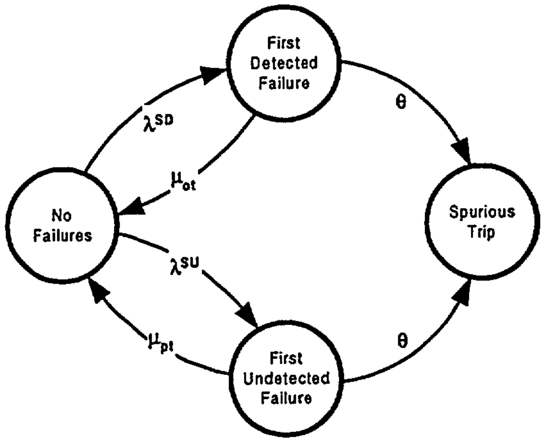
3.2.2 Solution Technique for Safe Failure Markov Model. The effective repair rate includes the repair for detected and undetected safe failures. Detected safe failures can be repaired on-line at a much faster rate. Undetected safe failures can only be repaired after the system is taken off-line for periodic 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

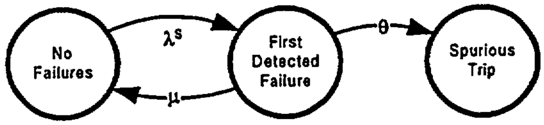
The generalized Markov model for safe failures is shown below:



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 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:

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

The MTTF can be determined from the Markov model by integrating the probability for the time that the system is in a non-failed states. States 1 through 11 are the non-failed states. Therefore, the MTTF is:

$$MTTF = \int_0^\infty [\sum_{i=1}^{11} P_i(t)]dt$$

Where:

$P_i(t)$ = Probability to be in the ith state at time t

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.

$$MTTF = \frac{1 + \sum_{i=2}^{11} \frac{\lambda_i}{\mu_i + \theta_i}}{\sum_{i=2}^{11} \frac{\lambda_i\, \theta_i}{\mu_i + \theta_i} + \lambda_{12}}$$

Making the following assignments:

λ_i = Failure rate from the initial state to the ith intermediate state
λ_i = $k_{1,i}$

θ_i = Failure rate from the i^{th} intermediate state to a spurious trip
θ_i = $k_{i,12}$
μ_i = Repair rate from the i^{th} intermediate state to the initial state
μ_i = $k_{i,1}$

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

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 only 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 ~~are~~ 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, 11, and 12—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 11 and 12 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:

$$k_{1,2} = 3\, n_d\, \lambda^{DU}_{ipd}$$
$$k_{1,3} = 3\, n_d\, n_{icd}\, \lambda^{DU}_{icd}$$

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

$$k_{2,11} = 2\,(\lambda^{DD}_{mp} + \lambda^{DD}_{ipd} + n_{icd}\, \lambda^{DD}_{icd})$$
$$k_{3,12} = 2\,(\lambda^{DD}_{mp} + \lambda^{DD}_{ipd} + \lambda^{DD}_{icd})$$
$$k_{11,2} = \mu_{ot}$$
$$k_{12,3} = \mu_{ot}$$

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

$$k_{2,20} = 2\,(\lambda^{DU}_{mp} + \lambda^{DU}_{ipd} + n_{icd}\, \lambda^{DU}_{icd})$$
$$k_{3,20} = 2\,(\lambda^{DU}_{mp} + \lambda^{DU}_{ipd} + \lambda^{DU}_{icd})$$

Where:

$k_{i,j}$ = Probability of transition from the i^{th} to the j^{th} state
λ^{DU}_{ipd} = Dangerous undetected failure rate of digital input microprocessor
λ^{DD}_{ipd} = Dangerous detected failure rate of digital input microprocessor
λ^{DU}_{icd} = Dangerous undetected failure rate of digital input circuit
λ^{DD}_{icd} = Dangerous detected failure rate of digital input circuit
λ^{DU}_{mp} = Dangerous undetected failure rate of main processor
λ^{DD}_{mp} = Dangerous detected failure rate of main processor
μ_{ot} = Repair rate when detected due to on-line testing

States 4, 5, 13, and 14—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 to an input module. States 13 and 14 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:

$$k_{1,4} = 3\, n_a\, \lambda^{DU}{}_{ipa}$$
$$k_{1,5} = 3\, n_a\, n_{icd}\, \lambda^{DU}{}_{ica}$$

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

$$k_{4,13} = 2\,(\lambda^{DD}{}_{mp} + \lambda^{DD}{}_{ipa} + n_{icd}\,\lambda^{DD}{}_{ica})$$
$$k_{5,14} = 2\,(\lambda^{DD}{}_{mp} + \lambda^{DD}{}_{ipa} + \lambda^{DD}{}_{ica})$$
$$k_{13,4} = \mu_{ot}$$
$$k_{14,5} = \mu_{ot}$$

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

$$k_{4,20} = 2\,(\lambda^{DU}{}_{mp} + \lambda^{DU}{}_{ipa} + n_{ica}\,\lambda^{DU}{}_{ica})$$
$$k_{5,20} = 2\,(\lambda^{DU}{}_{mp} + \lambda^{DU}{}_{ipa} + \lambda^{DU}{}_{ica})$$

Where:

$k_{i,j}$ = Probability of transition from the ith to the jth state
$\lambda^{DU}{}_{ipa}$ = Dangerous undetected failure rate of analog input microprocessor
$\lambda^{DD}{}_{ipa}$ = Dangerous detected failure rate of analog input microprocessor
$\lambda^{DU}{}_{ica}$ = Dangerous undetected failure rate of analog input circuit
$\lambda^{DD}{}_{ica}$ = Dangerous detected failure rate of analog input circuit

States 6, 7, 14, and 15— Digital Output

Each digital output module has a triplicated output processor with a quad voter output circuit. State 6 is the first dangerous undetected failure of a digital output microprocessor module, and state 7 is the first dangerous undetected failure of a digital output circuit from an output module. States 14 and 15 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:

$$\begin{aligned}
k_{1,6} &= 3\, m_d\, \lambda^{DU}{}_{opd} \\
k_{1,7} &= 4\, m_d\, n_{ocd}\, \lambda^{DU}{}_{ocd}
\end{aligned}$$

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

$$\begin{aligned}
k_{6,14} &= 2\,(\lambda^{DD}{}_{mp} + \lambda^{DD}{}_{opd} + n_{ocd}\, \lambda^{DD}{}_{ocd}) \\
k_{7,15} &= 2\,(\lambda^{DD}{}_{mp} + \lambda^{DD}{}_{opd} + \lambda^{DD}{}_{ocd}) \\
k_{14,6} &= \mu_{ot} \\
k_{15,7} &= \mu_{ot}
\end{aligned}$$

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

$$\begin{aligned}
k_{6,20} &= 2\,(\lambda^{DU}{}_{mp} + \lambda^{DU}{}_{opd} + n_{ocd}\, \lambda^{DU}{}_{ocd}) \\
k_{7,20} &= 2\,(\lambda^{DU}{}_{mp} + \lambda^{DU}{}_{opd} + \lambda^{DU}{}_{ocd})
\end{aligned}$$

Where:

$\lambda^{DU}{}_{opd}$ = Dangerous undetected failure rate of digital output microprocessor
$\lambda^{DD}{}_{opd}$ = Dangerous detected failure rate of digital output microprocessor
$\lambda^{DU}{}_{ocd}$ = Dangerous undetected failure rate of digital output circuit
$\lambda^{DD}{}_{ocd}$ = Dangerous detected failure rate of digital output circuit

States 8, 9, 17, and 18—Analog Output

Per Reference 8, each analog output module is triplicated for 3-2-1-0 capability meaning the triplicated input from the main processor requires three faults before a failure condition is reached. Since the probability of failure for the module is third order ($\sim\lambda^3$), its effect on the mean time to failure can be neglected. The transitions are:

$$k_{1,8} = 0$$
$$k_{1,9} = 0$$
$$k_{8,17} = 0$$
$$k_{9,18} = 0$$
$$k_{8,20} = 0$$
$$k_{9,20} = 0$$
$$k_{17,8} = \mu_{ot}$$
$$k_{18,9} = \mu_{ot}$$

State 10— Main Processor

There are triple redundant main processors. State 10 is the 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:

$$k_{1,10} = 3\,\lambda^{DU}{}_{mp}$$

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

$$k_{10,19} = 2\,[\lambda^{DD}{}_{mp} + n_d\,(\lambda^{DD}{}_{ipd} + n_{icd}\,\lambda^{DD}{}_{icd}) + n_a\,(\lambda^{DD}{}_{ipa} + n_{icd}\,\lambda^{DD}{}_{ica}) + m_d\,(\lambda^{DD}{}_{opd} + n_{ocd}\,\lambda^{DD}{}_{ocd})]$$
$$k_{19,10} = \mu_{ot}$$

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

$$k_{10,20} = 2\,[\lambda^{DU}{}_{mp} + n_d\,(\lambda^{DU}{}_{ipd} + n_{icd}\,\lambda^{DU}{}_{icd}) + n_a\,(\lambda^{DU}{}_{ipa} + n_{icd}\,\lambda^{DU}{}_{ica}) + m_d\,(\lambda^{DU}{}_{opd} + n_{ocd}\,\lambda^{DU}{}_{ocd})]$$

Effects of Common Cause Failures

The effects of dual or triple mode failure is modeled directly as a transition from the initial state to the fail-to-function state. The common cause failure includes two factors. The first factor (p_3) is for the chance of the remaining two channels failing after the first channel fails. Three safe failures or three dangerous detected failures of any channel would cause a spurious trip. The second factor (p_2) is for the chance of a second channel failing after the first fails. Two safe undetected failures would cause a spurious trip. The common cause failure transition is given by:

$$k_{1,20} = 3\,(p_2 + p_3)\,[\lambda^{DU}_{mp} + n_d\,(\lambda^{DU}_{ipd} + n_{icd}\,\lambda^{DU}_{icd}) + n_a\,(\lambda^{DU}_{ipa} + n_{icd}\,\lambda^{DU}_{ica}) + m_d\,(\lambda^{DU}_{opd} + n_{ocd}\,\lambda^{DU}_{ocd})]$$

3.3.2 Solution Techniques for Fail-to-Function 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:

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

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 20 × 20 transition matrix can be formed with each of the transition coefficients determined previously. The matrix diagonal elements (i.e., the probability of staying in the current state) is determined as the negative of the sum of the remaining transitions in a matrix row.

$$k_{i,i} = -[\sum_{j=1}^{i-1} k_{i,j} + \sum_{j=i+1}^{20} k_{i,j}]$$

Note that this is consistent with the following differential equation for remaining in the current state when assuming small time intervals and an exponential probability function for remaining in the state.

$$dP_i(t)/dt = k_{i,i}\,P_i(t)$$

The probability of being in each state at a given time can be determined by solving the system of differential equations developed using the following general formula for each of the twenty states. The rate of the change of the probability to be in a given state is equal to the probability to remain in a state plus the probability to enter the state from another state minus the probability to leave the state to another state.

$$\frac{dP_i(t)}{dt} = k_{i,i}\,P_i(t) + \sum_{j=1}^{20} k_{j,i}\,P_j(t) - \sum_{j=1}^{20} k_{i,j}\,P_i(t)$$

Where:

$P_i(t)$ = Probability to be in state i
$k_{i,j}$ = Element of transition matrix going from state i to state j
t = Time variable

The probability of failure on demand at a given time can be determined by summing the probabilities of being in a failed state (states 11 through 20) at a given time. The average probability of failure on demand can be determined by averaging the sum over the periodic test interval.

$$PFDavg = \frac{1}{PTI}\int_0^{PTI} \left[\sum_{i=11}^{20} P_i(t)\right] dt$$

Where:

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

The system of differential equations described above has been solved in Reference 5. The probability of being in an intermediate failed state (states 11 through 19) is:

$$P_i(t) = -\frac{k_{i-9,i}\,k_{1,i-9}}{\mu_{ot}\,(k_{1,1} + k_{i-9,20})}\,[e^{-k_{i-9,20}\,t} - e^{k_{1,1}\,t}]$$

Where:

μ_{ot} = Repair rate for failures detected by on-line testing

The integral of the above probability in the time domain is:

$$\int P_i(t)\,dt = \frac{k_{i-9,i}\,k_{1,i-9}}{\mu_{ot}\,(k_{1,1} + k_{i-9,20})}\,[\frac{e^{-k_{i-9,20}\,t}}{k_{i-9,20}} + \frac{e^{k_{1,1}\,t}}{k_{1,1}}]$$

The solution for the probability of being in the state of two dangerous undetected failures (state 20) is a little more complicated.

$$P_{20}(t) = -\frac{k_{1,20}}{k_{1,1}}\,(1 - e^{k_{1,1}\,t}) + \sum_{j=11}^{19}\,[\frac{-\,k_{i-9,20}\,k_{1,i-9}}{k_{1,1} + k_{i-9,20}}]\,[\frac{1 - e^{-k_{i-9,20}t}}{k_{i-9,20}} + \frac{1 - e^{k_{1,1}t}}{k_{1,1}}]$$

The integral of the above probability in the time domain is:

$$\int P_i(t)\,dt = -\frac{k_{1,20}}{k_{1,1}}\,(t - \frac{e^{k_{1,1}\,t}}{k_{1,1}}) + \sum_{j=11}^{19}\,[\frac{-k_{i-9,20}\,k_{1,i-9}}{k_{1,1} + k_{i-9,20}}]\,[\frac{t}{k_{i,20}} + \frac{e^{-k_{i-9,20}t}}{k_{i-9,20}^2} + \frac{t}{k_{1,1}} - \frac{e^{k_{1,1}t}}{k_{1,1}^2}]$$

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

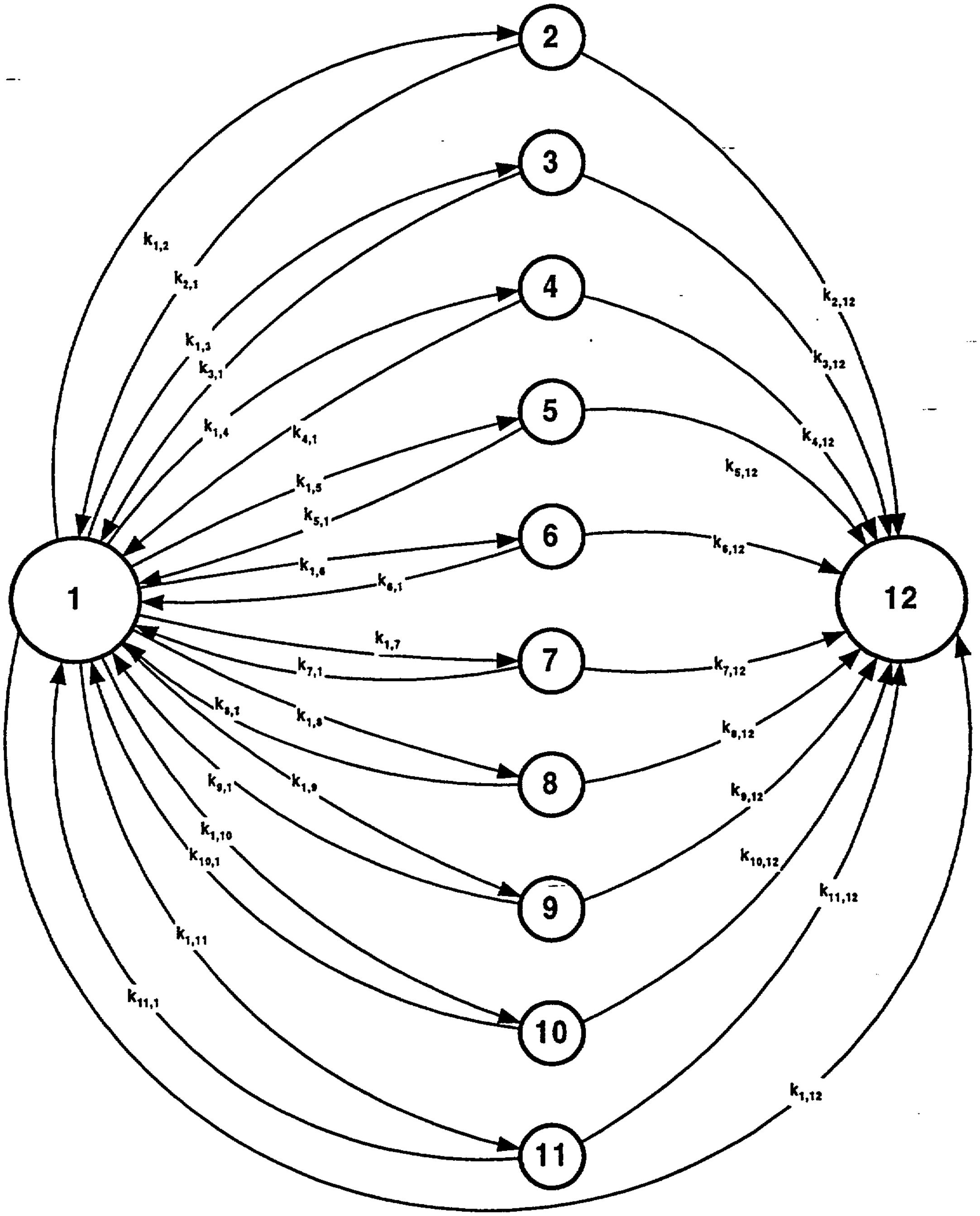


Figure 3-1. **Fail Safe Markov Model**

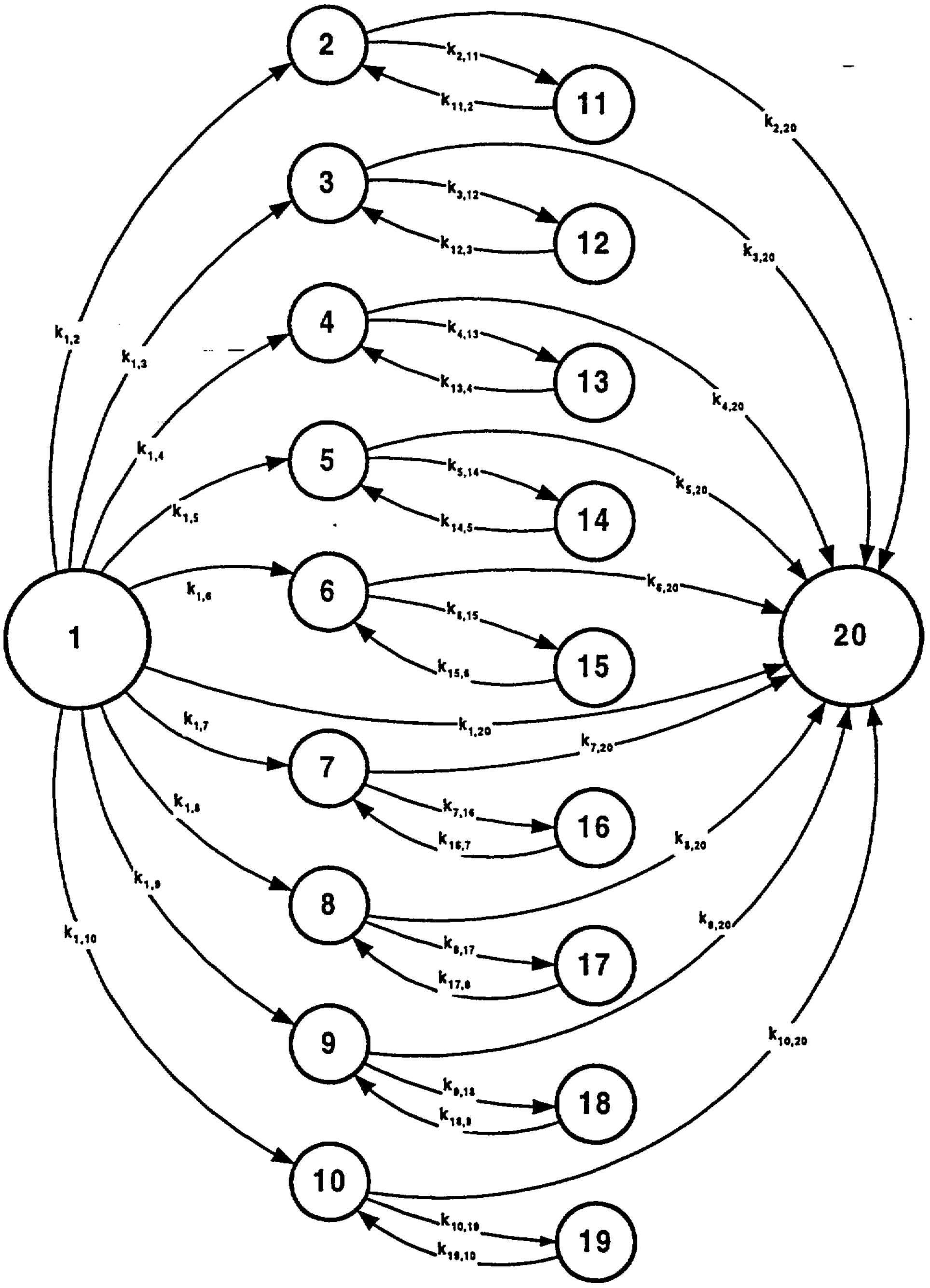


Figure 3-2. **Fail to Function Markov Model**

4. CALCULATION

4.1 Safe Failure Markov Model

The following table provides the inputs used in the model for safe failures:

Table 4-1. **Inputs to Safe Failure Markov Model**

Parameter		Value	Reference
Digital Input	Processor (n_d)	3	Ref. 1, Sec. 4.2.3.2
	Circuits (n_{icd})	0	Note 1
Analog Input	Processor (n_a)	2	Ref. 1, Sec. 4.2.3.2
	Circuits (n_{ica})	0	Note 1
Digital Output	Processor (m_d)	3	Ref. 1, Sec. 4.2.3.2
	Circuits (n_{ocd})	0	Note 1
Analog Output	Processor (m_a)	0	Note 2
	Circuits (n_{oca})	0	
Power Supplies		2	Note 3
Common Cause Failures	p_2	0	Note 4
	p_3	0	

Notes:

1. The total failure rate for the entire module (processor plus circuits) is used as the individual processor failure rate. Accordingly, the number of circuits is set to zero.

2. The analog output processors, selector circuits, and DACs are triplicated. Per Reference 8, faults in this circuit are third order effects and can be neglected in the Markov model.

3. The dual power supplies are modeled explicitly in the Markov model. Two pairs of power supplies are required for the number of modules provided. Consequently, two power supplies are input into the model.

4. Common cause failures are assumed to be zero.

The limiting failure ~~rate~~ data for each module is contained in Appendix A. The included in the data are 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 TMR. The results of the calculations are contained in the following tables.

Table 4-2. **Results of Safe Failure Markov Model**

Periodic Test Interval, months (Note 1)	Mean Time to Repair Failures Detected On-Line, hours (Note 2)	Mean Time to Failure due to a Spurious Trip		Overall Availability
		Hours	Years	
6	24	3,379,900	385.8	99.9993%
12		2,026,800	231.4	99.9988%
18		1,492,100	170.3	99.9984%
24		1,205,200	137.6	99.9980%
30		1,026,000	117.1	99.9977%

Table 4-3. **Results of Failure to Function Markov Model**

Periodic Test Interval, months (Note 1)	Mean Time to Repair Failures Detected On-Line, hours (Note 2)	Average Probability of Failure on Demand	Safety Availability
6	24	7.007×10^{-6}	99.9993%
12		4.686×10^{-5}	99.9953%
18		1.473×10^{-4}	99.9853%
24		3.351×10^{-4}	99.9665%
30		6.368×10^{-4}	99.9363%

Notes to Tables 4-2 and 4-3:

1. Per Section 4.2.3.3.B of Reference 1, availability calculations are performed for each of these periodic test intervals.

2. Per Section 4.2.3.3.C of Reference 1, the mean time to repair a failure detected on-line is equal to one day.

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. SINTEF Report STF48 F89023.

7. Factory Mutual Report FMRC J.I.003003840, "An Estimation of the Failure Rates for Modules Used in the Triconex Tricon 9 System," Volume 2, August 1999.

8. Triconex Memorandum from T. Fredrickson to M. Albers (MPR), "Markov Modeling of the TRICON Version 9," dated September 17, 1999.

Appendix A

FAILURE DATA FOR THE MOST LIMITING TRICON TMR MODULES

Module Type	Limiting Module	Total Failure Rate λ (Note 2)	Fraction Safe Failures f^S (Note 3)	Safe Failure Rate λ^S (Note 4)	Diagnostic Coverage Safe C^S (Note 3)	Safe Detected Failure Rate λ^{SD} (Note 4)	Safe Undetected Failure Rate λ^{SU} (Note 4)	Dangerous Failure Rate λ^D (Note 4)	Diagnostic Coverage Dangerous C^D (Note 3)	Dangerous Detected Failure Rate λ^{DD} (Note 4)	Dangerous Undetected Failure Rate λ^{DU} (Note 4)

----------TRICONEX PROPRIETARY---------- (b)

Appendix B

SOLUTIONS TO MARKOV MODELS

B.1 PURPOSE

The purpose of this appendix is to solve the safe failure and fail to function Markov models. The solution techniques are presented in Section 3 of the main body of the calculation. Inputs to the model are taken from Section 4 and Appendix A.

B.2 SAFE FAILURE MARKOV MODEL

For a periodic test interval of 6 months, the solution is:

Module Type	Intermediate State	First Failure Rate λ_i	Second Failure Rate θ_i	Effective Repair Rate μ_i	$\lambda_i / (\mu_i + \theta_i)$	$(\lambda_i \theta_i) / (\mu_i + \theta_i)$

	hours	years
MTTF	3379852	385.83
Availability	99.9993%	

-----------TR ICONEX PROPRIETARY-----------------

(b)

For a 12 month periodic test interval, the solution is:

Module Type	Intermediate State	First Failure Rate λ_i	Second Failure Rate θ_i	Effective Repair Rate μ_i	$\lambda_i / (\mu_i + \theta_i)$	$(\lambda_i \theta_i) / (\mu_i + \theta_i)$

------------TR ICONEX PROPRIETARY-------------------

(b)

	hours	years
MTTF	2026807	231.37
Availability	99.9988%	

For an 18 month periodic test interval, the solution is:

Module Type	Intermediate State	First Failure Rate λ_i	Second Failure Rate θ_i	Effective Repair Rate μ_i	$\lambda_i / (\mu_i + \theta_i)$	$(\lambda_i \theta_i) / (\mu_i + \theta_i)$

---------------TRICONEX PROPRIETARY-------------------------------

(b)

	hours	years
MTTF	1492134	170.33
Availability	99.9984%	

For a 24 month periodic test interval, the solution is:

Module Type	Intermediate State	First Failure Rate λ_i	Second Failure Rate θ_i	Effective Repair Rate μ_i	$\lambda_i / (\mu_i + \theta_i)$	$(\lambda_i \theta_i) / (\mu_i + \theta_i)$

------------TRICONEX PROPRIETARY------------ (b)

	hours	years
MTTF	1205222	137.58
Availability	99.9980%	

For a 30 month periodic test interval, the solution is:

Module Type	Intermediate State	First Failure Rate λ_i	Second Failure Rate θ_i	Effective Repair Rate μ_i	$\lambda_i / (\mu_i + \theta_i)$	$(\lambda_i \theta_i) / (\mu_i + \theta_i)$

---------------TRICONEX PROPRIETARY------------ (b)

	hours	years
MTTF	1026019	117.13
Availability	99.9977%	

B.3 FAIL TO FUNCTION MARKOV MODEL

The transition matrix for the fail to function Markov model is:

---------------TRICONEX PROPRIETARY--------------------- (b)

For a periodic test interval of 6 months, the solution is:

Markov State		P(t) Evaluated at		Average Probability to be in State
State	From State	Time t = 0	Time t = 4380	
			PFDavg	7.007E-06
			Safety Availability	99.9993%

----------TRICONEX PROPRIETARY---------- (b)

For a periodic test interval of 12 months, the solution is:

Markov State		P(t) Evaluated at		Average Probability to be in State
State	From State	Time t = 0	Time t = 8760	
			PFDavg Safety Availability	4.686E-05 99.9953%

(b)

---TRICONEX PROPRIETARY---

For a periodic test interval of 18 months, the solution is:

Markov State		P(t) Evaluated at		Average Probability to be in State
State	From State	Time t = 0	Time t = 13140	
			PFDavg Safety Availability	1.473E-04 99.9853%

(b)

---TR ICONEX PROPRIETARY---

Calculation No.	Prepared By	Checked By	Page B-7
426-001-CBS-01			

For a periodic test interval of 24 months, the solution is:

Markov State		P(t) Evaluated at		Average Probability to be in State
State	From State	Time t = 0	Time t = 17520	
			PFDavg	3.351E-04
			Safety Availability	99.9665%

(b)

TRICONEX PROPRIETARY

For a periodic test interval of 30 months, the solution is:

Markov State		P(t) Evaluated at		Average Probability to be in State
State	From State	Time t = 0	Time t = 21900	
			PFDavg	6.368E-04
			Safety Availability	99.9363%

(b)

TRICONEX PROPRIETARY

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 TMR PLC during a two week period after an accident.

C.2 RESULTS

For a two week post accident period, the overall availability is 99.7121%, and the safety availability is 99.9377%. Both of these values are greater than the recommended goal of 99% per Reference 1.

C.3 DISCUSSION

Post accident environmental conditions are more severe than the usual operating conditions of the Tricon PLC Controller. 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:

$$\lambda = (C_1 \pi_T + C_2 \pi_E) \pi_Q \pi_L \qquad \text{(Reference 3)}$$

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.

C.4 CALCULATION

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. As required by Section 4.2.3.3.F of Reference 1, the availability is calculated for the entire two week period. The calculations are contained in the following tables.

The overall availability is calculated in the following table. Note that the effective repair rates are determined assuming that the undetected failures cannot be repaired for at least the two week post accident period.

Module Type	Intermediate State	First Failure Rate λ_i	Second Failure Rate θ_i	Effective Repair Rate μ_i	$\lambda_i / (\mu_i + \theta_i)$	$(\lambda_i \theta_i) / (\mu_i + \theta_i)$

	hours	years
MTTF	8313	0.95
Availability	99.7121%	

------------TR ICONEX PROPRIETARY----------------

(b)

The transition matrix for the fail to function Markov model is given below. All failure rates are increased by a factor of 40; all repair rates are unchanged from previous evaluations.

(b)

TRICONEX PROPRIETARY

The safety availability for the two week post accident period is calculated below.

Markov State		P(t) Evaluated at		Average Probability to be in State
State	From State	Time t = 0	Time t = 336	
			PFDavg	6.234E-04
			Safety Availability	99.9377%

(b)

TRICONEX PROPRIETARY

TRICONEX

TRICONEX PROPRIETARY (attached pages only)
(attached pages deleted in non-proprietary version) (a)

Project:	NUCLEAR QUALIFICATION OF TRICON PLC SYSTEM
Purchase Order No.:	ST - 401734
Project Sales Order:	7286

CERTIFICATE OF CONFORMANCE

NUCLEAR QUALIFICATION TEST SPECIMEN

Document No: 7286-542

Revision 0

July 21, 2000

This is to certify that the items listed on the attached pages, as supplied for use in the Nuclear Qualification Test Specimen, met Triconex specifications for standard products produced in accordance with the Triconex Quality Program.

The Nuclear Qualification Test Specimen, as defined in Project documents and drawings, was assembled and inspected in accordance with Sales Order 7286/1388 and applicable drawings. Quality Assurance records for this equipment are on file.

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

7/21/00

A. Faber
Director, Product Assurance
TRICONEX CORPORATION

Date

TRICONEX

Project:	NUCLEAR QUALIFICATION OF TRICON PLC SYSTEM
Purchase Order No.:	ST - 401734
Project Sales Order:	7286

MASTER CONFIGURATION LIST (MCL)

Document No: 7286-540

Revision 22

September 29, 2000

NON-PROPRIETARY MARKUP VERSION
- Areas of proprietary information blanked.
- Adjacent letter (a, b, c, d, e, f) corresponds to Triconex proprietary policy categories (ref. 7/17/00 letter to NRC, Affidavit, section 5).

	Name	Signature	Title
Approvals:	Mitch Albers		Project Manager
	Gary McDonald		Nuclear Quality Engineer

TRICONEX

Document:	7286-540	**Title:**	MASTER CONFIGURATION LIST		
Revision:	22	**Page:**	2 of 18	**Date:**	9/29/2000

Document Ch[redacted]

Revision	[redacted]
0	[redacted]
1	[redacted]
2	[redacted]
3	[redacted]
4	[redacted]
5	[redacted]
6	[redacted]
7	[redacted]
8	[redacted]
9	[redacted]
10	[redacted]
11	[redacted]
12	[redacted]
13	[redacted]
14	[redacted]
15	[redacted]
16	[redacted]
17	[redacted]
18	[redacted]
19	[redacted]
20	[redacted]
21	[redacted]
22	[redacted]

(a)

1. PROJECT REQUIREMENTS DOCUMENTS- (Current Issue)

Document Description	Document Number	Revision	Date
STP Purchase Order/TOC	ST-401734	Rev 0	12/9/97
		Supplement 1	4/8/98
EPRI Specification	TR 107330	Rev 0	December 1996
			(final report)
Project Directives	(None issued. See Compliance Matrix in Summary Report)		

2. PROJECT QUALITY PLAN

Quality Plan	QPL-01	Rev 3	7/20/99

3. TEST PROCEDURES/DOCUMENTS

PROJECT TEST PROCEDURES			
PROCEDURE NO.	DESCRIPTION	REV. NO.	TCN
7286-500	Master Test Plan	3	
7286-502	System Set-up and Check-out Test	2	
7286-503	Operability Test	2	
7286-504	Prudency Test	2	
7286-506	Environmental Test	0	
7286-507	Seismic Test	0	
7286-508	Surge Test	1	
7286-509	Class 1E to Non 1E Isolation Test	0	
7286-510	EMI/RFI Test	1	
7286-513	TSAP Validation Procedure	0	
46992-10	Wyle EMI Test Procedure	B	
46992-20	Wyle Environmental & Seismic Test Procedure	A	

OTHER PROJECT DOCUMENTS

DOCUMENT NO.	DESCRIPTION	REV. NO.	
7286-517	TSAP Functional Requirements Specification	1	
7286-518	TSAP Design Specification	1	
7286-519	TSAP Program Listing	4	
7286-520	Simulator Program Description	2	
7286-521	Simulator/EMI Program Description	0	
7286-524	Pre-Qualification Test Report	0	
7286-525	Environmental Test Report	0	
7286-526	Seismic Test Report	0	
7286-527	EMI/RFI Test Report	0	
7286-528	Surge Test Report	0	
7286-529	Class 1E to Non 1E Isolation Test Report	0	
7286-530	Performance Proof Test Report	0	
7286-531	Reliability/Availability Study	0	
7286-532	Failure Modes & Effects Analysis (FMEA)	0	
7286-533	Radiation Hardness Evaluation	1	
7286-534	Tricon System Accuracy Specification	1	
7286-535	Software Qualification Report	1	
7286-536	TSAP V&V Report	0	
7286-537	Software QA Plan	2	
7286-540	Master Configuration List	22	
7286-541	Tricon Test Specimen Description	0	
7286-542	Certificate of Conformance	0	
7286-545	Qualification Summary Report (Final)	1	
41339-1	Wyle Test Report – Environmental & Seismic	A	
41339-2	Wyle Test Report – EMI Testing	0	

4. PROJECT DRAWINGS

INTEGRATION DRAWING LIST
(All drawings as-built per DRR – 010)

DRAWING NO.	REV.	DESCRIPTION	REF. DRR
Arrangement & Wiring			
7286-001 SHT 1			
7286-001 SHT 2			
7286-001 SHT 3			
7286-100 SHT 1			
7286-100 SHT 2			
7286-100 SHT 3			
7286-100 SHT 4			
7286-101 SHT 1			
7286-101 SHT 2			
7286-102 SHT 1			
7286-102 SHT 2			
7286-103			
7286-200			
7286-201 SHT 1			
7286-201 SHT 2			
7286-202			
7286-203 SHT 1			
7286-203 SHT 2			
7286-204 SHT 1			
7286-204 SHT 2			
7286-205 SHT 1			
7286-205 SHT 2			
7286-206			
7286-207			
7286-300			
7286-301			
7286-302			
7286-303			
7286-304			
7286-305			
7286-306			
7286-307 SHT 1			
7286-307 SHT 2			
7286-308			
7286-309			
7286-310 SHT 1			
7286-310 SHT 2			

(a)

DRAWING NO.	REV.	DESCRIPTION	REF. DRR
7286-311			
7286-312			
7286-313			
7286-314			
7286-315			
7286-316			
7286-317			
7286-318			
7286-319			
7286-320			
7286-321			
7286-322			
7286-324 SHT 1			
7286-324 SHT 2			
7286-324 SHT 3			
7286-325 SHT 1			
7286-325 SHT 2			
7286-325 SHT 3			
7286-326 SHT 1			
7286-326 SHT 2			
7286-326 SHT 3			
7286-327 SHT 1			
7286-327 SHT 2			
7286-327 SHT 3			
7286-328 SHT 1			
7286-328 SHT 2			
7286-328 SHT 3			
7286-329 SHT 1			
7286-329 SHT 2			
Functional			
7286-430			
7286-431			
7286-432, SHT 1			
7286-432, SHT 2			
7286-432, SHT 3			
7286-432, SHT 4			
7286-432, SHT 5			
7286-433			
7286-434			
7286-435			
7286-436 SHT 1			
7286-436 SHT 2			
7286-436 SHT 3			
7286-437			
7286-438 SHT 1			
7286-438 SHT 2			
7286-439			

(a)

DRAWING NO.	REV.	DESCRIPTION	REF. DRR
7286-440 SHT 1			
7286-440 SHT 2			
7286-440 SHT 3			
7286-440 SHT 4			
7286-441			
7286-442			
7286-443 SHT 1			
7286-443 SHT 2			
7286-443 SHT 3			
7286-443 SHT 4			
7286-443 SHT 5			
7286-443 SHT 6			
7286-443 SHT 7			
7286-443 SHT 8			
7286-443 SHT 9			
7286-443 SHT 10			
7286-443 SHT 11			
7286-444 SHT 1			
7286-444 SHT 2			
Loop			
7286-531 SHT 1			
7286-531 SHT 2			
7286-532 SHT 1			
7286-532 SHT 2			
7286-532 SHT 3			
7286-532 SHT 4			
7286-532 SHT 5			
7286-532 SHT 6			
7286-532 SHT 7			
7286-532 SHT 8			
7286-532 SHT 9			
7286-532 SHT 10			
7286-532 SHT 11			
7286-532 SHT 12			
7286-533 SHT 1			
7286-533 SHT 2			
7286-533 SHT 3			
7286-534 SHT 1			
7286-534 SHT 2			
7286-535 SHT 1			
7286-535 SHT 2			
7286-536 SHT 1			
7286-536 SHT 2			
7286-536 SHT 3			
7286-537 SHT 1			
7286-537 SHT 2			

(a)

TRICONEX

Document:	7286-540	**Title:**	**MASTER CONFIGURATION LIST**		
Revision:	22	**Page:**	8 of 18	**Date:**	9/29/2000

DRAWING NO.	REV.	DESCRIPTION	REF. DRR
7286-537 SHT 3	[redacted]	[redacted]	[redacted]
7286-538 SHT 1	[redacted]	[redacted]	[redacted]
7286-538 SHT 2	[redacted]	[redacted]	[redacted]
7286-538 SHT 3	[redacted]	[redacted]	[redacted]
7286-539 SHT 1	[redacted]	[redacted]	[redacted]
7286-539 SHT 2	[redacted]	[redacted]	[redacted]
7286-540 SHT 1	[redacted]	[redacted]	[redacted]
7286-540 SHT 2	[redacted]	[redacted]	[redacted]
7286-540 SHT 3	[redacted]	[redacted]	[redacted]
7286-540 SHT 4	[redacted]	[redacted]	[redacted]
7286-540 SHT 5	[redacted]	[redacted]	[redacted]
7286-540 SHT 6	[redacted]	[redacted]	[redacted]
7286-540 SHT 7	[redacted]	[redacted]	[redacted]
7286-540 SHT 8	[redacted]	[redacted]	[redacted]
7286-541 SHT 1	[redacted]	[redacted]	[redacted]
7286-541 SHT 2	[redacted]	[redacted]	[redacted]
7286-542 SHT 1	[redacted]	[redacted]	[redacted]
7286-542 SHT 2	[redacted]	[redacted]	[redacted]
7286-542 SHT 3	[redacted]	[redacted]	[redacted]
7286-543 SHT 1	[redacted]	[redacted]	[redacted]
7286-543 SHT 2	[redacted]	[redacted]	[redacted]
7286-543 SHT 3	[redacted]	[redacted]	[redacted]
7286-543 SHT 4	[redacted]	[redacted]	[redacted]
7286-543 SHT 5	[redacted]	[redacted]	[redacted]
7286-543 SHT 6	[redacted]	[redacted]	[redacted]
7286-543 SHT 7	[redacted]	[redacted]	[redacted]
7286-543 SHT 8	[redacted]	[redacted]	[redacted]
7286-543 SHT 9	[redacted]	[redacted]	[redacted]
7286-543 SHT 10	[redacted]	[redacted]	[redacted]
7286-543 SHT 11	[redacted]	[redacted]	[redacted]
7286-543 SHT 12	[redacted]	[redacted]	[redacted]
7286-543 SHT 13	[redacted]	[redacted]	[redacted]
7286-543 SHT 14	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]

(a)

TRICONEX

Document:	7286-540	**Title:**	MASTER CONFIGURATION LIST		
Revision:	22	**Page:**	9 of 18	**Date:**	9/29/2000

5. PROJECT SOFTWARE CONFIGURATION LIST *

TYPE	**IDENTIFICATION**	**VERSION**
PROGRAMMING SOFTWARE	TriStation 1131 (Qualified under this project)	2.0, B215
	TriStation MSW (used for initial TSAP) (1)	
FIRMWARE	TSX	
	IOC	
	COM	
	ICM	
	ACMX	
	NCMX	
	IICX	
	RXM	
	AI/NITC	
	EIAI/ITC	
	PI	
	EDI	
	HDI	
	EAO	
	EDO	(a)
	SDO	
	ERO	
	TSDO	
APPLICATION SOFTWARE /TSAP (2)	TSAP-TUT (EMI/RFI, Surge, Iso testing only)	5.0
	TSAP-TUT (All other testing)	4.0
		(a)

*) Software qualified 1E per Qualification Summary Report 7286-545, except as noted

(1) TriStation MSW not qualified for use in 1E applications. Used for test program only.

(2) Not qualified. Application programs only used for the test program.

6. MODULE CONFIGURATION DATA *

MODULE TYPE/DESCRIPTION	
Chassis	
8110 Main Chassis	
8111 Expansion Chassis	
8112 Remote Expansion Chassis	
Additional standard mounting bracket for rear of chassis above	
Power Supply	
8310 High Density Power Module, 115 V	
8311 High Density Power Module, 24 VDC	
8312 High Density Power Module, 230 VAC	(1)
Main Processor	
3006 Enhanced Main Processor II, V9, 2 Mb	
Remote Extender	
4210 Remote Extender Module	
4211 Remote Extender Module	
Communication	
4119A E. I. C. M., V9, Isolated	
4329 Network Communication Module, V9	
4609 Advanced Communication Module	
Analog Input	
3700A AI Module, 0-5 VDC, 6% Overrange	
3701 AI Module, 0-10 VDC	
3703E EAI Module, Isolated	
3704E HDAI Module, 0-5/0-10 VDC	
Analog Output	
3805E Analog Output Module, 4-20 mA	

*) Modules qualified 1E per Qualification Summary Report 7286-545, except as noted. See notes next page.

(a)

6. MODULE CONFIGURATION DATA (continued) *

MODULE TYPE/DESCRIPTION	
Digital Input	
3501E EDI Module, 115V AC/DC	
3502E EDI Module, 48V AC/DC	
3503E EDI Module, 24V AC/DC	
3504E HDDI Module, 24/48 VDC (24V)	
3505E EDI Module, 24 VDC, Low Threshold	
Digital Output	
3601E EDO Module, 115 VAC	
3603E EDO Module, 120 VDC	(2)
3603T EDO Module, 120 VDC (3603E replacement during Surge test)	
3604E EDO Module, 24 VDC	
3607E EDO Module, 48 VDC	
3611E SDO Module, 115 VAC	(3)
3623 SDO Module, 120 VDC	
3624 SDO Module, 24 VDC	
Pulse Input	
3510 Pulse Input Module	
Thermocouple	
3706A NITC Input Module	
3708E ITC Thermocouple Input Module	
Relay Output	
3636R ERO Module, N.O., Simplex	
Miscellaneous	
8105 Blank Module Panel	
8107 Seismic Balance Module	

(a)

*) Modules qualified 1E per Qualification Summary Report 7286-545, except as noted.

(1) Incomplete qualification on 230 VAC module. EMI and Surge Tests not completed.

(2) 3603E not qualified. Alternate module 3603T qualified.

(3) 3611E not qualified. Dropped from list during testing.

All modules: See Summary Report for specific qualification envelopes/exceptions.

7. TERMINATION PANELS *

	[redacted]
TERM. MODEL	
2790-310T	
2750-8	
2750-8	
9753-110 **	
2752-2	
(a) [redacted]	
2760-2	
2756-2	
2755-6	
2554-6	
2852-1	
2553-6	
2553-6	
2652-1	
9662-610 **	
2657-1	
2551-1	
2651-1	
9661-910 **	
(a) [redacted]	
9661-510 **	
(a) [redacted]	
9661-910 **	
2658-1	
2552-6	
	(a) [redacted]

*) All ETA panels 1E qualified per Qualification Summary Report 7286-545

**) Version 9 Termination Panels r [redacted] (a)

8. STANDARD CONNECTING CABLES *

PART NUMBER
4000016-050 (1)
4000015-050 (1)
1600010-015
4000056-099
4000056-006
CS5020 (AMP)
4000093-310
4000093-510
4000094-110
4000094-110
4000094-110
4000094-310
4000103-510
4000104-110
4000104-210
4000104-310
4000104-310
4000111-110
4000115-210
4000115-310
4000116-510
4000117-110
4000118-510
4000118-510
4000118-510
4000118-510
4000118-510
4000127-510

(a)

(a)

*) Connecting cables qualified 1E per Qualification Summary Report 7286-545, except as noted.
(1) Passed tests, but not considered 1E service connection.

9. RTD TERMINATION PANEL SIGNAL CONDITIONERS *

PART NUMBER
1600024-010
1600024-020
1600024-030
1600024-040
1600024-050 (1)
1600024-070 (1)

*) Signal Conditioners qualified 1E per Qualification Summary Report 7286-545, except as noted.
(1) Not qualified. Not specifically tested.

(b)

10. THIRD PARTY/INTEGRATION MATERIALS REQUIRING TRACEABILITY **

INTEGRATION COMPONENTS/MATERIALS		
DESCRIPTION	IPS/Part No.	S. N.
24 VDC Power Supply (Reference Dwg. 7286-10		
24 VDC Power Supply (Partially tested in conj of, the TRICON Test Specimen being qualified)		

(b)

**) Incomplete qualification on Lambda Power Supply. EMI and Surge Tests not completed.

(a)

11. TEST SPECIMEN VERSION: TRICON V9.3.1

(a)

(a)

(a)

(a)