



## **White Paper**

# **A Hybrid Fault Tolerant Architecture**

**New Levels of Performance, Availability and Safety Integrity**

Project:  
RTP 3000 System

Customer:  
RTP Corporation  
Pompano Beach, FL  
USA

Contract No.: Q06/10-16  
Report No.: RTP 06/10-16 R002  
Version V1, Revision R2, August 27, 2008  
William Goble - John C. Grebe



## Management summary

The RTP 3000 SIS System has a hybrid architecture that uses a set of advanced design techniques to provide SIL 3 safety integrity and high availability. Safety integrity and high availability are achieved on a system that also provides an unusual level of architecture flexibility and computing speed (5 msec. scan rates). This combination of safety integrity, high availability, flexibility and performance sets new levels of expectation among safety PLC users.

Architectures available include:

Input Module: Single 1oo1, Dual 1oo2, Triple 2oo3

CPU Module: Single 1oo1, Dual 1oo2, Triple 2oo3

Output Module: Single 1oo1D, Dual 2oo2D

Each subsystem and each I/O module can have a different architecture depending on the criticality of application functions using those modules. In this way a cost optimized system based on application risk can be designed.

Input modules with a single (1oo1) architecture provide cost effective inputs with a safety integrity rating of SIL 2. The dual architecture (1oo2) will provide high safety integrity to a rating of SIL 3. The triple architecture (2oo3) is used to provide higher availability of the input subsystem. Diagnostics are primarily provided via comparison in the Node Processor.

Node Processor modules can be configured with single, dual and triple architectures. The single (1oo1) architecture is the base configuration. A dual architecture (1oo2) is used to achieve high safety integrity. A triple architecture (2oo3) is used to achieve both safety integrity and high availability. Comparison diagnostics between the Node Processors provide high effectiveness fault detection even with transient bit errors and soft failures in small geometry integrated circuits. The approach of using detail comparison instead of extensive self-diagnostics also frees computing power to ensure higher application function performance.

Output modules with a single (1oo1D) architecture will provide high safety integrity to a rating of SIL 3 with no redundancy. The dual (2oo2D) architecture is used to provide higher availability for each output subsystem. Single channel safety integrity is achieved through automatic diagnostics which will initiate an output shutdown if potentially dangerous failures are detected. The diagnostics are run locally in the output module, in the chassis (I/O) processor and in some cases in the node processor.

A Markov model was developed to analyze the behavior of the RTP 3000 SIS system under fault conditions for two common configurations:

1. Maximum Safety (1oo2, 1oo1D)
2. Maximum Availability and Safety (2oo3, 2oo2D)

Using the Markov models and the failure rates from the FMEDA, example average Probability of Failure on Demand ( $PFD_{AVG}$ ) and Mean Time To Fail Spurious (MTTFS) values are calculated.

The results confirm the level of high safety integrity and high availability achieved by the design.



## Table of Contents

Management summary .....	2
1 Purpose and Scope .....	4
2 INTRODUCTION .....	5
2.1 Relay Based Redundant Systems .....	5
2.2 Redundant PLC Based Systems .....	5
2.3 Automatic Self-Diagnostics .....	6
2.4 Common Cause .....	7
3 RTP 3000 System .....	8
3.1 Configuration 1 .....	8
3.2 Configuration 2 .....	9
3.3 Physical Implementation .....	9
4 Markov Analysis .....	10
4.1 Failure rates .....	10
4.2 Assumptions .....	12
4.3 RTP 3000 SIS Configuration 1 – Safety Integrity .....	13
4.4 RTP 3000 SIS Configuration 2 – High Availability and Safety Integrity .....	16
5 Discussion of the Markov modeling results .....	21
6 Summary .....	22
7 Terms and Definitions .....	23
8 Project management .....	24
8.1 <i>exida</i> .....	24
8.2 Roles of the parties involved .....	24
8.3 Standards / Literature used .....	24
8.4 Reference documents .....	25
8.4.1 Documentation generated by <i>exida and RTP</i> .....	25
9 Status of the document .....	26
9.1 Liability .....	26
9.2 Releases .....	26
9.3 Future Enhancements .....	26
9.4 Release Signatures .....	26



## 1 Purpose and Scope

This report is prepared to explain the background, concepts and implementation of the RTP 3000 SIS System architecture. The redundancy options and the reasoning for using each option are reviewed. A detailed Markov model was developed to analyze the behavior of the RTP 3000 SIS system. This model is presented and sample results are calculated using failure rates obtained from a Failure Modes, Effects and Diagnostic Analysis (FMEDA).

## 2 INTRODUCTION

One important goal of any automation system design is to provide correct operation at all times. The system should be 100% available (availability) and without error (safety integrity). Many design techniques have been used in the attempt to meet that goal. One fundamental concept in virtually all designs is the use of extra components to provide functional redundancy. This design technique has been used with more or less success for many decades. The key question is “How does one get the redundant operational component to transparently replace the faulty component?”

### 2.1 Relay Based Redundant Systems

Early relay logic systems incorporated redundant relays that would continue to operate transparently for some failures. Four architectures became well known starting in the 1930's. These are shown in Table 1.

**Table 1: Relay Logic Architectures**

Name	Redundancy	Failure Mode Tolerance: De-energize to trip
1oo1	None-single	None
1oo2	Dual	Contact Short Circuit
2oo2	Dual	Contact Open Circuit
2oo3	Triple	Short and Open Circuit

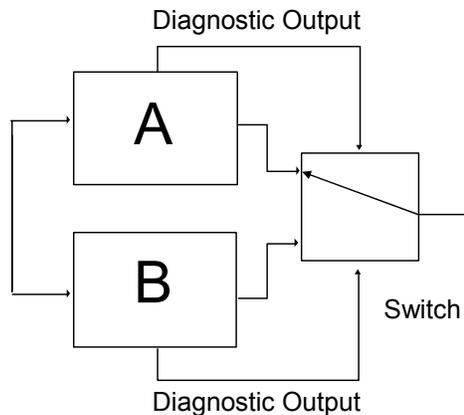
For example, the 1oo2 architecture would use two relay contacts wired in series. If one contact failed short circuit, the other contact would still open the circuit. Only if both contacts failed short circuit did the assembly fail short circuit. The disadvantage of this circuit is that the open circuit failure rate doubled since the circuit would fail open circuit if either contact failed open circuit. It can be seen that the only architecture that could tolerate both short circuit and open circuit failures is the 2oo3. A full description of all architectures is available in [N3, Chapter 14].

One issue with these designs was that any failure tolerated by the design would become hidden. Normal operation would continue even though individual relays had failed. When this happened, the fault tolerance was lost but the failure was typically not known to the operator or responsible maintenance personnel. A second failure would fail the system. Thus, the systems required frequent manual inspection and testing to prove that all the relays still worked completely. The operational cost of manual proof testing was high and this activity often was not performed. Without the frequent manual proof testing, the advantage of the redundancy was lost.

### 2.2 Redundant PLC Based Systems

When programmable logic controllers (PLC) were created in the 1970's to replace relay logic new concepts were possible. Automatic self-diagnostics were now possible. A simple “watchdog timer” circuit could detect between 60% and 75% of the CPU failures and became a standard part of each design. Other diagnostics were added subject to the limitations of the computing speed. Extensive diagnostics were not possible without using up all the CPU time.

With electronic input/output circuits and switching speeds faster than relays, it was possible and deemed practical to switch from one set of electronics to a backup set. Several manufacturers provided a level of fault tolerance via this “hot-standby” approach. The concept is shown in Figure 1.



**Figure 1: Hot-Standby Architecture**

The system would switch from A to B depending on diagnostic signals from the two CPU units (typically from the watchdog timer circuits). The switch would select whichever unit indicated it was good. This design could indeed provide good fault tolerance but depended on the automatic diagnostics. If the diagnostics did not detect a failure, the switch would not select the good unit. Reliability models show that if the diagnostics do not have an effectiveness in the 90% range, the overall availability of this design will not be better than a single unit [N3, Chapter 9].

### **2.3 Automatic Self-Diagnostics**

Diagnostic techniques were developed and improved through the succeeding generations of programmable logic controllers. Automatic self-diagnostics in single units compared measured signals to known references. When the signal varied by more than the allowed amount a fault was declared. FMEDA techniques were developed to measure the diagnostic effectiveness [N6, N7]. FMEDA analysis would show that new techniques were quite effective. However, these advanced self-diagnostic techniques consumed large amounts of computing time. Safety PLC designs were plagued with long program scan times (seconds) and some units even allowed the diagnostic time to be configurable to allow the end user to make the tradeoff between diagnostic timing and program scan time.

In systems with more than one CPU, comparison diagnostics could be done. Comparisons could be made between input scans, intermediate calculations and output results. Comparison diagnostics could also consume processing time but were generally more effective with less overall computing time than reference diagnostics. Therefore comparison diagnostics are used for the CPU in most safety PLC designs through today.

Fully triplicate designs with comparison diagnostics became the choice of many systems designed in the 1970's through the 1990's. In order to take full advantage of the comparisons, input and output circuitry was triplicated as well. These designs could be economically done by putting the triplicate circuitry on the same circuit board or even in the same integrated circuit.



## 2.4 Common Cause

Research published in the 1990's [N8] has shown that redundant systems can fail at the same time due to a common stress. This is known as a "common cause" failure. The impact of common cause on a redundant architecture is very significant and can ruin the safety integrity and availability of a design [N9]. The primary defense against common cause failure mechanisms is the use of diverse design redundant components or physical separation of redundant components [N10, N11]. Designers of recent systems have learned never to put redundant circuitry into a common integrated circuit and preferably never put redundant circuitry on the same circuit board.

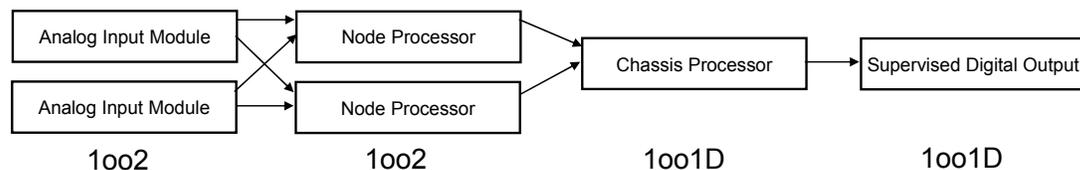
### 3 RTP 3000 System

The RTP 3000 System consists of Chassis assemblies, power supplies, Node Processors, Chassis Processors, Ethernet based communications and I/O modules of various types.

The 3000 System offers great flexibility in architecture with many variations possible. Two specific configurations show the primary attributes of the design:

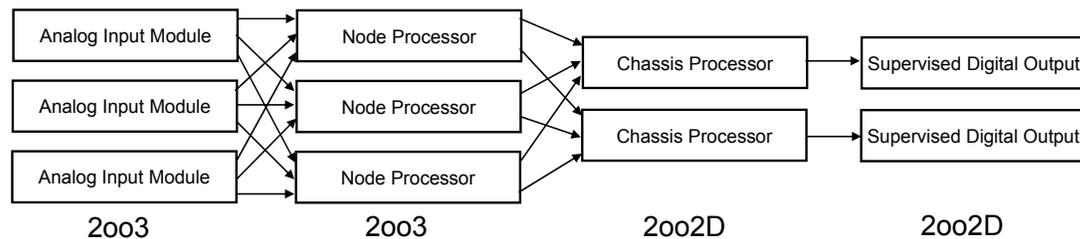
- Configuration 1 will achieve maximum safety integrity with SIL 3 capability using the minimum amount of hardware.
- Configuration 2 will achieve maximum availability and safety integrity with SIL 3 capability.

Configuration 1 is a hybrid architecture logically viewed as a combination 1oo2 and 1oo1D as shown in Figure 2. This architecture shows high safety integrity with a minimum number of modules.



**Figure 2: Logical Architecture of Configuration 1**

Configuration 2 is a hybrid architecture logically viewed as a combination 2oo3 and 2oo2D as shown in Figure 3. This architecture shows high availability and high safety integrity.



**Figure 3: Logical Architecture of Configuration 2**

#### 3.1 Configuration 1

Configuration 1 shows some of the basic design concepts used to achieve safety integrity in the RTP 3000. Input modules and the Node Processor are duplicated with diagnostic capability provided by comparison diagnostics. Comparisons are made of the input scans, intermediate results and calculated results. This comparison will detect an estimated 99% of failures that may be potentially dangerous. Additional self-diagnostics are performed by the Chassis Processor on the Node Processor, itself and the Output modules. Overall the combination of comparison diagnostics and automatic self-diagnostics provides an extremely high level of diagnostic effectiveness (99+%).



Without redundancy, the Chassis Processor and the Output modules form a 1oo1D architecture. This architecture is highly dependent on effective diagnostics to achieve safety integrity and the RTP 3000 provides this level via many methods including automatic dynamic pulse injection with full output read-back, redundant output switching, multiple independent watchdog timers and specific message comparison done with application specific integrated circuits (ASIC). Specific diagnostics are included that will detect failures in the diagnostic circuitry.

Common cause defense is provided to the maximum practical level via physical separation. Redundant circuitry is provided on separate modules, even for the Node Processor. No redundant circuits are implemented in a single integrated circuit, even functional and diagnostic circuits are placed in separate integrated circuits.

### **3.2 Configuration 2**

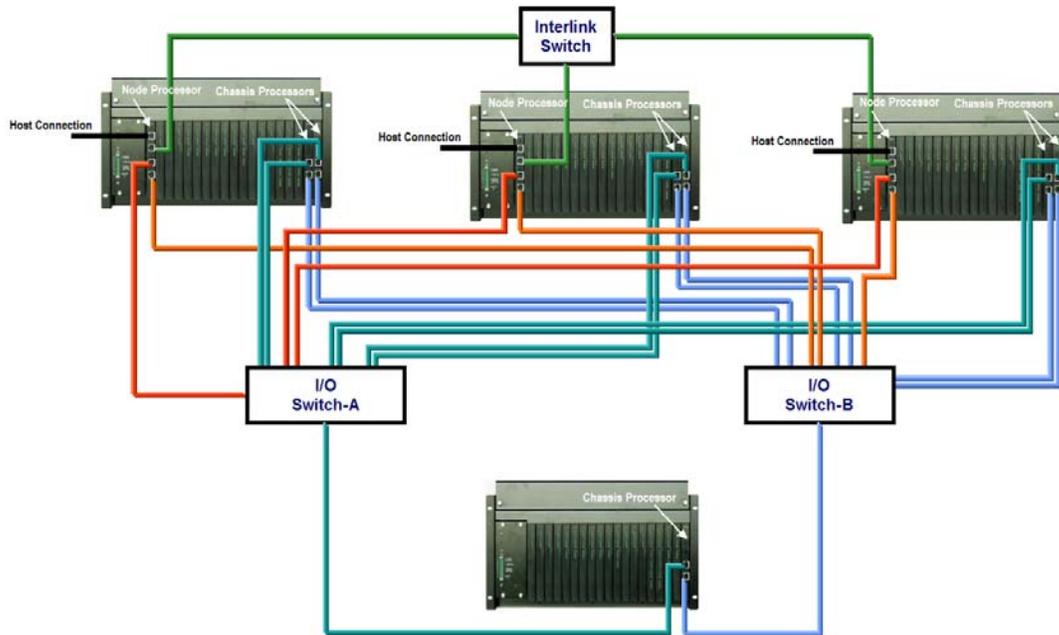
Configuration 2 (Figure 3) shows how additional redundancy is added to achieve both high safety integrity and high availability. A third input module and a third Node Processor may be added to achieve a 2oo3 architecture. Diagnostics are again provided by comparison diagnostics of the input scans, intermediate results and calculated results. Common cause defense is provided by separate modules.

For the Chassis Processor and the Output modules, a 2oo2D architecture is used. This provides maximum availability but the architecture is again highly dependent on exceptional diagnostic coverage. The FMEDA on this design has verified this has been achieved.

### **3.3 Physical Implementation**

A physical drawing of the 3000 system is shown in Figure 4. Since the communications networks provide fully redundant physical connections, high communications availability is achieved. Communications protocol errors are included in the PFDavg model based on a bit error rate of 0.01. Common cause communication system failures are also modeled but the impact is primarily on availability not safety integrity.

It can be seen that the redundant modules can be physically located apart. The end user may choose to even mount the Node Processors in different chassis.



**Figure 4: 3000 System Physical Implementation**

## 4 Markov Analysis

A detailed Markov analysis has been done on the RTP3000 system based on analysis done for the 2500 system [R2] to quantitatively show the result of the architectural design decisions. A single safety instrumented function (SIF) is modeled with three analog input signals and two digital output signals. This I/O count being typical of a simple SIL 3 SIF using three transmitters and two final elements.

### 4.1 Failure rates

The failure rate data used by *exida* in this analysis is from the Failure Modes, Effects and Diagnostic Analysis (FMEDA) performed for the 2500 System by RTP and reviewed by *exida* [R1].

In order to more accurately model the product behavior including the spurious trip rate, the FMEDA analysis of the SIS product includes additional differentiated failure modes beyond the safe and dangerous modes used in traditional published models. This includes failures of the diagnostics. It has been shown that for very high levels of safety integrity the diagnostics must continue to operate. The RTP 3000 includes automatic diagnostics to detect failures in the diagnostic circuitry. The following definitions for the failure modes of the product were developed for the FMEDA analysis.

*Fail-Safe State: State where module / unit output is de-energized.*

Fail Safe Detected	(SD) Failure that causes the module / unit to go to the defined fail-safe state without a demand from the process and that is detected by the system and annunciated to initiate repair.
--------------------	--



Fail Safe Undetected (SU) Failure that causes the module / unit to go to the defined fail-safe state without a demand from the process and that is undetected by the system (detection by operator because of spurious trip, depending on system architecture, is not considered)

*Fail Dangerous: Failure that prevent the module / unit from responding to a demand.*

Fail Dangerous Detected (DD) Failure that is dangerous but is detected by internal diagnostics and annunciated to initiate repair (System reaction is user configurable to automatically transition to safe state if desired).

Fail Dangerous Undetected (DU) Failure that is dangerous and that is not being diagnosed by internal diagnostics.

*Annunciation Failure: Failure that does not impact the ability to respond to a demand but represent a degraded condition within one unit such that automatic diagnostics do not operate.*

Annunciation Detected (AD) Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is detected by internal diagnostics.

Annunciation Undetected (AU) Failure that does not directly impact safety but does impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is covert.

Fail No Effect Failure of a component that is part of the safety function but that has no effect on the safety function.



## 4.2 Assumptions

The following assumptions have been made during the Markov Model Analysis of the RTP 3000 SIS.

- Constant failure rates and repair rates are assumed
- Only a single Safe or Dangerous failure plus one Annunciation failure is significant within one unit
- After an Annunciation failure the associated diagnostic can be assumed to have failed (worst-case)
- Models are based on de-energize to trip systems, safe system failures would cause the outputs to de-energize
- Diagnostic test time (seconds) is much shorter than the average repair time (hours)
- All components that are not part of the safety function and cannot influence the safety function (feedback immune) are excluded.
- Maintenance policies permit quick repair of systems that have dangerous detected failures without shutting down the process
- The models assume that common cause failures will be the same in both redundant units
- The models assume that the end user will configure their logic such that a shutdown will not occur on detected failures of the Analog Input subsystem and the Node Processor subsystem. Detected failures in the Chassis Processor and the Outputs automatically result in a shutdown by the embedded software.
- For the modeling it was assumed that the simplex configuration uses a single power supply and the redundant configuration uses redundant power supplies.

At the system level the average time to repair faults may vary according to the type of failure. The repair rate is represented by the Greek letter  $\mu$  and is equal to the reciprocal of the average repair time. The following types of repair rates are assumed for the model and its evaluation:

- Online repair rate,  $\mu_{ON}$  – repair rate of detected faults which do not result in trip to safe state
- Shutdown repair and restart rate,  $\mu_S$  – repair rate when process must be restarted after shutdown has occurred which includes repair time

### 4.3 RTP 3000 SIS Configuration 1 – Safety Integrity

Configuration 1 of the 3000 SIS system is modeled with three independent Markov models. This modeling technique can be used because the interconnection between logical sections is complete. Both Analog Input Modules are read by both Node Processors. The Chassis Processor receives messages from both Node Processors. Thus the Analog Input subsystem can be modeled as a modified 1oo2 architecture. The Node Processors can also be modeled as a modified 1oo2 architecture. The Chassis Processor and Supervised Digital Output Module combination is modeled as a 1oo1D architecture. The 1oo1D architecture is valid because the Supervised Digital Output module has independent output switching that will automatically de-energize when controlled by the diagnostic signal. The communication failures, power supply failures and backplane failures are included in the 1oo1D model. All three Markov models are solved by discrete time matrix multiplication. This eliminates approximations. Overall safety integrity and false trip metrics are obtained by combining the three Markov model results as a function of time. PFDavg is obtained by numerical averaging of the PFD state totals.

The complete Markov model for the RTP 3000 1oo2 architecture is shown in Figure 5.

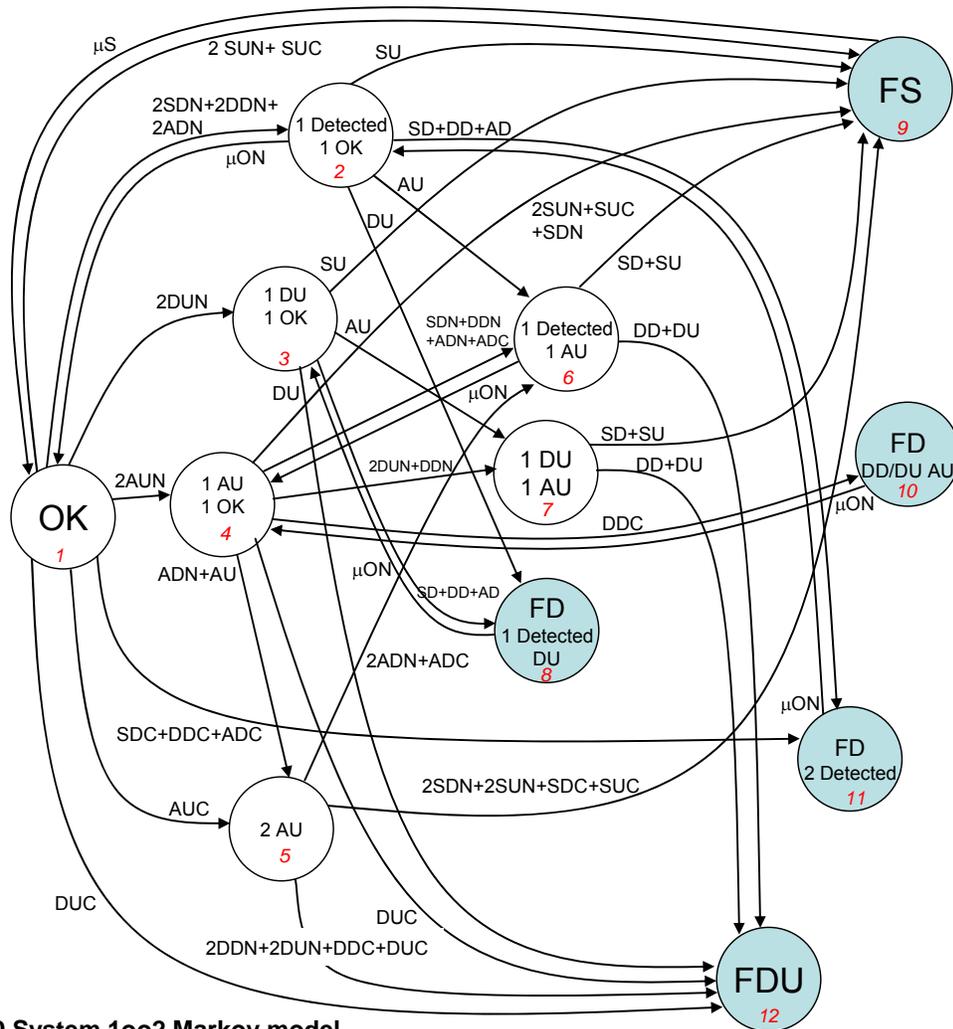


Figure 5: 3000 System 1oo2 Markov model



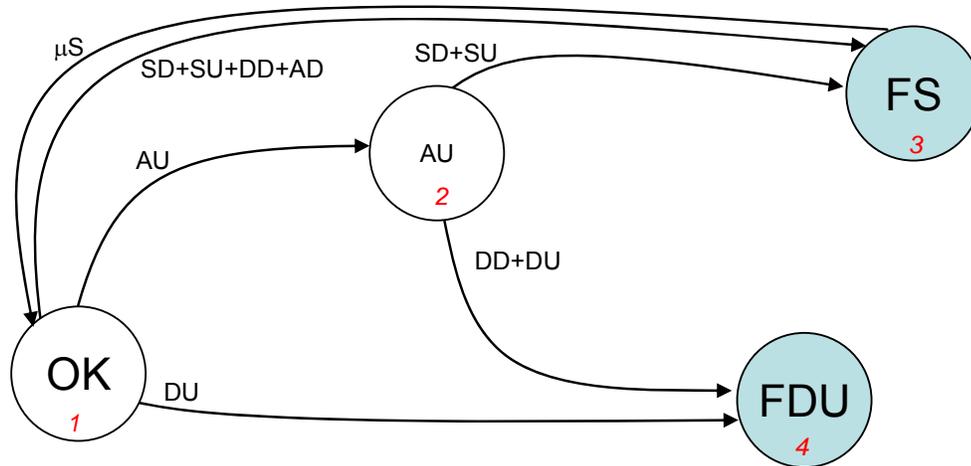
The model has twelve states and shows full detail. The state descriptions are as follows:

State Number	Module Conditions	System Condition
1	Both modules operating without failure	Success
2	One module has a detected failure. The failure is detected and may be repaired on-line. The other module is operating successfully.	Success
3	One module has a dangerous detected failure. The second module is operating correctly.	Success
4	One module has failed such that the automatic diagnostics are not dependable. The second module is working successfully.	Success
5	Both modules have failed such that the automatic diagnostics are not dependable.	Success
6	One module has failed in a detected manner, the second module has failed such that the automatic diagnostics are not dependable.	Success
7	One module has a dangerous undetected failure, the second module has failed such that the automatic diagnostics are not dependable.	Success
8	One module has a detected failure, the second module has a dangerous undetected failure.	Success
9	The system has failed such that it will de-energize outputs and cause a false trip.	Fail-Safe
10	One module has a dangerous detected failure, the second module has a dangerous undetected failure.	Fail-Danger
11	The system has two detected failures but will not respond to a demand.	Fail-Danger
12	The system has multiple dangerous undetected failures and will not respond to a demand.	Fail-Danger

A normal 1oo2 Markov model only has six states. This model is significantly more complicated as it accounts for diagnostic annunciation failures (AD, AU). The model also shows the affect of the assumption that the end user does not automatically shutdown on detected failures as stated in the assumptions.

The model solution shows clearly that states 5, 6, 7 and 10 have state probabilities several orders of magnitude lower than other states. Therefore these states could be pruned without any noticeable impact on the result. For the remainder of the Markov models developed, such tertiary failure states will not be developed.

The Markov Model for the 1oo1D portion of configuration 1 is shown in Figure 6.



**Figure 6 Markov Model 1oo1D subsystems**

From state 1, single failures are shown as transitions to other states. The system is successful in this state and will respond to a demand. In state 2 an assumption is made that no self diagnostic can be assumed to work. The system is still successful in state 2 and will respond to a demand. The Fail Safe State is state 3 and transition probabilities to this state will be considered for spurious trip calculations. The Fail Dangerous State is state 4. The probability of being in this state will be considered in the  $PFD_{AVG}$  calculation.



#### **4.4 RTP 3000 SIS Configuration 2 – High Availability and Safety Integrity**

Configuration 2 of the 3000 system is optimized to achieve high availability (low false trip rate) as well as high safety integrity. Configuration 2 of the 3000 SIS system is modeled with three independent Markov models. This modeling technique can be used because the interconnection between logical sections is complete. All three Analog Input Modules are read by all Node Processors. The Chassis Processors receive messages from all Node Processors. Thus the Analog Input subsystem can be modeled as a modified 2oo3 architecture. The Node Processors can also be modeled as a modified 2oo3 architecture. The Chassis Processor and Supervised Digital Output Module combination is modeled as a 2oo2D architecture. The 2oo2D architecture is valid because the Supervised Digital Output module has independent output switching that will automatically de-energize when controlled by the diagnostic signal. The communication failures, power supply failures and backplane failures are included in the 2oo2D model. All three Markov models are solved by discrete time matrix multiplication. This eliminates approximations. Overall safety integrity and false trip metrics are obtained by combining the three Markov model results as a function of operating time interval. The PFDavg was obtained by numerical averaging of the time dependent result. This eliminates any errors due to “averaging before logic.”

The Markov model for the 2oo3 subsystem of Configuration 2 is shown in Figure 7.

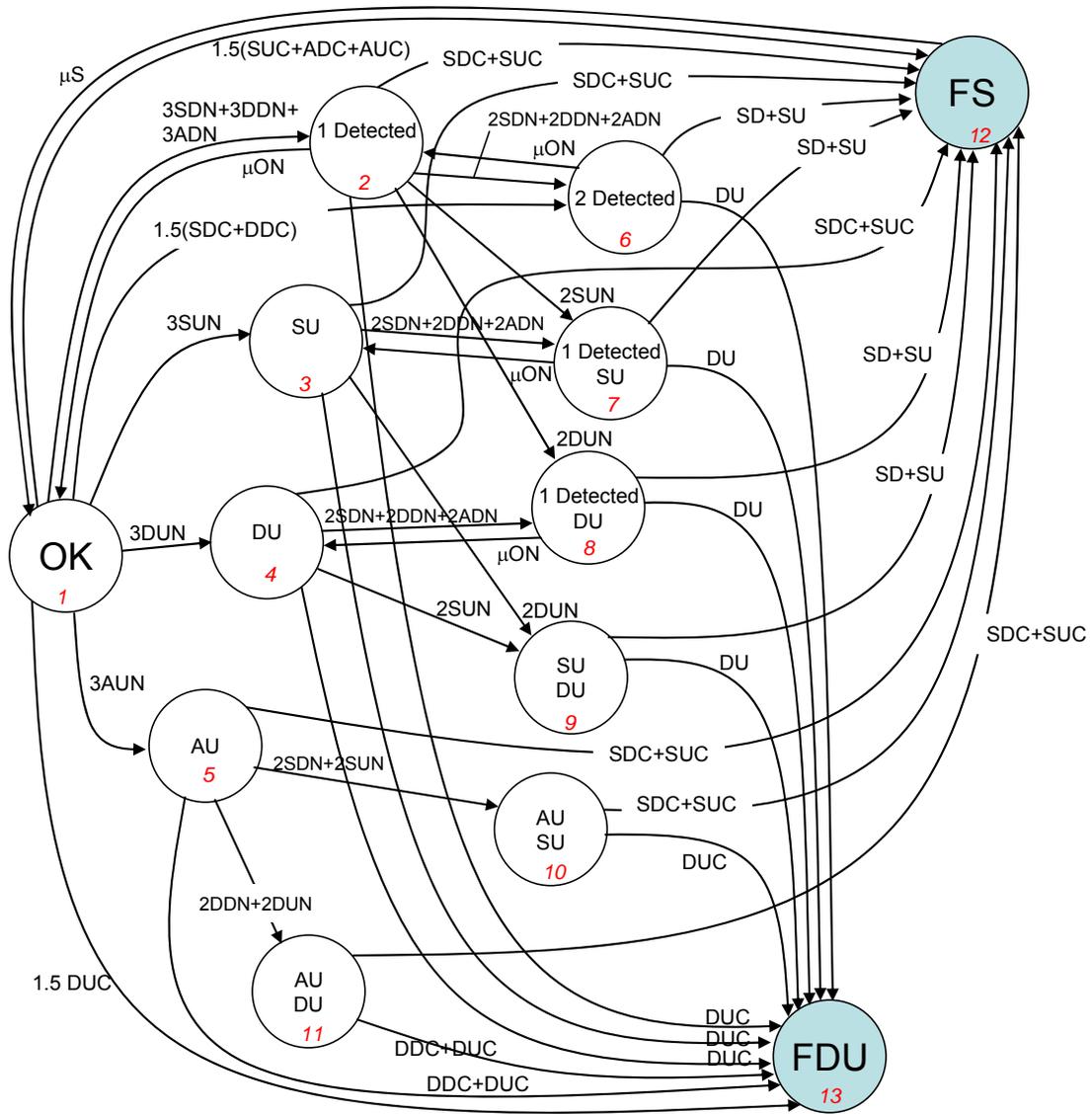


Figure 7: Markov model for the 2oo3 subsystem of Configuration 2



The states are defined as follows:

State Number	Module Conditions	System Condition
1	All modules operating without failure	Success
2	One module has a detected failure. The failure is detected and may be repaired on-line. Other modules are operating successfully.	Success
3	One module has a safe undetected failure. Other modules are operating successfully.	Success
4	One module has a dangerous undetected failure. Other modules are operating successfully.	Success
5	One module has a annunciation undetected failure. Other modules are operating successfully.	Success
6	Two modules have a detected failure. The failures may be repaired on-line. Other modules are operating successfully.	Success
7	One module has a detected failure. A second module has a safe undetected failure. The last module is operating successfully.	Success
8	One module has a detected failure. A second module has a dangerous undetected failure. The last module is operating successfully.	Success
9	One module has a safe undetected failure. A second module has a dangerous undetected failure. The last module is operating successfully.	Success
10	One module has a safe undetected failure. A second module has a annunciation undetected failure. The last module is operating successfully.	Success
11	One module has a dangerous undetected failure. A second module has a annunciation undetected failure. The last module is operating successfully.	Success
12	The system has failed such that it will de-energize outputs and cause a false trip.	Fail-Safe
13	The system has two or more dangerous undetected failures and will not respond to a process demand.	Fail-Danger

The Markov model for the 2oo2D subsystem of Configuration 2 is shown in Figure 8.

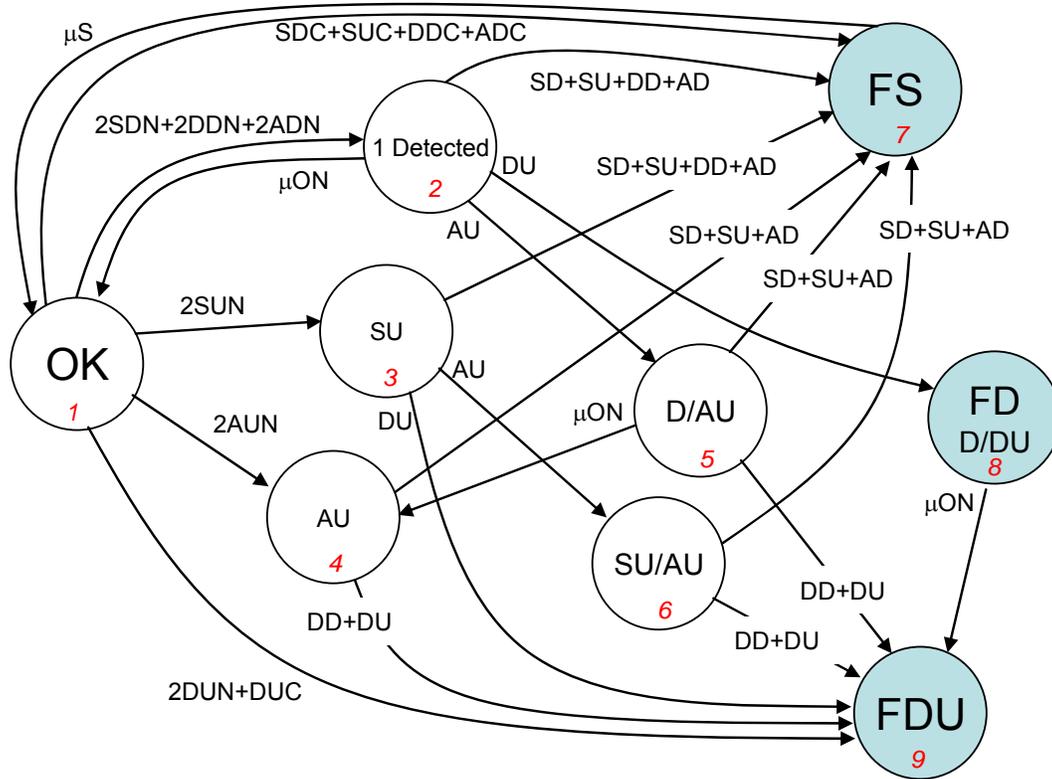


Figure 8: Markov model of the 2oo2D subsystem of Configuration 2



State Number	Module Conditions	System Condition
1	Both modules operating without failure	Success
2	One module has a detected failure. The failure is detected and may be repaired on-line. The other module is operating successfully.	Success
3	One module has a safe undetected failure. The other module is operating successfully.	Success
4	One module has a failure of the automatic diagnostics that is undetected. The other module is operating successfully.	Success
5	One module has a detected failure. The second module has a failure in the automatic diagnostics.	Success
6	One module has a safe undetected failure. The second module has a failure in the automatic diagnostics.	Success
7	The system has failed with outputs de-energized. A false trip has occurred.	Fail-Safe
8	The subsystem has failed dangerously. One module has a detected failure but when this is repaired the subsystem still has one dangerous undetected failure.	Fail-Danger
9	The subsystem has failed dangerously. One or more modules have dangerous undetected failures.	Fail-Danger

Traditional models for a 2oo2D system contain only six of these states. This model is more complex as it models the impact of diagnostic subsystem failures. As with the 1oo1D model diagnostic subsystems were classified into two groups, those that automatically initiate a trip and those that do not. Similar to the 1oo1D model, the worse case assumption is made that no diagnostic can be assumed to work once there has been a single Annunciation failure.



## 5 Discussion of the Markov modeling results

The calculations of the Markov models have been implemented in MS Excel and the exida exSILentia software.

The failure rates used in the calculations are from [R1]. The following additional input data was used:

- Average online repair time is 8 hours
- Average start-up time is 24 hours
- Beta factor is 2%
- Beta D factor is 1% (used on the 1oo1D and 2oo2D models as the modules have automatic shutdown)

Calculations were performed for low demand mode of operation:

*Typically, a system is regarded to be operating in the high demand mode when the demand rate is higher than twice the proof test frequency (see IEC 61511).*

Table 2 shows the results of the calculation for the two configurations.

**Table 2 Average Probability of Failure on Demand 3000 System**

Mission/operating time	Maximum Safety (1oo2,1oo1D)	Maximum Availability and Safety (2oo3, 2oo2D)
1 year	$3.95 * 10^{-5}$	$4.61 * 10^{-5}$
3 years	$1.39 * 10^{-4}$	$1.78 * 10^{-4}$
5 years	$2.65 * 10^{-4}$	$3.59 * 10^{-4}$

The table shows that high safety integrity is achieved with all configurations.

For SIL 3 applications, the  $PFD_{AVG}$  value needs to be  $\geq 10^{-4}$  and  $< 10^{-3}$ . This means that for a SIL 3 application, the  $PFD_{AVG}$  for a 5 year mission time of Configuration 1 is equal to 26.5% of the range. Similarly, for Configuration 2, the  $PFD_{AVG}$  is equal to 35.9%.

For SIL 2 applications, the  $PFD_{AVG}$  value needs to be  $\geq 10^{-3}$  and  $< 10^{-2}$ . This means that for a SIL 2 application, the  $PFD_{AVG}$  for a 5 year mission time of Configuration 1 is equal to 2.65% of the range. Similarly, for Configuration 2, the  $PFD_{AVG}$  is equal to 3.59%.

These results must be considered in combination with  $PFD_{AVG}$  values of other devices of a Safety Instrumented Function (SIF) in order to determine suitability for a specific Safety Integrity Level (SIL).

From the Markov model calculations, also the Mean Time to Fail Spurious (MTTFS) is derived. Table 4 shows the MTTFS results.

**Table 4 MTTFS results**

Maximum Safety (1oo2,1oo1D)	Maximum Availability and Safety (2oo3, 2oo2D)
31 years	2634 years

This clearly shows the improved availability for Configuration 2.



## 6 Summary

Overall the RTP3000 system provides a very flexible architecture where a system may consist of several different architectures depending on the criticality of the application. In its simplest form, a hybrid 1oo2/1oo1D architecture is used to achieve high safety integrity for the de-energize to trip mode. Additional modules may be added to expand the architecture to 2oo3/2oo2D to achieve both high safety integrity and high availability.

The use of comparison diagnostics for the Node Processor and Input modules provides high diagnostic coverage without extensive sacrifice of the computing speed. The result of this is a Node Processor capable of achieving high scan rates (5 msec. reported by RTP) relative to other systems on the market today. Comparison diagnostics in the Node Processor is particularly important for the detection of soft error failures in small geometry integrated circuits [N12]. Self-tests of memory are not effective to detect such failures which may be potentially dangerous and designs that depend on this testing are not nearly as safe and available.

The system provides flexibility, CPU performance, high safety integrity and high availability.



## 7 Terms and Definitions

ASIC	Application Specific Integrated Circuit
CPU	Central Processing Unit, typically refers to processing and memory
FIT	Failure In Time ( $1 \times 10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
IC	Integrated Circuit
Low demand mode	Mode, where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency.
$PFD_{AVG}$	Average Probability of Failure on Demand
PLC	Programmable Logic Controller
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Type A component	“Non-Complex” component (using discrete elements); for details see 7.4.3.1.3 of IEC 61508-2
Type B component	“Complex” component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2



[N10]	Beurden, I.J.W.R.J. van., 1997	Stress-strength simulations for common cause modeling, Is physical separation a solution for common cause failures?, PA: Spring House, Moore Products Co., 1997.
[N11]	Goble, W.M., 1998	The Use and Development of Quantitative Reliability and Safety Assessment in New Product Design, Eindhoven University of Technology, Netherlands: Eindhoven, 1998.
[N12]	Exida, 2006	Electrical – Mechanical Component Reliability Handbook, exida, 2006

## 8.4 Reference documents

### 8.4.1 Documentation generated by *exida* and *RTP*

[R1]	FMEDA Summary.xls	FMEDA Results, RTP 2500, exida, June 2006
[R2]	RTP 06/01-19 R001, V1, R4, 2006	Markov Model Analysis, RTP 2500 System, RTP Corporation, Pompano Beach, FL, USA, December 2006



## 9 Status of the document

### 9.1 Liability

*exida* performed the calculations based on methods advocated in applicable International standards. Failure rates are obtained from a detailed Failure Modes, Effects and Diagnostics Analysis. *exida* accepts no liability whatsoever for the use of these numbers or for the correctness of the standards on which the general calculation methods are based.

### 9.2 Releases

Version: V1  
Revision: R2  
Version History: V1, R2: Edited per client reiew  
V1, R1: Released to client  
V0, R1: Draft; based on 2500 report.  
Authors: William Goble - John C. Grebe  
Review: V1, R1: RTP  
V0, R1: Chris O'Brien, John Grebe  
Release status: Released to client

### 9.3 Future Enhancements

At request of client.

### 9.4 Release Signatures



\_\_\_\_\_  
John Grebe, Principal Engineer



\_\_\_\_\_  
Dr. William M. Goble, P.E., CFSE, Principal Partner