Technical Report

on the Calculation of the Safety Parameters

# of Safety-Related Programmable System RTP3000

Manufacturer:
RTP Corporation
1834 SW 2nd ST.
Pompano Beach
FL 33069-4325
USA

Report-No.: RP82997T
Revision 2.1
11 March 2010
Order-No.: 717502905

Testing and Certification Body
TÜV SÜD Rail GmbH
Rail Automation
Ridlerstraße 57
D-80339 München

This technical report may only be reproduced in the original wording. Use for advertising purposes requires prior written permission. It contains the results of a unique examination of the product submitted for testing and does not represent a general evaluation of current production features.

Executive Summary

This report summarizes the analysis of the RTP3000 system by means of Markov Modelling. By using the failure rates for each subsystem components which result from the component FMEA, the average probability of failure on demand (PFD_{avg}), and probability of failure per hour (PFH) are calculated.

The results of the calculation of the safety parameters according to IEC 61508 for the individual component of RTP 3000 system are depicted in the following table based on the mission time of 20 years.

Description	**AI**	**Chassis Processor**	**Node Processor**	**Chassis Processor**	**DO**
Type	**3007/02-007**	**3000/01**	**3000/02**	**3000/01**	**3005/08-000**
Architecture	**2oo4**	**2oo4**	**2oo4**	**3oo4**	**2oo2**
Useful life (a)	**20**	**20**	**20**	**20**	**20**
MTTR (h)	**8**	**8**	**8**	**8**	**8**
PFD	4.6510e-5	2.3840e-6	2.8770e-6	2.3840e-6	2.0130e-6
PFD_{avg}	2.3260e-5	1.192e-6	1.4380e-6	1.192e-6	1.0070e-6
PFH (/h)	2.6550e-10	1.3610e-11	1.6420e-11	1.3610e-11	1.1490e-11
SFF (%)	95.23	99.88	99.82	99.88	99.75

The RTP3000 system has the PFDavg of 2.808e-5 and PFH of 3.206e-10 per hour based on the mission time of 20 years.

The probability of safe failure (PFS) and the mean time to safe failure MTTFs were also determined by means of Markov model. The following table depicts the MTTFs of the RTP3000 system based on the mission time of 1,3, 5 and 20 years. Note that both parameters vary with the mission time.

Mission time	**PFS**	**MTTFs (a)**
1 year	4.550e-6	219720
3 year	1.733e-5	173059
5 years	3.501e-5	142811
20 years	3.213e-4	62242

Content:

Tables:

Figures:

Revision:

Version	Status	Date	Author	Mod. chap.	Reason of change
1.0	Initial	23.01.2009	Dr. Supavatanakul		
1.1	Update	09.02.2010	Dr. Supavatanakul		Additional parameters
2.0	Update	08.03.2010	Dr. Supavatanakul		MTTFs
2.1	Update	11.03.2010	Dr. Supavatanakul		Typo correction

1 Proceeding

The aim of the following analysis is to determine the safety parameters of the safety-related programmable system RTP3000 from RTP Corporation. This report summarizes the results of the calculation of the safety parameters by means of quantitative analysis and Markov modelling. The results of the calculation are used to determine if the required safety level specified by the standards IEC 61508 can be met.

For the probabilistic calculation according to IEC 61508, the following values have to be considered:

1. Failure rates
2. Safe Failure Fraction (SFF)
3. Diagnostic test interval(s)
4. Proof test interval (T_1, here T_1 = 20 years)
5. Common cause failure
6. Mean time to repair (MTTR, here 8h have been appreciated)
7. DC of every functional safety relevant module
8. PFD_{avg}
9. PFH value

2 Definitions

Abbreviation	Definition
1oo2	“one out of two”-channel (MooN means M out of N channel architecture, for example the system with 1oo2 channel it means that either of the two channels can perform the safety functions).
1oo4	“one out of four”-channel
2oo4	“two out of four”-channel
3oo4	“three out of four” -channel
DEQ	Differential equation
PFD	Probability of failure on demand
PFD_{avg}	Average probability of failure on demand
PFH	Probability of dangerous failure per hour (IEC 61508-6)
PFS	Probability of safe failure
P_i	Probability that the system can be found in the state i. “i” stands for dd, du, s, and ok.
λ-Base	Lambda base is the hardware failure rate [1/h]

λ_s	Lambda safe detected [1/h]
λ_{dd}	Lambda dangerous detected [1/h]
λ_{du}	Lambda dangerous undetected [1/h]
CCF	Common cause failure
ok-state	State, in which the system works without any failures
dd-state	Dangerous detected state
du-state	Dangerous undetected state
s-state	Safe state
DC	Diagnostic coverage
DC_{avg}	Average diagnostic coverage
SFF	Safe Failure Fraction, Mathematical Definition see IEC 61508
MTBF	Mean time between failure
$MTTF_S$	Mean time to safe failure
T1	Proof test interval
MTTR	Mean time to repair
t	Time
a	Year
h	Hour
FIT	Failure in Time (frequency unit), $10^{-9}\ h^{-1}$
TMR	Triple Modular Redundancy
QMR	Quad Modular Redundancy

3 Input Documents

/N1/	RTP3000-SIL Calculation			Dr. Erbay	23.01.2010
/N2/	Email on Markov model			Dr. Erbay	23.01.2010
/N3/	Markov model analysis (EXIDA)			Grebe	28.07.2006
/N4/	RTP3000 SIL Calculation – Quad Short			Dr. Erbay	24.02.2010
/N5/	Availability model Email discussion			Dr. Erbay	24.02.2010
/N6/	Availability model Email discussion			Dr. Erbay	25.02.2010

4 Standards

/S1/	IEC 61165:1995	Application of Markov techniques
/S2/	IEC 61508:1998	Functional safety of electrical/ electronic/ programmable electronic safety- related systems
/S3/	SN 29500:1999	Failure rates of components

5 References

/R1/	T. Winkovich, D. Eckardt	Reliability analysis of safety systems using Markov chain modelling
/R2/	Börcsök	Electronic safety systems: hardware concepts, models and calculations

6 System overview

6.1 *System architecture of RTP3000 series*

The RTP3000 series systems (RTP3000S, RTP3000D, RTP3000T, RTP3000Q and RTP3000M) are safety related programmable systems suitable for safety-related applications with a high level of potential danger e. g. Emergency Shutdown Systems (ESD), Burner Management Systems (BMS), Fire and Gas Detection Systems (F&G), Turbine Control Systems, etc.

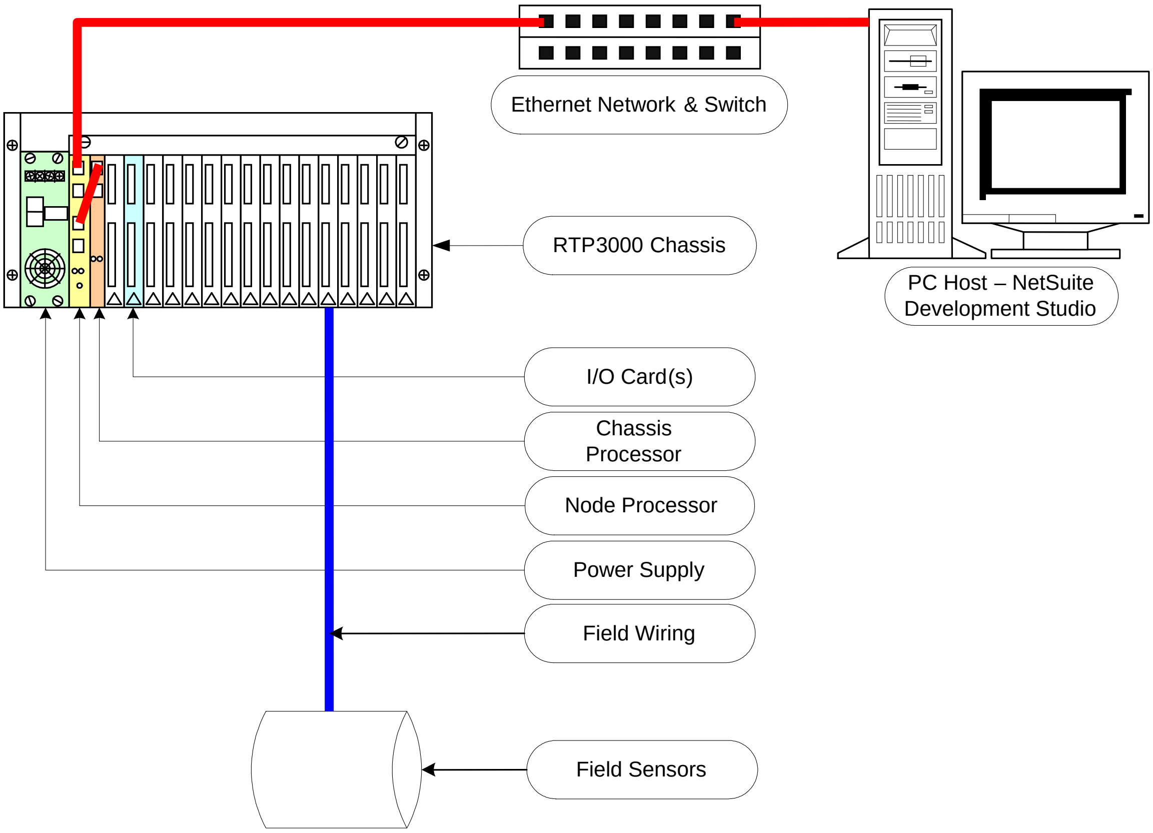

Figure 1 RTP3000 System

The basic RTP3000 system consists of a hardware chassis, a power supply, a node processor card, a chassis processor card and any optional input/output cards.
The RTP3000M system is built up similar whereas the node and chassis processor are included in one card and consists of only one non-expandable chassis.

6.2 *Processor*

The processor node could include safety related and non safety related library modules in an application, whereas the safety instrumented functions should be built up in a user application program while using the certified subset of the graphical languages.

Each node processor executes two copies of the user application program (PGM). I/O scanning of the processor is performed at the same point during program execution, using the same input data for both application programs. The outputs of each of the PGM are compared before sending them to the Chassis Processor.

6.3 I/O Modules

An I/O card is the component that provides basic I/O capabilities between the RTP system and field sensors/signals. The I/O itself will be performed asynchronously. All safety rated analog input cards and safety rated analog output cards shall satisfy SIL 2 requirements. SIL 3 requirement for this kind of I/O shall be accomplished by means of redundant architectures.

The I/O racks, and their installed I/O cards, can be organized as common (non-redundant) I/O racks, redundant I/O rack pairs, or redundant I/O triplets to match the required availability.

6.4 Communication

In a RTP3000 system, I/O data is passed between an I/O card and the chassis processor via the chassis back-plane bus. The chassis processor card communicates I/O data between the RTP3000 Processor card via Ethernet messages which can either be wired port to port or through a separate Ethernet network.

6.5 Architecture and redundancy

The architecture of the RTP3000 system components must be regarded for each application to receive the required SIL or the necessary availability. The following table summarizes possible configurations related to the different components and safety integrity levels. The RTP3000 system whose architectures are listed in Table 1 has been previously certified by TÜV SÜD.

Component	**Architecture for SIL 2**	**Architecture for SIL 3**	**Architecture for higher Availability**
Node Processor	Simplex	Dual	TMR / QMR
Chassis Processor	Simplex	Simplex	Dual / TMR / QMR
I/O Module	Simplex	Simplex / Dual (dependent on type of the cards)	Dual / TMR / QMR (dependent on type of the cards)
I/O Bus	Simplex	Simplex	Dual / TMR / QMR

Table 1: Architecture of RTP3000 system

Component architectures for higher availability have no influence onto the safety of the system. Techniques and measures are included to allow switching from a faulty module to the standby module within a time that allows carrying on the process in a safe manner without interruption.

7 Safety requirements and model parameters

7.1 Safety requirements

This report summarizes the determination of the safety parameters for the RTP3000 system whose configuration is depicted in Table 2.

Module	Analog input card	Chassis Processor	Node Processor	Chassis Processor	Digital output card
Identification	3007/02-007	3000/01	3000/02	3000/01	3005/08-000
Architecture	2oo4	2oo4	2oo4	3oo4	2oo2

Table 2: Architecture of RTP3000 system

The required safety integrity level of the RTP3000 system whose architecture specified in Table 2 is SIL 3 according to /S2/. Therefore, the probability of failure per hour (PFH) of the RTP3000 system has to meet the following requirement.

$$10^{-8} \le \text{PFH} < 10^{-7} \text{ /h}$$

In addition to the PFH, the safe failure fraction (SFF) has to be medium (for HFT = 2), i.e.

$$60\% \le \text{SFF} < 90\%$$

For the calculation of the safety parameters it is assumed that the average mean time to restoration is 8 hours and the mission time is 20 years.

7.2 System states of the modelled system

Markov model will be applied to determine the probability of failure per hour (PFH) for the RTP3000 system. A 2oo2-system, 2oo4-system and a 3oo4-system are modelled. The following tables summarize the related system states for the 2oo2-system 2oo4-system, and 3oo4-system. Note that the state description of 2oo4- and 3oo4-system is identical. The difference lies in the state transitions and the reachable states.

States of the 2oo2 System		
No.	**State Abbreviation**	**Description**
0	ok	The system works in its ordinary mode.
1	s	The system fails in safety state.
2	ok,dd	A dangerous detected failure occurs in one channel. The other works normally.
3	ok,du	A dangerous undetected failure occurs in one channel. The other works normally.
4	dd,dd	Dangerous detected failures occur in both channels. These failures can be detected by tests

States of the 2oo2 System		
No.	State Abbreviation	Description
5	du,dd	A dangerous undetected failure occurs in one channel, in the other channel a dangerous detected failure occurs.
6	du,du	In both channels occur dangerous undetected failures. These failures can`t be detected by tests.

Table 3: System states of the 2oo2-system

States of the 2oo4 and 3oo4 System		
No.	State Abbreviation	Description
0	ok	The system works in its ordinary mode.
1	s	The system fails in safety state.
2	ok,ok,ok,dd	A dangerous detected failure occurs in one channel. The other channels work normally.
3	ok,ok,ok,du	A dangerous undetected failure occurs in one channel. The other channels work normally.
4	ok,ok,dd,dd	Dangerous detected failures occur in two channel. The other channels work normally.
5	ok,ok,dd,du	A dangerous detected failure occurs in one channel and a dangerous undetected failure occurs in one channel. The other channels work normally.
6	ok,ok,du,du	Dangerous undetected failures occur in two channels. The other channels work normally.
7	ok,dd,dd,dd	One channel works normally. Dangerous detected failures occur in the other channels.
8	ok,dd,dd,du	Dangerous detected failures occur in two channels. A dangerous undetected failure occurs in one channel. The other channel works normally.
9	ok,dd,du,du	Dangerous undetected failures occur in two channels. A dangerous detected failure occurs in one channel. The other channel works normally.
10	ok,du,du,du	Dangerous undetected failures occurs in three channels. The other channel works normally.
11	dd,dd,dd,dd	Dangerous detected failures occur in all channels.
12	dd,dd,dd,du	Dangerous detected failures occur in three channels. The other channel has a dangerous undetected failure.
13	dd,dd,du,du	Dangerous detected failures occur in two channels and dangerous undetected failures occur in two channels.
14	dd,du,du,du	A dangerous detected failure occurs in one channels and dangerous undetected failures occur in three channels.
15	du,du,du,du	Dangerous undetected failures occur in all channels.

Table 4: System states of the 2oo4- and 3oo4-system

7.3 Transition rates of the models

In the following tables, the values of the failure rate per channel of each subsystem in the RTP3000 system are listed. These values will be used to determine the transition of the Markov models for the calculation of probability of dangerous failure per hour. These values are based on the FMEA performed by RTP Corporation given in /N1/. In Table 5, the highlighted values will be used for the calculation.

Note that in the following tables the annunciation failures are considered as safe failures and the don't care failures which do not affect the safety function will not be considered in the calculation of the probability of dangerous failure per hour.

Description	**AI**	**Chassis Processor**	**Node Processor**	**DO**
Type	**3007/02-007**	**3000/01**	**3000/02**	**3005/08-000**
Useful life (a)	**20**	**20**	**20**	**20**
λ-Common				
λsd	6,727050E-08	5,496480E-07	2,464110E-07	6,543900E-08
λsu	1,179500E-09	1,305200E-08	2,489000E-09	6,610000E-10
λdd	5,348744E-07	1,002841E-06	8,465838E-07	2,499250E-07
λdu	1,483565E-08	1,999300E-09	2,476200E-09	1,755000E-09
λad	2,208690E-07	6,245000E-08	8,373400E-08	2,266010E-07
λau	1,846100E-08	2,845000E-08	5,766600E-08	7,179000E-09
λdont care	1,435900E-07	2,437600E-07	6,439400E-07	8,252000E-08
λ-Channel				
λsd	0,000000E+00	1,335429E-07	1,374021E-07	5,613300E-08
λsu	3,450000E-09	4,147100E-09	1,387900E-09	5,670000E-10
λdd	1,470200E-09	6,168224E-08	5,990204E-08	0,000000E+00
λdu	2,760980E-08	7,776000E-11	5,796000E-11	0,000000E+00
λad	0,000000E+00	0,000000E+00	0,000000E+00	1,110365E-07
λau	6,000000E-10	0,000000E+00	0,000000E+00	1,913500E-09
λdont care	2,577000E-08	3,835000E-08	4,005000E-08	4,235000E-08
λ-per Channel				
λs	3,118300E-07	7,912900E-07	5,290900E-07	4,695300E-07
λdd	5,363446E-07	1,064523E-06	9,064858E-07	2,499250E-07
λdu	4,244545E-08	2,077060E-09	2,534160E-09	1,755000E-09
λdont care	1,693600E-07	2,821100E-07	6,839900E-07	1,248700E-07

Table 5 Failure rates of for different subsystems within RTP3000

8 Markov Model, Differential Equations and Conditions

To calculate the required probabilistic values, the following system of differential equations has to be solved:

$$\frac{d}{dt}\vec{x} = \hat{A}\vec{x} \qquad (1)$$

where $\hat{A}$ = Transition matrix of the system

and $\vec{x}(t = 0) = (1,0,...,0,0)^T$

The PFD (T_1= 20 a) -Value is calculated by the vector $\vec{x}(t = 20a)$. The value of 20 years is the expected life time of the product.

The PFDavg is given by the following relation (see /R2/)

$$PFD_{avg} = \frac{1}{T_1}\int_0^{T_1} PFD(t)dt \qquad (2)$$

The PFH-value is the result of the following relation (see /R1/):

$$PFH = \frac{PFD(20a)}{T_1} \quad [1/h] \qquad (3)$$

Conditions for the solution of the differential equation system are:

- It is assumed that the failure rates are constant within the lifetime (20 years).
- The total time of operation is assumed to be 20 years. After 20 years, the system must be totally checked (proof test) or replaced to ensure that the system is in as good as new condition. The test of the system must detect 100% of all dangerous failures.
- The system resides initially in a fault-less state (the state “ok”).
- There is no „don’t care“-state taken in the Markov models.
- After repair the system is as good as new. The repair re-establishes the faultless operation of the element / system.
- The β-factor is 1%.

8.1 Markov models

In this chapter, the figures of the used Markov models are shown. The Markov models for 2oo2, 2oo4 and 3oo4 architectures are depicted in Figure 2, Figure 3 and Figure 4, respectively. The nodes which are marked in red contribute to the probability of dangerous failure and will be used to determine the probability of dangerous failure per hour. Note that in Figure 4, the nodes marked in grey are not reachable.

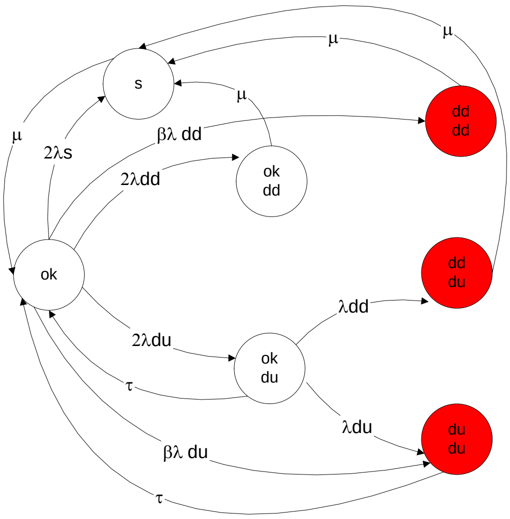

Figure 2: Markov model for 2oo2 architecture

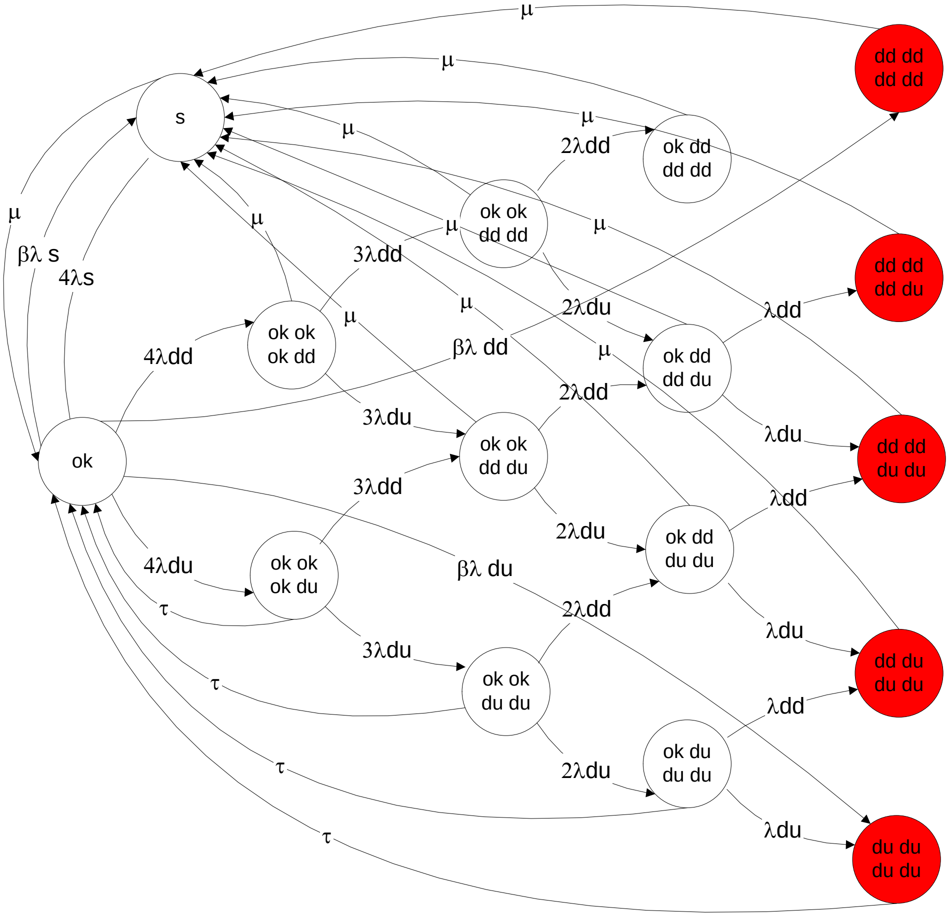

Figure 3: Markov model for 2oo4 architecture

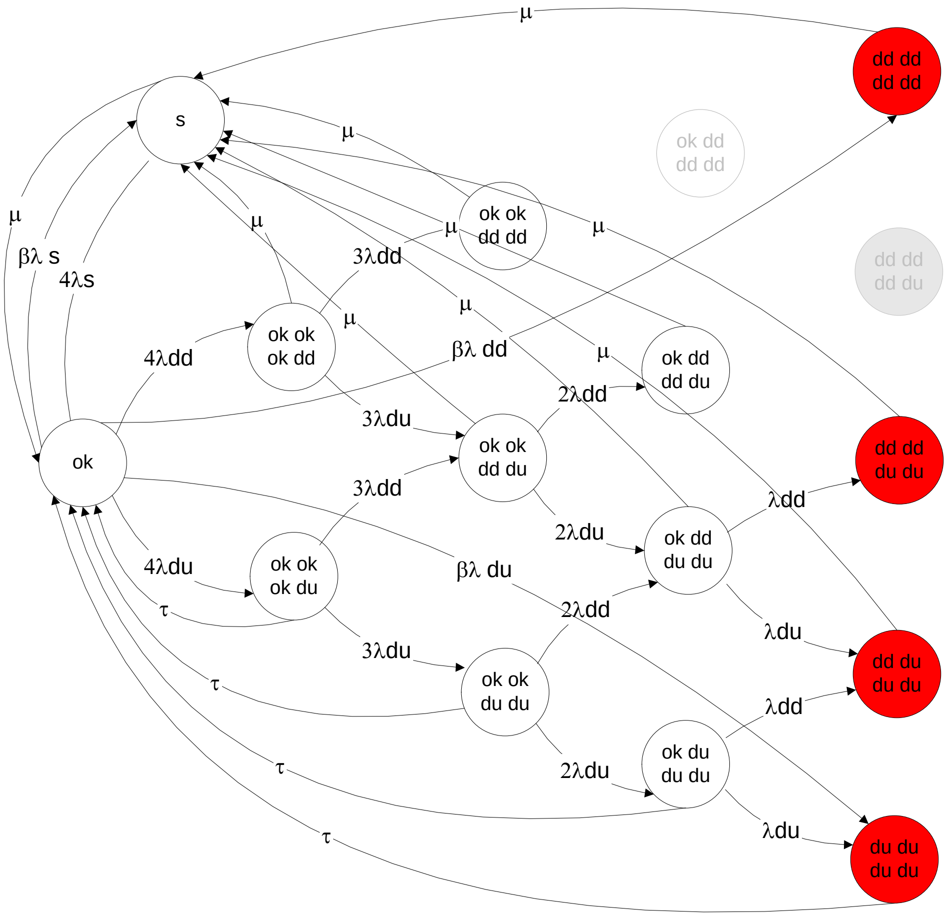

Figure 4: Markov model for 3oo4 architecture

8.2 Transition rates

The failure rates listed in Table 5 (highlighted part) are the basis for the calculation of the transition rates of the Markov models for the RTP3000 system. For the calculation it is assumed that the transition rates are constant over the life time of 20 years and the average mean time to repair is 8 hours.

8.3 Results

Table 6 summarizes the safety parameters for each subsystem within the RTP3000 system. The PFH value for the RTP3000 system can be obtained by the sum of PFH of all subsystems involved.

Description	AI	Chassis Processor	Node Processor	Chassis Processor	DO
Type	**3007/02-007**	**3000/01**	**3000/02**	**3000/01**	**3005/08-000**
Architecture	**2oo4**	**2oo4**	**2oo4**	**3oo4**	**2oo2**
Useful life (a)	**20**	**20**	**20**	**20**	**20**
MTTR (h)	**8**	**8**	**8**	**8**	**8**
PFD	4.6510e-5	2.3840e-6	2.8770e-6	2.3840e-6	2.0130e-6
PFD_{avg}	2.3260e-5	1.192e-6	1.4380e-6	1.192e-6	1.0070e-6
PFH (/h)	2.6550e-10	1.3610e-11	1.6420e-11	1.3610e-11	1.1490e-11
SFF (%)	95.23	99.88	99.82	99.88	99.75

Table 6 Safety parameters for individual subsystems of RTP3000 system with useful life 20 a

Based on the parameters in Table 6, the RTP3000 whose architecture given in Table 2, the RTP3000 system has the total PFD_{avg} of 2.8089e-5 and total PFH of 3.2063e-10 per hour. Based on these results, the RTP3000 system meets the quantitative requirements according to SIL 3 of IEC 61508.

8.4 Availability calculation

The following calculation concerns the availability calculation by means of Markov modelling. The availability calculation in this section uses the simplified Markov models for 2oo2, 2oo4 and 3oo4 system architecture as depicted respectively in Figure 5, Figure 6 and Figure 7 to determine the parameters related to availability. These simplified models are based on the suggestion from RTP Corporation (see /N4/, /N5/ and /N6/). The availability parameters are the probability of safe failure and the mean time to safe failure.

Note that the detected failure rates consist of λ_{sd}, λ_{dd}, λ_{ad} as given in Table 5.

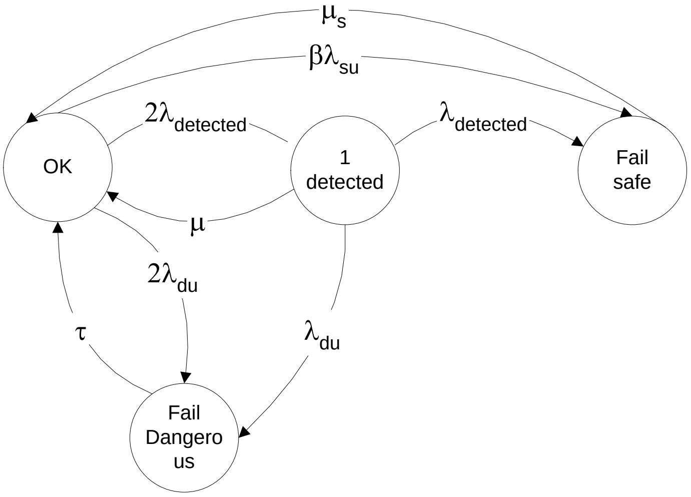

Figure 5: Markov model for 2oo2 architecture (Availability calculation)

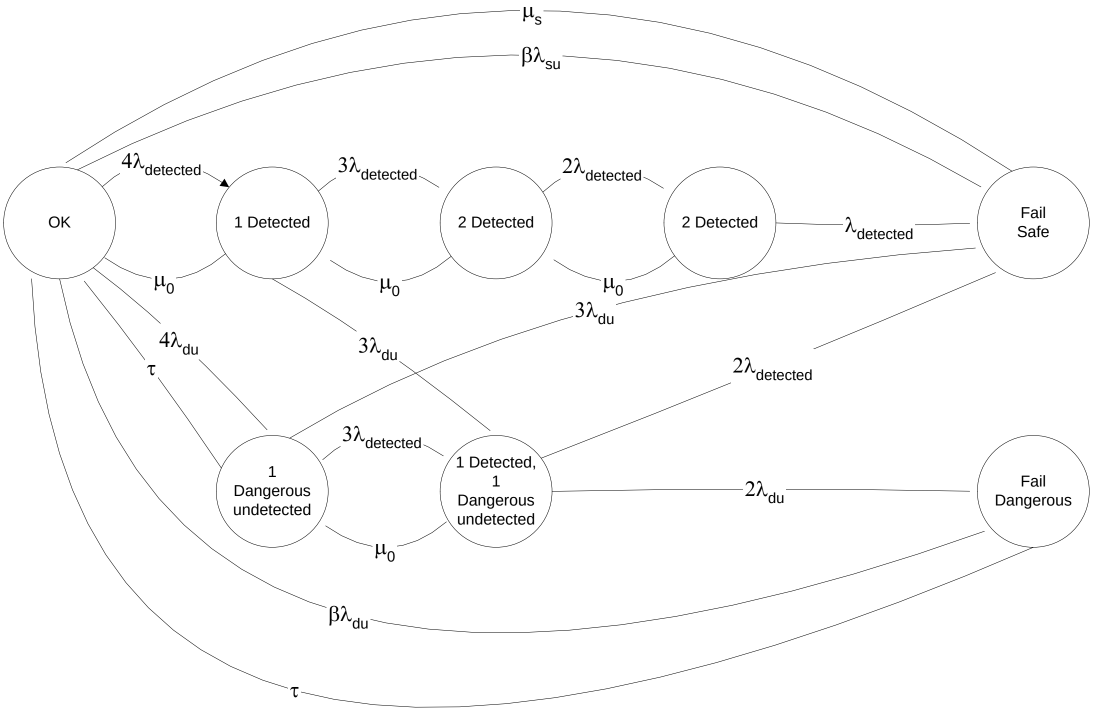

Figure 6: Markov model for 2oo4 architecture (Availability calculation)

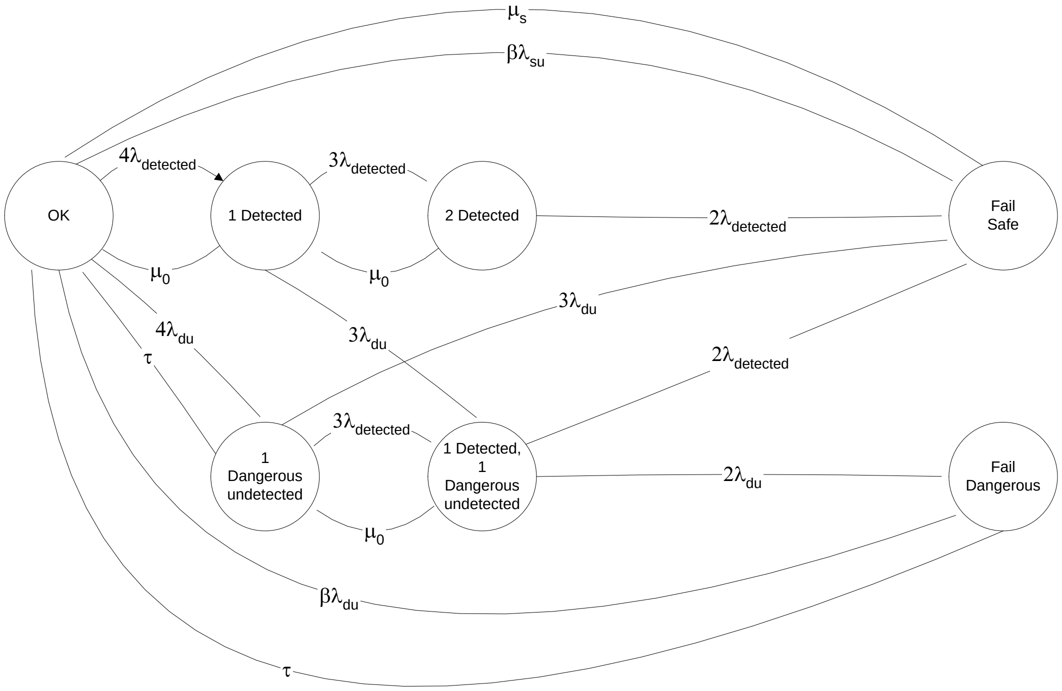

Figure 7: Markov model for 3oo4 architecture (Availability calculation)

Description	AI	Chassis Processor	Node Processor	Chassis Processor	DO
Type	**3007/02-007**	**3000/01**	**3000/02**	**3000/01**	**3005/08-000**
Architecture	**2oo4**	**2oo4**	**2oo4**	**3oo4**	**2oo2**
Useful life (a)	**5**	**5**	**5**	**5**	**5**
MTTR (h)	**8**	**8**	**8**	**8**	**8**
Probability of safe failure (PFS)	1.723e-5	7.569e-6	1.753e-6	7.570e-6	8.901e-7
Mean time to safe failure (a)	2.902e5	6.606e5	2.853e6	6.605e5	5.617e6

Table 7 Safety parameters for individual subsystems of RTP3000 system with useful life 5 a

The results of the availability parameters of individual subsystem are given in Table 7. The calculation is based on the useful life (mission time) of 5 years. The RTP3000 system, whose configuration given in Table 7, has the Mean Time to Safe Failure (MTTF$_S$) of 142811 years.

The probability of safe failure (PFS) and MTTFs vary with the mission time. Table 7 was calculated based on the assumption that the mission time is 5 years. Table 8 depicts the comparison of MTTFs for mission time of 1, 3, 5 and 20 years.

Mission time	PFS	MTTFs (a)
1 year	4.550e-6	219720
3 year	1.733e-5	173059
5 years	3.501e-5	142811
20 years	3.213e-4	62242

Table 8 MTTFs of RTP3000 system with useful life of 1, 3, 5 and 20 years.

Liability

TÜV SÜD Rail GmbH performed the calculations based on the methods given by the applicable international standards. The failure rates are obtained from the already executed component FMEA by RTP Corporation. TÜV SÜD Rail GmbH 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.

TÜV SÜD Rail GmbH
Rail Automation

Peter G. Weiß

i.A.
P. Weiß

i.A.
Dr. P. Supavatanakul