

Modern 2oo4-processing architecture for safety systems

PROF. DR.-ING. HABIL. JOSEF BÖRCSÖK
HIMA Paul Hildebrandt GmbH + Co KG
68782 Brühl, Albert-Bassermann-Str. 28
GERMANY
j.boercsoek@hima.com

Abstract: - An advanced safety architecture is the 2 out of 4-system (2oo4). In order to trigger the safety function at least two of the four channels must work correctly. It is said: “A 2oo4-system is 2-failure safe”. In order to classify the quality of a system we calculate different parameters. In the report equations are indicated for PFD for normal and common-cause-failures. Also the Markov-model for a 2oo4-architecture is introduced. We can calculate the MTTF (Mean Time To Failure) of this architecture with this Markov-model. The results are high availability and a high reliability.

Key-Words: - 2oo4-Architecture, Availability, IEC/EN 61508, Reliability, Markov-model, MTTF, PFD, SIL

1 Introduction

Modern technical systems, controlling and steering safety relevant processes are becoming more and more complex. There are multivarious reasons for this: On the one hand, the demands on high quality performance systems increase while simultaneously the required space for components has to decrease, and on the other hand it is necessary to offer technically enhanced and safer systems, due to a steadily growing of competitive globalization, - in order to remain competitive. This applies especially to the field of safety relevant digital processing and automation, in which complex digital circuits are integrated.

Digital processing systems of each size are particularly used for safety related tasks. Such tasks might be the supervising or controlling of vehicles, trains, aeroplanes or power plants and chemical processing units. Another important and growing application field is the medical field. In each of the indicated sectors failures and errors of the systems would increase the risk for immense damage up to the threat of human lives.

Today's controlling or application systems used for safety critical missions commonly consist of highly complex single components, implemented either as software or hardware. A hardware and a software model has to be generated, evaluating aspects like reliability and safety of a complex system. Reliability means to function without any failure under all circumstances. Safety here means that the system will not come into a critical state even if a failure occurs. The process's safe status is referred to as a status of no danger occurring. If a failure occurs the system has to be able to reach the safe status.

The various functional, non-functional and safety-technical demands to the system along with common system characteristics lead to a list of system specific features. This contains:

- Reliability, availability and failure safe operation
- System integrity and data integrity
- Maintenance and system restoring.

In order to have measurable parameters it was defined the widely used parameters “mean time to failure” (MTTF) and “probability of failure on demand” (PFD). The PFD characterizes the quality of a faultless system. The smaller the value the better the safety of the system. A systems's safety refers to all items in the loop. In automation a loop among others consists of a safety related system of the following components:

- Computing elements (logic processing devices such as analog and digital in- outputs, CPU)
- Sensors
- Termination elements such as actuators

Combing all elements of a system in a safety architecture the system can be classed with a defined safety level, safety integrity level (SIL).

Table 1 shows the various classifications of safety systems. The norm IEC 61508 defines two different criterions for the classification of the safety systems into the individual safety levels.

On the one hand, a system can be judged by its probability of a dangerous failure, i. e. an error occurs on the demand of a safety function and the system can no longer perform its safety function. IEC 61508 implies that the so called proof check interval lies at

- two years
- ten years.

This probability of failure is defined as “probability of failure on demand” (PFD). It has a dimension of 1 unit.

Table 1: SIL classification

Safety Integrity Level (SIL)	Low demand mode of operation $T_1 = 2 \text{ years or } T_1 = 10 \text{ years}$	High demand or continuous mode of operation $T_1 = 1 \text{ month or } T_1 = 2 \text{ months or } T_1 = 6 \text{ months or } T_1 = 1 \text{ year}$
1	$\geq 10^{-2} \text{ to } < 10^{-1}$	$\geq 10^{-6} \text{ to } < 10^{-5}$
2	$\geq 10^{-3} \text{ to } < 10^{-2}$	$\geq 10^{-7} \text{ to } < 10^{-6}$
3	$\geq 10^{-4} \text{ to } < 10^{-3}$	$\geq 10^{-8} \text{ to } < 10^{-7}$
4	$\geq 10^{-5} \text{ to } < 10^{-4}$	$\geq 10^{-9} \text{ to } < 10^{-8}$

IEC 61508 proposes a second possibility for classification of safety system. The probability of an occuring failure on demand leaving the system unable to perform its safety functions is calculated as well. Therefore a certain period of time is demanded for the proof check interval, either

- one month or
- three months or
- six months or
- one year.

This probability of failure is defined as probability of failure per hour (PFH). Unlike probabilities it has a dimension of 1/h. Systems demanding a continuous operation are highly significant for industrial systems.

Note that comparing both systems to its PFD or PFH value is only possible within limits, as they refer to different bases.

The probability of a failure on demand always has to be regarded as a statistical term. Even in safety systems there is no absolute safety given, since these systems may fail on demand.

By long lasting empirical studies on corresponding applications the distribution of a system’s failures can commonly be assumed as follows:

- 15 % of computing elements
- 50 % of sensors
- 35 % of termination elements such as actuators.

The whole system's failure rate λ is subdivided into safe failures λ_S and dangerous failures λ_D . In addition, safe failures are subdivided into safe undetected failures λ_{SU} and safe detected failures λ_{SD} . Whereas dangerous failures are subdivided into dangerous undetected failures λ_{DU} and dangerous

detected failures λ_{DD} . Fig. 1 shows the spreading of failure rates. Failure rates could be specified with the aid of standard specifications.

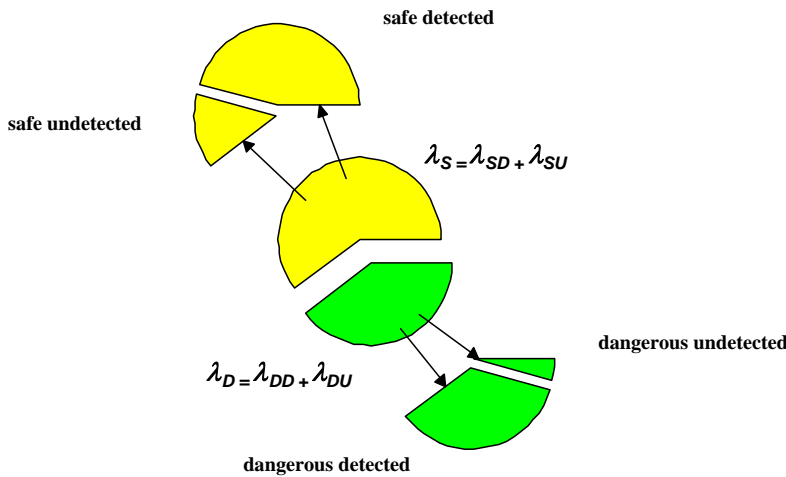


Fig. 1: Structural Software Creation for Safe Systems

A system's quality can be specified by defining its *PF*D value referred to its accuracy. The smaller this value the better is the system. However, the longer the system runs the higher will be the *PF*D value. The *PF*D value is calculated for a period of time called proof check interval T_1). After the maintenance of the system we proceed on the assumption that it works without any failures. Judging and comparing systems is mostly specified by the *PF*D average value ($PF_{D_{avg}}$) over a whole proof check interval.

The most known architectures in use for safety systems are the 1oo2- and 2oo3-architectures. 1oo2- (reading 1 out of 2) and 2oo3- (reading 2 out of 3) architectures are common for safety-related systems in industry.

A 1oo2-architecture, s. figure 2, contains two independent channels which are connected in manner so if one of the two serial output circles has a safety-related failure the other channel must work correctly and transmits the controlling process into the safe state.

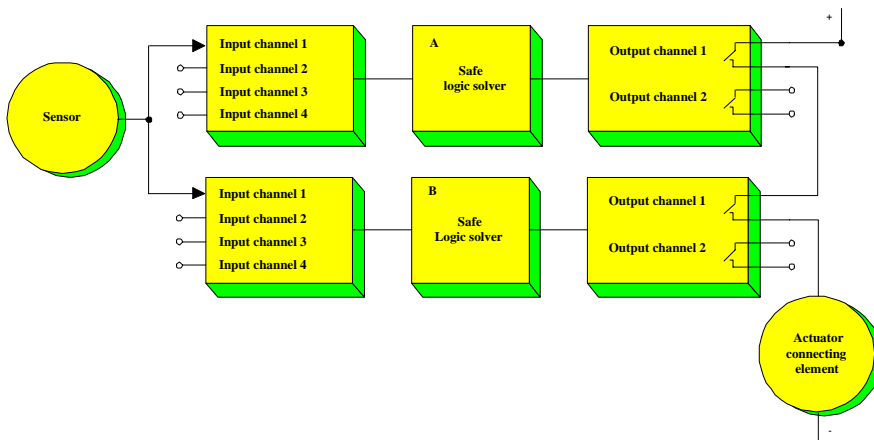


Fig. 2: Reliability block diagram of 1oo2-architecture

The 2oo3-architecture, s. figure 3, distinguishes by it that at least two of the four channels must work correctly in order to trigger the safety function. In order to meet all requirements for safety the 1oo2-architecture is sufficient.

If you (additional) require a high reliability you have to choose a 2oo3-architecture. In order to take advantage of both system in industry you must develop a 2oo4-architecture. This architecture will be described in the following.

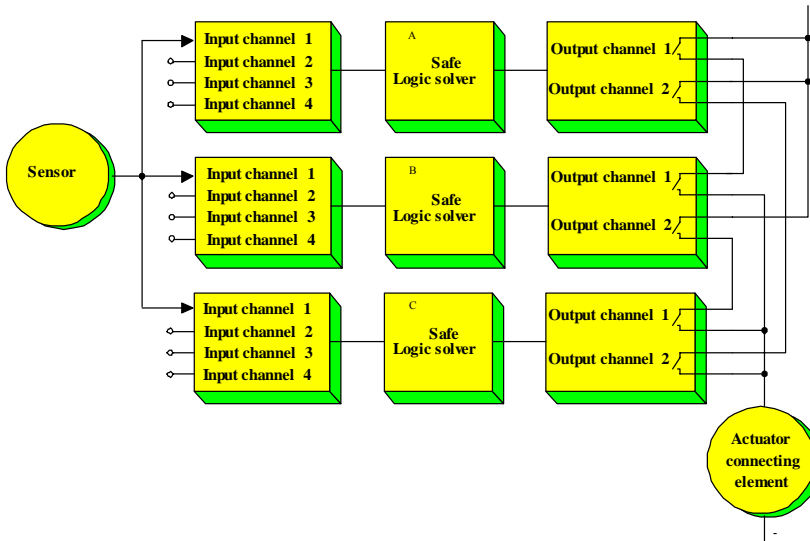


Fig. 3: Reliability block diagram of 2oo3-architecture

2 Description of the 2oo4-architecture for safety-related technology

The 2oo4-system normally contains four independent channels. The four channels are connected one with another. In order to trigger the safety function at least two of the four channels must work correctly. Even if two failures in two different channels occur the system can be transmitted into the safe state. It is said: "a 2oo4-system is 2-failure safe".

A dangerous breakdown of the system is generated if three of the four channels have dangerous failures themselves. Figure 4 shows a reliability block diagram of a 2oo4-architecture. Each single channel contains of an input circle, a safe processing unit and two serial output circles.

In a fault-tree-analysis you can determine the following which causes a system in a dangerous non safety state:

- There is in all four channels a dangerous detectable failure which all have a common cause
- There is in all four channels a dangerous undetectable failure which all have a common cause

- Three of four channels have a dangerous detectable or a dangerous undetectable failure which all have no common cause

Theoretically a 2oo4-system is immediately transmitted into the safe state if a dangerous failure arises. However in practise each detection of a failure is time consuming. If any more failure occurs in this time, so we have two failures at the moment. However due to its 2-failure-safety the 2oo4-system can definitively reach the safe state in contrast to a 2oo3-system. When a dangerous failure occurs then the system switches off the concerned channel. So the 2oo4-system degrades to a 2oo3-system itself. In this new system there is still another failure in the three correct operating channels possible.

In a 2oo3-system you have a majority of correct working channels if a dangerous failure will happen. The system is in a defined state and it decides to transmit into the safe state. In a 1oo2-system one of the two channels must work correctly. However if there are two failures in each channel there is no possibility to switch off the process in a safe state. So the difference between the 2oo4- and a 1oo2-system is higher availability of the 2oo4-system and it has a light better probability of the safe-function.

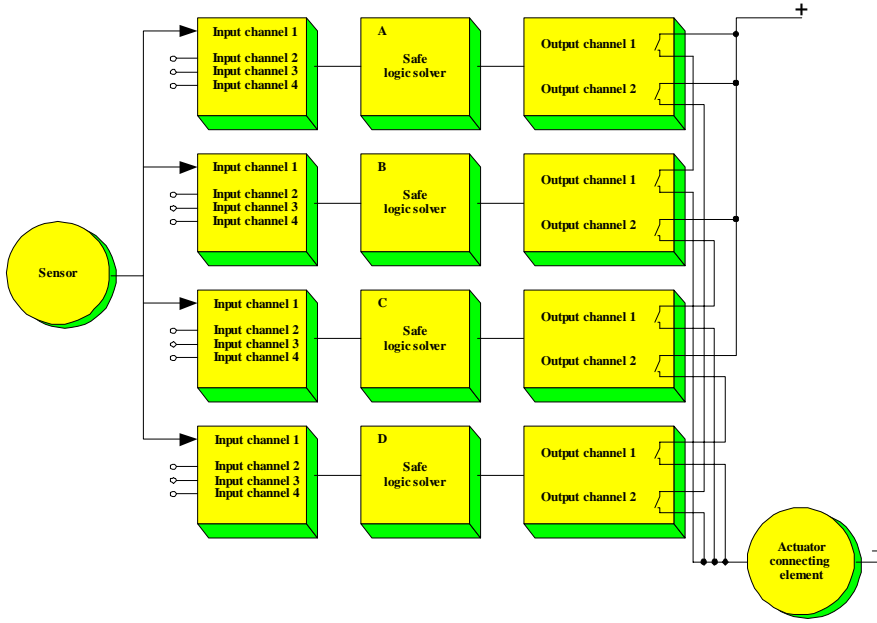


Fig. 4: Reliability block diagram of 2oo4-architecture

3 Calculation of probability distributions

You can apply the basic approach for determination of PFD_{avg} -equation of a 2oo4-system:

$$P(t) = P_{single} + P_{common\ cause} \quad (1)$$

$$= 4 \cdot P_1(t) \cdot P_2(t) \cdot P_3(t) + P_{DUC}(t) + P_{DDC}(t)$$

The index DUC means a dangerous undetected common-cause-failure, whereas DDC accounts for a dangerous detected common-cause failure.

3.1 Calculation of probability of normal failures

As already mentioned the 2oo4-system is 2-failure tolerant. Before we calculate the probability of normal failures for a 2oo4-system, we should reflect how is the probability for a 1-failure tolerant system, e. g. a 1oo3-system. If a 1oo3-system should fail with normal failures, we have the condition that each of the three channels must have a dangerous failure. If the probability is calculated for this case, then the product is derived from the probability of failure of each channel. The following equation results:

$$P_{normal}(t) = P_1(t) \cdot P_2(t) \cdot P_3(t) \quad (2)$$

$P(t)$ describes the probability of failure for the i^{th} channel with the failure rate of

$$\lambda = \lambda_{Di} \quad (3)$$

for a dangerous, normal failure in channel i and the probability of failure

$$P_i(t) = 1 - e^{-\lambda_{Di} \cdot t} \quad (4)$$

If the equation (4) and (2) are used with the general applicable PFD_{avg} equation

$$PFD_{avg}(T) = \frac{1}{T} \cdot \int_0^T P(t) \cdot dt, \quad (5)$$

we get the result

$$PFD_{avg,normal}(T) = 1 + \frac{e^{-\lambda_{D1}T} - 1}{\lambda_{D1}T} + \frac{e^{-\lambda_{D2}T} - 1}{\lambda_{D2}T} + \frac{e^{-\lambda_{D3}T} - 1}{\lambda_{D3}T}$$

$$- \frac{e^{-(\lambda_{D1} + \lambda_{D2})T} - 1}{(\lambda_{D1} + \lambda_{D2})T} - \frac{e^{-(\lambda_{D1} + \lambda_{D3})T} - 1}{(\lambda_{D1} + \lambda_{D3})T}$$

$$- \frac{e^{-(\lambda_{D2} + \lambda_{D3})T} - 1}{(\lambda_{D2} + \lambda_{D3})T}$$

$$+ \frac{e^{-(\lambda_{D1} + \lambda_{D2} + \lambda_{D3})T} - 1}{(\lambda_{D1} + \lambda_{D2} + \lambda_{D3})T} \quad (6)$$

This function can be developed into a power series with help from a Taylor development (exactly MacLaurin series). The condition that the $PF_{D,avg, single}(T)$ is a continuous function, which has a removable singularity at $T=0$ and thus all derivations at this point exist can be proved, e. g. in [3], [4]. After some calculation, see also [3], [4], we get the result

$$PF_{D,avg, normal}(T) = \frac{(\lambda_D)^3 \cdot T^3}{4}. \quad (7)$$

This is the result for the probability of failure on demand for a 1003-system for normal failure. You have to be aware that the parameter T is not equivalent to the parameter T_1 (proof check interval) in the IEC/EN 61508, see [1]. T_1 is only a part of T ! For the calculation of the $PF_{D,avg}$ value for a 2004-system in case of normal failures we can use the equation (7) of the 1003-system. This equation must be extended for the factor four as with four channels there are four possibilities that in two channels a failure exist – remember the 2004-system is two-failure tolerant.

The probability of failure for the 2004-system for normal failures is

$$PF_{D,avg, normal}(T) = (\lambda_D)^3 \cdot T^3. \quad (8)$$

3.2 Calculation of probability of common-cause failures

Now we want to calculate the failure probability for dangerous undetectable and dangerous detectable common cause failures P_{DUC} and P_{DDC} . Common cause failures are those failures that occur in all system channels at the same time and which have a common cause. When determining the $PF_{D,avg}$ this kind of failure is rated for a multi channel system through the β -factor. One differentiates between the β -factor for dangerous undetectable failures, with the weight β , and the β -factor for dangerous detectable failures, with the weight β_D . Calculating the common cause part of the total probability, you have to add the failure probabilities P_{DUC} and P_{DDC} .

$$P_\beta(t) = P_{DUC}(t) + P_{DDC}(t) \quad (9)$$

Analogue, these failure probabilities can be derived for a 1001-system with $\lambda_{D,1001} = \beta \cdot \lambda_{DU}$ respectively $\lambda_{D,1001} = \beta_D \cdot \lambda_{DD}$. A random common cause failure represents a 1001 function block! Therefore it is possible to apply the derived $PF_{D,avg}$ equation of the 1001-system for the calculation of probability of common cause failure, see [3], [4]. The general solution for the probability failure results in

$$PF_{D,avg} = \frac{\lambda_D \cdot T}{2}. \quad (10)$$

Since we have two common cause failure modes, $\lambda_{DUC} = \beta \cdot \lambda_{DU}$ and $\lambda_{DDC} = \beta_D \cdot \lambda_{DD}$, and with the two assumptions that

- a dangerous undetected common cause failure occurs within the time period $T_1 + MTTR$ (T_1 means the proof time interval, $MTTR$ means the mean time to repair) and
- a dangerous detected common cause failure occurs within the repair time $MTTR$,

we can calculate the $PF_{D,avg}$ value for common cause failures as

$$PF_{D,avg, \beta} = \frac{\beta \cdot \lambda_{DU}}{2} (T_1 + MTTR) + \frac{\beta_D \cdot \lambda_{DD}}{2} \cdot MTTR. \quad (11)$$

3.3 $PF_{D,avg}$ -equation for a 2004-system

The $PF_{D,avg}$ equation of a 2004-system taking into account the normal failures, equation (8), and the common cause failure, equation (11), is therefore:

$$PF_{D,avg} = (\lambda_D)^3 \cdot T^3 + \frac{\beta \cdot \lambda_{DU}}{2} (T_1 + MTTR) + \frac{\beta_D \cdot \lambda_{DD}}{2} \cdot MTTR \quad (12)$$

4 Markov-model of a 2004-architecture

Basically is the Markov-model of a 2004-“Single-Board System” accomplished with conventional calculation methods. The single transitions are shown in figure 5.

The state 0 represents the accuracy in all of the 4 channels. State 1 is the safe state in which the system devolves if a safe failure occurs. The transition-rate from state 0 to state 1 is $4 \cdot \lambda_S$, because in each of the four channels is a safe failure possible. On the

basis of state 3 we will describe the different transitions. For all other states obtain the same issues.

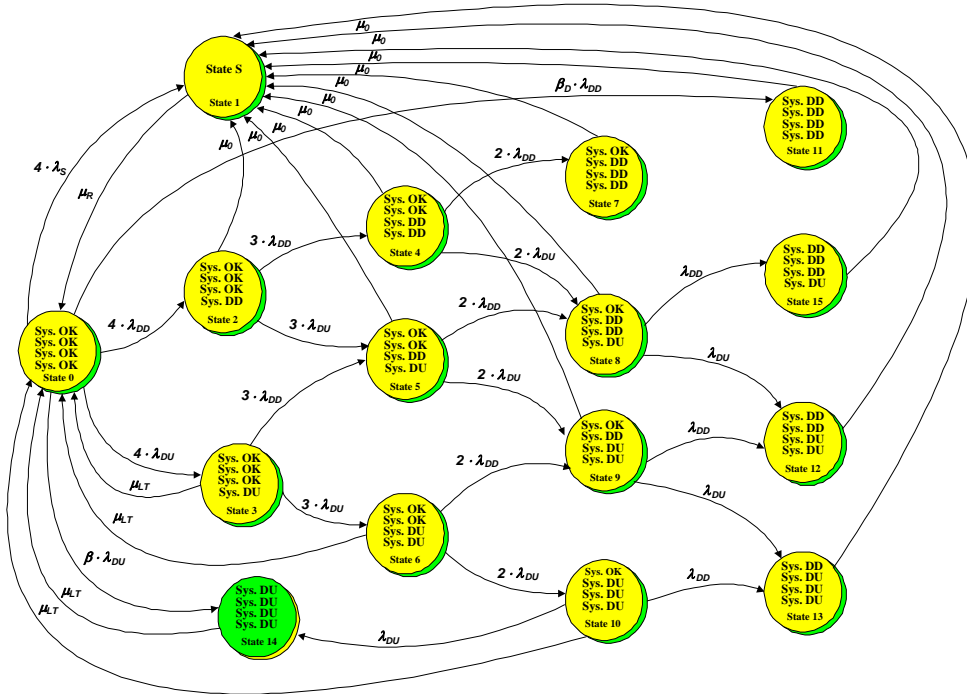


Fig. 5: 2004-Markov-model

In state 3 one of the four channels is operating with a failure. The occurring failure is dangerous and is not recognized by the failure diagnostics. The transition rate between the states 0 and 3 has the value $4 \cdot \lambda_{DU}$, as in one of the three channels a dangerous undetected failure can exist. No transition possibility exists for the system from state 3 into safe state 1 because the failure cannot be recognized within the test interval $\tau_{Test} = 1 / \mu_0$. From state 3 a transition takes place into state 5 respectively 6 if a failure occurs in the until then still failure-free channels. The system can only change to state 0 again, where the system is failure free, after τ_{LT} if during the total lifetime of the system in state 3 no further failures occur. In praxis this means: After time τ_{LT} the total system is exchanged.

If the second failure in state 3 is a dangerous detected failure then a transition takes place into state 5. The transition rate is $3 \cdot \lambda_{DD}$.

Therefore, in state 5 a dangerous undetected failure exists in one channel while at the same time in one of the other three channels a dangerous detected failure has occurred. The dangerous detected failure is revealed within the test interval when the system exists in state 5 and no further dangerous failures occur and then state 5 changes with transition rate $\mu_0 = 1 / \tau_{Test}$ into the safe state 1. The system exists in state 6 if another dangerous undetected second failure occurs in one of the three channels while the system is in state 3. The transition rate is $3 \cdot \lambda_{DU}$. State 6 is characterized by two dangerous undetected failures, one in two of four channels. No transition possibility exists for the system from state 6 into the safe state 1 because the failures are not recognized within the test interval $\tau_{Test} = 1 / \mu_0$.

Because of the failure detected within the test interval τ_{Test} a transition possibility exists for the system from the states 7, 8, 9, 11, 12, 13 and 15 into the safe state 1. The transition rate for this transition is $\mu_0 = 1/\tau_{Test}$.

The following two cases can be differentiated if a common cause failure occurs in a 2oo4-system:

- The common failure cause leads to dangerous detected failures. Then a transition exists from state 0 directly into the state 11. The transition rate is $\beta_D \cdot \lambda_{DD}$.
- The common failure cause leads to dangerous undetected failures. Then a transition exists from state 0 directly into the state 14. The transition rate is $\beta \cdot \lambda_{DU}$.

In summary we can note the following:

- If state 7 occurs the system immediately switches to state S.
- Failures that bring the 2oo4-system in the states 8, 9, 12, 13, and 15, result in a transition of the system into the safe state 1 after time, which is smaller than $4 \cdot \tau_{Test}$. The transition rate from these states into state 1 is always equal to $\mu_0 = 1/\tau_{Test}$.
- The states 1, 7, 11, 12, 13, 14 and 15 are absorbing states, that means, this states has only a transition to the safe state or to the state "system fully operational" and no further transitions exist.

In the states 0, 2, 3, 4, 5, 6, 8, 9 and 10 the system is operational. These states must be taken into account for the *MTTF* calculation of the 2oo4-systems.

4.1 Calculation of *MTTF*-value for a 2oo4-system

For the 2oo4 Markov model exists the transition matrix P . This transition matrix is 16 x 16 matrix, see [3], [4], because we have 16 states.

The P matrix is the basis for the Q matrix. The elements of the Q matrix are composed of the respective probability densities, where the corresponding states meet the following criteria:

- System operational
- Non absorbing state.

An operational system is possible for a 2oo4-system in the states 0, 2, 3, 4, 5, 6, 8, 9 and 10. The states 1, 7, 11, 12, 13, 14 and 15 should not be considered during the *MTTF* calculation, as they are absorbing states. Therefore the Q matrix has a 9 x 9 matrix form, see [3], [4].

For the considered Markov model we make the assumption $\tau_{LT} = \infty$. As such applies

$$\mu_{LT} = \frac{1}{\tau_{LT}} = 0. \quad (13)$$

The next step is to calculate the M -matrix. We get the M -matrix with the following formula:

$$I - Q = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix} \cdot dt = M \cdot dt. \quad (14)$$

For the 2oo4-system the M -matrix is also a 9 x 9 matrix. Now we can calculate the N -matrix. The N -matrix needs to be composed to derive the *MTTF* value of the system. The N -matrix is the inverse matrix of the M -matrix.

The *MTTF* value describes the mean time between the occurrences of two failures. One assumes state 0 at the start time, i.e. the state in which the system operates failure free. After the inversion the elements of the new matrix represent time dependent values. One needs to sum the first row of the N -matrix in order to derive the *MTTF* value of the system. The *MTTF* term of a 2oo4-system has the following form, see also [3], [4]:

$$MTTF_{2oo4} = \frac{1}{A_1} + \frac{4 \cdot \lambda_{DD}}{A_1 \cdot A_2} + \frac{4 \cdot \lambda_{DU}}{A_1 \cdot A_3} + \frac{12 \cdot \lambda_{DD}^2}{A_1 \cdot A_2 \cdot A_4} + \frac{12 \cdot \lambda_{DU}^2}{A_1 \cdot A_3 \cdot A_6} + A_{12} + A_{13} + A_{14} \quad (15)$$

with

$$A_1 = 4 \cdot \lambda_S + 4 \cdot \lambda_{DD} + 4 \cdot \lambda_{DU} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU}$$

$$A_2 = \mu_0 + 3 \cdot \lambda_{DD} + 3 \cdot \lambda_{DU}$$

$$A_3 = \mu_{LT} + 3 \cdot \lambda_{DD} + 3 \cdot \lambda_{DU}$$

$$A_4 = \mu_0 + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU}$$

$$A_5 = \mu_0 + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU}$$

$$A_6 = \mu_{LT} + 2 \cdot \lambda_{DD} + 2 \cdot \lambda_{DU}$$

$$A_7 = \mu_0$$

$$A_8 = \mu_0 + \lambda_{DU}$$

$$A_9 = \mu_0 + \lambda_{DD} + \lambda_{DU}$$

$$A_{10} = \mu_{LT} + \lambda_{DD} + \lambda_{DU}$$

$$A_{11} = \frac{12 \cdot \lambda_{DD} \cdot \lambda_{DU} \cdot (A_2 + A_3)}{A_1 \cdot A_2 \cdot A_3 \cdot A_5}$$

$$A_{12} = \frac{24 \cdot \lambda_{DD}^2 \cdot \lambda_{DU} \cdot (A_2 \cdot A_4 + A_3 \cdot A_4 + A_3 \cdot A_5)}{A_1 \cdot A_2 \cdot A_3 \cdot A_4 \cdot A_5 \cdot A_8}$$

$$A_{13} = \frac{24 \cdot \lambda_{DU}^2 \cdot \lambda_{DD} \cdot (A_2 \cdot A_5 + A_2 \cdot A_6 + A_3 \cdot A_6)}{A_1 \cdot A_2 \cdot A_3 \cdot A_5 \cdot A_6 \cdot A_9}$$

$$A_{14} = \frac{24 \cdot \lambda_{DU}^3}{A_2 \cdot A_3 \cdot A_6 \cdot A_{10}}$$

$$A_{15} = \frac{6 \cdot \lambda_{DD} \cdot \lambda_{DU} \cdot (A_4 + A_5)}{A_2 \cdot A_4 \cdot A_5 \cdot A_8}$$

$$A_{16} = \frac{6 \cdot \lambda_{DD} \cdot \lambda_{DU} \cdot (A_5 + A_6)}{A_3 \cdot A_5 \cdot A_6 \cdot A_9}$$

5 Conclusion

The more safe 2004-architecture will be established within high safety class computers in future. Such computers will be applied in various fields which require simultaneously both: availability and maximal safety. They are applied where human lives need to be protected and/or safed, either in material handling, energy production/distribution, in the medical field or in future industrial power plants in space.

As already mentioned in the introduction, today's technical systems will be more and more complex. Man will no longer be able to provide appropriate safety in processes which have to be monitored. Future safety control must support him, either in recording and analysing data, or in operation resulting from this. Advanced safety architectures like the introduced 2004-system have to be utilized in order to guarantee the required safety. This system combines the benefits of the 1002- and the 2003-system: simultaneously a higher availability and a higher safety than today's systems.

References:

- [1] IEC/EN 61508: *International Standard 61508 Functional safety: Safety-related System*, Geneva, International Electrotechnical Commission
- [2] Börcsök, J.: *International and EU Standard 61508*, Presentation within the VD Conference of HIMA GmbH + CO KG, 2002
- [3] Börcsök, J.: *Elektronische Sicherheitssysteme*, Hüthig publishing company, 2004.
- [4] Börcsök, J.: *Elektronic Safety Systems*, Hüthig publishing company, 2004.
- [5] Börcsök, J.: *Sicherheits-Rechnerarchitektur Teil 1 und 2*, lecture of University of Kassel, 2000/2001.
- [6] Börcsök, J.: *Echtzeitbetriebsysteme für sicherheitsgerichtete Realzeitrechner*, lecture of University of Kassel, 2000/2001.
- [7] DIN VDE 0801: *Funktionale Sicherheit, sicherheitsbezogenener elektrischer/elektronischer/programmierbarer elektronischer Systeme (E/E/PES)*, (IEC 65A/255/CDV: 1998), Page: 27f, August 1998
- [8] DIN V 19250: *Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen*, Beuth publishing company, Berlin 1998
- [9] DIN VDE 0801/A1: *Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben*, Beuth publishing company
- [10] IEC 60880-2: *Software für Rechner mit sicherheitskritischer Bedeutung*, 12/2001