Markov Models for 2004 Architecture for Safety Related Systems

JOSEF BÖRCSÖK
University of Kassel
HIMA GmbH + Co KG
Germany

EVZUDIN UGLJESA
University of Kassel
HIMA GmbH + Co KG
Germany

Keywords: 2oo4-architecture, Markov-model, MTTF, PFD, availability, reliability block diagram

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 a high availability and a high reliability.

1 Introduction

Modern technical systems, controlling and steering safety relevant processes are becoming more and more complex. There are multifarious 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 occuring. 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 save 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 system'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- and outputs, CPU)

- Sensors
- Termination elements such as actuators

Combining 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 an 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** TI = 2 years or TI = 10 years	**Continous/High demand mode of operation** TI = 1 month or TI = 3 months or TI = 6 months or TI = 1 year
1	$\geq 10^{-2}$ - $<10^{-1}$	$\geq 10^{-6}$ - $<10^{-5}$
2	$\geq 10^{-3}$ - $<10^{-2}$	$\geq 10^{-7}$ - $<10^{-6}$
3	$\geq 10^{-4}$ - $<10^{-3}$	$\geq 10^{-8}$ - $<10^{-7}$
4	$\geq 10^{-5}$ - $<10^{-4}$	$\geq 10^{-9}$ - $<10^{-8}$

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 an 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 save failures λ_S and dangerous failures. In addition, save failures are subdivided into save undetected failures λ_{SU} and save detected failures λ_{SD}. Whereas dangerous failures are subdivided into dangerous undetected failures λ_{DU} and dangerous detected failures λ_{DD}. Figure 1 shows the spreading of failure rates. Failure rates could be specified with the aid of standard specifications.

Figure 1: Failure rates

A system's quality can be specified by defining its PFD 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 PFD value. The PFD value is calculated for a period of time that lies between two proof check intervals. 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 PFD average value (PFD_{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) architecture 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. The 2oo3-architecture, s. figure 3, distinguishes by it that at least two of the three 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 systems in industry you must develop a 2oo4-architecture. This architecture will be described in the following.

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

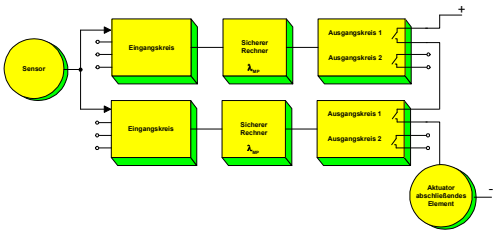

Figure 2: Reliability block diagram of 1oo2-architecture

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.

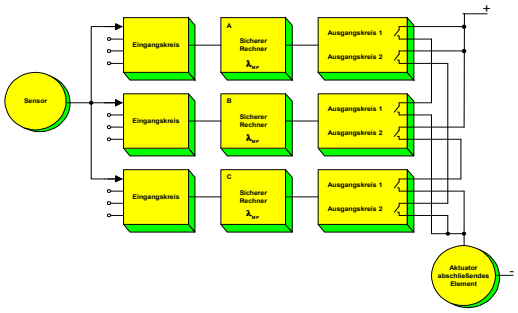

Figure 3: Reliability block diagram of 2oo3-architecture

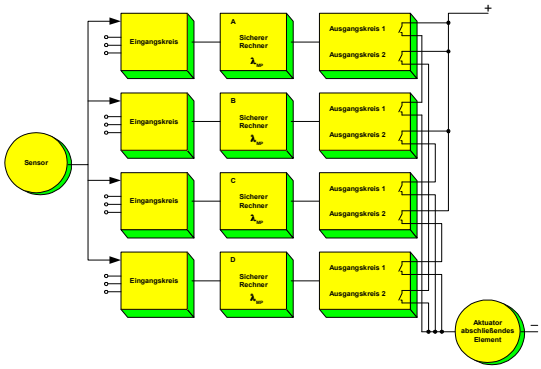

Figure 4: Reliability block diagram of 2oo4-architecture

In a fault-tree-analysis you can determine the following failures 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 / presents. 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 channels there is no possibility to switch off the process in a safe state. So the difference between the 2oo4-system and a 1oo2-system is the higher availability of the 2oo4-system and it has a light better probability of the safe-function.

3 Calculation of probability distributions

3.1 PFD_{avg}-equation for a 2oo4-system

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

$$P(t) = 4 \cdot P_1(t) \cdot P_2(t) \cdot P_3(t) + P_{DUC}(t) + P_{DDC}(t) \qquad (1)$$

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

3.2 Calculation of probability of normal failures

You can show after diverse conversions / calculations that the probability of simultaneous occured three normal failures can describe with the following equation:

$$\begin{aligned} PFD_{avg,\,einfach} &= 4 \cdot P_1(t) \cdot P_2(t) \cdot P_3(t) \\ &= 24 \cdot \lambda'^{\,3}_D \cdot t'_{CE} \cdot t'_{GE} \cdot t'_{SE} \end{aligned} \qquad (2)$$

with

$$t'_{CE} = \frac{\lambda_{DD}}{\lambda'_D} \cdot MTTR + \frac{\lambda_{DU}}{\lambda'_D} \cdot \left(\frac{TI}{2} + MTTR \right) \qquad (3)$$

$$t'_{GE} = \frac{\lambda_{DD}}{\lambda'_D} \cdot MTTR + \frac{\lambda_{DU}}{\lambda'_D} \cdot \left(\frac{TI}{3} + MTTR \right) \qquad (4)$$

$$t'_{SE} = \frac{\lambda_{DD}}{\lambda'_D} \cdot MTTR + \frac{\lambda_{DU}}{\lambda'_D} \cdot \left(\frac{TI}{4} + MTTR \right) \qquad (5)$$

$$\lambda'_D = (1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU} \qquad (6)$$

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \qquad (7)$$

3.3 Calculation of probability of common-cause failures

The equation of probability of dangerous detected and dangerous undetected common-cause failures P_{DUC} und P_{DDC} is identically with the equation of a 1oo2-system. The PFD_{avg}-equation for common-cause failures means:

$$PFD_{avg,\beta} = \left[\beta \cdot \lambda_{DU} \cdot \left(\frac{TI}{2} + MTTR \right) + \beta_D \cdot \lambda_{DD} \cdot MTTR \right] \qquad (8)$$

3.4 Calculation of probability of failure with simultaneous consideration of normal and common-cause failures

The PFD_{avg}-term of a 2oo4-system in consideration of normal and common-cause failures, equation (2) and (8), means:

$$\begin{aligned} PFD_{avg,\,2oo4} = {} & 24 \cdot \lambda'^{\,3}_D \cdot t'_{CE} \cdot t'_{GE} \cdot t'_{SE} + \beta_D \cdot \lambda_{DD} \cdot MTTR \\ & + \beta \cdot \lambda_{DU} \cdot \left(\frac{TI}{2} + MTTR \right) \end{aligned} \qquad (9)$$

4 Markov-model of a 2oo4-architecture

Basically is the Markov-model of a 2oo4-"Single-Board System" accomplished with conventional calculation methods. The single transitions are shown in figure 4. 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.

In state 3 is one of the four channels faulty. The occurred failure is dangerous and will not recognize by the failure-diagnostic. The occurrence of another failure in state 3 of one of the faultless channels passes the system over in state 5 or state 6. If in state 3 occur no more failures for the whole lifetime, the system passes over into state 0. In applications signifies

that: Is the time τ_{LT} expired the whole system will be exchanged.

In case the second failure in state 3 is a dangerous detectable failure the system is transferred to state 5. In state 5 is one of the channels afflicted with a dangerous detected failure and another channel with a dangerous undetected failure at the same time. If in state 3 the second failure is a dangerous undetected failure the system passes over to the state 6. State 6 is distinguished by two dangerous undetected failures in two of the four channels. There is no possible transition for the system to reach the safety state 1 into the test-interval τ_{Test}, because in state 6 is given no error detection. After the time τ_{LT} is expired the whole system will be exchanged.

If 2oo4-systems perform common-cause-failures, we have to distinguish two cases:

- The common failure-cause introduces to dangerous detected failures. In this case the system passes over from state 0 directly to state 11. Therefore obtains the transition-rate $\beta_D \cdot \lambda_{DD}$.
- The common failure-cause introduces to dangerous undetected failures. In this case the system passes over from state 0 directly to state 14. Therefore obtains the transition-rate $\beta \cdot \lambda_{DU}$.

In summary the following can be retained:

- Occurs the state 11, the system will be transferred immediately into the safe state 1.
- If the 2oo4-system resides into the states 8, 9, 12 or 13 because of occurred failures, the system will be into the safe state in less than $4 \cdot \tau_{Test}$ times. The transition-rates for this states are always $\mu_0 = \frac{1}{\tau_{Test}}$.
- The states 1, 11, 12, 13 and 14 are absorbing states, out of this states are no possible transitions to other states with additional failure modes available.

In the states 0, 2, 3, 4, 5, 6, 8, 9 and 10 the system is operating. These states must be considered for the MTTF-calculation of the 2oo4-system.

5 Calculating the MTTF-value

The MTTF-value describes the mean time elapsing between to occurring failures. The beginning state of the system without any failure is always state 0. The so-called transition-matrix **P** can be evaluated from the 2oo4-Markov-model. It describes mathematically the transitions between each state utilising probability densities. Evaluating the MTTF-value covers only those states, fulfilling the following criteria:

- System operating
- No absorbing state

These states are extracted from the **P**-matrix generating the **Q**-matrix. System operation, in this 2oo4-system, is possible in states 0, 2, 3, 4, 5, 6, 8, 9 and 10. Since states 1, 7, 11, 12, 13, 14 and 15 are absorbing states they need not to be considered while calculating the MTTF-value. In the used Markov-model the system's lifetime is assumed to be infinite. Next, the **N**-matrix has to be developed applying the following formula:

$$N = [I - Q]^{-1} \tag{10}$$

The **N**-matrix is the inverse matrix of the [**I** – **Q**]-matrix. After having inverted the matrix, the elements of the new matrix represent time-dependant terms. Calculating the system's MTTF-value, requires adding all elements along the first line of the **N**-matrix. Then the MTTF-value of an 2oo4-system can be described by the following equation:

$$MTTF_{2oo4} = \frac{1}{A_1} + \frac{4 \cdot \lambda_{DD}}{A_1 \cdot A_2} + \frac{4 \cdot \lambda_{DU}}{A_1 \cdot A_3} + \frac{12 \cdot \lambda_{DD}^2}{A_1 \cdot A_2 \cdot A_4} + A_{11} + \frac{12 \cdot \lambda_{Du}^2}{A_1 \cdot A_3 \cdot A_6} + A_{12} + A_{13} + A_{14} \tag{11}$$

6 Conclusion

The more save 2oo4-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 saved, 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 2oo4-system have to be utilised in order to guarantee the required safety. This system combines the benefits of the 1oo2- and the 2oo3-system: simultaneously a higher availability and a higher safety than today's systems.

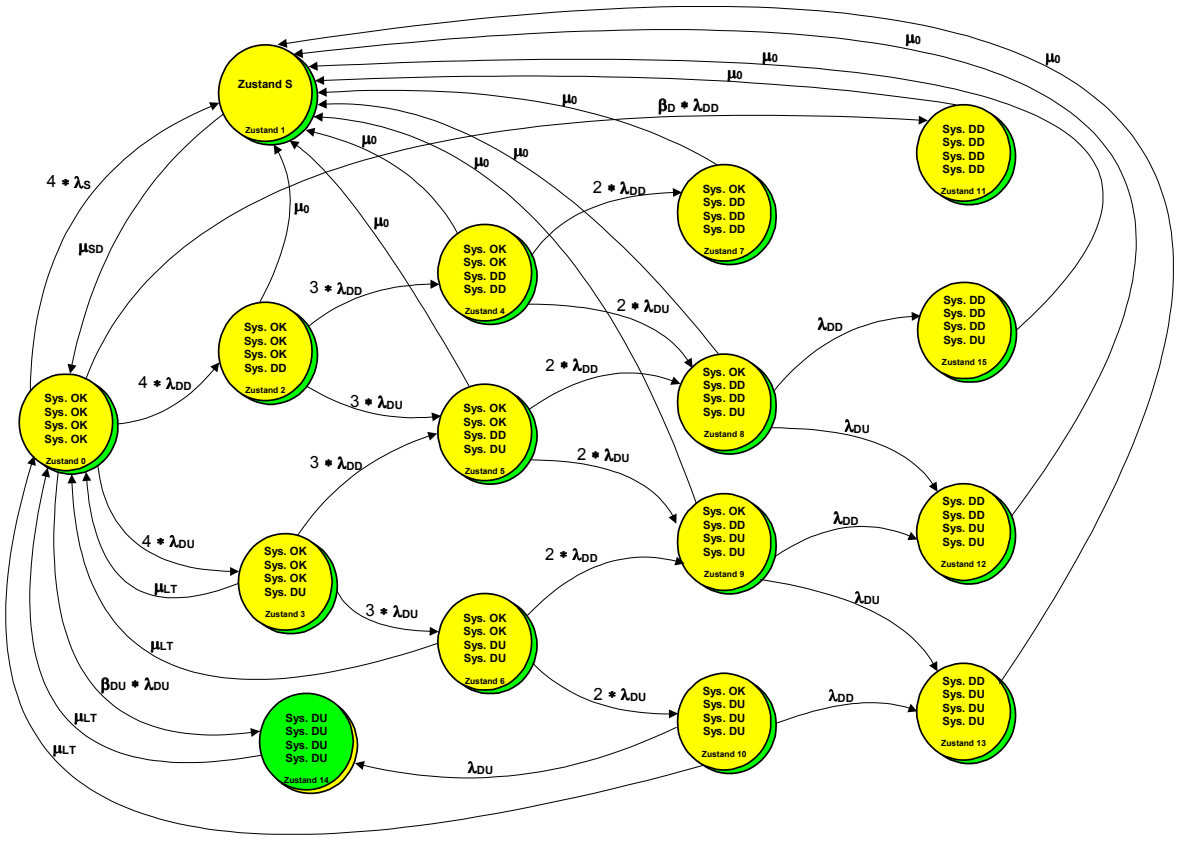

Figure 5: 2oo4-Markov-Modell

References

Baca, A., 1993, "Examples of Monte-Carlo-methods in reliability estimation based on reduction of prior information", *IEEE transaction on reliability*, Vol. 42, No. 4

Bellcore, 1995, "Reliability Prediction Procedure for electronic equipment", *NJ, Bellcore 4th Ed.,* TR-332,

Fishman, G. S., "Monte-Carlo Concepts, Algorithms and Applications", *Springer Verlag, Berlin*

Gnedenko, B. V. Rossberg, H.-J.; "Einführung in die Wahrscheinlichkeitstheorie", *Akademie-Verlag, Berlin*

Kumamoto, H. Henley, E. J., 1993, "Probabilistic Risk Assessment and Management for Engineers and Scientists", *New York IEEE*

Kim, Chul, Lee, H. K., 1992, "A Monte Carlo Simulation Algorithm for finding MTBF", *IEEE Transaction on Reliability*, Vol. 41, No. 2

Kim, Chul, 1989, "MTBF of a complex binary coherent system", *IEEE Transaction on Reliability*, Vol. 38, No. 4

Robert, C. P., Casella, G., "Monte Carlo; Statistical Methods", *Springer Verlag, Berlin*

Shanmugam, R., Richards, D. O., 1989, "On Estimating the Mean Time to Failure with unknown censoring", *IEEE Transaction on Reliability*, Vol. 38, No. 3

Shoeman, M. L., 1968, "Probabilistic reliability: An engineering approach", *Mc-Graw-Hill*, New York,

Sobol, M., 1985, "Die Monte-Carlo-Methode", *Verlag der Deutschen Wissenschaften*