Calculation of the Probability of Failure on Demand of Redundant Systems Using Markov Model

1,2 Yanli Zhang, 1 Jun Dai and 3 Dasheng Zhu
1 School of Physical and Mechanical Engineering, Xi’an University of Arts and Science, Xi’an, Shanxi, 710065, China
2 College of Mechanical Engineering, Nanjing Institute of Technology, Nanjing, Jiangsu, 211167, China

Abstract: It is necessary to calculate the "Probability of Failure on Demand" (PFD) and "Probability of Failure of Safety" (PFS) for the assessment of the "Safety Integrity Level" (SIL) of a Safety Instrumented System (SIS) in the international standard IEC 61508 (2000). To fulfill the high safety and availability requirements redundant channels are often used which are normally homogeneous. Whereas, in order to minimize the potential Common Cause Failures (CCF) for very high safety requirements (e.g. SIL 4) it may be advisable to build up a heterogeneous system with different hardware/software platforms. For such type of heterogeneous systems the calculation of the PFD is a challenge because the failure rates of the particular channels are different in general and no formulas are included in the standard. Within the scope of this work, the physical block diagram and the voting diagram for 2oo3 redundant system are introduced, then based on them, the Markov-model method is used to simulate these redundant systems, including both the homogeneous and the heterogeneous systems.

Key words: Functional safety, redundant system, probability of failure on demand, markov model

INTRODUCTION

It is necessary to calculate the "Probability of Failure on Demand" (PFD) of a safety function for the assessment of the "Safety Integrity Level" (SIL) of a Safety Instrumented System (SIS) with the international standard IEC 61508 (2000). To fulfill the high safety and availability requirements redundant channels are often used, 1oo2, 2oo2 or 2oo3. Standard formulas for PFD calculation of a homogeneous system (with identical channels) are given in IEC 61508 (2000), part 6. In applications with very high safety and/or availability requirements other configurations like homogeneous 2oo4 or heterogeneous 2oo3 have to be used. An example of a homogeneous 2oo4 system is the reactor power limitation system in some nuclear power plants (Ding, 2010), whereas in the airplane industry heterogeneous 2oo3 configurations (channels with different hardware/software components) are widely used (Burz, 2010). Heterogeneous systems with functional or equipment diversity are suitable to minimize the potential of Common Cause Failures (CCF) and Common Mode Failures (CMF) for very high safety requirements (e.g. SIL 4). For such type of heterogeneous systems the calculation of the PFD is a challenge because the failure rates of the particular channels are different in general and no formulas are included in the standard. Some investigations were performed under certain simplified assumptions (Hildebrandt, 2007; Hildebrandt et al., 2008).

Within the scope of this work, the physical block diagram and the voting diagram for 2oo3 redundant system are introduced and the complete formulas for 2oo3 structure are given following the principles of the IEC 61508 (2000), then based on them, the Markov-model method is used to simulate these redundant systems, including both the homogeneous and the heterogeneous systems.

PHYSICAL BLOCK DIAGRAM AND THE VOTING DIAGRAM

Safety Instrumented System (SIS) is the system configurations consisting of channels. In each channel, four different types of failures happen which differ in detected dangerous failure, undetected dangerous failure, detected safe failure and undetected safe failure. Fig. 1 shows the physical block diagrams of 2oo3 architectures. This architecture consists of three parallel channels connected to a majority decision. If only one channel changes the initial state while the other two channels do not change, then the output initial state is not changed. Fig. 2 shows that switches A and B are connected in

Corresponding Author: Jun Dai, School of Physical and Mechanical Engineering, Xi’an University of Arts and Science, Xi’an, Shanxi, 710065, China
The meaning of down time, $t_{d1}$: In the standard IEC 61508 (2000), system configurations are composed of channels. Each channel includes both detectable failures with rate $\lambda_{DD}$ by self-diagnosis and undetectable failures with rate $\lambda_{UD}$. The failure rates $\lambda_{DD}$ and $\lambda_{UD}$ are assumed to be constants. Hence, the times of occurrences for these two kinds of failures follow the exponential distributions. For the detected dangerous fault is repaired to be good, the MTTR is used. However, the undetectable dangerous fault cannot be detected until the next proof test. It follows such a process as shown in Fig. 3. In this figure, $t_d$ is the time of occurrence of the failure and $t_i$ is the duration of down time.

**THE FORMULA TO CALCULATE PFD of 2oo3**

In the standard, $t_d$ is not clearly defined. However it is the basis to get all results of average probability of failure on demand of typical system architectures. If its meaning is not clear it is not easy for a safety engineer to understand all of other solutions. Here, $t_{d1}$ is named equivalent mean down time for the undetectable fault in a channel. It is defined as follows:

$$t_{d1} = T_i - t_i + \text{MTTR}$$  \hspace{1cm} (1)

Suppose $t_i$ is the time when the average probability of failure for the undetectable fault in the interval $[0, T_i]$ occurs in a system. Since $\lambda_{UD}T_i < 1$ and $\exp(-\lambda_{UD}T_i) = 1 - \lambda_{UD}T_i$, Zhang et al. (2003) give the formula of $t_i$:

$$t_i = T_i/2$$ \hspace{1cm} (2)

Therefore:

$$t_{d1} = T_i/2 + \text{MTTR}$$ \hspace{1cm} (3)

Similarly, for 1oo2, 2oo3 architecture, the following formula can be obtained:

$$t_{d1} = T_i/3 + \text{MTTR}$$ \hspace{1cm} (4)

**The Equation of PFD**: Based on the above, following the method given by Hildebrandt (2007) and considering the PFD that is caused by CCF, the theoretical equation for the PFD of 2oo3 architecture can be derived and the detailed derivation process is abbreviated here.

$$PFD_{2oo3} = \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} \cdot \lambda_{UD}) + \frac{1}{3}T_i \cdot 2\cdot \text{MTTR} \cdot (\lambda_{DD} \cdot \lambda_{DD}^2 + \lambda_{DD} \cdot \lambda_{UD} + \lambda_{UD} 


When $\lambda_{D01} = \lambda_{D02} = \lambda_{DD0} = \lambda_{DD1} = \lambda_{DD2} = \lambda_{DD}$ this equation is the same with the following Equation which is given in the standard IEC 61508 (2000):

$$PFD = \Phi(1 - \beta)\lambda_{D0} + (1 - \beta)\lambda_{D1}\beta_{D} + \beta_{D}\lambda_{DD}\frac{MTTR}{MTTR} + \beta_{D}T_{p}/2 + MTTR$$

(6)

**VERIFICATION WITH MARKOV-MODEL**

**Markov model:** Based on the voting diagram shown in Fig. 2, the corresponding Markov state transmission process for homogenous and heterogeneous 2oo3 systems considering the common cause failure can be obtained. Guan (2011) gave the Markov state of homogeneous 2oo3 systems and the Markov state of heterogeneous 2oo3 systems are shown in Fig. 4.

Because the value of PFD cannot be affected by system safe failure, the states of safe failure are not considered for convenience in Fig.4. Besides, the situation of the channels 1, 2 and #3 failure simultaneously is not considered due to the product $\lambda_{0\alpha}$ and $T_{i}$ significantly smaller than unit one, so the simplified Markov-model for heterogeneous 2oo3 system can be obtained.

**Simulation result:** For a heterogeneous 2oo3 system with the following failure rates:

![Diagram](image-url)

- Channel #1: \( \lambda_{o|o} = 2 \times 10^{-7} \text{ h}^{-1} \), \( \lambda_{o|c} = 7 \times 10^{-6} \text{ h}^{-1} \)
- Channel #2: \( \lambda_{o|c} = 7 \times 10^{-6} \text{ h}^{-1} \), \( \lambda_{c|c} = 2 \times 10^{-5} \text{ h}^{-1} \)
- Channel #3: \( \lambda_{o|c} = 1 \times 10^{-6} \text{ h}^{-1} \), \( \lambda_{c|c} = 5 \times 10^{-6} \text{ h}^{-1} \)

The factors \( \Box \) and \( O \) for the common cause failure are assumed to be 1%. The proof test interval is defined as one year, the mean time to repair MTTR as 8 h. The calculated PDF by the Markov Model is \( 5.41 \times 10^{-6} \) while the result of formula is \( 6.41 \times 10^{-6} \). The results showed a good correspondence.

Considering a heterogeneous 2oo3 system with the following failure rates:

- Channel #1: \( \lambda_{o|o} = 1 \times 10^{-4} \text{ h}^{-1} \), \( \lambda_{o|c} = 9 \times 10^{-4} \text{ h}^{-1} \)
- Channel #2: \( \lambda_{o|c} = 2 \times 10^{-4} \text{ h}^{-1} \), \( \lambda_{c|c} = 18 \times 10^{-4} \text{ h}^{-1} \)
- Channel #3: \( \lambda_{o|c} = 5 \times 10^{-4} \text{ h}^{-1} \), \( \lambda_{c|c} = 48 \times 10^{-4} \text{ h}^{-1} \)

The factors \( \beta \) and \( \beta_c \) for the common cause failure are assumed to be 1% because the diversity is quite good due to the heterogeneous system design. The proof test interval is defined as one year and the mean time to repair MTTR as 8 hours which are the default value of the IEC 61508 (2000). The calculated PDF by the Markov Model is \( 3.88 \times 10^{-6} \).

Comparing it with a homogeneous 2oo3 system that have same failure rates:

\[ \lambda_{o|o} = 1 \times 10^{-4} \text{ h}^{-1} \]
\[ \lambda_{o|c} = 9 \times 10^{-4} \text{ h}^{-1} \]

The factors \( \beta \) and \( \beta_c \) for the common cause failure are assumed to be 10 and 5%. The calculated PDF by the Markov Model is \( 4.28 \times 10^{-4} \) which is higher than the heterogeneous 2oo3 system even the channels #2 and #3 have higher failure rates. The main reason is the influence of the common cause failure, i.e. the fractions of the common cause failure of the homogeneous system is higher than those of the heterogeneous ones.

**CONCLUSION**

Based on the ideas of IEC 61508 (2000), the formula and Markov model are for homogeneous and heterogeneous 2oo3 systems are given. The results showed a good correspondence. Compared with Markov model the formula is very simple and might be helpful for practical engineers.

Comparing the homogeneous and heterogeneous 2oo3 configurations showed that due to the influence of the common cause failure the PFD of the homogeneous system is higher than those of the heterogeneous ones. Failure rates that are not denoted in figure are:

- For Channel #1 from state "ok" to "DD"
- For Channel #1 from state "ok" to "DU"
- For detected CCF
- For undetected CCF

Maintenance rates in figure are:

- 1/MTTR, for detected CCF and Channel #1 from state "DD" to "ok"
- 2/(T_2+2MTTR), from undetected CCF and Channel #1 state "DU" to "ok"
- 3/(T_2+3MTTR), for two channels from state "DU" to "ok" simultaneously

**NOMENCLATUR:**

- SIS Safety Instrumented System
- SIF Safety Instrumented Function
- SIL Safety Integrity Level
- PFD Probability of Failure on Demand
- \( \lambda_f \) failure rate of safe failures (h\(^{-1}\))
- \( \lambda_c \) failure rate of dangerous failures (h\(^{-1}\))
- \( \lambda_{tc} \) failure rate of detected dangerous failures (h\(^{-1}\))
- \( \lambda_{tc} \) failure rate of undetected dangerous failures (h\(^{-1}\))
- \( t_{eq} \) channel equivalent mean down time (h)
- \( t_{eg} \) voted group equivalent mean down time (h)
- \( T_2 \) Proof Test Interval (h)
- MTTR Mean Time To Restoration (h)
- MDT Mean Down Time (h)
- \( \beta \) the fraction of undetected fault that have a common cause
- \( \beta_c \) the fraction of detected fault that have a common cause
- CCF Common Cause Failure
- CCF_U Undetected Common Cause Failure
- CCF_D Detected Common Cause Failure

**ACKNOWLEDGMENTS**

This study is supported by the fundamental of Nanjing Institute of Technology (CKJ2011001), the fund of Shanxi Department of Education and the fund of Xi'an Technology Bureau, PR China.

**REFERENCES**


