http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (20): 5477-5481, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.5477.5481

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

[1,2]Yanli Zhang, [1]Jun Dai and [2]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. SIL4) 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 homogenous 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 (Butz, 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. SIL4). 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

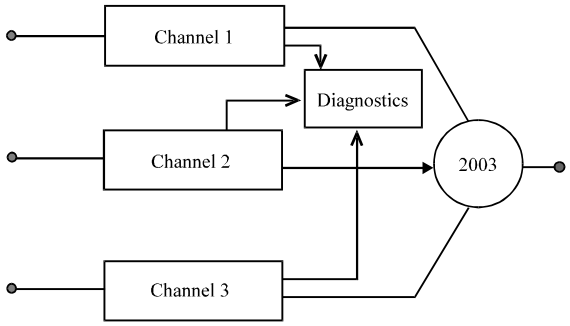

Fig. 1: Physical block diagrams (Zhang *et al*., 2003)

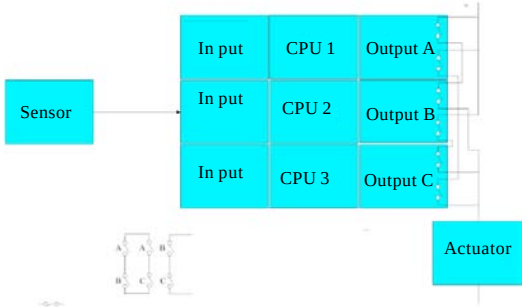

Fig. 2: 2oo3 Architecture voting diagram (Guan, 2011)

series, switches A and C are connected in series and switches B and C are also connected in series. All three series circuits are connected in parallel. When the first channel has a safe failure, switch A is always open, the circuit is dependent on switch B and C. And Switch B and C are connected in series which corresponds to the 1oo2 architecture. When the first channel has a dangerous failure, switch A always remains close, then if one of switches B and C change to close, the circuit is switched on which corresponds to the architecture 2oo2.

THE FORMULA TO CALCULATE PFD of 2oo3

Meaning of down time, t_{c1}: In the standard IEC 61508 (2000), system configurations are composed of channels. Each channel includes both detectable failures with rate λ_{DD} by self-diagnosis and undetectable failures with rate λ_{DD}. The failure rates λ_{DD} and λ_{DU} 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_a is the time of occurrence of the failure and t_d is the duration of down time.

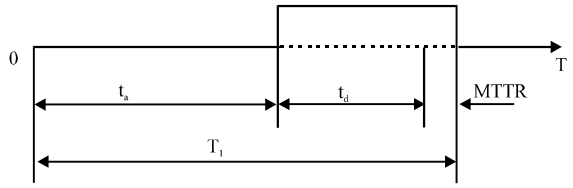

Fig. 3: Process for the undetected dangerous fault (Zhang *et al*., 2003)

In the standard, t_{c1} 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_{c1} is named equivalent mean down time for the undetectable fault in a channel. It is defined as follows:

$$t_{c1}=T_1-t_a+MTTR \quad (1)$$

Suppose t_a is the time when the average probability of failure for the undetectable fault in the interval $[0,T_1]$ occurs in a system. Since $\lambda_{DU}T_1<<1$ and $\exp(-\lambda_{DU}T_1)\approx 1-\lambda_{DU}T_1$, Zhang *et al*. (2003) gave the formula of t_a:

$$t_a \tilde{} T_1/2 \quad (2)$$

Therefore:

$$t_{c1}=T_1/2+MTTR \quad (3)$$

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

$$t_{c1}=T_1/3+MTTR \quad (4)$$

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.

$$\begin{aligned}
PFD_{2oo3} &= \frac{1}{3}\cdot T_1^2\cdot(1-\beta)^2(\lambda_{DU1}\cdot\lambda_{DU2}+\lambda_{DU1}\cdot\lambda_{DU3}+\lambda_{DU2}\cdot\lambda_{DU3})\\
&+\frac{1}{3}T_1\cdot MTTR\begin{Bmatrix}5(1-\beta)^2(\lambda_{DU1}\cdot\lambda_{DU2}+\lambda_{DU1}\cdot\lambda_{DU3}+\lambda_{DU2}\cdot\lambda_{DU3})\\+(1-\beta(1-\beta_D([\lambda_{DD1}(\lambda_{DU2}+\lambda_{DU3}(+\lambda_{DD2}(\lambda_{DU1}+\lambda_{DU3}(+\lambda_{DD3}(\lambda_{DU1}+\lambda_{DU2})]\end{Bmatrix}\\
&+2MTTR^2\begin{Bmatrix}(1-\beta((1-\beta_D)[\lambda_{DU1}(\lambda_{DD2}+\lambda_{DD3})+\lambda_{DU2}(\lambda_{DD1}+\lambda_{DD3})+\lambda_{DU3}(\lambda_{DD1}+\lambda_{DD2})]\\+2(1-\beta_D)^2(\lambda_{DD1}\cdot\lambda_{DD2}+\lambda_{DD1}\cdot\lambda_{DD3}+\lambda_{DD2}\cdot\lambda_{DD3})\\+2(1-\beta)^2(\lambda_{DU1}\cdot\lambda_{DU2}+\lambda_{DU1}\cdot\lambda_{DU3}+\lambda_{DU2}\cdot\lambda_{DU3})\\+(1-\beta)(1-\beta_D)[\lambda_{DD1}(\lambda_{DU2}+\lambda_{DU3})+\lambda_{DD2}(\lambda_{DU1}+\lambda_{DU3})+\lambda_{DD3}(\lambda_{DU1}+\lambda_{DU2})]\end{Bmatrix}\\
&+\beta\cdot\sqrt{\frac{1}{3}(\lambda_{DU1}\cdot\lambda_{DU2}+\lambda_{DU2}\cdot\lambda_{DU3}+\lambda_{DU1}\cdot\lambda_{DU3})}(\frac{T_1}{2}+MTTR)\\
&+\beta_D\cdot\sqrt{\frac{1}{3}(\lambda_{DD1}\cdot\lambda_{DD2}+\lambda_{DD2}\cdot\lambda_{DD3}+\lambda_{DD1}\cdot\lambda_{DD3})}\cdot MTTR
\end{aligned} \quad (5)$$

When $\lambda_{DD1} = \lambda_{DD2}$, $\lambda_{DD3} = \lambda_{DD}$, $\lambda_{DD1} = \lambda_{DD2} = \lambda_{DD3} = \lambda_{DD}$ this equation is the same with the following Equation which is given in the standard IEC 61508 (2000):

$$PFD = 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}(T_1/2 + MTTR) \quad (6)$$

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 btained. Guan (2011) gave the Markov state of homogenous 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 λ_{DDi} and T_1 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:

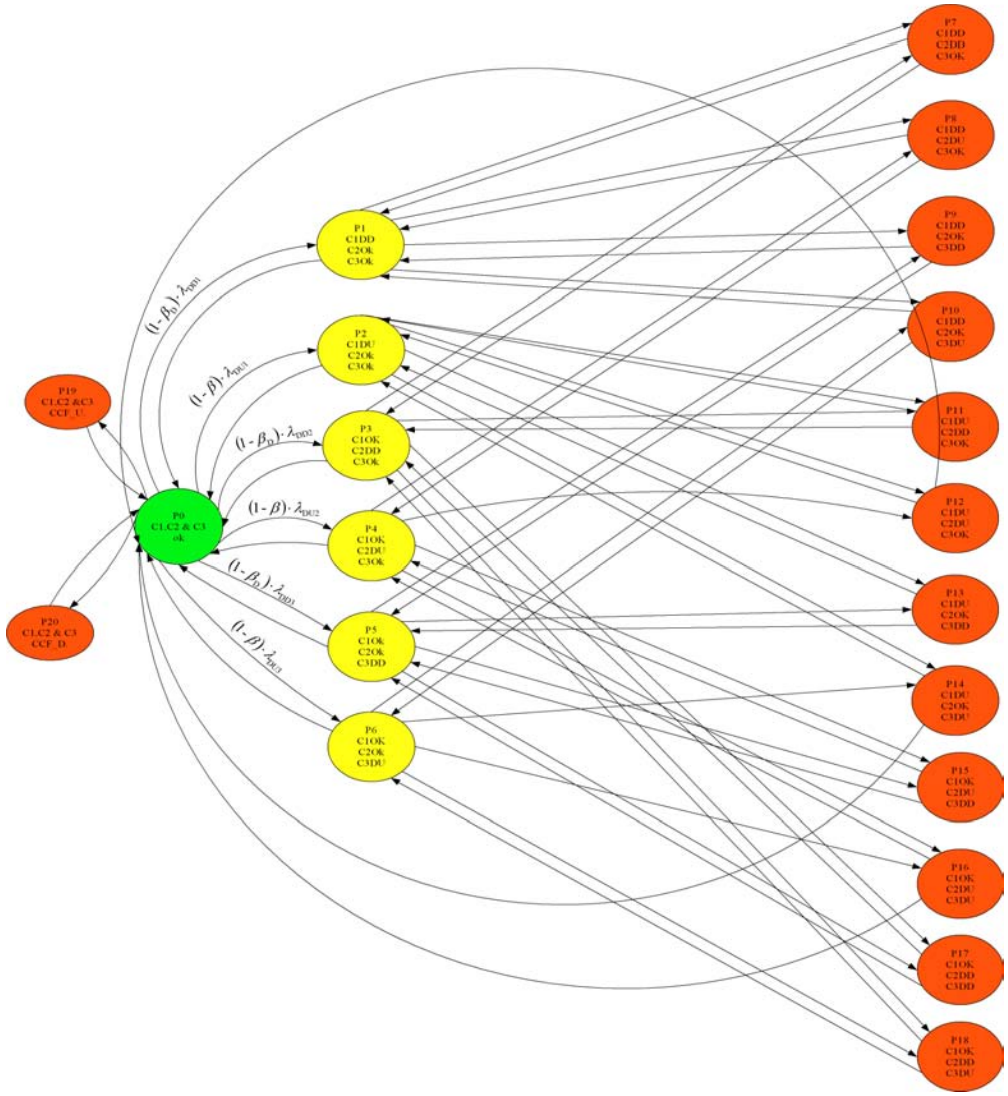

Fig. 4: Markov state transmission process for heterogeneous 2oo3

- Channel #1: $\lambda_{DUI} = 2\times10^{-7}\ h^{-1}$, $\lambda_{DDI} = 7\times10^{-6}\ h^{-1}$
- Channel #2: $\lambda_{DU2} = 7\times10^{-8}\ h^{-1}$, $\lambda_{DD2} = 2\times10^{-6}\ h^{-1}$
- Channel #3: $\lambda_{DU3} = 1\times10^{-6}\ h^{-1}$, $\lambda_{DD3} = 5\times10^{-6}\ h^{-1}$

The factors □ and $\square_D$ 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 5.41×10^{-6} while the result of formula is 6.41×10^{-6}. The results showed a good correspondence.

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

- Channel #1: $\lambda_{DUI} = 1\times10^{-6}\ h^{-1}$, $\lambda_{DDI} = 9\times10^{-6}\ h^{-1}$
- Channel #2: $\lambda_{DU2} = 2\times10^{-6}\ h^{-1}$, $\lambda_{DD2} = 18\times10^{-6}\ h^{-1}$
- Channel #3: $\lambda_{DU3} = 5\times10^{-6}\ h^{-1}$, $\lambda_{DD3} = 45\times10^{-6}\ h^{-1}$

The factors β and β_D 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 3.88×10^{-4}.

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

$$\lambda_{DU} = 1\times10^{-6}\ h^{-1},\ \lambda_{DD} = 9\times10^{-6}\ h^{-1}$$

The factors β and β_D for the common cause failure are assumed to be 10 and 5%. The calculated PDF by the Markov-Model is 4.28×10^{-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 #*i* from state"ok"to"DD"
- For Channel #*i* from state"ok"to"DU"
- For detected CCF
- For undetected CCF

Maintenance rates in figure are::

- 1/MTTR, for detected CCF and Channel #*i* from state "DD" to "ok"
- $2/(T_1+2MTTR)$, from undetected CCF and Channel #*i* state "DU" to "ok"
- $3/(T_1+3MTTR)$, 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
- λ_S failure rate of safe failures (h^{-1})
- λ_D failure rate of dangerous failures (h^{-1})
- λ_{DD} failure rate of detected dangerous failures (h^{-1})
- λ_{DU} failure rate of undetected dangerous failures (h^{-1})
- t_{CE} channel equivalent mean down time (h)
- t_{GE} voted group equivalent mean down time(h)
- T_1 Proof Test Interval (h)
- MTTR Mean Time To Restoration (h)
- MDT Mean Down Time (h)
- β the fraction of undetected fault that have a common cause
- λ_D 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 fund of Nanjing Institute of Technology (CKJ2011001), the fund of Shanxi Department of Education and the fund of Xi'an Technology Bureau, PR China.

REFERENCES

Butz, H., 2010. Achieving safety in aeronautic systems by fault tolerant design and cooperative human centered automation; 2. Proceedings of the Symposium Digital Safety I and C, September 23-24, 2010, Ehemaliges Hauptzollamt Hamburg,.

Ding, Y., 2010. Zuverlassigkeit eines Leitsystems mit 2004 Struktur. Automatisieren! Digitale Ausgabe atp, Oldenbourg Industrieverlag, June, 2010.

Guan, D., 2011. Zuverlaessigkeits modellierung mit Markov ketten und Vergleich der Nachweismethoden der Funktionalen Sicherheit. Unveroffentlicht Diplomarbeit, Hochschule Magdeburg-Stendal(FH).

Hildebrandt, A., 2007. Berechnung der Probability of Failure on Demand (PFD) einer heterogenen 1-aus-2-struktur in anlehnung an die EN 61508. Automatisierungstechnische Praxis (ATP), Oldenbourg Verlag, Oktober, 2007, pp: 73-802.

Hildebrandt, A., 2007. Calculating the Probability of Failure on Demand (PFD) of complex structures by means of Markov Models. Proceedings of the 4th European Conference on Electrical and Instrumentation Applications in the Petroleum and Chemical Industry, June 13-15, 2007, Paris, pp: 1-5.

Hildebrandt, A., D. Dupond and L. Litz, 2008. Berechnung der Ausfallwahrscheinlichkeit (PFD) von heterogenen mehrkanaligen Sicherheitskreisen mittels effektiver Fehlerraten. Automation 2008-Losungen fur die Zukunft, VDI/VDE-Berichte 2032, VDI-Verlag, Dusseldorf, April, 2008.

IEC 61508, 2000. Functional safety of electric/electronic/programmable electronic safety-related systems, parts. IEC 61508, October 1-7, 1998-May 2000. http://www.iec.ch/abou t/brochures /pdf/ technology/functional_safety.pdf

Zhang, T., W. Long and Y. Sato, 2003. Availability of systems with Self-diagnostic components-applying Markov model to IEC 61508-6. Reliability Eng. Syst. Safety, 80: 133-141.