Markov Modeling of Double 2-out-of-2 System with Imperfect Detection and Common Cause Failures*

Zengkai Liu, Yonghong Liu*, Baoping Cai, Ju Li and Xiaojie Tian

Mechanical and Electronic Engineering, China University of Petroleum, Qingdao 266580, China
{liuzengk & liuyhupc & caibaoping987 & lijumiao & tianxj20050101}@163.com

Abstract - This paper introduces the structure of the double 2-out-of-2 system and presents its Markov model for performance analysis. Transient reliability and safety of the system are obtained. In addition, the effects of imperfect diagnostic coverage and common cause failures on the reliability and safety of the system are researched. The results demonstrate that increasing the diagnostic coverage and decreasing the factor of common cause failures can improve the performance of the double 2-out-of-2 system.

Index Terms - Double 2-out-of-2 system; Markov; common cause failure; diagnostic coverage; reliability

1. Introduction

A computer control system makes use of computers or computer network to control the devices. In order to improve the reliability and safety of the system, redundancy technique is widely used in various control systems [1-5]. For example, a hot standby system in component level is usually realized with parallel hardware structure and several identical components work in parallel, improving the capacity of fault tolerance. For the complicated system with high reliability, especially the critical elements connecting with human safety, redundancy design has become the main method to ensure the reliability and safety. Redundancy technique can be divided into hardware redundancy, software redundancy, time redundancy and information redundancy [6]. The core of hardware redundancy is to backup the elements and set up the work pattern. The faulty elements will be deleted or replaced without affecting the normal operation of the system. The reliability of all parts of the control system, including the sensors, actuators and controlled device, can be improved by hardware redundancy [7]. The most classical hardware redundancy is triple modular redundancy structure and one fault can be masked using majority voting [8]. Hardware redundancy could increase the weight, volume and cost of the system. However, it is easily implemented and reliable. Hardware redundancy is still widely used in aviation, aerospace fields and safety-critical systems.

This paper introduces the structure of the double 2-out-of-2 system and presents its Markov model for performance analysis. This paper is structured as follows. Section 2 describes the proposed system. Section 3 presents the Markov model of the system. In section 4, the formula to calculate the reliability index is derived. Section 5 the results are discussed. Section 6 summarizes the paper.

2. System Description and Modeling

A double 2-out-of-2 system is shown in Figure 1. The system is comprised of two subsystems and a selector. For the subsystem, two identical modules and a voter is adopted. When the two modules are in normal operation, the voter will compare their output values of the modules. If the values are the same, they will be chosen by the output selector as the output value. If a module of the subsystem fails, the selector will block the subsystem.

In normal circumstances, output value of the active subsystem is chosen to control the device while the other subsystem is hot standby. Therefore, when there is a failure in the active subsystem, the selector will switch to the other subsystem and the hot standby subsystem will become active subsystem. The failure in the standby subsystem will not affect the selector.

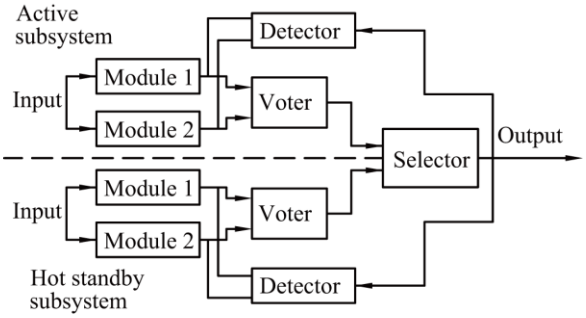

Fig.1 Architecture of the double 2-out-of-2 system

The Markov model of the double 2-out-of-2 system is presented based on the working schemes. Diagnosis and common cause failures are considered in the model. The states in the Markov model can be described as follows:

(1) State S0 denotes that the system is in normal operation. There is no failure in the two subsystems.

(2) State S1 denotes that only one module fails and the failure is detected. If the module in the hot standby subsystem fails, it will not affect the selector. The hot standby subsystem will become the active subsystem, when the failure happens in the active subsystem.

* This work is supported by the National High-Technology Research and Development Program of China (No. 2013AA09A220), Taishan Project of Shandong Province (TS20110823), the Fundamental Research Funds for the Central Universities (14CX06052A).

(3) State S2 denotes that both of the two modules in the hot standby subsystem fail and the failures are detected.

(4) State S3 denotes that both of the two modules in the hot standby subsystem fail, but only one failure is detected.

(5) State S4 denotes that only one module fails and the failure is undetected.

(6) State S5 denotes that system fails and is in fail-safe sate. When the system is in state S2, S3 or S4 and one module fails or both modules fail with their failures detected in the active subsystem, the system will enters the state FS.

(7) State S6 denotes that system fails and is in fail-unsafe sate. When the system is in state S2, S3 or S4 and both modules fail with their failures undetected in the active subsystem, the system will enters the state FS.

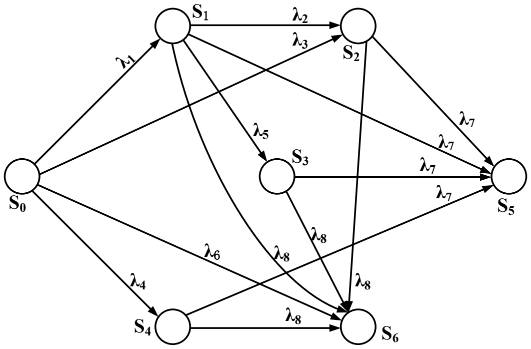

Fig.2 Markov model of the double 2-out-of-2 system

For redundant control system, the influences of diagnosis and common cause failures should not be ignorable. Although there is a detector in the subsystem, it can't be perfect for faults diagnosis. The diagnostic coverage c is used for the detector to describe the capability of faults diagnosis. In the model, the failure rate of the module λ is equal to 1e-5. For redundant components, it is possible that they fail simultaneously. Common cause failures are for this situation. β-factor is the most well known model for researching the common cause failures. For the double 2-out-of-2 system, common cause failures can only happen in the same subsystem.

In this paper, the diagnostic coverage c is equal to 90%. The factor to describe the common cause failures is $\beta = 0.05$. Repair rate is denoted by $\mu = 0.01$. According to the states transitions, the Markov matrix can be obtained as in

$$Q = \begin{bmatrix} q1 & \lambda_1 & \lambda_3 & 0 & \lambda_4 & 0 & \lambda_6 \\ 0 & q2 & \lambda_2 & \lambda_5 & 0 & \lambda_7 & \lambda_8 \\ 0 & 0 & q3 & 0 & 0 & \lambda_7 & \lambda_8 \\ 0 & 0 & 0 & q3 & 0 & \lambda_7 & \lambda_8 \\ 0 & 0 & 0 & 0 & q3 & \lambda_7 & \lambda_8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{1}$$

where, $q1 = -(\lambda_1 + \lambda_3 + \lambda_4 + \lambda_7)$, $q2 = -(\lambda_2 + \lambda_5 + \lambda_8 + \lambda_9)$, $q3 = -(\lambda_8 + \lambda_9)$, $\lambda_1 = 4c(1-\beta)\lambda$, $\lambda_2 = c(1-\beta)\lambda$, $\lambda_3 = 2c\beta\lambda$, $\lambda_4 = 4(1-c)(1-\beta)\lambda$, $\lambda_5 = (1-c)(1-\beta)\lambda$, $\lambda_6 = 2(1-c)\beta\lambda$, $\lambda_7 = c\beta\lambda + 2\lambda$, $\lambda_8 = (1-c)\beta\lambda$.

Here it is assumed that $p_i(t) = p(X(t) = i)$, which means the probability of the system in state *i at the time of t,* $i \in \{0,1,2,3,4,5,6\}$ .Then the system state probabilities expression is obtained as follows:

$$P(t)Q = dP(t)/dt \tag{2}$$

where, $P(t) = [p_0(t), p_1(t), \cdots, p_5(t)]$.

Solving (1) and (2) with $P(0) = [1,0,\cdots,0]$, the P(t) can be calculated. Reliability is the ability of a system to perform its functions during a specific time [7]. Therefore, reliability of the system at time t is:

$$R(t) = p_0(t) + p_1(t) + p_2(t) + p_3(t) + p_4(t) \tag{3}$$

Safety means freedom from unacceptable risk of harm. It is the probability of a system in a state where there is no dangerous failure. Safety of the system is:

$$S(t) = R(t) + p_5(t) \tag{4}$$

3. Performance Analysis

Based on (1)-(4), the transient reliability and safety of the system can be obtained as shown in Fig. (3) and Fig. (4). Fig. 3 shows that reliability of the system decreases quickly in the first 100000 hours and the downtrend becomes slow. Reliability will be zero in about 300000 hours. Fig. 4 illustrates that safety of the system decreases little as time goes by and reaches a stable value. The initial values of the reliability and safety are 1, but the stable value of reliability is 0 while the stable safety is about 0.995. According to the model, the system cannot stay in states S0-S4 forever, because these states will go into other states eventually. However, once the system enters into state S5 and S6, it will stay there forever. S5 and S6 are the absorbing states. Therefore, (3) and (4) illustrate that reliability and safety of the system have different stable values.

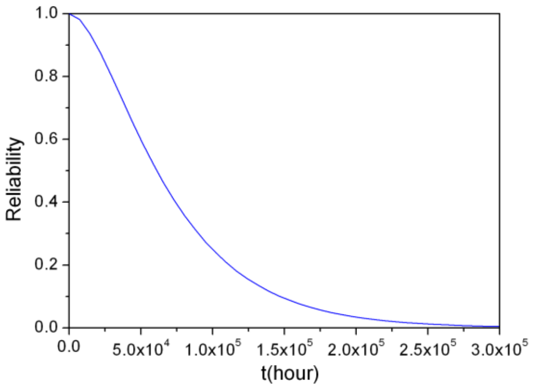

Fig.3 Reliability of the system

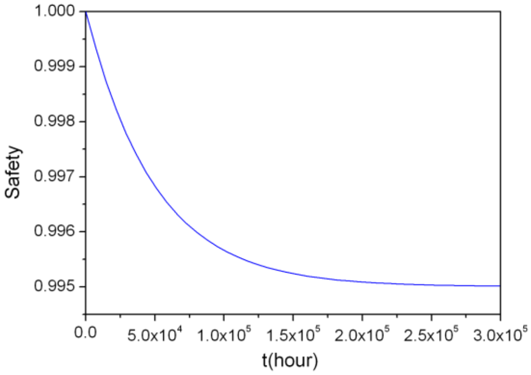

Fig.4 Safety of the system

The effects of β and c on reliability are shown in Fig.5 and Fig.6. Fig.5 shows that safety decreases as c increases and high diagnostic coverage can make the safety in high level. In Fig.6, safety increases as the factor of common cause failures decreases.

As the effects of β and c on reliability of the system are slight, the reliability at t=10000h is used. Therefore, the effects of reliability are shown in Fig.7 and Fig.8. Decreasing the value of β and increasing the value of c can improve the reliability of the system. In addition, c has greater effects on the safety of the double 2-out-of-2 system.

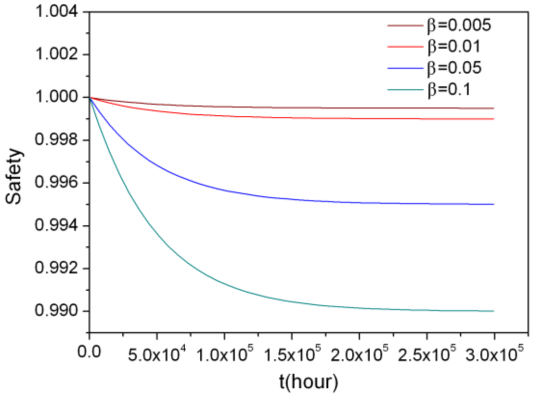

Fig.5 The effects of β on safety of the system

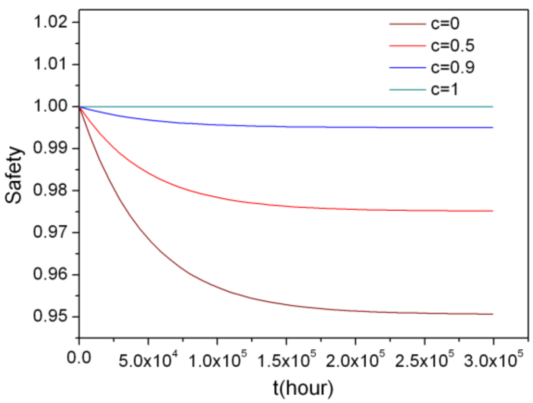

Fig.6 The effects of c on safety of the system

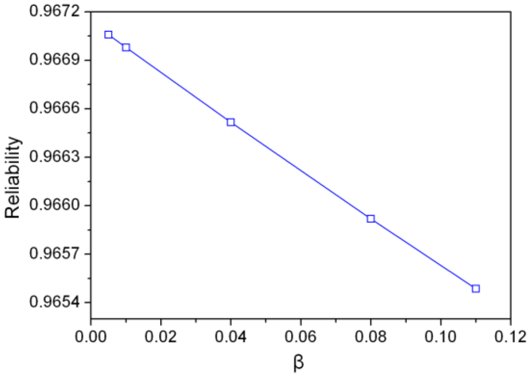

Fig.7 The effects of β on reliability of the system, t=10000h

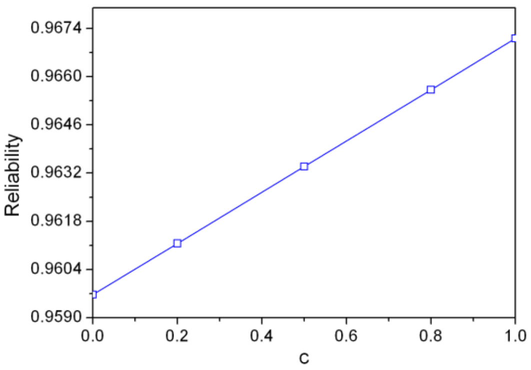

Fig.8 The effects of c on reliability of the system, t=10000h

4. Conclusions

In this paper, the structure and working scheme of the double 2-out-of-2 system is introduced. Based on the working states and failure states, the Markov model is presented with the imperfect diagnostic coverage and common cause failures taken into account. The performance analysis is conducted and the results show that diagnostic coverage and common cause failures have greater effects on safety than reliability. The reliability and safety of the system is more influenced by the imperfect diagnostic coverage than the factor of common cause failures. However, increasing the diagnostic coverage and decreasing the factor of common cause failures can improve the performance of the double 2-out-of-2 system.

5. Acknowledgment

The authors wish to acknowledge the financial support of the National High-Technology Research and Development Program of China (No. 2013AA09A220), National Natural Science Foundation of China (No.50874115), Taishan Scholar project of Shandong Province (TS20110823), Science and Technology Development Project of Shandong Province (2011GHY11520), the Fundamental Research Funds for the Central Universities (11CX04031A).

6. References

[1] X. Bao, L. Cui, “An Analysis of Availability for Series Markov Repairable System With Neglected or Delayed Failures”, IEEE Trans Reliab, vol. 59, no.4, pp. 734-743, December 2010.

[2] K. Jiang, C. Singh, “New Models and Concepts for Power System Reliability Evaluation Including Protection System Failures”, IEEE Trans Power Syst, vol. 26, no.4, November 2011.

[3] A. Ehsania, A.M. Ranjbara, A. Jafarib, M. Fotuhi-Firuzabada, “Reliability evaluation of deregulated electric power systems for planning applications”, Reliab Eng Syst Saf, vol. 93, pp.1473-1484, 2008.

[4] M. R. Haghifam, M. Manbachi, “Reliability and availability modelling of combined heat and power (CHP) systems”, Int J Electr Power Energy Syst, vol. 33, pp. 385-393, 2011.

[5] N. Ravishanker, Z. H. Liu, B. K. Ray, “NHPP models with Markov switching for software reliability”, Comput. Stat. Data Anal., vol. 52, pp. 3988-3999, 2008.

[6] H. Kim, H. Lee, K. Lee, “The design and analysis of AVTMR(all voting triple modular redundancy) and dual-duplex system”, Reliab Eng Syst Saf, vol. 88, pp.291-300, 2005.

[7] S. Wang, Y. Ji, W. Dong, S. Yang, “Design and RAMS Analysis of a Fault-Tolerant Computer Control System”, Tsinghua Sci. Tech., vol.12, no.S1, pp. 116-121, July 2007.

[8] Z. Chen, M. Ni, “Reliability and Security Analysis of 3-Module Redundancy System Based on Common Mode Fault”, Lect. Notes Electr. Eng., vol. 128 LNEE, pp.21-27, 2012.