Reliability analysis of partly repairable dual-mode redundant system

Hui Hongchao[a], Zhu Baoqiang[b] and Lin Zunqi[c]

Joint Laboratory for High Power Laser Physics, Shanghai Institute of Optics and Fine Mechanics, Chinese Academy of Sciences, No. 390, Qinghe Road, Jiading District, Shanghai, China

[a]13917856695@163.com,[b]baoqzhu@siom.ac.cn, [c]zqlin@fudan.sh.cn

Keywords: Reliability analysis, Markov model, maintenance, fault detection coverage rate.

Abstract. A reliability model of part repairable dual-mode redundant system is established and analyzed using Markov process to satisfy the reliability design requirements of multiple core parts of complex system redundant units. The model considers multi-factors, such as effects of maintenance, fault detection coverage rate, and common cause failure, all of which affect the reliability of redundant system. The model also analyzes two types of redundant system, namely, hot and warm-redundant systems. The relegation work and stop failure states are divided to ensure that the calculations conform to the actual situation. The reliability index of the two types of redundant system is calculated based on the state transition diagram and the equation of the model. As an example, a redundant server in a system is analyzed, results indicate that the redundant design can considerable improve the reliability of the systems. Moreover, fault detection coverage rate and common cause failure have a great influence on the reliability of redundant systems, whereas repair rate has an insignificant influence when the failure rate is low. In the end, this study provides suggestions for the design and improvement of redundant systems.

Introduction

Reliability is one of the most important attributes of components, products and complex systems and is closely associated with the performance and life span of related equipment, personal safety and economic benefits[1,2,3]. A complex system has high demands on life span and online maintenance, particularly safety, reliability, and accuracy, all of which are directly related to the success or failure of the entire system and its level of automation. Redundant design becomes an important method for improving the reliability of a system. In designing a redundant system, the factors of cost, online maintenance and reliability must be considered to analyze the reliability of the different modules of the redundant system and guide complete design.

This study analyzes two types of current techniques: hot and warm-redundant systems. A reliability model of most commonly used dual-mode redundant systems is established and analyzed using Markov process[4,5]. The model can analyze the reliability of two types of redundant system and consider multi-factors, such as fault detection coverage rate, common cause failure and maintenance rate. As an example, the redundant computer servers are used and analyzed, including their maintenance rate, fault detection coverage rate, and common cause failure that affects the reliability of the two types of redundant system. The model analysis and process presented in this paper are suitable for all dual-mode redundant systems in complex systems.

The Concept of Redundancy

Strictly speaking, redundancy is a method that constitutes a system by employing a specific or doubled number of components to achieve the required function. If one component fails, other backup components can still function through the hardware, software or some artificial procedure to ensure the normal operation of the system and reduce the downtime or fault loss.

(1) Hot-redundant: When the working component fails, the specific hardware units can compare the state of two or more components according to the comparison rules, and the system automatically switches to the backup components without clearance to ensure the normal operation of the system.

Hot-redundant is simple to implement and maintain and has a reliable performance, but has a high cost. It is suitable for systems and production processes that require a high reaction speed. The work component failure rate is unaffected by other components, so that the failure rate is equal.

(2) Warm-redundant: This type of system is implemented mainly by programming; special hardware devices and software are unnecessary. It has a low cost but its switching time is long; it is therefore suitable for slow-speed systems. The backup component failure rate is smaller than that of the work component, but the failure rate is greater than zero. If the failure rate of the work component is λ, then the hot-redundant failure rate is $\lambda_h=\lambda$, the warm-redundant failure rate is $\lambda_w<\lambda$.

Reliability Index of the Part Repairable Redundant System and Analysis Method

The Reliability Index. System reliability (R(t)) refers to the probability that a product will run normally during a set time and under specific conditions (i.e., temperature,voltage, etc.). It can be used to evaluate the ability of a system to fulfill the required functions over a specified lifetime. If T is expressed as the failure time of random variables, then the reliability at time t is $R(t)=P(T>t)$.

Unreliability (F(t)) refers to the probability of equipment failure in the time interval of 0 to t, $F(t)=1-R(t)=P(T\leq t)$.

Mean time to failure (MTTF) is defined as the failure time of expectations or the average. In a part repaired system, MTTF is the expected time at which system failure occurs and is calculated through the state transition probability matrix of mode[4].

Reliability Analysis Method. Two types of redundancy modes are inevitably present in large complex systems. A reliability analysis model should be established based on actual needs and must be capable of considering the effect of multi-factors. According to the theory of reliability, the Markov process is the most suitable method of analyzing systems that possess multiple failure modes. The Markov process can be used for any probability of a system state shifting from one to another. Such probability depends only on the current state and not the state of the history process.

The states of mutex and transitions between the states are first defined to establish the model. Based on the model, the Markov state equations can be obtained, the equations solved, and the reliability index and other important parameters of the system calculated. To ensure that the Markov model is authentic and capable of describing all the states and transition detailed, the failure modes are distinguished as follows:

(1) Component function of fault detection and diagnosis. Two kinds of failure may occur: measurable and unpredictable failure. The component failure rate is λ, and the fault detection coverage rate is c (0<c<1).Thus, measurable failure rate λ_d is $c\lambda$, unpredictable failure rate λ_u is $(1-c)\lambda$.

(2) Common cause failure. This type of failure is the same kind of stress caused by the failure of more than one component or system. The common cause failure model mainly includes the β model, which is relatively simple, and the multi-fault impact model (MESH). The fault rate can be divided into common cause and general failures through the use of the β factor. Experts define the β factor as the range of hardware failure from 0.005 to 0.11 and that of software failure from 0.05 to 0.6. The β factor can be estimated quantitatively in view of the specific redundant components[4,6]. According to the β model, the component failure rate can be divided into four types, measurable general failure rate λ_{dn} is $c(1-\beta)\lambda$, measurable common cause failure rate λ_{dc} is $c\beta\lambda$, unpredictable general failure rate λ_{un} is $(1-c)(1-\beta)\lambda$, unpredictable common cause failure rate λ_{uc} is $(1-c)\beta\lambda$.

Reliability Analysis Model of the Part Repairable Dual-Mode Redundant System

The following are assumed to simplify the model for analytical convenience.

(1) The work and redundant components are the same products; thus, their repair rates are equal and constant. The work component repair rate is λ, and the redundant component repair rate is λ_r. In a very short time interval, the system cannot rise to two and above the state transition. After the success

of the fault component maintenance, the time taken in configuring the work or redundant state can be ignored.

(2) When the component or system fails, only one group of staff is deployed for repair. The individual components can be found in any the following four states: working, backup, measurable failure and maintenance, and unpredictable failure states. If unpredictable failure occurs, the component cannot be repaired and is scrapped.

(3) The component fault detection coverage is c, and the common cause failure factor is β. They can be estimated quantitatively according to the actual situation.

The two components M and N are defined based on the two types of redundant system. The dual-mode redundant system that they form can be found in any of the following ten states. Table 1 shows the ten states in detail (a and b stand for the relegation work state).

Table 1 States of the part repairable dual-mode redundant system

State	Backup state	Working state	Measurable failure	Unpredictable failure
1	M	N		
2	N	M		
3(a)		N	M	
4(a)		M	N	
5(b)		M		N
6(b)		N		M
7			M,N	
8			M	N
9			N	M
10				M,N

State 1: N is in the working state; M is in the redundant state; neither fails. State 2: M is in the working state; N is in the redundancy state; neither fails. State 3: A measurable failure occurs in M when it is in working state, and the system deteriorates.N continues working instead of M, while M is being repaired. State 4: A measurable failure occurs in N when it is in working state, and the system deteriorates. M continues working instead of N, while N is being repaired. State 5: An unpredictable failure occurs in the redundant component N, and the system deteriorates. The working component M continues working, but the redundant components N cannot be repaired and is scrapped. State 6: An unpredictable failure occurs in the redundant component M, and the system deteriorates. The working component N continues working, but the redundant components M cannot be repaired and is scrapped. State 7: A measurable failure occurs in both M and N, and the system shuts down. M and N are repaired, but only one component can be repaired at a time. State 8: A measurable failure occurs in M, which is consequently switched into the repairing state. An unpredictable failure occurs in N, and N cannot be repaired and is scrapped. State 9: A measurable failure occurs in N, which is switched into the repairing state. An unpredictable failure occurs in M, and M cannot be repaired and is scrapped. State 10: An unpredictable failure occurs in both M and N. Both cannot be repaired and are scrapped. The entire system fails.

Figure.1 shows the state transition diagram of the redundant system based on the model and the ten states. These states may be described as follows:

States 1 to 3: After a measurable general failure occurs in the redundant component, the staff repairs the component, while the working component continues working. The system is deteriorating. States 2 to 4 are in the same way.

States 1 to 4: After a measurable general failure occurs in the working component, the staff repairs the component, and the redundant component continues working instead of the working component. The system is in deteriorating. States 2 to 3 are in the same way.

States 1 to 6: An unpredictable general failure occurs in the redundant component. The working component continues working, and the system is deteriorating. States 2 to 5 are in the same way.

States 1 to 7: A measurable common cause failure occurs in the system. The staff repairs one of the components, and the system temporarily stops. States 2 to 7 are in the same way.

State 1 to State 8: When an unpredictable general failure occurs in the working component, the redundant component fails to switch. The staff repairs the redundant component, and the system temporarily stops. States 2 to 9 are in the same way.

States 1 to State 10: An unpredictable common cause failure occurs in both the working and redundant components. The entire system immediately shuts down. The two components cannot be repaired and are scrapped. States 2 to 10 are in the same way.

States 3 to 1: In state 3, the staff repairs the unit that failed and configures it into the redundant state after the repair. States 4 to 2 are in the same way.

States 3 to 7: The system is at degradation state a. When a measurable failure occurs in the working component, the system is shuts down and remains at state 7, while the repair completed. States 4 to 7 are in the same way.

States 3 to 8: The system is at degradation state a. An unpredictable failure occurs in the working component, which is scrapped. The system shuts down and remains at state 8, while the repair of the other component completed. States 4 to 9 are in the same way.

States 5 to 8: The system is at degradation state b. A measurable failure occurs in the working component. The system shuts down and remains at state of 8, while the repair is completed. States 6 to 9 are in the same way.

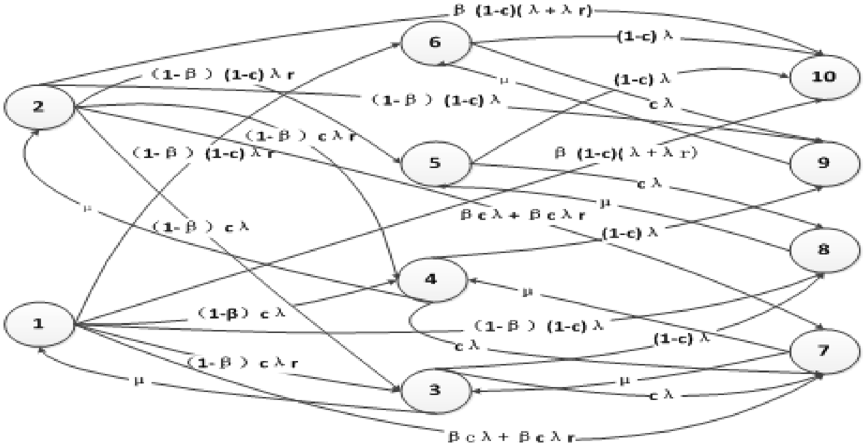


Fig.1 State transition diagram of the part repairable dual-mode redundant system

States 5 to 10: The system is at degradation state b. An unpredictable failure occurs in the working component. The system shuts down and fails. The components cannot be repaired and are scrapped. States 6 to 10 are in the same way.

States 7 to 3: The system can continue working if any maintenance component is repaired. However, if the other component is not successfully maintained, the system reverts to degradation state a. States 7 to 4 are in the same way.

States 8 to 5: Only one component can be repaired; the other is scrapped. The repairable component can continue working if it is successfully repaired. At this time, the system at degradation state b. States 9 to 6 are in the same way.

Reliability Analysis of The Model

Assuming that Pi(t) is the probability of state i (i=1,2,…,10), λ is the working component failure rate, and λ_r is the redundant component failure rate. The hot-redundant component failure rate is λ_r=λ_h=λ, the warm-redundant component failure rate is λ_r =λ_w <λ, (0<λ_w<λ).Based on the state transition diagram, the state transition differential equations (Eq.1) are obtained.

The following states are similar: States 1 and 2, States 3 and 4, States 5 and 6, States 8 and 9. Components M and N are interchangeable. Thus, defining the six new states a,b,c,d,e,f. Based on the Eq.1, the Eq.2 are obtained. Applying the Laplace transform to Eq.2 yields the Eq.3.

$$\begin{cases} \dot{P}_1(t)=-(\lambda+\lambda_r)P_1(t)+\mu P_3(t) \\ \dot{P}_2(t)=-(\lambda+\lambda_r)P_2(t)+\mu P_4(t) \\ \dot{P}_3(t)=(1-\beta)c\lambda_r P_1(t)+(1-\beta)c\lambda P_2(t)-(\lambda+\mu)P_3(t)+\mu P_7(t) \\ \dot{P}_4(t)=(1-\beta)c\lambda P_1(t)+(1-\beta)c\lambda_r P_2(t)-(\lambda+\mu)P_4(t)+\mu P_7(t) \\ \dot{P}_5(t)=(1-\beta)(1-c)\lambda_r P_2(t)-\lambda P_5(t)+\mu P_8(t) \\ \dot{P}_6(t)=(1-\beta)(1-c)\lambda_r P_1(t)-\lambda P_6(t)+\mu P_9(t) \\ \dot{P}_7(t)=(\beta c\lambda+\beta c\lambda_r)[P_1(t)+P_2(t)]+c\lambda[P_3(t)+P_4(t)]-2\mu P_7(t) \\ \dot{P}_8(t)=(1-\beta)(1-c)\lambda P_1(t)+(1-c)\lambda P_3(t)+c\lambda P_5(t)-\mu P_8(t) \\ \dot{P}_9(t)=(1-\beta)(1-c)\lambda P_2(t)+(1-c)\lambda P_4(t)+c\lambda P_6(t)-\mu P_9(t) \\ \dot{P}_{10}(t)=\beta(1-c)(\lambda+\lambda_r)[P_1(t)+P_2(t)]+(1-c)\lambda[P_5(t)+P_6(t)] \end{cases} \tag{1}$$

$$\begin{cases} \dot{P}_a(t)=-(\lambda+\lambda_r)P_a(t)+\mu P_b(t) \\ \dot{P}_b(t)=(1-\beta)c(\lambda+\lambda_r)P_a(t)-(\lambda+\mu)P_b(t)+\mu P_d(t) \\ \dot{P}_c(t)=(1-\beta)(1-c)\lambda_r P_a(t)-\lambda P_c(t)+\mu P_e(t) \\ \dot{P}_d(t)=P_7(t)=(\beta c\lambda+\beta c\lambda_r)P_a(t)+c\lambda P_b(t)-2\mu P_d(t) \\ \dot{P}_e(t)=(1-\beta)(1-c)\lambda P_a(t)+(1-c)\lambda P_b(t)+c\lambda P_c(t)-\mu P_e(t) \\ \dot{P}_f(t)=\beta(1-c)(\lambda+\lambda_r)P_a(t)+(1-c)\lambda P_c(t) \end{cases} \tag{2}$$

$$\begin{cases} sP_a(s)-P_a(0)=-(\lambda+\lambda_r)P_a(s)+\mu P_b(s) \\ sP_b(s)-P_b(0)=(1-\beta)c(\lambda+\lambda_r)P_a(s)-(\lambda+\mu)P_b(s)+\mu P_d(s) \\ sP_c(s)-P_c(0)=(1-\beta)(1-c)\lambda_r P_a(s)-\lambda P_c(s)+\mu P_e(s) \\ sP_d(s)-P_d(0)=(\beta c\lambda+\beta c\lambda_r)P_a(s)+c\lambda P_b(s)-2\mu P_d(s) \\ sP_e(s)-P_e(0)=(1-\beta)(1-c)\lambda P_a(s)+(1-c)\lambda P_b(s)+c\lambda P_c(s)-\mu P_e(s) \\ sP_f(s)-P_f(0)=\beta(1-c)(\lambda+\lambda_r)P_a(s)+(1-c)\lambda P_c(s) \end{cases} \tag{3}$$

At the initial time, no failure occurs, so that the system is at States 1 and 2, namely, State a. The initial state of the system is

$$[P_a(0),P_b(0),P_c(0),P_d(0),P_e(0),P_f(0)]=[1,0,0,0,0,0] \tag{4}$$

Eq. 4 is substituted into Eq. 3, and the Laplace transform expression of the probability of the six states can be obtained using the Matlab software. After calculating the inverse transformation of these six expressions and substituting the redundant system parameters into them, the probability $P_j(t)$ (j=a,b,…,f) that the system is in any state at any time t can be obtained.

State a, b and c are the normal operation states, and State d and e are the downtime states, although they can still be turned into the normal operation state through repair. State f is the state at which whole system fails and is scrapped. Thus, at any time t, the system reliability R(t) and unreliability F(t) are written as follows:

$$\begin{cases} R(t)=P_a(t)+P_b(t)+P_c(t) \\ F(t)=P_d(t)+P_e(t)+P_f(t) \end{cases} \tag{5}$$

The expression of the state probability $P_j(t)$ (j=a,b,…,f) is very complex when the condition of the parameters is unknown. Without loss of generality, the computer central server is selected as an example for the purpose of analysis and comparison. First, the system reliability index was calculated and analyzed. Second, the reliability of the two types of redundant systems was analyzed under various conditions of repair rate μ, fault detection coverage rate c, and common cause failure factor β. The parameters of the server are as follows: failure rate $\lambda=1.14\times10^{-5}$ /h, c=0.9, and β=0.1. In the hot-redundant mode, the parameters are $\lambda_r=\lambda_h=\lambda=1.14*10^{-5}$/h. In the warm-redundant mode, the parameters are $\lambda_r=\lambda_w=1.14*10^{-6}$/h<λ. Given that the repair rate is μ=1/24 /h.

Figure.2 shows the reliability and unreliability curves of the two redundant modes at different time t during a year (8760 hours) of continuous running. The time increment Δt is 1 hour. Among the two modes, the hot-redundant mode has the lower reliability (i.e., higher unreliability), whereas, the warm-redundant mode has the higher reliability (i.e., lower unreliability). Based on Eq.8, the reliability of the two modes after a year of continuous running are as follows: $R_h(8760)=0.9979$, and $R_w(8760)=0.9982$. The unreliability of the two modes are as follows: $F_h(8760)=0.0021$, and $F_w(8760)$）=0.0018. The stop time of the two modes are as follows: $T_h=18.4$ h, and $T_w=15.8$ h, based on document[4]. The mean time to failure (MTTF) of the two modes are as follows: $MTTF_h=2.5142\times10^5$ h, and $MTTF_w=2.8819\times10^5$ h. However, the same failure rate and running time of a single system are Rs=exp(-0.0000114×t)≈0.905, and Fs =0.095.

Figure.3 shows the reliability curves of the two types under various repair rate μ, fault detection coverage rate c, and common cause failure factor β. The reliability of the redundant systems can be improved and the system failure time reduced by increasing the repair and fault detection coverage rates and reducing the common cause failure.

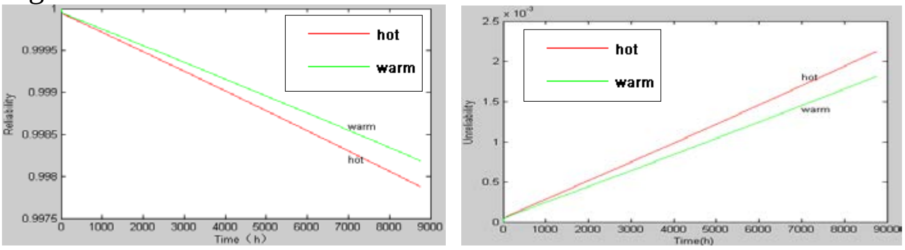
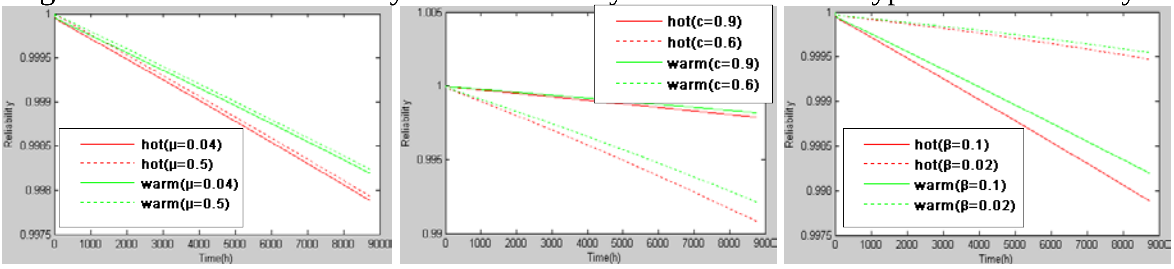


Fig.2: Instantaneous reliability and unreliability curves of the two types of redundant system



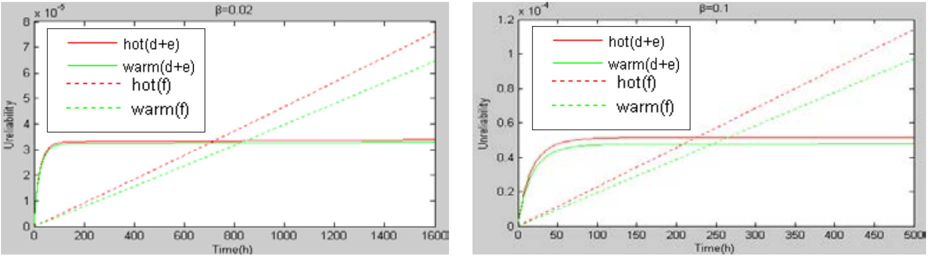
(a) (b) (c)

Fig.3: Reliability curves of the two types of redundant system
(a) different μ, (b) different c, (c) different β

Figure.3(a) shows that although the repair time is increased from 24h to 2h, the improvement in the reliability is not very obvious, mainly because the selected server failure rate is very low and the MTTF is very long. If the component failure rate is high, then improving the maintenance rate significantly improves the system reliability.

Figure.3(b) shows that the reliability of the system is obviously enhanced when the system has a high fault detection rate c. A high fault detection rate can reduce the system working time under the risk model and degraded mode. If the automatic diagnostic system can detect one fault accurately without delay, the fault can be immediately repaired and maintenance time saved. Otherwise, the fault may always be unknown, and potential danger may occur. Improving the fault detection rate requires one qualified technical personnel to frequently check the equipment. Moreover the self-inspection ability of a system can be improved through embedded software or hardware design, such as that using PLC. Such hardware design accomplishes reference diagnosis, and the fault detection coverage rate can reach more than 0.9.

Figure.3(c) shows the reliability curves when β=0.1 and β=0.02. The figure shows that a common cause failure exerts an obvious influence on the system reliability. Figure.4 shows the unreliability curves when β=0.1 and β=0.02; the difference in the figure is the probability in the downtime scrapped state f (dotted line) and the probability in the downtime for repair d+e (solid line), which are shown separately. When β is larger enough, the state f exceeds states d+e early on. In other words, the system enters state f early on. As a result, the MTTF is reduced, and very serious design faults may occur if the common cause failure is ignored in designing the redundant system. Specific methods should therefore be adopted to avoid mistakes, such as isolating the redundant units on a physical and electrical basis. Moreover, using asynchronous operations or different operating modes in the software can reduce the occurrence of common cause stress. The strengthen design, "diversity” technology[4,7], and others can also be used.



(a) (b)

Fig.4: Unreliability curves of the two types of redundant systems (a) β=0.02; (b) β=0.1

Conclusion

The development of complex systems increases the requirement for system reliability. The key components of a redundant system design have become an effective method of further improving system reliability, and the Markov process is very suitable in analyzing the reliability of redundant systems. This study established and analyzed a reliability model of part repairable dual-mode redundant system, based on the two kinds of redundancy. The reliability index of a redundancy system can easily be obtained from the state equation. The results of the analysis show that increasing the maintenance and fault detection coverage rates and reducing the common cause failure can improve the reliability of redundant systems. A suitable kind of redundancy and the characteristics specific applications, reliability requirements, cost, and other factors of the system itself are very important and must be considered in designing redundant system.

References

[1] Shen K, On the increase of system reliability by parallel redundancy, IEEE Transactions on Reliability, 39(5):607-611,(1990).

[2] Jonhston W, Increasing system reliability-a survey of redundant control methods, Programmable Control and Automation Technology Conference and Exhibition, Canadian (1988)

[3] YU Min, HE Zheng-you, QIAN Qing-quan, Reliability analysis of repairable hot stand-by redundant system based on Markov model, Computer Engineering and Design, 30(8):2040-2046 (2009).

[4] Goble. W. M. Goble, Control system safety evaluation and reliability (Second Edition) , Instrument Society of America, 138-260 (1998).

[5] Zhou Ji-chao; He Chen, An adaptive modulation method in MIMO-MRC system based on Markov model, Journal of Shanghai Jiaotong University,43(7):1095-9 (2009).

[6] Sun Xiao-zhe; Li Wei-qi; Chen Zong-ji, Hierarchical hybrid reliability modeling method for flight control computer system, Journal of Shanghai Jiaotong University, 45(2):277-83 (2011)

[7] Elsayed. A. E, Reliability engineering, Second Edition, Wiley Series in Systems Engineering and Management, 110-230 (2012).