TELKOMNIKA, Vol. 11, No. 5, May 2013, pp. 2594 ~ 2604
ISSN: 2302-4046

Reliability and Security Analysis on Two-Cell Dynamic Redundant System

Hongsheng Su
Dept. of Electrical Engineering, Lanzhou Jiaotong University, Lanzhou, China
88 West Anning Road, Lanzhou 730070, China
e-mail: shsen@163.com

Abstract

Based on analysis on reliability and security on three types of two-cell dynamic redundant systems which has been widely applied in modern railway signal system, whose isomorphic Markov model was established in this paper. During modeling several important factors, including common-cause failure, coverage of diagnostic systems, online maintainability, and periodic inspection maintenance, and as well as many failure modes, were considered, which made the established model more credible. Through analysis and calculation on reliability and security indexes of the three types of two-module dynamic redundant structures, the paper acquires a significant conclusion, i.e., the safety and reliability of the kind of structure possesses an upper limit, and cannot be inordinately improved through the hardware and software comparison methods under the failure and repairing rate fixed. Finally, the paper performs the simulation investigations, and compares the calculation results of the three redundant systems, and analysis each advantages and disadvantages, and gives out each application scope, which provides a theoretical technical support for the railway signal equipments selection.

Keywords: *two-cell dynamic redundant system, reliability, security, Markov, isomorphism*

1. Introduction

As large-scale applications of computers and programmable electronic products in the modern railway signal systems, many railway signal safety criticism systems with the purpose of safety make use of microprocessor, electronic chip and other programmable electronic products, such as station interlocking, interval block, automation train driving, train over-speed protection, and crossing protection, and etc [1]. To meet the requirements of the systems for high safety and high reliability, various redundancy and restructuring cells are widely applied in electronic product design to improve the reliability and safety of the systems, as well as online fault diagnosis technology. In terms of safety, reliability and cost, dual hot spare dynamic redundancy structure is a kind of ideal design scheme, and has already been widely applied in modern railway signal systems [2].

With the large-scale applications of two-cell dynamic redundancy structure in modern railway signal systems, the scholars at home and aboard have made extensive and in-depth investigations on its security and reliability. As in [3], the dynamic fault tree method is adopted to analyze the security and reliability of railway computer-based interlocking systems, and resolves some problems such as larger state space scale and tedious solving process while applying Markov process to model. But during modeling the influence of maintenance on system safety performance is not considered, and as well as common cause. Clearly, it is difficult for it to fit into the practice. In [4], the failure usability coefficient is proposed and introduced into the security and reliability analysis on two-cell dynamic redundancy systems with computer-based in modern railway signal systems according to the practical application cases, and thus a conclusion is acquired to improve the reliability under the premise that the security is invariant. In practice, this is impossible. Though system with local failure can continue working a period of time, from safety consideration, at the moment the system has already become unsafe. Likely, during analysis maintenance and common cause are not considered. In [5], two diverse dual hot spare redundancy structures are investigated, the acquired conclusion is that the one comparing their results each other in process of operation has higher safety than the other without comparing their results, and the latter possesses better availability. This conclusion is

Received January 6, 2013; Revised March 13, 2013; Accepted March 23, 2013

correct, but maintenance and common cause are still not considered. Liu [6] performs the comparison between dual hot spare redundancy system and double 2-vote-2 redundancy system, as a result, the former has higher reliability, and the latter possesses better safety. During analysis common cause is considered, but maintenance is not done. Simultaneously, a hypothesis is enforced that as long as one failure is detected the fault then guides safety. However, it is a pity that further measure is not considered after the fault guides safety what we then do. In fact, it only considers the situation where maintenance is nonexistent. Clearly, its role is limited. He [7] applies the fault tree to investigate the security of the switch control unit of all-electronic computer interlocking systems, but common cause failure and some other influence factors are not considered. Zhang [8] analyzes several common-used two-cell redundant structures, and compares their reliability and safety. But the established models are quite simple, and it is difficult to apply, practically. In [9], a reliability optimum design scheme is proposed, which better solves the contradiction among quality, cost, and reliability. But it is not adequate for reliability improvement. Seen from the above analysis, too much hypothesis in the existed modeling methods make the model simple so that it is difficult to make it accord with the practice in one hand. On the other hand, the models are also made complicated though state numbers increasing or usability coefficient introduced. Thus the system availability is calculated higher, but the safety decreases. Hence, the paper aims at three types of two-cell dynamic redundant systems which has already been widely applied in China high-speed railway, and synthetically considers the influence of many factors such as common-cause failure, coverage of diagnostic systems, online maintainability, and periodic inspection maintenance, and well as many failure modes, and finally establishes the united Markov model, and implements analysis and computation on reliability and security indexes. The work described in the paper will provides the new approaches on reliability and security calculation for railway signal safety criticism systems.

2. Related Concepts

2.1. Reliability, Availability and MTTF

Reliability is an index that the system can normally work, whose definition is that the product can complete the regulated function under specified conditions and in range of the prescribed time. Let T be a stochastic variable, and reliability can be defined as

$$R(t)=P(T>t) \tag{1}$$

Reliability requires system can continuously work without failure in the whole time interval, and does not allow repairing. For railway signal system to require maintenance, the index is still far from enough. People care for its availability more, which is defined as the probability that the product can normally work in t moment, and expressed using $A(t)$. Availability is different with reliability, the former is a function of failure rate, and repairing rate, and as well as running time, and could reach a steady value with time-increasing, finally. For the latter, as a function of failure rate and running time, it will change from one to zero.

Corresponding to the reliability, the unreliability can be defined as

$$F(t)=P(T\leq t)=1-R(t) \tag{2}$$

And then, the probability density function may be denoted as

$$f(t)=\mathrm{d}F(t)/\mathrm{d}t \tag{3}$$

Therefore, the failure rate function can be expressed by

$$\lambda(t)=f(t)/R(t) \tag{4}$$

Thus, mean time to failure (*MTTF*) can be presented by

$$MTTF=E(T)=\int_0^{+\infty} tf(t)\mathrm{d}t=-\int_0^{+\infty} t\mathrm{d}[R(t)]=\int_0^{+\infty} R(t)\mathrm{d}t \tag{5}$$

2.2. Security, Safety Failure Probability and Dangerous Failure Probability

Security refers to the ability that the system could not generate the dangerous side outputs when the fault occurs. When evaluating the security of one system, it is necessary to know its failure modes. Reliability, availability, and *MTTF* are only for the normal work of the system concerned. As the system enters into the failure state from the normal one, we can say that it breaks down and terminates the job, and cannot continue to perform the regulated function. At the moment, there are two significant states to need to be considered, that is, the security failure state and the dangerous failure state. The former is corresponding to a safe failure probability (*PFS*), and the latter is corresponding to a dangerous failure probability(*PFD*). Thus, the unreliability may be written as

$$F(t) = PFS(t) + PFD(t) \tag{6}$$

In terms of the repairable systems, the unavailability is

$$\bar{A}(t) = PFS(t) + PFD(t) \tag{7}$$

And so, the availability is

$$A(t) = 1 - [PFS(t) + PFD(t)] \tag{8}$$

The safety availability is different with the availability, and defined as

$$S(t) = 1 - PFD(t) \tag{9}$$

Another important index is safety risk reducing factor (*RRF*), and defined as

$$RRF = 1/PFD \tag{10}$$

The formula (10) may be understood as that if a system does not adopt any safety protection measures, and its inherent risk is one. When adopts the safety protection measures, its risk becomes *PFD*. Thus, its risk reducing level may naturally use the rate as in (10) to express.

2.3. Diagnosis Coverage, Repairing Rate, and Common Cause Failure

It goes without saying that it is an important characteristic for any control systems or security systems to possess the failure detection ability. Through online condition monitoring and fault diagnosis, we can reduce maintenance time and control the implementation of some tolerant structure. The diagnostic coverage rate can be applied to express the power of the diagnostic system, which reflects the probability that if a failure occurs it can be detected. In the numerical value, it equals the sum of the detected failure rates is divided by total failure rate. Hence, it is necessary to consider the influence of failure detection system when analyzing a system security.

As stated above, modern railway signal makes use of a lot of redundant fault-tolerant cells, and supplemented by online continuous diagnosis technology, so as to be able to achieve high reliability and high safety level. But anyway, the diagnosis detection technology can not find all the failures. Some failures will remain down all along, and develop as dangerous sources, finally. For this reason, railway signal department formulates strict maintenance regulations, which requires the relevant departments to perform a plan of half a year or a year of periodic maintenance. Assuming that periodic maintenance can do a thorough detection on equipments, and find all the questions, and implement the rapid and effective maintenance, i.e., periodic maintenance is perfect, thus, after regular maintenance the system can restore to its original state, and the probability of the system at risk side is zero. If periodic maintenance is not perfect, after regular maintenance the probability of the system at risk side will be reduced to a value greater than zero.

If the maintenance staff can implement quick repairing as system cell emerges a detected dangerous failure, the system can then remove the danger and restore to safety state. The shorter repair time is, the lower system failure risk is. Hence, the repairing rate has an important influence on system security and usability. Only as the dangerous failure occurs but can be undetected, the system will become unsafe. So until a next periodic maintenance arrival this risk can be removed.

Common cause failure is a kind of multiple-failure resulted in the same kind of stress, and widely existed in the engineering system. It increases the joint probability of each failure mode, and counteracts the advantages of the redundant system. If there is no proper consideration on the influence of common cause failure, the analysis results on security and reliability will become too optimistic. The modern railway signal system is a high safety and integrity system, so the established model must take into account the influence of common cause failure. The β model is commonly applied to tell the common cause failure from the normal failure.

2.4. Failure Rates Analysis

Firstly, without consideration common cause, the failure rate of the cell is partitioned as the two parts, that is, the safety failure rate λ^S and the failure rate λ^D, and then

$$\lambda=\lambda^S+\lambda^D \tag{11}$$

Consider the role of online diagnostic systems, the failure rateλ^S is divided as the two parts, that is to say, the detected safety failure rateλ^{SD} and the undetected safety failure rateλ^{SU}, and then

$$\lambda^S=\lambda^{SD}+\lambda^{SU} \tag{12}$$

For λ^D, likewise, we have

$$\lambda^D=\lambda^{DD}+\lambda^{DU} \tag{13}$$

where λ^{DD} expresses the detected dangerous failure rate, and λ^{DU} is the undetected dangerous failure rate.

Consider the common-cause influence, then, we have

$$\lambda^{SD}=\lambda^{SDN}+\lambda^{SDC} \tag{14}$$

$$\lambda^{SU}=\lambda^{SUN}+\lambda^{SUC} \tag{15}$$

$$\lambda^{DD}=\lambda^{DDN}+\lambda^{DDC} \tag{16}$$

$$\lambda^{DU}=\lambda^{DUN}+\lambda^{DUC} \tag{17}$$

where the superscript *N* shows a normal failure, and *C* means common-cause failure.

Let the diagnosis coverage rate be *c*, for λ^{SD}, we have

$$\lambda^{SDC}=c\,\lambda^{SD}=c\beta\,\lambda^S$$

$$\lambda^{SDN}=c\,\lambda^{SD}=c(1-\beta)\,\lambda^S$$

Simlarly, we may get other the failure rates.

3. Reliability and Security Analysis

3.1. System Structure

There are three types of two-module dynamic redundant structures applied in modern railway signal systems, which are here respectively defined as the fundamental mode, and the enhanced mode, and as well as the upgraded mode. For the fundamental mode, the two cells add electricity to work under normal state, and each cell performs single version program. Only the host cell controls the controlled objects, and the spare cell is in hot backup state. In process of operation there are no any comparisons between two cells. Every cell possesses strong fault detection and diagnosis function, and can automatically switch to standby cell after detecting the fault, and may realize online repairing. This kind of structure is aimed at those systems that the requirements for the security are not high, or when the faults occur the system safety could not be influenced. For example, some information systems in traffic command, and monitoring control machines in station interlocking systems, and as well as route walkthrough tache, and etc. The system structure is shown in Figure 1.

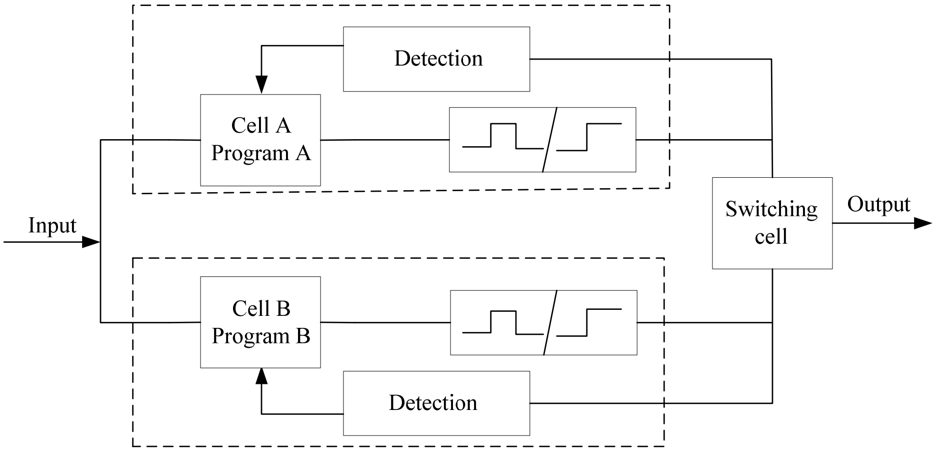

Figure 1. System structure of the fundamental mode

The working principle of the enhanced mode is basically consistent with the fundamental mode, but it adopts single cell to perform two-version software to ensure the system safety. This kind of structure realizes 2-vote-2 in software essentially, but the hardware security is guaranteed by hardware itself alone. This kind of structure is designed for those systems with higher requirements for the security such as TYJL—II, DS6-11, and EBILOCK850, and as well as computer-based interlocking systems. The system structure is shown in Figure 2.

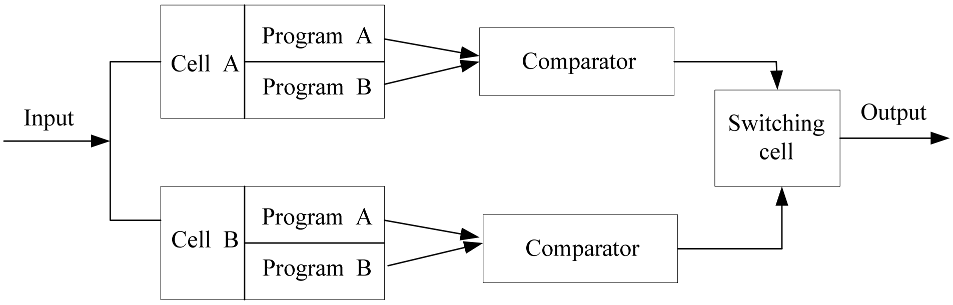

Figure 2. System structure of the enhanced mode

Single cell performing two-version program may find a large proportion of the risk during operation, but is difficult to detect the hardware faults. To change the situation, people develop the third kind of dynamic redundant structure again, and called as the upgraded mode. The kind of structure adopts single machine performing double- channel software, and each channel possesses the diverse software, which makes the system realize 2-vote-2 from the hardware to the software. This ensures the system safety, further. This kind of the structure can not only find most of the software errors in the process of operation, but also can detect the hardware failures. Therefore, its security is very high. This typical structure includes VPI computer-based interlocking systems, and JTI-CZ2000 locomotive signal onboard system. The system structure is shown in Figure 3. In addition, the special safety design and fault-tolerant technology make the system reliability and security quite high, and is very suitable to the safety criticism system with the high security and high reliability.

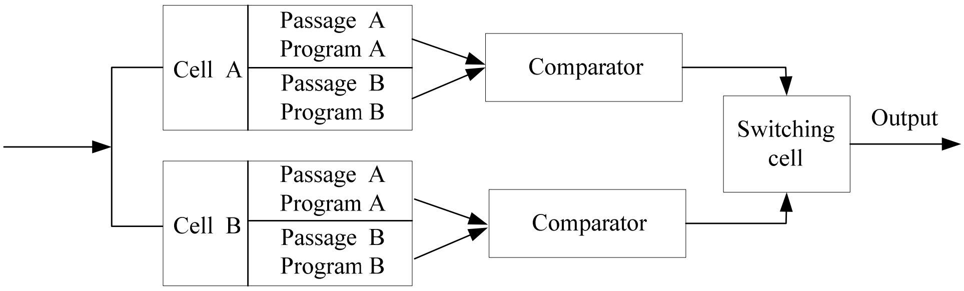

Figure 3. System structure of the upgraded mode

The main discrimination among the three kinds of structures as above lies in the realization of interlocking cell. In the fundamental two-cell hot spare system, the interlocking cell is composed of single channel hardware with single version software. In the enhanced mode, it is converted into single channel hardware with double-version software. In the upgraded mode, the interlocking cell is converted into double-channel hardware with double-version software. Generally speaking, each channel is equipped with self diagnosis program with continuous on-line detection and fault diagnosis function. The security of single channel with single version software only relies on channel own security, which is difficult to meet the safety requirements. Single channel with double-version software means that single cell implements two sets of software in turn, and compares the implementation results. As the comparing programs detect the inconsistency, it means that system fault occurs. The comparison programs offer another level of security protection function, namely, the comparison program can find one failure that the self-diagnostic program cannot detect. As stated above, the structure can find most of the software fault, but it is difficult to detect the hardware failure. And so it possesses very high requirements on hardware. Dual channel with double version software can not only detect the most software faults, but also can find the hardware faults, and the requirements on the hardware are not so high. Hence it has been widely applied in railway signal interlocking system in recent years. It is not hard to see that the main difference among three kinds of structures lies in countermeasures to improve the security, that is, the channel self-diagnostic program can not detect one failure that is found through the comparison program or hardware comparison, and converted to the safety side output, and the dangerous side outputs are therefore reduced. Let the parameter C_1 express the diagnosis coverage rate, and then C_1=0 means there are no any comparisons occur, at the moment, the system structure is the fundamental mode dual hot spare structure, and $0<C_1<1$ means the diagnosis is imperfect, there are some failures existing but cannot be detected, and C_1=1 is an ideal situation, which means the system possesses the perfect detection ability, and can find any faults. Clearly, C_1=1 represents the highest ability of the structures as such under the condition that the failure rate and repairing rate are given. In this case, If the system security still can not be ensured, and then we search other ways to satisfy the demands alone. Thus, through the definition on C_1, we may establish a united model for three kinds of structures. In fact, the models of three kinds of the structures are eaaentially isomorphic.

3.2. Analysis on Reliability and Security

The hardware redundancy exists in the structures from Fig.1 to Fig.3, and so common-cause failure should be considered. Simultaneously, combining with channel self-diagnostic ability and two sorts of the failure modes, there are eight kinds of the failures to need to be considered in all. Given that the failure rate at safety side and the one at dangerous side, and β factors, and as well as the diagnostic coverage rate *c* of self-diagnostic program, according to the former descriptions, it is not hard to solve the eight types of the failure rates.

If the self diagnosis program detects and prompts the emergence of a failure, then the failure can be immediately repaired, and otherwise it may not still known. To be able to find the failures early, the regular repairing and detecting on the equipments is necessary. Regular maintenance is implemented by the professional and technical personnel, who manually examine each part of the equipment to see whether they operate normally. Assume that the manual inspection can find all the problems, then two specific maintenance rates occur. One is on-line maintenance rate which occurs as the diagnosis programs detect and prompt the emergence of a failure, and the other is regular maintenance rate which occurs during periodic detection and maintenance, and includes the testing time and repairing time. Compared with on-line maintenance rate, the regular maintenance rate is lower.

Definition 1. Let online maintenance rate be μ_0, then

$$\mu_0=1/T_R \tag{18}$$

where T_R is the average repairing time, and suitable to all detected failure.

Definition 2. Under the case of periodic maintenance, the repairable time should equal to the sum of inspecting and repairing time. Assume that the failure may occur in any time in a period, and follows uniform distribution, then periodic maintenance rate is

$$\mu_P = \frac{1}{\frac{T_I}{2}+T_R} \tag{19}$$

where T_I is the inspection period.

In addition, we need to do some basic assumptions before safety and reliability analysis as follows.

- comparator and switching cell are perfect reliable, and reliability is one,
- different system modules possess same failure rate and repairable rate,
- inspection and repairable are perfect, i.e., after repairing the cell restores to its original state,
- the restart time is SD after a safety failure occurs,
- the diagnostic coverage rate of the comparable program is C_1, it may detect the failures that self-diagnostic system cannot find.

3.3. Markov Model Analysis on Two-Cell Dynamic Redundant Structure

According to the former analysis, the Markov models of three kinds of dynamic redundant structures are isomorphic. Hence, we may establish a unified model for them as shown in Figure 4.

In Figure 4, the state zero expresses the two cells are perfect and work normally, and the state one expresses one cell is in failure and can be detected, and the state two represents one cell generates the dangerous failure that self-diagnostic program cannot find but comparison program may detect out, and the state three represents one cell generates the safety failure that self-diagnostic program cannot find but comparison program may detect out, and the state four presents the system safety failure, and the state five expresses the system dangerous failure but can be detected, and the state six presents the system dangerous failure undetected. In process of modeling, we assume that when one cell gets inspection and maintenance, and another cell also will have a chance to get detection and repairing. In addition, we also assume a maintenance rule of online repairing system under the condition that the system is not terminated. Likewise, we also assume that periodic detection and maintenance is perfect and can find any problem, and after repairing the system restores to the initial state. Thus, we may ignore the service arc from the state six to the state zero, as well as its service rate u_p. In fact, in terms of high security and high reliability system, it is meaningless to solve the steady state indexes.

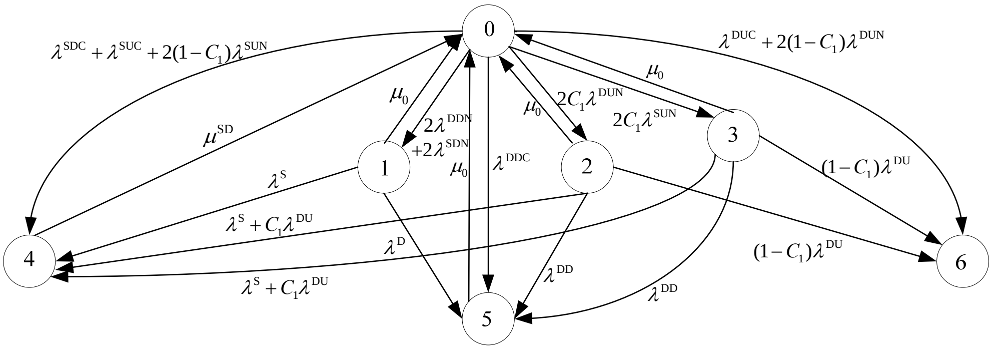

Figure 4. Isomorphic Markov model

Though observing carefully the state 2 and 3, we find that they possess the same transfer rates to any other states, and so they meet the condition of merger. The merged state transfer diagram is shown in Figure 5.

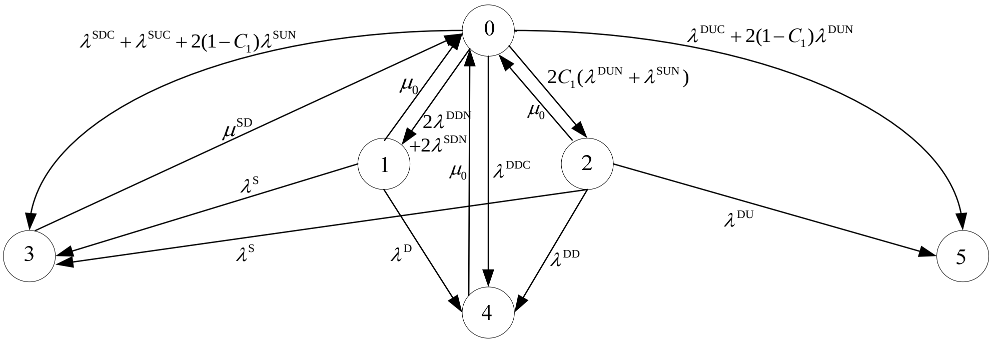

Figure 5. Merged Markov model

According to Figure 5, we can acquire its state transition matrix *P* below.

$$P=\begin{bmatrix} 1-(\lambda^{DC}+\lambda^{SC}+2\lambda^{DN}+2\lambda^{SN}) & 2\lambda^{DDN}+2\lambda^{SDN} & 2C_1(\lambda^{DUN}+\lambda^{SUN}) & \lambda^{SDC}+\lambda^{SUC}+2(1-C_1)\lambda^{SUN} & \lambda^{DDC} & \lambda^{DUC}+2(1-C_1)\lambda^{DUN} \\ \mu_0 & 1-(\lambda^{S}+\lambda^{D}+\mu_0) & 0 & \lambda^{S} & \lambda^{D} & 0 \\ \mu_0 & 0 & 1-(\lambda^{S}+\lambda^{D}+\mu_0) & \lambda^{S}+C_1\lambda^{DU} & \lambda^{DD} & (1-C_1)\lambda^{DU} \\ \mu_{SD} & 0 & 0 & 1-\mu_{SD} & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

As the matrix contains the absorbing states, as the normal work index of the system, to calculate the steady availability is no sense. The typical application of the absorbing state is on the failure not to be repaired in range of the interested time, actually. In accordance with the matrix, the transient availability at any moment can be calculated based on Markov chain method in a detection cycle. Assume that the initial state is S_0, and the *n*-step state transient probability is p^n, and then the transient probability at *n* moment is

$$S_n = S_0 P^n \qquad (20)$$

According to S_n, we may solve the *PFD*, *PFS*, and availability at *n* moment. *PFS* is the probability of state three, and *PFD* is the probability sum of state four and five, and the availability is the probability sum in state zero, one, and two.

To solve the *MTTF*, we firstly must eliminate the arcs from the failure states to work states in Markov model, and then, we will acquire a new state transient matrix. Secondly, the lines and columns related to all absorbing states are cancelled from the state transient matrix, at this moment we will get a section-matrix *Q*. Thirdly, *Q* is subtracted using unit matrix *I*, and we have *I-Q*. Fourthly, the matrix *I-Q* is inversed, and then order *N*=[*I-Q*].

Finally, according to *N* matrix and time increment, we may work out *MTTF* [10].

4. Examples

The security failure rate of two-cell hot spare system is expressed by λ_S=1.48×10-5h^{-1}, and λ_D=0.37×10-5h^{-1} is the dangerous failure rate. 90% of the safety and dangerous failures can be found by self-diagnostic program, and the diagnostic coverage rate of comparison program is 99.9%, and online maintenance rate μ_0 equals 0.1, and common-cause factor β equals 0.075. If the system generates a safety failure, then it could restart within 24 hours. As *t*=8760h, show that PFD, PFS, RRF, MTTF are, respectively, under the conditions of the fundamental mode with C_1=0.0%, the enhanced mode with C_1=95%, and the upgraded mode with C_1=99.9%. Below we take the enhanced mode for example to show the whole calculation process.

Firstly, according to (11) to (17), the diverse failure rates are calculated as shown in Table 1.

Table 1. Failure rate calculation

Failure rate type	Numerical value (×10^{-5}h^{-1})	Remarks
λ^{SDC}	0.0999	
λ^{SDN}	1.2321	
λ^{SUC}	0.0111	
λ^{SUN}	0.1369	
λ^{DDC}	0.024975	
λ^{DDN}	0.308025	
λ^{DUC}	0.002775	
λ^{DUN}	0.034225	

In addition, according to subject, we have μ_0=0.1, *SD*=24h, T_I=8760h, and C_1=0.95. Hence, T_R=10h, and μ_{SD}=0.041667.

Below we adopt Markov model to calculate *PFD*, *PFS*, and *RRF*.

Substituting the data in Table 1 into state transition matrix *P*, we then have

$$P = \begin{bmatrix} 0.99996 & 0.0000308 & 0.0000033 & 0.0000012 & 0.00000025 & 0.000000062 \\ 0.1 & 0.8999815 & 0 & 0.0000148 & 0.0000037 & 0 \\ 0.1 & 0 & 0.8999815 & 0.000008998 & 0.00000333 & 0.00000037 \\ 0.41667 & 0 & 0 & 0.958333 & 0 & 0 \\ 0.1 & 0 & 0 & 0 & 0.9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Given system initial state $\boldsymbol{S_0}$=[1 0 0 0 0 0], and time increment 1h, then according to (20), the probabilities of each state in 8760h are

$\boldsymbol{S_{8760}}$= $\boldsymbol{S_0}$×P^{8760} =[0.999084652418216 0.000307686318747 0.000032478000312 0.000030018838532 0.000002507681384 0.000542656743068].

Clearly, the system failure probability at the dangerous side equals the sum of the probabilities that it stays at the state 4 and 5, then

PFD= 0.000545164424452

From (10), we have

RRF=1834

Likewise, the system failure probability at the security side equals the probability that it stays at the state 3, then

PFS= 0.000014324753198

Below we calculate the *MTTF*. According to the former description, we firstly get section matrix *Q* as follows.

$$Q = \begin{bmatrix} 0.99996 & 0.0000308 & 0.0000033 \\ 0.1 & 0.8999815 & 0 \\ 0.1 & 0 & 0.8999815 \end{bmatrix}$$

And so, we easily get

$$N = [I - Q]^{-1} = \begin{bmatrix} 639009 & 197 & 20 \\ 638890 & 207 & 20 \\ 639890 & 197 & 30 \end{bmatrix}$$

From *N* matrix, we can predict the time that Markov chain from the state zero starting arrives at the absorbing state is 639226h, and 624345h for the state one starting, and 624345h for the state two starting. As the system starts at state zero, then

MTTF=639226h

In the same way, we also may calculate the security and reliability indexes of the fundamental mode and the upgraded mode. For convenient compassion, the security and reliability indexes of three kinds of dynamic redundant structures as shown in Table 2.

Table 2. Reliability and Security Indexes calculation of the diverse modes

Types	PFS	PFD	RRF	MTTF
Fundamental mode	0.000091850346768	0.006219886770141	161	207718
Enhanced mode	0.000030018838532	0.000545164424452	1834	639226
Upgraded mode	0.000026810406593	0.000251581925240	3975	715935

Seen from Table 2, the security and availability indexes of the upgraded mode are the highest, and the ones of the enhanced mode is inferior, and the ones of the fundamental mode is the lowest. For the hardware requirements, the enhanced mode is the highest, and the upgraded mode is inferior, and the fundamental is the lowest. From the hardware and software demands and technology implementation difficulty degree, generally, the upgraded mode is the highest, and the enhanced one is inferior, and the fundamental mode is the lowest. Hence, for modern railway signal system, it is very necessary to select the suitable redundant structures combining the requirements on safety and reliability, and cost, and the difficult-easy degree in technology realization. Simultaneously, we also see the difference between the enhanced model, and the upgraded mode, and as well as the fundamental mode lies in the added comparison channel. If the enhance mode possesses very high security and reliability, and whose hardware has quite high security to be able to meet the demands on the security and reliability indexes, and then it is unnecessary to adopt the upgraded mode system not to avoid the cost increasing and maintenance difficulty.

5. Conclusion

The paper analyses the security and reliability on three kinds of two-cell dynamic redundant systems widely applied in China modern railway signal systems, and establishes the isomorphic Markov model for them. On the basis of it, through analysis and calculation we find their difference only lies in the diagnosis capabilities of the added diagnostic channel. This shows that the measures to improve on the fundamental mode concern the software-hardware comparison and redundancy realization. Clearly, the ability of such an improvement is limited, and cannot be inordinately improved. If in this case the security requirements also cannot be met, and then we only search the other way to resolve.

Acknowledgments

This project is supported by Railways Ministry Science and Technology Research and Development Program (2012X003-B).

References

[1] M Li, F Wu. Railway Signal Reliability and Safety Theory and Confirmation. Beijing: China Railway Publishing House. 2008: 18-34.
[2] J Gao, J Zheng. Quantity Analysis of Reliability and Security in the Computer-based Interlocking System with Dual Computers. *Journal of Northern Jiaotong University*. 1998; 22 (5): 73-77.
[3] X Feng, X Wang. Analysis on Reliability and Performance of Computer-based Interlocking System with the Dynamic Fault Tree Method. *Journal of the China Railway Society*. 2011; 33(12): 78-82.
[4] L Sun, H Xu. Study of Security and Usability of the Dual Module Hot Spare Computer Interlocking Control System. *China Safety Science Journal*. 2004; 14(7): 30-33.
[5] J Yan, X Wang. Reliability and Safety Analysis of Two Modes of Dual Module Hot Spare Architecture. *Journal of the China Railway Society*. 2000; 22(3): 124-127.
[6] F Liu, H Wang. A Comparison Between Double 2-vote-2 and Dual Hot Spare Interlocking System with Computer-based. *Railway signaling and communication*. 2008; 44(2): 26-29.
[7] T He. Safety Analysis and Design for the Switch Control Unit of ALL-Electronic Computer Interlocking System. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2011; 10(5): 1057-1061.
[8] P Zhang, Y Zhao. Analysis on the Reliability and Safety of the Interlocking Control System of Railway Computer. *China Safety Science Journal*. 2003; 13(4): 48-50.
[9] K Sun, H Feng, J Zhou. Reliability Optimum Design of Spring in the Tools Stroage. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2011; 10(5): 1123-1129.
[10] WM Goble. Control System Safety Evaluation and Reliability. 3rd Edition. RaIeigh: ISA. 2010.