Reliability and Security Analysis on 3-vote-2 Voting System

Hongsheng Su

School of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China

shsen@163.com

Abstract

To aim at 3-vote-2 voting system which had already been widely applied in modern railway signal system, based on Markov model the paper analyzed its security and reliability indexes respectively under the three operating modes. During modeling some significant factors, such as common-cause failure, coverage rate of diagnostic systems, online maintainability, periodic inspection, and diverse failure modes, not only were considered, but also according to practical applications, the three types of Markov models were established for 3-vote-2 voting system with diversity version software on condition that secondary degradation was allowed, and secondary degradation was not allowed, and as well as not only secondary degradation was not allowed but also primary degradation was not be allowed too, that is 2oo2 model operating. They were respectively defined as Mode I, and Mode II, and Mode III. Based on the Markov models, the reliability and security indexes of the three modes were worked out. Compared with 3-vote-2 voting system with single version software, the results showed that the influence of diversity software versions on 3-vote-2 voting system security was unapparent, but quite dramatic for its reliability. In addition, the impacts on system reliability and security were unapparent whether considering secondary degradation or not, and the results tended to be conservative and the system was easy to realize while not considering secondary degradation. In the end, the investigations still showed that the impacts on system security performance were not very large, but relatively larger on system reliability under the Mode III, and the results tended more conservative and the system was easier to realize. Hence, after comprehensive consideration on reliability, and security, and as well as easy realization factor, we consider that the Mode III possesses better performance presentation, and is an ideal realization scheme for 3-vote-2 voting system.

Keywords: *3-vote-2 voting system, diversity version software, security, reliability, Markov, degradation*

1. Introduction

As large-scale application of computers and programmable electronic products in 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, automatic train driving, train over-speed protection, and *etc.* To satisfy the demands on high security and high availability, a large number of redundant architectures are applied in the design of security computer. The commonly used redundant structures include dual module hot spare, 2-vote-2 voting, 3-vote-2 voting system [1]. Two diverse dual hot spare redundancy structures are investigated in [2], the acquired conclusion is that the one comparing their results each other has higher safety than the other without comparing their results during operation, and the latter possesses better

availability. But during analyzing online maintenance and periodic inspection are not considered. In [3], the reliability and security on 2-vote-2 voting system is investigated. However, common-cause failure is not considered. This is unsuitable for the systems with high security and high reliability. In [4], a comparison is performed between dual hot spare system and double 2-vote-2 redundancy system. As a result, the former has higher reliability, and the latter possesses better safety. During analysis the maintenance is not considered after the system closes safely. As a fact, the servicing speed possesses important impacts on system security. As in [5], the dynamic fault tree 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 to model. But during modeling the influence of maintenance and common-cause on system safety performance is not considered, and so it is difficult for it to fit into the practice. In [6] 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 local failure can continue working a period of time, from safety consideration, at the moment the system has already become unsafe. Moreover, during analysis the common cause are not considered. In [7] several common-used two-cell redundant structures are analyzed and compared for their reliability and safety. But the established models are quite simple, and it is difficult to apply practically. Clearly, the above models possess the serious dependence on fault detection and positioning, and are difficult to meet the requirements on high security and reliability for rail transit at the same time. Hence, railway signal safety criticism systems widely use 3-vote-2 voting system. From failure-safety angle, 3-vote-2 voting technology is equal to 2-vote-2 technology, and only its redundant equipments reduce to half of the original. In [8] the reliability and security on 3-vote-2 voting system are analyzed based on Markov model, but common-cause failure and online diagnosis detection system are not considered in process of modeling. It is therefore difficult to apply. Similarly, the reliability and security are discussed on 3-vote-2 voting system using Markov model in [9], but where the consideration on failure modes is inadequate so that it is difficult to understand the model. In addition, the above discussed architecture on 3-vote-2 system is a kind of simpler architecture, *i.e.*, whose hardware adopts 3-vote-2 voting technology, and software only applies single version to ensure the fault-safety. But in practice, the 3-vote-2 voting system with complicated architecture is applied more, *i.e.*, whose hardware adopts 3-vote-2 voting technology, and software applies diversity version to ensure the fault-safety. That is to say, this architecture can ensure the fault-safety to the greatest extent through 3-host operating diversity version software. The related investigations show that it can not only find some software mistakes but also still detect some hardware faults during operating so as to be able to ensure the fault-safety to the greatest degree for diverse hosts operate different versions software. In actual applications, the 3-vote-2 voting system that we see more does not allow secondary degradation, and even can not degrade as 2oo2 mode operation. Hence, in this paper we firstly aim at 3-vote-2 voting system with diversity version software to implement the analysis on reliability and security under considering secondary degradation. Then combining with practice, respectively analyses its reliability and security indexes under the other two situations, *i.e.*, 3-vote-2 voting systems without allowing secondary degradation, and as well as the one without not only allowing secondary degradation but also degrading as 2oo2 model operating. And eventually, we perform analysis and comparison. Thus, the safety and reliability of 3-vote-2 voting systems are reflected more deeply.

2. System Architecture

3-vote-2 voting system is a set of fault-safety system composed of 3 sets of mutually independent interlocking modules and a set of high reliable voting module as shown in Fig.1, where three interlocking modules adopt peer isomorphism fault-tolerant structure, and realize safety isolation in electricity to guarantee the failure not to spread. Each interlock module consists of embedded security computer with high performance, whose channel generally possesses strong fault monitoring and self diagnosis ability. For the basic 3-vote-2 voting system, three computers are equipped with totally identical single version software, and so it is difficult to find software error itself in the operating process. But for some upgraded 3-vote-2 voting systems, three computers respectively fix three sets of interlocking software with diverse versions designed according to diversity principle, which means that it offer another level of security protection, namely, the comparison program can find one failure that the self-diagnostic program can not detect. Under the control of synchronous modules, three computers complete the synchronous acquisition of external input data and exchange data each other through data interaction modules, and implement the voting and outputting on three computers data through security relay.

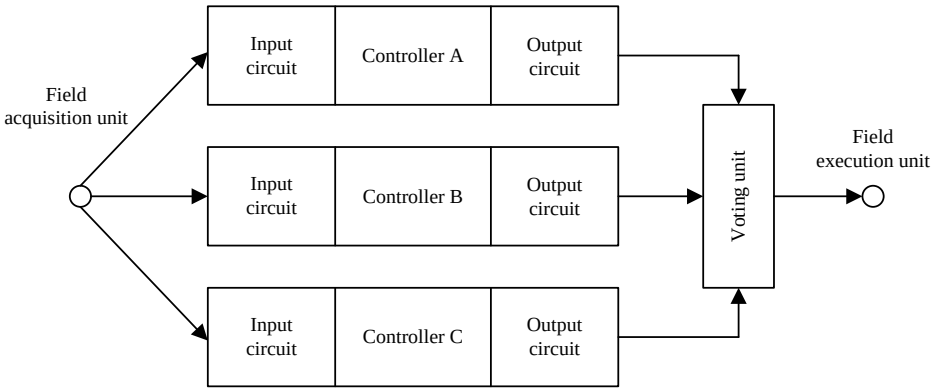

Figure 1. Architecture of 3-vote-2 Voting System

In Figure 1, the voting modules complete the consistency validation of the outputs of the three interlocking computers through majority voting principle. If the results are inconsistent, one inconsistent computer is then shut. Maintenance personnel may perform on-line maintenance and restarting on fault module without affecting the normal operation of the system. The voting circuit is shown in Figure 2.

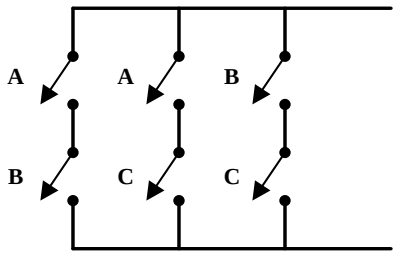

Figure 2. Voting Module

3. System Security and Reliability Analysis

It can be found that the system allows any one of the two failure modes through research on voting logic in Figure 2. As a danger or short circuit failure occurs in a cell, the system implements the degradation and then operates in 2oo2 mode. In another hand, when a cell shows safe or open circuit failure, the system degrades as 1oo2 mode. Under the two kinds of modes, the system can continue normal work all the time. The system will destroy only when arbitrary two cells simultaneously generate dangerous failure. This outcome is resulted in by four types of common-cause failures, for example, AB branch failure, and AC branch failure, and BC branch failure, and as well as the combination of the three independent failures. The failure probability more than two branches may be neglected relative to single branch. The detection coverage rate of self-diagnostic program requires to be considered when the security model is established for the system in Figure 1, then linked to common cause, clearly, the system totally generates eight types of failure modes.

Definition 1. Let the failure rate of single module be λ, the failure rate at system safety side be λ_S and the failure rate be λ_D at danger side, and then

$$\lambda=\lambda^S+\lambda^D. \tag{1}$$

Let the diagnosis coverage rate be C of the self-diagnostic program, and then

$$\lambda^{SD}=C\lambda^S \tag{2}$$

$$\lambda^{SU}=C\lambda^S \tag{3}$$

$$\lambda^{DD}=C\lambda^D \tag{4}$$

$$\lambda^{DU}=C\lambda^D \tag{5}$$

where λ^{SD} denotes the detected safety failure rate, and λ^{SU} means the undetected safety failure rate, and λ^{DD} expresses the detected dangers failure rate, and λ^{DU} is the undetected danger failure rate.

Consider common failure fault factor β, and then

$$\lambda^{SDC}=\beta\lambda^{SD} \tag{6}$$

$$\lambda^{SDN}=(1-\beta)\lambda^{SD} \tag{7}$$

$$\lambda^{SUC}=\beta\lambda^{SU} \tag{8}$$

$$\lambda^{SUN}=(1-\beta)\lambda^{SU} \tag{9}$$

$$\lambda^{DDC}=\beta\lambda^{DD} \tag{10}$$

$$\lambda^{DDN}=(1-\beta)\lambda^{DD} \tag{11}$$

$$\lambda^{DUC}=\beta\lambda^{DU} \tag{12}$$

$$\lambda^{DUN}=(1-\beta)\lambda^{DU} \tag{13}$$

where λ^{SDC} expresses the safe detected common-cause failure, and λ^{SDN} denotes the safe undetected normal failure, and λSUC denotes the safe detected common-cause failure, and λSUN denotes the safe undetected normal failure, and λDDC represents the dangerous detected common-cause failure, and λDDN means the dangerous detected normal failure, and

λDUC represents the dangerous undetected common-cause failure, and λDUN means the dangerous undetected normal failure.

If self-diagnosis program detects and prompts a failure, the failure can be then repaired, immediately. And otherwise it would be still unknown by people. Sometimes one failure can be found until it happens. 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, and 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 2. Let online maintenance rate be μ_0, then

$$\mu_0=1/T_R \tag{14}$$

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

Definition 3. 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

$$\mu_P = \frac{1}{\frac{T_I}{2}+T_R} \tag{15}$$

where T_I is the inspection period.

Definition 4. Let the reliability be $R(t)$, and the unreliability can be expressed as $F(t)$=1-$R(t)$, and then, the mean time to failure (*MTTF*) of the system can be denoted by

$$MTTF = E(T) = \int_0^{+\infty} tf(t)\mathrm{d}t = -\int_0^{+\infty} t\mathrm{d}[R(t)] = \int_0^{+\infty} R(t)\mathrm{d}t \tag{16}$$

According to the definition of the unreliability, it should contain the diverse failure modes. Clearly, we can have

$$F(t) = PFS(t) + PFD(t) \tag{17}$$

where *PFS* denotes as the safe failure probability, and *PFD* is the dangerous failure probability.

For the repairable systems, the unavailability can be denoted by

$$\bar{A}(t) = PFS(t) + PFD(t) \tag{18}$$

And then the availability can be expresses by

$$A(t) = 1-[PFS(t) + PFD(t)] \tag{19}$$

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

$$S(t) = 1-PFD(t) \tag{20}$$

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

$$RRF=1/PFD. \quad (21)$$

The formula (21) 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 in (21) to express.

In some more advanced system, 3-vote-2 voting system does not allow secondary degradation, sometimes even can not degrade as 2oo2 mode operation. To conveniently analyze the safe performances under diverse situations, we have the followings definitions.

Definition 5. For conveniently analysis, let the Mode I express 3-vote-2 voting system with diversity-version software under considering secondary degradation, and the Mode II present 3-vote-2 voting system with diversity-version software without considering secondary degradation, and Mode III express 3-vote-2 voting system with diversity-version software without not only considering secondary degradation, but also degrading as 2oo2 model operating.

In addition, some basic assumptions require to be given before the safety and reliability analysis.

- system voting cell is perfect reliable, and reliability is one,
- 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 diverse-version programs is C_1, and is independent on one of self-diagnostic program.

3.1. Security and Reliability Analysis on Mode I

Based on the former analysis and assumptions, the Markov model is established on Mode I as shown in Figure 3.

In Figure 3, the state zero expresses the three cells are perfect and system work normally, and the state one expresses one cell generates safe detected failure, and the state two represents one cell generates safe undetected failure, and the state three represents one cell generates the dangerous detected failure, and the state four presents one cell generates the dangerous undetected failure. At state one and state two, the system degrades as 1oo2 mode, and the system degrades as 2oo2 mode at state three and state 4.The state five expresses the case that one cell generates detected safe failure and another cell generates the detected danger failure, and the state six expresses one cell generates detected safe failure and another cell generates the undetected danger failure, The state seven expresses the case that one cell generates undetected safe failure and another cell generates the detected danger failure, and the state eight expresses one cell generates undetected safe failure and another cell generates the undetected danger failure. From state five and state eight, the system operates in secondary degradation state. The state nine expresses the system safety failure, and state ten expresses the system generates the danger failure but can be detected, and the state eleven expresses system danger failure but can not be detected. During modeling,

we assume that when one cell gets inspection and maintenance, and another cell also will have a chance to get detection and repairing.

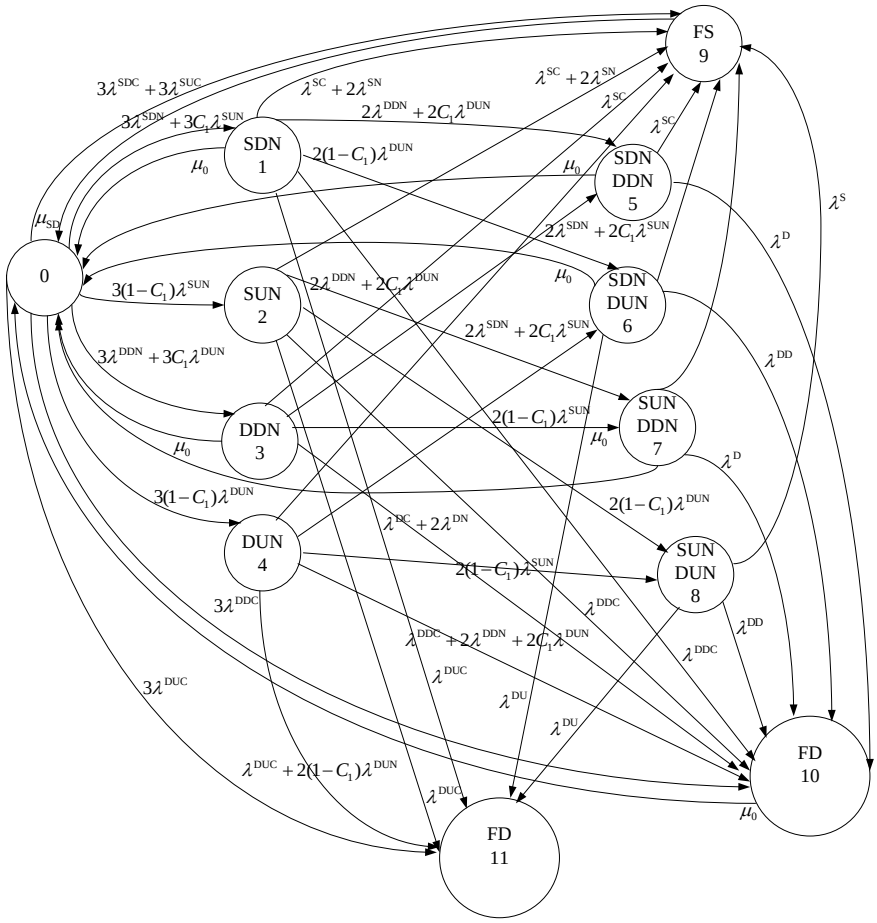

Figure 3. Markov Model of Mode I

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 eleven to the state zero, as well as its service rate u_p. In fact, for the high security and high reliability systems, it is meaningless to solve the steady state indexes.

According to Figure 3, the state transition matrix $\boldsymbol{P}$ can be easily written below.

$$P=\begin{vmatrix}
1-\Sigma & 3\lambda^{SDN}+3C_1\lambda^{SUN} & 3(1-C_1)\lambda^{SUN} & 3\lambda^{DDN}+3C_1\lambda^{DUN} & 3(1-C_1)\lambda^{DUN} & 0 & 0 & 0 & 0 & 3\lambda^{SDC}+3\lambda^{SUC} & 3\lambda^{DDC} & 3\lambda^{DUC} \\
\mu_0 & 1-\Sigma & 0 & 0 & 0 & 2\lambda^{DDN}+2C_1\lambda^{DUN} & 2(1-C_1)\lambda^{DUN} & 0 & 0 & \lambda^{SC}+2\lambda^{SN} & \lambda^{DDC} & \lambda^{DUC} \\
0 & 0 & 1-\Sigma & 0 & 0 & 0 & 0 & 2\lambda^{DDN}+2C_1\lambda^{DUN} & 2(1-C_1)\lambda^{DUN} & \lambda^{SC}+2\lambda^{SN} & \lambda^{DDC} & \lambda^{DUC} \\
\mu_0 & 0 & 0 & 1-\Sigma & 0 & 2\lambda^{SDN}+2C_1\lambda^{SUN} & 0 & 2(1-C_1)\lambda^{SUN} & 0 & \lambda^{SC} & \lambda^{DC}+2\lambda^{DN} & 0 \\
0 & 0 & 0 & 0 & 1-\Sigma & 0 & 2\lambda^{SDN}+2C_1\lambda^{SUN} & 0 & 2(1-C_1)\lambda^{SUN} & \lambda^{SC} & \lambda^{DDC}+2\lambda^{DDN}+2C_1\lambda^{DUN} & \lambda^{DUC}+2(1-C_1)\lambda^{DUN} \\
\mu_0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 & 0 & \lambda^{S} & \lambda^{D} & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 & \lambda^{S} & \lambda^{DD} & \lambda^{DU} \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & \lambda^{S} & \lambda^{D} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & \lambda^{S} & \lambda^{DD} & \lambda^{DU} \\
\mu_{SD} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{vmatrix}$$

In the above matrix the symbol $\sum$ expresses the sum of other elements located at same line except the primary diagonal element.

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

$$S_n = S_0 P^n \tag{22}$$

According to S_n, we may solve the *PFD*, *PFS*, and availability at *n* moment. *PFS* is the probability of state 9, and *PFD* is the probability sum of state 10 and 11, and the availability is the probability sum in state zero to eight.

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].

3.2. Security and Reliability Analysis on Mode II

In many practical applications, 3-vote-2 voting system does not allow secondary degradation, *i.e.*, it does not allow the occurrence of double faults of two or more than two modules. This means that the system would be failure when the number of the failure module is two. And so, the states from 5 to 8 are not allowed to act as normal work states of the system. Once the system enters into these states, the system would then be failure. The present problem is that system failure is only in the three states such as the state 9, 10, and 11, how we would merge the four states with single module work from 5 to 8 into the three types of system failure states. Through careful observation and comprehension on system operation behavior, it is thought to be reasonable that the state 8 should merge into the state 11, that is, the system would face an undetected danger failure when it enters into the state 8. The reason to do is that it is very much alike with the state 11, *i.e.*, at the state 8 the system possesses the undetected double-module fault, where the system is unable to return to normal states as not acquire timely maintenance, and only through the regular maintenance it possibly returns to the normal state, it is very much alike with the state 11. In addition, it is a conservative approach that the state 8 is attributed to the state 11, and so the relative analysis result is usable still. Similarly, the states from 5 to 10 are merged into the state 10, and seen as the detected danger failure. The reason is that at the states the system always has a detected failure, at the moment, the system returns to the working states as the attendant may implement online maintenance. It is identically conservative to do this, and so the result may be applied. The merged state transition diagram is shown in Figure 4.

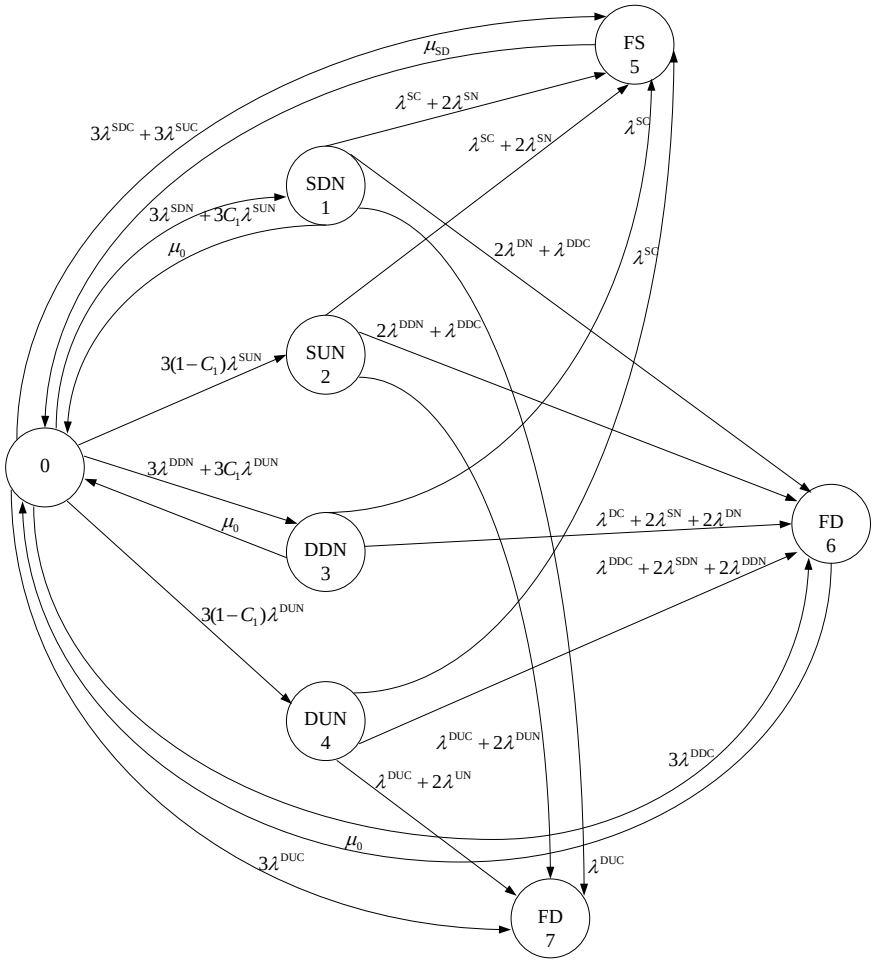

Figure 4. Markov Model on Mode II

The state transition matrix in Figure 4 can be written as follows.

$$P=\begin{vmatrix} 1-\Sigma & 3\lambda^{SDN}+3C_1\lambda^{SUN} & 3(1-C_1)\lambda^{SUN} & 3\lambda^{DDN}+3C_1\lambda^{DUN} & 3(1-C_1)\lambda^{DUN} & 3\lambda^{SDC}+3\lambda^{SUC} & 3\lambda^{DDC} & 3\lambda^{DUC} \\ \mu_0 & 1-\Sigma & 0 & 0 & 0 & \lambda^{SC}+2\lambda^{SN} & 2\lambda^{DN}+\lambda^{DDC} & \lambda^{DUC} \\ 0 & 0 & 1-\Sigma & 0 & 0 & \lambda^{SC}+2\lambda^{SN} & 2\lambda^{DDN}+\lambda^{DDC} & \lambda^{DUC}+2\lambda^{DUN} \\ \mu_0 & 0 & 0 & 1-\Sigma & 0 & \lambda^{SC} & \lambda^{DC}+2\lambda^{SN}+2\lambda^{DN} & 0 \\ 0 & 0 & 0 & 0 & 1-\Sigma & \lambda^{SC} & \lambda^{DDC}+2\lambda^{DN} & \lambda^{DUC}+2\lambda^{UN} \\ \mu_{SD} & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

The security and reliability can be acquired through the state transition matrix ***P*** using the same approach.

3.3. Security and Reliability Analysis on Mode III

In some 3-vote-2 voting systems more advanced, the system does not allow to degrade as 2oo2 mode operation when a module is in failure, the reason is that the system will become unsafe under operating in 2oo2 mode due to default of consistency comparison between two

or more cells. Hence, on the basis of 3-vote-2 voting system, an additional diagnostic channel is provided to ensure the system safety, further. The role of the additional diagnostic channel is to make a detected danger failure turn into the safety failure. In addition, to make the system safe more and realize easy, the role of the diversity among different-version programs also has dramatic change, *i.e.*, it makes a failure detected by multi-version programs but self-diagnostic program can not find directly turn into safety failure. Based on the above analysis and discussion, the Markov model in Figure 4 is changed into one in Figure 5.

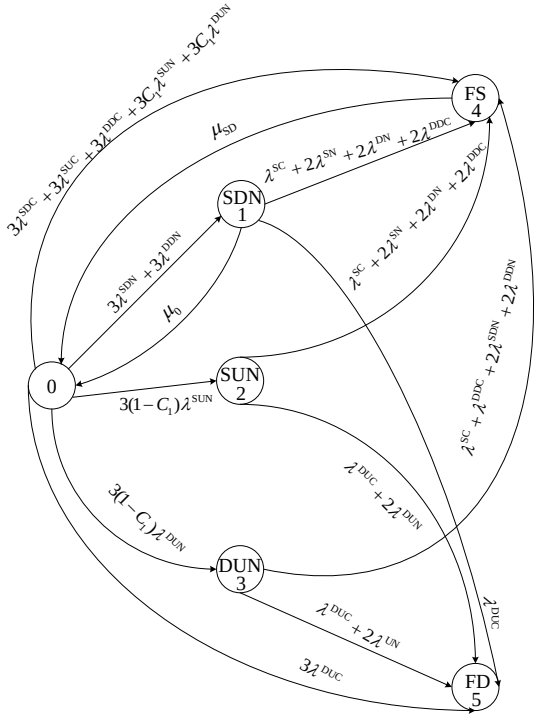

Figure 5. Markov Model on Mode III

According to Figure 5, the state transition matrix can be written below.

$$P=\begin{vmatrix} 1-\Sigma & 3\lambda^{SDN}+3\lambda^{DDN} & 3(1-C_1)\lambda^{SUN} & 3(1-C_1)\lambda^{DUN} & 3\lambda^{SDC}+3\lambda^{SUC}+3C_1\lambda^{SUN}+3C_1\lambda^{DUN}+3\lambda^{DDC} & 3\lambda^{DUC} \\ \mu_0 & 1-\Sigma & 0 & 0 & \lambda^{SC}+2\lambda^{SN}+2\lambda^{DN}+\lambda^{DDC} & \lambda^{DUC} \\ 0 & 0 & 1-\Sigma & 0 & \lambda^{SC}+2\lambda^{SN}+2\lambda^{DDN}+\lambda^{DDC} & \lambda^{DUC}+2\lambda^{DUN} \\ 0 & 0 & 0 & 1-\Sigma & \lambda^{SC}+\lambda^{DDC}+2\lambda^{DN} & \lambda^{DUC}+2\lambda^{UN} \\ \mu_{SD} & 0 & 0 & 0 & 1-\Sigma & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

The security and reliability indexes can still be calculated through the matrix ***P***.

4. Examples

The failure rate at security side of 3-vote-2 voting system is $\lambda^S=1.48\times10^{-5}h^{-1}$, and the failure rate at danger side is $\lambda^D=0.37\times10^{-5}h^{-1}$, and self-diagnostic program can find 90 percent of the safety and danger failures, and the diagnostic coverage rate of multi-version program is 95%, 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 under the Mode I, Mode II, and Mode III, respectively.

The whole calculation process is shown as follows.

Firstly, according to subject, we can know C=0.9 and β=0.075. From (1) to (13), the diverse failure rates are calculated as shown in Table1.

Table 1. Failure Rates Calculation

Failure rate type	Numerical value ($\times 10^{-5}h^{-1}$)	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=0.1h^{-1}, TI=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 Tab.1 into state transition matrix $\boldsymbol{P}$, we then have

$$P=\begin{bmatrix}
0.9999445 & 0.000040865 & 0.0000002 & 0.0000102 & 0.000000051 & 0 & 0 & 0 & 0 & 0.00000333 & 0.00000074925 & 0.00000008325 \\
0.1 & 0.899964 & 0 & 0 & 0 & 0.000006811 & 0.0000000342 & 0 & 0 & 0.00002849 & 0.00000024975 & 0.00000002775 \\
0 & 0 & 0.999964 & 0 & 0 & 0 & 0 & 0.000006811 & 0.0000000342 & 0.00002849 & 0.00000024975 & 0.00000002775 \\
0.1 & 0 & 0 & 0.899964 & 0 & 0.000027243 & 0 & 0.0000001369 & 0 & 0.00000111 & 0.000006438 & 0 \\
0 & 0 & 0 & 0 & 0.999964 & 0 & 0.000027243 & 0 & 0.0000001369 & 0.00000111 & 0.0000070605 & 0.00000006198 \\
0.1 & 0 & 0 & 0 & 0 & 0.8999815 & 0 & 0 & 0 & 0.0000148 & 0.0000037 & 0 \\
0.1 & 0 & 0 & 0 & 0 & 0 & 0.8999815 & 0 & 0 & 0.0000148 & 0.00000333 & 0.00000037 \\
0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.8999815 & 0 & 0.0000148 & 0.0000037 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.999815 & 0.0000148 & 0.00000333 & 0.00000037 \\
0.041667 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.958333 & 0 & 0 \\
0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.9 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}$$

Given system initial state $\boldsymbol{S_0}$=[1 0 0 0 0 0 0 0 0 0 0 0], and time increment 1h, then according to (22), the probability of each state as 8760h is

$\boldsymbol{S_{8760}}= \boldsymbol{S_0}\times P^{8760}$ =

[0.996772244272499 0.000407187114581 0.001499604583649 0.000101634453969
0.000382399168830 0.000000005541168 0.000000104195983 0.000000102159278
0.000000452501871 0.000080970600605 0.000007506633492 0.000728240628531]

Clearly, the system failure probability at the dangerous side equals the sum of the probabilities that it stays at the state 10 and 11, then

$$PFD= 0.000735$$

From (21), we have

$$RRF=1360$$

Likewise, the system failure probability at the security side equals the probability that it stays at the state 9, then

$$PFS= 0.000081$$

To work out *MTTF*, we firstly require to get section matrix ***Q***.

$$Q=\begin{bmatrix}
0.9999445 & 0.000040865 & 0.0000002 & 0.0000102 & 0.000000051 & 0 & 0 & 0 & 0 \\
0.1 & 0.899964 & 0 & 0 & 0 & 0.000006811 & 0.0000000342 & 0 & 0 \\
0 & 0 & 0.999964 & 0 & 0 & 0 & 0 & 0.000006811 & 0.0000000342 \\
0.1 & 0 & 0 & 0.899964 & 0 & 0.000027243 & 0 & 0.0000001369 & 0 \\
0 & 0 & 0 & 0 & 0.999964 & 0 & 0.000027243 & 0 & 0.0000001369 \\
0.1 & 0 & 0 & 0 & 0 & 0.8999815 & 0 & 0 & 0 \\
0.1 & 0 & 0 & 0 & 0 & 0 & 0.8999815 & 0 & 0 \\
0.1 & 0 & 0 & 0 & 0 & 0 & 0 & 0.8999815 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.999815
\end{bmatrix}$$

Clearly, it is easy to calculate ***N*** matrix according to the former approach.

$$N=[I-Q]^{-1}=\begin{vmatrix}
229821.2657 & 93.8830 & 1276.7848 & 23.4333 & 325.5801 & 0.0128 & 0.0887 & 0.0870 & 4.7696 \\
229755.2017 & 103.8525 & 1276.4178 & 23.4266 & 325.4865 & 0.0134 & 0.0887 & 0.0869 & 4.7682 \\
43472.8642 & 17.7588 & 28019.2937 & 4.4326 & 61.5865 & 0.0024 & 0.0168 & 1.9080 & 52.2535 \\
229801.4504 & 93.8749 & 1276.6747 & 33.4277 & 325.5520 & 0.0155 & 0.0887 & 0.0869 & 47.6921 \\
173885.0741 & 71.0328 & 966.0282 & 17.7299 & 28024.1149 & 0.0096 & 7.6332 & 0.0658 & 2091.6429 \\
229778.7567 & 93.8657 & 1276.5486 & 23.4290 & 325.5199 & 10.0109 & 0.0887 & 0.0869 & 47.6874 \\
229778.7567 & 93.8657 & 1276.5486 & 23.4290 & 325.5199 & 0.0128 & 10.0868 & 0.0869 & 47.6874 \\
229778.7567 & 93.8657 & 1276.5486 & 23.4290 & 325.5199 & 0.0128 & 0.0887 & 10.0851 & 47.6874 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 54054.0540
\end{vmatrix}$$

In accordance with the ***N*** matrix, we can predict the time that Markov chain starting from the state zero arrives at the absorbing state is 231546h, and the time 231489h starting from the state 1, and 71630h starting from the state 2, and 231536h from the state 3, and 203181h from the state 4, and 231513h from the state 5 which is same with the state 6 and 7, and 54054h starting from the state 8. As the system starts at state zero, then we have

$$MTTF=231546\text{h}$$

Similarly, we find that the Markov chain directly enters into the absorbing state almost without jumping starting from the state 8, the *MTTF* of which is 54054.054h. In fact, this time equals the *MTTF* under single module working, that is,

$$MTTF=\frac{1}{\lambda}=\frac{1}{\lambda_S+\lambda_D}=\frac{1}{(1.48+0.37)\times10^{-5}\,\text{h}^{-1}}=54054.054\text{h}$$

Moreover, the *MTTF* of the Markov chain starting from the state 2 or 4 is a bit partial small than the ones of other states, the reason that there is undetected cell failure at these states, which influences the reliability of the system as not to able to get timely maintenance. Even the Markov chains start from the state 2 and 4, their *MTTF* are not fully same. The reason is that the former implement the degradation into 1oo2 mode and the latter degrades as 2oo2 mode after one cell failure. Generally speaking, at the same situation, 2oo2 structure possesses larger *MTTF* than 1oo2 under same condition. However, from the angle of security, the *PFD* of 2oo2 is smaller than the one 1oo2 one to two orders of magnitude. Hence, after comprehensive consideration on reliability, security, and the characteristics of 3-vote-2 fault-tolerant system, we should try to prevent the emergence of the state 8.

In the original 3-vote-2 voting system, the hardware and software are totally identical and do not possess the diversity, *i.e.*, C_1=0. In the same approach, we may work out the indexes of reliability and security. For conveniently comparison, the related calculation results are shown in Table 2.

Table 2. Reliability and Security Indexes of the Mode I

3-vote-2 voting system	*PFS*	*PFD*	*RRF*	*MTTF*
Mode I(C_1=0)	0.000098	0.000728	1374	144297
Mode I (C_1=0.95)	0.000081	0.000735	1360	231546

Seen from Table 2, the impacts are not too great on system safety behavior adopting the diverse versions software. The reason is that the influence of the diversity on system safety performance is limited at system normal working states, that is, two or more modules normal working environment. If the system degrades into single module working environment, the diversity then loses its detection capability. At this time, the system safety performance becomes same with general 3-vote-2 voting system. And at two or more modules normal working environment, the system possesses certain fault tolerant ability. Even if some failures can not be detected out, the normal work of the system also will not be affected. In another hand, the diversity generates significant influence on system reliability. The reason that the diversity can detect out more failures, the system may return to the normal working state through online maintenance.

Likewise, we also may work out the reliability and security indexes without considering system secondary degradation from Figure 4 and transition matrix related to it. For conveniently comparison, the related calculation results are listed in Table 3.

Table 3. Reliability and Security Indexes of the Mode II

3-vote-2 voting system	*PFS*	*PFD*	*RRF*	*MTTF*
Mode II (C_1=0)	0.000098	0.000954	1048	128226
Mode II (C_1=0.95)	0.000081	0.000742	1347	227892

Seen from Table 3, the security and reliability properties of 3-vote-2 voting system with the diversity version software acquire the improvement under no consideration system secondary degradation situation. It is evidently better than the situation considering secondary degradation application at safety improvement aspect. The reason is that single module working situation under secondary degradation application offsets the benefits from the diversity of multi-version software.

Compared with Table 2, we find the *PFD* in Table 3 adds a bit. The reason is that we see the state 8 in Figure 3 as the undetected danger failure and merges into the state 11, which undoubtedly increases the system *PFD*. On the other hand, we eliminate the single module work state, and therefore the *MTTF* in Table 3 drops a bit. In addition, the *PFS* in Table 3 are same with Table 2. The reason lies in that the description on the state 9 does not change during the state combination from Figure 3 to Figure 4. Generally speaking, there are no especial differences for the data in Table 2 and Table 3, and they are at the same order of magnitude. However, if we do not consider secondary degradation, the system operating performance will become simple to make the system analysis convenient and realization easy, and the related calculating results tend to conservative, and therefore are usable.

For the 3-vote-2 voting systems with high security requirements, we may adopt the model in Figure 5, where the system is not allowed to degrade as 2oo2 mode operation. For this case, we also calculate its reliability and security indexes. For convenience analysis and comparison, the relative results are listed in Table 4 together with the former one.

Table 4. Reliability and Security Indexes Comparison between the Mode II and Mode III

3-vote-2 voting system	*PFS*	*PFD*	*RRF*	*MTTF*
Mode II (C_1=0.95)	0.000081	0.000742	1347	227892
Mode III (C_1=0.95)	0.000207	0.000738	1350	107805

From Table 4, we can see that there is a bit improvement in security aspects due to a slightly decreasing of the *PFD*, but the *PFS* improvement increases more. The reason is that the added diagnostic channel makes a detected danger failure turn into a safety failure. On the other hand, the reliability index *MTTF* reduces to about half almost, the reason lies in that the system will have more chance to enter into the safety failure mode due to the improvement in *PFS*. As previously mentioned, compared with the Mode II, the Mode III is easy to realize due to default in fault-location unit, *i.e.*, the system will automatically guide to safety immediately as long as a failure at danger side is found. From that we may get such a conclusion that the system sacrifices its reliability to win a technical convenience as far as possible under the premise of the same *PFD*. Hence, for the Mode III, we should pay more attention to its *MTTF*. In the end, it is noted that in Mode III, the system does not allow to degrade as 2oo2 mode operation, but according to Figure 5, as long as the system enters into the state 3, it then operations as 2oo2 mode. Clearly, this is inevitable due to one undetected danger failure exists in state 3. Fortunately, the probability that the system stay at this state is adequate small, and only is 0.04% in this instance.

5. Conclusions

The paper analyses the security and reliability indexes under the three kinds of operation modes in terms of 3-vote-2 voting system. The relative investigation results show that the role of the diversity is dramatic in terms of reliability improving, but for security, the role of which is obviously smaller. The research results also shows that the impacts of the diversity on security and reliability indexes is not too large respectively under the consideration of secondary degradation or not, and the results without the consideration of secondary degradation tend to conservative and the system is easy to realize. In addition, the investigations still show that the impacts on system security performance are not very large but relatively larger on system reliability under the Mode III, and the results tended more conservative, and the system is easier to realize. Hence, after synthetically consideration on reliability, security, and easy realization, the Mode III has been widely applied in modern railway signal systems.

Acknowledgements

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

References

[1] K. G. Shm and K. Hagbae, “A Time Redundancy Approach to TMR Failures Using Fault-state Likelihood”, IEEE Trans. on Computer, vol. 43, no. 11, **(1994)**, pp. 1151-1162.
[2] J. Yan and X. Wang, “Reliability and safety analysis of two modes of dual module hot spare architecture”, Journal of the China Railway Society, vol. 22, no. 3, **(2000)**, pp. 124-127.
[3] B. Zhang, Y. Lu and J. Hang, “Reliability and security analysis of double 2-Vote-2 redundancy system”, Journal of System Simulation, vol. 21, no. 1, **(2009)**, pp. 256-261.

[4] F. Liu and H. Wang, "A comparison between double 2-vote-2 and dual hot spare interlocking system with computer-based", Railway Signaling and Communication, vol. 44, no. 2, **(2008)**, pp. 26-29.
[5] X. Feng and X. Wang, "Analysis on reliability and performance of computer-based interlocking system with the dynamic fault tree method", Journal of the China Railway Society, vol. 33, no. 12, **(2001)**, pp. 78-82.
[6] L. Sun and H. Xu, "Study of security and usability of the dual module hot spare computer interlocking control system", China Safety Science Journal, vol. 14, no. 7, **(2004)**, pp. 30-33.
[7] J. Shen and D. Shan, "Reliability and safety analysis of TMR computer-based interlocking system", Journal of Northern Jiaotong University, vol. 22, no. 5, **(1998)**, pp. 111-114.
[8] P. Zhang and Y. Zhao, "Analysis on the reliability and safety of the interlocking control system of railway computer", China Safety Science Journal, vol. 13, no. 4, **(2003)**, pp. 48-50**.**
[9] Z. Chen and M. Ni, "Reliability and security analysis of triple-module redundancy system", Computer Engineering, vol. 38, no. 14, **(2012)**, pp. 239-245.
[10] W. M. Goble, Editor, "Control System Safety Evaluation and Reliability", ISA, Raleigh, **(2010)**.

Author

Hongsheng Su obtained his Master in Traffic Information Engineering and Control, Lanzhou Jiaotong University in 2001. He acquired his PhD in Power Systems and Its Automation, Southwest Jiaotong University. Now he is serving as a full-time professor at school of Automation and Electrical Engineering, Lanzhou Jiaotong University. His research interest includes System Security and Reliability, Intelligent Control, Power Systems and Its Automation, and etc.