Safety Analysis on Regional Computer Interlocking System Based on Dynamic Fault Tree

HONGSHENG SU, JUN WEN
School of Automation and Electrical Engineering
Lanzhou Jiaotong University
Lanzhou 730070
P.R.CHINA
shsen@163.com

Abstract: - Regional Computer Interlocking System (RCIS) is a signal control system which performs all interlocking logic operation and implements centralized control for multiple stations only using one set of interlocking equipment. Recently, the main method to analyze safety of dynamic redundancy systems structure is based on the Markov model at home and abroad. But in applying the Markov model to analyze the safety of regional computer interlocking system, the size of state space is quite larger such that the modeling and solving processes become very complex. To solve this issue, in this paper, Dynamic Fault Tree (DFT) model of RCIS is established from the perspective of system failure, and probabilistic approximation method is used to solve the probability of falling safety (*PFS*) and probability of falling danger (*PFD*). Eventually, a comparison is conducted between DFT probabilistic approximation method and Markov method. The relative researches show that DFT probabilistic approximation method possesses roughly same outcome with ones of Markov method, and tends to be more conservative in calculating probability indexes, which provides a new solution for complex dynamic redundancy system safety analysis.

Key-Words: - Regional Computer Interlocking System(RCIS); Dynamic Fault Tree(DFT); Probabilistic approximation method; Probability of falling safety(PFS); Probability of falling danger(PFD)

1 Introduction

For traditional railway signal interlocking systems, signal interlocking devices are established in each station, and can implement independent control on each station signal equipment. With the development of network technology, computer technology, and communication technology, it is possible to make centralized control in a certain range of signal equipment. The concept "range" here can be a station, multiple stations or multiple yards within the dominated scope, that is to say, the regional computer interlocking system (RCIS) completes the interlocking logic operation and implements the centralized control on the multiple stations only using one set of interlocking equipment in range of whole region [1,2]. Thus, the integrated control over station interlocking, section block and dispatching and the command is realized. The great progress of distributed control technology and intelligent terminals make it possible in developing distribute interlocking system [3,4]. But regional computer interlocking possesses the characteristics of centralized control, centralized dispatch and less maintenance, and has become the mainstream trend of the development of computer interlocking today.

Presently, this technology has been widely used in China railway main lines, e.g., some remote unmanned stations, as well as the subway, light rail and dedicated railway yard systems [5-10].

In the past, the regional interlocking is widely applied in industrial railways and private sidings in China. And now it is applied in main lines, for instance, Linyi station, and Jiben regional interlocking and so on. The regional interlocking is also widely used in hub stations and marshaling stations in which field operations are closely linked each other and the business is busy. In hub stations and marshaling stations, usually the centralized control of signaling equipment is applied, but it possibly brings the risk that the entire system would be paralyzed once the central interlocking equipment being in failure due to the tense and fault handling ability. In order to reduce the security risks, regional division is performed, namely, a centralized management of the area can be divided into two or even three areas to disperse the danger. The two regional computer interlocking system has been investigated in [11], and therefore the three regional computer interlocking system is analyzed alone in this paper. Compared with the two-regional-computer-interlocking, the mode of the three- region computer interlocking system is more complicated. The reason lies that it not only has primary degraded mode, but also the secondary degraded mode. In addition, its modeling process is more complicated. Therefore, in this paper, the interlocking area is divided into three parts. Below we define it as three-region RCIS.

The structure of three-region RCIS is shown in Figure 1, where the full control area is divided into three sub-regions with each sub-region being provided with a set of interlocking equipment.

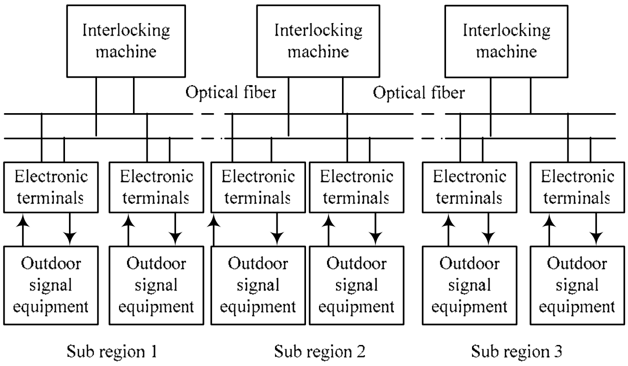


Fig.1 Structure of three-region RCIS

2 Related Concepts

2.1 Failure mode analysis

For convenience analysis, some basic assumptions are conducted below.

(1) System compactors, and voting cells, and interface circuits, and as well as communication lines to constitute interlocking cell are completely reliable.

(2) The interlocking machine in different sub-regions possesses the same failure rate, and both the repairing rate and the failure rate follow the exponential distribution.

(3) The failure rate of interlocking cell will increase as it takes over the task of other failure cells due to the heavy loads. Let the normal failure rate of one cell be λ, and then the failure rate of which becomes λ_1 after taking over one failure cell, and λ_2 for taking over two, and satisfying $\lambda_2>\lambda_1>\lambda$.

(4) Inspection and maintenance are perfect, that is, the cell can restore to its original state after repaired.

2.2 Common cause failure

Common cause failure (CCF) is defined as that the failure of multiple modules occurs at the same time aroused by single cause. Clearly, CCF offsets the advantages of fault-tolerant system. In the analysis on high safety and high reliability system, CCF is a factor that can not be ignored. Hence, in this paper, CCF is considered with β factor model.

After considering the diagnostic ability of the diagnostic system and CCF, the failure rate of the cell can be divided as eight-type, that is λ^{SDN}, and λ^{SDC}, and λ^{SUN}, and λ^{SUC}, and λ^{DDN}, and λ^{DDC}, and λ^{DUN}, and as well as λ^{DUC}. Here λ^{SDN} expresses the safe detected normal failure rate, and λ^{SDC} means the safe detected CCF rate, and λ^{SUN} denotes the safe undetected normal failure rate, and λ^{DDN} expresses the dangerous detected normal failure rate, and λ^{SUC} is safe undetected CCF rate, and λ^{DDC} means the dangerous detected CCF rate, and λ^{DUN} is the dangerous undetected normal failure, and λ^{DUC} means dangerous undetected CCF rate. Let the gross failure rate of the cell beλ, and the safety-side failure rate be λ^{S}, and the danger-side failure rate be λ^{D}. and then we obtain

$$\lambda^{\mathrm{S}} = \lambda^{\mathrm{SD}} + \lambda^{\mathrm{SU}} \tag{1}$$

$$\lambda^{\mathrm{D}} = \lambda^{\mathrm{DD}} + \lambda^{\mathrm{DU}} \tag{2}$$

Further, any one of the four failure rates at right side in (1) and (2) can be divided into two parts again according to normal failure and CCF, thus we obtained all 8-type failure rates. Let the diagnosis coverage rate be c and CCF factor be β, and then λ^{SDC} can be calculated by

$$\lambda^{\mathrm{SDC}} = \beta\lambda^{\mathrm{SD}} = \beta c\lambda^{\mathrm{S}} \tag{3}$$

Similarly, other 7-type failure rates are also easily worked out.

2.3 Discrete Markov model and matrix iteration

Markov process is a special kind of random process, it was first put forward in 1907. Due to the complicated structure of regional interlocking systems, it will bring us a computational complexity to get an analytic result while using Markov model. Therefore, this paper uses the Markov matrix iteration method to solve the security indexes of the system. The solving process is as follows.

The mathematical expression of Markov process is described by

$$\begin{aligned} &P\{X(t_n)=x_n \mid X(t_1)=x_1, X(t_2)\\ &=x_2,\dots,X(t_{n-1})=x_{n-1}\}=P\{X(t_n)\\ &=x_n \mid X(t_{n-1})=x_{n-1}\} \end{aligned} \tag{4}$$

where $X(t_i)=x_i$ expresses that the system is being at state x_i at time t_i.

For a discrete state and continuous time Markov chain, we have

$$\begin{aligned} &P\{X(t+k)=j \mid X(t)=i\}=\\ &P\{X(k)=j \mid X(0)=i\}=P_{i,j}(k) \end{aligned} \tag{5}$$

Substituting k using Δt, then $\boldsymbol{P}(\Delta t)$ can be written by

$$\boldsymbol{P}(\Delta t)=\begin{bmatrix} p_{1,1}(\Delta t) & p_{1,t}(\Delta t) & \dots & p_{1,n}(\Delta t)\\ p_{2,1}(\Delta t) & p_{2.t}(\Delta t) & \dots & p_{2,n}(\Delta t)\\ \dots & & & \\ p_{n,1}(\Delta t) & p_{n,t}(\Delta t) & \dots & p_{n,n}(\Delta t) \end{bmatrix}$$

In the process of calculation, taking the time increment Δt=1h, then the system state transition matrix can be written below.

$$\boldsymbol{P}=\begin{bmatrix} p_{1,1} & p_{1,t} & \dots & p_{1,n}\\ p_{2,1} & p_{2.t} & \dots & p_{2,n}\\ \dots & & & \\ p_{n,1} & p_{n,t} & \dots & p_{n,n} \end{bmatrix}$$

Let the initial state probability of the system be $\mathbf{S}_0$ with the first entry be one, and the remaining elements are zero, and the state transfer probability matrix be $\boldsymbol{P}$, and then according to Markov chain principle, the transient probability after n-step can be calculated by [12].

$$\boldsymbol{S}_n=\boldsymbol{S}_0\boldsymbol{P}^n \tag{6}$$

According to the above formula, each state probability of the system can be calculated out in 8760 hours. The system *PFS* equals the probability sum of all safety states, and the *PFD* equals the probability sum of all dangerous states.

3 Markov Analysis of Three-region RCIS

Three-region RCIS possesses three kinds of different work modes, which are respectively defined as the secondary degradation allowed model (SDAM), primary degradation allowed model (PDAM), and primary degradation not allowed model (PDNAM). From conservative consideration, PDNAM means that the total system will be failure as long as there is one region cell failure due to an undetected failure in there. Different from PDNAM, PDAM expresses that the rest of the cells in system still work normally if there is one cell ceases to work due to an undetected safety failure. On the basis of PDAM, if another sub-region cell then fails, at the moment, only the remaining one sub-region works normally, which is defined as SDAM in three-region RCIS.

3.1 Degradation not allowed Markov model of three-region RCIS.

System model is described below. System consists of three units, which are of same type. If any one of units generates a detected failure, then it is taken over by another units which works normally. For the sake of conservative, in the model of degradation not allowed and degradation allowed, if there is one unit generates a dangerous undetected failure, then the system failure.

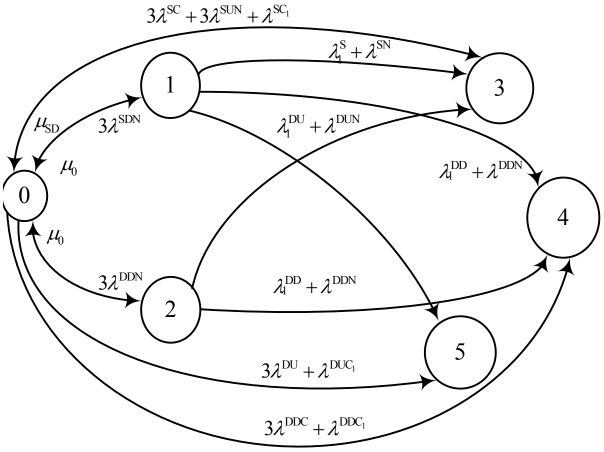

$3\lambda^{SC}+3\lambda^{SUN}+\lambda^{SC_1}$
$\lambda_1^{S}+\lambda^{SN}$
1
3
μ_{SD}
$3\lambda^{SDN}$
$\lambda_1^{DU}+\lambda^{DUN}$
μ_0
$\lambda_1^{DD}+\lambda^{DDN}$
0
4
μ_0
$3\lambda^{DDN}$
$\lambda_1^{DD}+\lambda^{DDN}$
2
5
$3\lambda^{DU}+\lambda^{DUC_1}$
$3\lambda^{DDC}+\lambda^{DDC_1}$

Fig.2 State transition diagram of degradation not allowed Markov model

The Markov model of degradation not allowed is shown in Figure 2. The state 0 expresses the three units are perfect and the system works normally, and the state 1 means that one unit fails and being repaired due to a detected safety failure, at this time, there is one unit overload and the remaining one is at normal state. At this state, one-unit normal failure or two-unit CCF possibly happens. At state 2, one unit generates a dangerous detected failure and being repaired, and one unit overloads and the remaining unit is at normal state. And the state 3 expresses the system safety failure, and the state 4 represents the system dangerous failure but it can be detected out, and the state 5 presents the system dangerous failure but can not be detected out. From the state 0 to the state 2, the system works normally. The parameter μ_0 is online maintenance rate, and $\mu_{\rm SD}$ is a reciprocal of the system restart time after a safety failure occurs.

The state transition matrix ***P*** can be written below.

$$\boldsymbol{P}=\begin{bmatrix} 1-\Sigma & 3\lambda^{\rm SDN} & 3\lambda^{\rm DDN} & 3\lambda^{\rm SC}+3\lambda^{\rm SUN}+\lambda^{\rm SC_1} & 3\lambda^{\rm DDC}+\lambda^{\rm DDC_1} & 3\lambda^{\rm DU}+\lambda^{\rm DUC_1} \\ \mu_0 & 1-\Sigma & 0 & \lambda_1^{\rm S}+\lambda^{\rm SN} & \lambda_1^{\rm DD}+\lambda^{\rm DDN} & \lambda_1^{\rm DU}+\lambda^{\rm DUN} \\ \mu_0 & 0 & 1-\Sigma & \lambda_1^{\rm S}+\lambda^{\rm SN} & \lambda_1^{\rm DD}+\lambda^{\rm DDN} & 0 \\ \mu_{\rm SD} & 0 & 0 & 1-\Sigma & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

3.2 Degradation allowed Markov model of three-region RCIS

Transition matrix ***P*** can be written below.

$$\boldsymbol{P}=\begin{bmatrix} 1-\Sigma & 3\lambda^{\rm SDN} & 3\lambda^{\rm SUN} & 3\lambda^{\rm DDN} & 3\lambda^{\rm SC}+\lambda^{\rm SC_1} & 3\lambda^{\rm DDC}+\lambda^{\rm DDC_1} & 3\lambda^{\rm DU}+\lambda^{\rm DDC_1} \\ \mu_0 & 1-\Sigma & 0 & 0 & \lambda_1^{\rm S}+\lambda^{\rm SN} & \lambda_1^{\rm DD}+\lambda^{\rm DDN} & \lambda_1^{\rm DU}+\lambda^{\rm DUN} \\ 0 & 0 & 1-\Sigma & 0 & \lambda^{\rm SC}+2\lambda^{\rm SN} & \lambda^{\rm DDC}+2\lambda^{\rm DDN} & \lambda^{\rm DUC}+2\lambda^{\rm DUN} \\ \mu_0 & 0 & 0 & 1-\Sigma & \lambda_1^{\rm S}+\lambda^{\rm SN} & \lambda_1^{\rm DD}+\lambda^{\rm DDN} & 0 \\ \mu_{\rm SD} & 0 & 0 & 0 & 1-\Sigma & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

The state transition diagram of three-region RCIS degradation allowed model is shown in Figure 3. System consists of three units, which are of same type. If any one of the three units generates a safety undetected failure, it is called a degradation working condition.

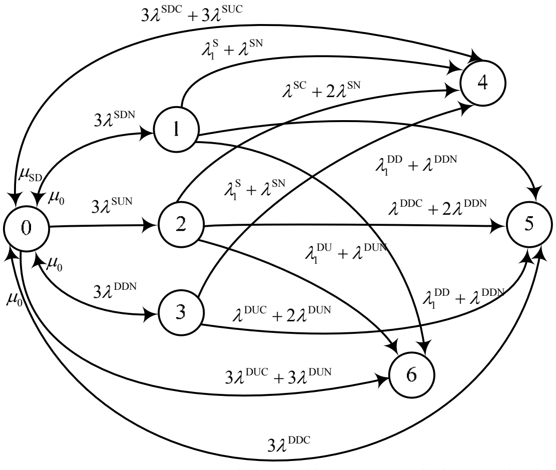

$3\lambda^{\rm SDC}+3\lambda^{\rm SUC}$
$\lambda_1^{\rm S}+\lambda^{\rm SN}$
$\lambda^{\rm SC}+2\lambda^{\rm SN}$
$3\lambda^{\rm SDN}$
$\mu_{\rm SD}$
μ_0
$\lambda_1^{\rm DD}+\lambda^{\rm DDN}$
$\lambda_1^{\rm S}+\lambda^{\rm SN}$
$3\lambda^{\rm SUN}$
$\lambda^{\rm DDC}+2\lambda^{\rm DDN}$
$\lambda_1^{\rm DU}+\lambda^{\rm DUN}$
μ_0
$3\lambda^{\rm DDN}$
$\lambda_1^{\rm DD}+\lambda^{\rm DDN}$
μ_0
$\lambda^{\rm DUC}+2\lambda^{\rm DUN}$
$3\lambda^{\rm DUC}+3\lambda^{\rm DUN}$
$3\lambda^{\rm DDC}$
0
1
2
3
4
5
6

Fig.3 State transition diagram of degradation allowed Markov model

3.3 Secondary degradation allowed Markov model of three-region RCIS

As shown in Figure 4, the descriptions on the state 0, and 1, and 2 are the same as degradation allowed model of three-region RCIS. In these states the system works normally. The state 3 expresses one cell generates a safety undetected failure. The state 6 expresses one cell generates a safety undetected failure, and one cell generates a safety detected failure. The state 7 expresses one cell generates a safety undetected failure, and one cell generates a dangerous detected failure. The state 3, and 6, and 7 represent the system primary degradation working state. The state 4 expresses two cell generate undetected safety failure. The state 10 represents the system safety failure. The state 11 presents the system dangerous failure but can be detected. The state 12 expresses the system dangerous failure but can not be detected out. The state 10, and 11, and 12 present the system failure states. As system works at state 3, and 6, and 7 there are two sub-regions working normally. As system being at state 4 only one sub-region normally works. The state 5 expresses one cell generates a safety detected failure, and one cell generates a dangerous detected failure. The state 8 expresses two cells find safety detected failure. The state 9 expresses two cells find dangerous detected failure. As the system being at state 5, and 8, and 9, the system finds two detected failures, and in these states, the system only has one cell working that completes the interlocking logical operation of the entire area. In this case the working principle of the system is equivalent to the centralized interlocking scheme.

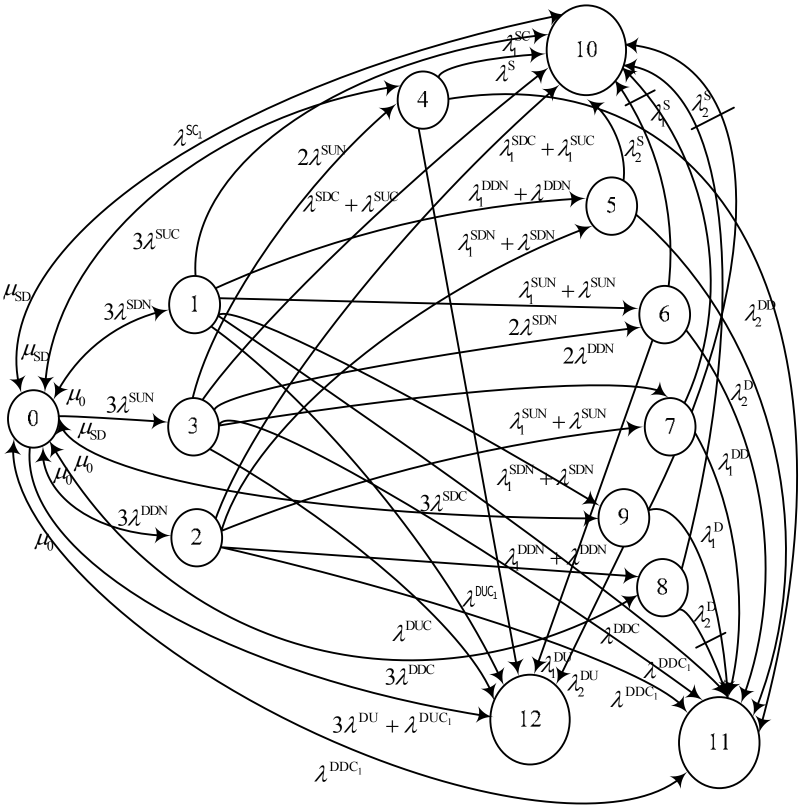


Fig.4 State transition diagram of secondary degradation allowed Markov model

4 DFT Analysis of Three-region RCIS

In the process of modeling, we introduce the following two logic gates. As shown in Figure 5. In or gate, there are three impute events, namely, X_1, X_2, X_3, respectively. At least one of the three occurs, the output Y then occurs. In the priority gate, there are two impute events, X and Y. The two events from left to right occur in turn, the output Z occurs.

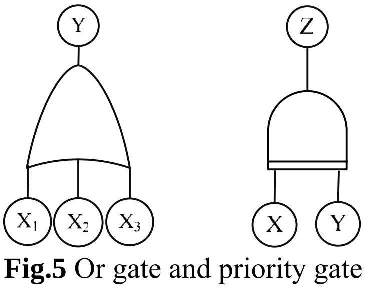


Fig.5 Or gate and priority gate

4.1 Three-region RCIS PFD fault tree

System consists of three units, which are of same type. If two units failure, the system then generates dangerous failure. Through analysis the following conditions may lead to dangerous failure of degradation not allowed model.

(1) From conservative consideration, the system is considered to be dangerous failure as long as there is a unit that generates an undetected dangerous failure.

(2) After a unit generates a safety detected failure, one of the other two units generates a dangerous failure or the remaining two units generate dangerous common cause failure.

(3) After a unit generates a dangerous detected failure, one of the other two units generates a dangerous failure or the remaining two units generate dangerous common cause failure.

(4) Dangerous CCF of two units, including dangerous detected common cause failure and dangerous undetected common cause failure.

As to the degradation allowed model, besides the above conditions, there is another condition that may lead to system dangerous failure. Namely, After a unit generates a safety undetected failure, one of the other two units generates a dangerous failure or the remaining two units generate dangerous common cause failure.

For convenience comparison, we drew the *PFD* fault tree of degradation not allowed and degradation allowed in the same Figure. *PFD* fault tree of three-region RCIS degradation allowed as shown in Figure 6. After removing the sub-tree of "SUN failure", the remaining fault tree is the *PFD* fault tree of three-region RCIS degradation not allowed.

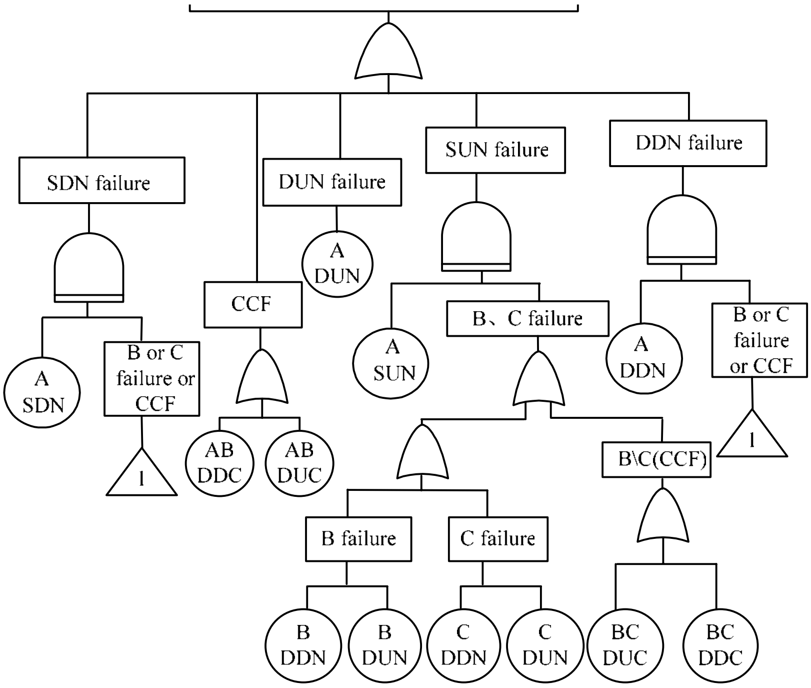


Fig.6 *PFD* fault tree of degradation allowed and degradation not allowed

In Figure 6, module 1 is shown in Figure 7.

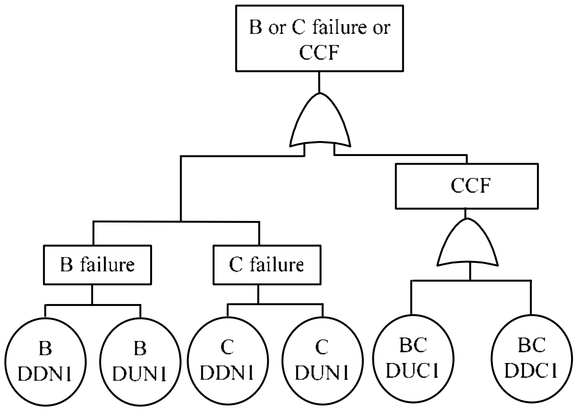


Fig. 7 Fault tree of B or C failure or CCF

As to the degradation not allowed model, the first-order approximate calculation formula of the dangerous failure probability is:

$$\begin{aligned}PFD_1 &= 3\lambda^{\mathrm{DDC}}\times T_{\mathrm{R}} + 3\lambda^{\mathrm{DUC}}\times T + 3\lambda^{\mathrm{DUN}}\times T \\ &+6\{[(\lambda^{\mathrm{SDN}}\times T_{\mathrm{R}})\times(\lambda^{\mathrm{DDN_1}}\times T_{\mathrm{R}} + \lambda^{\mathrm{DUN_1}}\times T + \\ &\lambda^{\mathrm{DDC_1}}\times T_{\mathrm{R}} + \lambda^{\mathrm{DUC_1}}\times T)] + [(\lambda^{\mathrm{DDN}}\times T_{\mathrm{R}})\times(\lambda^{\mathrm{DDN_1}} \\ &\times T_{\mathrm{R}} + \lambda^{\mathrm{DUN_1}}\times T + \lambda^{\mathrm{DDC_1}}\times T_{\mathrm{R}} + \lambda^{\mathrm{DUC_1}}\times T)]\}\end{aligned} \tag{7}$$

As to degradation allowed model, the first-order approximate calculation formula of the dangerous failure probability is:

$$\begin{aligned}&PFD_2 = 3\lambda^{\mathrm{DDC}} \times T_R + 3\lambda^{\mathrm{DUC}} \times T + 3\lambda^{\mathrm{DUN}} \times T\\ &+6\{[(\lambda^{\mathrm{SDN}} \times T_{\mathrm{R}}) \times (\lambda^{\mathrm{DDN_1}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUN_1}} \times T + \lambda^{\mathrm{DDC_1}}\\ &\times T_{\mathrm{R}} + \lambda^{\mathrm{DUC_1}} \times T)] + [(\lambda^{\mathrm{DDN}} \times T_{\mathrm{R}}) \times (\lambda^{\mathrm{DDN_1}} \times T_{\mathrm{R}} +\\ &\lambda^{\mathrm{DUN_1}} \times T + \lambda^{\mathrm{DDC_1}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUC_1}} \times T)] + [(\lambda^{\mathrm{SUN}} \times T_{\mathrm{R}})\\ &\times(\lambda^{\mathrm{DDN}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUN}} \times T + \lambda^{\mathrm{DDC}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUC}} \times T)]\}\end{aligned} \tag{8}$$

System consists of three units, which are of same type. Through analysis the following conditions may lead to dangerous failure of secondary degradation allowed model.

(1) From conservative consideration, the system is considered to be failure as long as there is a unit that generates a dangerous undetected failure.

(2) After a unit generates a safety detected failure, the remaining two units are both failure.

(3) After a unit generates a dangerous detected failure, the remaining two units are both failure.

(4) After a unit generates a safety undetected failure, the remaining two units are both failure.

(5) Dangerous CCF of two units, including dangerous detected common cause failure and dangerous undetected common cause failure.

(6) Dangerous CCF of three units, including dangerous detected common cause failure and dangerous undetected common cause failure.

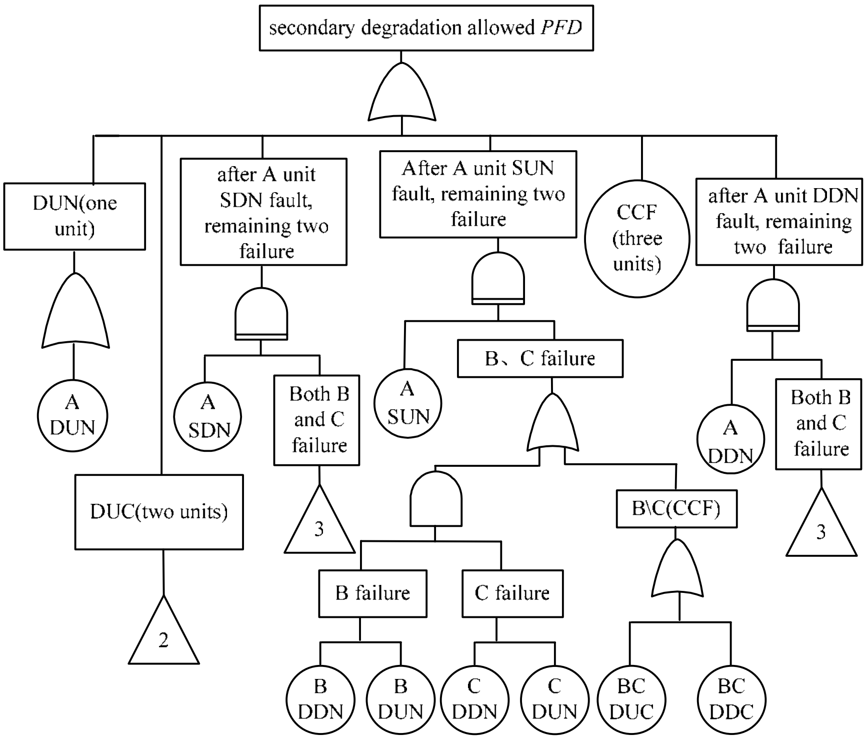


Fig.8 *PFD* fault tree of secondary degradation allowed

The *PFD* fault tree of three-region RCIS secondary degradation allowed as shown in Figure 8, module 2 in Figure 8 as shown in Figure 9, module 3 in Figure 8 as shown in Figure 10. The first-order approximate calculation formula of the dangerous failure probability is:

$$\begin{aligned}&PFD_3 = 3\lambda^{\mathrm{DUN}} \times T + 3\lambda^{\mathrm{DUC}} \times T + \lambda^{\mathrm{DC_2}} \times T\\ &+6\{(\lambda^{\mathrm{SUN}} \times T_{\mathrm{R}} \times (\lambda^{\mathrm{DDN}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUN}} \times T\\ &+\lambda^{\mathrm{DDC}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUC}} \times T) + 6\{(\lambda^{\mathrm{SDN}} \times T_{\mathrm{R}}\\ &\times(\lambda^{\mathrm{DDN_1}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUN_1}} \times T + \lambda^{\mathrm{DDC_1}} \times T_{\mathrm{R}}\\ &+\lambda^{\mathrm{DUC_1}} \times T) + 6(\lambda^{\mathrm{DDN}} \times T_{\mathrm{R}} \times (\lambda^{\mathrm{DDN_1}} \times T_{\mathrm{R}}\\ &+\lambda^{\mathrm{DUN_1}} \times T + \lambda^{\mathrm{DDC_1}} \times T_{\mathrm{R}} + \lambda^{\mathrm{DUC_1}} \times T)\}\end{aligned} \tag{9}$$

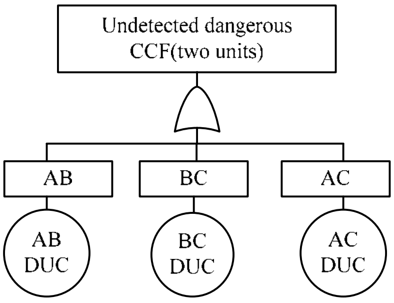


Fig. 9 Fault tree of undetected dangerous (two units)

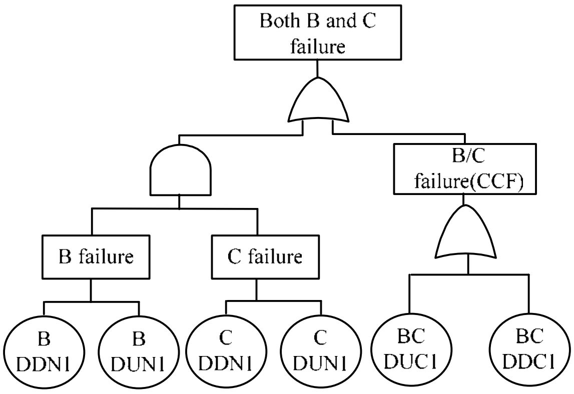


Fig. 10 Fault tree of both B and C failure

4.2 Three-region RCIS *PFS* fault tree

Through analysis the following conditions may lead to safety failure of degradation not allowed model.

(1) From conservative consideration, the system is considered to be safety failure as long as there is a unit that generates an undetected safety failure.

(2) Safety CCF of two units, including safety detected common cause failure and safety undetected common cause failure.

(3) After a unit generates a safety detected failure, one of the other two units generates a safety failure or the remaining two units generate the safety common cause failure.

(4) After a unit generates a dangerous detected failure, one of the other two units generates a safety failure or the remaining two units generate the safety common cause failure.

The degradation not allowed *PFS* fault tree model is shown in Figure 11.

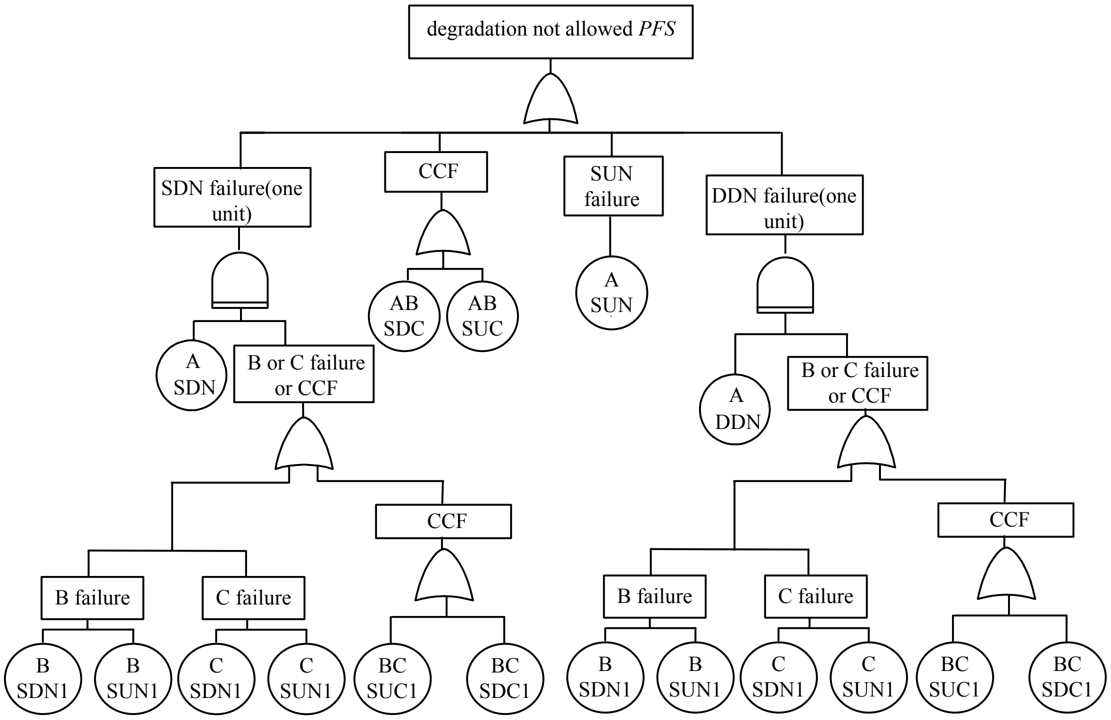


Fig.11 *PFS* fault tree of degradation not allowed

As to the degradation not allowed model, the first-order approximate calculation formula of the safety failure probability is

$$\begin{aligned}&PFS_1 = 3(\lambda^{\mathrm{SDC}} + \lambda^{\mathrm{SUC}}) \times \mathrm{SD} + 3\lambda^{\mathrm{SUN}} \times T \\ &+6\{(\lambda^{\mathrm{SDN}} \times T_{\mathrm{R}} \times (\lambda^{\mathrm{SDN_1}} \times T_{\mathrm{R}} + \lambda^{\mathrm{SUN_1}} \times T \\ &+\lambda^{\mathrm{SC_1}} \times \mathrm{SD}) + (\lambda^{\mathrm{DDN}} \times T_{\mathrm{R}} \times (\lambda^{\mathrm{SDN_1}} \times T_{\mathrm{R}} \\ &+\lambda^{\mathrm{SUN_1}} \times T + \lambda^{\mathrm{SC_1}} \times \mathrm{SD})\}\end{aligned} \tag{10}$$

As to the degradation allowed model, the following conditions may lead to system safety failure.

(1) Safety CCF of two units, including safety detected common cause failure and safety undetected common cause failure.

(2) After a unit generates a safety detected failure, one of the other two units generates a safety failure or the remaining two units generate the safety common cause failure.

(3) After a unit generates a dangerous detected

failure, one of the other two units generates a safety failure or the remaining two units generate the safety common cause failure.

(4) After a unit generates a safety undetected failure, one of the other two units generates a safety failure or the remaining two units generate the safety common cause failure.

The *PFS* fault tree of degradation allowed is shown in Figure 12.

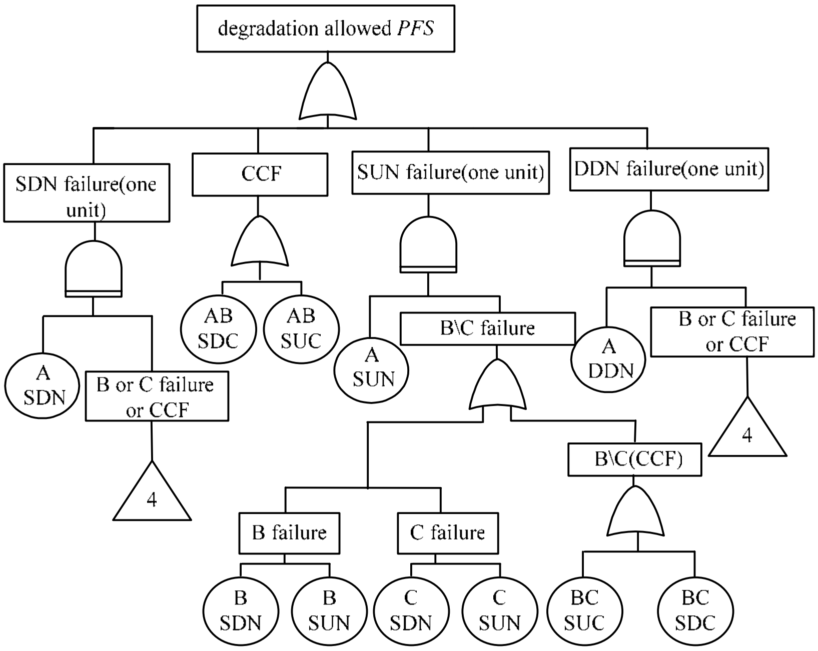


Fig.12 *PFS* fault tree of degradation allowed

As to the degradation allowed model, the first-order approximate calculation formula of the safety failure probability is:

$$
\begin{aligned}
&PFS_2 = 3(\lambda^{\mathrm{SDC}} + \lambda^{\mathrm{SUC}}) \times \mathrm{SD} \\
&+6\{[(\lambda^{\mathrm{SDN}} \times T_{\mathrm{R}}) \times (\lambda^{\mathrm{SDN_1}} \times T_{\mathrm{R}} + \lambda^{\mathrm{SUN_1}} \times T \\
&+\lambda^{\mathrm{SC_1}} \times \mathrm{SD})] + [(\lambda^{\mathrm{DDN}} \times T_{\mathrm{R}}) \times (\lambda^{\mathrm{SDN_1}} \times T_{\mathrm{R}} \\
&+\lambda^{\mathrm{SUN_1}} \times T + \lambda^{\mathrm{SC_1}} \times \mathrm{SD})] + [(\lambda^{\mathrm{SUN}} \times T_{\mathrm{R}} \\
&\times(\lambda^{\mathrm{SDN}} \times T_{\mathrm{R}} + \lambda^{\mathrm{SUN}} \times T + \lambda^{\mathrm{SC}} \times \mathrm{SD})]\}
\end{aligned} \qquad (11)
$$

As shown in Figure 12, module 4 is shown in Figure 13.

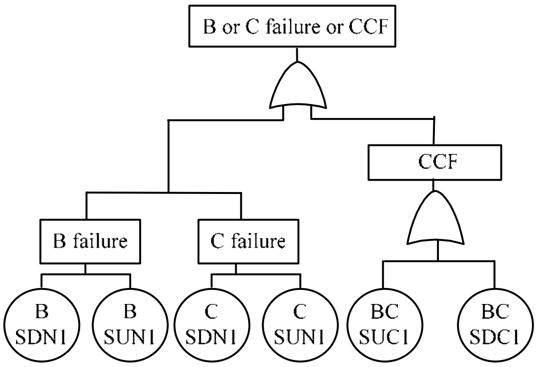


Fig.13 Fault tree of both B and C failure

As to secondary degradation allowed model. Through analysis the following conditions may lead to system safety failure.

(1) After a unit generates a safety detected failure, the remaining two units are both failure.

(2) After a unit generates a dangerous detected failure, the remaining two units are both failure.

(3) After a unit generates a safety undetected failure, the remaining two units are both failure.

(4) Dangerous CCF of three units, including dangerous detected common cause failure and dangerous undetected common cause failure.

According to the above analysis, the *PFS* fault tree of secondary degradation allowed as shown in Figure 14. In Figure 14, module 5 is shown in Figure 15.

The first-order approximate calculation formula of the safety failure probability is:

$$
\begin{aligned}
&PFS_3 = \lambda^{\mathrm{SC_2}} \times \mathrm{SD} + 6\{[\lambda^{\mathrm{SUN}} \times T_{\mathrm{R}} \\
&\times(\lambda^{\mathrm{SDN}} \times T_{\mathrm{R}} + \lambda^{\mathrm{SUN}} \times T + \lambda^{\mathrm{SC}} \times \mathrm{SD})] \\
&+[\lambda^{\mathrm{SDN}} \times T_{\mathrm{R}} \times (\lambda^{\mathrm{SDN_1}} \times T_{\mathrm{R}} + \lambda^{\mathrm{SUN_1}} \times T \\
&+\lambda^{\mathrm{SC_1}} \times \mathrm{SD})] + [\lambda^{\mathrm{DDN}} \times T_{\mathrm{R}} \times (\lambda^{\mathrm{SDN_1}} \\
&\times T_{\mathrm{R}} + \lambda^{\mathrm{SUN_1}} \times T + \lambda^{\mathrm{SC_1}} \times \mathrm{SD}]\}
\end{aligned} \qquad (12)
$$

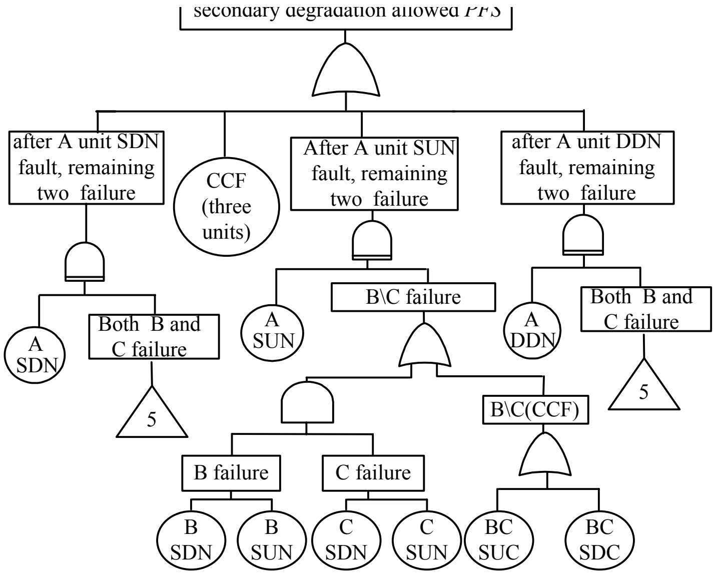

secondary degradation allowed PFS
after A unit SDN fault, remaining two failure
CCF (three units)
After A unit SUN fault, remaining two failure
after A unit DDN fault, remaining two failure
A SDN
Both B and C failure
5
A SUN
B\C failure
A DDN
Both B and C failure
5
B\C(CCF)
B failure
C failure
B SDN
B SUN
C SDN
C SUN
BC SUC
BC SDC

Fig.14 *PFS* fault tree of secondary degradation allowed

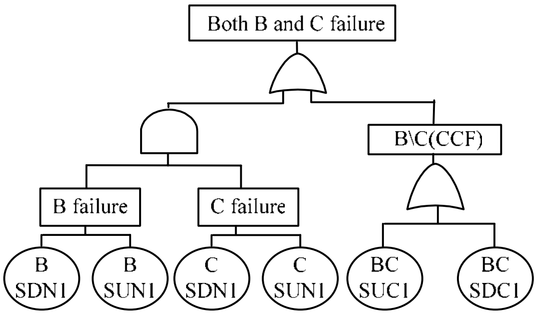


Fig.15 Fault tree of both B and C failure

5 Example

To depict the advantages and disadvantages of the two kinds of methods, from the view of system redundancy we implement the comparison for them. In the proposed RCIS, the diverse redundancies such as dual hot spare, 3-vote-2 voting, double 2-vote-2 voting, and single machine are considered. The calculation method of system failure rates with diverse redundancies refers to [13].

The simulation parameters are as follows. The failure rate of single interlocking cell is expressed by λ=1.0×10^{-5}h^{-1}, and the failure rate of interlocking machine after taking over one region increases to λ_1=1.11×10^{-5} h^{-1}, and the failure rate of interlocking machine after taking over two regions soars to λ_2=1.22×10^{-5} h^{-1}. The diagnostic coverage rate is expressed by c=0.999, and the CCF factor β_1 of the two cells is 0.075, and the CCF factor β_2 of the three cells is 0.025. The average repairing time is considered as 8 hour, and so the repairing rate is expressed by μ_0=0.125h^{-1}. Assume that the system shuts down if it detects a safety failure, it could then restart within 24 hours, and thus μ_{SD}=1/24h^{-1} [14].

Table. 1 Two methods comparison in *PFS* index

System structure of three-RCIS		DFT	Markov
Three-region	Single module	2.809332×10^{-7}	2.807799×10^{-7}
RCIS	Dual hot spare	4.49143444×10^{-11}	4.49143405×10^{-11}
PDNAM	3-vote-2 voting	1.347215×10^{-10}	1.347214×10^{-10}
	Double 2-vote-2	8.982869×10^{-11}	8.982868×10^{-11}
Three-region	Single module	2.809333×10^{-7}	2.807696×10^{-7}
RCIS	Dual hot spare	4.4914344×10^{-11}	4.4914341×10^{-11}
PDAM	3-vote-2 voting	1.347215×10^{-10}	1.347214×10^{-10}
	Double 2-vote-2	8.982869×10^{-11}	8.982868×10^{-11}
Three-region	Single module	2.648000×10^{-7}	2.472502×10^{-7}
RCIS	Dual hot spare	4.235783×10^{-11}	3.955495×10^{-11}
SDAM	3-vote-2 voting	1.270532×10^{-10}	1.186460×10^{-10}
	Double 2-vote-2	8.471567×10^{-11}	7.910997×10^{-11}

Table. 2 Two methods comparison in *PFD* index

System structure of three-RCIS		DFT	Markov
Three-region	Single module	5.476507×10^{-5}	5.470439×10^{-5}
RCIS	Dual hot spare	8.735720×10^{-9}	8.735719×10^{-9}
PDNAM	3-vote-2 voting	2.620299×10^{-8}	2.620298×10^{-8}
	Double 2-vote-2	1.7471449×10^{-8}	1.7471443×10^{-8}
Three-region	Single module	5.409988×10^{-5}	5.413007×10^{-5}
RCIS	Dual hot spare	8.629293×10^{-9}	8.629294×10^{-9}
PDAM	3-vote-2 voting	2.588376×10^{-8}	2.588377×10^{-8}
	Double 2-vote-2	1.725859×10^{-8}	1.725860×10^{-8}
Three-region	Single module	5.994012×10^{-6}	5.995995×10^{-6}
RCIS	Dual hot spare	9.5880988×10^{-10}	9.5880981×10^{-10}
SDAM	3-vote-2 voting	2.875970×10^{-9}	2.875968×10^{-9}
	Double 2-vote-2	1.9176197×10^{-9}	1.9176194×10^{-9}

Table 1 and Table 2 show the computational results on *PFS* and *PFD* indexes between Markov and DFT. Clearly, the results almost are fully consistent. However, DFT method is quit simple, and Markov is comples, relatively.

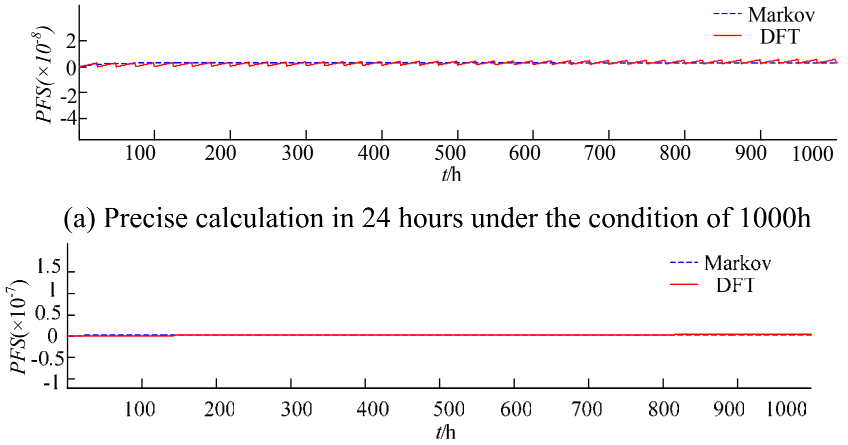
6 Comparison Between Markov and DFT Method

According to the former case, we know that the indexes of DFT are very close to that of Markov process. This shows that, to a certain extent, the two methods can simulate each other. In the following, we will discuss the conditions using DFT to simulate Markov method. As a case, we choose double 2-vote-2 redundant structure of three-region RCIS. Simulated conditions are as follows, respectively.

(1) Periodic maintenance time T=8760h, system restart time SD=24h, average repairing time T_R=8h, system running time T=10000h.

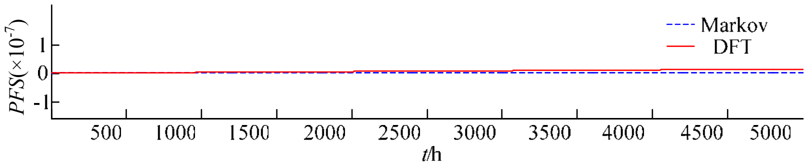
(2) Periodic maintenance time T=8760h, integral averaging in every 24 hours, average repairing time T_R=8h , system running time T=10000h.

(3) Periodic maintenance time T=8760h, integral averaging in every 24 hours, average repairing time T_R=8h , system running time T=10000h.



(a) Precise calculation in 24 hours under the condition of 1000h

(b) Integral averaging in every 24 hours under the condition of 1000h



(c) Integral averaging in every 24 hours under the condition of 5000h

Fig.16 Comparison between Markov and DFT method

Obviously, the results of the two methods are very close. To show the distinction clearly, Corresponding to the simulation conditions (1), (2), and (3), respectively, we selected part of local simulation curve. And so simulation curves are obtained, as shown in Figure 16(a), Figure 16(b) and Figure 16(c).

As can be seen from Figure 16(a), the simulation curve of DFT appear jagged. Through integral averaging in every 24 hours, thus obtained smooth curves, as shown in Figure 16(b) and Figure 16(c). Comparing Figure 16(b) with Figure 16(c), we can see that along with the growth of the time, values of the fault tree and Markov separate gradually, and the difference becomes bigger and bigger. This illustrated that using the fault tree to simulate Markov process, only effective within a certain amount of time. Since the numerical values obtained from the fault tree generally present the linear growth trend, we generally can not compare the two methods when system in steady state. Since computer interlocking system is the system with high reliability and security, in many cases we are only concern its transient behavior, it has not much significance to solve its steady state index. Therefore, we can replace Markov with DFT only in calculating the related transient index of the regional computer interlocking system. It is worth noting that probabilistic approximation method is just suitable for those systems which possess low failure rate and short maintenance time. Only in this time it possesses sense that we calculate system safety indexes. And so, DFT method is not be applied to solve system steady state indexes. Whereas the Markov method is not only suitable for the transient states, but also the steady state.

7 Conclusion

This paper makes use of the Markov and DFT method to analyses the safety of the RCIS, respectively. A comparison on RCIS safety indexes is then conducted between Markov and DFT methods, and the results show that the ones of the two methods are very close. In addition, DFT method reduces the modeling and computational complexity, and meets the requirement of real-time, better, this provides a new way for the complex dynamic redundancy system security analysis.

References:

[1] B. Liu, Analysis of application and implementation on the regional computer interlocking signal, TDCS, and the computer monitoring system, *Journal of Science and Technology and economy of Inner Mongolia*, No.13, 2008, pp.108-109.

[2] S. J. Wang, H. Guo, Y. T. Wang. Research of CTC based on regional computer interlocking, *Journal of the China Railway Society*, Vol.32, No.4, 2010, pp.130-133.

[3] Dobias R., Kubatova H., FPGA based design of the railway's interlocking equipment, *IEEE*, 2004, pp.467-473.

[4] Xinhong Hei, Takahashi S., Nakamura H.,Distributed interlocking system and its safety verification, *IEEE*, 2006, pp.8612-8615.

[5] P. Gao, Introduction of regional computer interlocking system and its practical application in domestic conditions, *Journal of Information Science and Technology*, No.6, 2009, pp.191-192.

[6] W. Z. Huang, The realization and implementation of regional computer interlocking system, *Railway Signaling and Communication*, Vol.41, No.9, 2005, pp.6-10.

[7] M. Hou, L. Bai, The design and implementation of Jiben regional computer interlocking communication, *Journal of Railway Signal Engineering*, Vol.3, No.1, 2006, pp.36-39.

[8] Y. L. Zhou, Study on computer interlocking

system of railway passenger dedicated line, *Journal of Railway Transportation and Economy*, Vol.30, No.3, 2008, pp.45-46.

[9] Y. F. He, Regional computer interlocking system of one station and two line location, *Journal of Railway Communication Signals*, Vol.40, No.1, 2004, pp.27-28.

[10] H. W. Chen, Technology and maintenance on regional computer interlocking system of DS6-K5B, *Railway Engineering*, Vol.24, No.61, 2005, pp.33-35.

[11] H. S. Su, J. Wen, Research on regional computer interlocking system safety analysis based on dynamic fault tree method, *Journal of the china railway society*, Vol.5, No.3, 2015, pp.46-53.

[12] W. M. Goble, *Control Systems Safety Evaluation and Reliability*, China Electric Power Publishing House, 2010.

[13] J. Yang, Study on subway main control system reliability evaluation method based on FTA, *Master thesis of Southwest Jiao Tong University*, 2009.

[14] Z. X. Zhao, *Computer Interlocking System Technology*, China Railway Publishing House, 2010.