Modeling and Simulation for Safety Redundant Architecture in Train Control System

Hongjie Liu[1,2,a], Bing Ning[1,2,b], Tao Tang[1,c] and Yu Mu[3,d]

[1]State Key Lab of Rail Traffic Control & Safety, Beijing Jiaotong University, Beijing, 100044, China

[2]National Engineering Research Center of Rail Transportation Operation & Control System, Beijing Jiaotong University, Beijing, 100044, China

[3]101 Institute of the Ministry of Civil Affairs, Beijing, 100044, China

[a]hjliu2@bjtu.edu.cn, [b]bning@bjtu.edu.cn, [c]ttang@bjtu.edu.cn, [d]11111045@bjtu.edu.cn

Keywords: train control system, Markov model, safety redundant architecture

Abstract. It is an effective way to enhance the safety of train control system by using safety redundant architectures. This paper consider the typical safety redundant architectures, including double hot standby, 2-out-of-2, 2*2-out-of-2, and 2-out-of-3, establishes models for these architectures by Markov chain. Then the safety of different architectures are simulated using Matlab. The simulation results can provide a certain reference when choosing redundant architectures in real engineering.

1. Introduction

As a safety-critical system, train control system should satisfy the requirements of high safety. It usually enhances the system safety by using redundant architectures. There have been already research on application of k-out-of-n safety redundant architecture in computer platform [1]. For redundant architecture, most researches are focused on reliability and availability [2-5], and a common method of analysis is Markov chain. However, there is seldom research on safety of redundant architectures, especially in train control system. Therefore, this paper establishes models of some typical safety redundant architectures with Markov chain.

This paper is organized as follows. Firstly, the typical safety redundant architectures are description briefly; Secondly, models of the different redundant architectures are established, and safety of these architectures are simulated and analyzed. Finally, some conclusions are drawn.

2. Safety redundant architecture

2.1. Double hot standby

It consists of 2 computation modules and 1 switcher, as shown in Fig. 1. Both computation modules works, but the switcher only chooses the results of the master computation module as output. When a fault is detected on the master computation module, the results of the hot standby module will be as output. The system works in single mode as 1 computation module is resected.

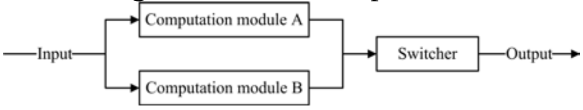

Fig. 1 Double hot standby

2.2. 2-out-of-2

It consists of 2 computation modules and 1 comparator, as shown in Fig. 2. Both computation modules works. The comparator executes 2-out-2 logical vote. If the results of the 2 computation modules are different, the output of the system will be oriented to fail-safe side.

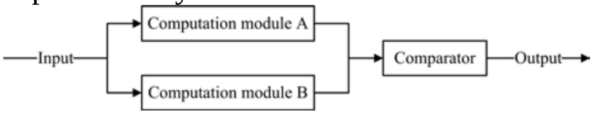

Fig. 2 2-out-of-2

2.3. 2*2-out-of-2

It consists of 4 computation modules, 2 comparators and 1 switcher, as shown in Fig. 3. There are 2 sets of hot standby. In each set there are 2 computation modules and 1 comparator, considered as 2-out-of-2. If failure happens on one computation module in one set, the whole set will have to be repaired, and the system switches to the other set, working in 2-out-of-2 working mode.

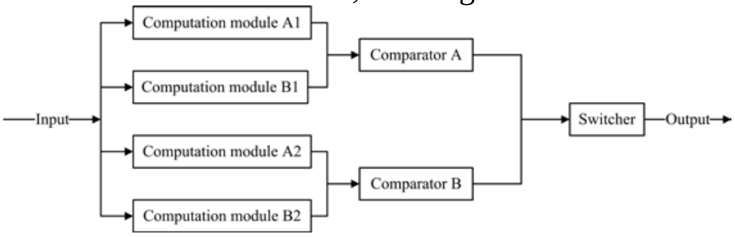

Fig. 3 2*2-out-of-2

2.4. 2-out-of-3

It consists of 3 independent computation modules and 1 comparator, as shown in Fig. 4. If failure happens on one computation module, the system will downgrade to 2-out-of-2 working mode. The whole system will not fail unless there are 2 or more failure computation modules.

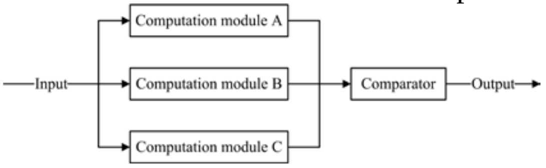

Fig. 4 2-out-of-3

3. Safety analysis of the different safety redundant architectures with Markov chain

Safety is defined as: the ability of the system to achieve required safety function in certain time and conditions, Fault is the direct reason to affect the safety. For the fault which could be detected, the system will make corresponding measures to be oriented to fail-safe side, and only the undetected fault will affect the safety of system, we assume that:

(1) The fault which could not be detected will orient the system to danger state;

(2) Once the system is in danger state, no other fault or repair is considered.

According to the definition of Markov process, Eq. 1 could describe the relationship between different states of the system:

$$\begin{aligned}
&P'(t) = P(t)D \\
&P(t) = [P_0(t), P_1(t)....P_N(t)] \\
&P_j(t) = 1; \mathrm{j} = 0; \\
&P_{\mathrm{j}}(t) = 0; \mathrm{j} = 1, 2...\mathrm{N};
\end{aligned} \qquad (1)$$

Where, $P_j(t)$ is the probability that the system is in state j at time t, j is the number of state space, and D is the state transition density matrix.

Set c as the probability that fault could be detected, the Markov model of state transition diagram for double hot standby, 2-out-of-2, 2*2-out-of-2, and 2-out-of-3 are shown in Fig. 5 ~ Fig. 8.

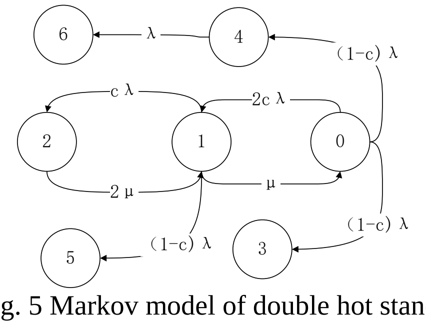

Fig. 5 Markov model of double hot standby

In Fig. 5, the meanings of each state are as follows:

State 0: the 2 units work, the system works, safe;

State 1: 1 unit is with detected fault, the system works in single mode, safe;

State 2: 2 units are with detected fault, the system is downtime, safe;
State 3: the master unit is with undetected fault, danger;
State 4: the standby unit is with undetected fault, safe;
State 5: 1 unit is with detected fault, and 1 unit is with undetected fault, danger;
State 6: the standby unit is with undetected fault, and the master unit is with detected fault, danger.

According to Fig. 5, state transition density matrix and safety of double hot standby are:

$$\mathrm{D_{hs}} = \begin{bmatrix} -2\lambda & \mu & 0 & 0 & 0 & 0 & 0 \\ 2c\lambda & -\lambda-\mu & 2\mu & 0 & 0 & 0 & 0 \\ 0 & c\lambda & -2\mu & 0 & 0 & 0 & 0 \\ (1-c)\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ (1-c)\lambda & 0 & 0 & 0 & -\lambda & 0 & 0 \\ 0 & (1-c)\lambda & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda & 0 & 0 \end{bmatrix} \quad (2)$$

$$S_{hs}(t) = P_0(t) + P_1(t) + P_2(t) + P_4(t)$$

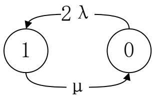

Fig. 6 Markov model of 2-out-of-2

In Fig. 6, the meanings of each state are as follows:
State 0: the 2 units work, the system works, safe;
State 1: 1 unit is failure, the system is downtime, danger.

According to Fig. 6, state transition density matrix and the safety of 2-out-of-2 are:

$$D_{2oo2} = \begin{bmatrix} -2\lambda & \mu \\ 2\lambda & -\mu \end{bmatrix} \quad (3)$$

$$S_{2oo2}(t) = P_0(t) + P_1(t) = 1$$

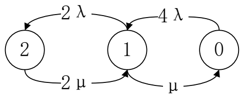

Fig. 7 Markov model of 2*2-out-of-2

In Fig. 7, the meanings of each state are as follows:
State 0: the 4 units work, the system works, safe;
State 1: 1 unit is failure, the system works in 2-out-of-2 mode, safe;
State 2: 2 units are failure, the system is downtime, danger.

According to Fig. 7, state transition density matrix and the safety of 2*2-out-of-2 are:

$$D_{2*2oo2} = \begin{bmatrix} -4\lambda & \mu & 0 \\ 4\lambda & -2\lambda-\mu & 2\mu \\ 0 & 2\lambda & -2\mu \end{bmatrix} \quad (4)$$

$$S_{2*2oo2}(t) = P_0(t) + P_1(t) + P_2(t) = 1$$

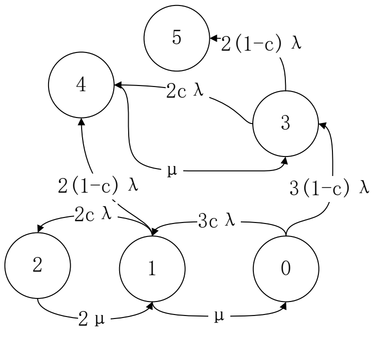

Fig. 8 Markov model of 2-out-of-3

In Fig. 8, the meanings of each state are as follows:
State 0: the 3 units work, the system works, safe;
State 1: 1 unit is with detected fault, the system works in 2-out-of-2 mode, safe;
State 2: 2 units are with detected fault, the system is downtime, safe;
State 3: 1 unit is with undetected fault, safe;

State 4: 1 unit is with undetected fault, 1 unit is with detected fault, the system is downtime, safe;
State 5: 2 units are with undetected fault, danger;

According to Fig. 8, state transition density matrix and the safety of 2-out-of-3 are:

$$D_{2oo3} = \begin{bmatrix} -3\lambda & \mu & 0 & 0 & 0 & 0 \\ 3c\lambda & -2\lambda-\mu & 2\mu & 0 & 0 & 0 \\ 0 & 2c\lambda & -2\mu & 0 & 0 & 0 \\ 3(1-c)\lambda & 0 & 0 & -2\lambda & \mu & 0 \\ 0 & 2(1-c)\lambda & 0 & 2c\lambda & -\mu & 0 \\ 0 & 0 & 0 & 2(1-c)\lambda & 0 & 0 \end{bmatrix} \tag{5}$$

$$S_{2oo3}(t) = P_0(t) + P_1(t) + P_2(t) + P_3(t) + P_4(t)$$

According to the above parameters, assuming *c*, the probability that fault could be detected is 0.95, the simulation results of safety of each redundant architectures are shown in Fig. 9.

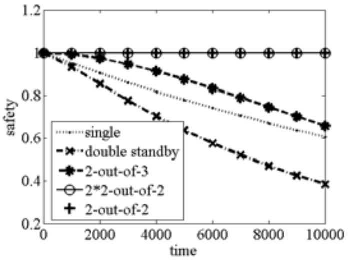

Fig. 9 Comparison of safety of different redundant architecture

It could be concluded that, the safety of 2-out-of-2 and 2*2-out-of-2 are the best, 2-out-of-3, single, double hot standby declines in turn, and decreases with simulation time.

4. Conclusion

Safety is one of the most important factors in train control system. Through comparison, 2-out-of-2 and 2*2-out-of-2 with a reasonable configuration, such as the probability that fault could be detected, will greatly improve the safety of the system, double hot standby has the lowest safety. However, 2-out-of-2 and 2*2-out-of-2 mean an increasing cost. Economizing on energy and reducing cost will become problems in our further research.

Acknowledgements

This work was financially supported by National Natural Science Foundation (O15A200011), National Basic Research Program of China (KWB114006534) and Railway Safety innovation (I15Y00010).

References

[1] Asadi M B I. The mean residual life function of a k-out-of-n structure at the system level. IEEE Transactions on Reliability, 2006, 55(2): 314-318

[2] Xu Chong. Reliability and safety of 2*2-out-of-2 system. Hefei Technology University, Hefei, 2013.

[3] Wang Yan. Reliability and availability of computer platform of railway transportation. Urban railway transportation, 2011, 4.

[4] Wu Xiaochun. Comparison of performance between dual-mode redundant-comparison system and three-mode redundant system. Automation and instrumentation, 2012.

[5] Wang Lihua. Analysis of reliability and safety of repairable three-mode redundant architecture. Journal of southwest jiaotong university, 2002