Reliability analysis and testing methods of the CTCS-3 train control system with DFTA in a simulation environment

W. ShangGuan[1,2,3], J. Xiao[1], B. Cai[1], B. Heydecker[3] & J. Wang[1,2]
[1]*School of Electronics and Information Engineering, Beijing Jiaotong University, China*
[2]*State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, China*
[3]*Department of Civil, Environmental and Geomatic Engineering, University College London, UK*

Abstract

Reliability is one of the key problems of an automatic system, especially to the huge, complex, multiple target-based, safety critical and reliability-dependent train control system. A system reliability analysis method based on a dynamic fault tree was proposed to analyse possible fault causes of a whole system in a HLA (High Level Architecture) simulation platform, and according to the principle of the dynamic fault tree model, the conversion from dynamic logic gates to Markov Chain was achieved. The reliability analysis through the dynamic fault tree method of train-ground communication subsystem was completed, which included a qualitative and quantitative analysis. A test of train-ground communication failure was established based on the fault injection method, the fault injection tool in a simulation environment enabled each module of the train control system running according to the fault testing program. The simulation result shows that compared with the conventional static fault tree analysis method, using dynamic fault tree analysis can conduct a better reliability analysis, using the fault injection method that can evaluate and test a simulation system based on HLA effectively, which can improve the reliability of the simulation system.
Keywords: train control system, reliability, dynamic fault tree analysis, high level architecture, importance degree, fault injection.

WIT Transactions on The Built Environment, Vol 155, © 2014 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CRS140171

1 Introduction

The high-speed railway has achieved great development in China in recent years, which includes thousands of kilo meters railway tracks, hundreds of high speed trains and dozens of railway station. Reliability is one of the key problems of automatic system, especially to the huge, complex, multiple targets based, safety critical and reliability depended train control system. On July 23rd of the year 2011, due to the fault of the train control system, two trains crashed on the Yong-wen railway lines in China, which caused a large number of deaths and injuries. In order to reduce such incidences and promote the healthy development of the high-speed railway, deep and careful research shall be conducted on the reliability of the train control system. However, it is very difficult to deal with the reliability problem in practical field, since it's dangerous to inject the fault in the real system. A simulation environment is necessary for reliability analysis and testing of train control system.

The classic reliability analysis methods include Fault tree analysis [1], Fault Model and Effect Analysis [2], Stochastic Petri Net [3], Markov Model [4] and etc. Dynamic Fault Tree [5] that combines the advantages of both fault tree analysis and Markov model can be used for reliability analysis of system having time sequence regularity. Bucci and Kirschenbaum [6] have studied a methodology that combines Markov modelling with the cell-to-cell mapping technique to construct dynamic fault trees and addresses the concerns with traditional fault tree methodology. Durga Rao and Gopika [7] extended traditional FT by defining additional gates for reliability and safety assessment of complex and critical engineering system, this method applied to a simplified scheme of electrical power supply system of nuclear power plant that is a complex repairable system having tested and maintained spares. Distefano and Puliafito [8] developed a new formalism derived from RBD: the dynamic RBD (DRBD), which is used to solve the overall system reliability evaluation through the entire phase of modelling and analysis. Therefore it is a reasonable choice for reliability analysis of train control system.

Fault injection technology is an important method for system reliability evaluation and testing. Chang Qing and Chen Jian-hui [9] have studied how to select injecting point to improve the efficiency of fault injection and enhance the reliability evaluation. Liu Lei and Mu Jian-cheng [10] proposed a method of fault injection testing technology based on the HLA architecture of CTCS-3 simulation and test platform to carry out single fault injection or multi faults coupling injection. The typical representatives of fault injection tool based on simulation are: VERIFY developed by Germany Erlangen-Nurnberg University, and MEFISTO-C developed by Technology University of Chalmers in Sweden, and etc. [11–13]. In train control system, it is used to test how the train system will reacts after a pre-defined fault happens.

In this paper, research on reliability of train control system will be done through the dynamic fault tree analysis method and the fault injection method in HLA based CTCS-3 train control simulation system.

2 CTCS-3 train control simulation system

The CTCS-3 train control system is an important component of China train control system (CTCS), applicable to the high-speed passenger dedicated railway line whose speed can get to 350 km/h. As shown in fig. 1, the system consists of ground equipment, on-board equipment and train control centre. The train-ground information transmission is based on GSM-R wireless communication system.

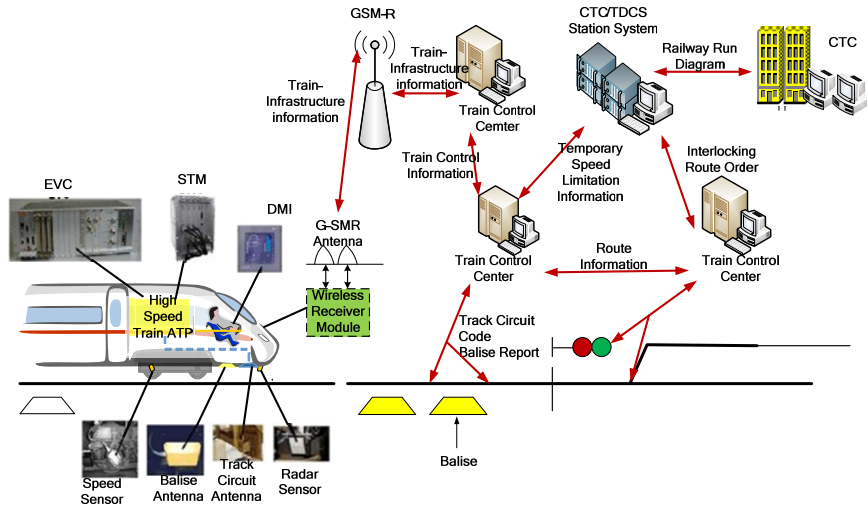

Figure 1: CTCS-3 train control system architecture.

A self-developed CTCS-3 train control simulation system is developed based on the High Level Architecture (HLA) simulation platform. HLA uses the object oriented method to design the simulation modules and construct the simulation federal. In the HLA based simulation system, each module is regarded as one of the federal members. HLA defines the information interaction principles between the members and the federal. All of the information interaction is executed by simulation manager module RTI. The CTCS-3 simulation system includes eight members: Radio Block Centre (RBC) simulation module, Temporary Speed Restriction Server (TSRS), on-board simulation module, trackside simulation module, Centralized Traffic Control (CTC) simulation module, Train Control Centre (TCC) simulation module, interlocking simulation module and GSM-R simulation module. Fig. 2 shows the information interaction between the members.

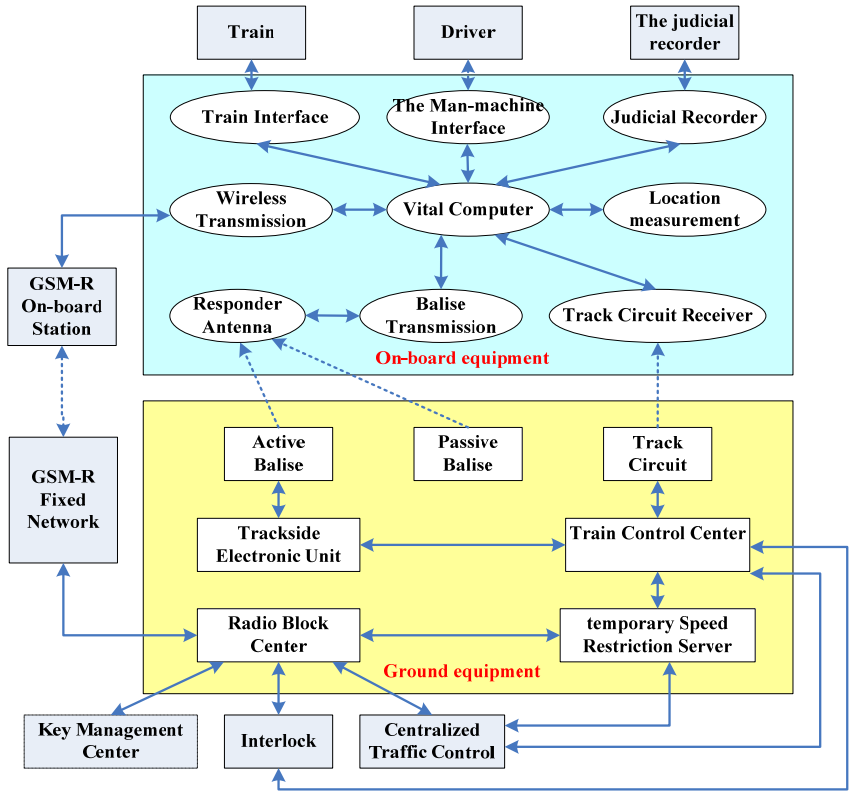

Figure 2: Information interaction of HLA based CTCS-3 simulation system.

3 Dynamic fault tree analysis of communications sub-system

A reliability analysis is performed on train-ground communication sub-system, which is a key component of CTCS-3 train control system. Fig. 3 shows dynamic fault tree of train-ground communication subsystem. Taking the failure of the communication as the top event, the system consists of 5 sub-tree (G1–G5) and 9 bottom events (E1–E9). Since G1 and G4 have hot standby, the failures happen only when the corresponding bottom events take place in determined sequences. We define these sub-trees as dynamic sub-trees. All of the other sub-trees are static sub-trees. The dynamic sub-trees and static sub-trees can also be determined by using the traversal method [14]. Table 1 shows the failure rate of the bottom events. They are obtained based on the simulation experiments on CTCS-3 simulation system.

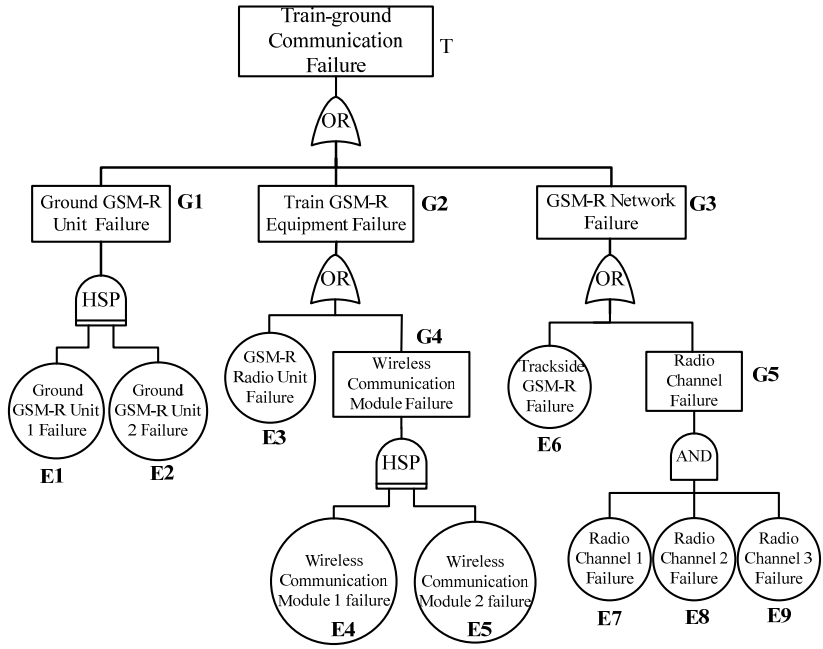

Figure 3: The dynamic fault tree of train-ground communication sub-system.

Table 1: Failure rate of the bottom events.

Component	Fault rate	Component	Fault rate
E1	2.10×10^{-4}	E6	1.20×10^{-6}
E2	2.10×10^{-4}	E7	1.49×10^{-5}
E3	1.45×10^{-8}	E8	1.49×10^{-5}
E4	1.80×10^{-4}	E9	1.49×10^{-5}
E5	1.80×10^{-4}		

3.1 Quantitative analysis

The failure probability of G1 and G4 cannot be obtained using traditional Boolean method [15]. Therefore Markov method is introduced. The sub-system G1 and G4 are changed into the Markov chains as shown in fig. 4.

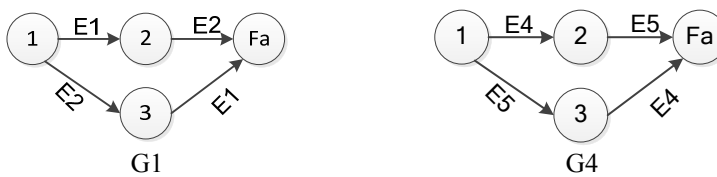

Figure 4: Markov State Transition Diagrams of dynamic sub-trees.

The number in a circle indicates different system state and 'Fa' means the system fails. The arrow between the circles indicates the bottom event that happens during the state transition. From the figure we can see, G1 and G4 have two failure chains '1-2-Fa' and '1-3-Fa'. The system failure probability is the sum of the failure probabilities of the two independent chains:

$$p(G1) = 1 + \frac{\lambda_{E2}e^{-\lambda_{E1}t} - \lambda_{E1}e^{-\lambda_{E2}t}}{\lambda_{E1} - \lambda_{E2}} + 1 + \frac{\lambda_{E1}e^{-\lambda_{E2}t} - \lambda_{E2}e^{-\lambda_{E1}t}}{\lambda_{E2} - \lambda_{E1}} = 4.41 \times 10^{-8} \quad (1)$$

$$p(G4) = 1 + \frac{\lambda_{E5}e^{-\lambda_{E4}t} - \lambda_{E4}e^{-\lambda_{E5}t}}{\lambda_{E4} - \lambda_{E5}} + 1 + \frac{\lambda_{E4}e^{-\lambda_{E5}t} - \lambda_{E5}e^{-\lambda_{E4}t}}{\lambda_{E5} - \lambda_{E4}} = 3.98 \times 10^{-8} \quad (2)$$

Taking G1 and G4 as two bottom events of train-ground communication subsystem fault tree, the fault tree is converted into a static system as shown in fig. 5.

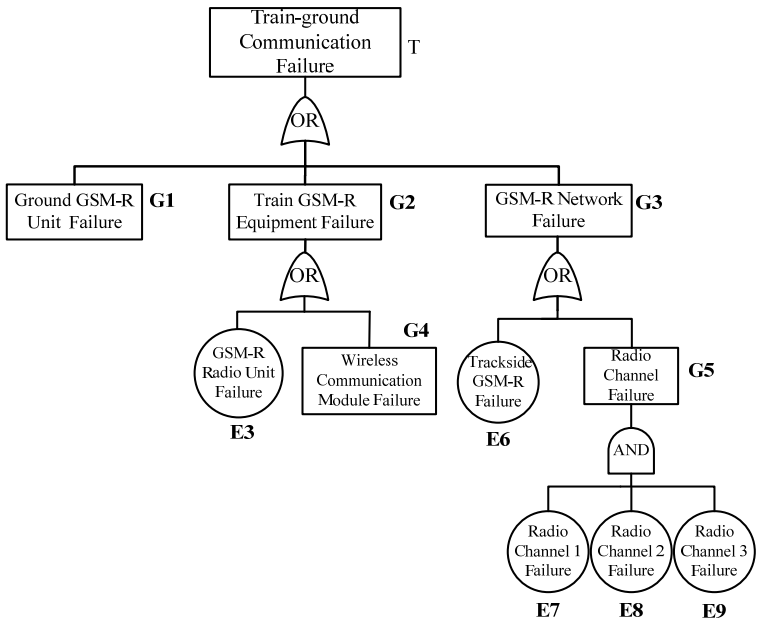

Figure 5: Equivalent static fault tree.

Using the theory of the Fussell-Vesely method we can work out the minimum cuts sets are: {G1}, {E3}, {G4}, {E6}, {E7, E8, E9}. The probability of the top event can be analyzed using traditional Boolean algebra method and can be calculated as:

$$P(T) = P(G1 + E3 + G4 + E6 + E7 * E8 * E9) = 1.29 * 10^{-6} \quad (3)$$

$$MTBF = {T(t)}/{R} = 7.75 \times 10^5 \tag{4}$$

3.2 Importance degree analysis

The analysis on importance degree is beneficial for supplying constructive suggestions to improve the reliability of the system. The typical importance degree indexes include structural importance degree and pivotal importance degree. Structure important degree analysis starts from the whole structure of the fault tree, investigating the importance degree of basic event in the fault tree structure, ignoring the probability that occur. The structural importance degree is described as

$$I_{st}(j) = \frac{1}{2^{n-1}} n_j \tag{5}$$

Here I_{st}(j) means the structural importance degree of bottom event E_j, n is the total number of bottom event and n_j is the total number of cut sets. From the formula, structural importance degree is irrelevant to the probability of the bottom event.

Pivot importance degree is the ratio of system failure probability change rate to the failure probability change rate of the corresponding bottom event which induces the change of the system failure probability. It is calculated as

$$I_{cr}(j) = \lim_{\Delta q_j \to 0} \frac{\Delta Q}{Q} / \frac{\Delta q_j}{q_j} \tag{6}$$

Here q is the failure probability of the bottom event and Q is the system failure probability. Pivot importance degree is not only describes the influence of the variance of the bottom event probability to the top event probability, but also indicates the ease or complexity of improving the system reliability by reducing the probability of the bottom event. In table 2 shows the structural importance degree and the pivot importance degrees of the 9 bottom events. From it, E3 and E6 have highest structural importance degree. The reliability of the corresponding device should be strengthened in structure design of the system. Compared to other bottom events, E3 has a much higher pivot importance degree. Therefore, by lowering the failure probability of E3, the failure probability of the system can be reduced effectively.

Table 2: The importance degree of bottom events.

	E1	E2	E3	E4	E5
Structure importance	0.5	0.5	1	0.5	0.5
Pivot importance	0.03633	0.03633	0.64214	0.28738	0.28738
	E6	E7	E8	E9	
Structure importance	1	0.25	0.25	0.25	
Pivot importance	0.03416	1×10^{-10}	1×10^{-10}	1×10^{-10}	

4 Reliability test based on fault injection method

Fault injection technology is an important evaluation and test method for system reliability, which injects fault modes into the system, and analyzes the response of the key equipment, so as to evaluate functional design of the system [16]. On the basis of CTCS-3 simulation system, a HLA based fault injection simulation system is established to verify whether the train control system responses properly when failure occurs. The information interaction of the fault injection simulation system is shown in fig. 6. A fault injection unit is added to the CTCS-3 simulation system. In the simulation process, the fault data is injected into the corresponding simulation modules through the interface. The fault injection is carried out through changing the logical value of the bottom events in the fault tree, in other words, changing the key equipment's working state to simulate the situation when the device fails. Meantime, the response of the simulation modules is recorded by the system in real time.

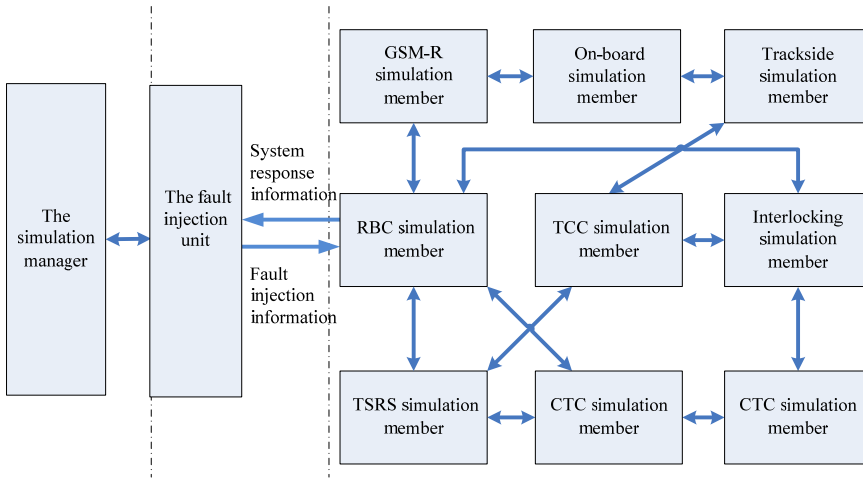

Figure 6: The train control fault injection simulation system.

4.1 Fault injection test

The fault injection includes four steps: 1) choose the fault type; 2) implement the fault injection; 3) collect the response; 4) analyse the results [17].A fault injection test is done on the train-ground communication subsystem. Taking E3, E4 and E5 as possible fault source, we get 8 different fault models generated by different fault combinations of E3, E4 and E5. The table 3 also lists the expected response generated by fault tree analysis method and the actual response results collected from the simulation system. In the table, "0" means the event is in a normal state and '1' means the event is under faulty condition.

Table 3: The expect response of train control simulation system.

No.	Fault injection			Expected response			Actual response		
	E3	E4	E5	G4	G2	T	G4	G2	T
1	0	0	0	0	0	0	0	0	0
2	1	0	0	0	1	1	0	1	1
3	0	1	0	0	0	0	0	0	0
4	0	0	1	0	0	0	0	0	0
5	1	1	0	0	1	1	0	1	1
6	0	1	1	1	0	1	1	0	1
7	1	0	1	0	1	1	0	1	1
8	1	1	1	1	1	1	1	1	1

The test results show that the train control simulation system has made the consistent responses with the dynamic fault tree's analysis, and followed the design principle of safety guide in malfunction. The fault injection has been implemented effectively. The fault injection tool can effectively test and verify the safety function of simulation system.

4.2 Validity verification of the fault injection simulation system

In order to verify the validity of the fault injection tool, 30 independent group experiments were carried out. In each group of experiment, 100 times of repeated fault injection tests are done. The validity is the ratio that obtained valid response tests to the total number tests. Fig. 7 shows the validity statistics of the 30 group of experiments. From the result, the validities for different group of experiment vary from 93% to 99% and the average validity gets to 96.6%. This indicates that the fault injection system is stable and valid. The simulation results derived from it can be used to reflect the performance of the real system in failure modes.

Similarly, we use the fault injection method to test and validity the sub-trees of G1 and G3, the validity statistics of them are shown as shown in fig. 8 and fig. 9. A large number of experiments show that the reliability test based on fault injection method can test and verify the reliability of the simulation system. Meanwhile, the tests show that dynamic fault tree is efficient to represent the fault model, which means compared with conventional static fault tree analysis method, using dynamic fault tree analysis can conduct reliability analysis better, using fault injection method can evaluate and test simulation system based on HLA effectively, which can improve the reliability of the simulation system.

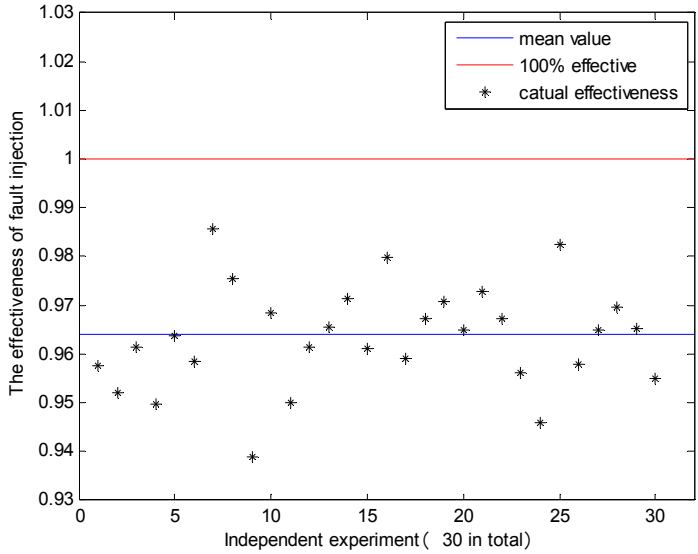

Figure 7: The validity statistics of the fault injection system.

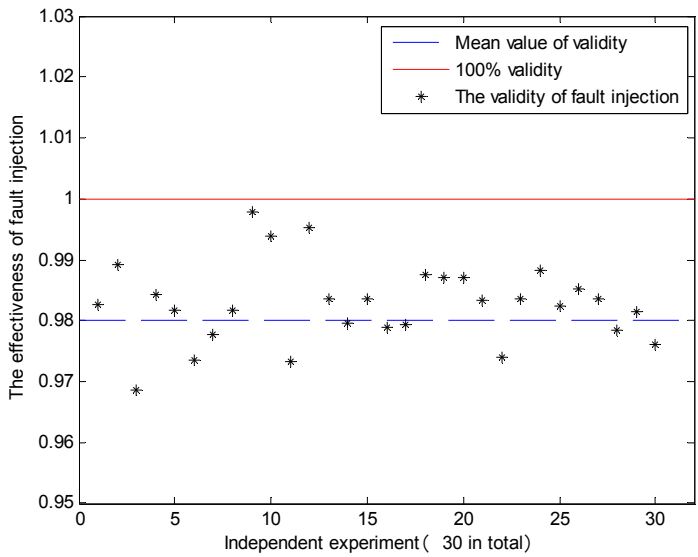

Figure 8: The validity statistics of G1.

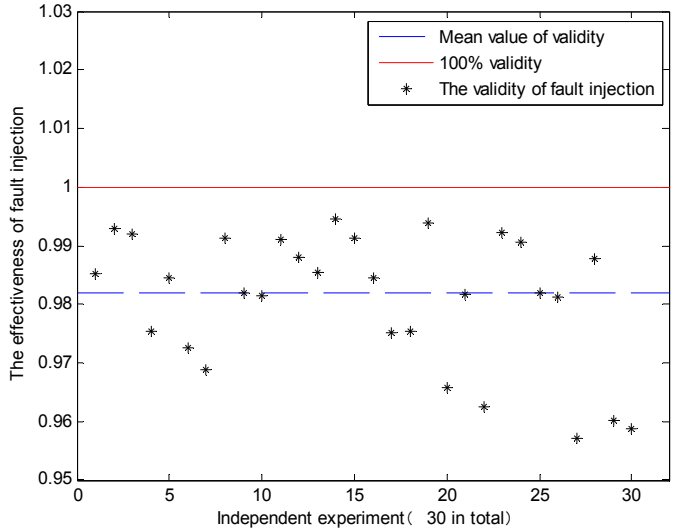

Figure 9: The validity statistics of G3.

5 Conclusion

This paper studied the reliability analysis and testing methods of CTCS-3 train control system in the simulation environment for it is very difficult to deal with the reliability problem in practical fields. A test of train-ground communication failure was established based on fault injection method, train control models were controlled by using fault injection tool in simulation environment. From the research, the following is concluded:

1) The dynamic fault tree based on HLA (High Level Architecture) simulation system was established to analysis possible fault causes of whole system from different system level. Then fault tree's modular was decomposed using traversal method, the reliability analysis was completed precisely, which include qualitative and quantitative analysis.
2) The reliability of the train control system, which has time sequence regularity such as hot/cold standby that cannot be analysed using traditional Boolean method, can be precisely analysed using Markov based dynamic fault tree analysis method.
3) Through importance degree analysis of the bottom events, the key event can be identified and constructive suggestions can be made for improving the reliability of the system.
4) A large number of fault injection experiment results show that the train-ground simulation system will reacts properly when fault occurs. The validity test results also show that the fault injection system is a stable and valid system that can be used.

Acknowledgements

The authors would like to thank the anonymous reviewers for their constructive comments during the review process.

This paper was supported by National Natural Science Foundation for Young Scholars of China (Grant No. 61104162), the State Key Program of National Natural Science Foundation of China (Grant No. U1334211), the Fundamental Research Funds for the Central Universities of China (Grant No. 2013JBM007), the Scientific and Technology development program of China Railway Corporation (Grant No. 2013X009-D), Beijing Higher Education Young Elite Teacher Project (Grant No. YETP0538), National Research Foundation for the Doctoral Program of Higher Education of China (Grant No. 20120009110029), National International Scientific and Technological Cooperation Project (Grant No. 2014DFA80260).

References

[1] Yang Yu, Liu Xiaoping, Fault tree logical reduction strategy for living probabilistic safety assessment. Atomic Energy Science and Technology, 39(5), pp. 433-437, 2005.

[2] Yong Ou, Dugan, J.B. Approximate Sensitivity Analysis for Acyclic Markov Reliability Models [J]. IEEE Transactions on Reliability, 52(2), pp. 220-230, 2003.

[3] LIN Chuang, WANG Yuan-zhuo. Research on Network Dependability Analysis Methods Based on Stochastic Petri Net [J]. ACTA ELECTRONICA SINICA, 32(2), pp. 322-331, 2006.

[4] J Zhao, AHC Chan and MPN Burrow. Reliability analysis and maintenance decision for railway sleepers using track condition information [J]. Journal of the Operational Research Society, 58(2), pp. 1047-1055, 2007.

[5] Xu Tianhua, Li Shu, TangTao. Dependability Analysis of Data Communication Subsystem in Train Control System [J].Journal of Beijing Jiaotong University, 3(15), pp. 23-26, 2007.

[6] Bucci, P. and Kirschenbaum, J. Construction of fault tree models from Markov approach to dynamic system reliability [J]. Reliability Engineering and System Safety, 93(11), pp. 1616-1627, 2008.

[7] Durga Rao, K. and Gopika, V. Dynamic fault tree analysis using Monte Carto simulation in probabilistic safety assessment [J]. Reliability Engineering and System Safety, 94(4), pp. 872-883, 2009.

[8] Distefano, S. and Puliafito, A. Dependability evaluation with dynamic reliability block diagrams and dynamic fault trees [J]. IEEE Transaction on Dependable and Secure Computing, 6(1), pp. 4-17, 2009.

[9] Chang Qing, Chen Jian-hui. Application of FTA in fault injection system [J]. Instrumentation Technology, 12(3), pp. 51-53, 2007.

[10] Liu Lei, Mu Jian-cheng. Study of CTCS-3 simulation and test based on fault injection [J]. Railway computer application, 20(4), pp. 51-53, 2011.

[11] Zhang Shi-jian, Xu Tong. A Dependability Evaluation System Based on Microprocessor Function Model [J]. Chinese Journal of Computers, 31(3), pp. 391-399, 2008.
[12] Antonio D.S., Alberto G.C., Josef M., Design and Implementation of a Java Fault Injector for Exhaustif. *Proc.of the 4st Int*. On Dependability of Computer Systems, Washington, DC, Elsevier: IEEE Computer Society, pp. 77-83, 2009.
[13] Peng Jun-jie, Huang Qing-cheng. A Software Fault Injection Tool for Evaluation of the Dependability of Onboard System [J]. Journal of Astronautics, 26(6), pp. 823-827, 2005.
[14] Yan Jianping. A Method to Find Modules of Fault Trees [J].Journal of Beijing jiaotong University, 24(5), pp. 63-66, 2000.
[15] Zhang Xiaojie, Zhao Haitao. The reliability analysis of satellite based on DFTA [J]. Journal of Astronautics, 30(3), pp. 49-54, 2009.
[16] Mu Ruiqi, Wang Dan. CBTC on-board test technology study based on fault injection [J]. Railway signalling & communication, 46(8), pp. 66-70, 2013.
[17] Yin Qing, Cai Baigen. The application of fault injection in train control system [J]. Railway signalling & communication, 49(1), pp. 43-46, 2010.