Fault Model-Based Safety Test Method and Application for CTCS-3 Train Control System

Yu Liu[1], Tao Tang [2], Kaicheng Li [1], Chenling Li [2]

[1] National Engineering Research Center Of Rail Transportation Operation And Control System,
Beijing Jiaotong University, Beijing, China
[2] State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, China
yuliu@bjtu.edu.cn

Abstract - As a safety critical system, train control system matters in passengers life and properties. It is important that how to guarantee the safety of train control system. Safety testing is an effective method to detect the safety holes and bugs in the system. However, most safety testing for train control system is manually executed based on expertise, which leads to a huge testing workload. Besides, manual generation will easily cause the problem of missing test cases.

In this paper, a model-based safety test method is introduced, hoping to solve this problem. We select a core function of onboard system in Chinese Train Control System level 3 (CTCS-3) as representative to study the method. This function was analyzed by Fault Tree Analysis (FTA) firstly, and a set of timed automata network model of this function is built using the tools of UPPAAL, the bottom events are used to turn to fault models, injected into the whole system model. Then COVER, the real-time test case generation tool, is used to generate the safety test cases from the system model (included fault models) automatically, and states transition criteria is customized based on preferences to achieve user-defined test, the test accuracy and efficiency is improved..

Index Terms – Safety Test, CTCS-3, Fault model-based.

1. Introduction

The CTCS-3 Onboard system is a typical safety-critical system, responsible for the implementation of train protection. The functional correctness of the onboard system reflected not only in the correctness of the logic output, but also in completion of time-constrained. Any fault would cause grave losses of life and property. Therefore, it is very important to ensure the functional correctness in the onboard system, and testing is the mainly method which focus on the conformance relation between the specification and the system under test.

Safety testing should be considered as much as possible besides the functional testing, it is executed with test cases including the unexpected events, which contain a huge and generally inexhaustible collection. For the train control system, we define an executable test case is a test sequence which starts from the initial state of the system, after a series changes of state, finally returns to the initial state.

Most of the traditional safety test cases for train control system are manually connected and generated based on the expert experience, which leads to a huge testing workload because of the complexity of train control system. Besides, manual generation will easily cause the problem of missing test contents. Therefore the method of automatic test cases generation will satisfy the need of safety testing for high-speed railway train control system better.

With the widespread of formal method, a lot of automatic test case generation technologies are introduced, and model-based testing (MBT) has been gradually used. It can provide structured, repeatable, optional test cases and avoid the subjectivity of manual generation. In this paper, we establish the test models based on the timed automata theory, and do the research on the method of model-based automatic safety test case generation for the onboard system.

Analyzing the safety-related functions of onboard system should be done before establishing the model. We use Fault Tree Analysis (FTA) to identify and analyze the faults and imported them into the under-test system (onboard system) models built to get safety test models.

2. Safety Function Analysis of Mode Transition Function

A. The characteristics of mode transition function

The CTCS-3 onboard system communicates with the environment by specified interfaces, includes the train, the driver, and the trackside external equipment.

Onboard system needs to manage different running modes according to the different conditions, and modes should be transited automatically or human involved. The mode transition function is one of the most important functions of the onboard system. Therefore, we take it as representative to do the method research. The onboard system model is simplified into that the onboard VC (Vital Computer) transports information with environment through specified interfaces and manages internal state information (mode), which is shown in Fig.1.

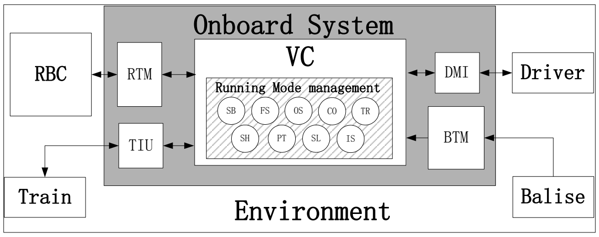


Fig. 1 Onboard system simplified model.

Mode transition function is mainly responsible for managing the operational mode. Thus, the train can run in certain mode, the safety supervision responsibilities of equipment and driver are determined. The onboard system of CTCS-3 train control system is divided into nine operating modes: Isolation Mode (IS), Sleeping Mode (SL), Standby Mode (SB), Shunting Mode (SH), Full Supervision Mode (FS), On Sight Mode (OS), Call On Mode (CO), Trip Mode (TR), Post Trip Mode (PT), the definition and transition conditions are described in detail in CTCS-3 System Requirement Specification (SRS).

The mode transition condition can be classified as following:

1) Integrity of the trackside information, such as the integrity of movement authority (MA);
2) Artificial responsible for driving;
3) Emergency situation treatment;
4) Special signals, such as the sleep signal, isolation signal, cab activation signal;
5) Train current state, such as stop, limit speed, etc.

According to their characteristics, the mode transition can be divided into upgrade transition and degrade transition. The definitions are as follows:

1) Upgrade transition: the condition before the transition is more strict than after, that means the former mode is more safety;
2) Degrade transition: the condition before the transition is less strict than after, that means the latter mode is more safety;

We should focus on the restricted speed changing and the equipment responsibility coverage in upgrade and degrade transition.

After a brief analysis of the mode transition function, the next step is to analyze it with FTA.

B. *Safety function analysis for mode transition based on FTA*

The core function of onboard system is to prevent the collision or derailment which caused by exceeding the safe speed or distance. So collision/derailment is selected as the core hazard of fault tree analysis for safety test.

If the human factors are not considered, the possible reasons of collision/ derailment could be further analyzed as following:

1) Exceeding the stop point, which is caused by failing to stop or reduce to certain speed at a specified point;
2) Invocatable physical fault in front section, like broken rail;

The fault of exceeding the stop point could be further decomposed into:

1) Wrong information from trackside equipment;
2) Unsuccessful mode transition, in which the state judgment is error and the train fails to brake.

According to above analysis, the system fault tree is shown in Fig. 2.

In conclusion, unsuccessful mode transition is one of the most important reasons. According to the definition, the mode transition can also be divided into safety-related transition and safety-unrelated transition.

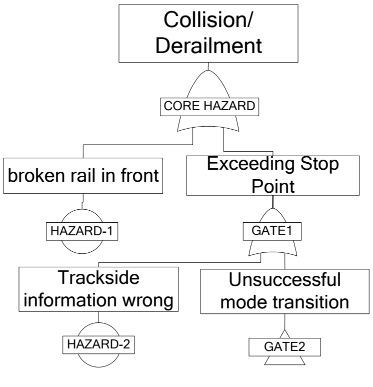


Fig. 2 System Fault Tree.

Safety-unrelated mode transition is decided with the following rules: 1. It is a upgrade transition, which transit from the high-limited state to the low-limited state, only operation efficiency is influenced by unsuccessful mode transition. Once the transition was unsuccessful, the constraints of environment would not be broken; 2. The train needs to stop when the mode is changing, failing in this kind of transition also won't lead to safety accidents.

Safety-related mode transition is decided with the following rules: 1. Brake is required to apply after the mode transition; 2. It is a degrade transition, the operation capacity of external environment declines, and it is necessary to reduce the running speed. Once the transition is not successful, it will break the constraints of the environment and cause accidents.

According to above analysis, we keep decomposing the fault and get the fault tree shown in Fig. 3.

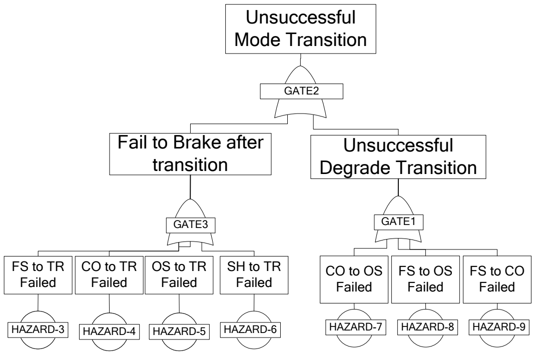


Fig. 3 Mode Transition Fault Tree.

According to the FTA result, mode transition in CTCS-3 are classified as Table I.

TABLE I Mode transition classification

Type	Mode Transition
Safety-related	SH->TR, OS->TR, CO->TR., FS->TR, CO>OS, FS->OS, FS->CO
Safety-unrelated	Other mode transition

Through the analysis of onboard function, we confirmed the safety-related mode transition. On this basis, it is possible to conduct the safety test case generation.

3. Automatic Generation of Test Cases for Onboard System

A. Establishing The Safety Function Model of Mode Transition

In order to get the safety test cases, we need to establish a safety function model of the system under test. According to the definition and the onboard system simplified model shown in Fig.1, the network automata model of the onboard system is established using the UPPAAL tool. As in Fig.4, the vital computer (VC) automaton is selected as the subject for study, the external environment includes train, Balise, RBC and Driver automaton.

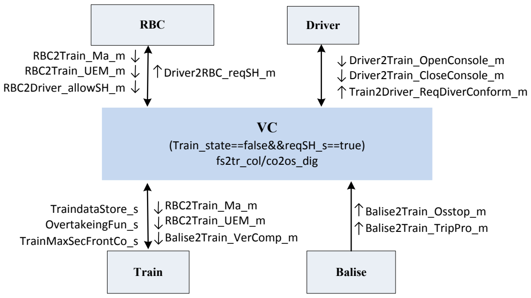


Fig. 4 Mode transition function model of onboard system.

The entire system network automata model is divided as kernel part and environment, i.e. VC ||Environment, V-E model for short. The automata are showed in Fig.5 to Fig.9.

The driver automaton is depicted in Fig.5, which realizes the following functions:

1) The driver opened/closed the cab, start/end the model running;
2) Sending the shunting requirement;
3) Acknowledgement the requirement from VC;

The balise automaton is depicted in Fig.6. It is mainly responsible for sending specific section information to the onboard equipment, including stop command in on sight section and trip protection command.

The RBC automaton is depicted in Fig.7, which realizes the following functions:

1) Sending MA to the onboard (VC), including normal MA and the emergency stop message;
2) Responsing the shunting requirement from Driver

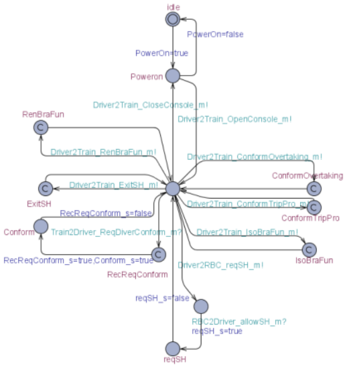

idle
PowerOn=false
PowerOn=true
Poweron
Driver2Train_CloseConsole_m!
Driver2Train_OpenConsole_m!
RenBraFun
Driver2Train_RenBraFun_m!
Driver2Train_ConformOvertaking_m!
ConformOvertaking
Driver2Train_ExitSH_m!
ExitSH
RecReqConform_s=false
Driver2Train_ConformTripPro_m!
ConformTripPro
Conform
Train2Driver_ReqDiverConform_m?
Driver2Train_IsoBraFun_m!
IsoBraFun
RecReqConform_s=true,Conform_s=true
RecReqConform
Driver2RBC_reqSH_m!
reqSH_s=false
RBC2Driver_allowSH_m?
reqSH_s=true
reqSH

Fig.5 Driver automaton

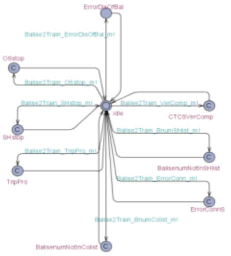


Fig.6 Balise automaton

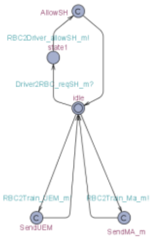


Fig.7 RBC automaton

The train automaton is depicted in Fig.8. It is mainly responsible for storing data and train states in the progress of interacting message with other automata

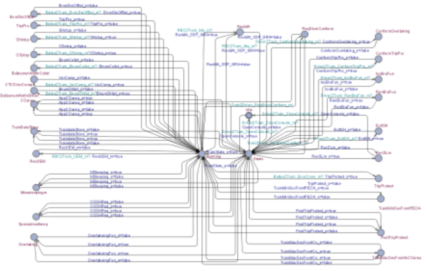


Fig.8 Train automaton

The VC automaton is depicted in Fig.9. It is mainly responsible for judging the mode transition conditions and finishing the transition according to the train state recorded by train automaton and message received from the external environment.

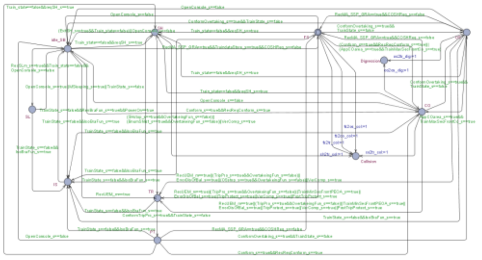


Fig.9 VC automata

According to the FTA result, we created two states, Collision and Derailment, when establishing the safety function model of VC, as shown in Fig.9. With FS to CO, for example, the transition variable fs2co_col turns to 1 from initial value 0 when the mode transition is failed, indicated the collision accident has accrued, then the VC model transits to the state of Collision, as indicated in yellow path in Fig.10.

B. Safety Test Cases Generation for Mode Transition

Based on the V-E model and Observer automata theory, we generated safety test cases for mode transition with CoVer, a tool developed by Uppsala University for real-time system automatic test cases generation.

Considering the feature of V-E network automata model and Observer Automata, we use user-defined coverage criteria (shown in Fig. 11) to generate the mode transition test cases by going through all the safety function variables of mode transition in the model.

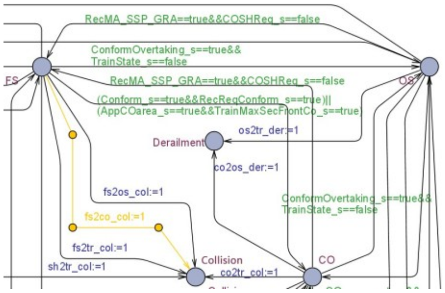
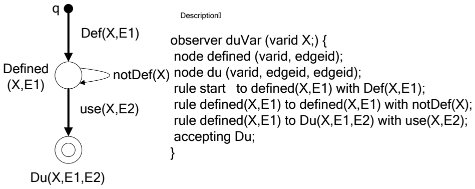

RecMA_SSP_GRA==true&&COSHReq_s==false
ConformOvertaking_s==true&&
TrainState_s==false
FS
OS
RecMA_SSP_GRA==true&&COSHReq_s==false
(Conform_s==true&&RecReqConform_s==true)||
(AppCOarea_s==true&&TrainMaxSecFrontCo_s==true)
os2tr_der:=1
Derailment
co2os_der:=1
fs2os_col:=1
fs2co_col:=1
ConformOvertaking_s==true&&
TrainState_s==false
fs2tr_col:=1
sh2tr_col:=1
Collision
CO
co2tr_col:=1

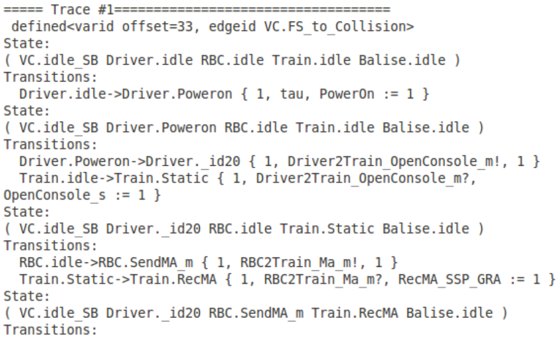
Fig.10 Fault states in VC model



```
observer duVar (varid X;) {
 node defined (varid, edgeid);
 node du (varid, edgeid, edgeid);
 rule start   to defined(X,E1) with Def(X,E1);
 rule defined(X,E1) to defined(X,E1) with notDef(X);
 rule defined(X,E1) to Du(X,E1,E2) with use(X,E2);
 accepting Du;
}
```

Fig.11 User-defined coverage criteria

According to above observer automata, coverage criteria and the definitions of safety-related mode transition variables, we have got safety test cases for mode transition testing. For example, we defined the search object to all the path satisfied the variable fs2co_col:=1, then we get the test suite of collision resulted from unsuccessful transition of FS to CO. It contains one test case(trace 1), the test steps and path is shown in Fig.12



```
===== Trace #1===================================
 defined<varid offset=33, edgeid VC.FS_to_Collision>
State:
( VC.idle_SB Driver.idle RBC.idle Train.idle Balise.idle )
Transitions:
  Driver.idle->Driver.Poweron { 1, tau, PowerOn := 1 }
State:
( VC.idle_SB Driver.Poweron RBC.idle Train.idle Balise.idle )
Transitions:
  Driver.Poweron->Driver._id20 { 1, Driver2Train_OpenConsole_m!, 1 }
  Train.idle->Train.Static { 1, Driver2Train_OpenConsole_m?,
OpenConsole_s := 1 }
State:
( VC.idle_SB Driver._id20 RBC.idle Train.Static Balise.idle )
Transitions:
  RBC.idle->RBC.SendMA_m { 1, RBC2Train_Ma_m!, 1 }
  Train.Static->Train.RecMA { 1, RBC2Train_Ma_m?, RecMA_SSP_GRA := 1 }
State:
( VC.idle_SB Driver._id20 RBC.SendMA_m Train.RecMA Balise.idle )
Transitions:
```

Fig.12 Test trace of a test case

As the method above, we have got the comprehensive test suites (cases) of mode transition shown in TABLE II.

TABLE II Safety Test Cases of Mode Transition

Coverage Criteria		Test suite		Generation Time(s)
status	Templates	Test case	Test steps	
Safety function (collision)	VC(FS->TR)	1	6	5.6s
	VC(SH->TR)	1	7	6.0s
	VC(CO->TR)	1	6	5.8s
	VC(FS->OS)	1	6	5.7s
	VC(FS->CO)	1	6	5.6s
Safety function (Derailment)	VC(OS->TR)	1	6	5.8s
	VC(CO->OS)	1	7	5.9s
Normal swap	VC	57	121	66s
Total	VC	64	165	106.4s

4. Conclusion

Traditional test cases of CTCS-3 onboard system are manually generated depending on expert experience, the test is subjective, low efficiency and time consuming, and it is difficult to ensure the test completeness. In this paper, a fault-model based method to generate test cases automatically for onboard system is proposed. Firstly, mode transition function was analyzed by FTA to get the safety-related functions; secondly, V-E timed network automata model of mode transition is established, based on the model and Observer automata theory, we have generated all the test cases for mode transition by CoVer using the user-defined coverage criteria, there are 7 safety-related test cases, 44 test steps, 57 other safety-unrelated test cases, 121 test steps. The safety test cases of mode transition are proven useful for classifying and testing the onboard subsystem. It can improve the test pertinence, efficiency and accuracy.

5. Acknowledgment

The authors would like to thank Lv Jidong, Yuan Lei and Li Chenling from SKLRTCS, Beijing Jiaotong University for their useful comments on case study. The research of the work reported here were supported by the project of National High-tech R&D Program of China: Safety certification and assessment technology of High-Speed railway signal system (2012AA112801); the Fundamental Research Funds for the Central Universities: Research of formal design and development method in High-Speed train control system (2012JBM024); the State Key Laboratory of Rail Traffic Control and Safety (Contract No. RCS2011K010), Beijing Jiaotong University.

6. References

[1] LV Jidong, Hierarchical Formal Modeling and Verification Train Control System[D], Beijing Jiaotong University, 2011.

[2] LV Jidong, Tang tao, et,al. Modeling and Verification of Time Constraints of Operation Scenarios of High-speed Train Control System[J]. JOURNAL OF THE CHINA RAILWAY SOCIETY. 2011.

[3] Yu Gang, Xu Zhongwei, Research on Automatic Safety Tests of Train Control System for Dedicated Passenger Line Based on Script Technique[J]. JOURNAL OF THE CHINA RAILWAY SOCIETY. 2011, 33(12):56-64.

[4] Beizer B.Black-Box Testing Technique for Functional Testing of Software and Systems, Wiley,New York, USA9,1995.

[5] Wu Daohua, Test Case Generation Based on Colored Petri Net and Its Application in Train Control System[D], Beijing Jiaotong University, 2010.

[6] Wang Qianqian, Research on the Optimal Generation Method of CTCS-3 Test Cases[D], Beijing Jiaotong University, 2010.