Movement authority security modeling and verification based on fault statechart

IOP Conf. Series: Materials Science and Engineering **569** (2019) 042056 doi:10.1088/1757-899X/569/4/042056

Movement authority security modeling and verification based on fault statechart

Fan Yu*, Minan Tang, Binbin Hao, Qianqian Wang

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

*Fan Yu's e-mail: 791509410@qq.com

Abstract. Communication Based Train Control System (CBTC) has become the development trend of train control system, and generating safe and reasonable movement authority is the key to ensure the normal operation of the whole system. Combined with the security of the system, a security analysis method based on fault tree information to construct fault Statechart is proposed. The fault tree that generates the abnormality of the movement authority is analyzed, and it is represented as a form that the Statechart can describe, thereby establishing a fault statechart of the movement authority generating abnormality. Finally, the formal modeling of the fault statechart is carried out by using the time automaton theory, and the fault state unreachable is taken as the attribute of the specification for inspection. The results show that the method of combining fault Statechart and time automata proposed in the paper is feasible and suitable for the analysis and verification of safety critical systems.

1. Introduction

In the safe and efficient operation of urban rail transit, CBTC system plays an irreplaceable role, and movement authority generation is the core function of CBTC, which affects the safety and efficiency of train operation. Therefore, it is necessary to conduct security modeling analysis [1] to ensure normal operation, avoid danger and meet the safety requirements.

Regarding the existing analysis and verification research of urban rail transit, Qiu Min used dynamic fault tree to realize safety analysis and control of vehicle-ground communication system [2]. Li Yao analysed the information interaction between CBTC subsystems, and established a time-safe state machine model to verify the function of cross-region switching [3]. Zhu Aihong adopted UML and colored Petri net models to analyze the influencing factors of train safety operation and driving efficiency [4]. Liu Jintao established PHAVer model and fault monitor model through the process analysis of system theory, and verified the security analysis of train control system with accessible set calculation [5].

The most representative of the system security analysis methods is the Fault Tree Analysis [6], but it cannot describe the time sequence and dynamic changes, so it is added to the state diagram for analysis. In this paper, the fault statechart of movement authority generation fault is established, but it lacks the high-precision formal meaning and cannot be verified directly. Furthermore, the time automaton [7-8] is used to formally describe and verify fault generated by movement authority.

2. Movement authority generation principle analysis

In order to accurately describe the driving conditions of the train, the concept of movement authority is introduced, which refers to allowing the train to operate within the infrastructure limits to a designated

location on the track [9]. Its generating process is divided into data preparation and data processing. Each subsystem transmits the position and driving information of the train within the controlled range to ZC, and ZC receives data information such as route, train location and version number, completes data preparation, enters data processing stage, and transmits movement authority information to the train through the DCS. The information between the subsystems is constantly interacting, and the system periodically generates movement authority for trains in the controlled area. Figure 1 is a mobile authorization generation state diagram obtained by analyzing the generation process in the literature [1, 10].

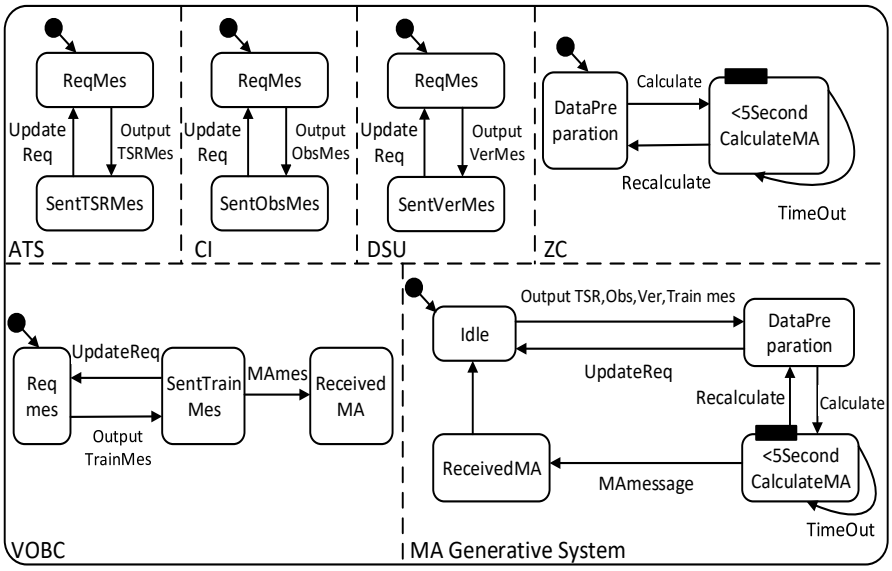


Figure 1. Movement authority generates statechart

3. Failure statechart construction

The Fault Tree analysis focuses on the cause and effect of failure and don't associate fault logic with system behavior, so it is impossible to confirm the existence of such faults. However, the statechart expresses the state change and behavior of the system and lacks a direct expression of fault information [11-12]. Therefore, the fault statechart is presented. It is a statechart that describes the functional behavior and security requirements of the system synchronously. The two characteristics of functional behavior and security requirement are orthogonal in functional domain and fault domain respectively. Functional domain refers to the collection of system object, state and transition described in fault statechart to realize system function behavior. The fault domain implements a set of logical relationships between fault situations and causes.

3.1. Description of security requirements

To establish the fault statechart generated by movement authority, the fault tree with the fault generated by movement authority as the top-level event should be established according to the generation principle of movement authority, and the security requirement information and fault logic relationship contained in the fault tree should be extracted by analyzing it. The specific fault tree is shown in figure 2.

In order to facilitate the description of each event, the top-level event is formally named as MAGenerateFault. The intermediate events are named as DataPrearationFault and DataProcessingFault; The basic events are named as Event1_TrainMesFault, Event2_TSRMesFault, Event3_ObsMesFault, Event4_ VerMesFault, Event5_TimeOut and Event6_NoReceivedMA.

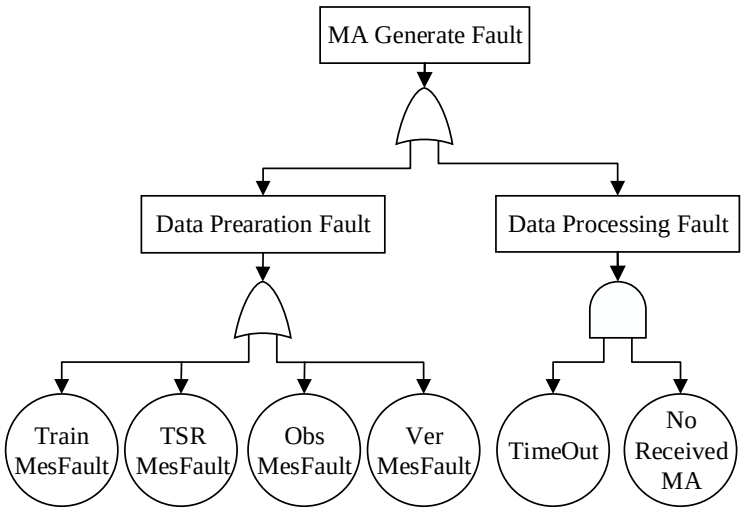


Figure 2. Movement authority generates abnormal fault tree

According to the logic and or gate relationship, the fault tree is analyzed from top to bottom. the security requirements are expressed with basic events. Finally, the minimum cut set that causes the occurrence of top-level events is determined as {Event1_TrainMesFault}, {Event2_TSRMesFault}, {Event3_ObsMesFault},{Event4_VerMesFault},{Event5_TimeOut,Event6_NoReceivedMA}.

The security requirements depicted by the fault tree of movement authority generating faults can finally be expressed by Boolean expressions composed of logical operators and basic events. If and only if expressions is true, the top-level event movement authority generating faults occurs, as detailed below.

DataPrearationFault=(∨,Event1_TrainMesFault,Event2_TSRMesFault,Event3_ObsMesFault, Event4_ VerMesFault)

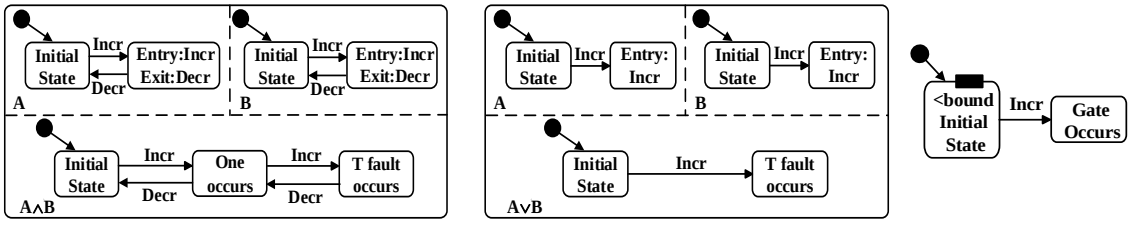
DataProcessingFault=(∧,Event5_TimeOut, Event6_NoReceivedMA)

MAGenerateFault=(∨,DataProcessingFault,DataProcessingFault)=(∨,(∨,Event1_TrainMesFault,Event2_TSRMesFault,Event3_ObsMesFault,Event4_VerMesFault),(∧,Event5_TimeOut,Event6_NoReceivedMA))

3.2. Transition rule

The above fault tree contains basic events and logical symbols. The logical symbol is transformed into an acceptable form of the statechart, which is connected with the basic event to express the logical behavior of the fault tree.

And gates are represented by a symbol ∧, meaning that only when all input events occur can occur output events, as shown in the figure3(a). Or gates are symbolized ∨, meaning that at least one input event occurs and the output events occur, as shown in the figure3(b). Incr and Decr represent incremental events and decrement events respectively; A and B represent input events, A∨B and A∧B represent output events. Boundary states and timeout events exist in the system, and events with continuous time need to be modeled. As shown in figure 3(c), when the time limit is exceeded, the timeout event can be triggered to make the system transition from the initial state to the event occurrence state.



(a) (b) (c)

Figure 3. Transition rule

3.3. Build the fault statechart of e movement authority generation fault

The fault statechart can describe the security requirements of the system and the functional behaviors of each subsystem synchronously. The functional information is reflected in the functional domain, and the logic of adding fault information is described as the fault domain. The two orthogonal domains constitute the abnormal fault statechart generated by movement authority as shown in figure 4. DataPreparationFault and DataProcessingFault two input events at least a occurred, all can cause top event. Event1, Event2, Event3 and Event4 four input events can cause DataPreparationFault occurred at least one. The DataProcessingFault occurs when both Event5 and Event6 input events occur.

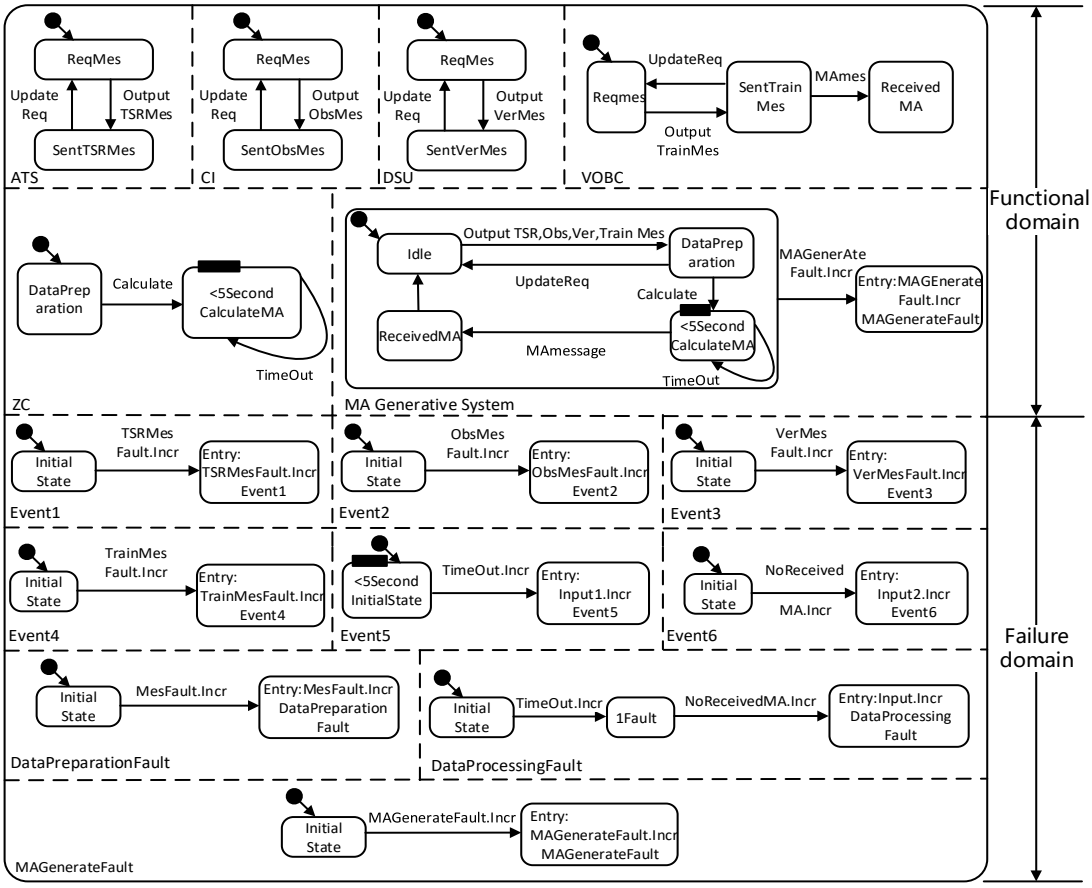


Figure 4. Movement authority generates abnormal fault Statechart

4. Formalized modeling and validation of fault statechart

4.1. Time automata and verification tool UPPAAL

In order to solve the problem of space explosion in finite state space, r. allur and Dill put forward the theory of time automata in 1994. UPPAAL is currently the most representative software tool for time-based automata, providing a formalized validator for describing and verifying system attributes, and supporting the modeling and verification of functional attributes of time-based automata.

4.2. Time automata model construction of movement authority fault generation

Due to the nature of the fault statechart and timed automata, same happens is a change in the state after certain events, but the fault statechart is a semi-formal description method, can directly express the fault causes and behavior process, not on the analysis of the model is effective, so set up mobile license generation abnormal timed automata model, as shown in figure 5.

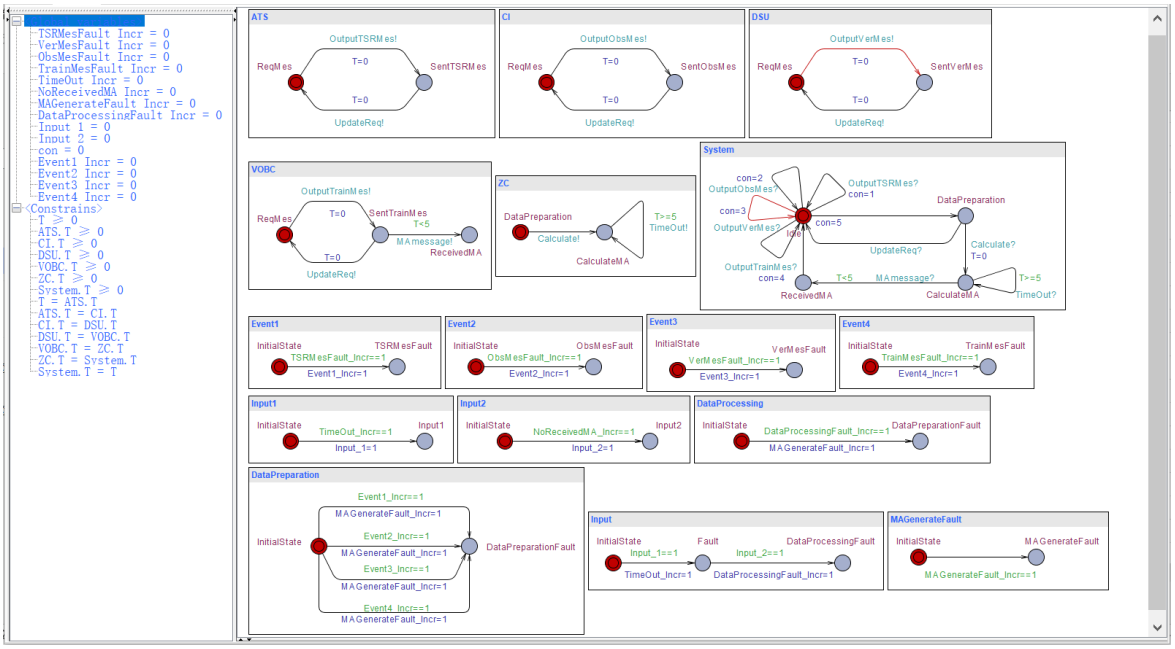


Figure 5. Movement authority generates Abnormal Time automata model

4.3. model verification

In this system, the top level fault event movement authorization generation fault should be avoided as much as possible. Therefore, the nature of verification is shown as whether the fault state is reachable, that is, whether the abnormal state generated by the movement authority is reachable.

The system sets the value of MAGenerateFault as 1 and 0, respectively representing the entered and not entered movement authority generates abnormal state. If E<>MAGenerateFault==1 is verified, and the state can be reached, it indicates that there is a defect in the system, and the defect can be located by verifying whether the minimum cut set is satisfied. If the verification fails, the state is unreachable, indicating that the system meets the security requirements described in the fault tree. The results are shown in figure 6. If the verification fails, the fault state is unreachable, indicating that the established movement authority generation system has no vulnerability.

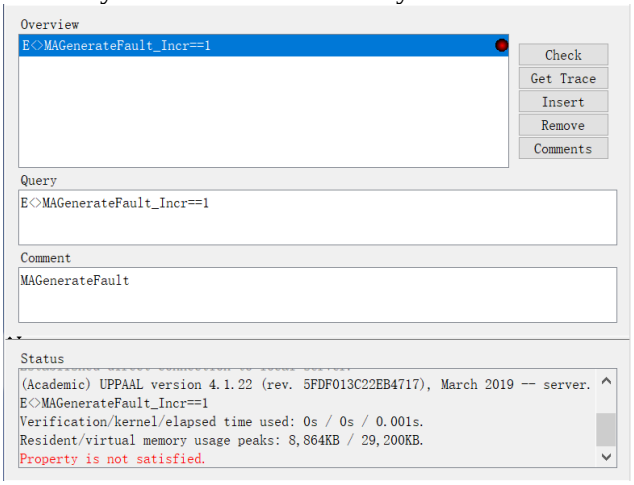


Figure 6. Model validation results

5. conclusion

(1)In this paper, the generation of movement authority is taken as an example to describe and verify the causal logic relationship between the faults occurring in the process.

(2) An analysis method based on fault statechart is proposed to extract fault information from the fault tree and represent it as a statechart. On the basis of retaining the description of system behavior by statechart, the description of fault situation is added to make the combination of security requirement and system function behavior more suitable for security verification.

(3) The modeling verification method combining the fault statechart with the time automata theory is feasible, which is not only used for the analysis and verification of the generation process of movement authority, but also suitable for other security critical systems.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants No.61763025 and No.61663021, and the University Science and Technology Project of Gansu Province, China under Grant No.2017A-025. The authors are very grateful to the referees for their helpful comments and valuable suggestions which have improved the paper.

References

[1] He,H.H., Chen,Y.G., Luo ,Y.Y., et al. (2015)Movement Authority Formal Modeling and Verification. Railway Standard Design, 59:118-121.
[2] Qiu,M. (2014)Risk Analysis and Control of Train Control System Based on Dynamic Fault Tree. Chengdu: Southwest Jiaotong University,8-17
[3] Li,Y., Chen,R.W., Guo,J., et al. (2015) Modeling and Verification of TSSM-Based CBTC Zone Controller for Urban Rail Transit [J]. Journal of Southwest Jiaotong University, 50:27-35.
[4] Zhu,A.H., Song,L.M. (2019)Modeling and Formal Analysis of Level Transition in Train Control System Based on UML and CPN. Computer Application Research,36:140-143+ 162.
[5] Liu,J.T., Tang,T., Zhao,L., et al. (2013) CTCS-3Level Train Control System Functional Safety Analysis Method Based on UML Model [J]. Journal of the China Railway Society, 35:59-66.
[6] Zheng,L.L., Song,L.H.,Guo,R., et al. (2011) Application of FAT in Information Security Risk Asses-sment. Computer Science,38:106-108+118.
[7] Hu,X.H., Han,J.R. (2016) Route Control Station Interlock Logic of Formal Methods. Computer Engineering and Application, ,52:229-234+270.
[8] Yang,L., Chen Y.G. (2018) Modeling and Verification of Switch Scene of Zone Controller Based on MSC and UPPAAL. Railway Standard Design,,62:171-174 +179.
[9] Huang,Y.N., Zhang P.J., Hou X.P., at al. (2016) Modeling and Verification Method of ZC Subsystem in Urban Rail Transit Based on Hybrid Automata.China Railway Science, 37: 114-121.
[10] Xu,H.W.,Lu,G.F.,Ding,Z.Y. (2018) Research on Movement Authority Generation Based on CBTC System.Industrial Control Computer,31:63-64.
[11] Huang,C.L., Huang,Z.Q. (2015) Research on Safety Verification of Extended SysML Activity Diagram for Embedded System Design . Journal of Chinese Computer Systems, 36:408-417.
[12] Cao,D.J., Huang,Z.Q., Lu,F, at al. (2016) Research of Safety Analysis Based on Integrating Fault Information into Functional Model. Journal of Chinese Computer Systems, 37:24-32.