Model-Based Safety Analysis of Movement Authority Scenario in TcCBTC system

Junting Lin1*, Xiaoqin Min1, Jinchuan Chai2

1 School of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China
2 National Railway Track Test Center, China Academy of Railway Sciences Corporation Limited, Beijing, China
*Corresponding author’s e-mail: linjt@lzjtu.edu.cn

Abstract. Train-centric communication based train control (TcCBTC) system contains a variety of uncertain factors in the operation process, and the generation scenario of movement authority is a real-time process. In order to judge the impact of uncertain factors on system safety, it is necessary to conduct formal modeling and analysis for this implementation process. Aiming at the modeling and analysis of the system in an uncertain environment, firstly, the implementation process of TcCBTC movement authority was analyzed, and the hazard source identification is carried out by combining the hazard and operability study (HAZOP) method. Secondly, the movement authority generation process is modeled based on the stochastic hybrid automata theory, and the statistical sample data are simulated in UPPAAL-SMC. Finally, the statistical model checking algorithm was used to analyze the model quantitatively. The results showed that the model could meet the functional attribute requirements of movement authority generation in TcCBTC system, and describe the uncertain environment in the process of system operation. SMC method could quickly verify the impact of uncertain factors on the system, and provide a certain theoretical basis for subsequent TcCBTC system development and relevant specifications.

1. Introduction

Train operation control system is one of the important technical means to ensure the safe and efficient operation of trains on the line. In recent years, the research on TcCBTC system has become a hot spot in the industry. The system simplifies the trackside equipment, and integrates the interlocking calculation and movement authority generation functions into the on-board, and uses wireless communication technology to realize the information interaction between trains, which shorten the train tracing interval. At present, TcCBTC system is in the stage of vigorous research and development, and the potential defects in its system requirements specification will bring risks to normal operation of the system. Moreover, the wireless communication between two different subsystems has random uncertain behavior. Therefore, it is the premise of successful development of TcCBTC system that modeling and verifying the system running in an uncertain environment, subsequently finding its potential defects.

EN50128 points out that ‘when the software safety integrity level (SIL) of the system is level 3 or level 4, it is strongly recommended to use formal methods to analyze and verify the system’ [1]. The focus of existing research on train control system modeling is not unified, and there is less analysis of system failure caused by random fault. Aiming at the modeling and analysis of movement authority generation scenario in uncertain environment, this paper takes stochastic hybrid automata theory as the modeling basis and statistical model detection as the safety analysis basis to formally model the
2. Fundamentals of system modeling and safety analysis

2.1. Stochastic hybrid automata model

Stochastic hybrid automata (SHA) comes from timed automata [2]. Its clock can be converted into different ratios in different states. The transition action between states can be expressed by discrete probability. The random semantics of SHA connects the probability distribution with the delay of a given state and the transition between states. It is widely used to model hybrid systems with random behavior. SHA model communicates with each other through broadcast channels and shared variables to form a network of stochastic hybrid automata (NSHA). The SHA model of TcCBTC system consists of a seven tuple \(< L, l_0, X, \Sigma, E, F, I >\) [3]. Where \(L\) is the finite location set of TcCBTC subsystem, \(l_0 \in L\) is the initial position, \(X\) is the set of continuous variables, real-time clock, \(\Sigma\) is a finite set of input and output actions, that is, guards, \(E\) is a finite set of migrating edges, \(F(l)\) is a function of time delay in position, \(I(l)\) represents an invariant on position.

2.2. Statistical model checking

Statistical model checking (SMC) is a model-based safety analysis method, which is regarded as the balance between testing and formal verification. In recent years, the methods based on NSHA and SMC have been widely used to solve the probability evaluation problem of safety critical systems [4]. The principle is that using the simulation-based method to simulate the system for many times to verify whether the model meets the specific properties, and evaluate the probability interval of meeting a certain attribute in the random operation process of NSHA model through the algorithm. If NSHA is defined as system model \(M\), then \(M\) runs randomly and the probability of satisfying the attribute \(\psi\) is \(PM(\psi)\). SMC algorithm performs a sufficient number of TcCBTC system model simulation runs at a predetermined significance level to obtain statistical evidence to test quantitative properties.

UPPAAL-SMC, a tool for statistical model checking, is a model checking tool built by David et al. combined with the principle of timed automata and SMC algorithm [5]. UPPAAL-SMC supports checking the quantitative attributes of the model on the basis of UPPAAL. Compared with other model checking tools, UPPAAL-SMC can provide a formal description of the random mixing characteristics of time systems, and has the advantages of modeling system in real-time, concurrency, hybrid-oriented and uncertain environment. It also allows users to use query statements to evaluate the probability that the established model meets a certain attribute, and visualize the value of the result in the window.

3. System modeling based on NSHA

3.1. Overview of system requirements

Movement authority (MA) is the basis of safe train operation, which directly affects the calculation of train headway, speed and train emergency braking curve. Before modeling and analyzing the MA generation scenario, we should first fully consider the system requirements, because the model established by formalization should be able to intuitively and accurately reflect the abstract attributes of the actual system. It is the starting point of formal modeling that understanding the system requirements.

In the process of MA generation, the most important thing is to obtain the conditions restricting the safe operation of the train, that is, the status and position information of obstacles. The specific process is described as follows: after the train goes online, the intelligent vehicle on board controller (IVOC) of train 1 applies for route from the dynamic capacity decision subsystem (DCD), and receives and analyzes the operation plan information sent by DCD. Train 1 requests to communicate with train control resource management unit (RMU), which receives and stores the basic information of train 1 and forwards all train information in the line to train 1. Subsequently, IVOC1 establishes communication with object controller (OC), queries trackside equipment status and requisitions movable resources [6].
The purpose of train sieving is to find out whether there are hidden trains in front of and behind the train within the shortest train length. During the actual operation of the train, the location reported to the on-board will have a certain measurement error, so it is necessary to calculate the safety location of the train. The front train identification module can identify the only front train of train 1 through information interaction with DCD and electronic map, and maintain periodic communication with the front train within the communication range. The ergodic obstacle module determines the terminal obstacle type in front of train 1 according to the above received information, and obtains the end of authority (EOA) position according to the ergodic results. Finally, MA information is calculated in real time through the received temporary speed restriction and other information, and ATP (automatic train protection) curve is generated to control the safe operation of the train. After analysis, the subsystems involved in MA calculation mainly include DCD, RMU, OC, IVOC1 and IVOC2. IVOC1 includes train sieving module, safety location calculation module, front train identification module and ergodic obstacle module.

3.2. System safety requirement analysis based on HAZOP

Stochastic hybrid automata mainly establishes the information interaction process between subsystems. HAZOP method can be used to analyze the uncertain factors existing in the interaction of information between interfaces. The communication interfaces mainly involved in the MA generation process include IVOC1 and RMU, IVOC1 and DCD, IVOC1 and OC, IVOC1 and IVOC2. Taking the communication interface between DCD and on-board as an example, the HAZOP analysis results are shown in table 1. The analysis shows that the uncertain factors in the whole MA generation process include subsystem failure, communication failure, communication delay and communication packet loss.

| interfaces | introducer | deviation            | cause                                      | consequence |
|------------|------------|----------------------|--------------------------------------------|-------------|
| on-board, DCD | None       | on-board did not receive plan | DCD fault, communication failure, on-board fault | collision   |
|            | Late       | on-board received delayed plan | DCD sending delayed plan, Communication delay | collision   |
|            | Error      | on-board received wrong plan | communication is damaged, DCD fault, on-board fault | collision   |
|            | Part of    | on-board received incomplete plan | DCD fault, packet loss during communication, on-board fault | collision   |

3.3. NSHA model generated by Movement Authority

The corresponding NAHS model is established according to the demand analysis, as shown in figure 1. Figure 1 (a) shows the DCD model of the subsystem. Firstly, after receiving the dcdcheck sent by IVOC1, the DCD subsystem performs fault inspection, which the time required for this operation follows the exponential distribution of $t_{44}$. The subsystem transfers to the ‘error’ state with the probability weight of parameter$\text{dcd1}$. If the subsystem is normal, DCD will send dcdpass information to IVOC1, and the location will be transferred to conDI. When receiving the application route request connectplan from IVOC1, DCD takes $\exp (t_{44})$ time to perform the necessary calculation and storage, and the probability weight of successfully sending the operation plan information plan to IVOC1 is $\exp (t_{22})$. And it is necessary to set ‘end-to-end transmission delay’ on SendPlan, i.e. $\exp (t_{13})$. Figure 1 (b) - (d) constructs the subsystem models of RMU, OC and IVOC2. Similar to the DCD model, it also includes communication delay, subsystem failure probability and communication failure probability. IVOC2 obeys the time delay of $\exp (t_{33})$ when sending information.

The modules of train sieving, safety location calculation, front train identification and ergodic obstacle module are abstracted into the subsystem function model according to the logic principle, which only complete the internal logic calculation of the model. The communication between subsystems other than IVOC1 is simulated by updating the ‘blue’ function and whether the ‘green’ guard condition is met, as shown in Figure 2 (e) - (h). The model $\text{obstraversal}$ represents the ergodic obstacle module. When
the on-board subsystem obtains the temporary speed restriction and other information, it sends *GetData* information to start the terminal obstacle calculation. If there is no platform within the train path, the EOA is the safe rear position of the front train. If there is a platform within the route inquiry range, the EOA is the beginning of axle counter in the platform area. After the EOA judgment is completed, the MA information is output. In this process, the information has the probability of loss with the weight of \( \text{loss1} \). Finally, MA generation is represented by the output of \( \text{MAinfor} \) information. In case of subsystem failure and communication failure, the consequences caused by the failure shall be determined according to the HAZOP analysis results, and the corresponding *collision*, *derailed* and *overspeed* information shall be output. After receiving such information, the on-board IVOC1 will be in the position of *fault1*, prompting the corresponding modules for maintenance, and the train shall brake in time.

![Diagram](image)

**Figure 1. NSHA model of MA generation**

### 4. Simulation analysis

In this paper, the model checking tool UPPAAL-SMC is used to model and verify the NSHA model. Firstly, various statements of the model are set in the editor, then the simulation operation in the simulator is running to observe whether the operation and state change of SHA model of each module
are consistent with the design expectation. The errors in the model can be modified in time according to the simulation operation. Deadlock is a priority attribute when verifying and analyzing the system model. Once the system enters the deadlock state during operation, other states including normal operation state will not appear. The model checking tool UPPAAL-SMC provides the query statements shown in equation (1) for deadlock verification, and the verification result meets this property. The safety of the system is further analyzed. It can be seen that the final state of the model includes output MA information and output system fault information. It is verified by equation (2), and the result is passed.

\[ A[] \text{not deadlock} \] (1)

\[ A <> (IVO1 \text{getMA} || IVO1 . fault1) \] (2)

On the premise of passing the above verification, the system is simulated. According to the description of MA generation scenario and the communication cycle between devices, the time period for completing mobile authorization is no more than 3000 ms. The system operation was simulated through equation (3) for 10000 times, the system output is normal within 3000 ms, that is, the time distribution of reaching the position getMA. The simulation results are shown in figure 2. It can be seen that the normal time of system output is scattered between 600-3000 ms.

\[ \text{simulate}[,<= 3000;10000];[IVOC1.getMA] \] (3)

| Table 2. reachability probability of MA generation failure |
|----------|----------|----------|----------|----------|
| p       | time 0.05 | time 0.02 | time 0.018 | time 0.016 |
| 1       | 8.9999e-8 | 9.5998e-7 | 6.4194e-5  | 3.1058e-4 |
| 2       | 1.7923e-7 | 1.0149e-6 | 7.5554e-5  | 3.2458e-4 |
| 3       | 2.6182e-7 | 1.1299e-6 | 8.1579e-5  | 3.3178e-4 |
| 4       | 3.5487e-7 | 1.2449e-6 | 8.7603e-5  | 3.4783e-4 |
| 5       | 4.4548e-7 | 1.3599e-6 | 9.3627e-5  | 3.6196e-4 |
| 6       | 5.3741e-7 | 1.4749e-6 | 1.0165e-4  | 3.8467e-4 |
| 7       | 6.2741e-7 | 1.5601e-6 | 1.2676e-4  | 4.0196e-4 |
| 8       | 7.1847e-7 | 1.69e-6    | 1.47e-4    | 4.3071e-4 |
| 9       | 8.0748e-7 | 1.7551e-6  | 1.6196e-4  | 4.5491e-4 |

Figure 2. normal time distribution of output  
Figure 3. cumulative probability generated by MA

When evaluating the probability of NSHA model, the parameter setting $\delta$ 0.001, $\alpha$, $\beta$ 0.0005, $\epsilon$ 0.0005. The network delay follows an exponential distribution, and the cumulative distribution function of the exponential distribution is shown in equation (4).

\[ F(x) = 1 - e^{-\lambda x} \] (4)
It can be seen that the smaller the delay, the longer the waiting time required to leave the location. Reference [7] shows that the value of end-to-end transmission delay is less than 150 ms (98%), so set $t_{11} = t_{22} = t_{33} \approx 0.02$. Because the information processing time and subsystem parameters are constantly changing in the train operation process, this paper mainly analyzes the impact of information processing time and fault parameters on the system. Setting the fault probability weight $\text{para-} = \text{loss} = p$ in figure 1, and the magnitude of the fault probability is $10^{-8}$. Changing the values of parameters $p$ and $t_{44}$, and calculating the reachability probability of MA generation failure in UPPAAL-SMC, that is, $P(\text{fault}) = 1 - \text{pr} \left[ <= 3000 \right]$ ($\leftrightarrow \text{IVOC1}.\text{getMA}$). The experimental results are shown in Table 2. The analysis shows that the existence of uncertain factors such as subsystem failure, communication failure, communication delay and communication packet loss have great influence on the generation process of MA. Therefore, the values of the above parameters should be adjusted to make the system reach the corresponding quantitative safety index when designing the system.

When the failure probability is $9 \times 10^{-8}$, $t_{44} = 0.02$, the calculated probability interval is $[0.998 998, 0.999 998]$ through 12837 simulation runs, and the relationship between running time and cumulative probability is obtained, as shown in figure 3. It can be seen that the time interval when the system has MA information output is $[600, 3000]$. The probability of MA calculation success in the first 900 ms is very small, reaching 99.9% at 2709 ms, and finally about 0.9 999 982 449 at 3000 ms, which meets the quantitative safety level QSL4 (failure probability < $10^{-5}$) [8].

5. Conclusion
According to the safety requirements of MA generation scenario, the uncertain factors existing in the interactive information between subsystems are analyzed by HAZOP method, and the causes and consequences of dangerous events are determined. Based on the principle of SHA and the results of safety requirements analysis, an NSHA model for MA generation is established, which dynamically describes the uncertain environment in the process of system operation. Finally, the above system model is analyzed qualitatively and quantitatively with SMC safety analysis method. The results show that the system is affected by uncertain factors during operation. In order to meet the corresponding quantitative safety level at the early stage of TcCBTC system design, the parameter values of uncertain factors should be set within a reasonable range, the communication delay between subsystems should be reduced and the speed of software processing data information should be improved. The method proposed in this paper can realize the safety analysis of TcCBTC system, has certain application value, and provides a theoretical basis for the further research of TcCBTC system.

Acknowledgments
This paper is jointly funded by National Natural Science Foundation of China (No.52162050) and Scientific research and development fund of China Academy of Railway Sciences Corporation Limited (No. 2021YJ232).

References
[1] BS EN 50128, Railway applications—communication, signaling processing systems—software for railway control protection systems [S]. 2011.
[2] David A, Larsen K G, Legay A, et al. UPPAAL SMC tutorial. International Journal on Software Tools for Technology Transfer [J], 2015, 17(4): 397-415.
[3] Zhao M Y, Chen X H, Sun H Y, et al. Formalizing railway interlocking domain specific language. Journal of Software [J], 2020, 31(6): 1638-1653.
[4] Chen M S, Bao Y X, Sun H Y, et al. Survey on formal method of trustworthy construction for communication-based train control systems. Journal of Software [J], 2017, 28(05): 1183-1203.
[5] David A, Du D H, Larsen K G, et al. Statistical model checking for stochastic hybrid systems. Electronic Proceedings in Theoretical Computer Science [J], 2012, 92(Proc. HSB 2012): 187-199.
[6] Zheng W. Research on modeling and verification of train-centric interlocking control[D]. Beijing: Beijing jiaotong university, 2019.

[7] T/CAMET 04006.4-2018, Long term evolution for metro (LTE-M)-interface specification. Part3: interface for CBTC. T/CA[S].

[8] Chen R J. The safety and reliability analysis methods for train operation based on hybrid automata[D]. Beijing: Beijing jiaotong university, 2019.