ARCHIVES OF TRANSPORT *ISSN (print):* *0866-9546*
Volume 61, Issue 1, 2022 ***e-ISSN (online):*** *2300-8830*
DOI: *10.5604/01.3001.0015.8147*

QUANTITATIVE SAFETY ANALYSIS OF TRAIN CONTROL SYSTEM BASED ON STATISTICAL MODEL CHECKING

Junting LIN[1], Xiaoqin MIN[2]

[1, 2] *Lanzhou Jiaotong University, School of Automation and Electrical Engineering, Lanzhou, China*

Abstract:

With the rapid development of communication technology, the Train-centric Communication-based Train Control (TcCBTC) system adopting the train-train communication mode to reduce the transmission link of control information, will become the direction of urban rail transit field development. At present, TcCBTC system is in the stage of key technology research and prototype development. Uncertain behavior in the process of system operation may lead to operation accidents. Therefore, before the system is put into use, it must undergo strict testing and security verification to ensure the safe and efficient operation of the system. In the paper, the formal modeling and quantitative analysis of train tracking operation under moving block are carried out. Firstly, the structure of TcCBTC system and the train tracking interval control strategy under moving block conditions are analyzed. The subsystem involved in train tracking and the uncertain factors in system operation are determined. Then, based on the Stochastic Hybrid Automata (SHA), a network of SHA model of train dynamics model, communication components and on-board controller in the process of train tracking is established, which can formally describe the uncertain environment in the process of system operation. UPPAAL-SMC is used to simulate the change curve of train position and speed during tracking, it is verified that the model meets the safety requirements in static environment. Finally, taking Statistical Model Checking (SMC) as the basis of safety analysis, the probability of train collision in uncertain environment is calculated. The results show that after accurately modeling the train tracking operation control mechanism through network of SHA, the SMC method can accurately calculate the probability of train rear end collision, which proves that the method has strong feasibility and effectiveness. Formal modeling and analysis of safety-critical system is very important, which enables designers to grasp the hidden dangers of the system in the design stage and safety evaluation stage of train control system, and further provides theoretical reference for the subsequent TcCBTC system design and development, practical application and related specification improvement.

Keywords: *statistical model checking, train control system, quantitative safety analysis, stochastic hybrid automata, UPPAAL-SMC*

To cite this article:

Lin, J., Min, X., (2022). Quantitative safety analysis of train control system based on statistical model checking. Archives of Transport, 61(1), 7-19. DOI: https://doi.org/10.5604/01.3001.0015.8147

Contact:
1) linjt@mail.lzjtu.cn [https://orcid.org/0000-0002-5763-5256],
2) 1947475837@qq.com [https://orcid.org/0000-0002-3374-4108] – corresponding author

1. Introduction

With the rapid development of urban rail transit construction, the safe driving distance between trains continues to shorten, consequently the safety requirements of trains have also improved. The train control system is the key factor to ensure the safe and efficient operation of trains on the line (Gao, 2018). At present, the reliable operation of the widely used Communication-based Train Control (CBTC) system, which depends on numerous ground equipment, has some problems such as low intelligence degree and complicated information interaction (Wang et al., 2018). In order to further optimize the structure of the train control system thus improving operation efficiency, it is imperative to develop a Train-centric CBTC (TcCBTC) system. This system integrates the functions of interlocking routes calculation and movement authority (MA) generation of the trackside equipment of CBTC system into the on-board equipment, which optimizes the system structure, and improves the integration degree of each subsystem. LTE-M technology is used in two-way and direct communication between trains with real-time and large capacity, which can simplify the complicated information interactions, as well as further improves the efficiency of train tracking operation while ensuring safety (Zhu et al., 2018). However, uncertain factors in the train operation process may affect the safe operation of the train. Therefore, to model and analyze the TcCBTC system operation process in an uncertain environment can timely find out the potential risks in the system requirements specification, subsequently providing a theoretical basis for TcCBTC development and the development of the train tracking operation plan of the TcCBTC system.

Train control system is a typical safety-critical system. Researchers always attached great importance to the safety of system operation in each stage of the whole life cycle of safety-critical system. In recent years, many researchers have investigated the safety of train control systems. The methods used are mainly divided into five classes. (1) the event chain-based analysis method; Guo et al. (2018) proposed a safety analysis method based on the combination of evidence theory and Failure Mode and Effects Analysis (FMEA). They provided a reasonable basis for evaluating the safety of the train control system by establishing a set of risk factors for temporary speed restriction and using evidence theory to identify conflicting evidences. (2) the probability graph model-based analysis method; Yang et al. (2016) and Zhang et al. (2020) built a Bayesian network model based on the conventional fault tree changes regarding to the common-cause failure, uncertain information and recovery mechanism problems in CTCS-3 (Chinese Train Control System level three). They not only identified the combination mode of leading to train control failures, but also found out the weak links of the system by combining its two-way thrust capability. (3) the network-based analysis method, Lin et al. (2020) verified the functional safety of the train control process in TcCBTC system based on CPN model, and proved that the modeling system has no design defects by using state space analysis. Wu et.al (2016) proposed a top-down approach of scenario-based modelling CPNs to design the on-board subsystem of a satellite-based train control system. (4) the system view-based analysis method; Regarding to the validation and security analysis problems of train control system in the demand stage, Liu et al. (2015) proposed a formal analysis method based on the system-theory process analysis theory. They transformed the control action temporal logic into a combination of equivalent simple logic formulas to analyze the improper control action through reduction rules. (5) the Statistical Model Checking (SMC)-based analysis method; Compared with other four types of methods, the SMC method is easy to implement, and effective to express the discrete, continuous and random behaviors and actions of the system. It can avoid the state space explosion problem through statical analysis of a small number of Trace samples generated by the system.

Stochastic Hybrid Automata (SHA) can be used to formal modeling and analysis of hybrid systems with random behavior. The SHA model can represent the discrete parts of the system by directed graph, and represent the dynamic properties of continuous parts of each discrete state with differential equations, and the modeling language has strict definition. SMC, a new proposed method in recent years, can be used to analyze and evaluate the security and reliability of large-scale complex systems (Du et al., 2015; Qiao et al., 2020). Its basic idea is to generate the system simulation Trace samples based on the model simulation. By analyzing the sample space with statistical method, the system attributes can be quantitatively evaluated. The SMC-based method has been successfully applied to safety analysis engineering in the rail transit field. For example, David et al. (2019) used Simulink and UPPAAL-SMC to formally model the movement

block signal system, and validated the feasibility of applying SMC method in the train control system. Bao et al. (2017) proposed an uncertainty AADL modeling method based on statistical model checking. Taking the mobile authorization scenario in CTCS-3 as the research object, the security and performance of the scenario in uncertain environment are quantitatively analyzed and evaluated. The existing research on analyzing the safety of train control system based on SMC method provides a basis for analyzing TcCBTC system in this paper. At present, there are few papers on formal modeling and safety analysis of TcCBTC system. More importantly, the research of the existing TcCBTC system mainly focused on using the static modeling technology to conduct simulation analysis on the related properties of the system, which was difficult to reflect the uncertain operating environment of the system. Therefore, how to accurately describe the operation process of TcCBTC system and analyze the system safety deserves further research. The research gaps inspire us to adopt the SMC method based on SHA model to quantitatively analyze the safety under an uncertain environment in the TcCBTC system.

The remainder of this paper is organized as follows. The Section 2 illustrates the system-level functional requirements structures of the TcCBTC and the control strategy of train tracking in section under moving block condition. In Section 3, we present an overview of the model-based safety analysis method, which provides preparation for formal modeling and safety analysis of subsequent TcCBTC system. In Section 4, this paper introduces how to model the discrete behavior, continuous behavior and random behavior of train operation in TcCBTC system. Then, through the static simulation analysis in UPPAAL-SMC, the correctness of the model is proved. Finally, the safety of the system model is quantitatively analyzed based on SMC method. We conclude our work in Section 5.

2. TcCBTC system

2.1. Structure of TcCBTC system

Fig. 1 shows the structure of TcCBTC system. The TcCBTC is a distributed control system with intelligent on-board equipment as the core that breaks the ground Zone Controller (ZC) centralized control method of conventional CBTC system. The TcCBTC system is mainly composed of an Intelligent Vehicle On-board Controller (IVOC), ground equipment, and Data Communication System (DCS) (Guo, 2019). Among them, the IVOC includes an interlocking calculation module, a train-train communication management module, an electronic map module, a movement authority calculation module, an overspeed protection module, an automatic train speed measurement and safety positioning module, as well as an automatic train operation module. The ground equipment mainly includes Resource Management Unit (RMU), Dynamic Capacity Decision (DCD), ground balise, Object Controller (OC) and other trackside equipment (such as switch), etc. The DCS mainly includes train-train communication network, train-ground communication network (Chrzan, 2021) and ground wired network.

The ground equipment of traditional CBTC system transmits the information such as the section status in front of the train, the current position of the train and the end of authority for the train to the on-board equipment (Zhang et al., 2020). The TcCBTC system integrates more functions of the train control system into the on-board equipment, such as ZC calculating MA and Computer-based Interlocking (CBI) calculating interlocking route in CBTC, which greatly simplifies the functions of the ground equipment. The IVOC communicates with OC to obtain the real-time status of the switch, Emergency Stop Button (ESB), and Platform Screen Door (PSD), and reserves movable resources. Meanwhile, train MA is calculated by receiving line information and location information of corresponding trains. Then it calculates train safety protection curve in real time according to the end of authority, the line information and running status of the front train under the moving block condition. The IVOC ensures automatic and safe operation of trains by supervising the safety protection curve (Wang et al., 2018). The TcCBTC system solves the problem that the existing CBTC system is highly dependent on the trackside equipment. It also reduces the control information transmission links and enhances system operation reliability, consequently cutting the construction, maintenance and operation costs of trains and line facilities, and further improves the operation capacity of the rail transit system.

2.2. Analysis of two-train tracking scenario

This study takes the tracking operation process of two mutually communicating trains in TcCBTC system as the modeling background, and the minimum safe tracking distance d as validation criteria. In TcCBTC system, the following train tracks the front train with

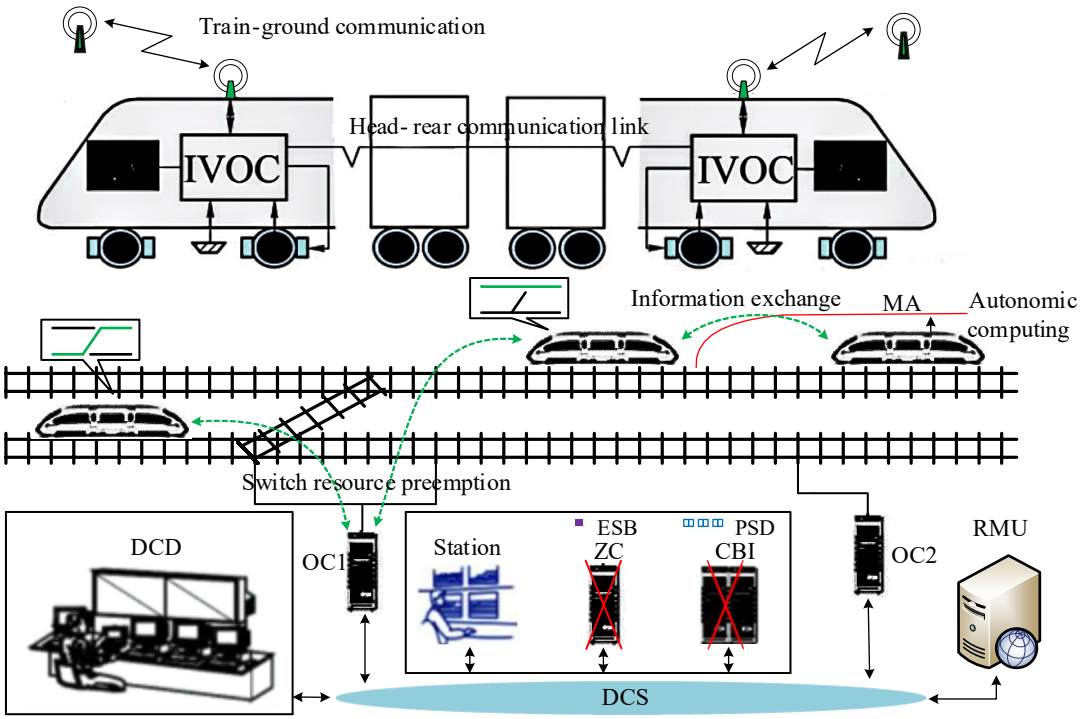


Fig. 1.Architecture of TcCBTC system

'hit soft wall' mode as shown in Fig. 2, that is the tracking terminal is the real position where the front train stops after emergency braking (Pan, et al, 2018). In the process that the following train tracks the front train, the IVOC of following train first analyzes and stores the tracking plan sent by the DCD center, and its on-board computer interlocking determines the fixed resource status and arranges the route automatically. Then, the on-board equipment communicates with RMU. The RMU transmits the line status information to the following train after receiving and storing basic information of the following train. Finally, the following train communicates with all trains within the communication range through LTE-M. By querying the electronic map, the unique front train ID of the local train is determined to maintain periodic communication with it. The IVOC of following train calculates the real-time MA according to the status information of the front train, and generates the automatic train protection (ATP) curve according to the minimum safe tracking distance in the movement block mode (Chen, 2019). The train thus is controlled within the minimum safe tracking distance d for safely running.

By summarizing the tracking interval of the train under the 'hit soft wall' mode and referring to Chen's research (2019), it can be seen that the minimum safe train tracking distance d of TcCBTC system in Fig. 2 was calculated by:

$$d = D_R + L - D_F \tag{1}$$

where, D_R is the braking distance required by the following train from triggering emergency brake to the train stop under the worst situation. D_R is calculated with Eq. (2). L is the safety margin reserved by the system. D_F is the braking distance required by the front running train from triggering emergency brake to the train stop under the best situation (note: the braking is instantly completed from triggering to taking effect). D_F is calculated by Eq. (3).

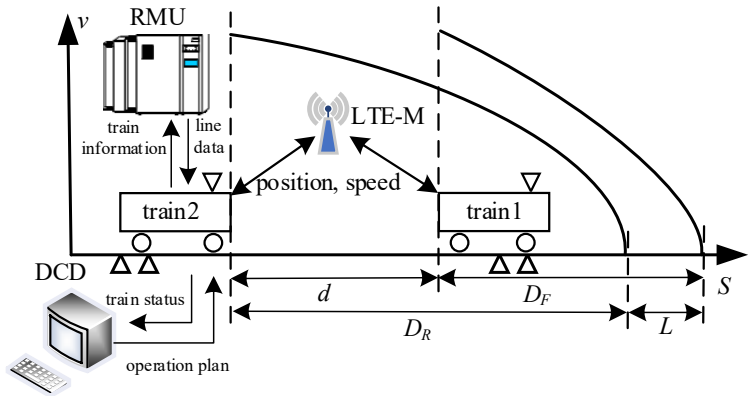


Fig. 2. TcCBTC system of train tracking scenario

$$D_R = v_2 t_1 + \frac{1}{2} a_{rq} t_1^2 + (v_2 + a_{rq} t_1) t_2 + \frac{1}{2} a_{rd} t_2^2 + \frac{(v_2 + a_{rq} t_1 + a_{rd} t_2)^2}{2 a_{rw}} \quad (2)$$

$$D_F = \frac{v_1^2}{2 a_{fb}} \quad (3)$$

where, v_2 is the current running speed of the following train. t_1 is the sum of the reaction time and the traction cut-off time of the ATP equipment of the following train, during this period, the train runs with the maximum traction acceleration. a_{rq} is the maximum traction acceleration of the following train. t_2 is the sum of the extra time for brake establishment and the emergency brake establishment time of the following train. a_{rd} is the maximum coasting acceleration of the following train. a_{rw} is the emergency braking acceleration of the following train under the worst situation. v_1 is the speed of the front train. a_{fb} is the braking acceleration of the front train under best situation.

3. Model-based safety analysis method

3.1. Stochastic hybrid automata

Considering that the time, speed and displacement during train operation belong to continuous behaviors, DCD representation belongs to discrete behaviors, and the transition of communication states and the distribution of communication delay have uncertain characteristics. Therefore, SHA was used to formally model the behavior of the system. The SHA model is an extension of the time automata, which can realize the clock change with different rates at different positions (David et al., 2015). The transition between states can be represented by discrete probabilities.

Definition 1: stochastic hybrid automata consist of a seven-tuple (Zhao et al., 2020), namely $SHA = (L, l_0, X, \Sigma, E, R, I)$. Where, L is a finite set of location. l_0 indicates the initial location. X is a finite set of clocks. Σ is a finite set of input and output actions. E is a finite set of transition edges, each of which contains a source location, a guard, an action, a set of clocks to be reset and a target location, that is, $(l, g, a, Y, l') \in E$. $R(l)$ is a time delay function on the location. $I(l)$ is an invariant declaration in location.

Multiple concurrent SHA interact through broadcast channels and shared variables, consequently forming a network of SHA (NSHA). The SHA components realize the uncertainty of the SHA model by setting the time delay function and the probability distribution of the state transition.

Definition 2: the transition rules between SHA:

(1) the transition of actions. The state of the system is $(l, v) \in L \times R_{\geq 0}^{X}$, where $v \models I(l)$. If there is a transition (l, g, a, Y, l') that makes $(l, v) \xrightarrow{a} (l', v')$ true, then $v \models g$, and $v' = v[Y]$.

(2) the transition of delayed, for state transition $(l, v) \xrightarrow{d} (l, v')$, where the delay $d \in R \geq 0$, the state remains unchanged, and the clock variable is $v' = v + \int_{v(\tau)}^{v(\tau)+d} R(l) d\tau$. Here, τ is the system clock, and $v(\tau)$ represents the system time to enter location l.

3.2. Statistical model checking and UPPAAL-SMC

SMC is a simulation-based analysis method, which can be seen as a trade-off between testing and formal validation. The main principle is to monitor its running track and validate whether the model satisfies specific properties through multiple simulations of the system. Then statistical analysis methods were used to obtain the probability value that the system model satisfies the attribute constraints at a certain confidence interval, and subsequently evaluating the safety of the entire system. The SMC method depends on the formal model of the system, which can explain the complex behavior characteristics of the system based on the formal semantics of the system (Lin et al., 2021).

This study mainly uses SMC to solve quantitative analysis problems. Quantitative analysis based on Monte Carlo simulation calculates the probability estimation interval $[p-\varepsilon, p+\varepsilon]$ generated with $p = P(\varphi)$ by running N times when the confidence is 1-α, where α is the significance level, and ε is the approximate parameter. According to the results of the above algorithm, if the repetition interval is estimated as N times, when $N \to \infty$, there are at least (1-α)N random runs that satisfy the specified attributes in the probability confidence interval of $p \pm \varepsilon$.

In order to better describe the random behavior of complex networks, researchers combined with the principle of SMC and proposed UPPAAL-SMC tool based on UPPAAL (David et al., 2012). UPPAAL-SMC, as an extension of the real-time validation tool UPPAAL, possesses the characteristic of effectively analyzing the NSHA model under natural random semantics. This tool not only supports UPPAAL standard model checking queries, but also provides many new query statements related to the random semantics of time automata. It allows user to visualize the value of the expression during simulation running, and better understand the behavior of the system through simulation. The simulation operation is realized by Eq. (4), where N is the time of simulations, and $E_1,...,E_k$ are k state-based expressions to be simulated and visualized.

$$simulate[<= bound; E]\{E_1,...,E_k\} \tag{4}$$

The query statement for probability calculation is shown in Eq. (5):

$$Pr[<= bound](< \ > expr) \tag{5}$$

where, *bound* is a natural number, which represents the time required for simulation; *expr* is the expression of system state. Eq. (5) expresses the probability of the system finally reaching the state *expr* within the specified time limit *bound*.

4. Simulation and analysis of train tracking operation model

4.1. The SHA model of front train

In the safety analysis of the train tracking operation process, it is assumed that the front train operates in un-faulty condition because this study mainly investigates the failure caused by the uncertain factors in the following train operation process.

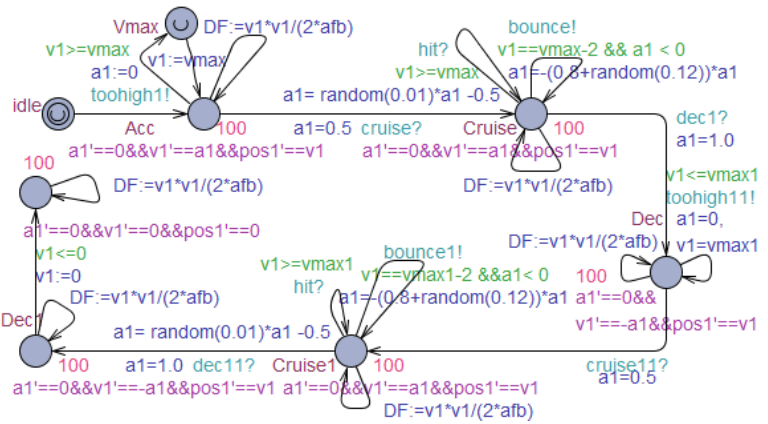


Fig. 3. The dynamic model of the front train

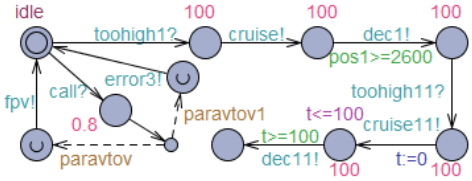


Fig. 4. Front train controller

The SHA model of the front running train includes the dynamics model shown in Fig. 3, and the controller model is shown in Fig. 4. The model includes train acceleration, cruise, and normal braking operation processes. **idle** is the logical starting location of the front running train. The running process of the front train is described as follows: the cycle starts at **idle** location, then enters the **Acc** location immediately (by setting the 'urgent' state on the location), and the train accelerates before speed reaches the speed limit value. The invariant 'a1'==0&&v1'==a1&&pos1'==v1' suggests that the acceleration change value is 0, the speed change value is a1, and the position change value is v1. When the speed reaches the limit value, the on-board equipment immediately sends speed warning message **toohigh1** to the controller. Then the controller sends the **cruise** command to the on-board equipment to make the speed of train 1 fluctuate between [vmax-2, vmax] (where 2 is the speed limit margin) till the pos1 reaches 2600m. The train1 then decelerates and enters the next speed limit section. After running for 100s in this section, the train1 brakes until it stops. The relevant variable declarations in Fig. 3 and 4 are shown in Table 1.

4.2. The SHA model of following train

Trains track in a movement block mode, and the front train is used as the tracking terminal during the tracking process. The following train dynamically runs according to the position of the front train and the line resources. The modeling process is shown in Fig. 5 to 9.

Fig. 5 shows the communication model of the DCD center. After receiving the request **begin** of the tracking plan sent by following train, the DCD performs necessary calculations and storage, and the required operating time obeys *exp*(0.8). The probability of the final tracking plan information **traceplan** being successfully sent is **paravehicleland**. The DCD stores the basic train information **train2msg** sent by train 2 at the same time. The DCD should send the warning message **error1** when a communication failure occurs between DCD and following train.

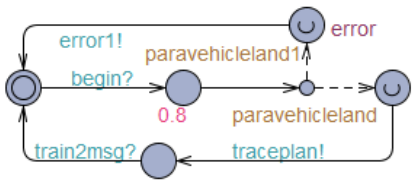


Fig. 5. DCD model

Table 1 Variable declaration of the front train motion model

Variable	Type	Significance
v1	clock	speed of front train
pos1	clock	position of the front train
a1	clock	acceleration of the front train
vmax、vmax1	int	speed restrictive value
toohigh1、toohigh11	channel	speed warning
cruise1、cruise11	channel	cruise command
dec1、dec11	channel	brake command
Acc	location	acceleration state
Cruise、Cruise1	location	cruise state
Dec、Dec1	location	brake state
hit	channel	clock sync message
bounce	channel	state triggering
DF	clock	emergency braking curve
pos1>=2600	boolean	speed restrictive position
call	channel	communication request of the following train
fpv	channel	message return
paravtov	int	communication normal weight

paravtov1	int	communication failure weight

Fig. 6 represents the sensor model. The speed measurement and positioning data is the core safety data for train control on the entire line. The emergency braking should be triggered once it lost. The sensor system performs necessary calculation and storage after receiving the positioning request and speed command **getsv** by on-board equipment, and the operation time follows exp(0.8). Lastly, return message **sv** was sent and the return value of the message loss function ***lost()*** was set as true. The message loss probability **datalost** is expressed in discrete form in SHA model, and the probability of complete message sending is represented by **datalost1**, as shown by the dotted line in Fig. 6.

Fig. 7 is the communication components of following train. It mainly completes data transmission with DCD and sensors, and communicates with front train in real time to exchange position and speed information. It sends the emergency braking command **eb** to on-board equipment in time when the warning message **error** is received.

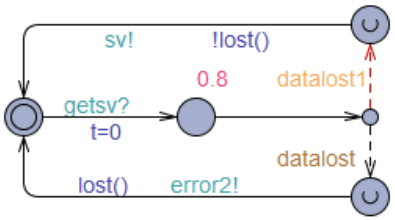


Fig. 6. Sensor model

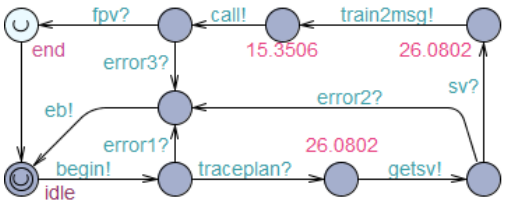


Fig. 7. Communication components

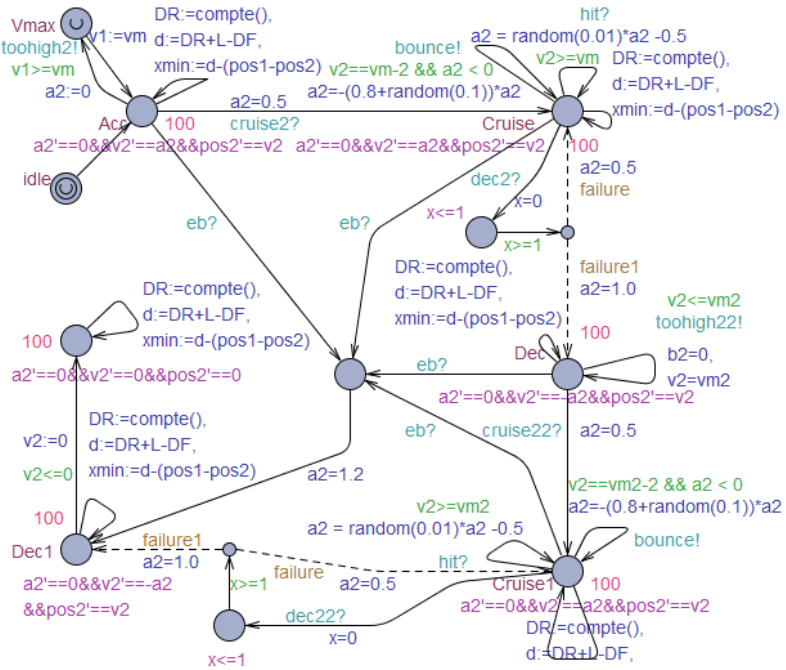


Fig. 8. The dynamic model of the following train

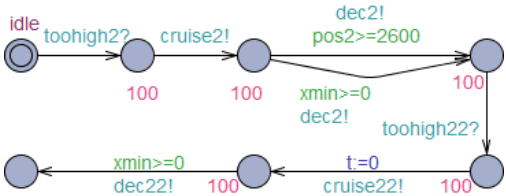


Fig. 9. The controller model of the following train

Fig. 8 and 9 show the dynamics model and controller model of following train. The operating process of following train includes acceleration, cruise and braking states. The train immediately enters the acceleration state from the **idle** location, and then enters the cruise state after the controller makes the train speed reach the speed restrictive value. After that, the controller determines whether to enter the next speed restrictive section by the condition 'pos2>=2600', or to make the deceleration of the train whether the actual train distance exceeds the minimum safe distance d by guard condition 'xmin>=0'. When the following train receives the braking request **dec2** (or **dec22**), the train enters the braking mode with a fixed control delay of 1s, and the control failure rate is represented by '**failure**', so that the train control command is in the state of the previous time. In the process of train tracking, the minimum distance control is implemented to ensure that the actual distance between two trains at each time is larger than the minimum safe distance d. In addition, emergency braking transfer is set in each state. When receiving emergency brake signal **eb**, the train slows down with a deceleration of 1.2m/s^2 till it stops. The emergency braking state can't be relieved midway until the train stops.

4.3. Model validation and result analysis

In the simulation process, some of our experimental parameter settings are referred to the current CBTC system parameter configurations in order to simulate the real scenario to a greater extent. For example, line parameters: the corresponding speed limit of the first speed limit section is 24 m/s; and the corresponding speed limit is 14 m/s after entering the second speed limit section at 2600 m. The configuration of train performance parameters is referred to Chen et al. (2019). The following assumptions are made combined with CBTC system train parameters: service braking is 1.0 m/s^2, traction acceleration is 0.9 m/s^2, emergency braking is 1.2 m/s^2, and the acceleration fluctuates between -0.5 ~ 0.5 m/s^2 during cruise. Train 2 tracks train 1, and the dynamic characteristics of the two trains are the same. The initial positions of the front and following train are 500 m and 0 m respectively, the initial speed is 0 m/s, and the safety protection distance is 200 m. In addition, considering the influence of uncertain factors on the train in the open environment, we set the failure rate of train-ground communication as 0.00107%, the failure rate of train-train communication as 0.0037% (Yao et al., 2018). The packet loss rate of communication as 0.01%, and the probability of brake failure as 0.00001% (Du et al., 2015).

The relevant parameters in Eq. (2) and Eq. (3) are set as follows: t_1=1.5 s, t_2=1.5 s, a_{rq}=0.9 m/s^2, a_{rd}=0.05 m/s^2, a_{rw}=1.2 m/s^2, a_{fb}=1.0 m/s^2 (Chen et al., 2019). The end-to-end communication delay obeys *exp*(26.0802), the train-train communication delay obeys *exp*(15.3506), and the necessary calculation and storage delay obeys exp(0.8) (Lin et al., 2021). Considering the cumulative distribution function $F(x) = 1 - e^{-\lambda x}$, the time delay should be as large as possible when a very short time interval is required at a certain point. The other position delays are set to obey *exp*(100) to ensure the continuity of the speed and position curves.

The simulation operation of the two trains tracking model was performed under normal scenario without setting fault migration. Eq. (6) validates whether there is a deadlock in NSHA, where no deadlock is the basic requisites for the model to work. Eq. (7) validates whether there is a path in which train2 can exceed train1. The result does not satisfy the validation, that is, it is impossible for the following train to collide with the front train under normal scenario.

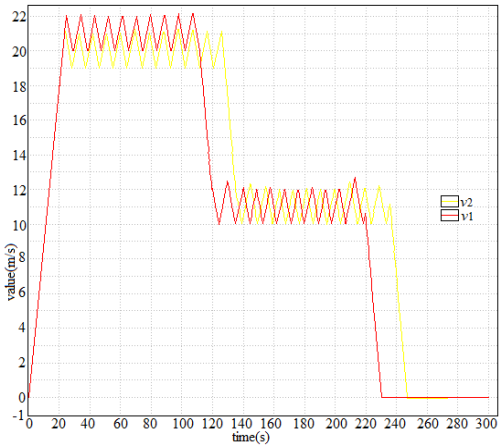
$$A[]\ not\ deadlock \tag{6}$$

$$E <> \ (pos2 >= pos1) \tag{7}$$

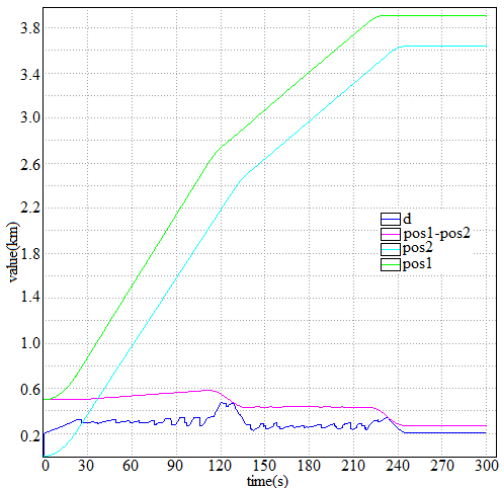
The two above Eqs. qualitatively analyzed the system model, and ensured the correctness of the system realization mechanism, that the system safety requirements were met. Then the statement *simulate [<=300;1] {v1, v2, pos1, pos2, d, (pos1-pos2)}* was used to query the operation of the two trains.

Fig. 10(a) shows the speed-time curve of the two trains in the tracking operation under normal scenario, which meets the line speed limit requirements. Train1 stops at 230.6s, and train2 stops at 247.9s. Fig. 10(b)

shows the position changes of the two trains over time. The initial distance between the two trains was 500m, and the actual distance between the two trains when they stopped was 261m. The figure also represented the changes of the minimum safe tracking distance curve d and the real distance curve pos1-pos2 of the two trains.



(a)Velocity time curve



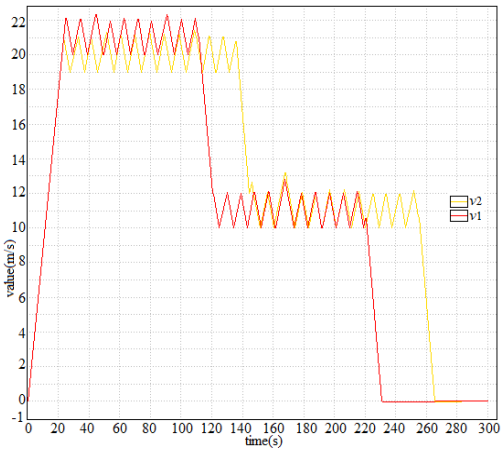
(b)Position time curve

Fig. 10. Train tracking operation without fault

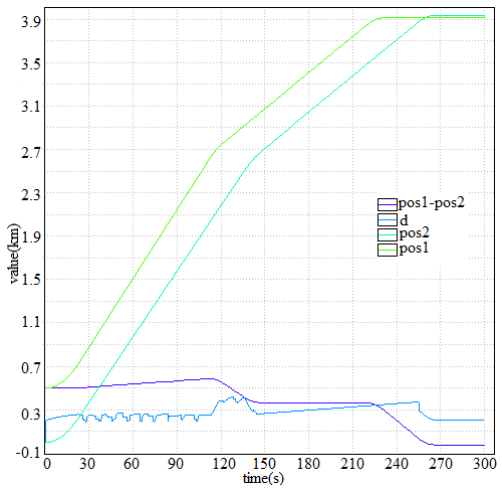
As can be seen from Fig. 10(b), the real distance of the two trains decreased with the increase of time, and the decrease of pos1-pos2 occurred near the junction of the two speed limit sections and the distance that the front train decelerated till it stopped. Because the front train firstly decelerated, the speed of the following train remained unchanged for a period of time, leading to a gradual decrease in the actual distance between the two trains. However, it is worth noting that the real distance between the two trains, pos1-pos2, is always larger than the minimum safe tracking distance d.

According to the model parameter configuration, the two-train tracking model was simulated after setting uncertain parameters such as fault probability and communication delay. Fig. 11(a) showed the speed-time curves of two trains when the following train failed to brake in time under uncertain scenario. Compared with Fig. 10(a), the speed change of the following train had a hysteresis, that the speed change was later than that of the normal scenario. Because the following train failed to brake in time but maintained cruise operation for a certain time due to some uncertain factors such as movement authority calculation error, communication failure, communication delay or communication packet loss when entering the second speed restrictive section or the guard condition 'xmin>=0' was met. Fig. 11(b) showed the position-time curves of two trains under an uncertain environment. The real distance between the two trains, pos1-pos2, decreased for the first time when the front train entered the second speed limit section until the following train entered the second speed limit section. The real distance pos1-pos2 between the two trains was close to the minimum safe interval d. At 227.2s, the real distance of two trains was less than the minimum safe distance d (satisfied the safeguard condition 'xmin>=0'), but the following train failed to brake in time due to the delay influence under uncertain scenario. The following train continued to run forward with the same speed, which adversely affected the safe operation of the train. It finally collided with the front train at 261.8s.

According to the simulation results of two-train tracking model under uncertain environment, there is possibility of collision between two-train. In order to calculate the probability interval of collision, the UPPAAl-SMC tool was used with the logic statement Pr[<=300](<> pos2>=pos1) to calculate the probability that the following train exceeds the front train within 300s. The probability interval of the final result is [2.17222×10^{-6}, 2.73584×10^{-6}] with 18579 simulation runs.



(a)Velocity time curve



(b)Position time curve

Fig. 11. Train tracking operation in uncertain environment

The cumulative probability with running time was shown in Fig. 12. It can be seen that the collision between trains unlikely happens in the first 192s. From 192s to 300s, the trains may collide, and the high-incidence area where the two trains collide is within 254s to 273s. The final cumulative probability at 300s is 2.56036×10^{-6}. It can be concluded that the probability of train collision is very low. However, these uncertain factors should be taken into consideration in the design stage, and effective prevention and control measurements should be carried out to minimize their influence on the normal operation of TcCBTC system, thus efficaciously improving the train control system safety.

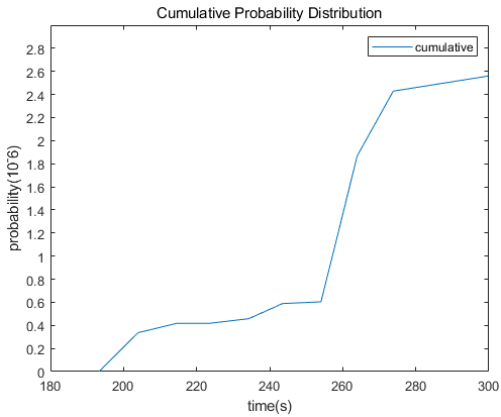


Fig. 12. Cumulative probability distribution plot for collision

5. Conclusion

Due to the redistribution of core functions, TcCBTC system has more advantages than CBTC system, which makes it more promising to become the future development direction of urban rail transit. A considerable amount of work has been done on the uncertain factors in the operation of train control system. Through modeling and quantitative analysis of the tracking process of train running in uncertain environment in TcCBTC system, the following conclusions were obtained:

1) The structure of TcCBTC system was analyzed and compared with traditional CBTC system. The analysis showed that TcCBTC system is more suitable for the development of rail transit field. According to the characteristics of TcCBTC system and the principle of "hit soft wall", the train tracking interval control strategy under moving block condition was obtained. According to the functional requirements, the subsystem model, information interaction requirements and uncertain environmental factors that participated in the train tracking process were obtained. In fact, there are more uncertain environmental factors and other factors to further explore.

2) Based on the SHA theory, the two-train tracking process model was established, and the continuous behavior, discrete behavior and random behavior in TcCBTC system are modeled. The train-train communication interaction environment and the uncertain

factors such as communication failure, communication delay and positioning error in the process of train operation were constructed, and the train tracking operation control mechanism was formally described. The shortcomings of traditional analysis methods in uncertain environment modeling were improved.

3) Through the quantitative safety analysis method based on SMC, the probability of collision between two trains in uncertain environment was calculated. The results showed that the cumulative probability of train-to-train collision in uncertain environment was approximately 2.56036×10^{-6} with 99.5% confidence. The experimental results showed that the uncertain environment affected the train running safety. Thus, it should be optimized to acceptable range in the design stage to reduce the operation risk. At the same time, it also proved the feasibility and effectiveness of SMC method in the safety analysis of complex hybrid systems.

In conclusion, our work aims to solve the lack of uncertain environment description in the formal verification analysis of TcCBTC system. After accurately modeling the train tracking operation control mechanism through SHA network, the probability of train tail collision can be accurately calculated by SMC method. In our future work, more standardized system specifications assist us to modify our models. Our models will consider more factors that the system runs in an uncertain environment, which makes it closer to the real running environment.

Acknowledgement

This paper is jointly funded by National Natural Science Foundation of China (No.52162050 and No.61763025) and Natural Science Foundation of Gansu Province (No. 20JR5RA375).

References

[1] Bao, Y. X., Chen, M., Zhu, Q., et al. (2017). Quantitative performance evaluation of uncertainty-aware hybrid AADL designs using statistical model checking, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 36(12), 1989-2002.

[2] Basile, D., Beek, M. H., Ferrari, A., et al. (2019). Modelling and analysing ERTMS L3 moving block railway signalling with SIMULINK and UPPAAL SMC, *Formal Methods for Industrial Critical Systems - 24th International Conference (FMICS).* Amsterdam, The Netherlands, 1-21.

[3] Chen, T. (2019). *Research on safety protection methods of train-centric CBTC system*. Beijing: Bejjng Jiaotong University.

[4] Chrzan, M., (2021). Study of the possibility of using transmission in the LTE system on a selected railway line for the purpose of running railway traffic. *Archives of Transport*, 57(1), 91-101.

[5] David, A., Du, D., Larsen, K. G., et al. (2012). Statistical model checking for stochastic hybrid systems. *Electronic Proceedings in Theoretical Computer Science*, 92, 187-199.

[6] David, A., Larsen, K. G., Legay, A., et al. (2015). UPPAAL SMC tutorial. *International Journal on Software Tools for Technology Transfer*, 17(4), 397-415.

[7] Du, D. H., Cheng, B., Liu, J. (2015). Statistical model checking for rare-event in safety-critical system. *Journal of Software*, 26(2), 305-320.

[8] Gao, C. H. (2018). *Communication-based Train Control System*. China Railway Publishing House. Beijing, (Chapter 2).

[9] Guo, H. N. (2019). *Online testing safety function of new train control system on-board ATP*. Beijing: Beijing Jiaotong University.

[10] Guo, S. N., Wu, X. C. (2018). Safety assessment of TSR processing function in train control center based on evidence theory. *Railway Standard Design*, 62(06), 156-160.

[11] Lin, J. T, Min, X. Q. (2021). Modeling and analysis of TcCBTC movement authority based on statistical model checking. *Control Engineering of China*, (20210119), 1-8.

[12] Lin, J. T., Xu, Q. (2020). Functional safety verification of train control procedure in train-centric CBTC by colored petri net. *Archives of Transport*, 54(2), 43-58.

[13] Liu, J. T., (2015). *A safety analysis method for high-speed railway train control system in requirements phase based on STPA*. Beijing: Beijing Jiaotong University.

[14] Pan, D., Luo, Q., Zhao, L. T., et al. (2018). A new calibration method for the real-time calculation of dynamic safety following distance under railway moving block system. *Mathematical Problems in Engineering*, 2018(PT.10): 3061034. 1-3061034.11.

[15] Qiao, S., Huang, Z. Q., Wang, J. Y., et al. (2020). DFT quantitative analysis method based on statistical model checking. *Systems Engineering and Electronic*s, 42(02), 480-488.

[16] Wang, H. F, Zhao, N., Ning, B., et al. (2018). Safety monitor for train-centric CBTC system. *IET Intelligent Transport Systems*, 12(8), 931-938.

[17] Wang, X., Liu, L., Tao, T., et al. (2018). Enhancing communication-based train control systems through train-to-train communications. *IEEE Transactions on Intelligent Transportation Systems*, 20(4), 1-18.

[18] Wu, D. H., Schnieder, E. (2016). Scenario-based modeling of the on-board of a satellite-based train control system with colored petri net. *IEEE Transaction on Intelligent Transportation System*, 17(11), 3045–3061.

[19] Yang, J. F., Zhang, Y. P. (2016). Reliability analysis on ATP system of CTCS-3 based on D-S evidence inference and Bayesian network. *International Journal of Control and Automation*, 9(7), 59-70.

[20] Yao, D. Y. (2018). *Reliability analysis of next generation train control data communication system based on DSPN.* Beijing: Beijing Jiaotong University.

[21] Zhang, F., Bu, B., Zhao, J. Y. (2020). Risk assessment method for information safety of train operation control system. *China Safety Science Journal*, 30(S1), 172-178.

[22] Zhang, Z. H., Wang, Y. R., Dang, J. W. (2020). Reliability analysis of on-board subsystem of train control system based on evidence theory and Bayesian network method. *Journal of Railway Science and Engineering*, 17(09), 2208-2215.

[23] Zhao, M. Y., Chen, X. H., Sun, H. Y., et al. (2020). Formalizing railway interlocking domain specific language. *Journal of Software*, 31(06), 1638-1653.

[24] Zhu, L., Yao, D. Y., Zhao, H. L. (2018). Reliability analysis of next generation CBTC data communication systems. *IEEE Transactions on Vehicular Technology*, 68(3), 2024-2034.