IET Intelligent Transport Systems

Research Article

IET Journals
The Institution of Engineering and Technology

Safety monitor for train-centric CBTC system

ISSN 1751-956X
Received on 2nd December 2017
Revised 11th May 2018
Accepted on 7th June 2018
E-First on 24th July 2018
doi: 10.1049/iet-its.2018.5231
www.ietdl.org

Haifeng Wang[1,2] ✉, Ning Zhao[3], Bin Ning[4], Tao Tang[4], Ming Chai[1,2]

[1]*National Engineering Research Centre of Rail Transportation Operation and Control Systems, Beijing Jiaotong University, Beijing, People's Republic of China*

[2]*Beijing Laboratory of Urban Rail Transit, Beijing, People's Republic of China*

[3]*Birmingham Centre for Railway Research and Education, University of Birmingham, Birmingham, UK*

[4]*State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing, People's Republic of China*

✉ *E-mail: hfwang@bjtu.edu.cn*

Abstract: Train-centric communications-based train control (TcCBTC) system is a new solution for urban transit signalling. Compared to traditional train control systems, the on-board equipment is becoming more powerful and more complex. Due to its safety-critical nature, specialised technologies must be adopted to guarantee the safety of the system. To address the safety verification difficulty of the control logic for the new system, this study presents an innovative topology-based method for guaranteeing the train control safety. First, a railway network is described as a metric space, and then, topological spaces are introduced to express the movement authority and train trajectory. On the basis of the topological description, the safety rules are checked by performing a series computation of topology theorems. Finally, a case study has been carried out on a real metro line in China. The result shows that the proposed method strictly meets the safety verification and achieves excellent performance.

1 Introduction

Communications-based train control (CBTC) system is a train control system developed for the urban rail transit. It aims to ensure train safety and assist in automated operations [1, 2]. Nowadays, the actual demands of passenger, operator and system supplier have started to move towards each other and meet at a point of system innovation. During the past years, a lot of works and research projects concerning the revolution of train control are sprung up all over the world. In order to address the future challenges, next-generation train control project, running in the frame of the EU FP7 programme, develops the convergence of both European train control system and CBTC system by investigating the commonality and differences of system requirement for mainline railway and urban transit [3]. With the intention of enhancing the functionality, safety and reliability of train control systems, a unified architecture was discussed in [4]. A substitution concept of railway operation based on a centralised train monitoring and processing and control without the use of interlocking systems and without the use of light signals was introduced in [5]. So as to innovate the railway operation, some solutions for the future train control system were also explored in Japan [6]. In China, numerous funds and programmes have also started to support the research on the innovation of train control technologies [7]. All these works show that one of the trends of next-generation train control system is that the on-board equipment will undertake more functionalities, and the on-board equipment will be smarter and further inclined to implement proactive safety. Train-centric communications-based train control (TcCBTC) system will be widely applied to urban lines with specific requirements. This trend has been put into practice in railway signalling industry [8].

In TcCBTC system, a number of additional functionalities are integrated into the on-board equipment, thereby increasing the challenges and risks. The system is very complex as it includes hundreds of different hardware devices, software components, huge amount of data, moving physical entities and an open environment. Unfortunately, such a complex design makes the system evaluation become difficult and time consuming. This is because the system safety properties and the control logic correctness are traditionally verified by different system testing and simulations.

Generally, classical approaches have been applied to deal with safety issues of critical systems [9–14]. Compared to traditional approaches, formal methods have become efficient ways to deal with safety critical issues in control system development since the 1990s [15, 16]. The standard EN50128 Railway applications for the safety of software for railway control and protection systems highly recommend the use of formal methods [17]. Over the past few decades, a large number of formal methods have been applied in railway safety critical applications [18–29]. However, some gaps still exist between academic formal methods and application [30].

From the authors' engineering practices, most of the ongoing researches are based on existing general methods, which do not perfectly response the train operation principles, and are inadequate to handle safety verifications for a complex TcCBTC system. During the past years, based on topology mathematics, the authors have made a lot of efforts on solving the modelling problems for the development of train control and railway signalling systems [31–33]. Essentially, these researches are based on discrete methods, and the train speed protection is not discussed. In this paper, considering the hybrid nature of TcCBTC system, the authors aim to establish a topology-based formal approach to guarantee the train safety. Addressed by topological space analysis, the train speed, protection curve and control logic are merged into a safety monitor. Additionally, a case study is carried out on a typical railway metro line, which evaluates the availability and performance of the method.

The remainder of the paper is organised as follows. Section 2 presents a description of the safety issue of TcCBTC systems. In Section 3, a topology-based safety guaranteeing method for train control systems is introduced. Section 4 describes the application of the method through a case study. Finally, Section 5 shows the conclusions.

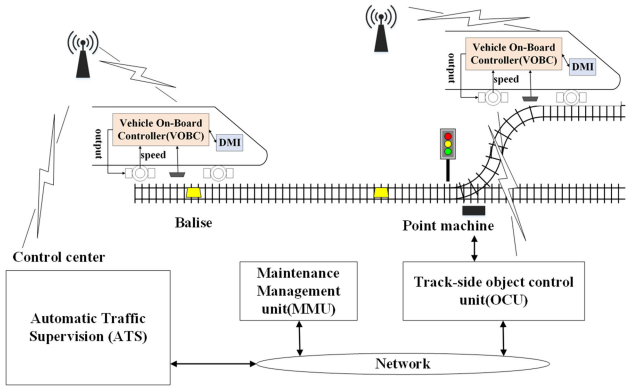

Fig. 1 *Architecture of TcCBTC system*

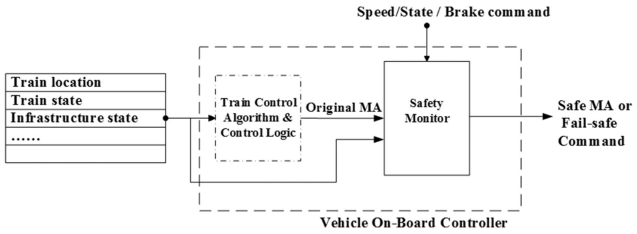

Fig. 2 *Schematic of TcCBTC safety monitor*

2 Safety issue of the TcCBTC system

2.1 TcCBTC system

A typical architecture of TcCBTC system is shown in Fig. 1. Different from conventional CBTC systems, in the new solution, parts of the route control and interlocking logic functions are moved to the on-board equipment. The track-side equipment is simplified to the maximum extent, and the conventional computer-based interlocking (CBI) system and zone controller (ZC) are no longer necessary.

The system mainly consists of automatic train supervision (ATS) subsystem, track-side object control unit (OCU) and the vehicle on-board controller (VOBC). In a TcCBTC system, movement authority (MA) calculation, automatic speed control and train operation are implemented by VOBC. The train locations are determined by on-board measuring equipment instead of track circuits or axle counters. The data transfer relies on continuous bi-direction communication between train on-board equipment and wayside control subsystems, ATS and OCU. Furthermore, the TcCBTC system supports direct train-to-train functional communication which can facilitate communication paths and achieve minimum information transmission times. In such a way, the track objects such as points, protection track sections preceding dangerous points and mask doors in platform are controlled by OCU, and they can be requisitioned via the communication between train and OCU directly. This makes the traditional interface between ZC and CBI sub-system unnecessary. The ATS subsystem monitors trains, adjusts the performance of individual trains to maintain schedules and provides data to adjust service to minimise inconveniences otherwise caused by irregularities. Timetable information is transmitted to VOBC from ATS, and the VOBC requests the track-side resources to the OCUs according to ATS command to set the route for the train. As a large amount of information can be transmitted in real time, the moving block principle is able to be implemented for train control.

2.2 Safety rules

Safety has been defined as freedom from unacceptable risk [34]. Functional safety refers to part of the overall safety relating to the equipment under control (EUC) and the EUC control system, which depends on the correct functioning of the safety-related systems, other technology safety-related systems and external risk reduction facilities. Compared with the understanding, this concept is difficult to be implemented in practice. In railways, the safety can be interpreted as no occurrences of collisions between trains, no derailments and no danger to passengers, the public and the environment. Train control safety is a complex system engineering problem. With respect to the principle and boundaries of the system, the safety impact factors for railway train control include the train state, infrastructure condition, control logic correctness, train driver performance, the maintenance work quality and the train operator skill. Overall, building a complete train control model is likely to be an impossible mission. Nevertheless, from the control system point of view, the safety is reflected in the control logic correctness under risk factors. In this paper, the authors focus on train control logic verification.

Essentially, train control and protection are implemented by the calculation and management of train movement authorities. Furthermore, speed protection function is also considered to confirm that the movement authorities are being executed correctly. For a CBTC system, the train MA is defined as follows.

A MA [2] is the authority for a train to enter and travel through a specific section of a track in a given travel direction. Movement authorities are assigned, supervised and enforced by a CBTC system to maintain safe train separations and provide protections through interlocking.

According to the system specification and risk analysis, the authors abstract function safety rules of train control, which are described as follows:

(i) Any device, infrastructure or information that may cause danger to trains must not be used by the train control system as an available element for calculating the train's MA, i.e. unlocked points or track sections, points with no position indications, unset routes, working area of rail line and so on;
(ii) If any element within the scope of the MA for a train enters a state that may cause danger to the train, for no matter what reason, the train control system must adjust the MA within a restricted time and the element should be removed from the MA. For example, if a point is contained in the MA of a train and the point suddenly turns while the train moves forward, it may cause a serious accident, so the MA must be reduced to limit the train such that it can stop before the point;
(iii) Considering the worst-case influencing factors and failure scenarios, the train control system shall confirm that the train will stop in a distance equal to or less than that restricted by the MA.

2.3 Schematic for safety monitor

A formal verification technique allows for the desired properties of a given system to be verified based on the system function model through exploring all states of the model. Conventionally, the system function is modelled with a kind of formal method. The designers define a set of properties with the same method, then perform state space checking to analyse whether the properties are satisfied.

In this paper, the authors proposed a safety monitor which is developed based on topology mathematics. Due to the complexity of the TcCBTC train control algorithm, it is difficult to use the mathematics directly to model and verify safety rules for the whole system. In this research, the major challenge is to provide system engineers and software designers with an efficient safety assurance method. As shown in Fig. 2, the safety monitor is implemented in a VOBC subsystem. The input of the model checker includes basic information for the MA algorithm, e.g. train data, line data and route states, the original MA generated by the train control algorithm, the speed and brake commands of the train. On the basis of topology mathematics, for the safety assurance model checker, the railway network is described as a metric space and the original MA for a train is abstracted as a topological space. The possible train trajectory is induced from the two parameters of speed and brake command and then also expressed as a topological space. Safety verification and assurance of the train are done by means of executing some topology-based safety property theorems. The output of the safety monitor is either a safe MA or a fail-safe command to the VOBC.

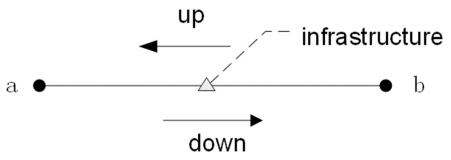

Fig. 3 *Track section of a railway network*

Table 1 Description of the parameters of section units

Section unit	ty	*s*	*l*
contains a signal	1	0 – failure 1 – proceeding aspect 2 – stop aspect	0 – released1 – route locked
contains a point	2	0 – indication unavailable 1 – normal position 2 – inverse position	0 – released1 – route locked
a plain track section	3	0 – unoccupied 1 – occupied by a train	0 – released 1 – route locked

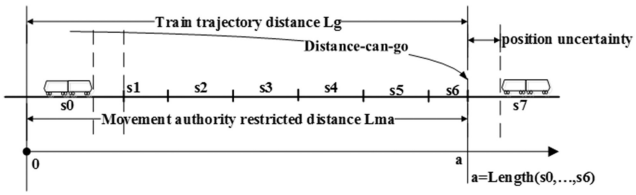

Fig. 4 *MA and train trajectory*

3 Topology based safety checking

Topology is a branch of mathematics which talks about the properties of topological spaces and the structures defined on them. It can be inherently used to describe the railway network characteristics. First, two fundamental definitions of topology are presented as follows, which are used as the basis of the method in this paper.

Definition 1: A metric space is a set X together with a real-valued function d given on $X \times X$ which satisfies the following axioms [35]:

1. D1.1a) $d(x, y) \geq 0$ for every pair $x, y \in X$ and $d(x, x) = 0$.
2. D1.1b) $d(x, y) = 0$ implies $x = y$.
3. D1.2) $d(x, y) = d(y, x)$ for every $x, y \in X$.
4. D1.3) $d(x, y) + d(y, z) \geq d(x, z)$ for every $x, y, z \in X$.

The first axiom states that the distance from x to y is non-negative and it is zero only if the two points coincide. The second axiom states that d is symmetric, the inequality which occurs in D1.3 is the so-called triangle inequality.

Definition 2: A topological space is a set U and a family of subsets O is called the open sets of the space such that the following axioms are satisfied [35]:

1. D2.1) $\varnothing \in O$ and $U \in O$.
2. D2.2) If $O_1 \in O$ and $O_2 \in O$, then $O_1 \cap O_2 \in O$.
3. D2.3) If $O_i \in O$ for every $i \in I$, then $\cup \{O_i : i \in I\} \in O$.

The second axiom implies that any finite intersection of open sets is open. The third axiom indicates that O contains all finite and infinite unions of sets $O_i \in O$. The family O is a topology defined on U, and the expression (U, O) is a topological space, where U is a non-void set. In simple, U can be assumed as a topological space.

3.1 Topology for train control

In this paper, a train is represented as a simple point. A railway network is composed of track sections from the train control logic point of view. Each section may contain an infrastructure component, e.g. point, signal and so on or just a plain-track section. Two directions, 'up' and 'down' exist for train operation. As shown in Fig. 3, a and b are endpoints of the section u. The authors use '1' to represent the up direction, and '−1' to indicate the down direction.

The authors choose the start point of the railway line in the down direction to be the origin of the reference coordinates. The section is denoted by a 6-tuple $\langle a, b, \mathrm{id}, \mathrm{ty}, s, l \rangle$, where a and b are endpoints of the section, id is identification of the infrastructure, ty is the type of the infrastructure, s is the state and l is the locking state of the infrastructure which is contained by the section. The authors write $u \cdot a$, meaning endpoint a of section u. The value of parameters of a section unit is noted in Table 1.

Then, a metric space for the railway network can be defined as follows.

Definition 3: The railway network is denoted by a metric space (X, d_X), for $x, y \in X$, where

$$d_X(x, y) = \begin{cases} 0, & \text{if } x = y \\ |y - x|, & \text{if } x \neq y \text{ and } x, y \text{ are linked} \\ \tilde{\infty}, & \text{if } x \neq y \text{ and } x, y \text{ are not linked} \end{cases} \quad (1)$$

where $\tilde{\infty}$ is a value greater than any distance between x and y in the space. The points x and y are linked means at a particular time, through the track sections and turnouts of the railway network, the train can reach point y from x. (X, d_X) satisfies the axioms of Definition 1 and it is indeed a metric space.

In a TcCBTC system, the VOBC computer calculates the protection profile curve required with a 'distance-to-go' principle, based on the distance restricted by the MA. IEEE 1747 presents a recommended brake model for the curve calculation [2]. The train's VOBC equipment monitors the speed of the train against the permitted speed limit. If the train goes above that speed, an emergency brake will be applied. Hence, the authors say that the train's behaviour is directly driven by the speed protection profile curve.

Equation (2) is a practical curve formula for VOBC

$$\frac{\mathrm{TV}^2}{2B_\mathrm{e}} + \left(t_1 + t_2 + \frac{at_1}{B_\mathrm{e}}\right)\mathrm{TV} + \left(\frac{1}{2}at_1^2 + at_1t_2 + \frac{at_1^2}{2B_\mathrm{e}}\right) - L_\mathrm{ma} = 0 \quad (2)$$

where L_ma is the distance that is limited by the MA, TV is the target speed, B_e is the emergency brake rate, t_1 is the safe braking response time of the system equipment, t_2 is the braking build-up time, a is the maximum acceleration.

Assuming that the train goes safely at a speed under the protection profile, no emergency brake is triggered. Inversely, replace the target speed (TV) with the current speed of the train (CV), the L_ma with the 'distance-can-go' L_g, then the authors can induce L_g by

$$L_g = \frac{\mathrm{CV}^2}{2B_\mathrm{e}} + \left(t_1 + t_2 + \frac{at_1}{B_\mathrm{e}}\right)\mathrm{CV} + \left(\frac{1}{2}at_1^2 + at_1t_2 + \frac{at_1^2}{2B_\mathrm{e}}\right) \quad (3)$$

As shown in Fig. 4, the area covered by the 'distance-can-go' curve is called the train trajectory area.

To verify the safety of train control logic, the original MA and train trajectory are abstracted as a topological space from the railway network metric space. The authors say that the metric space of a railway network is a continuous space. The MA calculation is based on interlocking routes for the train; it is a continuous part of the whole available route. As shown in Fig. 4, the MA includes track sections $u_0, u_1, u_2, \ldots, u_6$, and the length of these sections is the distance for the safety braking model of the train.

Definition 4: Let the track section sequence with order $\langle u_0 u_1 u_2 \ldots u_n \rangle$ be the MA calculated by the train control algorithm, X be the set which contains all section units of MA, and a family of subsets $\mathcal{T}$, the topological space $(X, \mathcal{T})$ is called a $V1$ space, which satisfies the following axioms:

1. D4.1) $\varnothing \in \mathcal{T}$, $\{u_0\} \in \mathcal{T}$ and $X \in \mathcal{T}$, u_0 is called the start unit of the space.
2. D4.2) If $\tau \in \mathcal{T}$ and $u_i \in \tau$, then $\tau \cup \{u_{i+1}\} \in \mathcal{T}$.

For the train trajectory, from (3), the distance-can-go L_g for the train is calculated. The following topological space can be considered as the possible behaviour result of the train at the current condition.

Definition 5: Let α be the location of the train on the railway network metric space, dir is the travel direction of the train, X is the set which contains all section units of the train trajectory and a family of subsets, the topological space $(X, \mathcal{T})$ is called a $V2$ space, which satisfies the following axioms:

1. D5.1) $\varnothing \in X$.
2. D5.2) if $d(\alpha, u_0 \cdot a) + d(\alpha, u_0 \cdot b) = d(u_0 \cdot a, u_0 \cdot b)$, then $\{u_0\} \in \mathcal{T}$, u_0 is called the start unit of the space.
3. D5.3) let $\tau \in \mathcal{T}$, for every $u_j \notin \tau$, if $d(\alpha, u_j \cdot a) < L_g$, $\mathrm{dir} \times \left[d(u_0 \cdot b, u_j \cdot a) - d(u_0 \cdot a, u_j \cdot a)\right] > 0$ and $d(\alpha, u_j \cdot a) = \min \{d(\alpha, u_k \cdot a): k \in I\}$ then $\{\tau \cup \{u_j\}\} \in \mathcal{T}$.

From this definition, a topological space for the train trajectory can be generated, for example, in Fig. 4, the space would be

$$(\varnothing, \{u_0\}, \{u_0\, u_1\}, \{u_0\, u_1\, u_2\}, \{u_0\, u_1\, u_2\, u_3\}, \{u_0\, u_1\, u_2, u_3\, u_4\},$$
$$\{u_0\, u_1\, u_2\, u_3\, u_4\, u_5\}, \{u_0\, u_1\, u_2\, u_3\, u_4\, u_5\, u_6\})$$

3.2 Safety checking

According to the definitions of $V1$ space and $V2$ space, based on topology mathematics, a safety checking method for train control is proposed in this section. First, some fundamental concepts of topology are proposed [33]. A set C in a topological space O is closed if its complement set is open. A topological space O is connected if the only sets in O which are both open and closed are the improper subsets $\varnothing$ and O. From this, the authors have a lemma that the space O is disconnected if and only if O is the union of two non-void disjoint open sets.

The following formula is for checking the interlocking state of a section unit:

$$h(u) = \begin{cases} 1, & \text{if interlocking state is available for the train} \\ 0, & \text{otherwise} \end{cases} \quad (4)$$

where the interlocking state refers to $u \cdot s$ and $u \cdot l$, it is determined by the OCU in the TcCBTC. If the section unit is occupied by a route, then the state of the unit should be locked, for sections with a point, the point should be at the required position by the route. The value '1' means that the section is safe for the train, '0' means unsafe.

Theorem 1: Let $(X, \mathcal{T})$ be a $V1$ space, $u_0 \in X$ is called the start unit of the space. There must exist a train with a location α satisfying $d(\alpha, u_0 \cdot a) + d(\alpha, u_0 \cdot b) = d(u_0 \cdot a, u_0 \cdot b)$.

It is immediately proven by means of Definitions 1 and 4. A $V1$ space is for describing the original MA generated by the train control algorithm. From the point of view of train control, the train must travel under a MA restriction, thus all of the MAs in the system must be generated for a particular train. This theorem will be used for checking the rationality of the original MA.

Theorem 2: Let $(X, \mathcal{T})$ be a $V1$ space, $(X, \mathcal{T})$ is safe if and only if for every point $u \in X$, $h(u) = 1$ is true.

In a TcCBTC system, an interlocking is an arrangement of infrastructures that prevents conflict between trains. Thus, the state of all units within an MA should be proved to be safe.

Theorem 3: If $(Z_A, \mathcal{T}_A)$ is a $V1$ space, $(Z_T, \mathcal{T}_T)$ is the related $V2$ space, $(Z_A, \mathcal{T}_A)$ and $(Z_T, \mathcal{T}_T)$ are safe for the train, then $(Z_A, \mathcal{T}_A)$ must be stronger than $(Z_T, \mathcal{T}_T)$, satisfy $\mathcal{T}_A \supseteq \mathcal{T}_T$ and $Z_A \supseteq Z_T$.

Proof: With respect to the definitions of $V1$ space and $V2$ space, $(Z_A, \mathcal{T}_A)$ and $(Z_T, \mathcal{T}_T)$ are possible topological spaces related to the train, Z_A, Z_T are subsets of railway network X. Due to the system principle, the train cannot run out of the MA restricted territory at any time. Otherwise it indicates that the train may move out of the MA area, thus it is unsafe. Hence, $\mathcal{T}_A \supseteq \mathcal{T}_T$ and $Z_A \supseteq Z_T$ holds. □

Theorem 4: If $(Z_A, \mathcal{T}_A)$ is a $V1$ space, $(Z_T, \mathcal{T}_T)$ is the related $V2$ space, $(Z_A, \mathcal{T}_A)$ and $(Z_T, \mathcal{T}_T)$ are safe for the train, then $\mathcal{T}_T$ on Z_T is the collection of sets $Z_T \cap U$ with $U \in \mathcal{T}_A$.

Proof: Using Theorem 3, it can be found that $Z_A \supseteq Z_T$. Let $j: Z_T \to Z_A$ be the inclusion map given by $j(y) = y$ for all $y \in Z_T$. Write $\sigma = \{Z_T \cap U : U \in \mathcal{T}_A\}$. Knowing that $\mathcal{T}_T$ is the smallest topology containing, since $Z_T \cap U = j^{-1}(U)$, if σ is shown as a topology on Z_T, then the result will follow. It is observed that:

(i) $\varnothing = Z_T \cap \varnothing$ and $Z_T = Z_T \cap Z_A$.
(ii) $\cup_{\alpha \in A} (Z_T \cap U_\alpha) = Z_T \cap \cup_{\alpha \in A} U_\alpha$.
(iii) $\cap_{j=1}^{n} (Z_T \cap U_j) = Z_T \cap \cap_{j=1}^{n} U_j$.

Therefore, Definition 2 is completely satisfied, σ is a topology on Z_T.

To ensure the train safety, it is necessary to prove that every step of the train is following a MA and at any time the trajectory space should not include an unsafe point; this can be verified with Theorem 4. □

Definition 6: Let (X, τ) be a topological space derived from railway network metric. The authors say that $x, y \in X$ are Authority Connected (Au-Connected) if (when $[a, b]$ is given its railway network metric) there exists a continuous function $\theta: [a, b] \to X$ with $\theta(a) = x \,.\, a$ and $\theta(b) = x \,.\, b$.

Theorem 5: If $(X, \mathcal{T})$ be a $V2$ space, then every pair of distinct points $x, y \in X$ are Au-Connected. In this case, X is a connected topological space.

Proof: Let θ be the inverse function of d; it is immediately proven by means of Definitions 3–5 that every pair of distinct points x, y is Au-Connected.

If X is not connected, say $X = A \cup B$ where A and B are non-void disjoint sets. Let $a \in A$ and $b \in B$ and let f be a function on an interval $[\alpha, \beta]$ with values in X and such that $\theta(\alpha) = a$, $\theta(\beta) = b$, then the sets $\theta([\alpha, \beta]) \cap A$ and $\theta([\alpha, \beta]) \cap B$ are non-void subsets of the separated sets A and B and hence they are separated. Their union $\theta([\alpha, \beta])$ is therefore not a connected set. Since the interval $[\alpha, \beta]$ is connected and the continuous image of a connected set is connected, θ cannot be a continuous function. This shows that the condition is sufficient.

If $V2$ spaces are connected, with respect to Theorems 3 and 4, the $V1$ spaces are then connected. The connectedness property is an important characteristic of $V1$ space and $V2$ space, Theorem 5 is used for checking the rationality of the control logic. □

Theorem 6: If (X, τ_1) and (Y, τ_2) are $V1$ space for different trains, the railway network is safe if and only if spaces (X, τ_1) and (Y, τ_2) are disjoint.

Proof: It can be immediately proven by means of train control principle, let (X, τ_1) be the space for Train 1 and (Y, τ_2) be the space

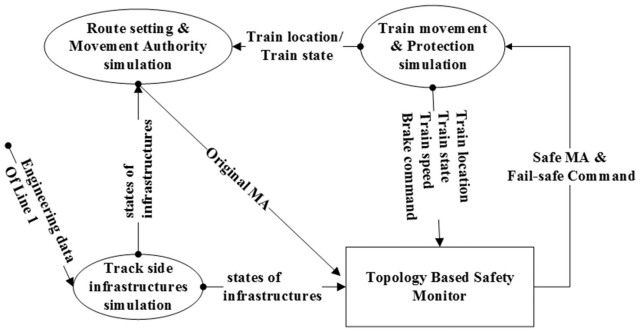

Fig. 5 *Schematic architecture of the case study*

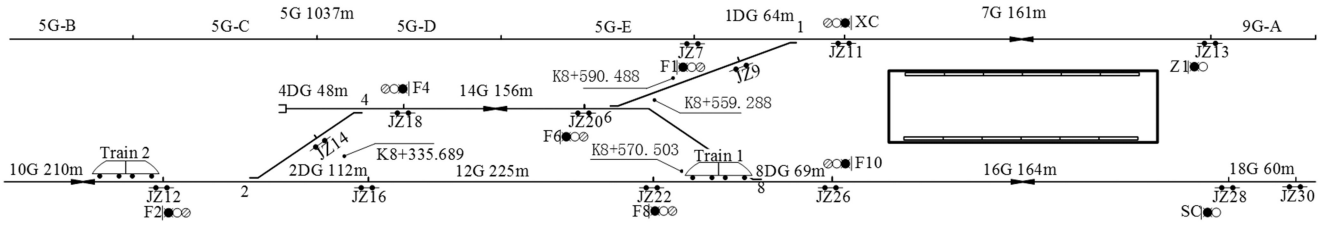

Fig. 6 *Part of the railway network from the Urumqi line 1*

Table 2 Engineering data of the example (note: K8 = 8000 m)

ID	Element	Engineering data Start point, m	Engineering data Endpoint, m	Contained infrastructure	Topological unit	Data construct
0	10G	K8 + 019.000	K8 + 229.000	plain-track	u_0	(8019, 8229, 0, 3, s_0, l_0)
1	F2	K8 + 226.000	K8 + 226.000	signal F2	u_1	(8226, 8226, 1, 1, s_1, l_1)
2	2	K8 + 322.000	K8 + 322.000	point no.1	u_2	(8322, 8322, 2, 2, s_2, l_2)
3	2DG	K8 + 229.000	K8 + 341.000	plain-track	u_3	(8229, 8341, 3, 3, s_3, l_3)
4	12G	K8 + 341.000	K8 + 566.000	plain-track	u_4	(8341, 8566, 4, 3, s_4, l_4)
5	F8	K8 + 563.000	K8 + 563.000	signal F8	u_5	(8563, 8563, 5, 1, s_5, l_5)
6	8	K8 + 613.000	K8 + 613.000	point no.2	u_6	(8613, 8613, 6, 2, s_6, l_6)
7	8DG	K8 + 566.000	K8 + 634.000	plain-track	u_7	(8566, 8634, 7, 3, s_7, l_7)
8	F10	K8 + 637.000	K8 + 637.000	signal F10	u_8	(8637, 8637, 8, 1, s_8, l_8)
9	train 1	K8 + 221.000	/	—	—	—
10	train 2	K8 + 605.000	/	—	—	—

for Train 2. If intersection $X \cap Y \neq \varnothing$, then it means that Train 1 can pass through the area of space (Y, τ_2), or Train 2 can pass through the area of space (X, τ_1). This must cause a collision between Train 1 and Train 2, hence it is unsafe.

This theorem can be used for checking the potential collisions between all of the trains within the CBTC system control area, to ensure the safety of the whole railway network. □

4 Case study

4.1 Simulation methodology

The case study of simulation considered in this paper is based on metro Line 1 in Urumqi, China. The Line 1 is currently under construction and will open in 2018. The length of the line is approximately 28 km long. It starts from Santunbei Station and ends at Urumqi Airport with 21 intermediate stations. Based on the layout of Line 1, a TcCBTC simulation system has been designed and developed. In this system, train protection and operation functionalities are implemented in a VOBC module. With respect to the safety checking principle shown in Fig. 2, the safety monitor is developed for the VOBC. To demonstrate the function of the safety monitor, the infrastructures state information is simulated by an OCU module. Moreover, the train control logic and train movement are also simulated in this case. The safety monitor and simulations are developed in MATLAB environment and the architecture of the case study is shown in Fig. 5. The train receives a new MA from the safety monitor at each control cycle. To verify safety, the model checker requires the infrastructure states, the original MA that was generated by the train control algorithm and parameters from the train. Based on these input data, topological spaces are formed and safety checking is performed by calculating the six theorems presented in Section 3. In this case study, 5000 infrastructure errors, original MA and train parameters are set at random intervals during each train journey, in which all types of error in the TcCBTC system are covered.

To demonstrate the safety checking approach in detail, an example scenario is presented, which is taken from Line 1 of the case study, as shown in Fig. 6, where F2, F8 and F10 are signals; 2 and 8 are points; 10G, 2DG, 12G, 8DG are track sections. In this scenario, three routes (from F2 to F6, from F6 to F8 and from F8 to F10) have been set for Train 1 and Train 2. The detail data of the example scenario is listed in Table 2.

According to the locations of the two trains, the topological units u_0 need to be adjusted using $u_0 = (8605, 8229, 0, 1, s_0)$. The safety checking approach can be divided into eight steps as follows.

Step 1: Let the track section sequence of the MA that is calculated by the VOBC subsystem be ⟨TRAIN2, 10G, F2, 2DG, 12G, F8⟩. With respect to Definition 4, the $V1$ space can be formed as follows:

$$(Q1, \mathcal{T}_A) = (\varnothing, \{u_0\}, \{u_0, u_1\}, \{u_0, u_1, u_2\}, \{u_0, u_1, u_2, u_3\}, \{u_0, u_1, u_2, u_3, u_4\}) \text{ and}$$
$$Q1 = \{u_0, u_1, u_2, u_3, u_4\}.$$

Table 3 Routes list considered in the case study

Up direction				Down direction			
Route ID	Number of point	Number of section	Number of signal	Route ID	Number of point	Number of section	Number of signal
1	3	3	2	101	1	2	2
2	0	2	2	102	0	2	2
3	0	2	2	103	0	3	2
4	0	2	2	104	1	2	2
5	0	2	2	105	0	1	2
6	0	2	2	106	0	2	2
7	0	2	2	107	0	2	2
8	1	2	2	108	2	3	2
9	2	3	2	109	2	3	2
10	0	3	2	110	0	2	2
11	0	3	2	111	0	3	2
12	0	2	2	112	1	2	2
13	1	2	2	113	0	2	2
14	0	3	2	114	0	3	2
15	0	3	2	115	0	4	2
16	1	2	2	116	1	2	2
17	3	3	2	117	0	2	2
18	0	1	2	118	0	2	2
19	0	2	2	119	0	2	2
20	0	2	2	120	1	2	2
21	1	2	2	121	0	2	2
22	0	3	2	122	0	2	2
23	0	2	2	123	2	3	2
24	1	2	2	124	1	2	2

Step 2: Let the current speed (CV) of Train 2 is 60 km/h; the emergency brake rate (B_e) is 1.10 m/s^2; the safe braking response time of the system equipment (t_1) is 1 s; the braking build-up time (t_2) is 3.5 s and the maximum acceleration (a) is 1 m/s^2. Using (3), the 'distance-can-go' can be calculated: $L_g = 221$ m. According to Table 2, track sections 10G and 2DG are included in L_g. Based on Definition 5, the $V2$ space for Train 2 can be built as follows:

$$(Q2, \mathcal{T}_T) = (\varnothing, \{u_0\}, \{u_0, u_1\}, \{u_0, u_1, u_2\}) \text{ and}$$
$$Q2 = \{u_0, u_1, u_2\}.$$

Step 3: Theorem 1 is used to check the start unit of topological space $Q1$. From the adjusted unit u_0 and the location of Train 2, the authors calculate $d(\alpha, u_0{\cdot}a) = d(8605, 8605) = 0$, $d(\alpha, u_0{\cdot}b) = d(8605, 8229) = 376$ and $d(u_0{\cdot}a, u_0{\cdot}b) = d(8605, 8229)$. Therefore, $d(\alpha, u_0{\cdot}a) + d(\alpha, u_0{\cdot}b) = d(u_0{\cdot}a, u_0{\cdot}b)$ is satisfied.

Step 4: According to safety checking Theorem 2, for every unit $u \in Q1$, $h(u)$ needs to be checked. Among sections 10G, 2DG and 12G, if any of the sections is occupied or unlocked, or Point 2 is not at its normal position, or Signal F8 shows a green or yellow aspect, then $h(u) = 0$. That is, the safety conditions for Train 2 are not satisfied.

Step 5: With respect to Theorem 3, the cardinality of $V1$ and $V2$ spaces can be checked. As $Q1 = \{u_0, u_1, u_2, u_3, u_4\}$ and $Q2 = \{u_0, u_1, u_2\}$, the authors have $\mathcal{T}_A \geq \mathcal{T}_T$ and $Q_A \supseteq Q_T$. Therefore, Train 2 is in a safe situation. Assume that the current speed (TV) of Train 2 is 60 km/h; B_e is 0.466 m/s^2; t_1 is 1 s; t_2 is 3.5 s and a is 1 m/s^2. Using (3), $L_g = 414$ m can be obtained. Thus, the $V2$ space for Train 2 can be calculated as follows:

$$(Q2, \mathcal{T}_T) = (\varnothing, \{u_0\}, \{u_0, u_1\}, \{u_0, u_1, u_2\}, \{u_0, u_1, u_2, u_3\},$$
$$\ldots \{u_0, u_1, u_2, u_3, u_4\}, \{u_0, u_1, u_2, u_3, u_4, u_5\})$$
$$Q2 = \{u_0, u_1, u_2, u_3, u_4, u_5\}.$$

Therefore, $\mathcal{T}_A \leq \mathcal{T}_T$ and $Q_A \subseteq Q_T$. That is, Train 2 is not in a safe situation.

Step 6: Then Theorem 4 can be used to check the relationship between the space $Q1$ and $Q2$

$$\Rightarrow \{u_0\} = Q2 \cap \{u_0\},$$
$$\Rightarrow \{u_0, u_1\} = Q2 \cap \{u_0, u_1\},$$
$$\Rightarrow \{u_0, u_1, u_2\} = Q2 \cap \{u_0, u_1, u_2\},$$
$$\Rightarrow \{u_0, u_1, u_2, u_3\} = Q2 \cap \{u_0, u_1, u_2, u_3\};$$
$$\Rightarrow \{u_0, u_1, u_2, u_3, u_4\} = Q2 \cap \{u_0, u_1, u_2, u_3, u_4\};$$

Therefore, for every open set S of the topological space $(Q2, \mathcal{T}_T)$, there is always an open U existing in the topological space $(Q1, \mathcal{T}_A)$. Such a result satisfies the equation $= Q2 \cap U$.

Step 7: According to Theorem 5, if the train control is in a safe situation, then for every pair of distinct points x, y within the MA territory, the authors have that x, y are Au-Connected. In this example, the spaces $Q1$ and $Q2$ are connected with each other. Let $V1$ space $Q1 = \{u_0, u_1, u_2, u_3, u_4\}$. It is assumed that there is an error existing (e.g. signal F2 is displaying a red aspect), and such error is not detected by the system. In such a situation, $L_g = 221$ m, and a connected space $Q2$ cannot be constructed. Therefore, it can be identified that the MA is in an unsafe situation.

Step 8: From Table 2, the $V1$ space for Train 1 can be calculated as $(Y, \mathcal{T}_T) = (\varnothing, \{u_5\}, \{u_5, u_6\}, \{u_5, u_6, u_7\}, \{u_5, u_6, u_7, u_8\}, \{u_5, u_6, u_7, u_8, u_9\}, \{u_5, u_6, u_7, u_8, u_9, u_{10}\})$. It is assumed that the $V1$ space of Train 2 is $(X, \tau_1) = (\varnothing, \{u_0\}, \{u_0, u_1\}, \{u_0, u_1, u_2\}, \{u_0, u_1, u_2, u_3\}, \{u_0, u_1, u_2, u_3, u_4\}, \{u_0, u_1, u_2, u_3, u_4, u_5\}, \{u_0, u_1, u_2, u_3, u_4, u_5, u_6\})$. Therefore, Train 2 can reach the unit u_7 (the track section 8DG). At this moment, if Train 1 still located in u_7 (the track section 8DG), a collision will occur. Therefore, it can be seen that Theorem 6 is used for checking the safety of different trains through the intersection of $V1$ spaces.

4.2 Simulation results

In total, there are 128 routes for the signalling system in Line 1. In this case, 48 main routes are considered and 24 routes in each direction. Components of these routes are listed in Table 3.

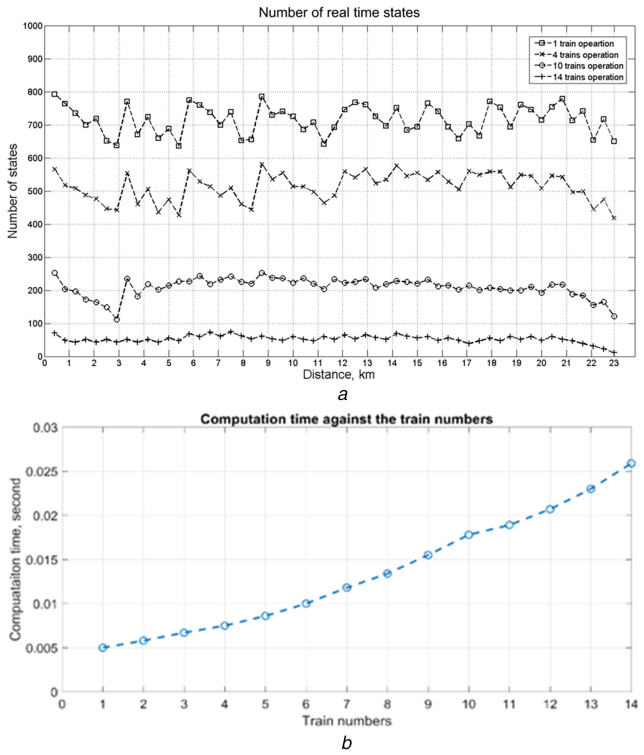

Fig. 7 *Case study simulation results*
(a) Number of real-time states, ***(b)*** Computation time against distance and number of trains

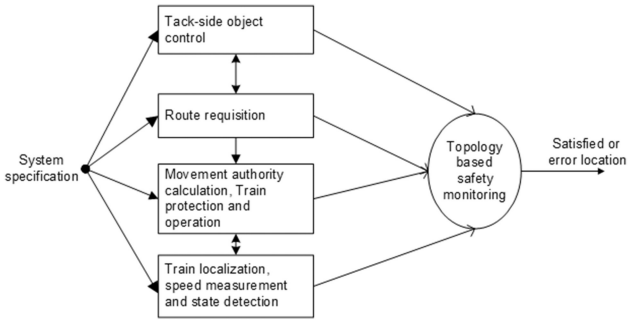

Fig. 8 *Topology-based safety monitoring for TcCBTC system*

The case study is implemented by using a computer equipped with Intel Core2 Q9550 (2.83 GHz) CPU and 3 GB memory. The computer is running Microsoft XP Professional SP3 and MATLAB version 7.11.0. The scalability of the proposed safety guaranteeing method is assessed by measuring the checking amount of states and execution time performance as the number of trains increase from 1 to 14. In this paper, five states for each point element are considered: (i) normal position, (ii) reverse position, (iii) normal position and locked, (iv) reverse position and locked and (v) position indication unavailable. For a track section, there are three states: (i) occupied, (ii) unoccupied and (iii) error. For a signal, there are four states: (i) green, (ii) yellow, (iii) red and (iv) error. Finally, a train has three states: (i) normal, (ii) brake and (iii) error. Fig. 7*a* shows the real-time checking amount of states; the numbers are collected as 1 train, 4 trains, 10 trains and 14 trains operating on the line. From this graph, the authors can deduce that the number of checking states is directly coupled with the number of elements within the MA; in other words, it relates to the route settings for the train. The maximum number in this graph shows that the state explosion problem of traditional model checking methods does not exist in our method.

Fig. 7*b* shows the performance of the safety monitor. The computation time covers the safety monitor, infrastructure simulation, train control simulation and train movement simulation. It can be observed that the average computation time for the one train operation is close to 5 ms, and the maximum computation time for 14 train operations is ∼26 ms, which totally fits for the real-time requirements of TcCBTC systems.

4.3 Discussion

In conventional formal verification techniques, safety properties are often characterised as 'nothing dangerous will happen', 'bad things should never occur' or 'deadlock will never happen'. Due to the complexity and huge number of states for the on-board equipment of a TcCBTC system, it is inadequate for existing techniques to model it. Furthermore, the safety properties of the system are difficult to describe with current tools.

In this paper, a new method for safety monitoring in TcCBTC systems is endeavoured to propose. Different from existing methods, the authors construct a topology-based safety model instead of traditional safety properties formalism. The safety model considers not only the safety rules of the system but also the abstraction of train control logic. On the basis of the safety model, safety checking is done by performing a series of topological theorems proofs. As shown in Fig. 8, due to the abstraction of the railway network metric space and the topological space description for the MA and train trajectory, both the route control and speed protection functional components of the TcCBTC system are handled by the safety model. Therefore, the proposed safety monitoring approach can verify the train control logic for the whole TcCBTC system.

In real train control system engineering, the time cycle of the VOBC subsystem is typically 200 ms; with respect to the performance result of the simulation, the safety model could definitely be integrated into the computing platform of the VOBC subsystem and could be synchronously executed with the train control algorithm module.

5 Conclusions

The method proposed in this paper is a novel topology-based technique for guaranteeing the safety of TcCBTC systems. The application of this methodology will contribute to achieve an even higher level of safety integrity for such systems. Essentially, this method provides topological operational semantics for railway networks, MA and the train trajectory, which are used for creating a safety model for the TcCBTC system. Particular aspects of the safety verification of the train control logic can be implemented with a series of precise calculation and proved based on topology mathematics. Consequently, the algorithm of the proposed method can be integrated into the VOBC subsystem of TcCBTC systems. Compared with the conventional manual system verification, the proposed methodology has significant advantages in terms of mathematical certainty.

A case study with a simulation model based on Urumqi metro Line 1 shows that the proposed method is suitable technique for guaranteeing the safety of TcCBTC systems. As the method originates from train control logic, it can be easily accepted in railway applications. Overall, the results of initial trials have been very promising, with a high performance of logic proving degree in the model implementation.

Considering the important results received from the methodology proposed in this paper, future research should be conducted to expand this model to other safety critical systems in the railway. However, the authors should also continue to improve the degree of automation of the method, and provide an easy to use development environment for system designers, which could assist the reduction of the system development cost.

6 Acknowledgments

This research was supported by the National Natural Science Foundation of China under grant 61473029, the Key Project of Chinese National Programs for Fundamental Research and Development (973 program) under grant 2014CB340703.

7 References

[1] Morar, S.: 'Evolution of communication based train control worldwide'. IET Professional Development Course on Railway Signalling and Control Systems (RSCS 2010), Birmingham, UK, June 2010, pp. 281–289

[2] IEEE 1474.1: 'IEEE standard for communications-based train control (CBTC) performance and functional requirements', 2004

[3] Gurník, P.: 'Next generation train control (NGTC): more effective railways through the convergence of main-line and urban train control systems', *Transp. Res. Procedia*, 2016, **14**, pp. 1855–1864

[4] Nakamura, H.: 'How to deal with revolutions in train control systems', *Engineering*, 2016, **2**, (3), pp. 380–386

[5] Ruf, A., Matejka, E., Sekaj, I.: 'Train control system without interlocking a new paradigm in railway control?'. Proc. of the Int. Conf. on Elektro, Rajecke Teplice, Slovakia, May 2014, pp. 490–493

[6] Nakamura, Y.: 'Overview of the next-generation railway operation system in the Tokyo metropolitan area'. JR East Technical Review, 2011, vol. **19**, pp. 3–6

[7] Wang, H., Li, K., Liu, H., *et al.*: 'Trend analysis of development on train control system technologies', *Railw. Signal. Commun.*, 2016, **52**, (8), pp. 1–4

[8] Pascal, P., Jacques, P.: 'Signal control systems innovations and future developments'. Proc. of the Institution of Railway Signal Engineers, London, UK, February 2015, pp. 56–66

[9] Quaglietta, E., Punzo, V.: 'Supporting the design of railway systems by means of a Sobol variance-based sensitivity analysis', *Transp. Res. C, Emerg. Technol.*, 2014, **44**, pp. 38–54

[10] Oukhellou, L., Côme, E., Bouillaut, L., *et al.*: 'Combined use of sensor data and structural knowledge processed by Bayesian network: application to a railway diagnosis aid scheme', *Transp. Res. C, Emerg. Technol.*, 2008, **16**, (6), pp. 755–767

[11] Beugin, J., Marais, J.: 'Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization', *Transp. Res. C, Emerg. Technol.*, 2012, **22**, pp. 42–57

[12] Li, S., Yang, L., Gao, Z.: 'Coordinated cruise control for high-speed train movements based on a multi-agent model', *Transp. Res. C, Emerg. Technol.*, 2015, **56**, pp. 281–292

[13] Song, H., Liu, J., Schnieder, E.: 'Validation, verification and evaluation of a train to train distance measurement system by means of colored petri nets', *Reliab. Eng. Syst. Saf.*, 2017, **164**, pp. 10–23

[14] Schnieder, E., Schnieder, L., Mueller, J.R.: 'Conceptual foundation of dependable systems modelling'. Dependable Control of Discrete Systems, Bari, Italy, June 2009, pp. 198–202

[15] Clarke, E.M., Wing, J.M.: 'Formal methods: state of the art and future directions', *ACM Comput. Surv.*, 1996, **28**, (4), pp. 626–643

[16] Woodcock, J., Larsen, P.G., Bicarregui, J., *et al.*: 'Formal methods: practice and experience', *ACM Comput. Surv.*, 2009, **41**, (4), pp. 1–36

[17] CENELEC: 'EN 50128: railway applications –communications, signalling and processing systems – software for railway control and protection systems', 2000

[18] Zingoni, N., Fantechi, A., Tempestini, M.: 'A story about formal methods adoption by a railway signaling manufacturer', *Lect. Notes Comput. Sci.*, 2006, **4085**, pp. 179–189

[19] Bodeveix, J.P., Filali, M., Lawall, J., *et al.*: 'Formal methods meet domain specific languages'. Int. Conf. on Integrated Formal Methods, 2005, pp. 187–206

[20] Haxthausen, A.E., Peleska, J., Kinder, S.: 'A formal approach for the construction and verification of railway control systems', *Form. Asp. Comput.*, 2011, **23**, (2), pp. 191–219

[21] Zimmermann, A., Hommel, G.: 'Towards modeling and evaluation of ETCS real-time communication and operation', *J. Syst. Softw.– Spec. Issue, Parallel Distrib. Real-time Syst.*, 2005, **77**, (1), pp. 47–54

[22] Barger, P., Schoen, W., Bouali, M.: 'A study of railway ERTMS safety with colored petri nets', *Reliab. Risk Saf., Theory Appl.*, 2009, **2**, pp. 1303–1309

[23] Amraoui, A.E., Mesghouni, K.: 'Colored petri net model for discrete system communication management on the European rail traffic management system (ERTMS) level 2'. UKSim-AMSS 16th Int. Conf. on Computer Modelling and Simulation, Cambridge, UK, 2014, pp. 248–253

[24] Damm, W., Mikschl, A., Oehlerking, J., *et al.*: 'Automating verification of cooperation, control, and design in traffic applications', in Jones, C.B., Liu, Z., Woodcock, J. (Eds.): *Formal methods and hybrid real-time systems*, Lecture notes in computer science vol **4700**, (Springer, Berlin, Heidelberg, 2007)

[25] Ghazel, M.: 'Formalizing a subset of ERTMS/ETCS specifications for verification purposes', *Transp. Res. C, Emerg. Technol.*, 2014, **42**, pp. 60–75

[26] Wang, H., Liu, S.: 'Study on model-based safety verification of automatic train protection system'. Asia-Pacific Conf. on Computational Intelligence and Industrial Applications (PACIIA), Wuhan, China, 2009, pp. 467–470

[27] Wang, H., Liu, S.: 'Modeling communications-based train control system: a case study'. Int. Conf. on Industrial Mechatronics and Automation (ICIMA), Wuhan, China, 2010, pp. 453–456

[28] Morzenti, A., Pradella, M., San Pietro, P., *et al.*: 'Model-checking TRIO specifications in SPIN'. Int. Symp. of Formal Methods Europe, Pisa, Italy, 2003, pp. 542–561

[29] Mekki, A., Ghazel, M., Toguyeni, A.: 'Validation of a new functional design of automatic protection systems at level crossings with model-checking techniques', *IEEE Trans. Intell. Transp. Syst.*, 2012, **13**, (2), pp. 714–723

[30] Parnas, D.L.: 'Really rethinking 'formal methods'', *Computer*, 2010, **43**, (1), pp. 28–34

[31] Wang, H., Schmid, F., Chen, L., *et al.*: 'A topology-based model for railway train control systems', *IEEE Trans. Intell. Transp. Syst.*, 2013, **14**, (2), pp. 819–827

[32] Wang, H., Tang, T., Roberts, C., *et al.*: 'A novel framework for supporting the design of moving block train control system schemes', *Proc. Inst. Mech. Eng. F-J. Rail Rapid Transit*, 2014, **228**, (7), pp. 784–793

[33] Wang, H., Xu, T., Yuan, T.: 'Novel online safety observer for railway interlocking system', *J. Transp. Eng.*, 2013, **139**, (7), pp. 719–727

[34] IEC 61508: 'Functional safety of electrical/electronic/programmable electronic safety-related systems', 2010

[35] Gaal, S.A.: '*Point set topology*' (Academic Press, USA, 1964)