# Safety monitor for Train-Centric CBTC System

Wang, Haifeng; Zhao, Ning; Ning, Bin; Tang, Tao; Chai, Ming

*DOI:*
10.1049/iet-its.2018.5231

*Citation for published version (Harvard):*
Wang, H, Zhao, N, Ning, B, Tang, T & Chai, M 2018, 'Safety monitor for Train-Centric CBTC System', *IET Intelligent Transport Systems*, vol. 12, no. 8, pp. 931–938. https://doi.org/10.1049/iet-its.2018.5231

# Safety monitor for Train-Centric CBTC System

Haifeng Wang[ad]*, Ning Zhao[b], Bin Ning[c], Tao Tang[c] , Ming Chai[ad]

[a] *National Engineering Research Centre of Rail Transportation Operation and Control Systems,*
*Beijing Jiaotong University, Beijing, China*
[b] *Birmingham Centre for Railway Research and Education, University of Birmingham, Birmingham,*
*United Kingdom*
[c] *State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing,*
*China*
[d]*Beijing Laboratory of Urban Rail Transit, Beijing, China*

**Corresponding author: hfwang@bjtu.edu.cn*

## Abstract

Train-centric Communications-Based Train Control system (TcCBTC) is a new solution for urban transit signalling. Compare to traditional CBTC, the on-board equipment is becoming more powerful and more complex. Due to its safety-critical nature, specialized technologies must be adopted to guarantee the safety of the system. To address the safety verification difficulty of the control logic for TcCBTC system, this paper presents an innovative topology-based method for guaranteeing the train control safety. Firstly, a railway network is described as a metric space, and then, topological spaces are introduced to express the movement authority (MA) 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.

Keywords: Train-Centric; Communications-Based Train Control; Safety monitor; Topology.

## 1 Introduction

CBTC is a train control system developed for the urban rail transit. It aims to ensure train safety and assist 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 sprang up all over the world. In order to address the future challenges, Next Generation Train Control (NGTC) project, running in the frame of the EU FP7 programme, develops the convergence of both European Train Control System (ETCS) 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 future train control system were also explored in Japan [6]. In China, there are also numerous funds and programmes have started to support the research on the innovation of train control technologies [7]. All these works show 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 furtherly inclined to implement proactive safety. Train-centric CBTC (TcCBTC) system will be widely applied to urban lines with specific requirements. And this trend has been being put into practice in railway signalling industry, Alstom had delivered a TcCBTC system, Urbalis Fluence, for Lille line 1 in France in 2015 [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 becomes 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 the safety issue of the critical systems. For example, in [9], the Sobol variance-based method was employed to determine sound design solutions for railway system. Similar issue was addressed in detection and diagnosis of broken rail for railway infrastructure, where Bayesian networks was adopted to analyse the sensor data [10]. In [11], by using the simulation of railway environments, the dependability and safety of satellite technique application in ERTMS system was assessed. Furthermore, a coordinated cruise control strategy for high-speed train control was designed based on LaSalles invariance principle in [12] . Compare to traditional approaches, formal methods have become efficient ways to deal with safety critical issues in control system development since the 1990s [13][14]. Based on mathematical techniques, the advantages of formal methods for the development of safety critical applications are widely recognized in the railway industry. The standard EN50128 Railway applications for safety of software for railway control and protection systems highly recommends the use of formal methods [15]. Over the past few decades, a large number of formal methods have been applied in railway safety critical applications [13][16][17]. Haxthausen et al. provide an approach for constructing and verifying tramway train control systems using Domain-Specific Language [18]. Petri Net is one of several popular mathematical modelling languages for the description of distributed systems. In order to achieve high safety and high quality braking, Zimmermann adopt Petri Net formalism to model the safety requirements of real time communication and operation of train control [19]. Using Coloured Petri Nets [20], Barger and Bouali modelled and analysed the safety of ERTMS[21]. Werner Damm, et al applied a verification methodology for cooperating traffic agents covering analysis of cooperation strategies, realization of strategies through control, and implementation of control to European Train Control System [22].

Pertinent work also was presented in [23], where model-checking technique was used to check the system specifications of ERTMS/ETCS. Wang and Liu presented a practice for the modelling and verification of train control systems in SCADE (Safety Critical Application Development Environment) [24][25]. In [26], Morzenti, A. introduced an application of model checking on the railway crossing problem through SPIN. Based on the translation of TRIO formulae into Promela programs, the system properties were verified. A model checking technique for the verification process of railway level crossings in Europe was presented in [27], and the specification of the level crossing was written in a formal notation of timed automata. However, some gaps still exist between academic formal methods and application [28].

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. A topology computational model of train movement authority under fixed-block signalling principle was presented in [29]. The train control logic was expressed by using point set topology methods. This method was extended to moving-block-principle train control system [30]. Furthermore, the point set topology mathematics was applied to railway interlocking system for online safety observation [31]. 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.

# 2 Safety issue of the TcCBTC system

## 2.1 TcCBTC System

A typical architecture of TcCBTC system is shown in Figure 1. Different from conventional CBTC systems [30], in the new solution, parts of the route control and interlocking logic functions are moved to the on-board equipment. The track-side equipment are simplified to the maximum extent, and the conventional Computer-Based Interlocking system (CBI) and Zone Controller (ZC) are no longer necessary.

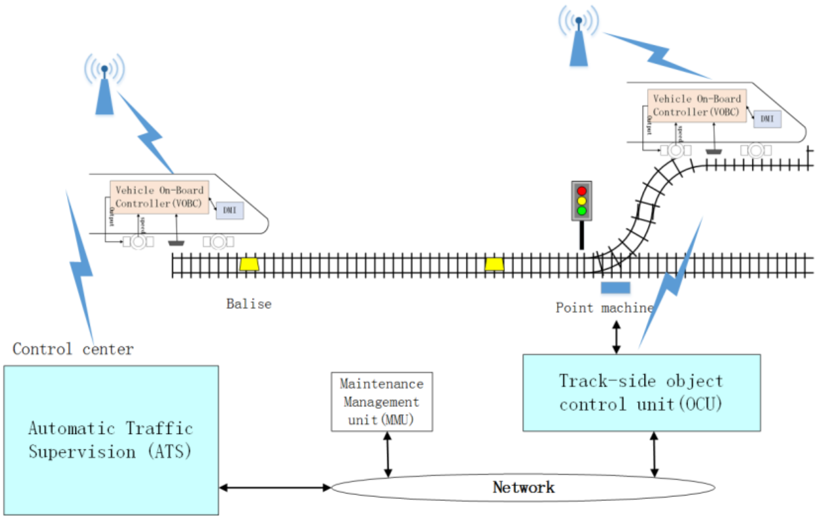
Vehicle On-Board Controller(VOBC)
DMI
Output
speed
Vehicle On-Board Controller(VOBC)
DMI
Output
speed
Balise
Point machine
Control center
Automatic Traffic Supervision (ATS)
Maintenance Management unit(MMU)
Track-side object control unit(OCU)
Network

**Figure 1 Architecture of TcCBTC system**

The system mainly consists of Automatic Train Supervision subsystem (ATS), 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 is rely 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 [33]. 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 [33]. Compared with the understanding, this concept, is difficult to be implemented in practise. 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 movement authority (MA) is defined as follows:

A movement authority [2] is the authority for a train to enter and travel through a specific section of 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.

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

(1) 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;

(2) 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;

(3) 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 Figure 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.

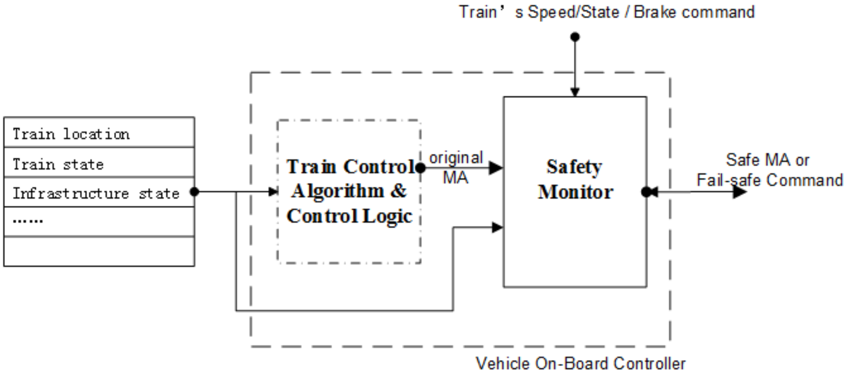
Train' s Speed/State / Brake command
Train location
Train state
Infrastructure state
……
Train Control Algorithm & Control Logic
original MA
Safety Monitor
Safe MA or Fail-safe Command
Vehicle On-Board Controller

**Figure 2.** Schematic of TcCBTC safety monitor.

# 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. Firstly, two fundamental definitions of topology are presented as follows, which are used as the basis of the method in this paper.

**Definition 1**: [34] A metric space is a set X together with a real-valued function d given on $X \times X$ which satisfies the following axioms:

D1.1a) $d(x,y) \geq 0$ for every pair $x,y \in X$ and $d(x,x) = 0$.

D1.1b) $d(x,y) = 0$ implies $x = y$ .

D1.2) $d(x,y) = d(y,x)$ for every $x,y \in X$ .

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 nonnegative 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 [34]:

D2.1) $\emptyset \in O$ and $U \in O$.

D2.2) If $O_1 \in O$ and $O_2 \in O$ , then $O_1 \cap O_2 \in O$.

D2.3) If $O_i \in O$ for every $i \in I$ then $\bigcup\{O_i : i \in I\} \in O$.

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 nonvoid set. In simple, $U$ can be assumed as a topological space.

## 3.1 Topology for Train Control

In this paper, the train is represented as a simple point. And the railway network is composed of track sections from the train control logic point of view. Each section may contains an infrastructure component, e.g. point, signal, etc. or just a plain-track section. Two directions, ‘up’ and ‘down’ exists for train operation. As shown in Figure 3, $a$ and $b$ are end points of the section $u$. The authors use ‘1’ to represent the up direction, and ‘-1’ to indicate the down direction.

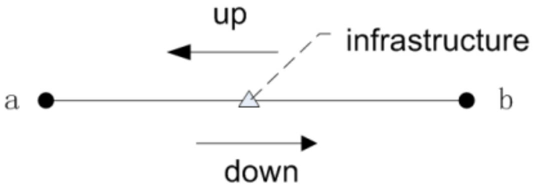

**Figure 3.** Track section of a railway network.

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 $< a, b, id, ty, s, l >$ , 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 $u.a$ , meaning endpoint a of section $u$. The value of parameters of a section unit is noted in Table 1as follows.

**Table 1.** Description of the parameters of section units.

| **Section unit** | $\boldsymbol{ty}$ | $\boldsymbol{s}$ | $\boldsymbol{l}$ |
|---|---|---|---|
| Contains a signal | 1 | 0 – failure<br>1 – proceeding aspect<br>2 – stop aspect | 0 – released<br>1 – route locked |
| Contains a point | 2 | 0 – indication unavailable<br>1 – normal position<br>2 – inverse position | 0 – released<br>1 – route locked |
| A plain track section | 3 | 0 – unoccupied<br>1 – occupied by a train | 0 – released<br>1 – route locked |

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

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

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 movement authority. 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,

$$\frac{TV^2}{2B_e} + \left(t_1 + t_2 + \frac{at_1}{B_e}\right)TV + \left(\frac{1}{2}at_1^2 + at_1t_2 + \frac{at_1^2}{2B_e}\right) - L_{ma} = 0 \tag{2}$$

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 Equation (3).

$$L_g = \frac{CV^2}{2B_e} + \left(t_1 + t_2 + \frac{at_1}{B_e}\right) CV + \left(\frac{1}{2}at_1^2 + at_1 t_2 + \frac{at_1^2}{2B_e}\right) \tag{3}$$

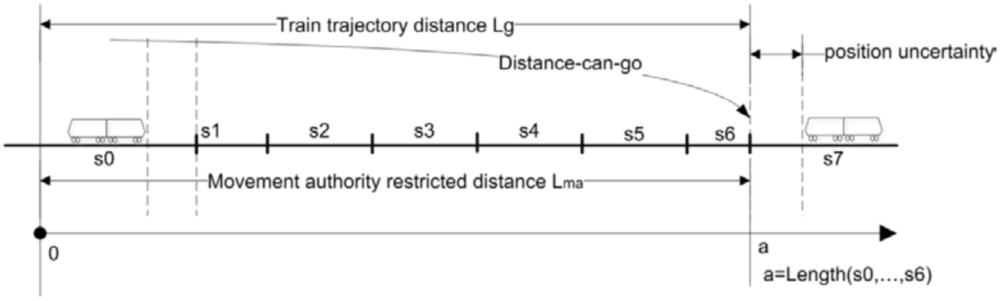
Train trajectory distance Lg
Distance-can-go
position uncertainty
s0
s1
s2
s3
s4
s5
s6
s7
Movement authority restricted distance Lma
0
a
a=Length(s0,…,s6)

**Figure 4.** Movement authority and train trajectory.

As shown in Figure 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 Figure 4, the movement authority includes track sections $u_0, u_1, u_2, \dots \dots, u_6$, 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 $< u_0, u_1, u_2, \dots \dots, u_n >$ be the MA calculated by the ZC 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:

D4.1) $\emptyset \in \mathcal{T}$ , $\{u_0\} \in \mathcal{T}$ and X $\in \mathcal{T}$, $u_0$is called the start unit of the space.

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 Equation (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:

D5.1) $\emptyset \in X$ .

D5.2) if $d(\alpha, u_0.a) + d(\alpha, u_0.b) = d(u_0.a, u_0.b)$, then $\{u_0\} \in \mathcal{T}$, u$_0$is called the start unit of the space.

D5.3) let $\tau \in \mathcal{T}$ , for every $u_j \notin \tau$ , if $d(\alpha, u_j.a) < L_g$ , $dir \times [d(u_0.b, u_j.a) - d(u_0.a, u_j.a)] >$ 0and $d(\alpha, u_j.a) = min\{d(\alpha, u_k.a): k \in I\}$ then $\{\tau \cup \{u_j\}\} \in \mathcal{T}$.

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

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

## 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. Firstly, some fundamental concepts of topology are proposed [34]. 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 $\emptyset$ 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:

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

where the interlocking state refers to $u.s$ and $u.l$ , 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 $\alpha$ satisfies $d(\alpha, u_0.a) + d(\alpha, u_0.b) = d(u_0.a, u_0.b)$.

It is immediately proven by means of Definition 1 and Definition 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 $\mathcal{T}_A \ \geq \ \mathcal{T}_T \ \ and \ \ Z_A \ \supseteq Z_T$.

Proof: Respect 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, $\mathcal{T}_A \ \geq \ \mathcal{T}_T \ \ and \ \ Z_A \ \supseteq Z_T$ 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 $\sigma$ is shown as a topology on $Z_T$, then the result will follow. It is observed that:

(1) $\emptyset = Z_T \cap \emptyset$ and $Z_T = Z_T \cap Z_A$.
(2) $\bigcup_{\alpha \in A}(Z_T \cap U_\alpha) = Z_T \cap \ \bigcup_{\alpha \in A} U_\alpha$ .
(3) $\bigcap_{j=1}^{n}(Z_T \cap U_j) = Z_T \cap \ \bigcap_{j=1}^{n} U_j$ .

Therefore Definition 2 is completely satisfied, $\sigma$ 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 movement authority and at any time the trajectory space should not include an unsafe point; this can be verified with Theorem 4.

Definition 6: Let $(X, \tau)$ 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 $\theta$ be the inverse function of $d$; it is immediately proven by means of Definition 3, Definition 4 and Definition 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, $\theta$ cannot be a continuous function. This shows that the condition is sufficient.

If $V2$ spaces are connected, with respect to the Theorem 3 and Theorem 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 $(X,\tau_1)$ and $(Y,\tau_2)$ are $V1$ space for different trains, the railway network is safe if and only if spaces $(X,\tau_1)$ and $(Y,\tau_2)$ are disjoint.

Proof: It can be immediately proven by means of train control principle, let $(X,\tau_1)$ be the space for Train 1 and $(Y,\tau_2)$ be the space for Train 2. If intersection $X \cap Y \neq \emptyset$, then it means that Train 1 can pass through the area of space $(Y,\tau_2)$, or Train 2 can pass through the area of space $(X,\tau_1)$. 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 Figure 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 Figure 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.

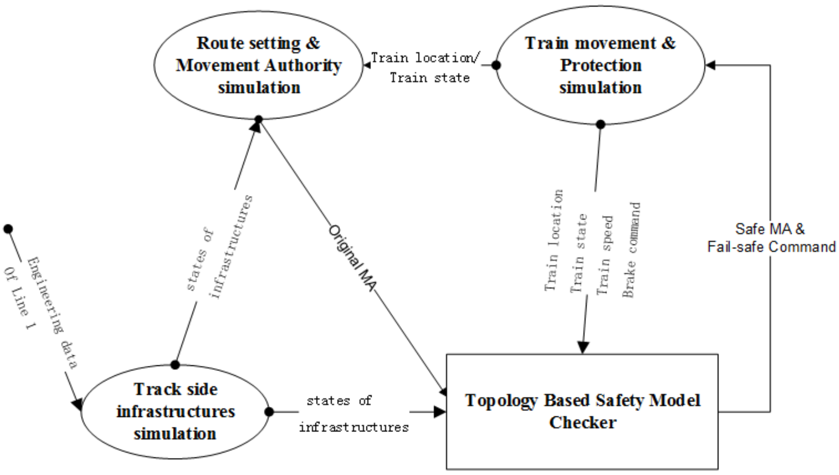

**Figure 5.** Schematic architecture of the case study.

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 Figure 6.

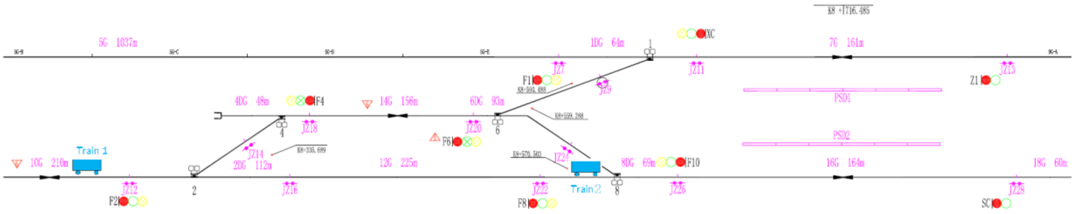

**Figure 6.** A part of the railway network from the Urumqi line 1.

where F2, F8, F6 and F10 are signals; 2 and 8 are points; 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 list in Table 2.

**Table 2.** Engineering data of the example.

| ID | Element | Engineering data Start point(m) | Engineering data End point(m) | Contained infrastructure | Topological unit | Data construct |
|---|---|---|---|---|---|---|
| 0 | F2 | K8+226.000 | K8+226.000 | Signal F2 | $u_0$ | (8226, 8226, 0,1, $s_0$, $l_0$) |
| 1 | 2 | K8+322.000 | K8+322.000 | Point No.1 | $u_1$ | (8322, 8322, 1,2, $s_1$, $l_1$) |
| 2 | 2DG | K8+229.000 | K8+341.000 | Plain-track | $u_2$ | (8229, 8341, 2,3, $s_2$, $l_2$) |
| 3 | 12G | K8+341.000 | K8+566.000 | Plain-track | $u_3$ | (8229, 8341, 3,3, $s_3$, $l_3$) |
| 4 | F8 | K8+563.000 | K8+563.000 | Signal F8 | $u_4$ | (8563, 8563, 4, 1, $s_4$, $l_4$) |
| 5 | 8 | K8+613.000 | K8+613.000 | Point No.2 | $u_5$ | (8613, 8613, 5, 2, $s_5$, $l_5$) |
| 6 | 8DG | K8+566.000 | K8+634.000 | Plain-track | $u_6$ | (8566, 8634, 6, 3, $s_6$, $l_6$) |
| 7 | F10 | K8+637.000 | K8+637.000 | Signal F10 | $u_7$ | (8637, 8637, 7, 1, $s_7$, $l_7$) |
| 8 | Train 1 | K8+221.000 | / | | | |

| | | | |
|---|---|---|---|
| 9 | Train 2 | K8+605.000 | / |

Note: K8=8000 m.According to the locations of the two trains, the topological units $u_0$ need to be adjusted using $u_0 = (15580, 15730, 0,1, s_0)$. The safety checking approach can be divided into 8 steps as follows:

**Step 1:** Let the track section sequence of the MA that calculated by the VOBC subsystem be $< TRAIN2, LK05009,\ F1,\ 1DG, LK05019, XC1 >$ . With the respect to Definition 4, the $V1$ space can be formed as follows:

$(Q1, \mathcal{T}_A) = (\emptyset,\ \{\mathrm{u}_0\},\ \{\mathrm{u}_0, \mathrm{u}_1\},\ \{\mathrm{u}_0, \mathrm{u}_1, \mathrm{u}_2\},\ \{\mathrm{u}_0, \mathrm{u}_1, \mathrm{u}_2, \mathrm{u}_3\},\ \{\mathrm{u}_0, \mathrm{u}_1, \mathrm{u}_2, \mathrm{u}_3, \mathrm{u}_4\})$ and $Q1 = \{\mathrm{u}_0, \mathrm{u}_1, \mathrm{u}_2, \mathrm{u}_3, \mathrm{u}_4\}$.

**Step 2:** Let the current speed $(CV)$ of the 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 Equation (3), the ‘distance-can-go’ can be calculated: $L_g = 221m$. According to Table 2, track sections LK05009, F1, 1DG are included in $L_g$. Based on Definition 5, the $V2$ space for the train 2 can be built as follows:

$(Q2, \mathcal{T}_T) = (\emptyset,\ \{\mathrm{u}_0\},\ \{\mathrm{u}_0, \mathrm{u}_1\},\ \{\mathrm{u}_0, \mathrm{u}_1, \mathrm{u}_2\})$ and $Q2 = \{\mathrm{u}_0, \mathrm{u}_1, \mathrm{u}_2\}$ .

**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 the train 2, the authors calculate $d(\alpha, u_0.a) = d(15580{,}15580) = 0$ , $d(\alpha, u_0.b) = d(15580{,}15730) = 150$ and $d(u_0.a, u_0.b) = d(15580{,}15730)$ . Therefore, $d(\alpha, u_0.a) + d(\alpha, u_0.b) = d(u_0.a, u_0.b)$ is satisfied.

**Step 4:** According to safety checking Theorem 2, for every unit $u \in Q1$, $h(u)$ needs to be checked. Among sections LK05009, F1, 1DG, LK05019 and XC1, if any of the sections is occupied or unlocked, or Point 1 is not at its normal position, or Signal XC1 shows a green or yellow aspect, then $h(u) = 0$. That is, the safety conditions for the 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, the train 2 is in a safe situation. Assume that the current speed $(TV)$ of the 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 Equation (3), $L_g = 414\ m$ can be obtained. Thus the $V2$ space for the train 2 can be calculated as follows:

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

$Q2 = \{u_0, u_1, u_2, u_3, u_4, u_5\}$ .

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 a 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 $Q1 = \{\mathrm{u}_0, \mathrm{u}_1, \mathrm{u}_2, \mathrm{u}_3, \mathrm{u}_4\}$. It is assumed that there is an error existing (e.g. Signal F1 is displaying a red aspect), and such error is not detected by the ZC subsystem. In such a situation, $L_g = 221m$, 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 the train 1 can be calculated as $(Y, \mathcal{T}_T) = (\emptyset,\ \{u_5\},\ \{u_5, u_6\},\ \{u_5, u_6, u_7\},\ \{u_5, u_6, u_7, u_8\},\ \{u_5, u_6, u_7, u_8, u_9\},\ \{u_5, u_6, u_7, u_8, u_9, u_{10}\})$. It is assumed that the $V1$ space of the train 2 is $(X, \tau_1) = (\emptyset,\ \{u_0\},\ \{u_0, u_1\},\ \{u_0, u_1, u_2\},\ \{u_0, u_1, u_2, u_3\},\ \{u_0, u_1, u_2, u_3, u_4\},\ \{u_0, u_1, u_2, u_3, u_4, u_5\},\ \{u_0, u_1, u_2, u_3, u_4, u_5, u_6\})$. Therefore, the train 2 can reach the unit $u_6$ (the track section 3DG). At this moment, if the train 1 still located in $u_5$ (the track section LK05021), a collision will occur. Therefore, it can be seen that Theorem 6 is used for checking the safety for different trains through the intersection of $V1$ spaces.

## 4.2 Simualtion Result

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

**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 |

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, there are 5 states for each point element are considered: 1) normal position, 2) reverse position, 3) normal position and locked, 4) reverse position and locked, 5) position indication unavailable. For a track section, there are 3 states: 1) occupied, 2) unoccupied, 3) error. For a signal, there are 3 states: 1) green, 2) yellow, 3) red, 4) error. Finally, a train has 3 states: 1) normal, 2) brake, 3) error. Figure 7 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 is not existing in our method.

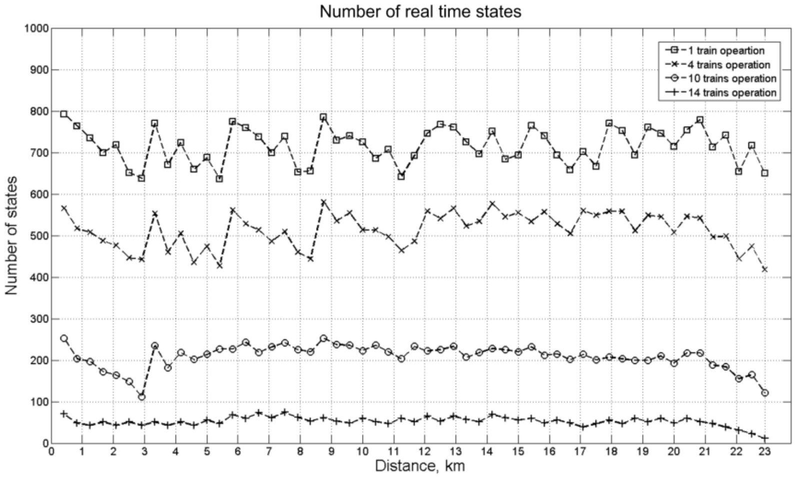

**Figure 7.** Number of real time states.

Figure 8 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 approximately 26 *ms*, which totally fits for the real-time requirements of TcCBTC systems.

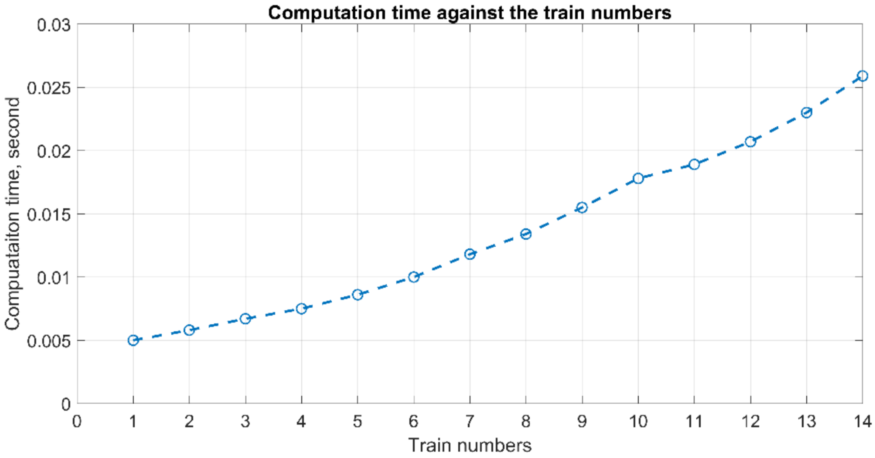

**Figure 8.** Computation time against distance and number of trains.

## 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 Figure 9, due to the abstraction of the railway network metric space and the topological space description for the movement authority 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.

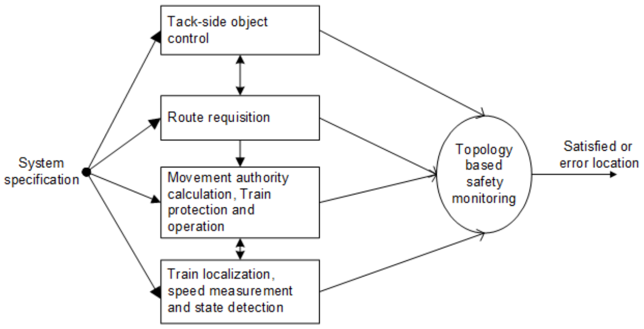
System specification
Tack-side object control
Route requisition
Movement authority calculation, Train protection and operation
Train localization, speed measurement and state detection
Topology based safety monitoring
Satisfied or error location

**Figure 9.** Topology based safety monitoring for TcCBTC system.

In real train control system engineering, the time cycle of the VOBC subsystem is typically 200ms; 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 ever higher level of safety integrity for such systems. Essentially, this method provides topological operational semantics for railway networks, movement authority 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 proving 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.

## Acknowledgments

This research was supported in part 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; and by the Beijing Laboratory of Urban Rail Transit, China.

## References

[1]. S. Morar, "Evolution of Communication Based Train Control worldwide." pp. 218-226.

[2]. I. V. T. Society, "1474.1TM IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements," 2004.

[3]. P. Gurník, “Next Generation Train Control (NGTC): More Effective Railways through the Convergence of Main-line and Urban Train Control Systems,” Transportation Research Procedia, vol. 14, no. Supplement C, pp. 1855-1864, 2016/01/01/, 2016.

[4]. H. Nakamura, “How to Deal with Revolutions in Train Control Systems,” Engineering, vol. 2, no. 3, pp. 380-386, 2016/09/01/, 2016.

[5]. A. Ruf, E. Matejka, and I. Sekaj, "Train control system without interlocking a new paradigm in railway control?." pp. 490-493.

[6]. Y. Nakamura, “Overview of the Next-generation Railway Operation System in the Tokyo Metropolitan Area,” no. 19, pp. pp 3-6, 2011.

[7]. W. Haifeng, L. Kaichegn, and L. Hongjie, “Trend Analysis of Development on Train Control System Technologies,” Railway Signalling & Communication, vol. 52, no. 8, pp. 1-4, 2016.

[8]. P. Pascal, and P. Jacques, “Signal Control Systems Innovations and Future Developments,” Proceedings of the Institution of Railway Signal Engineers, pp. 56-66, 2015.

[9]. E. Quaglietta, and V. Punzo, “Supporting the design of railway systems by means of a Sobol variance-based sensitivity analysis,” Transportation Research Part C: Emerging Technologies, vol. 34, pp. 38-54, 2013.

[10]. Oukhellou, E. Côme, L. Bouillaut, and P. Aknin, “Combined use of sensor data and structural knowledge processed by Bayesian network: Application to a railway diagnosis aid scheme,” Transportation Research Part C: Emerging Technologies, vol. 16, no. 6, pp. 755-767, 2008.

[11]. J. Beugin, and J. Marais, “Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization,” Transportation Research Part C: Emerging Technologies, vol. 22, pp. 42-57, 2012.

[12]. S. Li, L. Yang, and Z. Gao, “Coordinated cruise control for high-speed train movements based on a multi-agent model,” Transportation Research Part C: Emerging Technologies, vol. 56, pp. 281-292, 2015.

[13]. J. Woodcock, P. G. Larsen, J. Bicarregui, and J. Fitzgerald, “Formal Methods: Practice and Experience,” Acm Computing Surveys, vol. 41, no. 4, Oct, 2009.

[14]. E. M. Clarke, and J. M. Wing, “Formal methods: State of the art and future directions,” Acm Computing Surveys, vol. 28, no. 4, pp. 626-643, Dec, 1996.

[15]. CENELEC, "EN 50128: Railway applications –Communications, signalling and processing systems – Software for railway control and protection systems.," 2000.

[16]. N. Zingoni, A. Fantechi, and M. Tempestini, “A story about formal methods adoption by a railway signaling manufacturer,” Lecture Notes in Computer Science, vol. 4085, no. LNCS, pp. 179-189, 2006.

[17]. J. P. Bodeveix, M. Filali, J. Lawall, and G. Muller, "Formal methods meet domain specific languages," Integrated Formal Methods, Proceedings, Lecture Notes in Computer Science J. Romijn, G. Smith and J. VanDePol, eds., pp. 187-206, Berlin: Springer-Verlag Berlin, 2005.

[18]. A. E. Haxthausen, J. Peleska, and S. Kinder, “A formal approach for the construction and verification of railway control systems,” Formal Aspects of Computing, vol. 23, no. 2, pp. 191-219, Mar, 2011.

[19]. G. H. Armin Zimmermann, “Towards modeling and evaluation of ETCS real-time communication and operation,” Journal of Systems and Software - Special issue: Parallel and distributed real-time systems, vol. 77, no. 1, pp. 47-54, 2005.

[20]. P. Barger, W. Schoen, and M. Bouali, A study of railway ERTMS safety with Colored Petri Nets, 2010.

[21]. A. E. Amraoui, and K. Mesghouni, "Colored Petri Net Model for Discrete System Communication Management on the European Rail Traffic Management System (ERTMS) Level 2." pp. 248-253.

[22]. W. Damm, A. Mikschl, J. Oehlerking, E. R. Olderog, J. Pang, A. Platzer, M. Segelken, and B. Wirtz, "Automating verification of cooperation, control, and design in traffic applications," Formal Methods and Hybrid Real-Time Systems, Lecture Notes in Computer Science C. B. Jones, Z. Liu and J. Woodcock, eds., pp. 115-169, Berlin: Springer-Verlag Berlin, 2007.

[23]. M. Ghazel, “Formalizing a subset of ERTMS/ETCS specifications for verification purposes,” Transportation Research Part C: Emerging Technologies, vol. 42, pp. 60-75, 2014.

[24]. H. Wang, and S. Liu, "Study on model-based safety verification of automatic train protection system." pp. 467-470.

[25]. H. Wang, and S. Liu, "Modeling Communications-based Train Control system: A Case Study." pp. 453-456.

[26]. A. Morzenti, M. Pradella, P. San Pietro, and P. Spoletini, "Model-checking TRIO specifications in SPIN," Fme 2003: Formal Methods, Proceedings, Lecture Notes in Computer Science K. Araki, S. Gnesi and D. Mandrioli, eds., pp. 542-561, 2003.

[27]. A. Mekki, M. Ghazel, and A. Toguyeni, “Validation of a New Functional Design of Automatic Protection Systems at Level Crossings with Model-Checking Techniques,” Ieee Transactions on Intelligent Transportation Systems, vol. 13, no. 2, pp. 714-723, Jun, 2012.

[28]. D. L. Parnas, “Really Rethinking 'Formal Methods',” Computer, vol. 43, no. 1, pp. 28-34, 2010.

[29]. H. Wang, F. Schmid, L. Chen, C. Roberts, and T. Xu, “A Topology-Based Model for Railway Train Control Systems,” Ieee Transactions on Intelligent Transportation Systems, vol. 14, no. 2, pp. 819-827, Jun, 2013.

[30]. H. Wang, T. Tang, C. Roberts, C. Gao, L. Chen, and F. Schmid, “A novel framework for supporting the design of moving block train control system schemes,” Proceedings of the Institution of Mechanical Engineers Part F-Journal of Rail and Rapid Transit, vol. 228, no. 7, pp. 784-793, Sep, 2014.

[31]. H. Wang, T. Xu, and T. Yuan, “Novel Online Safety Observer for Railway Interlocking System,” Journal of Transportation Engineering, vol. 139, no. 7, pp. 719-727, Jul 1, 2013.

[32]. K. Akita, T. Watanabe, H. Nakamura, and I. Okumura, “Computerized Interlocking System for Railway Signaling Control: SMILE,” Industry Applications, IEEE Transactions on, vol. IA-21, no. 3, pp. 826-834, 1985.

[33]. IEC 61508 Second Edition:Functional Safety of Electrical/Electronic/Programmable Electronic Systems, 2010.

[34]. S. A. Gaal, Point set topology, New York, USA: Academic Press, 1964.