Petri Net Based Functional Safety Verification Framework on Rail Control System

She Xiaoli* and Yang Jian

Department of Electronic Enginnering, Tsinghua University, Beijing, 100084, P.R. China

Abstract
Rail control system acts very important safety role in both national railway and urban rail transportation. This paper provides a formal verification framework on functional safety desired by railway industry application. The presented work chooses Colored Petri Nets for functional modeling and verification. The modelling approaches of internal faults and undesired external influences are proposed by introducing a countering place, and the verification criteria is established based on credible hazard set. An application of this framework on Communication Based Train Control system is also presented.
Keywords: COLORED PETRI NETS, SAFETY CONTROL, RAIL CONTROL SYSTEM

1. Introduction

The ever increasing complexity of Rail control system has brought the challenging task of safety assurance. This challenge has made the CENELEC standards [1, 2] be practically mandatory in railway signaling application. According to this widely applied standard, functional safety should be demonstrated on correct functionality, under internal faults and external influence. However, such evidences were mostly provided via an informal way in practice.

In another hand, Formal methods have been proved to be an effective approach for safety critical system design and analysis, and widely applied on railway systems [3]. With all the formal methods, Petri Nets is advanced as its graphical representation, solid mathematics foundations and analysis techniques. Petri Nets has been widely used on railway application, such as railway network study [4, 5], interlocking system [6, 7], European Rail Traffic Management System (ERTMS) [8]. They were normally used for safety analysis [6] or failure analysis [9], forming supplementary safety demonstration towards a specific scene or event, but not integrated evidence towards functional safety.

To better applying Petri Nets on CENELEC safety verification concepts, this paper establishes a safety verification framework based on the concept of safety demonstration in CENELEC standard [2] with reasonable extensions. Colored petri nets (CPN) is adopted to model system functionality, in which countering place is introduced to model faults and external influence. Credible hazard set identified from risk analysis directly contributes to the verification rule to enhance the credibility of verification results. The modeling and analysis of interactions also strongly supports the study of local analysis in the context of global cooperation.

In this paper, Section 2 makes a conceptual introduction of this framework especially its extensions to CENELEC standard. Section 3 describes the concrete approach of this framework, including modelling method and verification rule. An application example of this framework is presented in Section IV along with the analysis towards its simulation result.

2. Functional safety verification framework

A safety critical system runs in different internal and external conditions. According to functional safety concept [2], safety should be proved with regular or fault conditions, and under normal or extreme environment. In this paper, the target of functional safety verification framework is established based on this concept, but propose reasonable extensions or give practical method from formal verification view.

CONDITION I: Correct functional operation and

safety under fault-free assumption.

This condition concerns functional correctness and safety under fault-free assumption. In our framework, the "fault-free" concept concerns not only internal fault-free operation within target system, but also the desired interaction between target system and external items / environment.

CONDITION II: Functional safety with effect of internal faults.

The target of this condition in EN 50129 [2] is to achieve system safety in the event of random or systematic faults within the target system. In our framework, an approach is proposed to model the action of single fault and multiple faults, which are the main concerns of internal faults for functional safety.

CONDITION III: Functional safety with external influence.

In EN 50129 [2], this condition concerns the ability of functional safety when subjected to specified external influences. Our framework extends the concept of "external influences" from extreme environmental influence to general undesired interaction with external items. It is more extensive and generalized, as extreme environment is one kind of recognized external influence. This paper also provides an approach to model transient or steady external influence.

This framework provides an integrated and applicable method for formal verification with its safety evidence desired by CENELEC standard on functional safety. As this framework is focused on a specific safety function instead of whole system, it is usually able to avoid state space explosion, which is a general problem of formal verification. It also strongly supports the study of subsystem actions under complex communication or logical dependence with other subsystems, thus provides a powerful approach of local analysis in the context of global cooperation. Another remarkable advantage of this framework is able to utilize important results from risk analysis: the recognized fault model of internal / external actions can provide guideline to functional modelling; all identified hazards from risk analysis can be directly adopted to establish the verification rule.

3. Functional safety verification with colored petri nets

This section describes the approach to realize the proposed framework with CPN, including a brief introduction of CPN in subsection 3.1, functional modelling method in subsection 3.2 and safety verification rule in subsection 3.3.

3.1. Colored Petri Nets

Petri Nets is a powerful approach because of its graphical representation and solid mathematic foundations. There also exists simulation and formal analysis techniques both for static structure and dynamic behaviors. Based on the ordinary Petri Nets, many extensions have been raised and applied, such as Timed Petri Nets analyzing timing attributes of the model, and the Stochastic Petri Nets modeling random phenomena.

CPN is another extension of the ordinary Petri Nets [10]. It has the same mathematic nature and formal verification principle with the original Petri Nets. Moreover, it introduces color set to allow token differentiation, thus able to establish a more concise model. Appendix gives a formal definition of CPN model and its reachability feature, which is adopted in this paper for safety proof.

3.2. Functional Modelling

In this subsection we deal with the functional modelling using CPN. In particular, we show the modelling approach of single / multiple faults, and transient / steady undesired external influence by introducing a counter place.

In this framework, three kinds of models are generated, i.e. working model under fault-free assumption, models reflecting internal single or multiple faults, and models reflecting undesired external influence. Each kind of model corresponds to one of the CONDITIONs defined in section 2.

The models reflecting deviations can be established based on the model of normal operations with adding faulty or undesired behaviors, i.e. "faulty" transitions in CPN model. Note that the fault or undesired behaviors to be modeled can normally come from the result of risk analysis such as Fault Tree Analysis, Failure Mode and Effect Analysis, Hazard and Operability Analysis, etc.

Regarding internal fault, both single fault and multiple faults should be considered. In this paper, a counter place is introduced. This counter place should act as a precondition of each faulty transition. The initial token in counter place limits the number of faults this model considers. When we analyze the effect of single fault or multiple faults, the initial token can be set to corresponding number respectively, thus get different models. Fig. (1) shows a typical model for single fault analysis, in which Tf_1 and Tf_2 indicate two different faulty actions, but share the same counter place "ErrCnt" as their inputs. When any faulty transition is fired, other faults are unactable because of the lack of precondition.

The modelling of external influences considers both transient and steady influence to the target system. The concept of counter place still works. Make the counter place be the input of transient transition.

Once the transition has been fired, the action can't happen again because of the lack of precondition of counter place. The modelling of steady external influence needn't to introduce the counter place, but only consider the interactions. Fig.(2) shows the typical models for both transient and steady influence.

Appling the functional modelling process, we get a set of models, defined as mdl_{CON1}, a set of mdl_{CON2} and mdl_{CON3} (to model different faults, external influence and set different initial conditions):

$$MDL = \{mdl_{CON1}, \{mdl_{COND2}\}, \{mdl_{COND3}\}\} \quad (1)$$

3.3. Formal Verification on Hazard

This subsection discusses formal verification approach on the established model set MDL (1). In this paper, the verification criterion is based on the concept of hazard and the proof method utilizes reachability feature of CPN.

A hazard state is defined as a condition that could lead to an accident. It's an important concept for a safety critical system, and much effort has been done to identify all hazards as possible [2]. An exhaustive set of identified hazards in practice is the fundamental for safety design. It's also the fundamental for our framework, in which the hazard set is adopted to provide verification criteria.

Each hazard is marked as hi. Make hazard set $HS=\{h_1,h_2,\ldots,h_N\}$. Each hazard state hi can be described in CPN model with a system state represented by the token of places. In general, a hazard state is only related to part of places. Therefore, each hazard state is corresponding to a set of system states. We note this relationship as ϕ:

$$\phi: h_i \rightarrow \mathcal{M}_{hi} = \{M_{i1}, \ldots, M_{ik}\} \quad (2)$$

Similarly, the hazard set HS corresponds to:

$$\Phi: HS \rightarrow \mathcal{M}_{HS} = \{\mathcal{M}_{h1}, \ldots, \mathcal{M}_{hN}\} \quad (3)$$

Then the verification criterion is as (4),

$$\forall mdl \in MDL,\ \mathbb{M}_{mdl} \cap \mathcal{M}_{HS} = \emptyset \quad (4)$$

Here $\mathbb{M}_{mdl}$ is the set of all reachable states from MDL (1), which is established according to (11):

$$\mathbb{M}_{mdl} = \{\text{for all } mdl \in MDL,\ \{M_{mdl} \in [M_0 \succ\}\} \quad (5)$$

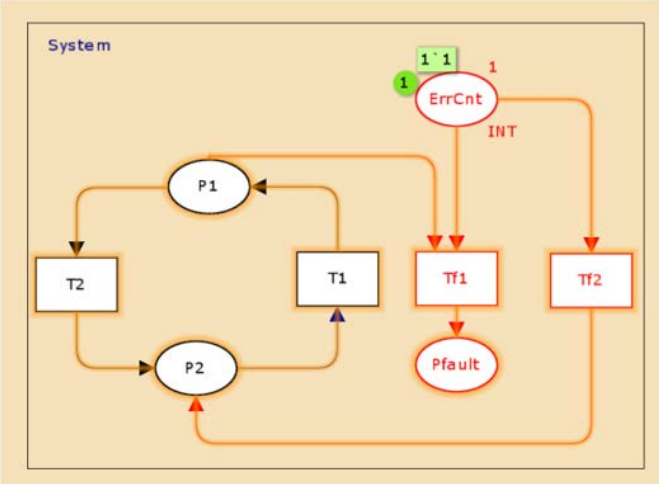
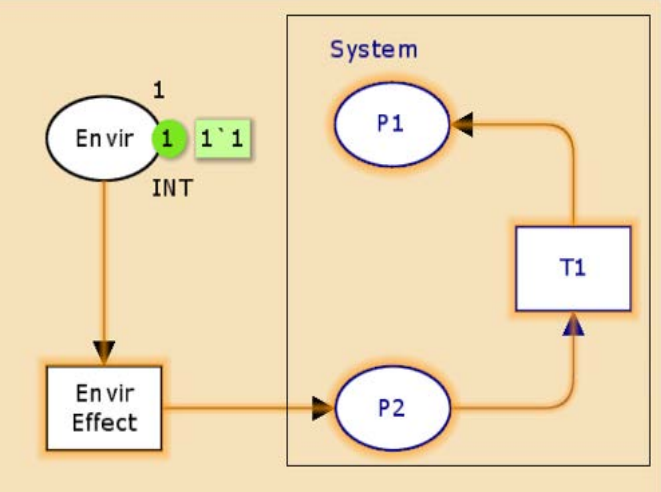
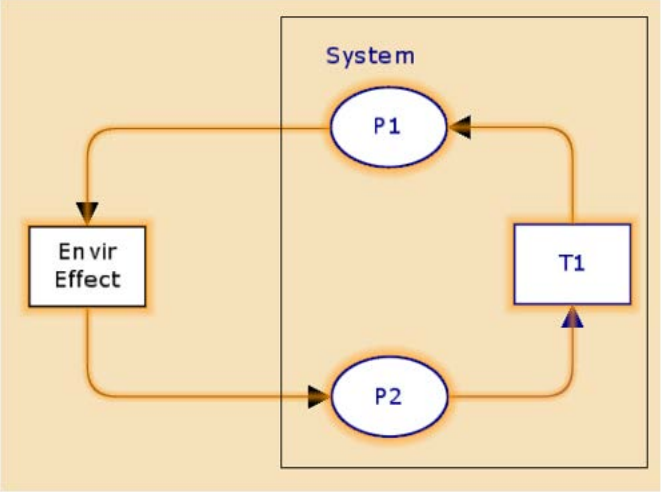


Figure 1. Example of Single fault analysis model



a) Transient influence model



b) Steady influence model

Figure 2. Example of external influence model

4. Application on communication based train control system

This section gives an application using the proposed framework. In this section, the route control function in Communication Based Train Control (CBTC) System is selected. CBTC is proposed from last century and has been commonly applied in the last ten years because of its capability to control smaller train interval.

To shorten tracing interval between the trains, CBTC system allows more than one trains entering the same route, which violates the traditional interlocking route control logic. In this section, we apply our approach to traditional interlocking route control function of CBTC system, to verify whether this violation introduces any hazard.

4.1. Functional Modelling of Interlocking Route Control

A simplified interlocking route control function in CBTC system is established. The model introduces two trains and models all tracks forming a loop to model two trains continuously tracing. The point control function is removed in our model to reduce its complexity, as point control function doesn't differ between traditional interlocking and CBTC system.

Fig.(3) shows a general view of this model, including two trains, tracks, signals and route. In this model, tracks, signals, route and their restrictions and interactions are the elements within the target system. The trains with their operation rules are out of the target system, but still be modeled to study the influence of external interaction.

Following the interlocking control logic in CBTC system, the model with correct operation shows in Fig.(4)-a, noted as mdl_1. In this model, the black part is the internal system behavior, and the blue part is the external operation rule of trains. The interactions between the two parts includes the permission / prohibition authorization from internal system to trains, and the track state acquisition from the external facilities to internal track states.

Based on mdl_1, we consider one of the undesired external influence caused by multiple data source of track state with different communication delay. This undesired influence may cause train "retreat", which will not happen in normal operation condition. The model considering this influence shows in Fig.(4)-b with red counter place and transition, noted as mdl_2.

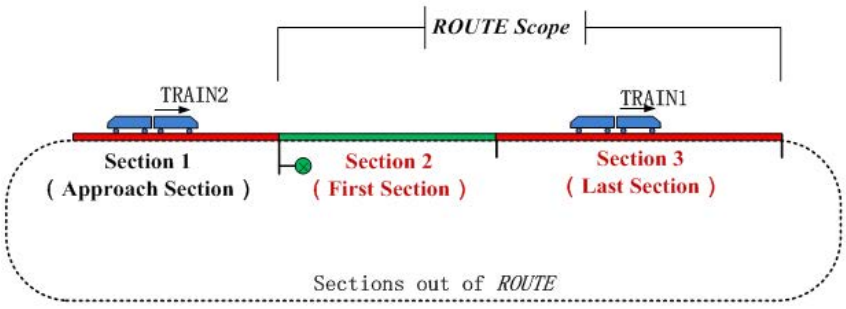
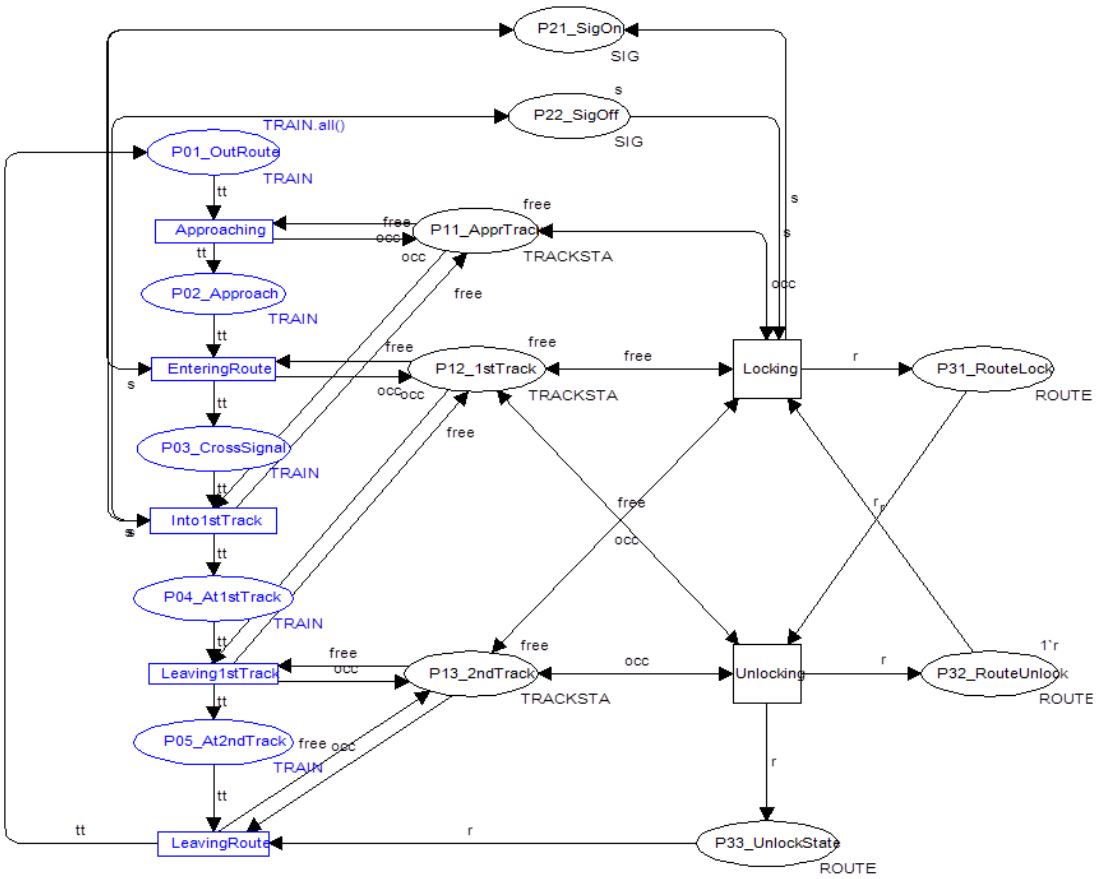
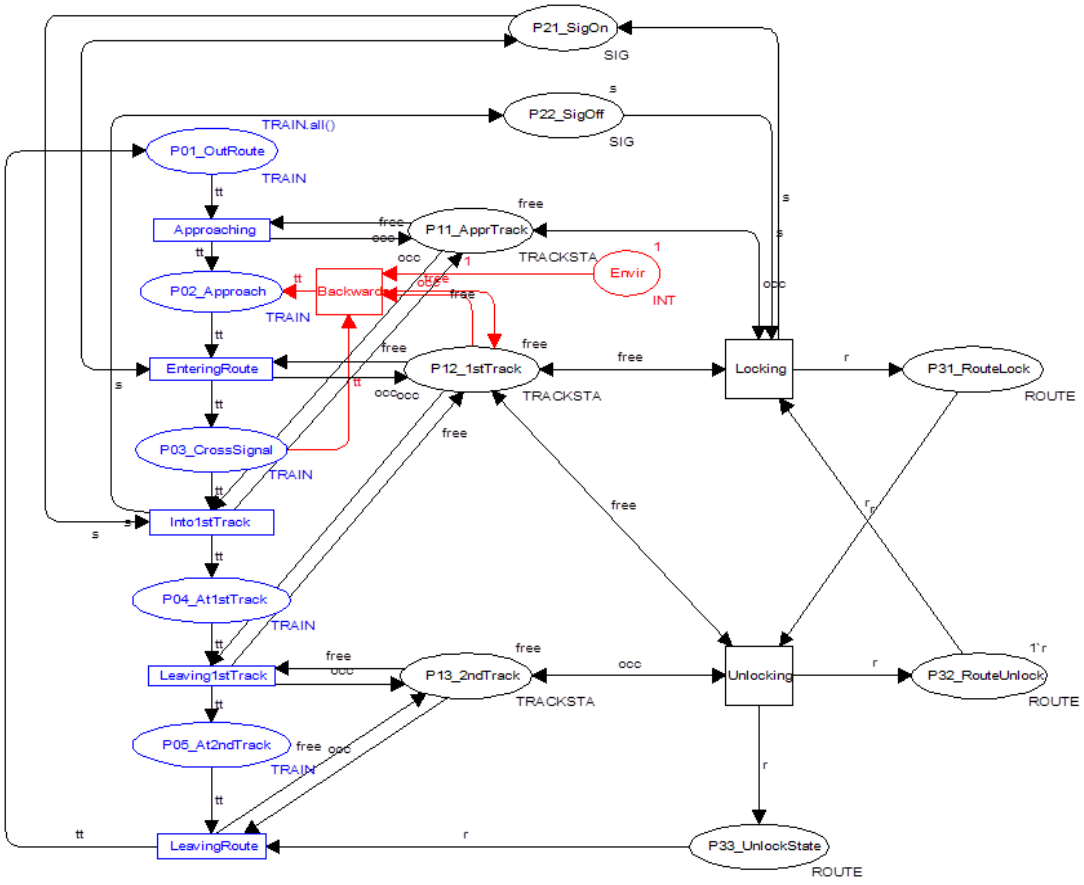


Figure 3. Simplified interlocking route control function of CBTC system



a) Functional model with correct operation



b) Functional model with unexpected external interaction.

Figure 4. Simplified interlocking route control model with CPN model

In both mdl_1 and mdl_2, we set the initial state as follows: two trains are both out of the route, all related tracks are free, and the authorization for the route is prohibited.

4.2. Formal Verification and Analysis

This subsection is to verify if all hazards are not reachable in all conditions mentioned in section 2. In this section we firstly confirm the hazard set relating to route control. The hazards and their corresponding states are listed in Table 1. Note that {*} indicates the other places can be with any value.

Table 1. Interlocking Route Control Related Hazard List

Hazard	Descriptions	States in CPN
h_1	Wrong route is selected.	Not applicable
h_2	Permit signal to trains for entering an unlock route.	$\mathcal{M}_{h2} = \{P_{21} = s, P_{32} = r,*\}$
h_3	Permit to operate points when route is locking	Not applicable
h_4	Unlock route incorrectly	$\mathcal{M}_{h4} = \{P_{02} = tt, P_{32} = r,*\} \cup \{P_{04} = tt, P_{32} = r,*\}$
h_5	Authorize higher speed than route permitted	Not applicable

Then we get

$$\mathcal{M}_{HS} = \{\mathcal{M}_{h2}, \mathcal{M}_{h4}\} = \{\{P_{21}, P_{32}, *\} \cup \{P_{02}, P_{32}, *\} \cup \{P_{04}, P_{32}, *\}\} \quad (6)$$

The reachable marking set can be calculated from model mdl1 and mdl2 following (10) and (11), denoted as $\mathbb{M}_1$ (the state space of a correct functional model) and $\mathbb{M}_2$ (that of a functional model under external influence) respectively. In this application, CPN Tools is adopted to calculate $\mathbb{M}_1$ and $\mathbb{M}_2$and simulation.

The simulation results shows

$$\mathbb{M}_1 \cap \mathcal{M}_{HS} = \emptyset \quad (7)$$

While

$$\mathbb{M}_2 \cap \mathcal{M}_{HS} \neq \emptyset \quad (8)$$

Result (8) doesn't satisfy the criterion (4), i.e. the model under external influence doesn't satisfy the criterion that no hazardous state is reachable. It shows that a system verified as safety in correct operation and functions may come into hazardous states with undesired internal faults or external influence. The traditional interlocking logic should be adapted when applied on CBTC system.

5. Conclusions

This paper proposes a functional safety verification framework and its realization with CPN. The application result shows that the proposed approach is powerful to verify whether a system is safe from functional safety point of view, and also helpful to find out hazardous states.

Conflict of interest

The author confirms that this article content has no conflict of interest.

Appendix

This appendix gives the formal definition of Colored Petri Nets.

$$mdl = (\Sigma, P, T, A, N, C, G, E, I)$$

The definition and constraint for each component is given below:

1.Place set P, transition set T, arc set A:

$$P \cap T = P \cap A = T \cap A = \emptyset.$$

2. Arc set N:

$$A \to P \times T \cup T \times P \wedge dom(A) \cup cod(A) = P \cup T.$$

3. Color function set $C: P \to \Sigma$.

4. Guard function set G:

$$T \to expr \wedge \forall t \in T: [Type(G(t)) = B \wedge Type(Var(G(t)) \subseteq \Sigma].$$

5. Arc function set: E:

$$A \to expr \wedge \forall a \in A: |Type(E(a)) = C(p(a))_{MS} \wedge Type(Var(E(a))) \subseteq \Sigma|.$$

6. The initial state

$$I: P \to expr \wedge \forall p \in P: [Type(I(p)) = C(p)_{MS}.$$

There are both static and dynamic features supporting safety analysis, such as boundness, liveness, invariance and reachability. The dynamic features are established on the firing of transition. A transition can be fired if it satisfied:

$$\forall p \in P: \sum_{(t,b)\in Y} E(p,t)\langle b\rangle \leq M(p) \quad (9)$$

The state changes from M_1 to M_2 when a transition is fired:

$$\forall p \in P: M_2(p) = \left(M_1(p) - \sum_{(t,b)\in Y} E(p,t)\langle b\rangle\right) + \sum_{(t,b)\in Y} E(t,p)\langle b\rangle \quad (10)$$

This process is noted as $M_1[Y \succ M_2$, which implies M_2 is reachable from M_1.

All reachable states from the initial state M_0, as

well as its firing transitions, consists of the reachability graph of M_0, noted as

$$\mathbb{M} = \{M \in [M_0 \succ\} \quad (11)$$

References

1. CENELEC, *EN 50126 Railway Applications– The Specification and demonstration of Reliability, Availability, Maintainability, and Safety (RAMS)*. London: British Standards Institution (BSI), 1999.
2. CENELEC, *EN 50129 Railway Applications-Safety-related electronic systems for Signalling*. London: British Standards Institution (BSI), 2003.
3. M. Pěnička, "Formal approach to railway applications," *Formal methods and hybrid real-time systems,* pp. 504-520, 2007.
4. S. Vanit-Anunchai, "Modelling railway interlocking tables using coloured petri nets," *in Coordination Models and Languages,* 2010, pp. 137-151.
5. W. M. van der Aalst and M. A. Odijk, "Analysis of railway stations by means of interval timed coloured Petri nets," *Real-time systems,* vol. 9, pp. 241-263, 1995.
6. N. G. Leveson and J. L. Stolzy, "Safety Analysis Using Petri Nets," *IEEE Transactions on Software Engineering,* vol. SE-13, pp. 386-397, 1987.
7. M. S. Durmus and M. T. Soylemez, "Railway signalization and interlocking design via Automation Petri Nets," *in Asian Control Conference*, 2009. , 2009, pp. 1558-1563.
8. P. Barger, W. Schön, and M. Bouali, "A study of railway ERTMS safety with colored Petri nets," *in The European Safety and Reliability Conference (ESREL'09)*, Prague, 2009, pp. 1303--1309.
9. A. Adamyan and D. He, "System failure analysis through counters of Petri net models," *Quality and Reliability Engineering International,* vol. 20, pp. 317-335, 2004.
10. K. Jensen, *Coloured Petri nets: basic concepts, analysis methods and practical use* vol. 1: Springer Science & Business Media, 2013.