FUNCTIONAL SAFETY ANALYSIS OF CBTC SYSTEM BASED ON CPN MODEL

ZHI. ZHA
JIN. GUO
YADONG. ZHANG
HAO. GAO

Summary: *In this paper, a method of functional safety analysis based on CPN is proposed, which focuses on characterization of hazard and its propagation and transformation in the process of function implementation. On the basis of Petri net model of function implementation, the algorithmes of identifying hazard and analyzing hazard transformation rule integrating with HAZOP and FTA tecnnology are presented. The method of establishing functional safety analysis CPN model is given. By using the CPN Tools simulation analysis, the key hazardes and their combination that cause the system functional failure are identified effectively. Taking CBTC overspeed protection for example, the proposed method is applied in modeling and analyzing the key hazardes that may lead to the failure of CBTC overspeed protection. The results show that the CPN model based method is validity to functional safety analysis of CBTC system.*

Keyword: *Functional safety analysis, Petri net, HAZOP, FTA, CBTC, Overspeed protection, CPN Tools.*

I. INTRODUCTION

In order to ensure the safety and efficiency of urban rail transit, advanced communication based train control (CBTC) system has been widely used. CBTC system adopts the high-resolution train location determination technology and continuous high capacity bidirectional train-to-wayside data communication system to achieve automatic train control [1]. It could control train running in real time accurately and safely, shorten the tracking interval and improve the efficiency. CBTC is a safety critical system. The effective methods should be used to analyze the functional safety of CBTC system to find out the hazards and their combination which cause the function failure, and then appropriate risk control measures would be taken. That is of great significance for enhancing the safety of CBTC system and ensuring the train operation safely and efficiently.

Currently there are many methods for system functional safety analysis. From the

This work was supported by the Key Research Projects of China Railway Corporation (2014X008-A, 2015X007-J and 2015X009-D) and the Fundamental Research Funds for the Central Universities (82014BR059).

Z. Zha, J. Guo, Y. Zhang and H. Gao are with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China (e-mail: zzha_Charli@126.com). Corresponding author: Y. Zhang (ydzhang@home.swjtu.edu.cn).

perspective of system modeling, they can be divided into the following three categories [2]:

a. The event-based safety analysis methods, including FTA, FMEA, HAZOP, etc, focus on describing the causal relationship between fault event and its cause or consequences. However, with the increasing of the complexity of system, it is very difficult to identify the causality.

b. The state-based safety analysis methods, such as SPN, ASCAP, and so on, place emphasis on system behavior modeling. But the accurate model is hard to establish for complex systems.

c. The failure model-based safety analysis methods, such as FPTN, Hip-HOPS etc, emphatically analyze the propagation and transformation of hazards in the system. But this method is lack of mature analysis tools, and the relevant computation is enormous.

CBTC system is a complex dynamic system. In the process of system function implementation, the propagation and transformation of hazards will occur dynamically. There are some problems such as modeling complexity and large computational quantity, while using the above approaches to analyze CBTC system functional safety. CPN is a relatively mature advanced Petri net [5]. The way of its formalized description is proper for modeling of system function implementation process, its color tokens are suitable for representing the system hazards, and there is a perfect analysis tool-CPN Tools.

Therefore, in this paper, a method of functional safety analysis based on CPN model integrating with Petri net modeling and simulation, HAZOP [3] and FTA [4] technology was proposed. The proposed method focuses on analyzing the propagation and transformation of hazards in the process of system function implementation. The method of establishing the functional safety analysis CPN model was presented. The hazards and their combination which cause the failure of system function were effectively identified through the simulation analysis. Taking CBTC overspeed protection for example, the proposed method was applied in modeling and analyzing of the functional safety of CBTC system.

II. FUNCTIONAL SAFETY ANALYSIS METHOD BASED ON CPN MODEL

The process of CPN model-based functional safety analysis is divided into four steps, as shown in fig 1.

Firstly, after a full analysis of the system functional requirement according to relevant standards and specifications, system function implementation Petri net model is established. To guarantee the accuracy and availability of the model, properties such as reachability, activity and non-collision, boundedness and security will be verified.

Secondly, by using the algorithm given in the following section B, the hazards will be identified and their propagation and transformation rules will be analyzed.

Thirdly, according to the definition of functional safety analysis CPN model given in the following section C, the CPN model of CBTC system functional safety analysis will be

constructed.

Lastly, with the aid of CPN Tools, a CPN simulation model will be built. The key hazards that cause the functional failure will be found out through the simulation result analysis.

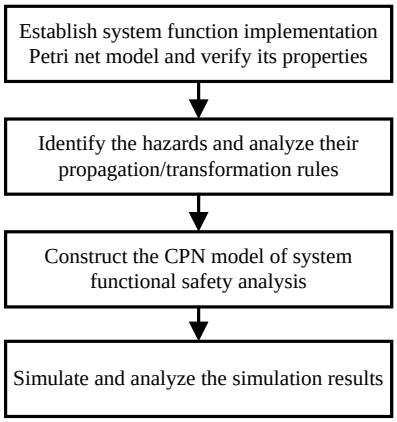

Fig 1. *The process of CPN model-based functional safety analysis*

This paper mainly studies the following three parts, namely, Petri net modeling of system function implementation, Petri net model-based hazard analysis and construction and analysis of functional safety analysis CPN model.

A. Petri Net Modeling of System Function Implementation

For the system function to be analyzed, based on the interaction between the functional modules in the process of function implementation, a Petri net model was constructed. This was accomplished by converting each functional module to one transition and using one place to represent an input or output information of each module. Therefore, the system function implementation Petri net (SFI-PN) model was defined as the following four-tuple in formalization

$$\text{SFI-PN} = (P, T, F, M) \tag{1}$$

Where, P is the set of system information, T is the set of functional module, F is the set of relationship between system functional module, and M is the state of system.

Given the external input information as the initial marking M_0, properties of the SFI-PN model including reachability, activity and non-collision could be verified with the aid of simulation analysis software such as CPN Tools.

B. Petri Net Model-Based Hazard Analysis

In the process of function implementation, system hazards may caused by the harmful deviation of input information or the failure of functional modules may occur and they are eventually reflected in the harmful deviation of system output information. From the perspective of harmful information deviations and their propagation and transformation, a new method of hazard analysis based on Petri net model of system function implementation (SFI-PN) was presented in this part. The main idea of this method is to achieve combination of the SFI-PN

model and traditional safety analysis method such as HAZOP and FTA. Specifically, based on the place variables of SFI-PN model, hazards that are harmful information deviations will be identified by using HAZOP technology. For each transition variable, the FTA technology was used to analyze the rules of hazard's propagation and transformation from input information to output information. The flowchart of the presented method is shown in fig 2. It includes the following two key parts.

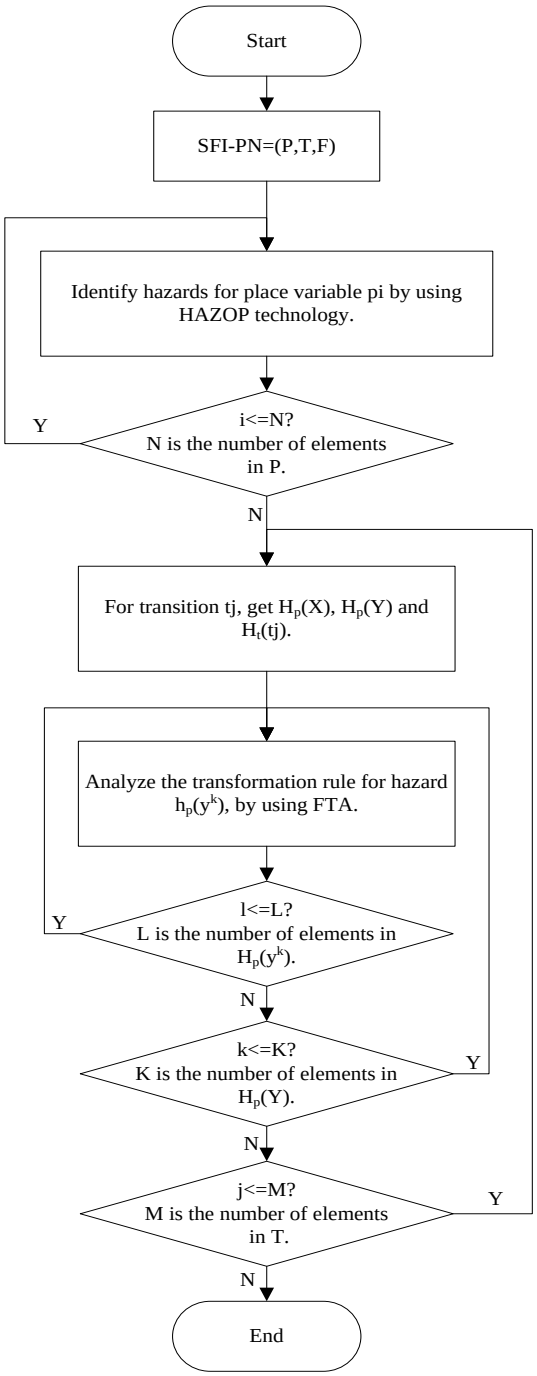

***Fig 2**. The flowchart of Petri net model-based hazard analysis*

1. Hazard Identifying Based on SFI-PN Model

Each place variable p ∈ P of the SFI-PN model represents a kind of system information. Place p can be seen as an element. In combination with some HAZOP guide words as shown in the table I, the information deviations, that are the system hazards, will be identified effectively. Generally, the hazard can be expressed as.

$$< \mathrm{id}, \mathrm{p}, \mathrm{type}, \mathrm{description} > \tag{2}$$

Where, id is a unique identifier for each hazard, p is a kind of system information, type is the type of information deviation, and description is the specific description of the hazard.

Taking the train speed information as an example, the deviations of it were identified, as shown in table II.

Table 1. *Guide words of information deviation*

Guide words	Meaning
No	The information is missing
Low	The value is lower than true value
High	The value is higher than true value
Ahead	The message arrived earlier than normal
Behind	Message delay

Table 2. *Train speed information deviations*

Element	Guide words	Deviation
Train speed	No	The train speed signal is missing
	Low	The speed value is lower than actual train speed value
	High	The speed value is higher than actual train speed value

2. Hazard Propagation and Transformation Rule Analysis Based on SFI-PN Model

Each transition t ∈ T of the SFI-PN model represents a functional module. It can be a board, a piece of code or a library. During its running process, the input information hazards transformed into the output information hazards by some rules. The FTA technology was used to analyze those rules.

Set X ⊆ P and Y ⊆ P is the pre-set and post-set of transition t respectively. $H_p(x^j)$ is the hazard space of $x^j \subseteq X$, $j \subseteq \{1,2,\ldots,M_x\}$, M_x is the number of elements in set X. $h_p(x^j) \subseteq H_p(x^j)$ is one hazard of x^j, which is expressed as formula (2). Then, the input information hazard space $H_p(X)$ of t is the Cartesian product of $H_p(x^j)$, that can be expressed as:

$$H_p(X) = H_p(x^1) \times H_p(x^2) \times \cdots \times H_p(x^{M_x}) \tag{3}$$

$H_t(t)$ is the hazard space of t ∈ T. $H_p(y^i)$ is the hazard space of $y^i \in Y$, $i \in \{1,2,\ldots,M_y\}$, M_y is the number of elements in set Y.

Take $h_p(y^i) \in H_p(y^i)$ as the top event of fault tree. $H_p(X) \cup H_t(t)$ is the basic event space. By using the Fault Tree Analysis, the following formula can be obtained

$$\text{if } h_p(X) \text{ and } h_t(t) \text{ then } h_p(y^i) \tag{4}$$

Where $h_p(X) \in H_p(X)$, $h_t(t) \in H_t(t)$, $h_p(y^i) \in H_p(y^i)$. That is the rule of hazard propagation and transformation.

C. Construction and Analysis of Functional Safety Analysis CPN Model

From the above analysis, a functional safety analysis CPN (FSA-CPN) model could be constructed. The FSA-CPN was defined as the following ten-tuple in formalization.

$$\text{FSA-CPN} = (P, T, A, \sum, V, N, C, G, E, I) \tag{5}$$

Where, P, T, A, Σ, V, N, C, G, E and I are the same as defined in general CPN [5] and the following six specific conditions should be satisfied.

1. Each place $p \in P$ represents a kind of system information. Each transition $t \in T$ represents a functional module. Each arc $a \in A$ represents interaction between system functional modules.

2. Color set Σ is the set of types of system hazard. Each place p has its color type $C(p) \in \Sigma$, which is expressed as formula (2), to represent that information deviation.

3. Every token in place represents one system hazard, that is, one type of information deviations.

4. The initial marking M_0 represents the hazards coming from external input information.

5. Under pre-conditions of marking M and constraint b, the firing condition of transition t was expressed as.

$$\sum_{p \in {}^{\cdot}t} E(p,t) < b > \leq M(p) \text{ and } G(t) < b > = \text{true}$$

6. After transition t is fired, system marking changes from M_1 to M_2, and for each $p \in P$, the following equation was satisfied.

$$M_2(p) = M_1(p) - \sum E(p,t) < b > + \sum E(t,p) < b >$$

And the rule of hazard transformation that was expressed as formula (4) should be satisfied too.

Due to the CPN model's formalized modeling ability and powerful description capability of the color token, it could be used to analyze the propagation and transformation of hazards in the process of system function implementation, integrating with traditional safety analysis method such as HAZOP and FTA, etc. With the use of mature simulation analysis tool—CPN Tools, the following results in three aspects were obtained.

1. The harmful information deviation that is system hazard was identified effectively and

comprehensively.

2. The rules of hazard propagation and transformation in the process of system functional implementation were obtained deductively by using FTA technology.

3. Through analyzing the simulation result of FSA-CPN model, the key hazard and hazard's combination which may cause the system functional failure was found out.

III. MODELING AND ANALYSIS OF CBTC OVERSPEED PROTECTION

In this paper, CBTC overspeed protection was taken as an example to show how to implement functional safety analysis of CBTC system based on CPN model.

A. Overspeed Protection of CBTC

Overspeed protection is one of the key functions of CBTC system to ensure train running safety [6]. The overspeed protection principle is shown in fig 3.

The train speed determination unit receives speed signal from speed sensor and calculates the current train speed value. Train location determination unit calculates the train location value based on train speed data and positioning data from tag on the ground. Data receive unit receives the ZC data through DCS system and sends MA information to MA analysis unit, which generates the MA data by synthesizing basic line information stored in the on-board database and MA information. Based on train location data, MA data and train traction calculation models, the train protection speed is calculated. The overspeed protection control unit judges whether current train speed value is greater than protection speed and outputs the control data. The control data is safety critical information. Any of its harmful deviation may cause failure of CBTC overspeed protection directly.

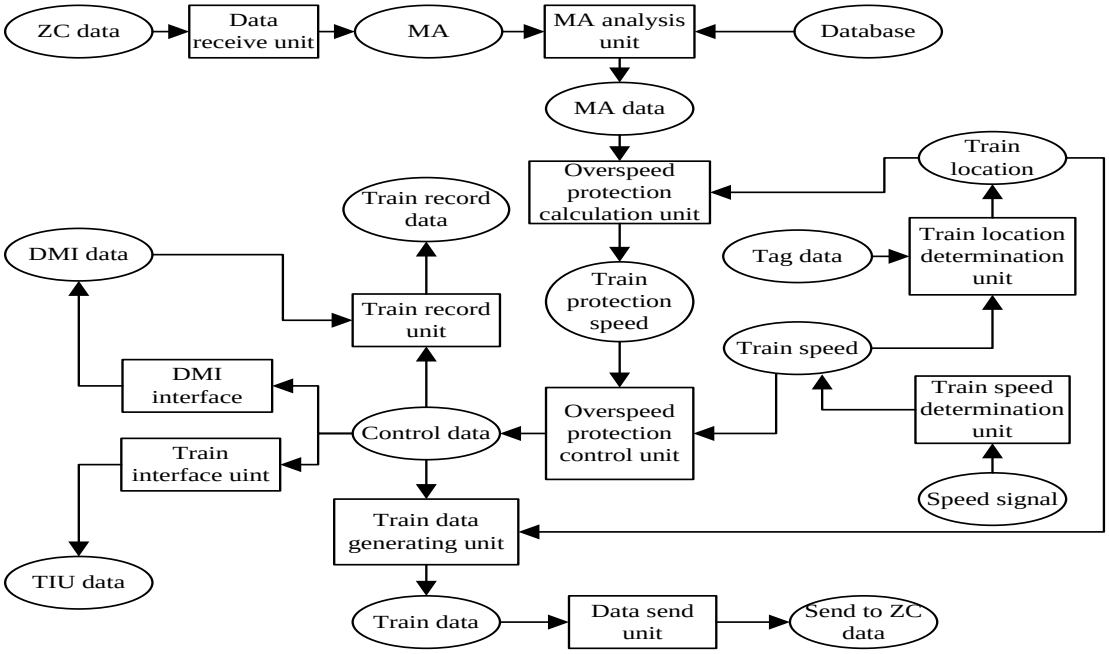

Fig 3. *The schematic diagram of CBTC overspeed protection*

B. FSA-CPN Modeling of Overspeed Protection

This section includes three parts, followed by SFI-PN modeling of overspeed protection, hazard analysis of overspeed protection and FSA-CPN modeling of overspeed protection.

1. SFI-PN Model of Overspeed Protection

On the basis of the above functional principle analysis, the SFI-PN model of overspeed protection has been constructed, as shown in fig 4. The description of Petri net model's place and transition is shown in table III.

It could be verified that the constructed Petri net model is bounded, security and activity. It can be used to describe the implementation process of CBTC overspeed protection reasonably.

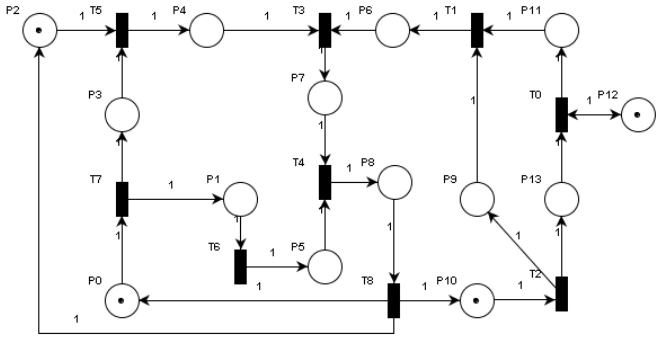

Fig 4. *The SFI-PN model of CBTC overspeed protection*

Table 3. *Description of place and transition*

Place	Description	Transition	Description
P0	Speed signal	T0	Access line data
P1	Train speed data	T1	Calculate overspeed protection curve
P2	Tag data	T2	Analyze MA information
P3	Train speed data for location	T3	Calculate train protection speed
P4	Train location value	T4	Overspeed protection dicision
P5	Train speed value	T5	Train location determination
P6	Overspeed protection curve	T6	Train speed determination
P7	Train protection speed	T7	Get train speed signal
P8	Control data	T8	Reset simulation
P9	MA data		
P10	MA information		
P11	Basic line information		
P12	Database data		
P13	Access database		

2. Hazard Analysis of Overspeed Protection Based on SFI-PN Model

To effectively accomplish the analysis in this paper, we make the following reasonable assumptions.

1. There is no failure of system functional module.

2. Since the on-board line data was strictly checked, so it does not has any hazard.

3. Here only one kind of hazard—information deviation was considered. For normal information, the deviation value is zero.

According to the method proposed in section II, hazards were identified, including train location information deviation, train speed information deviation, MA data deviation etc. Because of the limit of space, only train location information deviation was given here, as shown in table IV.

The rules of hazard propagation and transformation in the implementation process of CBTC overspeed protection were also obtained. There was five groups of rules in total, including train speed determination, train location determination, calculating overspeed protection curve, calculating train protection speed and overspeed protection dicision. Due to the limit of space, only partial hazard transformation rules of train location determination were given here, as shown in table V.

Table 4. *Train location information deviations*

Information	Deviations
Train location	<1, train location, high, the location value is bigger than actual value >
	<2, train location, low, the location value is smaller than actual value >
	<3, train location, no, the location information is lost>
	<4, train location, normal, the location value is correct>

Table 5. *Hazard transformation rule of train location determination (partial)*

Number	Description of rules
1	If <1, tag data, ahead, -> and <1, train speed, high, -> then <1, train location, high, ->
2	If <2, tag data, behind, -> and <2, train speed, low, -> then <2, train location, low, ->
3	If <3, tag data, normal, -> and <4, train speed, no, -> then <3, train location, no, ->
4	If <4, tag data, no, -> and <3, train speed, normal, -> then <4, train location, normal, ->

3. FSA-CPN Model of Overspeed Protection

On the basis of the above analysis results, The FSA-CPN model of CBTC overspeed protection was constructed, as shown in fig 5.

In the FSA-CPN model, the place represented a kind of system information. The color set of it was the description of information deviation i.e. the system hazard. The tokens in place were the representations of specific hazards.

When the fire condition of transition was satisfied, the transition fired with the transferring of tokens by the rules as shown in table V. That was the propagation and transformation of hazards.

The initial tokens of the net represented system input information hazards. The initial marking of the FSA-CPN model of CBTC overspeed protection was shown in table VI.

C. Simulation and Analysis

The simulation of CBTC overspeed protection FSA-CPN model was performed with CPN Tools. Through analyzing the simulation results, the key hazards and their combination that may cause the failure of CBTC overspeed protection were found out.

After the simulation has been running 10000 steps, there were 1250 tokens in the place P8 which represents system output information. It means that system has outputted 1250 pieces of control information, including both safe and unsafe ones. By statistical analysis, 21 kinds of hazard combination that may lead to the failure of CBTC overspeed protection were obtained, as shown in table VII.

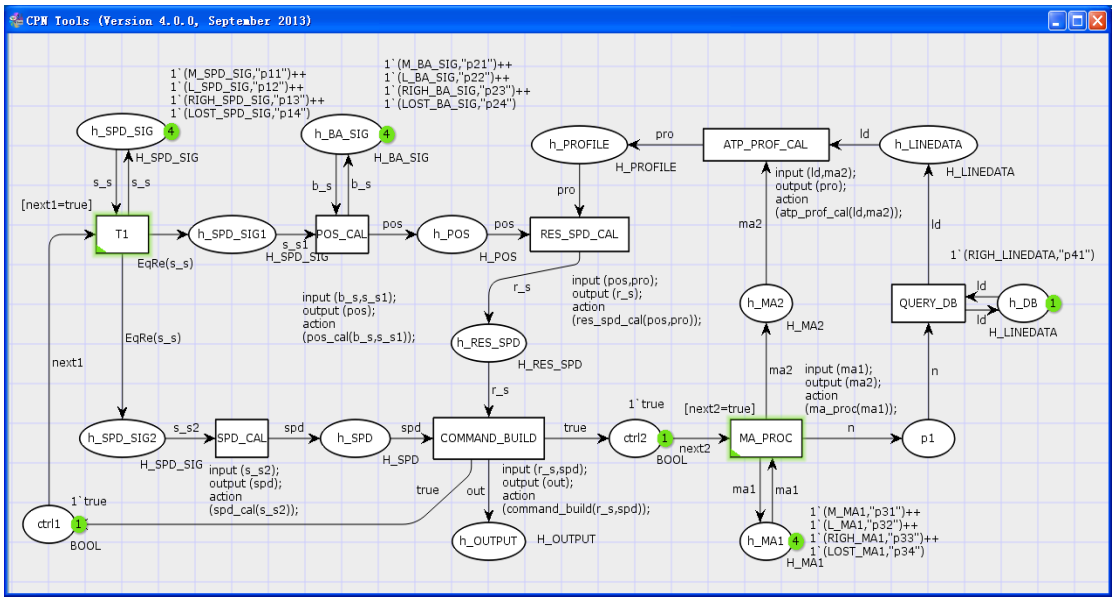

Fig 5. *The FSA-CPN model of CBTC overspeed protection*

Table 6. *The initial marking of cbtc overspeed protection FSA-CPN model*

Number	Place	Intial tokens
1	P0	<1, speed signal, high, - >, <2, speed signal, low, - >, <3, speed signal, normal, - >, <4, speed signal, no, - >
2	P2	<1, tag data, ahead, - >, <2, tag data, behind, - >, <3, tag data, normal, - >, <4, tag data, no, - >
3	P10	<1, MA information, high, - >, <2, MA information, low, - >, <3, MA information, normal, - >, <4, MA information, no, - >
4	P12	<1, database data, normal, - >

Table 7. *21 kinds of hazard combination of CBTC overspeed protection*

Number	Hazard combination
1	<1, tag data, ahead, - > and <1, speed signal, high, - > and <1, MA information, high, - >
2	<1, tag data, ahead, - > and <2, speed signal, low, - > and <1, MA information, high, - >
3	<1, tag data, ahead, - > and <3, speed signal, normal, - > and <1, MA information, high, - >
4	<2, tag data, behind, - > and <1, speed signal, high, - > and <1, MA information, high, - >
5	<2, tag data, behind, - > and <1, speed signal, high, - > and <2, MA information, low, - >
6	<2, tag data, behind, - > and <1, speed signal, high, - > and <3, MA information, normal, - >
7	<2, tag data, behind, - > and <2, speed signal, low, - > and <1, MA information, high, - >
8	<2, tag data, behind, - > and <2, speed signal, low, - > and <2, MA information, low, - >
9	<2, tag data, behind, - > and <2, speed signal, low, - > and <3, MA information, normal, - >
10	<2, tag data, behind, - > and <3, speed signal, normal, - > and <1, MA information, high, - >
11	<2, tag data, behind, - > and <3, speed signal, normal, - > and <2, MA information, low, - >
12	<2, tag data, behind, - > and <3, speed signal, normal, - > and <3, MA information, normal, - >
13	<3, tag data, normal, - > and <1, speed signal, high, - > and <1, MA information, high, - >
14	<3, tag data, normal, - > and <2, speed signal, low, - > and <1, MA information, high, - >
15	<3, tag data, normal, - > and <2, speed signal, low, - > and <3, MA information, normal, - >
16	<3, tag data, normal, - > and <3, speed signal, normal, - > and <1, MA information, high, - >
17	<4, tag data, no, - > and <1, speed signal, high, - > and <1, MA information, high, - >
18	<4, tag data, no, - > and <2, speed signal, low, - > and <1, MA information, high, - >
19	<4, tag data, no, - > and <2, speed signal, low, - > and <2, MA information, low, - >
20	<4, tag data, no, - > and <2, speed signal, low, - > and <3, MA information, normal, - >
21	<4, tag data, no, - > and <3, speed signal, normal, - > and <1, MA information, high, - >

From the number of times each hazard occurs in table VII, it could be known that the key hazards causing to the failure of CBTC overspeed protection are the following three in turn:

long MA data, low speed measurement value and forward deviation of tag position.

IV. CONCLUSION

The objective of this paper is to study the problem of hazard identifying and hazard propagation and transformation in process of system function implementation. By integrating Petri net modeling and simulation, HAZOP technology and FTA technology, a CPN based system functional safety analysis method is presented. The method focuses on characterization of hazard and its propagation and transformation in the process of function implementation and indentifying the hazard that may cause the failure of function implementation. Taking CBTC overspeed protection function as an example, the effectiveness and applicability of using the proposed method to functional safety analysis of CBTC system were verified. The analysis results show that the key hazards causing to the failure of CBTC overspeed protection are the following three in turn: long MA data, low speed measurement value and forward deviation of tag position.

On the other hand, the computational quantity of using the presented algorithm to analyze the hazard transformation rule may be large and the temporal factors do not be considered. That will be the next work of this research.

References

[1]. Rail Transit Vehicle Interface Standards Committee of the IEEE Vehicular Technology Society. IEEE Std1474.1-1999, IEEE standard for Communications-Based train control (CBTC) Performance and functional requirements, 1999.

[2]. *R. Niu, T. Tang*, A Model-based Framework for Safety Analysis of Computer-Based Railway Signaling System [C], COMPRAIL 2010, 2010.

[3]. *Hwang Jong-Gyu, Jo Hyung-Jeong, Kim Dong-Hee*. Hazard Analysis of Train Control System Using HAZOP-KR Methods [C]. International Conference on Electrical Machines and Systems, 2010: 1971-1975.

[4]. *Muttram R. I*, Railway Safety's Safety Risk Model [C]. Proceedings of the Institution of Mechanical Engineers, 2002, 216(2): 71-79.

[5]. *K. Jensen, L. M. Kristensen*, Coloured Petri Nets. Modeling and Validation of Concurrent Systems [M], Springer, 2009.

[6]. *X. J. Liu*, Research on the key technologies of communication based train control system in urban rail transit [D]. Lan zhou: Lanzhou Jiaotong University, 2009♦