

# Modeling and Verification of CTCS-3 On-board Equipment Based on Colored Petri Net

Han Jingjia<sup>1</sup> and He Tao<sup>2</sup>

<sup>1</sup>School of Lanzhou Jiaotong University, Lan Zhou, China

<sup>2</sup>Gansu Research Center of Automation Engineering Technology for Industry & Transportation, Lan Zhou, China

1558155326@qq.com

**Abstract.** The on-board control system is the kernel subsystem of the CTCS-3 train control system which is the key to ensure the safety of train operation. According to the complexity of CTCS-3 train control system, first of all, this paper analyzes the mode conversion rules of the on-board equipment of CTCS-3, establishes the model conversion scenario (MTCPN) model based on Colored Petri Net, and introduces the use branch in the CPN Tools. The sequential logic ASK-CTL formula and the non-standard state space query method formally verify the constructed MTCPN model, and the verification result is true, indicating that the constructed MTCPN model satisfies the rules of the CTCS-3 Train Control System Requirements Specification (SRS). The mode conversion function conforms to the on-board device mode conversion process, and through the verification result, the mode conversion scene of the on-board device is analyzed to have deadlock-free and transferability.

## 1. Introduction

China's high-speed railway uses thousands of kilometers of CTCS-3 train control system [1]. The train control on-board subsystem is mainly responsible for the overspeed protection of the train running speed. Its safety and reliability directly affect the safety of the train operation. The modeling of the on-board equipment mode transformation and the verification of the consistency between the functional realization of on-board equipment and its own requirements are helpful to timely find equipment problems and improve equipment performance, so as to guarantee the train safety.

There are many researches on modeling and verification of high-speed railway train control systems at home and abroad. For example, Platzer etc in the literature by using a differential dynamic logic based on differential invariants technology of train control system in Europe such as modeling, examination and validation, from which Europe's description found many not strictly, then they can strictly proved further by designing an security properties in the form of a model. There are also many researchers in China who try to model and formalize the Chinese high-speed railway train control system. For example, in the literature [2], the author proposed a set of modeling and validation methods of the train control system specifications according to the extensive application of UML in the industry and the advantages of SMV model inspection tool. In the literature [3], The author used Petri net to model and analyze the channel model of CTCS-3 and the time characteristics of data transmission, which provides the premise and basis for the design of relevant parameters in the CTCS-3 specification.

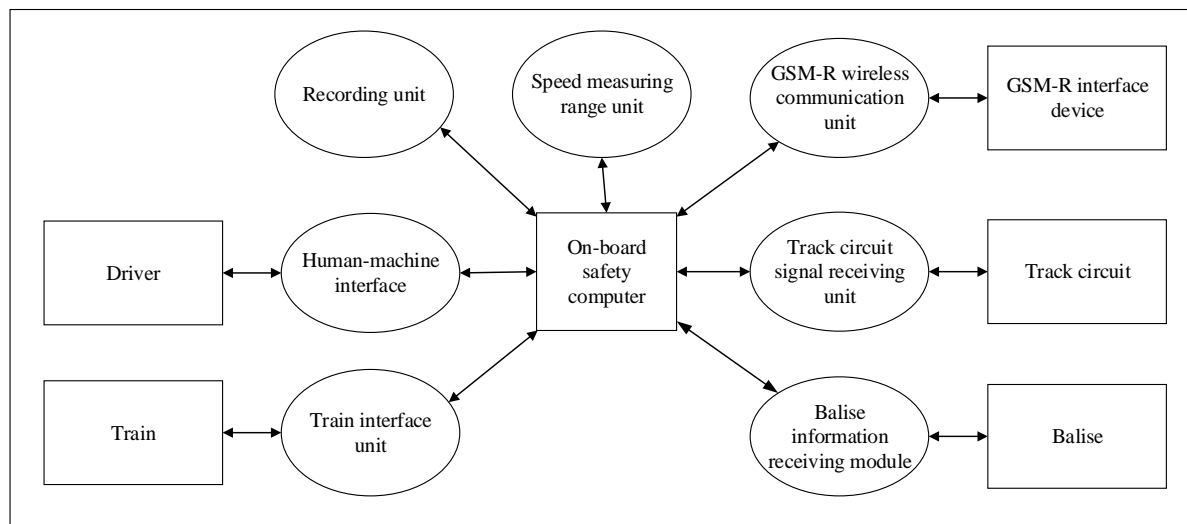


Among the many system modeling methods and languages, the model established by Colored Petri Net CPN (Colored Petri Net) is executable, which is beneficial to dynamic simulation and suitable for large systems with synchronization, concurrency and resource sharing [4]. At the same time, CPN has a formal mathematical definition with a good grammatical and semantic definitions, which is usually used for the verification of system functionality and logical correctness.

As can be seen from the above, the software and hardware development of the system needs to be evaluated by the security system, and the complexity of the system becomes a difficult problem for the security evaluation of the system, which is difficult to design and develop, and difficult to find some security risks [5]. Therefore, this paper establishes a model conversion model using a language based on Colored Petri Nets and verifies it with the CPN Tools.

## 2. Introduction to the on-board equipment of CTCS-3 train control system

The CTCS-3 consists of two parts: on-board equipment and ground equipment. Through the combination of in-vehicle information exchange and on-board equipment and EMU brake equipment, the train overspeed protection function is completed. The on-board equipment mainly include a on-board safety computer, a human-machine interface, a GSM-R wireless communication unit, a recording unit, a track circuit signal receiving unit, and speed measuring range unit, a balise information receiving module, a train interface unit and other components. The on-board equipment is an important ensure for the safe operation of the train. Its main features include: Receive information such as driving permission, temporary speed limit, and line parameters transmitted by RBC (Radio Block Center); Send train operation dynamic information to RBC; Receive information such as positioning reference information and train running direction provided by the transponder; Receive information such as line parameters transmitted by the track circuit; Train running speed real-time measurement and running distance and calculation of target distance mode control curve; When the train is overspeed, the automatically implemented of common brake or emergency brake; RBC/RBC handover; HMI management, judicial data recording function [6]. The structure of CTCS-3 on-board equipment is shown in Figure 1.

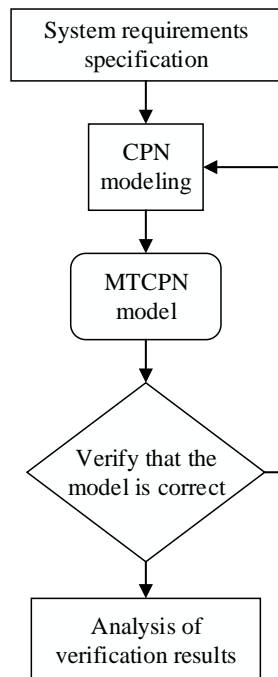


**Figure 1.** CTCS-3 train control system on-board equipment structure.

### 3. Construction of MTCPN model

#### 3.1. Modeling process

The overall framework of model transformation and verification of on-board equipment based on Colored Petri Net is shown in Figure 2.



**Figure 2.** On-board equipment modeconversion modeling and verification block diagram.

In the first step, according to the mode conversion part of the CTCS-3 Train Control System Requirements Specification (SRS) [7], the model transformation of the on-board equipment of the CTCS-3 is modeled by Colored Petri Nets. Process requirements strictly adhere to the on-board equipment mode conversion specification; In the second step, the MTCPN model is constructed based on the Colored Petri Net. The model adopts the hierarchical (2 layers) construction rules. The upper model shows the conversion path between the modes. The lower model shows the specific conversion process of each mode conversion; The third step is to introduce the formal verification of the constructed MTCPN model using the branch timing logic ASK-CTL formula and the non-standard state space query method in the CPN Tools to analyze whether the model meets the CTCS-3 Train Control System Requirements Specification (SRS) requires the mode conversion function and whether the model conforms to the on-board equipment mode conversion process. If not, return to the first step to re-use the Colored Petri Net to model the on-board equipment; In the fourth step, based on the correct model verification results, the attributes of the system are analyzed from two aspects: deadlock-free and transferability.

#### 3.2. Construction of MTCPN model

The mode conversion part of the CTCS-3 requirements specification defines the working mode and mode-related functions of the on-board equipment. The mode management function manages the working mode of the on-board system, continuously monitors the transition conditions between modes and performs mode switching to ensure that the train is transferred to a specific working mode under certain conditions, and works according to the safety duties specified by the mode. Different working modes are set for on-board equipment to realize different functions in different modes, so as to more effectively complete the requirements of train operation control.

The CTCS-3 train control system includes 9 operation modes: SB, SH, FS, OS, CO, SL, TR, PT, and IS [8]. The on-board equipment realizes the conversion between the nine modes according to the transition conditions between the functions and modes in each mode, so that the train can run under different conditions [9], and some working modes can be directly converted, but some work modes cannot be converted directly, only indirect conversions. As shown in Table 1, there are 39 pattern conversion instances.

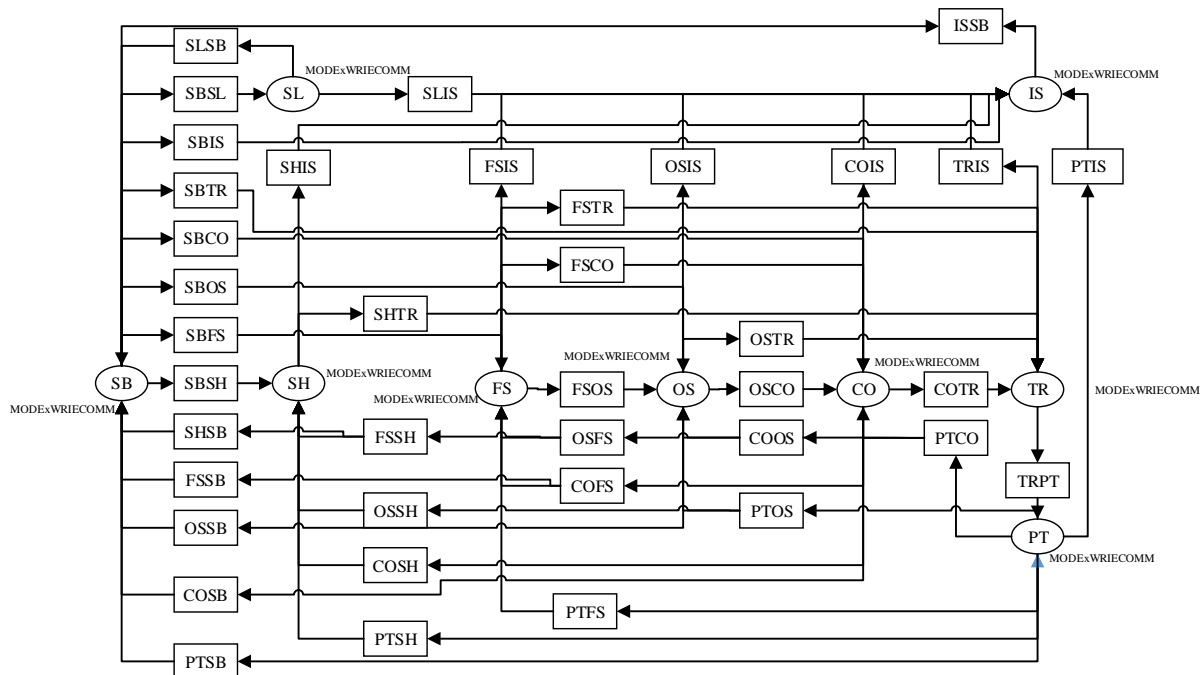
**Table 1.** More conversion of CTCS-3

Pattern classification	Mode conversion
SB	SB→SH, SB→FS, SB→OS, SB→CO, SB→SL, SB→TR, SB→IS
SH	SH→SB, SH→TR, SH→IS
FS	FS→SB, FS→SH, FS→OS, FS→CO, FS→TR, FS→IS
OS	OS→SB, OS→SH, OS→FS, OS→CO, OS→TR, OS→IS
CO	CO→SB, CO→SH, CO→FS, CO→OS, CO→TR, CO→IS
SL	SL→SB, SL→IS
TR	TR→PT, TR→IS
PT	PT→SB, PT→SH, PT→FS, PT→OS, PT→CO, PT→IS
IS	IS→SB

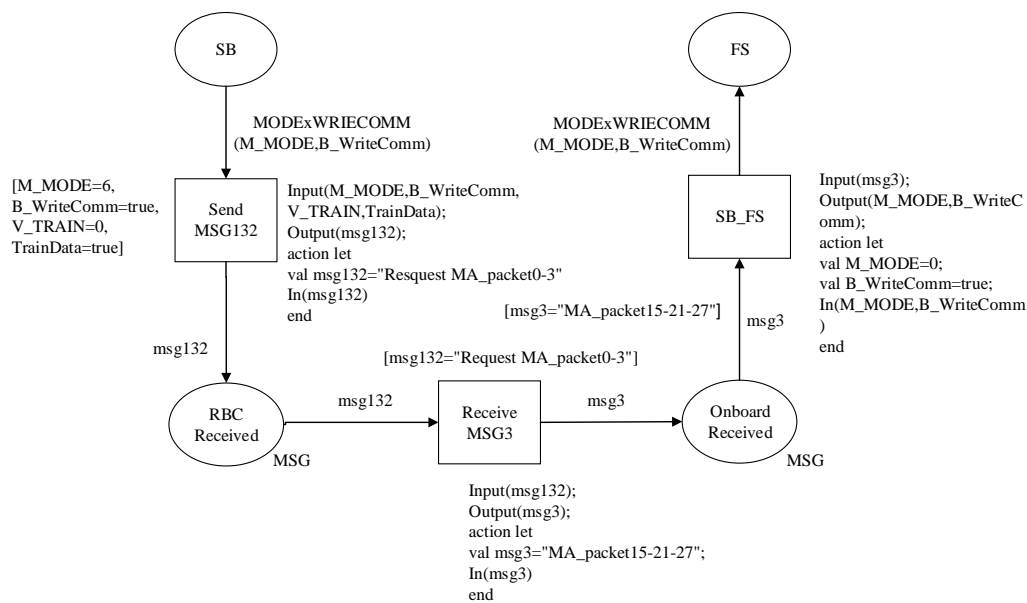
The following eight modeling rules are proposed according to the CTCS-3 Train Control System Requirements Specification (SRS) [10].

- The MTCNP model is constructed by layered (2 layers) modeling rules. The upper layer model shows the conversion path between the modes, and the lower layer model shows the specific conversion process of each mode conversion.
- "Conversion condition 18" in the CTCS-3 Train Control System Requirements Specification (SRS) is for the CTCS-2 level and will not be discussed in this paper.
- In order to make the MTCNP model simple and universal, except the SH, IS and SL modes, the default mode has established a communication session with the RBC, and only considers the mode conversion process, and does not process the mode after the mode conversion.
- In order to make the MTCNP model easy to analyze, all processes related to the balise are processed according to a single balise.
- The modeling process strictly abides by the on-board equipment mode conversion specification, and does not consider special circumstances.
- The mode conversion of the upper layer model of MTCNP is represented by alternative transition, and the specific conversion process is represented by the lower layer model of MTCNP.
- In the MTCNP model, the definitions of colors, variables, and libraries are all followed by certain rules to aid the algorithm.
- The judgment behavior of the data content is reflected in the guard function.

The MTCNP model is constructed. Among them, the upper model is shown in Figure 3. There are 39 lower-level models, and only the lower-level model of the SB mode to FS mode is given here, as shown in Figure 4.



**Figure 3.** Upper layer model of MTCPN model.



**Figure 4.** Underlying model of SB mode to FS model.

## 4. Formal verification of vehicle equipment mode conversion

### 4.1. Verification of MTCPN model

Mode conversion is a key part of the requirements specification, which describes the on-board equipment conversion of CTCS-3 in different working environments. Once the work environment changes, the corresponding mode conversion is required. The correctness of the conversion between

modes is one of the important factors affecting the control level, transportation capacity and safety of the train control system, so it is necessary to modify the on-board equipment.

The basic idea of model validation is to represent the behavior of the system with the state transfer system and describe the properties of the system with the modal/temporal logic formula. Therefore, in this section, based on the Colored Petri Net model detection theory, the constructed MTCPN model is verified by using the branch sequential logic ask-ctl formula and the non-standard state space query method.

For the deadlock verification of the model in Figure 3, the CTL formula used is: ! (Dead Marking & AX (AG (Dead Marking))), and the verification result is shown in Figure 5.

```
let
  val fid=TextIO.openOut"DeadMarking.txt"
  val _=TextIO.output(fid,"List of dead markings:\n")
  val _=EvalNodes(ListDeadMarkings(),)
  fn n=>INT.output(fid,n)
  val _=TextIO.output(fid,"\n Number of dead markings:")
  val _=INT.output(fid,length(ListDeadMarkings()))
in
  TextIO.closeOut(fid)
end;
```

**Figure 5.** Deadlock verification of MTCPN model.

For the transferability verification of the model for Figure 4, the CTL formula used is: EF (state = SB & EX (state = FS)), and the verification result is shown in Figure 6.

```
fun IsConsideredTs a=(TI.SBFS'SB_FS 1=ArcToTI a);
val myASKCTLformula=MODAL(POS(AF("Is Dead Transition",IsConsideredTs)));
eval_node myASKCTLformula InitNode;

fun IsConsideredTs a=(TI.FSTR'ReceiveMSG16 1=ArcToTI a);
val myASKCTLformula=MODAL(POS(AF("Is Dead Transition",IsConsideredTs)));
eval_node myASKCTLformula InitNode;
```

**Figure 6.** Transfer verification of MTCPN model.

#### 4.2. Model verification result analysis

According to the model verification results, the attributes of the system are analyzed from two aspects: deadlock-free and transferability:

**4.2.1. Deadlock-free verification.** No deadlock means that the system will not stay in a state forever. It can be seen from Figure 5 that the modeling verification result is true, indicating that the system has no deadlock in one mode, and thus it can be seen that the MTCPN model has no dead identification node and belongs to a strong connected graph, the MTCPN model constructed satisfies the mode conversion function required by the CTCS-3 Train Control System Requirements Specification (SRS), and has deadlock-free.

**4.2.2. Transferability verification.** Transferability refers to a 1-step migration relationship between one model and another in the model, the modeling verification result is true in Figure 6, indicating that the system can migrate from the SB state to the FS state through one conversion step, indicates that the system is transferable from SB mode to FS mode, it can be seen that the constructed MTCPN model conforms to the on-board equipment mode conversion process and has a transferability.

## 5. Conclusion

Since the on-board equipment is a safety-critical system with a safety level of 4, this paper mainly analyzes the safety issues involved in the design of CTCS-3 on-board equipment, and converts between the modes of the on-board system of CTCS-3. MTCPN modeling is carried out between the specific conversion process between path and mode, and the MTCPN model of the constructed MTCPN model is introduced in the CPN Tools by using the branch timing logic ASK-CTL formula

and the non-standard state space query method, the verification results show that the mode conversion MTCPN model satisfies the mode conversion function required by the CTCS-3 Train Control System Requirements Specification (SRS), which conforms to the on-board equipment mode conversion process, and analyzes whether the MTCPN model has no characteristics such as deadlock-free and transferability. Therefore, the modeling verification method has certain guiding significance for the design of safety critical system.

### Acknowledgments

Gansu industrial transportation automation engineering technology research center 2019 open fund GSITA201902 research on key technologies of scene conversion of high-speed railway signal system integrated experimental platform.

### References

- [1] Lu Jidong 2011 *Layered Formal Modeling and Verification Analysis of Train Operation Control System* (Beijing: Beijing Jiaotong University)
- [2] Tang Tao and Gao Chunhai 2005 *Analysis of ETCS and CTCS*. (Electr D Locomot) chapter 6 pp 1–3
- [3] Xu Tianhua and Zhao Hongli 2008 *Reliability analysis of wireless communication of ETCS using Colored Petri Net*. (RailSci) chapter 6 pp 38–42
- [4] Liu Jiankun 2013 *Study on some key issues of train control system based on Petri net* (Chengdu: Xihua University) p 4
- [5] Dong Wei and ShuiJing 2013 *Formal Modeling and Verification of CTCS-2 Level Train Control System* (Computer Engineering) pp 12-15
- [6] Mou Xiaoling and Ding Xiaoming 2012 *Research Progress of Test Case Generation Based on Petri Nets* (Journal of Chongqing Jiaotong University(Natural Science Edition)) pp 163-167
- [7] Department of Science and Technology of the Ministry of Railways 2009 *CTCS-3 Train Control System Standard Specification - CTCS-3 Level Control System System Requirements Specification (SRS) (Volume 1)* (Beijing: China Railway Publishing House)
- [8] Li Wei and Wang Haifeng 2010 *Optimization of test sequence of on-board equipment for CTCS-3 train control system* (Journal of Beijing Jiaotong University) pp 75-78
- [9] Wei Baiquan and Lu Jidong 2018 *Research on Test Case Generation Method of CTCS-3 Train Control System Based on TAO Variation Analysis* (Journal of Southwest Jiaotong University) pp 2-11
- [10] Zhao Xiaoyu and Yang Zhijie 2017 *Method for generating pattern conversion test sequence of vehicle equipment based on Colored Petri Nets* (China Railway Science) pp 115-122