

C3+ATO Function Simulation and Verification Analysis Based on Timed Automata

Jie YAO¹ and Zhenhai ZHANG

School of Automation and Electrical Engineering, Lanzhou Jiaotong University

Abstract. C3+ATO system plays an important role in controlling train operation and its function is related to the safety of train automatic operation. A simulation and verification method based on timed automata is proposed to verify the function of high-speed railway C3+ATO system. The functional requirements in the C3+ATO system specification are extracted and the timed automata models are established and then the timed automata network model is formed. The message sequence charts are generated and system safety, reachability, existence are verified. As a result, the models meet the functional requirements of the system which provide theoretical reference for the subsequent C3+ATO system design and development, test and measurement, practical application and related specification improvement.

Keywords. C3+ATO system, mode transition for on-board equipment, timed automata, UPPAAL

1. Introduction

At the end of 2019, the BeiJing-Zhang Jiakou Railway which is equipped with Chinese self-developed high-speed railway automatic operation system (C3+ATO system) officially opened and operated, marking the entry of China into the era of intelligent high-speed railway. The C3+ATO system is the key technology equipment to realize train automatic operation function. It is the high-speed train control system which adds the automatic operation function on the basis of the existing train control system (CTCS-2/CTCS-3) function. C3+ATO system is composed of on-board equipment and ground equipment [1]. Compared with the on-board equipment of existing control system, the number of equipment is expanded and the system function is increased. At the same time, with regard to the development planning of the next generation train control system, the number of side-rail equipment will gradually decrease and the function of on-board equipment will gradually increase. As the core equipment of C3+ATO system, it is of great significance to verify its functions.

According to [2], the formal method is a suitable method to verify the function of the train control system, which has been widely used in related research. Based on the timed automata, the function models of the on-board equipment of train control system

¹ Jie Yao, School of Automation and Electrical Engineering, Lanzhou Jiaotong University, China;
E-mail: 702399195@qq.com.

are established and verified [3,4]. The functional models of on-board equipment are established and carried out simulation verification based on random Petri network and colored Petri network [5,6]. A UML based multi-resolution fault analysis model is proposed for the safety of on-board equipment in CTCS-1 train control system [7]. Although the above literatures have achieved some results, it has not been involved in the functional verification and analysis of on-board equipment of C3+ATO system. C3+ATO system is a typical real-time safety demanding system and timed automata is widely used because of its good real-time characterization. As a result, this paper proposes a formal simulation and verification method for the mode transition function of on-board equipment based on timed automata. According to the technical specification of the C3+ATO system, the mode transition function sub-models of the on-board equipment are set up of each equipment and the timed automata network model is formed. Then, the message sequence charts and the corresponding verification statements are generated according to test specifications to carry out the formal verification analysis of the model.

2. Overview of C3+ATO System On-board Equipment

The on-board equipment of C3+ATO system is added ATO unit, GPRS radio station, wireless communication unit, ATO start button and related supporting equipment on the basis of the on-board automatic train protection(ATP) of the existing train control system, which realizes the functions of station automatic departure, interval automatic operation, train speed automatic control and compatible with on-board ATP function. The equipment composition is shown in Figure 1.

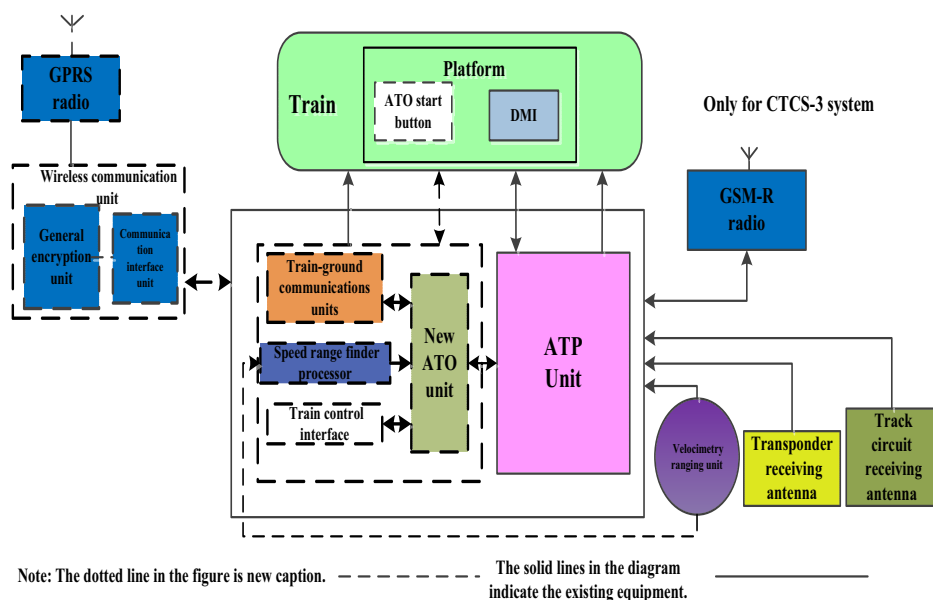



Figure 1. Composition diagram of on-board equipment for C3+ATO system

Among them, mode transition is an important function embodiment of C3+ATO system train-ground linkage control process and a prerequisite for the realization of automatic train operation function. The existing on-board equipment of train control system (excluding CTCS-2 train control system function) includes 9 working modes, full supervision mode (FS), shunting mode (SH), calling on mode (CO), on sight mode (OS), standby mode (SB), isolate system mode (IS), sleeping mode (SL), trip mode (TR) and post trip mode (PT), and automatic mode (AM) is added to C3+ATO system. The transformation relationship of ten modes of C3+ATO system is showed as Table 1.

Table 1. On-board equipment mode transition table

	AM	FS	SH	CO	OS	SB	IS	SL	TR	PT
AM	—	3	1	2	1	1	1	0	6	0
FS	1	—	1	2	1	1	1	0	6	0
SH	0	0	—	0	0	0	1	0	3	0
CO	0	1	1	—	1	1	1	0	6	0
OS	0	1	1	1	—	1	1	0	4	0
SB	0	1	1	1	1	—	1	1	1	0
IS	0	0	0	0	0	1	—	0	0	0
SL	0	0	0	0	0	2	1	—	0	0
TR	0	0	0	0	0	0	1	0	—	1
PT	0	1	1	1	1	1	1	0	0	—

3. Function Model of On-board Equipment Mode Transition Based on Timed Automata

The timed automata is a finite state automata increased clock constraints can be described by a six-element group $\langle S, S_0, \Sigma, X, I, E \rangle$. S represents the nonempty poor state set. S_0 represents the initial state set. Σ represents the poor event set. X represents the clock variable set. I represents a map that defines the clock constraint as a migration condition and E represents the state migration set [8-10]. A state transition $\langle s_i, a_i, \lambda, \phi(x), s_j \rangle$ represent when the state position s_i satisfies the migration event is a_i and the clock constraint is $\phi(x)$ is transferred to the state position s_j and $\lambda \in X$ is reset. UPPAAL is a formal modeling and verification tool based on timed automata including editor, simulator and verifier. The functional attributes to be verified are transformed into BNF(Backus Naur Form) verification statements, which can be divided into three types according to the path expression including reachability, safety and existence. The meaning of the verification statement is shown in Table 2.

Table 2. Meaning of BNF verification

Type of property	Expression	Meaning
Reachability	$E \Diamond p$	There is a path in which p is true.
	$A[]p$	For all paths, p is true in all states of any path.
Safety	$E[]p$	There is a path in which p is true in all states.
	$A \Diamond p$	For all paths, it is true in any state of the path for p.
Existence	$p \rightarrow q$	When p is true, q is true.

According to the description of the on-board mode transition function in Section 2, the TA_{ATO}, TA_{Balise}, TA_{RBC}, TA_{Driver} and TA_{Train} models are established [11]. In the model, the double circle represents the initial state position of the model. The TA_{ATO} model is taken as an example to illustrate the information interaction process.

The mode transition can be realized based on on-board equipment records and current ground equipment status information by on-board ATO. When the on-board ATP is in FS mode, if train confirms that the brake/traction handle is not operated through the state value of Brakinghandle, the allowable ATO mode information through the event confirmation DtoT_ConfirmATO_m is received and the on-board ATO is connected to the vehicle interface MVB bus normally through the state value of MVBbusConnect, the on-board equipment changes from FS mode to AM mode. The transition <FS,,,AM> of TA_{ATO} occurs. When the on-board ATO is in AM mode, if train confirms the train stop through the state value of TrainState and the driver presses the "visual operation" button through the event of DtoT_ConfirmTripPro_m, the on-board equipment changes from AM mode to OS mode. The main positions and variables meaning in the model are shown as Table 3. The transition <AM,,,OS> of TA_{ATO} occurs. The model is shown as Figure 2.

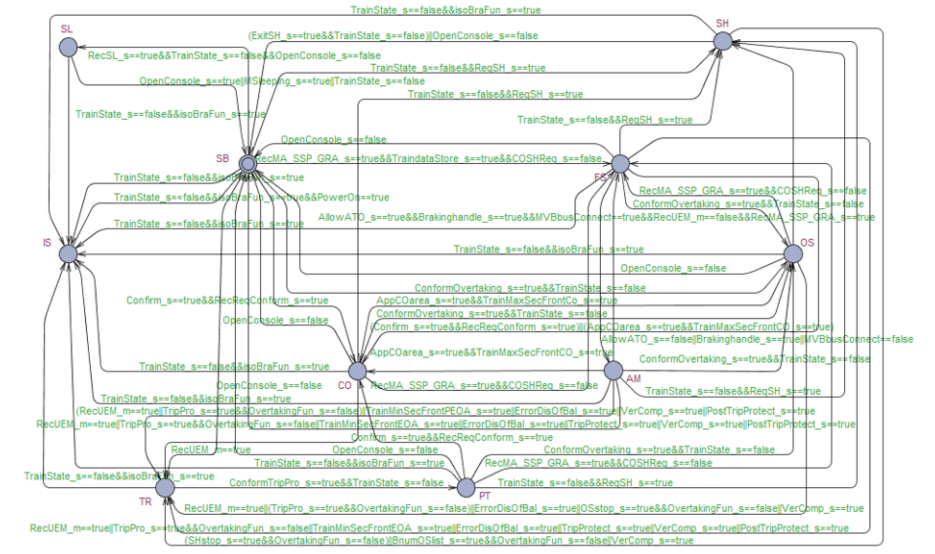


Figure 2. Timed automata sub-model of TA_{ATO}

Table 3. Key variables implications of the model

Number	Variables	Meaning	Number	Variables	Meaning
1	AllowATO	Whether or not a allow ATO signal is received ,0 means not received ,1 means received.	6	RecSL_m	Whether or not a sleep signal is received ,0 means not received ,1 means received.
2	Overtaking Fun	Whether or not overtaking function is activated ,0 means not activated ,1 means activated.	7	TrainState_s	Whether or not train stop, 0 means stop, 1 means not stop.
3	Brakinghandle_s	Whether or not the brakinghandle is operated ,0 means not operated ,1 means operated.	8	PostTripProtect_s	Whether or not to post trip protection ,0 means not protected ,1 means protected.
4	MSleeping	Whether or not a sleeping signal is received ,0 means not received ,1 means received.	9	CTCSVerComp	Whether or not the CTCS version is compatible ,0 means incompatible ,1 means compatible.
5	MVBbusConnect	Whether or not the MVBbus is normal ,0 means abnormal ,1 means normal.	10	RecUEM_m	Whether or not UEM signal is received ,0 means not received ,1 means received.

4. Formal Simulation and Verification Based on Timed Automata

The simulation of the model is mainly realized by generating the message sequence chart of the corresponding flow. The message sequence chart can observe the timing and content of the information interaction between the devices. Taking SB mode to SH mode and SB mode to IS mode as examples, the on-board equipment is in the default SB mode after the train is started. When the on-board equipment confirms that the train stops and the authorized shunting information is satisfied, the on-board equipment is transformed from SB mode to SH mode. When on-board equipment confirms that the disconnecter hits the isolation position, the on-board equipment is transformed from SB mode to IS mode. And the specific information interaction process is shown in Figure 3.

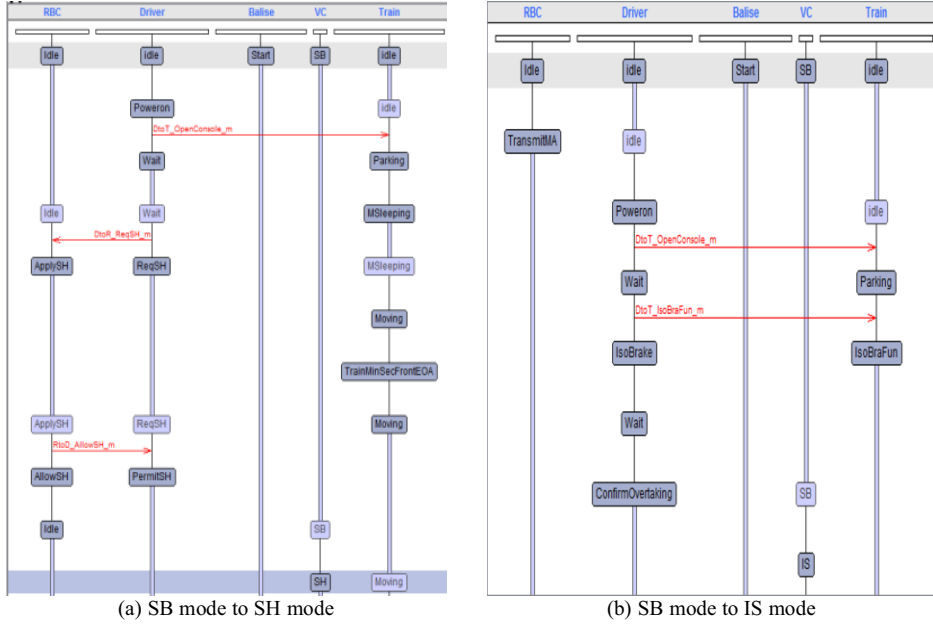


Figure 3. Model message sequence charts

The basic idea of model verification is to verify the reachability of state locations and whether state migration meets the current sequential logic constraints. After the model is established, the functional attributes are extracted and transformed into the corresponding BNF validation statements to verify the model [12]. The validation program entities are as follows.

System reachability verification.

- On-board ATO can complete the conversion process from initial SB mode to SH mode, from CO mode to FS mode and from OS mode to IS mode. $E \langle ((ATO.SB) \text{ imply } (ATO.SH)) \text{ and } ((ATO.CO) \text{ imply } (ATO.FS)) \text{ and } ((ATO.OS) \text{ imply } (ATO.IS))) \rangle$, passed verification.
- On-board ATO can complete the conversion from FS mode to AM mode, SB mode, SH mode, OS mode, CO mode, TR mode and IS mode. $E \langle ((ATO.FS) \text{ imply } (ATO.AM)) \text{ and } ((ATO.FS) \text{ imply } (ATO.SB)) \text{ and } ((ATO.FS) \text{ imply } (ATO.SH)) \text{ and } ((ATO.FS) \text{ imply } (ATO.OS)) \text{ and } ((ATO.FS) \text{ imply } (ATO.CO)) \text{ and } ((ATO.FS) \text{ imply } (ATO.TR)) \text{ and } ((ATO.FS) \text{ imply } (ATO.IS))) \rangle$, passed verification.

System safety verification.

- System not deadlock. $A[\text{not deadlock}]$, passed verification.
- When train confirms that the driver operates the train traction/braking handle or the "EMU allowed ATO mode" message is not received or the interface MVB bus fault between on-board ATO and train is a breakdown, on-board ATO exits from AM mode. $E[(((Train.AllowAM) \text{ imply } (Train.Moving)) \text{ or } (Train.AllowAM) \text{ imply } (Train.AllowAM)))]$, passed verification.

(Train.BrakeHandle) imply (Train.Moving) or (Train.MVBbusbreakdown) imply (Train.Moving)) and ((ATO.AM)imply(ATO.FS))), passed verification.

System existence verification.

- The on-board equipment can be changed from FS mode to AM mode when the train confirms that it has the conditions of permitted ATO mode information, not operated traction/brake handle, on-board ATO well connected to the train MVB bus, no emergency brake message received and MA received. On-board ATO can be changed from FS mode to AM mode. $A \triangleleft (((\text{Train.Moving}) \text{imply} (\text{Train.AllowAM}) \text{and} (\text{Train.Moving}) \text{imply} (\text{Train.BrakeHandle}) \text{and} (\text{Train.Moving}) \text{imply} (\text{Train.MVBbusbreakdown}) \text{and} (\text{Train.Moving}) \text{imply} (\text{Train.RecUEM}) \text{and} (\text{Train.Moving}) \text{imply} (\text{Train.RecMA})) \text{and} ((\text{ATO.FS}) \text{imply} (\text{ATO.AM}))),$ passed verification.
- When the train confirms the train stops and the driver confirms that the "visual" key is pressed, on-board ATO can be changed from AM mode to OS mode. $A \triangleleft (((\text{Train.ConformOvertaking}) \text{imply} (\text{Train.Parking})) \text{and} (\text{ATO.AM}) \text{imply} (\text{ATO.OS})),$ passed verification.

The above verification statements are input into the UPPAAL verifier for verification. All properties are verified. The results are shown in Figure 4.

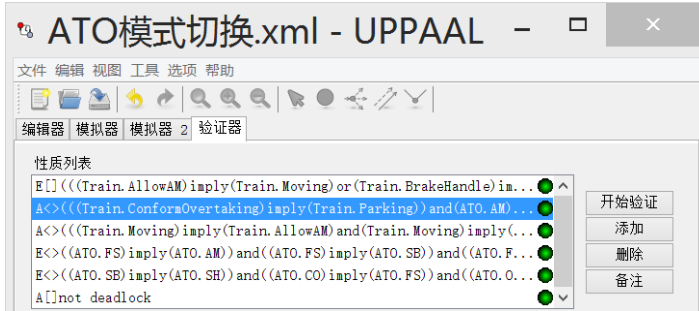


Figure 4. Model verification

5. Conclusion

C3+ATO system of high-speed railway has the characteristics of high operation efficiency, high degree of automation and intelligence, high level of safety and is related to train operation safety. If there are defects in system functions, it will endanger train operation safety. In this paper, the formal simulation and verification method based on timed automata is used. Taking the mode transition function of C3+ATO system on-board equipment as an example, the function model is established and the formal verification analysis is carried out. The main conclusions are as follows.

- The modeling and verification method of the system function is based on the technical specification, which the functional timed automata model is

established by extracting the functional requirements of the C3+ATO system technical specification to verify the functional requirements to be met. It is helpful to describe the system function comprehensively and accurately and to improve the scientificity, feasibility and organization of model verification.

- The message sequence chart between sub-models can help designers to deduce the communication process of the function deeply and understand the information interaction process of the whole system more vividly. According to the message sequence charts, we can reverse check whether there are errors in the process of establishing the model and perfect the defects in the system design and specification compilation.
- The analysis process of C3+ATO system function simulation and verification provides support for the theoretical research and practical application of the system. And the verified model can be used as the prototype of the system function test stage, which can provide theoretical reference for the function test and help to reduce the test input.

6. Acknowledgment

This research was supported by the National Natural Science Foundation of China (Grant No.61763025), Natural Science Foundation of Gansu (Grant No.18JR3RA124), China Postdoctoral Science Foundation funded project (Grant No.167306) .

References

- [1] Cheng JF, Feng K, Li K. C3+ATO system high speed railway train control technology. China Railway, 2019, (01): 74-77.
- [2] Kang RW. The Research on modeling methods and verification of Chinese train control system level 3 based on timed automata. Beijing, China:Beijing Jiaotong University, 2013.
- [3] Cao JY. Modeling and verification of on-board equipment of CTCS-3 train operation control system based on timed automata. Chengdu:Southwest Jiaotong University,2012.
- [4] Zhao WH. Scenario-based test cases generation for on-board subsystem. Beijing: Beijing Jiaotong University, 2014.
- [5] Hu XH, Wang YP, Chen Y. Modeling and simulation of vehicle equipment fault causing CTCS level conversation. Computer Engineering and Application,2016,52(18):208-213.
- [6] Zhao XQ, Zheng W, Tang T. Model-based formal approach for generating test cases and test sequences automatically by example of the ETCS-2[J]. Journal of the China railway society,2012,34(5):70-80.
- [7] Wang H. Safety analysis of CTCS-1 on-board equipment. Beijing:Beijing Jiaotong university,2017.
- [8] Alur R, Dill D L. A theory of timed automata. Theoretical Computer Science, 1994, 126: 183-235.
- [9] Yuan L, Lv JD, Liu Y, et al. Research on model-based test case generation method of on-board subsystem in CTCS-3. Journal of the China Railway Society, 2014, 36(8): 55-62.
- [10] Kunz G, Machado J, Perondi E. Using timed automata for modeling, simulating and verifying networked systems controller's specifications. Neural Computing&Applications, 2017, 28(5): 1031-1041.
- [11] Ministry of Science and Industry of the Railway Corporation[2018]No.8. Interim overall technical scheme of ATO system for high speed railway. Beijing: China Railway Corporation, 2018.
- [12] Ministry of Science and Industry of the Railway Corporation [2018]No.8. Temporary test case of ATO system for high-speed railway. Beijing: China Railway Corporation, 2018.