Hierarchical Modeling and Verification for High-speed Train Control Center by Time Automation

Lei Yuan
State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044，China
Email: lyuan@bjtu.edu.cn

Shiying Yang
State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044，China
Email: 12120291@bjtu.edu.cn

Dewang Chen
State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044，China
Email: dwchen@bjtu.edu.cn

Kaicheng Li
National Engineering Research Center of Rail Transportation Operation and Control System, Beijing Jiaotong University, Beijing, China
Email: kchli@bjtu.edu.cn

***Abstract*—Chinese Train Control System level three (CTCS-3) is a major technical system in Chinese high-speed rail and Train Control System (TCC) is indispensable component in the CTCS-3. Current researches on TCC are mainly based on the simulation, which cannot ensure that all conditions in TCC are tested. This paper presents a hierarchical modeling method and uses time automation (TA) to model the TCC software. We take the design of the active balise telegram editing, a major part in the TCC software, as an example. At first, the process of the active balise telegram editing is analyzed to obtain a hierarchical diagram containing several layers. Then, TA is employed to build one TA model for each layer. Lastly, we use UPPAAL (a model validation tool, developed by Uppsala University and Aalborg University) to construct a network of the TA models to verify the active balise telegram editing. The verification results demonstrate that this modeling method is feasible and the model can meet the functional requirements of the TCC software.**

***Index Terms*—TCC Software, Time Automation, UPPAAL, Hierarchical Modeling**

I. INTRODUCTION

The sustainable development of high-speed rail has been worldly recognized. In China, the Chinese Train Control System level three (CTCS-3) is significant technical equipment for guarantee of high-speed trains' speed at 350km/h. And, the TCC (Train Control Center) is key equipment in the CTCS-3 [1, 2]. So it is particularly important to guarantee the TCC's reliability in real-time operation which has significant influences on the overall management of high-speed trains' operations [3, 4].

There are some studies on TCC software. In most railway stations, the reliability of the TCC are still checked through continuous field tests [5], which cost too much in manpower, material and financial resources. The testing method cannot enable all the exiting problems reappear, so we cannot correct all of them. And during a comprehensive system test, the coverage rate of the test cases can hardly achieve 100% [6]. In addition, some simulation based on the HLA (High Level Architecture) for the TCC software was proposed [7]. Nevertheless, it is difficult to simulate all behaviors and every scene of a system through a simulation method [8].

To overcome the shortcomings of the simulation-based research on TCC software, we propose a hierarchical modeling method and uses time automation (TA) to model the TCC software. Hierarchical modeling emphasizes the graduated abstraction to simplify the system [9]. In a hierarchical model, the functions were enhanced layer by layer. Besides, the change of a layer is only associated with the parts of the upper layer and the lower layer. Hence, the hierarchical modeling can build up the scalability of the system. It can also strengthen the reusability of the model. Therefore, different scenes of the same layer can be used interactively. Using formal methods can maximize our understanding and analysis on a system and help us find the inconsistency, fuzziness, incompleteness or more [10-12]. TA, as a formal description method, has complete mathematical bases, which not only provide the methods of precise definition consistency and integrity, but also offer a method to prove the properties without running the system [13, 14].

In this paper, we take the process of active balise telegram editing process in the TCC software as an example. At first, the process of active balise telegram

doi:10.4304/jsw.9.6.1553-1560

editing is hierarchized to obtain a hierarchical diagram including some layers. Then, TA is employed to build one TA model for each layer. Lastly, we use UPPAAL (a model validation tool, developed by Uppsala University and Aalborg University) to obtain a network of the TA models, and verify them.

II. HIERARCHICAL MODELING OF TCC SOFTWARE

This section introduces the hierarchical design for the TCC software. And we take the process of the active balise telegram editing in the TCC software as an example to get a hierarchical model by TA. Firstly, we get the interface layer after analysis. Then we use TA to formally describe the interface layer to obtain its TA model. At last, we get other layers' TA models according to the same steps.

A. TCC's Hierarchy

As an important subsystem of CTCS-3, TCC has complex functions and a lot of information processing flows. Based on the idea of hierarchical modeling, we can build a TCC hierarchical model containing interface layer, scene layer, function layer and calculation layer. Combined with the function requirements of the train control, we get the hierarchical diagram of the TCC shown in Fig.1:

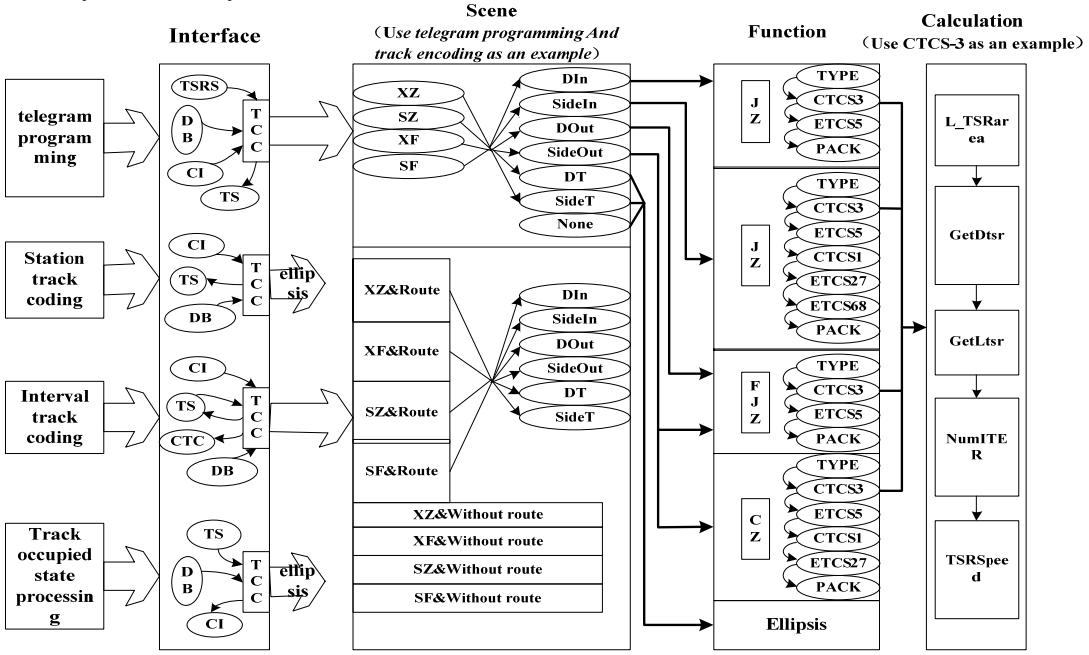

Fig.1 Hierarchy diagram of TCC

B. Hierarchical Modeling of the Active Balise Telegram Editing Function

The active balise telegram editing is an important part of the TCC software, which can help TCC send information to the train.

1. **Hierarchical design of the active balise telegram editing**

We will mainly introduce the interaction process between the TCC and the TSRS when editing the active balise telegram. In this case, the TCC needs to interact with the interlock, the TSRS, trackside emulator and database servers [15]. During the interaction, the interlock and the TSRS provide information to trigger the TCC active balise message's editing function. Fig.2 shows Interaction flow between the TCC and the TSRS, the TCC and the interlock.

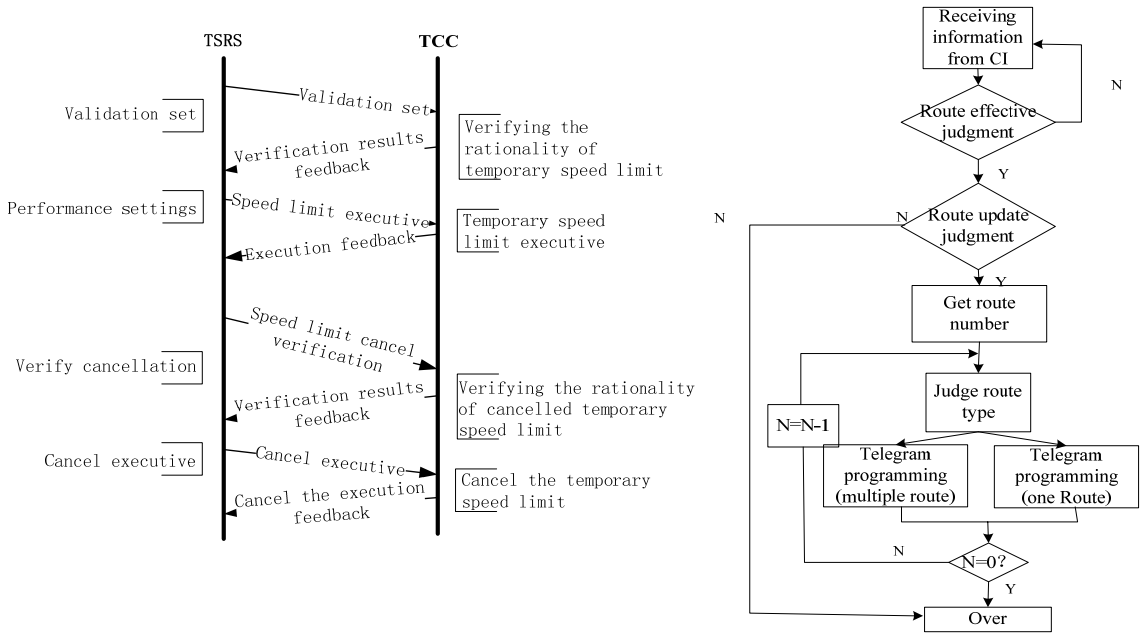

Fig.2 Interaction flow between the TCC and the TSRS (left); Interface flow between the TCC and the interlock (right)

2. **Hierarchical modeling of the active balise telegram editing**

We will use TA as the formal description to obtain TA models. First, we take the interface layer modeling of the active balise telegram editing as an example to introduce the modeling process. The interface layer includes the computer interlocking (CI) model and the temporary speed restriction (TSR) model. The interlock model includes six output models IFMsgCIOUT and one input model IFMsgCIIn. The six output models discharge the six routes and the input model judge the validity and real-time: if the information is effective and real-time, it feedbacks with receipt; otherwise, it asks the output model to resend the informationn. With the use of the TA, we establish the output model which is IFMsgCIOUT = $\langle S, S^0, A, X, I, E \rangle$:

a) Position set: S={WaitSendRoute, RouteSend, SendSuccess, SendFail, Update};
b) Initial position set: S^0={WaitSendRoute};
c) Channel set: A={route, sendfail, confroute};
d) Clock set: X={t, Tci};
e) State clock constraint: I={RouteSend：t<=10};
f) State transition path: E={<WaitSendRoute,route,RouteID==0,RouteSend>,<RouteSend,confroute,Tci<=T10,SendSuccess>,<RouteSend,sendfail,Tci<=T10,SendFail>,<SendFail,Update>,<Update,WaitSendRoute>}.

The input model IFMsgCIIn = $\langle S, S^0, A, X, I, E \rangle$ is

a) Position set: S={CIMsgIn HandleMsg Update};
b) Initial position set: S^0={CIMsgIn};
c) Channel set: A={route sendfail confroute circle Scn};
d) Clock set: X={t, Ttcc};
e) State clock constraint:I={HandleMsg t<=10&&Ttcc<=10};
f) State transition path: E={<CIMsgIn,route,t==0,HandleMsg >,<HandleMsg,sendfail,RsvTSR==0||j>7||Ttcc>=10,CIMsgIn>,<HandleMsg,circle,HandleMsg>,<HandleMsg,confroute,j<=7&&RsvTSR==1,Update>,<Updata,CIMsgIn,Scn>}.

The output model IFMsgCIOut and input model IFMsgCIIn are shown in Fig.3(a) (b).The input model receives channel signal “sendfail!” from the output model by sending “sendfail?” so that it can ask to resend the route information. And through the classifying commands given by the scene layer which are “directin!”, “sideout!”, “sidethrough!” and so on, the input model can ask to edit the required information package. In the end, we trigger the calculation of every information package obeying the instructions given by the function layer. Besides the aforementioned channels, we set the global variables to control the synchronization and asynchronism of the member automata. Here, the global variable RouteID is used to synchronize the route information and ITER is used to synchronously control the number of the segments. Then, the variable again is utilized to asynchronously control the update of the interlocking information receiver.

Then, we use TA to get the output model IFMsgTSROUT and the input model IFMsgTSRIn of TSR on the interface layer, which are shown in Fig.3(c) (d). Fig.4-Fig.6 are showing the scene layer model ScnMsgBuilder, the function layer model FunMsgBuilder and the calculation layer model CalMsgBuilder.

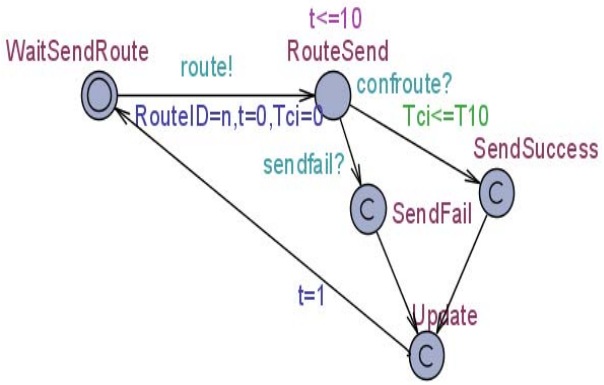

Fig.3 (a) Output model IFMsgCIOut of CI

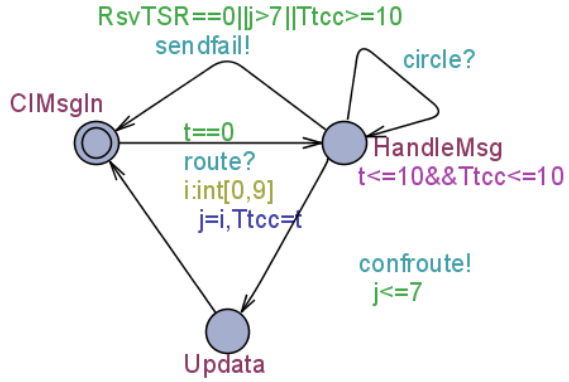

Fig.3 (b) Input model IFMsgCIIn of CI

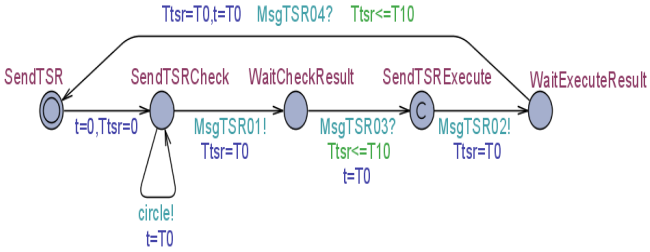

Fig.3 (c) Output model IFMsgTSROUT of TSR

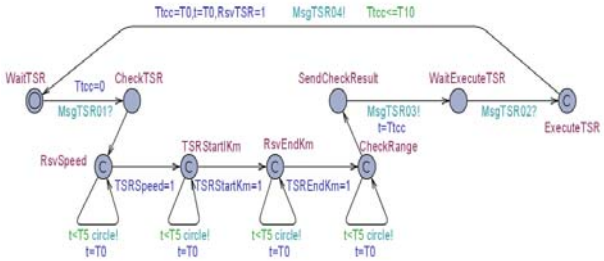

Fig.3 (d) Input model IFMsgTSRIn of TSR

Fig.3 Interface layer model IFMsgBuilder

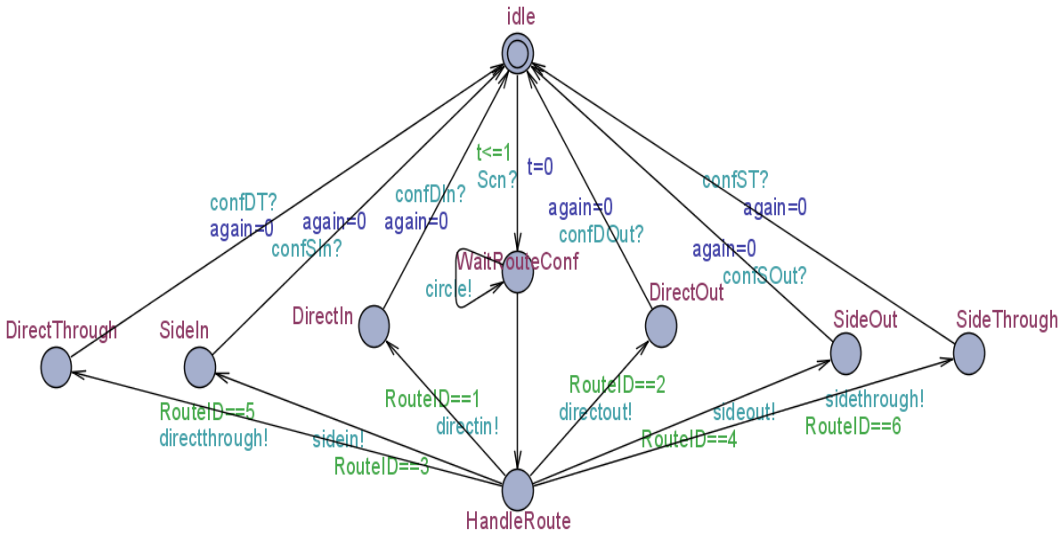

Fig.4 Scene layer model ScnMsgBuilder

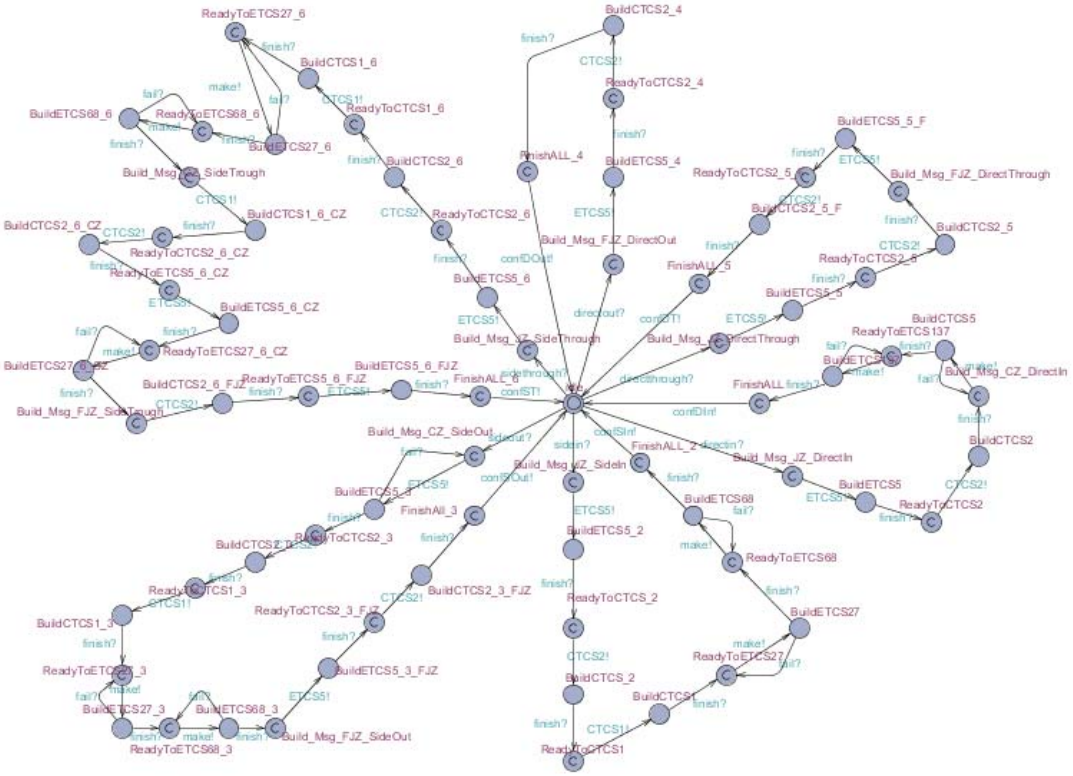

Fig.5 Function layer model FunMsgBuilder

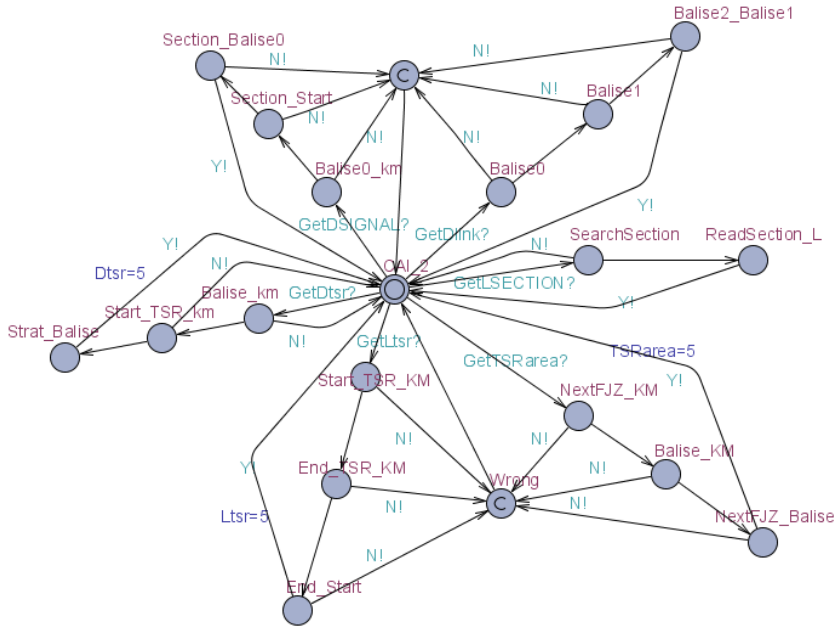

Fig.6 Calculation layer model CalMsgBuilder

III. SIMULATION AND VERIFICATION

According to the above mentioned hierarchical modeling for the active balise telegram editing in the TCC software, we will model the net of TA and check the function for positively down line direction and verify it. Besides, we also check other functions.

A. UPPAAL Model of the Process of the Active Balise Telegram Editing Function

With the UPPAAl, verification tool for TA models [16], we get the TA network called ISFC-MsgBuilder from the above models:

IFMsgCIOut||IFMsgCIIn||IFMsgTSROUT||IFMsgTSRIn||ScnMsgBuilder||FunMsgBuilder||CalMsg1||CalMsg2.T

his network can achieve the function of the active balise telegram editing through the coordination of each member TA model.

B. Verification of the Active Balise Telegram Editing

The ISFC-MsgBuilder model includes the interface layer, the scene layer, the function layer and the calculation layer. Then we will verify the ISFC-MsgBuilder model to find whether it meets the performance and function requirements of the TCC software, where, ISFC-MsgBuilder=IFMsgBuilder ||ScnMsgBuilder||FunMsgBuilder||CalMsgBuilder.

In UPPAAL, we can clearly see the changes of each state and the signal transceiver in the state transition process. Fig.7 shows the relationship of the state transition between the four automata. It implements the process from receiving the state of the side line pick-up approach to editing the balise information package. With the help of the UPPAAL, we can predict the process as soon as possible. Hence, the simulation plays an important role in developing the TCC software.

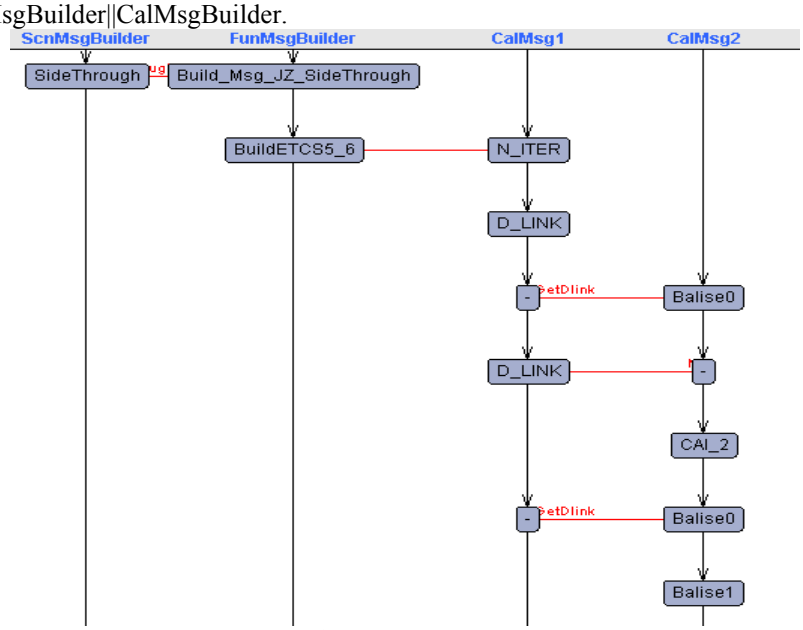

Fig.7 Using UPPAAL simulators to verify the message preparation process

In UPPAAL, we use the BNF(beat nation final) language to describe the function and performance of ISFC-MsgBuilder model. Specific information is as follows:

a) A[]not deadlock

No deadlock in system;

b)

E<>((IFMsgTSRIn.RsvSpeed)or(IFMsgTSRIn.TSRStartIKm)or(IFMsgTSRIn.RsvEndKm)or(IFMsgTSRIn.CheckRange))

The train receives the speed limit information and monitor.

c)

E<>((IFMsgCIOUT1.SendFail)imply(IFMsgCIOUT1.SendSuccess)or(IFMsgCIOUT2.SendFail)imply(IFMsgCIOUT2.SendSuccess)or(IFMsgCIOUT3.SendFail)imply(IFMsgCIOUT3.SendSuccess)or(IFMsgCIOUT4.SendFail)imply(IFMsgCIOUT4.SendSuccess)or(IFMsgCIOUT5.SendFail)imply(IFMsgCIOUT5.SendSuccess)or(IFMsgCIOUT6.SendFail)imply(IFMsgCIOUT6.SendSuccess))

The interlock information can be automatically updated, and eventually sent successfully;

d)

E<>((ScnMsgBuilder.DirectIn)or(ScnMsgBuilder.DirectOut)or(ScnMsgBuilder.SideIn)or(ScnMsgBuilder.SideOut)or(ScnMsgBuilder.DirectThrough)or(ScnMsgBuilder.SideThrough))

The verification results are shown in Fig.8 which indicates that the TCC software can achieve the active balise telegram editing through different approaches. We also verify other functions of the ISFC-MsgBuilder model:(1) the TCC software can send two basic kinds of route telegrams;(2) speed limit telegram can be sent when the station block has speed limit;(3) the TCC software can send absolute parking information to prevent aggressiveness and drop-in;(4) it can trigger the alarm when the TCC software link fail with other equipment;(5) the interlocking information can be updated in real-time and sent successfully. Fig.8 shows that the ISFC-MsgBuilder model can achieve the above functions. This confirms the reliability of the design for the TCC software.

Hence, this modeling method is feasible and the models we built by TA can meet the functional requirements of the TCC software.

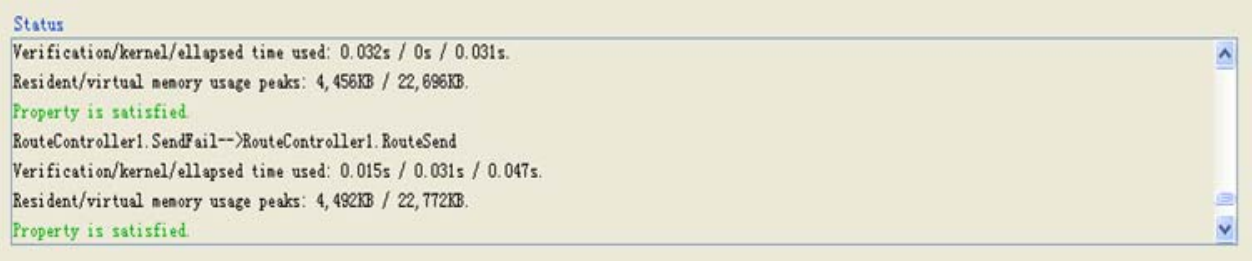

Fig.8 The verification results of UPPAAL

V. CONCLUSIONS

The paper proposes a hierarchical modeling method and TA to model the TCC software of the CTCS-3. After analyzing the whole system, we divide TCC software into four layers. Taking the active balise packet editing process as an example, we modeled the process of the active balise telegram editing and built the ISFC-MsgBuilder model. At last, we verify the performance of the obtained model in UPPAAL. The verification results demonstrate that hierarchical modeling by TA is a feasible and convenient for designing the TCC software. And the model we built by this method can meet the functional requirements of the TCC software.

Further on, some subjective factors may exist in modeling and analyzing, and standardizing the modeling process is a problem to be studied in the latter part of software verification.

ACKNOWLEDGMENT

This work is partially supported by the National High Technology Research and Development Program ("863" Program) of China under grant 2012AA112800, by New Scientific Star Program of Beijing under grant 2010B015, by the Fundamental Research Funds for the Central Universities under grant 2012JBM016, by the independent research project from the State Key Laboratory of Rail Traffic Control and Safety under grant RSC2011ZT001.

REFERENCES

[1] C.M. He, T.G. Ma, Zheng west passenger line CTCS-3 control system user needs verification. Journal of railway communication signal engineering technology, 1: 9-13, (2011).
[2] S.G. Zhang. Jinghu high speed railway system optimization research: China railway publishing house (2009).
[3] Y. Zhang, X.Y. Wei, C.M. He. Secure communication standard Subset-098 safety analysis: Railway Communication Signal, 11 (2009).
[4] Beijing traffic communication signal research institute, CTCS-3 control system and vehicle equipment introduction. 1 (2009).
[5] L. Liu, Research on control system field test and auxiliary tool for CTCS-3: Beijing Jiaotong university master dissertation (2010).
[6] X.Q. Li, Preliminary research of simulation technology for CTCS-3 based on Multi-Resolution Modeling: Beijing Jiaotong university master dissertation (2009).
[7] H.F. Wang, The formalization development method research. Beijing on safety critical systems: Beijing jiaotong university doctoral dissertation (2002).
[8] T.L. Gu, Software formalization method. Beijing: higher education press (2005).
[9] R. Alur, T. Dang, J. Esposito, Y. Hur, Hierarchical modeling and analysis of embedded systems, Proceedings of the IEEE, 91(1): 11-28, (2003).
[10] S.H. Yang, J.Z. Wu, A.P. He, Y.B. Rao, Derivation of OWL Ontology from XML Documents by Formal Semantic Modeling, Journal of Computers, 8(2):372-379,(2013).
[11] F. Yan, Rail transit train operation control system of the formal modeling and model test method. Beijing: Beijing Jiaotong university doctoral dissertation (2006).
[12] D.Craigen, Formal Methods EVES and Safety Critical Systems: Technical Report FR-94-5479-04.Minister of National Defence, Ontario, Canada (1994).
[13] H.D. Jin, Y.S. Zhang, Si.W. Gao, Train operation adjustment of optimization and simulation: Science and Technology, 12 (2007):18 - 22.
[14] J. Hoenicke, P. Maier, Model-Checking of Specification Integrating Processes: Data and Time, Lecture Notes in Computer Science, 3582: 465-480, (2005).
[15] Z. Yang, L. Yang, X.Y. Luo, L.R. Ma, B.S. Kou, K. Zhang, Model of Domain based RBAC and Supporting Technologies, Journal of Computers, 8(5):1220-1229,(2013).
[16] M. Benerecetti, N. Cuomo, A. Peron, TPMC: A Model Checker For Time–Sensitive Security Protocols, Journal of Computers, 4(5):366-377, (2009).

Lei Yuan was born in 1978. He received the M.S. degree in School of Electronic and Information Engineering, Beijing Jiaotong University, China in 2004. He is now working at the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing. His research interests include the method of design, simulation and test of train control system.

Shiying Yang was born in 1989. She received the B.S. degree in Electronics and Information Engineering, Beijing Jiaotong University, China in 2012. She is working toward the M.S. degree with the Electronics and Information Engineering, Beijing Jiaotong University. Her research interests include machine learning, principle curve.

Dewang Chen was born in 1976. He received the B.S. degree in Mechanical and Electrical Engineering and Ph.D. degree in Control Theory and Control Engineering from the Institute of Automation, Chinese Academy of Sciences in the M.S. degree in Control and Automation from Harbin Engineering University in 1998 and 2000, respectively, and the

2003. He is a Professor with the State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University since 2011. His current research interests include intelligent control, machine learning, soft computing, optimization and their applications in intelligent transportation systems and railway systems.

Kaicheng Li was born in 1966.He received the M.S. degree in Electronics and Information Engineering, Beijing Jiaotong University, China in 1991. He is now an associate professor with National Engineering Research Center of Rail Transportation Operation and Control System, Beijing Jiaotong University, Beijing, China. His research interests include automatic train operation, communications based train control.