Journal of System Simulation

Volume 33 | Issue 4 Article 23

4-14-2021

Modeling and Verification of Scene of C3+ATO System Based on Timed Automata

Zhenhai Zhang
School of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China;

Yao Jie
School of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China;

Modeling and Verification of Scene of C3+ATO System Based on Timed Automata

Abstract

Abstract: The C3+ATO system is in the experimental stage in our country and has the characteristics of high automation degree and high safety requirement at present. In order to confirm whether the specific function of the high-speed railway C3+ATO system meets the corresponding technical specification under the specific scene, a formal modeling and verification method based on the timed automata is proposed. *The station automatic departure scene is selected as the modeling object. The functional requirements of C3+ATO system specification are extracted and the timed automata model of the scene is established. The message sequence chart of the corresponding process is generated, and the functional attributes of the system are verified and the model is simulated at the C3+ATO train control simulation platform.* The simulation results show that the model meets the security function attributes and restricted activity attributes of the system technical specification, and can provide theoretical reference for the system design, practical application and improvement of related specifications.

Keywords

C3+ATO system, timed automata, UPPAAL, station automatic departure, message sequence chart

Recommended Citation

Zhang Zhenhai, Yao Jie. Modeling and Verification of Scene of C3+ATO System Based on Timed Automata[J]. Journal of System Simulation, 2021, 33(4): 951-961.

第 33 卷第 4 期 系统仿真学报© Vol. 33 No. 4
2021 年 4 月 Journal of System Simulation Apr. 2021

基于时间自动机的 C3+ATO 系统场景建模与验证

张振海，姚婕
（兰州交通大学 自动化与电气工程学院，甘肃 兰州 730070）

摘要：C3+ATO 系统目前在我国处于试验发展阶段且具有自动化等级高、安全标准高等特点。为验证具体场景下高速铁路 C3+ATO 系统功能是否符合对应技术规范，提出一种基于时间自动机的形式化建模与验证方法。*选取车站自动发车场景作为建模对象，提取 C3+ATO 系统规范中的功能需求，建立场景的时间自动机模型，生成对应流程的消息顺序图并对系统功能属性进行验证，在 C3+ATO 列控仿真平台仿真验证。*仿真验证结果证明：模型满足C3＋ATO系统的安全功能属性和受限活性需求，为后续系统设计开发、实际应用及相关规范完善提供理论参考。

关键词：C3+ATO 系统；时间自动机；UPPAAL；车站自动发车；消息顺序图
中图分类号：TP391.9 文献标志码：A 文章编号：1004-731X (2021) 04-0951-11
DOI: 10.16182/j.issn1004731x.joss.19-0662

Modeling and Verification of Scene of C3+ATO System Based on Timed Automata

Zhang Zhenhai, Yao Jie

(School of Automation and Electrical Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China)

Abstract: The C3+ATO system is in the experimental stage in our country and has the characteristics of high automation degree and high safety requirement at present. In order to confirm whether the specific function of the high-speed railway C3+ATO system meets the corresponding technical specification under the specific scene, a formal modeling and verification method based on the timed automata is proposed. *The station automatic departure scene is selected as the modeling object. The functional requirements of C3+ATO system specification are extracted and the timed automata model of the scene is established. The message sequence chart of the corresponding process is generated, and the functional attributes of the system are verified and the model is simulated at the C3+ATO train control simulation platform.* The simulation results show that the model meets the security function attributes and restricted activity attributes of the system technical specification, and can provide theoretical reference for the system design, practical application and improvement of related specifications.

Keywords: C3+ATO system; timed automata; UPPAAL; station automatic departure; message sequence chart

引言

2018 年末，我国自主研发的应用于时速 300 km 以上的高速铁路自动驾驶系统(C3+ATO 系统)成功完成评审，象征着我国高铁将迎来自动驾驶的新征程。高铁自动驾驶技术是保留现有的列控系统(CTCS-3 级，Chinese Train Control System Level Three)功能，同时增加自动驾驶功能的先进技术，而自动驾驶是由车载设备代替司机完成控车命令计算、速度调整等功能的技术。根据国际公共交通协会对轨道交通自动化等级的划分标准，C3+ATO 系统属于 GOA2 级(Grade of Automation Level

收稿日期：2019-12-19 修回日期：2020-05-29
基金项目：国家自然科学基金(61763025)；中国博士后科学基金(167306)
第一作者：张振海(1983-)，男，博士，副教授，研究方向为交通信息工程及控制。E-mail：764411629@qq.com

Two)。随着系统自动化级别的提高，列车运行也面临着更高的安全标准。因此，C3+ATO 系统具有自动化智能化等级高、运行效率高、安全要求高等特点，同时由于目前列车自动驾驶(Automatic Train Operation, ATO)技术仍处于研发试验阶段，而且在不同的运营场景下 C3+ATO 系统表现的功能不同。因此，研究具体运营场景下高速铁路 C3+ATO 系统功能是否满足相应的技术规范要求，是保障自动驾驶安全运行的基础。

目前，针对高速铁路 C3+ATO 系统功能特性建模与验证的研究相对较少，但是关于 CTCS-3 级列控系统建模与验证的研究已相对成熟。同时，大量应用实例表明，形式化方法适用于列控系统功能属性的验证分析。形式化方法是一种立足于系统功能属性，利用数学语义和文法定义系统功能、生成系统等效模型，并依据系统规范标准对模型进行验证的方法。常用的形式化方法有：TA (Timed Automata)，TPN(Timed Petri Net)，HCSP(Hybrid Communicating Sequential Engineering)等[1]。其中，有限状态自动机增加时钟约束条件构成时间自动机，它是一种面向实时系统形式化建模的理论，现已在 CTCS-3 级列控系统建模分析方面有广泛的实践和应用。康仁伟[2]利用时间自动机建立 CTCS-3 级列控系统等级转换场景、临时限速场景的网络模型，并分析其功能属性，有效验证了 2 个场景的实时性。万勇兵等[3]利用消息顺序图建立临时限速服务器(Temporary Speed Restriction Server，TSRS)和其他系统之间的信息交互模型，然后基于时间自动机理论建立等效网络模型，并验证系统的功能、性能属性。胡彩莲等[4]采用消息顺序图和时间自动机结合的方式建立 CTCS-3 级列控系统等级转换场景模型，仿真验证模型的安全性和受限活性。依据上述关于 CTCS-3 级列控系统形式化建模分析的实例，本文从功能角度出发将系统运营场景中不同设备之间的关联关系以模型的形式描绘出来。选取车站自动发车场景作为建模对象，提取 C3+ATO 系统技术规范中的功能需求，基于时间自动机利用 UPPAAL 建立场景模型，仿真生成场景对应流程的消息顺序图，并且根据高速铁路 ATO 系统测试案例标准生成系统功能属性的验证语句，验证场景的安全功能属性和受限活性需求。该模型的仿真验证过程为 C3+ATO 系统后续设计开发、系统相关规范内容完善以及系统间通信信息交互过程的相关理论研究和实际应用提供参考。

1 C3+ATO 系统概述

1.1 C3+ATO 系统特点

C3+ATO 系统是在 CTCS-2/CTCS-3 级列控系统的基础上，在系统软件、硬件设备以及功能方面增添新的需求，从而实现车站自动发车、区间自动运行、车站自动停车等功能的高铁自动驾驶系统[5]。

(1) 软件、硬件方面：车载设备增加 ATO 单元、GPRS 电台(General Packet Radio Service)及其他设备，地面设备在 TSRS，CTC(Centralized Traffic Control)，TCC(Train Control Center)上增加 ATO 功能，轨旁增设精确定位应答器，如图 1 所示。

(2) 系统功能方面：新增的车载 ATO 是基于 ATP(Automatic Train Protection)的行车许可，结合 GPRS 传输的运行计划、站间数据等信息实现车门/站台门联动控制、列车速度自动控制等功能；TSRS 保留现有功能，再增加转发运行计划以及站台门命令/状态信息等功能；CTC 保留现有功能，再增加运行计划发送等功能[6-7]。

1.2 C3+ATO 系统车站自动发车场景分析

车站自动发车不仅是 C3+ATO 系统典型运营场景之一，而且是 C3+ATO 系统重要的功能需求，同时又是整个自动驾驶过程实现的重要组成部分，分为始发站自动发车和中间站自动发车 2 种。考虑到始发站自动发车场景接收信息的复杂性、设备交互的频繁性，本文选取始发站自动发车作为建模场景。始发站自动发车场景的相关功能主要由车载 ATO，TSRS，CTC，Driver 或 Balise(应答器)实现，具体场景流程如下。

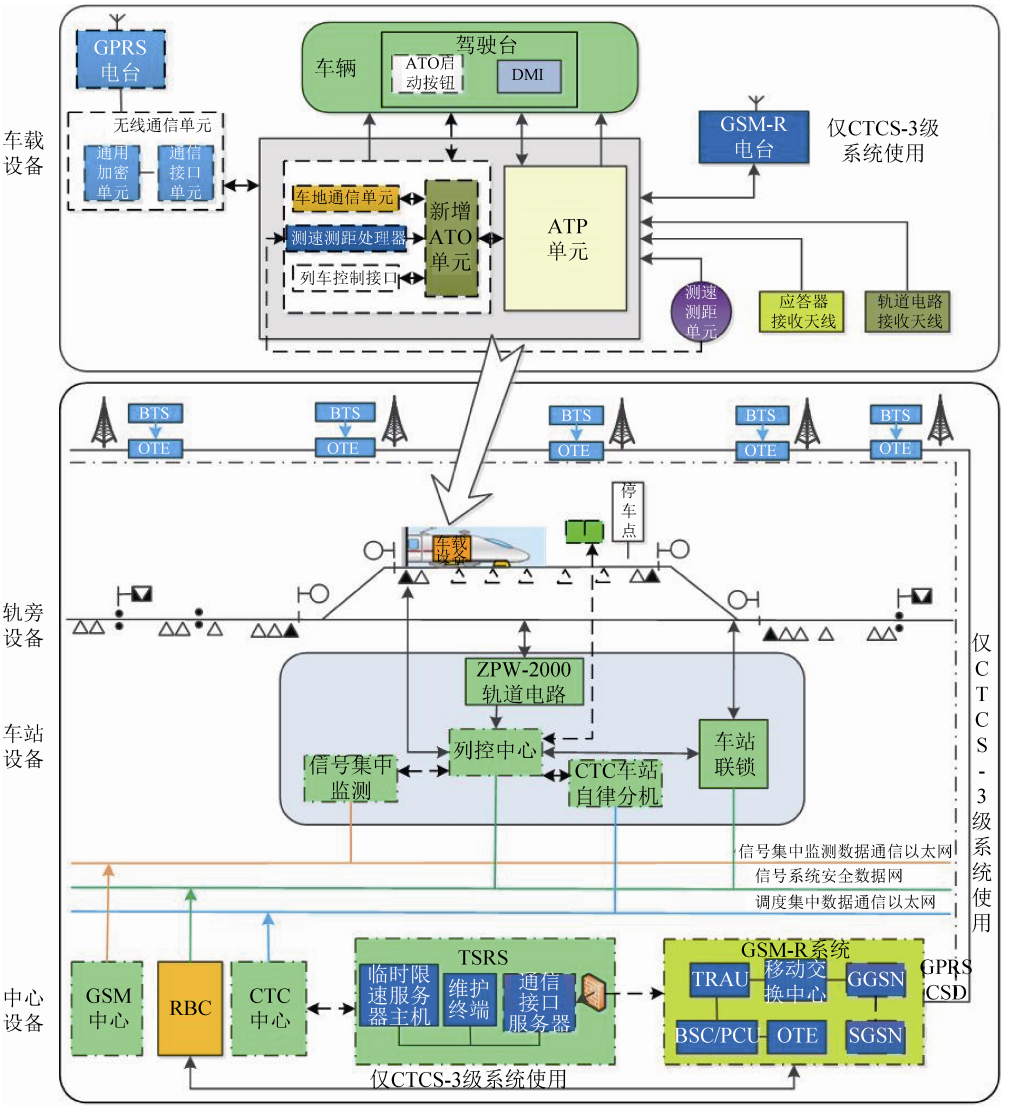
(1) 车载 ATO 与 TSRS 建立连接。车载 ATO 可根据司机输入或者应答器提供的 TSRS 编号呼叫

DOI: 10.16182/j.issn1004731x.joss.19-0662

TSRS，若车载 ATO 收到来自 TSRS 发送的系统版本，则表示通信会话建立成功；反之，则通信会话建立不成功。通信会话成功建立后，车载 ATO 将收到的系统版本和车载版本进行对比：若两版本不兼容则呼叫失败，车载 ATO 停止对 TSRS 的呼叫，通信会话结束；若两版本兼容则呼叫成功，列车在 TSRS 中注册该车载 ATO 设备信息，并将注册的车载信息发送至 CTC，CTC 登记该列车的注册信息。然后 TSRS 向车载 ATO 发送位置参数，车载 ATO 发送列车位置信息至 TSRS，TSRS 将收到的信息转发至 CTC，具体信息交互流程如图 2 所示。

(2) TSRS 判别列车位置信息。TSRS 对来自车载 ATO 的列车位置信息进行判断，判断结果分为以下 3 种情况：(1) 若列车位置信息无效或未知，则 TSRS 保持与车载 ATO 的通信会话；(2) 若列车位置有效，则 TSRS 向车载 ATO 发送对应的来自 CTC 的运行计划；(3) 若列车位置不属于 TSRS 管辖范围，则 TSRS 通知车载 ATO 结束通信会话、CTC 删除该列车相关信息，具体信息交互流程如图 3 所示。

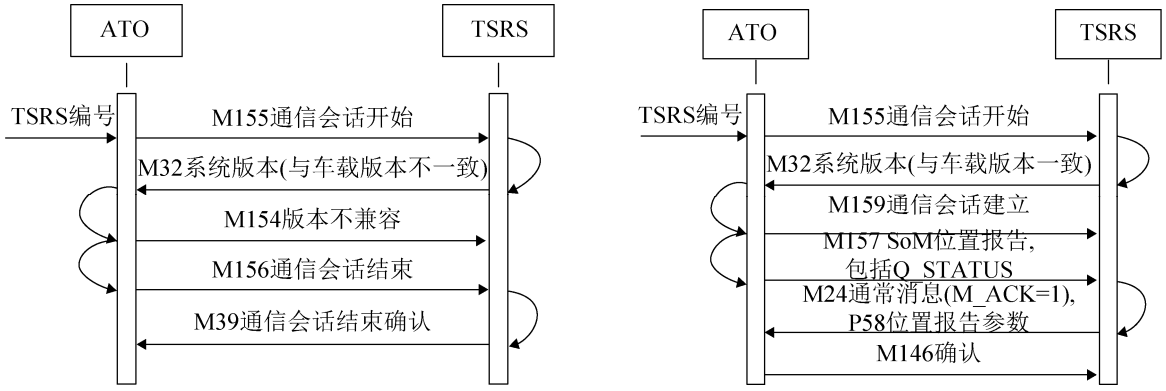
(3) 始发站自动发车。当运行计划有效且相关发车条件具备时，在 ATP 监督下列车以 PS(Partial Supervision Mode)发车。在发车过程中若满足进入 AM(Automatic Mode)的条件时，司机可按压“ATO 启动”按钮触发自动驾驶[8]。



注：图中虚线为新增内容 ——— 图中点划线为既有设备改造 — · — · — 图中实线示意为既有 ———

图 1　C3+ATO 系统架构

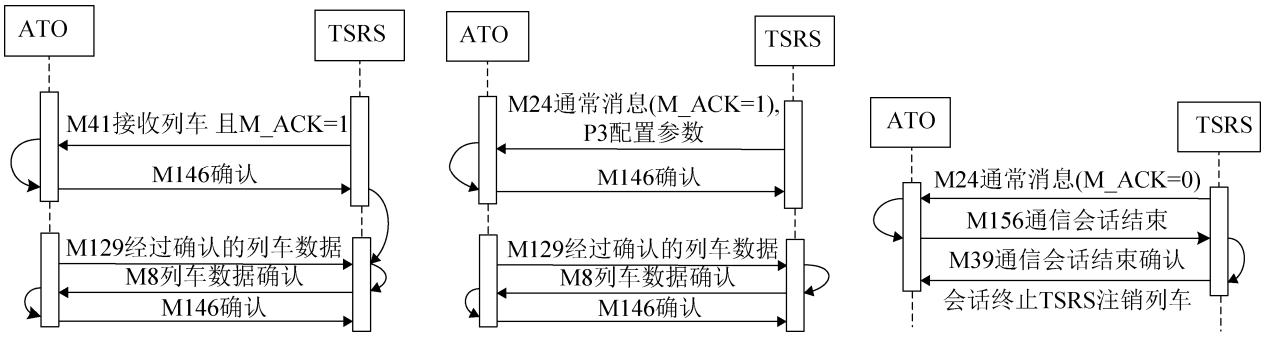
Fig. 1　Structure of C3+ATO system



(a) 版本不兼容 (b) 版本兼容

图 2 TSRS 判别两版本是否兼容信息交互图

Fig. 2 Information interaction of TSRS determines whether two versions are compatible



(a) 列车位置无效或未知 (b) 列车位置有效 (c) 列车位置不在管辖范围内

图 3 TSRS 判别列车位置信息交互图

Fig. 3 Information interaction of TSRS determines train position

2 始发站自动发车场景建模

2.1 时间自动机及模型验证工具 UPPAAL

时间自动机是含有时钟约束条件的有限状态自动机。在时间自动机模型中，任意状态位置只有当满足当前时钟约束条件时才会发生对应的状态迁移过程[9]。

定义 1：时间自动机可由一个六元组来描述 $<S, S^0, \sum, X, I, E>$，S 为非空有穷状态集；S^0 为初始状态集；$\sum$ 为有穷事件集；X 为时钟变量集；I 为一个映射，它定义 $x \in \phi(x)$ 作为状态位置的时钟约束；E 为状态迁移集。

定义 2：一个状态变迁 $<s, a, \lambda, \phi, s'>$ 表示当状态位置 s 满足变迁事件为 a 且时钟约束为 ϕ 时转移到状态位置 s'，$\lambda \in X$ 表示发生转移时被重置的时钟变量。

定义 3：假设一个六元组 $<S, S^0, \sum, X, I, E>$ 可以用来描述始发站自动发车场景的时间自动机网络模型，前提需要满足下列条件：

(1) 整个场景的时间自动机网络模型可由场景涉及设备的时间自动机之积表示，若 2 个设备的时间自动机分别为 $TA_1 =< S_1, S_1^0, \sum_1, X_1, I_1, E_1 >$ 和 $TA_2 =< S_2, S_2^0, \sum_2, X_2, I_2, E_2 >$ 且 X_1 和 X_2 不相交，则场景时间自动机记为 $TA = TA_1 \| TA_2$。因此，始发站自动发车场景的时间自动机记作 $TA = TA_{\text{ATO}} \| TA_{\text{TSRS}} \| TA_{\text{CTC}} \| TA_{\text{Driver\_Balise}}$。其中，$TA_{\text{ATO}}, TA_{\text{TSRS}}, TA_{\text{CTC}}, TA_{\text{Driver\_Balise}}$ 分别表示车载 ATO，TSRS，CTC 以及 Driver_Balise 的时间自动机模型。

(2) $S = S_{\text{ATO}} \cup S_{\text{TSRS}} \cup S_{\text{CTC}} \cup S_{\text{Driver\_Balise}}$（“∪”表示并集算法），$S_{\text{ATO}}, S_{\text{TSRS}}, S_{\text{CTC}}, S_{\text{Driver\_Balise}}$ 分别表示车载 ATO，TSRS，CTC，Driver_Balise 的时

间自动机模型的非空状态集。其中，S_{ATO} = {Initial, Edition, Callout, Callsuccess…}，S_{TSRS} = {Connect, EnrollATO, SoMreport…}，S_{CTC} = {Idle, Sendplan, DeleteATO…}，S_{Driver_Balise} = {Begin, Sendnumber}。

(3) S^0 = {Initial, Connect, Idle, Begin}，Initial, Connect, Idle, Begin 分别表示车载 ATO, TSRS, CTC, Driver_Balise 时间自动机模型的初始位置。

(4) $\Sigma = \Sigma_{ATO} \cup \Sigma_{TSRS} \cup \Sigma_{CTC} \cup \Sigma_{Driver\_Balise}$，$\Sigma_{ATO}$，$\Sigma_{TSRS}$，$\Sigma_{CTC}$，$\Sigma_{Driver\_Balise}$ 分别表示车载 ATO，TSRS，CTC，Driver_Balise 时间自动机模型的有限事件集合。模型中任一事件发生，当前以该事件作为变迁条件的状态发生迁移，从而实现模型间的相互通信。其中，Σ_{ATO} ={M155, M159, M157, M146,…}，Σ_{TSRS} = {M32, M41, M8, Logoff‥}，Σ_{CTC} = {Plan, M136, Callfail…}，Σ_{Driver_Balise} = {Logoff, TSRSnumber, Callfail}。

(5) 假设子模型间通信会话连接完好，与始发站自动发车场景有关的时间特性有“CTC 与 TSRS 通信正常，若未在给定时间内收到列车信息时，CTC 应删除该车载 ATO 的注册信息”“车载 ATO 未在规定时间内给 TSRS 发送信息，则判定为通信连接中断，TSRS 注销该车载设备并通知 CTC”等。因此设置时钟变量集 $X = \{T_0, T_1, T_2, T_3\}$ (单位：s)，相应的设置时钟集合 $\varphi(x) = \{T_0 > 600, T_0 \leqslant 600, T_1 > 300, T_1 \leqslant 300, T_2 := T_2 + 20, T_3 > 300, T_3 \leqslant 300\}$。

(6) 通过解读高速铁路 ATO 系统技术规范，可知发生状态迁移的条件。迁移集合为 $E = \{<$ Initial, TSRSnumber,,,Receivenumber $>$, $<$ Sendnumber, Logoff,,,Begin $>$, $<$ Landin,M157,,,SoMreport$>$, $<$ Traininfor,Plan,,,Sendplan $> \cdots\}$。

UPPAAL 是一个专门针对时间自动机理论的建模与验证工具，其简洁形象的模型描述过程以及友好的人机交互界面为模型验证分析提供了便利。UPPAAL 包括编辑器、模拟器、验证器 3 个界面：编辑器主要进行模型定义、过程描述；模拟器主要用于验证模型是否存在错误，同时可以仿真生成不同流程的消息顺序图；验证器主要用于检验模型是否具备相应的功能属性。UPPAAL 验证模型是基于 BNF 语法，每种表达的含义如表 1 所示[10-12]。

表 1 BNF 语法含义
Tab. 1 Grammatical Meaning of BNF

BNF 语法	含义
E<>p	存在一条路径，p 在该路径中某一状态下为真
E[ ]p	存在一条路径，p 在该路径中所有状态下均为真
A[ ]p	对于所有路径，p 在任一路径的所有状态均为真
A<>p	对于所有路径，p 在任一路径的某一状态为真
p→q	当 p 为真时，则 q 为真

2.2 基于 UPPAAL 的场景建模

考虑到整个始发站自动发车场景涉及的交互设备，最终选取车载 ATO, TSRS, CTC 以及 Driver_Balise 作为该场景建模对象。根据 1.2 节中描述的该场景工作流程分别建立车载 ATO, TSRS, CTC 以及 Driver_Balise 的时间自动机子模型 TA_{ATO}，TA_{TSRS}，TA_{CTC}，TA_{Driver_Balise}，如图 4~7 所示。模型中，“！”表示发送一个事件，“？”表示接收一个事件，借助事件完成模型间的同步信息交互。模型中的通道(Chan)是模型间信息交互以及事件传输的重要媒介。模型中双圆圈表示各子模型的初始位置，标有“∪”的圆圈表示紧急位置，各子模型中关键位置和变量的含义如表 2 所示。

第 33 卷第 4 期 系统仿真学报 Vol. 33 No. 4
2021 年 4 月 Journal of System Simulation Apr. 2021

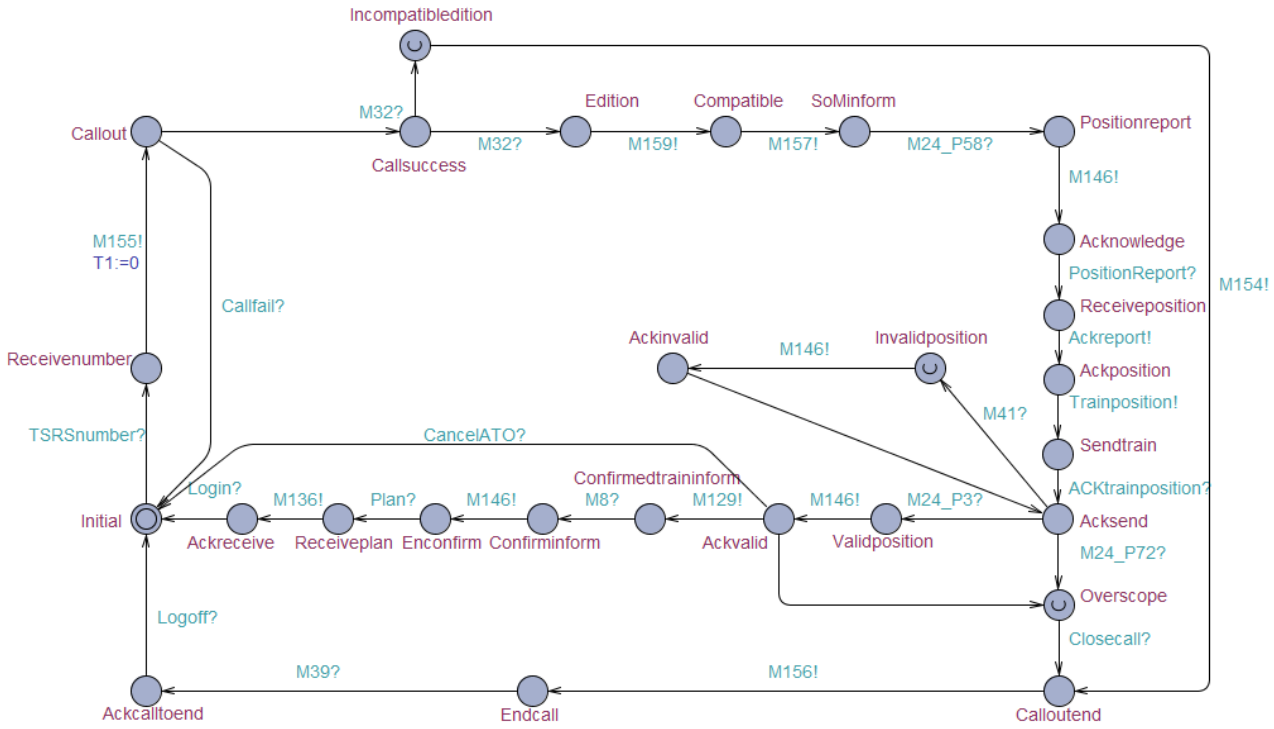


图 4 车载 ATO 时间自动机模型

Fig. 4 Timed automata of on-board ATO

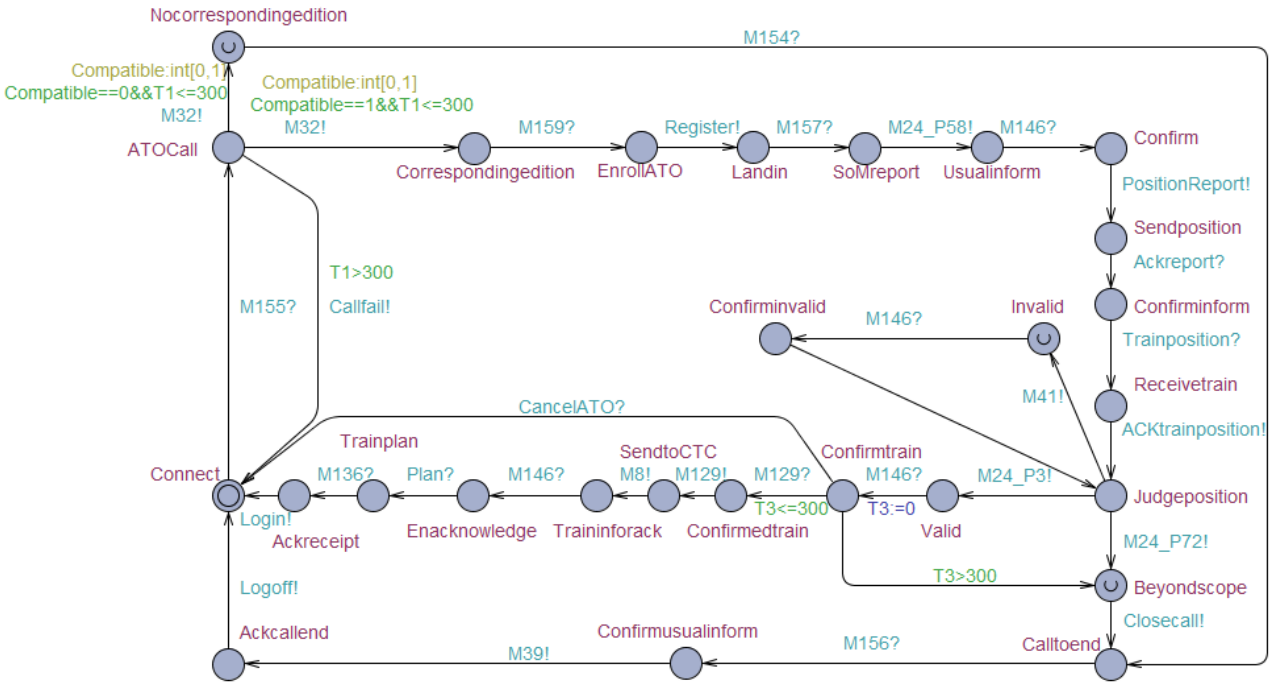


图 5 TSRS 时间自动机模型

Fig. 5 Timed automata of TSRS

DOI: 10.16182/j.issn1004731x.joss.19-0662

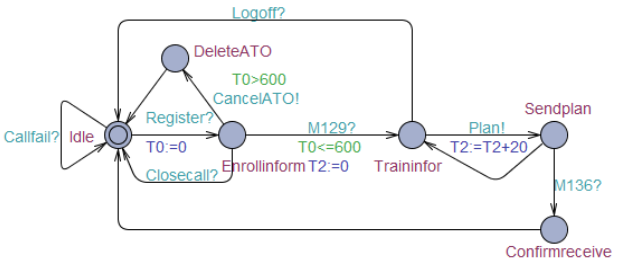


图 6 CTC 时间自动机模型
Fig. 6 Timed automata of CTC

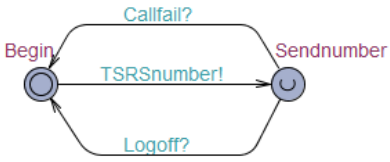


图 7 Driver_Balise 时间自动机模型
Fig.7 Timed automata of Driver_Balise

表 2 模型中关键位置和变量含义
Tab. 2 Meaning of key positions and variables

状态位置	含义	变量	含义
DeleteATO	注销 ATO	Compatible	版本状态，0 表示不兼容，1 表示兼容
Calltoend	关闭通信会话	T_0	CTC 与 TSRS 通信时间限制
Landin	注册成功	T_1	TSRS 与车载 ATO 通信时间限制
Sendnumber	发送 TSRS 编号	T_2	发送运行计划时间
Traininfor	列车位置信息	T_3	TSRS 与车载 ATO 通信时间限制

2.3 模型过程描述

以 TSRS 发送的系统版本与车载版本不兼容情况的过程为例进行模型过程说明。

(1) 车载 ATO 通过事件 M155 发起与 TSRS 的通信连接，当车载 ATO 接收到来自 TSRS 的系统版本信息时表示通信会话建立成功。TSRS 通过事件 M32 向车载 ATO 发送不兼容的系统版本时，TA_{TSRS} 发生转换 < ATOCall, M32,,, Nocorrespondingedition > 。同时，车载 ATO 通过事件 M32 接收到不兼容的系统版本信息，TA_{ATO} 发生转换 < Callsuccess, M32,,,Incompatibledition > 。

(2) 经由车载 ATO 判断系统版本与车载版本不兼容，通过事件 M154 将版本不兼容消息发送至 TSRS，TA_{ATO} 发生转换 < Incompatiblediton, M154,,,Calloutend > 。同时，TSRS 通过事件 M154 接收到版本不兼容的消息，TA_{TSRS} 发生转换 < Nocorrespondingedition, M154,,,Calltoend > 。

(3) 车载 ATO 通过事件 M156 向 TSRS 发送通信会话已结束的消息，TA_{ATO} 发生转换 < Calloutend, M156,,,Endcall > 。同时，TSRS 通过事件 M156 接收到通信会话已结束的消息，TA_{TSRS} 发生转换 < Calltoend, M156,,,Confirmusualinform > 。

(4) 当确认关闭后，TSRS 通过事件 M39 向车载 ATO 发送确认通信会话关闭消息，TA_{TSRS} 发生转换 < Confirmusualinform, M39,,,Ackcallend > 。

同时，车载 ATO 通过事件 M39 接收到通信会话确认关闭的消息，TA_{ATO} 发生转换 < Endcall, M39,,,Ackcalltoend > 。

(5) 当与车载 ATO 的通信会话确认关闭之后，TSRS 通过事件 Logoff 将注销列车信息传递至车载 ATO，TA_{TSRS} 发生转换 < Ackcallend, Logoff,,, Connect > ，并且回到模型的初始位置。

同时，车载 ATO 通过事件 Logoff 接收到注销列车的消息，TA_{ATO} 发生转换 < Ackcalltoend, Logoff,,,Initial > ，并且回到模型的初始位置。

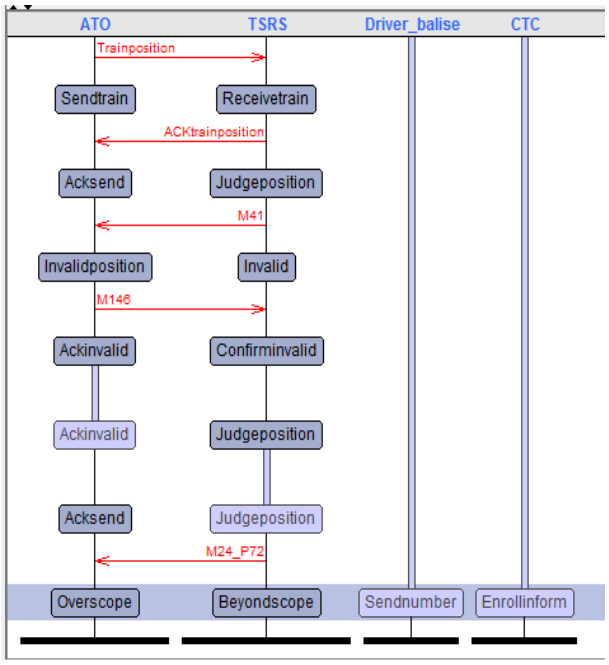
3 模型的形式化仿真与验证

对于所建模型的仿真与验证，主要通过生成消息顺序图和验证系统功能特性 2 方面来完成。

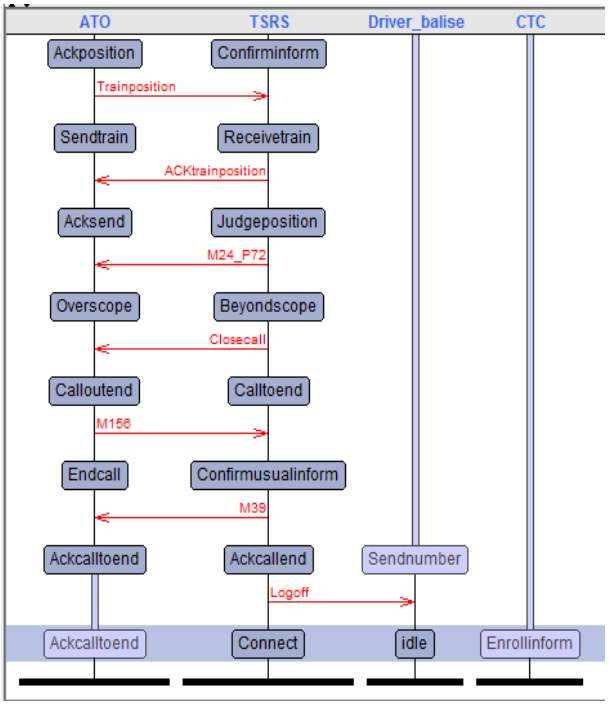
3.1 模型的仿真

模型的仿真主要通过生成相应流程的消息顺序图来实现。本文以 TSRS 对来自车载 ATO 的列车位

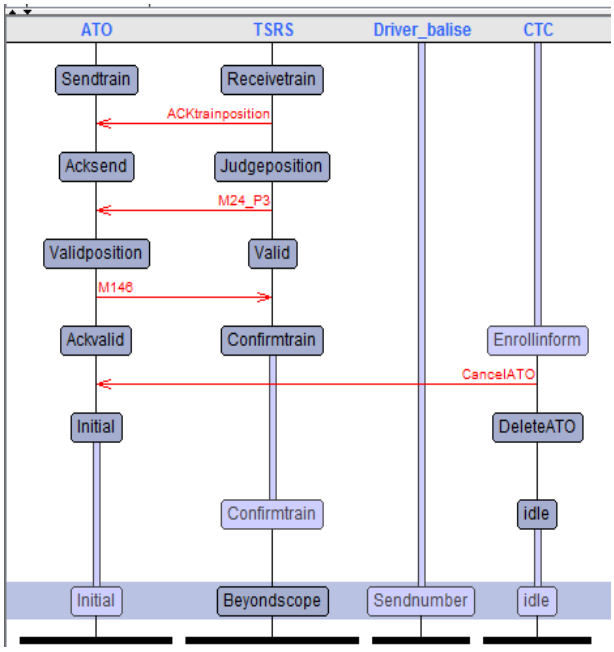
置信息进行判断的 3 种情形为例，分别为列车位置信息无效或未知、不在管辖范围内、有效，具体信息交互过程描述如 1.2 节中所述，相应的消息顺序图如图 8 所示，从图 8 中可以看出各个模型间信息交互内容以及各个子模型的状态位置变化情况。



(a) 列车位置无效或未知



(b) 列车位置不在管辖范围内



(c) 列车位置有效

图 8 模型消息顺序图

Fig. 8 Model message sequence chart

3.2 模型的验证

模型的验证主要从系统的安全功能属性、受限活性两方面来分析。对于安全功能属性，定义为一些行为可能在系统中出现，如“车载 ATO 根据来自 TSRS 的位置报告，应发送列车位置报告至 TSRS”；对于受限活性，定义为一些行为在系统运行过程中一定会发生，如“TSRS 判断与车载 ATO 通信中断，则注销该车载 ATO 并且通知 CTC”。在模型相应流程的消息顺序图生成之后，从高速铁路 ATO 系统测试案例中提取始发站自动发车场景需要测试的功能需求，并且转化为 UPPAAL 对应的 BNF 验证语句，验证程序实体如下:

系统安全功能属性验证

(1) 车载 ATO 根据司机输入或者应答器信息包发起与 TSRS 的通信会话，若车载 ATO 接收到 TSRS 发送的版本消息，则表明通信会话建立成功；若车载 ATO 未收到来自 TSRS 的版本消息，则表明通信会话建立失败： E<>((ATO.Receivenumber) imply(ATO.Initial)or(ATO.Receivenumber)imply(ATO.Edition)or(ATO.Receivenumber)imply(ATO.Incom

https://dc-china-simulation.researchcommons.org/journal/vol33/iss4/23
DOI: 10.16182/j.issn1004731x.joss.19-0662

patibledition))。

(2) 任务开始时，车载 ATO 根据来自 TSRS 的参数信息并向其报告列车位置：E<>((ATO.Acknowledge)imply(ATO.Receiveposition)and(TSRS.Confirminform)imply(TSRS.Receivetrain))。

(3) 列车位置为未知或无效时，TSRS 向车载 ATO 发送接收列车的消息：E<>((TSRS. Judgeposition)imply(TSRS.Invalid)and(ATO.Acksend)imply(ATO.Invalidposition))。

(4) 列车位置不在 TSRS 管辖范围内，TSRS 收到来自车载 ATO 的通信会话关闭消息后，向其传输通信会话确认关闭消息：E<>((ATO.Calloutend)imply(ATO.Endcall)and(TSRS.Confirmusualinform)imply(TSRS.Ackcallend))。

(5) 列车位置有效时，TSRS 向车载 ATO 发送配置信息，车载 ATO 向 TSRS 发送确认接收配置信息以及经过确认的列车数据，TSRS 收到列车数据后回复确认：E<>(((TSRS.Judgeposition)imply(TSRS.Valid)and(ATO.Validposition)imply(ATO.Ackvalid))and((ATO.Ackvalid)imply(ATO.Confirmedtraininform)and(TSRS.SendtoCTC)imply(TSRS.Traininforack)))。

系统受限活性验证

(1) TSRS 判断与车载 ATO 连接中断超时 5 min 时，应注销该车载 ATO 并通知 CTC：A<>(((TSRS.Confirmtrain)imply(TSRS.Beyondscope)and(T3>300))and(CTC.Enrollinform)imply(CTC.Idle))。

(2) CTC 判断与 TSRS 通信正常，但持续 10 min 未收到该列车的任何消息时，CTC 应删除注册信息：A<>((CTC.Enrollinform)imply(CTC.DeleteATO) and (T_0>600))。

将上述需验证的内容输入 UPPAAL 验证器窗口进行性质检验，根据验证器性质列表窗口后的小圆圈颜色来判断该条性质是否通过验证。若小圆圈为绿色，则表明所建模型满足该条性质；若小圆圈为红色，则表明所建模型不满足该条性质。所有性质均通过检验，验证结果如图 9 所示，表明模型满足高速铁路 C3+ATO 系统应具备的功能属性。

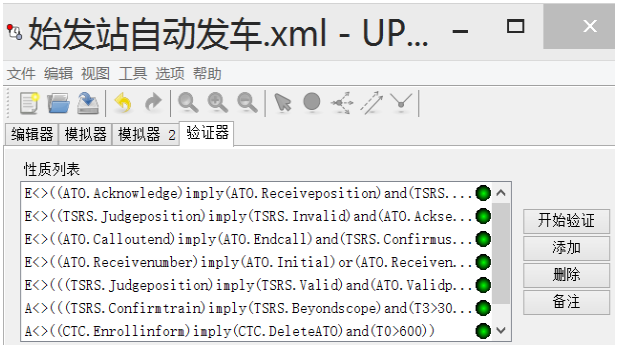


图 9 模型验证图
Fig. 9 Model validation chart

3.3 场景模型仿真实现

根据 2.2 节所建立模型，在 C3+ATO 列控系统仿真平台上构建了 4 站 3 区间的模拟线路环境，在各个模拟车站进行了车站自动发车场景模型仿真，以“犀浦站——九里站”的发车进路为例进行说明，仿真结果如图 10~12 所示。

图 10 DMI 仿真示意图
Fig. 10 DMI simulation diagram

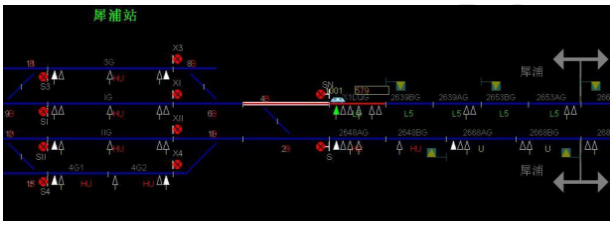


图 11 犀浦站自动发车示意图
Fig. 11 Schematic of Xipu station automatic departure

变量	取值	描述
NID_MESSAGE	159	建立通信会晤
L_MESSAGE	10	消息长度(字节)
T_TRAIN	7759	车载设备时钟(10 ms)
NID_ENGINE	2001	车载设备的ETCS标识号

变量	取值	描述
NID_MESSAGE	155	通信会晤开始
L_MESSAGE	10	消息长度(字节)
T_TRAIN	7598	车载设备时钟(10 ms)
NID_ENGINE	2001	车载设备的ETCS标识号

变量	取值	描述
NID_MESSAGE	32	系统配置
L_MESSAGE	11	消息长度(字节)
T_TRAIN	7598	车载设备时钟(10 ms)
M_ACK	0	不要求确认
NID_LRBG	167...	未知的最后相关应答器组
M_VERSION	16	CTCS语言版本

图 12 消息变量取值举例示意图

Fig. 12 Schematic diagram of value of a message variable

图 10 为车站自动发车场景中车载 ATO 与 TSRS 建立连接、TSRS 获得有效列车位置信息后，列车在 PS 模式监控下从犀浦站发车的 DMI 示意图，当满足相关条件时转入 AM 模式。图 11 为完成车站自动发车场景相关操作之后，列车从犀浦站自动发车的示意图。图 12 为车站自动发车场景实行过程中设备间进行交互的消息事件取值举例。其中，M155 取值表示车载 ATO 已请求与 TSRS 建立连接；M32 取值表示经车载 ATO 判断来自 TSRS 的系统版本与车载版本一致；M159 取值表示车载 ATO 已与 TSRS 成功建立连接，表明各设备已协作实现车站自动发车场景所需信息交互。因此，仿真结果表明仿真系统按照模型建立逻辑运行可实现车站自动发车功能。

4 结论

高速铁路 C3+ATO 系统具有运行效率高、自动化智能化程度高、安全等级高等特点，但目前仍处于测试试验阶段，而系统设计、系统规范若存在缺陷会危及列车行车安全。本文采用基于时间自动机的形式化建模与验证方法，以 C3+ATO 系统始发站自动发车场景为例，建立场景模型并进行形式化仿真、验证系统功能属性，主要结论如下：

(1) 基于技术规范对系统功能以及场景流程的建模与验证方法，通过提取 C3+ATO 系统技术规范的功能需求，建立场景的时间自动机模型，验证需满足的功能需求。有助于全面准确的描述系统功能，提高模型的科学性、可行性以及模型验证的条理性。

(2) 通过生成消息顺序图仿真子模型间信息交互场景，可以帮助设计者深入演绎场景的通信过程，更加形象地理解整个系统设备间的信息交互过程；同时根据消息顺序图可以反向检验模型建立过程是否存在错误，完善系统设计、规范编制中存在的缺陷。

(3) 对于 C3+ATO 系统场景建模与验证的分析过程，为系统理论研究和实际应用提供支持，验证通过后的模型可作为系统功能测试阶段的场景原型，为功能测试提供理论参考，有助于减少测试投入。

参考文献：

[1] 成雅靖. 自主化 CTCS-3 级列控系统复杂场景建模与验证[D]. 北京: 北京交通大学, 2018.
Cheng Yajing. Modeling and Verification of Complex Scenarios of Autonomous Chinese Train Control System Level 3[D]. Beijing: Beijing Jiaotong University, 2018.

[2] 康仁伟. 基于时间自动机的 CTCS-3 级列控系统建模方法与验证研究[D]. 北京: 北京交通大学, 2013.
Kang Renwei. The Research on Modeling Methods and Verification of Chinese Train Control System Level 3 Based on Timed Automata[D]. Beijing: Beijing Jiaotong University, 2013.

[3] 万勇兵, 徐中伟, 梅萌. CTCS-3 级列控系统临时限速服务器建模与形式化验证[J]. 系统仿真学报, 2013, 25(1): 132-138.
Wan Yongbin, Xu Zhongwei, Mei Meng. Modeling and Formal Verification of Temporary Speed Restriction Server for CTCS Level 3[J]. Journal of System Simulation, 2013, 25(1): 132-138.

[4] 胡雪莲, 陶彩霞. 基于MSC与UPPAAL的列控系统等级转换场景形式化验证[J]. 铁道标准设计, 2015, 59(2): 122-127.

DOI: 10.16182/j.issn1004731x.joss.19-0662

Hu Xuelian, Tao Caixia. Formal Verification of Level Transition Process in Train Control System Based on MSC and UPPAAL[J]. Railway Standard Design, 2015, 59(2): 122-127.

[5] 刘长青. 京张智能动车组——从“中国创造”向“中国智造”的里程碑式跨越[J]. 城市轨道交通研究, 2018, 21(2): 3.
Liu Changqing. Intelligent EMU for Beijing-Zhangjiakou Line—A Milestone form “Created in China” to “Intelligent Manufacturing in China”[J]. Urban Mass Transit, 2018, 21(2): 3.

[6] 程剑锋, 冯凯, 李科. 高速铁路 CTCS3+ATO 列控系统技术研究[J]. 中国铁路, 2019(1): 74-77.
Cheng Jianfeng, Feng Kai, Li Ke. CTCS3+ATO High Speed Railway Train Control Technology[J]. China Railway, 2019(1): 74-77.

[7] 朱少彤. CTCS3+ATO 高速列车自动驾驶系统关键设备研究[J]. 中国铁路, 2018(10): 1-6.
Zhu Shaotong. Research on Key Equipment for CTCS3+ATO System of High Speed Railway[J]. China Railway, 2018(10): 1-6.

[8] 铁总科信. 高速铁路 ATO 系统暂行总体技术方案: [2018]8 [S]. 北京: 中国铁路总公司, 2018.
Ministry of Science and Industry of the Railway Corporation. Temporary Overall Technical Scheme of ATO System for High Speed Railway: [2018]No.8 [S]. Beijing: China Railway Corporation, 2018.

[9] Song S, Chen Y D. A Test Sequence Generation Method of Zone Controller Based on Timed Automata[J]. Journal of Measurement Science and Instrumentation (S1674-8042), 2019, 10(3): 266-276.

[10] Chen Y G, Yang L, Wang D. Modeling Research of Train Tracing Based on UML Sequence Diagram and UPPAAL[J]. Journal of Measurement Science and Instrumentation (S1674-8042), 2019, 10(2): 157-167.

[11] Kunz G, Machado J, Perondi E. Using Timed Automata for Modeling, Simulating and Verifying Networked Systems Controller’s Specifications[J]. Neural Computing & Applications (S0941-0643), 2017, 28(5): 1031-1041.

[12] 杨璐, 陈永刚. 基于MSC与UPPAAL的区域控制器切换场景建模与验证[J]. 铁道标准设计, 2018, 62(5): 171-174.
Yang Lu, Chen Yonggang. Modeling and Verification of Switch Scene of Zone Controller Based on MSC and UPPAAL[J]. Railway Standard Design, 2018, 62(5): 171-174.