文章编号：1001-8360(2009)03-0059-06

基于UPPAAL的城市轨道交通CBTC区域控制子系统建模与验证

吕继东， 唐 涛， 燕 飞， 徐天华
（北京交通大学 轨道交通控制与安全国家重点实验室，北京 100044）

摘 要：CBTC(Communication Based Train Control)系统可有效提高轨道交通的列车运营效率，降低系统建设和维护费用。在系统研发过程中需对系统进行建模、仿真和验证，发现系统设计缺陷，以保证系统的安全性。CBTC区域控制子系统是一实时控制系统，它要求控制时间的精确性和控制过程的准确性。本文通过分析城市轨道交通CBTC区域控制子系统的结构，给出满足该子系统安全性的功能和性能要求，并结合时间自动机理论方法提出包含列车、速度距离控制器、区域控制器和多车控制队列的时间自动机网络模型。同时，应用UPPAAL验证工具对CBTC区域控制子系统进行仿真建模，并验证该子系统功能和性能要求，从而保证了系统模型的安全性和受限活性。

关键词：区域控制子系统；UPPAAL；时间自动机；自动验证
中图分类号：TP393；U283 **文献标志号**：A doi:10.3969/j.issn.1001-8360.2009.03.011

UPPAAL-based Simulation and Verification of CBTC Zone Control Subsystem in Rail Transportation

LÜ Ji-Dong, TANG Tao, YAN Fei, XU Tian-hua
(State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The Communication Based Train Control (CBTC) System enhances the train operation efficiency and reduces the system construction and maintenance cost, which is the most advanced train control system in the world nowadays. How to model and simulate the system to find the design defects in the research and development has become one of the key issues of CBTC research. The CBTC Zone Control Subsystem is a real-time control system, it requests the accuracy of control time and the correctness of the control process. This paper analyzes the structure of the CBTC Zone Control Subsystem and gives the function and performance requirements for safety. Combined with the theoretical method of timed automata, it presents the TTZQ automata network model that includes the train automata, speed and distance automata, zone controller automata and queue automata. It applies the various tools of UPPAAL to model the Zone Control Subsystem of CBTC and verifies the function and performance requirements, which guarantees the safety and bounded liveness properties of the model.

Key words: zone control subsystem; UPPAAL; timed automation; automatic verification

到2010年全国将有大约1 500km的地铁线路投入运营[1]，随着世界范围轨道交通的蓬勃发展，如何提高列车运营的效率和安全性以及降低系统的建设成本是各国关心的问题。开发先进的列车运行控制系统基本已成为各国主要研究机构解决上述问题的共识。CBTC(Communication Based Train Control)系统是列车运行控制系统的发展趋势[2-3]，世界主要发达国家都相继开发出自己的基于通信的列车运行控制系统。与传统的基于轨道电路的列车运行控制系统相比，其优点为：(1)通过列车-地面之间安全可靠的大容量的双向信息传输实现列车的闭环控制，提高了列车运行

收稿日期：2007-10-15；修回日期：2008-01-05
基金项目：国家自然科学基金项目(60634010)
作者简介：吕继东(1981—)，男，河北廊坊人，博士研究生。
E-mail：04120084@bjtu.edu.cn

的安全性;(2)可实现移动闭塞方式,提高线路的通过能力;(3)减少地面设备,降低了投资和维护的费用。在典型的CBTC系统中,区域控制子系统主要完成列车登陆控制、列车接管控制、列车移动授权(MA)的信息计算以及列车退出控制等功能。因此,在系统研发过程中对区域控制子系统进行建模、仿真和验证,发现系统设计缺陷,提高系统的安全性,从而辅助系统开发显得尤为重要。区域控制子系统是一个实时控制系统,它不仅要求产生的结果在逻辑上是准确的,而且要求在时间上也是准确的,因此需采用自动机理论规范和验证该实时子系统。然而传统的有穷状态自动机显然是不够的,随着时间自动机模型的逐步成熟,出现了很多使用时间自动机模型的验证工具,UPPAAL[4]就是其中之一,它通过将实时系统抽象成时间自动机网络模型来实现对实时系统的安全性和响应受限的自动验证。本文采用时间自动机理论,应用UPPAAL验证工具对CBTC区域控制子系统进行仿真建模,并且对该子系统模型的安全性(Safety)和受限活性(Bounded Liveness)进行验证。

1 UPPAAL简介[4]

UPPAAL由Aalborg大学和Uppsala大学于1995年联合提出,它适用于可以被描述为非确定的并行过程的积的系统。每一个过程被描述为由有限控制结构、实数值时钟和变量组成的时间自动机,过程之间通过管道和(或者)共享变量来进行通讯,管道用于保证不同自动机间的两个转换同时执行。UPPAAL主要通过快速搜索机制来验证时钟约束和可达性。它的主要优点是高效性和方便性。另外,也可以用于验证更复杂的系统。

UPPAAL的用户界面包括3个主要部分:1个系统编辑器(system editor)、1个模拟器(simulator)和1个验证器(verifier)。系统编辑器用于创建和编辑要分析的系统,1个系统被描述为一系列过程模板、一些全局声明、过程分配和1个系统定义。模拟器是1个确认工具,它用于检查所建系统模型可能的执行是否有错,以此在验证前发现一些错误。验证器通过快速搜索系统的状态空间来检查时钟约束和反应限制性质,它还为系统要求的规范和文件提供了1个需求规范编辑器。

UPPAAL为验证提供了一种BNF语法,Prop::$=A[]p \mid E<>p \mid E[]p \mid A<>p \mid P\rightarrow p$。其中,$E<>p$表示Possible,$E<>p$为真,当且仅当在转换系统中存在一个序列$s_0\rightarrow s_1\rightarrow\cdots\rightarrow s_n$,使得$s_0$是开始状态,$s_n$是$p$。$A[]p$表示Invariantly,等价于not $E<>$not p。$E[\,]p$表示Potentially always,$E[\,]p$为真,当且仅当存在一个序列$s_0\rightarrow s_1\rightarrow\cdots\rightarrow s_i\rightarrow\cdots\rightarrow$,使得$p$在所有状态$s_i$中都有效,并且这个序列无穷或者在状态$(l_n,v_n)$终止,对所有的$d$:$(l_n,v_{n+d})$满足$p$和Inv$(l_n)$或者从$(l_n,v_n)$出发没有转换。$A<>p$表示Eventually。$p\rightarrow q$表示Lead to,等价于$A[\,](p$ imply $A<>q]$。

2 CBTC区域控制子系统结构和功能

CBTC系统包括车载系统、轨旁系统和车站系统,如图1所示。其中,车站系统包含列车自动监控系统ATS(Automatic Train Supervision)、计算机联锁(Computer Interlocking)、区域控制器ZC(Zone Control)和数据通信系统DCS(Data Communication System);轨旁系统主要指轨旁无线接入点(Access Point);车载系统主要指车载控制器VOBC(Vehicle on Board Controller)。

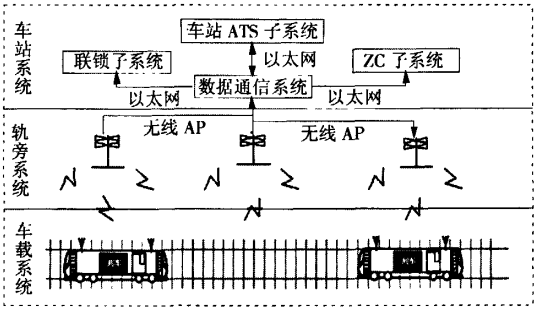


图1 CBTC系统结构图

ZC子系统(如图2所示)包含通信模块、信息接收模块、控制信息生成模块(列车控制信息和MA形成模块)和信息发送模块。该子系统主要完成列车登陆控制、列车接管控制、列车移动授权(MA)的信息计算以及列车退出控制等功能。它根据各列车的当前位置、速度及运行方向等因素,同时考虑列车进路、道岔状态、线路限速以及其它障碍物的条件,向列车发送移动授权(MA)信息,列车的MA是指从列车的车尾起到前方一定范围内的障碍物等信息。线路中的障碍物为影响列车运行速度的元素,可能是前行的另一列车、关闭的线路区域或道岔、防淹门、临时限速等。MA的范围需要合适的制定,既要保证当前列车的运行安全,又不能影响其它列车的运行效率。MA会有规律地、周期性地重建,即通知列车可以行使的距离和运行速度。

ZC是CBTC系统中的关键安全子系统,它的核心任务是为辖区内每列通信列车(装备无线通信设备

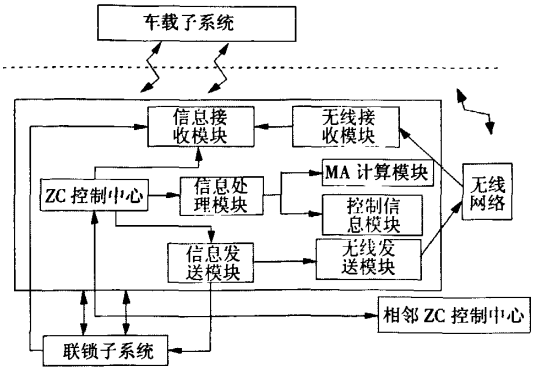


图 2　ZC 子系统结构图

的列车)提供 MA。设 ZC 区间有 $N(1\leqslant N\leqslant 40)$列列车运行,每列列车将完成在 ZC 中的登陆、控制接管、受控运行和离开的 4 个过程。根据该子系统的任务,必须具有以下功能和性能:

(1) 功能性要求:

①系统无死锁;

② 列车能完成在 ZC 区间的登陆、控制接管、受控运行和离开 4 个过程;

③ 列车能发送自己的位置信息到 ZC;

④ 列车能接收到 ZC 的控制信息;

⑤ 列车能根据控制信息更新自己的所在位置和速度。

(2) 性能要求:

① 列车登陆、受控接管在 T 个单位时间内完成;

② ZC 控制运行周期在$[0,U]$内,即:ZC 从收到列车报告的位置开始到结束对每列列车的运行控制完成要在 U 个单位时间内(T 为 ZC 的控制周期,$U=5T$)完成;

③ 两两列车间的运行距离大于保护距离;

④ 列车的最大运行速度小于线路限速。

3　建模与验证

3.1　基于 UPPAAL 的 ZC 子系统模型

(1) 模型结构分析

模型结构如图 3 所示,以线路上两列车追踪运行为例。两列车在 ZC 区间追踪运行,列车与 ZC 之间是用无线通信接入点 WCA(Wireless Communication Access Point)通信,列车周期性报告列车位置,同时 ZC 根据列车位置和其他相关条件返回给列车 MA,列车根据 MA 计算模式曲线,从而得出当前的限制速度。图中的曲线表示前行列车与后行列车的模式曲线,P 与 H 之间的距离为保护距离(Protection Distance)。

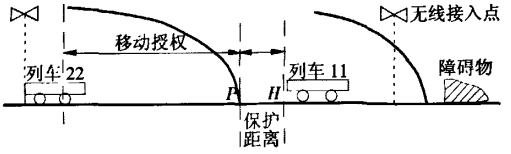


图 3　列车在 ZC 区间追踪运行图

ZC 通过网络接收到车载子系统汇报的列车实际位置和联锁子系统障碍物信息(道岔、前方通信列车等信息),并将这些信息存储到信息输入模块。信息解析模块再将这些输入信息按列车 ID 进行解析,并取出对应列车 ID 的信息送入控制信息生成模块。控制信息生成模块根据该列车信息生成控制信息(列车登录、列车接管、列车受控或者列车注销),最后将这些信息送入信息输出模块并通过通信网络发送到对应的车载子系统中。ZC 子系统控制流程如图 4 所示。

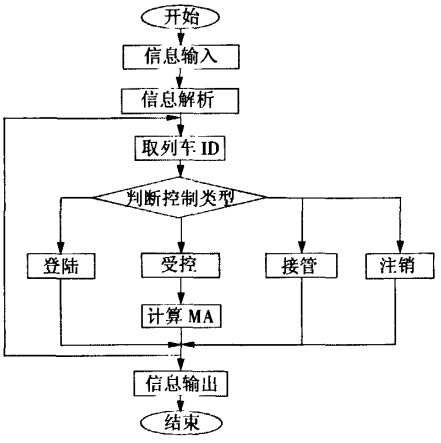


图 4　ZC 区间列车追踪运行的控制信息流图

该控制系统所涉及的对象主要有 ZC 控制中心和列车,二者视为并行过程。由于同一时段 ZC 要控制多辆列车,且列车的位置和速度要实时更新,故又增加了多列车队列控制和速度-距离控制两个过程。这 4 个并行的过程模型之间的关系如图 5 所示,其中 ZC

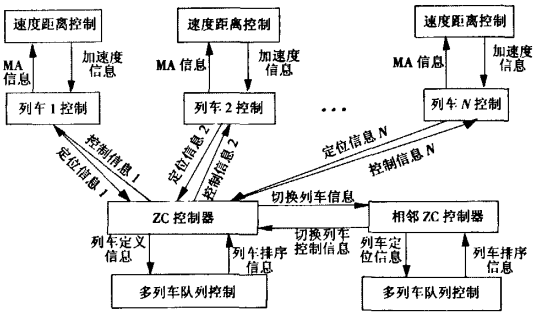


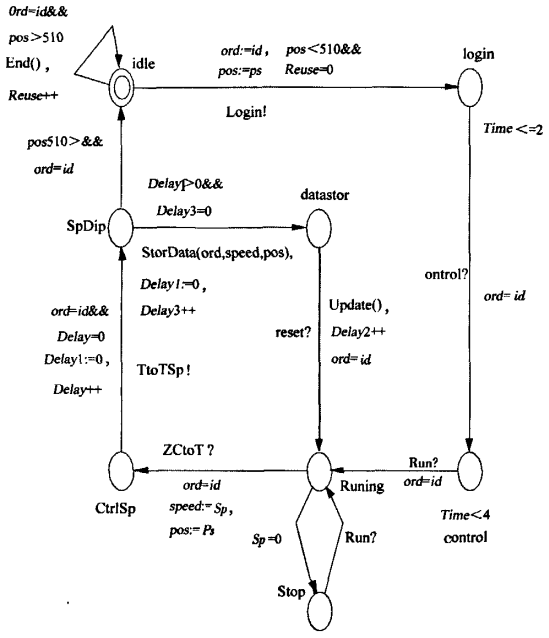
图 5　控制系统模型结构图

控制中心的功能为列车定位信息的接收、列车控制命令以及 MA 信息的发送;列车的控制功能为列车定位

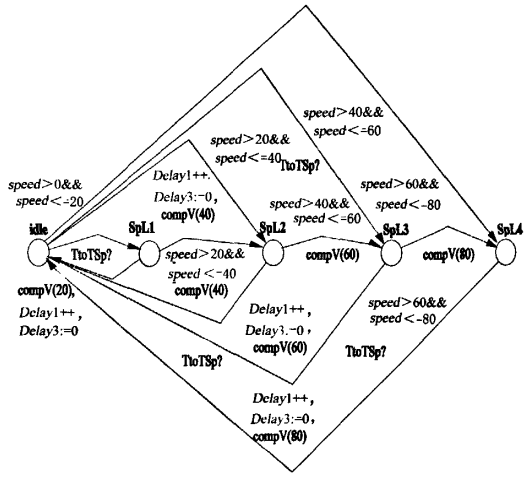
信息的发送、ZC 控制命令和 MA 信息的接收；多列车队列控制功能为对列车位置的排序，MA 信息雏形的计算；速度-距离控制功能为列车 MA 信息的解析、模式曲线的生成。

(2) 模型结构设计

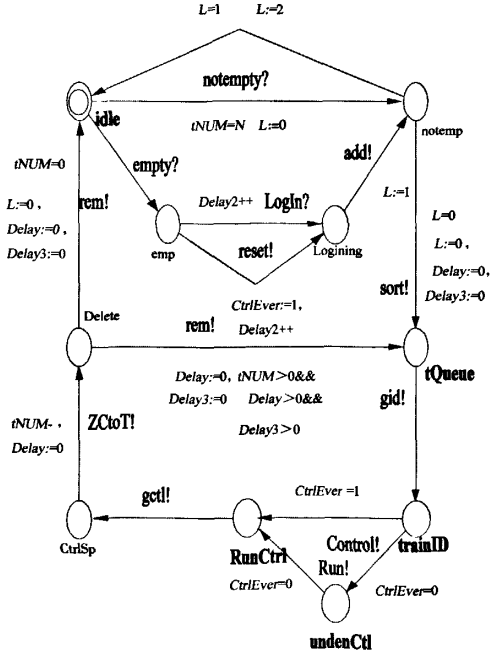
对以上 4 个过程建模，得到系统成员时间自动机模型分别为：Train(列车)、TSpAPs(速度-距离控制器)、ZCControl(ZC 控制器)和 Queue(多列车控制队列)，分别如图 6(a)～图 6(d)所示。那么，整个系统就



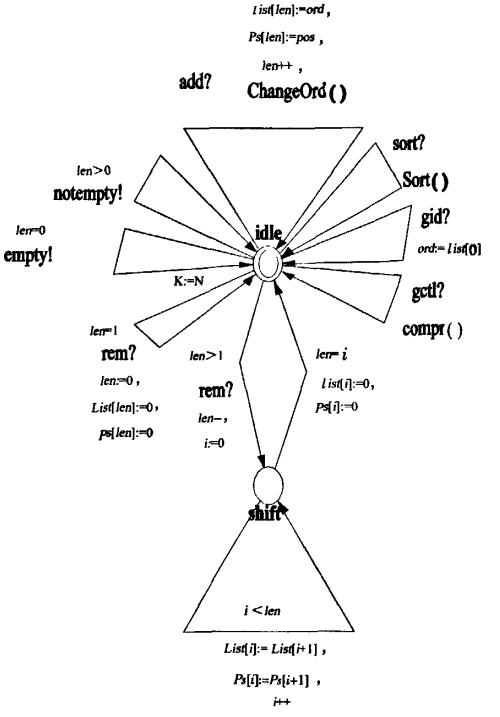
(a) 列车



(b) 速度-距离控制器



(c) ZC 控制器



(d) 多列车控制队列

图 6 TTZQ 网络模型图

是 4 者之积，即 Train ‖ TSpAPs ‖ ZCControl ‖ Queue，简称 TTZQ。模型中，以“!”结尾的标记表示发出此信号时转换发生；以“?”结尾的标记表示接收到该信号时转换发生，以此实现各模型中相同的转换同步发生。各成员自动机之间除了通过同步转换的标记传递信息外，还定义了自身的局部变量和成员函数，同时整个自动机网络模型还使用了全局变量进行通信，用来保证系统逻辑功能的正确性。

模型中主要位置和事件(标记)如表 1 所示。

表 1　模型中主要位置和事件

	列车		速度-距离控制器		ZC 控制器		多列车控制队列	
主要位置	login	列车登陆	SPL1	速度 1 级	emp	ZC 空闲	Shift	移位控制
	control	列车受控	SPL2	速度 2 级	logining	登陆控制		
	Running	列车运行	SPL3	速度 3 级	RunCtrl	运行控制		
	Stop	列车停车	SPL4	速度 4 级	Delete	删除控制		
	Exit	列车离开			Cross	离开控制		
主要事件	Run	运行	TtoTsP	速度更新	LogIn	登陆	empty	队列空
	Stop	停车			Control	控制	notempty	队列非空
	ZCtoT	接收 MA			gct	发送 MA	Sort	列车排序
	Exit	离开			add	入队列	gid	取列车 id
					rem	出队列		

模型所描述的过程如下：

列车 Train 到达 ZC 控制区域边界以后，向 ZCControl 发送 Login 消息，通知 ZCControl 该列车要登陆 ZC，与此同时 ZCControl 收到 Login 消息(由通道的同步性来保证)。ZCControl 的超时时钟判断该消息是否是在 T 个单位时间内收到的，如果是则发送 add 消息到其控制队列 Queue，控制队列 Queue 记录该列车的 ID 和位置。

在列车登陆完成以后，ZCControl 将 Timer 清零，进行对列车的控制过程进行操作。首先 ZCControl 向 Queue 发送 sort 消息，要求 Queue 对刚才加入控制队列的 3 辆列车进行排序(排序的原则是按照相对于 ZC 控制区域的起点：即列车的位置)。排序完成以后向 Queue 发送 gid 消息，要求 Queue 从队列中取出队头列车的 id，此时将 Timer 清零并对列车进行控制(控制过程包括 control 和 Running)。其次向 Queue 发送 gct 命令，要求 Queue 计算出当前列车的 MA(这里由于在追踪运行，仅考虑与前行列车间的追踪问题，因此 MA 为前、后列车之间的距离)。最后 ZCControl 向 Train 发送 ZCtoT 消息，通知 Train 提取相应的 MA(MA 定义为全局变量距离)。这个过程都是在 Timer $<$L 个时间单位内完成的。Train 收到 gct 命令以后，将 Timer1 清零同时发送消息 TtoTsP 到速度-距离控制模型 TSpAPs，TSpAPs 则收到 TtoTsP 消息以后，根据当前列车的速度、线路限制速度和 MA 计算列车的加速度(为了保证追踪间隔，取最大加速度值)，来更新列车的位置和速度，并存储起来。这一过程要求在 Timer1$<$U 个单位时间内完成，与此同时将 Timer1 清零。

3.2　模型的仿真与验证

该模型针对 3 列列车在区间追踪运行而设计，当然可以根据需要进行任意列车的追踪仿真模拟。模型中有 Train1、Train2、Train3、TSpAPs、ZCControl 和 Queue 共 7 个实体。该系统的活性由转换时间约束和位置的不变式来保证，而对于系统的安全性，在 UPPAAL 的模拟器中，对列车登陆、受控、运行、停车和离开的各种顺序进行组合。经过多次模拟运行，各列车均能顺利地登陆、受控、运行、停车和离开。图 7 为在模拟器中实验时，随机得到的一个各实体之间通过管道相互通信、控制的消息序列。

按照 ZC 子系统性能和功能要求，TTZQ 必须要满足这些特定的要求以保证系统的安全性和受限活性。应用 BNF 语言对该模型的性能和功能要求进行描述，描述的程序实体如下：

(1) 功能要求

① A[ ] not deadlock 系统无死锁；

② E$<>$((Train1. login) or (Train1. control) or (Train1. Running) or (Train1. stop) or (Train1. Exit)) and ((Train2. login) or (Train2. control) or (Train2. Running) or (Train2. stop) or (Train2. Exit)) and ((Train3. login) or (Train3. control) or (Train3. Running) or (Train3. stop) or (Train3. Exit))

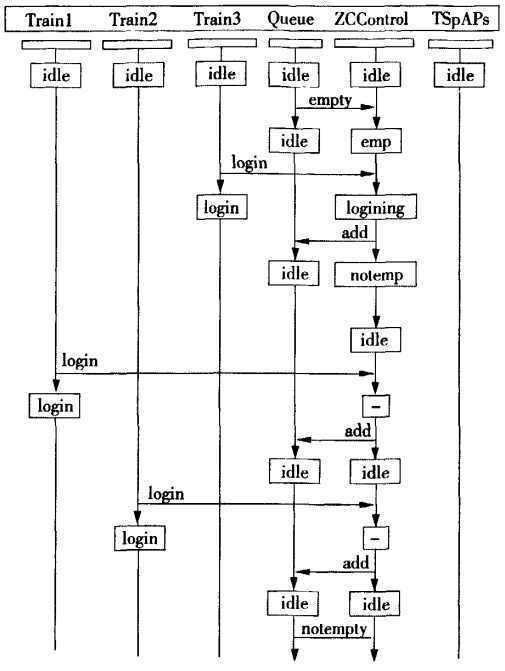


图7 控制消息序列图

每列列车都能完成在ZC区间的登陆、控制接管、受控运行和离开4个过程；

③ E<>((Train1. CtrlSp)or(Train2. CtrlSp)or(Train3. CtrlSp))

每辆列车都能得到控制信息；

④ E<>((Train1. SpDip)or(Train2. SpDip)or(Train3. SpDip))

列车能根据控制信息更新自己的位置和速度；

⑤ E<> ZCControl. CtrlSp

ZC能够发送MA信息。

(2) 性能要求

在初始状态下假定Train1、Train2和Train3在ZC中的位置是依次增加的，而且，两列车之间的保护距离为DisToP，线路限速为Vmax，则：

① A[ ]((Train1. login imply Train1. Time<=T) or (Train2. login imply Train1. Time<=T) or (Train3. login imply Train1. Time<=T))；

② A[ ]((Train1. control imply Train1. Time<=T)or(Train2. control imply Train1. Time<=T)or(Train3. control imply Train1. Time<=T))

列车登陆、受控接管在T个单位时间内完成；

③ A[ ]((Train1. Running imply Train1. Time<=U)or(Train2. Running imply Train1. Time<=U)or(Train3. Running imply Train1. Time<=U))

ZC控制运行周期在[0,U]内，即ZC从收到列车位置的报告开始到完成对每列列车的运行控制在U个单位时间内实现；

④ A[ ]((Train3. Ps-Train2. Ps>DisToP) and (Train2. Ps-Train1. Ps>DisToP))

前、后列车之间的运行距离大于保护距离；

⑤ A[ ]((Train3. Sp<=Vmax)and (Train2. Sp<=Vmax) and (Train1. Sp<=Vmax))

列车的最大速度小于线路限速。

在UPPAAL的验证器中执行上述程序体，各要求都能通过，表明TTZQ能满足这些要求，系统是安全的。

4 结束语

本文采用自动机理论，应用UPPAAL模型检验工具对CBTC区域控制子系统进行建模、仿真和验证。该验证模型称为TTZQ模型，它成功地验证了CBTC区域控制子系统中规定的性能要求，从而保证了该子系统的安全性和受限活性。因此UPPAAL能够对复杂的系统进行仿真验证。

参考文献：

[1] Bin Ning, Tao Tang, Ziyou Gao, Fei Yan, Fei-Yue Wang, Daniel Zeng. Intelligent Railway Systems in China[J]. IEEE Intelligent Systems, 2006,21: 80-83.

[2] 唐涛,郜春海,李开成,燕飞. 基于通信的列车运行控制技术发展战略探讨[J]. 都市快轨交通,2005,18(6):25.
TANG Tao , GAO Chun-hai, LI Kai-cheng, YAN Fei. A Discussion on the Development Strategy CBTC[J]. Urban Rapid Rail Transptation, 2005,18(6):25.

[3] 吴东勇,张勇. 基于通信的列车控制系统的有色Petri网模型的研究[J]. 系统仿真学报,2005,17(10):2388.
WU Dong-yong, ZHANG Yong. Researching Colored Petri Nets Model of Communication Based Train Control System[J]. Journal of System Simulation, 2005, 17(10): 2388.

[4] 周清雷,姬莉霞,王艳梅. 基于UPPAAL的实时系统模型验证[J]. 计算机应用,2004,24(9):130.
ZHOU Qing-lei ,JI Li-xia ,WANG Yan-mei. Model checking of real-time systems based on UPPAAL[J]. Computer Applications, 2004,24(9):130.

[5] 周清雷,姬莉霞. 基于时间自动机的道岔控制研究[J]. 控制工程,2004,11(增刊):146-147.
ZHOU Qing-lei ,JI Li-xia. On Automatic Turnout Control Based on Timed Automata[J]. Control Engineering of China, 2004,11(supplement):146-147.

(责任编辑 江 峰)

基于UPPAAL的城市轨道交通CBTC区域控制子系统建模与验证

作者： 吕继东， 唐涛， 燕飞， 徐天华， Lü Ji-Dong， TANG Tao， YAN Fei， XU Tian-hua
作者单位： 北京交通大学,轨道交通控制与安全国家重点实验室,北京,100044
刊名： 铁道学报 ISTIC EI PKU
英文刊名： JOURNAL OF THE CHINA RAILWAY SOCIETY
年，卷(期)： 2009,31(3)
被引用次数： 2次

参考文献(5条)

1. Bin Ning;Tao Tang;Ziyou Gao;Fei Yan Fei-Yue Wang Daniel Zeng Intelligent Railway Systems in China [外文期刊] 2006(6)

2. 唐涛;郜春海;李开成;燕飞 基于通信的列车运行控制技术发展战略探讨[期刊论文]-都市快轨交通 2005(06)

3. 吴东勇;张勇 基于通信的列车控制系统的有色Petri网模型的研究[期刊论文]-系统仿真学报 2005(10)

4. 周清雷;姬莉霞;王艳梅 基于UPPAAL的实时系统模型验证[期刊论文]-计算机应用 2004(09)

5. 周清雷;姬莉霞 基于时间自动机的道岔控制研究[期刊论文]-控制工程 2004(zk)

本文读者也读过(4条)

1. 朱莉.Zhu Li 基于通信的列车控制技术下城市轨道交通轨旁信号的分析[期刊论文]-城市轨道交通研究 2010,13(8)

2. 牛儒.唐涛.NIU Ru.TANG Tao 基于CPN的CBTC地面数据通信系统仿真和分析[期刊论文]-系统仿真学报 2008,20(17)

3. 周清雷.姬莉霞.王艳梅 基于UPPAAL的实时系统模型验证[期刊论文]-计算机应用2004,24(9)

4. 郭华.庄雷.张习勇.Guo Hua.Zhuang Lei.Zhang Xiyong UPPAAL---一种适合自动验证实时系统的工具[期刊论文]-微计算机信息2006,22(15)

引证文献(2条)

1. 赵显琼.李开成.唐涛.袁磊 基于UML的CTCS-3级列控系统运营场景分析方法研究及应用[期刊论文]-铁道通信信号 2010(8)

2. 张屹.魏学业.何春明 基于时间化UML的安全通信模型检测[期刊论文]-电子测量与仪器学报 2010(10)