

基于 UML 与 UPPAAL 的高铁列控 临时限速切换场景建模与验证

周翔

滨州市交通运输局, 山东 滨州 256600

摘要:为提高高速铁路列控临时限速命令在临时限速服务器(temporary speed restriction server, TSRS)与无线闭塞中心(radio block center, RBC)跨界重叠区域信息传递过程的时效性和安全性,建立 TSRS 切换与 RBC 切换跨界重叠区域限速流程的数学模型,根据中国列车运行控制系统(Chinese train control system, CTCS)CTCS-2/CTCS-3 高铁列控系统间临时限速命令交互的特点,采用统一建模语言(unified modeling language, UML)与时间自动机模型理论相结合的方法,采用形式化验证工具 UPPAAL 寻找临时限速命令在跨界重叠区域信息传递的不足和漏洞。研究表明:列控临时限速是高铁安全运行的重要组成部分,其与高铁列控高铁调度集中(centralized traffic control, CTC)、RBC、列控中心(train control center, TCC)等相关子系统有频繁的信息交互,不同子系统间信息传递过程不同,Timer(时间控制器)、Resend(重发控制器)、TSRS 和 RBC 时间自动机数学模型验证结果为 TSRS 切换与 RBC 切换信息在跨界重叠区域的传递时间小于 3 s,且时间自动机模型信息通道无锁死情况,大大提高高铁列车运行的时效性和安全性。

关键词:临时限速;时间自动机;UML;UPPAAL;高铁列控

中图分类号:U284.48

文献标志码:A

文章编号:1672-0032(2024)03-0031-08

引用格式:周翔. 基于 UML 与 UPPAAL 的高铁列控临时限速切换场景建模与验证[J]. 山东交通学院学报, 2024, 32(3): 31-38.

ZHOU Xiang. Modeling and verification of high-speed railway train control temporary speed limit switching scenarios based on UML and UPPAAL[J]. Journal of Shandong Jiaotong University, 2024, 32(3): 31-38.

0 引言

截至 2023 年底,我国高速铁路运营里程已达 4.5 万 km^[1]。高速铁路的飞速发展对运营安全性和时效性也提出更高要求。高铁列控系统是保障高铁安全运行的核心,其中二级临时限速系统又是重中之重^[2]。在传递临时限速命令时,须严格遵守中国国家铁路集团有限公司下发的技术规范要求,如文献[3]等。但实际运行中信息在跨界重叠区域传递时又存在特殊性,研究跨界重叠区域信息传递对提升高铁列车运行的时效性和安全性具有重要意义^[4-5]。

康仁伟^[6]提出基于时间自动机的列控系统建模与验证方法,以中国列车运行控制系统(Chinese train control system, CTCS)CTCS-3 级临时限速和等级转换运营场景为例,说明该建模与验证方法的有效性;赵荣亮^[7]采用时间自动机理论对临时限速系统进行建模,并结合高铁调度集中(centralized traffic control, CTC)系统调度台分界口、CTCS 等级转换,建立各自的时间自动模型,采用工具 UPPAAL 对模型进行时序逻辑的仿真,得到系统工作流程的仿真时序图,验证各模型的功能;安越^[8]采用统一建模语言(unified modeling language, UML)和时间自动机相结合,对无线闭塞中心(radio block center, RBC)进行

收稿日期:2023-07-07

作者简介:周翔(1989—),男,河北衡水人,工学硕士,主要研究方向为铁路通信信号控制, E-mail:zhouxiang0303@126.com。

建模验证,保证 RBC 控车的实时性和安全性;朱伟等^[9]总结 RBC 出行车许可异常缩短和无线通信超时故障,提出有效提高 CTCS-3 级列控系统运用质量的建议。高铁列控临时限速的研究目前还停留在无跨界信息的常规区段,较少涉及 2 个不同系统在交叉重叠区域临时限速信息传递的复杂性,研究手段单一。

本文采用 UML 和 UPPAAL 相结合的办法,对高铁列控子系统信息交互时重叠区域临时限速信息的交互过程进行建模,并采用消息顺序图(message sequence charts, MSC)、UML 时序图和时间自动机模型相互转换方式进行逐层分析,验证列控系统临时限速服务器(temporary speed restriction server, TSRS)和 RBC 信息交互重叠区域的时效性和安全性。

1 TSRS 切换与 RBC 切换重叠区域限速流程临时限速场景分析

高铁列控系统临时限速命令的交互过程具有阶段性和区域性,不同的子系统间信息传递过程不同,在跨界重叠区域的信息传递过程更复杂。相邻区段的列控系统均会产生信息传递的重叠区域,重叠区域不同子系统间也会产生信息交互。本文以列控系统跨界区域 A、B 两侧作为重叠区域,建立临时限速信息在重叠区域的数学模型,分析系统的安全性和时效性^[10-12]。

高铁列控系统与子系统信息交互的穿插重叠区域是关系高铁安全运行的特殊场景,跨界信息交互处于不同的列控设备控制区段,交互过程复杂,需通过 A、B 两侧不同的设备间互联互通完成信息的安全传递,其复杂性和不同的时效性易导致重叠区域的信息产生错乱,影响高铁的安全运行,进路信息和列车数据未得到有效传输。需建立 UML 和时间自动机模型,对信息交互过程进行建模验证,分析模型的安全性和时效性^[13-14]。临时限速在重叠区域的信息交互过程如图 1 所示。

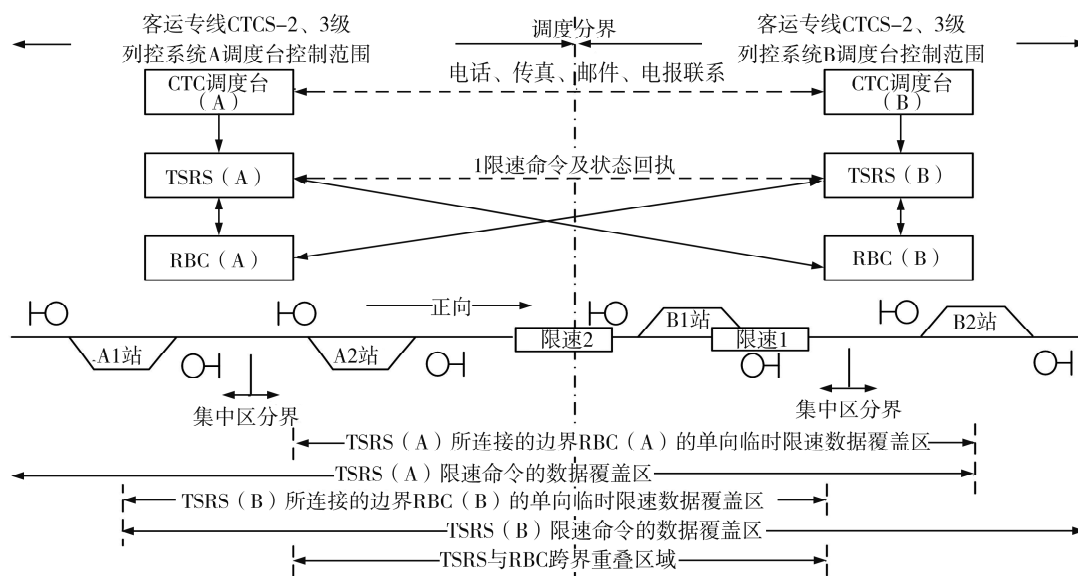


图 1 临时限速在重叠区域的信息交互过程

2 UML 模型

UML 模型表达内容全面、详细、简单、多样,但不具有广泛性,对需要形式化验证的模型不具有验证作用。从 3 个步骤分析具体模型:1)绘制 MSC 消息顺序图;2)从 MSC 转换为 UML 时序图;3)由 UML 时序图转换为时间自动机模型图,将最终转换图形由 UPPAAL 形式化验证工具输入巴科斯范式(Backus-Naur form, BNF)验证语句进行验证。本文主要研究重叠区域切换场景下的临时限速信息交互,采用 MSC 构建可视化时间信息交互模型,以此为依据同步构建 UML 模型和时间自动机模型^[15-17]。

2.1 基于 MSC 的系统建模

定义 1: MSC 是多个实体间进行形式化语言描述, 并采用二维图形概括消息交互通信实例的图形化语言, 构建关于区域关系的描述。形式化语言词组包括 $\langle \text{area1} \rangle$ contains $\langle \text{area2} \rangle$ 、 $\langle \text{area1} \rangle$ is followed by $\langle \text{area2} \rangle$ 、 $\langle \text{area1} \rangle$ is associated with $\langle \text{area2} \rangle$ 、 $\langle \text{area1} \rangle$ is attached to $\langle \text{area2} \rangle$ 、 $\langle \text{area1} \rangle$ above $\langle \text{area2} \rangle$ 、 $\{ \langle \rangle \}$ set。 $\langle \text{area1} \rangle$ contains $\langle \text{area2} \rangle$ 表示区域 1 包含区域 2, 通常用于描述嵌套或包含关系; $\langle \text{area1} \rangle$ is followed by $\langle \text{area2} \rangle$ 表示区域 1 紧随在区域 2 后, 通常用于描述顺序关系; $\langle \text{area1} \rangle$ is associated with $\langle \text{area2} \rangle$ 表示区域 1 与区域 2 相关联, 可能指二者间存在某种关联或联系; $\langle \text{area1} \rangle$ is attached to $\langle \text{area2} \rangle$ 表示区域 1 附加在区域 2 上, 描述二者间的连接或附属关系, 区域 2 必须为 1 个或 1 组图形符号, 构成消息传递路径, 如图 2 所示; $\langle \text{area1} \rangle$ above $\langle \text{area2} \rangle$ 表示区域 1 在区域 2 的上方并相连, 如图 3 所示, 通常用于描述空间位置关系; $\{ \langle \rangle \}$ set 表示 1 个集合, 通常用于收集或组织具有某种共同特征或属性的元素。

消息域中的消息在实例与环境间进行交换, 即消息入 (message in) 消息出 (message out)^[18], 如图 4 所示。

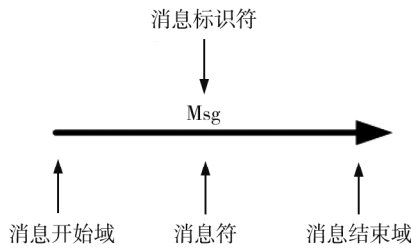


图2 消息传递路径



图3 消息垂直相连

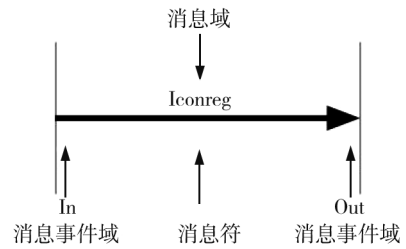


图4 实例与环境消息交互

定义 2: ::= 定义符。左边为非终结符, 右部为终结符; $\langle \rangle$ 括号内的符号为非终结符, 需进一步定义。

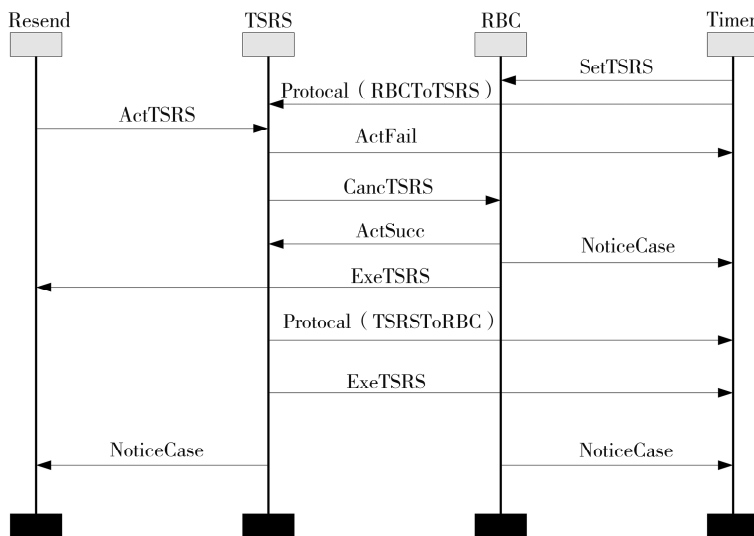
MSC 的主体包括参与者、消息、时间顺序和交互关系, 通过对象沿生命线的交互展现对象间的通信和消息触发关系, 强调消息传递的时间顺序和交互细节。MSC 的解释主体为^[19-21]:

$\langle \text{msc body area} \rangle ::= \{ \langle \text{instance layer} \rangle \langle \text{text layer} \rangle \langle \text{gate def layer} \rangle \langle \text{event layer} \rangle \langle \text{connector layer} \rangle \}$ set,

其中, 临时限速 MSC 主体为:

$\langle \text{SetTSRS area} \rangle ::= \{ \langle \text{Protocol (RBCToTSRS) layer} \rangle \langle \text{Protocol (TSRSToRBC) layer} \rangle \langle \text{ActTSRS layer} \rangle \langle \text{ExeTSRS layer} \rangle \langle \text{NoticeCase layer} \rangle \}$ set。

临时限速命令的交互 MSC 模型如图 5 所示。



Resend—重发控制器; Timer—时间控制器;
ActTSRS—激活临时限速服务器命令;
SetTSRS—设置临时限速服务器命令;
ActFail—激活失败; Protocol (RBCToTSRS)—
无线闭塞中心与临时限速服务器的协议;
CancTSRS—取消临时限速服务器命令;
ActSucc—激活成功; ExeTSRS—执行临时限速
服务器命令; Protocol (TSRSToRBC)—临时限
速服务器与无线闭塞中心的协议;
NoticeCase—预告信息。

图5 临时限速命令的交互 MSC 模型

2.2 基于 UML 时序图的建模

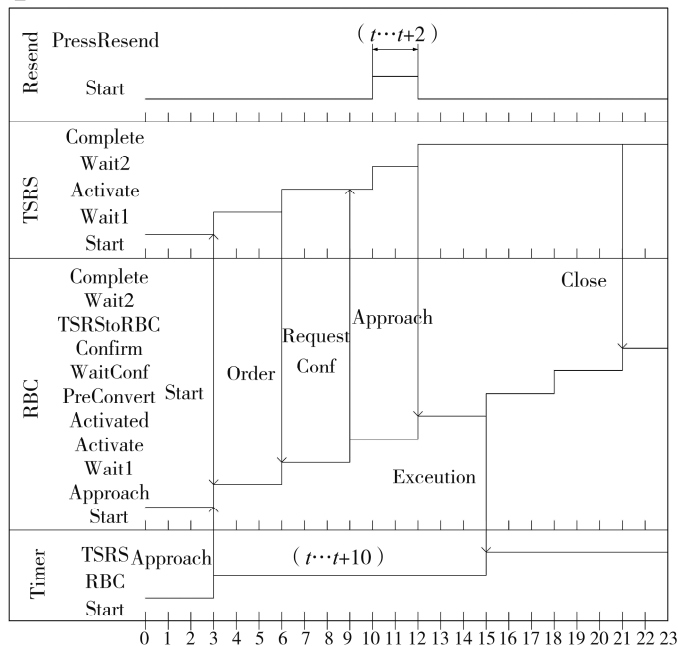
在 UML 时序图中分为横轴、纵轴和生命线,分别表示时间进行线、各对象的状态和系统运行的主要元素,系统运行对象的工作状态呈阶梯状态^[22]。在 UML 时序图中不同信息的交互对象由带实心箭头的生命线相互连接,表示从一种状态转移到另一种状态。这种对象状态的迁移需具体量化的时间变量表达,持续的时间变量为 t 。根据 2.1 节中 MSC 中交互的状态信息,建立 TSRS 切换与 RBC 切换重叠区域限速流程的 UML 时序图。TSRS 切换与 RBC 切换重叠区域限速流程中各信息交互对象的状态如表 1 所示^[23]。

表 1 TSRS 切换与 RBC 切换重叠区域限速流程中各信息交互对象的状态

对象	状态
Resend	Start PrePressResend(运行重发控制器)
TSRS	Start Buidconn ConnYes Wait1 Send Wait2 CaculateTSRS PreConvert Complete(临时限速服务器命令转换交互完成)
RBC	Start GRE ConnTSRS BuidConn-R ConnRBC ConnYes SendData WaitData(临时限速服务器与无线闭塞中心建立数据交换)
Timer	Start ConfData WaitTSRS NewData WaitRBC PreConvert WaitConf Complete TSRSStoRBC(临时限速服务器与无线闭塞中心等待新数据执行完毕)

采用 MSC 直观表述 4 个对象的信息交互流程,采用 UML 时序图表示时间信息交互过程。主要事件和发生对象的表述方式为:timeout-T=0 表示与 TSRS 建立的信息通信未超时;timeout-R=0 表示与 RBC 建立信息通信未超时;PressResend==1 表示临时限速信息和无线闭塞中心信息交互的可循环性,防止死循环;PressTimer==1 表示时间不会锁止,时间状态正循环。设置时间约束条件分别为:ConnTSRS(与临时限速服务器建立联系)时间状态为 10 s,ConnRBC(与无线闭塞中心建立联系)时间状态为 5 s,PressResend(运行重发控制器)循环时间为 1 s,PressTimer(运行时间控制器)防锁止时间循环为 2 s^[24-26]。根据以上信息建立 TSRS 切换与 RBC 切换重叠区域限速流程的 UML 时序图模型,如图 6 所示。

TSRS_RBC



Start—开始;Complete—完成;Wait—等待;
Activate—激活;TSRSStoRBC—临时限速服
务器至无线闭塞中心;Confirm—确认;
WaitConf—等待确认;PreConvert—预转
换;Activated—已激活;Approach—进场;
Order—命令;RequestConf—请求确认;
Close—关闭;Exceution—例外。

图 6 临时限速命令交互的 UML 时序图

2.3 UML 时序图向时间自动机模型的转换

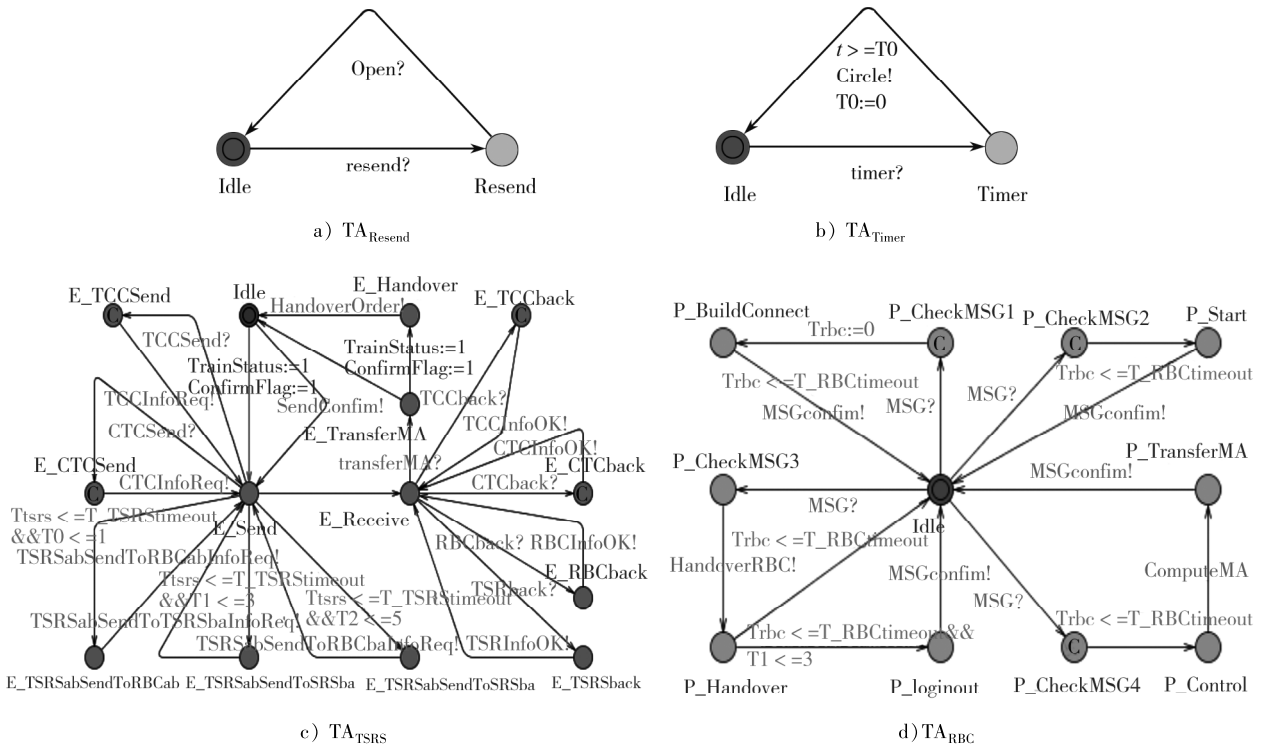
时序图中的生命线对应时间自动机模型中的 temple,表示 1 个对象或子系统;时序图中的状态 state 对应时间自动机模型中的位置 location,时间自动机的初始状态 idle 替换 UML 时序图中的初始状态 start,

时序图中的消息 message 对应时间自动机模型中的通道 channel, 时间线 timeline 对应时钟 clock, 事件 event 对应监管 guard, 根据对应关系, 在建立的时间自动机位置模型图中添加消息通道、时间约束和事件监管的信息。

2.4 基于时间自动机的系统建模

UPPAAL 是用于验证时间自动机模型正确性的工具, 它支持系统的建模、模拟和形式化特性验证, 能避免状态空间爆炸问题, 保证系统的正确性和安全性。采用形式化验证语言 BNF 验证 UPPAAL, 语法及其含义为 $\text{Prop} ::= E <> p \mid E[] \mid p \mid A <> p \mid A[] \mid p \mid p \rightarrow q^{[27]}$ 。

建立 TSRS 与 RBC 切换重叠区域时间自动机模型, 根据 2.1 节和 2.2 节中 MSC 消息顺序图和 UML 时序图中对信息的交互流程和时间事件的发生顺序, 对重叠区域信息的交互流程, 即 Resend、Timer、TSRS 和 RBC 等 4 个建模对象, 进行建模, 建立 $\text{TA}_{\text{Resend}}$ 、 TA_{Timer} 、 TA_{TSRS} 、 TA_{RBC} 等 4 个时间自动机模型, 如图 7 所示。



Idle—空闲; Open—开放重发命令; Circle—时间循环命令; E_Send—发送信息; E_Receive—接收信息; E_TCCSend—列控中心发送信息; E_CTCSend—调度集中发送信息; E_TSRSabSendToRBCab—临时限速服务器和无线闭塞中心 AB 两侧交换信息; E_TSRSabSendToTSRSba—临时限速服务器 AB 和临时限速服务器 BA 两侧交换信息; E_TSRSabSendToRBCba—临时限速服务器 AB 和无线闭塞中心 BA 两侧交换信息; E_TSRSback—临时限速服务器反馈信息; E_RBCback—无线闭塞中心反馈信息; E_CTCSback—调度集中反馈信息; E_TCCback—列控中心反馈信息; E_Handover—移交信息; P_CheckMSG1—检查 1 通信通道; P_BuildConnect—建立通信链接; P_CheckMSG3—检查 3 通信通道; P_Handover—移交信息; P_loginout—登录信息; P_CheckMSG4—检查 4 通信通道; P_Control—控制传递信息; P_TransferMA—转移移动授权信息; P_Start—开始传递信息; P_CheckMSG2—检查 2 通信通道; HandoverOrder—移交命令; MSGconfirm—信息通道确认; TCCSend—列控中心信息发送; TCCInfoReq—列控中心信息请求; TCCback—列控中心信息返回; TCCInfoOK—列控中心信息无误; CTCSend—调度集中信息发送; CTCInfoReq—调度集中信息请求; CTCback—调度集中信息返回; CTCInfoOK—调度集中信息无误; TSRSback—临时限速服务器信息返回; TSRSInfoOK—临时限速服务器信息无误; TrainStatus—列车状态; ConfirmFlag—确认状态; $\text{Tsrs} \leq T_{\text{TSRSStimeout}}$ —临时限速时间限制; $\text{Tsrs} \leq T_{\text{TSRSStimeout}} \& T1 \leq 3$ —TSRSab 和 TSRSba 的信息交互时间不超过 3 s; $\text{Tsrs} \leq T_{\text{TSRSStimeout}} \& T2 \leq 5$ —TSRSab 和 RBCba 的信息交互时间不超过 5 s; $\text{Trbc} \leq T_{\text{RBCStimeout}}$ —无线闭塞中心时间限制; $\text{Trbc} \leq T_{\text{RBCStimeout}} \& T1 \leq 3$ —RBC 切换信息的移交、控车流程时限为 3 s; ComouteMA—延伸移动授权信息; E_TransferMA—传递移动授权信息; transferMA—传递移动授权信息; SendConfirm—发送确认消息; RBCback—无线闭塞中心信息返回; RBCInfoOK—无线闭塞中心信息无误; TSRSabSendToRBCabInfoReq!—临时限速服务器和无线闭塞中心的 A、B 两侧分别进行通信信息请求; HandoverRBC!—移交无线闭塞中心信息。

图 7 TSRS 与 RBC 切换重叠区域时间自动机模型

设 TSRS 与 RBC 切换重叠区域时间自动机模型为:

$$T_A = \langle S, S^0, A, X, I, E \rangle,$$

式中: S, S^0, A, X, I, E 分别为时间自动机建模的过程状态、初始状态、触发事件、时间参数、整数变量、状态转移路径。

以 $T_{A,RBC}$ 时间自动机为例说明, 过程状态 $S = \{idle, P_CheckMSG1, P_BuildConnect\}$, 初始状态 $S^0 = idle$; 触发事件 $A = \{MSG?, MSGconfirm!\}$, 时间参数 $X = \{T_1, T_{rbc}, T_RBCtimeout\}$, 整数变量 $I = \{MSG?, MSGconfirm!\}$, 状态转移路径 $E = \{idle, P_CheckMSG4, P_Control, P_TransferMA, idle\}$, 其中, “P_” “E_” 开头分别表示限速命令的拟定、下达过程。

由图 7 可知: Resend 可在保障信息交互循环时防止信息循环锁死, Timer 是保障在无时间延迟的情况下防止时间信息锁死, 二者在保证无时间信息锁死的情况下进行 RBC 和 TSRS 时间自动机模型信息传递的闭循环。

RBC 切换时间自动机模型中, $Trbc > RBCtimeout$ 时, 说明信息传递失败, 移交命令超时, 根据操作者要求, 可重新下达命令, 从 Idle 重新发送。由图 7c) 可知: 有 3 个时间迁移变量端分别为 $E_TSRSabSendToRBCab$ 、 $E_TSRSabSendToTSRSba$ 、 $E_TSRSabSendToRBCba$, 为临时限速服务器和无线闭塞中心的 A、B 两侧分别进行通信信息的交叉传递。图 7 设 3 个时间约束, $T_{tsrs} \leq T_TSRStimeout \& \& T_0 \leq 1$ 表示 TSRSab 和 RBCab 的信息交互时间不超过 1 s, $T_{tsrs} \leq T_TSRStimeout \& \& T_1 \leq 3$ 表示 TSRSab 和 TSRSba 的信息交互时间不超过 3 s, $T_{tsrs} \leq T_TSRStimeout \& \& T_2 \leq 3$ 表示 TSRSab 和 RBCba 的信息交互时间不超过 3 s。

TSRS 与 RBC 切换重叠区域的主要位置为: Resend(重发控制器)、Timer(时间控制器)、E_Handover(移交限速命令)、E_TransferMA(传递移动授权信息)、E_Send(发送信息)、E_Receive(接收信息)、P_BuildConnect(建立通信链接)、P_Start(开始传递信息)、P_CheckMSG1(检查 1 通信通道)、P_Control(控制传递信息)。

TSRS 与 RBC 切换重叠区域的主要通信通道为: HandoverOrder(移交命令)、SendConfirm(发送确认消息)、transferMA(传递移动授权信息)、TCCSend TCC(发送信息)、TCCInfoReq TCC(信息需求)、RBCback RBC(返回信息)、RBCInfoOK RBC(信息返回正确)、MSGconfirm(信息通道确认)、Open(开放重发命令)、Circle(时间循环命令)。

3 系统模型的验证

将 UPPAAL 验证器导入已构建的时间自动机模型, 同时应用语法 BNF 验证 TSRS 与 RBC 切换重叠区域时间自动机模型满足安全性和受限活性的要求。

3.1 系统安全性要求

1) 系统没有死锁。 $A[] \text{ not deadlock}$, 验证通过。

2) RBC 建立通信协议, 完成 RBC 通信信息的传递。

$E \langle \rangle ((RBC.P_BuildConnect) \text{ and } (RBC.P_Start) \text{ and } (RBC.P_Control) \text{ and } (RBC.P_Handover))$, 验证通过。

3) TSRS 和 RBC 切换信息移交正常完成。

$E \langle \rangle ((RBCa.Idle) \text{ imply } (RBCa.P_Handover) \text{ and } (RBCb.Idle) \text{ imply } (RBCb.P_Handover) \text{ and } (TSRSa.Idle) \text{ imply } (TSRSa.E_TSRSaSendToRBCb) \text{ and } (TSRSa.Idle) \text{ imply } (TSRSb.E_TSRSbSendToRBCa))$, 验证通过。

4) 在列车非减速状态下 RBC 切换信息正常移交。

$E \langle \rangle ((RBC.newspeed \geq RBC.oldspeed) \text{ imply } (RBC.P_Handover))$, 验证通过。

3.2 系统受限活性要求

1) TSRS 和 RBC 在 A、B 两侧 1 s 内完成通信信息的移交。

$A[]((TSRSab. ControlRBCab) \text{ imply } (TSRSab. E_TSRSabSendToRBCab) \text{ and } (T0 \leq 1))$, 验证通过。

2) TSRS_A 和 TSRS_B 在 3 s 内完成临时限速命令的切换。

$A[]((TSRSa. ControlTSRSb) \text{ imply } (TSRSab. E_TSRSabSendToTSRSba) \text{ and } (T1 \leq 3))$, 验证通过。

3) TSRS_A 和 RBC_B, TSRS_B 和 RBC_A 在 3 s 内进行临时限速命令的双向传递, 同时在 A、B 两侧对无线闭塞中心的信息传递做出必要的时间限制。

$A[]((TSRSab. ControlRBCba) \text{ imply } (TSRSabE_TSRSabSendToRBCba) \text{ and } (T2 \leq 3))$, 验证通过。

通过验证分析可知: 跨界重叠区域的时间自动机模型通过 UPPAAL 验证工具的状态验证, 满足安全性和时效性应用, 达到客运专线列控系统临时限速技术规范要求。验证语句在验证中正常通过, 形成模拟器状态图。

4 结束语

本文采用 MSC 和 UML 建立 TSRS 与 RBC 切换重叠区域的基础时间约束模型, 为方便自动机模型的转换, 在 MSC 和 UML 的建模过程中描述时间约束条件和状态转移过程。采用时间自动机方法建立 TSRS 与 RBC 切换重叠区域时间自动机模型, 采用形式化验证工具 UPPAAL 进行模型验证。结果表明 TSRS 与 RBC 切换重叠区域信息在具体时间限制内可顺利完成信息交互, 说明其具有安全性和时效性, 保证高铁列控系统在 TSRS 和 RBC 切换情况下的安全运行。

后续的研究中可进一步论证 2 个相邻区段 TSRS 和 TSRS 重叠区域信息交互的复杂性, 为铁路通信信号研究提供技术支撑。

参考文献:

- [1] 新京报. 我国高铁达到 4.5 万公里[N/OL]. (2024-01-09)[2024-06-30]. <http://www.xinhuanet.com/fortune/20240109/7e9f592edefe48d8b9a0a67fab44da2b/c.html>.
- [2] 宋莉, 刘伯鸿. 基于 UPPAAL 的列控系统临时限速建模与验证[J]. 铁路计算机应用, 2020, 29(5): 12-16.
- [3] 中国国家铁路集团有限公司, 中国铁道科学研究院集团有限公司通信信号研究所. 列控中心接口规范 第 7 部分: 列控中心与临时限速服务器接口: Q/CR 864. 7—2021[S]. 北京: 中国铁道出版社, 2021.
- [4] 冯婷婷. 基于 UML 活动图模型测试用例生成的研究[D]. 衡阳: 南华大学, 2020.
- [5] 宋菲. 基于时间自动机的 RBC 控车场景建模与验证[D]. 成都: 西南交通大学, 2017.
- [6] 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.
- [7] 赵荣亮. 列控系统 TSRS 形式化建模分析与验证[D]. 成都: 西南交通大学, 2014.
- [8] 安越. 基于 UML 和 TA 的 RBC 系统形式化建模与分析[D]. 兰州: 兰州交通大学, 2016.
- [9] 朱伟, 冯飞. RBC 典型问题原因分析及处置[J]. 铁道通信信号, 2022, 58(10): 35-39.
- [10] 施汀瑞. 基于时间自动机的 RBC 切换的建模分析与实现[D]. 北京: 北京交通大学, 2019.
- [11] 彭丽维, 宋鹏飞, 江雪莹, 等. 基于模型的联锁软件测试用例生成方法[J]. 铁路通信信号工程技术, 2022, 19(11): 32-36.
- [12] 铁道部. 客运专线 CTCS-2 级列控系统列控中心技术规范: 科技运[2007]158 号[S/OL]. (2023-06-20)[2018-11-11]. <https://www.doc88.com/p-7778434233848.html>.
- [13] 李耀, 张晓霞, 郭进. 铁路信号系统软件测试建模方法[J]. 西南交通大学学报, 2022, 57(2): 392-400.
- [14] 于潇. CBTC 联锁系统的形式化建模与验证方法研究[D]. 北京: 中国铁道科学研究院, 2017.
- [15] 张广泉. 形式化方法导论[M]. 2 版. 北京: 清华大学出版社, 2023.
- [16] 贺伟. 基于时间自动机的行车许可的建模与验证[D]. 成都: 西南交通大学, 2017.
- [17] 王观宁. 基于 UPPAAL 的联锁进路控制流程建模与验证[D]. 北京: 北京交通大学, 2009.
- [18] 张鹏基. 基于时间自动机的 ZC 子系统建模与验证[D]. 北京: 北京交通大学, 2017.
- [19] 张志斌, 张耀回. 空口监测在 CTCS-3 级列控系统无线超时分析中的应用研究[J]. 铁道通信信号, 2022, 58(10): 71-75.

- [20] 刘艳平,李海浩.基于序列图和状态图的软件测试用例生成方法[J].电子设计工程,2019,27(24):167-170.
- [21] 卢佩玲,郝韬,徐强.高铁联络线不利条件下 CTCS3CTCS2 等级转换方案研究[J].铁道标准设计,2022,66(12):137-142.
- [22] 王建.基于随机 Petri 网的高铁列控系统 C2/C3 等级转换过程建模及仿真[D].成都:西南交通大学,2015.
- [23] 袁磊,王俊峰,康仁伟,等. CTCS-3 级列控系统临时限速建模与验证[J].西南交通大学学报,2013,48(4):708-714.
- [24] 周翔,武晓春.基于 MSC 与 UPPAAL 的高铁跨界临时限速建模与验证[J].铁道标准设计,2016,60(10):126-131.
- [25] 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.
- [26] 李胜,王维.普速铁路 CTC 中心站集中控制技术的研究与应用[J].铁路通信信号,2021,57(12):12-15.
- [27] HORSTE M Z, SCHNIEDER E. Modeling train control system with petri nets-a functional reference-architecture[C]//Proceedings of the IEEE International Conference on System, Man and Cybernetics. [S.l.]:IEEE, 2000:884471.

Modeling and verification of high-speed railway train control temporary speed limit switching scenarios based on UML and UPPAAL

ZHOU Xiang

Binzhou Jiaotong Bureau, Binzhou 256600, China

Abstract: To improve the timeliness and safety of the information transmission process in the cross-border overlapping area between the temporary speed restriction server (TSRS) and the radio block center (RBC) for high-speed rail train control temporary speed restriction commands, a mathematical model of the TSRS switch and RBC switch cross-border overlapping area speed restriction process is established. Based on the characteristics of temporary speed restriction command interaction between the Chinese Train Control System (CTCS) CTCS-2/CTCS-3 high-speed rail train control systems, a combined approach of unified modeling language (UML) and Timed Automata model theory is adopted. The formal verification tool UPPAAL is used to identify deficiencies and vulnerabilities in the information transmission of temporary speed restriction commands in the cross-border overlapping area. The research results indicate that train control temporary speed restriction is an important component for the safe operation of high-speed rail. There is frequent information interaction between temporary speed restriction, centralized traffic control (CTC), RBC, train control center (TCC), and other related subsystems. The information transmission processes between different subsystems vary. The verification results of the Timer, Resend, TSRS, and RBC Timed Automata mathematical models show that the transmission time of TSRS switch and RBC switch information in the cross-border overlapping area is less than 3 s, and the information channel of the Timed Automata model does not lead to deadlock situations, significantly improving the timeliness and safety of high-speed rail train operation.

Keywords: temporary speed limit; timed automata; UML; UPPAAL; high-speed railway train control

(责任编辑:王惠)