软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2017,28(5):1183−1203 [doi: 10.13328/j.cnki.jos.005217]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于通信的列车控制系统可信构造:形式化方法综述*

陈铭松[1], 鲍勇翔[1], 孙海英[1], 缪炜恺[1], 陈小红[1], 周庭梁[2]

[1](上海市高可信重点实验室(华东师范大学),上海 200062)

[2](卡斯柯信号有限公司,上海 200071)

通讯作者: 陈小红, E-mail: xhchen@sei.ecnu.edu.cn

摘 要: 基于通信的列车控制系统(communication based train control system,简称 CBTC)已经成为世界范围内建造轨道交通信号系统的标准制式.CBTC 采用更加灵活和精确的列车控制,并提供连续的安全列车间隔保证和超速防护,在很大程度上提高了轨道交通运输的效率和安全性.尽管 CBTC 能够精确地实施实时控制,但由于 CBTC 涉及计算、通信与控制这 3 个方面的实时协同,系统设计与实现异常复杂.由设计缺陷而导致严重的灾难、事故和损失屡见不鲜.作为一个典型的安全攸关系统,如何保证 CBTC 的可信构造已成为领域研发人员关注的焦点与面临的最大挑战.鉴于在软硬件领域的成功经验,形式化方法目前已被公认为是保障 CBTC 可信性的一种有效方案.围绕 CBTC 的可信构造,从其生命周期的 3 个重要阶段,即系统需求分析、设计建模与底层实现入手,针对 CBTC 在可信方面的典型特征,梳理分析了 CBTC 系统在可信构造方面面临的挑战、国内外研究现状和发展趋势,全面介绍了形式化方法在 CBTC 可信构造中扮演的角色.

关键词: 基于通信的列车控制系统;安全攸关;可信构造;形式化方法

中图法分类号: TP311

中文引用格式: 陈铭松,鲍勇翔,孙海英,缪炜恺,陈小红,周庭梁.基于通信的列车控制系统可信构造:形式化方法综述.软件学报,2017,28(5):1183−1203. http://www.jos.org.cn/1000-9825/5217.htm

英文引用格式: Chen MS, Bao YX, Sun HY, Miao WK, Chen XH, Zhou TL. Survey on formal method of trustworthy construction for communication-based train control systems. Ruan Jian Xue Bao/Journal of Software, 2017,28(5):1183−1203 (in Chinese). http://www.jos.org.cn/1000-9825/5217.htm

Survey on Formal Method of Trustworthy Construction for Communication-Based Train Control Systems

CHEN Ming-Song[1], BAO Yong-Xiang[1], SUN Hai-Ying[1], MIAO Wei-Kai[1], CHEN Xiao-Hong[1], ZHOU Ting-Liang[2]

[1](Shanghai Key Laboratory of Trustworthy Computing (East China Normal University), Shanghai 200062, China)

[2](CASCO Signal Ltd., Shanghai 200071, China)

Abstract: Communication-based train control system (CBTC) has become the mainstream infrastructure for the railway signal systems around the world. Unlike traditional track circuit-based railway control systems, CBTC adopts a more flexible and accurate control mechanism to provide uninterrupted services to enable guarantee safeguard between adjacent trains and protection for over-speeding. Therefore, CBTC significantly improves the efficiency and safety of train-based transportation. Although CBTC can accurately conduct real-time control, its design and implementation are extremely complex due to the integration of heterogeneous computation,

* 基金项目: 国家自然科学基金(91418203, 61672230, 61402178); 上海市青年科技英才扬帆计划(14YF1404300)

Foundation item: National Natural Science Foundation of China (91418203, 61672230, 61402178); Yangfan Projet for Youth Scientist of Shanghai Science and Technology Committee (14YF1404300)

收稿时间: 2016-07-29; 修改时间: 2016-09-25; 采用时间: 2016-12-07; jos 在线出版时间: 2017-01-20

CNKI 网络优先出版: 2017-01-20 16:06:35, http://www.cnki.net/kcms/detail/11.2560.TP.20170120.1606.009.html

© 中国科学院软件研究所 http://www.jos.org.cn

communication and control components. Consequently, breakdowns caused by CBTC design flaws are inevitable. Therefore, how to guarantee the trustworthiness of CBTC, as for any typical safety-critical system, becomes a big challenge for researchers and practitioners. Due to the huge success in both hardware and software domains, formal methods are now considered as a promising means for trustworthy construction of CBTC systems. This article surveys the three most important stages during the trustworthy construction of CBTC systems, i.e., requirement analysis, design modeling, and bottom-level implementation. It not only comprehensively presents the important roles of the state-of-the-art formal methods and tools during the trustworthy CBTC construction, but also introduces the development trends as well as technical challenges for future CBTC.

Key words: communication-based train control system; safety-critical; trustworthy construction; formal method

基于通信的列车控制技术(communication based train control,简称 CBTC)已经成为我国轨道交通信号系统选型的主流制式[1].它打破了传统的基于轨道电路的铁路信号的固有限制,通过软件计算、网络通信和自动化控制三大技术的协同,提供更加灵活和精确的列车控制、连续的安全列车间隔保证和超速防护,使列车可以在更短的运行间隔追踪运行,极大地提高了轨道交通运输的效率和安全性.与其他制式的列车控制技术相比,由于追求更高精度的车辆控制和更密集的车辆运能投放,CBTC 控制的精准性需求更高、实时性更强、安全性需求更突出.此外,由车-地之间无线通信方式而引入的众多不确定因素,更加深了解决这些问题的难度.作为 CBTC 控制系统的核心组成部分,CBTC 控制软件的正确性、安全性和可靠性直接关系到整个系统的成败.因此,如何确保 CBTC 系统中各类控制软件的正确性和安全性,是当前 CBTC 领域科学研究和工程实践的重要问题.目前已有 EN50128、EN50129 等欧洲铁路控制与防护标准[2]规范轨道交通系统不同安全级别(SIL0~SIL4)的软件设计与测试.但是,由于 CBTC 涉及计算、通信与控制这 3 个方面的高频实时协作,其系统设计与实现异常复杂,因设计缺陷而导致严重的灾难、事故和损失屡见不鲜.例如,2011 年 9 月 27 日,上海地铁 10 号线由于新天地站设备故障,造成地铁追尾事故,导致 271 人受伤,其中约 20 人重伤.2014 年 5 月 2 日,韩国首尔地铁 2 号线由于自动安全距离保持装置出现故障,导致 170 余名乘客受伤.

为确保 CBTC 系统的安全性,CBTC 系统的研发必须采用可信构造技术.所谓可信构造技术,是指采用自身可证的全流程方法在系统开发过程中逐步形成系统的可信属性.对 CBTC 系统而言,主要的可信属性包括实时性、安全性和可靠性. EN50128,EN50129 等标准是目前 CBTC 研发企业用于确保其系统开发过程可信性的准绳.其本质是通过对 CBTC 研发过程各个阶段实施严格的过程控制和质量保证来规范系统的开发过程,从而保证系统的开发质量.这些标准通过推荐相关的方法,例如形式化建模和验证、系统的仿真和测试等来引导系统开发人员和评测人员实施可信保障的工程活动.但是这些标准只是一个框架,本身并没有给出保障 CBTC 可信性的系统化构造方法和技术.换言之,当前 CBTC 系统的开发过程仍然缺乏有科学理论为基础的系统化工程方法,进而导致 CBTC 系统的可信性特别是其软件可信性难以令人充分信赖,无论是学术界还是工业界,都迫切需要以可信理论为依据的系统化工程方法引导 CBTC 系统的可信构建.

形式化方法以严密的数学理论和相关推理为基础,通过保证各开发活动的一致性的精化关系达到构造可信系统的核心目标,是一种系统的开发方法.由于形式化方法本身是自证正确的,因此非常适合应用于苛求质量的 CBTC 系统的各种研发活动,也被业界视为最具有潜力和应用前景的可信构建方法[3,4].随着形式化技术的不断成熟和发展,越来越多的高安全等级信号系统设计已经在其相关的研发活动中开始采用形式化的方法与工具[5].EN50128 标准明确表示强烈推荐在信号系统设计与验证的过程中使用形式化方法与技术.对比最新颁布的航空航天安全规范标准 DO-178C 可以预见,在不久的将来,采用形式化方法的设计与验证将成为 CBTC 系统开发过程中不可或缺的一环.

但是,形式化方法在 CBTC 领域的应用仍存在诸多挑战.首先,形式化方法与当前软件工程特别是工业界开发流程的融合尚不成熟,缺乏系统化的以形式化理论为基础的工程方法.诸多传统的软件工程技术,例如需求模型的审查等,仍然没有被形式化理论所支持.而另一方面,形式化方法的数学基础要求较高,对于众多工程人员而言难以快速接受,企业面临较高的培训成本.其次,形式化方法在软件可信保障活动中,例如针对特定安全性质的形式化验证中展现了较大优势,但是对于大型复杂系统,特别是全系统级别的验证仍然面临状态爆炸等问

© 中国科学院软件研究所 http://www.jos.org.cn

题.再次,当前的形式化方法还处于各有所长阶段,众多方法和技术可能长于软件建模而短于验证或仿真,尚未出现覆盖软件全生命周期且能在工程应用中取得理想效果的方法,工具支撑亦不成熟完善.惟其如此,当前各种 CBTC 标准中也无法给出使用形式化方法的路线图.对于研究者和工业界的实践者来说,迫切需要一个与工程紧密结合、覆盖系统开发全生命周期、统一的形式化方法来引导 CBTC 系统的可信构造.

本文围绕 CBTC 的可信构造,从需求、设计和实现这 3 个核心开发阶段系统地调研了国内外各种 CBTC 构造方法和工具,并结合自身研究和工程实践经验,归纳并提出了以形式化方法为主要技术切入点的 CBTC 可信构造框架,如图 1 所示.在该可信构造框架中,基于系统功能特性与非功能特性(实时性和安全性)建立的原始需求是 CBTC 可信构造框架的初始输入源.研究 CBTC 构造过程的需求、设计和实现这 3 个阶段,每个阶段均提供相应的形式化方法与工具以确保各阶段内关键可信属性的达成以及阶段间输出产物的一致性.这些工具形成了支持 CBTC 系统可信构造的工具链,支持全生命周期内 CBTC 系统功能与非功能属性的建模与验证.

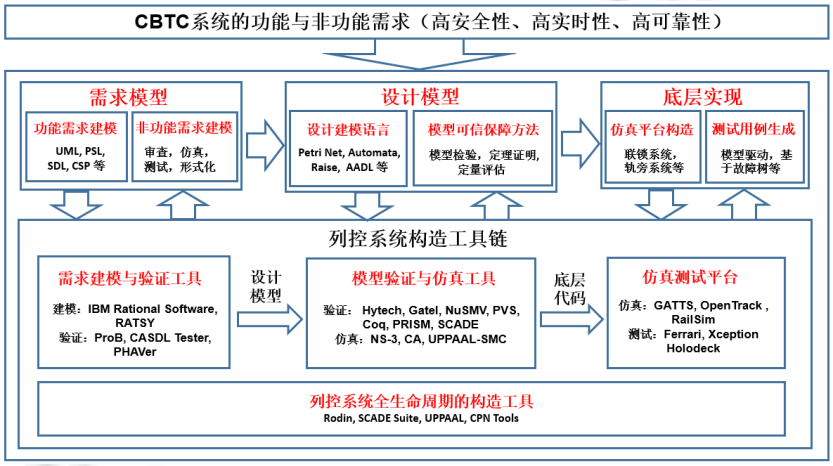

Fig.1 Trustworthy construction framework for CBTC based on formal methods

图 1 基于形式化方法的 CBTC 可信构造框架

本文第 1 节分析 CBTC 系统可信构造在需求、设计和实现层面上的困难与挑战.第 2 节说明 CBTC 系统需求可信建模技术及其验证方法和工具.第 3 节介绍 CBTC 系统设计层次的模型验证、评估方法和相关工具.第 4 节综述 CBTC 系统实现涉及的可信测试技术.第 5 节介绍支持多层次建模与验证的平台工具.第 6 节总结全文并指出未来的挑战.

1 CBTC 系统可信构造研究的挑战

CBTC 系统是基于通信的移动闭塞列车控制系统,支持自由无线、波导等多种方式的车-地无线传输方式.CBTC 通过轨旁和车载设备之间的实时大容量通信实现列车的动态定位和移动授权.作为典型的安全攸关系统,安全性、实时性、混成性、反应性是 CBTC 公认的关键系统属性,也是系统可信构造关注的焦点和难点.

典型的 CBTC 系统由联锁系统 CBI(computer based interlocking)、列车自动控制系统 ATC(automatic train control)、数据通信系统 DCS(data communication system)、列车自动监控系统 ATS(automatic train supervision)组成.CBI 负责管理轨旁设备、实现设备联锁;ATC 主要包括车载控制子系统 CC(carborne controller)和区域控制子系统 ZC(zone controller)两部分,CC 负责列车超速防护和定位,ZC 负责列车移动授权;ATS 主要为维护提供支持信息,监测各种设备的状态;DCS 为各子系统间的通信提供信息交互通道.这些子系统既独立又相互依存,导致 CBTC 系统结构异常庞杂,增加了系统可信构造的难度.除此之外,由于 CBTC 系统运行在开放的物理环境下,运行过程中存在着诸多不确定因素,极易导致安全事故,因此需要在设计阶段充分评估这些因素产生的影

© 中国科学院软件研究所 http://www.jos.org.cn

响.对这些不确定性的处理,再次加剧了 CBTC 可信构造的难度.

面对复杂的异构子系统及其特有的复杂运行环境,CBTC 系统在可信构造的需求、设计和实现阶段存在着以下几个方面的挑战.

1) 需求阶段

随着多核处理器和无线网络在 CBTC 中的应用,频繁的网络交互与信息处理引入了大量并发性与不确定性,系统性能难以评估,这给 CBTC 的需求实施带来了困难.其主要问题有:

(1) 缺乏建立于功能需求之上非功能需求的获取、建模与验证的方法,无法系统地从功能需求中获取安全性需求和实时性需求等非功能需求;

(2) 缺乏支持复杂环境下功能需求建模、仿真与验证的方法与工具;

(3) 缺乏非功能需求,尤其是安全性需求与实时性需求的统一建模框架,难以权衡非功能需求间的冲突,做出合理的需求决策.

2) 设计阶段

CBTC 设计涉及到多种异构的计算部件与物理部件.由于这些部件的行为存在巨大的差异使得 CBTC 的设计异常复杂.CBTC 系统在设计阶段主要存在以下挑战:

(1) 缺乏不确定性建模与分析手段,难以评估不确定性对系统功能与性能的影响;

(2) 缺乏统一开发框架支持异构部件的协同建模、仿真与验证,设计出来的系统很难满足功能与非功能的需求;

(3) 形式化验证可扩展性低,由于 CBTC 系统部件既具有离散的属性又具有连续的属性,在协同验证时极易出现“状态空间爆炸”,难以获得验证结果.

3) 实现阶段

鉴于 CBTC 底层实现的复杂度,对其实施严格的形式化证明或验证代价巨大,因此通常采用半形式化的测试方法来确认实现是否满足需求以及是否存在错误.作为苛求安全的复杂硬实时系统,目前 CBTC 底层实现的可信保障主要围绕测试生成展开,其主要问题有:

(1) 测试序列的实时性问题,即在测试序列生成过程中如何构造精确的输入发生时间点和相应的输出时限;

(2) 同步测试问题,即如何检测各部件间采用的同步策略是否符合期望的需求;

(3) 测试用例的揭错能力问题,即需要建立测试用例与系统安全属性之间的关系,以提高测试的揭错能力,而不只是单纯地以代码覆盖率为测试准则.

4) 各构造阶段的一致性保障

CBTC 系统从需求分析到底层实现需要经历多个阶段,不同阶段在建模、分析、验证等方面采用的方法迥异.由于缺乏自动化的精化方法与工具,不同阶段之间的构造过程相互独立.这不仅使得系统构造总体时间大为增加,而且人工的干预极易导致不同构造阶段结果间的功能与非功能属性的不一致.因此,如何实现不同层次间模型的自动精化以及验证结果重用,确保需求、设计以及底层实现的一致性已成为 CBTC 可信构造的挑战之一.

2 CBTC 系统需求规约可信建模和验证

一个可信的 CBTC 系统开发过程在早期阶段,系统部署或实现之前,就必须通过特定的构造过程,获取软件需求规约,确定其安全性需求与实时性需求等非功能需求,并以此为依据构造该系统.CBTC 的需求规约构造包括两部分:需求建模与需求的可信保障.

2.1 需求建模

2.1.1 CBTC 系统功能需求建模

列控制系统的功能需求一般包括列车注册与注销、等级转换、行车许可、调车、紧急情况处理、临时限速、RBC 切换等功能.学术界和工业界在长期研究与实践中提出了各种功能需求的构建方法.与这些建模方法

© 中国科学院软件研究所 http://www.jos.org.cn

相匹配的建模语言也应运而生.目前 CBTC 软件需求建模方法主要包括:基于统一建模语言(unified modeling language,简称 UML)的方法、基于属性描述语言(property specification language,简称 PSL)[6]的方法、基于规约描述语言(specification description language,简称 SDL)的方法,以及基于逻辑与进程代数的方法.

基于统一建模语言的方法.UML 对系统提供可视化描述,是一种半形式化的方法.由于 UML 有统一的规范,因此常被用作列控系统的基本需求建模语言.常用的模型有用例模型、状态图、顺序图和类图.这些模型可以单独使用,也可以组合使用.例如,文献[7]基于顺序图对建立列控系统等级转换过程中消息的交互行为进行建模,利用 UML 状态图对等级转换的所有错误状态以及这些状态之间的转移进行建模,以描述导致系统转换失败的各种情况.文献[8]采用状态图对列控系统中的模式转化进行建模,给出了列控系统的车载设备在不同工作环境中的工作模式转化,另外,它还使用类图描述了模式转换中涉及到的实体类.文献[9]基于顺序图对列控系统场景中轨旁子系统和车载子系统消息交换建模,并利用状态图描述移动需求授权管理.

此外,由于列控系统需求规范的复杂性和实时性等,在利用 UML 进行规范建模时,有些工作进行了扩展.诸如文献[10]为了得到可执行的规约,用动作规约语言对 UML 进行了扩充,加强了可执行语义,增加了时间约束、外部信息、内部信息,从而建立了列控系统需求规范的可执行模型.

基于属性描述语言的方法.PSL 作为一种形式化的属性规范语言,具有易于读写、语法精简、语义严格清晰等优点.基于 PSL 的模型可以直接运用 RATSY(requirements analysis tool with synthesis)[11]仿真,因此避免了复杂转换过程.一般来说,利用 PSL 对列控系统建模包括 3 个产物[12−14]:形式化的需求模型,用于描述列控系统行为和环境行为;断言属性集,用来描述的列控系统行为必须满足的属性;允许属性集,用来描述列控系统行为中允许的属性.例如,文献[12,13]以无线闭塞中心切换场景为例说明基于属性的需求分析方法在列控领域中的应用,其断言属性集包括如列车不能同时发送行车许可和接收行车许可等属性,其允许属性集包括允许车载设备与 RBC 通信中断的时间为 7s~20s,若超过这段时间则降级处理等属性.文献[14]基于 PSL 对车载设备的模式转换建模,构建了列控行为,诸如当停车时处于哪种模式、当移动授权拒绝时应该启用哪种模式等行为,以及允许属性集,包括当处于初始状态时,车载设备可以处于哪种状态等.

基于规约描述语言的方法.SDL 是一种为了构建实时响应的、事件驱动的系统而设计的语言,具有严谨性、清晰性、一致性、可移植性以及可扩展性等特点.在列控系统的需求建模中,SDL 支持自顶向下的系统功能行为建模[15,16].文献[16]基于 SDL 对车载设备的功能需求进行建模,从系统级定义了车载设备的功能接口和数据交换格式,从模块级描述了模块功能的交互场景和数据流,在底层对详细的车载设备功能建模.

此外,还有一些工作扩展 SDL.例如,文献[17]提出了一种 SDL 的扩展语言 ScOLA(scenario oriented molding language).这种语言可以让工程师们以类似自然语言的方式定义形式化的系统,它以列车车门管理场景为例进行了功能建模,并验证了其安全性.

基于逻辑的方法.基于逻辑的方法一般是基于集合论与一阶逻辑,采用逻辑推理或者定理证明的方式实现系统的功能精化与正确性证明.这类方法的代表有 Z[18]、B 方法[19]和 Event B[20]等.其中 Z 可以对系统中的数据和操作建模.B 方法与 Event B 可以实现对需求规约的精化.例如,文献[19]采用 B 方法对轨旁子系统的数据进行确认的过程进行了建模,并纠正了规约中的一些错误.文献[18]使用 Z 对系统需求中的复杂数据类型进行建模,给出了欧洲列控系统的无线闭塞中心的描述.

基于进程代数的方法.基于进程代数的方法关注并发行为,强调对不同模块并发过程之间的交互进行建模.这类方法的代表工作主要是通信系统演算(a calculus of communicating systems,简称 CCS)[21]和通信顺序进程(communication sequential processes,简称 CSP)[22].其中,CSP 进程是图灵奖获得者 Hoare 于 1978 年建立的一种适合于分布式并发软件规格和设计的形式化方法.在轨道交通需求阶段,该类方法主要用于形式化地描述与验证可控系统的并发性与不确定行为.例如,文献[18]利用 CSP 对系统进程的控制流建模,主要包括两个并发的进程:列车运行控制进程和紧急信息处理的控制进程.

此外,为了增加其他能力,例如,为了处理混成性,一些工作提出了基于进程代数方法的混成扩展,并将其应用到列控系统中.例如,Zou 等人[23]调研了如何对中国列车控制系统级别 3(Chinese train control system 3,简称

© 中国科学院软件研究所 http://www.jos.org.cn

CTCS-3)的系统需求规约进行形式化的描述与验证,所提出的方法采用了混成CSP(hybrid CSP,简称HCSP)对列车预期行为的每一个基本操作场景进行建模.例如,对移动授权场景建模了无线闭塞中心和列控系统的并发行为,对模式转换中能否转换成功的不确定性建模等.

2.1.2 CBTC系统非功能需求建模

作为典型的实时安全攸关系统,非功能需求在CBTC系统的构造中扮演着重要的角色[24].在CBTC需求建模过程中,与可信相关的重要的非功能需求主要包括安全性需求和实时性需求.

安全性需求是列控系统最重要的非功能需求.在CBTC需求建模阶段,安全性需求一般采用基于时序逻辑的方法描述[9,25].例如,文献[9]采用CNL(controlled natural language)语言描述列控系统的安全性,CNL语言集成了LTL(linear temporal logic)、正则表达式、一阶逻辑和混成等建模元素,可以全面地对CBTC系统进行安全建模.例如,为了表达“任意两辆列车不能同时出现在同一列轨位置”,我们可以采用CNL公式“for all Train t1,t2, such that t1 !=t2 then never(t1.position=t2.position)”来描述这一安全需求.此外,文献[25]在深入研究高速列控系统行为时序规律的基础上,扩展了LTL的语法与语义,定义了控制行为时序逻辑(control action temporal logic,简称CATL),并提出和证明了CATL逻辑的约简法则,将其引入基于系统理论的危险分析过程中.该工作被成功地应用于中国列车运行控制系统3级的安全需求建模,为系统需求规范的完善提供了依据.

实时性是指时间约束.实时性需求一般分为两种:一种是定性约束,描述事件之间的序关系,例如列车门必须在列车开启之前关闭;另一种是定量约束,例如CBTC中的列车与列车,列车与RBC间的通信都必须要在5ms内完成[26].对于实时性需求的建模一般都是在其他功能需求模型基础上的扩展.例如,对UML的扩展实时嵌入式系统的建模和分析(modeling and analysis of real-time embedded systems,简称MARTE)[27],CSP的实时扩展Timed CSP.另外,比较经典的还有Alur和Dill提出的时间自动机(timed automata,简称TA)[28],它在有限状态自动机的基础上增加了取实数值的时钟变量以刻画连续变化的时间,可以准确地表示实时系统的各种带时间约束的行为.由周巢尘院士等人提出的时段演算(duration calculus)[29],能够应用于对混合系统的实时性需求进行刻画和精化,用来计算关于系统需求的满足概率.另外,还有基于时态逻辑的描述(LTL,CTL)及其扩展(TCTL,RTTL)等等.

2.1.3 需求建模方法比较及支持工具

在上述调研中,发现很多非功能需求的建模是对功能需求模型进一步扩展的结果,例如,CSP针对实时性需求的扩展Timed CSP.总结上述CBTC的需求模型构建,我们分别将这些方法的建模能力、优点及其建模工具进行了整理与比较,得到表1.其中,建模能力分别从系统的功能、安全性和实时性需求等方面进行描述.在工具支持上,由于建模工具只需提供对模型的编辑能力,一种模型可能有多种建模工具支持.例如,支持UML的建模工具多达40多种[30].本文只列举应用比较广泛的建模工具.

从表1中可以看出,基于UML,PSL和SDL的方法侧重对需求功能的建模,但也可以通过扩展的方式增加非功能建模的能力.基于逻辑和进程代数的方法由于形式化程度较高,能够比较全面地对需求建模.但不难看出,目前还不存在一个统一的框架,支持对功能需求、安全性需求与实时性需求的统一建模,因此,对这些非功能需求的冲突检测、评估与权衡也很难展开.

Table 1 Comparison of requirement modeling methods and supporting tools

表1 需求建模方法比较与支持工具

需求建模方法	功能需求	安全性需求	实时性需求	优点	建模工具
基于UML的方法	√	×	√	图形化,直观	Rational Rose[31] PowerDesigner[32]
基于PSL的方法	√	√	×	可直接被仿真,使用方便	RATSY[11]
基于SDL的方法	√	×	×	支持自顶向下的系统行为建模	PragmaDev Studio[33] Rational SDL Suite[34]
基于逻辑的方法	√	√	√	通过逻辑推理实现系统的功能精化与正确性证明	OVADO[19]
基于进程代数的方法	√	√	√	支持描述并发行为	PAT[35]

© 中国科学院软件研究所 http://www.jos.org.cn

2.2 需求可信保障方法

由于 CBTC 系统的复杂性、实时性以及极高的安全性要求,仅依靠经验制定的系统需求规范不可避免地存在某些漏洞或者安全隐患.因此十分有必要对列控系统需求模型进行验证.通常在需求验证阶段,人们关注需求模型的正确性、安全性、完整性和可靠性.系统需求规范的可靠性和安全性常见验证方法有审查、仿真、测试和形式化验证.其中,审查是一种传统的需求模型检查方法.该方法因其简单、易于执行,在工业界得到了广泛应用,其主要方法是组织需求分析人员,对需求模型中的内容逐条进行解读阐释以确定需求描述是否正确地反映了用户需求[36],或者是将自然语言描述的需求转化成某一特定模型,再根据模型的审查标准审查[37,38].仿真一般通过模型检测和规约执行来实现.测试主要采用将需求模型视为可执行对象的方案,测试者从该系统应满足的场景产生测试数据,用以测试需求模型,并根据实际测试结果和预期输出的一致性比对来判定需求模型是否正确地刻画了用户的需求.类似地,测试者也可以观察需求模型是否满足安全性等性质.形式化的验证方法主要采用模型检测和定理证明对模型进行自动验证.表 2 归纳了当前在列控领域较为主流的需求模型可信保障方法.从中可以看出,形式化方法可靠性最高,但是方法最复杂.而基于审查的方法其可靠性主要依赖于审查者的经验,可信保障程度最低.需求仿真和测试这两种方法的可靠性处于两者之间.因此,在列控系统的需求分析时,对于安全等级较低的模块或子系统通常采用审查、测试的方法,而对于安全等级较高的模块或子系统,建议采用形式化方法.

Table 2 Comparison of trustworthiness guarantee methods for CBTC requirements

表 2 CBTC 需求可信保障方法比较

需求可信保障方法	优点	适用系统规模	缺点	对应建模方法	工具	可信保障程度
审查	易于执行	各种规模均适用	依赖于审查者经验,自动化程度低	自然语言等	IBM Requisite Pro[39]	低
仿真	可以直观地观察系统运行过程	各种规模均适用	仿真耗时长	基于属性描述语言等	ProB[40], UPPAAL[41]	中
测试	工程化程度高	各种规模均适用	无法发现所有错误	基于 UML 等	CASDL Tester[42]	中
形式化方法	自动化程度高,验证结果完备	小规模	需要专业知识,状态空间爆炸	基于逻辑公式、自动机等	PHAVer[43], ARMC[44,45]	高

目前形式化方法已广泛应用于 CBTC 需求的验证,主要用于检验其安全性、正确性等.例如,文献[25]对需求阶段的高速列控系统安全分析问题,提出基于 STPA(system-theory process analysis)的高速列控系统安全分析方法.文中建立形式化的状态迁移模型,并使用形式化工具 PHAVer(polyhedral hybrid automaton verifier)[43]来实施模型检测.此外,在进行验证分析的同时,还对系统建立了故障模型,将故障行为建立在系统的正常行为模型之上,利用模型检测技术进行安全分析.文献[46]通过相位事件自动机(phase event automata,简称 PEA)将 CSP-OZ-DC 所建立的模型转换变迁约束系统(transition constraint system,简称 TCS),然后通过模型检测器 ARMC[44,45]自动验证.文献[23]通过逻辑推理证明验证给定的 HCSP 模型是否满足指定的属性.

需要指出的是,虽然形式化方法能够有效地避免需求描述的二义性,支持需求模型验证以检验需求模型逻辑的正确性,但是目前已有的方法还不能保证所获得的需求模型能够真实并完整地体现用户的意图.此外,现有的形式化需求建模方法与技术并没有充分考虑到外部不确定环境的作用,因此通过这些方法获得的需求模型并不能保证最终实现的 CBTC 系统在真实的复杂轨道交通运行环境下满足用户真实的需求.作为一个典型的异构并发系统,CBTC 的需求模型极为复杂,在采用形式化的模型检验或定理证明时极易出现“状态空间爆炸”的问题.虽然目前通过多种方法(例如,抽象解释、无关状态空间约减等)能够降低需求模型的验证代价,但是目前此类方法对于处理较大规模的复杂系统还是效果欠佳.

3 CBTC 系统设计的形式化建模及验证

在理想状态下,需求模型应能自动化地转换为底层实现.但由于目前从需求层次到实现层次的综合过程自

© 中国科学院软件研究所 http://www.jos.org.cn

动化程度较低,需求层次的描述很难直接转化为底层的实现(例如 Esterel[47]与 Simulink[48]),因此在工程上,需求模型通常要进一步转化为设计模型.而当前这种转换主要还是人工实现.随着 CBTC 系统的复杂度越来越高,运行环境不确定,人工设计极易出现设计层次的模型的错误.为了保证设计模型的正确性与可靠性,需要对 CBTC 设计模型进行充分的验证与评估,以保障其可信性[4].

3.1 CBTC系统设计的形式化建模

一般来说,设计模型应该包括结构与行为两部分.结构模型为静态模型,主要描述系统的模块组成关系;而行为模型为动态模型,主要描述系统的运行行为.

3.1.1 CBTC 系统设计的结构建模

在列控系统设计过程中,结构模型主要用来描述系统的结构组成.结构模型不仅可以支持高层的体系架构描述,也可以支持低层的软硬件部件描述.目前,列控系统设计的结构模型主要有基于 AADL 的架构建模和基于 UML 的结构建模.

基于 AADL(architecture analysis & design language)的架构建模.AADL 是一种体系结构描述语言[49].它是由美国汽车工程师学会提出的建模标准.相对于其他建模方法,AADL 特别适用于对嵌入式实时系统的软件和硬件结构建模和分析.AADL 拥有开源工具平台 OSATE[50],可用于列控系统的架构建模.例如,文献[51]基于 OSATE 对 ATC 建模和分析,给出了列车自动防保系统 ATP(automatic train protection)、列车自动驾驶系统 ATO (automatic train operation)和列车自动监控系统 ATS(automatic train supervision)的 AADL 模型.文献[52]利用 AADL 对 CTCS-3 中的移动授权场景中系统结构建模,结构中包含无线闭塞中心、列车和列车控制器等.另外,AADL 提供的附件(annex)建模扩展机制在 CBTC 的结构设计中也有很多应用,例如,在文献[51]利用数据建模附件对自动列车控制系统中的复杂数据类型建模,文献[52]利用行为附件对列控中的控制器行为建模,利用混成附件对列车内的连续实体建模.

基于 UML 的结构建模.UML 及其变种(例如 SysML)被广泛应用于软硬件的设计建模.UML 由多种类型的图组成,它既包含结构图(例如类图与包图),又包括行为图(例如活动图与顺序图).在结构图中,包图用于组织层次结构,可用于架构设计,类图用于定义组成实体,这两种图被广泛应用.例如,文献[53]利用 UML 类图从静态的角度对 ATP 进行了结构描述.文献[54]对区域控制器以及区域控制器的主要功能-移动授权计算建立了 UML 类图,建立了区域控制器内部功能的静态关系.这些工作都展现了 UML 在列控系统领域对系统结构建模方面取得的良好效果.

3.1.2 CBTC 系统设计的行为建模

由于结构建模只是静态模型,不能描述系统(组件)的交互和协同等行为,因此,需要适当的方法对列控系统的行为建模.目前常用的列控系统行为建模的方法主要有以下几类.

基于 UML 的方法.使用 UML 模型进行行为建模主要使用交互图(包括顺序图与协作图)、状态图、活动图.例如,在文献[53]中,利用 UML 顺序图描述了自动列车保护系统场景,从动态的角度对系统交互进行描述.文献[54]分别使用了用例图、顺序图和活动图对区域控制子系统以及其中的列车管理功能、区域切换功能建模设计,完整地设计了区域控制器应用软件的形式化模型.

基于自动机的方法.自动机是有限状态机(finite state machine,简称 FSM)的数学模型,适用于对列控系统中的不同层次的系统行为进行建模.为了应对 CBTC 的某些特征,学术界研究者常常使用扩展的自动机对 CBTC 设计建模,例如,为了建模混成性使用的混成自动机[55].文献[56]利用混成自动机对 CBTC 中的移动授权场景建模.为了应对高实时性,使用时间自动机进行建模.例如,文献[57]建立了 ZC 的时间自动机模型,并应用其验证工具 UPPAAL 对 CBTC 区域控制子系统的功能和性能要求进行验证,从而保证了系统模型的安全性和受限活性.此外,基于自动机的建模可以被直接仿真,因此可以直观地观察系统的运行状态.目前工业界主流的列控系统建模工具 SCADE[47,58],Simulink[48],UPPAAL[41],其底层核心计算模型采用的都是自动机或其变种.

基于 Petri 网的建模方法.Petri 网是 1962 年德国学者 Petri 在其博士学位论文中提出的描述事件和条件关系的网络,适合于描述异步的、并发的计算机系统模型.因此,Petri 网常被用作对列控系统中的并发行为进行建

© 中国科学院软件研究所 http://www.jos.org.cn

模.例如,文献[59]利用 Petri 网对列车调度操作建模,以确保这些列车可以准时到站并且不会相撞.文献[60]利用 Petri 网开发了联锁和信号系统,并对其进行了安全验证.文献[61]利用 Petri 网对列车在相邻的 RBC 区域间切换的模型进行建模.此外,针对列控系统的特性,很多工作还应用 Petri 网的变种建模系统行为.例如,文献[62]采用扩展的 Petri 网——Open 网去建模系统列车控制中不同组件之间的协同性.它通过 Open 网来验证系统组件之间的交互性.文献[63]利用高阶 Petri 网对列控系统中的安全攸关场景建模,例如安全监管程序、联锁系统,特别是包括人员因素对系统的影响.

为了提高对系统的并发性建模能力,丹麦 Aarhus 大学的 Jensen 提出了有色 Petri 网(colored Petri net,简称 CPN)[64].CPN 除了支持带颜色(不同颜色代表不同值)的标记之外还支持带约束的状态弧,因此能够描述比传统 Petri 网更复杂的行为.CPN 已被广泛地应用于列控系统设计的行为建模.例如,文献[65]采用 CPN 对欧洲列车控制系统进行了功能方面的形式化描述.其描述的 CPN 模型包含 3 个子模型:环境模型、车载系统与轨旁系统.实验结果显示,基于 CPN 的方法支持从顶层需求到底层实现的逐步精化.文献[66]利用 CPN 对 CTCS-3 整体建模,包括混线模式下 CTCS-3 和 CTCS-2 间转换建模,为 CTCS-3 系统的设计及联调联试提供形式化依据.文献[67]分析了基于无线通信的 CTCS-4 级列控系统的构成及功能、移动闭塞系统列车最小追踪间隔原理以及应用 Petri 网对系统建模的建模理念,为建立高速列车追踪过程的 CPN 模型提供了理论基础.它应用 CPN 工具对高速铁路列车追踪过程进行建模,对后行列车车载 ATP 以及 ATO 设备进行详细描述,体现了移动闭塞下列车实时调整加速度的特点.为了降低轨道交通联锁系统的建模复杂度,文献[68]基于层次有色 Petri 网(hierarchical CPN,简称 HCPN)对法国铁路联锁系统及其信号控制系统进行了分层次建模.

应用随机 Petri 网(SPN)支持对系统中的不确定性进行建模.SPN 在基本 Petri 网中引入了时间参数,赋予每个变迁一个随机延迟时间.文献[69]建立了 ETCS-2 和 ETCS-3 级的 GSM-R(GSM for railway)无线通信系统的信道 SPN 模型.该模型分析了火车和无线闭塞中心传输的位置和移动授权数据丢失情况.性能评估结果展示了数据传输延迟和丢失对列控系统可信操作有很大的影响.

基于马尔可夫决策过程的建模方法.马尔可夫决策过程(Markov decision processes,简称 MDP)是指决策者周期地或连续地观察具有马尔可夫性的随机动态系统,根据新观察到的状态,再做新的决策,依此反复进行.基于 MDP 的建模可以实现物理行为、正常行为和故障行为的并发建模,这是 Petri 网、自动机等其他行为模型所不具备的优势.由于列控系统某一时刻系统行为概率分布并不依赖于之前的历史状态而只与当前状态有关,这种行为符合马尔可夫的无记忆性,因此非常适合采用 MDP 进行建模.例如,文献[70]通过 Markov 决策过程方法建立列车通过区间场景的综合行为模型(comprehensive behavior model,简称 CBM),准确地描述了区段占用设备状态和逻辑状态的判决关系,并验证了 CBM 模型的完整性和安全性,最后通过定量计算危险失效概率证明了设计的危险风险在可接受范围之内.文献[71]为了对列控系统进行量化分析,利用马尔可夫决策过程建立了物理世界的不确定行为模型、正常行为模型和错误行为模型.通过量化分析,可以从设计角度降低错误发生的概率.

基于 RAISE 的建模方法.RAISE 建模方法支持从最初的抽象规约描述到设计层次建模[72].它提供了一套工具,支持基于 RSL(RAISE specification language)的软件建模和开发.RAISE 方法在列控系统中应用有较多的优点,例如,RAISE 方法能够对正在运行的多个任务进行描述,很好地支持并发和分布式的特性的建模.同时,RAISE 引入了安全约束的 RSL 描述以及若干个列控系统的 RSL 公理模型,支持对典型的列控系统进行安全性验证[73].为了描述实时性,Timed RAISE 在 RAISE 语言上加入了时间因子.文献[74]利用 Timed RAISE 对 CTCS-3 级列控系统规范中的 RBC 切换协议进行建模,对系统模型的正确性和实时性进行验证.

3.1.3 CBTC 系统设计建模方法比较与工具支持

表 3 总结了列控领域的设计模型、方法和语言,归纳其支持的建模特性、优点及建模工具.从表 3 中可以看出,随着 CBTC 系统日趋精密复杂,所有的这些方法为了能够描述更多的系统结构和行为性质,都经过了不同程度的扩展以应对现实需要.同时,我们也应注意到,当前任一列控系统建模方法皆有所长,亦有所短,因此使用单一建模语言/模型几乎不可能达到理想效果,必须将多种建模方法和语言进行有机地结合才能应对日趋复杂

© 中国科学院软件研究所 http://www.jos.org.cn

的CBTC系统.因此,如何构建系统的科学方法,将当前主流的建模手段进行有效地统一并引导工程实践,是一个值得深究的问题.

Table 3 Comparison of modeling methods and supporting tools in design phase

表 3 设计阶段建模方法比较与工具支持

模型/语言/方法	实时性建模	并发性建模	不确定环境建模	混成性建模	优点	建模工具
基于自动机的方法	√	√	√	√	图形化,支持仿真	UPPAAL[41],Simulink[48]
基于 Petri Net 的方法	√	√	√	×	很强的并发建模能力	CPN Tools[64]
基于 AADL 的方法	×	×	×	√	支持层次化建模	OSATE[50]
马尔可夫过程	×	√	√	×	支持并发建模	Matlab,PLASMA[75]
基于 RAISE 方法	√	√	×	×	支持从需求到设计的精化	Eden[72],rsltc[72]
基于 UML 的方法	√	√	×	√	图形化,应用广泛	Rational Software[31]

3.2 设计层次的可信保障

设计模型在 CBTC 的可信构造过程中起着承上启下的作用,它既要能够描述系统的行为又要作为“黄金参考模型”支持底层实现的产生,因此其正确性与可靠性是CBTC系统可信构造的关键,在功能与非功能方面需要进行充分的验证与评估,即设计模型需要满足顶层需求分析所获取的结果.为了保障 CBTC 设计模型的可信,目前通常采用的方法主要分为仿真确认、形式化验证与定量分析这三大类方法.表 4 给出了这些方法的比较.

Table 4 Comparison of trustworthiness guarantee methods for design models

表 4 设计模型的可信保障方法比较

类别	可验证的性质类型	手段	形式化程度	保障手段	模型表达能力	自动化程度	状态空间爆炸	常用工具
仿真确认	可靠性,安全性,实时性	仿真	低	建模+执行	强	高	无	UPPAAL, Simulink, Modelica[76], SCADE[58]
形式化验证	安全性,实时性	模型检验	高	建模+验证	弱	高	存在	CPN, UPPAAL, CHARON[77], NuSMV[78], SCADE
		定理证明	高	建模+证明	强	低	存在	Coq[79], Rodin[80]
定量分析	可靠性,实时性	概率模型检验	高	建模+验证	弱	高	存在	PRISM[81]
		统计模型检验	中	建模+执行	强	高	无	UPPAAL-SMC[41], PLASMA

3.2.1 3.2.1 基于仿真确认的方法

与测试类似,在设计模型完成时,对于可执行模型,设计人员需要通过仿真的手段来执行该模型,以确认该模型是否满足需求.一般来说,列控系统的仿真工具主要包含两种类型:基于事件的仿真工具和基于时间的仿真工具[82].作为一个典型的反应式嵌入式系统,在CBTC软硬件设计时需要对系统内外部事件及其时序建模,这时通常采用基于事件的方法,例如着色 Petri 网 CPN.同时,作为一个实时系统,是否能够在规定的截止时间之前完成相应的操作,也是系统所需要确认的一个关键非功能属性,对于这类问题,在仿真过程中还需要考虑时间方面的仿真.例如,基于时间自动机的方法.通常,支持时间的仿真需要较长的仿真时间.而基于事件的仿真工具比较节省计算时间,但是准确度也有所降低.

3.2.2 3.2.2 基于形式化验证的方法

作为轨道交通 EN 标准(EN50129,EN50128)强烈推荐采用的技术,形式化验证已经逐渐被越来越多的轨道交通系统生产厂商所采用.目前来说,在轨道交通领域主要采用两种形式化验证技术,即模型检验与定理证明.模型检验已被广泛地应用于设计模型的自动化验证.对于一个采用形式化语言描述的设计模型以及用户给定的设计属性,模型检验方法通过遍历检查所有状态空间来自动化地验证该模型是否满足给定的属性.在 CBTC 系统中,模型检验技术被广泛应用于联锁系统的验证,因为联锁系统的安全属性可以直接使用时序逻辑描述,并且联锁说明所依靠的控制表可以直接被转化为模型检验的形式化输入.此外,模型检验还被用于 RBC 子系统的安全性验证.例如,在 Ansaldo STS 项目中,模型检验技术被用于对 ETCS 系统中的 RBC 子系统进行验证[83].文献

© 中国科学院软件研究所 http://www.jos.org.cn

[84]通过对列控系统中的安全速度和加速限制进行形式化建模,并通过 NuSMV 对模型属性的正确性进行建模.此外,在线模型检验技术也被用于保证 CBTC 系统实时控制参数的正确性[56].同时,多种形式化模型(例如混成自动机、时间自动机、CPN)支持 CBTC 的设计建模,通过采用已有的模型检验工具(例如 UPPAAL,HyTech[43],CHARON 等),可以实施对 CBTC 系统模型的安全性和活性的验证[56,57].模型检验虽然自动化程度较高,但是由于需要访问所有状态空间,在验证复杂 CBTC 设计时,模型检验方法很容易引起“状态空间爆炸”问题,需要的验证时间极长.例如,目前国内信号厂商使用较多的是 SCADE 平台,采用 SCADE 内嵌的证明器可以完成对布尔运算模型、有限状态机模型的形式化证明.但是由于“状态空间爆炸”的问题,目前 SCADE 数据流模型证明器无法对复杂模型实施验证.为此,文献[85]采用切片技术针对复杂 SCADE 区域控制器模型进行了处理,能够有效降低 SCADE 模型的验证时间.该切片方法能够有效降低状态搜索空间,使传统方法不能验证的问题变为可能.

除模型检验外,定理证明也被应用在 CBTC 系统的分析与验证上,CMU 的 André Platzer 系统地提出了针对混合系统验证的差分动态逻辑与差分不变式,并开发了定理证明器 KeYmaera[86].该工具已被成功地运用在轨道交通系统领域的模型与协议的形式化证明.中国科学院软件研究所詹乃军等人研究了如何将 Simulink 模型转化为 HCSP 模型,并提出利用混成霍尔逻辑来对 HCSP 模型进行验证,相关工作已被成功运用于高铁 3 级控制系统(CTCS-3)的验证上[87].

3.2.3 3.2.3 基于定量评估的方法

作为一般原则,铁路安全最终是以牺牲可用性来实现的,强制让列车停止是实现安全的基本方式.开放环境下轨道交通控制系统在运行过程中存在多种类型的不确定因素,以上的措施很容易降低铁路设施可用性和服务质量.为了保证 CBTC 系统的非功能属性得到满足,且最大程度地利用铁路设施,设计时需要对预期故障场景以及非功能属性(例如可用性、实时性等)进行定量评估.例如,文献[88]利用贝叶斯网络对列控系统建模,利用贝叶斯学习算法对列控系统进行了量化分析.基于随机概率与统计的方法是目前面向 CBTC 模型定量评估的有效方法[46,89,90].例如,文献[89]采用随机回报网模型(stochastic reward net,简称 SRN)对数据通信系统进行建模,支持对不同配置情况下的系统进行定量的评估与比较.与形式化模型检验不同,统计模型检验(statistical model checking,简称 SMC)[91,92]采用的假设检验的方法对系统模拟路径的样本空间进行统计分析,评估系统满足属性约束的概率区间.统计模型检验技术支持定量分析、评估与优化控制策略的性能,有效提高模型验证的效率[93].例如,针对 CBTC 系统中存在不确定性,文献[94]创新地提出了不确定时间活动图.该模型支持针对活动图活动执行时间不确定性的建模与分析.该方法被成功地应用于 CBTC 自动控制子系统建模.通过将不确定时间活动图建模结果自动转化为 UPPAAL-SMC[41],该方法支持不确定环境下自动控制系统完成时间的定量分析.由于统计模型检验基于仿真与数学统计方法,与传统形式化模型检验相比需要较小的内存与执行时间,不会出现“状态空间爆炸”问题,因此非常适用于对复杂的系统进行定量评估.可以预见,SMC 将为解决 CTBC 模型的非功能属性评估提供一种可行的、具有创新性的解决方案.

4 列控系统实现的测试

来自包括轨道交通等各安全攸关领域的相关数据表明,导致灾难性事故的原因通常是在系统运行上下文中产生了引起子系统失效,继而导致灾难性事故发生的场景[95−98].因此,在目前相关理论和技术尚不完备的背景下,面对规模庞大、逻辑复杂的 CBTC 系统,仅通过单一的形式化验证等静态推理方法并不能足以保证系统最终运行时的正确性.与形式化验证不同的是,仿真测试是面向系统上下文运行环境的动态验证方法,能够针对系统实现进行验证,其核心问题是高效的测试生成.

基于形式化或半形式化模型的测试生成以系统实现是否满足期望规约模型中定义的系统行为作为测试生成的切入点.如果说一个实现相对于期望的规约是一致的(正确的)当且仅当实现的行为集合是规约行为集合的子集,其达成程度可以通过对规约模型的覆盖程度给予衡量.从使用的规约建模方法角度来看,针对 CBTC 的测试生成方法可以分为基于标号迁移系统的测试、基于时间自动机的测试、基于 UML 模型的测试和基于故障模式的测试.表 5 对这 4 种 CBTC 测试方法进行了归纳比较.值得注意的是,CBTC 系统的组成复杂,每个子系统

© 中国科学院软件研究所 http://www.jos.org.cn

有自身特征,而在实现中每个子系统的建模语言可能也存在差异,目前很难找到一种通用的一致性测试方法来完成测试.从测试者角度而言,针对不同子系统的特征和测试目标,采用形式化程度较高的描述语言对测试对象进行建模并构建定制化的测试方法,可能是一种更为有效的方式.下面将逐一对目前的 CBTC 实现的测试生成方法进行介绍.

Table 5 Comparison of test case generation methods for CBTC implementations

表 5 CBTC 系统实现测试生成方法比较

方法名称	针对系统行为特征	形式化程度	典型应用场景
基于标号迁移系统的测试生成	安全性,并发性	高	列车自动防护系统
基于时间自动机的测试生成	实时性	高	联锁软件、车载控制系统
基于 UML 模型的测试生成	功能与场景正确性	中	列车自动控制系统
基于故障模式的测试生成	故障行为	低	列车定位系统、区域控制器

4.1.1 基于标号迁移系统的测试生成

标号迁移系统(labeled transition system,简称 LTS)是 EN50128 中推荐使用的各种形式化语言的通用语义模型.LTS 通过系统状态集合和状态之间带有标签的迁移关系定义系统运行时行为.输入输出标号迁移系统 IOLTS(input output labeled transition system)是 LTS 在测试领域的变体,它能区分测试输入和输出.基于标号迁移系统测试生成的理论基础是定义系统规约与被测系统之间的一致性关系.文献[99]针对使用 LTS 定义的信号协议,在对其进行安全性和活性模型检查的基础上,使用 UIO(unique input output)测试生成算法设计并实现了可以检测系统实现是否与期望安全性和活性一致的测试方法.文献[100]在基于时间受限的输入输出一致性关系基础上,提出了一种针对安全性测试的测试生成方法并将其应用于列车自动防护系统的测试生成.该方法建立并证明了在时间受限条件下安全性验证与一致性测试之间的形式化关系,并以此为基础构造了可同时检测常规一致性缺陷和安全性缺陷的测试生成框架.针对 CBTC 系统并发特性的测试也是很重要的工作.文献[101]针对列控系统的并发特征,提出了使用 CPN 对系统行为进行建模验证并构造其基于 IOLTS 语义模型作为生成测试序列参考的方法.该测试方法借助模型检测工具的反例生成能力,以定义期望故障模型测试目的属性公式作为测试序列生成手段,设计并实现了一种面向列控系统故障测试的测试序列生成形式化方法.

4.1.2 基于时间自动机的测试生成

CBTC 是典型的硬实时系统,因此,验证系统功能是否能够在期望的时限内正确地输出是 CBTC 系统测试的核心需求.在测试领域中,为了刻画实时系统与环境交互时,系统对环境输入的非阻塞性和环境对系统输出的非阻塞性,通常会采用 TA 的测试变体－时间输入输出自动机 TIOA(timed input output automata),建模系统的测试模型.从结构角度上说,TIOA 不同于 TA 之处在于,TIOA 是将经典 TA 的动作集合划分为不相交的输入动作集合和输出动作集合.UPPAAL-TRON[102]和 UPPAAL Cover[103]是具有代表性的基于 TIOA 实现的实时一致性测试工具.基于环境的时间受限输入输出一致性关系是其测试生成的理论基础[104].文献[105]基于 UPPAAL-TRON 的在线测试方法,在使用时间自动机对典型系统行为进行建模的基础上,构造了一种可以对闭塞中心切换过程中联锁消息传递延时的非确定性进行在线测试的一致性测试方法.文献[106]提出了一种基于时间自动机的车载系统测试生成方法.该方法首先构建基于时间自动机网络的场景树作为测试生成的基础,然后根据运行场景与列车模式之间的关系,借助 UPPAAL Cover 工具以基于观测自动机的覆盖标准为基础生成车载系统的测试集合,此外,为了构造有效的测试序列集合,该方法还定义了测试序列的筛选标准及其相关实现算法.文献[107]针对车载系统时间自动机模型中存在的非确定性会导致测试用例不满足期望覆盖准则问题,提出了一种基于全状态全变迁覆盖准则的测试生成算法,并借助 UPPAAL Cover 对算法进行实现.

4.1.3 基于 UML 模型的测试生成

作为事实上的工业建模标准,UML 以其直观、易学受到了 CBTC 产业界的青睐.相关研究人员也提出了各种以 UML 模型为测试生成参考的测试方法.例如,文献[108]提出了一种采用扩展 UML 活动图为列车控制系统安全攸关场景建模的方法,并基于简单路径覆盖思想定义了安全攸关场景测试覆盖准则及相应的测试用例生

© 中国科学院软件研究所 http://www.jos.org.cn

成方法.文献[109]也给出了一种基于 UML 用例和活动图生成列控测试用例的方法.该方法利用分类划分方法对功能输入域数据进行分割并结合相应覆盖准则从活动图中提取测试路径生成测试用例.由于列车控制系统存在计算进程与物理进程交互的特点,因此,在测试生成过程中只包含系统的离散行为是不够充分的.文献[110]针对列控系统的混成特性,采用同时基于可描述系统离散行为的状态图和物理特性的参数图的方式生成测试用例.该方法首先根据相关覆盖准则,基于状态图生成抽象的测试输入序列用例,然后,以此为基础,结合参数图和约束求解器对条件约束进行求解以获取具体的测试用例.但是上述方法都是直接基于 UML 模型本身生成测试集合,没有考虑到 UML 模型缺乏严格一致的语义会影响生成测试集合的可信性问题.因而,其在功能和安全性方面的揭错能力有待评估.

4.1.4 基于故障模式的测试生成

故障-安全导向是 CBTC 系统实现安全性的重要设计策略.这种设计策略要求系统设备或部件发生故障时,以特殊的方式做出反应并将系统行为导向安全状态,例如暂停运行或者部分暂停运行、降级使用、故障声光报警等[111].对这些故障检测及处理代码的执行通常依赖于概率低、触发条件苛刻且无法穷举的异常事件和稀有事件的发生.因而,如果仅采用以覆盖规约模型结构为主要特征的测试生成方法则很难满足高覆盖的测试需求.

基于故障模型的测试方法是以验证被测对象中不存在预定义缺陷为目标的测试技术[112].故障注入测试是其典型代表,在轨道交通信号各系统的测试过程中有着广泛的应用.故障注入测试是指按照特定的故障模型,采用人为故意的方式产生可以加速系统失效发生的故障,并作用于被测系统,以验证系统对所注入故障的响应情况是否符合预期[113].基于软件的故障注入方法因其可支持故障种类多、便于实施、开发周期短、成本低廉等优势成为被广泛采用的故障注入测试方法,运行时故障注入法是其典型代表.Ferrari,Doctor,Xception,Ftape,Fiat,Holodeck 等工具都是比较经典的运行时故障注入工具.但是,这些工具都是在系统实现完成后在测试执行阶段才能予以实施的方法,不能支持测试用例的自动生成.因此,在模型驱动开发方法已经成为 CBTC 主流研发方法学的背景下,如何有效地融合基于规约模型的测试生成与采用故障注入的测试执行方法以提高 CBTC 系统实现的覆盖度,是一个值得关注的话题.基于变异的测试生成为该问题的解决提供了一种可行的方法.

变异测试(mutation testing)是一种基于故障的软件测试方法.传统上,该方法用于评估和提高测试集合的有效性和充分性.近年来,随着对以覆盖准则为核心技术的测试生成方法揭错能力的疑问越来越多[73,114],基于变异的测试生成方法越来越受到研究人员的关注,尤其是其在提高安全攸关代码测试质量上的表现,使得变异测试成为一种极具潜力的针对安全攸关系统实现的测试方法[115].文献[116]提出了一种基于 IOLTS 规约变异的安全代码一致性测试方法,并将其应用于列车定位系统的测试中.该方法通过定义作用于需求规约上的变异算子,为安全攸关代码在实际测试时所面临的无限故障域生成、故障置入和触发等问题提供了自动化的解决方案,可提高安全代码测试的覆盖度.与文献[116]在规约层面实施变异的测试生成策略不同,文献[117]选择在测试生成之后针对测试场景实施变异,将变异测试策略应用于基于时间自动机建模的高速列车控制系统测试生成中.该方法选择了 14 个主要测试场景,并使用 15 个变异算子对其进行变异,以衡量和提高测试序列的有效性.

5 支持 CBTC 多抽象层次可信构造的方法与工具平台

基于形式化模型的开发方法以严密的数学定义和推理为基础,通过保证模型从抽象的需求定义到具体的实现代码的精化过程中所涉各研发阶段输出产物的一致性达到构造可信系统的最终目标.支持这样一个过程的全生命周期开发平台是实现基于形式化模型开发方法的核心.在过去的几十年中,研究人员对可支持高安全系统全生命周期研发的开发工具进行了广泛而深入的研究,产生了很多相应的研究成果,其中,Rodin[80]、SCADE 套件[58]、UPPAAL[41]、CPN 工具[64]等工具是研发高可信 CBTC 系统时被广泛关注和应用的开发平台.本文侧重介绍这些工具在需求分析、设计与实现 3 个阶段针对可信构造的研究应用情况.

5.1 Rodin

Rodin[80]是支持 Event-B 的建模与验证平台.Event-B 是基于相继式演算系统的形式化建模方法[77],支持系统层次的建模和分析.不同于经典的 B 语言,为了易化建模和证明过程,在 Event-B 中,系统模型被分成定义在环

© 中国科学院软件研究所 http://www.jos.org.cn

境中的静态部分和定义在机器中的动态部分,通过逐步引入状态变量和约束对模型进行精化,同时在精化过程中通过证明义务保证各层次之间的一致性.作为 B 语言家族中的一员,Event-B 是当前在轨道交通领域中使用得最为广泛的形式化建模方法之一,Thales 公司的联锁系统、Siemens 公司的区域控制系统和车载控制系统、Systerel 公司的列车控制和信号系统、AeS 公司的铁路建设项目、CASCO 公司的区域控制器等都是其典型的工业案例.Rodin 支持定义环境和机器,支持对机器的精化和环境的扩展并且可以通过集成的 Event-B 证明器自动完成对证明义务(proof obligation)的形式化验证.但是,随着机器中逐步引入的状态变量和卫士条件的增加,证明义务也会越来越多,机器的正确性证明的难度也随之加大.

5.2 SCADE套件

SCADE(safety-critical application development environment)[58]是 Esterel 公司研发的安全攸关软件系统综合开发环境,其核心是同步语言 Lustre.SCADE 开发环境提供了包括图形建模、形式化验证、代码自动生成、测试、仿真等全流程工具的支持.此外,SCADE 还可以与需求管理工具、配置管理工具和第三方仿真工具进行链接.因此,SCADE 是 4 个工具平台中对 CBTC 研发全流程活动支持程度最完整的一个.在 SCADE 建模过程中,物理环境的描述是通过定义数据类型、常量和传感器等完成的,而系统行为的建模则是通过构建用户自定义运算符进行的.运算符是 Lustre 在 SCADE 中图形化建模的可视化结果,对应于流表达式,用于表示一个执行周期中的值序列.与 Event-B 主要关注于系统层面的功能建模不同,SCADE 的建模过程类似于高级程序语言的开发过程并且可以自动生成满足 EN50128 规范的代码,因而经常被应用于开发轨道交通系统中相关安全攸关软件,典型的如列车自动控制和防护系统、区域控制器、联锁系统.

5.3 UPPAAL

UPPAAL[41]是以时间自动机为基础的针对实时系统的形式化集成开发环境,提供包括图形化建模、模型检测、测试生成等功能在内的工具集合.UPPAAL 的系统模型以时间自动机网络表示.在 UPPAAL 中,每个系统进程可被建模成一个由有穷控制结构、时钟、变量、用户自定义函数等构成的扩展的时间自动机,进程之间的通信可以基于管道同步和共享变量完成.此外,UPPAAL 还提供可调度性分析工具,以确定系统中的各个任务是否能够在期望时间内完成.铁道口问题是 UPPAAL 经典的实时系统模型验证案例[77].文献[57]基于 UPPAAL 构建了针对 CBTC 区域控制子系统的时间自动机网络模型,并对模型的实时属性和安全性进行了验证.文献[118]提出了一种基于 UPPAAL 的安全计算平台建模和验证方法,构造了基于冗余结构的安全计算平台模型,并以此为基础对安全计算平台的关键系统属性进行了形式化验证.有关 UPPAAL 测试工具在 CBTC 系统中的研究应用情况已在第 4.1.2 节进行了描述.

5.4 CPN工具

CPN 工具[64]是以有色 Petri 网为核心的形式化建模工具集,支持层次化的图形建模、仿真、分析、验证等功能,但在模型验证功能中并不支持反例的生成.区别于其他工具平台,CPN 工具的显著特点是,对异步通信方式的模拟使得其可以支持真正的并发而非交错式并发的建模.文献[119]采用有色 Petri 网对车载软件进行了形式化建模,并利用状态空间分析对相关功能进行了安全性验证和仿真.文献[101]构造了一种基于 CPN 的列车车载软件形式化测试序列的自动生成方法,在对 CPN 工具功能进行扩展的基础上,针对系统进行了建模和测试.

上述工具平台都是以形式化方式对系统和期望的属性进行建模和定义,通过自动搜索系统所有可能执行路径,给出系统模型能够满足期望属性的证明,存在“状态空间爆炸”的瓶颈问题.因此,构造有效的状态空间约减方法是将这些工具平台应用于 CBTC 系统研发的关键环节.表 6 将各工具特性进行了对比.

© 中国科学院软件研究所 http://www.jos.org.cn

Table 6 Comparison of construction tool features for CBTC

表 6 现有 CBTC 构造工具特性比较

工具名称	功能特性	主要用途	可信验证类型	形式化程度	典型应用场景
Rodin[80]	采用定理证明技术支持多抽象层次规约精化的一致性	需求阶段,设计阶段	安全性验证	高	联锁系统、车载系统、区域控制系统
SCADE 套件[58]	支持图形化建模与仿真,自动代码生成,支持形式化设计模型验证	设计阶段,实现阶段	安全性验证	低	联锁软件、列车自动控制和防护软件
UPPAAL[41]	支持时间属性建模,具有图形化的系统建模仿真用户界面,支持自动化模型检查	需求阶段,设计阶段	安全性验证,实时性验证	高	区域控制器、列车自动控制系统
CPN 工具[64]	支持层次化的并行行为建模,支持系统级模型的图形化建模、仿真、分析和验证	需求阶段,设计阶段	安全性验证	中	列车车载软件、区域控制器

6 总结与展望

在我国大力发展高铁与城市轨道交通等关乎国计民生同时又安全攸关的产业之际,我们仍然缺乏对关键 CBTC 子系统的自主研发能力,如何实现自主产权 CBTC 系统的可信保障成为一项极具挑战性的任务.而 CBTC 特有的复杂运行环境,使其可信保障变得愈加困难.为了提高 CBTC 开发的效率,降低早期 CBTC 设计的复杂性,目前大多数的 CBTC 系统设计采用的是自顶向下的开发流程.由于系统自身的复杂性以及所处环境的复杂性,CBTC 在开发过程中依然存在如下问题.

- 在需求阶段,对于 CBTC 这种运行在不确定环境下的复杂系统,现有的方法与工具难以有效地支持功能与非功能需求的建模,难以实现从系统需求到软件需求的自动转换.由于缺少不确定环境下 CBTC 系统需求的抽取方法,无法开展针对 CBTC 系统体系架构的探索与非功能需求冲突的权衡,这就导致难以评估不确定环境对 CBTC 系统带来的影响,并且难以做出正确、合理的需求决策.因此,不确定环境下需求模型与规约的正确性与合理性难以得到保证.
- 在设计阶段,虽然目前存在各种用途的建模和验证的工具,但仍缺乏有效的通用模型转换语言及支持工具,不同模型之间难以集成.在设计模型正确性方面,由于涉及到实现的细节,复杂的设计模型在形式化验证过程中极易引起“状态空间爆炸”等问题,导致目前已有的工具无法在规定的时间内完成形式化验证的任务.
- 在系统实现方面,由于综合(synthesis)自动化程度低,CBTC 的需求模型与设计模型很难自动地生成底层的代码,在 CBTC 设计自顶向下的精化过程中需要大量的人工干预,因此在自顶向下的设计与开发过程中不可避免地存在着大量错误.
- 在自顶向下的构造过程中,由于缺乏不同抽象模型之间协同验证的方法,CBTC 需求与设计模型的验证与系统实现层次的验证相互独立,验证结果无法重用,功能的一致性与正确性难以维护.这导致大量的产品开发时间消耗在系统功能的确认与验证上,严重制约了 CBTC 系统整体的开发速度.

虽然形式化方法已成为 CBTC 领域最有前景的系统可信性保障手段并取得了令人鼓舞的成果,但是目前还远未在实际的工业界得到全面应用.随着 CBTC 领域从单核计算到多核计算,从 GSM-R 通信到 4G LTE 通信[120],以及从简单控制到复杂系统的发展,可以预期,工业界花费在 CBTC 设计、开发与验证上的代价将更加巨大.在竞争激烈的 CBTC 系统行业,如何在保证所构造的 CBTC 的可靠性的同时又能行之有效地减少可信构造的代价,已经成为 CBTC 研发的严峻挑战.因此,学术界和工业界还需在理论方法、工具平台以及工程实践等多方面进一步投入,研究如何在保障 CBTC 可信构造的同时,缓解或避免使用形式化方法所带来的诸多限制.

References:

[1] Gao CH. Research on the key techniques of the independent and innovative CBTC. Modern Urban Transit, 2011,24(4):1−4 (in Chinese with English abstract).

© 中国科学院软件研究所 http://www.jos.org.cn

[2] European Committee for Electrotechnical Standardization. EN50128, Railway Applications—Software for Railway Control and Protection Systems. Brussels: CENELEC, 1997.

[3] Cao Y, Tang T, Xu TH, Mu JC. Application of formal methods in train control system. Journal of Traffic and Transportation Engineering, 2010,10(1):112−126 (in Chinese with English abstract).

[4] Tang T, Zhao LB. Train Control System Design and Verification Methods Based on Model. Beijing: China Railway Publishing House, 2014 (in Chinese).

[5] Fantechi A. Twenty-Five years of formal methods and railways: what next. In: Proc. of the Int'l Conf. on Software Engineering and Formal Methods. Springer Int'l Publishing, 2013. 167−183. [doi: 10.1007/978-3-319-05032-4_13]

[6] IEEE Std 1850-2010. IEEE Standard for Property Specification Language (PSL). 2010. 1−182.

[7] Hu XL. Modeling and verification of level transition scene in CTCS-3 level train control system based on UML and UPPAAL [MS. Thesis]. Lanzhou: Lanzhou Jiaotong University, 2015 (in Chinese with English abstract).

[8] Liu JT, Tang T, Xiu TH, Zhao L. Formal verification of CTCS-3 system requirements specification based UML model. China Railway Science, 2011,32(3):93−99 (in Chinese with English abstract).

[9] Chiappini A, Cimatti A, Macchi L, Rebollo O, Roveri M, Susi A, Vittorini B. Formalization and validation of a subset of the European train control system. In: Proc. of the Int'l Conf. on Software Engineering. 2010. 109−118. [doi: 10.1145/1810295.1810312]

[10] Zhang QX. Research on the method of verification of train control system requirements specification based on xUML [MS. Thesis]. Beijing: Beijing Jiaotong University, 2011 (in Chinese with English abstract).

[11] Bloem R, Cimatti A, Greimel K, Hofferek G, Könighofer R, Roveri M, Seeber R. RATSY—A new requirements analysis tool with synthesis. In: Proc. of the Int'l Conf. on Computer Aided Verification (CAV). Berlin: Springer-Verlag, 2010. 425−429. [doi: 10.1007/978-3-642-14295-6_37]

[12] He LY, Zhao L, Chen RJ. Property-Driven modeling and verification for requirements of train control system. Railway Computer Application, 2014,(2):1−6 (in Chinese with English abstract).

[13] Chen RJ, Zhao L, He LY. UML-Based requirements analysis methods and attributes used in the train control system requirements specification. Railway Signaling & Communication, 2013,(2):80−84 (in Chinese with English abstract).

[14] Zhao L, Tang T, Cheng RJ, He LY. Property based requirements analysis for train control system. Journal of Computational Information Systems, 2013,9(3):915−922.

[15] Sommerville I, Sawyer P. Requirements Engineering. Wiley Publishing, 1998.

[16] Yuan L, Tang T, Li K. Modelling and verification of the system requirement specification of train control system using SDL. In: Proc. of the Int'l Symp. on Autonomous Decentralized Systems. 2011. 81−85. [doi: 10.1109/ISADS.2011.17]

[17] Issad M, Koul L, Rauzy A. A contribution to safety analysis of railway CBTC systems using Scola. In: Safety and Reliability of Complex Engineered Systems. CRC Press, 2015. 459−467. [doi: 10.1201/b19094-64]

[18] Faber J, Jacobs S, Sofronie-Stokkermans V. Verifying CSP-OZ-DC specifications with complex data types and timing parameters. In: Proc. of the Int'l Conf. on Integrated Formal Methods. Berlin: Springer-Verlag, 2007. 233−252. [doi: 10.1007/978-3-540-73210-5_13]

[19] Abo R, Voisin L. Formal implementation of data validation for railway safety-related systems with OVADO. In: Proc. of the SEFN Workshops. Springer Int'l Publishing, 2014. 221−236. [doi: 10.1007/978-3-319-05032-4_17]

[20] Abrial JR. Modeling in Event-B: System and Software Engineering. Cambridge University Press, 2010.

[21] Milner R. A Calculus of Communicating Systems. New York: Springer-Verlag, 1980. [doi: 10.1007/3-540-10235-3]

[22] Hoare CAR. Communicating Sequential Processes. Englewood Cliffs: Prentice Hall Int'l, 1985.

[23] Zou L, Lü JD, Wang SL, Zhan NJ, Tang T, Yuan L, Liu Y. Verifying Chinese train control system under a combined scenario by theorem proving. In: Proc. of the Int'l Verified Software: Theories, Tools, and Experiments. Berlin: Springer-Verlag, 2013. 262−280. [doi: 10.1007/978-3-642-54108-7_14]

[24] Pohl K. Requirements Engieering: Fundamentals, Principles, and Techniques. Springer-Verlag, 2010.

[25] Liu JT, Tang T, Xiu TH, Zhao L. Formal verification of CTCS-3 system requirements specification based UML model. China Railway Science, 2011,32(3):93−99 (in Chinese with English abstract).

© 中国科学院软件研究所 http://www.jos.org.cn

[26] Ahmad E, Dong YW, Larson B, Lu J, Tang T, Zhan NJ. Behavior modeling and verification of movement authority scenario of Chinese train control system using AADL. Science China Information Sciences, 2015,58(11):1−20 (in Chinese with English abstract).

[27] Andre C, Mallet F, Simone RD. Modeling time(s). In: Proc. of the Int'l Conf. on Model Driven Engineering Languages and Systems (MoDELS). Berlin: Springer-Verlag, 2007. 559−573. [doi: 10.1007/978-3-540-75209-7_38]

[28] Alur R, Dill D. A theory of timed automata. Theoretical Computer Science, 1994,126(2):183−235. [doi: 10.1016/0304-3975(94)90010-8]

[29] Zhou CC, Hoare CA, Ravn AP. A calculus of duration. Information Processing Letters, 1991,40(5):269−276. [doi: 10.1016/0020-0190(91)90122-X]

[30] UML Tools. 2016. https://www.wikiwand.com/en/List_of_Unified_Modeling_Language_tools

[31] IBM Rational Software. 2016. https://www.ibm.com/software/rational

[32] SAP PowerDesigner. 2016. http://go.sap.com/product/data-mgmt/powerdesigner-data-modeling-tools.html

[33] PragmaDev Studio. 2016. http://www.pragmadev.com/

[34] IBM SDL Suite. 2016. http://www-01.ibm.com/software/awdtools/sdlsuite/

[35] PAT Model Checker. 2016. http://www.patroot.com/

[36] Aceituna D, Do H, Lee SW. SQ^2E: An approach to requirements validation with scenario question. In: Proc. of the Int'l Conf. on Asia Pacific Software Engineering. 2010. 33−42. [doi: 10.1109/APSEC.2010.14]

[37] Aceituna D, Do H, Lee SW. Interactive requirements validation for reactive systems through virtual requirements prototype. In: Proc. of the Int'l Conf. on Model-Driven Requirements Engineering Workshop (MoDRE). 2011. 1−10. [doi: 10.1109/MoDRE.2011.6045361]

[38] Lee YK, In HP, Kazman R. Customer requirements validation method based on mental models. In: Proc. of the Int'l Conf. on Asia-Pacific Software Engineering Conf. 2014. 199−206. [doi: 10.1109/APSEC.2014.39]

[39] IBM Rational Requisite Pro. http://open-services.net/software/ibm-rational-requisite-pro/

[40] The ProB Animator and Model Checker. https://www3.hhu.de/stups/prob/

[41] UPPAAL. http://www.uppaal.org/

[42] Maio WK, Pu GG, Yao YB, Su T, Bao DZ, Liu Y. Automated requirements validation for ATP software via specification review and testing. In: Proc. of the Int'l Conf. on Formal Engineering Methods (ICFEM). Springer Int'l Publishing, 2016. 26−40. [doi: 10.1007/978-3-319-47846-3_3]

[43] Frehse G. PHAVer: Algorithmic verification of hybrid systems past HyTech. Int'l Journal on Software Tools for Technology Transfer (STTT), 2008,10(3):263−279. [doi: 10.1007/s10009-007-0062-x]

[44] Podelski A, Rybalchenko A. Transition predicate abstraction and fair termination. ACM SIGPLAN Notices, 2005,40(1):132−144. [doi: 10.1145/1047659.1040317]

[45] Podelski A, Rybalchenko A. ARMC: The logical choice for software model checking with abstraction refinement. In: Practical Aspects of Declarative Languages. Berlin: Springer-Verlag, 2007. 245−259. [doi: 10.1007/978-3-540-69611-7_16]

[46] Olderog ER. Automatic verification of combined specifications: An overview. Electronic Notes in Theoretical Computer Science, 2008,207:3−16. [doi: 10.1016/j.entcs.2008.03.082]

[47] Cho C, Choi D, Quan Z, Choi S, Park G, Ryou M. Modeling of CBTC carborne ATO functions using SCADE. In: Proc. of the Int'l Conf. on Control, Automation and Systems. 2011. 1089−1093.

[48] Simulink. 2016. https://www.mathworks.com/products/simulink

[49] Feiler PH, Gluch DP, Hudak JJ. The architecture analysis & design language (AADL): An introduction. Technical Report, CMU/SEI-2006-TN-011, Carnegie Mellon University, 2006.

[50] OSATE2. 2016. http://osate.github.io/

[51] Li C, Zhang L. Train control system modeling and design based on AADL. In: Proc. of the Int'l Conf. on Software Engineering and Service Science. 2015. 474−477. [doi: 10.1109/ICSESS.2015.7339100]

© 中国科学院软件研究所 http://www.jos.org.cn

[52] Ahmad E, Dong YW, Larson B, Lü J, Tang T, Zhan NJ. Behavior modeling and verification of movement authority scenario of Chinese train control system using AADL. Science China Information Sciences, 2015,58(11):1−20. [doi: 10.1007/s11432-015-5346-2]

[53] Yang CS, Lim JL, Um JK, Han JM, Bang Y, Kim HH, Yun YH, Kim CJ, Cho YJ. Developing CBTC software using model-driven development approach. In: Proc. of the WCRR. 2008.

[54] Yang SW. Modeling and safety verification of zone controller in CBTC with UML [MS. Thesis]. Beijing: Beijing Jiaotong University, 2008 (in Chinese with English abstract).

[55] Henzinger TA. The theory of hybrid automata. In: Proc. of the IEEE Symp. on Logic in Computer Science. Berlin: Springer-Verlag, 1996. 278−292. [doi: 10.1007/978-3-642-59615-5_13]

[56] Bu L, Wang Q, Chen X, Wang L, Zhang T, Zhao J, Li X. Toward online hybrid systems model checking of cyber-physical systems' time-bounded short-run behavior. ACM SIGBED Review, 2011,8(2):7−10. [doi: 10.1145/2000367.2000368]

[57] Lü JD, Tang T, Yan F, Xu TH. UPPAAL-Based simulation and verification of CBTC zone control subsystem in rail transportation. Journal of the China Railway Society, 2009,31(3):59−64 (in Chinese with English abstract).

[58] SCADE Suite. 2016. http://www.esterel-technologies.com/products/scade-suite/

[59] Ren X, Zhou MC. Tactical scheduling of rail operations: A Petri net approach. In: Proc. of the Int'l Conf. on Intelligent Systems for the 21st Century. 1995. 3087−3092. [doi: 10.1109/ICSMC.1995.538256]

[60] Hei X, Takahashi S, Nakamura H. Distributed interlocking system and its safety verification. In: Proc. of the Int'l Conf. on Intelligent Control and Automation. 2006. 8612−8615. [doi: 10.1109/WCICA.2006.1713661]

[61] Hörste MM, Schnieder E. Modelling and simulation of train control systems using Petri nets. In: Proc. of the World Congress on Formal Methods. Berlin: Springer-Verlag, 1999. 1867−1867. [doi: 10.1007/3-540-48118-4_58]

[62] Ren GB. Modelling and analysis of high-speed train tracking process based on high-level Petri net. [Ph.D. Thesis]. Lanzhou: Lanzhou Jiaotong University, 2015 (in Chinese with English abstract).

[63] Boudi Z, Collart-Dutilleul S, Khaddour M. High level Petri net modeling for railway safety critical scenarios. In: Proc. of the Int'l Conf. on Formal Methods for Automation and Safety in Railway and Automotive Systems. 2014. 65−75.

[64] CPN Tool. 2016. http://cpntools.org/

[65] Wu DY, Zhang Y. Researching colored Petri nets model of communication based train control system. Journal of System Simulation, 2005,17(10):2388−2391 (in Chinese with English abstract).

[66] Zhao SX, Wang XL. Movement authority process formal modeling for China train control system-3. Computer Engineering and Design, 2013,34(6):2119−2124.

[67] Ahmad E, Dong YW, Larson B, Lü J, Tang T, Zhan NJ. Behavior modeling and verification of movement authority scenario of Chinese train control system using AADL. Science China Information Sciences, 2015,58(11):1−20. [doi: 10.1007/s11432-015-5346-2]

[68] Sun P, Collart-Dutilleul S, Bon P. A formal modeling methodology of french railway interlocking system via HCPN. WIT Trans. on the Built Environment. 2014,135:1−10. [doi: 10.2495/CR140711]

[69] Zimmermann A, Hommel G. Towards modeling and evaluation of ETCS real-time communication and operation. Journal of Systems and Software, 2005,77(1):47−54. [doi: 10.1016/j.jss.2003.12.039]

[70] Zhou G, Zhao HB. Modeling and safety analysis of track occupancy checking logic in section signaling. Journal of the China Railway Society, 2016,38(4):66−73 (in Chinese with English abstract).

[71] Zhou G, Zhao H. Modeling and quantitative safety analysis of Chinese train control system of systems. In: Proc. of the Int'l Conf. on Intelligent Transportation Systems (ITSC). 2015. 381−386. [doi: 10.1109/ITSC.2015.71]

[72] Rigorous Approach to Industrial Software Engineering. 2016. http://spd-web.terma.com/Projects/RAISE/

[73] Haxthausen AE, Peleska J. Formal development and verification of a distributed railway control system. IEEE Trans. on Software Engineering, 2000,26(8):687−701. [doi: 10.1109/32.879808]

[74] Xu SZ. Modeling and analysis of RBC handover based on timed RAISE [Ph.D. Thesis]. Lanzhou: Lanzhou Jiaotong University, 2015 (in Chinese with English abstract).

[75] PLASMA Lab. 2016. https://project.inria.fr/plasma-lab/

© 中国科学院软件研究所 http://www.jos.org.cn

[76] Modelica. 2016. https://www.modelica.org/

[77] CHARON. 2016. https://rtg.cis.upenn.edu/mobies/charon/

[78] NuSMV. 2016. http://nusmv.fbk.eu/

[79] The Coq Proof Assistant. 2016. https://coq.inria.fr/

[80] Rodin. 2016. http://www.event-b.org/

[81] Probabilistic Symbolic Model Checker. 2016. http://www.prismmodelchecker.org

[82] Goodman CJ, Siu LK, Ho TK. A review of simulation models for railway systems. In: Proc. of the Int'l Conf. on Developments in Mass Transit Systems. 1998. 80−85. [doi: 10.1049/cp:19980101]

[83] Cimatti A, Corvino R, Lazzaro A, Narasamdya I, Rizzo T, Roveri M, Tchaltsev A. Formal verification and validation of ERTMS industrial railway train spacing system. In: Proc. of the Int'l Conf. on Computer Aided Verification. Berlin: Springer-Verlag, 2012. 378−393. [doi: 10.1007/978-3-642-31424-7_29]

[84] Hemmat MHA, Mohamed OA, Boukadoum M. Formal modeling, verification and implementation of a train control system. In: Proc. of the Int'l Conf. on Microelectronics (ICM). 2015. 134−137. [doi: 10.1109/ICM.2015.7438006]

[85] Qian J, Liu J, Chen XH, Sun JF. Modeling and verification of zone controller: The SCADE experience in china's railway systems. In: Proc. of the Int'l Workshop on Complex Faults and Failures in Large Software Systems. 2015. 48−54. [doi: 10.1109/COUFLESS.2015.15]

[86] Platzer A. Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics. Berlin: Springer-Verlag, 2010. [doi: 10.1007/978-3-642-14509-4]

[87] Zou L, Zhan NJ, Wang SL, Fränzle M, Qin SC. Verifying simulink diagrams via a hybrid Hoare logic prover. In: Proc. of the Int'l Conf. on Embedded Software, Vol.9. 2013. 1−10. [doi: 10.1109/EMSOFT.2013.6658587]

[88] Zhou X, Zhang Y. Security analysis about a train control center based on a Bayesian network. In: Proc. of the Int'l Conf. on Transportation Engineering. Reston: American Society of Civil Engineers. 2015.

[89] Xu TH, Tang T, Gao CH, Cai BG. Dependability analysis of the data communication system in train control system. Science in China Series E: Technological Sciences, 2009,52(9):2605−2618. [doi: 10.1007/s11431-009-0183-4]

[90] Zhao HL, Xu TH, Tang T. Towards modeling and evaluation of availability of communication based train control (CBTC) system. In: Proc. of the Int'l Conf. on Communication Technology and Applications. 2009. 860−863. [doi: 10.1109/ICCOMTA.2009.5349076]

[91] Bu L, Wang Q, Chen X, Wang L, Zhang T, Zhao J, Li X. Toward online hybrid systems model checking of cyber-physical systems' time-bounded short-run behavior. ACM SIGBED Review, 2011,8(2):7−10. [doi: 10.1145/2000367.2000368]

[92] Lü JD, Tang T, Yan F, Xu TH. UPPAAL-Based simulation and verification of CBTC zone control subsystem in rail transportation. Journal of the China Railway Society, 2009,31(3):59−64 (in Chinese with English abstract).

[93] David A, Du D, Larsen KG, Legay A, Mikučionis M. Optimizing control strategy using statistical model checking. In: Proc. of the NASA Formal Methods Symp. Berlin: Springer-Verlag, 2013. 352−367. [doi: 10.1007/978-3-642-38088-4_24]

[94] Gu F, Zhang XQ, Chen MS, Grosse D, Drechsler R. Quantitative timing analysis of UML activity diagrams using statistical model checking. In: Proc. of the Int'l Conf. on Design, Automation & Test in Europe Conf. & Exhibition (DATE). 2016. 780−785. [doi: 10.3850/9783981537079_0339]

[95] McDermid J, Kelly T. Software in safety critical systems-achievement and prediction. Nuclear Future, 2006,(2):140−146. [doi: 10.1680/nuen.2006.2.3.140]

[96] Ellims M. On wheels, nuts and software. In: Proc. of the Australian Workshop on Safety Critical Systemsand Software. Parlinghurst: Austranlian Computer Society, 2004. 67−76.

[97] Heimdahl MPE. Safety and software intensive systems: Challenges old and new. In: Proc. of the Future of Software Engineering. 2007. 137−152. [doi: 10.1109/FOSE.2007.18]

[98] Lutz RR. Software engineering for safety: A roadmap. In: Proc. of the Future of Software Engineering. New York: ACM, 2000. 213−226. [doi: 10.1145/336512.336556]

[99] Leea JH, Hwanga JG, Shina D, Leea KM, Kimb SU. Development of verification and conformance testing tools for a railway signaling communication protocol. Computer Standards and Interfaces, 2009,31(2):362−371. [doi: 10.1016/j.csi.2008.05.011]

© 中国科学院软件研究所 http://www.jos.org.cn

[100] Didrich K, Herbs S, Vieria M. Applying model-based testing to a train control system. In: Proc. of the INFORMATIK. 2006. 249−256.

[101] Zhang Y. Fault related formal test method of the software in train control system [Ph. D Thesis]. Beijing: Beijing Jiaotong University, 2012 (in Chinese with English abstract).

[102] UPPAAL-TRON. 2016. http://people.cs.aau.dk/~marius/tron/

[103] UPPAAL Cover. http://www.hessel.nu/CoVer/

[104] Hessel A, Larsen KG, Mikucionis M, Nielsen B, Pettersson P, Skou A. Testing real-time systems using UPPAAL. In: Proc. of the Formal Methods and Testing. 2008. 77−117. [doi: 10.1007/978-3-540-78917-8_3]

[105] Lü JD, Zhu XL, Wang HF, Li KC, TANG T. Research on conformance testing for nondeterministic delay in high speed train control system based on UPPAAL-TRON. Journal of the China Railway Society, 2016,38(1):54−64 (in Chinese with English abstract).

[106] Lü JD, Ren PC, Lei C, Li KC, Tang T. Model-Based test case generation for function testing of CTCS-3 onboard subsystem. Journal of Control and Automation, 2015,8(1):171−178. [doi: 10.14257/ijca.2015.8.10.17]

[107] Yang L, Lü JD, L Y, Li CL, Zhao WH. Research on model-based test case generation method of onboard subsystem in CTCS-3. Journal of the China Railway Society, 2014,36(8):55−62 (in Chinese with English abstract).

[108] Chen X, Jang P, Zhang YF, Huang C, Zhou Y. Method of automatic test case generation for safety-critical scenarios in train control systems. Ruan Jian Xue Bao/Journal of Software, 2015,26(2):269−278 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4780.htm [doi: 10.13328/j.cnki.jos.004780]

[109] Yin YF, Liu B, Ni HY. Real-Time embedded software testing method based on extended finite state machine. Journal of Systems Engineering and Electronics, 2012,23(2):276−285. [doi: 10.1109/JSEE.2012.00035]

[110] Hilken C, Hübner F, Peleska J. Combination of behavioral and parametric diagrams for model-based testing. Technical Report, openECTS Report 2014-11-25, University of Bremen, 2015.

[111] Ministry of Railway of the People's Republic of China. TB/T 2615-1994 Railway Signal Failure—Safety Principles. Beijing: China Railway Publishing House, 1995 (in Chinese).

[112] Morell LJ. A theory of fault-based testing. IEEE Trans. on Software Engineering, 1990,16(8):844−857. [doi: 10.1109/32.57623]

[113] Tu HY, Wu FM. Embedding fault in simulation environment for software black-box testing. Ruan Jian Xue Bao/Journal of Software, 1998,10(5):516−520 (in Chinese with English abstract).

[114] Gay G, Staats M, Whalen M, Heimdahl M. The risks of coverage-directed test case generation. IEEE Trans. on Software Engineering, 2015,41(8):803−819. [doi: 10.1109/TSE.2015.2421011]

[115] Baker R, Habli I. An empirical evaluation of mutation testing for improving the test quality of safety-critical software. IEEE Trans. on Software Engineering, 2013,39(6):787−805. [doi: 10.1109/TSE.2012.56]

[116] Sun HY, Chen MS, Zhang M, Liu J, Zhang Y. Improving defect detection ability of derived test cases based on mutated UML activity diagrams. In: Proc. of the Annual Computer Software and Applications Conf. 2016. 275−280. [doi: 10.1109/COMPSAC.2016.136]

[117] Li T, Li KC, Lv JD, Yuan L, Fu Q, Wen T. Mutation testing for evaluating the completeness of test cases in high-speed train control system. In: Proc. of the Int'l Conf. on Intelligent Transportation Systems. 2015. 777−782. [doi: 10.1109/ITSC.2015.131]

[118] Wang X, Ma LC, Tang T. Study on formal modeling andverification of safety computer platform. Advances in Mechanical Engineering, 2016,8(5):1−13. [doi: 10.1177/1687814016649115]

[119] Lu QJ. Modeling and analysis of CBTC onboard equipment based on colored Petri net [MS. Thesis]. Beijing: Beijing Jiaotong University, 2008 (in Chinese with English abstract).

[120] Zhu L, Ning B. The design of the CBTC train-ground communication system based on IEEE 802.11g standard. China Railway Science, 2010,31(5):119−124 (in Chinese with English abstract).

附中文参考文献:

[1] 郜春海.自主创新 CBTC 系统的核心技术研究.都市快轨交通,2011,24(4):1−4.

[3] 曹源,唐涛,徐田华,穆建成.形式化方法在列车运行控制系统中的应用.交通运输工程学报,2010,10(1):112−126.

© 中国科学院软件研究所 http://www.jos.org.cn

[4] 唐涛,赵林编.基于模型的列车运行控制系统设计与验证方法.北京:中国铁道出版社,2014.
[7] 胡雪莲.基于 UML 和 UPPAAL 的 CTCS-3 级列控系统等级转换场景建模与验证[硕士学位论文].兰州:兰州交通大学,2015.
[8] 刘金涛,唐涛,徐田华,赵林.基于 UML 的 CTCS-3 级列控系统需求规范形式化验证方法.中国铁道科学,2011,32(3):93−99.
[10] 张庆新.基于 xUML 的列控系统需求规范验证方法研究[硕士学位论文].北京:北京交通大学,2011.
[12] 何丽芸,赵林,程瑞军.属性驱动的列车控制系统需求建模与验证.铁路计算机应用,2014,(2):1−6.
[13] 程瑞军,赵林,何丽芸.基于 UML 及属性的需求分析方法在列控系统需求规范中的应用.铁道通信信号,2013,(2):80−84.
[25] 刘金涛.基于 STPA 的需求阶段的高速列车运行控制系统安全分析方法研究[博士学位论文].北京:北京交通大学,2015.
[54] 杨旭文.基于 UML 的 CBTC 系统区域控制器的建模与安全性验证[硕士学位论文].北京:北京交通大学,2008.
[57] 吕继东,唐涛,燕飞,徐天华.基于 UPPAAL 的城市轨道交通 CBTC 区域控制子系统建模与验证.铁道学报,2009,31(3):59−64.
[62] 任国彬.基于高级 Petri 网的高速列车追踪运行过程建模与分析[硕士学位论文].兰州:兰州交通大学,2015.
[65] 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.系统仿真学报,2005,17(10):2388−2391.
[70] 周果,赵会兵.区间占用检查逻辑的建模与安全分析.铁道学报,2016,38(4):66−73.
[74] 徐世泽.基于 Timed RAISE 的 RBC 切换建模与分析[硕士学位论文].兰州:兰州交通大学,2015.
[101] 张岩.列车运行控制系统软件故障相关形式化测试方法[博士学位论文].北京:北京交通大学,2012.
[105] 吕继东,朱晓琳,王海峰,李开成,唐涛.基于 UPPAAL-TRON 的高速铁路列控系统非确定性时延一致性测试研究.铁道学报,2016,38(1):54−64.
[107] 袁磊,吕继东,刘雨,李辰岭,赵伟慧.一种全覆盖的列控车载系统测试用例自动生成算法研究.铁道学报,2014,36(8):55−62.
[108] 陈鑫,姜鹏,张一帆,黄超,周岩.一种面向列车控制系统中安全攸关场景的测试用例自动生成方法.软件学报,2015,26(2):269−278. http://www.jos.org.cn/1000-9825/4780.htm [doi: 10.13328/j.cnki.jos.004780]
[111] 中华人民共和国铁道部.TB/T 2615-1994 铁道信号故障——安全原则.北京:中国铁道出版社,1995.
[119] 陆启进.基于有色 Petri 网的 CBTC 车载设备应用软件的建模与分析[硕士学位论文].北京:北京交通大学,2008.
[120] 朱力,宁滨.基于 IEEE 802.11g 标准的 CBTC 车地通信系统设计.中国铁道科学,2010,31(5):119−124.

陈铭松(1982－),男,江苏泰兴人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为信息物理融合系统,嵌入式系统设计自动化,软件工程.

鲍勇翔(1991－),男,硕士生,主要研究领域为形式化方法,计算机体系结构.

孙海英(1976－),女,讲师,CCF 专业会员,主要研究领域为形式化建模,形式化测试,时空逻辑.

缪炜恺(1983－),男,博士,讲师,主要研究领域为软件工程,软件需求与建模,软件测试.

陈小红(1982－),女,博士,副教授,CCF 专业会员,主要研究领域为信息物理融合系统,需求工程.

周庭梁(1980－),男,高级工程师,主要研究领域为轨道交通列车控制系统,安全苛求软件,可信测评.

© 中国科学院软件研究所 http://www.jos.org.cn