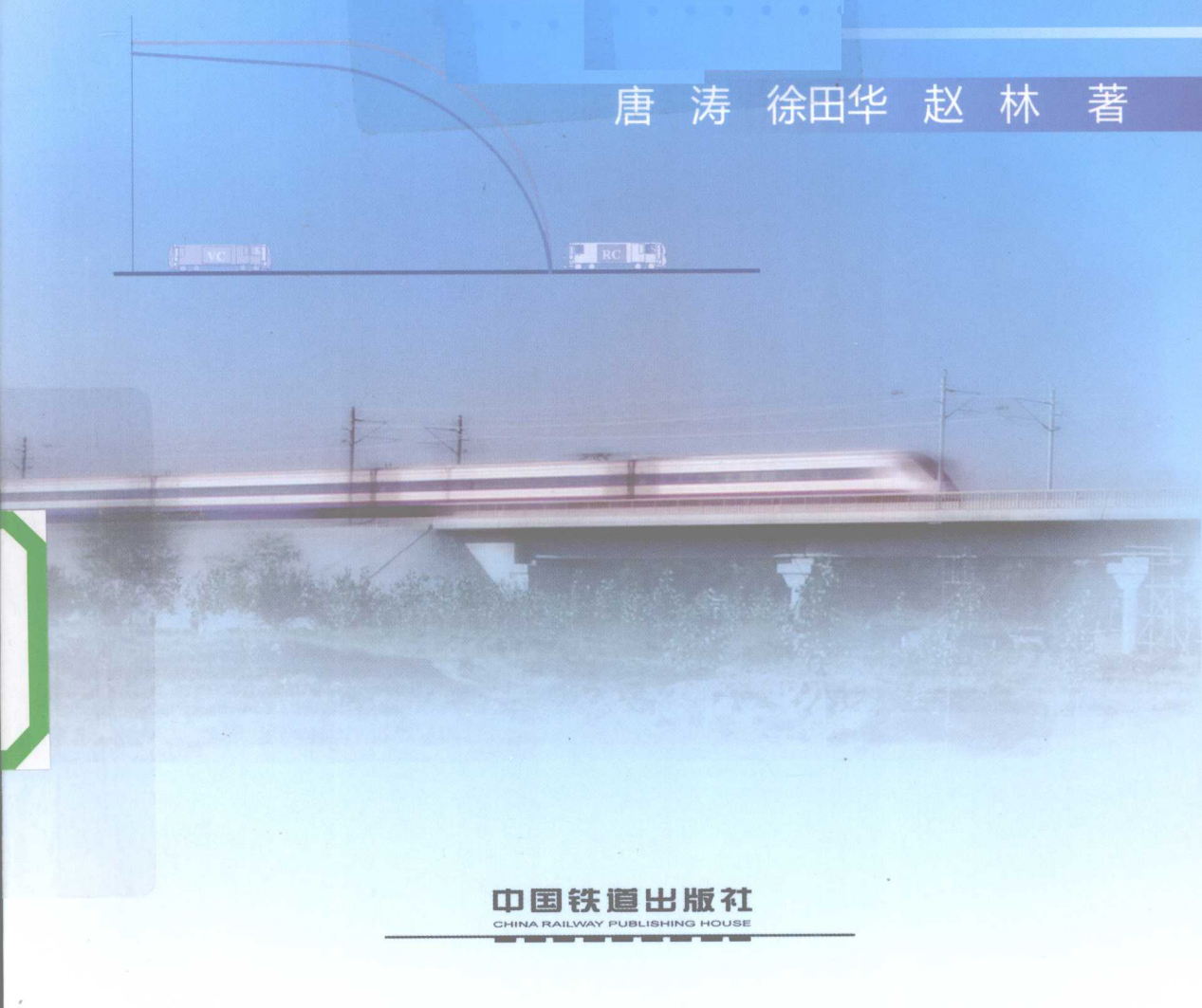
国家自然科学基金——铁道联合重点项目（60634010）资助

列车运行控制系统规范建模与验证

唐 涛 徐田华 赵 林 著



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书主要介绍了实现列控系统需求规范的严格建模与验证所必须的理论、方法和关键技术，内容包括现代列车运行控制系统的特点和相关标准规范、系统规范的严格建模与验证体系、模型检验相关基础知识、需求规范的管理和追踪、列控领域的 UML 建模以及针对 CTCS－3 系统规范展开的实例分析。

本书内容丰富，注重背景，可以作为研究生、教师以及轨道交通控制领域相关的科研人员了解列控系统规范的建模与验证的基本思想和方法的参考书。

图书在版编目（CIP）数据

列车运行控制系统规范建模与验证/唐涛，徐田华，赵林著．
—北京：中国铁道出版社，2010.6
ISBN 978-7-113-11460-2

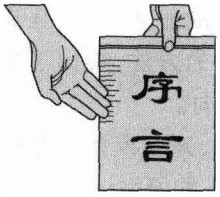
Ⅰ.①列… Ⅱ.①唐… ②徐… ③赵… Ⅲ.①列车—运行—控制系统—系统建模②列车—运行—控制系统—验证 Ⅳ.①U284.48

中国版本图书馆 CIP 数据核字（2010）第 096554 号

书　　名：列车运行控制系统规范建模与验证
作　　者：唐　涛　徐田华　赵　林　著

责任编辑：朱雪玲　魏京燕　**电话**：路（021）73115　**电子信箱**：dianwu@vip.sina.com
封面设计：冯龙彬
责任印制：郭向伟

出版发行：中国铁道出版社（100054，北京宣武区右安门西街 8 号）
网　　址：http://www.tdpress.com
印　　刷：北京市彩桥印刷有限责任公司
版　　次：2010 年 6 月第 1 版　2010 年 6 月第 1 次印刷
开　　本：700 mm×1 000 mm　1/16　印张：13.25　字数：227 千
书　　号：ISBN 978-7-113-11460-2
定　　价：30.00 元



轨道交通具有运能大、能耗低、污染小、安全舒适等优势，是最具可持续性和环境友好性的交通运输系统，在我国综合交通体系中具有不可替代的突出地位。作为一种大容量公共交通工具，轨道交通系统的安全性直接关系到广大乘客的生命财产安全，必须采用高性能的列车运行控制系统（简称列控系统）保证列车安全、正点、快捷、舒适、高密度不间断运行。随着科学技术的飞速发展，计算机技术、通信技术已经广泛地应用于轨道交通，列控系统已发展成为以安全计算机为核心的覆盖轨道交通全线所有站点、所有列车的网络化复杂控制系统——自动列车运行控制系统。

作为保证轨道交通列车运行安全的安全控制系统，列车运行控制系统必须有很高的 RAMS（Reliability Availability Maintainability and Safety）性能，安全完善度等级（SIL）应达到 SIL 4。为此，系统须按照国际安全标准推荐的“V”模型进行开发，在系统安全生命周期内进行全程质量管理和安全管理。作为系统开发的首要环节，系统需求规范表征了用户对列车运行控制系统的各类功能需求及性能需求，是联系用户和开发团队的桥梁。需求规范当中潜在的缺陷会对整个系统的开发过程产生影响，如果这些缺陷在系统开发阶段不能及时地发现，很可能会导致列控系统在运行阶段失效，从而带来灾难性的后果。

为适应复杂安全系统设计开发需要，使系统需求规范更好地体现用户的需求，消除模棱两可的、容易引起歧义的描述，使相关各方容易理解规范的内涵，系统需求规范的开发正在从朴素的、非形式的设计方法，向着更加严格、更加形式化的方向转变。通过采用具有严格数学基础、精确数学语义的描述方法，使系统需求规范具有较高的可信度和正确性，能更好地满足用户要求，为后续的开发、设计和实现打下坚实的基础。

本书针对列车运行控制系统的特点，介绍了实现列控系统需求规范的严格建模与验证所必须的理论与关键技术，重点阐述了建立在 UML 和符号模型检验基础上的列车运行控制系统需求规范形式化建模和验证方法。作为应用实例，介绍了如何使用本书介绍的理论和方法对 CTCS－3 级列控系统规范中的模式转换功能进行建模和形式化验证。

本书各章的主要内容如下：

第一章论述了列控系统的发展趋势以及列控系统所呈现出的显著特点，强调列控系统规范和标准的重要意义。针对目前对规范建模和验证的方法，指出了基于严格数学基础的形式化方法是规范严格建模和分析的发展方向。

第二章对本书中系统需求规范建模与验证需要用到的概念、开发模型等基础知识进行介绍，包括系统需求规范概念、验证和确认概念、系统开发模型以及 UML 的背景知识和相关的模型检验概念和原理。

第三章论述列控系统需求规范的验证内容和体系，着重从需求管理、需求验证和需求跟踪这三个方面，提出需求规范严格建模与分析理论体系。

第四章论述了需求规范的管理的一般方法以及意义。

第五章从列控系统模型库的建立、传统的 UML 模型与扩展的 UML 模型三个方面，论述了列控系统规范的 UML 建模。

第六章主要论述了列控系统规范的形式化验证。首先给出 UML 模型到 NuSMV 的转换规则，然后重点从系统模型的约简、规范验证结果的分析，提出了形式验证的理论基础。

第七章综合前几章中介绍的理论基础，以 CTCS－3 级列控系统规范中的模式转换为例，说明规范验证的流程。内容包括：规范管理、UML 建模、UML 与规范的跟踪关系、SMV 模型、验证结果与反例跟踪。

本书的研究工作是在国家自然科学基金——铁道联合重点项目“列车运行控制及组织的基础理论与关键技术研究”（编号：60634010）、教育部“新世纪优秀人才支持计划”及轨道交通控制与安全国家重点实验室的资助下完成的，在此表示衷心感谢。

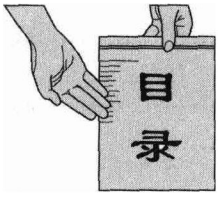
在本书的撰写过程中，得到了轨道交通控制与安全国家重点实验室（北京交通大学）和轨道交通运行控制系统国家工程研究中心大力支持和帮助。谢雨飞、唐武梅、刘金涛、曹妍、柴铭、李宪等研究生在本书撰著中发挥了重要作用，在此谨向他们表示衷心的感谢。

最后，对所有在本书的写作和出版过程中给予热情帮助和支持的朋友们表示感谢。由于作者水平有限，书中难免有不当之处，敬请同仁和读者不吝赐教。

作　者

2010 年 2 月

于轨道交通控制与安全国家重点实验室（北京交通大学）



第一章　概　　述 …… 1

第一节　轨道交通列控系统发展趋势 …… 1
第二节　列控系统规范验证的意义 …… 3
第三节　列控系统规范的建模验证方法 …… 6
第四节　列控系统规范的严格建模与验证体系 …… 12
本章参考文献 …… 15

第二章　系统需求规范建模与验证基础 …… 19

第一节　系统需求规范 …… 19
第二节　验证和确认的概念 …… 21
第三节　系统开发模型 …… 26
第四节　UML 基础知识 …… 34
第五节　符号模型检验 …… 44
本章参考文献 …… 56

第三章　列控系统的需求规范验证内容与体系 …… 58

第一节　列控系统需求规范验证内容 …… 58
第二节　列控系统需求规范验证方法体系 …… 66
第三节　列控系统需求规范验证流程 …… 72
本章参考文献 …… 74

第四章　需求规范的管理 …… 75

第一节　需求规范管理的概念与意义 …… 75
第二节　需求规范管理的任务 …… 78
第三节　需求规范管理流程 …… 83
本章参考文献 …… 88

第五章 列控系统的 UML 建模 …… 89

第一节 列控系统 UML 模型库 …… 89
第二节 列控系统规范的 UML 模型 …… 97
本章参考文献 …… 106

第六章 列控系统的形式化验证 …… 107

第一节 列控系统规范 UML 模型到 NuSMV 的转换 …… 107
第二节 列控系统模型的约简 …… 121
第三节 列控系统规范验证结果分析 …… 140
本章参考文献 …… 148

第七章 实例分析 …… 149

第一节 背景介绍 …… 149
第二节 需求规范管理 …… 153
第三节 CTCS－3 级系统需求规范的 UML 建模 …… 161
第四节 NuSMV 转换 …… 176
第五节 验证结果分析 …… 183
本章参考文献 …… 195

附录 A NuSMV 系统简介 …… 197
附录 B 系统开发模型介绍 …… 201

第一章 概 述

一个完善的列控系统开发过程必须从系统规范开始并依据规范进行，规范成为系统成功的起点和关键环节，如何保证规范的正确性，自然而言地成为一个核心问题。需求规范当中潜在的缺陷会对列控系统的开发过程带来重大的影响，这些缺陷如果在系统开发阶段不能及时的发现，很可能会导致列控系统在运行阶段失效从而带来灾难性的后果。对列控系统规范进行严格的验证，包括理解、形式描述（建模）和分析验证系统需求的完整过程，是消除规范的歧义性、非协调性的关键手段，对保障列控系统安全高效运行具有重要意义。

本章主要介绍了列控系统发展趋势和技术特点，讨论了列控系统规范验证的重要意义。回顾了目前对列控系统规范建模和验证的方法和实践，其中具有严格数学基础的形式化方法是当前研究发展的主要方向。

第一节 轨道交通列控系统发展趋势

列控系统是轨道交通信号系统的重要组成部分之一，其主要任务是控制列车运行的间隔和速度，保证列车安全、高效地运行。列控系统的发展已经历了机械设备、电气设备、电子设备等阶段。近年来随着无线通信技术的飞速发展，无线通信的可靠性、可用性大大提高。基于通信的列车运行控制（Communication Based Train Control，CBTC）系统已在高速铁路及城市轨道交通中应用，图 1－1 为典型的 CBTC 系统结构框图。

与传统的列车运行控制系统不同，CBTC 可以不再依赖轨道电路等进行列车定位，而是通过速度里程计、应答器等传感器实现列车测速定位，有效提高列车的定位精度。高性能的无线通信实现了车地间双向实时安全信息传输，后续列车可以前方列车尾部为目标点追踪运行，实现移动闭塞，有效提高列车运行安全性和效率。随着系统的功能和自动化程度不断增强，与轨道交通运输组织、车辆、牵引供电等专业的关系也越来越密切，已发展成为通过地面有线网、车地间无线网络覆盖列车运行所经的所有站点，对运行中所有运行的列

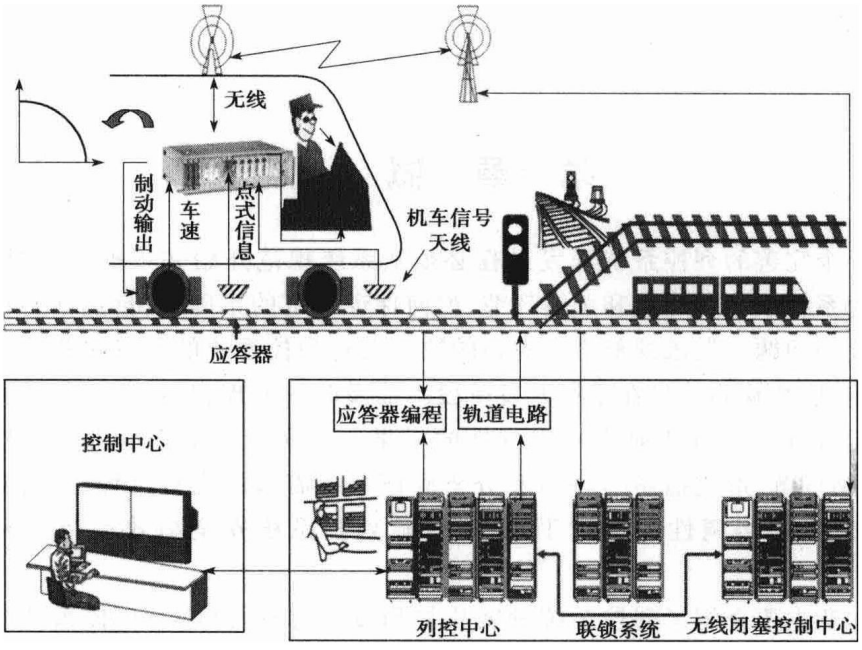


图 1-1 CBTC 系统结构框图

车实行全过程实时控制的复杂大系统。CBTC 有如下显著的特点[1]：

(1)系统化。信号系统不再是调度、联锁、闭塞、信号机等设备的一个简单组合，而是向集调度指挥、运行控制及自动驾驶为一体的功能完善、层次分明的自动化系统方向发展。

(2)网络化。通过地面局域网、广域网及车地间的无线通信网，将轨道交通的控制中心、车站及列车连成一个包含控制中心、轨旁及车载三级，覆盖轨道全线及所有运行列车，基于现代信息技术的复杂网络化控制系统，使地面区域列车控制中心、运行控制中心能够全面实时地了解辖区内的所有列车、车站及线路实时状况，实施安全、高效的调度指挥及运行控制。

(3)信息化。网络化使轨道交通的各类信息能够迅速上通下达，准确获得轨道交通系统运营的各类实时信息，在保证轨道交通系统安全、高效运营的同时，大大提高了维护、旅客服务水平智能化。

(4)通信信号一体化。通信技术在轨道交通信号系统中广泛运用，使通信信号趋于一体。

(5)智能化。智能化使调度指挥系统根据轨道交通系统的实际情况，借助先进的计算机控制技术来及时自动调整列车运行，实现列车自动驾驶(Auto-

matic Train Operation, ATO), 甚至全自动驾驶(Full Automatic Operation, FAO), 使整个轨道交通系统性能进一步优化, 提高运行效率, 大大减小了劳动强度。

第二节 列控系统规范验证的意义

规范是系统开发的起点和基础, 系统规范的缺陷将给项目成功带来极大的风险。美国专门从事跟踪 IT 项目成功/失败的权威机构 Standish Group 公布的 IT 项目成败原因的分析结果表明, 在项目成功的前 10 大因素中, 排在前 5 名的成功因素就有 4 项是与需求相关的。对于有问题的项目和失败的项目中引起问题出现的原因, 排在前 3 名的都是与需求相关的, 占引起问题原因的 1/3以上。尤其是航空航天、轨道交通、核电、医疗等领域的系统, 其失败往往会带来无法估量的人员和财产损失[2]。

随着列控系统的功能不断增强, 其与运输组织、车辆、牵引供电等专业的关系也越来越密切, 已成为一个连接控制中心、车站及列车, 覆盖整个轨道交通网络的复杂大系统。为实现不同厂商设备间、地面设备与车载设备间互联互通, 使列车能够在轨道交通网中跨线运行, 必须把列控系统的技术规范与技术标准作为系统研究的核心。

自 20 世纪 90 年代, 欧美各国为制定轨道交通系统的技术规范做了许多工作, 先后已制定多个有关轨道交通系统技术规范。在欧盟委员会的支持下, 由国际铁路联盟(UIC)、欧洲铁路信号工业界(UNSIG)和欧洲各国铁路当局共同研究的欧洲列车控制系统(ERTMS/ETCS)[3]规范自 1990 年开始已历时近 20 年, 整个发展研究过程可以分为 5 个阶段: 制定基本规范、评估与分类、测试与改进、标准化及应用推广, 并在应用推广中不断完善和充实。

美国电气电子工程师协会早在 1996 年成立了轨道运输车辆接口标准委员会(IEEE RTVISC), 已开发了 IEEE 1473[4]、IEEE 1474 等 10 个经认证通过的 IEEE 标准。

2002 年由欧洲城市轨道交通运营商、信号设备供应及教育机构共同组成一个 UGTMS 联盟, 在欧盟委员会资助下研究了城市轨道交通管理系统。UGTMS的宗旨是研究干线线路的 ERTMS/ETCS 技术规范在城市轨道交通中的适用性, 进而研究适于城市轨道交通运行控制系统的技术规范。

国际电工委员会(IEC)第九技术委员会(TC/9)的 WG39 小组正负责制定城市自动化无人驾驶系统的安全要求方面相应标准。WG40 小组则关注制定 CBTC 的完整标准, 包括功能需求、系统结构、子系统要求和接口规格。

上述各个标准规范之间的关系如图 1-2 所示。

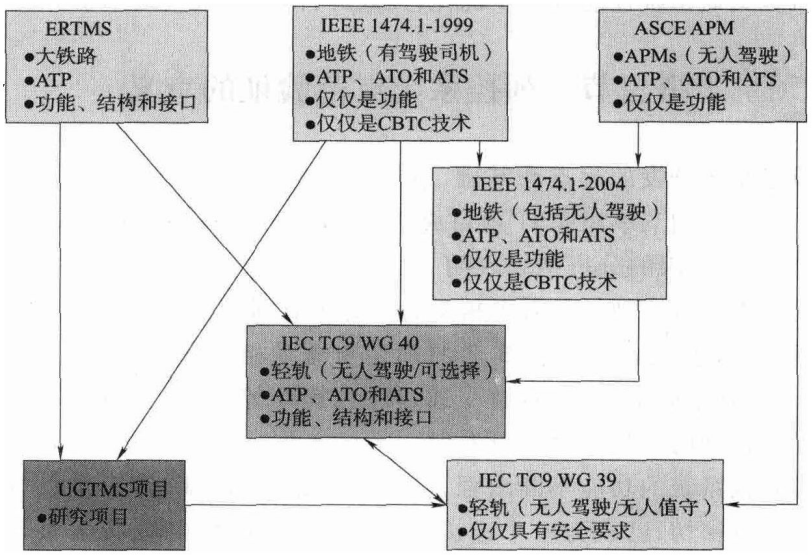


图 1-2 各种规范标准间的关系

ATO—列车自动运行，ATP—列车超速防护，ATS—列车自动监督。

近年来，国内逐渐开始重视列控系统规范的研究。铁道部在 2002 年提出发展中国列车运行控制系统（CTCS），实施引进和自主研发并举的发展战略，在消化吸收国外先进技术的同时，实现引进设备的国产化，发展 CTCS 系统。技术规范是轨道交通系统的核心，为保证我国轨道交通持续稳定发展，必须在借鉴欧美国家轨道交通系统相关技术标准的基础上，结合中国轨道交通需要，研究制定 CTCS 技术规范。否则，中国轨道交通列车运行控制设备将成为“万国博览会”，由此会带来设备安装维护、兼容性及系统升级换代等一系列问题，也难以发展具有自主知识产权的先进轨道交通运行控制系统。

信息技术与传统轨道交通信号技术的完美结合，使轨道交通列车运行控制系统的技术面貌发生了巨大变化。软件子系统及子系统分布结构一方面提高了轨道交通系统的整体安全性和使用效率，另一方面也正使列控系统的开发方法及系统安全设计策略发展变革，传统的标准规范也与之不相适应。

在铁路行业，对于安全相关的系统功能需求或者是具有高安全要求的操作场景，很多的国际标准，如欧洲电工标准化委员会（CENELEC）提出的欧洲铁路标准 EN 50126、EN 50128、EN 50129，以及国际安全苛求系统的通用标准 IEC 61508，均要求对系统需求规范的安全性进行评估，而且系统需求规范的评

估过程须由独立的监管机构来完成。然而目前面临的问题是,这些标准只规定了必须做的事情,但对于如何在具体的项目中实现这些要求,标准仅仅给出了很少的指导建议。因此在系统需求阶段,必须使用不同的技术和方法来描述系统以实现相关的安全策略。

另外,列控系统规范及其开发过程不仅要满足相关行业标准,而且要求所采用的方法、技术及理论对于系统需求规范开发过程所涉及的各个部门是易用和易于理解的。首先是作为用户的运营部门,以德国的铁路行业为例,该部门是"德国联邦铁路(Deutsche Bahn)"。它的职责是根据标准来制定系统需求规范,通常是通过行业开发商来实施,或者与开发商合作完成,此处的开发商即为第二个独立的部门。第三个重要部门是管理部门(或安全部门),职责是审查系统需求规范以确认其满足相关的标准。同样以德国为例,该部门为"铁路管理局(Eisenbahn-Bundesamt)"。但是他们通常将审查任务交与独立的评估机构来完成,参与审查的评估人员一般都是领域专家。在系统需求规范被接受之后,行业开发商以供应商的身份实现系统需求规范。但在此之前,他们必须了解用户的真正需求,对规范正确地理解,以便能够以系统设计规范(目标规范)的形式制定更为精确的需求。通过上述的过程,运营管理部门能确认开发商是否正确地理解了用户需求。因此,在列控系统需求规范的开发过程中,安全性不仅要被满足,而且要通过独立的审查机构的评估予以证明,这些安全证明是系统需求规范获得认可的基础。这意味着审查机构要清楚地知道安全性是如何被满足的,因此,所使用的方法和技术同时也要被评估人员所理解。

对于列控系统这样安全苛求系统而言,系统需求规范中的任何缺陷都有可能由潜在的风险演变成系统失效从而导致安全事故的发生。采用形式化的方法来描述系统需求规范,使得需求以唯一的方式被解释,从而排除了当自然语言被读者解释时经常产生的二义性。基于集合论和逻辑符号的描述手段使得工程人员能够创建清晰的关于需求的陈述。系统的正确性不是孤立的、绝对的概念,而是相对于给定的系统需求规范。形式化的需求规范描述,为进一步的形式化分析和验证提供了可能性。在需求阶段引进严格的形式化描述,就可以对早期成果进行分析和推理,为系统设计和实现打下更好的基础。应该注意的是,使用形式化方法来描述规范并不能完全消除规范文档里的问题。换句话说,如果需求文档里存在一个错误或一项疏漏,该错误或疏漏也很可能出现在抽象模型里。但是,通过对需求规范的形式化模型进行分析和验证,可以揭示出需求规范当中潜在的缺陷。从实用的角度来看,通常没有必要对系

统的每个方面都应用形式化方法，那些安全关键的部件是首选对象，然后才是那些不允许出错（出于商业理由）的部件。

对列控系统需求规范的验证包括理解、形式描述（建模）和分析验证系统需求的完整过程。形式语言虽然具有严格的语法和语义定义，可以准确地描述系统模型，但所包含的数学理论，限制了大多数设计人员的学习和使用。大多数的形式化语言和形式化验证技术对于设计人员来说，并不熟悉而且难以理解，因此造成了形式化方法实用方面的困难。在这其中，可理解性起了很重要的作用。首先，铁路行业的开发者一般都不具备形式化方法方面的背景，那么所使用的符号以及技术一定要易于理解，尤其是在团队开发中。其次，评估人员和监管机构一定要能够理解描述整个系统的模型和所使用分析验证技术。这也就意味着，他们必须熟悉并信任所使用的技术，例如，他们必须能够重现规范验证的过程。否则，他们将无法接受系统需求规范。对于开发商来说另一个重要的要求是方法的易用性。如果需要通过长期高强度训练的方式来引进新方法，那么这些新方法将难以被接受，方法的优点也将会被质疑。

基于这些原因，在对列控系统需求规范进行验证的过程中，必须考虑在现有方法中哪些是开发者熟悉的，哪些会在行业开发中变得越来越重要。采用基于统一建模语言（Unified Modeling Language，UML）的通用建模方法其优点是显而易见的，尤其是在团队合作中，各个成员都可以轻易理解系统模型。从工程师的角度来看，规范验证阶段使用的系统模型在设计阶段也具有重用价值。

第三节　列控系统规范的建模验证方法

规范建模与验证的途径是多方面的。首先对系统的需求分析要全面而准确，不能有任何实质性的漏洞，以便产生正确的系统规范。建立系统规范准确的模型，进行反复的模拟或仿真，是目前进行硬件设计规范验证的主要途径。但是一般来讲，模拟只能用典型的情况对系统进行考察，对系统进行穷尽的模拟是不可能的。在大型系统中，要模拟系统完全的行为可能要连续运行多年时间，这显然是不实际的。

形式化方法提供了规范验证的另一条重要途径。它用数学方法表达系统的规范或系统的性质，并且根据数学理论来证明模型满足系统的规范或具有所期望的性质。在不能证明所期望的性质时，则可能发现错误。形式化方法通过形式规范和证明来增强对系统的理解，从而发现用其他传统方法不能找

到的设计错误。大量实践证明,在计算机系统从上层规范到最终实现的过程中,采用形式化语言对于系统规范进行描述,选用合适的形式化工具,对于系统进行辅助设计和安全验证,可以在很大程度上减少由于系统开发人员造成的设计故障,提高系统的安全性[4~6]。近年来,形式化方法越来越显示出其优越性,已经在许多工业领域得到了成功的应用,比如航空航天[7,8]、电子仪器[9]、硬件[10]、医疗设备、核反应堆系统、保密系统、电信系统、通信协议、生产过程控制等等,典型的案例有 IBM 商用信息控制系统、英国伦敦空中交通管理、空中交通防碰撞系统 TCAS 等等。在列控领域同样有应用形式化方法的成功案例[11~17]。目前,国内外学者针对列控系统规范开展了富有成效的研究,主要代表性成果反映在以下五个方面。

一、规范的逻辑特性验证研究

列控系统表现出复杂的逻辑关联,其运行控制软件需要监测和控制列车地面设备状态,导致输入输出变量之间存在复杂的逻辑关系。规范的逻辑特性验证成为形式化验证的一个重要的研究内容。

迄今为止,逻辑特性的形式化验证存在较为成熟的方法和工具,代表性的模型检验工具如针对同步离散状态系统验证的 SMV[18],针对异步离散状态系统验证的 SPIN。在轨道交通信号控制中,规范的逻辑特性的形式化验证多集中在联锁设备的模型检验上,如 Eriksson 等提出使用形式化方法实现安全苛求系统的功能规范分析、设计和验证[19],文中介绍了直接证明安全特性的软件验证方法,利用 SMV 和 Lesar Moch 模型检验工具给出了 AZD Prague 公司开发的铁路联锁系统的形式化验证,并讨论了目前方法的优缺点和系统开发的测试阶段使用模型检验算法的可行性。Vicky[20]等利用符号模型检验能够自动穷尽式搜索系统状态空间,验证系统特性在所有的状态空间上是否满足的特性,检验中、大规模车站的联锁系统,查找潜在的异常行为,减少系统严重错误的发生,同时降低系统维护的代价。Banci 等提出利用 statechart 验证分布式联锁系统[21],给出如何利用分布式模型开发,确保整个联锁系统的基于形式化验证。

二、实时特性验证的研究

列控系统是一个实时控制系统,系统运行的正确性除了取决于系统能够做出正确的响应外,还取决于响应事件的顺序是否正确以及是否在规定的时间内做出响应。为此,在规定的时间内做出正确的响应,即系统的实时性验证成

为一个重要的研究内容。目前实时系统的验证分为即时性质(Instant Property)的检验和时段性质(Duration Property)的检验。即时性质的检验是检验实时系统在某一时间点上的性质;时段性质的检验是检验实时系统在某一时间区段上的性质。其中,Meyer[22]等提出时段演算(Duration Calculus,DC)公式转换为基于自动机语义的自动转换算法,从而极大地推广了可处理的 DC 逻辑子集。算法的思想是将 DC 描述的整体特性分解为独立的子特性(Sub-Properties),后者可以独立进行验证。文中将提出的算法应用于包含数据、通信和实时特性的欧洲列车控制系统(ETCS),验证了列车追踪中,前车出现事故的情况下,后续列车在规定的时间不发生碰撞的安全特性。Veloudis 等研究时段演算在安全苛求系统的安全规范和功能需求描述方面的有效性[23]。文中使用能够体现复杂和安全性能的铁路信号系统作为典型案例,说明了时段演算由于其描述系统的时段特征和直观语法构造的优点,成为系统规范描述的有效手段。Faber 等推广了 Meyer等提出的验证技术[24],将不变量检验和有界模型检验归约为复杂理论的证明(Proving in Complex Theories),提出有效的分层推理方法,并将提出的改进 CSP-OZ-DC 语言描述 ETCS 中无线闭塞中心(RBC)规范,给出经阶段事件自动机(PEA)转换后的模型检验和分层推理验证方法。

三、混杂系统特性验证的研究

对于列控系统来说,时间并不是系统中唯一连续变化的成分。由于系统中存在着除时钟外的其他连续成分,对这类系统的描述就需要采用比时间自动机更强的描述方法,即采用混杂系统描述和验证方法。

目前,列控系统混杂特性的形式化验证成为研究的热点。Platzer[25]引入一阶动态逻辑,提出针对一阶动态逻辑的顺序序贯演算(Sequent Calculus),用于包含离散和连续行为混杂程序验证,并将上述逻辑用于证明包含离散和连续变量的列控系统中速度监控的安全约束。Ferreira[26]等将自动验证引入地铁控制软件的开发,利用有界模型检验(Bounded Model Checking,BMC)和归纳证明用于预测控制软件中的错误。Jacobs[27]提出分级推理用于验证复杂系统的特性,使用局部定理展开链(Chains of Local Theory Extensions)建模 ETCS 案例。文中给出如何将测试不变量和有界模型检验自动归约为建立在基集理论(Base Theory)上的公式可满足性。Platzer[28]结合一阶动态逻辑和时态逻辑,提出微分动态逻辑,支持包含一阶可定义流和离散、连续演化的混杂系统验证。在此基础上,文章提供了模块验证演算,将混杂系统的时态行为化简为非时态推理。文中利用上述逻辑演算,分析列控系统的安全不变量和参数安全

约束。

交通领域联合研究中心联合 Freiburg、Oldenburg 和 Saarbrücken 的研究力量,致力于复杂系统自动验证分析(Automatic Verification and Analysis of Complex Systems,AVACS),尤其是交通运输复杂系统的分析与自动验证。他们从三个方面开展混杂系统的验证研究。H1 研究小组——Deduction and Automata Based Approaches(演绎和基于自动机方法)关注求解整数和实数域上的一阶约束技术及其在混杂系统分析中的应用。此研究小组已经增强不同、互补的约束解程序,其优化算法和数据结构大大低于内存需求[29]。H1 子研究计划组和研究小组 H2——混杂数值符号技术,研究数值不确定部分的稳健约束[30,31,32],简化概念和度量距离(Metric Distance)的推理,以及在自动抽象方法中使用混杂符号、数值约束解,从而在基于抽象验证中[32],通过计算特定精简(concise)抽象,降低了状态空间爆炸问题。

H2 研究小组,命名为有界模型检验和归纳混杂系统验证(Bounded Model Checking and Inductive Verification of Hybrid System),处理分类的、无量词约束逻辑的满足性检验,并将其用于有界模型检验和自动归纳混杂系统验证的优化。他们推广目前的 SAT(可满足性)求解技术,并近期开发了一个完全基于 SAT 技术、处理非确定数学中涉及 transcendental 函数的大的约束集合(成千个实数和布尔变量)的验证方法。

H3 研究小组—Automatic Abstraction of Hybrid Controller 研究大规模混杂系统的分解,将组合推理(Compositional Reasoning)和自动抽象(Automatic Abstraction)应用于离散模型验证,从而降低混杂系统验证的复杂性[33]。

H4 研究小组—Automatic Verification of Hybrid System Stability 着重自动构建混杂系统的稳定和收敛证明。李雅普诺夫函数(Lyapunov Function)和权重函数已广泛用于证明稳定性和收敛性,但是缺乏自动执行的能力。H4 研究小组试图解决上述问题,并将其集成在一个统一的框架内。线性矩阵不等式方法,组合状态空间的自动分割[34],和基于分支松弛算法可以构建多项式自由度(Polynomial Degrees)的类李雅普诺夫函数(Lyapunov-like Function)。另外,文[35]提出的方法表明:通过自动分解和构建线性权重函数,可以自动分析一类混杂系统的活性。

四、随机特性验证的研究

列控系统固有的随机特性使得验证其概率特性成为形式化分析的一个重要内容。目前,列控系统的随机特性分析的研究工作集中于 Petri 网的形式化

分析[36,37]。Petri 网属于基于网络的形式化分析方法，根据网络中的数据流，显式地给出系统的并发模型，能够有效描述系统中的并发、同步、冲突、竞争等特性。

另外，随机模型检验方法和工具，在符号模型检验的基础上，将用于逻辑检验的二叉判决图（BDD）推广到描述实数域的多端点二叉判决图（MTBDDs），使得检验在规定的时间、以规定的顺序响应事件的概率特性成为可能。代表性的工具如英国伯明翰大学研制的 PRSIM 概率模型检验平台[38]。

五、形式化验证集成的研究

列控系统的上述特性并不是独立存在的，而是构成不可分割的整体。单独使用一种或几种形式化方法不能涵盖列控系统的多种特性，而且未经集成的几种形式化方法会导致规范的不一致。例如，如果列控系统，部分采用行为描述语言，部分采用基于状态的语言，若无清晰的语义说明这两部分是如何交互的，最终导致规范的不一致。因此，研究组合列控系统各种特性集成的形式化方法是一个重要方向，也是未来形式化方法领域的一个主要发展方向。目前形式化集成的研究有如下几个方面：

1. 基于 UML 的形式化集成研究

Knapp 等提出一致性的模型检验工具 HUGO/RT[39]，自动验证由时间约束 UML 协作图（Collaboration）描述的场景与时间 UML 状态机（Timed UML State Machine）实现的一致性。HUGO/RT 将 UML 时间状态机模型编译成时间自动机，并将时间协作图转换为观察器（Observer），使用 UPPAAL 模型检验工具进行一致性验证。文中将提出的工具应用于典型案例——推广的铁路道口（Generalized Railroad Crossing, GRC）的安全特性的验证。Trowitzsch 等提出 UML 状态机到确定随机Petri网的映射规则[40]，补充了 UML 缺乏定量分析的缺陷。通过 ETCS 通信链路分析，验证了提出方法的有效性。Hermanns 等通过组合时间、随机和概率自动机语义和 I/O 自动机语义，将 UML 中的 STATECHART 推广为随机 STOCHARTS，利用 STOCHARTS 与基于代数的形式化进程语言 Modest的语义映射，使用 MOTRO/MOBIUS 工具验证 Modest 描述的系统性能。文中使用 STOCHARTS 建立了 ETCS 中 GSM-R 设备的 QoS 规范简化模型，给出 GSM-R 通信可靠性能、延迟概率和列车速度、位置报告周期等参数对通信性能影响的分析与验证。Marcano 等提出时间扩展的 B 语言与 UML 的集成，前者为后者提供精确的形式语义，利用 B 工具验证 UML 图的一致性。文章上述的集成方法成功应用于平交道口的规范建模和精化[41]。

2. 基于故障树的形式化集成研究

Görski [42]引入特殊的时间迁移系统和一阶谓词逻辑，Dugan[43]等引入马尔可夫模型解决故障树的歧义性。Buuns 和 Anderson[44]使用 μ 演算语义检验形式化系统模型的有效性。Hansen[45]给出故障树的时段演算语义，利用故障树分析推导给定故障树的安全需求，但是并没有考虑是否所构建的故障树的正确性。在 FORMOSA 工程[46,47]中，考虑时段演算、CTL(计算树逻辑)和 ITL(积分时态逻辑)的语义，并使用离散时间模型检验工具 Raven[48]和 SMV，并给出案例的故障树分析。ESACS 项目组[49]将故障树分析和模型检验应用于不同的领域，研究故障树产生测试案例，将描述故障树模型的自动机编译成布尔公式，进一步开发从 statemate 模型到故障树的自动生成工具，但是工具没有考虑时间和事件顺序。Schäfer 等[50]利用带有活性性质的时段演算逻辑(Duration Calculus with Liveness，DCL)，给出嵌入实时特性和事件的故障树分析语义，通过将故障树对应的时段演算公式转化为 Phase 自动机，使用 Moby/DC 完成模型检验，验证故障树分析的完备性和正确性。文中对列控系统进行故障树形式化分析，验证在一定实时条件下的系统安全特性。

3. 基于 Z 语言的形式化集成研究

为建模复杂系统的组件之间通信，组件内的状态转换，通信和状态迁移的实时约束等特征，文献[51,52,53]提出组合通信顺序进程(CSP)、面向对象的 Z 语言(OZ)和时段演算(DC)组合的 CSP-OZ-DC 规范语言，用来描述复杂实时系统的规范需求。Faber 等在形式化描述方面，将 CSP-OZ-DC 规范描述语言进行了如下两方面的推广[54]：第一，使用抽象数据结构表达和描述系统构件数量参数(即无限数据类型 infinite data type)，从而得到更为一般性的验证结论；第二，引入时间参数指代 OZ 数据结构中的时间常数，使得描述时间约束更具灵活性。在模型验证方面，Faber 等推广了 Meyer 等提出的验证技术[55]，将不变量检验和有界模型检验归约为复杂理论的证明(Proving in Complex Theories)，提出有效的分层推理方法，并将提出的改进 CSO-OZ-DC 语言描述 ETCS 中 RBC 规范，给出经 PEA 转换后的模型检验和分层推理验证方法。

4. 集成规范管理和形式验证的研究

欧洲的 RINA，Fondazione Bruno Kessler 和 DR. Craband&Partner 联合开发了 ETCS Tool，实现 ETCS 规范的建模和验证[56]。ETCS tool 的结构是在 Rational Software Architect(RSA)的基础上建立起来的。RSA 是一个集设计、管理、商业开发和团队服务为一体的综合设计平台。在 ETCS Tool 工程中，RSA 还能够联合使用其他的工具，以扩充 ETCS 规范验证过程中所需要的功能。比如 Req-