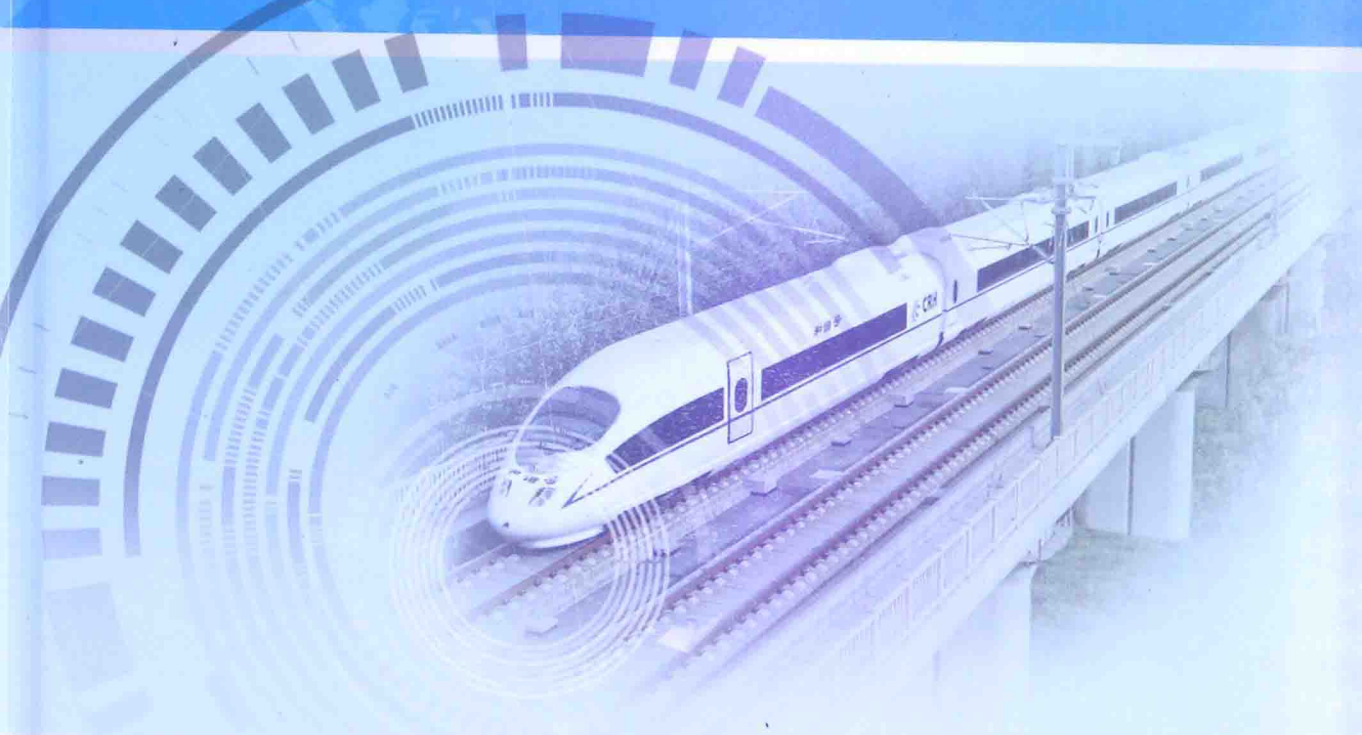
JIYU MOXING DE LIECHE YUNXING KONGZHI XITONG SHEJI YU YANZHENG FANGFA



基于模型的列车运行控制系统设计与验证方法

唐涛 赵林 徐田华 吕继东 牛儒 张路 著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

铁路科技图书出版基金资助出版

基于模型的列车运行控制系统设计与验证方法

唐　涛　赵　林　徐田华
吕继东　牛　儒　张　路　著

中　国　铁　道　出　版　社
2014·北　京

内 容 简 介

本书主要介绍基于模型的列车运行控制系统设计与验证方法，着重阐述设计与验证方法的原理、实现技术以及应用。全书共六章，主要内容包括：列控系统需求的建模与验证，列控系统的安全分析，基于模型的列控系统软件设计，基于模型的测试，列控系统的运行时验证。

本书可以作为轨道交通控制专业研究生的学习用书，也可以供有关工程技术人员参考。

图书在版编目（CIP）数据

基于模型的列车运行控制系统设计与验证方法/唐涛等著．—北京：中国铁道出版社，2014.3

ISBN 978-7-113-15929-0

Ⅰ.①基… Ⅱ.①唐… Ⅲ.①列车—运行—控制系统设计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（2012）第 318890 号

书　　名：基于模型的列车运行控制系统设计与验证方法

作　　者：唐　涛　赵　林　徐田华　吕继东　牛　儒　张　路　著

责任编辑：崔忠文　李嘉懿　**电话**：（010）51873146　**电子信箱**：dianwu@vip.sina.com

封面设计：郑春鹏

责任校对：胡明锋

责任印制：陆　宁

出版发行：中国铁道出版社（100054，北京市西城区右安门西街 8 号）

网　　址：http://www.tdpress.com

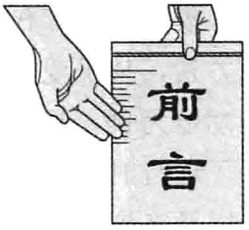
印　　刷：中煤涿州制图印刷厂北京分厂

版　　次：2014 年 3 月第 1 版　　2014 年 3 月第 1 次印刷

开　　本：700 mm×1 000 mm　1/16　**印张**：13.25　**字数**：240 千

书　　号：ISBN 978-7-113-15929-0

定　　价：45.00 元



高速铁路作为当代高新技术的集成，具有输送能力大、速度快、安全性高、正点率高、占用土地资源少、能耗低、环境污染小、全天候运行的特点，是交通运输体系中具有可持续性和环境友好性的运输模式。

高速铁路列车运行控制系统融入了先进的计算机、通信以及控制技术，系统的自动化程度、控制精度以及响应速度得到大幅提升。列车运行控制系统已经不再是调度、联锁、闭塞、信号机等设备的简单组合，而是向集调度指挥与运行控制为一体、功能完善、层次分明的综合自动化系统方向发展，呈现系统化、网络化、智能化及通信信号一体化的特点。

本书针对轨道交通列控系统的发展历程和特点、传统开发方法面临的挑战，分析总结了基于模型的设计与验证方法的优势。在需求层面，针对列控系统的信息－物理融合属性进行了建模和形式化验证，使用的模型包括扩展 UML 模型、混合通信进程（HCSP）模型以及混成自动机模型。并进行了系统安全分析，论述了经典安全分析方法和应用，重点介绍基于模型的安全分析技术。在设计构造环节，论述了基于模型的列控系统软件设计方法，基于 SCADE 和基于 DSL-R 的开发工具和实例。对于列控系统测试，介绍了基于模型的测试用例自动生成方法，结合观测自动机理论进行了列控系统车载设备测试用例自动生成，并搭建了适合于 CTCS-3 级列控系统车载设备的互联互通测试平台。作为运行阶段的安全保障技术，主要介绍运行时验证技术，其核心是监控需求的精确表达和监控器的生成。

全书共六章。第一章为绪论。第二章针对列控系统混成特性的建模需求，利用 UML 扩展方法和混合通信进程（HybridCSP）方法从工程应用和精确分析的角度描述列控系统相关运营场景，并结合混成自动机理论，验证了列控系统的关键安全特性。第三章围绕轨道交通系统开发过程中的安全分析过程，主要介绍国际上最为推崇的失效传播模型、故障注入和混合建模三种基于模型的安全分析建模思路；并且，阐述了每一种思路的典型方法和工具；最后分别以 CBTC 系统和 CTCS-3 级列控系统为例展示了该方法的应用。第四章论述了基于模型的列控系统开发方法、工具和具体的列控系统设计案例，着重阐述基于

SCADE 的同步设计语言，基于领域建模语言的列控系统元模型、模型转换和代码生成方法。第五章介绍基于时间自动机模型的列控系统建模方法，基于观测自动机的测试准则与测试算法；并以列控系统典型的模式转换功能为例，阐述在不同覆盖准则下模式转换测试案例的自动生成。第六章讨论了运行时验证的基本原理、应用背景，详细阐述 LTL 的预测语义和多值语义，以及在这两种语义的基础上发展起来的两种不同风格的监控方法：基于自动机的监控和基于公式重写的监控；最后，通过两个列控领域的实例演示了在领域应用中关键监控特征提取和监控实施过程。

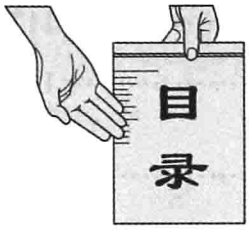
本书是在国家高技术研究发展计划（863 计划）项目“面向信息－物理融合的系统平台”子课题——“轨道交通 CPS 系统的感知、运行和安全技术应用验证”以及北京交通大学轨道交通控制与安全国家重点实验室的资助下完成的。在本书的撰写过程中，还得到了北京交通大学轨道交通运行控制系统国家工程研究中心大力支持和帮助，在此一并表示衷心的感谢。

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

2013 年 6 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 绪 论

本章主要介绍列车运行控制系统及其开发方法的发展趋势，讨论列控系统的研究现状，总结了列控系统规范建模和验证的研究方法，指出列控系统建模的研究发展方向。

第一节 列车运行控制系统

自19世纪铁路诞生以来，科学技术日新月异，工业领域先后经历了机械化、电气化、信息化三个发展时期。列车运行控制逐步从机械控制、电气控制发展到计算机控制。1804年世界首条铁路在英国运营的开始，就产生了如何控制列车间隔以保证行车安全的问题，从而产生了行车闭塞法。为防止列车相撞，在线路上安装各种信号设备。通过地面信号显示系统，以物体大致形状、灯光的数目和颜色等视觉信号或音响等听觉信号给司机以各种运行条件的指示，提醒司机采取相应的措施，以免发生列车正面冲突和追尾事故。1832年，美国开始在车站上设置信号机，为站与站之间传送信息。这一时期，主要是依靠信号工的眼睛观测，通过人控制的信号给司机传递行车命令，由信号工控制列车间隔。列车完全由司机驾驶，并负责列车的运行安全。

1872年，美国人鲁宾逊发明了轨道电路，实现了列车占用钢轨线路状态自动检查。利用轨道电路检查列车占用轨道的状态信息控制信号显示，由此出现了地面自动信号，使地面信号显示能真实反映线路空闲状态。列车的间隔调整采用半自动闭塞或自动闭塞，地面信号显示仅仅指明列车前方线路状态，列车完全由司机驾驶，安全掌握在司机手中。

以地面信号显示为主的铁路信号系统只是向司机提供地面视觉信号。但由于地面信号显示有时受到自然环境（如雾、风沙、大雨等）的影响以及地形的限制，司机往往不能在规定的距离上及时瞭望前方信号机的信号显示，因而存在冒进信号的危险。为将列车运行前方所接近信号机的显示情况及时通告司机，发明了机车信号设备，将地面的视觉信号通过技术手段引入司机室，这样

司机就能够在任何条件下从容地驾驶列车,且当前方信号为禁止信号时能及时采取制动措施,提高了列车运行的效率和安全程度。需要指出的是,在以地面信号为主体信号的信号系统中,地面信号显示仍是行车凭证,机车信号只是地面信号的复示信号。

无论地面信号还是机车信号都只能确保显示正确可靠,提醒司机及时采取措施,无法防止由于司机失去警惕而发生危及列车运行安全的事故。因此,人们又研制了列车自动停车设备,其功能是当地面信号的"禁止命令"未被司机接受时就自动实施紧急制动,强迫列车停车。尤其是电码化轨道电路的出现,使得利用轨道电路向机车传送信息成为可能,地面轨道电路、机车信号与自动停车装置结合,构成简单的列车运行自动控制系统(简称列控系统),当"禁止信号"未被司机接受及时停车时,自动停车装置就自动实施紧急制动,强迫列车停车。这样,列控系统不再只是指明安全运行条件,列车的安全由设备和司机共同保证。

20 世纪 60 年代后,高速铁路的发展给列车运行控制提出了更高的要求。传统的以地面信号显示传递行车命令,司机按行车规定操纵列车运行已不能满足要求。行车控制逐步由地面信号显示传递行车命令的阶段,发展到由车载列车超速防护设备给司机显示地面发送的信息并自动监督列车运行的阶段。现代列控系统是根据列车在线路上运行的客观条件和实际情况,对列车运行速度及制动方式等状态进行监督、控制和调整的技术装备,确保列车以安全的速度高密度运行。列控系统包括地面设备与车载设备两部分,地面设备提供监控列车所需要的允许速度、行车许可等基础数据;车载设备将地面传来的信息进行处理,形成列车速度控制数据及列车制动曲线,监控列车安全运行。

列控系统在迅速发展的电气、电子、信息及自动化技术推动下,功能不断增强完善、自动化程度不断提高。传统的列控系统与基于计算机的列控系统性能对比如表 1 - 1 所示。计算、通信以及控制(3C)技术的广泛应用与融合是列控系统发展的趋势,新技术所占比重的增加为满足更复杂的运营需求带来了便利和效率,但也为系统的安全性带来了前所未有的挑战。系统需求完备性缺失、开发设计过程中系统错误客观存在、复杂多变的外界运行环境、软硬件的故障耦合和人员操作失误等因素,导致列控系统发生错误的概率大为提高,关键设备故障而引起的灾难性事故时有发生。例如:2007 年 10 月 16 日,发生在德国弗鲁蒂根地区的勒奇山基底隧道附近的列车脱轨事故,该脱轨事故是由于 ETCS-2 级列控系统的无线闭塞中心(RBC)接入时一个与列车移动授权延伸的相关软件错误而引起的。2011 年 7 月 23 日发生在中国的"甬温

线”两辆动车追尾事故，事故的主要原因之一是列控中心设备中的自检模块存在严重设计缺陷。

表 1-1 不同时期列控系统特性对比

基于继电器的传统列控系统	基于计算机的现代列控系统
故障安全继电器	半导体管、计算机
故障率不对称器件	故障率对称器件
不需附加措施即可构建安全系统	需采用自检、表决等措施才能构建安全系统
纯硬件：分离元件	硬件：大规模集成电路 软件：结构复杂、规模庞大
容易审核、测试	难以审核、无法完备测试

安全是一种相对于危险而言的系统状态，系统安全实际上是指系统所面临的风险被控制在可接受的范围之内。在轨道交通行业，系统的安全性通过其可接受的风险来量化表示。列控系统的安全性受多方面因素的制约，包括系统功能的复杂程度，软硬件的可靠性，容错结构，开发人员对安全需求正确理解和分析的能力、正确实现的能力，对风险的控制能力，系统开发过程和管理水平等。使用传统的开发方法越来越难以应对由于系统复杂性带来的诸多问题。

第二节 列控系统开发方法的发展趋势

一、列控系统开发过程

现代列控系统是一种涵括计算、网络和物理环境的复杂安全相关系统，通过 3C 技术与铁道信号技术的有机融合与深度协作，实现列车安全、正点、高密度的运行。列控系统开发流程包括需求、安全分析、设计、实现和测试等关键开发环节，如图 1-1 所示。

需求阶段的任务是确定设计任务和设计目标，并提炼出系统需求规范，作为正式设计指导和验收的标准。系统的需求一般分功能性需求和非功能性需求两方面。功能性需求是系统的基本功能，如超速防护、等级转换等。非功能需求包括系统的性能、安全性、可用性等指标。在列控系统需求规范的开发过程中不仅要满足安全性，而且要通过独立的审查机构的安全评估予以证明，这些安全证明是系统需求规范获得认可的基础。铁路行业安全相关需求的分析仍然过度依赖于领域知识和专家经验，缺乏与实际开发流程匹配的实用技术手段与支持工具。

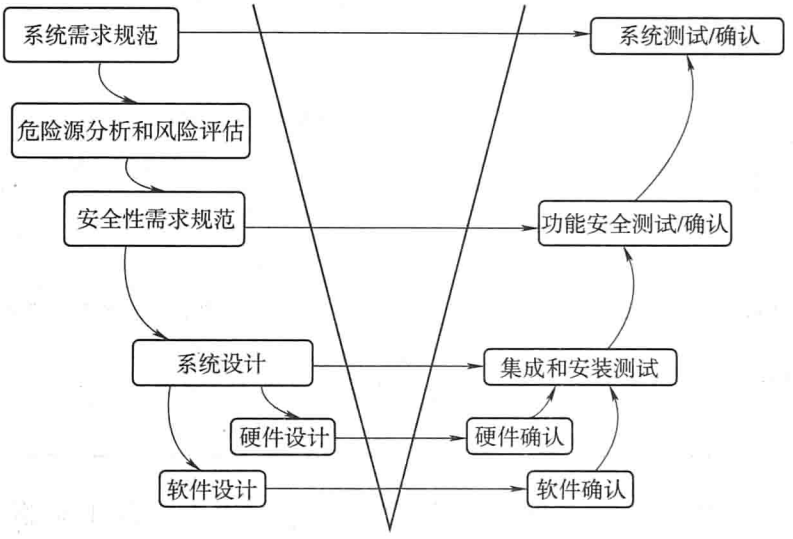


图 1-1 列控系统开发流程

为了使系统的设计在安全上达到可以接受的水平,要求在开发过程中识别、分析和评价系统的危害,把这些危害消除或控制在可接受的范围内,以使系统能够正常运行并保证安全。系统安全分析的工作就是在整个系统寿命周期内,发现、识别、消除或控制危害,这是安全苛求系统开发过程中的一个重要程序和核心组成部分。系统安全分析通过对系统的全面分析,找出系统存在的危险性,估计事故发生的概率及其对人员产生伤害和造成设备损失的严重程度,从而为采取防范措施、预防事故发生提供依据。

设计阶段描述如何实现系统的功能和非功能需求,包括对硬件、软件的功能划分。好的体系结构是设计成功与否的关键,基于体系结构对系统的软件、硬件进行详细设计和编码,最后进行验证和确认(Verification and Validation, V&V)。把系统的软件、硬件和执行装置集成在一起进行调试,发现并改进单元设计过程中的错误。在过去的 20 ~ 30 年间,系统开发经历着从简单、小规模向复杂、大规模演化,验证和确认方面的工作在开发过程中所占的比重逐渐增大。在整个的系统开发周期中将 V&V 当作独立的过程来对待,覆盖了整个系统生命周期,由系统开发中的独立组织来实施。在列控系统的开发中,V&V 与安全评估的关系越来越密切,是支持安全认证的一个主要因素。

国际上在安全苛求系统的设计开发中引入形式化技术是一个趋势,这类技术可以用在开发过程中的各个阶段。根据用户实际需求生成形式化的系统需求规范,然后对需求规范进行验证,判断其是否满足用户的意图、是否存在不一致和不完整等错误、是否具有所期望特性。之后,以规范为基础,对其进

行逐步精化，每一步精化都降低一些抽象程度或增加了一些设计细节，最终得到可执行程序代码。在精化的过程中，需要保证各步精化所得结果之间的一致性。理论上，只要有一个正确的满足用户需要的形式化规范，经过一系列的程序变换后，应该能生成正确的、可以接受的代码。严格的形式化方法可以最大限度地保证开发过程的质量，尤其适用于安全苛求系统的开发，同时，可以改善开发效率、有效控制开发进度。在列控领域，巴黎地铁 14 号线是将 B 方法（B 方法是一种软件开发方法）用于工业领域实际开发的一个成功案例。但从目前的现实来看，完全的形式化开发在实用方面还存在困难，尤其是开发人员的培训方面。

传统的开发方法对解决列车在高速度、高密度下安全可靠高效运行，避免安全事故的发生等一系列重大问题上存在很大的局限性和被动性。例如：众多的人工环节可能产生不可预料的设计缺陷。另外，由于缺乏可执行规范，在开发过程前期无法进行连续、增量式的验证和确认。而系统级的测试一直要到在软件或硬件中实现完成后才能执行，后期的测试不能及时发现和消除所有潜在的缺陷，导致系统的质量和安全性不能得到保障，同时延误了开发周期、增加了开发成本。信息技术正在经历着新的变革，如“云计算”、“无线传感网”、“物联网”、“信息物理系统”等技术的出现与发展。新技术的出现一方面提高了列控系统的整体安全性和使用效率，另一方面也必然促使列控系统的开发方法及系统安全设计策略发生巨大的改变。

二、基于模型的开发

如何切实有效地提高列控系统设计研发质量，缩短开发周期，降低设计成本，保证列控系统持续安全地运行，是摆在相关工程和科研人员面前的一个突出问题。面对这样的挑战，学术界和工业界都提出了很多新的方法，其中最突出的一个是基于模型的开发。当模型成为系统开发过程不可或缺的一部分，这种模型的使用特征被称之为基于模型的（Model - Based）。

基于模型的开发过程利用模型来实现对复杂系统的掌控，通过模型和算法提高开发过程的自动化程度，降低人为引入的缺陷和错误。通过使用模型进行更准确的需求分析以及早期的验证，这使开发人员能够在开发过程中更早、更多地发现缺陷。从通过建模分析来验证需求到设计实现和测试，模型是开发过程的真正核心。模型在整个开发过程中不断被细化，与自然语言形式的规范相比，模型能使开发人员更深入了解真实设计意图的动态表现。基于模型的开发支持不同抽象层次的设计、仿真、自动代码生成，以及在开发的各

个阶段进行连续测试、仿真和验证。在开始编码之前的很长时间就对模型进行验证和测试,可以确保需求的完整性和正确性。自动代码生成避免了手工拼写错误和对设计的误解,同时基于模型的测试案例自动生成可以让开发人员获得基于需求并可重用的测试用例。

IEC 61508 和 EN 50128 等国际安全标准提出了安全苛求系统需要满足特定安全完整度等级(Safety Integrity Level,SIL)的概念,系统所能达到的安全完整度等级,不仅体现了系统硬件环境的可靠性指标,也能反映出开发过程中所使用的分析、构造与验证技术,更体现了系统规避与容忍风险的能力。为了保证最终产品达到 SIL4 级(最高等级)标准,基于模型的安全分析、需求确认、设计实现、测试验证方法在上述行业标准是强烈推荐采用的。一些著名的 IT 公司,如 IBM、Microsoft、Mathworks、ESTEREL 等都在积极推动基于模型开发方法的研究和产品的实现。国外高校和研究机构,如卡耐基梅隆大学,奥登堡大学等均致力于基于模型开发的关键环节的前沿理论和技术研究。基于模型的开发已成为国内外研究的热点和未来安全相关系统开发的主流方向。

(一)模型的本质与特征

模型是对客观事物、过程或概念的一种抽象表示和体现。模型过滤了许多非本质的细节,从而突出了复杂问题的本质,这样就使问题更容易理解。建模和抽象是人类解决复杂问题的一种常用手段。在学术界和工程技术领域,模型的概念被广泛地使用,为了研究一个过程或事物,可以通过在某些特征(行为或结构等)方面与它相似的“模型”来描述或表示。模型可以是所研究对象的实物模型,如建筑模型、教学模型等;也可以是对象的数学模型,如公式或图形等。它能反映出有关因素之间的关系。

对于计算机系统而言,模型就是以某种确定的形式(如文字、符号、图表、实物、数学公式等),对系统某一方面本质属性的描述。建模的过程就是对研究的实体进行必要的抽象,并用适当的形式或规则把所关心的主要特征描述出来。同时,建模也是一个层次化的过程,在建模过程中的每一个抽象层次可以采用不同的视点和表达。模型的表达形式是多样的,每种表达方式与建模的目的紧密关联。在某个领域,模型可能是一个代数方程组,而在另一个领域,模型很可能是一个仿真程序,即便是对于相同的建模对象,模型也可以以不同的形态存在。例如:模型可以是白纸上画出的图案或建模工具中的图形,用来充当交流的媒介;也可以是规范的 XML 文档,用于存储和计算机辅助分析。

基于模型的开发是一种以模型作为主要工件的高级别抽象的开发方法。

模型用于表示系统的功能、结构和行为等不同方面。在需求、分析、设计、实现、测试和运行维护等不同阶段都会存在多种模型。在基于模型的设计和验证中,经常使用图形化的模型,如 UML 和各种自动机模型。但模型并非只能是图形化的,也可以使用文本或其他方式来表示,如一阶逻辑模型、CSP 模型,这些模型在开发过程中服务于不同的应用目的。模型忽略系统逻辑行为的复杂底层实现,而直接展现问题域。建立模型便于捕获领域知识和进行知识管理,可以加强领域专家对系统开发过程的直接影响。

模型有助于理解问题,便于沟通以获得对系统的某些方面具有更加准确、清晰的认识。模型还能借助计算机进行辅助分析和设计,能够使设计更清晰,系统更具可维护性。基于模型的开发将复杂的业务逻辑和最佳实践经验封装在模型中,并将这些模型应用到开发,代码生成,测试和维护当中,通过建模将开发工作抽象到更高的层次。不同的模型在列控系统开发过程中的各个关键环节发挥其各自不同的作用。模型要能真实的反映客观事物需要一个论证的过程,这就要求模型的建立过程是严谨的,并且结果是可追溯和验证的。

(二)开发效率的提升

在传统开发流程中,需求、设计、实现和测试任务在不同的工具环境下依次执行,其中涉及多个人工步骤。不同类型的设计和分析工作使用不同的专门工具实现,然后人工将设计转换成代码,而系统级测试要到软件和硬件实现完成后才能执行,这是个耗时且容易引入缺陷的过程。缺少公用工具环境、多个人工步骤以及后期才能发现缺陷等因素都会延长开发时间、增加开发成本。

基于模型的开发方法一般利用形式化的系统描述语言和建模技术更加科学、严谨地发现系统潜在危险,并推演、分析危险事件的可能致因因素。在此基础上借助计算机的高效处理能力,代替繁复、单调的人工计算处理过程,从而提高分析设计工作的效率、准确性和完备性,使之能够更好的配合列控系统的开发规模和开发进度。

以安全分析过程为例,传统的安全分析方法大都是从工程实践中总结提炼出来的程序化方法。这些方法原理简单、容易掌握,且有成熟工具予以辅助。但是,推演或归纳的过程仍需要人工完成,要求使用者具有丰富的专业知识和经验,以及较强的逻辑推理能力,否则无法满足大规模复杂系统的需要。随着系统复杂程度的提高,出自分立元件设备分析经验的传统安全分析方法逐渐显现出他们的不足。传统安全分析方法,如 FTA、FMEA 等通常使用自然语言描述系统行为和失效,而且往往对于其语句的句型结构和语法结构不加任何约束,安全工程师完全根据自己的经验和当时的思维组织语句。这样的

语句往往不能准确描述系统，甚至遗漏重要的约束、条件信息。而基于模型的安全分析方法定义了明确、清晰、严谨的语法和语义，消除了自然语言可能带来的歧义，而且能够保证语义的完整和语法的正确。方便不同开发成员之间的交互，以及模型的检查和更新。基于模型的安全分析过程可以实现高度的自动化，从而使安全工程师从大量繁杂的计算、整理工作中解脱出来，将工作重心放在系统特性的分析和理解上。另一方面，自动化的分析过程和标准化的输出也节省了安全分析的时间成本和人力成本，能够更好地配合系统的工程周期。

（三）系统质量和安全性的提升

在基于模型的系统开发过程中，开发中心从代码转变为高抽象级别的模型，通过基于模型的分析与验证、模型转成、基于模型的测试等手段来提高开发过程的自动化程度，保证系统的质量和安全性。基于模型的设计与验证方法由于采用了清晰定义的描述语言和计算机辅助分析工具，与传统开发方法相比，它的描述能力和分析方式都发生了巨大变革。

需求与代码分离的发展趋势，使得需求的有效沟通、需求规范化、需求的验证与确认等问题变得更加突出，制约着开发过程。在需求层面应用模型要能够清楚地描述系统需求，并且能够将需求模型转化为计算机能够理解的模型。系统需求的确认和验证是安全苛求系统主要关注的问题，铁路行业欧标 EN 50128 和 EN 50129 明确要求在设计和集成的每一阶段需对系统进行验证和确认工作，它贯穿在整个开发过程。在以代码为中心的传统开发方式中，只有在开发阶段的中后期（编码实现后）才能对系统进行精确的验证与确认。在此之前，验证与确认只能在文档的基础上依赖专业人员的经验来开展，不仅耗时而且过程质量得不到保证。基于模型的设计为早期的验证和确认提供了更多的选择，如仿真、形式化验证和硬件在环测试等。

在系统需求阶段进行精确的建模和分析，通常可显著减少系统需求中潜在的不一致和多义性，提升需求规范的整体质量。如果要用描述性的文字把需求当中隐含的意思全部表达出来，并且一点歧义没有，文字的可阅读性将大大降低。不同利益干系人通常对系统工作的业务范围具有不同的理解，基于集合论、逻辑符号以及图形化标记等描述手段使得工程人员能够创建清晰的关于需求的模型，从而有助于消除这些理解差异。需求模型一方面是描述系统、辅助沟通的工具，另一方面为进一步基于计算机的自动化分析和验证提供了可能性。

基于模型的设计和传统流程具有相同的需求开始，但是，这些需求并不作为文本规范的基础，而是用于以模型的形式开发可执行规范。开发人员使用

这些模型来明确需求与规范，然后对这些模型进行细化，以开发需求更具体的设计。使用基于模型的设计工具，工程师可以在系统级对设计进行仿真，在实现之前发现缺陷，完成设计之后，工程师借助这些模型自动生成产品级代码和测试案例。此工作流程使开发人员从需求到测试阶段都能够处于同一环境中，从而减少了人工工作量。此外，当开发人员在模型中仿真可执行规范来验证其是否满足需求时，在需求阶段即可开始测试，这样便可及早发现和消除缺陷，降低开发总成本。

测试是列控系统开发全生命周期中的关键环节，是保证系统功能的实现与规范一致性的重要途径和手段。传统的列控系统功能测试主要由手工完成，测试的效率低、耗时长，并且测试工作量会随着系统规范的改变而增大。基于模型的测试能够提供自动化、可重复性、可选择性的测试案例，从而避免手工测试的主观性，提高测试的效率。基于模型进行测试的一个主要方面是包括预测信息(Test Oracle)的可执行测试案例生成。预测信息以被测系统行为的模型为基础，其生成过程包括输入数据的生成、测试序列的生成以及预测信息(可以检查被测系统的输出)的生成。其优点是对于一个给定的合适的模型，可以自动完成测试过程，并可以生成完整的测试序列，以便转化为可执行的测试脚本，提高测试的执行效率和覆盖度。

相比黑盒测试，基于模型的测试不用根据需求文档人工编写测试案例，取而代之为建立包含系统需求规范的行为模型。利用被测系统的模型，通过基于模型的测试工具自动生成测试案例套。测试案例套是一系列抽象测试案例的集合，每一个测试案例又是特定输入和预期输出关系的操作序列。利用测试工具可以将这些抽象的测试案例自动转换为可执行的测试脚本，并通过运行这些测试脚本以检测被测系统是否存在失效。基于模型的测试是黑盒测试设计的自动化，其利用多种生成算法和策略生成被测系统行为模型的测试案例，能够高效的自动完成列控系统功能正确性测试。

(四)重用性和可维护性的提升

以代码和文档为中心的开发方法的一大弊端就是灵活性和可重用性差。代码和文档作为开发过程的中心，系统规范、分析、设计等都是为代码生成服务。一旦需求发生变动往往需要对系统重新进行分析，原系统的分析结果和过程都无法重新使用，因此，这种方法往往存在疲于应付需求的不断变更，文档迅速地失效和维护困难等突出问题。基于模型的开发方法通常都采用分层、模块化建模，同时大量采用标准化的模型库，如故障模式库、系统运行场景库等。对于开发过程中的各类人员都可以通过模型了解系统的设计过程，同

时模型也很好地描述了系统的实现过程，系统的维护过程从模型开始，这样大大提高系统的可维护性。

另外，系统的某些行为可能只有在运行的时候才能观测到，或者只有在运行的时候才能方便的验证。复杂的外界环境因素也是造成系统运行时刻失效的一个重要原因，如硬件损坏、恶劣天气以及操作人员的人为失误等因素造成的故障，这种类型的故障情况很难在系统开发阶段借助测试和形式化验证来完全杜绝。如果系统的行为依赖于环境对其的影响，需要对环境的精确描述做大量的假设，很可能这些假设并不合理或者根本无法获得，因此，仅仅使用传统的验证技术已经不足以保证列控系统持续、安全地提供高质量的服务，需要在系统运行阶段提供额外的主动安全保障措施来弥补。以形式化方法和模型为基础的运行时监控与保障技术的出现，为提高安全苛求系统的安全性和运行维护的便利性开辟了一条新的途径。

三、国内外研究现状

在以轨道交通、航空航天为代表的安全苛求系统应用领域，基于模型的开发逐渐成为一种趋势。这方面的研究主要致力于将安全分析融入开发过程，运用形式化方法领域的研究成果提高设计和验证的自动化程度以实现构建正确(Correct-by Construction)的理想目标，在保证系统安全性的前提下缩短开发周期、降低开发成本。国内外已经有了很多相关的研究工作。

德意志科学联合会(DFG)项目 AVACS(Automatic Verification and Analysis of Complex Systems)[1]研究前沿方法来保证复杂系统的自动设计、分析和验证技术，主要以轨道交通列控系统为应用对象。在该项目中，Olderog 等结合时段演算(Duration Calculus，DC)、CSP 和 OZ 理论提出了一套对轨道交通列控进行建模和验证的方法，相关结果已经在剑桥大学出版专著[2]。Platzer 等利用微分动态逻辑和微分不变量技术对 ETCS 需求规范进行建模和验证[3]，发现了需求规范的非形式描述中隐藏的错误。

欧洲太空总署项目 COMPASS(Correctness，Modeling and Performability of Aerospace Systems)[4]重点研究航空领域安全苛求系统的建模、正确性验证以及性能评价。建模与分析工作基于统一的模型，使用 SLIM(System - Level Integrated Modeling)语言进行描述，SLIM 是在 AADL 的基础上扩展形成的一种建模语言，能够描述系统中软硬件的架构、功能、故障行为以及故障修复。SLIM 语言采用面向组件的分层建模的思想，可以描述系统的正常功能和以一定概率发生的故障行为，特别的是，SLIM 具备描述系统连续行为的能力，支持