

城市轨道交通运行安全、运营安全与信息安全的矛盾与统一^{*}

孙来平^{1,5} 洪海珠² 施 聪³ 虞 翊⁴

(1. 同济大学道路与交通工程教育部重点实验室, 201804, 上海; 2. 上海轨道交通技术研究中心, 201100, 上海;
3. 上海地铁维护保障有限公司通号分公司, 200235, 上海; 4. 同济大学国家磁浮交通工程技术研究中心, 201804, 上海;
5. 上海电气泰雷兹交通自动化系统有限公司, 200120, 上海//第一作者, 工程师)

摘 要 对城市轨道交通信号系统的安全性研究主要集中在确保列车的运行安全方面,而在运行控制、运营管理和信息传输等各个学科领域划分的边界上往往存在着研究的盲点。因此,如何将系统安全提升到设备-人-环境-管理的广义本质安全层面,以提升城市轨道交通系统的整体安全性,优化安全输出的安全技术研究有待进一步深入。在分析城市轨道交通运行安全、运营安全与信息安全的定义和事故发生诱因的基础上,围绕信号系统的“故障-安全”(故障导向安全)是否就意味着整体运营和运行安全的问题,讨论了运行安全、运营安全与信息安全的矛盾和统一关系,对列车控制系统提出了整体运营安全的要求,将运行、运营和信息的安全统一到系统整体安全性这一终极目标上。

关键词 城市轨道交通; 信号系统; 运行安全; 运营安全; 信息安全

中图分类号 U298

DOI: 10.16037/j.1007-869x.2019.06.004

Contradiction and Unity Between Railway Operation Safety, Service Safety and Information Safety

SUN Laiping, HONG Haizhu, SHI Cong, YU Yi

Abstract The safety research of urban rail transit signal system concentrates on ensuring the system safety. However, there are blind spots on the boundary of various research disciplines such as operation control, operation management and information transmission. Therefore, how to upgrade the system safety to an integral safety level of system-human-environment-management scope with generalized essence, to improve the overall safety of urban rail transit system, and to optimize the technology of safety output needs further researches. Through analyzing the definitions on operation safety, service safety and information security of urban rail transit and the causes of accidents, and focusing on whether the “failure-safe”

(fault-oriented safety) about the signal system means the overall operation and operation safety, the contradiction and unified relationship of operational safety, service safety and information security are discussed. The overall operational safety requirements of the train control system are put forward, and the operation, service and information safety are finally unified to the ultimate goal of the system overall security.

Key words urban railway transit; signaling system; operation safety; service safety; information safety

First-author's address State Key Laboratory of Road and Traffic Engineering, Tongji University, 201804, Shanghai, China

1 运行安全、运营安全与信息安全

安全是“在人类生产过程中,将系统的运行状态对人类的生命、财产、环境可能产生的损害控制在人类能够接受水平以下的状态。”^[1]众所周知,在轨道交通领域里,安全是列车控制信号系统的灵魂,“故障-安全”(故障导向安全)原则是轨道交通安全运行不可逾越的底线^[2]。当系统设备发生故障、错误、失效的情况时,系统应作出导向安全的反应,以确保行车安全。但作为一个高效、大运量的公共交通工具,列车控制系统仅满足“故障-安全”这个底线是远远不够的。广义的本质安全是指“人-机-环境-管理”这一系统表现出的整体安全性能^[3]。不可否认,经过长期的研究和不懈的经验积累,无论在轨道交通的安全标准里,还是在日常工作中,轨道交通信号专业的研究人员已对信号系统的各个子系统的安全行为作了极为详尽的研究,尽一切可能确保系统在故障情况下导向安全输出。然而,对于如何引导、辅

^{*} 上海市科委科研计划项目(18DZ1205800);上海市磁浮与轨道交通协同创新中心基金项目(20132223)

助和提高整个城市轨道交通系统的运营安全,以及如何全局把控整体运营和运行安全,列车控制信号系统还有很大的提升空间,与之相关的安全技术研究

有待进一步开展。本文结合安全及广义本质安全的定义,将轨道交通安全划分为3大类型:运行安全、运营安全 and 信息安全,其基本特征如表1所示。

表1 轨道交通运行安全、运营安全 and 信息安全的基本特征

安全分类	安全责任主体	安全责任主体的归属	安全原则	安全的体现形式
运行安全	系统	设备级安全	“故障-安全”;可靠、可用、可维护	状态安全——系统的运行状态
运营安全	人员	管理级安全	资质培训及考核;作业行为的全过程控制;规程的制定和执行	行为安全——人员操作
信息安全	环境	环境级安全	信息的保密性、真实性、完整性	封闭性——连贯且封闭

1.1 运行安全及其表现形式

系统运行是指系统应执行的工作以及执行该工作所需的条件^[4]。在轨道交通中,运行安全集中体现在行车安全上。信号系统的安全设计遵循“故障-安全”原则。系统对运行状态进行实时计算,一旦计算结果与预期的安全状态不吻合,或者2套/多套并行处理器的仲裁结果不一致时,系统将立即作出反应,将系统导向安全一侧,最大限度确保安全停车。典型的事例包括列车紧急制动(EB)模式不可用,区域封锁/轨道关闭、停车点/进路移动授权回撤等。

1.2 运营安全及其表现形式

运营安全集中体现在安全管理规定的制定和执行上,特别在列车自动防护失效或者信号设备故障的情形下,控制中心行车调度、列车驾驶员、车站值班人员等相关运营人员必须严格依照相应的管理规定进行作业,这是运营安全的基石^[4]。

由此可见,影响运营安全最主要因素是人。当突发行车事故时,调度员必须能够按照规定向有关部门及上级报告,迅速采取救援措施,及时恢复列车正常运行最大限度减小对运营造成的影响。轨道交通列车驾驶员是列车安全正点运行的另一个重要保障,他们必须熟知驾车行驶的相关法律法规以及驾驶知识,具备熟练驾驶技能,具备良好的服务意识;更为重要的是,他们必须具备应变能力,能及时应变,保护车上人员安全。除了线路本身的运营与维护外,运营安全也与乘客息息相关,大客流下的换乘、导客、限流、疏散,以及与其它交通系统(如道路交通等)的联动等都与乘客的公共意识和公共素养直接相关,如何正确引导乘客,减少因乘客导致的运营安全事故,也是运营安全管理的焦点之一。

1.3 信息安全及其表现形式

信息安全集中体现在数据的完整和有效,即须保证信息的保密性、真实性、完整性方面,以及将这些信息作为输入的系统的接口安全性^[5]。信息安全

可分为两方面:狭义的信息安全是建立在以密码论为基础的计算机安全领域;广义的信息安全是一门将管理、技术、法律等问题相结合的综合性学科。当今的城市轨道交通中有线和无线通信的可靠性和安全性已经是列车全自动运行最重要的基本条件之一^[6]。例如,对于基于通信的列车控制(CBTC)系统,如何防止通信延时、报文丢失、通信中断、网络风暴、黑客入侵(截取、记录、监听、篡改甚至接管)等安全^[5],是城市轨道交通系统信息安全防护工作的重点。

1.4 影响运行安全、运营安全 and 信息安全的因素

回顾轨道交通的运营历程,重大事故的发生往往同时伴随着设备的故障、人员的不安全行为、相关环境的负反馈。在研究了全球近30年的轨道交通安全事故及原因^[7]后,可以看到事故主要原因集中在以下几个方面:①人为过失、管理不善;②设备故障、车辆本身的原因;③不可抗力(飓风、海啸、泥石流等);④地基塌陷、线路偏移、城市建设影响、停电等。其中,人为过失、管理不善和设备故障所导致的事故占整个事故总量的80%以上。这一惊人的高比例反映出一个事实:城市轨道交通列车控制系统的安全性仍存在较大的局限性,安全更多的体现在各个“点”(设备故障、人员误操作等)上,而没有将这些“点”联结成一个“面”(设备-人-环境-管理)。所以,城市轨道交通列车控制系统安全防范的边界有待进一步扩展和完善。

2 运行安全、运营安全、信息安全的矛盾现象与根源

为保证整体的安全性,首先需要了解事故的发生机理,理清整个过程中所有参与系统活动中的人、设备、环境等因素是如何进入危险状态的,从而总结出运行安全、运营安全 and 信息安全的矛盾现象及其根源。

2.1 安全性研究的重要问题

从1930年开始,交通运输、航空、航天、采矿、冶金、医疗急救、消防等行业安全领域的国内外学者和专家们在几十年的时间里相继提出了众多各种场景和行业的安全事故模型,如Adams模型^[3,8]、Vird模型^[8]、奶酪模型^[3]、多线性时间序列模型(MES)^[8]、基于系统论的STAMP^[9,11]模型、Heinrich事故致因模型^[9,11]等。通过研究和总结这些事故模型,分析导致危险的整个过程,可找出导致危险的矛盾、原因和风险,从而为设计更具针对性的安全系统、制定合理的措施与应急预案提供支撑。

综合各类安全模型研究,可知事故与事故诱发因子(或事故致因)之间的关系为:事故的诱发因子是离散量而非线性数据;事故的发生是其诱发因子共同作用的结果,其中诱发因子间不乏相互关系。据此,可以把事故以有限非空集合的方式表示如下:

$$\text{事故(Accident)} = \{\text{Sys-F, H-E, Unsafe-E, SafeCtrl-E}\} \quad (1)$$

式中:

Sys-F (System Failure)——设备故障/系统失效;

H-E (Human Error)——人员操作失误;

Unsafe-E (Unsafe Environment)——必备环境的缺失/周边环境的刺激;

SafeCtrl-E (Safe Control Error)——安全管理流程的漏洞/处置预案的缺失。

从安全研究的角度分析,式(1)涵盖了3个重要问题:

(1) 针对每一个事故诱发因子,各个学科/专业领域是否进行了详细的研究和分析。

(2) 各诱发因子一定是集中出现才会导致事故发生,还是存在着先后/因果/诱导、互斥/抵触/限制等关系,即运行安全、运营安全和信息安全是否存在着内在的联系。更为关键的是,一种类型的安全行为是否会由于处置的不恰当,而将危险致因转嫁给其它相关领域,从而降低整体安全。

(3) 采取怎样的手段能够最大限度地同时抑制事故诱发因子的出现,以达到整体安全。

2.2 运行安全、运营安全、信息安全的矛盾

从相关领域的技术论文、科学报告,特别是事故分析报告可以看到存在这样一种现象:安全风险转嫁,即:参与系统运营安全的某个专业领域在处理安全风险时,可能会直接或间接地将安全风险责任输出给其它安全相关的学科/专业。轨道交通几种比较常见和典型的风险转嫁举例见表2。

表2中安全风险的转移凸显了矛盾的现象:安全领域内,各个学科的研究人员将设计和实现本学科或领域内的系统安全行为作为工作的重点,而未考虑其安全行为可能会对后续或周边的学科、专业、操作和管理带来困难,甚至引入新的安全风险。显然,这样的安全性远远无法达到安全完整度等级4级(SIL4)的要求。

表2 运行安全、运营安全和信息安全之间的风险转嫁示例

示例	风险转嫁	安全风险	采取的安全手段	后续操作及处置	矛盾—风险转嫁分析
示例1	运行安全风险→运营安全风险	车-地通信在车辆出发咽喉区中断,信号系统在此区域失去对列车的追踪	信号系统采取了安全措施:①紧急制动停车;②在最终失去通信的相关区域封闭轨道,防止其他进路或列车穿越该区域	在实际操作中,由于重复开放信号等操作消耗大量时间,行车调度为确保正常发车可能采取完全人工操作取代列车自动保护(ATP),以尽快恢复故障。例如:①司机采取切除车载ATP方式动车;②电话闭塞,红灯冒进动车;③手摇道岔;等等	信号系统的紧急制动、关闭丢失通信的轨道区域符合“故障—安全”原则;但由于为确保安全,后续的故障恢复延时长、操作繁琐。在特定时段特殊区域,运行管理人员和维护人员可能采取切除信号系统运行的方式维持运营。在此种情况下,由于“诱发”了完全的人工操作和紧急处置,系统的整体安全等级可能大大降至SIL4以下
示例2	信息安全风险→运行/运营安全风险	传输控制协议(TCP)中传输中断/连接异常	TCP/IP网络协议在传输控制层如果发生报文丢失、连接中断、校验失败等情况,会试图重新连接并通知应用层等待,挂起相应进程直到通信双方重新握手成功	由于TCP底层通信进程挂起,导致信号系统应用程序报文发送/接收队列积压,在规定时间内无法完成命令发送—状态回采的控制闭环,导致宕机或输出导向安全侧处理,从而将触发降级运行同时人工介入,以确保后续运营的连接	信号系统(特别是CBTC系统)各个子系统间的信息通信周期均以ms为单位,对信息的实时性要求很高。由于信息安全问题触发的网络信息通信延时,对信号系统、人工处置乃至整系统运行的安全等级(SIL4)提出了严苛的要求
示例3	运营安全风险→运行/信息安全风险	运营时调度、司机、车站值班人员、维护保障人员等的人为失误	人工防护(由于人为操作失误、维护不当等原因导致信号系统宕机/ATP防护失败,系统安全由操作人员负责)	降级运行、电话闭塞、人工驾驶、手摇道岔等	由于缺乏设备层面的安全保障,误操作或人员疏忽是导致事故发生的主要原因

3 运行安全、运营安全、信息安全的统一

运行安全、运营安全与信息安全的统一符合人-机-环境-管理的本质安全的定义。所以,将运行安全、运营安全 and 信息安全最终统一在系统整体安全这一终极目标上,实现土建、信号、运营管理、车辆、供电等各个专业/部门的联动,是降低城市轨道交通整体安全风险、给出优化安全输出的理想途径。举例而言,安全、节能、高度自动化的无人驾驶轨道交通系统是目前城市轨道交通发展的趋势之一,而人-机-环境-管理的整体安全是实现全自动无人驾

驶的基石。如无人驾驶列车因故障迫停区间场景下的列车救援、乘客逃生、后续运营恢复、与其他交通系统信息交互与联动等,都是运行安全、运营安全 and 信息安全三者统一的必要性的力证。

3.1 系统整体安全性的影响因素

基于式(1)中提到的第三个问题,综合运行安全性、运营安全性和信息安全性等多个维度上的技术和机理,对轨道交通列车控制系统提出整体运营安全需求,让系统给出一个优化的安全输出,更加“智慧”地决策安全,成为了亟待解决的问题。系统的整体安全性影响因素可以如图1所示^[2]。

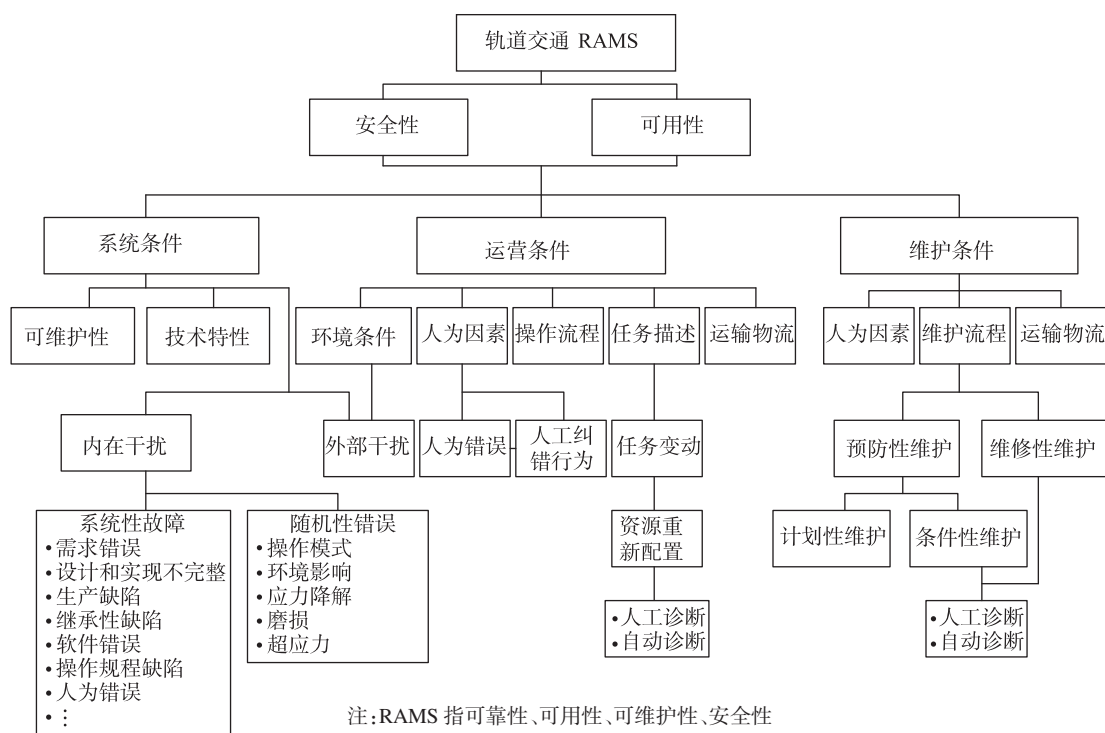


图1 轨道交通系统整体安全性的影响因素

图1摘自铁路欧洲标准EN 50126《可靠性、可用性、可维护性和安全性标准》。由图1可知,安全性的影响除了受制于系统条件外,还与运营条件、维护条件息息相关,各个分支的子节点均同时对最终的安全性和可用性产生影响^[2],具体表现为:

(1) 安全是整体的安全,受所有条件影响,不存在部分的安全,也不存在不同条件(系统、运营、维护)下的安全;

(2) 系统条件和运营条件之间存在横向的联系(外部干扰),所以孤立地针对不同条件展开研究多少存在盲区;

(3) 人为错误、运输物流、故障诊断等穿插在各

个应用条件中,而这些因素背后反映的是运营管理的水平^[13]。

所以,通过上述分析可知,安全是人-机-环境-管理的整体安全。在运行、运营和信息等不同范畴内的安全,最终必将统一到整个系统的安全上来。

3.2 系统优化安全解

从轨道交通系统设计伊始,就应考虑整体安全的概念。具体而言,系统的优化安全解可以从以下几个方面开展:

(1) 以运营场景为导向:信号、车辆、网络、维护管理等的系统功能性设计应直接面向运营场景,在充分理解运营场景要求的情况下给出设计方案,而

非以实现功能为导向的方式进行。

(2) 新技术、新手段:为轨道交通信号系统注入新技术、新理念,借鉴、复用、提炼其它领域先进的系统运行方案,减少或取代传统人工操作、运营维护等,降低安全风险。例如,借鉴云平台的安全实时控制特性、分布式计算和数据存储、集群替代冗余、实时故障容错和安全数据回滚技术等;再如,大数据已经引入城市轨道交通领域,借鉴引入大数据的信息安全保障措施,利用大数据进行趋势预测,进一步提升预防性维修维护水平等,也是研究进一步深入的可选方向之一。

(3) 联营、联动:信号、运营管理、车辆、供电、调度等各个岗位在设计联络阶段便可制定详尽的联合调试计划、阶段性系统演练计划等,而无需等到最终的系统交付、出厂验收才介入系统的使用。例如,轨道交通运营人员可以参与到开发或验证阶段的实验室测试工作,从而对系统有较为深入的认知,可降低人为误操作。

(4) 更具操作性的紧急预案:在系统研发过程中,开发商和轨道交通运营方可进行系统失效评估和对运营影响的分析,制定出有针对性和操作性强的故障恢复预案。从而在设备发生故障时,确保人工控制前提下的运营安全;在运行系统交付时,相应的运营方案和故障处置方案也可相应完成。

4 结语

本文从安全概念出发,对运行安全、运营安全和信息安全的表现形式及其之间存在的矛盾进行了分析,提出了解决方法的设想,为进一步优化和提高系统的整体安全性研究提供参考。无论是目前的CBTC和联锁后备模式协同,还是方兴未艾的全自动无人驾驶,全自动化、智能处理、高度集中控制是其技术核心和优势,同时也对安全控制中的设备、人员、运行环境间更加紧密有机地结合提出了更高的要求。所以,运行安全、运营安全和信息安全的统一变得更为重要。

如何在无人值守的条件下将运行、运营、通信

(信息)等重要功能协同工作,以运营场景为纲,实现专业接口协同、人机接口协同,为城市轨道交通提供更为灵活的操作模式,同时避免人为误操作所引起的风险,更加“智慧”地给出安全输出,使列车运行更安全,是业内需要不断深入研究的课题。

参考文献

- [1] 中国国家标准委员会.轨道交通可靠性、可用性、可维修性和安全性规范及示例:GB/T 21562—2008[S].北京:中国标准出版社,2008.
- [2] CNE/CENELEC. Railway Applications Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS): EN 50126—2001[S]. Brussels: CMCC, 2001.
- [3] 孙肖,周新蕾,林佳,等.事故模型理论发展与应用研究[J].质量与可靠性,2014,170:19.
- [4] CNE/CENELEC. Railway Application Communication, Signalling and Processing Systems Software for Railway Control and Protection Systems: EN 50128—2011[S]. Brussels: CMCC, 2011.
- [5] CNE/CENELEC. Railway Application Communication, Signalling and Processing Systems: EN 50159—2010[S]. Brussels: CMCC, 2010.
- [6] ANDRESS J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice [C] // Syngress M. WASHINGTON, D.C.: National Research Council, 2014:32.
- [7] 毕湘利,邓奇.ATP失效模式下的城市轨道交通列车运行安全保障措施研究[J].城市轨道交通研究,2014(10):1.
- [8] BENNER L. Accident investigation multi-linear events sequencing methods[J]. Journal of Safety Research, 1975, 7(2):67.
- [9] SONG T, ZHONG D, ZHONG H. ASTAMP analysis on the China-yongwen railway accident[J]. SAFECOMP 2012 LNCS, Magdeburg: SAFECOMP, 2012:376.
- [10] 赵文祥,刘婷婷.海因里希事故因果连锁理论模型及其应用[J].经济论坛,2009(9):94.
- [11] 王昊,刘中田,徐越.基于多层 STAMP 模型的 CTCS-1 级列控系统功能安全分析方法[J].铁路计算机应用,2017(5):28.
- [12] LEVESON N. A new accident model for engineering safer systems [J]. Safety Science, 2004, 42(4):237.
- [13] 康茹,傅贵,高平,等.消防员伤亡案例的事故致因“2-4”模型解读[J].消防科学与技术,2016,12(35):1756.

(收稿日期:2019-02-10)

欢迎订阅《城市轨道交通研究》

服务热线 021-51030704