

全自动智能化运行平台安全指南研究*

王潇骁¹ 赵华华^{2,3} 楚彭子^{2,3} 洪海珠¹ 袁建军^{2,3} 虞 翊^{2,3}

(1. 上海申通地铁集团有限公司技术中心, 201103, 上海; 2. 同济大学磁浮交通工程技术研究中心, 201804, 上海;

3. 同济大学上海市磁浮与轨道交通协同创新中心, 201804, 上海//第一作者, 工程师)

摘 要 全自动智能化运行模式是全自动运行系统发展趋势之一。针对全自动智能化运行平台的安全开发与安全实施, 探讨了安全指南研究流程; 分析了运营场景特性, 并就安全风险以及安全要求进行了阐述; 给出了风险管控意见。在全自动智能化运行平台的研究与实践中, 需要关注运行安全、运营安全以及信息安全的重要性。

关键词 城市轨道交通; 智能化运行; 安全指南; 场景驱动; 风险管控

中图分类号 U239.5

DOI: 10.16037/j.1007-869x.2022.01.011

Research on Safety Guidelines for Intelligent Fully Automatic Operation Platform

WANG Xiaoxiao, ZHAO Huahua, CHU Pengzi, HONG Haizhu, YUAN Jianjun, YU Yi

Abstract The intelligent FAO (fully automatic operation) mode is one of the development trends of FAO system. Regarding the safety development and safety implementation of the intelligent FAO platform, the research process of safety guidelines is discussed; the characteristics of operating scenarios are analyzed; safety risks and safety requirements are elaborated; risk management and control opinions are given. The importance of operating safety, operation safety and information security requires emphatical attention in the research and practice of the intelligent FAO platform.

Key words urban rail transit; intelligent operation; safety guidelines; scenario driven; risk management and control

First-author's address Technical Center of Shanghai Shentong Metro Group Co., Ltd., 201103, Shanghai, China

近几年, 为了更好地服务乘客, 全自动无人驾驶系统在国内已经逐步建设并掀起热潮, 信号系统与其他系统一体化的“大综控”技术方案得到关注。在实施效果上, 通过将传统 ATS (列车自动监控) 和

ISCS (综合监控系统) 两套系统进行整合, 为中心调度提供了集成化的人机操作界面^[1], 大大提高了调度人员的工作便利度及场景处理效率。在无人驾驶模式下, 原先由驾驶员执行的工作被自动化设备代替, 系统的可靠性和集成度要求更高, 运行或运营场景更为复杂, 对旅客服务质量的要求也更高。

由此可见, 具备综合自动化、一体化和智能化特征的城市轨道交通全自动智能化运行行车指挥模式将是运控系统的发展方向之一^[2]。从系统设计及实施层面看, 由于各子系统从根源上是独立设计的, 安全完整性等级 (SIL) 各不相同。例如: 信号系统的中央层设备 ATS 的 SIL 要求应达到 2 级; 轨旁及车载设备层, 如 ZC (区域监视器)、CI (计算机联锁)、VOBC (车载控制器) 等的 SIL 要求应达到 4 级; 而对于综合监控系统而言, 相应的 SIL 较低^[3]。因此, 基于孤立子系统进行场景及安全性分析难以满足日益复杂的子系统联动安全需求。

全自动智能化运行平台是一类以信号系统为核心, 以乘客服务为导向, 以各系统数据汇集或信息融合为抓手, 以安全、可靠、高效、经济等指标为目标的面向调度和运维的智能化多系统联动决策与自动运行的系统^[2]。子系统间的相互影响与协作使得全自动智能化运行平台可视为一个有机整体。以运营场景为核心, 研究与分析安全特性对其正常运行十分有益, 也有助于系统的全生命周期闭环管理^[4]。本文在文献[2]的基础上, 探讨“全自动智能化运行平台安全指南”(以下简称为“安全指南”)的框架与内容, 为城市轨道交通全自动智能化运行平台的设计、开发和应用提供指导。

1 安全指南研究流程

安全指南的研究在于为系统安全设计、安全运

* 国家重点研发计划项目 (2016YFB1200602-02); 上海市科学技术委员会科研计划项目 (18DZ1205803); 上海市磁浮与轨道交通协同创新中心基金项目 (20132223)

行和安全评估等提供指导性文件。这需要了解系统的功能范围、系统边界以及应用场景。基于此,可以先从概念、功能、架构和接口等方面出发,把握平台属性,剖析涉及的场景,尤其是特有的场景。基于运营场景分析风险事件、概率与严重性等级,进而从运行安全、运营安全、信息安全以及技术管控与组织管控等角度提出相应的安全要求与管控措施,最终形成具有指导意义的安全指南,如图 1 所示。

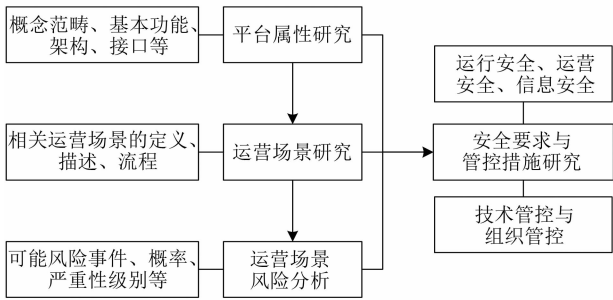


图 1 安全指南研究流程示意

Fig.1 Schematic diagram of the safety guideline research process

2 运营场景特性分析

运营场景的研究有助于系统的开发设计、工程的建设与管理^[4-5]。全自动智能化运行平台存在多个业务子系统之间的联动功能,需要制定具体的需求规范,并以运营场景的形式来描述。鉴于该平台子系统间的联动复杂,可将这些存在联动关系的场景视为复杂运营场景。这种复杂性与该平台的特性有关。首先,复杂运营场景涉及平台集成方案中的多个子系统,子系统之间存在安全接口;同时,复杂运营场景的处置方案体现在涉及多个专业系统,或者是涉及多种专业的调度人员;此外,复杂运营场景需要反映系统功能,体现出平台广度以及联动处理能力。

对于运营场景或复杂运营场景的描述涉及不同主体的行为及其基本流程。针对上海轨道交通全自动运行系统的运营场景,文献[6]结合上海轨道交通 14 号线、15 号线和 18 号线的建设经验,将场景分为正常场景、故障场景与应急场景。同时,上海申通地铁集团有限公司的企业标准《上海轨道交通全自动运行运营场景及功能分配》对复杂运营场景做出了类似的描述。就全自动智能化运行平台的复杂运营场景而言,正常运营场景包括

早间车辆基地准备、自动开站、自动关站和站台候车引导 4 大项。故障运营场景包括车辆设备故障、信号设备故障、站台门故障、供电故障、机电设备故障和线路故障等 6 大项复杂运营场景。应急运营场景包括乘客摔倒、大客流、挤岔、脱轨、列车在站台发生火灾、列车在区间发生火灾、车站火灾、区间火灾、列车在站台疏散、列车在区间疏散、区间因故停车、列车救援和检测到紧急报警等 11 大项复杂运营场景。

以“站台门故障”为例,可将该场景分为涉及站台门与信号接口电路故障、一扇或多扇站台门故障和对位隔离故障(如图 2 所示)3 个子场景来讨论。对于“站台门与信号接口电路故障”子场景,车辆、通信、综合监控、站台门等专业均存在联动或接口关系,接口间存在一定的时序关联性,在运营人员配合下形成完整处置闭环,是典型的跨多子系统联动的复杂运营场景。

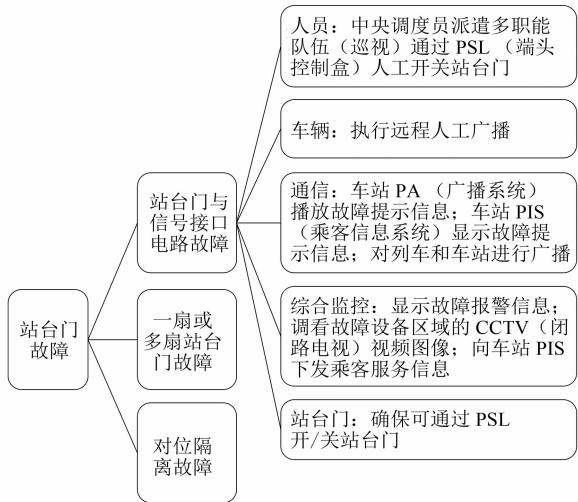


图 2 站台门故障场景示意

Fig.2 Schematic diagram of platform door failure scenario

3 安全要求

全自动智能化运行平台围绕着服务乘客的核心目标,实现 ATS 核心功能、一体化综合监控功能、联动功能、综合运维功能以及辅助管理功能等。明确平台功能的安全性要求,对保障城市轨道交通大系统的整体安全十分重要。

3.1 安全风险范畴

广义的安全着眼于“人-机-环境-管理”所表现出的整体安全性^[10]。文献[7]将轨道交通安全划分为运行安全、运营安全 and 信息安全,并认为运行

安全属于以系统为主体的设备级安全;运营安全是以人员为主体的管理级安全;信息安全是以环境为主体的环境级安全。根据全自动智能化运行平台的内涵及其“大综控”“服务乘客”“智能化运行”的思想,该平台的安全风险也可以从这三方面进行综合考虑,并权衡三者的对立与统一关系^[7-8]。

对于运行安全,可靠、可用、可维护是其安全原则,体现在系统的运行状态是安全的。作为安全苛求系统,全自动智能化运行平台的设计必须遵循“故障-安全”原则,最大限度确保行车安全。该目标的实现需要对平台的运行安全风险进行研究,设计判断机制以及安全侧,以达到应有的安全性要求。就运营安全而言,严格的资质培训及考核、作业行为的全过程监控、规章制度的完善与落实是其安全原则,体现在组织行为的安全性,尤其是故障情形下不同主体的协作。作为服务乘客的智能化运行平台,如何正确地跨专业协同与引导乘客,减少与降低运营风险,是该平台应关注的内容。从信息安全的角度,信息的保密性、真实性与完整性是其原则,主要体现在信息的封闭性与连贯性。全自动智能化运行平台是CBTC(基于通信的列车控制)系统,相关子系统也会涉及数据信息的产生、传输、显示和存储等,信息安全防护对于该平台同样至关重要。

3.2 智能化运行的安全指南要求

3.2.1 运行安全要求

全自动智能化运行平台对列车的运行安全有着严格的要求,包括其自身的安全性要求(即系统安全性要求)以及与之相连的外部子系统之间安全性要求(即外部接口安全性要求)。

在系统安全方面,需参考的安全性要求有:全自动智能化运行平台的安全完整性等级应为 SIL2;系统生命周期各阶段的 RAMS(可靠性、可用性、可维护性和安全性)管理流程应符合 GB/T 21562—2008《轨道交通可靠性、可用性、可维修性和安全性规范及示例》要求;系统安全相关电子系统研发过程中的质量管理、安全管理、功能安全和技术安全证据、安全验收和审批应符合 GB/T 28809—2012《轨道交通 通信、信号和处理系统 信号用安全相关电子系统》的要求;系统控制和防护软件的需求规范、结构、设计与实现、验证与测试、软件/硬件集成、软件确认、评估和质量保证应符合 GB/T 28808—2012《轨道交通 通信、信号和处理系

统 控制和防护系统软件》的要求;系统或设备应遵循故障-安全机制,并应符合 TB/T 2615—2018《铁路信号故障-安全原则》的要求;系统或设备采用封闭式传输系统时,其功能完整性、安全完整性、安全规程、安全编码应符合 GB/T 24339.1—2009《轨道交通 通信、信号和处理系统 第1部分:封闭式传输系统中的安全相关通信》的要求;系统或设备采用开放式传输系统时,数据传输的防护应满足 GB/T 24339.2—2009《轨道交通 通信、信号和处理系统 第2部分:开放式传输系统中的安全相关通信》要求。

在外部接口安全方面,应根据全自动智能化运行平台与外部子系统之间的接口所应实现的功能和性能,以及接口失效后可能会造成的事故后果及其严重程度,定义接口的安全性要求。外部接口的安全性要求需按照接口双方安全完整性等级较高一方的要求,对接口的设计标准和安全性进行要求。涉及的内容有:全自动智能化运行平台与轨旁信号系统设备之间的通信属于安全相关设备之间的通信,其中全自动智能化运行平台的安全完整性等级保持与 ATS 同样的等级,即 SIL2,而轨旁信号系统的安全完整性等级为 SIL4,两者之间的接口需要遵循 GB/T 24339.1—2009,满足轨旁信号系统对接口安全性的要求(SIL4);全自动智能化运行平台通过与外部系统接口,实现对 PSCADA(电力监控与数据采集)、BAS(环境监控系统)、FAS(火灾报警系统)、CCTV、PIS、PA、ACS(门禁系统)、PSD(站台门)、AFC(自动售检票)、ILS(仪表着陆系统)、RC(无线通信)、CLK(时钟)和车辆系统的监控功能。全自动智能化运行平台的安全完整性等级为 SIL2,如果外部系统故障或接口失效,有可能会造成全自动智能化运行平台对其的监控功能失效或 ATS 系统功能的受影响。为了防止外部系统故障对全自动智能化运行平台的影响,在外部系统接入全自动智能化运行平台时,要采取接口隔离的安全措施,并制定相应的操作规程、应急预案和规章制度。接口隔离的安全性要求可参照 GB/T 24339.1—2009 和 GB/T 24339.2—2009。

3.2.2 运营安全要求

为了更好地服务乘客,需要严格保障运营安全,需参考的内容有:GB/T 38707—2020《城市轨道交通运营技术规范》中运营管理要求的相关规定;GB/T 30012—2013《城市轨道交通运营规范》

中对于行车组织、客运组织、车辆及基地管理、设施设备管理、人员管理以及安全管理相关规定;GB/T 33668—2017《地铁安全疏散规范》中对于设备系统的疏散技术要求和安全疏散运营管理要求等。

同时,还应参考 T/CAMET 04017.7—2019《城市轨道交通 全自动运行系统规范第 7 部分:运营管理》中对于行车组织、客运组织与服务、设备设施管理、人员管理及要求,以及安全与应急管理相关规定;另外,还应参考 DB11/T1166—2015《城市轨道交通运营安全管理规范》中对于人员安全管理、行车安全管理、客运安全管理、设备设施安全管理、事故和事件管理、风险和应急管理这些方面的规定等。

此外,全自动智能化运行平台还应考虑路网协同,体现在能够在应急或故障场景下做到快速调图,结合工作人员的应急组织,尽可能地减小延误,以保证乘客服务质量。

3.2.3 信息安全要求

对于信息安全要求,需参考的内容有:根据 GB/T 22240—2008《信息安全技术信息系统安全等级保护定级指南》,全自动智能化运行平台的信息系统安全等级保护定级为第三级;系统应满足 GB/T 22239—2008《信息安全技术信息系统安全等级保护基本要求》中第三级的安全保护能力及其安全保护的技术要求和管理要求,即:应能够有效防护主要资源损害,能够发现安全漏洞和安全事件,并能够在系统遭到损害后,较快恢复绝大部分功能。

同时应参考 GB/T 25070—2010《信息安全技术信息系统等级保护安全设计技术要求》中第三级系统安全保护环境的设计技术要求,构建安全计算环境、安全区域边界、安全通信网络以及安全管理中心。通过安全互联部件和跨定级安全管理系统中心,实现与外部其他子系统相同或不同等级的定级系统安全保护环境之间的安全连接,应保持用户身份、主/客体标记、访问控制策略等安全要素的一致性,对互联系统之间的互操作和数据交换进行安全保护。

此外,全自动智能化运行平台作为一个工业控制系统,还应根据 GB/T 32919—2016《信息安全技术 工业控制系统安全控制应用指南》的要求,从安全软件选择与管理、配置和补丁管理、边界安全防护、物理和环境安全防护、身份认证、远程访问安全、安全监测和应急预案演练、数据安全等方面做

好工控安全技术防护。

3.3 安全要求的落实

全自动智能化运行平台属于一类全自动运行系统,涉及内容较多。上述安全要求的落实需要根据拟开发的平台进行探讨,进而根据涉及的子项及其要求(标准或规定)逐项对照,以确保所开发系统具备应有的安全性能。

4 风险管控

针对全自动智能化运行平台风险管控,可从开发过程和安全评估两方面做出要求。开发过程中,在落实上述安全要求的基础上,还应尽可能多地发现与规避风险源。必要时,需采用技术管控来降低风险概率,并辅以管理措施,以降低危害。风险因素识别以及安全验证的方法有很多,如故障树、头脑风暴、鱼骨图、形式化验证等^[9,11],方法也相对成熟,本文不再赘述。

安全评估是对系统安全性能的鉴定。对于全自动智能化运行平台,评估范围包括系统功能、性能和接口关系,涵盖系统开发与使用的全过程。评估时,应委托具有安全评估资质的第三方进行安全评估。

5 结语

全自动智能化运行是一种跨线网与跨专业的智能化协同运行模式。本文探讨了全自动智能化运行平台安全指南的构建流程,并就其中多方面的内容进行了阐述。安全指南的构建有助于该平台的研究与实施,研究内容能够为全自动智能化运行模式下城市轨道交通运行控制系统的开发提供参考。

参考文献

- [1] 朱莉,胡恩华. 全自动无人驾驶一体化智能运控系统研究[J]. 铁道通信信号,2019(10):69.
ZHU Li, HU Enhua. Research on integrated intelligent operation and control system of FAO[J]. Railway Signalling & Communication, 2019(10):69.
- [2] 杨志慧,楚彭子,王潇骁,等. 城市轨道交通全自动一体化智能运行系统研究[J]. 铁道通信信号,2020(4):73.
YANG Zhihui, CHU Pengzi, WANG Xiaoxiao, et al. Study on integrated intelligent fully automatic operation system for urban rail transit[J]. Railway Signalling & Communication, 2020(4):73.
- [3] 王媛媛,施广德,李鹏. 基于安全完整性 SIL2 级的城市轨道交通

交通综合监控系统[J]. 江苏科技信息, 2020(35):68.

WANG Yuanyuan, SHI Guangde, LI Peng. Comprehensive monitoring system of urban rail transit based on safety integrity SIL2 grade[J]. Jiangsu Science & Technology Information, 2020(35):68.

- [4] 洪海珠. 基于关键运营场景的城市轨道交通全自动运行系统全生命周期闭环管理[J]. 城市轨道交通研究, 2020(增刊2):4.

HONG Haizhu. Closed-loop management method of FAO system full life cycle based on key operation scenarios[J]. Urban Mass Transit, 2020(S2):4.

- [5] 陈光. 常导高速磁浮铁路运营场景分析探讨[J]. 机车电传动, 2020(6):56.

CHEN Guang. Analysis and discussion on operation scene of high-speed EMS maglev railway[J]. Electric Drive for Locomotives, 2020(6):56.

- [6] 施挺. 上海城市轨道交通全自动运行系统运营场景研究[J]. 城市轨道交通研究, 2020(增刊2):160.

SHI Ting. Research on the operation scenario of Shanghai metro fully automatic operation system[J]. Urban Mass Transit, 2020(S2):160.

- [7] 孙来平, 洪海珠, 施聪, 等. 城市轨道交通运行安全、运营安全和信息化安全的矛盾与统一[J]. 城市轨道交通研究, 2019(6):15.

SUN Laiping, HONG Haizhu, SHI Cong, et al. Contradiction

and unity between railway operation safety, service safety and information safety[J]. Urban Mass Transit, 2019(6):15.

- [8] 吴越. 城市轨道交通运行安全与运营效率的矛盾和统一[J]. 城市轨道交通研究, 2020(11):22.

WU Yue. The contradiction and unification between urban rail transit operation safety and revenue efficiency[J]. Urban Mass Transit, 2020(11):22.

- [9] 宁滨, 郜春海, 李开成, 等. 中国城市轨道交通全自动运行系统技术及应用[J]. 北京交通大学学报, 2019(1):1.

NING Bin, GAO Chunhai, LI Kaicheng, et al. Technology and application of fully automatic operation system for urban rail transit in China[J]. Journal of Beijing Jiaotong University, 2019(1):1.

- [10] 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(2):19.

SUN Xiao, ZHOU Xinlei, LIN Jia, et al. Research on development and application of accident model theory[J]. Quality and Reliability, 2014(2):19.

- [11] 虞翔. 城市轨道交通运营设备的寿命与安全评价方法[J]. 城市轨道交通研究, 2014(2):148.

YU Yi. Lifespan and safety evaluation method of urban rail transit operating equipment[J]. Urban Mass Transit, 2014(2):148.

(收稿日期:2021-05-21)

(上接第52页)

1) 轨缝设计。结合轨缝与悬浮传感器的影响关系,建议轨缝按照标准建议值 16 mm 设计,既可保证轨排热胀冷缩要求,又能满足车辆悬浮传感器的检测要求。同时,应严格控制线路中最大轨缝值不能超过 40 mm,避免悬浮传感器出现 2 路探头检测失效的情况,从而影响悬浮控制的稳定性。

2) 轨道接头结构。J II 型和 J III 型接头中的连接板长度应能保证悬浮传感器前后 2 个探头不会同时失效,但悬浮传感器在过双缝的时候,连接板的长度会影响悬浮传感器连续受激励时间,从而影响控制系统辨识。建议 J II 型接头设计时适当增大中间连接板的长度,一般路段按不小于 500 mm 设计,困难路段按不小于 300 mm 设计。

参考文献

- [1] 中华人民共和国住房和城乡建设部. 中低速磁浮交通设计规范: CJJ/T 262—2017[S]. 北京: 中国建筑工业出版社, 2017.
Ministry of Housing and Urban-Rural Development of the

People's Republic of China. Code for design of medium and low speed maglev transit: CJJ/T 262—2017[S]. Beijing: China Architecture & Building Press, 2017.

- [2] 彭奇彪, 罗华军, 佟来生, 等. 中低速磁浮车辆悬浮架的技术特征[J]. 电力机车与城轨车辆, 2012(6):7.

PENG Qibiao, LUO Huajun, Tong Laisheng, et al. Characteristics of maglev bogie for mid-low speed maglev vehicle[J]. Electric Locomotives & Mass Transit Vehicles, 2012(6):7.

- [3] 林科文. 低速磁浮列车过轨道台阶的悬浮控制研究[D]. 长沙: 国防科学技术大学, 2010.

LIN Kewen. Research on suspension control of low-speed maglev train running on step railway[D]. Changsha: National University of Defense Technology, 2010.

- [4] 刘建超, 赵春发, 姚力, 等. 温差和列车荷载作用下中低速磁浮轨道结构变形分析[J]. 铁道建筑, 2015(12):110.

LIU Jianchao, ZHAO Chunfa, YAO Li, et al. Deformation analysis of medium-low speed magnetic levitation track structure under temperature difference and train load action[J]. Railway Engineering, 2015(12):110.

(收稿日期:2021-04-19)