 DOI: https://doi.org/10.12349/edc.v4i11.994

Safety Protection System and Construction of Urban Rail Transit Signal System

Zhifan Hu Xiaowei Chen Jianwei Jing

Zhejiang Zhonghe Technology Co., Ltd., Hangzhou, Zhejiang, 310000, China

Abstract

With the continuous acceleration of national economic construction, the comprehensive development level of urban areas is improving day by day, the process of urban rail transit construction is facing development opportunities and challenges. Urban rail transit construction has become an important foundation in the infrastructure construction and planning content of the major cities. At the same time, the country and the society have gradually increased the importance of the safety of rail transit, therefore, the construction of safety protection system has been imminent. Based on this, this paper analyzes and discusses the safety protection system in the construction process of urban rail transit signal system, and makes a comprehensive analysis of the system construction process, in order to provide the corresponding reference and reference for the research of relevant scholars.

Keywords

urban rail transit signal system; safety protection system; construction; quality

城市轨道交通信号系统安全防护体系及构建思考

胡志帆 陈晓伟 荆剑伟

浙江众合科技股份有限公司，中国·浙江 杭州 310000

摘 要

随着国民经济建设速度的不断加快，城镇综合发展水平日益提升，城市轨道交通建设工作开展过程中正面临着发展机遇和挑战。城市轨道交通建设已经成为各大城市基础设施建设、规划内容中的重要基础。与此同时，国家和社会也逐渐提高了对轨道交通安全问题的重视程度，因此，安全防护体系的构建工作已经迫在眉睫。基于此，论文就城市轨道交通信号系统建设过程中的安全防护体系进行分析和讨论，并对体系构建过程进行全面分析，以期为相关学者的研究提供相应的参考和借鉴。

关键词

城市轨道交通信号系统；安全防护系统；构建；质量

1 引言

在计算机技术基础上，中国通信技术和信号系统已经逐渐实现有机结合，城市轨道交通的通信系统可以利用多种方式实现与其他公共系统的网络互连，如综合轨道监控系统、旅客信息登记系统、语音系统等，所以容易被网络病毒影响。由于公共网络连接的系统数量较多，再加上信号系统本身就存在一定的安全风险，所以一旦被网络病毒威胁，病毒威胁就会迅速向其他系统进行扩散。如果在扩散过程中被不法人员利用，那么就可能会影响社会生产生活的正常进行，大幅度提高行车安全事故发生率，因此加强信号系统的安全防护体系建设是无可厚非的[1]。

【作者简介】胡志帆（1983–），男，中国甘肃通渭人，本科，工程师，从事城市轨道交通通信信号的发展研究。

2 信号系统安全防护体系构建过程中所面临的诸多问题

城市轨道交通的网络建设工作已经成为中国轨道交通行业发展的“必经之路”。现阶段，大多数城市在对轨道交通建设过程中仍然面临着网络建设正处于起步阶段的问题，所以各方面内容都正处于探究和摸索阶段，影响建设的主要原因如下所示。

2.1 设备问题

由于轨道交通控制系统在应用过程中，与信息系统中的终端连接设备和控制设备的安全防护工作不到位，所以导致经常出现黑客入侵、违规操作，以及翻墙访问等问题，不仅会影响城市轨道交通信号系统的正常运转，还会导致该系统出现病毒感染的风险大大提高。

2.2 软件问题

城市轨道交通控制体系在应用过程中，由于在对信息系统进行远程操作和命令时，目录系统以及相关命令执行系

统等普遍存在系统漏洞问题和系统风险问题，所以导致控制系统中的敏感信息容易出现泄漏情况，服务器权限也可能会被不法分子进行恶意操控。这些问题是导致城市轨道交通控制体系应用效果无法得到有效保障的关键因素。

2.3 制度问题

由于部分管理人员并未意识到，城市轨道交通控制体系和信息系统网络安全相关规章制度以及应急方案和系统的重要性，所以并未对其进行完善构建，应急体系如图 1 所示。

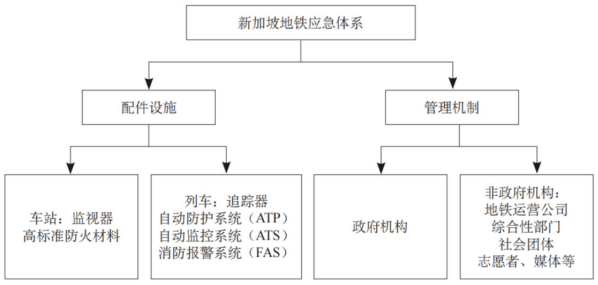

图 1 应急体系

3 信号系统安全防护体系构建过程中所面临的各项风险因素

作为指挥列车日常运行和调配的重要系统，信号系统的控制系统以及操作指令等行为等都与列车行进、停靠等密切相关。外界的恶意攻击或者是内部的错误操作等，都是导致安全问题频发的因素，通常这些错误操作以及控制指令都会通过网络系统进行传播，而大多数为操作指令都隐藏在看似较为常规的网络系统中，从网络的运行状态和运行过程来看，管理人员无法对流量所携带的内容，合法性和合理性进行精准判断，但是恶意操作指令势必会导致轨道交通信号系统出现中断情况，致使列车调度出现问题，运行停滞。通过全方位分析，可能导致轨道交通信号系统出现安全风险的主要因素如下所示。

3.1 区间内并未对访问控制系统进行设置

由于缺少相应的隔离防护措施，所以信号系统在运行过程中存在一定的不足之处。例如，信号系统在与轨道交通其他外部系统进行互联时，频繁发生无法正确识别外界不利影响因素，同时在各部门信息交流过程中经常出现信息串联现象，所以导致网络期间内的信息交流较为混乱，无论是哪个系统遭受网络病毒影响和感染，都会影响其他外部系统的正常运行，从而导致整体信号网络出现不良情况 [2]。

3.2 网络操作的不当行为

在信号系统网络信息交流过程中，由于大多数列车的运行数据不断交叉重叠，所以当出现异常不当操作行为时，势必会影响列车行经全过程。信号系统网络的故障问题主要是由于部分工作人员在网络操作时，出现不当行为所导致的，同时，如果缺乏有效的监管和审计，一旦发生安全问题，管理人员只能盲目地对问题的发生原因和过程进行探究，无法及时有效地解决问题。

4 城市轨道交通信号系统的具体构建过程探究

4.1 安全通信网络设计

由于城市轨道交通信号系统在应用过程中，本身就属于较为独立的实时控制数据传输系统，并且具备较为独立的专用网络，因此在对信号系统安全防护体系进行构建时，设计人员应该建立在公共防火墙技术上，实现安全防护体现与其他系统的安全隔离，并在安全措施基础上，提高对各个系统信息数据传输，以及未经授权的违法通信行为的限制 [3]。信息系统与其他外部系统之间的隔绝、阻断需要依赖于部署工控防火墙才能实现。在此情形下，信息系统的安全稳定性和独立完整性能够得到有效保障，避免信息系统受到其他系统故障问题的影响，同时能够实现对进出信号系统流量利用全过程的监管，避免异常流量和其他不当流量侵占轨道交通信号系统网络。

4.2 安全区域边界设置

4.2.1 访问控制防护系统设计

由于信号系统需要建立在业务基础上，所以信号系统再用过程中需要同时连接多种类型子系统，从而形成综合系统。就信号系统的构建过程可以得出，要想更好地形成区域范围内的安全保护，信号系统与其内部其他系统应该进行统一协调，从而保证信号系统的应用效率 [4]。与此同时，信号系统在构建过程中，仍然与其他外部系统有着紧密联系，如实时广播、轨道交通监控体系等。与轨道交通其他系统相比，信号系统网络较为独立，以这种设计方式，可能会导致企业对外互联边界模糊，在遭受外部恶意攻击后，通过互联网流量造成的信号系统问题会直接影响信号系统的正常运转。针对边界模糊问题，管理人员应该对安全威胁问题进行全方位分析和讨论，利用访问控制技术和外部互联系统对企业进行合理管控。信号系统在与其他系统进行我连接时，可以利用公共防火墙技术对系统的引擎和内容进行检测，同时对白名单技术进行访问、控制，实现通信全过程的精细化管理，保证信号系统所允许的业务交流和常规操作能够在清晰的边界范围内进行访问，避免出现并未经由业务系统的恶意访问行为，同时对信号系统的运行全过程进行实时监测，从而保证信号系统的安全稳定运行，检测范围如图 2 所示。

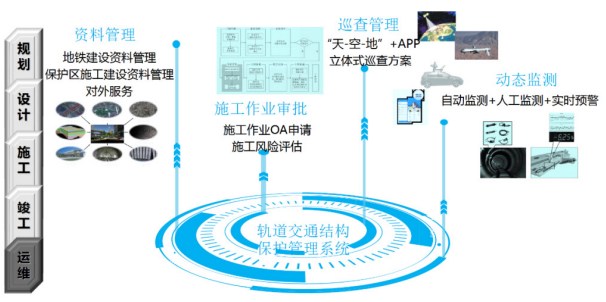

图 2 检测全过程

4.2.2 网络入侵防范管理

在对网络的入侵行为进行合理管控和防范时，主要是通过对各类信息数据拦截和异常不当行为的全方位分析并解决实现的。现阶段，在科技手段和信息化技术结构不断丰富的背景下，网络入侵防范技术得到了全面发展。网络流量和主机行为在信号系统网络构建过程中难度系数较低，所以较为简易。在白名单基础上对入侵防范技术进行设计，不仅能够有效提高网络防入侵效率，还能保证列车的安全稳定工作，这种方式更适用于信号系统的业务流程。通过对部署公共入侵检测和网络信号进行检测时，管理人员应该在控制中心基础上，设计并进行相应的安全方案以及功能，从而保证信号系统运行的安全稳定运转和审计能力。

4.3 防范恶意代码

由于城市轨道交通建设范围较为广泛，且涉及多种施工技术，所以建设难度较大。在构建信号系统时，设计人员主要采用的软件和协议都是具有合格生产厂家所签订的协议和专用的软件，所以具备较为强烈的行业特点。在部署访问控制数被构建过程中，管理人员应该提高对信号系统区域边界和、信号系统与其他外部系统之间的联系情况进行全面分析，在保证业务流程常规进行的同时，在最小化原则基础上，只有拥有专有协议的信号系统才能投入使用，而其他未经由专业协议认可的系统无法投入常规信号网络系统中。以这种方式，不仅可以有效降低恶意代码的安全风险，还能有效降低安全事故发生概率，保证信号系统的安全稳定运行[5]。

4.4 安全审计防护工作

审计工作需要建立在安全方案基础上，在记录用户信息和系统活动时，对操作事件的身体环境以及活动流程进行全面检测和验证，可以及时发现信号系统的漏洞问题以及其他入侵行为等。在此基础上，设计人员可以对交通信号系统的性能进行优化改善，在对信号系统的安全风险系数进行全面审查、评估时，管理人员和相关设计人员应该提出适当的改善措施，从而保证系统的安全稳定性。安全审计不仅能够帮助管理人员实时监控外界的入侵行为和不良影响因素，还能对内部人员的违规操作和恶意破坏行为进行全天监控，为网络违法行为以及其他犯罪行为的调查研究提供强有力的数据支持。

4.5 构建良好的安全计算环境

结合信号系统网络运行现状以及实际安全计算环境的特点，设计人员可以开启信号系统终端的安全防护体系，在“白名单”机制上实现对网络系统运行安全的防护。由于信号系统的建设过程较为复杂，所以系统应用存在一定的局限性、无法长时间在网络连接的基础上进行消毒库更新。由于工业组织的特点较为鲜明，所以传统的安全维护体系无法在长时间内进行信号系统完善、升级。对此，设计人员应该严格阻止白名单以外其他与信号系统无关的软件安装，同时对信号系统的运行全过程进行实时监测，从而保证信号系统的安全稳定运行[6]。

5 结语

由于城市轨道交通建设范围较为广泛，且涉及多种施工技术，所以建设难度较大。由于信息系统容易受到其他系统故障问题的影响，所以在安全防护体系及构建过程中，相关工作人员应该对安全通信网络、安全区域边界、防范恶意代码进行设计，同时做好安全审计防护工作，构建良好的安全计算环境，从而保证信号系统的安全稳定运行。

参考文献

[1] 曾小华.城市轨道交通信号系统互联互通的思考[J].中国信息化,2022(12):73-74.

[2] 曹启滨.城市轨道交通信号系统互联互通技术应用探讨[J].铁路通信信号工程技术,2022,19(11):59-64+88.

[3] 戴翌清.城市轨道交通信号系统更新改造需求分析[J].城市轨道交通研究,2022,25(11):14-17+22.

[4] 王春军.城市轨道交通信号系统安全防护体系建设研究[J].中国新通信,2022,24(10):107-109.

[5] 陈鑫鑫.城市轨道交通信号系统安全防护体系建设方案[J].自动化博览,2021,38(1):42-46.

[6] 王晔,陈丽娟,衣然保.2.0时代城市轨道交通信号系统网络安全防护新思路[J].信息技术与网络安全,2020,39(3):1-5.