

轨道交通工业控制系统信息安全：分析与展望

李浥东¹, 章子凯², 董海荣², 张洪磊¹, 陈灏瑜¹, 韩瑜珊¹

(1. 北京交通大学计算机与信息技术学院, 北京 100044;
2. 北京交通大学轨道交通控制与安全国家重点实验室, 北京 100044)

摘要: 轨道交通工业控制系统是国家重要的基础设施之一。随着信息技术的迅速发展和网络形势的逐渐严峻, 轨道交通工业控制系统信息安全受到了越来越多的关注。分析了轨道交通工业控制系统的系统组成, 总结了轨道交通工业控制系统面临的安全威胁种类, 举例剖析了轨道交通工业控制系统信息安全风险演化, 并进一步对轨道交通工业控制系统信息安全威胁趋势进行了解析。最后, 给出了轨道交通工业控制系统信息安全技术的发展建议。

关键词: 轨道交通工业控制系统; 工业控制系统信息安全; 威胁分析

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-6652.202114

Information security of the industrial control system for rail: analysis and prospect

LI Yidong¹, ZHANG Zikai², DONG Hairong², ZHANG Honglei¹, CHEN Haoyu¹, HAN Yushan¹

1. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China
2. State Key Lab of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China

Abstract: As one of the important national infrastructures, more and more attentions are attracted by the industrial control system for rail (ICS-R), with the rapid development of information technology and the increasingly severe network situation. The system composition of ICS-R was analyzed, the types of security threats faced by the ICS-R were summarized and analyzed, the practical cases of threat propagation were given, and the information security threat trend of ICS-R was analyzed considering the development trend of technology. Finally, several development suggestions were prospected as promising techniques.

Key words: industrial control system for rail, information security of industrial control system, threat analysis

1 引言

工业控制系统是计算设施、信息采集存储器、自动化操作的设备、生产线上的管理与监督等技术手段的总和, 由各种自动化控制组件以及对实时数据进行采集和监测的过程控制组件共同构成。保障工业控制系统信息安全是实施制造强国和网络强

国战略的重要保障。轨道交通工业控制系统(industrial control system for rail, ICS-R)是工业控制系统的一种特定类型, 作为关键信息基础设施, 其安全高效运行对于保障人民群众生命财产安全、维护社会安全稳定具有重要意义。

与传统的工业控制系统相比, 轨道交通工业控制系统有以下3个特点。第一, 轨道交通工业控制

收稿日期: 2021-04-15; 修回日期: 2021-05-15

通信作者: 章子凯, 18111064@bjtu.edu.cn

基金项目: 国家重点研发计划基金资助项目(No.2018YFB0803500); 工业企业侧安全数据采集设备项目(No. KKB920001534); 国家自然科学基金资助项目(No.KKA118001533)

Foundation Items: The National Key Research and Development Program of China (No.2018YFB0803500), Safety Data Acquisition Equipment for Industrial Enterprises (No. KKB920001534), The National Natural Science Foundation of China (No.KKA118001533)

系统的场景更复杂,包含车辆、车站、隧道、牵引供电系统等大量基础设施;第二,它包含的子系统内涵不清晰、场景不明确以及系统间的耦合机理缺乏深入研究;第三,轨道交通工业控制系统与传统工业控制系统的根本区别是以人为本,而人与系统的关系定义比较复杂。针对以上特点,轨道交通工业控制系统需要进一步分析和探讨。

截至2020年年底,我国累计开通运营城市轨道交通里程达到7 913 km,铁路运营里程达到14.63万 km,其中高速铁路运营里程达3.79万 km。随着轨道交通事业的蓬勃发展,其安全运行压力日趋加大。针对系统信息化融合趋势以及信息安全攻击愈演愈烈的形势,轨道交通信息安全面临巨大的威胁。因此,本文对轨道交通工业控制系统的内涵进行了梳理,分析了轨道交通工业控制系统的组成及其信息安全问题,并举例分析了其风险演化过程,最后结合信息技术与系统结构发展趋势对轨道交通工业控制系统的信息安全挑战进行了分析,并展望了未来防御技术的发展。

2 轨道交通工业控制系统内涵与构成

2.1 轨道交通工业控制系统的内涵

笔者在工业控制系统的基础上凝练轨道交通工业控制系统的内涵。作为工业控制系统的一种,轨道交通工业控制系统是指在轨道交通各主要子系统环境(如网络、信号、通信、列车控制系统等)以及各种业务流程(如交通管理、基础设施管理、维护、车站管理、旅客信息等)中参与过程控制、监控、自动化运行的多种控制组件以及提供相关信息服务的设备仪器的总称。

轨道交通工业控制系统与一般工业控制系统有以下区别。

- 距离:轨道交通系统覆盖了广阔的范围,其每个区域都必须与其相邻的区域、操作控制中心以及备份操作控制中心进行通信。
- 通信:通信机构需要与轨道上或附近的维修人员联络,与工程师/司机合作,在列车组和轨旁设备之间通信,以及在控制和信号装置之间通信。
- 系统结构:轨道交通工业控制系统中子系统繁多,分布式架构、集中式架构、分布集中式架构都在轨道交通工业控制系统中有所应用,系统层次以及宽度都远超一般的系统。
- 运行环境:轨道交通工业控制系统现场环

境比较复杂,有些设备现场环境比较恶劣,有些设备可以轻易地被非工作人员接触。

- 服务对象:轨道交通系统的目的是运送旅客。旅客是系统中宝贵的“货物”,他们希望、需要被安全“交付”。交通系统有许多大型的公共区域,包括出入口、站台、等候区和设施(如厕所、咖啡馆等),这些区域必须允许每个人进入;还有其他需要限制的领域,如设备和电力室、轨道、信号系统、员工区域等。

- 系统业务:轨道交通系统业务是离散业务与流程业务的混合。从轨道交通子系统来看,大部分与运输相关的子系统可以被看作流程业务,确保轨道交通的每一个环节在工作期间正常运行是管理的重点,任何一个环节出现故障,都会引起整个系统的瘫痪。但是,在面向旅客服务的相关系统中(例如车站子系统),单台设备的故障不会对整个过程产生严重的影响,一般只需要重点管理关键、瓶颈设备。

轨道交通工业控制系统与其他系统的区别见表1。

2.2 轨道交通工业控制系统的构成

轨道交通工业控制系统可以分为运行控制系统、牵引供电系统、车站系统、车载系统以及工务线路系统五大部分,如图1所示。其中运行控制系统包括中央控制系统、通信网络、地面控制系统和车载控制系统;牵引供电系统包括接触网系统、受电弓系统、牵引变电所系统、供电综合监控系统、供电安全检测监测系统(6C系统)和综合自动化系统;车站系统即车站上与自动控制相关的系统,包括旅客服务系统和运营保障系统;车载系统是指列车上除了车载运行控制系统之外的工业控制系统,包括车门系统、转向架系统、牵引系统、高压系统、辅助供电系统、制动系统、列车网络控制系统、供排水与卫生系统、车内环境控制系统以及烟雾报警检测系统;工务线路系统包括工务安全系统、线路检测维修系统、防灾安全监测系统和轨旁监测系统。轨道交通工业控制系统在各个系统的协同工作下,为旅客提供安全高效的出行服务。

(1) 运行控制系统

运行控制系统^[1]包括中央控制系统、地面控制系统、车载控制系统以及通信网络,负责对列车的运行速度进行控制,对列车和调车作业进行调度,以及对列车进行动态定位和收集道路的占用信息

表1 轨道交通工业控制系统与其他系统的区别

对比项	传统 IT 信息系统	一般工业控制系统	轨道交通工业控制系统
性能要求	不要求实时 可以忍受高时延和抖动 高吞吐量	实时通信 响应时间很关键 时延和抖动都在一定阈值内 适度吞吐量	部分子系统对实时通信要求更高 部分子系统可以忍受高时延和抖动，但是要求高吞吐量
风险管理	数据机密性和完整性最重要，可用性和容错次要，允许停机重启	操作人员的人身安全最重要，生产过程的保护和容错其次，不允许暂时停机	旅客和操作人员的人身安全最重要，生产过程的保护和容错其次，部分系统允许暂时停机
网络结构	扁平化结构 主从关系不明显	纵向高度集成 主从关系明显	庞大混杂的结构，既存在扁平化结构，也存在纵向高度集成
网络边缘	通用计算机 物理安全需求不高	传感器和远动装置 对物理环境有要求 对员工区域有限制，可以进行设备隔离	工业计算机、服务器、传感器、远动装置 物理环境复杂多样，对物理安全有更高的要求 部分设备容易被非操作人员接触到
通信内容	一般信息	遥测、遥信、遥控、遥调信息	既有用于操作人员间及操作人员与设备间合作联络的一般信息，也有遥测、遥信、遥控、遥调信息
系统业务	信息的传播、处理、存储	离散工业或流程工业业务	人员运输业务，其每个子过程都可以被看作流程工业业务 旅客服务业务、离散工业业务以及一般信息服务业务

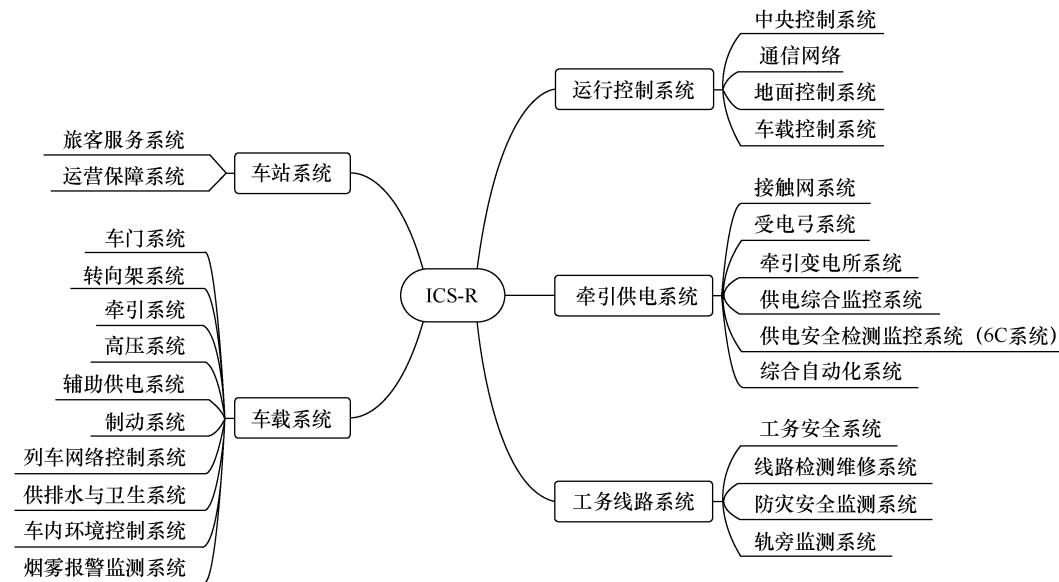


图1 轨道交通工业控制系统

等，确保列车运行安全，提高运输效率。

(2) 牵引供电系统

根据电力系统的服务方式，牵引供电系统^[2]可以被分为基础供电和安全检测两大类工业控制系统。基础供电工业控制系统包括接触网系统、受电弓系统、牵引变电所系统以及综合自动化系统，负责连接变电所内的强流设备和高压设备，并通过受电弓系统与接触网系统使高速列车获得持续稳定的动力供给。安全检测工业控制系统包括供电综合监控系统以及供电安全检测监测系统，负责对现场牵引变电所、AT 所和分区所的运行设备进行监视和控制，对高速接触网悬挂参数和弓网运行参数进行实时检测，保证供电设备的安全。

(3) 车站系统

车站系统^[3]包含旅客服务系统和运营保障系统。旅客服务系统的主要目的是保障旅客和工作人员的人身安全，方便旅客购票、休息、乘车。车站系统具体包含安检系统、自动检票系统、自动门禁系统、客运广播系统、视频监控系统、电子引导系统、旅客求助系统等。运营保障系统主要是为了保障车站的正常运营以及对列车进行服务，主要包括智能车辆防溜系统、车号自动识别系统、智能上水系统、电源及环境监测系统、火灾消防系统、机电设备管理系统、旅服设备监控系统、气力垃圾收集输送系统以及污水处理自动控制系统等。

(4) 车载系统

车载系统^[4]分为两类,一类是列车运行基础控制系统,另一类是车载生活配套控制系统。列车运行基础控制系统包括车门系统、转向架系统、牵引系统、高压系统、制动系统、列车网络控制系统等,负责列车的安全运行控制、列车内部系统的控制和诊断以及与牵引系统的连接,保障列车正常行驶。车载生活配套控制系统包括辅助供电系统、供排水与卫生系统、车内环境控制系统、烟雾报警监测系统等,主要负责高速列车内部的供电、照明、排水、环境控制以及火灾监测。

(5) 工务线路系统

工务线路系统主要包括工务安全系统^[5]、线路检测维修系统^[6]、防灾安全监测系统^[7]以及轨旁监测系统^[8]4个部分。

工务安全系统包含路基安全系统、隧道运营机械通风监控系统、桥梁水文检定检算系统以及沿线地理地貌系统等,负责对铁路沿线的路基、隧道、桥梁等设施进行相关监测及灾害报警,同时将路网的设备和资源存储在计算机中,提供自动化信息处理工具和决策支持,与铁路的其他信息系统沟通交流。

线路检测维修系统包括轨检、动检、探伤、道岔缺口监测、道岔阻力监测、轨温监测等功能,设备分为便携式和车载式两种,其工业控制系统比较简单,集成度不高^[9]。

防灾安全监控系统包括大风预警系统、融雪监测系统、雨量监测系统、冻土监测系统、异物侵限系统等,负责铁路沿线风、雨、雪、洪水等自然灾害的监测,以及轨道沿线的异物入侵检测和突发事件的安全监控与报警^[10]。

轨旁监测系统包含地面安全监测系统、红外线轴温探测系统、车辆运行故障动态图像检测系统、线路状态监测系统以及通信信号设备监测系统等,负责对线路轨旁的通信信号、列车运行状态以及线路设备和环境影响进行安全监测,保证行车安全。

3 轨道交通工业控制系统信息安全分析

3.1 轨道交通工业控制系统的信息安全威胁分析

过去轨道交通工业控制系统的安全问题一直聚焦在功能安全的范畴,认为轨道交通工业控制系统依赖专有的、隔离的网络,使用特定的协议管理、通信和发送信号,不存在较大的信息安全威胁。然而,随着信息技术推动轨道交通工业控制系统的不断

断进步,轨道交通工业控制系统信息安全将面临许多挑战。面对信息安全挑战,笔者对各个轨道交通工业控制子系统进行安全分析,总结出6种主要的轨道交通工业控制系统信息安全威胁。

(1) 运行环境导致的信息安全威胁

雷击、温度、湿度等物理环境导致设备损坏^[11],电压电流异常引起交直流电源设备故障,进而影响设备正常运行。

例如,由于铁路供电电源电压波动较大,网络防火墙等网络安全设备在此环境下很容易损坏,造成后期维护难度大、故障率高、使用效果不佳等问题。以某变电所为例,电网电能质量差,电压谐波大,电压波动范围达到 $\pm 30\%$;防灾系统抗雷击能力较差,汛期经常遭雷击及雨水侵蚀而损坏;轨旁信号系统抗极寒能力较差,冬季可能会造成宕机^[12]。

(2) 网络结构导致的信息安全威胁

该类信息安全威胁包括网络接口导致的漏洞^[13]、网络协议导致的漏洞、网络权限管理导致的漏洞、网络风险传播导致的安全威胁等^[14]。

例如,列车通信网络是列车总线和车辆总线的二层结构,列车总线连接不同的车辆或动车组单元,贯穿整个列车。高速动车组 CRH1 和 CRH3 采用多功能车辆(multifunction vehicle bus, MVB)+绞线式列车(wire train bus, WTB)总线,CRH5 采用 MVB+WTB 总线及控制器局域网络(controller area network, CAN)总线、CRH380CL 采用 RS485 通信^[15]。MVB 协议及 Modbus 协议存在缺乏认证、缺乏授权、缺乏加密、在设计时对安全问题的考虑很少以及功能码的滥用等问题。此外,WTB 节点处于终端模式时,其两个通道相互独立,为中间人攻击提供了物理基础。对于 CAN 总线来说,其内置安全功能主要是为了保证通信的可靠,而不是网络安全,因此,CAN 无法防止车载网络免受网络攻击。

门禁的控制建立在特定的智能化系统上^[16],并为相关人员进行操作留出了外部接口。当这些系统被入侵时,攻击者就会获得全部权限,对系统进行任意操作。目前常见的门禁控制系统漏洞有 IDenticard Systems 公司门禁系统产品 IDenticard Premisys 的信任管理问题漏洞 CVE-2019-3909,该漏洞源于系统默认的用户名和密码。远程攻击者可利用该漏洞获取全部访问权限。

客运服务、运营商、车站、运营、维护等系统

被由不同的网络硬件、网络软件和网络管理服务组成的通信网络连接在一起。系统的互联互通是一把双刃剑。广泛的通信网络连接允许所有相关伙伴传输信息,提高了系统间协作效率,但它们也带来了新的网络入侵路径,增大了系统安全风险。

(3) 平台系统导致的信息安全威胁

该类信息安全威胁包括工业主机漏洞,数据库及云平台安全漏洞,主机、传感器、控制器故障导致的信息错误或缺失等。例如,供电监控系统上线后基本不会升级,而操作系统漏洞会导致操作站和服务器暴露在风险中。

在目前轨道交通 IT 系统中广泛应用的 Windows 和 UNIX 操作系统中,也存在着大量的安全漏洞,很容易受到外部攻击,引发信息安全事件。操作系统漏洞主要表现在获取控制、拒绝服务、获取信息 3 个方面^[17]。常见的获取控制漏洞主要有 Microsoft Windows 远程过程调用安全漏洞 CVE-2021-1664、Microsoft Windows 远程执行代码漏洞 CVE-2016-0118、Microsoft Windows 远程桌面模块访问控制错误漏洞 CVE-2021-1674 等。常见的拒绝服务漏洞主要有 Linux kernel 拒绝服务漏洞 CVE-2016-9919、Microsoft Windows 本地安全认证子系统服务拒绝服务漏洞 CVE-2016-7237、Microsoft Windows 拒绝服务漏洞 CVE-2016-3369 等。常见的获取信息漏洞主要有 Linux 敏感信息漏洞 CVE-2013-3235、Microsoft Windows 信息泄露漏洞 CVE-2020-1033、Microsoft SharePoint 信息泄露漏洞 CVE-2019-1202 等。

此外,在系统权限上,还存在注入攻击及跨站脚本攻击威胁。注入攻击对存储在系统中的数据进行随意的增删改查。常见的注入攻击漏洞有 Maxum Rumpus 命令注入漏洞 CVE-2020-27575、Kentico SQL 注入漏洞 CVE-2021-27581、Matthias Van Woensel qcubed SQL 注入漏洞 CVE-2020-24913 等。跨站脚本攻击在系统中植入个人脚本,当正常用户进行访问时,脚本会对用户输入的信息进行窃取,或者对用户的信息进行恶意修改。常见的跨站脚本漏洞有 TIBCO Spotfire Server 跨站脚本漏洞 CVE-2021-23273、Time in Status 跨站脚本漏洞 CVE-2021-27222 等。

(4) 通信导致的信息安全威胁

该类信息安全威胁包括电磁干扰、拒绝服务、消息篡改、错误信息注入、未经授权访问、被动窃

听、主动拒绝控制和承担控制权攻击等。

牵引变电所设备由于缺乏网络安全措施,容易遭到黑客各种形式的恶意攻击和破坏,甚至遭到集团式攻击,严重时可导致电气化铁路牵引变电所内网络系统崩溃,严重影响铁路的正常运行^[18]。为了加强网络防护,牵引变电所内部增加了普通防火墙,但是,防火墙一般在进行 IP 数据包转发的同时通过对 IP 数据包的处理实现对 TCP 会话的控制,对应用数据的内容不进行检查。该工作方式无法防止泄密,也无法防止病毒和黑客程序的攻击。如果在防火墙的基础上增加隔离装置,又与铁路设备高集成度且功能多元化的要求背道而驰。

对于铁路综合数字移动通信系统(global system for mobile communications-railway, GSM-R)来说,虽然其在无线通信中进行了加密,但是在其骨干网中没有加密,存在和 GSM 一样的安全漏洞。

对于轨旁信号系统及其设备来说,存在电磁干扰(存在于应答器设备,损害其信息可用性)、拒绝服务(存在于多种人机接口)、消息修改(存在于轨旁监测系统)及未经授权的访问(存在于信息显示系统)、被动窃听、主动拒绝控制和承担控制权等安全威胁^[19-20]。

(5) 应用软件导致的信息安全威胁

调度软件、控制软件等专业应用程序在开发之初就考虑到了安全问题,因此相对安全。然而,其他服务器软件、办公软件、打印机软件等常见商业软件存在大量的漏洞,对信息安全造成了潜在的风险。

例如,对于办公软件来说,存在快捷方式文件解析漏洞(MS10-046)^[21]、各种 Office 漏洞(cve-2017-11882、CVE-2018-0802 等),这些漏洞利用办公文件及软件进行运行,加载指定的恶意 DLL 文件,从而触发后者中的恶意代码。

打印机漏洞^[22]更是层出不穷。利用打印机漏洞,黑客们可以进行远程代码执行、横向移动、无线跳变、数据盗窃、拒绝服务、远程代码执行、权限升级,以及造成物理损坏(甚至引发火灾)^[23]。

路由器漏洞也通过 IT 系统进一步威胁控制系统的安全,常见的漏洞有应用程序托管漏洞 CVE-2019-1663、授权控制中的特权提升漏洞 CVE-2020-3227、远程命令/代码执行漏洞(remote code execution, RCE)、远程执行代码漏洞 CVE-2020-3198 和命令注入漏洞 CVE-2020-3205 等。

(6) 人员疏忽或误操作导致的信息安全威胁

工作人员在系统配置时没有对一些系统中的默认值做安全性配置,访问口令往往极易被破解,如果工作人员疏忽或进行违规操作,就极有可能使系统遭受非法攻击。此外,工作人员的非法网络访问、非法硬件接入、非法权限管理等操作都能对信息安全造成巨大威胁^[24]。

例如,系统在初始状态时有统一的默认用户名和密码,如果工作人员对此不做修改,就极有可能使系统遭受非法攻击。

高铁供电综合监控系统具有分层分布式大型检测监测系统的结构特性。在供电安全检测监测过程中,存在随意使用 U 盘、光盘、移动硬盘等移动存储介质的现象,有可能将传染病病毒、木马等威胁因素带入生产系统。加上防病毒软件的安装不全面或者即使安装后也不及时更新防恶意代码软件版本和恶意代码库,出现问题后无法及时确定产生问题的原因、影响范围,以及追究责任^[25]。

对于供电综合监控系统来说,存在上线前未关闭多余的系统服务以及未对系统的密码策略等进行安全加固的问题。除此之外,运维人员在调试过程中需要对操作站和服务器安装一些软件,为了方便调试,会开启一些操作系统远程服务功能,上线后通常不会屏蔽这个功能,从而使得安全配置略为薄弱的操作站系统特别容易遭受攻击^[26]。电力基础设施在实际的运行期间,相关生产设备经常存在一些安全隐患。例如,相关设备长时间在大风、多雨的恶劣环境下运行,其主要功能会发生一定的变化,加上人为因素的不断破坏,电力系统会在得不到有效维护的同时,发生一系列的网络安全故障,丢失大量重要信息,影响自动化调度工作的有效进行。在电网调度过程中,自动化拨号的管理模式会使系统的安全性下降^[27]。

3.2 轨道交通工业控制系统信息安全风险演化案例分析

笔者在第 3.1 节总结了 6 种主要的轨道交通工业控制系统信息安全威胁,然而轨道交通工业控制系统是一个复杂的控制系统,各子系统之间既存在网络通信上的耦合关系,又存在业务功能上的耦合关系。因此,对轨道交通工业控制系统的信息安全分析不仅要考虑当前系统各子部分或者单个设备上的信息安全风险,还要考虑信息风险的演化引发的网络安全风险以及业务功能安全风险。以工务线

路系统、运行控制系统和牵引供电系统为例,在工务线路系统中的防灾预警子系统与运行控制系统的通信进行耦合。而工务线路系统与运行控制系统又需要牵引供电系统提供电力才能正常运行。

轨道交通工业控制系统信息安全风险分析如图 2 所示,以工务线路系统操作终端为起点,可以由网络通信将风险传播至运行控制系统。攻击者首先从工务线路系统操作终端入侵监控网,如果此时获取监控站机的控制权限,就可以将风险传播至通信控制服务器;利用通信控制服务器的安全漏洞,获取分散自律调度集中系统(centralized traffic control system, CTC)接口的控制权限,然后就可以将风险传播至 CTC 车站自律机;CTC 车站自律机又可以将风险传播至计算机联锁,然后利用路由器漏洞或者配置不当漏洞将风险扩散至维护网和信号数据网;利用网络通信协议漏洞,可以进一步将风险传播至轨旁设备。与此同时,牵引供电系统与工务线路系统和运行控制系统有安全隔离。然而,牵引供电系统若存在信息安全风险,则会导致工务线路系统和运行控制系统部件的非正常运行,进而会导致系统信息的缺失或者系统的瘫痪。

通过以上分析,笔者建立了基于图的轨道交通工业控制系统风险演化模型,如图 3 所示。风险演化图 $G=(N, E)$ 。其中, N 是风险演化图中的节点,对应轨道交通工业控制系统中各子部分; E 是风险传播路径,对应轨道交通工业控制系统中各子部分之间的风险耦合关系。 X 表示节点的风险属性矩阵, A 表示风险图的邻接矩阵,其中 X_i 表示 N_i 的风险集合向量, A_{ij} 表示风险在 N_i 和 N_j 之间的传播概率。定义轨道交通工业控制系统风险演化图中的节点所对应的安全威胁程度为 $W=\{w_i\}$,其中 w_i 为 N_i 的安全风险系数。

在 n 次风险传播后,轨道交通工业控制系统风险演化图的风险矩阵 $P(P \in R^{N \times N})$ 、风险度量向量 $Risk(Risk \in R^{N \times 1})$ 可以由式 (1)、式 (2) 计算得到:

$$P=(A+I_A)^n \cdot X \quad (1)$$

$$Risk=P \cdot W \quad (2)$$

其中, I_A 表示邻接矩阵 A 的对角矩阵。

定义安全威胁影响因子为 $F=\{f_i\}(F \in R^{N \times 1})$,其中 f_i 为 N_i 的安全风险在整个系统里的影响水平。那么,在 n 次风险传播后,轨道交通工业控制系统风险演化图的整体风险 R_s 为:

$$R_s=Risk^T \cdot F \quad (3)$$

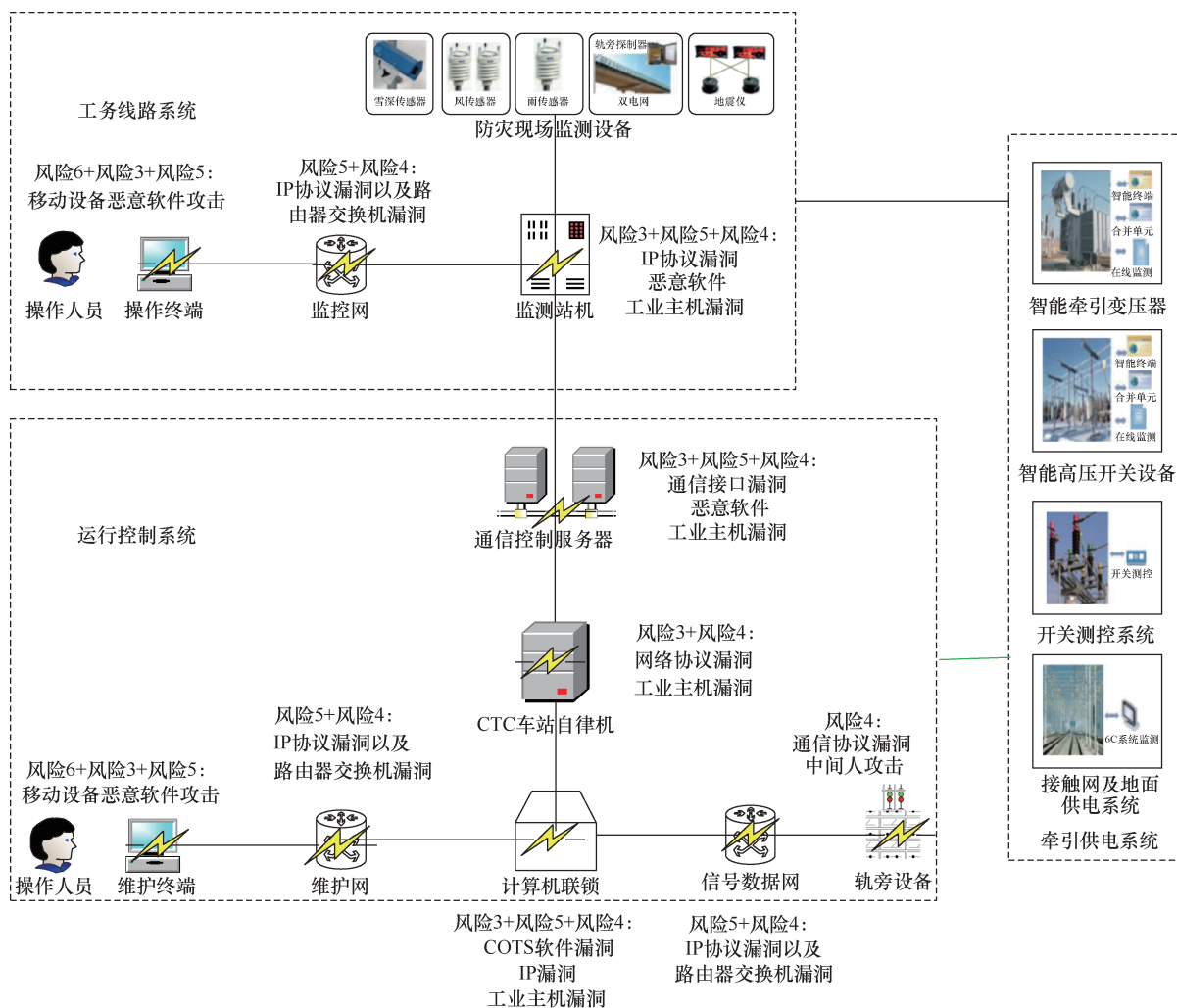


图2 轨道交通工业控制系统信息安全风险分析

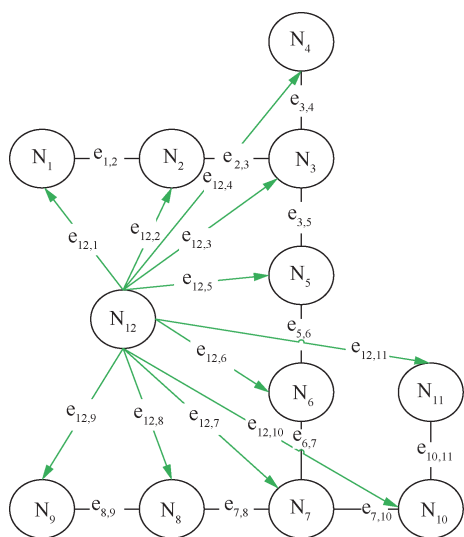


图3 基于图的轨道交通工业控制系统信息安全风险演化模型

总而言之，各风险源（或风险传播途径）对信息安全的威胁不仅受到其自身传播概率和危害程

度的影响，也与风险网络耦合关系以及风险属性密切相关。轨道交通工业控制系统之间的耦合关系十分复杂，给系统信息安全带来了更大的挑战。为此，研究人员需要仔细梳理各系统之间的耦合关系，延展信息安全边界，在更大范围内建立整体的、动态的、开放的、相对的和共同的安全观^[28]，为轨道交通工业控制系统建立信息安全纵深防御体系提供基础支撑。

3.3 轨道交通工业控制系统信息安全发展趋势分析

多年以来，轨道交通工业控制系统信息安全得到了广泛的研究，并产生了一些行之有效的解决方案。但是，随着技术的进步和工业控制技术的发展^[29]，人们又面临着一些新的问题。

（1）轨道交通系统越来越互接和开放，资源共享越来越普遍，协议越来越标准化。例如：轨道交通工业控制系统底层数据接口接入数据中心（以计

算机联锁为例,联锁的内部数据不仅在本地保存,还通过维护网络上传到云数据中心,用于设备故障分析和健康管理);轨道交通工业控制系统通信通道不再是信令专有和独占的,而是与其他服务或类型的用户共享的;轨道交通工业控制系统使用的协议和组件从专有技术和协议到标准化逐渐发展。

(2) 铁路技术正变得越来越具有互操作性和一致性。基于 TCP/IP,轨道交通工业控制系统在网络层会受到与一般系统同样的攻击。

(3) 威胁(基于人力和自动化技术)正在快速适应传统安全检测方法。近年来针对商业和个人计算机的恶意代码攻击显著增加,如勒索病毒、分布式拒绝服务(distributed denial of service, DDoS)攻击,由于工业化系统很少做安全升级,商用系统已修复的熟知的安全漏洞也可能被攻击者利用。

(4) 轨道交通基础设施的异构性和广泛的地理分布使系统的多层网络物理拓扑更容易暴露在网络攻击之中,潜在地在相同或不同的安全区域涉及或触发多米诺骨牌效应。

(5) 随着产品集成度的提高,软件代码量成倍增长,开发者将开源库作为工业控制系统软件基础组件。因此,开源软件的潜在漏洞可能被攻击者利用,从而对工业控制系统安全造成威胁。

4 轨道交通工业控制系统信息安全的展望

随着技术的进步和轨道交通行业的发展,轨道交通工业控制系统信息安全存在一些新的问题。面对这些问题,故步自封、拒绝采用新技术是不可取的。完全替换或重新设计现有的系统和基础设施是不现实的,甚至是不可能的。从防御的角度出发,在现有的系统基础上,为了适应技术的发展趋势,需要进一步研究的内容如下。

(1) 更加智能化的实时风险评估

风险评估是进行信息安全风险防御的第一步,是信息安全中心进行信息安全监控的重要组成部分。获取不同等级的安全信息,进行实时的安全信息融合和分析预测,是信息安全事件快速响应的前提。面对新的安全威胁,快速的安全防御是消减安全破坏等级和保证运行效率的必要手段。

(2) 纵深防御与安全边界

网络安全的纵深安全防御原则与网络架构的合理安全边界划分能够限制网段之间以及网段与工业主机之间的流量,进行不同层级与不同区域的

安全隔离,减少系统以及子系统的攻击面,限制信息安全风险的传播,减少信息安全风险的影响。

(3) 异常风险检测与识别

异常风险检测与识别技术是有效的轨道交通工业控制系统方法,能够在风险发生之前或者风险发生早期对系统进行保护。与防火墙技术、加密技术、虚拟专用网络(virtual private network, VPN)技术相比,异常风险检测与识别技术更加主动地对系统进行防御,对不同层级的目标(设备、数据、软件、网络、系统等)进行检测,能够适用于信息和业务高耦合的轨道交通工业控制系统。

(4) 交互限制、流量分割与虚拟化技术

针对轨道交通的业务特点,可以采用单向安全隔离网关技术和网络虚拟化技术,对信息流进行控制和分离。当网络流量在不受信任的网络上传输时,可以在加密隧道中隔离。例如, certMILS^[30]是基于 EURO-MILS 项目的研究成果,通过虚拟化提供安全隔离,减轻关键基础设施中的新网络威胁。美国国家安全局(National Security Agency, NSA)提出了3种不同的机制对网络进行分离,分别是通过 VLAN(virtual LAN)的流量控制机制、通过 IPsec(Internet protocol security)的加密网络通道机制、通过 SSH(secure shell)的加密应用通道和 TLS(transport layer security)机制。

5 结束语

本文从轨道交通工业控制系统的内涵、系统组成以及各子系统的信息安全问题出发,总结并分析了轨道交通工业控制系统面临的安全威胁种类,列举并分析了轨道交通工业控制系统信息安全风险演化案例,并结合安全技术、体系结构和软件技术的发展趋势,分析了轨道交通工业控制系统信息安全问题的未来风险,进而从防御的角度展望了技术发展的趋势。

参考文献:

- [1] 中国铁路总公司. CTCS-3 级列车运行控制系统[M]. 北京: 中国铁道出版社, 2013.
China Railway Corporation. CTCS-3 train operation control system[M]. Beijing: China Railway Publishing, 2013.
- [2] 钱清泉, 高仕斌, 何正友, 等. 中国高速铁路牵引供电关键技术[J]. 中国工程科学, 2015(4): 9-20.
QIAN Q Q, GAO S B, HE Z Y, et al. Study of China high-speed railway traction power supply key technology[J]. Engineering Science, 2015(4): 9-20.

- [3] 中华人民共和国交通运输部. 城市轨道交通运营技术规范: GB/T 38707-2020[S]. 2020.
Ministry of Transport of the People's Republic of China. Regulation for operation technology of urban rail transit: GB/T 38707-2020[S]. 2020.
- [4] 梁建英, 杨中平, 张济民. 中国高铁丛书: 高速列车[M]. 上海: 上海科学技术文献出版社, 2019.
LIANG J Y, YANG Z P, ZHANG J M. China high speed rail series: high speed train[M]. Shanghai: Shanghai Scientific and Technological Literature Press, 2019.
- [5] 马化洲. 城市轨道交通线路轨道系统安全风险评价[D]. 北京: 北京交通大学, 2011.
MA H Z. Safety risk assessment of urban rail transit line rail system[D]. Beijing: Beijing Jiaotong University, 2011.
- [6] 梁建英, 杨中平, 张济民. 中国高铁丛书: 高铁线路工程[M]. 上海: 上海科学技术文献出版社, 2019.
LIANG J Y, YANG Z P, ZHANG J M. China high speed rail series: high speed rail line engineering[M]. Shanghai: Shanghai Scientific and Technological Literature Press, 2019.
- [7] 李晓宇, 刘敬辉. 高速铁路自然灾害及异物侵限监测系统可靠性分析与优化研究[J]. 中国铁路, 2019(5): 27-32.
LI X Y, LIU J H. Reliability analysis and optimization of HSR natural disaster and intrusion monitoring system[J]. China Railways, 2019(5): 27-32.
- [8] 王俊, 王江丽. 高速铁路防灾安全监控系统设计[J]. 中国安全科学学报, 2018, 28(S1): 39-45.
WANG J, WANG J L. Design of disaster prevention and safety monitoring system for high-speed railway[J]. China Safety Science Journal, 2018, 28(S1): 39-45.
- [9] 侯智雄, 李颖, 魏世斌, 等. 城市轨道交通轨道检测系统关键设备研制及应用[J]. 铁道建筑, 2020, 60(1): 103-107.
HOU Z X, LI Y, WEI S B, et al. Development and application of key equipments for urban rail transit track detection system[J]. Railway Engineering, 2020, 60(1): 103-107.
- [10] 孙汉武. 铁路安全检查监测保障体系及其应用研究[D]. 成都: 西南交通大学, 2010.
SUN H W. Study on railway safety inspection and monitoring of security system[D]. Chengdu: Southwest Jiaotong University, 2010.
- [11] 赵治国, 徐跃, 马谢, 等. 雷电电磁环境对高速列车影响分析方法研究[J]. 通信技术, 2019, 52(9): 2207-2211.
ZHAO Z G, XU Y, MA X, et al. Analysis method of impact of lightning electromagnetic environment on high-speed trains[J]. Communications Technology, 2019, 52(9): 2207-2211.
- [12] 廖喜. 铁路防灾安全监控系统的组成[J]. 铁道运营技术, 2017, 23(2): 67-70.
LIAO X. The composition of railway disaster prevention and safety monitoring system[J]. Railway Operation Technology, 2017, 23(2): 67-70.
- [13] 陈超群, 陈勃, 刘布麒, 等. 轨道交通网络信息安全防护系统研究与设计[J]. 电气技术, 2020, 21(2): 50-55.
CHEN C Q, CHEN B, LIU B Q, et al. Research and design of information security protection system for rail transit network[J]. Electrical Engineering, 2020, 21(2): 50-55.
- [14] 戎志杰. 轨道交通车辆 MVB 总线安全态势感知方法的仿真研究[D]. 太原: 太原科技大学, 2018.
RONG Z J. Simulation research on MVB security situational awareness method of rail vehicles[D]. Taiyuan: Taiyuan University of Science and Technology, 2018.
- [15] 万海, 孙雷, 王恬, 等. 列车通信网络 WTB 链路层攻击方法研究[J]. 清华大学学报(自然科学版), 2016, 56(1): 42-50.
WAN H, SUN L, WANG T, et al. Analysis of a method for attacking WTB link layers in a train communication network[J]. Journal of Tsinghua University (Science and Technology), 2016, 56(1): 42-50.
- [16] 华鹏, 李艳娇, 辛久元. 高速列车车门系统 FMEA 及风险评估案例研究[J]. 现代城市轨道交通, 2018(3): 18-21.
HUA P, LI Y J, XIN J Y. Case study on FMEA and risk assessment of high speed train door system[J]. Modern Urban Transit, 2018(3): 18-21.
- [17] 付淳川. 高速铁路信号系统网络安全风险评估方法研究[D]. 成都: 西南交通大学, 2017.
FU C C. Research on network security risk assessment method for high-speed railway signal system[D]. Chengdu: Southwest Jiaotong University, 2017.
- [18] 王朋成. 电铁牵引变电所内部数据传输网络安全防护研究[J]. 电气化铁道, 2020, 31(z2): 66-68.
WANG P C. Research on internal data transmission network security protection of electric railway traction substation[J]. Electric Railway, 2020, 31(z2): 66-68.
- [19] 廖元媛, 王剑, 田开元, 等. 基于贝叶斯推理的铁路信号安全数据网信息安全动态风险评估[J]. 铁道学报, 2020, 42(11): 84-93.
LIAO Y Y, WANG J, TIAN K Y, et al. Dynamic information security risk assessment for railway signaling safety data network based on Bayesian inference[J]. Journal of the China Railway Society, 2020, 42(11): 84-93.
- [20] 郭亮, 余骞, 袁雪冰. 典型地面信号系统的信息安全分析[J]. 中国铁路, 2020(2): 11-16.
GUO L, YU Q, YUAN X B. Information security analysis of typical ground signal system[J]. Chinese Railways, 2020(2): 11-16.
- [21] 张伟, 李宁, 杨康. Windows 快捷方式漏洞分析[J]. 网络安全技术与应用, 2011(1): 29-31.
ZHANG W, LI N, YANG K. Analysis of Windows shortcuts vulnerability[J]. Network Security Technology and Application, 2011(1): 29-31.
- [22] 田思. 网络打印机应用层协议安全检测技术研究与实现[D]. 北京: 北京邮电大学, 2019.
TIAN S. Research and implementation of network printer application layer protocol security detection technology[D]. Beijing: Beijing University of Posts and Telecommunications, 2019.
- [23] National Security Agency. Commercial solutions for classified Handbook[S]. 2017.
- [24] 高尚省, 郭勇, 高智伟, 等. 广东省数字政府网络安全评估体系与实践[J]. 大数据, 2021, 7(2): 182-188.
GAO S X, GUO Y, GAO Z W, et al. Practice of digital government network security index evaluation system in Guangdong Province[J]. Big Data Research, 2021, 7(2): 182-188.
- [25] 何正友, 冯玓, 林圣, 等. 高速铁路牵引供电系统安全风险评估研究综述[J]. 西南交通大学学报, 2016, 51(3): 418-429.
HE Z Y, FENG D, LIN S, et al. Research on security risk assessment for traction power supply system of high-speed railway[J]. Journal of Southwest Jiaotong University, 2016, 51(3): 418-429.
- [26] 王捷, 王晋, 刘畅. 电力调度自动化网络安全防护系统研究[J]. 电

力系统装备, 2017(11): 88-89.

WANG J, WANG J, LIU C. Research on network security protection system of power dispatching automation[J]. Electric Power System Equipment, 2017(11): 88-89.

- [27] 马英晖. 高速铁路牵引供电系统安全风险综述[J]. 区域治理, 2018(46): 198.

MA Y X. Research on security risk for traction power supply system of high-speed railway[J]. Regional Governance, 2018(46): 198.

- [28] 李涪东, 张俊, 陶耀东, 等. 平行安全: 基于 CPSS 的生成式对抗安全智能系统[J]. 智能科学与技术学报, 2020, 2(2): 194-202.

LI Y D, ZHANG J, TAO Y D, et al. Parallel security: generative adversarial systems for intelligent security in CPSS[J]. Chinese Journal of Intelligent Science and Technology, 2020, 2(2): 194-202.

- [29] 赵亚楠. 工业控制系统信息安全 2020 年十大发展趋势[J]. 自动化博览, 2020, 37(3): 14-17.

ZHAO Y N. Ten development trends of industrial control system information security in 2020[J]. Automation Panorama, 2020, 37(3): 14-17.

- [30] TVERDYSHEV S. Security by design: introduction to MILS[C]// MILS Workshop. [S.l.:s.n.], 2017.

[作者简介]



李涪东 (1982-), 男, 博士, 北京交通大学计算机与信息技术学院副院长、教授、博士生导师, 智能交通数据安全与隐私保护技术北京市重点实验室副主任。主要研究方向为大数据智能、数据隐私保护、先进计算、智能交通等。在 *IEEE Transactions on Information Forensics and Security*、*IEEE Transactions on Knowledge and Data Engineering*、*IEEE Transactions on Intelligent Transportation Systems*、*IEEE Transactions on Computers* 等国际学术期刊和 SIGKDD、CVPR、AAAI 等会议上发表学术论文 100 余篇。曾主持国家自然科学基金重大/重点项目、国家重点研发计划、工信部工业互联网创新发展工程项目等 20 余项省部级以上课题。担任中国计算机学会理事、青年计算机科技论坛主席、大数据专家委员会委员、高性能计算专业委员会委员, 中国自动化学会控制理论专业委员会副秘书长、大数据专业委员会委员、平行智能专业委员会委员。曾担任多个国际会议的程序委员会主席、分会主席、程序委员会委员。曾获北京市科学技术进步奖二等奖、中国自动化学会科学技术进步奖一等奖、詹天佑铁道科学技术奖专项奖, 以及 IEEE 国际会议最佳论文奖等。



章子凯 (1989-), 男, 北京交通大学轨道交通控制与安全国家重点实验室博士生, 主要研究方向为工业控制系统安全、信息安全、人工智能。



董海荣 (1974-), 女, 博士, 北京交通大学轨道交通控制与安全国家重点实验室教授, 主要研究方向为列车运行智能控制与优化、调度控制一体化。



张洪磊 (1993-), 男, 北京交通大学计算机与信息技术学院博士生, 主要研究方向为人工智能安全、推荐系统、隐私保护。



陈颖瑜 (1995-), 男, 北京交通大学计算机与信息技术学院博士生, 主要研究方向为隐私保护、智能交通。



韩瑜珊 (1996-), 女, 北京交通大学计算机与信息技术学院硕士生, 主要研究方向为计算机视觉。