城市轨道交通 ACLC 系统信息安全研究

周品荣

(绍兴市轨道交通集团有限公司,浙江 绍兴 312000)

摘 要:主要研究了城市轨道交通领域中 ACLC 系统的信息安全。通过分析防护现状以及存在的安全隐患,结合信息安全相关政策,提出了一种基于安全管理中心的 ACLC 系统信息安全防护方案,并首次应用于轨道交通 ACLC 专业。该方案能够有效保护 ACLC 系统不受外部或内部的入侵和攻击,确保城市轨道交通的安全稳定运行。

关键词:信息安全;安全管理中心;清分及多线路中心

中图分类号:TP309.2 **文献标识码**:A **DOI**:10.19358/j.issn.2096-5133.2020.08.014

引用格式:周品荣. 城市轨道交通 ACLC 系统信息安全研究[J].信息技术与网络安全,2020,39(8):72-75.

Research on information security of urban rail transit ACLC system

Zhou Pinrong

(Shaoxing Rail Transit Group Co., Ltd., Shaoxing 312000, China)

Abstract: This paper mainly studies the information security of the ACLC system in the field of urban rail transit. By analyzing the protection status and existing security risks, and combining with information security related policies, an information security protection solution for the ACLC system based on security management center is proposed and applied to rail transit ACLC specialty firstly. The solution can protect the ACLC system from external or internal intrusions and attacks, and ensure the safe and stable operation of urban rail transit.

Key words: information security; security management center; ACLC

0 引言

城市轨道交通是城市公共交通系统的骨干,是城市综合交通体系的重要组成部分[1]。作为关键信息基础设施,其安全运行对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。城市轨道交通中信号系统、通信系统、综合监控系统、清分中心系统和自动售检票系统等弱电系统是支撑城市轨道交通安全、稳定运行的关键控制系统和信息系统,如果这些系统一旦突发安全事故,将严重影响区域内人们的生活和工作,造成严重的经济损失,甚至可能造成人员伤亡,因此如何保障这些系统的网络安全是当前亟需研究并解决的重大问题。

近年来,全国各地铁公司都在大力加强城市轨道交通信息安全特别是弱电系统信息安全的建设,但是地铁公司弱电系统信息安全在系统项目招标中,各系统业务项目独立招标,业务系统的网络安全建设纳入所在业务项目中,导致各业务系统选择各自独立的安全厂商、产品、防护方案,缺少总体防护和深度防护的思想。由于安全厂商的设备功能、设备、接口的差异,导致安全信息无法共享和集中管控,从而形成安全防护体系的漏洞。信息安全防护不仅需要技术保障,同时也需要管理及制度的保障,合理的安全管理机构设置,制定和执行完善的信息安全建设、运营等管理制度,是保障城市轨道交通关键信息基础设施信息安全的必需手段[2]。

清分及多线路中心(ACLC)作为负责城市轨道交通全线资金清算管理的重要系统,其重要性不言而喻,因此必须结合《网络安全法》等相关要求,以城市轨道交通相关政策为基础,进行 ACLC 系统网络安全的一体化顶层设计,通过建立集一体化设计、建设和管理为一体的 ACLC 系统网络安全等级保护解决方案,实现全天候协同持续监控、防御、检

测、响应、预测和分析等功能。基于安全管理中心的ACLC系统信息安全防护方案可以有效避免各线路自动售检票系统(Automatic Fare Collection System, AFC)信息安全等级保护建设不同期、安全防护分设无关联、防护范围受局限、厂商执行标准不统一、安全责任不明确等实施风险,较传统等保方案优势明显。

1 ACLC系统构成

ACLC系统主要由多线路清分中心和各线路AFC系统组成。系统包含五个层次的设备:清分及多线路中心(ACLC)、车站中心、终端设备、读卡器、票卡,如图1所示。

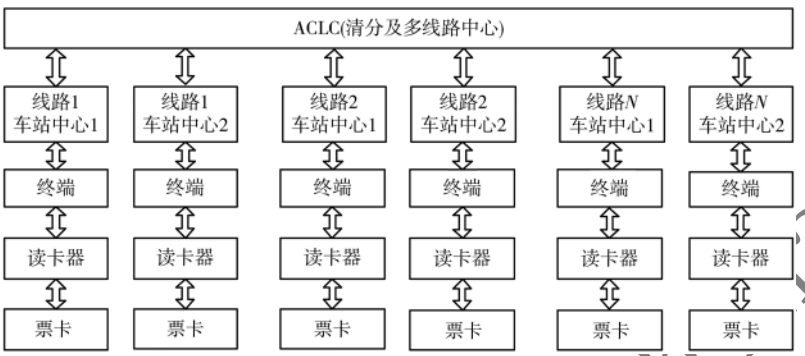

图1 ACLC系统设备层次结构图

清分及多线路中心(ACLC)是整个网络的资金清算管理中心,负责地铁系统内部各条线路及与其他商业实体之间的财务清算和运营管理,由数据处理服务器、前置通信服务器、历史数据服务器、文档管理服务器、网络管理服务器、运营管理服务器及附属设备共同构成,实现对各线路系统中所有设备进行监视,对全部数据进行收集和处理,对运营、票务、财务、维修进行集中管理。

车站中心由车站服务器及监控工作站、票务工作站和打印机及各种车站终端设备、紧急按钮构成,实现对本车站内部所有设备的实时监控,对车站AFC系统运营、票务、收益及维修的集中管理功能。

终端设备主要包括自动售票机、自动检票机、半自动售票机、自动查询机及手持设备等,是整个AFC系统中重要的组成部分。AFC系统中终端设备收集乘客在其上的每笔交易数据并上传给车站中心进行统计分析;终端设备接收车站中心下传的各类参数,根据参数进行不同的业务处理。

2 ACLC系统安全现状与隐患分析

近年来城市轨道交通建设保持高速增长,ACLC系统作为负责资金清算的核心系统,属于关键信息基础设施,但其信息安全整体防护薄弱,不能为安全运营提供有力保障。ACLC系统的终端设备也面临着高危漏洞和后门、工业网络病毒、高级持续性威胁以及无线技术应用带来的风险,使ACLC系统面临着日益严峻的威胁。

目前城市轨道交通ACLC系统的安全措施仅限于安装防火墙和部署杀毒软件等初级保护措施,无法避免信息被泄露、系统被攻击等事件的发生,即使发现了也无法对事件进行事故反演。同时,在轨道交通建设过程中,每条线路的系统都是被分别建设和管理的,缺乏顶层设计,形成了一个个信息安全孤岛。

3 ACLC系统信息安全防护方案

针对目前国内城市轨道交通ACLC领域尚无对网络设备进行统一管理的现状,本方案从全局出发,从顶层设计,提出了以计算环境安全为基础,以边界安全、通信网络安全为保障,以安全管理中心为核心的“一个中心,三重防护”信息安全整体防护方案,能够有效保障ACLC系统的网络安全、主机安全、应用安全和数据安全,实现整体安全态势的感知、溯源和应急处理,防止业务数据被非法访问和篡改[3]。本防护方案包括以下三个方面。

3.1 ACLC安全管理中心设计方案

在ACLC中心建设网络安全管理中心,实现对网络链路、安全设备、网络设备和主机设备的运行状况进行集中管控,实现对各线车站的主机设备、网络设备上的审计数据的收集汇总和集中分析,实现对业务系统网络发生的各类安全事件的识别、报警和分析。ACLC安全管理中心的设计方案包含如下3部分:

(1)安全管理中心设计方案

本方案在ACLC中心设计一个管辖各线车站系统的全线网络安全管理中心。各线路ACLC系统直接通过网络边界的工控防火墙连接到安全管理中心,利用安全管理中心实现ACLC系统中心与各站段安全防护设备和软件的集中管理。

(2)安全态势感知平台设计方案

在安全管理中心设计安全态势感知平台,实现对所有安全设备的安全事件的统一收集、关联分析,

达到安全态势感知，宏观展现系统的安全态势[4]。通过对业务系统的安全信息进行统一、持续的监测，对采集到的各系统数据进行深度分析和信息挖掘，发现面临的网络安全威胁态势，对正在发生的以及将来的威胁进行集中展示和告警，为安全风险威胁提供分析手段，为安全保障措施提供客观的决策依据[5]，保障线路中各业务系统网络安全、高效、有序运行。

(3)信息安全数据传输方案

在 ACLC 安全管理中心和各站段中心、车站、车辆段、停车场之间建设信息安全专网，建立一条安全的信息传输路径，实现对分散的各车站系统及安全设备的统一管理。安全设备的设备监测、安全日志等信息通过信息安全专网发送至 ACLC 安全管理中心，ACLC 安全管理中心通过信息安全专网向各线车站的安全设备下发安全策略。

3.2 ACLC 中心防护方案

ACLC 安全管理中心防护示意图如图 2 所示。ACLC 系统信息安全防护技术从网络安全、主机安全、应用安全、数据安全、漏洞扫描、数据库审计、运维审计等方面采取安全措施，实现 ACLC 系统业务应用的可用性、完整性和保密性保护，同时考虑各种技术的组合和功能的互补性，提升多重安全措施的综合防护能力，形成从外到内、从高层到底层的纵深安全防御体系，确保信息系统整体安全。中心防护方案包括如下 6 部分：

(1)边界隔离方案

在 ACLC 系统与其他外部系统的网络边界部署工控防火墙来隔离非法访问，拒绝非法入侵，实现边界完整性检查，实现隔离与访问控制，保证 ACLC 管理中心的自身安全。

(2)入侵检测方案

在 ACLC 管理中心核心交换机业务节点处旁路部署入侵检测系统，接收镜像的网络流量，并分析网络内是否存在异常流量、操作等行为，保证安全管理中心的自身安全，一旦发现攻击及时上报至安全管理中心。

(3)数据库审计方案

在中心 ACLC 系统中部署数据库审计系统，针对数据库操作行为进行细粒度审计的合规性管理，实现对数据库系统的数据访问审计、数据变更审计、权限操作审计以及数据库的安全审计。

(4)主机防护方案

在 ACLC 系统的工作站上安装主机安全防护软

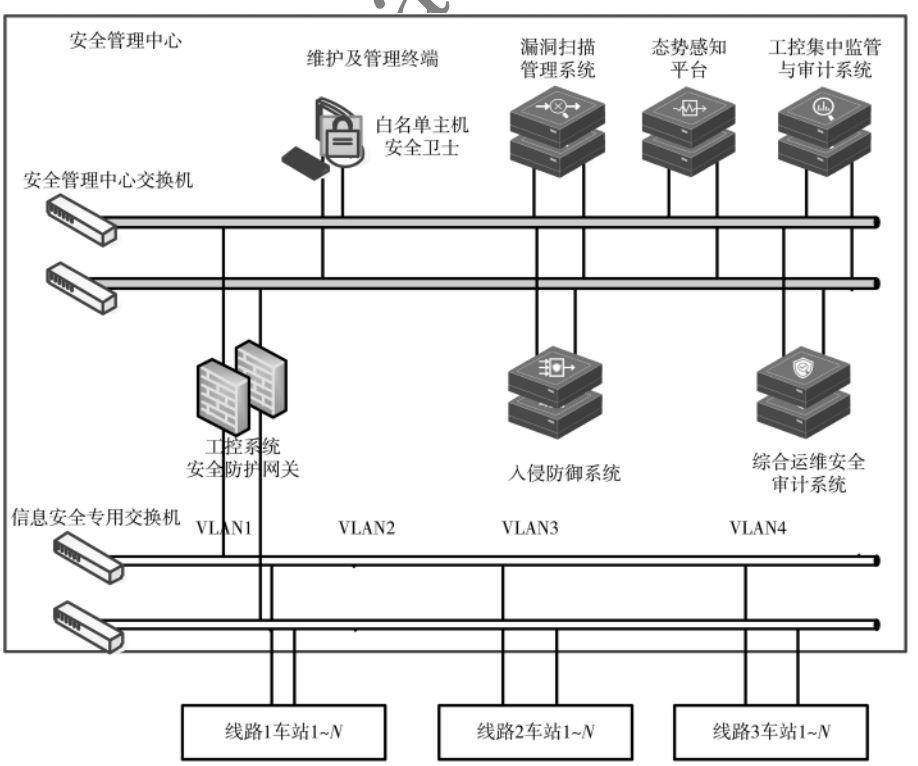

图 2 ACLC 安全管理中心防护示意图

件，加强恶意代码防范和对主机的入侵防范。主机安全防护软件由 ACLC 安全管理中心统一管理，进行权限推送，在受控情况下完成日常软件和配置变更操作，防止木马、病毒等未授权软件的运行。

(5)安全运维方案

在 ACLC 安全管理中心部署综合运维安全审计系统，实现对运维人员的统一认证管理、权限划分，实现对资源的统一授权，同时对授权人员的运维操作进行记录、分析、展现，实现集中审计和管理[6]。

(6)漏洞扫描方案

在安全管理中心部署漏洞扫描管理系统，定期对业务系统进行漏洞扫描，快速发现并识别网络资产属性，全面扫描安全漏洞，定性安全风险，提出修复建议，采取预防措施，实施修复方案。

3.3 ACLC 站段防护方案

ACLC 站段系统包括车站、车辆段和停车场，站段防护从网络安全、主机安全、应用安全、数据安全等方面采取安全措施，只部署边界隔离功能和入侵检测功能，其他功能复用安全管理中心功能。图 3 所示为站段安全防护示意图。站段防护方案包括以下两部分：

(1)边界隔离方案

在站段级 ACLC 系统与其他外部系统(PA、CCTV 等)的边界部署工控防火墙来实现隔离和边界完整性检查，实现边界入侵检测和防范，实现安全的访问控制。

(2)入侵检测方案

在站段 ACLC 交换机业务节点旁路部署入侵检测系统，接收镜像的网络流量，并分析网络内是否存在异常流量、操作等行为，一旦发现攻击及时上报至 ACLC 安全管理中心。

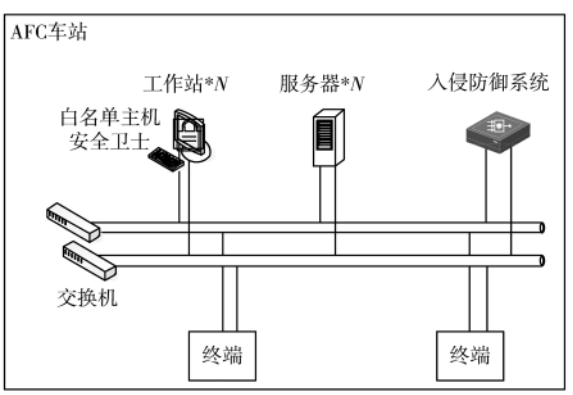

图 3 AFC 安全防护示意图

4 结束语

ACLC 系统作为城市轨道交通关键信息基础设施，其安全的重要性不言而喻。我国已经初步形成了以《中国人民共和国网络安全法》为法律基础、以《信息安全技术网络安全等级保护基本要求》为依据、以中国城市轨道交通协会行业政策发文为推力的城市轨道交通 ACLC 系统信息安全防护工作办法，为信息安全系统的实施提供了法律保障。

本方案通过顶层设计，建立起统一的 ACLC 系统信息安全保护体系，对各线、各站段系统进行集中管理，从边界防护、入侵防御、运维审计、漏洞扫描、白名单主动防御、集中监管等几个方面进行考虑，实施集中的安全审计与运维，实现信息的集中与融合，从技术层面提升防护能力。另一方面要强化 ACLC 系统的信息安全管理意识，从管理角度去杜绝各种潜在的安全隐患，完善各种规章制度，从人、设备、制度，建立起针对 ACLC 系统的安全管理体系，避免各种可能的攻击与破坏。只有这样，才能全面提升 ACLC 系统的安全防护水平。本文提出的方案对后续线路或其他项目的建设具很好的参考价值。

参考文献

[1] 王晔，陈丽娟，衣然.等保 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.

[2] 洪秀敏，周品荣.绍兴轨道交通网络安全防护的探究与实践[J].信息技术与网络安全，2019，38(12)：33-36.

[3] 孙云，江毅，李冰，等.轨道交通安保大数据平台建设与应用[J].警察技术，2020(4)：16-19.

[4] 王冬梅，钟辉.浅谈信息安全建设[J].珠江水运，2016(15)：94-95.

[5] 李彬，叶新晨.市域(郊)铁路车辆选型研究[J].城市交通，2020，18(1)：36-43.

[6] 马陈燕.高校电子类实验室安全管理探析[J].科技视界，2020(18)：222-223.

(收稿日期：2020-07-27)

作者简介：

周品荣(1986-)，男，本科，高级工程师，主要研究方向：轨道交通工程综合监控系统、通信系统、清分票务系统、信号系统等的网络安全防护。

版权声明