doi：10.3969/j.issn.1672-6073.2017.01.006

城市轨道交通ATC系统信息安全建设方案

贾晓哲
（北京通号国铁城市轨道技术有限公司，北京 100160）

摘　要：随着计算机和网络的发展，信息安全越来越受到关注，越来越多的城市在城市轨道交通信号工程招标文件中对列车自动控制（ATC）系统提出了需满足信息安全等级三级的要求。以目前城市轨道交通ATC系统中主流的CBTC系统为研究对象，按照信息安全标准分析物理安全、网络安全、主机安全、应用安全及数据安全等方面的要求。根据分析结果，对系统中较薄弱的网络安全、主机安全等环节通过增加安全审计、边界防护、入侵防护的方式进行改进。

关键词：城市轨道交通；基于通信的列车控制（CBTC）系统；信息安全；列车自动控制（ATC）系统
中图分类号：U231　　**文献标志码**：A　　**文章编号**：1672-6073(2017)01-0026-03

Information Security of Automatic Train Control System for Urban Rail Transit

JIA Xiaozhe
（Beijing Urban Transit Technology Co., Ltd., Beijing 100160）

Abstract: With the development of computer and Internet technology, information security has attracted more and more attention, so has the ATC (automatic train control) system of urban rail transit. More and more cities have specified in their invitation of tender that signaling system shall meet Level-3 requirements for information security. The paper analyzes the physical security, network security, host security, application security and data security according to the criteria for evaluation of information security, taking CBTC (communications-based train control) system, which is currently used in most urban rail transit projects, as the subject. The analysis results indicate that the vulnerable network security and host security could be improved by strengthening security audit, border protection and intrusion prevention. These findings may be used as references for the information security for ATC system.

Keywords: urban rail transit; communication-based train control (CBTC) system; information security; automatic train control (ATC) system

随着计算机及网络的发展，城市轨道交通列车自动控制系统（ATC）也普遍采用了基于计算机和通信技术的移动闭塞（CBTC）系统。CBTC系统具有传输信息量大，传输速度快，运营效率高等优点，但同时做好信息安全的防护，也变得越来越重要。近年来，国家提出了采用信息安全等级保护策略来解决我国的信息网络安全问题，并制定了《信息系统安全等级保护基本要求》《信息安全技术信息系统安全等级保护实施指南》《信息安全技术信息系统安全等级保护测评要求》[1-3]等一系列标准。作为城市轨道交通安全、高效运营的核心系统，其安全可靠的运行直接影响民众的出行安全和社会的稳定。因此，对CBTC系统信息安全的加强，防止其被侵入和破坏有着极为重要的意义。

收稿日期：2016-06-22　**修回日期**：2016-11-28

作者简介：贾晓哲，男，硕士，工程师，主要研究方向为城轨信号系统集成、开发测试、工程管理，mailxzjia@126.com

1　信息安全等级保护的要求

《信息安全技术信息系统安全等级保护定级指南》[4]将信息系统的安全保护等级根据其在国家安全、经济建设、社会生活中的重要程度，以及信息系统遭到破坏后对国家安全、社会秩序、公共利益及公民、法人和其他组织合法权益的危害程度等因素分为五级

（见表1）。

表1　信息安全等级划分

Tab. 1　Levels of information security

等级	对象	侵害客体	侵害程度	监管强度
第一级	一般系统	合法利益	损害	自主性保护
第二级	一般系统	合法权益	严重损害	指导性保护
		社会秩序和公共利益	损害	
第三级	重要系统	社会秩序和公共利益	严重损害	监督性保护
		国家安全	损害	
第四级	重要系统	社会秩序和公共利益	特别严重损害	强制性保护
		国家安全	严重损害	
第五级	极端重要系统	国家安全	特别严重损害	专控性保护

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

根据上述安全等级的划分，目前，北京、重庆、沈阳等城市轨道交通信号系统在工程招标文件中均明确提出了需至少满足三级的要求。等级保护三级的基本要求包括技术和管理两大部分，其中技术部分包括物理安全、网络安全、主机安全、应用安全、数据安全与备份恢复。

2　城轨ATC系统信息安全的现状

目前，城轨ATC系统主流采用CBTC系统[5]，系统结构见图1。系统在建设时已考虑了部分信息安全防护的要求，但还存在一些不足，具体分析详见表2。

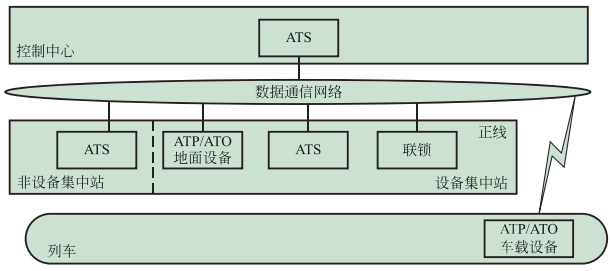

图1　CBTC系统结构

Fig. 1　Structures of a typical CBTC system

表2　CBTC系统信息安全现状

Tab. 2　Assessment of CBTC information security

信息安全要求内容		CBTC系统满足情况
物理安全	物理位置的选择	系统建设时配置了防雷、防火、电源及UPS等配套设备； 系统投入使用后制定完善的管理制度； 基本满足相关要求
	物理访问控制	
	防盗窃和防破坏	
	防雷击	
	防火	
	防水和防潮	
	防静电	
	温湿度控制	
	电力供应	
	电磁防护	
网络安全	结构安全	系统采用冗余的网络结构，并留有足够的余量； 系统具备基本的安全协议防护； 系统缺少安全审计、边界检查等功能
	访问控制	
	安全审计	
	边界完整性检查	
	入侵防范	
	恶意代码防范	
	网络设备防护	
主机安全	身份鉴别	系统具备身份鉴别、访问控制等基本功能； 系统缺少安全审计、入侵防范等功能
	访问控制	
	安全审计	
	剩余信息保护	
	入侵防范	
	恶意代码防范	
	资源控制	
应用安全	身份鉴别	系统各产品均通过安全完整性等级认证； 系统各产品留有足够的余量； 系统缺少安全审计等功能
	访问控制	
	安全审计	
	剩余信息保护	
	通信完整性	
	通信保密性	
数据安全与备份恢复	数据完整性	系统具备数据完整性和保密性； 系统具备备份与恢复功能； 基本满足相关要求
	数据保密性	
	备份与恢复	

3　信息安全建设方案

针对系统中尚不满足的地方，建设方案见图2。

3.1　安全审计建设

在控制中心建立安全审计中心，实现网络环境计算机信息系统安全审计与评估的集中管理，实时收集

各安全代理程序的审计信息，并进行记录分析与保存，满足网络行为审计和数据库访问审计要求。

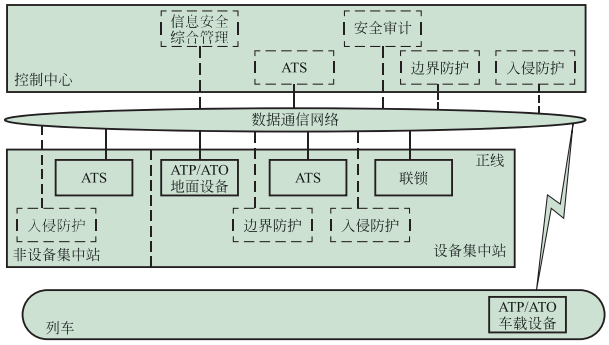

图2 信息安全改进方案

Fig. 2 Structures of information security for CBTC

设置跨平台的安全审计机制，对安全事件快速进行评估并作出响应，向管理人员提供各种系统使用情况、出现的可疑迹象、运行中发生的问题等有价值的统计和分析信息，运用统计方法学和审计评估机制给出智能化审计报告及趋向报告，达到综合评估系统安全现状的目的。

3.2 边界防护建设

在控制中心、正线各集中站、车辆段建立边界防护安全域，部署安全防护网关系统，通过安全防护网关将各设备集中站进行隔离。安全域是根据等级保护要求、信息性质、使用主体、安全目标和策略等方面的不同来划分的，是具有相近安全属性需求的网络实体的集合。同一级安全域之间的安全需求包括隔离需求和连接需求两方面。隔离需求对应着网络边界的身份认证、访问控制、不可抵赖、审计等安全服务；连接需求对应着传输过程中保密性、完整性、可用性等安全服务。

3.3 入侵防护建设

在控制中心、正线各集中站、非集中站，车辆段建立入侵防御系统，入侵防御系统对数据进行检测，通过模式匹配和异常检测、统计分析以及抗 IDS/IPS 逃逸等多种检测技术，防止蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等多种攻击造成的侵害，通过向运维人员做出告警，及时做出应急响应。

3.4 信息安全综合管理

在控制中心部署信息安全综合管理系统，对安全审计、边界防护、入侵防护等系统进行综合管理。

安全综合管理系统能够对网络进行统一的管理，对各种设备进行自动远程实时监控和分析，寻找出故障点和原因，以便及时采取相应措施，并且能够对网络设备流量进行分析。同时，可以将流量、配置、故障报警、异常报警、设备利用率等分析的数据信息，以直观的图形、图表形式输出到显示设备上，方便值班人员查看网络系统运行状况。

4 结语

本文介绍了信息安全的基本要求，并通过分析既有城市轨道交通 CBTC 系统信息安全方面的不足，提出一种信息安全建设方案。方案通过在安全审计、边界防护以及入侵防护等方面进行建设，加强了系统网络、主机以及应用等方面的信息安全性，但由于 CBTC 系统信息安全建设尚无应用案例，因此后续将针对此方案在信息安全保护中能否达到相应的效果，以及对既有 CBTC 系统是否存在影响等方面进行深入的研究。

参考文献

[1] 信息系统安全等级保护基本要求：GB/T 22239—2008[S]. 北京：中国标准出版社，2008.
Baseline for classified protection of information system: GB/T 22239—2008[S]. Beijing: Standards Press of China, 2008.

[2] 信息安全技术信息系统安全等级保护实施指南：GB/T 25058—2010[S]. 北京：中国标准出版社，2010.
Implementation guide for classified protection of information system: GB/T 25058—2010[S]. Beijing: Standards Press of China, 2010.

[3] 信息安全技术信息系统安全等级保护测评要求：GB/T 28448—2012[S]. 北京：中国标准出版社，2012.
Testing and evaluation requirement for classified protection of information system: GB/T 28448—2012[S]. Beijing: Standards Press of China, 2012.

[4] 信息安全技术信息系统安全等级保护定级指南：GB/T 22240—2008[S]. 北京：中国标准出版社，2008.
Classification guide for classified protection of information system: GB/T 22240—2008[S]. Beijing: Standards Press of China, 2008.

[5] IEEE Standard for communication based train control (CBTC) performance and function requirements[S]. The United States of America: the Institute of Electrical and Electronics Engineers, Inc., 1999.

（编辑：郝京红）