国产密码在城市轨道交通综合监控系统中的应用

赵　晗[1]　王燕娜[2]　李建峰[2]

（1. 郑州地铁集团有限公司，450052，郑州；2. 河南辉煌城轨科技有限公司，450052，郑州//第一作者，高级工程师）

摘　要　通过深入分析城市轨道交通综合监控系统中可能存在的 4 类安全风险，采用相应的国产密码应用方案来解决安全风险，保证城市轨道交通关键基础设施的安全自主可控，推动国产密码产业生态健康发展。国产密码应用于郑州市市民文化服务区地下交通工程综合监控系统，范围包括 1 个中心、6 个车站和 1 个车辆段。自 2019 年 10 月开通运营以来，系统始终保持安全稳定运行。

关键词　城市轨道交通；综合监控系统；安全风险；国产密码应用

中图分类号　U29-39

DOI：10.16037/j.1007－869x.2021.05.036

Application of Domestic Cryptographic Password in ISCS of Urban Rail Transit

ZHAO Han，WANG Yanna，LI Jianfeng

Abstract　Through in-depth analysis of the four types of security risks that may exist in the integrated supervision and control system（ISCS）of urban rail transit，the corresponding domestic cryptographic password application scheme is adopted to dissolve the security risks，ensuring the safety，independency and control of key infrastructure of urban rail transit，and promoting the ecological and healthy development of domestic cryptography industry. The domestic cryptographic password is applied in the integrated monitoring system of the underground traffic engineering in Zhengzhou citizen cultural service area，covering 1 center，6 stations and 1 depot. Since the launch in October 2019，the system has been operating safely and stably.

Key words　urban rail transit；integrated supervision and control system（ISCS）；security risk；domestic cryptographic password application

First-author's address　Zhengzhou Metro Group Co.，Ltd.，450052，Zhengzhou，China

城市轨道交通具有运量大、速度快、安全舒适、班次密、准点率高、节能环保等优点，是广大市民出行首选的绿色交通。ISCS（综合监控系统）是城市轨道交通安全运营、可靠运营的保障，一旦发生系统安全风险，会直接影响乘客的生命安全，对社会、经济的影响也非常大。

2017 年 4 月，中央密码工作领导小组办公室印发了《关于做好金融和重要领域国产密码试点工作的通知》。2017 年 11 月，中共河南省委密码工作领导小组印发了《河南省金融和重要领域国产密码应用试点工作方案》。郑州地铁集团有限公司作为全国唯一的城市轨道交通国产密码应用试点单位承担试点任务，选取城市轨道交通 4 大核心系统先期进行国产密码应用试点研究。

ISCS 是城市轨道交通四大核心系统之一。本文主要就 ISCS 内部可能存在的安全风险进行分析，详细介绍相应的国产密码应用解决方案，以及在郑州市市民文化服务区地下工程中的实际应用。

1　ISCS 安全风险分析

1.1　系统结构

ISCS 是用系统化方法将分散独立的各类自动化系统联结为一个有机整体，从而形成一个新的综合型自动化监控系统。该系统解决了城市轨道交通中各专业系统之间的信息互通、资源共享等问题，提高各系统的协调配合能力，实现系统间的高效联动机制。在技术层面上，该系统提供了高效的技术手段，增强了运营管理人员对各种突发事件的应变能力，提高了反应速度，增强了灾害事故的抵御能力，从而提高了城市轨道交通运营服务质量和服务水平。

ISCS 采用两级管理、三级控制的结构体系。两级管理分别为中央级、车站级，三级控制分别为中央级、车站级和现场级。

中央级综合监控系统对全线重要监控对象的状态、性能数据进行实时收集和处理，通过各种调度员工作站和大屏幕，以图形、图像、表格和文本的形式显示出来，供调度人员控制和监视。同时，根据一定的逻辑关系自动向分布在各站点的被监控

对象或系统发送模式、程控、点控等控制命令，或由调度员人工发布控制命令，从而完成对全线环境、设备和客流信息的集中监控。

车站级综合监控系统对本站监控对象的状态、性能数据进行实时收集和处理，通过操作员工作站以图形、图像、表格和文本的形式显示出来，供车站值班人员控制和监视。当中央级和主干网络发生故障时，车站级仍可在车站范围内继续进行控制。

现场级是由 BAS（环境监控系统）、FAS（防灾报警系统）、PSCADA（电力监控与数据采集）、PSD（站台屏蔽门）、ACS（门禁系统）、ATS（列车自动监控系统）、AFC（自动售检票系统）、CCTV（闭路电视）、PA（公共广播）、PIS（乘客信息系统）、CLK（时钟）等系统的现场层设备组成。ISCS 与 BAS、FAS、PSCADA、PSD、ACS、ATS、AFC、CCTV、PA、PIS、CLK 等系统在车站级或中央级进行接口。一般采用工业控制网络或现场总线，进行分散控制结构。

1.2 系统现状及潜在安全风险

综合监控系统是一个相对封闭的局域网系统，具有分布范围广、设备数量大、系统使用人员多、软件功能复杂等特点。目前综合监控系统的身份认证采用用户名和密码登录方式实现，并未对传输的信息数据进行加密。

因此，系统主要存在以下 4 类潜在安全风险：

1）非法用户登录风险。在目前的综合监控系统中，每个操作人员都有一个对应的用户名和密码。一个非法用户在获取他人的登录名和密码的情况下，可以正常地登录系统平台，一旦其在人机界面下发出控制命令，系统因无法识别出该类非授权的操作而正常执行，就会造成不可预知的后果。

如何确认登录用户身份的合法性以保证非法用户无法正常登录，就需要采取更可靠的手段来加以保证。

2）非法设备接入风险。综合监控系统为分布式大型集成系统，系统用到的服务器、FEP（前置机）、工作站等分散在中心和车站的各个房间，中心和各车站一般采用双环网的方式组建骨干网，目前只要接入到系统环网交换机就能够访问系统资源。若一个未经授权的设备接入了综合监控系统网络，通过篡改或伪造控制命令，对电力、环控、门禁、售检票、屏蔽门等系统设备进行控制，将会造成非常严重的后果。

如何保证接入网络的计算机设备都为合法的授权设备，非授权设备无法通过网络环境进入系统，这就是系统设备的认证加密需求。

3）伪造控制命令下发风险。在综合监控系统内部存在多种通信链路，包括系统数据、设备实时状态、历史归档信息、事项记录、控制命令及结果反馈等，这些信息具有不同的数据流向，使用 TCP（传输控制协议）或 UDP（用户数据包协议）不同方式进行传输。在数据传输中，控制数据流尤为重要，其他数据流在操作员界面大多是进行数据的显示处理，而控制数据流赋予了操作员工作站对系统监控设备的控制功能，一旦篡改或伪造的控制命令下发，无疑会对系统的正常运行造成损害。上述数据流通过数据扫描工具非常容易监测到网络上的数据报文，进而窃取数据，同时也很容易伪造 TCP 或 UDP 数据包，进而对网络上的设备发起攻击。

如何保证通信网络上的重要数据内容不被窃取，如何防止非法设备伪造发送控制指令，维护系统正常的控制管理规则，是网络通信安全必须要解决的问题。

4）数据泄露或被篡改风险。从数据存储形式来看，综合监控系统数据主要有系统配置文件、数据库文件、图形文件 3 种。系统配置文件里包括系统正常运行所必需的配置参数；数据库文件主要包括用户信息、系统参数、各监控设备的信息以及事件信息等；图形文件主要包括页面、设备图元等。目前，这些数据均是采用明文的方式进行存储。

系统配置参数通常以操作系统文件的形式在本地保存，一旦配置文件泄露，将造成综合监控系统平台无法正常启动，或者可能会构造一个虚假系统平台对原有系统控制设备发送伪造控制命令。

数据库文件中，用户信息的安全是系统正常登录的保障，因此要避免用户信息被篡改或盗用。另外，一些重要且敏感的历史数据也需要安全防护，避免被意外泄露，确保无权限操作人员无法查看系统的敏感数据，有权限操作人员查看的数据为真实可靠的。

如何保证数据库关键字段以及重要的系统配置文件不被窃取，是数据存储应重点考虑的问题之一。

2 综合监控系统国产密码应用方案

针对上面 4 类安全风险，本文进行了深入分析，形成了综合监控系统的国密应用方案。该方案主

要由系统认证、通信加密和存储加密 3 个部分组成。

国产密码应用于综合监控系统后的系统结构如图 1 所示。

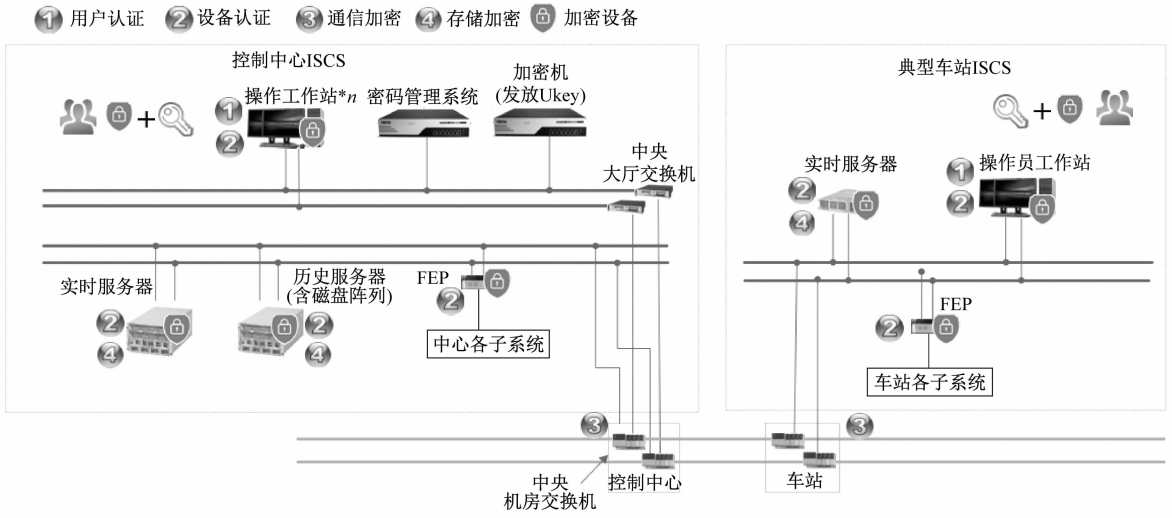

图 1　综合监控系统结构示意图

2.1　系统认证

系统认证包括对综合监控系统的服务器、工作站、FEP 等设备的身份认证，以及对综合监控系统的操作人员的用户身份认证，这是整个系统安全性的基础。

对设备和用户的身份认证，使用 UKey（智能密码钥匙）设备，采用 SM2 椭圆曲线公钥密码算法和 SM9 标识密码算法来实现数字签名和认证功能，保证只有授权合法用户有权访问系统。UKey 具有完善的身份鉴别功能，能区分两个不同的个体。将一个 UKey 与人或设备绑定，只有持有该 UKey 的人才具有相对应的权限，别人无法冒名登录，也无法有权限执行。另外，利用 UKey 的追溯和防抵赖机制，能够确认网络上执行的操作就是本人操作。用户认证过程如图 2 所示。

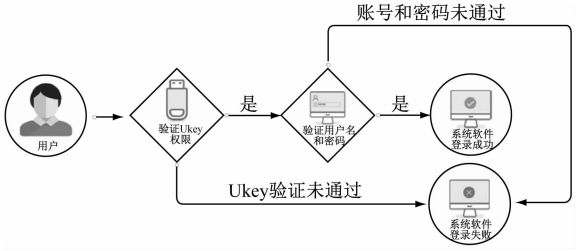

图 2　用户认证过程

设备认证过程如图 3 所示。

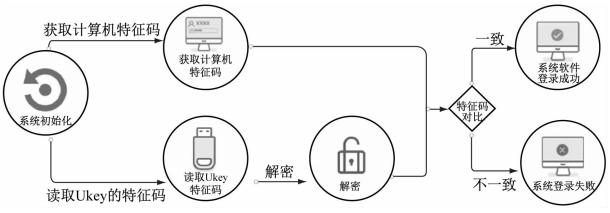

图 3　设备认证过程

综合监控系统软件平台记录认证结果，认证未通过时，平台软件模块不能正常启动，该登录失败操作将被记录。通过系统的登录日志可以查看非法用户登录记录，也可以查看非法设备接入记录，为系统问题的调查提供依据。

2.2　通信加密

系统内部通信时，关键数据采用密文形式传输，以保证网络通信的安全。数据传输过程如图 4 所示。

图 4　数据传输过程

用户通道建立加密通信前,先进行用户密钥的认证,通过认证后即可通过各种加密密钥和存储密钥进行数据的交换,密钥都是动态产生,防止了密钥的泄露。

首先,由数据的发送方采用接收方的标识密钥对传输数据进行加密;然后,发送给接收方,接收方收到数据后,用自身的标识向密钥管理中心申请认证标识的私钥,密钥管理中心认证成功后将私钥发送给接收方,数据的接收方即可使用该私钥进行数据解密。

2.3 存储加密

由于综合监控系统涉及的数据库数据和文件数据非常多,因此考虑到系统的性能,只对系统的关键核心数据(如用户名和密码、车站、关键配置等)进行加密存储,其他数据仍采用明文方式存储。数据存储加密通过调用符合国密要求的 SDK 软件开发包来实现。

数据的存储加密采用软件 SDK 加密包的方式,使用 SM3 密码杂凑算法和 SM4 分组加密算法来实现数据库字段和配置文件存取的加解密功能。在数据存储前,调用加密算法进行数据加密,然后进行数据库存储或文件存储。在使用数据库数据或配置文件前,先调用解密算法,对读取的密文数据解密后再使用。在加解密过程,所需的加密和解密密钥在设备 UKey 中保存。

通过数据的加密存储,使数据的意外泄露造成的损失降到最低,为系统的稳定运行提供一个良好、安全、可靠的数据环境。

3 国产密码在郑州市市民文化服务区工程综合监控系统中的应用

3.1 现场设备配置

郑州市市民文化服务区工程综合监控系统一期工程范围包括 1 个中心、6 个车站和 1 个车辆段。

硬件:在中心部署 1 台加密机,1 套密管系统;在中心、车站、车辆段的各个服务器、FEP、工作站上配置 1 个设备 UKey;对每个操作人员配置 1 个用户 UKey。

操作系统:服务器为 Solaris;FEP、工作站为 Redhat。

软件平台:在中心、车站、车辆段的各个服务器、FEP、工作站上部署辉煌城轨自动化监控平台(MAS)V2.0。

3.2 国密功能

郑州市市民文化服务区工程现场国密功能测试结果如表 1 所示。

表 1 现场国密功能测试结果

序号	测试项	预期结果	测试结果
1	用户身份认证	登录系统时,只有用户名密码正确且使用合法授权的 Ukey,才能进入系统	通过
2	设备身份认证	具有合法授权 Ukey 的设备,其上的软件才能接入系统	通过
3	系统内数据通信加密	综合监控系统内部的重要数据是以密文的形式进行传输	通过
4	数据存储加密	数据库中的关键字段和重要的系统配置文件以密文的形式进行存储	通过

3.3 国产密码应用于综合监控系统后的系统性能

郑州市市民文化服务区工程现场性能测试结果如表 2 所示。

表 2 系统性能测试结果

测试对象	设备状态传输时间/s	控制命令下发时间/s	冗余服务器切换时间/s	冗余 FEP 切换时间/s	服务器负载率/%	FEP 负载率/%	工作站负载率/%
实验室无加密	0.828	1.298	0.278	0.387	12.2	16.50	5
实验室国密应用	0.892	1.321	0.309	0.414	13.6	18.20	7
现场国密应用	0.914	1.598	0.352	0.421	15.0	19.67	10
国标要求	<2	<2	<2	<1	<30	20	30

根据测试结果,综合监控系统增加国密功能后性能指标仍然符合 GB/T 50636—2018《城市轨道交通综合监控系统工程技术标准》。

(下转第 178 页)

根据以上 3 个车站的实测数据,得出以下结论:① 传统方案的绝缘电阻对湿度十分敏感,绝缘电阻随湿度增加而大幅下降,这是因为表面电阻大幅降低的结果,当湿度大于 90% 时,其绝缘电阻趋于零;② 新方案绝缘电阻值比传统方案绝缘电阻值大大提高;③ 新方案绝缘电阻值也随湿度增大而降低,但是下降幅度较小,即便湿度大于 90%,站台门绝缘电阻值仍然较高。

6 结语

本文从目前地铁站台门绝缘普遍失效及绝缘可靠性差的现实背景入手,通过理论分析得出空气湿度与物体表面电阻是负相关的,而表面电阻与站台门绝缘电阻是正相关的。因此,要提高站台门绝缘性能必须提高物体的表面电阻。进而提出一个颠覆传统站台门绝缘结构的方案,即在站台土建结构上设置绝缘,由嵌入结构板中的绝缘体阻断体电流,结构板表面设置绝缘涂层,阻断表面电流,从而全面增大站台门绝缘电阻。该方案将使站台门绝缘性能得以普遍提高,通过实施案例,其绝缘电阻的检测数据证明了该方案理论的正确性,具有工程化应用前景。

参考文献

[1] 《电子电气绝缘技术手册》编辑委员会. 电子电气绝缘技术手册[M]. 北京:机械工业出版社,2008.

[2] 中华人民共和国住房和城乡建设部,中华人民共和国国家质量监督检验检疫总局. 地铁设计规范:GB 50157—2013[S]. 北京:中国建筑工业出版社,2013.

[3] 叶宏,凌人. 屏蔽门门体绝缘及站台绝缘的探讨[J]. 现代城市轨道交通,2012(6):27.

[4] 孙增田,李华,程强. 屏蔽门接轨保护及绝缘保护必要性分析[J]. 城市轨道交通研究,2006(8):44.

[5] 陈韶章. 地下铁道站台屏蔽门系统[M]. 北京:科学出版社,2005:137.

(收稿日期:2020 - 06 - 29)

(上接第 174 页)

4 结语

在郑州市市民文化服务区地下交通工程综合监控系统的 1 个中心、6 个车站、1 个车辆段的现场环境下,进行了综合监控系统国密应用方案的测试和长期试点应用,实现了用户和设备的身份认证、访问控制、信息安全传递,提升了综合监控系统的安全性。该国密方案中使用的国产密码算法、技术和设备均为国内自主设计、自主研发,符合国家对信息安全的"自主、安全、可控"要求。该系统的研发为城市轨道交通信息化安全建设提供了新的思路,可更好地为公众提供安全、便捷的出行。

参考文献

[1] 中华人民共和国住房和城乡建设部,中华人民共和国国家质量监督检验检疫总局. 城市轨道交通综合监控系统工程技术标准:GB/T 50636—2018[S]. 北京:中国建筑工业出版社,2018.

[2] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. 信息安全技术 SM2 椭圆曲线公钥密码算法:GB/T 32918.5—2017[S]. 北京:中国标准出版社,2017.

[3] 国家密码管理局. SM3 密码杂凑算法:GM/T 0004—2012[S]. 北京:中国标准出版社,2012.

[4] 国家密码管理局. SM4 分组密码算法:GM/T 0002—2012[S]. 北京:中国标准出版社,2012.

[5] 国家密码管理局. SM9 标识密码算法:GM/T 0044—2016[S]. 北京:中国标准出版社,2016.

[6] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. 基于 IBC 技术的身份鉴别规范:GM/T 0057—2018[S]. 北京:中国标准出版社,2018.

[7] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. 信息系统密码应用基本要求:GM/T 0054—2018[S]. 北京:中国标准出版社,2018.

(收稿日期:2020 - 06 - 24)