doi:10.3969/j.issn.1672-6073.2013.02.019

# 地铁AFC系统安全性探究

杨 珂
（西安地下铁道有限公司运营分公司 西安 710000）

**摘 要** 针对AFC系统的不同安全威胁对象，描述AFC系统可能遇到的设备、网络、系统、数据威胁，并针对这些威胁，结合西安地铁2号线的实践提出一些应对办法，为后续新线AFC系统的安全性建设提供参考。

**关键词** 城市轨道交通；AFC系统；系统设备；地铁运营；安全
**中图分类号** U231.92 **文献标志码** A
**文章编号** 1672-6073(2013)02-0074-03

地铁AFC系统与地铁运营的票务收益息息相关，同时也是面向广大乘客的窗口，在整个地铁的运营中起着至关重要的作用。因此，地铁AFC系统的安全性值得新开线路的关注，在健全的安全机制下保证AFC系统可靠、无故障运行，对地铁的平安运营有着极其重要的意义。笔者结合西安地铁的实际情况，对AFC系统所涉及的安全问题分类，并对安全管理机制的建立以及系统所面临的安全问题进行讨论。

## 1 AFC系统安全性概述

地铁中的现金流和乘客交互窗口的角色要求AFC系统必须是安全的，然而，AFC系统却面临着来自内部和外部的两大类威胁。外部威胁主要是来自系统以外的网络，入侵者可能通过网络远程进入系统，对系统进行多种方式的入侵，如拒绝服务攻击、针对各种服务的攻击（DNS、FTP、SMTP、HTTP等）、各种后门攻击、针对Windows和Unix的网络攻击等等。内部威胁主要来自地铁系统内部使用者以及乘客对系统造成的威胁，乘客可能对AFC系统设备造成物理上的威胁，而地铁内部人员在系统的维护过程中，任何操作都有可能对票务数据、系统内部管理数据及系统稳定性带来极大的威胁。在系统使用过程中，由于对现金的管理和操作，也会带来收益上的安全威胁。因此，对于AFC系统来说，其所涉及的安全问题，不仅仅体现在通常认识的网络安全、系统安全性、人员安全性上，还应体现在票卡安全、设备安全、软件安全、数据安全、收益安全等多方面。按照AFC系统安全涉及的对象，可将AFC系统的安全性划分为设备安全性、网络安全性、软件安全性、数据安全性和管理策略安全性5大类。

**收稿日期**：2012-08-27

**作者简介**：杨珂，女，硕士，AFC专业主管，工程师，从事自动售检票设备技术研究、系统设备维修维护管理及地铁票务收益管理工作，ymmk163@163.com

## 2 AFC系统安全对策

针对AFC系统涉及的设备、网络、系统软件、系统数据以及管理策略等几大类安全问题，结合西安地铁的实际情况，分别对每类安全问题做出分析并提出一些意见，以便为后续线路的建设和运营提供依据。

### 2.1 加强设备安全性设计

AFC系统具有数目众多的站级终端设备，因此设备的安全性不容忽视，设备安全性主要表现在两个方面。

1）作为与乘客交互最多的设备，首先需要保障维修维护人员以及乘客的人身安全，为了达到这一点，需要在AFC系统终端设备设计制造时遵循一定的原则：如所有设备应具备相应的安全保护，设备防水性能良好，设备内各模块应固定防止随意移动，所有接头应具有固定措施；所有设备应有良好的接地措施保证设备金属外壳不带电，所有设备及通信线路应具备相应的电源保护措施，所有设备都应配有UPS电源，以防止突然断电带来的系统威胁；闸机通道具有人员通过安全保护机制，扇门需要刚柔适中能够承受乘客的猛烈撞击对设备带来的损害，同时也能让乘客在强制闯过扇门时不受到伤害。另外，设备内部结构设计需要合理，便于人员维修操作，不应有尖利部位导致人员的划伤。

2）作为与现金收益有直接关系的系统设备应该重视收益安全的设计，钱箱和票箱都应加锁，且所有钱箱在设备中具有密封性，操作人员不能直接接触到TVM内

找零用的现金、钱箱内的现金和车票，在设备发售车票或者车票回收的过程中，即使是设备的某些部件发生故障，车票只能按设定的路径进入取票口或者回收箱中，不应散落在设备的其他部位。设备中经常需要更换的票箱与钱箱，由于经常搬运和卸载，因此需要有较宽的接触面不易倾斜，西安地铁 2 号线就是由于票箱立面较窄，易倾斜磕碰而造成票箱的损坏。涉及钱款的部件在拆卸和更换过程中必须经系统授权和身份认证，系统中钱箱的更换都应有日志记录，可明确显示卸载人以及卸载时间，卸载时钱箱中钱款的情况，比如西安地铁现在使用的 TVM 和检票机钱箱、票箱都配置唯一的电子标志，TVM 和检票机还配备了电子储存模块，对钱箱使用情况进行记录，进入该钱箱的可累计现金金额、最后一次装入设备和从设备取出的时间、最后一次取出时的该钱箱内的现金金额以及最后一次取出时的操作人员号码等内容。

## 2.2 实现网络安全性

目前，世界上有 65% 以上的网站瘫痪是源于病毒、黑客的入侵与攻击。防火墙和入侵检测系统是防御这类攻击的有效办法，西安地铁 2 号线 AFC 系统处于独立的专网中（网络结构见图 1），仅在小清分系统与西安市一卡通系统留有外部接口，并在此处安装防火墙，隔离 AFC 网络系统和外部网络，此处的防火墙配置了 DOS/DDOS 功能，可实现对各种拒绝服务攻击的有效防范，还配置了 ARP 欺骗攻击防范，以及超大 ICMP 报文攻击防范，设置了防火墙的告警策略，启动了防火墙日志功能。

除此之外，采用基于状态的特征检测技术，基于协议异常分析的检测技术和基于流量异常分析的检测，对付来自外网和内网的攻击，缩短发现黑客入侵的时间。入侵检测技术与防火墙共同协作，对 AFC 系统网络入口进行多层次安全保护，形成整体纵深的安全防护体系。

虽然 AFC 系统处于专网环境中，但由于系统升级等需求不可避免地会与外界存储设备存在交互，因此对于内网的管理，除了应用网络防病毒体系外，还可以采用漏洞扫描和日志告警功能，使得系统在遭受攻击之前，可以了解和修复自身网络安全问题，提早发现漏洞，阻断病毒传播。另外，系统还应该具备外部存储设备的认证功能，即只有被认证过的设备才可以在系统中使用，防止外界存储设备给系统感染病毒。

## 2.3 关注软件和数据安全性

在整个 AFC 系统中，乘客应用 AFC 系统在不同层次将产生各种类型的数据，这些海量的数据存在丢失、损坏、被篡改的风险，因此各层次下设备需要根据其自身的需求对相应的数据进行保护，主要工作如图 2 所示。

对这些安全需求系统应该采取以下措施：

1）需要有安全产品的应用，即涉及数据的设备都需要有防病毒软件，以保护系统数据不被外界损坏，硬件采用专用的 Unix 操作系统，采用 Oracle 数据库产品系列。

2）需要安全密钥系统的应用，通过 ISAM 和 PSAM 卡保证所有设备的合法性，通过 TAC 码来确保终端交易数据的合法性。西安地铁 2 号线采用了 3DES 对称密钥算法，确保数据的加密与外界的隔离，有效地达到了认证的安全性。

3）为了防止数据在阐述过程中被篡改，系统需要应用 CRC 码进行校验。

4）系统需要提供细致的权限管理，在运营过程中由于维护人员众多，角色不一，因此对系统的误操作很容易破坏系统的数据，因此，系统需要提供细致的权限管理功能，维护人员为不同角色的人员提供相应权限，防止误操作和数据的恶意破坏。

5）为了保证系统数据的安全性，系统提供数据冗余功能和数据跟踪功能。西安地铁 2 号线 SLE 设

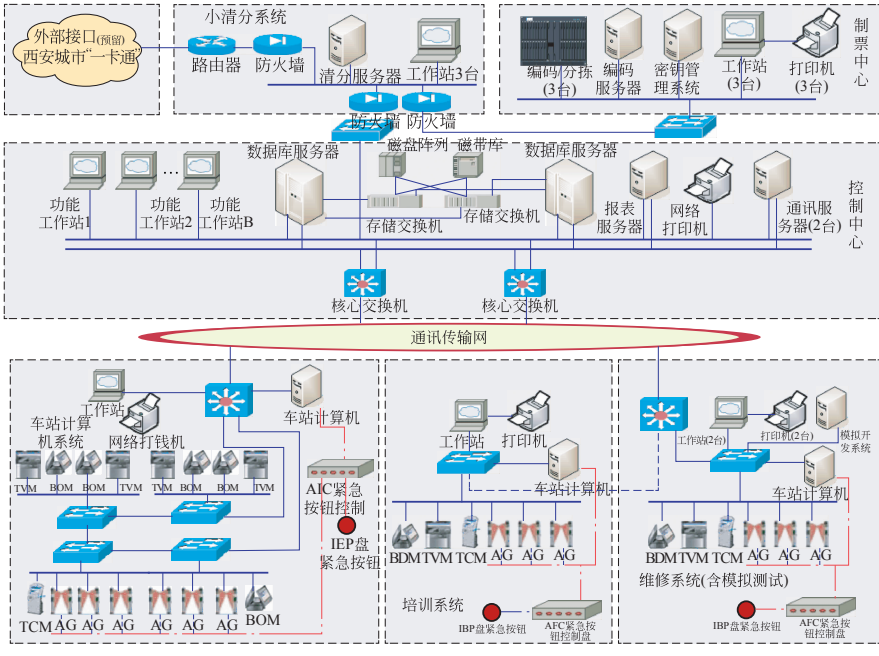


图 1　线路 AFC 网络构成

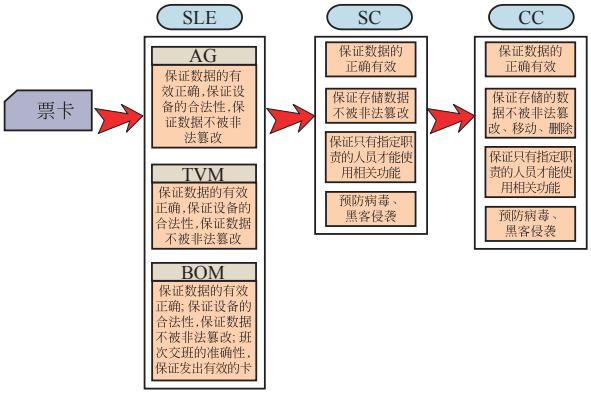


图2 线路AFC各层次数据需求

备中的数据在打包向上层设备传输前，将数据保存在设备的两个不同物理空间上，SC、CC将数据再向上层传输前，保存4份数据，系统数据根据不同设备分别保存数据的期限为15天或者30天不等，并且提供专门的票卡跟踪模块。

6）系统需要提供数据审计功能，系统各个层级不但要对数据的连续性进行审计跟踪，还要将累计数据进行检查，防止数据的重复或者丢失。

### 2.4 完善策略安全性制度

不管整个AFC系统设计得多么完善，由于AFC系统与乘客以及内部管理人员有着密切的交互，因此保证系统的安全性还需要严格的安全策略来配合。AFC系统的安全策略除了体现在通常所知的对人、票、现金及设备严格的管理制度上，还体现在具有完善的应急管理制度，即具备较为完善的应急预案。

对于人的管理首先需要确定人员与系统交互时的安全等级，根据安全等级，确定安全管理的范围；对于系统的核心部位中心机房，制定严格的出入管理制度，做好出入登记，实行分区控制，限制工作人员出入与己无关的区域，并严格限定人员使用系统的权限，对工作调动和离职人员及时调整相应的授权；对于票务管理应该在票务政策中明确各种票卡的使用场景，控制特种票卡的发行数量，做好日常的票卡使用情况分析。西安地铁2号线对员工票卡的使用建立了一套跟踪分析系统，监控票卡使用次数和票卡使用地点，如员工的工作地点主要在某一车站，而票卡分析的结果却是全线频繁使用，那么这类票卡将被调查分析；对于现金的管理，尽量在人员可能触碰到现金的地方增加摄像头做好物理保护，然后明确人员职责，坚持多人负责的原则，制定现金清点、结算、售票等相关规章；对于设备的管理则要制定完备的系统维护制度，维护时必须先经主管和协作部门批准，特别是软件系统的维护一定需要在测试环境中验证通过，并在运营结束后进行升级，且升级过程中使用到的外置存储设备必须获得系统的认证。涉及钱票时需要有监督人员在场，对故障原因、维护内容和维护前后的情况均详细记录，已备查阅，制定设备维护台账时应增加需要填写具体数值的内容，而不仅仅是对所维护内容进行简单的确认，这样的台账才能较为真实地反映实际维修维护情况。

## 3 结语

AFC系统的安全性问题包括的不仅仅是通常所认知的网络安全、数据安全等问题，还包含了设备、管理等安全问题，涵盖的内容非常广泛。总之，为了保证AFC系统正确无误地平稳运行，不但需要从设计角度出发，关注硬件、软件、网络的设计问题，也要根据系统架构制定相应的安全管理制度予以配合，才能保证AFC系统良好地运行，真正成为地铁公司的现金流，成为地铁的一个亮丽的窗口。

### 参考文献

[1] 李立纲，洪澜. 广州地铁自动售检票系统安全性探讨[J]. 都市快轨交通，2006，19(4)：33-35.
[2] 丁耿，卢曙光，刘乐. 深圳地铁系统安全性研究[J]. 都市快轨交通，2006，19(2)：89-92.
[3] 广州地下铁道设计研究院. 西安市地铁二号线一期工程（北客站-韦曲南站）自动售检票系统集成采购项目[G]. 广州，2009.
[4] 王志海. 上海轨道交通售检票系统的应用与发展[J]. 城市轨道交通研究，2009(4)：52-56.
[5] 沈正华. 基于J2EE的自动售检票系统及实现[D]. 上海：复旦大学，2006.
[6] 祁国俊. 西安地铁的运营筹备管理[J]. 城市轨道交通研究，2011(7)：19-22.

（编辑：郝京红）

# Research on the Security of Metro AFC System

**Yang Ke**

（Affiliated Company of Operation, Xi'an Metro Company Limited, Xian 710000）

**Abstract**: This article describes the probable threats which the metro Automatic Fare Collection system possibly faces in terms of equipment, network, system and data. And in view of these threats the author proposes countermeasures against typical risks based on the practical experience from the operation of Xi'an metro Line 2. This may be of help for the security of AFC system on future new lines.

**Key words**: urban rail transit; Automatic Fare Collection system; system equipment; metro operation; security