文章编号：1005-8451（2017）11-0009-04

编组站综合自动化系统数据安全技术研究

刘珍珍，徐永梅
（中国铁道科学研究院 通信信号研究所，北京 100081）

摘 要：编组站综合自动化（SAM）系统中，数据是保证系统平稳有效运行的基础，数据安全是系统走向智能化的保障。为探究系统数据的安全性，从数据采集、传输、存储、应用的角度对系统数据安全防护体系进行分析。研究了以环境控制、边界安全、通信安全、访问控制等技术结合的SAM系统防护体系，提出了提高系统数据安全的完善建议。

关键词：编组站综合自动化系统；数据安全；安全控制中心；边界安全技术；应用安全
中图分类号：U284.6：TP39 **文献标识码：**A

Data security technology of marshalling station integrated automation system

LIU Zhenzhen, XU Yongmei
(Signal and Communication Research Institute, China Academy of Railway Sciences, Beijing 100081, China)

Abstract: In railway marshalling station integrated automation system, the data is the basis to ensure the smooth and effective operation of the system, and the data security is the guarantee for the system intelligent. In order to explore the security of system data, the system data security protection system was analyzed from the aspects of data acquisition, transmission, storage and application. This article studied on the protection system which was combined with the environmental protection technology, boundary security technology, communication security technology, access control technology and so on, and put forward suggestions for improving the data security of the system.

Keywords: marshalling station integrated automation system; data security; safety control center; boundary security technique; application security

编组站综合自动化（SAM）系统是以分散控制、集中操作、分级管理为基本思想，综合了计算机（computing）、通信（communication）、显示（CRT）和控制（control）等4C技术的复杂控制系统。SAM系统已在新丰镇、兰州北、丰台西等10余个路网型编组站投入使用，在提高编组站作业效率和安全控制水平方面发挥了重要作用。随着SAM系统的应用，以及系统本身的计算机控制和网络系统属性，决定了系统数据安全的重要性。另一方面，随着网络技术和信息技术的进一步发展，SAM系统在未来发展中必将接入更多的信息源点，系统更加开放，采集和处理的数据量更大，并且逐步从自动化走向智能化，系统面临的数据安全问题也日益增长。单一的数据安全技术很难保证系统安全、有序和有效地运行。数据安全主要面临的问题有恶意软件攻击，敌对威胁入侵，设备故障等[1]。因此，构建健全的数据安全防护体系，保证系统平稳有效的运行是SAM系统面临的重要课题[2]。

1 数据安全防护体系构成

SAM系统数据安全防护体系基于纵深防御的设计思想，采用软硬件环境控制技术、边界安全技术、通信安全技术、访问控制技术结合的方案，实现数据采集、传输、存储和应用全方位的安全防护，全面防止数据泄露、篡改等危险事件的发生，保障数据准确、完整、实时有效[3-4]。SAM系统数据安全防护体系架构如图1所示。

系统通过一个由电务维护中心、网络管理服务器、防病毒管理控制中心组成的安全控制平台实现对内部运行环境状态、通信网络状态、作业人员操作进行全面的监控和管理。

收稿日期：2017-08-09
基金项目：中国铁路总公司科技研究开发计划课题（2016X003-D）。
作者简介：刘珍珍，助理研究员；徐永梅，助理研究员。

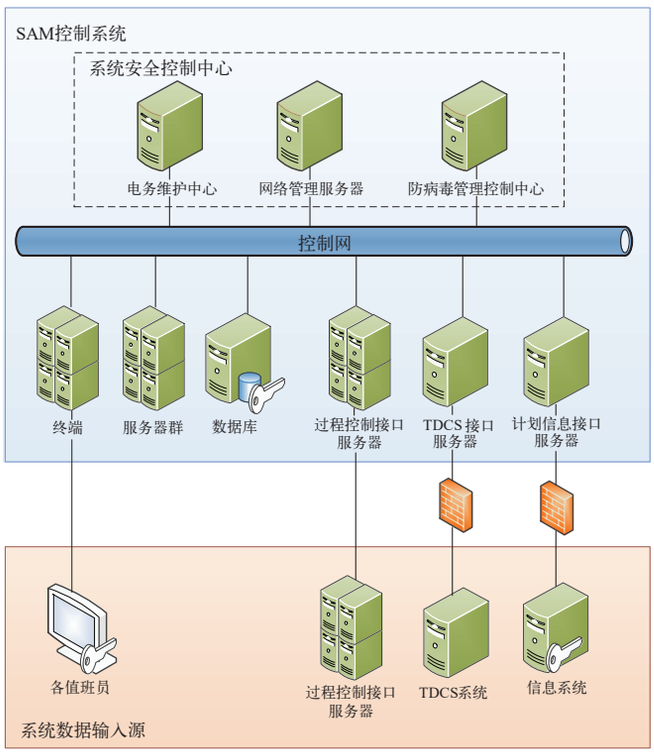

图1　SAM系统数据安全防护体系架构

下面从安全控制平台、数据采集、传输、存储、应用的角度介绍SAM系统的数据安全防护体系。

1.1　基于安全控制平台的软硬件环境控制

系统通过安全控制平台实现软硬件环境监测与控制。控制平台由电务维护中心、网络管理中心、防病毒管理控制中心组成，实现对系统的网络设备、应用服务器、接口服务器、终端设备的统一监测，实现作业过程中的实时状态、通信日志、运行日志、安全事件的记录。

（1）电务维护平台：统一监测系统设备运行状态。系统的每一台终端设备、应用服务器、接口服务器上均布置电务维护客户端（SMC，Signal MaintenanceClient）硬件监测程序，全面掌握设备的CPU、内存、网卡、串口等硬件运行状态；同时部署Comm软件和通信监测程序，实时监测软件运行状态、检验和过滤通信数据、收集通信日志和软件运行日志。提供电务维护终端软件，将运行状态、运行日志图形化展示出来，便于监测系统状态。

（2）防病毒管理：设置一台专用服务器作为防病毒管理控制中心，并在每台生产设备上布置防病毒软件，监测设备防控情况，统一管理、升级终端的安全软件，解决安全统一管理的需求。

（3）网络管理中心：监测系统双环网的各个核心交换机、接入交换机的状态，均衡网络中数据流量，防止网络风暴的发生。

1.2　数据采集

SAM系统数据来源可分为两类：（1）与列车运行调度指挥系统（TDCS）、车站管理信息系统、计算机联锁系统、驼峰自动化系统、停车器控制系统等接口获取的阶段计划、调度命令等信息、调车作业计划、站场表示信息等数据；（2）由值班员人工输入和修正的数据。

1.2.1　基于边界安全技术的系统接口设计

通过设置专用的接口设备、接口通信协议、边界安全设备等边界安全技术，实现与外部系统安全接口。

（1）设置专用的接口机，采用双机热备技术，4个通道交叉互联，故障发生时实现主备机、主备用通道无间隙切换，最大程度的保障通信的连续性，数据的实时性[7]。

（2）接口通信采用专用可靠的通信协议、安全编码、数据校验报文，具有异常中断自动重新建立连接机制，实现通信和通道状态的实时监测，数据正确性实时检验[8]。

（3）接口软件具有详细的日志记录功能，记录通信交互信息和原始数据信息，在发生软件异常、数据错误、数据篡改等问题时提供查找和定位的依据。

（4）接口设备布置防病毒软件，检测和防御入侵行为，防止数据被截获、修改和删除，防止控制命令执行错误，实现多重、全面防护。

（5）SAM系统与TDCS接口时，建立专用局域网络，接口机与路由器之间采用网闸设备进行物理隔离，如图2所示。实现不同系统间的物理隔离，避免了SAM系统与TDCS直接相连，仅允许双方接口机以指定的IP、确定的端口进行访问。

（6）SAM系统与管理信息系统接口时，通过网闸接入管理信息系统3层交换机，单方面访问信息系统数据库，实现访问控制，保障系统数据的完整性、有效性，有效的防止非法用户间的接入、黑客攻击等问题，如图3所示。

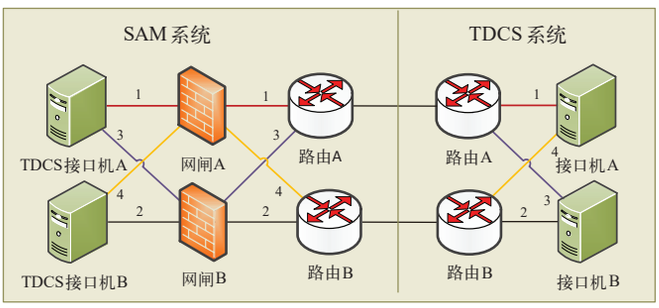

图2　SAM系统与TDCS接口

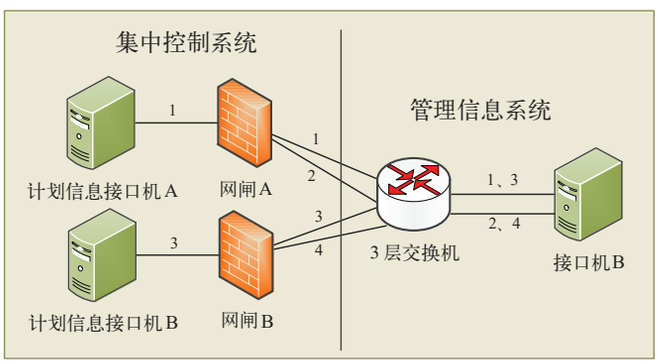

图3　SAM系统与管理信息系统接口

1.2.2　人工输入数据校验机制设计

SAM 系统的人机交互界面允许值班员根据实际作业情况修正和录入数据，通过信息融合、统计分析、机器学习等技术手段，结合提供输入备选方案、输入数据合法性检查、异常数据明确提示、错误数据拒绝接受等方法保证人工输入数据的有效性[5]。例如，值班员在修改行车计划的股道和方向时，系统会根据行车计划、运行图、固定进路等数据提供填写范围；在排列进路时，系统拒绝下达合法进路集以外的进路命令等。

1.3　数据传输

SAM 系统通过定制的网络通信程序、组播通信技术、安全通信协议等通信安全技术保证数据传输安全。系统利用局域网传输大量的作业状态数据，为防止数据在传输的过程中被第三方截取、破译、利用，系统统一采用定制的网络通信程序进行组播通信，禁止列表以外的多播组和数据流的输入、输出，通信程序对数据包配备唯一编码，实现数据唯一性、时序性控制，避免数据的重复解析。数据传输过程采用内部专用安全通信协议，运用 IP 地址和端口号限定处理，检查数据包的源地址、目标地址、传输协议、安全标记等，确定数据包的合法性，保证传输过程中数据的安全性和可靠性[6]。

1.4　数据存储

数据库服务器是 SAM 系统主要数据存储设备，存储了大量的与生产调度紧密相关的实时、历史数据，为保障数据在存储周期内不丢失、满足 7×24 h 不间断作业，系统通过以下方式保障数据的安全性和可靠性。

（1）数据库服务器采用双机热备硬件架构，配备一组磁盘阵列，采用 RAID10 的独立冗余磁盘阵列，提高数据并行响应速度的同时具有高可靠性和可修复性。

（2）根据数据访问需求，SAM 系统应用软件通过指定的账户访问数据库，对于终端用户访问数据库的需求，应设置不同的用户账户和访问权限，防止业务数据的泄露、更改和破坏。

（3）利用数据库系统的审计功能，监视和记录 SAM 系统中用户的操作信息，记录账号的登录事件，跟踪用户行为，一旦出现非法篡改、删除数据的行为做到有迹可循。

（4）建立完善的数据生命周期管理制度，对于实时库中的过期数据定期整理至历史库，以减轻应用软件的运行压力和数据库的响应速度。对于历史库中超过数据存储周期的数据定时清除，减轻数据库磁盘存储压力。

1.5　应用安全

1.5.1　访问控制技术

访问控制技术和身份认证技术是保证网络环境安全的重要手段，SAM 系统将作业终端设备、维护终端设备划分为安全访问区域，生产调度人员和系统维护人员仅允许通过安全访问区域的终端软件访问系统。终端设备采用身份认证技术，合理划分访问权限，防止用户的越权操作，禁止非法用户访问系统。合理的访问控制策略能够有效的降低对终端设备、应用服务器、数据库的安全威胁，防止数据篡改和泄密。

1.5.2　数据检查与修正

数据在运用的过程中，当系统检测到数据异常、明显偏离阈值时及时报警，提示作业人员对数据进行核实和修正。

（下转 P21）

提供了一种新的解决办法。

参考文献：

[1] Szpigel B. Optimal train scheduling on a single line railway[C]. //Operation Research, 1973:343-352.

[2] Hirao Y, Hasegawa Y. Developmentofauniversal train simulator (UTRAS) and evaluations of signaling systems [R]. Railway Technical Research Institute Quarterly Reports, 1995, 36.

[3] Hooghiemstra J, Teunisse M. The use of simulation in the planning of the Dutch railway services[C]. //Winter Simulation Conference, 1998:1139-1145.

[4] Zhang Y, Jin W. Simulation and Study of Gradient Search Algorithm of Single-track Railway Rescheduling[J]. Journal of System Simulation, 2010 (11): 2496-2501.

[5] 曹家明．双线铁路行车调度调整的优化方法 [J]. 西南交通大学学报，1995（5）：520-526.

[6] 彭其渊，朱松年．网络列车运行图的数学模型及算法研究 [J]. 铁道学报，2001（1）：1-8.

[7] Satoh A, Ohkawa Y, Ikeda H. Two studies on a computer aided train schedule adjustment[J]. Control in Transportation Systems, 1984: 67-74.

[8] Shi M, Maged D. Scheduling freight trains traveling oncomplex networks[J]. Transportation Research Part B: Methodological,2011, 8(7): 1103-1123.

[9] 聂　磊，张星臣．高速铁路列车运行调整策略的研究 [J]. 铁道学报，2001（4）：1-6.

[10] Chen L, Schmid F, Dasigi M, et al. Real-time train rescheduling in junction areas[J]. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 2010, 224(6): 547-557.

责任编辑　陈　蓉

（上接 P11）

1.5.3　日志与历史信息维护

建立完善的日志维护策略，详细记录操作记录、过程处理、通信交互、异常信息等 4 类日志，提供日志的集中管理和界面化的查询功能，便于维护人员查询和管理，对用户和系统的操作、行为进行审计追溯，保障数据安全。

2　未来展望

随着信息化的推进，SAM 系统将会不断完善数据安全技术方案，建立更加强大的防御体系，目前，系统正在以下方面做出改进：

（1）改进 SAM 系统的身份认证技术，远期实现支持数字证书方式的身份认证，以实现更高的安全性。

（2）开发 SAM 系统电务维护中心的数据管理及发布功能，功能上线后数据变更将实现统一平台发布，更利于数据的发布、变更版本控制，形成更加全面的安全监管。

（3）系统网络管理中心的网络管理软件目前还缺乏有效手段，未来将引入一种更为有效的网络分析软件，提供更为成熟的故障预防和定位功能，实现网络周期性安全审计、故障分析功能，有力保障数据的实时传输。

3　结束语

编组站综合自动化系统的数据安全是保证系统正常有效运行的基础，本文从数据采集、数据传输、数据存储、应用安全的角度全面分析了系统保障数据安全采取的技术手段，通过安全控制平台与边界安全技术、通信安全技术、访问控制技术的结合，达到数据独立完整、安全可靠的目的。

参考文献：

[1] 范科峰，姚相振，周睿康，等．信息安全技术工业控制系统安全控制应用指南 [M]. 北京：科学出版社，2016.

[2] 范　渊．智慧城市与信息安全 [M]. 北京：电子工业出版社，2016：247-249.

[3] 祝咏升，张　彦，姚红磊，等．铁路信息系统安全防护体系的研究 [J]. 中国铁道科学，2012（33）：139-143.

[4] 王　志，李　波．中国机车远程监测与诊断系统（CMD 系统）数据安全研究 [J]. 中国铁路，2017（4）：8-14.

[5] 蒋元华，姚宇峰．综合自动化技术条件下提高编组站作业信息质量的探讨 [J]. 铁路计算机应用，2015，24（10）：32-35.

[6] 祝咏升，丁　妍，张　彦．铁路客票系统信息安全技术方案设计 [J]. 铁道科学与工程学报，2012，9（5）：119-124.

[7] 高博文，刘艳君．编组站综合自动化系统与 TDCS 信息共享的实现 [J]. 中国铁路，2010（7）：57-59.

[8] 徐晓英．编组站综合自动化系统管控结合信息交换接口技术 [J]. 铁路计算机应用，2013，22（7）：31-32.

责任编辑　陈　蓉