铁路通信综合网络管理系统网络安全建设的研究

方晓君

摘　要：随着铁路通信技术的迅速发展和信息化水平的提升，铁路通信综合网络管理系统成为确保铁路安全高效运行的关键，结合《铁路通信网络安全技术要求第1部分总体技术要求》（Q/CR 783.1−2021）中的安全要求，对综合网管系统的网络安全进行研究和分析，旨在探讨通过现代网络安全技术和措施保障铁路通信网络的安全性。基于对铁路通信综合网络管理系统的网络安全风险分析，提出访问控制、入侵防御、行为检测、安全审计、终端防护和安全漏洞管理等措施，以提高铁路通信网络安全水平，确保铁路运输安全。

关键词：铁路通信；综合网络管理系统；网络安全建设

铁路作为国家重要的交通运输方式在经济社会发展和人民出行中扮演着关键角色。随着通信和信息技术的广泛应用，铁路通信综合网络管理系统已成为确保铁路安全高效运行的核心。然而，随着网络技术普及和网络攻击手段升级，铁路通信网络面临着前所未有的安全挑战。因此，建设安全、可靠、高效的铁路通信网络管理系统尤为重要。

一、铁路通信综合网络管理系统概述

1. 系统结构与功能

铁路通信综合网络管理系统是支持铁路通信的关键后台系统，整合软硬件技术为前端业务和信息处理提供全面保障，优化网络资源利用。系统以分层架构设计为基础，包括采集、数据、应用和展示层。在采集层，系统通过标准接口协议与通信子系统网管互联，实现网管原始数据的采集，收集关键性能指标数据。网络传输设备负责将这些数据通过网络安全可靠地传送到中央处理系统。数据层在此基础上将原始数据转换为标准数据，进行分析、存储和预处理，利用大数据和智能算法对收集到的信息进行深入分析，以识别潜在的故障和性能瓶颈。应用层主要依托数据层的数据提供基础的应用功能或者应用平台。最后，展示层将处理后的数据以图形化界面展示给管理人员，使其能够清晰地了解网络状态，并据此作出管理决策。系统的功能包括实时监控、告警管理、性能管理、拓扑管理、资源管理和配置调度等，旨在确保铁路通信的顺畅和安全。综合网络管理系统软件架构如图1所示。

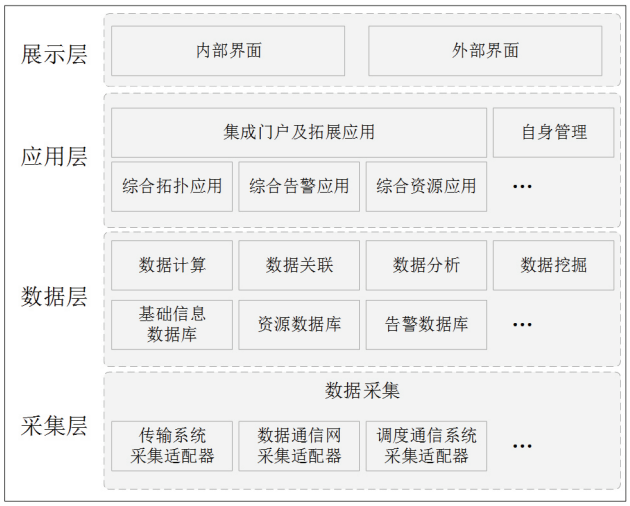

图1　综合网络管理系统软件架构图

2. 系统运行环境

软件环境方面，系统建立在稳定的操作系统之上，常见的有Linux或Unix系统，它们以其开放性和稳定性成为优选。硬件方面，需要可靠的服务器、存储设备、网络设备以及防火墙等支撑系统的持续运行。从人员的角度，需要专业的管理维护团队负责系统的日常维护、故障排除和系统升级，团队成员需掌握相应的网络管理和信息安全知识。

二、铁路通信综合网络管理系统网络安全风险分析

在铁路通信综合网络管理系统早期建设中，安全方面仅限于在网络边界部署防火墙进行防护。参考Q/CR 783.1–2021的要求，除了加强区域边界防火墙的安全项要求，还增加了对安全计算环境、安全通信网络和安全管理中心的要求，形成了以安全管理中心为核心，围绕安全通信网络、安全区域边界和安全计算环境构建的铁

作者简介：方晓君（1991.08——），女，汉族，本科学历，中级工程师，主要从事铁路通信工程设计与研究方面的工作。

威胁种类	威胁来源	防护对象	威胁描述
软硬件故障	环境因素	机房、办公场所、软硬件自身	设备硬件故障、系统本身或软件缺陷造等问题，对系统接入和运行产生影响。
网络攻击	恶意人员	传输或安全边界、操作系统和系统软件	通过网络，对信息系统进行攻击和入侵。
篡改	恶意人员	传输、应用系统、数据	非法修改信息，破坏信息的完整性，使系统的安全性降低或信息不可用。
越权或滥用	恶意人员	传输、网络架构、安全边界、操作系统和系统软件、应用系统、数据	超越权限访问了本来无权访问的资源，或者滥用职权，破坏信息系统。
恶意代码	恶意人员	操作系统和系统软件	故意在计算机系统上执行恶意任务的程序代码。
身份假冒	恶意人员	接入边界、应用系统	伪造或盗取合法人员身份进行非法访问信息资源。
泄密	恶意人员	数据	信息泄露给不应了解的他人。

路网络安全技术框架。结合综合网管的特点和网络安全标准规范的实施，上表是对铁路通信综合网络管理系统部分网络安全风险的分析。

三、铁路通信综合网络管理系统网络安全防护

根据国铁集团铁路通信系统定级要求，遵循《铁路通信网络安全技术要求 第1部分：总体要求》（Q/CR 783.1–2021），铁路通信网络安全对终端安全、补丁修复、漏洞补丁推送、身份鉴别、访问控制、终端管控、用户审计、防黑加固、资源控制及网络边界等安全防护等功能的要求，通过对铁路通信综合网络管理系统安全风险的分析，提出网络安全架构建设方案，实现网络安全监测预警、集中管控及响应处置。网络整体架构和传输线路是否具备可靠性、稳定性和保密性，是衡量系统安全的基本条件，通信网络的安全主要包括：网络架构安全、通信传输安全、边界安全、防入侵、网络安全审计和网络安全的集中管控等方面。即四个层面：安全通信网络、安全区域边界、安全计算环境和安全管理中心。具体安全防护内容如下。

1.安全通信网络

（1）网络架构安全

网络架构的合理性直接影响其是否能有效满足业务需求，应具备冗余性、足够带宽以满足高峰时段数据传输需求，并采用合理的网段和VLAN划分。

（2）通信完整性与保密性

数据在网络中存储和传输时可能面临信息丢失、重复或传输错误，甚至遭受攻击或欺诈行为，导致信息不一致。为保障信息传输过程的一致性，必须确保发送、接收和保存的信息内容一致，并提供有效的检测机制以确保通信的完整性。此外，在数据传输过程中，为抵御各类攻击并防止数据泄露，应采用加密措施确保数据的保密性。

2.安全区域边界

（1）边界隔离与访问控制

边界安全要求对接入网络和外联进行双重管控，铁路通信综合网络管理系统虽然方便了业务子系统的接入分析，但也带来了潜在的安全风险。未经阻拦的外部用户接入可能破坏网络安全边界，导致蠕虫传播、数据泄露等问题。因此，需实施非法客户端禁入措施，并限制或审查内部用户连接到外部网络的行为。

（2）防入侵和防病毒

现代病毒趋势呈现出黑客程序和蠕虫病毒结合、网络传播增加等特点。一旦病毒进入系统网络，将对综合网管系统造成破坏。因此，病毒防护应在系统边界部署，进行网络层病毒检测，防止感染内部主机。此外，针对来自非可信网络的各类攻击，需要通过安全措施主动阻止各种威胁，如病毒、木马、间谍软件、端口扫描等，以保护系统核心资产免受攻击危害。

3.安全计算环境

铁路通信综合网络管理系统存储和处理着大量的铁路业务数据，也是攻击者的最终目标，主机系统自身的漏洞一旦被攻击者利用，获取系统权限，将直接导致数据泄露甚至信息系统遭受破坏。此外，应用和数据是安全保护的对象，应用系统在开发过程中由于技术的局限性和开发管理的漏洞，总是存在一些安全漏洞，在系统上线后，被恶意攻击者利用，进而给铁路的经济利益、业务、甚至声誉带来影响。

计算环境安全需求包含对主机和应用系统用户进行身份认证、访问控制、主机防病毒以及终端安全防护等措施。具体内容如下：

（1）系统层面双因素认证

实现登录操作系统和数据库系统的身份识别和验证，采用用户名和密码方式进行本地登录，远程登录应采用

用户名、密码和数字证书组合认证。引入新型多因素认证和单点登录等技术，平衡用户身份验证的易用性与安全性。

（2）系统访问控制

系统应实现以下访问控制方面的功能：

1）关闭不必要的端口和服务；

2）根据安全策略限制用户文件访问权限，关闭默认共享；

3）数据库系统应限制用户对文件或系统设备的操作权限；

4）角色管理对权限做出标准划分，分配最低权限；

5）设置不同特权用户，合理分离权限；

6）删除多余和过期账户，如GUEST；

7）禁止多人共享相同账户；

8）操作系统最小化安装，及时更新系统补丁。

（3）主机防病毒

终端和服务器主机需防恶意代码软件，定期更新软件版本和病毒库。

（4）终端安全防护

所有终端安全防护工作遵守以下要求：

1）资产信息管理，包括资产收集、配置核查、和在线管理；

2）终端入网安全性评估；

3）补丁管理，建立独立分发服务器，保持补丁及时更新；

4）控制移动存储介质使用。涉密介质需要注册，实现违规使用报警；

5）建立企业级病毒防护系统，统一病毒库、全网监测和统计。

4.安全管理中心

在铁路通信综合网络管理系统建设安全管理中心，实现集中安全管控，主要通过安全设备实现统一管控、查杀、病毒库更新和日志审计等功能，具体如下：

（1）日志审计能力

1）集中采集、统一管理、存储、统计分析各类系统日志；

2）满足等保合规要求，便于资产管理和安全事件取证；

3）严格按照等保和铁路通信网络安全规定留存审计记录至少6个月；

4）实时采集不同厂商的安全设备、网络设备、主机、操作系统和应用系统产生的日志，经过标准化处理后解析和存储。

（2）运维审计能力

1）统一运维管理和审计，包括铁路通信综合网络管理系统中的网络设备、数据库、安全设备、主机系统和中间件等资源。

2）记录用户身份认证和操作行为，实现权限管理和行为审计。

综合以上研究，综合网管系统的网络安全建设架构如图2所示。

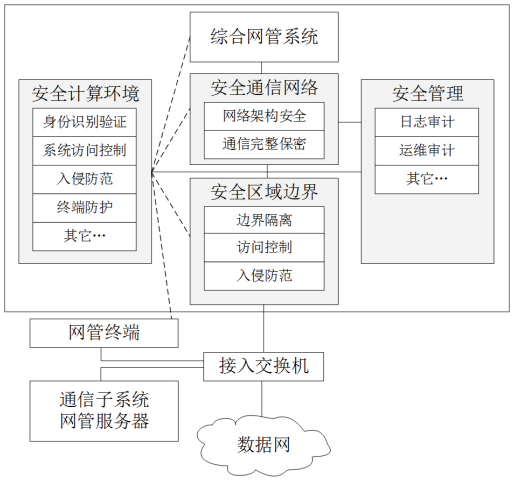

图2　综合网管系统网络安全建设架构图

结语

通过深入探讨通信网络存在的安全风险及安全威胁，根据国家网络安全等级保护要求，分析铁路通信综合网络管理系统的实际安全需求，建立符合需求的网络安全保障框架结构，提出安全保障方案，综合提升系统的安全保障能力和防护水平，确保系统安全稳定运行。

参考文献

[1]中国国家铁路集团有限公司.铁路通信网络安全技术要求第1部分：总体技术要求：Q/CR783.1-2021[S].北京：中国铁道出版社，2021.

[2]乔桢.铁路数据通信网网管系统安全防护的研究[J].铁路通信信号工程技术，2017，14（4）：23-25.

[3]国家铁路局.铁路通信设计规范：TB10006-2016[S].北京：中国铁道出版社，2016.

[4]赵圣娜.铁路通信承载网网络安全方案研究[J].数字通信世界，2023（6）：13-16.DOI：10.3969/J.ISSN.1672-7274.2023.06.004.

[5]魏旻.铁路通信综合网络管理系统网络安全建设的研究[J].铁路通信信号工程技术，2024，21（03）：42-46+88.