交通通信工程中数据安全防护策略探讨

师　飞
京台高速公路廊坊事务中心　河北　廊坊　065000

摘　要：数字化赋能下，交通通信工程数据体量持续增长，涵盖业务、隐私、运维三类核心数据，全生命周期流转存在多重安全风险。当前行业存在防护技术老旧、动态防御能力薄弱、数据分级防护缺失、安全管理制度不完善等问题。本文结合数据安全防护原则与立体防护架构，从技术、管理、运维、应急多维度提出优化策略，构建全流程智能防护体系，旨在化解数据泄露、篡改等风险，全面提升交通通信工程数据安全防护水平。

关键词：交通通信工程；数据安全；防护策略

引言：智慧交通建设持续推进，交通通信工程数字化、智能化程度不断提升,各类数据已成为交通运营、路网管控、工程运维的核心支撑。交通数据具备实时性强、流转复杂、关联性高的特点，同时伴随多元化安全隐患。现阶段传统防护模式难以适配新型网络攻击与数据流转需求，数据安全漏洞频发。在此背景下，深入剖析数据安全风险与现存短板，探索科学完善的防护策略，对保障交通基础设施稳定运行、守护用户数据安全具有重要现实意义。

1 交通通信工程数据安全相关理论与概述

1.1 交通通信工程核心数据概述

（1）数据分类：交通通信工程运行过程中产生的海量数据，可划分为三大核心类型。其一为交通业务数据，包含实时路况信息、车辆通行统计数据、交通调度管控数据等，是交通运营调度、路网管理的核心依据。其二为用户隐私数据，涵盖公众出行轨迹、出行偏好、个人身份登记信息等，直接关联用户个人信息安全。其三为工程运维数据，主要包括通信设备运行参数、网络运维日志、系统配置与升级数据等，是保障交通通信网络稳定运行的基础数据。（2）数据特征：交通通信工程数据具备鲜明的行业特性。整体实时性极强，需动态更新以适配交通流量的实时变化；数据流转链路复杂、传输节点繁多，需跨设备、跨区域、跨平台传输交互。同时各类数据关联性极高，业务、用户、运维数据相互交织，且涉密性差异化显著。其中部分核心业务与运维数据，直接关乎公共交通安全与交通基础设施稳定运行，安全防护优先级更高[1]。

1.2 数据安全核心内涵与防护原则

（1）数据安全核心内涵：交通通信工程数据安全以数据保密性、完整性、可用性为核心三大要素，同时兼顾数据可控性与可追溯性。核心目标是实现数据采集、传输、存储、应用、销毁全生命周期的规范化管控，杜绝数据泄露、篡改、丢失、滥用等风险，确保数据合法、安全、有序流转。（2）安全防护基本原则：防护工作严格遵循五大核心原则，即最小权限、全程可控、分层防护、合规适配、动态迭代。在筑牢安全防护屏障的同时，兼顾交通通信业务的运行效率与服务质量，平衡安全管控与业务发展需求，避免过度防护影响交通运营效能。

1.3 交通通信工程数据安全防护架构

（1）分层防护架构：构建物理层、网络层、数据层、应用层、运维层五层立体防护体系，各层级独立履职、联动协同。从物理设备防护、网络传输防护，到数据内容、应用场景、运维全程防护，形成全方位、无死角的安全防护格局。（2）全生命周期防护框架：覆盖数据采集、传输、存储、共享应用、销毁全流程，搭建闭环式安全管控体系，实现每一个数据流转环节的可监管、可防护、可追溯，全面提升交通通信工程数据安全防护能力。

2 交通通信工程数据安全风险与防护现存问题

2.1 数据全生命周期安全风险分析

（1）数据采集风险：交通通信工程数据采集终端分布范围广泛、部署点位分散，涵盖道路监测设备、车载终端、站点通信设备等多种类型。多数野外终端设备运行环境复杂，硬件防护与安全防护能力薄弱，缺乏完善的入侵防护机制。在数据采集过程中，极易出现非法设备接入、非法采集数据的情况，同时设备故障、外界干扰或人为入侵，会导致采集的数据失真、缺失，恶意人员可通过攻破终端设备篡改原始采集数据，直接影响后续交通调度与运维决策的准确性。（2）数据传输风险：交通通信数据传输体系较为复杂，存在公网与专网交叉混用、多链路并行传输的特点，数据流转节点多、路径不固定。复杂的网络传输环境大幅提升了安全风险，数据在传输过程中容易被非法窃听、链路劫持，恶意攻击者可拦截传输数据包并篡改核心数据。同时，网络拥堵、

链路故障等问题会造成数据延迟、丢包，不仅影响交通业务实时运转，还会导致数据传输完整性受损，引发各类安全隐患[2]。（3）数据存储与应用风险：现阶段交通通信数据呈海量化、集中化存储特点，大量业务数据、隐私数据集中存储于核心服务器中，一旦服务器被攻破，极易造成批量数据泄露，引发大规模安全事故。在数据共享与业务应用环节，系统权限管控不严，存在用户越权访问、工作人员违规调取使用涉密数据等问题。此外，业务操作后数据留存不规范、冗余数据未及时清理，进一步加剧了数据滥用和泄露的风险。

2.2 技术层面防护短板

（1）防护技术老旧：目前部分交通通信工程基础设施建设时间较早，长期沿用传统的安全防护设备与技术体系。传统加密算法、入侵检测技术迭代更新滞后，仅能抵御基础的常规网络攻击，无法适配当下多样化、新型的网络攻击手段，对高级渗透、隐蔽式数据窃取、恶意代码攻击等新型风险的抵御能力严重不足。（2）动态防护能力不足：现有防护体系多以静态被动防御为主，缺乏智能化、实时化的安全监测与预警机制。系统无法对数据访问、网络流转行为进行全天候动态监测，难以快速识别异常访问、隐蔽性攻击和数据违规流转行为，往往在安全事件发生后才能发现问题，无法实现事前预警、事中拦截，整体防护时效性较差。（3）数据分级防护缺失：多数交通通信工程未建立完善的数据分级分类防护体系，未依据数据涉密等级、业务重要程度划分防护标准。核心涉密的调度数据、用户隐私数据与普通运维数据采用统一防护模式，既造成安全防护资源的浪费，又导致核心数据防护力度不足，极易成为安全攻击的突破口。

2.3 管理与运维层面现存问题

（1）安全管理制度不完善：行业现有通用安全制度无法完全适配交通通信工程的专属场景，针对性的data安全管控制度存在空白。数据权限分配、日常操作审计、涉密数据保密、设备运维管控等相关规范落地流于形式，缺乏严格的执行监督机制，导致制度无法有效约束各类数据操作行为。（2）人员安全素养不足：一线运维人员、业务操作人员的数据安全专业素养参差不齐，常态化安全培训机制缺失。多数人员安全意识薄弱，日常操作中存在违规传输涉密数据、弱密码使用、账号随意共享等问题，人为操作不规范成为数据安全风险的重要诱因。（3）应急处置体系不健全：行业尚未形成标准化、系统化的数据安全应急处置体系，针对数据泄露、系统入侵、数据篡改等安全事件的应急预案不完善。安全事件发生后，存在响应流程混乱、处置效率低下的问题，且缺乏事后复盘、问题整改、机制优化的闭环流程，无法有效规避同类风险再次发生。

3 交通通信工程数据安全防护优化策略

3.1 数据全生命周期技术防护策略

（1）采集环节防护：针对交通通信终端设备分散、数据易篡改失真的问题，全面强化终端安全管控工作。对道路监测终端、通信站点设备、车载采集终端等各类设备进行安全升级，统一部署终端安全监测模块，实时监控终端运行状态与采集行为。同时严格规范数据采集技术标准与操作流程，搭建标准化数据校验、甄别机制，对采集数据的完整性、真实性、有效性进行实时核验，从源头拦截虚假数据、异常篡改数据，杜绝不合格数据录入系统，保障原始数据的精准可靠。（2）传输环节防护：为解决数据传输窃听、劫持、丢包等风险，全方位优化数据传输防护体系。针对公网、专网交叉传输的复杂场景，采用AES等高强度加密算法对所有传输数据包进行加密处理，杜绝明文传输漏洞。优化交通通信专属专网传输通道，清理冗余传输链路，提升通道稳定性与安全性。同时搭建专属VPN加密传输链路，实现核心业务数据、涉密隐私数据的独立传输，有效抵御网络窃听、链路劫持与数据篡改攻击，保障数据传输全程安全稳定[3]。（3）存储与应用环节防护：推行精细化数据分级分类存储模式，根据数据涉密等级、重要程度划分存储区域，将核心调度数据、用户隐私数据进行隔离加密存储，规避批量泄露风险。同步部署数据脱敏、异地备份、故障恢复技术，对公开共享数据进行脱敏处理，定期完成数据备份，防止数据丢失损毁。搭建动态权限管控与全程溯源体系，按需分配访问权限，实时记录数据查阅、调用、下载行为，实现数据应用全程留痕、可追溯、可监管。

3.2 多层级智能安全防护技术优化

（1）网络层防护升级：对传统网络防护设备进行迭代升级，优化智能防火墙、入侵检测与防御系统的防护规则，适配交通通信网络的运行特性。部署智能化流量分析与异常识别模块，对网络访问行为、数据传输流量进行全天候动态监测，精准甄别异常访问、恶意扫描、渗透攻击等行为，自动阻断非法操作，封堵网络安全漏洞，构建主动式网络安全防护屏障。（2）应用层安全加固：针对交通通信各类业务系统开展常态化安全加固工作，定期开展漏洞扫描、风险检测，及时修复系统代码漏洞与安全缺陷。搭建全方位业务行为审计系统，全面记录系统接口调用、账号权限变更、涉密数据下载、业务操作执行等各类日志，实现应用场景全行为监管。通过常态化审计溯源，及时发现违规操作与安全隐患，保

障业务系统稳定安全运行[4]。（3）引入新型防护技术：打破传统静态防护局限，引入零信任架构、区块链存证、同态加密等前沿安全技术。依托零信任“永不信任、持续验证”的核心理念，摒弃固定信任机制，实现每一次数据访问、交互的动态核验，适配复杂网络环境。利用区块链存证技术保障操作日志、数据记录不可篡改，依托同态加密技术实现加密状态下的数据运算与交互，全方位提升数据隐私安全与日志真实性。

3.3 完善数据安全管理体系

（1）健全规章制度：结合交通通信工程行业特性、业务场景及合规要求，搭建系统化、专属化的数据安全管理制度体系。细化完善数据分级分类管理、账号权限管控、涉密数据保密、日常操作审计、安全责任划分等规章制度，明确各部门、各岗位的数据安全职责，细化操作规范与惩戒机制，杜绝制度空白、执行流于形式等问题，实现数据安全管理有章可循、有据可依。（2）强化人员管控与培训：构建常态化数据安全培训体系，定期面向运维人员、业务操作人员、管理人员开展专项培训，覆盖安全法律法规、操作规范、风险识别、应急处置等内容，全面提升全员安全意识与实操能力。建立健全人员安全考核与责任追责机制，将数据安全工作纳入岗位考核，约束人员操作行为，从根源杜绝人为违规操作引发的安全隐患。（3）落实常态化安全审计：建立常态化风险排查与合规审计机制，定期对数据采集、传输、存储、应用全流程开展安全审计与漏洞排查。针对排查出的安全风险、制度漏洞、技术缺陷，建立问题台账，落实整改责任与整改时限，实现闭环管控。通过常态化审计排查，持续规避潜在风险，构建长效化安全防控机制[5]。

3.4 构建高效应急处置与运维体系

（1）制定专项应急预案：结合交通通信工程常见安全风险，针对数据泄露、系统入侵、数据丢失、数据篡改等不同类型安全事件，制定差异化、标准化的专项应急预案。明确各类事件的处置流程、权责分工、应对措施，细化预警、处置、止损、恢复全流程操作规范，确保突发安全事件发生时可快速响应、规范处置。（2）搭建实时监测预警平台：依托SIEM安全信息与事件管理系统，搭建一体化数据安全实时监测预警平台，整合网络、设备、数据、系统全维度安全数据。实现对数据安全状态的全天候实时监控，智能识别异常访问、数据违规流转、网络攻击等风险，自动触发预警提示，大幅提升安全风险的预判与前置防控能力。（3）完善事后复盘优化机制：建立安全事件闭环复盘优化体系，每起安全事件处置完成后，组织专业人员开展全面复盘分析，深挖技术、管理、运维层面的问题短板。结合复盘结果迭代优化防护策略、管理制度与应急预案，针对性补齐安全防护短板，规避同类风险重复发生，持续提升整体数据安全防护水平。

结束语

本文系统梳理了交通通信工程数据安全的核心理论，全面分析数据全生命周期的安全风险，总结了技术、管理、运维层面的防护短板，并针对性提出全流程技术防护、智能防护升级、管理制度完善、应急体系搭建的一体化优化策略。全方位筑牢交通通信数据安全屏障，可有效规避各类数据安全风险，保障数据有序安全流转，助力智慧交通行业安全、稳定、高质量可持续发展。

参考文献

[1]邹智荣.列车通信网络安全现状分析及应对方案研究[J].机车电传动,2023,16(1):78-85.

[2]王春军.城市轨道交通信号系统安全防护体系建设研究[J].中国新通信,2022,24(10):77-79.

[3]徐彦飞.轨道交通弱电系统信息安全等级保护整体防护思考[J].数字通信世界,2021,31(2):159-162.

[4]肖兰.电子通信工程信息安全防护探讨[J].中国信息界,2024,25(4):220-222.

[5]沈宗果.浅谈电子信息通信工程中设备抗干扰问题[J].内江科技,2022,43(8):92-96.