新形势下铁路TDCS/CTC系统网络安全防护机制构建研究

刘　剑　丁景新　檀晓羽　刘晓畅　朱新宜
北京铁路通信信号运维中心　北京　100038

摘　要：随着“交通强国”战略的深入实施与新一代信息技术在铁路行业的深度融合，铁路列车调度指挥系统（TDCS）与调度集中系统（CTC）正面临网络攻击武器化、攻击面泛化、供应链安全风险攀升等新挑战，传统以安全隔离加固为主的防护模式持续经受考验。在此新形势下，TDCS/CTC系统作为行车调度核心，关乎运输安全与效率，本文剖析其核心架构与安全需求，梳理安全威胁、风险传导路径及防护短板。构建涵盖事前、事中、事后及全生命周期管控的一体化防护机制，并从技术、制度、人才、协同四方面提出实施保障与优化建议，为提升系统防护能力建言献策。

关键词：铁路TDCS/CTC系统；网络安全；防护机制构建

引言：当前，全球科技革命与产业变革加速演进，铁路行业正迈向智能化、数字化发展新阶段，TDCS/CTC系统作为铁路行车调度指挥的“神经中枢”，其功能覆盖列车运行监控、调度命令传输等关键环节，战略地位愈发凸显。然而，新形势下网络空间安全态势日趋复杂，定向攻击、勒索病毒等恶意行为频发，给TDCS/CTC系统带来严峻安全挑战。因此，深入研究TDCS/CTC系统网络安全防护机制构建，对筑牢铁路网络安全防线，推动铁路行业高质量发展具有重要现实意义，本文就此展开系统探讨。

1　新形势下铁路 TDCS/CTC 系统网络安全核心架构与安全需求

网络安全等级保护2.0系列标准及要求发布以来，铁路TDCS/CTC系统运营部门积极遵循其技术要求，以“一个中心、三重防护”为核心指导思想，构建了符合自身保护等级要求的安全防护体系，该体系依托安全通信网络、安全区域边界、安全计算环境和安全管理平台，形成多层纵深防御机制，其中安全通信网络作为防护体系的根基，基于双线冗余、专网专线等安全特性，确保网络通信的高可用性和数据安全；安全区域边界作为防护体系的前沿阵地，通过边界隔离、安全审计等安全防护模块，构建动态防御屏障，有效抵御外部威胁渗透；安全计算环境作为防护体系的内核，采用强制访问控制、外设管控等安全控制机制，强化系统内部的计算组件安全，防止内部违规操作和数据泄露；安全管理平台作为防护体系的大脑，实现对各安全平面的统一监测、智能联动和集中管控，确保整体防护体系高效协同，形成从网络、边界到计算环境的纵深防御闭环[1]。

在当前网络安全新形势下，铁路TDCS/CTC系统作为关键信息基础设施和网络安全等级保护四级系统，其安全防护需求可归纳为四大核心维度：数据机密性保障，需重点防护调度命令、列车运行状态等核心业务数据的防窃取与防篡改能力，确保信息传输存储安全。系统可用性保障，建立高可靠机制，保证在网络攻击或设备故障等极端情况下调度功能持续运行，维持列车运营秩序。身份可信性保障，要求构建多因素认证体系，实现设备接入、人员操作的精准身份鉴别与权限控制，阻断非法访问路径。合规性保障，需严格遵循《铁路关键信息基础设施安全保护要求》等标准规范，满足等保四级及行业安全要求。上述四维需求相互支撑，共同构成TDCS/CTC系统的安全防护目标体系，为纵深防御机制建设提供明确导向[2]。

2　新形势下铁路 TDCS/CTC 系统网络安全威胁与风险分析

2.1　安全威胁类型与演化特征

基于等保2.0的网络安全保障体系显著提升了铁路TDCS/CTC系统的综合安全防护水平，为后续的安全防护工作开展打下了坚实基础。但考虑到铁路关基在国家铁路运输体系中的重要地位、网络安全威胁环境的不断演变，以及持续收紧的政策要求，仅依靠等保2.0安全保障体系并不能完全满足铁路关基复杂的安全需求及日益严格的政策法规要求[3]。

新形势下，铁路TDCS/CTC系统面临的安全威胁呈现出三个显著特征：威胁来源多元化，攻击主体已从个体黑客扩展至有组织专业团体，攻击手段日趋复杂；攻击方式精准化，攻击者针对系统特定漏洞开展定向攻击，利用高级持续性威胁（APT）等手段实施精确打击；攻击产业链成熟化，从漏洞挖掘到攻击实施的完整产业链已

经成形，大大降低了攻击门槛。同时，技术漏洞威胁也不容忽视，系统核心组件、第三方软件及老旧设备存在的安全漏洞，易被攻击者利用形成安全突破口。运维管理威胁持续存在，人员违规操作、权限配置不当及安全意识薄弱等不足，可能引发内部安全事件。

2.2 风险传导路径与影响后果

TDCS/CTC系统安全风险传导具有显著的链式扩散特征，核心传导路径包括三条：一是通过信息技术系统（IT）作为跳板，逐步侵入并控制运营技术系统（OT），将传统网络攻击手段转化为对物理设备的实际控制，最终威胁生产安全；二是从终端设备向核心节点蔓延，利用车站终端、接入网络等薄弱环节，逐步渗透至调度中枢；三是通过供应链传导，在设备采购、软件安装等环节引入恶意组件，形成潜伏性风险。风险一旦爆发，直接影响列车调度指挥系统，间接影响运输中断导致的经济损失，造成不良社会影响。

2.3 当前防护体系存在的短板

当前铁路TDCS/CTC系统的安全防护体系在应对新型网络安全挑战时，仍存在一些需要完善的地方。具体表现在以下几个方面：首先，主动防御主要依靠“一个中心、三重防护”等基础防护手段，在面对日益增多的定向攻击和高级持续性威胁时，配套网络安全监测分析、追踪溯源等手段不足，防御监测仍需持续巩固。其二，在技术适应性上，部分安全防护方案需要充分考虑系统对实时性的严格要求，在安全性和业务连续性之间寻求更好的平衡。其三，在访问控制管理方面，当前的身份认证机制还存在优化空间，主要表现为权限分配不够精细、设备账号共享等情况。此外，系统常态化风险评估、应急演练等应急响应能力也需强化，以提升安全事件发生后的快速处置和系统恢复能力[4]。最后，跨部门的协同配合机制还需进一步完善，技术运维与调度指挥等部门之间的联动配合，对整体防护效能的提升至关重要，通过加强部门协作，可以有效避免出现防护"孤岛"现象。

3 铁路 TDCS/CTC 系统网络安全防护机制构建

3.1 防护机制总体框架设计

基于纵深防御理论与“设计即安全”理念，构建“多层防御、全流程管控、多维度协同”的TDCS/CTC系统网络安全防护总体框架。框架纵向分为物理层、网络层、应用层、数据层四层防护，物理层强化设备与机房安全防护，网络层构建分区隔离与访问控制体系，应用层加强软件漏洞防护与权限管控，数据层实现全生命周期加密与完整性校验。横向覆盖事前预防、事中监测控制、事后处置恢复全流程，形成闭环管控。同时融入技术、制度、人才等多维度支撑要素，实现“技术防御+管理保障”协同发力。框架核心目标是实现对安全威胁的精准识别、快速响应与有效处置，兼顾系统安全性与运行实时性，为TDCS/CTC系统安全稳定运行提供全方位保障。

3.2 事前预防机制：源头风险管控

事前预防机制聚焦源头管控，筑牢安全第一道防线。建立全要素安全准入制度，对接入系统的设备、软件进行严格合规性检测，审核供应商资质与安全能力，杜绝不合格产品入库；对运维人员、调度人员实行分级身份认证，采用多因子认证技术强化身份核验；构建常态化漏洞管理体系，定期开展系统漏洞扫描与风险评估，建立漏洞台账，按严重程度分级处置，及时推送补丁并验证修复效果；优化系统架构设计，采用分区隔离技术划分安全域，设置访问控制策略，限制跨域数据流动；在关键节点部署安全网关，过滤非法访问请求。此外，制定完善的安全管理制度与操作规范，开展全员安全培训，提升人员安全意识与操作水平，从源头降低安全风险[5]。

3.3 事中监测与控制机制：动态风险拦截

事中监测与控制机制以动态防御为核心，实现风险精准拦截。构建多维度安全监测体系，整合流量监测、行为分析、日志审计等技术，对系统运行状态、数据传输过程进行实时监控，建立正常行为基线，一旦发现异常流量、违规操作等情况，立即触发预警；强化精细化访问控制，基于角色与属性构建权限管控模型，严格限制不同用户、设备的访问范围，实现“最小权限”原则；利用安全区域边界、主机安全加固技术固化访问规则，提升权限管理的精准性与不可篡改性；加强数据传输与安全防护，采用国密算法对敏感数据进行全链路加密，通过哈希校验确保数据完整性，防止数据被篡改。同时，部署入侵检测与安全隔离设备，对恶意攻击行为进行实时监测与阻断，保障系统运行安全。

3.4 事后处置与恢复机制：风险止损与系统复原

事后处置与恢复机制聚焦风险止损与快速复原，降低安全事件影响。建立分级应急响应体系，依据安全事件严重程度划分等级，制定对应的响应流程与处置方案；组建专业应急团队，开展常态化应急演练，提升应急处置能力。优化系统恢复策略，针对设备重要等级、不同安全事件制定差异化恢复方案，缩短系统设备影响时间。建立事件溯源与复盘机制，通过日志分析、行为回溯等技术精准定位攻击源头与传播路径，总结事件教训；结合复盘结果优化防护体系，修补安全漏洞，提升系统防御能力，形成“处置-复盘-优化”的闭环管理。

3.5 全生命周期管控机制：长效安全保障

网络安全生命周期管控机制贯穿系统设计、建设、运维、报废全流程，实现长效安全保障。设计阶段融入“设计即安全”理念，开展安全需求分析与风险评估，将安全防护要求嵌入系统架构设计，从源头规避安全隐患。建设阶段严格执行安全合规标准，对设备采购、软件开发、系统集成等环节进行安全管控，开展安全测试与验收，确保系统建成即达标。运维阶段建立常态化安全管理机制，定期开展安全评估、漏洞扫描与补丁更新及安全培训，规范运维操作流程，提升运维团队专业能力。报废阶段制定安全处置方案，对设备、数据进行妥善处理，销毁敏感信息，拆除存储介质，防止设备复用或数据泄露引发安全风险。

4 防护机制实施保障与优化建议

4.1 技术保障：关键技术融合与创新应用

技术保障需聚焦关键技术融合与创新，提升防护机制效能。推动国密算法与身份认证、数据溯源等环节深度融合，构建可信身份认证体系与数据追溯链路，强化系统安全可信性。构建人工智能与安全分析相结合的威胁识别模型，提升对新型攻击的精准识别与预警能力；优化加密技术应用，针对系统实时性需求，选用轻量化加密算法，在保障数据安全的同时，避免影响业务信息处理效率。

4.2 制度保障：完善合规性与管理制度体系

制度保障需构建完善的合规与管理体系，规范防护机制落地。对标铁路网络安全相关法规，制定适配TDCS/CTC系统的安全管理制度，明确安全目标、责任分工与操作规范，健全合规性审查机制，定期开展安全合规评估，及时整改不合规问题，确保防护机制符合运营监管要求。此外，建立安全管理制度动态更新机制，结合技术发展与威胁演化，及时优化制度内容，提升制度的适配性与实效性。

4.3 人才保障：打造专业化安全团队

人才保障需聚焦专业化团队建设，夯实防护机制实施基础。构建多层次人才培养体系，培养兼具铁路业务知识与网络安全技能的复合型人才，加强现有团队培训，重点提升在新型攻击应对等方面的防御处置能力。强化人员安全意识培养，定期组织安全警示教育与案例分享，提升全员对安全风险的认知与防范能力，打造一支“业务精、能力强、意识高”的专业化安全团队。

4.4 协同保障：构建网络安全管理与共享平台

强化协同联动机制，建立完善铁路TDCS/CTC网络安全管理与共享平台，规范威胁信息、漏洞数据及防护经验的上报与共享流程，实现安全风险的早发现、早预警、早处置，整体提升TDCS/CTC安全防御能力。另外，合理划分自主防护与外包服务边界，在核心技术自主可控的基础上，引入专业安全服务机构提供渗透测试、应急响应等增值服务，形成“自主核心+外包补充”的协同模式，构建多方优势互补、风险共防的安全生态体系。

结束语

新形势下，铁路TDCS/CTC系统网络安全防护机制构建是保障铁路运输安全的重要举措，也是铁路数字化转型的重要支撑。因此，防护机制的有效落地需坚持技术创新与管理优化并重，实现网络安全主动防御与全域防护持续深化。未来，随着智能铁路建设推进，需持续关注技术发展与威胁演化，不断优化防护机制，推动国密算法、人工智能等新技术深度应用，筑牢铁路网络安全防线，为铁路行业高质量发展提供坚实安全保障。

参考文献

[1]张晶,余卫巍.铁路信号系统网络安全风险分析与防护措施研究[J].铁道通信信号,2022,58(11):48-52.

[2]吕涛,潘清越.铁路调度指挥系统的网络安全风险与防护研究[J].交通运输工程学报,2023,23(6):1025-1031.

[3]杨洪权.新形势下铁路关键信息基础设施安全保护工作建议[J].铁道通信信号,2024,60(11). 41-48.

[4]伍翔庭,黄正岱.列控系统中信息交互安全技术探讨[J].铁路通信信号工程技术,2024,20(1):38-43.

[5]汪升华.新形势下计算机通信网络安全防护策略[J].数字技术与应用，2022，40(07)：234-236.