

电力调度数据网的安全防护体系构建与实现

黎家成 张 庆 申 涛 刘铁磊

国网湖北省电力有限公司随州供电公司 湖北 随州 441300

摘 要：电力调度数据网是电网稳定运行的核心载体，面临内外网络攻击、设备漏洞、数据失安等多重风险，现有防护体系存在碎片化、智能化不足、老旧设备适配性差等问题。本文结合电力安全防护规范，构建分层、分区、分级的立体化安全防护体系，从网络、终端、数据多维度设计防护模块，搭建智能监测与应急响应机制。经测试验证，该体系可大幅提升攻击拦截率、缩短风险处置时长，全面强化调度数据网安全稳定性。

关键词：电力调度数据网；安全防护；体系构建；实现

引言：电力调度数据网承载核心调度业务，具备高实时性与不间断运行特征，其安全关乎电力系统生产安全。当前，电网智能化升级与网络攻击手段迭代，使传统碎片化防护难以应对新型威胁，设备老旧、监测滞后、应急薄弱等问题凸显。为契合电力监控系统安全防护标准，本文针对性分析调度数据网安全风险，系统构建立体化防护体系并落地实践，旨在为电网安全运维提供实操支撑。

1 电力调度数据网基础架构与安全风险分析

1.1 电力调度数据网总体架构

(1) 调度数据网层级划分与组网结构：采用国家-网调-省调-地调-县调五级分层结构，骨干层与接入层协同组网，骨干环网保障高可靠性，接入星型结构覆盖末端站点，双冗余链路提升容灾能力。(2) 核心业务传输数据类型与运行特征：承载 SCADA 实时数据、PMU 动态数据、电量计量信息及调度指令，具备高实时性（毫秒级响应）、高连续性（7×24 小时不间断）及强确定性（固定优先级队列调度）特征。(3) 网络设备、终端与通信链路组成体系：包含路由器、交换机、纵向加密装置、正反向隔离设备、工作站及 RTU/FTU 终端，通信链路以 SDH/MSTP 光传输为主，4G/5G 无线为备份，关键节点部署时间同步系统^[1]。

1.2 电力调度数据网安全防护规范与原则

(1) 国家电力监控系统安全防护相关标准规范：依据《电力监控系统安全防护规定》（发改委 27 号令）、《网络安全法》等，细化等保 2.0 三级要求，定期开展安全风险评估与等级保护测评。(2) “安全分区、网络专用、横向隔离、纵向认证”核心防护原则：生产控制大区与管理信息大区物理/逻辑隔离，横向部署

正向/反向隔离装置；纵向采用数字证书、IPsecVPN 加密认证，确保数据传输身份可信与完整性。(3) 调度数据网安全防护核心目标：保障电网调度指令的机密性、完整性、可用性，防止非授权访问与数据篡改，确保电力生产控制系统安全稳定运行。

1.3 网络安全风险与威胁分析

(1) 外部网络攻击、恶意入侵与病毒渗透风险：APT 攻击、DDoS 洪水攻击、勒索病毒通过边界漏洞或运维通道渗透，可能导致调度指令延迟或误发；供应链攻击通过第三方设备固件植入后门。(2) 内部设备漏洞、权限滥用与操作不规范风险：老旧设备存在未修复 CVE 漏洞，默认口令未修改；运维人员越权操作、违规外联 U 盘，或误配置路由策略引发网络风暴。(3) 数据传输篡改、泄露、丢失的安全隐患：明文传输的遥测遥信数据可能被中间人劫持篡改，历史数据库未加密存储存在泄露风险，链路故障时数据丢包影响电网状态感知。

1.4 现有安全防护体系存在的问题

(1) 防护手段碎片化，缺乏系统性层级防护架构：边界防火墙、IDS/IPS 等分散部署，策略未协同联动，缺乏全域态势感知平台，难以形成纵深防御闭环。(2) 老旧设备兼容性差，安全加固难度大：早期投运的交换机和 RTU 终端不支持 SM 系列国密算法，固件版本停止更新，打补丁可能影响实时业务稳定性。(3) 安全监测智能化不足，应急响应能力薄弱：主要依赖静态规则告警，对未知威胁检测率低；应急预案流程冗长，自动化处置工具缺失，安全事件平均识别时间长达数小时。

2 电力调度数据网安全防护体系构建设计

2.1 防护体系总体设计思路与架构

(1) 体系设计的总体目标与设计原则: 以“实战化、体系化、常态化”为目标, 坚持动态防御与纵深防御结合, 兼顾安全性与业务实时性, 确保防护措施不引入显著时延, 同步遵循国产自主可控要求, 优先采用国密算法与可信计算技术。(2) 分层、分区、分级的立体化防护整体架构: 纵向划分骨干层、汇聚层、接入层三层防护域, 横向生产控制大区与管理信息大区隔离, 按业务重要性与风险等级设定 I 级(核心调度)、II 级(重要站点)、III 级(一般站点)差异化安全策略, 形成“纵向分层拦截、横向分区隔离、按级精准管控”的立体矩阵架构^[2]。(3) 技术、管理、运维一体化防护体系框架: 技术层部署边界防护、入侵检测、加密认证等工具链; 管理层建立安全责任矩阵、配置变更审批、第三方接入审查制度; 运维层构建资产台账数字化、漏洞闭环管理、安全运维审计三位一体机制, 三轴联动形成持续改进的安全生态。

2.2 网络层安全防护模块设计

(1) 安全分区优化与网络专用隔离方案设计: 将调度数据网划分为实时子网(承载 SCADA/PMU)与非实时子网(承载电量计量/故障录波), 采用 MPLSVPN 实现逻辑隔离; 管理信息大区与生产控制大区之间部署单向光闸, 确保物理级数据流向可控, 杜绝反向通道。(2) 横向物理隔离、防火墙策略配置与访问控制设计: 边界处部署工业级防火墙, 执行“白名单”策略——仅允许预先定义的 IP、端口及协议通过; 跨区数据交换经正反向隔离装置摆渡, 所有访问行为启用深度包检测, 阻断异常应用层指令, 策略更新周期不大于 30 天。(3) 纵向加密认证隧道搭建与通信链路安全防护: 省一地一县三级纵向链路部署国家认证的纵向加密装置, 采用 SM2/SM3/SM4 国密算法建立 IPsecVPN 隧道, 实现数据加密与完整性校验; 主备链路毫秒级切换, 通信链路实时监测误码率和时延, 异常时自动降级至备份无线通道并上报告警。

2.3 系统与终端层安全防护模块设计

(1) 调度主机、服务器操作系统安全加固方案: 对 Linux/Windows 服务器执行安全基线加固——关闭非必要端口与服务, 启用强制访问控制(SELinux/AppArmor), 部署主机防火墙和入侵检测代理, 定期进行系统漏洞扫描与补丁自动化验证, 补丁更新前经仿真环境测试。(2) 终端准入控制、权限分级与账号安全管理设计: 采用基于 802.1x 的终端网络准入, 对接入工作站进行 MAC+ 数字证书双因子认证; 权限按

“三权分立”原则划分为系统管理员、安全管理员、审计管理员, 账号启用强密码策略(长度 ≥ 12 位、含特殊字符)及 90 天强制更换, 离职账号实时注销^[3]。(3) 老旧设备适配改造与安全漏洞修复机制: 针对十年以上投运的 RTU、老式交换机组, 采用前置安全网关进行协议代理透传, 屏蔽底层漏洞; 对无法升级固件的设备纳入重点监控清单, 通过外挂式轻量级入侵检测探针实施流量镜像分析, 漏洞修复采用虚拟补丁技术(如 WAF 规则拦截)过渡, 同步制定三年替换计划。

2.4 数据与应用层安全防护模块设计

(1) 调度业务数据传输加密、完整性校验方案: 实时数据流采用 SM4-GCM 模式加密传输, 配合 SM3-HMAC 确保数据完整性; 关键指令报文附加数字签名, 接收端验签通过后方可执行, 所有加密操作由硬件密码机承载, 保障加解密性能满足毫秒级要求。(2) 敏感数据脱敏、存储安全与备份恢复策略: 历史数据库中的用户身份信息、操作日志等敏感字段进行动态脱敏显示, 存储层采用透明数据加密(TDE); 全量数据每日增备、每周全备, 备份存储于异地容灾中心, 定期开展数据恢复演练, $RPO \leq 15$ 分钟, $RTO \leq 2$ 小时。(3) 业务应用系统安全审计与防篡改机制: 调度自动化系统等关键应用启用操作审计日志(记录用户、时间、操作类型及结果), 日志存储周期 ≥ 6 个月且不可删除; 部署文件完整性监控, 对应用程序二进制文件、配置文件进行实时哈希比对, 发现篡改立即阻断进程并触发应急响应流程^[4]。

3 电力调度数据网安全防护体系实现与效果验证

3.1 防护体系软硬件部署实现

(1) 安全防护设备选型与网络拓扑部署实施: 依据三级调度架构差异化选型, 省级骨干部署万兆级工业防火墙、纵向加密网关及正反向隔离装置, 地县接入层部署千兆级综合安全网关。拓扑采用双设备热备+双链路冗余, 核心节点经 SDH 环网互连, 接入层星型上联, 关键链路设光旁路保护, 确保设备故障时业务无感知切换。(2) 加密认证、隔离防护系统的配置与调试: 纵向加密装置完成 IKE 策略配置、证书导入及 IPsec 隧道协商, 建立省一地一县三级加密隧道矩阵; 横向隔离装置配置单向摆渡策略, 仅允许特定格式实时遥测数据通过; 防火墙遵循最小权限原则, 逐条下发四元组过滤规则, 调试时以全流量回放验证策略, 确认后分批割接上线。(3) 安全防护软件平台、日志审计系统搭建实现: 部署集中安全管理平台, 统一管理防火墙、加密装置、IDS 等 30 余类设备; 搭建日志审计集群(Elastic-

search+Logstash+Kibana), 日均处理 50GB 日志, 原始日志保留不少于 180 天, 支持多维关联检索与合规报表自动生成。

3.2 智能安全监测与应急响应机制实现

(1) 安全态势感知平台数据采集与分析功能实现: 在骨干节点部署流量探针, 采集 NetFlow、SNMP、Syslog 多源数据, 经预处理后送入分析引擎; 基于历史流量基线构建动态行为模型, 运用统计异常检测与轻量级聚类算法, 实现对突发流量、异常连接、协议违规的实时感知, 综合风险评分在大屏端可视化呈现。(2) 异常流量、入侵行为智能识别与预警机制: 构建“特征规则+行为基线”双引擎检测架构, 特征库覆盖已知攻击类型 5000 余种, 行为分析针对慢速扫描、隐蔽隧道、畸形报文等未知威胁; 告警分级为红橙黄三级, 分别对应立即处置、15 分钟核实、30 分钟关注, 通过短信、弹窗、声光三通道同步推送, 误报率控制在 5% 以内^[5]。(3) 网络安全事件分级处置与应急响应流程落地: 依据事件影响范围与危害程度制定四级分类标准, 明确每级对应的启动条件、指挥体系与处置措施; 编制标准作业指导书, 涵盖断网隔离、数据取证、系统恢复、溯源分析等关键环节的操作细则, 每半年组织实战演练, 确保事件响应及时率 $\geq 95\%$ 。

3.3 防护体系测试与效果分析

(1) 网络渗透测试、漏洞扫描与安全性能测试: 邀请第三方团队开展内外网双视角渗透测试, 模拟 APT 攻击、中间人劫持、DDoS 等攻击场景 56 项; 使用专业漏洞扫描工具对全部在线设备进行基线核查, 同时测试加密隧道吞吐量、新建连接速率及极端负载下的设备资源占用情况。(2) 防护前后网络安全风险对比分析: 部署后外部攻击拦截率由 58.6% 提升至 98.7%, 高危漏洞数量由 41 个下降至 2 个, 违规外联事件清零; 安全事件平均发现时间由 3.8 小时缩短至 6 分钟, 各项指标符合《电力监控系统安全防护评估规范》要求。(3) 体系运行稳定性、安全性与实用性验证: 连续运行 90 天, 核心安全设备零故障、零重启, CPU 负载峰值 $\leq 60\%$, 加密处理对调度指令时延增量为 0.8~1.5ms; 运维人员通过统一平台

完成 95% 日常安全操作, 经满意度测评达 4.7/5.0 分。

3.4 体系运行优化与运维保障策略

(1) 定期安全巡检、漏洞更新与策略优化机制: 执行双周巡检制度, 检查设备运行状态、日志异常与策略命中率; 每月同步 CNNVD 漏洞库并评估影响, 季度开展策略精简优化, 清理冗余规则保持防火墙性能最优。(2) 人员安全培训、管理制度与运维规范完善: 每年组织全员安全专项培训 (不少于 24 学时), 覆盖钓鱼攻击识别、口令管理、应急上报等内容; 修订《调度数据网运维操作规范》, 明确双人操作、全程录屏、审批授权等硬性要求。(3) 常态化安全防护升级与长效保障方案: 建立年度滚动规划机制, 每 24 个月评估并升级关键设备固件, 跟踪零信任、可信计算等新技术适用性; 与上级应急中心签订联动协议, 实现威胁情报共享与技术支持, 确保持续演进能力。

结束语

本文完成了电力调度数据网安全防护体系的架构设计、模块搭建与落地实现, 有效解决了传统防护体系碎片化、智能化不足等痛点, 显著提升了电网调度网络的抗攻击能力与风险处置效率。体系兼顾安全性与业务实时性, 适配各级调度网络运行需求。后续将持续跟进网络安全新技术, 常态化开展设备升级、策略优化与人员培训, 持续完善长效运维机制, 实现调度数据网安全防护的动态迭代与长效稳固。

参考文献

- [1] 赵晨, 王浩. 智能调度数据网动态安全防护技术体系研究 [J]. 电网技术, 2023, 47(11): 361-369.
- [2] 周宇轩. 电力调度数据网网络安全隐患排查与防护体系优化实现 [J]. 电工技术, 2025, 11(10): 132-135.
- [3] 凌根. 电力调度数据网络传输安全策略与防护体系构建 [J]. 数字通信世界, 2023, 19(05): 170-172.
- [4] 吴迪. 基于等保 2.0 的电力调度数据网安全防护体系建设 [J]. 信息技术, 2024, 48(06): 89-94.
- [5] 郑凯. 电力调度自动化数据网主动安全防护体系设计与实现 [J]. 工程技术研究, 2024, 9(18): 102-104.