变电站监控系统常见网络安全隐患及整改防护措施研究

邓燚，高飞，李洪池
南京国电南自电网自动化有限公司，江苏 南京 211106
DOI:10.61369/RSTD.2026030003

摘　　要： 本文主要围绕变电站监控系统网络安全展开，深入剖析该系统的架构以及相关特性，明确指出它面临着外部攻击、内部管理存在漏洞、架构设备有缺陷还有数据传输存储方面风险等诸多隐患。在此基础上，提出进行防火墙部署、做好入侵检测防御、强化内部管理工作、优化架构设备情况、保障数据安全传输存储等整改防护措施，并且经过实践验证这些措施有效提升了系统的安全性。

关 键 词： 变电站；监控系统；网络安全；整改防护；措施

Research on Common Network Security Risks and Rectification and Protective Measures in Substation Monitoring Systems

Deng Yi, Gao Fei, Li Hongchi
Nanjing SAC Power Grid Automation Co., Ltd., Nanjing , Jiangsu 211106

Abstract: This article mainly focuses on the network security of the substation monitoring system. It deeply analyzes the architecture and related characteristics of the system, and clearly points out that it faces many hidden dangers such as external attacks, internal management vulnerabilities, architectural equipment defects, and data transmission and storage risks. On this basis, rectification and protection measures such as firewall deployment, intrusion detection and defense, strengthening internal management, optimizing infrastructure equipment, and ensuring safe data transmission and storage are proposed. These measures have been proven in practice to effectively improve the security of the system.

Keywords: substation; monitoring system; network security; rectification and protection; measures

变电站监控系统属于电网的关键组成部分，伴随数字化不断发展其网络安全问题更突出，外部攻击手段呈现出多种多样的态势，内部管理存在着一些明显的漏洞，架构设备有着不同程度上的缺陷，数据传输和存储过程面临较大风险。因此，研究常见隐患及对应的整改措施，对保障电网安全稳定运行具有重要意义。

一、变电站监控系统架构与网络安全特性

（一）系统架构概述

变电站监控系统把分层分布式架构当作核心，构建起“感知－传输－处理－管控”一体化体系，保障电网实时监测与精准控制，其架构从下往上分为三层。感知层依靠智能终端、传感器以及摄像头，实时采集设备运行参数、环境数据和现场影像以实现设备状态全感知；网络层以工业以太网、光纤专网作为核心，搭建安全传输通道保障数据高效且可靠地传递至上层系统；应用层集成监控主机、SCADA 系统和管理平台，完成数据存储、分析决策、远程控制和可视化展示来支撑运维人员对变电站全方位管控。三层架构协同联动既满足电网运行实时性与稳定性需求，又为网络安全防护提供基础框架，各层级通过标准化接口衔接形成闭环管理体系以适配不同规模变电站运维需求[1]。系统架构如图1所示。

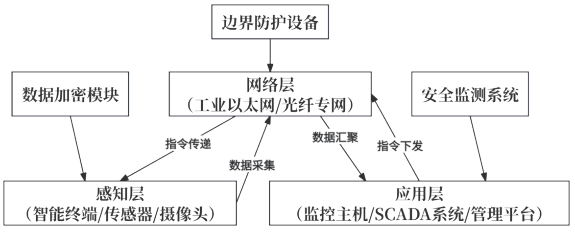


图1：变电站监控系统架构图

（二）网络安全特性

变电站监控系统的网络安全特性有着鲜明工业场景属性，核心围绕“实时性、可靠性、封闭性、合规性”这四大维度来构建。在实时性上，系统需要保障毫秒级的数据采集与指令传输工作，因为任何网络延迟和数据丢包都可能引发设备误动作，所以网络架构需采用工业级低延迟设备来确保关键业务优先传输，在可靠性方面，系统作为电网运行的核心支撑需要具备高可用性，

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

工业级硬件冗余设计和双链路备份机制是基础要求。同时，还需抵御断电、链路中断等突发故障以保障7×24小时稳定运行，封闭性体现为系统大多依托电力专网运行且与公网进行物理隔离，这大幅降低了外部攻击面，但内部设备间的通信需严格管控以避免横向渗透，合规性要求系统严格遵循电力行业网络安全标准，从设备接入、数据传输到存储的全流程都要落实安全防护要求，以此确保满足电网安全运行的监管规范，为系统抵御安全风险奠定基础[2]。

二、变电站监控系统常见网络安全隐患

（一）外部网络攻击风险

变电站监控系统身为电力关键信息基础设施，正面临着复杂的外部网络攻击威胁，伴随数字化转型加速推进，APT攻击、勒索软件入侵等新型攻击手段不断涌现，攻击者能够通过漏洞利用、协议伪造等方式渗透系统，如：基于TCP/IP协议的通信网络容易遭受IP窃听、假冒攻击。并且相关非安全通信协议存在被伪造、篡改及重放攻击的风险，恶意节点一旦入侵就可能造成电力系统大规模停电，APT攻击凭借隐蔽性强、持续时间长的特性，会长期潜伏于系统之中窃取数据或者破坏控制功能，严重威胁到电网的稳定运行。外部攻击所具有的复杂性与破坏性，让变电站监控系统面临着极高的安全风险，迫切需要构建具有针对性的防护体系。

（二）内部安全管理漏洞

内部安全管理漏洞是变电站监控系统网络安全隐患的核心根源，集中体现在责任落实、操作规范与人员意识这些层面，部分企业存在网络安全责任划分模糊的状况，问题整改闭环管理不严格且基础台账记录混乱，导致安全制度仅仅流于形式，运维人员操作存在不规范的情况，如：弱口令设置、违规外联以及未授权访问核心系统等，为外部入侵提供了可乘之机。同时，人员安全意识较为薄弱，对钓鱼邮件、恶意链接的识别能力明显不足，容易因误操作触发安全事件，此外权限管理方式比较粗放，未严格执行基于角色的访问控制，导致出现越权操作的风险，这些管理漏洞相互叠加起来形成系统性风险，需从制度、培训、监督等多维度强化内部管控[3]。

（三）网络架构与设备缺陷

变电站监控系统的网络架构和设备缺陷是引发网络安全隐患关键因素，部分系统网络架构设计存在不合理情况，有分区模糊以及边界隔离失效等诸多问题，未严格按照“安全分区、网络专用、横向隔离”防护原则执行，导致不同安全区域间发生数据非法流转现象，让攻击容易出现跨域扩散的状况。在设备层面，主机安全防护表现较为薄弱，未及时对安全补丁进行更新存在固件漏洞，网络设备配置存在不恰当的地方，如：交换机和路由器访问控制策略不够完善，没办法有效对非法流量进行拦截。此外，老旧设备兼容性比较差难以适配新型安全防护技术，部分设备还缺乏物理防护容易遭受人为破坏或电磁干扰，这进一步加剧了系统安全风险，这些架构和设备的固有缺陷使系统抗攻击能力不足，需要从架构优化和设备升级这两方面来进行整改。

（四）数据传输与存储安全风险

变电站监控系统的数据传输与存储风险，会直接对电力数据机密性完整性和可用性造成威胁。在数据传输的过程中，如果没有采用高强度的加密协议，电网拓扑、设备运行参数这类敏感数据就容易被拦截、窃取或者篡改，尤其是在公网或者非专用通道进行传输时，这些关键数据很容易成为攻击目标。传输链路如果缺乏可靠性保障，容易出现中断而导致数据丢失，进而影响到实时监控以及调度决策。在数据存储的环节中，如果缺失数据分级加密措施，并且敏感数据没有采用专用密钥进行管理的话，便存在数据泄露的风险，如果备份机制完善性不足，没有实现异地容灾备份的话，一旦遭遇火灾、设备故障等灾难情况，数据就会出现永久性丢失。存储介质如果缺乏物理防护和加密，在被非法窃取之后，其中数据就能够被直接获取[4]。

三、变电站监控系统常见网络安全整改防护措施

（一）网络安全防护技术应用

1. 防火墙部署

防火墙是变电站监控系统和外部网络的关键隔离屏障，需要按照系统业务逻辑与安全等级来精细化部署，它会制定严格的访问控制策略，只让合法合规的业务数据和控制指令在内外网之间流通，能有效阻断非法IP访问和恶意端口扫描等攻击行为。同时，防火墙可以实时监控网络流量，对异常访问行为进行告警并且拦截，防止外部威胁渗透到监控系统内部，守护生产控制区的安全边界以保障变电站设备远程控制和数据采集等核心业务稳定运行。

2. 入侵检测与防御系统

入侵检测与防御系统是变电站监控系统动态安全哨兵，它能够对网络流量以及系统操作进行实时监测与智能分析，此系统借助预设的攻击特征库精准识别病毒传播等入侵行为，异常协议攻击和非法操作都能识别出来，一旦识别到就第一时间触发告警并且自动阻断攻击链路，以此实现对威胁的主动防御。与此同时，IDPS还可以留存攻击日志，这能为后续安全溯源以及漏洞修复提供数据支撑，进而形成闭环安全管理机制，从而有效弥补防火墙被动防御方面的不足，最终全面提升监控系统对未知威胁和高级持续性攻击的抵御能力[5]。

（二）内部安全管理强化

在变电站监控系统网络安全整改工作中，和边界安全防护、设备漏洞修补等技术层面防护措施相比，强化内部安全管理十分重要。如果变电站监控系统内部出现人员操作不规范、安全制度落实不到位等问题，任何外部技术防护都很难完全规避安全风险，所以必须要从内部管理层面夯实基础。要构建“人员管控、制度执行、技术审计”相互协同支撑的三维防护体系，从人员资质、操作行为、制度落地、行为回溯等多个维度覆盖内部管理全流程环节，还要引入量化评估模型对各环节管理质量进行精准打分和精准把控，清晰掌握不同维度管理效能水平，及时发现管理

 Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.

短板并定向优化，以此确保内部安全管理能真正发挥兜底防护作用。以风险管控效能公式为例：

$$R=\frac{S\times(1+e^{-0.1T})}{1+0.2L}$$

其中 S 为人员安全培训覆盖率，T 为制度响应时效（小时），L 为违规操作频次。若整改前 $S=70\%$ 、$T=48h$ 、$L=15$ ，计算得 $R_1\approx4.2$ ；整改后人员培训全覆盖 $S=100\%$ 、制度响应缩至2小时 $T=2$ 、违规频次降至2次 $L=2$ ，算得 $R_2\approx7.6$ 。效能提升近81%，充分凸显强化内部管理对筑牢监控系统安全屏障的关键价值，为变电站稳定运行提供坚实保障[6]。

（三）网络架构与设备优化

变电站监控系统的网络架构和设备优化工作，要围绕拓扑结构、冗余设计以及设备性能升级来开展，构建起高可靠且低风险的网络体系，基于相关标准进行分层分区设计，把系统划分为过程层、间隔层、站控层安全区，通过防火墙和隔离装置实现区域隔离以防止风险扩散。同时，采用双中心交换机和双环路冗余配置，借助 VLAN 技术隔离流量从而降低广播风暴影响。在设备层面，核心交换机、路由器等硬件需要升级到高性能型号，关闭冗余服务并强化访问控制[7]。某变电站网络架构优化前后关键指标对比如表1所示。

表1：某变电站网络架构优化前后关键指标对比

指标	优化前	优化后
网络可用性	95%（单点故障易瘫痪）	99.9%（冗余保障稳定）
数据传输延迟	50ms（高峰拥堵）	≤15ms（流量精准管控）
安全漏洞数量	月均12个	月均2个（加固后减少）

（四）数据传输与存储安全保障

1. 数据安全传输机制

变电站监控系统要保障数据安全传输，应构建全链路加密与动态认证体系，采用国密 SM2/SM4 算法对实时遥测和遥控指令做端到端加密，结合 TLS1.3 协议搭建安全可靠的传输通道来阻断中间人攻击，引入动态令牌认证机制对操作人员身份进行二次核验，以此确保数据传输主体符合相关规定。同时，部署入侵检测系统（IDS）实时监测传输流量情况，自动拦截并对异常数据包进行告警处理。某省级电网在2023年升级传输机制之后，数据传输加密覆盖率从62%提升到了100%，传输中断率从每月0.8次降低到了0次且未发生数据泄露，保障了电网调度指令能够可靠传递，筑牢了变电站稳定运行的传输防线。

2. 数据安全存储方案

变电站监控数据存储要同时兼顾完整性和抗篡改能力，因此应全力构建多层级冗余存储架构。针对核心数据采用本地 SSD 阵列和异地灾备中心双活存储模式，并且依托 RAID6 技术来筑牢数据冗余存储的防线，这样就算遇到单盘故障数据也能保持稳定可用状态。同时，引入区块链技术对关键操作以及设备数据进行存证固化，从根本上杜绝数据被篡改的风险隐患。此外，搭建细粒度访问控制体系严格依照岗位进行精准权限赋予，全方位防范越权操作守护数据安全[8]。

四、结束语

总之，变电站监控系统作为电网非常关键的组成部分，其网络安全至关重要。本文深入剖析该系统面临外部攻击、内部管理漏洞、架构设备缺陷以及数据传输存储风险等各类隐患，并提出针对性的整改防护措施，通过实践证明这些措施有效提升了系统的安全性。未来，要持续强化网络安全防护技术的应用，优化网络架构与设备，加强内部的安全管理，构建全方位且多层次的防护体系以保障变电站安全稳定运行。

参考文献

[1] 方慧琴，闫卓武，石静 . 绿色低碳的变电站设备故障智能监控系统设计与实现 [J]. 现代工业经济和信息化 ,2025,15(12):128-130.

[2] 纪静 . 变电站监控系统的安全策略分析 [J]. 电子技术 ,2025,54(7):336-337.

[3] 刘娜 . 电力智能变电站中智能化技术的应用探究 [J]. 电工技术 ,2024,(S2):206-208.

[4] 李洪池，汤成俊，高飞 . 基于可信计算的变电站监控系统网络安全数据采集方法研究 [J]. 电工技术 ,2024,(18):152-155.

[5] 寇鹏伟，李彬，张吉祥，姚德振，孙运乾 . 数字变电站监控系统的安防措施分析 [J]. 电子技术 ,2023,52(3):154-155.

[6] 戴洋 . 浅析智能变电站监控系统网络安全渗透技术 [J]. 网络安全技术与应用 ,2023,(1):91-93.

[7] 赵中华，马莉 . 网络安全监测在变电站监控系统中的应用研究 [J]. 电工技术 ,2022,(16):130-133.

[8] 施畅，汤向华 . 变电站监控系统网络安全防护措施及方案 [J]. 农村电气化 ,2018,(7):5-7.

Copyright © This Work is Licensed under A Commons Attribution-Non Commercial 4.0 International License.