水电厂电力监控系统安全防护策略浅析

浦璐妮
金安桥水电站有限公司　云南　丽江　674100

摘　要：随着智能电网快速发展，水电厂电力监控系统作为电力生产核心环节，其安全稳定运行至关重要。当前，系统面临网络攻击、设备故障及人为误操作等多重安全威胁。为此，需从网络安全防护、设备安全管理、人员管理培训及应急响应机制等多维度制定防护策略。通过构建多层次防护体系，可有效提升系统抵御安全风险能力，保障水电厂电力供应的可靠性与稳定性，为电力行业安全运行提供有力支撑。

关键词：水电厂电力；监控系统；安全防护；策略

引言

在数字化与智能化深度融合的电力行业发展进程中，水电厂电力监控系统承担着实时监测、控制电力生产的关键职能。日益复杂的网络环境与系统自身复杂性，使该系统面临网络恶意攻击、设备老化故障、人员操作失误等安全隐患，严重威胁电力生产安全。本文基于对水电厂电力监控系统安全威胁的深入分析，针对性提出强化网络防护、设备管理、人员培训及应急响应等安全防护策略，旨在为保障电力监控系统安全稳定运行提供理论与实践参考。

1 水电厂电力监控系统概述

水电厂电力监控系统作为保障水电能源高效、安全、稳定生产的核心技术体系，通过分层分布式架构实现对水电厂生产过程的全面监测与精准控制。该系统涵盖厂站控制层与现地控制单元层，厂站控制层部署操作员工作站、工程师工作站及数据服务器等核心设备，承担系统数据处理、人机交互与高级应用功能；现地控制单元层则分布于水电厂各生产环节，包含机组现地控制单元、开关站现地控制单元等，实时采集水轮发电机组、变压器、断路器等设备运行参数，并执行控制指令。基于高速可靠的通信网络，水电厂电力监控系统将分布于全厂的智能电子设备进行互联互通，采用符合国际标准的通信协议实现数据的快速传输与交互。通过智能传感器与智能采集装置，系统能够实时获取机组振动、摆度、温度、流量以及电气量等海量数据，经数据处理模块的滤波、转换与分析，为运行人员提供直观准确的设备运行状态信息。借助先进的控制算法与策略，系统可自动调节水轮机导叶开度、励磁电流等关键参数，实现机组有功、无功功率的优化分配，确保机组在高效工况下稳定运行。水电厂电力监控系统集成故障诊断与预警功能，运用大数据分析与人工智能技术，对设备运行数据进行深度挖掘与趋势预测。一旦检测到异常数据或潜在故障征兆，系统立即触发报警机制，并通过可视化界面展示故障类型、位置及严重程度，辅助运行人员快速定位故障根源并采取有效处置措施。系统还具备完善的安全防护体系，通过身份认证、数据加密、访问控制等技术手段，保障电力监控系统免受网络攻击与非法入侵，维护水电厂生产运行的安全性与可靠性。

2 水电厂电力监控系统面临的安全威胁

2.1 网络攻击威胁

水电厂电力监控系统网络架构融合了工业控制网络与信息网络，这种复杂的网络环境为网络攻击提供了多样化的切入点。高级持续性威胁（APT）组织利用0day漏洞和定制化恶意软件，可长时间潜伏在系统中，通过隐蔽信道窃取核心控制参数与实时运行数据。例如，针对电力监控系统通信协议栈的漏洞攻击，攻击者能伪造合法设备身份，向可编程逻辑控制器（PLC）发送恶意控制指令，篡改水轮机导叶开度、调节闸门启闭时间，致使机组运行失稳，甚至引发连锁停机事故。随着工业物联网设备的广泛应用，智能电表、传感器等边缘设备的安全防护薄弱性逐渐凸显。攻击者可通过未加密的无线通信链路或弱认证机制，入侵这些设备并作为跳板，向监控系统核心网络渗透。网络钓鱼攻击借助精心构造的恶意邮件或虚假登录页面，诱使系统管理员或运维人员泄露账号密码，一旦凭证泄露，攻击者便能突破系统访问控制边界，直接操控关键业务流程。基于供应链的攻击也不容忽视，恶意篡改的设备固件或软件组件被植入系统后，可在特定条件下激活，造成系统功能异常或数据损毁。分布式拒绝服务（DDoS）攻击同样对电力监控系统构成严重威胁。攻击者控制大量僵尸网络，向监控系统服务器或关键通信节点发送海量无效请求，耗尽系统带宽与计算资源，导致SCADA（数据采集与监视控制系

统）平台无法正常接收和处理实时数据，使调度人员失去对水电厂运行状态的有效监控。针对工业协议的中间人攻击可拦截、篡改设备间的通信数据，破坏电力监控系统的完整性与可用性，干扰正常的功率调节与负荷分配，对电力生产安全构成直接威胁[1]。

2.2 设备安全威胁

水电厂电力监控系统包含大量专用设备，其硬件与软件的安全状况直接关系到系统运行可靠性。老旧的工控设备受限于设计年代的安全技术水平，存在诸多未修复的安全漏洞。例如，早期的PLC缺乏完善的访问控制机制，攻击者可通过串口或以太网接口直接上传恶意程序，修改设备控制逻辑。部分设备的硬件防护能力不足，容易受到电磁干扰或物理篡改，攻击者可利用探针技术读取存储在设备中的密钥信息，进而破解通信加密机制，窃取敏感数据。设备固件升级过程中的安全风险也不容忽视。由于电力监控系统对设备运行稳定性要求极高，部分单位延迟或忽略固件更新，导致设备长期暴露在已知漏洞风险下。即使进行升级，若未严格验证固件来源与完整性，也可能引入恶意代码。设备老化引发的故障会造成数据采集异常与控制失效，传感器的精度漂移会使监控系统获取错误的水位、流量等关键参数，影响调度决策；通信模块的性能下降则会导致数据传输延迟与丢包，破坏系统实时性要求。智能设备的引入虽然提升了系统智能化水平，但也带来新的安全挑战。物联网设备的资源受限特性导致其难以部署复杂的安全防护机制，弱密码、未授权访问等问题普遍存在。设备间的互操作性需求使得不同厂商的设备在通信协议和安全标准上存在差异，攻击者可利用这种差异实施协议欺骗攻击，干扰设备间的协同工作，破坏电力监控系统的整体稳定性与安全性。

2.3 人为操作威胁

人为操作失误是电力监控系统运行过程中不可忽视的安全风险因素。在水电厂复杂的运行环境下，监控系统操作界面信息呈现密度高、操作流程复杂，运维人员在长时间工作或高压力状态下，容易出现误操作。例如，在机组启停、负荷调节等关键操作环节，误输控制参数或错误触发操作指令，可能引发设备过载、系统振荡等严重后果。对新投运设备或升级后的系统功能不熟悉，也会导致操作失误，未能正确配置设备参数或启用新的安全防护功能，为系统运行埋下隐患。内部人员的恶意行为同样会对电力监控系统造成重大损害。掌握系统核心权限的管理员若存在不良动机，可利用职务之便绕过安全审计机制，非法修改系统配置、删除历史运行数据或泄露敏感信息。外部人员通过社会工程学手段获取内部人员信任，进而获取系统访问权限，实施恶意操作。缺乏有效的权限管理与操作审计，使得不当操作行为难以被及时发现和制止，增加了人为因素导致的安全事件发生概率。随着电力监控系统智能化程度提升，自动化操作流程逐渐增多，但人机协同机制不完善也带来新的风险。当自动化程序出现逻辑错误或遭遇异常工况时，运维人员若未能及时介入并采取正确处置措施，可能导致故障扩大。对自动化系统过度依赖，使得运维人员的操作技能与应急处理能力下降，在面对突发安全事件时，无法迅速准确地进行人工干预，影响系统的安全恢复能力[2]。

3 水电厂电力监控系统安全防护策略

3.1 强化网络安全防护

（1）构建多层次纵深防御体系，在水电厂电力监控系统网络边界部署高性能防火墙与入侵检测设备，形成严密防护屏障。防火墙依据预先设定的访问控制规则，精准识别并拦截非法网络流量，对进出网络的数据进行深度检测与过滤，阻断恶意攻击的渗透路径。入侵检测设备则实时监测网络中的异常行为与攻击迹象，通过对网络流量、用户行为等多维度数据的分析，及时发现潜在威胁，并触发相应的告警机制，为系统安全运行提供实时预警。（2）采用虚拟专用网络（VPN）技术建立安全加密通道，确保远程维护、数据传输过程中的信息安全。VPN利用加密算法对传输数据进行加密处理，即使数据在公网传输过程中被截取，攻击者也无法获取真实内容。通过严格的身份认证机制，只有经过授权的用户才能接入VPN网络，防止非法用户的入侵，保障远程访问的安全性与可控性。（3）对电力监控系统网络进行合理的子网划分与VLAN配置，实现网络隔离。将不同功能的设备与业务系统划分到不同子网，限制网络广播域的范围，降低网络攻击的扩散风险。各子网之间通过访问控制策略进行通信管理，仅允许必要的业务数据流通，有效减少网络攻击面，提升系统整体网络安全性。

3.2 加强设备安全管理

（1）建立完善的设备资产台账，对水电厂电力监控系统内的各类设备进行详细登记与管理。记录设备的型号、配置、安装位置、使用状态等关键信息，实时掌握设备全生命周期数据。通过定期的设备巡检与维护，及时发现设备运行过程中出现的硬件故障、软件漏洞等问题，并采取针对性的修复措施，确保设备稳定可靠运行。（2）对设备固件与软件进行及时更新与补丁修复，增强设备的安全防护能力。随着技术的发展与安全威胁

的演变，设备厂商会不断发布新的固件版本与安全补丁，修复已知的安全漏洞，提升设备性能。及时跟进并部署这些更新，能够有效抵御新型攻击手段，降低设备被入侵的风险，保障设备安全运行。（3）在设备接入电力监控系统网络前，进行严格的安全检测与准入控制。通过对设备的身份验证、安全配置检查、病毒查杀等操作，确保接入设备符合系统安全要求。只有通过安全检测的设备才能获得网络接入权限，防止携带恶意程序或存在安全隐患的设备接入系统，避免其对整个系统造成安全威胁[3]。

3.3 完善人员管理与培训

（1）对接触电力监控系统的人员进行严格的权限划分与访问控制。根据不同岗位的工作需求，赋予相应的操作权限，遵循最小权限原则，确保人员只能访问和操作其工作所需的系统资源。采用多因素身份认证方式，如用户名密码结合动态令牌、生物识别等技术，增强人员身份验证的准确性与安全性，防止非法用户冒用他人身份进行操作。（2）定期对系统操作人员进行专业技能培训，提升其对电力监控系统的操作水平与安全意识。培训内容涵盖系统操作规范、常见安全问题处理方法、新型攻击手段识别等方面。通过理论讲解与实际操作演练相结合的方式，使操作人员熟练掌握系统操作技能，能够及时发现并处理系统运行过程中出现的安全问题，有效降低人为操作失误带来的安全风险。（3）建立人员操作审计机制，对人员在电力监控系统中的操作行为进行全程记录与审计。审计日志详细记录操作人员的账号、操作时间、操作内容等信息，便于对操作行为进行追溯与分析。通过对审计日志的定期检查与分析，及时发现异常操作行为，如未经授权的访问、敏感数据的异常修改等，并采取相应的措施进行处理，确保人员操作的合规性与安全性。

3.4 建立应急响应机制

（1）制定完善的电力监控系统安全事件应急预案，明确各类安全事件的应急处理流程与责任分工。预案涵盖网络攻击、系统故障、数据泄露等多种可能发生的安全事件场景，针对不同场景制定详细的处理步骤与应对措施。明确应急响应团队各成员的职责与任务，确保在安全事件发生时，能够迅速、有序地开展应急处置工作。（2）定期对应急预案进行演练与评估，检验预案的可行性与有效性。通过模拟真实的安全事件场景，组织应急响应团队按照预案流程进行应急处置操作，发现预案中存在的问题与不足。演练结束后，对应急演练过程进行全面评估，总结经验教训，对预案进行修订与完善，确保预案能够适应不断变化的安全形势与实际需求。（3）建立安全事件快速响应通道与信息通报机制。当安全事件发生时，现场人员能够迅速通过快速响应通道向上级部门与应急响应团队报告事件情况，确保信息的及时传递。应急响应团队在接到报告后，能够快速启动应急处置流程，同时将事件信息通报给相关部门与人员，实现信息共享，协同开展应急处置工作，最大程度减少安全事件对电力监控系统造成的影响与损失[4]。

结语

综上所述，水电厂电力监控系统的安全防护需多管齐下，综合运用网络安全技术、设备全生命周期管理、人员素质提升及应急体系优化等策略。通过建立健全安全防护体系，可显著降低系统安全风险。随着电力行业技术革新，安全威胁也在不断演变。未来，还需持续关注新技术应用带来的新挑战，动态调整安全防护策略，确保水电厂电力监控系统始终处于安全、可靠的运行状态。

参考文献

[1]潘峰.水电厂电力监控系统安全防护策略浅析[J].中国新通信,2020,22(17):149-150.

[2]孙建强.水电厂电力监控系统安全防护策略浅析[J].大科技,2023(48):31-33.

[3]吴鹏.水电厂电力监控系统安全防护策略浅析[J].魅力中国,2021(47):430-431.

[4]刘中坚.水电厂电力监控系统安全防护策略研究[J].电子制作,2020(6):87-88,12.