 DOI: https://doi.org/10.12345/slkxyjs.v9i2.37154

Application of Computer Network Security Protection System in Hydropower Plant Centralized Control and Automation System

Huajun Li

Guangdong Hydropower Yunnan Investment Jinping Electric Power Co., Ltd., Honghe, Yunnan, 661500, China

Abstract

The centralized control automation system in hydropower plants plays a vital role in enhancing operational efficiency and remote management capabilities. However, it faces increasingly severe cybersecurity threats. This paper addresses the cybersecurity challenges of hydropower plant control systems by establishing a comprehensive security framework centered on network isolation, access control, intrusion detection, and data encryption. Through in-depth analysis of system architecture and attack patterns, the study proposes hierarchical and multi-dimensional security measures. The results demonstrate that this framework effectively mitigates common cyberattacks while improving system stability and security. The research findings provide theoretical support and practical references for cybersecurity infrastructure development in hydropower plants and similar industrial automation scenarios.

Keywords

hydropower plant; network security; centralized control automation; security protection system; intrusion detection

计算机网络安全防护体系在水电厂集控自动化系统中的应用

李华俊

广东水电云南投资金平电力有限公司，中国 · 云南 红河州 661500

摘　要

水电厂集控自动化系统在提升运行效率与远程管理能力方面发挥着重要作用，但面临日益严峻的网络安全威胁，本文围绕水电厂集控系统的网络安全问题，构建以网络隔离、访问控制、入侵检测和数据加密为核心的安全防护体系，研究基于对系统架构与攻击方式的深入分析，提出分层次、多维度的安全防护措施。结果显示该体系能有效防范常见网络攻击提升系统稳定性与安全性，研究成果为水电厂及类似工业自动化场景提供网络安全建设的理论支持与实践参考。

关键词

水电厂；网络安全；集控自动化；安全防护体系；入侵检测

1 引言

随着水电厂自动化水平的不断提升，集控系统在运行调度、远程监控和数据管理中发挥着核心作用，网络通信的高度集成使其在提升效率的同时也暴露出更多安全隐患，面临病毒攻击、非法入侵、数据泄露等多重威胁，严重影响系统的稳定性和运行安全，建立科学完善的网络安全防护体系已成为保障水电厂集控系统可靠运行的关键课题，本文结合系统特点与网络安全需求，探索针对性的防护策略，以提升整体网络防御能力和信息保障水平。

【作者简介】李华俊（1999–），男，中国云南红河州人，本科，助理工程师，从事水电厂集控自动化研究。

2 水电厂集控系统概述

2.1 系统结构

水电厂集控自动化系统是以计算机技术、网络通信技术和自动化控制技术为基础构建的综合性平台，主要由主控中心、现场设备层、通信网络层和远程监控终端组成，主控中心作为系统的核心，集中处理各类运行数据并完成调度与控制命令的下发。现场设备层包括传感器、执行器、可编程逻辑控制器等自动化装置，承担实时数据采集与执行控制任务。通信网络层实现各层之间的信息传输，采用工业以太网、光纤通道或专用通信协议进行连接，具备高可靠性和低延迟特性。远程监控终端可部署于调度中心或管理单位，实现跨区域监测与远程运维 [1]。整个结构具有分层清晰、功能互补、集成度高的特点，满足水电厂复杂工况下的运行需求与远程集成管理要求。

2.2 功能特点

水电厂集控系统具备集中控制与分布协同相结合的运行模式，能够完成实时监测、水位调节、设备启停、故障诊断和能效管理等关键功能，系统采用高精度传感技术与智能化数据处理算法，实现运行状态的精细感知和多维数据融合分析。根据人机界面展示运行工况与预警信息，辅助调度人员快速判断系统状态并作出调控决策 [2]。功能设计注重稳定性与可扩展性，既适应现有设备运行，又支持后续智能模块的接入与升级，系统在数据完整性、控制实时性和运行可靠性方面提出严格技术要求，并根据软硬件一体化设计实现高效协同，广泛满足水电站群远程集控、一体化调度与多能源协同运行的管理目标。

3 网络安全威胁分析

3.1 常见攻击方式

水电厂集控系统由于大量依赖网络通信与自动化控制设备，容易成为多种网络攻击的目标，在实际运行环境中攻击者可能利用系统开放端口、协议漏洞或身份认证薄弱环节发起拒绝服务攻击，使关键服务长时间瘫痪，导致自动控制指令无法正常传输，恶意代码注入是一种常见的手段，攻击者可在不被发现的情况下将木马或病毒植入控制系统内部，长时间潜伏并在特定时间触发控制指令的篡改或屏蔽，影响水电厂调度策略与运行逻辑的准确性。网络钓鱼与社交工程攻击手段也频繁出现在电力控制场景中，攻击者根据伪造邮件、操控管理终端或诱导操作人员下载非法软件，实现对内部系统的访问与数据窃取。高级持续性威胁表现为针对性极强的长期攻击过程，通常以目标系统为唯一攻击目标，依赖对网络拓扑、控制逻辑与数据流的深度研究进行潜伏并逐步控制关键节点，使攻击具备隐蔽性与不可预见性。此外，通信协议劫持与数据包中间人攻击也成为控制系统安全中的高频风险，这类攻击能够实现对指令内容的篡改、重放与伪造，进而改变设备运行逻辑或导致异常动作，影响系统整体安全态势 [3]。

3.2 安全风险点

水电厂集控系统在实际部署与运行过程中存在多个安全风险点，其中最关键的是系统架构设计中的信任边界不清以及防护机制不完善问题，通信链路长期处于持续运行状态，部分链路缺乏加密机制，使得数据传输过程中的敏感信息易被截获或篡改，操作系统与工业控制软件未及时更新补丁或使用过时版本，在未隔离的网络环境下极易被利用系统漏洞进行远程控制，此外远程维护接口作为运维支持手段，若缺乏严格的访问认证与行为审计措施，将可能被攻击者利用获取系统管理权限，从而绕过物理防线直接控制核心功能。访问控制策略若设计不当，如权限分级不清、账户管理混乱或缺少动态认证机制，也会导致非授权访问行为的频繁发生。对于设备层而言，嵌入式控制器或可编程逻辑设备普遍安全防护能力较弱，在未部署安全模块的情况下容易成为攻击的突破口。存储设备上的运行数据与控制记录若未实施加密与访问保护，面临泄露、篡改与恶意删除的风险，进而引发调度故障或运行误判 [4]。此外，缺乏统一的安全监测系统使得安全事件难以及时发现与定位，攻击行为在系统内部传播速度较快，威胁范围易扩大并造成系统级安全崩溃。整体而言水电厂集控系统的安全风险呈现结构复杂、边界模糊与攻击路径多样化等特点，必须从系统架构与运行机制层面进行全面审视与防护策略设计。

4 安全防护体系设计

4.1 网络隔离机制

水电厂集控自动化系统的网络隔离是保障其网络安全的基础环节，其核心在于构建分区明确、边界清晰的多层级网络结构，将控制系统、办公网络、远程接入网络与互联网进行有效物理或逻辑隔离，控制系统网络作为最关键的通信区域应处于最内层严禁与外部网络直接互联，采用工业防火墙进行边界访问管理并配合数据隔离装置阻断非授权的双向通信流，通信采用单向传输通道或专用协议转换网关，使外部只能接收特定数据流而无法向内部写入指令从架构上避免外部命令对核心系统的影响，在分区设计上将现场设备层与主控中心分设不同子网，并采用访问控制列表和虚拟局域网技术精细化控制不同网络节点之间的数据流动 [5]。办公网络仅允许访问经过授权的历史数据或中间数据，完全隔离实时控制指令和系统运行状态，远程维护网络必须部署在单独的安全区域并根据跳板服务器和双重身份验证实现安全接入，此外还需针对每个子网部署独立的入侵检测模块与日志分析系统，实现分区内部与边界之间的实时安全监测提高隔离策略的动态调整能力。

4.2 访问控制策略

访问控制策略是防止非授权操作与非法访问行为的重要手段，针对水电厂集控系统的多角色、多权限运行特点，需构建基于最小权限原则的动态访问控制体系，系统应采用多级权限划分模式，将运维人员、监控人员、管理人员及外部维护人员进行严格角色分离，并限定其在特定时间、特定网络、特定操作范围内的访问权限，身份认证机制应采用多因素认证方式，包括密码、智能卡、指纹识别或人脸识别等组合验证手段，降低单一认证方式被破解的风险，访问控制不仅应限制用户账户权限，还需控制终端设备的接入行为根据设备识别码与数字证书管理机制实现对终端身份与接入行为的可信验证。对关键操作如系统参数修改、远程启停命令或数据清除操作应设置多级审批与联合确认机制，避免单点权限引发重大安全事件，对于日常维护过程中的远程访问需求需启用跳板机制和专用 VPN 通道，并结合行为审计系统记录访问轨迹与操作日志实现全过程可追溯管理 [6]。在权限策略更新方面建立周期性审查机制，保障账户状态、角色

变更与权限边界始终与组织结构同步避免出现权限滥用或权限遗留问题。

4.3 入侵检测系统

入侵检测系统作为发现异常行为和防范攻击活动的重要组成部分，应全面部署于水电厂集控系统的关键网络节点与通信路径中，系统应采用基于网络特征分析与主机行为监测相结合的多维检测机制，从数据流、命令执行与系统状态等维度动态识别潜在攻击行为，网络层面可根据部署深度包检测引擎，对进出数据包的协议结构、访问频率、来源地址与访问路径进行实时分析，识别包括扫描探测、指令重放、异常流量等特征行为，主机层面则根据系统日志、进程调度与内存调用行为的智能比对，发现木马驻留、权限越权与异常操作痕迹。检测系统应具备自学习能力，基于历史行为建立正常通信基线，对偏离模型的数据触发告警并进行优先级分类。为提高系统响应能力入侵检测系统需与防火墙、身份认证与访问控制模块联动形成闭环响应机制，实现自动封锁、警报联动或恢复快照等操作防止攻击扩散。所有检测结果需统一归档至安全事件管理平台进行集中处理与分析，并提供图形化展示界面辅助安全管理人员进行态势研判与决策分析，在系统设计中需充分考虑检测系统对通信性能的影响，合理配置系统资源与响应策略以保障安全防护与系统实时性的平衡。

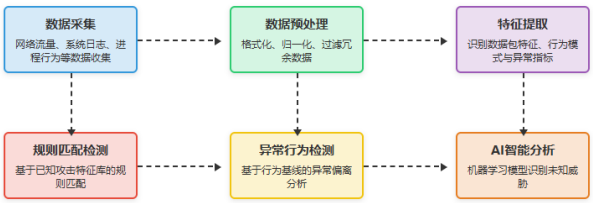

图 1 入侵检测系统工作原理图

4.4 数据安全保护

水电厂集控系统在运行过程中生成大量涉及调度逻辑、运行参数与历史操作记录的数据，其完整性与机密性直接关系到运行的安全性与管理的科学性，数据安全保护应覆盖数据的采集、传输、存储与访问全过程，构建端到端的加密与审计体系，在数据采集环节采集设备应部署加密芯片或嵌入式安全模块，对原始数据进行数字签名处理防止伪造与篡改，在传输过程中采用工业专用加密协议或基于 TLS 的安全通道对通信数据进行加密封装，有效防止中间人攻击与数据监听行为，对于存储环节应对关键数据文件实行分级分类加密，使用国密算法或高强度对称加密技术提高数据抗破解能力，重要配置文件与策略参数需设置访问锁并限定修改权限，访问数据的行为需经过统一认证授权平台调度，记录所有访问过程、操作时间、用户身份与数据类别形成完整的审计链条用于事后回溯与责任追踪，在数据备份策略上应采用定期全量备份与实时增量备份相结合的方法，将数据同步至异地灾备中心并进行周期性恢复演练验证备份有效性，为应对物理介质失效、勒索攻击或非授权删除，建议引入数据快照技术与只读防篡改存储介质，提高数据不可更改性与恢复灵活性。针对未来智能化管理需求，可将数据保护策略与人工智能算法结合，实现数据流动态识别与访问行为智能分析逐步构建具有自主防御能力的数据安全体系。

5 结论

构建完善的网络安全防护体系对于保障水电厂集控自动化系统的稳定运行具有重要意义，应从网络架构优化、访问权限细化、入侵行为识别与数据保护等多方面协同推进，不断提升系统的抗风险能力与智能防御水平，随着工业控制系统与信息技术的深度融合，网络威胁形态日趋复杂，安全体系需具备动态适应与持续演进能力为水电厂运行管理提供坚实的信息保障支撑。

参考文献

[1] 刘松林,吴礼贵,李光耀,等. 水电厂工控系统网络安全防护一体化平台探究[J].水电站机电技术,2024,47(12):50-52+74.

[2] 冯前. 桌面云系统在某水电厂信息网络中的应用实践[J].广西电业,2024,(06):12-17.

[3] 游伟民. 水电厂电力监控系统网络安全防护体系建设探析[J].网络安全和信息化,2024,(04):132-134.

[4] 赵亮. 水电厂电力监控系统的信息安全防护策略分析[J].集成电路应用,2024,41(01):332-334.

[5] 傅水祥. 华光潭水电厂电力监控系统网络安全防护建设研究[J].水电站机电技术,2023,46(10):42-44.

[6] 何战勇,段春晖,薛松,等.浅谈水电厂电能量系统网络安全防护的研究及应用[C]//中国水力发电工程学会自动化专业委员会.中国水力发电工程学会自动化专委会换届大会暨2023年全国水电厂智能化应用学术交流会论文集.华能澜沧江水电股份有限公司糯扎渡水电厂;,2023:89-91.