 DOI: https://doi.org/10.12345/bdai.v7i1.35264

Data Security Risks and Protection System Construction in the Digital Transformation of Hydropower Station

Xinglin Cao

Honghe Guangyuan Hydropower Development Co., Ltd., Yuxi, Yunnan, 653100, China

Abstract

During the digital transformation process, hydropower stations have extensively adopted information technology equipment and intelligent systems, significantly enhancing operational efficiency and management capabilities. However, data security challenges have become increasingly prominent. This study aims to ensure the security of hydropower station digital infrastructure by conducting systematic analysis across multiple dimensions, including cyber attack risks, internal data breaches, and system integration vulnerabilities. By examining current practical conditions, the research identifies root causes and establishes a comprehensive protection framework centered on network defense, access control, and secure operations. The findings demonstrate that implementing a multi-layered, multi-faceted data security mechanism can strengthen overall defense capabilities for hydropower stations. This approach holds practical significance and provides valuable guidance for promoting coordinated development of digitalization and security in the energy sector.

Keywords

hydropower station; digital transformation; data security; protection system

水电站数字化转型中的数据安全风险与防护体系构建

曹兴林

红河广源水电开发有限公司，中国·云南 玉溪 653100

摘　要

水电站在数字化转型过程中大量引入信息化设备与智能化系统，极大提升了运行效率与管理水平，但随之而来的数据安全问题日益突出。研究以保障水电站数字基础设施安全为目标，围绕网络攻击风险、内部数据泄露、系统融合漏洞等多个维度进行系统分析，结合当前实际情况探讨成因，并构建以网络防护、权限管理、安全运维为核心的防护体系。研究结果表明，建立分层次、多环节的数据安全机制，有助于增强水电站整体防御能力，对推动能源行业数字化与安全协同发展具有现实意义和指导价值。

关键词

水电站；数字化转型；数据安全；防护体系

1 引言

随着新一代信息技术在能源领域的深入应用，水电站正在加快数字化进程，实现设备自动化、系统智能化与运维信息化管理，推动生产效率与资源调度水平持续提升。在这一转型过程中，数据作为核心资源日益集中并高频交互，面临的安全威胁日趋复杂。网络攻击手段多样、内部管理疏漏以及系统深度集成等因素共同导致安全风险暴露点显著增加，一旦发生数据泄露或系统瘫痪，将直接影响水电站的安全稳定运行。构建科学有效的数据安全防护体系已成为水电站数字化转型的重要课题，对保障能源基础设施安全与推动数字中国建设具有重要意义。

【作者简介】曹兴林（1998–），男，中国云南华宁人，本科，助理工程师，从事水电站数字化转型中的数据安全风险与防护体系构建研究。

2 数据安全风险分析

2.1 网络攻击威胁类型

水电站在数字化过程中依赖于大量联网设备与实时信息系统，在开放网络环境下运行的关键基础设施更易成为攻击目标。攻击者常利用勒索软件植入业务服务器与控制终端，一旦核心系统被加密锁定，将导致设备无法远程控制与自动化指令执行受阻，严重干扰发电调度与运维作业。分布式拒绝服务攻击则通过大量伪造流量迅速耗尽网络带宽或系统资源，引发平台响应缓慢甚至瘫痪，进而影响数据采集传输与远程操作链路的稳定性。一些高级持续性威胁利用未知漏洞持续潜伏于系统内部，收集敏感信息或伺机干扰控制逻辑，其攻击具有目标性与隐蔽性，给传统防护手段带来极大挑战。水电站作为能源供应的重要节点，其网络安全

事件可能造成区域性电力系统波动，引发严重的社会与经济影响。

2.2 内部数据泄露隐患

水电站在日常运行中积累大量运行数据与设备参数信息，涉及调度指令、工况状态、维护记录等敏感内容，这些数据的存储与使用高度依赖信息化平台。在实际管理中，部分操作人员对信息安全规则理解不充分，可能存在弱密码使用、重复账号共享、外部存储设备随意接入等问题，这类操作行为为恶意代码或窃取程序植入提供路径。一些岗位缺乏合理权限划分，长期授权范围过大或未按职责及时回收账号，导致数据访问边界模糊，增加非授权泄露风险。在数据传输过程中，若缺乏加密通道或有效审计机制，信息易被中间环节监听截获。管理者与外部维护人员的行为缺少全流程记录，也易引发隐蔽型泄露行为。数据泄露不仅危及系统完整性，也可能为竞争者获取运行模式提供机会，影响水电站在行业中的战略地位。

2.3 系统集成带来的新风险

水电站的数字化建设涉及大量自动化控制系统、传感终端与管理平台的深度集成，IT 系统与 OT 系统的边界逐渐模糊，控制信号与运行数据在统一网络结构中频繁交互，这种融合模式打破了传统的封闭式安全架构。在未充分考虑隔离策略与协议兼容性的情况下，OT 系统容易因开放标准接口暴露给外部网络，从而引入潜在攻击路径。一些控制设备运行老旧，缺乏安全更新能力，与新型管理系统间的协议适配依赖中间件，这种中间转换层在设计上往往缺乏安全机制，使得攻击者可能借此切入控制域实施非法指令注入或参数篡改。此外，在系统升级过程中，业务连续性与数据完整性保障难度加大，版本不一致或配置残留易形成新的攻击面，进一步加剧安全管理的复杂程度。系统融合本身提升了运行效率与监测能力，但其带来的安全挑战需要从架构设计阶段就纳入整体防护策略，否则将成为数字化转型中的关键薄弱环节 [1]。

3 风险成因剖析

3.1 安全意识薄弱

水电站在加快数字化进程的同时，部分管理人员与一线操作人员对数据安全的理解仍停留在传统物理防护层面，对于信息系统安全管理的重视程度不高。在实际工作中，数据权限的管控依赖制度设定但缺乏执行反馈机制，操作流程存在形式化倾向，部分员工在日常作业中未对数据存储、传输和使用环节的敏感性形成明确认知。新技术引入后，系统功能复杂性提升，部分操作行为未及时进行培训规范，使得错误操作和配置疏漏频繁发生，增加安全事件发生的可能性。管理层对信息安全投入不足，在预算分配与项目规划中更多聚焦系统建设与业务功能提升，而忽视了数据保护与网络防护体系的同步建设，这种资源投入失衡导致整体安全能力滞后于系统复杂度上升的速度。员工安全培训不定期开展，考核机制缺乏实效，使得多数从业者在面对攻击行为时缺乏判断与处置能力，不利于在风险发生初期快速阻断事件传播路径，延长了安全响应的时间窗口。

3.2 防护机制不完善

水电站现有的数据安全防护体系在设计上多数延续传统封闭型架构，面对高度互联的运行环境缺乏动态适配能力。在网络边界方面，部分系统未部署细粒度的访问控制策略，缺少东西向流量的深度检测能力，使得一旦攻击者突破外围防线，便可在内网中自由横向移动。数据保护措施多停留在存储层面的权限设定，未在数据传输与处理链路中建立全生命周期的加密与追踪机制，导致信息在跨系统交互中易被窃取或篡改。权限管理存在层级模糊、授权过宽与审核缺失等问题，多个岗位间存在权限交叉与冗余，缺乏最小授权原则的有效落实，形成内部潜在风险点。日志记录与审计机制部署不完整，部分关键操作缺乏溯源能力，使得事后排查缺乏有效依据。针对应急响应的技术手段与组织机制不健全，缺少预案演练与动态更新策略，导致面对真实威胁时处置节奏混乱与协调效率低下。整体防护体系缺乏闭环管理，在面对持续演化的威胁场景中表现出脆弱性与滞后性 [2]。

3.3 第三方设备与服务隐患

在推动智能化管理过程中，水电站大量引入第三方设备与服务平台，包括远程监控系统、外包运维平台与边缘计算终端等，这些系统的接入极大丰富了数据采集能力与管理手段，但也带来了复杂多变的安全挑战。部分外部设备未经过统一的安全评估与兼容性测试便接入核心网络，其固件版本、协议配置与认证机制不透明，存在被远程利用或植入恶意代码的可能。外包服务在项目管理过程中缺乏统一的准入标准与行为监管机制，个别供应商在远程运维中存在管理账号共享、通信链路未加密或操作记录不完整等问题，这种服务链条上的薄弱环节容易成为攻击者的突破口。一些设备生产商未提供定期的安全补丁更新机制，长期运行中积累漏洞无法修复，形成风险堆积效应。对第三方系统缺乏统一的身份认证和权限隔离策略，使得其访问范围难以控制，与核心业务系统的边界管理失效，增加横向渗透风险。在采购与项目验收阶段，缺乏针对安全性能的系统性评估，使得部分技术方案在功能满足的同时忽略了潜在的安全隐患，难以在运行中实现高可靠性保障。

4 防护体系构建路径

4.1 网络边界安全防护

水电站信息系统的核心数据与控制指令均依托网络传输完成，网络边界成为外部攻击最易触及的入口。构建分层分域的网络防护体系，是提升整体安全性的关键措施。在网络架构设计上，应设立清晰的业务分区和安全域边界，将生产控制区、管理信息区与外部接入区进行物理隔离或逻辑隔

离，避免单点暴露引发连锁风险。部署多层防火墙与入侵检测系统对各安全域之间的访问行为进行精细化控制与实时监测，能够显著降低未授权通信与异常流量的渗透概率。以某大型水电站为例，其在实施三层防护体系后，日均可疑访问记录从原来的 2400 次下降至 820 次，恶意端口扫描行为数量减少至 200 次以内，说明边界隔离策略在阻断外部探测与试探方面成效显著。部分防护区域还引入深度包检测技术，对应用层流量进行语义识别，可有效识别异常命令注入或加密隧道通信行为，为安全事件溯源与处置提供了数据支撑。构建动态访问控制与白名单机制，在边界层面限定协议类型与通信方向，有助于阻断非授权访问链路，增强对外攻击面的控制能力 [3]。

4.2 数据访问与权限控制

在数据资源高度集中的数字化环境中，权限分配的合理性直接决定数据流转的安全性与透明度。应依据岗位职责与操作需求，建立清晰的分级授权体系，将数据访问权限划分为读取、编辑、传输、下载等多个层次，并结合岗位变动或职责调整动态更新授权策略。权限审计机制应覆盖全生命周期，包括账号创建、权限变更、登录行为与数据操作记录等，确保敏感数据在全流程中处于可控状态，表 1 是某西南水电企业的敏感数据访问统计表：

表 1：A 水电站 2024 年 7 月典型岗位敏感数据访问统计

岗位名称	授权访问数量（次）	实际访问数量（次）	超范围访问次数
值班工程师	460	440	3
运维主管	310	328	7
外包维护人员	125	211	22

（数据来源：A 水电站信息中心 2024 年 8 月内部报告）

该表显示，外包维护人员在授权访问 125 次的情况下，实际访问达 211 次，超范围访问 22 次，远高于其他岗位。在运维主管岗位中，虽授权为 310 次，但实际访问 328 次，存在 7 次越权行为。这说明部分岗位在未严格执行访问控制策略时存在隐性安全风险，尤其是外部人员管理缺乏实时监督与强制限制机制。针对这一问题，该水电站引入基于行为模型的权限动态调整策略，将访问异常行为与访问时间、频率、内容进行匹配，对超出常规范围的操作自动发出告警，并通过多因素认证拦截风险操作，超范围行为在一个月内下降至 5 次以内。

4.3 安全运维与应急响应

在数字化基础设施高度复杂的背景下，运维管理的安全性直接影响系统的连续性与稳定性。水电站应建立集成化安全运维平台，实现对终端设备、控制系统、数据链路与管理应用的统一监测和状态感知。构建主动检测与被动预警相结合的风险识别机制，通过关联分析模型识别出潜在异常行为，有助于提前介入风险环节。在某次针对 30 个重点节点设备的运行态扫描中，共识别出 57 个配置异常项，其中 17 项属于弱加密协议使用，9 项为默认口令未更改，其余为系统服务未及时更新等问题。在运维策略制定中，应强调最小干预原则与变更可追溯机制，将每一次配置变动纳入日志体系，并设立审批流与验证机制，降低人为操作误差的干扰。建立分级应急响应流程，将事件严重性划分为预警、告警与紧急三类，匹配不同的响应时效与处置策略，提升事发时的联动效率与控制能力，定期组织安全演练与风险通报，对历史事件进行复盘分析，是提升组织处置能力与安全文化建设的有效手段 [4]。

5 结语

水电站在数字化转型过程中面临多维度的数据安全挑战，网络攻击、内部泄露与系统融合带来的风险不断增多，对运行稳定性构成威胁。建立覆盖网络边界、权限控制与运维管理的多层防护体系，是提升系统安全性的关键路径。安全意识、机制完善程度以及对第三方环节的管理深度，共同决定数据安全水平的高低。构建以预防为主、响应高效的安全框架，能够有效降低安全事件发生概率，增强水电站数字系统的稳定性与可靠性，对推动能源行业高质量发展具有重要支撑作用。

参考文献

[1] 樊增,鄢立强. 新质生产力驱动下叶巴滩水电站人力资源数字化转型研究——基于TOE框架的分析[J].四川水力发电,2025,44(05):70-73.

[2] 肖楚生. 水电站机电设备智能运维系统的关键技术与应用展望[J].小水电,2025,(04):64-69.

[3] 徐册利,代荣艳. 数字化技术在水电站检修技改中的应用[J].低碳世界,2025,15(03):82-84.

[4] 秦金鹏. 以数字化转型为目标的水电运行班组管理方法[J].云南水力发电,2025,41(03):161-164.