水电站网络安全防护体系建设与风险评估

赵航航
大唐陕西发电有限公司水电事业部　陕西　安康　725200

摘　要：水电站作为关键基础设施，其网络安全至关重要。本文聚焦水电站网络安全防护体系建设与风险评估，首先概述水电站网络安全内涵与重要性；接着剖析面临的外部黑客攻击、内部人员不当操作及新技术应用等威胁；随后从物理隔离、设备部署、数据加密、监测感知、备份恢复、人员管理等方面构建防护体系；最后探讨风险评估方法与流程。旨在为水电站网络安全提供全面指导，提升其应对网络安全威胁的能力，保障水电站安全稳定运行。

关键词：水电站；网络安全；防护体系；风险评估

引言：在数字化浪潮席卷的当下，水电站作为国家能源体系的关键构成，其运行管理高度依赖网络信息系统。网络安全不仅关乎水电站自身的稳定运行、发电效率与经济效益，更与国家能源安全、社会正常秩序紧密相连。然而，随着网络技术的飞速发展，水电站面临的网络安全威胁日益复杂多样，外部黑客的恶意攻击、内部人员的违规操作以及新技术的潜在风险等，都给水电站网络安全带来巨大挑战。因此，构建科学有效的网络安全防护体系，并开展全面深入的风险评估，成为保障水电站安全运行的迫切需求。

1 水电站网络安全的概述

水电站作为国家能源体系的关键基础设施，承担着发电、防洪、灌溉等重要职能，其安全稳定运行关乎国计民生。在数字化、智能化发展趋势下，水电站广泛运用计算机网络技术实现设备监控、数据采集、远程调度等功能，极大提升了运行效率与管理水平。水电站网络安全是指通过采取一系列技术、管理和措施，保障水电站网络系统的硬件、软件及数据不受偶然或恶意原因的破坏、更改和泄露，确保网络服务的连续性和可靠性。它涵盖了多个层面，从物理层面的设备安全防护，到网络层面的通信加密与访问控制，再到应用层面的软件安全与数据完整性保护。水电站网络安全具有特殊性，其网络系统不仅连接着内部众多生产控制设备，还可能与外部电网、上级调度中心等进行数据交互，一旦遭受攻击，可能导致设备故障、数据丢失、调度失控等严重后果，甚至影响整个电力系统的稳定运行。因此，加强水电站网络安全防护，构建完善的网络安全体系，是保障水电站安全、稳定、高效运行的重要前提[1]。

2 水电站网络安全面临的威胁

2.1 外部黑客攻击

外部黑客为达非法目的，常将水电站网络系统作为攻击目标。他们凭借精湛技术，利用系统漏洞、弱口令等，试图突破网络防线。一旦成功入侵，可能篡改控制指令，使水电站设备运行异常，影响发电效率与稳定性；还能窃取关键数据，如设备参数、运行日志等，这些数据若被恶意利用，会给水电站带来难以估量的损失。而且黑客攻击手段不断翻新，从传统的病毒、木马攻击，到高级持续性威胁（APT）攻击，让水电站网络安全防护面临巨大挑战。

2.2 内部人员不当操作

内部人员因对系统熟悉，其不当操作对水电站网络安全威胁不容小觑。部分人员安全意识淡薄，违规使用移动存储设备，可能将外部病毒、恶意软件引入内部网络；在操作设备时，不遵循规范流程，误删除重要文件、错误配置参数，导致系统故障或数据丢失；还有个别人员为谋取私利，故意泄露敏感信息，破坏系统安全策略，给水电站网络安全埋下严重隐患，影响其正常运行与数据安全。

2.3 新技术应用风险

随着科技发展，新技术不断应用于水电站，如物联网、大数据、人工智能等。这些新技术虽带来诸多便利与效率提升，但也带来新风险。物联网设备数量众多、分布广泛，其安全防护能力参差不齐，易成为攻击入口；大数据汇聚了大量水电站运行数据，数据泄露风险增加；人工智能算法若被恶意攻击或数据被篡改，可能导致决策失误。而且新技术更新换代快，安全标准与规范相对滞后，使得水电站在应用新技术时面临更多不确定的安全威胁[2]。

3 水电站网络安全防护体系建设

3.1 物理隔离与访问控制

物理隔离是水电站网络安全的基础防线。通过将关键网络区域，如生产控制大区与管理信息大区进行物理

分隔，能有效阻止外部网络直接接入核心系统，降低外部攻击风险。例如，采用独立的网络线路、专用设备，确保不同区域间无直接物理连接。同时，严格的访问控制至关重要。在水电站各网络边界设置访问控制设备，依据预设规则，对进出网络的流量进行筛选，仅允许授权的IP地址、端口和协议通过。对进入水电站的人员，实施身份认证与权限管理，不同岗位人员分配不同访问权限，仅能访问其工作所需资源。物理隔离与访问控制相结合，从物理层面和访问层面构建起坚固屏障，防止非法访问和恶意入侵，保障水电站网络系统的物理安全与访问安全，为网络安全防护奠定坚实基础。

3.2 安全防护设备部署

安全防护设备是水电站网络安全的关键保障。防火墙作为第一道防线，部署在网络边界，依据安全策略过滤进出网络的流量，阻止非法访问和恶意攻击。入侵检测系统（IDS）与入侵防御系统（IPS）实时监测网络流量，及时发现并阻断异常行为和攻击活动。防病毒软件安装在各类终端设备上，定期更新病毒库，防范病毒、木马等恶意软件感染。此外，还可部署漏洞扫描设备，定期对网络系统和设备进行漏洞扫描，及时发现并修复安全漏洞。加密设备对重要数据进行加密处理，确保数据在传输和存储过程中的保密性。这些安全防护设备各司其职、协同工作，形成多层次、全方位的安全防护体系，有效抵御各类网络安全威胁，保障水电站网络系统的安全稳定运行。

3.3 数据加密与传输安全

数据是水电站运行的核心资产，保障数据加密与传输安全至关重要。数据加密技术通过对数据进行加密处理，将明文转换为密文，即使数据在传输或存储过程中被窃取，攻击者也无法获取其真实内容。对于水电站的关键数据，如设备运行参数、控制指令等，应采用高强度的加密算法进行加密。在数据传输方面，采用安全的传输协议，如SSL/TLS协议，为数据传输提供加密通道，确保数据在网络传输过程中的保密性和完整性。同时，对数据传输的源和目的地进行身份认证，防止数据被篡改或伪造。此外，还应建立数据访问控制机制，对数据的访问进行严格授权，只有经过授权的人员才能访问和解密数据。通过数据加密与传输安全措施，有效保护水电站数据的安全，防止数据泄露和恶意攻击。

3.4 安全监测与态势感知

安全监测与态势感知是水电站网络安全的重要环节。安全监测系统实时收集网络流量、设备状态、系统日志等安全相关信息，通过分析这些数据，及时发现潜在的安全威胁和异常行为。利用大数据分析、机器学习等技术，对海量安全数据进行深度挖掘和分析，识别攻击模式和趋势，提前预警可能发生的安全事件。态势感知平台将安全监测数据与业务信息相结合，从整体上把握水电站网络的安全状况，直观展示安全态势。通过可视化技术，将安全态势以图表、地图等形式呈现，使管理人员能够快速了解网络安全状况，及时做出决策。安全监测与态势感知能够帮助水电站及时发现和处理安全威胁，提高安全防护的及时性和有效性，保障网络系统的安全稳定运行。

3.5 备份与恢复机制

备份与恢复机制是水电站网络安全的重要保障措施。为防止数据丢失和系统瘫痪，应建立完善的数据备份策略。定期对水电站的重要数据进行备份，包括设备运行数据、系统配置数据、业务数据等。备份方式可采用全量备份、增量备份和差异备份相结合的方式，以提高备份效率和减少存储空间占用。同时，将备份数据存储在安全可靠的位置，如异地数据中心或磁带库等，防止因本地灾难导致数据丢失。在系统出现故障或遭受攻击后，能够快速进行恢复。制定详细的系统恢复流程和应急预案，定期进行恢复演练，确保在紧急情况下能够迅速、有效地恢复系统和数据。通过备份与恢复机制，最大程度减少数据丢失和系统停机时间，保障水电站网络系统的连续性和可用性。

3.6 人员培训与管理

人员是水电站网络安全的关键因素，加强人员培训与管理至关重要。定期组织网络安全培训，提高员工的网络安全意识和技能水平。培训内容包括网络安全基础知识、安全操作规范、应急处理流程等，使员工了解网络安全的重要性，掌握基本的安全防护技能。建立严格的人员管理制度，对员工的网络访问行为进行规范和监督。限制员工对敏感数据的访问权限，实行最小权限原则，确保员工只能访问其工作所需的信息。同时，加强对离职人员的安全管理，及时收回其访问权限和相关设备，防止信息泄露。此外，建立网络安全责任制度，明确各部门和人员的网络安全职责，对违反安全规定的行为进行严肃处理。通过人员培训与管理，提高员工的网络安全素质和责任意识，减少人为因素导致的安全风险[3]。

4 水电站网络安全风险评估

4.1 风险评估方法

（1）概率统计法。它通过收集过往网络安全事件的发生频率、损失程度等数据，运用概率论和数理统计知识，计算特定风险事件发生的概率及可能造成的损失。

这种方法以客观数据为支撑，能较为准确地量化风险，为风险评估提供科学依据。不过，其依赖充足且准确的历史数据，若数据缺失或不准确，会影响评估结果的可靠性。（2）主观评分法。专家根据自身对水电站网络系统、安全威胁等方面的了解，对各个风险因素进行打分，再综合这些分数确定整体风险水平。此方法操作相对简便，能在数据不足时发挥作用，可快速对风险有个大致判断。但评估结果受专家主观因素影响较大，不同专家可能给出不同评分，导致评估结果存在一定主观性和不确定性。（3）德尔菲法。组织者选取相关领域专家，以匿名方式向他们征求对风险的意见和看法，经过多轮反馈与汇总，使专家意见逐渐趋于一致，从而确定风险评估结果。该方法能充分利用专家的智慧和经验，避免个别专家意见的片面性，结果相对客观、全面。但过程较为繁琐、耗时较长，且对组织者的协调和沟通能力要求较高。

4.2 风险评估流程

(1)风险识别。它旨在全面、系统地找出可能影响水电站网络安全的各类风险因素。通过收集相关资料、开展调研访谈、分析系统架构等方式，识别出外部黑客攻击、内部人员误操作、设备故障、自然灾害等潜在风险源，以及这些风险源可能引发的安全事件，为后续的风险分析提供基础，确保不遗漏关键风险点。(2)风险分析。运用合适的方法，如定性分析判断风险的性质和影响程度，定量分析计算风险发生的概率和可能造成的损失。分析风险之间的相互关系和作用机制，确定风险的关键影响因素。通过风险分析，能更清晰地了解风险的本质和特征，为准确评价风险和制定处置措施提供科学依据，使风险评估更具针对性和有效性。(3)风险评价。风险评价是在风险分析的基础上，对水电站网络安全风险的整体水平进行评估和判断。依据预先设定的风险评价标准和指标体系，将风险分析结果与标准进行对比，确定风险的等级，如高、中、低风险。明确哪些风险需要优先处理，哪些风险可以暂时监控。风险评价结果能为水电站制定合理的安全策略和资源分配方案提供重要参考，保障网络安全防护工作的有序开展。(4)风险处置。风险处置是根据风险评价结果，针对不同等级的风险采取相应措施的过程。对于高风险，通常采取规避、降低或转移等策略，如加强安全防护设备部署、购买网络安全保险；对于中风险，可采取改进、监控等措施；对于低风险，进行常规监控即可。通过风险处置，能有效降低风险发生的可能性和影响程度，将水电站网络安全风险控制在可接受范围内，保障网络系统的安全稳定运行。(5)复查与更新。复查与更新是水电站网络安全风险评估的持续环节。随着时间推移、技术发展和环境变化，新的风险可能出现，原有风险的影响程度也可能改变。定期对风险评估结果进行复查，检查风险处置措施的实施效果，及时发现新的风险因素[4]。根据复查情况，更新风险评估文档和风险处置策略，确保风险评估始终与水电站网络安全实际状况相适应，持续提升网络安全防护能力。

结束语

水电站网络安全防护体系建设与风险评估是保障其稳定运行、维护能源安全的关键所在。构建完善的防护体系，从物理隔离到人员管理多管齐下，能为水电站网络筑牢坚实防线；科学的风险评估流程，精准识别、分析、评价并处置风险，可提前化解潜在威胁。然而，网络安全形势动态变化，新技术不断涌现，挑战也持续增加。未来，需持续优化防护体系，紧跟技术发展更新风险评估方法，不断提升水电站网络安全防护能力，以应对日益复杂的网络环境，为国家能源安全与经济社会发展提供可靠保障。

参考文献

[1]陈曦.智能化水电站监控系统网络安全问题与对策[J].水电站设计,2022(01):24-28+42.

[2]孔德明.水电站控制系统网络安全现状及探究[J].市场周刊:商务营销,2020,(059):134

[3]李黎,靳帅.电力监控机房安全监测系统在枕头坝水电站的建设与应用[J].现代工业经济和信息化,2021,11(11):269-270+274.

[4]谢秋华,杨廷勇,杨云等.主动免疫的水电站电力监控系统网络安全防护方案设计[J].水电站机电技术,2021(08):13-16+120.