水利信息化网络安全防护体系

朱　林　沈汝潮　叶建国　周祖乾　蒙永务
珠江水利委员会西江局西江水利综合技术中心　广西　南宁　530007

摘　要：水利信息化在提升水资源管理效率的同时，也面临严峻网络安全挑战。本文聚焦水利信息化网络安全防护体系构建，阐述其遵循综合性、风险管理、可靠性、可扩展性及动态适应性等原则，详细介绍涵盖物理层、网络层、应用层、数据层与管理层的多层架构，并深入探讨动态威胁情报、人工智能与机器学习、区块链、零信任架构等关键技术，旨在为水利信息化网络安全防护提供全面、系统的理论支撑与实践指导，保障水利信息系统的安全稳定运行。

关键词：水利信息化；网络安全防护体系；多层架构；关键技术

引言：随着信息技术的飞速发展，水利信息化进程不断加快，各类水利信息系统在防汛抗旱、水资源调配、水生态保护等方面发挥着关键作用。然而，网络空间的开放性与复杂性，使水利信息化系统面临诸多安全威胁，如黑客攻击、数据泄露、恶意软件感染等，严重威胁水利业务正常开展与国家水安全。构建科学有效的网络安全防护体系，成为水利信息化建设的紧迫任务。文章旨在深入剖析水利信息化网络安全防护体系的构建原则、架构及关键技术，为提升水利信息化网络安全防护能力提供有益参考。

1 水利信息化网络安全防护体系构建原则

1.1 综合性原则

水利信息化网络安全防护需秉持综合性原则，从多层面、多角度构建防护体系。涵盖物理层对设备与环境的保障，网络层对数据传输与访问的管控，应用层对系统漏洞与操作行为的规范，数据层对数据存储与访问的加密，以及管理层对策略制定与人员管理的强化。各层面相互协作、紧密配合，形成全方位、立体化的防护网络，共同抵御各类网络安全威胁，保障水利信息化系统的稳定运行。

1.2 风险管理原则

风险管理原则要求全面识别水利信息化面临的各类安全风险，如网络攻击、数据泄露、设备故障等。对风险进行细致评估，分析其发生的可能性和影响程度。依据评估结果，合理分配资源，优先处理高风险问题。制定针对性的风险应对策略，如风险规避、降低、转移或接受。通过持续的风险监测与评估，动态调整防护措施，确保在风险发生时能够有效应对，将损失降至最低[1]。

1.3 可靠性原则

可靠性原则强调水利信息化网络安全防护体系必须具备高度的稳定性与可用性。选用质量可靠、经过严格测试的硬件设备和软件系统，确保其在长时间运行过程中不易出现故障。建立冗余备份机制，对关键数据和系统进行备份，当主系统出现问题时能够迅速切换至备用系统，保障业务的连续性。同时，具备完善的故障恢复能力，能在短时间内修复故障，恢复系统正常运行，减少因安全问题导致的业务中断时间。

1.4 可扩展性原则

随着水利信息化业务的不断发展和技术的持续更新，网络安全防护体系需具备良好的可扩展性。在设计架构时，要预留足够的扩展空间，便于后续增加新的安全防护模块、设备或功能。能够适应不断变化的网络环境和业务需求，如新增水利监测站点、拓展业务应用系统等，无需对现有防护体系进行大规模改造。通过灵活的扩展，确保防护体系始终能够满足水利信息化发展的安全需求，为业务的持续创新提供有力支撑。

2 水利信息化网络安全防护体系架构

2.1 物理层安全防护

(1)设备安全。要确保水利信息化所使用的各类硬件设备，如服务器、网络设备、存储设备等，具备高质量与高可靠性。选用经过严格检测认证的设备，防止因设备自身缺陷引发安全隐患。定期对设备进行巡检与维护，及时更换老化部件，保证设备稳定运行。同时，为设备配备不间断电源，防止因突然断电造成数据丢失或设备损坏，从硬件层面筑牢水利信息化安全防线。(2)环境安全。要为设备提供适宜的运行环境，建设专门的机房，确保机房具备合适的温度、湿度和洁净度。安装温湿度调节设备和空气净化装置，避免设备因环境因素出现故障。配备防火、防水、防雷、防电磁干扰等设施，降低自然灾害和意外事件对设备的损害。加强机房的物理隔离，防止无关人员随意进入，减少人为破坏和干扰，保障设备安全稳定运行。(3)访问控制。在机房入

口设置门禁系统，采用刷卡、指纹识别、人脸识别等技术，限制人员进出，只有授权人员才能进入机房。对不同区域和设备设置不同访问权限，根据工作人员职责分配相应权限，防止越权访问。在设备操作层面，设置操作密码和权限管理，操作人员需输入正确密码并获得授权才能进行操作。通过多层次的访问控制，有效防止非法人员接触和操作水利信息化设备。

2.2 网络层安全防护

(1)防火墙与入侵防御。防火墙作为网络层安全防护的第一道防线，通过设定访问规则，严格管控进出网络的数据流，阻止非法访问和恶意攻击。它能依据预设策略，对不同来源和目标的数据包进行筛选，仅允许符合规则的通过。入侵防御系统则进一步增强防护能力，实时监测网络流量，主动识别并阻断正在进行的入侵行为，如恶意代码传播、端口扫描等。二者协同工作，有效抵御外部网络威胁，为水利信息化网络构建起坚固的安全屏障。(2)网络隔离与访问控制。网络隔离是将水利信息化网络划分为不同安全区域，如内部核心业务区、办公区、外部接入区等，通过物理或逻辑隔离手段，限制各区域间的随意访问，降低安全风险扩散的可能性。访问控制则基于用户身份、角色和权限，对网络资源访问进行精细管理。只有经过授权的用户，在满足特定条件下才能访问相应资源，防止非法用户获取敏感信息，确保网络资源的安全性和可用性。(3)数据传输加密。数据传输加密技术通过对传输的数据进行加密处理，将明文转换为密文，即使数据在传输途中被截获，攻击者也无法获取其真实内容。采用对称加密和非对称加密相结合的方式，在保证加密效率的同时，增强数据传输的安全性。同时，定期更新加密密钥，防止密钥泄露导致数据安全受损，保障水利数据在传输过程中的保密性和完整性。(4)网络监测与审计。通过网络监测工具，实时收集网络流量、设备状态等信息，及时发现网络异常行为，如流量突增、异常连接等。审计功能则对网络操作和访问行为进行详细记录，包括操作时间、操作人员、操作内容等。通过对监测和审计数据的分析，能够追溯安全事件源头，评估网络安全状况，为调整安全策略提供依据，及时发现并解决潜在安全隐患，确保水利信息化网络稳定运行[2]。

2.3 应用层安全防护

(1)代码审计与漏洞修复。代码审计是对水利信息化应用系统的源代码进行全面审查，以发现其中存在的安全漏洞、编码缺陷等问题。通过专业的审计工具和人工审查相结合，深入分析代码逻辑，识别可能被攻击者利用的薄弱环节。针对发现的问题，及时进行修复和优化，从源头上消除安全隐患，防止因代码漏洞引发的数据泄露、系统被入侵等安全事件，提升应用系统的安全性。(2)应用安全加固。应用安全加固是对水利信息化应用系统采取一系列增强安全性的措施。包括对应用系统的身份认证机制进行强化，采用多因素认证方式提高用户身份验证的可靠性；对访问控制策略进行优化，严格限制用户对系统资源的访问权限；对应用系统的输入输出进行严格过滤和验证，防止恶意代码注入。(3)安全审计与日志管理。安全审计对应用系统的操作行为、访问记录等进行全面审查，确保所有操作符合安全策略。日志管理则详细记录应用系统运行过程中的各类事件，包括用户登录、数据访问、系统异常等。通过对审计和日志数据的分析，能够及时发现潜在的安全威胁，追溯安全事件的发生过程，为安全事件的调查和处置提供有力依据。

2.4 数据层安全防护

(1)数据加密存储。在存储环节，运用先进的加密算法，如AES等，将水利数据转化为密文。无论是存储在本地服务器还是云端，未经授权者即便获取数据，也难以解读其真实内容。同时，合理管理加密密钥，采用密钥分层、分散存储等方式，防止密钥泄露。通过加密存储，有效防止数据在存储过程中被窃取或篡改，确保水利数据的保密性和完整性。(2)数据备份与恢复。定期对水利数据进行全面备份，可采用全量备份与增量备份相结合的方式，既保证数据的完整性，又提高备份效率。备份数据应存储在异地或隔离的环境中，防止因本地灾害或攻击导致数据全部丢失。当数据出现丢失或损坏时，能迅速启动恢复流程，依据备份数据将系统恢复到正常运行状态，保障水利业务的连续性。(3)数据访问控制。基于用户身份、角色和权限，为不同用户分配不同的数据访问级别。只有经过授权的用户，在满足特定条件下才能访问相应的数据资源。通过精细的访问控制，防止数据被非法访问和滥用，确保水利数据的安全使用。

2.5 管理层安全防护

(1)安全策略制定。需依据水利信息化业务特点和安全需求，制定全面且细致的安全策略，涵盖网络安全、数据安全、应用安全等各方面。明确安全目标、原则和规范，规定不同场景下的安全操作流程和责任分工。同时，定期评估和更新安全策略，以适应不断变化的网络环境和业务需求，确保其有效性和针对性，为水利信息化安全提供明确的指导方向。(2)人员培训与意识提升。开展定期的安全培训，内容涵盖安全知识、操作技能、

应急处理等方面，提升工作人员的安全素养。通过案例分析、模拟演练等形式，增强员工对安全威胁的识别和防范能力。同时，强化安全意识教育，让员工深刻认识到安全的重要性，自觉遵守安全规定，形成良好的安全习惯，从人员层面减少安全风险的发生。(3)应急响应与恢复。建立完善的应急响应机制，明确应急处置流程和责任分工，确保在安全事件发生时能够迅速响应。组建专业的应急团队，定期进行应急演练，提高团队的应急处理能力。同时，制定详细的恢复计划，包括数据恢复、系统重建等，确保在事件处理后能够快速恢复水利信息系统的正常运行，降低安全事件对业务的影响[3]。

3 水利信息化网络安全防护体系的关键技术

3.1 动态威胁情报技术

动态威胁情报技术是水利信息化网络安全防护的核心支撑。通过构建水利网络安全威胁情报中心，整合多源异构数据，实时采集全流量网络行为、恶意样本特征及攻击者画像等信息。利用大数据分析平台进行关联挖掘，可提前识别APT攻击、零日漏洞等新型威胁，并自动生成动态防御策略。例如，某省级水利单位通过部署威胁情报系统，成功阻断针对水库调度系统的定向攻击，将威胁发现时间从72小时缩短至15分钟，实现从被动防御向主动防御的转变。

3.2 人工智能与机器学习技术

人工智能与机器学习技术为水利网络安全提供智能化决策能力。基于深度学习的流量分析模型可识别异常通信模式，如某流域水文监测站通过部署AI驱动的入侵检测系统，利用LSTM算法分析传感器数据流，精准检测出针对SCADA系统的隐蔽攻击。机器学习技术还能优化安全运维效率，通过聚类分析自动归类海量告警信息，将误报率降低80%。在智慧防汛场景中，AI模型可结合气象数据与历史灾情，预测洪水演进路径，为应急调度提供科学依据。

3.3 区块链技术

区块链技术为水利数据安全构建可信存证体系。采用分布式账本技术记录数据全生命周期操作日志，确保水文监测数据、工程调度指令等核心信息的不可篡改性。某国家级水利枢纽通过区块链平台实现跨部门数据共享，利用智能合约自动执行水资源分配规则，将交易透明度提升90%。在设备管理领域，区块链可追溯PLC控制器、RTU终端等工控设备的供应链信息，防止预置后门攻击。结合国密算法SM2/SM4的加密传输，形成“数据可溯、访问可控、传输可信”的三维防护机制。

3.4 零信任架构

零信任架构重塑水利网络边界防护模式。通过实施“永不信任、始终验证”原则，对用户、设备、应用进行多维度身份认证。某省级水利云平台采用零信任网关，结合多因素认证（MFA）与持续行为分析，将横向移动攻击阻断率提升至95%。在远程运维场景中，基于SDP（软件定义边界）技术实现最小权限访问，确保工程师仅能操作授权范围内的泵站控制系统。结合微分段技术，将水利网络划分为200余个安全域，即使单个节点被攻破，攻击者也无法横向渗透至核心调度系统，显著提升整体安全韧性[4]。

结束语

水利信息化网络安全防护体系的构建，是保障水利事业稳健发展的关键基石。秉持综合性、风险管理、可靠性、可扩展性与动态适应性等原则，融合动态威胁情报、人工智能、区块链、零信任架构等关键技术，我们搭建起多层次、全方位的安全屏障。这不仅守护着水利数据的安全与完整，更确保了水利系统的高效稳定运行。未来，随着技术的持续革新与水利业务的不断拓展，我们将持续优化和完善防护体系，以更加智能、灵活、强大的安全能力，为水利信息化发展保驾护航，助力水利事业迈向更高水平的现代化征程。

参考文献

[1]李琳.水利信息化网络安全防护体系浅议[J].互联网周刊,2022(08):54-56.

[2]廖晓玉,高远,金思凡,刘媛媛.水利信息化网络安全防护体系浅议[J].中国防汛抗旱,2022,32(02):40-43+53.

[3]李丽.水利信息化网络安全防护体系浅议[J].山西水利,2021(12):25-29.

[4]赵慧,周红娟.水利信息化网络安全防护体系浅议[J].海河水利,2021(06):115-117+121.