水利工程信息化管理网络安全风险评估与防护体系构建研究

朱森森　张煜坤
中国南水北调集团中线有限公司渠首分公司　河南　南阳　473000

摘　要：在数字化时代，水利工程信息化管理关乎水利事业发展与社会公共安全，其网络安全至关重要且具独特挑战。需开展风险评估，精准识别、分析风险并选择合适评估方法。构建防护体系要遵循全面性等原则，从技术、管理、人员层面协同发力，采取综合防护措施，保障水利工程信息化管理系统安全稳定运行。

关键词：水利工程；信息化管理；网络安全风险评估；防护体系构建研究

引言：在数字化浪潮席卷之下，水利工程信息化管理成为水利事业发展的核心驱动力，其网络安全的重要性愈发凸显。水利工程关乎国计民生，一旦网络安全失守，造成数据泄露、系统瘫痪等后果，将不堪设想。同时，水利工程信息化管理网络具有覆盖广、系统多、数据敏感等特点，网络安全防护挑战巨大。为此，需精准开展网络安全风险评估，遵循科学构建原则搭建防护体系框架，并从技术、管理和人员层面实施关键防护措施，全方位保障水利工程信息化管理网络安全。

1 水利工程信息化管理网络安全的重要性与特点

在当今数字化时代，水利工程信息化管理已成为推动水利事业高效、精准、科学发展的关键力量。它广泛涵盖了水利工程建设的全生命周期管理、日常运行调度的智能化控制以及防汛抗旱等应急管理的决策支持等多个关键且核心的环节。而网络安全作为水利工程信息化管理的坚实基石，其重要性不言而喻，直接紧密关联着水利工程的正常运转以及社会公共安全。（1）水利工程作为国家基础设施的重要组成部分，承担着防洪、灌溉、供水、发电等众多关乎国计民生的重要职能。信息化管理系统的稳定运行是保障这些职能得以顺利实现的前提条件。一旦网络安全出现问题，其后果不堪设想。数据是水利工程信息化管理的核心资产，涵盖了工程结构数据、水文气象数据、运行调度数据等大量敏感且关键的信息。网络攻击可能导致这些数据的丢失、篡改或泄露，使得管理人员无法获取准确的信息，进而做出错误的决策，严重影响水利工程的运行效率和安全性。更为严重的是，系统瘫痪可能使水利工程失去控制，无法按照预设的程序进行运行调度，在防汛抗旱等紧急情况下，这可能导致洪水泛滥、干旱加剧等灾难性后果，直接威胁到人民群众的生命财产安全和社会稳定。（2）水利工程信息化管理网络具有一系列独特的特点，这也使得其网络安全防护面临着更大的复杂性和挑战性。其覆盖范围极为广泛，不仅包括了水利工程现场的各类监测设备、控制终端，还延伸至各级水利管理部门的信息中心，形成了庞大而复杂的网络体系。涉及的系统众多，涵盖了工程监测系统、调度控制系统、决策支持系统等多个不同类型的系统，这些系统之间相互关联、相互影响，任何一个环节出现安全问题都可能引发连锁反应。数据敏感性高，其中包含的大量信息涉及到国家秘密、商业秘密和个人隐私，一旦泄露将造成严重的损失。此外，水利工程信息化管理网络与物理设施关联紧密，网络攻击可能直接影响到水利工程的实体设施，如大坝、水闸等，从而对工程安全构成直接威胁。我们必须高度重视水利工程信息化管理的网络安全问题，采取切实有效的措施加强防护，确保水利工程的信息化管理系统安全稳定运行，为水利事业的可持续发展和社会公共安全提供有力保障[1]。

2 水利工程信息化管理网络安全风险评估

2.1 风险识别

风险识别作为网络安全风险评估的基石环节，在水利工程信息化管理网络安全保障中起着至关重要的作用，其核心目标在于精准找出该网络中潜藏的安全威胁与脆弱性。就安全威胁而言，既涵盖外部的恶意攻击，如黑客凭借先进技术手段，试图非法入侵系统以窃取或篡改关键数据；病毒入侵会破坏系统正常运行，导致数据丢失或系统瘫痪；网络钓鱼则通过伪装合法信息，诱骗用户泄露敏感信息。同时，内部因素也不容忽视，操作失误可能因人员疏忽引发系统故障，违规行为更是会直接破坏网络安全秩序。脆弱性主要体现在网络结构设计不合理，使得网络易受攻击；系统漏洞为攻击者提供

了可乘之机；安全策略不完善，无法有效防范各类威胁；硬件设备老化会降低系统稳定性和安全性。通过对网络系统、软硬件设备、数据传输过程等进行全方位、深层次的梳理，能够系统且全面地识别潜在风险点，为后续的风险评估和应对提供坚实依据。

2.2 风险分析

在完成风险识别工作后，风险分析成为进一步把控水利工程信息化管理网络安全的关键步骤。它聚焦于对已识别出的风险展开深度剖析，以此精准确定各类风险发生的可能性大小，以及一旦风险实际发生可能引发的具体影响程度。从技术维度深入分析，需要详细探究威胁利用脆弱性的具体途径和发生概率。例如，黑客可能通过系统存在的未修复漏洞，采用特定攻击代码实现入侵，要评估这种攻击手段成功的几率。从业务层面考量，需全面评估风险对水利工程信息化管理各项功能的干扰与破坏情况。比如，数据完整性受损可能导致决策失误，可用性降低会影响实时调度，保密性泄露会带来安全隐患。综合技术与业务层面的分析结果，依据统一标准明确风险的等级和优先级，为后续制定针对性的风险应对策略提供科学、可靠的依据[2]。

2.3 风险评估方法

风险评估方法是精准衡量水利工程信息化管理网络安全风险的关键手段，主要涵盖定性评估与定量评估这两大类别。（1）定性评估侧重于对风险的性质和特征展开细致描述与深入分析。它凭借专家的经验、知识以及历史案例等信息，综合判断风险在严重程度上的相对排序，能快速识别出关键风险因素，为风险管理提供宏观方向的指引。（2）定量评估则是通过严谨的数学模型和统计方法，量化风险发生的概率以及可能造成的损失程度，进而得出具体、直观的风险数值。这种方式能为风险决策提供精确的数据支持，使风险管理更具科学性和针对性。（3）在水利工程信息化管理网络安全风险评估的实际工作中，不能单一地依赖某一种评估方法。应根据具体场景、数据获取的难易程度等因素，灵活选择合适的评估方法，甚至将两种方法有机结合、综合运用，以此提高评估结果的准确性和可靠性，为水利工程的网络安全保障筑牢坚实防线。

3 水利工程信息化管理网络安全防护体系构建原则与框架

3.1 构建原则

在水利工程信息化管理网络安全防护体系构建过程中，严格遵循科学合理的构建原则是保障网络安全的基础与前提。（1）全面性原则要求防护体系必须全方位覆盖网络系统的各个环节和层面，从网络架构的底层硬件设施，到上层的应用软件和数据传输过程，都要纳入防护范围，确保不存在任何防护死角，避免因局部漏洞而引发整体网络安全危机。（2）动态性原则强调要根据不断变化的网络安全形势以及系统的升级更新情况，及时、灵活地调整和优化防护策略。网络安全威胁时刻处于演变之中，只有保持动态适应，才能使防护体系始终具备有效的抵御能力。（3）最小权限原则需严格控制用户和程序的访问权限，仅赋予其完成工作所必需的最小权限，避免权限过度分配，从而降低因权限滥用或泄露而带来的安全风险。（4）纵深防御原则要构建多层次、多维度的防护机制，形成层层设防、环环相扣的防护体系，有效提高防护的整体有效性，为水利工程信息化管理网络安全提供坚实保障。

3.2 整体框架

在水利工程信息化管理网络安全防护体系里，整体框架的搭建至关重要，它主要由技术层、管理层和人员层三个关键层面构成，各层面相互协作、缺一不可。（1）技术层作为防护体系的基础支撑，涵盖多种先进且有效的技术手段。网络边界防护如同坚固的城墙，阻挡外部非法网络访问；终端安全防护确保每一台接入网络的设备安全稳定运行；数据安全防护则对水利工程中的关键数据进行加密、备份等操作，防止数据泄露与丢失。（2）管理层是保障防护体系有序运转的关键，通过建立健全安全管理制度，明确安全责任与规范；规范操作流程，使各项网络操作有章可循；实施安全审计，对网络活动进行实时监测与审查，确保防护措施能够切实有效地执行。（3）人员层处于核心地位，通过开展专业培训、安全教育等活动，提升人员的安全意识和操作技能，从而减少因人为疏忽、违规操作等因素导致的安全风险，为水利工程信息化管理网络安全保驾护航[3]。

3.3 各层级关联

在水利工程信息化管理网络安全防护体系里，技术层、管理层和人员层紧密相连、相辅相成，共同构建起坚固的安全防线。（1）技术层作为物质基础，为管理和人员防护提供了丰富多样的工具与手段。先进的网络边界防护技术、精准的数据加密技术等，如同锐利的武器，能够直接抵御外部的网络攻击，保障网络系统的安全稳定运行。（2）管理层则发挥着规范和约束的重要作用，它为技术的应用和人员的行为制定了明确的准则。通过建立健全的安全管理制度、规范操作流程，确保技术手段能够得到合理、有效的运用，同时引导人员按照正确的方式开展工作，避免因操作不当而引发安全风

险。（3）人员层是技术实施和管理执行的关键主体，他们操作技术设备、遵循管理规定。只有三个层级协同配合、无缝衔接，充分发挥各自的优势，才能形成一个完整、高效、具有强大防御能力的水利工程信息化管理网络安全防护体系。

4 水利工程信息化管理网络安全防护体系关键措施

4.1 技术层面防护措施

在水利工程信息化管理网络安全的技术防护层面，需综合运用多种先进技术构建严密的安全防护网。（1）利用防火墙、入侵检测系统（IDS）与入侵防御系统（IPS）等，精心构筑网络边界防护屏障。防火墙如同忠诚的卫士，依据预设规则严格过滤进出网络的流量，阻止非法访问的尝试；IDS 实时监测网络中的异常行为，及时发现潜在的安全威胁；IPS 则能在检测到攻击时迅速采取行动，阻断攻击流量，为网络边界提供全方位、多层次的保护。（2）部署终端安全管理软件，可对终端设备进行全面、细致的安全管控，包括设备接入认证、软件安装管控、病毒查杀等，确保终端设备的安全性和合规性。（3）采用数据加密技术，对水利工程中的关键数据在传输和存储过程中进行加密处理，保障数据的保密性和完整性。建立安全补丁管理机制，及时为系统和软件打上补丁，修复已知漏洞。

4.2 管理层面防护措施

在水利工程信息化管理网络安全体系中，管理层面防护措施是保障网络安全稳定运行的关键支撑。（1）要构建一套完善且细致的网络安全管理制度，清晰界定各部门和人员在网络安全中的具体职责，做到责任到人，避免出现安全管理的盲区和漏洞。（2）制定全面且具有针对性的安全策略。访问控制策略严格规范用户对网络资源和数据的访问权限；数据备份与恢复策略确保在数据丢失或损坏时能够及时恢复，保障业务的连续性；应急响应策略则能在面对突发安全事件时，迅速启动应对机制，降低损失。（3）定期开展全面且深入的安全检查和审计工作，通过专业工具和技术手段，及时发现系统中潜藏的安全隐患，并督促相关部门和人员及时整改。此外，还需加强对系统建设、运维等全过程的安全管理，从项目规划、开发到日常维护，确保每一个环节都严格遵循安全规范，为水利工程信息化管理网络安全筑牢坚实的管理防线[4]。

4.3 人员层面防护措施

在水利工程信息化管理网络安全防护工作中，人员层面防护措施至关重要，是筑牢安全防线的关键一环。（1）要大力加强对相关人员的网络安全意识培训。通过定期组织专题讲座、案例分析研讨会等形式，让工作人员深入了解各类网络安全威胁的呈现形式、潜在危害以及防范要点，切实提高他们对网络安全威胁的敏锐识别能力和主动防范意识，从思想根源上杜绝因疏忽大意而引发的安全风险。（2）开展专业技能培训也必不可少。根据不同岗位需求，有针对性地设置培训课程，使工作人员熟练掌握必要的安全操作技能，如数据加密、访问权限设置等，同时学会在面对突发安全事件时，能够迅速、准确地采取应急处理方法，将损失降到最低。（3）建立科学合理的人员考核与奖惩机制，对在网络安全防护工作中表现优秀的人员给予表彰和奖励，对违规操作的人员进行相应处罚，以此规范人员行为，充分调动其积极参与网络安全防护工作的主动性和积极性。

结束语

水利工程信息化管理网络安全是保障水利事业稳健发展的核心要素。通过全面且深入的风险评估，精准识别、分析风险并选用合适评估方法，为安全防护筑牢认知根基。遵循科学构建原则搭建技术、管理、人员层协同的整体框架，从技术防护、管理规范到人员素养提升多管齐下，采取一系列关键防护措施。唯有如此，才能构建起坚不可摧的网络安全防护体系，确保水利工程信息化管理系统稳定运行，为水利事业可持续发展与社会公共安全提供长久有力的支撑。

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.