

水利数字孪生网络安全防护体系构建与风险评估方法研究

李 浩 珠 娅 张 岳 葛子依 刘凤莲

内蒙古河套灌区水利发展中心 内蒙古 巴彦淖尔 015000

【摘要】水利行业在数字化转型过程中,数字孪生技术被广泛应用于水利设施的监控与管理中。随着数字孪生技术的不断深入,网络安全问题日益突出,尤其是在水利基础设施的安全性与数据保护方面。本研究构建了水利数字孪生网络安全防护体系,并提出了一套有效的风险评估方法。分析了水利数字孪生系统中的主要安全风险,随后结合现有技术提出了防护体系架构。通过对水利数字孪生系统进行全面的风险评估,为提高系统的安全性与可靠性提供理论支持与实践指导。

【关键词】水利数字孪生;网络安全防护;风险评估;安全体系;数字化转型

DOI:10.12417/2811-0722.25.12.058

引言

水利系统作为国家基础设施的一部分,其数字化转型的重要性日益增加。水利数字孪生技术通过虚拟化真实水利设施和运行环境,使管理者能够更精确地监控与调度。随着这些技术的应用,水利系统的安全问题也成为亟待解决的挑战。数字孪生模型本身与网络环境紧密结合,使得网络安全成为水利数字化转型中的关键环节。本研究旨在构建一个完备的水利数字孪生网络安全防护体系,并结合风险评估方法,为水利行业提供更强大的安全保障,确保水利设施在数字化管理环境中的稳定与安全。

1 水利数字孪生系统的关键技术与安全挑战

水利数字孪生系统结合了虚拟现实、物联网、大数据和人工智能等多项前沿技术,旨在通过创建一个水利设施的数字化镜像,实现对水利工程、环境变化和资源流动的实时监控与管理。通过精准的实时数据采集与分析,能够为水利系统的运行提供科学决策依据,提升水利管理效率。随着数字孪生系统的逐步推广,水利领域面临的安全挑战也愈加复杂。数字孪生系统的核心在于其对实时数据的依赖。水利系统中,涉及到的数据量庞大且种类繁多,从水位、流量到气象变化、设备状态等,这些数据的安全性直接影响到整个系统的稳定性。网络传输的过程中,数据可能遭受篡改、丢失或泄露等风险,尤其在水利设施的关键节点,如水坝、泵站等处,安全漏洞可能带来严重的后果。数字孪生系统需要应对数据传输过程中的加密问题、身份认证问题及访问控制问题,以确保数据的完整性和机密性。

数字孪生系统的网络环境也面临着许多潜在的威胁。随着水利设施逐步实现自动化与远程监控,控制系统的网络化特征使其更加暴露于网络攻击的风险。尤其是分布式架构下,各种设备和传感器的互联互通,容易成为黑客攻击的入口。恶意攻击可能导致系统失控,甚至引发设备损坏或大规模的灾难。水利数字孪生系统中的网络安全防护不仅要防范常规的网络攻击,还要面对包括内部人员的非法操作、数据泄露等安全隐患。系统的复杂性也是数字孪生面临的一个巨大挑战。随着技术的

不断进步,水利数字孪生系统不仅涉及单一的水利设施,还需结合生态环境、气候变化等多种因素,构建一个全局性、综合性的虚拟模型。

2 水利数字孪生网络安全防护体系架构设计

在水利数字孪生系统的网络安全防护体系架构设计中,关键的任务是构建一个多层次、全方位的安全防护框架,确保数字孪生技术在复杂的水利系统中安全有效地运行。这个架构不仅需要应对外部网络攻击,还需防范内部安全隐患,保障整个系统的稳定性与可持续性。架构设计的首要任务是实现数据的安全传输与存储。数据采集端需要采用高强度的加密技术,防止传输过程中数据被篡改或截取。对数据进行端到端加密,确保无论是在网络传输过程中,还是在存储过程中,数据的机密性和完整性都能得到保障。除了加密技术,身份认证与访问控制机制的设计至关重要。每个操作用户和设备都必须通过严格的身份验证,只有经过授权的用户和设备才能访问敏感数据或执行关键操作。基于角色的访问控制(RBAC)机制可以有效限制不同用户权限,从而避免权限滥用或恶意操作。

防护体系的另一层重要设计是在物理层和网络层的防御。水利设施通常地理分布广泛,数字孪生系统所依赖的传感器、执行器和控制系统的互联互通给网络安全带来不小挑战。为了确保系统的抗攻击能力,架构设计中需要采用多重防火墙、入侵检测与防御系统(IDS/IPS)等手段,对网络进行实时监控与防御。结合威胁情报与人工智能技术,可以实现对异常行为的自动识别与响应,从而提高系统的实时防御能力。对于水利数字孪生系统中的数据中心,还需设计物理与网络隔离措施,防止外部或内部威胁通过物理接入网络进行攻击。系统的冗余与容错设计也至关重要。在防护体系架构中,容灾与备份机制应当得到充分考虑,确保在遇到攻击或故障时,系统能够迅速恢复。通过采用分布式架构,水利数字孪生系统能够在某一节点或区域遭受攻击时,避免整个系统的瘫痪。通过实时备份与数据同步技术,可以将关键数据实时复制到异地或云端,保证在发生突发事件时数据的可恢复性。

水利数字孪生网络安全防护体系的建设需要动态监测与

持续评估。在设计架构时，应嵌入实时监控模块，持续跟踪网络流量、设备状态以及安全事件。借助大数据分析与机器学习技术，可以从海量数据中挖掘潜在的安全威胁，及时发现并修复系统漏洞。定期的风险评估与安全审计可以有效发现架构中可能存在的薄弱环节，并针对性地进行优化升级，确保系统始终保持在高安全水平。该防护体系不仅需要在技术上实现多层次防护，更要在管理和流程上落实安全策略，通过全面的安全措施保障水利数字孪生系统在运行中的安全性与稳定性。

3 水利数字孪生系统中的主要安全风险分析

水利数字孪生系统在提高水利管理效率的同时，也面临着多种安全风险。这些风险不仅来源于系统的技术复杂性，还涉及到数据传输、设备管理、用户权限等多个层面。在这些风险中，数据安全问题尤为突出，特别是数据的采集、存储和传输过程中可能遭遇的篡改、泄露和丢失等问题。水利数字孪生系统依赖于大量实时数据，这些数据往往涉及到水位、流量、气象、设备状态等关键参数，一旦被恶意篡改或泄露，将对系统的正常运行产生严重影响。因此，保障数据的完整性、机密性以及可用性成为系统设计中的核心任务。

除了数据安全，网络安全风险同样不可忽视。水利数字孪生系统通常依赖于物联网技术，通过大量传感器和执行器实现对水利设施的远程监控与管理。这些设备往往位于偏远地区，通信链路不稳定，网络攻击的可能性大大增加。通过网络对水利设施进行远程操作或调整，一旦受到黑客攻击，可能导致控制系统失灵，进而对水利设施造成物理破坏，甚至引发严重的灾难性后果。尤其是在水坝、泵站等关键设施中，任何网络攻击都可能导致系统的崩溃或无法及时响应，造成灾难性损失。设备层的安全风险也是水利数字孪生系统不可忽视的一环。水利系统中涉及的传感器、控制设备、通信模块等硬件设备，常常面临着硬件故障、环境因素影响等问题。由于设备运行在恶劣环境中，硬件老化、损坏的风险较高。一旦设备出现故障，可能导致数据采集的中断或错误，影响到整个系统的稳定性和安全性。设备之间的通信协议若未得到充分加密，可能会遭到外部攻击者的操控，进一步加剧了系统安全隐患。

权限管理和身份认证问题也是水利数字孪生系统中的重要安全隐患。系统内的用户和操作人员需要具备不同的访问权限，且权限管理需要动态调整。然而，随着系统复杂度的提升，用户身份验证的环节可能出现漏洞。若出现权限滥用、非法登录或管理员权限泄露等情况，可能会导致系统的敏感操作被未经授权的人员执行，从而造成不可逆的损害。网络钓鱼、社交工程攻击等手段也可能被攻击者用来获取系统权限，从而对系统安全构成威胁。

水利数字孪生系统规模持续扩展，复杂性与系统互联互通催生新安全挑战。跨区域跨部门数据共享和交互扩大系统攻击面，跨域信息交换、设备互联互通需精细化安全策略规避风险。

任一环节出现安全漏洞，整个系统安全性都可能受到威胁。系统各模块协同与防护措施需更为严密，防范各类潜在风险，保障水利数字孪生系统正常运作。系统安全风险种类多样且相互交织，在设计和运维过程中需全面考量多维度安全防护，及时识别修补潜在漏洞，保障水利数字孪生系统在复杂环境和多变威胁下仍能高效稳定运行。

4 水利数字孪生系统的风险评估方法与应用

风险评估不仅要涵盖系统的技术漏洞，还要考虑可能的环境、操作和管理风险。为了实现这一目标，基于系统性思维的风险评估框架至关重要，该框架能够整合技术分析、数据流动和安全控制等多个方面，形成一个综合的评估体系。在评估过程中，首先需要对水利数字孪生系统中的各个组件进行详细的威胁分析。通过对水利设备、数据传输网络、控制中心等关键环节的安全性进行逐一审查，能够明确每个模块的潜在漏洞。特别是在传感器数据采集和信息传输环节，评估其可能遭受的网络攻击、数据篡改或丢失等风险。在此基础上，量化每种风险的发生概率和潜在损失，采用概率论与统计学方法为各类风险赋予具体的数值模型，评估系统在面对特定威胁时的脆弱性。

除了技术层面的风险评估，操作管理层面的安全风险也必须纳入考虑。通过模拟不同类型的攻击情景，如内部人员泄密或操作错误，能够评估系统在遭遇人为因素时的反应能力和恢复能力。水利数字孪生系统的多层次权限控制和身份认证机制也应作为评估的重点，检查是否存在权限滥用或非法操作的可能性。结合应用实践，风险评估的结果可以为防护措施的制定提供依据。通过识别出数据传输过程中的薄弱环节，可以优先采用加密技术和安全传输协议，以确保数据的安全性。对于设备层面出现的风险，采取冗余备份和故障恢复方案来减少损失。评估结果还可用于指导安全架构的优化，确保每个安全防护措施都能与具体的风险相匹配，提升水利系统整体的抗风险能力。通过定期的风险评估，能够持续监控系统的安全状态，及时调整防护措施，应对新的威胁挑战。这种动态评估方法不仅提升了水利数字孪生系统的安全性，还为今后的数字化转型提供了坚实的保障。

5 构建有效的防护机制与提升系统安全性

在此过程中，首先需要为系统建立一套多层次的防御架构，涵盖数据、网络、硬件和操作等各个层面，以应对不断变化的安全威胁。数据安全防护是其中的基础环节，对所有从传感器采集到存储的数据进行严格加密，并通过身份认证和访问控制机制来防止未经授权的访问或篡改。通过采用强加密算法和密钥管理方案，确保数据在传输过程中不受攻击，同时加强数据存储层的保护，防止数据丢失或泄漏。

网络安全防护是数字孪生系统不可或缺的组成部分，尤其

在水利行业中，设施的分布广泛，数据传输链路复杂，网络攻击的风险较高。采取入侵检测与防御系统（IDS/IPS）对于实时监测网络流量和识别异常行为至关重要。网络防火墙和虚拟私有网络（VPN）能够进一步隔离关键系统与外部网络，防止外部攻击通过网络侵入。通过建立分布式架构，将关键节点的数据和控制分散，避免单点故障导致整个系统的崩溃。硬件层面的安全同样不容忽视。水利数字孪生系统中使用的各类传感器、执行器和控制设备大多分布在不同的地理位置，这些设备常常面临着恶劣的环境条件，易受物理损坏或外界干扰。对此，应通过冗余设计和容错机制，确保系统在个别设备失效时能够平稳过渡，防止对整体系统产生影响。设备的物理隔离和硬件加密措施也能有效防范外部攻击者通过物理手段破解系统安全。

在防护体系的构建中，操作管理和权限控制措施同样至关重要。通过细化用户权限和执行操作的审计机制，可以确保只有经过授权的人员能够对系统进行调整或操作。权限管理系统

应具备灵活性与可扩展性，以应对不同岗位与职能的需求，并对关键操作进行实时记录和审查，确保系统的每次操作都可追溯并受到监控。定期进行漏洞扫描和安全审计，对发现的潜在威胁进行及时修补。持续的安全性评估与改进是防护机制长期有效性的保障。随着技术的进步和攻击手段的演变，防护机制应保持灵活性，定期进行系统的安全漏洞检测和应急响应演练，以应对日益复杂的安全威胁。通过这一系列措施的落实，能够显著提高水利数字孪生系统的抗攻击能力，确保系统在日常运行中的安全性与稳定性。

6 结语

通过构建完善的水利数字孪生网络安全防护体系和有效风险评估方法，可以大幅提升水利设施在数字化转型过程中的安全性。随着技术的不断发展和安全威胁的多样化，持续加强安全防护、优化风险评估机制，以及提升系统的抗风险能力，将为水利行业的可持续发展提供坚实保障。

参考文献：

- [1] 王亮,张磊.水利数字孪生系统的架构与安全防护研究[J].水利科技与经济,2022,28(4):34-40.
- [2] 赵青,陈伟.基于数字孪生技术的水利设施管理与安全防护分析[J].水利工程学报,2021,52(5):122-128.
- [3] 李洋,何杰.水利行业数字化转型中的信息安全风险及防护措施[J].信息安全与技术,2023,39(1):55-61.
- [4] 周婷,王国良.水利数字孪生技术与网络安全风险评估方法研究[J].网络安全技术与应用,2021,16(3):45-52.
- [5] 刘翔,薛琳.数字孪生技术在水利领域的应用与挑战[J].智能科学与技术,2022,13(2):98-104.