

数智水利应用风险及其防控对策

蒋云钟^{1,2}, 冶运涛^{1,2*}

(1. 中国水利水电科学研究院, 100038, 北京; 2. 水利部数字孪生流域重点实验室, 100038, 北京)

摘要:我国数智技术的水利领域应用从试点探索逐步进入体系化建设新阶段, 深度嵌入日常管理、运行决策、工程控制的核心环节, 在显著提升治理效能的同时, 也使系统运行面临风险隐患。为系统识别数智水利应用风险, 保障系统安全、可靠、可信、可控运行, 本文基于数字孪生水利架构和运行原理, 分析数智水利应用对数据、模型、算力、知识、网络及集控的六大强依赖特性, 揭示强依赖特性所衍生的数据风险、模型风险、算力风险、知识风险、网络风险、集控风险等复合型挑战, 并从制度构建、技术防护、人才强基、韧性提升四个维度提出立体化风险防控体系对策, 涵盖国家战略与综合安全框架制定、法律法规与标准规范健全、协同监管与第三方审计机制建立、数据全生命周期治理、可信AI与模型综合治理、自主弹性算力与韧性网络建设、组织重塑与流程再造、数智人才强基、人机协同与知识管理、联邦式混合韧性架构设计、常态化攻防演练、极端情景应急预案制定等关键举措, 为防范化解数智水利系统性风险提供技术支撑。

关键词:数智水利; 数字孪生水利; 强依赖特性; 复合型风险; 可信AI; 韧性架构; 风险防控

Risk analysis and prevention strategies for digital-intelligent water conservancy applications

JIANG Yunzhong^{1,2}, YE Yuntao^{1,2*}

(1. China Institute of Water Resources and Hydropower Research, Beijing 100038, China;

2. Key Laboratory of River Basin Digital Twinning of Ministry of Water Resources, Beijing 100038, China)

Abstract: As the application of digital-intelligent technologies in China's water conservancy sector gradually transitions from pilot exploration to a new stage of systematic development, these technologies are becoming deeply embedded in the critical junctures of daily management, operational decision-making, and engineering control. While this integration substantially enhances governance efficiency, it also exposes system operations to emerging risks and vulnerabilities. To systematically identify the risks inherent in digital-intelligent water conservancy applications and ensure their safe, reliable, trustworthy, and controllable operation, this study, based on the architecture and operational principles of digital twin water conservancy, identifies six strong dependency characteristics of these applications—namely, on data, models, computing power, networks, knowledge, and centralized control. The study further reveals the composite challenges arising from these dependencies, including data risks, model risks, computing risks, knowledge risks, network risks, and centralized-control risks. In response, a multi-dimensional risk prevention and control framework is proposed from four interconnected dimensions—institutional development, technical safeguards, capacity building, and resilience enhancement. Key measures encompass the formulation of national strategies and comprehensive

收稿日期: 2026-02-05 修回日期: 2026-06-28

作者简介: 蒋云钟, 正高级工程师, 主要从事智慧水利、水文水资源相关研究工作。

通信作者: 冶运涛, 正高级工程师, 主要研究方向为水文水资源、智慧水利。E-mail: yeyuntao@iwhr.com

基金项目: 国家重点研发计划项目(2023YFC3209302-03); 国家自然科学基金面上项目(52279031); 国家自然科学基金青年项目(52309040)。

security frameworks, the improvement of laws, regulations, and standards, the establishment of collaborative oversight and third-party audit mechanisms, full life-cycle data governance, trusted AI and comprehensive model governance, the development of autonomous and resilient computing power and network infrastructure, organizational restructuring and process re-engineering, the cultivation of digital-intelligent talent, human-machine collaboration and knowledge management, the design of federal hybrid resilient architectures, routine red team vs. blue team cyber defense exercises, and the development of extreme scenario emergency plans. This research provides technical support for preventing and mitigating systemic risks in digital-intelligent water conservancy applications.

Keywords: digital-intelligent water conservancy; digital twin water conservancy; strong dependency characteristics; composite risk; trusted AI; resilient architecture; risk prevention and control

中图分类号: TV+TP18 文献标识码: A 文章编号: 1000-1123(2026)15-0001-08

DOI: 10.3969/j.issn.1000-1123.2026.15.001

当前,全球正处于新一轮科技革命与产业变革浪潮之中,以数据科学、人工智能(AI)、机器人等领域迅猛突破触发的新一轮科技革命开启了数智时代。水利作为关系国计民生的基础性行业,其现代化进程与国家水安全保障能力紧密相连,以新质生产力重塑水利发展模式和提升水利效率效能成为时代的选择和行业数智化转型的必经之路。以物联网、大数据、数字孪生、人工智能为核心的数智技术深度融合正引领水利行业迈向以数字化、网络化、智能化为特征的新发展阶段。我国高度重视数智水利建设,国家层面战略部署大力推进以数字孪生水利为代表的数智水利建设,数字孪生流域、数字孪生水网、数字孪生水利工程建设试点成绩斐然,当前正从局部试点向流域性、系统性应用全面铺开。

数智水利集成“天空地水工”一体化监测、高性能计算、专业模型与人工智能算法,旨在实现对物理水利系统(包括流域、水网、工程)的全要素、全过程的数字化映射、智能化模拟与精准化决策,其在提升水旱灾害防御“四预”(预报、预警、预演、预案)能力、优化水资源配置、强化河湖生态保护管控、赋能水利工程智能化运行维护等方面,展现出前所未有的巨大潜力。从黄河、长江等大江大河的洪水风险模拟与调度决策支持,到南水北调等重大水利工程的数字化运维与安全监控,数字孪生正从概念验证逐渐与业务深度融合。

然而,随着数智水利建设的大规模高强度推进,其系统复杂性与业务耦合度呈指数级增长。未来,数智水利不再仅仅是辅助分析的可视化工具,而会成为日常管理不可或缺的“数字底盘”、科学决策倚重的

“模拟推手”乃至工程控制潜在的“智能中枢”。这种深刻的功能演进,使得系统运行的基础性、命脉性依赖特征愈发凸显,由此伴生的新型风险也日益复杂和严峻。传统的单一技术风险或管理风险,正演变为技术失效、数据污染、网络攻击、算法偏见、伦理冲突与制度不适配等多重风险交织的复合型、系统性挑战。任何对潜在风险(如数据质量控制不足、模型验证不充分、安全防护薄弱等)的忽视或应对不力,都可能使耗资巨大的数智水利系统的输出可信度显著降低,甚至可能因系统误判、失控或遭受攻击而导致实体水利系统运行风险,直接威胁人民群众生命财产安全和国民经济稳定运行。因此,在全面推进数智水利建设的进程中,必须前瞻性地开展数智水利应用风险分析,系统识别、科学评估并防范化解其应用风险。

我国将水利信息安全作为工作重点,2008年明确把水利网络与信息安全保障系统作为当时阶段水利信息化八大重点工程之一,提出了水利网络与信息安全基本技术要求,指导全国水利网络与信息安全建设。近年来,水利行业已全面推进网络与信息安全保障体系建设,在安全设计、态势感知、安全管理平台等方面取得显著进展。然而,面对数智水利带来的新型风险(如模型算法偏见、数据投毒攻击、知识污染等),现有研究仍显不足,亟须开展更具前瞻性和系统性的风险分析。本文聚焦数智水利在大规模应用背景下的核心依赖特性,深入剖析其衍生的主要风险,并提出一套系统性、可操作、具有韧性的风险防控对策框架,以期构建安全、可信、高效、负责任的数智水利体系提供理论支撑与实践指引。

一、数智水利应用风险特点分析

我国正在协同推进数字孪生流域、数字孪生水网、数字孪生工程建设,三者互补替代、各有侧重、互联互通、信息共享,应用范围已从单个工程(“点”)向河流水系(“线”)、流域或区域(“面”)不断延伸,深度融入流域防洪、水资源管理与调配等“2+N”业务中,成为全面认识水利、全方位洞察水利、全过程管理水利的重要工具,形成了鲜明的系统性依赖特性。这些依赖特性的本质是系统运行不可或缺的关键要素及其内在脆弱性,是应用风险产生的根源。

1. 对数据的强依赖:从经验判断到数据驱动

随着信息化的快速发展,管理模式正经历从依赖个人经验、人工巡检与周期性报表的传统模式向以数据为感知和判断依据的精准化、实时化管理的深刻转型。作为转型载体的数字孪生体已成为覆盖业务全链条的智能中枢。对流域态势的掌握、工程安全状态的判断、水资源调配计划的制定、河湖库“四乱”(乱占、乱采、乱堆、乱建)问题的发现与督办等业务各环节都与数据流紧密连接。数据的及时性、准确性、完整性决定了系统感知能力。任何关键数据的缺失、延迟或失真都会导致数字孪生体出现“信息黑洞”或“扭曲镜像”,影响决策可靠性。因此,系统对数据具有不可替代的强依赖,数据质量即系统质量成为系统能否发挥作用的重要因素。

2. 对模型的强依赖:从定性会商到定量预演

在水旱灾害防御、水资源调度等重大公共安全决策中,数字孪生技术推动决策模式从基于历史经验和定性会商的经验决策升级为基于实时仿真与多方案定量比选的科学决策。水文水动力模型、水资源配置模型、工程安全评估模型等专业数学模型成为决策链条中不可或缺的“智能参谋”。模型的精度、计算速度和稳定性直接决定了预演结果的可信度,而模型固有的简化假设、参数率定的不确定性以及极端工况下可能出现的失真都会直接传导至决策环节。对模型强依赖意味着模型的失准将导致整个决策链失去科学依据。

3. 对算力的强依赖:从离线分析到在线推演

数智技术驱动水利决策控制的时效性标准正从“长延时离线分析”向“快速在线推演”转变。过去复杂的水文分析、工程安全评估、调度方案生成允许以小时、天甚至周为单位完成离线分析。然而,数智水

利“四预”功能的核心价值要求在“实时”或“超前实时”等极短时间内完成计算。算力供给的可靠性、弹性与稳定性直接决定了系统能否在关键时刻完成计算任务,而算力波动、延迟或中断都会导致预演超时,使“四预”闭环断裂。算力已从辅助支撑跃升为系统运行的“发动机”,其脆弱性决定了系统的脆弱性。

4. 对知识的强依赖:从静态规则到动态学习

一个具有数智能力的数智水利系统必须具备持续学习进化能力。这种进化不仅依赖于算法从新增数据中自动优化参数,更根本的是依赖于高质量的知识注入与更新,包括显性知识(如水文手册、设计规范、调度规程等)和隐性知识(如专家经验)。系统智能水平的上限受限于所注入知识的质量与真实性,知识本身存在偏差、错误或过时就会使系统在错误认知基础上进行决策。特别是从数据中自动挖掘的“伪知识”具有极强隐蔽性,一旦被采纳就会导致系统性、方向性错误。因此,系统对知识的强依赖使智能演进过程中存在“认知陷阱”。

5. 对网络的强依赖:从局部连通到全面连接

数智水利要求将散布在广阔流域内的感知设备、管理节点和工程控制单元全部接入融合的通信网络,实现数据与指令的畅通流动。传统模式下单个工程拥有相对独立的监控系统,而数智水利打破了局部连通格局。网络的稳定性、安全性和实时性直接决定了系统的感知控制能力。任何关键通信节点的故障都会导致大范围的数据传输中断或指令调度受阻,使数字孪生体出现“区域性失明”或“局部肢体瘫痪”,瓦解基于全局协同的优化调度逻辑。同时,全面连接将原本分散的网络安全边界整合为庞大攻击面,网络的脆弱性被大幅度放大。

6. 对集控的强依赖:从分散自治到协同优化

数智技术的重要价值在于突破单个工程的管理边界,在流域或水网尺度上实现系统性和全局性的优化调度与风险协同防控。这要求改变传统“各自为政”的分散管控模式,将部分调度权与决策建议权上移至集控中心(如国家、流域或省级调度中心)。系统整体效能高度集中于中心节点,该节点集成了全系统的核心数据、关键模型和最终决策算法。一旦中心节点因故障、攻击或误操作失能,其负面影响将迅速传导至所有下属工程,可能引发大范围运行失调甚至瘫痪。因此,集控在提升效率的同时,也将风险高度浓缩于单一战略点。

二、数智水利应用主要面临的风险挑战

基于上述六大强依赖特点分析,在大规模应用场景下,数智水利主要面临以下交织叠加的多维风险(见图1)。

1. 数据风险:源头失真、治理失序与决策失灵

在数据采集源头,感知设备因环境干扰、老化或人为破坏产生漂移或数据错误,导致水位、流量等关键信息失准。例如,失准水位计报送的数据会扭曲下游的流量推算与洪水预报结果。在传输与存储环节,网络延迟、丢包可能导致数据“断流”,存储中心若安全防护不足则面临数据被篡改、窃取或勒索的威胁。在多元异构数据融合处理环节,来自卫星、地面、社会的海量数据在时空基准、精度与格式上各异,低效或错误的融合算法会放大单一错误,生成矛盾乃至虚假的融合信息,导致“低质量数据输入,不可靠决策输出”的恶性循环。如果基于失真数据进行洪水模拟、水资源调配预演,并使用其结论指挥工程调度,轻则降低运行效率,重则可能引发工程事故,将虚拟空间的数据风险转化为物理世界的真实灾害。

2. 模型风险:从“黑箱”失准到信任危机

传统机理模型是水利决策的核心工具,水利部正统筹推进其研发,不断提高精度与可靠性。然而,在极端复杂边界或超历史极值工况下,任何模型(包括机理模型和AI模型)都存在不确定性。人工智能模型(尤其是深度学习模型)因其“黑箱”特性,在可解释性、泛化能力方面面临独特挑战,可能产生难以预料的输出,决策者既无法理解其推理过程,也难以预知其何时会失效,这种不可解释性严重阻碍了其在重大安全决策中的可信应用。需要强调的是:机理模型与AI模型并非对立,而应融合互补;当前水利行业以机理模型为主、AI模型为辅,本文所讨论的模型风险主要针对AI模型的特殊脆弱性,也强调所有模型均需进行严格的验证与不确定性管理。此外,模型面临被攻击风险,攻击者可通过“数据投毒”,在训练阶段植入后门或精心构造“对抗性样本”,在应用阶段诱使模型作出错误判断。

3. 算力风险:数字基座的“供血”危机与单点故障

数智水利系统在洪水演进三维可视化、多方案并

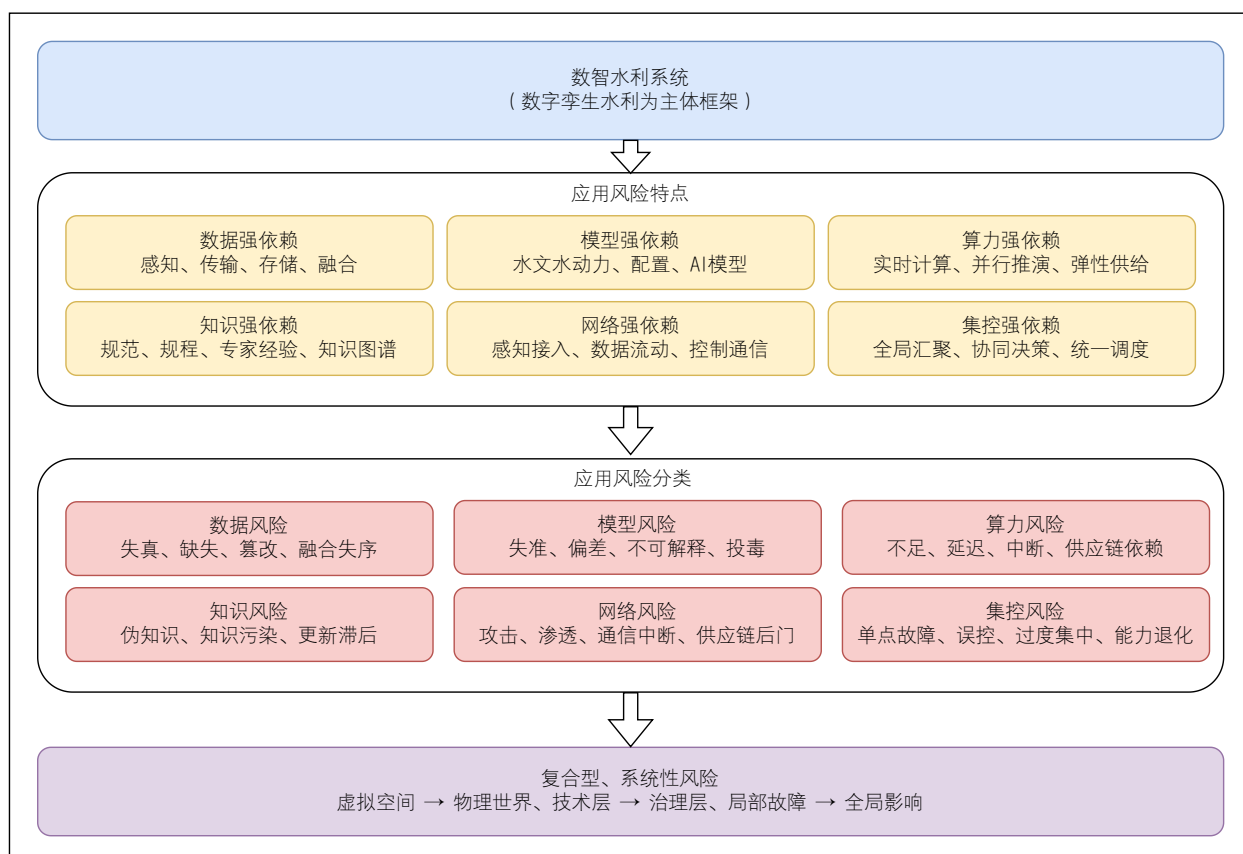


图1 数智水利六大强依赖特性及复合型风险传导机制

行预演、实时数据同化等典型场景中,对算力的瞬时爆发能力、弹性扩展能力和持续稳定性提出了较高要求。以大流域洪水预报为例,系统需在数分钟内完成多个调度方案的并行模拟,若算力供给不足,将直接导致“四预”功能时效性降低。其次,如果数据中心、通信网络、电力供应设备等遭受自然灾害、设备故障、供电中断等传统物理风险,整个数字孪生体可能随之瘫痪。此外,高性能计算芯片、仿真软件、数据库系统等仍存在较强对外依存,地缘政治博弈可能引发技术断供或“卡脖子”风险。算力成本也给运营单位带来较大压力。

4. 知识风险:智能演进的“认知陷阱”与“伪知识”污染

数智水利系统的高阶智能核心驱动力源于对海量数据背后规律的挖掘与凝练,即“知识”的自动发现与应用。“伪知识”或低质知识的生成与注入会影响系统智能水平和决策可靠性。人工智能训练数据存在偏差、噪声或历史局限,可能使算法学习片面、错误甚至荒诞的“规律”,一旦这些“规律”被采纳固化到预测决策模型中,将导致系统性、方向性的误判。其次,隐性知识断层和知识更新滞后会带来“智能鸿沟”。专家头脑中大量至关重要的判断难以结构编码;同时,若知识库更新不能适应水利学科知识、工程标准、调度规程的不断演进和外部环境持续变化,系统“认知”将与现实脱节。因此,充斥着“伪科学”认知或固守着陈旧经验法则的“数字大脑”可能比一无所知更为危险。

5. 网络风险:从数字空间到物理世界的传导失控

数智技术打通网络空间与物理世界的边界,网络攻击的靶标从数据升级为工程实体。国家级高级持续性威胁(APT)和勒索软件攻击可能长期潜伏,窃取敏感数据或在冲突时夺取系统控制权;勒索软件可加密业务数据或锁定控制系统,迫使工程运行中断。更为危险的是,攻击者可能借着信息层和操作层的深入融合,侵入某个普通信息系统作为跳板篡改闸门、泵站等核心工程控制系统指令,以数字攻击实现物理破坏。例如,恶意篡改水库调度指令可人为制造泄洪事故。系统攻击面因海量物联网终端的接入而急剧扩大,数以万计的水位计、摄像头等感知设备安全防护薄弱,极易被攻破并用作入侵内网的“肉鸡”。此外,内部人员失误或恶意操作以及通过软硬件供应链植入的后门,构成了难以防范的深层隐患。

6. 集控风险:效率背后的系统性脆弱

国家水网集控可能成为影响全局的单一故障点,该节点若受数据、算法、知识等影响带来的决策误判或错误指令下达,可能导致整个工程控制系统失去协调指挥。同时,长期依赖中心发出的精细化、自动化指令,地方管理机构和工程现场人员的独立分析判断能力和应急处置能力可能弱化。当中心失效需要切换至本地手动控制时,响应速度和处置有效性可能大打折扣。此外,集中式智能优化决策在极端情景下可能引发复杂的系统性权衡与伦理挑战。为保障重点城市或目标,算法生成的方案可能要求某些区域承担更大风险,这类涉及重大价值判断的决策权限是否应交由中央算法、如何保障其公平性与透明度等,都是亟待解决的问题。

三、数智水利应用风险防控对策

为有效应对上述多维复合型风险,必须坚持制度为纲、技术为盾、人才为基、韧性为本的核心理念,从顶层设计、技术防护、管理变革、系统韧性4个维度系统阐述具体的对策与实施路径,构建各维度相互支撑、有机衔接的多层次、立体化、具有主动适应性的风险防控体系,保障数智水利系统安全、可靠、可信、可控运行(见图2)。

1. 强化顶层设计与制度构建,明确规则与责任

制度是防范系统性风险的根本保障。数智水利建设涉及跨部门、跨层级、跨业务的复杂协同,必须从国家战略高度构建权责清晰、标准统一、监管有力的制度框架。

(1) 制定国家战略与综合安全框架

由水行政主管部门牵头,联合网信、发展改革、科技、工业和信息化、标准化管理等相关部门,共同发布数智水利发展中长期规划与安全战略,明确未来发展愿景、核心原则、技术路线图和分阶段目标。确立安全可控和高效智能并重原则,以及安全前置、内生安全理念,界定数据、模型、算力、知识、网络、集控等安全域,落实“同步规划、同步建设、同步运行”的刚性要求。

(2) 健全法律法规与标准规范体系

推动水法、防洪法等上位法的修订,增设数智水利建设、运营、数据权属、算法问责等相关条款。优先出台水利数据资源管理办法、水利模型运维管理办法、水利关键信息基础设施安全保护条例(数字孪生专题)等专项法规,明确数据分类分级保护要求、核心系统认定、运营者主体责任以及事故问责流程。构建一个基础通用、关键技术、安全测试、行业应用四位一体的标

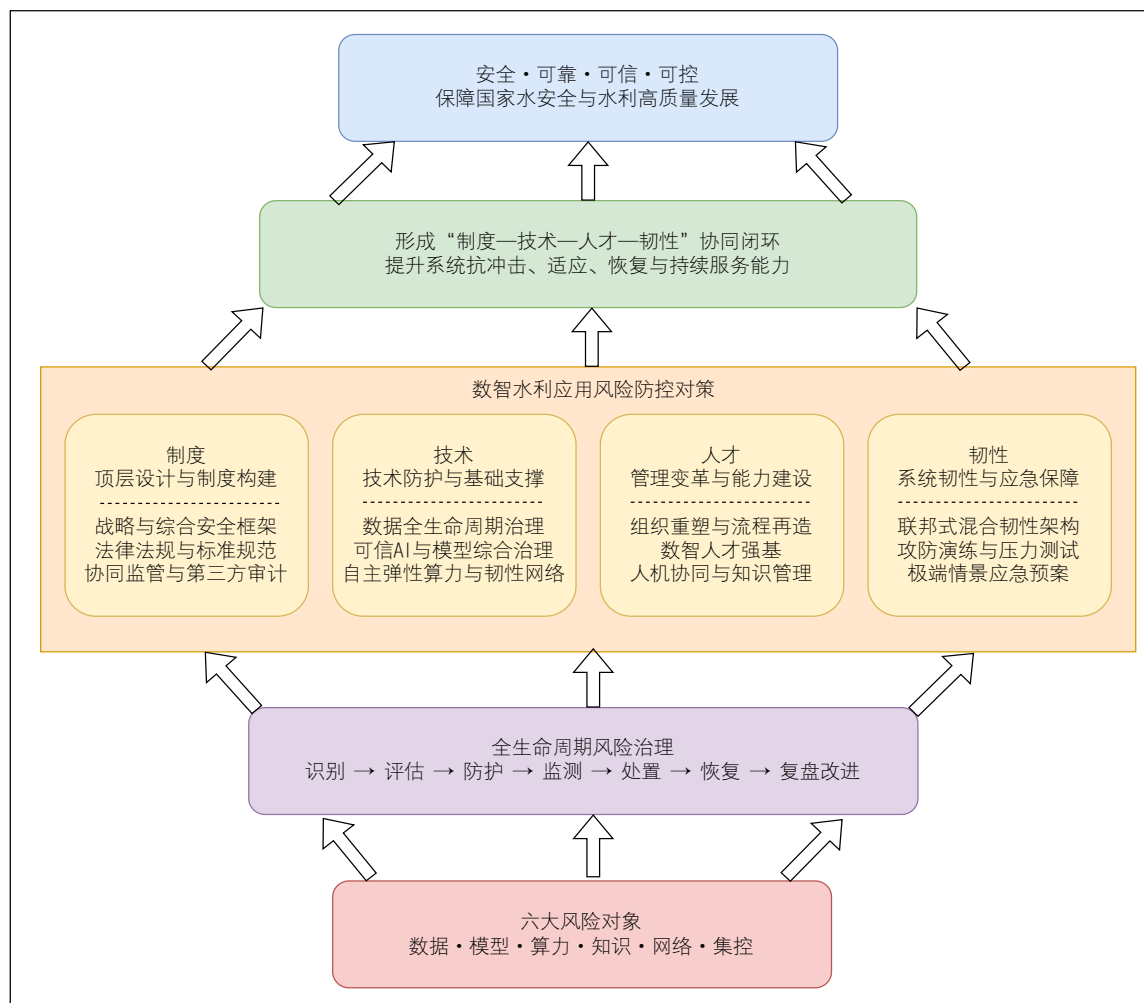


图2 风险防控体系

准体系，覆盖数据、模型、算力、知识、网络、集控全要素风险防控。

（3）建立协同监管与第三方审计机制

设立由水利、网信、公安、保密、密码管理等相关部門参与的常态化协同监管联席会议机制，负责政策协调、风险信息共享、重大安全事件联合研判与应急指挥。引入独立的第三方专业安全审计机构，定期对数据治理流程、模型算法稳定性、知识的时效性和全面性、网络安全防护体系、应急响应预案等全面审计。以“监管+审计”的模式推动合规检查转向风险监控，形成战略引领、法规兜底、监管保障的严密制度闭环，提升系统整体的透明度和可信度。

2. 夯实技术防护与基础支撑，打造可信数字底座

先进、可靠、自主的技术体系是应对风险的屏障，必须构建涵盖数据、模型、算力、知识、网络、集控全生命周期的主动免疫和纵深防御技术体系。

（1）实施数据全生命周期治理

推行智能感知终端安全准入、远程标校和可信状态证实，对核心数据和控制指令采用国密算法的端到端加密传输。利用区块链技术对关键数据（如特征水位、调度指令）建立不可篡改的存证和追溯链。部署基于机器学习的异常数据实时检测、修复和数据质量可信度动态评分中间件。推广联邦学习、安全多方计算、可信执行环境等隐私计算技术，实现跨域数据“可用不可见、不出域”。

（2）发展可信AI与模型综合治理体系

优先发展机理—数据融合模型和可解释AI技术，为复杂模型的决策提供归因分析。建立严格的模型供应链安全管理与认证制度，设立国家级或流域级模型测试验证中心，对核心业务AI模型实施强制性安全认证与性能基准测试。研发并部署模型监控与防御工具，实时检测模型输入输出的分布偏移与对抗性样本攻

击,具备模型降级或切换的应急能力。

(3) 建设自主弹性算力与韧性网络

融入国家“东数西算”总体布局,建设“国家算力枢纽—流域算力中心—工程边缘计算节点”三级协同的算力网络。加大国产CPU、GPU、专用加速芯片及仿真软件适配推广。在控制核心区部署基于零信任架构的工业防火墙和访问控制系统,构建覆盖全网的威胁感知和智能防御平台,建立统一的海量物联网终端安全接入网关和终端安全管理平台,实施准入控制、脆弱性扫描和固件升级管理。

3. 推进管理变革与能力建设,适配数智化转型

适配的组织和合格的人才才是驾驭系统的关键,必须同步推动组织架构、业务流程、人才队伍的全面变革,避免出现技术先进、管理滞后“两张皮”现象。

(1) 推动组织重塑与流程再造

整合相关信息化管理部门,设立实体化的数智水利运营中心,融合水利业务、数据科学、模型算法工程和网络安全等跨职能团队,负责系统的日常运营、迭代优化和应急指挥。以数字孪生体能力提升为牵引,系统性重构核心业务流程,将防洪调度等核心流程升级为“实时监测—自动预警—多方案预演—人机协同决策—指令智能下发—效果跟踪反馈”的数字化闭环。

(2) 实施数智人才强基计划

在具备条件的高等院校增设智慧水利交叉学科,培养“水利为体、数智为用”的复合型领军人才和骨干力量。实施现有水利干部职工数智素养提升计划,编制水利干部职工数智能力框架,开展领导干部“数智决策力”、业务骨干“数智应用力”、技术人员“数智创新力”的差异化、滚动式分类分层次培训。设立数智水利首席专家、数据工匠等岗位,完善激励与职业发展通道。

(3) 构建人机协同与知识管理体系

制定颁布数智水利系统人机协同决策管理规定,以风险等级和决策影响范围划定“机主(系统自动执行)、人辅(系统建议、人工确认)、人主(系统辅助、人工决策)”三种模式的适用范围,保留清晰、便捷的人工紧急干预通道。启动数智水利知识工程,构建动态更新的专业知识图谱和案例库,实现行业隐性知识的显性化、体系化传承。

4. 聚焦系统韧性提升,防范集中性崩溃风险

韧性是保证系统在遭受冲击、压力或故障时能够承受、适应、快速恢复并持续交付关键服务的能力,必须从架构设计、常态演练到极端预案进行全面革新。

(1) 设计分层的联邦式混合韧性架构

设计“集中智能、分布自治”的联邦式架构,顶层中心负责全局信息汇聚、宏观战略协调和跨区域优化,关键的下层节点(如大型水利枢纽、重要分洪闸)被赋予基于本地简化可靠模型、实时监测数据和预设规则的“离线自治”能力,在极端情况下能够根据既定程序执行保底的安全操作,并能在相邻节点间实现有限的应急联动。通过系统架构上核心功能模块化解耦,确保单一模块(如洪水预报模块)出现故障时,其他模块(如工程监控模块)仍能独立运行。

(2) 开展常态化攻防演练与压力测试

定期组织数智水利护网专项行动,在完全仿真沙盘环境中对真实系统或其高保真镜像开展高强度、实战化的对抗攻击,模拟数据污染、模型欺骗、知识老旧、网络渗透、控制篡改等复合性致险影响。开展超出设计容量的极限测试(如注入10倍的常态数据洪峰、并发海量控制请求),主动暴露脆弱性,以检验系统的性能边界和崩溃模式,将发现的问题纳入严格整改闭环。

(3) 制定并演练极端情景应急预案

针对数据中心等战略节点,制定涵盖中心物理损毁、大范围断网、核心团队失能、网络攻击等情景的应急预案,明确清晰的分级降级运行路径,规定指挥权转移流程,制定无数字系统支持下的最低限度调度方案。定期进行桌面推演和尽可能真实的实战盲演,确保极端情况下整个体系能够有条不紊地切换至“生存模式”。

四、结 语

本文以数智水利为研究对象,构建了“依赖特性分析—风险类型识别—防控对策设计”系统分析框架,识别了数智技术大规模应用背景下形成的数据、模型、算力、知识、网络、集控的深度依赖特性。这些依赖特性衍生出数据链风险、模型算法风险、算力基础设施风险、知识风险、网络安全风险、集中管控衍生风险等复合型风险,揭示了从虚拟空间向物理世界传导、从技术层面向治理层面蔓延的内在机理,验证了“强依赖特性—复合型风险”的传导逻辑。从顶层设计、技术防护、管理变革、系统韧性4个维度,提出了制度构建、技术防护、人才强基、韧性提升的立体化风险防控体系,可为水利管理部门、工程建设单位及技术研发机构提供可操作的决策参考。

数智水利应用风险研究作为新兴领域,需要在以下方向深化:一是构建数智水利风险量化评估模型,建

立涵盖发生概率、危害等级、耦合强度的多维度风险指标体系;二是探索基于区块链的可信数据与模型共享机制,解决跨域协同中数据主权与信任问题;三是研发水利领域可解释性AI技术,提升模型决策的透明度和可信度;四是建立动态知识更新与验证机制,研发增量学习算法,结合专家审核过滤“伪知识”,保障知识源的权威性与时效性;五是开展典型水利工程的实证研究,验证混合韧性架构与极端预案的实际效果;六是推动跨学科研究,联合法学、伦理学等领域,完善算法责任认定规则与数据隐私保护机制。通过持续推动数智水利应用风险理论创新与实践应用的双向迭代,将数智水利转化为推动水利高质量发展、保障国家水安全的可靠智慧引擎。

参考文献:

- [1] 杨卫.数智力学:驾驭数智时代的力学[J].力学进展, 2024, 54(4):629-638.
- [2] 李国英.推动水利高质量发展 保障我国水安全 为确保基本实现社会主义现代化取得决定性进展作出水利贡献[J].中国水利, 2026(1):1-9.
- [3] Wang Xiaopeng, Wu Biqiong, Zhou Guoliang, et al. How a vast digital twin of the Yangtze River could prevent flooding in China[J].Nature, 2025, 639(8054): 303-305.
- [4] 彭静.水科学数据的未来:赋能国家水安全[J].中国水利, 2024(23):1-6.
- [5] Peng Jing. Digital twin technology and its application in water governance: China's practices and achievements[J].International Journal of Water Resources Development, 2025, 41(5-6):974-989.
- [6] 胡四一.全面推进水利信息化八大重点工程建设[J].中国水利, 2008(19):8-9.
- [7] 邓坚.水利信息化推进“八大重点工程”[J].中国计算机用户, 2009(10):46-47.
- [8] 水利部.水利网络与信息安全体系基本技术要求[A].2010.
- [9] 田宾.水利信息系统的安全设计思考[J].河南水利与南水北调, 2017, 46(8):87-89.
- [10] 周维续.水利信息系统安全保障[J].信息网络安全, 2005(9):56-57.
- [11] 张健.水利信息系统安全设计[J].水利建设与管理, 2009, 29(12):19-23+86.
- [12] 许源.水利信息安全态势感知系统建构及应用[J].海河水利, 2020(4):69-70.
- [13] 陈岚, 詹全忠.水利信息安全管理平台研究与应用[J].水文, 2011, 31(6):67-69+85.
- [14] 许峰, 吕鑫.可信水利信息系统构建研究[J].水利信息化, 2010(5):23-26.
- [15] 刘蒙琦, 尹君逸.水利信息系统的网络安全风险评估与防护措施研究[J].中国宽带, 2025, 21(5):58-60.
- [16] 李存斌, 李小鹏, 田世明, 等.能源互联网电力信息深度融合风险传递:挑战与展望[J].电力系统自动化, 2017, 41(11):17-25.
- [17] 蒋云钟, 冶运涛, 王浩.智慧流域及其应用前景[J].系统工程理论与实践, 2011, 31(6):1174-1181.
- [18] 蒋云钟, 冶运涛, 赵红莉, 等.智慧水利解析[J].水利学报, 2021, 52(11):1355-1368.
- [19] 蒋云钟, 刘家宏, 梅超, 等.智慧水利DIS体系构建研究与展望[J].中国水利水电科学研究院学报(中英文), 2022, 20(6):492-496.
- [20] 冶运涛, 蒋云钟, 梁犁丽, 等.数字孪生流域:未来流域治理管理的新基建新范式[J].水科学进展, 2022, 33(5):683-704.
- [21] 冶运涛, 蒋云钟, 寇怀忠.数字孪生水利建设的进展成效、关键问题与对策举措[J].中国水利, 2026(5):36-45.
- [22] 李文正.数字孪生流域系统架构及关键技术研究[J].中国水利, 2022(9):25-29.
- [23] 蒋云钟, 冶运涛.数字孪生灌区内涵解析及建设思路与关键技术[J].中国水利, 2025(13):24-33.
- [24] 张云姣, 李莹, 葛召华, 等.数据-模型-知识三重驱动在山东省数字孪生水利中的应用[J].中国水利, 2026(9):55-65.

责任编辑 刘磊宁