水利自动化系统网络安全防护与运维管理体系建设

吕文广　葛瑞雪
南水北调中线信息科技有限公司　北京　100038

摘　要：随着水利信息化进程加快，水利自动化系统网络安全面临诸多挑战。本文聚焦水利自动化系统网络安全防护与运维管理体系建设。先阐述建设的必要性，分析系统面临的外部攻击、内部安全威胁及自身安全漏洞等网络安全威胁。接着提出构建纵深防御体系、强化安全监测与预警等网络安全防护策略。最后从智能化状态监测、高效化运维处置等方面探讨运维管理体系建设，旨在通过全面构建安全防护与运维管理体系，保障水利自动化系统安全稳定运行，提升水利行业信息化水平与管理效能。

关键词：水利自动化系统；网络安全防护；运维管理体系

引言：在水利行业信息化进程加速的背景下，水利自动化系统发挥着愈发关键的作用，其涵盖水情监测、水资源调度等诸多核心业务。然而，随着网络技术的广泛应用，水利自动化系统面临的网络安全形势日益严峻，外部黑客攻击、内部人员违规操作以及系统自身安全漏洞等问题频发，严重威胁着系统的安全稳定运行，甚至可能影响水利工程的正常功能，危及社会公共安全。因此，构建一套科学、完善的水利自动化系统网络安全防护与运维管理体系迫在眉睫，这对于保障水利事业可持续发展具有至关重要的意义。

1 水利自动化系统网络安全防护与运维管理体系建设的必要性

在水利行业数字化、智能化加速推进的当下，水利自动化系统已成为保障水资源合理调配、防洪减灾、水生态保护等核心业务高效开展的关键支撑。其涉及大量敏感数据，涵盖地理信息、水文数据以及工程运行参数等，一旦泄露或遭到破坏，将严重影响水利工程的正常运转，甚至危及社会公共安全与稳定。当前网络环境复杂，各类恶意网络行为层出不穷，外部的不法分子可能利用系统漏洞，非法获取数据或干扰系统指令，导致监测数据失真、调度指令错误，使水利工程无法发挥应有作用。内部人员若操作不当或权限管理混乱，也可能引发数据误删、系统故障等问题。此外，系统自身软硬件存在的安全缺陷，在复杂网络环境下，极易成为安全隐患的突破口。因此，构建完善的网络安全防护与运维管理体系，能全方位保障系统安全，提升其可靠性与稳定性，确保水利业务连续性，为水利行业的可持续发展提供坚实有力的网络保障[1]。

2 水利自动化系统面临的网络安全威胁

2.1 外部攻击威胁

在开放的网络环境中，水利自动化系统时刻面临来自外部的多样攻击威胁。随着网络技术的发展，恶意软件传播途径增多，如通过电子邮件附件、恶意网站下载等方式，一旦水利自动化系统相关设备感染，可能导致数据被窃取、系统被控制。网络扫描与探测行为频繁，不法分子利用专业工具对系统进行扫描，试图发现系统开放的端口、服务及存在的漏洞，为后续攻击做准备。此外，分布式拒绝服务攻击（DDoS）也较为常见，攻击者通过控制大量僵尸网络，向水利自动化系统的服务器发送海量请求，使服务器资源耗尽，无法正常响应合法用户的请求，导致系统瘫痪，严重影响水利业务的连续性，如水情监测数据无法及时上传、水资源调度指令无法下达等。

2.2 内部安全威胁

水利自动化系统内部安全威胁同样不容忽视。内部人员可能因疏忽大意，如使用弱密码、随意共享账号密码等，导致账号被非法获取，进而使攻击者能够以合法身份访问系统，窃取或篡改关键数据。部分人员安全意识淡薄，可能会在连接不安全的公共网络时访问系统，增加系统被攻击的风险。同时，存在个别内部人员因利益驱使，主动泄露系统敏感信息，如水利工程的布局、运行参数等，给水利设施的安全运行带来严重隐患。而且，内部权限管理不善，如权限分配不合理、未及时回收离职人员权限等，也可能导致内部人员越权操作，干扰系统的正常运行。

2.3 系统自身安全漏洞

水利自动化系统自身存在多种安全漏洞。硬件方面，部分设备可能因设计缺陷或老化，出现性能不稳定、容易受到电磁干扰等问题，影响数据的准确采集和传输。软件层面，操作系统、数据库管理系统以及应用软件可

能存在未修复的漏洞，如缓冲区溢出漏洞、SQL注入漏洞等，攻击者可利用这些漏洞获取系统控制权或窃取数据。通信协议也存在安全隐患，一些老旧的通信协议缺乏加密和认证机制，数据在传输过程中容易被窃取或篡改。此外，系统集成过程中，不同厂商的设备和应用软件之间可能存在兼容性问题，导致系统出现异常，也为攻击者提供了可乘之机，威胁着水利自动化系统的整体安全[2]。

3 水利自动化系统网络安全防护策略

3.1 构建纵深防御体系

构建纵深防御体系是保障水利自动化系统网络安全的关键举措，它通过多层次、多手段的安全防护，形成立体化的安全屏障。在边界防护层面，部署防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）。防火墙作为第一道防线，依据预设规则过滤进出网络的流量，阻止非法访问；IDS实时监测网络中的异常行为，如异常的数据包传输、频繁的端口扫描等，并及时发出警报；IPS则能主动阻断检测到的攻击行为，防止其对系统造成损害。内部网络中，采用网络分段技术，将水利自动化系统划分为不同的子网，限制子网间的非法访问，降低攻击者在内部网络横向扩散的风险。同时，部署主机安全防护软件，对服务器、工作站等主机设备进行实时监控和防护，防止恶意软件感染和非法操作。此外，建立数据加密机制，对传输和存储的敏感数据进行加密处理，确保数据的保密性和完整性。

3.2 强化安全监测与预警

强化安全监测与预警对于水利自动化系统网络安全而言至关重要，它如同系统的“敏锐触角”，能及时发现潜在的安全威胁并发出警报。在监测方面，需构建全面的监测体系。利用流量监测工具，实时分析网络中的数据流量，识别异常流量模式，如突发的流量激增或异常的通信协议使用，这可能是攻击者发起攻击的迹象。部署主机监测软件，对系统内各主机的运行状态、进程活动、文件访问等进行细致监控，一旦发现异常的主机行为，如不明进程启动、敏感文件被篡改，立即记录并上报。同时，加强对数据库的监测，跟踪数据库的访问操作，防止非法数据查询和修改。预警机制要高效且精准。设定合理的预警阈值，当监测指标超过阈值时，及时触发预警。通过多种渠道发布预警信息，如短信、邮件、系统弹窗等，确保相关人员能第一时间收到通知。此外，建立预警分析模型，对预警信息进行分类和评估，判断威胁的严重程度和影响范围，为后续的应急处置提供准确依据，从而有效保障水利自动化系统的网络安全[2]。

3.3 提升应急响应能力

提升应急响应能力是水利自动化系统网络安全防护中应对突发安全事件的关键环节，关乎能否快速、有效地控制安全危机，减少损失。首先，要制定详细且针对性强的应急预案。明确不同类型安全事件的响应流程、责任分工，涵盖从事件发现、初步处置到全面恢复的各个环节，确保在紧急情况下行动有章可循。其次，组建专业的应急响应团队，成员应具备丰富的网络安全知识和实践经验，定期开展培训和演练，提升团队成员对安全事件的敏感度和处理能力，保证在事件发生时能迅速投入工作。再者，配备必要的应急资源，如备份设备、安全工具软件等，确保在系统遭受攻击或出现故障时，能及时替换受损设备，利用工具进行数据恢复和系统修复。同时，建立与外部安全机构、同行的应急协作机制，在遇到重大安全事件时，可快速获取外部技术支持和经验分享，形成应急处置的合力，保障水利自动化系统尽快恢复正常运行。

3.4 完善安全管理制度

完善安全管理制度是水利自动化系统网络安全的重要基石，为系统安全稳定运行提供坚实的制度保障。在人员管理方面，建立严格的账号与权限管理制度。明确不同岗位人员的系统访问权限，遵循最小权限原则，确保员工仅能访问工作所需资源，防止权限滥用。同时，规范人员入职、离职和调岗时的账号处理流程，及时回收或调整权限，避免出现账号闲置或越权访问的情况。设备管理上，制定设备采购、使用、维护和报废的全生命周期管理制度。对新购设备进行安全评估和检测，确保其符合安全标准；在使用过程中，定期进行设备巡检和维护，及时更新设备固件和软件；设备报废时，进行安全清理，防止数据泄露。此外，建立安全审计和监督机制，定期对系统安全状况进行审计，检查制度执行情况，发现问题及时整改[3]。

4 水利自动化系统运维管理体系建设

4.1 智能化状态监测

智能化状态监测是水利自动化系统运维管理体系建设的关键环节，能实时、精准掌握系统运行状况，为运维决策提供可靠依据。借助先进的传感器技术，在水利自动化系统的各类设备上部署多种类型传感器，如温度传感器、湿度传感器、压力传感器等，实时采集设备的运行参数，像设备的温度变化、振动频率等，全面感知设备的物理状态。同时，利用网络监测工具，对系统的网络流量、通信质量等进行实时监测，及时发现网络拥塞、丢包等异常情况。运用大数据分析和人工智能算法，对采集到的海量监测数据进行深度挖掘和分析。通过建

立数据模型，预测设备可能出现的故障趋势，提前发出预警，实现从“事后维修”到“事前预防”的转变。此外，开发智能化的监测平台，将各类监测数据进行可视化展示，运维人员可通过直观的界面，快速了解系统的整体运行状态，精准定位故障位置，大大提高运维效率和准确性，保障水利自动化系统的稳定运行。

4.2 高效化运维处置

高效化运维处置是确保水利自动化系统稳定运行的核心环节，它能在系统出现故障或异常时，快速响应并解决问题，将影响降到最低。建立标准化的运维流程至关重要。明确从故障发现、报告、分析到处理、验证的每一个步骤，让运维人员清楚知晓在何种情况下该采取何种行动，避免处理过程的混乱和延误。例如，规定在接到故障报警后，运维人员需在多长时间内到达现场，按照怎样的顺序进行故障排查。引入自动化运维工具可极大提升处置效率。利用脚本和自动化程序，实现常见故障的自动修复，如系统服务的自动重启、配置文件的自动修正等。同时，借助远程控制技术，运维人员无需亲临现场，就能对远程设备进行操作和调试，快速解决故障。此外，加强运维团队的建设和培训也不可或缺。定期组织技术培训和应急演练，提高运维人员的专业技能和应急处理能力，确保在面对复杂故障时能够迅速、准确地做出处置，保障水利自动化系统的持续稳定运行。

4.3 常态化评估优化

常态化评估优化是水利自动化系统运维管理体系持续完善、保持高效运行的重要保障。定期开展系统全面的评估工作，从多个维度对运维管理体系进行审视。一方面，评估系统运行性能，通过收集设备运行数据、网络流量信息等，分析系统响应时间、资源利用率等指标，判断系统是否满足水利业务的需求，是否存在性能瓶颈。另一方面，评估运维流程的合理性和有效性，检查运维流程是否清晰、规范，是否存在繁琐环节影响处置效率，以及运维人员是否严格按照流程执行操作。基于评估结果进行针对性优化。对于性能不足的系统设备，及时进行升级或更换；对不合理的运维流程进行简化和改进，提高运维工作的流畅度。同时，根据新技术的发展和水利业务的变化，不断引入新的运维管理理念和工具，提升运维管理的智能化水平。

4.4 资源保障与风险控制

资源保障与风险控制是水利自动化系统运维管理体系建设不可或缺的部分，对系统的稳定运行意义重大。在资源保障方面，要确保人力、物力和财力资源的充足。配备专业且数量合理的运维人员，涵盖系统、网络、设备等多个领域，定期组织培训与技能提升活动，保证其具备应对各类运维问题的能力。储备充足的备品备件，如服务器、传感器等关键设备，以应对突发故障，缩短设备更换时间。同时，安排专项运维资金，用于系统升级、设备维护和新技术引入等，为运维工作提供坚实的经济支撑。风险控制上，全面识别运维过程中可能面临的风险，如设备老化风险、网络攻击风险等。针对不同风险制定相应的应对策略，对于设备老化风险，建立设备健康档案，定期巡检和更换；对于网络攻击风险，加强网络安全防护措施。此外，制定应急预案，开展应急演练，提高应对突发风险的能力，将风险对水利自动化系统的影响降至最低，保障系统的安全稳定运行[4]。

结束语

水利自动化系统的网络安全防护与运维管理体系建设，是保障水利事业稳定发展的关键支撑。通过构建纵深防御体系、强化安全监测预警等举措，筑牢了网络安全防线；借助智能化状态监测、高效化运维处置等手段，提升了运维管理水平。然而，网络安全形势瞬息万变，运维管理需求也在不断更新。未来，我们仍需持续探索创新，紧跟技术发展潮流，不断完善防护与运维体系，以更坚定的决心、更有力的措施，确保水利自动化系统安全稳定运行，为水利行业的可持续发展保驾护航。

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]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,2023(06):115-117+121.

[4]陈亚燕.水电厂信息网络安全防护策略探究[J].网络安全技术与应用,2022,(3):103-104.