水利工程工控系统网络安全及防护设计

孙静

（河北省水务中心　河北　石家庄　050000）

[摘　要]随着计算机和网络技术的发展，水利工程工控系统越来越多地采用以太网方式组网、通用通信协议、windows操作系统、通用硬件和组态软件等，这些通用设备和软件的漏洞将带来极大安全隐患。而在机组运行期间很少能进行漏洞修补，致使控制系统存在明显安全风险。同时无论进口还是国产控制系统，其关键芯片、嵌入式操作系统等仍没有做到自主可控。水利工程工业控制系统在技术和管理两方面都存在较多薄弱点，亟须建立技术与管理并重，具备深度防御能力的安全防护体系，以确保水利工程工业控制系统安全稳定运行。

[关键词]水利工程；工控系统；网络安全；防护设计

【DOI】10.12252/j.issn.2096-627X.2021.07.051

1 项目背景

岗南水库位于海河流域子牙河系滹沱河中游平山县境内，控制流域面积15900平方公里，总库容17.04亿立方米，设计洪水标准为500年一遇，校核洪水标准为10000年一遇，相应泄流分别为11169m^3/s、17955m^3/s，是一座以防洪为主，结合灌溉、供水、发电的大（Ⅰ）型水利枢纽工程，是石家庄市区的重要水源地，担负着石家庄市居民生活用水和工业用水，以及下游地区耕地的供水任务。岗南水库事务中心机房是自动化系统综合管理平台的监控中枢，在水库日常管理及防汛、度汛中发挥着重要作用。现有机房环境存在如下众多问题：缺少安保监控系统、动环监测系统、自动消防灭火系统、新排风系统，另外，网络安全防护系统还不成熟，应有防护设备暂未配置齐全，物理环境缺乏环境监测和预警能力，网络环境存在安全风险漏洞，根据省水利厅网络安全相关要求，需要对现有机房进行提升改造，建设一个安全可靠、功能完备、布局合理、设施先进、投资合理的现代化网络机房，切实为水库关键信息设备提供安全、可靠的运行环境，保障水库枢纽健康运行，同时也为管理维护人员提供安全、高效的管理手段。

2 水利工程工控系统的网络安全现状

2.1技术方案现状

网络结构：虽然水利工控系统网络内部采取了一些安全隔离或访问认证措施，如水平隔离、垂直加密等措施，以提高网络安全性，但仍然缺乏全面有效的网络边界保护，访问加密、身份验证和其他安全保护措施。一些水利工控系统通过网络连接直接连接到办公网络，网络之间没有针线，工控系统的网络访问控制设备和入侵防护设备使工控系统面临嗅探、入侵、，来自办公网络的病毒传播和恶意代码攻击。设备本体：液压工控系统中的工控机、PLC、移动媒体、开关等大部分采用国外品牌。这些设备中存在大量未及时修复或修复的漏洞，并且缺乏必要和有效的保护措施。这些漏洞中的大多数是拒绝服务、远程代码执行和缓冲区溢出。如果这些漏洞被黑客利用，将导致设备故障或非法操作。行为审计：现有的水利工控系统大多缺乏必要的技术手段对工控网络进行监控和审计；未部署监控和审计设备及时监控工控网络中的异常流量；工控系统账目未定期审计，缺乏对非法操作、未授权访问等行为的监控和审计。

2.2运营管理状况

管理机制不完善：管理中忽视预防，缺乏有效的安全策略和管理流程，对工控系统的网络安全构成一定的威胁，如访问控制策略松懈，安全管理人员角色/职责划分不清，工控系统没有分级和记录等。缺乏安全意识：许多水利人员对工控系统信息安全的紧迫性和重要性认识不足，安全意识淡薄，企业工控系统安全风险评估不足，防范措施单一，技术和资金投入不足。

3 水利工程工控系统网络安全及防护设计

3.1网闸主要技术

①采用2+1系统架构即内网单元+外网单元+FPGA专用隔离硬件；②机箱要求：2U标准机架式机箱，冗余电源；③物理接口：不少于6个10/100/1000MBASE-TX接口；④并发连接数≥2万；⑤最大吞吐量≥500Mbps；⑥系统延时<1ms；⑦可实现双向文件传送，支持自定义的、TCP/UDP的数据隔离交换；⑧支持HTTPS的Web方式管理，可实时监控CPU、内存、硬盘、网络流量等状态；⑨系统提供ping，traceroute，TCP端口探测、抓包等工具方便管理员在配置策略或调整网络时排查问题。

3.2防火墙主要技术

①1U机架空间；②支持中英文管理Web界面；③最大并发连接数≥400万；④吞吐量≥4Gbps；⑤每秒新建连接数≥7万；⑥最大并发连接数≥400万；⑦千兆Combo接口≥8，万兆光口≥2，SSLVPN并发数≥1000IPSecVPN隧道≥1000；⑧具有未知威胁的检测能力，能够基于时间、用户、用户组、安全组、应用层协议、IP地址、端口等进行安全策略配置；⑨支持静态路由，策略路由；⑩支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、ORACLE、MSSQL）的口令暴力破解防护功能。

3.3入侵防御系统主要技术

①双冗余电源，≥4个千兆电口，≥4个千兆光口；②内置特征防御事件数量不少于4000条，并支持手动或自动升级，含3年特征库升级许可；③支持主动防御拦截黑客攻击、蠕虫、

网络病毒、Dos/DDoS等恶意流量；④支持透明部署在业务网关键链路；⑤支持统计分析、直观展示，中文管理Web面板；⑥整机吞吐率≥10GbpsIPS吞吐率≥1Gbps；⑦最大并发连接数≥100万；⑧支持基于IP地址、应用、地理位置、时间段等对象下发指定的安全策略；⑨支持URL关键字检测及阻断，日志告警等。

3.4堡垒机主要技术

①实配管理的设备节点数≥100；②标准2U专用千兆硬件平台，千兆电口≥6个；支持2个扩展插槽，支持扩展2*10GE光口，最大支持12个网口，1+1冗余电源；③支持常用的运维协议：SSH、TELNET、FTP、SFTP、rlogin；可通过应用发布的形式进行协议扩展；④支持用户多角色划分功能，可对各类角色进行细粒度的权限管理；⑤支持用户批量导入导出，分组；⑥支持用户安全策略功能；⑦支持通过堡垒机页面对本地客户端应用的配置和直接调用；⑧支持对运维操作会话的在线监控，实时阻断、操作命令记录、操作内容；⑨内置丰富的报表统计模板并支持导出。

3.5日志审计系统主要技术

①支持日志备份机制；②系统配置冗余交流电源；③系统含应包含1个RJ45串口，≥2×GE管理口。≥4个100/1000M自适应以太网接口，≥1个接口扩展槽；系统SATA硬盘容量应≥4TB，支持扩容；④支持≥100个日志源接入；支持的最大设备节点数≥3000个；⑤系统支持可扩展日志源接入数量；⑥系统应支持不少于每秒9000EPS的日志解析能力；⑦系统支持采集的日志范围包括不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等；⑧系统支持的数据采集方式包括但不限于SYSLOG、SNMPTrap、FTP、ODBC、JDBC、专用Agent等方式采集日志；⑨支持海量数据的收集、保存、快速检索能力；⑩支持界面化配置；⑪支持网络环境下的agent部署模式；⑫支持日志全文检索、模糊检索。

3.6漏洞扫描主要技术

①标准1U机型，具备≥4个千兆电口，内置硬盘容量≥1T，含3年漏洞库升级许可；②具体系统扫描、Web扫描、数据库扫描功能，可扫描主机数≥512个；③支持≥10个并发任务，支持≥60个并发主机扫描；④支持已建任务的复制、再编辑，快速生成新任务，包括扫描目标、扫描策略、任务调度、扫描参数；⑤支持对windows系列、Linux、国产化系统等目标主机的系统进行扫描；⑥支持断点续扫功能；⑦支持主流数据库的漏洞的检测：Oracle、SQLserver、MySQL、DB2等；支持数据库登录扫描，包括数据库账号、密码、数据库名称、实例名称及实例号等登录选项的设置；⑧支持Web登录扫描；⑨支持预警功能、扫描风险图显示、支持日志存储告警；⑩支持自动或人工方式，远程或本地升级漏洞库，支持本地升级系统自身版本和补丁程序。

3.7Web应用防护主要技术

①标准机架式WAF硬件设备；冗余电源，吞吐率≥1000M，最大http吞吐量≥500M，设备最大HTTP并发连接数≥200万；②提供1个10/100M管理接口，4个10、100、1000M以太网网口、4个SFP接口。端口总数应支持≥10个；③支持针对基于HTTP/HTTPS协议的蠕虫攻击、木马后门、间谍软件、网络钓鱼等行为进行检测与防护；④内置Web应用防护事件库，并提供定期升级，能够针对最新及热点Web攻击事件进行快速响应；⑤支持针对重点URL的网页防篡改功能；⑥支持基于URL的应用层访问控制功能；⑦支持多设备拓扑显示功能；⑧能够对Web系统主流的应用层攻击（如SQL注入和XSS攻击、CRSF攻击）进行检测防护。

3.8网络安全监控审计

在水利工控系统的通信层、监控层、本地层旁路部署监控审计平台，对网络通信流量进行监控，判断存在的风险因素和威胁。在内网运行中，审计平台主要实现对非法采集生产数据、恶意篡改数据、恶意攻击、非法操作等不良行为的判断和审计，并在第一时间发出报警提示相关人员处理。此外，审计平台还具有恢复事件和提供线索的能力，为网络安全管理人员的工作提供参考，并在发现攻击和非法操作时自动报警。

3.9安全集中监控

液压工控系统网络安全设备在安全监控平台的支持下，实现安全监控与运维一体化。此时，依托监控平台，现场安防设备可以完成对威胁情报信息的实时采集和分析。与安全分析模型相结合，可以实现全局安全预警和策略动态适应的效果。同时，可自动发出现场安全报警，指导运维管理人员在第一时间进行处理，实施及时的安全防护响应，达到更好的水利工控系统网络防护效果。

结论

当前水利工程工业控制系统的安全防护仍较为薄弱，难以抵御网络攻击、恶意代码入侵等威胁。由于这类系统直接涉及防洪、航运、调水等公共利益，一旦发生安全事件，影响巨大，因此需要采取管理和技术措施，研究并实施网络安全技术防护措施、建立深度防御安全体系、落实网络安全制度，提高水利工程工业控制系统网络安全保障能力。

参考文献

[1]郭江，张志华，付志远等.水库大坝安全监测监控系统网络安全风险评估及防护技术解决方案[J].水电站机电技术，2019，42（07）：41-43.

[2]杨旭，谢丰，任旭诚.水利工程工业控制系统网络安全研究[J].水利信息化，2019（03）：20-23.