核电站实物保护系统网络安全体系构建研究

潘航，王鼎业
国核示范电站有限责任公司，山东 荣成 264300

DOI:10.61369/ETQM.2026010027

摘　　要： 随着工业互联网与信息技术的深度融合，核电站实物保护系统的网络安全已成为关乎国家能源安全与公共安全的核心议题。本文系统分析了当前核电站实物保护系统在设备、人员与系统配置等方面所面临的网络安全挑战，提出从设备安全加固、人员管理策略和系统配置防御三个层面构建综合防护体系。具体措施包括采用安全认证设备、实施全生命周期设备管理、强化物理安全措施；开展体系化网络安全教育、实行基于最小权限的访问控制、建立常态化审计机制；推进网络隔离与分段、强化多因素认证与通信加密、实施系统化漏洞与补丁管理等。

关 键 词： 核电站；实物保护系统；网络安全；纵深防御；访问控制；安全审计

Research on the Construction of Cybersecurity Architecture for the Physical Protection System in Nuclear Power Plants

Pan Hang, Wang Dingye
State Nuclear Power Demonstration Plant Company Ltd., Rongcheng, Shandong 264300

Abstract: With the deep integration of industrial internet and information technology, cybersecurity in nuclear power plant physical protection systems has become a critical issue concerning national energy security and public safety. This paper systematically analyzes the current cybersecurity challenges faced by nuclear power plant physical protection systems in terms of equipment, personnel, and system configuration, proposing a comprehensive protection framework from three dimensions: equipment security reinforcement, personnel management strategies, and system configuration defense. Specific measures include adopting security-certified devices, implementing lifecycle management of equipment, and strengthening physical security measures; conducting systematic cybersecurity education, enforcing access control based on least privilege, and establishing regular audit mechanisms; promoting network isolation and segmentation, enhancing multi-factor authentication and communication encryption, and implementing systematic vulnerability and patch management.

Keywords: nuclear power plant; physical protection system; network security; defense in depth; access control; security audit

引言

核电站作为国家能源战略的重要支柱，其安全性具有极高的公共性与政治敏感性。实物保护系统是保障核材料与核设施免遭盗窃、破坏与非法转移的核心技术手段。然而，在数字化、网络化转型的浪潮下，传统的、相对封闭的实物保护系统正日益与工业控制网络、管理信息系统集成，这在提升运营效率的同时，也使其暴露在更为复杂的网络攻击威胁之下。从震网（Stuxnet）病毒到针对关键基础设施的勒索软件攻击，历史事件一再警示我们，网络安全已成为实物保护系统不可分割的组成部分。近年来，随着5G、物联网等新技术在核电站的广泛应用，系统互联程度不断提高，网络攻击面持续扩大，使得实物保护系统面临的安全形势更加严峻。本文旨在超越泛泛而谈的安全原则，从设备、人员、配置三个实操层面入手，构建一个多层次、可落地的网络安全加固框架，以应对日益严峻的混合型安全威胁。

一、设备层面的安全加固：构筑硬件基石

设备是实物保护系统的物理载体，其安全性是整个体系的基石。在数字化、智能化转型的背景下，设备安全不仅包括传统的物理防护，更需要关注其作为网络节点的安全性[1]。

（一）采用经过安全认证的专用设备

在设备选型阶段，应优先采购符合国家等级保护制度与行业安全规范（如IEEE 802.1X, IEC 62443）的产品。对于核心组件

作者简介：潘航（1994.08-），男，陕西咸阳人，本科，中级，研究方向：实物保护，通讯。

（如门禁主控制器、交换机、服务器、网络安全设备等），应选用经过严格渗透测试与可靠性认证的工业级产品，从源头降低因设备固有漏洞导致的安全风险[2]。具体而言，门禁主控制系统应采用通过国家安全认证的专用设备，具备防拆解、防篡改等物理防护特性。视频监控设备应选用具备加密传输、完整性校验等功能的产品，防止视频数据被窃取或篡改。周界入侵检测设备应具备抗干扰、防欺骗能力，确保报警信息的真实性和可靠性。此外，所有设备在投入使用前，都应经过严格的安全测试，包括但不限于渗透测试、漏洞扫描、性能测试等，确保设备在各种工况下都能稳定可靠运行[3]。

（二）实施全生命周期的设备安全管理

设备安全并非一劳永逸。应建立设备资产清单与安全档案，对每一台入网设备进行登记。定期（如每季度）执行安全扫描与健康状态评估，及时更新设备固件与嵌入式操作系统补丁。对于到达生命周期末期（End-of-Life）且无法获得安全更新的设备，必须制定严格的隔离或替换计划。在设备运行维护阶段，要建立完善的运维管理制度，包括定期巡检、预防性维修、标准故障处理等流程。对于关键设备，还应建立冗余备份机制，确保单点故障不会影响系统整体运行。设备退役时，要严格执行数据销毁流程，确保存储的敏感信息得到彻底清除。同时，要建立设备供应链安全管理机制，对设备供应商进行安全评估，确保设备从源头上就是可信的[4]。

（三）强化配套的物理安全措施

网络安全需以物理安全为前提。部署实物保护系统的网络设备、服务器机柜及通信线路应置于受控区域，通过视频监控、生物识别门禁、防篡改机箱等措施，防止未经授权的物理接触。关键网络节点应考虑采用光纤通信以增强抗电磁干扰与窃听能力[5]。具体而言，服务器机房应按照最高安全等级进行建设，配备门禁系统、视频监控、入侵报警等多重防护措施。网络设备间要实行严格的出入管理，所有进出记录都要完整保存。室外设备箱要采用防破坏设计，并设置周界报警装置。对于重要的网络线路，要采用管道敷设、桥架封闭等物理防护措施，防止线路被搭接或破坏。此外，还要定期对物理安全设施进行检查测试，确保其始终处于良好工作状态[6]。

二、人员管理的安全策略：管控人为风险

人是网络安全中最活跃的因素，也是最薄弱的环节。统计数据显示，超过70%的安全事件都与人为因素有关。因此，建立完善的人员安全管理体系至关重要。

（一）开展体系化的网络安全意识教育

定期举办针对所有员工的网络安全培训，内容应覆盖社会工程学攻击（如钓鱼邮件）、密码安全、数据保护法规等。培训不应流于形式，可通过模拟钓鱼攻击、红蓝对抗演练等方式检验培训效果，并将结果纳入绩效考核。培训计划应当系统化、常态化，新员工入职必须接受基础网络安全培训，在职员工每年至少参加一次复训[7]。对于不同岗位的员工，培训内容应有所侧重。例如，系统管理员需要深入理解系统安全配置和漏洞管理，而普通员工则更需要掌握基本的安全操作规范。此外，还要通过海报、内部网站、定期通报等多种形式，持续强化员工的安全意识，使网络安全成为企业文化的重要组成部分。

（二）实行基于最小权限原则的访问控制

必须建立并严格执行基于角色的访问控制（RBAC）模型。确保员工只能访问其职责所必需的系统资源和数据。对特权账户（如系统管理员）的管理应尤为审慎，推行"双人原则"和操作日志审查，防止权限滥用。访问权限的分配应当遵循"按需知密"原则，根据岗位职责和工作需求动态调整。对于敏感操作，如系统配置变更、核心数据访问等，要实施多级审批和操作留痕。特权账户要实行严格管理，包括定期更换密码、限制使用范围、监控使用行为等[8]。对于第三方人员访问，要建立专门的管理制度，通过临时账户、行为审计等措施，确保其访问行为可控可溯[9]。

（三）建立常态化安全审计与问责机制

部署安全信息与事件管理（SIEM）系统，对全网的登录行为、配置变更、数据访问等操作进行集中日志采集与分析。审计记录应妥善保存不少于6个月，以便在发生安全事件时进行追溯与取证，并形成明确的责任认定。审计内容应当全面覆盖网络设备、安全设备、服务器、应用系统等各个环节[10]。对于关键系统和数据，要实施更加细致的审计策略，记录完整的操作轨迹。审计分析要智能化、自动化，通过建立异常行为模型，及时发现可疑操作。审计结果要定期向管理层报告，重大安全事件要立即上报。同时，要建立完善的责任追究制度，对违规操作要严肃处理，形成有效的震慑力[11]。

三、系统配置的纵深防御：构建技术屏障

科学合理的系统配置是抵御网络攻击的最后一道技术防线。在系统层面实施纵深防御策略，可以最大限度地提高攻击者的入侵成本，有效保护核心资产安全。

（一）实施严格的网络隔离与分段

遵循"纵深防御"理念，通过部署防火墙、网闸等设备，将实物保护系统网络与办公网、互联网进行逻辑或物理隔离。在实物保护系统内部，进一步根据安全等级进行VLAN划分或微隔离，将门禁、周界报警、视频监控等子系统分隔开来，即使某一区域被突破，也能有效遏制攻击横向移动。网络隔离策略应当细化到功能模块级别，例如，将管理平面、控制平面和数据平面进行分离。对于特别敏感的系统，如门禁控制服务器，可以考虑采用物理隔离措施。同时，要严格控制网络跨区访问，只有经过严格审批的业务流量才允许穿越安全区域边界。所有跨区访问都要经过防火墙等安全设备的检查，并记录完整的访问日志[12]。

（二）强化多因素认证与通信加密

在所有关键系统的访问入口（如管理后台、远程维护通道）强制实施多因素认证（MFA），结合密码与动态令牌、生物特征等因素。系统内部各组件之间的数据传输，必须采用国密算法或AES等高强度加密协议，防止数据在传输过程中被窃取或篡改。

认证机制要依据系统的重要程度设置不同的安全等级，对于核心系统的管理员登录，应当采用硬件令牌或生物特征等更高安全等级的认证方式。通信加密要覆盖所有网络层次，包括网络层的 IPSec VPN、传输层的 TLS/SSL以及应用层的报文加密。加密密钥要实行严格的生命周期管理，定期更换并安全存储。对于无线通信，要采用 WPA3等最新安全协议，防止无线信号被窃听或干扰。

（三）推行系统化的漏洞与补丁管理

建立漏洞预警与响应机制，主动跟踪国家漏洞库（CNNVD）及设备厂商发布的安全公告。对补丁安装前需在测试环境中进行充分验证，以确保其与现有系统的兼容性。对于无法立即打补丁的漏洞，应制定并实施临时性的缓解措施。漏洞管理应当形成完整闭环，包括漏洞发现、评估、处置、验证等环节。要定期开展系统性的漏洞扫描和渗透测试，重点检查对外服务端口、Web应用、数据库等常见攻击面[14]。补丁管理要分级分类，根据漏洞的危害程度和影响范围，制定不同的修复时限。对于生产环境中的关键系统，补丁安装要选择业务低峰期，并做好完整的系统备份和回退预案。同时，要建立漏洞信息共享机制，及时获取行业内的最新威胁情报，提前做好防护准备[13]。

四、结论

核电站实物保护系统的网络安全是一个动态的、持续对抗的过程，它并非单一技术或管理措施的简单叠加，而是一个需要设备、人员、配置三者协同作用的系统工程。本文提出的加固策略，旨在构建一个从硬件到软件、从技术到管理的立体化防御体系。通过设备层面的安全加固，可以确保系统运行的物理基础安全可靠；通过人员管理的安全策略，能够有效防范人为因素导致的安全风险；通过系统配置的纵深防御，可以建立起多层次的技术防护屏障。这三个层面相互支撑、相互补充，共同构成了完整的网络安全防护体系。未来，随着人工智能、威胁情报等技术的发展，核电站实物保护系统的网络安全防御体系必将向更加智能化、主动化的方向演进。通过引入基于机器学习的异常检测、自动化响应处置等新技术，可以进一步提升系统的安全防护水平。同时，还要加强网络安全人才培养，完善应急响应机制，建立常态化的攻防演练制度，不断提升系统的整体防护能力。只有通过技术和管理并重、防护与检测并举的综合防控措施，才能构建起无时不有、无处不在的防护能力，为国家核安全提供坚不可摧的保障。

参考文献

[1]国家能源局 . 电力行业网络安全管理办法 [S].2022.

[2]肖立新 , 王鹏 . 核电站工控系统网络安全防护体系研究 [J]. 核科学与工程 , 2021, 41(3): 654-660.

[3]刘畅 , 李哲 . 基于 IEC 62443的工业控制系统安全体系构建 [J]. 自动化博览 , 2020, 37(5): 78-83.

[4]张强 , 周磊 . 核设施实物保护系统与信息安全的融合策略 [J]. 核安全 , 2019, 18(4): 58-64.

[5]赵雨薇 , 陈建国 . 多因素认证技术在关键信息基础设施中的应用研究 [J]. 信息安全研究 , 2022, 8(2): 45-51.

[6] International Atomic Energy Agency. Computer Security at Nuclear Facilities[R]. Vienna: IAEA, 2021.

[7]王志军 , 杨光 . 纵深防御策略在电力监控系统安全中的应用 [J]. 电力系统自动化 , 2018, 42(14): 165-171.

[8]胡海峰 , 徐明 . 核电站网络安全审计与日志分析技术研究 [J]. 现代电子技术 , 2020, 43(21): 112-116.

[9]罗晓丹 , 郑毅 . 工业互联网背景下核电站设备安全管理研究 [J]. 中国安全科学学报 , 2021, 31(9): 132-138.

[10]黄海波 , 刘伟 . 核电厂网络安全漏洞全生命周期管理实践 [J]. 核动力工程 , 2019, 40(6): 120-125.

[11]国家计算机网络应急技术处理协调中心 .2022年我国网络安全态势报告 [R]. 北京 : CNCERT, 2023.

[12]冯建军 , 董磊 . 社会工程学攻击防范与员工安全意识培养 [J]. 信息网络安全 , 2020, 20(7): 88-94.

[13]李明 , 张华 . 核电站网络安全防护技术研究进展 [J]. 核安全 , 2022, 21(2): 45-51.

[14]王磊 , 刘洋 . 工业控制系统安全防护体系研究 [J]. 自动化仪表 , 2021, 42(4): 78-82.

