 DOI: https://doi.org/10.12345/dlynyqy.v3i11.33444

Research on safety risk assessment and protection strategy of power plant information system operation and maintenance

Juncheng Song

Huadian International Power Co., Ltd., Tianjin Development Zone Branch, Tianjin, 300270, China

Abstract

The intelligent transformation of power plants under Industry 4.0 has broken the physical isolation between production and management systems, posing severe cybersecurity challenges. This paper systematically discusses the significance, risk assessment, and protection strategies for the operational security of power plant information systems. The research holds practical value in ensuring production continuity, protecting data, and meeting compliance, alongside theoretical significance for enriching industrial control security frameworks. A systematic risk assessment process covering identification, analysis, and evaluation is constructed. Based on the findings, a multi-layered protection system integrating technology, management, and personnel is proposed, aiming to provide an effective path for securing critical infrastructure and ensuring stable energy supply.

Keywords

Power Plant information system; Operational Security; Risk Assessment; Multi-layered Protection

发电厂信息系统运维安全风险评估与防护策略研究

宋珺琤

华电国际电力股份有限公司天津开发区分公司，中国 · 天津 300270

摘　要

随着工业4.0发展，发电厂智能化转型打破了生产与控制系统的物理隔离，使其面临严峻网络安全挑战。本文系统探讨了电厂信息系统运维安全的研究意义、风险评估与防护策略。研究在保障电力生产、保护数据及满足合规方面具实践价值，并对深化工控安全理论具理论意义。文章构建了涵盖风险识别、分析与评价的系统性评估流程，并据此提出了融合技术、管理、人员三位一体的纵深防护体系，旨在为筑牢电厂基础设施安全防线、保障能源稳定供应提供有效路径。

关键词

发电厂信息系统；运维安全；风险评估；纵深防护

1 引言

随着工业 4.0 时代与能源革命的深入推进，云计算、大数据、物联网等新一代信息技术与发电生产过程的融合日益紧密，驱动着电厂向数字化、智能化方向加速转型。这一趋势在提升生产效率与管理精细度的同时，也彻底打破了发电厂信息系统，尤其是生产控制大区与管理信息大区之间传统的物理隔离边界。使得原本相对封闭、稳定的工业控制系统暴露在更为开放、复杂的网络环境之中，面临来自互联网的网络攻击、病毒渗透、数据篡改等安全威胁的严峻挑战。近年来，国内外因信息安全事件导致的电力生产事故屡见不鲜，充分暴露出电厂信息系统在运维安全管理上的脆弱性。在此背景下，仅依靠传统的、静态的边界防护已不足以应对日益演进的威胁。因此，如何系统性地开展运维安全风险评估，并据此构建一套覆盖技术、管理与人员的动态、纵深防护体系，已成为保障电厂安全、稳定、经济运行，乃至维护国家关键信息基础设施安全的迫切课题。本文旨在结合电厂信息运维实践，对此展开深入探讨。

2 发电厂信息系统运维安全研究意义

2.1 实践意义

发电厂作为国家关键信息基础设施的核心组成部分，其信息系统的稳定运行直接关系到电网安全、能源供应和社会稳定。随着“两化融合”的深入推进，发电厂的生产控制系统（如 DCS、SIS）与管理信息系统（如 MIS、ERP）的互联互通日益紧密，这使得传统封闭的工业控制环境面临前所未有的安全挑战。研究信息系统运维安全，其首要实践意义在于保障电力生产的连续性和可靠性。通过系统性的风险评估与防护，能够有效预防因网络攻击、系统故障或人为误

【作者简介】宋珺琤（1980–），男，中国河北保定人，硕士，工程师，从事控制工程专业研究。

操作导致的生产中断、非计划停运甚至设备损坏等重大事故，确保发电过程的稳定可控。其次，它有助于保护核心生产数据与商业机密。发电厂的运行参数、设备状态、燃料信息、报价策略等数据是企业的核心资产，一旦泄露或被篡改，将造成巨大的经济损失和竞争优势丧失 [1]。最后，健全的运维安全体系是满足国家法律法规和行业监管要求（如《网络安全法》、《关键信息基础设施安全保护条例》、电力监控系统安全防护规定）的必然选择，能够帮助企业规避合规风险，履行社会责任。

2.2 理论意义

从理论层面看，本研究是对工业控制系统安全理论在电力这一特定垂直领域的深化与拓展。传统信息安全理论（如 CIA 三元组：保密性、完整性、可用性）在工控环境中，其优先级往往需要调整，可用性通常被置于最高位。本研究通过探索发电厂信息系统运维安全的特殊规律，有助于丰富和发展工业互联网安全框架和关键基础设施防护理论。同时，发电厂信息系统是一个典型的“人 - 机 - 环 - 管”复杂系统，其安全风险是技术漏洞、管理缺陷和人员因素耦合作用的结果。本研究通过构建涵盖风险识别、分析、评价的全流程风险评估模型，并集成技术、管理、人员三位一体的防护策略，能够为复杂系统安全工程理论提供鲜活的案例支持和模型验证。此外，该研究还能推动安全运维（SecOps）理念在重工业领域的落地实践，探索如何将动态、自适应的安全能力无缝嵌入到日常的 IT 与 OT 运维流程中，形成理论指导实践、实践反哺理论的良性循环。

3 发电厂信息系统运维安全风险评估

风险评估是构建安全防护体系的基础和前提，其科学性与系统性直接决定了后续防护策略的有效性。

3.1 风险识别

风险识别是发现、列举和描述风险要素的过程。在发电厂信息系统中，风险识别应覆盖所有资产、威胁和脆弱性。资产识别方面，需全面梳理包括过程控制层（如 DCS、PLC）、生产监控层（如 SIS）、经营管理层（如 ERP、OA）的硬件（服务器、工作站、网络设备、控制器）、软件（操作系统、数据库、应用软件）和数据（实时数据库、历史数据、操作指令）。威胁识别则需聚焦于内部威胁（如运维人员的误操作、越权访问、恶意破坏）和外部威胁（如网络攻击、病毒木马、APT 攻击、自然灾害）。特别需要关注的是通过管理信息网渗透至生产控制网的“摆渡”攻击。脆弱性识别则需通过技术扫描、渗透测试、配置核查、审计日志分析等手段，发现系统存在的技术漏洞（如未打补丁的操作系统、默认口令、不安全的通信协议）和管理短板（如职责不清、应急预案缺失、访问控制策略宽松）

3.2 风险分析

风险分析是对识别出的风险要素，评估其可能造成的影响以及发生的可能性。这是一个定性与定量相结合的过程。对于可能性分析，可以结合历史安全事件统计数据、威胁源的动机和能力、脆弱性的被利用难度以及现有控制措施的有效性进行综合判断。例如，针对“运维人员使用 U 盘导致病毒传入控制网”这一风险，其可能性取决于 U 盘管理制度的严格程度和技术的隔离措施。对于影响分析，则需从安全三要素（保密性、完整性、可用性）出发，评估风险一旦发生对发电生产业务造成后果的严重程度。例如，控制服务器感染病毒导致系统宕机，其影响是“灾难性的”，直接导致机组非停；而办公电脑中毒，其影响可能仅为“轻微的”。通过构建风险矩阵，将可能性和影响进行组合，可以初步对风险进行等级划分（如高、中、低），为后续的风险评价和处置提供依据。

3.3 风险评价

风险评价是将风险分析的结果与既定的风险准则进行比较，以确定哪些风险需要处理以及处理的优先顺序。在这一阶段，需要企业决策层和安全管理人员共同参与，确定一个可接受的风险阈值。对于那些被评价为“高风险”和“中风险”的项，必须制定相应的风险处置计划。例如，对于“外部黑客通过防火墙薄弱点入侵 SIS 系统并篡改运行参数”这一极高风险，必须优先投入资源进行处置。而对于“办公网某终端设备密码强度不足”这一低风险，则可以列入长期改进计划。风险评价的输出是一份经过优先级排序的《风险处置计划》，它直接指导下一阶段防护策略的制定与实施，确保将有限的安全资源投入到最需要、最关键的领域，实现安全投入效益的最大化 [2]。

4 发电厂信息系统运维安全防护策略

基于风险评估的结果，构建“技术、管理、人员”三位一体的纵深防护体系，是提升发电厂信息系统运维安全水平的根本途径。

4.1 技术防护策略

技术防护是构建安全防线的硬实力。首先，必须坚持“安全分区、网络专用、横向隔离、纵向认证”的电力监控系统安全防护基本原则。通过部署工业防火墙、网闸等设备，严格隔离生产控制大区与管理信息大区，并在控制区内根据不同业务功能进行更细粒度的逻辑分区。其次，构建纵深防御体系：在网络边界部署下一代防火墙、入侵检测 / 防御系统；在主机层面实施白名单机制、加固操作系统、及时安装安全补丁（需经过严格测试）；在应用层面加强代码安全、对数据库进行加密和访问控制。最后，应建立统一的安全运维中心，利用安全信息和事件管理系统对全网的日志、流量和告警进行关联分析，实现安全态势的可视化感知和威胁的快速响应，变被动防御为主动预警。天津开发区分公司 MIS 信息管理系统网络结构分为外联区、核心区、办公区、信息安全区、服务器区，核心设备包括深信服防火墙

（V8.0 系列）、博达 S6800 06E 核心交换机、深信服态势感知（V3.0.64）、杭州盈高科技 ASM6300 AS 准入系统等；服务器搭载 Windows2012 6.2.9200 操作系统、SQL Server 13.0.1601.5 数据库、Tomcat 7.0.90 中间件等等。病毒库及入侵防护规则库及时更新、部署堡垒机等集中管理平台、业务数据本地备份、服务器安装防病毒软件，核心交换机采用 HTTPS 等国家认可加密技术保证通信完整性、及时更新病毒库与防护规则库、部署日志审计平台集中管理日志（留存 180 天）、为服务器安装防病毒软件并更新病毒库、配置终端本地备份策略（每周全量备份）及业务数据异地备份、部署可信验证组件。

4.2 管理防护策略

“三分技术，七分管理”，健全的管理体系是技术措施有效落地的保障。首先，应建立系统化的信息安全管理制度体系，包括但不限于：《信息安全总体方针》、《网络安全管理制度》、《账号与权限管理制度》、《变更管理制度》、《数据备份与恢复制度》和《应急预案》。其次，要强化运维过程的标准化与规范化。严格实行账号、权限的分级分权管理，遵循最小权限原则；对所有系统变更、网络接入实行严格的审批流程；定期进行安全配置核查和漏洞扫描；建立完善的数据备份与灾难恢复机制，并定期组织演练。最后，要建立持续的监督与改进机制。通过定期的内部审核和管理评审，检查各项安全策略和制度的执行情况，并根据风险评估的动态变化和业务发展需求，持续优化安全管理体系。定期开展漏洞扫描、外来计算机或存储设备接入必须做病毒检查、安全设计方案需要专家论证批准意见、形成正式恶意代码检查报告、对应用安全性进行测试评估；细化防火墙访问控制策略（端口级颗粒度、白名单部署）、定期开展漏洞扫描并修补漏洞、外来设备接入前强制病毒检查、完善安全设计方案专家论证及恶意代码检查流程、每年开展第三方安全评定、按《电力数据安全管理办法》修订制度 [3]。

4.3 人员防护策略

人是安全中最关键也最薄弱的环节。人员防护策略的核心在于提升全员的安全意识和技能。第一，开展常态化、分层次的安全培训与意识教育。对高层管理人员，侧重于安全战略和合规要求的宣贯；对 IT 和 OT 运维人员，侧重于安全技术、操作规范和应急响应技能的培训；对普通员工，则侧重于基本的安全意识教育，如密码安全、钓鱼邮件防范等。第二，明确岗位安全职责，将安全责任落实到人，并纳入绩效考核体系，建立奖惩机制。第三，加强对第三方人员的管理，包括供应商、承包商等，必须通过签署保密协议、进行背景审查、限制其访问权限、监控其操作行为等方式，严格控制其带来的安全风险。通过营造“网络安全，人人有责”的企业安全文化，将安全内化为每一位员工的自觉行动。重命名系统默认账户、设置密码复杂度（含字母 / 数字 / 特殊字符）及 90 天定期更换规则、限制管理员远程登录 IP、按三权分立原则划分账户权限、强化岗位安全责任清单执行、开展工业控制系统安全实操培训，按最小权限划分审计员 / 管理员 / 安全员账户、默认账户（root/admin 等）重命名、配置密码复杂度及定期更换策略、管理员远程登录地址需要限制、终端 / 数据库需要设置登录超时及失败处理功能。

5 结语

综上所述，发电厂信息系统的运维安全是一个动态、复杂的系统工程。本文从研究意义出发，系统阐述了对其进行安全风险评估与防护策略研究的理论与实践价值。进而，通过风险识别、风险分析、风险评价三个步骤，构建了一套科学的风险评估流程。最后，基于评估结果，提出了融合技术、管理、人员三个维度的纵深防护策略体系。面对日益严峻的网络安全形势，发电企业必须树立动态、综合的防护理念，将信息安全与生产安全置于同等重要的地位，持续完善安全体系，强化运维能力，方能筑牢电力关键信息基础设施的安全防线，为社会的稳定运行和经济的持续发展提供坚实可靠的能源保障。对电厂快速排查安全漏洞、减少系统瘫痪 / 数据泄露等事故、降低经济损失、保证电力生产连续、满足行业安全资质审核要求、增强新型电力系统构建竞争力，充实能源行业信息系统运维安全理论架构、创建技术 - 管理 - 人员三维风险评价体系、打破“技术为主、管理为辅”传统认知、为电力及石油化工等流程工业提供可复用研究框架。同时验证电厂现有安全防护体系有效性、明确整改方向、保障系统符合网络安全等级保护二级要求、支撑能源数字化转型安全根基，满足《电力数据安全管理办法》《信息安全等级保护管理办法》等法规要求，为后续安全资质复核、行业安全审核奠定基础。

参考文献

[1] 杨春芳.基于物联网技术的发电厂智能运维系统设计改造研究[J].价值工程,2024,43(29):28-30.

[2] 张露,钱波安,陆习良.发电厂电力监控系统网络安全关键技术研究[J].云南水力发电,2022,38(S1):95-96+100.

[3] 吴永存.移动式发电厂工控系统安全运维装置的研制[J].自动化博览,2020,(10):108-111.