智慧电厂环境下热工控制系统信息安全防护策略研究

邵新玉

新疆天富能源股份有限公司天河热电分公司 新疆维吾尔自治区 石河子 832000

【摘　要】：随着信息技术与电力行业的深度融合，智慧电厂建设成为电力行业发展的重要方向。本研究聚焦智慧电厂环境下热工控制系统的信息安全问题，深入分析其面临的网络攻击、系统漏洞、数据泄露等风险。通过研究智慧电厂热工控制系统的架构特点与运行模式，结合信息安全技术发展趋势，从技术防护、管理优化、应急响应等方面提出系统性的信息安全防护策略，旨在保障智慧电厂热工控制系统的稳定运行，提升电厂整体信息安全水平，为智慧电厂的安全发展提供理论与实践参考。

【关键词】：智慧电厂；热工控制系统；信息安全；防护策略；网络安全

DOI:10.12417/2705-0998.26.05.005

引言

热工控制系统作为智慧电厂实现自动化、智能化生产的核心，负责对电厂的发电设备运行状态进行监测与控制，其运行的稳定性和安全性直接关系到电厂的安全生产和经济效益。然而，在智慧电厂环境下，热工控制系统接入大量智能设备、与外部网络互联互通，面临着日益严峻的信息安全威胁。一旦热工控制系统遭受网络攻击或出现信息安全漏洞，可能导致设备故障、生产中断，甚至引发严重的安全事故。因此，研究智慧电厂环境下热工控制系统的信息安全防护策略具有重要的现实意义。

1 智慧电厂热工控制系统信息安全现状与问题分析

1.1 系统架构与运行特点

智慧电厂热工控制系统融合了物联网、大数据、云计算等先进技术，其架构通常包括现场设备层、控制层、管理层和企业信息层。现场设备层由传感器、执行器等智能终端设备组成，负责采集生产数据和执行控制指令；控制层通过分布式控制系统（DCS）、可编程逻辑控制器（PLC）等实现对生产过程的自动控制；管理层对生产数据进行分析处理，为决策提供支持；企业信息层实现与外部网络的连接，进行数据交互与共享。这种复杂的架构使得系统数据交互频繁，网络边界模糊，增加了信息安全防护的难度。

1.2 主要信息安全威胁

1.2.1 网络攻击威胁

智慧电厂热工控制系统与外部网络相连，容易成为黑客攻击的目标。攻击者可能通过网络入侵系统，篡改控制指令、破坏数据，导致设备异常运行。例如，恶意软件攻击可能使传感器数据失真，影响系统的正常控制决策；分布式拒绝服务（DDoS）攻击可能导致系统网络瘫痪，无法正常通信。

1.2.2 系统漏洞风险

热工控制系统中使用的软件、硬件设备可能存在安全漏洞，如操作系统漏洞、应用程序漏洞等。这些漏洞若未及时修复，攻击者可利用其获取系统控制权，窃取敏感信息或破坏系统功能。此外，部分老旧设备由于技术更新滞后，难以满足当前信息安全防护要求，成为系统的安全隐患。

1.2.3 数据安全隐患

热工控制系统在运行过程中产生大量的生产数据、设备参数等敏感信息，这些数据的安全至关重要。然而，在数据存储、传输和处理过程中，可能存在数据泄露、篡改等风险。例如，数据在网络传输过程中若未进行加密处理，容易被窃取；数据库管理不善可能导致数据被非法访问和修改。

1.2.4 人员操作风险

操作人员的安全意识和操作规范对系统信息安全有重要影响。部分操作人员缺乏信息安全知识，可能在操作过程中误点击恶意链接、使用弱密码，导致系统被入侵。此外，内部人员的违规操作或恶意行为，也可能造成信息泄露和系统破坏。

表 1 安全威胁类型

安全威胁类型	具体表现	潜在危害
网络攻击威胁	恶意软件入侵、DDoS 攻击等	设备异常运行、系统网络瘫痪
系统漏洞风险	软件硬件存在安全漏洞	系统被控制、功能被破坏
数据安全隐患	数据泄露、篡改	生产数据失真、决策失误
人员操作风险	误操作、违规操作	系统被入侵、信息泄露

2 智慧电厂热工控制系统信息安全防护策略

2.1 技术防护策略

2.1.1 加强网络边界防护

在智慧电厂热工控制系统与外部网络的连接边界，部署多层次、立体化的安全防护设备是筑牢网络安全防线的关键。防火墙作为网络安全的第一道屏障，可基于预先设定的访问控制规则，对进出网络的数据包进行筛选。例如，可限制仅允许特

定 IP 地址段的设备访问热工控制系统，禁止外部网络对内部关键控制节点的直接访问，有效阻止非法的网络连接请求。入侵检测系统（IDS）通过实时监测网络流量，分析其中的异常行为模式和特征，能够及时发现潜在的攻击行为。当检测到黑客尝试利用已知漏洞进行入侵时，IDS 会立即发出警报。入侵防御系统（IPS）则更具主动性，不仅能检测攻击，还能在攻击行为发生时自动采取阻断措施，如丢弃恶意数据包、关闭异常连接等，将攻击拦截在系统之外。

虚拟专用网络（VPN）技术通过加密隧道技术，在公网环境下建立安全的专用通信通道。在智慧电厂中，当工作人员需要远程访问热工控制系统进行维护和管理时，可通过 VPN 连接，所有传输的数据都会被加密处理，即使数据在公网传输过程中被截获，攻击者也无法读取其真实内容，从而保障了数据传输的安全性和私密性。例如，某智慧电厂部署 VPN 后，远程工程师可安全地对控制系统进行参数调整和故障排查，同时避免了外部网络对系统的潜在威胁。

2.1.2 强化系统漏洞管理

建立完善的系统漏洞扫描和修复机制是保障热工控制系统安全运行的重要环节。定期使用专业的漏洞扫描工具，如 Nessus、OpenVAS 等，对热工控制系统的操作系统、应用程序、数据库等软件以及硬件设备固件进行全面扫描。这些工具能够检测出系统中存在的已知漏洞，包括缓冲区溢出、SQL 注入、未授权访问等安全隐患。对于扫描发现的漏洞，需根据其严重程度进行分级处理。对于高危漏洞，应立即安排技术人员进行修复，可通过安装厂商发布的补丁程序来解决。例如，当操作系统出现严重的远程代码执行漏洞时，及时下载并安装对应的补丁，可有效防止黑客利用该漏洞获取系统控制权。

对于老旧设备，由于其可能无法兼容最新的安全补丁或升级版本，需进行全面的安全风险评估。评估内容包括设备的使用年限、功能重要性、存在的安全漏洞以及修复的可行性等。若评估结果显示设备存在严重安全风险且无法通过常规手段修复，应考虑进行升级或替换。此外，在引入第三方软件和插件时，要严格进行安全检测，审查其源代码、数字签名以及安全认证情况，确保其不携带恶意代码，不会为系统引入新的安全隐患。

2.1.3 保障数据安全

数据安全是智慧电厂热工控制系统的核心关注点之一，在数据存储和传输过程中采取有效的防护措施至关重要。在数据存储方面，采用先进的加密技术对敏感数据进行加密处理。例如，对于涉及发电设备运行参数、生产工艺数据等核心信息，可使用高级加密标准（AES）进行加密存储。AES 算法具有高强度的加密性能，能够抵御多种形式的密码攻击，即使存储介质被盗取，攻击者也无法解密获取真实数据。同时，建立完善的数据备份与恢复机制，定期对重要数据进行全量备份和增量备份。备份数据可存储在异地的专用存储设备或云存储平台上，以防止因自然灾害、硬件故障等原因导致数据丢失。当发生数据丢失或损坏事件时，可通过备份数据快速恢复系统正常运行，确保生产过程不受影响。

在数据传输过程中，采用安全可靠的通信协议和加密算法。SSL/TLS 协议是目前广泛应用于网络数据传输的安全协议，它在应用层协议（如 HTTP、FTP 等）和网络层协议之间建立安全连接，对传输的数据进行加密、认证和完整性校验。例如，在热工控制系统与管理层之间的数据交互过程中，启用 HTTPS 协议（基于 SSL/TLS 的 HTTP 协议），可保证数据在传输过程中不被窃取和篡改。同时，结合 AES 等加密算法对数据进行二次加密，进一步增强数据传输的安全性。

2.1.4 应用工业互联网安全技术

工业互联网安全技术针对智慧电厂热工控制系统的工业特性，提供了定制化的安全防护方案。工业防火墙与传统防火墙相比，能够深度解析工业协议，如 Modbus、OPCUA 等。它可根据工业协议的特点和控制逻辑，对工业网络中的数据流量进行精确控制。例如，工业防火墙可限制 Modbus 协议的数据读写操作仅在授权的设备和地址范围内进行，防止非法设备对控制系统进行恶意操作。工业入侵检测系统能够识别工业网络中特有的攻击模式和异常行为，如对工业设备的异常指令发送、频繁的设备状态查询等。一旦检测到异常，系统会及时发出警报，并提供详细的攻击信息，便于安全人员进行处理。

工业安全审计系统则对热工控制系统的操作行为和数据访问进行全面记录和审计。它可记录操作人员的登录时间、操作内容、数据访问记录等信息，通过对这些日志的分析，能够发现潜在的安全违规行为和操作失误。例如，当审计系统发现有异常的设备参数修改记录时，可及时追溯到操作来源，查明原因，避免安全事故的发生。通过实时监测系统运行状态，工业互联网安全技术能够及时发现异常行为并进行预警，为热工控制系统的安全运行提供有力保障。

2.2 管理优化策略

2.2.1 完善安全管理制度

制定并完善热工控制系统信息安全管理制度，明确各部门和人员的安全职责，规范系统操作流程。建立安全审计制度，对系统操作、数据访问等行为进行审计和记录，以便追溯和分析安全事件。同时，加强对第三方服务商的安全管理，在合同中明确安全责任和要求。

2.2.2 加强人员安全培训

定期对热工控制系统操作人员、管理人员进行信息安全培训，提高其安全意识和操作技能。培训内容包括网络安全法律法规、信息安全基础知识、系统操作规范、应急处理流程等。

通过培训，使相关人员了解信息安全的重要性，掌握基本的安全防护技能，避免因人为因素导致安全事故。

2.2.3 建立安全评估机制

定期对热工控制系统的信息安全状况进行评估，采用风险评估方法，识别系统存在的安全风险，并制定相应的风险应对措施。根据评估结果，不断优化信息安全防护策略和措施，确保系统的安全水平始终满足要求。

2.3 应急响应策略

2.3.1 制定应急预案

结合智慧电厂热工控制系统的特点，制定完善的信息安全应急预案，明确应急响应流程、各部门和人员的职责。应急预案应包括网络攻击、数据泄露、系统故障等不同类型安全事件的应对措施，确保在安全事件发生时能够迅速、有效地进行处置。

2.3.2 开展应急演练

定期组织开展信息安全应急演练，检验和完善应急预案的可行性和有效性。通过演练，提高相关人员的应急处置能力，增强各部门之间的协同配合能力。同时，对应急演练过程中发现的问题进行总结和改进，不断优化应急预案。每次演练结束后，需及时组织复盘总结。成立由技术专家、管理人员和一线操作人员组成的评估小组，从事件响应速度、处置措施有效性、部门协作效率等维度，对照应急预案进行逐项评估。例如，统计从事件发现到应急响应启动的时间间隔，分析是否满足预案要求；评估处置过程中采取的技术手段是否成功阻断攻击、恢复系统。针对演练中发现的问题，如部分人员对应急流程不熟悉、部门间信息传递存在延迟等，制定详细的改进计划，对应急预案进行修订和完善。通过持续的演练和优化，确保应急预案始终贴合实际需求，有效提升智慧电厂热工控制系统的应急响应水平。

2.3.3 建立应急响应团队

组建专业的信息安全应急响应团队是智慧电厂热工控制系统有效应对安全事件的核心力量。应急响应团队应具备多元化的专业知识和技能，成员构成涵盖网络安全专家、系统运维工程师、数据分析员、法律顾问等不同领域专业人才。为保证应急响应团队高效运作，需建立完善的培训和考核机制。定期组织团队成员参加网络安全技术培训、应急处置流程培训等课程，邀请行业专家分享最新的安全威胁趋势和应对策略，提升团队成员的专业素养和实战能力。同时，制定科学的考核指标，从事件响应速度、处置成功率、团队协作表现等方面对成员进行定期考核，考核结果与绩效奖励挂钩，激励团队成员积极提升自身能力，保障应急响应团队始终保持高水平的战斗力，在安全事件发生时能够迅速、有效地开展工作，将损失降至最低。

3 结论

智慧电厂环境下热工控制系统的信息安全防护是一项复杂的系统工程，关系到电厂的安全生产和稳定运行。通过对热工控制系统信息安全现状与问题的分析，本文从技术防护、管理优化、应急响应等方面提出了一系列防护策略。在实际应用中，应结合智慧电厂的具体情况，综合运用多种防护手段，不断完善信息安全防护体系，提升热工控制系统的信息安全水平，为智慧电厂的可持续发展提供坚实保障。未来，随着信息技术的不断发展，还需持续关注热工控制系统信息安全的新问题、新挑战，进一步优化和创新防护策略。

参考文献：

[1] 李璞.基于模型预测控制技术的电厂热控保护装置误动和拒动研究[J].自动化应用,2025,66(11):274-276+279.

[2] 隽丽艳.基于改进模糊逻辑的电厂热工仪表自动控制研究[J].电气技术与经济,2025,(03):195-197+201.

[3] 邢智成.电厂热控 DCS 控制保护回路误动作原因与处理措施研究[J].电力设备管理,2024,(21):67-69.

[4] 阮忠龙.电厂热控 DCS 控制保护回路误动作原因和解决对策[J].装备维修技术,2024,(04):62-64.

[5] 王春.电厂热工自动控制系统运行中存在的问题分析及优化措施[J].中国设备工程,2023,(22):119-121.