火电厂集控运行系统的网络安全防护研究

李思聪　王旭东　杨生睿　马　乾
华能平凉发电有限责任公司　甘肃　平凉　744000

摘　要：火电厂集控运行系统作为电力生产的核心枢纽，其网络安全直接关系到能源供应的稳定性与安全性。本文针对该系统展开研究，分析其组成、功能及在火电厂中的关键作用，指出系统面临的操作系统漏洞、应用软件安全隐患、硬件设备脆弱性、移动介质风险及网络攻击等多重安全威胁。基于此，从安全分区、防护设备部署、数据加密与访问控制、管理制度完善、人员培训等维度提出针对性防护策略，旨在为火电厂集控运行系统构建全方位的网络安全防护体系，保障电力生产的可靠运行。

关键词：火电厂集控；运行系统；网络安全；防护研究

引言：在能源数字化与智能化发展背景下，火电厂集控运行系统通过集成控制技术实现了发电过程的自动化与高效化，成为电力生产不可或缺的核心环节。然而，随着系统与网络融合程度加深，其面临的网络安全风险日益复杂——从底层硬件到上层应用，从内部操作到外部攻击，各类安全隐患可能导致系统故障甚至引发大面积停电事故。当前，火电厂集控运行系统的网络安全防护仍存在体系不完善、技术应用滞后等问题。因此，深入研究该系统的安全风险并构建科学防护策略，对提升火电厂安全生产水平、保障能源网络安全具有重要的现实意义。

1 火电厂集控运行系统概述

1.1 系统组成与功能

火电厂集控运行系统是一个高度集成的复杂体系，由硬件设备、软件系统及通信网络三大部分构成。硬件层面，涵盖传感器、控制器、执行机构等设备，传感器负责实时采集锅炉、汽轮机、发电机等关键设备的温度、压力、转速等运行参数；控制器对采集数据进行分析处理，依据预设规则生成控制指令；执行机构则按照指令调节设备运行状态。软件系统包含监控软件、数据处理软件及优化控制软件，实现对设备运行的实时监控、历史数据存储分析以及生产流程的智能优化。通信网络作为数据传输的“神经脉络”，确保各环节信息高效交互。

1.2 系统在火电厂中的重要性

火电厂集控运行系统是保障电力稳定供应的关键枢纽，在火电厂运营中占据核心地位。从生产效率角度看，系统通过自动化控制与优化调度，可精准调节机组运行参数，减少人工干预带来的延迟与误差，使机组始终保持高效运行状态，显著提升发电效率。在能源利用方面，系统能够根据负荷变化实时调整生产策略，优化煤炭、天然气等能源的消耗，降低发电成本，实现节能减排目标。安全管理层面，系统凭借实时监测与故障预警功能，可及时发现设备异常，避免重大事故发生，保障火电厂安全稳定运行[1]。

2 火电厂集控运行系统面临的网络安全风险

2.1 操作系统存在的安全风险

火电厂集控运行系统中，部分操作系统由于兼容性和稳定性要求，仍沿用老旧版本，如Windows XP、Windows 7等，这些系统早已停止官方更新支持，存在大量已知安全漏洞，极易被恶意程序利用。此外，为保障系统运行稳定性，火电厂通常避免频繁更新操作系统补丁，导致新发现的安全漏洞无法及时修复。同时，部分系统默认配置安全性不足，用户权限设置不合理，一旦攻击者突破外围防护，就能利用这些漏洞获取系统控制权，篡改运行参数，干扰正常生产流程，甚至导致系统崩溃。

2.2 应用软件存在的安全风险

集控系统的应用软件在开发过程中，可能因代码编写不规范、缺乏严格的安全测试，存在缓冲区溢出、SQL注入等安全漏洞。这些漏洞会使软件在运行时面临数据泄露、被恶意篡改的风险。并且，随着系统功能需求的不断增加，应用软件间的交互愈发复杂，接口安全防护若不到位，就会成为攻击者渗透系统的薄弱点。此外，一些应用软件开发商因市场份额较小或技术能力有限，难以持续提供安全更新和维护，进一步加剧了应用软件的安全隐患。

2.3 硬件设备存在的安全风险

火电厂集控系统中的硬件设备，如传感器、控制器等，由于长时间处于高温、高湿、电磁干扰等复杂环境

中运行，容易出现老化、故障，导致数据采集和传输异常，进而影响系统对设备状态的准确判断。同时，部分硬件设备在设计制造时，未充分考虑网络安全防护，存在通信协议漏洞，攻击者可通过无线或有线方式接入，篡改硬件设备的控制指令，造成设备误动作。此外，硬件设备的固件更新机制不完善，难以抵御新型攻击，一旦被恶意修改固件，设备将失去正常功能，严重威胁火电厂的安全生产。

2.4 移动介质存在的安全风险

在火电厂日常运维过程中，移动介质（如U盘、移动硬盘）的使用较为频繁。若工作人员使用未经安全检测的移动介质，其中携带的病毒、木马等恶意程序就可能被引入集控运行系统。一旦恶意程序激活，不仅会破坏系统数据，还能利用系统漏洞在内部网络中快速传播扩散，感染更多设备。此外，部分工作人员安全意识薄弱，随意将移动介质在外部计算机与集控系统设备间交叉使用，进一步增加了病毒入侵风险，可能导致系统数据泄露、运行紊乱等严重后果。

2.5 网络攻击威胁

随着工业控制系统与网络的深度融合，火电厂集控运行系统面临的网络攻击威胁日益严峻。黑客、网络犯罪组织甚至敌对势力，可能通过钓鱼攻击、勒索病毒、DDoS攻击等手段，尝试突破系统的网络防护。钓鱼攻击通过伪装合法网站或邮件，诱骗工作人员泄露账号密码，获取系统访问权限；勒索病毒加密系统数据，迫使火电厂支付高额赎金；DDoS攻击则通过大量恶意流量堵塞网络，导致系统无法正常通信和运行。这些攻击一旦得逞，将严重破坏火电厂的正常生产秩序，甚至威胁国家能源安全[2]。

3 火电厂集控运行系统网络安全防护策略

3.1 加强安全分区与网络专用

将火电厂集控运行系统网络划分为生产控制区、信息管理区等不同安全区域，依据各区域的功能与安全需求，制定差异化防护策略。生产控制区作为核心区域，仅允许专用网络通信，禁止与外部非信任网络直接连接，从物理层面阻断外部攻击路径。同时，通过设置严格的区域边界防护，限制不同区域间的访问权限，仅允许必要的业务数据按照指定规则交互。例如，信息管理区的办公设备无法直接访问生产控制区的关键设备参数，需经安全隔离与数据验证后方可获取有限数据，以此降低内部攻击风险，保障集控系统核心功能稳定运行。

3.2 部署安全防护设备

3.2.1 工业防火墙

工业防火墙针对火电厂集控系统的工业通信协议特点进行深度优化，能够精准识别Modbus、DNP3等工控协议的合法数据流量，有效过滤非法指令与恶意数据。通过在网络边界和关键区域节点部署工业防火墙，可建立多层防护屏障。例如，在生产控制区与信息管理区之间设置工业防火墙，可实时监控并阻断不符合安全策略的访问请求，防止外部攻击者利用网络漏洞渗透至核心生产系统。同时，工业防火墙具备细粒度的访问控制策略配置功能，可依据设备、用户、时间等维度进行精准管控，进一步提升系统网络安全性。

3.2.2 入侵检测系统（IDS）

入侵检测系统通过对网络流量和系统日志的实时分析，能够快速发现潜在的网络攻击行为。在火电厂集控运行系统中部署IDS，可持续监测网络中异常的数据流量模式、非法的设备访问行为等威胁。例如，当检测到某一设备短时间内频繁向外部发送大量数据，或出现异常的协议请求时，IDS将立即触发警报，并记录攻击来源与行为特征。此外，IDS还可与其他安全设备联动，如自动通知工业防火墙封禁攻击源IP，及时阻断攻击扩散，为系统提供主动式安全防护。

3.2.3 工控安全隔离网闸设备

工控安全隔离网闸设备采用“物理隔离+数据摆渡”技术，实现不同安全等级网络间的安全数据交换。在火电厂集控系统中，隔离网闸可部署于生产控制区与外部网络之间，当信息管理区需要获取生产数据时，隔离网闸先将数据进行拆解、重组与深度检测，确保数据无病毒、无恶意代码后，再以非网络连接的方式传输至目标区域。这种物理隔离机制从根本上杜绝了网络层攻击穿透的可能，同时保证了必要数据的安全交互，在保障系统安全性的前提下，满足火电厂业务数据共享需求。

3.3 强化数据加密与访问控制

3.3.1 数据加密

在火电厂集控运行系统中，数据加密是保护核心生产数据、防止泄露篡改的关键手段。对传输过程中的数据，采用SSL/TLS等安全协议进行加密，确保数据在不同区域、设备间传输时，即使被截获也无法被非法读取。例如，在传感器采集数据上传至控制系统，以及控制系统下发指令给执行机构的过程中，加密处理可避免数据被恶意修改导致设备误操作。对于存储在数据库中的历史运行数据、设备参数等静态数据，运用AES等高强度加密算法，防止数据被非法访问或窃取。同时，定期更新加密密钥，提升加密安全性，保障火电厂生产数据全生命周期的安全。

3.3.2 访问控制

访问控制通过严格的权限管理与身份认证，限制用户对系统资源的访问。采用基于角色的访问控制（RBAC）模型，根据岗位职能为不同用户分配相应权限，如运维人员仅可查看设备运行状态与进行基础维护操作，而系统管理员才具备修改核心配置参数的权限。结合多因素身份认证机制，除传统的用户名与密码外，引入动态验证码、生物识别（指纹、人脸识别）等技术，确保只有合法用户才能登录系统。同时，建立详细的操作日志记录，实时监控用户操作行为，一旦发现异常访问或越权操作，立即触发告警并采取限制措施，从而有效防止内部人员误操作或恶意攻击带来的安全风险。

3.4 完善安全管理制度与应急响应机制

3.4.1 安全管理制度

安全管理制度是保障火电厂集控运行系统网络安全的核心框架。在设备管理方面，从采购阶段引入安全评估机制，优先选择具备安全认证、支持安全升级的硬件与软件产品；设备接入网络前，需通过专业安全检测工具完成漏洞扫描与补丁修复，并提交详细的检测报告，经审批后方可入网；设备退役时，严格执行数据彻底清除与物理销毁流程，防止敏感信息泄露。账号权限管理采用“三权分立”模式，将系统管理、审计监督与安全操作权限分离，定期开展权限审查，及时撤销离职或转岗人员权限。日志管理不仅要求完整记录系统操作与数据访问行为，还需对日志进行实时分析，利用机器学习算法识别异常操作模式。针对外部人员，实施“最小权限+全程监控”策略，提供临时受限账号，并通过屏幕监控与操作审计，确保第三方运维过程安全可控。

3.4.2 应急响应机制

应急响应机制是火电厂抵御网络安全威胁的最后防线。首先，依据安全事件影响范围与危害程度，将事件划分为一般、较大、重大、特别重大四级，针对不同级别制定标准化处置流程，明确各部门职责与协同要求。依托人工智能驱动的态势感知平台，对网络流量、设备状态、用户行为等进行多维度实时监测，利用异常行为分析模型主动识别潜在威胁，触发自动化预警机制。定期组织全流程应急演练，涵盖桌面推演、模拟实战等多种形式，模拟APT攻击、系统崩溃等复杂场景，检验预案的有效性并持续优化。建立与网络安全应急响应中心、行业专家团队的紧密合作关系，搭建信息共享平台，及时获取最新攻击情报与处置方案；同时，储备必要的应急物资与技术工具，确保在遭遇重大安全事件时，能够快速隔离故障区域、恢复业务系统，最大限度降低对电力生产的影响。

3.5 加强人员培训与安全意识教育

人员是网络安全防护的核心要素，需构建系统化、分层次的培训体系。针对普通操作人员，开展以网络安全基础规范为核心的培训，包括密码安全策略（如定期更换、强密码设置）、移动介质使用准则（禁止随意接入外部设备）、钓鱼邮件识别技巧等内容，并通过情景模拟测试巩固学习效果。技术人员培训聚焦专业技能提升，涵盖漏洞挖掘与修复、入侵检测与溯源、安全加固方案设计等进阶课程，组织参与CTF竞赛、攻防演练等实战活动，提升应急处置能力。管理人员培训则注重战略层面，包括网络安全法律法规解读、风险评估与管理体系构建、安全资源统筹调配等内容，强化安全决策能力。此外，通过每月安全主题活动、典型案例警示教育、安全知识线上学习平台等多样化形式，营造全员参与的网络安全文化氛围；建立培训考核与激励机制，将安全知识掌握程度与绩效考核、岗位晋升挂钩，切实提升全体员工的网络安全意识与防护技能[3]。

结束语

火电厂集控运行系统的网络安全防护关乎电力稳定供应与能源安全。本文系统分析了系统面临的安全风险，并从安全分区、设备部署、数据加密、制度完善、人员培训等多维度提出防护策略。这些措施相互配合，构建起全方位、多层次的防护体系。但随着网络攻击手段的不断演变，火电厂需持续关注安全技术发展，动态优化防护策略，加强多方协同与技术创新。唯有如此，才能有效抵御网络威胁，保障集控运行系统安全稳定运行，为国家能源安全筑牢防线。

参考文献

[1]张俊.探析火力发电厂热控系统可靠性的优化技术[J].数码设计（下）,2020,009(001):124-125

[2]傅国刚,王娜.火电厂热控保护系统故障分析与预防措施研究[J].河北农机,2021(6):224-226

[3]陈付印.铝电企业的火电厂热控保护系统的可靠性研究[J].中国金属通报,2020(6):278-29