

电厂信息网络安全防护研究

许 晶

国能亿利能源有限责任公司电厂 内蒙古 鄂尔多斯 014300

摘 要：在能源体系中，电厂地位关键，其信息化趋势下，安全问题直接影响生产与能源供应。本文围绕电厂信息网络安全防护展开研究，分析了电厂信息网络分层架构，明确生产控制网与管理信息网的隔离及接入原则；梳理了安全建设现状，识别外部威胁与内部问题；随后从网络边界、数据、终端与设备、安全可视化四个维度，阐述关键防护技术的应用要点；最后构建包含组织职责、制度流程、人员管理的安全管理体系。研究表明，通过技术与管理协同，才能有效提升电厂信息网络安全防护能力，为电厂安全生产与稳定运营提供保障，对推动电力行业信息安全发展具有参考价值。

关键词：电厂；信息网络安全防护；关键技术；安全管理体系构建

引言：当前电厂信息网络面临外部攻击、供应链隐患等威胁，内部存在分区不明、设备老旧等问题，且不同规模电厂安全投入差距大，标准落地有偏差。现有研究虽涉及部分防护技术，但缺乏体系化整合。因此开展电厂信息网络安全防护研究，构建技术与管理结合的防护体系，对解决安全痛点、保障电厂安全运行意义重大。

1 电厂信息网络的架构

电厂信息网络通常采用分层架构设计，核心分为生产控制网与管理信息网两大板块，两大网络板块通过特定边界设备实现隔离与有限数据交互，避免管理网侧风险向生产控制网渗透。在网络设备部署上，遵循功能分区与安全防护结合的逻辑，交换机、路由器等设备根据不同网络层级与功能需求进行合理布局，同时配备专门的安全防护设备，构建多层次防护屏障。

关键业务系统的接入遵循按需分配、安全优先的原则，不同业务系统根据其功能属性与安全等级，接入对应的网络板块：直接参与生产控制的系统接入生产控制网，确保数据传输的实时性与安全性；用于企业管理的系统接入管理信息网，保障业务数据的交互效率；通过严格的接入认证与权限控制，规范各类业务系统的网络访问行为，避免未经授权接入带来的安全风险，整体架构既满足功能需求，又兼顾安全防护^[1]。

2 电厂信息网络安全现状与风险识别

2.1 电厂信息网络安全建设现状

国内电厂信息网络安全建设呈现差异化发展态势，不同规模电厂在安全防护投入上存在明显差距，资源更多向大型发电集团倾斜，中小电厂在安全设备更新、技术升级等方面相对滞后。从整体防护体系来看，现有措施覆盖范围有限，多集中在核心生产控制环节，对管理

信息网、设备运维网络的防护力度不足，导致安全防护存在短板。行业标准虽已明确安全建设要求，但在落地过程中面临执行偏差，部分电厂存在标准理解不到位、制度与实践脱节等问题，使得安全防护未能充分发挥作用，整体安全建设仍需进一步完善。

2.2 电厂信息网络面临的外部安全威胁

外部安全威胁对电厂信息网络的针对性和危害性不断提升，网络攻击手段持续升级，攻击目标更聚焦于电厂关键业务系统，可能导致生产中断、数据泄露等严重后果。外部人员非法入侵风险不容忽视，不法分子通过技术手段突破网络边界，试图窃取电厂敏感信息，对电厂运营安全构成威胁。供应链安全隐患逐渐凸显，第三方提供的设备、软件可能存在安全漏洞，若未经过严格检测便投入使用，易成为外部攻击的突破口，给电厂信息网络带来潜在风险。

2.3 电厂信息网络存在的内部安全问题

电厂信息网络内部存在以下诸多安全漏洞，（1）网络分区不明确是突出问题之一，不同功能区域间缺乏有效隔离，一旦某一区域出现安全问题，易引发横向渗透，扩大安全事故影响范围。（2）部分老旧设备与系统因技术限制，安全漏洞难以修复，长期运行过程中形成安全隐患，无法有效抵御新型安全威胁。（3）员工安全意识薄弱引发的操作风险频发，不规范的操作行为可能直接破坏网络安全防护体系，为安全事故的发生埋下隐患，内部安全管理亟待加强^[2]。

3 电厂信息网络安全防护关键技术

3.1 网络边界防护技术

网络边界是电厂信息网络抵御外部威胁的首要屏障，要通过以下多层次技术部署构建严密防护体系。

(1) 下一代防火墙(NGFW)作为边界防护的核心设备,要具备精细化的访问控制能力,能基于业务需求、用户身份、终端类型等多维度制定访问策略,同时集成威胁检测功能,可对网络流量中的恶意代码、异常数据包进行实时识别与拦截,保障边界流量的安全性。(2) 入侵检测与防御系统(IDS/IPS)需与NGFW协同工作,IDS负责对网络流量进行深度分析,通过特征匹配、异常行为分析等方式发现潜在安全威胁,并生成告警信息;IPS则在此基础上具备主动防御能力,可直接阻断攻击流量,防止威胁渗透至内部网络。在部署过程中,需根据电厂网络架构特点,合理规划IDS/IPS的监测范围,确保覆盖核心业务链路。(3) 工业防火墙其设计需充分考虑工业协议的特性,支持对Modbus、DNP3等常用工业协议的深度解析与过滤,能够基于协议字段、操作码等精细化维度制定防护规则,有效阻止非授权的工业控制指令传输。

3.2 数据安全防护技术

数据安全是电厂信息网络安全的核心内容,要从以下数据存储、传输、使用全生命周期构建防护体系。

(1) 关键业务数据的加密保护需采用符合国家相关标准的加密算法,在数据存储环节,对数据库中的敏感数据进行加密处理,确保即使数据存储介质被非法获取,也无法泄露数据内容;在数据传输环节,通过建立加密传输通道,对跨网络、跨系统传输的关键数据进行加密,防止数据在传输过程中被窃取或篡改。(2) 数据备份与恢复机制的构建需采用“本地备份+异地容灾”的双重模式,本地备份可实现对数据的快速备份与恢复,满足日常数据故障处理需求;异地容灾则需在地理上相距较远的位置建立容灾中心,定期将本地数据同步至容灾中心,当电厂本地数据因重大安全事件遭受破坏时,可通过异地容灾中心快速恢复数据,保障业务的连续性。在备份策略制定上,需根据数据的重要性与更新频率,划分不同的备份等级,制定差异化的备份周期与备份方式。(3) 数据泄露防护(DLP)系统的部署需覆盖数据产生、流转、使用的关键节点,通过对终端、网络、存储设备的数据活动进行实时监控,识别并阻断非授权的数据导出、拷贝、传输行为。DLP系统需具备数据识别能力,可通过关键词匹配、正则表达式、文件指纹等技术,精准识别敏感数据。

3.3 终端与设备安全防护技术

终端与设备是电厂信息网络的重要组成部分,其关键技术如下。(1) 生产控制终端的安全加固需从硬件、系统、软件多维度入手,在硬件层面,对终端的USB端

口、光驱等外部接口进行管控,根据业务需求限制接口的使用权限,防止外部存储设备接入导致病毒传播或数据泄露;在系统层面,对终端操作系统进行最小化配置,关闭不必要的服务与端口,删除冗余组件,减少系统漏洞;在软件层面,建立严格的软件安装管控机制,仅允许安装经过安全认证的必要软件,禁止安装无关软件,防止恶意软件感染。(2) 工业控制设备的安全防护要重点关注漏洞管理与固件安全,定期对PLC、SCADA等工业控制设备进行漏洞扫描,及时发现设备存在的安全漏洞,并根据设备厂商提供的漏洞修复方案,制定合理的固件更新计划。在固件更新过程中,需采取严格的安全措施,对固件文件进行完整性校验与合法性验证,防止安装恶意固件或被篡改的固件,同时需制定回滚预案,确保在固件更新失败时,能够恢复设备的正常运行状态。(3) 终端安全管理系统(EDR)的部署需实现对全网终端的统一管控,通过在终端安装客户端软件,收集终端的硬件信息、系统配置、软件安装、网络连接、进程活动等数据,实现对终端状态的全面掌握。EDR系统需具备异常行为分析能力,可通过建立终端正常行为基线,识别终端的异常操作(如频繁的文件修改、异常的网络连接、未知进程启动),并及时发出告警信息。

3.4 安全可视化与态势感知技术

安全可视化与态势感知技术能够帮助电厂管理人员实时掌握网络安全状态,其关键技术如下:(1) 电厂信息网络安全态势感知平台的架构设计要采用分层架构,底层为数据采集层,通过部署在网络设备、安全设备、终端、服务器上的数据采集探针,收集日志数据、告警数据、流量数据、资产数据等多源安全数据;中间层为数据处理层,对采集到的原始数据进行清洗、标准化、关联分析,去除冗余数据与噪声数据,提取有价值的信息;顶层为态势呈现与预警层,通过可视化界面直观展示网络安全态势,提供风险预警、事件溯源、趋势分析等功能。(2) 多源安全数据的汇聚与分析是态势感知平台的核心能力,需建立统一的数据汇聚机制,支持对不同格式、不同来源的数据进行标准化处理,实现数据的集中存储与管理。在数据分析环节,需综合运用关联分析、统计分析、机器学习等技术,对多源数据进行深度挖掘,发现数据间的潜在关联,识别隐藏的安全威胁。如通过将防火墙告警数据与终端进程数据进行关联分析,判断是否存在终端被恶意程序控制并发起攻击的情况;通过对网络流量数据的统计分析,识别异常流量patterns,判断是否存在DDoS攻击迹象。(3) 安全风险的可视化呈现与预警机制需以直观、易懂的方式展示

网络安全状态,通过仪表盘、拓扑图、热力图等可视化组件,实时呈现网络资产分布、安全事件数量、风险等级、威胁类型等关键指标,帮助管理人员快速掌握网络安全整体情况。建立科学的风险评估模型,根据安全事件的严重程度、影响范围、发生频率等因素,对网络安全风险进行量化评估,划分风险等级,并针对不同等级的风险制定相应的预警策略,当风险达到预警阈值时,及时通过短信、邮件、系统告警等方式通知相关人员,以便采取应急处置措施,防范安全事件的发生与扩大^[3]。

4 电厂信息网络安全管理体系构建

4.1 安全组织与职责体系

(1) 电厂要设立信息安全领导小组,成员涵盖企业管理层、生产部门负责人及技术骨干,主要负责制定信息网络安全战略规划,审批重大安全投入方案,决策安全事件处置中的关键事项,确保安全工作与企业整体发展目标一致。(2) 安全管理部门与技术执行团队需明确职责划分:安全管理部门负责统筹安全工作,包括制度起草、风险评估、合规检查及跨部门协调;技术执行团队专注于技术落地,承担安全设备运维、漏洞修复、应急技术支撑等任务,两者需建立定期沟通机制,确保管理要求与技术实施无缝衔接。(3) 各业务部门(生产、运维、管理)需建立安全协同机制,明确各部门安全联络员,负责传递安全要求、反馈部门安全问题。生产部门需配合做好生产控制网安全防护,运维部门需保障设备安全运行,管理部门需规范内部数据使用,通过跨部门协作形成安全管理合力。

4.2 安全制度与流程建设

(1) 核心安全制度制定需结合电厂实际,网络安全管理制度应明确网络接入、分区管控、设备配置等规范;数据安全管理制度需界定敏感数据范围,规定数据采集、存储、传输、销毁各环节要求,制度内容需符合行业标准与法律法规,确保可执行、可监督。(2) 安全事件处置流程需实现标准化,明确“发现-上报-处置-复盘”全流程节点:发现环节要求员工及时反馈异常,上报环节需明确上报路径与时限,处置环节需制定分级响应措施,复盘环节需形成事件分析报告并提出改进方

案,避免同类事件重复发生。(3) 定期安全检查与审计流程需规范实施,检查频率可按季度或月度设定,检查内容涵盖设备状态、制度执行、漏洞修复等;审计工作需覆盖网络日志、操作记录、数据流转等,通过检查与审计及时发现安全隐患,督促问题整改到位。

4.3 人员安全管理与培训

(1) 员工安全准入需与岗位安全职责匹配,入职时需签订安全责任书,明确岗位对应的安全要求,例如生产岗位员工需掌握终端安全操作规范,管理岗位员工需遵守数据保密规定,同时建立岗位安全资质认证机制,未通过认证者不得上岗。(2) 定期安全培训体系构建需分层分类开展:新员工入职培训需覆盖基础安全知识与企业安全制度;全员定期培训需结合最新安全威胁,更新防护技能内容,培训形式可采用线上学习与线下实操结合,确保培训效果。(3) 安全意识考核与应急演练需常态化开展,考核内容需贴合岗位实际,检验员工安全知识掌握程度;应急演练需模拟常见安全事件场景,锻炼员工应急处置能力,演练后需总结不足,优化应急预案,提升整体安全防护水平^[4]。

结束语:本文系统研究电厂信息网络安全防护,明确了网络架构特点,剖析了安全现状与风险,提出关键防护技术,构建了完整管理体系。该研究为电厂提供了可操作的安全防护方案,助力解决实际安全问题。未来将进一步优化防护技术与管理策略,持续完善电力行业信息网络安全防护体系,为能源领域数字化转型筑牢安全屏障。

参考文献

- [1]钱鹏,黄君.试论电厂信息网络安全的防护研究和建设[J].科学与财富,2022,14(31):157-159.
- [2]李敏.电厂电力监控网络安全防护系统的运维管理研究[J].电脑采购,2025(24):19-21.
- [3]盛红玉.电力系统信息通信的网络安全及防护研究[J].世界家苑,2021(18):148-149.
- [4]朱金庆.智慧电厂下的数据网络安全体系研究[J].数码设计(上),2020,9(2):23-24.