智能电网环境下电力系统信息安全防护体系构建研究

丁江涛¹, 彭炳楠²

1. 河南省蒲安建设工程有限公司, 河南 长垣 453400

2. 河南立新监理咨询有限公司, 河南 郑州 450000

DOI:10.61369/ME.2024100003

摘要：随着智能电网的快速发展，电力系统的信息化与智能化水平不断提升，信息安全问题逐渐成为制约其稳定运行的核心挑战。本文聚焦智能电网环境下电力系统的信息安全防护体系构建，从物理、网络、数据三个维度分析其安全需求，探讨加密技术、入侵检测、身份认证等关键技术的作用机理，设计涵盖技术架构、管理机制与维护策略的一体化防护体系。

关键词：智能电网；电力系统；信息安全；防护体系；分层防御

Research on the Construction of Power System Information Security Protection System in Smart Grid Environment

Ding Jiangtao¹, Rong Bingnan²

1. Henan Pu'an Construction Engineering Co., Ltd., Changyuan, Henan 453400

2. Henan Lixin Supervision Consulting Co., Ltd., Zhengzhou, Henan 450000

Abstract：With the rapid development of smart grid, the level of informatization and intelligence of power system has been continuously improved, and information security has gradually become the core challenge that restricts its stable operation. This paper focuses on the construction of information security protection system of power system in smart grid environment, analyzes its security requirements from three dimensions of physics, network and data, discusses the mechanism of key technologies such as encryption technology, intrusion detection and identity authentication, and designs an integrated protection system covering technical architecture, management mechanism and maintenance strategy.

Keywords：smart grid; electric power system; information security; protection system; layered defense

引言

智能电网作为新一代电力系统，融合现代信息技术与电力技术，是能源革命与数字经济发展的关键支撑。它在提升电力供应效率、推动新能源消纳等方面发挥关键作用。然而，随着智能电网中信息交互量剧增，其信息安全面临严峻挑战。恶意攻击、数据泄露、系统漏洞等问题频发，一旦信息安全防线被突破，不仅会造成电力系统运行紊乱，还可能危及国家能源安全和社会稳定。因此，深入研究智能电网环境下电力系统信息安全防护体系构建，对保障电力系统安全稳定运行，推动能源产业可持续发展具有重要的现实意义。

一、智能电网环境下电力系统信息安全需求

（一）物理安全需求

智能电网的物理安全需求源于其底层基础设施对实体设备的深度依赖。作为连接物理世界与数字系统的关键接口，智能电表、传感器、控制终端等硬件设备直接暴露于物理环境威胁中。电磁干扰可能造成设备信号失真或通信中断，例如变电站高频电磁场可能干扰邻近智能设备的运行稳定性。极端环境条件同样构成潜在风险，高温、高湿或震动可能加速硬件老化，导致数据采集误差或设备故障^[1]。此外，物理破坏行为的威胁不容忽视，针对

对电力设施的非法入侵或恶意损毁可能直接瘫痪局部电网功能。为应对这些挑战，设备冗余设计成为基础保障，例如部署双路电源模块或备份通信链路，确保单一节点故障不影响整体系统运行。环境监测系统需实时感知温度、湿度、振动等参数，通过阈值预警机制触发保护措施。

（二）网络安全需求

智能电网的网络安全需求聚焦于其多层次网络架构的脆弱性。在发电、输电、配电与用户侧构成的复杂网络中，通信协议的开放性可能被利用进行中间人攻击或数据篡改。例如，缺乏加密的 SCADA 系统通信可能被截获并注入虚假指令，导致断路器误

动作。网络边界模糊化加剧了威胁扩散风险，分布式能源接入点与云端管理平台的互联互通使攻击面呈指数级扩张^[2]。拒绝服务攻击可能通过泛洪式数据包阻塞通信信道，延迟关键控制指令的传递。为此，网络拓补需遵循最小化暴露原则，通过虚拟局域网划分隔离不同业务流量，限制横向渗透的可能性。流量加密技术需覆盖从终端到云端的全链路，确保协议交互过程中指令与数据的机密性。

（三）数据安全需求

数据作为智能电网的核心资产，其安全需求贯穿采集、传输、存储与处理全流程。在数据采集环节，智能电表与传感器产生的海量运行数据需防范恶意篡改，例如通过时间戳校验与哈希值比对确保数据源的真实性^[3]。数据传输过程中，无线通信信道易受窃听威胁，需采用端到端加密技术防止敏感信息泄露。数据存储阶段面临的关键挑战包括非授权访问与持久性潜伏攻击，例如利用数据库漏洞植入恶意代码以长期窃取用户用电行为数据。数据完整性需通过多副本校验与区块链存证技术保障，防止历史记录被篡改。此外，数据聚合分析过程中存在隐私泄露风险，例如通过用电负荷数据反推用户生活习惯。为此，需建立细粒度访问控制策略，基于角色权限限制数据调阅范围。

二、智能电网环境下电力系统信息安全防护技术

（一）加密与防火墙技术

智能电网的加密技术通过算法转换保障数据在传输与存储过程中的不可读性，形成抵御窃听与篡改的核心防线。对称加密算法以效率优势适配终端设备间实时通信场景，例如智能电表与集中器之间的高频数据交互；非对称加密则通过公私钥机制解决密钥分发难题，适用于云端平台与分布式节点的身份验证^[4]。防火墙技术作为网络边界守护者，基于预定义规则对进出流量进行深度检测，传统包过滤防火墙通过分析IP地址与端口信息拦截非法访问，而下一代智能防火墙引入协议识别与行为分析功能，可识别伪装成合法流量的恶意指令。在智能电网异构网络环境中，防火墙需支持工控协议深度解析，例如对Modbus、DNP3等电力专用协议的指令合规性校验，防止攻击者伪造控制报文引发设备误动作。

（二）入侵检测与防御系统

入侵检测系统通过持续监控网络流量与设备行为识别潜在威胁，其核心能力体现在对已知攻击特征的精准匹配与未知异常模式的自适应发现。基于特征的检测方法依赖规则库比对，可高效识别勒索软件、木马程序等已知攻击签名；基于行为的检测则通过机器学习建立正常操作基线，对偏离常态的登录频次、数据包大小等指标触发预警。防御系统需实现检测与响应的闭环联动，例如当检测到SQL注入攻击时自动阻断源IP并隔离受感染节点。在智能电网高动态环境中，防御策略需具备实时更新能力，通过威胁情报平台获取最新攻击特征库，同步调整检测规则与阻断阈值。针对高级持续性威胁，系统需融合多源日志进行关联分析，例如将防火墙日志、身份认证记录与设备运行状态交叉验证，识

别跨层攻击链条^[5]。

（三）身份认证与访问控制技术

身份认证技术通过多维度验证确保操作者身份真实性，防止非法人员冒用合法凭证渗透系统。动态口令认证结合时间因子与硬件令牌生成一次性密码，有效抵御重放攻击；生物特征认证利用指纹、虹膜等生理标识提升认证强度，适用于调度中心等高安全区域^[6]。访问控制技术基于最小权限原则限制用户操作范围，角色基访问控制模型将运维人员、设备厂商等主体划分为不同权限组，实现设备调试、数据查询等功能的细粒度管控。属性基加密技术进一步拓展控制维度，依据用户属性动态解密数据，例如仅允许具备“故障检修”属性的工程师访问特定变电站的故障日志。在零信任架构下，持续认证机制取代传统的一次性登录验证，通过分析用户行为模式、设备指纹与环境风险实施动态权限调整。

三、智能电网环境下电力系统信息安全防护体系的构建

（一）防护体系的构建原则

智能电网信息安全防护体系的构建需以风险动态适应为核心准则，通过威胁建模与风险评估确定防护优先级。风险导向原则要求依据电力业务场景划分安全域，例如将调度控制中心与用户侧计量系统划分为不同保护等级，针对性配置加密强度与访问控制策略。技术与管理协同原则强调软硬件防护措施与制度规范的联动，防火墙规则更新需同步调整运维人员操作权限，漏洞修补流程需与设备停机维护窗口期匹配。持续演进原则体现为防护能力的迭代升级，通过攻防演练验证现有机制的有效性，结合新型攻击模式优化检测算法与响应逻辑^[7]。标准化原则要求统一安全基线配置，例如规定智能电表固件版本强制升级周期、通信协议最低加密等级，避免异构设备因配置差异形成安全短板。弹性设计原则确保系统在遭受攻击时维持核心功能运行，例如通过流量重定向机制绕过受感染节点，保障电力监控数据的持续采集与传输。

（二）防护体系的架构设计

分层防御架构将智能电网安全防护划分为物理层、网络层、数据层与应用层四个逻辑层级。物理层防护聚焦设备可靠性，采用防电磁屏蔽机柜与抗震安装支架保护关键控制器，部署红外热成像仪监测设备过热风险。网络层构建多级隔离机制，在变电站内部部署工业防火墙分割控制网与办公网，利用虚拟专用网络建立跨区域加密隧道^[8]。数据层实施全生命周期管控，采集端嵌入轻量级加密芯片防止原始数据泄露，存储系统采用分布式账本技术确保操作记录不可篡改。应用层通过沙箱技术隔离第三方软件运行环境，限制非授权程序调用电网控制接口。横向协同机制连接各层级防护模块，当网络层检测到异常访问时自动触发数据层的访问日志分析，同步通知物理层启动设备状态检查。纵向纵深防御通过部署入侵检测系统、蜜罐诱捕节点与终端响应代理，形成从边界到核心的梯度式防护网。

(三) 防护体系的管理维护

全周期安全管理要求建立覆盖规划、实施、监控、优化的闭环流程。规划阶段制定资产清单与威胁图谱,明确变电站、智能电表等关键节点的防护等级与责任主体。实施阶段采用灰度发布策略,先在试点区域测试新防火墙规则对业务连续性的影响,再逐步推广至全网。监控阶段部署统一安全运营中心,聚合设备日志、网络流量与用户行为数据,利用关联分析引擎识别跨系统攻击痕迹^[9]。优化阶段建立漏洞响应知识库,将每次安全事件的处置方案转化为标准化操作手册。人员能力建设需设计阶梯式培训体系,基层运维人员掌握设备安全配置技能,管理人员精通风险评估与应急决策。供应链安全管理要求对硬件供应商实施安全资质审核,在设备固件中植入防篡改芯片,确保第三方组件符合电网安全标准^[10]。持续审计机制通过自动化工具定期检查防火墙策略有效性,人工抽查核心系统的权限分配合规性,形成内外结合的监督体系。退役设备处理流程需彻底清除存储介质数据,物理

销毁无法擦除信息的芯片组件,阻断敏感数据通过二手设备流通的泄露风险。

四、结语

综上所述,智能电网环境下电力系统信息安全防护体系构建是一项复杂且关键的任务。从物理安全、网络安全到数据安全,明确其多样化的安全需求是防护体系建设的基础;加密与防火墙、入侵检测与防御等先进技术的合理运用,为信息安全提供了有力的技术支撑;遵循系统性、动态性等原则进行架构设计,并通过完善的管理维护机制保障运行,构成了完整的防护体系框架。然而,智能电网信息安全威胁不断演变,未来需持续关注新兴技术带来的安全风险,进一步优化防护体系的动态适应性与协同性。

参考文献

- [1] 许正利. 电力系统信息安全管理体系建设技术分析 [J]. 电工技术, 2024, (S2): 478-480.
- [2] 宋凯. 电力系统信息安全威胁与漏洞分析及防范研究 [J]. 中国信息化, 2024, (08): 81-82.
- [3] 孙军鹏, 殷衡. 探究电力系统信息安全防护体系的构建与完善 [J]. 数字通信世界, 2020, (08): 263-264.
- [4] 靳玉晨, 王兴, 陈施, 等. 电力系统信息安全基线标准体系的构建策略探究 [J]. 长江信息通信, 2021, 34(11): 153-155.
- [5] 刘嘉琪, 潘凌玲. 电力系统中的内部网络信息安全措施分析 [J]. 电子技术, 2022, 51(11): 242-243.
- [6] 周泽元, 班秋成, 陶佳冶. 电力系统信息安全的重要性及防护探微 [J]. 网络安全技术与应用, 2021, (04): 151-152.
- [7] 王玉菲. 电力系统信息安全管理体系建设技术分析 [J]. 信息系统工程, 2021, (03): 37-39.
- [8] 张莉. 智能电网技术在电力系统中的应用与前景 [J]. 江西电力, 2023, 47(06): 36-39.
- [9] 曾梦好, 李斯陶. 从物理电网到数字电网——电力系统技术发展历程与趋势展望 [J]. 中国电力企业管理, 2022, (19): 90-93.
- [10] 郑皓元. 智能电网在电力技术及电力系统规划中的应用分析 [J]. 中国科技投资, 2021, (16): 14-15.