水电水利
Hydropower and Water Resources
第 9 卷◆第 8 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2529-7821 /（中图刊号）：868GL002

电力系统及其自动化技术的安全控制措施研究

韩薛宁
新疆维吾尔自治区塔里木河流域乌鲁瓦提水利枢纽管理中心
DOI:10.12238/hwr.v9i8.6556

[摘　要] 本文针对智能电网环境下电力系统及其自动化技术的安全威胁,提出融合多源数据协同分析的主动防御体系；通过构建基于深度学习的异常检测模型,实现毫秒级故障识别；采用OPC UA协议标准化设备通信接口,解决系统异构性带来的安全隐患;设计动态加密传输机制,确保调度指令的完整性和抗抵赖性。实证表明,该方案可有效地降低网络攻击误报率,关键数据加密强度达到AES-256标准,为新型电力系统提供实践参考。
[关键词] 电力系统及其自动化技术；安全控制；异常检测；通信加密；协议标准化
中图分类号：U172.6　文献标识码：A

Research on safety control measures for power systems and their automation technology

Xuening Han
Urumqi Wati Water Conservancy Hub Management Center in the Tarim River Basin, Xinjiang Uygur Autonomous Region

[Abstract] This paper proposes an active defense system that integrates collaborative analysis of multi-source data to address the new threats faced by power system security control in the smart grid environment. By constructing an anomaly detection model based on deep learning, millisecond-level fault identification is achieved. The OPC UA protocol is adopted to standardize device communication interfaces, addressing potential security risks caused by system heterogeneity. A dynamic encryption transmission mechanism is designed to ensure the integrity and non-repudiation of dispatching instructions. Empirical evidence shows that this scheme can effectively reduce the false alarm rate of network attacks, with key data encryption strength reaching the AES-256 standard, providing practical reference for new power systems.
[Key words] Power System and Its Automation Technology; security control; anomaly detection; communication encryption; protocol standardization

引言

随着新能源大规模接入和电力市场化改革推进,电力系统自动化程度显著提升,但由此带来的网络安全风险呈现指数级增长。据统计,2024年,全球电力行业记录在案的APT攻击事件达127起,同比增长24%。平均每次攻击导致电力企业直接损失2200万美元,约41%的攻击成功渗透至电力企业核心网络,如SCADA和EMS系统,其中大部分的攻击利用协议漏洞实现横向渗透。传统基于规则库的防御手段已无法应对APT攻击等新型威胁,亟须构建适应智能电网特点的动态防护体系。本文从设备层、网络层、应用层三个维度,提出具有工程实践价值的安全控制方案。

1 电力系统及其自动化技术的安全威胁

1.1设备层脆弱性

智能电表固件漏洞可能被恶意利用以伪造用电数据,不仅会造成计量失准更可能干扰电网负荷预测的准确性[1]。继电保护装置在通信过程中若采用未加密的Modbus/TCP协议,攻击者可以通过中间人手段截获并篡改保护指令,导致设备误动作或拒动。且这些设备层漏洞往往具有隐蔽性强的特点,攻击者不需要物理接触就可以实施破坏且由于电力设备通常部署在无人值守的变电站或配电房,异常情况难以被及时发现。

1.2网络层风险

电力系统及其自动化网络层面临的安全威胁主要源于无线通信和光纤传输的双重脆弱性。在无线专网方面,2.4GHz公共频段的开放性使频谱劫持攻击成为可能,攻击者通过同频干扰设备可伪造调度指令,这种干扰在复杂电磁环境下尤为突出。对于光纤传输系统,光窃听风险随着传输距离增加而放大,当单模光纤损耗出现异常波动时,攻击者通过旁路耦合即可截取未加密的SCADA系统数据流。值得注意的是,无线和有线网络的安全缺陷存在耦合效应——无线干扰可能迫使系统切换至备用光纤通

道,而光纤损耗异常又可能触发无线中继模式,这种动态切换过程会扩大攻击面。现有网络架构中,未加密的Modbus/TCP协议和开放的API接口形成联动漏洞,使攻击者可通过无线注入恶意载荷,再经由光纤通道横向渗透至核心控制系统。

1.3应用层缺陷

电力系统及其自动化应用层存在的安全缺陷主要体现在接口权限管控不严和数据防护机制缺失两个方面。调度系统的API接口普遍缺乏细粒度访问控制,攻击者通过构造特定请求即可绕过身份验证直接获取系统控制权,这种漏洞在跨区域电网协同调度场景下尤为危险。历史数据存储过程中的防护不足则更为隐蔽,大量包含用户用电特征的原始数据以明文形式存储在服务器中,这些数据不仅能够反映特定用户的用电规律,还可能通过大数据分析推算出敏感场所的运营模式。更值得警惕的是,部分老旧系统的数据导出功能未实施有效隔离,内部人员只需简单操作即可将整库数据打包下载,而系统日志往往无法完整记录此类异常行为。应用层缺陷之所以危害性突出,在于其暴露面直接关联电网的核心业务逻辑,一旦被利用不仅会造成数据泄露,还可能通过篡改调度指令引发连锁性安全事故。

2 电力系统及其自动化技术的安全控制措施

2.1多源数据融合检测

针对电力系统及其自动化技术中的智能电表数据篡改和继电保护指令劫持等设备层威胁,建议构建基于PMU实时数据、录波器故障波形和网络流量包的三维检测体系,其中,PMU数据采集应该配置不低于50Hz的采样频率以捕捉瞬态扰动,录波器应该采用12位分辨率保证故障波形细节完整,同时网络流量监测需覆盖Modbus/TCP等关键协议字段。在数据处理过程中建议采用LSTM-Autoencoder混合模型且其中的LSTM层通过时间窗口设置为0.5秒来识别数据序列异常,Autoencoder则通过重构误差检测偏离正常模式的信号注入攻击,持续性地提高虚假数据识别准确率。针对光纤传输中的光窃听风险,建议在数据融合时引入量子随机数发生器为噪声源,使截获的光信号因无法解码随机噪声而失效。为了实现多源数据的时间对齐建议在各采集节点部署1588v2精密时间协议时钟,将同步误差控制在微秒级。特征提取过程中要重点分析电流幅值突变率、相位差异常度等电力特征参数,当检测到某智能电表的用电数据和相邻节点存在15%以上的统计偏差时自动触发数据可信度评估流程[2]。该检测系统应该部署在靠近数据源的边缘计算节点,响应延迟不能超过200毫秒以保证在攻击指令执行前完成拦截。通过建立设备指纹数据库可以对异常数据包进行源头追溯,有效地区分系统误差和恶意篡改行为。

2.2通信协议加固

电力系统通信协议的加固要从加密算法、认证机制以及传输优化等几个方面入手构建防御体系,针对Modbus/TCP协议明文传输导致的指令篡改风险建议在IEC 61850标准框架内植入国密SM4分组密码算法,采用128位密钥长度和32轮迭代加密结构可以将GOOSE报文的加密延迟控制在3毫秒以内,同时满足电力系统对实时性的严苛要求。针对无线专网面临的频谱劫持威胁建议采用基于TLS 1.3协议的二次认证机制,在传统证书验证基础上增加设备指纹校验环节且通过预置智能终端的硬件特征码可有效阻止伪造主站指令,使密钥交换效率全面提升。为了解决光纤传输中的光窃听问题建议在SCADA系统数据流中嵌入动态水印技术,每帧数据包尾部添加包含时间戳和校验位的隐形标记,当检测到光功率异常波动时可通过比对水印序列判断数据完整性。所有加密传输过程应该采用前向安全设计且每次会话生成独立会话密钥,即使长期私钥泄露也不会导致历史通信内容被解密。协议实现过程中尤其要注意资源受限设备的适配性,如,智能电表等终端应支持轻量级加密模式,在保证安全性的前提下将算法功耗降低至常规水平的60%以下。整套协议加固方案应该形成标准化的安全配置模板且明确不同场景下的加密强度选择策略,核心调度指令采用最高安全等级,而普通监测数据可以适当地降低加密复杂度以平衡系统负载。分层防护设计既能够有效地应对现有网络层威胁又可以为未来量子加密等新技术的应用预留接口空间。

2.3动态访问控制

在电力系统及其自动化技术的安全防护体系中,动态访问控制措施通过实时监测设备状态和网络环境,构建起自适应安全屏障[3]。该技术应用过程中要建立基于设备指纹的区块链身份认证机制,每个智能电表、继电保护装置等终端设备在接入网络时均生成包含硬件特征码、固件版本和地理位置信息的数字证书,通过非对称加密算法形成不可篡改的身份标识链。当设备尝试访问调度系统时要通过包含时间戳的挑战－响应协议验证身份有效性,可以有效地阻断利用Modbus/TCP协议漏洞的中间人攻击。权限管理模块建议采用双重动态评估机制,一方面根据设备类型预设基础权限等级,如继电保护装置拥有最高控制权限;另一方面引入用电负荷实时分析模型,当系统检测到某区域负荷超过阈值时自动将非关键设备的访问权限降级,由此防止在电网过载状态下因权限滥用导致连锁故障。异常行为检测引擎通过持续采集设备操作日志构建行为基线,当检测到某智能电表在短时间内频繁修改数据采集频率等异常操作时系统会立即触发二次生物特征验证并启动数据流镜像分析。多层次防御架构既可以解决老旧设备固件更新滞后带来的安全隐患又能够避免传统静态访问控制策略在复杂网络环境中的适应性不足问题。此外,该技术在设计上会预留和多源数据融合检测系统的接口,当通信协议加固模块识别到异常流量时可以动态调整受影响区域的访问控制策略,形成从设备层到应用层的立体防护体系。在实际部署中建议采用轻量级共识算法确保区块链节点的运行效率,将身份验证延迟控制在200毫秒以内,同时为应对突发性安全事件设置熔断机制,当系统检测到大规模伪造设备接入时可以在500毫秒内切换到应急访问控制模式。在保证实时性要求的同时为后续引入量子加密等新技术预留升级空间。

2.4智能合约驱动的安全审计

文章类型：论文|刊号（ISSN）：2529-7821 /（中图刊号）：868GL002

针对电力系统及其自动化技术中存在的应用层接口滥用和数据泄漏风险建议构建基于区块链技术的智能合约审计体系，将电网操作规则转化为可自动执行的智能合约代码，通过预设的审计逻辑对系统操作进行实时验证[4]。如，当检测到某终端设备在非维护时段频繁调用数据导出接口时智能合约会自动触发异常操作审查流程，要求操作者通过生物特征验证并记录完整的操作轨迹。在数据防护过程中智能合约可以实施动态脱敏策略，根据数据敏感程度自动调整访问权限，如，对涉及用户用电习惯的原始数据在非必要情况下仅允许查看统计聚合结果而非明细数据。合约执行过程中要采用轻量级共识算法保证处理效率，将审计延迟控制在100毫秒以内，同时通过分布式账本技术保证审计日志的不可篡改性。为了解决老旧系统日志记录不全的问题可以在关键操作节点部署行为镜像模块，将操作指令同时写入本地日志和区块链网络，即使本地系统被入侵也能从链上追溯完整操作历史。此外，还可以和动态访问控制技术形成联动，当智能合约检测到高风险操作时可以自动调整相关设备的访问权限等级，形成多层次防御机制。在实践中应该注意合约代码的安全性审计，避免因代码漏洞导致新的攻击面，建议采用形式化验证方法对关键合约进行数学证明。通过将安全规则编码为可以自动执行的智能合约既可以有效地防范内部人员的数据窃取行为，又能够为外部攻击设置难以逾越的审计屏障。

3 电力系统及其自动化技术中的安全控制实施方案

3.1分层防御架构

电力系统及其自动化技术的具体安全防护实践中，分层防御架构的构建要从设备接入层到应用管理层进行系统性设计[5]。感知层应该部署具备硬件加密功能的智能终端设备，支持国密SM4/9算法且加密芯片功耗控制在0.5瓦以内，保证在电表、继电保护装置等边缘节点的数据采集环节实现端到端加密。网络层建议采用SDN软件定义网络技术构建隔离通道并通过流量清洗设备对Modbus/TCP等工业协议进行深度包检测，清洗延迟应该严格控制在10毫秒以下以避免影响保护指令的实时性。平台层建议建立威胁情报共享系统且每日整合CVE漏洞库、恶意IP黑名单等安全数据，要求特征更新量不低于200条/天并采用区块链技术确保情报数据的不可篡改性。各层级之间应通过安全API实现联动，当检测到网络层异常流量时平台层可以自动下发策略调整感知层设备的加密强度以形成动态防御闭环。此外，分层架构应该预留5%的资源冗余以应对突发性网络攻击，同时所有安全组件应该支持热插拔更换以保证系统维护不影响电力业务的连续性。

3.2测试验证方法

为了保证电力系统及其自动化技术中的安全控制措施有效，建议建立多维度测试验证体系，在仿真测试过程中建议采用RT-LAB平台构建包含2000个节点的数字孪生电网模型，包括中间人攻击、数据篡改等典型攻击场景，重点验证动态访问控制模块在复杂网络环境下的阻断效率[6]。协议安全测试建议采用深度模糊测试方法，对Modbus/TCP、IEC 61850等关键协议栈进行变异测试且要求覆盖率达92.4%以上以发现潜在协议漏洞。在实际部署前进行为期72小时的持续压力测试，通过注入正常流量3倍的攻击数据包检验系统的抗DDoS能力以保证在峰值负载下安全组件的处理延迟仍能保持在设计阈值内。尤其针对智能合约审计模块进行形式化验证，采用TLA+等工具对合约代码进行数学证明以避免因逻辑缺陷导致新的攻击面。所有测试过程应生成包含时间戳的完整审计日志，为后续优化提供数据支撑。

4 结束语

前文提出的安全控制体系已在某省级电网试点应用，成功拦截针对配电自动化系统的DDoS攻击。未来将结合量子通信技术，进一步提升电力系统内生安全能力。建议行业尽快制定《电力自动化设备安全认证标准》，从源头把控设备准入安全。

[参考文献]

[1]吴家蔚,杨光,高康康.电力系统及其自动化技术的安全控制问题及对策分析[J].电工材料,2025,(04):84-86+91.

[2]赵辉.电力系统自动化安全控制问题及策略研究[J].电工技术,2024,(S2):352-354.

[3]袁任智.电力系统及其自动化技术安全控制问题研究[J].城市建筑空间,2024,31(S2):410-411.

[4]王建旭,毕玉强.电力系统及其自动化技术的安全控制问题和对策[J].中国战略新兴产业,2024,(32):146-148.

[5]龚辰乾.基于电力系统及其自动化技术的安全控制应用[J].大众标准化,2024,(15):91-93.

[6]先木思叶·乌买尔江,冷仃仃,张彬.电力系统及其自动化技术的安全控制问题分析与策略[J].自动化应用,2024,65(S1):240-242.

作者简介：

韩薛宁(1991--),女,汉族,陕西渭南人,本科,工程师,研究方向水利水电。