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

# 基于智能终端接入的电力营销安全策略探析

左学飞
国网河北省电力有限公司武安市供电分公司
DOI:10.12238/hwr.v9i7.6466

[摘　要] 随着智能电网建设深入推进,智能终端设备在电力营销系统中的应用日益广泛。智能终端接入过程中的安全防护问题逐渐凸显,严重影响电力营销业务的稳定运行。通过分析智能终端电力营销接入技术架构,深入探讨终端认证机制漏洞、传输通道安全缺陷及用户数据保护不足等薄弱环节。针对识别出的安全隐患,提出终端身份认证加强、传输加密通道构建以及用户数据分级保护等防护技术方案。同时构建包含安全监测预警、综合防护配置和应急处置在内的电力营销安全策略,形成全方位的安全防护机制。研究成果对提升电力营销系统安全防护水平、保障智能终端可靠接入具有重要实践指导意义。
[关键词] 智能终端；电力营销；安全防护；身份认证；数据保护
中图分类号：TM727　文献标识码：A

## Analysis of Power Marketing Security Strategies Based on Intelligent Terminal Access

Xuefei Zuo
Wu 'an Power Supply Branch of State Grid Hebei Electric Power Co., LTD

[Abstract] With the in-depth advancement of smart grid construction, the application of intelligent terminal devices in the power marketing system is becoming increasingly widespread. The security protection issues during the access process of intelligent terminals have gradually emerged, seriously affecting the stable operation of power marketing business. By analyzing the technical architecture of the power marketing access of intelligent terminals, this paper deeply explores the weak links such as the loopholes in the terminal authentication mechanism, the security defects of the transmission channel, and the insufficient protection of user data. In response to the identified security risks, protective technical solutions such as enhanced terminal identity authentication, construction of transmission encryption channels, and hierarchical protection of user data are proposed. At the same time, a comprehensive operation support system including safety monitoring and early warning, integrated protection configuration and emergency response should be constructed to form an all-round safety protection mechanism. The research results have significant practical guiding significance for enhancing the security protection level of the power marketing system and ensuring the reliable access of intelligent terminals.
[Key words] Intelligent terminal Electric power marketing Safety protection; Identity authentication Data protection

## 引言

智能电网建设快速推进促使电力营销业务走向智能化转型,智能终端设备作为电力用户和营销系统间重要接口,承载用电信息采集与费用结算等核心业务功能。随着智能终端接入规模持续不断扩大,设备认证机制缺陷、数据传输安全威胁、用户信息保护不足等问题逐渐显现出来,严重制约着电力营销业务的安全稳定开展。智能终端接入安全涉及设备、通信、数据等多个不同层面,需要建立起一套系统化的防护体系,深入研究智能终端接入安全防护相关技术,构建起完善的安全运行支撑体系,对保障电力营销业务安全稳定运行有着重要现实意义[4]。

## 1 智能终端电力营销接入技术架构

### 1.1营销业务接入模式

智能终端设备是电力营销系统重要的数据采集和业务交互节点,采用分层分布式接入模式。在物理层面,终端设备通过无线通信网络、光纤专网等多种方式接入营销主站系统,在逻辑层面,基于统一身份认证平台来实现设备接入鉴权。营销业务接入模式涵盖客户用电信息采集、电费结算、用电分析等多项功能,各项业务数据通过标准化接口传输至营销主站以实现业务全流

程线上交互,该接入模式依托数据加密传输通道构建了端到端的安全防护机制,在数据传输过程中采用身份认证、访问控制等多重安全措施来确保数据传输安全可靠。智能终端接入系统支持灵活扩展,可根据业务需求动态调整接入配置以满足电力营销业务快速发展需求,系统运行过程中通过实时监测和性能优化保障接入系统稳定运行。

1.2终端设备部署框架

终端设备部署采用“集中管理、分散接入”这种框架结构,在用户侧安装智能电表和采集终端等设备以负责采集用电数据,在网络层部署通信单元来确保数据可靠地传输,在系统层设置接入网关以统一管理终端设备接入认证。部署框架里各组件之间通过标准化协议进行通信从而实现数据的安全交互。设备部署过程严格执行安全规范对终端设备做统一编码和注册管理并建立设备台账确保设备可管可控,框架设计充分考虑系统可扩展性预留接口支持新型终端设备接入,设备部署采用模块化设计让各功能模块独立运行且相互协同以提高系统整体可靠性。设备管理平台实现终端设备全生命周期管理涵盖设备注册、参数配置、状态监测、远程维护等功能保障终端设备规范化运行。

## 2 智能终端营销系统接入安全薄弱点

2.1终端认证机制漏洞

智能终端设备接入电力营销系统时认证机制有多个安全隐患点,设备认证过程采用静态密钥管理且密钥更新周期长会有被非法截获和破解风险,认证协议设计实现时未充分考虑防重放攻击机制让认证过程易受中间人攻击。部分终端设备用简单用户名密码认证且密码强度不足存储形式单一增加非法接入风险,设备身份标识容易被仿冒攻击者可篡改标识信息实现非授权接入规避系统安全审计。认证过程中,会话管理机制不完善以及会话密钥易泄露会致使认证状态被劫持,设备认证机制缺乏动态适应能力不能根据安全威胁等级调整认证策略。多终端并发接入场景下认证性能降低会影响业务响应效率,认证日志记录不完整难以实现安全事件有效追溯和责任界定,同时认证系统缺乏统一的认证策略管理平台各终端认证参数配置分散难以集中管控增加运维管理难度。认证过程中的密钥更新机制执行不严格存在过期密钥继续使用情况,从而加大系统安全风险。

2.2传输通道安全缺陷

营销系统的数据传输通道目前正面临极为严峻的安全威胁,通信协议存在加密算法选择不恰当以及密钥管理机制薄弱等诸多问题,这使得数据传输过程中机密性保护处于明显不足的状态。传输通道因缺乏有效的完整性校验机制,导致数据容易被篡改且无法得到及时发现,网络层面未实施严格的访问控制策略,进而致使传输通道容易遭受拒绝服务攻击。数据传输过程中的协议交互信息未进行脱敏处理,使得关键业务参数容易被窃取,通信链路加密强度不够,难以应对量子计算等新型解密技术带来的挑战。传输通道的带宽资源分配存在不合理情况,容易造成业务数据传输出现拥塞现象,链路冗余设计不够完善,单点故障风险表现得十分突出显著[3]。传输过程中缺乏实时流量监测和异常检测机制,难以及时发现和有效处置网络攻击行为,安全通信协议版本更新比较滞后,已知漏洞修复不够及时。传输通道安全配置参数缺乏定期检查和更新机制,部分配置参数长期处于默认状态,增加了系统安全隐患,传输链路质量监控能力不足,无法及时发现信道衰减和干扰问题。

2.3用户数据保护不足

智能终端采集的用户数据在存储处理环节存在明显安全缺陷,数据加密存储机制不完善易使敏感信息遭未授权访问,数据分级管控制度执行不到位致不同安全等级数据未有效隔离,数据访问权限管理粗放且缺乏基于角色的细粒度授权机制。数据备份恢复策略不健全难以应对勒索软件等恶意攻击,用户隐私保护意识不足导致数据采集范围超业务必要性,数据脱敏规则不严谨间接提升用户敏感信息泄露风险,数据销毁流程不规范使得历史数据残留问题比较突出。数据处理过程中审计追踪能力欠缺无法有效监控数据流转,数据共享接口安全防护不足让跨系统数据交换存在隐患,数据质量控制机制缺失影响数据分析结果准确可靠。同时数据安全管理制度执行力度不够且缺乏有效监督考核机制,导致各项安全措施落实不到位,数据安全培训体系不完善使相关人员安全意识和技能水平有待提升。

## 3 电力营销终端接入防护技术研究

3.1终端身份认证加强

针对终端认证机制存在的漏洞构建多因素动态认证体系,引入基于硬件信任根的设备指纹技术并结合设备唯一标识码、物理特征信息生成设备身份标识以提升设备身份真实性。采用非对称密钥基础设施(PKI)实现设备证书的全生命周期管理且支持证书自动更新与吊销,部署动态令牌认证机制基于时间戳和随机挑战响应实现防重放保护。建立分级认证模式根据业务安全等级动态调整认证强度,优化认证协议采用国密算法SM2、SM3、SM4构建安全通道抵御量子计算威胁。设计会话管理机制实现认证会话的自动超时与强制注销,完善认证日志记录采集设备接入全流程信息支持安全事件追溯分析,构建认证性能优化机制采用多线程并发处理提升认证效率。设计认证协议兼容框架支持多种认证方式灵活切换,建立认证策略动态调整机制根据威胁情报及时更新认证规则,实现认证状态实时监控快速识别异常认证行为。

3.2传输加密通道构建

建立起端到端的加密传输机制来保障数据传输安全,部署轻量级安全传输协议(DLTS)并支持国密算法套件以确保传输通道机密性和完整性,实现传输报文的分组加密并采用CBC模式保护数据块链接关系,设计密钥协商机制且支持会话密钥定期轮换从而降低密钥泄露风险。构建传输通道的冗余备份以实现链路故障时自动切换,部署深度包检测技术用于实时监测数据流量异常情况,建立传输通道的准入控制并基于白名单机制限制非法连接,优化带宽资源调度算法来保障关键业务数据优先传输。实现传输协议版本兼容并支持协议安全补丁动态更新,设计传输质量监测机制采集链路状态指标评估传输性能,构建传输

通道安全隔离区域防止业务数据出现串扰，部署传输通道负载均衡以提升数据传输的整体效率[1]。建立传输异常告警机制实现故障的快速定位工作，实现传输通道动态扩容满足业务不断增长的需求。

3.3用户数据分级保护

构建起全方位的数据安全防护体系来达成用户数据精细化管理，建立好数据分类分级标准并制定差异化保护策略，部署一套数据加密存储系统采用双重加密方案保护敏感数据。实现数据访问控制矩阵基于最小权限原则开展授权管理，设计出数据脱敏规则引擎支持多种脱敏算法灵活配置，建立起数据全生命周期管控机制规范数据各环节全过程。部署一套数据防泄漏系统实时监测异常的数据访问行为，优化数据备份策略采用增量备份方式减少存储开销，实现数据容灾备份以此保障业务运行的连续性。建立数据质量评估体系从多维度对数据质量进行考核，设计数据共享接口规范达成安全可控的数据交换操作，构建数据安全审计平台详细记录数据操作的具体轨迹[2]。部署数据识别引擎以便自动发现数据里的敏感信息，实现数据访问行为分析准确识别异常操作的模式，建立数据安全应急响应机制快速处置各类数据安全事件。

## 4 基于智能终端接入的电力营销安全策略

4.1构建安全监测预警机制

构建起全方位的安全态势感知平台以达成智能终端接入过程的立体化监控，部署智能安全探针来采集终端接入行为、数据传输状态以及系统运行指标等多维数据，建立安全事件关联分析引擎并融合设备状态信息、网络流量特征和用户行为模式等数据以构建安全威胁识别模型。设计分级预警机制且依据威胁等级自动触发相应的响应策略，开发异常行为检测算法并基于机器学习技术识别潜在的安全风险，实现安全态势的可视化展示从而直观呈现系统的安全状况。构建预警信息推送机制以支持多渠道的告警通知，建立安全监测指标体系用于量化评估系统的安全水平，设计监测性能优化机制从而降低系统资源的占用，部署监测节点灾备方案来确保监测服务的持续性[5]。完善监测数据存储机制以支持历史数据的统计分析，建立监测规则动态更新机制从而适应新型的安全威胁。

4.2搭建综合防护体系配置

搭建起多层级纵深防御体系以此实现智能终端接入全流程安全防护，部署边界防护设备进而构建终端接入区域安全隔离环境，实现网络访问控制并基于身份识别和行为特征做精细化管控，建立安全基线配置标准来规范终端设备安全参数设置。设计防护策略联动机制从而实现多防护设备协同响应，构建安全策略智能调优系统以动态优化防护规则，部署高可用防护架构用于消除单点防护风险，建立防护效果评估机制并定期开展渗透测试验证。实现防护设备集中管理达成统一策略下发与状态监控，优化防护资源调度算法以此提升系统整体防护效率，完善防护日志审计功能用以支持安全事件追踪分析，构建防护知识库来积累防护经验沉淀最佳实践。

4.3科学设计应急处置流程

建立一套完善的应急响应体系来提升安全事件处置能力，制定分级响应预案明确不同类型安全事件处置流程，建立应急指挥决策机制确保响应过程统一协调。设计快速隔离方案防止安全事件扩散蔓延，构建应急资源调度平台实现人员设备快速调配，开发应急处置工具集提供自动化的处置手段，建立事件溯源分析机制查明事件原因及影响范围。设计应急演练方案定期开展实战训练提升处置水平，完善事件总结复盘机制持续优化应急预案内容，构建知识经验共享平台促进应急处置能力提升，实现应急处置全程记录以支持事后评估改进工作。建立跨部门协同机制提升综合应急处置效率，设计恢复方案验证机制确保业务系统可靠恢复，完善应急预案定期更新机制以适应新型安全威胁。

## 5 结语

智能终端接入电力营销系统的安全防护是一项系统工程，需要从技术架构、安全防护到运行支撑等多个维度协同推进。通过构建多层次的身份认证机制、建立安全可靠的传输通道、实施严格的数据分级保护，能够有效应对当前面临的各类安全威胁。同时，借助安全监测预警、综合防护配置和应急处置流程，形成闭环管理机制，不断提升系统整体安全防护水平。未来，随着新技术的发展，智能终端接入安全防护体系还将持续优化完善，为电力营销业务的安全稳定运行提供更加可靠的保障。

## [参考文献]

[1]汤心韵,张成林,曾红艳,等.混合现实技术用于电力营销安全培训综述[J].电脑知识与技术,2024,20(34):110-112+116.

[2]张成林,徐振宇,孙文彬,等.MR虚实融合技术在电力营销现场作业安全培训中的应用[J].大众用电,2024,39(10):54-55.

[3]段凯,李竹,刘锋,等.浅析电力营销数据开放与共享安全治理[J].中国新通信,2023,25(02):125-127.

[4]曹小霞.电力营销中的安全风险问题及其治理对策分析[J].营销界,2022,(16):80-82.

[5]卫程.基于5G技术的电力营销安全智能化现场作业系统研究[J].电工电气,2021,(11):63-67.

## 作者简介：

左学飞(1985--),男,汉族,河北省武安市人,本科,助理工程师,研究方向：营销安全。