

# 《电力无线局域网安全体系结构要求》编制说明

（征求意见稿）

## 一、工作简况

### 1 主要工作过程

起草筹备阶段：由国网山西省电力有限公司电力科学研究院牵头，成立标准编写工作组。工作组按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》要求，结合电力无线局域网应用场景与安全需求，开展调研分析，明确标准覆盖范围、核心框架及关键技术方向，制定标准大纲并形成草案稿。

标准立项阶段：2025年11月，在南京召开了第一次标准的专家立项评审会，经中国电工技术学会标准工作委员会专家组审议，批准《电力无线局域网安全体系结构要求规范》标准立项；

编写研制阶段：

标准编写组围绕电力无线局域网安全目标、安全原则、攻击威胁分析、安全体系设计、加密与解密、安全审计与监控、设备安全等核心内容，开展多轮研讨与技术论证。针对标准草案稿中的技术细节、条款表述、合规性要求等进行反复打磨，优化完善安全体系架构、加密算法选型、事件处理流程等关键内容，最终形成《电力无线局域网安全体系结构要求》征求意见稿，为电力无线局域网全生命周期安全管理提供标准化依据。

### 2 主要参加单位和起草工作组成员及其所做的工作

标准编写组收集了近几年来电力无线局域网安全体系方面的相关资料，通过对比整理分析确定了标准主要技术内容，由国网信息通信产业集团有限公司牵头完成标准编制、整理和完善，其他参与单位配合并负责收集相关资料、提出建议。

本文件起草单位：国网山西省电力有限公司电力科学研究院、北京中电飞华通信有限公司、南京博洛米通信技术有限公司、华北电力大学、国网信息通信产业集团有限公司研发中心。

本文件主要起草人：刘泽辉、琚贇、刘泽三、刘松阳、许剑、芦山、徐哲男、柴超、郭旻、孟雨、甘信灿、彭涛、丛诗奇、贾少堃、肖志鸿、王尧、周续然、刘浩宇、吴明锋、袁绪跃、闫俊、王成、武子杨、宋欣茹、陈靖语、刘志兵、何清榕、李飞扬、李春朋、孙芑岳。

## **二、标准编制原则和主要内容、**

### **1、标准编制原则**

a.本标准的起草遵循《GB/T 1.1—2020 标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定，以科学性、先进性和经济性为原则，坚持实事求是，遵守国家有关法律、法规，同时符合团体标准要求。本标准以可信计算、动态密钥管理及三层防御架构技术为基础，推动电力无线局域网安全防护体系的规范化建设工作。

b. 采用会议讨论的形式，集合密码学、通信协议、可信计算、电力系统安全等专家，将不同业务维度的专业技术融合一体，体现出标准编制的科学性、实用性和先进性。

### **2、标准主要内容**

本标准分为 10 个章节，（1）范围；（2）规范性引用文件；（3）术语和定义；（4）符号、代号和缩略语；（5）总则；（6）安全体系结构框架；（7）加密与解密；（8）无线局域网安全审计与监控；（9）设备安全。主要内容如下：

总则：提出保密性/可用性等 6 大安全目标，定义多层次防御等 7 项原则；

安全体系结构框架：构建 “终端防护-接入控制-全局监控” 三级协同防御架构，融合可信计算与分层设计方法论；

加密与解密：要求 AES-256/ECC 算法，规范密钥全生命周期管理；

无线局域网安全审计与监控审计与监控：定义日志完整性保护、SIEM 实时威胁关联分析机制；

设备安全：从物理防拆设计到软件沙箱隔离，覆盖硬/软件安全配置。

### **3、主要技术差异**

本标准为新制度标准，无主要技术差异。

### **4、解决的主要问题**

本文件解决电力无线局域网架构松散、行业定制缺失、认证机制不统一、密钥静态化、终端防护薄弱及合规难落地六大痛点，为电力、企业及公共 WLAN 提供全链路安全方案。

### 三、主要试验（或验证）情况

本标准不涉及试验（或研制）情况。

### 四、标准中涉及专利的情况

经关联，本标准的相关内容主要涉及以下五项专利，具体信息如下：

专利名称为《一种基于自适应蜜罐的智能安全接入方法及系统》，专利号为 CN202411152858；

专利名称为《一种电力物联网的安全防御方法及系统》，专利号为 CN202411153545.6；

专利名称为《一种智能化扫描非法网络的网络拟态与诱骗的方法及系统》，专利号为 CN202411153547.5；

专利名称为《一种网络隐身安全策略统一管控和快速编排的方法及系统》，专利号为 CN202411152854.1；

专利名称为《一种数据安全防护方法及系统、存储介质、计算机设备》，专利号为 CN202211347552.0。

### 五、预期达到的社会效益、对产业发展的作用等情况

（1）降低公共 Wi-Fi、电力行业企业网络被攻击风险，保护公民隐私与数据安全，防范金融诈骗、信息泄露等社会隐患；

（2）强制高等级加密（AES-CCMP）和双向认证（802.1X/WAPI），使得设备制造商、运营商淘汰落后技术，加速安全芯片、可信硬件等产业链创新；

（3）集中化管理降低企业运维成本，标准化设计推动跨厂商设备兼容，为智慧城市、工业互联网等场景提供可信无线底座，激发数字经济新业态。

### 六、与国际、国外对比情况

本文件在起草过程中参考和引用了以下国际与国内标准：

国际标准：

（1）IEEE 802.11-2020：无线局域网介质访问控制（MAC）和物理层（PHY）规范；

（2）IEEE 802.11i-2004：介质访问控制（MAC）安全增强；

（3）RFC 5246：传输层安全协议 TLS 1.2；

（4）RFC 3531：一种灵活管理 IPv6 地址块位分配的方法。

国内标准：

- (1) GB/T 20273-2019: 信息安全技术 数据库管理系统安全技术要求;
- (2) GB/T 17964-2021: 信息安全技术 分组密码算法的工作模式。

## **七、在标准体系中的位置，与现行相关法律、法规、规章及相关标准，特别是强制性标准的协调性**

本标准与现行标准体系协调一致。

## **八、重大分歧意见的处理经过和依据**

标准编制过程中广泛征集了专家意见，所有意见均按照标准编制程序进行了采纳，不存在重大分歧意见。

## **九、标准性质的建议说明**

建议本团体标准的性质为推荐性团体标准。

## **十、贯彻标准的要求和措施建议**

建议本标准批准发布 7 天后实施。

## **十一、废止现行相关标准的建议**

无

## **十二、其他应予说明的事项**

无