ICS 27.100
CCS F06/03

团　体　标　准

T/CES XXX-XXXX

电力无线局域网安全体系结构要求

Security Architecture Requirements for Electric Power Wireless Local Area Networks

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中国电工技术学会 发布

目 次

前　言

本文件按照 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》给出的规则起草。

请注意本文件的某些内容可能涉及专利，本文件的发布机构不承担识别专利的责任。

本文件由中国电工技术学会提出。

本文件由中国电工技术学会标准工作委员会能源智慧化标准工作组归口。

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、琚赟、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、孙芃岳。

本文件为首次发布。

电力无线局域网安全体系结构要求

1 范围

本文件规定了电力无线局域网（WLAN）安全体系结构的总体框架、安全目标、加密解密、安全审计与监控、设备安全等核心要求，覆盖终端接入至网络管理全流程安全要素。

本文件适用于电力无线局域网的规划、设计、建设、运营及维护，涉及设备制造商、网络运营商、系统集成商及相关组织和个人，适用于基于 IEEE802.11 系列标准或融合 WAPI 等安全机制的电力专用 WLAN 场景。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 17964-2021 信息安全技术 分组密码算法的工作模式

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 33565-2024 网络安全技术 无线局域网接入系统安全技术要求

IEEE 802.11i-2004 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范 修正案 6：媒体访问控制安全性增强

3 术语和定义

3.1

MAC 地址欺骗 MACaddress Spoofing：

通过修改设备网络接口卡（NIC） 的 MAC 地址，冒充其他设备身份以绕过访问控制或窃取信息的攻击手段。

3.2

中间人攻击 Man-in-the-Middleattack：

攻击者在两个通信方之间秘密插入并控制连接，冒充双方通信以窃听、拦截或篡改数据的攻击方式。

3.3

伪装 aP 攻击 RogueaPattack：

攻击者架设与合法无线网络同名的恶意接入点（AP），诱骗用户连接以窃取数据或凭证的攻击。

3.4

战争驾驶攻击 Wardrivingattack：

攻击者携带无线探测设备，在特定区域移动扫描并记录开放或存在安全漏洞的无线网络信息的行为。

3.5

无线 Mesh 网络 Wireless Mesh Network：

采用多跳拓扑的无线网络，通过节点间协作扩展覆盖范围，分为骨干型（路由器构成骨干）、客户端型（客户端参与路由）和混合型。

4 符号和缩略语

下列符号、代号和缩略语适用于本文件。

WLAN：无线局域网（Wireless Localarea Network）

TKIP：临时密钥完整性协议（Temporal Key Integrity Protocol）

DoS：拒绝服务攻击（Denial of Service）

DDoS：分布式拒绝服务攻击（Distributeddenial of Service）

MAC：媒体访问控制（Mediaaccesscontrol）

RSN：强健安全网络（Robust Security Network）

PKI：公钥基础设施（Public Key Infrastructure）

IBC：基于身份的密码学（Identity-Basedcryptography）

TPM：可信平台模块（Trusted Platform Module）

RADIUS：远程认证拨号用户服务（Remoteauthenticationdial-In User Service）

EAP：可扩展认证协议（Extensibleauthentication Protocol）

PEAP：受保护的可扩展认证协议（Protectedextensibleauthentication Protocol）

LEAP：轻量可扩展认证协议（Lightweightextensibleauthentication Protocol）

PFS：完全前向保密（Perfectforward Secrecy）

KKS：密钥协调服务器（Key Koordination Server）

WIDS：无线入侵检测系统（Wireless Intrusiondetection System）

OCSP：在线证书状态协议（Onlinecertificate Status Protocol）

ASLR：地址空间布局随机化 （Address Space Layout Randomization）

5 总则

5.1 安全目标

安全目标包括以下方面：

a） 保密性：通过合规加密技术防止非授权用户窃听电力监控、计量采集等敏感数据；

b） 完整性：利用消息完整性校验机制防止数据传输过程中被篡改；

c） 可用性：抵御 DoS/DDoS 等攻击，保障合法用户对网络资源的正常访问；

d） 接入可控性：通过标准化认证机制限制非授权用户及设备接入；

e） 不可否认性：借助数字签名等技术确保通信双方无法否认已发生的通信行为；

f） 移动性安全：终端漫游切换时维持安全关联，减少时延以保障业务连续性；

g） 实时性适配：加密、认证流程时延应≤50ms，适配电力监控指令等实时业务需求；

h） 专用设备兼容：支持 RTU、DTU 等电力专用终端的安全接入与身份认证。

5.2 安全原则

安全原则应遵循：

a） 多层次防御原则：从终端、接入点、管理平台多层面构建协同防护体系；

b） 主动防御与风险管理原则：以风险控制为核心，实现从被动修补到主动防护的转变；

c） 兼容与扩展性原则：兼容不同安全机制，支持新安全协议的插件化扩展；

d） 效率优先原则：优化认证、密钥协商及切换流程，降低计算与通信开销；
e） 终端安全强化原则：实现终端漏洞自动修复、安全引擎加载，弥补终端安全短板；
f） 可信第三方支撑原则：依赖可信认证服务实体实现身份认证和密钥管理，保障认证权威性。

6 安全体系结构框架

6.1 攻击威胁分析

6.1.1 逻辑攻击

电力无线局域网面临的逻辑攻击主要包括以下类型：
a） WEP 协议攻击可利用 WEP 无线加密协议中 RC4 算法漏洞和初始化向量 IV 重用的弱点，收集大量数据包来破解网络密码的攻击；
b） MAC 地址欺骗可通过将设备的网络接口卡 NIC 的 MAC 地址修改为其他设备的地址，冒充该设备或绕过网络访问控制的攻击手段；
c） 拒绝服务攻击（Dos）可通过向目标系统发送海量请求或消耗其关键资源，使其超载而无法为合法用户提供正常服务的攻击，分布式拒绝服务攻击 DDoS 是其更强大的形式；
d） 中间人攻击可通过秘密插入并控制两个通信方之间的连接，冒充双方进行通信，进而窃听、拦截或篡改传输的数据。

6.1.2 物理攻击

针对电力无线局域网的物理攻击主要有以下形式：
a） 伪装 AP 攻击可通过架设一个名称与合法无线网络相同的恶意 AP，诱骗用户连接以窃取其通信数据或凭证；
b） 战争驾驶攻击可通过驾车或步行携带无线探测设备，在城市或区域中移动扫描并记录开放的或有弱点的无线网络的位置和信息；
c） 设备复位攻击可利用物理接触或某些漏洞，强行将网络设备恢复出厂设置，以禁用安全配置并获取控制权。

6.2 安全体系演练

6.2.1 无线 Mesh 网络安全需求

无线 Mesh 网络可通过多跳拓扑扩展 WLAN 覆盖范围，但其动态性和分布式特性引入了新的安全挑战：
a） 网络结构分类需求可分为由路由器构成骨干网的骨干型、客户端直接参与路由的客户端型，以及融合前两者的混合型，支持灵活的组网；
b） 安全认证需求应实现节点间双向认证，支持高效漫游机制，避免冗余认证，并提供集中式与分布式认证方案。

6.2.2 安全体系结构设计方法

基于 5.2 安全原则，电力无线局域网安全体系应采用以下设计方法：
a） 三层架构构建：终端安全层集成防火墙、漏洞修复引擎；接入管理层通过安全网关和中间件统一异构协议；安全管理层基于风险评估系统实现动态策略调整；
b） 关键技术选型：采用协议插件化、主动防御与可信启动的多元安全机制，实现认证兼容性、攻击防护及终端可信链构建；
c） 演进方向规划：聚焦跨域统一身份管理与基于 AI 的自动化防御，适配电力业务扩展需求。

6.3 安全体系设计

6.3.1 安全体系结构框架

应采用“终端防护层-接入控制层-全局管理层”三级分层架构，实现终端防护、接入控制与全局管理的协同，如图 1 所示。各层级与对应平台的关系如下：

a） 终端防护层（对应移动终端安全平台）：集成漏洞修复引擎，支持动态加载安全模块，通过自动推送策略实现终端加固与应用隔离；

b） 接入控制层（对应集成化接入管理平台）：通过安全网关隔离核心网，利用安全中间件统一异构协议接口，基于安全引擎动态调度认证模块，通过驱动适配层封装网卡差异；

c） 全局管理层（对应 WLAN 安全管理平台）：集中管理漏洞库与病毒特征库，通过危害评估系统实现风险动态感知，依托基础数据库支持跨区域协同防御。

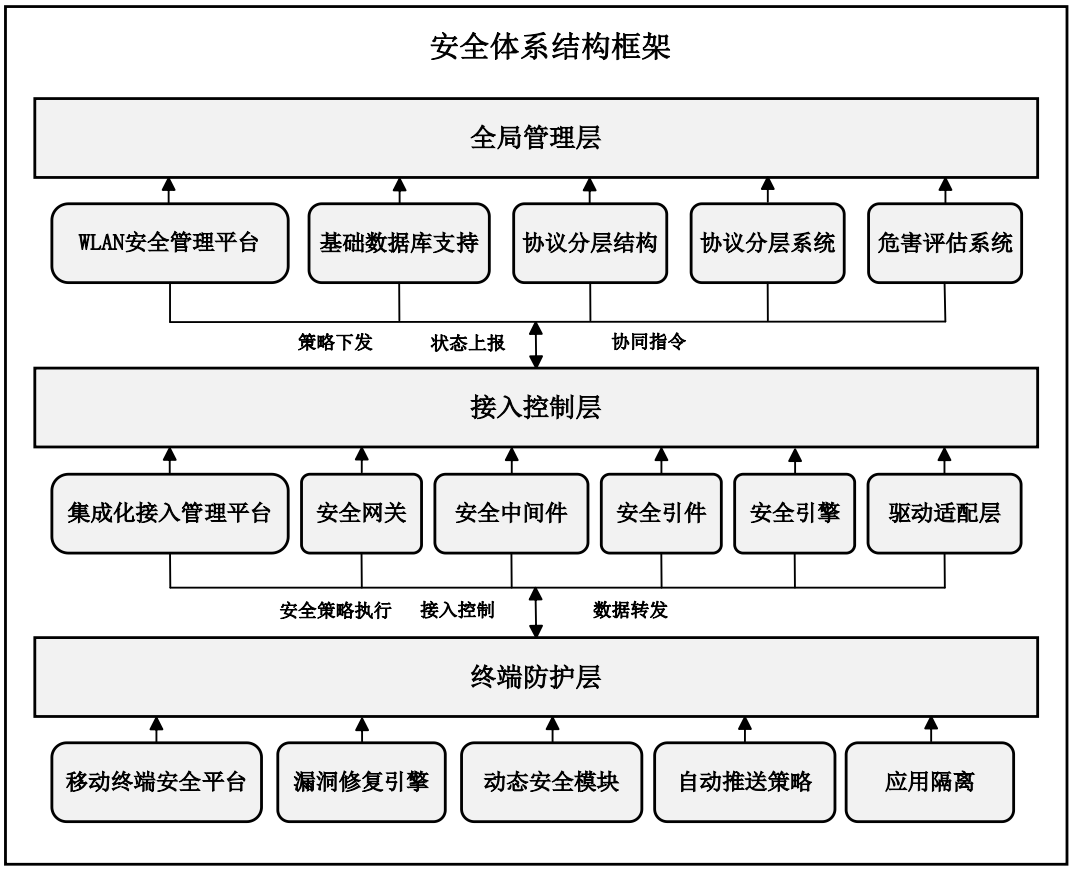

图 6-1 安全体系结构框架

6.3.2 核心组件的安全功能实现与分析

核心组件可通过模块化设计实现异构环境下的安全功能：

a） 安全引擎。可基于 Java KVM 实现安全模块热加载，隔离用户应用与安全功能；

b） 安全中间件。可采用移动代理技术实现异步通信以降低无线链路开销，并在传输控制层实现数据压缩与格式转换，同时适配多网卡驱动；

c） 终端自修复机制。可在开机认证后主动上报状态，通过隔离区自动修复漏洞并更新库，流程涵盖认证、版本比对、隔离修复及重新接入等。

通过模块化设计可构建异构环境下的综合安全体系：安全引擎可利用 Java KVM 实现模块热加载，有效隔离电力用户应用与安全功能，提升部署灵活性与核心安全性；安全中间件可结合移动代理技术降低无线通信开销，并在传输层集成数据压缩、格式转换及多网卡驱动适配，优化通信效率和网络兼容性；终端自修复机制则从开机认证开始，通过状态上报、隔离区自动修复漏洞、更新库及安全重接入等标准化流程，可实现终端的主动式生命周期管理。

6.4 管理框架构建

6.4.1 分层管理体系

a） 策略管理层。应定义全局安全策略，如认证机制选择、密钥更新周期、PFS 保障等级等，可通过策略服务器动态下发配置至执行层，支持基于网络状态的自适应调整；
b） 协议执行层。应承载 IKEv2、WIKE 等协议，可通过协议适配引擎实现异构网络互通，并利用基于 CK 模型的密钥派生模块处理认证、密钥协商及会话建立，保障 PFS 与 KKS 安全性；
c） 监控审计层。可通过部署轻量级探针捕获链路层数据，实时采集协议日志、密钥状态及异常事件，并基于安全事件库进行关联分析以识别攻击特征，实现安全监控与审计溯源。

6.4.2 管理框架核心组件的安全实现与分析

管理框架的核心组件聚焦管理类功能的安全实现，具体如下：

a） 证书管理子系统。可基于 PKI/IBC 颁发实体证书并支持在线 CRL/OCSP 验证，同时通过桥接 CA 或联合身份管理实现多安全域证书互认；
b） 密钥托管机制。可通过 TPM 硬件模块安全存储主密钥并支持密钥分片备份，同时实现生命周期自动管理，包括触发周期性更新及联动认证服务器撤销密钥；
c） 协议调度引擎。可根据终端能力与网络场景动态选择协议，并通过预计算 dH 参数、缓存会话状态优化性能以降低时延。

三个组件相互协同，形成了一个有机整体：证书管理子系统建立了可靠的身份认证和跨域互认框架；密钥托管机制在此基础上，为核心密钥提供了硬件级保护、备份容灾和智能化的全生命周期管理，是安全性的关键保障；协议调度引擎在前两者建立的安全信任基础上，可智能地优化通信效率，确保安全协议在实际应用中的高性能与良好适应性。

7 加密与解密

7.1 加密算法

7.1.1 对称加密算法

a） 宜使用 AES-128 或 aES-256：具备硬件加速支持，适合对大批量时序数据、历史档案以及批处理文件进行加解密；
b） 可兼容 RC2、XTEA、Blowfish、DES/3DES、IDEA 等算法，以满足不同系统兼容性和轻量级设备的性能需求。

7.1.2 非对称加密算法

a） 宜使用 RSA-OAEP：密钥长度不低于 2048 bit，适用于密钥交换与小数据量加密；
b） 可支持椭圆曲线密码学（ECC） ，如 secp256r1、Curve25519 等，提供更高的安全强度与更低的计算开销。

7.2 密钥管理

7.2.1 密钥生成

a） 系统应提供安全可靠的密钥生成机制，可支持不同应用场景的需求，密钥生成过程应基于高质量的随机数生成器，确保密钥的随机性和不可预测性；
b） 系统应记录密钥生成的时间、用途及责任人等信息，以便后续审计；
c） 密钥生成应符合相应的安全规范和标准，可提供不同安全级别的密钥选择。

7.2.2 密钥分发

a） 系统应提供安全高效的密钥分发机制，可支持 Diffie-Hellman 密钥交换协议、Kerberos 密钥分发服务等，确保密钥在网络传输过程中不被泄露或篡改；
b） 密钥分发过程中应采用加密通道传输，并应进行身份认证以避免密钥泄露；
c） 密钥分发过程应记录详细的分发记录，包括接收方身份、分发时间、密钥有效期等信息。

7.2.3 密钥更新

a） 系统应提供定期和事件触发的密钥更新机制，确保密钥有效性，防止密钥泄露或长期使用带来的安全风险；
b） 更新密钥的过程应遵循严格的审批流程，更新操作应完整记录并备份；
c） 密钥更新机制应具备及时性和可靠性，保证业务连续性和安全性。

7.2.4 密钥存储

a） 系统在密钥存储方面应符合以下要求：
1） 密钥存储应进行严格的访问控制和保护；
2） 宜密钥存储需进行严格的访问控制和保护；
3） 宜使用硬件安全模块（HSM）或可信平台模控制和保护；
4） 宜使用硬件安全模块（HSM）或可信平台模块（TPM）进行长期密钥的安全存储；
5） 应确保密钥备份与恢复机制的完备性和安全性；
b） 系统应定期审查密钥存储的安全性，防范密钥非法访问和盗取；
c） 密钥存储管理应提供清晰的密钥生命周期状态管理，可支持密钥废止、销毁和归档等操作。

7.3 加密解密流程

7.3.1 数据加密流程

a） 应用层提交待加密数据和对应的安全上下文标识，包括数据的类型、敏感程度、使用场景以及安全策略等相关信息；
b） 系统安全模块根据提供的安全上下文标识，自动匹配并检索对应的加密密钥和初始化向量（IV），确保密钥的准确性和有效性；
c） 系统调用加密算法引擎进行数据加密处理，生成相应的密文，并生成消息认证码（MAC）用于后续数据完整性校验；数据加密过程中应采用适当的填充方式以确保数据块长度的规范化；
d） 通信组件接收到加密模块输出的密文与消息认证码（MAC），随后对密文进行封装，按照既定的通信协议要求完成数据封包、标记，并通过加密安全通道执行网络传输；
e） 系统对数据加密过程的记录及异常处理应符合以下要求：
1） 系统应对整个数据加密过程的关键步骤进行详细记录；
2） 详细记录的信息应包括密钥调用时间、数据加密算法的使用情况、数据流向以及封包后的传输情况等；
3） 系统应对可能发生的异常情况进行实时监控和告警。

7.3.2 数据解密流程

a） 通信组件接收网络传输的数据，对密文进行拆解和初步处理，检查数据包格式是否符合协议要求，并进行报文的完整性验证，确保数据未被篡改或破坏；
b） 系统安全模块根据报文信息中的安全上下文标识，精确检索并获取解密过程所需的相应密钥

和初始化向量（IV），密钥和 IV 应经过严格的权限校验后方能使用；

c） 系统安全模块调用解密算法引擎对密文进行解密，解密完成后，对消息认证码（MAC） 进行详细校验，确保解密后的数据未被篡改，验证数据的真实性和完整性；

d） 系统对经过验证的数据及验证未通过数据的处理应符合以下要求：

1） 若经验证的数据通过校验，系统安全模块应将明文数据整理后交付给应用层进一步处理；

2） 若数据解密失败或验证未通过，系统应明确拒绝该数据包，并详细记录事件到日志系统，记录内容应包括数据源、错误原因及时间戳等信息，以备后续安全分析和审计。

e） 系统应对解密过程中的各项操作，包括密钥调用、算法执行、完整性校验和结果交付等环节进行详细记录，可支持实时监控及告警机制，确保一旦发生异常事件，能够快速响应并处理。

8 电力无线局域网安全审计与监控

8.1 审计机制

8.1.1 审计记录内容

审计日志应包含足够信息，以支持事件重建、来源识别、责任主体确定及影响评估。必须记录的内容包括：

a） 电力用户身份认证：登录尝试、用户名、终端 MAC/IP 地址、接入点标识、时间戳、认证方法；

b） 管理员操作：WLAN 控制器、认证服务器、防火墙、接入点（AP）等核心组件的配置更改，含更改内容、管理员账户、时间戳、源 IP；

c） 网络访问控制：电力用户 / 专用设备接入的授权 / 拒绝记录，含拒绝原因；

d） 敏感数据操作：电力监控数据、计量采集数据的查询、修改、导出等操作记录，含操作人、操作时间、数据标识。

8.1.2 审计日志管理

为确保日志有效性和安全性，需实施以下策略：

a） 日志应实时传输至专用安全中央日志服务器（Syslog/SIEM）集中存储，与设备分离；

b） 应采用 HMAC 或数字签名技术保障日志完整性，防止篡改；

c） 敏感信息字段应通过 TLS 传输，采用 AES-256 加密存储，保障机密性；

d） 日志访问应遵循最小权限原则，仅授权安全管理员和审计人员访问，且应记录所有访问行为；

e） 日志存储保留期限应满足法规和策略要求，一般不应少于 80 天，关键事件日志应不少于 180 天或按要求延长；

f） 所有网络组件应使用 NTP 服务器实现时间同步，确保日志时间戳一致；

g） 应每季度或基于事件驱动开展日志审查，识别异常行为和安全威胁；

8.2 监控机制

8.2.1 监控方法

监控机制旨在实时观察 WLAN 运行状态、安全态势和性能指标，主动发现异常。

采用以下方法实现全方位监控：

a） 设备监控应通过 SNMP、NETCONF/YANG、API 从控制器、AP、交换机等网络设备采集状态和事件信息；

b） 流量监控宜部署专用探针或利用 AP 捕获无线空口及有线侧流量，进行性能分析和威胁检测；

c） 代理监控可在客户端部署轻量代理收集连接状态和安全信息，部署过程应符合隐私保护相关要求；

d） 主动探测应定期模拟客户端行为，测试网络连通性、性能指标和关键服务可用性；

e） 安全信息与事件管理（SIEM）宜整合各类日志和事件数据，提供统一的安全态势视图。

8.2.2 监控指标

监控以下指标并设定告警阈值：

a） 信道利用率、干扰、AP/控制器资源、监控变电站控制室、配电台区等场景的客户端连接数、WEP、延迟、丢包率、关键服务响应时间；

b） 认证/未认证客户端数量、安全协议分布、WIDS/WIPS 警报、认证失败率、异常流量、漏洞设备数量；

c） AP/控制器及关键链路状态。

8.3 事件处理流程

8.3.1 事件检测

标准化流程确保安全事件及时检测、响应和报告，减少损失。

a） SIEM、WIDS/WIPS、流量检测系统生成精准告警，包含上下文（IP/MAC、事件类型、严重等级）；

b） 通过日志审查、仪表板、电力用户报告发现异常。

8.3.2 事件响应

按响应预案处置：

a） 确认与分类：验证事件，评估性质和严重性；

b） 隔离受影响主机/AP、阻断恶意 IP、吊销凭证；

c） 清除恶意软件、修复漏洞、移除流氓设备；

d） 从备份恢复系统，重建配置；

e） 分析原因、改进策略和规则，责任追究。

8.3.3 事件报告

a） 向管理层、技术团队、合规部门报告事件进展和结果；

b） 按《网络安全法》等法规要求，向监管机构、客户等报告，保护敏感信息；

c） 保存事件全过程记录，用于审计和复盘。

9 设备安全

9.1 物理安全

9.1.1 安装位置要求

物理安全中，安装位置的合理选择是防范物理攻击与信号泄露的基础，应以 “可控性、抗干扰性、防接触性” 为核心原则，具体要求如下：

a） 应选择信号覆盖范围可控的位置，限制无线信号于目标区域，避免泄露至室外或非授权区域；可通过调整 AP 发射功率、天线方向实现，降低战争驾驶攻击风险；
b） 应远离强电磁干扰源（如变电站高压设备、电机设备），避免信号传输质量下降引发安全漏洞；
c） 宜避开物理可达的公共区域（如走廊角落、窗台），防止未授权人员直接接触设备进行物理篡改。

9.1.2 防破坏措施

物理安全中，防破坏措施是抵御设备篡改、移除、非法复位等物理攻击的关键防线，应通过硬件设计、物理固定、环境监控及操作管控等多重手段，保障设备物理完整性与功能安全性，具体要求如下：

a） 应采用防篡改外壳设计，设备被拆卸或开盖时，应自动触发警报并锁定无线接口、清除临时密钥等关键功能；
b） 应对 AP 等设备进行物理固定，宜使用防盗螺丝、锁定支架等方式，防止设备被移除或替换；
c） 宜部署环境监控传感器，监测温度、振动、非法接入尝试等异常情况，应实时上报至安全管理平台；
d） 应加强设备复位保护，禁用物理复位按钮或设置复位密码；复位操作应经安全管理平台远程授权，并记录操作人员、时间、原因等操作日志。

9.2 软件安全

9.2.1 操作系统安全

操作系统是 AP、安全网关等无线局域网设备运行的基础，其安全性直接影响整个网络安全防线，应通过系统加固、服务管控、补丁管理、安全机制启用及账户权限控制等手段，构建底层安全屏障，具体要求如下：

a） 运行在设备上的管理工具、安全引擎等应用程序，应经过数字签名验证，确保来源可信，防止恶意程序植入；
b） 应用程序应遵循安全开发生命周期（SDL），宜通过静态代码分析、动态渗透测试等手段，检测输入验证漏洞、缓冲区溢出等安全缺陷；
c） 应集成嵌入式防火墙、防恶意代码模块等安全引擎，实时监控应用程序行为，应阻断未授权文件读写、网络连接等异常操作；
d） 应限制应用程序的资源访问权限，宜通过沙箱技术隔离不同应用程序的运行环境，防止单个应用被攻破后影响整个设备。

9.2.2 应用程序安全

应用程序是 AP、安全网关等无线局域网设备安全功能与业务逻辑的核心载体，其安全性直接关系设备抗攻击能力与功能可靠性，应通过来源验证、开发规范、行为监控及权限隔离等手段构建应用层安全防线，具体要求如下：

a） 设备上运行的管理工具、安全引擎等应用程序，应经过数字签名验证，确保来源可信，防止恶意程序植入；
b） 应用程序应遵循安全开发生命周期（SDL），宜通过静态代码分析、动态渗透测试等手段，检测输入验证漏洞、缓冲区溢出等安全缺陷；
c） 应集成嵌入式防火墙、防恶意代码模块等安全引擎，实时监控应用程序行为，应阻断未授权文件读写、网络连接等异常操作；

d） 应限制应用程序的资源访问权限，宜通过沙箱技术隔离不同应用程序的运行环境，防止单个应用被攻破后影响整个设备。

9.3 安全配置

9.3.1 配置管理

配置管理是保障无线局域网设备安全配置一致性、可控性的核心手段，应通过集中化平台实现全生命周期管控，具体要求如下：

a） 应建立集中化配置管理平台，统一管理 AP、控制器、网关等设备的安全配置（含 AES-256 加密算法、802.1X/EAP-TLS 认证方式、访问控制列表）；平台应支持配置模板标准化下发与版本控制，可追溯变更历史；

b） 设备首次部署应强制修改默认配置：管理员密码需符合复杂度策略（≥12 位，含大小写字母、数字、特殊字符）；按场景关闭或配置 SSID 广播，清除出厂默认密钥；禁用 WEP 加密、开放认证等弱机制，强制启用 AES-CCMP 加密、802.1X 双向认证；

c） 关键配置（如密钥协商参数、防火墙规则、访问控制策略等）的变更需遵循严格审批流程：由申请方提交变更请求（说明变更原因、影响范围），经安全管理团队审批通过后执行；变更完成后，需记录变更请求单号、审批人、执行结果，并同步至配置基线，确保变更可审计、可回溯；

d） 应采用 “白名单” 限制配置项，仅允许使用经安全验证的配置（如 AES-128/256 加密、802.1X/EAP-TLS 认证、四步握手密钥管理）；禁止 WEP 加密、TKIP 协议、静态密钥长期不变等不合规配置。

9.3.2 配置审计

配置审计是确保无线局域网设备配置符合安全策略、保持一致性及及时修复漏洞的关键环节，需通过定期检查、日志记录、自动化检测及全范围覆盖实现持续合规，具体要求如下：

a） 应每月至少开展一次设备配置合规性审计，核查强加密启用、不安全协议禁用等安全策略落实情况，生成审计报告并跟踪整改闭环；

b） 应启用配置日志功能，完整记录操作人员、操作时间、变更内容、IP 地址等配置变更信息；日志应加密存储，保留期限不低于 180 天，且支持溯源分析；

c） 应利用自动化配置扫描工具检测弱密码、冗余开放端口等配置漏洞，与漏洞管理平台联动，优先整改高风险问题；宜建立漏洞分级处置机制，提升修复效率；

d） 审计范围应覆盖 AP、控制器、网关等所有 WLAN 相关网络设备，确保配置一致性；可结合电力业务场景细化审计指标。