|  |  |
| --- | --- |
| ICS  |   |
| CCS  | 点击此处添加CCS号 |

|  |
| --- |
|  43 |

湖南省地方标准

DB 43/T XXXX—XXXX

电力物联网安全接入及检测技术规范

Technical specifications for secure access and detection of Electric Internet of Things

（本征求意见稿完成时间：2025年02月17日）

XXXX - XX - XX发布

XXXX - XX - XX实施

湖南省市场监督管理局  发布

目次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 电力物联安全接入总体框架 2

6 电力物联安全接入技术要求 3

6.1 感知层终端安全 3

6.1.1 物理安全 3

6.1.2 接入安全 3

6.1.3 通信安全 4

6.1.4 设备安全 4

6.1.5 数据安全 4

6.2 感知层本地通信 4

6.2.1 有线连接方式 4

6.2.2 无线连接方式 4

6.3 网络层接入 5

7 电力物联安全接入检测要求 5

7.1 感知层终端 5

7.1.1 物理安全 5

7.1.2 接入安全 6

7.1.3 通信安全 6

7.1.4 设备安全 7

7.1.5 数据安全 8

7.2 感知层本地通信 9

7.2.1 有线连接方式 9

7.2.2 无线连接方式 9

7.3 网络层接入 10

附录A（资料性） 电力物联终端分类（示例） 11

1. 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》的规定起草。

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。

本文件由中共湖南省委网络安全和信息化委员会办公室提出。

本文件由湖南省网络安全标准化技术委员会归口。

本文件起草单位：

本文件主要起草人：

电力物联网安全接入及检测技术规范

* 1. 范围

本文件规定了电力物联安全接入总体框架、电力物联安全接入技术要求、电力物联安全接入检测要求。

本文件适用于电力企业、电力设备制造企业的电力物联网网络安全防护。

* 1. 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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 33745 物联网 术语

GB/T 36951 信息安全技术 物联网感知终端应用安全技术要求

GB/T 37024 信息安全技术 物联网感知层网关安全技术要求

GB/T 37093 信息安全技术 物联网感知层接入通信网的安全要求

GB/T 40287 电力物联网信息通信总体架构

DL/T 2747 电力物联网 术语

* 1. 术语和定义

GB/T 25069、GB/T 33745-2017和DL/T 2747界定的以及下列术语和定义适用于本文件。

电力物联网 electric internet of things; eIoT

在电力领域应用的物联网，充分应用移动互联、人工智能等信息新技术、先进通信技术，对电力系统状态全面感知、信息高效处理，支撑电力行业数字化的智能服务系统。

[来源：DL/T 2747-2024, 3.1.2]

电力物联终端 electric perception layer terminal

一种能够对电网对象或环境的状态进行感知，并具有简单数据处理、通信、人机交互等全部或部分

功能的专用装置。

边缘物联代理 edge IoT agent

通过在网络边缘节点上部署代理设备、软件，实现对物联设备的管理、控制、数据处理、边缘计算及与云端或其他终端设备的通信。

智能业务终端 intelligent business terminal

集信息采集、设备状态监测及通信组网、就地化分析决策及控制、主站通信及协同计算等功能于一体的智能化终端设备，硬件采用平台化设计，支持边缘计算架构，能够以软件定义的方式实现功能灵活扩展。

现场采集部件 field acquisition component

部署在采集监控对象本体内部或附近，对设备或客户的状态量、电气量和环境量等进行采集量测的终端装置，根据需要可具有数据处理和通信功能。

智能终端 intelligent terminal

在终端设备或二次设备本体中集成传感器，具备状态感知、数据处理和网络通信能力的设备。

[来源:DL/T 2747-2024, 3.3.7]

涉控涉敏终端 control or sensitive terminal

涉控终端指涉及物联器件控制的电力物联终端。涉敏终端指涉及传输线路和设备参数、地理位置信息等敏感信息的电力物联终端。

* 1. 缩略语

下列缩略语适用于本文件。

APP: 应用程序(Application)

APN：接入点（Access Point Name）

JTAG：联合测试行动组（Joint Test Action Group）

LoRa：长距离无线电（Long Range Radio）

LoRaWAN：长距离广域网（Long Range Wide Area Network）

MAC：媒体访问控制地址（Media Access Control Address）

OTAA：空中激活（Over-The-Air Activation）

PIN：个人识别码（Personal Identification Number）

SSID：服务集标识（Service Set Identifier）

SWD：串行线调试（Serial Wire Debug）

TLS/SSL：传输层安全/安全套接层（Transport Layer Security/Secure Sockets Layer）

USB：通用串行总线(Universal Serial Bus)

VPN：虚拟私人网络（Virtual Private Network）

WAPI：无线局域网鉴别与保密基础结构（Wireless LAN Authentication and Privacy Infrastructure）

Wi-Fi：IEEE 802.11系列协议（IEEE  802.11 Series Protocols）

WPA2-PSK：Wi-Fi保护访问2-预共享密钥（Wi-Fi Protected Access 2 - Pre-Shared Key）

ZigBee：紫蜂协议（基于IEEE 802.15.4标准的低功耗局域网协议）

* 1. 电力物联安全接入总体框架

5.1 电力物联网安全接入总体架构见图1。

5.2 电力物联网终端接入按接入层级可分为感知层接入和网络层接入，感知层接入主要指现场采集部件通过本地通信网络接入边缘物联代理。网络层接入主要指智能业务终端、边缘物联代理通过远程通信网络接入平台层。

5.3 接入方式按通信通道类型，接入方式可分为有线方式和无线方式。

5.4 典型电力物联终端是否为智能终端、涉控涉敏终端，见附录A。



1. 电力物联网终端接入整体架构
	1. 电力物联安全接入技术要求
		1. 感知层终端安全
			1. 物理安全

电力物联感知层终端物理安全要求如下：

1. 应符合电力物联感知层终端应符合GB/T 22239-2019、GB/T 36951-2018物理安全要求；
2. 应将设备或主要部件进行固定，并设置明显的不易除去的标记；
3. 户外部署的终端宜采取防雷击措施，将感知层设备通过接地系统安全接地，必要时采取措施防止感应雷击，例如设置防雷保安器等；
4. 涉控终端、涉敏终端宜提供短期的备用电力供应，满足设备断电情况下的正常运行不小于2小时要求。
	* + 1. 接入安全

电力物联感知层终端接入安全要求如下：

1. 应符合GB/T 36951-2018、GB/T 37093-2018接入安全要求；
2. 感知层终端直接接入电力内部网络时，应具备加密、认证和访问控制等安全防护能力；
3. 边缘物联代理宜具备对接入的智能业务终端、现场采集部件等设备的接入管理能力及安全防范能力，应支持通过设定终端接入方式或网络范围对接入设备进行限制；
4. 边缘物联代理宜通过基于标识密码体系或硬件指纹等轻量级认证技术，对于接入的智能业务终端、现场采集部件设立指纹白名单进行认证，在满足合法终端即插即用的同时，防止攻击者持有非法攻击工具仿冒合法终端接入；
5. 边缘物联代理及智能业务终端宜具备远程通信的访问控制能力，当访问地址、端口、协议等超出限定范围时，能终止当前会话。
	* + 1. 通信安全

电力物联感知层终端通信安全要求如下：

1. 应符合GB/T 36951-2018通信安全要求；
2. 应具有可用于物联网中通信识别的唯一标识，并且该标识应具备防篡改保护；
3. 涉控终端宜采用数字签名等密码算法或组合算法保障控制指令的来源可鉴别；
4. 涉控终端、涉敏终端宜采用硬件密码模块的方式进行身份认证和加密保护，硬件密码模块宜采用通过国家有关检测机构检测认证的安全芯片。
	* + 1. 设备安全

电力物联感知层终端设备安全要求如下：

1. 应符合GB/T 22239-2019、GB/T 36951-2018设备安全要求；
2. 应支持本地及远程对设备进行补丁更新、固件更新等，具备升级失败回退功能；
3. 涉控终端、涉敏终端应关闭设备调试接口，包括USB、JTAG、SWD 接口等，防范软硬件逆向工程。
4. 涉控终端、涉敏终端宜采取审计记录保护措施，防范审计记录被非法读取、篡改或删除等；
5. 涉控终端、涉敏终端宜采用具备国产商用密码算法的安全存储芯片作为存储载体，为设备固件数据提供安全保护；
6. 智能终端宜确保APP应用发布的渠道可信，发布前宜进行统一加固、统一检测。
	* + 1. 数据安全

电力物联感知层终端数据安全要求如下：

1. 应符合GB/T 36951-2018数据安全要求；
2. 应采用密码技术保证电力重要数据在数据采集过程中的保密性；
3. 应对终端本地存储的用户口令等关键数据进行加密保护；
4. 涉控涉敏智能终端应支持控制指令执行、用户信息数据获取等本地涉控涉敏操作记录日志本地保存，记录至少保留6个月；
5. 涉控涉敏智能终端应对涉控涉敏数据的完整性进行校验，防止数据篡改；
6. 涉控涉敏智能终端宜采用具备国产商用密码算法的安全芯片，对终端位置、控制指令、用户信息等涉控涉敏数据进行应用层加密传输、存储。
	* 1. 感知层本地通信
			1. 有线连接方式

电力物联感知层终端有线连接方式包括光纤、双绞线、串口线等,应符合以下要求：

1. 采用专用线路、通道等进行连接；
2. 使用串口进行通信时，通信链路具有防物理破坏的措施，并有效接地。
	* + 1. 无线连接方式

电力物联感知层终端无线连接方式包括蓝牙、Wi-Fi、ZigBee、LoRa、WAPI等，要求如下：

1. 无线网络应具备抗电磁干扰、协议攻击、频段劫持能力；
2. 无线网络应具备身份认证和数据加密功能，防止非授权入网及信息泄露；
3. 本地的各类网络设备、通信设备及无线接入控制器应配置适宜的安全策略，包括但不限于设置登录用户名和密码、绑定MAC 地址、非法 信号屏蔽等；
4. Wi-Fi 通信应关闭 SSID 广播功能，启用安全性不低于WPA2-PSK 的安全模式，并设置连接强口令；
5. 使用蓝牙通信方式连接的终端如智能充电桩、信息采集器等，应设置 PIN 码用于认证；
6. 应避免使用 LoRa 方式传输涉控涉敏数据，LoRa 通信应采用安全版本的 LoRaWAN 协议，并使用 OTAA 模式实现终端节点激活入网；
7. 使用 ZigBee 通信方式的网络应设置本地信任中心，应加密数据帧；
8. 宜使用WAPI方式传输涉控涉敏数据，应采用三元对等双向安全认证的方式。
	* 1. 网络层接入

电力物联接入通道网络层接入安全要求如下：

1. 应符合GB/T 37024-2018、GB/T 40287-2021安全隔离要求；
2. 涉及电网运行与并网控制相关的物联终端，应接入电力物联网络，不应接入互联网等公共网络；
3. 应遵循专网专用原则，避免单一感知层终端同时接入生产控制大区、管理信息大区，或与互联网通信，造成大区间隔离体系被破坏或数据外发行为；
4. 感知层终端接入电力内部网络时，应使用物联或虚拟网络接入通道；或应设置安全接入区，通过安全接入区实现和电力内部网络的交互；
5. 感知层终端在采用无线方式接入时，或涉控终端、涉敏终端接入时，应部署具备认证、加密和访问控制等功能的安全设备实现安全接入；
6. 宜采用WAPI等具备加密、认证功能的无线通信协议，满足变电站、营业厅、发电场站等管理信息大区本地无线网络的终端安全接入。
	1. 电力物联安全接入检测要求
		1. 感知层终端
			1. 物理安全
				1. 选型

本项要求包括：

1. 应验证设备是否持有有效的质量认证证书；
2. 应检查电力物联感知层终端是否已完成第三方检测机构的信息安全检测，并获取相应报告；
3. 宜测试设备外壳防护情况。
	* + - 1. 选址

本项要求包括：

1. 应实地考察部署环境，验证其防盗窃、防水防潮、防极端温度等能力；
2. 宜进行信号质量测试，确保部署位置无显著干扰、屏蔽或阻挡。
	* + - 1. 供电

本项要求包括：

1. 应通过模拟供电故障测试，验证电力物联感知层终端的供电稳定性及备用电力供应的可靠性；
2. 应测试备用电力供应,在模拟断电条件下，测试涉控终端、涉敏终端的备用电源系统，确保其能在断电后自动启动并维持设备运行至少2小时，以满足紧急情况下的持续运行需求。
	* + - 1. 防盗窃和防破坏

本项要求包括：

1. 应评估部署位置的安全性，避免在不受控的非安全场所部署；
2. 应验证防盗窃和防破坏措施的有效性，如物理锁具、报警系统等；
3. 应检查设备固定与标记,验证设备或其主要部件是否已稳固固定，并检查是否设有难以去除的明显标记，以确保设备的安全性。
	* + - 1. 防雷和防静电

本项要求包括：

1. 应检查重要电力物联感知层终端是否安装有避雷针、防雷器等防雷设施，并测试其有效性；
2. 应验证防静电措施，如接地处理、防静电材料等，是否到位并有效。
	* + 1. 接入安全
				1. 网络接入认证

本项要求包括：

1. 应通过模拟网络接入环境，验证终端是否具有唯一且不可伪造的网络身份标识；
2. 应测试终端是否支持并正确实现至少一种指定的身份鉴别机制，包括基于网络身份标识、MAC地址、通信协议、通信端口、对称密码机制和非对称密码机制的鉴别；
3. 应模拟鉴别失败场景，验证系统能否正确处理并响应，包括但不限于锁定账户、记录日志等；
4. 应检查密钥的存储和交换过程，确保采用安全的方式（如加密存储、安全传输协议等）进行；
5. 应执行双向认证测试，验证电力物联感知层终端与其接入网络间至少支持一种指定的身份鉴别机制，并确认认证过程的安全性；
6. 应通过模拟攻击和渗透测试，验证电力物联感知层终端在接入电力内部网络时是否有效实施了加密、认证机制，并检查访问控制策略是否被正确执行，确保数据传输的安全性；
7. 边缘物联代理应进行接入管理能力检测，应模拟不同接入方式和网络范围的终端，测试边缘物联代理是否能够有效管理这些终端的接入，并验证其能否正确限制非授权接入。
	* + - 1. 网络访问控制

本项要求包括：

1. 应使用端口扫描工具检查并确认所有非业务需求相关的通信端口已被禁用；
2. 应配置网络访问控制策略，并测试其有效性，确保仅允许授权的网络访问请求通过，对非法请求进行拦截和记录；
3. 应检查网络访问控制策略是否定期更新和审计；
4. 应构造超出限定范围的访问请求（如错误地址、端口、协议等），测试边缘物联代理及智能业务终端是否能够即时发现并终止这些非法会话，确保北向访问的安全性；
5. 应测试边缘物联代理是否采用标识密码体系或硬件指纹等技术建立指纹白名单，并通过尝试接入伪造终端验证其能否有效识别和阻止非法终端的接入。
	* + 1. 通信安全
				1. 无线电安全

电力物联感知层终端的无线电安全检测应通过无线电频谱分析设备，检测电力物联感知层终端使用的无线电频段是否符合国家规定，并验证其辐射强度是否在安全范围内。

* + - * 1. 传输完整性

本项要求包括：

1. 应测试电力物联感知层终端是否实现了数据传输的完整性校验机制，如校验和、哈希校验等，确保数据传输过程中未被篡改；
2. 应模拟通信延时和中断场景，验证电力物联感知层终端是否具有相应的处理机制，能够恢复通信并确保数据的完整传输；
3. 应验证电力物联感知层终端是否具有唯一的、防篡改的通信标识，通过尝试修改该标识并观察系统反应，确认其防篡改机制的有效性；
4. 应模拟发送伪造的控制指令，测试涉控终端是否能通过数字签名等密码算法正确鉴别指令来源，确保控制指令的真实性和完整性。
	* + - 1. 传输保密性

本项要求包括：

1. 应捕获并分析电力物联感知层终端传输的敏感信息（如鉴别信息、隐私数据和重要业务数据），验证其是否进行了加密保护，并检查加密算法是否符合国家密码相关规定；
2. 应验证加密密钥的生成、存储、交换和使用过程的安全性，确保密钥不被非法获取或滥用；
3. 应检查涉控终端、涉敏终端是否采用硬件密码模块进行身份认证和加密保护，并确认该硬件密码模块是否已通过国家有关检测机构的检测认证；通过模拟攻击测试，验证硬件密码模块在身份认证和加密保护方面的有效性。
	* + 1. 设备安全
				1. 标识和鉴别

本项要求包括：

1. 应测试使用用户名和口令进行身份鉴别的有效性，验证口令复杂度（包含字母、数字及特殊字符，长度不小于8位）是否符合要求；
2. 对于具有执行能力的电力物联感知层终端，应通过模拟发送控制指令，验证其是否能有效鉴别下达执行指令者的身份。
	* + - 1. 访问控制

本项要求包括：

1. 应通过操作系统权限管理工具，检查用户权限分配是否合理，确保用户仅被授予完成任务所需的最小权限；
2. 应测试电力物联感知层终端对数据的本地和远程访问控制机制，验证其能否有效限制非法访问；
3. 应检查电力物联感知层终端的远程配置功能是否具备安全措施，如访问控制列表、加密传输等；
4. 应验证涉控终端、涉敏终端是否采用具备硬件加密功能的安全存储芯片，并检查该芯片是否能为设备固件数据提供足够的安全保护；
5. 对于具有固件升级能力的电力物联感知层终端，模拟本地及远程升级过程，验证是否支持补丁更新、固件更新，并检查在升级失败时是否具备回退至上一版本的功能。
	* + - 1. 日志审计

本项要求包括：

1. 应检查涉控涉敏终端日志生成功能，验证其是否能记录日期、时间、操作用户、操作类型等信息；
2. 应测试涉控涉敏终端审计功能的开启和关闭权限是否仅限于安全审计员；
3. 验证涉控涉敏终端审计记录查阅功能，确保安全审计员能方便地查阅审计记录，审计记录查阅功能应能遵循权限最小原则，仅安全审计员能查看；
4. 应检查涉控涉敏终端已存储的审计记录是否受到保护，防止未授权的修改、删除或覆盖；
5. 应尝试非法访问、篡改或删除审计记录，验证涉控终端、涉敏终端的审计记录保护机制是否有效，确保审计记录的安全性和完整性。
	* + - 1. 失效保护

本项要求包括：

1. 应通过模拟设备故障，验证电力物联感知层终端的自检和告警功能是否有效；
2. 应测试操作系统崩溃时的重启机制，确保其能自动或手动恢复运行；
3. 应检查具有执行能力的电力物联感知层终端是否具有本地手动控制功能，并验证其优先级高于自动控制功能。
	* + - 1. 软件安全

本项要求包括：

1. 应检查电力物联感知层终端上安装的软件是否均为授权软件；
2. 应验证软件补丁更新和升级策略的执行情况，确保数据来源合法且完整；
3. 应检查所安装的软件是否满足业务安全功能需求，并正确配置及使用；
4. 应在软件补丁更新和升级前进行安全测试验证，确保更新不会引入新的安全风险；
5. 应检查智能终端APP应用的发布渠道是否可信，并验证发布前是否进行了统一的加固和检测流程，确保APP应用的安全性。
	* + - 1. 恶意代码防范

应通过模拟恶意代码攻击，验证终端恶意代码防范能力的有效性。

* + - * 1. 物理接口安全

本项要求包括：

1. 应检查电力物联感知层终端的外部设备接口使用情况，确保闲置接口已被禁用；
2. 应验证外接存储设备自启动功能是否已被禁用，防止未授权的数据访问或恶意软件传播；
3. 应检查涉控终端、涉敏终端的USB、JTAG、SWD等调试接口是否被物理关闭或软件禁用，防止通过这些接口进行软硬件逆向工程。
	* + 1. 数据安全
				1. 数据可用性

本项要求包括：

1. 应通过模拟数据传输过程，验证电力物联感知层终端是否对数据新鲜性进行了有效标识，确保数据在传输过程中的时效性；
2. 应检查电力物联感知层终端的冗余部署配置，验证其是否能在主采集系统失效时，自动或手动切换到备用系统，确保重要数据的持续采集；
3. 应审查涉控涉敏终端是否支持控制指令执行、用户信息数据获取等操作的记录日志功能，并验证日志记录是否至少保留6个月，确保可追溯性。
	* + - 1. 数据完整性

本项要求包括：

1. 应验证电力物联感知层终端生成的数据完整性证据（如校验码、消息摘要、数字签名等）的正确性和有效性，确保数据在传输和存储过程中未被篡改；
2. 应模拟数据完整性错误场景，检查电力物联感知层终端是否能及时发现并采取相应的恢复措施，如重新采集、数据恢复等；
3. 应测试涉控涉敏智能终端是否通过数字签名或单向散列（如SHA-256）等机制对涉控涉敏数据进行完整性校验，防止数据被篡改。
	* + - 1. 数据保密性

本项要求包括：

1. 应通过审查电力物联感知层终端的加密配置和加密算法，验证其是否采用了符合国家密码相关规定的密码算法对敏感信息进行存储和传输加密保护；
2. 应尝试非法访问存储的敏感信息，验证加密措施的有效性，确保敏感信息在存储和传输过程中的保密性；
3. 应检查涉控涉敏智能终端是否集成了采用国产商用密码算法的安全芯片，并验证该芯片是否支持对终端位置、控制指令、用户信息等数据进行应用层加密传输和存储。同时，应测试是否支持按照数据分类分级设置不同的存储策略，确保数据的安全性和合规性；
4. 应检查本地存储的用户口令等关键数据是否经过加密处理，并尝试通过非授权方式访问这些数据，验证加密保护的有效性；
5. 应验证电力物联感知层终端是否采用密码技术（如国密算法）对企业重要数据进行存储过程中的保密性保护，确保数据不被未授权访问。
	* 1. 感知层本地通信
			1. 有线连接方式

本项要求包括：

1. 专用线路与通道检测：应检查有线连接方式（光纤、双绞线、串口线等）是否采用专用线路或通道进行连接，确保通信路径的独立性和安全性；
2. 串口通信链路防护检测：在使用串口进行通信时，应检查通信链路是否具备防物理破坏的措施，如物理防护罩、加固安装等，并验证通信链路是否有效接地，以防止电气干扰和物理损害。
	* + 1. 无线连接方式

本项要求包括：

1. 抗电磁干扰与协议攻击检测：应模拟电磁干扰环境和协议攻击场景，验证无线网络是否具备有效的防护措施，确保通信稳定且数据不被非法截获或篡改；
2. 身份认证与数据加密检测：通过尝试非法接入和捕获传输数据，验证无线网络是否实施了身份认证和数据加密功能，确保只有授权用户能访问网络且传输信息不被泄露；
3. 网络设备安全策略配置检测：检查本地网络设备、通信设备及无线接入控制器的安全策略配置，包括但不限于登录用户名和密码的复杂度、MAC地址绑定情况等，确保所有安全策略得到有效实施；
4. Wi-Fi通信安全配置检测：关闭SSID广播功能后，尝试通过非广播方式连接Wi-Fi，并验证是否仅允许WPA2-PSK或更高安全模式的连接，且连接时需使用强口令；
5. 蓝牙通信PIN码认证检测：检查使用蓝牙通信的终端（如智能充电桩、信息采集器等）是否设置了PIN码，并尝试通过无PIN码或错误PIN码进行连接，验证PIN码认证的有效性；
6. LoRa通信协议与模式检测：确认LoRa通信使用的协议版本不低于1.0.3，并检查是否采用OTAA模式实现终端节点激活入网，以防范安全风险；
7. ZigBee通信安全配置检测：检查ZigBee网络是否设置了本地信任中心，并验证数据帧是否加密传输，确保通信过程的安全性；
8. WAPI通信安全检测：在涉控涉敏数据传输场景中，应验证是否采用WAPI通信方式，并检查是否实现了三元对等双向安全认证，确保数据传输的机密性、完整性和认证性。
	* 1. 网络层接入

本项要求包括：

1. 应验证网络层接入是否严格遵循专网专用原则，通过检查网络配置和流量日志，确保没有电力物联感知层终端违规跨接生产控制大区和管理信息大区，从而维护大区间的有效隔离体系。此外，还需利用网络扫描工具检查是否存在未经授权的网络连接或端口开放，进一步确认网络隔离的完整性。
2. 对于电力物联感知层终端接入电力内部网络的情况，检测需确认是否使用了专线作为接入通道。若采用其他方式，则应检查是否设置了安全接入区，并评估其安全控制措施的有效性，如防火墙规则、入侵检测系统（IDS）等，以确保与电力内部网络的交互安全。同时，利用网络流量分析工具监控并分析网络流量，检查是否存在异常或未经授权的数据传输。
3. 在电力物联感知层终端采用无线方式接入，或涉控终端、涉敏终端接入时，检测应验证是否部署了具备认证、加密和访问控制功能的安全设备。这包括但不限于无线接入点（AP）的安全配置、认证服务器的运行状态以及加密协议的实施情况。或者检测应确认是否采用了如WAPI等具备加密、认证功能的无线通信协议，并检查其配置是否正确，以确保变电站、营业厅、发电场站等管理信息大区本地无线网络的终端安全接入。此外，还需利用无线安全测试工具对无线网络进行渗透测试，以发现潜在的安全漏洞和威胁。
4.
5. （资料性）
电力物联终端分类（示例）

根据电力全过程业务场景物联网终端智能程度、业务特点等，对各专业主要终端进行分类示例，如表A.1所示。

* 1. 电力物联终端分类表

| 业务场景 | 设备名称 | 智能终端 | 涉控涉敏终端 |
| --- | --- | --- | --- |
| 发电侧 | 北斗卫星终端、智能巡检机器人、无人机、智能摄像头、供水通风控制、移动作业终端、智能可穿戴等 | √ | × |
| 保护装置、测控装置、智能合并单元、远动装置、光伏控制器 | √ | √ |
| 发电设备监测、温湿度/光照度/气象传感器、消防/安防传感、可编程逻辑控制器等、普通摄像头等 | × | × |
| 输电侧 | 边缘物联代理、无人机、巡检机器人、智能摄像头、移动作业终端等 | √ | × |
| 气象/覆冰/温度/杆塔监测、普通摄像头等 | × | × |
| 变电侧 | 边缘物联代理、巡检机器人、无人机、智能摄像头、供水通风控制、移动作业终端、智能可穿戴等 | √ | × |
| 保护装置、测控装置、智能合并单元、远动装置 | √ | √ |
| 变电设备监测、温湿度/光照度/气象传感器、消防/安防传感、普通摄像头等 | × | × |
| 配电侧 | 三遥终端、配电保护装置、智能融合终端、储能控制器、智能逆变器、智能断路器、分布式电源监测终端、智能配变终端等 | √ | √ |
| 二遥终端、巡检机器人、智能摄像头等 | √ | × |
| 低压配电监测设备、熔断监测、故障指示器、温湿/光照/气象传感器、消防/安防感知、普通摄像头等 | × | × |
| 用电侧 | 融合终端、用采集中器、负控终端、智慧用能终端、充电桩、智能逆变器、智能断路器、智能换相开关、光伏/空调/供热/供冷/给水系统及设备等 | √ | √ |
| 电能表（费控）、断路器、空气开关，空调变频器、照明开关等可控负荷终端 | × | √ |
| 营销移动终端、营业厅自助终端、智能摄像头等 | √ | × |
| 普通摄像头、消防/安防感知等 | × | × |
| 其他 | 边缘物联代理、智能可穿戴、无人机、仓储机器人、智能摄像头、智能安全帽、移动布控球等 | √ | × |
| 环境感知、状态感知、消防/安防感知、普通摄像头等 | × | × |