ICS
CCS 点击此处添加 CCS 号

T/ZJSEE

浙 江 省 电 力 学 会 标 准

T/ZJSEE XXXX—XXXX

5G 电力终端接入安全技术要求及测试规范

Safety Technical requirements and test specifications for access of 5G power terminals

（征求意见稿）

2023－XX－XX 发布　　2023－XX－XX 实施

浙 江 省 电 力 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》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这些专利的责任。

本文件由浙江省电力学会提出。

本文件由浙江省电力学会归口。

本文件起草单位：

本文件主要起草人：

5G 电力终端接入安全技术要求及测试规范

1 范围

本文件规定了浙江省电力行业5G电力终端的5G电力终端划分、5G电力非涉控终端接入技术要求、5G电力涉控终端接入技术要求和测试要求。

本文件适用于5G电力终端通过5G电力虚拟专网接入的安全技术要求和测试规范。

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。

本文件无规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

5G 电力终端 5G power terminal

具备5G通信能力，通过5G虚拟专网接入电力系统用于电力生产、管理、服务的物联网终端。

3.2

5G 电力虚拟专网 5G power virtual private network

在电信运营商 5G 网络中，基于网络切片、能力开放等技术，于接入、承载、核心网等环节构建出面向电力行业的虚拟专用网络。

4 符号、代号和缩略语

下列术缩略语适用于本文件。

AAA：认证授权计费系统（Authentication, Authorization, Accounting）

ACL：访问控制列表（Access Control List ）

AMF：认证管理功能（AuthenticationManagementFunction）

AMS：终端通信接入网管理系统（Access Management System）

APN：接入点名称（Access Point Name）

DDOS：分布式拒绝服务（Distributed Denial Of Service）

IDS：入侵检测系统（Intrusion Detection Systems）

NSA：非独立组网（Non-Standalone）

SA：独立组网（Standalone）

SIM：客户识别模块（Subscriber Identity Module）

SSL：安全套接字协议（Secure Sockets Layer）

UIM：用户识别模块（User Identity Module）

VLAN：虚拟局域网（Virtual Local Area Network）

VPDN：虚拟专用拨号网（Virtual Private Dial—up Networks）

VPN：虚拟专用网络（Virtual Private Network）

5G：第5代移动通信技术（5th Generation Mobile Communication Technology）

5 5G 电力终端划分

5.1 5G 电力终端可分为 5G 电力涉控终端与 5G 电力非涉控终端。

5.2 5G 电力非涉控终端指通过 5G 网络接入的除涉控外的电力物联终端。

5.3 5G 电力涉控终端指通过 5G 网络接入的涉及物联器件控制的电力物联终端。

注：视频摄像头的控制、物联终端运行参数修改等操作不属于涉控范围。

6 5G 电力非涉控终端接入技术要求

6.1 虚拟专网安全

6.1.1 通道合规

5G电力虚拟专网通道合规应满足下列技术要求：

a) 采取必要措施进行伪基站鉴别，防止通过伪基站接入；

b) 支持空口信令 DDOS 攻击防御；

c) 支持检测 GPS 信号欺骗/干扰攻击。

6.1.2 切片隔离

5G电力虚拟专网切片隔离应设置不同等级的切片应用，实现访问隔离。

6.1.3 边界隔离

5G电力虚拟专网边界隔离应满足下列技术要求：

a) 在电力边界处部署访问控制机制，配置并启用访问控制规则，保证规则有效性；

b) 在电力边界处部署网络入侵检测/防御设备，配置并启用入侵检测/防御策略；

c) 在电力边界处，部署恶意代码检测和清除设备，并维护恶意代码的升级与更新；

d) 通过必要措施识别 DoS/DDoS 攻击异常流量并丢弃，放行正常网络访问流量。

6.2 终端安全接入

6.2.1 访问控制

5G电力非涉控终端访问控制应限制访问的IP地址和采取机卡绑定。

6.2.2 认证与鉴权

5G电力非涉控终端认证与鉴权满足下列技术要求：

a) 宜通过部署电力专用鉴权服务器对通信终端进行二次鉴权；

b) 地址分配应采用固定 IP。

6.2.3 固件要求

5G电力非涉控终端固件要求满足下列技术要求：

a) 宜通过验证可信根的方式对固件的硬件控制和硬件加解密程序等进行可信验证，可采用人工上传非官方升级固件或文件的方式进行检测验证；

b) 在使用过程中应避免存在注入攻击、缓冲区溢出、远程系统调用、信息泄露等风险漏洞。

6.2.4 身份验证

5G电力非涉控终端身份验证应满足下列技术要求：

a) 对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b) 具有登录失败处理功能，配置结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c) 采取必要措施防止鉴别信息在网络传输过程中被泄露。

6.2.5 密钥协商认证

5G电力非涉控终端密钥协商认证满足下列技术要求：

a） 应至少启用一种加密算法用于空口数据加密和完整性保护；
b） 宜采取硬件密码模块或软件密码模块等方式实现通道加密；
c） 终端数据安全传输、敏感内容加密、数字签名应采用国家认可的加密算法；

6.2.6 终端本体鉴别

5G电力非涉控终端终端本体在网络内应有唯一身份标识，并采取必要措施进行终端本体鉴别。

6.3 5G 数据传输安全

6.3.1 完整性

5G电力非涉控终端完整性应采用国家认可的密码技术保证数据传输过程中的完整性，采取数据校验和重传，实现数据恢复。

6.3.2 保密性

5G电力非涉控终端保密性满足下列技术要求：
a） 在传输时可采用具有一定强度的前向安全性加密算法或其他措施对信息进行加密；
b） 密码技术应使用由可信方提供的密钥和数字证书；
c） 采用国家密码主管部门认可的密码算法保证传输过程中数据的保密性。

6.3.3 可用性

5G电力非涉控终端可采用必要措施实现抗重放攻击。

7 5G 电力涉控终端接入技术要求

7.1 一般要求

5G电力涉控终端接入技术应在5G电力非涉控终端接入技术要求基础上扩展。

7.2 5G 电力虚拟专网安全

7.2.1 通道合规

5G电力虚拟专网通道合规应满足下列技术要求：
a） 采取必要措施进行伪基站鉴别，防止通过伪基站接入；
b） 支持空口信令 DDOS 攻击防御；
c） 支持检测 GPS 信号欺骗/干扰攻击

7.2.2 切片隔离

5G电力虚拟专网切片隔离应满足下列技术要求：
a） 设置不同等级的切片应用，实现访问隔离；
b） 设置硬切片通道资源预留，包括 RB 资源、FLexE。

7.2.3 电力专用 UPF 加固

5G电力虚拟专网电力专用UPF加固应满足下列技术要求：
a） 电力专用 UPF 加强基线配置、安全加固；
b） 电力专用 UPF 限制开放端口，仅允许授权账号登录；
c） 电力专用 UPF 避免存在注入攻击、缓冲区溢出、远程系统调用、信息泄露等风险漏洞。

7.2.4 边界隔离

5G电力虚拟专网边界隔离应满足下列技术要求：
a） 在电力边界处部署访问控制机制，配置并启用访问控制规则，保证规则有效性；
b） 在电力边界处部署网络入侵检测/防御设备，配置并启用入侵检测/防御策略；
c） 在电力边界处部署恶意代码检测和清除设备，并维护恶意代码的升级与更新；

d） 通过必要措施识别 DoS/DDoS 攻击异常流量并丢弃，放行正常网络访问流量；
e） 电力边界应部署专用流量分析装置，并具备实时采集、协议识别、文件还原、特征检测等安全功能；
f） 电力边界宜部署深度异常行为感知、溯源分析、安全可视化等安全增强技术措施。

7.3 5G 终端安全接入

7.3.1 访问控制

5G电力涉控终端接入访问控制应满足下列技术要求：
a） 限制访问的 IP 地址；
b） 采取机卡绑定；
c） 5G 电力终端支持基站绑定。

7.3.2 认证与鉴权

5G电力涉控终端认证与鉴权满足下列技术要求：
a） 宜通过部署电力专用鉴权服务器对通信终端进行二次鉴权；
b） 地址分配应采用固定 IP。

7.3.3 固件安全

5G电力涉控终端固件安全满足下列技术要求：
a） 宜通过验证可信根的方式对固件的硬件控制和硬件加解密程序等进行可信验证；
b） 在使用过程中应避免存在注入攻击、缓冲区溢出、远程系统调用、信息泄露等风险漏洞。

7.3.4 身份验证

5G电力涉控终端身份验证应满足下列技术要求：
a） 对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
b） 具有登录失败处理功能，应配置结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
c） 采取必要措施防止鉴别信息在网络传输过程中被泄露；
d） 采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

7.3.5 密钥协商认证

5G电力涉控终端密钥协商认证满足下列技术要求：
a） 至少启用一种加密算法，用于空口数据加密和完整性保护；
b） 宜采取硬件密码模块或软件密码模块等方式实现通道加密；
c） 终端数据安全传输、敏感内容加密、数字签名应采用国家认可的加密算法；
d） 终端纵向传输应采用经认证的加密传输协议，使用专用密钥协商，通过密钥协商后方可与应用系统进行连接。

7.3.6 终端本体鉴别

5G电力涉控终端终端本体鉴别应满足下列技术要求：
a） 在网络内有唯一身份标识，采取必要措施进行终端本体鉴别；
b） 采用白名单技术限制终端本体接入。

7.4 5G 数据传输安全

7.4.1 完整性

5G电力涉控终端应采用国家认可的密码技术保证数据传输过程中的完整性，采取数据校验和重传，实现数据恢复。

7.4.2 保密性

5G电力涉控终端保密性满足下列技术要求：

a) 在传输时可采用具有一定强度的前向安全性加密算法或其他措施对信息进行加密；
b) 密码技术应使用由可信方提供的密钥和数字证书；
c) 应采用国家密码主管部门认可的密码算法保证传输过程中数据的保密性；
d) 建立数据传输通道前，应对发送方和接收方进行身份鉴别，会话初始化也应采用加密技术加固。

7.4.3 可用性

5G电力涉控终端可采用必要措施实现抗重放攻击。

8 测试要求

8.1 5G 电力非涉控终端接入测试规范

8.1.1 测试工具

5G电力非涉控终端测试工具见表1。

表1 5G 电力非涉控终端测试工具

序号	仪器设备名称	接入位置编号
1	网络性能测试仪	②③④⑩⑪⑫
2	5G 路测工具	⑤
3	5G 信令安全测试仪	⑧⑨
4	5G 核心网测试仪	⑧⑨
5	协议模糊测试工具	①②⑧⑨
6	漏洞扫描工具	①②⑥⑧⑩⑫
7	抓包工具	①②⑥⑧⑩⑫
8	逆向分析工具	①②⑥⑧⑩⑫
9	漏洞验证工具	①②⑥⑧⑩⑫
10	端口扫描工具	① ②⑥⑧⑩⑫

8.1.2 测试环境

5G电力非涉控终端测试环境见图1。

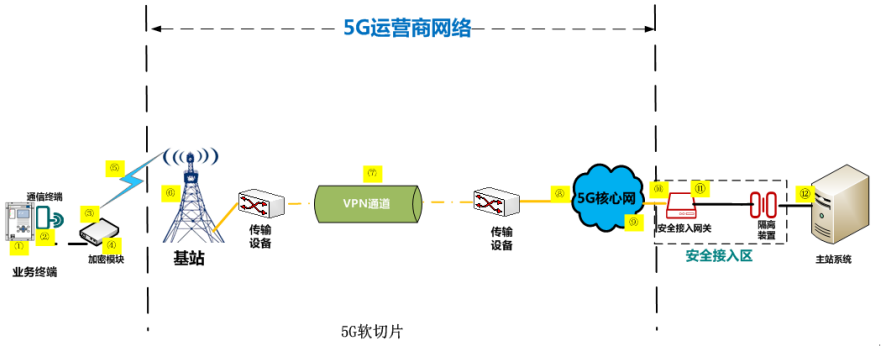

图1 5G 电力非涉控终端测试环境图

8.1.3 测试单元

8.1.3.1 通道合规

通道合规测试单元应满足下列技术要求：

a) 测试实施：

1) 采取必要措施进行伪基站鉴别，防止通过伪基站接入，设立伪基站进行测试接入，检测是否能够实现伪基站识别。

2) 支持空口信令 DDOS 攻击防御: 可使用测试仪器模拟发起空口信令 DDOS 攻击，检测基站在泛洪攻击下是否正常提供通信服务

3) 基站应支持伪造 GPS、北斗等信号的检测和防御：利用测试仪器模拟 GPS 位置攻击或者时间欺骗

b) 预期结果：

1) 能够实现伪基站识别；

2) 终端遭受 SYN Flood、UDP Flood 等攻击时，终端运行正常，通信正常；

3) 无线信号被干扰不会导致业务通信延迟。

c) 单元判定：如果上述 b）、c)预期结果为肯定，则基本符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.2 切片隔离

切片隔离测试单元应满足下列技术要求：

a) 测试实施：应设置不同等级的切片应用，实现访问隔离。通过抓包工具、5G 核心网测试仪，验证每个切片及对应 NF 使用独立的网络资源、流量互相隔离。

b) 预期结果：每个切片间的流量互相隔离；

c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.3 边界隔离

边界隔离测试单元应满足下列技术要求：

a) 测试实施：

1) 在电力边界处部署访问控制机制，配置并启用访问控制规则，保证规则有效性：验证用户所具有的权限是否与设定的访问控制规则一致；

2) 在电力边界处部署网络入侵检测/防御设备，配置并启用入侵检测/防御策略：采用漏洞扫描工具，验证入侵检测/防御策略是否生效；

3) 在电力边界处部署恶意代码检测和清除设备，并维护恶意代码的升级与更新：采用漏洞扫描工具，验证恶意代理检测策略是否生效；

4) 通过必要措施识别 DoS/DDoS 攻击异常流量并丢弃，放行正常网络访问流量：使用发包工具模拟大量非法数据量接入。

b) 预期结果：

1) 用户所具有的权限与设定的访问控制规则一致；

2) 入侵检测/防御策略能识别网络入侵行为；

3) 恶意代码检测策略能识别病毒木马；

4) 不会因大量发包而拒绝服务，能阻止 ddos 攻击。

c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.4 访问控制

访问控制测试单元应满足下列技术要求：

a) 测试实施：

1) 限制访问的 IP 地址：设置非白名单地址测试访问；

2) 采取机卡绑定：人工查看，SIM 卡插入其他设备验证是否可以正常上网。

b) 预期结果：

1) 无法访问终端；

2) 机卡分离后约 5 分钟 sim 卡停机，无法上网。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.5 认证与鉴权

认证与鉴权测试单元满足下列技术要求

a） 测试实施：
1） 宜通过部署电力专用鉴权服务器对通信终端进行二次鉴权：更换未绑定的通信终端并启用二次鉴权功能，在核心网抓包查看二次鉴权是否通过；
2） 应配置固定 IP 地址：查看通信终端 IP 地址及配置方式，检测静态 IP 地址是否固化在终端类，或授权通过后，才允许修改。

b） 预期结果：
1） 使用非法终端接入网络，二次鉴权失败；
2） 静态 IP 地址固化在终端中，或通过认证授权后，才允许修改。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.6 固件要求

固件要求测试单元满足下列技术要求：

a） 测试实施：
1） 宜通过验证可信根的方式对固件的硬件控制和硬件加解密程序等进行可信验证：通过逆向分析工具、协议模糊测试工具对固件程序进行检测；
2） 在使用过程中应避免存在注入攻击、缓冲区溢出、远程系统调用、信息泄露等风险漏洞：通过逆向分析工具、协议模糊测试工具对固件程序进行检测。

b） 预期结果：
1） 更改固件程序后，无法通过可信验证及安装；
2） 固件程序逻辑正确，未发现明显的漏洞。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.7 身份验证

身份验证测试单元满足下列技术要求：

a） 测试实施：
1） 对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换：通过抓包工具、5G 核心网测试仪检测，5G 通信终端初始注册时，SUPI 应加密成 SUCI；
2） 具有登录失败处理功能，应配置结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施：人工查看核查相关配置；
3） 采取必要措施防止鉴别信息在网络传输过程中被泄露：通过抓包工具，获取到明文或可被解码的鉴别信息。

b） 预期结果：
1） 在基站或核心网或终端侧抓取数据包，验证终端初始注册的交互过程，并不能获取解密后的 SUPI；
2） 存在密码复杂度及安全登录措施；
3） 无法获取到明文和可被解码的鉴别信息。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.8 密钥协商认证

密钥协商认证测试单元满足下列技术要求：

a） 测试实施：

1) 至少启用一种加密算法，用于空口数据加密和完整性保护：在设备本地或通过镜像方式获取 N2 口数据，查看是否至少启用 AES、snow3G、ZUC 中的一种，用于完整性、机密性保护算法；
2) 宜采取硬件密码模块或软件密码模块等方式实现通道加密：查看业务终端是否集成安全密码芯片；
3) 终端数据安全传输、敏感内容加密、数字签名应采用国家认可的加密算法：通过抓包工具查找有没有 client hello 和 server hello 等签名校验机制的身份认证报文，确认业务数据进行加解密。

b) 预期结果：
1) N2 口至少启用 AES、snow3G、ZUC 中的一种，用于完整性和机密性保护算法；
2) 终端集成安全密码芯片；
3) 认证通过后，业务终端通过 SM2 或其他国家加密算法进行加解密。

c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.9 终端本体鉴别

终端本体鉴别测试单元应满足下列技术要求：

a) 测试实施：在网络内应有唯一身份标识，采取必要措施进行终端本体鉴别：通过抓包工具验证各类终端数据中身份标识是否唯一；
b) 预期结果：终端身份标识唯一，且通过身份标识进行身份验证及接入；
c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.10 完整性

完整性测试单元应满足下列技术要求：

a) 测试实施：采用国家认可的密码技术保证数据传输过程中的完整性，采取数据校验和重传，实现数据恢复：抓取终端上报的数据包，查看业务数据是否具备完整性校验码；
b) 预期结果：业务数据包中包含完整性校验，且校验通过；
c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.11 保密性

保密性测试单元应满足下列技术要求：

a) 测试实施：
1) 在传输时可采用具有一定强度的加密算法或其他措施对信息进行加密：查看终端是否支持通过安全密码芯片或外置加密机等，与主站业务系统进行双向身份认证；
2) 密码技术应使用由可信方提供的密钥和数字证书：认证完成后，分别在终端侧、主站业务系统侧抓取业务数据包，查看是否为密文；
3) 采用国家密码主管部门认可的密码算法保证传输过程中数据的保密性：查看安全密码芯片型号、认证及加密使用的加密算法。

b) 预期结果：
1) 终端集成安全密码芯片或外置加密机等基于数字证书技术，与主站业务系统实现双向身份认证；
2) 终端出口、主站业务系统入口侧业务数据包为密文；
3) 记录安全密码芯片型号、认证及加密使用的加密算法。

c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.1.3.12 可用性

可用性测试单元应满足下列技术要求：

a) 测试实施：可采用必要措施实现抗重放攻击：采用抓包工具对对关键数据包例如登录入口、修改密码入口进行重放；
b) 预期结果：重复发送数据包无法得到响应；
c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2 5G 电力涉控终端接入测试规范

8.2.1 测试工具

5G电力涉控终端接入测试工具见表2。

表2 5G 电力涉控终端测试工具

序号	仪器设备名称	接入位置编号
1	网络性能测试仪	②③④⑩⑪⑫
2	5G 路测工具	⑤
3	5G 信令安全测试仪	⑧⑨
4	5G 核心网测试仪	⑧⑨
5	协议模糊测试工具	①②⑧⑨
6	漏洞扫描工具	①②⑥⑧⑩⑫
7	抓包工具	①②⑥⑧⑩⑫
8	逆向分析工具	①②⑥⑧⑩⑫
9	漏洞验证工具	①②⑥⑧⑩⑫
10	端口扫描工具	① ②⑥⑨⑩⑫

8.2.2 测试环境

5G电力涉控终端接入测试环境见图2。

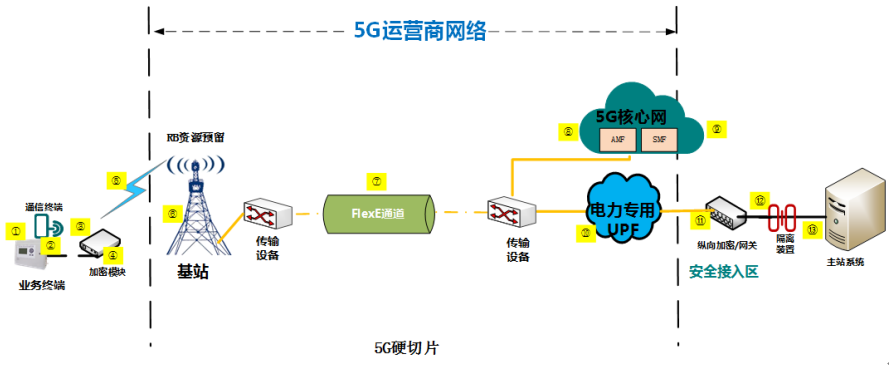

图2 5G 电力涉控终端测试环境图

8.2.3 测试单元

8.2.3.1 通道合规

通道合规测试单元应满足下列技术要求：
a) 测试实施
1) 应采取必要措施进行伪基站鉴别，防止通过伪基站接入；设立伪基站进行测试接入，检测是否能够实现伪基站识别。
2) 支持空口信令 DDOS 攻击防御： 可使用测试仪器模拟发起空口信令 DDOS 攻击，检测基站在泛洪攻击下是否正常提供通信服务
3) 基站应支持伪造 GPS、北斗等信号的检测和防御：利用测试仪器模拟 GPS 位置攻击或者时间欺骗
b) 预期结果：

1) 能够实现伪基站识别；
2) 终端遭受 SYN Flood、UDP Flood 等攻击时，终端运行正常，通信正常；
3) 无线信号被干扰不会导致业务通信延迟。

c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.2 切片隔离

切片隔离测试单元应满足下列技术要求：

a) 测试实施：
1) 设置不同等级的切片应用，实现访问隔离：通过抓包工具、5G 核心网测试仪，验证每个切片及对应 NF 使用独立的网络资源、流量互相隔离；
2) 设置硬切片通道资源预留，包括 RB 资源、FLexE：验证接入网是否启用 RB 资源预留功能且承载网使用 FlexE 功能，以实现硬切片，并通过发包工具测试资源预留情况。

b) 预期结果：
1) 每个切片间的流量互相隔离；
2) 接入网通过 RB 资源预留，承载网使用 FlexE 通道，完成硬切片划分。

c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.3 电力专用 UPF 加固

电力专用UPF加固测试单元应满足下列技术要求：

a) 测试实施：
1) 电力专用 UPF 应加强基线配置、安全加固：UPF 应支持 IPSec 加密传输，UPF 应支持虚拟防火墙功能以及其他安全配置；
2) 电力专用 UPF 应限制开放端口，仅允许授权账号登录：使用不同权限用户登录 UPF，查看其具有的权限是否相同；验证 UPF 是否能够依据访问控制策略，限制对 SMF、基站的访问控制；
3) 电力专用 UPF 应避免存在注入攻击、缓冲区溢出、远程系统调用、信息泄露等风险漏洞：采用协议模糊测试工具，对 UPF 进行安全测试。

b) 预期结果：
1) 按照设置的策略对系统账号口令、登录限制、文件目录进行加固；
2) 只有 SMF、基站的 IP 在 UPF 访问控制策略允许的范围内，SMF、基站与 UPF 才能正常通信；
3) UPF 使用的协议不存在安全漏洞，UPF 不存在非授权访问。

c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.4 边界隔离

边界隔离测试单元应满足下列技术要求：

a) 测试实施：
1) 在电力边界处部署访问控制机制，配置并启用访问控制规则，保证规则有效性：验证用户所具有的权限是否与设定的访问控制规则一致；
2) 在电力边界处部署网络入侵检测/防御设备，配置并启用入侵检测/防御策略：采用漏洞扫描工具，验证入侵检测/防御策略是否生效；
3) 在电力边界处部署恶意代码检测和清除设备，并维护恶意代码的升级与更新：采用漏洞扫描工具，验证恶意代理检测策略是否生效；
4) 通过必要措施识别 DoS/DDoS 攻击异常流量并丢弃，放行正常网络访问流量：使用发包工具模拟大量非法数据量接入；
5) 电力边界应部署专用流量分析装置，并具备实时采集、协议识别、文件还原、特征检测等安全功能：人工查看专用流量分析装置对业务流量的识别效果；

6） 电力边界宜部署深度异常行为感知、溯源分析、安全可视化等安全增强技术措施：采用漏洞扫描工具及人工验证，验证安全技术措施有效性。

b） 预期结果：

1） 用户所具有的权限与设定的访问控制规则一致；

2） 入侵检测/防御策略能识别网络入侵行为；

3） 恶意代码检测策略能识别病毒木马；

4） 不会因大量发包而拒绝服务，能阻止 ddos 攻击；

5） 完成相应安全设备部署，并启用相应策略；

6） 完成相应安全设备部署，并启用相应策略。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.5 访问控制

访问控制测试单元应满足下列技术要求：

a） 测试实施：

1） 限制访问的 IP 地址：设置非白名单地址测试访问；

2） 采取机卡绑定：人工查看，SIM 卡插入其他设备验证是否可以正常上网；

3） 5G 电力终端支持基站绑定：验证终端是否能接入非绑定 5G 基站。

b） 预期结果：

1） 无法访问终端；

2） 机卡分离后约 5 分钟 sim 卡停机，无法上网；

3） 终端无法接入非绑定 5G 基站。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.6 认证与鉴权

认证与鉴权测试单元满足下列技术要求：

a） 测试实施：

1） 宜通过部署电力专用鉴权服务器对通信终端进行二次鉴权：更换未绑定的通信终端并启用二次鉴权功能，在核心网抓包查看二次鉴权是否通过；

2） 应配置固定 IP 地址：查看通信终端 IP 地址及配置方式，检测静态 IP 地址是否固化在终端类，或授权通过后，才允许修改。

b） 预期结果：

1） 使用非法终端接入网络，二次鉴权失败；

2） 静态 IP 地址固化在源代码中，或通过认证授权后，才允许修改。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.7 固件要求

固件要求测试单元满足下列技术要求：

a） 测试实施：

1） 宜通过验证可信根的方式对固件的硬件控制和硬件加解密程序等进行可信验证：通过逆向分析工具、协议模糊测试工具对固件程序进行检测；

2） 在使用过程中应避免存在注入攻击、缓冲区溢出、远程系统调用、信息泄露等风险漏洞：通过逆向分析工具、协议模糊测试工具对固件程序进行检测。

b） 预期结果：

1） 更改固件程序后，无法通过可信验证及安装；

2） 固件程序逻辑正确，未发现明显的漏洞。

c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.8 身份验证

身份验证测试单元满足下列技术要求：

a) 测试实施：
   1) 对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换：通过抓包工具、5G 核心网测试仪检测，5G 通信终端初始注册时，SUPI 应加密成 SUCI；
   2) 具有登录失败处理功能，应配置结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施：人工查看核查相关配置；
   3) 采取必要措施防止鉴别信息在网络传输过程中被泄露：通过抓包工具，获取到明文或可被解码的鉴别信息；
   4) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现：人工查看核查相关配置。
b) 预期结果：
   1) 在基站或核心网或终端侧抓取数据包，验证终端初始注册时，根据 Public Key 把 SUPI 加密成 SUCI，并发送初始注册请求，AMF 转发 SUCI 给 AUSF 和 UDM 进行认证，并获取解密后的 SUPI；
   2) 存在密码复杂度及安全登录措施；
   3) 无法获取到明文和可被解码的鉴别信息；
   4) 采用多种方式进行身份鉴别；
c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.9 密钥协商认证

密钥协商认证测试单元满足下列技术要求：

a) 测试实施：
   1) 至少启用一种加密算法，用于空口数据加密和完整性保护：在设备本地或通过镜像方式获取 N2 口数据，查看是否至少启用 AES、snow3G、ZUC 中的一种，用于完整性、机密性保护算法；
   2) 宜采取硬件密码模块或软件密码模块等方式实现通道加密：查看业务终端是否集成安全密码芯片；
   3) 终端数据安全传输、敏感内容加密、数字签名应采用国家认可的加密算法：通过抓包工具查找有没有 client hello 和 server hello 等签名校验机制的身份认证报文，确认业务数据进行加解密；
   4) 终端纵向传输应采用经认证的加密传输协议，使用专用密钥协商，通过密钥协商后方可与应用系统进行连接：人工核查查看终端纵向加密是否采用专用加密设备。
b) 预期结果：
   1) N2 口至少启用 AES、snow3G、ZUC 中的一种，用于完整性和机密性保护算法；
   2) 终端集成安全密码芯片；
   3) 认证通过后，业务终端通过 SM2 或其他国家加密算法进行加解密；
   4) 部署专用加密设备。
c) 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.10 终端本体鉴别

终端本体鉴别测试单元应满足下列技术要求：

a) 测试实施：
   1) 在网络内应有唯一身份标识，采取必要措施进行终端本体鉴别：通过抓包工具验证各类终端数据中身份标识是否唯一；
   2) 采用白名单技术限制终端本体接入：采用非标识终端进行测试接入。

b） 预期结果：
1） 终端身份标识唯一，且通过身份标识进行身份验证及接入；
2） 非标识终端无法进行接入。
c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.11 完整性

完整性测试单元应满足下列技术要求：
a） 测试实施：采用国家认可的密码技术保证数据传输过程中的完整性，采取数据校验和重传，实现数据恢复：抓取终端上报的数据包，查看业务数据是否具备完整性校验码；
b） 预期结果：业务数据包中包含完整性校验，且校验通过。
c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.12 保密性

保密性测试单元应满足下列技术要求：
a） 测试实施：
1） 在传输时可采用具有一定强度的加密算法或其他措施对信息进行加密：查看终端是否支持通过安全密码芯片或外置加密机等，与主站业务系统进行双向身份认证；
2） 密码技术应使用由可信方提供的密钥和数字证书：认证完成后，分别在终端侧、主站业务系统侧抓取业务数据包，查看是否为密文；
3） 采用国家密码主管部门认可的密码算法保证传输过程中数据的保密性：查看安全密码芯片型号、认证及加密使用的加密算法；
4） 建立数据传输通道前，应对发送方和接收方进行身份鉴别，会话初始化也应采用加密技术加固：通过抓包工具，验证会话初始过程中，重要信息是否加密。
b） 预期结果：
1） 终端集成安全密码芯片或外置加密机等基于数字证书技术，与主站业务系统实现双向身份认证；
2） 终端出口、主站业务系统入口侧业务数据包为密文；
3） 记录安全密码芯片型号、认证及加密使用的加密算法；
4） 会话初始过程中，重要信息实现加密。
c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

8.2.3.13 可用性

可用性测试单元应满足下列技术要求：
a） 测试实施：可采用必要措施实现抗重放攻击：采用抓包工具对对关键数据包例如登录入口、修改密码入口进行重放；
b） 预期结果：重复发送数据包无法得到响应；
c） 单元判定：如果以上测评实施内容为肯定，则符合本单元测评要求，否则不符合本单元测评指标要求。

附 录 A
（规范性）
电力终端 5G 接入场景及安全等级要求

A.1 电力终端 5G 接入典型应用场景、切片等级、组网方式、运营商类型以及安全等级等见表 1。

表 A.1 电力终端 5G 接入场景及安全等级要求

业务名称	时延	切片等级	接入运营商	组网方式	应用场景
10kV分布式电源调控	无线≤60s	硬切片	移动、电信、联通	SA	涉控类场景
配电自动化“三遥”	<3s	硬切片	移动、电信、联通	SA	涉控类场景
毫秒级精准负荷控制	毫秒级业务<50ms；	硬切片	移动、电信、联通	SA	涉控类场景
0.4kV低压分布式光伏	无线≤60s	软切片	移动、电信、联通	SA	非涉控类场景
输电架空线路/电缆监测	≤1s	软切片	移动、电信、联通	SA	非涉控类场景
一次设备在线监测	≤2s	软切片	移动、电信、联通	SA	非涉控类场景
动环监测	≤2s	软切片	移动、电信、联通	SA	非涉控类场景
配电站房环境状态监测	传感业务≤2s；	软切片	移动、电信、联通	SA	非涉控类场景
用电信息采集	采集业务：≤6s； 负控业务：≤2s； 分钟级采集业务：≤5s	软切片	移动、电信、联通	SA	非涉控类场景
电动汽车充电桩	<3s	软切片	移动、电信、联通	SA	非涉控类场景
配电站房环境状态监测	图像视频业务≤300ms	软切片	移动、电信、联通	SA	非涉控类场景
输电线路无人机巡检	<300ms	软切片	移动、电信、联通	SA	非涉控类场景
掌上电力	毫秒级/秒级	软切片	移动、电信、联通	NSA	非涉控类场景
网上国网	毫秒级/秒级	软切片	移动、电信、联通	NSA	非涉控类场景
其他用户、电厂	毫秒级/秒级	软切片	移动、电信、联通	NSA	非涉控类场景