

ICS 点击此处添加 ICS 号

CCS 点击此处添加 CCS 号

DL

中华人民共和国电力行业标准

DL/T XXXXX—2023

电力 5G 网络安全测试规范

5G Network Security Test Specification of Power security

(点击此处添加与国际标准一致性程度的标识)

(征求意见稿)

XXXX - XX - XX 发布

20XX - XX - XX 实施

国家能源局 发布

目 次

| | |
|-------------------------------------|-----|
| 前 言 | III |
| 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 5G 网络安全测试环境要求 | 2 |
| 5.1 测试组网架构图 | 2 |
| 5.2 测试条件 | 3 |
| 5.3 测试仪表 | 3 |
| 6 电力 5G 网络通道安全测试规范 | 4 |
| 6.1 电力 5G 网络安全隔离——逻辑隔离 | 4 |
| 6.1.1 无线网 QoS 优先级保障功能 | 4 |
| 6.1.2 传输网 VLAN 隔离 | 4 |
| 6.1.3 核心网 UPF 隔离（可选） | 4 |
| 6.1.4 电力 5G 业务逻辑隔离 | 5 |
| 6.2 电力 5G 网络安全隔离——物理资源隔离 | 5 |
| 6.2.1 无线网 PRB 资源预留 | 5 |
| 6.2.2 传输网 FlexE 通道隔离 | 5 |
| 6.2.3 传输网 MTN 通道隔离 | 5 |
| 6.2.4 5G 核心网 UPF 隔离 | 6 |
| 6.3 电力 5G 网络核心网网元安全 | 6 |
| 6.3.1 IPv4/IPv6 访问控制安全 | 6 |
| 6.3.2 N3 接口传输的用户数据机密性保护（可选） | 6 |
| 6.3.3 N4 接口信令数据机密性保护（可选） | 6 |
| 6.3.4 电力专用 UPF 对电力 5G 终端的互访控制 | 7 |
| 6.3.5 电力 UPF 敏感数据保护 | 7 |
| 6.3.6 电力 UPF 数据删除 | 7 |
| 6.3.7 电力 UPF 漏洞扫描 | 7 |
| 6.3.8 电力 UPF 攻击防范 | 7 |
| 6.4 电力 5G 网络安全区域边界 | 7 |
| 7 电力 5G 终端安全测试规范 | 8 |
| 7.1 电力 5G 终端安全 | 8 |
| 7.1.1 可信验证 | 8 |
| 7.1.2 身份鉴别 | 8 |
| 7.1.3 安全存储 | 8 |
| 7.1.4 访问控制 | 8 |
| 7.1.5 机卡标识关联 | 8 |
| 7.2 电力 5G 终端接入安全 | 8 |
| 7.2.1 次认证 | 8 |
| 7.2.2 防火墙 | 8 |
| 7.2.3 安全接入 | 8 |
| 7.2.4 eSIM 芯片国密算法支持 | 9 |
| 8 电力 5G 管理平台安全测试要求 | 9 |
| 8.1 平台自身安全管理 | 9 |
| 8.1.1 账号管理 | 9 |

| | | |
|-------|----------------------|----|
| 8.1.2 | 用户认证 | 9 |
| 8.1.3 | 权限管理 | 9 |
| 8.1.4 | 平台访问控制 | 9 |
| 8.1.5 | 日志管理 | 10 |
| 8.2 | 网络态势感知安全测试 | 10 |
| 8.2.1 | 5G 核心网性能监控 | 10 |
| 8.2.2 | 5G 基站性能监控 | 10 |
| 8.2.3 | 5G 核心网告警 | 10 |
| 8.2.4 | 5G 基站告警 | 11 |
| 8.2.5 | 终端网络异常告警 | 11 |
| 8.2.6 | 链路告警 | 11 |
| 8.2.7 | 电力 5G 虚拟专网态势呈现 | 11 |
| 8.3 | 事件审计管理安全测试 | 11 |
| 8.3.1 | 审计事件记录 | 12 |
| 8.3.2 | 审计事件管理 | 12 |
| 8.4 | 安全应急处置 | 12 |
| 8.4.1 | 终端强制下线 | 12 |

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。

本文件由中国电力企业联合会提出。

本文件由电力行业信息标准化技术委员会（DL/TC27）归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

本文件在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条1号，100761）。

电力 5G 网络安全测试规范

1 范围

本文件规定了电力5G网络安全测试规范,包括电力5G网络通道安全测试、电力5G终端接入安全测试、电力5G管理平台安全测试等。

本文件适用于电力5G网络的安全测试。

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 28448-2019 信息安全技术—网络安全等级保护测评要求
- GB/T 36572-2018 电力监控系统网络安全防护导则
- GB/T 41266-2022 网络关键设备安全检测方法 交换机设备
- DL/T 2613-2023 电力行业网络安全等级保护测评指南
- DL/T 2614-2023 电力行业网络安全等级保护基本要求
- DL/T XXXX-XXXX 电力5G终端测试规范
- DL/T XXXX-2023 电力5G安全技术要求
- YD/T 3973-2021 5G网络切片 端到端总体技术要求
- YD/T 3992-2021 灵活以太网(FlexE)链路接口测试方法

3 术语和定义

GB/T 28448-2019、GB/T 36572-2018、GB/T 41266-2022、DL/T 2613-2023、DL/T 2614-2023、DL/T XXXX-2023界定的以及下列术语和定义适用于本文件。

3.1

网络切片 network slice

提供特定网络能力和网络特征(如资源隔离、SLA保障特性等)、为客户提供多种业务属性的逻辑网络。

[来源: YD/T 3973-2021, 3.1.1]

3.2

电力 5G 网络 5G power network

电力企业基于基础电信企业 5G 网络部署的电力 5G 行业虚拟专网。

[来源: DL/T XXXX-2023, 3.1]

3.3

电力专用 UPF power private UPF

电力企业独立部署、独立使用,并与公共 5G 网络用户面或其他行业 5G 网络用户面实现物理隔离的 5G 用户面设备。

[来源: DL/T XXXX-2023, 3.2]

3.4

共享 UPF sharing UPF

基础电信企业部署,供多个行业共享使用,并与公共 5G 网络用户面网元实现物理隔离的 5G 用户面设备。

[来源: DL/T XXXX-2023, 3.3]

3.5

电力 5G 终端 5G power user equipment

通过外部线缆或内部接口方式实现 5G 接入的电力通信终端设备,包括集中器终端、智能配变终端、台区智能终端、能源控制器终端、电力 CPE 终端等类型。

[来源: DL/T XXXX-2023, 3.4]

3.6

电力 5G 业务 5G power service

承载于 5G 网络的电力业务,包括 5G 控制类业务、5G 采集类业务、5G 移动应用类业务、5G 多站融合业务等。

[来源: DL/T XXXX-2023, 3.5]

3.7

电力 5G 管理平台 5G power management platform

实现基础电信企业 5G 网络管理能力开放与电力 5G 业务管控的平台,支持网络管理、终端管理、审计管理等功能。

[来源: DL/T XXXX-2023, 3.6]

4 缩略语

下列缩略语适用于本文件。

AKA: 第三代移动通讯网络的认证与密钥协商协议 (Authentication and Key Agreement)

AMF: 接入和移动性管理功能 (Access and Mobility Management Function)

DMZ: 隔离区 (Demilitarized Zone)

DNN: 数据网络标识 (Data Network Name)

EAP: 可扩展认证协议 (Extensible Authentication Protocol)

FlexE: 灵活以太网技术 (Flexible Ethernet)

L2VPN: 承载层二业务的虚拟专用网 (Layer 2 Virtual Private Network)

IMSI: 国际移动用户识别号 (International Mobile Subscriber Identification Number)

IP: 网际互连协议 (Internet Protocol)

MPLS: 多协议标签交换 (Multi-Protocol Label Switching)

MPLS-TP: 面向传送的多协议标签交换 (Multi-Protocol Label Switching Transport Profile)

MTN: 城域传输网络 (Metro Transport Network)

PDU: 协议数据单元 (Protocol Data Unit)

PRB: 物理资源块 (Physical Resource Block)

QoS: 服务质量 (Quality of Service)

SMF: 会话管理功能 (Session Management Function)

SNMP: 简单网络管理协议 (Simple Network Management Protocol)

SSH: 安全外壳协议 (Secure Shell)

SUCI: 订阅隐私标识符 (Subscription Concealed Identifier)

UDM: 统一数据管理 (Unified Data Management)

UDP: 用户数据报协议 (User Datagram Protocol)

UPF: 用户面功能 (User Plane Function)

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

VPN: 虚拟专用网 (Virtual Private Network)

5 电力 5G 网络安全测试环境要求

5.1 测试组网架构图

电力 5G 网络安全测试基本组网架构如图 1 所示,电力 5G 虚拟专网包括电力 5G 终端、5G 基站、传输网、5G 核心网等部分,通过网络切片、FlexE、PRB 资源预留、QoS 设置、VLAN 等技术实现 5G 网络通道的隔离。经 UPF 处理后接入电力安全隔离装置并进入电力系统区域,通过认证、加解密装置等实现业务的认证。各部分可通过计算机、数据网络测试仪、5G 网络信令工具等开展测试。

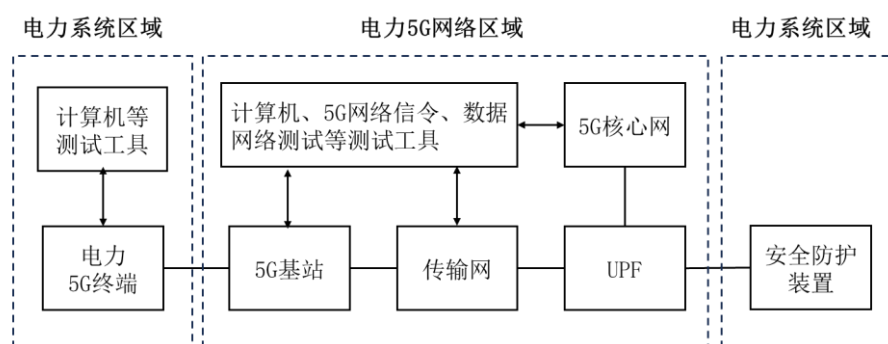


图1 电力5G网络安全测试基本组网架构图

电力5G网络UPF隔离测试组网架构如图2所示，电力5G虚拟专网根据业务类型分别通过共享UPF或电力专用UPF与电力安全隔离装置连接，通过计算机、数据网络测试仪、5G网络信令分析仪等工具开展测试。

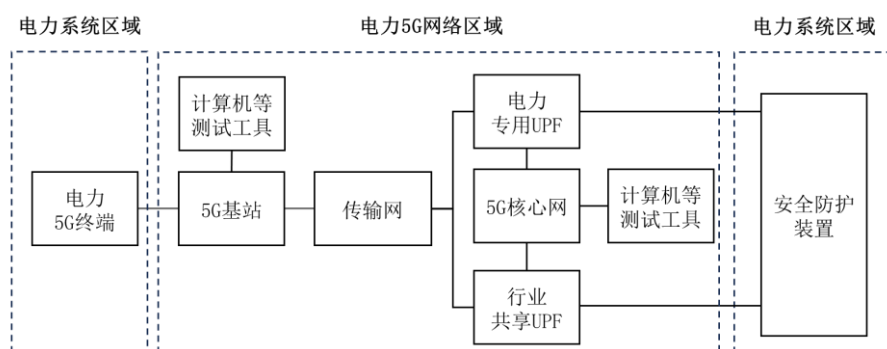


图2 电力5G网络UPF隔离测试组网架构图

电力5G网络管理平台测试架构如图3所示，电力5G管理平台连接电力5G虚拟专网，并通过计算机装载测试工具，通过页面或借助FTP等工具执行测试。

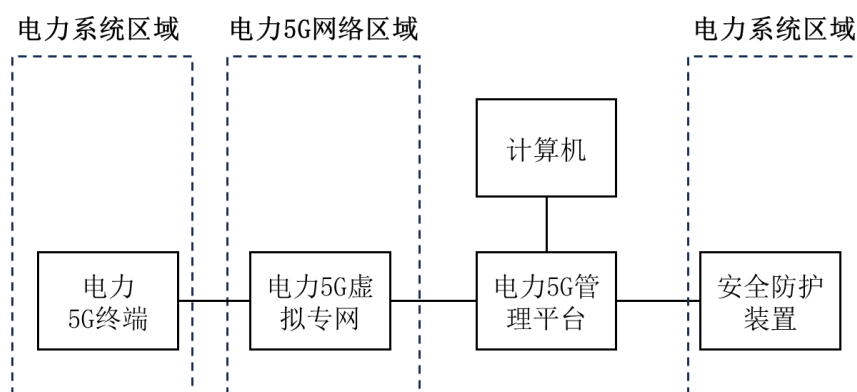


图3 电力5G网络管理平台测试架构

5.2 测试条件

- 电力5G虚拟专网硬件软件全部工作正常，数据正确配置并正常运行；
- 电力5G终端、5G基站和5G核心网的各项配置根据标准场景完成。

5.3 测试仪表

本测试规范涉及的测试仪表包括但不限于：

- a) 5G 网络信令分析工具：主要用于抓取并分析电力 5G 终端、5G 基站、5G 核心网等部分主要接口和参考点（服务化接口、N4 参考点等）上的信令消息，配合完成业务流程的测试分析；
- b) 数据网络测试仪：主要用于网络不同层级通信中的数据检测和分析，如报文分析、协议仿真等。

6 电力 5G 网络通道安全测试规范

电力 5G 网络通道安全根据电力业务系统的主要分区进行测试，包括验证生产控制大区与基础电信企业 5G 公网之间的物理资源隔离，以及生产控制大区不同安全区之间、管理信息大区与基础电信企业 5G 公网之间的逻辑隔离。

6.1 电力 5G 网络安全隔离——逻辑隔离

针对电力 5G 虚拟专网无线网的 QoS 优先级保障、传输网的 VLAN 等逻辑隔离技术要求进行测试，验证电力 5G 网络可实现逻辑隔离。

6.1.1 无线网 QoS 优先级保障功能

- a) 测试目的：验证电力 5G 网络无线网的 QoS 优先级保障功能。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 在 5G 基站侧配置电力 5G 终端 1 的 QoS 为高优先级，配置电力 5G 终端 2 的 QoS 为较低优先级；
 - 2) 电力 5G 终端 1 和电力 5G 终端 2 在 5G 基站的同一小区进行接入；
 - 3) 在核心网侧通过 5G 网络信令分析工具获取并查看电力 5G 终端 1 和电力 5G 终端 2 接入信令。
- d) 预期结果：

电力 5G 终端 1 和电力 5G 终端 2 成功接入电力 5G 网络，且信令日志中电力 5G 终端 1 优先级配置高于电力 5G 终端 2，电力 5G 网络无线网实现 QoS 优先级保障。

6.1.2 传输网 VLAN 隔离

- a) 测试目的：验证电力 5G 网络传输网基于 VLAN 划分实现通道隔离。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 在 5G 核心网侧配置网络切片 1 和网络切片 2；
 - 2) 配置 5G 基站与核心网之间传输网对应 VLAN ID1 和 VLAN ID2；
 - 3) 配置电力 5G 终端 1 和电力 5G 终端 2 分别支持网络切片 1 和网络切片 2 接入；
 - 4) 电力 5G 终端 2 启动上行 UDP 业务，在 5G 基站侧通过 5G 网络信令分析工具获取并查看电力 5G 终端 2 上行速率；
 - 5) 电力 5G 终端 1 启动切片内上行满 buffer UDP 业务，在基站侧通过 5G 网络信令分析工具获取并查看电力 5G 终端 2 上行速率变化情况；
 - 6) 通过 5G 网络信令分析工具获取并观测电力 5G 终端侧、基站侧、核心网侧切片 ID 信息。
- d) 预期结果：

电力 5G 终端 2 的业务不受影响且上行速率基本稳定，电力 5G 终端 1 与电力 5G 终端 2 切片 ID 与配置信息一致，电力 5G 网络传输网实现 VLAN 隔离。

6.1.3 核心网 UPF 隔离（可选）

- a) 测试目的：验证电力 5G 网络可基于独立部署的 UPF 实现隔离。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 在终端侧配置电力 5G 终端 1 接入共享 UPF，电力 5G 终端 2 接入电力专用 UPF；
 - 2) 电力 5G 终端 1 发起 UDP 业务，在核心网侧抓包查看数据流目的地址走向；

- 3) 电力 5G 终端 2 发起 UDP 业务，在核心网侧抓包查看数据流目的地址走向。
- d) 预期结果：
 - 1) 电力 5G 终端 1 的数据成功转发到共享 UPF，并流向主站；
 - 2) 电力 5G 终端 2 的数据成功转发到电力专用 UPF，并流向主站。

6.1.4 电力 5G 业务逻辑隔离

- a) 测试目的：验证电力 5G 业务可通过电力 5G 网络实现终端到电力 5G 安全接入装置之间的逻辑隔离。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 在 5G 核心网侧配置网络切片 1 和网络切片 2；
 - 2) 5G 基站与 5G 核心网之间传输设备分别配置 VLAN ID1 和 VLAN ID2；
 - 3) 配置电力 5G 终端 1 支持切片 1，电力 5G 终端 2 支持切片 2，且电力 5G 终端 1 的 QoS 优先级高于电力 5G 终端 2；
 - 4) 电力 5G 终端 1 启动上行满 buffer UDP 业务，在核心网侧查看电力 5G 终端 1 上行速率；
 - 5) 电力 5G 终端 2 启动上行满 buffer UDP 业务，在核心网侧查看电力 5G 终端 1 上行速率变化情况。
- d) 预期结果：

电力 5G 终端 2 启动上行业务后，电力 5G 终端 1 上行速率基本无变化，电力 5G 业务基于电力 5G 网络实现逻辑隔离。

6.2 电力 5G 网络安全隔离——物理资源隔离

针对电力 5G 网络无线网的 PRB 资源预留、传输网的 FlexE 或 MTN、核心网 UPF 独立部署等技术要求进行测试，验证电力 5G 网络可实现物理资源隔离。

6.2.1 无线网 PRB 资源预留

- a) 测试目的：验证电力 5G 网络可通过无线网的 PRB 资源预留实现物理资源隔离。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 通过网管平台在 5G 核心网侧配置网络切片 1 和网络切片 2；
 - 2) 通过网管平台在 5G 核心网侧为网络切片 1 配置一定数值的上下行 PRB 资源；
 - 3) 在终端侧配置电力 5G 终端 1 支持网络切片 1，电力 5G 终端 2 支持网络切片 2；
 - 4) 电力 5G 终端 1 启动上行网络切片内满 buffer 业务，速率稳定后，查看 5G 基站侧 PRB 利用率；
 - 5) 电力 5G 终端 2 启动上行网络切片满 buffer 业务，速率稳定后，查看 5G 基站侧 PRB 利用率；
 - 6) 停止电力 5G 终端 1 和电力 5G 终端 2 上行业务；
 - 7) 电力 5G 终端 1 启动下行网络切片满 buffer 业务，速率稳定后，查看 5G 基站侧 PRB 利用率；
 - 8) 电力 5G 终端 2 启动上行网络切片满 buffer 业务，速率稳定后，查看 5G 基站侧 PRB 利用率。
- d) 预期结果：
 - 1) 电力 5G 终端 2 接入前，电力 5G 终端 1 占据上/下行 PRB 资源与配置数值一致；
 - 2) 电力 5G 终端 2 接入后，电力 5G 终端 1 业务不受影响，占据的上/下行 PRB 资源不变，且与配置数值一致，电力 5G 网络通过 PRB 预留方式实现物理资源隔离。

6.2.2 传输网 FlexE 通道隔离

传输网 FlexE 接口通道化能力测试应按照 YD/T 3992-2021 中 7.1 和 7.2 章节相关测试方法进行测试。

6.2.3 传输网 MTN 通道隔离

- a) 测试目的：验证电力 5G 网络传输网通过 MTN 实现隔离。
- b) 测试拓扑：测试拓扑图 3。
- c) 测试步骤：
 - 1) 在传输网侧配置网元 1、网元 2、网元 3 三个节点，在网元 1 与网元 2 之间创建经过网元 3 的 MTN 通道 1 和 MTN 通道 2；
 - 2) 在网元 1 与网元 2 之间创建 MPLS-TP 隧道 1，并承载于 MTN 通道 1，创建 MPLS-TP 隧道 2 和 MPLS-TP 隧道 3，且均承载于 MTN 通道 2；
 - 3) 在网元 1 与网元 2 之间创建 L2VPN 业务 1，并承载于 MPLS-TP 隧道 1，创建 L2VPN 业务 2 和 L2VPN 业务 3，并分别承载于 MPLS-TP 隧道 2、隧道 3；
 - 4) 通过数据网络测试仪同时向 3 条 L2VPN 业务发送双向业务流，包长固定，且远低于 MTN 通道带宽，记录 3 条业务的收发包数及时延；
 - 5) 配置 L2VPN 业务 3 优先级高于 L2VPN 业务 1、L2VPN 业务 2；
 - 6) L2VPN 业务 1，L2VPN 业务 2 持续发流，L2VPN 业务 3 发流数据大于 MTN 通道带宽，记录 3 条业务的收发包数及时延。
- d) 预期结果
 - 1) 配置 L2VPN 业务 3 优先级之前，3 条业务收发包正常，无丢包；
 - 2) L2VPN 业务 3 发流数据变化后，L2VPN 业务 2、L2VPN 业务 3 拥塞丢包，L2VPN 业务 1 无丢包，传输网实现 MTN 通道隔离。

6.2.4 5G 核心网 UPF 隔离

- a) 测试目的：验证电力 5G 网络基于电力专用 UPF 实现物理资源隔离。
- b) 测试拓扑：测试组网架构图 2。
- c) 测试步骤：
 - 1) 在核心网网管侧配置电力 5G 终端 1 接入共享 UPF，电力 5G 终端 2 接入电力专用 UPF；
 - 2) 电力 5G 终端 1 发起 UDP 业务，在核心网侧通过 5G 网络信令分析工具抓包查看数据流目的地址走向；
 - 3) 电力 5G 终端 2 发起 UDP 业务，在核心网侧通过 5G 网络信令分析工具抓包查看数据流目的地址走向。
- d) 预期结果：

电力 5G 终端 1 的数据成功转发到共享 UPF，并流向电力系统区域的安全装置；电力 5G 终端 2 的数据成功转发到电力专用 UPF，并流向电力系统区域的安全装置，可基于电力专用 UPF 方式实现物理资源隔离。

6.3 电力 5G 网络核心网网元安全

6.3.1 IPV4/IPv6 访问控制安全

- a) 测试目的：验证通过 IPV4/IPv6 为远程连接用户提供 UPF 访问控制。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 在核心网侧配置 UPF 管理接口同时支持 IPV4、IPV6；
 - 2) 配置远程连接的用户和相应密码；
 - 3) 通过计算机向 UPF 设备管理接口发起 Telnet 连接，进行远程接入。
- d) 预期结果：

通过用户名密码实现远程访问，错误用户名和密码无法接入，实现 UPF 的访问控制。

6.3.2 N3 接口传输的用户数据机密性保护（可选）

基站和电力 UPF 之间的 N3 接口用户数据机密性保护测试与 YD/T 3807-2020 与 4.2.3.2.4 节保持一致。

6.3.3 N4 接口信令数据机密性保护（可选）

SMF 与 UPF 之间的 N4 接口信令数据机密性保护测试与 YD/T 3807-2020 4.2.3.2.4 节保持一致。

6.3.4 电力专用 UPF 对电力 5G 终端的互访控制

- a) 测试目的：验证电力专用 UPF 支持电力 5G 终端之间互访。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 在核心网侧配置网络切片和对应的 DNN，设置 DNN 内用户互访功能；
 - 2) 在 DNN 激活 2 个电力 5G 用户，分别对应电力 5G 终端 1 和电力 5G 终端 2；
 - 3) 电力 5G 终端 1 和电力 5G 终端 2 分别接入网络，进行互访；
 - 4) 电力 5G 终端 1 和电力 5G 终端 2 去附着，关闭 DNN 内用户互访功能；
 - 5) 在 DNN 下激活 2 个电力 5G 用户，分别对应电力 5G 终端 1 和电力 5G 终端 2；
 - 6) 电力 5G 终端 1 和电力 5G 终端 2 分别接入网络，进行互访。
- d) 预期结果
在设置 DNN 用户互访功能情况下电力 5G 终端 1 和电力 5G 终端 2 可实现互访，关闭后无法互访，电力专用 UPF 可实现终端互访控制。

6.3.5 电力 UPF 敏感数据保护

- a) 测试目的：验证电力 5G 网络 UPF 具备敏感数据保护功能；
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 登录 5G 核心网网管界面或导出包含口令的配置文件，查看 UPF 中的用户口令和协议加密口令的存储和显示方式；
 - 2) 查看运行系统中查看/配置/修改/使用各类口令的存储和显示形式；
 - 3) 查看配置文件中的各类口令存储和显示形式。
- d) 预期结果：
UPF 的用户口令和协议加密口令、运行系统中查看/配置/修改/使用各类口令、配置文件中存储的口令均以密文形式存储或不显示，实现 UPF 敏感数据保护功能。

6.3.6 电力 UPF 数据删除

- a) 测试目的：验证电力 UPF 是否具备数据删除功能；
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 登录电力 5G 网络网管系统；
 - 2) 使用授权账户和非授权账户对系统中的日志信息进行删除；
 - 3) 使用授权账户和非授权账户对系统中存储的配置文件进行删除。
- d) 预期结果：
 - 1) 授权账户可以成功删除系统中的日志信息，删除前应支持对删除操作进行确认；
 - 2) 非授权账户无法删除系统中的日志信息；
 - 3) 授权账户可以成功删除系统中存储的配置文件，删除前应支持对删除操作进行确认；
 - 4) 非授权账户无法删除系统中存储的配置文件。

6.3.7 电力 UPF 漏洞扫描

电力5G核心网漏洞扫描测试内容应与GB/T 41266-2022第6.3.1节保持一致。

6.3.8 电力 UPF 攻击防范

电力5G核心网网元攻击防范应包括大流量攻击防范、用户凭证猜解攻击防范、用户连接限制、Web管理功能安全、SSH管理功能安全、SNMP管理功能安全等内容，攻击防范测试应与GB/T 41266-2022中第6.6节相关内容保持一致。

6.4 电力 5G 网络安全区域边界

电力5G网络的安全区域边界应按照DL/T 2613-2023中的第9.1.1.3章节内容进行测试。

7 电力 5G 终端安全测试规范

7.1 电力 5G 终端安全

7.1.1 可信验证

电力 5G 通信终端可信验证测试应与《电力 5G 终端测试规范》第 8.1 节保持一致。

7.1.2 身份鉴别

电力 5G 通信终端身份鉴别测试应与《电力 5G 终端测试规范》第 8.2 节保持一致。

7.1.3 安全存储

电力 5G 通信终端安全存储测试应与《电力 5G 终端测试规范》第 8.3 节保持一致。

7.1.4 访问控制

电力 5G 通信终端访问控制测试应与《电力 5G 终端测试规范》第 8.4 节保持一致。

7.1.5 机卡标识关联

- a) 测试目的：验证电力 5G 终端可获标识及用户卡标识的关联。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 核心网侧配置电力 5G 终端标识，并与用户卡标识关联；
 - 2) 电力 5G 终端发起数据业务；
 - 3) 通过指定接口向电力 5G 终端获取终端标识信息；
 - 4) 通过指定接口向电力 5G 终端获取用户卡标识信息；
 - 5) 修改电力 5G 终端关联配置，使电力 5G 终端标识与用户卡标识不匹配；
 - 6) 重复测试步骤 2-4。
- d) 预期结果：

电力 5G 终端标识与用户卡标识关联正确，数据业务正常；反之电力 5G 终端发出告警提示，电力 5G 终端具备机卡标识关联功能。

7.2 电力 5G 终端接入安全

7.2.1 次认证

- a) 测试目的：验证电力 5G 终端支持基于 EAP 的次认证。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 在核心网侧配置电力 5G 终端的签约数据，包含接入特定 DNN 时需执行次认证的要求；
 - 2) 电力 5G 终端发起新的 PDU 会话申请。
- d) 预期结果：

电力 5G 终端建立 PDU 会话成功，电力 5G 终端支持次认证。

7.2.2 防火墙

电力 5G 通信终端防火墙功能测试应与《电力 5G 终端测试规范》6.6 节保持一致。

7.2.3 安全接入

- a) 测试目的：验证 UDM 能根据签约选择 5G AKA 认证方式。
- b) 测试拓扑：测试组网架构图 1。
- c) 测试步骤：
 - 1) 电力 5G 终端签约 5G AKA 认证选项；
 - 2) 电力 5G 终端使用 SUCI 发起鉴权注册流程；
 - 3) 抓取信令流程，查看 AMF 收到的响应消息。

- d) 预期结果：
AMF收到鉴权成功的信令消息。

7.2.4 eSIM 芯片国密算法支持

支持eSIM芯片的电力5G终端国密算法测试应与《电力5G终端测试规范》7.3节加密算法测试项保持一致。

8 电力 5G 管理平台安全测试要求

电力5G管理平台承载生产控制类业务应按照DL/T 2613-2023第9章第三级测评要求、承载管理信息类业务应用按照DL/T 2613-2023第8章第二级测评要求的基础上，开展以下测试。

8.1 平台自身安全管理

8.1.1 账号管理

- a) 测试目的：验证电力 5G 管理平台账号管理功能。
- a) 测试拓扑：测试组网架构图 4。
- b) 测试步骤：
 - 1) 打开电力 5G 管理平台账号管理界面；
 - 2) 检查界面展示是否正常；
 - 3) 查看在线用户信息；
 - 4) 强制退出/注销部分账号。
- c) 预期结果：
账号管理界面展示正常，查询在线用户信息正常，可对部分账号进行强制退出/注销。

8.1.2 用户认证

- a) 测试目的：验证电力 5G 管理平台用户认证功能。
- b) 测试拓扑：测试组网架构图 4。
- c) 测试步骤：
 - 1) 登录电力 5G 管理平台时输入正确的账号密码；
 - 2) 登录电力 5G 管理平台时输入错误的账号密码。
- d) 预期结果：
账号密码正确可进入平台，账号密码不正确无法登录平台。

8.1.3 权限管理

- a) 测试目的：验证电力 5G 管理平台权限功能是否正常。
- b) 测试拓扑：测试组网架构图 4。
- c) 测试步骤：
 - 1) 打开电力 5G 管理平台权限管理界面；
 - 2) 检查界面展示是否正常；
 - 3) 设置账号访问权限，将账号进行分权分域；
 - 4) 使用不同账号进行登录访问，记录呈现界面和功能。
- d) 预期结果：
不同账号登录后显示的界面功能不同，可执行的操作权限不同，与预设内容一致。

8.1.4 平台访问控制

- a) 测试目的：验证电力 5G 管理平台访问控制功能。
- b) 测试拓扑：测试组网架构图 4。
- c) 测试步骤：
 - 1) 将用户 1 列入白名单、用户 2 列入黑名单；
 - 2) 查询电力 5G 管理平台黑白名单用户列表；

- 3) 使用白名单用户登录平台;
- 4) 使用黑名单用户登录平台。
- d) 预期结果:
黑白名单录入成功, 用户列表正常区分并显示黑白名单, 用户 1 登录成功, 用户 2 登录失败。

8.1.5 日志管理

- a) 测试目的: 验证电力 5G 管理平台登录/操作日志功能。
- b) 测试拓扑: 测试组网架构图 4。
- c) 测试步骤:
 - 1) 打开电力 5G 管理平台日志管理界面;
 - 2) 检查界面展示是否正常;
 - 3) 使用不同账号, 多次登录平台;
 - 4) 在平台进行修改访问权限, SIM 卡激活等。
- d) 预期结果:
登录界面正常, 界面展示正常, 平台可记录账号登录信息, 并正确记录操作信息。

8.2 网络态势感知安全测试

8.2.1 5G 核心网性能监控

- a) 测试目的: 验证网络性能监控中的相关下沉的 5G 核心网网元性能监控功能。
- b) 测试拓扑: 测试组网架构图 4。
- c) 测试步骤:
 - 1) 打开电力 5G 管理平台的网络性能监控界面;
 - 2) 检查界面展示是否正常;
 - 3) 使用多个电力 5G 终端接入待验证的基站和核心网, 进行上下行数据传输业务, 验证相关下沉的核心网网元性能指标;
 - 4) 可通过 FTP 工具下载性能报表。
- d) 预期结果:
界面正常加载, 可按照指标展示性能统计结果, 相关下沉的核心网网元性能指标上报正确, 性能报表统计正确。

8.2.2 5G 基站性能监控

- a) 测试目的: 验证网络性能监控中的相关下沉的核心网网元性能监控功能。
- b) 测试拓扑: 测试组网架构图 4。
- c) 测试步骤:
 - 1) 打开电力 5G 管理平台网络性能监控界面;
 - 2) 检查界面展示是否正常;
 - 3) 使用多个电力 5G 终端接入待验证的基站和核心网, 进行上下行数据传输业务, 验证基站性能指标上报是否正确;
 - 4) 可通过 FTP 工具下载性能报表。
- d) 预期结果:
界面正常加载, 可按照指标展示性能统计结果, 5G 基站性能指标上报正确, 性能报表统计正确。

8.2.3 5G 核心网告警

- a) 测试目的: 验证电力 5G 管理平台对 5G 核心网告警功能的监控。
- b) 测试拓扑: 测试组网架构图 4。
- c) 测试步骤:
 - 1) 打开电力 5G 管理平台告警界面;
 - 2) 检查界面展示是否正常;

- 3) 验证核心网网元告警监控和展示是否正常，如宕机、负荷过高、CPU 负载过高等；
- 4) 可通过 FTP 下载告警统计报表。

d) 预期结果：

正常打开告警界面，告警界面各功能正常，可展示告警上报结果、上报时间、告警级别等信息，核心网告警上报正常，告警统计报表内容正确。

8.2.4 5G 基站告警

a) 测试目的：验证电力 5G 管理平台对 5G 基站告警功能的监控。

b) 测试拓扑：测试组网架构图 4。

c) 测试步骤：

- 1) 打开电力 5G 管理平台告警界面；
- 2) 检查界面展示是否正常；
- 3) 验证基站告警监控和展示是否正常。如：宕机、单板复位、小区异常等；
- 4) 可通过 FTP 下载告警统计报表。

d) 预期结果：

正常打开告警界面，告警界面各功能正常，可展示告警上报结果、上报时间、告警级别等信息，基站告警上报正常，告警统计报表内容正确。

8.2.5 终端网络异常告警

a) 测试目的：验证电力 5G 管理平台支持终端网络异常告警。

b) 测试拓扑：测试组网架构图 4。

c) 测试步骤：

- 1) 打开电力 5G 管理平台告警界面；
- 2) 当电力 5G 网络运行正常时，查看告警信息；
- 3) 当电力 5G 终端无法接入电力 5G 网络时，查看告警信息。

d) 预期结果：

电力5G网络运行正常时无告警信息，电力5G终端无法接入电力5G网络时有告警信息。

8.2.6 链路告警

a) 测试目的：验证电力 5G 管理平台对 5G 链路的告警功能。

b) 测试拓扑：测试组网架构图 4。

c) 测试步骤：

- 1) 打开电力 5G 管理平台告警界面；
- 2) 检查界面展示是否正常；
- 3) 验证网元间链路告警进行监控和展示是否正常，如：设备中断脱网、接口异常；
- 4) 下载告警统计报表。

d) 预期结果：

正常打开告警界面，告警界面各功能正常，可展示告警上报结果、上报时间、告警级别等信息，链路告警上报正常，告警统计报表内容正确。

8.2.7 电力 5G 虚拟专网态势呈现

a) 测试目的：验证电力 5G 管理平台是否具有电力 5G 专网统一态势呈现功能。

b) 测试拓扑：测试组网架构图 4。

c) 测试步骤：

- 1) 查看是否有针对电力 5G 网络的态势感知的功能模块；
- 2) 相关功能模块中是否能呈现 5G 安全相关内容。

d) 预期结果：

可呈现电力5G网络资源监控、性能监控、网元告警等安全内容。

8.3 事件审计管理安全测试

8.3.1 审计事件记录

- a) 测试目的：验证电力 5G 管理平台是否支持详细记录所有事件。
- b) 测试拓扑：测试组网架构图 4。
- c) 测试步骤：
 - 1) 查看电力 5G 管理平台是否记录所有鉴别机制；
 - 2) 查看电力 5G 管理平台是否记录所有资源访问行为，以及对资源的操作；
 - 3) 查看安防设备与电力 5G 管理平台的记录是否完备；
 - 4) 查看电力 5G 管理平台事件记录的信息是否充分，包括但不限于事件发生的事件、类型、身份主体等。
- d) 测试结果：

电力 5G 管理平台记录网络中所有事件，且事件信息完备。

8.3.2 审计事件管理

- a) 测试目的：验证电力 5G 管理平台事件审计记录管理是否符合要求。
- b) 测试拓扑：测试组网架构图 4。
- c) 测试步骤：
 - 1) 查看电力 5G 管理平台是否限制审计记录访问，除具有明确访问权限的管理员外，禁止所有其他用户访问审计记录；
 - 2) 查看电力 5G 管理平台是否禁止审计记录修改，所有用户均没有权限更改审计记录的任何信息；
 - 3) 查看电力 5G 管理平台审计记录的存储事件是否符合要求，审计记录的最低存储事件不少于 6 个月。
- d) 测试结果：

无明确访问权限的用户无法访问电力 5G 管理平台审计记录，所有用户无法修改审计记录信息，审计记录存储时间不少于 6 个月。

8.4 安全应急处置

8.4.1 终端强制下线

- a) 测试目的：验证电力 5G 管理平台终端强制下线功能。
 - b) 测试拓扑：测试组网架构图 4。
 - c) 测试步骤：
 - 1) 打开电力 5G 管理平台终端强制下线界面；
 - 2) 验证界面展示是否正常；
 - 3) 输入某个终端的 IMSI，平台将信息传递给网管或 5G 核心网。
 - d) 预期结果：

界面登录和显示正常，终端可强制下线。
-