ICS 点击此处添加 ICS 号
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 电力虚拟专网环境零信任安全接入及交互技术要求

Zero-trust secure access and interaction specification for 5G electric virtual private network environment

（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。

本文件由浙江省电力学会提出并解释。

本文件起草单位：国网浙江省电力有限公司杭州供电公司、国网浙江省电力有限公司、国网浙江省电力有限公司电力科学研究院、国网浙江省电力有限公司信息通信分公司、国网浙江省电力有限公司经济技术研究院、浙江浙能数字科技有限公司、杭州电子科技大学

本文件要起草人：钱锦、李昂、刘伟浩、王文、韩嘉佳、孙歆、韩荣杰、孙智卿、刘箭、王源涛、杜猛俊、蒋锦霞、向新宇、刘兴业、王剑、吕磅、袁翔、王以良、陈元中、黄佳斌、孙望舒、徐汉麟、徐李冰、张吉、许俊渊。

本标准为首次发布。

5G电力虚拟专网环境零信任安全接入及交互技术要求

1 范围

本文件规定了5G电力虚拟专网环境零信任安全接入与交互的总体架构、访问主体技术要求、接入通道技术要求、安全交互技术要求和支撑系统技术要求。

本文件适用于5G电力虚拟专网环境零信任安全接入与交互设计、开发和选型。

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 29242-2012 信息安全技术 鉴别与授权 安全断言标记语言

GB/T 37032 物联网标识体系总则

QGDW 12098-2021电力物联网术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

边缘物联代理 IoT edge agent

在智慧物联体系中部署于边缘侧的装置或软件模块，利用本地通信网络对(智能）传感器、采集控制终端、表计、监测装置等终端进行统一接入，实现对多种通信方式和协议规约的适配，根据统一边缘计算框架对数据进行边缘处理和标准化建模，并通过安全接入平台发送到物联管理平台或主站系统。

[来源：QGDW 12098-2021，3.3.7]

3.2

终端零信任代理 terminal zero trust agent

代理终端完成零信任处理的软件实体，身份认证和访问控制的策略执行点。物联网中，终端零信任代理和物联网终端可为不同的物理实体，但终端和终端零信任代理之间应有可信通道进行交互。

3.3

安全接入 secure access

提供基于零信任的内网应用资源接入，通过身份认证、权限控制等模块，确保更安全、更隐私地访问业务。

3.4

安全交互 secure access and interaction

基于零信任的内网应用资源安全信息交互的过程。

3.5

访问主体 access subject

能访问客体的主动实体。

[来源：GB/T 29242-2012，3.7]

注：访问主体可以是发起访问的设备、用户、应用等。

3.6

访问客体 access object

被访问的目标资源。

注：访问客体例如服务器、数据库、打印服务、网络等。

3.7

终端 terminal

电力5G终端，包含CPE、FTU、DTU、融合终端等。

3.8

5G 核心网 5G core network

采用第五代移动通信技术，对用户面和控制面分离，采用服务化架构设计，主要由网络功能（NF）组成，采用分布式的功能，根据实际需要部署，新的网络功能加入或撤出，并不影响整体网络的功能。

3.9

切片 Network Slicing

电信运营商从统一电信基础设施分离出的虚拟网络，实现端到端资源隔离，以适配各种类型的业务应用。基于不同技术实现方式，依照资源隔离强度高低网络切片可分为硬切片和软切片两种类型。

3.10

电力专用 UPF User Plane Function

电力系统负责处理数据传输的数据平面功能。

3.11

边缘计算节点 Edge computing node

在靠近用户的网络边缘侧构建的业务平台，提供存储、计算、网络等资源，将部分关键业务应用下沉到接入网络边缘，以减少网络传输和多级转发带来的宽度和时延损耗。边缘节点位置介于用户和云中心之间，相比较传统的云中心，边缘节点更接近用户（数据源）。

3.12

共享运营商 UPF Shared operator User Plane Function

适用于共享运营商的无线网和核心网的用户平面功能，5G核心网系统架构的重要组成部分，主要负责5G核心网中用户平面数据包的路由和转发相关功能。为不同业务UPF部署虚拟防火墙或专用资源块进行访问控制与资源隔离。

3.13

零信任探针 zero trust NET probe

围绕资源访问控制的安全策略、技术与过程中侦听网络数据包的网络探针。

4 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表（Access Control List）
CPE：用户驻地设备（Customer-premises Equipment）
DTU：数据传输单元（Data Transfer unit）
FTU：馈线终端装置（Feeder Terminal Unit）
IP：互联网协议（Internet Protocol）
IPsec：互联网安全协议（Internet Protocol Security）
MAC：媒体访问控制（Media Access Control）
MEC：移动边缘计算（Mobile Edge Computing）
NAT：网络地址转换（Network Address Translation）
NEF：网元功能（Network Element Function）
QoS：服务质量（Quality of Service）
RAN：无线接入网（Radio Access Network）
SSAL：国家电网公司安全应用层协议（State Grid Secure Application Layer）
SSL：安全套接字协议（Secure Sockets Layer）
SMF：业务管理功能（Service Management Function）
TLS：传输层安全（Transport Layer Security）
UPF：用户面功能（User Plane Function）
VPN：虚拟专用网络（Virtual Private Network）

5 总体架构

5.1 5G 电力虚拟专网零信任安全防护架构，主要包括安全接入（包括访问主体和接入通道）和安全交互（包括支撑系统和访问客体）两个部分，架构示意图见图 1。

5.2 接入主体为能访问客体的各类电力 5G 终端，主要形式为：CPE、FTU、DTU、融合终端等。

5.3 接入通道为 5G 电力虚拟专网，实现终端接入通信。

5.4 支撑系统为零信任管理平台，包含零信任安全代理和零信任安全控制中心。零信任安全控制中心应具备对整个访问过程的持续安全监测、信任评估和动态更新访问控制策略等功能，零信任安全代理应具备访问流量的重定向和访问控制策略执行、流量加密等功能。

5.5 访问客体为主体访问的电力信息系统及其资源。

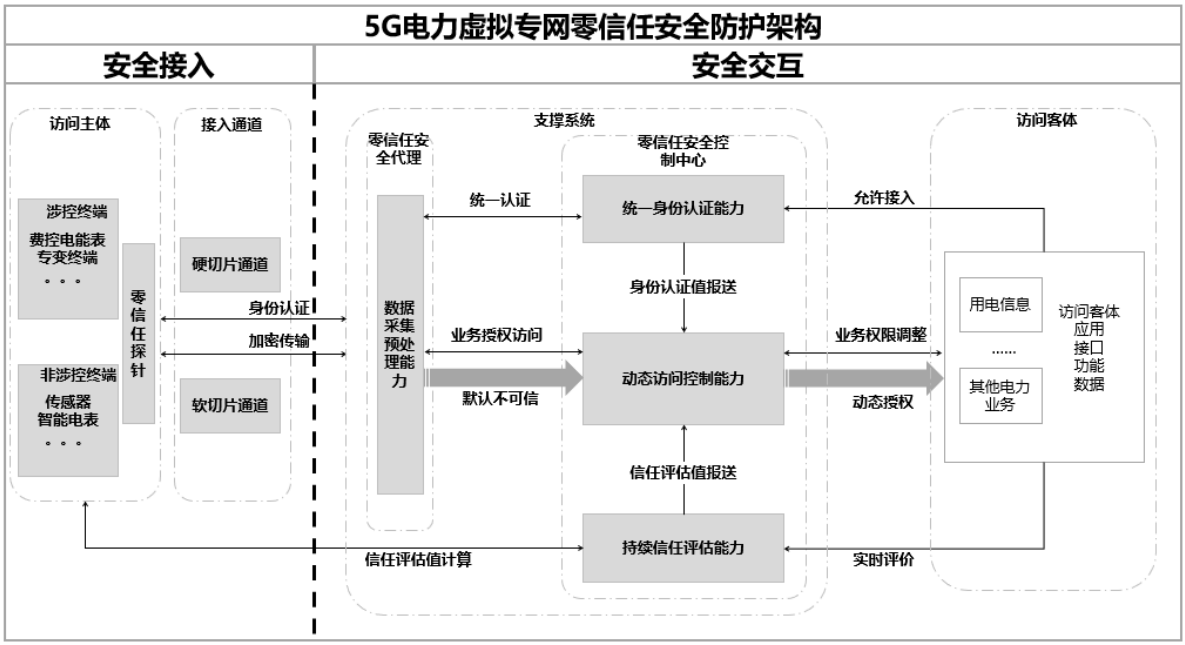

图1 5G 电力虚拟专网零信任安全防护架构

6 访问主体技术要求

6.1 终端要求

6.1.1 身份要求

终端身份满足下列技术要求：

a) 为终端赋予全局唯一性编码，可以内置芯片、内置证书或者设备唯一性标识为基础，编码方式可参照 GB/T 37032 执行；

b) 终端宜能存储终端身份信息，无法存储终端身份信息的终端，终端身份信息应存储在终端零信任代理所在实体上，零信任代理应能够根据终端属性索引终端身份；

c) 处理零信任相关业务的数据包中应携带终端身份信息。

6.1.2 密钥协商

密钥协商认证应满足下列技术要求：

a) 终端数据安全传输、敏感内容加密、数字签名采用国家密码部门认可的加密算法；

b) 终端与接入网关通信采用 SSL/TLS、IPSec、SSAL 等安全协议；

c) 通过密钥协商后方可与应用系统进行连接；

d) 协商完成后，后续数据传输经加密处理。

6.1.3 边界隔离安全要求

边界隔离应满足下列技术要求：

a) 在边界处部署防火墙、ACL 等访问控制机制，配置必需的访问控制策略；
b) 在电力边界处部署网络入侵检测装置，配置并启用入侵检测规则；
c) 在电力边界处部署恶意代码检测装置，启动阻断能力；
d) 电力边界具备流量分析和存储能力，流量存储时间大于 6 个月。

6.1.4 认证与鉴权

接入认证与鉴权应满足下列技术要求：

a) 支持 APN 拨号功能，支持终端注册功能；
b) 支持二次鉴权功能。

6.2 加密传输

6.2.1 终端加密

终端加密应满足下列技术要求：

a) 终端默认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) 终端通信加密应采用硬件密码模块或软件密码模块实现。

6.2.2 数据加密

数据加密技术应满足下列技术要求：

a) 传输内容加密：采用传输层加密保护方式，对传输的数据进行通道加密；
b) 控制指令加密：执行控制操作时，对控制指令进行应用层加密保护。

7 接入通道技术要求

7.1 5G 电力虚拟专网

7.1.1 5G 电力虚拟专网应满足下列技术要求：

a) 防止不可信任的终端接入网络；
b) 采用数字证书等方法设置双向的身份认证机制，提高连接的可靠性和安全性；
c) 终端接入网络时，建立一个加密的传输通道，提高数据的安全性；
d) 提升防护物理硬件，加强集成度，缩减其容易被侵入的物理接口；
e) 5G 核心网采用 IPsec 等保护措施，提高 N2、N4 信令数据及 N3、N6 口用户业务数据的机密性和完整性；
f) 5G 核心网设置不同等级的切片应用，支持不同等级应用切片的访问隔离；
g) 5G 核心网具备切片间虚拟机资源隔离能力，缩减其资源故障影响；
h) 电力专用 UPF 在边界处部署防火墙实现逻辑隔离；
i) 边缘计算节点承载的业务应用，使用虚拟防火墙或 VLAN 方式进行业务访问控制与业务隔离；
j) 为不同业务共享运营商 UPF 部署虚拟防火墙或专用资源块进行访问控制与资源隔离。

7.2 MEC 环境

7.2.1 连接要求

MEC 应具备向上连接 5G 运营商核心网，向下连接终端设备能力，应支持云端算力下沉、终端算力上移。

7.2.2 能力开放要求

能力开放要求包括 MEC 平台能力开放、无线网络能力开放和核心网能力开放，MEC 平台开放应可与 5G 运营商核心网进行能力协同，并应满足下列技术要求：

a) 无线网络能力开放：无线网络（RAN）的接口（API）与 MEC 接口网关（API GW）协同，将用户位置信息、单元（Cell）/用户/承载带宽信息开放给终端设备；
b) 核心网开放：MEC 接口网关向中心 NEF 获取用户计费、QoS、业务控制等策略。用户策略更新后，中心 NEF 将策略下发到 MEC 接口网络上，或由 SMF 下发到 UPF 上；
c) MEC 平台能力开放：编解码转换、IP 安全协议、人工智能等能力，通过开放接口提供给本地终端设备。在边缘节点的 MEC 平台上可以集成不同种类的第三方应用，对不同的 MEC 商业场景，可额外部署防火墙、NAT 等网络功能。

8 安全交互技术要求

8.1 统一身份认证

8.1.1 身份认证应为访问主体与零信任管理平台的交互过程。
8.1.2 终端身份认证技术应满足下列要求：
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，配置并启用结束会话、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) 当进行远程管理时，采取必要措施防止鉴别信息在网络传输过程中被窃听。

8.2 持续信任评估

8.2.1 持续信任评估应为零信任管理平台内部对各类数据的计算处理交互过程。
8.2.2 终端信任评估技术应满足下列要求：
a) 基于终端信任度量开展持续动态信任评估；
b) 以终端设备信息、终端运行数据为基础评估数据；
c) 可根据当前认证方式、风险状态、环境因素等相关信息进行动态信任值调整；
d) 常见的影响信任评估的物理或行为因素包括下列内容：
1) 包括主体（所对应的数字身份）个体行为的基线偏差；
2) 主体与群体的基线偏差、主体环境的攻击行为；
3) 主体环境的风险行为等影响信任的关键要素。
e) 当信任值低于设定阈值应进行报警操作，提示异常行为，并依据信任策略进行进一步操作。

8.3 动态访问控制

8.3.1 动态访问控制应为零信任管理平台与访问客体的交互过程。
8.3.2 动态访问控制能力应基于统一身份认证能力和持续信任评估能力。

8.3.3 访问控制策略

访问控制策略技术应包含：
a) 结合当前身份认证值、信任评估值等数据，生成基于当前环境下的最小访问策略；
b) 访问控制持续接收来自信任评估引擎的评估数据，以会话为基本单元，遵循最小权限原则，对所有的访问请求进行基于上下文属性，信任等级和安全策略的动态权限判定，最终决定是否为访问请求授予资源的访问权限；
c) 动态访问控制，可通过实时信任评估，实现信任值低于设定阈值的危险访问会话自动终止等能力。

8.4 5G 核心网安全交互

8.4.1 5G 核心网安全交互应为零信任管理平台与 5G 核心网的交互过程。
8.4.2 5G 核心网安全交互技术应支持下列内容：
a) 通过获取 UPF 的业务转发数据流，作为零信任管理平台分析数据；

b) 通过能力开放应用，获取 5G 运营商核心网终端注册、认证等控制数据流，作为零信任管理平台分析数据。

9 支撑系统技术要求

9.1 终端零信任探针

9.1.1 探针部署

零信任探针部署应满足下列技术要求：

a) 兼容主流的厂商、设备与芯片，包括：
5G 智能网关、无线 5G CPE、台区智能融合终端、边缘物联代理、5G MEC/UPE、工业路由器等物联终端设备；

a) 支持动态负载调节、心跳监控和可裁剪软件架构；

b) 部署方式多样，支持软件、容器、固件、模组等多形态灵活化部署方式。

9.1.2 数据采集

终端设备可通过内置探针方式采集终端设备信息、终端运行数据，应至少包括下列内容：

a) 终端设备信息：操作系统信息、CPU 信息、内存信息、存储信息、网卡信息；

b) 终端运行数据：端口信息、进程信息、文件信息、软件信息。

9.2 零信任管理平台

9.2.1 安全技术要求

9.2.1.1 零信任安全代理应实时接收零信任安全控制中心发送的策略决定和动态调整策略，应采用动态会话管理。

9.2.1.2 零信任安全代理执行策略决定，包括建立或阻断终端和资源之间的数据访问信道，应满足下列技术要求：

a) 策略管理：零信任安全代理负责建立终端与资源之间的连接，将生成终端用于访问资源的任何身份认证令牌或凭证；

b) 策略引擎：零信任安全控制中心负责收到访问请求后，进行信任评估、策略决定，确定拒绝或授予对被访问资源的访问权限；

c) 策略执行：零信任安全控制中心负责实施动态身份鉴别，启动、监控和终止终端与资源之间的数据访问信道。

9.2.2 终端信任度量

信任度量应满足下列技术要求：

a) 终端信任计算：具备终端信任度量基准，明确终端信任等级，信任度量作为终端接入和业务访问判定条件；终端信任算法使用安全策略和 IP 黑名单、威胁情报等外部源作为输入；

b) 终端信任度量：信任度量算法基于终端属性计算终端信任值，信任度量属性集可包括终端厂商和版本信息、终端可信评估值、终端监测软件评估信息；

c) 信任度量调整：信任度量属性集和信任度量算法根据安全因素和环境形式动态调整。

9.2.3 访问控制策略

访问控制策略技术应满足下列技术要求：

a) 包括身份认证策略和访问控制策略；

b) 包括主体身份、客体身份信息；

c) 管理可采用基于属性的访问控制模型。

9.2.4 访问通道管控

访问通道管控应满足下列技术要求：

a) 访问通道的建立采用先认证再通信的模式；

b) 采用会话管理措施，确保所有流量在访问控制策略许可下传输。