5G电力虚拟专网环境零信任安全接入及交互技术要求

编　制　说　明

目　　次

1 编制背景

新型电力系统建设的背景下，大量“源、荷、储”等领域的新兴业务终端将以多种方式接入电力网络，5G通信在电力行业的试点广泛落地，大量5G+新技术的实际应用在现阶段投入使用。面对不断增加的5G终端接入，安全、时延需求，电力行业将5G与零信任紧密集合，采用以身份为中心的零信任安全防护理念，建立基于持续信任评估和授权的动态访问控制体系，实现数据交互的持续监测和精细化访问控制，适用于电力行业主要业务场景终端的高效、安全可信接入。在电力行业内，5G+零信任作为新兴技术在近几年实现落地示范应用，但相关标准体系还未构建，缺少权威性、规范化、体系化标准指导，不利于电力行业整体推广应用。目前，国内主要执行的标准有GB/T 40594-2021 《电力系统网源协调技术导则》、GB/T 38438-2019 《电力通信网运行评估指标体系》、DL/T 1870-2018 《电力系统网源协调技术规范》、DL/T 1379-2014 《电力调度数据网设备测试规范》等，暂无相关标准，通过标准起草，使电力行业拥有一个统一的5G电力虚拟专网环境零信任安全接入及交互规范标准，保证终端的统一接入流程，保证电力终端在5G虚拟专网下的安全性。

本标准立项编号2022001，本标准的制定将会推进电力行业网络安全中5G+零信任建设的规范化，能够满足电力网络对源网荷储海量资源的敏捷响应需求，有效提高电力网络安全领域的工作效率，进一步加强电力网络安全防御能力，为新型电力系统的建设和平稳有效运营提供安全支撑，为电力行业实现数字化跨越式发展铺平道路。

2 编制主要原则

本标准在制定过程中重复考虑了现有标准的有关技术资料和实践经验。在标准的制定过程中参考了GB/T 40594-2021 《电力系统网源协调技术导则》、GB/T 38438-2019 《电力通信网运行评估指标体系》、DL/T 1870-2018 《电力系统网源协调技术规范》、DL/T 1379-2014 《电力调度数据网设备测试规范》等多个相关的国家、行业、地方标准、团体标准和公开的技术文献与资料信息及检测数据，进行研究分析。

3 与其他标准文件的关系

本标准在制定过程中力求与现行的法律法规和强制性标准相一致的原则，制定的过程中认真的学习了相关的法律、法规、规章、强制性标准等文件和文件精神，参考了相关的技术文献和研究成果，使标准及其说明与相应法律法规和强制性标准之间尽可能得以衔接、协调。

4 主要工作过程

4.1 第一次专家讨论会

2022年12月8日，编制组邀请电力行业和标准化行业专家在线召开了标准编制第一次专家讨论会。根据专家意见，将标准主要技术内容重新梳理，初步明确了标准框架为：总则（设计原则、总体框架、架构组成）、基础技术要求（终端要求、5G电力虚拟专网、MEC环境、零信任基础）、安全接入技术要求（接入终端本体、终端安全接入、MEC环境）、安全交互技术要求（访问控制策略、访问通道管控、终端侧策略执行）。同时，将标准范围明确为：“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”领域。

4.2 标准推进会

2023年03月14日下午14:00-17:00，浙江省电力学会信通专业委员会组织召开了浙江省电力学会标准《5G电力虚拟专网环境零信任安全接入及交互规范》团体标准编制推进会，会议由吴秋晗主持，王志强、洪道鉴、张烨华、苏斌、钱锦、孙嘉赛、张辰等参加了会议。

会议对标准《5G电力虚拟专网环境零信任安全接入及交互规范》的草案内容进行讨论，专家提出如下意见：

（1）进一步明完善标准的术语内容，包括零信任、5G电力虚拟专网等。

（2）需要进一步补充引用内容，尽可能引用更全面。

（3）进一步完善标准架构，参考标准编写要求调整大纲，按照技术规范要求进行编写，应把5G网络架构中设计应切片和软切片，即涉控与非涉控类纳入进来，同时把可能涉及的问题详细描述，并把可选、必选项进行详细描述。

（4）进一步完善标准内容，第二部分交互内容篇幅偏少，需要参照第一部分安全接入部分适当填充内容。

（5）需充分考虑到电力网络接入的情况，补充内容并在图1中有所体现。

（6）需完善补充安全接入的主体、支撑系统（应用）和客体（资源）。

（7）建议将题目修改为《5G电力虚拟专网环境零信任安全接入及交互技术要求》。

4.3 第二次专家讨论会

2023年6月3日，编制组按照第一次专家讨论会意见，完成标准征求意见稿初稿编制工作，在线召开了第二次专家讨论会，专家组对标准进行了广泛而深入的讨论，对上一版本标准结构中的不足进行了调整，按照技术要求的形式重新进行梳理，按照架构组成进行标准章节划分。标准章节重新划分为总体架构、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。

专家讨论会针对标准新的架构进行全文基本完成查漏补缺。按照专家意见进行了技术条款补充，在征求意见初稿上完成了逐字逐句的修改工作。

5 标准结构和内容

5.1 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。

5.2 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。

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

5.3 术语和定义

主要包括：边缘物联代理、终端零信任代理、安全接入、安全交互、访问主体、访问客体 、终端、5G核心网、切片、电力专用UPF 、边缘计算节点 、共享运营商UPF、零信任探针

5.4 缩略语

主要包括：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：边缘计算技术（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（StateGrid 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）

5.5 总体架构

5G电力虚拟专网零信任安全防护架构相关内容，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。

5.6 访问主体技术要求

5.6.1 终端要求

规定终端身份要求、密钥协商要求、边界隔离安全要求、认证与鉴权技术要求。

5.6.2 加密传输

规定终端加密和数据加密技术要求。

5.7 接入通道技术要求

5.7.1 5G电力虚拟专网

规定5G电力虚拟专网相关技术要求。

5.7.2 MEC环境

规定连接要求和能力开放要求。

5.8 安全交互技术要求

规定统一身份认证、持续信任评估、 动态访问控制、访问控制策略和5G核心网安全交互技术要求。

5.9 支撑系统技术要求

5.9.1 终端零信任探针

规定探针部署和数据采集技术要求。

5.9.2 零信任管理平台

规定安全技术要求、终端信任度量、访问控制策略、访问通道管控技术要求。