《虚拟电厂云边协同数据安全与隐私保护技术规范》编制说明（征求意见稿）

一、工作简况

1. 主要工作过程

起草（草案、调研） 阶段：2025 年 3 月，根据中国电工技术学会标准制修订计划，成立标准编写组，讨论确定了标准的主要内容及分工；

2025 年 4 月开始，标准编写组向各单位进行调研分析，收集资料。2025 年 5 月标准编写组根据意见和建议，完成标准初稿，2026 年 6 月-7 月，标准编写组对初稿进行讨论修改后形成标准草案。

2025 年 8 月召开了第一次标准的专家评审会， 对标准草案进行讨论修改，形成了征求意见稿。

2. 主要参加单位和工作组成员及其所做的工作

标准编写组收集了近几年来国内相关虚拟电厂云边协同数据安全与隐私保护技术的相关资料，通过整理分析，确定了标准主要技术内容，主要由国网江苏省电力有限公司宿迁供电分公司牵头完成标准初稿编制，其他参与单位配合编制，并负责收集相关资料、提出建议。

主要参与单位有：国网江苏省电力有限公司宿迁供电分公司、东南大学、双创中心、国网信息通信产业集团有限公司、南京邮电大学、国网江苏省电力有限公司。

二、标准编制原则和主要内容

1. 标准编制原则

本标准按照 GB/T 1.1－2020《标准化工作导则第 1 部分：标准化文件的结构与起草规则》的规定起草，遵循科学性、先进性、经济性，坚持实事求是，以先进的技术和丰富的实践经验为基础，遵守国家有关法律、法规，符合合团体标准要求，目的在于加强虚拟电厂云边协同数据安全与隐私保护技术规范化管理，提高作业效率，提升安全运行水平。

在标准编制过程中，主要依据系统性参照 GB/T 22239-2019、GB/T 35273-2020、GB/T 41373-2022、GB/T 36572-2018、GB/T 20986-2023、IEC 62351、ISO/IEC 27001/27002/27018 等文件，并结合电力行业云边协同与隐私计算工程实践经验。

此外，本标准同时依据并参考查阅了《中国电工技术学会标准化工作管理办法（试行）》（电技学发字［2022］051 号）有关规定。

2. 标准主要内容

本标准主题章分为十章，虚拟电厂云边协同数据安全与隐私保护的覆盖范围、规范性引用文件、术语和定义技术、技术要求、安全要求、试验与检验规则、管理维护。

3. 解决的主要问题

填补技术标准空白　面向虚拟电厂云边协同的数据安全与隐私保护，现阶段国内外缺乏统一的技术规范，导致采集、训练、聚合与验收口径不一。制定本标准可规范系统架构、数据敏感度评估、隐私预算分配、自适应梯度裁剪与通信加密等关键要求，明确性能与合规模块的量化指标，解决工程落地“无据可依”的问题，推动行业有序发展。

支撑政策与市场需求　响应新型电力系统与“数据要素”相关政策，契合源网荷储与园区级负荷聚合的快增需求（如工业园区、公共建筑、充换电与分布式光储场景）。通过标准化的流程与测试方法，可提升项目审批与并网侧评估效率，降低跨厂商对接成本，助力虚拟电厂规模化、低成本、可审计运行。

国际竞争力与贸易壁垒　以标准先行，形成云—边—端一体化的安全与隐私技术话语权，减少因算法、接口与合规差异带来的国际互认障碍与出口限制；同步对齐 IEC/ISO 等框架，提升与国际市场的互操作与可验证性，促进中国企业在联邦学习与隐私计算产业链中的主导地位。

4. 主要技术差异

本标准为新制度标准，无主要技术差异。

三、主要试验（或研制）情况

1 系统与组件（软件/硬件）准备

虚拟电厂云边协同数据安全与隐私保护系统（VPP-CE-DSPP）在试验（或研制）阶段宜完成如下配置并满足对应要求：

a) 云端与边缘组件：服务器端（聚合/授权）、虚拟电厂边缘终端（采集/预处理/本地训练）、加密通信通道与（可选）半可信计算平台的功能应完整，接口与协议与第 5 章保持一致。

b) 安全通信：传输层应采用 TLS/DTLS（符合 IEC 62351），禁用 SHA-1、MD5、RSA-1024 等弱算法；建议采用 AES-256/GCM、SHA-256/SM3 等算法，证书与密钥管理与撤销流程应可追溯。

c) 本地与云端存储：边缘与云端静态数据应加密存储（参考 GB/T 36572、ISO/IEC 27002），密钥分离与轮换机制应明确。

d) 模型与数据对象：数采、特征、梯度/模型参数、日志、审计记录等对象的数据分类分级与敏感度标注应与第 7.1、8.5 一致。

e) 联邦训练栈：应具备 TCN/其他时序模型、本地训练器、梯度裁剪与噪声注入、聚合器（如 FedAvg）等模块；差分隐私库应支持 ε 、δ 、σ 参数化与账本化统计。

f) 接口适配：SCADA/EMS/AMI/IoT 数据接入宜通过统一 API 适配层，格式与编码与第 5.2.2 及行业规约一致。

2 试验前准备与安全措施

a) 试验方案与应急预案：试验前应形成试验方案、风险评估与应急预案，覆盖通信中断、异常告警、密钥失效、预算透支、模型异常收敛等情形，配备必要的应急工单与回退策略。

b) 参数基线核查：核查系统规格、访问控制策略、证书有效性、加密套件清单、边云时钟同步、DP 参数、梯度裁剪阈值 θ 与平滑系数 α 、通信轮次与采样率等。

c） 能量与数据状态：除另有规定外，边缘节点本地缓存与训练样本集宜处于可复现的“基线快照”状态；DP 预算账户应清零或重置至计划值。

d） 试验环境：应在具备网络/电源/机房安全与访问审计能力的条件下进行；测试/准生产隔离，禁止与生产密钥、生产个人信息混用。

e） 人员权限：试验人员应具备数据安全、网络安全与电力业务知识，具备相应的系统访问授权与最小权限；变更与操作应留痕。

3 仪器、工具与平台校准

a） 计量与校验：抓包器、流量计、时间同步/时延测试工具、性能基准工具（如 iPerf3）、日志与链路监控平台应在有效校验周期内；时间源应统一。

b） 安全基线：测试主机与探针应通过基线核查与恶意软件扫描；测试账户、API Token、证书应专用管理并可追溯。

四、标准中涉及专利的情况”

本标准不涉及专利问题。

五、“预期达到的社会效益、对产业发展的作用等情况”

云—边—端协同与联邦学习（FL）、差分隐私（DP）、TLS/DTLS 等关键技术已工程化，在电力负荷预测、配电自动化、充换电与园区级能管平台等领域具有可复制的商业应用；边缘侧数据采集/预处理、模型本地训练与云端聚合的流程在配用电、充电站、楼宇群控等场景已有示范；电力通信安全（参照 IEC 62351）、等保与个人信息保护框架可无缝迁移至本标准；在模型侧，自适应梯度裁剪+DP 噪声的组合策略已在多源非 IID 场景验证有效，工具链与算子库成熟，易于集成。

边缘节点采用模块化设计，就地完成特征处理与增量训练，支持远程参数下发、可观测性与告警联动；与既有 SCADA/EMS/AMI 系统通过统一 API 对接，减少现场改造。边端设备具备本地加密存储与密钥托管能力，结合“授权解密+最小权限”机制控制模型使用边界；标准化的日志/审计留存与预算账本降低日常维护复杂度，便于 AI 智能巡检与自动化运维。

虚拟电厂通过本地训练与分层聚合，减少原始数据出域与回传带宽，降低通信与中心算力开销；云边协同减少重复 AC/DC“数据往返”的系统性损耗，在满足指标（端到端时延、通信轮次、聚合时长）的前提下，整体效率显著提升。统一的数据敏感度评估与隐私预算分配规则，避免“过噪”或“泄露”两难，在隐私—精度—成本之间形成可量化的最优点；项目级经济性模型可复用既有能管平台与边缘算力，缩短改造周期、降低集成成本。

面向高密度城市园区、公共建筑群、充电站与分布式光储等场景，标准化的云边流程减少中心侧扩容与链路拥塞风险；弱网/丢包条件下的鲁棒性测试与 KPI 门槛保障业务连续性，适合地上空间紧张、边缘节点多点分布的应用形态；统一的合规模块与接口基线有利于多厂商互联互通与规模化复制。

国内“新型电力系统”“数据要素安全流通”与“新型储能”相关政策鼓励数据安全可用、隐私合规流通与关键核心技术标准化；本标准与 GB/T 等保 2.0、个人信息保护规范、数据分类分级指南对齐，加速项目审批与并网评估。国际层面，参照 IEC/ISO 信息安全与电力通信安全框架，呼应欧盟、北美对数据与模型使用的合规要求，前瞻对接国际互认趋势，减少技术差异带来的贸易壁垒，提升我国在联邦学习与隐私计算+虚拟电厂领域的话语权与出口竞争力。

六、“与国际、国外对比情况”

本标准在通信与数据安全、管理体系与隐私合规方面与国际主流框架保持一致（IEC 62351、ISO/IEC 27001/27002/27018、GDPR 等），可无缝对接大多数跨国项目的合规审查。面向虚拟电厂（VPP）的“敏感度评估—隐私预算分配—自适应梯度裁剪—云边协同 KPI”成体系量化要求，在国际现有标准中尚属空白或仅有原则性指导，具有工程化与可验证优势。国外规范多对隐私增强技术（PETs）给出原则性要求，但缺少联邦学习（FL）在电力场景的端到端量化门槛；本标准提供可测 KPI 与验收程序。通过协议/算法白名单与弱算法禁用清单、日志与审计留存周期要求，可与海外常见实践互认；少量参数口径（如 ε 的项目级上限）需在跨境实施时映射与换算。

七、在标准体系中的位置，与现行相关法律、法规、规章及相关标准，特别是强制性标准的协调性

本标准与现行相关法律、法规、规章及相关标准保持一致。

八、重大分歧意见的处理经过和依据

标准编制过程中广泛征集了专家意见，所有意见均按照标准编制程序进行了是否采纳，不存在重大分歧意见。

九、标准性质的建议说明

建议本团体标准的性质为推荐性团体标准。

十、贯彻标准的要求和措施建议

（1）规定相关从事虚拟电厂云边协同数据安全与隐私保护技术规范作业人员或团体，按照此标准相关要求开展作业。

（2）中国电工学会牵头推广《虚拟电厂云边协同数据安全与隐私保护技术规范》，组织企业、单位进行试点应用。

十一、废止现行相关标准的建议

无。

十二、其他应予说明的事项

无。