ICS 27.010
CCS F10

T/GDEA

团　　体　　标　　准

T/GDEA 020—20xx

综合能源平台建设技术规范

Technical specification for integrated energy platform

（征求意见稿）

（本草案完成时间：2026-06-11）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

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专利的责任。

本文件由中国能源建设集团广东省电力设计院有限公司提出。

本文件由广东省能源协会归口。

本文件起草单位：

本文件主要起草人：

本文件在执行过程中的意见或建议反馈至广东省能源协会。

相关意见反馈联系方式：广东省能源协会标准化日常管理办公室（电子邮箱：gdpeima@163.com；电话：020－83275211）。

综合能源平台建设技术规范

1 范围

本文件规定了综合能源平台建设的总体要求、总体架构、功能要求、运营管理、数据接口要求、安全性要求和运行维护要求，描述了对应的证实方法。

本文件适用于综合能源平台的建设和运行维护。

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 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 36572—2018 电力监控系统网络安全防护导则

GB/T 40684—2021 物联网 信息共享和交换平台通用要求

DL/T 890.301—2016 能量管理系统应用程序接口（EMS-API） 第301部分：公共信息模型（CIM）基础

DL/T 890.401—2006 能量管理系统应用程序接口（EMS-API） 第401部分：组件接口规范（CIS）基础

3 术语和定义

下列术语和定义适用于本文件。

3.1

综合能源系统 integrated energy system；IES

采用两种及两种以上能源，为用户同时提供能源供应，或在不同能源间实现互动、协调，使得在一定区域范围内的能源供应、存储、利用达到较高的自平衡和自给率，是能源互联网在用户侧的典型形态。

注：一个涉及多种能源的复杂系统，它包括能源的生产、存储、转换、分配和使用等多个环节。

3.2

综合能源平台 digital energy system

采用智能化、自动化、信息化等先进技术，对区域综合能源系统的分布式产能、用能预测、购入存储、加工转换、输送分配、调度运行、交互协同、终端使用和能源计量器具等实施集中动态监控和智慧化管理的系统。

注：综合能源平台是综合能源系统的重要组成部分，负责综合能源系统的数字化支撑。

3.3

需求侧响应 demand response；DR

用户根据实时电价、相关激励措施,主动做出调整用电需求的反应。

3.4

分布式能源 distributed energy resources

建设在用户侧的能源供应类型，可独立运行，也可并网运行，以资源和环境效益最大化为原则，确定其方式和容量，将用户多种能源需求以及资源配置状况进行系统整合优化，并采用需求应对式设计和模块化配置的新型能源系统。

3.5

微服务 microservice；MS

一种将单一应用程序构建为一系列小型、自治、松耦合服务的架构模式，各服务可独立开发、部署、扩展，通过轻量级机制通信。

[来源：GB/T 42568—2023，3.1.3，有修改]

4 缩略语

下列缩略语适用于本文件。

CIM：公共信息模型（Common Information Model）

CIS：组件接口规范（Component Interface Specification）

GIS:地理信息系统（Geographic Information System）

4A：账号、认证、授权和审计（Account, Authentication, Authorization, Audit）

CMDB：配置管理数据库（Configuration Management Database）

RTO：恢复时间目标（Recovery Time Objective）

RPO：恢复点目标（Recovery Point Objective）

MTTR：平均修复时间（Mean Time To Repair）

5 总体要求

5.1 综合能源平台应按照分层的结构化设计思路，采用微服务架构技术路线，结合云计算、大数据、物联网、移动通讯、人工智能等技术，支持平台能力的弹性扩展和应用功能的松耦合配置以及二次开发能力。

5.2 综合能源平台应遵循 DL/T 890.301 和 DL/T 890.401 的相关规定，基于 CIM 和 CIS 实现异构系统间的信息集成与共享。

5.3 综合能源平台应能够支撑综合能源系统运行，整合和管理不同类型的能源资源，包括可再生能源和传统能源。支持多种能源设备和系统的接入，如太阳能光伏、风力发电、燃气轮机、储能设备和能源管理系统等。

5.4 综合能源平台用户终端界面设计应采用中文为主的交互界面，直观易用、交互方便，界面文字清晰、简洁，易懂易学，便于管理和维护。

5.5 综合能源平台应建立信息安全保障体系，涉及电力监控运营者的平台其信息安全防护要求应符合 GB/T 22239、GB/T 25070 和 GB/T 36572 的相关规定。

5.6 综合能源平台应建立完善的运行维护保障机制，配备专门的常态化运行维护队伍，保障平台的稳定运行。按照数据和应用重要性，建立适配的容灾机制。

6 总体架构

6.1 设计原则

6.1.1 整体优化与高效利用：统筹能源流，实现多能源形式的高效转换与协同利用。

6.1.2 模块架构与弹性扩展：采用模块化设计，支持灵活调整和未来升级。

6.1.3 智能控制与数据驱动：集成智能化控制与大数据分析，优化能源管理及需求预测。

6.1.4 用户协同与兼容互联：鼓励用户互动，确保系统与现有设备及网络的兼容互操作。

6.1.5 可靠运行与安全防护：构建高可靠性架构，保障系统稳定并抵御外部威胁。

6.1.6 三层结构化架构设计：平台应按照应用层、信息层和物理层，分层建设。

6.2 体系结构

6.2.1 综合能源平台典型架构

综合能源平台典型架构应包含应用层、信息层、物理层，综合能源平台典型架构图如图 1 所示。

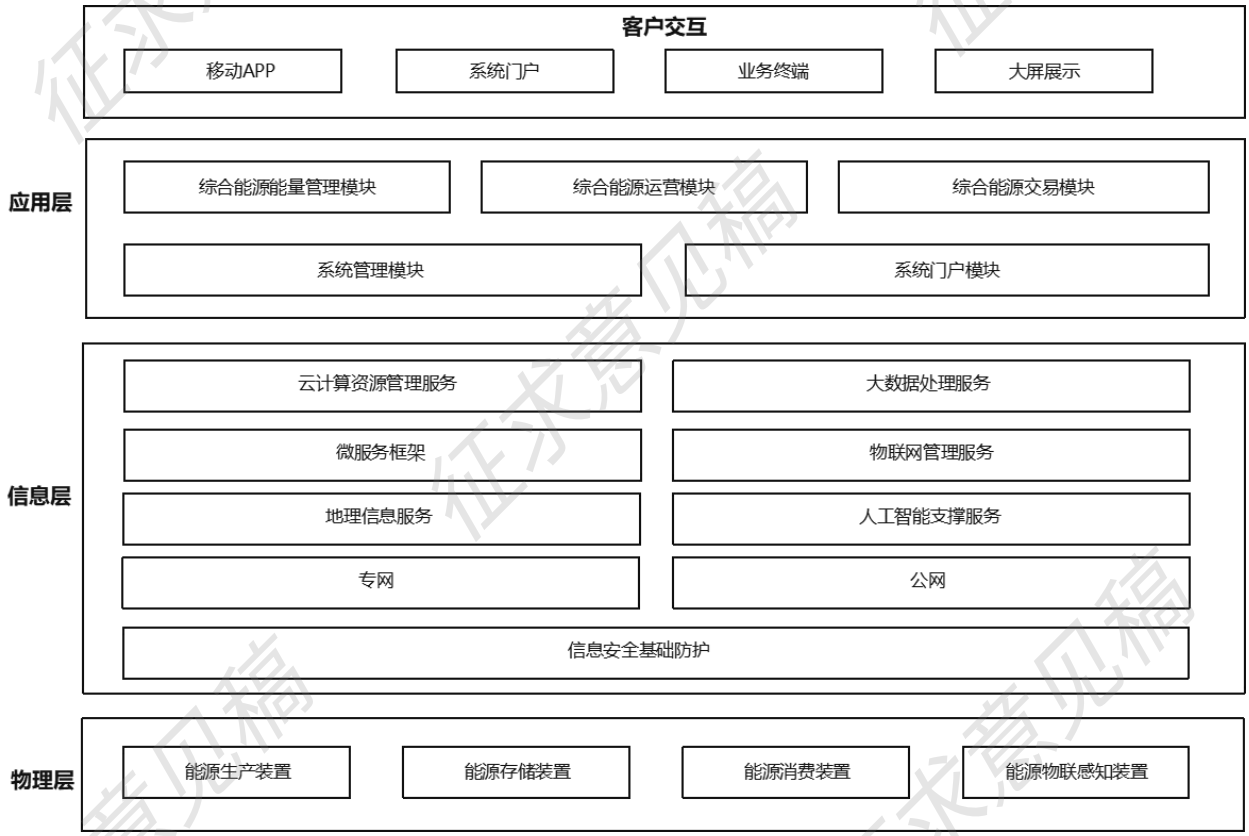

图 1 综合能源平台典型架构图

6.2.2 应用层

面向电网、政府、供能企业、用户、售电等多方主体，提供综合能源运营、综合能源交易、综合能源能量管理、系统管理、系统门户服务等应用服务，实现综合能源系统的数字化管理与运营。

6.2.3 信息层

为平台提供信息化必要的计算能力、智能算力、数据存储、网络与安全资源支撑，具备云计算资源管理、大数据处理、地理信息服务、微服务框架、人工智能支撑和物联网管理等能力，实现与物理层设备设施交互和与应用层信息化基础服务支撑。

6.2.4 物理层

由分布式能源生产装置、能量储存装置、能源消费装置和能源物联感知装置为主构成的冷、热、水、电、气等综合能源运行体系，实现综合能源的生产、存储和消费，具备综合能源系统物联监控能力，能与新型电力系统实现交互协同。

7 功能要求

7.1 物理层要求

7.1.1 综合能源系统物理设备自身应具备运行数据采集能力和物联网通信能力，运行数据应能上送到信息层。若不具备物联感知能力设备，应通过改造或加装等方式实现物联感知能力。

7.1.2 能源物联感知设备应符合信息层物联管理服务的接入和管理要求。

7.1.3 综合能源系统中开断设备和可调设备，在满足信息安全防护要求的基础上，支撑调度控制系统或智能边缘网关调控，具备与信息层和应用层的互操作能力。

7.2 信息层要求

7.2.1 信息层应具备与物理层设备的信息连接通道，信息通讯要求应符合国家电力监控系统网络安全防护导则相关要求，宜建设专网和公网接入区域，实现多样化的综合能源系统物理设备接入，设备接入量不低于 1 万台，信息层内通信通道带宽不低于 100MB。

7.2.2 信息层应提供云计算资源算力供给，实现云计算资源的弹性管理和维护。

7.2.3 信息层应提供信息安全基础防护能力，支撑平台达到信息安全等级保护二级及以上防护能力。

7.2.4 信息层应提供微服务框架和服务容器，支撑应用层功能运行。

7.2.5 信息层应提供物联网管理服务，服务能力应符合 GB/T 40684—2021 要求。

7.2.6 信息层应提供大数据处理能力，实现数据资源管理、大数据统计分析等服务，支撑秒级数据的接入与处理。

7.2.7 信息层应提供 GIS 服务，支撑综合能源系统的设备设施管理，实现物理设备空间位置管理与综合能源系统的能源拓扑网络管理。

7.2.8 信息层宜提供人工智能支撑服务，提供通用智能计算算力服务、计算机视觉服务、自然语言处理服务、语音与多模态服务、通用决策与预测算法服务等。

7.3 应用层要求

7.3.1 基本要求

应依据综合能源管理业务需求，建设相适应业务应用模块，包括综合能源能量管理模块、综合能源运营模块、综合能源交易模块、系统管理模块、系统门户模块。

7.3.2 综合能源能量管理模块

平台建设综合能源能量管理模块，支持设备台账管理、综合能源调度与控制和虚拟电厂管理服务，应满足以下要求：

a) 应具备综合能源系统设备功能位置管理、设备资产管理和综合能源拓扑网络管理等功能，设备模型应满足 CIM 建模要求；

b) 支持综合能源设备通过调度系统或设备直连两种形式的遥测、遥调和遥控；

c) 支持综合能源设备运行方式与运行计划的制定和执行，实现综合能源日前计划编制与执行，支撑日间 96 点的调度指令编排与执行；
d) 支持综合能源设备日内滚动，滚动窗口应支持每 15 分钟一次启动，支撑综合能源日前计划的调整与优化；
e) 支持管理区域内综合能源的资源聚合、负荷调整、需求侧响应全过程记录、响应收益计算等功能，支撑虚拟电厂运行；
f) 宜基于大数据和人工智能技术，分析综合能源系统多种能源运行曲线，在确保园区正常用能前提条件下，拟合多种能源协同优化运行曲线，探索多种能源协同运行最优。

7.3.3 综合能源运营模块

平台建设综合能源运营模块，支持综合能源设备运维和综合能源客户管理服务，应满足以下要求：
a) 应具备综合能源系统设备运维组织管理，实现班组、人员管理；
b) 支持综合能源运维服务计划编排和执行管理，实现巡视路径、巡视记录、维护记录和设备预试定检周期管理等；
c) 支持综合能源系统设备运维工单管理，以工单形式实现运维服务中各类工作的闭环管理；
d) 支持综合能源客户档案管理，实现客户档案信息、计量点信息和合同信息的基础管理；
e) 支持综合能源客户用能监测管理，支持用户 96 点综合能源能量运行负荷曲线与能源用量自动抄表服务；
f) 支持综合能源客户用费用管理，支持用户分日的用能费用统计管理，日费用统计出数时间应在五个工作日内；
g) 应支持综合能源用户用能故障的报障管理服务，实现用能故障闭环管理；
h) 宜基于大数据和人工智能技术，自动分析客户综合能源系统历史运行工况，实现客户综合能源系统节能优化的智能诊断，提供初步的节能优化节点和运行策略建议。

7.3.4 综合能源交易模块

平台建设综合能源交易模块，支持园区参与电力交易市场，实现园区电力市场交易申报、挂牌、交易和结算等服务，应满足以下要求：
a) 应具备电力交易市场中责任主体的能源运行特征分析服务；
b) 应具备电力交易市场历史交易信息查询服务，包括自身历史交易信息和市场交易信息查询服务；
c) 应具备按照本地区电力交易市场交易产品实现自身交易产品管理服务；
d) 应具备电力交易市场交易产品的数据汇聚与分析服务；
e) 宜基于大数据和人工智能技术，具备获取电力交易市场中需求响应邀约信息，并根据自身运行特征自动拟合需求响应策略的服务。

7.3.5 系统门户模块

平台建设系统门户模块，为用户提供综合能源平台各功能模块的访问入口，应满足以下要求：
a) 支持平台运维人员向全体用户或指定用户发布综合能源系统相关信息；
b) 支持平台用户在门户中获取进入不同功能模块的访问入口；
c) 支持平台用户在门户网站上向客服人员咨询问题或信息，实现平台运营、运维人员与用户的友好互动。

7.3.6 系统管理模块

平台建设系统管理模块，为用户提供综合能源平台系统管理服务，应满足以下要求：

a) 支持日志管理，自动生成用户操作系统、系统报错信息和数据接口信息等，提供时间查询和分类统计服务，具备信息筛选功能；

b) 支持用户在平台申请、注销用户账号，后台运维管理人员对用户进行分组管理，与身份认证和权限管理集成，实现功能模块级别的权限用户和用户组分配管理；

c) 平台应具备 4A 统一安全管理能力，实现账号、认证、授权和审计的统一管理，支持功能模块级别的权限控制。

8 信息安全保障

8.1 平台作为支撑能源系统运行的关键信息化基础设施，应建立覆盖“安全策略、安全管理、安全技术、安全运维”四位一体的信息安全保障体系。

8.2 信息安全工作应贯穿平台规划、设计、建设、运行、维护和废弃全生命周期，实行“谁主管谁负责、谁运营谁负责”的责任制。

8.3 平台信息安全防护应遵循“安全分区、网络专用、横向隔离、纵向认证”的总体原则，满足国家网络安全等级保护制度要求。

8.4 应对平台数据进行分类分级管理。

8.5 平台应用系统开发应遵循安全编码规范，防范常见 Web 安全漏洞。

8.6 应建立安全漏洞管理机制，定期开展漏洞扫描、风险评估和补丁更新。对于高危漏洞，应在发现后 72 小时内完成修复或采取临时缓解措施。

8.7 应每年至少开展一次全面的信息安全风险评估，形成风险清单，制定整改计划并跟踪闭环。

8.8 应定期组织运维人员、开发人员和管理人员开展信息安全培训，内容包括网络安全政策、典型攻击手段、应急处置流程等，提升全员安全意识。

8.9 外部系统接入平台应遵循“先评估、再接入、后监控”的原则，接入前需通过安全评估，签署安全责任协议。

9 平台运维要求

9.1 基本要求

9.1.1 平台应建立覆盖运维人员、运维管理过程、运维技术手段和运维资源配置的全生命周期运维体系，保障平台正常运行。

9.1.2 运维体系应支持平台的日常监控、故障响应、性能优化、版本升级和应急处置等关键活动，并具备持续改进能力。

9.1.3 运维工作应遵循“预防为主、快速响应、闭环管理”的原则，建立健全运维管理制度和技术规程，明确职责分工，落实责任到人。运维活动应全过程留痕，支持审计追溯。

9.2 运维人员要求

9.2.1 应配备专职运维团队，团队成员应具备信息技术、能源系统、网络安全等相关专业知识，熟悉综合能源平台架构、业务流程及关键技术组件。

9.2.2 运维人员应经过岗前培训并定期开展技能复训，掌握平台运行维护规程、应急预案操作流程及

常见故障处理方法。

9.2.3 运维团队应设置岗位职责分工，包括但不限于系统管理员、数据库管理员、网络管理员、安全管理员、应用运维工程师和客服支持人员，关键岗位应实行主备双人岗值守。

9.2.4 运维人员应严格执行访问控制策略，禁止越权操作，所有操作行为应纳入 4A（账号、认证、授权、审计）统一管理体系，实现操作可追溯。

9.3 运维管理过程要求

9.3.1 事件管理

应建立事件管理制度，对平台运行过程中发生的异常告警、系统故障、服务中断等事件进行及时发现、记录、分类、处理和关闭，事件响应时间应按照实际业务需求分级管理。

9.3.2 问题管理

应对重复发生或根本原因复杂的事件开展问题根因分析，制定并实施长期解决方案，防止同类问题再次发生。问题处理过程应形成知识库条目，用于后续运维支持。

9.3.3 变更管理

所有涉及平台软硬件配置、系统参数、网络结构、安全策略的变更操作均应纳入变更管理流程。变更前应进行影响评估、风险分析和审批，变更后应进行验证和回滚预案准备。重大变更应在非业务高峰时段执行，并提前公告。

9.3.4 配置管理

应建立配置管理数据库（CMDB），记录平台所有软硬件资产、服务组件及其相互关系。配置项信息应动态更新，确保与实际环境一致，支持变更影响分析和故障定位。

9.3.5 发布管理

平台功能升级、补丁更新、版本发布应制定发布计划，经过测试验证后方可上线。发布过程应支持灰度发布、滚动升级等机制，降低对业务的影响。

9.3.6 服务请求管理

应建立用户服务请求受理机制，支持用户通过系统门户提交咨询、报障、权限申请等服务请求，实现工单化闭环管理，自用户提交请求之时起，服务响应时间应不超过 24 小时。

9.4 运维技术要求

9.4.1 监控与告警

监控与告警应满足以下要求：

a) 应实现对服务器、网络设备、数据库、中间件、微服务组件、应用性能和安全状态的实时监控。监控指标应包括 CPU 使用率、内存占用、磁盘 I/O、网络流量、服务可用性、接口响应时间等；

b) 应支持多级阈值告警机制，通过短信、邮件、企业微信等方式通知相关人员。告警信息应具备去重、收敛、优先级排序功能，避免告警风暴。

9.4.2 日志管理

日志管理应满足以下要求：

a) 应集中采集系统日志、应用日志、安全日志和操作审计日志，日志保存时间不少于 180 天，涉及安全事件的日志应永久保留或按监管要求存档；

b) 日志内容应支持关键字检索、时间范围查询和可视化分析。

9.4.3 备份与恢复

备份与恢复应满足以下要求：

a) 应制定数据备份策略，关键业务数据每日增量备份、每周全量备份，备份数据异地存放；

b) 数据库、配置文件、应用代码等核心资产应具备快速恢复能力，恢复时间目标（RTO）不超过 24 小时，数据丢失量目标（RPO）不超过 120 分钟。

9.4.4 容灾与高可用

容灾与高可用应满足以下要求：

a) 平台关键业务系统应部署在高可用架构下，支持负载均衡、故障自动切换和集群容错；

b) 平台宜建设同城双活或异地灾备中心，定期开展容灾演练，确保灾难发生时能快速接管业务。

9.4.5 性能优化

应定期开展系统性能评估，识别性能瓶颈，优化数据库查询、缓存机制、接口响应和资源调度策略，保障平台在高并发场景下的稳定运行。

9.5 运维资源要求

9.5.1 硬件资源

应配备满足平台运行需求的服务器、存储设备、网络设备和安全设备，并预留不少于 20%的冗余资源，支持弹性扩容。

9.5.2 软件资源

应配备满足平台运行需求的运维软件，定期更新补丁。

9.5.3 第三方服务支持

对于依赖的云服务、通信链路、安全测评等第三方服务，应签订服务水平协议（SLA），明确服务范围、响应时间、故障赔偿等条款，并定期评估服务质量。

9.6 运维文档管理

9.6.1 应建立完整的运维文档体系，包括但不限于：

——系统架构图与部署拓扑图；

——网络配置手册；

——数据库设计文档；

——接口说明文档；

——运维操作手册；

——应急预案与演练记录；

——变更日志与发布记录；

——安全策略配置文档。

9.6.2 所有运维文档应统一归档管理，版本可控，更新及时，便于查阅和审计。电子文档应存储在受控的文档管理系统中，纸质文档应妥善保管。

9.7 应急管理与演练

9.7.1 应制定平台运行应急预案，涵盖电力中断、网络攻击、数据泄露、硬件故障、自然灾害等典型场景，明确应急组织、处置流程、通信机制和资源调配方案。

9.7.2 应每年至少开展一次综合性应急演练，每半年至少开展一次专项应急演练（如网络安全攻防演练、数据恢复演练），演练后应形成总结报告，提出改进建议并落实整改。

9.8 运维评估与持续改进

9.8.1 应建立运维绩效评估机制，定期对平台可用性、故障率、平均修复时间（MTTR）、用户满意度等指标进行统计分析，形成运维分析报告。

9.8.2 应结合评估结果、用户反馈和技术发展，持续优化运维流程、提升自动化水平。