ICS 35.240.01
CCS L 70

T/CS

团 体 标 准

T/CS 546—2026

智慧园区一体化数字底座技术标准

Technical standard for integrated digital infrastructure of smart parks

2026－08－26 发布 2026－08－26 实施

中国商品学会 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　总体要求 2
4.1　基本原则 2
4.2　系统功能 2
4.3　统一编码 2
4.4　数据共享 2
4.5　安全可靠 3
4.6　国产化适配 3
5　数字孪生底座 3
5.1　一般要求 3
5.2　模型接入 3
5.3　空间层级管理 3
5.4　模型轻量化 4
5.5　二三维融合展示 4
5.6　数字空间映射 4
5.7　模型更新 4
6　物联感知 4
6.1　一般要求 4
6.2　协议兼容 4
6.3　设备管理 5
6.4　边缘网关 5
6.5　实时采集 5
6.6　云边协同 5
7　数据治理 5
7.1　一般要求 5
7.2　数据采集 6
7.3　数据标准 6
7.4　数据治理 6
7.5　数据存储 6
7.6　数据服务 6
8　AI 智能引擎 7
8.1　一般要求 7
8.2　AI 能力建设 7
8.3　智能应用 7

9 融合应用门户 8
9.1 开放兼容要求 8
9.2 可扩展性要求 8
10 能碳管理 8
10.1 能耗与碳排放监测 8
10.2 能碳分析与核算 8
10.3 能碳分析与优化 8
11 信息安全 8
11.1 系统安全 8
11.2 数据安全 9
11.3 权限管理 9
11.4 日志管理 9
12 运行维护 9
12.1 运维体系 9
12.2 日常运维 9
12.3 应急与容灾 9
13 验收与评价 10
13.1 测试要求 10
13.2 项目验收 10
13.3 运行评价 10
附录A（资料性）性能测试方法与判定准则 12
参考文献 13

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。

本文件由浙江华聪建筑数字科技有限公司提出。

本文件由中国商品学会归口。

本文件起草单位：浙江华聪建筑数字科技有限公司、宁波市房屋建筑设计研究院有限公司、宁波华聪建筑节能科技有限公司。

本文件主要起草人：李志磊、戚文杰、鲍科峰、陈军、胡迪、周仲浩、高伟杰、马孝长、俞韵、尹金戈、高家绪、胡莹坚、应小勇、高杰、曾宝玺、徐迪、励婷、俞涵、胡小兵。

智慧园区一体化数字底座技术标准

1 范围

本文件规定了智慧园区一体化数字底座的总体要求、数字孪生底座、物联感知、数据治理、AI智能引擎、融合应用门户、能碳管理、信息安全、运行维护、验收与评价。

本文件适用于新建、改建和扩建智慧园区一体化数字底座的设计、建设、验收和运行维护。居住社区可参照使用。

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 20988 网络安全技术 信息系统灾难恢复规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 36073 数据管理能力成熟度评估模型

GB/T 36625（所有部分） 智慧城市 数据融合

GB/T 51366 建筑碳排放计算标准

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧园区 smart park

以信息技术为支撑，通过感知、分析、整合园区运行核心系统的各项关键信息，对园区安防、通行、能耗、环境、资产等各类需求做出智能响应，实现园区管理与服务智慧化的新型园区形态。

3.2

一体化数字底座 integrated digital infrastructure

以数字孪生技术为核心，融合物联网、人工智能、大数据等技术，为智慧园区提供空间数据基础设施、设备接入管理、数据融合治理、智能分析决策等基础能力的综合技术平台。

3.3

数字孪生 digital twin

通过数字化方式创建物理实体的虚拟模型，借助数据模拟物理实体在现实环境中的行为，实现物理世界与信息世界的双向映射与实时交互。

3.4

建筑信息模型 building information modeling

在建设工程及设施全生命周期内，对其物理和功能特性进行数字化表达，并依此设计、施工、运营的过程和结果的总称。简称BIM。

3.5

轻量化处理 lightweight processing

通过几何简化、材质压缩、实例化、LOD分级等技术手段，降低三维模型的几何面数和纹理大小，提升模型在Web端和移动端加载与渲染效率的技术方法。

3.6

数据治理 data governance

对数据进行标准化、质量管理、元数据管理、血缘追踪等过程，确保数据的可用性、一致性和安全性的管理体系。

3.7

能碳管理 energy and carbon management

对园区内能耗数据进行采集、监测、统计分析，并对碳排放量进行核算、报告与优化控制的管理体系。

4 总体要求

4.1 基本原则

智慧园区一体化数字底座建设应遵循下列基本原则：

a) 一体化原则：统一空间基准、统一数据标准、统一身份认证、统一服务入口，实现园区全域信息的集成与协同；
b) 数据驱动原则：以数据融合和分析为核心驱动力，实现园区从经验管理向数据驱动管理的转变；
c) 开放兼容原则：支持多协议、多品牌、多系统的兼容接入，提供标准化开放接口，构建开放生态；
d) 轻量化高效原则：模型处理高效，系统响应及时，支持多终端流畅运行，降低硬件与算力依赖；
e) 国产化自主原则：优先选用国产技术栈，保障核心技术自主可控；
f) 安全可靠原则：构建纵深防御安全体系，保障数据安全与业务连续性；
g) 持续演进原则：支持模块化部署与能力扩展，适应业务需求变化和技术迭代。

4.2 系统功能

智慧园区一体化数字底座应采用“云-边-端”三级协同的总体架构，分为五大功能模块：

a) 数字孪生底座：提供空间建模、轻量化渲染、二三维一体化能力，作为园区的空间数据基础设施；
b) 物联感知：提供设备接入、协议转换、边缘计算、实时采集能力，实现园区全域感知；
c) 数据治理：提供数据采集、治理、标准、存储与服务能力，构建统一的园区数据底座；
d) AI 智能引擎：提供大模型融合、本地小模型部署、智能分析与决策能力；
e) 融合应用门户：提供统一入口、多端协同、开放生态与业务应用服务能力；
f) 能碳管理：提供能耗与碳排放的实时监测、分析核算与优化控制能力，支撑园区绿色低碳运营。

4.3 统一编码

4.3.1 应建立园区统一的编码体系，覆盖空间单元、设备资产、数据资源三大类对象，对园区、建筑、楼层、房间、设备、资产等进行分层唯一编码。

4.3.2 编码应具备层级性、唯一性与可扩展性，可通过编码识别对象所属层级、类型与归属关系，支持新增对象的编码平滑扩展。

4.3.3 编码应与国家、行业相关标准兼容，支持与城市级 CIM 平台、政务空间平台的数据对接。数据共享接口应符合国家或行业现行数据交换标准，如 JSON、XML 格式，并支持 RESTful API 协议。

4.3.4 编码应实现物联数据、业务数据、空间模型的映射，支撑空间化、可视化的数据查询与管理。

4.3.5 编码体系应符合 GB/T 36625（所有部分）的规定。

4.3.6 编码应具备校验机制，防止编码录入错误；编码生成、变更、注销应履行审批流程，留存变更记录。

4.4 数据共享

4.4.1 应构建园区统一的数据共享机制，实现不同子系统、不同部门之间的数据互通，消除数据孤岛。

4.4.2 数据共享应遵循“按需共享、授权使用、安全可控”的原则，明确数据共享范围、权限与方式。

4.4.3 应支持与上级政务平台、城市级平台的数据对接与共享，满足政务数据互联互通要求。
4.4.4 共享数据应采用标准化格式，提供统一的数据服务接口，降低数据对接成本。
4.4.5 应建立数据共享审核机制，对数据共享申请进行审批，对共享行为进行全程审计，保障数据共享安全。

4.5 安全可靠

4.5.1 安全体系定级应符合 GB/T 22240 的规定，安全体系应符合 GB/T 22239 规定的相应等级要求，重要园区安全体系不应低于网络安全等级保护第三级。
4.5.2 安全防护应覆盖物理、网络、数据、应用、身份全维度，构建纵深防御体系。
4.5.3 核心组件应采用冗余部署架构，关键节点无单点故障，保障系统连续稳定运行。
4.5.4 应建立完善的安全管理制度与应急响应机制，保障系统与数据安全。

4.6 国产化适配

4.6.1 底座应采用国产化技术路线，从底层硬件到上层应用逐步实现自主可控，降低供应链安全风险。
4.6.2 应支持国产服务器芯片、国产操作系统、国产数据库、国产中间件的适配运行，适配主流国产化基础软硬件生态。
4.6.3 核心功能模块应基于国产化技术栈开发，关键算法与核心代码自主可控，避免依赖非授权技术组件。
4.6.4 应支持国产密码算法应用，在身份认证、数据加密、签名验签等场景优先采用国密算法，符合国家密码管理相关规定。

5 数字孪生底座

5.1 一般要求

5.1.1 底座应实现园区物理实体与数字空间的实时映射、数据融合与双向交互，支撑可视化管理、应急指挥、仿真分析等场景。
5.1.2 底座应具备多终端适配能力，支持 Web 端、大屏端、移动端的三维场景流畅运行。

5.2 模型接入

5.2.1 底座应支持城市级 CIM 实景三维模型与单体建筑级 BIM 精细模型的融合接入，实现园区与城市级空间数据的无缝衔接。
5.2.2 应支持主流模型格式接入，包括但不限于 IFC、RVT、OSGB、FBX、glTF、3D Tiles 等格式。
5.2.3 模型应按细节层次分为 LOD100 至 LOD400 四级，不同应用场景适配对应精度模型：

a) LOD100：概念级模型，用于园区整体概览，表现建筑外形与整体布局；
b) LOD200：方案级模型，用于园区分区管理，表现建筑结构、道路、绿化等主要要素；
c) LOD300：构件级模型，用于楼宇级管理，表现建筑内部结构、主要设备与空间划分；
d) LOD400：精细级模型，用于房间级与设备级管理，表现房间细节、设备参数与内部构造。

5.3 空间层级管理

5.3.1 底座应支持“园区－楼宇－楼层－单户－房间－设备点位”六级粒度的精细化空间建模与管理，并符合下列规定：

a) 园区级：提供园区全景视角，展示建筑分布、道路、绿化、设施等宏观信息；
b) 楼宇级：支持单栋建筑的独立查看与精细化管理；
c) 楼层级：支持建筑内部结构的逐层拆解展示，包含墙体、门窗、管线等构件；
d) 单户级：支持以“户”为坐标的空间离散化表达，实现“一户一档”；
e) 房间级：支持以房间为坐标的空间表达；
f) 设备点位级：支持设备单元独立建模与空间精确定位。

5.3.2 各层级空间应具备清晰的层级归属关系，支持层级间的无缝切换与联动定位。
5.3.3 每个空间单元应绑定对应的属性信息与业务数据，支持点击查询空间单元的全维度信息。

5.4 模型轻量化

5.4.1 底座应具备自动化模型轻量化处理能力，可对大体积 BIM 模型、倾斜摄影模型进行几何简化、纹理压缩、实例化处理，在保证核心视觉效果与业务精度的前提下大幅降低模型体量。
5.4.2 轻量化处理应保留模型的核心几何结构、关键属性与空间拓扑关系，不影响业务场景的使用精度。
5.4.3 百万平方米规模的园区 BIM 模型，经轻量化处理后，Web 端首次加载时间不应大于 5 s，模型加载效率较原始模型提升不应低于 60%。
5.4.4 轻量化后的模型应支持流式加载与按需加载，根据浏览视野动态加载对应精度模型，提升运行效率。
5.4.5 应支持批量模型轻量化处理，可对多栋建筑、多类模型进行批量自动化处理并输出标准化格式，提升建模实施效率。

5.5 二三维融合展示

5.5.1 底座应实现二维 GIS 地图与三维场景的无缝切换与联动，二维与三维数据保持一致的空间坐标系与编码体系。
5.5.2 应支持在三维场景中叠加二维业务图层、点位标注、热力图、轨迹线等数据，实现二、三维数据融合展示。
5.5.3 应具备通用空间分析能力，包括空间查询、距离测量、面积测量、路径规划、视域分析等，二、三维场景下分析结果保持一致。
5.5.4 应支持多场景可视化效果切换，包括白天、夜晚、雨雪天气等环境模拟，适配不同展示需求。
5.5.5 应支持自定义图层管理，用户可根据业务需求自主开关各类业务图层，调整图层显示顺序与样式。

5.6 数字空间映射

5.6.1 应建立物理园区与数字空间的映射关系，实现物理实体状态向数字空间的实时同步。
5.6.2 物联感知数据、业务运行数据应与空间模型进行关联绑定，实现数据在三维空间中的可视化呈现，支持告警事件的空间定位与高亮展示。
5.6.3 应支持数字空间向物理实体的反向控制，可通过三维场景下发设备控制指令，实现虚实双向交互。
5.6.4 应支持基于数字孪生的场景仿真，可模拟设备故障、应急事件等场景下的园区运行状态，辅助决策分析。

5.7 模型更新

5.7.1 应建立模型更新机制，明确更新触发条件、更新流程与责任主体，保障数字空间与物理实体的一致性。
5.7.2 园区建筑改造、设备增减、空间调整后，应在 30 个工作日内完成对应模型的更新；日常设备参数变更应实现数据属性的实时同步。
5.7.3 模型更新应保留历史版本，支持版本回溯与对比，记录每次更新的内容、时间与责任人。

6 物联感知

6.1 一般要求

6.1.1 物联感知体系应作为园区统一的设备接入与数据采集枢纽，实现各类设备与子系统的标准化接入、统一管理与数据汇聚。
6.1.2 设备接入稳定性不应低于 99.5%，满足大型园区的设备接入需求。
6.1.3 应具备高可用架构，关键节点采用冗余部署，避免单点故障导致设备接入中断。

6.2 协议兼容

6.2.1 应全面覆盖主流物联网协议，支持的协议不应少于 10 种，包括但不限于：MQTT、HTTP、TCP、

CoAP、LoRa、NB-IoT、Modbus、BACnet、ONVIF、OPC UA 等。

6.2.2 应支持协议自定义扩展能力，可通过配置化方式新增私有协议适配，无需修改核心代码。

6.2.3 协议解析应具备标准化输出能力，将不同协议的异构数据转换为统一格式的标准化数据，向上层提供一致的数据接口。

6.2.4 应支持主流厂商设备的快速适配，兼容市场主流品牌的安防、能耗、机电、门禁等设备。

6.3 设备管理

6.3.1 应提供全生命周期设备台账管理能力，支持设备注册、配置、上线、离线、故障、报废全状态管理。

6.3.2 应支持设备批量接入与自动发现，提升大规模设备部署效率。

6.3.3 应实时监控设备运行状态，包括在线状态、运行参数、告警状态等，设备异常时自动生成告警并推送。

6.3.4 应支持设备远程配置、固件升级、重启控制等远程运维操作，降低现场运维成本。

6.3.5 应支持设备分组、分区域管理，可按空间位置、设备类型、所属系统等维度进行分组管控。

6.4 边缘网关

6.4.1 应采用边缘网关作为园区现场设备接入的核心节点，负责本地设备协议转换、数据预处理与本地控制。

6.4.2 边缘网关应支持多协议本地解析，可直接接入不同协议的终端设备，实现数据本地汇聚。

6.4.3 边缘网关应具备本地计算能力，可在本地执行数据清洗、聚合、告警判断与联动规则，减少云端带宽压力。

6.4.4 边缘网关应支持断网自治能力，网络中断时可独立运行，保障本地设备监控、联动控制等基础功能正常可用。

6.5 实时采集

6.5.1 应支持设备数据的实时采集，采集频率可根据设备类型与业务需求灵活配置，关键设备数据采集频率不应低于 1 次/s。

6.5.2 数据采集应具备完整性与准确性，关键数据采集成功率不应低于 99.9%。

6.5.3 应支持数据采集异常自动重试与补传，网络恢复后自动补传断网期间的历史数据，保障数据连续性。

6.5.4 应支持对采集数据的初步校验与过滤，剔除异常脏数据，保障上传数据质量。

6.6 云边协同

6.6.1 应建立云端与边缘端的协同机制，云端负责全局设备管理、策略配置与大数据分析，边缘端负责本地实时处理与设备控制。

6.6.2 云端可统一下发设备控制策略、联动规则与计算模型到边缘节点，边缘节点本地执行策略与规则。

6.6.3 应实现云边数据双向同步，边缘端数据定期上传云端，云端配置与策略同步至边缘端，保持云边数据一致性。

6.6.4 应支持协同计算调度，根据计算需求与网络状态，动态分配云端与边缘端的计算任务，兼顾效率与成本。

7 数据治理

7.1 一般要求

7.1.1 应构建园区数据全链路采集、治理与服务体系，打造园区统一的数据资产中心与数据服务枢纽。

7.1.2 应实现园区全量数据的统一标准、统一存储、统一治理与统一服务，支撑数据共享复用与业务创新。

7.1.3 应遵循“一数一源、一源多用”的原则，保障数据的一致性与权威性。

7.2 数据采集

7.2.1 应支持多源异构数据的统一采集，采集范围应包括物联感知数据、空间模型数据、业务系统数据、外部共享数据。

7.2.2 应支持异构数据源的统一采集，数据源类型包括但不限于：

a) 关系型数据库（MySQL、PostgreSQL、Oracle 等）；
b) 时序数据库（设备运行数据）；
c) 文件系统（CSV、JSON、XML 等）；
d) 消息队列（Kafka、RabbitMQ 等）；
e) API 接口（RESTful、WebSocket 等）。

7.2.3 应集成 ETL 工具，支持关系型数据库、非关系型数据库、文件、API 接口、消息队列等多种数据源的采集接入。

7.2.4 应支持多种采集方式，包括实时采集、定时采集、增量采集、全量采集等，可根据数据特性适配最优采集方式。

7.3 数据标准

7.3.1 应建立园区统一的数据标准目录，规范数据的命名、格式、编码、口径与质量要求，实现数据标准化。

7.3.2 数据标准目录应覆盖以下核心数据域：

a) 空间数据标准（建筑、楼层、房间编码规则）；
b) 设备数据标准（设备分类、属性字段、状态枚举值）；
c) 业务数据标准（通行记录、能耗账单、告警事件等）；
d) 用户数据标准（身份信息、角色权限、访问记录等）。

7.3.3 数据标准应与国家、行业相关数据标准兼容，保障跨平台、跨系统的数据互通。

7.3.4 应建立数据标准的发布、修订、废止全流程管理机制，保障标准的时效性与适用性。

7.3.5 新增数据接入应遵循统一数据标准，不符合标准的数据应进行清洗转换后方可入库。

7.4 数据治理

7.4.1 宜采用 ODS、DWD、DWS、ADS 多层递进式数据架构，对原始数据进行清洗、转换、关联、聚合，形成分层数据资产。可根据园区规模和实际需求，对数据分层架构进行简化或合并。

7.4.2 应具备数据质量管控能力，对关键数据集规定完整率、有效率、重复率、及时率等阈值及计算方法，对异常数据进行自动告警与处理。

7.4.3 应建立数据资产目录，对园区数据资产进行分类分级管理，支持数据资产的检索、溯源与权限管控。

7.4.4 应支持数据全链路血缘追踪，可追溯数据从采集到加工、应用的完整流转过程，支撑问题定位与影响分析。

7.4.5 应建立数据治理长效机制，定期开展数据质量评估与治理优化，持续提升数据质量。

7.4.6 数据治理能力宜参考 GB/T 36073 中数据管理能力成熟度模型进行建设。

7.5 数据存储

7.5.1 应采用混合存储架构，根据数据类型与使用场景适配不同存储组件：

a) 关系型数据库：存储结构化业务数据、配置数据与管理数据；
b) 时序数据库：存储高并发、高频次的物联时序数据；
c) 非关系型数据库：存储半结构化、非结构化数据；
d) 对象存储：存储文件、图片、视频、模型文件等非结构化数据。

7.5.2 存储系统应具备线性可扩展性，支持存储容量在线扩容，满足园区数据持续增长需求。

7.5.3 应建立数据备份机制，遵循 3-2-1 备份原则，定期执行全量备份与增量备份，备份数据加密存储。

7.5.4 应支持数据生命周期管理，对不同热度的数据采用差异化存储策略，降低存储成本。

7.6 数据服务

7.6.1 应提供标准化的数据服务接口，支撑上层应用的各类数据需求。
7.6.2 数据服务应支持下列交付方式：
a) 实时查询：通过 API 接口提供即时的数据查询服务；
b) 批量导出：支持大数据量的离线导出；
c) 订阅推送：支持数据变更的主动推送通知。
7.6.3 数据服务接口应具备访问控制、流量限制和数据脱敏等安全措施。

8 AI 智能引擎

8.1 一般要求

8.1.1 AI 能力体系应融合通用大模型与园区行业小模型，为园区各场景提供智能化分析与决策支撑。
8.1.2 AI 能力应采用模块化、服务化设计，可被上层应用灵活调用，支撑不同业务场景的智能化升级。
8.1.3 应支持 AI 模型的持续迭代优化，提升智能化应用的准确性与适配性。

8.2 AI 能力建设

8.2.1 应按应用风险分级，规定训练/评测数据来源与授权、数据脱敏、模型和提示版本管理、输出标识、内容安全、知识引用、访问控制、调用审计、提示注入防护、效果漂移监测、回退和停用机制。涉及设备控制、人员权益或安全决策的输出应经规则校验或人工确认，不得由生成式模型直接执行高风险控制。
8.2.2 AI 能力建设宜支持对接符合国家相关法律法规要求的 AI 大模型服务商 API 接口。
8.2.3 通用大模型融合包括：
a) 应支持对接主流 AI 大模型服务商的 API 接口，实现自然语言交互能力；
b) 应支持通过自然语言交互方式实现数据查询、报表生成、知识问答等功能；
c) 大模型调用应具备内容安全审核机制，防止输出违规内容。
8.2.4 本地专用模型部署包括：
a) 应支持面向园区场景的本地化专用模型训练和部署；
b) 本地模型应覆盖能耗预测、碳排评估、故障诊断、异常检测、智能调度等专业场景；
c) 模型推理应在边缘侧或本地服务器完成，保障低延迟响应和数据安全。
8.2.5 应提供 AI 管理平台，具备下列管理功能：
a) 渠道管理：配置上游 AI 服务商的 API Key、模型映射、优先级等；
b) 模型管理：对外开放模型列表及参数配置；
c) 模型部署：支持自建/私有模型的接入与版本管理；
d) 系统设置：运营管理、使用量统计、速率限制等精细化配置；
e) 训练场：提供在线测试环境，用于模型效果验证和调试。
8.2.6 AI 模型的训练和使用应符合国家关于人工智能安全与伦理的相关规定，涉及敏感数据的 AI 应用应采用私有化部署。

8.3 智能应用

8.3.1 AI 引擎应支撑下列核心智能应用场景：
a) 智能问答：基于园区空间数据、设备数据和业务数据的自然语言查询与分析，支持“数据能说话、会思考”的智能交互体验；
b) 能耗预测：基于历史能耗数据、天气数据、人流量等因素，实现分区域、分系统的能耗趋势预测与异常识别；
c) 碳排放评估：基于能耗数据和排放因子，自动计算碳排放量，生成碳排放报告，支撑碳减排目标跟踪；
d) 故障诊断：基于设备实时运行数据和历史故障数据，实现设备故障预测、根因分析和维护建议；
e) 智能报表：基于数据仓库自动生成运营分析报表，支持可视化展示和数据导出。
8.3.2 智能应用应具备持续学习与模型迭代优化能力，适应园区运行特征和业务需求变化。

8.3.3 应建立智能应用效果评估机制，通过准确率、响应时间、用户满意度等指标持续优化模型质量。

9 融合应用门户

9.1 开放兼容要求

9.1.1 应采用开放的技术架构与标准化接口，支持不同厂商的设备、系统与应用接入。
9.1.2 应兼容主流的物联协议、模型格式、数据格式与数据库类型，降低适配成本。
9.1.3 应提供完善的 API 开放文档与开发工具包，支撑第三方应用快速构建与生态扩展。
9.1.4 应支持国产化软硬件环境适配，适配国产操作系统、国产数据库、国产中间件等基础软件。

9.2 可扩展性要求

9.2.1 应支持设备接入规模、数据存储容量、用户并发数量的在线平滑扩展，满足园区逐步建设的需求。
9.2.2 功能模块应采用松耦合、组件化设计，可根据业务需求灵活增删功能模块。
9.2.3 应支持算法模型、业务规则的灵活配置与扩展，适配业务场景的持续迭代。
9.2.4 应预留与新技术融合的扩展接口，支持未来新技术的快速接入与应用。

10 能碳管理

10.1 能耗与碳排放监测

10.1.1 应建立分类分项能耗监测体系，覆盖电力、水、燃气、热力等主要能源类型，实现园区级、楼宇级、设备级三级能耗监测。
10.1.2 应通过物联感知设备实时采集能耗数据，关键能耗节点数据采集频率不应低于 1 次/15min。
10.1.3 碳排放监测范围应覆盖园区直接排放与间接排放，对应能源消耗、生产过程、废弃物处理等排放源。
10.1.4 应支持碳排放因子的配置与更新，保障核算结果的时效性与准确性。

10.2 能碳分析与核算

10.2.1 应按照 GB/T 51366 的相关要求，结合园区实际场景建立碳排放核算模型，自动核算园区碳排放总量与结构。
10.2.2 应支持多维度能碳统计分析，包括时间维度（时、日、月、季、年）、空间维度（园区、楼宇、楼层）、能源类型维度等。
10.2.3 应支持能碳对标分析，可与历史同期、行业标杆、定额指标进行对比，识别节能降碳潜力。
10.2.4 应支持能碳数据可视化展示，通过图表、看板等形式直观呈现园区能碳状况。
10.2.5 应自动生成能碳统计报表与分析报告，支撑日常管理与上报需求。

10.3 能碳分析与优化

10.3.1 应基于 AI 引擎提供能碳优化策略建议，包括但不限于：
a) 设备运行参数优化（空调温度策略、照明时段控制等）；
b) 用能结构优化（峰谷用电调整、新能源利用最大化等）；
c) 可再生能源配置方案（光伏、储能等）。
10.3.2 应支持节能改造效果量化评估，对比改造前后能耗和碳排放变化。
10.3.3 能碳数据分析结果应以可视化报表、驾驶舱图表等形式呈现。

11 信息安全

11.1 系统安全

11.1.1 网络应进行安全区域划分，不同安全等级的区域之间实施隔离，边界部署防火墙、入侵防御等安全设备。

11.1.2 服务器、主机等计算资源应进行安全加固，关闭不必要的服务与端口，配置安全策略。
11.1.3 应部署恶意代码防护软件，开启实时防护，定期开展病毒查杀，保障系统环境安全。
11.1.4 应定期开展系统漏洞扫描与安全加固，高危漏洞应在发现后 72 h 内完成修复。
11.1.5 系统投入运行前，应按照 GB/T 22240 确定的等级，通过符合国家认证认可要求的测评机构进行等级保护测评，并依法向公安机关完成备案。

11.2 数据安全

11.2.1 应按照数据分类分级要求对园区数据进行分级管理，不同级别数据采用差异化的安全防护策略。
11.2.2 敏感数据传输应采用加密通道，存储应采用加密方式，保障数据传输与存储的机密性。
11.2.3 个人信息处理应符合《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、GB/T 35273 的要求，遵循合法、正当、必要原则，保障个人信息主体权益。
11.2.4 应部署数据防泄漏能力，对敏感数据外发行为进行监控与管控，防止数据违规泄露。
11.2.5 应建立数据备份与恢复机制，定期开展备份恢复测试，保障数据可用性。

11.3 权限管理

11.3.1 应建立统一的身份认证体系，支持账号口令、短信验证码、动态令牌等多种认证方式，高安全场景采用多因素认证。
11.3.2 应遵循最小权限原则分配用户权限，不同岗位用户仅授予完成工作必需的最小权限。
11.3.3 管理员等特权账号应重点管控，实行专人专用，操作全程审计。
11.3.4 应建立权限定期复核机制，每季度至少开展一次权限审计，及时清理冗余、过期权限。
11.3.5 人员异动时应及时变更或注销账号、回收权限，防止权限滥用。

11.4 日志管理

11.4.1 应开启系统全组件安全审计功能，审计范围覆盖用户登录、关键操作、配置变更、数据访问等。
11.4.2 审计日志应包含时间戳、事件类型、操作主体、操作对象、操作结果等要素。
11.4.3 审计日志应进行防篡改保护，可采取只读存储、数字签名等措施。
11.4.4 日志保存时间应不少于 6 个月，重要日志应延长保存期限。
11.4.5 应支持日志实时分析和异常告警，对高危操作应实时通知管理员。

12 运行维护

12.1 运维体系

12.1.1 应建立完善的运维管理体系，明确运维岗位职责、操作流程与服务标准。
12.1.2 应配置专职运维人员，负责底座的日常监控、故障处置、优化升级等工作。
12.1.3 应建立运维管理制度，包括日常巡检制度、变更管理制度、故障处置制度、应急响应制度等。

12.2 日常运维

12.2.1 应定期开展系统巡检，检查服务器运行状态、设备在线状态、安全告警情况、数据运行状态等，形成巡检记录。
12.2.2 应实时监控系统资源使用情况，包括 CPU、内存、磁盘、带宽等，资源不足时及时扩容。
12.2.3 应建立故障闭环管理机制，故障发现、派单、处置、验证全流程留痕，重大故障及时上报。
12.2.4 应建立系统版本升级机制，定期更新系统功能、修补安全漏洞、优化性能，升级前制定方案与回滚预案。

12.3 应急与容灾

12.3.1 应制定系统应急预案，覆盖服务器故障、网络中断、数据泄露、网络攻击等常见应急场景。
12.3.2 应定期开展应急演练，每年至少开展一次应急演练，检验应急预案的有效性，优化应急处置流程。
12.3.3 重要系统应具备灾难恢复能力，关键数据异地备份，恢复指标符合 GB/T 20988 相关要求。
12.3.4 安全事件发生后，应按预案启动应急响应，控制事态发展，排查原因，恢复系统，事后形成复

盘报告。

12.3.5 应按业务重要性规定服务可用率、计划停机处理、故障响应时间、平均修复时间、RTO、RPO、备份恢复成功率和演练频次。

13 验收与评价

13.1 测试要求

13.1.1 系统测试应包含下列内容：

a) 功能测试：验证底座各模块功能是否完整，是否符合本文件与项目需求要求，功能运行正常、逻辑正确；
b) 性能测试：验证底座的响应时间、并发能力、设备接入稳定性、模型加载效率、数据处理能力等性能指标，测试方法见附录 A；
c) 兼容性测试：验证底座对不同协议设备、不同格式模型、不同终端设备、不同操作系统的兼容适配能力；
d) 安全性测试：验证底座的安全防护措施是否有效，是否存在安全漏洞与风险；
e) 可靠性测试：验证底座的连续运行稳定性、故障恢复能力与容灾能力。

13.1.2 测试前应制定详细的测试方案，明确测试内容、测试方法、测试环境与判定标准。

13.1.3 测试应覆盖全部核心功能与关键性能指标，测试用例应完整、可复现。

13.1.4 性能测试应在典型运行环境下开展，测试结果应具有代表性。

13.1.5 测试完成后应形成正式测试报告，记录测试结果、发现的问题与整改情况。

13.2 项目验收

13.2.1 满足以下条件后方可启动验收：

a) 完成合同与设计文件规定的全部建设内容；
b) 系统连续试运行不少于 1 个月，运行稳定，功能与性能满足要求；
c) 完成系统测试，问题已整改完毕并通过复测；
d) 交付文档齐全，符合归档要求。

13.2.2 建设单位提交验收申请与全套验收资料；

a) 组建验收工作组，可邀请行业专家、第三方机构参与；
b) 听取项目建设情况汇报，审查验收文档；
c) 开展现场查验与功能演示，核验系统实际效果；
d) 结合测试报告与现场查验情况，形成验收意见；
e) 验收通过的正式交付，验收不通过的限期整改后重新验收。

13.2.3 验收应交付的文档包括但不限于：

a) 项目建设方案、设计文档；
b) 系统测试报告、试运行报告；
c) 用户手册、运维手册；
d) 设备清单、配置清单、接口文档；
e) 其他项目过程文档。

13.3 运行评价

13.3.1 底座正式投入运行后，每年应至少开展一次全面运行评价，也可根据管理需求开展专项评价。

13.3.2 运行评价应包含下列维度：

a) 功能符合性：底座功能是否持续满足业务需求，功能完好率、使用率情况；
b) 运行稳定性：系统可用率、故障发生率、设备在线率等运行指标；
c) 应用成效：管理效率提升、运维成本降低、节能降碳效果等业务价值；
d) 安全性：安全措施有效性、安全事件发生情况、数据安全保障能力；
e) 可持续性：运维保障能力、技术迭代能力、扩展适配能力。

13.3.3 评价流程应符合下列要求：

a） 制定评价方案，明确评价指标、评价方法与评分规则；
b） 收集运行数据、业务数据与用户反馈；
c） 开展现场核查与指标核验，进行量化评分；
d） 形成运行评价报告，总结成效，分析问题，提出改进建议；
e） 根据评价结果落实整改优化措施，持续提升底座能力与应用效果。

附 录 A
（资料性）
性能测试方法与判定准则

A.1 系统响应时间测试

测试方法：选取核心功能页面与常用查询接口，模拟典型并发用户数，连续调用 100 次，记录每次响应时间，计算平均值。

判定标准：页面平均响应时间≤5s，接口平均响应时间≤500 ms，无超时错误，请求成功率≥99.9%。

A.2 设备接入稳定性测试

测试方法：接入不少于 1000 台模拟设备，连续运行 72 h，统计设备在线时长与数据上报成功率。

判定标准：设备在线率≥99.5%，连接成功率≥99.9%，消息到达率≥99.5%，有效数据率≥98%，端到端采集成功率≥99.9%，数据上报成功率≥99.9%。

A.3 模型加载性能测试

测试方法应包括：

a) 倾斜摄影模型加载测试：加载地面分辨率优于 3 cm 的倾斜摄影模型；
b) BIM 场景加载测试：访问百万平方米建筑面积级别的 BIM 场景；
c) VR 全景加载测试：加载 VR 全景数据，记录从发起请求到全景画面完全加载并可交互的时间，重复测试 5 次取平均值；
d) Web 端二三维浏览性能测试：在 Web 端打开包含二三维全空间数据的城市综合场景，进行平移、缩放、旋转等常规浏览操作，使用性能分析工具记录并计算平均帧速率。

判定标准应包括：

a) 倾斜摄影模型加载过程无崩溃、报错、模型缺失等情况；
b) BIM 场景加载过程无崩溃、报错、模型缺失等情况；
c) VR 全景平均加载时间≤100 ms，加载过程无崩溃、报错、画面缺失等情况；
d) Web 端二三维全空间数据浏览时，平均帧速率≥30 帧/秒，画面流畅无明显卡顿。

A.4 并发性能测试

测试方法：使用压力测试工具模拟对应等级并发用户数，同时执行登录、查询、场景浏览等常规操作，持续运行 30 min。

判定标准：系统无崩溃、无明显卡顿，请求成功率≥99.9%，平均响应时间符合要求。

A.5 数据采集成功率测试

测试方法：选取 100 台关键设备，连续运行 24 h，统计应上报数据条数与实际成功上报数据条数。

判定标准：数据采集成功率≥99.9%，数据补传机制有效。

参 考 文 献

[1] 《中华人民共和国数据安全法》（中华人民共和国主席令 第八十四号）
[2] 《中华人民共和国个人信息保护法》（中华人民共和国主席令 第九十一号）