ICS Xx.xxx.xx
CCS X xx

T/ZGCIT

中 关 村 智 能 科 技 发 展 促 进 会 团 体 标 准

T/ZGCIT 0xx—2026

基于 AI 与数字孪生协同技术的文旅可视化综合管控平台建设指南

Guidelines for the Construction of a Comprehensive Management and Control Platform for Cultural Tourism Visualization Based on AI and Digital Twin Collaborative Technology

2026- 0x - xx 发布　　2026 - 0x- xx 实施

中关村智能科技发展促进会　　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。

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。

本文件由中关村智能科技发展促进会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件首次发布。

基于 AI 与数字孪生协同技术的文旅可视化综合管控平台建设指南

1 范围

本文件规定了基于AI与数字孪生协同技术的文旅可视化综合管控平台（以下简称“平台”）的建设要求、架构要求、功能要求、技术要求、运维管理、安全要求等内容。

本文件适用于基于AI与数字孪生协同技术的文旅可视化综合管控平台的开发、应用、管理等环节。

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 信息安全技术 网络安全等级保护基本要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 30247-2013 信息技术数字版权管理 术语

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 39786 信息安全技术 信息系统密码应用基本要求

CH/T 9015 三维地理信息模型数据产品规范

GB/T 45909-2025 网络安全技术、数字水印技术实现指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字孪生 digital twin

基于传感器更新、运行历史、物理模型等孪生数据,完成从物理实体到信息虚体的模型映射,以及从信息虚体反馈至物理实体的过程。

[来源：GB/T 40021-2021，3.11]

3.2

恢复点目标 recovery point objective;RPO

灾难发生后，业务系统可接受的最大数据丢失量，通常以时间衡量。

3.3

恢复时间目标 recovery time objective;RTO

灾难发生后，业务系统从宕机状态恢复到可运行状态所需的最长容忍时间。

3.4

数字水印 digital watermark

一种将特定信息嵌入数字内容中的技术，需要时可以根据预定义的提取算法把相关信息提取出来，从而证明数字内容的版权信息。

[来源：GB/T 30247-2013,2.3.13]

4 建设要求

平台建设应符合以下原则：

a） 平台建设应以文旅行业的运营管理、游客服务、资源保护与应急指挥等核心业务需求为出发点；

b） 平台应采用分层、模块化的总体技术架构。各层级之间应通过标准化接口进行交互，具备可扩展性、可维护性及技术组件的可替换性；

c） 平台应建立统一的数据资源体系，实现多源异构数据的有效汇聚、治理与共享；

d） 平台应采用开放的技术体系与标准协议，支持与既有及未来新增的相关信息系统、物联网设备及第三方服务进行数据交换和业务集成；

e） 平台应满足国家网络安全、数据安全及个人信息保护的相关法规与标准要求，建立贯穿设计、开发、部署、运维全生命周期的安全保障体系；

f） 平台应提供可视化交互界面，并具备完善的系统监控、故障告警、日常维护与升级更新能力。

5 架构要求

5.1 总体架构

平台架构如图1所示。

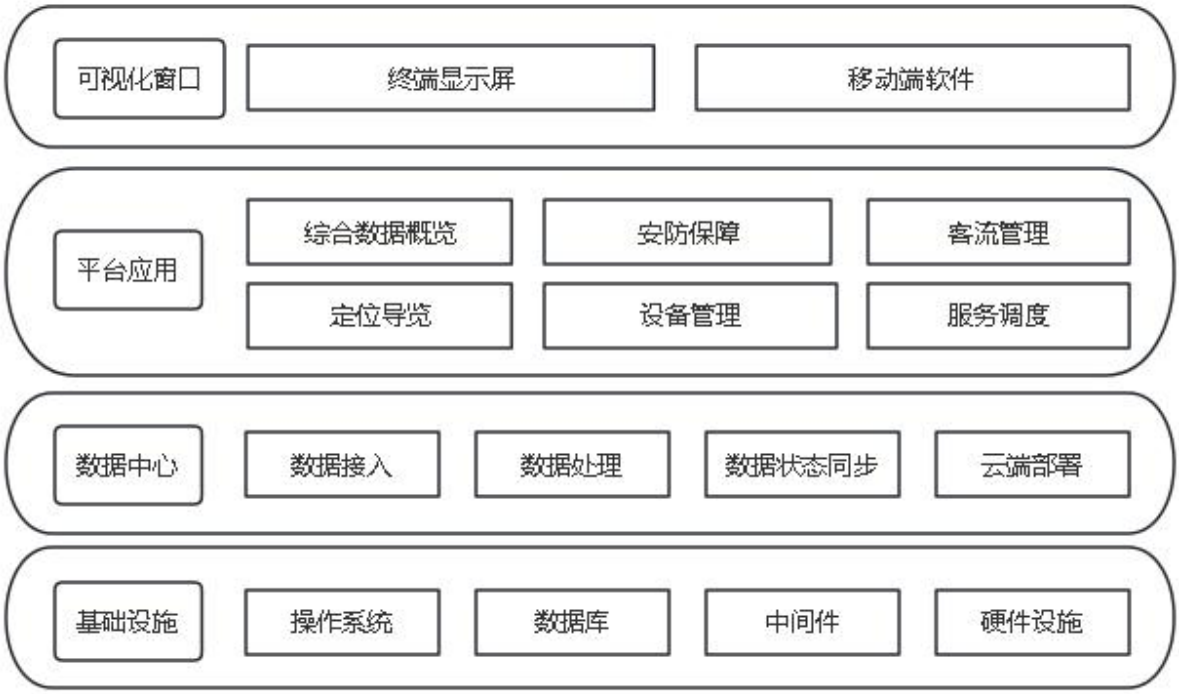

图1 基于AI与数字孪生协同技术的文旅可视化综合管控平台架构

5.2 可视化窗口

可视化窗口为不同终端用户提供人机交互与信息呈现能力，主要包括：

a） 终端显示屏：支持大屏端综合态势展示，具备三维数字孪生场景渲染、多视图联动与指挥调度能力，面向管理后台或信息发布场景，提供数据查询、业务操作与状态监控界面；

b） 移动端软件：面向移动管理人员或游客，提供便捷的移动操作、消息推送与轻量化可视化能力。

5.3 平台应用

平台应用是面向文旅场景提供业务管理与运营支撑的功能模块，应满足第6章中的要求，主要包括：

a） 综合数据概览：提供多维数据可视化仪表盘，支持关键指标动态监测与分析；

b） 安防保障：实现人员定位、异常行为识别、~~应急预警与联动处置能力~~；

c） 客流管理：支持客流实时监测、密度分析、拥堵预警~~与疏导调度~~；

d） 定位导览：提供基于位置服务的智能导航、路径推荐与AR互动体验；

e） 设备管理：实现对终端设备的远程监控、状态诊断~~与运维调度~~；

~~f） 服务调度：支撑人员、物资、应急资源的调度与任务闭环管理。~~

5.4 数据中心（数据存储与刷新频率）

数据中心负责实现多源数据的统一接入、融合处理、状态同步与云端协同，主要包括：

a） 数据接入：支持物联网设备、业务系统、第三方平台等多源数据实时接入，具备协议适配能力；

b） 数据处理：提供数据清洗、融合、分析及AI推理能力，支撑数字孪生模型构建与动态更新；

c） 数据状态同步：实现物理实体与数字孪生体之间的状态一致性同步；

d） 云端部署：支持公有云、私有云或混合云部署方式，具备弹性伸缩与跨域协同能力。

5.5 基础设施

基础设施为上层提供稳定、安全、可扩展的运行环境与基础资源，主要包括：

a） 操作系统：支持主流服务器操作系统，具备高可用性与兼容性，保障服务稳定运行；

b） 数据库：支持结构化与非结构化数据存储，具备高并发读写、数据备份与恢复能力；

c） 中间件：提供消息队列、缓存、服务调度等中间件服务，支撑系统间高效协同；

d） 硬件设施：包括服务器、存储设备、网络设备及边缘计算节点，满足算力、带宽与可靠性要求。

6 功能模块

6.1 综合数据概览

6.1.1 全域资源空间一张图

6.1.1.1 应基于二维地图或三维数字孪生场景，将建筑边界及内部空间划分、各展厅/常设展区/特展区、重点文物展位、文化服务设施、观众参观流线与出入口、生态与室外区域等核心资源进行数字化标绘与分层管理。

6.1.1.2 每个空间对象应能关联其属性信息（如展厅面积、容纳人数、~~展品数量、~~开放时间）及实时数据接口（如客流、温湿度、安防状态）。

6.1.1.3 各类资源应支持按类别、状态、热度等进行差异化图标显示与筛选，实现全域资源“一图尽览”。

6.1.1.4 应支持从全域概览到单个展厅或重点展柜的缩放浏览，缩放过程中地物细节与标签信息应平滑过渡与加载。

6.1.1.5 在大范围查看时，同类点状要素~~应~~宜能根据视图比例尺自动聚合显示为热力图或聚类图标，点击后可查看详情。

6.1.2 指标可视化监测

6.1.2.1 应在“全域资源空间一张图”侧边或面板上，以图表等形式集中展示关键运营指标，指标宜包括：

a） 客流指标：总在馆人数、各展厅实时客流、~~展厅饱和度、~~预约到馆率、参观停留时长；

b） 服务状态指标：票务闸机通行状态、导览设备借用率、互动展项使用情况、服务台排队时长；

c） 运营概览指标：当日预约人数、已入场人数、瞬时承载量预警、~~展厅舒适度指数、文物巡检完成率~~。

6.1.2.2 指标展示宜支持数据实时刷新，关键指标刷新延迟应不大于 15 秒，可配有趋势箭头或同比/环比简析。

6.1.3 全局态势感知

6.1.3.1 应能在“全域资源空间一张图”上呈现全域实时动态态势，宜包括：

a) 客流热力图：通过色块渐变直观展示各展厅、走廊、出入口等区域的客流聚集程度，支持按楼层、展厅维度切换查看；

~~b) 观众流线图：动态显示主要参观路径的人流走向及拥堵情况，辅助引导分流与紧急疏散决策；~~

c) 事件态势图：将安防告警、设备故障等事件以图标形式精准定位落图。

6.1.3.2 宜支持一键切换至任“热点区域”的详情视图，关联调取周边视频监控、资源列表及详情数据，辅助管理人员快速研判与调度。

6.2 安防保障（简化）

6.2.1 全域态势可视化监控

6.2.1.1 应基于“全域资源空间一张图”，对全域安防资源进行可视化管理，支持按类型、状态、管辖区域分层分类显示与快速检索，安放资源包括但不限于：

a) 视频监控（含普通摄像机、热成像摄像机）；

b) 电子巡更点；

c) 门禁系统（含展厅入口、库房门禁、办公区门禁）；

d) 消防设施（消防栓、烟感、温感、手动报警装置）；

e) 应急物资（灭火器、应急照明、疏散指示标识）；

f) 文物专用安防设备（展柜震动传感器、红外对射、玻璃破碎探测器）。

6.2.1.2 应支持重点区域的视频画面在数字孪生场景中关联调取，实现“点位－视频”一键联动。。

6.2.1.3 视频监控系统的互联互通宜遵循 GB/T 28181 的要求。

6.2.2 智能视频分析预警

6.2.2.1 应集成或对接智能视频分析系统，结合 AI 视觉识别能力，对实时视频流进行自动分析，宜实现以下场景的智能识别与告警：

a) 安全防范类：

i. 展厅瞬时客流超限；

ii. 区域超员；

iii. 人员异常聚集、推搡或争执；

iv. 夜间人员闯入、非开放时段非法入侵。

b) 消防安全类：

i. 烟雾识别、火焰识别；

ii. 观众违规吸烟行为识别。

c) 特定场景类：

i. 观众进入封闭展区、藏品库区等非开放区域；

ii. 观众攀爬展台、翻越隔离栏或触碰展柜；

iii. 展柜异常开启、观众肢体越过警戒线；

iv. 激光或震动传感器触发的文物接近告警联动确认。

6.2.2.2 AI 识别告警事件宜自动在数字孪生场景中定位，并以弹窗、声音、图标闪烁等方式实时推送。目标检出率宜不低于 90%，关键安防场景的告警延迟宜不大于 5 秒。

6.2.3 安全事件可视化

6.2.3.1 当发生告警或上报的安全事件时，宜支持：

a) 一键调取事件点位周边的视频监控画面、应急预案、可用安防及救援资源；

b） 在数字孪生场景中快速定位事件位置，并自动关联展示周边展品信息与人员分布。

6.2.3.2 应支持在场景中进行指挥调度，包括：

a） 在三维场景中划定警戒区域；

b） 规划最优安保或救援路径；

c） 调度安保或救援力量，并将指令下发给一线人员移动端。

6.2.3.3 应支持与广播系统、信息发布屏、展厅导览屏联动，在事件区域或疏散路径上进行语音播报和文字警示，必要时可定向发布疏散引导信息。

6.2.4 设施安全

6.2.4.1 应支持接入消防物联网传感器、展柜环境监测传感器、机电设备传感器等数据，并在数字孪生场景中以三维模型或图标形式展示其实时状态。

6.2.4.2 应对关键设施的运行状态参数进行可视化监测，支持阈值告警，告警信息宜与场景中的设备模型联动。

6.2.4.3 消防物联网数据的传输与通信宜符合 GB/T 26875 系列标准中的要求。

6.3 客流管理

6.3.1 客流实时监测与热力图可视化

6.3.1.1 应利用票务闸机、视频智能统计等多源数据，展示全域及重点区域的客流数量、分布密度与流动方向。

6.3.1.2 宜支持通过热力图、色块图或粒子流等可视化方式，呈现客流聚集程度。热力图应支持分级色带显示，并能根据预设阈值自动变色告警。对于多楼层博物馆，应支持按楼层切换查看客流分布。

6.3.1.3 客流数据统计与可视化更新频率宜不低于 30 分钟/次。

6.3.2 承载量预警与分级管控

6.3.2.1 应支持设定全域、各展厅及各功能分区的多级客流承载量阈值，包括最大承载量和瞬时最大承载。

6.3.2.2 当实时客流接近或超过设定阈值时，应在数字孪生场景中自动高亮预警区域，并通过弹窗、声音等多方式发布分级预警。

6.3.2.3 预警发布的同时，应能关联提示或一键启动预设的管控预案，采用暂缓入园、单向通行、远端疏导等行动。

6.3.3 客流预测

6.3.3.1 宜支持基于历史数据、实时客流、天气、节假日等因素，利用 AI 模型对未来短期的客流总量及关键节点客流趋势进行预测，预测结果应以图表形式可视化展示。

6.3.3.2 宜支持在数字孪生环境中进行客流疏导预案的模拟推演。模拟调整出入口开放策略、改变游览路线后，对关键区域客流压力的影响，为决策提供可视化参考。

~~6.3.4 疏导与调度~~

6.3.4.1 在发生拥堵或预警时，应支持在数字孪生地图上手动或半自动规划疏导路线，并通过联动信息发布屏、展厅导览屏、广播系统、官方 APP/小程序等渠道，向馆内观众发布疏导提示。

6.3.4.2 应支持调度一线服务人员前往指定区域进行现场引导，并可通过移动应用查看疏导任务与反馈结果。

6.3.4.3 模块宜与票务预约系统联动，实现基于客流预测的分时段预约和限量售票的动态调控。

6.4 定位导览（从工作人员角度）

6.4.1 室内外融合定位能力

6.4.1.1 宜支持场馆内外一体化定位能力，实现对观众、工作人员、移动设备及重要资产的实时位置感知。

6.4.1.2　定位技术宜融合蓝牙信标、超宽带、Wi-Fi、北斗/GPS 等多种方式，结合 AI 算法进行位置优化。

~~6.4.1.3　定位数据宜在数字孪生场景中实时映射，支持按人员类型或设备类型进行分层显示与筛选。~~

~~6.4.2　智能导览与个性化推荐~~

6.4.2.1　宜基于观众实时位置、参观偏好、停留时长、参观动线及历史行为数据，利用 AI 模型生成个性化参观路线推荐。推荐内容宜包括：

a）　基于当前客流分布的避堵路线；

b）　基于观众兴趣的重点展品推荐；

c）　基于特展排期与展品维护状态的动态调整建议。

6.4.2.2　应支持在移动端 APP/小程序及数字孪生场景中，以 AR 导航、3D 路径引导、地图路线绘制等方式，向观众提供实时导航指引。导航过程中应支持关键节点的语音播报与文字提示。

6.4.2.3　导航路线宜支持无障碍模式，优先选择坡道、电梯等无障碍通道，并关联展示无障碍服务设施位置。

6.5　设备管理

6.5.1　设备接入

6.5.1.1　应支持对场馆内各类设备进行统一接入与数字孪生建模，实现设备在三维场景中的映射与可视化呈现。设备类型宜包括但不限于：

a）　安防设备：视频监控摄像机、门禁、电子巡更点、红外对射、震动传感器、玻璃破碎探测器；

b）　消防设备：烟感探测器、温感探测器、手动报警装置、消防栓、灭火器、电气火灾监测设备；

c）　环境监测设备：温湿度传感器、光照传感器、二氧化碳传感器、PM2.5传感器、震动监测仪；

d）　展陈设备：展柜照明、恒温恒湿系统、互动展项设备、投影仪、触控屏；

e）　机电设备：空调系统、新风系统、电梯、扶梯、配电柜、照明系统；

f）　服务设备：票务闸机、自助售票机、导览设备租赁终端、信息发布屏、广播系统。

6.5.1.2　每个设备应在数字孪生场景中以三维模型或标准化图标形式呈现，并关联设备基础信息及实时运行数据接口。

6.5.2　设备状态监测

6.5.2.1　应支持对接入设备的运行状态进行实时监测，并在数字孪生场景中以颜色、图标动画等形式直观呈现设备状态。

6.5.2.2　监测数据应在数字孪生场景中支持点选查看实时数值、历史曲线及趋势分析。

~~6.5.3　预测性维护~~

6.5.3.1　宜基于设备运行参数与历史故障模式，自动识别设备异常状态，给出故障类型判断与处置建议。

6.5.3.2　宜基于设备运行时长、损耗趋势、历史维修记录等数据，预测设备剩余使用寿命，提前推送维护提醒与备件更换建议。

6.5.3.3　诊断结果与维护建议应在数字孪生场景中关联设备模型展示，并支持生成维护工单推送至相关人员移动端。

6.5.4　设备运维

6.5.4.1　应支持在平台中进行设备运维任务的闭环管理，包括：

a）　设备告警或故障可自动生成维修工单，工单内容应包括设备信息、故障描述、位置信息、建议处置方式；

b）　支持按周期或运行时长设定预防性维护计划，自动生成巡检或保养工单；

c） 支持将工单派发至指定维修人员，维修人员可通过移动端接收工单、查看设备详情、上传维修记录与现场照片；

d） 支持维修完成后的验收确认，记录维修时长、更换备件、故障原因等信息，形成设备运维档案。

6.5.4.2 宜支持设备运维数据的统计分析，包括设备故障率、平均修复时间、维护完成率等指标的可视化展示。

~~6.5.5 设备资产全生命周期管理~~

应支持对设备资产进行全生命周期管理，记录设备从采购入库、安装部署、运行维护到报废退出的完整轨迹。管理内容宜包括：

a） 设备台账：设备基本信息、技术参数、供应商信息、采购日期、保修期限；

b） 备件管理：关键设备备件库存信息、备件使用记录；

c） 维保记录：历次维修、保养、巡检记录及文档附件；

d） 设备文档：设备操作手册、安装图纸、维保合同等电子文档关联存储。

6.6 服务调度

6.6.1 多渠道服务请求受理

6.6.1.1 应整合电话、一键求助桩、移动应用（App/小程序）、二维码扫码、巡逻人员上报等多渠道服务请求，形成统一的待处理服务工单池。

6.6.1.2 所有包含位置信息的服务请求，宜自动在数字孪生地图上定位，以图标形式显示其类型、状态与紧急程度。

6.6.2 交通管理

6.6.2.1 宜在数字孪生地图上整合呈现与场馆相关的外部交通要素，包括：

a） 场馆周边主要连接道路及公共交通站点；

b） 场馆停车场（库）的入口、出口、车位分布。

6.6.2.2 宜实现动态交通态势的可视化，包括但不限于：

a） 通过颜色直观显示场馆周边主要道路的实时拥堵状态；

b） 动态显示各停车场（库）的车位总数、剩余空位数、饱和度，支持与预约系统联动，向预约观众推送停车余位信息。

6.6.2.3 当停车场饱和度超过预设阈值或周边道路出现严重拥堵时，应自动预警，并在数字孪生场景中高亮显示。宜能关联启动预案，通过信息发布屏、官方 APP/小程序等渠道向计划到馆观众发布绕行提示或公共交通出行建议。

用户角色权限不同　页面

7 技术要求

7.1 数据接口规范

7.1.1 接口通用要求

7.1.1.1 平台内部微服务之间、平台与外部第三方系统之间的数据交换接口，应采用基于 HTTP/HTTPS 协议的 RESTful API 或基于 WebSocket 的实时数据推送协议。

7.1.1.2 接口通信应进行身份认证与授权，宜采用基于令牌的认证机制。

7.1.1.3 所有接口应提供 API 文档，描述其功能、请求/响应格式、参数定义及错误代码。

7.1.2 数据内容与质量标准

7.1.2.1 接口交换的数据应包含明确的元数据信息。

7.1.2.2　数据提供方应保证通过接口传输数据的时效性、完整性与准确性。
7.1.2.3　个人信息的接口传输与处理宜符合 GB/T 35273 中的要求，采取加密、脱敏等安全措施。

7.2　平台部署环境要求

7.2.1　平台应支持本地部署或云端部署模式，可根据实际需求与安全策略选择适宜方式：

a)　本地部署：平台部署于场馆自有数据中心或机房，适用于对数据安全、网络隔离要求较高的场景，支持与场馆现有安防、消防、楼宇自控等内部系统直接对接；

b)　云端部署：平台部署于公有云或私有云环境，适用于希望降低硬件投入、弹性扩展资源的场景。

7.2.2　部署架构应具备高可用性，核心服务应支持集群化部署，避免单点故障。关键服务宜实现跨节点或跨可用区容灾。

7.3　基础设施资源

7.3.1　服务器应满足平台应用、AI 模型推理、三维渲染等负载需求。推荐配置具备 GPU 加速能力的服务器用于 AI 分析和高性能三维可视化。容器化部署时，应支持主流容器编排工具。
7.3.2　应根据数据类型配置相应的存储系统，支持集中式存储、分布式存储、块存储、对象存储、文件存储等多种存储方法，支持结构化数据、半结构化数据和非结构化数据等多种数据类型存储。
7.3.3　应支持磁盘容错技术，如磁盘故障后节点的自动平衡和重构、硬盘故障检测和处理、集群节点出现单盘故障时不影响业务运行等。

7.4　国产化技术

7.4.1　宜优先选用国产服务器、存储设备、网络设备、专用计算设备、输入输出设备和其他硬件。采用国外技术的硬件产品，应有国产替代方案，并支持主流国产操作系统及虚拟化/容器化环境。
7.4.2　宜采用在国产操作系统或开源可控操作系统，鼓励采用国产数据库、中间件、开发框架及工具链，避免采用具有安全缺陷的和在风险名单中的软件。在可视化渲染等关键环节、数字孪生可视化工具中，宜优先选用或兼容支持自主可控的国产三维渲染引擎、图形库及可视化开发工具。相关基础软件与可视化组件应具备自主知识产权，并提供可持续的技术支持、安全更新与性能优化服务。
7.4.3　在数据格式、接口协议、编码规范等方面应符合国家或行业标准，并具备与国产化软硬件生态的兼容能力。宜采用自主可控的数据压缩、加密、水印等技术，数据在国产化环境中应安全、高效处理且长期可读。
7.4.4　架构应具备良好的开放性与模块化设计，支持国产化组件与国外同类组件的平滑替换。在 AI 框架、地理信息引擎、可视化渲染等核心技术环节，应逐步建立并完善国产化技术栈，降低对外部技术体系的依赖。

7.5　容灾能力

平台部署应具备高可用与容灾能力，应满足以下要求：

a)　核心服务应采用多节点集群部署，单节点故障时自动切换，业务不中断；

b)　数据库应采用主从复制或集群模式，支持自动故障切换；

c)　关键数据应配置每日自动备份，备份数据应存储于不同物理位置或云存储；

d)　本地部署场景宜提供应急恢复方案，包括系统镜像、配置备份、快速部署脚本等，支持系统故障后的快速重建。

7.6　性能要求

7.6.1　界面与交互性能

在常规网络环境及标准配置客户端下，应满足以下要求：

a)　平台主界面加载完成时间宜≤5秒；

b)　数字孪生三维场景初始化加载时间宜≤8秒；

c)　图形画面显示帧率宜≥30帧/秒；

d) 用户常规界面操作的响应时间宜≤1秒；

e) 二三维地图的缩放、平移操作应流畅，无明显卡顿。

7.6.2 服务性能

7.6.2.1 平台宜支持不低于 500 路视频流（1080P）的并发接入与管理，支持不低于 800 个/秒的物联网传感数据点的并发接入与处理。

7.6.2.2 实时数据从接入到在平台界面更新的端到端延迟宜≤5 秒。

7.6.2.3 标准 API 接口的平均响应时间宜≤1 秒。响应失败的处理

7.6.3 可靠性

7.6.3.1 平台核心业务服务的可用性宜不低于 99.9%。

7.6.3.2 平台应具备数据备份与恢复机制，支持定期全量备份与增量备份。在发生故障时，应能进行数据恢复，核心业务数据的恢复点目标（RPO）宜≤30 分钟，恢复时间目标（RTO）宜≤2 小时。

7.6.3.3 平台应支持 7×24 小时不间断稳定运行，平均无故障时间（MTBF）宜不低于 10000 小时。

8 运维管理

8.1 运维监控体系

8.1.1 监控范围与指标(监控摄像头设备)

8.1.1.1 监控范围包括但不限于：

a) 基础设施：服务器CPU/内存/磁盘/网络使用率、虚拟机/容器状态；

b) 平台服务情况：数据库连接数、消息队列堆积、API网关吞吐量与延迟、微服务健康状态；

c) 应用与数据：关键业务功能模块可用性、数字孪生渲染引擎帧率、AI模型服务响应时间、核心数据流水线时效性。

8.1.1.2 应定义明确性能基线、容量阈值与告警规则，对异常情况进行多级别、告警。

8.1.1.3 监控日志应集中采集与管理，便于审计与故障排查。

8.1.2 监控与告警实施

8.1.2.1 应采用主动监控与被动采集相结合的方式，关键指标采集频率宜不低于 1 分钟/次。

8.1.2.2 告警信息应通过可视化大屏、声光、短信、移动应用等多种渠道，推送给相关运维人员。告警应包含清晰的事件描述、发生位置、影响范围和推荐处理建议。

8.1.2.3 应建立告警事件处理流程的跟踪与闭环管理机制。

8.2 备份与更新

8.2.1 数据备份与恢复

8.2.1.1 应制定并执行分级分类的数据备份策略。核心业务数据、配置数据及数字孪生模型数据应进行定期全量备份和更频繁的增量备份。

8.2.1.2 备份数据应在物理上与生产环境隔离存储，并定期进行恢复演练，验证备份数据的有效性与恢复流程的可行性，演练每年应至少进行一次。

8.2.1.3 数据恢复点目标（RPO）与恢复时间目标（RTO）应符合 7.3.3 中的要求。

8.2.2 系统更新与补丁管理

8.2.2.1 应建立平台软件、中间件、操作系统及安全设备的版本与补丁管理制度。在测试环境中验证通过后，可在业务低峰期对生产环境进行更新部署。

8.2.2.2 更新过程应支持灰度发布与快速回滚机制，升级失败时应能恢复至上一版本。

8.2.2.3 所有更新操作应有详细记录，包括更新内容、操作人、时间、回滚预案等信息。

8.2.3 变更管理

对平台架构、核心配置、关键业务流程的任何变更，均应执行变更申请、评审、批准、实施与复核流程。变更实施前应进行风险评估与影响分析，并制定应急回退方案。

9 安全要求

9.1 数据安全

9.1.1 数据加密国密的标准

9.1.1.1 涉及敏感数据或个人信息的数据在通过公共网络传输时，应采用基于 TLS 1.2 及以上版本的安全传输协议进行加密。
9.1.1.2 视频监控等流媒体数据的传输应采取加密或专用安全通道等保护措施。
9.1.1.3 密码技术应用宜符合 GB/T 39786 中的规定。
9.1.1.4 对于存储在数据库或文件系统中的个人敏感信息、重要业务配置数据及关键模型数据，应进行加密存储。
9.1.1.5 应建立密钥管理体系，对加密密钥进行全生命周期的安全生成、存储、分发、使用、更新、备份、恢复和销毁，严禁使用硬编码密钥或默认密钥。
9.1.1.6 关键多媒体数据应同时采用隐形数字水印技术进行防护鉴权，数字水印应满足 GB/T 45909-2025 的要求。

9.1.2 访问控制

9.1.2.1 所有访问平台数据的用户应进行身份鉴别，应采用口令、数字证书、动态令牌等至少一种鉴别技术，并支持双因素认证用于高权限账户或敏感操作。口令策略应符合复杂性、长度和定期更换的要求。
9.1.2.2 应实施基于角色的最小权限访问控制模型。不同角色应被授予完成其职责所必需的最小数据访问和操作权限。权限分配和变更应有审批记录。
9.1.2.3 应对平台内数据进行分级分类管理。在开发、测试、数据分析等非生产必要场景中，应对敏感个人信息进行去标识化或脱敏处理。
9.1.2.4 应对所有用户的重要数据访问和操作行为进行日志记录。审计日志应包含时间、用户、操作对象、操作类型、操作结果等信息，防止被非授权删除或篡改。

9.2 网络安全

9.2.1 网络架构安全

9.2.1.1 应按照“纵深防御”原则划分网络安全区域，区域之间通过防火墙等设备进行逻辑隔离和访问控制。
9.2.1.2 应限制从互联网到平台内部服务的直接访问。仅必要的、对外提供服务的 API 接口或门户才应在受控条件下对互联网开放，并通过 Web 应用防火墙等设备进行防护。
9.2.1.3 网络设备的配置应符合安全基线要求，关闭不必要的端口和服务。

9.2.2 入侵防范与安全审计

9.2.2.1 应在关键网络节点部署入侵检测/防御系统，监控并阻断恶意攻击和异常网络行为。
9.2.2.2 应部署网络安全审计系统，对网络流量、用户行为、安全事件进行集中收集、分析和留存，留存时间不少于 6 个月，宜符合 GB/T 22239 中国家网络安全等级保护二级及以上的要求。
9.2.2.3 应建立漏洞管理机制，定期对网络设备、安全设备、服务器操作系统、中间件及数据库进行漏洞扫描和安全评估，并及时修复中高风险漏洞。

9.2.3 通信安全

9.2.3.1 平台内部各组件之间的通信，应进行加密和完整性校验。
9.2.3.2 应防止网络设备、通信线路的物理损坏或逻辑中断导致的单点故障。
9.2.3.3 关键网络链路和设备应具备冗余能力。