T/CITSA 26-2022

ICS 43.020

T 00

团 体 标 准

T/CITSA 26-2022

综合客运枢纽智慧化规划建设指引

Intellectualization systems planning and construction guideline for integrated passenger transportation hub

2022-09-07 发布　　2022-09-07 实施

中国智能交通协会 发布

目 次

前　言

本文件按照 GB/T 1.1—2020 《标准化工作原则 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。

本文件由深圳市城市交通规划设计研究中心股份有限公司提出。

本文件由中国智能交通协会归口。

本文件起草单位：深圳市城市交通规划设计研究中心股份有限公司、杭州海康威视数字技术股份有限公司、海能达通信股份有限公司、北京天融信网络安全技术有限公司、禾麦科技开发有限公司、深圳地铁置业集团、深圳力维智联技术有限公司、深圳达实智能股份有限公司、华南理工大学、同济大学、深圳大学、中电科新型智慧城市研究院有限公司。

本文件主要起草人：张晓春、孙超、林涛、邵源、吕国林、张俊峰、陈永茂、徐主梁、黄愉文、李锋、吴岳、覃裔、徐丹、程驰、曹惠、林钰龙、韩广广、陆超、洪倩雯、张永捷、陈华林、吴超峰、刘宏、姚子毓、杨剑、凌育杰、甘海洋、于洋、程之龙、陈小天、徐晓东、赵莹、夏辉林、姚开方、邬蓬宇、卢凯、郭静秋、邹亮、夏鹏。

综合客运枢纽智慧化规划建设指引

1 范围

本文件规定了综合客运枢纽智慧化规划建设应遵循的设计原则、通用框架、建设内容，以及综合客运枢纽智慧化工程基础设施、支撑平台、智慧化应用的一般性要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 28181-2016 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 51419 无线局域网工程设计标准

GB/T 22239-2019 信息安全技术 信息系统安全等级保护基本要求

GB/T 39335-2020 信息安全技术个人信息安全影响评估指南

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 20090.2-2013 信息技术 先进音视频编码 第2部分:视频

JT/T 1065-2016 综合客运枢纽术语

JT/T 980-2015 综合客运枢纽智能化系统建设总体技术要求

YD/T 5230-2016 移动通信基站工程技术规范

3 术语、定义和缩略语

3.1 缩略语

下列缩略语适用于本文件。

3.1.1 QoS——服务质量（Quality of Service）

3.1.2 POL——无源全光局域网（Passive Optical LAN）

3.1.3 BIM——建筑信息模型（Building Information Modeling）

3.1.4 VPC——虚拟私有云（Virtual Private Cloud）

3.1.5 IP-SAN——存储局域网联（Internet Protocol Storage Area Network）

3.1.6 FC-SAN——光纤存储区域网络（Fiber Channel Storage Area Network）

3.2 术语和定义

下列术语和定义适用于本文件。

3.2.1 **综合客运枢纽** Integrated passenger transportation hub

将一种及以上对外运输方式与城市交通的客流转换场所在同一空间（或区域）内集中布设，实现设施设备、运输组织、公共信息等有效衔接的客运基础设施。[来源：JT/T 1065-2016]

3.2.2 **综合客运枢纽智慧化系统** Intelligent systems for integrated passenger transportation hub

集成应用现代信息、通信、控制和系统工程等技术，具有运行监测、安全应急与疏散、乘客综合信息服务、协同联动支持、载运工具停泊管理和综合信息管理等功能，支持综合客运枢纽实现高效组织运行、安全保障和信息服务的综合性系统。[来源：JT/T 980-2015]

3.2.3 **关键信息基础设施** Critical information infrastructure

支撑关键基础设施运行的计算机信息系统、控制系统及通信网络的统称。

3.2.4 **网络安全** Cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.2.5 **数据安全** Data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

3.2.6 **个人信息** Personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

3.2.7 **元数据** Metadata

是定义和描述其他数据的数据，元数据用于描述数据的内容、覆盖范围、质量、管理方式、数据的所有者、数据的提供方式等有关的信息。

3.2.8 **数据元** Data element

数据元是通过一系列的描述来实现的，数据元包含内部标识符、中文名称、英文名称、中文首拼、标识符、版本等内容。

3.2.9 **数据字典** Data dictionary

是描述数据的信息集合，是对系统中使用的所有数据元素定义的集合。

3.2.10 **标准数据集** Standard data set

是由若干数据元组成的数据集合，对同类型的业务进行规范化管理。

4 智慧化系统需求分析

4.1 需求分析原则

枢纽智慧化系统建设需求分析应结合枢纽已有信息化建设情况、实际业务需求、未来发展规划、项目投资水平，遵循实用性、前瞻性、先进性的要求开展。

4.2 综合监测需求

综合监测需求分析应包括：综合客运枢纽公共区域、重点作业区域、客流、载运工具、设施设备、环境能耗等的监测。

4.2.1 客流监测与分析

围绕枢纽大厅、通道、楼梯口等关键客流集聚区域的客流密度、速度、排队长度等监测开展需求分析。

4.2.2 载运工具监测与分析

围绕综合枢纽站场、周边道路、枢纽内部道路上运行的载运工具开展监测需求分析，如小汽车、公交车、自行车等流量、速度等候时间的监测需求。

4.2.3 能耗监测与分析

综合枢纽内部照明、空调、通风等设施设备使用水电气等能源的监测需求分析。

4.3 旅客出行服务需求

旅客出行服务需求分析应包括：综合客运枢纽中旅客出行导航、信息引导、全链条出行服务。

4.3.1 信息服务

围绕综合客运枢纽中旅客对出租车、网约车、公共汽电车、轨道交通、自行车等各种接驳交通和其它对外交通方式，以及枢纽进出口排队、停车等信息服务需求开展需求分析。

4.3.2 出行导引

在综合客运枢纽进出站区域、停车区、换乘大厅、换乘通道、换乘广场等主要决策点设置动态出行信息屏指引的需求分析，以及信息屏显示内容、分级指引、布设位置的需求分析。

枢纽室内导引服务建设需求分析，有必要建设时应补充出行导引内容、导引服务载体、功能要求等需求分析。

4.3.3 中转联程服务

围绕铁路客运、公路客运、航空客运、水路客运等对外客运方式之间，以及与城市轨道、市域铁路、城市轨道、需求响应公交、常规公交、出租汽车、网约车、停车服务等多种出行方式的出行信息服务、出行方案比较、路线规划、联程购票、一站支付、无感支付、一卡通行、一码通行等方面开展需求分析。

4.3.4 弱势群体服务

枢纽行动出行不便群体的综合信息服务需求分析，如无障碍设施指引、医疗服务指引以及求助信息通道等诱导需求。

4.4 一般运行管理需求

一般运行管理的需求分析应包括：综合客运枢纽业务管理、组织引导、人员通行、设施运维等的智慧化需求。

4.4.1 业务管理

综合枢纽内人员信息统计、财务分析、流程管理等业务系统的管理需求分析。

4.4.2 组织引导

综合枢纽内设置一定的组织引导设施以指引人、车按照制定流线流动的需求分析。

4.4.3 出入管理

围绕综合枢纽对人、车出入信息进行统计、分类、白黑名单等操作，以及严格实行人、车出入管理等方面开展需求分析。

4.4.4 设施运维

围绕综合枢纽对区域内的设施进行统一管理，对设施位置、运行状态、维保时间等进行建档，并结合设施状态实时进行运维等方面开展需求分析。

4.5 安全应急与协调管理

安全应急与协调管理的需求分析应包括：枢纽内安全安防管理、突发事件处置、预案管理、应急联动等。

4.5.1 安全安防管理

应在满足《中华人民共和国反恐怖主义法》等公安安全相关法规及当地有关部门要求的情况下，从枢纽安全高效运行的根本目的出发，考虑设备复用、降本增效、多网融合等多种因素，开展安全事件识别、安全风险量化评估、安检通关、枢纽智能巡检等方面的建设需求分析。

4.5.2 突发事件处置

针对大客流、火灾、爆炸等异常突发事件，围绕突发事件下客流、车流疏解特点识别，以及提前制定规范化的处置流程等方面开展需求分析。

4.5.3 预案管理

综合枢纽内各类应急预案进行电子化管理的需求分析。

4.5.4 应急联动

枢纽智慧化系统应与当地应急管理机构形成系统对接并支撑应急指挥联动的需求分析。

5 智慧化系统总体框架

5.1 设计原则

智慧化框架的设计应满足兼容性、拓展性、安全性、实用性等原则。

5.2 总体框架

枢纽智慧化总体框架由如图 1 所示的数字基础层、平台层、应用层、网络/信息安全保障体系、政策及标准规范体系、统一运维/统一运营体系等模块，以及各个模块所包含的系统、组件、设施、应用等组成。

图 1 综合客运枢纽建设技术框架模型

5.3 系统设计要求

5.3.1 系统性能

稳定性：系统正常工作时间占比应不小于系统运行时间的 99.9%，系统大面积功能故障的恢复时间应小于 30 分钟，页面报错、闪退、个别功能故障恢复时间应小于 10 分钟。

响应时间：桌面端和移动端等不同平台登录、查询、业务办理、导出的简单操作响应时间应不大于 3 秒。

用户数及系统并发要求：应对系统最大用户数进行设计评估，并至少具备设计用户数的 10%扩容承载能力，系统并发用户量应不低于设计最大用户数的 20%。

5.3.2 数据质量及交换

应保证数据在传输、存储等过程的安全，并对关键数据进行至少 1 份的备份。

应保证不同系统之间的数据交换、共享符合国家对数据安全、保密的要求，符合地方交换、共享的标准规范要求。

5.3.3 网络安全

网络信息安全应符合 GB/T 22239—2019 的相关规定。

5.4 外部系统对接

综合客运枢纽智慧交通管理系统应具备与智慧城市管理系统、公安信息化系统、交通信息系统、交警信息化系统等管理系统进行充分的数据与系统对接功能。

6 智慧化基础设施

6.1 智能基础设施

综合客运枢纽智能基础设施的组成包括但不限于智能客流监测设施、智能视频监控设施、智能环境感知设施、智能设备监测设施、智能终端以及其他智能基础设施。

6.1.1 智能客流监测设施

智能客流监测设施应满足下列要求：

1）应具备运营期间内对监测范围内的客流量进行实时监测功能。

2）应具备对各个客流检测设备点位信息的综合、统一控制管理功能。

3）客流监测设备及其控制系统应具备平滑、弹性扩容调整的能力。

4）应提供统一的通讯接口进行集成，并支持标准 IP 网络通信能力。

5）应提供设备健全管理、设备状态、信令、消息订阅等接口。

6.1.2 智能视频监控设施

智能视频监控设施应满足下列要求：

1）应支持摄像机的统一管理、视频图片存储和转发、点播、回放和权限管理等视频监控管理功能。

2）应支持将视频设备位置信息按照统一标准进行设置，以满足视频巡检等业务需求。

3）应具备在全天候不同光照水平、室内外不同温湿度环境下的可靠性。

4）应支持将多个视频融合拼接以反映全局整体态势的能力，支持将视频以及音频在实景图片的对映位置播放的能力，支持视频画中画类型的细节展现形式。

5）应支持将视频流在枢纽视频专网中直接传送的能力。

6）应支持将视频资源通过 GB/T 28181 协议与公安视频专网、上级管理部门等外部视频监控平台对接共享。

7）应结合业务需求在不同场景下能提供热成像能力、人脸结构化分析能力、人体结构化分析能力、车辆计数能力、车辆结构化分析能力、车牌识别能力、物品结构化分析能力。

8）视频监控设备及其控制系统应具备平滑、弹性扩容调整的能力。

9）应提供统一的通讯接口进行集成，支持标准 IP 网络通信能力。

6.1.3 智能环境感知设施

智能环境感知设备应当包括但不限于下列要求：

1）应支持对枢纽室外风向风速、室外温度湿度、室内各主要分区温湿度、亮度的实时监测。

2）应具备对各环境感知设备进行设备管理、连接管理、应用支撑及安全管理等功能。

3）应具备平滑、弹性扩容调整的能力。

4）应提供统一的通讯接口进行集成，支持标准 IP 网络通信能力。

6.1.4 智能设备监测设施

智能设备监测设备应当包括但不限于下列要求：

1）应支持对枢纽用水、用电、通信、存储、计算、消防、照明等设备运行状态、相关指标的实时监测。

2）应具备对各监测设备进行设备管理、连接管理、应用支撑及安全管理等功能。

3）应具备平滑、弹性扩容调整的能力。

4）应提供统一的通讯接口进行集成，支持标准 IP 网络通信能力。

6.1.5 智能终端

智能终端应满足乘客与相关的服务信息方互动，主要用于出入口以及换乘大厅为乘客提供线路引导、信息检索查询、枢纽运营公共信息、配合移动端应用程序互相联动，屏幕采用与周边空间环境相匹配的规格采用多点电容多点触摸方式配套硬件平台，实现与乘客互动所需的互动信息显示。

6.1.6 其他智能基础设施

其他智能基础设施应当在满足业务应用需要的前提下，满足但不限于下列要求：

1）应具备对各设备进行远程管理、连接管理、应用支撑及安全管理等功能。

2）应具备平滑、弹性扩容调整的能力。

3）应提供统一的通讯接口进行集成，对于不支持标准 IP 网络通信能力的，需支持部署具有边缘计算能力的网关。

6.2 网络传输设施

网络传输设施包括但不限于传输网络架构、固定通信网、无线通信网、物联接入网。

6.2.1 传输网络架构

1）传输网络应进行分级设计，根据规模可采用核心-接入两级架构或采用核心-汇聚-接入三级架构。

2）传输网络应根据功能划分进行分区，应包括但不限于核心交换区、管理区、接入区、服务区、出口区。

3）传输网络业务应识别优先级，并根据不同优先级对网络 QoS 业务保障提出设计要求。

4）传输网络包含的有线、无线各类网络应规划统一网管，实现统一的资源管理。

5）传输网络应采用冗余设计，对出口区、核心交换区应规划冗余的设备和链路，避免单点故障。

6）传输网络应具备统一的边界防护体系，保证外部进入信息的安全可靠。

6.2.2 固定通信网

1）固定通信网应考虑近期和远期的业务需求，选择合适的网络设备。网络带宽应支持高清视频流数据、图片数据、结构化数据的高并发和低延时传输。

2）核心交换机设备应满足可靠性要求，并采用双节点冗余设计；

3）接入层设备宜采用 POL 设备或框式交换设备，应满足可安装及日常维护要求；

4）接入层网络设备应具备满足不同终端带宽需求，接入设备应具备基础电信运营企业端口接入能力。

6.2.3 无线通信网

1）无线通信网包括移动通讯网和无线局域网，应覆盖主要的公共空间、换乘空间、办公空间，满足移动通信和无线热点覆盖的需求。

无线通信网规划应符合现行行业标准《移动通信基站工程技术规范》YD/T 5230 和国家标准《无线局域网工程设计标准》GB/T 51419 的规定。

无线通信网设备用最新的技术标准，应支持 5G、WiFi6 等通信技术。

无线通信网应确保不同无线业务的隔离与安全。

6.2.4 物联接入网

1）物联接入网应支持电力线载波网络、Wi-Fi、4G/5G、NB-IoT 等接入方式。

2）物联接入网应满足感知终端即插即用快速联网要求，可自动发现、自动识别感知设备。

3）应满足物联安全要求，对感知终端具备身份认证，对认证报文具备加密能力。

4）应具备感知终端接入与管理能力，宜实现感知终端的在线监测、故障预测告警等管理功能。

6.3 计算存储设施

计算存储设施包括但不限于边缘计算节点、本地计算、云计算等设施。

6.3.1 总体部署原则

计算存储设施总体上需满足以下要求：

1）计算存储设施所依托的软硬件资源，应符合国家有关部门对计算存储服务器产品、网络产品、网络安全产品等硬件产品的强制性要求。

2）云计算平台软件应基于业界主流架构，物理基础设施资源应由国产 X86 或 ARM 架构的服务器构

成，应支持通过云操作系统将 CPU、GPU、网络、存储等资源虚拟化，对外应能够提供计算存储资源池、虚拟机、容器、存储、运营运维等基础服务，同时 API 接口应具备兼容性及互操作性。

3）整体系统应采用分层和模块化体系架构，软硬件解耦，支持节点横向扩展，支持添加节点，支持单机扩集群。

4）应具备对现有硬件设备的兼容能力，实现充分利旧。

5）应支持节点高可用功能，虚拟化组件支持全容器化部署模式。

6）应能够自主控制系统与数据的迁移，提供多途径的系统与数据迁移服务；支持 P2P（物理机至物理机）、V2V（虚拟机至虚拟机）、P2V（物理机至虚拟机）或 V2P（虚拟机至物理机）。

7）应支持通过运维管理模块实现对云服务、硬件服务器、存储设备、网络设备统一管控，实现 IT 资源集中管控、运营运维。

6.3.2 云计算服务设施

计算服务设施则应当满足以下要求：

1）应支持多种计算资源（通用服务器、ARM 服务器、通用/嵌入式 GPU 服务器、裸金属）的统一接入管理并提供虚拟化服务。

2）应支持对虚拟机的生命周期进行管理，包括创建、批量创建、调整规格、启动、关闭、重启、挂起及恢复、暂停、取消暂停、编辑修改、删除、批量删除、重建及控制台等功能。

3）应支持在线虚拟机迁移，支持虚拟机跨不同类型主存储的在线迁移。

4）应支持虚拟机的冷迁移功能。

5）应支持在线修改虚拟机规格，包括 CPU、内存、磁盘和网卡。

6）应支持虚拟机卡死及蓝屏的检测功能，并自动重启。

7）应支持创建虚拟机时导入用户自定义数据和云虚拟主机秘钥，包括对云虚拟主机做定制化配置或完成特定运维任务等。

8）虚拟机应可实时接入或转发前端视频。

9）应支持对虚拟机的快照进行统一管理，支持可视化界面进行快照查看、删除、创建、恢复和策略编辑等操作，执行快照时虚拟机业务无中断。

10）应支持基于特定的虚拟机实例创建自定义镜像，并可基于自定义镜像创建新的虚拟机。

11）应支持为虚拟机添加云硬盘，可调节云硬盘大小、更新云硬盘状态，支持对云硬盘进行备份。

12）应支持虚拟化资源池网络资源信息的概况和展示，查看平台网络拓扑图。

13）应支持 VPC 服务，支持通过 VPC 机制为租户提供的独享的虚拟网络。支持为应用提供独占的网络容器，支持租户自助创建、配置 VPC 资源。

14）应支持弹性 IP 服务，支持将公网 IP 地址和 VPC 内的虚拟机绑定。支持用户自助进行弹性 IP 的申请、绑定、解绑定、释放等操作。

15）应支持虚拟机网络负载均衡，支持创建、删除、更新负载均衡设备，查看已有负载均衡设备的信息，为虚拟机绑定或解绑浮动 IP。

16）应支持 K8S（Kubernetes）容器集群生命周期管理，通过向导式配置，以全虚拟机、全裸金属

以及混合部署的形态，快速构建 K8S（Kubernetes）容器集群。

17）应支持对创建 K8S 集群的虚拟机或者裸金属资源规格配置进行设置（vCPU/CPU、内存、存储），支持虚拟机和裸金属方式的配额管理。

18）应支持通过云平台容器服务，全容器化部署大数据服务，裸金属服务统一管理大数据服务的裸金属资源。

19）应支持裸金属服务器的生命周期管理，操作包括注册、纳管、加入/移出裸机池、部署、释放、删除。支持单个/批量开机、关机、重启，并支持操作系统重新部署、重置密码、导出列等。

6.3.3 云存储服务设施

存储服务设施则应当满足以下要求：

1）应支持接入多种存储后端（IP-SAN、FC-SAN、CEPH、本地）并统一管理。

2）应支持 IP-SAN、FC-SAN 存储部署方式，支持存储双控双活。

3）应支持 CEPH 分布式存储部署方式，CEPH 存储采用 Linux 存储专用操作系统，支持控制器架构，控制器可支持热插拔，单控制器支持双系统应用。

4）应支持分布式块存储技术，支持根据数据对象的重要性、访问频率等属性按照预先设定的分层存储区域自动分层存储。

5）应支持云硬盘创建、编辑、扩容和删除；支持对云硬盘进行备份及恢复操作。

6）应支持云硬盘快照，当已创建快照的云硬盘出现问题时，可通过快照快速恢复到未出问题时的状态。

7）应支持云硬盘集群外备份，将云硬盘数据全量备份到集群之外的 NAS 服务器，即使集群异常，云硬盘备份的数据也能保全。

8）应支持云硬盘创建在宿主机自身系统盘、IP-SAN、CEPH 存储池；支持云硬盘跨多种后端存储使用，云硬盘支持挂载到位于本地存储、IP-SAN、CEPH 存储上的虚拟机；支持云硬盘随虚拟机一起热迁移和冷迁移。

9）应支持通过对象存储服务控制台进行创建、编辑、删除存储空间，支持存储空间列表展示和基础信息概览展示。

10）应支持通过 http/https 协议方式和域名方式对对象存储空间进行操作。

11）应支持通过 OSS 和 S3 协议对对象存储空间进行对象存储功能操作。

12）应支持对用户使用的对象存储资源进行按量计费并生成费用清单，并支持以图表的形式展示费用趋势、资源使用趋势。支持根据资源类型展示单个/所有用户的资源消费明细。

13）数据应支持多副本，每个副本分布在不同节点，数据分片在资源池内，硬盘故障，全局参与重建。

14）应支持纠删编码、副本、故障域数据冗余保护机制，保障磁盘级别、节点级别、机柜级别、数据中心级别的数据安全性。

6.3.4 计算、存储设施运营维护

计算、存储设施的运营、维护应满足以下要求：

1）用户首次登录系统，必须创建新密码，应支持密码安全级别校验。

2）应支持提供资源使用情况和资源使用详细清单。

3）应支持统计云平台管理的租户用户数量、虚拟机数量、裸金属服务器数量、容器 K8S 集群数量、云硬盘数量、对象存储 Bucket 数量、浮动 IP 数量等指标。

4）应支持租户管理，包含：租户审核、配额管理、权限管理等。

5）应支持环境管理，可以创建多个区域、可用区。

6）应支持多用户的管理，支持多用户并发登录操作。

7）应支持宿主机性能监控数据图形化展示。

8）应支持裸金属物理服务器性能监控数据图形化展示。

9）应支持虚拟机性能监控数据图形化展示。

10）应可对监测项设置告警等级、告警参数，开启和关闭监测项、告警通知，告警方式应包括 Email、短信和界面显示。

11）应支持以图形化展示告警情况和告警信息，管理员用户可查看所有告警信息，并可按照告警源类型、告警等级、触发时间、告警状态和起止时间查询告警信息。

12）应支持自动对平台服务异常、数据库异常、资源消耗异常、设备宕机等多种故障进行自我诊断，并可按照设定的恢复策略进行恢复。

13）应支持系统健康巡检，并支持巡检报告结果导出。

14）应支持在可视化的 WEB 管理平台上查看虚拟分布式存储对应的容量大小、容量使用率、实时的 IOPS 读写次数、IOPS 读写数据量等信息。

15）应支持对频繁上报的同一个告警信息进行分析过滤，经过告警分析规则的过滤后，支持在指定时间后再一次上报到运维平台。

16）应支持对租户配额进行监控，当容量不足时可进行告警。

17）应支持对租户云资源用量（虚拟机数量、云硬盘数量、容器集群、对象存储、裸金属服务器、浮动 IP 等）进行监控，实时了解用户使用量。

7 智慧化支撑平台

7.1 数据服务平台

数据服务平台的技术要求包括数据标准、数据接入、数据处理、数据组织、数据服务、数据治理、算法仓库、数据安全等。

7.1.1 数据接入

应根据业务需求接入数据，提供数据流转机制，根据数据情况，将数据接入到数据中心，完成与数据提供方的数据对账。

7.1.2 数据处理

数据处理主要包括数据提取、数据清洗、数据关联、数据比对、数据标识和数据分发。数据处理过程中的技术要求如下：

1）应提供数据批处理与流计算任务，用于满足模型开发需求。

2）应支持不同的数据类型任务。

3）应支持不同的输入输出数据源类型，包括但不限于 MySQL、Postgresql、Oracle、sqlserver、kafka、kudu、cassandra、elasticsearch、mariadb、mongoDB。

4）应支持 DDL 建表服务。

5）应支持任务自定义函数处理。

6）应支持模型管理的功能。

7）应支持算法包管理、算法包分组和算子管理。

8）应支持数据处理过程易用、可展示需求等。

7.1.3 数据组织

应按照数据定义的标准统一流程规范的组织方案，实现数据资源分类建库。

数据组织应包括但不限于构建原始库、资源库、主题库、知识库、业务库、业务要素索引库等。

7.1.4 数据服务

数据服务包括以下内容：

1）查询检索：此类服务包括数据资源情况和查询检索接口、以及各类结构化和非结构化数据的查询检索接口，应支持返回数据统计汇总信息、判定查询关键词（实体）是否命中的信息，以及数据摘要或明细信息。

2）比对订阅：比对订阅服务是针对一种或多种动态活动开展的信息订阅业务。

3）模型分析：指根据业务需要，对数据进行统计、分析、规律性探索、预测等，并返回结构，以支撑应用功能层业务场景复杂、多变的需求。

4）数据推送：是各个部门间进行数据交换和信息推送的基础核心能力。

5）数据鉴权：基于数据的访问控制规则，实现数据的访问权限鉴别的过程。

6）数据操作：指数据及数据表的增加、删除、修改等操作接口服务。

7）数据管理：指按需将数据治理和数据服务的能力进行接口封装，为其他应用系统、平台内其他子系统提供服务。

7.1.5 数据治理

数据治理主要包括数据资产管理（如数据资源目录、数据血缘）、数据安全管理（数据分级分类）、数据开发管理（模型管理、标签管理）、数据质量管理和数据运维管理等内容。

7.1.6 算法仓库

算法仓库应提供统一的算法集成和调度框架，并提供算法包与算法系统接入的标准方式。具备智能算法调度引擎，提供多算法快速接入方式。具备对不同业务场景算法的统一管理与调度能力，具备根据计算资源池进行按需、灵活的算法调度能力。

7.1.6.1 算法仓库功能

1）算法上传与下载

应支持上传新的算法，可对算法进行断点续传并查看上传进度。上传成功后应支持对算法进行文件校验和解析，提取出算法的基本信息（厂商、适用平台、版本、算法功能等）进行入库保存。

应提供算法下载和分发能力，支持对前端、后端分析设备下载算法。

算法下载并发量大时，应支持对算法下载并发的控制。针对系统组件的不稳定性和网络的不稳定等问题，应支持对算法包下载断点续传。

2）算法基础管理

应支持根据算法名称、算法功能名称、创建人、创建时间、目标类型、所属行业、所属场所等条件检索，检索出的算法应支持查看详情。算法仓库应支持对算法基本描述信息的维护编辑，支持对算法的删除，支持对算法功能进行下架操作。

3）算法标签管理

应提供算法标签的标签管理功能，包括算法标签的新增、删除、修改，算法标签的分类。支持默认标签的初始化导入，算法打标签、算法删除标签、按标签搜索算法等功能。

4）算法功能展示

算法功能展示是以算法功能为单位，展示算法仓库内提供的全部能力，并应支持从各个维度展现算法仓库的统计数据。

7.1.6.2 算法结构标准

1）算法包结构

算法包的应提供动态库目录、模型目录、配置文件目录和算法描述文件，并封装提供。

2）算法结构化描述建议字段表

算法结构化描述建议字段表参见详见附表一。

7.1.6.3 第三方算法接入标准

算法仓库应具备第三方算法接入能力，具体通过定义算法包规范来实现第三方算法包的接入。算法包的规范应当遵守算法包结构的规定；应当遵守算法包结构化描述文件字段和格式的规定；算法文件应统一接口。

7.1.6.4 算法仓库级联

算法仓库应支持上级算法仓库从其他的多个下级仓库拉取算法，或者向多个下级仓库推送算法；应支持从老版本的仓库向新版本仓库拉取算法；应支持从其他平台按照用户同步算法到算法仓库。

7.1.7 数据安全

枢纽数据安全应当具备有效的防止在全生命周期中，由于硬件故障、断电、死机、人为的误操作、程序缺陷、病毒或黑客等原因造成的数据库损坏、数据丢失以及某些敏感或保密的数据、模型、算法被不具备资格的人员获取的能力。

7.2 基础信息及管理平台

7.2.1 视频管理子平台

7.2.1.1 视频设备治理

应对视频前端设备进行统一标准命名、编辑属性信息、赋予空间位置信息等点位资源治理。包括但不限于治理清单管理、设备空间信息治理、设备场所类型标定、室内外标定、设备关联关系标定、勘误上报管理、批量关联管理、设备坐标系转换、场景画面标定。

7.2.1.2 视频资源调度

视频资源调度应实现视频资源、存储资源、计算资源、视频算法分析任务管理调度等各类资源的统一管理。

7.2.1.3 视频接入管理

对枢纽已建、新建的视频设备应当进行统一接入管理。

7.2.1.3.1 直接接入

对于新建视频设备的应采用 GB/T 28181 国标协议接入，已建的视频设备应首先考虑采用 GB/T28181 国标协议接入，其次考虑采用 ONVIF 协议接入，也可以根据点位实际重要性，采用点位改造替换或者采用 SDK 开发接入。

7.2.1.3.2 级联接入

对于视频设备已形成平台的，如需进行资源对接，应满足 GB/T28181 的标准要求。

7.2.1.4 视频计算存储资源池

7.2.1.4.1 视频通用计算资源池

应建立专用于视频存储、分析的通用计算资源池，提供可靠、稳定、灵活的基础计算能力。

7.2.1.4.2 视频智能计算资源池

对需要使用视频进行智能分析的，应当建立智能计算资源池，实现对 GPU 服务器资源进行统一管理。

7.2.1.4.3 视频通用存储资源池

应当通过存储虚拟化技术构建统一、可靠、大容量的通用存储资源池，用于存储视频前端设备及视频分析后产生的非流式对象数据。

7.2.1.4.4 视频流式存储资源池

应当通过集群化、离散化、负载均衡管理等技术，构建高稳、高效、高能的视频流式资源存储池，并提供对流式对象的海量存储服务能力。

7.2.1.5 视频资源管理规则

7.2.1.5.1 视频资源描述规则

应对视频点位进行统一的资源描述，具体描述规则参见附表二。

7.2.1.5.2 视频资源使用管理

视频资源的共享开发及智能分析应当安全、可控，并建立视频资源使用管理规范。规范应当包括但不限于视频资源申请、受理、授权、答复的流程，视频资源使用权限管理、使用范围管理、协商监督机制、安全保密机制。

7.2.1.5.3 视频分析智能算法接入流程

视频的分析智能算法应当具备可迭代、可拓展的特性，对后期导入的智能算法应当参照算法仓库中对算法标准规范的要求。

7.2.2 物联设备管理

7.2.2.1 物联设备点位治理

应包括但不限于为所有物联设备进行唯一编号，并打上设备类型、管理部门、设备位置等标签信息，并提供基于物联设备标签信息的搜索功能。

7.2.2.2 物联设备运行状态反馈

应能汇聚枢纽各类物联设备运行状态数据，并能根据状态数据，对异常状态进行反馈、跟踪。

7.2.2.3 物联设备采集信息分类汇聚

应能汇聚枢纽各类物联感知设备采集的感知数据，并能根据感知数据，对异常状态进行反馈跟踪。

7.2.3 集成展示平台

应当为枢纽建立统一的集成展示平台，作为集成、融合、发布、维护枢纽空间资源的载体，并为枢纽智慧化体系中各个系统提供标准空间信息服务。

7.3 技术使能平台

技术使能平台包括人工智能算法子平台、视频管理、BIM 平台、物联设备管理、集成展示、交通动态推演仿真等共用能力，并具备与枢纽 BIM 子平台互联互通的能力。

7.3.1 算法子平台

提供面向枢纽各项业务、各类场景的通用业务算法、人工智能算法、统计分析算法等各项能力。

7.3.2 交通仿真推演子平台

建立枢纽交通仿真推演子平台，提供适应枢纽日常态集疏运和应急态疏散下的客流组织、仿真预案演练、仿真结果评估等能力，辅助支撑制定枢纽集疏运管理策略。

7.4 应用支撑

7.4.1 统一门户服务

1）统一门户服务提供统一入口，应支持统一鉴权。

2）应支撑页面集成、功能集成、应用集成，统一各模块风格。

3）应适配各类浏览器。

4）应具备图表等数据展示、消息等功能。

7.4.2 权限管理服务

1）权限管理服务支撑系统对用户、角色、组织、全局配置，应包括但不限于信息的增、删、改、查功能。

2）权限管理服务应支撑对不同角色权限的全局配置，应包括但不限于功能权限、数据权限、API接口权限的增、删、改、查。

7.4.3 集成管理服务

1）集成管理服务支撑系统间的集成通讯，应包括但不限于数据集成、API 集成、消息集成。

2）数据集成支持从各种异构数据源提供数据同步功能，应支持跨网络的数据同步。

3）API 集成提供 API 接入开放网关，应支持 API 的注册、发布、路由、流控、升降级和接入认证等能力。

4）消息集成支持跨网络消息中间件，应支持消息的发布与订阅，提供消息的发布、订阅、存储、传输功能。

8 智慧应用

8.1 枢纽综合运控应用

8.1.1 交通态势综合感知

态势综合感知功能主要包括：图像监测与分析、客流监测与分析、载运工具监测与分析。

8.1.1.1 图像监测与分析

1）应实现综合客运枢纽内公共区域和重点作业区域的图像监控，应覆盖以下区域：安检区、售票区、候车区、换乘区、行李托运区、重要设备区、主要通道、楼梯口、停车场、枢纽出入口相连道路、

人行天桥及桥梁。

2）应实时监控综合客运枢纽内乘客安检、候乘等秩序情况，以及踩踏等异常事件。

3）应实时监控进出综合客运枢纽的火车、长途客运车辆、船舶、飞机、公共汽电车、城市轨道交通车辆、出租车以及其他运输工具的通行秩序，以及违停、碰撞等异常事件。

4）应对综合客运枢纽内及可能影响综合客运枢纽正常运行的周边区域的异常事件进行实时监测和预警。

5）应对综合客运枢纽内视频图像等非结构化数据统一管理和存储，视频图像存储应符合 GB/T 20090.2-2013 的相关规定。

8.1.1.2 客流监测与分析

1）应对综合枢纽集疏运体系的整体客流监测，包括集疏运道路车流、轨道交通、常规公交客流、出租车网约车到达离开情况等。

2）应实现综合客运枢纽内主要区域和周边重要区域的客流监测，应涵盖以下区域：出入口，上/下客通道、换乘区、售票区、安检区。

3）应实现客流数量和方向的采集。

4）应实现综合客运枢纽内客流拥挤等异常事件的自动监测与报警，如突发聚集、逆行。

5）应实现综合客运枢纽内、重点区域、重点断面的客流统计、分析、查询，能生成相应的客流分析图表。

6）应实现对客流数据按时间、空间、交通方式的预测功能。

7）应实现客流枢纽整体客流 OD 的运行分析，提供更为精准的对外客流出行习惯、进出站特征和站内衔接分析。

8.1.1.3 载运工具监测与分析

1）应实现对进出综合客运枢纽载运工具的实施监测，包括载运工具标识和数量。

2）应实现对进出综合客运枢纽的各类载运工具整体运行状况及异常事件的监测与报警功能，如长时间滞留、逆行等。

3）应实现对进出综合客运枢纽的各类载运工具整体运行信息汇总、统计和查询，并能够输出数据。

8.1.2 运力协同调度

应具备公共汽电车、出租车、网约车、轨道交通的运力协同、调度指令统一下发的功能。

8.1.3 客流疏解预案管控

应提供对应急预案的结构化、电子化存储及编辑功能。

应提供不同客流强度、应急疏散等场景下的疏散预案，提供预案编辑、业务协同、信息发布、事件分拨等能力。

应提供客流疏解预案仿真演练能力，提供仿真预案信息管理、参数配置、指标输出与结果评估等能力。

应提供对疏解预案执行效果的评估能力，输出客流疏散时间、排队长度、疏散速度、交通方式占比等指标。

8.1.4 设施设备运行监测

应实现与客运枢纽建筑门禁、楼宇自控和消防报警等基础弱电系统的数据对接，实现对基础弱电设施设备以及可能影响枢纽正常运行的其他设施设备工作状态的实时监测。

8.2 旅客出行服务应用

8.2.1 信息导引

应以电子信息屏的形式，按照分级信息指引的原则，对出租车、公交车、轨道交通等的接驳区域、步行距离、发车时间、预计排队时间、现场排队情况信息进行分层级、动态展示。

应提供枢纽内购票区、服务台、安检区、候车区、行李托运区、重要设备区、枢纽出入口、楼梯口、接驳区、停车场、购物、餐饮等区域的室内外一体化出行导引服务。

应满足于乘客与相关的运营信息互动，线路引导、信息检索查询、枢纽运营公共信息查询、并配合移动端应用程序互相联动。

8.2.2 移动服务端

应提供 APP、小程序或者公众号的移动服务端，面向出行者提供枢纽对外交通、枢纽接驳城市公共交通、出租汽车、网约车、公共停车、导航服务等一体化信息服务，宜提供多种出行方式换乘衔接时刻表服务、联程购票服务、室内外一体化导航服务等一站式查询、支付服务。

8.2.3 智慧停车

应根据枢纽停车运行服务特征，提供客运枢纽预约停车、车位导航、反向寻车、在线缴费、停车信息发布等功能。

8.3 安防类应用

枢纽安防类应用包括但不限于以下方面。

8.3.1 枢纽安防状态综合监测

应提供枢纽安防相关信息数据统一汇聚能力，将枢纽各安防子系统（包括但不限于视频监控子系统、安全检查与探测子系统、入侵报警子系统、进出口及直梯权限管理子系统等）状态数据汇聚展示。

8.3.2 枢纽安全风险趋势评估

应结合空间地理信息数据对综合换乘大厅、停车场、商业综合体、公寓、办公楼等枢纽功能分区，

进行风险类别（设备、环境、消防、人员、车辆等）的实时监控，形成各分区的风险量化指标，并根据风险值对各分区进行风险分级（重大风险、较大风险、一般风险、低风险）。

8.3.3 安防资源管理

应实现对安防基础数据（人员/车辆/设备等）、用户权限、安保区域等基础数据的统一管理。

8.3.4 安防综合管控

8.3.4.1 事件联动

应通过开放的规则定义实现场景化的事件应用，支持事件处置流程自动化，实现在“特定条件”下执行“特定动作”。

8.3.4.2 图上监控

应在地图上展示各类资源点的地理位置，通过接收事件服务中资源点的报警事件，实现报警信息的可视化。

8.3.4.3 智能监控

应具备人脸识别能力，通过前端视频和后端比对分析设备，对人脸、人体、车辆进行抓拍、分析和应用。

8.3.4.4 融合监控

应融合监控可同时汇聚监控视频、门禁、停车场出入口等信息，并根据需要对多种设备同时进行控制。

8.3.5 安防视频监控

应对枢纽室内全部区域、室外重点区域（室外停车场、出入口、人行通道等）实现视频监控的全覆盖，并能对前端编码设备、后端存储设备、中心传输显示设备、解码设备的集中管理和业务配置，实现视频安防设备接入管理、实时监控、录像存储、检索回放、智能分析、解码上墙控制等功能。

8.3.5.1 视频设备管理

视频设备管理主要包括视频的编码设备、监控点、报警器的管理，应包含对视频资源的增删改查等操作。

8.3.5.2 视频监控配置

视频监控配置包括视频预览、录像计划、抓图计划、事件布撤防及通用参数的配置，应通过各参数的配置，达到预览回放等相关业务的实现。

8.3.6 智慧安检

安检子系统应当具备对人、物的智慧安检能力，包括但不限于对过检包裹的图片、视频具备智能识物能力，对过检人员具备人脸识别及测温能力。

8.3.7 周界入侵防范

应当具备对枢纽内部禁止区域侵入、枢纽地面周界侵入、区域上空无人机侵入等入侵行为的实时监控、识别能力。

8.3.8 异常事件识别

应当具备对枢纽内对公共安全、环境安全、消防安全、运营安全有影响的各类异常事件（如人员行为异常、人员滞留、人员高频出入、扶梯运行异常、物品遗留异常、通道异常堵塞、环境温度异常、区域入侵异常、区域音量异常等）的监测、识别能力。

8.3.9 进出口及直梯智慧控制

应为枢纽内部需要权限控制的进出口、通道、直梯配备安全控制系统，提供人脸、指纹、刷卡、扫码等多种验证方式，并将门禁、梯控与巡更、考勤、食堂消费、员工日常测温等功能融合。

8.3.10 视频远程巡检

视频远程巡检应当提供视频巡检、全景巡检、实景巡检等多种方式，并可实现巡检计划在线编排，形成巡检日志。

8.3.11 高空抛物监管

对于上盖高密度开发的枢纽应当具备高空抛物监测功能，并具备全天候抛物轨迹还原、楼层计算、快速定位能力。

8.3.12 防疫测温

枢纽防疫测温应当对枢纽进出口实现测温全覆盖，并通过在枢纽关键区域的测温覆盖，实现进出枢纽及枢纽内部人员体温无异常。

8.3.13 在线巡检

在线巡检功能应按照巡查流程，可对巡检过程和结果进行线上管理。同时，在关键巡查点提供人脸、刷卡、二维码、RFID 等多方式打卡形式。

8.3.14 报警管理

报警管理功能应能接入报警主机、动环主机、紧急报警设备、智慧消防设备，对枢纽各重要区域进行防区布防和对环境量监控，并应具备安防系统联动消防系统的能力。

8.3.14.1 入侵报警

入侵报警系统应能感知枢纽指定范围内的入侵行为或意外事件。

8.3.14.2 紧急报警

枢纽内部公共区域应当提供紧急报警手段，并在枢纽设立接警控制中心，对接枢纽公安，处理突发的紧急事件、紧急求助，完成报警求助接警。

8.3.14.3 动环检测

枢纽设备机房、枢纽建设工地或枢纽上盖楼宇等环境量变化影响较大区域，应当提供动态环境监控能力，实现目标地点的环境变量监控。

8.3.14.4 安消联动

枢纽消防管理应提供消防设施、通道的运行状况监控能力。枢纽综合安防系统应具备安消联动能力，辅助远程指挥与疏散调度。

8.3.15 商业经营安全监管

对于枢纽商业，应具备从装修到日常运营的安全监管能力。

9 网络安全保障

9.1 基础环境安全

应符合 GB/T 22239—2019 中 8.1 的要求，并满足下列要求：

9.1.1 安全物理环境

9.1.1.1 物理位置选择

物理位置选择应符合下列要求：

1）应避免将机房场地设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

2）应避免将机房场地设在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

9.1.1.2 物理访问控制

应对出入机房的外来人员进行身份核实，并记录外来人员身份信息、联系电话、接待人、时间等详细情况。应采用监控设备对机房人员进出情况进行实时监控。

9.1.1.3 防火

应在机房及相关的工作房间和辅助房间采用具有耐火级别的建筑材料，配备符合消防管理要求的灭火设备。

9.1.1.4 防水和防潮

应对穿过机房墙壁和楼板的水管增加有效所防护措施，机房屋顶和活动地板下铺有水管的应采取防护措施。

9.1.1.5 温湿度控制

应在机房设置温、湿度自动调节设施，使机房内的温度和湿度的变化在设备运行所允许的范围内。建议机房温度范围 23±1℃，湿度范围 40%-50%。

9.1.2 安全通信网络

9.1.2.1 网络架构

网络结构应符合下列要求：

1）应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要，建议在平峰业务情况下 CPU、内存等占用率不高于 60%。

2）应保证传输线路网络的带宽满足业务高峰期需要；建议在平峰业务情况下带宽占用率不超过 60%。

3）应根据业务职能、重要性和所涉及信息的重要程度等因素。并为各网络区域分配地址，应通过有效措施对各网络区域进行技术隔离。

4）应提供通信链路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性，与其他平台通信应采用双机热备。

5）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。如与互联网应用存在数据交换，应通过设置网闸或者防火墙方式实现隔离。

9.1.2.2 通信传输

通信传输应符合下列要求：

1）应采用校验技术或密码技术保证通信传输过程中数据的完整性，不宜采用 UDP、FTP 协议；各个专线链路应支持统一可视化管理。

2）应采用符合国家密码管理局相关规范要求的密码算法保证通信过程中的保密性。

9.1.3 安全区域边界

9.1.3.1 边界防护

边界防护应符合下列要求：

1）互联网边界应部署具备状态监测功能的安全设备。

2）应对无线网络的移动通讯网和无线局域网进行管控，保证无线网络通过受控的边界防护设备接入内部网络。

3）对不同网络安全等级系统、不同业务系统、不同区域之间的互操作、数据交换和信息流向进行严格控制。建议采取措施限制数据从高网络安全等级系统流向低网络安全等级系统。

4）应对未授权设备进行动态检测及管控，只允许通过运营者自身授权和安全评估的软硬件运行。

9.1.3.2 访问控制

范围控制应符合下列要求：

5）应优化防火墙等安全设备的访问控制列表，删除多余或无效的访问控制规则，使访问控制规则数量最小化。

6）应在网络出口和核心网络进行网络质量保证和网络连接数量限制。

9.1.3.3 入侵防范

入侵防范应符合下列要求：

1）应在关键网络行点处检测、防止或限制从外部发起的网络攻击行为，包括但不限于端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等行为。

2）应在关键网络行点处检测、防止或限制从内部发起的网络攻击行为，包括但不限于端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等行为。

9.1.3.4 恶意代码防范

应在网络中部署恶意代码防范功能的设备（如边界防火墙增加防病毒模块等）对恶意代码进行检测和清除。

9.1.3.5 安全审计

安全审计应符合下列要求：

1）应启用网络、服务器、中间件、数据库、终端及应用等计算设备安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；系统不支持该要求的，应采用第三方安全审计产品。

2）应将审计日志留存时间应符合相关要求。并且系统图像存储时间应不少于 30 天,涉及重大事件的录像应永久保存;相关业务数据存储时间应不少于 5 年;警情信息存储时间应不少于 1 年,录音文件的存储时间应不少于 6 个月。

9.1.4 安全计算环境

9.1.4.1 身份鉴别

身份鉴别应符合下列要求：

1）应对登录网络、服务器、中间件、数据库、终端及应用等计算环境的用户进行身份标识和鉴别，且保证用户名具有唯一性。

2）应采用由大小写英文字母、数字、特殊字符 3 种以上组成、长度不少于 10 位，每 90 天更换的用户口令。

3）应启用登录失败处理功能，登录失败后采取结束回话、限制非法登录次数和自动退出等措施，如连续 5 次登录失败锁定 10 分钟。

4）应采取 SSH、HTTPS 等方式进行远程管理，防止管理数据、鉴别信息在网络传输过程中被窃听。

5）应明确重要业务操作或异常用户操作行为，并形成清单。

9.1.4.2 访问控制

访问控制应符合下列要求：

1）应对登录网络、服务器、中间件、数据库、终端及应用等计算环境的用户分配账户和权限。

2）应通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度至少为用户组。

9.1.4.3 安全审计

安全审计应符合下列要求：

1）应启用网络、服务器、中间件、数据库、终端及应用等计算设备安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。系统不支持该要求的，应采用第三方安全审计产品。

2）应将审计日志留存时间应符合相关要求。并且系统图像存储时间应不少于 30 天，涉及重大事件的录像应永久保存；相关业务数据存储时间应不少于 5 年；警情信息存储时间应不少于 1 年，录音文件的存储时间应不少于 6 个月。

9.1.4.4 入侵防范

入侵防范应符合下列要求：

1） 应将服务器、终端等遵循最小安装的原则，仅安装需要的组件和应用程序。

2） 应采用受控方式对接入服务器、终端的移动介质进行管控。

3） 应定期开展漏洞扫描工作，及时发现可能存在的漏洞，并在经过充分测试评估后，及时修补

漏洞。

4） 应具备系统主动防护能力，及时识别并阻断入侵和病毒行为。

9.1.4.5 恶意代码防范

应采用具有与网络防恶意代码产品不同的恶意代码库，支持防恶意代码统一管理、升级、检测和查杀的主机防恶意代码产品。

9.1.4.6 数据完整性

应采用符合国家密码管理局相关规范要求的密码算法。

9.1.4.7 数据保密性

应采用符合国家密码管理局相关规范要求的密码算法。

9.1.4.8 数据备份恢复

应提供关键业务数据、服务支持数据、重要个人数据等的本地数据备份与恢复功能，每周至少进行一次全备份，每天进行增量备份。

9.1.4.9 个人信息保护

参照本文件第 9.7 章节进行体系化建设。

9.1.5 安全管理中心

9.1.5.1 系统管理

应对系统管理员、审计管理员、安全管理员进行身份鉴别，只允许其分别通过特定的命令或操作界面分别进行系统资源配置、安全审计、安全策略配置操作，并对这些操作进行审计。

9.1.5.2 集中管控

集中管控应符合下列要求：

1）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测分析，对异常情况进行告警。

2）应使用自动化工具来支持系统账户、配置、漏洞、补丁、病毒库等的管理。对于漏洞、补丁，应在经过验证后及时修补。

9.2 云计算环境安全

应符合 GB/T 22239—2019 中 8.2 的要求，并满足下列要求：

9.2.1 物理环境安全

部分系统部署在私有云平台（含虚拟化资源池）或公有云平台（含专属云平台）应遵循云安全扩

展要求。使用公有云平台应确保其云计算基础设施位于中国境内，并提供高于系统等级的备案证明。

9.2.2 通信网络安全

9.2.2.1 网络架构

网络架构应符合下列要求：

1）应能够提供虚拟网络之间的隔离能力，提供按需配置通信传输、边界防护、入侵防范等安全机制的能力。

2）应允许接入第三方安全产品或服务。

9.2.3 安全区域边界

9.2.3.1 访问控制

访问控制应符合下列要求：

1）应采取措施保证虚拟机无法通过网络非授权访问宿主机。

2）应在虚拟化网络边界（云平台与其他计算环境、虚拟子网与虚拟子网间）部署访问控制机制，设置访问控制规则。

9.2.3.2 入侵防范

入侵防范应符合下列要求：

1）应能检测到内部虚拟机发起的或者针对虚拟网络节点的网络攻击行为，并记录攻击类型、攻击时间和攻击流量等。

2）应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量，并进行告警。

9.2.3.3 安全审计

应对通过云平台对应用系统和数据进行的操作进行审计。

9.2.4 安全计算环境

9.2.4.1 访问控制

应允许设置不同虚拟机之间的访问控制策略。

9.2.4.2 数据完整性和保密性

应采用符合国家密码管理局相关规范要求的密码算法。

9.2.4.3 数据备份恢复

数据备份恢复应符合下列要求：

1） 应保证业务应用和数据存储在若干个可用的副本，各副本之间的内容应保持一致。

2） 应为业务系统及数据迁移到其他云计算平台和本地系统提供技术手段。

9.3 物联网安全

应符合 GB/T 22239—2019 中 8.4 的要求，并满足下列要求：

9.3.1 安全物理环境

应具备防水、防潮、防尘设计，防护等级应不低于 IP55。

9.3.2 安全区域边界

9.3.2.1 接入控制

应为计算设备和通信设备提供设备认证能力，保证只有授权的设备可以接入。

9.3.3 安全计算环境

9.3.3.1 设备安全

设备安全应符合下列要求：

1）设备的合法用户应具有统一的用户标识、不得使用默认口令，使用具有一定复杂度的用户口令（用户口令须由大小写英文字母、数字、特殊字符 3 种以上组成、长度不少于 8 位），90 天进行更新，具有登录失败和登录超时处理功能，连续 5 次登录失败锁定 10 分钟。

2）应启用 SSH、HTTPS 等管理方式进行远程管理，加密管理数据、鉴别信息，防止被网络窃听。

9.4 工业控制系统安全

应符合 GB/T 22239—2019 中 8.5 的要求。

9.5 大数据环境安全

应符合 GB/T 22239—2019 中附录 H 的要求。

9.6 数据安全保障措施

9.6.1 范围

数据安全范围应包括路况信息、管控信息、营运信息、业务调度等业务处理活动所产生或收集的数据。

9.6.2 基本要求

应符合下列要求：

1）进行数据处理活动的基础网络环境以及承载业务数据的应用系统应满足本文件第 9.1 章节至第 9.4 章节安全保障的要求。

2）在中华人民共和国境内采集和生成的各类数据须在境内存储。因业务需要，确需向境外提供的，应获得数据所有者同意，并遵循国家和有关部门的相关规定和技术标准进行出境安全评估和审批。

3）应识别业务活动涉及的数据，形成数据保护目录，并对数据进行分级分类保护。个人信息的识别以及保护要求见本文件第 9.7 章节“个人信息保护要求”。

9.6.3 数据生命周期安全

应符合下列要求：

应根据国家与行业相关数据管理法律、法规、规范的要求，建立覆盖数据全生命周期的安全保障体系，防范和控制数据处理的风险，数据生命周期的各阶段可参考 GB/T 37988-2019 第 5 章节。

针对业务数据全生命周期采取必要措施，数据安全保障措施宜包含以下内容：

1）数据采集阶段

数据采集应当遵循合法、正当、必要原则，按照法定范围和程序，明确采集数据的范围、目的和用途，规范数据格式，同时采取必要措施，保证采集数据的真实性、准确性、时效性、完整性、可用性和可追溯性。

2）数据传输阶段

应采取链路冗余、密码技术、校验技术、审计技术等保证数据传输过程中机密性、完整性、可用性及可追溯性，针对重要数据应采用国家密码管理部门核准的密码技术保证数据传输的机密性。

3）数据存储阶段

应根据数据安全等级采取分级分域的存储处理策略，采取必要的认证、防泄漏、加密、容灾备份等措施保证数据存储安全。

4）数据处理阶段

数据处理应遵循必要性和合法性，以确保数据正当使用。应保证在安全的环境下开展数据处理活动，加强对数据处理过程风险监测及处理，采取审核、脱敏、审计等手段保证数据处理阶段安全。

5）数据交换阶段

应在安全的环境下开展数据交换活动，数据交换过程中，应采取审核、加密、脱敏、备份、审计等措施保证安全。

6）数据销毁

宜按照相关的法律法规要求，制定数据清理和过期数据销毁流程。针对数据销毁，需采取技术手段防止溯源，且针对数据销毁过程审计及记录。

9.6.4 数据安全管理保障

应符合下列要求：

1）应加强对数据资源的安全分类分级管理，落实数据收集、存储、提供、使用等环节的安全管理责任，防范数据被泄露、滥用和篡改。

2）应明确数据资源管理各环节安全责任主体，建立数据安全评估机制、数据备份恢复机制、数据安全应急预案、安全责任认定机制和重大安全事件及时处置机制。

3）应加强对第三方技术服务单位、供应商的管理，要求其依法履行数据资源安全保护义务，防止数据资源泄露。

4）应当建立安全检查机制，定期检查数据资源的收集、汇聚、共享、开放、应用等情况，对发现的问题及时整改。

5）宜针对定期组织相关人员进行应急演练，保障数据安全。

9.7 个人信息保护要求

9.7.1 个人信息和个人敏感信息识别

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理应包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。个人信息的识别可参照 GB/T 35273-2020 附录 A（资料性附录）个人信息示例，个人敏感信息识别可参考附录 B（资料性附录）个人敏感信息判定。

9.7.2 个人信息处理原则

个人信息控制者开展个人信息处理活动应遵循合法、正当、必要的原则，具体包括：

1）合法正当：个人信息的处理活动，应当遵守国家法律法规的要求，以及通过正当的形式开展。

2）权责一致：采取技术和其他必要的措施保障个人信息的安全，对其个人信息处理活动对个人信息主体合法权益造成的损害承担责任。

3）目的明确：具有明确、清晰、具体的个人信息处理目的。

4）选择同意：向个人信息主体明示个人信息处理目的、方式、范围等规则，征求其授权同意。

5）最小必要：只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息。

6）公开透明：以明确、易懂和合理的方式公开处理个人信息的范围、目的、规则等，并接受外部监督。

7）确保安全：具备与所面临的安全风险相匹配的安全能力，并采取足够的管理措施和技术手段，保护个人信息的保密性、完整性、可用性。

8）主体参与：向个人信息主体提供能够查询、更正、删除其个人信息，以及撤回授权同意、注销账户、投诉等方法。

9.7.3 个人信息活动基本安全

个人信息活动基本安全包括：

1）应满足本文件第 9.6.2 章节要求。

2）根据开展业务的需求，在涉及个人信息处理活动的各个环节，如个人信息的收集、个人信息的存储、个人信息的使用、个人信息的主体权利等处理活动的过程，宜符合 GB/T 35273-2020 第 5 章至第 11 章的要求。

3）在开展业务处理活动过程中，如有可能对个人信息主体合法权益造成不利影响的风险，宜根据 GB/T 39335-2020 开展个人信息安全影响评估。

9.7.4 个人信息安全保障

应符合下列要求：

1）个人信息控制者应根据有关国家标准的要求，建立适当的安全保障能力，落实必要的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。

2）应设置指导和管理个人信息保护的工作机构，明确机构的职责，配备个人信息保护专岗人员明确岗位职责，针对岗位人员的背景、专业技能等进行审查，并签订保密协议。

3）应设立制定个人信息保护的总体方针和安全策略等相关规章制度和文件，包括个人信息管理操作规程、安全策略、管理制度和记录表单，并确保个人信息管理的制度和文件执行落实。

4）应加强对第三方涉及个人信息处理活动的人员，如技术服务单位、供应商的管理，签订保密协议，加强第三方人员涉及个人信息过程的监督和审计，防止个人信息泄露。

5）应当建立安全检查机制，定期针对个人信息处理活动流程、个人信息管理制度执行、个人信息岗位人员情况进行检查，对发现的问题及时整改。

6）应建立健全网络安全风险评估机制，定期对个人信息处理活动进行风险评估，对发现的问题及时整改，修订完善个人信息处理活动流程。

7）应定期（至少每半年一次）组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程，留存应急培训和应急演练记录；应定期对原有的应急预案重新评估，修订完善。

附表

附表一

表 1 算法结构化描述建议字段表

名称	字段		字段类型	是否必填
算法 ID	id		String	是
算法名称	name		String	是
算法代号	code		String	是
算法版本	version		String	是
算法标识	tag		String	是
功能描述	description		String	
算法包类型	AlgorithmPackageType		String	是
神经网络版本	neuralNetworkVersion		String	
芯片类型	ChipType		String	是
算法位宽	bitWide		String	是
来源厂商	vendor		String	是
算法文件名	packageName		String	是
算法版权	copyright		String	
创建时间	createTime		Timestamp	
算法发布说明	releaseNote		String	
算法文件 MD5 值	md5		String	是
授权地址类型	authorizedAddressType		List<String>	是
运行设备端	adapter		String	是
算法包描述	packageDescription		JSON	
设备需求	requirement		JSON	
扩展信息	extensions		List<JSON>	
模型映射关系	model_mapping		List<JSON>	是
算法功能	functions		List<JSON>	是
功能名称	functions	name	String	是
功能描述		description	String	
事件代码		eventCode	String	是
标签		tag	String	是
目标类型		targetType	List<String>	是
分析类型		analysisType	List<String>	是
分析源类型		analysisSourceType	String	是
分析源规格		analysisSourceSpecification	List<JSON>	
准确率		precision	INT	
回收率		recall	INT	
行业分类		industry	List<String>	

名称	字段		字段类型	是否必填
场所分类		place	List<String>	
封面图片		cover	String	
分析能力		abilityInfos	List<JSON>	
调度参数		dispatchParameter	JSON	
状况		condition	JSON	
规则		regulation	JSON	
场景		scene	JSON	
免责声明		disclaimer	String	
标签		labels	List<String>	
应用案例		cases	List<JSON>	
算法示例		examples	List<JSON>	

附表二

表 2 视频资源描述规则表

字段名	类型	长度	约束	描述
id	int8		PRIMARYKEY	主键标识
platform_index	varchar	64	NULL	数据来源平台
external_index_code	varchar	64	NULL	国标编码
index_code	varchar	64	NULL	源表数据 ID
internal_index_code	varchar	64	NULL	内部编码
org_internal_index_code	varchar	64	NULL	所属组织内部编码
device_name	varchar	64	NULL	监控点名称
device_alias	varchar	255	NULL	监控点别名
place_alias	varchar	64	NULL	点位俗称
longitude	numeric		NULL	经度
latitude	numeric		NULL	纬度
altitude	float4		NULL	海拔高度
geom	geometry		NULL	监控点对应地图值
region_code	varchar	64	NULL	行政区划
cascade_code	varchar	64	NULL	级联编号
camera_type	int2		NULL	摄像机类型 0:枪机,1:半球,2:快球,3:带云台枪机
camera_core_function_type	int2		NULL	摄像机核心功能类型(0:普通视频点位;1:人脸抓拍机;2:车辆抓拍机;3:微车;4:神捕;5:高空瞭望;6:全局;7:全景;8:全结构;9:热成像;10:车载;11:单兵;12:人证;13:鹰眼);10 和 11 是移动点位，其余是非移动点位
camera_function_type	varchar(32)		NULL	摄像机功能类型 1.车辆卡口；2.人员卡口；3.微卡口；4.特征摄像机；5.普通监控；6.高空瞭望摄像机；99.其他
camera_encoding_format	int2		NULL	1.MPEG-4；2.H.264；

字段名	类型	长度	约束	描述
				3.SVAC；4.H.265
camera_point_type	int2		NULL	监控点位类型 1.一类视频监控点；2.二类视频监控点；3.三类视频监控点；4 公安内部视频监控点；9.其他点位。参照公安部《关于进一步加强公安机关视频图像信息应用工作的意见》（公通字〔2015〕4 号）定义
camera_place_type	varchar	128	NULL	按照枢纽内部区域划分进行定义
capability_set	varchar	1024	NULL	能力集
intelligent_set	varchar	1024	NULL	智能分析能力集
ext_capability_set	varchar	1024	NULL	扩展能力集
pixel	int2			像素(1.普通；2.130 万高清；3.200 万高清；4.300 万高清；5.400 万高清；6.500 万高清；7.600 万高清；8.700 万高清；9.800 万高清；10.900 万高清；11.2400 万高清；12.3200 万高清)
fill_light_properties	int2		NULL	1.无补光；2.红外补光；3.白光补光；9.其他补光
is_outdoor	int2		NULL	1.室外；0 室外
monitoring_direction	int2		NULL	1.东；2.西；3.南；4.北；5.东南；6.东北；7.西南；8.西北；9.全向
monitoring_direction_angle	int2		NULL	监控方位角度，0-359
installation_time	timestamp	6	NULL	安装时间
installation_height	float4		NULL	安装高度
installation_address	varchar	255	NULL	安装地址

字段名	类型	长度	约束	描述
photo_url	varchar	255	NULL	照片地址
device_manufacturer	int2		NULL	1.海康威视；2.大华；3.天地伟业；4.科达；5.安讯士；6.博世；7.亚安；8.英飞拓；9.宇视；10.海信；11.中星电子；12.明景；13.联想；14.中兴；15.华为；99.其他
device_model	varchar	128	NULL	设备型号
device_mac	varchar	64	NULL	Mac 地址
device_status	int2		NULL	设备状态(1.在用；2.维修；3.拆除)
is_networking	int2		NULL	已联网接入公安机关的摄像机即视为已联网
video_storage_day	int2		NULL	录像保存天数
decode_tag	varchar	64	NULL	解码标签
channel_no	int2		NULL	通道号
channel_type	varchar	32	NULL	通道类型(0.模拟通道；1.数字通道；2.零通道；3.镜像通道；4.录播通道)
trans_type	int2		NULL	传输协议(0.UDP；1.TCP)
treaty_type	varchar	32	NULL	接入协议("hiksdk_net:海康 SDK;gb_reg:GB/T28181;ehome_reg:EHOME;dhsdk_net:大华 SDK;onvif_net:ONVIF")
stream_type	int2		NULL	码流类型(0.主码流；1.子码流；2.三码流)
device_index_code	varchar	64	NULL	设备编号编码
horizontal_view	numeric	(25,20)	NULL	水平视场角
vertical_view	numeric	(25,20)	NULL	垂直视场角

字段名	类型	长度	约束	描述
pitch_angle	varchar	10	NULL	俯仰角
build_type	int2		NULL	设备分类(1 公安自建、2 社会点位)
system_code	varchar	64	NULL	系统平台 code
management_unit_code	varchar	64	NULL	管理单位
police_unit_code	varchar	64	NULL	所属辖区公安机关
device_department	varchar	32	NULL	所属部门/行业编码
build_unit	varchar	128	NULL	建设单位
construction_unit	varchar	128	NULL	承建单位
maintenance_unit	varchar	128	NULL	维护单位
visual_angle	varchar	10	NULL	可视域角度
visual_range	varchar	10	NULL	可视域距离
record_location	varchar	64	NULL	录像存储位置
is_videoing	int2		NULL	是否正在视频
tag	varchar	1024	NULL	标签(多个@分隔)
tag_path	varchar	2048	NULL	标签路径(多个@分隔)
source_type	varchar	64	NULL	数据来源
create_time	timestamp	6	NULL	入库时间
update_time	timestamp	6	NULL	更新时间
isvalid	int2		NULL	有效性(0.否;1.是)
floor_number	int8		NULL	楼层
plane_coordinates_x	numeric	(12,8)	NULL	平面坐标 X
plane_coordinates_y	numeric	(12,8)	NULL	平面坐标 Y
three_dimensional_x	numeric	(12,8)	NULL	3D 坐标 X
three_dimensional_y	numeric	(12,8)	NULL	3D 坐标 Y
three_dimensional_z	numeric	(12,8)	NULL	3D 坐标 Z
place_type_list	varchar	255	NULL	所属场所类型集
place_list	varchar	255	NULL	所属地名集
scene_list	varchar	255	NULL	所属场景集
tag_list	varchar	255	NULL	所属标注集