

ICS 35. xxx  
CCS Lxx

# 团 体 标 准

T/ISC XXX—XXXX

## 视联网通用技术能力

(征求意见稿)

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中国互联网协会

发布



## 目 次

前 言 .....	III
引 言 .....	IV
视联网通用技术能力要求 .....	1
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
3.1 视联网 video networking .....	1
3.2 视联网平台 video networking platform .....	2
3.3 视联网终端 video networking terminal .....	2
3.4 边缘节点 edge node .....	2
3.5 平台节点 platform node .....	2
3.6 级联 cascading .....	2
3.7 跨域 cross-domain .....	2
3.8 多模态数据 multimodal data .....	2
3.9 结构化元数据 structured metadata .....	2
3.10 媒体流 media stream .....	2
3.11 数据接入 data ingestion .....	2
3.12 数据处理任务 data processing task .....	2
3.13 资源池 resource pool .....	2
3.14 资源跨域管理 cross-domain resource management .....	2
3.15 算法服务 algorithm service .....	3
3.16 模型服务 model service .....	3
3.17 在线推理 online inference .....	3
3.18 批量推理 batch inference .....	3
3.19 关键功能 key function .....	3
4 缩略语 .....	3
5 视联网概述与通用架构 .....	5
5.1 通用结构 .....	5
5.2 业务特征 .....	5
5.3 主要应用场景 .....	5
6 视联网平台通用能力要求 .....	6
6.1 视联网基础资源管理 .....	6
6.2 视联网终端管理 .....	7
6.3 视联网数据接入管理 .....	7
6.4 视联网数据传输管理 .....	7
6.5 视联网数据存储 .....	8

6.6	视联网数据处理	8
6.7	兼容开放能力	9
6.8	运维运营能力	9
6.9	质量管理能力	9
7	视联网安全技术能力要求	10
7.1	安全总体目标	10
7.2	总体安全要求	10
7.3	视联网基础资源管理安全	10
7.4	视联网终端安全	10
7.5	数据接入管理安全	10
7.6	视联网数据传输调度安全	10
7.7	视联网数据存储安全	11
7.8	视联网数据处理安全	11
7.9	视联网业务处理安全	12
7.10	兼容开放能力安全	12
7.11	运维运营与安全管理	12
8	视联网人工智能服务能力要求	12
8.1	模型开发及运营服务	12
8.2	模型场景应用服务	14
A.7	功能覆盖度	18
A.8	效益型指标	18
A.9	成本型指标	19
A.10	性能达成度	20
A.11	服务质量	20
A.12	综合评价	20

## 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。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、联通数字科技有限公司、天翼视联科技股份有限公司、中国移动通信集团、浪潮通信信息技术有限公司等。

本文件主要起草人：

# 引 言

《视联网通用技术要求》旨在建立统一的视联网技术标准体系，指导跨平台、跨行业的互联互通。本标准为该系列标准的第一部分（通用要求），后续将围绕《视联网 终端技术要求》、《视联网 平台互联接口规范》、《视联网 安全防护技术细则》等内容持续推出系列标准。

# 视联网通用技术能力要求

## 1 范围

本标准适用于视联网平台及相关系统的规划设计、建设改造、集成部署、运行维护、能力评估和验收测试，可供政府、行业用户、平台建设单位、系统集成单位、运营单位和第三方测评机构参考使用。

本标准面向视联网通用技术能力提出要求，重点覆盖平台通用能力、平台安全能力和人工智能能力。本标准规定了视联网系统在平台、终端、网络层面的通用技术与功能架构要求，旨在推动跨平台、跨行业的互联互通与开放兼容，侧重于人工智能服务的框架性及多模态协同能力要求。涉及密码、等级保护、个人信息保护、数据安全、人工智能治理等专项要求时，应与相关法律法规、强制性标准和专项标准配套使用。

## 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 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 28181—2022	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 35273—2020	信息安全技术	个人信息安全规范
GB/T 37964—2019	信息安全技术	个人信息去标识化指南
GB/T 39786—2021	信息安全技术	信息系统密码应用基本要求
GB/T 41479—2022	信息安全技术	网络数据处理安全要求
GB/T 41867—2022	信息技术	人工智能 术语
GB/T 42888—2023	信息安全技术	机器学习算法安全评估规范
GB/T 43208.1—2023	信息技术服务	智能运维 第1部分：通用要求
GB/T 43697—2024	数据安全技术	数据分类分级规则
GB/T 45081—2024	人工智能	管理体系

## 3 术语和定义

GB/T 28181—2022、GB/T 35273—2020、GB/T 37964—2019、GB/T 41479—2022、GB/T 41867—2022、GB/T 42888—2023 界定的以及下列术语和定义适用于本文件。

### 3.1 视联网 video networking

以视频、图片、音频和相关结构化元数据为主要对象，通过网络实现终端接入、媒体传输、数据存储、处理分析、共享交换和业务协同的网络化应用体系。

### 3.2 视联网平台 video networking platform

为视联网终端、网络、计算、存储、数据、算法/模型和业务应用提供统一接入、管理、处理、开放和安全控制能力的软件和硬件系统集成。

### 3.3 视联网终端 video networking terminal

接入视联网平台并采集、发送、接收或处理视频、图片、音频、文本或结构化元数据的设备或设备组合。

### 3.4 边缘节点 edge node

部署在靠近数据采集侧或业务现场侧，并提供接入、缓存、存储、预处理、推理或转发能力的计算、存储和网络资源集合。

### 3.5 平台节点 platform node

承载视联网平台服务并可独立或协同完成资源管理、数据处理、业务服务和安全控制的逻辑或物理节点。

### 3.6 级联 cascading

不同视联网平台、平台节点或业务系统之间按照约定接口进行层级互联，实现资源目录、信令、媒体流、事件、告警或元数据交换与协同的过程。

### 3.7 跨域 cross-domain

跨越不同区域、组织、租户、网络边界、安全域或平台节点开展资源访问、数据传输、业务联动或安全管理的场景。

### 3.8 多模态数据 multimodal data

由视频、图片、音频、文本、结构化元数据等两种或两种以上数据形态构成，或可通过时间、空间、设备、事件等关系进行关联的数据集合。

### 3.9 结构化元数据 structured metadata

对视联网资源、媒体内容、事件、告警、目标、轨迹、时间、位置等对象或过程进行结构化描述的数据。

### 3.10 媒体流 media stream

以连续时序方式传输的视频、音频或音视频数据及其必要控制信息。

### 3.11 数据接入 data ingestion

通过接口、协议、文件、消息或任务等方式，将视联网终端、边缘节点、平台节点或第三方系统产生的数据接入视联网平台的过程。

### 3.12 数据处理任务 data processing task

对视联网数据执行转封装、切片、截图、增强、分析、推理、迁移、同步或导出等处理操作的可管理作业单元。

### 3.13 资源池 resource pool

对计算、存储、网络、加速资源等资源进行统一纳管、分配、调度和隔离的逻辑集合。

### 3.14 资源跨域管理 cross-domain resource management

对多区域、多节点、多集群或多安全域中的资源开展统一发现、注册、同步、调度、可视化和权限控制的管理活动。

### 3.15 算法服务 algorithm service

将算法能力以接口、任务或组件等形式对外提供，并可进行调用、配置、监控、审计和版本管理的服

### 3.16 模型服务 model service

将训练完成的模型部署为可调用、可监控、可管理的推理或分析服务。

### 3.17 在线推理 online inference

模型服务对实时请求、实时媒体流或实时事件进行推理并返回结果的过程。

### 3.18 批量推理 batch inference

模型服务对离线文件、历史数据或批量任务进行推理并输出结果的过程。

### 3.19 关键功能 key function

对目标场景目标实现、风险控制或结果判定具有决定性影响，未覆盖时不应判定为满足要求的功

## 4 缩略语

下列缩略语适用于本文件。

缩略语

AI 人工智能 (Artificial Intelligence)

API 应用程序编程接口 (Application Programming Interface)

CPU 中央处理器 (Central Processing Unit)

DASH 基于HTTP的动态自适应流媒体 (Dynamic Adaptive Streaming over HTTP)

F1 F1 值 (F1-score)

FN 假负例 (False Negative)

FNR 漏报率 (False Negative Rate)

FP 假正例 (False Positive)

FPR 误报率 (False Positive Rate)

GPU 图形处理器 (Graphics Processing Unit)

HLS HTTP Live Streaming

HTTP 超文本传输协议 (Hypertext Transfer Protocol)

HTTPS 安全超文本传输协议 (Hypertext Transfer Protocol Secure)

IoT 物联网 (Internet of Things)

mAP 均值平均精度 (Mean Average Precision)

NPU 神经网络处理器 (Neural-network Processing Unit)

QoS 服务质量 (Quality of Service)

Recall 召回率

Precision 精确率

RTP 实时传输协议 (Real-time Transport Protocol)

RTMP 实时消息传输协议 (Real Time Messaging Protocol)

T/ISC XXX—XXXX

RTSP 实时流传输协议 (Real Time Streaming Protocol)

SDK 软件开发工具包 (Software Development Kit)

SLA 服务等级协议 (Service Level Agreement)

TN 真负例 (True Negative)

TP 真正例 (True Positive)

WebSocket 一种在单个TCP连接上进行全双工通信的协议

Webhook 基于HTTP回调的事件通知机制

## 5 视联网概述与通用架构

### 5.1 通用结构

视联网采用“端、边、网、云、用”五层技术拓扑架构，通过跨层级的高效协同，实现海量多模态视听觉数据的智能感知、高效传输、弹性算力调度与业务敏捷构建。各层级定义及协同关系如下：

- 端侧（感知与采集层）：主要包括超高清摄像机、物联网传感器、高精视联终端、车载/无人机载视频采集设备等。负责多源异构视听觉数据、物联感知数据的实时采集、预处理与高安全接入。
- 边侧（边缘计算层）：由边缘网关、边缘云节点及算力资源池组成。部署在靠近用户或数据源头的边缘网络，承担低时延业务的本地化解析、视频结构化分析、流媒体本地缓存及协同调度。
- 网侧（网络传输层）：基于确定性网络、第五代/第六代移动通信（5G/6G）、全光网络等技术构建的超大带宽、超低时延、高可靠性视联网传输专网。负责保障海量视频流与控制流的端到端安全、确定性传输。
- 云侧（平台与算力层）：由视联网核心云平台、分布式算力基础设施和多模态大模型矩阵组成。提供全网视联资源的集中式调度、视听觉大数据存储、模型训练与推理算力支撑，并向应用层开放标准化的微服务接口。
- 用侧（业务应用层）：面向各行业、各场景的端到端业务系统。通过调用云侧和边侧开放的能力接口，实现视联网技术与行业业务流程的深度融合。

层级协同关系：

- 算力云边协同：云侧负责通用大模型训练、全局算力调度与策略下发，边侧负责局部、高实时性算力的按需分配与边缘推理，形成“云端训练、边缘执行”的算力弹性协同机制。
- 数据端网协同：端侧根据网侧的实时带宽、丢包率和抖动情况，动态调整视频编码码率、帧率及传输策略（如自适应码率路由），确保网络劣化条件下的视频传输质量。
- 感知数视协同：端侧物联感知数据（如雷达、红外、传感器轨迹）与视频流在边侧或云侧进行时间戳同步与空间对齐，实现多模态数据的深度融合与协同表征。

### 5.2 业务特征

视联网在实际运营和技术实现中，展现出以下典型业务特征：

- 超低时延传输：通过音视频编解码优化、边缘缓存及确定性网络调度，使端到端视听觉流传输与控制信令交互的时延达到毫秒级，满足工业精准控制和应急高实时指挥的需求。
- 大规模并发调度：具备承载千万级跨地域、异构视联终端的并发接入能力，支持百万级视频流的同步分发、转发与动态集群调度，具备高弹性与高容错性。
- 多模态数视融合：支持将传统视频、音频与空间点云、物联感知数据（如温度、速度、位置等）进行异构关联，通过多模态融合算法提升全局时空态势的感知精度。
- 感知与视频协同：实现“感知触发视频，视频反哺感知”的闭环机制。物联感知异常自动触发视频联动跟踪与高码率录像；视频智能分析结果反向修正感知终端的运行策略。

### 5.3 主要应用场景

视联网的通用技术能力广泛赋能以下产业界共识的典型场景：

- 智能数字城市：依托全网高大并发调度与视频 AI 分析，赋能城市综合治理的分钟级自动巡检派单、社会治安的立体化综合防控以及灾害现场“空天地”可视化一体应急指挥调度。

- 大健康医疗：基于确定性低时延与超高清流传输，支持远程 4K/8K 无损手术会诊指导与机器人协同控制，以及隔离病房的微距智能监护与异常行为秒级告警。
- 工业微距视联：部署于自动化产线，利用微距超高清相机与边缘 AI 推理对精密元器件进行表面缺陷在线检测，并通过工业 AR 眼镜实现远端专家多视角检修协同。
- 智慧交通：融合路口摄像头与雷（光）达等异构感知数据，实现路口数字孪生、弱势群体避撞主动预警，并基于全网态势感知自动下发信号灯自适应控制策略。
- 无人机视联感知：构建低空高安全视联网，支持无人机在电力高压线、油气管道、森林及河道等场景下进行全自动航线巡航、可见光/红外双光流回传与隐患智能识别。
- 智慧能源与矿山：覆盖变电站、配电房及极端恶劣的地下矿井等核心节点，实现设备开关状态自动辨识、人员违规行为秒级联动告警以及无人化远程集中可视化控制。

## 6 视联网平台通用能力要求

### 6.1 视联网基础资源管理

#### 6.1.1 网络资源管理

- 应支持网络资源清单化管理，并支持按区域、节点、租户或业务系统进行组织管理（分组/标签）。网络资源清单信息至少应包括网络类型、地址/网段、接入点/出口、链路标识及关键配置参数，并支持查询、导入/导出与变更记录。
- 应支持网络连通性与网络状态的监测与告警，至少应支持链路可达性及网络质量相关统计信息的采集、展示与告警。

#### 6.1.2 计算资源管理

- 应支持对平台计算资源的统一纳管，包括物理机、虚拟化环境、容器/集群环境及加速资源（如 GPU/NPU 等），并支持资源台账、状态信息与使用统计的查询与导出。
- 应支持计算资源的资源池化管理，支持按租户/业务域/任务类型进行配额、优先级与隔离策略配置。
- 应提供计算资源与任务运行状态的可观测能力，支持对资源占用、任务状态、失败原因等信息的采集与展示，并支持导出统计报表。

#### 6.1.3 存储资源管理

- 应支持对平台使用的存储资源进行统一管理，至少应包括存储池、卷、桶、目录等资源对象的登记、查询、配置与状态维护，并支持容量、使用情况和运行状态信息的采集、展示与告警。
- 应支持按租户、业务类型和数据类型进行存储配额与分级策略配置，并支持策略的生效范围管理、变更记录和审计追溯。
- 应支持存储资源与数据目录、元数据之间的关联管理，保证数据存放位置、复制迁移过程及结果可查询、可追溯。

#### 6.1.4 资源跨域管理

- 应支持多节点/多区域/多集群资源的统一视图与分级管理，至少应包括资源发现/注册、状态同步、告警汇聚与权限隔离。
- 应支持跨域资源信息同步与一致性校验机制，支持同步策略配置、同步结果记录与异常告警。
- 应支持跨域资源调度策略的配置与下发，并支持策略接口开放；策略应可追溯到生效范围、生效

时间与变更记录。

## 6.2 视联网终端管理

- 应支持多类型终端接入与统一管理，终端类型至少应覆盖视频终端、图片采集设备、音频终端及具备多模态采集能力的边缘设备。
- 应支持多种接入形态，至少应支持终端直连接入、网关/边缘代理接入与平台级联接入，并对接入形态进行标识与管理。
- 应支持终端分组与标签管理，并支持按分组/标签进行批量操作与权限配置。
- 应支持多种协议接入（如 GB/T 28181，私有协议等）。
- 应支持终端从注册/入网、配置、运行监测、故障处置、升级、替换到注销/退网的全生命周期管理，并对关键状态变化形成可追溯记录。
- 应支持终端在线状态、健康状态与关键告警的监测与通知，并支持告警确认与处置闭环跟踪（如适用）。
- 应支持终端批量管理能力，包括批量导入/导出、批量配置下发、批量启停/重启等，并支持关键操作审计。

## 6.3 视联网数据接入管理

- 应支持多模态数据接入，至少应包括视频、图片、音频、文本及结构化元数据（如时间、位置、事件、告警、目标/轨迹等）。
- 应支持接入数据的基础质量校验与异常处理，至少应支持数据格式/编码校验、字段完整性校验、时间戳有效性校验，并记录校验结果与处置结果。
- 应支持流式与文件式两类接入方式的协议对接：流式用于实时媒体与实时事件，文件式用于离线归档、历史补录与批量导入。
- 应支持通过标准化接口进行数据接入（如基于 HTTP(S) 的 API），并提供接口文档、字段定义与错误码说明。
- 宜支持基于消息订阅/发布机制的数据接入方式（如适用）。
- 应支持推送与拉取两种接入方式，并支持按业务场景配置接入方式与接入策略（如实时/定时/触发式）。
- 应支持接入任务的任务化管理，至少应支持任务创建、启停、状态查询、结果统计与异常告警。
- 应支持接入失败的异常处理机制（如重试、补偿、人工介入等），并记录失败原因与处理结果。

## 6.4 视联网数据传输管理

- 应支持跨节点视频流互通与路由选择，满足视联网跨节点协同需求。
- 应支持级联场景下的数据同步与一致性校验。
- 应支持级联场景下的权限管理，避免跨域访问越权。
- 应支持在公网、专网、互联网、局域网等网络环境下部署与运行，并支持跨网络访问所需的连接参数配置与管理。
- 应支持多网络接入的路由选择与访问策略配置。
- 应支持视联网业务所需的媒体承载、会话控制与元数据传输相关协议对接。
- 应支持 GB/T 28181 场景下的信令与媒体传输机制，并支持会话状态监测与异常告警。
- 宜支持工程常用的媒体访问/分发协议（如 RTSP、RTP、RTMP、HTTP-FLV、HLS/DASH 等），

具体支持范围以平台提供的清单为准。

- 应支持媒体流传输会话的统一管理，至少应包括会话建立/释放、会话状态查询与会话异常记录。
- 应支持视频流的 QoS 保障与优先级控制，包含动态带宽分配、拥塞控制与弱网自适应（降码率/降帧/重传等）。
- 应支持端到端链路可观测能力：对时延、抖动、丢包、码率变化等关键指标进行采集、统计与告警。
- 宜提供面向业务的传输 SLA 目标配置与达标分析（如首帧时间、端到端时延、卡顿率）。
- 宜支持跨协议适配/转封装能力（如适用），并可与“视联网数据处理”章节中的转封装/转码能力衔接

### 6.5 视联网数据存储

- 应支持非结构化媒体数据的存储能力，至少应支持视频、图片、音频等媒体对象的写入、读取与删除管理。
- 应支持结构化数据的存储能力，至少应支持终端与通道信息、目录与元数据、事件与告警、运维日志等结构化数据的存储与查询。
- 应支持集中式或分布式存储的部署方式，并支持按节点/区域配置存储资源与容量配额。
- 应支持云边端协同存储策略配置（如边缘缓存、边缘存储与中心存储的回传/归档策略），并记录策略生效范围与变更记录。
- 应支持热—温—冷分级存储与生命周期管理；分级策略与生命周期策略应可配置并可追溯。
- 应支持备份、归档与迁移能力，并支持迁移/恢复过程中的一致性校验与结果记录。
- 应支持跨节点的数据目录与元数据同步或映射管理，保证跨节点访问时资源标识可识别、可追溯。
- 应支持跨节点的数据复制与迁移任务管理，至少应支持任务创建、进度监测、失败重试与结果记录。
- 应支持存储可靠性保障机制，至少应包含数据冗余、故障恢复与完整性校验能力，并支持输出校验结果与异常记录。
- 应支持数据保留与销毁策略配置，满足业务留存、合规与取证需。
- 应支持按通道/设备、时间范围、地理位置、事件类型等条件的组合检索。

### 6.6 视联网数据处理

- 应支持数据处理任务管理，至少应支持任务创建、启停、状态查询与结果查询。
- 应支持对媒体数据的基础处理能力，至少应支持按时间范围切片、截图/关键帧提取，并输出与原始媒体的关联标识。
- 应支持对媒体数据进行解封装、封装与转封装处理（如适用）。
- 宜支持媒体增强类处理能力（如去噪、去雾、稳像、超分辨等）。
- 应支持视频点播/回放/取证导出等播放环节能力，包含如检索定位、倍速、时间轴定位与多格式导出等能力。
- 应支持视联网数据在云侧、边缘侧和终端侧的协同处理，支持按业务需要将采集、预处理、分析、汇聚和分发等处理环节部署在不同节点协同完成。
- 应支持跨节点/跨域场景下的来源与去向可追溯，至少应记录数据来源节点、处理节点与输出位置（或等效信息）。

### 6.7 兼容开放能力

- 应提供平台能力开放接口（如 API/SDK），并提供接口文档、字段定义、错误码与版本信息。
- 应支持 WebSocket/Webhook 等实时推送能力，满足事件与状态的实时订阅。
- 应支持第三方能力接入与集成（如地图、IoT 平台、身份系统、工单系统等）。

### 6.8 运维运营能力

- 应支持视联网业务在多个平台节点、区域节点或子节点之间进行联动处理，支持事件、告警、任务或处置信息按规则进行跨节点分发、协同处置、状态同步和结果汇总。
- 应支持告警/事件统一管理，至少应支持产生、确认、处置、关闭/归档等状态流转，并记录状态变化。
- 应支持告警联动处置编排，可自动触发录像、通知、工单或第三方系统联动。
- 应支持事件/告警订阅与对外推送（回调/消息订阅任选其一或多种），并记录推送结果与失败原因（如有）。
- 应支持资源与业务双维度可视化监控视图，资源视图：如终端/边缘/网络/算力资源指标，业务视图：业务运营指标（如在线率、并发路数、告警量、SLA 达标等）。
- 应支持端到端链路追踪与分段定位（接入-承载-处理-存储-分发），并支持告警关联与智能排障辅助。
- 应支持变更与发布管理（灰度、回滚、配置版本管理）以及关键操作审计。
- 宜支持智能运维能力：异常检测、容量预测、预测性维护（如硬盘寿命、GPU 显存异常等）。
- 宜支持服务保障能力：面向用户的服务目录、SLA 管理、工单与处置闭环统计。

### 6.9 质量管理能力

- 应支持视频质量、服务质量、资源质量多维指标体系，以及“监测、评估、控制、优化”的全生命周期闭环质量管理框架能力。
- 应支持全链路可观测的质量监测能力：从基础设施（计算、存储、网络）、平台服务、业务应用（视频调阅、AI 分析）的全栈数据。7x24 小时采集视频质量、服务质量、资源质量等核心指标，输出形成统一和集中的质量数据。
- 应支持质量评估能力：基于预设的质量指标阈值和 SLA 进行实时比对与趋势分析，通过数据分析定位故障点，通过关联数据分析发现潜在隐患。通过统一的管理驾驶舱以图表、仪表盘等形式动态展示平台健康度，并对异常状态进行多级（警告、严重）告警。
- 应支持质量控制能力：根据评估结果进行实时或预定精准干预。包括在并发过高时自动触发流控策略对非关键业务限流，检测到主线路视频流质量劣化时自动切换至备份线路或降低码率，计算节点负载过高时自动调度任务至空闲节点实现负载均衡，同时提供管理界面允许运维人员手动执行设备重启、服务隔离、策略下发等操作。
- 应支持质量优化能力：基于历史数据分析识别性能瓶颈，驱动基础设施扩容、设备选型优化或代码算法重构。将质量控制中有效的临时策略固化为平台标准能力，根据业务发展持续调整和优化质量指标的阈值与评估模型，形成知识沉淀反哺监测、评估和控制环节。

## 7 视联网安全技术能力要求

### 7.1 安全总体目标

- 应构建覆盖终端安全、网络传输安全、平台安全和数据全生命周期安全的纵深防御体系。
- 应确保视频流与控制流的机密性、完整性、可用性和不可否认性，防止未经授权的访问、恶意控制、数据泄露及网络攻击，确保视联网业务的连续稳定运行。

### 7.2 总体安全要求

- 应建立平台安全对象的统一标识体系，至少包括终端、边缘节点、平台节点、租户/用户、应用与接口调用方。
- 应建立统一的认证与授权机制，支持对终端接入、接口调用、媒体访问、数据操作与跨域互通等行为实施访问控制。
- 应支持安全策略的集中配置、下发与生效范围管理，并对策略变更进行审计记录与导出。
- 应支持安全事件与安全告警的统一管理，形成从发现、处置到关闭的记录闭环。

### 7.3 视联网基础资源管理安全

- 应支持基础网络安全服务配置与管理（如访问控制、入侵防护/防护策略等），具体实现方式不限定。
- 应支持多租户隔离或等效隔离机制（如资源配额、命名空间隔离等）。
- 应支持存储介质/存储服务的机密性保护能力（如加密存储或等效机制），并支持密钥/证书管理对接（如适用）。
- 应支持跨域资源同步/注册过程的身份认证与信任关系管理，并支持信任关系配置、变更与吊销。
- 应支持跨域资源可见范围与访问权限控制，避免跨域越权访问。

### 7.4 视联网终端安全

- 应支持终端与平台之间的身份认证与接入授权，防止未授权终端接入。
- 应支持证书或密钥的生命周期管理，包括申请/下发、更新、失效与吊销。
- 应支持终端或边缘节点软件升级的来源校验与升级失败回滚（如适用）。
- 应支持终端关键配置的访问控制与变更审计，至少应记录变更主体、变更内容、变更时间与结果。

### 7.5 数据接入管理安全

- 应对数据接入接口（API/SDK/消息接入等）实施身份认证与授权控制，并支持接口调用审计。
- 宜支持对接入接口进行访问频率控制与异常调用告警（按项目选用）。

### 7.6 视联网数据传输调度安全

- 应支持跨网络访问的边界防护策略配置与审计（如访问控制、黑白名单等，具体实现方式不限定）。
- 应对媒体流的拉流、播放、转发等操作实施访问控制，防止未授权访问与扩散。
- 应支持媒体会话建立过程中的鉴权与完整性保护，并记录会话标识、协商结果与异常原因，防止会话劫持与篡改。
- 应支持媒体流在传输过程中的机密性保护（加密传输或等效机制），并支持加密策略按业务/安全

域配置。

- 应对关键操作（拉流、转推、导出）进行审计记录，并支持统计与导出。
- 
- 注：媒体流保护级别（如机密性/完整性/访问控制）可参考相关视频联网信息安全标准的分级思想进行配置，但本标准不规定固定分级阈值。
- 应支持跨域互联场景下的双向认证与信任关系管理，并支持信任关系的配置、变更与吊销。
- 应支持跨域资源标识映射与权限映射规则配置，并支持规则导出与变更审计，避免越权访问。
- 应支持跨域访问的审计记录，至少应记录如访问主体、访问对象、授权依据（如策略/映射规则标识）、结果与失败原因。
- 应支持跨域互联接口调用的异常检测与告警（如认证失败、越权拦截、异常调用频率等）。

## 7.7 视联网数据存储安全

- 应支持存储数据机密性保护（加密存储或等效机制）与密钥管理对接（如适用）。
- 应支持数据完整性校验或等效机制，并保留校验结果与异常记录。
- 应支持备份与恢复过程的授权与审计记录。
- 应支持跨域复制/迁移任务的授权控制与审计记录，至少记录任务发起方、任务范围、目标域、结果与失败原因。
- 应支持跨域数据同步/复制过程的传输保护（加密传输或等效机制）与完整性校验（如适用）。
- 宜支持跨域复制/迁移任务的暂停、回滚或补偿机制（按项目选用）。
- 应支持数据保留与销毁策略配置，并记录策略生效范围、变更记录与执行记录。
- 应支持备份策略配置与备份结果记录，并支持恢复操作的授权与审计。
- 宜支持异地备份/容灾切换的操作记录与审计（按项目选用）。
- 宜支持对外共享或取证导出的流程化授权管理，至少应包括申请、审批/授权、交付、撤销（如适用）与记录留存。
- 宜支持共享/导出内容与原始数据的关联追溯，至少应包含资源标识、时间范围、导出人/审批人、导出用途标识与导出结果记录。
- 应支持在播放/共享/导出等使用环节对敏感信息进行脱敏或遮挡处理，并与权限策略联动，记录脱敏策略标识与适用范围。
- 宜支持共享/导出内容的水印标记与追溯。

## 7.8 视联网数据处理安全

### 7.8.1 常规数据处理安全

- 应支持数据处理任务与处理链路的访问控制与审计记录。
- 应支持处理组件/插件的注册与版本管理（如适用），并支持来源可信校验、启停控制与回滚（如适用）。
- 应支持处理输出结果与输入数据的关联追溯。
- 宜支持处理链路异常的告警与处置闭环记录（按项目选用）。

### 7.8.2 AI 模型资产及推理安全

- 宜支持对算法/模型服务调用的身份认证、授权与调用审计（按项目选用）。
- 宜支持训练数据、推理数据与模型资产的隔离存储与访问审计（按项目选用）。

- 宜支持对 AI 输出结果的安全风险控制（如敏感信息外泄控制、输出可追溯标识等，按项目选用）。

### 7.9 视联网业务处理安全

- 应支持告警联动处置编排的授权控制与审计，避免未授权触发录像、通知、工单或第三方联动。
- 应支持跨平台/跨域业务联动的授权控制与审计记录，并可追溯到跨域信任关系与权限映射规则。
- 宜支持对高风险处置操作的二次确认或审批（按项目选用）。

### 7.10 兼容开放能力安全

- 应提供开放接口（API/SDK）的鉴权、访问控制与调用审计能力，并提供接口版本与权限范围说明。
- 应支持接口访问凭据（如 Key/Token/证书等）的生命周期管理与吊销机制（实现方式不限定）。
- 应支持 Webhook/WebSocket 等实时推送的安全控制（如回调地址校验、签名校验/重放防护、推送失败记录等）。
- 宜支持对开放接口进行访问频率控制与异常调用告警（按项目选用）。

### 7.11 运维运营与安全管理

- 应支持安全事件、操作记录、系统状态等日志的集中采集与查询，并支持导出。
- 应明确日志覆盖范围，至少应覆盖：
  - 终端/边缘接入认证与授权（成功/失败及原因）；
  - 媒体拉流/回放/转推/导出等关键操作；
  - 跨域互联建立/断开、双向认证失败、权限映射变更与越权拦截；
  - 接口调用（含回调推送）与异常调用；
  - 数据共享/取证导出、数据删除/销毁、备份/恢复；
  - 关键配置与策略变更。
- 应支持对平台节点、组件或插件、接口、证书或密钥、策略对象等安全相关资产进行统一登记、查询和状态管理。
- 应支持安全事件的分级处置记录与事后追溯。
- 应支持安全事件处置过程中的证据材料留存与关联（含日志、媒体片段、处置动作等）。

## 8 视联网人工智能服务能力要求

### 8.1 模型开发及运营服务

#### 8.1.1 资源服务

- 应支持对不同类型的算力资源（CPU/GPU/NPU等）进行统一管理，并支持按租户或业务设置配额。
- 应支持查看资源使用状态，并支持告警通知。
- 应支持算法/模型镜像的自动化部署与升级，并记录版本变更信息。
- 宜支持国产芯片适配能力，并提供已适配范围说明。

#### 8.1.2 数据服务

- 应支持数据集全生命周期管理（如导入、清洗、版本、授权、归档/删除等）。

- 应支持数据预处理（如抽帧、转码、去噪/增强、时空元数据关联等）。
- 应支持将结构化元数据与对应的视频/图片片段建立关联（例如按时间戳、设备/通道标识关联），并支持查询与追溯。
- 宜支持半自动标注与标注审核，降低人工标注工作量，并支持标注过程回溯。

### 8.1.3 模型服务

#### 8.1.3.1 模型管理服务

- 应支持模型导入/导出、模型元信息管理（如类型、版本、适用场景、依赖、输入输出规范等）。
- 应支持多版本管理、灰度发布与回滚；
- 应支持模型服务注册/注销与配置变更审计。
- 应支持查看平台所有的预置模型，可按模型类别、模型系列、算法框架筛选，支持查看每个模型详情，基本信息包含模型名称、模型类型、模型描述等
- 应支持模型评估与报告生成，报告应包含如测试集说明、指标口径、结果汇总、数据来源、评估环境、评估时间等可追溯信息。
- 宜支持模型仓库/资产中心，支持模型生命周期（上架、下架、归档）与合规审查记录。

#### 8.1.3.2 模型训练服务

- 应支持训练任务创建、启动、暂停、终止与可视化监控；
- 应支持 GPU/NPU 等多硬件环境训练。
- 宜支持模型优化（如增量训练、微调、压缩或量化等），并能保存训练配置与训练产物信息，便于复现与追溯。
- 宜支持持续评估（上线前后对比）与自动化回归测试。

#### 8.1.3.3 模型推理服务

- 应支持以“服务”的方式对外提供推理能力（如在线接口、离线任务等），并支持服务启停、版本切换与运行状态查看。
- 应支持本地 / 分布式推理，包括离线批量推理、在线API推理等；
- 应支持多路算法分析任务并行推理与多模型协同推理；
- 应支持视频数据在线推理与批量推理服务。
- 应支持服务监控（如健康状态、资源占用、请求量、服务/推理错误率等）与告警，支持日志留存与查询。
- 宜支持服务限流、熔断、降级与自愈机制，以保障关键业务连续性。
- 应支持云/边缘部署形态选择与统一纳管；
- 应支持模型与配置的边缘下发、更新与回滚；
- 宜支持跨节点任务迁移，并记录迁移过程与结果。

### 8.1.4 运营服务

- 应支持账号与用户管理，支持边缘用户与中心管理员分级账户体系。
- 应支持 API/SDK 等方式对外提供服务调用与结果获取，支持调用审计与配额管理。
- 宜支持与视联网业务系统对接（如告警、工单、指挥调度），实现事件从发现、通知到处置的闭环。

## 8.2 模型场景应用服务

### 8.2.1 模型功能覆盖度

评价目的：验证视联网人工智能平台所部署模型是否具备多种面向视频智能分析场景的应用功能；  
功能分类：

- 目标检测：能够对来自视频流的关键目标（如人员、机动车、非机动车、特殊物体等）进行识别和定位，并输出类别标签与空间边界框，用于支持布控、识别、结构化等任务；
- 行为识别：能够识别人物在视频序列中的行为类型，如奔跑、打架、摔倒、抽烟等，适应城市安防、应急预警等场景需求；
- 事件监测：针对连续视频内容中的复杂时空事件，如人员越界、徘徊、异常聚集、火情等，进行事件级判断与告警，支持时序信息关联和规则配置；
- 宜支持内容分析：对视频中的语义内容进行结构化提取和标签生成；
- 应要求参评方提供“算法服务目录”，目录至少应包含：算法服务名称、算法类型/适用场景、输入类型（图片/视频流/片段等）、输出字段说明、部署形态（云/边）、版本信息与调用方式（API/SDK/任务）。
- 应按标准规定的功能分类对算法服务进行归类。
- 应对每一类功能至少选取代表性算法服务进行验证，验证内容至少包括：可调用性、输入输出符合性、输出可追溯信息（时间戳、资源标识等）与错误码/异常返回等。
- 宜支持参评方声明扩展能力（标准分类以外的特色算法服务），并纳入目录记录。

### 8.2.2 模型性能优越性

- 应要求参评方提供算法服务性能评估报告。报告至少应包含：测试数据说明、指标口径说明、评估环境、评估时间、结果汇总与适用范围说明。
- 应根据算法类型选择适用的指标进行报告，不同算法类型的指标不要求统一，但应说明选择依据：
- 检测类可采用 mAP、Precision、Recall 等(见A.1-A.3)；
- 识别/分类类可采用 Precision、Recall、F1 等（见A.4）；
- 告警/事件类可采用误报率、漏报率等(见A.5-A.7)；
- 其他类型按其任务特点给出可解释的指标。
- 应记录服务质量类指标（与算法类型无关），包括但不限于：推理服务响应时间统计、错误率统计、资源消耗统计（CPU/GPU/NPU、显存/内存等）。

### 8.2.3 模型场景应用服务能力综合评价

#### 8.2.3.1 总则

- 模型场景应用服务能力应结合功能覆盖情况、性能达成情况和服务质量情况进行综合评价。
- 不同任务类型可采用不同性能指标。不同任务的原始性能指标值不应直接进行横向比较，应转换为标准化评价结果后进行综合评价。
- 综合评价所涉及的场景、功能项、算法服务、评价指标、权重和判定规则应在测试实施前确定。

#### 8.2.3.2 评价内容

模型场景应用服务能力综合评价包括下列内容：

##### a) 功能覆盖度；

- b) 性能达成度;
- c) 服务质量;
- d) 综合评价结果。

### 8.2.3.3 评价步骤

模型场景应用服务能力综合评价应按下列步骤进行:

- a) 确定测试场景及场景需求;
- b) 确定场景所需功能类别和代表性算法服务;
- c) 按 5.2.1 进行功能覆盖情况评价;
- d) 按 5.2.2 进行算法服务性能测试;
- e) 将性能测试结果转换为标准化评价结果;
- f) 对服务质量指标进行评价;
- g) 形成综合评价结果。

### 8.2.3.4 功能覆盖度

功能覆盖度用于评价模型对目标场景所需功能的满足程度。

应依据场景需求,对所需功能类别及代表性算法服务进行逐项核验。功能覆盖情况分为完全覆盖、部分覆盖和未覆盖。功能覆盖度计算(见 A.8):

$$F = \sum (w_i \times c_i)$$

其中:

$F$ ——功能覆盖度得分;

$w_i$ ——第  $i$  项功能评价项权重,且  $\sum w_i = 1$ ;

$c_i$ ——第  $i$  项功能评价值(完全覆盖=1,部分覆盖=0.5,未覆盖=0)。

场景关键功能项未覆盖时,不应判定为满足要求。

### 8.2.3.5 性能达成度

性能达成度用于评价模型在已覆盖功能上的任务完成效果。

效益型指标(见 A.9):

$$s = \begin{cases} 0, & x \leq L \\ (x - L)/(U - L) \times 100, & L < x < U \\ 100, & x \geq U \end{cases}$$

成本型指标(见 A.10):

$$s = \begin{cases} 100, & x \leq U \\ (L - x)/(L - U), & U < x < L \\ 0, & x \geq U \end{cases}$$

性能达成度(见 A.11):

$$P = \sum v_j \times p_j$$

#### 8.2.3.6 服务质量

服务质量用于评价模型服务的可用性和稳定性。服务质量（见 A.12）：

$$Q = \sum (\beta_k \times q_k)$$

#### 8.2.3.7 综合评价

综合得分：

$$C = \alpha F + \beta P + \gamma Q$$

当出现以下情况时，不应评为优秀：

- a) 关键功能未覆盖；
- b) 性能未达最低值；
- c) 服务质量不满足要求。

## 附录 A 指标计算方法

### A.1 平均精度 (Mean Average Precision, mAP)

均值平均精度用于评估模型在多类别或多查询任务中的整体性能，是各类别平均精度的均值。其计算公式如下：

(A.1.1)

$$mAP = \frac{1}{N} \sum_{i=1}^N AP_i$$

式中：

$mAP$ —— 均值平均精度；

$N$ —— 类别数量；

$AP_i$ —— 第  $i$  类的平均精度。

### A.2 精确率 (Precision)

精确率是分类问题中的一种重要评测指标，它衡量了模型预测为正例的样本中，实际为正例的比例。其计算公式如下：

(A.2.1)

$$Precision = \frac{TP}{TP + FP}$$

式中：

$Precision$  —— 精确率；

$TP$  —— 真正例的数量，即模型正确预测为正类的实例数量；

$FP$  —— 假正例的数量，即模型错误预测为正类的负类实例数量。

### A.3 召回率 (Recall)

召回率衡量在所有实际为正类的样本中，被正确识别的比例。其计算公式如下：

(A.3.1)

$$Recall = \frac{TP}{TP + FN}$$

式中：

$Recall$  —— 召回率；

$TP$  —— 真正例的数量；

$FN$  —— 假负例的数量，即模型错误预测为负类的正类实例数量。

### A.4 F1 值 (F1-score)

F1 值是精确率和召回率的调和平均值，用于综合评价模型性能。其计算公式如下：

(A.4.1)

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

式中：

*Precision* —— 精确率；

*Recall* —— 召回率；

*F1* —— 精确率和召回率的调和平均值。

#### A.5 误报率 (False Positive Rate, FPR)

误报率表示在所有实际为负类的样本中，被错误预测为正类的比例。其计算公式如下：

(A.5.1)

$$FPR = \frac{FP}{FP + TN}$$

式中：

*FPR* —— 误报率；

*FP* —— 假正例数量；

*TN* —— 真负例数量。

#### A.6 漏报率 (False Negative Rate, FNR)

漏报率表示在所有实际为正类的样本中，被错误预测为负类的比例。其计算公式如下：

(A.6.1)

$$FNR = \frac{FN}{FN + TP}$$

式中：

*FNR* —— 漏报率；

*FN* —— 假负例数量；

*TP* —— 真正例数量。

#### A.7 功能覆盖度

功能覆盖度用于评价模型对目标场景所需功能的满足程度。应依据场景需求，对所需功能类别及代表性算法服务进行逐项核验。功能覆盖度按公式计算：

(A.7.1)

$$F = \sum_{i=1}^m w_i \cdot f_i$$

式中：

*F* —— 功能覆盖度得分；

$w_i$  —— 第 *i* 项功能的权重；

$f_i$  —— 第 *i* 项功能的覆盖情况取值。

#### A.8 效益型指标

效益型指标用于衡量指标值越大越优的性能指标，其计算如下：

(A.8.1)

$$s_j = 1, \quad v_j \geq U_j$$

(A.8.2)

$$s_j = \frac{v_j - L_j}{U_j - L_j}, \quad L_j < v_j < U_j$$

(A.8.3)

$$s_j = 0, \quad v_j \leq L_j$$

式中：

 $s$ ——指标得分； $x$ ——实际测量值； $L$ ——指标下限值； $U$ ——指标上限值。 $s_j$ ——第  $j$  项性能指标标准化后的得分（取值范围为 [0,1]）； $v_j$ ——第  $j$  项性能指标的实际测试观测值； $U_j$ ——第  $j$  项性能指标的指标要求上限（目标值/最优阈值）； $L_j$ ——第  $j$  项性能指标的指标要求下限（基准值/合格阈值）。

## A.9 成本型指标

成本型指标用于衡量指标值越小越优的性能指标，其计算如下：

(A.9.1)

$$s_j = 1, \quad v_j \leq L_j$$

(A.9.2)

$$s_j = \frac{U_j - v_j}{U_j - L_j}, \quad L_j < v_j < U_j$$

(A.9.3)

$$s_j = 0, \quad v_j \geq U_j$$

式中：

 $s$ ——指标得分； $x$ ——实际测量值； $L$ ——指标上限值； $U$ ——指标下限值。 $s_j$ ——第  $j$  项性能指标标准化后的得分（取值范围为 [0,1]）； $v_j$ ——第  $j$  项性能指标的实际测试观测值； $U_j$ ——第  $j$  项性能指标的指标要求上限（当实际值超过该不可接受的上限时，不得分）； $L_j$ ——第  $j$  项性能指标的指标要求下限（当实际值低于该值时得 1 分）。

### A.10 性能达成度

性能达成度按如下计算：

(A.10.1)

$$P = \sum_{j=1}^n s_j \cdot p_j$$

式中：

$P$  —— 性能达成度得分；

$s_j$  —— 第  $j$  项指标权重；

$p_j$  —— 第  $j$  项指标得分。

### A.11 服务质量

服务质量用于评价模型服务的可用性和稳定性。

(A.11.1)

$$Q = \sum_{k=1}^l w_k \cdot q_k$$

式中：

$Q$  —— 服务质量得分；

$w_k$  —— 权重；

$q_k$  —— 指标得分。

### A.12 综合评价

综合得分按如下计算：

(A.12.1)

$$C = \alpha \cdot F + \beta \cdot P + \gamma \cdot Q$$

式中：

$C$  —— 综合得分；

$F$  —— 功能覆盖度；

$P$  —— 性能达成度；

$Q$  —— 服务质量；

$\alpha$ 、 $\beta$ 、 $\gamma$  —— 权重系数，且  $\alpha + \beta + \gamma = 1$ 。