**视频融合赋能平台使用指南**

**V1.0**

目录

[1 方案概述 1](#_Toc29041)

[1.1 建设背景 1](#_Toc26454)

[1.2 建设目标 1](#_Toc27950)

[1.3 设计依据 1](#_Toc12990)

[2 需求分析 2](#_Toc29621)

[2.1 现状问题 2](#_Toc30479)

[2.2 建设需求 3](#_Toc26798)

[3 总体设计 3](#_Toc30074)

[3.1 设计原则 3](#_Toc27662)

[3.2 业务架构 4](#_Toc11161)

[3.3 系统架构 5](#_Toc21655)

[3.4 数据架构 6](#_Toc28272)

[3.5 技术架构 7](#_Toc16221)

[4 资源管理调度平台设计 9](#_Toc6749)

[4.1 概述 9](#_Toc25721)

[4.2 架构设计 9](#_Toc26495)

[4.3 功能设计 9](#_Toc8785)

[4.4 性能设计 13](#_Toc11871)

[4.5 资源规划 13](#_Toc31771)

[5 算法仓库设计 13](#_Toc1762)

[5.1 概述 13](#_Toc28042)

[5.2 架构设计 14](#_Toc15309)

[5.3 功能设计 14](#_Toc17600)

[5.4 智能算法 18](#_Toc8033)

[5.5 实施服务 24](#_Toc31998)

[5.6 性能设计 24](#_Toc29144)

[5.7 资源规划 24](#_Toc10154)

[6 视频融合赋能平台设计 26](#_Toc20680)

[6.1 概述 26](#_Toc7836)

[6.2 架构设计 26](#_Toc7874)

[6.3 功能设计 26](#_Toc20957)

[6.4 实施服务 40](#_Toc3225)

[6.5 性能设计 40](#_Toc21552)

[6.6 资源规划 40](#_Toc31288)

[7 智能存算资源池设计 41](#_Toc9509)

[7.1 智能计算资源池 41](#_Toc21246)

[7.2 视图存储资源池 48](#_Toc27783)

[8 部署方案设计 54](#_Toc27107)

[8.1 通用计算资源配置 54](#_Toc14938)

[8.2 智能计算资源配置 55](#_Toc15361)

[8.3 视图存储资源配置 56](#_Toc14291)

[9 保障体系设计 56](#_Toc29754)

[9.1 安全保障体系 56](#_Toc22755)

[9.2 运营维护体系 69](#_Toc8447)

[9.3 标准规范体系 72](#_Toc23376)

# 方案概述

## 建设背景

*//本节建议结合项目实际背景进行完善。以下内容仅为参考。*

近年来，各地依托“天网工程”、“雪亮工程”等项目，实现了城区主要道路、重点区域、重点部位、重点场所等公共区域视频监控的全覆盖，并在社会治安整治、城市防汛指挥、城市日常管理等方面发挥着积极作用，取得了良好的应用成效。随着各地数字政府建设的持续推进，按照统一规划、统一标准、统一要求，需要进一步统筹规划数据资源和公共支撑平台的集约建设和共享复用，实现共性赋能，推进公共区域视频监控建设一体化，促进公共区域视频监控的共建、共享、共用成为各地数字政府的重点建设任务。

在视频监控为城市治理带来帮助的同时，仍然面临视频感知能力建设分散、系统技术标准不统一、智能应用需求迫切等问题。通过本地政务数据交换共享平台已经能够实现各委办局业务数据的汇聚整合和共享，但针对全域已建的大量视频资源，尚无有效手段实现视频资源的汇聚整合和复用共享，难以将视频资源的建设价值最大化。因此，亟需构建城市统一的视频能力服务平台，进一步提升视频资源的联网整合、智能分析、开放共享等方面能力，推动视频资源和能力服务的统筹规划和规范建设，提升各委办局的整体视频应用水平。

智慧城市视频云中台（以下简称“视频云中台”）是数字政府建设的组成部分，是全域视频监控相关系统统筹建设、开放共享、运维管理、应用构建的重要抓手。视频云中台将依托视频联网、云计算、大数据、人工智能等先进技术，实现全域视频资源的一体化接入、整合、管理、解析和运维等，并向各委办局提供视频资源的查询、申请、审批、编排、调度、事件推送等在线化服务。

## 建设目标

*//本节建议结合项目实际目标进行完善。以下内容仅为参考*

视频云中台以全域视频资源为基础，基于视频图像、云计算、大数据、人工智能等技术，为城市打造统一的视频基础能力平台，构建视频的汇聚治理、智能解析、融合挖掘、运维管理、开放共享等能力，全面提升城市视频资源的共建、共享、共用水平，赋能各委办局便捷、高效、精准的构建可视化、智能化应用，提升在实时图像获取、历史情况回溯、事件智能巡查、问题处置验证等方面业务能力，充分释放视频资源蕴含价值，助力政府构建现代化治理能力，提升城市精细化管理水平。

## 设计依据

### 标准规范

（1）《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 28181-2022）；

（2）《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）；

（3）《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）；

（4）《智慧城市公共信息与服务支撑平台 第1部分：总体要求》（GB/T 36622.1-2018）。

### 政策文件

*//本节建议结合项目当地的政策文件进行描述，以下内容仅为参考。*

本方案依据国家相关法律规章、国家和行业相关政策依据和技术标准、相关研究成果、地方政策及指导性文件等资料进行规划设计，具体依据如下：

（1）《中华人民共和国国民经济和社会发展第十四个五年规划和2035 年远景目标纲要》；

（2）《关于加强数字政府建设的指导意见》（国发〔2022〕14号）。

# 需求分析

## 现状问题

*//建议结合项目的现状及需求进行完善，明确建设内容。以下内容仅为参考*

### 视频资源汇聚整合程度较低

各地已经在城区主要道路、重点部位、重点场所等公共区域建设了大量的视频监控资源，各类视频资源分散于各委办局在不同网络环境中独立运行，目前各地方缺少视频资源汇聚整合的标准和手段，仅部分委办局相互之间实现了视频监控资源的有限互通，全域范围内视频监控资源的联网汇聚、共享交换尚未实现，部分委办局还存在无视频可用或者仅少量视频可用的情形，与全域公共视频监控资源共建、共享、共用的应用目标之间存在较大差距。

### 视频智能分析能力参差不齐

各地通过前期建设已经具备了一定规模的视频智能分析能力，但从全局角度看视频监控的智能分析能力则是参差不齐，存在建设成本高昂、维护麻烦、升级困难、算力不足、无法扩展等问题，同时部分委办局因为缺少技术支撑导致无视频智能分析系统可用。当前视频智能分析系统主要以烟囱模式由各委办局独立建设，仅考虑自身当前的智能应用需求，未从全局统筹考虑算法、算力的建设、管理和应用，带来一定程度的视频算法及算力资源的重复及浪费的问题，当前建设模式也无法支撑城市级视频智能应用的构建。

### 视频跨部门共享应用能力弱

当前部分委办局建设了以人工调阅为主的基础视频应用，这些基础视频应用在功能能力方面基本相同或者类似，所以存在较多基础视频应用重复建设的问题，基础通用视频应用尚未实现统筹共建共用；部分地方开始探索跨部门视频共享交换、管理应用等能力的建设，但在视频资源的查询检索、申请管理、应用支撑等方面能力较弱，导致视频资源存在查找难、获取难、应用难等问题，限制了视频资源价值的有效释放。

## 建设需求

*//建议结合项目的需求进行完善，明确建设需求。以下内容仅为参考*

### 视频资源汇聚需求

汇聚整合城市已建的视频资源，形成城市统一的视频资源池。视频云中台需接入汇聚各委办局在公安视频专网、行业视频专网、运营商专网等网域已建的视频资源，并汇聚整合互联网上社会单位已建视频资源，实现全域涉及公共区域已建视频资源跨部门、跨区域的统一汇聚、编目共享，解决当前部分委办局无视频资源可用或视频资源较少的问题。

### 视频智能分析需求

视频云中台需建设满足当前各委办局业务需求的视频智能分析算法，提供技术手段帮助各委办局生成新的视频算法或者对视频算法进行迭代优化，以持续支撑各委办局智能应用需求。视频云中台需结合当前各委办局的智能应用需求，构建统一的、可扩展的智能算力资源中心，解决部分委办局算力不足的问题，已建智能算力资源应纳入统一的调度系统，实现算力资源的集中管理和高效调度。视频云中台需提供统一的算法描述规范和配套工具，实现不同类型、不同厂商成熟算法的统一管理、统筹复用和效能评价。视频云中台需按照各委办局不同的业务需求提供算法编排、智能解析、事件研判、策略过滤、订阅推送等应用服务，将海量视频资源与丰富智能算法进行有效融合，向各委办局推送共享视频智能事件数据，赋能各委办局快速构建视频智能化应用。

### 视频开放共享需求

视频云中台需为各委办局用户提供视频广场、点位搜索、电子地图、视频监控等视频基础通用应用，方便各委办局用户通过视频云中台或者自身业务平台来调取视频图像开展可视化应用。视频云中台需为各委办局用户提供视频点位资源的申请、审批及管理等共享功能，方便各委办局获取跟自身业务相关的视频资源。视频云中台需提供统一的视频智能分析服务开放能力，提供算法超市、智能分析申请、事件订阅申请、审批及管理等功能，方便各委办局获取跟自身业务相关的算法资源，并能通过统一的智能分析服务获取视频产生的智能事件。视频云中台需为各委办局业务应用平台提供资源目录服务、视频码流转发、设备联动控制、事件订阅推送、视频数据查询等服务接口，赋能各委办局基于视频云中台快速开发并构建可视化、智能化应用。

# 总体设计

## 设计原则

*//本节建议结合项目实际情况进行完善。以下内容仅为参考。*

视频云中台建设遵循“整体性、开放性、先进性、实用性、标准化、可扩展性、安全性和可靠性”的原则，确保系统的设计和建设满足智慧城市、数字城市的持续构建。

（1）整体性

以“兼容已有、立足现在、着眼未来”的设计思路进行项目的整体规划设计，在系统架构、网络传输、点位布建等方面，既要考虑已有资源接入和兼容，又要运用成熟的先进技术满足本方案建设需求，还要为将来的扩容、扩展和升级打下基础。

（2）开放性

系统设计时，采用业界主流的设备、操作系统、数据库及标准协议，充分考虑软件与硬件解耦、算法与算力解耦、应用与数据解耦，保证基础设施、数据、算法、应用等各层能力的开放。

（3）先进性

系统设计时，充分考虑架构和技术的先进性，确保选用的架构和技术符合未来发展趋势，使系统具有较强的生命力，有长期使用价值。充分考虑信息技术迅速发展的趋势，在技术上应具有一定的超前性，采用国际或国内的先进技术，以适应现代科学技术的发展，总体设计一步到位。以适度超前的意识为指导原则，设计中采用先进的系统设备及系统软件和开发工具，以集成化、数字化和智能化的主流产品为核心设备，以保证系统在技术上领先，成熟稳定，符合今后的发展趋势。

（4）实用性

采用成熟和实用的技术和设备，最大限度地满足现在和未来几年的功能需要，项目建设突出实用性，鉴于系统技术复杂，投资较大，在建设中要以现实需求为导向，以有效应用为核心，以技术建设与工作机制的同步协调为保障，确保系统能有效服务于各委办局的需要。从用户业务需求出发，坚持采用科学、先进、成熟的技术，设计科学的应用支撑体系，各子系统既能相对独立性，又能够密切联系、有机配合，通过科学化的建设提升城市级视频综合服务能力。

（5）标准化

系统建设按照统一标准，在符合国家和行业相关标准及地方标准的建设要求基础上，采用先进的技术手段和系统架构，整合已建和社会视频资源，在统一的标准框架下实现统一部署、资源共享、平台共用。

（6）可扩展性

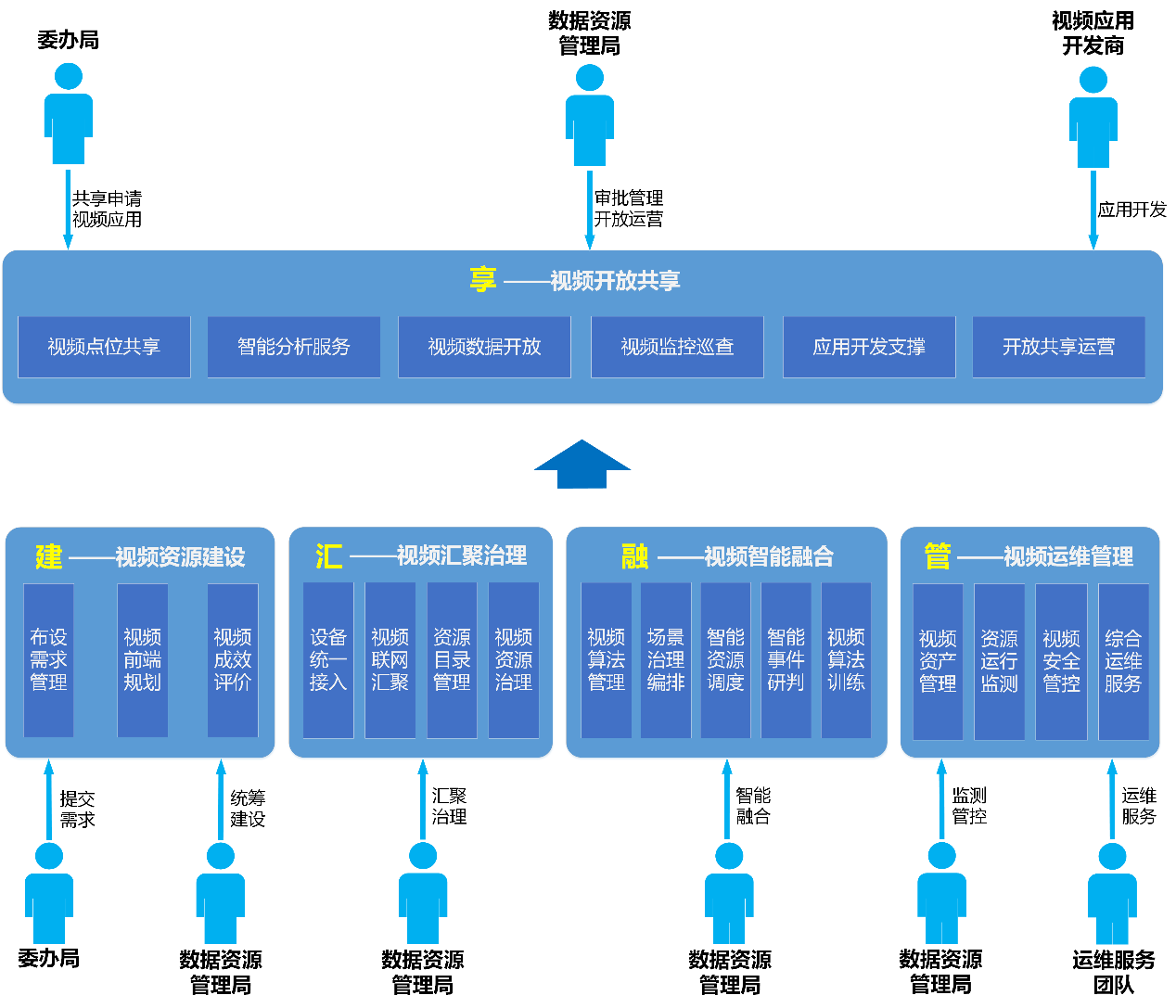
系统总体结构具有兼容性和可扩展性，可兼容不同类型的产品，使整个系统可以随着技术的发展与进步，不断得到充实、完善、改进和提高，并在设计上留有冗余，以便于将来的系统能力扩展。

（7）安全性和可靠性

系统具有容错措施，单点、局部设备故障不影响整体系统的功能和性能，核心和关键资源采用冗余配置。

## 业务架构

视频云中台核心业务是支撑城市构建完整的视频资源建设、共享及应用体系，实现城市视频资源接汇聚整合，并按统一的标准、规范进行视频资源编目与治理，准确、高效地支撑上层应用构建；实现视频资源与智能算法的融合编排，充分挖掘释放视频资源蕴含价值，有效支撑委办局智能分析需求；构建高效的视频运维管理体系，保障视频资源的可靠、稳定、安全的运行；向委办局提供统一的视频应用、资源共享、服务开放等能力，支撑委办局构建丰富的视频智能应用。视频云中台的业务整体上可以概括为“建、汇、融、管、享”五个方面。具体业务架构如图1所示。



1. 视频云中台业务架构图

在视频资源建设（建）方面，由各委办局根据自身业务需要，对视频前端的建设提出需求，由数据主管部门统筹前端需求，利用点位布建工具进行视频建设规划及评价，更加科学合理的开展城市视频前端建设。

在视频资源治理（汇）方面，由数据主管部门开展设备统一接入、视频联网汇聚、视频资源管理、视频资源治理等工作，形成完整、规范的城市视频资源目录及档案。

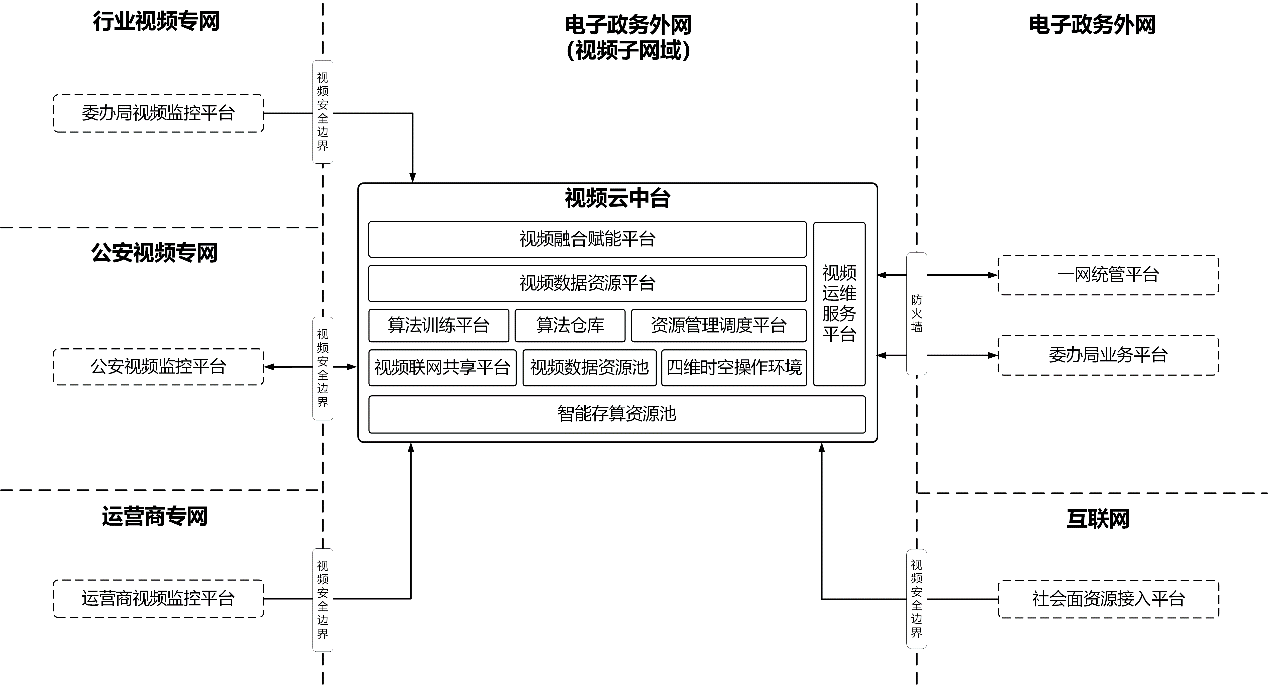
在视频智能融合（融）方面，由数据主管部门开展视频算法管理、智能算法编排、智能资源调度、智能事件研判、智能算法训练等工作，是高效、准确支撑委办局构建视频智能化应用的重要环节。

在视频运维管理（管）方面，由数据主管部门开展视频资产管理、资源运行监测、视频安全管控等工作，由运维服务团队开展视频综合运维服务。

在视频共享服务（享）方面，由委办局提出视频共享、智能分析、事件订阅、服务接口等申请，由数据主管部门进行申请审批，申请通过后即可获取相应的视频资源和服务，委办局可以使用视频通用应用或者视频应用开发商构建的智能应用，数据主管部门进行视频资源的开放共享运营管理。

## 系统架构

各委办局业务应用主要基于电子政务外网进行构建，所以视频云中台需要通过电子政务外网为各委办局业务应用提供可视化、智能化支撑。为满足视频云中台对视频资源的汇聚以及视频图像的传输、解析需求，降低视频传输对电子政务外网现有业务系统的影响，方案设计基于电子政务外网构建视频子网域， 通过视频子网域实现视频资源的汇聚、解析、融合和共享，视频云中台整体部署在视频子网域中，视频云中台通过防火墙等安全设备为电子政务外网提供服务。详细系统架构如图2所示。

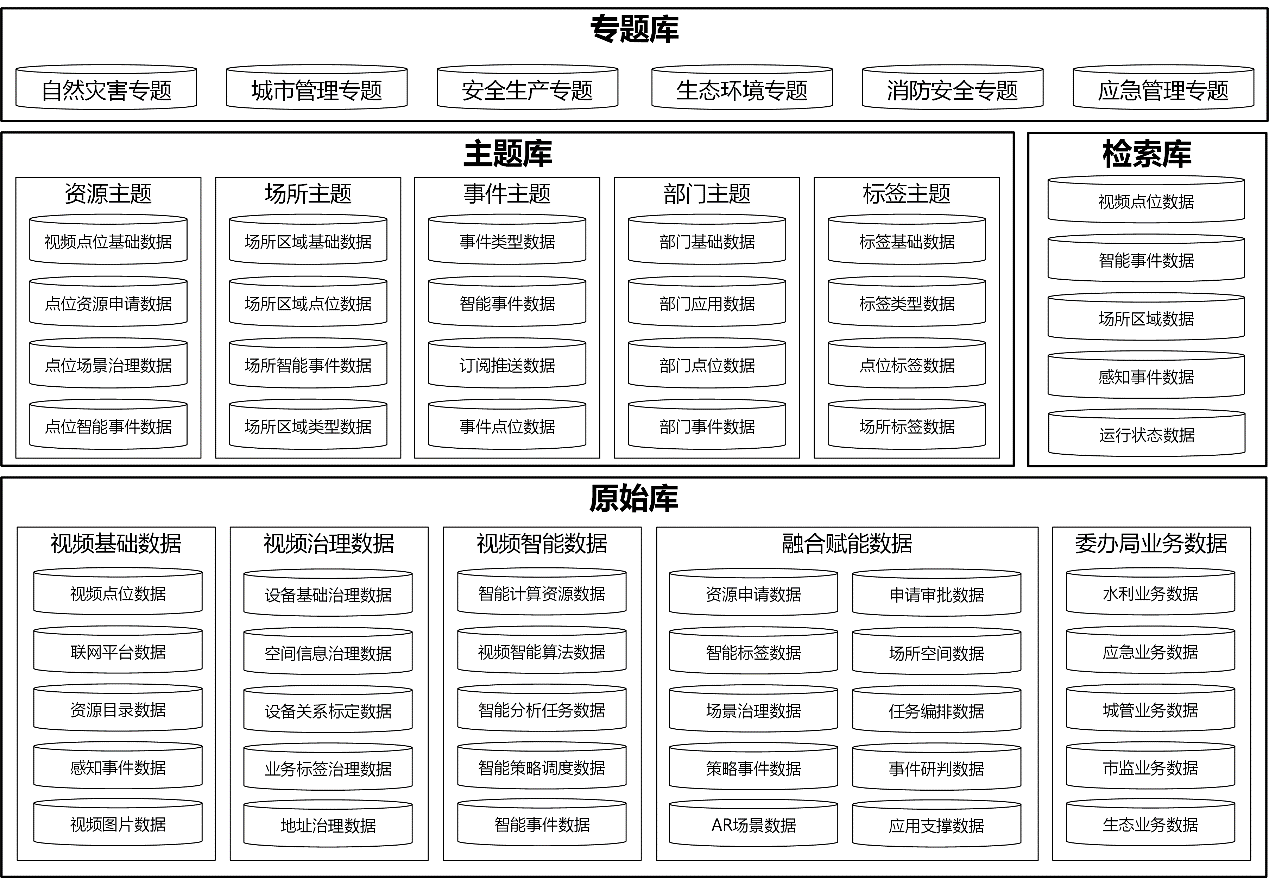


1. 方案系统架构图

视频云中台通过视频安全边界汇聚来行业视频专网、公安视频专网、运营商专网、互联网等网络中的视频资源，向电子政务外网的一网统管平台和委办局业务应用提供视频开放共享、应用支撑，也可以按需为公安视频专网提供视频级联推送。视频云中台建设内容包括视频联网共享平台、资源管理调度平台、视频数据资源平台、视频数据资源池、视频融合赋能平台、算法训练平台、算法仓库、四维时空操作环境、视频运维服务平台、智能存算资源池。

## 数据架构

视频云中台汇聚各类视频资源、感知数据、智能事件及各委办局相关业务数据，并遵从标准规范对各类数据进行汇聚、治理、挖掘，形成原始库、主题库、专题库、检索库等数据组织，为上层应用或其他外部系统提供视图数据服务。



1. 数据架构图

原始库主要包括视频基础数据、视频治理数据、视频智能数据、融合赋能数据、委办局业务数据等内容，原始库数据来自内外部不同平台或系统，是支撑主题库、专题库构建的基础。

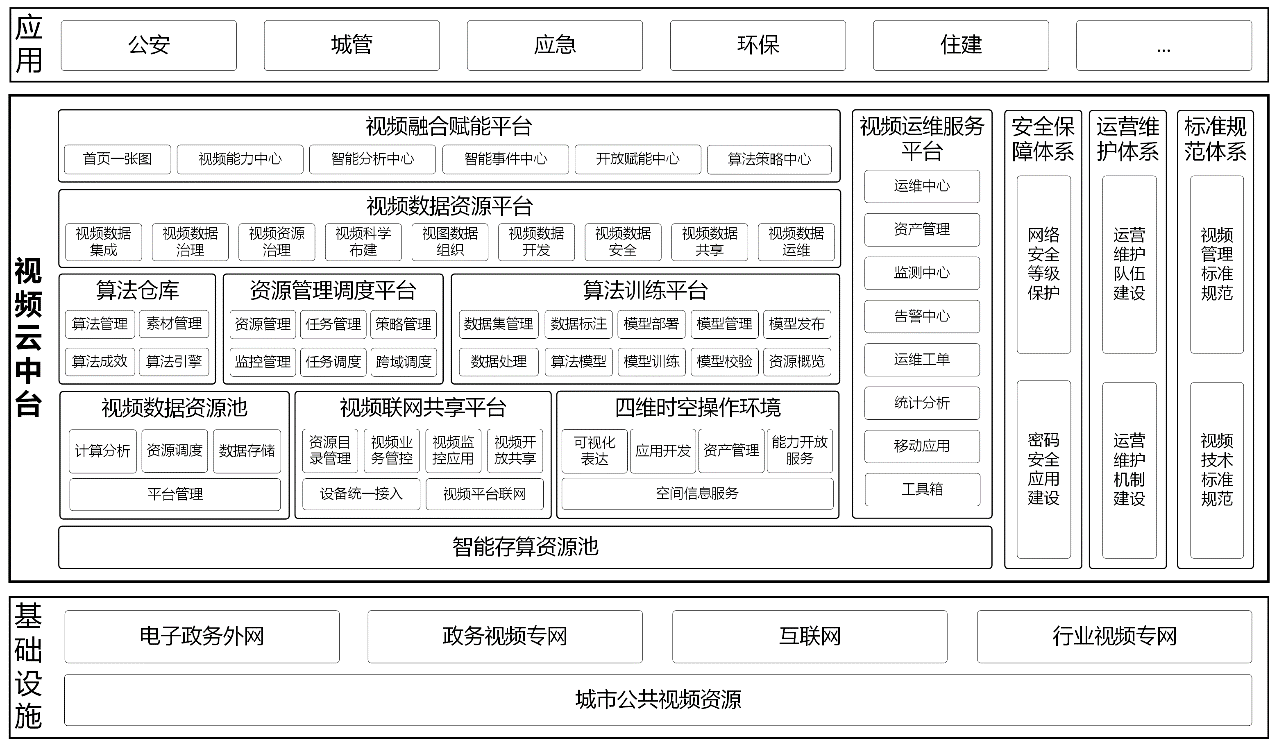
主题库是融合各类原始数据和资源数据而建立的能标识的主题对象，从更高层次对主题对象进行抽象，形成跨业务领域的设备、事件的统一视图，包括资源主题、场所主题、事件主题、部门主题、标签主题等。

专题库则需根据各类专题业务应用场景，构建起对应的专题数据内容，高效支撑专题应用。

检索库为上层应用提供高效的数据检索服务，包括视频点位数据、智能事件数据、场所区域数据、感知事件数据等内容的查询检索。

## 技术架构

视频云中台利用来自公安视频专网、行业视频专网、互联网、运营商专网的视频资源，以视频联网、云计算、大数据、人工智能为核心技术构建视频云中台。详细技术架构如图4所示。



1. 技术架构图

构建智能存算资源池，建立高效、可靠、稳定的计算、存储环境，支撑平台软件及视频智能算法的持续运行，提供海量视频、图片的存储能力。

构建视频联网共享平台，支持设备统一接入、视频平台联网、视频目录管理、视频业务管控、视频监控应用和视频开放共享等能力。

构建视频数据资源平台，支持视频数据、智能事件数据及相关业务数据的汇聚、治理、组织、挖掘和服务，实现对视频点位、业务要素、视图数据的常态化治理，构建视图数据组织，进而开展视图数据挖掘和开放服务，提供视频点位科学布建能力。

构建视频融合赋能平台，提供算法编排、事件推送、策略增效等视频融合能力，以及资源展示、申请管理、运行管理等视频赋能管理能力，实现“一视频多算法、一事件多流向”，满足各委办局不同视频应用需求。

构建资源管理调度平台，支持算力管理、任务管理、策略管理、监控管理、任务调度和跨域调度等能力，实现多类型算力及算法的统一管理与调度，支持基于多种调度策略的算力最优化利用，能够对任务执行状态进行监控管理，并支持跨网络的智能任务调度和智能结果同步。

构建算法仓库，提供算法管理、算法评价、素材库等功能，支持多类型视频智能算法的统一管理和高效使用，并支持同算法训练平台同步图片素材和算法模型。

构建四维时空操作环境，为视频云中台和外部业务应用提供统一的可视化表达、地图态势标绘、空间信息服务等基础能力。

构建算法训练平台，提供本地化算法训练、算法优化服务，帮助各委办局更加深入的开展视频智能分析，精细、精准提升自身业务能力。

构建视频运维服务平台，支持视频资产统一管理、运行状态统一监测、故障处置统一闭环等能力。

构建视频安全保障体系，包括网络安全等级保护、密码应用安全建设。

构建视频运营维护体系，包括运营维护队伍建设和运营维护机制建设。

构建视频标准规范体系，包括面向视频统筹建设管理、视频统一联网共享、视频统一开放服务相关的技术标准和管理规范。

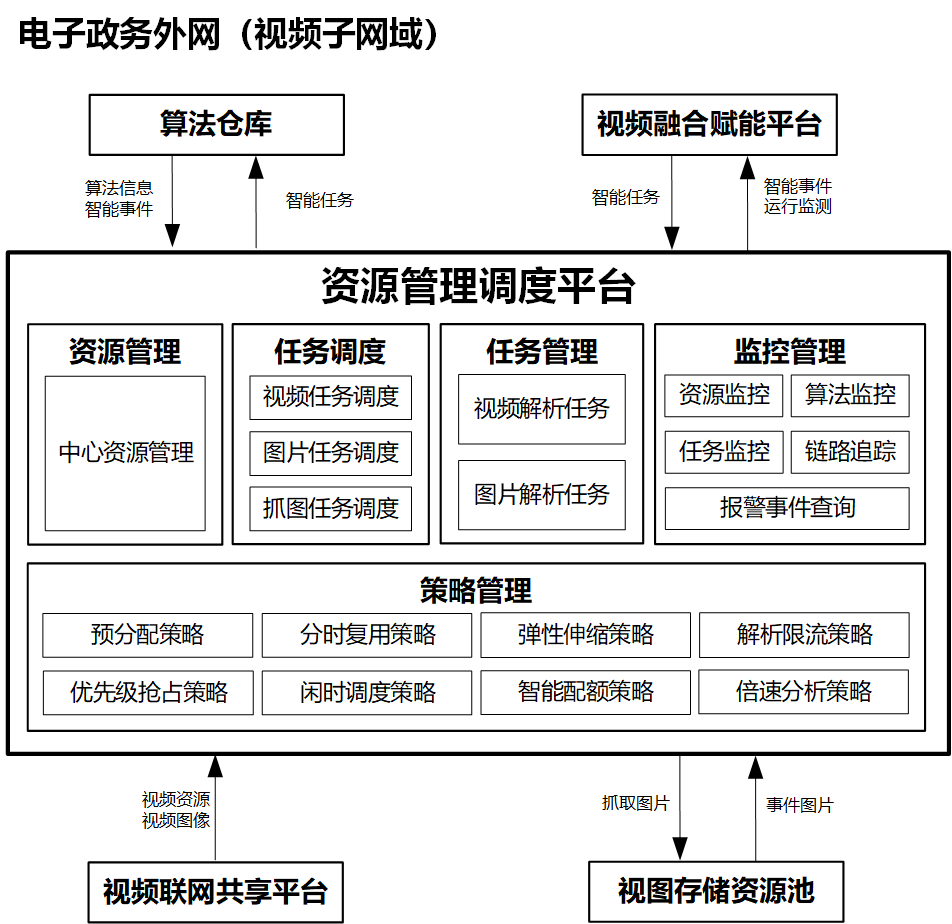
# 资源管理调度平台设计

## 概述

资源管理调度平台是整个视频云中台智能相关的管理调度中心，基于各类视频智能分析任务，对智能算力资源进行整体管理并按需调度，实现对各类智能计算资源的高效、合理利用。平台提供多种智能算力资源的集中管理能力，并结合丰富、灵活的智能调度策略，接收上层应用平台智能分析任务，利用有限的智能计算资源高效地处理智能分析任务，并对全过程进行监控和管理。资源管理调度平台主要功能包括资源管理、任务管理、策略管理、监控管理、任务调度、跨度调度。

## 架构设计

资源管理调度平台基于视频联网共享平台获取视频码流图像，将抓取的视频图片存储到视图存储资源池中，从算法仓库中获取相应的智能分析算法包，将智能分析工作任务调度到智能计算资源池中执行，将智能事件接入到视频数据资源平台，事件图片则存入到视图存储资源池中，并最终推送智能事件、运行监测等内容到视频融合赋能平台。详细架构如图6所示。



1. 资源管理调度平台架构图

## 功能设计

资源管理调度平台功能模块包括：资源管理、任务管理、策略管理、监控管理、任务调度、跨域调度。

### 资源管理

资源管理调度平台支持对中心端各类智能计算资源的接入、管理，是高效开展智能分析的基础。

#### 中心资源管理

提供对各类中心智能计算资源的接入，支持获取查看计算资源的设备名称、设备类型、设备IP、算力类型、算力数量、设备状态等信息，并能通过控制操作权限对设备进行智能算法同步，可以将算法仓库中最新的特定算法包文件同步给指定智能分析服务。

### 任务管理

平台支持创建和管理特定的智能分析任务，包括视频解析任务、图片分析任务等，实现计划任务和临时任务的分析。

#### 视频解析任务

支持实时视频、在线录像分析任务的创建、删除、编辑、查询和导出。新建任务时，支持填写任务的基本信息、数据源、输出地址等信息，基本信息包括任务名称、任务类型、算法信息、码流类型、时间计划，数据源支持以目录选点、地图选点、文件导入等方式选择待分析的点位。支持基于任务名称、算法名称、任务来源、任务类型对视频解析任务进行检索；支持检索条件的重置。支持分页展示任务名称、任务类型、算法名称、任务来源、任务状态、数据源、创建时间等信息。支持批量删除选中任务；支持启动或停止任务；支持导出选中数据或全部数据。

#### 图片解析任务

平台支持创建实时抓拍图片分析任务、名单库分析任务，实现图片中目标检测、建模、属性分析。

##### 图片流解析任务

支持图片流分析任务的添加、删除、编辑和数据导出。新建任务时，支持填写任务的基本信息、输入地址和输出地址；基本信息包括任务名称、算法信息以及是否开启闲时分析；输入地址包含分析数据类型、队列名称，支持以目录选点、地图选点、文件导入等方式选择待分析的点位。支持基于任务名称、算法名称、任务来源、任务状态对图片流分析任务进行检索；支持检索条件的重置。支持分页展示任务名称、算法名称、任务来源、任务状态、数据源、创建时间等信息。支持批量删除选中任务；支持启动或停止任务；支持导出选中数据或全部数据。

##### 图片库解析任务

支持基于任务名称、算法名称、任务来源、任务状态对图片库分析任务进行检索；支持检索条件的重置。支持展示任务名称、算法名称、任务来源、任务状态、数据源、创建时间等信息。支持批量删除选中任务，支持启动或停止任务，支持导出选中数据或全部数据。

### 策略管理

平台支持基于多种策略对算力资源进行合理调度分配，在满足用户解析分析需求的同时保障资源的利用效率最大化。

#### 预分配策略

针对对智能计算资源有高稳定需求的业务应用和算法任务，平台可以提供资源预分配策略，将特定范围、数量的智能计算资源直接分配给特定的应用对象或者算法任务，从而可以有效保障计算资源的可靠、稳定和持续。支持对不同的视频、图片算法进行计算资源的预分配；支持对每个算法分配计算资源的预分配量、动态分配最大量等参数进行配置。

#### 优先级抢占策略

高优先级任务优先分析，实现紧急任务、重点任务的资源保障和及时处理；对于允许抢占的场景，高优先级任务可以抢占低优先级任务优先执行。支持通过开关配置开启或关闭视频流任务抢占功能。支持按点位名称、任务类型、任务状态对任务进行查询，展示内容包括子任务编号、点位名称、所属任务名称、算法名称、任务类型、任务状态、优先级等信息。支持按照子任务名称、子任务编号、子任务状态对任务进行检索，支持检索条件的重置。支持分页展示子任务编号、子任务名称、所属任务名称、任务类型、算法名称、子任务状态、子任务优先级、被强占的子任务编号。支持对子任务的优先级进行编辑修改。

#### 分时复用策略

分时复用策略是一种采用同一计算资源不同时间段来加载不同的算法的功能，能达到一算力、多算法的目的。通过对统一计算资源不同时段来加载不同的算法，实现一算力，多算法的调度；支持时复用策略查看，查看一个计算单元不同时序加载的不同的算法，支持通过颜色区分算法加载时段。

#### 闲时调度策略

在计算资源不足时，闲时调度策略能够实现缓存分析要求实时性不高的任务，等智能计算资源空闲时，再进行分析处理。支持配置最大分析延时；支持对视频算法、图片算法配置闲时分析模式；支持展示配置后的算法调度情况。支持按时间段设置任务，并自动下发任务进行执行，实现多个任务、多种算法的调度。

#### 弹性伸缩策略

计算资源运行过程中，实际情况可能与预期有一定差距，例如不同图片大小分析资源消耗不同等。弹性伸缩策略通过实时监控计算资源使用情况、分析任务延时、等待任务队列大小等指标项，进一步调整资源分配，使用户计算资源达到最佳使用效率。支持弹性伸缩配置的展示，包括图片算法和视频算法的展示；支持弹性伸缩记录的展示。支持查看每种算法当前的动态并发量；支持设置每个算法动态分配算力资源的最大量上限。

### 监控管理

平台支持对中心端资源、算法运行状态、智能任务状态、事件报警等信息进行统一查看和管理。

#### 资源监控

支持实时监控中心端计算节点的IP、端口、在线状态、计算单元类型、计算单元使用量等基本信息及在线状态。支持展示每个计算节点下启用计算单元的基本信息，包括所属计算节点IP、计算单元编号、剩余资源量、在线状态、加载算法、加载名单库等信息。

#### 算法监控

支持监控当前所有计算节点的运行状态、计算单元类型、计算单元数量。支持监控当前所有算法的加载状态以及运行的计算节点、计算单元。支持监控当前所有GPU卡是否空闲、当前加载的算法、名单加载状态等信息。

#### 任务监控

提供视频和图片智能分析任务的监控。

##### 视频任务监控

支持实时监控视频任务的基本信息和运行状态；支持查看视频任务所包含的各监控点或离线视频文件的分析执行情况及关联的计算资源、运行的算法情况等信息。支持查看每个视频任务的分析结果，包括分析结果统计情况、分析报告等。

##### 图片任务监控

支持实时监控图片任务的基本信息和运行状态；支持实时监控图片任务的分析结果；支持实时监控分析过程中的分析异常记录信息。

#### 报警事件查询

支持配置报警策略；支持查看并处理算法异常报警、算法授权报警、任务异常报警等报警信息。

#### 链路追踪

链路智能追踪支持对数据从生产到消费过程中的全链路进行监控；支持查看全链路过程中数据的生产速率、消费速率和数据积压未处理的数据量。

### 任务调度

平台支持对视频分析任务、图片分析任务以及抓拍任务进行按需调度。

#### 视频任务调度

支持基于可用算力将视频任务调度到对应合适的GPU资源上；

支持对网络抖动等异常引起的视频取流失败进行重试，自动恢复任务执行；

支持基于优先级、强制等调度策略对视频分析任务进行调度；

支持基于用户需求对视频任务调度参数进行配置。

#### 图片任务调度

支持基于可用算力将图片任务调度到对应合适的GPU资源上；

支持对网络抖动等异常引起的图片调用失败进行重试，自动恢复任务执行；

支持异步、同步等不同的图片分析调度策略；

支持基于用户需求对图片任务调度参数配置。

#### 抓图任务调度

支持根据视频融合赋能平台算法编排需求，按照设定的预置位、时间间隔从视频联网共享平台调阅实时视频流进行抓图操作，并推送抓拍图片进行分析；

支持基于周期计划（预置点、巡航等）对抓拍任务进行调度；

支持基于抓拍限流等调度策略动态生成抓拍任务计划。

## 性能设计

（1）图片分析调度性能

图片分析最大支持1000张/s并发调度。

（2）视频分析调度性能

后端视频分析最大支持5000路并发调度。

（3）视频抓图性能

单节点（千兆网络环境）可实现4M码流 100路并发取流抓图。

## 资源规划

（1）平台应用服务器

需配置1台平台应用服务器（CPU：32核2.2GHz及以上；内存：64GB；硬盘：300G SAS；网络：1GbE，可以采用同规格虚拟机）用于部署资源管理调度服务。

（2）视频抓图服务器

视频抓图服务器部署抓图服务。单节点（CPU：32核2.2GHz及以上；内存：64GB；硬盘：300GB SAS，1000GB SATA；网络：1GbE，可以采用同规格虚拟机）可实现4M码流并发100路取流抓图，考虑网络延迟及平台处理，预估每个视频点位10秒完成抓图工作，则单节点一分钟可以抓图600路，五分钟可以抓图3000路。

*//项目智能分析需求需要对一万路视频点位每隔五分钟进行抓图分析，则需要四台抓图服务器节点才能完成该工作。*

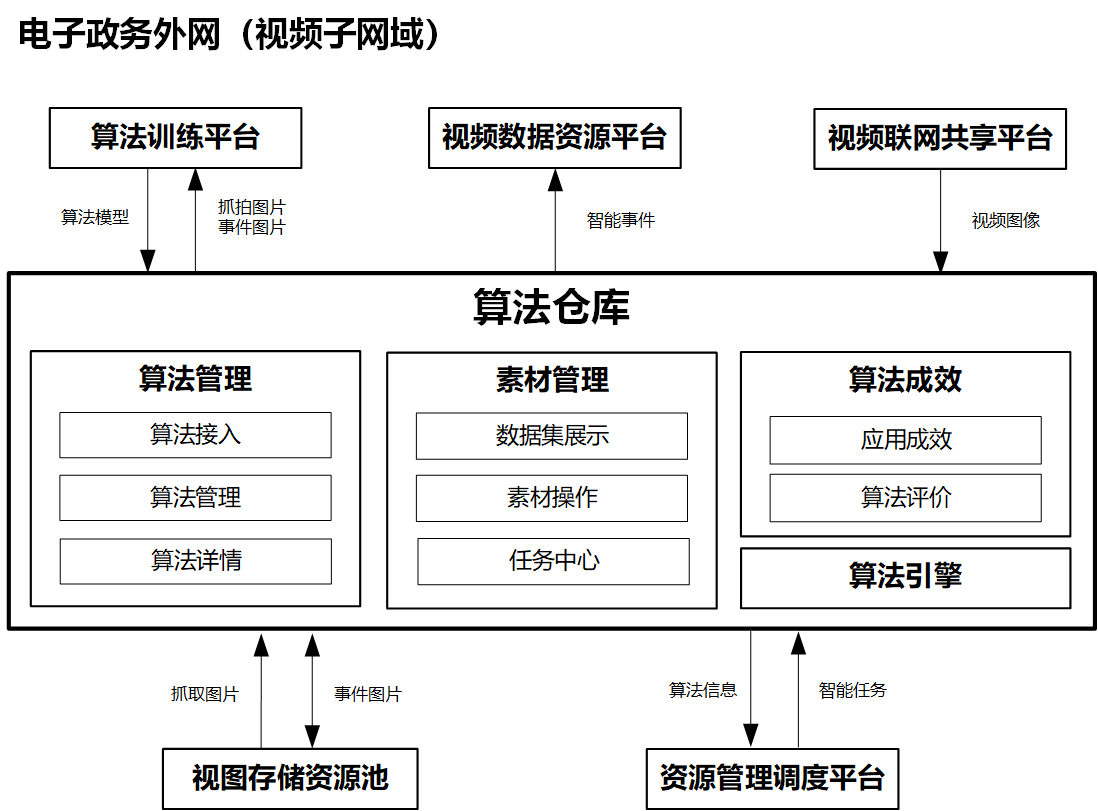
# 算法仓库设计

## 概述

算法仓库为视频云中台提供视频智能分析算法的集中管理能力，实现算法的全生命周期管理，包括算法的导入、封装、发布、更新等功能。算法仓库可以对边缘端、中心端的检测算法、建模算法、比对算法等算法包进行管理，提供算法的统一授权体系，为统筹开展算法的调度与应用提供基础。算法仓库可以为用户构建视频算法相关的技术标准体系，支持外部的算法包的导入，也支持外部算法服务的接入。算法仓库主要功能包括算法管理、素材管理、算法成效。

## 架构设计

算法仓库可以从算法训练平台同步视频智能算法，并将算法信息发布给视频融合赋能平台支撑算法编排工作，也需要将算法信息给到资源管理调度平台，以支持资源管理调度平台将智能任务下发到算法仓库中的算法引擎，算法引擎则通过视频联网共享平台拉取具体视频资源的图像执行分析工作。详细架构如图7所示。



1. 算法仓库架构图

## 功能设计

算法仓库功能模块包括：算法管理、素材管理、算法成效、算法引擎。

### 算法管理

算法仓库提供算法管理和展示能力，平台管理员可以对算法的基本描述信息（算法名称、算法描述）进行编辑，还可以对算法进行增、删、改、查等操作，同时还支持对外部算法包进行接入管理。

#### 算法接入

（1）算法包接入

支持上传按照标准封装好的算法包；支持上传算法模型，填写描述信息、版本迭代说明后按照算法封装标准将算法模型封装成规范化的算法包；支持中心端通用GPU服务器、前端摄像机、智能NVR各计算平台的算法包。

（2）算法系统接入

支持接入外部算法系统，自动获取对接的算法系统中的算法。

（3）算法系统镜像接入

支持算法镜像的接入。

（4）算法模型同步、打包

支持对接算法训练平台，将算法训练平台上训练的算法模型列表，同步到算法仓库；支持选择模型后直接在算法仓库中添加算法描述信息，封装成算法包，最终打成的算法包在算法仓库保存并可以被调用。

（5）算法包合规性校验

采用统一标准化方式对集成开发算法、外部算法、算法训练平台算法进行导入管理；自动校验上传的算法包是否符合规范，支持对不符合规范的算法包进行封装处理；上传算法包时，批量校验算法包中的每个算法授权情况，包含授权检测。

（6）算法包自动更新

支持算法训练平台的训练模型自动更新；首次打包训练模型时，需从模型同步列表手动选择要打包的模型，在算法封装页面填写算法信息进行打包；开启自动更新的算法，被关联的模型编号如有更新的模型版本，自动封装新的算法包至算法仓库，版本号自动累加；支持在“自动更新管理”页面查看自动更新的算法列表及更新记录，支持选择“自动更新”开关。

（7）自动切换任务中的算法版本

支持同一个算法快速选择不同版本，切换查看算法详情信息；支持通过算法任务切换功能，将运行中的算法任务切换至选择的算法版本，校验算法版本能无感切换后，自动切换运行算法任务中的算法版本。

#### 算法管理

（1）算法授权激活

支持跳转至授权服务器进行算法授权。

（2）算法上/下架

支持本地上传算法包中的算法以及级联算法上架、下架，下架算法时，弹窗提示进行二次确认，下架算法可能影响已编排的任务，是否确认下架相应算法。

（3）算法检索

支持直接通过算法名称关键字检索算法。

（4）算法筛选

支持按算法状态（上下架状态、授权状态、级联共享状态）、分析源类型、计算平台、来源厂商、算法入库时间、算法标签分组等标签对算法进行筛选。

（5）算法删除

支持已上传算法、级联算法单次批量删除；删除时弹窗提示：删除算法可能影响已编排的任务，是否确认删除算法。

（6）算法列表

展示算法仓库内有的所有算法，包含算法封面、算法名称、算法版本、入库时间、分析源类型、来源厂商、计算平台、分析类型、算法授权（已授权、未授权）/共享/上架等信息，支持进行算法上/下架、算法共享、添加分组、删除算法、查看详情等操作。

#### 算法详情

（1）算法信息

支持查看算法的可用范围、技术指标等详情信息，包含算法封面、算法名称、算法标识、算法描述、技术规格、分析源类型、分析目标、适用行业、场所、硬盘/内存/显存占用、CPU核数、来源厂商、计算平台、运行环境、输入源规格、计算能力等信息。

（2）算法信息编辑

支持以算法的维度编辑修改算法信息，允许修改信息：算法封面、算法名称、算法描述、分析目标、适用行业、业务、场所、来源厂商。

（3）算法检出项

显示每个算法能检测的事件检出项；设定唯一的算法检出项事件码；可进行检出项事件码映射，以便对应已定义过的下发给设备的事件码。

（4）算法模型信息

展示算法训练平台训练出的模型的相关信息：模型名称、数据集版本编号、模型版本、模型版本编号。

（5）算法状态

显示算法算法授权（已授权、未授权）/上架等信息。

（6）算法操作

支持进行算法上/下架、算法详情查看、算法添加分组、算法删除等操作。

（7）算法版本管理

支持在算法详情查看该算法的不同版本内容，多版本一卡片展示，记录历史算法版本迭代说明，支持切换算法版本号，查看同一算法不同版本号的算法详情介绍。

（8）应用条件

支持查看图片格式、目标像素要求、目标遮挡粘连、画面质量、其他要求等算法应用条件信息。

（9）场景说明

针对算法适用场景、不适用场景进行详细的图片、文字描述。

（10）算法声明

支持展示算法在极端情况下产生误报或漏报的声明信息。

### 素材管理

素材管理支持所有视图素材集中统一管理，支持对素材进行操作，对接算法训练平台，推送素材进行算法训练，为现场算法迭代优化提供技术支撑。

#### 数据集展示

（1）数据集管理

支持图像数据集的创建、编辑、查询，区分训练集（用于真实算法训练所需的素材集）和校验集（用于进行算法推理校验的素材集）；支持素材集名称搜索。

（2）创建新版本

每个素材集支持创建新版本，可选择本地上传还是平台推送，平台推送需要选择关联算法和算法版本号。数据集支持继承、发布、删除、版本信息展示，校验集支持用于算法测试；显示数据集信息：算法类型、最新版本、素材来源（本地上传、平台推送）、标签数量、标注进度、研判进度、发布状态、清洗状态、增强状态、标注状态、操作；支持操作导入、清洗、增强、质检、下载、标注、研判、删除。

#### 素材操作

（1）数据管理

支持数据的导入、数据的展示以及检索，数据的导入支持本地导入和已有数据集导入，支持按照已标注、未标注、待确认过滤展示数据，支持按照上传时间正序/倒序展示数据；支持上层业务平台按照素材回流标准协议回流导入，导入的素材需要携带算法类型参数。

（2）数据回流

支持图像单分类、图像多分类、物体检测模型、混合模型四种模型数据的回流功能。

（3）标签管理

支持标注标签的新增、修改、删除、选择。

（4）素材清洗

支持针对一个数据集版本创建一个清洗任务，清洗任务支持覆盖原有版本和生成新版本两种方式。覆盖原版本则直接在原版本把满足清洗条件的数据删除掉，生成新版本则会自动创建一个新的版本，然后新的版本中不包含被清洗掉的数据；支持选择清洗方案：去除相似图片、去除重复图片、去除小目标图片、去除过暗图片、去除过曝图片、去除模糊图片；清洗任务支持异步进行，在列表中体现清洗进度（选择覆盖原有的，直接在清洗状态显示，选择生产新版本的，新版本的清洗状态展示）；支持创建、删除、查看清洗任务，支持清洗后根据结果过滤查看；支持查看清洗任务的详情，支持查看每种清洗效果清洗掉的数据和清洗之后保留的数据。

（5）素材增强

支持针对一个数据集版中的部分或全部图片进行增强处理，增强方式有覆盖原有版本和生成新版本两种方式，覆盖原有版本的方式是在原来的版本上新增增强后的数据，生成新版本则表示先才能创建一个继承该版本的新的版本，然后增强数据新增到新的版本中去。

（6）素材质检

支持素材质检，进入素材质检界面，内容有分辨率分布、宽高比分布、图片亮度分析、图片模糊分析、正负样本统计；支持导出质检报告，查看数据集的数据诊断结果，标注信息统计、标注占原面积比、标注区域宽高比分布比、标注区域堆叠情况、图片亮度分析、图片模糊分析、分辨率分布、宽高比分布。

（7）素材下载

支持创建、删除、查看下载任务记录，支持素材打包下载，可选已标注、未标注数据。

（8）素材标注

支持素材数据在线标注的功能，单分类和多分类模型支持选择标签，其他模型支持框选目标并选择标签，支持选择图片感兴趣区域；所有素材可分为已标注、未标注；支持素材导入，支持文件和文件夹形式；展示标注区域，区域内提供标注工具，标注类型、放大、缩小、复位、撤销、恢复、裁剪、删除、下载，标注图片切换，采用方向快捷键；标注状态有已达到训练标准、未达到训练标准，提供未达到标准的解释；针对物体检测和混合模型支持智能标注功能，智能标注支持主动学习和预标注两种标注方式，先进行预标注，用户确认，然后系统迭代预标注，结束智能标注。

（9）素材研判

仅平台推送素材，所有算法产生的数据，提供抽样研判模式；对回流的数据支持全部研判和抽样研判。

（10）素材级联

支持素材级联发起方主动选择素材库中的某一数据集，选择接收方平台，与接收方建立该数据集的级联关系；支持选择是否要推送标注信息，以及推送模式（手动模式/自动模式），默认选择自动模式；支持在数据级联管理中，展示所有数据集级联关系的列表信息。包括级联数据集名称、首次建立级联时间、数据级联接收方/发起方名称、数据级联状态、结束级联/重新级联按钮；支持查看某个数据级联关系下的每次推送任务详细信息；支持结束级联或删除级联关系；支持展示级联数据集和级联状态，仅支持查看级联数据集中的内容。如要使用“级联数据集”的数据，需将“级联数据集”内的数据导入（或合并）至一个新建的（或已有的）“训练集/校验集”中，再对数据进行操作。

#### 任务中心

（1）任务中心

清洗任务、增强任务、下载任务的进度展示界面，默认在素材版本列表页创建任务后自动开启，可在此模块进行手动停止任务或删除，任务删除必须是已停止或已完成状态。

（2）展示各项任务

清洗任务：任务提交时间、数据集、版本号、任务状态（已停止、清洗中、已完成）、操作（停止、开启、删除）；

增强任务：任务提交时间、数据集、版本号、任务状态（已停止、增强中、已完成）、操作（停止、开启、删除）；

下载任务：任务提交时间、数据集、版本号、任务状态（已停止、下载中、已完成）、操作（停止、开启、删除）。

### 算法成效

结合素材管理，对智能算法的成效进行统计，包括应用成效和算法评价。

#### 应用成效

支持对算法实际使用过程中的数据进行研判，根据研判的结果输出算法指标：

（1）算法总体精确率、每个目标精确率、算法分析总张数、已研判总张数、已研判目标数；

（2）区分总体数据、每日数据（可以切换为每日、每周、每月、每年数据）。

#### 算法评价

支持使用固定校验集，对不同厂商的同一个算法，或同一厂商不同版本的算法进行算法测试，输出算法的评估指标，包括检出率、检准率等。

### 算法引擎

算法引擎是视频智能分析的核心模块，支持加载不同的视频分析算法，运行在各类智能计算资源环境之上，执行视频图像内容的解析工作，输出智能分析结果数据。

## 智能算法

城市治理过程中常用的视频智能分析算法如表1所示，具体可结合项目实际需求选择使用。

*//如果项目有做过调研，建议把具体项目需要的算法清单内容进行表格呈现*

1. 城市治理视频智能算法列表

| 序号 | 算法名称 | 功能说明 | 适用场所 |
| --- | --- | --- | --- |
| 1 | 暴露垃圾检测 | 根据输入的图片进行检测、分析，识别出图片中公共场所内未放入垃圾容器的生活垃圾，主要指未打包、散乱在公共场所的垃圾 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 2 | 打包垃圾检测 | 检测图像画面中是否存在，装好的打包垃圾，没有按规定放入垃圾箱，而是堆放在街面或者道路上的情况 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域，居住建筑/住宅建筑/周边路段，居住建筑/住宅建筑/垃圾分类点 |
| 3 | 道路破损检测 | 检测道路是否存在裂缝、松散、坑槽、塌陷等道路破损问题 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 4 | 道路污水检测 | 检测画面中是否存在随意排放污水到人行道等影响市容、污染环境的情况 | 道路/市内道路/道路周边 |
| 5 | 道路遗撒物识别 | 检测街面道路上是否存在车辆运输或装卸过程中产生的遗撒物 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 6 | 动物尸体未清理 | 通过对公共场所的输入图片检测、分析，识别出图片中没有及时清理的动物尸体目标 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 7 | 非装饰性树挂检测 | 检测非挂饰树上是否存在违规挂饰的现象 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 8 | 废弃家具检测 | 通过对输入图片分析、检测，识别出未经许可丢弃在公共场所的废弃家具 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域，居住建筑/住宅建筑/周边路段 |
| 9 | 焚烧垃圾树叶检测 | 通过对输入图片的检测、分析，识别出图片中的焚烧垃圾树叶的目标或行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 10 | 管线杆线架设检测 | 识别违反城市管理规定，擅自在城市道路等架设管线、杆线等设施的行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 11 | 积存垃圾渣土检测 | 检测图像中是否存在建筑拆建或房屋装修产生的弃土、弃料及其它废弃物堆积 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 12 | 空调外机低挂检测 | 检测在房屋外墙是否有空调外机低挂，影响市容市貌的情况 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 13 | 垃圾桶不规范检测 | 识别公共区域内没有按照城市管理或者小区管理要求使用符合要求的垃圾桶，如使用了竹篓、 塑料桶（篓），油漆桶代替规范垃圾箱的现象 | 居住建筑/住宅建筑/垃圾分类点，居住建筑/配套服务设施建筑/垃圾分类点 |
| 14 | 垃圾箱满溢检测 | 通过对输入的生活垃圾箱的图片进行检测、分析，判断垃圾箱装满或溢出后未及时处理的现象 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 15 | 露天烧烤检测 | 通过对输入图片进行检测和分析，识别出图片中存在的露天场所烧烤行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 16 | 乱堆物堆料检测 | 识别未经许可在公共场所堆放的物料，包含桶子、水泥砖块、模板、建设用具、施工用具、房屋拆卸物 | 居住建筑/住宅建筑/消防通道 |
| 17 | 绿地脏乱检测 | 通过对输入的图片进行检测、分析，识别出图片中的绿地中是否存在垃圾、脏乱等现象 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 18 | 绿化弃料检测 | 检测区域内是否存在绿化工作遗留没有及时进行清理的绿化弃料，如：修剪树木，花草，等产生的枝叶，泥土等，影响城市市容环境卫生 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 19 | 气模拱门检测 | 检测婚礼，开业庆典等场景下是否存在占用公共区域，违规使用气模拱门的情况 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 20 | 水域不洁检测 | 通过对输入图片进行检测、分析，检测公共水域水面是否存在垃圾、水藻，水域是否清洁 | 河道/水道/水道区域 |
| 21 | 饲养家禽家畜检测 | 检测道路周边或者小区内，是否存在未经批准，擅自饲养家禽家畜，在笼中或散养鸡、鸭、兔等，污染环境，影响市容环境卫生 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 22 | 违规撑伞检测 | 检测街面上是否存在经营撑伞的现象，如在店门口撑伞经营，路边撑伞经营 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 23 | 违章接坡检测 | 检测是否存在擅自用铁架子、钢板、三角木块或者混泥土等材质，连接机动车道与人行道而设置的斜坡行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 24 | 沿街晾挂检测 | 检测主要道路及公共场所的树木、护栏、路牌及电线杆等设施上是否存在吊挂晾晒的物品 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 25 | 店外经营检测 | 检测经营商品超出店面范围，摆放到人行道、车行道，影响车辆通行的经营行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 26 | 非机动车乱停检测 | 识别在未经许可、未合法设置停车泊位的地点停放非机动车，或乱序停放的行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 27 | 废品收购占道检测 | 检测道路周边、桥梁等场景是否存在占用公共区域，进行废品回收行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 28 | 机动车乱停检测 | 检测街面道路上是否存在违反交通规章制度，违规停放机动车辆的行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 30 | 无照游商检测 | 检测画面中是否存在无证经营或者游商行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 31 | 占道经营检测 | 检测是否有占用城市道路、桥梁、城市广场等公共场所进行盈利性买卖商品或服务的行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 32 | 工地物料乱堆检测 | 通过对施工场所的图片进行检测、分析，识别出图片中堆放的施工物料，判断是否存在违规堆放或未及时清理的现象 | 建筑住宅/建筑工地/重点施工区域 |
| 33 | 施工废弃料检测 | 通过输入的图片进行检测、分析，识别出在施工结束后，没有及时清理施工废弃料的现象 | 建筑住宅/建筑工地/重点施工区域 |
| 34 | 施工占道检测 | 检测是否有违反道路管理，设置道路障碍、占用道路施工的行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 35 | 牌匾破损检测 | 通过对输入图片的分析、检测，对比完好广告牌，识别出广告牌是否破损 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 36 | 宣传栏破损检测 | 通过对输入图片的检测、分析，识别出图片中公共宣传栏目标，判断宣传栏是否存在以下异常：破损、移位、凹陷或凸起、废弃 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 37 | 道路积水检测 | 通过图像识别技术，检测各低洼路段的积水水位，当道路积水达到未税水位，发布内涝积水预警 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 38 | 路面塌陷检测 | 检测道路是否存在自然或者人为因素导致的道路塌陷，影响行车 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 39 | 非法小广告检测 | 对街道两旁、公交站牌等公共区域进行检测，识别是否存在非法张贴的广告 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 40 | 街头散发广告检测 | 通过对输入图片进行检测、分析，识别出图片中是否存在街头散发广告的行为现象 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 41 | 违规户外广告检测 | 识别设置在户外，以灯箱、霓虹灯、电子显示装置、展示牌等为载体的广告设施 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 42 | 违规牌匾检测 | 对街道两旁、公交站牌等公共区域进行检测，识别是否存在非法悬挂的牌匾 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 43 | 宣传幅检测 | 检测公共区域（如城市道路两侧的建筑物、围墙、树木、杆体、交通护栏、立交桥体、人行天桥等）是否有悬挂的标语、条幅、气球直幅 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 44 | 电力设施异常 | 通过对输入的电力设施图片进行检测、分析，对电力设施状态进行识别，判断电力设施是否异常 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 45 | 井盖异常检测 | 检测道路上的井盖是否存在丢失、井盖未盖紧等异常情况 | 其他设施/城市井盖/周边区域 |
| 46 | 消防设施损坏检测 | 通过对输入的消防设施图片进行检测、分析，对消防设施状态进行识别，判断消防设施是否存在异常以下异常：破损、 歪倒、老旧，缺件，锈蚀的消防栓 | 道路/市内道路/道路周边，居住建筑/住宅建筑/消防通道 |
| 47 | 雨水箅子损坏检测 | 通过对输入图片进行检测、分析，识别出图片中路边的雨水箅子目标，并对比完好的目标对象，判断是否损坏 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 48 | 雨水箅子堵塞检测 | 通过对输入图片进行检测、分析，识别出图片中路边的雨水箅子目标，并对比完好的目标对象，判断是否堵塞 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 49 | 便道桩异常检测 | 检测道路中间便道桩是否存在颜色褪色、破损等异常情况 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 50 | 防撞桶破损检测 | 通过对输入图片的分析、检测，识别出公共场所的防撞桶目标，并对比完好的目标对象，判断防撞桶是否已破坏 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 51 | 柔性隔离体破损检测 | 检测柔性防护网、柔性护栏等柔性隔离体是否存在破损、歪斜、倒伏情况 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区 |
| 52 | 护树设施损坏检测 | 检测护木设施如护树架等是否存在破损情况 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 53 | 树木倒伏检测 | 检测树木是否有成片繁盛歪斜甚至全株匍倒在地的现象，如：狂风吹致使树木倒地 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 54 | 临街屠宰检测 | 检测监控的街道区域是否存在宰杀家禽加粗的行为，此处特指悬挂或放在地上的明显的屠宰行为 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 55 | 违建检测 | 通过图片分析识别技术，对图片中的建筑物进行检测，识别出图片中的违建建筑，可适用于城市管理市政等场景，包括压路机、渣土车、水泥搅拌机、砂石堆、土工布、沙土堆、挖掘机、推土机、塔吊、施工人员、活动板房、农用机械、传送机械、人力推车、货车、水泥车、吊车、围墙挡板、砖头堆、脚手架、违建房屋等 | 居住建筑/住宅建筑/消防通道 |
| 56 | 工程车检测 | 利用视频图像技术对监控区域内的车辆进行识别、检测，根据分析车辆特征识别出常见的工程车车型，包括压路机、渣土车、挖掘机、推土机、货车、水泥车、吊车、人力推车、三轮车等 | 道路/大型桥梁/通行区，道路/过街天桥/通行区，道路/跨河桥/通行区，道路/立交桥/通行区，道路/隧道/通行区，建筑住宅/建筑工地/重点施工区域 |
| 57 | 漂浮物检测 | 提供漂浮物检测的能力，可以使用在河道、湖区水面清洁检测场景，对水面的漂浮物进行检测和识别，包括塑料漂浮物、其他漂浮物、植物漂浮物、水葫芦等 | 水环境/地表水水质监测站/地表水环境水体，水环境/地表水水质监测站/饮用水取水口 |
| 58 | 可见光船只检测 | 通过视频图像分析技术，对指定画面中的船只进行识别，包括渔船、货船、客船、工程船、执法船、白艇、竹筏、沙船、散装船、灌装船、高速客船、散货船、采砂船、挖泥船等，适用于河道、湖泊等场景 | 河道/水道/水道区域，国土/水域及水利设施用地/湖泊水面 |
| 59 | 未戴安全帽检测 | 通过图像分析技术，检测出监控区域内没有戴安全帽的对象 | 建筑住宅/建筑工地/重点施工区域 |
| 60 | 非法采砂检测 | 检测图像中是否存在渣土车、砂石堆、挖掘机、推土机、货车等目标，适用于水道区域、河流采砂区域和非法采砂高发区 | 水利/其他场所/非法采砂高发区，水利/河流/采砂区域 |
| 61 | 烟雾检测 | 通过视频图像分析技术，识别施工区域周边是否存在尘土飞扬的情况，包括白色烟雾、黑色烟雾、扬尘 | 道路/市内道路/道路周边，居住建筑/住宅建筑/周边区域 |
| 62 | 垃圾堆检测 | 通过图像分析技术，检测并识别道路旁的建筑垃圾、生活垃圾等垃圾堆。适用于河道周边的垃圾堆 | 道路/市内道路/道路周边、居住建筑/住宅建筑/周边区域、居住建筑/住宅建筑/周边路段、居住建筑/住宅建筑/垃圾分类点 |

## 实施服务

### 算法开发服务

提供算法定制发开发服务，按照项目中场景化需求，根据提供的素材，进行新算法的开发， 包括数据清晰、标注、训练等，实现一个可运行的算法，并不断优化。

### 算法优化服务

针对项目现场实际场景与算法适用场景不匹配的情况，提供算法新场景适配服务。

## 性能设计

（1）算法管理数

平台最大可支持管理1024个算法包。

（2）算法并发调度数

平台最大可支持64个算法并发调度使用。

（3）素材库性能规格

图片数据上限1000万张、标注数据上限5000万个、单数据集版本数据上限100万条、单次上传图片上限1000张、素材下载zip包大小上限5G、zip包上传文件大小上限1G。

## 资源规划

（1）算法仓库服务器

需要配置1台算法仓库服务器（CPU：16核2.2GHz及以上；内存：32GB；硬盘：300GB SAS，1200GB SSD；网络：1GbE，可以采用同规格虚拟机）用于部署算法仓库管理服务。

（2）智能分析服务器

需配置智能分析服务器算法引擎组件开展视频智能分析工作，智能分析服务器配置如下：

CPU：2颗处理器，核数16核，主频2.2GHz

内存：16GB DDR4 \* 4，32个内存插槽

硬盘：480G SSD硬盘

GPU：8张高性能GPU卡

网口：2个千兆电口，2个万兆光口

智能分析服务器的数量计算过程如表2所示。

*//智能资源的计算需基于项目实际所需算法类型和要分析视频路数进行调整，这里只是给出计算过程示例参考。*

1. 智能资源计算参考表

| 序号 | 智能算法 | 算法类型 | 分析时段及频率 | 点位数量 | 总数 | GPU卡性能 | GPU卡数量 | 汇总 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 占道经营 | 图片分析 | 6:00-24:00每5分钟 | 200 | 图片分析总路数3200张，平均每秒10.67张图片。  理想情况下，16种算法作为独立算法包预加载到GPU卡中。  实际情况中，1-10算法可打成一个算法组合包。 | 考虑算法每种算法复杂度不一样，平均按每张卡每秒处理2张图片进行设计。 | 理想情况下，算法独立打包预加载到16张卡，每张卡平均每秒解析0.67张，取最大值是16张。  实际情况中，1-10算法组合包预加载，每秒解析6.67张，需要4张卡，共需要10张卡。 | 总共需要26张加速卡，考虑部分临时智能任务和卡硬件的冗余，所以考虑配置30张加速卡，保障系统的高性能、高可用。 |
| 2 | 店外经营 | 图片分析 | 200 |
| 3 | 路面塌陷 | 图片分析 | 200 |
| 4 | 乱堆物堆料 | 图片分析 | 200 |
| 5 | 打包垃圾 | 图片分析 | 200 |
| 6 | 垃圾满溢 | 图片分析 | 200 |
| 7 | 户外广告 | 图片分析 | 200 |
| 8 | 经营撑伞 | 图片分析 | 200 |
| 9 | 沿街晾挂 | 图片分析 | 200 |
| 10 | 暴露垃圾 | 图片分析 | 200 |
| 11 | 违建分析 | 图片分析 | 6:00-18:00每5分钟 | 200 |
| 12 | 违章建筑检测 | 图片分析 | 6:00-18:00每5分钟 | 200 |
| 13 | 安全帽检测 | 图片分析 | 8:00-18:00每5分钟 | 200 |
| 14 | 工作服穿着检测 | 图片分析 | 8:00-18:00每5分钟 | 200 |
| 15 | 后厨人员穿戴检测 | 图片分析 | 6:00-24:00每5分钟 | 200 |
| 16 | 水库、河道偷钓检测 | 图片分析 | 0:00-24:00每5分钟 | 200 |
| 17 | 消防通道占用检测 | 视频分析 | 0:00-24:00 | 25 | 100 | 平均并发处理10路 | 共需要10张卡 |
| 18 | 楼梯拥堵检测 | 视频分析 | 8:00-18:00 | 25 |
| 19 | 漂浮物识别 | 视频分析 | 8:00-18:00 | 25 |
| 20 | 区域入侵检测 | 视频分析 | 0:00-24:00 | 25 |

汇总整个计算结果，可以得出在最大情况下需要2张GPU卡才能满足计算分析需求，本次项目采用配置有8张GPU卡的智能分析服务器，所以总计需要2台智能分析服务器。

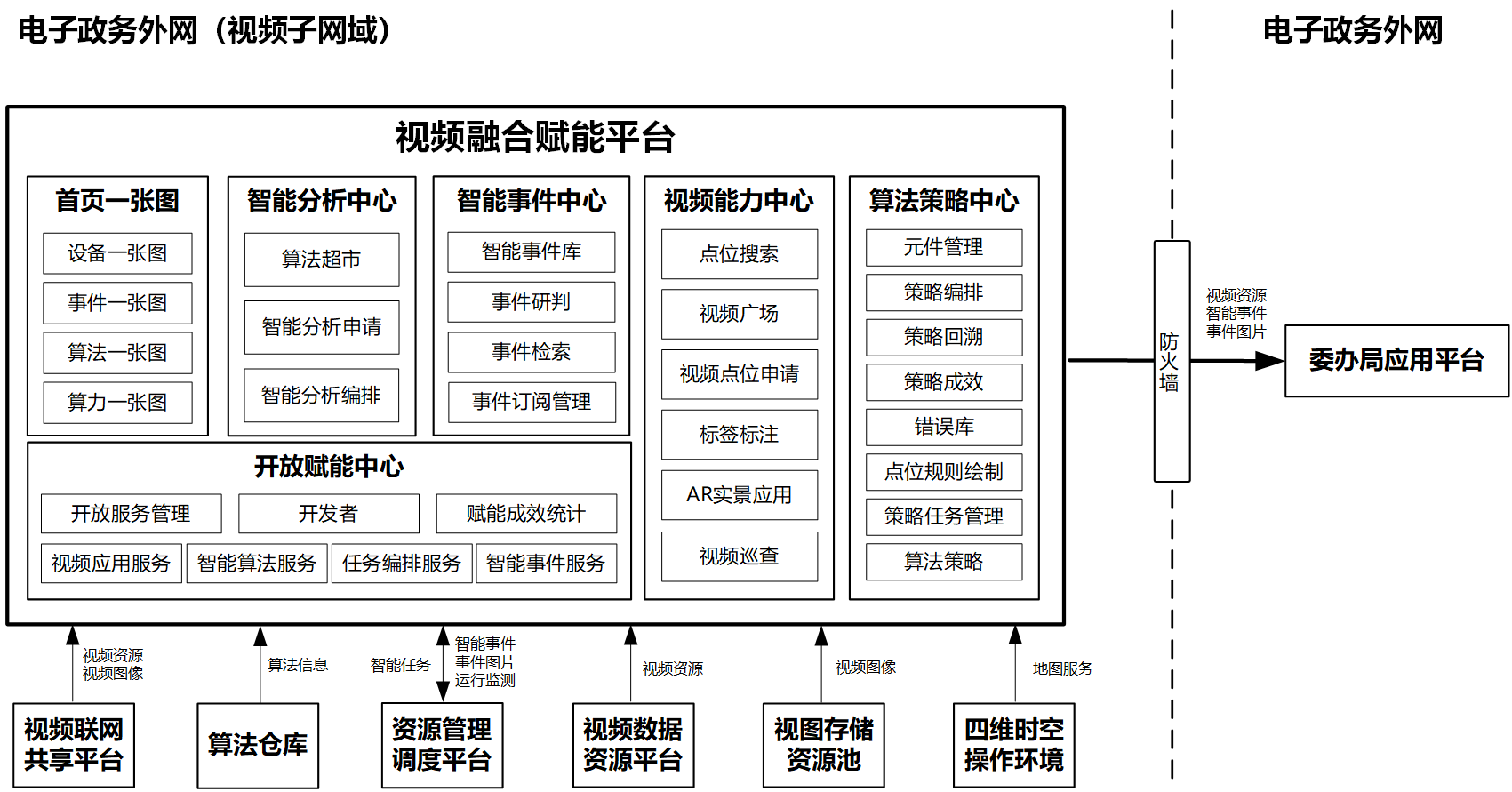
# 视频融合赋能平台设计

## 概述

视频融合赋能平台是视频云中台实现视频资源、智能算法高效融合并对外进行开放赋能的核心平台。平台对接上层业务开展过程中需要的视频、智能需求，提供资源展示检索、智能融合编排、事件研判分析、多维开放赋能等能力，对上层业务应用实现视频赋能、AI赋能。视频融合赋能平台主要功能包括首页一张图、视频能力中心、智能分析中心、智能事件中心、开放赋能中心、算法策略中心等。

## 架构设计

视频融合赋能平台基于视频联网共享平台接入视频资源和视频图像，通过视频资源治理平台获取治理后的视频资源点位信息，从视图存储资源池获取视频点位录像，从算法仓库同步智能算法数据开展算法编排，将编排好的视频智能分析任务下派到资源管理调度平台，接收来自资源管理调度平台的智能事件、事件图片及运行监测等数据，为各委办局应用平台提供视频点位、智能事件、应用开发等资源及服务支撑。详细架构如图8所示。



1. 视频融合赋能平台架构图

## 功能设计

### 首页一张图

提供首页一张图的能力，分别集中展示设备、事件、算法、算力等内容的具体情况，方便用户快速掌握平台各方面资源的整体态势。

#### 设备一张图

设备一张图模块展示设备相关的统计数据，包括设备接入类型总数，按照设备二级分类统计设备类型总数；统计所有设备总数和各个类型设备的在线、离线数据；统计设备的治理情况，按照设备治理指标统计已治理数、未治理数；统计委办单位接入的设备、申请的设备排行榜；地图上显示所有点位信息，可以根据委办单位、设备类型、设备状态和行政区划在地图上标注点位信息。

#### 事件一张图

事件一张图模块展示事件相关模块的统计数据包括事件类型总数和各个类型事件与总数的占比；事件研判排行榜，按事件统计事件研判、未研判统计数据；统计今日新增加的事件总数；当前1分钟上报的事件列表；以及委办单位接入设备总数，并按委办单位维度进行统计排名；委办单位申请的设备总数和排名；使用行政区划、事件类型和时间查询事件列表，并和地图联动显示对应的设备点位。

#### 算法一张图

算法一张图模块用于展示算法相关的统计数据，包括统计算法类型总数并按类型总数排名，统计算法总数，统计算法接入情况和算法任务情况；统计所有算法的策略准确率、算法准确率进行分析，统计高频使用算法排行；统计委办单位信息，委办单位算法运行状况以及委办单位算法排行，根据委办单位统计算法任务分布及任务占比。

#### 算力一张图

算力一张图模块用于展示算力相关的统计数据，包含中心端、边缘端GPU使用情况、GPU可用情况、GPU分布情况、设备信息等功能；也包含服务器使用情况（CPU使用率、内存使用情况、磁盘使用情况）、文件存储、普通云存储使用情况、资源预警占比等功能模块。

### 视频能力中心

视频能力中心提供视频资源的开放共享和管理，用户可以通过点位搜索、视频广场等功能获取自身需要的视频资源，也可以对自己部门的视频资源或者申请到视频资源进行内容标注，方便高效支撑上层视频应用，用户也可以基于有权限的视频点位开展视频巡查和AR全景应用。

#### 点位搜索

通过点位搜索，实现视频资源在多种筛选条件下的快速搜索，并通过地图模式和列表模式结合展示搜索结果。搜索方式包括：支持标签搜索，按照资源目录、智能标签、管理单位、点位类型、标签进行多维度复合检索；支持关键字搜索，通过别名、场所、地址等对象的关键字来进行快速检索；支持空间搜索，在地图上框选、圆选、多边形选、线选等绘制区域，查询地图上绘制范围内点位；支持将搜索关键字和标签组合条件保存为常用搜索，支持用户查看常用搜索和历史搜索记录，通过常用搜索和历史搜索直接查看搜索结果。

#### 视频广场

视频广场展现视频资源的点位情况、基本能力及场所位置等内容，视频广场帮助各委办局用户了解全域的视频资源基本情况及分布情况，视频资源通过业务标签、场所分类、资源目录等方式进行资源查询筛选，可以快速过滤、定位自身业务需求相关的视频点位资源。

#### 标签标注

标签标注模块负责视频点位标签标注管理，标签包含自定义标签、智能标签。结合AI算法对视频点位的抓拍图片或者视频流进行算法分析，然后识别出智能标签并与该点位进行关联，同时支持人工标注视频点位与自定义标签的关联关系，以支撑用户快速检索、过滤视频点位资源。

##### 自定义标签管理

支持自定义标签管理，支持自定义标签的导入和导出，支持移动标签改变标签父子关系；支持用户创建多个标签树，标签树支持4级；标签支持两种展示模式，卡片模式展示标签的使用状态、发布状态、下级标签的数量，列表模式展示标签的使用状态、发布状态、下级标签的数量最近编辑时间、创建时间。

委办局用户可以将自定义标签发布，发布标签需要经过数据主管部门审批。发布是以标签树的维度发布，发布后所有人都可见可用，标签的修改删除权限也归数据主管部门所有。

##### 智能标签管理

智能标签包括AI标签和场所标签。

（1）场所标签

场所标签主要是场所的分类如商场、医院、银行等通用描述标签。场所标签可以配合场所地名来一起使用，实现通过场所快速检索设备。

（2）AI标签

AI标签是AI 场景算法对视频图片识别出来的标签。AI标签是为了解决用户手动打标签的大量枯燥重复的工作，通过AI算法智能的识别出所有点位匹配的标签，帮助用户快速的过滤了大多数的点位，大大提升了工作效率。

##### 智能标注

智能标注包括自动标注和手动标注两部分。

（1）手动标注

手动标注是人工去给点位关联相应的标签，在已知这个点位所属场所、所属业务等前提下人工去打标签。

（2）自动标注

AI 标签标注是通过AI场景算法分析点位抓拍图片的内容，识别出图片上的画面是否与算法匹配，如果匹配则会给点位打上相应的标签， 例如，选择一批点位与森林标签检测算法建立AI标签标注任务，后台任务会使用森林检测算法分析这些点位的拍摄图片内容，并根据识别结果判断是否给点位打上森林标签。

### 智能分析中心

智能分析中心提供视频和智能融合的相关能力，包括视频智能能力的展示、智能分析任务的创建和具体算法任务编排。

#### 算法超市

算法超市为委办局用户提供平台智能算法的展示和查看能力，了解平台的算法能力内容，并能结合自身业务需求，选择视频智能算法支撑业务开展，提供已发布算法的算法展示查询、算法详情查看等功能。

（1）算法展示查询

算法超市集成了已开放的算法资源，支持按行业、分析目标、分析源类型等算法分类进行算法筛选，支持按算法浏览量、热门度、上传时间、上架时间进行算法排序，支持在算法卡片中查看算法名称、示例图片、算法描述等简要信息，支持算法查询检索。

（2）算法详情

支持结合业务需要选择相应的算法进行详情查看，查看算法的应用条件、场景说明、技术指标可用范围；支持算法功能演示，支持使用算法包内自带的算法示例图对算法进行快速演示，查看算法运行结果，并将分析结果与算法示例图的预期结果进行对比；支持算法版本管理，记录同一算法不同版本的信息，支持切换算法版本，查看同一算法不同版本号的算法详情介绍。

（3）算法关注

可以提供算法能力关注功能，用户可以对自己感兴趣的算法能力进行收藏和管理。支持将算法加入到我的关注中进行收藏，支持用户查看已关注的算法。

#### 智能分析申请

面向各委办局用户提供AI算法的申请共享能力，支持选择单个算法或多个算法进行申请；支持算法申请结果推送配置，包括消息、邮件、短信三种模式；支持算法分析计划的配置，包括全天计划，工作日计划，分时段计划；支持分析点位的预览，帮助申请者、审批者对申请点位的确认；支持申请点位的联动配置，包括抓图联动，录像联动，云台联动、视频上墙，报警联动；支持申请审批管理，支持多级审批，支持按照申请单查看审批进度及审批意见。

#### 智能分析编排

基于各委办局用户的智能分析需求，平台提供智能分析编排，由运营人员开展场景治理、算法编排工作，合理的利用点位和算法资源进行编排配置，高效利用有限的智能分析资源。

##### 点位场景治理

对于各类视频点位资源和智能分析算法，需要基于场景进行算法、规则等配置，包括但不限于在视频画面中绘制分析区域、配置分析规则、关联事件发生地址、配置后场景核验等，场景配置是视频、算法融合实现“一视频多算法”的基础，也是平台高效、准确开展智能分析的前提。该模块提供对点位进行预先治理的功能，也可对分析申请中的待治理的点位生成场景治理清单，清单可以指派给他人进行治理。按照清单生成的方式，分为自建/系统分配两种类型。在场景治理中可以对点位进行算法参数设置如：分析区域，屏蔽区域，置信度，灵敏度等，根据不同的算法设置对应的规则参数。

##### 实时视图分析

用户可以结合自身业务需求，基于平台现有的算法和视频资源，提交实时视图分析申请，申请开展相关智能分析工作。平台提供实时视图分析列表，用户可以查看相关的实时视图分析任务，查看当前状态包括待提交、审批中、编排中、分析中、分析到期五种状态。用户可以新建实时视图分析申请，为后续的智能分析工作开展提供输入。

##### 历史视图分析

历史视图分析满足用户对视频录像、本地图片、本地视频文件进行智能解析，通过算法识别关键信息的需求。平台提供历史视图分析列表，用户可以查看相关的历史视图分析任务，查看当前状态包括待提交、审批中、编排中、分析中、分析暂停、已完成六种状态。用户可以新建历史视图分析申请，为后续的智能分析工作开展提供输入。

### 智能事件中心

平台产生的各类智能事件汇聚到研判智能事件中心模块进行集中处理，提供事件真伪研判、推送分发、查询统计、事件库管理等能力，是对外赋能的关键环节。

#### 智能事件库

智能事件库将各类事件按照基础信息和事件协议模板两大要素进行建模，其中事件基础信息包括事件名称、事件描述、事件来源单位、事件关联场景、事件关联标签等；事件协议定义事件报文格式与映射字段，其中事件编号、事件类型、上报时间、点位编号为必须映射的字段，且映射字段与事件协议一一对应。通过事件，模型对事件信息进行封装和定义，实现事件信息标准化管理。事件模型创建成功后，启动事件上报任务，实时接收事件信息。

#### 事件研判

提供智能事件预警研判处理的工作台，按照事件类别对事件进行逐项研判，研判过程中可查看事件基本信息、分析规则、联动信息，其中分析规则与联动信息在实时视图分析的任务编排中配置，一并在此处展示方便用户进行比对。因分析规则导致事件识别效果不佳，例如检测区域绘制存在超出或遗漏导致事件误报或漏报，用户可一键跳转至实时视图分析编排页面修改分析规则。

事件研判支持视频实时预览，将视频实时画面与事件图片画面进行比对，确定事件是否已失效；支持事件视频片段回放、图片下载、录像下载，获取事件更详细的视频画面信息；支持跳转至策略信息，查看在策略模块过滤的事件信息。

支持以事件类型为分类，汇总各种类型事件当前需核验的总数，然后从高到低进行排列，选择某事件类型后，可以逐个进行核验。

#### 事件检索

提供智能事件的查询检索能力，为平台的事件检索、事件回溯、配置优化等提供数据支撑。提供统一的智能事件的查看页面，以列表或者缩略图的方式进行展示，支持通过点位、事件地址、时间等维度进行检索快速定位。提供待核验、全部、正报、误报、不核验五种分类方式，并展示相关分类下面当前总体事件数量，可以在相应分类下面进行查看、检索。对待待核验的事件，可以进行核验和误报处置。

事件详情信息支持查看事件基本信息、分析规则、联动信息；支持视频实时预览，将视频实时画面与事件图片画面进行比对，确定事件是否已失效；支持事件视频片段回放、图片下载、录像下载，获取事件更详细的视频画面信息；支持跳转至策略信息，查看在策略模块过滤的事件信息。

支持事件导出，选择一个或多个事件进行事件导出，导出过程中支持配置导出事件的全量基础信息或者部分基础信息。

#### 事件订阅管理

平台需要将解析后的智能事件数据按需推送给各委办局进行处置，平台设置了事件订阅功能，委办局用户可根据需要订阅各类智能事件。

### 开放赋能中心

开放赋能中心对外进行视频和智能的能力共享，提供开放服务管理、开发者、赋能成效统计等模块，并对外提供包括视频应用、智能算法、任务编排、智能事件等相关的服务接口。

#### 开放服务管理

开放服务管理模块提供开发者管理、审批管理、服务管理、应用管理、开放台账等功能，高效支撑服务接口开放的同时，实现开放服务的完整闭环管控。

##### 开发者管理

开发者是具体的资源关联、资源使用的核心对象，通过为开发者配置相应的功能及权限，方便开发者在平台进行登录使用应用功能，或者通过平台API网关进行服务接口访问支撑二次开发。开发者管理模块主要实现对开发者的添加、删除、编辑、启用、禁用等功能，支持对开发者的基本信息进行维护，包括开发者名称、所属单位，手机号码，应用权限和申请时间等。

##### 审批管理

平台将审批管理划分为应用审批、服务审批、接口审批和权限审批，其中应用审批支持数据主管部门和委办局进行应用登记审批，管理应用名称、登记类型、申请时间、申请描述等信息；服务审批支持数据主管部门和委办局进行API服务接口审批审批，管理申请编号、所属应用、申请理由、申请时间、审批状态等信息。

##### 服务管理

此模块面向运营人员，为运营人员提供服务管理，对服务接口进行上线、下线和标注，并支持批量操作。在此模块下，运营人员亦可申请新增服务接口，并实时查看审批记录。对于被驳回的接口发布申请，运营人员在二次编辑后可再次提交申请。

##### 应用管理

应用管理数据主管部门、委办局名下所有开发者所有已申请应用的合集，可使用应用状态、应用名称等字段，增加应用查询的准确度。获取到符合条件的应用列表后，前端使用卡片模式、列表模式展示。

##### 运营台账

通过运营台账可以管理开放赋能中心的基础面板，帮助数据主管部门用户清晰直观掌握开放赋能中心的综合数据，了解现在开放赋能中心的运行情况和委办局调用数据的情况。主要展示API接口总数，应用总数，开发者总数，以及委办局和数据主管部门用户数。服务类型分布情况，接口上下线分布情况，一周内调用API次数趋势图，应用场景调用次数排行榜TOP10。

#### 开发者

平台作为视频能力支撑平台，需要为不同委办局的开发者提供服务，为开发者提供学习、交流、合作和服务的开放平台，开放技术和服务，提供产品孵化、研发支持、统计分析等服务。提供包括我的应用和服务开放两块功能。

##### 我的应用

此模块面向开发者用户，为开发者提供应用开发流程指导、对应的流程操作和操作记录查询。应用开发流程包含应用登记、服务申请、接口调试等。开发者工作台包含我的应用和我的资源两个模块。其中我的应用中提供包括应用登记，应用列表查询，应用编辑等应用相关的功能。我的资源中包含资源申请，资源编辑，查看等资源相关的能力。

##### 服务开放

服务开放模块的核心功能是收录平台所有底层组件接口，屏蔽内部核心接口，分类各个组件接口功能。用户通过场景功能搜索合适的接口，展示API接口详情及使用方式，支撑用户高效、合理进行二次应用开发。

#### 赋能成效统计

通过赋能成效统计模块，帮助用户从多个维度将平台对外开放赋能的情况进行统计展示，包括成效报表和成效一张图两种方式。

##### 成效报表

（1）汇聚成效

支持查看点位接入汇聚、接入监控点种类总数、监控点类型、管理单位点位接入情况、近七天点播趋势、计算资源资源情况、计算资源节点数量、GPU资源使用趋势、算法资源情况。

（2）融合成效

支持展示场景治理情况、事件累计上报数量、点位共享情况、任务数据情况、场景策略成效、调度策略成效、一周任务排队情况。

融合中的策略成效为策略具体成效泛化抽象后，合并为统一一个维度来表示，旨在降低用户学习成本，体现平台价值。具体策略成效需至对应组件查看。

（3）赋能成效

通过服务开放情况、事件推送情况、工单申请情况三大模块对平台对外赋能、开放价值进行展示，支持展示事件推送情况、服务接口开放情况、服务对象开放情况、服务开放情况、开发者开放情况、工单申请情况。

##### 成效一张图

赋能成效包括三张图：分别为设备汇聚、事件产生、赋能流程。

设备汇聚：根据设备级联链路追溯父子级联节点，展示各级级联平台详情，设备端到本级联入端，下级平台和本级指向本级平台，本级平台到上级应用平台，显示实际取流路数。展示设备汇聚一张图，展示各级设备的汇聚和数据流向。

事件产生：展示平台数和实际的取流路数，普通设备、智能设备指向事件库，下级设备指向事件级联服务，事件级联服务再指向事件库，事件库统一指向事件中心，事件中心到本级策略模块再到上层应用平台，展示各级设备产生事件并汇聚、存储、共享的流程。

赋能流程：展示平台服务接口数和实际的接口调用数，服务对象分为设备资源服务，工单服务，算法服务，标签服务等。

#### 视频应用服务

提供视频抓图、视频标签、实景场景等视频应用服务，支撑上层业务高效开发视频基础应用。

##### 视频抓图服务

提供同步、异步两种抓图方式，按照抓图手段又分为PTZ抓图、预置点抓图、区域缩放抓图，在抓图前需要调接口配置抓图结果存储地址。视频抓图服务可以有效支撑各委办局周期自动巡查抓图、比对分析相关的视频应用。

##### 视频标签服务

提供视频标签查询、获取服务，针对有权限的视频点位资源，可以查询指定点位对象的视频标签数据，包括统一治理形成的公共标签和用户给视频点位标注的自定义标签。

##### 实景地图服务

实景地图服务提供AR高点场景资源获取，AR高点全景场景详情信息获取、AR高点全景场景切换、标签模板查询、标签管理（添加、删除、修改）、标签更新、标签模板权限查询、高点场景变更、高点场景切换等能力接口。同时提供了AR业务标签插件、业务可视化面板插件、报警信息联动插件、AR软件界面 WEB/CS集成的开放能力。

#### 智能算法服务

提供算法仓库中发布的算法能力集、算法信息详情等内容获取服务。该部分数据是一般用户后续其他服务分类API的输入参数条件。

##### 算法类别获取

提供算法类别查询获取服务，可以获取算法仓库中建立的算法类别分类信息。

##### 算法能力获取

提供按全量、分类、算法编号等方式或者算法仓库中算法能力的信息。

#### 任务编排服务

提供视频智能分析任务的接入功能，外部应用可以通过任务编排服务提交视频分析任务、图片分析任务、场景编排任务。

##### 视频分析任务

外部应用可以创建实时视频分析、录像视频分析、离线视频文件分析等任务，可以通过视频任务通用接口对视频任务进行启停、删除操作，可以对智能任务的执行状态查询。

##### 图片分析任务

外部应用可以创建图片分析任务，图片来源包括离线图片批次上传或者指定图片数据来源位置两种方式， 可以通过图片任务通用接口对图片分析任务进行启停、删除操作，可以对图片任务的执行状态进行查询。

##### 场景编排任务

外部应用可以创建针对具体视频点位场景的智能分析任务，任务主要由监控点信息、算法信息、分析目标信息构成，拼接这些信息后可以调用新增统一编排任务进行任务下发，可以通过删除统一编排任务对任务进行删除操作，也可以对分页查询编排任务进行运行状态查询。

#### 智能事件服务

提供视频智能事件的订阅、推送、查询检索等服务。

##### 智能事件订阅

提供按事件类型进行订阅、取消订阅智能事件的服务。

##### 智能事件推送

支持根据订阅的情况向外部应用推送智能事件，提供实时智能事件的完整内容信息。

##### 智能事件检索

提供多条件查询智能事件，可以根据能力名、事件发生地址、事件发生时间、事件核验状态、是否去重等来查询事件，并提供获取事件详情的能力。

##### 事件编码获取

提供事件类型编码获取服务，包括父事件码获取、子事件码获取，一个父事件码下面有多个子事件码。

### 算法策略中心

算法策略中心为平提供高效的智能事件规则（误报、重复、多算法叠加等）处理能力。视频智能事件从产生到业务应用的过程中，需要经过一定规则处理后才能形成可使用的事件，为提高事件得有效性和准确性，需要对原始事件进行去重、去误报、业务规则转化等操作。基于各行业算法优化沉淀的经验，算法策略中心提供策略编排、策略管理、策略成效分析等能力，接收视频智能分析事件，通过叠加算法应用策略计算后，输出有效事件到上层平台，实现多样化智能增效策略，帮助解决单一算法与业务场景的偏离的难题。算法策略中心主要功能包括元件管理、策略编排、策略回溯、策略成效、错误库、点位规则绘制、策略任务管理、算法策略等。

#### 元件管理

提供各类元件的管理，包括元件的导入导出，元件类型包括事件、策略算法、策略函数等元件。元件是组成策略的基本单元，主要包含了事件元件、函数元件、策略算法元件等。元件管理中主要是定义了各类事件元件、封装和定义了函数元件和策略算法元件以及各类元件的管理。

##### 元件导入

支持针对事件元件、策略算法元件、函数元件进行导入，元件包要求为小于1G的zip文件，导入后支持对包进行解析，识别出元件名称、版本、描述等，支持用户选择需要真正导入的元件。

##### 元件导出

支持单个以及批量按照zip的方式导出事件元件、策略算法元件、函数元件元件。

##### 事件元件

（1）事件元件总述

事件元件定义了来源的事件和输出的事件，输入事件主要定义了事件的名称、消息队列以及相关的需要加入编排的字段；输出事件主要定义了事件码以及消息队列。

（2）事件元件列表

以列表的形式展示元件信息，主要包含了元件名称、元件版本、事件标识、事件源类型、解析类型、消息队列类型、消息队列IP、端口、消息队列、创建人等。

（3）事件元件详情

展示事件元件的详细信息，主要包含了元件信息、消息队列、引用关系。

（4）事件元件新增

描述了新增事件元件的过程，主要包含了事件报文、元件信息、消息队列等信息。

（5）事件元件删除

支持单个或多个事件元件的删除。

（6）元件检索

支持按照元件名称、事件标识、消息队列类型、事件源类型来检索事件元件。

（7）修改消息队列

支持对单个或者多个元件进行批量的消息队列的修改，可节省修改的时间。

##### 策略算法元件

（1）策略算法元件总述

函数元件包含了各类cpu算法元件，主要包含了烟雾检测算法元件、车辆检测算法元件等。

（2）策略算法元件列表

支持以列表形式展示策略算法元件，主要包含了元件名称、元件版本、元件标识、描述等信息。 操作包含编辑、详情和导出、删除等操作。

（3）策略算法元件新增

描述了新增策略算法元件的过程，主要包含了元件信息、算法信息等内容。

（4）策略算法元件删除

支持单个或多个策略算法元件的删除。

（5）策略算法元件检索

支持以元件名称、元件版本、元件标识来检索策略算法元件。

##### 策略函数元件

（1）函数元件总述

函数元件包含了各类逻辑规则的元件，主要包含了过滤、去重、聚合、运算等类型的元件。

（2）函数元件列表

以列表展示函数元件的信息，主要包含了元件名称、元件版本、函数类型、元件标识、描述等信息。操作包含了编辑、详情和导出、删除等操作。

（3）函数元件新增

描述了新增函数元件的过程，主要包含了元件信息、函数信息等内容，输出包含了字段标识、字段类型、字段名称信息，支持对输入和输出信息编辑相关的字段名称。

（4）函数元件删除

支持单个或多个函数元件的删除。

（5）函数元件检索

支持元件名称、函数类型、元件版本、元件标识来进行检索。

#### 策略编排

策略编排采用可视化画布、低代码的方式对实时事件进行策略的编排，管理及运行。策略编排中涉及到对多个策略分组进行统一的管理，策略参数灵活设置适用各类场景。

##### 策略分组

（1）分组总述

策略分组用以对策略进行分类管理，方便用户可以根据业务场景来管理对应的策略。

（2）分组新增

支持填写分组名称、描述。

（3）分组编辑

支持对分组和描述信息进行修改。

（4）分组检索

支持以分组名称来检索分组。

（5）分组删除

要求分组内的策略均删除后，分组才能够进行删除。

##### 策略编排

（1）新建策略

系统分组中支持新增策略，并可进行策略基本信息（策略名称、描述和策略封面）的编辑操作；策略的画布中包含了元件列表、画布区域、元件参数信息展示三大区域；其中最左侧是元件列表展示，支持按照元件名称进行元件检索，方便用户快速找到编排所需的元件；中间区域是画布区域，支持拖拉拽元件形成策略，支持撤销、重做、放大缩小等操作；右侧区域是元件参数信息展示区域，能够对元件的参数进行修改。查看策略名称后，右侧区域也可展示策略信息，支持策略封面自定义，若不上传封面，默认用策略的拓扑图；策略编写过程中支持快捷修改事件元件的事件参数。

（2）策略删除

支持单个或多个策略的删除。

（3）策略详情

通过拓扑图或者封面图可查看策略的详情，包含了策略描述、策略编号、状态、拓扑图等信息。

（4）策略编辑

针对未运行的策略可进行编辑操作，任何策略信息均可以编辑。

（5）策略校验

支持检测策略的完整性。

（6）策略运行

支持对策略执行运行动作（针对未运行的策略）。

（7）策略导入

支持策略进行导入。

（8）策略复制

支持策略的复制。

（9）策略导出

支持单个或者多个策略按照zip方式进行导出。

（10）策略运行配置

支持配置策略运行的时间计划和涉及到的相关的监控点，默认为所有监控点和所有时间；自定义情况下，用户可选择对应的时间计划，对于系统默认的时间计划（全天、工作日模板）等不满足的情况下，用户可自行设置时间计划，可定位到分钟，监控点支持用户进行单选或者多选。

（11）策略移动

支持将策略在系统界面中的显示位置变更至指定的策略分组中。

（12）点位策略详情

支持按照点位维度展示点位所配置的各个策略的情况，并且支持根据监控点名称、策略分组、执行计划、策略状态、关联事件等进行条件检索。

（13）回溯

通过回溯可快速查看策略对应的事件检索页面。

（14）预置成熟策略

产品预置的成熟策略只允许编辑、配置、运行、快速查看策略对应的回溯页面，其中编辑只允许修改部分的参数。

（15）策略调试

策略校验通过后，支持通过报文模拟和离线图片分析的方式进行策略调试。

报文模拟：后台自动填充报文，加入编排的字段支持用户手动修改，包括手动选点，手动上传图片等，针对数组对象支持手动添加多个；

离线图片分析：支持选择算法，上传图片，对对应的图片进行分析。

（16）策略调优

历史数据用新的策略执行一次，可比较前后的策略差异，主要包含了输出事件总数和拦截事件总数的变化，针对变化的事件结果，会对事件打上“有变化”的标签，针对无差异的事件，会打上“无变化”标签，支持用户按照监控点名称、有无变化进行筛选策略调优结果。支持针对研判数据进行调优，可以直观的输出对应的检出率和检准率以及算法的检准率和检出率，其中页面上呈现的算法检出率均为100%。可查看策略处理的正报或者误报（正报是指策略正确拦截或者正确输出的事件）。

#### 策略回溯

策略回溯主要展示各个经过策略处理后的事件，能够详细展示事件经过如何经过策略，最终是被拦截还是会输出，拦截是被哪个元件拦截，拦截原因是什么均能进行展示。

##### 事件检索

支持按照事件类型、上报时间、事件点位、策略识别结果、研判结果、拦截元件等进行检索；并以卡片或者列表形式展示检索结果。支持对检索结果中的图片进行放大查看操作。

##### 事件列表

支持按照列表或者图片的形式展示事件结果。

##### 事件详情

支持展示详情中的事件图片、事件关联的图片（聚合事件的图片、监控点元件抓图的图片）、策略信息、策略拓扑图、策略识别结果，事件信息（事件类型、事件编号、研判状态、拦截原因、策略执行起止时间、耗时等），策略拓扑图中针对拦截的事件，标红拦截的元件，方便用户快速找到对应的元件；支持对事件进行上一条、下一条的切换展示操作；支持根据事件抓拍信息（点位信息、抓拍时间）进行录像回放操作；支持将点位事件信息添加到对应的事件类型的错误库集中。当错误库图片锁定超过数量后，提醒用户“图片锁定已超过错误库中图片最大数量，请先删除锁定的图片，“跳转错误库”，可以直接跳转到点位对应预置点的错误库页面中；针对策略详情交互进行优化，针对二次分析的元件可在图片上直接展示对应的标签，展示策略的起止时间和耗时；支持展示事件报文、关联事件和策略执行报文。

##### 策略研判

支持对事件进行研判，策略输出事件支持研判为正报或误报，策略拦截事件支持研判为漏报事件或者正报事件，当存在多个输出时，针对漏报事件可选择对应的输出事件，针对上层应用中巡视的的研判结果进行回归，巡视的研判结果主要为正报或者误报。

#### 策略成效

支持通过统计原事件数量和策略拦截事件及结果事件的数量，统计出策略在事件流转过程中所起的作用。通过对系统内策略编排数量统计、原事件统计、有效事件统计输出策略成效进行可视化展示，支持以下成效内容展示。

（1）支持展示策略统计信息，内容包括策略总数、策略分组数、策略状态统计信息；

（2）支持展示事件统计信息，内容包括事件数量，策略输出事件和策略拦截事件的数量和占比；

（3）支持按照今日、近一周、近一个月和自定义时间区间的方式、查询并展示策略输出事件占比和策略输出事件总数排名；

（4）支持以智能事件和智能策略的方式展示智能事件成效统计信息。内容包括事件类型、原始事件、输出事件（占比）、拦截事件（占比）、事件研判数（占比）以及各个占比（查看事件趋势）。

#### 错误库

错误库中按照事件类型、点位的角度展示所有已加入到错误库中的事件图片，一般与错误库分析元件搭配使用。若策略中包含了错误库分析元件，则相同点位相同事件上来后会先与错误库中的图片进行比对，若相似度高于某一阈值，则认为当前事件为错误事件，自动进行拦截；支持展示事件下每个点位的错误库；支持按照事件类型、点位删除错误库图片；支持按照配置文件来设置每个点位的预置点中错误库数量，需注意：该数量不建议调整到很大，会对数据的处理速度有影响，比对的数量过多，时效性会降低。

#### 点位规则绘制

点位规则绘制一般搭配规则查询元件一起使用，主要是为实现点位的精细化策略，可针对不同的规则区域设置不一样的策略；支持按照所属区域、监控点名称、监控点编号、IP、配置状态进行配置的点位查询；支持添加、编辑点位规则绘制，内容包括了选择点位对应预置点或者实时画面，进行点位的规则线和规则框的绘制；支持删除配置了规则的点位。

#### 策略任务管理

提供策略任务管理模块，可以对平台内部的策略任务进行启停、分组等操作，并可以对异常任务进行守护，有效保障策略任务正常运行。

##### 列表展示

支持以列表的形式展示各类策略执行的任务，主要包括了任务编号、任务名称、运行模式、任务分组、运行状态等。

##### 任务检索

支持按照任务名称、任务分组、任务运行状态、任务类型等进行查询，方便快速定位到对应的任务。

##### 任务配置

支持对单个或者多个任务进行参数配置，主要包含了JVM、flink配置、java环境变量等。

##### 加入分组

支持单个或者多个任务加入到分组中。

##### 移除分组

支持从分组中删除单个或者多个任务。

##### 任务守护

支持实时监控任务运行状态，提供任务异常自动拉起功能。

##### 日志下载

支持针对每个任务下载对应的日志任务，方便排查对应的问题。

#### 算法策略

*//这里给出部分已经累积可用的算法策略包，可以结合项目需求灵活选用。*

（1）乱堆物堆料去误报策略

利用策略去除临时卸货、重复预警、小目标以及点位的误报数据。

（2）沿街晾挂去误报策略

利用策略去除临时晾晒、小目标以及重复的晾挂数据。

（3）暴露垃圾去重策略

利用策略去除重复预警和小目标预警。

（4）钓鱼策略包

利用策略去除钓鱼算法中无效报警。

（5）烟雾图片检测策略包

对烟雾图片算法和火点检测算法进行算法二次复核。

（6）路面塌陷去重策略

利用策略去除重复预警和小目标预警。

（7）道路积水达到阈值上报策略

利用策略去除道路积水面积未达阈值的数据，去掉重复数据。

（8）树木倒伏去重策略

利用策略去除重复预警和小目标预警。

（9）占道经营去重策略

利用策略去除临时卸货、重复预警和小目标预警数据。

（10）店外经营去误报策略

利用策略去除临时经过的以及去除重复的店外经营数据。

（11）漂浮物策略包

针对漂浮物频发的区域，利用漂浮物检测算法对漂浮物进行检测，去除小目标、重复预警以及业务中不关心的预警。

## 实施服务

### 基础运营运维服务

提供平台安装部署，资源接入配置，并根据平台联网协议，提供平台对接服务和系统日常运维服务，根据国标、SDK等协议，提供视频资源的接入服务。

### 场景治理服务

提供场景治理服务能力，针对视频画面，按照业务需求和智能分析算法，进行分析场景治理，治理后的场景与智能分析算法自动关联，并在能力超市中进行统一展示，用户查看后，可以选择对应算法进行算法编排申请，实现智能分析事件的轻松创建。

### 策略优化服务

根据业务场景需求，提供策略优化服务，根据业务需求提升事件的准确率。

### 策略开发服务

针对项目中的新的业务场景提供新策略的编写工作，包含其中新元件的开发和策略创建工作。

## 性能设计

（1）智能分析编排任务性能

智能分析编排单任务支持最多30个算法；智能分析编排单任务支持最多1000个预置点。

（2）算法策略性能

算法策略数量最多支持500种，策略事件转发最大支持500条/s。

（3）AR实景应用性能

支持最大场景数10000个，单个场景最大支持标签数500个。

## 资源规划

（1）平台应用服务器

平台基础服务器部署内容包含首页一张图、视频共享中心、智能分析中心、开放赋能中心、运维监控中心、系统管理中心等应用。需要配置1台服务器（CPU：32核2.2GHz及以上；内存：64GB；硬盘：600G SAS；网络：1GbE，可以采用同规格虚拟机）。

（2）平台日志服务器

平台日志服务器部署日志服务，需要配置1台服务器（CPU：8核2.2GHz及以上；内存：16GB；硬盘：300G SAS，1200GB SATA；网络：1GbE，可以采用同规格虚拟机）。

（3）策略应用服务器

需要配置1台策略应用服务器（CPU：32核2.2GHz及以上；内存：64GB；硬盘：300G SAS；网络：1GbE，可以采用同规格虚拟机）用于部署算法策略中心基础应用模块。

（4）策略扩展服务器

策略扩展服务器（CPU：16核2.2GHz及以上；内存：16GB；硬盘：300G SAS；网络：1GbE，可以采用同规格虚拟机）部署运行各类算法策略组件。

*//节点数量根据智能事件数量、算法策略数量、算法元件数量等因素动态变化，建议再明确具体算法策略内容后跟产品经理确认服务器具体数量配置，简单考虑的话可以按每个节点支持15类智能策略的运行来设计。*

（5）AR实景服务器

需要配置1台AR实景服务器（CPU：16核2.2GHz及以上；内存：32GB；硬盘：300GB SAS；网络：1GbE，可以采用同规格虚拟机）用于部署AR实景应用。

# 智能存算资源池设计

智能存算资源池为视频云中台的平台运行、算法解析、视图存储提供基础、稳定、可靠的计算存储环境，包括智能计算资源池和视图存储资源池两部分。

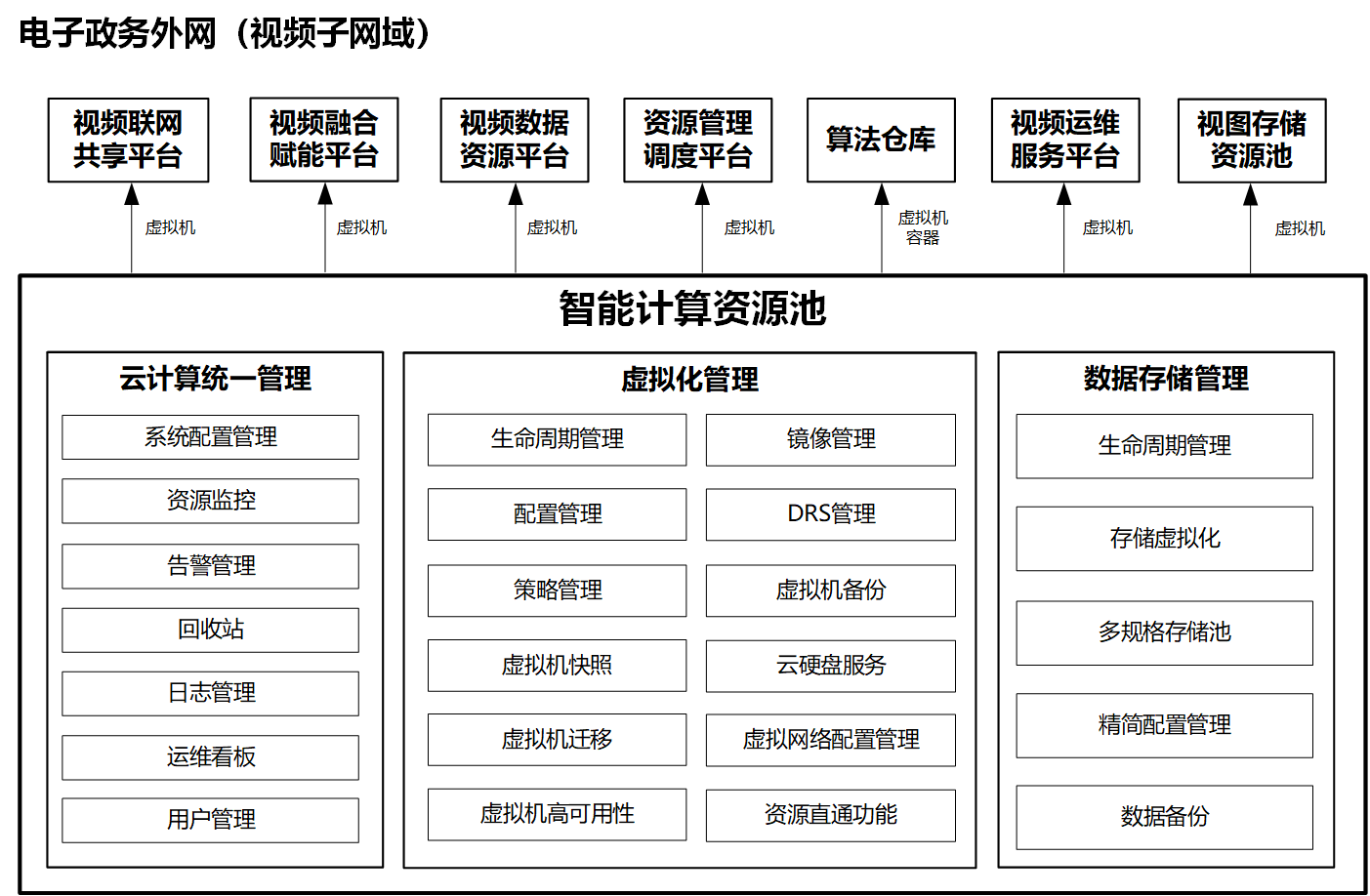
## 智能计算资源池

### 概述

智能计算资源池采用云计算技术构建，通过智能计算资源池，视频云中台可以通过网络方便快捷的获取到所需的IT资源和技术能力，既降低成本，又满足灵活部署、高效率和不断变化的业务需求。智能计算资源池使用虚拟化技术对通用服务器和智能服务器资源进行整合，可以有效提高物理服务器的资源利用率和管理效率，保障视频云中台的持续、可靠、稳定运转。

### 架构设计

智能计算资源池向视频联网共享平台、视频融合赋能平台、视频数据资源平台、资源管理调度平台、算法仓库、视频运维服务平台提供虚拟机环境，平台软件的高效、可靠、稳定的运行。详细架构如图14所示。



1. 智能计算资源池架构图

### 功能设计

智能计算资源池包括云计算统一管理、虚拟化管理、数据存储管理三个模块。

#### 云计算统一管理

云计算统一管理包括系统配置管理、资源监控、告警管理、回收站、日志管理、运维看板、用户管理等功能。

##### 系统配置管理

支持CPU资源的超分比、使用阈值的全局配置；

支持内存资源使用阈值的配置；

支持存储资源的超分比和使用阈值的全局配置；

支持NTP校时配置。

##### 资源监控

支持对物理机、虚拟机、容器、宿主机、数据存储等各种云计算资源的运行状态进行统一监测；

支持一键巡检，可对集群、服务、状态、资源进行检查，输出巡检评分和巡检报告。

##### 告警管理

支持采集系统内所有告警事件，包括未处理和已处理的告警事件；

支持展示告警事件详情；

支持对告警事件进行处理。

##### 回收站

支持将虚拟机、云硬盘等云服务删除后放入回收站进行缓存；

支持对回收站中的云服务进行还原操作。

##### 日志管理

支持对操作日志文件的采集、查询等操作。

##### 运维看板

资源展示：支持集中展示云计算集群中的计算资源、存储资源、网络资源的使用情况；

告警展示：支持按照三种不同色彩的告警级别展示系统的告警数量，以及最新的告警信息。

##### 用户管理

支持用户管理，包括创建、编辑和删除用户；

支持对用户权限进行管理；

支持对用户登录密码进行管理。

#### 虚拟化管理

智能计算资源池可以对各类物理服务器进行虚拟化管理，为上层应用创建各种规格的虚拟机，实现虚拟机的生命周期管理、配置管理、策略管理、快照、迁移、高可用、镜像管理、动态资源调度、备份、云硬盘服务、虚拟网络配置管理、资源直通等功能。

##### 生命周期管理

支持虚拟机的开机、关机、重启、删除、暂停、挂起、在线克隆、重建等功能。

##### 配置管理

支持对虚拟机的配置进行修改，如添加/删除cpu、内存、硬盘、网卡等，主要功能包括：

支持不停机修改虚拟机规格，增加CPU、增加内存和增加系统盘；

支持不停机修改虚拟机网卡配置，修改网络IP、增加网络地址；

支持不停机修改虚拟机名称；

支持停机升级CPU、内存和磁盘。

##### 策略管理

云计算平台在创建虚拟机时，支持通过配置各种策略，满足业务需求。

支持虚拟机亲和性组，将同一组内的虚拟机实例尽量分配到同一物理主机上；

支持虚拟机反亲和性组，将同一组内的虚拟机实例尽量分配到不同的物理主机上；

vCPU绑物理CPU策略： 将虚拟机的vCPU与物理机的物理 CPU进行一对一绑定，减少CPU上下文切换，提高虚拟机的性能；

虚拟机绑定宿主机策略：支持配置虚拟机与宿主机的绑定关系，绑定后的虚拟机只在几个宿主机之间疏散。

##### 虚拟机快照

支持创建快照，对启动中的虚拟机系统磁盘创建即时快照，能够指定快照名称、描述信息；

支持还原快照，将虚拟机还原到指定快照的状态；

支持查询快照，获取单个快照的详细信息，包括对应的虚拟机标识、名称、创建日期、大小等信息；

支持在线快照，虚拟机不关机即可完成快照的创建；

支持删除单个快照，支持批量删除快照；

支持对虚拟机和云硬盘同时做快照；

支持虚拟机定时快照，按每n小时、每n天创建一份快照。

##### 虚拟机迁移

虚拟机迁移支持虚拟机热迁移和冷迁移。

支持虚拟机热迁移，虚拟机不关机时，将虚拟机手动迁移至指定计算节点；

支持虚拟机冷迁移，虚拟机关机时，将虚拟机手动迁移至指定计算节点。

虚拟机冷迁移，需要提前将内存中的数据保存至磁盘，然后再迁移至目标节点。

而虚拟机热迁移又叫动态迁移、实时迁移，主要为保存和恢复虚拟机。因此，除了虚拟机的磁盘数据进行保存之外，对虚拟机的内存运行状态也会完整保存下来。迁移以后，虚拟机仍能够平滑运行，对用户而言不会察觉到任何差异，这种方式更适用于不能中断业务的重要应用。相比冷迁移来说，热迁移的难点在于内存数据的迁移。

##### 虚拟机高可用性

支持虚拟机高可用，当虚拟机故障或操作系统蓝屏崩溃时，系统自动将故障的虚拟机在正常的计算节点上重新创建，使故障虚拟机快速恢复；

支持高可用全局开关，可一键开启或关闭集群内所有虚拟机的高可用特性；

支持应用高可用，通过内置脚本监测虚拟机中的应用程序，当检测到应用程序崩溃时，系统自动将虚拟机在正常的计算节点上重新创建，使故障的应用程序快速恢复。

##### 镜像管理

镜像包括普通镜像（ISO镜像）和虚拟机镜像，普通镜像可以通过虚拟光盘的方式挂载到虚拟机，也可以通过系统ISO镜像安装虚拟机操作系统；虚拟机镜像是由虚拟机制作而成的，可通过虚拟机镜像快速地创建虚拟机。镜像管理主要提供的功能包括：

（1）支持导入、上传多种格式的镜像文件；

（2）支持自定义选择镜像，创建虚拟机；

（3）支持虚拟机镜像的导出。

##### DRS管理

DRS管理功能主要实现当多台计算节点上负载量差距较大时，支持配置负载均衡策略、包括定时时间配置、CPU负载差阈值配置、监控取样时间配置、最大内存阈值配置，将云服务器从负载高的宿主机热迁移到负载低的宿主机，从而实现计算节点的使用资源的负载平衡，来保障云服务器的性能。

虚拟化管理平台的这种负载均衡功能可以自动平衡计算节点的压力负载，为业务的连续性提供有力保障。

##### 虚拟机备份

支持创建虚拟机备份任务，选择指定的备份服务器对虚拟机进行备份，当虚拟机故障或被删除后，能够通过备份及时恢复。主要功能包括：

（1）支持虚拟机备份到本地磁盘，并从本地磁盘恢复；

（2）支持虚拟机备份到共享存储，从共享存储恢复；

（3）支持列举虚拟机的所有备份信息；

（4）支持在线备份，虚拟机不关机即可完成备份的创建；

（5）支持从选定备份创建虚拟机；

（6）支持备份池管理，可创建本地备份、集群共享存储和远端共享存储；

（7）支持虚拟机备份至远端共享存储，包括文件存储和对象存储。

##### 云硬盘服务

（1）支持创建云硬盘，指定云硬盘的名称及空间大小；

（2）支持挂载云硬盘，将创建云硬盘挂载至云主机；

（3）支持卸载云硬盘，将挂载的云硬盘从云主机卸载；

（4）支持扩容云硬盘，扩大未挂载或虚拟机关机时的云硬盘空间；

（5）支持云硬盘快照，对单独云硬盘或已挂载的云硬盘做快照保护；

（6）支持云硬盘备份，可对指定云硬盘进行备份；

（7）支持云硬盘定时任务，可对指定云硬盘进行定时快照和定时备份。

##### 虚拟网络配置管理

云计算平台按需创建各类虚拟机后，需要通过配置虚拟网络，满足虚拟机之间及虚拟机和外部之间数据交互的需求。基于虚拟交换机实现网络的虚拟化，主要实现如下功能包括：

（1）支持创建虚拟交换机，并可通过虚拟机交换机创建VLAN类型网络；

（2）支持网络流量控制，控制上行/下行链路流量，和网络优先级；

（3）支持创建虚拟IP，并进行统一管理，支持提供浮动IP服务。

云计算平台的虚拟交换机使用服务器的CPU和内存来实现虚拟交换的功能，每个虚拟交换机都有两种端口：unlink port用来绑定一个物理网卡，downlink port用来连接虚拟机。

##### 资源直通功能

资源直通主要是指宿主机的网卡、磁盘和USB端口可之间分配给某台虚拟机使用，以提升虚拟机的性能。

（1）网卡直通

1）支持SR-IOV网卡直通，物理网卡可虚拟成多个虚拟网卡；

2）支持虚拟机多网卡，单个虚拟机可配置多个网卡，使用多网域；

3）支持带SR-IOV网卡的虚拟机进行疏散和冷迁移。

（2）磁盘直通

支持将宿主机中的磁盘直通给虚拟机使用。

（3）USB直通

支持将宿主机的USB直接分配给指定虚拟机，可以使该虚拟机挂载USB设备。

#### 数据存储管理

智能计算资源池通过Ceph技术，提供了虚拟化存储功能。通过存储虚拟化，可以将底层的存储设备抽象出来，作为一个统一的、可靠的、大容量的存储资源池提供给用户即可，不用关注底层的存储设备类型以及其所提供的存储能力。该技术有效的提高了存储资源的利用率，保证了数据的可靠性，同时经过虚拟化后的存储资源存在较好的迁移性，提高了可维护性 可扩展性。

##### 生命周期管理

支持创建、扩容、删除存储资源池，满足创建虚拟机时的存储资源需求；

扩容存储池：支持扩容存储池，将集群内的空闲硬盘，加入存储池内，增加存储池的可用容量；

设置默认池：支持将存储池设置为默认池，当需要选择存储池时优先展示；

删除存储池：支持删除指定存储池，删除时该存储池中没有资源实例。

##### 存储虚拟化

支持采用Ceph等分布式存储技术，将各云计算服务器本地硬盘资源构建一个存储资源池，进行统一管理，并按需分配给虚拟机使用。

##### 多规格存储池

支持创建多种规格的存储资源池，包括：

（1）支持自定义选择集群内的SSD和HDD硬盘，创建相应的存储池；

（2）支持设置存储池副本数，可按需设置2副本和3副本；

（3）支持设置存储类型，可设置普通型（适用通用场景）和快速型（适用高性能场景）。

##### 精简配置管理

支持精简配置，对分配的块存储容量根据实际用量进行动态分配。

##### 数据备份

支持一套系统内同时创建多种类型的备份池，包括本地存储备份池和远端存储备份池，其中本地存储包括本地硬盘和本地共享存储，远端存储包括支持标准NFS协议的文件存储和支持标准S3协议的对象存储。

### 性能设计

（1）云计算管理性能

支持管理的计算节点数量为1到16个。

（2）镜像文件管理性能

当个镜像文件最大支持100GB。

（3）虚拟机创建性能

支持批量创建虚拟机的数量为最大10个。

### 资源规划

（1）云平台计算节点服务器

方案设计选用的云计算节点服务器详细配置如下：

CPU：配置2颗Xeon® Gold 4214R 核数≥12核，主频≥2.4GHz；

内存：配置128G DDR4，16根内存插槽，最大支持扩展至2TB内存；

硬盘：配置2块600G 10K 2.5寸 SAS硬盘，2块 480G SSD硬盘，2块4T 7.2K SATA硬盘 配置8个硬盘插槽；

阵列卡：配置SAS\_HBA卡，支持RAID 0/1/10；

PCIE扩展：最大可支持6个PCIE扩展插槽；

网口：配置2个千兆电口，2个万兆光口。

（2）服务器数量计算

*//云平台计算节点服务器数据计算需根据具体的需求来设计，这里主要给出详细的数量推送过程。*

为了保证虚拟机的可靠性，在发生计算节点异常故障时，使得故障计算节点的虚拟机能在其它计算节点通过云平台高可靠性功能运行起来，尽量减少业务的中断时间，所以在系统部署时，系统计算节点的CPU、内存和存储资源需按照表4所示考虑一定的冗余。

1. 云计算配置参数一览表

| 参数名称 | 数值 | 说明 |
| --- | --- | --- |
| CPU超分 | 2或1.5 | 物理CPU总线程数\*CPU超分比=可分配的虚拟CPU资源数量（vCPU默认为线程数，内存以及存储不作超分）。 |
| 超线程 | 2 | x86 CPU默认为2。 |
| CPU需求冗余占比 | 20% | CPU冗余资源占总资源池比例，默认预留20%。 |
| 内存需求冗余占比 | 5% | 内存冗余资源占总资源池比例，默认预留10%。 |
| 存储需求冗余占比 | 20% | 存储冗余资源占总资源池比例，默认预留20%。 |
| CPU资源系统损耗（vCPU） | 8 | 部署计算资源池所消耗的CPU资源，默认8vCPU |
| 内存资源系统损耗（GB） | 20 | 部署计算资源池所消耗的内存资源，默认20GB。 |
| 计算节点内存阈值 | 90% | 为保证系统运行稳定，计算节点内存阈值最大值为90%。 |
| 存储副本数 | 3 | 分布式存储使用3副本。 |
| 存储硬盘进制转换 | 0.9 | 硬盘10进制和2进制转化。 |
| 高可用 | 开启/不开启 | 节点大于3台支持高可用，开启高可用功能需冗余1台节点。 |

云平台计算节点服务器的资源总量需要从vCPU、内存和存储三个维度满足资源总需求，计算节点数量公式如下：

计算节点数量 = MAX（vCPU维度下计算节点数，内存维度下计算节点数，存储维度下计算节点数）。

（1）vCPU维度下计算云平台计算节点数量

本次选型的云平台计算节点CPU为2颗4214R（12核 2.4GHz）， CPU开启超线程，同时开启2倍CPU超分，同时考虑上层部署的计算资源池所消耗的8个vCPU，因此单服务器可供虚拟机使用的CPU核数为：

单台服务器可供虚拟机使用的CPU核数=（（单台计算节点的vCPU数 – CPU资源系统损耗） \*CPU超分比。

因此，按照上述业务所需的vCPU需求可以计算硬件服务器数量：

vCPU维度下云平台计算节点数= Roundup （ 总vCPU数 \*（1 + CPU需求冗余占比）/（（单台计算节点的vCPU数 – CPU资源系统损耗） \*CPU超分比 ））。

（2）内存维度下计算云计算节点数量

本次选型的云平台计算节点内存大小为128GB，为保证系统运行稳定，计算节点内存阈值最大值为90%，同时考虑部署计算资源池所消耗的20GB内存资源，得到单台服务器可提供的内存为：

单台服务器可供虚拟机使用的内存=（单台计算节点的内存大小–内存资源系统损耗）\*宿主机内存阈值 ）。

因此，按照上述业务所需的内存需求可以计算硬件服务器数量：

内存维度下云平台计算节点数= Roundup （总内存 \* （1 + 内存需求冗余比）/（（单台计算节点的内存大小 – 内存资源系统损耗）\*宿主机内存阈值 ））。

（3）存储维度下计算云平台计算节点数量

本次选型的云平台计算节点硬盘总量8 TB，考虑到十进制和二进制的转换比约为0.9，因此单台服务器可提供的存储容量为：

单服务器可提供的存储容量=单台计算节点的硬盘总量 \* 存储硬盘进制转换比=8 \* 0.9 = 7.2T

云平台在数据存储时采用了3副本形式进一步保障上述业务数据的安全性。因此，根据CLE-TB业务所需的存储需求可以计算硬件服务器数量：

存储维度下云平台计算节点数量= Roundup（ 总硬盘 \* （1 + 硬盘需求冗余比）\* 存储副本数 / （单台计算节点的硬盘总量 \* 存储硬盘进制转换比 ））。

（4）云平台计算节点需求汇总

综合CPU、内存和存储三个维度，取计算节点服务器台数最大值，得到最终计算节点服务器台数为：

云平台计算节点服务器台数 = Max（vCPU维度下云计算节点数，内存维度下云计算节点数，存储维度下云计算节点数）。

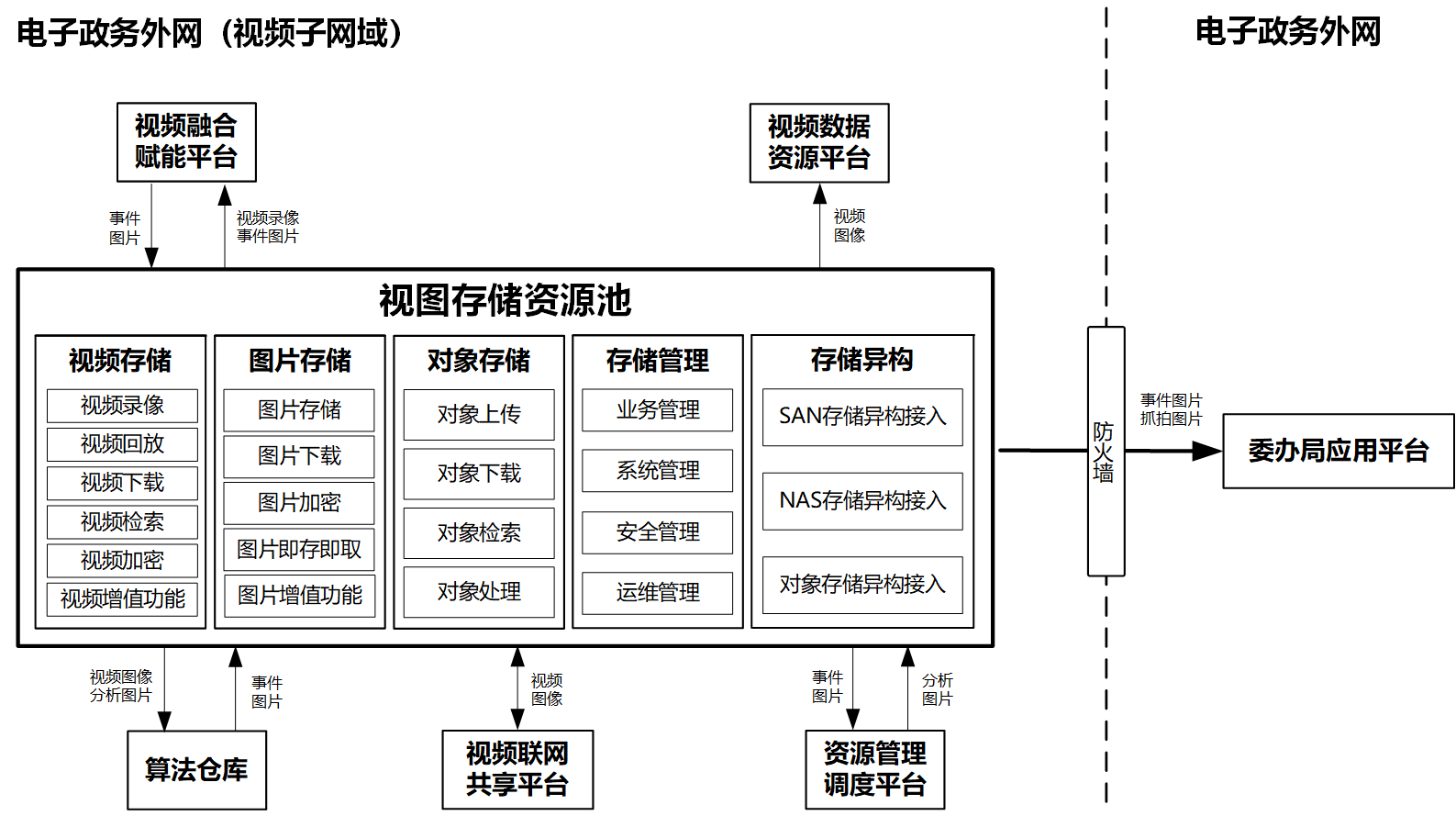
## 视图存储资源池

### 概述

视图存储资源池是一套云存储系统，面向视频流式数据存储场景提供高效的视频、图片存储和管理方案，打造一站式存储资源池。云存储是在云计算概念上延伸和发展出来的一个新的概念，是指通过集群应用、网格技术或分布式文件系统等功能，应用存储虚拟化技术将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供多维数据（如视频、图片等）存储和业务访问功能的一个系统。视图存储资源池结合先进的集群化技术、虚拟化技术、离散存储技术等，通过特有的流式文件系统对存储资源进行虚拟化和应用化整合，全面优化存储系统在视频监控领域的存储效率，为用户提供高性能、高稳定、高扩展性的数据存储服务，提供包括视频、图片在内的存储能力。

### 架构设计

基于新建或者现有的存储资源构建视图存储资源池，支撑支撑视频联网共享平台、资源管理调度平台、视频运维服务平台、算法仓库、视频融合赋能平台、视频数据资源平台、委办局应用平台的视频图片的存取需求。详细架构如图15所示。



1. 视图存储资源池架构图

### 功能设计

视图存储资源池包括存储管理、视频存储、图片存储、对象存储、存储异构五个模块。

#### 存储管理

存储管理模块包括业务管理、系统管理、安全管理、运维管理。

##### 业务管理

支持视频、图片、文件、对象数据混合存储，提供融合云存储服务；

支持对视频、图片、文件、对象数据执行不同的数据存储策略，实现对数据生命周期管理。

##### 系统管理

云存储系统管理支持集群化管理、负载均衡管理、虚拟化管理、分散存储管理、生命周期管理、在线扩展、权限管理。

（1）集群化管理

采用集群化管理，存储系统内所有节点采用全工作模式；存储应支持集群容灾，无单点故障，保证存储录像的稳定运行。

（2）负载均衡管理

采用虚拟IP技术，对外提供统一的入口IP形式，将集群的访问在集群中根据各种算法进行分摊，降低单个节点的访问压力。后端硬件节点压力应进行实时监控、反馈和调整，当单台硬件节点压力过大时能根据智能算法将业务平滑迁移至其他硬件节点，达到整个集群间负载均衡目的。

（3）虚拟化管理

采用虚拟IP技术，支持对系统内存储设备的统一管理，将系统内可用存储资源统一虚拟化为资源池，且将虚拟资源划分为块进行管理。

（4）分散存储管理

支持将前端数据通过特定算法，平滑分散至各个硬件节点，从而降低大量回放对单台硬件节点的压力。

（5）生命周期管理

支持业务数据的存储周期管理。可按策略对业务数据进行自动清理，存储周期可以按容量或时间方式进行配置。

（6）在线扩展

支持系统在线扩展提升系统规模、性能、容量能力。

（7）权限管理

支持多级用户管理，对用户和资源池进行绑定，对用户的行为权限进行限定；存储交互协议应采用摘要验证和加密机制，确保网络交互协议的安全。

##### 安全管理

云存储安全管理支持纠删码保护、N+M在线调整、数据安全保护、业务安全保护、录像安全保护、智能重构、开放兼容。

（1）纠删码保护

支持Erasure Code算法，支持N+M级别数据保障机制。（注：N表示有效数据块，M表示校验数据块）。

（2）N+M在线调整

支持N+M根据系统设备规模进行在线调整，调整后系统可以按照新的数据安全级别进行保存。

（3）数据安全保护

支持N+M级别下，条带中M个以内的块单元故障数据可恢复，支持多硬盘故障数据可以恢复，读写不中断，支持多设备故障数据可以恢复，读写不中断。

（4）业务安全保护

支持存储设备故障，业务可自动进行切换业务持续性。

（5）录像安全保护

支持N+M级别下，条带中M个以上的块单元损坏，剩余数据依然可读，录像依旧可以进行回放。

（6）智能重构

支持设置数据级别，按优先级顺序进行数据重构。

##### 运维管理

云存储运维管理支持系统信息获取、系统故障告警、存储设备告警、标准协议对接等。

（1）系统信息获取

支持系统信息：版本、CPU、内存、网卡、磁盘等信息的获取。

（2）系统故障告警

支持系统故障（CPU、内存等超过阈值）主动告警到运维平台。

（3）存储设备告警

支持设备故障、掉线会主动告警到运维平台。

（4）标准协议对接

支持标准的SNMP协议对接。

#### 视频存储

视频存储模块用于满足视频直存、转存等存储场景需求，以及视频回放、视频下载、视频检索、视频锁定、视频封面等业务应用需求，支持视频加密确保视频安全。

##### 视频录像

支持按照用户制定的计划保存前端设备采集的录像数据，录像类型、录像开始时间由用户指定，存储开启相关的资源；

支持动态修订录像类型，即在前端采集视频数据过程中，按报警类型可以修改录像的类型，修改后采集的视频数据即时保存到存储中；

支持视音频流能直接在融合云存储系统上进行存储，支持采用流媒体直存转发方式，由存储服务器本机直接对流媒体进行存储转发，无需配置存储转发/流媒体服务器。

##### 视频回放

支持根据编码器名称以及时间段、录像类型对录像数据进行回放，存储应支持根据编码器名称以及时间段对录像数据进行回放时间定位；

支持特殊模式的回放，包括快/慢回放、倒序回放、I帧回放、手动停止回放等。

##### 视频下载

支持根据编码器名称以及时间段对录像数据进行下载，支持断网等条件下，前端设备能够将本地保存的数据补录到存储中。

##### 视频检索

支持按监控点编号、录像类型、时间组合、锁定、标注等条件查询录像数据。

##### 视频加密

对视频数据提供安全存储保护，关键数据加密存储，授权访问，保护隐私数据。

##### 视频增值功能

（1）视频封面

支持针对实时流、视频文件、流式对象上传视频生成视频封面功能。

（2）视频锁定

支持用户指定监控点位时间段数据进行锁定存储。

#### 图片存储

图片存储模块用于满足图片直存、转存、即存即取等存储场景需求，以及图片下载、图片马赛克、图片水印、图片锁定等业务应用需求，支持图片加密确保图片安全。

##### 图片存储

支持图片按RESTful协议，从前端直写存储；

支持图片通过中间服务器转发写入存储；

支持采用http和https协议上传图片。

##### 图片下载

支持按URL下载单张指定图片；

支持采用http和https协议下载图片；

支持外部授权下载。

##### 图片加密

对图片数据提供安全存储保护，关键数据加密存储，授权访问，保护隐私数据。

##### 图片即存即取

支持大小图即时进行提取，提升图片提取效率。

##### 图片增值功能

（1）图片马赛克

支持对图片任意指定矩形区域进行马赛克处理。

（2）图片归一化

支持对图片任意指定矩形区域进行归一化处理。

（3）图片水印

支持图片下载时在指定区域增加水印文字。

（4）图片锁定

支持按图片URL锁定图片，保证资源池内锁定图片不被资源池覆盖策略提前被覆盖。

（5）图片裁剪

支持对指定图片按用户规划指定矩形区域坐标进行裁剪。

#### 对象存储

对象存储模块用于满足案件数据、零散口袋数据、音视频文件等的存储场景需求，以及视频合成、转码、水印等数据处理业务应用需求。

##### 对象上传

（1）支持将整个文件切分成多个分片独立上传，全部分片上传完成后，将分片合并成一个文件。

（2）支持将上传结果回调给第三方服务器。

（3）支持流式对象上传，使数据同时具备流式和对象数据特性。

##### 对象下载

（1）支持一次性返回所有数据的下载方式。

（2）支持断点续传下载，指定下载开始偏移与结束偏移，返回指定偏移段内数据。

（3）支持通过URL分享，授权第三方下载。

##### 对象检索

支持根据需要获取某个Bucket下的所有Object列表，用户可以添加入前缀等参数增加获取结果速度。

##### 对象处理

（1）图片处理

支持图片压缩、图片剪裁、图片缩放、图片格式转换。

（2）视频处理

支持视频多画面合成、视频转码、视频压缩、视频水印、视频转封装。

#### 存储异构

存储异构模块用于满足现有外部存储接入管理、外部存储利旧等业务场景，支持SAN、NAS、对象存储异构接入及管理。

##### SAN存储异构接入

支持异构多厂家IP-SAN（iSCSI）、FC-SAN（FC）存储；

支持SAN设备直写祼盘接入；

支持iSCSI、FC异构方案多类型功能。

##### NAS存储异构接入

支持异构多厂家NAS（CIFS/NFS)存储，并支持NAS设备虚拟化一个或多个存储卷接入。

##### 对象存储异构接入

支持异构S3（V4）、阿里OSS对象存储。

### 性能设计

（1）前端接入存储性能

单云最大可支持30000路前端点位接入。

（2）存储节点管理性能

单云最大可支持300台存储节点管理。

（3）存储容量管理性能

单云最大可支持300PB存储容量管理。

### 资源规划

*//可以参考公司云存储计算工具，结合项目存储需求，合理进行云存储软硬件配置。*

（1）视图存储设备

视图存储设备的需满足视频和图片的存储需求，本方案视频存储、图片存储和对象存储需求计算过程如下。

1）视频存储需求

按照前端类型的不同，H.265 视频编码的码流在不降码率的情况下存储空间要求为：200万像素以2Mbps的实时码流存储，400万像素以4Mbps的实时码流存储，800万像素以8Mbps的实时码流存储，1600万像素以20Mbps的实时码流存储。本期项目前端点位XX个，录像存储周期XX天。

按照一般的容量计算方法，给出其存储空间计算公式：单路实时视频的存储容量（TB）＝（视频码流大小（Mb）×60秒×60分×24小时×存储周期/8）/1024/1024。

根据计算，视频数据存储共需XXTB的存储空间。

2）图片存储需求

本方案图片存储涉及到视频抓图分析、视频实时分析结果两部分，200万像素摄像头抓图大小按1MB考虑、400万像素摄像头抓图大小按2MB考虑。

视频抓图分析部分：结合智能分析业务需求，需要 XX路视频点位进行抓图分析，每小时分析XX次，每张图片按2MB、按30天存储考虑。

计算过程如下：抓拍数量\*每小时频次\*24小时\*存储天数\*图片大小/1024/1024=抓拍图片存储容量

视频实时分析结果部分：结合智能分析业务需求，总共约XX路视频分析，预估每天按XX个有效事件（XX个事件/路），取每个事件1张图片进行存储设计，每张图片按2MB、按90天进行存储考虑。

计算过程如下：每天有效事件数\*存储天数\*图片大小/1024/1024=视频实时分析图片容量

根据计算，图片共需XXTB的存储空间。

3）对象存储需求

算法仓库的素材库需要利用对象存储，对各类算法训练或者校验使用的图片素材进行存储和管理，素材库可存储、管理的图片数据上限1000万张，每张图片按2M设计，则需要20TB左右的存储容量。

综合前面计算结果，视频、图片和对象存储共需XXTB的存储空间。方案设计采用24盘位8TB硬盘的流式存储设备，设备支持原始视频、图片数据存储。整体考虑系统容量冗余5%、数据重构冗余5%、磁盘格式损失5%、EC纠编码冗余13%、二进制换算损失9%等因素。

1. 视图存储资源

| 配置要求 | 参数 |
| --- | --- |
| 容量需求（TB） | XX |
| EC纠编码冗余 | 0.13 |
| 系统容量冗余率 | 0.05 |
| 系统热备率 | 0.05 |
| 二进制换算损失 | 0.09 |
| 裸容量需求（TB） | XX |
| 设备数量（8T/24盘位） | XX |

共计需要XX台存储设备。

（2）管理节点服务器

需要配置N台管理节点服务器（CPU：16核2.2GHz及以上；内存：32GB；硬盘：300G SAS，960G SSD；网络：1GbE，可以采用同规格虚拟机）用于部署视图存储资源池的运维管理模块。

*//需根据视频云存储节点的多少来看具体管理节点数量，存储节点小于10可不配置管理节点。*

（3）存储运维服务器

需要配置1台存储运维服务器（CPU：16核2.2GHz及以上；内存：16GB；硬盘：300G SAS，480G SSD；网络：1GbE，可以采用同规格虚拟机）用于部署视图存储资源池的运维管理模块。

# 部署方案设计

## 通用计算资源配置

通用计算资源是指用于部署各平台软件的服务器，这里汇总前面各平台软件服务器配置需求，便于统一进行通用计算资源配置。

### 视频融合赋能平台

1. 视频融合赋能平台硬件配置表

| 服务器 | 推荐配置 | 数量 | 配置说明 |
| --- | --- | --- | --- |
| 平台应用服务器 | CPU：32核2.2GHz及以上  内存：64GB  硬盘：600G SAS  网络：1GbE | 4台 | 必配 |
| 平台日志服务器 | CPU：8核2.2GHz及以上  内存：16GB  硬盘：300G SAS +1200G SATA  网络：1GbE | 1台 | 选配，数量根据资源规划章节计算得出 |
| 策略应用服务器 | CPU：32核2.2GHz及以上  内存：64GB  硬盘：300G SAS  网络：1GbE | 1台 | 必配 |

### 资源管理调度平台

1. 资源管理调度平台硬件配置表

| 服务器 | 推荐配置 | 数量 | 配置说明 |
| --- | --- | --- | --- |
| 平台应用服务器 | CPU：32核2.2GHz及以上  内存：64GB  硬盘：300GB SAS  网络：1GbE | 1台 | 必配 |
| 视频抓图服务器 | CPU：32核2.2GHz及以上  内存：64GB  硬盘：300G SAS  网络：1GbE | 1台 | 选配，数量根据资源规划章节计算得出 |

## 智能计算资源配置

1. 智能分析服务器配置表

| 服务器 | 推荐配置 | 数量 | 配置说明 |
| --- | --- | --- | --- |
| 智能分析服务器 | 处理器：HG7255\*2（16核，32线程，2.2GHz）  GPU卡：8张高性能GPU卡；单卡提供64TOPS INT8算力  内存：16GB DDR4 \* 4 ，32个内存插槽  硬盘：480GB SSD \* 1  网络接口：1个千兆IPMI管理端口，2个板载千兆电口，10GbE \* 2光口  硬盘接口：前置：可支持24个3.5'' SATA/SAS硬盘接口（可支持2.5'' HDD/SSD），24盘需3张HBA/Raid支持，板载：可支持2个M.2接口  PCIe扩展能力：20个 PCIE3.0 × 16扩展槽，最多支持16个GPU卡  内存插槽数：32个DDR4内存插槽 | 3台 | 必配，数量根据前面计算得出。建议主推国产化+KT2 |

## 视图存储资源配置

需要部署视频图像存储设备，支撑视频点位录像智能分析抓图、智能分析结果等业务的视图存储需求。

1. 视图存储设备配置表

| 服务器 | 推荐配置 | 数量 | 配置说明 |
| --- | --- | --- | --- |
| 视图存储设备 | 4U机架式24盘位，64位多核处理器；16GB缓存；冗余电源；24块8T的企业级IoT硬盘；6个千兆网口；1个系统SSD盘，支持网络RAID，支持视音频、图片、直接写入，支持视频高速预览、回放、下载，支持云内容灾备份，支持一体化运维，支持GB/T 28181、Onvif、RTSP、H265、SVAC等标准视频协议 | 2台 | 必配，存储设备上运行云存储软件。 |

# 保障体系设计

## 安全保障体系

### 网络安全等级保护

*//此部分需根据项目具体的网络方案情况进行调整，以下内容供参考。*

网络安全等级保护制度在今天已上升为法律，并在法律层面确立了其在网络安全领域的基础、核心地位，等级保护正式进入了2.0时代。等保2.0相关的《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准正式发布，也已于2019年12月1日开始实施。网络安全等级保护制度是国家网络安全保障的基本制度、基本策略、基本方法。开展网络安全等级保护工作是保护信息化发展、维护网络安全的根本保障，是网络安全保障工作中国家意志的体现。

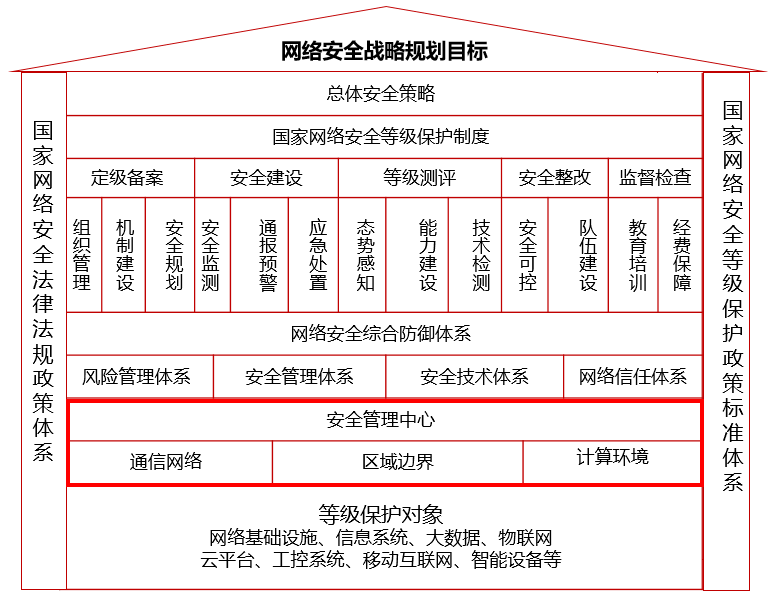
本方案主要涉及到电子政务外网、电子政务外网视频子网域、委办局专网、互联网等网络对象，电子政务外网视频子网域为新建的网络，该网络需打通和其他网络的实现视频图像和数据的汇聚与应用，所以此部分重点考虑电子政务外网视频子网域的网络安全等级保护。

#### 网络安全架构

根据“一个中心、三重防护”理念搭建体系框架，构建安全机制和策略，形成定级系统的安全保护环境。分别对区域边界、通信网络、计算环境体系进行管理，实施多层隔离和保护，以防止某些薄弱环节影响整体安全。

“一个中心”是指安全管理中心，即构建先进高效的安全管理中心，实现针对系统、产品、设备、策略、信息安全事件、操作流程等的统一管理；“三重防护”是指构建安全区域边界、安全计算环境、安全通信网络三维一体的技术防御体系。

本方案针对系统的通信网络、区域边界、计算环境等方面，采用访问控制、入侵检测、恶意代码法防范、安全审计、防病毒等多种技术和措施，实现业务应用的可用性、完整性和保密性保护，并在此基础上实现综合集中的安全管理，并充分考虑各种技术的组合和功能的互补性，合理利用措施，从外到内形成一个纵深的主动的安全防御体系，保障信息系统整体的安全保护能力。



1. 网络安全等级保护体系框架

#### 安全物理环境

在安全物理环境中，机房物理位置选择应避开高层、地下室等位置，如果已经完成机房位置的选择，则需要加强响应的防水、防潮等防护。

对于机房人员出入要设置电子门禁等方式进行控制，并且进行鉴别和记录。对机房所在楼宇或者机房中要有防雷击或者过压保护等装置。在防火、防水、防潮等部署专业的消防设施及精密空调等设备。对机房电力采用冗余或者并行的电力电缆供电等措施满足等保相关要求。

*注：安全物理环境通常指机房建设，此部分需按照机房相关要求进行建设。不做详细描述。*

#### 安全通信网络

##### 网络架构设计

为了系统实现良好的安全保障，需要对系统网络架构进行安全设计，并且参照等级保护的要求对系统安全区域进行划分设计。区域划分后使整个网络逻辑结构清晰，同时也可以根据需求进行更细粒度的安全防护，最终实现业务系统、数据中心、流量转发之间的安全防护。

根据等保要求，在架构设计产品选型以及区域划分中参考以下原则：

（1）计算业务流量并且规划3-5年的业务增长情况，保证业务处理能力满足业务高峰期需要和日后增长的需求。

（2）重要网络区域主要是业务区域，不要规划在边界处，而且有隔离手段。

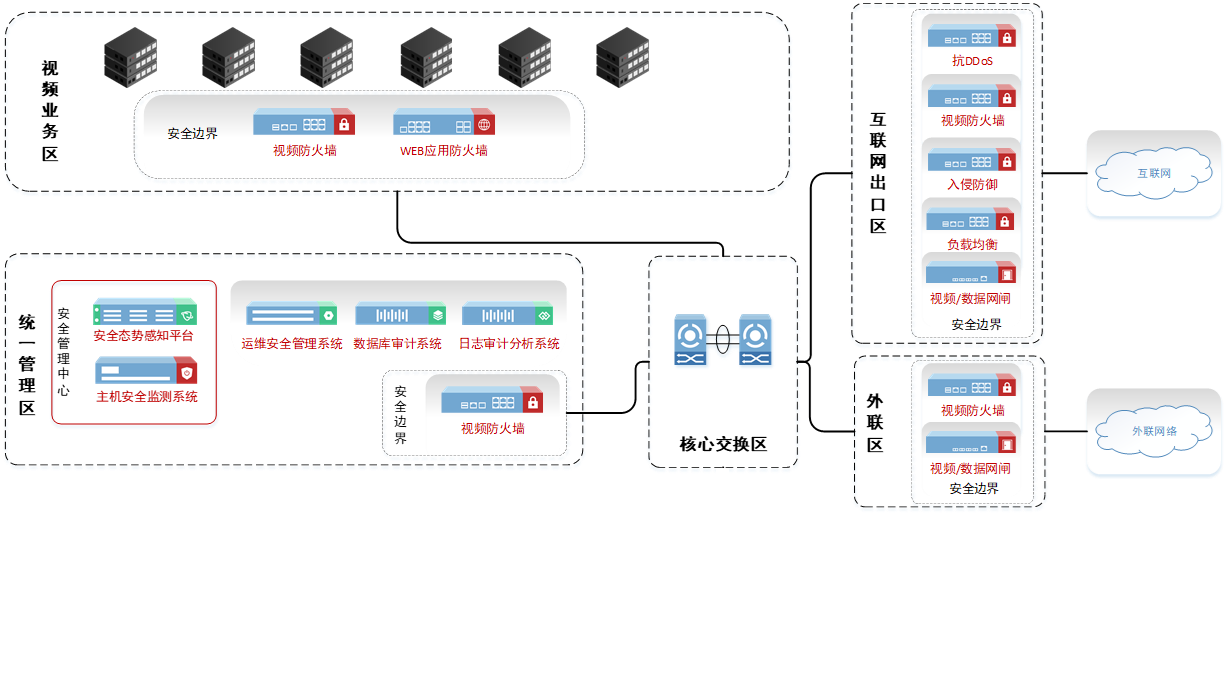
（3）业务的通信线路采用冗余线路，保证系统的可用性。

（4）在划分不同业务区域时，应按照方便管理和控制的原则为各网络区域分配地址，严格控制掩码长度，避免大段地址的浪费，提高网络地址利用率的同时，能简化策略的配置。

合理的安全域设计是重中之重，各个区域应该按照业务属性、业务重要程度和业务等级区分类别。如，办公网与服务器网不能处于同一区域，三级和三级的业务系统也要相对隔离。

因此，本方案分别对整个网络进行安全区域的划分，将电子政务外网视频子网域建设区域分为统一管理区、视频业务区、外联区、互联网出口区等五个部分。具体如图17所示：

*//网络安全架构需结合项目实际情况进行设计调整。*



1. 电子政务外网视频子网域等保建设方案拓扑图

（1）统一管理区

统一管理区中态势感知平台作为安全管理中心，具备策略管理、漏洞管理、攻击监控、流量监控等功能，同时联动其他网络安全产品形成统一的网络安全防护体系。三审产品（日志审计分析系统、数据库审计系统、运维安全管理系统）满足等保标准中身份鉴别与安全审计的要求。

（2）视频业务区

视频业务区中视频防火墙产品可满足边界安全防护的要求，同时利用WEB应用防火墙产品对WEB攻击行为进行自动防护，减少网站运营的安全风险。

（3）外联区

外联区域通过视频防火墙、边界接入平台（视频边界、数据边界）等设备对边界进行安全防护，满足连接外部服务过程中边界安全防护的要求。

（4）互联网出口区

互联网出口区主要针对外网边界进行安全防护，通过部署视频防火墙满足视频访问控制与威胁防护的要求，通过负载均衡产品满足链路流量动态平衡的需求。入侵防御设备可对外部入侵活动与攻击性网络流量进行实时阻断，提供针对病毒、木马、僵尸网络等攻击的防护措施，全方位防护各种攻击。抗拒绝服务攻击系统可抵御大流量的DDoS攻击与CC攻击，保证业务系统稳定可靠。边界接入平台（视频边界、数据边界）确保电子政务外网视频子网域与互联网间的物理隔离和单向传输。

##### 通信传输设计

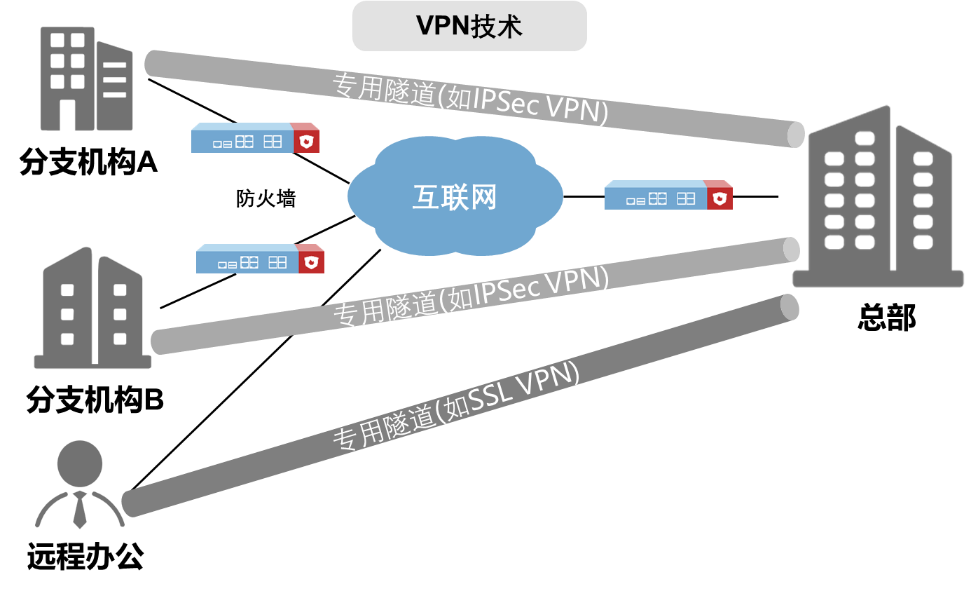
在电子政务外网视频子网域系统中，存在通过互联网访问内部业务系统的需求。或者分支与总部之间通过互联网进行纵向互联的需求。

确保敏感信息在网络传输过程中的完整性和保密性是通信传输的重要要求，对此，可采用的手段包含IPSec VPN或SSL VPN技术。

IPSec VPN：IPSec是IETF制定的三层隧道加密协议，它为互联网上传输的数据提供了高质量的、基于密码学的安全保证，是一种传统的实现三层VPN的安全技术。IPSec通过在特定通信方之间（例如两个安全设备之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPSec隧道。

SSL VPN: SSL VPN是以HTTPS为基础的VPN技术，充分利用了SSL协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，可以为通信建立安全连接。

防火墙支持IPSec VPN和SSL VPN技术，通过IPSec VPN可实现总部与分支机构之间通过互联网的纵向互联；通过SSL VPN可以实现远程访问总部内网资源。VPN连接如下图：



1. VPN 远程访问

远程访问内网资源过程中，基于SSL安全传输协议而构建的VPN系统，实现对传输数据的加密、传输数据的完整性校验。

在通过互联网实现纵向互联的过程中，通过IPSec VPN技术，将实现如下的保护：

机密性保护：在传输过程中对数据进行加密，从而防范了被篡改的风险；

完整性保护：在传输过程中，通过HASH算法，对文件进行摘要处理，当到达接收端时再次进行HASH，并与发送端HASH后形成的摘要进行批对，如果完全相同则证明数据没有被篡改，从而保障了传输过程的完整性。

#### 安全区域边界

在等保2.0相关要求中，安全区域边界设计包括边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范以及安全审计五个部分。本次项目重点考虑横向同各委办局专网及电子政务外网的边界安全的设计。

##### 电子政务外网边界安全防护

电子政务外网视频子网域与电子政务外网边界安全防护通过部署安全网关（防火墙）实现：

对登录视频云中台的用户进行身份鉴别，用户身份管理和认证管理由安全基础设施统一提供；

对视频云中台应用服务进行API攻击防护，检测、识别、拦截针对API接口的攻击；

对视频云中台应用服务进行应用层DDoS攻击防护，阻断恶意发送大量合理请求、消耗目标系统服务资源的DDoS攻击行为；

对邮件协议、内容和附件进行深度分析，检测并阻断垃圾邮件传播；

对视频云中台应用内容进行安全防护，防止自动化工具攻击和数据爬取。

##### 其他网络边界安全防护

（1）视频交换通道设计

其他网络主要包括委办局专网及互联网，其他网络接入电子政务外网视频子网域的视频交换通道，应部署视频防火墙、视频安全交换系统、视频网闸等设备，实现其他网络及互联网与电子政务外网视频子网域的视频数据的单向导入和单向导出。

1）安全网关（防火墙）或视频防火墙

通过部署安全网关（防火墙）或视频防火墙，实现：

对登录视频云中台的用户进行身份鉴别，用户身份管理和认证管理由安全基础设施统一提供；

对视频图像应用服务进行API攻击防护，检测、识别、拦截针对API接口的攻击；

对视频图像应用服务进行应用层DDoS攻击防护，阻断恶意发送大量合理请求、消耗目标系统服务资源的DDoS攻击行为；

对邮件协议、内容和附件进行深度分析，检测并阻断垃圾邮件传播；

对视频云中台视频应用内容进行安全防护，防止自动化工具攻击和数据爬取。

2）视频安全交换系统

通过部署视频安全交换系统，实现：

视频接入认证服务器对接入对象（终端、视频服务器等）进行设备认证并与之交互，获取视频。视频用户认证服务器对电子政务外网视频子网域上使用视频资源的终端用户进行统一注册、身份认证和访问控制，并提供视频服务；

对视频数据与控制信令严格区分，分别处理后进行传输；

对视频信令格式检查及内容过滤：能够识别视频控制信令、视频传输协议，阻断未注册的协议和数据格式；

对视频接入设备进行身份认证，禁止未认证设备连接视频接入链路；

对用户进行身份认证和访问控制，保证仅允许认证通过的用户才能访问已授权的视频资源；

3）视频网闸

通过部署视频网闸，实现：

网络隔离：实现网络隔离，切断所有基于网络协议的连接，使外部终端无法直接访问内网，确保电子政务外网视频子网域的安全；

访问控制：能够对接入的视频数据的源地址及端口进行访问控制，以保证数据源的合法性，防止非法数据进来；

内容检查：能够进行视频传输协议格式检测，即使对所传输的视频流实时进行分析和过滤，并对非法的视频流进行阻断和报警，从而保证视频接入业务只传制定格式的视频流而不传输其他任何非视频信息；

防病毒：采用视频协议过滤等技术手段实现视频信息防木马和病毒；

数据加密：能够保证对敏感的视频信息传输进行通信机密性保护，防止敏感数据外泄。

（2）数据交换通道设计

其他网络接入电子政务外网视频子网域的数据交换通道，应部署安全网关（防火墙）、安全数据交换系统、双向网闸，实现其他网络与电子政务外网视频子网域的图片、数据的共享。

1）安全网关（防火墙）

通过部署安全网关（防火墙），实现：

对登录视频云中台的用户进行身份鉴别，用户身份管理和认证管理由安全基础设施统一提供；

对视频云中台应用服务进行API攻击防护，检测、识别、拦截针对API接口的攻击；

对视频云中台应用服务进行应用层DDoS攻击防护，阻断恶意发送大量合理请求、消耗目标系统服务资源的DDoS攻击行为；

对邮件协议、内容和附件进行深度分析，检测并阻断垃圾邮件传播；

对视频云中台应用内容进行安全防护，防止自动化工具攻击和数据爬取。

2）安全数据交换系统

通过部署安全数据交换系统，实现：

对文件、数据库数据安全交换，支持各种类型文件的交换；支持各种主流数据库的交换，支持异构数据库交换；

对设备认证、格式检查、内容过滤、病毒查杀、安全审计等安全功能。

3）双向网闸

通过部署双向网闸，切断所有委办局专网基于网络协议的连接，实现：

其他网络对电子政务外网视频子网域访问的物理隔离，确保电子政务外网视频子网域的独立性；

所有过往的流量的通信协议剥离，保证所有协议剥离和再生过程都接受安全审计，并且具有防范各种网络协议攻击的能力。

#### 安全计算环境

为提高区域边界内设备及应用系统的安全性，保障各种设备及应用的正常运行，需要对设备、应用系统、操作系统、数据库等系统进行一系列的安全加固措施，满足等级保护2.0的三级等级保护对象系统性合规性要求。主要通过在重要主机、服务器上安装主机安全监测客户端进行主机设备的安全加固。

##### 身份鉴别及访问控制

针对等保2.0中，安全计算环境对设备、操作系统、应用系统和数据库系统身份鉴别、访问控制方面的要求，需要对区域内的设备进行安全加固，该部分内容要求主要通过各设备、应用系统、数据库系统基线配置来满足。

本方案提供主机安全监测系统设备，通过在资产上部署主机安全监测系统客户端，由主机安全监测管理平台统一对终端资产进行管理，发现安全入侵事件并及时告警，实现对终端资产安全实时检测。

同时，本方案中部署的主机安全监测系统和运维安全管理系统等安全设备，具备符合要求的身份鉴别和访问控制能力。具体如下：

对于用户进行身份鉴别的行为，本方案中的安全产品支持登录失败处理功能，支持结束会话和当登录连接超时自动退出等相关措施；

当进行远程管理时，本方案中的安全产品均支持通过HTTPS/SSH等必要措施防止鉴别信息在网络传输过程中被窃听。

##### 安全审计

区域边界内的设备及应用系统审计要求包括：应启用安全审计功能，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；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；应对审计进程进行保护，防止未经授权的中断等。

通过集中部署日志审计系统，可对视频网络中摄像机、视频存储、安防管理平台、网络设备、安全设备、服务器等设备的日志采集与分析，实现视频网络内大量分散设备异构日志的分布式采集、集中存储、可视化分析和快速检索，满足日志存储不少于六个月的要求。

通过部署数据库审计系统，可具备对数据库访问行为进行实时审计、对数据库的恶意攻击与数据库违规访问等行为进行识别的能力。同时兼容国内外主流的数据库系统，内置大量安全规则，可有效识别SQL注入、数据泄露、违规操作等事件。

应用层安全审计是对业务应用系统行为的审计，需要与应用系统紧密结合，此审计功能应与应用系统统一开发。应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

##### 入侵防范和恶意代码防范

针对安全计算环境要求中的入侵防范和恶意代码防范安全项，本方案提供主机安全监测系统设备，通过在资产上部署主机安全监测系统客户端，由主机安全监测管理平台统一对终端资产进行管理，发现安全入侵事件并及时告警，实现对终端资产安全实时检测。同时支持对主机进行基线核查、漏洞检测等资产脆弱性评估，保证资产安全稳定。基于智能病毒检测引擎可快速发现高危漏洞，并通过病毒文件隔离机制切断病毒文件传播途径，防止病毒文件出现大范围扩散。

（1）客户端兼容性

主机安全监测系统客户端支持Windows server 2008/2012/2016、win 7、win 10、Centos 5.0 +、Redhat 5.0 + 、 Suse11 +、 Ubuntu 14 +等主流操作系统，同时支持中标麒麟、银河麒麟等国产操作系统。除了PC、服务器等设备，同时兼容IPC、智慧屏、视频存储设备等IOT终端设备，可很好地适应视频物联网主机安全防护场景。

（2）脆弱性检测能力

弱口令检测：针对主机系统自身存在弱口令配置的情况，支持对主机进行全面检测；支持自定义配置弱口令字典，用户可按需求进行灵活配置，充分保护主机系统的口令安全。

配置稽查：支持基线核查与应用合规检查，通过一键化检测功能可自动发现系统存在配置问题，并给出合理化的建议，用于完善主机系统存在的薄弱配置，加强系统自身稳定性。

漏洞检测：利用自主研发的漏洞识别引擎对系统进行主动扫描，可精准检测到当前主机系统中存在的安全漏洞，同时支持对漏洞库进行定期更新。

（3）丰富的特征库

基于丰富的漏洞库、病毒库和基线配置库的支撑，结合自主研发的检测引擎，使检测高效且准确性高，帮忙用户快速发现终端安全隐患。

##### 数据完整性与保密性防护

数据存储过程中的完整性与保密性防护应由应用系统构建，通过消息摘要机制可完成完整性校验；而对于用户数据特别是身份鉴别信息的数据保密，应用系统采用密码技术进行数据加密实现鉴别信息的存储保密性。

数据传输过程的完整性与保密性防护，可通过配置防火墙自带的VPN功能，可以用来保障数据包的数据完整性、保密性、可用性。目前主流的VPN组建，主要采用两种方式，即基于IPSec协议的VPN以及基于SSL协议的VPN，通过以上两种方式均能实现数据传输的安全性与保密性。

##### 数据备份恢复

安全计算环境的数据备份与恢复安全要求如下：应提供重要数据的本地数据备份与恢复功能；应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；应提供重要数据处理系统的热冗余，保证系统的高可用性。该部分安全需求建设由业务系统承担。

##### 剩余信息保护及个人信息保护

剩余信息保护要求应对当前的重要应用系统进行安全检查与安全整改与加固，确保应用系统鉴别信息所在的存储空间被释放或重新分配前得到完全清除；确保存有敏感数据的存储空间被释放或重新分配前得到完全清除。该部分安全需求建设由业务系统承担。

个人信息保护要求明确业务系统所需要的数据内容，避免过量采集、非法采集个人信息。该部分安全需求建设由业务系统承担。

#### 安全管理中心

安全管理中心部分是针对整个系统提出的安全管理方面的技术控制要求，通过技术手段实现集中管理。涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。安全管理中心是有效帮助管理人员实施好安全措施的重要保障，是实现业务稳定运行、长治久安的基础。通过安全管理中心的建设，真正实现安全技术层面和管理层面的结合，全面提升用户网络的信息安全保障能力。

在本方案中，划定统一管理区，等保三级方案需通过物联网安全态势感知平台、主机安全监测系统、三审产品（日志审计分析系统、数据库审计系统、运维安全管理系统）进行建设，等保二级方案则通过主机安全监测系统、日志审计分析系统进行建设。

##### 系统管理

通过部署运维安全管理系统，设置系统管理员，对登录设备资源的所有用户身份进行认证，针对网络系统进行管理操作；设置审计管理员，对所有的操作和维护进行审计并分析；设置安全管理员，对访问电子政务外网视频子网域系统的安全策略进行统一配置和授权。运维安全管理系统具体能力如下：

（1）完备的统一操作运维平台

提供统一的C/S运维操作平台，用户可以通过SecureCRT、Putty等字符终端类远程管理客户端软件及微软远程桌面客户端软件，直接登录终端运维平台，集中管理字符终端及图形终端； 支持命令穿透调用运维客户端程序。

提供统一的B/S运维操作平台，用户可以通过B/S运维平台，调用现有SecureCRT、Putty、微软远程桌面客户端等远程管理客户端软件，通过一次一密认证系统，完成单点登录。

（2）集中帐号管理

实现集中化、基于角色的的主从帐号管理，建立自然人与设备帐号之间的一一对应关系，并对设备帐号进行统一管理，定期进行密码修改。

（3）严格权限控制

对用户使用业务系统中资源的具体情况进行合理分配，实现不同用户对不同部分实体资源的合法访问，杜绝非法访问和越权访问。

（4）完善的安全审计

对运维操作的过程进行完全记录，完整保存运维操作的所有日志；统计自然人对资源的访问情况，在出现安全事故时，可以故障定为和责任追踪；对人员的登录过程、操作行为进行审计和处理，建立完善针对“自然人→资源”访问过程的完整审计；为监管部门提供审计平台和审计数据。

##### 审计管理

建立集中集统一的管理平台，实现自动化的监控审计，满足在多种场景下的日志审计需求。

（1）数据库审计

通过部署数据库审计系统，可具备对数据库访问行为进行实时审计、对数据库的恶意攻击与数据库违规访问等行为进行识别的能力。同时兼容国内外主流的数据库系统，内置大量安全规则，可有效识别SQL注入、数据泄露、违规操作等事件。数据库审计系统支持审计主流的数据库系统，比如Oracle、Mysql、SQLServer、DB2、MongoDB、HANA、人大金仓、Hbase、Hive等。

（2）运维操作审计

运维安全管理系统可以对运维操作的过程进行完全记录，完整保存运维操作的所有日志；统计自然人对资源的访问情况，在出现安全事故时，可以故障定为和责任追踪；对人员的登录过程、操作行为进行审计和处理，建立完善针对“自然人→资源”访问过程的完整审计；为监管部门提供审计平台和审计数据。

（3）集中审计

通过集中部署日志审计系统，可对对电子政务外网视频子网域中视频存储、管理平台、网络设备、安全设备、服务器等设备的日志采集与分析，实现视频网络内大量分散设备异构日志的分布式采集、集中存储、可视化分析和快速检索，满足日志存储不少于六个月的要求。具体安全能力如下：

##### 安全管理

建立集中的和统一的管理平台（部署运维安全管理系统），通过运维安全管理系统对电子政务外网视频子网域系统的主体、客体统一进行安全标记，准确识别电子政务外网视频子网域合法用户和系统资产。

通过设置针对电子政务外网视频子网域系统的安全策略，对内网的主体、客体进行授权，确保已标记的主体能访问到电子政务外网视频子网域相对应的系统资源。

针对已进行安全标记的主体设置可信验证策略，提高了已标记主体的合法性，进一步加强了电子政务外网视频子网域的安全性。

##### 集中管理

根据集中管理要求，通过部署视频物联网安全态势感知平台来构建安全管理中心，集防御、检测、分析、响应、持续监测于一体，旨在为用户提供有效的整体安全防护方案。

平台以电子政务外网视频子网域全流量分析为基础，实时监测捕获全网流量数据，结合数据统计、关联分析和大数据挖掘方法，细粒度、多维度及持续地对安全威胁进行实时动态分析，实现对视频物联网的整体感知、以及安全事件的应急处理和溯源分析。

平台面向电子政务外网视频子网域，具备多重分析感知能力：

（1）资产感知：通过对网段内设备的主动扫描和日志分析，发现视频网内活跃的安防设备、网络设备、安全设备、服务器等IP资产。

（2）流量感知：通过对流量数据的协议解析，发现其中的设备取流、视频操作等视频行为。

（3）风险感知：通过风险扫描和日志分析，能够主动发现视频资源存在的脆弱性风险（弱口令、漏洞、配置风险），以及视频资源状态异常（私接、仿冒和掉线）、API接口风险和设备运行风险。

（4）威胁感知：基于检测规则库对资产进行实时监控与流量解析，发现视频网内潜在的威胁事件和基线异常行为。

平台基于全网流量数据，从资产脆弱性、内部异常风险、外部威胁攻击三大维度进行安全监测。同时围绕视频数据安全防御（资产评估、防御攻击）、检测（指纹识别、漏洞检测）、分析、响应（修复、封禁、追查）、持续监测五个维度，形成可持续、可循环的安全防护机制。

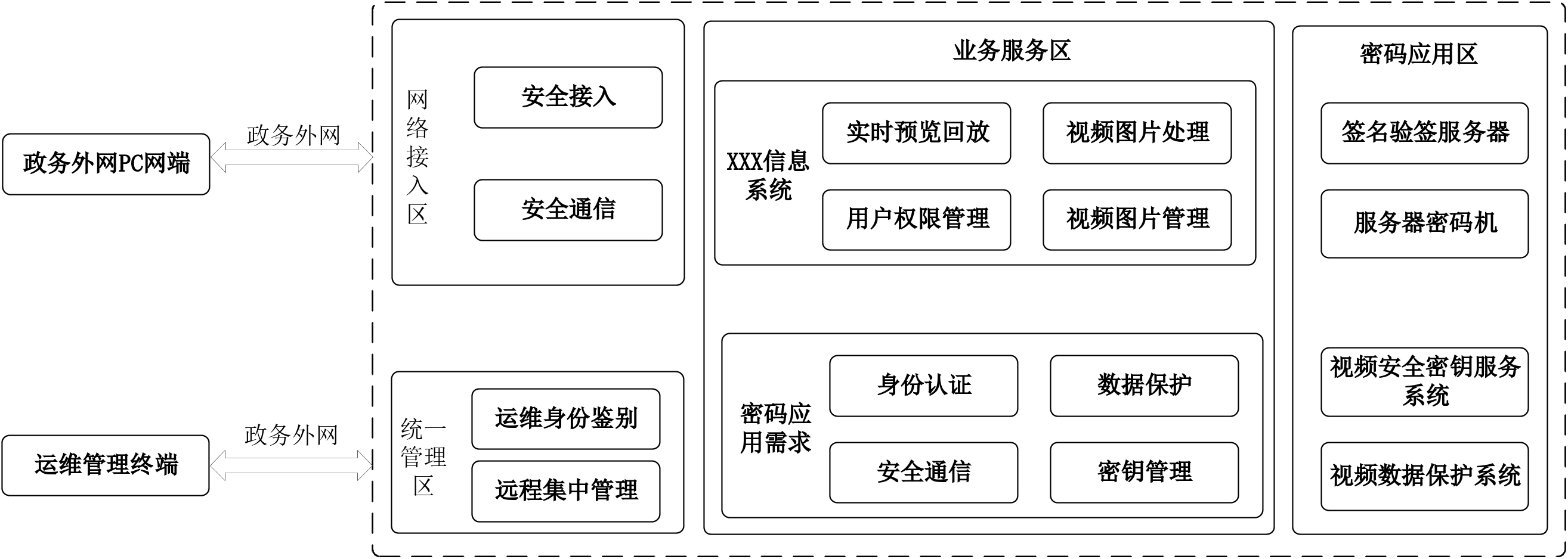
### 密码应用安全建设

*//此部分需根据项目具体的密码应用需求情况进行调整，以下内容供参考。*

为贯彻落实《中华人民共和国密码法》关于信息系统密码应用的要求，结合《国家电子政务建设指导意见》，本方案按照国家信息系统等级保护及密码应用相关安全防护要求对信息系统进行安全防护。依据《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）的第三级别要求，从系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面进行密码应用安全性分析，并设计密码应用方案，以确保本方案系统达到GB/T 39786-2021的要求。

#### 密码应用技术框架

本方案密码应用技术架构如图所示，其中密码应用区是本系统网络拓扑中新增区域，用于部署签名验签服务器、服务器密码机、视频安全密钥服务系统、视频数据保护系统等密码产品，以满足本系统的密码应用需求。



1. 密码应用技术框架图

安全门禁系统：采用密码技术，确定用户身份和用户权限的门禁控制系统。对机房进出人员进行管理，提供基于SM1算法的身份认证方式，提供基于SM2数字签名的密码技术，实现对人员进出记录的完整性保护。

安全视频监控系统：对机房环境进行监控和记录，内置PCI-E密码卡提供基于SM2数字签名或HMAC-SM3，实现对视频监控记录的完整性保护。

多制式统一身份认证网关：采用数字证书为应用系统提供用户管理、身份鉴别、单点登录、传输加密、访问控制和安全审计服务的设备。

VPN综合安全网关：基于SSL/TLS协议，在通信网络中构建安全通道的设备。

视频数据传输加密网关：内置国密TLS协议解析，支持自定义协议转换规则，适配复杂场景下的网关需求，支持视频数据传输加密。

服务器密码机：能独立或并行为多个应用实体提供密码运算、密钥管理等功能的设备。主要为应用系统提供数据加解密、签名验签、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护，同时提供安全、完善的密钥管理功能。

签名验签服务器：用于服务端的，为应用实体提供基于PKI体系和数字证书的数字签名、验证签名等运算功能的服务器。

视频安全密钥服务系统：为视频图片的存储的加解密提供的密钥管理，确保密钥管理全生命周期的合规性、正确性和有效性。

视频数据保护系统：应用统一身份认证，支持视频及抓图文件导出加密和完整性保护。

智能密码钥匙（USBKey）：主要提供签名验签、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书或电子印章等用户数据。本系统中智能密码钥匙（USBKey）存放标识用户身份的数字证书，主要用于对用户身份真实性的鉴别功能。

##### 物理和环境安全

物理和环境安全层面使用的密码算法、密码技术、密钥管理由符合密码相关国家、行业标准的电子门禁系统、视频监控系统、PCI-E密码卡实现。

（1）设计原理

在系统所在机房部署符合国密要求的电子门禁系统以及视频监控系统，并对电子门禁记录数据以及视频监控记录数据进行存储完整性保护。

（2）身份鉴别

针对物理环境的身份鉴别指标，在系统所在机房部署符合密码相关国家、行业标准的电子门禁系统，使用SM1算法进行密钥分散，实现门禁卡的“一卡一密”，并基于SM1算法对人员身份进行鉴别。

（3）电子门禁记录存储完整性

在系统所在机房部署符合密码相关国家、行业标准的电子门禁系统，使用SM2数字签名技术或HMAC-SM3对电子门禁系统进出记录进行完整性保护，其中SM2密钥由密码卡生成，存储在密码卡中，不涉及密钥分发、导入与导出，密钥的备份与恢复、归档和销毁由密码设备管理员负责。

（4）视频监控记录数据存储完整性

在系统所在机房部署符合密码相关国家、行业标准的视频监控系统，使用SM2数字签名技术或HMAC-SM3对视频监控系统视频记录等数据进行完整性保护，其中SM2密钥由密码卡生成，存储在密码卡中，不涉及密钥分发、导入与导出，密钥的备份与恢复、归档和销毁由密码设备管理员负责。

##### 网络和通信安全

网络和通信安全层面使用的密码算法、密码技术、密钥管理由符合GB/T 38636-2020《信息安全技术 传输层密码协议（TLCP）》、GM/T 0025-2014《SSL VPN网关产品规范》、GM/T 0026-2014《安全认证网关产品规范》的安全认证网关；GM/T 0023-2014《视频数据传输加密网关网关产品规范》、GB/T 37092-2018《信息安全技术 密码模块安全要求》二级密码模块要求的SSL VPN网关、视频数据传输加密网关实现。

（1）设计原理

针对跨网络边界的网络通道，部署符合密码相关国家、行业标准的VPN网关类设备，实现网络通信实体的身份鉴别和国密安全传输通道的搭建，保证通信过程中重要数据的机密性以及完整性。

（2）身份鉴别

针对网络层面的身份鉴别指标，采用基于PKI体系的SM2数字证书实现登录人员的身份鉴别，数字证书由通过国家密码局检测认证的电子认证服务商提供证书认证服务或自签发。采用智能密码密钥、VPN安全网关实现登录人员身份认证。

（3）通信数据完整性

通过部署VPN网关类设备，建立安全传输通道。通信过程中，采用国密SSL协议实现登录客户端与服务端之间的密钥协商，采用ECC（SM2）\_SM4\_SM3的SSL算法套件，使用SM3算法实现通信数据的完整性保护。

针对前端感知设备采集过程中的通信数据完整性，通过部署视频数据传输加密网关网关，保证前端感知设备与平台通信过程中数据的完整性。

（4）通信过程中重要数据的机密性

通过部署VPN网关类设备，建立安全传输通道。通信过程中，采用国密SSL协议实现登录客户端与服务端之间的密钥协商，采用ECC（SM2）\_SM4\_SM3的SSL算法套件，使用SM4算法实现通信数据的机密性保护。

针对前端感知设备采集过程中的通信数据完整性，通过部署视频数据传输加密网关，保证前端感知设备与平台通信过程中数据的完整性。

（5）网络边界访问控制信息的完整性

部署VPN网关类设备，对授权访问用户的访问控制权限进行统一管理。采用“组+用户”的授权策略，针对不同用户的角色，划分到不同用户组进行单独的授权管理。VPN网关类设备通过对访问控制授权列表进行SM2数字签名，实现访问控制信息的完整性保护。

##### 设备和计算安全

设备和计算安全层面所使用的密码算法、密码技术、密码服务、密钥管理由符合GM/T 0030-2014《服务器密码机技术规范》、GM/T 0027-2014《智能密码钥匙技术规范》、GM/T 0028-2014《密码模块安全技术要求》的USBKey、服务器密码机实现。

（1）设计原理

设备和计算安全层面涉及的设备包括通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟设备，以及提供相应功能的密码产品。在实际项目设计过程中，主要围绕相应设备运维管理过程中的密码安全。

（2）身份鉴别

针对设备层面的身份鉴别指标，主要通过VPN网关类设备，向运维管理员配发智能密码钥匙（USBKey），由通过国家密码局检测认证的电子认证服务商提供证书认证服务，将SM2数字证书签发到智能密码钥匙中。对登录设备的用户进行双因子认证，实现身份鉴别，防止非授权人员登录。

（3）远程管理通道安全

针对远程管理通道安全指标，主要通过搭建部署VPN网关类设备，搭建运维管理VPN通道，或通过管理口直连等限制远程运维管理方式保证远程管理通道安全。

（4）系统资源访问控制信息完整性

针对系统资源访问控制信息完整性指标，主要通过对系统内部各资源访问控制信息调用密码计算API/SDK的HMAC-SM3消息鉴别码接口，计算HMAC值，并在需要进行鉴权或权限审计时进行验签以确认其完整性，HMAC密钥通过视频安全密钥服务系统保护。

（5）日志记录完整性

针对设备日志记录完整性指标，设备日志统一通过日志审计系统进行日志审计，通过对接调用服务器密码机，对设备日志记录调用密码计算API/SDK的HMAC-SM3消息鉴别码接口，计算HMAC值，HMAC密钥通过视频安全密钥服务系统保护。

##### 应用和数据安全

应用和数据安全层面所要求的密码算法、密码技术、密码服务、密钥管理由符合GM/T 0030-2014《服务器密码机技术规范》、GM/T 0034-2014《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》、GMT 0029-2014《签名验签服务器技术规范》、GM/T 0028-2014《密码模块 安全技术要求》等标准要求的密码模块（二级）、服务器密码机、视频安全密钥服务系统、签名验签服务器等密码产品实现。

（1）设计原理

应用和数据安全层面的设计主要围绕应用本身的登录身份鉴别过程、访问控制过程以及重要数据在传输、存储过程中的安全保护。

（2）身份鉴别

针对应用层面的身份鉴别指标，在互联网、电子政务外网和电子政务外网视频子网域PC端向相关用户配发USBKey，在网络接入区边界部署VPN网关，对互联网、电子政务外网和电子政务外网视频子网域PC端用户进行身份鉴别，防止非授权人员访问应用。

（3）访问控制信息完整性

通过部署签名验签服务器，使用SM2数字签名技术或HMAC-SM3对应用用户访问权限控制列表进行完整性保护，防止应用资源被非授权用户获取。

（4）重要数据传输机密性、完整性

1. 重要数据传输机密性、完整性要求

| 序号 | 重要数据 | 传输机密性 | 传输完整性 |
| 1 | 视频数据 | SM4 | HMAC-SM3 |
| 2 | 图片数据 | SM4 | HMAC-SM3 |
| 3 | 平台鉴别数据 | SM4 | HMAC-SM3 |
| 4 | 平台日志数据 | 不适用 | HMAC-SM3 |
| 5 | 其他业务数据 | SM4 | HMAC-SM3 |

通过国密SSL协议保证数据传输安全。客户端部署支持国密SSL协议的安全浏览器，采用ECC（SM2）\_SM4\_SM3算法的SSL协议，实现https访问，保证数据传输机密性以及完整性；未部署国密安全浏览器的用户，通过部署VPN客户端，实现基于国密SSL协议的安全访问。

重要数据存储机密性、完整性

1. 重要数据存储机密性、完整性要求

| 序号 | 重要数据 | 存储机密性 | 存储完整性 |
| 1 | 视频数据 | SM4 | HMAC-SM3withSM2 |
| 2 | 图片数据 | SM4 | HMAC-SM3withSM2 |
| 3 | 平台鉴别数据 | SM4 | HMAC-SM3 |
| 4 | 平台日志数据 | 不适用 | HMAC-SM3 |
| 5 | 其他业务数据 | SM4 | HMAC-SM3 |

在本系统基础设施区部署视频安全密钥服务系统、视频数据保护系统，在相关设备上部署国产化密码卡，在图片存储过程中，使用SM3算法对图片数据存储的完整性进行保护，实现图片数据防篡改。

在本系统基础设施区部署服务器密码机，应用通过调用服务器密码机，使用SM4算法对登录用户身份鉴别数据、系统中流转的重要数据进行存储机密性、完整性保护，实现身份鉴别数据、重要数据防窃取和防篡改。

（6）密钥管理

本系统无独立的对称密钥管理系统，系统使用的应用系统站点数字证书和电子签章使用的数字证书均由具备资质的电子认证服务机构签发。

本系统选用通过检测认证的VPN综合安全网关、多制式统一身份认证网关、视频数据传输加密网关、USBKey、服务器密码机、签名验签服务器、视频安全密钥服务系统、安全门禁系统、安全视频监控系统等商用密码产品，根据这些商用密码产品提供的安全策略，制定密钥管理方案，并严格遵照该方案进行使用和实施。

#### 密码应用部署

本系统部署和使用了VPN综合安全网关、多制式统一身份认证网关、视频数据传输加密网关、USBKey、服务器密码机、签名验签服务器、视频安全密钥服务系统、安全门禁系统、安全视频监控系统等商用密码产品，均具备相应的商用密码产品认证证书。

#### 密码应用功能模块组成

为实现本系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用功能，需开发适配若干密码应用功能模块。

（1）服务器设备日志/访问控制信息完整性模块

开发服务器设备日志/访问控制信息完整性模块，调用服务器密码机提供的HMAC-SM3功能接口，实现应用服务器、数据库服务器等设备日志/访问控制信息的完整性保护。

（2）用户访问控制信息签名验签模块

开发用户访问控制信息签名验签模块，调用签名验签服务器提供的SM2算法数字签名功能接口，实现应用系统用户的访问控制列表完整性保护。

（3）应用系统重要数据加解密模块

开发应用系统重要数据加解密模块，调用服务器密码机提供的SM4算法加解密功能接口，实现用户身份鉴别数据等重要数据的存储机密性保护。

（4）应用系统重要数据签名验签模块

开发应用系统重要数据签名验签模块，调用签名验签服务器提供的SM2算法数字签名验签功能接口，实现用户身份鉴别数据、业务日志的存储完整性保护。

## 运营维护体系

城市海量的视频资源，需要持续不断开展资源接入、点位治理、事件处置等工作，才能有效发挥视频云中台的价值；同时也需要对平台本身的服务、软件等运行状态进行监测，保障平台持续、稳定、可靠的进行运转，赋能上层感知能力；也需要配套相应的运营维护人员队伍和管理机制，支撑视频云中台的整体运营维护工作的开展。本方案建设涉及到运营管理工作内容如下。

（1）资源接入管理

随着城市的不断建设和发展，视频云中台需要持续开展视频资源的接入工作，需要运维人员能够及时对新的视频点位资源及时接入到视频云中台，并挂载到相应资源目录下面，设置资源的属性、共享权限等信息。

（2）点位信息治理

对接入到平台中的点位资源持续开展治理工作，对点位的基础信息、空间位置、场所分类、业务标签等内容进行持续治理。

（3）智能分析配置

需要运维人员对视频云中台的算法进行管理维护，形成算法管理发布目录，同时根据审批通过的智能分析需求，对视频点位进行具体算法进行编排配置和管理。需优先保障紧急、高等级的智能分析任务得到充分的智能分析资源，需定期对智能分析任务的执行情况进行分析，对异常任务进行及时维护。

（4）感知预警研判

对应平台产生的大量智能感知事件，对于需要进行人工审核的事件，则由运维人员继续基本准确情况的判断，是真实事件则进行推送分发出去，属于误报或者不确定的事件则不进行推送分发，保障平台推送出去的事件是真实可靠的。

（5）日常维护管理

对平台进行基础管理维护，包括用户、角色和资源权限的管理分配，同时对平台组件进行运行监控与问题排查，及时发现和解决问题，为整体平台提供有力的后台保障。实现对城市视频资源的状态、图像质量等情况进行综合监测，并定期输出资源整体情况统计分析报告。

（6）算法训练管理

需要统一汇聚、受理各委办局上报的视频算法模型训练需求，对各委办局汇总的图片素材进行高效管理，并按委办局应用场景需求，对图片素材进行标注，并通过算法训练平台进行模型训练、测试和上传，并对算法的版本和迭代进行持续跟进，保障算法模型的可靠和高效。

### 运营维护队伍建设

考虑视频领域的专业性，需要构建一支专业的运维管理队伍，构建起专业的城市视频资源的运行监测、维护管理、事件处置等工作，保障城市视频资源的持续可用性，最大限度让视频资源持续发挥价值。运维队伍中需要包括具备下角色人员。

（1）资源接入管理人员

负责日常视频资源的接入、资源目录的管理发布等维护工作。该角色在初期完成各类视频平台接入之后，后续的接入和管理工作将会较少，但偶尔会有视频资源的接入维护工作。

（2）点位资源治理人员

负责视频点位的基础信息、空间信息、场所分类、业务标签等内容的治理，初期接入大量的视频资源，治理工作量会较大，但后续会随着视频的持续接入，也需要配套做相关点位的治理工作任务。

（3）算法编排管理人员

需要运维人员对视频云中台的算法进行管理维护，形成算法管理发布目录，同时根据审批通过的智能分析需求，对视频点位进行具体算法进行编排配置和管理。需要该人员具体一定的智能算法认识和基础，同时对视频云中台的算法管理、算法编排等功能十分熟悉。负责视频云中台智能分析任务的日常管理维护工作，包括智能任务的新建、维护、启用、停用、运行分析等工作。

（4）智能预警研判人员

负责对视频产生的各类智能感知事件进行人工审阅，判断事件是否真实、有效，该角色日常工作量会比较大，随着算法、场景、编排等逐步优化，事件处理的工作量会逐步较少，但该角色需要一直存在，保障视频云中台智能解析中心输出事件的有效。

（5）日常维护管理人员

负责平台基础的各类配置管理、权限分配、软硬件的运行监测、问题排查处理，是保障视频云中台的稳定、可靠、持续运行的关键角色。

（6）算法训练管理人员

负责基于各类外部用户的算法训练需求汇聚和响应，基于提供的图片进行特征标注，并利用算法训练平台进行模型训练，生成特定作用的算法模型，并持续对算法模型进行管理和优化。

### 运营维护机制建设

针对城市视频资源和能力构建统一的视频相关运营维护管理机制，围绕城市视频资源的管理、应用、维护等过程，构建起完整的工作规范，高效保障城市资源的持续、可靠运转。

（1）智能事件处置

运维人员需通过事件处置功能，对平台产生的视频智能事件进行及时审阅处理，保障智能事件能够得到及时的推送和分发，保障视频云中台的建设成效。对于紧急类事件需要实时进行处理，对于一般类事件则需尽快进行处理，一般类事件如果已经过了时效，则可以不进行推送，如果判断事件还有效，则需要推送。

（2）维护响应时间

维护相应时间包括故障级别定义和故障响应时间两个方面，具体要求可以结合项目情况进行调整。

故障级别定义如表22所示。

1. 故障级别定义

| 级别 | 故障级别 | 系统症状 |
| --- | --- | --- |
| A | 紧急 | 系统出现严重问题，无法正常进行。造成安全事故和损失。 |
| B | 关键 | 系统出现问题，但关键业务可以使用。可能造成安全事故和给客户造成损失。 |
| C | 较严重 | 系统基本正常，偶尔出现非致命性错误，业务基本不受影响。 |
| D | 一般 | 轻度影响功能或性能，或操作不方便。 |
| E | 轻微 | 不影响产品的功能，但性能偏慢，或操作界面不够友好。 |

故障响应时间如表23示。

1. 故障响应时间

| 级别 | 电话响应时间 | 恢复时间 | 现场响应时间 |
| --- | --- | --- | --- |
| A | 7\*24小时 | 半小时内 | 1小时； |
| B | 7\*24小时 | 半小时内 | 1小时 |
| C | 5\*8小时 | 1小时内 | 2小时 |
| D | 5\*8小时 | 2小时内 | 3小时 |
| E | 5\*8小时 | 2小时内 | 4小时 |

（3）运行异常上报

运营维护人员在日常运维过程，如果发现了有影响到整体视频云中台正常运行的事件或者情况，需要及时向用户进行反馈和汇报，并和用户沟通处置方案，及时进行响应的处理和调整，将影响降低到最低。

（4）运维信息安全

1）运维工作人员不得捏造数据、弄虚造假；

2）不得私自将数据以任何方式泄露给他人；

3）不得因私查看、下载、修改视频录像；

4）不得在公共场合谈及数据内容；

5）不得私自将用户名密码等信息泄露给他人；

6）不得将未授权设备接入系统；

7）不得私自通过手机、DV、照相机等设备翻录视频；

8）违反上述信息安全要求的按情节严重性给予批评教育、行政处罚、解除劳动合同、追究刑事责任等。

## 标准规范体系

城市视频相关标准规范也是视频云中台构建过程中不可缺少的部分，只有制定形成统一、完善、规范的相关技术标准规范，才能保障视频云中台的作用和成效持续发挥。

城市视频云中台体系的标准规范体系，包含相应的技术标准、管理规范、流程制度等。

根据平台业务开展需要，提供包括视频资源接入、资源管理、资源服务等技术规范。

根据业务需要，协同业主完成视频云中台相关管理规范与流程规范编制。