

## 第六章 采购需求

### 1. 项目概况

本项目为裕安区城市大脑公共场所视频监控资源整合共享项目。

按照“统一整体规划、统一建设运维、统一平台共享、统一技术标准、统一监督管理”的原则，结合六安市裕安区实际，以“规范化、智能化、精细化、全域感知、全网共享、全时响应、全程可控”为目标，开展公共安全视频资源建设，加强视频资源分级分类治理，促进视频资源共享及融合应用，提升社会治理能力，逐步形成公共视频资源建设、治理、共享和应用的完整体系。

### 2. 技术要求

#### 2.1. 建设内容

按照《关于深化全省公共场所视频监控资源整合共享工作的指导意见》、《关于深化全市公共场所视频监控资源整合共享工作的指导意见》、《裕安区城市大脑可行性研究报告》文件精神，本项目主要建设内容包括以下五大部分：

##### （1）前端感知设备及网络

针对现有重复点位资源整合 6 处监控点位；针对政府部门和单位的过保（超过 5 年）设备，更新前端视频监控摄像机 233 台；针对委办局新建需求，新建前端视频监控资源 74 路。为了更好地实现公共场所视频监控资源整合，新建整合域和互联网、整合域和公安视频专网之间、与六安市社会视频资源整合平台上联专线 3 条，六安云计算中心至各委办局间的专线 47 条，租赁至各单位（小区等）互联网线路 261 条。

##### （2）视频监控基础平台

利旧裕安区现有的视频分析平台作为六安市社会视频资源整合平台裕安区前置平台（以下简称裕安区前置平台），作为市社会视频资源整合平台的前置接入汇聚节点，两者共同构成市、区统一的社会资源整合平台。裕安区前置平台

整合六安公安视频图像信息应用平台（雪亮工程平台）推送的裕安区公安分局自建视频资源，并对现有平台进行优化使其具备整合全区公共场所视频监控资源的功能和性能。裕安区前置平台，整合汇聚各单位建设的公共场所视频监控资源，实现各级政府机关、各单位已建设待整合公共场所视频监控资源的统一接入，前置汇聚整合后统一推送至筹建中的六安市级社会视频资源整合平台，并同步考虑通过安全边界推送至六安公安视频图像信息应用平台（雪亮工程平台）作为备选路径。同时，考虑到裕安区有大量的小区、水厂等单位的监控资源未进行整合，在互联网接入相关单位的已建视频监控资源进行汇聚后通过安全手段推送至整合域。

同时，裕安区前置平台相关视频数据资源应同步接入裕安区城市大脑。

根据裕安区社会治理需求，落地闭环四类视频场景算法应用。

### **（3）运维管理**

为保障裕安区公共场所视频监控资源整合共享运行维护工作的质量和效率，制定相对完善、切实可行的运行维护管理制度和规范，确定各项运维活动的标准流程和相关岗位设置等。

### **（4）安全管控**

本项目安全管控主要建设内容如下：

完成整合域与公安视频网的安全互联，实现数据资源和视频资源的共享；按照《GA/T 1788.3-2021 公安视频图像信息系统安全技术要求 第 3 部分：安全交互》要求，建设整合域与公安视频网之间的横向边界交互平台，实现整合域与公安视频网数据资源和视频资源的交互共享。

完成整合域与互联网的安全互联，并对互联网进行安全防护；按照《GA/T 1788.3-2021 公安视频图像信息系统安全技术要求 第 3 部分：安全交互》要求，建设整合域与互联网之间的横向边界交互平台，实现整合域与互联网上视频资源 and 数据资源交互。

对整合域进行安全防护。在整合域部署网络防病毒、内网安全与补丁管理系统、入侵检测、准入控制与违规外联监测系统、漏洞扫描、日志审计、运维堡垒机、视频应用安全审计系统、边界安全运维审计系统等安全设备，依照等级化保护进行安全防护体系设计与实现，保证视频传输网中传输数据信息的安全性、完整性、真实性及抗抵赖性，形成事前防护，事中安全检测，事后审计

取证于一体的安全防护体系，达到实体安全、应用安全、系统安全、管理安全，以满足公共场所视频监控资源整合共享安全防护要求，保障核心区域业务安全。

### **(5) 存储**

为支撑视频监控基础平台高效稳定运行，搭建基础云平台、云计算系统，其中按可信云要求配置管理/应用及解析服务器，并配置 12.2PB 视频云存储容量，作为市级平台的前置节点，设置在视频专网；并在六安云计算中心租赁 12 个标准机柜。

## **2.2. 项目背景**

### **2.2.1. 项目的背景和依据**

#### **(1) 加快整合，做到应整尽整**

全面梳理已建公共场所视频监控资源的数量、位置、型号、应用等，形成目录式、表格化资源清单。制定公共场所视频监控资源整合方案，做到应整尽整，推动重复建设清零，对场景、功能重复的前端监控设备，通过一机多用、以迁代拆、以租代建、杆塔复用、算法升级等方式，优化点位布局，充分发挥存量视频监控资源效能。

#### **(2) 加快接入，做到应联尽联**

政府投资建设的公共场所视频监控资源应无条件接入本级“雪亮平台”，暂不具备接入技术条件的，充分论证系统升级改造的成本后确定是否接入。行业监管部门应落实监管主体责任，推动行业监管领域企事业单位等自建的公共场所视频监控资源接入，消除“孤岛”。

#### **(3) 严格审批，规范建设模式**

公共场所视频监控类项目应按程序统一立项审批，未经批准的不得建设。落实公共场所视频监控类项目“双把关”审核机制，由各级数据资源管理部门和公安部门共同依据公共场所视频监控资源建设规划对项目进行审核，按照政府投资及政务信息化项目管理相关办法全流程监督管理。鼓励以政府购买服务方式集中统一实施。

#### **(4) 扩充能力，加快共享应用**

以应用需求为导向，优化平台视频接入、传输、处理、转发和计算能力，提升裕安区前置平台视频共享能力。建立“按需共享、授权使用”的机制，各部门提出共享应用需求，按程序审核同意后，进行公共场所视频监控资源共享。

#### **(5) 落实责任，确保数据安全**

按照国家有关法律法规要求，建立数据安全管理机制，落实各相关方安全责任，确保公共场所视频监控数据安全，防止发生公共场所视频监控信息被滥用、泄露或被控制等安全事件。加大公共场所视频监控安全技术措施保障力度，加强网络安全传输、系统安全保障、重要信息安全管理等技术手段建设，提升安全可控水平。

### **2.2.2. 公共场所视频监控建设现状**

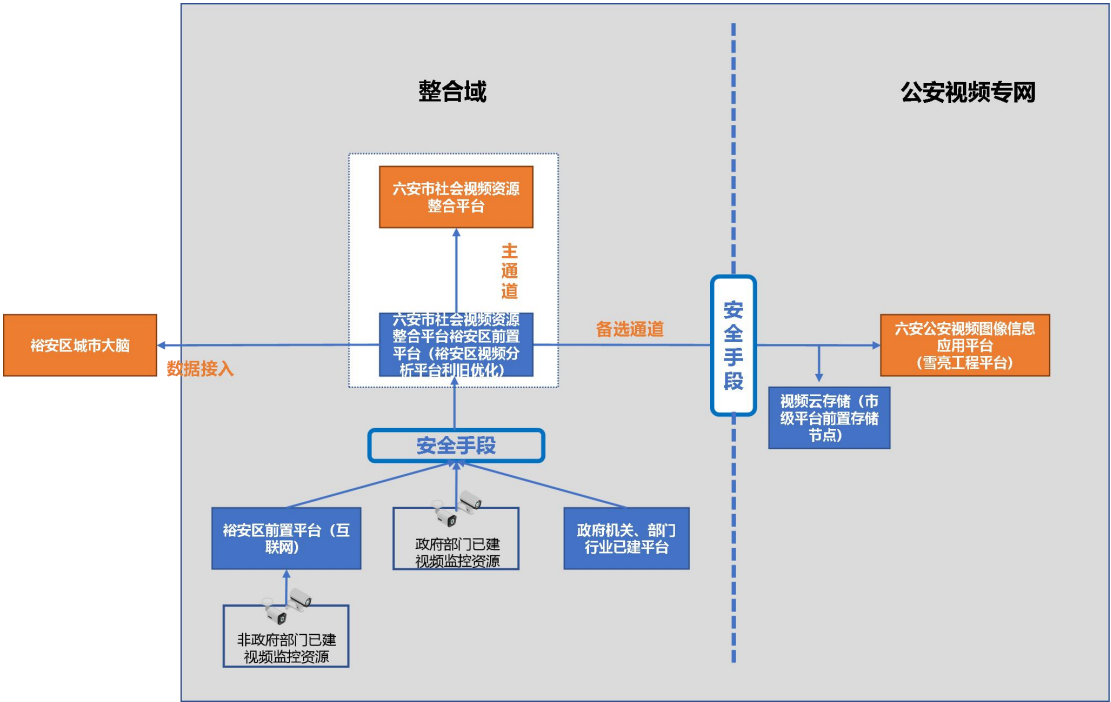
裕安区公共场所视频监控资源存在着前端感知设备老化、网络形式复杂、缺少汇聚整合平台、视频应用不足、运维管理无序、安全管控缺失等问题，需要通过本项目进行系统改造提升。

## 2.3. 架构要求

### 2.3.1. 总体系统架构要求

公共场所视频监控资源整合共享是以视频为核心的基础能力开放平台，基于云计算、云存储、人工智能、大数据等先进技术进行构建，按照统一整体规划、统一技术标准、统一建设运维、统一平台共享、统一监督管理“五统一”的建设思路，推进全区公共区域视频监控建设一体化，实现“最大化集约建设、最大化节约成本、最大化提升效率、最大化安全应用”，通过统一门户为外部用户提供视频赋能、AI 赋能、数据赋能和应用赋能，为多跨应用场景提供可视化、智能化的高质量支撑服务。

遵循安徽省全省公共场所视频监控资源整合共享的要求，按照“应整尽整、逐步推进”的原则，对裕安区全域的公共场所视频监控资源进行整合共享，总体架构如下所示：



六安市裕安区公共场所视频监控资源整合共享逻辑架构图

#### (1) 整合域

利旧裕安区现有的视频分析平台作为六安市社会视频资源整合平台裕安区前置平台（以下简称裕安区前置平台），作为市社会视频资源整合平台的前置接

入汇聚节点，两者共同构成市、区统一的社会资源整合平台。裕安区前置平台整合六安公安视频图像信息应用平台（雪亮工程平台）推送的裕安区公安分局自建视频资源，并对现有平台进行优化使其具备整合全区公共场所视频监控资源的功能和性能。裕安区前置平台，整合汇聚各单位建设的公共场所视频监控资源，实现各级政府机关（重点实现市辖区外，乡镇、街道等单位的视频资源接入）、各单位已建设待整合公共场所视频监控资源的统一接入，前置汇聚整合后统一推送至筹建中的六安市级社会视频资源整合平台，并同步考虑通过安全边界推送至六安公安视频图像信息应用平台（雪亮工程平台）作为备选路径。其他政府部门需建设个性化视频综合应用，可申请裕安区前置平台视频接口服务进行调用。同时，考虑到裕安区有大量的小区、水厂等单位的监控资源未进行整合，在互联网接入相关单位的已建视频监控资源进行汇聚后通过安全手段推送至整合域。

裕安区前置平台通过通用存储资源池具备按需配置的流式存储能力，通过视频接入管理服务提供各类视频资源的接入、管理服务，包括本地视频资源、联网视频资源。本地视频资源主要通过设备 SDK、GB/T28181、ONVIF、EHOME 等多种协议方式接入；联网视频资源则通过平台级联的方式，支持通过国标协议或者平台 SDK 的方式进行联网接入。

同时，裕安区前置平台相关视频数据资源应同步接入裕安区城市大脑。

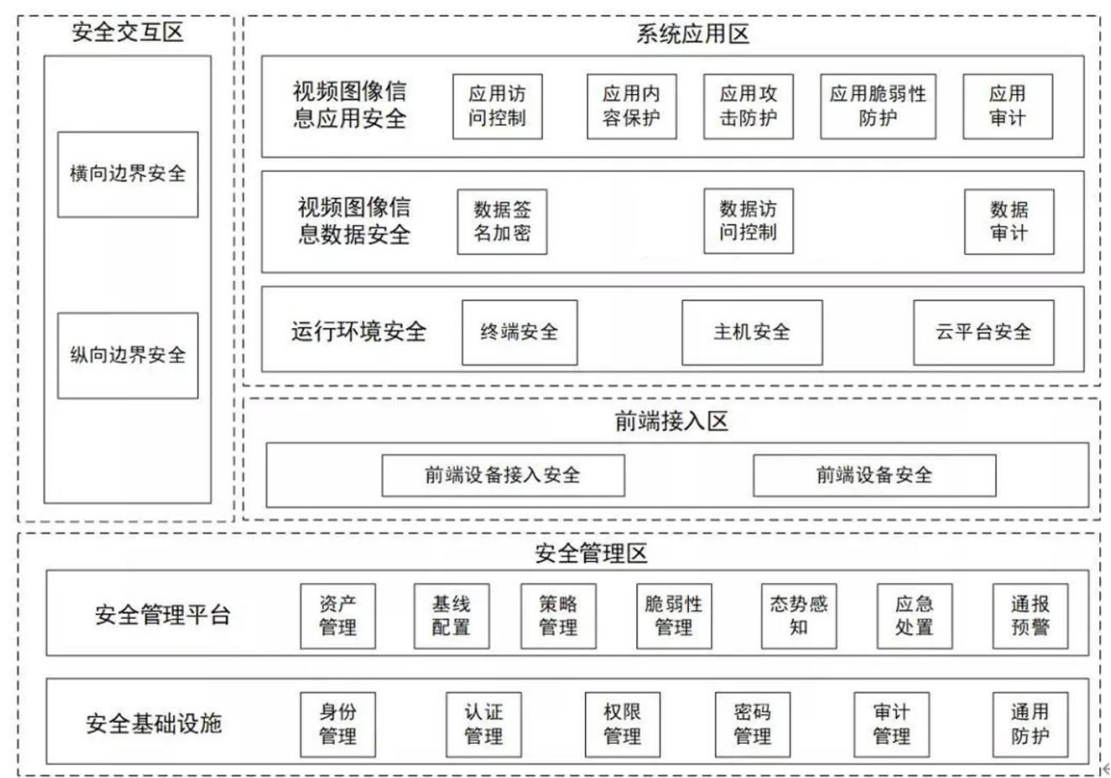
## （2）视频专网

六安公安视频图像信息应用平台（雪亮工程平台）由六安市公安局统筹建设，已经汇聚全市公安自建公共场所视频监控资源。本项目对裕安区公共场所视频监控资源整合后通过安全边界实现整合域和视频专网的资源共享。

在视频专网建设视频云存储作为作为市级平台的前置节点。

### 2.3.2. 总体安全架构要求

公安视频图像信息系统应从前端安全，边界/接入安全（包括横向边界安全和纵向防护安全）、运行环境安全、视频图像数据安全、视频图像应用安全、安全管理平台、安全基础设施等维度构建安全技术总体框架。



总体安全架构图

(1) 安全检测

针对系统的数据交互进行实时检测，发现入侵行为、恶意代码、高可持续威胁、未知代码与程序并进行分析与虚拟执行，当研判为威胁时联动防御系统阻断。同时将运行情况上报管理平台展示分析。

(2) 安全防御

针对系统数据交互进行严格控制。阻断不允许的访问；阻断入侵行为数据和恶意代码；阻断基于 web 架构的应用系统攻击；阻断终端的非法外联；阻断移动介质的非法接入；阻断 Ddos 攻击等。同时将运行情况上报管理平台展示分析。

(3) 安全审计

针对系统的安全设备、网络设备、服务器设备、边界等运行维护信息及网络流量信息进行长期记录与统计，保障记录不可随意删除。同时将运行情况上报管理平台展示分析。

(4) 安全管理

针对安全设备、网络设备、服务器设备、边界等进行统一管理，执行策略下发与远程配置。收集防御、检测、审计设备发送的日志进行存储、建模分

析、可视化展示、风险预警。同时通过安全拓扑、运行监控、工单管理、报表管理、合规管理等模块进行安全运维。

## 2.4. 前端感知设备及网络建设要求

### 2.4.1. 前端感知设备建设要求

本着“应整尽整，统筹共建，应联尽联，充分共享”的思路，对场景重叠、机箱重复、杆件重复等问题点位进行排查，做到应整尽整，推动重复建设清零。通过一机多用、一机多摄、以迁代改、搭杆复用等方式，对公共视频监控点位进行布局优化，整合已有链路资源，拆并重复设备，改造升级老旧设备，移位利旧重复设备，摸排整改安全隐患设备设施，提升公共视频监控资源复用率和有效率。

#### （1）整合原则

可视范围重叠且功能重复的监控，以及监控有效抓拍范围内类型重复的杆件，均以性能优、年限近者保留，多余设备、杆件拆除；过保且不在线的监控，以及老旧且未安装监控的杆件，考虑统一拆除。

#### （2）改造原则

前端为老式模拟摄像机的，改造为数字摄像机；前端机箱功能存在缺陷的，改造为新机箱；现有杆件存在安全隐患的，改造为新杆件。

#### （3）接入原则

对于未接入公安视频专网的政府投资建设的视频监控资源，具备接入条件的全量接入，不具备接入条件的，经充分论证改造成本后确定是否接入；非政府投资建设的视频资源，具备接入条件的全量接入，不具备接入条件的非必要可不接

本项目需实现对下面汇总表中各单位视频资源的整合，参照《公共安全重点区域视频图像信息采集规范（GB 37300-2018）》中关于采集部位的界定，实现对重点公共区域和重点行业、领域的覆盖，目前统计约为 40932 路视频需实现整合，除去已接入公安雪亮平台的 5000 路，还需本项目整合 35932 路。还需本项目整合的 35932 路公共场所视频监控中有 6890 路（覆盖一览表中序号 1 至 20）为重点部位和场景视频，需对其按照 30 天标准进行统一存储。



如在上述范围外涉及到各单位整合或新建需求，本项目应予配合。

裕安区公共场所视频监控对重点公共区域和重点行业、领域覆盖一览表

序号	采集部位		覆盖数量	其中已接入公安雪亮平台数量	本项目还需整合数量
1	重点公共区域	凯旋国际广场、金外滩广场、街道文化广场、绍虞广场、石湖广场、信德时代广场、紫竹禅林寺广场、淠河文化墙广场、北塔公园广场、中大财富广场、周谷堆美食广场、红达广场等具有政治历史意义、经常性举办重大群众性集会、商业服务、文化宣传、宗教活动等公共活动的露天广场的主要区域、周边重要路段、路口	19	10	9
2		城市、乡镇主要路段、路口、立交桥，城市地下人行通道、隧道、过街天桥等主要通行区域	1093	600	493
3		高速公路、国道、省市县际、城镇道路主要出入口、卡口、公安检查站、收费站通道、高速公路服务区	44	30	14
4		大型桥梁、隧道主要通行区域	24	20	4
5		城镇商业金融聚集区主要出入口、周边主要路段、路口	109	60	49
6		民用机场、铁路车站、港口、码头、长途汽车站等场所外的露天广场主要区域、重要通道、周边路段、路口	262	200	62
7		城市轨道交通车站周边路段、路口	0	0	0
8		城市普通道路路段、路口，及一般单位出入口及采集的图像能够覆盖到单位外围一定范围的部位	6981	2295	4686
9	重点行业、领域涉及	党政机关：单位主出入口及采集的图像能够覆盖到单位外围一定范围的部位	354	280	74
10		民用机场、铁路车站、港口、码头、城市轨道交通车站及列车、长途汽车站、城市公共汽电站、加油(气)站等：民用机场航站楼安检区以外开放区域	268	200	68

序号	采集部位		覆盖数量	其中已接入公安雪亮平台数量	本项目还需整合数量
	公共区域	和航站楼周边区域的人员聚集部位；铁路车站、港口的出入口、售票大厅、候车大厅等开放区域的人员聚集部位；城市轨道交通列车及车站出入口车站通道、安检区、车站站厅、站台等开放区域；长途汽车站的出入口、售票大厅、候车大厅等开放区域的人员聚集部位；城市公共汽电站区及周边一定范围；加油(气)站车辆出入口、服务区			
11		银行营业场所等金融机构：营业网点、自助网点主出入口及其外部一定区域，运钞交接区营业大厅	17	15	2
12		寄递单位、物流园区等：寄递单位营业场所主出入口、营业大厅交寄接收区，物流园区主出入口	9	6	3
13		电力、电信、广电、油气、水利等行业：重点单位周边一定区域、重点线路沿线	119	90	29
14		大型商贸中心和大型农贸市场等：单位主出入口、营业场所人员聚集部位、运钞交接区及押运通道	109	70	39
15		学校、幼儿园等教育单位：单位主出入口及其外部一定区域	1140	298	842
16		医院：医院主出入口、挂号大厅、候诊大厅等开放区域的人员聚集部位及采集的图像能够覆盖到单位外围一定范围的部位	1174	733	441
17		歌舞娱乐厅、电子游戏厅、互联网上网服务营业场所等场所：场所出入口及采集的图像能够覆盖到场所外围一定范围的部位	54	30	24
18		旅馆业、洗浴中心：宾馆、酒店等旅馆业营业场所及洗浴中心的主出入口、大厅、前台及采集的图像能够覆盖到场所外围一定范围的部位	5	3	2
19		展览场馆、大型文化、体育场所和其他大型群众性活动举办场所等：活动场所的出入口安检区、室外人员聚集区域(部位)	29	20	9

序号	采集部位		覆盖数量	其中已接入公安雪亮平台数量	本项目还需整合数量
20		旅游景区：旅游景区主出入口、人员聚集区域(部位)	80	40	40
21		（党政机关、学校、小区）内部主要部位	29042	0	29042
合计（序号 1-21 之和）			40932	5000	35932
其中重点部位和场景（序号 1-20 之和）			11890	5000	6890

六安市裕安区视频资源整合汇总表

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间（天）	网络类型	平台描述	建设时间	前端点位数
1	文旅局-横排头景区	全市旅游视频管理平台	华为	是	7	运营商-移动	管理 4A 级景区出入口视频	——	20
2	文旅局-独山革命旧址群	视频监控系統	大华	是	15	运营商-电信	管理 4A 级景区出入口视频	2020.11	39
3	文旅局-独山革命旧址群	视频监控系統	——	——	7	运营商-电信	游客中心	——	18
4	市场监管局	裕安区市场监督管理局食品	大华	是	20	数据专网	管理辖区主要生产企业、餐饮单位、流通单位主要部位视频远程监控	2021.03	823

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
		安全智慧监管平台							
5	教体局	裕安校园联网项目	大华 DH-ICC-B8900-U	——	——	网络设备建立 VPN 隧道	——	2021.12	10475
6	生态环境局	裕安区环境保护局视频监控监控系统	海康威视 DS-8832N-K8	是	——	局域网	——	2017.05	79
7	民政局	裕安区民政局办公楼视频监控系统	大华 DH-NVR4432	是	——	局域网	内部监控	2016	16
8	卫健委	——	——	——	——	——	——	——	441
9	裕安区妇幼保健院	智慧园区视频管理平台	V3 版本平台 / 大华型号服务器	是	15	局域网	裕安区妇幼保健院公共场所视频	2020.03	714

序号	建设单位	平台名称	平台厂商	是否符合GB/T 28181	存储时间(天)	网络类型	平台描述	建设时间	前端点位数
10	税务局	六安市裕安区地税办税服务用房智能化系统	科达	是	——	局域网	覆盖局主要办公场所	2015.11	55
11	融媒体中心	——	——	——	——	——	——	2020.03	33
12	机关事务管理局	六安市裕安区政府视频监控	海康威视DS-7816	是	10	局域网	裕安区政府内部	2018.03	64
13	火车站	六安火车站出站口疫情防控视频监控	海康威视	是	50	电信互联网	火车站出站口疫情防控视频监控	2020	15
14	火车站	六安火车站站	海康威视	是	50	电信互联网	火车站站前路综合执法视频监控	2022	10

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
		前路综合执法视频监控系统							
15	退役军人事务局	退役军人事务局大厅视频监控系统	大华 DH-NVR104HC-P-HDS3	是	——	局域网	大厅监控	2020.01	2
16	区残联	区残联办公区域监控	海康 DS-7808NVR	是	15	局域网	内部监控	2016.03	6
17	工企改制中心	办公区域监控	海康威视 7804N-F1	是	——	局域网	办公区域监控	2021.05	5
18	征收办	裕安区土地和房屋征收管理处视频监控	大华 /DH-NVR4432-HDS2	是	30	局域网	管理处办公室公共区域安全监测	2019.11	48

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
		控系统							
19	公安分局	公安视频图像信息应用平台 (雪亮工程平台)	海康	是	30	公安视频专网	公安视频监控	2021.12	5000
20	住建局	六安市建设工程远程视频监控服务系统项目平台	大华	是	30	中国联通互联网专线	住建工地及搅拌站现场监测	2017.1	220
21	城管局	——	——	——	——	——	——	——	21879
22	交通局	裕安交通大厦监控系统	海康 DS-7732N-E4	是	——	局域网	内部监控	2013.03	78

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
23	交通局-交通信息中心	省部共建治超联网信息管理系统	安徽省联通公司	——	90	专线	治超联网数据上传和视频监控上传	2013/2021	27
24	水利局	淠河治理工程裕安区段管理设施护堤房配套工程	大华	是	30	互联网	管理河道日常情况	2022.03	20
25	水利局-裕安水厂	裕安水厂视频监控系统	海康威视 DS-8616N-I8	是	30	局域网	水厂监控	2019.12	16
26	水利局-分路口水厂	分路口水厂视频监控系统	海康威视 DS-8616N-I8	是	30	局域网	水厂监控	2019.12	16
27	水利局-徐集水厂	徐集水厂	海康威视 DS-	是	30	局域网	水厂监控	2019.12	16



序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
		视频监控 系统	8616N -I8						
28	水利局-钱集 水厂	钱集 水厂视 频监 控系 统	海康威 视 DS- 8616N -I8	是	30	局域 网	水厂监控	2020.12	16
29	水利局-陶洪 集水厂	陶洪 集水 厂视 频监 控系 统	海康威 视 DS- 8616N -I8	是	30	局域 网	水厂监控	2020.9	16
30	公管局	海康 4200 单机	海康威 视 CVR DS- A8062 4S	是	90	局域 网	内部监控	2020.11/ 2021.11	22
31	平桥乡	平桥 乡政 府大 院视 频监 控系 统	DS- 7804N -F1 / DS- 7808N -F1 / DH- NVR2 216- HDS3/ DH-	是	100/ 20/1 5	局域 网	内部监控	——	20

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
			NVR2108HC-HDS2						
32	城南镇	市容市貌管理平台	电信云平台	是	30	电信网络	管理重点道口市容市貌视频	2022.05	41
33	城南镇	政府内部视频平台	DS-7932N-E4 硬盘录像机设备自带	是	30	局域网	管理政府内部视频	2016.06	26
34	城南镇	政府大院视频平台	DS-7816N-R2 硬盘录像机设备自带	是	30	局域网	管理政府大院视频	2021.05	13
35	青山乡	青山乡政府内部监控	——	是	——	——	内部监控	2019.01	30
36	苏埠镇	政府大楼	大华	是	30	互联网	政府一楼、二楼出入口	2017.03	2
37	苏埠镇	食堂	TP	是	7	互联网	食堂大厅	2017.03	1
38	石板冲乡	石板冲乡政府	天视通	是	30	移动网络	区域监控	2021.11	14

序号	建设单位	平台名称	平台厂商	是否符合GB/T 28181	存储时间(天)	网络类型	平台描述	建设时间	前端点位数
		视频监控 系统							
39	石板冲乡	综治中心 视频监控 系统	天视通	是	——	移动 网络	区域监控	2022.08	2
40	韩摆渡镇	世友视频 监控系统	世友 32nvr	是	——	局域 网	内部监控	——	25
41	分路口镇	分路口镇 行政服务 中心安防 监控系统	宇视 NVR 304- 32S- DT	是	30	局域 网	内部监控	2020.04	24
42	狮子岗乡	狮子岗乡 乡政府政 府大楼内 部监控	雄迈 MN31 09B VO	是	30	政府 内部 外网	政府大楼办公 区域安防设施	2021.09	22
43	独山镇	视频 监控 系统	大华 DH- NVR4	是	15	局域 网	内部监控	2016.06	13

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
			432						
44	西河口乡	西河口乡政府政府大楼内部监控平台	雄迈 MN3109B VO	是	30	接入政府内部外网	政府大楼办公区域安防设施；政务大厅办公区域安防设施；路口安防设施。	2020.03	21
45	石婆店镇	石婆店镇政府内部视频监控系统	海康 7816-K8	是	30	局域网	——	2019.05	61
46	徐集镇	徐集镇政府视频监控系系统	联想 海康威视 32 路硬盘录像机 DS-7932N-R4	是	30	局域网	——	2022.03	20
47	江家店	江家店镇政府监控系统	宇视 NVR-B100-E4@16	是	30	局域网	内部监控	2017.12	11
48	罗集乡	——	——	是	——	局域网	——	2022	10

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
49	顺河镇	——	——	——	——	——	——	——	1
50	固镇	视频监控 系统	海康版本平台 /DS-8832N-R8 型号 NVR	是	——	局域网	——	2022.06	26
51	单王乡	数字乡村 平台	中维世纪	是	7	互联网-电信网	每个村主要路口	2020.03	17
52	丁集镇	政府内部 视频监控	电信赛达	是	15	局域网	管理政府内部 出入视频	——	3
53	鼓楼街道	鼓楼街道 视频监控 系统	海康威视 DS-7816N-K2(D)	是	12	未联网	——	2020.11	10
54	鼓楼街道	月亮岛社区 视频监控 系统	海康威视 DS-7816N-K2(D)	是	12	未联网	——	2015.09	1
55	鼓楼街道	大田拐社区 视频监控	海康威视 SDIPC 5081-	是	12	未联网	——	2018.09	2

序号	建设单位	平台名称	平台厂商	是否符合GB/T 28181	存储时间(天)	网络类型	平台描述	建设时间	前端点位数
		控系统	1R-F(B)						
56	鼓楼街道	锥子庙社区视频监控系统	海康威视 SDIPC 5081-1R-F(B)	是	12	未联网	——	2018.09	2
57	鼓楼街道	小东街社区视频监控系统	海康威视 SDIPC 5081-1R-F(B)	是	12	未联网	——	2018.09	2
58	小华山街道	小华山街道办事处及文化站视频监控系统	海康 DS-7108N-F1	是	10	局域网	大厅及大门前部分区域	2019.07	14
59	小华山街道	小华山街道园艺场社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
60	小华山街道	小华山街道十里岗社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
61	小华山街道	小华山街道华府社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
62	小华山街道	小华山街道和顺社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
63	小华山街道	小华山街道恒生社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
		统							
64	小华山街道	小华山街道天盈社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
65	小华山街道	小华山街道春江社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
66	小华山街道	小华山街道河滨社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
67	小华山街道	小华山街道六梅路社区视频	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2



序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
		监控系统							
68	小华山街道	小华山街道香樟社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
69	小华山街道	小华山街道江南社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
70	小华山街道	小华山街道政务社区视频监控系统	海康威视 ISC	是	——	互联网	办事大厅	2020.01	2
71	新安镇	电信小翼管家	中国电信	是	——	互联网 (中国电信)	新安镇人民政府办公楼内部楼道和淠河河道监控	2021.03	18

序号	建设单位	平台名称	平台厂商	是否符合 GB/T 28181	存储时间 (天)	网络类型	平台描述	建设时间	前端点位数
72	西市街道	西市街道办事处视频监控系统	海康 DS-7932N-R4 型号 NVR	是	25	局域网	——	2021.07	47
73	西市街道	凤凰桥社区新时代文明实践站视频监控系统	大华 DH-NVR4432 型号 NVR	是	30	局域网	——	2022.1	25
74	西市街道	紫竹林社区视频监控系统	型号 NVR7916N-R4	是	60	局域网	——	2021	14
75	西市街道	西市街道南门社区视频监控系统	海康 32 路硬盘录像机	是	10	局域网	——	2020.03	20
76	高新区	六安高新	曙光	是	30	中国联	实现“两园一中心”物业监	2022.06	150

序号	建设单位	平台名称	平台厂商	是否符合GB/T 28181	存储时间（天）	网络类型	平台描述	建设时间	前端点位数
		技术产业开发区智慧园区				通，GPON	控、新增高空热成像等汇聚		
77	裕安区劳动保障监察大队	内部视频监控管理平台	大华	是	15	局域网	内部视频监控	2013	7
78	劳动就业管理服务中心	内部视频监控管理平台	深圳博深	是	——	局域网	内部视频监控	2019	4
合计									40932

2.4.1.1. 重复点位资源整合要求

实施中对下列重复点位根据需求和上级要求，并进行核实后进行整合。

重复点位资源整合需求表

序号	重复点位	
	公安局	城南镇
1	城南大道宝小路西北角球机 城南大道宝小路东南角球机	城南大道与宝小路交叉口球机
2	佛子岭路龙井沟路西北角球机 佛子岭路龙井沟路西北角东侧球机	佛子岭西路与龙井沟路交叉口球机
3	佛子岭路将军路西北角球机 佛子岭路将军路西南角球机 佛子岭西路将军路东北角球机 将军路佛子岭路西北角球机	将军路与佛子岭西路交叉口球机
4	将军路青山路西北角球机 将军路青山路东北角球机	将军路与青山路交叉口球机
5	龙井沟路青山路球机	龙井沟路与青山路交叉口球机
6	南河大道淠滨路西南角球机 淠滨路南河大道东北角球机	南河大道与淠滨路交叉口球机

2.4.1.2. 前端感知设备建设要求

针对由政府财政资金投资的过保（超过 5 年）设备和委办局新建需求进行前端感知设备建设，主要建设需求如下：

过保（超过 5 年）设备建设需求表

序号	建设单位	平台名称	建设时间	前端设备总数	枪机	球机	半球
1	生态环境局	裕安区环境保护局视频监控系统	2017.05	79	79		
2	民政局	裕安区民政局办公楼视频监控 系统	2016	16		10	6
3	区残联	区残联办公区域监控	2016.03	6	6		
4	交通局	裕安交通大厦监控系统	2013.03	78	8	8	62
5	城南镇	政府内部视频平台	2016.06	26	26		
6	苏埠镇	政府大楼	2017.03	2			2
7	苏埠镇	食堂	2017.03	1			1
8	独山镇	视频监控系统	2016.06	13	13		

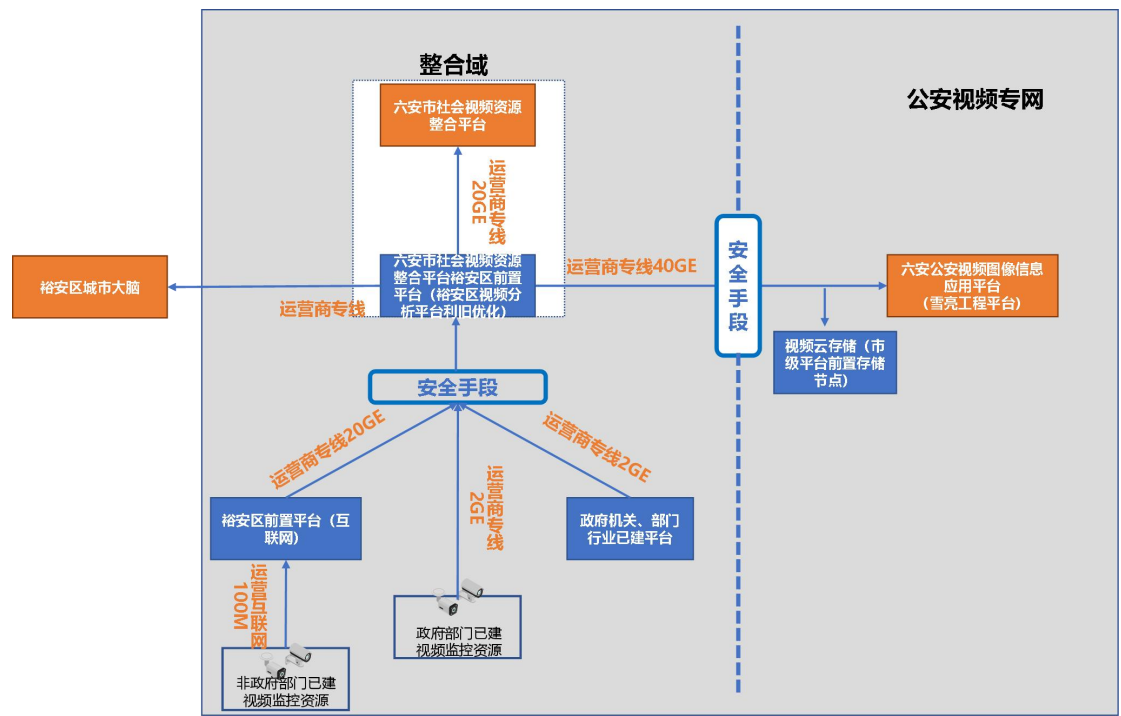
序号	建设单位	平台名称	建设时间	前端设备总数	枪机	球机	半球
9	江家店	江家店镇政府监控系统	2017.12	11	10	1	
10	鼓楼街道	月亮岛社区视频监控系统	2015.09	1		1	
合计				233	142	20	71

委办局新建需求表

建设单位	建设总需求	枪机	球机	半球	人脸相机	应用场景
交通局-交通信息中心	30	11	11		8	路段路口
水利局	6			6		单位内部
青山乡	3		3			单位出入口
江家店	19	4		15		单位内部
罗集乡	16		10	6		单位内部
合计	74	15	24	27	8	

### 2.4.2. 网络建设要求

新建整合域和互联网、整合域和公安视频专网之间、与六安市社会视频资源整合平台上联专线 3 条，六安云计算中心至各委办局间的专线 47 条，租赁至各单位（小区等）互联网线路 261 条。



六安市裕安区公共场所视频监控资源整合共享网络架构图

公共场所视频监控资源整合共享接入统计表（专线）

序号	建设单位	平台名称	接入方式
1	文旅局-横排头景区	全市旅游视频管理平台	运营商专线
2	文旅局-独山革命旧址群	视频监控系统	运营商专线
3	市场监管局	裕安区市场监督管理局食品安全智慧监管平台	运营商专线
4	教体局	裕安校园联网项目	运营商专线
5	生态环境局	裕安区环境保护局视频监控系统	运营商专线
6	民政局	裕安区民政局办公楼视频监控系统	运营商专线
7	卫健委	——	运营商专线
8	裕安区妇幼保健院	智慧园区视频管理平台	运营商专线
9	税务局	六安市裕安区地税办税服务用房智能化系统	运营商专线
10	融媒体中心	内部视频管理系统	运营商专线
11	机关事务管理局	六安市裕安区政府视频监控系统	运营商专线
12	火车站	六安火车站出站口疫情防控视频监控系统/六安火车站站前路综合执法视频监控系統	运营商专线
13	退役军人事务局	退役军人事务局大厅视频监控系统	运营商专线

序号	建设单位	平台名称	接入方式
14	区残联	区残联办公区域监控	运营商专线
15	工企改制中心	办公区域监控	运营商专线
16	征收办	裕安区土地和房屋征收管理处视频监控 系统	运营商专线
17	住建局	六安市建设工程远程视频监控系统服务 项目平台	运营商专线
18	城管局	——	运营商专线
19	交通局	裕安交通大厦监控系统	运营商专线
20	交通局-交通信息中心	省部共建治超联网信息管理系统	运营商专线
21	水利局	淠河治理工程裕安区段管理设施护堤房 配套工程	运营商专线
22	公管局	海康 4200 单机	运营商专线
23	平桥乡	平桥乡政府大院视频监控系统	运营商专线
24	城南镇	市容市貌管理平台/政府内部视频平台/ 政府大院视频平台	运营商专线
25	青山乡	青山乡政府内部监控	运营商专线
26	苏埠镇	政府大楼/食堂	运营商专线
27	石板冲乡	石板冲乡政府视频监控系统/综治中心 视频监控系统	运营商专线
28	韩摆渡镇	视频监控系统	运营商专线
29	分路口镇	分路口镇行政服务中心安防监控系统	运营商专线
30	狮子岗乡	狮子岗乡乡政府政府大楼内部监控	运营商专线
31	独山镇	视频监控系统	运营商专线
32	西河口乡	西河口乡政府政府大楼内部监控平台	运营商专线
33	石婆店镇	石婆店镇政府内部视频监控系统	运营商专线
34	徐集镇	徐集镇政府视频监控系统	运营商专线
35	江家店	江家店镇政府监控系统	运营商专线
36	罗集乡	——	运营商专线
37	顺河镇	——	运营商专线
38	固镇	视频监控系统	运营商专线
39	单王乡	数字乡村平台	运营商专线
40	丁集镇	政府内部视频监控	运营商专线
41	鼓楼街道	鼓楼街道视频监控系统	运营商专线
42	小华山街道	小华山街道办事处及文化站视频监控系	运营商专线

序号	建设单位	平台名称	接入方式
		统	
43	新集镇	电信小翼管家	运营商专线
44	西市街道	西市街道办事处视频监控系统	运营商专线
45	高新区	安徽六安高新技术产业开发区智慧园区一期	运营商专线
46	裕安区劳动保障 监察大队	内部视频监控管理平台	运营商专线
47	劳动就业管理服务中心	内部视频监控管理平台	运营商专线
48	裕安区前置平台（整合域）至六安公安视频图像信息应用平台（公安视频专网）线路		运营商专线
49	裕安区前置平台（整合域至互联网）线路		运营商专线
50	裕安区前置平台（整合域）至六安市社会视频资源整合平台线路		运营商专线

公共场所视频监控资源整合共享接入统计表（互联网）

序号	项目名称	地址	接入方式
1	安豪小区	六安市龙河路	互联网
2	安惠视频监控系统	裕安区 龙河路（安惠小区）	互联网
3	安康安置小区一二期	丰原大道	互联网
4	安康三期	丰原大道	互联网
5	裕苑 安置小区	城南大道	互联网
6	裕丰 安置小区	城南镇政府西边	互联网
7	百川名庭视频监控系统	小华山街道江南社区	互联网
8	百建世纪城小区	平桥大道与兴华路路口	互联网
9	柏林印象小区	松林路	互联网
10	宝业君悦绿苑（东区）智能化工程	学府路与观林路交口	互联网
11	碧桂园凤凰城南苑物业	裕安区平桥乡领春路与天堂寨路交叉口	互联网
12	滨河小区	龙河西路	互联网
13	城南家园小区	城南镇玉兰路	互联网
14	春天嘉苑二期视频监控系统	裕安区小华山街道	互联网
15	春苑新村监控系统	裕安区大别山路与磨子潭路交口	互联网
16	嘉泰丹霞公馆	闻堰路与天堂寨交叉口	互联网
17	帝都豪园小区	裕安区齐云路帝都豪园小区	互联网



序号	项目名称	地址	接入方式
18	渡槽二期视频监控	南辅道南侧渡槽路西侧	互联网
19	振华翡翠湾二期视频监控系统	裕安区平桥乡磨子潭路与闻堰路交叉口东南角	互联网
20	振华翡翠湾	振华路与磨子潭路交叉口	互联网
21	丰泰卡地亚湾视频监控系统	清溪路与滨河大道交叉口	互联网
22	凤凰花园城视频监控系统	六安市 312 国道与樊花路交汇处	互联网
23	凤凰苑小区视频监控系统	裕安区大别山西路凤凰苑小区	互联网
24	南河福龙湾小区	城南镇	互联网
25	富安新城视频监控系统	大别山路	互联网
26	皋城公馆小区	大别山中路 15 号	互联网
27	皋城王府雏菊苑	文盛路与响铃庵路交叉口	互联网
28	皋城王府郁金苑	龙井沟路与大别山路交叉口	互联网
29	皋城王府金桂苑	响铃庵路与磨子潭路交叉口	互联网
30	皋城王府兰香苑	磨子潭路与响铃庵路交叉口	互联网
31	皋城王府玫瑰苑	大别山路与磨子潭路交叉口	互联网
32	皋城王府牡丹苑	龙井沟路与大别山路交叉口	互联网
33	高皇东村	平桥乡百建路高皇东村	互联网
34	国悦府	安徽省六安市裕安区大别山路与响洪甸路交叉口	互联网
35	国祯健康城	平桥大道与顺达路交叉口	互联网
36	海亮江湾城视频监控系统	裕安区新安镇滨河大道与清溪路路口	互联网
37	海亮官邸视频监控系统	平桥乡裕安区闻堰路 33 号楼 2 楼	互联网
38	翰林苑小区	裕安区解放中路 617 号	互联网
39	豪门花园视频监控系统	解放路大别山路	互联网
40	六安恒大御景湾视频监控系统	六安恒大御景湾	互联网
41	恒生阳光城	佛子岭路于解放路交叉口	互联网
42	裕安区鼓楼街道恒宇小区	解放中路 259 号	互联网
43	华邦新华城畅华园	响洪甸路与响铃庵路交叉口	互联网
44	福华园	三里街路与草市街路交叉口	互联网
45	和华园	三里街路与嵩寮岩路交叉口	互联网
46	华邦锦绣华府	六安市解放南路与佛子岭路交叉口	互联网
47	荣华园	三里街路与响洪甸路交叉口	互联网
48	禧华园	三里街路与项洪甸路交叉口	互联网

序号	项目名称	地址	接入方式
49	华邦新华城祥华园	响洪甸路与响铃庵路交叉口	互联网
50	华山小区监控系统	南苑路与齐心路交叉口	互联网
51	华山新村	华山新村	互联网
52	嘉利豪庭	东至紫花路南至裕南路西至繁花路北 至兰花路	互联网
53	嘉利学府二期视频监控系统	城南镇学府路	互联网
54	江南世家小区	江南世家北门	互联网
55	金大地紫金府	六安市裕安区横排头路与嵩寮岩路交 汇处	互联网
56	金马西苑	莲香路 212	互联网
57	金马社区视频监控系统	天堂寨路	互联网
58	金色南郡	城南镇 312 国道与六佛路交叉口	互联网
59	金裕小区	解放中路与五牌里巷	互联网
60	锦成国际视频监控系统	六安市裕安区佛子岭路、家园路	互联网
61	九星嘉园	九星嘉园	互联网
62	聚福园视频监控系统	六安市裕安区响铃庵路	互联网
63	丽水康城 C 区	六安市解放南路与振华东路交叉口	互联网
64	丽水康城 E 区	六安市梅山南路与振华路交叉口	互联网
65	丽水康城佳苑	裕安区解放路西	互联网
66	丽水康城浅水湾	振华西路	互联网
67	丽水康城悦府	振华东路	互联网
68	华邦禄华园视频监控系统	六安市裕安区三里街路	互联网
69	梅花西苑监控系统	裕安区青山路，近赤壁路	互联网
70	梅花新村	2017 年	互联网
71	梅园安置小区监控系统	磨子潭路与霍山路交叉口	互联网
72	明珠广场	淮王街	互联网
73	明珠广场二期	淮王街	互联网
74	明珠国际城	龙河东路与解放南路交汇处	互联网
75	南城安置小区	六安市裕安区城南镇磨子潭路与富裕 路 交汇处	互联网
76	南城佳苑视频监控系统	六安市裕安区城南镇磨子潭路与富裕 路交汇处	互联网
77	南河佳苑	裕安区城南镇南河大道	互联网
78	南河别墅	裕安区城南镇南河大道	互联网

序号	项目名称	地址	接入方式
79	六安市裕安区南门塔四期	南至紫竹林路，北至南通巷	互联网
80	南塔一二期视频监控系统	裕安区西市街道文盛街	互联网
81	淠滨安置小区视频监控系统	淠滨小区	互联网
82	平安东东苑 A 区视频监控 系统	裕安区龙井沟路	互联网
83	平安东苑 B 区	龙井沟路于闻堰路交叉口	互联网
84	平安东苑 C 区	龙井沟路	互联网
85	平安小区	龙井沟路 315 号	互联网
86	瑞华园视频监控系统	六安市裕安区响铃庵路	互联网
87	上城国际小区	佛子岭路 305 号	互联网
88	上海花园	上海花园	互联网
89	盛世华庭视频监控系统	六安市裕安区大别山路、磨子潭路	互联网
90	时光小镇东区	红石谷路与嵩寮岩路交叉口西 260 米	互联网
91	振兴·时光小镇西区	将军李与佛子岭路交叉口	互联网
92	首建·一品铭城	六安市 312 国道裕南西路交口处	互联网
93	舒怡花园监控系统	裕安区大别山路 557 号	互联网
94	双桥湾视频监控系统	六安市裕安区横排头路与西环路交叉 口	互联网
95	水云涧。名居	裕安区解放南路 246 号	互联网
96	四季清风园视频监控系统	云路街 142 号	互联网
97	四季阳光	城南镇玉兰路	互联网
98	嵩旺佳苑小区	佛子岭路与磨子潭路交叉口	互联网
99	腾逸水岸名城视频监控系统	裕安区城南镇梅花大道	互联网
100	天盈上城小区（正宇物业）	105 国道与学府路交叉口	互联网
101	天筑丽景	龙河路与磨子潭路交叉口	互联网
102	同济万象城	城南镇牯牛头社区学府西路 1 号	互联网
103	皖西大市场视频监控系统	312 国道与梅花路交叉口	互联网
104	万华佳苑视频监控系统	长安路与南华路交叉口	互联网
105	万嘉学府春天小区	学府西路与松林路交汇处	互联网
106	万融领秀城	裕安区小华山路与万佛路交汇	互联网
107	万鑫御园（城南新苑）监控 系统	城南大道与宝丰路交叉口	互联网
108	文汇大厦视频监控系统	文汇大厦	互联网
109	裕安区吴巷东扩小区视频监	吴巷新村	互联网

序号	项目名称	地址	接入方式
	控系统		
110	吴巷新村	天堂寨路	互联网
111	梧桐嘉苑小区	解放中路 626 号	互联网
112	西苑新村监控系统	裕安区大别山路	互联网
113	香格里拉视频监控系统	裕安区佛子岭中路 441 号	互联网
114	香樟公寓二期	梅山南路 173 号	互联网
115	香樟公寓一期	梅山南路与龙湖路交叉口	互联网
116	香樟公寓三期	百合巷 58 号	互联网
117	新桥小区监控系统	南和大道于凌云街路口附近	互联网
118	信德时代广场视频监控系统	大别山路信德时代广场	互联网
119	星汇苑小区	皋城西路	互联网
120	兴美三期	淮王街 7 号	互联网
121	兴美四期	明珠三街 64 号 49 号	互联网
122	兴美花园一期	东大街	互联网
123	兴美花园二期	东大街	互联网
124	鼓楼新天地小区	云路街	互联网
125	古城花园	黄大街	互联网
126	阳光小区	解放北路	互联网
127	永安南苑	永安南苑	互联网
128	永安西扩	裕安区 龙河西路	互联网
129	永安一二期	将军路	互联网
130	御龙湾小区视频监控系统	光明西路与淠河路交叉口	互联网
131	裕豪小区	六安市龙河路与厚朴巷交叉口	互联网
132	裕民新村	裕安区经济开发区 312 国道	互联网
133	月亮岛小区视频监控系统	裕安区鼓楼街道月亮岛小区	互联网
134	振兴共和城	六安市裕安区佛子岭西路和响洪甸路交叉口	互联网
135	振兴佳园	六安市龙河路	互联网
136	振兴温莎小镇	六安市裕安区佛子岭西路和响洪甸路交叉口	互联网
137	正东.凯景观邸	红石谷与嵩寮岩交口处	互联网
138	正东.凯旋名门	响洪甸路	互联网
139	中辰一品小区视频监控系统	中辰一品小区	互联网
140	六安望璟台视频监控系统	城南镇横排头路与将军路路	互联网

序号	项目名称	地址	接入方式
141	中央公馆视频监控系统	裕安区紫荆路 13 号 5 栋 20 号 24 栋	互联网
142	众安玖珑府视频监控系统	城南大道与创新路交叉口	互联网
143	周谷堆视频监控系统	六安市裕安区城南镇磨子潭路与裕南路交汇处	互联网
144	康城帝景智能化工程	兴华路独山路	互联网
145	紫竹林安置小区监控项目	紫竹林小区	互联网
146	新安名城视频监控系统	六安市裕安区六单路	互联网
147	和顺名都城	解放南路与天河西路交叉口	互联网
148	六安疊街	裕安区淠河路和均河路东南角六安疊街	互联网
149	新状元楼	淮王街内	互联网
150	振华家园 视频监控系统	振华路路口与磨子潭路交叉口	互联网
151	振华西苑 视频监控系统	振华路中段	互联网
152	振华路小区 视频监控系统	振华路中段	互联网
153	振华山庄、新村 视频监控系统	龙湖路中段	互联网
154	和谐嘉苑	龙河西路	互联网
155	关塘安置小区	新安镇清溪路	互联网
156	碧水云天	城南镇磨子潭路	互联网
157	江南世家小区	江南世家北门	互联网
158	明珠国际城	龙河东路与解放南路交汇处	互联网
159	清华家园	磨子潭路	互联网
160	凤凰东苑	大别山路西站旁	互联网
161	华山小区监控系统	南苑路与齐心路交叉口	互联网
162	渡槽希望新村，渡槽安置一期	渡槽路，南侧辅路	互联网
163	振兴江山赋辰熙小区二期	裕安区佛子岭西路与龙井沟路交口	互联网
164	江山赋一期视频监控系统	磨子潭路与青山路交口	互联网
165	星耀裕龙城	龙河西路	互联网
166	大唐美林湾	天堂寨路	互联网
167	南洋现代城	裕安区兰花路与繁花路交叉口南洋现代城小区	互联网
168	邦发·66#公馆	磨子潭路丰源大道西南	互联网
169	公园首府	南河大道和滨河北路交汇	互联网

序号	项目名称	地址	接入方式
170	星河府	磨子潭南路 600 号	互联网
171	华安小区	华安小区内	互联网
172	裕安区城南镇红达星河城	樊通桥星河路	互联网
173	裕安区小华山街道国际轻工城小区	火车站东侧 312 国道南	互联网
174	裕安区小华山街道浙东玲珑苑	解放南路平桥路口	互联网
175	金隆嘉园	磨子潭路	互联网
176	六安和顺沁园春雅园小区视频监控系统	佛子岭路与南屏路交叉口处	互联网
177	六安和顺 1911 商业街视频监控系统	解放南路西边与佛子岭路北	互联网
178	新城悦六安吾悦华府小区	六安市裕安区梅山南路 1440 号吾悦华府小区	互联网
179	天盈星城小区视频监控系统	佛子岭西路	互联网
180	嘉利学府	磨子潭路	互联网
181	京都豪园视频监控系统	裕安区云路街龙须巷 6 号	互联网
182	圆方居小区	梅山南路春江河滨新村	互联网
183	水利局-裕安水厂	裕安水厂视频监控系统	互联网
184	水利局-分路口水厂	分路口水厂视频监控系统	互联网
185	水利局-徐集水厂	徐集水厂视频监控系统	互联网
186	水利局-钱集水厂	钱集水厂视频监控系统	互联网
187	水利局-陶洪集水厂	陶洪集水厂视频监控系统	互联网
188	鼓楼街道	月亮岛社区视频监控系统	互联网
189	鼓楼街道	大田拐社区视频监控系统	互联网
190	鼓楼街道	锥子庙社区视频监控系统	互联网
191	鼓楼街道	小东街社区视频监控系统	互联网
192	小华山街道	小华山街道园艺场社区视频监控系统	互联网
193	小华山街道	小华山街道十里岗社区视频监控系统	互联网
194	小华山街道	小华山街道华府社区视频监控系统	互联网
195	小华山街道	小华山街道和顺社区视频监控系统	互联网
196	小华山街道	小华山街道恒生社区视频监控系统	互联网
197	小华山街道	小华山街道天盈社区视频监控系统	互联网
198	小华山街道	小华山街道春江社区视频监控系统	互联网

序号	项目名称	地址	接入方式
199	小华山街道	小华山街道河滨社区视频监控系统	互联网
200	小华山街道	小华山街道六梅路社区视频监控系统	互联网
201	小华山街道	小华山街道香樟社区视频监控系统	互联网
202	小华山街道	小华山街道江南社区视频监控系统	互联网
203	小华山街道	小华山街道政务社区视频监控系统	互联网
204	西市街道	凤凰桥社区新时代实践站建设项目视频监控 频监控系统	互联网
205	西市街道	紫竹林社区视频监控系统	互联网
206	西市街道	西市街道南门社区视频监控系统	互联网

2.5. 裕安区前置平台优化要求

2.5.1. 平台概述

裕安区前置平台作为整合域的视频汇聚总平台，需具备强大的接入、共享性能以及足够的稳定性和兼容性，以满足裕安区社会视频资源接入及各政府部门、社会公众视频共享需求。

同时，考虑到裕安区有大量的小区、水厂等单位的监控资源未进行整合，在互联网接入相关单位的已建视频监控资源进行汇聚后通过安全手段推送至整合域。

2.5.2. 平台功能

2.5.2.1. 基础应用

2.5.2.1.1. 视频接入

(1) 直接接入

部分委办局已经建设了部分视频资源或者打算新建部分视频资源，但缺少视频平台，可以采用设备接入的方式进行整合接入。视频直接接入包括两种方式，一种是常规视频设备接入，指只需要接入基本视频的设备，另一种是智能视频设备接入，指除基础视频接入外，还需要接入设备通过智能分析算法产生的抓拍图片、事件等内容。

普通视频设备接入包括对新建设备和已建设备的设计考虑，新建的智能摄

像机均应采用 GB/T28181-2016 国标协议接入视频系统，已建的存量视频监控设备，应首先考虑采用 GB/T28181-2016 国标协议接入，其次考虑采用 ONVIF 协议接入，也可以根据点位实际重要性，点位改造替换或者采用 SDK 开发接入。

包括 GB/T28181-2016 国标协议接入、ONVIF 协议接入、设备 SDK 接入。

## **(2) 级联接入**

可以通过平台联网的方式接入各类下级平台的视频资源，上下级平台的联网对接应满足《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/T28181-2016）的标准强制项要求。

针对已建的其他视频监控平台，应采用 GB/T28181-2016 国标协议实现与平台对接。

### **1. GB/T28181 国标协议对接**

已建的符合《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/T28181-2016）要求的视频监控平台，按照 GB/T28181-2016 国标协议进行互联对接。

### **2. 非标平台升级改造对接**

对于不符合 GB/T28181-2016 要求的视频监控平台，此类视频监控平台应通过自身软件升级改造方式实现信令协议、设备 ID、媒体传输协议、数据封装格式、媒体码流的标准化改造，满足 GB/T28181-2016 标准要求，输出标准信令与标准码流，并采用 GB/T28181-2016 国标协议实现与平台的无缝级联对接。

### **3. 非标平台网关改造对接（SDK 对接）**

对于无法实现软件自身升级的非标视频监控平台，增加符合 GB/T28181-2016 标准要求的联网网关，实现对此类非标平台的国标化改造，将非标平台的信令协议、设备 ID、媒体传输协议、数据封装格式、媒体码流进行标准化的转换，保证平台接收到的始终是标准的信令流和标准的媒体流。

## **2.5.2.1.2. 视频基础服务**

基础视频预览回放：视频实时预览即为对监控实时画面的预览。视频预览方式主要分直连预览、非直连预览、级联预览。直连预览为平台直连设备进行预览；非直连预览为平台过设备接入组件进行预览；级联预览为平台通过视频



联网网关进行预览。

视频应用：支持视频预览、视频轮巡、录像回放、云台控制。支持推荐、历史观看点位，收藏夹和预案设置展示；支持画面抓图、录像、电子放大、3D放大、云台控制、打开声音、打开对讲、切换主子码流、打开视频智能信息、一键上墙、点位分享、切换录像回放、关闭画面等功能，抓图时支持上传至暂存架；支持实时监控预览上墙、回放上墙、桌面上墙功能。

### 2.5.2.1.3. 视频联网管理

支持通用视频联网标准协议（GB/T28181）；

支持配置信令网关、媒体网关；

支持配置本域、上级域、下级域级联关系；

支持资源选择性共享：针对本域或外域的资源进行选择共享操作；

支持资源检索：针对本域和下级域，进行检索查询操作；

支持资源信息统计：在运行概况里展示本级域与下级域的资源状态，以及共享给上级的资源信息；

支持视频级联操作能力：包括摄像机控制、实时预览、录像查询、录像取流、回放控制、录像文件下载、手动录像、设备信息查询、设备状态查询、设备远程启动、设备校时。

### 2.5.2.1.4. 视频转发管理

支持通过 RTSP 标准协议提取实时流；

支持跨路线，单点位取流；

支持降码率、降分辨率，非标准码流转标准码流。

### 2.5.2.1.5. 平台运维管理

运维管理模块对平台组件进行运行监控与问题排查，可提供自动化指标检测和告警、批量集中部署配置、高效问题定位等能力，帮助运维人员及时发现和解决问题，提升交付和运维效率，为整体平台提供有力的后台保障。

### （1）整体情况

提供了整个系统的健康状况概览，支持在首页全局性地查看各服务器和摄像头的健康状况，当系统有异常，告警时，支持通过点击发生异常的摄像头/服务器，快捷跳转到摄像头/服务器状态监控页面。

### （2）状态监控

图形化展示服务器、摄像头运行拓扑、运行状态，并展示告警与状态统计；支持投放大屏展示当前服务器、摄像头运行状态；支持根据系统当前实际运行状态，通过评分量化系统运行情况；支持统计服务器在线率及各服务在线详情；支持统计摄像头在线率及各摄像头在线详情；支持统计系统最近 7 天每日告警数；支持统计系统最近 7 天每日的用户活跃数。

### （3）告警处理

提供告警展示、查询、处理、策略配置功能，实现对告警的全生命周期管理。支持针对所管理的服务器、云存储设备、摄像头和服务的运行状态进行监控，如果有异常则会产生告警。支持查看各服务器、云存储设备、摄像头及服务的监控详情（服务器信息、服务器监控指标、关键进程）、告警详情（支持告警数据导出）以及维护记录（信息包括时间、用户、操作、结果及终端地址），支持查看有未处理告警的资源，支持模糊搜索。

### （4）系统维护

支持进行平台安装部署操作，包括软件安装包、资源包、补丁包的安装与管理。分类显示已安装的组件及其版本，支持手动卸载、升级和回滚。支持安装补丁，支持一台服务器上批量安装多个补丁，且可还原最近一次安装的补丁。支持服务参数、客户端参数、告警策略、校时、多线路和防火墙策略进行配置，并支持配置下发。支持设置自动备份策略，定时对数据进行全量备份，支持针对备份文件进行删除、还原操作。

### （5）日志分析

支持查看对应服务器、摄像头和服务的系统日志信息，支持查看日志中的错误码（一串由数字和英文字母组成的蓝色字符）详细了解系统错误内容及解决建议。支持查看操作日志及系统日志中的调用链，以了解一次业务操作中涉及到的所有组件之间的调用关系，以及这些组件的异常状况及其相关日志，快速定位异常问题的原因。

## 1.感知设备运维管理

系统感知设备运维管理应主要包含感知设备状态监控、视频录像监控。系统支持通过 SDK、Onvif、Ehome、国标、SNMP 等主流协议对监控摄像机、存储设备、卡口设备、移动特征采集设备、视频/图像结构化设备、WIFI、RFID 开展统一的运维管理。对上述设备具备状态巡检功能，显示异常设备信息并进行状态标识（如：设备掉线），生成异常信息报表，并具有报表导出功能。系统具备对监控点位进行录像完整性检测，可以根据不同时间来进行查看所巡检时间范围内的录像完整性情况。系统能够结合 GIS（地理信息系统）实现空间地理可视化管理，应支持将所有运维资源信息、运维人员的实时位置都通过 GIS 展示和操作。系统支持查看资源的周围地理信息，也可以通过地理位置查询资源，用户可以快速检索 GIS 地图迅速定位到故障点。

## 2.中心设施运维管理

### 1) 主机设备管理

中心设施运维管理应支持对主机设备管理、标准应用监控、网络传输监控、视频存储监控。系统应支持以列表化方式显示主机的常用管理参数，详细的主机基本管理参数、单个系统的 CPU、内存增长趋势、服务进程、单个系统存储空间实时和变化情况。系统应支持对统计范围内的主机进行详细的实时分析数据，便于用户关联分析出需要重点关注的主机，以实时 CPU 利用率的主机排序、实时内存利用率的主机排序、实时连续运行时间的主机排序、各个操作系统的存储空间已使用情况分析。系统应能提供主机一体化显示，按照不同的操作系统进行数据分类，系统提供基础信息、运行信息、进程管理、事件与告警等各类管理信息。标准应用监控功能应支持文件传输应用（ftp）、网页服务（http）、邮件服务（pop3、smtp）的监控。

### 2) 网络传输监控

系统应具备对当前网络线路的流量、带宽占用比等信息进行排名查看，并可进一步查看指定线路的性能负载历史记录。使运维管理人员可及时了解当前负载较高的线路，在网络负载过载前，及时进行处置，保障网络不间断的平稳运行。系统应具备对视频图片存储的容量采集管理，监控硬盘存储容量、可用容量、已用容量，分析已用容量占比。具备存储设备的状态监控，包括 CPU 负载、内存占用、带宽占用等。

### 3.视频数据质量管理

系统采用轮巡的方式，具备对前端设备的码流进行解码与图像质量评估，实现对视频信号中存在的问题进行智能分析、判断和告警。具有 14 种常见视频故障以及码流时延（关键帧时延、信令时延、码流时延）情况的检测能力，如清晰度异常（图像模糊）、亮度异常（过亮、过暗）、偏色、噪声干扰（雪花、条纹、滚屏）、画面冻结以及信号丢失等，可有效预防因硬件设备导致的图像质量问题而带来的损失。系统具备为用户展现图像异常原因的能力，需包括登陆失败、取流失败、解码失败、图像异常。平台提供字幕标注功能，可进行页面水印设置，支持水印信息以及呈现方式设置。平台提供时钟同步功能，可设定校时时钟源，可设置为中心、外部时钟源，支持服务器自动校时、服务器手动校时，可全部立即校时，或指定服务器校时。

平台提供根据下级联网检测、视频图像质量检测结果情况，自动生成考核报表。

### 4.集中监控管理

集中监控管理功能应包含综合告警展现、告警通知等功能。综合告警展现功能提供了一个运维信息的综合展现、操作界面。通过此界面，用户能够实时掌握系统整体运行状态，并及时发现发生的故障、告警等信息问题。综合监控展现功能为整个监控管理功能提供了主体功能界面。告警列表实时更新监控，实时刷新刚产生的告警信息，并且不同告警的严重程度可以设定不同的颜色。系统具备以卡片形式展示告警通知规则设置，支持通知时间定义，可进行通知规则的模板管理，并能以短信、邮件、消息的方式，通知到相应的运维管理人员。

### 5.运维过程管理

运维过程管理功能应包含服务级别管理功能、合同及客户管理、工单管理、应急演练与预案。SLA 服务等级协议（简称：SLA，全称：service level agreement）是指运维管理部门和运维服务供应商之间关于运维服务质量的约定，其目标是确保运维服务质量。系统支持通过技术手段对 SLA 服务级别配置进行固化，提供服务等级协议的新增、启用，并与系统内的设备指标、设备类型做关联。当指定设备发生故障时，会形成相应的故障事件，进而对服务协议的执行情况进行统计。系统具备以单位的组织形式对用户客户信息进行管理，

支持按客户名称进行检索，支持对维保项目进行管理，包含维保的起止时间、附件的保存及相应运维资源的关联，支持按名称进行检索。根据不同的事件，系统应可将工单定义为故障单、问题单、巡查单等多个维度，进行工单分类管理；系统具备针对重大故障、灾难事件进行应急演练与预案的管理。为保证各类信息化软件设备的调整与变更的规范性与信息动态更新，系统应支持提供通过标准化流程来控制和管理设备配置项发生的变更管理能力。配置管理，系统应具备对运维管理过程各项内容的配置能力，并能记录运维管理过程中各类配置项的变化，以方便进行责任追踪。用户能够根据自己的权限，在工单处理过程中的任一环节均可实时看到自己正在处理或应处理的工单的流转情况。系统具备变更管理，能提供配置变更审核，能追溯变更的资源名称、变更属性、以及变更前后变化、变更人、变更时间等，并能进行变更审核操作，以支持标准化操作流程。

## 6. 运维工单管理

监控告警管理对设备的运行态势进行故障告警，并以短信、邮件、消息等手段及时通知维护人员，保障快速响应，及时排除故障。

工单管理统一受理电话、微信、邮件等渠道来源的故障报修，并为维护部门提供派单、跟踪、确认的流程处理。系统提供定期巡查工单，组织一线运维人员，定期巡查前端感知设备、网络通信、服务器、应用软件、中间件等环境设施情况，并反馈异常情况。系统面向一线运维人员提供移动运维管理，基于终端的移动性及卫星定位，进行运维任务分派、运维过程跟踪、运维考核等有力手段。

### 2.5.2.1.6. 视频调阅

视频调阅是为了实现各级部门用户对视频资源的快速调取，主要包括视频片段、片段调阅详情、平台信息、平台拓扑图和平台配置信息。

系统提供用于不同部门/行业平台基于权限控制的、共享视频资源的查看及调阅，以及视频点位资源的信息同步；

系统支持按行业、行政区划属性分类展示资源目录，同时支持根据用户自定义方式展示资源目录；

系统支持符合 GB/T 28181-2016 中要求的注册、保活、视音频实时点播、云镜控制、录像检索、录像回放、录像下载、报警和语音广播等基本应用功能；

系统支持资源目录的自动和手动刷新；

系统支持视频资源的多路径及按推荐路径访问；

视频调阅系统支持视频片段管理功能，包括视频片段的生成、权限设置、查询、回放、删除等功能。

### 2.5.2.1.7. 视频统筹布建

目前城市视频建设都基本是委办局各自开展，缺乏有效的统筹和规划，容易产生重复建设、建设不合理等问题，对前端感知设备建设，缺乏科学、合理的评价模型以及高效的评价与规划工具。本方案可以帮助用户统筹构建一套城市级前端布建评价体系，建立城市视频评价模型，科学、有效认知感知前端建设缺陷，从整体的角度对视频资源的建设、应用等方面进行分析、评价和布建规划指导，提升城市视频前端布建的科学化水平，同时也可以让平台更高效发挥作用。

前端评价与规划系统用于实现对物联感知前端资源的建设成效进行评价，还支持对物联感知前端布建设计方案进行评价，并且可在评价基础上动态化的完成布建规划。

#### （1）应用场景

系统充分考虑了场景化的前端建设，结合场景中的感知能力要求，匹配前端设备的感知能力，并且要考虑设备状态情况，前端设备目前能提供的感知能力与场景中的感知要求进行评判。评判的过程利用系统设计的“评价指标体系”，包括点位布建评价模型（含指标规则），再通过调用各个前端设备的布建数据，结合布建安保等级要求，对前端点位建设效能给出评价报告，报告中列出布建场景中存在的问题和总体建议，为后续项目建设、规划提供参考，提升整体前端布建的科学化水平。

#### （2）系统功能

“前端布建系统”核心功能包括评价/规划项目管理（评价与规划项目管理

和点位布局规划管理)、报告管理和基础配置管理。

包括评价与规划项目管理、点位布局规划管理、报告管理及基础配置管理。

### (3) 整体工作流程

评价工作流程

“前端评价与规划系统”如何完成一次评价任务，系统里面有一个概念叫“项目”，评价对象就是一个项目，通过系统化工作流程，先完成评价前准备工作、再创建评价项目、最终生成评价报告，完成一次评价任务。

包括评价前准备工作、创建评价项目、生成评价报告等。

## 2.5.2.2. 共享中心

### 2.5.2.2.1. 数据管理

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

通过图形化的配置页面来配置接口，无需去写 SQL 写代码，让不会编程的人也可以自由配置内部接口、对外接口。

基于服务标准规范，将能够提供的服务资源，以服务接口的方式统一注册到城市大脑，构建统一的服务请求方注册、服务请求方审批、服务接口访问申请及接口授权服务资源管理流程，建立统一的服务资源管理制度，对上层系统应用开发提供有力的支持。

### 2.5.2.2.2. 资源共享中心

资源共享中心对服务器资源、数据源信息、表信息、函数算法信息、资源注册信息、菜单信息、权限信息进行展示和管理。可对服务器进行分组、添加服务器资源，对计算资源进行管理，在数据表管理中，可以对基本信息、建表参数、字段、生命周期等信息进行管理，可以查看数据血缘、数据地图、表关联度分析。函数算法管理中，包含预设算法包，可以新增公有算法包和私有算法包，可对预设函数、公有函数和私有函数进行注册。

底层使用 ELK 架构，应用 RocketMQ 和 HMS 技术实现对资源的管理。作为平台统一的资源共享中心，创建不同的角色，集中管理数据开放平台中的菜单、库表元数据等资源信息，并且这些资源信息都是可以在资源管控中心对第三方开发者配置使用权限。

#### **2.5.2.2.3. 数据资源开放**

支持专业的数据开发团队通过服务接口、数据资源目录、数据订阅、数据库视图等方式获取数据共享服务，深度挖掘数据价值，为智能应用实现数据赋能。支持原数据资源、主题库、专题库、关系库、标签库的数据获取。

### **2.5.2.3. 认证中心**

#### **2.5.2.3.1. 统一认证**

对系统用户、部门、接入系统和系统使用用户进行管理，对不同的用户和角色设置权限，可以对应用进行配置，实现各组件模块统一认证，同时可以同步各组件的用户和部门。

统一认证中心系统将分散的应用系统用户身份全局统一认证和角色授权管理进行了整合，简化了用户访问各业务系统的过程，用户只需要通过一次身份认证过程就可以访问具有相应权限的所有资源。

#### **2.5.2.3.2. 统一鉴权**

通过数据权限、红名单配置、屏蔽、数据脱敏、数据预设条件、碰撞权限配置管理，实现认证安全管理、集中存储安全。独立分布应用开放平台和数据开放平台的权限管理。

数据权限，为不同用户角色配置数据使用权限，包括数据字段的权限、基于数据条件的权限、数据碰撞权限。实现了数据权限条件与实体用户信息自动关联，对应权限区划的用户只能查看特定区划的数据、使用特定区划的数据。



### 2.5.2.3.3. 日志审计

数据操作日志审计功对系统操作、应用访问、接口调用、数据接入等日志进行审计，提供审计档案，通过日志倒查，可追溯系统访问轨迹。

审计中心满足用户审计需求，对系统操作动作进行收集，对审计人员进行管理和作业支持。审计中心通过采集 SDK 规范化处理和汇集日志，满足审核要求，收集应用操作、数据访问和接口调用等日志信息，为审计任务提供数据支撑。

### 2.5.2.4. 运行中心

运行中心为运营人员提供运行监控、运行统计、运行报告生成，是辅助运营人员掌握平台运行情况的功能模块。

#### 2.5.2.4.1. 运行监控

提供运行概览能力，帮助运维人员及管理人员了解平台整体运行情况，包括点位资源情况、任务执行情况、算力运行情况、算法使用情况、智能分析情况、事件输出情况、分析异常情况等。

包括点位资源情况、任务执行情况、算力资源情况、算法使用情况、分析总量情况及事件输出情况。

#### 2.5.2.4.2. 运行统计

运行统计将平台运行的数据进行分类统计，主要包含视频共享统计、算法调度统计、数据资源使用统计、事件推送统计等。包括视频共享统计、算法调度统计、数据调用统计与事件推送统计。

#### 2.5.2.4.3. 运行报告

提供整体运行报告自动生成功能，方便进行平台运行工作汇报。可以按天灵活进行统计输出，输出内容包括运行概述、数据分析两大块内容。

## 2.5.2.5. 开放中心

通过插件、CS 客户端及平台级联三种方式提供视频应用，应用内容包括视频管理服务，实现视频预览、录像回放、视频上墙、视频事件监控服务能力。

委办局视频上墙需要额外增配本地播放平台，视频源可由平台推送。

### 2.5.2.5.1. 视频应用服务

#### （1）视频能力

提供视频实时预览、网络录像回放、语音对讲取流 URL 获取能力；

提供设备控制能力；

提供预置点管理能力；

提供视频图片获取能力；

提供手动录像控制能力。

#### （2）视频资源

提供分页获取监控点资源、查询监控点列表、获取区域下级监控点列表、获取单个监控点详细信息能力；

提供分页获取编码设备资源、查询编码设备列表、获取区域下级编码设备列表、获取单个编码设备详细信息能力。

#### （3）视频网管

提供监控点、视频编码设备在线状态查询能力；

提供视频质量诊断结果查询能力；

提供录像完整性结果查询能力。

### 2.5.2.5.2. 目录资源服务

用户可通过资源目录完成对资源目录库中摄像机信息的录入、校验、修改、删除。同时在开放中心提供资源目录，支持按行业、行政区划属性分类展示资源目录，同时支持根据用户自定义方式展示资源目录。

### 2.5.2.5.3. 应用服务

基于平台提供的基础视频、智能解析、视频数据等开放能力，在满足各委办局基础业务视频能力支撑的同时，还可以结合业务应用需求，构建单一场景智能应用、跨时空场景智能应用管理等类型的创新应用。包括但不限于街道路面整治、店外秩序管控、河湖环境保护、秸秆燃烧监管与安全生产预警等应用。

### 2.5.3. 平台性能

**整合域：**平台需具备不低于 5 万路的视频接入能力，不低于 500 路 4M 码流实时并发能力，不低于 1 万路的视频存储能力。

**互联网：**平台需为用户提供用户登录访问及视频并发调阅服务支撑，平台需具备不低于 4 万路的视频接入能力，不低于 400 路 4M 码流实时并发能力，不低于 8000 路的视频存储能力。

### 2.5.4. 与其他平台关系

裕安区前置平台，整合各单位建设的公共场所视频监控资源，实现各级人民政府机关（重点实现市辖区外，乡镇、街道等单位的视频资源接入）、各单位已建设待整合公共场所视频监控资源的统一接入，整合后统一推送至筹建中的六安市级社会视频资源整合平台，并同步考虑通过安全边界推送至六安公安视频图像信息应用平台（雪亮工程平台）作为备选路径。其他政府部门需建设个性化视频综合应用，可申请裕安区前置平台视频接口服务进行调用。

### 2.5.5. 视频场景算法应用

根据裕安区社会治理需求，建设以下四类算法应用，总共不少于 1000 路视频分析算法授权，并通过党建平台推送给相关部门实现管理闭环。算法应用同时纳入裕安区城市大脑算法仓库，并与市平台算法做到共用、互补。

#### （1）校园安全算法应用

为提高学生的人身安全保障，采用人脸识别技术构建的校园安全体系，是传统安防系统的有效升级和补充，能够对非校内人员进行实时视频监控分析、运动跟踪、聚众检测、人脸检测及识别，将海量的抓拍人像及视频数据转化为人脸标签的数据。

该系统基于视频智能分析技术，实现对人员异常行为的控制，当发生人员剧烈活动、倒地、人群过密等情况时，会自动发出警报，通知管理人员到现场处置。从而及时有效地防范校园恶性事件，大幅度地减少校园事故的发生。同时系统具备强大的数据查询、检索、处理功能，为平安校园提供了强有力的技术支撑。运用 AI 智能视频分析技术，校园安保人员实时查看学校的围墙周界、教学楼周边、校园食堂、操场等地带状况，了解校园环境变化。智能监控系统将告警信息推送给校园管理人员，也有助于其采取应对措施，以此防范突发恶性事件对学生造成伤害。

智慧校园智能算法包括：人脸识别、聚众检测、攀爬识别、校园危险区域、校园防踩踏、校园烟火、抽烟、打手机、闯入、打架、摔倒等服务。

### （2）智慧社区算法应用

通过社区出入口、公众活动场所等重点区域部署高清监控摄像头+AI 智能算法，实现当出现人员摔倒、人群聚集、人员打架等情况时，系统将及时告警至后台，工作人员能够尽快了解情况，并及时派遣人员处理。同时系统还可以实现消防通道异常、人数统计、区域聚集、人员滞留、区域闯入、车牌识别、社区巡逻、烟雾识别、偷盗监测、破坏公物识别。有效提升社区安防系统作用，为居民带来更快捷、安全、智能的全新体验，提升生活幸福感。

智慧社区智能算法包括：消防通道异常、区域聚集、人员滞留、区域闯入、打架、跌倒检测、烟雾识别、偷盗监测、破坏公物等识别。

### （3）安全生产算法应用

辖区内企业较多，安全隐患与风险点多，安全生产监管人力不足，隐患排查无法深入细致，隐患及时性无法保证，企业隐患整改情况无法实时了解；通过视频监控智能分析，进行风险预警，消除安全隐患，降低安全生产事故率。

将云计算、智慧物联网技术通过与边缘计算、人工智能技术结合，提升对于高要求场景的支撑能力，比如人脸识别、烟火识别、着装检测、睡岗离岗检测、人员入侵检测、周界入侵检测等，当监测到异常情况时，系统立即抓拍、触发报警，并推送消息至管理人员，监控中心的管理人员也可以根据平台发送的告警信息进行人为干预处理。

系统基于视频智能分析，自动实时监测场景中的人、车、物、行为，实现安全生产少人、无人化、智能化监管，降本增效，降低人力成本。平台支持级

联、数据互联互通，可有效实现多方监管，满足各部门的辅助监督需求。

安全生产智能算法包括：人员出入、边界跨越、人员逗留监测，人员摔倒（跌倒）识别、人员异常聚集；佩戴安全帽识别、防护服穿戴识别、反光衣识别，烟雾识别、火焰识别；抽烟识别、拨打电话识别、玩手机识别、人员拥堵识别等。

#### （4）智慧城管算法应用

“城市六乱”是指乱搭乱建、乱堆乱放、乱设摊点、乱拉乱挂、乱贴乱写乱画、乱扔乱吐等严重影响城市秩序、容貌和环境卫生的违法行为，让市民深恶痛绝。针对上述乱象，充分运用现代信息技术，开展视频智能分析实战应用。

通过选取店外经营、占道广告、游商小贩、乱扔乱倒、乱堆物料、垃圾满溢、垃圾暴露、沿街晾晒、余泥渣土运输等市民群众比较关注的城市管理易发多发问题，开展视频智能分析实战训练应用，提升城管部门的工作效率，同时也大大降低了工作强度，通过利用先进的视频智能分析技术，城市管理实现了“人工监看”向“智能采集”、“事后处理”向“实时追踪”、“被动监控”向“精准监控”的三个转变。

视频智能分析技术可以全天候紧盯城区主次干道，对重要景观地段乱摆卖、占道经营、乱扔乱倒、乱堆物料、垃圾满溢、余泥渣土超载洒漏等城市管理易发多发问题进行智能抓拍、智能识别、自动报警，形成了广覆盖、宽范围、快速发现、快速处置问题的城市管理新模式，实现城市管理问题 AI 智能巡查及城市管理态势适时感知、可视化。

## 2.6. 运维管理要求

### 2.6.1. 运维原则

完善的运维服务制度与流程。为保障运行维护工作的质量和效率，应制定相对完善、切实可行的运行维护管理制度和规范，确定各项运维活动的标准流程和相关岗位设置等，使运维人员在制度和流程的规范和约束下协同操作。

高素质的运维服务队伍。运维服务的顺利实施离不开高素质的运维服务人员，因此必须不断提高运维服务队伍的专业化水平，才能有效利用技术手段和

工具，做好各项运维工作。

运维界面：本项目运维管理主要针对由本项目新建的前端感知设备及网络、视频监控基础平台、安全管控和存储等设备。同时对于由本项目接入的已建视频监控摄像机，通过平台运维管理功能实时监测其在线状态，当设备离线时通知原运维单位进行修复。

### 2.6.2. 运维目标

- 1、保障平台的稳定性和可靠性；
- 2、保障平台的安全性和可恢复性；
- 3、故障的及时响应与修复；
- 4、提升人员系统操作水平；
- 5、保障系统用户信息及时更新。

### 2.6.3. 运维期限

应用软件提供验收后 5 年免费质保，硬件设备免费质保 5 年。

### 2.6.4. 运维内容

#### 2.6.4.1. 前端设备运维服务

对利旧设备及新建设备的统一纳管、平台账户管理、可信四码数据导入能力，满足日常运营运维需求。

##### 终端采集设备

通过对终端采集设备的智能发现，实现终端采集设备归类、重启、升级、复位、设备情况导出、设备信息检索。

##### 1、终端采集设备智能发现

分析接入的终端采集设备信息数据，智能发现新接入终端采集设备。

##### 2、终端采集设备参数配置

支持对已发现的终端采集设备参数及板卡参数进行调整，可通过配置文件导入或手动调整方式修改终端采集设备或板卡参数。

终端采集设备参数配置：支持对网络配置、点位信息、数据回传配置、本地存储等参数进行修改配置。板卡参数配置：支持对同步方式、同步端口、同步频点、工作频点、功率等级等参数进行修改配置。

### 3、终端采集设备概览

根据片区分类，展现不同片区所包含所有终端采集设备信息，当终端处于游离状态时，系统自动识别游离状态终端并进行状态展示。

### 4、终端采集设备移动

以网格化概念对终端采集设备进行分类，支持将终端采集设备移入不同片区中。

### 5、终端采集设备启用

支持一键式终端采集设备启用。

### 6、终端采集设备停用

支持一键式终端采集设备停用。

### 7、终端采集设备重启

支持一键式终端采集设备重启。

### 8、终端采集设备升级

支持一键式终端采集设备升级更新。

### 9、终端采集设备复位

支持一键式终端采集设备复位。

### 10、终端采集设备导出

支持对一个或多个采集设备配置参数导出。

### 11、终端采集设备检索

支持通过设备编号、设备串号、IP 地址、设备状态、厂商编号、最后上号时间条件对终端采集设备信息进行单一条件或多条件联合查询。

## 图像采集设备

通过对图像采集设备的智能发现，实现图像采集设备归类、配置、设备信息检索。

### 1、图像采集设备智能发现

分析接入的图像采集设备信息数据，智能发现新接入图像采集设备。

### 2、图像采集设备参数配置

支持一键式跳转已发现图像采集设备的本地配置管理系统。

### 3、图像采集设备概览

根据片区分类，展现不同片区所包含所有图像采集设备信息，当终端处于

游离状态时，系统自动识别游离状态终端并进行状态展示。

#### 4、图像采集设备移动

以网格化概念对图像采集设备进行分类，支持将图像采集设备移入不同片区中。

#### 5、图像采集设备检索

支持通过设备编号、设备状态、最后上号时间条件对图像采集设备信息进行单一条件或多条件联合查询。

### 域组管理

以网格化概念将部署在不同地区的利旧前端感知设备、新建前端感知采集设备按域组进行网格化划分，同时对域组内的利旧或新建前端感知设备进行统一管理。

#### 1、域组概览

展现区域内的域组情况，展示域组域组编号、域组名称、域组经纬度、域组功能、域组状态、备注信息。

#### 2、地区新建、删除

支持自定义添加地区信息，如北京市东城区朝阳门街道。同时支持对地区进行删除。

#### 3、地区信息检索

支持通过关键字对地区信息进行检索。

#### 4、域组信息概览

展现区县小区所包含的所有域组信息，展示域组编号、域组名称、中心经度、中心纬度、域组功能等。

#### 5、域组新建

支持在区县级辖区新建域组，可自定义设置域组名称、中心经度、中心纬度、域组功能、去重窗口时间、关联窗口时间、备注信息。

➤ 域组功能：域组功能是对域组实现功能的描述，包括 IMSI、IMEI、MAC、人像、车辆。

➤ 去重窗口时间：支持对 IMSI、IMEI、MAC、人像、车辆设定去重窗口时间，可设定去重窗口时间为 60 秒、120 秒、180 秒、300 秒。

➤ 关联窗口时间：支持对人像-人像、人像-IMSI、人像-车辆、IMSI-车



辆、IMSI-IMEI、车辆-IMSI、车辆-车辆等关联关系设定关联窗口时间，可设定关窗口时间为 60 秒、90 秒、120 秒、180 秒、300 秒。

#### 6、域组编辑

支持对域组进行编辑修改。

#### 7、域组启用

实现一键式域组启用。

#### 8、域组停用

实现一键式域组停用。

### 四码数据导入

支持手动批量导入可信四码关联关系数据，为感知数据处理，形成关联关系提供可信知识。

#### 1、可信四码数据批量导入

可下载模板添加可信四码数据，支持上传可信四码数据模板，批量导入可信四码数据。

#### 2、可信四码数据检索

支持通过 IMSI、IMEI、MAC、手机号码、入库时间对四码数据进行单一条件或多条件联合查询。

## 2.6.4.2. 系统运维应急处理

系统运维应急处理是对中断或严重影响业务的故障，如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将损失降到最低。在系统维护过程中，突发事件的出现将是很难完全避免的，针对这种情况，要完善的突发事件应急策略。

系统巡检人员要定期规范检查各硬件设备的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

对发现的问题在报负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，

要形成问题汇报，避免以后类似重大紧急情况的发生。

当获悉出现突发事件时，技术支持人员可以立即从知识库中获取相应的应急策略，并综合具体情况，给出相关解决方案，然后在第一时间以电话、邮件支持或现场服务的方式解决问题，尽最大努力减小突发事件对日常应用的影响。

**2.6.4.3. 信息资产统计服务**

服务内容包括：

- 1、硬件设备型号、数量、版本等信息统计记录；
- 2、软件产品型号、版本和补丁等信息统计记录；
- 3、网络结构、网络路由、网络 IP 地址统计记录；
- 4、综合布线系统结构图的绘制；
- 5、其它附属设备的统计记录。

**2.6.4.4. 数据库系统运维服务**

包括主动数据库性能管理，数据库的主动性能管理对系统运维非常重要。通过主动式性能管理可了解数据库的日常运行状态，识别数据库的性能问题发生在什么地方，有针对性地进行性能优化。同时，密切注意数据库系统的变化，主动地预防可能发生的问题。

数据库运行维护服务还包括快速发现、诊断和解决性能问题，在出现问题时，及时找出性能瓶颈，解决数据库性能问题，维护高效的应用系统。

主要工作是使用技术手段来达到管理的目标，以系统最终的运行维护为目标，提高工作效率。

**2.6.4.5. 网络安全运维服务**

从网络的连通性、网络的性能、网络的监控管理三个方面实现对网络系统的运维管理。网络、安全系统基本服务内容：

网络、安全系统基本服务内容表

序号	服务模块	内容描述
----	------	------

序号	服务模块	内容描述
1	现场备件安装	配合用户进行，按备件到达现场时间工程师到达现场
2	现场软件升级	首先分析软件升级的必要性和风险，配合用户进行软件升级
3	现场故障诊断	按服务级别：7×24 小时、5×8 小时
4	电话远程技术支持	7×24 小时
5	问题管理系统	对遇到的问题进行汇总和发布

2.6.5. 运维系统

2.6.5.1. 数据对接中心

通过建设“数据对接中心”对接其他各系统。

数据对接中心是智能运维平台的核心子系统，通过数据采集中心，可以将视频监控设备、车辆卡口设备、人像卡口设备、一机一档设备信息等数据进行集中精准采集，以准确掌握视频监控设备、人像卡口、车辆卡口等前端设备的运行情况。

数据对接中心为运维平台智能诊断和大数据分析挖掘提供基础数据支撑。通过实时性，全面性，精准性的数据采集对前端设备，机房设备，网络安全事件等数据汇总，将各种信息以大数据的形式汇聚，进行有效的内部管理，加强信息的透明程度，最终实现资源信息的整合，从而实现全设备、全网络、全流程的管理与服务。从而确保智能运维平台对各类问题展开全面诊断和分析，以发挥智能运维管理平台的实战应用价值，提高公安部门运维管理水平。

视频监控对接

在对接社会单位监控资源时需要在符合 GB/T 28181-2016 标准的基础上，通过固定 IP 地址、动态域名解析或主动注册等方式。不具备以上功能的，需采用 SDK 方式接入或更换符合接入要求的设备，可通过更换硬盘录像机（DVR）或网络硬盘录像机(NVR)、前端摄像机等设备接入。

根据软件开发工具包（SDK）、接口开发文档及 DEMO 示例，用于视频监控平台应用业务的二次开发。

该 SDK 接口内容，包括视频监控设备组织机构列表、设备信息、实时视频

图像预览、视频解码数据获取。

a.获取设备的所属分组或者管辖单位的信息；

b.获取当前用户有操作权限的摄像机点位列表；

获取摄像机基本信息，如国标编号、设备平台编号、设备名称、IP 地址、端口地址、设备类型（枪机、半球、快球、云台或高清等属性）、行政编码、设备品牌、设备型号、设备分组(或设备所属辖区)、是否支持云台(或云镜)控制、是否支持雨刷控制、设备硬件厂家品牌、视频解码库标识（如海康威视解码库、大华解码、科达解码库、宇视解码库等）。

c.获取解码后的图像。支持多个摄像机同时播放，并通过设置回调函数方式，对每个在做视频播放的设备，进行视频数据获取。视频数据包括拼帧前、拼帧后和解码图片数据。回调函数的设置，支持本地播放、实况播放和录像回放等播放业务。对于视频监控应用开发而言，在视频数据上，必须能够获取到拼帧前的视频数据，以及解码图片数据。

视频实时流回调或解码回调，设置及取消的注意事项。设置及取消回调函数时，只需要提供播放窗口信息，如播放窗口索引（0 到 16）、播放通道号、播放句柄。允许指定用户参数（在回调函数中返回该参数），但无法指定设备编号。允许对指定播放窗口进行取消回调操作。

d.扩展信息：设备建设方、设备维保单位、设备管理方、设备使用方、设备接入时间、所属建设项目、设备启用时间。

## 2.6.5.2. 智能巡检分析中心

### 视频监控图像质量检测算法

视频监控的故障诊断采用人工智能算法领域中的卷积神经网络，实现算法的深度学习功能。系统支持人工智能算法的高频迭代升级，算法适应性强，可快速适应不同场景的故障诊断与识别需求，使用海量数据对卷积神经网络进行训练，并对训练模型进行验证，调整训练参数，以确保算法的检测的高准确率。视频图像质量检测算法可对清晰度异常、彩色条纹、雪花、过亮、过暗、色偏、黑屏、蓝屏，树叶遮挡、角度异常等视频图纸质量进行识别和自动诊断。

### 视频监控网络故障诊断

视频监控联网状态诊断可对取流判断、国标 alive 状态与多源数据交叉验证设备状态进行设备联网状态检测：

- (1) 在线检测：设备在线；
- (2) 离线检测：设备离线；
- (3) 取流超时检测：设备在约定的时间内无法获取到视频码流；
- (4) 失联的检测：设备在视频共享平台上失联。

### **录像完整性检测算法**

检测前端设备的每日录像，检测其整体完整性;根据健康、异常、间歇性三种状况显示。同时系统支持掉线摄像头自动不告警。

系统监测 30 天录像是否被覆盖，如被覆盖系统将自动报警。

可按月、周、天分时段对录像完整性进行检查、

根据录像诊断，生成相关报表。

系统分类显示每个摄像头录像情况，并以颜色代表是否健康、不健康、间接性健康及其他问题，系统并显示 3 个月内的录像诊断信息、显示每个摄像头中断的时间点。

录像状态实时检测反馈：支持对单个或多个设备发起即时检测，并反馈检测结果。

根据录像计划检测录像是否完整，录像丢失时自动产生报警并显示录像丢失时间段。

支持以小时为单位进行录像完整率统计，且以不同的颜色显示录像丢失状态，支持每小时丢失的录像片段的详情查看。

支持按照时间、录像保存天数和关键字进行查询录像，查询结果包含设备的录像状态、录像保存天数、当天录像情况，支持查询结果导出 EXCEL。

### **录像完好性检测算法**

检测前端设备的录像完好性，检测其是否能正常播放及录像画面质量是否正常（不正常画面包括画面丢失、信号中断、遮挡、存储调用失效、画面干扰、画面模糊）；

支持录像中断告警阈值自定义设置。

### **视频监控 NTP 校时检测算法**

检测视频监控设备画面时间戳显示是否正常。以市公安局 NTP 服务器为基

准，使用机器视觉算法获取设备图像，经过图像预处理后，使用卷积神经网络定位时间戳位置后再进行分割，分割后的图片使用 OCR 字符识别，获取图像上的字符信息并利用对比算法对其进行分析，得出时间戳不一致的阈值进行判断，支持阈值后台自定义设置。

该算法主要的解决时间戳的位置不固定、现场环境的光线变换、时间戳受背景影响变半透明化容易与背景融为一体。通过图像预处理及使用图像预识别字符定位字符位置进行定位再进行 OSD 字符识别时间戳，进行智能自动识别比对校时服务器当前时间进行排查。

#### **视频监控图像 OSD 规范识别算法**

检测视频监控设备 OSD 字符是否符合国标 GA/T751-2008《视频图像文字标注规范》；获取图像上的字符信息并利用对比算法对其进行分析标注的字符位置、与画面的边距，得出分析结果，自持阈值后台自定义设定。

#### **车辆卡口流量异常检测**

与厂商平台（或第三方平台）进行数据接口对接，支持车辆卡口平台及单个车辆卡口设备的数据整理，实现车辆卡口流量异常分析。车辆卡口数据异常诊断算法主要对车辆卡口有无数据、过车趋势等进行检测和分析。

#### **人像卡口图像质量检测**

与厂商平台（或第三方平台）进行数据接口对接，检测图像质量故障，人像卡口故障诊断包括人像卡口图像质量、人像卡口数据异常等方面的故障检测。其中，人像卡口质量诊断算法可对人像卡口图像模糊不可用、完全不可用、过暗、过亮等故障类型进行诊断。

### **2.6.5.3. 设备档案管理模块**

#### **接入管理**

待对接设备名称、国标编号、设备通道号、首次同步时间、最近同步时、地点代码的编辑和录入。支持待对接设备单选、多选、全选的方式进行接入、忽略、屏蔽操作，支持模糊查询，支持对接模糊查询、支持对指定同步时间段的查询，支持按照全部/需接入/无需接入三种状态的查询，支持对接设备组合查询及查询条件重置，支持点位管理。

设备接入状态定义：

- (1) 未接入（同步到设备清单但未接入的设备）
- (2) 接入待验收（接入后计划验收的设备，不纳入考核统计，纳入验收统计，必填字段：承建单位等）
- (3) 遗留验收（验收未通过设备）
- (4) 暂不接入（暂时不接入巡检平台的设备，进行黑名单屏蔽，分为本次不接入、短期不接入、永久不接入）
- (5) 调试设备（接入巡检平台，不纳入考核统计，必填字段：调试时长）
- (6) 已接入：已接入巡检平台设备
- (7) 失联：无法被同步到且未在平台进行注销的设备

### 设备基础资料管理

#### (1) 设备运维信息

施工单位下拉框选择添加、设备厂商下拉框选择添加、建设单位添加、建设单位联系方式添加、维保单位下拉框选择添加、维保单位联系方式添加、维保起止日期日历组件添加、保修时间单位（年/月/日）下拉框选择添加、保修期（单位天）添加、设备方向下拉框选择添加、路口类型下拉框选择添加、网络线路类型下拉框选择添加、所属网络线路添加、设备状态下拉框选择添加、使用状态下拉框选择添加、巡检任务分组下拉框选择、网络运行商下拉框选择添加、备注 1 文本输入框、备注 2 文本输入框、备注 3 文本输入框、保存与取消按钮。

#### (2) 操作

批量修改设备基本资料功能、支持设备基本资料选中数显示、修改设备基本资料维保开始时间与结束时间、修改设备基本资料使用状态、修改设备基本资料状态变更类型、修改设备基本资料维保单位、修改设备基本资料设备类型、添加设备使用备注输入文本框、设备基本资料批量确认及取消按钮

#### (3) 查询列表

符合查询条件的设备数量统计、列表设备编号、设备主管单位、设备类型、点位名称、地点代码、设备 ip 地址、设备维保单位、设备使用状态、设备经度、设备维度；

支持列表点位单选、多选、全选功能。

#### (4) 组织机构树

组织机构树

组织机构树显示、隐藏切换

点击组织显示该组织所有设备列表

#### （5）维保信息查询

是否维保到期查询、设备平台接口类型类型、清晰度类别查询、解码接口类型查询、确认状态查询、查询提交按钮及跳转到上层页面、查询条件显示

#### （6）高级查询

可通过关键字进行设备档案信息查询，报表显示样式可以进行横向与纵向切换，用户可自定义列表显示内容，包括设备编号、点位名称、使用状态、设备类型、添加时间、主管单位、操作等报表项都可以自定义配置，支持通过选择设备类型、使用状态等条件进行过滤显示，针对最新更新数据，可以通过一键刷新按钮进行刷新。此外，页面还支持高级查询，通过点击绿色的高级查询按钮，弹出查询弹框，可以通过输入点位名称、IP 地址、设备编号、起始时间、结束时间、设备类型、工作状态、主管单位等字段信息进行高级查询。

支持高级查询按钮及弹窗操作界面、基本信息设备功能单选、多选功能、路口类型下拉框查询、接入时间范围查询及日历组件、同步时间范围查询及日历组件、重点关注预设组查询、状态变更原因查询、是否启用录像查询、设备三天以上未同步查询、接入来源查询。

#### （7）基础资料查询

支持设备资料模糊查询、开头和结尾条件查询、查询条件缩起/展开功能、设备资料类型下拉框单选、多选查询、设备唯一编号查询、设备 ip 查询、建设项目关键字查询、使用状态单选、多选查询、维保单位下拉框单选、多选查询、设备地点代码查询、行政区划下拉框查询、资料查询。

### 2.6.5.4. 运维工单管理

#### 运维闭环工单

（1）支持对人工或系统上报、第三方告警的故障工单进行管理；

（2）支持 KPI 指标展示、进度条动态进行动态显示，指标包括完好率、响应率、完成率、标注率等，并且展示各指标占比详情；（提供产品功能截图并加盖制造商公章）



(3) 支持故障处理各项操作；（提供产品功能截图并加盖制造商公章）

(4) 支持预览图。预览图包含网络状态、视频图像质量、数据质量的检测结果；支持运维流程图，运维流程图以时间轴的形式显示设备运维过程中的关键节点。（提供产品功能截图并加盖制造商公章）

(5) 支持通过主管单位、设备类型、流程状态、故障类型、下发状态等条件对表格内容进行筛选展示，列表内容可进行横向/纵向显示切换，支持关键字搜索查询，可通过点击导出按钮对统计数据批量导出，针对新增数据，通过点击刷新按钮实现数据实时刷新功能。

(6) 支持用户自定义列表显示内容项，可选项包括状态、来源、工单编号、设备类型、故障时间、故障类型、主管单位、预览图、操作等，通过点击选项前的复选框，可进行显示配置。

### 1.报修流程

故障报修（又称运维管理）主要是利用系统自动上报和人工手动上报两种方式，对发生故障的前端设备进行上报，并在系统中形成故障工单，然后由警务人员对故障工单进行分派（又称工单下发），将故障工单分派到各下辖单位，由各下辖单位对所管辖的前端故障设备进行维修，待维修完成后，需等待系统再次巡检（又称系统复检），系统检测通过后，该设备方可恢复工作状态。故障报修流程的关键节点如下所示：

(1) 故障上报。故障上报包括系统检测自动上报和人工上报，系统自动上报会自动添加故障描述；人工上报需要手动添加故障描述，选择故障类型、设备类型等信息，并且需要上传设备故障的现场照片。

(2) 故障处理。支队的相关警务人员将故障工单下发到对应辖区大队，该大队的相关警务人员对故障工单进行处理，安排具体的设备维护商进行现场维修。针对误报的故障工单，可以进行误报处理，无需将工单进行下发。

(3) 完成反馈。对故障维修完成进行反馈，报告设备故障情况及故障维修完成情况，通知可以重新开始使用。

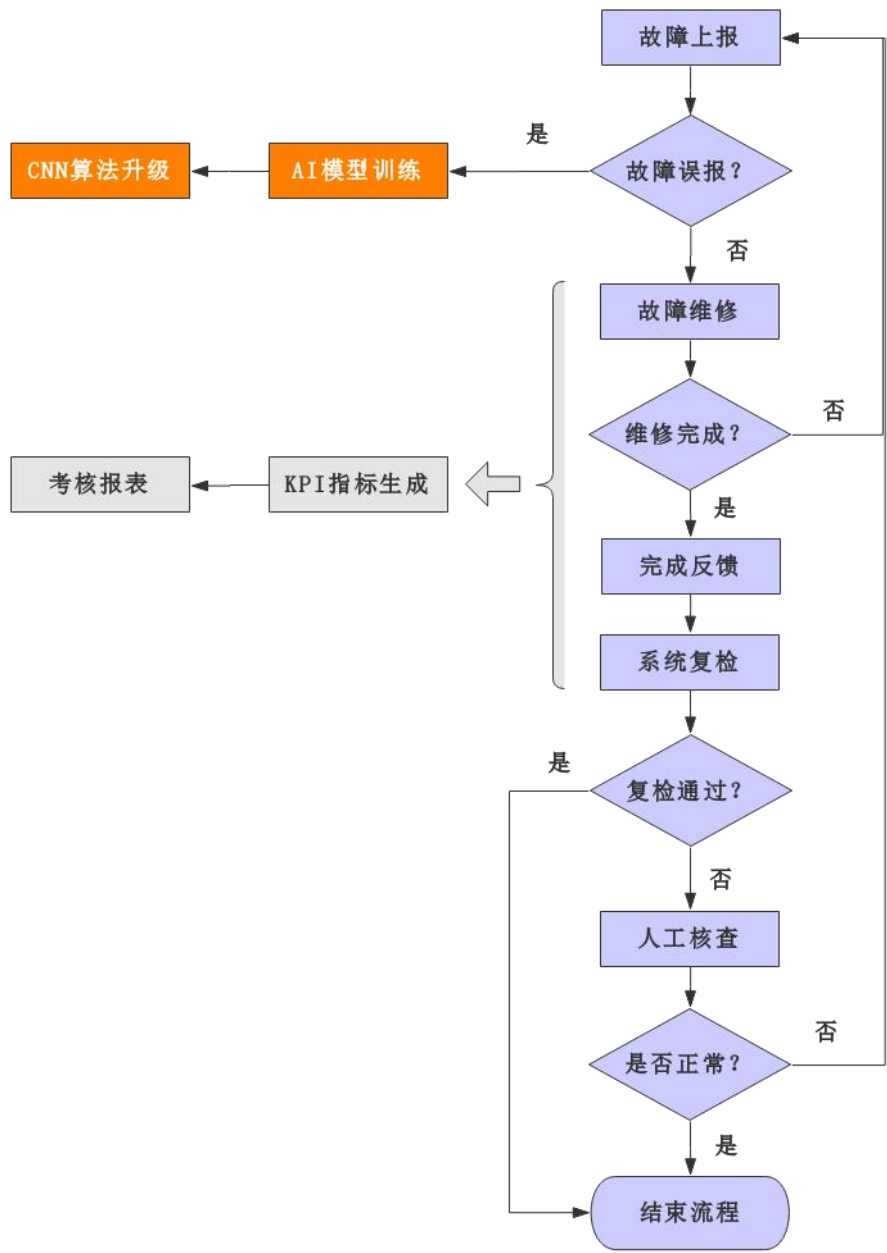
(4) 系统复检。对于反馈完成的故障，将由系统进行复检，判断前端设备是否已恢复正常。

(5) 复检通过。对反馈已完成维修的故障设备，系统自动对其进行复检且通过的，设备状态自动修改为正常状态。

（6）复检未通过。对于反馈已完成维修的故障设备，系统进行复检且未通过的，需要人工进行审核，将由工作人员决定该故障流程下一步状态。

（7）人工处理。工作人员对系统复检未“不通过”对故障点位进行人工核查，对实际中已可正常使用的设备，工作人员需手动确认“通过”，经人工核查后，对仍不能正常使用的设备选择“返工”处理。

（8）误报。工作人员对系统复检未“不通过”对故障点位进行核查，对属于系统误报的故障选择“误报”处理，系统将此类故障作为样本进入 AI 训练样本进行训练迭代。



报修流程图

2.人工上报

人工上报模块用于用户对前端设备进行故障上报操作，人工进行故障上报时，需要填写的信息包括故障点位、故障类别、故障时间、故障描述、文件上传等必填项，均用红色星号“\*”标识，若有不填写，则不能进行人工上报操作，其中，故障点位项可以通过点击右侧紫色选择按钮进行选择，点击选择按钮后，弹出选择框，可直接勾选对应的点位信息前方的复选框进行选择，点位

选择信息列表包括摄像机 id、设备名称、国标编号、主管单位等字段，可以通过搜索框进行搜索查询，点击搜索框右侧的刷新按钮，可以实现点位信息列表刷新。

为了用户填写方便，故障类别和故障描述项均是通过下拉列表方式让用户点击选择进行自动填写。填写故障时间时，点击时间按钮，弹出时间选择弹框，鼠标选中后，该项自动填写故障时间，方便快捷，节省用户故障上报时间，简化用户故障上报流程。

点击选择文件按钮，可以选择相应的文件进行上传操作，另外，为了提示应上传的文件格式，按钮下方标有红色字体的上传文件提示说明，提示上传文件的类型（JPG、PNG、GIF）、文件数量等。

### 停用与恢复管理

设备停用功能适用于特殊场景下设备无法继续使用的情況，如道路施工、机房改造、设备改造、网络故障等场景致使设备无法正常使用或需要停止设备维修工作，以待道路施工完成、机房或设备改造完成、网络故障修复等。设备停用流程包括：

（1）设备停用申请。对于道路施工、机房改造、设备改造、网络故障等特殊场景造成设备无法正常使用的情況，可通过申请设备停用，使设备处于停用状态。须填写停用时间段、状态去向、报备点位、停用原因、设备停用计划审批表附件等信息。

（2）设备停用审核。对于申请的停用工单，由警务人员根据申请原因及实际情况，决定是否允许停用，批准回复内容包括批准意见、状态去向、批准描述等信息。

（3）设备停用通知。对于审核通过的停用工单，通知到各下辖单位，并由各下辖单位查收确认。

（4）停用到期提醒。在设备停用到期的前一天，及到期后 10 天内，提醒管辖单位申请停用延时，或申请设备恢复。

### （5）停用记录模块

用于对停用的点位设备进行统计和管理，页面中报表内容包括流程状态、设备名称、设备编号、状态去向、计划开始时间、计划截止时间、申请单位、审核时间等字段信息，为了方便用户筛选信息，可以点击列表上方的主管单

位、流程状态等筛选条件进行过滤显示，如，点击流程状态按钮，弹出下拉列表框，列表框中可以选择待批准、已批准、未批准、已恢复等筛选项。为满足不同用户需求，系统支持列表的横向/纵向切换显示，通过点击显示切换按钮，实现数据列表的横向与纵向显示切换。点击列表自定义设置按钮，用户可以设置列表显示内容项，在设置弹框中，可以通过勾选流程状态、设备名称、设备编号、状态去向、计划开始时间、计划截止时间、申请单位、审核时间等项前的复选框，实现对应项的显示与隐藏设置。除了设置主管单位与流程状态等条件外，可以通过在搜索框中输入流程状态、设备名称、设备编号等关键字进行模糊查询。针对新增信息，可以通过点击一键刷新按钮实现列表内容的实时更新，可以通过点击批量导出按钮，实现对列表信息进行批量导出功能。

#### (6)计划审批

计划审批模块用于对设备的停用与恢复、报废、拆除等计划申请、设备恢复等功能。计划审批列表项包括流程状态、工单编号、状态去向、申请时间、计划开始时间、计划截止时间、申请单位、审核描述、操作等，用户可以根据主管单位、流程状态、计划类型等条件进行信息筛选，而且数据列表可以进行横向/纵向切换显示，可对信息列表进行一键刷新操作。用户可自定义列表显示内容项，可以设置的选项包括流程状态、工单编号、状态去向、申请时间、申请原因、计划开始时间、计划截止时间、申请单位、审核时间、审核描述、操作等，通过勾选选项前的复选框，实现该项的显示设置。

对设备的停用与恢复、报废、拆除进行计划申请时，点击绿色的计划申请按钮，弹出申请弹框，需要填写的内容包括状态去向、报备点位、申请原因、开始时间、结束时间、申请描述、文件上传等字段。其中，报备点位项可自动填写，点击紫色的选择按钮，弹出点位选择弹框，在点位选择弹框页面内，可通过设备名称、国标编号、主管单位等关键字进行点位信息搜索，点击刷新按钮，可进行点位列表刷新操作，申请原因通过下拉列表方式进行自动填写，点击选择按钮右侧的绿色导入按钮，可实现点位批量导入操作。针对批量导入操作，系统提供模板下载功能，通过点击文件上传下方的蓝色字体，浏览器自动下载计划申请表模板。

设备恢复功能主要是针对设备停用到期后需要恢复正常使用状态，点击蓝色的设备恢复按钮，弹出设备恢复弹框，可通过勾选设备信息前的复选框，是

新啊对设备进行批量恢复操作，该列表支持关键字搜索功能，通过设备名称、主管单位等关键字进行信息搜索，还可点击一键刷新按钮进行列表信息刷新操作。针对人工发起设备恢复申请，系统自动审核，针对停用到期的设备，系统会自动进行恢复。

数据采集模块用于对巡检平台中的基础设备信息进一步完善，特别是针对基础信息残缺的进行补全，点击橙黄色数据采集按钮，弹出数据采集弹框，红色字体提示数据采集步骤，清晰简洁易懂，先点击绿色批量导出按钮，将巡检平台中的相应大队所有设备信息导出，点击导出按钮后，浏览器自动下载 Excel 形式的设备基础信息表，表格内容包括组织、设备名称、设备类型、国标编号、运维形式、运维单位名称、运维开始时间、运维截止时间、运维单位联系人等字段内容，将以上字段内容全部补充完整后，点击蓝色字体下载模板，将补全设备信息粘贴到模板上，然后点击选择按钮，将该文件进行上传，即可实现数据采集过程。

针对新增卡口报备情况，点击报备按钮，弹出报备弹框，弹框中针对如何进行了友好提示和指导帮助，首先点击蓝色字体报备流程图，查询和了解相关报备流程，点击蓝色设备接入报备表，浏览器自动下载报备表，用户根据实际情况对申请时间、申请单位、报备描述、报备总数、设备厂商、设备类型、数量等内容进行填写，然后将该报备表进行上传即可。

针对用户已报备的工单，需要审核人员进行审核批准，点击操作栏中的批准按钮，对新增计划进行审批，弹框中信息包括批准意见、状态去向、批准描述、附件下载等，审核人员可快速对设备报备信息做出审批操作，方便、效率高。

### **重要工单**

(1) 支持将重要设备列入重要点位分组，并加强巡检，一经发现异常立即派单，并发送给运维人员和设置好的角色。

(2) 支持点位编号校验。

## **2.6.5.5. 运维考核管理**

### **故障上报统计**

故障上报统计模块主要是对人工上报、系统上报等方式上报的故障情况进

行统计，页面顶部是 KPI 综合统计，下部分是最新巡检获取的故障上报数据。KPI 综合统计以动态进度条形式对完好率、响应率、完成率、标注率、在线率、录像完好率等考核指标进行展示，包括各指标的数量和占比等详情数据展示。最新巡检详情统计，将人工发起、系统发起的设备故障进行统计展示，表格内容包括流程状态、超时统计、故障上报来源、点位名称、设备类型、故障时间、故障类型、责任单位、故障上报人、故障预览图、操作栏等字段，支持一键刷新和一键批量导出功能，可通过关键字进行查询，显示样式切换，用户可自定义列表显示内容，支持通过选择流程状态、设备类型、故障类型、故障上报来源等条件进行过滤显示。

### 故障分类统计

故障分类统计用于各辖区的故障维修情况及新增故障进行统计，故障分类报表包括各辖区主管单位、设备总数、故障上报总数、新增故障、正在维修、待响应、已完成等字段，支持通过设置时间段、设备类型进行查询，支持对报表的一键导出功能。

### 维修统计

维修统计报表用于对点位设备的维修记录及维修时间进行统计，统计列表内容包括序号、维修单号、设备名称、故障时间、响应时间、反馈时间、设备类型等字段，支持通过设备名称、地点代码、设备编号、设备类型、响应时间段、反馈时间段、上报时间段等进行维修记录查询，支持批量导出功能。

### 停用统计

停用统计报表用于对停用的设备进行统计和分析，停用统计报表包括流程状态、设备名称、设备编号、状态去向、计划开始时间、计划截止时间、申请单位等字段内容，支持一键刷新和一键批量导出功能，可通过关键字进行查询，显示样式切换，用户可自定义列表显示内容，支持通过选择流程状态、主管单位等条件进行过滤显示。

## 2.6.5.6. 用户管理模块

### 账号管理

账号管理用于对登录系统的账号进行管理，支持新增账号、对已有账号进行修改、修改登录密码等，系统支持对已有账号进行一键删除操作。用户信息

应包括账号、用户基本信息（如用户名称、联系方式、工作单位、证件号码等）、角色名称、角色等级、账号启用状态等内容，支持根据关键字搜索账号信息。

### 权限管理

权限管理用于对用户账号的数据权限和功能权限进行配置和管理，用户权限管理设计符合 RBAC 规范，支持对角色进行新建、编辑、删除等操作，支持对已创建角色的数据权限、功能权限等方面进行授权管理。

此外，支持用户组管理，将相应的权限赋予该用户组，用户可以加入该用户组并获取相应权限，具体可参考组织机构相关内容。

#### 1.功能权限

功能权限用于界定用户可以在平台中开展的操作行为范围，包括查询、新建、修改、删除等权限。

比如，故障维修结果审核权限应归属于公安（或交警）主管部门，维保单位不具有该权限，只具有申请权限，因此维保单位登录平台时，则不能访问到故障维修审核页面及相关功能页面。

某些设备敏感信息，低级别账号只具有查询功能，不具有修改和删除权限，因此该账号访问的相关页面不显示针对该敏感数据的修改按钮和删除按钮。

#### 2.数据权限

数据权限用于界定用户可以管理的设备类型范围、设备历史数据范围、区域范围。其中，设备类型范围包括视频监控、车辆卡口、人像设备、超级卡口、网络设备、服务器等，区域范围包括市（公安局、交警支队）、区县（公安分局、交警大队）、乡镇（派出所、交警中队）等。

例如，视频监控维保单位只可以获取到本单位所负责的视频监控信息，不可以获取到其他设备信息，如车辆卡口数据，亦不可以获取到非本单位负责的视频监控信息。

某区公安分局普通账户通过该平台只能查询到该区的设备信息，不可以获取到其他区、乃至全市范围内的设备信息（除非获得相应授权）。

关于历史数据范围的界定，例如，高级别权限的账号可以获取设备所有历史记录信息，低级别的账号只可获取最近 7 天的历史数据。



## 组织管理

支持对设备所属原有组织机构信息进行管理，包括同步、修改、删除等操作。支持新建组织机构，并对新建组织机构进行修改、删除操作，支持将设备赋予该组织机构。

支持用户加入/退出组织机构。

组织结构可以对账号所属的组织结构进行新建、编辑、删除等操作，同时可对用户所属的组织机构进行权限设置，通过组织类型、启用状态进行过滤筛选，并可以在输入框中输入部门编号、部门名称等字段进行查询搜索。新建组织内容包括上级单位、网络接口类型、组织类型、组织级别、工作职责、排序号、功能职责、是否统计、同级序号、开始工作时间、结束工作时间、联系人、联系人电话、联系人地址等字段信息进行配置，实现对组织结构的定义。

### 2.6.5.7. 安全管理

安全管理支持对用户从平台登录、具体操作、退出等全过程进行全面监督管理，确保账号密码、用户行为等处于信息安全保障之内。

#### (1) 登录安全

支持 UKEY 登录方式，UKEY 内置 SM2 国密算法，支持 jsp、asp、php、vbnet、c# 各种开发语言，内置 172K，支持 IE、360、腾讯、遨游、opera、google、firefox、chrome 等浏览器。使用 UKEY 直接通过 USB (通用串行总线接口) 与计算机相连，通过 UKEY 认证系统里面的组件 SecureLogon 可实现安全登录的功能，有效防止非法登录。UKEY 认证系统的密码总管组件 SecureEntry 可以自动记忆存储基于网页和基于程序的密码，直接插入电脑即可实现系统登录，无需输入账号密码。UKEY 认证系统里面的文件安全分发功能组件 SecureVia 提供多种加密功能，可保证文件传输的安全性和文件存放的安全性。

#### (2) 操作日志

用户日志页面用于记录用户在该平台上的所有操作，平台记录该账号关联的 PC 端和移动端上的操作日志，具体包括登录/退出时间、访问页面、操作事件、访问时间等内容，支持根据关键字进行日志查询。此外，系统还支持日志记录的删除和批量导出功能（注：需要高级别权限账号）。

#### (3) 水印加密

为进一步提高用户操作安全性，防止机密数据的人为泄露，平台采用数字水印加密技术，数字水印是一种基于内容的、非密码机制的计算机信息隐藏技术。它是将一些标识信息（即数字水印）直接嵌入数字载体当中（包括多媒体、文档、软件等）或是间接表示（修改特定区域的结构），且不影响原载体的使用价值，也不容易被探知和再次修改。但可以被生产方识别和辨认。通过这些隐藏在载体中的信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印是保护信息安全、实现防伪溯源、版权保护的有效办法。采用位置加密和灰度值加密相结合的双因子加密方法对加密，混沌序列可以达到安全系数极高的数字水印加密效果。

## **2.6.5.8. 项目运维管理**

### **2.6.5.8.1. 运维供应商管理**

运维供应商是指各类视频监控类项目的软硬件运维服务提供商，运维供应商保证了各类系统的运行稳定性。建设运维供应商信息库，是后续实现运维人员、工时、安全、考核管理的基础。

#### **（1）供应商管理**

建立供应商信息库，实现供应商信息集中管理，统一供应商编码，相关人员录入的供应商信息，由责任部门负责审核，审核完毕同步供应商信息库。

1、支持供应商信息的申请、审核、变更、同步等功能。

2、支持供应商信息与项目合同关联。

3、供应商信息应包括基本信息、身份类信息、资质类信息、经营类信息、财务类信息、证明类信息、代理类信息、供应商和大数据中兴合作过程中系统自动建立起来的信息等。

通过供应商信息库，可以随时查询供应商信息。

#### **（2）变更管理**

对供应商变更的基础信息，变更的供应商信息由责任部门负责审核，审核通过后信息可同步在本系统中实时变更，支持供应商信息历史版本查看。

#### **（3）删除管理**

提供供应商信息删除功能，删除供应商操作由责任部门负责审核，审核通

过后信息可同步在本系统中实时删除，删除信息自动留痕。

#### **（4）供应商查询**

提供关键词在线检索功能，可在页面内查询所需要的供应商信息。

### **2.6.5.8.2. 运维预警**

对项目运维合同到期的关键时间节点进行监控和预警提醒，支持新建智能化、信息化项目合同到期运维节点预警及运维项目合同到期预警，及时完成各类智能化信息化项目运维合同。

#### **（1）新建项目合同到期预警**

根据新建项目合同内运维服务到期时间节点要求，支持进行运维服务到期时间临期提醒功能。

#### **（2）运维项目合同到期预警**

根据运维项目合同内服务到期时间节点要求，支持进行运维服务到期时间临期提醒功能。

### **2.6.5.8.3. 运维人员池**

通过建设运维供应商运维人员池，对运维人员的工时信息进行及时统计，为运维供应商的评估提供事实依据。

#### **（1）运维人员管理**

相关人员可在平台内录入运维人员基础信息，录入字段包括人员姓名、人员编号、等级、角色、加入时间、离开时间、所属供应商、关联合同等，支持运维人员信息修改。

#### **（2）运维人员查询**

用户点击用户查询按钮，进入查询页面，系统提供姓名、编号、供应商这三个维度进行查询，查询结果在下方已列表展示，支持详情查看。

#### **（3）运维人员退出管理**

提供离职运维人员退出管理功能，可对退出人员进行信息删除操作，删除该人员系统内个人信息。

#### 2.6.5.8.4. 运维人员工时管理

各供应商运维人员的工时付出与运维供应商的考核结果息息相关，通过建设运维人员工时管理模块，对所有运维人员的工作成果进行日常管理。

##### (1) 工时上报

可以根据设定的工时上报周期（每天、每周、每月），由运维人员在系统内上报工作内容和工时信息。

##### (2) 工时审核

对运维人员在系统内上报工作内容和工时信息，由责任单位负责审核上报信息真假。

- 1、系统按设定周期向运维人员推送运维工时填报待办任务；
- 2、运维人员工时填报总数不能大于系统提供的出勤数；
- 3、运维人员工时填报总数不能大于系统提供的在职时间；
- 4、按项目汇总运维项目工时，责任单位审核通过后工时数据生效。

#### 2.6.5.8.5. 运维安全管理

责任单位对各运维供应商在项目日常运维安全中的设施管理、网络安全、操作系统安全、用户访问授权、密码管理、防病毒管理、系统补丁管理、介质管理、信息交换管理、安全监控和审计管理、数据备份和恢复管理等各类运维安全监管项进行监督。

##### (1) 运维安全检查

根据设定的检查周期（每周、每月、每季度、每年），由责任单位对运维供应商发起运维安全检查，并录入运维安全检查结果，根据结果生成各供应商运维安全评分。

##### (2) 运维安全工单

对运维安全检查发现的运维问题，向相应运维供应商推送运维安全整改工单，由运维供应商在系统内接收工单。

##### (3) 运维安全整改反馈

运维供应商接收整改工单后，完成安全整改，并将整改反馈已工单处理形

式反馈责任单位，由责任单位确认完成工单闭环。

支持项目运维安全评分及整改工单查询功能

#### **2.6.5.8.6. 运维供应商考核**

项目建设单位协同有关部门通过系统发起运维供应商考核流程，项目建设单位按考核需求提供运维有关资料。责任单位将评价结果作为下一年度运维安排的重要依据。

##### **（1）供应商考核模板**

相关人员维护供应商评估时的模板名称以及模板中的各指标项详情和指标等级设置信息，用于为评估的合同分配打分模板，打分人员按照模板定义的指标进行评分。

##### **（2）供应商考核**

相关人员发起供应商考核，可发起综合实力评估、合同额评估、季度评估、履约评估、年度综合评估等考核评估，主观项由项目建设单位及有关单位填写后，经责任单位审核生成考核结果。

## 2.7. 安全管控要求

### 2.7.1. 安全功能

#### 2.7.1.1. 边界安全管控

六安市裕安区公共场所视频监控资源整合域作为一个与其他网络隔离的视频传输应用传输网，在与其他网络连接时按照公安部的有关规范和等级保护的原则，严格部署网络安全隔离设施，确保视频传输网边界清晰、管控有效。

在整合域部署边界安全运维平台，通过采集业务日志、流量日志、系统日志，对进出边界接入平台的人、事、数据、设备进行集中监管、安全审计。向用户集中展示边界建设现状，辅助用户掌握边界违规建设情况，对边界运行状态进行监控与记录，当出现违规业务、数据窃取等行为，即可报警并记录，为用户提供事前的防护、事中的管控、事后的追溯。

#### 2.7.1.2. 安全风险检测

整合域部署基于分布式入侵检测系统构架的网络入侵检测系统，采用自主的安全引擎，综合使用会话状态检测、应用层协议完全解析、误用检测、异常检测、内容恢复、网络审计等入侵分析与检测技术，全面监视和分析网络的通信状况。在入侵监控的基础上，遵循 CSC 关联安全标准，可主动发包或与多种第三方设备联动来自动切断入侵会话，实现实时有效的防护，为网络创建了全面纵深的安全防御体系。

部署安全风险检查系统，系统具备漏洞扫描、WEB 扫描、弱口令扫描、安全基线检查、变更检查等功能；实现视频传输网内所有设备安全漏洞的及时发现。

#### 2.7.1.3. 终端安全管控

在整合域部署内网安全管理系统和网络防病毒系统，制定安全策略实现补丁和病毒库的安全更新，实现视频传输网内所有设备安全漏洞的实时修复。

#### 2.7.1.4. 设备安全准入

准入控制系统通过对整合域内设备自动发现与注册管理，对终端提供各种控制、运行监测与管理。以旁路控制技术为主，秉承不改变现有网络结构的特性，为用户解决终端入网的合规性要求，支持包括身份认证、安全隔离、安全修复、可配置的多种准入控制手段和访问控制手段等功能，满足整合域对专用网络边界、终端安全接入防护的相应要求。

支持通过扫描监测、流量分析、脚本分析发现网络设备非授权违规外联；支持非法 DHCP、违规 DNS、匿名 FTP 等非法网络服务监测预警；支持边界发现、网中网发现。

#### 2.7.1.5. 全网安全审计

部署运维堡垒机，对整合域业务环境下的用户运维操作进行控制和审计的合规性管控，避免采用直连或远程登录服务器等较低安全级别运维方式。

部署日志审计系统，对整合域网络设备、其他软硬件系统（包括操作系统、数据库、中间件、应用软件及各类硬件设备等）的运行状况、用户访问操作行为等进行日志审计。

部署视频应用安全审计系统，实时记录网络中的视频访问行为，对视频操作进行细粒度审计和合规性管理，发现实时入网设备、发现非授权访问行为、发现授权用户异常访问行为，对敏感信息泄露、侵犯公民隐私的非法行为进行取证、溯源。

### 2.7.2. 密码安全要求

#### 2.7.2.1. 物理和环境安全

六安云计算中心在设备间部署符合 GM/T 0036-2014 标准要求《采用非接触卡的门禁系统密码应用指南》的电子门禁系统对进出机房人员进行身份鉴别和进出记录数据的存储完整性保护。使用 SM4 算法进行密钥分散，实现门禁卡的“一卡一密”，并基于 SM4 算法对人员身份进行鉴别。

在系统环境监控区部署符合 GM/T0030-2014《服务器密码机技术规范》的

服务器密码机，使用 HMAC-SM3 技术对电子门禁系统进出记录和视频监控系統视频记录等数据进行完整性保护，其中 HMAC-SM3 密钥由环境监控区服务器密码机生成，存储在服务器密码机中，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。

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 GM/T0036-2014《采用非接触卡的门禁系统密码应用指南》、GM/T0030-2014《服务器密码机技术规范》、GM/T0028-2014《密码模块安全技术要求》的电子门禁系统和服务器密码机实现。

### 2.7.2.2. 网络和通信安全

在系统运维管理区部署符合 GM/T0025-2014《SSLVPN 网关产品规范》的 SSLVPN 安全网关，建立安全的集中管理通道。

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《SSLVPN 安全网关产品规范》（GM/T 0025-2014）、《智能密码钥匙技术规范》（GM/T 0027-2014）、《密码模块安全技术要求》（GM/T 0028-2014）的 SSLVPN 安全网关、智能密码钥匙 USBKey、密码服务平台、服务器密码机，使用的密码算法包括 SM2、SM4/CBC 和 SM3/HMAC。

### 2.7.2.3. 设备和计算安全

在本系统安全统一管理区 PC 端部署安全浏览器，并向系统管理员配发 USBKey，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护，防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。

在本系统应用服务区部署符合 GM/T 0030-2014《服务器密码机技术规范》的服务器密码机，并在应用服务器外挂符合 GM/T 0027-2014《智能密码钥匙技术规范》的 USBKey，应用服务器中所有重要程序或文件在生成时通过调用服务器密码机使用 SM2 数字签名技术进行完整性保护；使用或读取这些程序和文件时，通过 USBKey 进行验签以确认其完整性；公钥存放在 USBKey 中。

调用部署在应用服务区中的服务器密码机，使用 HMAC-SM3 对应用服务器、数据库服务器等设备的日志记录进行完整性保护，防止日志记录被篡改。



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、密钥管理由安全浏览器、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》标准规范的 USBKey、服务器密码机实现。

#### 2.7.2.4. 应用和数据安全

在网络接入区边界部署符合 GM/T 0026-2014《安全认证网关产品规范》标准规范的安全认证网关，在系统密码基础设施区部署符合 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》的证书认证系统，通过证书认证系统向移动端密码模块（二级）、安全认证网关配置数字证书，实现移动端登录应用用户的安全身份鉴别，防止非授权人员登录；在本系统业务终端接入区 PC 端部署安全浏览器，在网络接入区边界部署符合 GM/T 0025-2014《SSL VPN 网关产品规范》标准规范的 SSL VPN 安全网关，并向相关用户配发 USBKey，实现对 PC 端登录应用用户的安全身份鉴别，防止非授权人员登录应用系统。

在网络接入区部署符合 GM/T 0029-2014《签名验签服务器技术规范》相关标准规范的签名验签服务器，使用数字签名技术对身份认证系统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。

在应用服务区分别部署符合 GM/T 0030-2014《服务器密码机技术规范》标准规范的服务器密码机和符合 GM/T 0025-2014《SSL VPN 网关产品规范》标准规范的 SSL VPN 安全网关，应用通过调用服务器密码机，对 PC 端登录用户身份鉴别数据、系统中流转的重要数据进行传输、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保护；PC 端安全浏览器与 SSL VPN 安全网关之间使用合规的 SSL 协议，建立安全的数据传输通道，实现数据传输机密性、完整性保护。应用通过调用部署在应用服务区的服务器密码机，使用 HMAC-SM3 对应用日志记录进行完整性保护，防止应用日志记录被非授权篡改。

在密码基础设施区部署符合 GM/T 0031-2014《安全电子签章密码技术规范》、GM/T 0033-2014《时间戳接口规范》标准规范的电子签章系统、时间戳服务器，使用密码技术对在信息系统中流转的重要数据进行数字签名、验签，并

加盖时间戳，实现操作行为的不可否认性。

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、密钥管理由安全浏览器、符合 GM/T 0027-2014《智能密码钥匙技术规范》、GM/T 0029-2014《签名验签服务器技术规范》、GM/T 0030-2014《服务器密码机技术规范》、GM/T 0031-2014《安全电子签章密码技术规范》、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》、GM/T 0033-2014《时间戳接口规范》、GM/T 0014-2012《证书认证系统密码协议规范》、GM/T 0028-2014《密码模块安全技术要求》等标准要求的 USBKey、签名验签服务器、服务器密码机和证书认证系统实现。

### 2.7.2.5. 密钥安全管理

密钥是密钥安全管理的核心，在密钥的生成、密钥分发、密钥更新、密钥撤销、密钥恢复、密钥归档、密钥备份和恢复等整个生命周期过程中，都需要通过密码技术对密钥进行保护，以确保密钥的全生命周期安全。

本次建设选用通过检测认证的服务器密码机、SSL VPN 安全网关、智能密码钥匙 USBKey、LRA 注册信息点、签名验签系统等商用密码产品提供的密钥管理方案，并严格遵照其要求进行使用和实施。

同时，在各密码应用子系统中，采用符合《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》（GM/T0034）标准，并获得商用密码产品认证证书的密钥管理系统提供的密钥管理服务实现密钥的安全管理，对重要配置文件、数据的存储加密、完整性保护提供相关密钥的全生命周期管理；同时，通过对接每个业务系统的应用和数据层，结合密码服务平台实现相关业务数据的全生命周期管理。

系统使用的数字证书由证书认证系统颁发，制定严格的 CA 管理操作规程，保证密钥等信息和系统的部署、使用安全。

## 2.7.2.6. 安全管理方案

### 2.7.2.6.1. 制度

根据《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》中安全管理制度方面的要求，制定与本系统相适应的密码安全管理制度和操作规程，内容至少包含密码建设、运维、人员、设备、密钥等 6 个方面，并同步在单位现有的制度发布流程中补充密码相关管理制度发布流程，待新制定的密码安全管理制度和操作规程内部评审通过后，按照密码相关管理制度发布流程予以发布并遵照执行。

密码安全管理制度和操作规程发布后，每年年底，在本单位内部组织专家和密码相关人员对密码安全管理制度和操作规程在使用过程中的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

### 2.7.2.6.2. 人员

根据《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》中安全管理人员方面的要求，对本系统现有的人员管理制度进行补充和完善。

一是设置内部密码专题培训机制，每 6 月组织一次，由内部人员或聘请外部专家担任培训讲师（具备国家认证的信息安全人员高级资质），内容涉及密码相关法律法规和标准规范、商用密码应用、商用密码应用安全性评估等多个方面，使相关人员了解密码相关的法律和法规，掌握密码基本原理，并遵照执行；

二是在本系统完成密码应用建设后，安排项目建设单位、相关密码设备厂商对本系统部署使用的所有密码产品进行操作培训，确保相关人员能够正确配置使用本系统中部署的密码产品；

三是结合本系统情况，分别设立密钥管理员、安全审计员、密码操作员等岗位，明确各岗位职责，每个岗位均由 2 人担任；

四是在现有的安全管理制度中，补充密码相关人员考核、奖惩、保密、调离制度，每年对密钥管理人员、安全审计人员、密码操作人员组织一次考核，对考核成绩优异的予以表扬和奖励，考核成绩不合格者，进行批评教育；密钥

管理人员、安全审计人员、密码操作人员与单位订保密协议，承担保密义务，相关人员若要调离岗位时，按照制定的人员调离制度承担相应的保密义务。

### 2.7.2.6.3. 实施

完成本方案编制后，委托密评机构对本方案进行评估，评估通过后，将本系统密码应用方案向当地密码管理部门备案，并同步对本系统进行密码应用建设，选用通过检测认证合格的签名系统服务器、SSL VPN 安全网关、智能密码钥匙 USBKey 等商用密码产品，合规、正确、有效的建设密码保障系统。

依据评估通过的密码应用方案建设完成后，委托密评机构对本系统进行密评，密评通过后上线运行，上线运行后，每年对本系统进行一次密码应用安全性评估，并根据评估意见进行整改。当本系统在运行过程中发现重大密码应用安全隐患时，将停止系统运行，制定整改方案，按照整改方案对系统进行整改和密码应用安全性评估，评估通过后重新上线运行。

### 2.7.2.6.4. 应急

根据《GB/T39786-2021 信息安全技术信息系统密码应用基本要求》中安全管理应急方面的要求，对本系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施；当本系统发生密码相关安全事件时，在事发后 3 小时内向建设使用单位进行报告；事件处置完成后 2 个工作日内，向建设使用单位汇报安全事件发生情况及处置情况。并在时间处置完成后，向星系系统主管部门以及归属的密码管理部门报告事件发生情况以及处置情况。

### 2.7.2.6.5. 密码安全测评

裕安区公共场所视频监控资源整合共享汇集多网系接入，多业务汇集，上下联通、左右衔接，为保证各类数据在传输、应用、共享过程中的保密性、持续性、完整性，严格执行和落实《国家网络安全法》、《密码法》等相关法律、标准、政策规范要求，开展和建设信息网络安全和密码应用建设与测评，为业

务系统提供立体、纵深的安全保障防御体系，形成“事前有防范、事中有应对、事后可追溯”的安全闭环能力，提升公共场所视频监控资源整合共享系统整体的安全防护能力。

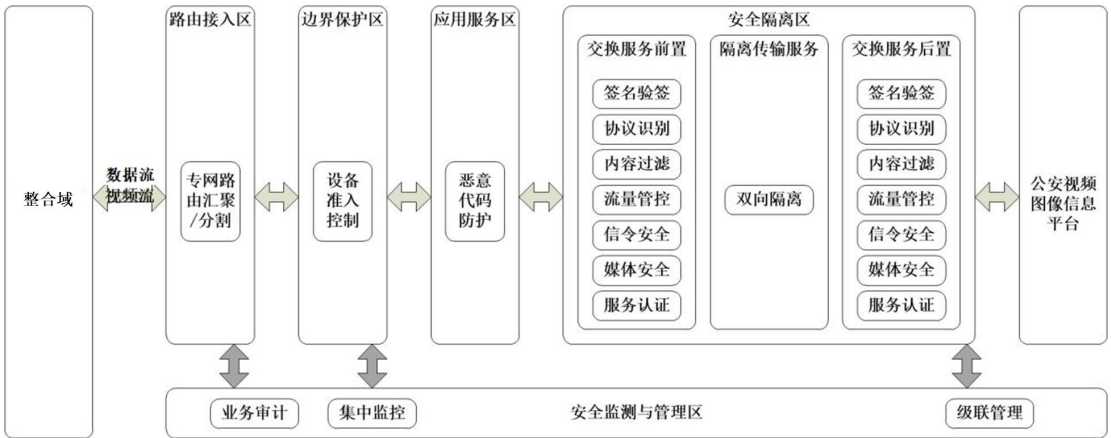
裕安区公共场所视频监控资源整合共享系统密码应用测评参照等级保护测评等级三级相关要求，进行同等级同步商用密码应用测试评估。

2.7.3. 整合域与公安视频专网联网共享安全

2.7.3.1. 技术要求

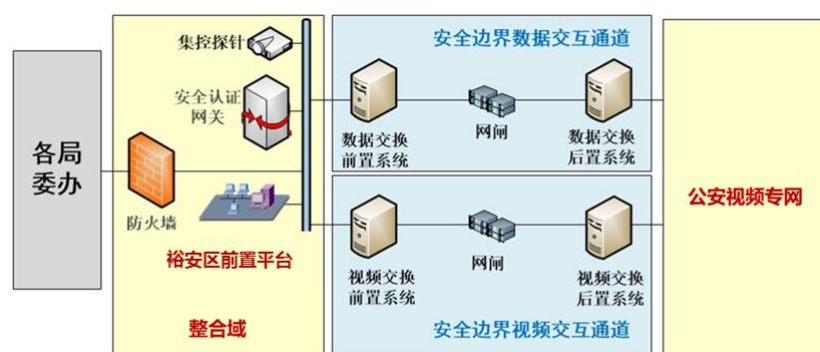
按照《GA/T 1788.3-2021 公安视频图像信息系统安全技术要求 第 3 部分：安全交互》要求，建设整合域与公安视频专网之间的横向边界交互平台，实现整合域与公安视频专网之间视频资源和数据资源的交互。要求平台具备安全审计、安全隔离、视频控制信令格式检测、视频数据格式检测、视频数据与视频控制信令分别处理和传输、数据安全、数据传输方向可控、集中监控报警等安全功能。

整合域与公安视频专网共享边界功能架构共包含五个安全域：路由接入区、边界保护区、应用服务区、安全隔离区和安全监测与管理区，每个安全区域实现不同的安全功能。



整合域与公安视频专网共享边界功能架构

## 2.7.3.2. 建设方案



整合域与公安视频专网联网共享安全建设方案

### 2.7.3.2.1. 防火墙

采用防火墙设备对“裕安区前置平台”进行安全防护，启用访问控制功能，制定详细的访问控制策略，实现端口级、细颗粒度的访问控制，保障对访问行为的有效管控。防火墙内置入侵防御功能，通过实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试，当发现网络违规攻击行为和未授权的网络访问时进行实时阻断。

### 2.7.3.2.2. 安全认证网关

用于外部网络终端设备以及用户的认证授权管理。主要功能包括:用户身份认证、设备认证、访问控制、权限管理、传输加密、终端加固、监控审计等。

### 2.7.3.2.3. 视频应用安全审计系统

部署一套视频应用安全审计系统，从裕安区前置平台的应用日志以及网络流量入手，实现对用户、设备、应用访问服务/数据的行为过程的完整记录，并在日志审计基础上开展异常行为分析，实现“追踪的下去、查的到源头、取的到证据、异常可发现”能力，规范公共安全视频图像信息资源使用和管理，保障公民、法人和其他组织的合法权益。防止因为数据盗取、违规操作、越权访问等造成公安敏感信息泄露、数据破坏、侵犯公民隐私的现象。

#### 2.7.3.2.4. 视频图像信息系统安全

对登录视频图像信息系统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；

对用户访问进行授权，并根据用户的不同角色、级别、所属机构、任务和场景进行鉴权、授权，实现功能级访问控制；

对视频图像信息系统应用内容进行安全防护，防止自动化工具攻击和数据爬取；

记录视频图像业务应用的操作日志，操作日志应包含操作人、操作时间、操作终端、操作对象、操作条件、返回结果等；

能够基于业务日志的行为发生 IP、行为发生时间范围、行为发生时间周期、行为结果等进行分析，分析用户异常行为。

#### 2.7.3.2.5. 数据交换系统

数据交换系统由数据交换前置服务器和数据交换后置服务器组成，部署在安全隔离区，用于内外网之间的数据交换，实现对交换数据的内容检查过滤；同时实现由内部监管系统对外部网络、应用、设备的监管，以及日志收集。

#### 2.7.3.2.6. 视频交换系统

包括视频接入认证服务器、视频用户认证服务器，实现外主机对接入对象（终端、视频服务器等）进行设备认证；实现内主机对内网终端用户进行统一注册、授权管理和访问控制。对视频数据与视频控制信令严格区分，分别处理后进行传输。支持视频数据的双向传输模式和视频控制信令双向传输模式。

#### 2.7.3.2.7. 安全隔离网闸

2U 机架式；采用 2+1 架构和专用硬件隔离技术，属完全自主开发且不可从外部编程控制；保证信任网络和非信任网络之间链路层的断开，彻底阻断 TCP/IP 协议以及其他网络协议。

### 2.7.3.2.8. 三层交换机

利用三层网络交换机可根据接入应用进行路由选择和虚拟专网的划分，保证不同业务应用通道之间的相互隔离。

### 2.7.3.2.9. 集控探针

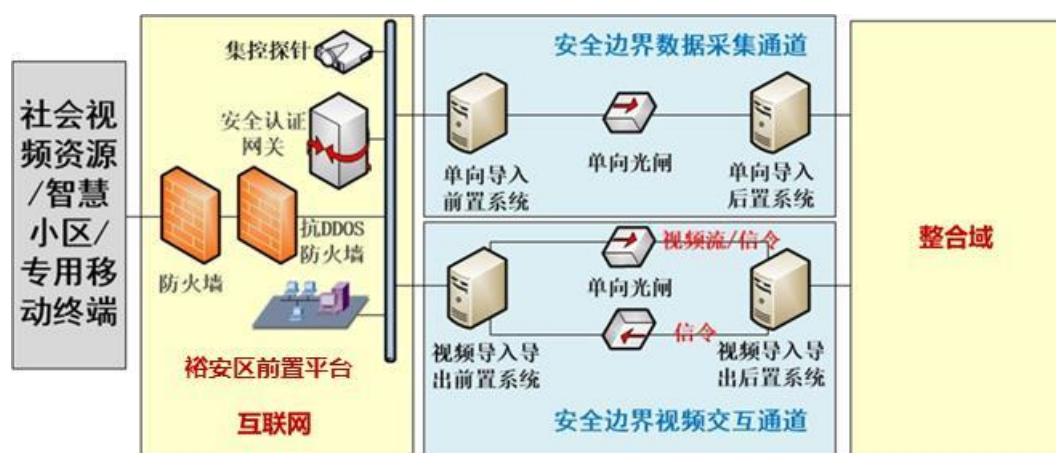
用于监听监控防火墙、三层交换机等设备日志和所有网络设备的流量信息、异常事件等，并上报到视频专网安全边界集控系统。

## 2.7.4. 整合域与互联网联网共享安全

### 2.7.4.1. 技术要求

按照《GA/T 1788.3-2021 公安视频图像信息系统安全技术要求 第 3 部分：安全交互》要求，建设整合域与互联网之间的横向边界交互平台，实现整合域与互联网上视频资源和数据资源的单向采集。要求平台具备单向导入、单向导出、签名验签、格式检查、内容过滤、流量管控、服务认证、信令安全、媒体安全、安全隔离、集中监控报警等安全功能。其中视频流和数据流都采用单向传输的方式。

### 2.7.4.2. 建设方案



整合域与互联网联网共享安全建设方案



#### 2.7.4.2.1. 防火墙

采用防火墙设备对平台进行安全防护，启用访问控制功能，制定详细的访问控制策略，实现端口级、细颗粒度的访问控制，保障对访问行为的有效管控；防火墙内置入侵防御功能，通过实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试，当发现网络违规攻击行为和未授权的网络访问时进行实时阻断。

#### 2.7.4.2.2. 抗 DDOS 网关

平台接入区部署抗 DDOS 网关设备，能够检测与防御流量型 DDoS 攻击、应用型 DDoS 攻击、DoS 攻击和非法协议攻击等四大类拒绝服务攻击形式，保证正常流量不受影响。

#### 2.7.4.2.3. 安全认证网关

用于外部网络终端设备以及用户的认证授权管理。主要功能包括:用户身份认证、设备认证、访问控制、权限管理、传输加密、终端加固、监控审计等。

#### 2.7.4.2.4. 视频图像信息系统安全

对登录视频图像信息系统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；

对用户访问进行授权，并根据用户的不同角色、级别、所属机构、任务和场景进行鉴权、授权，实现功能级访问控制；

对视频图像信息系统应用内容进行安全防护，防止自动化工具攻击和数据爬取；

记录视频图像业务应用的操作日志，操作日志应包含操作人、操作时间、操作终端、操作对象、操作条件、返回结果等；

能够基于业务日志的行为发生 IP、行为发生时间范围、行为发生时间周期、行为结果等进行分析，分析用户异常行为。

#### 2.7.4.2.5. 单向光闸

单向光闸由内网单元、外网单元、分光单向传输单元三个逻辑部分组成，基于光隔离平台的通信服务，采用经过优化的传输和分组算法，将数据传输的功能整合统一。系统采用 2+1 架构和多模分光器隔离技术，纯物理部件通过光单向传输数据；提供数据冗余校验功能，提升单向数据传输的可靠性；接收端提供高速缓存功能，预防大流量传输时的数据失。

#### 2.7.4.2.6. 单向导入系统

系统由两台设备组成（导入前置机、导入服务器），实现各类数据信息的单向导入；系统具有灵活的文件交换冲突选项，支持重名策略：覆盖、放弃、重命名。系统支持多种同步方式：触发器方式，全表采集方式，同表单向的数据同步，主从表单向的数据同步，删除源数据等同步方式。

系统能够事先定义任务的过滤规则，并根据过滤规则对数据进行严格的格式检查和过滤；系统可以根据系统管理员配置任务规则进行单向传输，对数据进行深层次细粒度的过滤检查，可对内容过滤，可对大字段内容检查；系统支持多种主流数据库的同步，包括：Oracle、MS SQL Server、MySQL 等；支持多种同步方式：触发器方式，全表采集方式，同表单向的数据同步，主从表单向的数据同步，删除源数据等同步方式。

#### 2.7.4.2.7. 双光闸视频导入导出系统

系统由视频导入导出前置系统和视频导入导出后置系统组成，部署在单向光闸的两端。系统支持对网络内终端、服务器等设备基于证书、IP 和 MAC 等信息的注册和认证，拒绝非注册设备的访问请求。

前置系统负责对外网流媒体和信令进行采集与安全处理，并对内网导出流媒体和信令审核校验与处理；后置系统负责对外网流媒体和信令进行完整性校验，并负责采集内网待导出流媒体和信令的处理。

#### 2.7.4.2.8. 三层交换机

利用三层网络交换机可根据接入应用进行路由选择和虚拟专网的划分，保证不同业务应用通道之间的相互隔离。

#### 2.7.4.2.9. 集控探针

用于监听监控防火墙、三层交换机等设备日志和所有网络设备的流量信息、异常事件等。

### 2.7.5. 整合域安全防护

本方案按照“严控边界、纵深防御、主动监测、全面审计”的防护原则要求，通过在整合域建立和完善 IT 资源监控和安全管理、终端安全管控、用户身份认证和权限管控措施；

本方案通过建立科学合理的安全管理和运维管理制度，通过全网安全加固、防护体系部署实施、专业的安全运维服务、定期安全巡检，确保全网在信息安全方面可管可控，保障公共安全视频监控平台及网络的安全稳定运行，保障公安信息网的安全稳定运行。

#### 2.7.5.1. 网络防病毒

配置一套网络版杀毒软件，支持对视频专网操作终端安装的杀毒软件进行统一管理、防病毒策略统一下发、病毒库统一升级。

#### 2.7.5.2. 内网安全管理系统

内网安全管理系统以终端管理为核心，形成集主机监控审计、补丁管理、桌面应用管理、信息安全管理、终端行为管控等安全行为一体的管理体系，为视频资源共享平台的稳定运行提供一个安全的、可靠的、稳定的运行环境。

#### 2.7.5.3. 入侵检测

核心交换机侧旁路部署入侵检测系统，对整合域中各种溢出攻击、RPC 攻击、WEBCGI 攻击、拒绝服务、病毒木马、蠕虫、网络异常、受控主机、系统

漏洞攻击等行为进行入侵检测和告警，实现全网威胁分析和展现。

#### 2.7.5.4. 漏洞扫描系统

系统具备漏洞扫描、WEB 扫描、弱口令扫描、安全基线检查、变更检查等功能；

能够识别出运行的服务和端口，内置漏洞库 58000 条以上，支持 CVE、CNVD、CNNVD、BugTraq 等，拥有完备的知识体系；

系统内置安全基线检查策略，同时提供新建策略功能；

支持一次性任务、立即任务、周期任务等多种调度方式；支持漏洞扫描、WEB 扫描、弱口令扫描、安全基线检查、变更检查的五合一任务；

支持对周期任务的多次执行任务结果进行比对，比对结果中详细展示报告间的异同之处；

变更列表可以显示系统内被监控的重要文件、文件夹、注册表、启动项、进程等变更状态；

以列表的方式展示告警，支持告警策略自定义、告警声音设置、告警过滤策略。

#### 2.7.5.5. 终端准入控制与违规外联监测系统

终端准入控制系统通过对视频专网内设备自动发现与注册管理，对终端提供各种控制、运行监测与管理。以旁路控制技术为主，秉承不改变现有网络结构的特性，为用户解决终端入网的合规性要求，支持包括身份认证、安全隔离、安全修复、可配置的多种准入控制手段和访问控制手段等功能，满足视频专网对专用网络边界、终端安全接入防护的相应要求。

支持通过扫描监测、流量分析、脚本分析发现网络设备非授权违规外联；支持非法 DHCP、违规 DNS、匿名 FTP 等非法网络服务监测预警；支持边界发现、网中网发现。

#### 2.7.5.6. 日志审计系统

日志审计系统对全网设备日志进行集中管理。一旦有安全事件发生，日志

审计系统可以帮助开展行之有效的调查。例行的日志检查及深入分析保存日志不但可以立即识别出出现不久的安全事件、违反政策情况、欺诈活动以及运作问题，还有助于提供有价值的信息，从而解决问题。

日志审计系统提供全面的 60 天标准的系统日志和详尽的报告功能。通过对日志进行分析可以让管理员跟踪 IT 基础设施的活动，是评估服务器数据泄密事件是否发生、如何发生、何时发生、在何处发生的有效方法。

#### **2.7.5.7. 运维堡垒机**

配置一台运维堡垒机，对整合域业务环境下的用户运维操作进行控制和审计的合规性管控，避免采用直连或远程登录服务器等较低安全级别运维方式。

#### **2.7.5.8. 视频应用安全审计系统**

部署一套视频安全审计系统，从公安视频图像信息应用系统、视频监控共享平台的应用日志，以及网络流量入手，实现对用户、设备、应用访问服务/数据的行为过程的完整记录，并在日志审计基础上开展异常行为分析，实现“追踪的下去、查的到源头、取的到证据、异常可发现”能力，规范公共安全视频图像信息资源使用和管理，保障公民、法人和其他组织的合法权益。防止因为数据盗取、违规操作、越权访问等造成公安敏感信息泄露、数据破坏、侵犯公民隐私的现象。

针对视图库安全审计，系统通过交换机镜像获取视图库操作的原始网络流量数据包，从数据包中还原解析得到视图库原始操作信令，从原始控制信令中还原出操作终端 IP/MAC 地址、登录账号、查询条件（图片及图片特征属性的结构化信息）、检索结果（图片及图片特征属性的结构化信息）、检索来源、查询类型、操作时间等信息，其中操作类型记录涵盖视图库的创建、查询、更新、删除、布/撤控及其它操作等。

#### **2.7.5.9. 边界安全运维系统**

部署一套边界安全运维系统，通过采集业务日志、流量日志、系统日志，对进出边界接入平台的人、事、数据、设备进行集中监管、安全审计。向用户

集中展示边界建设现状，辅助用户掌握边界违规建设情况，对边界运行状态进行监控与记录，当出现违规业务、数据窃取等行为，即可报警并记录，为用户提供事前的防护、事中的管控、事后的追溯。

### **2.7.6. 安全服务要求**

#### **2.7.6.1. 日常巡检**

系统正式运行后，应每月对联网边界接入平台以人工、自动等方式检查主机系统和网络设备的日志信息、安全配置以及审计信息等，提出安全策略建议，并提供后续技术提供，配合问题的查处解决。

#### **2.7.6.2. 风险评估**

采用工具扫描（漏洞扫描、数据库扫描）、人工评估、渗透测试三种相结合的方式，对公共场所视频监控资源整合共享的网络设备、主机系统进行风险评估。

#### **2.7.6.3. 安全加固**

对公共场所视频监控资源整合共享中视频传输网与联网边界接入平台的物理环境、网络结构、应用系统、数据库、服务器及网络设备的安全性、安全产品和服务的应用状况以及管理体系是否完善进行加固。

### **2.7.7. 信创及国产化替代要求**

按照可信云要求配置管理/应用及解析服务器，并与裕安区城市大脑信创云的建设保持架构、管理的统一；本期所建系统要求能够支撑后期国产化替代工作的充分测试和实践，能够在不影响业务运行的前提下，进行平滑升级替代，确保业系统安全稳定运行。

2.8. 存储及机房租赁要求

2.8.1. 云存储系统

1、项目视频云存储单路空间计算

视频云存储单路空间计算表

序号	设备类型	像素	存储时间	存储码流	空间/月
1	球机/枪机	400 万	30 天	4 兆	1.24T

2、项目视频云存储可用存储空间计算

项目视频云存储可用存储空间计算表

序号	设备类型	像素	存储时间	存储（T）	设备数量	可用空间（PB）
1	球机/枪机	400 万	30 天	1.24	6890	8.54

视频需要净空间 8.54PB，计算冗余 0.7 系数后实际需要约 12.2PB 存储容量，作为市级平台的前置节点，设置在视频专网。

2.8.2. 机房租赁

租用六安云计算中心机房标准机柜 12 台。并满足以下条件：

（1）机房要求

- 机房的强电和弱电线电缆必须分别走各自线槽。光纤主干应走专用线槽，主从线槽必须独立分开。
- 要求机房大楼市电的供电方式为双电源（两路同供，不联络），供电电压 $\geq 10KV$ 。
- 配置发电机。
- 机房照明包括日常照明和应急照明。应急照明要能在机房市电停电情况下自动启动。
- 在市电配电柜、UPS 输入、输出柜处各加相应型号的防雷浪涌吸收装置。
- 本次提供机柜为独立专用空间。
- 提供 1 对（1+1 主备）万兆线路，用于本项目相关的数据传输。

- 单个机柜 $\geq 42\text{U}$ 。

## (2) 温、湿度及防尘要求

根据国家标准 GB50174-2017《数据中心设计规范》，本方案中计算机主机设备工作环境要求：

温度： $5^{\circ}\text{C}$  至  $45^{\circ}\text{C}$

湿度：8%~80%

同时露点温度不大于  $27^{\circ}\text{C}$

每立方米空气中大于或等于  $0.5\mu\text{m}$  的悬浮粒子数

## (3) 电源与防雷要求

计算机设备供配电系统提供的质量好坏直接影响着计算机系统的稳定性和可靠性。根据国家标准 GB50174-2017《数据中心设计规范》，本方案中计算机主机设备电源要求：

稳态电压偏移范围  $+7\sim-10\%$

稳态频率偏移范围  $\pm 0.5\text{ Hz}$

输入电压波形失真度  $\leq 5\%$

允许断电持续时间  $0\sim 10\text{ ms}$

## (4) 机房运维管理要求

具备动力环境监控功能（负载电压、电流、温湿度、水浸、烟感检测等）



有专门的值守用房、设备、制度，提供 7\*24 小时值班。

（5）网络安全要求

满足《信息安全等级保护管理办法（公通字[2007]43 号）》第三级信息系统运营、使用单位的管理要求。

2.9. 设备清单

序号	名称	技术要求	单位	数量
一、前端感知设备及网络				
1	枪型摄像机	1、相机像素要求：不小于 400 万； 2、镜头支持电动变焦，并可对拍摄物体进行自动聚焦； 3、最低照度：彩色不大于 0.0005 lux，黑白不大于 0.0001 lux； 4、相机水平中心分辨力不小于 1400TVL； 5、防护等级不低于 IP67； 6、符合《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 28181-2016）》标准； 7、包含摄像机、高清镜头、室外防护罩、电源适配器、安装万向节、支架、抱箍等。	套	167
2	球型摄像机	1、相机像素要求：不小于 400 万； 2、变焦倍数：不小于 24 倍光学变倍； 3、最低照度：彩色不大于 0.0005 lux，黑白不大于 0.0001 lux； 4、红外补光距离不低于 150 米； 5、防护等级不低于 IP67； 6、支持预置位不低于 300 个； 7、符合《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 28181-2016）》标准； 8、包含摄像机、高清镜头、电源适配器、安装万向节、支架、抱箍等； 9、具有防尘、防水、网络防雷、防浪涌等功能。	套	54
3	半球型摄像机	1、相机像素要求：不小于 400 万； 2、防护等级不低于 IP67； 3、符合《公共安全视频监控联网系统信息传输、交换、控制技术	套	116

		<p>要求（GB/T 28181-2016）》标准；</p> <p>4、包含摄像机、高清镜头、电源适配器、安装万向节、支架、抱箍等。</p> <p>5、具有防尘、防水、网络防雷、防浪涌等功能。</p>		
4	人脸抓拍摄像机	<p>1、适用于道路（1 米至 8 米）人脸抓拍场景；</p> <p>2、相机像素要求：不小于 800 万；</p> <p>3、内置 GPU；</p> <p>4、最低照度要求：彩色不大于 0.0002 lx，黑白不大于 0.0001 lx；</p> <p>5、镜头要求：支持自动变焦；</p> <p>6、支持同时检测并且抓拍不小于 40 张人脸；</p> <p>7、支持检出两眼瞳距像素点最小值为 20 的人脸图片；</p> <p>8、人脸抓拍捕获率不小于 99%；</p> <p>9、人脸抓拍重复率不大于 1%；</p> <p>10、设备支持检出戴口罩等遮挡方式的人脸；</p> <p>11、支持人脸与人体的关联显示；</p> <p>12、符合《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 28181-2016）》标准；</p> <p>13、防护等级：不低于 IP67；</p> <p>14、包含摄像机、高清镜头、室外防护罩、电源适配器、安装万向节、支架、抱箍等；</p> <p>15、具有防尘、防水、网络防雷、防浪涌等功能。</p>	套	8
5	监控杆件	<p>1、材质：采用 Q235B 钢板，一次成型卷板，八棱形杆，杆高 7m，上口径 <math>\phi 340\text{mm}</math>，下口径为 <math>\phi 400\text{mm}</math>，主杆壁厚 8mm；底板法兰：<math>\phi 650\text{mm} \times 20\text{mm}</math>；</p> <p>2、横臂：长度定制；</p> <p>3、地笼：8-M30*1800mm，要求热镀锌喷塑，加工时清除毛刺，锐边倒钝，焊接保证强度，焊缝均匀牢固，无虚焊、假焊；</p> <p>4、混凝土基础 C30 砼，尺寸：1600mm*1600mm*2000mm；</p> <p>5、接地：-4*40*1000mm+40*40*1000mm 镀锌扁铁角钢。</p>	套	18
6	借杆横臂	借杆横臂 0.5m-2m；材质 Q235B。横臂采用 $\phi 60$ 钢管加工制作而成，厚度 $\geq 2.75\text{mm}$ ，采用 8.8 级紧固件，整体热镀锌，静电喷涂，配置 2 个枪机法兰。	套	5
7	壁装支架	相机配套壁装支架，0.1m-0.5m。	套	20
8	吊装支	相机配套吊装支架，0.1m-1m。	套	20

	架			
9	设备机箱	箱体采用优质冷轧钢，抱杆箱体厚度 1.2mm。尺寸：高 500mm、宽 400mm、深 200mm。采用静电喷塑防锈处理工艺，平均塑层厚度 $\geq 80\mu\text{m}$ ，表面统一按照国标色卡 GSB05-1426-2001 标准着色；箱体采用斜屋顶外形设计，具有防水、防尘、通风散热、抗紫外线（防老化）、防盗、防锈、耐酸碱腐蚀等功能，至少保证 5 年不能发生锈蚀。环境工作温度： $-40^{\circ}\text{C}$ 到 $85^{\circ}\text{C}$ ，工作湿度 $0\sim 95\%\text{RH}$ ；符合国家防尘防水 IP55 标准要求，按需求方要求丝印门板标识。配备不锈钢豪华平面门锁、配电单元保护板、设备导轨、5 位接地铜排，设备层板，包含抱箍及相关连接件(套)，并采用模块化结构布局。箱体喷涂样式需根据甲方要求定制。	套	38
10	二合一防雷器	电源防雷、网络防雷。	只	400
11	光缆 I	12 芯光缆，室外单模。	米	500
12	光缆 II	4 芯光缆，室外单模。	米	2000
13	电缆 I	YJV $3\times 4\text{mm}^2$ 。	米	500
14	电缆 II	RVV $3\times 2.5\text{mm}^2$ 。	米	3000
15	电缆 III	RVV $3\times 1\text{mm}^2$ 。	米	29150
16	网线	室外，STP 超五类八芯线。	米	29150
17	前端工业接入交换机	1. 千兆以太网口 $\geq 8$ 个；千兆 SFP 光口 $\geq 2$ 个； 2. 交换容量 $\geq 56\text{Gbps}$ ；包转发率 $\geq 14.88\text{Mpps}$ 。	套	128
18	千兆单模 20 公里光模块	工业级 SFP 千兆单模光模块，单模，1310nm，最大传输距离 20km，接头类型：LC。	套	256
19	前端工业汇聚交换机	1. 千兆电口 $\geq 24$ 个，千兆 SFP 光口 $\geq 4$ 个，Console 口 $\geq 1$ 个； 2. 交换容量 $\geq 336\text{Gbps}/3.36\text{Tbps}$ ；包转发率 $\geq 96\text{Mpps}/126\text{Mpps}$ 。	套	12
20	万兆单模 20 公里光模块	SFP+ 万兆单模光模块，单模，1310nm，最大传输距离 10km，接头类型：LC。	套	12

21	智能电表	自动计量消耗电量，并在平台记录信息，生成用电信息报表。	个	20
22	外场设备用电费用	本目前端点位电表开户，挂表取电，点位前端设备 5 年电费。	项	20
23	PE 管敷设	地埋管 PE90。	米	200
24	钢管	SC100 镀锌钢管。	米	100
25	线槽	PVC 墙面明装方形走线槽。	米	2000
26	水泥路开挖及回填	拆除路面 30cm，深度为 50cm，管道预埋后使用人工摊铺中粒式沥青混凝土。	米	100
27	挖沟槽土方及回填	二类土，人工开挖严禁机械挖掘。宽度 30cm，深度 40cm；开挖后一侧弃土，管道预埋后使用原土恢复。	米	100
28	沥青路开挖及回填	宽度 30cm，深度 50cm。	米	100
29	人行道板砖开挖及回填	宽度 30cm，深度 50cm。	米	100
30	绿化带开挖及回填	宽度 30cm，深度 40cm。	米	100
31	手孔井	方井，井体外径 450*450mm，深度大于 600mm；底部使用黄沙覆盖，采用带有标识的复合材料井盖。	个	10
32	运营商线路租赁	裕安区前置平台（整合域）至六安公安视频图像信息应用平台（公安视频专网）线路 1 条，运营商专线租赁，裸纤，带宽不少于 40GE；线路租赁期 5 年，需保证视频图像质量传输无卡顿延迟现象，若出现延迟卡顿现象，运营商应无条件提升链路带宽直至满足使用。	条	1
33	运营商线路租赁	裕安区前置平台（整合域）至裕安区前置平台（互联网）线路 1 条，运营商专线租赁，裸纤，带宽不少于 20GE；线路租赁期 5 年，需保证视频图像质量传输无卡顿延迟现象，若出现延迟卡顿现象，运营商应无条件提升链路带宽直至满足使用。	条	1

34	运营商 线路租 赁	裕安区前置平台（整合域）至六安市社会视频资源整合平台线路 1 条，运营商专线租赁，裸纤，带宽不少于 20GE；线路租赁期 5 年，需保证视频图像质量传输无卡顿延迟现象，若出现延迟卡顿现象，运营商应无条件提升链路带宽直至满足使用。	条	1
35	运营商 线路租 赁	裕安区前置平台（整合域）至除公安外政府部门平台线路，运营商专线租赁，裸纤，带宽不少于 2GE；线路租赁期 5 年，需保证视频图像质量传输无卡顿延迟现象，若出现延迟卡顿现象，运营商应无条件提升链路带宽直至满足使用。	条	47
36	运营商 线路租 赁	裕安区前置平台至各单位前端设施设备线路条，运营商线路租赁，带宽不少于 100M；线路租赁期 5 年，需保证视频图像质量传输无卡顿延迟现象，若出现延迟卡顿现象，运营商应无条件提升链路带宽直至满足使用。	条	261
<b>二、视频监控基础平台</b>				
1	裕安区 前置平 台优化	1、优化满足社会视频资源整合基础应用、共享中心、认证中心、运行中心、开放中心等功能要求；（详见需求文件） 2、具备不低于 5 万路的视频接入能力，不低于 500 路 4M 码流实时并发能力。	项	1
2	联网网 关	1、国标联网网关一体机，从非标平台中取视频流，转换为国标后，通过安全边界将数据进行汇聚，实现视频应用。 2、网关配置不低于 4210×2/64GDDR4/600G/10KSAS×4(RAID_1)/SAS_HBA/1GbE×2；单台支持独立转码不低于 40 路。	台	4
3	视频场 景算法	支持 GB/T 28181、ONVIF、RTSP 等协议的 video 接入，提供校园安全（包括人脸识别、聚众检测、攀爬识别、校园危险区域、校园防踩踏、校园烟火、抽烟、打手机、闯入、打架、摔倒等）、智慧社区（包括消防通道异常、区域聚集、人员滞留、区域闯入、打架、跌倒检测、烟雾识别、偷盗监测、破坏公物等识别）、安全生产（包括人员出入、边界跨越、人员逗留监测，人员摔倒（跌倒）识别、人员异常聚集；佩戴安全帽识别、防护服穿戴识别、反光衣识别，烟雾识别、火焰识别；抽烟识别、拨打电话识别、玩手机识别、人员拥堵识别等）、智慧城管（包括店外经营、占道广告、游商小贩、乱扔乱倒、乱堆物料、垃圾满溢、垃圾暴露、沿街晾晒、余泥渣土运输等）四类视频分析场景算法闭环，总共不少于 1000 路视频分析算法授权，根据业主需求可更换算法。	项	1
<b>三、运维管理</b>				
1	运维管 理系统	具备数据对接中心、智能巡检分析中心、设备档案管理模块、运维工单管理、运维考核管理、用户管理模块、安全管理、项目运维管	项	1

		理等功能。		
2	运维服务	<p>1、为保障视频监控资源正常运行，需成立专业运维团队。提供全天候 7×24×365 不间断服务支持，24 小时应急热线电话，快速响应项目维护需求。</p> <p>2、提供不少于每年 2 人的驻场服务，服务期 5 年。常驻运维人员需要大学专科以上学历（要求计算机、通信、信息化等相关专业），有参与过相关工作经验。</p> <p>3、常驻专职维护管理人员每天应当主动检查监控的视频图像是否正常，每天应人工巡检二次以上；主动发现故障并进入维护流程。每天记录维护日志，每周形成周维护报告，每月形成月维护报告。</p> <p>4、维护人员除每天的抢修维修工作外，每月对工程范围内的设备箱、设备及其供电系统进行一次巡检维护，包括设备除尘、排除遮挡物、排除故障隐患、摄像机除尘清洁等，以确认所有设备及系统工作正常，并将巡检工作在月维护报告体现。</p> <p>5、维护具体内容包括（但不限于）：前端摄像机的镜头调试、设备除尘除雾、位置调整、摄像机维修及更换（摄影机设备由建设单位提供）、故障排除等；光纤线路、摄像机控制线路和接口检测、隐患排查、故障排除；摄像机传输设备的维护和故障排除。</p>	项	1
<b>四、安全管控</b>				
1	防火墙	<p>1、标准≥2U 机架式设备，网络处理能力≥19Gbps，并发连接≥500 万，标准配置≥16 个 10/100/1000M 自适应电、≥4 个 SFP 光接口，≥4 个 SFP+光接口，≥2 个扩展插槽，内置≥4T 存储硬盘；</p> <p>2、产品满足 GB/T20281-2020、JCTJ 005-2016 信息安全技术要求和标准。</p>	台	1
2	前端视频准入系统	<p>1、标准 2U 机架式设备，提供≥6 个千兆电口，≥2 个万兆 SFP+接口，提供≥2T 存储硬盘，另外具备≥2 个扩展槽，支持至少 5000 路前端设备接入，支持双机热备 HA 高可用方式部署。</p> <p>2、支持 GB/T28181 及 GB35114 标准的识别，可以筛选出支持 GB/T28181 及 GB35114 协议的视频设备并禁止不支持的终端入网。</p>	台	1
3	万兆视频交换系统	<p>1、由视频认证服务器、用户认证服务器、安全隔离网闸三台设备组成，保证兼容性和稳定性；</p> <p>2、视频认证服务器：标准 2U 设备，具备≥6 个 10/100/1000Base-T 接口，≥2 个万兆 SFP+接口，冗余电源；</p> <p>3、用户认证服务器：标准 2U 设备，≥6 个 10/100/1000Base-T 接口，≥2 个万兆 SFP+接口，冗余电源；</p> <p>4、安全隔离网闸：标准 2U 机架设备，冗余电源，面板具有液晶显</p>	套	1

		<p>示屏，内网接口<math>\geq 6</math>个 10/100/1000Base-T 端口，<math>\geq 4</math>个 SFP 插槽，<math>\geq 2</math>个 SFP+插槽；外网接口<math>\geq 6</math>个 10/100/1000Base-T 端口，<math>\geq 4</math>个 SFP 插槽，<math>\geq 2</math>个 SFP+插槽，</p> <p>5、数据吞吐量<math>\geq 7\text{Gbps}</math>。</p> <p>6、支持信令双向传输，视频数据单向传输，对内外网数据均有安全检查机制；</p> <p>7、支持多种协议格式检查，包括视频信令协议格式（SIP）、视频传输协议格式及主流视频监控公司的私有协议视频信令协议格式等；</p> <p>8、具备对接国标 GB/T 28181-2016 标准平台能力。</p>		
4	集控探针	<p>1、1U 软硬件一体化设备，提供<math>\geq 6</math>个 10/100M/1000M 电口，<math>\geq 1</math>个 Console 口、<math>\geq 2</math>个 USB 口、<math>\geq 1</math>个扩展槽，可灵活扩展电口光口；</p> <p>2、支持采集交换机、路由器、防火墙、入侵检测、可信边界网关等边界接入链路外网侧常用设备的运行状态信息。</p>	台	1
5	三层交换机	<p>1. 支持 100M/1G/2.5G/5G/10G Base-T 以太网端口<math>\geq 24</math>个、万兆 SFP+端口<math>\geq 24</math>个、25GE SFP28 端口<math>\geq 4</math>个、40GE QSFP+端口<math>\geq 2</math>个；</p> <p>2. 性能：交换容量<math>\geq 24\text{Tbps}</math>，包转发率<math>\geq 1000\text{Mpps}</math>。</p>	台	2
6	防火墙	<p>1、标准<math>\geq 2\text{U}</math>机架式设备，网络处理能力<math>\geq 19\text{Gbps}</math>，并发连接<math>\geq 500</math>万，标准配置<math>\geq 16</math>个 10/100/1000M 自适应电、<math>\geq 4</math>个 SFP 光接口，<math>\geq 4</math>个 SFP+光接口，<math>\geq 2</math>个扩展插槽，内置<math>\geq 4\text{T}</math>存储硬盘；</p> <p>2、产品满足 GB/T20281-2020、JCTJ 005-2016 信息安全技术要求和标准。</p>	项	3
7	万兆视频交换系统	<p>1、由视频认证服务器、用户认证服务器、安全隔离网闸三台设备组成，保证兼容性和稳定性；；</p> <p>2、视频认证服务器：标准 2U 设备，具备<math>\geq 6</math>个 10/100/1000Base-T 接口，<math>\geq 2</math>个万兆 SFP+接口，冗余电源；</p> <p>3、用户认证服务器：标准 2U 设备，<math>\geq 6</math>个 10/100/1000Base-T 接口，2 个万兆 SFP+接口，冗余电源；</p> <p>4、安全隔离网闸：标准 2U 机架设备，冗余电源，面板具有液晶显示屏，内网接口<math>\geq 6</math>个 10/100/1000Base-T 端口，<math>\geq 4</math>个 SFP 插槽，<math>\geq 2</math>个 SFP+插槽；外网接口<math>\geq 6</math>个 10/100/1000Base-T 端口，<math>\geq 4</math>个 SFP 插槽，<math>\geq 2</math>个 SFP+插槽；</p> <p>5、数据吞吐量<math>\geq 7\text{Gbps}</math>；</p> <p>6、支持信令双向传输，视频数据双向传输，对内外网数据均有安</p>	套	2

		<p>全检查机制；</p> <p>7、支持多种协议格式检查，包括视频信令协议格式（SIP）、视频传输协议格式及主流视频监控公司的私有协议视频信令协议格式等；</p> <p>8、具备对接国标 GB/T 28181-2016 标准平台能力。</p>		
8	集控探针	<p>1、1U 软硬件一体化设备，提供<math>\geq 6</math> 个 10/100M/1000M 电口，<math>\geq 1</math> 个 Console 口、<math>\geq 2</math> 个 USB 口、<math>\geq 1</math> 个扩展槽，可灵活扩展电口光口；</p> <p>2、支持采集交换机、路由器、防火墙、入侵检测、可信边界网关等边界接入链路外网侧常用设备的运行状态信息。</p>	台	2
9	网络防病毒	配置网络防病毒，支持对视频专网操作终端安装的杀毒软件进行统一管理、防病毒策略统一下发、病毒库统一升级	套	1
10	内网安全管理系统	<p>1、外设管理：支持对终端各种外设、接口设置使用权限，并支持生效时间设置。持外设库管理，可统计终端外接的各种设备。支持对外设进行多维度的放行，通过添加实现例外或加黑；</p> <p>2、进程管理：支持对单点维护功能，可远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行、内存占用、签名、产品名称、公司名称等，支持远程结束进程；支持终端进程红名单、黑名单、白名单功能；</p> <p>3、违规外联：支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。支持例外白名单添加；</p> <p>4、网络防护：支持对网卡进行防护，支持阻止终端修改 IP 地址、使用动态 IP 地址、热点创建和 IPV6 地址使用等，可自定义提示内容和生效时间；</p> <p>5、终端安全基线检查：可自定义基线检查项，可自定义终端端定性标准，通过基线检查分数设定，定义出高危、中危、低危和安全；</p> <p>6、终端调查：对指定终端当下的状态进行深入调查，包括终端登录日志、启动项、计划任务、正在运行的服务等，以及最近一段时间内终端的行为数据信息；</p> <p>7、威胁事件评估：对全网终端进行威胁事件风险性评估。并支持一键响应处置能力；</p> <p>8、高级威胁防护：支持无文件攻击防护、文档攻击防护、横移渗透攻击防护、内存攻击防护。</p>	套	1



11	入侵检测	1、标准 2U 机架式设备，设备面板具有液晶显示屏，≥6 个 10/100/1000M 自适应以太网口，≥2 个万兆 SFP+接口，≥1 个扩展插槽，网络吞吐率≥10Gbps，应用吞吐率≥5Gbps，≥1T 存储空间，支持全部日志按天和统一格式存储； 2、提供入侵检测特征库。并提供基于正则表达式匹配方式的自定义特征检测策略。	台	1
12	漏洞扫描系统	1、标准 2U 机架式，≥1TB 硬盘，标准配置≥6 个 10/100/1000M 自适应电口，≥2 个 SFP 插槽，≥2 个扩展插槽，液晶屏，Web 扫描域名无限制，Web 扫描任务并发数为≥5 个域名。 2、系统扫描 IP 地址最大支持 1024 个，支持扫描 A 类、B 类、C 类地址，系统扫描支持≥150 个 IP 地址并行扫描。能够提供系统扫描、WEB 扫描、数据库扫描、弱口令扫描等功能模块。	台	1
13	终端准入控制系统	标准机架式设备，提供≥6 个千兆电口，提供≥4T 存储硬盘，支持至少 500 路设备准入，支持双机热备 HA 高可用方式部署。	套	1
14	日志审计系统	1、事件采集性能≥3000EPS，事件处理性能≥2000EPS，提供≥4 个千兆电口，≥4TB 硬盘，提供≥85 个日志源 IP 授权节点，百亿条日志量查询平均响应时间≤10 秒； 2、产品须通过 GB/T 20945-2013《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》测评认证。	台	1
15	运维堡垒机	1、标准机架式，支持≥6 个千兆电口，≥2 个扩展槽位，≥4TB 硬盘，配置≥100 个设备审计节点许可。	台	1
16	视频准入防护系统	1、标准 2U 机架式设备，提供≥6 个千兆电口，≥2 个万兆 SFP+接口，提供≥2T 存储硬盘，另外具备≥2 个扩展槽，支持双机热备 HA 高可用方式部署； 2、支持 GB/T28181 及 GB35114 标准的识别，可以筛选出支持 GB/T28181 及 GB35114 协议的视频设备并禁止不支持的终端入网。	套	1
17	边界安全运维系统	1、网口配置：不低于 4 个千兆电口； 2、平均页面响应时间 ≤ 5S； 3、最大日志存储量≥500GB； 4、最大存储记录数≥5 亿条； 5、每秒可接收日志条数不小于 200 条。	套	1
18	安全认证网关	1、标准 2U 机架，标配≥6 个 10/100/1000M 自适应电口，≥1 个扩展槽，≥2 个 USB，RJ-45 串口管理，标配≥1T 工业级硬盘，标配国密卡，液晶显示屏，SSL 单台最大可支持并发用户数（CUs）≥1000，在线并发用户数≥200。	台	1

19	签名验 签服务 器	1、2U 机箱， 内存 $\geq 16G$ ，硬盘 $\geq 120G$ ，千兆电口 $\geq 2$ 个，设备支持机械锁，开机箱需要钥匙开锁； 2、支持生成各类对称密钥（SM1、SM4、DES、AES 等）和非对称密钥（SM2、RSA1024/2048 等）； 3、支持 C、JCE、P11 接口，API 接口符标准接口规范《GM/T 0029-2014 签名验签服务器技术规范》。	台	1
20	服务器 密码机	1、2U 机箱，内存 $\geq 16G$ ，硬盘 $\geq 120G$ ，千兆电口 $\geq 2$ 个，设备支持机械锁，开机箱需要钥匙开锁； 2、对称算法：支持国密 SM1/SM4 算法和国际 DES/3DES/AES 算法；摘要算法：支持国密 SM3 算法和国际 MD5/SHA1/SHA256/SHA384/SHA512 等算法；非对称算法：支持国密 SM2 和国际 RSA(1024-2048)算法； 3、支持生成各类对称密钥（SM1、SM4、DES、AES 等）和非对称密钥（SM2、RSA1024/2048 等）。	台	1
21	证书服 务系统	具有高可靠性的安全机制及完善的管理及配置策略，可以提供自动化地密钥和证书管理服务，支持多操作系统。系统对整个证书的生命周期进行管理，主要功能包括初始化、系统管理、证书模板管理、RA 管理、CA 证书服务、CRL 管理、证书发布、日志审计和接口服务等。	台	1
22	USBkey	与证书服务系统配套使用。	个	100
<b>五、存储</b>				
1	管理/ 应用服 务器	1、2U 机架式服务器，非 OEM 产品，自主研发，国产品牌； 2、配置 $\geq 2$ 颗国产 CPU，每颗 CPU 核心数 $\geq 16$ 核，每颗 CPU 主频 $\geq 2.5GHz$ ； 3、配置 $\geq 256GB$ DDR4 3200MHz 配置 $\geq 2$ 块 2.5 寸 480G SSD 硬盘，配置 $\geq 8$ 块 3.5 寸 8T SATA 硬盘，配置 $\geq 1$ 块 1.92TB NVME SSD 硬盘，可支持 SAS/SATA 硬盘、SSD 混插； 4、配置 $\geq 2*10GE$ （含光模块），配置 $\geq 2*GE$ 电口； 5、配置 $\geq 2GB$ Cache 的 RAID 控制器，支持 RAID 0/1/5/10/50/60； 6、配置 $\geq 2$ 个标准电源，支持 1+1 冗余。	台	18
2	图片解 析服务 器	1、机架式服务器，非 OEM 产品，自主研发，国产品牌； 2、配置 $\geq 2$ 颗国产 CPU，每颗 CPU 核心数 $\geq 24$ 核，每颗 CPU 主频 $\geq 2.2GHz$ ； 3、本次配置 $\geq 384GB$ DDR4 4、配置 $\geq 2$ 块 2.5 寸 480G SSD 硬盘，配置 $\geq 6$ 块 2.5 寸 1.92T	台	5

		<p>SSD 硬盘，可支持 SAS/SATA 硬盘、SSD 混插；</p> <p>5、配置<math>\geq 2 \times 10\text{GE}</math>（含光模块）；</p> <p>6、配置<math>\geq 2\text{GB}</math> Cache 的 RAID 控制器，支持 RAID 0/1/5/10/50/60；</p> <p>7、本次配置<math>\geq 8</math> 块 16GB 图象处理加速卡；</p> <p>8、配置<math>\geq 2</math> 个标准电源，支持 1+1 冗余。</p>		
3	万兆接入交换机	<p>1. 交换容量<math>\geq 25\text{T}</math>，包转发率<math>\geq 1600\text{Mpps}</math>；</p> <p>2. 支持万兆 SFP+端口<math>\geq 48</math> 个、40/100GE QSFP28 端口<math>\geq 6</math> 个，支持可插拔双电源，独立可插拔风扇<math>\geq 4</math> 个；</p> <p>3. 支持 MAC 地址表<math>\geq 128\text{K}</math>、ARP 表<math>\geq 128\text{K}</math>、IPv4 路由表<math>\geq 192\text{K}</math>，IPv6 路由表<math>\geq 64\text{K}</math>；</p> <p>配置：</p> <p>配置交流电源<math>\geq 2</math>，冗余风扇模块；配置 3 米 40G 互联线缆（含两端光模块）<math>\geq 1</math> 根。</p>	台	8
4	万兆核心交换机	<p>1. 性能：交换容量<math>\geq 500\text{Tbps}</math>，包转发率<math>\geq 192000\text{Mpps}</math>，支持单槽位转发能力<math>\geq 4.8\text{Tbps}</math>；</p> <p>2. 硬件架构：主控引擎<math>\geq 2</math>，独立交换网板<math>\geq 4</math>，整机业务板槽位数<math>\geq 12</math>，独立风扇框数<math>\geq 5</math>，系统电源槽位<math>\geq 6</math>；</p> <p>3. 整机支持 MAC 地址<math>\geq 512\text{K}</math>、ARP 表项<math>\geq 256\text{K}</math>、IPv4 FIB 表项<math>\geq 512\text{K}</math> IPv6 FIB 表项<math>\geq 256\text{K}</math>；</p> <p>硬件配置要求：</p> <p>1. 四个交换机网板，48 口万兆光口接口板<math>\geq 4</math> 个、96 个万兆多模模块，16 个万兆单芯单模光模块，万兆虚拟化线缆 2 根。</p>	台	2
5	云存储系统	<p>存储系统含云存储软硬件、企业级硬盘，按重点部位监控存储 1 个月的量计算，存储系统至少提供 12.2PB 的容量。</p> <p>1. 品牌：国产品牌，存储产品为软硬一体，由同一厂商生产制造；</p> <p>2. 在多节点系统中，任何一个存储节点出现故障，应不影响数据的正常存取；</p> <p>3. 存储系统可对外提供多种类型数据混合存储，同时支持分布式文件存储；统一命名空间，将所有物理存储资源虚拟化成统一的存储空间；</p> <p>4. 支持存储空间虚拟化管理；支持多存储设备容量整合，形成录像池；可根据用户业务分配视频、图片等类型存储空间；</p> <p>5. 支持在线弹性伸缩录像池的容量空间，不影响业务继续读写数据分散存储到存储节点上，数据呈离散式分布；</p> <p>6. 支持按照接入任务数实现自动负载均衡，支持前端设备自动分配</p>	项	1

		到存储节点； 7. 要求能存储主流视频厂家前端设备的视频、图片等数据。		
6	NVR 网络硬盘 监控主机	1、USB3.0≥2 个、USB2.0≥2 个； 2、可接入≥8 块接口为 SATA 的硬盘； 3、可接入 H.265、H.264、MPEG4、Smart264、Smart265、SVAC 编码格式的前端设备并解码显示输出；可开启前端设备的智能编码模式； 4、可接入 G.711a、G.711u、G.722.1、G.726、G.729、PCM、AAC 音频编码格式的 IPC；可将音频采样率设置为 8kHz、16kHz、32kHz、48kHz、64kHz；支持双音轨 IPC 两路音频同时接入； 5、支持 Raid 功能，包括 Raid0、Raid1、Raid5、Raid6、Raid10、Raid50、Raid60、JBOD，支持一键创建 RAID5 阵列功能。 6、支持不少于 32 路 IPC 接入，可接入 ONVIF、PSIA、RTSP 标准、GB28181 协议的网络摄像机，并支持以私有协议方式接入第三方摄像机，可添加和激活局域网内的网络摄像机。	台	14
7	专用 IDC 数据 机柜 托管	1、满足《数据中心设计规范（GB 50174-2017）》B 级机房建设要求； 2、满足《信息安全等级保护管理办法（公通字[2007]43 号）》第三级信息系统运营、使用单位的管理要求； 3、具备与六安市公安局现有机房的双链路专网通信资源，专网通信需满足公安业务网络使用需求； 4、承担机房设备用电费用，承担机房内设备上架的综合布线费用； 5、提供 12 个 42U 标准机柜 5 年托管服务，并预留 12 个 42U 标准机柜用于后期扩容； 6、机房空间封闭独立使用（机柜环境封闭相对独立，不允许有与本项目无关的设备），并提供机房托管服务所必须的温湿度控制、环境监测、视频监控、网络（需无条件允许和支持 4 家运营商线路接入）等相关配套设施、设备、服务。	项	1
六、三级等保测评				
1	三级等 保测评 费	5 年三级等保测评	项	1

## 3. 服务要求

### 3.1. 项目建设要求

(1) 本项目需在 2023 年 6 月 20 日前项目建设完成，由中标供应商提出验收申请，采购人组织验收。验收合格后，中标人提供五年免费项目运维（软硬件系统），并提供软件系统的终身免费升级。投标供应商应按照以上要求，制定详细、可行的项目实施计划。

(2) 中标供应商在申请项目最终验收时，需提供第三方软件检测机构出具的检测报告，验收有关的三级等保测评、专家评审费等费用均包含在投标报价中，采购人不另行支付费用。评测内容涉及系统所有视频整合、业务逻辑、软件功能的全覆盖评测。包含但不限于以下内容：

适合性：功能促使指定的任务和目标实现的程度。

正确性：产品或系统提供具有所需精度的正确的结果的程度。

完备性：功能集对指定的任务和用户目标的覆盖程度。

### 3.2. 项目人员要求

投标供应商须提供详细的项目实施人员安排，人员组成应包括：项目经理、技术负责人、需求分析人员、系统设计人员、系统开发实施人员、系统测试人员等。在项目建设期内，项目组现场实施人员须协助业主方完成与相关单位的数据对接、沟通协调等建设工作，本项目要求常驻现场实施人员不低于 30 人。

在质保期内中标人应根据采购人相关要求配置相应的运维人员驻场服务，确保运维响应迅速、高效。提供不少于每年 2 人的驻场服务，服务期 5 年，有参与过相关工作经验。服务内容包括软件升级、版本更换、业务联调、技术支撑、重点保障、应急响应、风险评估、安全巡检、故障解决等。

### 3.3. 项目培训要求

供应商负责对采购人相关部门及指定的用户进行培训。供应商须根据项目实施的进度及时安排培训和授课。培训的主要内容应侧重于对系统的使用及系统的基本维护、常见问题及解决办法等方面，并提供实践性的操作，使受训者熟悉系统设计的思路，掌握系统的操作和维护等。投标供应商须制定详细的培训计划，明确培训目标、参训人员、课程内容、时间、场地、考核等相关安排。供应商需为采购人培训 2 至 3 名具备 ITSS 或 CISP 或 CCRC 等证书的维护人员。

### 3.4. 项目维保要求

投标供应商须为本项目开发的应用软件提供 5 年免费质保和终身免费升级，硬件设备提供 5 年免费质保。

质保期自项目终验之日起计算，质保期内维保要求如下：

（1）需成立专业运维团队。提供全天候 7×24×365 不间断服务支持，24 小时应急热线电话，快速响应项目维护需求，随时提供技术支持与使用指导，包括故障排除、性能调优、技术咨询等。

（2）常驻专职维护管理人员每天应当主动检查监控的视频图像是否正常，每天应人工巡检二次以上；主动发现故障并进入维护流程。每天记录维护日志，每周形成周维护报告，每月形成月维护报告。须定期安排相关技术工程师到业主方现场进行软、硬件系统及中心机房的全面巡检服务，例行检测、排除隐患，对软、硬件系统的整体运行状态进行评估分析，提供详细巡检报告，并给出优化调整建议。

（3）维护人员除每天的抢修维修工作外，每月对工程范围内的设备箱、设备及其供电系统进行一次巡检维护，包括设备除尘、排除遮挡物、排除故障隐患、摄像机除尘清洁等，以确认所有设备及系统工作正常，并将巡检工作在月维护报告体现。

（4）维护具体内容包括（但不限于）：前端摄像机的镜头调试、设备除尘除雾、位置调整、摄像机维修及更换（摄影机设备由建设单位提供）、故障排除等；光纤线路、摄像机控制线路和接口检测、隐患排查、故障排除；摄像机传

输设备的维护和故障排除。

（5）对项目范围内的软件、硬件设备故障问题，须及时处理。如出现故障在 1 小时内作出响应，紧急问题在 4 小时内解决。一般问题在 24 小时内解决，如果 24 小时内无除不可抗力外，设备出现故障、损坏，须及时免费更新维护。投标供应商应按照以上要求，规划设计合理可行的售后服务方案。

（6）故障响应服务完成后整理详细的事故处理报告，内容至少包括事故原因分析、已造成的影响、处理办法、处理结果、预防和改进建议。

#### （7）应急保障

在遇到重大的活动和事件以及用户需要时，及时调派足够的技术力量，为公共场所视频监控资源整合共享安全体系的正常运行提供应急保障。

### 3.5. 项目验收要求

（1）中标供应商完成工作内容后向采购人提验收申请，经采购人组织评审通过视为验收合格。

（2）采购人负责组织实施工程各阶段的验收工作，中标供应商须协助采购人配合采购人完成各阶段验收工作的准备，包括但不限于：整理完成各类文档（电子、纸质）、准备验收环境、各类支撑工具。

（3）中标供应商对于工程各阶段的验收中发现的问题，组织提出有效解决办法和措施。

（4）中标供应商对于工程各阶段验收中有关本项目的内容提供电子和纸质两种介质的产出物，并保持版本一致，纸质的须经采购人签字认可。

（5）中标供应商提供的各类文档应内容完整、描述清晰、版本最新，各类方案要求实现目标明确、工作措施得力、可操作性强、具有前瞻性。

（6）项目竣工时，中标供应商需提供气象部门出具的防雷检测报告。