# 东莞市水务集团管网有限公司智能安防系统项目

# 用户需求书

## 一、项目概况

### **（一）项目业主**

东莞市水务集团管网有限公司

东莞市莞泽水环境投资有限公司

东莞市东信水环境投资有限公司

东莞市东泽水环境投资有限公司

东莞市清泽水环境投资有限公司

东莞市莞清水环境投资有限公司

东莞市东江水环境投资有限公司

### **（二）招标人**

本项目由项目业主委托东莞市水务集团有限公司作为招标人进行招标，确定中标人后，由项目业主共同与中标人签订采购合同。

### **（三）项目名称**

东莞市水务集团管网有限公司智能安防系统项目

### **（四）采购预算**

本项目不含税最高投标限价为813,295.49元，其中东莞市水务集团管网有限公司及各直属企业（以下按各公司简称）之间的费用分摊比例约为：管网公司10%，莞泽公司10%，东信公司10%，东泽公司20%，清泽公司20%，莞清公司15%，东江公司15%。

## 二、项目内容

### **（一）项目建设背景**

根据管网公司实际业务需求，构建管网公司级智能安防系统，作为水务集团智能安防管理平台的二级组成部分，对接水务集团智能安防管理平台，统一管网公司视频等安防系统，计划2025年年底前系统上线试运行。

### **（二）工作目标**

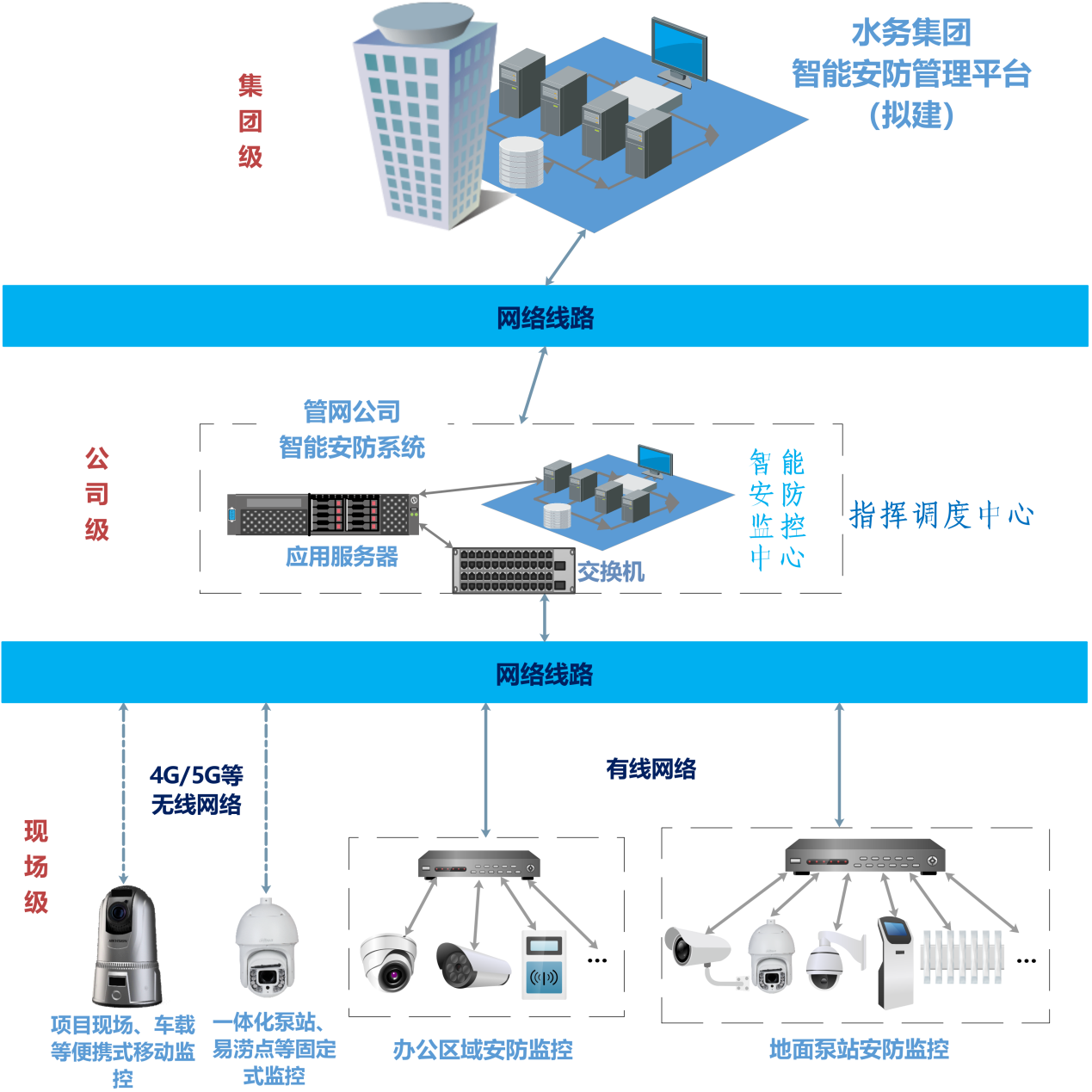
通过本项目建设，建设公司级、现场级多级联动、联网共享、分级指挥的智能安防软件系统，实现管网公司办公区域、生产运营区域、工程施工区域安防监控数据的统一汇聚，实现对外部入侵、人员访问、车辆进出、区域监控、行为监控的及时预警、数据共享、联动指挥，达到防入侵、防破坏、防事故的成效，提高公司整体智能安防水平，并进一步提高对项目现场的远程管理水平，提高管网公司各管理部门及分公司管理人员对项目生产运营现场监管力度及效率。

### **（三）项目建设内容**

管网公司智能安防系统是利用软件系统对安全防范的视频监控系统、出入口控制系统、入侵报警系统、电子巡查系统、访客管理系统等安防子系统及相关信息系统进行集成，实现全公司范围内的实体防护系统、电子防护系统和人力防范资源的有机联动、信息的集中处理与共享应用、风险事件的综合研判、事件处置的指挥调度、系统和设备的统一管理与运行维护等功能的软件系统。

**1.系统总体架构**

本次项目拟建设内容为管网公司智能安防系统，计划通过统一汇聚的智能安防系统从软件系统层面统筹公司级安防系统及现场级安防系统。现场各类安防设备通过有线网络或4G/5G无线网络连接方式提供网络通信数据，传输至智能安防系统专用服务器，实现各子系统的关联畅通，总体架构如下：



**管网公司智能安防系统总体架构**

**2.系统功能模块**

管网公司智能安防系统除智能安防管理系统子模块外，还包含视频监控系统、出入口控制系统、入侵报警系统、电子巡查系统、访客管理系统等安防子系统模块。各子系统主要软件功能如下：

**（1）智能安防管理系统**

智能安防管理系统是面向公司级安防监控、事件处置、指挥调度业务的安防管理应用中心，其主要功能应包括联动监控、设备管理、人员管理、车辆管理、指挥调度、基础信息管理、系统管理、系统校时、系统安全、日志管理、统计分析、移动端等。

主要实现对各子系统及系统、用户权限的管理，包括：实现与上下级联网的管理、认证和日志。支持监控点管理、系统管理、用户管理及权限管理功能，可对用户优先级进行设置管理。提供对运行日志、操作日志的查询、导出、打印功能，运行日志应能记录系统内设备启动、自检、异常、故障、恢复、关闭等状态及发生时间；操作日志应能记录操作人员进入、退出系统的时间和主要操作情况。

**（2）视频监控子系统**

视频监控系统为智能安防系统最重要的组成部分，可根据视频图像采集、目标识别的需要和现场环境条件等因素进行设计，并选择相应的设备。具备对监控区域和目标进行视频采集、传输、处理、控制、显示、存储与回放等功能，在此基础上可扩展AI视频分析功能，实现对人、车、事件等要素的自动识别、预警功能。

主要用于接入管网公司办公区域、办公及生产运营车辆、施工现场（含维修、清疏、导排等）、巡检现场（含巡查、检测、测量等）、泵站、隧道、易涝点、积水点、溢流点以及通沟污泥处置（含暂置场所、转运和处置场所全链条）等区域视频设备，实现远程视频接入、数据展现与管理，具体实现功能如下：

①视频查看

支持基于虚拟视频组的自动轮巡功能，支持按组轮巡和按窗口轮巡两种模式，可自由设定触发序列和时间间隔，视频组图像可在单个画面内和多个画面轮巡显示，支持实时监控、实时截图、实时录制功能。

实现对智能摄像头采集的事件信息进行集中展示、查询，事件可分级分类并触发报警，支持通过事件播放关联相关视频的录像，实现任意采集通道的图像信息切换给任意监视终端。

支持画面进行放大、缩小、全屏显示操作，支持可最多同时查看不低于25路（5\*5）图像信息，支持摄像机显示列表、列表排序、快速搜索功能，对监控区域内的人员及机动车的出入、活动情况进行24h实时监控并录像。

▲支持全景摄像机，实现360度的全景监控，可以对全景区域内的多个目标进行穿越警戒面、区域入侵、进入区域、离开区域行为的检测。

▲支持在预览监控点画面时进行一键上墙、 云台控制、语音对讲。

▲支持低功耗相机接入，实现休眠唤醒并进行预览、回放。

②视频控制

实现对各分控点监控设备进行远程控制。能实现对摄像机、镜头、云台等部件的自动或远程手动控制功能，自动控制支持光检测信号触发、事件触发、周期触发等触发机制，远程手动控制支持电源开启关闭、镜头运动、镜头变焦、防护罩/雨刷/风扇的开启、关闭，视频的录像、放像、停止。

③视频转发

支持视频分发功能，节点互联、监控客户端、电视墙服务、视频存储服务的视频传输通过流媒体技术进行码流复制转发，支持基于流媒体转发的存储管理功能，中心可对监控点任意一路视频图像进行备档存储。

④录像管理

提供录像检索、录像回放、回放控制功能，支持多路视频录像回放及下载，可按日期、时间、类型、服务器、通道检索客户端本地、存储服务器、前端设备的录像文件。

支持同时查看多路同一时间的录像回放，拖动时间轴时多路录像能同时定位到任意时间的录像；支持录像普通下载，框选下载功能。

▲支持配置级联点位录像计划。

▲支持中心存储录像计划，支持配置备份资源池，实现双备份。

⑤视频编辑

支持视频帧标记功能，可为每帧图像增加标记，以帧标记作为索引条件进行录像文件的快速检索。实现对视频图像进行解码、转发、图像嵌入与文字叠加等处理，以及图像地址、时间等符号在画面上叠加。

▲支持视频画面叠加水印，包括视频预览、录像回放、即时回放、录像剪辑、手动录像和录像下载时叠加。

⑥有限空间、密闭空间预警与监测

涉及有限空间、密闭空间作业管理情况下，应能支持对有限空间、密闭空间等作业情况进行实时视频的查看和预警，预警信息应及时推送相关安全管理人员，实现远程作业预警、监管功能。

⑦设备管理

提供灵活的配置管理功能，可在线对全网的视频设备进行配置管理和维护管理，支持对设备设置控制级别和权限管理。

支持在电子地图实时显示视频系统设备正常、异常、报警工作状态。

支持异构设备（硬盘录像机、视频服务器、网络摄像机、网络硬盘录像机等）、异构视频监控平台、报警主机、语音主机模块，以实现与各类异构资源的接入管理。

支持设备管理、业务管理、网络管理、运维统计等功能，设备管理包括服务器、数字视频设备、数字矩阵等，业务管理包括数据状态、视频状态、CPU占用、内存占用、网卡连接状态，网络管理包括网口实时流量、磁盘状态、RAID状态等，运维统计包括统计摄像机、监视器、设备连接的信息。

客户端、录像服务器、存储转发服务器提供日志管理功能，同时日志信息应自动上传中心视频监控管理服务器，中心视频监控管理服务器对日志进行统一管理，可通过用户或时间进行分类搜索。

有防干扰、防拆、防破坏、防雷、视频信号丢失报警等功能。

▲支持视频质量诊断的监控点总数统计展示，包括图像正常数、图像异常数、诊断失败数、未检测数。

▲支持查看设备告警总数、设备掉线告警数、设备总数、设备在线、离线、未检测数。

⑧与其他系统联动

视频监控图像应与出入口控制系统、入侵报警系统等实现联动，报警信息与图像联动响应时间≤4s。

此外，视频监控子系统利用视频数据进行智能分析，实现智能巡检管理功能，提供模型管理、模型下发、智能分析配置、抓图计划配置。通过将AI模型下发至设备，为设备通道配置智能分析任务，使设备拥有针对特定对象和场景的智能分析能力，能够解决碎片化场景下的智能分析问题并支持其他算法拓展及提供算法训练功能，同时支持智能巡检计划管理与管理及报警事件的处置等功能。

**（3）出入口控制子系统**

出入口控制应用系统应具备处理、通信、配置、出入口控制、监测、告警等功能，可远程监控各控制器工作状态，支持对泵站等区域重要部位的通行门以及主要的通道口进行出入权限控制，支持统一授权用户下发、黑白名单用户下发，可对不同角色分类、授权。

出入口控制系统的管理控制功能应符合以下要求：

接收识读部分传来的操作和钥匙信息，与预先存储、设定的信息进行比较、判断，对目标的出入行为进行鉴别和校核；对符合出入授权的目标，向执行部分发出予以放行的指令。

远程设定识别方式、出入口控制方式，输出控制信号，处理报警情况，发出报警信号。

出入口控制系统应与视频监控系统实现联动，报警信息与图像联动响应时间≤4s。

联网控制型系统中编程/控制/数据采集信号的传输可采用有线或无线传输方式，且应具有自检、巡检功能，应对传输路径的故障进行监控。

应具有事件记录功能：将出入事件、操作事件、报警事件等记录存储于系统的相关载体中，并能形成报表以备查看。

▲要求支持在访客平台中登记过的访客车辆进入停车场时自动放行。

**（4）入侵报警系统**

入侵报警系统需具备远程对入侵报警、故障、被破坏进行记录，并对前端硬件进行控制等功能。

入侵报警系统需与视频监控系统联动，泵站等重点区域的入侵报警信号与联动视频图像应发送到智能安防管理系统。报警传输系统应具有自检、巡检功能。

报警发生时，能够在电子地图上显示、局部放大报警部位，并以声、光信号显示报警的具体位置。

系统需具备实时记录系统开机、关机、操作、报警、故障等信息，并具有查询、打印、防篡改功能。

▲要求支持获取报警主机的防区信息及扩展防区信息；支持对扩展防区进行布防、撤防、旁路、旁路恢复操作；支持接收扩展防区的上报事件。

**（5）****访客管理系统**

支持访客身份证、人脸、车辆等信息录入与来访审批，可识别身份证的身份信息，人脸信息与身份信息可自动比对，确认人员身份。

应能登记和管理外来人员的基本信息、访问联系人、访问地址、访问时间，并具备增加、修改和删除功能。

应具备人员基本信息的查询、统计和报表打印功能。

▲支持接入访客机（带扫描仪），可通过扫描护照、市民卡、驾照、港澳通行证、中国台湾通行证等证件来获取证件信息并留档。

▲支持访客足迹查看，包含门禁人员出入事件、可视对讲出入事件、人脸监控记录、梯控事件、停车场出入事件。

具体结合各业务线具体应用场景需求的各子系统详细功能及AI智能分析功能详见**本用户需求书附件1：《管网公司智能安防系统建设方案》**。

**3.设备数据接入**

根据对全公司各部室分公司的调研数据，管网公司预计要接入的安防监控设备接入的数据量主要如下（详细清单详见**本用户需求书附件2：《管网公司安防监控设备清单收集表(202405)》**）：

（1）视频监控摄像头至2024年底约1866路，考虑远期暂定3200路接口；

（2）车辆道闸至2024年底约12路，考虑远期暂定50路接口；

（3）ID/IC、人脸、指纹等类型门禁至2024年底约107路，考虑远期暂定300路接口；

（4）电子围栏至2024年底约25套，考虑远期暂定100路接口。

此外，所有类型设备接入路数均需支持未来进一步增加数量拓展及类型升级。

中标人在整个系统质保期完结之前需对项目业主购买的数据接入路数范围内，对项目业主已建、在建的支持安防系统GB28181、onvif、SIP等国家/行业标准及开放物联接入协议OTAP等行业通用协议的安防监控设备提供数据接入服务，并进行调试保障接入设备的数据传输稳定。

### **（四）采购清单**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **模块** | **名称** | **技术规格** | **单位** | **数量** | **备注** |
| 1 | 联动监控模块 | 视频监控应用 | 视频监控应用提供视频管理服务，支持编码设备通过GB28181协议、ONVIF协议接入平台，实现视频预览、录像回放、视频上墙、视频事件监控服务能力，并且在网络带宽不足、有流量限制的网络环境下可以通过以图片替代视频的模式提供监控服务。 一、视频预览 1.支持视频实时预览能力，实现预览窗口布局切换、预览画面自适应及全屏切换； 2.支持云台控制、实时抓图、紧急录像、即时回放、主子码流切换、声音开启\关闭、辅屏预览（1个辅屏）、对讲、广播、报警输出控制的能力； 3.支持智能规则展示的能力（如：针对热成像设备温度信息实时展示）； 4.支持资源视图管理能力，以视图形式管理监控点、视频预览轮巡等自定义资源组，其中视图类型包含公有视图和私有视图； 5.支持全景视频监控预览能力，支持球型鹰眼、全景摄像机的全景模式； 6.支持为不同账号配置视频预览时长，到达预览时长后自动停止取流，避免因忘记关闭视频画面导致的流量浪费 7. 支持太阳能摄像机的电量显示、低功耗唤醒，热成像摄像机的温度数据、事件数据接收，AI摄像机的告警事件接收等应用功能 二、录像回放 1.支持录像计划管理能力，支持实时录像计划、录像回传计划； 2.支持录像回放能力，支持多画面同步回放和异步回放切换、超高倍速回放、分段回放、录像下载、录像剪辑、录像标签、录像锁定、录像抓图； 三、图片监控 1.支持视频预览与图片实时监控模式切换能力，实现图片监控模式； 2.支持图片查询回放能力，实现按监控点、时间段展示抓拍图片； 3.支持图片自动播放能力，支持图片自动播放速度可设置； 4.支持图片下载能力； 四、视频上墙 1.支持电视墙场景管理能力，实现场景窗口配置、场景切换计划配置以及轮巡计划的管理； 2.支持上墙控制能力，实现场景一键上墙、场景切换、电视墙切换、监控点上下墙、轮巡控制操作； 五、视频事件 支持视频事件布撤防能力，可按计划模版进行布防，事件类型包括移动侦测、视频丢失、视频遮挡、报警输入、报警输出； | 路 | 3200 |  |
| 2 | 视频联网管理 | 提供视频点位联网服务能力，用于平台域间视频联网，基于视频通用标准协议（GB/T28181-2011,GB/T28181-2016）与外域平台互联互通，实现平台视频资源点位推送等操作控制。 1.支持上下级域注册管理能力，实现平台数据级联； 2.支持资源同步能力； 3.支持级联视频点位实时预览、录像回放、录像下载、语音对讲能力； 4.支持级联视频点位设备操作控制能力。 | 套 | 1 |  |
| 3 | 门禁事件管理 | 支持对接门禁设备 1.支持配置平台接收到事件类型； 2.支持配置事件保存时长； 3.支持查询人员出入事件和设备事件； 4.支持人员进出事件实时展示，包括人员基础信息、抓拍图片、进出时间、设备名称等，可全屏展示 | 门 | 300 |  |
| 4 | 出入口管理 | 支持对接停车道闸设备，获取过车数据 1.支持查看车道的过车记录，包含过车时间、车牌号码、车辆类型、停车库、入库口等 2.支持远程查看各车道设备的在线状态 3.支持远程控制车道，对车道进行开闸、关闸、常开和呼叫的操作 | 车道 | 50 |  |
| 5 | 入侵报警管理 | 入侵报警应用基于前端防区探测器进行园区范围内的入侵行为或意外事件的迅速感知和处理，实现针对园区内部的高效安全防范。 1.支持报警子系统管理能力，包含布防、撤防、消警控制操作； 2.支持防区管理能力，包含旁路、旁路恢复操作； 3.支持实时入侵报警能力； 4.支持历史入侵报警事件查询及导出能力 | 路 | 100 |  |
| 6 | 设备管理模块 | 系统管理 | 1.提供门户首页内容自定义能力，支持自定义快捷入口、自定义菜单内容、自定义页面元素设置；支持门户展示元素自定义，包括页面logo图标、修改网站标题、设置并添加网站外部链接； 2.提供统一的认证、鉴权管理、应用管理、菜单管理、用户管理、角色管理、组织管理、资源管理等能力； 3.提供用户权限管理能力，包括菜单权限、组织权限、区域权限、资源权限、功能控制权限； 4.提供组织、区域、设备、人员、卡片、车辆等资源统一管理； 5.提供用户安全管理，支持账户绑定用户mac地址及IP地址能力，提供账户安全设置，支持账户密码有效期设置，支持登录类型（Web端、PC客户端、移动端）和认证方式（密码、PKI）的配置； 6.提供NTP校时服务能力，支持对设备和服务器统一校时; 7.提供数据、服务等统一开放能力； 8.提供系统运行状态监测能力，包括运行服务监控、运行服务统计、运行数据报告和运行服务解析概览。 | 套 | 1 |  |
| 7 | 设备运维台账 | 将设备资产统一数字化建档，对设备设施运行全生命周期的管理：  1.设备台账：直观展示当前项目上的设备资产总体情况（包括使用中设备数量、报废设备数量等），提供设备明细列表，支持按照设备分类、设备名称、使用状态、设备用途等关键字段查询，支持台账数据导出Excel表；  2.设备档案，提供完整的设备档案信息管理，采用多级设备分类，支持自定义设备分类，支持扩展属性登记，为设备创建唯一二维码身份标识；档案信息包括设备基础信息、维修记录、保养记录等；  3.设备报废：对设备报废的的流程进行标准化管理，包括设备报废申请，设备报废审批，设备报废记录，更新设备档案。 | 套 | 1 |  |
| 8 | 设备在线运维管理 | 设备网络管理应用，对接入平台的视频设备，门禁设备进行在线巡检，及时发现故障设备和掉线设备，使运维工作更加高效，便利。 一、视频网络管理 1.支持监控摄像机、编码设备、存储设备、解码设备等物联设备在线状态、工作状态、硬盘状态、指标采集。 2.支持监控点通道的在线状态、录制状态、录像完整性、录像保存天数指标检测。 3.支持告警信息统计展现。并支持对监控点、编码设备、解码设备、视频综合矩阵、NVR/CVR、云储存、门禁设备、门禁点、读卡器、梯控设备/梯控读卡器/可视对讲的告警阈值进行配置。 4.提供视频运维报表统计能力，包含区域综合排名统计、录像完整性统计、录像存储达标统计、在线状态统计、离线时长统计报表。 5.支持巡检计划配置，可以按照类型和资源以及自定义的巡检周期进行巡检计划配置。 二、门禁运维管理 1.提供门禁设备在线状态监测能力； 2.提供门禁设备运维报表统计能力。 三、可视对讲运维管理 1.提供门口机、室内机、管理机、围墙机设备在线状态监测能力； 2.提供可视对讲设备运维报表统计能力； 四、停车场出入口运维管理 1.提供岗亭缴费终端、出入口控制设备、出入口显示设备、读卡设备在线状态监测能力； 2.提供停车场出入口设备运维报表统计能力； | 套 | 1 |  |
| 9 | 视频质量诊断 | 视频质量诊断应用，提供视频图像诊断和监测服务。 1.支持监控点通道的图像质量诊断结果统计和查看。 2.支持图像模糊、图像过亮、图像偏色、图像过暗、图像过亮、视频抖动、视频丢帧、场景变换、视频遮挡、对比度、条纹干扰、噪声干扰、信号丢失、黑白图像指标诊断。 3.支持码流分辨率、编码格式指标采集。。 4.支持诊断对比图查看和诊断结果矫正功能。 5.支持巡检计划配置，可以按照类型和资源以及自定义的巡检周期进行巡检计划配置。 6.支持监控点图像质量统计报表，展现各类诊断故障数量。 7.支持海康SDK、大华SDK、ehome、isup5.0、GB28181.部标808.Open Network Video Interface、ISAPI协议。 | 路 | 3200 |  |
| 10 | 人员管理模块 | 通行权限管理 | 1.支持按组织、人员、人员分组、门禁点维度配置权限； 2.支持设置权限有效期、计划模板、假日计划； 3.支持按人员特征属性生成人员分组，如证件类型、岗位等级、职称等； 4.支持权限增量下发、初始化下发； 5.支持按时段配置门的常开常闭状态； 6.支持认证方式设置，可按不同时段设置不同的认证方式，如刷卡+人脸、刷卡+指纹； 7.支持首卡常开，刷首卡可使门保持常开至常开时间段结束，若此期间再次刷首卡，门恢复正常状态； 8.支持特殊卡设置，包括残疾人卡（可延长开门时间）、黑名单卡（无法开门）、胁迫卡（正常开门并上报胁迫报警）、超级卡（不受限于门常闭、刷卡+密码认证需要密码确认的规则，刷卡直接开门）； 9.针对刷卡开门方式，即使卡片权限未同步到设备，也可通过中心平台完成权限认证开门。 10.支持调整已超出或即将超出设备容量的人员生物特征； 11.支持按门禁点、人员、组织、区域等多维度，综合查询权限配置、下发状态等信息； | 套 | 1 |  |
| 11 | 访客管理 | 访客管理提供访客预约、访客登记、人证比对、访客签离、访客权限管理、短信通知、来访记录查看等功能。针对不同的场景可自定义访客单内容、短信内容、访客信息字段等。 一、提供访客预约管理应用 1.支持管理员在平台端进行访客预约操作； 2.支持访客自助预约，通过扫描二维码或者通过被访人提供的手机H5网页链接进行预约操作； 3.支持访客邀约，被访人通过手机浏览器进入H5网页发起访客邀约，填写访客基本信息； 4.支持被访人访客预约审核，访客通过H5自助预约的信息，需要经过被访人审核，审核后短信通知访客审核结果； 5.支持访客黑名单识别，黑名单中的访客无法进行预约； 二、提供访客登记管理应用 1.支持人工访客机已预约登记，已预约访客通过二维码、身份证、验证码在人工访客机进行登记； 2.支持人工访客机未预约登记，未预约访客通过刷身份证或手动输入在人工访客机上进行未预约登记； 3.支持自助访客机已预约登记，已预约访客通过二维码、身份证、验证码在自助访客机进行登记； 4.支持自助访客机未预约登记，未预约的访客，由内部员工刷员工卡，授权访客进行自助登记； 5.支持访客登记时进行人证比对； 6.支持访客黑名单识别，黑名单中的访客无法进行登记； 5.支持离线登记，访客客户端断网或者连接服务器失败时，启用离线登记模式进行本地登记，客户端在线后将登记数据回传到平台； 6.支持预约免登记，设置预约免登记后，已预约的访客，预约完成后自动完成登记，无需现场通过访客机再次登记，直接进入拜访； 三、提供访客权限管理应用 1.支持设置访客权限组，权限范围包括门禁、梯控、门口机、停车场、人脸管控； 2.支持设置默认访客权限组，访客登记时默认具有该权限组的权限； 3.支持登记时指定访客权限组，登记完成后访客具有指定权限组的权限； 3.支持权限变更，在人工访客机上对已登记访客进行权限范围和权限时长修改； 4.支持针对下发失败的权限重新下发； 四、提供访客签离管理应用 1.支持在访客机上人工签离； 2.支持设置门禁点位自助签离点，访客在门禁点完成自助签离； 3.支持自动签离，针对超期未签离的访客，系统在当天23:59分后自动完成签离； 4.支持签离后回收访客权限； 五、提供短信通知管理应用 1.支持预约、登记、签离流程的短信通知启用或关闭，且短信内容支持自定义； 2.短信通知模板包括邀约通知访客、预约待审核通知被访对象、审核失败通知访客、预约成功通知访客、取消预约通知访客、预约成功通知被访对象等； 六、提供访客记录查询应用 1.支持访客预约记录查询； 2.支持访客来访记录查询； 3.支持在来访记录中查看访客足迹，包括在门禁点、门口机、梯控设备、抓拍摄像机上产生的访客记录，足迹在地图上按时间顺序展示； 4.支持异常访客记录查看 | 套 | 1 |  |
| 12 | 移动端访客预约（微信、飞书、APP等） | 为提高外来人员的来访体验及登记效率，提供移动端访客预约应用，主要包括在微信公众号中访客自助预约或被访人邀约,也支持在综合安防APP、企业微信、钉钉、飞书中进行被访人邀约、被访人审批。 一、访客自助预约 1.支持访客通过移动端进行预约申请； 2.访客自助预约后，支持通过移动端向被访人发送审核通知消息，被访人审核处理完后，移动端消息通知访客； 3.支持快速再次预约，访客可在历史预约记录基础上修改预约时间进行快速预约； 4.访客可查看预约信息中的二维码凭证，作为访客身份验证的凭证。 二、被访人邀约 1.支持被访人通过移动端进行访客邀约； 2.被访人邀约后，支持通过移动端向访客发送邀约通知消息，访客进行应邀处理，应邀处理完成后，消息通知被访人； 3.被访人可以在未超过访客拜访时间内，取消邀约，并消息通知访客。 三、被访人审批 1. 支持被访人审批访客自助预约信息，可选择通过或退回，退回需说明原因，并消息通知访客。 四、记录查看 1. 支持访客查看预约记录、受邀记录； 2.支持被访人查看邀约记录、审批记录、被访记录。 | 套 | 1 |  |
| 13 | 车辆管理模块 | 车辆权限管理 | 1.支持固定车、临时车、预约车、黑名单车辆的管理 2.支持黑名单车辆管控，黑名单车辆进出报警提醒 3.支持预约车管理，按次预约和按时段预约 | 套 | 1 |  |
| 14 | 数据可视化模块 | 安防数据可视化看板 | 为用户提供安防数据看板，展示内容包括： 1.重点区域点位视频实时监控； 2.今日、近一周、近一个月告警统计：总事件量、已处置事件量、未处置事件量、处置率；近一周、近一个月告警事件数量趋势； 3.实时告警展示列表（图片形式）：展示内容包括告警类型、事件源、所属区域、发生时间； 4.今日、近一周、近一个月告警事件类型统计，事件类型包括入侵报警、紧急报警、视频报警、陌生人告警、重点人员识别告警、安检告警； 5.今日、近七天、近一个月告警事件数量区域TOP5排名； 6.今日巡更情况展示：展示内容包括已巡数量、未巡数量、巡更异常数量； 7.今日设备运维：全量设备运维统计（数量、在离线状态）。 | 套 | 1 |  |
| 15 | 人员态势数据可视化看板 | 为用户提供人员态势数据可视化看板，展示内容包括： 1.人员信息统计（总人数、卡片数、人脸数、男女比例）； 2.部门人员数量TOP5统计； 3.今日访客数量统计、今日、近一周、近一月访客来访趋势； 4.重点通行点位视频、人员通行实时记录展示； 5.今日人员告警事件统计； 6.今日、近一周、近一月人员通行趋势； 7.今日通行TOP10的门禁通道统计； | 套 | 1 |  |
| 16 | 设备运维数据可视化看板 | 为用户提供运维数据可视化看板，展示内容包括： 1.视频设备运维统计，包括视频设备在离线统计、监控点在离线统计、视频质量诊断统计、视频录像诊断统计； 2.门禁设备、可视对讲设备、梯控设备、停车场设备、消防设备、其他类设备的在离线统计； 3.近一周、近一月各类设备在线趋势图； 4.设备告警事件统计、区域设备在离线设备统计； 5.设备离线次数TOP10区域统计。 | 套 | 1 |  |
| 17 | 访客数据可视化看板 | 为用户提供访客数据可视化看板，展示内容包括： 1.总预约人数、在访人数（预约到访、未预约到访）、已签离人数、滞留人数 2.按今日、7日、30日、自定义日期统计来访人数趋势 3.按被访组织排行TOP5，按来访事由排行top5 4.实时展示最新来访人员 5.查看来访人员信息记录，内容包括照片、姓名、车牌、被访人、来访时间、权限组、来访事由等 | 套 | 1 |  |
| 18 | AI事件分析模块 | 智能监控应用 | 一、人员管控应用以人脸技术为核心，通过前后端分析设备对人脸图片进行比对分析，实现人脸自动识别，以提供人员管控服务的能力。 1.支持配置重点人员识别计划、陌生人识别计划、高频人员识别计划； 2.支持接收重点人员、陌生人、高频人员实时事件； 3.支持配置智能分析规则，实现智能分析服务器的事件上报； 二、智能检索应用以人脸技术、视频结构化技术为核心，通过前端视频和后端比对分析设备对人体、车辆抓拍图片进行分析，以提供智能检索服务的能力。 1.支持配置人体、车辆识别计划；支持接收人体、车辆实时事件； 2.支持人脸、人体、车辆的以图搜图；支持人员运行轨迹展示； 3.支持人脸记录查询； 三、实时视频/录像文件结构化分析：应用于园区、办公大楼、写字楼、厂区场景，利旧已有视频资源，针对实时、历史视频数据进行智能结构化分析。 1.通过配置实时流分析任务完成视频流实时智能分析，包括重点人员、陌生人、高频人员、人体/车辆结构化分析； 2.支持配置录像点位及目标时段，对录像码流中的人、车数据进行结构化录像码流分析，实现智能分析事件快速查询。 | 套 | 1 |  |
| 19 | AI算法模型管理 | 提供模型管理、模型下发、智能分析配置、抓图计划配置。通过将AI模型下发至设备，为设备通道配置智能分析任务，使设备拥有针对特定对象和场景的智能分析能力，能够解决碎片化场景下的智能分析问题。 1.算法管理，提供智能算法包的上传，删除，展示及查看功能； 2.任务管理，为所有用户提供图片和视频人脸，车辆，人体分析任务及人员聚类任务的创建功能，同时支持已创建任务的控制（启动，停止，删除）和查询等； 3.参数管理，主要针对管理员用户提供任务优先级配置、计算资源动态调整配置，及存储资源配置（保存智能分析结果使用）的等操作。 | 套 | 1 |  |
| 20 | 安防AI场景治理 | 支持场景清单创建，邀请多人协同场景治理，可对枪机、球机做场景治理，完成不同算法的规则配置。 新建场景治理：在清单治理界面新建治理清单，填写清单名称，自动生成治理清单编号，创建人为当前用户，选择算法（从算仓获取算法分组列表，可以多选）。 治理指派：治理清单可指派给他人进行治理，指派后的单子会在个人工作台有消息提醒。 场景治理：支持为区域+能力定位的场景配置多条分析规则，支持基于不同能力配置不同分析规则，支持城管类能力配置置信度、灵敏度规则参数，支持AI开放平台训练出来的图片类算法配置全分析规则，支持AI开放平台训练出来的视频配算法配置智能事件分析（IED）规则 治理进度统计：算法维度——对算法进行筛选，查看指定算法的治理进度，展示每个算法下的点位的治理详细信息；点位维度——对组织下的点位展示关联的算法和治理的情况 | 套 | 1 |  |
| 21 | 智能分析资源管理 | 面向公司各级用户（公司级及现场级），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，帮忙申请者、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。支持从点位搜索、视频广场、工作台（若有）直接发起智能分析申请。 | 套 | 1 |  |
| 22 | 指挥调度模块 | 事件中心 | 提供系统报警事件接收、事件处理、事件联动、事件检索能力，提供场景化的事件联动应用（在“特定条件”下执行“特定动作”），报警事件产生时，可以通过多种方式、多种联动场景提醒安保人员，联动方式包含视频弹窗、视频上墙、录像联动、云台联动、短信联动、邮箱联动、IO联动、抓图联动、门禁反控联动等。 一、事件联动管理 1.支持事件联动规则配置管理，包括规则增删改查，支持自定义联动规则模板； 2.支持事件规则计划模板，包括全天候模式、工作日模式、周末模式及自定义模式； 3.支持多种报警事件配置联动，包括：视频事件、入侵报警事件、IO事件、门禁事件、停车场事件、可视对讲事件、行车监控事件、梯控事件、动环事件、紧急报警事件、人脸事件、卡口事件、消防事件、测温事件等事件联动动作配置； 4.提供7种高级联动规则模版配置，支持配置满足在指定时间段存在多个触发事件类型而联动多个并发动作的场景。 二、事件检索管理 1.支持报警事件自定义时间存储，最长支持36个月存储； 2.支持多种维度检索报警事件，包括：区域、位置、事件源、事件等级、时间、状态等维度； 3.支持事件详情查看，包括抓图、录像等； 4.支持对报警事件进行标记、处理以及导出。 | 套 | 1 |  |
| 23 | 图上监控 | 提供各类资源图上展示及控制操作，在地图上可展示各类资源点的地理位置，通过接收资源点报警事件，实现报警信息可视化展示。 1.支持地图配置能力，包含在线地图、离线GIS地图（高德、自定义等）； 2.支持资源上图配置能力，实现资源的地图可视化展示及控制操作，资源类型包含监控点、报警输出、报警输入、门禁点、出入口、停车场、传感器、手持视频终端、园区卡口资源、防区、报警输入、报警输出、报警主机IO输出、消防设备等； 3.支持事件可视化监控能力，实时展示报警事件，支持历史报警事件查询； | 套 | 1 |  |
| 24 | 告警事件处置 | 事件处置应用提供事件联动的报警事件处置能力，通过移动端及客户端应用的方式，实现报警事件真实性的确认，能人工指派相关处理人进行处置并保存事件处置记录，帮助用户实现报警处置业务闭环 ，提升用户针对报警事件处置的及时性和工作效率。 1.支持事件处理意见的自定义； 2.支持确认事件处理意见，明确事件是否误报； 3.支持线上处置记录自动存储，保留操作痕迹； 4.支持线下处置记录人工存储，可上传事件现场相关处置图片、视频素材； 5.支持人工指派处理人，可多次选择不同人员进行事件处理 | 套 | 1 |  |
| 25 | 工作台 | 平台通知公告发布 | 通知公告（发布文件和通知，文件通知下发和用户未阅读提醒），提供对首页通知公告的管理，创建、修改、删除、实时发布、特定时间发布、下架、查询功能。并提供开放能力,即提供API接口供外部调用及小部件，来提供模块的扩展性与易于集成特性 | 套 | 1 |  |
| 26 | 平台门户自定义 | 1.提供超级管理员、安保管理员、后勤管理员、行政管理员、运维管理员五类用户角色门户工作台； 2.提供工作台自定义能力，用户可以自由配置业务展示内容，制定专属的工作台显示内容； 3.提供应用菜单导航、应用快捷入口等能力。 | 套 | 1 |  |
| 27 | 安防综合检索 | 1.系统按照关键字搜索和多条件组合查询任务列表，浏览任务信息，包括任务名称、锁定状态、运行状态、增量激活状态、策略激活时间、节点数、所属分组、创建人和创建时间等信息。 2.系统根据字段值等条件进行数据过滤，可按多个条件组合过滤。 3.系统定义告警策略，包括任务运行异常 、增量异常、数据断流、数据加载异常、插件运行异常、运行环境（CPU、内存、磁盘、网络IO）异常等，同时设置推送到消息中心和设置告警等级。 4.支持查看登录、查询、新增、更新、删除、退出、授权等类型的操作日志；支持按用户名、操作类型、操作状态、开始时间、结束时间进行日志筛选。 | 套 | 1 |  |
| 28 | 移动APP | 移动APP | 提供移动APP端应用，包含应用搜索、消息、待办及各类业务应用。 1.支持管理员和员工登录APP，根据管理员的角色权限展示对应的管理应用； 2.支持事件、消息、代办内容的提醒和查看功能，使管理人员能够实时知晓和处理业务事件； 3.提供安防管理应用，包括：视频预览、录像回放、图片查询、巡更、图上监控、报警监测管理应用； 4.提供通行管理应用，包括访客、门禁控制、车辆管理应用； 5.提供人员进出、访客到访数据统计，提供设备在离线、告警信息的数据统计。 | 套 | 1 |  |
| 29 | 消息代办 | 面向管理员、员工提供APP消息、待办、事件推送提醒服务，并支持在APP锁屏时收到弹窗消息提醒。 1.提供消息页面，支持访客来访、访客签离消息提醒； 2.提供待办页面，支持事件处置、访客申请审批待办事项的提醒。 3.支持根据事件中心管理设置，事件发生时支持弹窗提醒。 | 套 | 1 |  |
| 30 | 高可用 | 双机热备 | 1.提供高可靠管理应用组件实现业务组件实现高可靠的部署，以扩展资源包的方式快速集成组件的高可靠部署方案，在系统故障发生时实现故障转移，保障系统可用性。 2. 提供统一的高可靠管理界面，支持实时查看高可靠集群状态。 | 套 | 1 |  |
| 31 | 中间件 | 配套中间件 | 国产化主流中间件，需与部署的服务器及系统高度适配。 | / | 1 |  |
| 32 | 接口开发 | API接口 | 需具备完善的对外API接口，包括但不限于视频、图像、报警信息、地理信息等数据 | / | 1 |  |
| 33 | 集成对接 | 设备对接、系统配置 | 提供不低于1500路摄像头、20路门禁、1路电子围栏等设备或系统的数据接入、系统配置等服务，具体集成对接数量以项目完工实施结束前1个月确定的设备及系统数量为准，总接入数量不超过2000路。 | / | 1 |  |

## 三、项目服务要求

### **（一）技术服务标准和要求**

**1.项目建设进度要求**

中标人必须在合同签订后30个日历日内在管网公司提供的服务器中完成智能安防系统主要功能模块部署、调试，并接入部分安防设备进行试运行。系统试运行期间完成全部建设内容并接入项目实施前期调研及实施方案编制阶段确认的符合接入条件的安防监控设备，稳定运行30个日历日后开展初步验收；初步验收通过后，系统进行正式运行期并稳定运行不少于6个月，期间接入管网公司全部但不超过2000路安防设备后（因设备老旧提供不了接口的，经管网公司同意后，可不接入），开展最终验收。

**2.软件建设要求**

（1）中标人必须向项目业主提供建设方案中列举的所有功能的全部内容，并完成软件的安装测试、在软件安装中负责及时解决全部技术问题。

（2）中标人应本着认真负责态度组织技术队伍，做好报价的整体方案并提出长期保修、维护、服务以及今后技术支持的措施计划，承诺并协助项目业主推动智能安防系统培训使用，并根据公司企业文化进行个性化UI设计。

（3）系统建设工作开始后，中标人应允许项目业主的工作人员参与系统的安装、测试、诊断及解决问题等各项工作，并协助企业完成基础安防硬件的选型和数据对接。

（4）中标人应负责在项目初验前完成使用手册的编写和交付，并在项目终验时将系统的全部有关技术文件、资料及测试、验收报告、使用手册等全套文档汇编成册交付项目业主。

（5）中标人应对投标文件中所列“管网公司智能安防系统”全部功能验收合格后方视为该项目全部完成。

**3.人员投入要求**

中标人应投入人员：1名项目负责人、1名技术负责人及数量充足的技术人员，保证技术工作有序、顺利完成。

### **（二）系统性能要求**

智能安防系统软件基于成熟的技术架构，具备良好的健壮性、扩展性和稳定性，保障系统具备海量接入和并发访问的能力。

1.支持不少于500个用户使用并发量，在服务器及网络等配套硬件满足条件下，一般功能页面数据查询操作响应时间不得大于3秒钟，综合数据统计报表查询呈现时间不得大于15秒钟，仪表盘（图表）呈现时间不得大于15秒钟。

2.系统可靠性达到99.99%（即年度系统不可用时间不得超过50分钟），以系统终验合格之日起第一年为评估期间。

3.系统失效后可自动启动后台服务，人工恢复相关服务或软件时间不得大于30分钟。

4.需在项目业主提供的服务器中进行高可用配置，实现定期备份数据，保证数据的高可用，并做到了异地容灾。

### **（三）技术支持与售后服务要求**

1.本项目要求所有软件系统质保期为3年，自双方代表在终验验收单上签字之日起计算。中标人在质保期内必须向项目业主承诺技术后援支持，为用户的系统维护提供免费技术支持，包括但不限于系统BUG修复、系统功能优化。

2.系统质保期内，系统根据行业发展情况享受对应系统功能免费升级服务及配套培训。

3.系统质保期内，非产品技术问题需在4小时内回复，产品技术问题需在8小时内回复。

4.中标人必须提供完整的用户手册及视频教学，同时应为项目业主相关人员提供免费的培训服务。其中线下提供至少2次全面的系统培训和至少6次小规模培训，保障项目业主的人员能熟练使用、维护本项目建设系统。

## 四、费用支付

项目合同签订后，项目建设服务费分预付款、初验款、终验款、质保金四个阶段进行支付。

1.预付款：签订合同后，中标人向项目业主提供等额有效的增值税专用发票、请款报告等请款资料，经项目业主确认无误后20个工作日内，项目业主向中标人支付合同价的30%作为项目预付款；

2.初验款：项目完成全部建设内容进行试运行不少于30日并经初步验收合格后，中标人向项目业主提供等额有效的增值税专用发票、请款报告等请款资料，经项目业主确认无误后20个工作日内，项目业主向中标人支付合同价的30%作为项目初验款；

3.终验款：项目初验通过并整改完成后稳定运行不少于6个月，开展最终验收并合格后，中标人向项目业主提供等额有效的增值税专用发票、请款报告等请款资料，经项目业主确认无误后20个工作日内，项目业主向中标人支付至最终结算价的90%作为项目终验款；

4.质保金：质保期结束并通过项目业主确认后30日内，中标人向项目业主提交支付申请及符合项目业主要求的增值税专用发票等请款材料，经项目业主审核无误后20个工作日内，项目业主向中标人支付剩余款项即对应最终结算价总额的10%作为项目质保金。

若因中标人或客观因素导致中标人未能完全按用户需求建设且项目业主和中标人无法商榷出合理的解决方案，经项目业主同意，中标人在承担其违约责任的基础上（客观因素导致不能完全按用户需求建设除外），项目业主可按实际验收合格的系统建设模块（或功能）报价所占总报价的比例予以按实结算及支付，最终支付实际金额为实际验收通过的功能点报价费用，若已支付金额超出最终需支付金额的，在结算完成后，由中标人在7个工作日内退回至项目业主账户。

## 五、其他要求

1.中标人对软件产品保证不侵犯任何第三方的知识产权，如发生上述问题，由此产生的一切法律后果和经济赔偿，均由中标人单独承担，由于软件产品的知识产权问题导致项目业主有任何影响，项目业主有权终止合同，并赔偿该分项价格50%给项目业主。

2.项目业主使用软件形成的数据，中标人不能以任何方式取得及保留；合同期间及提供其它服务期间所知悉相关信息，包括但不限于系统数据、经营信息、文件资料等，中标人应严格予以保密，未经项目业主同意中标人不得以任何方式向任何第三方泄露。签订合同时中标人需与项目业主签订保密协议。

## 附件1：

**管网公司智能安防系统建设方案**

**第一章 项目现状及必要性分析**

**1.1 项目建设现状**

**1.1.1 项目建设背景**

目前集团公司及各直属企业安全防范系统建设现状相对落后，智能化程度较低，仅满足基本安防监控需求。存在问题主要包括：一是集团公司及各直属企业安防系统建设缺乏总体规划，缺少有效协同和响应机制，信息传递共享滞后，无法支撑快速、准确地应对各类安全事件，难以满足集团安防保障要求；二是设备相对落后，对人工依赖程度较高，影响工作效率；三是现有安防系统功能单一，缺少风险态势分析、智能预警、数据统计、视频分析、应急指挥调度等功能，技术安全防范能力有待提升；四是智能安防技术标准体系建设缺失，不同系统之间存在兼容性问题，缺少统一安防管理平台，无法满足系统集成及安全可靠等要求。

目前经过前期调研工作，已基本调研清楚管网公司的安防系统现状，计划统一建设一套兼容目前安防现状、改善现有安防问题、满足未来业务需求、稳定开放的管网公司智能安防系统。

**1.1.2 信息化建设现状**

经过调研，管网公司及各分公司目前安防系统现状如下：

管网公司目前已在使用有视频监控、门禁、停车出入等系统，且各个系统相对独立，基本未进行关联与集成，其中以视频监控系统为典型，管网公司当前确定在用的视频监控系统有9个，其中多数是使用的摄像头厂商自带的免费版云平台。

管网公司目前已在使用及本年度有规划的视频监控摄像头、通道闸机、门禁设备、电子围栏等设备约2010路（已安装1355路，计划新增655路），其中视频监控摄像头约1866路、车辆道闸约12路、门禁约107路、电子围栏约25套（详细清单见附件《管网公司安防监控设备清单收集表 (2405)》）。考虑远期需求，总安防监控设备数量将超过4000路。

**1.2 项目建设必要性分析**

目前管网公司内部各分公司及相关业务部门涉及的安防系统几乎均为分批多次独立采购硬件，使用配套免费软件平台，并由使用方各分公司各部门独立建设、独立管理，管网公司作为集团子公司需建设面向公司级安防监控、事件处置、指挥调度业务的安防管理应用中心，本次项目拟建设的为公司级和现场级平台。

通过智能安防系统的建设，管网公司各部门分公司对应业务场景的安防数据将被打通，通过对接分公司的现场级子系统，实现远程监测和现场级子系统的联动监控，满足公司安防指挥调度业务要求。

构建覆盖全公司的智能安防系统，实现统一接入和管理所有安防设备，具有显著的经济效益和社会效益。第一，本系统通过智能化的监控和预警功能，能够为公司缓解一线运维人员的工作压力，确保运营区域及办公区域的人员出入安全及有效监管；第二，本系统的实时监控功能可实现问题的快速发现和响应，缩短安防及生产运营紧急事件的处理时间，提高工作效率；第三，业务部门可根据实际需求布设相应的安防监控设备，将相应安防设备接入本系统后，公司可对工程施工现场、巡检现场等项目运营现场进行实时监控，实现对项目现场人员的有效监管，保障施工现场的安全；第四，在排水泵站的监管方面，将泵站相关安防监控设备接入本系统后，可与泵站集控系统进行联动，协同运转实现对泵站设施运行状态的实时监控、有效监管，为未来实现泵站远程集控、无人值守提供基础支撑；第五，将易涝点、积水点、隧道、溢流点、污泥处置点等重点关注区域的安防监控设备接入本系统后，可查看对应区域的实时监控画面，有助于及时发现和处理水污染、城市内涝等问题，从而减少居民投诉，提高主管部门及居民满意度，保护生态环境，保障居民出行安全。

此外，本系统建立后，公司可通过全局的数据可视化管理辅助业务决策；通过统一的数据管理、数据应用减少日常的重复管理工作，优化管理流程；通过AI分析能力发现以往的监管盲区，提高工作效率。

**第二章 需求分析**

**2.1 业务需求分析**

**2.1.1 安防设备统一管理需求**

目前管网公司本部及各分公司安防系统独自采购使用，难以统筹进行业务管理调度。本次拟建设的管网公司智能安防系统需解决安防数据统一汇聚的问题，接入管网公司各类安防数据，保证通过系统实现对整体安防情况全域可知、全时可用。

在未来实现整个管网公司安防设备的统一规划、统一接入、统一管理、统一维护，形成合理、开放的安防设备建设标准，各部室分公司依据标准采购安防安装使用设备，本部对应管理部门依据标准管理设备、提供应用。

**2.1.2 各级应用按需扩展需求**

管网公司各部室分公司根据自身业务开展情况，具备个性化的安防业务应用需求，办公区、泵站、施工现场、巡检现场、重点关注点（易涝点、积水点、隧道、溢流点）及通沟污泥处置现场等现场级安防系统可结合业务需求在满足标准的情况下部署个性化安防设备，如车载监控设备、移动便携监控设备、太阳能监控设备等，充分满足现场一线人员工作需要，公司级智能安防系统应具备丰富的应用扩展能力，在提供必要的公司级安防管理应用的同时，需支持重点现场业务的应用扩展和功能深化，实现更高效、灵活的现场级应用赋能和经验推广。

**2.1.3 智能安防赋能业务需求**

目前管网公司各部室分公司对安防系统的应用大多局限于视频监控人工查看，在调研过程中，各分公司也提出了针对安全劳保用品、溢流口、火点等智能分析检测需求，智能安防系统应提供成熟、可靠的视频智能分析能力和个性化的视频智能分析扩展能力，满足已有的智能分析需求、考虑未来可能新增的智能分析需求，降低管网公司日常工作的人工成本，提高管理效率。

**2.1.4 报警事件处理需求**

安防系统支持智能识别告警功能，能够自动识别部分异常事件并上报平台产生告警。因管网公司安防系统应用场景庞大、数量多，环境、技术等各类因素会影响安防告警的稳定性形成误报，安防系统需要具备报警处置流程，实现误报初筛、报警分级分类推送，避免管理调度人员被过多事件数据干扰，以提升工作效率。

**2.1.5 数据可视化需求**

系统需提供统一查看入口和可视化界面，以简洁直观地展示所关注的数据，查看所有安防区域的资源情况、设备状态、报警数据等，辅助进行监管及决策。

**2.2 功能需求分析**

**2.2.1** **联动监控需求**

支持与集团统一智能安防管理平台、各分公司的现场级智能安防子系统的联网，实现信息交换与共享，信息传输、交换、控制协议应符合国家现行相关标准的规定。

智能安防管理系统宜具备视频监控系统、出入口控制系统、入侵报警系统、访客管理系统等系统的软件功能。

系统建设期间应形成详细的下级系统、设备接入标准，用于指导下级系统、设备接入系统的方案设计、开发实施。支持在一个操作界面上对接入的视频监控系统、出入口控制系统、入侵报警系统、访客管理系统等所有系统和设备集中管理和控制。

**2.2.2** **设备管理需求**

需对智能安防子系统的设备在线状态进行监测，宜对系统内设备进行统一编址、寻址、注册和认证等管理。

需支持对系统和设备的运行状态进行实时监控，对设备生命周期进行管理，及时发现故障，保障系统和设备的正常运行。

系统建设阶段应同步形成设备接入标准，可满足主流品牌设备的接入条件。

**2.2.3** **人员管理功能**

应对公司内外部人员信息、出入口授权信息、内部安防人员巡查信息实现集中展示和查询，实现人员的黑白名单管理，对防区内人员的出入情况进行记录管理，对非法人员入侵情况进行预警管理。

**2.2.4** **车辆管理需求**

按需对接车辆出入口管理系统，采集车载监控、卫星导航等数据，实现车内外视频图像及车辆位置联合巡查、视频预案巡检等功能，可查看行驶轨迹、驾驶员状态是否正常，对异常轨迹、行为及时干预。

支持录像和行驶路线同步回溯，协助管理人员回溯安全事件发生时车辆内外部情况。

**2.2.5** **AI事件分析需求**

应基于视频、设备监测数据实现智能事件研判分析功能，如安全帽识别、违规行为识别、施工围挡识别、火点识别等。

支持利用已建视频监控设备，通过后端 AI 算法分析实现智能事件检测。

支持对接前端智能化设备，获取智能化设备的智能分析结果，智能化设备需开放相应接口。

**2.2.6** **指挥调度需求**

系统支持各类安防数据、安防事件的统一管理，通过对人员、设备、行为等各类信息的综合掌控，实现对资源的统一调配和应急事件的快速处置。

支持预案管理，事件发生时可根据编制的预案快速联动。

**2.2.7** **移动端应用需求**

支持移动端进行设备管理、人员管理、车辆管理、接收事件推送、报警信息处理、实时视频查看，支持Harmony、Android等主流移动终端。

**2.2.8** **系统对接方式**

现场级安防系统应提供主流的软件数据接口，可供智能安防系统获取数据。应支持实时流、离线型数据对接方式。设备应通过主流的设备对接协议接入现场子系统。现场子系统应向上提供主流的软件数据接口，通过软件数据接口供智能安防系统获取数据。

**2.2.9** **集约化建设、运维**

现场智能安防子系统宜与管网公司智能安防系统统筹建设，便于集约化建设、运维。

**2.3 性能需求分析**

**2.3.1** **数据接入性能需求**

根据对全公司各部室分公司的调研现状数据结合长远需求，管网公司预计要接入的安防监控设备数据量主要如下：

（1）视频监控摄像头至2024年底约1866路，考虑远期暂定3200路接口；

（2）车辆道闸至2024年底约12路，考虑远期暂定50路接口；

（3）ID/IC、人脸、指纹等类型门禁至年底约107路，考虑远期暂定300路接口；

（4）电子围栏至2024年底约25套，考虑远期暂定100路接口。

此外，所有类型设备接入路数均需支持未来进一步增加数量拓展及类型升级，数量拓展及升级单价费用不得高于本次项目报价单价。

**2.3.2** **数据存储性能需求**

安防系统数据存储，如下表所示：

**表2-1 系统信息存储时间要求表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **系统名称** | **视频监控系统** | **出入口控制系统** | **入侵报警系统** | **访客管理系统** |
| 信息存储时间 | 1）普通场景录像≥30d  2）反恐等特殊场景录像≥90d  3）实验室录像＞365d  4）周界入侵事件（含图片）≥180d | 1）区域出入场所≥3d  2）关键生产区域及核心办公室的记录宜≥30d  3）危化品储存场所≥180d | 系统布防、撤防、报警、故障等信息≥180d | ≥30d |

目前已建的安防系统，数据存储满足要求的可继续使用，不满足要求的需及时按要求整改。

**2.3.3** **网络带宽需求**

**2.3.3.1 带宽计算方式**

根据需求，视频监控设备分辨率不小于400万像素，故按照4Mbps/路的码流计算网络带宽要求，常态化轮巡时可降低码流按照2Mbps/路的码流计算网络带宽要求。

由于公司级平台不对前端视频直接做实时存储，视频取流主要用来进行视频预览和智能分析，公司到各视频监控点之间的带宽理论值计算为：

W码流带宽=W预览带宽+W解析带宽=4M+4N

其中，4指视频码流为4Mbps，M为全管网公司同一时间预览的前端点位数量，包括解码上墙的视频路数和客户端预览的视频路数，N为同一时间利用服务器资源进行智能分析的视频点位数量。

考虑码流突发及信道开销，有效带宽一般占设备规格的50%，另外再预留20%的带宽给信令、图片等其他信息。综上，建议的经验带宽为：

W经验带宽=W码流带宽/（1-20%）/50%=2.5W码流带宽

**2.3.3.2 网络带宽建议**

结合管网公司内部实际业务开展情况预估，管网公司对于视频实时预览的并发量约为200路（本部及各分公司），总并发预计不超过200路4Mbps码流视频。安防系统计划部署在管网公司本部机房，远期部署至集团数据中心。根据调研所需接入的安防系统情况，具体带宽要求如下：

**1.地面泵站/分公司办公点带宽要求**

以每个泵站/分公司最大情况下有5个监控点被同时调用预览或10个摄像头轮巡预览预估，每个泵站/分公司和本部机房之间的带宽应满足上行4M\*5/（1-20%）/50%=50Mbps。

按每个分公司的监控电视墙按同时轮巡预览16路2Mbps码流视频、同时预览2路4Mbps码流视频预估，每个分公司和本部机房之间的带宽应满足下行2M\*16/（1-20%）/50%+4M\*2/（1-20%）/50%=100Mbps。

**2.管网本部带宽要求及无线网络要求**

由于各分公司的视频预览通过总部流媒体取流，总部需为每个分公司的视频预览需求预留对应的100Mbps上行带宽。

此外，和其他移动式视频监控点的网络：计划采用4G/5G无线网络。

考虑手机通过APP查看视频的需求，建议管网公司本部预留总计200Mbps上行带宽。

综合以上情况，每个地面泵站预计不低于50Mbps上行带宽网络线路需求，管网公司本部预计不低于800Mbps上行带宽网络线路需求。

**2.3.4 系统软硬件安全可靠需求**

管网公司智能安防系统需满足安全可靠需求，系统软件需支持安全可靠部署环境，部署软件的硬件服务器和PC需采用安全可靠CPU，CPU型号需在中国信息安全测评中心的《安全可靠测评结果公告》公示范围内。

系统配套的数据库、操作系统需满足安全可靠要求，需在中国信息安全测评中心的《安全可靠测评结果公告》公示范围内。

系统配套的中间件需采用国产自主研发产品。

**2.3.5 数据迁移需求**

管网公司智能安防系统需实现目前已建和后续规划的现场级安防系统的数据汇聚、设备管理、应用赋能，实现各分公司、各部门已建安防系统的数据对接，不改变已建安防系统软硬件架构，暂无数据迁移。

**2.4 用户分析**

结合实际调研情况并考虑管网公司后续安防系统使用方向，管网公司智能安防系统将使用者分为系统管理用户及系统服务用户，其中系统管理用户主要为信息化线业务同事及设备线业务同事，系统服务用户主要为运营、设备、工程、安监、办公后勤等业务线同事，预计总用户数不超过500人。

**2.4.1** **系统管理用户分析**

系统管理用户作为系统管理员，主要职责是负责系统的管理和维护，基于管网公司组织架构和安防系统设备量较庞大的现状，暂计划系统管理员主要分为本部及分公司信息化人员、设备管理人员及调度中心人员，分别对应部门为管网公司本部信息管理部、设备管理部、运营管理部以及分公司运营工作部、设备工作部，具体用户分配如下：

**表2-2 系统管理用户角色分配表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 部门 | 角色 | 职责 | 人数 | 备注 |
| 信息管理部 | 管理员 | 系统总管理员，系统总体运维 | 1 |  |
| 信息管理部 | 子管理员 | 本部安防系统运维管理、权限设置、用户开户等 | 1 |  |
| 运营管理部  (调度中心) | 子管理员 | 调度中心安防系统调度中心大屏管理、调度处置等 | 1 |  |
| 设备管理部 | 子管理员 | 设备线安防系统硬件对接监管、权限管理等 | 1 |  |
| 分公司  运营工作部 | 子管理员 | 分公司安防系统运维管理、权限设置、用户开户等，并协助分公司进行硬件对接 | 6 | IT专员 |
| 分公司  设备工作部 | 子管理员 | 设备线安防系统硬件建设、设备管理、系统对接及分公司监控大屏管理等 | 6 |  |

**2.4.2** **系统服务用户分析**

系统服务用户作为系统日常使用的普通用户，主要职责是各业务线同事。根据调研情况，系统普通用户主要分为本部及分公司运营线、设备线、工程线、安监线、办公后勤线等业务线同事，其主要需求为预览、查看、调用保存其业务职责范围内场景安防视频图像等安防数据，具体用户分配如下：

**表2-3 系统服务用户角色分配表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 部门 | 角色 | 主要使用模块 | 人数 | 备注 |
| 办公室 | 普通用户 | 视频监控、出入口控制、入侵报警、访客管理等 | 2 |  |
| 运营管理部 | 普通用户 | 视频监控 | 2 |  |
| 工程管理部 | 普通用户 | 视频监控等 | 2 |  |
| 设备管理部 | 普通用户 | 视频监控、出入口控制、入侵报警、访客管理等 | 2 |  |
| 安全监管部 | 普通用户 | 视频监控等 | 2 |  |
| 分公司  综合部 | 普通用户 | 视频监控、出入口控制、入侵报警、访客管理等 | 按需分配 |  |
| 分公司  运营工作部 | 普通用户 | 视频监控等 | 按需分配 |  |
| 分公司  工程工作部 | 普通用户 | 视频监控等 | 按需分配 |  |
| 分公司  设备工作部 | 普通用户 | 视频监控、出入口控制、入侵报警、访客管理等 | 按需分配 |  |
| 分公司  安全监管部 | 普通用户 | 视频监控等 | 按需分配 |  |

**2.5 信息安全保障需求**

本项目信息安全设置遵循公安部颁布的信息安全技术规范进行，系统工程的风险等级和防护等级均为二级。

项目运营过程中可能存在重要数据业务数据泄露、重要数据被破坏等网络层风险；采用的操作系统可能存在的安全漏洞和病毒威胁风险；应用系统中用户提交的业务信息被监听或修改、外网非法用户对内部网和服务器的攻击等风险。为了保障信息安全可采用网络边界防火墙等成熟产品和技术实现网络边界安全，防范非法用户入侵；采用入侵安全检测系统，提供实时的入侵检测及采用相应的防护手段。

**2.6 关联系统和接口需求**

**2.6.1** **现场级安防系统接口需求**

结合实际调研情况和管网公司后续安防业务规划，现场级安防系统需具备如下开放接口：

**1.视频监控系统**

所有视频监控设备需支持国标GB/T 28181协议，满足音视频传输需求。

智能分析类设备（如前端智能摄像机、智能NVR等）需开放事件数据、图片数据相关接口，接口内的字段需可支撑形成完整的业务闭环逻辑。

移动便携类设备和车载监控设备需开放卫星导航定位相关接口。

太阳能供电设备需提供电量显示数据接口。

热成像类设备需提供温度数据接口和告警事件接口。

**2.出入口控制系统**

门禁类设备需开放通行事件数据、异常事件数据、图片数据、权限下发接口，满足智能安防系统对门禁系统的事件获取和人员权限下发需求，智能安防系统不对门禁系统做直接控制，门禁控制由门禁子系统自行实现。

车辆道闸类设备需开放通行事件数据、异常事件数据、图片数据、权限下发接口，满足智能安防系统对过车事件获取和车辆权限下发需求，智能安防系统不对车辆道闸系统做直接控制，车辆道闸控制由车辆道闸子系统自行实现。

出入口控制系统相关的门禁类、车辆道闸类等设备的接口需提供对应标准要求，以便于后续根据该标准采购符合接入要求的设备。

**3.入侵报警系统**

入侵报警类设备需开放事件数据接口，以便智能安放平台及时获取入侵告警信息。

**4.访客系统**

访客系统可由智能安防系统统一提供，各分公司的门禁设备需开放人员权限下发接口，以便智能安防系统完成访客预约后及时下发人员通行权限。

**2.6.2** **系统边界说明**

**表2-4 系统边界说明**

|  |  |  |
| --- | --- | --- |
| **边界划分** | **管网智能安防管理系统** | **现场级智能安防管理子系统** |
| 远程监测控制 | 对接下属机构的现场级子系统，应实现远程监测，根据控制权限宜实现远程控制，满足公司安防指挥调度业务要求。 | 对接生产区、办公区、施工工地的现场设备，应实现远程监测、控制，满足现场安防指挥调度业务要求。 |
| 智能安防应用 | 实现对接入的现场级子系统进行联动监控，以及设备、人员、车辆的安防业务管理。 | 各智能安防子系统实现各专业应用功能。 |
| 系统对接方式 | 下级系统应提供主流的软件数据接口，可供公司级平台获取数据。应支持实时流、离线型数据对接方式。 | 设备应通过主流的设备对接协议接入现场子系统。现场子系统应向上提供主流的软件数据接口，可供上级平台获取数据。 |
| 集约化建设、运维 | 本部信息部牵头建设、运维。 | 现场安防子系统安防设备部分由所属分公司牵头建设，软件部分接入管网智能安防管理系统统筹建设，便于集约化建设、运维。 |

**2.6.3** **与其他业务系统的接口交互需求**

管网公司的安防业务应用数据通过管网智能安防系统汇聚、管理，管网智能安防系统需具备完善的对外接口，包括但不限于视频、图像、报警信息、地理信息数据等，各类事件数据和必要的业务数据支持通过对外接口推送至水务集团安防平台、管网公司泵站SCADA集控平台、雨污同治升级项目平台、基础数据管理平台等系统平台。

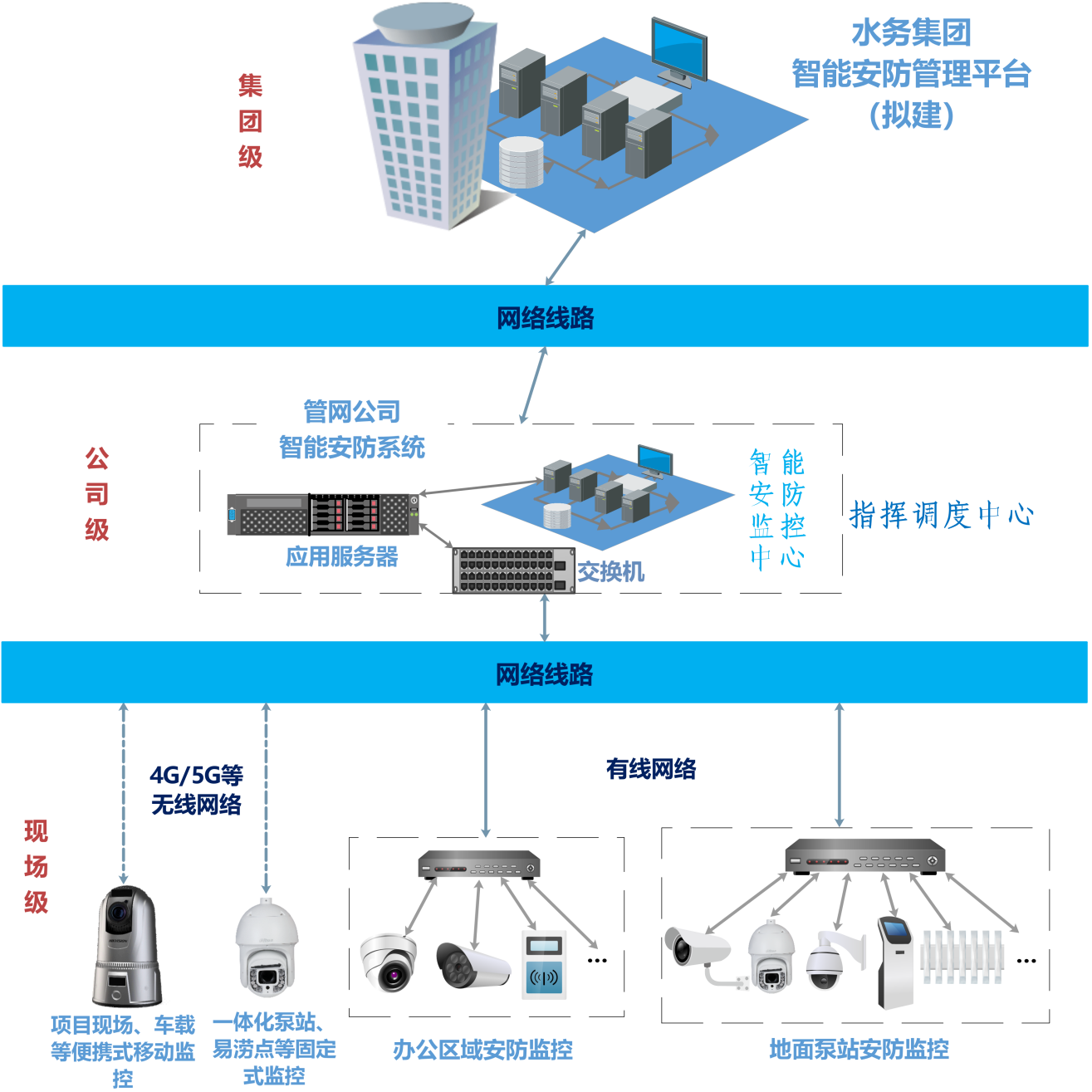
**第三章** **项目建设方案**

**3.1 建设目标**

通过本项目建设，建设公司级、现场级多级联动、联网共享、分级指挥的智能安防软件系统，实现管网公司办公区域、生产运营区域、工程施工区域安防监控数据的统一汇聚，实现对外部入侵、人员访问、车辆进出、区域监控、行为监控的及时预警、数据共享、联动指挥，达到防入侵、防破坏、防事故的成效，提高公司整体智能安防水平，并进一步提高对项目现场的远程管理水平，提高管网公司各管理部门及分公司管理人员对项目生产运营现场监管力度及效率。

**3.2 系统结构**

本次项目拟建设内容为管网公司智能安防系统，计划通过统一汇聚的智能安防系统从软件系统层面统筹公司级安防系统及现场级安防系统。现场各类安防设备通过有线网络及4G/5G无线网络连接方式提供网络通信数据，传输至智能安防系统专用服务器，实现各子系统的关联畅通，总体架构如下：



**图3-1 管网公司智能安防系统总体架构**

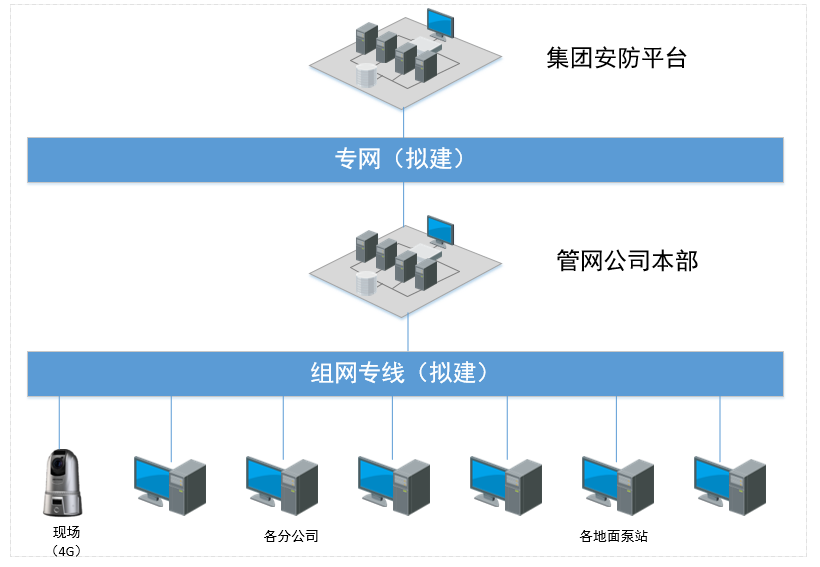
**3.2.1** **系统技术架构**

系统采用分布式组件化部署，包含结构化的业务数据、资源数据、录像数据、图片数据及缓存数据，各类数据按类别分类存储、管理，方便后续升级、迁移、扩容及维护，如下图所示。

****

**图3-2 管网公司智能安防系统技术架构**

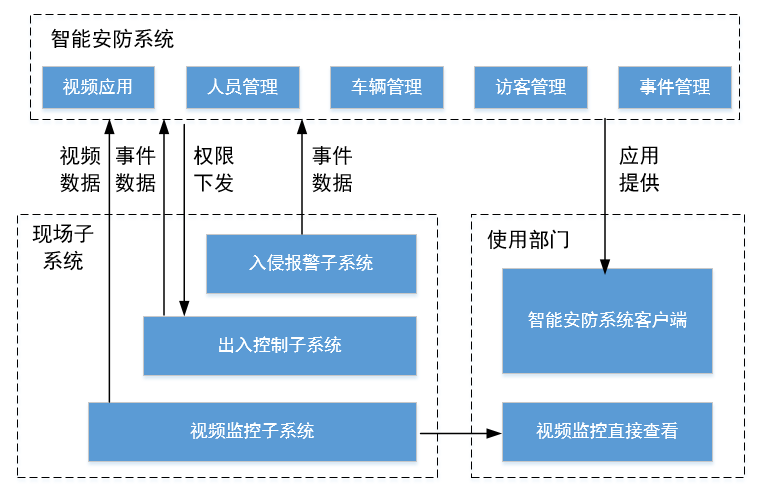
**3.2.2** **系统网络架构**



**图3-3 管网公司智能安防系统网路架构**

**3.2.3** **系统应用架构**

智能安防系统建设完成后，各分公司建设的现场级安防子系统为智能安防系统提供数据，通过智能安防系统客户端统一提供安防应用，应用架构如下图。



**图3-4 管网公司智能安防系统应用架构**

考虑到管网本部的网络带宽和流媒体压力，各分公司查看自建的现场级视频时，也可采用直连视频监控设备的方式查看实时视频、录像。

**3.2.4** **现有系统整合方案**

1.视频监控系统

现有视频监控设备基本支持国标GB/T 28181协议，通过国标协议接入智能安防系统，确实不支持国标的监控设备需考虑整改。

部分专用监控设备（如智能监控、车载监控、移动监控等）支持国标协议但暂未获取非标数据开放接口的，先通过国标协议完成视频数据上传。

2.出入控制系统

各分公司自建的门禁设备需支持开放通行事件数据、异常事件数据、图片数据、权限下发接口，智能安防系统通过接口对接设备通行数据及统一下发权限，门禁设备的人员权限认证由现场门禁系统实现，无法开放接口的设备需进行整改。

各分公司自建的车辆道闸设备需支持开放通行事件数据、异常事件数据、图片数据、权限下发接口，智能安防系统通过接口对接设备通行数据及统一下发权限，现场的车辆权限认证由现场车辆道闸系统实现，无法开放接口的设备需进行整改。

3.入侵报警系统

各分公司自建的入侵报警系统需开放事件数据接口，智能安防系统通过接口对接告警事件信息，无法开放接口的设备需进行整改。

4.访客系统

各分公司均未建设访客系统，访客系统作为新建规划，各分公司的门禁设备需满足权限下发要求。

**3.3 建设内容**

**3.3.1** **应用系统建设**

管网公司智能安防系统是利用软件系统对安全防范的视频监控系统、出入口控制系统、入侵报警系统、访客管理系统等安防子系统及相关信息系统进行集成，实现全公司范围内的实体防护系统、电子防护系统和人力防范资源的有机联动、信息的集中处理与共享应用、风险事件的综合研判、安防报警事件处置、系统和设备的统一管理与运行维护等功能的软件系统。

**3.3.1.1 系统功能建设**

系统具体功能模块如下表：

**表3-1 应用系统功能模块说明表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **子系统或模块** | **功能说明** | **性能说明** | **应用部门和业务** | **备注** |
| 1 | 联动监控模块 | 提供视频实时预览、录像回放、视频上墙、门禁信息查看、车辆信息查看、报警信息查看、访客信息查看功能，提供安防数据标准接入体系 | 满足不少于3200路视频监控、50路车辆道闸、300路门禁、100路电子围栏设备的接入管理 | 各分公司、各部门日常工作使用 |  |
| 2 | 设备管理模块 | 应对智能安防子系统的设备在线状态进行监测，宜对系统内设备进行统一编址、寻址、注册和认证等管理。  宜支持对系统和设备的运行状态进行实时监控，对设备生命周期进行管理，及时发现故障，保障系统和设备的正常运行。 | 满足不少于3200路视频监控、50路车辆道闸、300路门禁、100路电子围栏设备的接入管理 | 运维管理人员使用 |  |
| 3 | 人员管理模块 | 智能安防系统实现公司内部人员名单管理、访客预约管理，应能管理接入的门禁设备实现内部人员和访客的出入口授权，能够复查所有门禁点位的全部通行记录，应能支持黑白名单管理和陌生人管理，对非法人员入侵情况进行预警管理。 | 满足不少于2000人的人员管理能力 | 运维管理人员使用，访客审批人员使用 |  |
| 4 | 车辆管理模块 | 智能安防系统实现公司内部车辆名单管理、访客车辆预约管理，应能管理接入的车辆道闸设备实现内部车辆和访客车辆的出入口授权，能够复查所有过车记录。  针对安装了车载监控的车辆，支持车辆实时定位、行驶轨迹追踪与回放以及车外360°全景影像的调阅与录像回溯等功能。 | 满足不少于50处车辆道闸的车辆管理能力 | 运维管理人员使用，访客审批人员使用 |  |
| 5 | AI事件分析模块 | 结合需求调研结果，本次建设需满足如下智能分析能力：  1.人脸比对  2.陌生人识别  3.安全帽检测  4.反光衣检测  5.施工围挡检测  6.溢流点检测  7.水体颜色检测 | 支持智能分析路数扩展、智能分析算法扩展，暂定50路 | 各分公司、各部门日常工作使用 |  |
| 6 | 安防报警事件处置模块 | 支持各类事件接收、事件预案、事件处置，支持根据不同事件情况结合预案通知相关人员处理，提供事件闭环流程，事件处置记录可查。 | 支持不少于100条/秒的事件接受能力 | 各分公司、各部门日常工作使用 |  |
| 7 | 移动端 | 提供移动端的视频查看、事件处理能力，支持Harmony、安卓等主流移动操作系统。 | 支持不少于50路的移动端并发 | 各分公司、各部门日常工作使用 |  |

**3.3.1.2 系统需对接接入设备**

本期管网公司智能安防系统项目建设主要接入项目实施结束前管网公司已建的安防设备，其中预计摄像头不低于1500路、门禁不低于20路门、电子围栏不低于1套，具体集成对接数量以项目完工实施结束前1个月确定的设备及系统数量为准，总接入数量不超过2000路。现有设备具体数量如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **部门/分公司** | **现有安防设备** | **本期需接入系统**  **安防设备** | **需改造后才能接入系统安防设备** |
| 第一分公司 | 第一分公司现有摄像头232路，门禁2套 | 本期第一分公司需接入摄像头232路，门禁2套（各1路门禁） | / |
| 第二分公司 | 第二分公司现有摄像头309路，门禁1套 | 本期第二分公司需接入摄像头309路 | 第二分公司现有1套门禁为未知品牌，提供不了对接接口，后期根据需要改造接入，不纳入本期接入范围 |
| 第三分公司 | 第三分公司现有摄像头225路 | 本期第三分公司需接入摄像头225路 | / |
| 第四分公司 | 第四分公司现有摄像头397路，门禁5套 | 本期第四分公司需接入摄像头397路，门禁1套（5路门禁） | / |
| 第五分公司 | 第五分公司现有摄像头137路 | 本期第五分公司需接入摄像头137路 | / |
| 第六分公司 | 第六分公司现有摄像头45路，门禁1套，电子围栏1套 | 本期第六分公司需接入摄像头45路，门禁1套（6路门禁），电子围栏1套 | / |
| 安全监管部 | / | 安全监管部正在走采购流程采购70个摄像头，本期接入该项目摄像头70路 | / |

**3.3.2 现场级安防子系统建设**

**3.3.2.1 视频监控系统**

视频监控系统设计应根据视频图像采集、目标识别的需要和现场环境条件等因素，选择相应的设备。具备对监控区域和目标进行视频采集、传输、处理、控制、显示、存储与回放等功能，在此基础上可扩展AI视频分析功能，实现对人、车、事件等要素的自动识别、预警功能。

主要用于接入管网公司办公区域、办公及生产运营车辆、施工现场（含维修、清疏、导排等）、巡检现场（含巡查、检测、测量等）、泵站、隧道、易涝点、积水点、溢流点以及通沟污泥处置（含暂置场所、转运和处置场所全链条）等区域视频设备，实现远程视频接入、数据展现与管理。

结合前期调研情况，系统提供接口应满足如下种类监控设备接入：

1.满足要求的枪机、半球、球机等设备；

2.专用车载设备，部署在车辆上，支持云台功能，能够控制覆盖作业现场；

3.移动便携设备：便携球、安全帽相机等，外场作业时使用；

4.太阳能供电设备：部署在河道、溢流口等取网取点困难点位，建议采用长续航产品；

5.热成像设备：部署在仓库、泵站等有火灾风险的点位，具备实时测温功能。

具体实现功能如下：

①视频查看

支持基于虚拟视频组的自动轮巡功能，支持按组轮巡和按窗口轮巡两种模式，可自由设定触发序列和时间间隔，视频组图像可在单个画面内和多个画面轮巡显示，支持实时监控、实时截图、实时录制功能。

实现对智能摄像头采集的事件信息进行集中展示、查询，事件可分级分类并触发报警，支持通过事件播放关联相关视频的录像，实现任意采集通道的图像信息切换给任意监视终端。

支持画面进行放大、缩小、全屏显示操作，支持可最多同时查看不低于16路图像信息，支持摄像机显示列表、列表排序、快速搜索功能，对监控区域内的人员及机动车的出入、活动情况进行24h实时监控并录像。

②视频控制

实现对各分控点监控设备进行远程控制。能实现对摄像机、镜头、云台等部件的自动或远程手动控制功能，自动控制支持光检测信号触发、事件触发、周期触发等触发机制，远程手动控制支持电源开启关闭、镜头运动、镜头变焦、防护罩/雨刷/风扇的开启、关闭，视频的录像、放像、停止。

③视频转发

支持视频分发功能，节点互联、监控客户端、电视墙服务、视频存储服务的视频传输通过流媒体技术进行码流复制转发，支持基于流媒体转发的存储管理功能，中心可对监控点任意一路视频图像进行备档存储。

④录像管理

提供录像检索、录像回放、回放控制功能，支持多路视频录像回放及下载，可按日期、时间、类型、服务器、通道检索客户端本地、存储服务器、前端设备的录像文件。

支持同时查看多路同一时间的录像回放，拖动时间轴时多路录像能同时定位到任意时间的录像；支持录像普通下载，框选下载功能。

⑤视频编辑

支持视频帧标记功能，可为每帧图像增加标记，以帧标记作为索引条件进行录像文件的快速检索。实现对视频图像进行解码、转发、图像嵌入与文字叠加等处理，以及图像地址、时间等符号在画面上叠加。

⑥有限空间、密闭空间预警与监测

涉及有限空间、密闭空间作业管理情况下，应能支持对有限空间、密闭空间的作业情况、异常预警情况、实时视频的查看，预警信息应及时推送相关安全管理人员，实现远程作业预警、监管功能。

⑦设备管理

支持对设备设置控制级别和权限管理。

提供灵活的配置管理功能，可在线对全网的视频设备进行配置管理和维护管理，支持对设备设置控制级别和权限管理。

支持在电子地图实时显示视频系统设备正常、异常、报警工作状态。

支持异构设备（硬盘录像机、视频服务器、网络摄像机、网络硬盘录像机等）、异构视频监控平台、报警主机、语音主机模块，以实现与各类异构资源的接入管理。

支持设备管理、业务管理、网络管理、运维统计等功能，设备管理包括服务器、数字视频设备、数字矩阵等，业务管理包括数据状态、视频状态、CPU占用、内存占用、网卡连接状态，网络管理包括网口实时流量、磁盘状态、RAID状态等，运维统计包括统计摄像机、监视器、设备连接的信息。

客户端、录像服务器、存储转发服务器提供日志管理功能，同时日志信息应自动上传中心视频监控管理服务器，中心视频监控管理服务器对日志进行统一管理，可通过用户或时间进行分类搜索。

有防干扰、防拆、防破坏、防雷、视频信号丢失报警等功能。

⑧与其他系统联动

视频监控图像应与出入口控制系统、入侵报警系统等实现联动，报警信息与图像联动响应时间≤4s。

此外，视频监控子系统利用视频数据进行智能分析，实现智能巡检管理功能，提供模型管理、模型下发、智能分析配置、抓图计划配置。通过将AI模型下发至设备，为设备通道配置智能分析任务，使设备拥有针对特定对象和场景的智能分析能力，能够解决碎片化场景下的智能分析问题并支持其他算法拓展及提供算法训练功能，同时支持智能巡检计划管理与管理及报警事件的处置等功能。

**3.3.2.2 出入口控制子系统**

出入口控制应用系统应具备处理、通信、配置、出入口控制、监测、告警等功能，可远程监控各控制器工作状态，支持对泵站等区域重要部位的通行门以及主要的通道口进行出入权限控制，支持统一授权用户下发、黑白名单用户下发，可对不同角色分类、授权。人员出入需支持人脸、ID/IC卡识别，宜同时支持指纹识别。

出入口控制系统的管理控制功能应符合以下要求：

接收识读部分传来的操作和钥匙信息，与预先存储、设定的信息进行比较、判断，对目标的出入行为进行鉴别和校核；对符合出入授权的目标，向执行部分发出予以放行的指令。

远程设定识别方式、出入口控制方式，输出控制信号，处理报警情况，发出报警信号。

出入口控制系统应与视频监控系统实现联动，报警信息与图像联动响应时间≤4s。

联网控制型系统中编程/控制/数据采集信号的传输可采用有线或无线传输方式，且应具有自检、巡检功能，应对传输路径的故障进行监控。

应具有事件记录功能：将出入事件、操作事件、报警事件等记录存储于系统的相关载体中，并能形成报表以备查看。

**3.3.2.3 入侵报警系统**

入侵报警系统需具备远程对入侵报警、故障、被破坏进行记录，并对前端硬件进行控制等功能。

入侵报警系统需与视频监控系统联动，泵站等重点区域的入侵报警信号与联动视频图像应发送到智能安防管理系统。报警传输系统应具有自检、巡检功能。

报警发生时，能够在电子地图上显示、局部放大报警部位，并以声、光信号显示报警的具体位置。

系统需具备实时记录系统开机、关机、操作、报警、故障等信息，并具有查询、打印、防篡改功能。

**3.3.2.4 访客管理系统**

支持访客身份证、人脸、车辆等信息录入与来访审批，可识别身份证的身份信息，人脸信息与身份信息可自动比对，确认人员身份。

应能登记和管理外来人员的基本信息、访问联系人、访问地址、访问时间，并具备增加、修改和删除功能。

应具备人员基本信息的查询、统计和报表打印功能。

**3.3.3** **数据处理和存储系统建设**

管网公司智能安防系统各类数据存储方式如下：

1.视频数据：视频数据在建设前端现场级监控子系统时配套采购视频存储设备，录像存储时长需满足相关部门、行业要求，视频存储设备形态不限，可结合实际情况选择SD卡、NVR、磁盘阵列、云存储等多种存储方式。

2.事件数据、人车通行数据等各类数据：在安防系统数据库中长期保存。

3.随事件一同上传的事件截图、人车截图等图片数据：在安防系统服务器中长期保存。

4.管理人员自行下载的视频数据：保存在下载所使用的PC、手机上。

**3.3.4** **其他系统建设**

其他系统包括智能安防系统配套的通用服务器和安防PC。

管网公司智能安防系统需满足安全可靠需求，系统软件需支持安全可靠部署环境，部署软件的硬件服务器和PC需采用安全可靠操作系统、CPU和数据库，操作系统、CPU和数据库需在中国信息安全测评中心的《安全可靠测评结果公告》公示范围内。

**第四章 项目信息资源规划方案**

本次项目拟采用如下信息资源进行规划设计：

通用服务器资源：提供安全可靠服务器，搭建云计算环境。

智能解析资源：根据公司智能分析需求同步提供。

网络资源：采用有线网络及4G/5G无线网络，根据业务需求提升网络带宽/网速。

数据库和中间件：需采用安全可靠产品，数据库需经过安全可靠测评，在安全可靠环境下部署配置。

**4.1 资源体系划分**

数据资源体系的数据来源于集团数据中心、集团内部及各直属于企业、集团各直属企业下属供水厂、二供泵房、营业厅、污水处理厂、泵站、施工现场、办公区等场所的基础数据、业务数据，同时对于基础信息资源、监测监控信息、物联网设备信息等数据资源。吸收来源于互联网、行业专网的开放数据，通过落地传输方式获取的扩展数据，作为发展基础数据的有益补充。

完成基础资源库的建立后，按照“组织、系统、人员、车辆、设备、事件、应急处置”等不同数据分别对基础资源库的数据融合关联后存储至不同的主题库中，实现集团安防数据的可视化分析与一张图展示，便于领导和管理人员洞察安防动态，及时发现安防预警信息。

**4.2 数据资源构成**

参照以往应急管理工作过程的总结，暂时将数据资源划分成“基础数据、业务数据、监测数据和扩展数据”，各类数据内容范围、构成方式情况如下：

基础数据：基础数据是包含东莞水务集团的整体组织架构中的各级部门信息、人员信息、数据关联信息、数据字典等内容所组成。

业务数据：业务数据指东莞水务集团在以往的管理工作中，产生的各类管理信息、任务信息、事件信息、报送信息、演练信息、预案信息、值班信息等信息数据。

监测数据：监测数据指东莞市水务集团已经建成的物联网感知设备所传递回来的监测数据、预警数据、设备数据、视频监控数据等。

扩展数据：扩展数据泛指在东莞市水务集团应急指挥中心在建设各项数据指标或需要使用时，发现的当前未产生的、暂时无法实时接入的业务数据，例如气象数据、气象灾害监测数据等非本单位产生的数据。

**第五章 项目的安全设计**

**5.1 信息系统安全等级定级**

根据《GB∕T 28448-2019 信息安全技术 网络安全等级保护测评要求》和《GB∕T 28449-2018 信息安全技术 网络安全等级保护测评过程指南》等标准，对管网公司安防系统网络开展符合性测评工作，针对信息系统安全整改后的安全情况，衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。

本项目信息安全设置遵循公安部颁布的信息安全技术规范进行，系统工程的风险等级和防护等级均为二级。

**5.2 信息系统安全风险分析**

**5.2.1 风险分析**

传统网络层对Web服务器的防护方式主要是使用防火墙作为安全防护的基础设施，同时辅以IPS设备作为应用层安全检测设备，同时在服务器端安装杀毒软件作为最后一道防线。这样的解决方案存在如下弱点：

（1）防火墙设备对于开放端口的Web服务没有防护能力

一般的网络中都会部署防火墙作为安全防护设备，但防火墙仅能控制非授权IP对内不得访问，对外应用服务器，是被防火墙允许的访问。由于实现原理的限制，防火墙对于病毒或黑客在应用层面的入侵攻击“视而不见”。

（2）入侵检测防御系统（IPS）对于病毒的攻击行为反应缓慢

IPS主要负责监测网络中的异常流量，对受保护网络提供主动、实时的防护，特别是那些利用系统漏洞进行攻击和传播的黑客工具以及蠕虫病毒。由于IPS对WEB的检测粒度很粗，随着网络技术和Web应用的发展复杂化，IPS在更需要专业安全防护特性的WEB防护领域已经开始力不从心。

Web服务器端是Web安全防护的重要环节，虽然Web服务器做了相关的安全防护。但服务器端的安全设置较为专业、复杂，一旦设置不合理，就使得Web服务器端很容易成为恶意攻击入侵的对象。

**5.2.2 控制措施**

可以采用WEB应用防火墙对WEB应用进行安全防护。WEB防火墙可针对WEB应用实现以下防护功能。

**5.2.2.1 漏洞防护**

Web应用防火墙能够对SQL注入、跨站脚本、代码执行、目录遍历、脚本源代码泄露、CRLF注入、COOKIE篡改、URL重定向等多种漏洞攻击进行有效防护。

**5.2.2.2 攻击防护**

Web应用防火墙能够对用户请求提供多重检查机制和智能分析，确保对高安全风险级别攻击事件的准确识别率。针对Flood攻击、SQL注入、跨站脚本、目录遍历等主要攻击手段， WAF系统提供了有效识别、阻断并告警。

**5.2.2.3 网页代码检查**

Web应用防火墙能够对用ASP、ASPX、JSP、PHP、CGI等语言编写的页面，对用SQL Server、MySQL、Oracle等数据构建的网站进行检查，能够在客户网站被挂马之前发现网站的脆弱点，从而使客户可以未雨绸缪，避免挂马事件的发生。

**5.2.2.4 访问加速**

Web应用防火墙通过在现有的互联网中增加一层新的网络架构，将网站服务器内容缓存到系统内存中，使用户可以就近取得所需内容，降低服务器的压力，解决互联网拥挤的状况，提高用户访问服务器的响应速度。从而解决由于网络带宽小、用户访问量大、网点分布不均等原因所造成的用户访问网站响应速度慢的问题。

**5.2.2.5 挂马检测**

多数攻击者在成功入侵并不采取直接的网站篡改，为了获取更多的经济利益往往采取比较隐蔽的方式，其最终目的是为了盗取用户的敏感信息，如各类账号密码，甚至使用户电脑沦为攻击者的“肉鸡”。一旦网站服务器成为传播病毒木马的“傀儡帮凶”，将会严重影响到网站的公众信誉度。

**5.2.2.6 网页防篡改**

Web应用防火墙内置有网页防篡改监控平台，可以对网页防篡改客户端进行实时监控。当网页防篡改客户端与Web应用防火墙的网络中断时，网页文件会被自动锁定，所有“写”的权限进行封锁，只有“读”的权限。当网络恢复中，所有相关权限会自动下发，网站正常恢复更新。

**5.2.3 日志审计**

**5.2.3.1 风险分析**

为了不断应对新的安全挑战，也为了满足等级保护的要求，防病毒系统、防火墙、入侵检测系统、漏洞扫描系统、UTM等等安全系统都仅仅防堵来自某个方面的安全威胁，形成了一个个安全防御孤岛，无法产生协同效应。更为严重地，这些复杂的IT资源及其安全防御设施在运行过程中不断产生大量的安全日志和事件，安全管理人员面对这些数量巨大、彼此割裂的安全信息，操作着各种产品自身的控制台界面和告警窗口，显得束手无策，工作效率极低，难以发现真正的安全隐患。

另一方面，日益迫切的信息系统审计和内控、以及不断增强的业务持续性需求，也对当前日志审计提出了严峻的挑战。等级保护制度，明确要求二级以上的信息系统必须对网络、主机和应用进行安全审计。因此需要一个全面的、面向业务和组织IT资源（信息系统保护环境）的、集中的安全审计平台及其系统，这个系统能够收集来自企业和组织IT资源中各种设备和应用的安全日志，并进行存储、审计、分析、报警、响应和报告。

**5.2.3.2 控制措施**

1.日志资产管理

按照日志资产重要程度和管理域的方式组织日志资产，提供便捷的添加、修改、删除、查询与统计功能，支持日志资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需日志资产的信息，并对资产进行关键度赋值。

2.日志采集

支持对各类网络设备、安全设备、操作系统、数据库、应用系统的日志、事件、告警信息进行全面的日志采集。处理的结果分享给网内其它控制中心和终端，以提高全网的安全防护能力，完成对一次攻击及其报警的闭环防御流程。

3.日志实时监视

系统提供实时的日志滚动显示和查询，可自定义实时监视的日志内容，可查看实时日志详细信息，可通过雷达图等直观显示目前日志量，可以控制日志对管理员账号的可见性管理，在实时监视日志上可悬浮提示资产和常用端口信息。

4.日志实时分析和统计

可对收集的日志进行分类实时分析和统计，从而快速识别安全事故。分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新。

5.关联分析

可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则。

6.告警和响应管理

通过关联分析，对于发现的严重事件可以进行自动告警，告警内容支持用户自定义字段。告警方式包括邮件、短信、SNMP Trap、Syslog等。

7.统计报表

提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报表，满足等保等其他合规性要求，提供自定义报表，用户可根据自身需要进行定制。

8.日志备份归档

支持按照日志存储周期进行备份，当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志，并进行告警。手动备份和恢复时，可以显示恢复和备份的进度。

**5.3 信息系统安全技术方案**

**5.3.1 入网安全评估服务**

网络安全评估是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施。为防范和化解信息安全风险，将风险控制在可接受的水平，从而最大限度地为保障信息安全提供科学依据。

通过开展网络安全评估服务，对部署的云环境的网络安全、主机安全、应用安全、数据安全等开展安全评估，形成网络安全整体分析报告，清晰呈现整体信息安全状况。

通过安全评估及时发现网络安全短板，提供风险安全所需的技术服务支持，对主机、网络设备、数据库、中间件、应用系统等从技术等层面提供专业的安全整体规划方案、提供整改建议、并协助实施合理的风险控制措施，将系统的安全风险控制在可接受的范围内，最大程度的防止各类安全事件的产生，保障业务网络与信息系统的安全、稳定运行。

针对收集的信息系统资产，需要进行安全评估以发现当前业务系统存在的安全脆弱性及薄弱点。安全评估主要有三个层面：互联网侧安全评估、业务网络安全评估、业务系统安全评估。

互联网侧安全评估：能够发现系统暴露在互联网层面的安全问题。这类问题时刻面临互联网侧的攻击威胁，提高系统运行风险。针对互联网侧安全评估的主要手段有：系统漏洞扫描、web应用漏洞扫描等。

业务网络安全评估：主要针对业务网络体系安全防护手段及网络设备配置的安全型进行评估。根据最小权限原则对网络设备配置及设备本身安全性进行评估。主要手段有：网络设备漏洞扫描，网络设备配置合规检查，网络体系安全分析等。

业务系统安全评估：针对重要应用资产在网络安全防护内部进行安全评估。挖掘纵深体系层面存在的安全风险。主要手段与互联网评估相同：系统漏洞扫描、web应用漏洞扫描等。

**5.3.2 代码审计服务**

代码审计是由具备高技能和高素质的安全服务人员发起，检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。

代码审计服务的目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。信息安全问题时刻都有新的变化，新的攻击方法层出不穷，攻击者攻击的方向越来越侧重于利用软件本身的安全漏洞，例如SQL注入漏洞、跨站脚本漏洞、CSRF漏洞等，这些漏洞主要由不良的软件架构和不安全的编码产生。

开展源代码审计能够降低源代码出现的安全漏洞，构建安全的代码，提高源代码的可靠性，提高应用系统自身安全防护能力。源代码安全检测能够帮助开发人员提高源代码的质量，从底层保障应用系统本身的安全，从早期降低应用系统的开发成本。

**5.3.2.1 渗透测试服务**

渗透测试是通过模拟黑客攻击的手法对某个特定网络系统进行测试，以期发现和挖掘网络系统中存在的漏洞。渗透测试不同于漏洞扫描等安全评估服务，它是遵从黑客通用的攻击流程和路线，利用多种手段对网络系统进行侵略性测试，而漏洞扫描只会以一种非侵略性的方式，仔细地定位和量化系统的所有漏洞。

**5.3.2.2 系统层安全渗透测试**

系统安全脆弱点测试包括但不限于如下内容：

1.口令猜解

针对操作系统、数据库等应用的口令登录安全进行测试，利用自动化工具，并通过使用密码字典文件，大量尝试登录单位内部的系统，进而找出存在空口令、弱口令的系统账号。该测试存在一定的安全风险，因为当系统设备启用密码登录安全策略时，大量的尝试会造成账号锁定，导致拒绝服务攻击发生，故执行相关操作时需特别当心。

2.溢出测试

当无法直接利用帐户口令登陆系统时，也会采用系统溢出的方法直接获得系统控制权限，此方法有时会导致系统死机或从新启动，但不会导致系统数据丢失，如出现死机等故障，只要将系统从新启动并开启原有服务即可。

3.敏感信息泄露

敏感信息的泄露会使系统存在于风险当中，如开启了不需要的服务、服务端口不恰当的对非授权区域开放、DNS区域传送机制未合理配置、特定系统服务（如Telnet、SSH、FTP等）旗标未修改屏蔽等，此类敏感信息的不合理控制，会给攻击者的信息收集以及系统攻击工作带来极大便利，因此，在本服务测试中将对此类信息进行重点排查。

4.系统安全管理

严格管理系统账户、有效控制系统服务，优化系统的安全配置，启用系统必要的安全控制措施，避免系统发生故障或遭受攻击。

5.系统漏洞

针对业务系统所需要的系统服务进行优化管理和配置。

6.系统访问控制和审计

对系统进行有效访问控制和日志审计。

**5.3.2.3 Web中间件渗透测试**

针对Web常见的软件，例如Apache、IIS、Tomcat中间件等各类应用软件中常用到的软件，自身存在一些由于版本较低或配置不当所造成的安全隐患和漏洞，作为渗透测试的一些主要内容和方向。

**5.3.2.4 Web应用渗透测试**

针对Web常见的应用，重点是由于应用软件在设计和开发的过程中，由于安全设计不足和开发不规范所造成的隐患和漏洞。

**5.3.2.5 整改建议和复测**

根据渗透测试工作开展情况，出具详细的《渗透测试报告》，重点描述测试发现的问题、严重程度，同时在报告中提供对安全漏洞及问题的整改建议，同时配合用户单位或者第三方公司一起讨论具体加固实施办法，规避安全整改风险，通过安全加固工作修复安全漏洞，降低安全风险。

## 附件2：

**管网公司安防监控设备清单收集表(202405)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **分公司** | **普通摄像头 （个）** | | | **智能摄像头 （个）** | | | **人员通道闸机 （套）** | | | **车辆道闸 （套）** | | | **ID/IC门禁 （套）** | | | **人脸门禁 （套）** | | | **指纹门禁 （套）** | | | **脉冲电子围栏 （套)** | | | **红外/激光对射围栏（套)** | | | **备注** |
| **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** | **现有** | **品牌及对应数量** | **计划新增** |
| 第一分公司 | 232 | 海康221 大华8 科维视3 | 79 | 0 |  | 12 | 0 |  | 0 | 0 |  | 0 | 0 |  | 0 | 1 | ZK（中控）1 | 0 | 1 | ZK（中控）1 | 0 | 0 |  | 0 | 0 |  | 0 |  |
| 第二分公司 | 309 | 海康309 | 40 | 0 |  | 15 | 0 |  | 0 | 0 |  | 0 | 0 |  | 0 | 1 | 未知品牌1 | 15 | 0 |  | 0 | 0 |  | 0 | 0 |  | 0 |  |
| 第三分公司 | 118 | 海康118 | 39 | 107 | 海康107 | 15 | 0 |  | 0 | 0 |  | 6 | 0 |  | 0 | 0 |  | 11 | 0 |  | 0 | 0 |  | 0 | 0 |  | 0 |  |
| 第四分公司 | 377 | 海康威视377 | 70 | 20 | 海康威视20 | 10 | 0 |  | 0 | 0 |  | 0 | 0 |  | 0 | 5 | 海康威视5 | 50 | 0 |  | 0 | 0 |  | 11 | 0 |  | 0 |  |
| 第五分公司 | 131 | 海康131 | 92 | 6 | 莹石云6 | 12 | 0 |  | 0 | 0 |  | 6 | 0 |  | 6 | 0 |  | 6 | 0 |  | 0 | 0 |  | 6 | 0 |  | 6 |  |
| 第六分公司 | 45 | 19大华 26海康 | 57 | 0 |  | 10 | 0 |  | 0 | 0 |  | 0 | 0 |  | 0 | 0 |  | 10 | 1 | 大华1 | 0 | 1 | 艾礼安1 | 1 | 0 |  | 0 | 1套门禁包含6路门禁 |
| 安监部 |  |  | 65 |  |  | 5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 已采购 |
| **合计** | **1212** |  | **442** | **133** |  | **79** | **0** |  | **0** | **0** |  | **12** | **0** |  | **6** | **7** |  | **92** | **2** |  | **0** | **1** |  | **18** | **0** |  | **6** | 根据与设备部沟通，未来几乎所有地面泵站均需安装脉冲电子围栏，预计脉冲电子围栏总缺口54套。（红外/激光对射围栏暂不考虑） |
| **注意： 1.本次收集统计为截止2024年5月底现有安防设备及至2024年年底拟安装安防设备数据； 2.本次统计的安防设备需为国标数字设备，确认非国标非数字设备（如老旧的模拟信号摄像头）及确认费标准化的车辆自带行车记录仪请勿统计，门禁等不确认的电子设备均按现状进行填写。** | | | | | | | | | | | | | | | | | | | | | | | | | | | | |