**滨江区智慧防潮安全管理系统项目**

**建设方案**

**项目编号：**

**设计编号：**

**建设单位：****杭州市滨江区农业农村局**

**设计单位：北京华麒通信科技有限公司**

**北京华麒通信科技有限公司**

（原：北京市电话通信设计院有限公司）

**2019年7月**

**滨江区智慧防潮安全管理系统项目**

**建设方案**

**总 经 理： 付 刚 毅**

**总 工： 方 宇**

**设计总负责人： 郭 文 川**

**设计负责人： 黄 赵 良**

**审 核 人： 高 建 全**

**概预算审核人： 高 建 全**

**概预算证号： 通信（费用）字170100597**

**概预算编制人：** **车 顺 庆**

**概预算证号： 通信（费用）字170100157**

**目 录**

[第一章 项目概述 3](#_Toc20047787)

[1. 项目背景 3](#_Toc20047788)

[2. 项目需求 3](#_Toc20047789)

[2.1 视频安防需求 3](#_Toc20047790)

[2.2 应急预警需求 3](#_Toc20047791)

[2.3 巡查管理需求 4](#_Toc20047792)

[2.4 人员管理需求 4](#_Toc20047793)

[3. 建设目标 4](#_Toc20047794)

[4. 设计原则 4](#_Toc20047795)

[5. 设计依据 6](#_Toc20047796)

[第二章 系统总体设计 7](#_Toc20047797)

[1. 系统架构 7](#_Toc20047798)

[2. 子系统组成 7](#_Toc20047799)

[3. 视频监控系统 8](#_Toc20047800)

[3.1 点位布置 8](#_Toc20047801)

[3.2 警戒线规划 13](#_Toc20047802)

[3.3 存储方式 13](#_Toc20047803)

[3.4 应用场景举例 13](#_Toc20047804)

[4. 信息发布系统 14](#_Toc20047805)

[4.1 系统架构 14](#_Toc20047806)

[4.2 系统功能 15](#_Toc20047807)

[4.3 信息发布系统的安装 17](#_Toc20047808)

[5. 公共广播系统 18](#_Toc20047809)

[5.1 系统结构 18](#_Toc20047810)

[5.2 系统功能 19](#_Toc20047811)

[6. 安全管理平台 19](#_Toc20047812)

[6.1 系统基本功能 19](#_Toc20047813)

[6.2 报警功能 20](#_Toc20047814)

[6.3 巡查管理 21](#_Toc20047815)

[6.4 各系统的联动功能 22](#_Toc20047816)

[6.5 数据统计报表分析功能 22](#_Toc20047817)

[6.6 其他功能要求 22](#_Toc20047818)

[7. 网络安全等级保护要求 23](#_Toc20047819)

[7.1 机房安全要求 23](#_Toc20047820)

[7.2 网络安全要求 23](#_Toc20047821)

[7.3 网络安全设备 25](#_Toc20047822)

[8. 其他要求 35](#_Toc20047823)

[81. 设备安装方面 35](#_Toc20047824)

[8.2 电源引入方面 35](#_Toc20047825)

[8.3 防雷接地方面 35](#_Toc20047826)

[第三章 设备配置 36](#_Toc20047827)

[1.网络详细拓扑 36](#_Toc20047828)

[2.设备材料配置 37](#_Toc20047829)

# 第一章 项目概述

## 1. 项目背景

钱塘江潮被誉为“天下第一潮”，是世界一大自然奇观，它是天体引力和地球自转的离心作用，加上杭州湾喇叭口的特殊地形所造成的特大涌潮，因此观潮期会吸引广大群众来江边观潮。不仅如此，沿江还设有“最美跑道”供市民散步运动，江边无论是在观潮期，休息节假日还是工作日，都有不少人员在江边活动。

钱塘江滨江区段南起华家排灌站，东至七甲排灌站，沿江约17公里。钱塘江沿江安全管理任务艰巨而繁重，要保障江堤边人员的安全活动，严防发生重大安全生产事故与人员安全事故。

为了预防和减少钱塘江潮汐引发的人员伤亡事件，保护人民群众生命财产安全，维护社会稳定，加强钱塘江防潮安全管理工作尤为重要。随着钱塘江南岸最美跑道的建成，傍晚在江堤边休闲锻炼的群众也越来越多，给江堤的安全和科学管理带来了非常大的挑战；随着最美跑道里程的不断增大，江堤环境差异大，对安防系统的全面性和适应性提出了要求；江堤巡查工作越来越大，但是巡查人员有限，单凭人力，很难做到全覆盖管理；游客对钱江潮威力了解不足，安全意识弱，如何提升游客的安全意识，也是政府部门的重要工作之一。管理挑战方面：由于历史建设原因，各部门安防子系统分阶段建设，系统、产品众多，各自独立运行，缺乏联动和统一管理。同时大部分设备仅仅检测江堤道路上的情况，未对翻越江堤护栏的行为予以有效监测；当前的系统主要还是事后查看和取证，缺乏事前防范和事中应急机制。

## 2. 项目需求

### 2.1 视频安防需求

防潮人员潮前潮后、夜间重点时间段需进行江堤安全防护工作，但现场巡查人员有限，江堤安防管理存在监控覆盖漏洞。控制中心需通过视频监控等辅助手段，在重点时间段对江堤下方进行监管。

### 2.2 应急预警需求

近年来因违规翻越护栏引发潮水吞人的事件频发，如何进行全局资源的调度整合，快速处理此类突发事件，争取更多的主动性，尽可能的降低事件的影响，建设一套扁平化、立体化、自动化的应急指挥系统，成为安全管理系统的迫切需求。控制中心需通过信息化手段，对翻越江堤护栏，下到江堤下方的情况及时、准确预警，并实时跟踪确认人员是否离开。

### 2.3 巡查管理需求

钱塘江畔日常巡查工作中，控制中心需实时获知巡查人员巡查路线、所在位置。突发事件发生时，巡查人员可以对现场情况进行录像、拍照，证据留存。

### 2.4 人员管理需求

钱塘江畔的樱花大道，已成为滨江一道新的风景线，游客越来越多，江堤下方相对开放，管理难度较大，目前管理方法主要依赖于人工，无法形成一套行之有效的，集事前、事中和事后的人员管理措施。为预防和减少钱塘江潮汐引发的人员伤亡事件，保护人民群众生命财产安全，所以对安全管理系统的建设提出了很高的要求。

## 3. 建设目标

* 实现不同业务统一平台管理，视频监控系统、信息发布系统、公共广播系统等的运行管理接入安全管理平台实现业务管理；
* 通过视频监控系统实现江堤护栏翻越报警，并且对异物干扰产生的误报警，系统能够自动过滤；
* 视频监控系统报警信息能够及时上传至管理平台，安全管理平台自动联动广播系统播放告警提醒，并在告警提醒未起效的情况下，将警情发送到就近巡检人员手持终端上，巡检人员能够第一时间对紧急情况进行处理；
* 信息发布系统发布各种宣传告示、潮水涨退时间等信息，让游客了解钱江潮，增强游客的安全意识；
* 安全管理平台可通过大数据分析，实现重点时段重点区域重点管理；
* 安全管理平台预留与其他平台（如公安平台、雪亮工程平台、城市大脑平台等）的数据对接功能。

## 4. 设计原则

为了达到国内领先的目标，安全管理系统的建设应该充分考虑系统的合理性、先进性、实用性、可靠性、稳定性和可扩展性的原则。

**合理性原则**

为了保证整个系统从设备配置到系统构成的合理性，系统建设需根据滨江区农业农村局等相关部门的具体要求，充分满足用户在使用中的各项功能要求。为了保证系统的应用，本系统提供开放的软件接口，接受SDK封装接入，兼容其他品牌设备的SDK按照一定标准再次封装，消除产品质量差异性，稳定、高效地接入到系统平台中。

**先进性原则**

当前，计算机及通信技术高速发展，使得系统的设计不但要考虑充分利用当前的最新技术，而且还必须考虑随着技术的进一步发展，能在系统中不断溶入新技术，使系统始终充满活力，始终保持一定的先进性。同时采用先进的具有高度扩展性的架构，为系统扩展应用打好基础，系统建成后符合发展趋势，具备科技的先进性。

**实用性原则**

此系统的建设应以实用性为基本原则。系统功能必须满足采、传、存、显、控的基本要求，硬件和软件平台界面友好、易学易用、使用方便、图像清晰；采用统一的系统标准和通信协议，使整个系统中各个子系统间能互联互控，充分发挥整个系统的功能。

**可靠性原则**

在考虑技术先进性和开放性的同时，还应从系统结构、技术措施、设备性能、系统管理、厂商技术支持及维修能力等方面着手，确保系统运行的可靠性和稳定性，达到最大的平均无故障时间（MTBF）。

系统建设的关键，需要保证系统的完整性、正确性和可恢复性。系统的不稳定因素要从硬件、软件系统协同运行中给予充分的防止。如有发生也应做到可即时地恢复。

本系统的规模无论在网络、系统平台，还是在系统应用方面都应具有相当的规模，系统的运行可靠性是主要性能之一。

系统的可靠性主要表现在以下几个方面：

* 前端摄像系统的可靠性
* 视频存储系统的可靠性
* 安全管理平台的可靠性

## 5. 设计依据

系统规划设计必须按照国际、国家和本地区的有关标准和规范进行。本设计将依据和参照以下的设计规范和要求进行：

**城市联网监控报警系统设计方面：**

* 《城市监控报警联网系统技术标准》（GA/T669-2008）
* 《跨区域视频监控联网共享技术规范》DB33/T 629-2007

**安防视频监控系统设计方面：**

* 《中华人民共和国公安部行业标准》（GA70-94）
* 《视频安防监控系统技术要求》（GA/T367-2001）
* 《安全防范系统通用图形符号》（GA/T75-2000）

**视频系统网络设计方面：**

* 《信息技术开放系统互连网络层安全协议》（GB/T 17963）
* 《计算机信息系统安全》（GA 216.1－1999）
* 《计算机软件开发规范》（GB8566-88）

**视频系统工程建设方面**

* 《安全防范工程程序与要求》（GA/T75-94）
* 《安全防范工程技术规范》(GB 50348-2004)

**网络安全等级保护方面**

* 《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）
* 《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T25070-2019）

# 第二章 系统总体设计

## 1. 系统架构

智慧防潮安全管理系统基于新增网络建设实现纯网络化数字架构。系统建设采用热成像双目球型摄像机，提供高质量图像，实现真正意义上的高清数字化视频系统。系统存储采用后端NVR集中本地存储，提高系统视频图像的管理性、预览实时性、控制灵敏性等功能。

安全管理中心可以对所有图像进行实时浏览、控制、录像查询和回放，可以对所有翻越报警进行查询处置，可以对巡查工作进行管理。

安全管理系统通过视频监控子系统实现江堤护栏翻越报警，报警信息能够及时上传至安全管理平台，平台自动联动广播子系统告警提醒，并在告警提醒未起效的情况下，将警情发送到就近巡检人员的手持终端上，巡检人员能够第一时间对紧急情况进行处理；并能通过LED屏发布宣传公告及潮水信息，让游客了解钱江潮，增强游客的安全意识。



网络拓扑图

## 2. 子系统组成

本项目主要包括以下子系统：



视频监控系统、信息发布系统、公共广播系统采用租用运营商专线形式，将其信号从前端设备传输至局控制中心。

租用运营商的VPN专线即可减少传输链路的建设投资，又减轻后期运行维护成本，同时运营商的网络采用多接点接入、环路保护等方式建设，相比滨江区农业农村局自建传输链路可靠性更高、安全性更好。本项目需要租用专线：6\*20M+49\*10M。

## 3. 视频监控系统

视频监控系统是整个智慧防潮安全管理系统规划的重点，它是一个分布式的系统，提供安全监管、设备监控、管理运维、案发后查、证据提取等有效的技术手段。

该子系统具有智能化、高效率特点，系统采用数字化采集、全网络传输、集中存储、控制及显示，主要由前端摄像机设备、视频显示设备、控制键盘、视频存储设备、相关应用软件以及其它传输、辅助类设备组成。

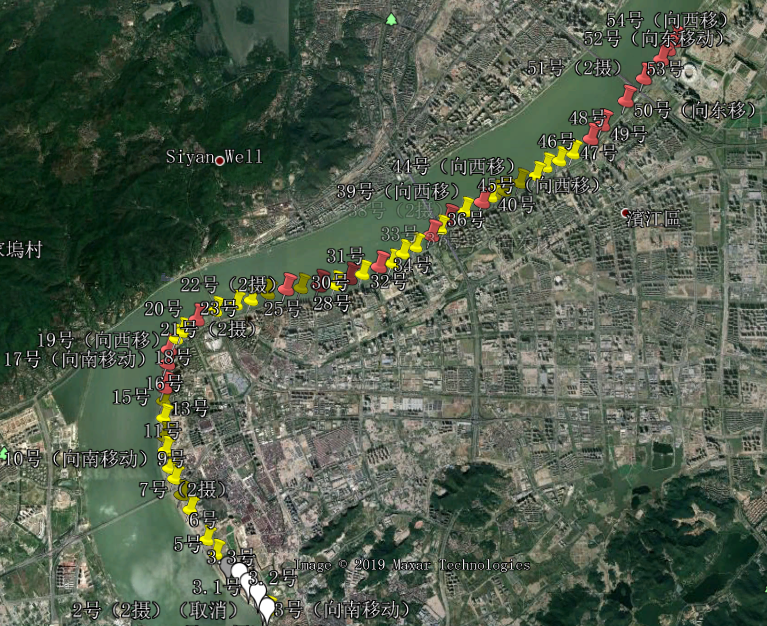
系统具有可扩展和开放性，以方便未来的扩展和与其他系统的集成。视频监控子系统最直接、最主要的作用就是使管理人员能远程实时掌握各重要区域发生的情况，保障监管区域内部人员及财产的安全。

### 3.1 点位布置

钱塘江滨江区段南起华家排灌站，东至七甲排灌站，沿江约17公里，沿岸共设55块防潮警示牌，警示牌上安装热成像双目球型摄像机，分为3种选型，明确能自动识别200米、350米、500米。

本项目共安装61个摄像机，其中：

* 能识别200米的摄像机15个；
* 能识别350米的摄像机41个；
* 能识别500米的摄像机5个。



| **点位编号** | **警示牌** | | **与下一点位直线距离（米）** | **摄像头** | | | **附近标志物** | **备注** | **专线接入** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **有无警示牌** | **是否安装LED** | **数量** | **规格** | **朝向** |
| 3号 | 有 | 无 | 190 | 1 | 200m | 朝北 | 华家排灌站 | 警示牌向南移动至景观台转弯处 | 10M |
| 3.1号 | 无 | 无 | 230 | 1 | 350m | 朝北 |  | 新设警示牌 | 10M |
| 3.2号 | 无 | 无 | 235 | 1 | 350m | 朝北 |  | 新设警示牌 | 10M |
| 3.3号 | 无 | 无 | 225 | 1 | 350m | 朝北 |  | 新设警示牌 | 10M |
| 4号 | 无 | 无 | 450 | 1 | 500m | 朝北 | 越浪点1 | 新设警示牌 | 10M |
| 5号 | 有 | 无 | 280 | 1 | 350m | 朝北 |  |  | 10M |
| 6号 | 有 | 无 | 605 | 1 | 350m | 朝北 |  |  | 10M |
| 7号 | 有 | 无 | 305 | 2 | 350m 350m | 朝南 朝北 |  |  | 20M |
| 8号 | 有 | 无 | 305 | 1 | 350m | 朝北 |  |  | 10M |
| 9号 | 有 | 无 | 180 | 1 | 200m | 朝北 | 9和10之间有突出 |  | 10M |
| 10号 | 有 | 无 | 330 | 1 | 350m | 朝北 |  | 警示牌向南移动至平台转弯处 | 10M |
| 11号 | 有 | 无 | 255 | 1 | 350m | 朝北 |  |  | 10M |
| 12号 | 有 | 无 | 325 | 1 | 350m | 朝北 |  |  | 10M |
| 13号 | 有 | 无 | 310 | 1 | 350m | 朝北 |  |  | 10M |
| 14号 | 有 | 无 | 270 | 1 | 350m | 朝北 |  |  | 10M |
| 15号 | 有 | 有 | 405 | 1 | 500m | 朝北 | 东信大道口 |  | 10M |
| 16号 | 有 | 有 | 250 | 1 | 350m | 朝北 | 新和路口 |  | 10M |
| 17号 | 有 | 有 | 205 | 1 | 350m | 朝北 | 17和18之间外面有建筑物 | 17号只做监控，向南移动至转弯处 | 10M |
| 18号 | 有 | 无 | 150 | 1 | 200m | 朝北 | 有3块牌 | 18号只做监控 | 10M |
| 19号 | 有 | 无 | 325 | 1 | 350m | 朝东 |  | 警示牌向西移动至转弯处 | 10M |
| 20号 | 有 | 有 | 380 | 1 | 200m | 朝东 | 六和路口 |  | 10M |
| 21号 | 有 | 无 | 390 | 2 | 200m 200m | 朝西 朝东（到桥） | 20和21之间有转弯 |  | 20M |
| 22号 | 有 | 无 | 300 | 2 | 200m 350m | 朝西（到桥） 朝东 | 21和22之间是钱江大桥 |  | 20M |
| 23号 | 有 | 无 | 330 | 1 | 350m | 朝东 |  |  | 10M |
| 24号 | 有 | 无 | 290 | 1 | 350m | 朝东 |  |  | 10M |
| 25号 | 有 | 有 | 290 | 1 | 350m | 朝东 | 东信大道口 |  | 10M |
| 26号 | 有 | 无 | 315 | 2 | 200m 350m | 朝西 朝东 | 25和26之间有转弯 |  | 20M |
| 27号 | 有 | 有 | 290 | 1 | 350m | 朝东 | 伟业路口 |  | 10M |
| 28号 | 有 | 无 | 260 | 1 | 350m | 朝东 |  |  | 10M |
| 29号 | 有 | 有 | 270 | 1 | 350m | 朝东 | 火炬大道口 |  | 10M |
| 30号 | 有 | 无 | 305 | 1 | 350m | 朝东 |  |  | 10M |
| 31号 | 有 | 有 | 240 | 1 | 350m | 朝东 | 信诚路口 |  | 10M |
| 32号 | 有 | 无 | 255 | 1 | 350m | 朝东 |  |  | 10M |
| 33号 | 有 | 无 | 260 | 1 | 350m | 朝东 | 柳岸阁对面 |  | 10M |
| 34号 | 有 | 无 | 305 | 1 | 350m | 朝东 |  |  | 10M |
| 35号 | 有 | 有 | 210 | 1 | 350m | 朝东 | 35和36之间有平台 | 警示牌向东移动至平台上 | 10M |
| 36号 | 有 | 无 | 205 | 1 | 350m | 朝东 |  |  | 10M |
| 37号 | 有 | 有 | 360 | 1 | 200m | 朝东 | 钱江四桥下 |  | 10M |
| 38号 | 有 | 无 | 335 | 2 | 200m 350m | 朝西 朝东 | 37和38之间有转弯 |  | 20M |
| 39号 | 有 | 有 | 200 | 1 | 200m | 朝东 |  | 警示牌向西移动至坝东 | 10M |
| 40号 | 有 | 无 | 125 | 1 | 200m | 朝东 |  |  | 10M |
| 41号 | 有 | 无 | 135 | 1 | 200m | 朝东 | 41和42之间有排灌站 | 41号只做监控 | 10M |
| 42号 | 有 | 无 | 310 | 1 | 350m | 朝东 | 萧山排灌站 |  | 10M |
| 43号 | 有 | 无 | 315 | 1 | 350m | 朝东 | 钱王射潮 |  | 10M |
| 44号 | 有 | 无 | 250 | 1 | 350m | 朝东 | 44和45之间有3个亭子 | 警示牌向西移动至转弯处 | 10M |
| 45号 | 有 | 无 | 275 | 1 | 350m | 朝东 |  | 警示牌向西移动至坝东 | 10M |
| 46号 | 有 | 无 | 275 | 1 | 350m | 朝东 | 星光大道西侧 |  | 10M |
| 47号 | 有 | 无 | 430 | 1 | 500m | 朝东 | 星光大道东侧 |  | 10M |
| 48号 | 有 | 有 | 330 | 1 | 350m | 朝东 |  |  | 10M |
| 49号 | 有 | 有（没显示） | 615 | 1 | 350m | 朝东 |  |  | 10M |
| 50号 | 有 | 有 | 500 | 1 | 350m | 朝西 |  | 警示牌向东移动至坝西 | 10M |
| 51号 | 有 | 有 | 480 | 2 | 500m 500m | 朝西 朝东 | 钱江三桥下 |  | 20M |
| 52号 | 有 | 有 | 230 | 1 | 350m | 朝东 | 52和53中间有坝 | 警示牌向东移动至坝东 | 10M |
| 53号 | 有 | 有 | 200 | 1 | 200m | 朝东 | 53和54之间有转弯 |  | 10M |
| 54号 | 有 | 有 |  | 1 | 200m | 朝东（萧山） | 七甲排灌站 | 54号只做监控 | 10M |
| **统计** | **共55块（4块未安装）** | **18块已装LED,37块未装LED** |  | **61** | **200m\*15 350m\*41 500m\*5** |  |  | **前端扬声器:55个 远端机箱:55个** | **(6\*20M+49\*10M)** |

### 3.2 警戒线规划

江边现有立杆距离护栏较远，沿江最小为6米，最大可达22米。若将警戒线划在护栏位置，因视频画面为2D，故人员在跑道上走动即会触发告警；若将警戒线的位置划在人员走动无法触发的位置，则人翻越护栏等情况将无法触发警戒线造成漏报。

故本项目对警戒线规划有以下要求：

* 摄像机安装在警示牌的上面，根据摄像机可视情况，需要部分加高或需横杆往河面上跳出一段长度（具体根据现场实际情况决定）；
* 警戒线位置划在护栏外江侧30-50cm；
* 在有人员经常进出的堤坝、码头、排灌站等位置，根据业主要求，不需划线，避免发生误报警。

### 3.3 存储方式

视频图像文件存储有两种方式，本地用户管理中心存储与公有云存储。本地存储和云存储位于两个不同的位置。本地存储使用本地的硬件和软件，也就是说，硬件是由滨江区农业农村局拥有和管理的，而不是云服务提供商。公有云存储驻留在远程服务器上，可以跨越城市，也可以跨越全国，它通常由大型云计算公司提供。

本地存储：存储资源由滨江区农业农村局采购、拥有和管理；滨江区农业农村局负责保护及维护存储资源和数据；存储资源归滨江区农业农村局所有。

公有云存储：存储资源由第三方拥有和管理；存储资源可以在预付费或按需付费的基础上购买；存储资源可以在多租户环境中共享。

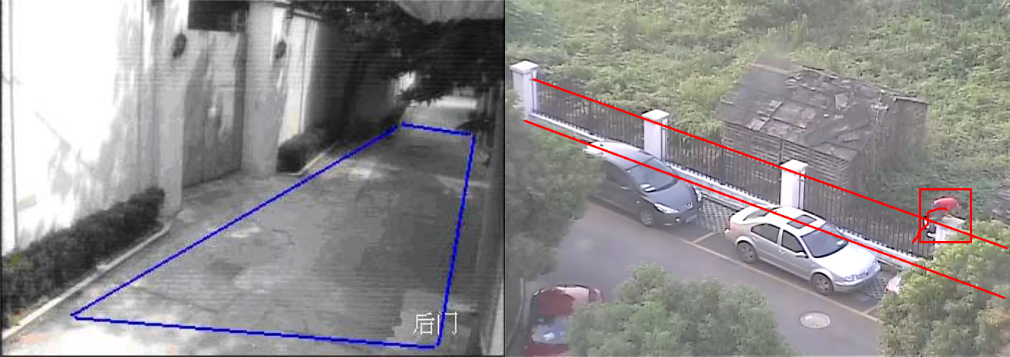
本项目采用本地存储方式，项目要求视频录像存储时间1个月，为保证本地存储安全性，配置不间断电源系统（UPS）。

### 3.4 应用场景举例

* 江堤周界

传统周界防范系统主要是采用红外对射等技术来检测违规人员入侵，但是此类防范措施有其自身的局限性。红外对射设备安装都是显性，入侵人员可有意识的避开。红外对射设备无法判别闯入人员行为方向。

红外对射设备是依据周界形状安装，一旦防范周界发生改变，又需重新安装。在传统防范系统基础上，采用智能视频分析技术可以有效的避免上述的局限性。周界入侵可采用多种智能分析相结合，以提高预警的准确性，如区域徘徊+绊线检测。



* 防落水

钱塘江边常会发生人员翻越江堤或者意外落水等安全事故。通过视频监控的智能分析功能，可以对以上状况及时报警，对于危险区域，还可以设计多级防区，提前告警，预防人员进入危险区域。



## 4. 信息发布系统

信息发布系统是滨江区农业农村局通过在原有警示牌的基础上，进行加装改造，安装显示屏和播放终端，来发布各种宣传告示、潮水涨退时间等信息。

### 4.1 系统架构

信息发布系统是利用信息发布屏将文字、图片、视频等各类多媒体信息全方位展现出来的一种高清多媒体显示技术。它作为一种迅速发展的综合性电子信息技术，能够综合处理文本、图形、图像、音频、视频等多媒体信息，使多种信息建立逻辑连接，集成为一个系统并具有强大的交互性。



* 信息发布管理服务器

信息发布管理服务器具有资源管理、播放设置、终端管理及用户管理等主要功能模块，用户通过安装管理客户端，可对播放内容进行编辑、审核、发布、监控等，对所有信息发布终端进行统一管理和控制。

* 信息发布主机

主要接收传送过来的多媒体信息，将画面内容展示在显示终端上，可提供高质量的播出效果以及安全稳定的播出终端。

* 显示终端

前端的显示设备可以为室内/外LED全彩屏、液晶拼接屏、液晶监视器、信息发布屏或信息发布一体机，用户可以根据自身需要自主选择。

### 4.2 系统功能

信息发布系统管理软件主要包括节目制作、节目发布、播放管理、节目素材管理、系统设置、终端管理、系统备份还原、动态数据组件、数据统计、日志管理等基本功能以及扩展的功能应用。主要功能如下：

* 所见即所得的节目制作

用户登录系统管理端后可制作节目，灵活组合背景图、视频、音频、图片、字幕和实时数据等，排版组合成多媒体节目，各区域播放内容使用单独的播放列表进行控制，并可以设置节目单有效播放时间。也可以使用节目模板对界面排版进行快速制作，同时支持节目单导入导出功能，对节目单进行快速更改。实现不同的场所、不同受众、不同时间段播放不同的信息内容。

* 强大的动态数据组件

信息发布系统软件集成了动态数据组件，通过网页解析、文本文件、数据库、WebServices、Socket、RSS、FTP传输或者其他特定格式文件等方式，从数据源取得动态实时数据，以直观可视化方式排版显示。

* 全效的节目播放控制

**垫片播放：**默认播放垫片节目。可多个垫片节目循环播放。垫片节目存入系统存储单元中，没有节目单播放时默认播放垫片节目。防止终端出现不播放黑屏现象。

**周期播放：**可按月/周设定循环播放，可单独设定周期内每天的播放时段。同时配合定时开关机、时段音量控制，既可进行信息发布又不至于打扰受众休息，引起反感。

**定时播放：**可根据需要自由设定节目播放的具体日期区间与时间段组合。可对不同的受众进行定时的信息投放，或特定提示、常规信息播放等。

**间隔插播：**每隔一段时间固体播放几个节目，一般常用于广告投放。

**独占节目插播：**在周期播放、自定义播放方式中，可选独占节目选项，即为设置的时间内只播放该节目，也可由外部人员控制触发，可用于紧急信息广播、温馨提示，常规信息播报等

**分组播放：**不同终端，进行区域分组，每组内容可以播放同样的内容，不是组播放不同内容。

以上几种播放方式组合，不同终端播放不同的节目内容，不同的时间段可播放不同的节目内容（分黄金时间与非黄金时间）。这样使播放的节目内容更具有针对性，大大提高关注度。

* 严谨的系统权限管理

**节目审核：**用户上传的节目必须经过审核方可进行节目单编辑及播放终端播放。配合用户权限管理可以对播放素材可控性管理。

**节目加密：**节目素材经过审核后并将素材进行加密，没经过加密的素材终端不会播放，保护播放内容的可控性。

**用户权限管理：**管理用户的个人信息，配置用户的所属机构及角色权限。可以配置是否具体素材审核权限及具体终端管理权限。

用户权限管理、节目审核及加密能够控制一切非平台审核通过的节目在终端上播放。能有效控制信息内容的安全发布。

* 实时的终端监控维护

**远程控制：**支持远程设置终端的开始播放/停止播放、定时开关机、连接中心服务器设置、流媒体播放、紧急信息插播、固件升级等，便捷实现终端的远程控制及维护。

**实时监控：**管理人员可实时监控各播放终端当前播放的节目、插播消息、播放日程安排、终端在线状态显示、终端状态反馈、终端播放内容截图。同时支持播放日志、下载日志、系统状态日志等查看，确保播放内容的正常安全。

### 4.3 信息发布系统的安装

充分利用原有警示牌的基础上进行加装改造，可利用原来警示牌对警示牌的LED系统进行整合，提升改造成为在线式系统共并与新平台对接，新制作告示牌的LED屏为在线式系统。并在人员密集区域或易发危险区域安装5块LED大屏，用于宣传及播放信息，安装位置由滨江区农业农村局指定。



## 5. 公共广播系统

公共广播的功能用于提供背景音乐、发布业务信息、寻呼以及强行插入包括泄洪预警、突发事故的紧急广播，伴随着经济发展及城市建设速度的加快，公共广播的运用范畴不断扩展。

本项目的公共广播将对钱塘江沿江人员聚集区提供业务信息覆盖、突发事故的紧急广播功能。对沿江江堤区域进行有效覆盖，对危险情况发布警示信息，避免发生涉水等意外事故。

### 5.1 系统结构

本系统采用了网络化架构，从管理中心到其它各个解码终端均通过网络数字传输，可以实现远程广播；通过程序控制可以实现定点、定时、分区、全体广播讲话、播放背景音乐，当出现危险情况，安全管理平台可通过视频系统联动广播系统自动广播提醒，中心工作人员也可以手动向各个区域广播提醒。

公共广播系统主要由广播系统管理服务器、网络编码器、音源设备、人工呼叫站、功率放大器（带解码功能）、扬声器及相关系统接口组成。

功放的容量按本区域扬声器最大功率进行计算。一般情况，输出功率满足现场要求，满足全域的全音量需要。

由于本次前端扬声器位置较为分散，采用功放就地放置（或前端扬声器内置功放）的方式。系统电源就近引自景观照明配电箱。扬声器要求声音传播距离200-300米。



### 5.2 系统功能

**公共广播：**即根据本项目的需要，可以实现对整个区域的整体广播；

**定时播放：**实现背景音乐、安全提示、天气预报等自动播放；

**智能管理：**实现自动开关机，默认执行该天的播放列表达到无人值守功能；

**分区控制：**分区管理，既可整体播放，也可单个或多个区域组合播放；

**可视对讲：**寻呼话筒主机之间可相互呼叫、双向可视化对讲，寻呼话筒主机可与终端实现单向可视化对讲；

**紧急呼叫：**满足广播通知，支持应急广播，可对全区或分区进行紧急呼叫；

**报警联动：**总控中心（监控中心）接到紧急情况信号后，直接传给广播终端，触发广播系统立即切入紧急广播状态。

## 6. 安全管理平台

安全管理平台就像给各子系统装上“大脑”，使其具备“人脑思维”，成功代替人对视频画面进行24小时全年无休的监控和分析，并做出提前预警报警等动作。

### 6.1 系统基本功能

* 实时监控

通过实时监视功能，实现对监控网点全天候、全方位的视频监视功能。对监视目标进行实时、直观、清晰的监视，全天24小时均可观察到前端现场的监控状况。

* 录像回放

监控系统的建设除了实时监视和报警，防患未然外，还有一个重大的作用就是事发后有据可查，因此，录像的检索、连续流畅、多功能播放也是平台的一个很重要的功能。

* 视频巡查

平台可自定义危险区域，根据巡查时间及频率要求，对重点区域视频监控进行自动循环播放，实现自动视频巡查。

* 运动目标事件检测和分析

在摄像机监视的场景范围内，对出现的运动目标进行检测、分类及轨迹追踪，可应用于各种监控目的，如周界警戒及入侵检测、绊线检测、非法停车车辆检测等。可根据需要设置各种警戒要求，一旦系统检测到的运动目标及其行为符合预先设定的警戒条件，则自动产生报警信息。

在摄像机监视的场景范围内，对出现的运动目标进行监测、分类识别及轨迹追踪。可根据需要设置各种警戒要求，一旦系统监测到的运动目标及其行为符合预先设定的警戒条件，则自动产生报警信息。

* 运动物体流的统计

运动物体检测技术就是在视频场景内能找到和发现符合规格要求的运动物体。既然能找到该物体，从视频背景里面区分出来，就可以做到对该物体流的数量的统计。软件并且可以设定物体流经过的区域和流向来判断是否做为统计目标，就有非常广泛的应用。

* 周界警戒及入侵检测

在摄像机监视的场景范围内，可根据监控需要和目的设置警戒区域，系统可以自动检测入侵到警戒区域内的运动目标及其行为，一旦发现有满足预设警戒信息，并用告警框标示出进入警戒区的目标，同时标识出其运动轨迹。

* 广播管理

通过系统平台管理广播提供背景音乐、发布业务信息、寻呼以及强行插入包括泄洪预警、突发事故的紧急广播。

* 信息发布管理

通过安全管理平台可实现对信息发布平台的管理及操作。

### 6.2 报警功能

平台根据采集的视频，进行翻越行为智能分析。根据现场监控安装位置，在平台设置警戒线位置，平台自动检测从江堤翻越警戒线到江堤下方的行为，一旦发现人员翻越江堤护栏，平台自动进行翻越预警，提醒相关人员进行异常处置。



* 翻越报警管理

翻越报警管理提供翻越报警信息罗列和查询过滤操作。报警等级通过不停颜色进行区分，报警的信息包括处理状态、报警类型、时间、事件类型、报警设备、通道、报警等级。用户可以指定报警类型、时间段，对相关的设备进行报警信息的查询。

* 报警预案

平台支持添加，删除，修改报警预案；支持各种报警源（设备，监控点，报警输入点，智能通道）及对应的丰富报警事件类型；联动动作支持录像，邮件，短信，上墙（预录支持设置预录时间与录像时间）；支持报警预案的预览。

* 报警模板

平台支持系统报警类型与自定义报警类型（系统报警组合，方便配置）；支持批量设置报警时间间隔；支持批量关闭报警时间间隔；支持报警时间模板的创建，修改，复制，删除；支持单时间段与循环时间段；支持一个模板多个时间设置；支持时间设置的联动等级区分（分三等级）。

### 6.3 巡查管理

该模块主要依据现场终端定位技术，获取人员的实时位置数据。平台实时获取巡查人员手持终端定位数据，在平台展现定位分布与巡查路径。

控制中心使用平台端，对巡查人员位置分布、巡查轨迹进行监管查询，一旦发生异常情况时，可根据就近原则，进行现场人员调派。

巡查人员发现异常事件时，通过手持终端巡查记录功能，现场录屏拍照，将视频图像上传，证据留存。

* 人员分布

通过实时定位功能，在GIS地图上显示现场巡查人员位置分布情况。对未到工作岗位人员进行提醒和统计。

* 巡查轨迹

通过实时定位功能，结合巡查路径要求，对巡查人员巡查轨迹进行查询管理，监督人员潮前潮后重点巡查时间段是否按任务、按路径进行巡查。

* 证据留存

巡查人员发现异常事件时，通过手持终端巡查记录功能，现场录屏拍照，将视频图像上传，进行证据留存。控制中心人员通过证据留存管理，对现场情况进行分析研判。

### 6.4 各系统的联动功能

摄像头触发报警与广播系统的联动功能：如10号摄像头有人穿越警戒线，引起平台告警，同时触发10号摄像头处相邻的广播进行自动喊话（喊话次数可设置，喊话可根据时间段设置），若翻越人员返回可自动关闭广播；若自动喊话次数完成后，翻越人员仍未返回，管理人员可通过平台远程喊话，并可通过单兵系统通知现场巡查人员进行劝阻。

多人翻越后摄像头引起平台告警，如有一人返回，警戒线内还有人员未返回，告警及广播需持续提醒直至最后一人返回后，停止告警及广播。

### 6.5 数据统计报表分析功能

平台可按天/月/年/自定义时间等统计各摄像头触发报警次数，并输出报表分析，管理人员可根据报警次数情况对重点区域进行重点管理。

### 6.6 其他功能要求

安全管理平台需在兼容性方面需具备：

* 预留运营商短信通知功能，如江堤内3-5米划线，有人员穿越后通过短信提醒该人员功能。
* 安全管理平台与其他平台（如公安平台、雪亮工程平台、城市大脑平台等）的数据对接功能；提供开放的数据接口。

## 7. 网络安全等级保护要求

网络安全等级保护是国家网络安全保障的基本制度、基本策略、基本方法。在方案设计阶段，以《网络安全等级保护基本要求》、《网络安全等级保护安全设计技术要求》等国家标准文件，并结合行业特性要求、监管单位要求、用户提出的额外安全需求进行系统性方案设计。

本项目网络安全等级保护要求按照网络安全等级保护2.0三级标准建设。

### 7.1 机房安全要求

根据现有机房情况，需做以下改造：

* 水浸传感器（漏水测试绳）等漏水报警系统
* 烟感、温感，声光报警器。钢瓶式七氟丙烷气体灭火系统。
* 机房窗户最好密封，双层防护。
* 机房温湿度达到要求，需配置湿度调节器、温湿度仪表。
* 机柜需按要求接地。
* 关键设备实施电磁屏蔽。

### 7.2 网络安全要求

**移动互联安全扩展要求：**

* 入侵防范：应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。
* 边界防护：应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。
* 访问控制：无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。
* 入侵防范：a)应能够检测到非授权无线接入设备和非授权移动终端的接入行为；b）应能够检测到针对无线接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为；c）应能够检测到无线接入设备的SSID广播、WPS等高风险功能的开启状态；d）应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID广播、WEP认证等；e）应禁止多个AP使用同一个认证密钥；f）应能够阻断非授权无线接入设备或非授权移动终端。
* 移动终端管控：应保证移动终端安装、注册并运行终端管理客户端软件；移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程擦除等。
* 移动应用管控：应具有选择应用软件安装、运行的功能；应只允许指定证书签名的应用软件安装和运行；应具有软件白名单功能，应能根据白名单控制应用软件安装、运行。
* 移动应用软件采购：应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名；应保证移动终端安装、运行的应用软件由指定的开发者开发。
* 移动应用软件开发：应对移动业务应用软件开发者进行资格审查；应保证开发移动业务应用软件的签名证书合法性。
* 配置管理：应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别。

**物联网安全扩展要求（视频监控涉及，将感知节点设备通过互联网等网络连接起来构成的系统）**

* 感知节点设备物理防护：a)感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；b)感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；c)感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；d)关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）。
* 接入控制：应保证只有授权的感知节点可以接入。
* 入侵防范：应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。
* 感知节点设备安全：应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更；应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力；应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。
* 网关节点设备安全：a)应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力；b)应具备过滤非法节点和伪造节点所发送的数据的能力；c)授权用户应能够在设备使用过程中对关键密钥进行在线更新；d)授权用户应能够在设备使用过程中对关键配置参数进行在线更新。
* 抗数据重放：应能够鉴别数据的新鲜性，避免历史数据的重放攻击；应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。
* 数据融合处理：应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用。
* 感知节点管理：应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

### 7.3 网络安全设备

本项目配置等保一体机平台、入侵防御及安全管控中心设备。

**（1）等保一体机平台**

等保一体机硬件平台包括：下一代防火墙组件、SSL VPN组件、负载均衡组件、数据库审计组件、企业终端安全管理软件ESM、运维堡垒主机组件、日志审计系统组件、配置安全评估组件、上网行为管理组件等。

等保一体机硬件平台需支持软、硬件一体化与软硬件解耦两种部署方式；持网桥、路由、旁路模式部署。

等保一体机硬件平台基本要求：

* 平台包含下一代防火墙组件、SSL VPN组件、上网行为管理组件、数据库审计组件、运维审计组件、日志审计组件、主机杀毒等安全功能组件。

平台可根据实际业务环境定义业务安全区域，简化运维管理

* 在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑的编排，并且可以连接、开启、关闭虚拟网络设备。
* 平台可以展示详细主机状态、磁盘状态及应用状态，以及业务遭受的入侵风险、僵尸主机风险及外发流量异常等相关安全信息。
* 台支持模板化的组件部署模式，至少支持出口边界安全模板、等保合规安全模板。
* 支持内置的安全市场，可根据业务需要灵活选择所需要的安全产品。
* 支持故障迁移功能，当主机发生故障迁移后，可自动将组件迁移到其他主机上运行。
* 为了提供更好的排障手段，支持在平台内节点抓包分析分析功能，能够设置抓包的网口、过滤条件、文件大小等参数。
* 平台支持关键安全组件双机功能，保障安全组件高可用；在双机场景下，管理平台要支持双机配置同步，在硬件故障时保障无感知切换。

下一代防火墙功能要求：

* 支持静态路由，ECMP等价路由，支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议，支持多播路由协议，支持路由异常告警功能。
* 提供基本的安全防御，包括但不限于4-7层访问控制、入侵防御、病毒过滤、网页防篡改等安全功能。
* 对所有应用系统进行漏洞的攻击防护，包括防跨站、防SQL注入、防篡改、防木马、防黑客攻击等。
* 支持根据国家/地区来进行地域访问控制。
* 支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞。
* 可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则。
* 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。

SSL VPN功能要求：

* 支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务。
* 支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用。
* 支持用户登录界面、服务界面的完全自定义，上传单独的Web页面作为用户登录界面、服务界面。
* 支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证。
* 提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作。

上网行为管理功能要求：

* 支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限。
* 支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等。
* 必须支持以USB-Key方式验证接入数据中心的管理员身份；支持以USB-Key方式分配管理员的日志审计权限。
* 支持把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽，以及单用户最高带宽属性对外网IP有效。
* 支持基于访问行为的目标IP/IP组实现带宽划分与分配。
* 支持多种事件进行邮件告警，包括攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等。

数据库审计功能要求：

* 采用B/S管理方式。
* 支持多种数据库类型的审计，支持Oracle数据库审计、SQL-Server数据库审计、DB2数据库审计、MySQL数据库审计、Informix数据库审计、达梦数据库审计、人大金仓数据库审计、postgresql数据库审计、sysbase数据库审计、cache数据库。
* 支持白名单审计，系统使用审计白名单将非关注的内容进行过滤，不进行记录，降低了存储空间和无用信息的堆砌，白名单内容包括以下4个维度:SQL模板、业务系统、URL地址及数据库条件。
* 支持自动基线学习数据库语义语法，并支持提取参数自动生成SQL模板，可以减少审计日志的重复写入和节省磁盘的存储空间。
* 支持基于SQL命令的webshell检测，提供webshell日志查询；
* 可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现威胁。

运维审计功能要求：

* 内置配置管理员、密码管理员、审计管理员、系统管理员、系统审计员、普通运维用户等管理角色。
* 针对RDP、VNC、X11等图形终端操作的连接情况进行记录及审计；记录发生时间、发生地址、服务端IP、客户端IP、操作指令、返回信息、操作备注、客户端端口、服务器端口、运维用户帐号、运维用户姓名、审批用户帐号、审批用户姓名、服务器用户名等信息。
* 能够记录RDP协议中的活动窗口名称、删除文件等动作，并能记录RDP会话中的键盘输入信息。

日志审计功能要求：

* 系统能从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段。
* 对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义。
* 系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间地占用。

漏洞扫描功能要求：

* 主机类支持：windows、Unix、solaris、HP-Unix、AIX、 Linux等。
* 网络设备支持：华为、H3C、Cisco、Juniper、中兴等，防火墙：华为、天融信、H3C、Fortigate、Cisco、Juniper、迪普防火墙等。
* 数据库支持：Mysql、DB2、Oracle、Sqlserver、Sybase等，中间件：Tomcat、IIS、Webservices、Apache、Weblogic、Resin、Nginx等，虚拟化平台：VMware ESXi、VMware Center、XenServer。
* 支持扫描器登录到目标系统中对特定应用进行深入扫描。

**（2）安全管控中心**

根据网络安全要求，安全管控中心设备功能方面需具有：

* 提供CMDB功能，基于面向对象的思路，实现资产建模，建模内容包括属性建模，与关系约束建模。
* CMDB提供多种内置的资产模型与关系约束类型。资产模型覆盖以下属性字段：资产名称，资产编号，IP/URL，资产权属，资产类型，操作系统，用途，品牌，型号，维保，硬件配置等。关系约束类型覆盖放置、虚拟化、运行在、使用、包含、组成、连接等关系。
* 针对内置的资产模型，CMDB预置了各模型间的关系约束。
* 提供资产全生命周期管理功能，详细记录资产上线到报废过程中所有的管理、变更、配置等信息。
* 提供资产分组功能，用户可建立自定义分组，设定分组包含的资产，并按照分组对资产进行导航。
* 提供拖拽式拓扑绘制的功能，支持对绘制的节点进行分组，支持分组展开与折叠。
* 提供IP基准功能，建立基准表，绑定IP与MAC的映射关系，发现未授权的设备接入。
* 提供资产的硬件配置变动监测功能，并列表呈现所有的变动记录。
* 支持无代理采集，基于 ssh，snmp，syslog，jdbc，jmx，smi-s，ipmi，wmi等协议，对资产的动态数据进行采集，包括：性能数据、运行日志、告警等。采集任务的执行周期可配置。
* 实现对物理服务器的工况信息进行监控，可支持以下监控项：电压、风扇转速、电源状态、硬盘状态、机箱温度等。
* 实现对vmware虚拟机的监控，可支持以下指标的监控：CPU利用率、内存利用率、存储器信息、网口信息等。
* 实现对网络设备的监控，可支持以下监控项：总流速、收包率、接收流速、接收利用率、接收丢包率、接收错误率、发包率、发送流速、发送利用率、发送丢包率、发送错误率、CPU利用率、路由信息等。
* 实现对安全设备的监控，涵盖防火墙、堡垒机、IDS、IPS、WAF等，可支持以下监控项：总流速、收包率、接收流速、接收利用率、接收丢包率、接收错误率、发包率、发送流速、发送利用率、发送丢包率、发送错误率、CPU、内存利用率等。
* 实现对JVM堆内存、活动线程、HTTP线程、守护线程、峰值线程、启动线程的监控。
* 实现对存储设备/系统的监控，涵盖IP FC SAN、分布式NAS等存储服务器，可支持阵列、RAID 组和 LUN级别的监控，可支持以下监控项：总速率（字节、次数）、读速率（字节、次数）、写速率（字节、次数）、存储利用率、读写占比率等。
* 实现对操作系统，如 Windows、Linux、Unix 等系统的性能、容量、进程、连接、接口等进行监控，可支持以下监控项：系统运行时长、CPU利用率、内存利用率、分区使用情况、进程信息、虚拟内存利用率、磁盘IO速率等。
* 实现对关系数据库系统的监控，与自定义SQL查询等功能，涵盖MySQL、Oracle、MS SQL、DB2、Sybase、达梦等数据库，针对不同的数据库可支持相对应的监控指标项。
* 实现对Web/消息中间件的监控，涵盖Nginx、Tomcat、金蝶Apusic等，针对不同的中间件可支持相对应的监控指标项。
* 提供阈值告警功能，当指标项超出指定的阈值时，进行告警，当指标项回复到阈值范围内时，可自动解除告警状态。支持对连续出现的重复告警进行合并。
* 提供流程建模功能，支持拖拽式编排，支持多种控制逻辑，包括条件、跳转、并发、汇合，支持多人会签。
* 支持流程超时控制，用户可对处理节点设置处理时限，超过处理时限，自动通知催办。
* 提供可视化的流程跟踪界面，图形化呈现执行步骤，用户可直观查看流程的进展情况，以及各节点的处理记录与处理结果。
* 提供审计汇聚功能，支持其它外部系统审计数据汇聚和审计，审计汇聚接口采用syslog协议和sftp/ftp协议，方便对接。支持审计数据自动定时备份，以及备份恢复功能，防止审计信息丢失。
* 提供在线操作入口，所有的操作必须通过在线操作入口进行，从而对操作资产的行为进行管控与审计。由在线操作入口对所有的操作进行授权，只有获得授权，才能执行操作。
* 在线操作入口提供安全策略控制，限制对资产执行敏感命令。同时操作全程受到监控，平台会记录命令序列，并提供命令回放功能。
* 提供双因子登录认证，支持账号口令、短消息、动态口令等组合身份验证。支持多次认证失败自动锁定账号功能，及超时重新登录功能。
* 权限设置支持三权分立，系统管理员、审计管理员、安全管理员权限独立，避免一个用户权限最大没有制约给系统造成危害。
* 支持平台用户行为审计，记录登录用户在平台做的所有操作，包括：账号、时间、操作、操作结果等。
* 平台采用B/S架构，可兼容firefox与chrome浏览器。
* 平台的所有软件组件，均需支持分布式部署，支持负载均衡，与高可用。
* 平台的软件组件间采用低耦合设计，一个组件的变更或异常不影响其他组件的运行。

**（3）入侵防御**

入侵防御（IPS）设备的配置要求：

* 系统应为机架式独立IPS硬件设备，全内置封闭式结构。具有交流冗余电源模块，管理口≥2个，可检测流量≥8G，≥6个千兆电口。
* 为保证设备运行稳定性，系统须安装在专用的CF卡中，审计数据存储在磁盘中，防止操作系统故障导致审计数据丢失。

入侵防御（IPS）设备的检测能力要求：

* 检测深度：可以为用户提供2~7层深度入侵检测和阻断能力，不仅可以检测系统层面的攻击，还可以检测SQL注入、僵尸网络等多种常见的应用层面的攻击；备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS/IPS逃逸等多种技术，准确识别各种黑客入侵。
* 检测数量：入侵防御系统应具有较为全面的攻击检测能力，能够检测9000+为正偏离。包括操作系统漏洞利用防护，WEB漏洞利用防护，中间件、虚拟机、办公软件等类型的漏洞利用防护。
* 检测覆盖面：可协助检测网络异常行为，并可检测网络资源滥用流量；系统应提供SSL加密流量检测；系统支持IPV4/IPV6检测。
* 支持基于SCADA等工控协议的相关漏洞攻击检测。
* 流量分析：能够对经过IPS系统的网络流量进行分析并展示，可察看网络实时流量，包括：流量协议分布、流量IP分布、自定义察看某种流量TOP10、常见流量TOP10等。

入侵防御（IPS）设备的控制能力要求：

* 入侵威胁检测及防御：利用入侵防御系统内置的入侵规则库和病毒规则库可检测已知的网络入侵及病毒传播。
* 外联威胁检测及防御：当内部主机外联僵尸网络CC控制主机时能及时检测并阻断；当内部用户访问外部植入木马或被标记为恶意站点的网站时应能及时检测并阻断；要求IPS设备能与外部云端的恶意站点信誉库、僵尸网络信誉库进行联动检测，借助外部的威胁共享情报帮助单位及时发现更多的安全威胁。
* 支持识别某IP上登录的用户并将用户名关联在该IP触发的安全事件上；用户信息来源包括：邮件用户、文件传输、即时通信用户、远程登录用户、网站登录用户、数据库用户等。
* 系统应提供中英文网页过滤数据库，超过1,000万条的URL，多种精细分类（如不良言论、色情暴力、网络“钓鱼”、论坛聊天等），实现全面、高效的高风险、不良网站过滤。
* 系统应支持工作轨迹记录功能，记录管理员执行过的日志查询和报表生成结果，随时查看查询结果，无需再次执行复杂的配置过程，以减少日常维护工作量。
* 系统应具备地址簿功能，在报表中直观显示IP地址所处国家、地区或某个部门。支持自定义私有IP地址库。
* 系统应支持百万级病毒数量防护，支持流式防病毒、启发式防病毒（文件还原技术）检测和阻断。
* 未知威胁检测与控制：要求IPS设备不仅能检测已知威胁还具备未知威胁检测能力，具备与本地沙箱或云端沙箱的联动检测能力；能够展示沙箱检测文件的历史统计数据。
* APT检测与控制：要求对各类文件进行检测，包括音频视频类、程序类、文档类、脚本类等文件，提供界面截图证明，当检测到可疑文件时可传输到沙箱，确认是否为威胁文件。支持通过管理界面下载高级威胁分析日志样本供事件追查。
* 流量控制：为避免内网主机成为肉鸡后往外发送大量的FLOOD报文导致网络出口拥塞影响正常使用，要求IPS设备应具有传输速率控制方面的专业性技术。
* 异常外联控制：部署的入侵防御系统应能通过自学习机制，自学习所保护的信息系统的正常访问行为，并以此为基线检测出该信息系统的非法外联行为。
* 敏感文件外传控制：部署的入侵防御系统在检测到批量外传敏感文件时，应能及时告警或阻断。例如，可以通过IPS检测到在带有10个身份证账号的excel文件或带有20个手机号码的WORD文档外传时及时告警，可在IPS上根据需要设置告警阈值。
* 攻击源追踪：在发现某IP或某恶意文件对单位内信息系统产生影响时，可通过自动联动的云端信誉数据帮助判断是否为恶意文件、是否为恶意网址、是否为僵尸控制主机。
* 攻击源追踪：除以上攻击源自动跟踪能力，本项目中还可以为用户单位提供云端数据的查询权限，在发现单位内网络中某IP或某文件存在可疑行为时，可在云端情报库中查询该IP或该文件或该站点的历史犯罪记录，帮助单位判断该事件是否为风险点。

入侵防御（IPS）设备的集中监控能力要求：

* 应兼容本项目招标的态势感知（安全管理中心），支持将入侵防御系统的检测到的安全威胁发送到态势感知大数据平台，利用大数据平台感知整体的安全风险。
* 威胁监控：支持在管理界面显示活跃在单位网络中威胁情况：僵尸主机CC数量、病毒数、被攻击主机数、恶意文件数、高位入侵事件数等。
* 阻断情况监控：支持展示IPS阻断情况统计数据，包括恶意文件、恶意站点、僵尸网络、病毒传播。
* 趋势监控：可通过监控中心可按攻击源IP、攻击目的IP、攻击地理位置等维度按时间轴展示攻击趋势。
* 攻击排名及比例监控：支持通过友好的界面直观展示攻击排名及比例，包括攻击源地图分布情况及及比例、信誉防护事件比例。
* 设备硬件异常状态监控：可监控设备CPU温度，主板温度，风扇的转速。

入侵防御（IPS）设备的系统管理要求：

* 系统应支持独立式多路IPS工作模式，各路IPS相互独立，可单独配置策略。
* 系统应支持IPS和IDS的混合运行模式，同时提供入侵防护和入侵检测功能。
* 系统应提供策略模板，减少配置工作量，提高部署效率。
* 系统须支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略，为IPv6环境提供入侵防护。
* 解决远程应急管理的需求并提高系统自身的安全性，系统支持带外管理（OOB）功能，可以通过专用管理口，进行NIPS引擎管理。
* CDN场景下告警日志能够展示真实的源IP地址。
* 系统应支持A/S（A：Active，S：Standby）高可用部署方式，出现设备宕机、端口失效等故障时，完成主机和备机的即时切换，确保关键应用的持续正常运转。

入侵防御（IPS）设备的运维要求：

* 入侵防御系统应具备攻击快照功能，可详细记录触发告警的数据特征，以便做进一步的事件分析。
* 支持IPS设备回滚系统历史版本，即保留最近升级的多个历史版本于历史版本库中，在系统意外出错或升级错误后可根据备份的版本回滚到历史健康版本。
* 应支持“一键巡检”功能，可根据设备运行过程中反馈的数据进行全面分析，并生成图表相结合的安全报告。
* 应支持内置和内置Bypass，网络接口应具备内置fail-open特性，产品出现故障时，能自动转变成通路，不影响业务流量的正常传输。

## 8. 其他要求

### 81. 设备安装方面

室外摄像头、广播设备和LED屏的安装需要安全可靠，而且线路布置要求合理、整齐，远端机箱安装在警示牌下，安装标准为《通信系统用室外机柜安装设计规定》YD/T5186-2010。

### 8.2 电源引入方面

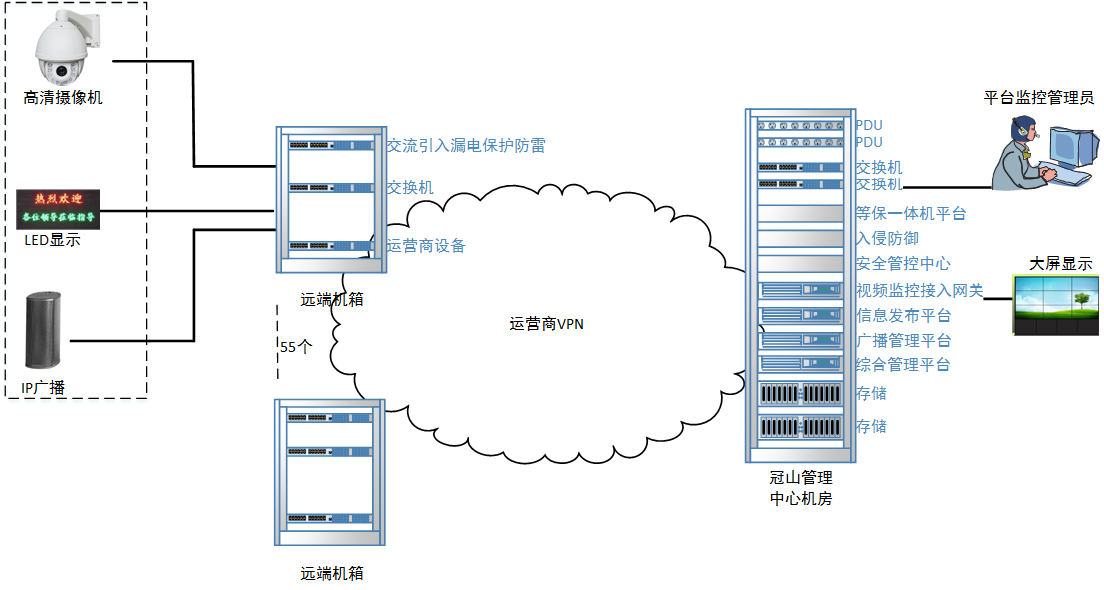
系统远端机箱电源就近引自景观照明配电箱，具体引入点由滨江区农业农村局在工程前协调。

### 8.3 防雷接地方面

室外摄像头、广播设备和LED屏都安装在位置较高处，因此在设备安装处以及机箱内需安装相应防雷器及做好可靠接地对其进行保护。

# 第三章 设备配置

## 1.网络详细拓扑



## 2.设备材料配置

本项目主要设备材料配置情况如下。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **参 数** | **数量** | **单位** |
| **一、监控监控系统** | | | | |
| 1 | 热成像双目球型摄像机 | 采用非制冷氧化钒焦平面探测器，探测器分辨率≥350\*250，热灵敏度NETD≤30mk 热成像镜头焦距25mm 防太阳灼伤功能：太阳直射热成像镜头5分钟后，热成像视频图像可在30分钟内恢复正常输出 可见光图像传感器：1/1.9英寸CMOS，总像素≥200万 ★可见光镜头焦距不低于35倍变倍 最低照度：彩色≤0.001lx、黑白≤0.0001lx 支持红外补光，补光距离不小于150m ★水平旋转角度：0°～360°连续旋转；垂直：-20°～90°。 ★水平最大速度≥200°/s，垂直最大速度≥40°/s 通过一个IP地址连接到设备，设备同时输出可见光和热成像两路视频图像 测温范围可达-40℃到750℃，测温规则支持点、线段、矩形、多边形、圆、椭圆测温规则 ★支持超温报警、温度变化趋势报警、温差报警 支持软件集成的开放式API，支持标准协议(ONVIF、GB28181、CGI) 基于可见光和热成像的智能算法，支持区域入侵、绊线入侵、物品移除、物品遗留、越界检测、进入/离开区域检测 ★支持IP地址、MAC地址白名单和黑名单功能，可添加不少于128个地址 ★支持多种供电模式，DC24V±15%、AC24V±15% 整机功耗≤50W； 工作温度：-40℃～+70℃； ★全密封防水设计，IP67防护等级及以上。 支持自动聚焦、强光抑制、透雾功能、电子防抖 支持雨刷功能 受到剧烈打击时,可通过客户端软件给出语音及文字报警提示并可弹出实时监视画面。 以上所有加★参数需提供公安部权威检测机构出具的整机产品检测报告，投标者须提供加盖了原厂投标章的检测报告复印件； | 15 | 个 |
| 2 | 热成像双目球型摄像机 | 采用非制冷氧化钒焦平面探测器，探测器分辨率≥350\*250，热灵敏度NETD≤30mk热成像镜头焦距35mm防太阳灼伤功能：太阳直射热成像镜头5分钟后，热成像视频图像可在30分钟内恢复正常输出可见光图像传感器：1/1.9英寸CMOS，总像素≥200万★可见光镜头焦距不低于35倍变倍最低照度：彩色≤0.001lx、黑白≤0.0001lx支持红外补光，补光距离不小于150m★水平旋转角度：0°～360°连续旋转；垂直：-20°～90°。★水平最大速度≥200°/s，垂直最大速度≥40°/s通过一个IP地址连接到设备，设备同时输出可见光和热成像两路视频图像测温范围可达-40℃到750℃，测温规则支持点、线段、矩形、多边形、圆、椭圆测温规则★支持超温报警、温度变化趋势报警、温差报警支持软件集成的开放式API，支持标准协议(ONVIF、GB28181、CGI)基于可见光和热成像的智能算法，支持区域入侵、绊线入侵、物品移除、物品遗留、越界检测、进入/离开区域检测★支持IP地址、MAC地址白名单和黑名单功能，可添加不少于128个地址★支持多种供电模式，DC24V±15%、AC24V±15%整机功耗≤50W；工作温度：-40℃～+70℃；★全密封防水设计，IP67防护等级及以上。支持自动聚焦、强光抑制、透雾功能、电子防抖支持雨刷功能受到剧烈打击时,可通过客户端软件给出语音及文字报警提示并可弹出实时监视画面。以上所有加★参数需提供公安部权威检测机构出具的整机产品检测报告，投标者须提供加盖了原厂投标章的检测报告复印件； | 41 | 个 |
| 3 | 热成像双目球型摄像机 | 采用非制冷氧化钒焦平面探测器，探测器分辨率≥350\*250，热灵敏度NETD≤30mk热成像镜头焦距50mm防太阳灼伤功能：太阳直射热成像镜头5分钟后，热成像视频图像可在30分钟内恢复正常输出可见光图像传感器：1/1.9英寸CMOS，总像素≥200万★可见光镜头焦距不低于35倍变倍最低照度：彩色≤0.001lx、黑白≤0.0001lx支持红外补光，补光距离不小于150m★水平旋转角度：0°～360°连续旋转；垂直：-20°～90°。★水平最大速度≥200°/s，垂直最大速度≥40°/s通过一个IP地址连接到设备，设备同时输出可见光和热成像两路视频图像测温范围可达-40℃到750℃，测温规则支持点、线段、矩形、多边形、圆、椭圆测温规则★支持超温报警、温度变化趋势报警、温差报警支持软件集成的开放式API，支持标准协议(ONVIF、GB28181、CGI)基于可见光和热成像的智能算法，支持区域入侵、绊线入侵、物品移除、物品遗留、越界检测、进入/离开区域检测★支持IP地址、MAC地址白名单和黑名单功能，可添加不少于128个地址★支持多种供电模式，DC24V±15%、AC24V±15%整机功耗≤50W；工作温度：-40℃～+70℃；★全密封防水设计，IP67防护等级及以上。支持自动聚焦、强光抑制、透雾功能、电子防抖支持雨刷功能受到剧烈打击时,可通过客户端软件给出语音及文字报警提示并可弹出实时监视画面。以上所有加★参数需提供公安部权威检测机构出具的整机产品检测报告，投标者须提供加盖了原厂投标章的检测报告复印件； | 5 | 个 |
| 4 | 视频综合平台 | 插卡式模块设计，可根据市场需求灵活配置；业务卡支持热插拔，可方便进行维护支持远程获取和配置参数，支持远程导出和导入参数产品要求为19"机架尺寸，≤14U高度机箱，提供≥10个板卡插槽，嵌入式系统，模块化设计，整机最大支持60路HDMI视频输出接口。★要求投标产品具有国家及公安部安全防范报警系统产品质量检测机构提供的检验检测报告，符合GA/T646-2016 安全防范视频监控矩阵设备通用技术要求（供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章）★支持双电源冗余。具有2组风扇，每组6个风扇（支持热插拔、冗余；支持吹和抽两种模式同时工作)。（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章）★投标设备主控及控制板至少具有1个VGA接口，不少于2个千兆网口、3个USB接口，4路RS232接口，1路RS485接口。支持报警手动消除功能。（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章）★支持多网口绑定，无需NAT功能，整机通过一个IP地址即可完成IP设备、模拟设备、SDI设备视音频数据的接入、转发和存储；（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章）★投标产品支持接入分辨率不小于8640×3840的视频。（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章）★电视墙支持单屏及拼接屏的1、4、6、8、9、12、16、25、32、36分割显示；支持视频切换流畅无黑屏现象，视频断开后保留最后一帧图像。（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章或投标专用章）★支持视频开窗、漫游、图层叠加功能，支持在底图上开窗漫游；单个输出端口具备≥64个窗口的开窗性能；单通道支持16个图层叠加，图层支持置顶或置底设置。（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章）支持接入网络键盘，进行云台操作、上墙控制。支持系统日志记录和查询，用户权限管理，支持录像查询、回放及下载。★要求设备支持字符叠加功能，最大支持20条，并可在任意位置叠加；支持多种自定义OSD样式，并且能够修改保存。（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章或投标专用章）要求设备支持多种信号输入接口：DVI、HDM、VGA输入板，4K采集板、BNC（单板至少32路，具备RS485）、HD-SDI、3G-SDI、同轴模拟高清输入板（单板至少8路）。要求设备支持多种信号输入接口：DVI、HDM、VGA输入板，4K采集板、BNC（单板至少32路，具备RS485）、HD-SDI、3G-SDI、同轴模拟高清输入板（单板至少8路）。投标产品支持H.265、H.264、MPEG4、MJPEG格式的视频解码 ,支持G.711、PCM等格式音频解码。（提供公安部权威检测机构出具的检测报告原件或复印件，并加盖原厂商公章）提供中国国家强制性产品认证证书（中国质量认证中心出具3C证明）。提供相关证书原件或复印件，并加盖原厂商公章或投标专用章。要求投标产品具有公安部权威检测机构出具的符合GBT28181标准的检测报告，提供检测报告复印件，并加盖原厂商公章或投标专用章。要求投标产品非OEM产品，控制软件需提供国家软件著作权登记证书原件或复印件。投标产品具备图像同步控制相关的发明专利（提供相应的专利证书复印件加盖原厂公章）控制设备符合GB/T24021-2001 idt ISO14021：1999 《环境管理 环境标志与申明 自我环境声明（II型环境标志）》的要求；提供CEC出具的认证证书； | 1 | 台 |
| 5 | 4路HDMI编码卡 | H.264/MPEG4；单板4路1080P，支持1080P/720P/UXGA/SXGA+/SXGA/XGA/SVGA/VGA分辨率 | 1 | 张 |
| 6 | 6路HDM解码卡 | 支持8路4096\*2160@25fps，8路3840\*2160@30fps ，32路1080p@30fps（H.264、H.265），72路720p@30fps，150路D1解码；支持8路1080P的SVAC解码；支持24路非标D1码流解码；1/4/6/8/9/16/25/36画面分割，自由分割 | 2 | 张 |
| 7 | 云存储数据存储节点 | 高性能多核CPU；整机标配32GB DDR4，最高可扩展至64GB；标配8个千兆电网口；标配一块2.5寸1TB机械硬盘，一块480GB SSD硬盘；前置2个USB2.0，后置2个USB3.0，1个eSATA接口；冗余电源，支持在线更换；支持24个2.5"或3.5"的SATA硬盘或者SAS硬盘，独立硬盘支架，支持硬盘热插拔。管理平台应支持对关键程序、关键数据、关键程序模块采取备份、冗余措施，有较强的容错和系统恢复能力，对管理平台整体性能有影响的关键设备宜支持负载均衡；（公安部检测报告体现）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，唯一IP地址对外提供存储服务，实现存储资源的统一管理和分配；可根据用户业务按需分配不同的存储空间和创建不同容量的资源池，支持灵活修改资源池的属性；支持对象存储，采用分布式文件系统，支持文件存储，采用纠删码或者多副本技术，读写过程不产生索引数据，不存在单独索引盘；管理节点集群模式时，可支持32个管理节点。管理节点和存储节点都为对等工作模式对外提供服务，支持管理节点的元数据多达64份多副本备份。支持集群容灾，在至少80%磁盘利用率下，最大容忍M台（N+M可设，比如：4+1，8+2，16+4等）节点同时故障（网络故障、断点、节点硬盘全部故障等情况），历史数据不丢失，数据全部完整，业务不中断；具备节点间容错能力下，容忍大于16台节点同时故障后，只要有1台以上节点正常，即可保证录像可写入，写入录像依然具备磁盘间容错能力；（公安部检测报告体现）内置分布式实时图片处理集群，支持自动负载均衡容错；支持多种图片类型，jpg、png、gif、bmp实时处理缩略和裁剪，实时处理性能每台节点不小于1000张/s，并支持线性扩展；提供图片格式转换支持配置存储池功能，存储空间虚拟化管理，多存储设备容量整合，形成录像池，支持自动配置存储池；支持异构存储节点隔离，分别划分到不同存储池；支持精简存储池配置，实现自动化存储池扩容；支持存储池级冗余，支持存储池级多副本及N+M数据冗余；支持存储池级别负载均衡；支持用户空间物理隔离，同一朵云内，为不同用户创建不同的存储池，使用不同的存储节点服务器；支持用户绑定使用特定存储池，根据用户业务分配通用、文件、视频、图片、语音、智能特征、结构化数据备份等类型存储空间，支持用户共享存储池；支持多用户、通道、权限和容量控制，在线弹性伸缩存储池的容量空间，不影响业务继续读写（公安部检测报告体现）云存储设备支持系统盘关键数据备份到数据盘中，并生成16份副本，系统盘更换或重装后，云存储软件自动从数据盘检索最新数据，恢复数据库、配置文件及路线索引文件，将系统盘恢复到故障前状态视频云平台安全系统，可通过HTTPS协议实现认证与会话控制、支持统一授权管理、角色权限管理、在线用户信息查看及用户在线签退等功能。（公安部检测报告体现）存储接入能力：单台存储节点支持5000路摄像机接入，同时支持500路视频点播支持时间轴展示智能目标密度，支持随着时间轴缩放动态展示目标密度；支持智能目标连续跳跃播放，支持智能目标逐帧正放，逐帧倒放，倍速播放，倒放；支持一个文件有多种N+M:b容错机制，能自适应调整N+M:b，系统根据当前节点情况自动配置使用哪种容错算法以达到最可靠的容错，以实现最大化节点容错能力接入管理平台的设备和用户，都需要进行必要的接入认证，以保证接入的安全性，通过https协议加密传输信息（公安部检测报告体现）支持针对实时报警方式的自定义SQL处理，单节点支持实时处理性能不低于10万条/秒按需弹性扩容，仅需添加新增存储节点IP地址，无需配置RAID。扩容过程无需RAID，LVM等配置，一分钟之内完成。支持X86和GPU服务器的硬件虚拟化，作为资源池统一管理，支持节点标签设置，支持服务容器异常迁移，支持节点调度的开关控制（公安部检测报告体现）★支持网络故障自动发现和隔离，在1秒内感知到故障节点，1秒内进行隔离，提升系统可靠性；支持回收站功能，防止数据误删，支持回收时间配置；（公安部检测报告证明）★支持服务日志采集、展示、搜索，支持日志告警、告警趋势分析，可根据日志完成服务链路的追踪分析（公安部检测报告证明） | 2 | 台 |
| 8 | 硬盘 | 4000G；7200RPM；128M；SATA | 48 | 个 |
| 9 | 交换机 | 室外宽温交换机，4\* 10/100M，1\*100/1000M RJ45电口，1\*1000MSFP光口，工作温度： -40℃～+75℃，DC12V\1A | 44 | 个 |
| 10 | 交换机 | 室外宽温交换机，8\* 10/100M，1\*100/1000M RJ45电口，1\*1000MSFP光口，工作温度：-40℃~+75℃，DC12V\1A | 11 | 个 |
| **二、信息发布系统** | | | | |
| 1 | 双基色屏 | P4.75双基色屏 像素间距：4.75mm 像素密度：44321点/㎡ 亮度：≥500cd/㎡ 视角：≥120° 峰值功耗：≤500W/㎡ 总尺寸：1600mm×320mm 显示尺寸:1525mm×305mm 含配套控制卡、转接板、开关电源、线材等" | 55 | 套 |
| 2 | 户外全彩常规屏 | P4，1.35㎡一套（3072\*2048) 像素间距：≤ 4mm；使用环境：室外； 像素密度：≥ 62500 pixels/m2； 亮度均匀性≥98%； 模组间缝隙≤0.03mm，水平视角≥170°，垂直视角≥170°； 通过抗拉力5000N和抗压力50000N测试； 刷新率支持1920~4800Hz可调； 低亮高灰性能：100%亮度时，16bits 灰度；20%亮度时，12bits 灰度； 平均无故障工作时间≥100000小时，故障平均修复时间MTTR不超过10分钟； 平均功率≤150W/m²，峰值功率≤400W/m² 设备具有防潮、防虫、防腐蚀、防尘、防静电、防燃烧、防电磁干扰等功能，并具有过流、短路、过压、欠压保护和抗震抗风的功能； 显示单元具备3C证书； 为保证产品屏体的稳定性，需提供国家级检测机构出具的户外屏IP65防护等级证书或者提供国家级权威机构出具的LED户外显示屏具备防雨前维修技术证书复印件。 ★显示屏生产厂家服务能力符合国家标准《商品售后服务评价体系》GB/T27922-2011，且能力达到五星级；（提供相关证书） ★为了保证产品使用稳定性，其LED显示屏具备一种驱动电路板保护电路技术，提供国家级权威机构出具的证书复印件 | 5 | 套 |
| 3 | 联网信息发布平台 | Windows Server 2008 ； Intel Xeon 3106 1.7G 9.6UPI 11M 8C 85W\*1 ；16GB DDR4 2666 REG内存\*1 ；1T 3.5吋 7200转 6Gb SATA热插拔硬盘\*2 ；4个千兆网口 ； 1+1冗余电源 ；1U；导轨具备完善的现代化信息采集、信息处理、信息发布、决策管理和指挥调度的统一信息平台。 | 2 | 台 |
| **三、公共广播系统** | | | | |
| 1 | 网络化广播中心 | 管理服务器软件平台、智能寻呼站、受控调谐器、播放机、音频采 | 1 | 套 |
| 2 | 远端室外有源IP音箱及功放 | 远端室外有源IP音箱及功放，扬声器要求声音传播距离200-300米（达到滨江区海塘17公里全覆盖） | 55 | 套 |
| **四、管理平台** | | | | |
| 1 | 安全管理平台 | 实时监控 "支持1/4/6/8/9/13/16/20/25/36/64多分屏画面显示，并支持自定义画面分割，根据用户需要自由选择，支持画面比例调整：满屏，1:1,16:9,4:3,5:4,4:5,3:4,9:16及64:9"业务组织 支持自定义业务树，可生成多种组织结构业务树，可任意调整通道等节点的排列顺序电子地图展示动环，支持动环实时信息展示及报警通知支持录像回放上墙支持秒级存储及回放，确保可回放设备断网/断电前一秒录像即时回放，支持在实时画面回放前30s录像，并可单帧前进或后退录像，也可以保存此段录像★支持当前配置的广播任务展示（以公安部检验报告为准）具有视频质量诊断功能，能够分析图像的亮度、偏色、对比度、清晰度、视频丢失等属性，并图形化展示统计结果支持接受并统计行为分析、人数统计、人脸检测、全景拼接服务器数据对接进行实际应用支持接入管理云存储设备★支持当前配置信息发布任务展示（以公安部检验报告为准）。支持淡忘存储，将指定天数的录像进行抽帧存储子系统管理，支持将子系统分成独立模块，通过加密狗对子系统进行授权控制。支持自定义调整模块的尺寸和位置★数据概览功能，支持系统评分、评级，对设备在线率、服务器在线率、中心服务器资源使用情况、存储异常、设备报警及服务器报警等状态综合评分支持最近登录用户展示，显示当前在线人数及在线率支持当前新闻公告展示支持当前报警日志展示支持设备在线率的统计，统计IPC、存储设备、解码资源及报警主机的在线率并以图表形式展示支持动环实时数据统计，并能以折线图、柱形图形式展现支持动环外设报警率统计，能显当前外设正常、报警及总数目支持当前配置的广播任务展示支持当前配置信息发布任务展示支持根据用户自定义配置业务数据的展示，并能调整模块位置转发&存储性能多址模式： 码流接入：800Mbps码流转发：800Mbps绑定模式： 码流接入：1500Mbps 码流转发：1500Mbps多址模式：码流存储：800Mbps绑定模式：码流存储：1500Mbps以上所有加★参数需提供公安部权威检测机构出具的整机产品检测报告，投标者须提供加盖了原厂投标章的检测报告复印件； | 1 | 套 |
| 2 | 平台软件开发 | 摄像头触发报警与广播系统的联动功能；巡查人员管理功能等开发 | 1 | 套 |
| 3 | 视频监控设备接入网关服务器 | 嵌入式Windows 7 ；Intel Xeon E3-1230 v5；8G DDR4；1T 3.5吋 7200转 6Gb SATA硬盘；2个千兆；显示屏无；单电源；250W；1U机架式 集成第三方编码设备的SDK、以及GB28181、Onvif等标准协议，实现与第三方设备的通信，从而快速、稳定地将第三方设备接入平台，以较好的兼容性解决平台软件和第三方设备间互联互通的问题 | 1 | 个 |
| 4 | 手持移动终端 | 内置4核1.3G的CPU,2GB RAM+32GB Flash1300万背照式摄像头支持1路外置摄像机，最高支持1080P4.02英寸工业触摸屏，分辨率854x480支持屏幕亮度自动调节支持扩展1张TF卡，最大支持256G支持4G全网通、北斗/GPS双+A25:E29模，WIFI、蓝牙支持一键录像、一键录音、一键拍照，一键报警支持PTT功能支持按压式指纹识别支持车牌识别1080P/10h，720P/11h超长使用时间★设备支持IP67防水防尘等级 | 25 | 台 |
| 5 | 全千兆网管交换机 | 室内宽温全千兆网管交换机，24\*10/100/1000Base-T，4个1000Base-X SFP光口(COMBO)，无风扇自然散热、防尘设计，工作温度：-25-55°，适用室内非标准机房应用 | 1 | 个 |
| 6 | 操作终端电脑 |  | 1 | 台 |
| 7 | UPS | 10KVA在线式不间断电源UPS杋房断电延时4小时10KVA，12V120AH电 | 1 | 套 |
| **五、配套设备材料** | | | | |
| 1 | 19英寸机柜 | 2000\*600\*1000,2块交流PDU，≥8位/块 | 1 | 架 |
| 2 | 远端机箱 | 配置PDU、漏电保护及防雷模块 | 55 | 只 |
| 3 | 交流电缆 | 室外交流电力电缆3\*10mm2 | 13000 | 米 |
| 4 | 交流电缆 | 室外交流电力电缆3\*2.5mm2 | 1100 | 米 |
| 5 | PVC管 |  | 14000 | 米 |
| 6 | 双绞线缆 | 室外超五类非屏蔽双绞线 | 15 | 箱 |
| 7 | 摄像机支撑件 |  | 61 | 根 |
| 8 | 辅助材料 |  | 55 | 套 |
| 9 | 机房配套材料 | 接地、烟感、水浸、监控（1个200万高清红外摄像半球机）等 | 1 | 套 |
| **六、网络安全设备** | | | | |
| 1 | 等保一体机硬件平台 | 下一代防火墙组件工作模式：支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备；支持静态路由、策略路由、RIP、OSPF、ISP路由，其中ISP路由支持自定义，并可提供基于应用的策略路由，提供web配置界面截图；接口默认属于root，创建VRF后可把接口添加到VRF内，一个接口只能属于一个VRF；支持针对Web服务器防护，包括网页防爬虫、网页防篡改、HTTPS防护、DDoS攻击防护、Web攻击过滤、漏洞防护等（提供产品截图或官方技术说明文档）；不同vrf下的接口可以配置相同的ip地址；接口实际配置支持second IP地址，每个接口要求支持至少200个second IP（提供产品截图或官方技术说明文档）；支持针对Web服务器防护，包括网页防爬虫、网页防篡改、HTTPS防护、DDoS攻击防护、Web攻击过滤、漏洞防护等（提供产品截图或官方技术说明文档）；支持IPSecVPN接入，支持DES、3DES、AES等加密算法（提供产品截图或官方技术说明文档）；IPsec VPN支持第三方对接和快速配置，自有设备对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址，支持配置国密，（提供Web界面配置截图）；支持自定义URL过滤，并支持URL的模糊匹配（提供Web界面配置截图）；支持审计HTTPS加密邮箱，支持审计主题、内容、附件等，支持本地下载邮件原件；支持本地认证、Portal认证、Radius认证、LDAP认证、免认证；支持对接IMC、AAS、SAM、ACMP等常见AAA服务器；支持配置强制重新认证间隔，支持设置认证无感知间隔，支持配置认证通过后重定向URL，提供以上功能web界面配置截图；支持三权管理方式，包括权限管理员、账号管理员、审核官和管理员，各管理员权限制约；权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限云堡垒机子模块：运维审计系统的操作系统版本不得低于CentOS6.5；★支持与get、post、soap发送方式的http短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动（须提供相关截图证明并加盖原厂公章）；支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令。（须提供相关截图证明并加盖原厂公章）；★基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证（须提供相关截图证明并加盖原厂公章）；支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机。（须提供相关截图证明并加盖原厂公章）；IE代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码（需提供国家权威机构证明并加盖原厂公章）；★支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备；★支持在mac电脑里使用navicat工具通过堡垒机登录mysql、oracle等数据库服务器；支持保存SFTP/FTP传输的原始文件（提供第三方权威机构检测报告证明及功能截图）；支持运维空闲会话时间全局设置限制功能（需提供功能截图证明并加盖原厂公章）云综合日志审计子模块：产品获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具产品检验报告。所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》，并提供完整的检测报告复印件（行标三级）；独立完成审计日志采集，不依赖于设备或系统自身的日志系统；审计工作不影响被审计对象的性能、稳定性或日常管理流程审计结果存储于独立存储空间；自身用户管理与设备或主机的管理、使用、权限无关联；提供全中文WEB管理界面，无需安装任意客户端软件或插件；采用解决方案包上传对产品进行功能扩展，无需要代码开发。（提供截图并加盖公司公章）；支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能。（提供截图并加盖公司公章）；支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器。（提供截图并加盖公司公章）；支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器。（提供截图并加盖公司公章）；具备安全评估模型，评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。（提供截图并加盖公司公章）；支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以CVE、Bugtraq、OWASP公开协议和标准为为基础（提供第三方检测报告）；性能监控：通过在目标主机上安装agent程序，支持监控目标主机的CPU利用率、内存使用率、磁盘使用情况、流量、进程数等信息，并支持设置报警阈值。（提供第三方检测报告） | 1 | 套 |
| 2 | 入侵防御 | 硬件指标：标准2U专用万兆硬件平台，内置交流双电源，硬盘≥1T支持IPv4/6抗应用型DOS攻击防护，如HTTP Flood、DNS query flood等攻击防护;支持抗流量型攻击防护，如syn flood、udp flood、icmp flood，tcp flood等攻击防护；抗常见DOS攻击防护，jolt2、land\_base、ping\_of\_death syn flag、 tear\_drop 、winnuke 、smurf、 ip spoof等；支持IP-MAC绑定，支持对防火墙自身DOS防护和防止扫描功能产品资质具备公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证（增强级）》具备中国信息安全认证中心颁发的《中国国家信息安全产品认证证书（增强级）》具备中国国家版权局颁布的《计算机软件著作权证书》具备国家保密科技测评中心颁布的《涉密信息系统产品检测证书》具备全球IPv6测试中颁布的《IPv6 Ready Phase 2证书》 | 1 | 套 |
| 3 | 安全管控中心 | 安全管理平台：要求云安全管理平台和被管理的每个安全产品模块拥有独立的销售许可证书，必须带『云安全』名字；要求安全管理平台具备CSA云安全CAS CSTR（增强级）证书；要求安全管理平台需具备国家信息安全漏洞库CNNVD兼容性资质证书 数据库审计模块： 支持在目标数据库安装agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计，提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告；支持大数据平台部署，具有成熟的大数据hadoop平台处理，支持后期无缝扩展大数据版本，支持审计数据外送至大数据平台，检索性能高达100亿数据仅需6-8秒，存储数据量高达3000亿以上；（需提供大数据合同关键页面复印件）；支持对SQLserver 2005以上版本采用通讯加密的数据库，可以导入证书的方式实现审计解密；（需提供功能截图并盖原厂公章，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）；★支持数据库请求和返回的双向审计，支持返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小； (提供功能截图证明并盖原厂公章，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告)  综合漏洞扫描子模块 ：支持按照用户需求自动部署在安全资源池虚拟机上，支持按需获取安全资源池的虚拟计算资源、存储资源、网络资源等实现自动化部署；提供扫描操作日志自动审计功能，用户可以根据操作内容、操作账户、操作IP、操作开始时间、操作结束时间等自定义日志审计规则。并将审计结果发送到指定邮箱当中，用户可自定义审计结果发送的频率和时间；支持识别国内外主流Web应用防火墙品牌（提供产品截图）； ★产品具备国家信息安全漏洞库《兼容性资质证书》。提供有效证书的复印件 | 1 | 套 |

**备注说明：各设备要求详见本项目建设方案设计要求。**

**为确保产品实际质量及性能满足需求，在签订采购合同前将按招标要求对中标产品功能进行一一测试，测试相关费用由投标方承担，若中标产品未通过测试，将取消中标资格并追求相应责任。**