亳州芜湖现代产业园区智慧亳芜

智慧消防信息化服务项目方案

**2024年5月**

目录

第一章 项目概述 1

1.1 项目建设背景 1

1.2 建设必要性 2

1.3 编制依据 2

1.3.1 政策法规 2

1.3.2 标准和规范 3

1.3.3 其他编制依据 4

1.4 建设内容 4

1.4.1 消防安全检测 4

1.4.2 消防安全物联网建设 4

1.4.3 完善智慧消防平台功能 4

1.4.4 智慧消防运营服务 5

1.4.5 智慧亳芜相关扩容 5

1.5 项目总投资及资金来源 5

第二章 现状分析 6

2.1 业务现状 6

2.2 业务应用系统现状分析 6

2.3 可用资源现状 6

2.4 重点单位消防管理现状 6

第三章 需求分析 7

3.1 业务需求 7

3.1.1 重点单位的消防安全检测需求 7

3.1.2 全面接入的消防安全感知需求 7

3.1.3 智慧消防平台功能升级需求 7

3.1.4 智慧消防运营服务需求 7

3.2 存储需求 8

3.3 网络建设和部署需求 8

3.4 安全需求 9

3.5 性能需求 9

3.6 业务协同需求 10

第四章 建设内容 11

4.1 设计原则 11

4.2 建设目标 11

4.3 设计思路 12

4.4 总体框架 13

4.5 建设方案 14

4.5.1 重点单位消防安全检测 14

4.5.2 智慧消防安全物联网 24

4.5.3 智慧消防平台功能升级 31

4.5.4 智慧消防运营服务 32

4.6 系统安全 34

4.6.1 系统安全基础设施建设方案 34

4.6.2 设计规范 43

第五章 项目投资概算 45

5.1 资金来源与落实情况 45

5.2 软件开发费用 45

5.3 专业设备、网络、服务及施工概算 47

5.4 其它预算 53

第六章 项目管理 55

6.1 项目管理体系 55

6.1.1 领导和管理机构 55

6.1.2 项目实施机构 56

6.1.3 人员配置计划 56

6.1.4 人员培训方案 56

6.2 项目建设周期 57

6.3 项目进度计划 58

6.4 质量管理与控制 58

6.5 风险分析与管理 59

6.5.1 风险识别与分析 59

6.5.2 风险对策与管理 60

6.6 运行维护方案 61

6.6.1 运维管理规范 61

6.6.2 运维服务内容 61

6.6.3 运维服务提供方式 62

6.6.4 运维服务工作量估算 62

6.6.5 应急措施 63

第七章 效益分析 69

7.1 经济效益 69

7.2 社会效益 69

# 项目概述

## 项目建设背景

近年来，全国范围内重特大事故时有发生，造成了重大的人员伤亡和财产损失，消防救援队伍面临的任务愈发艰巨，迫切需要信息化手段提供更加有力的支撑和服务。消防“十四五”规划中明确提出了消防信息化的重点任务，包括创新社会消防安全治理与服务、推进移动警务应用、健全应急通信体系、优化系统架构、拓展基础网络、完善硬件基础、完善业务功能和基础数据库及健全保障技术体系。

2017年10月10日，公消〔2017〕297号文件《关于全面推进“智慧消防”建设的指导意见》指出后期消防信息化建设的目标，要求各省、市需按照《消防信息化“十四五”总体规划》要求，综合运用物联网、云计算、大数据、移动互联网等新兴信息技术，加快推进“智慧消防”建设，全面促进信息化与消防业务工作的深度融合，为构建立体化、全覆盖的社会火灾防控体系，打造符合实战要求的现代消防警务勤务机制提供有力支撑，全面提升社会火灾防控能力、队伍灭火应急救援能力和队伍管理水平，实现“传统消防”向“现代消防”的转变。指导意见明确指出了今后几年内各省市消防信息化建设的原则、目标、内容、工作重点和完成任务指标、时间指标，为消防信息化建设提供了有利的政策支撑和指导。

2019年5月，中共中央和国务院联合印发了《关于深化消防执法改革的意见》，提出了消防执法改革的5个方面12项主要任务(5+12)；在加强事中事后监管方面：完善“互联网+监管”，运用物联网和大数据技术，实时化、智能化评估消防安全风险，实现精准监管。

2019年12月，应急管理部《关于推进全国智慧消防建设的提案》的回函中提到，将进一步提升消防工作信息化、科技化、智能化水平，更好地适应火灾防控新形势、新挑战。积极建设智慧消防大数据平台和物联网系统，整合各地智慧消防系统资源，统一关键数据接口标准，明确系统建设协议开放要求，共享各地数据资源，建立完善各级火灾防控大数据管理平台。进一步指导和支持地方推进智慧消防建设。督促各地充分应用远程监控、温度传感器、火灾烟雾监测、水压监测、电气火灾监测等感知设备，拓展消防设施、防火巡查自检工作的监测感知覆盖范围，通过消防安全移动互联网、物联网、消防管理APP等建设应用，实现信息采集自动化、汇聚智能化，提升消防安全信息化监管和风险预测预警能力。

综上所述，根据国家的战略和指导意见，借鉴部分地市的先进经验，结合亳芜智慧园区的前期建设基础，在经过调研和论证的前提下，我们提出了整合现有资源，创新服务模式，在把握总体规划、统一部署、因地制宜、分步实施的建设原则的前提下，完善园区广覆盖、多元共治的火灾预警防控体系。

## 建设必要性

消防安全关系到百姓生命财产安全、城市形象、社会稳定等众多方面，随着社会、经济的不断发展，现有的管理手段已无法满足实际工作需要，创新消防管理模式，实现防控自动化、执法规范化、救援指挥智能化、日常管理精细化、全程可视化，实现智慧防控、协调作战、智慧执法、智慧管理，全面推动消防工作向信息化、智能化、智慧化方向发展是现代化消防业务发展的新趋势和新要求。

智慧化是当今消防发展的趋势和潮流，大力推进信息化，是消防现代化建设的战略举措和破解发展难题的重要手段。物联网、云计算、大数据、人工智能、移动互联网等新兴信息技术日新月异的发展，为消防信息化发展带来了新技术、新方法。通过新技术的应用，消防信息被全面感知、共享开放，可具有预警预测、分析研判、辅助指挥决策的功能，实现实时、动态、互动、融合的消防信息采集，传递和处理，全面促进与提高消防监督与管理水平，提升消防管理智能化、社会化水平。

## 编制依据

### 政策法规

（1）《中华人民共和国安全生产法》（主席令〔2014〕13号）；

（2）《中华人民共和国网络安全法》（主席令〔2016〕53号）

（3）《公安机关互联网安全监督检查规定》公安部令第151号

（4）《中华人民共和国消防法》（主席令〔2018〕6号）；

（5）《安全生产许可证条例》（国务院令第397号）；

（6）《国务院关于特大安全事故行政责任追究的规定》（国务院令302号）；

（7）《消防安全责任制实施办法》；

（8）国务院《关于积极推进“互联网+”行动的指导意见》；

（9）国务院《关于印发促进大数据发展行动纲要的通知》；

（10）国务院办公厅《关于运用大数据加强对市场主体服务和监管的若干意见》；

（11）国务院《国务院关于加强和改进消防工作的意见》；

（12）中共中央办公厅、国务院办公厅《关于深化消防执法改革的意见》；

### 标准和规范

（1）《电子政务术语》（GB/T 25647-2010）；

（2）《信息安全技术 术语》（GB/T 25069-2010）；

（3）《IT网络安全 第1部分：网络安全管理》（GB/T 25068.1-2012）；

（4）《IT网络安全 第2部分：网络安全体系结构》（GB/T 25068.2-2012）；

（5）《IT网络安全 第3部分：使用安全网关的网间通信安全保护》（GB/T 25068.3-2010）；

（6）《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）

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

（8）《信息安全技术网络安全等级保护测试评要求》（GB/T 28448-2019）

（9）《信息安全技术网络安全等级保护设计技术要求》（GB/T 25070-2019）

（10）《安全生产信息资源目录体系第1部分：总体框架》；

（11）《安全生产信息资源目录体系第2部分：技术要求》；

（12）《安全生产信息资源目录体系第3部分：核心元数据》；

（13）《安全生产信息资源目录体系第4部分：信息资源分类》；

（14）《安全生产信息资源目录体系第5部分：信息资源标识符编码方案》；

（15）《安全生产信息资源目录体系第6部分：技术管理要求》；

（16）《消防信息代码》（GA/T 974-2011）；

（17）《消防基础数据平台接口规范》（GA/T 1036-2012）；

（18）《消防公共服务平台技术规范》（GA/T 1038-2012）。

### 其他编制依据

（1）《中华人民共和国国民经济和社会发展第十四个五年规划纲要》；

（2）《“十四五”国家综合防灾减灾规划》；

（3） 亳州市国民经济和社会发展第十四个五年规划纲要；

（4） 应急管理部《应急管理信息化发展战略规划框架》；

（5）《消防救援队伍信息化发展规划（2019~2022）》；

（6）《关于全面推进“智慧消防”建设的指导意见》；

（7）应急管理部消防救援局关于印发《消防救援局2019年工作要点》的通知应急消〔2018〕53号。

## 建设内容

本期围绕消防安全检测、消防安全物联网建设、智慧消防平台功能升级、消防安全监测运营服务进行建设，建设内容如下：

### 消防安全检测

针对亳芜园区内消防重点单位开展消防设施检测，出具《安徽省建筑消防设施检测报告》，对检测不合格的单位出具问题清单及整改意见，待整改完成后再次检测排查问题、出具检测报告。

### 消防安全物联网建设

针对亳芜园区内未接入消防安全物联网系统的单位，接入单位消防报警主机、消防水系统、电气火灾、火灾烟雾、消控室人员在岗监测、应急通道占用监测等状态数据，统一接入在智慧园区二期智慧消防平台内展示、统计，采集点位信息并标注，建立各单位消防电子档案，部署企业级消防安全物联网应用。对于在建工地单位，采购消防物联网设备，待完工后由中标单位安装实施。

### 完善智慧消防平台功能

拓展智慧消防平台功能，实现维保业务管理、安消联动、运营数据日志分析等功能拓展；完善原有系统功能，优化系统界面；开发视频存储功能，支持消控室监控视频存储不低于2周。

### 智慧消防运营服务

参照智慧园区二期建设模式，引入智慧消防运营服务，将本期新增联网的单位消防设施设备运行状态数据和告警数据接入运营中心，及时响应火灾预警、消除火灾隐患。

**1.4.5 智慧亳芜相关扩容**

完善智慧工地模块相关功能与算法解析能力。

## 项目总投资及资金来源

本项目预算资金为333.60万元，由亳芜现代产业园区管委会支出。

# 现状分析

## 业务现状

亳芜产业园管委会承担着园区安全综合监管职责，其主要业务如下：

1、履行消防安全监督管理职能。通过监督执法，强化企业单位消防安全主体责任落实，有效消除各类消防安全隐患问题，纠治各类消防安全违法行为，发现并推动化解重大消防安全风险，提高社会面火灾防控整体水平。

2、综合统筹行业、领域、系统消防安全责任落实。通过落实相关法律法规、政策标准和技术规范等措施，推动各行业、领域、系统消防安全责任落实，规范其消防安全管理，并依托考核、督导、督办等措施手段，推动政府、部门落实法定消防安全责任和必要的火灾预防工作措施。

3、推动落实消防安全基础设施建设保障。以编制落实消防事业发展规划为抓手，组织指导各级政府、部门落实消防安全基础设施建设保障工作，按照法定职责任务，组织各有关部门落实消防安全基础设施的维护、保养，不断强化社会面火灾预防的硬件基础。

## 业务应用系统现状分析

目前，亳芜产业园已建成智慧园区一期、二期系统，其中智慧消防平台已接入园区内38家重点单位消防物联网数据，并通过消防安全运营服务降低安全风险。园区内尚未完成单位全部联网接入，亟待消防安全物联网全覆盖监测。

## 可用资源现状

本项目依托亳州市政务云资源建设部署，政务云平台提供存储资源、计算资源、云安全服务和网络基础设施。

## 重点单位消防管理现状

经现场勘查发现消防重点单位存在消防设施设备状态异常、消防通道堵塞、消防安全巡查落实不到位、消防台账不清等问题。

# 需求分析

## 业务需求

### 重点单位的消防安全检测需求

需安排专业检测团队按照国家相关消防法规标准为采购人提供建筑消防设施年度检测，并出具《消防设施检测报告》；根据消防设施检测报告，督促各单位限时完成消防隐患整改和消防设施设备修复；检测机构再次开展消防检测并出具报告，消防安全监管部门根据第二次检测报告开展相关检查工作。

### 全面接入的消防安全感知需求

按照火灾预警防控需求，利用物联感知手段，接入园区内未联网的单位消防设施设备运行状态，实时动态感知。通过“物联网+运营”的建设模式，加强对人流、物流聚集的重点场所、区域的消防安全管控，综合提升园区安全治理水平。

该项目消防安全物联感知设备接入消防安全监测预警系统、“城市大脑”。

### 智慧消防平台功能升级需求

基于前期智慧消防平台，需要拓展隐患整改分析、设备离线分析、安全周报、维保业务管理、安消联动、运营数据日志、运营记录分析等平台功能；完善原有系统功能，优化系统界面。

另外根据业务需求，感知网络数据统一进入消防大脑，以推动消防救援大数据的有效应用，同步在消防安全监测预警系统上增加维保计划管理、维保监管、维保任务提醒等功能。

本次升级为在前期智慧亳芜平台基础上进行实施，须与现有系统和硬件做好兼容对接。

### 智慧消防运营服务需求

持续构建园区监管平台、运营中心、企业三级级物联感知接入架构，接入智慧消防物联监测系统、消防远程监控系统、智慧用电系统等安全监测数据，支撑火灾隐患预警分析、火警及时响应侦查。

针对辖区内海量传感器、网关等感知资源，面向其长时间持续高效稳定运行的需求，通过准确掌握各类感知资源的状态，对感知资源进行科学组织，准确控制其入网、在网和离网等各个环节，实现对消防安全感知网络所包括的各类感知终端及相关感知资源的有效管理，为各项上层业务持续高效开展提供管理保障。

## 存储需求

系统建设数据存储需求估算如下表所示。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统名称** | **子系统** | **年数据量（TB）** |
| 1 | 感知网络 | 预计第一年接入100万个传感器，按每个传感器年数据量约1MB（清洗后） | 1 |
| 2 | 智慧消防服务平台功能升级 | 资源管理、日志分析、运营记录等数据 | 2 |
| 3 | 视频存储 | 已建和本次建设中的智慧消防监控视频实现存储并在至亳芜视频平台汇聚，存储时间不低于2周 | 50 |
| 合计 | 53 |

在上述信息采集和处理过程中，应对其进行分类管理，确定不同数据类别的安全等级和访问权限，以保障数据安全。

## 网络建设和部署需求

本项目软件平台部署于电子政务外网，各个子系统的数据处理、数据分析、数据传输等算法实现都依托于电子政务云资源来实现，服务器复用智慧亳芜二期相关服务器，不够可进行扩容。系统对服务器的要求（参考）如下表所示。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **云主机资源** | **CPU（核）** | **内存（GB）** | **存储（GB）** | **数量** | **备注** |
| 虚拟主机 | 8 | 32 | 1024 | 2 | / |
| 虚拟主机 | 4 | 16 | 1024 | 2 | / |
| 虚拟主机 | 4 | 16 | 2048G | 2 | 文件存储系统2\*20M |
| 虚拟主机 | 2 | 8 | 100G | 2 | 需配置互联网接口2\*20M |
| \***其他资源或服务需求** | **资源描述** | \***数量** | **备注** |
| 网络资源服务 | 1\*100M专线 | 1 | 与备份云服务互联互通 |

## 安全需求

 系统数据要求安全，通过严格的权限控制体系实现用户的操作权限管理，确保用户在拥有合法的业务操作权限的前提下才能够进行业务操作；用户进行的所有数据操作要保留日志，保证数据提供和使用过程可跟踪、可审计。

因此，需要在各个层面为系统提供安全性、完整性、可用性、鉴别，抗抵赖等安全服务，主要涉及安全管理、安全协议、加密，签名与认证、密钥管理，安全评测、公钥基础设施等方面。

数据安全包括：

数据加密：对数据库进行整体加密，确保数据安全；

数据传输的安全：对传输中的数据流加密，以防止通信线路上的窃听、泄漏、篡改和破坏；

数据库安全技术：大型数据库管理系统应具有如下能力：

自主访问控制（DAC）：DAC用来决定用户是否有权访问数据库对象；

验证：保证只有授权的合法用户才能注册和访问；

授权：对不同的用户访问数据库授予不同的权限；

审计：监视各用户对数据库进行操作的过程记录，数据库管理系统应能够提供与安全相关事件的审计能力，如：试图改变访问控制许可权；试图创建、拷贝、清除或执行数据库；系统应提供在数据库级和纪录级标识数据库信息的能力。

## 性能需求

为确保平台运行效率满足使用需求，业务系统运行需满足以下性能需求：

1. 在硬件条件符合设计要求的前提下，系统支持多人并发，系统的登录时间在标准配置下运行将达到流畅和稳定；
2. 系统中查询响应时间很重要，如果时间长，将大大浪费时间，影响工作效率。系统性能优，将查询响应时间控制在3-5秒以内；
3. 采用结构化、面向服务的设计，可做到灵活扩展；
4. 系统应具有较好的健壮性，能容忍非法输入数据、相关软件或硬件组成部分的缺陷或发生异常的情况，整个系统将保持正常运行；
5. 整个平台系统在7×24小时连续运行时，年平均故障不超过5天，系统修复时间不超过3小时；
6. 平台整体界面设计符合主流操作系统的操作方法，让使用者能很自然的接受平台的操作方法，整个平台操作界面和管理界面都很友好。

## 业务协同需求

 本项目软件平台部署于电子政务外网，结合亳州市数据资源局已有的数据资源实际情况，本期开发、开放系统标准统一接口，为后期逐步完善城市大脑数据资源，分批次对接其它部门资源数据做好系统对接和业务协同。

# 建设内容

## 设计原则

按照公共安全工作“党政同责、一岗双责、失职追责”的要求，坚持统一规划、统一标准、统一建设，紧紧依靠党委政府领导，由政府牵头组织相关部门和单位共同参与，齐抓共管，强化协作，落实社会单位消防安全主体责任。

结合当前技术发展状况及趋势，在系统的设计过程中我们严格遵循以下原则：

1）科技引领，服务实战

充分运用当代云计算、大数据、物联网、NB-IOT通信等新兴技术，立足服务火灾防控工作，提升火灾预警防控和隐患治理水平。

2）开放共享，深度整合

打破地区、行业、单位之间的信息壁垒和信息孤岛，深度融合政府部门、社会单位信息资源，整合现有消防资源，实现消防内部全域开放共享，与政府部门、社会单位和公民有条件的开放共享。

3）统一规划，分步实施

按照“十四五”国家消防工作规划，对“智慧消防”平台建设总体框架、实施步骤、关键技术研究、综合保障等进行整体规划，制定分步实施方案，逐年逐项落实目标任务。

## 建设目标

 本次项目按照“规划引领、分步实施、急用先行、服务实战”的原则，依托物联网、云计算、大数据、移动互联网等新兴信息技术，按照“物联网+运营”的建设模式。依托信息化手段，形成“火灾防控多元共治、公众服务普惠、便捷火灾防控的防火监督信息化新格局，推动园区消防安全工作的革新。

结合亳芜产业园智慧消防建设需要和信息化现状，通过本项目建设，提高园区安全综合治理水平，本期项目建设目标如下：

1. 针对亳芜园区接入平台的重点单位开展消防设施检测，出具《安徽省建筑消防设施检测报告》，对检测不合格的单位出具问题清单及整改意见，待整改完成后再次检测排查问题、出具检测报告。
2. 针对亳芜园区内未接入消防安全物联网系统的44家单位，接入单位消防报警主机、消防水系统、火灾烟雾、消控室人员在岗监测、应急通道占用监测等状态数据，统一接入在智慧园区二期智慧消防平台内展示、统计，采集点位信息并标注，建立各单位消防电子档案，部署企业级消防安全物联网应用。
3. 升级软件平台功能：完善优化平台功能，实现隐患整改分析、设备在线分析、安全周报等数据分析可视化；加强对维保合同和维保过程管理，确保消防维保工作落实到位；开发安消联动和视频存储功能，支持消控室监控视频存储不低于1周，提升报警现场快速响应能力和火警事件追溯能力；展示运营数据和日志，实现对运营服务工作的考核监督。
4. 参照智慧园区二期建设模式，引入智慧消防运营服务，将本期联网的44家单位消防设施设备运行状态数据和告警数据接入运营中心，及时响应火灾预警、消除火灾隐患。

## 设计思路

以数据驱动和智能化为主线，吸收“快速迭代、小步快跑”等互联网思维，秉承“统筹集约、业务引领、创新驱动”原则，按照“大平台、小前端、富生态”新体系，调整架构、整合资源、深化应用，构建开放共享的智慧消防支撑体系，打造高效运行的“消防大脑”，通过数据赋能和流程再造，全面实现桌面端向移动端延伸，真正发挥信息化在改革发展中的支撑引领、减负增效、提质升级等作用建设中要把握好四大关系：

1、纵向的统分结合关系。遵循统一体系架构、技术路线、标准规范和共性功能，明确政府监管和运营的协同关系。

2、横向的协同共享关系。与城市大脑、相关部门、单位的业务协同和数据共享。

3、前后的继承发展关系。根据新一代信息技术的要求，对基础设施和应用系统进行梳理、整合和提升，同时对以往信息化建设整理出的需求进行修订，着眼新起点，解决痛点、难点，开发新一代信息系统。对于有迫切急用需求且必须建立的业务系统，遵循“急用先行”原则，实行统一规划、按需采购。

4、点面的一体共进关系。分步骤全面推进亳芜园区安全信息化建设，先行重点突破，再以点带面全面铺开。

## 总体框架

（1）基础设施层

基础设施层，又称信息采集、接收前端系统，包括各类信息采集、接收前端和物联网接入网关，是智慧消防完成系统功能的基础，既是原始数据的来源，也是自动控制的末端。

在本层系统中包括：用户信息传输、消防用水监测、视频监测、消防栓监测等前端设备实时信息采集。除了前端的采集设备之外，还包括各种基础设施的网络传输设施、平台搭建的硬件支撑设施。

（2）数据层

数据层包含由基础设施采集而来的数据和其他相关部门的基础数据，然后在建立对应的数据库。在智慧消防综合管理服务平台中数据层起到汇聚基础数据、服务平台应用系统的功能。

本次项目将基于政务云基础框架，整合各社会单位基础数据建立消防大数据平台。

（3）平台层

平台层为业务应用提供数据存储、分析和推送的支撑，是体现消防信息化的关键。平台层集成了四大基础应用平台，包括消防安全感知网络、消防智慧大脑、城乡火灾防控平台和消防公共信息服务平台。

（4）展现层

展现层解决的是信息处理和人机界面的问题，网络层传输来的数据在平台层进行信息转换、组合、分析处理后，通过各种设备与操作人员进行交互。通过不同的设备，展现出不同的应用系统。

展现层是由智慧消防平台核心软件及其展示功能组成，作为深度信息化的重要体现，也是智慧消防平台建设的关键内容，是智慧消防平台的触发点和落脚点，本次项目在二期平台基础上完善软件功能，同时与市级智慧消防平台、市级视频监控平台实现数据共享交换。

## 建设方案

### 重点单位消防安全检测

建筑消防设施是指建（构）筑物内设置的火灾自动报警系统、自动喷水灭火系统、消火栓系统等用于防范和扑救建（构）筑物火灾的设备设施的总称。常用的有火灾自动报警系统、自动喷水灭火系统、消火栓系统、自动水泡系统、自动雨淋系统、气体灭火系统、泡沫灭火系统、干粉灭火系统、防烟排烟系统、安全疏散系统等各系统。它是保证建筑物消防安全和人员疏散安全的重要设施，是现代建筑的重要组成部分。对保护建筑起到了重要的作用，有效的保护了公民的生命安全和国家财产的安全。

#### 消防供电系统检测

① 供电等级符合要求

② 配电柜的外观应完整，其型号、规格符合设计要求

③ 查看并记录供电电源回路是否符合技术要求。

④ 消防用电是不是专用回路。

⑤ 对最末级配电箱主备电源进行手动、自动切换试验 观察并记录切换情况。

⑥ 设有主备电源的场所：消防控制室、消防电梯机房、防排烟设备机房、火灾应急照明配电箱、各楼层消防配电箱、消防水泵房。

⑦ 一类高层建筑自备发电设备:应设有自动启动装置 并能在 30s 内供电。

二类高层建筑自备发电设备:当采用自动启动有困难时可采用手动启动装置。

查看自备发电设备起动运行情况,并记录起动时间。

⑧ 专用接地干线应采用铜芯绝缘导线,其线芯截面面积不应小于25㎜2专用接地干线宜穿硬质塑料管埋设至接地体。

#### 火灾自动报警系统检测

火灾报警控制器是火灾自动报警系统的心脏，应是工作的重点，所以在人员分散前应对消防控制室及火灾报警控制器进行认真细致的检测。

火灾报警系统的传输网络不应与其他系统的传输网络合用。

A. 消防控制室

a 设置应符合国家现行的防火规范的规定。

b 送、回风管，在其穿墙处应设防火阀。其内严禁与其无关的电气线路及管道穿过。

c 应设应急照明灯，且照度不低于150LX。其温、湿度应满足所放设备对环境的要求

d 应设置外线电话。

e 控制中心报警系统应设置火灾应急广播，集中报警系统宜设置火灾应急广播。

f 未设置火灾应急广播的火灾自动报警系统，应设置火灾警报装置。

g 入口处有明显标志，门应向疏散方向开启。应有消防平面图或模拟图。

h 当用一台区域火灾报警控制器或一台火灾报警控制器警戒多个楼层时，应在每个楼层的楼梯口或消防电梯前室等明显部位，设置识别着火楼层的灯光显示装置。

i 消防控制室周围不应布置电磁场干扰较强及其他影响消防控制设备工作的设备房。

j 消防控制室的最小使用面积不宜小于 30 ㎡。

B.控制器

a 应有保护接地。

b 主电源为消防专用电源。

c 主电源的保护开关不应为漏电保护开关。

d 主电源引入线严禁用插头。

e 测量其安装尺寸，记录。

f 其型号要与提供资料一致。

g 看其柜内配线 并用手轻拉试其牢固程度。

h 导线编号与图纸相符。接线端子的接线根数不超过两根。导线应绑扎成捆。

i 控制器的接地标志应明显持久。

j 要有主电源线标志。

k 看其是否用腐蚀性的助焊剂。

l 切断主电源，备电自动投入，然后恢复主电源，备用电源，自动切除，电源切换时指示灯有指示。

m 看其自检、手检功能。

C.探测器

在检测完控制室后 留一人在控制器处 余下之人去检测火灾探测器。

a 看火灾探测器的安装位置。

b 探测器的外观。

c 手感探测器的牢固程度。

d 测量其距端墙距离。并记录（小于安装间距的一半）。

e 看其确认灯的方向。

f 用烟杆或温杆对其测试，探测器要在报警同时，启动探测器确认灯。

g 报警时，控制室的控制器能报警、能消音、能复位、能二次报警、有记忆功能。

h 对探测器先造一个故障当控制器显示成功后再造一个火警试验控制器的火灾优先功能。

i 把控制器按钮打到联动上，人造一个火警，看声光报警器能否发出声光讯号，并连动相关层，用声压计量声强和环境声强并记录。

j 测量手报的高度，宜为 1.5m 并记录。按下手报按钮，手报显示灯亮，控制室控制器有警报，在距其 1m 处用声压计测量控制器的声强并记录。对任意两手报间的距离进行测量看是否合乎标准。

k 在检测探测器的同时，可检测每层的广播，并记下距其最远处的声强和环境声强。

l 对消防广播进行选层广播和强行切换。

m 同时可对每层的电话插孔进行检测，看其是否与控制室能清晰通话。

n 上到顶楼 可对其消防电梯进行检测，看其是否能在 1min 内到达底层一般电梯停止使用。

15. 消防专用电话网络应为独立的消防通信系统。

16. 特级保护对象的各避难层应每隔 20m 设置一个消防专用电话分机或电话塞孔。

#### 自动喷水灭火系统检测

泵房是整个水灭火系统的心脏，应集中起来共同细致的检测。

A 先分散到水泵接合器、室外消火栓处对其检测。

a 地下式的水泵接合器应有防水，防锈措施，四阀齐全，其接口距地面≤0.45m。

b 地上式的水泵接合器，其接口距地宜为 0.7 m。

c 测试室外消火栓是否有压力，并记录。测量其与水泵接合器的距离，并记录。

d 消防水池的取水口距最近建筑物边墙距离在 5＜ L ＜100 m之间，并测量记录。消防水池的体积符合要求，消防水池的取水口深度 6＜ m。

B 室内部分

室内部分分下、中、上三个分部。

a 下：消防（喷淋、雨淋）泵

湿式（干式）报警阀组

ⅰ）消防（喷淋、雨淋）泵

① 消防（喷淋、雨淋）泵的进水出水管是否符合要求。

② 消防（喷淋、雨淋）泵的铭牌并记录。

③ 远距离或现场启动泵，保证在 5min 内泵开始运转。现场或远距离停泵。

④ 看水泵与动力机械是否直接连接。

⑤ 应检查泵的配电柜内接线状况，并看其是否有明显的接地线标志和接地线。

⑥ 切断主电，看是否有备用电源投入运行。

⑦ 启动主泵，给主泵选一故障，看备泵是否能自动投入运行。

⑧ 看泵的进水是否是自灌式的或有可靠的充水设备。

⑨ 泵的出水管上应设实验和检查用的压力表和放水阀门。

ⅱ 湿式（干式）报警阀组

① 看其组件是否完整。

② 测量报警阀到侧墙的距离≥0.5m。距地高度宜为 1.2m 正面距墙为 1.2m。

③ 报警阀地面上有相应的排水措施。

④ 当有两个或两个以上的报警阀时，进水管应为环状。

⑤ 水力警铃的安装位置及其连接管径应符合要求。

⑥ 打开湿式报警阀组的试验阀。看水力警铃在 5-90s内是否能连续报警，并在其 3m 远处测量其声强 ≥70dB 。

⑦ 打开试验阀时，压力开关有动作。水力警铃报警。

⑧ 关闭总控制阀，水力警铃停止动作。压力开关停止动作，延迟器无出水。

⑨ 用秒表测量延迟器的排水时间 （≤5min ）

⑩ 打开和关闭报警阀门，报警阀上的前后压力表应动作一致，且指示正常。

11 各消防管道应固定牢靠，且有红色环道标记。

b 中： 消火栓箱

消火栓按钮

喷头

管道

① 看消火栓箱的位置是否与图纸一致。

② 看消火栓的组件是否齐全。

③ 栓口的方向与地面的距离、与箱底边的距离、与近箱侧边的距离、与封挡玻璃的距离，测量并记录。

④ 按下消火栓按钮 能启动消防喷淋泵。并在控制器上有显示。

⑤ 消火栓按钮有保护措施。

⑥ 各喷头的安装质量。各喷头的安装间距应符合要求。喷头与隔断墙、梁柱间的距离符合技术要求。

⑦ 管道应与其隐蔽记录相符。

⑧ 看消防审核意见书或设计变更通知单上提到的是否已经更该或已经变更。

c 上： 末端试水装置

检查用的消火栓

消防水箱增压装置

ⅰ） 末端试水装置

① 每个系统分区的最末端均应设置末端试水装置。

② 装置有便于操作的试验阀和便于观察记录的压力表。

③ 先记下最不利点的静压。

④ 打开试验阀，记录动压，并用流量计测量末端流量。

⑤ 打开试验阀后 5min 内泵启动 控制器有显示 水流指示器有动作。

⑥ 试验管直径不小于 25 ㎜。

ⅱ） 检查用的消火栓

① 用压力表测试检查用消火栓栓口的静压 并记录。

② 按下消火栓按钮启动消防泵记录。检查用消火栓的动压。

③ 在最低层的消火栓看其静压，并记录。启动消防泵，测其动压，并记录。看是否超压如果超压，看其是否有减压措施。

ⅲ） 消防水箱

① 容积符合建筑要求，测量长、宽、高算容积。

② 水箱距箱墙距离测量与各边墙的距离并记录>0.7m

③ 与建筑物顶部的距离。量与建筑物顶部最低点的距离>0.6 m。

④ 看水箱是否有保证消防用水的措施，是否有水位指示器。

⑤ 管道穿过水箱时宜直接焊接，且在焊接处做防锈处理。

⑥ 消防管道的阀门应是常开的。

ⅳ） 增压装置

① 有配电柜，看其柜内配线是否整齐。

② 配电柜内的接地线应有明显标志。

③ 有双电源或双回路电源。

④ 气压罐的容积符合技术规范要求。

⑤ 气压罐上有安全阀，压力表，泄水管。

⑥ 气压给水装置的进水、出水管、充气管上应安装止，回阀和闸阀，充气管上还应有安全阀和气压表。

⑦ 气压罐的铭牌、记录、外观完好。

⑧ 气压罐的净空距≥0.7 m 罐体任何部件距地面≥0.5 m 罐顶至建筑物结构最低距离≥1.0 m。

⑨ 切断主电源，备电源自动投入。

ⅴ） 联动试验

① 打开末端试验装置。

② 增压装置启动。

③ 水流指示器动作 湿式报警阀打开。

④ 控制室有信号显示。

⑤ 水力警铃动作。

⑥ 泵启动。

⑦ 增压装置停止运行。

#### 防火卷帘、防火门检测

疏散通道上的防火卷帘，应分两步动作，用作防火分隔的防火卷帘，应一步到位。

A 防火卷帘

a 防火卷帘的安装位置，应符合设计要求。

b 防火卷帘的外观应完好。

c 防火卷帘的安装质量应良好。

d 防火卷帘的水平直度符合要求。

e 防火卷帘卷轴的平行引度符合要求。

f 防火卷帘开降速度符合要求。

g 应急操作时，将拉力弹簧的挂钩挂在手拉链或摇把上测手拉链力≤150N 手摇力≤50N。并记录。

h 手动启动防火卷帘启动力 用拉力弹簧测启动力≤120N。

⑨ 探测器距卷帘表面 1m--1.6m。两种火灾探测器间距应大于 1m。实地查看并记录。

i 第一种探测器动作 卷帘下降至距地面的距离测量、记录。

j 第二种探测器动作后 卷帘下降到底。

k 操作手动按钮 观察卷帘启闭情况。

l 控制器上显示其动作。

m 火警状态下关闭的卷帘仍处于关闭状态 水幕喷水保护。

B 防火门

消防控制设备对常开的防火门的控制门任一侧的火灾探测器报警后 防火门应自动关闭。

a 钢质防火门

① 外观应完整

② 其材料及配件应齐全。

③ 采用合页不得采用双向弹簧作用的合页。

④ 单扇门应设置能自动关闭的闭门器。

⑤ 双扇门的中缝有盖缝板，并有闭门器和顺序器。

⑥ 应采用与门相同耐火等级的防火玻璃。

⑦ 启动释放开关看门关闭后的情况并记录。

b 木质防火门

① 外观完整。

② 看材料及配件是否齐全。

③ 用塞尺测量木质防火门安装留缝宽度并记录。

④ 检查防火门的启闭性能和开启方向。

⑤ 用测力计测定木质防火门的开启力是否符合技术要求。 ≤80N

( 5 )防排烟装置

A 送风

① 看加压送风口的位置应符合规范要求。

② 看送风管道的材料是否为不燃材料，内部是否光滑，其隔热层是否采用不燃材料制作。

③ 试验加压送风阀应能手动、电动及远距离开启，并能手动复位。

④ 用风速仪测量送风口的风速≤7m/s。

⑤ 风机有主备电源，且切换正常。

⑥ 风机启动后运转正常。

⑦ 风机现场，远程启停正常。

⑧ 用微压计分别测试相关部位的余压值。

B 排烟

① 用风速仪测定排烟口风速≤10m/s。

② 排烟风机的风量符合设计要求。

③ 排烟口的位置符合设计要求。

④ 排烟口平时应处于关闭状态 并没有手动和自动开启装置可手动复位 其手动开启高度符合要求。

⑤ 防火阀的位置符合设计要求。

⑥ 防火阀平时是开启的。

⑦ 手动、电动关闭时动作正常手动可以复位。

C 系统联动

① 手动开启任一送风口，排烟口，控制室有信号，确认后，风机启动，该分区的所用通风设备，空调设备及相关的防火阀能关闭。

② 用火灾探测器报警，观察送风口风机，空调，防火阀的动作情况是否正常。

#### 气体灭火系统检测

A 瓶组与储罐

① 储罐及其组件应固定牢固,手动操作装置的铅封应完好,压力表正面应朝向操作面且压力显示处于设计允许范围值内。

② 储罐上应注明灭火剂名称和编号,灭火剂驱动装置和选择阀应有明显的分区标志牌且标示正确、清晰 选择阀手动启闭应灵活。

③ 带有承重装置的储罐,其称重装置应正常,并应有原始重量标记。

④ 高压二氧化碳储罐在灭火剂的失重量达到设定值时,应能发出报警信号。

⑤ 低压二氧化碳储罐的制冷装置应正常运行,温度和压力的控制值应符合设定值,储罐上应设置有安全泄压装置。

⑥ 储罐的存放位置及环境应符合其安全、正常运行的要求。

B 喷嘴

① 喷嘴的型号规格符合设计要求,喷口方向应正确、无堵塞现象。

② 喷嘴应有表示其型号、规格的永久性标志。

③ 对于多尘或腐蚀性场所,喷头应有相应的防护措施。

C 气体灭火控制器

① 气体灭火控制器的技术要求应符合报警设备规范的要求。

② 自动、手动转换功能应正常，手动操作启动方式在灭火控制器处于自动或手动状态时均可实现。

③ 灭火控制方式所处状态应有明显的标志或灯光显示,反馈信号显示应正确。

D 系统功能

① 防护区内及其入口处的声光报警装置和入口处的安全标志、紧急启停按钮应正常。

② 火灾报警控制器确认火灾报警后的延时启动时间应符合设定值。

#### 出具检测报告

1、现场检测完结后，应给委托方出具一份整改意见书，以待该项工程不完备的地方加以整改，达到合格要求。

2、检测完后，整理所记资料，与提供资料相协调，出具报告初稿，待委托方要求复检时，根据复检的情况出具公正、准确的正式报告纸质版有效检测报告3份、电子版有效检测报告1份。

3、最后把所有资料存档保管。

### 智慧消防安全物联网

#### 业务流程



图 消防安全感知网业务流程图

消防安全感知网业务流程如图所示。感知前端按照预设规则进行数据采集，并将采集到的数据向数据中心传输。在此过程中，感知资源综合管理模块监听到上传意图时，会立即对数据源的注册情况进行判断。如果感知前端已在综合管理模块注册则允许上传，若尚未注册则拒绝上传，至此业务流程结束。

消防安全感知网链接拓扑图如下：



图 消防安全感知网链接拓扑图

#### 系统组成

系统包括火灾防控感知和公共信息感知两个部分。其中，火灾防控感知包括火灾自动报警系统接入、电气系统感知、消防水系统感知、视频监控系统接入，公共信息感知包括舆情信息相关系统接入，感知资源综合管理包括设备资源虚拟化、资源池、分布式资源同步、感知资源上图。

火灾自动报警系统接入主要通过用户信息传输装置接入火灾报警主机及下挂探头状态信息；

电气系统感知主要通过电气火灾监测终端设备实现；

消防水系统感知主要通过液位压力感知终端、智能末端试水终端、消火栓监测终端、物联网网关、无线遥测终端、雷达式水位计、多普勒明渠流量计等设备实现；

室外消火栓感知主要通过在室外消火栓加装监测设备，实现全天候对消火栓实时监测，包括压力监测、用水量、撞倒倾斜、报警定位功能等数据和功能，解决人工巡查难题；

可燃气体感知主要通过可燃气体感知终端，实现对天然气、液化气遗漏进行监测、预警等功能；

独立式烟感探测感知主要通过在九小场所、养老院、三合一等场所安装联网独立式感烟探测器，实现对小场所早期火灾预警，当有警情发生，系统发出警情提醒，警情定位等功能。

视频监控系统接入主要通过高清摄像机实现；

舆情信息相关系统接入主要通过系统接口实现；

感知资源综合管理主要通过软件开发实现。

消防物联感知设备标准化安装接入系统图如下：



#### 系统功能设计

##### 火灾自动报警系统感知

针对消防安全重点单位、火灾高危单位既有的火灾自动报警系统，通过与其系统主机进行对接，获取相关数据，并通过用户信息传输装置进行本地汇聚，最后通过接口总线至数据中心。

经接口总线接入的标准化内容包括以下部分，实际接入内容根据具体单位对象的火灾自动报警系统真实数据情况进行调整：

报警主机状态接入：能够获取主机的工作状态信息；

报警主机报警信号接入：能够获取主机发出的报警信号；

感烟探测器信号接入：能够获取感烟探测器的报警和工作状态信号；

感温探测器信号接入：能够获取感温探测器的报警和工作状态信号；

火焰探测器信号接入：能够获取火焰探探测器的报警和工作状态信号；

手动火灾报警按钮信号接入：能够获取手动火灾报警按钮的报警和工作状态信号；

报警阀信号接入：能够获取报警阀的动作信号；

喷淋消防泵信号接入：能够获取喷淋消防泵的启停信号；

压力开关信号接入：能够获取压力开关的动作信号；

水流指示器信号接入：能够获取水流指示器的动作信号；

消火栓泵信号接入：能够获取消火栓泵的启停信号；

消火栓按钮信号接入：能够获取消火栓按钮的动作信号；

气体灭火控制器信号接入：能够获取气体灭火控制器的动作信号；

泡沫灭火控制器信号接入：能够获取泡沫灭火控制器的动作信号；

加压送风口信号接入：能够获取加压送风口的动作信号；

加压送风机信号接入：能够获取加压送风机的启停信号；

电动挡烟垂壁信号接入：能够获取电动挡烟垂壁的动作信号；

排烟口信号接入：能够获取排烟口的动作信号；

排烟阀信号接入：能够获取排烟阀的动作信号；

排烟防火阀信号接入：能够获取排烟防火阀的动作信号；

排烟风机信号接入：能够获取排烟风机的启停信号；

防火门监控器信号接入：能够获取防火门监控器的动作信号；

防火卷帘控制器信号接入：能够获取防火卷帘控制器的动作信号；

消防电梯信号接入：能够获取消防电梯的动作信号；

消防应急广播信号接入：能够获取消防应急广播的动作信号；

消防应急照明信号接入：能够获取消防应急照明的动作信号；

消防疏散指示信号接入：能够获取消防疏散指示的动作信号。

##### 电气系统感知

包括针对消防安全重点单位、火灾高危单位和九小场所的电气系统感知需求的物联网感知设备的建设部署，相关物联网设备通过物联网网关进行级联并最终汇聚至数据中心。

通过部署电气火灾监控设备实时监测线路的电压、电流、故障电弧、剩余电流、温度等信息，并通过接口总线汇聚至数据中心。

经电气火灾监控设备感知的标准化内容包括以下部分，实际感知内容根据具体单位对象的电气系统真实情况进行调整：

电压传感器信号：获取电压传感器采集到的实时电压数据；

电流传感器信号：获取电流传感器采集到的实时电流数据；

故障电弧传感器信号：获取线路关键节点位置故障电弧发生数据；

剩余电流传感器信号：获取线路中剩余电流数据；

线路温度传感器信号：获取线路关键节点位置温度数据。

##### 消防水系统感知

消防水资源感知。能够获取建筑消防水系统的水池水位、管路压力等参数信息，涉及消防水池、室内消火栓、高层超高层末端试水，能够感知市政消火栓消火栓情况、天然取水点情况。

针对消防安全重点单位、火灾高危单位的消防水系统感知需求，通过部署传感器设备实时监测上述水系统的状态，并由接口总线汇聚至数据中心。经相关设备感知的标准化内容包括以下部分，实际感知内容根据具体单位对象的消防水系统真实情况进行调整：

水压传感器信号：获取水压传感器采集到的压力数据；

流量传感器信号：获取流量传感器采集到的流量数据；

液位传感器信号：获取液位传感器采集到的液位高度数据。

##### 室外消火栓感知

主要通过在室外消火栓加装监测设备，实现全天候对消火栓实时监测，包括压力监测、用水量、撞倒倾斜、报警定位功能等数据和功能。

##### 独立式烟感探测感知

主要通过在高危场所、九小场所、养老院、三合一等场所安装联网独立式感烟探测器，实现对小场所早期火灾预警，当有警情发生，系统发出警情提醒、信息推送和警情定位等功能，做到智能化联网火灾预警，防止小火亡人。

##### 消防视频监控感知

针对消防安全重点单位和火灾高危单位，通过ONVIF及GB/T 28181等协议接入主流监控视频流，在此基础上可进行人工智能模型分析识别，监测烟雾、火焰等火灾特征，并将识别结果与原始监控视频叠加，可进一步进行视频智能分析，实现火灾报警、在岗监控和消防通道占用识别等功能。

主要功能包括：

烟雾识别：识别视频监控信号中出现的烟雾；

火焰识别：识别视频监控信号中出现的火焰；

人员在岗识别：识别视频监控信号中出现的人员在岗/离岗情况；

消防通道占用识别：识别视频监控信号中出现的疏散通道占用情况。

 

### 4.5.2.3.7 火灾报警按钮

手动报警按钮安装在公共场所，可以人为手动触发报警按钮主动触发警情，并可以本地化联动输出开关信号，可用于联动警铃、喇叭、音柱、门禁等设备，数据管理平台收到报警信息后，并通过4G网络上传告警信息至平台，可立即显示出报警按钮的安装位置及登记信息并发出报警提示。当报警按钮需要报警恢复时，可通过专用的复位钥匙进行复位。对安全隐患或早期火灾及时联动预警，以便及时通知人员、疏散、干预，减少损失，保障人身安全。

基于良好的4G网络覆盖，极大的扩展了应用场景。该报警器可广泛应用于九小场所、加工厂、出租屋、公租房、高层建筑、老旧小区、景区、古建、乡镇、村落等消防改造类场景等消防防护建设

**4.5.2.3.8 火灾声光报警器**

火灾声光警报器，是一种安装在现场的火灾声光警报设备，用于当发生火灾时提醒现场人员注意并疏散。可以人为手动触发报警按钮主动触发警情，本地启动声光报警，及时并通过4G网络上传告警信息至平台。对安全隐患或早期火灾及时联动预警，以便及时通知人员、疏散、干预，减少损失，保障人身安全。

基于良好的4G网络覆盖，极大的扩展了应用场景。该报警器可广泛应用于九小场所、加工厂、出租屋、公租房、高层建筑、老旧小区、景区、古建、乡镇、村落等消防改造类场景等消防防护建设。

### 智慧消防平台功能升级

维保管理：系统支持用户对应急维保订单和例行维保任务生成的报告进行管理与下载存档。可查看当前计划对应的单位名称、计划名称、开始结束时间、维修设备数等。提供基于后台监测到维保过程中触发设备报警及状态数据的对比和维保过程核实

维保监管：向维保单位提供维保过程监管及统计工具；支持维保过程实时数据的接入在消防安全管理Web系统同步展示。自动生成维保过程指标包括维保及时性、设备更换率等，并支持针对现场维保人员、维保公司领导等不同角色的月度、年度与综合统计分析

维保任务提醒："根据消防物联网监测异常数据，将异常设备信息推送至维保单位生成动态维保计划，确保维保工作能及时消除消防设备运行隐患。支持在APP端提醒维保任务，系统滚动提示当前待完成的例行和应急维保任务，包括任务要求时间、任务对应业主单位、任务当前状态等"

运营中心工作量统计："支持运营中心工作人员对物联网监 测历史和实时全量信息的查询需要，展示物联网监测数据的全量信息，根据时间展示每条有效信号信息记录。支持运营中心人员处置火警、故障、逾期、离岗等异常事件的工作量统计，可按年、按月、按日对隐患进行多维度统计分析"

安消联动：基于建筑平面图位置算法的安消联动方案，当设备报警时，可通过调用周边视频，第一时间了解现场情况；确认为真警时，画面自动跳转至关联的附近视频。

视频融合与存储：开发视频存储功能，将智慧园区二期智慧消防项目监控视频和本期新增联网单位新增视频监控数据，接入至亳芜园区视频监控平台，支持跨平台的统一调度查看（监管大屏系统、企业端平台），支持视频数据存储不低于2周。

同步在消防安全监测预警系统上增加维保计划管理、维保监管、维保任务提醒等功能。

### 智慧消防运维运营服务

项目建成后由亳芜产业园管委会按照联网单位数量购买运营方服务，中标单位需要提供本地化运营服务，数据运营需接入智慧亳芜二期项目运营中心统一管理。数据通过运营中心推给智慧亳芜智慧消防物联网监测平台等，由运营中心全面负责系统的运行、维护和组织管理；协调系统内部有关系统运行的工作。

本项目包含3年智慧消防数据运营、系统运维和硬件运维服务，智慧亳芜二期智慧消防软硬件及接入单位服务结束后，纳入该项目一并提供运维运营。

该项目运维运营到期后，后续每年运维运营费用不高于项目中标价格的10%。

项目建设或运维运营期间，中标单位提供因上级要求、实际业务需要等导致的系统升级改造服务。

项目建设或运维运营期间，根据实际工作需要，该项目软件系统应实现与市级其他软件系统对接。

#### 运营服务内容

1. 运营中心服务：建立本地消防运营服务中心，运营中心提供监测大厅、接待区与值守坐席；运营中心值守人员同时不少于2人。
2. 值守监测服务：实时动态传输消防物联网软件覆盖的设备设施信息，对消防设施运行状态（如自动报警系统、水位、水压、电气火灾、烟雾等）进行7×24小时的专人监测值守服务，实时监测各类消防设施的运行状态数据，发现故障隐患第一时间通过软件和人工值守提醒；
3. 隐患管理：提供隐患提醒、隐患上报、状态追踪、整改详情闭环管理等服务，帮助业主将隐患自查整改制度信息化、流程化，切实提高隐患处置效率，确保消防隐患及时整改和消除。
4. 如业主有改、扩建工程，及时更新总图，并相应扩充数据库；
5. 每年为企业提供2次培训；
6. 为企业软件运行提供技术支持；
7. 根据园区管委会和消防安全部门管理需求提供数据，每周、每月安排专人向重点单位安全管理人员提交专业分析报告。

#### 联网单位的权利和义务

1.联网单位应保证托管服务范围内的建（构）筑物具有真实、完整、有效、合法的建筑手续，联网单位应提供有关证明材料以供运营中心和消防部门备查。

2.联网单位保证服务范围内消防设施设备在联网接入起始时处于完好状态，且无任何权利瑕疵，否则运营中心有权不提供运营服务。

3.联网单位应派专门工作人员积极配合运营中心提供的服务，并对可能影响或损坏自动消防设施设备的不良因素进行整改，以确保消防设施设备的正常运行。

4.联网单位应在遇到火情时立即通知消防救援机构或运营中心，并在救灾后保持火灾现场完整，如因未及时通知消防救援机构或运营中心、火灾现场被破坏，影响保险公司进行火灾损失评估，导致不能进行赔付的后果由联网单位承担。

5.如因联网单位人员虚报、误报警情导致运营中心联系119报警所产生的法律责任和费用，由联网单位承担。

6.在服务期内，因联网单位违法违规行为产生的法律责任（包括但不限于行政处罚，如消防罚款等），由联网单位自行承担。

#### 运营中心的权利和义务

1.运营中心及其委托单位应按运营服务内容及要求为联网单位和监管部门提供相应服务，并接受监管部门的监督。

2.运营中心有权因技术进步或国家法律、政策变动等原因对运营服务服务内容、业务功能、操作方法等做出调整，但应在调整前告知联网单位和监管部门。

3.在服务期限内，如运营中心及委托单位发现联网单位消防设施设备存在、出现问题（以下简称“故障设备”），并需对该等设施设备进行维修或改造的，应自发现之日起3个工作日内，向联网单位提出整改建议并告知不予整改可能产生的不利后果（以下合称“整改意见”）。如联网单位在收到整改意见后未予整改（包括但不限于明示或暗示不接受整改意见，或未能完成整改等）或整改结果未获乙方认可，则因故障设备所造成的后果，由联网单位自行承担。

4.运营中心应及时提醒联网单位按照运营中心的服务标准中的规定执行或运用“企业消防安全管理标准化应用软件”开展工作，如经运营中心提醒仍未予以改正的，由此所造成的损失由联网单位自行承担。

5.如联网单位对服务范围内的建（构）筑物进行改造的（包括但不限于改变联网单位生产经营场所使用性质、改变建筑原有防火分区、改造消防系统等），联网单位应在改造完成后30日内以书面形式通知运营中心，运营中心在接到联网单位通知后更新单位信息。

## 系统安全

### 系统安全基础设施建设方案

#### 方案概述

按照国家信息安全等级保护和商用密码建设的要求，从系统建设安全管理和系统运维安全管理等方面，做到对消防系统信息安全管理制度建设与信息安全技术系统建设的协调统一，进一步加强业务平台和安全系统的同步建设，确保平台消防工作的高效安全。

#### 安全通信网络设计

通信网络是信息系统中完成计算环境之间信息传输的部件。通信网络主要指本项目连接其它外部网络时所通过的连接部件。本项目依据《网络安全等级保护安全设计技术要求》中的第三级系统“通用安全通信网络设计技术要求”，同时参照《网络安全等级保护基本要求》、《网络基础安全技术要求》，对等级保护对象涉及到的安全通信网络进行设计。

项目运行于政务云，提供网络安全基础设施，通信网络安全防护效果如下：

1、登录保护

实现受登录保护产品服务的云主机及登录账号集中管理功能，可随时控制云主机账号的登录保护状态，统一记录受登录保护产品服务的云主机登录认证日志，为管理员提供云主机登录集中审计功能。

1. 平台应用保护

Web威胁检测，具有检测各类应用网络攻击行为的能力，如SQL注入、XSS攻击、远程溢出攻击、漏洞扫描、Bash漏洞攻击、远程命令执行、敏感文件访问。

IP信誉库检测，内置的IP信誉库，用于阻断库中的恶意IP访问，放行库中合法的访问。

事件管理，攻击事件日志、事件通知等集中管理和处置。

1. 通信网络数据传输完整性保护

SSL VPN支持国际商用加密算法，用户可根据业务系统重要程度按需选择加密算法和秘钥长度。通过标准加密算法保障数据传输安全。SSL VPN提供独立日志中心可以详细记录接入用户的访问行为，确保用户的访问过程可追溯。同时可以提供详尽报告，作为网络规划的依据。此外日志中心具备管理员权限分级功能，提高了管理安全性。

1. 通信网络可信接入保护

对远程接入采用SSL安全协议、和网络密码机等网关设备实现数据远程传输的完整性、保密性和可信链接。

#### 安全计算环境设计

计算环境是消防业务系统位于物理上受保护的边界内部，一般包括完成信息处理与存储的主机、操作系统、数据库管理系统、云计算和数据服务组件、业务系统、外部设备及其连接部件。

依据《网络安全等级保护安全设计技术要求》中的第三级系统“通用安全计算环境设计技术要求”，同时参照《网络安全等级保护基本要求》等标准要求，对等级保护对象涉及到的安全计算环境进行设计，本次设计主要针对业务应用系统本身安全进行设计，内容包括用户身份鉴别、自主访问控制、标记和强制访问控制、系统安全审计、用户数据完整性保护、用户数据保密性保护、数据备份恢复、客体安全重用、可信验证、配置可信检查、入侵检测和恶意代码防范、个人信息保护等方面。

##### 用户身份鉴别

身份鉴别在整个等级保护对象中处于基础的、关键的地位。网络安全最基本和关键的保护就是要从身份鉴别入手来提高和控制整个系统的安全。身份鉴别除了必要的技术手段保证外，与之配套的管理制度规范也是必不可少的。

等级保护对象设计将加强终端登录、应用系统等身份鉴别管理，通过身份鉴别系统对用户的账户、密码、证书进行统一管理，防止非法用户随意接入访问应用服务器数据资源。所有等级保护对象内终端将增设开机CMOS密码，加强CMOS修改权限的保护，防止通过改变系统启动设置等参数、非授权使用终端。具体设计如下：

1、用户身份标识

在应用系统身份鉴别及跟踪方面，可以在等级保护对象应用系统层面设定标识，并与应用环境如数据库存储、操作系统以及网络传输进行更深入的绑定，使更深层次的审计成为可能。

由应用系统统一生成唯一的用户身份标识符，无论在系统生命周期还是在应用过程中，该标识符是唯一的，并贯穿于业务系统应用始终。该身份标识符存放在数据库特殊位置，并进行保护。在数据库列表不被非授权地访问、修改或删除；用户如果要以特权用户访问该资源，必须要有两种或以上身份验证的方法。用户标识符应与安全审计相关联，保证系统发生安全亊件时的可核查性。

2、登录失败处理

当用户身份鉴别尝试失败次数达到5次后，应采取以下措施：对于本地登录，将进行登录锁定，同时形成业务系统和数据库审计事件并告警。对于应用程序，禁止使用该程序或延长一定时间后再允许尝试。

3、重新鉴别

用户身份鉴别成功登陆系统后，如果当其空闲操作的时间超过规定值（通常为10分钟以内）后，在该用户需要执行其他操作之前，将对该用户重新进行身份鉴别。

4、远程管理传输

远程管理的设置是为了方便管理员随时随地进行管理操作，当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。为此，需要对鉴别信息进行加密处理，而网络传输过程中最经常使用的是SSL加密。SSL加密用以保障在网络传输数据的安全，利用数据加密技术，确保数据在网络上的传输过程中不会被截取及窃听。

5、双因子认证

在等级保护对象中，服务器、用户终端、应用程序以及网络和安全设备的本地登录、远程登录均进行用户身份鉴别。身份鉴别方式采用USB Key智能密码钥匙+ PIN 码的相结合的双因子认证方式。

##### 自主访问控制

自主访问控制是一种常用的访问控制方式，它基于对主体或主体属性的主体组的识别来限制对客体的访问，这种控制是自主的。自主是指主体能够自主地（可间接地）将访问权限或访问权的某个子集授予其它主体。

对于自主创建的文件，除了对文件做机密性、完整性保护外，还需要进行访问控制的操作。文件属主通过操作系统自带的访问控制功能实现对受保护文件的统一“读”、“写”、“执行”等操作管理。普通用户对这些文件进行访问，不能违背这些规定，否则，操作不能进行。另外，也可以通过部署统一认证及权限管理系统的访问控制功能实现文件级的访问控制。

针对等级保护对象的主机系统访问控制策略需要对服务器及终端进行安全加固，加固内容包括：限制默认账户的访问权限，重命名系统默认账户，修改帐户的默认口令，删除操作系统和数据库中过期或多余的账户，禁用无用帐户或共享帐户；根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；启用访问控制功能，依据安全策略控制用户对资源的访问。

关闭操作系统开启的默认共享，对于需开启的共享及共享文件夹设置不同的访问权限，对于操作系统重要文件和目录需设置权限要求。

设置不同的管理员对服务器进行管理，分为系统管理员、安全管理员、安全审计员以实现操作系统特权用户的权限分离，并对各个账户在其工作范围内设置最小权限。通过主机内核加固系统，实现服务器的内核级安全加固。

##### 标记和强制访问控制

强制访问控制是指由系统（通过专门设置的系统安全员）对用户所创建的对象进行统一的强制性控制，按照规定的规则决定哪些用户可以对哪些对象进行什么样操作类型的访问，即使是创建者用户，在创建一个对象后，也可能无权访问该对象。等级保护对象中强制访问控制，通过以下方式实现。

1、应用系统层面的强制访问控制安全机制

应用系统层面的强制访问控制的实现，可以在需要控制的文件、数据库服务器外部部署统一认证及权限管理系统实现对用户的授权，利用基于角色的访问控制模型（RBAC）结合应用系统的安全功能开发，实现对用户功能操作的强制访问控制，等级保护对象应用系统实现对用户资源的强制访问控制。即：由安全管理员通过在统一认证及权限管理系统对所有主体（用户）进行标记，强制访问控制主体的粒度为用户级。通过应用系统对所有客体（文件、数据库中的数据）进行安全标记，客体的粒度为文件或数据库表级，将用户类别与安全标记文件对应，从用户的访问请求中取得要访问的资源和操作。通过访问控制列表，检查用户与此进行安全标记的文件是否有访问权限，实现对文件的强制访问控制。

文件在整个生存周期中，除非经安全管理中心重新定级，否则安全标记全程有效。强制访问控制，是根据安全策略来确定该用户能否对指定的受控文件进行操作。比如安全策略规定，高密级用户可以访问同密级和低密级文件；反之，低密级用户则被强制禁止访问高密级文件。当然，管理中心可以根据实际应用环境制定相应的安全策略，从而实现标识和强制访问控制目标。

##### 用户数据完整性保护

数据完整性指传输和存储的数据没有被非法修改或删除，也就是说数据处于未受损未丢失的状态，它通常表明数据在准确性和可靠性上是可信赖的。其安全需求与数据所处的位置、类型、数量和价值有关，涉及访问控制、消息认证和数字签名等安全机制，具体安全措施包括防止对未授权数据进行修改、检测对未授权数据的修改情况并计入日志、与源认证机制相结合以及与数据所处网络协议层的相关要求相结合等。

数据完整性保障技术的目的是对数据完整性进行预防和恢复。预防是指对威胁数据完整性的各种不利因素采取预防措施，如常用的数据备份等；恢复是指在数据遭受损失或破坏后，采取有效的恢复技术，使得被破坏的数据尽快得到恢复。确保数据完整、正确性的方法包括数据校验技术、数字签名技术等。

1、数据校验

数据校验技术是为了保证数据的完整性，用一种指定的算法对原始数据计算出的一个校验值。接收方用同样的算法计算一次校验值，如果和原始数据提供的校验值一样，就说明数据是完整的。

2、数字签名

数字签名是为了保证对信息主体的认证，以实现信息的真实性、完整性和不可抵赖性，它提供了一种保护电子文档的真实性和完整性的方法。在公钥机制下，数字签名通过一个单项函数对要传送的报文进行处理，得到用以核实报文是否发生变化的一个字母数字串，以此来判断报文的完整性。在私钥机制下，通过专属私钥加密报文，接收方只能通过对应公钥进行解密，证明该报文的真实来源，用以核实报文的不可抵赖性。

对等级保护对象的用户数据完整性防护，重点体现在数据库中的结构化数据上。对数据完整性的保护体现在两个方面。一方面，在数据的存储与操作时，在数据库管理系统中，利用对数据表的主键、外键来保障数据完整性；另一方面，在数据的传输时，应尽量利用数字签名、VPN等加密技术，保障数据传输的完整性。

##### 用户数据保密性保护

数据保密性是指防止信息被未经授权者访问和防止信息在传递过程中被截获并解密的功能。

数据保密性可分为动态信息保密性和静态信息保密性。动态信息保密性表现为数据在传输过程中的保密性，而静态信息保密性表现为数据在存储过程中的保密性。

1、动态数据加密

在动态数据保密性方面，通过部署VPN、安全通信协议或其他密码技术等措施实现数据传输过程中的保密性防护，如通过VPN实现同城、异地备份中心的传输加密。

对鉴别信息、重要业务数据和重要个人信息进行加密传输，即确保传输的数据是加密后传输。

2、静态数据加密

在静态数据保密性方面，一般通过密码加密技术实现数据存储过程中的保密性防护。对于特别重要的数据，使用数据加密系统或其他加密技术实现关键管理数据、鉴别信息以及重要业务数据存储的保密性。

##### 数据备份恢复

数据备份恢复作为网络安全的一个重要内容，其重要性却往往被人们忽视，只要发生数据传输、存储和交换，就有可能产生数据故障，如果没有采取数据备份和灾难恢复的手段与措施，就会导致数据丢失并有可能造成无法弥补的损失。一旦发生数据故障，组织就陷入困境，数据可能被损坏而无法识别，而允许恢复时间可能只有短短几天或更少。如果系统无法顺利恢复，最终可能会导致无法想象的后果。因此组织的信息化程度越高，数据备份和恢复的措施就越重要。

1、数据备份

数据备份是为了在系统出现故障时，能够确保恢复整个系统，因此需要制定详细的备份策略，明确何时进行备份、用什么备份方法、备份哪些数据等。

2、数据异地备份

从地理位置上来看，异地备份提供了一种新的备份方式，使得备份后的数据不一定要保存在本地，也可保存在网络上的另一服务器上，这种方式是将数据在另外的地方实时产生一份可用的副本，此副本的使用不需要做数据恢复，可立即投入使用。

3、数据恢复

恢复是备份的逆操作，但恢复的操作比备份复杂，也容易出问题。

备份与恢复包括两方面内容，一方面是数据备份与恢复，另一方面是重要数据处理系统（关键网络设备、安全设备、应用服务器和数据库服务器等）热冗余，重要数据处理系统的冗余对数据备份起到重大作用，为数据的备份和恢复提供支持，保证系统的高可用性。

##### 入侵检测和恶意代码防范

在重要的业务服务上部署操作系统免疫保护平台，采用可信计算主动防御机制，提供执行程序可信度量，阻止未授权及不符合预期的执行程序运行，实现对已知、新型恶意代码的主动防御，降低操作系统完整性及可用性被破坏的风险。从管理角度出发，提供程序安装接口，仅允许通过程序安装接口对操作系统的可信软件进行完整性安装，同时可以生成采集模板，经管理员授权批准，实现程序批量安装，从而阻止未知来源的软件、插件进行安装，保证节点系统安全、有效地运行。

##### 个人信息保护

等级保护对象中业务系统在需要采集个人信息时，应当仅采集和保存必需的用户个人信息，与业务无关的个人信息应当禁止被业务系统或其组件采集。可以采用上网行为管理等设备的部署或应用安全配置项，通过访问控制限制对用户信息的访问和使用进行限制，实现禁止未授权访问和非法使用用户个人信息。同时，组织应当按照等级保护相关要求，制定保障个人信息安全的管理制度和流程，严格按照个人信息保护管理制度和流程进行操作，对违反个人信息保护管理制度和流程的人员进行处罚，保障用户个人隐私数据信息和利益不受到侵害。

#### 安全管理体系设计

建立统一的信息安全管理体系，落实各项管理制度。所谓“三分技术，七分管理”，技术和产品是基础，安全管理是关键，建立一个优秀的安全管理框架，让好的安全策略在这个框架内可重复实施，才能实现等级保护对象的持续安全。从安全管理制度、安全管理策略等方面进行系统规划设计，建立统一的网络安全管理系统，落实各项管理制度，让用户的安全管理体系，有宏观的设计、有清晰的责任权限、有合理的制度要求。

##### 安全策略和管理制度

依据《网络安全等级保护基本要求》及组织网络安全管理工作的特点从安全策略、管理制度、制定和发布以及评审和修订等方面进行安全管理制度设计。

###### 安全策略

1、策略框架

建立一套关于物理、主机、网络、应用、数据、建设和管理等六个方面的安全需求、控制措施及执行程序，并在关联制度文档中定义出相关的安全角色，并对其赋予管理职责。

2、主机安全策略

登录操作系统和数据库系统的用户必须进行身份标识和鉴别；

操作系统和数据库系统管理用户身份标识不能出现同名用户，口令应有复杂度要求并定期更换；

操作系统和数据库系统必须启用登录失败处理功能；

对服务器进行远程管理时，必须采取必要措施，防止鉴别信息在网络传输过程中被窃听；

操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性，不能出重名情况；

操作系统和数据库必须及时删除多余的、过期的账户，避免共享账户的存在；

主机必须开启日志审计功能；

3、应用安全策略

应用系统必须在登录时要求输入用户名和口令；

登录应用系统必须进行两种或两种以上的复合身份验证方式；

应用系统中设置的用户都必须是用户，不能名称相同；

应用系统必须开启登录失败处理功能；

应用系统必须开启登录连接超时时自动退出等措施；

应用系统必须开启身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数；

应用系统必须开启日志审计功能；

应用系统存储用户信息的设备在销毁、修理或转做其他用途时，必须清楚内部存储信息。

4、数据安全策略

业务应用数据和设备配置文档都必须进行备份，以便发生问题时进行恢复；

数据备份至其他设备上时，必须使用专门的备份通道，保证数据传输的完整性；

数据本机备份时应检测其完整性；

数据备份时必须使用专业的备份设备和工具，在数据传输和数据存储时，都必须是加密传输和存储；

数据进行异地备份时，必须利用通信网络将关键数据定时批量传送至备用场地。

###### 管理制度

对安全管理活动中的各类管理内容建立安全管理制度，对管理人员或操作人员执行的日常管理操作建立操作规程，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系，从而指导并有效地规范信息安全管理工作。

### 设计规范

（1） 《电子政务术语》（GB/T 25647-2010）

（2） 《电子政务系统总体设计要求》（GB/T 21064-2007）

（3） 《电子政务业务流程设计方法 通用规范》（GB/T 19487-2004）

（4） 《信息安全技术 术语》（GB/T 25069-2010）

（5） 《网络型入侵防御产品技术要求和测试评价方法》（GB/T 28451-2012）

（6） 《IT网络安全 第1部分：网络安全管理》（GB/T 25068.1-2012）

（7） 《IT网络安全 第2部分：网络安全体系结构》（GB/T 25068.2-2012）

（8） 《IT网络安全 第3部分：使用安全网关的网间通信安全保护》（GB/T 25068.3-2010）

（9） 《IT网络安全 第4部分：远程接入的安全保护》（GB/T 25068.4-2010）

（10） 《IT网络安全 第5部分：使用虚拟专用网的跨网通信安全保护》（GB/T 25068.5-2010）

（11）《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）

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

（13）《信息安全技术网络安全等级保护测试评要求》（GB/T 28448-2019）

（14） 《信息安全技术网络安全等级保护设计技术要求》（GB/T 25070-2019）

（15） 《消防信息代码》（GA/T 974-2011）

（16） 《消防基础数据平台接口规范》（GA/T 1036-2012）

（17） 《消防公共服务平台技术规范》（GA/T 1038-2012）

（18） 《城市消防远程监控系统技术规范》（GB 50440—2007）

（19） 《城市消防远程监控系统》（GB 26875－2011）

（20） 《火警受理系统》（GB 16281-2010）

（21） 《消防通信指挥系统设计规范》（GB 50313—2013）

（22） 《移动消防指挥中心通用技术要求》（GB 25113-2010）

# 项目投资概算

## 资金来源与落实情况

本项目预算资金为333.60万元，由亳芜现代产业园区管委会支出。该项目分为软件服务定制开发、硬件设备、运营服务、消防检测服务、网络费、施工及耗材采购等相关服务内容，具体如下:

## 软件相关信息

软件功能清单如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **系统模块** | **建设内容** | **功能模块** |
| 1 | 智慧消防 | 维保管理 | 系统支持用户对应急维保订单和例行维保任务生成的报告进行管理与下载存档。 |
| 提供当前计划对应的单位名称、计划名称、开始结束时间、维修设备数等可查看功能。 |
| 提供基于后台监测到维保过程中触发设备报警及状态数据的对比和维保过程核实 |
| 维保监管 | 向维保单位提供维保过程监管及统计工具；支持维保过程实时数据的接入在消防安全管理Web系统同步展示。 |
| 自动生成维保过程指标包括维保及时性、设备更换率等。 |
| 支持针对现场维保人员、维保公司领导等不同角色的月度、年度与综合统计分析，并自动推送至大屏系统显示。 |
| 维保任务提醒 | 根据消防物联网监测异常数据，将异常设备信息推送至维保单位生成动态维保计划，确保维保工作能及时消除消防设备运行隐患。 |
| 在APP端提醒维保任务，系统滚动提示当前待完成的例行和应急维保任务，包括任务要求时间、任务对应业主单位、任务当前状态等 |
| 运营中心 | 支持运营中心工作人员对物联网监 测历史和实时全量信息的查询需要，展示物联网监测数据的全量信息，根据时间展示每条有效信号信息记录。 |
| 工作量统计 | 支持运营中心人员处置火警、故障、逾期、离岗等异常事件的工作量统计，可按年、按月、按日对隐患进行多维度统计分析，并推送至大屏系统可显示。 |
| 安消联动 | 基于消防设备和视频监控之间的相对位置关系，结合建筑平面图，建立安消联动算法模型。 |
| 实现平台安消联动方案。当设备报警时，可通过调用周边视频，第一时间了解现场情况；确认为真警时，画面自动跳转至关联的附近视频。 |
| 视频融合与存储 | 开发视频存储功能，将智慧亳芜智慧消防模块监控视频和本期新增联网单位新增视频监控数据，同步接入园区视频监控平台，支持实时视频查看功能，支持跨平台的统一调度查看（包括监管大屏系统、企业端平台），支持视频数据存储不低于2周。 |
| 2 | 智慧工地扩容完善 | 管理平台 | 智能物联综合管理平台，包括系统管理、视频管理、工地管理等业务系统。其中; 智能物联综合管理平台服务器硬件参数：1、处理器：IntelXeonE3-1225V5CPU;2、芯片组：IntelC236chipset，3、内存：DDR4内存条-8GB-VLP-ECC-UDIMM\*4;4、IO接口：1个DB-15VGA接口;4个千兆网口;1个BMC管理网口;支持后置2个USB3.0接口和前置2个USB3.0接口。智能物联综合管理平台，包括系统管理、视频管理、工地管理等业务系统。其中; 1、支持基础资源（组织、设备、人、卡、车等信息）管理，提供事件中心、数据存储、电子地图、日志记录等基础功能;2、支持标准开放平台，提供rest ful 等多维度接口，显示数据互联互通；3、支持光栅、矢量、3D 三种类型，不同厂家的地图；4、支持按照用户配置的权限过滤展示组织设备树、部门人员树、数据查询；6、数据看板-支持通过看板形式展示数据概览，多维度进行工地信息展示7、支持实时视频、录像回放、录像下载、电视墙、热成像;8、支持手机移动客户端进行实时视频监控，音频播放，本地截图，本地录像，云台控制，远程视频回放;9、工地基础数据管理，支持企业基础信息、企业资质、企业不良行为、企业良好行为、企业黑名单信息维护的增加、删除、修改、查询，企业基础信息支持导入与导出；10、项目展示，支持项目信息展示，包含:项目基础信息、参建企业、班组信息、民工工资、考勤展示，考勤展示中支持查看考勤明细，考勤展示信息支持导出；11、渣土车监管，支持配置车辆冲洗区域，支持冲洗记录上报，针对冲洗异常的情况可生成车辆冲洗异常报警记录，支持渣土车逆行检测上报；12、安全帽管理，支持安全帽检测记录上报，可检测有无佩戴；13、工服检测，支持未穿戴工服检测上报；支持检测记录支持按时间段、项目名称和检测地点模块检索；14、环境监测，支持地表裸土覆盖异常监测报警上报，支持按时间、项目名称、检测地点进行查询检索及结果导出；16、含平台软件、硬件服务器、支持500路视频接入通道、60个工地管理通道等。 |
| 3 | 智慧工地扩容完善 | 智能分析平台 | 1、主处理器：Intel I7-6700、64位4核8线程主频4GHz、内存：4根8GB 三星UDIMM DDR4内存；2、操作系统：国产欧拉操作系统，欧拉操作系统版本：21.09；3、接入路数：384路；4、硬盘接口：支持24个、SATA 3.0、单盘最大20TB；硬盘配置：4个8TB硬盘；5、网络带宽：1280Mbps接入、1280Mbps存储、1280Mbps转发；6、分辨率：32MP;24MP;16MP;12MP;8MP;6MP;5MP;4MP;3MP;1080p;720p7、解码能力：2路24MP，3路24MP(24fps)，4路16Mp(25fps)，7路12MP (20fps)，7路8MP (30fps)，14路8MP (15fps)，9路6MP(30fps)，11路5MP(30fps)，13路5MP (25fps)，14路4MP (30fps)，22路4MP (20fps)，18路3MP (30fps)，22路3MP (25fps)，14路1080p (60fps)，28路1080p (30fps)，63路720p (30fps)；8、电源接口：1+1冗余电源；9、网络接口：4个RJ-45，支持10/100/1000/2500Mbps自适应以太网口；10、视频输出：1路VGA输出，4路HDMI输出，其中VGA1和HDMI1同源输出支持4K显示；11、人数统计：配套前端摄像机，支持绊线人数统计；区域人数统计；排队人数统计；拥堵检测；12.支持识别吸烟、打电话、未戴安全帽、未穿工作服等违规操作人员，可联动录像、抓图、蜂鸣报警、邮件、本地报警输出、前端报警输出、门禁、音频以及日志记录；支持按姓名检索违规人员的具体个人信息；支持数据存储和按事件类型检索；支持查看违规操作人员的姓名(需提公安部检测报告的影印件或扫描件并加盖原厂公章)13、产品尺寸：机箱：446mm×543.4mm×175mm（宽×长×高）最大尺寸：482.6mm（含挂耳）×543.4mm×175mm（宽×长×高）；14、历史抓拍库容量：以各算法参数为准。；15、供电方式：100–127/200–240VAC,50/60Hz,7/3.5A；/1616、功耗：工作（满接硬盘）：≤420W工作（不含硬盘）：≤150W额定：≤800W17、算法：同时支持算法220路，其中区域入侵检测100路，人员聚集检测40路，安全帽、工装检测30路，烟火检测15路，裸土覆盖检测15路，渣土车清洗检测20路，算法支持在摄像机间调整，厂家提供授权账号供业主根据实际需要进行算法调整。 |

## 专业设备、网络、服务及相关资料

清单如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **系统模块** | **功能名称** | **设备参数** | **数量** | **单位** |
| 1 | 消防报警主机远程联网接入 | 用户信息传输装置（含协议卡） | 1、产品需取得应急管理部消防产品合格评定中心执行国家标准GB26875.1-2011《城市消防远程监控系统第1部分:用户信息传输装置》的消防产品认证证书。2、采用高性能4G无线模块，支持移动、联通或电信网络制式。3、交流输入电压220V50Hz，蓄电池备用供电（待机24小时以上），直流备电12V7Ah铅酸电池一节。4、设备功能支持：（1）手动报警：具有手动火警按钮，可以向管理平台上传人工火灾报警信息；（2）断网续传：网络断网恢复后，接续上传断网期间的数据；（3）值班查岗：支持值班查岗功能。5、设备最多可支持5台火灾自动报警主机的接入。支持WEB远程配置和本机显示屏配置两种配置方式。6、（1）设备接口支持：具有2路RS232，2路485，1路CAN通信口，1路RJ45口，2路开关量输出，1路开关量输入。设备通过增加输入输出模块，可拓展5路开关量输入和2路5V电源输出接口；通过增加串口模块，可拓展至4路RS232和4路RS485接口。（2）提供第三方CNAS或CMA认证报告。7、（1）投标人所投消防主机联网装置的电路有亚克力板保护，印有警示提示语。（2）提供第三方CNAS或CMA认证报告。8、支持查找历史记录：历史火警、历史请求/反馈、历史故障、历史操作各1000条。9、提供液晶显示（128x64），提供实时时钟。10、工作温度0℃～+50℃，工作湿度≤95%RH。 | 52 | 套 |
| 2 | 主机协议卡 | 根据现场消控主机品牌型号进行分析接入。 | 52 | 套 |
| 3 | 消防水系统监测 | 消防水系统监测综合网关（有线式） | 1、通讯方式：4G全网通无线通讯或RS485有线通讯。2、采集量类型及通道数：6通道开关量及12通道模拟量。3、MQTT协议，AES-128加密。 | 18 | 个 |
| 4 | 消防水系统监测综合网关（无线式） | 1、通讯方式：上行：LAN下行：RS485。2、接口：两路传感器接口，1路RS485,1路输入接口，RJ45，电源接口。3、工作温度：-20~70℃，工作湿度：5%~95%RH（无凝露）。4、防护等级：IP30。5、电量检测：支持电池电量显示功能。6、（1）多中心数据上报：能够同时向四个中心发送数据。（2）提供第三方CNAS或CMA认证报告。7、分体式结构：采用航空接头对接方式。 | 29 | 个 |
| 5 | 智能液位监测终端 | 1、供电电压：3.6VDC。2、（1）测量范围：0～10m水位；测量精度：±0.5%FS。（2）提供第三方CNAS或CMA认证报告。3、（1）工作环境：-20～65℃，0～100%RH。（2）提供测试报告。4、防护等级：IP68。5、通讯方式：4G。6、（1）防盐雾：8h。（2）参考标准GBIT10125-2021，提供第三方CNAS或CMA认证报告。7、安装方式：投入式。 | 53 | 个 |
| 6 | 液位监测终端 | 1、工作电压：24VDC。2、测量范围：0～10m水位。3、测量精度：±0.5%F.S。4、工作环境：-20～65℃，0～100%RH。5、防护等级：IP68。6、安装方式：投入式。 | 42 | 个 |
| 7 | 智能压力监测终端 | 1、供电电压：3.6VDC。2、（1）测量范围：0～1.6MPa，测量精度：±0.3%FS;防护等级：IP68。（2）提供第三方CNAS或CMA认证报告。3、工作环境：-20～65℃，0～100%RH4、通讯方式：NB-IoT或4G。 | 51 | 个 |
| 8 | 压力监测终端 | 1、工作电压：24VDC。2、测量范围：0～1.6MPa。3、测量精度：±0.5%FS。4、工作环境：-20～65℃，0～100%RH。5、防护等级IP68。 | 170 | 个 |
| 9 | 消防巡查标签 | 电子标签 | 1、通讯协议：ISO14443A。2、通信频率：14.6Mhz。3、通信距离：4.5-5cm。4、芯片容量：888字节。5、可擦写次数：10万次。6、使用温度：-10~50℃。 | 5500 | 个 |
| 10 | 视频智能分析应用 | 消控室在岗监测摄像机 | 1、智能报警：物理遮挡报警、电瓶车进电梯报警、室内通道堵塞报警、岗位值守情况报警、区域入侵、越界侦测。2、（1）具有状态指示灯，备绿灯指示正常状态，黄灯指示故障报警。（2）提供公安部或公安部授权机构的公安部检测报告。3、最大图像尺寸：2560×1440；传感器类型：1/2.7"ProgressiveScanCMOS。4、镜头：水平视场角104°，垂直视场角58°，对角视场角123°；调整角度：水平:0°~360°;垂直:0°~70°;旋转:0°~360°。5、存储功能：支持microSD/SDHC/SDXC卡(128G)断网本地存储及断网续传；异常侦测：遮挡报警,网线断,IP地址冲突,非法登录,存储器满,存储器错。6、（1）支持人员在离岗检测功能，当人员离开设定的监控区域，且时间达到设定值时，触发离岗告警，并上传现场抓拍照片，支持报警录像。（2）提供第三方CNAS或CMA认证报告。7、（1）可手动对镜头进行旋转0°~360°调节。（2）提供第三方CNAS或CMA认证报告。8、支持协议：TCP/IP,HTTP,HTTPS,DHCP,DNS,RTP,RTSP,RTCP，NTP，IPv4,UDP。9、接口协议：开放型网络视频接口ONVIF(PROFILES,PROFILEG),ISAPI,GB28181。10、屏蔽区域：可自定义配置4个矩形区域。11、报警接口：1路报警输入(Alarmin),1路报警输出(Alarmout,最大支持DC30V/1A或AC125V/0.3A)；音频接口：1路内置麦克风，1路内置扬声器；通讯接口：1个RJ4510M/100M自适应以太网口。12、电源：DC12V±25%，支持POE供电，标配电源适配器。13、使用环境：-10℃~40℃,湿度小于95%(无凝结)。 | 46 | 个 |
| 11 | 视频存储服务器 | 1、（1）具有2个HDMI接口、2个DP接口、2个V-DP接口、1个VGA接口、4个RJ452、5Gbps网络接口；2个USB2.0接口、4个USB3.0接口、1个RS232接口、1个RS485接口（可接入RS485键盘）、1个eSata接口；1+1冗余电源，1+1冗余风扇；具有1路音频输入接口、1路音频输出接口、16路报警输入接口、8路报警输出接口、可内置16块SATA3.0接口硬盘。可选配4个千兆网络光口;可选配2个V-SAS接口（可接入2个存储扩展柜）；前面板可选配1个7英寸LCD屏幕。（2）提供公安部或公安部授权机构的公安部检测报告。2、（1）可插拔式安装主板、风扇、电源模块，并且风扇、冗余电源模块可热插拔。（2）提供第三方CNAS或CMA认证报告。3、（1）支持最大接入带宽1024Mbps，最大存储带宽1024Mbps，最大转发带宽1024Mbps。（2）提供第三方CNAS或CMA认证报告。4、主板支持8通道输出，包括HDMI1、HDMI2、DP1、DP2、V-DP1、V-DP2、VGA和选配的前面板，各输出口均支持显示系统主菜单；且每路均可分别进行预览、录像、查看及配置操作。提供公安部出具的检测报告。5、（1）支持3种输出模式：4K模式、单8K模式和双8K模式。在4K模式下，支持选取HDMI1/HDMI2/DP1/DP2或者HDMI1/HDMI2/V-DP1/V-DP2作为输出口，输出4组异源4K(4096×2160)视频图像。在单8K模式下，支持选取DP1/DP2/V-DP1/V-DP2四个输出口中的任一个输出口为8K(7680×4320)输出口，HDMI1和HDMI2仍可为异源4K(4096×2160)输出。在双8K模式下，仅可选择DP1/DP2或者V-DP1/V-DP2输出异源双8K(7680×4320)视频图像。（2）提供第三方CNAS或CMA认证报告。6、（1）可同时显示输出64路2MP、H.265编码、25fps、1920×1080格式的视频图像。（2）提供第三方CNAS或CMA认证报告。7、（1）最大支持128个分屏预览；用户可自定义画面分屏。（2）提供第三方CNAS或CMA认证报告。8、（1）接入警戒摄像机，支持对IPC的声音和闪光参数进行配置，支持通过移动侦测、区域入侵、越界侦测、进入区域和离开区域事件联动一个或多个IPC的声光报警，可以对声光联动一键撤防。（2）以第三方CNAS或CMA认证报告为准。9、（1）可接入128路高空抛物行为检测摄像机，支持在预览界面实时展示高空抛物事件轨迹并弹窗回放轨迹信息。（2）提供第三方CNAS或CMA认证报告。10、（1）可实现高空抛物检测区域的隐私保护，自动过滤屏蔽区域内的抛物目标，支持设置最多8个隐私遮蔽区域；可手动预标定楼层，报警后自动匹配画面中疑似抛物的楼层信息。（2）提供第三方CNAS或CMA认证报告。11、含16个10T硬盘。 | 1 | 台 |
| 12 | 智慧消防分析仪 | 1、所投设备具有应急管理部消防产品合格评定中心出具的技术鉴定证书。2、分析路数：16路。3、智能分析功能：烟火检测、室内消防通道堵塞、室外消防通道堵塞、消控室岗位值守情况检测、消控室人员持证上岗检测、抽烟检测、电瓶车检测、灭火器检测。4、报警输入：16路开关量报警输入；报警输出：8路开关量报警输出。5、USB接口：2个USB2.0，1个USB3、0；音频接口：RCA接口，1路单声道输入和1路单声道输出；HDMI输出：1路HDMI高清视频信号输出，最大支持4K@60P；网口：2个千兆网口，10M/100M/1000M自适应；串行接口：1个RS232，1个RS485。6、（1）设备应有2个SATA数据接口，标配2块4TB容量的机械硬盘;设备应有USB数据接口，USB3.0接口数应大于等于1个，USB2.0接口数应大于等于2个。（2）提供第三方CNAS或CMA认证报告。7、硬盘容量：8TB；电源：220V；功耗：不超过120W。8、机箱规格：19英寸1、5U标准机箱。9、工作温度：-10℃~55℃；储藏温度：﹣40℃~＋70℃,；工作湿度：10％~90％，无凝露。 | 2 | 台 |
| 13 | 火灾烟雾探测 | 联网独立式烟感 | 1、工作原理：双光路、光电式感知技术。2、空间温湿度感知：支持。3、静态电流：≤15μA，报警电流：≤50mA。4、本地报警方式：声、光报警，报警音量：≥85dB@3m（A计权）。5、供电电压：DC3V，电池容量：2800mAh，锂电池CR17505，DC3.0V。6、通讯方式：NB-IoT。7、电池设计寿命：平均寿命5年。8、使用环境温度：-10℃～55℃；相对湿度：≤95%。9、执行标准：GB20517-2006。10、安装指示：信号查询、入网注册指示功能。11、系统设计规范GB50116-2013《火灾自动报警系统设计规范》。12、安装规范：GB50166-2019《火灾自动报警系统施工及验收标准》。13、（1）设备应具有1个红外光信号发射管、1个蓝光信号发射管、1个光信号接收管、1个温湿度传感器和1个红外遥控接收管等内部传感器。（2）提供第三方CNAS或CMA认证报告。14、（1）当蜂鸣器出现故障时，设备应能产生蜂鸣器故障报警，并上报至手机APP端与平台端。（2）提供第三方CNAS或CMA认证报告。15、（1）设备应具有抗水汽干扰功能；受试样品通电状态，放置在具有25℃、RH99%的环境下，持续4h；试验期间无误报情况发生。（2）提供第三方CNAS或CMA认证报告。 | 55 | 个 |
| 14 | 手动火灾报警按钮 | 联网手动火灾报警按钮 | 1、产品执行标准：GB19880-2005《手动火灾报警按钮》。2、工作原理：手动触发。通讯方式：4G。3、报警输出：1路，继电器容量（24VDC/1A）。4、电源：锂电池2400mAh，DC3V；电池使用寿命：平均3年（根据实际使用情况，电池寿命可能有所缩减）。5、工作电流：待机状态≤30μA，报警状态≤60mA。6、工作温度：0℃~55℃；工作湿度：≤95%。7、产品需符合GB19880-2005《手动火灾报警按钮》要求，并取得国家消防电子产品质量监督检验中心出具的型式试验报告。8、产品需符合GB19880-2005《手动火灾报警按钮》要求，取得应急管理部消防产品合格评定中心出具的强制性产品认证证书。9、产品需获得无线电发射设备型号核准证和进网许可证。 | 50 | 个 |
| 15 | 声光警报器 | 联网火灾声光警报器 | 1、产品执行标准：GB26851-2011《火灾声和/或光警报器》。2、通讯方式：4G。3、报警音量及声光方式：蜂鸣指示（75~115dB），消防变频音调声响。4、报警指示灯：1个，红色：报警，黄色：故障，绿色：状态。5、电源：主电：DC12V1A。6、工作电流：待机功耗18mA,≤60mA（触发状态下）。7、工作温度：0℃~55℃；工作湿度：≤95%。8、产品需符合GB26851-2011《火灾声和/或光警报器》要求，并取得国家消防电子产品质量监督检验中心出具的型式试验报告。9、产品需符合GB26851-2011《火灾声和/或光警报器》要求，取得应急管理部消防产品合格评定中心出具的强制性产品认证证书。10、产品需获得无线电发射设备型号核准证和进网许可证。 | 50 | 个 |
| 16 | 室外消火栓监测 | 室外消火栓监测终端 | 1、供电方式：锂亚电池供电。2、工作温度：-20~70℃，工作湿度：5%~95%RH(无凝露)。3、报警类型：支持水压上限报警、下限报警、波动报警、倾斜报警、碰撞报警、支持偷盗报。4、设备使用法兰盘的安装方式，支持DN100和DN150的口径，DN100的法兰盘采用椭圆孔，可兼容外径205和225法兰盘。5、（1）主机和传感器采用防护电源线连接，可根据项目现场定制不同的长度。（2）提供第三方CNAS或CMA认证报告。6、（1）设备具备太阳能和锂亚电池供电模式（可选配理亚电池单独供电模式）。（2）提供第三方CNAS或CMA认证报告。7、本地调试：蓝牙实现升级和调试。参数配置：支持远程配置设备参数。8、安装方式：法兰盘式安装，不破坏原有的结构。9、通讯方式：采用NB通讯方式。10、防护等级：IP68。 | 29 | 个 |
| 17 | 网络设备 | 路由器 | 千兆有线：1个千兆WAN口，4个千兆LAN口。 | 46 | 个 |

## 其它服务

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **描述** | **数量** | **单位** | **备注** |
| 1 | 智慧消防运维运营服务 | 消防物联网设备运维运营服务（包括监测设备通信、设备维修、定期巡查、电池更换、设备资产信息维护等）；软件平台运维，平台数据运营服务，定期提供数据分析报告 | 3 | 年 | 7\*24小时监测值守（至少2人同时值守、三班次轮流）。工作日同步管委会上班时间安排1人在亳芜运营中心值班（无需提供社保）。 |
| 2 | 消防检测服务 | 本次消防检测聘请第三方专业有资质的服务机构，给园区接入平台的企业，包含亳芜智慧消防一期和二期的所有单位（101家单位），进行三年的消防检测服务，每年每家单位至少进行一次检测服务。(包括火灾自动报警系统、消防给水、室内外消火栓系统、应急疏散系统等)，出具消防检测报告。 | 3 | 年 | / |
| 3 | 网络通信服务（含三年通讯服务） | 4G物联网卡100M/月。 | 47 | 张 | 含三年费用 |
| 4 | NB物联网卡100M/月。 | 278 | 张 | 含三年费用 |
| 5 | 数据专网接入100M。 | 46 | 套 | 含三年费用 |
| 6 | 单位消防电子档案 | 联网单位消防图纸录入、主机信息采集标注、非主机点位录入等。 | 1 | 项 | / |
| 7 | 系统集成 | 硬件设备安装、调试（含辅材）。 | 1 | 项 | / |

备注：所有检测报告检测时间需在投标截止日期前，否则视为无效报告；评分办法服务团队要求的人员需提供近半年（开标之日起上推6个月）投标人为其连续缴纳的3个月社保证明（社保管理单位出具）。

# 项目管理

## 项目管理体系

### 领导和管理机构

为了保证项目高质量如期完成，项目建设过程中必须采取严格和科学的管理手段，成立专门的项目组织机构，有效地组织与管理工程建设。同时，项目引入监理制度，对项目的投资、建设、招投标、进度、质量目标等内容进行全程监理。本项目建设将成立领导和管理机构、规划设计机构、项目实施机构、运行维护机构，确保项目的顺利进行。



图 20 项目建设管理组织机构

为了确保本项目顺利开展，成立建设领导小组，在领导小组的指导下，按照规划设计组编制的总体规划要求，开展项目的设计和建设。由平台建设小组负责项目指导和协调工作，保障项目建设顺利进行。本项目建设小组协调各部门间的关系，处理其它有关设计和建设的重大问题，并对各方工作开展情况进行监督。

### 项目实施机构



 图 21 项目实施机构架构图

项目建设由三个工作小组具体负责，其主要分工如下：

1、综合协调小组：负责协调开展系统建设工作，负责系统运行相关管理制度制订和系统实施组织管理工作。

2、技术开发小组：负责项目的业务需求分析和技术方案设计论证工作，负责信息资源共享和互联接口的开发协调工作，负责项目的技术管理、宣传培训和技术验收工作。

3、立项投资小组：负责项目立项申报工作、项目招标工作、财务管理工作和项目审计报送工作。

4、建立例会制度：工作小组每周定期召开工作推进例会，研究解决工作中出现的实际问题。

### 人员配置计划

项目承建单位主要职责：按照项目合同要求，按时、保质地完成项目承研、建设、培训、质量保证等各项任务和工作；协助建设单位完成各项技术保证和售后服务工作等。

承建单位将组成项目团队，由不同层次的人员组成，包括：资深项目负责人、系统设计人员、程序开发人员、系统测试人员等。

### 人员培训方案

为了保障项目的实施、应用和后继维护工作的顺利进行，伴随着项目的实施和试运行过程中，让用户更快速、方便、有效地掌握、需提供整套培训计划，对使用人员进行全面技术培训。培训内容以系统（含软硬件）技术性能、使用、测试、维护及故障排除为主，同时用户根据实际需求自由选择、自由组合，以确保在最短的时间内掌握和精通系统运行维护管理。分别对部门的管理人员、系统维护人员、系统使用人员进行不同层次的培训和宣传，利用扎实的培训促进信息系统应用管理工作。

培训的目的是提高用户的使用技能，加强用户对产品设备和系统的理解，使他们能够有效地履行产品设备的操作和系统的管理职责。

需按以下步骤对用户进行培训：

1、制定培训计划：在培训计划中确定培训目的，培训时间，培训地点，培训方式，课程设计。

2、确定培训对象：通常接受培训的人员是本工程项目涉及和影响的部门和个人，包括客户方高级管理者，使用用户，潜在用户及其部门管理人员。

3、培训内容和资料：包括与工程项目相关的操作手册、使用手册、实施方法和步骤等项目交付成果的使用说明等相关课程内容和资料。

4、培训的方式和方法：根据条件尽量采用可重复的，便捷的方式进行，包括课堂讲解，计算机辅助教学，在培训者指导下的自学，操作等。

5、培训设施：包括运行环境，可重复的联系环境等。

6、培训效果评价：确定受训人员的满意的完成准则，收集，评审培训的反馈信息，对培训效果进行评价，以便考虑培训的改进措施。

7、培训记录：保存培训的全程记录，包括所有人员的培训课程和培训活动记录，以便为岗位选择合适人选。

## 项目建设周期

本项目建设周期为180日历天，分四个阶段。

第一阶段：项目准备阶段（10日历天）

完成项目的需求调研、方案评优、方案评审、数据资料整理等工作。

第二阶段：建设实施阶段（145日历天）

开展项目平台设计、应用软件开发、联网单位建设等工作，完成感知网试点部署及数据接入等工作，完成系统的部署、系统用户的培训。

第三阶段：试运行阶段（15日历天）

项目实施工作完成后进入系统试运行阶段，按照项目有关技术规范，整理系统试运行记录，并对试运行期间出现的系统问题进行及时修复。

第四阶段：项目验收阶段（10日历天）

项目试运行结束即进入项目验收阶段，承建单位按照项目相关技术规范、验收方法、验收步骤等准备项目验收文档资料，向建设单位申请项目竣工验收，通过验收后，系统正式上线投入运行。

## 项目进度计划

表 实施计划安排表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目** | **主要内容** | **所需时间** | **阶段成果** | **备注** |
| 1 | 需求调研深化设计 | 需求调研深化设计 | 14天 | 需求调研 | 交付需求调研计划 |
| 2 | 系统开发、设备安装调试 | 系统设计、开发编码以及研发自测，设备安装调试 | 60天 | 完成开发 | 交付代码与单位联网接入 |
| 3 | 系统测试 | 系统内部联调测试、调整 | 14天 | 完成联调测试，代码调整 | 软硬件联调 |
| 4 | 系统部署 | 系统的现场部署安装调试 | 7天 | 完成系统现场安装调试 |  |
| 5 | 系统培训 | 系统培训 | 7天 |  | 与系统部署同步进行 |
| 6 | 试运行 | 系统试运行 | 14天 | 系统试运行 |
| 7 | 项目验收 | 系统、文档验收 | 7天 | 完成项目最终验收 |

## 质量管理与控制

1、按照质量管理体系标准要求，贯彻落实项目的各个质量环节，确保项目的顺利验收。

2、项目启动后，须在项目计划中制定项目质量计划，确定质量目标和质量控制措施，让项目组成员明确自己的工作质量标准和要求，并对项目全过程实施有效的质量控制，做好质量记录。

3、组织开展需求调研，保证实施方案满足需求和相关政策、标准和规范要求。

4、加强对项目正式文档和过程文档的管理，项目验收时要把所有文档都归档。

## 风险分析与管理

### 风险识别与分析

为确保成熟稳定，本平台采用的相关技术和产品，在许多地区都有成功应用案例，并收获了很好的建设成效，因此项目风险较低。但由于项目建设的复杂性，仍存在部分潜在风险因素。

项目可能的潜在风险因素：

1. 需求范围不确定风险

由于该项目涉及的用户业务工作范围比较广，应用部门比较多，时间紧、任务重，在项目初期与用户交流不够充分，因此在项目成本、进度、质量等方面存在较大风险。

1. 需求变更频繁风险

由于项目建设内容理念新，在项目初期用户不能提供完整，明确的需求。项目组在与诸多用户单位沟通迭代过程中，不断修订完善建设方案。但由于项目内容前沿，国际国内均没有参考案例，用户需求仍存在变更的风险。

1. 设计通用性风险

该项目在需求上既需要考虑首装用户的需求，又要考虑将来列装各部门的通用性要求，若平台功能设计过于特殊化，就导致系统适应性降低，可扩展性较弱，业务需求的细致变化都可能带来巨大的维护工作量，导致维护成本增加。反之，若设计时采用过于灵活和通用的软件结构，会使系统复杂性上升，实现难度增加，进而在实现和测试阶段带来风险。

1. 数据集成风险

由于该项目是综合信息化平台，各系统采用的技术体制及数据库都存在差别，数据格式各不相同，以及部分数据较敏感无法接入平台，给数据集成带来一定风险。

1. 资金风险

本项目建设、采购设备资金需求量较大，在项目建设过程中，如果资金不及

时到位，将导致建设工期延长，工程造价升高，甚至可能导致项目建设停滞，从而影响项目的顺利建设及设备采购与投入运营，进而影响原定投资效益目标的实现。

1. 部门责权划分对系统的业务覆盖不全或界定不清的风险

系统涉及各业务部门间的业务协同与综合管理，必然会出现业务部门的现有责权无法覆盖系统中部分业务或者互有交叉界定不清的情况，使得系统部分业务功能的无法确定用户。

1. 组织风险

组织风险主要包括由于组织内部成员对目标未达成一致，管理高层对项目不重视，工程参与人员知识与技能欠缺、团队合作精神不足、人员激励机制不当等因素导致建设队伍不稳定，建设资金不足，与其它项目存在资源冲突等。

1. 项目管理风险

在项目实施中无法有效控制各项开发建设成本费用和建设的进度，将造成投资成本的增加以及工期的延长，增加项目的风险，影响项目的财务效益。

1. 操作风险

操作风险主要是来自项目建设实施工作中，主要表现在施工单位与用户在项目实施过程中的密切配合程度，是直接影响到项目能按期、按质量完成的关键，具有一定的实施操作风险。

### 风险对策与管理

为规避相应风险因素，采取以下措施：

1、增加与用户交流沟通，在需求分析阶段，尽可能让用户多参与，通过需求评审、需求确认的方式尽可能界定需求范围，达成双方共识。

2、一方面在业务建模阶段多让用户参与，及时得到反馈意见，达成共识；另一方面及时做好变更控制和配置管理工作，及时针对需求变化，更新相应设计，降低风险造成的影响。

3、广泛听取各方用户的意见和需求，了解各类前沿开发技术，综合分析，谨慎确定，在通用性和特殊性上做出权衡。

4、深入、细致地分析各系统数据库技术体制及数据内容，采取多种技术手段尽可能降低该风险造成的影响。

5、充分完善资金使用规划，注重资金来源之间的合理期限搭配，搞好资金流量的安排，注重优化资金使用结构，从总体上减少资金风险。

6、针对各业务部门的当前责权划分对智慧消防的业务覆盖不全或界定不清的风险，需与各业务部门加强沟通，促进与智慧消防相适应的管理机制创新及政策法规建立。

7、本项目设立项目建设领导小组，由亳芜产业园管委会领导、安全应急部门领导、各共建、成员单位领导等组成，共同参与项目建设管理过程。现有行政组织架构能够支撑本项目的项目管理，并为本项目建设成立了领导小组为核心的决策机制。将有效地保障本项目建设的项目管理更加高效。

8、为确保工程管理的高效率，将对项目进行有效策划，制定并落实严格的项目实施具体计划，应用先进管理工具和方法提高进度计划管理、跟踪水平。同时将借鉴行业项目管理实践的经验，合理估算项目工作量，明确项目间依赖关系和先后顺序，突出关键项目，进一步分解项目工作任务，使每个里程碑阶段均应有工作量估算、时间进度、以及可操作、可管理和可检查的交付物。

9、提高建设方与实施方的双方对项目重视程度与配合密切度来减少操作风险。

综上所述，通过合理的规划设计和有力的推进管理，平台建设能够有效规避风险，达到预期的建设目标并充分发挥建设成效。

## 运行维护方案

### 运维管理规范

建设单位组建运行维护机构，在工作领导小组的领导下，将全面负责本平台的运行、维护和组织管理。

### 运维服务内容

在运维期内，能实时响应系统故障，接到故障电话后，运维人员及时对故障进行评估，对于普通问题，运维人员1小时内响应，提供远程支持服务；对于较严重问题，如出现报错或报警，但业务能继续运行且性能影响较小的，运维人员在半小时内响应，4小时内提出故障处理方案并跟踪故障处理流程；对于紧急问题，如系统崩溃、业务停止、服务中断等，运维人员20分钟内响应，2小时内提供故障处理方案并跟踪故障处理流程。

### 运维服务提供方式

本项目提供以下三种方式的运维服务：

1、远程维护。通过网络、电话、电子邮件、传真等方式进行系统故障的处置、技术支持、咨询服务等工作。

2、定期巡查。定期对系统进行全面检查，优化系统，同时做好各类系统运行情况的记录。

3、运维培训。可根据需求，在现场对用户进行系统管理、日常维护及使用操作等方面的培训。

### 运维服务工作量估算

项目过保后的硬件设备维护和软件升级更新，所需的维护费用从每年的信息系统常态运行经费中考虑。

运维服务工作量估算如下：

| **名称** | **序号** | **相关内容** | **维护要求** | **备注说明** |
| --- | --- | --- | --- | --- |
| 一、应用系统 |
| 业务系统等 | 1 | 系统性能日常维护 | 定期巡检（周期：月）或按需提供 | 定期补丁升级、日志检查分析、错误分析及统计 |
| 2 | 系统故障检测及排除 | 响应时间及排除故障时间 | 按照单位的业务保障需求提供 |
| 3 | 系统运行状态监控及预警 | 监控具体指标内容 | 可作为日常管理项目考虑 |
| 4 | 系统重部署及调试 | 内容及时间要求 | 按照单位的业务保障需求，可纳入系统故障检测及排除的项目考虑 |
| 5 | 二次开发 | 开发相关需求，实施周期 | 包括原系统基础上对功能或接口等开发，按开发量评估 |
| 6 | 应用软件业务定制服务 | 根据具体的需求，针对应用系统相关适应性开展定制调整服务，如OA中的流程整理等。 | 根据具体工作量评估 |
| 7 | 系统性能优化 | 数据分离、数据优化、代码适应性优化、系统优化 | 根据具体工作量评估 |
| 二、其他内容与服务 |
| 综合管理 | 1 | 人员技能培训 | 人/次/项 | 运维管理培训、技术培训等 |
| 2 | 其他 | 　 | 未纳入本表描述的其他项目 |
| 运维咨询 | 1 | 管理体系咨询 | 运维规划设计咨询、服务管理现状评估分析，体系实施规划与设计、管理制度与业务流程设计，体系推广与认证，服务成果审计等 |  |
| 安全服务 | 1 | 信息系统安全服务 | 日常监控、安全漏洞扫描、安全风险评估、安全加固等；安全保护等级相应的服务。 |  |

### 应急措施

#### 网络安全事件分类

根据网络安全事件的发生原因、性质和机理，主要分为以下三类：

1、攻击类事件：指网络系统因计算机病毒感染、非法入侵等导致业务中断、系统宕机、网络瘫痪等情况。

2、故障类事件：指网络系统因计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪等情况。

3、灾害类事件：指因爆炸、火灾、雷击、地震、台风等外力因素导致网络系统损毁，造成业务中断、系统宕机、网络瘫痪等情况。

#### 应急联动机制

发生故障时，成立网络安全应急工作小组，按照“谁主管谁负责”原则；对于一般故障，维护人员应先在管理范围内排查故障，再排查互联系统故障，查明原因。对于较大故障，应安排技术骨干前往处理；对于特别重大或重大故障，需要报相关单位领导。

运行维护人员在处理故障时，必须对现场各种告警信息、故障显示、故障记录报告等进行认真分析处理，应不影响正在使用的业务或任意扩大影响范围，并严格按照故障处理相关办法进行处理。在处理故障时，未经上级运行维护部门同意，不得擅自对关键设备进行重启，以免造成更大范围的影响。

因本项目不涉及自建云计算及网络通讯系统，当出现云计算资源及网络系统故障时，将第一时间通告相关机构进行应急处置。

#### 应急处理流程

出现灾情后值班人员要及时通过电话、传真、邮件、短信等方式通知单位领导及相关技术负责人。 值班人员根据灾情信息，初步判定灾情程度。能够自身解决，要及时加以解决；如果不能自行解决故障，由领导现场指挥，协调各部门力量，按照分工负责的原则，组织相关技术人员进入抢险程序。

一般应急处理流程如下图：



图 5‑98 应急处理流程

#### 应急处理措施

1、黑客攻击事件紧急处置措施

当有关值班人员发现发现有黑客正在进行攻击时，应立即向网络安全应急负责人通报情况。

网络安全应急相关负责人应在接到通知后立即赶到现场，并首先将被攻击的服务器等设备从网络中隔离出来，保护现场，并将有关情况向本单位领导汇报。

对现场进行分析，并写出分析报告存档，必要时上报主管部门。

恢复与重建被攻击或破坏系统

网络安全应急小组组长召开小组会议，如认为事态严重，则立即向主管部门和公安部门报警。

2、病毒事件紧急处置措施

当发现有计算机被感染上病毒后，应立即向网络安全应急负责人报告，将该机从网络上隔离开来。

网络安全应急相关负责人员在接到通报后立即赶到现场。

对该设备的硬盘进行数据备份。

启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。

如果现行反病毒软件无法清除该病毒，应立即向本单位领导报告，并迅速联系有关产品商研究解决。

网络安全应急小组经会商，认为情况严重的，应立即向主管部门和公安部门报警。

如果感染病毒的设备是主服务器，经本单位领导同意，应立即告知各部门做好相应的清查工作。

3、软件系统遭破坏性攻击的紧急处置措施

重要的软件系统平时必须存有备份，与软件系统相对应的数据必须按本单位容灾备份规定的间隔按时进行备份，并将它们保存于安全处。

一旦软件遭到破坏性攻击，应立即向网络安全应急负责人报告，并将该系统停止运行。

检查信息系统的日志等资料，确定攻击来源，并将有关情况向领导汇报，再恢复软件系统和数据。

网络安全应急小组组长召开小组会议，如认为事态严重，则立即向主管部门和公安部门报警。

4、数据库安全紧急处置措施

在有条件的地区，主要数据库系统应按双机热备设置，并至少要准备两个以上数据库备份，平时一个备份放在机房，另一个备份放在另一安全的建筑物中。

一旦数据库崩溃，值班人员应立即启动备用系统，并向网络安全应急负责人报告。

在备用系统运行期间；信息安全工作人员应对主机系统进行维修并作数据恢复。

如果两套系统均崩溃而无法恢复，应立即向有关厂商请求紧急支援。

5、广域网外部线路中断紧急处置措施

广域网主、备用线路中断一条后，值班人员应立即启动备用线路接续工作，同时向网络安全应急负责人报告。

网络安全应急相关负责人员接到报告后，应迅速判断故障节点，查明故障原因。

如属我方管辖范围，由工作人员立即予以恢复。

如属电信部门管辖范围，立即与电信维护部门联系，要求修复。

如果主、备用线路同时中断，网络安全应急相关负责人应在判断故障节点，查明故障原因后，尽快研究恢复措施，并立即向本单位领导汇报。

6、局域网中断紧急处置措施

设备管理部门平时应准备好网络备用设备，存放在指定的位置。

局域网中断后，网络安全应急相关负责人员应立即判断故节点，查明故障原因，并向网络安全应急组组长汇报。

如属线路故障，应重新安装线路。

如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

如有必要，应向主管部门领导汇报。

7、设备安全紧急处置措施

服务器等关键设备损坏后，值班人员应立即向网络安全应急负责人报告。

网络安全应急相关负责人员立即查明原因。

如果能够自行恢复，应立即用备件替换受损部件。

如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

如果设备一时不能修复，应向本单位领导汇报。

8、停电紧急处置措施

（1）定期检查机房供电设备的运行状况和电路线缆器材情况，当发生下列突发事件时，按照以下方案进行处置：

（2）当机房发生市电供电突然停电或是电源异常时。首先应和馆内强电部门联系确认正常停电以及预计停电时间。检查不间断电源的电池可供电时间，确保设备正常运行，如遇到突然断电，应及时将空调等不在UPS电源供电范围内的设备及时断电，预防突然来电时瞬间电流过大导致设备损坏等现象。

（3）当确定停电时间超出机房UPS承载范围后，首先确定停电的范围以及受影响的设备范围。并及时通知各部门和网络安全应急小组做好停电应急准备。然后通知机房电源维护人和设备的负责人到达现场，做好各设备的电源停电准备。在UPS供电电量仅剩10%之后，严格按操作手册停掉各服务器的电源，最后停核心交换机和路由器，等待电力恢复。

（4）当确定停电原因是在本身供电系统范围内，立即汇报给负责领导，并及时联系相关维护人员达到现场检修。对于恢复时间无法预计的，要通知各部门做好停电应急准备。

（5）恢复供电后，严格按照操作程序逐步恢复机房设备和UPS的供电，以防瞬间电流过大造成设备损坏。

9、火灾紧急处置措施

（1）上班工作时间发生火警，还在机房工作的人员应及时紧急撤离，并立刻拨打119报警并立刻通知网络安全应急相关负责人和相关部门领导。在确保自身安全的情况下，应尽量使用灭火器进行灭火，减少电子设备的损坏。同时采取关闭电源总闸等措施，尽量减少可能造成的损失和破坏。

（2）非工作时间或节假日休息时间值班人员发现火情后，要立刻拨打119报警，并立刻通知网络安全应急相关负责人和相关部门领导，做好火灾的处置工作。

（3）火情结束之后，机房相关人员应全体赶赴现场，并向相关部门汇报。同时立即联系电信、联通、移动等相关网络公司和设备相关厂家，及时评估事故损失情况，研讨恢复网络系统正常运行的最佳解决方案。

10、其他自然灾害紧急处置措施

发生自然灾害后，首先应该组织人员撤离现场。当确认灾害不会造成人生伤害后，在回到机房检查设备，评估灾害受损范围，立刻向网络安全应急小组组长和公司领导汇报，并联系相关网络和设备厂家，积极做好灾后恢复工作，确保在最短时间内恢复机房正常运行。

11、发生盗抢事件紧急处置措施

发生盗抢事件后，要保护好现场然后报警，并向网络安全应急小组组长和市公司领导汇报情况。待现场处理完毕后，要组织相关人员估计损毁情况，并联系相关网络和设备厂家，积极做好恢复工作。

# 效益分析

## 经济效益

本项目按照“急需、适用、先进”的原则，推进亳芜产业园消防救援信息化、智能化的普及和应用，有利于直接推动亳芜产业园消防信息资源共享，保障人民群众生命安全和财产安全，提升业务工作开展、业务管理决策的效率和准确性，客观上也将在相关平台人员的工作强度、工作时间，以及消耗成本方面产生综合经济效益。

1、减少财产损失和人员伤亡

本项目重点针对防火重点单位、人群密集场所、火灾高危单位和火灾隐患较高场所监控，能够及时预警重大隐患，有效提高这些场所的火灾管控水平，预计未来五年能够降低25%到40%的火灾起数，预计能够减少经济损失1亿元，减少人员死亡人。

2、提升工作效率，弥补消防防火力量不足

消防监管和救援人员存在较大缺口，通过本项目建设，可减少各部门业务数据采集、处理、统计分析的工作量，降低办公成本；通过物联网技术手段及时获取消防管理动态情况，有效减少管理部门非常规巡查的次数，降低人力成本和动力消耗；同时通过对消防大数据挖掘分析，提高防火的科学性，因此，本项目建设将能有效弥补支队防火力量不足问题。

## 社会效益

目前亳芜产业园消防安全工作形势的严峻性和紧迫性，为最大限度地保障人民群众生命财产安全，防止失控漏管，提高对全社会的消防管理水平和能力，在目前信息共享不足、社会管理信息化平台建设需求急迫的现实情况下，建设亳芜产业园智慧消防系统，对于加大、加强消防部门的监督、管理手段和力度，提高企事业单位火灾预防能力，最大限度地减少社会和人民群众生命财产的安全十分重要和现实的意义。

本项目立足满足火灾防控“自动化”、感知网络“全覆盖”的实际需求，大力借助和推广大数据、物联网、地理信息等新一代信息技术，创新消防管理模式，实现消防业务重构。

本项目建设早抓一步就能先人一步，就能抢占创新型城市建设的制高点、战略性新兴产业的制高点、城市未来发展的制高点。本项目将现代信息技术与消防工作紧密融合，把科技应用能力作为核心战斗力来抓，不断创新消防管理方式方法，有效提升了社会火灾防控水平。将火灾防控纳入当地科技信息化建设总体规划，借助物联网、大数据、云计算、移动互联网等技术手段，不断提升消防工作的科技化、信息化和智能化水平。

1、适应经济社会发展需求、创新消防管理方式方法

经过多年的发展，信息化已经成为维持城市稳定运行、保障经济健康发展、改善市民生活品质、提高行政效能的重要支撑。在新的发展阶段，通过信息化手段实现消防大数据实时采集，消防信息一网打尽；通过物联网让消防安全监管动态化、火灾防控现代化、监管手段多元化；利用大数据云计算为实战提供“精准化”服务，灭火救援高效化。通过技术创新，打造基于大数据、物联网、云计算的“防消互联”新模式。

2、打通数据壁垒，实现资源整合、构建消防感知网

消防数据每天，每小时，甚至每分每秒都在快速变化着，以感知网建设为依托，整合全市消防设施、消防力量和视频监控、城市部件、管线、学校、物业等信息资源，利用地理信息展现技术，在基层管理、资源配置、信息研判和应急管理等方面，逐步实现从静态管控到动态管控，从单一管理到综合管理利用，依托亳芜产业园智慧消防体系，打破各部门信息壁垒，提高消防业务处理效率，充分发挥社会力量参与社会管理的基础作用，实现消防工作的大融合，改进消防管理方式，和电子政务其他信息系统互联互通，高度共享，彻底打破信息壁垒。

3、创新驱动融合共享，开创消防工作全新大格局

本项目建设将实现消防大数据实时采集，多元化化信息交互，消防设备物联网实效运用，动态化安全监管，融合共享现代科技，全面呈现着一年365天全部所有消防相关信息和运行轨迹，实现了信息共建共享、互联互通、监管群防群治、实时实效、救援联勤联动、精确精准，开创互联网与大数据时代消防工作全新大格局。