智慧消防平台项目

初步设计（代可研）

湖南天道信息技术咨询有限公司

二〇二五年三月

编制单位：湖南天道信息技术咨询有限公司

资质证书：工程咨询单位甲级资信证书

发证机关：中国工程咨询协会

资质证书等级：甲级

证书编号：91430102785381578S-18ZYJ18

法定代表人：谭塘芳

技术负责人：龚银元

项目负责人：申 光

编制人员名单

编制：申光　邱伟良 肖勇

校验：文秀

审核：邱伟良

审定：龚银元

批准：谭塘芳

注册工程师章印：

目 录

第一章　项目简介

1.1　项目名称

智慧消防平台项目（以下简称本项目）。

1.2　项目建设单位

项目建设单位：浏阳汇远实业有限公司

1.3　编制单位

编制单位：湖南天道信息技术咨询有限公司

发证机关：中华人民共和国国家发展和改革委员会中国工程咨询协会

资信等级：甲级

资信证书编号：914301027853815785-18ZYJ18

1.4　编制依据

1.4.1　国家及省市政策指导依据

1. 公安部消防局《公安部消防局2017年工作要点》（公消〔2016〕411号）；
2. 公安部消防局《关于全面推进“智慧消防”建设的指导意见》（公消〔2017〕297号）；
3. 国务院《关于深化消防执法改革的意见》（厅字〔2019〕34号）；
4. 国务院安委会《全国安全生产专项整治三年行动计划》（安委〔2020〕3号）；
5. 工信部办公厅《关于推动工业互联网加快发展的通知》（工信厅信管〔2020〕8号）；
6. 工信部、应急管理部《“工业互联网+安全生产”行动计划（2021-2023年）》（工信部联信发〔2020〕157号）；
7. 浙江省人大代表常委会《关于修改浙江省消防条例的决定》（浙江省第十三届人民代表大会常务委员会公告第64号）；

8. 广东省人大代表常委会《广东省实施〈中华人民共和国消防法〉办法》（广东省第十三届人民代表大会常务委员会公告第107号）；
9. 新疆维吾尔自治区人大代表常委会《关于修改新疆维吾尔自治区消防条例的决定》（新疆维吾尔自治区第十三届人民代表大会常务委员会第三十四次会议）；
10. 国务院安委会《“十四五”国家消防工作规划》（安委〔2022〕2号）；
11. 广西壮族自治区人大代表常委会《广西壮族自治区实施〈中华人民共和国消防法〉办法》（广西壮族自治区第十四届人民代表大会常务委员会第三次会议）；
12. 福建省人大代表常委会《福建省消防条例》（福建省第十四届人民代表大会常务委员会第四次会议修改）；
13. 重庆市人大代表常委会《重庆市消防条例》（重庆市第六届人民代表大会常务委员会第七次会议）；
14. 海南省人民政府《海南省消防安全责任制规定》（海南省人民政府令第323号）；
15. 湖南消安委《湖南省“十四五”消防救援事业发展规划》（湘消安〔2021〕5号）；
16. 长沙人民政府办公厅《关于印发长沙市“十四五”应急管理和安全生产规划 （2021—2025年） 的通知》（长政办发〔2021〕74号）；
17. 国务院安委会《安全生产治本攻坚三年行动方案（2024—2026年）》（安委〔2024〕2号）。

1.4.2 相关技术标准及规范

1. 《中华人民共和国个人信息保护法》；
2. 《消防设施通用规范》（GB55036-2022）；
3. 《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）；
4. 《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）；
5. 《国家电子政务信息安全标准化工作规范》（GW0102-2014）；
6. 《国家电子政务外网安全接入平台技术规范》（GW0202-2014）；

7. 《国家电子政务外网信息安全标准体系框架》（GW0101-2014）；
8. 《接入政务外网的局域网安全技术规范》（GW0206-2014）；
9. 《计算机软件需求规格说明规范》（GB/T9385-2008）；
10. 《计算机软件测试文件编制规范》（GB/T9386-2008）；
11. 《计算机软件产品开发文件编制指南》（GB/T8567-2006）；
12. 《长沙市政府投资信息化建设项目管理办法》（长政办发〔2021〕20 号）；
13. 《长沙市政务数据资源管理办法》（长政办发〔2021〕80 号）；
14. 《长沙市政务信息资源共享管理办法》（长政办发〔2018〕22 号）；
15. 《信息安全技术电子文件密码应用指南》（GB/T38541-2020）；
16. 《信息安全技术动态口令密码应用技术规范》（GB/T38556-2020）；
17. 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）；
18. 《信息安全技术数据库管理系统安全技术要求》（GB/T20273-2019）；
19. 《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）；
20. 《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）；
21. 《长沙市政务信息项目及系统命名规范》（CSDZ10027-2019）；
22. 《电子政务工程建设项目项目建议书编制规范》（CSDZ 10015-2018）；
23. 《长沙市电子政务服务标准体系》（CSDZ10001-2018）；
24. 《电子政务服务标准化工作指南》（CSDZ10002-2018）；
25. 《政务信息资源目录编目规则》（CSDZ10003-2018）；
26. 《政务信息资源提供方编码》（CSDZ10004-2018）；
27. 《政务信息资源分类与代码》（CSDZ10005-2018）；
28. 《云平台应用部署规范》（CSDZ10011-2018）；
29. 《电子政务系统第三方测试规范》（CSDZ10013-2018）；
30. 《政务信息系统整合共享通用规范》（CSDZ10023-2018）；
31. 《长沙市政府投资信息化建设项目可行性研究报告编制指南（A 版）》；
32. 《商用密码应用安全性评估管理办法（试行）》；
33. 《政务信息化项目网络安全审查规范》（DB43/T 2013-2022）；

34. 《网络安全等级保护容器安全要求》（T/ISEAA 004-2023）；
35. 《网络安全等级保护大数据安全基本要求》（T/ISEAA 002-2021）；
36. 《信息安全技术数据安全能力成熟度模型》（GB/T 37988-2019）；
37. 《信息安全技术政务信息共享数据安全技术要求》（GB/T 39477-2020）。
38. 《消防控制室通用技术要求》（GA767—2008）/（GB25506-2010）；
39. 《城市消防远程监控系统技术规范》GB50440-2007；
40. 《城市消防远程监控系统》系列标准 GB26875-2011；
41. 《消防联动控制系统》GB16806-2006；
42. 《消防主机》GB4717-2005；
43. 《消防控制室图形显示装置软件通用技术要求》GA/T847-2009；
44. 《消防主机设计规范》GB50116-2013；
45. 《消防主机施工及验收规范》GB50166-2007；
46. 《视频安防监控系统技术要求》（GA/T367-2001）。

1.4.3 投资估算编制依据

1. 《湖南省招标代理服务收费标准》（湘招协〔2015〕6 号）；
2. 《长沙市财政评审中心政府投资建设信息化项目评审指南》（长财评综〔2023〕12 号）；
3. 长沙市近年来类似项目工程概算、市场报价和其他相关资料；
4. 湖南省、长沙市及其他地市政府采购网设备报价。

1.5 项目建设目标、规模、内容、建设期

1.5.1 项目建设目标

相比于传统消防，智慧消防是当下更先进、更高效的解决方案。它利用物联网、大数据等技术让消防管控自动化、智能化、系统化和精细化，打通消防系统间的信息孤岛，提升消防管理人员的预警能力和应急指挥能力。

本项目建设目标是为了响应公安部消防局、湖南省、长沙市等要求加快智慧消防建设，推进信息化预警系统建设的要求，并参考借鉴多个省市通过消防远程监控系统实现远程操作后可进行消控室每班单人值班的政策规定，针对浏

阳汇远实业有限公司下辖园区消防运维成本居高不下、设施状态难把握、信息化管理水平不足等消防管理现状，通过建设智慧消防平台，实时监控浏阳汇远实业有限公司下辖园区消防设施运行状态，实时感知状态，多维度预警，从而优化人员配置，节省人力成本，也提升了火灾事前预警能力及险情处置能力。

具体项目建设目标如下：

（1）实时感知状态，多维度预警：前端设备对 13 个消控室的各种品牌型号的消防主机进行整合联网，通过智慧消防平台，可实现消防主机报警、设备故障等实时预警，并通过系统消息、短信等多种方式通知相关负责人。督查人员对事件进行现场查看落实，并将处理结果录入系统，系统事件自动分类存储，实现消防管理工作闭环的同时，也为消防安全工作提供高效、便捷的数据支持。

（2）远程联动管控，提升工作效率：通过智慧消防平台，实现对消防主机的远程消音、复位等操作。根据消防主机探点的报警情况，可操作远程启停消防水泵、排烟风机等设施，保障险情发生时及时启动消防设施。同时通过远程监测设施故障运行状态，及时安排人员处理故障，提升消防设施的维护效率，平台预留接口，后期可按需接入其它物联网设备及联动门禁、道闸等业务系统。

（3）优化人员配置，节省人工运维成本：智慧消防平台可实时监控各消控室消防主机报警、故障运行状态，用户单位可按需释放值班人员，无需常年“蹲守”消控室，实现各消控室值班合理减员，有效解决持证人员配置不足的问题，优化人员配置，降低人力成本。

1.5.2 建设内容

本项目将建设单位辖区（含产业园区、公租房小区、商业办公楼宇以及金阳集团办公楼、文化馆、金阳文化艺术中心等消防控制室）范围的智慧消防平台，对 13 个消控室的各品牌各型号的消防主机进行整合联网，统一管理。

本期建设内容主要包括：

建设一套智慧消防平台，通过前端设备对 13 个消控室的消防主机进行整合统一管理，实现消防主机的报警，设备故障情况的实时预警。可通过智慧消防平台远程对消防主机进行手动/自动切换、消音、复位及远程启停消防水泵、排烟风机等操作，保障险情发生时能及时启动消防设施。

设立智慧消防监控中心，设在智中心公租房 1 栋 1 楼。智慧消防平台实时预警，可将系统界面投屏，一目了然，辅助总监控中心对现场情况进行迅速判断，方便应急调度。对各消控室划分区域，报警时发送报警短信给各自区域的负责人，提醒及时处理。

分控室远程联动控制建设：使用智能网关采集消防主机报警、故障运行状态，系统实时预警；通过控制终端及针对园区当前各品牌型号主机定制开发不同的驱动软件，实现主机远程手动/自动切换、消音及复位，水泵、风机远程启停等远控操作。

视频辅助系统建设：每个主消控室安装摄像头，值班人员可查看消控室视频，及指导现场人员操作主机。

监控室同步优化：因大部分项目消控室内设有监控室，并由消控室值班人员兼管。综合考虑监控管理的实操性及监控室改造投入运营成本，拟采用单个园区或项目集中区域设置总监控室，以确保消控室整合后监控室值班同步优化。

平台预留接口：预留第三方业务系统接口，可在未来按需接入其它物联网设备或联动门禁、道闸等业务系统。

1.5.3 建设周期

本项目建设周期为 6 个月，前期准备阶段 1 个月；施工阶段、试运行阶段以及项目验收阶段 5 个月。

1.6 项目总投资及资金来源

本期项目总投资概算为 2206858 元，信息系统建设费为 1932370 元，其他费用 169400 元，预备费为 105088 元，所需资金由浏阳汇远实业有限公司自筹解决。

1.7 经济与社会效益

1.7.1 社会效益

提高浏阳汇远实业有限公司消防监管及服务工作的整体效率：智慧消防平台项目通过实时监测和数据分析，能够及时发现潜在的消防隐患，提高消防监

管的效率和准确性，从而提升园区消防安全管理的效率。

提升单位的整体社会形象：智慧消防平台项目的建设和应用，有利于为浏阳汇远实业有限公司树立紧跟信息化新时代建设的形象，为其他单位的消防管理树立标杆、提供借鉴的经验。

提高所辖范围居民的满意度和安全感：智慧消防平台项目通过实时监测和预警，能够在火灾发生时迅速响应，有效降低火灾损失，保障生命财产安全，从而提高所辖范围居民的安全感和满意度。

加强园区治理能力：智慧消防平台项目作为园区智慧建设的重要组成部分，能够从消防角度加强城市治理能力，提升园区管理的现代化水平。

增强应急救援能力：系统能够在设备检测到报警或故障时，进行风险预警，提醒相关人员密切关注并采取措施，防止消防安全事故的发生，增强应急救援能力。

增强应急响应速度：智慧消防平台项目能够实现信息的快速传递和共享，一旦发生火灾，系统可及时通知相关值班人员，无论是就地灭火还是通知相关专业消防人员进行灭火，处理速度都将大大提升。

增强公众安全意识：所辖范围居民普遍消防意识薄弱，对于消防不够重视，认知不够清晰，往往容易忽略日常消防隐患，通过智慧消防平台的宣传和推广，能够增强公众的消防安全意识和自救互救能力，提高全社会对消防安全的重视程度，营造更加安全的生活环境。

1.7.2 经济效益

提升日常管理水平：引入先进的信息技术，智慧消防可以实现对消防设施的故障运行状态的实时监测，确保消防主机处于良好的工作状态，提升消防设施的完好率和维护效率。

消防数据支撑：日常消防主机报警、故障信息自动存档，便于用户分类查询，同时为用户的消防管理工作提供数据支撑。

推动消防产业升级：智慧消防平台能促进相关技术的研发和应用，如物联网、大数据等，有助于推动消防产业向高科技、智能化方向转型升级，提高整个行业的竞争力。

节省人力成本支出：通过智慧消防平台建设，实现对消防主机的实时监控，用户可根据单位实际情况合理的缩减部分值班人员，释放出来的部分消控室值班人员，充分降低了人力成本支出。

1.8 可行性分析

1.8.1 政策可行性

随着城市化的不断发展，基础设施的不断增加，火灾隐患也愈来愈多，近些年国内消防事故频发，国家十分重视消防安全工作，中央及各地政府近些年陆续颁布了《关于全面推进“智慧消防”建设的指导意见》、《“十四五”国家消防工作规划》、《《湖南省“十四五”消防救援事业发展规划》》、《安全生产治本攻坚三年行动方案(2024-2026 年)》等重要指导文件，推进“智慧消防”建设，加速推进现代科技与消防工作的深度融合。参考借鉴《广东省实施〈中华人民共和国消防法〉办法》、《广西壮族自治区实施〈中华人民共和国消防法〉办法》、《重庆市消防设施管理规定》（详见正文 1.4.1 中 7.8.9.11.12.13.14 项政策）等多个省市关于远程控制的政策规定（消防控制室实行 24 小时值班制度，每班不少于二人，通过城市消防远程监控系统实现远程操作消防控制室所有控制功能的，每班不少于一人），本项目有关消防远程控制的设计思路在全国已有成熟案例，相关政策土壤已非常成熟。可以预见，智慧消防是当下乃至未来很长一段时间消防事业的发展重点，未来相关性政策会越来越多。因此，参考借鉴临省相关规定，本项目的建设是符合相关政策的。

1.8.2 技术可行性

智慧消防技术主要包括智能火灾报警、消防物联网、视频监控等，通过这些技术，实现消防主机报警、设备故障等实时预警，实现对消防主机的远程消音、复位等操作，并根据消防主机探点的报警情况，可操作远程启停消防水泵、排烟风机等设施，保障险情发生时及时启动消防设施。2017 年，中国公安部消防局发布了《关于全面推进“智慧消防”建设的指导意见》，提出标志着智慧消防开始进入全面推进阶段，加上过去十数年间的技术积累，智慧消防的相关技术已相对成熟。近年来，这些技术已在国内多个城市级智慧消防平台进行广

泛应用，技术已非常成熟，技术具备可行性。本项目有包括泰和安、利达、北大青鸟、依爱、海湾等 5 个品牌 9 个型号（包括泰和安 TX3016A、利达 LD128E（Ⅱ）、利达 LD188EL、北大青鸟 11SF-C4、北大青鸟 11SF、北大青鸟 11SF-S8、依爱 EI6000G、海湾 GST5000 等型号）的消防主机，经市场调研，以上品牌型号的主机均支持通过串口（RS232、RS485、CAN 等）进行联网，市场技术较为成熟，技术可行性较高。

1.9 主要结论与建议

本项目经过充分论证，依据国家、湖南省及长沙市相关政策，分析了项目建设的必要性和迫切需求、研讨了技术方案和技术可行性、分析了项目建设的社会和经济效益，得出以下结论：

本项目建设符合国家、湖南省及长沙市智慧消防相关政策原则及规定，项目的实施将充分解决目前用户单位消防设施分散管理难、运行状态难把握、人力成本支出高昂等的问题。

本项目建设符合国家、湖南省及长沙市相关政策法规和技术标准规范的要求，项目建设目标明确、需求内容详实、设计规范，建设内容、建设规模、进度安排和资金安排合理，建设方案和项目组织机构落实、投资估算满足可行性研究报告的要求，其建设可行。建议尽快立项，并给予资金支持。

第二章　项目建设单位概况

2.1　项目建设单位与职责

湖南金阳投资集团有限公司成立于 1999 年 11 月，原名湖南浏阳工业园开发投资有限公司，是由浏阳市人民政府全额出资，浏阳经济技术开发区管理委员会直接管辖的国有独资企业，注册资本 110 亿元，总资产 483 亿元，集团主体资信等级 AA+。

公司现有员工 218 人，设有党委、董事会、监事会、经理层；下设集团办公室、党群工作部、纪检监督室、财务融资部、法务内控部、战略发展部、投资部七个部门；下辖浏阳汇远实业有限公司、湖南浏阳经开区水务股份有限公司、浏阳鑫能配售电有限公司 3 家主要子公司。其中浏阳汇远实业有限公司主要负责标准厂房、公租房建设运营；湖南浏阳经开区水务股份有限公司主要负责自来水供应、污水处理、管网施工等公共服务业务；浏阳鑫能配售电有限公司主要负责光伏发电、配售电等新能源业务。

自成立以来，公司以助推国家级浏阳经开区发展为中心，整合优势资源，创新经营模式，深入参与浏阳经开区经济建设与社会发展，全力服务经开区发展，逐步建立起集城市服务、公共服务、产业服务和股权投资于一体的业务体系，成长为园区重要的国有资本运营公司。

公司与中信建投资本、招银国际、祥峰投资、恒信华业及华润资本等行业内顶尖投资机构建立了稳固的合作关系，围绕园区主导产业设立了多支股权投资基金，投资了一批优质项目已上市。集团下属水务公司于 2017 年 12 月在新三板挂牌，已整合金阳新城范围内自来水供应业务，供水能力达到 23 万吨/日。建设运营了浏阳经开区北园污水处理厂、南园污水处理厂，污水处理能力 13.5 万吨/日。下属汇远实业具备房地产开发一级资质，建设运营的工业地产、公共租赁住房面积超过 100 万平米。汇远实业依托长沙 e 中心、金阳智中心等项目开展产业招商，通过连续三年的持续深耕，已累计入驻医疗器械企业近 160 家，初步形成医疗器械产业集群。集团下属鑫能公司是湖南省首批参与电力市场交易的企业之一，目前分布式光伏发电规模 50MW，年收入超过 1800 万元。

展望未来，公司将坚持市场化运作，聚焦经营性业务，深化产业整合，推进资本经营，持续助力园区电子信息、智能制造、生物医药、健康食品等产业集群集聚，促进产业升级和产城融合，力争成为中部地区顶尖的产城综合服务集成商和国内一流的国有资本运营公司。

浏阳汇远实业有限公司（简称汇远实业）是湖南金阳投资集团有限公司全资子公司，成立于 2001 年，注册资本 3 亿元，具备房地产开发一级资质，成立以来深耕产业地产和租赁住房板块，已成长为长沙市首批规模化、专业化租赁住房运营商。

组织架构方面，公司内设部门 6 个，分别为办公室、招商营销部、资产管理部、工程建设部、安全管理部、运营中心（下辖企业服务部、租赁住房部）；拥有全资子公司 3 个（云普检测、金阳智慧、云智运营），控股子公司 1 个（建工汇远，控股 65%），同时托管公司 1 个（汉元）。截至目前，干部职工（含带编）34 人。

产业地产方面，汇远实业精心建设运营长沙 e 中心、金阳智中心、创新创业园、金阳新能源、中欧汽车零部件等五大产业园，主导产业为医疗器械、电子信息、汽车零配件、新能源新材料。建设运营的资产规模达 126.13 万㎡，其中厂房 83.96 万㎡，商业配套 11.31 万㎡、租赁住房 30.86 万㎡，为项目入驻提供全周期要素保障。截至目前，五大产业园共引进企业 339 家，其中高新企业 60 家，规上企业 36 家；其中 10 家上市企业在园内设立了子公司。2023 年实现亩均税收达 27 万元。

租赁住房方面，汇远实业秉承“服务民生、留住人才”的宗旨，在租赁住房领域精耕细作多年，目前运营汇远东郡、镶龙华府、紫星园、金凯莱公寓、智中心人才公寓等 10 个租赁住房项目，其中镶龙华府为长沙租赁住房示范项目，汇远东郡为住建部广厦奖专家组推荐项目。租赁住房项目共计持有房源 5602 余套，为园区的企业高管和职工提供了优质的居住环境，目前已有约 1.2 万人入住。

未来，汇远实业将进一步加强谋划、打造精品、优化布局，向中部地区领先的产业地产企业、长沙市示范性住房租赁企业迈进，在金阳新城建设中展现

国企担当、贡献更大力量。

2.2 项目实施机构与职责

本项目的实施机构为浏阳汇远实业有限公司（简称汇远实业），其职责如下：

1. 负责项目申请立项、可行性研究报告评审和经费管理等工作。配合有关部门进行项目可行性论证，负责项目可行性研究报告评审及项目经费申请和计划管理，政府采购、项目验收的组织管理工作。
2. 全面负责项目的建设实施工作，完成项目的财务管理、业务实现、技术实现、系统推广等工作。

第三章　需求分析及项目建设必要性

3.1　项目提出的背景和依据

消防安全工作是保障经济发展、社会安定、人民生命财产安全的重要基础工作，消防设施是现代化城市建设的重要基础保障。随着城市化的不断发展，基础设施的不断增加，火灾隐患也愈来愈多。浏阳经开区作为发展浏阳地区高新技术产业、促进产业集聚的重要平台，已经成为浏阳各地区域经济发展的重要助推器。在园区建设蓬勃开展的背景下，随着园区日益增多，日常消防管理愈发重要，部分园区消防安全缺失，管理弱化，必须采取有效对策消除存在的安全隐患，强化消防安全管理，才能推动消防安全环境持续向好，抓好园区消防安全工作已经成为迫切要求，需要技术先进、稳定可靠的智慧消防平台项目来保障园区消防安全。

近年来浏阳汇远实业有限公司下辖园区逐步加大消防安全投入，消防设施建设不断得到改善，抗御火灾的整体能力得到很大的提高，但技防能力不足，依托于人工进行管理，人工运维成本越来越大，由于园区分散，规模大，依托于人防的管理模式效率不足，无法满足现有消防管理要求。因此，目前园区消控室分散、人工运维成本高、信息化水平不足等迫在眉睫的消防痛点亟需解决，近些年国内消防事故频发，国家十分重视消防安全工作，国家及湖南省政府近些年陆续颁布了《关于全面推进“智慧消防”建设的指导意见》、《“十四五”国家消防工作规划》、《《湖南省“十四五”消防救援事业发展规划》》、《安全生产治本攻坚三年行动方案(2024-2026 年)》等重要指导文件推进“智慧消防”建设，加速推进现代科技与消防工作的深度融合。《广东省实施〈中华人民共和国消防法〉办法》、《广西壮族自治区实施〈中华人民共和国消防法〉办法》、《重庆市消防设施管理规定》等多个省市也推出关于远程控制及单人值班的政策。为了解决目前浏阳汇远实业有限公司下辖园区的消防痛点，也为了响应国家号召，推进消防智能化、信息化建设，拟建设智慧消防平台，结合前端设备实现对消防主机的集中实时监控管理，实现消防安全管理工作的

智能化、信息化，充分节省企业人工运维成本支出，实现降本增效，增强火灾事前预警和事后处置能力，保障园区生命财产安全。

3.2 智慧消防国内建设现状

近年来，我国的消防事业包括消防科技和器材产业等都有大幅度的进步。但是，消防事业的发展仍然落后于世界先进水平，也不能适应国家现代化建设的需要。面对当前的火灾隐患，现有的消防管理无论是技术与知识，还是装备与能力均感力不从心。只有建立更加完善的消防体制，加速消防产业的改造、整合，才能适应新世纪消防事业发展的需要。

当前的消防行业呈现出一种数字化转型的态势，数字经济时代已经悄然来临。在智能化这个大架构下，物联网、大数据将成为新时期消防新业态的典型特征，也为消防管理注入多元价值，对于提升城市公共安全管理水平、创新社会治理、服务民生具有重要意义。智慧消防是城市消防建设的必然趋势，智慧消防建设顺应智慧城市的建设潮流，是智慧城市和消防信息化建设的重要内容，智慧消防在消防中发挥重要作用，可以对消防管理涉及的对象、事件等进行快速数据采集和自动过程记录，大数据的普及应用，将进一步拓展消防监管手段，如消防巡检过程记录、消防设施维修与排查等，可以有效保证数据质量，让消防管理更加便捷、高效。

智慧消防广泛应用于全国范围内的住宅小区、学校、医院、商场等人员密集、贵重仪器物品多的场所，伴随着物联网技术发展及智能化设备普及，智慧消防逐渐进入大众的视野，也逐渐进行了广泛的应用。至 2017 年，中国公安部消防局发布了《关于全面推进“智慧消防”建设的指导意见》，提出标志着智慧消防开始进入全面推进阶段。越来越多的单位在应用智慧消防实现了消防主机联网、消防水系统监测、电气火灾监测等方面。智慧消防在城市消防事业中发挥越来越重要的作用，为构建安全、和谐的社会环境贡献力量。

3.3 园区消防设施现状

经过调查，我们了解到浏阳汇远实业有限公司下辖产业园区、公租房小区、商业办公楼宇以及金阳集团办公楼、文化馆、金阳文化艺术中心消防控制室共

计 15 处，目前已投运 13 处。因各园区为分批建设，消控室未实行集中统一管理，各消控室均需安排人员进行 24 小时值班。目前园区有泰和安、利达、北大青鸟、依爱、海湾等多个品牌型号的消防主机共 35 台，分散在各个消控室内。

序号	项目名称	消控室所处位置	消防主机品牌	数量	安防监控室位置
1	长沙 e 中心	e 中心综合楼	利达、泰和安	1 处	e 中心综合楼
2		e 中心三期 B2 栋 1 楼	泰和安	1 处	
3		e 中心三期 B3 栋门卫室	泰和安	1 处	
4	东郡公租房	6 栋 1 楼	泰和安	1 处	
5	企业总部	C1 栋地下室	泰和安	1 处	
6	智中心	公租房 1 栋 1 楼	北大青鸟	1 处	公租房 1 栋 1 楼
7	蓝郡公租房第 3 批次	门卫室隔壁房间	北大青鸟	1 处	门卫室隔壁房间
8	创新创业园	A1 栋 104	北大青鸟、泰和安	1 处	A1 栋 104
9	中欧园	西门卫室	泰和安	1 处	西门卫室
10	新能源产业园	西门卫室隔壁房间	依爱、泰和安	1 处	西门卫室隔壁房间
11	金阳集团办公楼	办公楼 1 楼	海湾	1 处	办公楼 1 楼
12	金阳艺术中心	地下车库	海湾	1 处	地下车库
13	医药文化馆	门卫室	海湾	1 处	门卫室
14	龙熙顺景	龙熙顺景 1 楼	泰和安	1 处	龙熙顺景 1 楼
15	金盛园保租房	\	\	1 处	建设中
消控室合计 15 处，目前除 e 中心三期 B3 栋、金盛园保租房外共 13 处消控室投入运行。					

3.4 消防管理问题分析

3.4.1 消防主机分散，无法统一监控管理

浏阳汇远实业有限公司下辖园区各建筑物的消防主机分布较为分散且各自独立，缺乏集中统一的管理平台。由于历史原因，目前园区应用的消防主机设备种类繁多，分散在产业园区、公租房小区、金阳集团办公楼、金阳文化艺术中心等区域的 15 个消控室内(正式启用的 13 个)。消防主机则包括泰和安、利达、北大青鸟、海湾、依爱等不同品牌型号的消防主机共 35 台（正式启用的 33 台）。园区的 35 台不同品牌型号的消防主机分散在不同区域的 15 个消控室内就造成了管理部门无法实时全览所有区域的消防安全状态。

同时，由于各设备没有国家统一通信标准，过去的技术手段无法联网，由此造成各个主机各自为政，信息无法共享，无法统一管理。各种消防主机以独立个体方式存在（或独立组网），成为一个个消防信息孤岛，缺乏纵向有效监督。只能采用分散被动管理，且大部分情况依靠人防。各类主机报警信息只能采用分散被动管理，不能及时有效响应。预警手段的不足导致管理人员对整体安全防范形势无法把握，对重点安防工作的指导也不能统一落实。

3.4.2 依托人防，运维成本高，效率低

按《消防控制室通用技术要求》（GA767—2008）/（GB25506-2010）相关规定，每个消控室需 24 小时值班，且都需持证上岗。浏阳汇远实业有限公司下辖园区包括泰和安、利达、北大青鸟、海湾、依爱等不同品牌型号的消防主机共 35 台分散在各个消控室内。由于地理位置分散，没能集中监控，所需人工运维成本居高不下。沉重的人工运维成本也给企业造成很大压力。目前消防主机无法实现远程控制，人员现场确认消防主机发生的报警、故障事件后仍需折返回消控室消防主机上进行消音复位。为避免误报引发消防主机联动，常规情况下消防主机为手动状态，因此消防水泵、排烟风机等设施的启动、停止需要人员现场操作，不仅产生巨大的工作量，险情发生时也难以第一时间启动消防设施。

3.4.3 消防管理信息化水平较低

目前，浏阳汇远实业有限公司下辖园区的日常消防管理主要依托纸质台账，缺乏信息化管理平台。纸质档案归档耗时，信息查询、溯源难。对维护和值守人员没有统一的指挥和调度平台，尤其是园区消防设施运行状况、防火检查发现的消防隐患、以及隐患是否整改到位等信息依托纸质文件，缺乏对消防维保单位的必要的监督和考核手段，消防检查工作的闭环不足。因此，消防安全责任人对园区消防安全缺乏整体把控能力，淹没在海量日常信息中，影响其在消防安全方面的判断及决策等，不利于园区消防安全管理。监控管理工作各自为阵，对事前预防、事中跟踪、事后分析缺乏有效的支撑手段，对维护和值守人员不能统一指挥和调度，缺乏必要的监督和考核手段，设备的运行和维护情况管理也不到位。

3.5 业务需求分析

3.5.1 打通传统消防设施信息孤岛

在传统消防管理模式中，都是以消防主机为核心，将建筑中的烟雾探测器、温度探测器、手动报警控制器、声光报警器、报警阀、消防泵等相关设备进行连接，获取消防系统运行的故障数据、报警数据、状态数据，并进行相关联动。但是，传统消防的监控系统存在着局域局限性，即只能在本地（该建筑消控室）查看、报警、联动等，无法实时了解消防安全的动态数据，传统消防存在着数据无法互通、共享，业务无法联动。因此，需要加快打通消防设施的信息孤岛，实现统一管理、业务联动。

利用物联网手段获取消防主机的相关报警、故障运行状态，对园区的消防安全状况的动态状况进行实时监测预警。方便园区消防设施的统一管理，也方便管理人员能及时的、远程了解园区的建筑消防情况，及时处置设备报警、故障等隐患，保障建筑、人员、财产的安全。

通过数据互通，可随时查看本地消控室视频。未来可根据实际需要进行报警视频弹窗。

3.5.2 丰富消防物联感知手段

建筑消防主要涉及消防给水及消防栓系统、火灾自动报警控制系统等，本期建设目标旨在将分散在各地的消防主机集中到智慧消防平台上做统一监控管理，同时预留端口，未来可根据实际需求进行其余消防系统的信息化扩容建设。包括传统消防消防主机的集中管理，实时监测、预警等；预留端口，未来可拓展消防水压、消防水池、电气火灾监测等其他业务模块。

3.5.3 消防管理降本增效

目前消防主机中出现报警、故障事件时，人员在现场确认处理完后仍需折返回消防主机上进行消音和复位。为避免误报引发消防主机联动，常规情况下消防主机为手动状态，因此消防水泵、排烟风机等设施的启动、停止需要人员在现场操作，不仅产生了巨大的工作量，险情发生时也难以第一时间启动消防设施。通过智慧消防平台，可实现如下操作，从而降本增效。

1、监控人员可根据现场报警情况，判断形式及时进行远程控制，提升消防事件的处置效率，根据单位实际情况可适当缩减值班人员。

2、通过智慧消防平台实现对消防主机的远程消音、复位；

3、通过智慧消防平台实现对消防主机下辖的消防水泵、排烟风机等重要消防设施的远程启动、停止，手自动切换；节省人力工作量，保障险情时能第一时间启动消防设施。

3.5.4 消防工作监督落实与闭环

消防安全责任落实一直是消防安全管理的一大难点，消防安全责任不明晰、相互推诿、安全隐患处理不及时、监管不到位等，都给消防安全责任落实带来了较大的困难。另外消防主机中出现报警、故障事件时均需要去现场确认，核实完现场情况后反馈并记录，通常是以纸质文件的方式记录存档。通过智慧消防平台实现消防事件从发生到处理完成的记录存档，园区消防事件处理结果的反馈，记录进系统方便查询溯源，谁去、何时处理、事件发生原因一一记录，实现消防事件处理的闭环，同时实现消防管理工作的电子化、信息化。

3.5.5 深化消防数据应用价值

有限的安保力量淹没在海量的消防数据之中，通过消防主机集中联网，对各类数据进行分类梳理存档，可视化展示，给消防数据应用、深化带来了极大的价值，实现消防安全评估的需要。通过对消防数据的分类梳理，结合列表、图形等展示方式，直观展现消防报警、故障数据，辅助用户决策。

3.6 功能需求分析

智慧消防平台应综合接入各类消防设施以及相关的系统，利用智能网关、物联网传感器、大数据等技术手段，实时监测各类消防设施运行状态。系统对各类消防设施运行状态和报警进行数据采集处理，实时报警、存储、联动，并提供以下功能：

（1）数据总览模块：支持一张图总览用户所关注的数据，能综合展示报警情况、监控场所情况、设备数量、设备运行情况等。

（2）实时监控管理模块：支持接入消防主机，实现设施报警、故障等信息的实时接收；报警支持弹窗，弹出报警点信息及电子地图，报警时进行声音、闪烁警示等；报警除在系统显示外，还支持短信方式进行推送；支持视频联动。

（3）设施管理模块：支持设施名称、类型、地点等多种方式查询设施信息；设施报警故障记录查询，实时数据查看等；设施报警、故障信息复核审计，报警、故障发生原因录入系统等；支持阈值配置、隔离配置等。

（4）网格管理模块：支持以列表形式展示权限范围内的所有的楼宇信息，可以新建，修改楼宇基本信息。

（5）智能巡查模块：支持任务查询、添加，后台可查看任务完成情况。

（6）档案管理模块：支持人员证件、合同、消防法规文件等上传、查询等。

（7）数据分析模块：支持图文展示实时报警、故障数据，分布图、趋势图查看等。

（8）系统设置模块：支持用户管理，账号添加修改，管辖范围分配、日志查看等。

3.7 配套设备需求

3.7.1 监控中心设备需求

智慧消防监控中心增加短信服务器 1 台，监控电脑 2 台，为方便监控调度，增加 100 寸显示大屏（非拼接屏幕，便于移动）1 台，1 台网络硬盘录像机及相应硬盘（从未来 e 中心三期 B3 栋、金盛园保租房消防主机启用后需增加摄像头以及冗余的角度考虑，配置 10 块 8T 监控硬盘）用于前端消控室视频辅助设备的存储。

3.7.2 前端联网设备需求

13 个消控室各品牌型号消防主机的联网采集接入及远程控制，需要配置智能网关、控制终端及消防主机通信模块。

3.7.3 消控室视频辅助设备需求

每个消控室需配置 2 台高清网络摄像机，监控中心值班人员可查看消控室视频及指导现场人员操作主机。

3.7.4 网络传输需求

租用运营商的光纤资源（20M）组成智慧消防业务网（局域网）。

3.7.5 安防监控室配套改造需求

当前部分园区安防监控中心由消防值守人员兼管，智慧消防系统实施后，将优化前端消控室值守人员，为满足后期安防管理需求，并且不增加安防管理人员，本项目需将 2 个安防监控室迁移至门岗室。

3.8 安全防护需求分析

3.8.1 系统安全防护能力需求

本期安全防护体系建设是以园区消防信息安全为目标，以业务需求为主导，构建和平台业务需求相匹配的综合安全防护能力，并通过安全管理制度落地，加强运维过程中的预警监测能力和应急处置工作，不断提高单位的抗攻击能力，同时在安全保障工作中通过定期培训、加强应急预案演练、协同应急处置等方面的工作加强人员的安全技能。最终在整个安全保障工作中全面提升单位的综合防护能力。

3.8.2 网络安全防护需求

本项目系统部署在浏阳经开区数据中心机房，复用浏阳经开区数据中心机房提供的网络安全防护措施。

3.8.3 数据安全需求

本项目设备中的服务器、存储设备、电脑等应采取防盗、电源保护等安全保护措施。应制定运行维护管理制度，配备管理人员。系统应提供备份和恢复系统数据的功能，可使用多种介质备份和恢复系统数据。系统应实现权限的分散管理，按照功能进行授权管理，不应出现权限的漏洞，使得某些用户拥有本不该拥有的权限。

3.8.4 个人信息安全保护需求

本项目业务系统不对互联网公众提供服务，内部需要保存园区、企业、用户的个人数据。有些数据对单位而言是重要的数据，一旦泄露，会对单位安全运营造成严重损害，因此必须对业务系统涉及的安全数据进行严格的保护措施，防止未授权访问和非法使用相关信息，从而保证数据的安全。

3.9 消防主机底层数据需求

本项目在实施过程中需要采集以下消防主机底层数据：

1）需联网的所有消防主机探点编码表；

2）需联网的所有消防主机探点点位图；

3）需联网的所有消防主机下辖楼宇的平面图。

为了数据的准确性及缩短数据生成的时间，需尽量提供电子版文件。

3.10 网络安全建设需求

网络安全建设有以下几点需求：

1. 数据安全：保护数据资产安全，防止数据泄露和丢失，是业务网络安全建设的基础需求。
2. 网络稳定性：保证业务网络的稳定性，防止网络故障和崩溃，是网络安全建设的核心需求。

3. 业务系统连续性：保证业务系统的连续性，防止业务中断和损失，是网络安全建设的重点需求。
4. 人员培训和管理：加强建设单位网络安全人员的培训和管理，提升员工的安全意识和技能水平，是网络安全建设的长期需求。
5. 安全策略制定和执行：制定适合单位的安全策略，并确保其得到有效执行，是网络安全建设的核心需求。

3.11 其他资源需求

每个消控室需具备 1 个 AC220V 设备取电端口。

3.12 信息量分析预测及性能需求分析

3.12.1 信息量预测

每台消防主机每日报警估算约 20 条，报警记录每条约 20 K，33 台主机每年约有 33*20*365*20=4818000K/1024/1024=4.59G，一年约有 4.59G 数据量,每台消防主机每日故障估算约有 10 条，故障记录每条约 20 K,33 台主机每年约有 33*10*365*20=2409000K/1024/1024=2.29G，每年合计数据量约 6.88G。

配置 26 台摄像机，每台摄像机按 2M 码率，存储 90 天估算，所需录像容量约为 53.02 TB。

3.12.2 用户量测算

监控中心值班用户估算：2 个。

浏阳汇远实业有限公司管理人员用户估算：3 个。

属地管理分控点用户估算：5 个

以上用户均为同时使用，合计 10 个，预估未来可能增加的用户量 10 个，考虑冗余，系统同时并发用户量计算应至少能容纳 40 个用户同时使用。

3.12.3 系统性能需求分析

系统操作简单、管理方便，能对人工输入的数据以及来自不同接口的数据进行合法性检查，确保流程的通畅性，并且能够对错误数据进行自动纠错处理。整体性能指标包括：

1.统一性

平台所有应用应能符合平台的统一规划和部署要求，能够保证使用平台、数据的一致、完整和准确。

2.开放性

基于目前先进开发技术和标准开放，具备信息共享，接口交互的能力。

3.易用性

能够提供友好的 GUI 界面，满足管理人员日常管理监控业务，同时满足相关业务人员在可视化界面下灵活方便的实现数据交换的各种方式。

4.稳定性

确保系统 7×24 小时连续运行，平均年故障时间（平均每年出现故障的总时长）<=1 天，平均故障修复时间（发生故障时平均需要花费的修复时间）<=30 分钟；软件的缺陷<=0.2%、故障率<=0.5%，确保基础平台稳定可靠的运行，硬件故障率<=0.001%，系统年运行可用性>=99.9%。

5.快速响应

在网络正常无延迟的情况下，应做到：

（1）系统响应消防主机报警、故障事件≤3 秒；

（2）系统远程控制主机操作的响应时间≤3 秒；

（3）系统查询响应时间 ≤ 3 秒；

（4）统计、报表查询等 ≤5 秒。

6.可扩展性

支持现有环境下用户并发量、存储量等平滑扩展和硬件随需扩展需求，在未来系统信息量、用户量不断扩大的情况下，系统能够同步扩展增长。

7.可移植性、可重用性

具有较强的可移植性、可重用性，保证在将来发展中迅速采用最新出现的技术、适应硬件系统升级以后的平台、长期保持系统的先进。

8.兼容性

平台支持 Chrome、FireFox、360 等浏览器。支持 IPV6 协议。

9.稳定性

系统数据每日备份，数据丢失时间段不超过 1 天，系统从宕机到恢复，整体恢复时间应不超过 1 小时。由于自然灾害等不可抗因素导致的服务器损毁等严重灾害，整体恢复时间应不超过 1 天。

3.13 项目建设的必要性

3.13.1 基于园区管理的实际出发

目前园区消控室分散、主机状态难把握、人力成本支出高、信息化水平不足等消防痛点一直无法解决。因此建设智慧消防平台，能充分实现：

（1）提升日常管理水平：引入先进的信息技术，智慧消防平台可以实现对消防主机的联网整合统一管理，一则实现主机的报警、故障运行状态的实时监测，也充分加强了预警能力。二则确保消防主机处于良好的工作状态，提升消防设施的完好率和维护效率。

（2）消防数据支撑：不再依托纸质文件，实现消防数据管理的电子化，日常消防主机报警、故障信息自动存档，便于用户分类查询，同时为用户消防管理工作当中的事前预防、事中跟踪、事后分析提供充足的数据支撑，辅助用户分析和进行决策。

（3）节省人力成本支出：通过智慧消防平台实现对消防主机的实时监控，用户可根据单位的实际情况，缩减部分值班人员，释放出来的部分消控室值班人员可充分降低人力成本支出。

3.13.2 顺应国家消防发展智能化的浪潮

近些年国内消防事故频发，国家十分重视消防安全工作，中央及各地政府近些年陆续颁布了《关于全面推进“智慧消防”建设的指导意见》、《“十四五”国家消防工作规划》、《《湖南省“十四五”消防救援事业发展规划》》、《安全生产治本攻坚三年行动方案(2024-2026 年)》等重要指导文件推进“智慧消防”建设，加速推进现代科技与消防工作的深度融合。

3.13.3 有助优质企业形象的树立

通过智慧消防平台的建设，一则提高园区人员的满意度和安全感：智慧消

防平台项目通过实时监测和预警，能够在火灾发生时迅速响应，有效降低火灾损失，保障生命财产安全，提高园区人民的安全感和满意度。进而提升单位的整体社会形象，二则智慧消防平台的建设和应用，有利于为建设单位树立紧跟信息化新时代建设的形象及为其他园区消防管理树立标杆、提供借鉴的经验，间接为推动行业消防管理的进步提供素材和主力。

第四章　总体设计方案

4.1　建设原则和策略

智慧消防平台建设应立足于实际，充分考虑整体性、开放性、安全性等方面，具体原则如下。

1）整体性

智慧消防平台建设应充分考虑整体性，不仅基于本次的项目内容建设，还要为将来的扩容、拓展进行预留，未来新增消防主机的接入无需在软件层面做过多改动，仅需增加硬件设备、进行数据录入等即可。

2）开放性

智慧消防平台建设应充分考虑开放性，系统应预留接口，未来可根据用户单位的实际需求对接其它业务系统。

3）安全性

智慧消防平台建设应充分考虑安全性，所采用的操作系统需为成熟稳定，不易被攻击的操作系统。同时，基于消防安全考虑，平台方案设计需遵循不影响消防主机本身功能的原则，不能改变主机架构，影响主机正常运行。

4.2　项目定位

本项目定位为企业智慧消防平台，针对企业所辖园区消控室分散、主机状态难把握、人力成本支出高、信息化水平不足等消防痛点，通过信息化技术，助力用户实现消防设施的集中实时监控、消防管理工作的信息化、消防人力成本的合理节省，能有效实现单位降本增效的目标的同时加强火灾事前预警能力及险情处置能力。

4.3　总体目标

项目总体目标如下：

基于智慧消防平台，先行搭好基础，未来在条件允许的情况下，根据单位的实际情况，可进行各场景的智慧消防拓展建设，充分应用物联网技术，综合

有线、无线传输，通过各类物联感知设备实现对园区消防水压、消防水池、电气火灾等场景的实时监测预警，全面深化智慧消防建设，实现消防感知能力的实时性、多样性。在未来，可结合实际情况对接其他业务系统实现联动，拓宽智慧消防应用范围。

具体项目建设目标如下：

（1）实时感知状态，多维度预警：前端设备对 13 个消控室的各种品牌型号的消防主机进行整合联网，通过智慧消防平台，可实现消防主机报警、设备故障等实时预警，并通过系统消息、短信等多种方式通知相关负责人。督查人员对事件进行现场查看落实，并将处理结果录入系统，系统事件自动分类存储，实现消防管理工作闭环的同时，也为消防安全工作提供高效、便捷的数据支持。

（2）远程联动管控，提升工作效率：通过智慧消防平台，实现对消防主机的远程消音、复位等操作。根据消防主机探点的报警情况，可操作远程启停消防水泵、排烟风机等设施，保障险情发生时及时启动消防设施。同时通过远程监测设施故障运行状态，及时安排人员处理故障，提升消防设施的维护效率，平台预留接口，后期可按需接入其它物联网设备及联动门禁、道闸等业务系统。

（3）优化人员配置，节省人工运维成本：智慧消防平台可实时监控各消控室消防主机报警、故障运行状态，用户单位可按需释放值班人员，无需常年“蹲守”消控室，实现各消控室值班合理减员，有效解决持证人员配置不足的问题，优化人员配置，降低人力成本。

4.4 总体设计方案

4.4.1 总体框架图

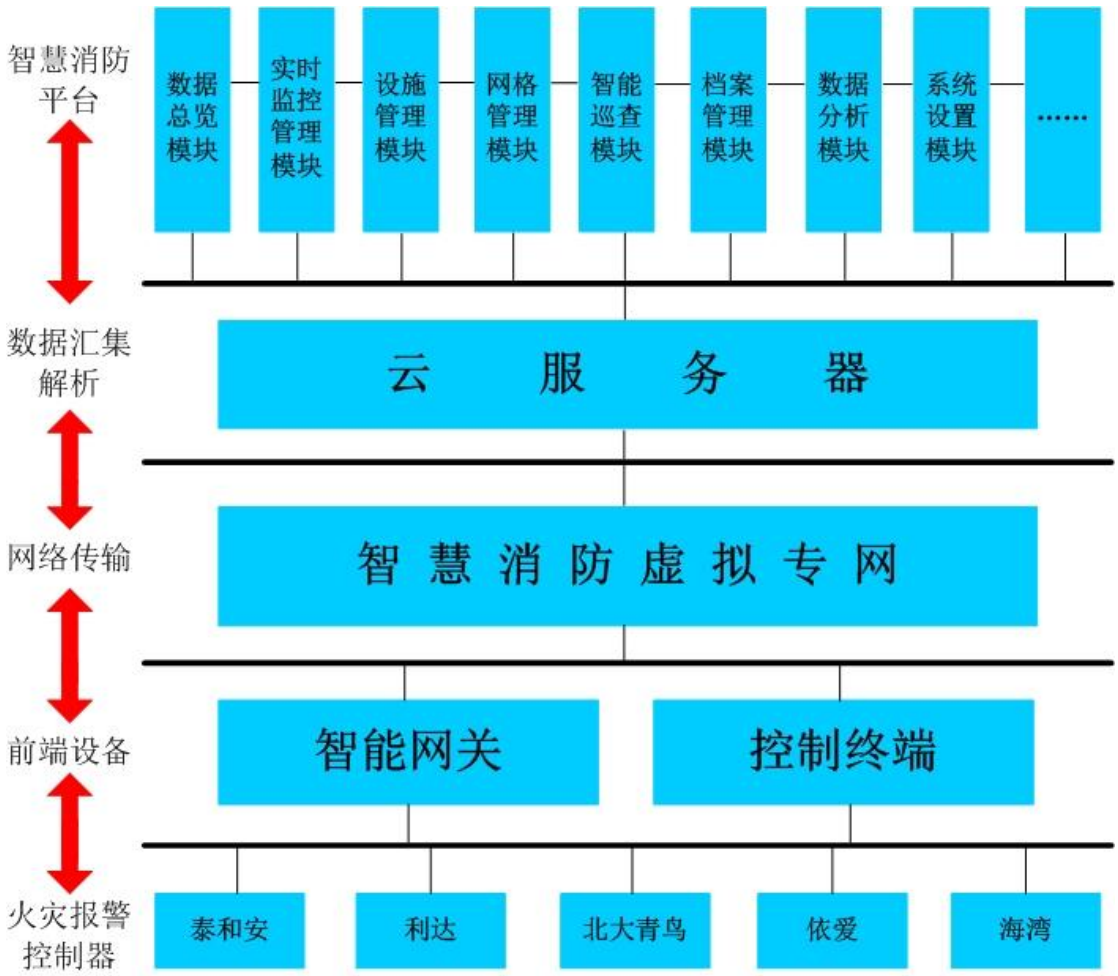


图 4.5-1 总体框架图

前端使用智能网关、控制终端对现有 5 个品牌消防主机进行采集及控制，本项目服务器采用云资源实现，租用经开区云服务器，部署于经开区云上。

4.4.2 监控中心值班流程图

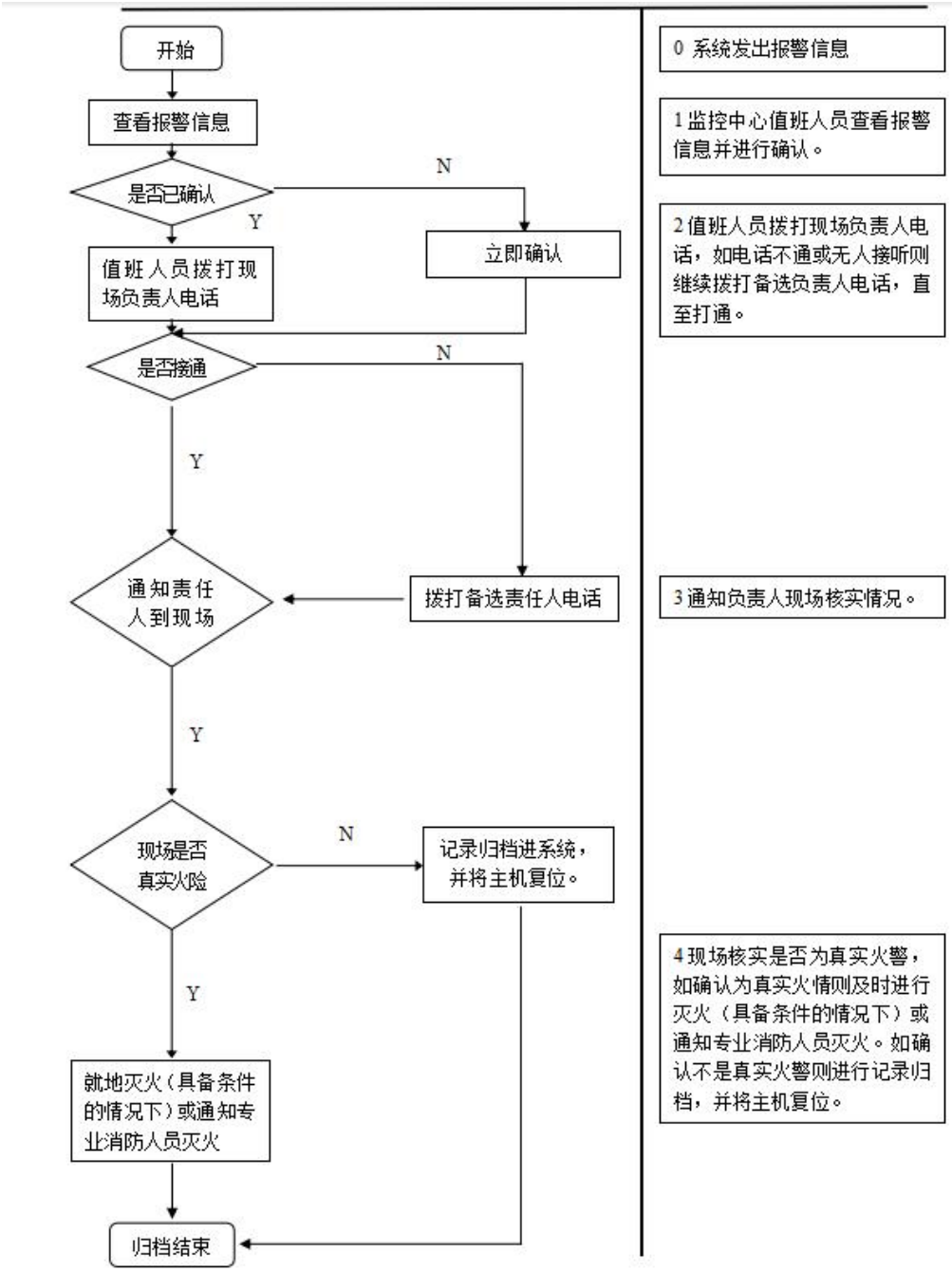


图 4.5-2 总体业务流程图

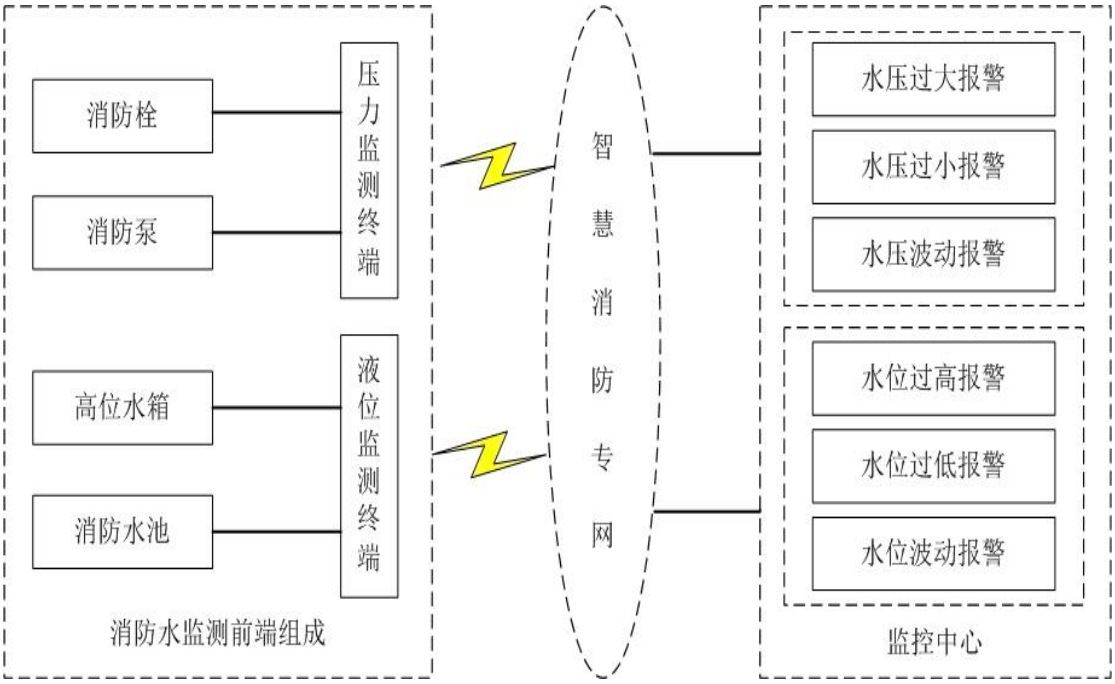
4.4.3 系统数据共享、对接设计

本项目系统数据不限于浏阳汇远实业有限公司内部使用，如汇远公司内部其它业务系统或园区其它业务需要，也可进行数据共享，故虽本项目不计划对接其它业务系统，但需预留接口，未来可通过 API 等方式进行业务系统对接。

4.5 可扩充设计

4.5.1.1 消防水监测

园区消防水压及消防水池需要人员定期检查运行状态，无法第一时间获取运行状况，消防水系统作为火情时的“救命稻草”，水压是否充足、有水无水无法第一时间知晓，存在安全隐患。针对此隐患，未来建设单位可对智慧消防平台进行扩容，通过增加前端物联网设备，应用无线传输技术（前端设备采用无线安装、电池供电，无需布线）如无线水压探测器、无线水池探测器等实现对园区消防水压、消防水池的实时监测预警，接入智慧消防平台项目保障消防水系统在险情下的正常运行，水压过大过小、水池水位过高过低等均可报警，在系统上显示出直观的具体数值。有水无水可第一时间知道，避免火灾时消防水系统无法正常运行。同时节省日常消防巡查的频次，减轻消防工作量，提高工作效率。

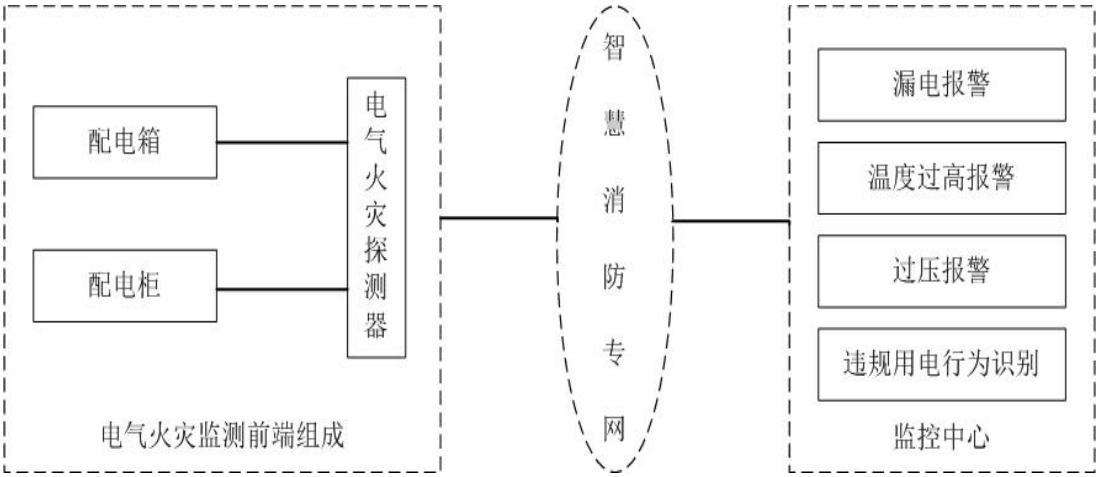


功能示意图

4.5.1.2 电气火灾监测

园区电气线路由于历史原因，部分线路有不同程度老化，大功率电器的使

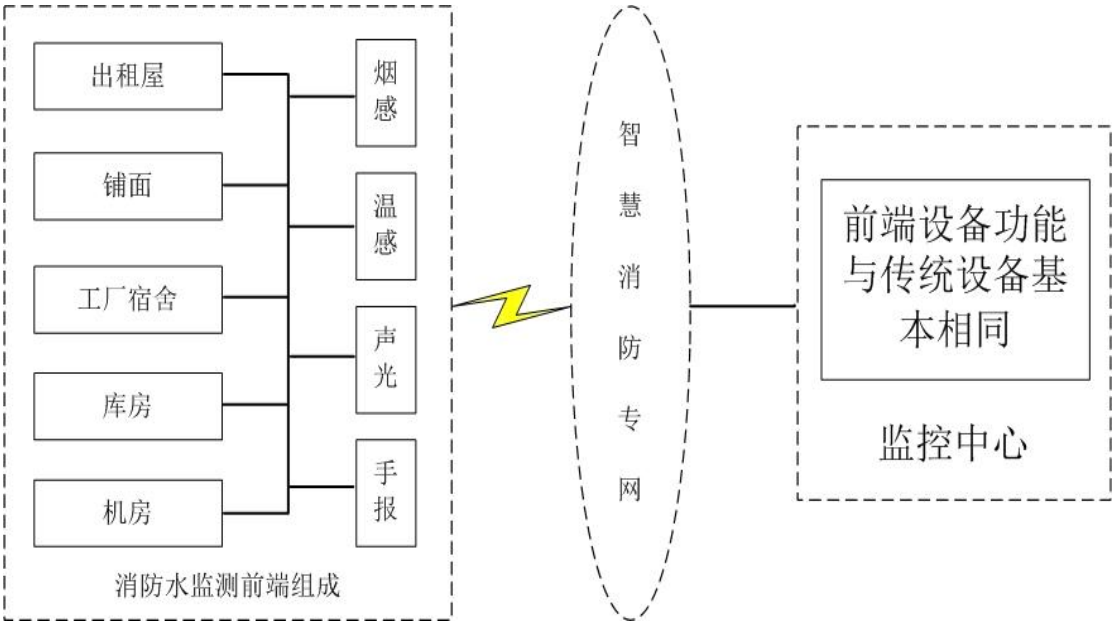
用使得用电量激增，用电高峰时期线路超负荷运转，存在安全隐患。未来建设单位可对智慧消防平台进行扩容，通过增加前端物联网设备，如电气火灾探测器对电柜/电箱进行覆盖监控，实时监测漏电、温度状态，电动车非法充电状态等，充分保障园区用电安全。



功能示意图

4.5.1.3 消防主机覆盖盲区补盲

企业所辖园区内部分出租屋、铺面、工厂宿舍、库房等场景消防主机覆盖有零星盲区，针对这些零星盲区如进行传统消防模式增设设备成本过高，安装复杂，极易影响日常的生产运营活动，未来建设单位可对智慧消防平台进行扩容，通过增加前端物联网设备应用无线传输技术（前端设备采用无线安装、电池供电，无需布线）安装无线烟感、无线声光、无线手报等无线传感器进行覆盖补盲。



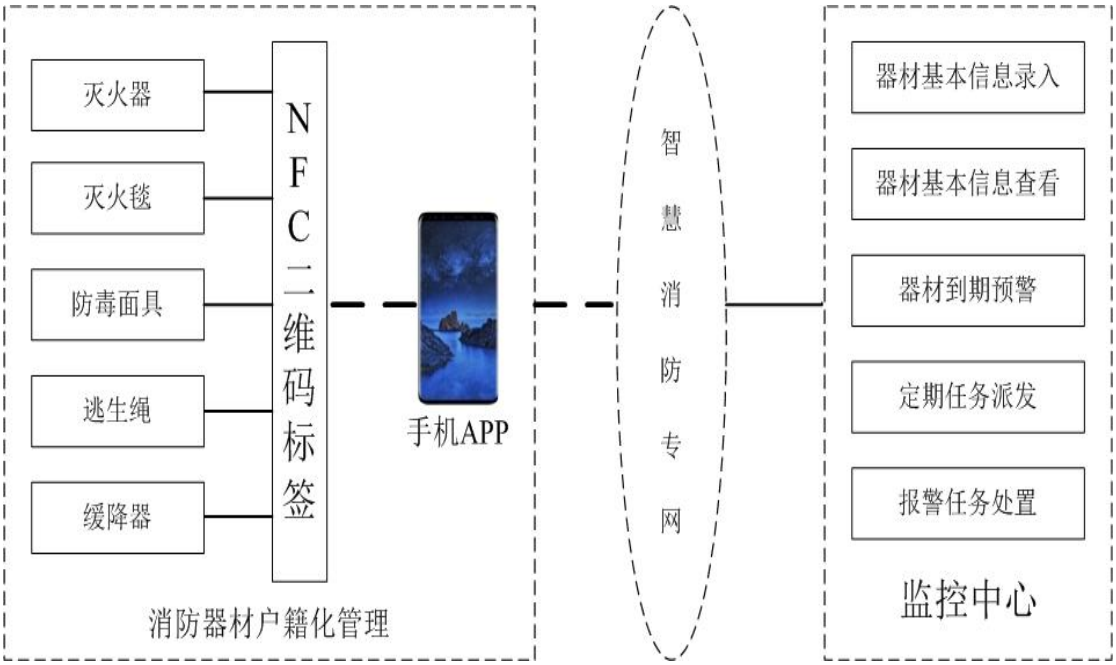
功能示意图

4.5.1.4 消防器材户籍化管理

随着消防配套设施日渐增加，日常消防安全工作量激增，人手短缺，传统消防设施管理模式已难以应对现有消防安全需求。当前企业所辖园区消防器材缺乏信息化管理，相关信息依托纸质台账，信息录入、查询费时费力，纸质文件易丢失；消防设施的数量、种类、批次多，依靠传统的记录方式难以提前有计划的进行更换，对于日常巡查人员缺乏监督手段。未来建设单位可对智慧消防平台进行扩容，通过增加 NFC 二维码标签一一对应消防器材，将器材信息录入系统，实现如下功能：

1、消防器材纳管：对于园区消防器材，可对每个消防器材张贴“NFC+二维码”标签，将消防器材信息录入系统统一管理，可进行设施到期提醒。现场使用手机 APP 扫码或 NFC 感应可查看消防设施信息，便于维护保养。

2、巡检监督：可设置巡查任务，派发工单给相关负责人，巡查人员使用手机 APP 现场 NFC 打卡，监督每日巡查任务完成状况，后台可查看任务完成情况与统计。



功能示意图

4.6 关键技术路线

4.6.1 物联网 IOT 技术

IOT 技术是指以网络为载体，建立的一种万物互联的信息系统，也就是物联网。通过物联网技术可有效地对系统内的信息节点进行精准定位，依托于固定的信息服务协议，将承接物联网信息采集的传感器进行有效关联，保证数据信息在采集与应用过程中实现精准定位以及全过程跟踪。

本项目将消防主机的各类报警、状态等信息进行全方位的信息化处理和利用，实现智慧化、网络化、远程控制等管理，管理人员可以根据报警信息，快速做出反应和对策。

4.6.2 大数据技术

大数据技术的应用则是对信息价值本身进行深度挖掘，其通过精准的数据模型，来对内部信息的某一个节点进行多维度统计，结合变化趋势，进而挖掘出信息在相关领域中起到的作用，为相关人员提供决策类信息。在生命周期过程中，由于数据源信息的传输渠道具有较大差异性，传统的数据整合形式无法对信息进行高效率处理，而通过大数据技术即可实现数据管理的集成化与综合

化，通过相关信息的界定来分析出符合园区需求的决策类信息。大数据技术的应用，消防大数据技术将多而繁杂的相关数据进行归集、整合，并通过展示中心可视化、直观化、图形化数据的汇集分析，满足事件监测预警、指挥调度、分析决策及对外宣传需要，从微观到宏观各角度进行精细管理。

4.7 实施方式

智慧消防平台建设依托于局域网，新建一套软件系统，通过前端设备实现对消控室消防主机的联网集中监控，项目实施由中标第三方厂商负责，应用系统运维则由建设单位负责。

4.8 主要硬件性能需求

4.8.1 系统服务器

云资源实现，租用浏阳经开区政务云的服务器资源，要求 CPU 8C，内存 16G，硬盘容量 1T，双向 100M 网口。

4.8.2 监控电脑

处理器 i7，内存 16G，最大支持 128GB，硬盘 1TB ，键盘、鼠标、显示屏。

其余详见技术参数指标。

4.8.3 大屏

大小及清晰度：100 寸，分辨率 3840 x 2160。

亮度：500 尼特以上。

刷新率：120HZ 以上。

其余详见技术参数指标。

4.8.4 智能网关

要求兼容网络协议 TCP/IP 协议。

支持以太网连接。

支持通信线路检测和故障管理。

具备 RJ45、RS232、RS485、CANBUS、继电器输出、采集通道等接口。

其余详见技术参数指标。

4.8.5 控制终端

支持 DI 输入，DO 输出。

支持以太网连接。

支持 RJ45、RS232、RS485、CAN。

其余详见 11.1 投资估算明细表。

第五章　本期建设方案

5.1　建设目标、规模与内容

5.1.1　建设目标

本项目建设目标是为了响应公安部消防局、湖南省、长沙市等要求加快智慧消防建设，推进信息化预警系统建设的要求，基于浏阳汇远实业有限公司下辖园区消防人力成本居高不下、设施状态难把握、信息化管理水平不足等消防管理现状，通过建设智慧消防平台，实时监控浏阳汇远实业有限公司下辖园区消防设施运行状态，实时感知状态，多维度预警，从而优化人员配置，节省人力成本，也提升了火灾事前预警能力及险情处置能力。

具体建设目标如下：

（1）实时感知状态，多维度预警：前端设备对 13 个消控室的各种品牌型号的消防主机进行整合联网，通过智慧消防平台，可实现消防主机报警、设备故障等实时预警，并通过系统消息、短信等多种方式通知相关负责人。督查人员对事件进行现场查看落实，并将处理结果录入系统，系统事件自动分类存储，实现消防管理工作闭环的同时，也为消防安全工作提供高效、便捷的数据支持。

（2）远程联动管控，提升工作效率：通过智慧消防平台，实现对消防主机的远程消音、复位等操作。根据消防主机探点的报警情况，可操作远程启停消防水泵、排烟风机等设施，保障险情发生时及时启动消防设施。同时通过远程监测设施故障运行状态，及时安排人员处理故障，提升消防设施的维护效率，平台预留接口，后期可按需接入其它物联网设备及联动门禁、道闸等业务系统。

（3）优化人员配置，节省人工运维成本：智慧消防平台可实时监控各消控室消防主机报警、故障运行状态，用户单位可按需释放值班人员，无需常年“蹲守”消控室，实现各消控室值班合理减员，有效解决持证人员配置不足的问题，优化人员配置，降低人力成本。

5.1.2　建设规模

本项目将建设单位辖区（含产业园区、公租房小区、商业办公楼宇以及金

阳集团办公楼、文化馆、金阳文化艺术中心等消防控制室）范围的智慧消防平台，对 13 个消控室的各品牌各型号的消防主机进行整合联网，统一管理。

5.1.3 建设内容

本项目将建设单位辖区（含产业园区、公租房小区、商业办公楼宇以及金阳集团办公楼、文化馆、金阳文化艺术中心等消防控制室）范围的智慧消防平台，对 13 个消控室的各品牌各型号的消防主机进行整合联网，统一管理。

本期建设内容主要包括：

建设一套智慧消防监控管理系统，结合前端设备对 13 个消控室的消防主机进行整合统一管理，实现消防主机的报警、设备故障情况的实时预警，并可通过智慧消防平台项目远程对消防主机进行手自动切换、消音、复位及远程启停消防水泵、排烟风机等重要消防设施，保障险情发生时能及时启动消防设施。

设立智慧消防平台监控中心，设在智中心公租房 1 栋 1 楼。智慧消防平台实时预警，可将系统界面投屏，一目了然，辅助总监控中心对现场情况进行迅速判断，方便应急调度。对各消控室划分区域，报警时发送报警短信给各自区域的负责人，提醒及时处理。

分控室远程联动控制建设：使用智能网关采集消防主机报警、故障运行状态，系统实时预警；通过控制终端及针对园区当前各品牌型号主机定制开发不同的驱动软件，实现主机远程手动/自动切换、消音及复位，水泵、风机远程启停等远控操作。

视频辅助系统建设：每个主消控室安装摄像头，值班人员可查看消控室视频，及指导现场人员操作主机。

监控室同步优化：因大部分项目消控室内设有监控室，并由消控室值班人员兼管。综合考虑监控管理的实操性及监控室改造投入运营成本，拟采用单个园区或项目集中区域设置总监控室，以确保消控室整合后监控室值班同步优化。

平台预留接口：预留第三方业务系统接口，可在未来按需接入其它物联网设备或联动门禁、道闸等业务系统。

5.2 技术架构设计

5.2.1 概述

（1）监控中心建设

设立智慧消防监控中心，暂定于智中心公租房 1 栋 1 楼，主机报警、故障事件监控中心智慧消防平台项目实时预警。将系统界面投屏至大屏，一目了然，辅助监控中心对现场情况进行迅速判断，方便应急调度。对各消控室划分区域，报警时发送报警短信给各自区域的负责人，提醒及时处理。

（2）前端建设

使用消防主机采集智能网关采集消防主机报警、故障运行状态，系统实时预警；通过控制终端及驱动软件，实现主机远程手自动切换、消音及复位，水泵、风机远程启停等远控操作。

视频辅助，每个主消控室安装摄像头，值班人员可查看消控室视频及指导现场人员操作主机。

5.2.2 监控中心建设

设立智慧消防监控中心，暂定于智中心公租房 1 栋 1 楼，系统服务器、监控终端、大屏、消控室视频存储设备等部署于监控中心。配置 1 台 100 寸大屏放置在监控中心，系统界面投屏至大屏，在大屏上一目了然，方便应急调度。

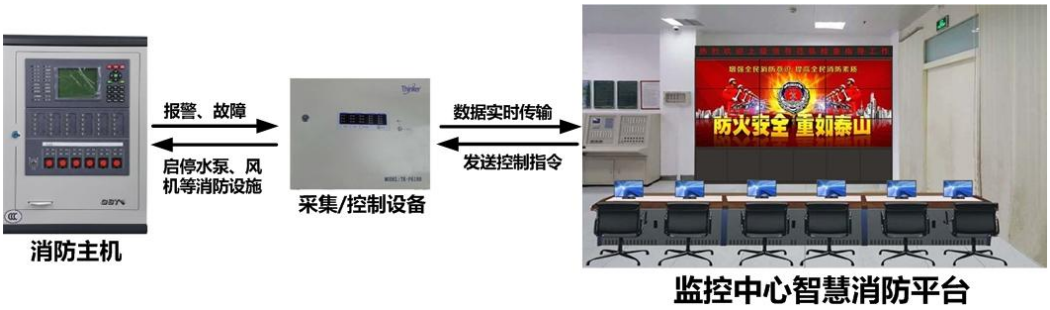
监控中心示意图

5.2.3 消防主机联网监控

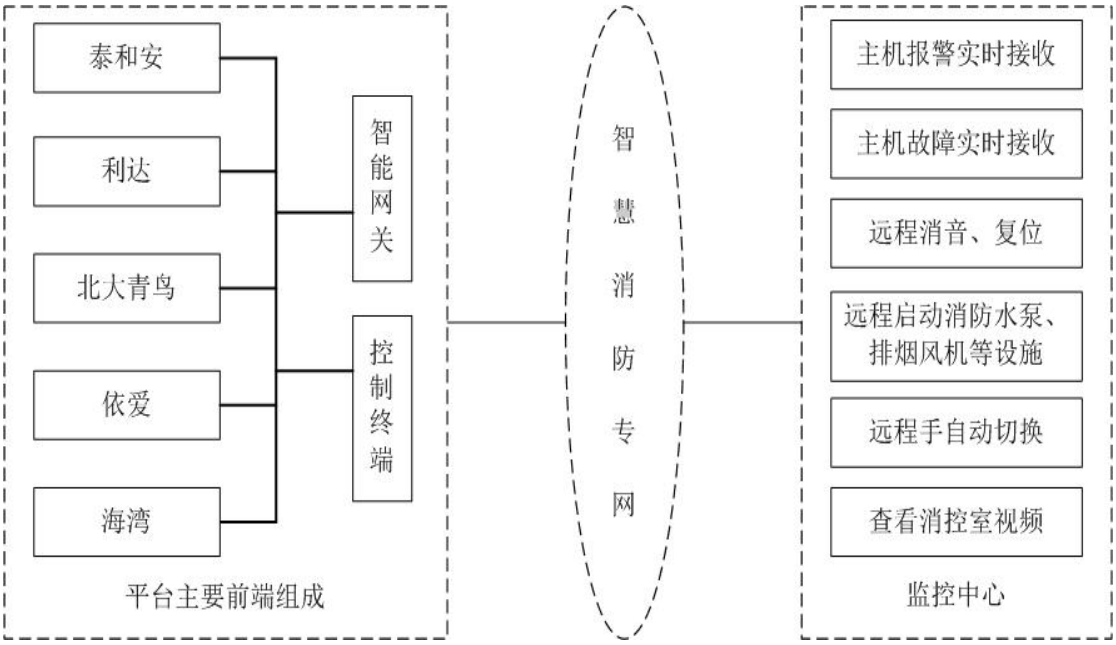
园区现有泰和安、利达、北大青鸟、海湾、依爱等不同品牌型号的消防主机共 35 台，分散在 15 个消控室内。本期项目需要联网的是 13 个消控室的 33 台主机。由于地理位置分散，没能集中监控，主机运行状态无法实时把握，所需人力成本也居高不下；如按《消防控制室通用技术要求》（GA767-2008）/（GB25506-2010）关于消控室值班人员数量的相关规定，每个消控室每班至少有 2 名值班人，一天 3 班倒，一天就需至少 6 人值班，再加 1 人轮休，且都需持证上岗；目前主机无法实现远程控制，人员现场确认主机发生的报警、故障事件后仍需折返回消控室主机上进行消音复位；为避免误报引发主机联动，常规情况下主机为手动状态，因此消防水泵、风机等设施的启动、停止需要人员在现场操作，沉重的人力成本和消防工作量也给企业造成很大压力，消防控制室则由于某些主客观原因，存在值班人手不够的问题。为节省成本，加强火灾报警应急调度和统一管理。拟使用智能网关采集消防主机的报警、故障运行状态，系统实时预警；通过控制终端及驱动软件，在智慧消防平台项目上实现主机远程手自动切换、远程消音及复位，水泵、风机远程启停等远程控制操作。缓解消防工作人手紧缺的问题，同时根据实际情况灵活缩减值班人员，节省人

员成本，减轻企业消防工作压力，又能保障在险情时能及时启动相关消防设施。根据建设单位提供的图纸，将主机点位一一对应生成电子地图，一目了然。

每个消控室配置 2 台高清网络摄像机进行视频辅助，监控中心值班人员可查看消控室视频及指导现场人员操作主机。



联网监控示意图



功能示意图

5.2.4 短信分区推送

根据园区消控室分布及负责人情况，划分不同的区域，主机报警在系统上显示的同时根据不同区域发送短信给各自区域的负责人，便于属地化管理。

5.3 标准规范建设

5.3.1 参考标准

本项目标准规范体系建设是依托于国家及各省市智慧消防相关政策及规范，主要参考如下标准目录，详见下表：

表 3-1 智慧消防相关标准规范表参考

序号	标准名称	标准编号
1	公安部消防局《关于全面推进“智慧消防”建设的指导意见》	（公消〔2017〕297 号）
2	湖南消安委《湖南省“十四五”消防救援事业发展规划》	（湘消安〔2021〕5 号）
3	国务院安委会《“十四五”国家消防工作规划》	（安委〔2022〕2 号）
4	国务院安委会《安全生产治本攻坚三年行动方案（2024—2026 年）》	（广东省第十三届人民代表大会常务委员会公告第 107 号）
5	广东省人大代表常委会《广东省实施〈中华人民共和国消防法〉办法》	（安委〔2024〕2 号）
6	《广西壮族自治区实施〈中华人民共和国消防法〉办法》	（广西壮族自治区第十四届人民代表大会常务委员会第三次会议）
7	《重庆市消防设施管理规定》	（重庆市第六届人民代表大会常务委员会第七次会议）
8	《消防控制室通用技术要求》	（GA767—2008）/（GB25506-2010）
9	《城市消防远程监控系统》	GB26875-2011
10	《火灾自动报警系统设计规范》	GB50116-2013

5.3.2 本期新建规范

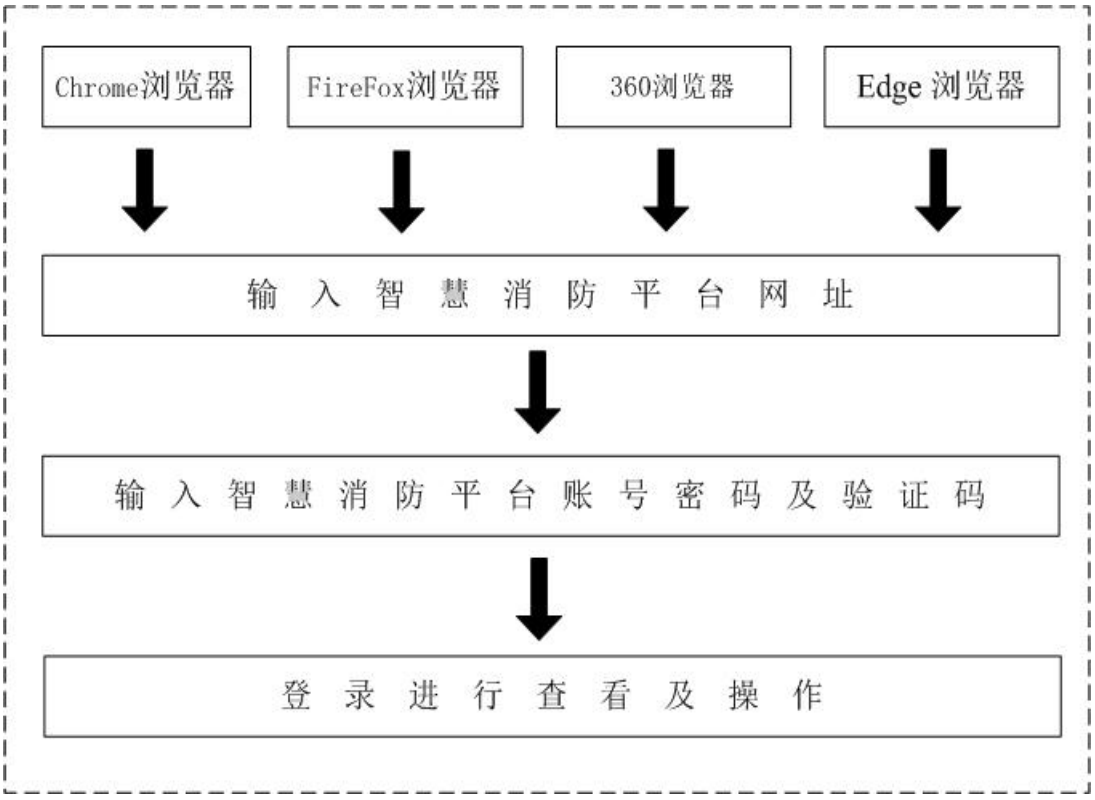
本期项目不新建标准规范。

5.4 应用系统建设方案

本期智慧消防平台包含但不限于数据总览、实时监控管理、设施管理、网格管理、智能巡查、档案管理、数据分析、系统设置等基本功能。同时需预留未来可拓展的端口，根据未来的园区实际需求增加新的功能模块。

5.4.1 系统登录

采用 B/S 架构，将系统功能实现的核心部分集中到服务器上，简化了系统的开发、维护和使用。用户通过浏览器输入网址、账号、密码即可直接登陆，无需安装客户端软件，多个账号的开通和使用只需使所用电脑位于同一网段内，通过浏览器输入网址、账号、密码即可登陆，无需安装客户端 APP，部署和后期维护、升级都很方便。



登录示意图

5.4.2 数据总览

该功能模块支持一张图总览单位消防设备数据，综合展示报警情况、监控

场所情况、设备数量、设备运行情况、报警趋势、报警分类等信息。一目了然，直观明了。

数据总览对用户使用的当前账号下管辖的所有设备的归纳统计展示，具体功能如下：

（1）设备的最新报警情况，审计确认的真实火警情况。

（2）设备数量统计展示。

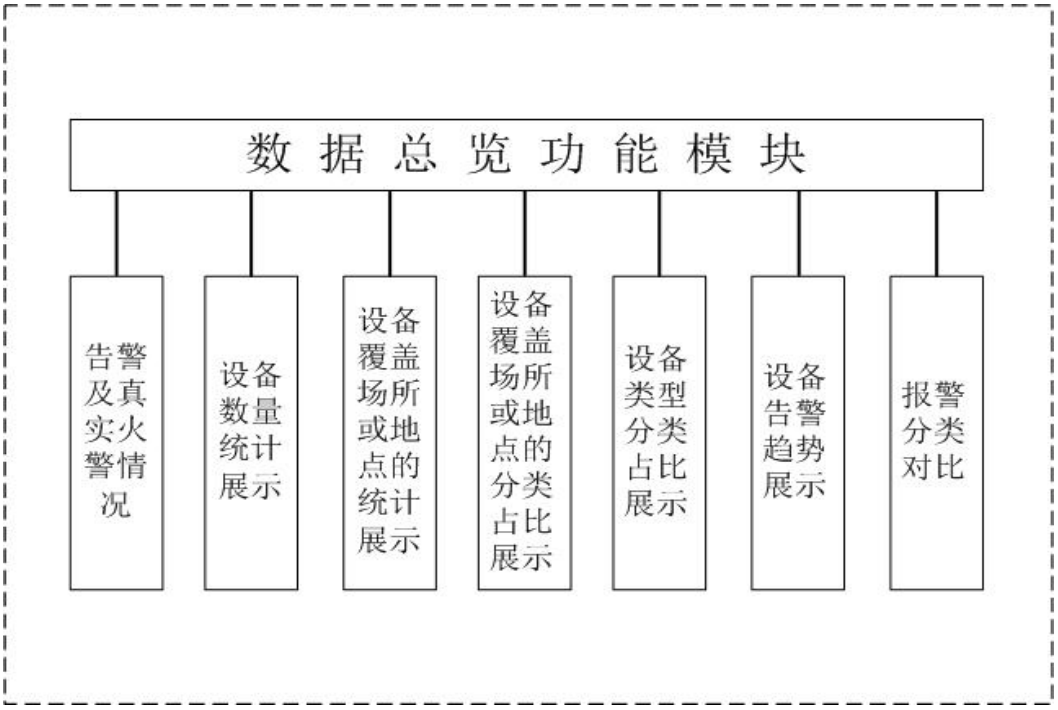
（3）设备覆盖场所或地点的统计展示。

（4）设备覆盖场所或地点的分类占比展示。

（5）设备类型的分类占比展示。

（6）设备的报警趋势的展示。

页面的模块构成并非固定，可以根据用户的实际需求展示其关心的重点数据，各个模块可放大缩小观看，便于用户的查看，如设备报警情况、设备数量、所管辖的场所或地点这些重要的数据，需能在数据总览界面点击查看简单的信息，至于具体的信息则进入详细的功能模块进行查询。



功能示意图

5.4.3 实时监控管理

该功能模块支持接入消防主机（本期接入，未来亦可接入其他智慧消防相

关的设备），实现设备报警、故障等信息的实时接收，报警支持弹窗，弹出报警点信息及电子地图，报警时进行声音、闪烁警示等；报警除在系统显示外，还支持短信方式进行推送，支持视频联动。

在网络正常的情况下，系统需支持 24 小时监控报警，具体功能如下：

（1）实时报警弹窗

发生报警时需能弹出报警点信息及与报警点对应的电子地图，报警时进行声音、闪烁警示，设备恢复正常后界面自动恢复正常显示。报警时闪烁红色最好，较为显眼。

（2）实时报警滚动显示

在页面显眼的地方滚动报警点的文字信息。

（3）报警点所在楼宇的建筑信息查看

可查看如建筑平面图、楼宇面积、楼层高度、建筑负责人、联系方式等基本信息。

（4）报警点所在楼宇的设备信息查看。

（5）报警短信推送

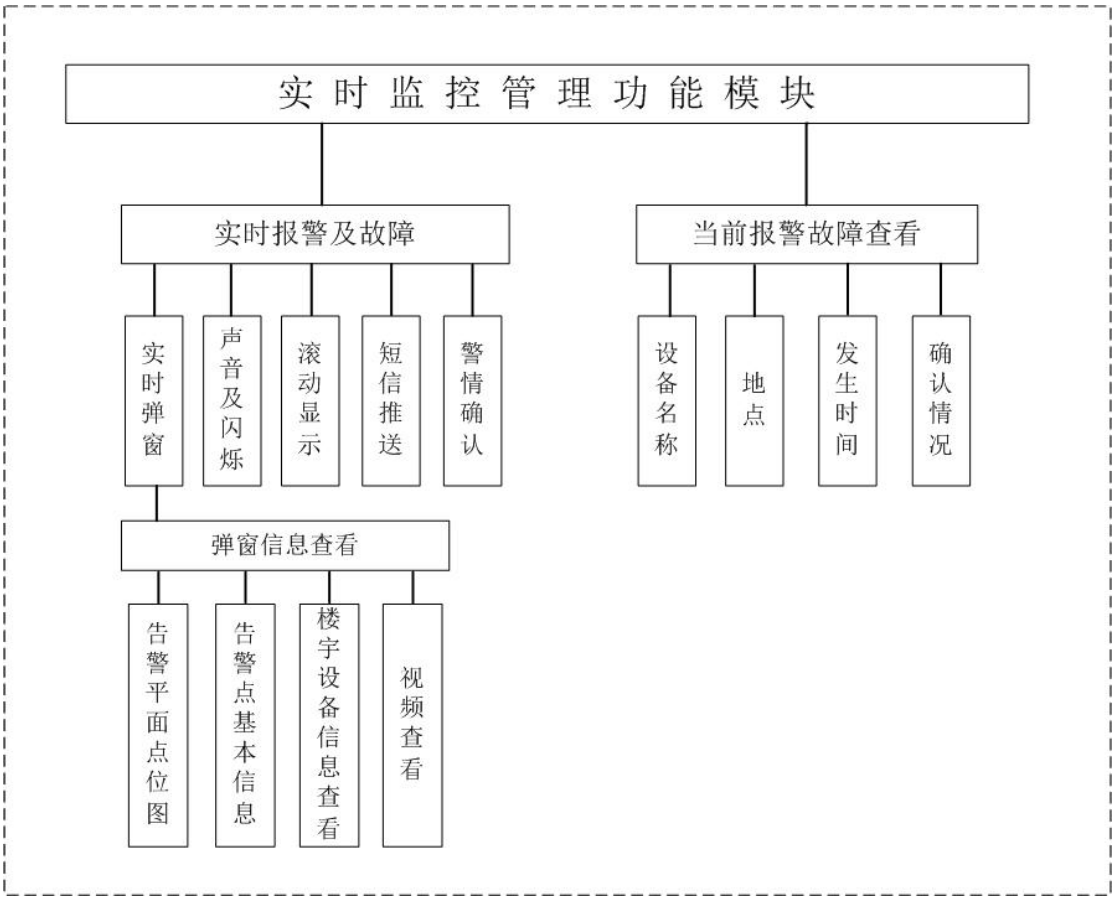
报警除了在系统界面显示外，同时发送报警短信给相应区域的负责人，便于属地化管理。

（6）报警视频查看

可查看报警点对应消控室视频。

（7）当前报警、故障列表显示

界面可点击查看当前设备报警、故障信息列表，简单展示即可，具体进入设备管理模块查询更多信息。



功能示意图

5.4.4 设备管理

该功能模块支持设备名称、类型、地点等多种方式查询设备信息；设备报警故障记录查询，实时数据查看等；设备报警、故障信息复核审计，报警、故障发生原因录入系统等；支持隔离配置等。

具体功能如下：

（1）设备信息查询

支持按设备名称、设备类型、设备所在地点等多种方式单独或组合查询设备详情等，并可将查询的结果以表格的形式导出，便于用户管理单位的消防设备信息。

（2）设备告警、故障信息查询

支持按设备名称、设备类型、设备所在地点等多种方式单独或组合查询设备的报警、故障详情。并可将查询的结果以表格的形式导出，便于用户管理单

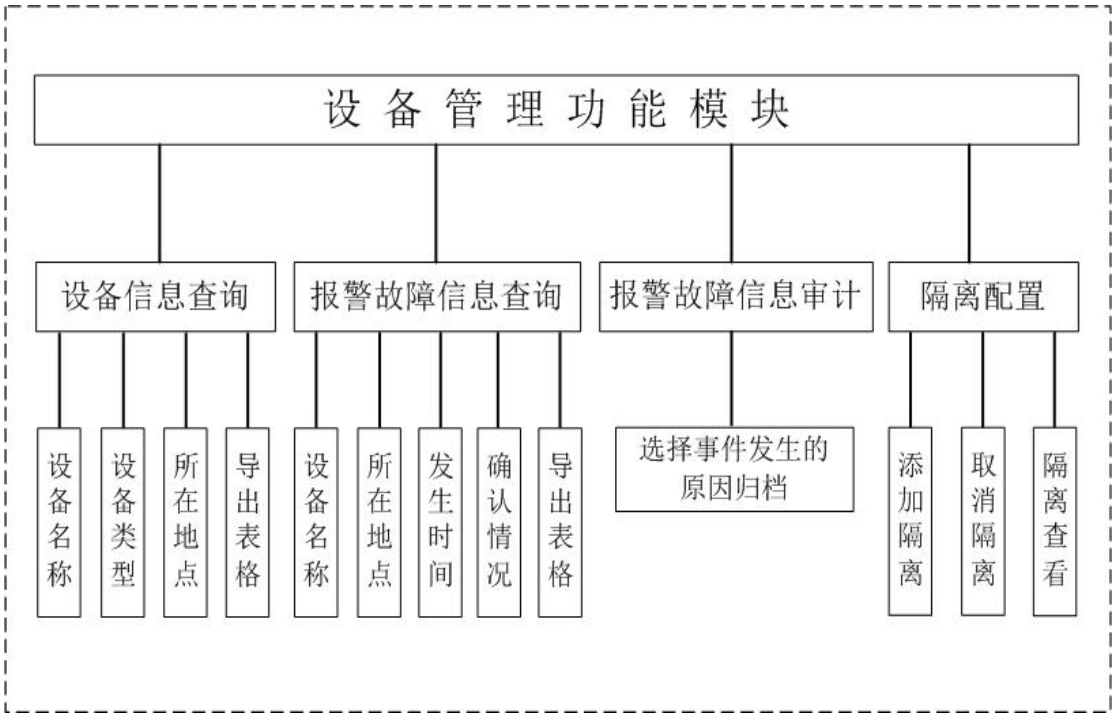
位的消防设备事件信息。

（3）设备告警、故障信息审计

支持设备告警、故障信息审计，监控中心值班人员可根据现场反馈的实际情况选择预设好的设备告警或设备故障原因对告警及故障信息进行归档，如可选择实际报警、误报报警、实际故障、误报故障等原因对事件进行归档，原因可根据实际修改，便于用户单位消防工作的闭环，也方便用数据辅助用户日常的决策。

（4）支持进行隔离配置

园区日常消防维保单位进行消防测试时会产生大量报警，可在系统上进行隔离配置，对需要测试的点进行隔离设置，避免大量的测试报警影响值班人员的判断。



功能示意图

5.4.5 网格管理

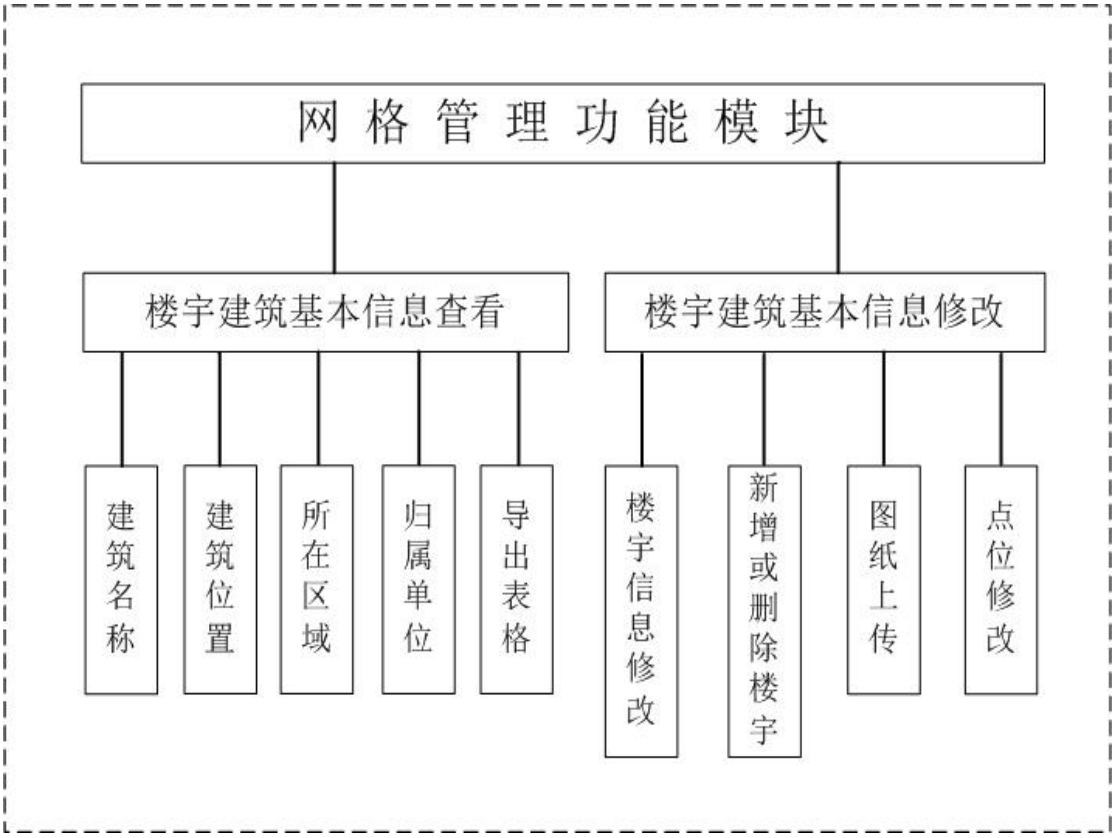
该功能模块支持以列表形式展示权限范围内所有的楼宇建筑信息，可以查看管理账号管辖的楼宇。具体功能如下：

（1）楼宇建筑基本信息查看

支持查看楼宇建筑名称、位置、区域、归属单位等基本信息，可查看到楼层、房间，并支持以表格的形式导出，便于用户管理单位的建筑楼宇信息。

（2）楼宇建筑基本信息修改

对账号管辖范围内的楼宇进行增加或者删除，并可对楼宇建筑名称、位置、区域、归属单位等基本信息修改、调整楼宇显示顺序、上传及更改楼宇建筑的平面图信息等。



功能示意图

5.4.6 智能巡查

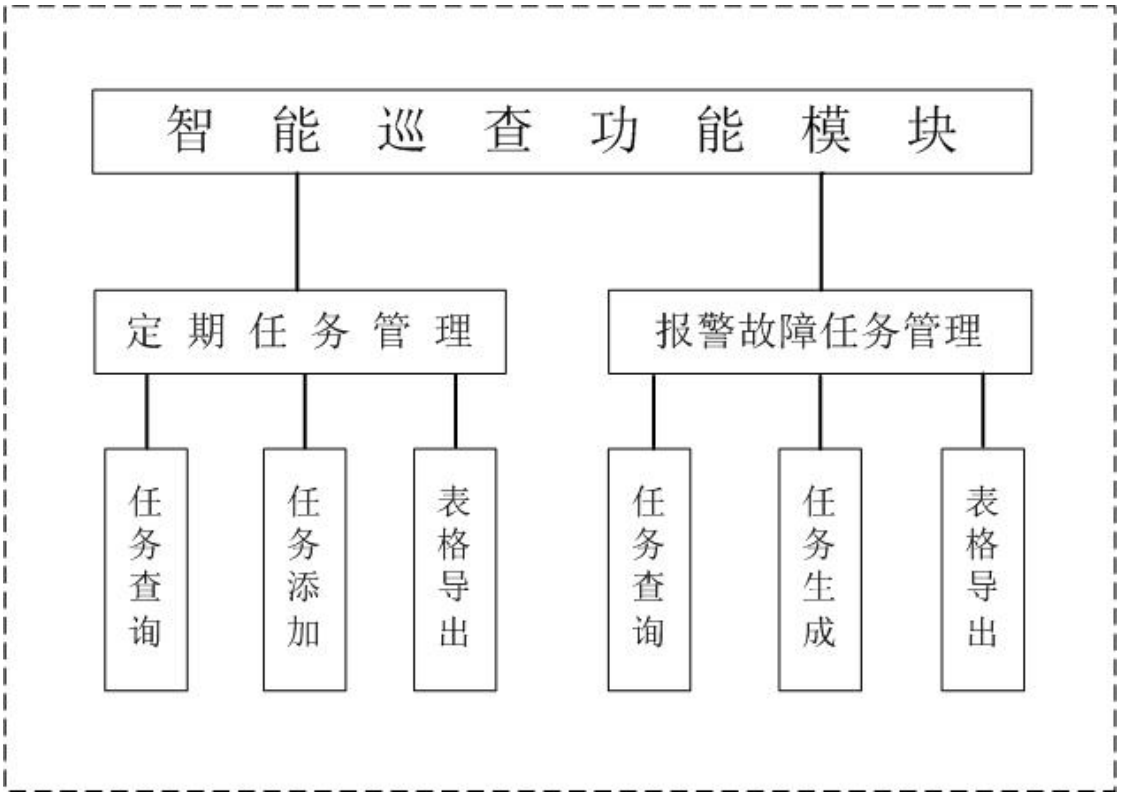
该功能模块支持派发任务，监督维保人员任务完成情况，保障消防设备正常运行，后台可查看任务完成情况。具体功能如下：

（1）定期任务管理

定期任务查询、添加，可查询当前定期任务的明细，可添加定期任务，规定定期任务的检查范围及检查频次等，如可按单次、日、周、月派发定期任务进行检查，任务完成情况后台均可查看，并支持以表格的形式导出。

（2）报警、故障任务管理

系统报警、故障信息均可自动生成任务工单，任务完成情况后台均可查看，并支持以表格的形式导出。



功能示意图

5.4.7 档案管理

该功能模块支持支持人员证件、合同、保险、消防法规文件等文件的上传添加、查询。具体功能如下：

（1）人员证件管理

可以列表形式显示人员证件情况，包括：用户名、证照分类、证照编号、签发日期、有效日期等，支持证照信息添加。

（2）人员合同管理

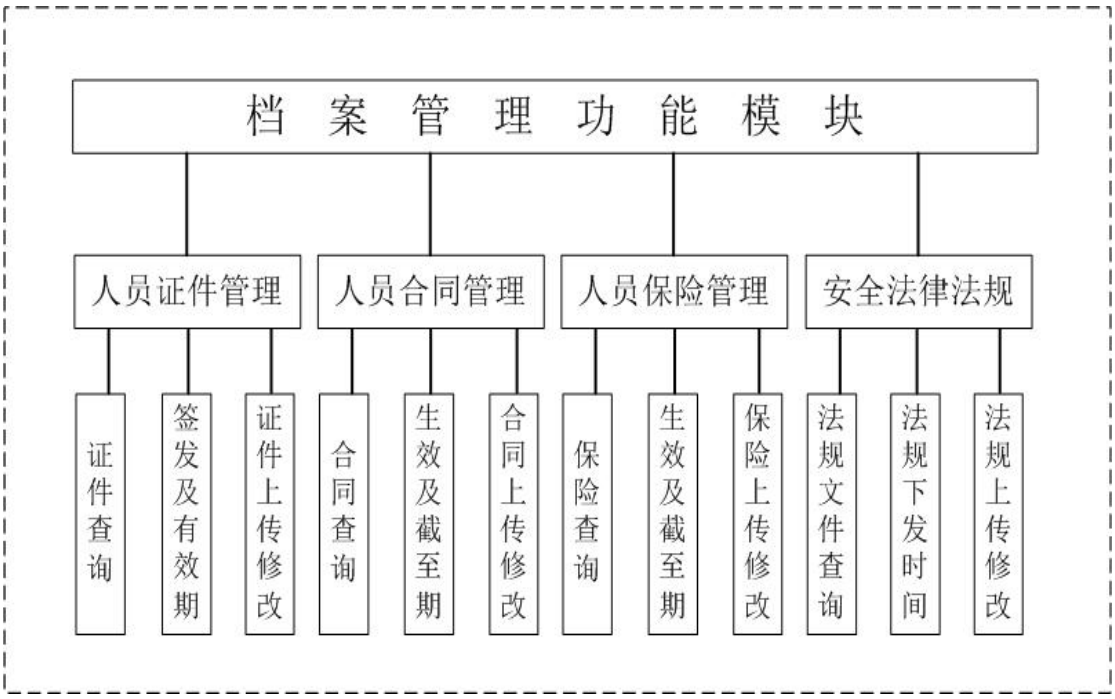
可以列表形式显示合同信息，包括：用户、合同分类、合同编号、生效日期、截止日期等，支持合同信息上传、添加。

（3）人员保险管理

可以列表形式显示保险信息，包括：用户、保险分类、保险编号、生效日期、截止日期等，支持保险信息添加。

（4）安全法律法规

可以列表形式显示消防法规文件信息，包括：文件分类、文件名称、下发时间、关键词等，支持法律法规文件添加。



功能示意图

5.4.8 数据分析

该功能模块图文展示实时告警、故障数据，分布图、趋势图查看等。具体功能如下：

（1）实时险情

图文展示当前实时告警、故障汇总数据，占比等，支持图片保存。

（2）险情分布图

以地图方式展示险情分布情况。

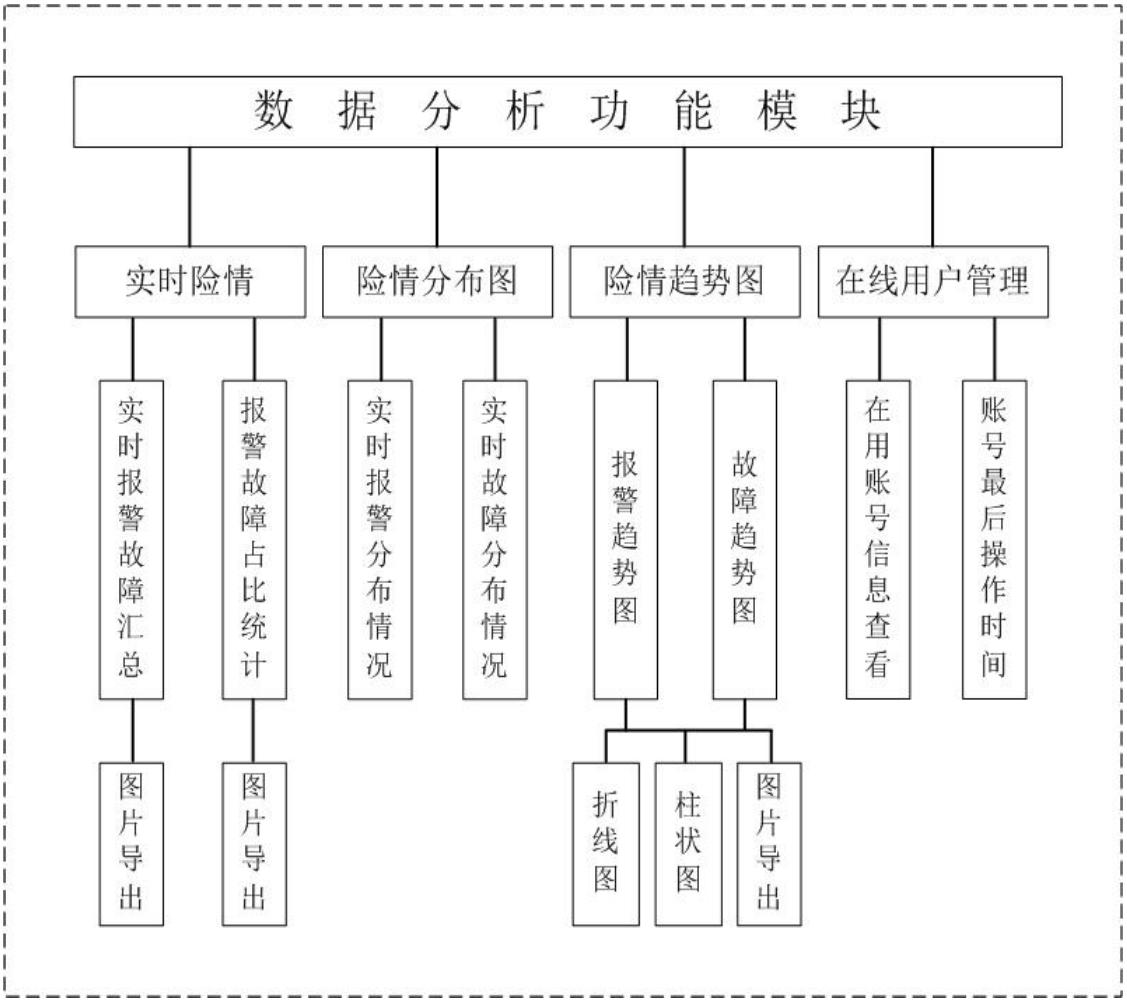
（3）险情趋势图

统计告警及故障险情情况，支持以柱状图、折线图等多种方式进行展示，

支持图片保存。

（4）在线用户管理

以列表形式，显示用户登录名、角色、手机号码、有效日期、最后操作时间等信息。



功能示意图

5.4.9 系统设置

系统支持对用户账号进行添加、修改、删除等操作，可给每个用户分配管辖范围权限等，支持告警原因等系统数据定义，支持菜单栏修改等。具体功能如下：

（1）用户管理

可以对用户账号进行添加、修改、删除等操作，可给用户分配管辖范围权限等。

（2）系统数据定义

支持对告警原因、设施类型分组等系统数据进行定义，支持添加、修改、删除等操作。

（3）短信管理

支持不同的查询条件（接收人、手机号码、事件类型等）单独或组合查询短信发送详情，是否已发送短信，并支持以表格的形式导出。

（4）日志查询

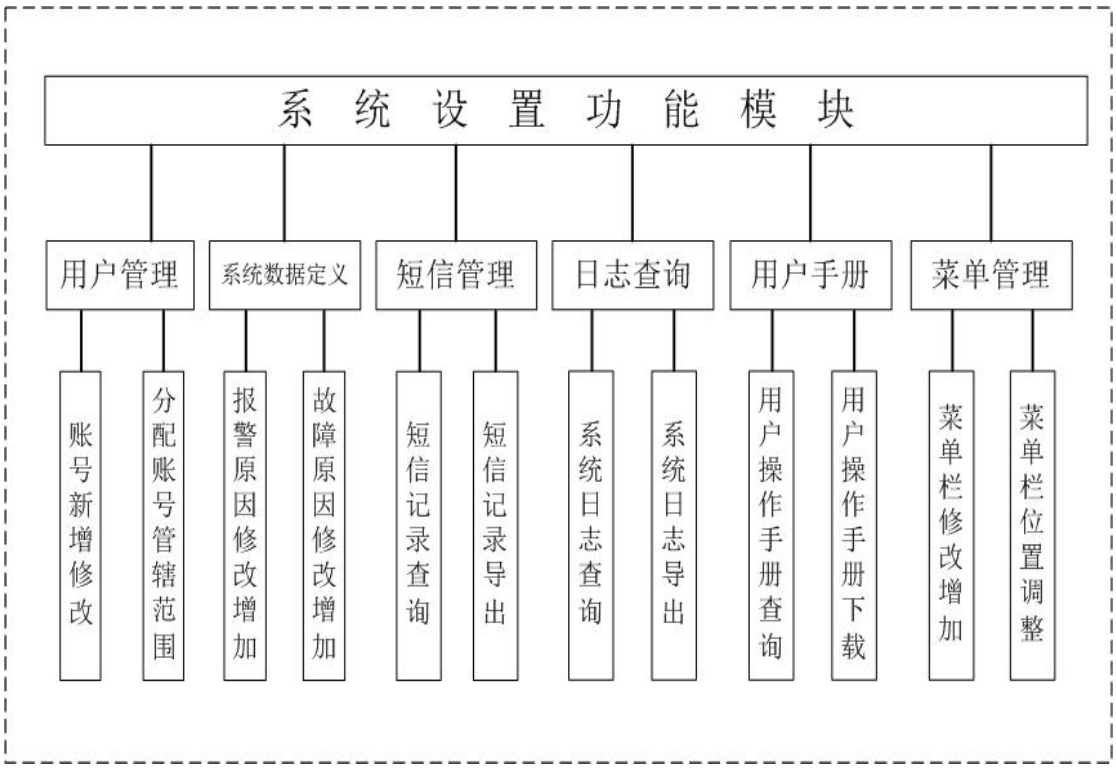
支持系统日志查询，包括每个账号的登录时间、IP 地址等信息，并支持以表格的形式导出。

（5）用户手册

支持内置系统操作手册，用户可随时下载查看，便于系统操作。

（6）菜单管理

支持对系统菜单栏进行修改，包括菜单栏名称、菜单栏增加及修改、菜单栏位置调整等。



功能示意图

5.5 配套工程建设方案

对于本项目消防主机的联网监控，为保证数据传输的稳定性及可靠性，前端设备应尽可能采用有线的形式连接，有线网络稳定性高，能保证数据的可靠传输。

5.5.1 前端消控室改造

前端消控室配置智能网关、消防主机通信模块、控制终端，采集消防主机告警、故障运行状态，系统实时预警；通过控制终端及驱动软件，实现主机远程手自动切换、消音及复位，水泵、风机远程启停等远控操作。

同时每个前段消控室安装摄像头，值班人员可查看消控室视频及指导现场人员操作主机。

5.5.2 安防消控室改造

创新创业园、新能源产业园两处安防监控中心由消防值守人员兼管，为满足后期安防管理需求，并且不增加安防管理人员，将该 2 处安防监控室迁移至所在园区门岗室。主要涉及硬盘录像机、监视器大屏、交换机等设备的迁移及系统调试，及少量综合布线。

5.5.3 网络系统建设方案

传输设备：采用高性能的交换机，至少支持千兆以太网接口的交换机，以满足网络传输需求，交换机也需预留 2 口以上的冗余。

网络连接施工：根据建筑结构和设备分布情况，规划合理的网络布线方案。对于有线网络部分，要避免与强电线路平行布线，防止电磁干扰。在布线过程中，做好线缆的标识和保护，便于后期的维护和管理。

网络带宽要求：租用运营商的光纤资源（20M）组成智慧消防业务网（局域网）。

5.6 安全体系建设方案

5.6.1 项目基本情况

本项目依据《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）第二级进行安全环境搭建，平台部署在浏阳经开区数据中心机房。

依据《信息安全技术关键信息基础设施确定指南》（试行），本项目主要为实现公司所辖消防室的监控信息统一管理。不涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，同时本项目信息遭到破坏、丧失功能或者数据泄露时，不会出现严重危害国家安全、国计民生、公共利益的情况，因此本项目不属于关键信息基础设施。

本项目数据不涉及跨组织流动，因此不涉及数据跨境管理。

5.6.2 安全设计目标及原则

围绕《信息安全技术网络安全等级保护基本要求》中关于政务信息系统在系统规划阶段的安全体系要求，综合考虑本项目建设平台的“安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理”等层面的安全需求，设计合规、正确、有效的网络安全方案，满足《基本要求》中二级指标要求，并为通过网络安全性评估奠定基础。

网络安全设计应遵循以下原则：

（1）总体性原则。通过从整体层面，对本系统的网络安全开展顶层设计，明确安全需求和预期目标，并与本系统网络安全保护等级相结合，通过系统的设计形成涵盖技术、管理、实施保障的整体方案，为在本系统中落实网络安全相关要求奠定基础。

（2）完备性原则。围绕本系统实际业务应用与安全保护等级，站在整体角度，通过自上而下的体系化设计，综合考虑物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等多个层面网络安全需求，设计本系统网络安全方案。

（3）经济性原则。结合本系统规模，在合理、够用的前提下，设计满足

《基本要求》的网络安全改造，确保本系统网络安全投资合理，规模适度，避免资金浪费和过度保护。

5.6.3 安全需求分析

5.6.3.1 系统安全需求

- 符合国家要求的应用系统安全等保要求，按系统性质分类做好安全防护；
- 对现有主机系统进行安全检查，并进行相应的安全配置、加固；
- 保护服务器上的数据以及服务器提供的服务，防止非授权的访问；
- 建立防病毒系统，保证全网不被病毒的侵害；
- 提供及时自动化进行系统修补的解决方案；

5.6.3.2 应用安全需求

- 应提供访问控制功能，依据安全策略控制用户对文件、数据库等客体的访问；
- 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；
- 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
- 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。

5.6.3.3 数据安全需求

- 应能够检测系统管理数据、鉴别信息和重要业务数据在存储、传输过程中完整性是否受到破坏，并在检测到完整性错误时采取必要的恢复措施；
- 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；
- 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性；
- 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据的存储保密性；

5.6.3.4 网络安全需求

- 对现有网络设备进行安全检查、加固，并进行相应的升级；
- 实现政务外网与互联网及不信任域之间的隔离与访问控制并做日志；
- 建立合理的网络结构，对接入区进行分类汇聚和隔离；

5.6.3.5 安全管理需求

- 建立安全组织结构，确定安全管理职责；
- 建立制定一套完整可行的安全策略和管理策略；
- 建立安全响应制度，并建立安全响应小组；
- 提供全面的安全知识培训，增强整体人员的安全意识及反黑技术。

5.6.3.6 等级保护合规安全需求

安全物理环境需求：安全物理环境是信息系统安全运行的基础和前提，是系统安全建设的重要组成部分。在等级保护基本要求中将物理安全划分为技术要求的第一部分，从物理位置选择、物理访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等方面对信息系统的物理环境进行了规范。

安全通信网络需求：安全通信网络是在安全计算环境之间进行信息传输及实施安全策略的软硬件设备，是本次项目建设系统的重要基础设施，也是保证数据安全传输和业务可靠运行的关键，更是实现平台数据内部纵向交互、对外提供服务、与其他单位横向交流的重要保证。

安全区域边界需求：安全区域边界安全对安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关软硬件设备。区域边界安全防护是实现各安全域边界隔离和计算环境之间安全保障的重要手段，是实现纵深防御的重要防护措施。通过边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证，实现保护环境的区域边界安全。

安全计算环境需求：安全计算环境是对系统的信息进行存储、处理及实施安全策略的相关软硬件设备，安全计算环境包括各类计算服务资源和操作

系统层面的安全风险。

5.6.4 安全技术方案

5.6.4.1 安全物理环境防护

信息系统等级保护二级对物理层的防护要求包括：物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等方面，智慧消防平台部署在浏阳经开区数据中心机房，物理环境由浏阳经开区云平台提供支持。

5.6.4.2 安全通信网络防护

5.6.4.2.1 通信传输

应采用校验技术保证通信过程中数据的完整性。

（1）拓扑还原，绘制与当前运行情况相符的网络拓扑结构图；

（2）建立双冗余链路，通过网络拓扑结构图，分析网络单故障点，建立双核心交换机，通过楼层交换机与双核心交换机建立冗余链路，消除网络安全风险；

（3）路由控制，在系统业务终端与业务服务器之间进行路由控制建立安全的访问路径。

根据智慧消防平台的服务对象、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段，实现对单位信息系统的安全域划分。

一是确定服务对象和重要性，本次系统服务的对象为浏阳汇远实业有限公司下辖园区各服务机构。

二是分析所涉及信息的重要程度，系统涉及的信息包括消防报警相关数据，分析各类信息的重要性和敏感性，以便进行安全域划分。

三是划分不同的子网或网段，由于本次系统部署在浏阳经开区数据中心机房，用户为国企以及政府部门，不再划分子网。

5.6.4.2.2 可信验证

可基于可信根对通信设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。包含以下工作：

（1）分区：根据智慧消防平台的所属不同、功能区别等将具有同种性质的系统划分到同一个区域进行防护，本次系统部署于浏阳经开区政务外网，并按照用户不同，对系统进行分区。

（2）分级：根据系统的重要程度不同，将重要程度一致的系统划分到同一级别的区域进行防护，如划分成安全和非安全（普通）或根据等级保护的要求划分一、二、三等各级别的安全网络等；本次项目分级按照等保二级要求执行。

（3）分域：将系统的应用程序及应用服务、中间件、数据库及备份等分在不同的作用域中分别进行防护。本项目部署在浏阳经开区数据中心机房，分域措施由浏阳经开区云平台提供。

5.6.4.3 安全区域边界防护

5.6.4.3.1 边界防护

在智慧消防平台的区域及网络边界利用云平台部署的防火墙系统进行网络边界的安全防护，保障跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。

利用智慧消防平台部署的网络准入控制管理系统防止设备非法接入内网及防止内网用户非法外联。

防止设备非法接入内网主要是通过身份认证等手段确认接入终端合法性，合法终端放行入网，一旦发现非法终端即采用技术手段中断其网络访问权限，拒绝其接入网络。

非法外联监控主要解决发现和管理用户非法自行建立通路连接非授权网络的行为。通过非法外联监控的管理，可以防止用户访问非信任网络资源，并防止由于访问非信任网络资源而引入安全风险或者导致死亡数据信息泄密。

智慧消防平台部署在浏阳经开区云平台的内部数据中心区，在同一个网络数据层交互对接进行使用云平台的智能网关做好网络策略安全控制。需要共享数据的外部单位或系统，需提出申请，经过严格的管控程序，通过边界访问区实现数据的互通和共享。

5.6.4.3.2 访问控制

通过调研和分析其网络现状，参照等级保护要求在相关边界利用云平台部署的防火墙系统进行访问控制，对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，除允许通信外受控接口拒绝所有通信，杜绝越权访问，防止各类非法攻击行为。

本项要求包括：

应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出。

5.6.4.3.3 可信验证

可基于可信根对边界设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警

5.6.4.3.4 入侵防范

在网络的区域边界利用云平台部署的入侵防御系统，提供 4～7 层的安全检测，防御从互联网来的网络攻击行为，并针对入侵行为进行检测，并能够阻断来自外部的数据攻击以及垃圾数据流的泛滥。

同时，将通过部署威胁检测与防御系统对全网流量进行准确监测，提供动态的、深度的、主动的安全防御。

提供全方位的 APT 攻击检测：深度分析已知漏洞攻击和 0day 攻击，帮助用户发现真正的黑客攻击；通过 web、邮件、文件检测系统的配合检测，全方位地发现 APT 攻击；关联分析能力强，快速识别 APT 攻击行为；直观展现 APT 攻击路径，安全威胁可视化。结合安全运维服务，对于用户无法确定的攻击行为和攻击样本，可提供高级技术支持，协助用户对攻击进行分析，用以对抗高技术的黑客。

系统为用户记录相关的攻击告警事件，支持分析事件结果并进行归纳统计，

具有极强的关联分析能力，为用户决策提供直观可靠依据。定期自动生成安全形势的总体分析报告，提供固定时间范围内的监控记录，并对监控记录进行分析、得出结论，形成风险分析报告，以供分析网络安全状况，提供依据。

5.6.4.3.5 恶意代码防范

利用云平台部署的防病毒网关系统，采用透明接入方式，在最接近病毒发生源安全边界处进行集中防护，对夹杂在网络交换数据中的各类网络病毒进行过滤，能够对网络病毒、蠕虫、混合攻击、端口扫描、间谍软件、P2P 软件带宽滥用等各种广义病毒进行全面的拦截。阻止病毒通过网络的快速扩散，将经网络传播的病毒阻挡在外，可以有效防止病毒从其他区域传播到内部其他安全域中。通过部署防病毒网关，截断了病毒通过网络传播的途径，净化了网络流量。

5.6.4.3.6 安全审计

利旧云平台部署的网络安全审计系统针对关键节点的用户行为进行审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。同时还将部署了安全事件统一管理系统针对设备以及主机日志进行统一的收集与审计，审计记录包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

5.6.4.4 物理安全设计

本项目服务器端使用的数据中心机房为现有浏阳经开区云平台机房，云平台机房环境条件满足国家标准《电子计算机机房设计规范》（GB50174-2008）、《电子计算机场地通用规范》（GB2888-2008）的要求，在场地、防火、防水、防震、电力、布线、配电、温湿度、防雷、防静电等方面达到 A 类机房标准要求。机房的建设和管理都严格保密，建设信息只有少数人员掌握。进入机房需建设单位授权同意。

另外云平台机房严格按照生产系统机房建设，配电系统、空调系统、防静电、防雷、消防、防水等均能满足相关要求。所有设备接入 UPS 电源，并配置发电机。机房设备使用双电源，当有一路电源失效时，仍可正常工作，同时做到系统的网络设备与公用网络相关设备实现物理隔离。

云平台机房在物理设备配置上，核心交换机、防火墙、出口路由器等核心通信设备均成对配置，以避免出现单点设备故障，满足物理安全的需求。

本项目智慧消防平台部署在浏阳经开区云平台机房的数据中心，安全防护等级为二级，浏阳经开区云平台机房提供的物理环境可满足系统安全建设要求。

5.6.4.5 网络安全设计

本项目依托云平台部署在网络安全上，充分利用云平台在网络中配置的防火墙、日志审计、入侵防范、漏洞扫描等安全设备保障本平台的网络安全。

配置入侵防范系统（IPS/IDS），在关键网络节点处检测、防止或限制从外部发起的网络攻击行为，当检测到攻击行为时，记录攻击源 P、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警和防御能力。

配置堡垒机，其基于 B/S（https）方式管理，提供基于静态口令认证的身份鉴别功能。通过鉴别用户可以根据预设的权限访问服务器，并记录用户登录成功和失败的审计日志。提供用户单点登录和运维操作行为审计功能，并能基于远程管理方式（包括 SSH、RDP 等协议）、登录地址、访问对象、账号等条件进行限制。

配置安全日志审计，其支持收集应用主机、数据库、应用、操作系统等日志数据源日志，收集的日志采用 ES 存储。支持通过标准协议 Syslog 和日志文件导入方式收集日志，能够按照预定义的策略对指定日志源的日志进行收集和分析，并提供日志数据的筛选、转换、整合、拆分、挖掘、事件分级管理、异常行为分析、关联事件分析，以及事件告警等相关功能。

配置漏洞扫描，其提供不少于 4 个 100/1000M 扫描电口，单扫描任务并发 100 个非固定 IP 授权，可同时创建多个扫描任务），总 IP 数量不限。支持检查各类操作系统、应用系统（数据库系统、Web 应用系统等）、网络主机、网络设备、常用软件等存在的安全威胁。支持识别缓冲区溢出、拒绝服务、弱/空口令、SQL 注入、XSS 攻击等漏洞。可以执行周期性、大批量的扫描任务，扫描过程不对扫描对象产生影响。

5.6.5 浏阳经开区云平台安全体系设计

本项目依托浏阳经开区云平台提供的安全体系，包括通用安全（安全物联环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心）、云计算安全、移动互联网安全、物联网安全等。通过部署安全一体机、安全审计系统、终端安全管理和 web 安全防护系统，同时依托云平台部署应用安全网关、虚拟化防火墙、虚拟化 Web 应用防火墙、虚拟化数据库审计、虚拟化日志审计、虚拟机防病毒、虚拟化堡垒机、终端检测与响应、密码机、漏洞扫描以及物联网安全网关等安全技术手段，结合安全管理手段，实现本项目云平台安全体系。

5.6.5.1 通用安全

通用安全主要从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五方面去考虑。

5.6.5.1.1 安全物理环境

本项目通过浏阳经开区云平台提供的基础设施资源，提供包括物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护 10 方面的安全要求。如下表：

图 5.8- 6 物理安全要求表

序号	控制点	要求	具体措施
1	物理位置的选择	机房和办公场地选择在具有防震、防风和防雨等能力的建筑内。	云平台的机房建设应严格按照国家对信息系统机房的建设标准
2	物理访问控制	机房出入口安排专人值守，控制、鉴别和记录进入的人员；需进入机房的来访人员经过申请和审批流程，并限制和监控其活动范围。	
3	防盗窃和防破坏	将通信线缆铺设在隐蔽处，可铺设在地下或管道中；对介质分类标识，存储在介质库或档案室中；主机房安装必要的防盗报警设施。	
4	防雷击	机房建筑设置避雷装置，设置交流电源地线。	
5	防火	机房应设置灭火设备和火灾自动报警系统。	
6	防水和防潮	水管安装，不得穿过机房屋顶和活动地板下；采取措施防止机房内水蒸气结露和地下积水的转移与渗透。	
7	防静电	关键设备采用必要的接地防静电措施。	
8	温湿度控制	机房设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。	
9	电力供应	提供短期的备用电力供应（如 UPS），至少满足关键设备在断电情况下的正常运行要求。	
10	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。	

5.6.5.1.2　安全通信网络

云平台的网络资源，需满足包括网络架构、通信传输和可信验证 3 方面的信息安全要求。如下表：

图 5.8- 7 安全通信网络要求表

安全要求点	安全要求项	对应技术措施
网络架构	1.应保证网络设备的业务处理能力满足业务高峰期需要；	主要网络设备和安全设备的性能满足要求。设备选型时网络吞吐量达到千兆、万兆要求。
	2.应保证网络各个部分的带宽满足业务高峰期需要；	防火墙、核心交换机、网管系统具备带宽管理功能。可基于内网、外网、用户、应用、时间段等参数设置带宽策略
	3.应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	防火墙区域隔离，安全域划分功能、网络设备交换机 VLAN 划分功能
	4.应避免将重要网络区域部署在网络边界处且没有边界防护措施；	内部应用区域等重要网络区域采用防火墙（网闸或网关）进行隔离和访问控制。防火墙具备安全域、Vlan、地址组功能可实现边界安全防护
	5.应提供通信线路、关键网络设备的硬件冗余，保证系统的可用性。	
云计算扩展要求网络架构	1.应保证云计算平台不承载高于其安全保护等级的业务应用系统	应用系统上云管理制度
	2.应实现不同云服务客户虚拟网络之间的隔离	虚拟化交换机进行网络隔离
	3.应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全	虚拟化交换机、虚拟化防火墙的边界隔离功能

安全要求点	安全要求项	对应技术措施
	机制的能力	
	4.应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略	通过云平台建设的云安全管理平台的安全策略管理功能
	5.应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。	通过云平台建设的云安全管理平台的安全服务申请
通信传输	1.应采用校验码技术或密码技术保证通信过程中数据的完整性；	通过云平台建设的 VPN 等通信加密技术手段
	2.应采用密码技术保证通信过程中敏感信息字段或整个报文的保密性。	通过云平台建设的 VPN 等通信加密技术手段

5.6.5.1.3　安全区域边界

通过云平台提供的基础设施资源，提供包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证 6 方面的信息安全要求。具体包括：

图 5.8- 8 安全区域边界要求表

安全要求点	安全要求项	对应技术措施
边界防护	1.应保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信。	边界设备（防火墙、交换机、网闸、路由器等）的访问控制策略功能（外部边界和内部边界）。
	2.应能够对非授权设备私自联到内部网络的行为进行限制或检查；	关闭网络设备闲置端口，部署网络准入控制设备，通过白名单策略功能对私自连到内部网络的行为进行限制
	3.应能够对内部用户非授权联到外部网络的行为进行限制或检查；	部署终端安全管理系统的违规外联检查功能，通过探测外网地址可实现非法外联的限制

安全要求点	安全要求项	对应技术措施
访问控制	1.应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	防火墙、网闸、交换机、路由器等的访问控制策略功能
	2.应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	防火墙、网闸、交换机、路由器等的访问控制策略
	3.应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；	防火墙、网闸、交换机、路由器等的访问控制策略功能
	4.应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制精度为端口级；	防火墙、网闸、交换机、路由器等的访问控制策略功能
	5.应在关键网络节点处对进出网络的信息内容进行过滤，实现对内容的访问控制。	网络审计系统对流量的审计分析功能
云计算扩展要求	1.应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；	虚拟化防火墙的访问控制策略
访问控制	2.应在不同等级的网络区域边界部署访问控制机制，设置访问控制规则。	虚拟化防火墙的访问控制策略
入侵防范	1.应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；	IPS、抗 DDOS 攻击系统、APT 检测设备的检测攻击行为功能
	2.应在关键网络节点处检测和限制从内部发起的网络攻击行为；	IPS、APT 检测设备的检测攻击行为功能
	3.应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；	APT 检测设备的未知恶意代码或漏洞攻击检测功能

安全要求点	安全要求项	对应技术措施
	4.当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提前报警。	IPS、APT 检测设备、抗 DDOS 攻击系统的攻击定位和溯源功能
云计算扩展要求入侵防范	1.应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；	安全资源池的虚拟化防火墙、虚拟化 IPS 组件
	2.应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；	安全资源池的虚拟化防火墙、虚拟化 IPS 组件
	3.应能检测到虚拟机与宿主机、虚拟机与虚拟机的异常流量；	安全资源池的虚拟化防病毒组件
	4.应能检测到网络攻击行为、异常流量情况时进行告警。	安全资源池的虚拟化防病毒组件
恶意代码和垃圾邮件防范	1.应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；	下一代防火墙的恶意代码检测功能
	2.应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。	下一代防火墙的应用层访问控制功能
安全审计	1.应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	网络审计系统、态势感知平台的日志、行为审计功能
	2.审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	日志审计系统、数据库审计系统、态势感知平台的审计功能
	3.应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	日志审计系统、态势感知平台支持将日志记录导出，可实现定期备份

安全要求点	安全要求项	对应技术措施
	4.应确保审计记录的留存时间符合法律法规要求；	日志留存时间不少于 6 个月，配备足够容量硬盘存储空间
	5.应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。	日志审计系统、网络审计系统的关联分析功能
云计算扩展要求安全审计	1.应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；	安全资源池的虚拟化日志审计组件
	2.应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。	安全资源池的虚拟化日志审计组件

5.6.5.1.4　安全计算环境

安全计算环境本部分主要是针对应用系统本身主机安全、应用安全和数据安全进行防护。需提供包括身份鉴别、访问控制、安全审计、入侵防护、恶意代码防护、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等方面的信息安全要求。具体包括：

图 5.8- 9 安全计算环境要求表

安全要求点	安全要求项	对应技术措施
身份鉴别	1.应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	身份认证系统、堡垒机的访问认证功能
	2.应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	身份认证系统、堡垒机的访问控制功能
	3.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；	身份认证系统、堡垒机加密措施
	4.应采用两种或两种以上组合的鉴别技术对用户进	身份认证系统、堡垒机的身份

安全要求点	安全要求项	对应技术措施
	行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。	认证功能
云计算扩展要求身份鉴别	1.当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制；	身份认证系统的CA电子认证
访问控制	1.应对登录的用户分配账号和权限；	堡垒机策略、网络设备、安全设备策略、应用访问控制功能及策略
	2.应重命名或删除默认账户，修改默认账户的默认口令；	配置检查工具
	3.应及时删除或停用多余的、过期的账户，避免共享账户的存在；	配置检查工具
	4.应授予管理用户所需的最小权限，实现管理用户的权限分离；	堡垒机策略、网络设备、安全设备策略、应用系统管理用户权限及策略（三员分离）
	5.应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；	堡垒机策略、网络设备、安全设备策略、应用系统管理用户权限及策略（三员分离）
	6.访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；	应用系统访问控制功能
	7.应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	应用系统访问控制功能
云计算扩展要求访问控制	1.应保证当虚拟机迁移时，访问控制策略随其迁移；	虚拟化交换机、虚拟化防火墙的策略迁移
	2.应允许云服务客户设置不同虚拟机之间的访问控制策略	虚拟化交换机、虚拟化防火墙的策略控制

安全要求点	安全要求项	对应技术措施
安全审计	1.应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；	日志审计、数据库审计系统日志审计功能
	2.审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；	日志审计、数据库审计系统日志审计功能
	3.应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；	日志审计、数据库审计系统记录保护功能
	4.应对审计进程进行保护，防止未经授权的中断。	日志审计、数据库审计系统记录保护功能
入侵防范	1.系统应遵循最小安装的原则，仅安装需要的组件和应用程序；	终端安全管理系统配置检查工具
	2.应关闭不需要的系统服务、默认共享和高危端口；	终端安全管理系统配置检查工具
	3.应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	应用系统输入有效性验证功能
	4.应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；	应用系统输入有效性验证功能、WAF 的代码检测
	5.应能发现可能存在的漏洞，并在经过充分测试评估后，及时修补漏洞；	漏洞扫描设备的脆弱性评估功能
	6.应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提前报警。	WAF、入侵防御设备的入侵检测功能
云计算扩展要求入侵防范	1.应能检测虚拟机之间的资源隔离失效，并进行告警；	云安全管理平台的资源监控功能
	2.应能检测非授权新建虚拟机或者重启虚拟机，并进行告警；	云安全管理平台的资源监控功能
	3.应能检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警；	安全资源池的虚拟化防病毒组件

安全要求点	安全要求项	对应技术措施
恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。	终端安全管理系统的主机防病毒功能
云计算扩展要求镜像和快照保护	1.应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；	终端安全管理系统的主机加固功能
	2.应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；	数据备份
	3.应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；	数据备份
数据完整性	1.应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；	应用系统安全功能开发
	2.应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。	应用系统安全功能开发
数据保密性	1.应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；	应用系统安全功能开发
	2.应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。	应用系统安全功能开发
云计算扩展要求数据完整性和保密	1.应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；	云平台数据管理制度
	2.应确保只有在云服务客户授权下，云服务商或第	云平台数据管理制度

安全要求点	安全要求项	对应技术措施
性	三方才具有云服务客户数据的管理权限；	
	3.应使用校验码或者密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；	数据备份系统、备份策略
数据备份恢复	1.应提供重要数据的本地数据备份与恢复功能；	数据备份系统、备份策略
	2.应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；	数据备份系统、备份策略
	3.应提供重要数据处理系统的热冗余，保证系统的高可用性。	应用系统双冗余
云计算扩展要求数据备份恢复	1.云服务客户应在本地保存其业务数据的备份；	数据备份系统、备份策略
	2.应提供查询云服务客户数据及备份存储位置的能力；	数据备份系统、备份策略
	3.云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；	数据备份系统、备份策略
	4.应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。	数据备份系统、备份策略
剩余信息保护（S）	1.应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；	应用系统安全功能开发、主机安全配置
	2.应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。	应用系统安全功能开发、主机安全配置
云计算扩展要求剩余信息保护	1.应保证虚拟机所使用的内存和存储空间回收时得到安全清除；	云管理平台策略功能
	2.云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除；	云管理平台策略功能

安全要求点	安全要求项	对应技术措施
个人信息保护（S）	1.应仅采集和保存业务必需的用户个人信息；	业务应用需求
	2.应禁止未授权访问和非法使用用户个人信息。	应用系统访问控制功能

5.6.5.1.5　安全管理中心

本项目通过云平台建设的安全管理中心，提供包括系统管理、审计管理安全管理和集中管控等方面的安全要求。具体如下：

图 5.8- 10 安全要求表

安全要求点	安全要求项	对应技术措施
系统管理	1.应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；	堡垒机、态势感知系统的身份认证策略
	2.应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	堡垒机、态势感知系统、网管系统的统一访问授权
审计管理	1.应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	堡垒机的操作审计功能
	2.应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	堡垒机的审计报表功能
安全管理	1.应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计	堡垒机的身份认证
	2.应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。	堡垒机的访问控制和授权

安全要求点	安全要求项	对应技术措施
集中管控	1.应划分出特定的管理区域，对分布式网络中的安全设备或安全组件进行管控；	区域划分有单独的安全管理区，云安全管理平台的安全组件管理
	2.应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；	建立独立管理网络
	3.应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；	网管系统、态势感知系统的资产管理监测
	4.应对分散在各个设备上的审计数据进行收集汇总和集中分析；	态势感知系统、日志审计系统的统一日志审计
	5.应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；	态势感知系统的集中安全管控
	6.应能对网络中发生的各类安全事件进行识别、报警和分析；	态势感知系统的威胁管理和场景分析
云计算扩展集中管控	1.应能对物理资源和虚拟资源按照策略做统一管理调度与分配；	云管理平台的管理调度
	2.应保证云计算平台管理流量与云服务客户业务流量分离	网络设备策略，建立独立管理网络
	3.应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；	云安全管理平台的三权分立、审计管理
	4.应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。	云安全管理平台的资源监控

5.6.5.2 云计算安全设计

《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）的7.2章节“云计算安全扩展要求”为云计算的安全要求设计提供了具体的指导和规

范。

1、虚拟化安全：

云计算平台应确保虚拟机之间的有效隔离，防止虚拟机之间的非法访问和信息泄露。

应对虚拟化环境进行安全加固，包括虚拟化管理层和虚拟机操作系统的安全更新和漏洞修复。

2、数据安全与保护：

在云计算环境中，应实施严格的数据访问控制和加密措施，确保数据的机密性、完整性和可用性。

对于敏感数据，应采取脱敏、匿名化等处理手段，降低数据泄露的风险。

3、安全审计与日志记录：

云计算平台应建立完善的安全审计机制，对虚拟机的创建、运行、删除等操作进行记录，便于事后追溯和分析。

同时，应定期对审计日志进行查看和分析，及时发现潜在的安全风险。

4、安全管理与运维：

云计算平台应实施严格的安全管理策略，包括用户权限管理、安全事件响应等。

运维人员应经过专业培训，具备相应的安全知识和技能，确保云计算平台的稳定运行。

5、供应链安全：

对于云计算平台的供应链，包括硬件设备、软件系统等，应进行严格的安全审查和风险评估。

确保供应链的可靠性和安全性，防止因供应链问题导致的安全风险。

综上所述，GB/T 22239-2019 的 7.2 章节为云计算的安全要求设计提供了全面的指导。在实际应用中，应根据云计算平台的具体情况和业务需求，结合这些要求制定详细的安全策略和措施，确保云计算环境的安全性和稳定性。

5.6.5.3 物联网安全设计

参考 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》7.4 章

节“物联网安全扩展要求”，从以下几个方面进行安全设计：

一、设备安全

设备认证与授权：所有物联网设备在接入网络前，必须进行严格的身份认证和授权，确保设备的合法性和安全性。

设备固件安全：对设备固件进行安全加固，及时更新固件版本，防止因固件漏洞导致的安全风险。

设备访问控制：实施严格的设备访问控制策略，限制对设备的非法访问和操作，防止设备被恶意控制或篡改。

二、通信安全

加密通信：采用安全的通信协议和加密算法，对物联网设备间的通信数据进行加密传输，确保数据的机密性和完整性。

安全接入：对物联网设备的接入过程进行安全控制，防止非法设备的接入和恶意攻击。

通信协议安全：对使用的通信协议进行安全评估和优化，防止协议漏洞被利用。

三、数据安全

数据保护：对物联网设备产生的数据进行保护，包括数据的存储、传输和处理过程，防止数据泄露和滥用。

数据脱敏与匿名化：对敏感数据进行脱敏和匿名化处理，降低数据泄露的风险。

数据审计与追溯：对数据的使用和流转过程进行审计和追溯，确保数据的合法性和合规性。

四、安全管理与运维

安全管理策略：制定物联网安全管理策略，明确安全目标、责任和措施，确保安全管理工作的有效实施。

安全培训与教育：对物联网设备的使用和管理人员进行安全培训和教育，增强他们的安全意识和技能。

安全监测与应急响应：建立物联网安全监测和应急响应机制，及时发现和

处理安全事件，降低安全风险。

综上所述，物联网安全要求设计需要综合考虑设备、通信、数据和安全管理与运维等多个方面。通过参考 GB/T22239-2019 的 7.4 章节“物联网安全扩展要求”，可以制定更为全面和有效的物联网安全策略和措施，确保物联网系统的安全性和稳定性。

5.6.6 数据安全设计

业务数据主要为不涉密的消防相关信息，依托云平台已有数据安全措施以及系统本身建设的数据安全措施进行安全管理应用。

5.6.6.1 数据分类分级

数据分级分类是根据政务资源元数据的属性或特征，将全市数据资源按照一定的原则和方法进行区分和归类，以便更好地管理和查询数据资源。

依据《网络数据安全标准实践指南—网络数据分类分级指引》（全国信息安全标准化技术委员会秘书处 2021 年 12 月 V1.0-202112）数据分级要求，本项目数据分级见下表：

表 5.6- 1 本系统数据分级表

序号	类别	对象	描述	安全需求
1	核心数据	消防信息	报警、消防点位等信息。	重要
2	重要数据	账号信息表	GB/T35273-2020《信息安全技术个人信息安全规范》所定义的个人敏感信息，包括内部用户身份证号、用户实名、手机号码。	重要
3		系统日志数据	系统日志包括系统日志、应用程序日志和安全日志。	完整性

5.6.6.2 数据分类方案

数据分类分级需由相关部门配合完成，过程中需要与各业务部门深入沟通，在理解业务流程和特点并考察实际业务实现的基础上评估数据的类别和级别，不应只按照数据库内容或设计文档等材料执行分类分级工作。分类分级的结果应与相关部门充分沟通校正，以求满足本项目的实际需求。服务过程必须由专

业的安全服务人员按照规范的服务流程执行，服务过程中各环节的输入输出应有记录。

5.6.6.3 数据全流程防护

5.6.6.3.1 数据访问安全准入防护

身份验证与授权：建立严格的身份验证机制，确保只有经过认证的人员才能访问智慧消防系统。同时，根据人员的角色和职责，设定不同的访问权限，确保敏感数据只能被授权人员访问。

多重认证方式：使用多种认证方式，提高身份验证的准确性和安全性。

访问控制策略：制定详细的访问控制策略，包括访问时间、访问地点、访问频率等，限制对敏感数据的访问。

安全培训与教育：定期对智慧消防系统的用户进行安全培训和教育，提高他们对数据安全和隐私保护的意识，减少因人为因素导致的数据泄露风险。

5.6.6.3.2 数据访问日志审计

日志收集与存储：确保智慧消防系统的所有操作日志都能被完整、准确地收集，并存储在安全可靠的存储介质中。

日志分析与监控：利用日志分析工具对收集到的日志进行实时分析和监控，发现异常行为和安全事件。同时，设定告警机制，当发现潜在风险时及时发出告警通知。

定期审计与报告：定期对智慧消防系统的日志进行审计，检查敏感数据的访问、修改、删除等操作是否符合规定。同时，生成审计报告，向管理层汇报系统的安全状况。

保留与销毁：根据相关法律法规和公司内部政策，对日志进行保留和销毁。确保在需要时能够提供有效的证据，同时避免数据过度保留带来的安全风险。

5.6.6.4 数据采集安全

本项目建设系统在接收业务数据时，需要对数据来源、数据完整性及可追溯性进行验证数据采集安全是数据安全生命周期的第一个过程，是对数据来源安全的管理，所有的后续工作都是以此为基础。可以通过在数据采集阶段，通过用户认证、设备认证等方式，保障数据本身的完整性和真实性，确保数据来

源的安全和可信，防止伪冒数据源的数据层安全攻击和破坏。

数据采集阶段的安全认证，主要包括采集系统到数据源系统（数据库－数据库）的接口认证、采集设备接入认证以及用户身份认证，通过身份认证和账号确权方式确保对端双向数据连接的安全。

5.6.6.5 数据传输安全

在数据传输阶段，需要保证数据传输的安全性，做好安全防护。数据传输安全主要是防止明文数据传输时丢失、泄露、篡改，所带来的安全隐患。其常见防护措施有专线传输、加密传输等。专线传输指专网传输，通过特定通道传输数据。加密传输是指使用一些加密算法保障传输的安全，常见协议为 HTTPS，常见算法有 RSA、国密算法等。

在本项目中主要通过 httpsSSL 协议+国密算法技术，实现数据传输加密来保障的业务系统数据的机密性和完整性。

在应用层面使用基于国密技术的数据传输加密方法，包括如下步骤：

（1）获取来自内网口的数据；

（2）通过数据报文获取 ip 的五元组；

（3）根据五元组查询所属会话，若会话不存在、则创建新的会话，若会话存在、执行步骤（4）；

（4）检查会话密钥合法性，若会话密钥不合法、内网口与外网口进行密钥协商形成会话密钥，若会话密钥合法、执行步骤（5）；

（5）根据会话密钥分组加密的长度对数据报文的长度进行分组检查；

（6）采用会话密钥对数据报文进行分组加密，生成加密载荷；

（7）将 ip 报文和加密载荷发送至外网口。

5.6.6.6 数据存储安全

针对敏感数据在数据库中存储的安全风险，通过采用将重要的数据表进行加密保存和授权访问，尤其是涉及敏感信息的数据表，加密后的数据在存储层以密文形态存在，只有授权的用户才可查看密文信息，而非授权用户看不到，即使整库被拖，拿到这些数据文件，也“看不懂”。

本项目建设系统采集的数据（流式数据、数据库、文件等类型的数据）在数据库存储后，需要防范敏感数据和内部数据泄露、数据丢失等问题。为解决数据存储阶段的风险问题，应基于数据进行数据加密存储。

本项目复用云平台密码资源池能力，结合数据资产梳理服务形成的《数据分类分级表》实现对敏感数据的加密控制，实现对数据资产内容安全的保护控制，服务器密码机能按业务要求选择不同等级的加密算法，通过对称加密和非对称加密，选择适合的国密算法，如 SM2、SM4 等。服务器密码机为平台提供数据加密工具为指定数据加密，以确保无论数据物理上存储在哪里都受到保护。

5.6.6.7 数据处理安全

本项目复用智慧消防平台运行时依托的云平台数据处理安全体系。

（1）身份鉴别

1、登录人员身份鉴别并记录相关登录信息及操作信息。

2、用户账号及密码信息存储都采用加密保护，并以密文方式存在。

（2）访问控制

访问权限设计采用基于角色的访问控制，它的基本思想是将权限与角色联系起来，在系统中根据应用的需要为不同的工作岗位创建相应的角色，同时根据用户职务和责任指派合适的角色，用户通过所指派的角色获得相应的权限，实现功能或资源的访问。它支持最小特权、责任分离以及数据抽象三个基本的安全原则。这里的角色就是业务系统中的岗位、职位或者分工。它和用户组的最主要的区别在于，用户组是作为用户的一个集合来对待，并不涉及其他的授权许可；而角色则既是一个用户的集合，又是一个授权许可的集合。角色是指具有一定技能，可以执行某些工作的人员（或资源）集合。通过给成员赋予不同的角色，对成员的多职能进行表达，提供约束成员不同权限范围变化的依据。

1、用户注册

应有正式的用户注册和注销流程来授权对数据中心的信息和服务的访问。

2、用户访问权的审核

确保对数据和信息服务访问的有效控制，管理人员应该定期地执行对用户访问权的检查。

数据操作

1、事务管理

通过事务管理机制，从而保证数据操作的完整性。

2、操作日志

对数据操作、导入导出进行跟踪检测，形成日志文件，并给予相应的提醒功能。

5.6.6.8 数据共享交换安全

随着云计算、大数据等新兴技术应用，数据已经不可能成为一个孤岛，智慧消防平台的数据需要共享给应用系统开发、大数据分析、其他单位信息资源共享等，在数据的共享过程中必须对相应数据进行脱敏、变形处理，才能提供给各种共享环境下的使用，严格防止敏感数据泄露。

数据资源在共享过程中，需先审批授权后共享使用，针对个人隐私信息等高敏感数据（姓名、地址、身份证号码等）进行匿名化处理，防止数据泄漏。针对数据共享的接口进行发现、监控和审计，防止数据泄露。所有数据访问操作进行身份认证，结合本项目数据分组分类方案中的《数据分类分级表》，建设共享库，共享库只存储《数据分类分级表》中可以对外公开共享的数据，防止核心数据、敏感数据和一般不适合公开数据的泄露，保证数据的有效性和可用性，使数据能够安全地应用于测试、开发、分析，和第三方使用环境中。

5.6.6.9 数据销毁安全

数据销毁安全指采取各种技术手段来完全破坏存储介质中数据的完整性，以防非授权用户利用残留数据恶意恢复，达到保护数据的目的。在数据生命周期结束后，数据未被彻底删除，或存有敏感数据的介质未被销毁，一旦数据被恢复就会引发数据泄漏的风险；数据销毁方法不当，导致被逆还原的风险。

本项目在数据销毁安全设计上沿用行业标准，需要结合数据分组分类方案中的《数据分类分级表》明确各类数据销毁的方法和步骤，实现数据销毁的安全保护。销毁防护的技术有很多种，有个共性特点是几乎都有不可逆转的销毁技术和程序，并且有严密的监督销毁监测机制。在实际工作中，采取何种数据销毁方式，需要结合本项目的情况进行综合考虑。

5.6.6.10 数据安全其他方面设计

5.6.6.10.1 业务数据安全

本项目数据安全保障参考最新信息相关安全要求，符合《网络安全等级保护基本要求》（GB/T22239-2019）等相关标准规范，全面提升信息安全防护能力，打造“攻击可防御、行为可检测、攻击可回溯、危险可预警、事件可处置”的安全防护体系。

智慧消防平台从多个维度、全方位保障数据安全，主要包括：数据访问控制、数据安全管理、数据追踪监管、数据备份管理等安全防护措施。

数据访问控制：对系统内案卷、文件、电子文件等内容进行访问控制，根据密级、类别等对条目/原文权限包括读写目录、只读目录、只读原文、读写原文、禁读原文，打印等。

数据安全管理：基于云平台已有物理安全、网络安全、主机安全设置，对数据进行安全管理和传输，确保数据管理、使用、运维过程中敏感信息的安全和完整性。

数据追踪监管：分系统管理员、数据库所有者、数据库对象所有者和其他用户四类，对数据库权限管理及日志进行追踪监管。

数据备份管理：对系统数据进行定期备份，采用全备份方式每天备份 1 次，保留所有备份数据，强化数据安全。

5.6.6.10.2 访问限制

访问权限设计采用基于角色的访问控制，它的基本思想是将权限与角色联系起来，在系统中根据应用的需要为不同的工作岗位创建相应的角色，同时根据用户职务和责任指派合适的角色，用户通过所指派的角色获得相应的权限，实现功能或资源的访问。它支持最小特权、责任分离以及数据抽象三个基本的

安全原则。这里的角色就是业务系统中的岗位、职位或者分工。它和用户组的最主要的区别在于，用户组是作为用户的一个集合来对待，并不涉及其他的授权许可；而角色则既是一个用户的集合，又是一个授权许可的集合。角色是指具有一定技能，可以执行某些工作的人员（或资源）集合。通过给成员赋予不同的角色，对成员的多职能进行表达，提供约束成员不同权限范围变化的依据。

1、用户注册

应有正式的用户注册和注销流程来授权对数据中心的信息和服务的访问。

2、用户访问权的审核

确保对数据和信息服务访问的有效控制，管理人员应该定期地执行对用户访问权的检查。

5.6.6.10.3　身份鉴别

1、登录人员身份鉴别并记录相关登录信息及操作信息。

2、用户账号及密码信息存储都采用加密保护，并以密文方式存在。

5.6.6.10.4　数据脱敏

数据的保密性是指数据在传输、使用过程中，确保重要的、私有的信息不会泄漏，客户端和客户端之间、客户端和服务器之间传输的数据不会被第三方所获取。系统的登录、认证采用 SSL 等安全传输协议在传输层对网络连接进行加密，保证敏感信息在传输过程中不被非法入侵者读取。本次项目基于长沙市密九云安全体系统一提供的脱敏软件进行数据保密处理。

主要对系统中的敏感数据进行脱敏存储，防止恶意获取政府相关数据进行破坏行为。如储存位置、储存数量等。

5.6.6.10.5　数据操作

1、事务管理

通过事务管理机制，从而保证数据操作的完整性。

2、操作日志

对数据操作、导入导出进行跟踪检测，形成日志文件，并给予相应的提醒功能。

5.6.7　容器安全设计

根据 T/ISEAA 004-2023《网络安全等级保护容器安全要求》这一标准要求。

容器安全设计包括：

容器镜像安全：确保容器镜像的来源可靠，防止恶意代码注入。对于每一个部署到生产环境的容器镜像，都应当经过严格的安全审查，包括漏洞扫描、恶意软件检测等。

容器隔离与访问控制：通过容器技术实现应用之间的隔离，降低潜在的安全风险。同时，实施严格的访问控制策略，确保只有经过授权的用户或系统才能访问和操作容器。

资源限制与监控：为容器分配必要的资源，并设置合理的资源限制，防止因资源耗尽导致的安全风险。同时，对容器的运行状态进行实时监控，及时发现并处理异常行为。

安全审计与日志记录：对容器的创建、运行、销毁等关键操作进行审计和日志记录，以便于事后追溯和分析。这有助于发现潜在的安全问题，并为安全事件的调查提供证据。

安全更新与维护：定期更新容器运行时环境、镜像库等组件，以修复已知的安全漏洞。同时，建立容器的维护流程，确保容器的安全和稳定运行。

总之，容器安全设计需要综合考虑多个方面，包括镜像安全、隔离与访问控制、资源限制与监控、安全审计与日志记录以及安全更新与维护等。依照T/ISEAA 004-2023《网络安全等级保护容器安全要求》这一标准，可以有效地提升容器的安全性，保护用户的数据和隐私安全。

5.6.8 数据备份方案设计

本项目建立数据备份系统和相关工作机制，灾备运维分析管理平台应具有一定兼容性，在特殊情况下各系统间可互为备份。

本地部署网络应满足《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）二级（含）以上要求。对于其他非关键性业务达到二级要求，实现数据级容灾保护。

系统应实现数据备份功能，所有静态数据表和录入的资料在运行机器外必须有一个数据库的备份和一个通用格式文件的备份；每日发生数据变更应在运行机器外至少保存有数据库的增量备份和对应的通用格式文件的备份。

5.6.8.1 本地备份方案

本地备份方案说明：

1）依托于云平台本地备份服务，针对运行在虚拟机或者物理机的各种操作系统、虚拟机、文件、应用和数据库进行统一本地备份管理保护。

2）本项目的备份系统将每周做一次全备份，每天做增量备份或介于全备和增备两者之间的差分备份，每 3 周进行一次循环，得出所需备份存储约为 4.5TB。

2）在新增加的需要备份的服务器上安装备份客户端软件，为每个客户端配置备份代理。

3）本地部署本地备份一体机，业务数据先将汇集与压缩。

4）通过备份系统管理员或者云租户创建备份任务、设置备份策略，定时或者手动执行数据备份。

5）备份任务通过审批，自行发起数据备份和恢复。

6）备份平台将按策略将本地产生的备份数据，实现本地与异地备份数据冗余。

本项目选用本地备份方案。

5.6.8.2 异地备份方案

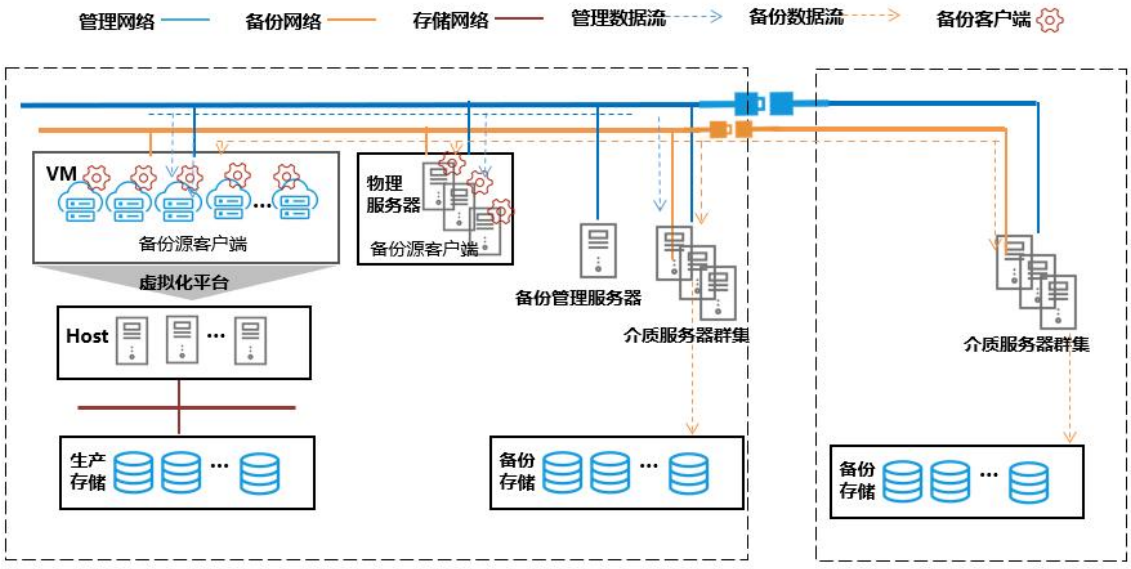


图 5.8- 15 异地备份图

- 适用场景：

该场景适用于非常重要的业务数据保护，在本地备份的同时，增加异地远程备份，防止本地数据中心发生灾难，数据可以从异地进行恢复。

- 技术特点：

在异地的数据中心部署备份一体机，通过专线或者备份网络进行数据的备份以及数据恢复。

- 部署要求：

备份管理端需要与备份一体机及客户端三层打通，使用 IPSEC 等加密隧道技术实现互通，实现备份数据的异地复制。

依托云平台主机房和同城机房实现提供本地备份、同城主备容灾能力满足业务的备份和容灾需求。针对运行在虚拟机或者物理机的各种操作系统、虚拟机、文件、应用和数据库进行统一异地备份管理保护，提供主流备份厂商的异地备份服务，所需备份存储约为 4.5TB。

5.6.8.3 备份云服务管理

数据备份是一种定时数据保护机制，在指定的时间发起备份作业，对需要保护的数据进行读取，然后写入备份介质中。当被保护的数据发生损坏或者丢失的时候，可以通过发起恢复作业，从备份介质中将数据恢复，进而保证数据的安全。

介质增加异地备份设备，数据恢复可以从本地备份介质取回数据集，也可以从异地取回备份集。

5.6.8.4 系统备份

备份系统主要解决本地数据备份问题，当数据出现故障时，可用备份系统的数据进行恢复，保证了智慧消防平台的数据安全。本地备份系统建设从层次上分为硬件备份、应用级备份和数据级备份，从时效上分为在线备份和离线备份。

硬件备份主要指关键网络设备实现冗余运行，关键服务器设备具有备机，能确保在发生硬件故障时，能快速将故障设备替换；应用级备份指对关键业务系统应用双机热备或集群技术进行备份，确保业务能不间断提供服务；数据级

备份指对数据进行可靠冗余备份，确保现有数据遭到破坏时能尽量减少损失且能快速恢复数据。

数据和文件是每天不断增长的，采用合适的备份方式与完善的备份策略对数据的备份具有重要的作用：

数据备份有多种方式包括全量备份、增量备份、差分备份、按需备份等。全备份：备份系统中所有的数据；

增量备份：只备份上次备份以后有变化的数据；

差分备份：只备份上次完全备份以后有变化的数据；

按需备份：根据临时需要有选择地进行数据备份。

全备份所需时间最长，但恢复时间最短，操作最方便，当系统中数据量不大时，采用全备份最可靠；但是随着数据量的不断增大，每天做全备份难以实现，采用周末做全备份，其他时间做增量备份或采用介于两者之间的差分备份。各种备份的数据量不同：全备份〉差分备份〉增量备份。在备份时要根据它们的特点灵活使用。

定期备份：为了防范数据丢失或损坏的风险，应定期对智慧消防系统的关键数据和配置进行备份。备份频率可以根据业务需求和系统变更的频率进行调整，一般建议至少每日备份一次，对于重要数据或关键业务时段，可以考虑实时备份或更高频次的备份。

备份存储：备份数据应存储在安全可靠的地方，可以是本地服务器、云存储或其他可靠的存储介质。同时，为了确保数据的冗余性和可恢复性，建议采用多份备份的策略，并将备份数据分散存储在不同的物理位置。

备份验证：定期对备份数据进行验证和测试，确保备份的完整性和可用性。这可以通过恢复部分备份数据到测试环境，并检查其是否能够正常运行和访问来实现。

5.6.8.5 **系统恢复**

灾难恢复预案的制定要遵循完整性、易用性、明确性、有效性和兼容性的原则。

完整性是指灾难恢复预案（以下称预案）应包含灾难恢复的整个过程，以

及灾难恢复所需的尽可能全面的数据和资料；

易用性是指预案应运用易于理解语言和图表，并适合在紧急情况下使用；

明确性是指预案应采用清晰的结构，对资源进行清楚的描述，工作内容和步骤应具体，每项工作应有明确的责任人；

有效性是指预案应尽可能满足灾难发生时进行恢复的实际需要，并保持与实际系统和人员组织的同步更新；

兼容性是指灾难恢复预案应与其他应急预案体系有机结合。

恢复计划：制定详细的系统恢复计划，包括恢复流程、所需资源、时间预估等。这有助于在发生数据丢失或系统故障时，能够迅速而有效地进行恢复操作。

快速恢复：在发生故障或数据丢失时，应根据恢复计划尽快启动恢复流程。这包括从备份中恢复数据、重新配置系统、验证系统功能等步骤。为了加速恢复过程，可以考虑使用自动化工具和脚本。

恢复测试：定期对恢复计划进行演练和测试，确保在真实故障发生时能够顺利执行恢复操作。同时，通过测试可以发现潜在的问题和不足，进而优化恢复计划和流程。

5.7 运维维护体系建设方案

5.7.1 运行管理原则

智慧消防平台的运行管理应遵循预防为主、及时响应、专业操作、数据管理等原则，具体为：

预防为主：定期检查智慧消防平台软硬件，确保其处于最佳状态，避免因设备故障导致的误报或漏报。

及时响应：对系统发出的任何警报都要迅速响应，及时排查原因，确保问题得到及时解决，并进行记录归档。

专业操作：如发现智慧消防相关软硬件出现故障，尽量由专业维护人员进行维护修复，避免非专业人员操作导致加重或损坏。

数据管理：定期备份系统数据，以防数据丢失，对于消防主机数据的更改

及增加，应及时整理并提供给厂家，以便保障平台数据的同步更新，避免因数据变动导致系统收不到报警。

环境适应性：应根据天气变化保持对设备的检查，避免因回南天等天气引起的湿度过大损伤设备。

5.7.2 运维管理范围

对项目的运维服务包括对构成项目的所有设施、数据、应用软件等的维护、维修、更换等，本项目中标单位将于终验后提供一年免费质保服务。

5.7.3 运维管理要求

提供服务期内详细的运行维护保障服务方案，包括服务内容、服务形式和服务保障措施。运维服务方案应满足以下具体要求：

（1）系统质量保证：质保服务期内，供应商应保障软硬件能满足项目中的性能指标要求。

（2）服务期内，设立 7×24 小时热线服务电话，受理系统故障申告、技术咨询。在收到系统故障申告后，必须按要求及时解决。

（3）应明确针对不同的故障等级的故障处理时间：

一级故障：平台系统完全瘫痪，24 小时内完全修复；

二级故障：硬件故障引起部分区域无法正常运行联网功能，24~48 小时内完全修复；

三级故障：影响系统或硬件效率的故障，但相关设备或相关系统仍然可以运行，24-72 小时内完全修复；

对在现场不能修复的设备需离场维修的，离场维修的时间应控制在 72 小时内，同时应立即首先换上性能良好的备用件，保证系统的正常运行。如项目设备已停产，应提供同等次或以上质量的设备用作替换。

供应商维护人员应根据按服务承诺要求，赶赴故障现场进行排障，完成排障后，将排障过程和结果填写在《故障登记及处理表》中，并交用户代表签字确认。如在排障过程中，需要维修或更换故障件进行排障，按相关服务内容进行处理。

5.7.4 运维任务分工要求

运行维护由建设单位及中标单位共同负责，日常主要依靠浏阳汇远实业有限公司相关管理人员，由相关部门担任信息化系统维护的相关专职人员负责；同时要求中标服务商配备相关技术人员对项目提供运维支撑。

智慧消防平台服务的运行维护，系统平台日常值班、报警故障事件的核实处理等需要建设单位安排专人负责，技术支持、应急事件的处理、数据库备份等由供应商负责。

5.8 软硬件参数及配置清单

5.8.1 设备参数测算

本项目硬件设备参数测算依据主要采用对市场主流的设备厂家进行询价，获取他们的参数配置及报价。

5.8.2 软硬件参数配置清单

序号	名称	参数描述	单位	数量
一、智慧消防平台				
软件系统基于 LINUX 开发运行环境，具备较强的安全性和高度可定制性。				
1.1	数据总览模块	支持一张图总览用户所关注的数据，能综合展示报警情况、监控场所情况、设备数量、设备运行情况等。	项	1
1.2	实时监控管理模块	（1）支持接入消防主机，实现设施报警、故障等信息的实时接收（2）报警支持弹窗，弹出报警点信息及电子地图，报警时进行声音、闪烁警示等。（3）报警除在系统显示外，还支持短信方式进行推送。（4）支持视频联动。	项	1
1.3	设施管理模块	（1）支持设施名称、类型、地点等多种方式查询设施信息。（2）设施报警故障记录查询，实时数据查看等。（3）设施报警、故障信息复核审计，报警、故障	项	1

		发生原因录入系统等。（4）支持隔离配置等。		
1.4	网格管理模块	支持以列表形式展示权限范围内的所有的楼宇信息，可以新建，修改楼宇基本信息。	项	1
1.5	智能巡查模块	支持任务查询、添加，后台可查看任务完成情况。	项	1
1.6	档案管理模块	支持人员证件、合同、消防法规文件等上传、查询等。	项	1
1.7	数据分析模块	支持图文展示实时报警、故障数据，分布图、趋势图查看等。	项	1
1.8	系统设置模块	用户管理，账号添加修改，管辖范围分配、日志查看等。	项	1
1.9	远程控制驱动模块	消防主机远程控制驱动软件模块，通过消防主机协议解析，在智慧消防平台实现消防主机远程手自动切换、消音、复位，消防水泵、风机等设施远程启动、停止等远程控制功能。（支持对园区现有泰和安 TX3016A、利达 LD128E（Ⅱ）、利达 LD188EL、北大青鸟 11SF-C4、北大青鸟 11SF、北大青鸟 11SF-S8、依爱 EI6000G、海湾 GST5000 等型号的远程控制）	套	9
	小计一			
2、联网硬件设备				
2.1	云服务器	CPU 8C，内存 16G，硬盘容量 1T，双向 100M 网口。	台	1
2.2	监控中心专线	分控室到监控中心数据专线 13 条，监控中心至经开区云中心数据专线 1 条，带宽≧20MB；	条	14
2.3	短信服务器	1.主板:M4OH； 2.处理器:I3； 3.内存:4G；	台	1

		4.硬盘:1T； 5.电源:300W； 6.机箱:RK-808MB-HJ； 7.专用短信模块。		
2.4	监控终端	1.处理器：i7； 2.内存：16G DDR4； 3.最大支持内存容量：128GB； 4.硬盘：1TB； 5.配键盘鼠标； 6.含显示屏。	台	2
2.5	显示大屏	1.尺寸：100 寸含支架； 2.分辨率：3840 x 2160； 3.运行内存：4GB； 4.存储内存：128GB； 5.整机功率：450W； 6.亮度：不低于 500 尼特； 7.刷新率：不低于 120hz。	台	1
2.6	硬盘录像机	1.2U 机架式 9 盘位嵌入式网络硬盘录像机，整机采用短机箱设计，搭载高性能 ATX 电源； 2.存储接口：9 个 SATA 接口，支持硬盘热插拔，可满配 12TB 硬盘； 3.视频接口：2×HDMI，2×VGA； 4.网络接口：2×RJ45 10/100/1000Mbps 自适应以太网口； 5.报警接口：16 路报警输入，9 路报警输出（其中第 9 路支持 CTRL 12V）； 6.反向供电：1 路 DC12V 1A； 7.串行接口：1 路 RS-232 接口，1 路全双工 RS-485 接	台	1

		口； 8.USB 接口：2×USB 2.0，2×USB 3.0; 9.扩展接口：1×eSATA; 10.输入带宽：384Mbps（开启 RAID 后为 200Mbps）； 11.输出带宽：256Mbps（开启 RAID 后为 200Mbps）； 12.接入能力：64 路 H.264、H.265 格式高清码流接入; 13.解码能力：最大支持 32×1080P; 14.显示能力：最大支持双 4K 异源输出; 15.RAID 模式：RAID0、RAID1、RAID5、RAID6、RAID10，支持全局热备盘; 16.目标识别应用：支持目标抓拍、比对报警；支持以图搜图、按姓名检索、按属性检索； 17.目标名单库：支持 16 个名单库，总库容 5 万张； 18.目标抓拍：4 路视频流（2MP）； 19.目标比对：16 路图片流。		
2.7	监控硬盘	1.容量：8T； 2.3.5 英寸； 3.运行环境：0℃至 65℃； 4.存储环境：-40℃至 70℃。	个	10
2.8	24 口交换机	1. 二层 web 网管交换机，交换容量 336Gbps，包转发率 78Mpps； 2. 24 个 10/100/1000Mbps 自适应电口，4 个 SFP 千兆光口； 3. 支持 VLAN、ACL、端口镜像、端口聚合等功能。	台	1
2.9	光纤跳线	FC-FC	根	26
2.10	机柜	42U	个	1
2.11	辅材	网线、电源线、管线等	项	1
二、消控室改造				

1、前端硬件				
1.1	智能网关	1.兼容网络协议 TCP/IP 协议，支持动态 IP 地址环境； 2.支持以太网、4G/5G 联网方式； 3.支持本地声光报警； 4.支持报警信号优先级别控制； 5.支持查岗和巡检功能； 6.支持第三方系统联动接口； 7.支持通信线路检测和故障管理； 8.备用电池，可使用 24 小时以上，主备电自动切换； 9.信号接口：具备 RJ45、RS232、RS485、CANBUS、继电器输出、采集通道等接口； 10.工业级机箱； 11.供电电压：220VAC 12.内含嵌入式 LINUX 系统。 13.通过国家强制性产品认证证书。	台	25
1.2	消防主机通信模块	消防主机原厂通信模块。	块	25
1.3	控制终端	1.工作电压：12VDC（DC12～48V）； 2.工作电流：<500mA (12VDC)； 3.支持 DI 输入； 4.支持 DO 输出（继电器可设置常开或常闭）； 5.支持 RS232 通讯； 6.支持 RS485 通讯； 7.支持 CAN 串口通讯； 8.具备 RJ45 网络接口； 9.具备 TF 卡接口； 10.具备 USB 接口；	台	25

		11.DC5V 输出（<500mA）； 12.工作环境：温度-20℃～60℃、湿度 5%～93%。		
1.4	摄像机	1.400 万定焦智能筒型网络摄像机； 2.支持越界侦测，区域入侵侦测，进入区域侦测和离开区域侦测，支持联动声音报警； 3.最高分辨率可达 2688 × 1520 @25 fps，在该分辨率下可输出实时图像； 4.支持背光补偿，强光抑制，3D 数字降噪，120 dB 宽动态，适应不同环境； 5.支持 ROI 感兴趣区域增强编码，支持 Smart265/264 编码，可根据场景情况自适应调整码率分配； 6.1 个内置麦克风，1 个内置扬声器，支持双向语音对讲； 7.智能补光，支持白光/红外双补光，红外最远可达 50 m，白光最远可达 30 m； 8.符合 IP66 防尘防水设计，可靠性高； 9.传感器类型：1/3″ Progressive Scan CMOS； 10.最低照度：彩色：0.005 Lux @（F1.2，AGC ON），0 Lux with IR； 11.宽动态：120 dB ； 12.焦距& 13.视场角：4 mm，水平视场角：78.3°，垂直视场角：42.9°，对角视场角：91.2° 6 mm，水平视场角：49.1°，垂直视场角：26.3°，对角视场角：57.2° 8 mm，水平视场角：37.5°，垂直视场角：20.7°，对角视场角：43.3° 12 mm，水平视场角：23.4°，垂直视场角：13.3°，	台	26

		对角视场角：26.8° 14.补光灯类型：智能补光，可切换白光灯、红外灯 补光距离：红外光最远可达 50 m，白光最远可达 30 m； 15.防补光过曝：支持； 16.红外波长范围：850 nm ； 17.最大图像尺寸：2688 × 1520； 17.视频压缩标准：主码流：H.265/H.264； 19.子码流：H.265/H.264/MJPEG； 20.第三码流：H.265/H.264 ； 21.网络：1 个 RJ45 10 M/100 M 自适应以太网口； 22.音频：1 个内置麦克风，1 个内置扬声器。		
1.5	支架	壁装	台	26
1.6	定制机柜	定制	个	13
1.7	10 口 POE 交换机	1. 二层 web 网管交换机，交换容量 192Gbps，包转发率 30Mpps； 2. 8 个 10/100/1000Mbps 自适应电口(支持 POE/POE+，整机 PoE 最大输出功率 125W，单端口最大输出功率 30W)，2 个 SFP 千兆光口； 3. 支持 VLAN、ACL、端口镜像、端口聚合等功能。	台	13
1.8	光模块	10km，单模双纤	对	13
1.9	辅材		项	1
2、集成服务				
2.1	智能网关		项	25
2.2	摄像机、机柜		项	39
2.3	组态联调费消防主机	主机探点数据生成	项	25

三、监控室移位改造				
1、创新创业园改造				
1.1	监视器移位	含解码器	台	15
1.2	光纤收发器	千兆	对	1
1.3	机柜	12U 机柜	台	1
1.4	交换机	1. 非网管型交换机，交换容量 16Gbps，包转发率 11.9Mpps； 2. 8 个 10/100/1000Mbps 自适应电口； 3. 桌面式铁壳小端口交换机； 4. 支持标准交换、端口隔离两种模式切换。	台	1
1.5	光纤跳线	sc-sc	根	4
1.6	辅材	网线、电源线、管线	项	1
2、新能源产业园改造				
2.1	监视器移位	含 NVR	台	2
2.2	POE 交换机	1. 非网管型交换机，交换容量 20Gbps，包转发率 14.9Mpps； 2. 10 个 10/100/1000Mbps 自适应电口(支持 POE/POE+，整机 PoE 最大输出功率 120W，单端口最大输出功率 30W)； 3. 支持 PoE 看门狗； 4. 桌面式铁壳小端口交换机； 5. 支持标准交换、端口隔离、长距离传输三种模式切换	个	1
2.3	交换机	1.非网管型交换机，交换容量 16Gbps，包转发率 11.9Mpps； 2.8 个 10/100/1000Mbps 自适应电口； 3.桌面式铁壳小端口交换机； 4.支持标准交换、端口隔离两种模式切换	台	1

2.4	机柜	12U 机柜	台	1
2.5	枪机	1.400 万定焦智能筒型网络摄像机； 2.支持越界侦测，区域入侵侦测，进入区域侦测和离开区域侦测，支持联动声音报警； 3.最高分辨率可达 2688 × 1520 @25 fps，在该分辨率下可输出实时图像； 4.支持背光补偿，强光抑制，3D 数字降噪，120 dB 宽动态，适应不同环境； 5.支持 ROI 感兴趣区域增强编码，支持 Smart265/264 编码，可根据场景情况自适应调整码率分配； 6.1 个内置麦克风，1 个内置扬声器，支持双向语音对讲； 7.智能补光，支持白光/红外双补光，红外最远可达 50 m，白光最远可达 30 m； 8.符合 IP66 防尘防水设计，可靠性高； 9.传感器类型：1/3″ Progressive Scan CMOS； 10.最低照度：彩色：0.005 Lux @（F1.2，AGC ON），0 Lux with IR； 11.宽动态：120 dB ； 12.焦距&视场角：4 mm，水平视场角：78.3°，垂直视场角：42.9°，对角视场角：91.2° 6 mm，水平视场角：49.1°，垂直视场角：26.3°，对角视场角：57.2° 8 mm，水平视场角：37.5°，垂直视场角：20.7°，对角视场角：43.3° 12 mm，水平视场角：23.4°，垂直视场角：13.3°，对角视场角：26.8° 13.补光灯类型：智能补光，可切换白光灯、红外灯；	台	1

		14.补光距离：红外光最远可达 50 m，白光最远可达 30 m； 15.防补光过曝：支持； 16.红外波长范围：850 nm ； 17.最大图像尺寸：2688 × 1520； 18.视频压缩标准：主码流：H.265/H.264； 19.子码流：H.265/H.264/MJPEG； 20.第三码流：H.265/H.264 ； 21.网络：1 个 RJ45 10 M/100 M 自适应以太网口； 22.音频：1 个内置麦克风，1 个内置扬声器。		
2.6	枪机支架	壁装	个	1
2.7	辅材	网线、电源线、管线	项	1

第六章　项目招标方案

为实现对本项目建设的规范化、标准化和制度化管理，提高项目建设的水平和质量，提高项目资金的使用效率，本项目将根据《中华人民共和国政府采购法》（以下简称《政府采购法》）和《中华人民共和国招标投标法》的规定，组织实施项目中货物的采购。

6.1　招标范围

按照政府采购的要求，对项目建设中的前期咨询、项目设计、监理和硬件、软件以及系统集成等适合以招标方式采购的产品和服务，原则上进行招标采购，本项目的招标范围主要内容包括：项目软硬件货物、初步设计及项目前期相关咨询、监理等。

6.2　招标方式

根据《中华人民共和国招标投标法》，招标分为公开招标和邀请招标。公开招标，是指招标人以招标公告的方式邀请不特定的法人或者其他组织投标。邀请招标，是指招标人以投标邀请书的方式邀请特定的法人或者其他组织投标。根据《中华人民共和国政府采购法》，政府采购采用以下方式包括公开招标、邀请招标、竞争性磋商、竞争性谈判、单一来源采购、询价以及国务院政府采购监督管理部门认定的其他采购方式。本项目实施建议采用竞争性磋商方式。

6.3 招标组织形式

招标组织形式包括自行招标和委托招标。其中，自行招标，是指招标人自身具有编制招标文件和组织评标能力，依法可以自行办理招标；而委托招标，是指招标人委托招标代理机构办理招标事宜。本项目招标组织形式采取委托招标。

6.4 招标原则

本项目应遵循《中华人民共和国招标投标法》第五条规定的招标投标活动基本原则，即“招标投标活动应当遵循公开、公平、公正和诚实信用原则。”

（一）公开原则

公开原则是指招投标的程序应透明，招标信息和招标规则应公开，有助于提高投标人参与投标的积极性，防止权钱交易等腐败现象的滋生。

（二）公平原则

公平原则是指参与投标者的法律地位平等，权利与义务相对应，所有投标人的机会平等，不得实行歧视。

（三）公正原则

公正原则是指投标人及评标委员会必须按统一标准进行评审，市场监管机构对各参与方都应依法监督，一视同仁。

（四）诚实信用原则

诚实信用原则是指招标、投标人都应诚实、守信、善意、实事求是，不得欺诈他人，损人利己。

（五）优先中小微企业采购原则

根据《政府采购促进中小企业发展管理办法》中相关规定，本项目符合优先中小微企业采购原则。

6.5 招标要求

招标方案中必须要求投标供应商对设计内容进行响应，招标文件中未表述完全的内容必须参照初步设计方案内容进行响应。

第七章　项目组织机构与人员培训

7.1　项目工作方案

近年来，随着物联网、大数据等技术的迅猛发展，为推动消防安全管理提供了新机遇，浏阳汇远实业有限公司积极探索消防物联网管理的新模式，将消防工作提升列为安保首要工作，多措并举，通过人员素质提升、专项活动开展、物联网建设等方面，不断提升园区的消防安全管理能力和火灾防控水平。

一、提升消防信息化管理手段

重视信息化管理：通过信息技术手段，对消防安全工作进行科学化、规范化和智能化的管理，提高消防安全管理的效率和质量，降低管理成本，及时发现和解决潜在的火灾隐患。

智慧消防平台建设：构建一套智慧消防平台，实现实时监控管理、设施管理、网格管理、智能巡查、档案管理、数据分析、系统设置、远程控制等功能。

二、固化工作机制

组织领导与协作机制：成立智慧消防平台项目工作领导小组，明确各部门的职责和任务，确保项目顺利推进。建立跨部门协作机制，加强信息共享和资源整合，形成工作合力。

人员培训与考核机制：制定培训计划，对服务人员进行智慧消防平台操作培训，提高他们的业务素质和服务水平。建立考核机制，对监控值守人员的工作绩效进行评价和奖惩，激励他们积极参与相关工作。

7.2　领导和管理机构

项目建设管理机构的设立应本着“统一领导、分工明确、职责清晰、协调配合”的原则，贯穿项目开始至进场乃至验收、售后运行等的全过程。项目管理机构各部成员管理与职责分工如下：

项目推进：牵头负责项目立项、采购招标、评审、批复、验收等相关流程推进、各子项项目组之间协调及项目相关文档管理。

项目咨询设计：经过规范的招标程序，项目领导小组委托具有相应资质和

实力的咨询设计单位，对项目提供项目建议书编制、技术方案编制、初步设计、初步设计编制等服务。

项目监理：经过规范的招标程序，项目领导小组委托第三方有大型信息系统工程监理资质的单位派出专家组成项目监理办事机构。具体承担项目建设的监理工作，代表甲方（或建设单位）确保项目建设的质量、进度以及投资的合理性。

运维组：项目建设完成后，安排专员在监控中心值班，专门负责智慧消防平台，同时定期测试系统各项功能，并保持跟供应商的积极沟通。在质保期内由中标单位负责技术支持与维保。

同时聘请外部技术专家，负责为本项目的设计与实施提供咨询和建议，协助审核各阶段的技术方案、实施方案及方案投资报价。

7.3 人员培训

7.3.1 培训方案

提供一套完整的培训服务体系，能在短时间内提高信息化水平提供有力的保障，中标单位应安排参与实施的工程师共同参与到培训计划中，为本项目制定详细的培训计划，确认同意后就可以按照制定的培训计划实施。

（1）培训计划在培训内容、时间、人数、地点以及人员安排等方面需符合用户的培训服务要求，培训内容包括但不限于：了解系统的基本组成原理、系统基本结构；了解系统和前端设备的基本功能、基本结构、参数；掌握系统及前端设备的基础操作、使用和简单维护保养方法；能够对系统及设备的一般故障进行有效处理。

（2）培训时间要求在试运行期间进行，培训对象包括值班人员及管理人员，培训时长不少于两天。采用两种培训方式，课堂培训和系统演示相结合的培训。

（3）提供每人一套详细完备、通俗易懂的使用手册；施工方派出专业的培训人员，拥有丰富的工程施工、设备安装调试实践经验，所有的培训课程采用中文授课。

第八章　项目实施进度

8.1　项目建设期

本项目建设周期为6个月，前期准备阶段1个月；施工阶段3个月；试运行与培训阶段1个月；项目验收阶段1个月。

8.2　实施进度计划

本项目的进度计划编制遵循科学性、客观性的原则，做到既考虑系统全局，又兼顾施工的特殊性。具体项目进度计划表（根据实际情况可能会有变动），实施计划如下：

本项目规划预计分四个阶段，建设周期约为6个月。

第一阶段：前期工作阶段，预计1个月。

本阶段主要包括项目立项、设计、招标、合同签订等工作。

第二阶段：施工阶段，预计3个月。

本阶段包括施工准备、设备及材料订购、设备安装。

第三阶段：试运行与培训，预计1个月。

本阶段包括试运行、培训及竣工验收交付使用。

第四阶段：验收阶段，预计1个月。

本阶段包括验收资料的准备、验收的安排以及软硬件设备的移交等。

当项目公示完成并签订合同完成后，根据总体施工计划的安排，按招标要求按时完成工程，并保证质量合格。完成整个项目全部工作任务（包括最终验收）的分项施工计划和时间表，由具有丰富施工经验的专人负责实施。为了合理安排进度在现场设备安装阶段，我们采取将同类设备合期进行安装，这样便于整体进度上的总协调。

说明：项目具体建设时间以完整招投标节点为准，向前或向后顺延。

第九章　项目资金安排和投资估算

9.1　投资估算总体说明

9.1.1　估算总体说明

智慧消防建设项目可行性研究报告投资估算的编制，是根据项目的建设规模编制的。在编制本投资估算时采用了2024年下半年的价格水平，部分设备单价参考当前市场平均价格。

本项目投资估算的主要费用包括软件及硬件费用、施工费等。

项目其他费用通常由可研报告编制费、招标代理服务费用等组成。

9.1.2　主要费用估算

本项目主要费用包括智慧消防平台费用、前端消控室改造费用、监控室移位改造费用等，详见9.2项目总投资概算表、11.1投资估算明细表。

9.1.3　其他费用

9.1.3.1　**初步设计（代可研）编制费**

本项目考虑实际情况，初步设计（代可研）编制费按合同计取，金额为8.15万元。

9.1.3.2　**预算编制费**

按照《长沙市财政评审中心政府投资建设信息化项目评审指南》（长财评综〔2023〕12 号）规定，预算编制费分段计费，并乘以专业调整系数。本项目预算编制费含在初步设计（代可研）编制费中，不再另行计取。

9.1.3.3　**监理服务费**

按照《长沙市财政评审中心政府投资建设信息化项目评审指南》（长财评综〔2023〕12 号）规定，监理费分段计费，并乘以专业调整系数。本项目包括软件工程和硬件采购，调整系数计算为：（103 * 1.2 + （83.88） * 0.5 + 6.36 * 1.0)/ （193.24） = 0.89

监理费为：193.24 * 2.6% * 0.89= 4.47 万元。

9.1.3.4 软件测评费

按照《长沙市财政评审中心政府投资建设信息化项目评审指南》（长财评综〔2023〕12 号）规定，软件测评费分段计费。

费用为：103 * 2.25% = 2.32 万元。

9.1.3.5 安全等级保护测评费

按照《长沙市财政评审中心政府投资建设信息化项目评审指南》（长财评综〔2023〕12 号）规定，等保二级每个系统 ≤ 4 万元/个，本项目按照一个系统进行计取，共计 4 万元。

9.1.3.6 招标代理费

按照《长沙市财政评审中心政府投资建设信息化项目评审指南》（长财评综〔2023〕12 号）规定，并结合市场化询价，本项目招标代理费按照 2 万元计取。

9.2 项目总投资概算

经概算，本期项目总投资概算为 2206858 元，信息系统建设费为 1932370 元，其他费用 169400 元，预备费为 105088 元，所需资金由浏阳汇远实业有限公司自筹解决，项目总投资概算如下表所示。

表 9.2-1 总投资概算表

序号	费用名称	计算公式	金额（元）	所占比例	取费依据
一	信息系统建设费		1932370		
1	智慧消防平台费用				
1.1	软件开发费		1030000		
1.2	联网设备采购费		126970		
1.3	集成费		10000		
2	前端消控室改造费用				
2.1	硬件采购费用		711875		
2.2	集成服务		41240		
3	监控室移位改造费用				
3.1	创新创业园改造费用		7230		

3.2	新能源产业园改造		5055		
二	工程建设其他费		169400		
1	初步设计（代可研）编制费		81500		按合同价计取
2	监理服务费		44700		长财评综〔2023〕12 号
3	软件测评费		23200		长财评综〔2023〕12 号
3	招标代理费		20000		
三	预备费	（一+二）*5%	105088		长财评综〔2023〕12 号
四	项目总费用	一+二+三	2206858		

9.3 资金来源和落实情况

本期项目所需资金由浏阳汇远实业有限公司单位解决。本项目保证合理使用项目资金，做到专款专用，抓计划的基础上做好调度工作，使资金发挥最大效益。

第十章　效益和风险分析

10.1　项目预期收益

10.1.1　社会效益

提升火灾预警能力：智慧消防平台能够全天候对园区消防主机进行监控，及时发现火灾隐患并提前预警，便于及时处置。

增强应急响应速度：智慧消防平台能够实现信息的快速传递和共享，一旦发生火灾，系统可同时发送短信通知附近值班人员。

增强公众安全意识：通过智慧消防的宣传和推广，能够增强公众的消防安全意识和自救互救能力，提高全社会对消防安全的重视程度，营造更加安全的生活环境。

10.1.2　经济效益

1．提升日常管理水平：引入先进的信息技术，智慧消防可以实现对消防设施的故障运行状态的实时监测，确保消防主机处于良好的工作状态，提升消防设施的完好率和维护效率。

消防数据支撑：日常主机报警、故障信息自动存档，便于用户分类查询，同时为用户的消防管理工作提供数据支撑。

推动消防产业升级：智慧消防的发展促进了相关技术的研发和应用，如物联网、大数据等，有助于推动消防产业向高科技、智能化方向转型升级，提高整个行业的竞争力。

节省人力成本支出：通过智慧消防建设实现对消防主机的实时监控，用户可释放部分消控室值班人员，充分降低人力成本支出。

10.2　风险分析及对策

10.2.1　风险识别和分析

10.2.1.1　**政策风险**

我国当前正处在社会主义现代化建设的发展过程中，全面深化改革的各项新

政策在不断地制定和调整中，由于政策的调整滞后于信息技术及市场的发展。因此，也就给项目带来了一定的政策性风险，需要用户与相关部门充分沟通。

10.2.1.2 组织风险

本项目涉及调研、设计、建设实施等每个项目建设过程中，需要各相关单位之间进行充分的沟通。如何在项目建设过程中协调所有单位，使得项目顺利完成，存在一定的组织风险。

在建设完成之后，除了日常的使用，还要对系统进行维护，对数据进行更新和维护，相关过程中也涉及各个单位，在平台使用和维护过程中也存在一定的组织风险。

10.2.1.3 管理风险

项目实施单位的项目管理能力是项目实施过程中系统质量的重要因素。如果实施方没有建立起统筹管理和控制、分任务的管理和控制，对于项目实施的质量都存在风险。

10.2.1.4 技术风险

信息化建设项目的技术风险，主要是 IT 行业技术高速发展所带来的风险。IT 行业技术日新月异，项目建设需充分考虑兼容性与可拓展性。

10.2.2 风险对策和管理

10.2.2.1 政策风险对策

主要涵盖已经明确政策的领域，依托大方向原则，部分政策细节未明确给项目带来的政策风险不大，在可控范围。

10.2.2.2 组织管理风险对策

设立项目建设管理机构，本着“统一领导、分工明确、职责清晰、协调配合”的原则，贯穿项目开始至进场乃至验收、售后运行等的全过程。

项目推进：牵头负责项目立项、采购招标、评审、批复、验收等相关流程推进、各子项项目组之间协调及项目相关文档管理。

项目咨询设计：经过规范的招标程序，项目领导小组委托具有相应资质和实力的咨询设计单位，对项目提供项目建议书编制、技术方案编制、初步设计、初步设计编制等服务。

项目监理：经过规范的招标程序，项目领导小组委托第三方有大型信息系统工程监理资质的单位派出专家组成项目监理办事机构。具体承担项目建设的监理工作，代表甲方（或建设单位）确保项目建设的质量、进度以及投资的合理性。

运维组：项目建设完成后，安排专员在监控中心值班，专门负责智慧消防平台，同时定期测试系统各项功能，并保持跟供应商的积极沟通。在质保期内由中标单位负责技术支持与维保。

同时聘请外部技术专家，负责为本项目的设计与实施提供咨询和建议，协助审核各阶段的技术方案、实施方案及方案投资报价。

10.2.2.3 技术风险对策

为了降低项目建设内容复杂性对项目实施造成的风险，应选择具有相关项目实施经验的承建单位和项目经理，减少项目实施风险。本着项目的实际要求，坚持技术的先进性和稳定性相结合，同时兼具可拓展性与兼容性，降低技术风险。

10.2.2.4 资金风险对策

资金及时到位是项目建设按期完成的重要条件之一，本项目的建设资金应由浏阳汇远实业有限公司单位统一划拨。对于承建单位，一方面要控制需求，另一方面要优化方案与或创新管理，尽量降低成本支出。如果确因客观原因造成超预算，应相互协商，从其他经费中协调，或追加预算。

第十一章　附录和附件、附表

11.1　投资估算明细表

序号	名称	参数描述	单位	数量	单价（元）	总价（元）	备注
一、智慧消防平台							
软件系统须基于 LINUX 开发运行环境，具备较强的安全性和高度可定制性。							
1、软件开发费							
1.1	数据总览模块	支持一张图总览用户所关注的数据，能综合展示报警情况、监控场所情况、设备数量、设备运行情况等。	项	1	50,000	50,000	
1.2	实时监控管理模块	（1）支持接入消防主机，实现设施报警、故障等信息的实时接收（2）报警支持弹窗，弹出报警点信息及电子地图，报警时进行声音、闪烁警示等。（3）报警除在系统显示外，还支持短信方式进行推送。（4）支持视频联动。	项	1	50,000	50,000	

1.3	设施管理模块	（1）支持设施名称、类型、地点等多种方式查询设施信息。（2）设施报警故障记录查询，实时数据查看等。（3）设施报警、故障信息复核审计，报警、故障发生原因录入系统等。（4）支持隔离配置等。	项	1	50,000	50,000	
1.4	网格管理模块	支持以列表形式展示权限范围内的所有的楼宇信息，可以新建，修改楼宇基本信息。	项	1	50,000	50,000	
1.5	智能巡查模块	支持任务查询、添加，后台可查看任务完成情况。	项	1	50,000	50,000	
1.6	档案管理模块	支持人员证件、合同、消防法规文件等上传、查询等。	项	1	50,000	50,000	
1.7	数据分析模块	支持图文展示实时报警、故障数据，分布图、趋势图查看等。	项	1	50,000	50,000	
1.8	系统设置模块	用户管理，账号添加修改，管辖范围分配、日志查看等。	项	1	50,000	50,000	

1.9	远程控制驱动模块	消防主机远程控制驱动软件模块，通过消防主机协议解析，在智慧消防平台实现消防主机远程手自动切换、消音、复位，消防水泵、风机等设施远程启动、停止等远程控制功能。（支持对园区现有泰和安 TX3016A、利达 LD128E（Ⅱ）、利达 LD188EL、北大青鸟 11SF-C4、北大青鸟 11SF、北大青鸟 11SF-S8、依爱 EI6000G、海湾 GST5000 等型号的远程控制）	套	9	70,000	630,000	按主机型号计，泰和安、利达、北大青鸟、依爱、海湾等品牌型号
	小计一					1,030,000	
2、联网硬件设备							
2.1	云服务器	CPU 8C，内存 16G，硬盘容量 1T，双向 100M 网口。	台	1	18，000	18，000	根据使用需求，按年租用金阳运中心云服务器、运硬盘。
2.2	监控中心专线	分控室至监控中心数据专线 13 条，监控中心至经开区云中心数据专线 1 条，带宽≧20MB	条	14	3,000	42,000	根据使用需求，按年运营商数据专线。
2.3	短信服务器	1.主板:M4OH；	台	1	6,000	6,000	报警短信推送，短信卡

		2.处理器:I3； 3.内存:4G； 4.硬盘:1T； 5.电源:300W； 6.机箱:RK-808MB-HJ； 7.专用短信模块。					需用户自行申请（不限运营商，普通短信卡即可）
2.4	监控终端	1.处理器：i7； 2.内存：16G DDR4； 3.最大支持内存容量：128GB； 4.硬盘：1TB； 5.配键盘鼠标； 6.含显示屏。	台	2	6,000	12,000	监控电脑
2.5	显示大屏	1.尺寸：100 寸含支架； 2.分辨率：3840 x 2160； 3.运行内存：4GB； 4.存储内存：128GB；	台	1	15,000	15,000	

		5.整机功率：450W； 6.亮度：不低于500尼特； 7.刷新率：不低于120hz。					
2.6	硬盘录像机	1.2U机架式9盘位嵌入式网络硬盘录像机，整机采用短机箱设计，搭载高性能ATX电源； 2.存储接口：9个SATA接口，支持硬盘热插拔，可满配12TB硬盘； 3.视频接口：2×HDMI，2×VGA； 4.网络接口：2×RJ45 10/100/1000Mbps自适应以太网口； 5.报警接口：16路报警输入，9路报警输出（其中第9路支持CTRL 12V）； 6.反向供电：1路DC12V 1A； 7.串行接口：1路RS-232接口，1路全双工RS-485接口； 8.USB接口：2×USB 2.0，2×USB 3.0;	台	1	6,500	6,500	

		9.扩展接口：1×eSATA; 10.输入带宽：384Mbps（开启 RAID 后为 200Mbps）; 11.输出带宽：256Mbps（开启 RAID 后为 200Mbps）; 12.接入能力：64 路 H.264、H.265 格式高清码流接入; 13.解码能力：最大支持 32×1080P; 14.显示能力：最大支持双 4K 异源输出; 15.RAID 模式：RAID0、RAID1、RAID5、RAID6、RAID10，支持全局热备盘; 16.目标识别应用：支持目标抓拍、比对报警；支持以图搜图、按姓名检索、按属性检索； 17.目标名单库：支持 16 个名单库，总库容 5 万张； 18.目标抓拍：4 路视频流（2MP）；					

		19.目标比对：16路图片流。					
2.7	监控硬盘	1.容量：8T； 2.3.5英寸； 3.运行环境：0℃至65℃； 4.存储环境：-40℃至70℃。	个	10	1,800	18,000	
2.8	24口交换机	二层web网管交换机，交换容量336Gbps，包转发率78Mpps； 24个10/100/1000Mbps自适应电口，4个SFP千兆光口； 支持VLAN、ACL、端口镜像、端口聚合等功能。	台	1	2,500	2,500	
2.9	光纤跳线	FC-FC	根	26	45	1,170	
2.10	机柜	42U	个	1	2,800	2,800	
2.11	辅材	网线、电源线、管线等	项	1	3,000	3,000	
	小计二					126970	
3、集成服务							

3.1	集成服务		项	1	10,000	10,000	
	小计三					10，000	
二、消控室改造							
1、前端硬件							
1.1	智能网关	1.兼容网络协议 TCP/IP 协议，支持动态 IP 地址环境 2.支持以太网、4G/5G 联网方式 3.支持本地声光报警 4.支持报警信号优先级别控制 5.支持查岗和巡检功能 6.支持第三方系统联动接口 7.支持通信线路检测和故障管理 8.备用电池，可使用 24 小时以上，主备电自动切换。 9.信号接口：具备 RJ45、RS232、RS485、CANBUS、继电器输出、采集通道等接口。	台	25	12,500	312,500	消防主机联网监控

		10.工业级机箱 11.供电电压：220VAC 12.内含嵌入式 LINUX 系统。 13.通过国家强制性产品认证。					
1.2	消防主机通信模块	消防主机原厂通信模块	块	25	5,000	125,000	
1.3	控制终端	1.工作电压：12VDC（DC12～48V）； 2.工作电流：<500mA (12VDC)； 3.支持 DI 输入； 4.支持 DO 输出（继电器可设置常开或常闭）； 5.支持 RS232 通讯； 6.支持 RS485 通讯； 7.支持 CAN 串口通讯； 8.具备 RJ45 网络接口； 9.具备 TF 卡接口； 10.具备 USB 接口； 11.DC5V 输出（<500mA）；	台	25	8,500	212,500	

		12.工作环境：温度-20℃～60℃、湿度5%～93%。					
1.4	摄像机	1.400万定焦智能筒型网络摄像机； 2.支持越界侦测，区域入侵侦测，进入区域侦测和离开区域侦测，支持联动声音报警； 3.最高分辨率可达2688 × 1520 @25 fps，在该分辨率下可输出实时图像； 4.支持背光补偿，强光抑制，3D数字降噪，120 dB宽动态，适应不同环境； 5.支持ROI感兴趣区域增强编码，支持Smart265/264编码，可根据场景情况自适应调整码率分配； 6.1个内置麦克风，1个内置扬声器，支持双向语音对讲； 7.智能补光，支持白光/红外双补光，红外最远可达50 m，白光最远可达30 m；	台	26	980	25,480	每个主消控室安装

		8.符合 IP66 防尘防水设计，可靠性高； 9.传感器类型：1/3″ Progressive Scan CMOS； 10.最低照度：彩色：0.005 Lux @（F1.2，AGC ON），0 Lux with IR； 11.宽动态：120 dB ； 12.焦距& 13.视场角：4 mm，水平视场角：78.3°，垂直视场角：42.9°，对角视场角：91.2° 6 mm，水平视场角：49.1°，垂直视场角：26.3°，对角视场角：57.2° 8 mm，水平视场角：37.5°，垂直视场角：20.7°，对角视场角：43.3° 12 mm，水平视场角：23.4°，垂直视场角：13.3°，对角视场角：26.8° 14.补光灯类型：智能补光，可切换白光灯、红					

		外灯 补光距离：红外光最远可达 50 m，白光最远可达 30 m； 15.防补光过曝：支持； 16.红外波长范围：850 nm ； 17.最大图像尺寸：2688 × 1520； 17.视频压缩标准：主码流：H.265/H.264； 19.子码流：H.265/H.264/MJPEG； 20.第三码流：H.265/H.264 ； 21.网络：1 个 RJ45 10 M/100 M 自适应以太网口； 22.音频：1 个内置麦克风，1 个内置扬声器。					
1.5	支架	壁装	台	26	25	650	
1.6	定制机柜	定制	个	13	500	6,500	

1.7	10口POE交换机	1. 二层web网管交换机，交换容量192Gbps，包转发率30Mpps； 2. 8个10/100/1000Mbps自适应电口(支持POE/POE+，整机PoE最大输出功率125W，单端口最大输出功率30W)，2个SFP千兆光口； 3. 支持VLAN、ACL、端口镜像、端口聚合等功能。	台	13	1,500	19,500	
1.8	光模块	10km，单模双纤	对	13	365	4,745	
1.9	辅材		项	1	5,000	5,000	
	小计一					711,875	
2、集成服务							
2.1	智能网关		项	25	700	17,500	
2.2	摄像机、机柜		项	39	160	6,240	
2.3	组态联调费消防主机	主机探点数据生成	项	25	700	17,500	
	小计二					41,240	

三、监控室移位改造							
1、创新创业园改造							
1.1	监视器移位	含解码器	台	15	250	3,750	
1.2	光纤收发器	千兆	对	1	450	450	
1.3	机柜	12U 机柜	台	1	500	500	
1.4	交换机	1. 非网管型交换机，交换容量 16Gbps，包转发率 11.9Mpps； 2. 8 个 10/100/1000Mbps 自适应电口； 3. 桌面式铁壳小端口交换机； 4. 支持标准交换、端口隔离两种模式切换。	台	1	1,350	1,350	
1.5	光纤跳线	sc-sc	根	4	45	180	
1.6	辅材	网线、电源线、管线	项	1	1,000	1,000	
	小计一					7,230	
2、新能源产业园改造							
2.1	监视器移位	含 NVR	台	2	250	500	
2.2	POE 交换机	1. 非网管型交换机，交换容量 20Gbps，包转	个	1	1200	1,200	

		发率 14.9Mpps； 2. 10 个 10/100/1000Mbps 自适应电口(支持 POE/POE+，整机 PoE 最大输出功率 120W，单端口最大输出功率 30W)； 3. 支持 PoE 看门狗； 4. 桌面式铁壳小端口交换机； 5. 支持标准交换、端口隔离、长距离传输三种模式切换。					
2.3	交换机	1. 网管型交换机，交换容量 16Gbps，包转发率 11.9Mpps； 2. 8 个 10/100/1000Mbps 自适应电口； 3. 桌面式铁壳小端口交换机； 4. 支持标准交换、端口隔离两种模式切换。	台	1	850	850	
2.4	机柜	12U 机柜	台	1	500	500	
2.5	枪机	1.400 万定焦智能筒型网络摄像机； 2.支持越界侦测，区域入侵侦测，进入区域侦	台	1	980	980	

		测和离开区域侦测，支持联动声音报警； 3.最高分辨率可达 2688 × 1520 @25 fps，在该分辨率下可输出实时图像； 4.支持背光补偿，强光抑制，3D 数字降噪，120 dB 宽动态，适应不同环境； 5.支持 ROI 感兴趣区域增强编码，支持 Smart265/264 编码，可根据场景情况自适应调整码率分配； 6.1 个内置麦克风，1 个内置扬声器，支持双向语音对讲； 7.智能补光，支持白光/红外双补光，红外最远可达 50 m，白光最远可达 30 m； 8.符合 IP66 防尘防水设计，可靠性高； 9.传感器类型：1/3″ Progressive Scan CMOS； 10.最低照度：彩色：0.005 Lux @（F1.2，AGC					

		ON），0 Lux with IR； 11.宽动态：120 dB ； 12.焦距&视场角：4 mm，水平视场角： 78.3°，垂直视场角：42.9°，对角视场角： 91.2° 6 mm，水平视场角：49.1°，垂直视场角： 26.3°，对角视场角：57.2° 8 mm，水平视场角：37.5°，垂直视场角： 20.7°，对角视场角：43.3° 12 mm，水平视场角：23.4°，垂直视场角： 13.3°，对角视场角：26.8° 13.补光灯类型：智能补光，可切换白光灯、红外灯； 14.补光距离：红外光最远可达 50 m，白光最远可达 30 m； 15.防补光过曝：支持；					

		16.红外波长范围：850 nm ； 17.最大图像尺寸：2688 × 1520； 18.视频压缩标准：主码流：H.265/H.264； 19.子码流：H.265/H.264/MJPEG； 20.第三码流：H.265/H.264 ； 21.网络：1 个 RJ45 10 M/100 M 自适应以太网口； 22.音频：1 个内置麦克风，1 个内置扬声器 。					
2.6	枪机支架	壁装	个	1	25	25	
2.7	辅材	网线、电源线、管线	项	1	1,000	1,000	
	小计二					5,055	
	总计					1,932,370	