福建省数字福建建设项目
福建省智慧消防云平台
可行性研究报告暨初步设计方案

项目名称：福建省智慧消防云平台

申报单位：福建省消防救援总队

地址： 福建省福州市鼓楼区北二环西路 196 号

邮编：350001

项目单位主管或分管领导：

项目责任人：

电话：

传真：

主持部门：

申报日期：2021 年 10 月

福建省智慧消防云平台
可行性研究报告暨初步设计方案
（全套文件）

项目编号：

建设单位：福建省消防救援总队

编制单位：中通服中睿科技有限公司

二〇二一年十月

文件组成

全一册　福建省智慧消防云平台可行性研究报告暨初步设计方案

咨询设计文件分发表

发往单位或部门	全套文件	说明及图纸
建设单位	10	0
咨询设计单位存档	0	0
合计	10	0

总工程师：宋永胜

报告负责人：曾哲君

审核：中通服中睿科技有限公司

主要编制人：何明、梁广智、黄其彬

咨询设计资格证书

工程咨询单位甲级资信证书

资信类别：　专业资信

单位名称：　中睿通信规划设计有限公司

住　所：　广东省广州市天河区陶育路78号201房(一照多址)

统一社会信用代码：　914400005989387729

法定代表人：　李宝文　　技术负责人：　宋永胜

证书编号：　914400005989387729-18ZYJ18

业　务：　电子、信息工程(含通信、广电、信息化)

发证单位：中国工程咨询协会

2018年09月30日

中华人民共和国国家发展和改革委员会监制

目 录

第1章 项目概述

1.1.项目名称

项目名称：福建省智慧消防云平台

1.2.项目建设单位和负责人、项目责任人

项目建设单位：福建省消防救援总队

项目建设单位分管领导：

项目负责人：

项目联系人：

1.3.项目背景

城市治理和管理不仅是国家治理体系的重要组成部分，同时也是全球互联网治理体系的重要载体和构建网络空间命运共同体的重要基础。过去的几年间，我国众多城市开展了智慧城市建设试点，有效改善了公共服务水平，提升了管理能力，促进了城市经济发展。十八届三中全会提出推动国家治理体系和治理能力现代化，随着国家治理体系和治理能力现代化的不断推进，和“创新、协调、绿色、开放、共享”发展理念的不断深入，随着网络强国战略、国家大数据战略、“互联网+”行动计划的实施和“数字中国”建设的不断发展，城市被赋予了新的内涵和新的要求，这不仅推动了传统意义上的智慧城市向新型智慧城市演进，更为新型智慧城市建设带来了前所未有的发展机遇。

近年来，随着社会的发展进步，城市高层、大型建筑和各类场所单位日益增多，消防安全形势异常严峻，消防安全监督管理部门人员有限，消防安全监管缺乏有效的技术手段支撑和社会化手段配合，无法及时发现、消除、整改重大火险隐患，火灾风险的发生几率仍然居高不下。

2016 年 6 月，原公安部消防局组织全国各省（区、市）消防救援总队总队长、防火监督部部长等领导召开创新消防管理暨 2016 年防火监督工作会议。原公安部消

防局局长于建华对该次会议作出重要批示，他表示，“智慧消防”的创新实践，充分凸显“防消互联”理念，通过现代科技的深度应用，有效打通了消防安全责任落实的“最后一公里”，将消防社会化工作格局提升到一个新的高度，代表着消防工作未来转型发展的方向，也将为平安中国建设增添新的助推力量。原公安部消防局《2017年消防工作总体思路和重点工作》通知中强调消防工作要“加快构建基于大数据、依托‘智慧城市’、综治网络社会化消防安全管理平台”，“借助公安视频监控平台、社会单位视频平台等，推动建设可视化的火灾监控系统”。《公安消防“四项建设”三年规划－公消[2015]63 号》中指出“依托‘智慧城市’建设，充分利用公安视频图像等资源，开展城市消防物联网远程监控系统示范建设，并推动纳入综治平台同步建设”。所以消防安全平台统一规划、基于大数分析、消防与视频结合是建设消防物联网远程监控系统的三个必要条件。2017 年 10 月 10 日公安部发布《关于全面推进“智慧消防”建设的指导意见》，要求在全面推进“智慧消防”建设的基础上，按照“急需先建、内外共建”的方式，重点抓好城市消防物联网监控系统、基于“大数据”“一张图”的实战指挥平台、高层住宅智能消防预警系统、数字化预案编制和管理应用平台、“智慧”社会消防安全管理系统等“五大项目”建设内容，并提出重要的工作要求和四个强化。根据原公安部消防局《关于全面推进“智慧消防”建设的指导意见》（公消[2017]297 号）及福建省人民政府办公厅《福建省“十三五”消防事业发展专项规划》文件精神，为提高全省消防工作科技化、信息化、智能化水平，进一步加强火情预测预警预防能力，全面提升我省消防安全管理和综合监测能力，做到力争“消防安全管理全国最优，消防信息化建设全国一流”，福建省消防救援总队提出建设“福建省智慧消防云平台”项目。

“智慧消防”作为新型“智慧城市”建设的重要一环，是实现消防监管、消防管理、消防服务、消防宣传以及消防全民共建的重点智慧城市信息化建设工作任务，新时代下建立智慧型消防监管服务体系，是保障人民群众生命财产安全、保障社会生产生活、提高民众对政务服务满意度评价、体现社会制度优越性的有效手段之一。

随着智慧城市建设的不断推进，全国各地的智慧消防建设和规划也是如火如荼，就像雨后春笋一样。当前福建省内部分地市、区县已陆续开展或规划“智慧消防”系统平台或相关消防物联网远程监控系统等信息化建设。作为省级平台，由福建省消防救援总队主导，在规划设计和建设“福建省智慧消防云平台”时，在汲取全国

各地智慧消防建设经验和教训的基础上，如何从各地纷繁复杂的消防物联网、智慧消防平台建设迷雾中跳出来，以更清晰的视角、更高的格局来审视和规划全省智慧消防建设大局，这是福建省智慧消防云平台的规划设计所要达成的一个首要目标。因此，福建省智慧消防云平台，必须站在省级高度，对当前全省智慧消防建设大盘进行统筹和引导，实现标准的统一、平台的统一、制度的统一，让全省大大小小的智慧消防平台，融合起来，形成先进、高效、有序、有机的整体。脱离于消防行业纵向与横向业务体系的独立建设，只会形成平台孤岛，不利于消防业务的全省统筹、调度协同及信息共享。

1.4.项目可研暨初设编制依据

1.4.1. 编制依据清单

1.4.1.1. 政策法规

1．中共中央办公厅、国务院办公厅印发《国家信息化发展战略纲要》；

2.国务院办公厅印发《“互联网+政务服务”技术体系建设指南》（国办函〔2016〕108号）；

3．福建省国民经济和社会发展第十四个五年规划和二〇三五年远景目标纲要；

4．原公安部消防局：关于印发《公安部消防局 2018 年工作要点》的通知（公消〔2017〕378号）；

5.原公安部消防局:《关于全面推进“智慧消防”建设的指导意见》（公消〔2017〕297号）；

6．公安部、中央综治办、民政部、住房和城乡建设部、国家安全生产监督管理总局、国家能源局：关于印发《高层建筑消防安全综合治理工作方案》的通知（公消〔2017〕218号）；

7．国务院安全生产委员会《关于开展智慧安全用电综合治理工作的通知》（安委〔2017〕4号）；

8．原公安部消防局：《关于加强超大城市综合体消防安全工作的指导意见》（公消〔2016〕113 号）；

9．公安部、中央机构编制委员会办公室、发展改革委、民政部、财政部、住房城乡建设部：《关于加强城镇公共消防设施和基层消防组织建设的指导意见》（公通字〔2015〕24 号）；

10．原公安部消防局：关于印发《公安消防“四项建设”三年规划（2015—2017年）》的通知（公消〔2015〕63 号）；

11．原公安部消防局：《关于认真贯彻落实孟建柱同志重要指示精神深入推进消防工作社会化有关重点工作的通知》（公消〔2011〕351 号）；

12．原公安部消防局：关于印发《推进和规范城市消防安全远程监控系统建设应用的指导意见》的通知（公消〔2008〕466 号文件）；

13．原公安部消防局：关于印发《建筑消防设施及火灾报警远程监控系统技术论证及推广应用座谈会纪要》的通知（公消〔2006〕139 号文件）；

14.《国家电子政务工程建设项目管理暂行办法》（国家发展改革委员会 2007）；

15.《福建省电子政务建设和应用管理方法》（福建省政府令 156 号）；

16.《福建省数字福建建设领导小组办公室关于印发福建省数字福建建设项目管理办法的通知》（2011 年 1 月）；

17.《福建省人民政府办公厅关于印发福建省“十三五”数字福建专项规划的通知》（闽政办〔2016〕71 号）；

18.《福建省人民政府办公厅关于印发 2018 年数字福建工作要点的通知》（闽政办〔2018〕24 号）；

19.《福建省政务外网建设技术规范》；

20.《福建省政务外网网络业务接入规范》；

1.4.1.2. 标准和规范

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

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

7.《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）；

8.《计算机信息系统安全保护等级划分准则》（GB 17859-1999）；

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

10.《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）

11.《信息安全技术网络安全等级保护定级指南》（GA/T1389-2017）；

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

13.《信息安全技术网络安全等级保护安全设计技术要求》（GB/T 25070-2019）；

14.《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）；

15.《信息安全技术信息系统安全保障评估框架》（GB/T 20274-2008）；

16.《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）；

17.《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）；

18.《计算机软件文档编制规范》（GB/T 8567-2006）；

19.《计算机软件需求规格说明书规范》（GB/T 9385-2008）；

20.《计算机软件测试文档编制规范》（GB/T 9386-2008）；

21.《数据和交换格式》（GB/T 7408-2005）；

22.《综合布线系统工程验收规范》（GB 50312－2016）；

23.《安全生产信息资源目录体系第 1 部分：总体框架》；

24.《安全生产信息资源目录体系第 2 部分：技术要求》；

25.《安全生产信息资源目录体系第 3 部分：核心元数据》；

26.《安全生产信息资源目录体系第 4 部分：信息资源分类》；

27.《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》；

28.《安全生产信息资源目录体系第 6 部分：技术管理要求》；

29.《消防信息代码》（GA/T 974-2015）；

30.《消防基础数据平台接口规范》（GA/T 1036-2012）；

31.《消防公共服务平台技术规范》（GA/T 1038-2012）；

32. GB26875-2016《城市消防远程监控系统》；

33. 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》

34. GB26875.2-2011《城市消防远程监控系统 第 2 部分：通信服务器软件功能要求》

35. GB/T26875.3-2011《城市消防远程监控系统 第 3 部分：报警传输网络通信协议》

36. GB/T26875.4-2011《城市消防远程监控系统 第 4 部分：基本数据项》

37. GB26875.5-2011《城市消防远程监控系统 第 5 部分：受理软件功能要求》

38. GB26875.6-2011《城市消防远程监控系统 第 6 部分：信息管理软件功能要求》

39. GB/T26875.7-2015《城市消防远程监控系统 第 7 部分：消防设施维护管理软件功能要求》

40. GB/T26875.8-2015《城市消防远程监控系统 第 8 部分：监控中心对外数据交换协议》

41. GB16806-2006《消防联动控制系统》；

42. GB25201-2010《建筑消防设施的维护管理》；

41. GB28184-2011《消防设备电源监控系统》；

43. 城市消防远程监控系统技术标准（征求意见稿 GB 50440-2020）。

1.4.1.3. 其他编制依据

1.《中华人民共和国国民经济和社会发展第十三个五年规划纲要》;

2.《国家突发事件应急体系建设“十三五”规划》;

3.《国家综合防灾减灾规划（2016—2020 年）》;

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）。

1.4.2. 重要参考依据明细选摘

1.4.2.1. 公消〔2017〕297 号

为深入贯彻落实中央政法委和公安部党委关于提升政法及公安工作现代化水平的部署要求，加速推进现代科技与消防工作的深度融合，全面提高消防工作科技化、信息化、智能化水平，实现信息化条件下火灾防控和灭火应急救援工作转型升级，现提出如下意见：

一、基本原则

（一）突出精准防控。按照“纵向贯通、横向交换、条块融合”的原则，统一数据标准、规范数据来源，对消防内部、外部数据资源进行汇聚和挖掘分析，为火灾风险研判、灭火救援指挥、队伍管理分析、消防宣传服务和领导指挥决策等提供信息支撑。

（二）突出协同共治。建设消防安全治理工作平台，推进面向政府部门、社会单位、中介组织和社会公众的消防社会化发展进程，创新社会消防安全治理新模式，

形成多元共治、齐抓共管、全民参与、全社会共享的社会消防安全治理新格局。

（三）突出服务实战。按照“信息互通、快速便捷、辅助指挥”的原则，建立覆盖全国的应急通信系统，提升应急通信网络覆盖能力，搭建“一张图”的实战指挥平台，整合灭火应急救援基础信息和社会资源，做到灭火救援预案随机调阅查询、作战全程评估和灾害事故发展趋势预判，确保各级消防队伍指挥作战响应迅捷、决策科学、处置高效。

（四）突出服务民生。全面提升消防移动业务工作效能和移动信息化服务水平，为消防基层基础工作向深度、广度延伸提供保障，为社会公众个性化消防安全需求提供服务，做到让数据多跑路、群众少跑腿。

（五）突出消地融合。牢固树立“警力有限、民力无穷、科技力无尽”的理念，坚持走“消民联合、消地融合”的道路，充分发挥天津、上海、沈阳、四川消防研究所的作用，加强与龙头企业、高等院校、科研机构等深度合作，借助社会优势资源，借助“外力”联合开展项目攻关和关键技术研究，充分运用先进实用的消防科技成果。

二、工作目标

按照《消防信息化“十三五”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勤务机制提供有力支撑，全面提升社会火灾防控能力、消防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。

三、重点任务

在全面推进“智慧消防”建设的基础上，按照“急需先建、内外共建”的方式，

近两年重点抓好“五大项目”建设，实现动态感知、智能研判、精准防控，为消防工作和消防队伍建设提供信息化支撑。

（一）建设城市物联网消防远程监控系统

1．打造城市消防远程监控系统“升级版”，综合利用 RFID（射频识别）、无线传感、云计算、大数据等技术，依托有线、无线、移动互联网等现代通信手段，整合已有的各数据中心，扩大监控系统的联网用户数量，完善系统报警联动、设施巡检、单位管理、消防监督等功能。在传统监测火灾自动报警系统的运行状态及故障、报警信号基础上，利用图像模式识别技术对火光及燃烧烟雾进行图像分析报警；监测室内消火栓和自动喷淋系统水压、高位消防水箱和消防水池水位、消防供水管道阀门启闭状态、防火门开关状态，利用单位视频监控系统监控安全出口和疏散通道、消防控制室值班情况；接入电气火灾监控系统或装置，实时监测漏电电流、线缆温度等情况；研发手机 APP 系统，动态监控、立体呈现联网单位消防安全状态，全面提升社会单位消防安全管理水平和消防监督执法效能。

2．依托“智慧城市”建设，调整城市物联网消防远程监控系统运营现有的“中介模式”，推行由政府投资运营或政府委托有关机构运营的“政府模式”。各级消防部门主动向当地政府报告，申请专项经费投资建设，单位免费接入，每年安排运行经费预算，不向单位收取运行管理费，不增加单位经济负担，确保系统有序建设、规范运营、健康发展。

3．在直辖市、省会市、首府市以及计划单列市基本建成的基础上，逐步向有条件的城市推开物联网消防远程监控系统，2018 年底地级以上城市建成并投入使用。目前已建成系统的城市，2017 年底 70%以上的火灾高危单位和设有自动消防设施的高层建筑接入系统，2018 年底全部接入。新建系统的城市，2018 上半年 30%以上的

火灾高危单位和设有自动消防设施的高层建筑接入系统，2018 年底全部接入。

（二）建设基于“大数据”“一张图”的实战指挥平台

1．充分运用大数据、云计算、移动互联网、地理信息等技术，依托公安网（消防信息网及指挥调度网）、边界接入平台和公安 PGIS 地图，实现灭火救援的一张图指挥、一张图调度、一张图分析、一张图决策。灾情信息实时化，通过城市重大事故及地质性灾害事故救援两大应急通信系统，实时获取灾害现场图像、语音和数据，掌握灾情动态及发展态势；作战对象精准化，逐级汇聚一体化消防业务信息系统等数据，关联作战对象的地理位置、概况、结构、消防设施和数字化预案，以及周边道路、水源、重大危险源等信息，为分析研判作战对象提供立体式支撑；力量信息精确化，优化基础信息采集维护手段，实现辖区消防队站、多种形式消防队伍、装备器材、保障物资等信息上图展示，为科学指挥和力量调度提供准确信息参考；作战指挥可视化，应用位置定位、物联网、移动指挥终端等设备，掌握调动力量所在位置、数量和状态，实现移动式信息推送、一键式力量调度和前后方信息交互；通过共享对接政府应急联动部门、社会应急联动单位、联勤保障单位等信息资源，提高接警出动、联合处置、联动协同效能。在深度整合信息资源的基础上，实现灭火救援信息要素的“一张图”展示和“大数据”分析，为各级指挥员提供辅助决策支撑，不断提升消防队伍灭火救援科学化、智能化水平。

2．各级平台按照“统一数据标准、统一关键技术、属地组织建设、体现层级差异”的原则建设，确保在指挥体系上的完整和数据的共享互通。应急管理部消防救援局平台突出全国信息资源共享查询分析、国家级应急联动指挥、宏观态势研判和跨省指挥调度；总队平台发挥承上启下作用，突出对属地灾情处置和作战指挥的精确管控；支队平台在拓展现有消防接处警系统功能的基础上，建设个性化研判分析

工具和辅助指挥应用，突出各类信息收集、上报、精细化指挥和全过程科学战评。

3．2017 年底，各总队、支队按照《城市重大事故及地质性灾害事故救援应急通信系统建设技术方案》，完成全国 10 支应急通信保障分队和两大应急通信系统示范建设；按照《实战指挥平台建设技术指导意见》，完成本级实战指挥平台建设或升级改造项目方案编制立项，实现 10 类基础信息采集、上报，并在本级地图上加载，满足应急管理部消防救援局实战指挥平台调用需要。2018 年底，总队、支队按技术方案和技术指导意见，完成本级实战指挥平台建设、升级改造及两大应急通信系统建设，实现应急管理部消防救援局、总队、支队三级实战指挥平台联网运行，各类信息资源数据在平台上实现常态化采集维护。

（三）建设高层住宅智能消防预警系统

1．结合当地智慧用电、用气、用水系统建设，整合高层住宅建筑各类监控系统和视频资源，建立智能消防预警系统。在新建高层住宅应用城市物联网消防远程监控系统，对消防设施、电气线路、燃气管线、疏散楼梯等进行实时监测。在老旧高层住宅建筑加装应用独立式火灾探测报警器、简易喷淋装置、火灾应急广播以及独立式可燃气体探测器、无线手动报警、无线声光警报等设施。

2．研发手机 APP 系统，利用移动互联网技术将各类监测信息与手机互联互通，消防监督员、公安派出所民警、社区网格员、物业管理人员、微型消防站队员以及楼栋居民，可实时接收火灾报警信号，查看消防设施、安全疏散、电气燃气等各项监测数据，实现高层住宅消防安全信息化管理。

3．结合城市物联网消防远程监控系统，同步建设高层住宅智能消防预警系统。目前已建成城市物联网消防远程监控系统的城市，2017 年底 70%以上设有自动消防设施的高层住宅接入系统、应用 APP 平台，2018 年底全部接入应用。新建系统的城

市，2018 上半年 30%以上设有自动消防设施的高层住宅接入系统、应用 APP 平台，2018 年底全部接入应用。2018 年上半年，50%以上的老旧高层住宅加装简易消防设施，2018 年底全部加装。

（四）建设数字化预案编制和管理应用平台

1．充分利用物联网、移动互联网及各类传感器技术，采集作战对象的基础数据和消防队伍基础信息，制作满足消防队伍日常熟悉演练、作战指挥需要的数字化预案；预案能够通过全景、三维建模等方式展示灭火救援要素，动态展现灾情演变或作战效能；预案管理应用平台与 119 接警调度系统、“六熟悉”管理系统和实战指挥平台进行融合、双向互通，在现场可实现力量查询、地理信息测量、作战部署标绘、辅助单兵定位等功能，辅助指挥员开展计划指挥和临机指挥；在室内开展熟悉演练、战例复盘、作战指挥推演、三维场景展示，辅助指战员开展业务学习。

2．应急管理部消防救援局研发数字化预案管理应用平台，规范预案输出和数据交换格式，研发“六熟悉”管理系统，自动采集重点单位基础信息和动态信息数据，同步导入一体化信息系统基础信息，实现“一张图”可视化管理；各地根据预案等级和作战指挥需求，采取基于地理信息系统的二维图片、全景照片、三维立体建模、无人机倾斜摄影等技术编制数字化预案。

3．2017 年底前，总队、支队和大队完成数字化预案模板；2018 年 6 月前，完成预案管理应用平台研发，与实战指挥平台、熟悉演练平台、移动指挥终端的无缝联接；2018 年底，各地完成总队、支队级预案编制，实现案例复盘、模拟演练培训，各消防救援站级预案完成 50%，实现移动终端远程查询，作战指挥中心远程推送。

（五）建设“智慧”社会消防安全管理系统

1．各地特别是国家“智慧城市”试点地区，要主动争取当地政府支持，协调综

治、科技、工信、住建等部门，将“智慧消防”纳入“智慧城市”建设总体规划，在汇聚整合消防部门数据资源、强化“纵向贯通”基础上，重点强化与政府有关部门数据的“横向交换”，形成外部数据“为我所用”、输送数据“共治共享”的工作格局。

2．提请当地政府将“智慧消防”嵌入“智慧城市”管理，重点将监管部门、行业部门消防管理责任纳入城市综合管理服务 “一张网”，各司其职、各负其责，在各自行业领域同步落实消防管理，建立起政府统一领导下的监管部门、行业部门、基层组织、社会单位齐抓共管的消防安全责任体系。

3．积极创新社会消防管理，引导社会单位利用移动互联网技术建立单位内部消防安全管理系统，实现消防安全信息网上录入、巡查流程网上管理、检查活动网上监督、整改质量网上考评、安全工作网上研判，强化落实主体责任。引导消防产品生产企业提供产品终身服务，鼓励企业的远程服务系统免费接收联网用户信息。结合社会信用信息平台建设，建立消防安全诚信信息系统，完善消防安全不良行为“黑名单”制度，建立消防诚信信息与相关部门的互通互认机制。

4．拓展社会公众消防安全服务平台功能，完善“统一受理、协同办理、按需发布”的服务模式，丰富信息服务资源，创新信息服务手段，增加执法透明度、简化优化服务流程、提高办事效率、提升群众满意度。

四、工作要求

（一）强化组织领导。各总队要成立由主官负总责的“智慧消防”建设工作领导小组，建立实体化运行机制，统筹“智慧消防”建设规划、项目把关、指挥决策和对外协调。要针对“五大项目”逐项制定具体实施方案和工作计划，建立完善保障奖惩机制，统一规划、统一部署、协调推进，确保项目有效推进，取得实效。

（二）强化顶层设计。按照应急管理部消防救援局《消防信息化“十三五”总体规划》要求，坚持以块为主、条块结合，应急管理部消防救援局负责制定下发相关指导意见、消防大数据平台建设技术方案，总队负责本地“五大项目”统筹规划与协调建设，支队负责本地“五大项目”的业务支撑与实战应用。

（三）强化建设保障。要充分利用“智慧城市”试点建设的契机，积极争取地方政府和有关部门多层次、多渠道立项，加大建设投入，落实资金预算，纳入重点保障。要在政府的统一领导下，引导鼓励社会资本参与“五大项目”建设，按照政府购买服务或外包租赁等方式，落实有关建设经费。

（四）强化考核评估。要将“五大项目”建设纳入年度重点工作任务，按照项目化管理的方式，对目标任务推进落实情况实施过程评估、督导、考核。对工作成绩突出的单位和个人给予表彰奖励，对任务推进缓慢、工作成效不明显的要及时约谈。

1.4.2.2. 福建省国民经济和社会发展第十四个五年规划和二〇三五年远景目标纲要（草案）

该份目标纲要有关智慧消防建设相关的内容摘要如下：

1．建设智慧城市和数字乡村

推进“数字城市大脑”建设，加快城市运行“一网统管”步伐，深化社会治理智慧化应用，实现“观管防”有机统一。加强城市“神经元”感知系统建设，提供城镇交通、给排水、能源、通信、环保、应急、消防、防灾与安全生产等智慧应用服务。建设数字乡村，推进农村基层政务信息化应用，加快现代信息技术与农村生产生活全面深度融合。推进益农信息社建设。

2．提升城市综合承载能力

统筹城市规划、建设、管理，促进城市更加健康安全宜居。改善城市公用设施，实施老旧小区改造、市政管网建设、智慧设施建设等城市更新重大工程。推动城市生态修复和功能完善，完善绿地系统布局，增加生态休闲空间，提升绿化美化彩化水平。完善绿道网络，建设依山傍水、串联城乡的“万里福道”。提升城市抵御冲击和应急保障能力，加强城市防洪、抗震、人防、消防、排水防涝的设施建设，合理规划应急避难场所、方舱医院等，打造海绵城市、韧性城市。建设智慧城市，大力发展智慧管网、智慧水务等，支持智能停车、智慧门禁、智慧消防、智慧养老等智慧社区应用和平台建设。保护城市历史文化，挖掘底蕴，扩大福州、泉州、漳州、长汀等历史文化名城国内外知名度和影响力。提升建筑业发展质量，发展工程总承包和装配式建筑，培育新时期建筑业产业工人大军。

3．健全救灾体系

提升综合抢险救灾能力，整合优化省级专业应急救援中心，统筹自然灾害、消防、安全生产事故救援等专业力量，健全快速调动机制，增强森林火灾、洪涝灾害、地震灾害等应急处置能力，提高危险化学品、矿山、金属冶炼等重点行业领域专业应急救援能力。实施基层应急能力提升示范点和基层防灾减灾示范工程，推进综合性基层应急队伍建设，完善防灾减灾工作预案，确保预警到乡、预案到村、责任到人，提高农村抵御防范各类灾害能力。完善社会力量参与防灾减灾政策，建立社会力量参与防灾减灾救灾工作平台。

4．加强应急保障能力建设

健全应急管理体制机制，完善标准体系和组织体系，优化风险防控、监测预警、应急联动、应急新闻工作、信息发布、恢复重建等机制。统筹利用社会资源，加快新技术应用，强化应急协同保障能力。完善消防安全共治共享机制，加强城乡公共消防基础设施建设，优化消防救援队伍、森林消防队伍人员及装备配置。健全突发事件和应急处置风险防控监测预警服务体系，完善应急预案评估与演练机制。加强防汛、抢险、救助物资储备，构建统一应急物资储备信息化管理平台，建立省市县乡四级应急物资储备网络。

5．专栏 41：应急保障重大工程

应急救援体系：推进应急预案体系、应急救援力量、应急救援航空体系等建设。建设感知网络、通信网络、应急指挥视频调度系统、应急数据治理系统、应急管理综合应用平台等。建强国家综合性消防救援队伍，壮大政府专职消防队、志愿消防队、微型消防站等多种形式消防队伍，补充消防救援队伍力量，推进“防消一体化”，实现城乡消防救援力量全覆盖。

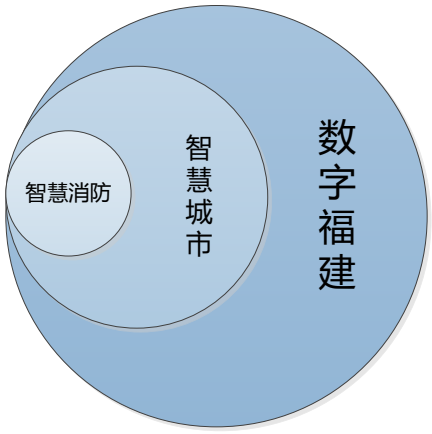
公共消防基础设施建设：适应“全灾种、大应急”需要，加强消防救援站、消防供水、消防通信、先进消防装备、消防车通道和省市两级消防训练基地、国家级消防科普教育基地建设。建设“智慧消防”平台。

1.5.项目建设目标、建设内容、建设期限

1.5.1. 建设目标

1.5.1.1. 总体目标

“智慧消防”是智慧城市的重要组成部分，而智慧城市又是福建省委、省政府历年来针对“数字福建”整体和阶段规划部署工作的首要目标之一。所以，智慧消防建设必须依托于福建省关于“数字福建”相关政策法规、建设管理制度和项目建设管理办法等进行统一开展。



智慧消防、智慧城市、数字福建三者关系图（子集）

“数字福建”，即信息化的福建。数字福建建设的主要目标，是将全省各部门、各行业、各领域、各地域的信息通过数字化和计算机处理，最大程度地加以集成和利用，快速、完整、便捷地提供各种信息服务，实现福建省国民经济和社会信息化。“数字福建”的主要内容包括以下几个方面：第一，加强对信息基础设施建设，扩大利用互联网，健全公共信息网；促进电信、有线电视、计算机三网结合；实现各种信息网络互联互通，构成覆盖全省的信息共享体系。第二，开发和整合利用各种信息资源。第三，建立和发展“数字福建”的技术支撑体系。第四，以信息化带动工业化。第五，建设“电子政府”，推进政府系统信息化建设。第六，开发建设重点领域信息应用系统。

智慧消防主要侧重于上述数字福建主要内容中的第六点建设。在消防监管、消防服务、消防产业等领域，通过智慧消防平台的建设，辐射覆盖全省消防各领域，以技术促进业务发展，以技术整合消防领域产业经济信息要素。信息技术只是手段，最终目标是在先进信息技术手段的加持下，以规范的监管、高效的服务，促进消防产业“数字经济”的大发展，为“数字福建”的中长期规划建设做好扎实的铺垫与补充。

另外，智慧消防除在本消防领域的建设发展外，还将按照“数字福建”的全省信息共享体系建设要求，在横向与纵向上建立消防政务信息、消防服务信息、消防产业信息等各种类型信息的对外共享机制。例如：在横向上，与各省直职能部门之间实现开放式政务信息互联互通与数据共享，消除因职能差异和行政壁垒而产生的消息数据不流通；在纵向上，实现消防体系从上至下的信息快速传递交换与信息穿透，消除因行政层级关系而形成的信息数据请求与下发障碍，确保数据流通顺畅。

1.5.1.2. 具体目标

根据原公安部消防局《关于全面推进“智慧消防”建设的指导意见》（公消[2017]297 号）及福建省委、省政府《新时代数字福建发展纲要》《福建省“智慧消防”建设实施意见》等文件精神，为加快推进福建省火灾智能防控体系建设，创新社会消防治理模式，推动消防安全治理现代化，全面提升消防工作数字化、网络化、智慧化水平，福建省消防救援总队提出建设“福建省智慧消防云平台”项目。

十八届三中全会指出，“全面深化改革的总体目标是完善和发展中国特色的社会主义制度，推进国家治理体系和治理能力的现代化”。因此，在当前信息化高速发展运用的大背景下，有必要采用现代化治理能力，提高政府、社会、城市的综合治理水平，要依托先进、主流的计算机信息技术作为辅助手段，加强城市治理，创新政府行政管理手段和服务方式。

“智慧消防”作为国家及城市治理体系中的重要一环，关系到政府执政能力、社会秩序稳定、民生安全保障、民众满意度等多方面问题。推进“智慧消防”建设，首要目标就是要依托“数字福建”的整体规划，在消防领域构建新时期消防工作格局，着力推动责任落实无缝化、火灾防控立体化、灭火救援实战化、基础保障全城化，不断提升消防工作的信息化服务保障能力，促进消防工作事业持续快速发展。

目前全省、乃至全国各地都陆续建设了与智慧消防相关的应用系统或平台，诸如消防物联网远程监控系统、电气火灾监测系统、智能火灾报警系统、消防高清视频识别监控系统等，有诸多亮点建设，解决了许多消防工作难题，但是存在的问题也不断呈现，并不能从整体上解决消防安全监管及服务的问题。如何从全国、全省各地纷繁复杂的消防物联网、智慧消防平台建设迷雾中跳出来，以更清晰的视角、更高的格局来审视和规划全省智慧消防建设大局，统筹全省智慧消防平台的指导性思想框架和统一技术及应用框架建设，这是本次福建省智慧消防云平台可研设计规划，站在省级平台的高度所要达成的一个首要的、总体的目标。

本方案通过“一平台、两个统一、三项标准、四大性能、五个保障、八大关键技术、N 个业务应用”，从体系上介绍对福建省消防救援总队消智慧消防的场景理解、顶层架构设计、落地实施、客户运营服务全过程。

（一）核心目标需求

1. 数据治理分析

“数据”是整个智慧消防平台的核心，所有的技术工作都是为数据的整个生命周期做支撑保障。在智慧消防平台及其各应用系统中，通过海量、复杂、冗余的数据所反映出来的直观现象，抽丝剥茧地看到消防事件的源头本质，进而追求消防工作效率和消防业务效益的全面提升。

福建省智慧消防云平台的规划设计及后续建设，就是要通过智慧消防平台，将全省各地市、各县区的消防管理数据、物联网监测数据、初步分析结果数据等，汇聚到省级平台，通过对海量数据进行 AI 智能模型分析和 BI 业务模型分析，得出所需要的结果，为消防监管和消防救援提供有价值的辅助决策依据。

2．强化业务能力、保障民生安全

通过智慧消防平台建设，结合数据治理分析成果，为全省各级消防行政主管部门、技术服务单位、消防联防单位机构等提供丰富、规范、高效的信息技术手段，加强城市消防安全管理、监管及服务能力，实现纵向全省各级、横向各部门之间的消防安全快速联动，做到有效日常消防巡查、消防知识普及宣传、消除消防安全隐患、降低消防安全风险、促进救援能力提升，最终达到降低火灾事故发生率、人员伤亡率、财产损失率等目标，成为提升全省各级、各城市综合治理水平的一项重要正向指标。

（二）具体目标需求

1．进行全省智慧消防平台体系统筹，节约财政投资

针对当前福建省内各地待建（规划中）、已建的各种智慧消防信息化应用（如消防物联网），以及众多未建设地区，可由省消防救援总队进行全省统筹规划设计和建设，建设一套 SAAS（软件即服务）模式的智慧消防综合应用平台，涵盖多项全省通用的应用软件系统及功能，实现全省智慧消防、消防物联网业务的统一。另外，省级智慧消防平台还提供 PAAS（平台即服务），省、市、县三级消防部门都可根据自身的特殊业务需求，在省级平台依托 PAAS 进行业务二次开发或挂接外部应用。各

地市已建业务系统，均可通过省级智慧消防平台开放的数据接口，实现与省级平台的快速数据对接。

通过省总队对智慧消防平台软件进行统筹统建的方式，以及提供足够的开放性，既可以节约财政投资，防止极易失败的尝试性建设和重复建设，又兼顾了全省业务的统一和各地市、区县的业务特殊性与差异性。

2．统一技术标准、统一应用架构、统一业务目标

省级智慧消防平台，通过制定一系列技术标准，由省、市、县三级消防部门共同遵守该技术标准进行业务应用开发；通过统一的应用架构定义和设计，让各地市、区县在后续的业务应用开发过程中，可直接使用省级平台提供的应用功能，也可在省级平台应用架构基础上，专注于业务层的开发，无需过多考虑应用架构层的功能支撑和性能稳定情况，从而缩短业务层开发周期，使业务模型快速成型和投入实战；通过统一的业务目标，将省、市、县三级消防部门的业务目标统一起来，不至于在各自进行智慧消防建设过程中，形成各种各样、五花八门的智慧消防应用，无法形成符合规范的、符合消防业务类别的应用及数据，不利于将来的全省消防数据汇聚及后续消防大数据分析。

3．按照“前端－后端”模式进行分工建设

这里提出的“前端”指的是智慧消防最根本、最核心的“数据”资源的采集、传输、存储、初加工的阶段。“前端”实际上就是由各地市、区县建设的消防物联网感知网络——“物联感知网”，全省各地市、区县各自建设感知网，实现数据的前端采集存储，完成终端消防场景动态数据采集目标。“后端”指的是由省总队统建的省级智慧消防平台应用系统，各地市可通过省级平台提供的各种业务管理、数据管理、数据分析等功能对前端“感知网”数据进行治理加工，最终实现本级消防部门的业务目标。

总而言之，就是省级主导“平台”建设、市县主导“感知网”建设。

4．实现全省消防数据汇聚和数据治理

省级平台建设的其中一个关键目的，在于对全省消防物联网监测数据、消防动态业务管理数据进行汇聚整合，形成“消防大数据中心”，并在大数据池中，对各种规范和不规范、逻辑和非逻辑、有价值和无价值的数据统一进行数据治理（包括数据清洗、数据归类、数据整合、数据分析、数据共享），打造全省消防大数据互联互

通平台。

5．打造消防大数据“一张图”综合应用和展示系统

所有采集获取和分析完成的数据，均要以直观的形式对各级消防用户（领导、业务处/科室、基层一线部门及指战员）进行呈现。因此，要牢牢抓住大数据、可视化的要义，打造福建省消防大数据防火监督综合应用系统，在全省及各地市、区县消防“一张图”的基础上，深化消防数据的获取与使用、分析与应用、辅助与决策，服务省、市、县三级防火监督业务。

6．建立“1 个平台、1 个大数据中心、N 个应用”（1+1+N）平台业务架构

建设福建省智慧消防云平台，旨在建立一个省级智慧型消防体系、消防物联网信息化大平台框架，汇聚各种数据（基础数据、监测数据、过程数据、统计分析数据等）形成消防大数据中心，并在框架和数据基础上开展各种业务应用，如消防物联网远程监控系统、消防教育远程培训平台、消防物联网智能预警系统、市政消防设施智慧管理系统、电动车智能充电桩系统、消防安全社会化管理系统、“互联网+消防监管”业务系统等，最终达到“统一平台、统一数据、统一应用”的目标，避免重复建设、信息孤岛、多头管理等情况发生。

7．建设系统安全架构体系，保障系统在各种环境下的运行安全

平台的设计规划及建设，还涉及到平台的系统安全保障。根据各级党政机关和网络信息化安全部门要求，必须按照计算机信息系统等级保护的相关要求，建立完善的安全防护体系，并进行相应的网络安全咨询与评测，确保智慧消防平台在各种网络环境下（应急通信网、政务资源网、互联网、局域网等）的信息安全。

本次省级智慧消防平台的计算机信息系统登等级保护的定级标准为：三级。

8．建设完善的平台运维保障体系

智慧消防平台建成后，为保障平台软硬件系统的长期稳定运行，确保智慧消防业务的可持续运作，需要从“技术运维”和“业务运维”两方面入手，辅以技术及人力资源，建立智慧消防平台运维保障体系，为平台提供长期的技术及业务支撑。

1.5.2. 建设内容

本期福建省智慧消防云平台的建设内容如下：

1．基础硬件架构建设（注：依托于电子政务云平台网络及存储资源）

（1）存储及网络服务

（2）服务器集群和硬件资源虚拟化（云化）

（3）服务器系统软件信创建设（国产化）

2．系统安全架构建设（注：依托于电子政务云平台的安全防护资源）

（1）基于计算机信息系统等级保护条例，建立平台网络信息安全防护体系；

（2）进行网络安全咨询与测评（等保二级）

3．软件应用基础架构建设（SAAS 和 PAAS）

（1）底层应用支撑架构建设，包括：微服务（网关）、微服务（服务治理）、各种基础组件集群、基础支撑服务、ESB 企业服务总线、运营/运维服务、流程处理 BPM；

（2）中台服务建设（含 PAAS），包括：业务中台、技术中台、数据中台；

（3）统一用户注册认证与安全管理（含 SAAS）

4．业务应用系统建设（基于 SAAS 云服务应用架构）

第一层：数据采集与数据管理层级应用

（1）大数据管理维护中心

（2）接口应用（外部应用接入、本地数据共享接口）

（3）消防物联网感知网设备接入管理平台

第二层：业务管理层级应用

（4）城市消防物联网远程监控系统

（5）消防值班运维管理系统（运维监控中心）

（6）消防教育远程培训服务平台

第三层：统计分析与数据呈现层级应用

（7）消防大数据基础统计分析系统

（8）消防大数据“一张图”综合展示系统

具体云应用架构说明如下：

（1）统一全省消防用户体系，建立统一用户认证体系和基础授权体系；

（2）各层级消防管理用户（含消防其他相关单位），可针对本层级单位的特点，以及在省平台应用授权和数据授权的基础上，扩充自身用户规模，并对自建用户进行应用与数据授权。

（3）在云应用架构下，所有层级消防单位的应用数据均统一集中存储（物理集

中、逻辑独立），并可将本层级数据发布为数据服务，实现数据云共享。

（4）各层级消防单位的特殊应用（包括：使用省平台中台服务进行的二次开发、遵循省平台标准的外部独立开发），均可以云应用形式进行挂载。

5．运维服务架构建设

（1）业务运维服务，主要针对省消防救援总队提供日常智慧消防及物联网监测相关运维服务；

（2）技术运维服务，主要提供日常技术维护、技术咨询、功能二次开发等。

6．信创（国产化）建设

针对国家及福建省要求的党政信息化信创工程（国产化）建设要求，福建省智慧消防云平台从设计到建设、部署等各阶段，均要将信创工程设计规划在内，并在消防云平台建成后，除了能适应现有电子政务云平台的环境要求外，应用软件、数据库、云主机及云存储等均要能够满足信创云（国产化改造升级的政务云）的技术标准、部署和运行环境要求。

（1）应用软件的信创（国产化）建设，开发完成后的应用软件能够运行于国产化硬件及系统软件环境；

（2）数据库系统的信创建设，如使用人大金仓、达梦等国产数据库系统；

（3）中间件的信创建设，将传统的 TOMCAT、WEBLOGIC、WEBSPHERE 等中间件替换成国产 WEB 中间件，应用软件必须兼容国产中间件。

（4）云主机和云存储信创建设，依托已完成信创改造升级的福建省电子政务云平台（国产化平台）。

1.5.3. 建设期限

本项目的建设周期包括可行性研究报告暨初步设计方案批复在内为 16 个月（智慧消防平台建设第一期）。

项目实施进度计划（第一期完成目标）如下：

持续时长 1 个月：发出招标通知后一个月内完成项目招投标工作。

持续时长 1 个月：合同签订后，协调相关部门一个月内完成需求调研。

持续时长 8 个月：项目需求确认后，八个月内完成系统开发及调试。

持续时长 1 个月：系统功能开发完成后，协调相关部门一个月内完成系统对接

联调，并初验交付使用。

持续时长 3 个月：初验完成后，系统试运行三个月。

持续时长 1 个月：试运行完成后，开展第三方测试。

持续时长 1 个月：第三方测试完成后，一个月内完成项目终验。

1.6.投资概算及资金来源

本报告方案总投资概算为 5834.4 万元，其中工程费用 5304 万元，工程建设其他费用 530.4 万元。

项目由福建省发改委批准立项，建设资金申请从以下几个渠道综合安排：

1．财政厅年度信息化专项资金。

2．省政府专项经费。

3．“数字福建”建设经费。

4．云资源经费每年单列，不计入建设资金。

项目由福建省消防救援总队负责组织实施，详细预算表格参见“投资概算和资金来源”章节。

1.7.效益与风险

本项目具有良好的经济效益和社会效益，对保障全省消防安全、促进提高全省消防安全、改善全省消防监管和服务具有重要意义，建议加快推进福建省智慧消防云平台的立项和建设。

1．经济效益：节约全省智慧消防建设的财政投入；平台建成投入使用后，为各级消防部门提供防火防灾工作辅助决策分析依据，可尽早发现消防隐患和在消防事故初期提供有效的预案决策辅助，及时阻断，降低损失，保障社会及民众生命财产安全。

2．社会效益：全面提高消防监管及服务工作的整体效率，提升部门机构整体社会形象，提高社会民众满意度和安全感，从消防角度加强城市治理能力，直观反映党和政府优良的执政与行政能力。

本项目建设规模庞大、工程管理复杂繁琐，存在风险的主要包括政策风险、决

策风险、全省各级消防监管部门协调风险、管理风险、成本风险、法律风险等。

1.8.主要结论和建议

福建智慧消防平台项目涉及的系统总体技术框架、应用支撑平台、关键技术路线为信息领域成熟先进技术，采用成熟稳定产品，在国内的项目中有着广泛的应用，具有良好的技术保证；本项目的建设基础良好，项目建设是可行的。在业务方面，结合国内智慧城市、智慧消防近年来的开展和推进形势，各地取得的成就、存在的问题，以及站在省级高度，迫切需要解决的全省统筹问题，建设统一的“省级智慧消防平台”当前是可行的、是必要的。

本项目的建设按照相关规范文件要求，建设目标明确、建设需求内容详实、建设方案可行、建设规模合理、进度安排合理可行、实施方案和项目组织机构落实、投资估算满足控制设计概算的要求。

因此，本项目的开发建设具有重要意义，目前平台建设的条件已基本成熟，技术可行、业务可行，可开始投入实施。

第2章 项目建设单位概况

2.1. 建设单位职能、内部机构设置及在编人数

福建省消防救援总队在应急管理部和省委省政府领导下，主要承担城乡综合性消防救援工作，负责指挥调度相关灾害事故救援行动，重要会议、大型活动消防安全保卫工作；负责火灾预防、消防监督执法以及火灾事故调查处理相关工作，依法行使消防安全综合监管职能，推动落实消防安全责任制；参与拟订消防专项规划，参与起草地方性消防法规、规章草案并监督实施；负责消防安全宣传教育，组织指导社会消防力量建设等工作。

2018 年，根据中央改革部署，公安消防部队集体退出现役，成建制划归应急管理部，组建国家综合性消防救援队伍。消防救援人员作为综合性常备应急骨干力量，定位为应急救援主力军和国家队，承担着防范化解重大安全风险、应对处置各类灾害事故的重要职责。根据中央《组建国家综合性消防救援队伍框架方案》，国家综合性消防救援队伍由应急管理部管理，实行统一领导、分级指挥，设有专门的衔级职级序列和队旗、队徽、队训、队服。

省、市、县级分别设消防救援总队、支队、大队，城市和乡镇根据需要按标准设立消防救援站，形成统一高效的领导指挥体系。

2.2. 信息化工作机构和技术人员配备情况

信息化领导小组是本单位信息化工作的领导机构，负责审议信息化项目规划、方案、经费预算及执行情况，并对信息化建设重大事项进行决策。综合性系统项目由信息化领导小组确定主责牵头部门和配合部门。

信息通信部门负责统筹信息化规划和方案编制，联系协调内外部有关单位，并负责信息化基础设施及通用类项目建设，以及系统整合、信息共享，为项目建设提供技术支撑。

2.3. 项目组织实施机构与职责

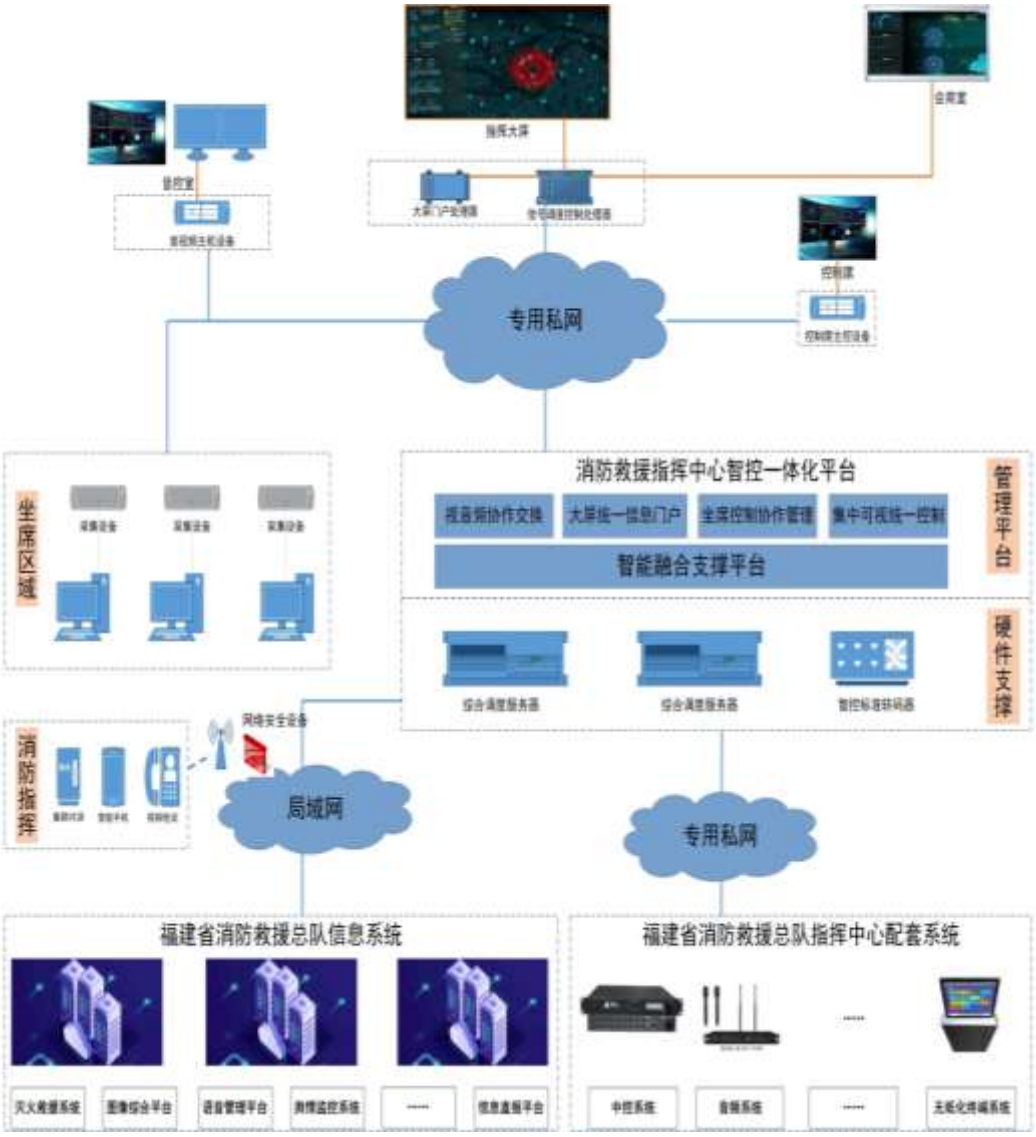
业务部门负责本级业务领域信息系统的业务需求、项目申报，全程参与项目立项、实施、试点和验收，组织项目培训，推进系统应用。

第3章 现状分析与建设必要性

3.1. 指挥中心架构现状

本次“福建省智慧消防云平台”项目将依托福建省政务云平台进行部署和运行开展。届时将可能与指挥中心的网络线路资源进行对接，使用智慧中心座席资源等。因此，需要对总队指挥中心的整体网络现状、应用现状、架构现状等进行分析说明。

3.1.1. 指挥中心总体架构



福建省消防救援总队指挥中心总体架构图

福建省消防救援总队指挥中心通过整体装饰装修，建设包含显示大屏、综合布线、计算机网络、音视频、微模块机房在内的硬件基础设施，部署安全运营平台，构建起“一平台两控制一门户”的指挥中心统一支撑管理体系。

“一平台”，即智能融合支撑平台，可对接入信号、信息、数据进行统一管理，通过统一的操控界面，实现跨系统、跨平台的综合信息可视化汇聚。

“两控制”即融合面向指挥中心运维管理的中央可视控制子系统和面向指挥调度应用的坐席管理协作子系统。可实现对指挥大厅和指挥室等空间的可视化管控，对不同网络上的各类业务应用进行统一操作，实现应急协同指挥，提升整体响应效率。

“一门户”即大屏幕统一信息门户，可作为指挥中心所有应用的统一入口和管理中心，所有应用汇聚到一个画面，实现统一操作与控制。未来可以根据指挥中心的实际应用需求扩展构建各类专题应用。

3.1.2. 总队指挥中心业务现状

目前，福建省消防救援总队指挥中心主要有 3 种运行状态、4 个数据网络、5 套应用系统及众多通信技术，具体业务现状如下表所示：

表 指挥中心业务现状

序号	名称	说明
1	运行状态	战备值班：由值班长、作战值班、行政值班、通信值班、指挥助理五人值守，掌握全省消防救援队伍执勤战备和值班情况，及全省各地灭火和应急救援动态信息。 作战指挥：接到重大灾情报告后转入作战指挥状态，各科室相关人员进驻指挥中心，通过应急通信系统实时了解现场情况，开展灭火救援战斗行动的组织指挥工作，按要求遂行出动。 视频会议：主要有灾害处置连线、值班视频调度会、工作视频调度会，涉及 4 套视频会议终端设备，分别为华为、科达、宝利通、华平。
2	数据网络	互联网、政务外网、应急指挥网、指挥调度网，日常办公主要访问互联网及政务外网。
3	应用系统	灭火救援系统：部署于指挥调度网 图像综合平台：部署于指挥调度网 语音管理平台：部署于指挥调度网 信息直报平台：部署于指挥调度网 舆情监控系统：部署于互联网
4	通信技术	卫星电话、PTT 公网对讲手机、350M 常规对讲、350M 集群对

序号	名称	说明
		讲、短波通信、固定电话、移动电话等。

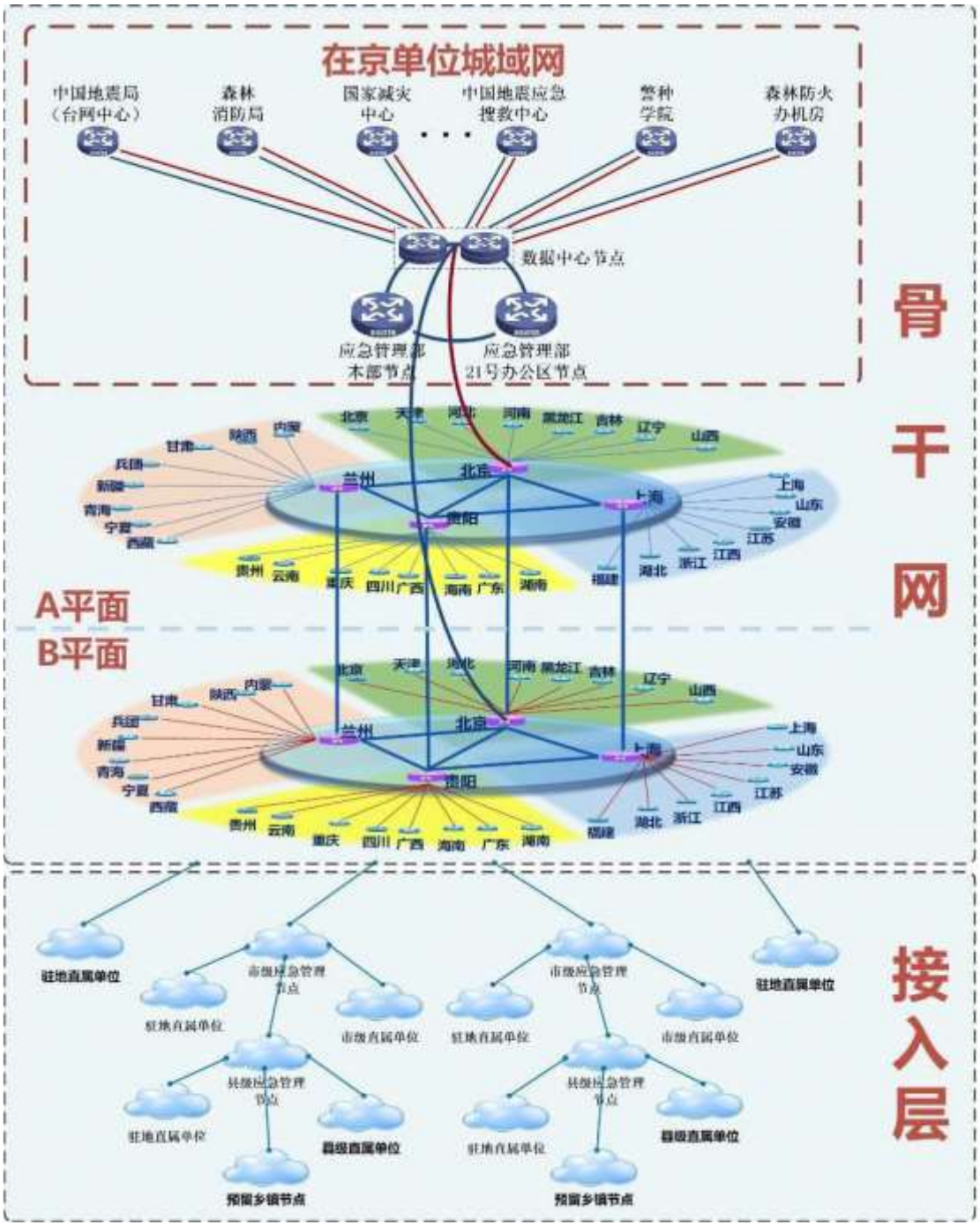
3.2. 网络部署及安全体系现状

3.2.1. 应急通信网络发展现状

应急通信网络由指挥信息网、卫星通信网和无线通信网、国家电子政务外网、国家电子政务内网和互联网组成。指挥信息网承载应急决策、指挥调度、协同会商、态势分析等核心业务系统；国家电子政务外网承载政务办公、风险监测预警等应用；国家电子政务内网用于承载和处理涉密信息；互联网面向社会公众提供信息发布和政务服务。应急通信网络在充分整合消防救援、地震、森林消防、煤监等单位存量通信网络资源基础上，依托国家天地一体化信息网络工程，实现“全面融合、全程贯通、随遇接入、按需服务”，为应急救援指挥提供统一高效的通信保障。

3.2.1.1. 指挥信息网

指挥信息网作为应急通信网络的主体和核心，是承载应急救援指挥等关键业务和传输大容量信息数据的地面有线通道。指挥信息网按照信息安全等级保护三级要求设计，属于非涉密网络，由核心层、汇聚层和接入层组成，应用 IPv6、软件定义网络（SDN）等先进组网技术，覆盖部、省、市、县四级。其中，核心层、汇聚层和在京城域网组成骨干网，与国家电子政务外网、互联网进行安全互联，实现双环骨干、分层汇聚、逐级接入，体现“主备双路、柔韧抗毁、全域覆盖、敏捷高效”的特点。



指挥信息网网络拓扑示意图

核心层网络实现指挥信息网跨区域数据的高速交换和传输，综合考虑数据中心部署、运营商资源、人才资源等因素，选取北京、上海、兰州和贵阳四个城市作为核心层骨干节点组建环状核心网，具备双平面链路冗余能力，链路带宽 1Gbps（支持 10Gbps/40Gbps/100Gbps 平滑升级）。

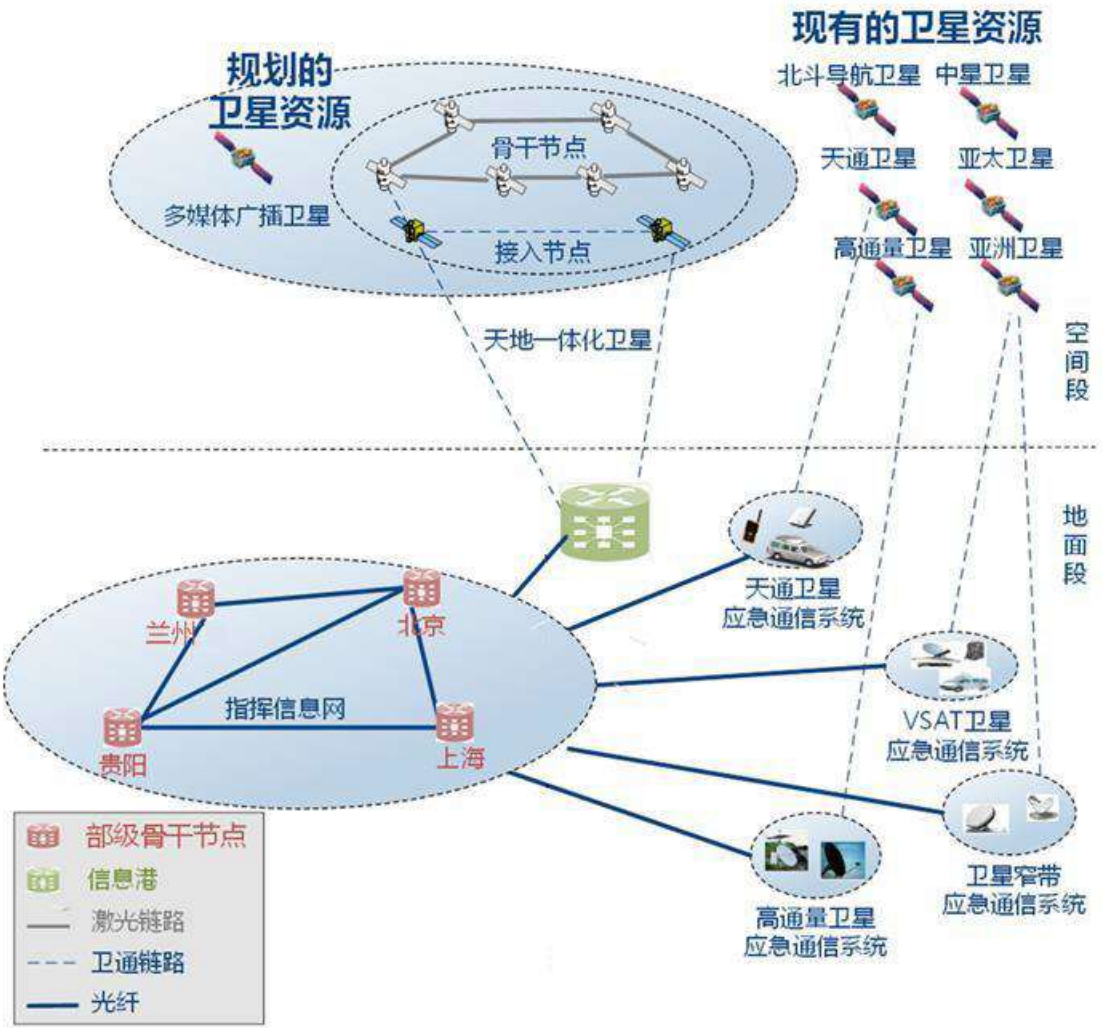
汇聚层网络实现省内数据流量的汇聚和控制转发，全国 32 个省级节点（含新疆建设兵团）通过双链路上连至核心层骨干节点。

接入层网络实现省内各级网络节点逐级接入指挥信息网，覆盖省、市、县各级应急管理部门和直属驻地单位，预留乡镇网络接口。省级应急管理节点部署于省级应急管理部门和消防救援总队，市、县两级应急管理节点部署于所在辖区应急管理部门（消防支队、消防大（中）队）。整合消防救援、地震、森林消防、煤监等单位存量网络资源，按照就近原则，将直属单位就近接入对应层级网络节点。市级和县级节点可采用双链路上联到上级网络节点，所有链路均具备链路保护能力。

3.2.1.2. 卫星通信网

按照自主可控的原则，形成广域覆盖、随遇接入、资源集成的应急管理卫星通信网。网络采用 VSAT、卫星移动通信、高通量等卫星通信技术，利用我国现有卫星资源（各种传统通信卫星、天通卫星、高通量卫星）和未来的卫星资源（天地一体化卫星、移动多媒体广播卫星等），紧密结合天地一体化信息网络工程，支撑应急现场远距离通信保障和扁平化的应急指挥。

卫星通信网由空间段和地面段两部分组成，空间段包括传统通信卫星、天通卫星、高通量卫星及其他卫星，地面段包括 VSAT 卫星应急通信系统地球站、天通卫星应急通信系统终端、卫星窄带应急通信系统远端站、高通量卫星应急通信系统远端站及天地一体化信息网络信息港等各类地球站，体现“广域覆盖、资源集成、随遇接入”的特点。



卫星通信网网络架构图

VSAT 卫星应急通信系统：利用传统通信卫星，实现应急指挥中心与灾害事故现场之间的话音、数据、视频等信息的远程传输。系统能够智能调配卫星资源，实现各类 VSAT 卫星地球站的统一管控，主要由部级中心站、二级主站、远端站（含固定地面站、车载站、便携站、机载站等站型）等部分组成。

高通量卫星应急通信系统：重点实现应急现场高清视频、数据的远程传输，具有便携小巧、高带宽等特点。系统由高通量统一接入服务系统、各类高通量卫星远端站等部分组成。

天通卫星应急通信系统：建设天通卫星应急通信系统，使用“国家应急通信专用号段”，实现灾害事故现场第一时间的情况上报。系统支持话音、短信和低速数据传输，具有覆盖范围广、便于携带、与公网无缝衔接等特点，主要由天通统一接入服务系统、各类天通终端等部分组成。

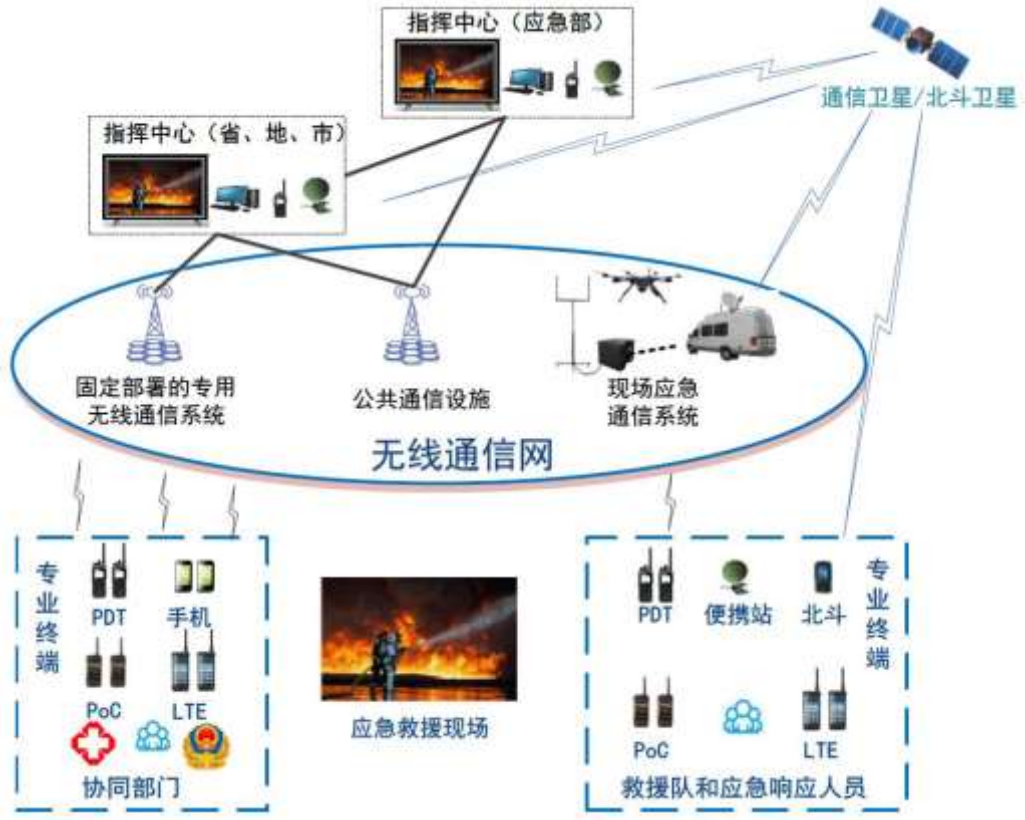
卫星窄带应急通信系统：利用卫星窄带通信，实现公网无法覆盖区域的环境数

据采集、预警信息发布、状态监控等信息的传输，由卫星窄带统一接入服务系统、各类无人值守卫星远端站等部分组成。

天地一体化信息网络：开展天地一体化信息网络工程示范应用，向抢险救灾机构、指挥人员提供全天时、全天候、高精度的信息支援。

3.2.1.3. 无线通信网

无线通信网作为应急通信网络的重要组成部分，采用“公专互补、宽窄融合、固移结合”的多维组网形态，充分利用 PDT 数字集群、LTE 宽带专网、Mesh 自组网、卫星定位等多种技术手段，解决不同应用场景下语音、图像、视频、数据的高速传输和时间校对、位置服务等各类需求，助力各级部门开展指挥调度、日常办公、监督执法等业务工作，为应急响应中的救援队伍、联动部门、社会公众和国际救援与协作提供应急通信服务，确保协同救援和日常移动通信中全地域、全过程、全天候的通信保障。无线通信网主要由固定部署的专用无线通信系统、基于公共通信设施的无线通信系统、时空统一服务系统、现场应急通信系统和专业无线通信终端五部分组成，体现“多制式融合、多部门协同、多形态共用”的特点。



无线通信网网络架构图

3.2.2. 福建省电子政务云平台现状

福建省已完成电子政务云平台基础建设。福建省电子政务云平台分为政务外网和政务信息网，具体情况如下：

3.2.2.1. 政务外网

根据业务类型的不同，将整个政务外网区域划分为公用网络区、互联网接入区、专用网络区以及云平台管理区，每个区域的具体业务划分如下：

一、公用网络区

主要面向政务外网公用网络区的应用，包括面向协作式电子政务应用平台的核心基础服务模块。

二、互联网接入区

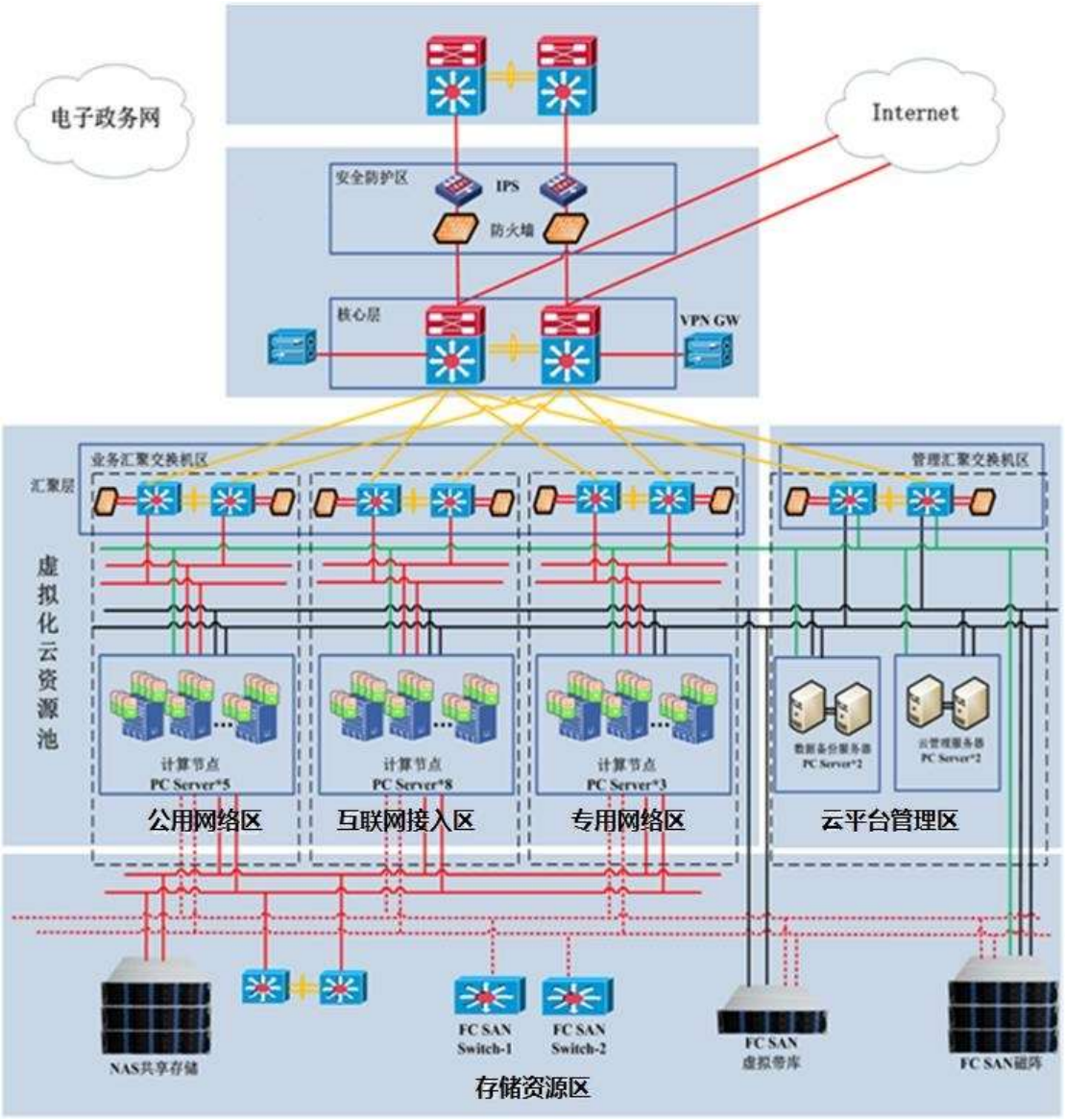
主要面向互联网用户提供公共服务的平台。

三、专用网络区

主要面向各专业厅局提供服务器的托管服务，各专业厅局相关的专业应用托管在该区域。如政协、税务、财务、环保等托管的业务。

四、云平台管理区

管理云平台中的网络设备、计算资源和存储等设备。



政务外网电子政务云平台拓扑图

网络分为两个层次，核心层和汇聚层（接入控制层）。核心层通过防火墙和 IPS 防护设备之后与省经济信息中心机房连接。

核心层采用双机部署方式，即在马尾机房部署两台核心交换机，向上通过千兆链路连接到防火墙及 IPS 安全设备之后，最终连接至省经济信息中心机房 IDC 网络，向下通过万兆链路分别连接汇聚层（接入控制层）四个区域（公共网络区、互联网接入区、专用网络区以及云平台管理区）。

汇聚层（接入控制层）四个区域均采用 2 台三层汇聚交换机和 2 台防火墙安全设备，并通过万兆链路双归属上联到核心层交换机。

除了核心层和汇聚层之外，在安全防护区部署安全防护设备，如上图所示，即在马尾机房的安全防护区部署两台 IPS 和两台防火墙以及带宽管理设备，安全防护

区向上通过两对独立的裸光纤与省经济信息中心实现互联互通，实现马尾云平台利用现有省经济信息中心的互联网、政务外网骨干网出口，向下通过千兆链路与核心层交换机连接。

3.2.2.2. 政务信息网

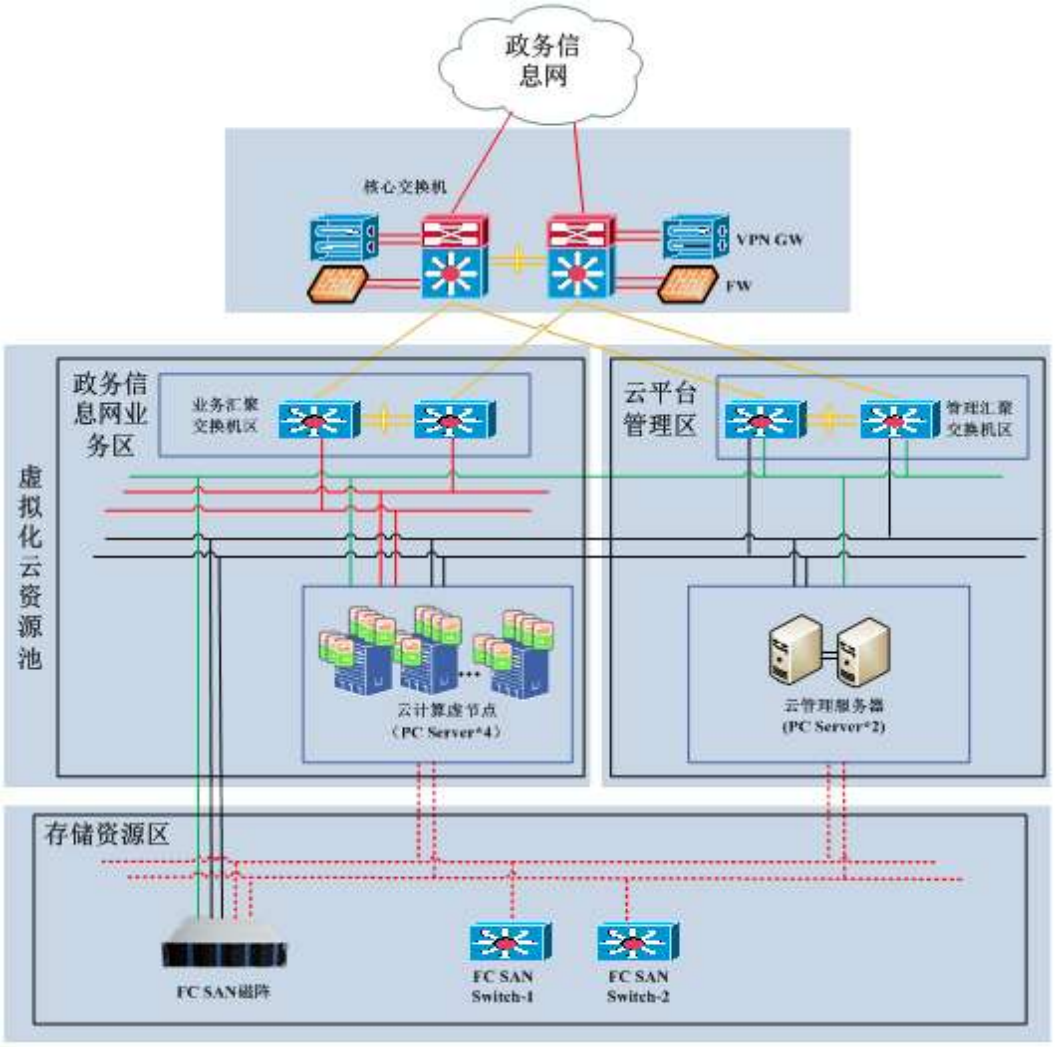
根据业务类型的不同，将整个政务信息网区域划分为政务信息网业务区以及云平台管理区，每个区域的具体业务划分如下：

一、政务信息网业务区

主要载面向政务信息网的应用，包括政务信息网网站、办公自动化应用等。

二、云平台管理区

主要管理政务信息网中的网络设备、计算资源和存储等设备。

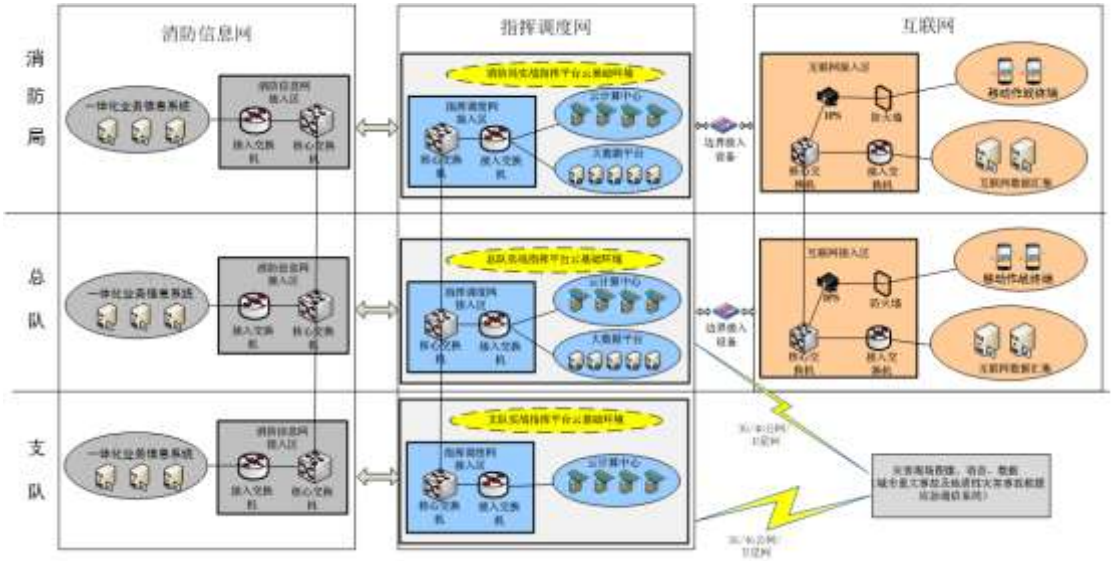


政务信息网电子政务云平台拓扑图

3.2.3. 网络安全体系现状分析

3.2.3.1. 网络现状

福建省消防救援总队现有的消防信息网、消防指挥调度网、互联网三张网络之间物理隔离。原消防信息网隶属于公安信息网，自 2018 年消防系统从公安体系划到应急管理局，根据应急管理部《信息化建设战略规划（2018-2022 年）》文件要求，全国各级应急管理部门和相关转隶单位要采用分级接入方式，按照属地原则就近接入国家电子政务外网，并依托政务外网开展政务办公。



实战指挥平台网络架构图

应急管理部消防救援局、总队、支队各级实战指挥平台均部署于指挥调度网，横向与互联网通过安全边界实现数据共享与交换。

指挥调度网内，各级数据中心通过部署的云计算中心和大数据平台承载的实战指挥平台相关业务应用，实现平台三级纵向联网应用，指令上下贯通，数据汇聚共享；城市重大事故及地质性灾害事故救援现场的图像、语音和数据通过 3G/4G/卫星等无线通信网络，汇聚到总队、支队指挥调度网，并逐级向上汇聚到应急管理部消防救援局实战指挥平台。

消防信息网内，各级现有的一体化业务信息系统按照统一数据汇聚接口，实现基础数据向实战指挥平台的逐级汇聚。

互联网内，应急管理部消防救援局、总队两级通过部署实战指挥平台涉消舆情、

预警信息对接访问、视讯通等互联网服务，向总、支队移动作战终端和专职队、微型消防站终端提供对接服务，互联网采集的数据资源以及物联网终端采集的数据通过安全边界进入实战指挥平台云计算中心和大数据平台。

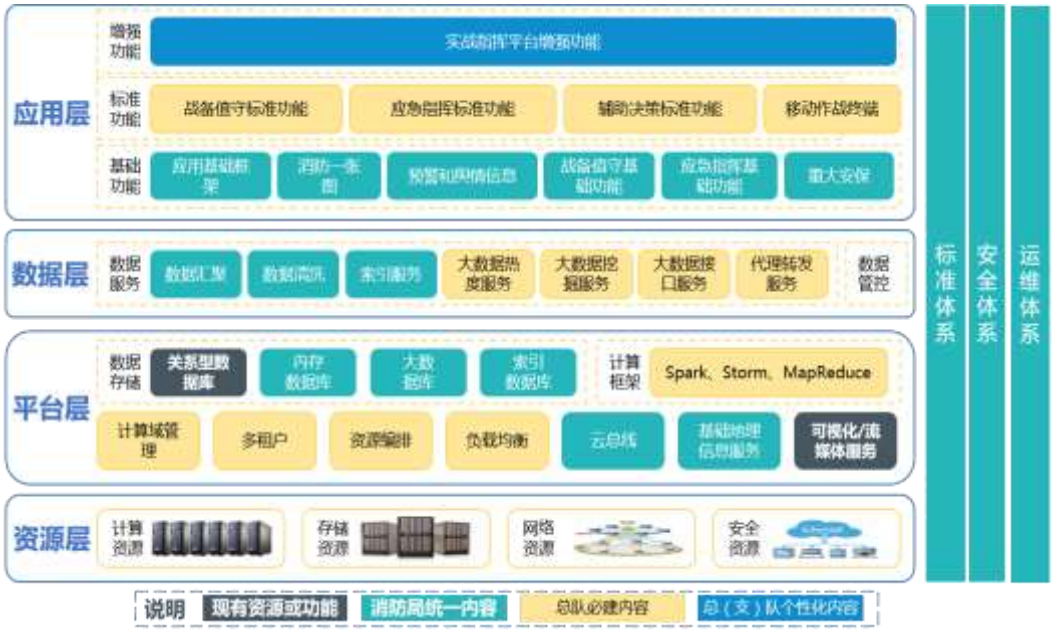
3.2.3.2. 业务现状

为构建新一代全方位、立体化的信息化实战指挥支撑体系，以云计算和大数据技术为支撑，以一体化业务信息系统、各地自建业务系统、社会采集信息、联动信息、城市重大事故及地质性灾害事故救援应急通信系统（以下简称两大应急通信系统）等为基础和数据来源，建设基于“大数据、一张图、一键式、可视化”的实战指挥平台。

实战指挥平台在应急管理部消防救援局、总队、支队三级部署（直辖市总队所辖支队可使用总队平台），支撑应急管理部消防救援局、总队、支队、大队、消防救援站、救援现场五级应用。

为兼顾地域特点和个性需求，各总队实战指挥平台建设包含两部分，即统一要求建设内容和各总队自行建设内容。在实战指挥平台建设过程中，各总队必须统筹本总队所属各支队的实战指挥平台规划和建设，统一建设要求和技术标准。

实战指挥平台系统架构如图所示。



实战指挥平台系统架构图

实战指挥平台架构包括分为资源层、平台层、数据层和应用层四个横向组成部分，以及标准、安全、运维三个纵向支撑体系，其中应用层即实战指挥平台软件，资源层、平台层、数据层为应用层提供基础支撑。按照模块化云服务设计，对各层级中的组成部分划分为现有资源或功能、应急管理部消防救援局统一内容、总队必建内容和总（支）队个性化内容四种类型。其中：

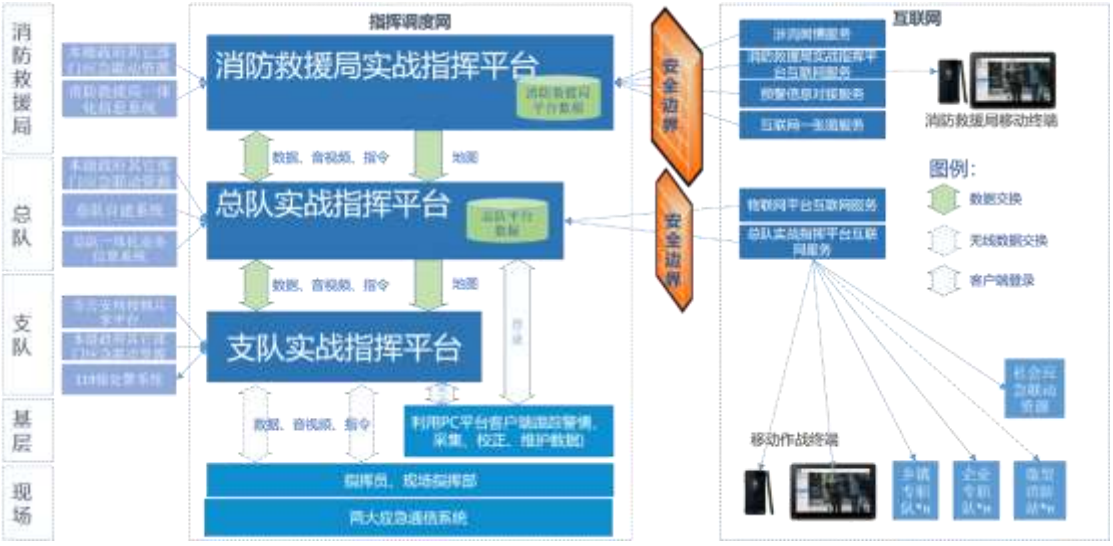
- 现有资源或功能泛指各级已有的计算资源、业务系统和数据等，可根据本次建设内容进行升级或扩展；
- 应急管理部消防救援局统一内容特指为保证三级数据和指令的贯通，而必须统一的服务或软件组件，包括基础地理信息服务、Docker 基础镜像、本地地图缓冲、云总线、内存数据库、索引数据库等内容以及应用层的基础功能部分，这些组件由应急管理部消防救援局向各总队、支队免费提供。
- 总队必建内容特指应急管理部消防救援局统一规划必须建设，但由各总（支）队自行组织实施的实战指挥平台建设内容（或基础软硬件支撑环境）；
- 总（支）队个性化内容泛指在应急管理部消防救援局统一规划的必建内容之外，由各地根据本地特点规划并自行组织建设的其它个性化业务功能。

3.3. 省消防救援总队应用系统现状

3.3.1. 实战指挥系统架构设计

3.3.1.1. 业务架构

消防实战指挥系统业务架构如图所示：



消防实战指挥系统业务架构图

根据各级消防指挥中心实体化运行要求，通过实战指挥系统，为各级指挥员提供作战指挥的多角度、全方位信息支撑，提升各级指挥中心战备值守、应急指挥、重大安保和辅助决策能力。

福建省消防救援总队实战指挥系统与消防救援局实战指挥系统级联，从消防救援局实战指挥系统获取消防救援局统一对接的自然资源部、工业和信息化部、气象局、水利部、地震局、林业局、国家减灾中心等国家级相关部门的各类灾害预警及其他作战所需的辅助信息等应急联动资源。福建省消防救援总队、支队在此基础上，结合本地实际和需求，对接本级相关部门，获取其他必要的预警及作战辅助信息等应急联动资源。

福建省消防救援总队实战指挥系统和本级一体化业务信息系统、自建系统对接，获取相关信息。一体化业务信息系统和实战指挥系统目前采用直接与数据库对接的方式，下一步根据工作需要，一体化业务信息系统所在的网络将统一规划，但与实战指挥系统的对接方式保持不变。福建省消防救援总队自建系统，采用云总线消息服务的方式向实战指挥系统进行数据汇聚。

福建省消防救援总队所辖支队的实战指挥系统接收来自接处警系统的警情信息、灾害事故现场的语音、图像和数据等信息，通过移动作战终端和城市重大事故及地质性灾害事故救援应急通信系统回传至现场指挥部，供现场指挥员指挥决策。各级指挥中心可通过实战指挥系统查看灾害事故现场的语音、图像和数据，掌握现场态势，指导现场进行救援和指挥。现场指挥部接收到的灾害事故现场语音、图像和数据也可回传至后方指挥中心，供指挥中心指挥决策使用。上级指挥中心可通过实战

指挥系统，向下级指挥中心和现场指挥部发送各类作战指令与数据信息。

实战指挥系统汇聚各类应急联动资源、社会联动资源、一体化业务信息系统数据、自建业务系统数据、物联网采集数据等信息，并根据应急救援实战指挥需要，开展各类信息资源的深度整合和综合应用。

3.3.1.2. 业务框架图

消防实战指挥系统业务框架如图所示

消防实战指挥系统业务框架图

福建省消防救援总队消防实战指挥系统在应急管理部消防救援局实战指挥系统基础框架下进行规划设计，系统技术架构遵循云架构设计体系。分为基础资源层、支撑服务层、应用层。

基础资源层包括了作战指挥中心、中心机房等基础环境；路由器、交换机、防火墙等网络及安全资源；以及提供资源池化、应用管理、服务管理、安全管理、数据治理等的消防云系统支撑环境。

支撑服务层提供包括一体化业务数据库、基础库、外部交换数据库、主题库、

全文库等各类数据库支撑；以及一张图、图像语音综合服务。

消防实战指挥系统应用层分为三类：

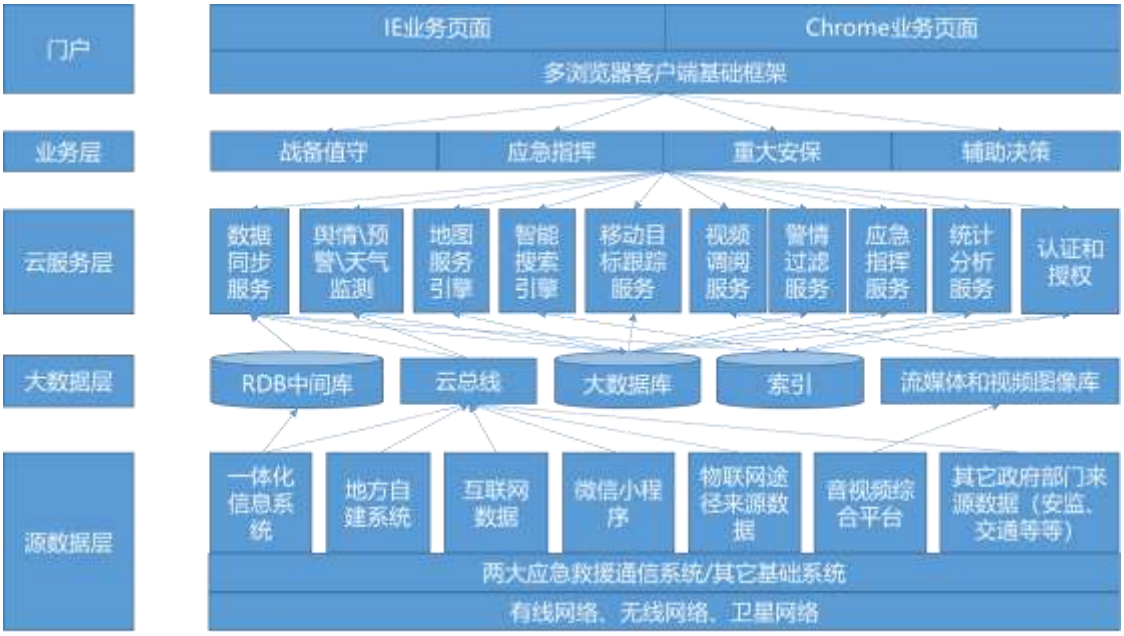
基本功能应用包括：基础框架、一张图基础功能、战备值守基础功能、应急指挥基础功能、重大安保基础功能、案例库基础功能以及消防视讯通；

标准功能应用包括：一张图标准功能、战备值守标准功能、应急指挥标准功能、重大安保标准功能、辅助决策标准功能、案例库标准功能、移动作战终端；

增强功能应用包括：战备值守增强功能、应急指挥增强功能、应急准备。

3.3.1.3. 应用层次架构图

消防实战指挥系统应用层次架构图如图所示



消防实战指挥系统应用层次架构图

整个系统分为源数据层、大数据层、云服务层、业务层以及应用门户。

数据层：主要是消防系统的各类数据来源，包括：一体化信息系统、地方自建系统、互联网数据、音视频数据、物联网数据以及其他政府部门数据等；

大数据层：主要完成各类数据的汇聚、清洗，并对外提供标准的数据服务；

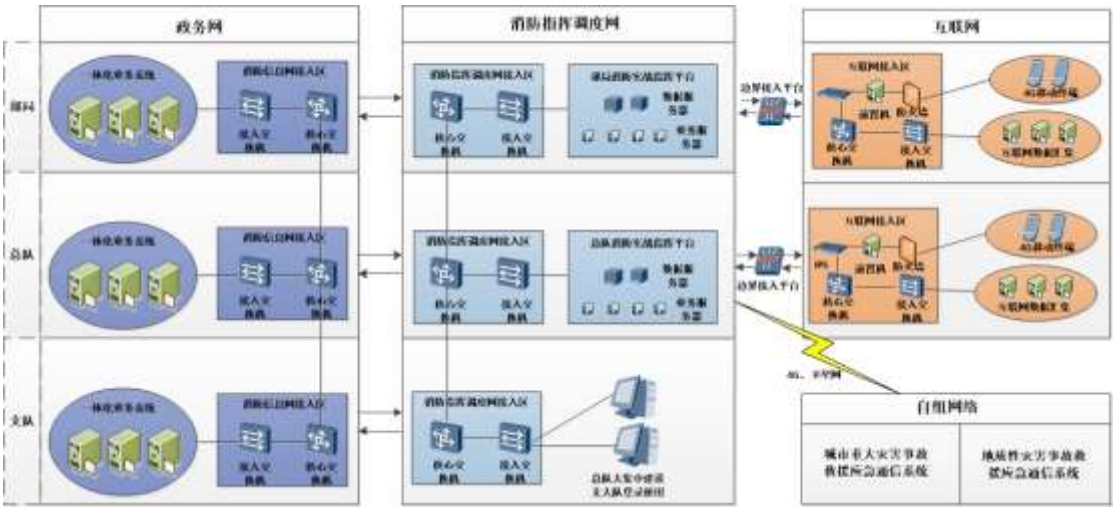
云服务层：主要提供各类基础服务，包括：数据同步、地图服务、智能搜索服务、移动目标跟踪、视频调阅、警情过滤、应急指挥等等服务；

业务层：分为战备值守、应急指挥、重大安保、辅助决策四大业务模块；

门户：可提供 Chrome 等业务页面供用户进行使用；

3.3.1.4. 网络架构

消防实战指挥系统网络架构如图所示



消防实战指挥系统网络架构图

本次建设的福建省消防救援总队、支队实战指挥系统均部署于指挥调度网，横向与互联网通过安全边界实现数据共享与交换。

指挥调度网内，福建省消防救援总队数据中心通过部署的云计算中心和大数据系统承载福建省消防救援总队实战指挥系统相关业务应用，实现应急管理部消防救援局、总队、支队系统二级系统纵向联网应用，指令上下贯通，数据汇聚共享；城市重大事故及地质性灾害事故救援现场的图像、语音和数据通过 3G/4G/卫星等无线通信网络，汇聚到福建省消防救援总队、支队指挥调度网，并逐级向上汇聚到消防救援局实战指挥系统。

福建省消防救援总队正在实施公安网的剥离，后续一体化业务系统等各类办公系统将部署在政务外网，政务外网的数据将通过统一的数据汇聚接口，实现基础数据向福建省消防救援总队实战指挥系统的汇聚。

互联网内，福建省消防救援总队通过部署实战指挥系统涉消舆情、预警信息对接访问、视讯通等互联网服务，向总、支队移动作战终端和专职队、微型消防站终端提供对接服务，互联网采集的数据资源以及物联网终端采集的数据通过安全边界接入实战指挥系统云计算中心和大数据系统。

3.3.2. 省消防救援总队建设现状

福建省消防救援总队信息化建设在应急管理部消防救援局的统一领导下，通过“十一五”“十二五”两个五年专项建设，信息化基础网络和硬件设施不断完善，完成了一体化综合业务系统、119 接处警、信息化综合集成、GPS 车辆定位、通信指挥中心等信息化项目建设，消防信息化应用已覆盖消防工作主要领域，改变了执法监督手段、指挥决策模式、社会服务方式和队伍管理机制，在火灾防控、灭火救援和队伍管理等方面取得了显著成效。

随着社会高速发展，消防救援队伍面临的任务更加艰巨，迫切需要信息化提供更有力的支撑。但现有消防信息化项目建设不能完全满足消防业务工作和队伍管理的需要，存在资源整合不足、数据质量不高、缺乏大数据分析、缺乏实战指挥数据支撑等问题。

实战指挥系统是2016年应急管理部消防救援局党委结合指挥中心升级改造和部领导“关于指挥中心要实体化、实战化运行”的总要求，提出的重点建设项目。要求在系统设计上紧扣实战需求，充分运用云计算、大数据、一张图、物联网、人工智能等先进技术理念，满足新时代要求下的各级消防作战指挥需要。2017 年实战指挥系统被列为全面推进“智慧消防”建设五大项目之一，总体目标是通过建设实战指挥系统，实现灭火救援的一张图指挥、一张图调度、一张图分析、一张图决策，提升消防队伍灭火救援科学化、智能化水平。

3.3.3. 一体化消防业务信息系统现状

开展消防实战指挥系统建设，是支撑消防队伍适应体制改革和职能转变、推动形成“大应急”条件下作战指挥新模式的重要手段，也是推动新形势新任务下的作战指挥由“传统经验”向“科学智能”转变的一项基础性工程。

在这之前，应急管理部消防救援局为了满足消防抢险救灾中高效调度指挥的需求，确保消防执勤保卫任务圆满完成，集多种功能业务于一体，建设一体化消防业务信息系统。同时，充分运用云计算、大数据、物联网、移动互联网等先进技术，实现灭火救援的一张图指挥、一张图调度、一张图分析、一张图决策，为各级消防队伍，特别是各级指挥员应急救援指挥提供多种形式的信息支持和辅助决策。

建设系统如下：

1．执勤实力管理系统：应急管理部消防救援局内部对消防车辆、执勤人员、消防装备等信息进行录入、管理、维护。

2．消防监督系统：将社会隐患排查系统采集到的火灾隐患数据统一管理，并按行业、区域等进行多维度统计与分析，依据分析结果形成科学的巡查计划。

3．涉消舆情信息管理系统： 基于互联网，对涉及灭火、抢险救援事故处置、社会救助等舆情，实施不间断的监控，满足应急管理部消防救援局对涉消舆情信息的搜索、关注、分析等需要。

4．OSM 系统：建立社会单位的单位基本情况、消防安全管理制度及职责、机构及人员、建筑及消防设施、消防工作记录等五大类消防安全基础档案信息库，提供社会单位用户进行消防安全管理人员、消防设施维护保养、消防安全自我评估等三项消防安全报告备案。

5．装备系统：对消防装备进行智能管理和动态监测，使分管领导、消防装备管理部门、库管员等各级人员能从不同的视角实时掌握消防装备的分布情况、动用情况，数质量情况等，

6．灭火救援系统：在灭火救援过程中，对救援力量调派，以及灾情周边消防栓、消防水鹤、自然水源、消防码头、消防水池等周边资源快速分配，以及灭火救援火灾风险单位智能关联。

7．信息值报系统：提供《每日消防信息》信息，供应急管理部消防救援局领导参阅，便于上级领导快速了解基层消防队伍情况、统揽全局、科学决策。

3.3.4. 属地政府应急联动系统现状

福建消防救援总队与工业和信息化部及地方相关部门联动对接，重特大事故灾害发生后获取应急通信保障队伍联动信息。

联动福建省气象局公共气象服务和省预警信息发布中心，获取灾害事故区域的温度、湿度、风向、风速等信息及变化趋势，以及重大灾害性天气、台风、暴雨、暴雪等极端自然天气情况和范围情况。

联动减灾中心，获取灾害事故区域的卫星遥感影像信息和受灾区域核心指标的快速评估等辅助决策信息。

联动福建省地震局对接，获取地震震源及余震分布、烈度分布等地震监测信息和地震影响范围及人员伤亡预评估等辅助信息；与国家防汛抗旱指挥部对接，获取汛情监测与预测等信息；与森林防火指挥部对接，获取森林火灾地点、范围等信息。

3.3.5. 互联网舆情监控系统现状

福建消防救援总队互联网舆情监控系统主要是展示各种舆情，从海量的互联网信息中搜索并过滤出“消防救援”及“应急救援”相关的信息，及时通报重大、敏感舆情，起到舆情第一时间发现的目的。

系统主要是通过 PC 端的网页、微信、企业微信、手机 APP 展示与各单位相关的舆情信息、统计数据，也可按用户需求定制展示信息，同时也是部局、总队、支队级舆情工作台，可对信息和数据进行管理，并输出所需的舆情报告。此外还提供舆情应急处置功能，如舆情上报、舆情分析、文件传输、个人管理功能，为处置决策提供数据参考和数据支撑。

3.3.6. 消防救援局实战指挥系统现状

3.3.6.1. 一期建设内容

1．战备值守：根据指挥中心开展日常值守工作的实际需要，系统可显示各消防机构值班排班信息、领导批示、重点关注、灾情预警、涉消舆情、要事提示、待办事项、值班文件，并根据现有一体化消防业务信息系统中的当前重大灾情数据进行统计分析，并以统计图、趋势图、地图等形式展现统计结果：

◆ 值班动态：局机关、各消防救援总队机关、各消防支队机关值班排班；

◆ 领导批示：中央、应急管理部消防救援局领导作出的批示、指示；

◆ 灾情预警：国家气象、地震、国土资源、卫生防疫、农业等部门发布的与消防救援相关灾害、疫情预警信息；

◆ 涉消舆情：与消防监督执法、火险隐患整改、火灾原因认定、火灾损失赔偿、队伍管理、车辆违章违规、指战员作风纪律、清正廉洁、以及火灾救援的相关涉消舆情；

◆ 要事提示：重要事件的提示，包括：局领导参加的党委会议、专项会议等提示；

◆ 待办事项：应急管理部消防救援局领导同志交办重要事项，需要持续关注的火灾、灾害事故等；

◆ 值班文件：应急管理部消防救援局、局指挥中心制定印发的与战备值班管理相关的制度、规定、机制。

◆ 警情地图：综合展示全年、当月、昨日、当日各级消防机构的警情分布情况及 24 小时警情趋势

◆ 重大安保：为方便领导全面掌握专项行动的安保部署、消防安保工作动态等信息，系统可显示专项行动安保部署、安保动态、安保要事、社会联动、重点提示、增援力量和实战演练功能。重大安保模块提供如下功能：

◆ 安保部署：可查看安保 24 小时警情数据、社会面火灾防控数据、涉会场所及预案、安保动态和各指挥部、指挥所联系方式；

◆ 重大安保力量部署：地图实时展示涉会场所、安保力量部署、涉会场所周边火灾风险单位；

◆ 安保动态：展示安保活动的动态情况；

◆ 现场指挥部：展示所有重大安保现场指挥部的相关信息；

◆ 安保活动重点节点：可按时间轴方式直观展示安保活动重要节点。

2．应急指挥：以实战指挥为牵引，突出作战指挥和数据查询两个功能模块，做到一旦发生灾害事故，可实现“灾情信息、力量调度、作战指挥、社会联动等信息自动上传系统和实时可查；火灾风险单位信息、重大危险源、地震带、超高层建筑、大型综合体等基础信息实时可查”。灾情处置过程中，可通过应急管理部消防救援局实战指挥系统查看灾情位置、周边情况、力量调派部署情况、灾情处置情况，跟踪灭火救援作战指挥过程，根据不同火灾类型查阅相关信息，分析评估灾情，作出指挥决策，与现场指挥部通信，下达作战命令等。应急指挥模块提供如下功能：

◆ 灾情位置定位：通过从接处警系统获取的当前灾情报警人手机、固定电话、位置等信息，在实战指挥系统的地图上定位灾情位置，同时支持在实战指挥系统上进行二次定位。

◆ 周边信息查询：指挥员通过应急管理部消防救援局实战指挥系统能够查阅处置对象及周边信息，其内容包括单位概况、建筑情况、主要危险性等信息和其周边的水源、执勤实力、装备药剂、道路等信息。

◆ 灾情处置情况：查阅灾情处置情况，其内容包括查看灾情的燃烧物质信息、燃烧面积信息、火势控制情况、人员被困和伤亡、着火部位平面图、周边力量情况、现场图像、现场决策等实时处置情况。

◆ 力量部署情况：应急管理部消防救援局实战指挥系统可实时显示消防车和消防人员的位置，并可进行实时视频、实时通话；

◆ 联动信息：根据灾情属地及类型自动生成应急联动单位、联勤保障单位以及各级消防专家信息

◆ 工具：提供作战地图标绘、泡沫计算、危化品查询等一系列工具

◆ 可通过应急管理部消防救援局实战指挥系统查阅处置对象及周边详细信息，如地震带分布、高层建筑、石油化工、核电站分布、泡沫厂家、火灾风险单位等信息。

3．辅助决策：以消防队伍的基础数据、业务数据和数据仓库为基础，以辅助决策需要为牵引，从多种维度数据进行关联分析和挖掘，通过直观的图表展现数据之间的关系、发展趋势和规律，为首长决策提供辅助支撑。

◆ 重点对象统计：对高层建筑、地下建筑、大型综合体、石油化工、核电站、油气管线、水库水电站、地震带八大重点资源进行深度的数据统计分析

◆ 消防监督：对各消防机构的监督检查情况、执法动态情况进行统计分析

◆ 战备实力统计：从多个维度（人员、特种装备、车辆药剂等等）对各级消防机构的战备实力进行统计分析。

3.3.6.2. 二期建设内容

3.3.6.2.1. 基础框架建设

为保证应急管理部消防救援局、总队、支队二级实战指挥系统上下数据指令贯通和联网运行，构建全国实战指挥系统的基础框架，统一建设基础服务和软件组件，各总队、支队通过搭建应急管理部消防救援局统一提供的实战指挥系统基础框架软件，标准部署服务以及标准数据对接服务，同时完成二级联网运行调试，实现数据逐级汇聚，指令上下贯通，跨省调度指挥。

3.3.6.2.2. 地图云服务系统建设

建设统一地图云服务系统为全国实战指挥系统提供一张图服务，应急管理部消防救援局在指挥调度网部署统一的基础地理信息服务以及全国的地图数据，各总队、支队在本地部署统一的基础地理信息服务以及地图缓冲服务，按需对本级所需的地图数据进行缓存和更新，为本级实战指挥系统提供基础地理信息服务。

3.3.6.2.3. 应急指挥

通过与两大应急通信系统、应急管理部辅助决策指挥信息系统的对接，集成移动终端、应急通信装备等，增强应急指挥功能。基于大比例尺电子地图，以灾害事件为中心，实现基础业务信息、车辆位置、人员定位和图传设备等资源的上图展示与互动，指挥调度层级延伸到灾情现场，及时获取现场灾情的多媒体信息，并下达指令，用“一张图”完成从灾情感知到智能研判再到救援调度的整个救灾流程，实现一张图调度、一张图指挥、一张图研判和一张图决策。

3.3.6.2.4. 应急通信装备管理

研发应急通信装备管理模块，嵌入实战指挥系统，实现对无人机、单兵图传、卫星便携站等重要通信装备的实时状态、位置、使用情况等信息的统一采集、监控管理和“一张图”展示。提供无人机、单兵图传、卫星便携站等重要通信装备的录入维护管理。可按照应急管理部消防救援局、总队、支队分级进行管理，也可对图像、语音、数据采集、传输设备进行分类管理，并可实现设备按照类型、完好度、使用情况等不同方式进行统计分析；通过与两大应急通信系统对接，可实现对灾害现场所有应急通信设备上线状态进行采集汇聚，能够按照灾害现场、前方指挥部、后方指挥中心通信节点部署位置，分别对单兵、图像传输设备、数据传输等不同类型的设备进行区分展示，并实时显示监控设备状态；通过与两大应急通信系统对接，可实现对灾害现场所有应急通信设备地理位置的汇聚，并能在实战过程中实时展示，通过框选操作，可实现对选定区域通信设备的数量、类型、状态的快速统计，并以列表方式显示；在地图上，点击某一图像采集设备可显示采集的图像信息，并能对

具有云台控制功能的设备进行拖动和局部缩放操作；可以对单兵佩戴的空呼器、生命体征信息数据采集设备发出单体/群体告警撤离指令（如空呼压力过低、心跳数据异常等），并显示出定位设备的应答状态。

3.3.6.2.5. 数据监测

通过可视化的方式监控系统数据来源以及数据质量情况，以便用户快速掌握数据资源汇聚情况，定期汇总通报源头数据质量情况和数据贡献度，以便有针对性地开展数据治理工作。根据《实战指挥系统建设技术指导意见》中的数据项要求，制定数据核查规则，对每个数据表的字段建立数据检测项，展示数据质量检测结果，并定期汇总通报源头数据质量情况；对实战指挥系统汇聚的各种数据，系统对数据被调用的情况进行统计，了解不同数据的使用频度，协助了解各部分数据对实战指挥的价值；提供灾情定位使用情况的统计页面。可通过该页面查看各总队、支队对灾情进行二次定位以及三次定位的修正情况。统计页面应能够按照机构和灾情进行定位统计，应急管理部消防救援局以此作为对各总队、支队实战指挥系统使用的一项考核指标。

3.3.6.2.6. 移动指挥应用

通过建设移动指挥应用，总队领导可通过移动作战终端以多种方式参加作战、与火场指挥员之间可通过移动作战终端进行文字、语音沟通；对于有坐标位置的灾情，指挥员、参战员均可通过移动作战终端调用高德地图、百度地图等第三方 APP 进行灾情的路线导航；总队领导可在作战终端上设定车辆集结地、物资集结地、特种装备集结地，并可扩展其他集结地；指挥员通过移动作战终端可实时接收系统推送的灾情信息；查看处置对象的基础信息、远程感知预案、各类相关图纸集合等内容；查看周边的水源（500 米、1000 米消防水源、5000 米天然水源）、重要保卫目标等；查阅力量调度情况，包括到场力量和途中力量，并可按照不同方式进行展示；查阅系统推送的相关社会联动单位信息和专家的联系方式，可实现联动单位的检索和专家库的智能匹配；快速进行所需灭火药剂数据量的计算工具、查看各类危化品的理化性质和处置方式等信息。

3.3.7. 图像综合管理系统现状

福建消防救援总队、支队通过指挥调度网接入视频专网的视频共享系统，获取视频点位相关信息，以华平图像综合管理系统，汇聚了包括指挥视频、营区监控（通讯室、车库）、布控球、4G 单兵图传、卫星通信等视频资源，指挥中心通过图像综合管理系统组会进行视频会商和手动调阅灾害现场视频画面，第一时间了解作战队伍的出动情况和现场的救援情况，及时进行资源调动、为前方救援人员和后方指挥部领导的命令上传下达，提供了有力保障。

3.3.8. 北斗定位导航系统现状

福建消防救援总队利用安装车辆定位功能的装备，及时接入北斗导航定位系统，采集注册的消防车辆定位信息，掌握消防车辆实时行车轨迹。

3.3.9. 119 接处警系统现状

福建消防救援总队全省目前都已按三台合一方式进行 119 接处警，其模式目前有以下四种情况：

1．三方通话，消防主接：福州、泉州。

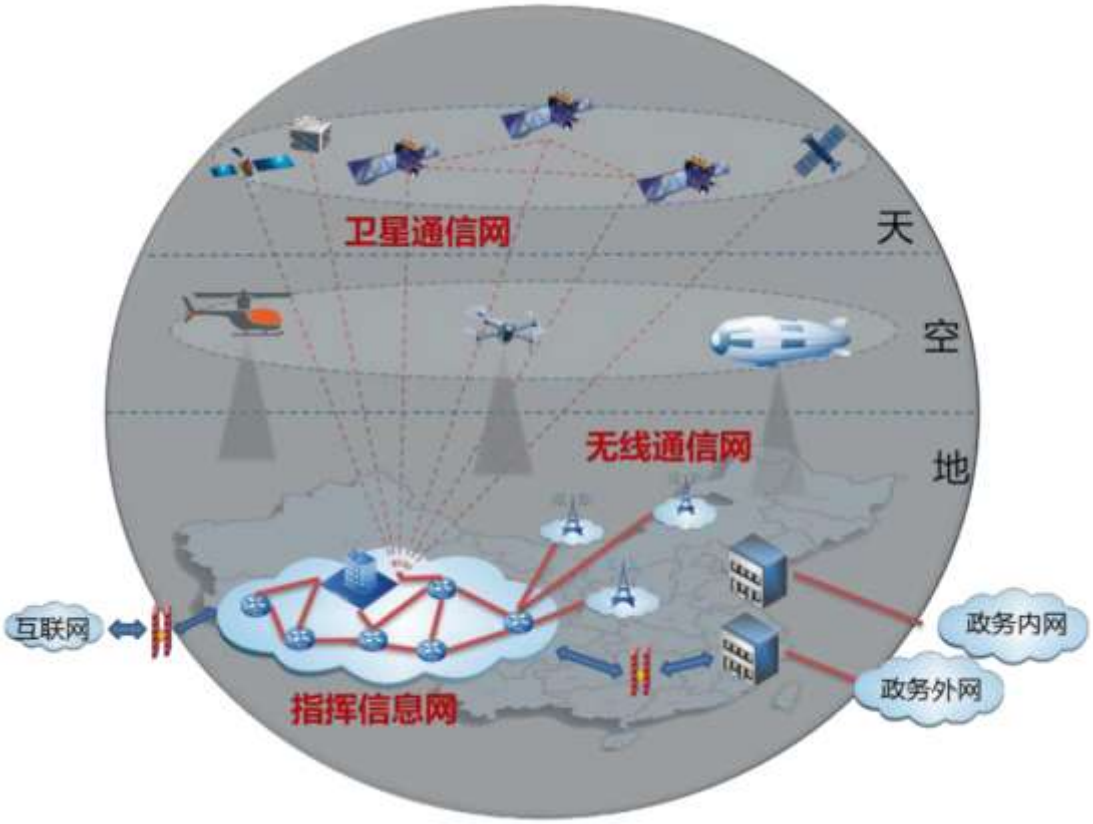
2．同步振铃，消防主接：厦门、漳州、龙岩、宁德。

3．同步振铃，公安主接：莆田、三明、南平。

4．平潭支队未建设指挥中心，直接采用公安的接处警系统。

3.3.10. 应急消防网络建设现状

消防通信网络由指挥信息网、卫星通信网和无线通信网、国家电子政务外网、国家电子政务内网和互联网组成。指挥信息网承载应急决策、指挥调度、协同会商、态势分析等核心业务系统；国家电子政务外网承载政务办公、风险监测预警等应用；国家电子政务内网用于承载和处理涉密信息；互联网面向社会公众提供信息发布和政务服务。应急通信网络在充分整合消防救援、地震、森林消防、煤监等单位存量通信网络资源基础上，依托国家天地一体化信息网络工程，实现“全面融合、全程贯通、随遇接入、按需服务”，为应急救援指挥提供统一高效的通信保障。



应急通信网络示意图

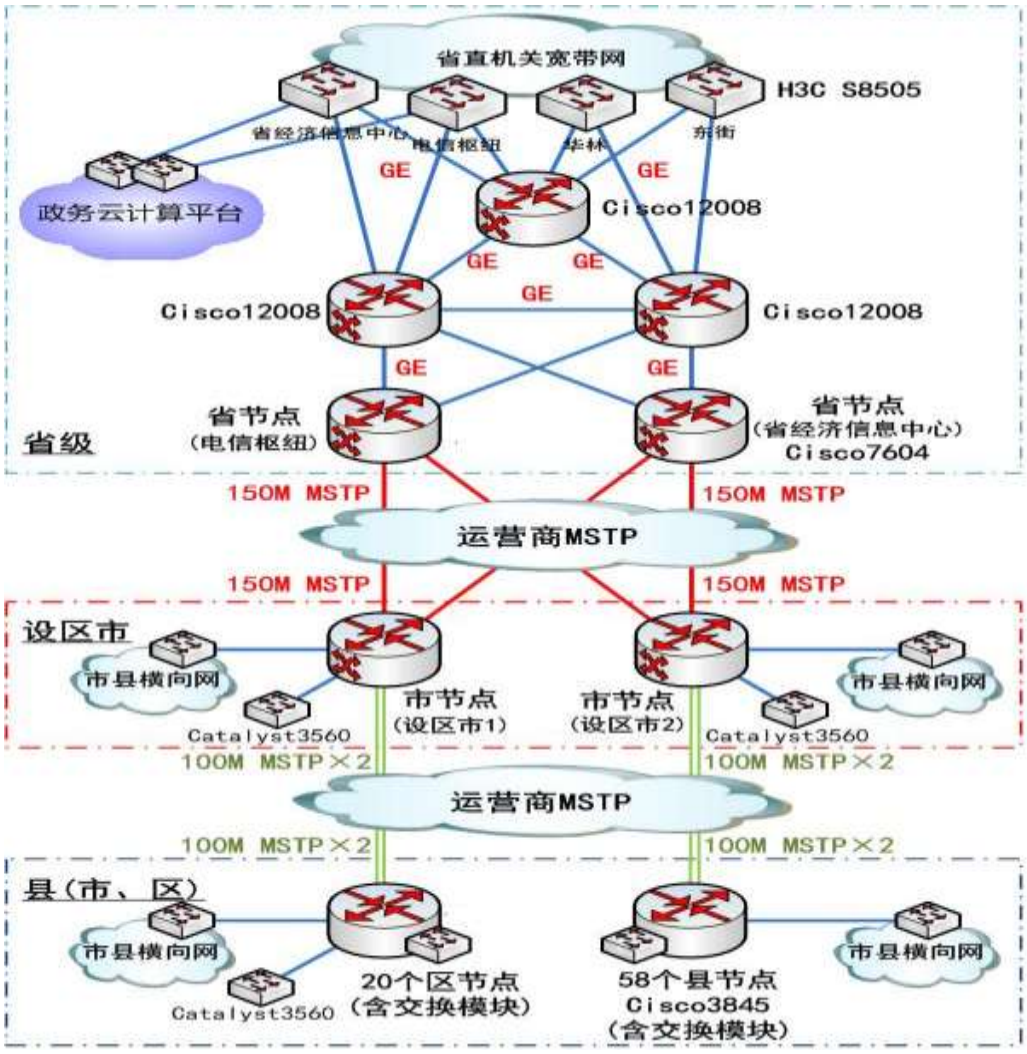
3.4. 福建省信息化公共基础平台建设情况

3.4.1. 福建省政务信息网

福建省政务信息网分为省直机关宽带网、市县纵向网和市县横向接入网三大部分。福建省政务信息网络工程由省直机关各单位接入点 200 多个组成省直机关宽带网，全区 9 个设区市、平潭综合实验区以及所属的 83 个县（市、区）接入点组成市县纵向网，9 个设区市、平潭综合实验区和所辖县（市、区）的各单位约 6000 多个节点组成市县横向接入网。

省政务信息网在省、市、县三级已建成以大城域网（省直机关宽带网、市县横向接入网），省直机关宽带网由核心层、汇聚层、接入层组成，核心层与汇聚层采用半网状结构，接入层采用星型结构。设区市横向接入网、县（市、区）横向接入网一般由核心层、接入层组成，采用星型结构。省政务网由省、9 个设区市、平潭综合

实验区、83 个县（市、区）的核心设备构成 P/PE，共有 3 个 P，105 个 PE，构成 MPLSVPN 网络骨干。省政务网 MPLSVPN 网已于 2007 年建成。福建省政务网信息网络拓扑结构如下图所示：



福建省政务信息网网络拓扑图

3.4.2. 福建省电子政务外网

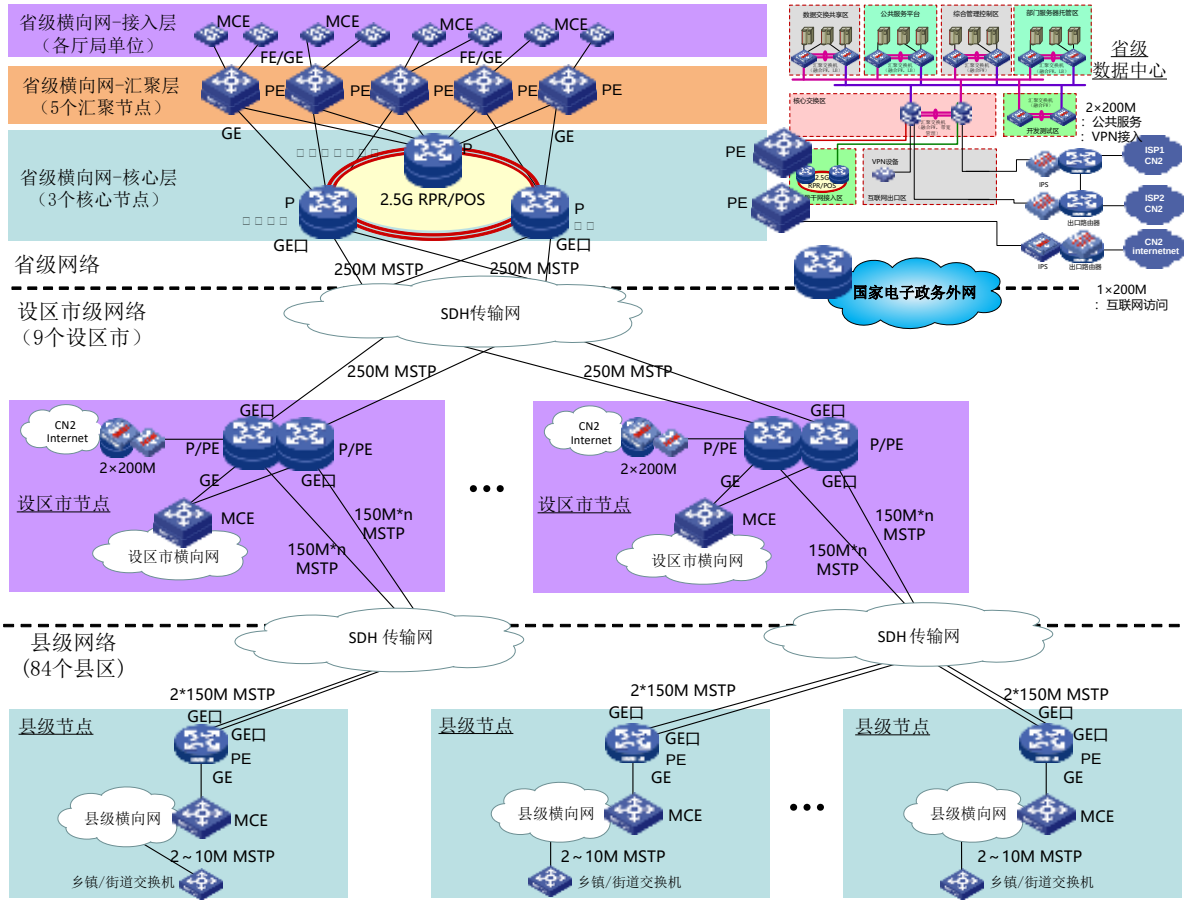
电子政务外网是政府的业务专网，支持 MPLSVPN，主要用于政务部门面向社会的专业性服务和运行政务部门不需要在政务网上运行的业务，实现网络业务承载和政务信息服务，支持数据、语音、视频业务，并实现网络管理和运行服务支撑。政务外网与政务网物理隔离，与互联网逻辑隔离，为政府部门的业务系统提供网络、信息、安全等支撑服务，为社会公众提供政务信息服务。我省电子政务外网的覆盖范围主要包括省级横向网、省－市－县三级纵向网、市县横向网、乡镇和行政村（社

区）互联网 VPN 接入系统。

省－市－县三级纵向网在省级配置 3 台核心路由器形成 2.5GRPR/POS 的核心网，每个设区市配置 2 台路由器，采用 2 条 250MMSTP 线路上联省级节点，每个县（区）配置 1 台路由器，采用 2 条 150MMSTP 线路上联设区市节点。

在省、设区市外网主干节点的互联网出口部署 VPN 网关设备及接入认证设备，行政村通过互联网 VPN 接入政务外网。

MPLSVPN 技术能满足政府业务模型，可在整个网络平台划分多个纵向专网给各个部门使用，各单位用户能访问本部门纵向网络的相应资源。同时，各单位用户经授权能访问横向网络资源，即其它专网的资源。



福建省政务外网网络平台 MPLSVPN 拓扑图

2010 年 9 月 30 日，我省政务外网已完成省－市－县三级纵向骨干网、省级横向网、省级数据中心一期工程的建设，政务外网节点已覆盖全省所有市县和乡镇一级区域，已具备了在我省外网平台上大规模部署政务及公共服务应用的条件。

3.4.3. 福建省电子政务云平台

福建省电子政务云平台建设政务信息网、政务外网两个电子政务云平台，为用户提供包括云计算、云存储、网络、安全、服务器托管、物理机服务在内的各类资源服务，满足未来 3~5 年省直部门数据中心整合对包括服务器、存储、系统软件在内等基础架构服务的需求。

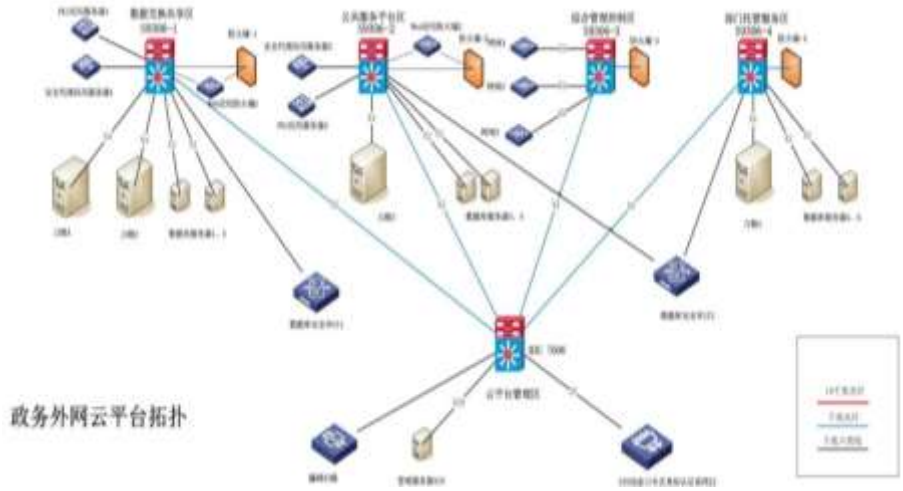
电子政务云平台是建设政务外网统一的电子政务应用平台、统一的基础架构支撑平台，为省直各部门提供基础架构服务、应用平台服务和应用软件服务，实现统一建设、统一维护，统一技术支撑、统一安全保障，推进政务信息化应用整合和信息共享。

电子政务云平台的基础设施服务层(IaaS)，包括硬件基础设施子层、虚拟化与资源池化子层、资源调度与管理自动化子层。

（1）硬件基础设施子层：包括主机、存储、网络及其他硬件在内的硬件设备；

（2）虚拟化与资源池化层：通过虚拟化技术进行整合，形成一个对外提供对资源的池化管理（包括网络池、服务器池、存储池等），同时通过云管理平台，对外提供运行环境等基础服务；

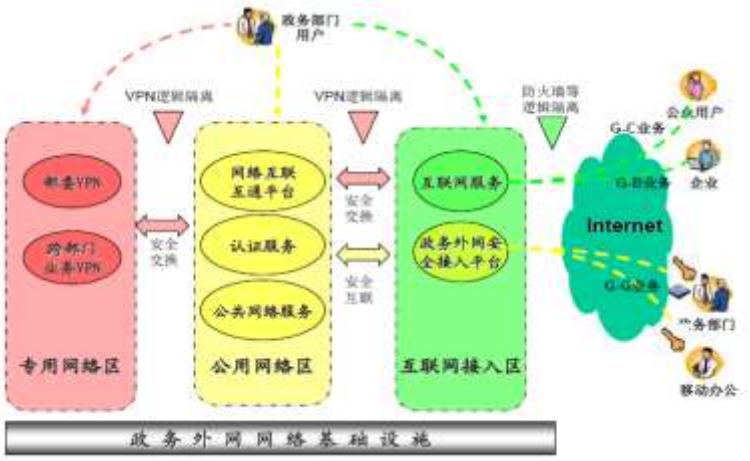
（3）资源调度与管理自动化子层：在对资源（物理资源和虚拟资源）进行有效监控、管理的基础上，并且通过对服务模型的抽取，提供弹性计算、负载均衡、动态迁移、按需供给、自动化部署等功能。



政务外网云平台拓扑图

3.4.4. 政务外网业务网络模型

根据政务外网所承载的业务和系统服务类型的不同，在逻辑上将政务外网划分为公用网络区(Global)、专用网络区(MPLSVPN)和互联网接入区(InternetVPN)三个功能域，分别提供政务外网互联互通业务、专用 VPN 业务和互联网业务。如下图所示：



政务外网业务网络模型

公用网络区：即采用国家政务外网公用地址(即从 CNNIC 注册的地址)的网络区域，是国家政务外网的主干道，实现各部门、各地区互联互通，为跨地区、跨部门的业务应用提供支撑平台；国家政务外网公用网络区仅路由国家政务外网公用地址。

专用网络区：是依托国家政务外网基础设施，为有特定需求的部门或业务设置的 VPN 网络区域，实现不同部门或不同业务之间的相互隔离，VPN 网络区域主要为少数部门的特定业务数据传输提供安全通道。国家政务外网采用 VPN 技术将特定业务数据与其他数据安全隔离，用于满足部门特殊需求。该区域主要采用私有地址，在骨干网上采取标签方式进行交换。

互联网接入区：是各级政务部门通过逻辑隔离手段安全接入互联网的网络区域，满足各级政务部门利用互联网的需要。在互联网接入区，采取了综合的安全防护措施，对互联网接入业务提供安全防护。中央和地方按照统一的安全策略，分级接入互联网，中央政务外网为中央部门单位提供互联网业务服务，采用 BGP 协议连接互联网服务提供商。各地政务外网自行出口，采取 NAT 技术，通过静态路由连接本地互联网。

功能域相互之间安全隔离，公用网络区用于实现各部门、各地区互联互通，专

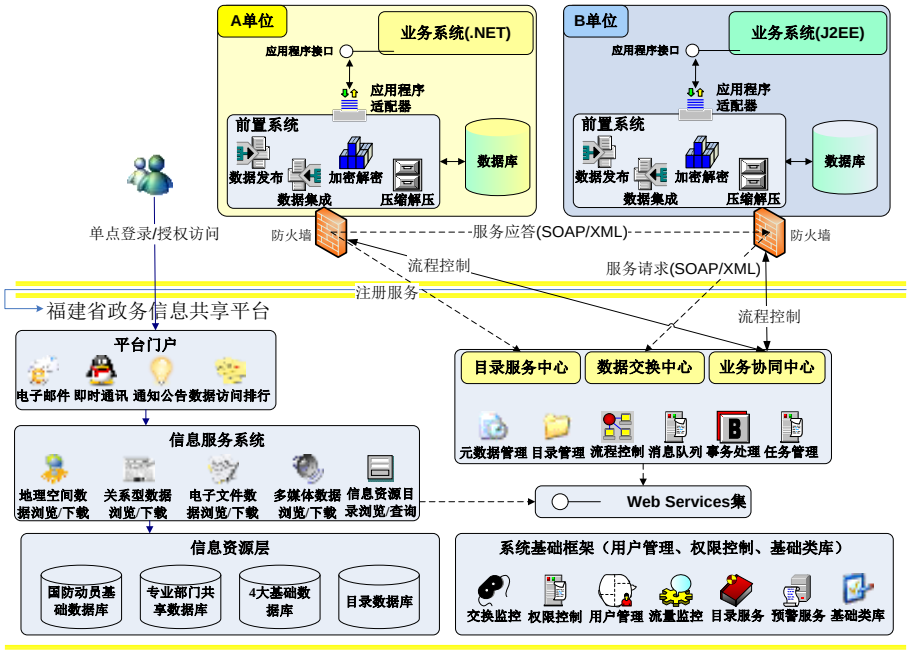
用网络区用于实现不同部门或不同业务之间的 MPLSVPN 相互隔离，互联网接入区用于实现各级政务部门通过逻辑隔离手段安全接入互联网，提供面向社会的公共服务和互联网访问。

政务外网通过构建互联网安全接入平台，实现各级政务部门移动办公的公务人员利用互联网通道，通过数字证书认证和密码技术，安全接入政务外网，访问指定的业务应用系统。

3.4.5. 福建省政务信息共享平台

福建省政务信息共享平台是架构于信息网络、信息资源、信息安全等基础设施之上的信息资源共享服务平台。它为“数字福建”政务信息资源的目录服务、数据交换、信息共享、业务协同和应用集成提供统一的底层构架和解决方案。

福建省政务信息共享平台系统架构如下图所示：



福建省政务信息共享平台系统架构

共享平台采用交换中心－前置系统的分布式软件架构，交换中心部署在固定节点，主要负责用户管理、权限控制、整合工作流控制、日志管理、性能监控等中心控制功能；前置系统部署在各部门的接入节点，主要负责部门共享数据库的抽取发布、下载另一节点的共享数据库、以及和参与业务协同的业务系统进行交互等功能。

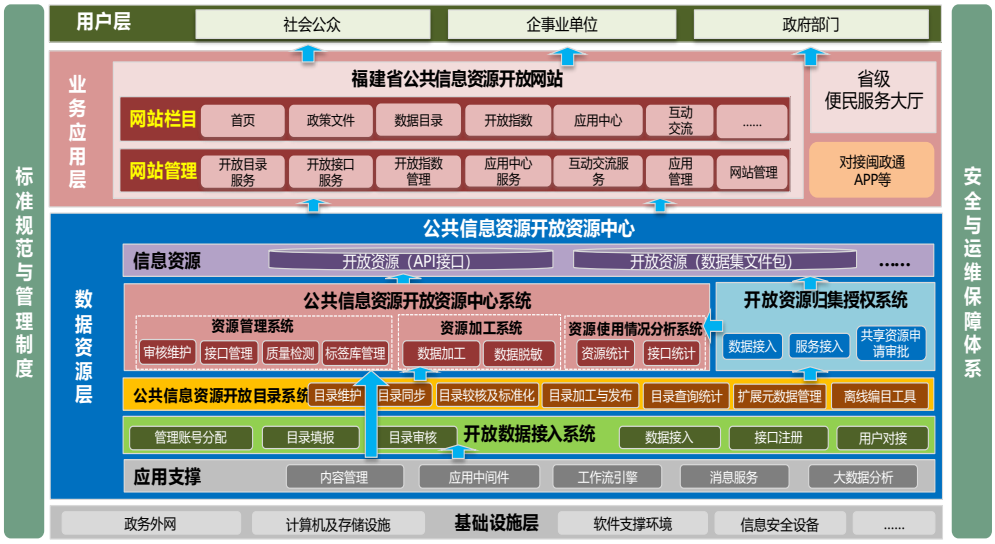
福建省政务信息共享平台系统结构包括中心系统及前置系统。中心系统包括单

点登录与统一授权管理、消息中心、信息服务、整合工作流等子系统；前置系统包括数据抽取、数据集成和应用程序适配器三个子系统。

3.4.6. 福建省公共信息资源统一开放平台

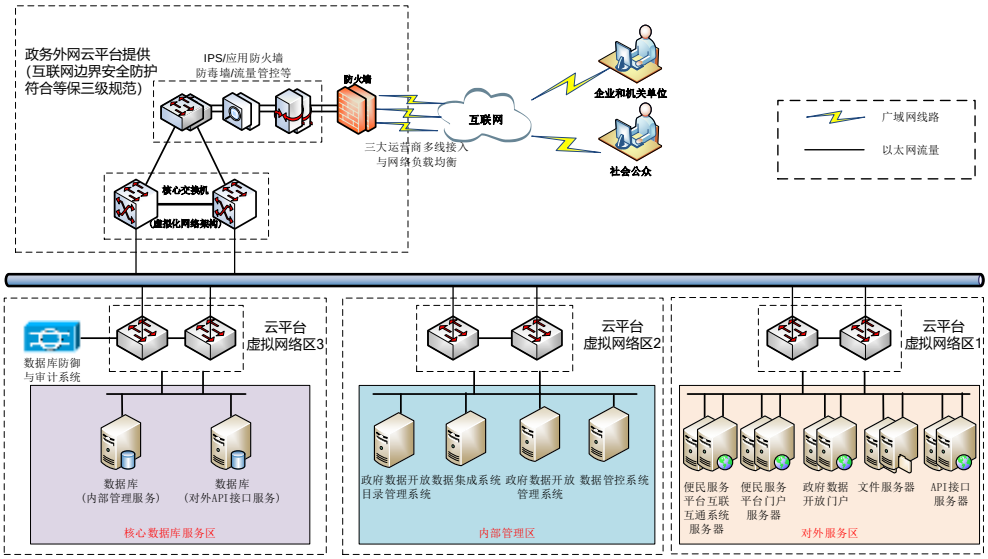
福建省公共信息资源统一开放平台依托省政务外网云平台，与福建省人民政府门户网站实现前端整合，与福建省政府数据整合汇聚共享平台衔接，并基于省级和各设区市政府数据汇聚共享平台的资源进行建设。通过“梳理、集成、处理、开放、开发”，打造“覆盖全省，统筹利用，统一开放”的公共信息资源开放统一平台。

3.4.6.1.1. 平台架构



福建省公共信息资源统一开放平台架构

3.4.6.1.2. 网络拓扑图



福建省公共信息资源统一开放平台网络拓扑结构图

3.5. 密码应用现状与需求

3.5.1. 密码应用现状分析

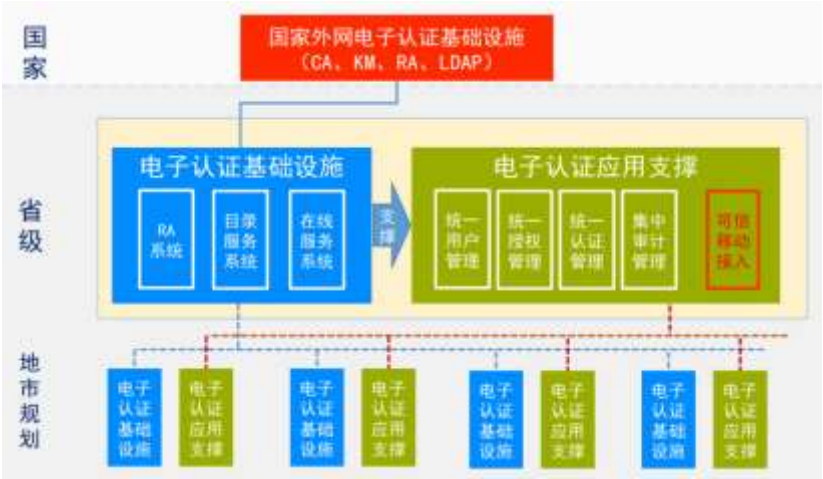
福建省电子政务认证服务平台项目由省经济信息中心负责建设、管理，并对接国家政务外网管理中心，省数字办、省密码管理局负责管理和监督。平台为国家电子政务外网数字证书中心（国家政务外网 CA）的福建省级 RA，采用符合国密算法的 SM2 双证书，平台统一为政务信息网、省电子政务外网和数字福建无线政务专网等用户提供政务数字证书服务。平台支持的数字证书类型：机构（单位）证书、个人证书、设备（服务器）证书，支持的数字证书介质：USBKey、SIMKey、SDKey、设备文件证书。

3.5.1.1. 信任体系

全国电子政务外网证书信任体系如下图所示，采用三级架构，分布式部署，集中式数据汇总。

全国电子政务外网证书信任体系架构图

3.5.1.2. 认证服务平台总体架构



福建省电子政务认证服务平台总体架构图

3.5.1.3. 电子认证基础设施（RA 中心）

电子认证基础设施（RA 中心）包含 RA 系统、密码机、目录服务系统和证书在线服务系统。RA 提供数字证书生命周期管理包括：证书注册/下载、证书更新、证书注销、证书冻结/解冻、证书归档。

证书在线服务系统提供证书用户的在线更新和延期。

3.5.2. 合规性需求

福建省智慧消防云平台安全等级定级为第三级。按照等保三级的要求，密码合规性需求主要包含以下几点：

（1）国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度，被保护对象的安全防护要求和涉密程度，被保护对象被破坏后的危害程度以及密码使用部门的性质等，确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的，应当遵照《信息安全等级保护密码管理办法》《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。

（2）信息系统安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。

（3）信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的，应报经国家密码管理局审批，密码的设计、实施、使用、运行维护和日常管理等，应当按照国家密码管理有关规定和相关标准执行；采用密码对不涉及国家秘密的信息和信息系统进行保护的，须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准，其密码的配备使用情况应当向国家密码管理机构备案。

（4）运用密码技术对信息系统进行系统等级保护建设和整改的，必须采用经国家密码管理部门批准使用或者准予销售的密码产品进行安全保护，不得采用国外引进或者擅自研制的密码产品；未经批准不得采用含有加密功能的进口信息技术产品。

（5）信息系统中的密码及密码设备的测评工作由国家密码管理局认可的测评机构承担，其他任何部门、单位和个人不得对密码进行评测和监控。

（6）各级密码管理部门可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评，对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中，发现存在安全隐患或者违反密码管理相关规定或者未达到密码相关标准要求的，应当按照国家密码管理的相关规定进行处置。

3.5.3. 密码应用需求

3.5.3.1. 物理安全需求

信息系统安全等级保护第三级，物理安全基本技术要求在电子门禁系统方面需

要用到密码技术。相关的密码技术的应用需求点归纳如下：

1．重要区域进入人员身份的真实性

2．电子门禁系统记录的完整性

3.5.3.2. 网络安全需求

信息系统安全等级保护第三级网络安全基本技术要求在安全访问路径、访问控制和身份鉴别方面需要用到密码技术。相关的密码技术的应用需求点归纳如下：

1．安全访问路径中通信主体身份的真实性

2．安全访问路径中数据的机密性

3．安全访问路径中数据的完整性

4．网络边界和系统资源访问控制信息的完整性

5．审计记录的完整性

6．网络设备用户身份的真实性

7．传输过程中鉴别信息的机密性

3.5.3.3. 主机安全需求

信息系统安全等级保护第三级，主机安全基本技术要求在身份鉴别、访问控制、审计记录和程序安全方面需要用到密码技术。相关的应用需求点归纳如下：

1．操作系统和数据库系统用户身份的真实性

2．传输过程中鉴别信息的机密性

3．系统资源访问控制信息的完整性

4．重要信息资源敏感标记的完整性

5．审计记录的完整性

6．重要程序的完整性

3.5.3.4. 应用安全需求

信息系统安全等级保护第三级应用安全基本技术要求在身份鉴别、访问控制、审计记录和通信安全方面需要用到密码技术。相关密码技术的应用需求点归纳如下：

1．应用系统用户身份的真实性

2．文件、数据库表等客体访问控制信息的完整性

3．重要信息资源敏感标记的完整性

4．审计记录的完整性

5．通信过程中数据的完整性

6．通信双方身份的真实性

7．通信过程中整个报文或会话过程的机密性

8．数据原发行为的抗抵赖

9．数据接收行为的抗抵赖

3.5.3.5. 数据安全及备份恢复

信息系统安全等级保护第三级数据安全及备份恢复基本技术要求在数据传输安全和数据存储安全方面需要用到密码技术。相关的密码技术应用需求点归纳如下

1．传输过程中系统管理数据、鉴别信息和重要业务数据的完整性、机密性

2．存储过程中系统管理数据、鉴别信息和重要业务数据的完整性、机密性

综上所述，密码技术在第三级信息系统中的应用需求归纳如下：

■ 机密性服务

通过加密和解密数据　防止数据的未授权泄露。数据包括存储数据、传输数据和流量信息。

■ 完整性服务

通过检测、通知、记录和恢复数据修改　防止数据的未授权修改。数据修改包括改值/替换、插入、删除/丢失、重复/复制、变序/错位等。

■ 真实性服务

通过标识和鉴别活动主体的身份防止身份的冒用和伪造。

■ 抗抵赖服务

通过提供行为证据防止活动主体否认其行为。证据内容包括行为主体、行为方式、行为内容和行为时间等。

3.6. 存在问题分析

截至目前，福建省消防救援总队已建成较多消防业务应用系统，如上述“省消

防救援总队应用系统”现状中分析可知，主要集中于指挥中心实战指挥平台和应急联动管理平台中。针对消防业务中防火监管管理要素（如基层消防力量、一线受监管的火灾风险单位、消防服务人员、消防器具设施等）暂未形成一套全省性完整统一的、体系化的管理机制。主要存在问题列举如下：

3.6.1. 消防安全监管力度及监管对象安全意识存在问题

全国各级消防主管部门，都将“人防、技防、物防”等要素充分融入消防安全监管工作中，特别是防火监督工作。但随着时代和社会环境的快速发展变化，消防安全监管力量与社会消防安全防范意识，或多或少都存在“掉队”的情况。

1．消防监督执法人员不足

随着社会经济的不断发展，城市化的不断推进和城市规模的不断扩大，消防安全火灾风险单位越来越多，日常监督检查的任务越来越重，再加上每年开展的很多消防安全专项整治以及消防工作的全面开展，消防监督执法工作量极大，而基层大队的消防监督干部普遍只有 5-7 名。全省各级消防的监督执法、消防救援与行业服务等业务工作量也不断攀升，消防人力不足属于全省性、乃至全国性的常态化。由于消防人力资源不足明显警力不足，导致消防监督执法人员长期处于繁重的消防安全日常监督任务之中。但是，通过粗放型的简单堆砌消防人力资源，为整个消防工作带来边际效应已不明显，甚至可能导致机构臃肿、人员繁杂、沟通运行效率低下等负效应。同时，纵观近几年消防监督执法工作、消防应急救援工作、消防服务工作等业务量大、业务繁杂度高、技术性与应急性强、业务逻辑关系错综复杂等业务特点，以及工作内容跟随社会形势的快速发展变化，必须采取高效先进的技术手段来代替人力堆砌，坚持“向科技要警力，以科技促业务”的原则，推进消防工作的高效、高质开展，也减少消防救援过程中不必要的人员伤亡与财产损失。

2．监管火灾风险单位与全省各级消防监管部门信息传递渠道不畅

全省各地市、区县尚未实现各类消防安全在线监测信息在政府层面上服务于全省消防安全监管的共享；各地市、区县消防监管部门和联网火灾风险单位之间缺乏全省性的消防安全信息和关联基础信息的获取渠道；大部分的全省各级消防主管部门对于辖区内火灾风险单位的消防安全情况，由于探查手段的限制，暂时无法实时监测和预警，对于存在的消防隐患无法形成快速、直接的监管与督促机制，缺乏入

口统一、渠道顺畅的应急事件上报途径。

3．部分社会单位及民众消防防范意识淡薄

近几年来，福建省消防救援总队以及各地市消防支队、县区消防大队，各地消安委、火灾隐患协防机构等，利用传统媒体和移动互联网时代的新媒体，在社会消防安全宣传、教育、培训等方面常年持续不断投入力量和加大宣传力度，并取得了不错的宣传效果和安全宣传社会影响力，极大提高了社会民众在生产、生活中的消防安全意识。但考虑到社会民众数量、社会机构数量、社会产业数量等基数较大，仍有少部分的社会单位及社会民众的消防安全防范意识较弱。消防安全无小事，即便为“少部分”，在缺乏消防安全意识的前提下，仍可能存在巨大的消防安全隐患和带来巨大生命财产损失。因此，尽可能扫除消防安全教育“死角”，提高和加强民众消防安全防范意识，仍为消防安全宣传与消防事故预防的重中之重，将消防事故扼杀于萌芽阶段。

4．全省消防在线监测能力不够

从源头来看，随着我市经济快速发展、人口持续增长、城镇化率逐步提高，工业、生活和火灾隐患排查意识的淡薄，给消防安全带来了威胁。由于相关人员安全意识、专业检测监管不到位等问题，造成了消防安全的盲点和空白区。目前全省各地市、区县众多联网火灾风险单位中的消防安全监测以人工监测为主，容易造成疏忽、遗漏等问题，应该建立物联网在线监测机制，消除消防安全事故隐患，完善事故应急设施，架设消防安全立体监测网络，加强其在线监测能力。

3.6.2. 全省消防信息化建设及应用现状

全省消防各支队、各大队日常使用原公安部消防局、省总队前期建设的多个消防应用系统（如实战指挥平台、双随机监督执法系统），能够基本满足上级部门的任务指示要求与本级部门的行政职能要求。

但是根据消防监管的“技防”要求（即消防科技信息化建设要求），各级消防主管部门针对本区域、本辖区内的消防安全监管工作的“信息化”辅助业务开展处于不同的发展阶段和水平。

具体消防信息化建设及应用现状如下：

1．各地规划和建设进度及水平参差不齐、建设成果不能全面反映和解决问题

限于经济发展水平与财政状况的不同，全省各地的区域性消防安全监管信息化建设水平参差不齐，部门地区已初步建成消防物联网系统或试点应用，不同地区的建设模式及成果也不尽相同，但大部分地区还处于建设规划中或暂无相关计划。

依照目前全国各地的消防信息化应用系统的研发建设及应用情况来看，其建设成果所解决的问题较为片面，欠缺整体性，并未从根源上或整体上解决消防安全监督管理工作中的“痛点”。

2．技术标准、业务方向不统一，各地重复、无序建设

由于有关智慧消防、消防物联网远程监控系统等的相关国家标准出台较早且未及时更新，无法完全适应时代发展要求，从而无法全面指导全省智慧消防建设。全省智慧消防、消防物联网等信息化应用建设，各地均采用自行财政预算投入和招标的方式进行项目建设，这就存在各地采用技术规范、技术标准不统一的问题。同时，按照各级消防部门对智慧消防的理解不同，也会导致业务方向不一致，随着时间的推移，容易造成一个区域一个样、一盘散沙、各自为战的局面，不利于后续的全省统筹。

同时，各地在没有统一指导、统一规划的前提下争相独立、重复、无序建设，也会造成信息化财政重复投资、效益产出低下，造成公共资源浪费。

3．过度追求新技术，脱离业务搞建设，不接地气

随着互联网信息时代的高速发展，各种新技术不断推出台面，例如 5G 通信、物联网、大数据、AI 人工智能、BI 业务分析、BIM/CIM、区块链、云计算、3D 建模、3D 电子地图、AR/VR 虚拟技术、无人机、仿生机器人等，这些技术创新为各种智慧型业务的设计与开发提供了更广阔的空间，使得原来超前的想法也逐步变成现实。技术虽好，但也不能无度堆砌，有些地区在建设各种智慧消防平台时，往往以高大上的技术亮点作为噱头，以宣传项目的先进性，这其实是在建设智慧城市过程中为了迎合“智慧”而容易陷入的误区，并不是新技术越多越好。新的技术能带来效率的提升、问题的改善，但同时也需要投入更多的人力、物力、财力配套来推动新技术的运用，这就极有可能会造成有限的资源力量捉襟见肘，且开发完成的信息化系统脱离实际业务，接不了地气，最后在消防行政管理工作中给监管对象和监管者自身造成工作负担。

4．数据分散、信息孤岛、对接成本高，不利于数据汇聚整合与共享

目前已有地市、区县消防部门建成智慧消防相关应用系统，其他地市县区也在陆续跟进建设或规划中。按照目前独立建设趋势，未来几年内，全省将形成大大小小近百个区域消防数据中心，由于所采用的技术体系、技术规范不同，开发建设厂商不同等，将会导致数据严重分散，形成大大小小的信息孤岛，对接和汇聚成本高，即时对接完成也会存在数据不完整的情况，无论在横向和纵向上无法形成有效的消防安全监管与救援协同，无利于将来的全省消防大数据中心建设，更不用提进行 AI 人工智能、BI 大数据智能分析研判。

3.7. 需求分析

3.7.1. 具体业务需求（按角色）

福建省消防救援依托应急通信网、政务信息网等，完成了指挥中心信息化建设和后续升级改造，建设了诸多本级和全省性的消防综合应用系统，如实战指挥系统、双随机执法监督系统等，都取得了不错的实战应用效果。

智慧消防平台的建设，要充分体现其智慧性，除了在技术上要提升、要突破、要创新之外，还需要在业务适用范围上进行大范围拓展，将整个社会当前已有的或潜在的消防安全管理、消防技术服务、消防宣传教育、社会消防安全保障等方面需求一同纳入到智慧消防平台中，让智慧消防平台实现社会化、城市化、公众化联合运作，充分发挥智慧消防平台的“联防保障、社会共建”智慧特性。

3.7.1.1. 消防救援总队/支队/大队三级消防监管业务需求

针对消防管理中常见的管理痛点，将“人防、物防、技防”三者结合应用于传统的消防管理和监督中。在督促“单位自主管理”的消防责任落实的基础上，充分利用物联网、视频、大数据等新技术，对消防核心系统的关键信息进行感测、分析、整合、研判，对消防状态做出智能响应；能够基于消防救援“一张图”，查询辖区消防装备、救援力量、救援设施等的分布，接入现场图像，指挥调度、多级联动、作战互通，并做出救援决策分析。

3.7.1.2. 消防管理行业主管部门业务需求

能够通过电脑、手机终端等渠道，实时、快速了解到本辖区范围内的消防责任企业的实时数据（物联网监控数据、企业自主管理信息等）、数据分析结果，为消防监管单位开展消防执法检查提供参考，使执法检查有依据，准确执法、科学调配，并做到执法标准化。

3.7.1.3. 市县消安委及领导业务需求

可以随时通过网站、手机查看各个区域的消防整体责任落实情况，抽查各级监督机构培训执法情况，对本辖区的消防状况保持实时关注。

3.7.1.4. 街道办及派出所业务需求

街道办可以实时查看消防数据，督导责任辖区落实，派出所通过系统数据分析，开展街道层面的执法检查，使执法检查有依据，做到执法标准化。对检查不到位或有重大隐患的企业进行执法检查，并处理，使执法检查有理有据，精确执法，科学化调配警力，做到执法标准化。

3.7.1.5. 消防技术服务机构业务需求

按照国家有关法律法规和国家工程建设消防技术标准，对建筑消防设施实施维护管理，确保建筑消防设施完好有效。对城市消防远程监控系统中的消防设施进行定期检查，记录维修、保养等过程中产生的信息，做好全覆盖辖区所有消防重点安全单位的维保过程管理，做到“底数清、情况明”。基于技术服务单位服务记录数据、防火巡查数据、火灾隐患数据等信息为基础，依据《中国消防行业信用等级评价总体方案》进行综合统计分析，能够对消防技术服务机构完成阶段性的信用评价，促进消防技术服务机构工作水平的提升，落实消防安全责任制。

3.7.1.6. 消防运营单位业务需求

依据 GB/T 26875.3-2011《城市消防远程监控系统》等相关国家标准，对物联网监控布置的相关设备进行日常维护，对消防联网火灾风险单位 24 小时不间断监管服

务，提高消防监督效率，有效落实社会单位自我管理能力。

3.7.1.7. 消防火灾风险单位业务需求

将智慧消防物联网设备所采集的信息及运行状态信息，传输至消防物联网远程监控系统以及单位消防责任人手机上，通过系统或者手机客户端随时随地掌握单位消防设施状况。同时，能够满足本单位消防安全信息网上录入、巡查流程网上管理、检查活动网上监督、整改质量网上考评、安全形势网上研判的需求，完成“单位自主管理”的消防责任落实。

3.7.1.8. 社会机构或社会公众业务需求

消防安全是与社会各界息息相关的安全大事，所有社会机构及公众个人都有权利以各种各样的形式参与到消防安全共建工作当中来。因此，智慧消防云平台的建设，应当为社会机构及公众个人提供消防安全相关的访问入口、诉求入口、学习入口，例如为社会机构及公众个人提供消防隐患的监督上报、投诉举报，提供消防安全知识的网络学习空间，从真正意义上将“智慧消防”打造成“智慧城市”建设的重要一环，而不是将“智慧消防”仅仅定位于消防职能部门、消防服务部门、消防重点监管对象等。

3.7.2. 具体功能需求

3.7.2.1. 消防安全管控功能需求

针对消防管理中常见的管理痛点，结合物联网、大数据等新技术发展，解决传统管理方式的弊端，向科技要效率，实现消防管理工作智能化、可视化、痕迹化。

能够实现传统消防系统联网监控，并将消防电源监控系统、消防水监控系统、消火栓可视化管理、视频监控、设备设施巡查管理、小微场所火灾预警等通过物联网的方式，将消防基础数据信息化，统一汇聚至系统，将“人防、物防、技防”三结合应用于传统的消防管理和监督。

能够对消防核心系统关键信息进行感测、分析、整合，从而对消防监督业务活动的各种需求做出智能响应。

打破各消防监督业务系统之间的信息壁垒，使消防信息资源更有效地实现供需对接，推动消防工作模式从传统向现代、被动向主动、单一向综合、人工向智能的发展。

3.7.2.2. 消防联网火灾风险单位物联接入及自主管理功能需求

通过联网火灾风险单位的接入，将自动火灾报警主机前端感知设备的报警信息及运行状态信息，传输至消防物联网远程监控系统以及单位消防责任人手机上，通过系统或者手机客户端随时随地掌握单位消防设施状况。

此外，将消防用水实时监控、消火栓监控、无线火灾报警监控、消防电源监控等智慧消防物联网设备所采集的信息统一汇聚至消防远程物联网监控系统。

同时，以社会单位责任主体、消防部门依法监督为业务原则，开发了针对性的业务模块，满足消防安全信息网上录入，巡查流程网上管理，检查活动网上监督，整改质量网上考评，安全形势网上研判的需求，完成“单位自主管理”的消防责任落实。

3.7.2.3. 消防关键区域视频接入及管理功能需求

本期及后续规划能够将全省设有消防控制室机构（机关、团体、企事业单位等）的消防控制室、建筑消防通道、安全出口、重点部位、危险区域现场等场所的视频图像统一接入，进行远程调阅、录像回放，并支持与消防相关物联网监控系统进行联动，确保相关消防责任人时刻掌握重点区域的视频情况。

本期设计首先选取 1 个地市作为试点，将接入该市所有火灾风险单位消控室视频接入，实现消控室值班人员在岗情况监控。但系统的接入能力设计，将远远大于本期试点接入数量，在软件架构和硬件资源的冗余设计方面，能满足后期大量监控视频接入需求。

3.7.2.4. 消防大数据可视化综合展示应用功能需求

能够将各类系统的资源和数据进行深度的分析和展示上墙功能，有效呈现消防设施情况、消防管理数据分析、警情分析、隐患分析、天气等，形成以业务为导向的大数据指挥作战图墙，直观地了解消防设施实时信息、消防管理情况以及警情的

及时汇总情况，实现灭火救援的“一张图”指挥、“一张图”调度、“一张图”分析和“一张图”决策，为科学指挥和力量调度提供准确信息参考，为各级监督员、指挥员提供辅助决策支撑，不断提升消防救援部门灭火救援科学化、智能化水平。

3.7.2.5. 消防数据共享服务需求

针对消防物联网监测数据及对其分析研判结果数据、消防日常业务过程数据、消防基础公共数据等，可主动公开或经许可公开的消防数据，对其进行归类和命名定义，并通过开放数据接口形式（包括传参接口和非传参接口），发布为消防领域政务公共信息数据服务，为其他各级政府职能部门、社会公共机构、社会公共平台等提供数据共享服务。

3.7.2.6. 消防教育培训需求

智慧消防平台，为体现其智慧性、社会化和城市化等特点，必须将消防教育提上平台建设需求日程安排中。

消防教育培训主要针对其中几块：

1．消防主管部门自身消防力量培训，包括基础培训、新技术培训（如消防训练VR 产品等）等，可以纳入智慧消防平台的其中一项功能版块，作为全省各级消防主管部门的固定线上培训内容之一。

2．社会服务机构培训。社会消防技术服务机构作为消防监管部门的社会化工作的极大力量补充，需要对其进行规范和长期可持续性的培训，避免社会服务机构及其附属技术服务人员因技术欠缺、意识薄弱，造成无法及时发现消防隐患或因工作疏漏造成更大隐患直至酿成消防火灾事故。

3．社会民众的消防教育培训需求。社会民众作为城市活动的个体和主体，时时刻刻身处各种消防安全因素之中，也时刻影响着消防安全形势走向。因此作为消防安全的被动因素和主动因素，为社会民众提供各种无偿公益或适量有偿的消防安全知识教育培训，是智慧消防平台的主要目标之一。

3.7.3. 系统非功能性需求

3.7.3.1. 系统性能指标

在全省应用和数据集中模式下，充分考虑时间消耗及资源利用状况，以满足不同层次用户的响应能力需求，确保业务高效运行。

在网络稳定的环境下，面向相关监管部门的数据采集和处理、预警生成和处置、在线监测应用、企业服务应用、移动应用等，支持不少于 10000 个用户并发应用业务请求，具体性能要求：

（1）操作界面单一操作的响应时间小于 1 秒；

（2）带有复杂条件的查询响应时间小于 2 秒；

（3）一般查询统计的响应时间小于 3 秒；

（4）1 亿条数据统计分析时间在 5 分钟以内。

3.7.3.2. 系统可靠性要求

1．稳定性

（1）要求系统具有高可靠性和高稳定性。关键设备应采用负荷分担、分布式多处理机结构，主要冗余度至少为 1＋1。

（2）系统各服务器应保证数据实时的一致性、可用性，主备倒用时间＜3 分钟。

（3）系统故障恢复时间＜30 分钟。

（4）设备必须支持热插拔功能。

（5）系统应满足 7×24 小时不间断工作。

2．备份和恢复

（1）存储设备应具有极高的可靠性，有良好的备份和恢复策略。系统数据和业务数据可联机备份、联机恢复，恢复的数据必须保持其完整性和一致性。

（2）应对系统的配置数据、操作日志进行备份，进行永久保存。

（3）在系统失效的情况下，应可从数据记录中恢复最近的数据。

3.7.3.3. 系统扩展性需求

系统应根据系统容量、存储要求、物联网并发量等要求规划和部署服务器。当

系统需要扩容时，可做到灵活扩展，平滑升级。

系统应采用化部署结构，可根据实际需要通过业务的增加来实现系统功能的扩张和扩容，为今后系统的升级、扩建留有余地。

在系统的容量与处理能力等设计时应留有冗余量，可对外提供标准的开放接口，方便扩展其它深度应用。

3.7.3.4. 视频质量需求

1．视频图像质量需求

（1）系统内视音频信息的显示、存储、播放应具有原始完整性，即在色彩还原性、图像轮廓还原性（灰度级）、事件后继性等方面均应与现场场景保持最大相似性（主观评价）。

（2）系统的最终显示图像质量符合 GB50198-94《民用闭路监视电视系统工程技术规范》要求，达到四级（含四级）以上图像质量等级，对于电磁环境特别恶劣的现场，图像质量应不低于三级。

（3）保证对目标监视的有效性。重点监控点图像存储、回放的图像分辨率满足 GA/T367-2016《视频安防监控系统技术要求》规定要求。

（4）经智能化处理的图像，其质量不受上述等级划分要求的限制。但对指定目标的智能化处理，其处理前后的主要图像特征信息保持一致。

2．视频编码质量需求

对于前端视频监控设备，视频编码须采用 H.265/H.264 压缩标准，视频编码设备须符合 GB28181《安全防范视频监控联网系统信息传输、交换、控制技术要求》标准。

编码、传输和存储的视频图像数据不低于 720P（1280×720）格式的图像分辨率。实时视频图像及存储视频图像帧率不低于 25 帧/秒，视频图像码流不大于 2Mbps。

3.7.3.5. 软件设计要求

1．易于维护性

要求系统的数据、业务以及涉及电子地图的维护方便、快捷，系统应充分考虑建设和运行环境状况、使用人员情况等实际因素，为系统的故障检修提供简便、易

用的维护方法和措施，以减少故障恢复时间和难度，降低维护成本，提高系统的应用性能。

2．安全性

系统安全体系的建设是为了保证系统运行的安全，并在系统遇到故障时（包括硬件损坏和软件系统崩溃等），能够有效地避免信息丢失或损坏，并尽快恢复系统的正常运行。

系统安全体系的建设应在国家信息安全战略、法规、政策和方针指导下，积极防御、综合防范，要求保障系统数据安全，防止侵入、干扰、窃取信息或破坏，确保系统安全、稳定运行。

系统安全指标：能检查应用通信而不止检查数据包；能监测并防范加密攻击；能保护应用基础设施部件；能防止敏感数据泄漏；能使 Web 基础设施合理化；能为所有应用部署一致的安全策略；能根据应用环境动态调整安全策略。

3．可扩展性

可扩展性是系统使用寿命的关键决定性因素，其内容应包括系统本身的不断升级和完善，同时还包括对新的内容的可接纳性能。系统应从规模上、功能上易于扩展和升级，为今后的应用和发展预留必要的接口和提供平台，以便于系统本身不断得到完善，同时延长系统的整体使用寿命，使其发挥出更多的综合效益。

4．数据精确度

项目涉及不同类型的数据，数据从采集到入库，经过多种工序，要保证数据精度需要。在数据处理过程中，系统对地形数据、模型运算等的精度有一定要求，如地形数据在采集过程中的精度，模型输入、输出数据精度等。

5．时间特性

项目涉及多级监管单位，业务流程复杂，尤其是实时监控、数据监测业务处理等方面，对系统的响应时间、更新处理时间、数据转换与传输时间及运行效率都有一定的要求，因此，在系统设计、模型算法等方面要有所考虑，采用高效合理的方法和算法，以提高系统运行效率。

6．适应性

系统在操作方式、运行环境、与其他软件的接口以及开发计划等发生变化时，应具有的适应能力。

3.7.4. 网络带宽需求

3.7.4.1. 省级平台接入量和宽带

全省约 15000 家火灾风险单位，每个企业同时登录省级消防平台 SAAS 应用系统平均有 10 人，那么企业同时在线人数差不多有 15 万。按照二八原则同时在线的有 3 万个用户，按照平均并发用户数的计算可以得知并发量在 800 左右，按照平均每个请求的数据是 40K/S 来计算，差不多需要 31Mbps 的带宽左右。

3.7.4.2. 感知网分中心接入量和带宽

根据福建省消防情况分析全省总有有 15000 家火灾风险单位，平均每家火灾风险单位接入 20 台设备。以智慧用电为例，智慧用电正常是 20 秒发送一次数据给平台，每次发送约等于 1K 的数据；那么每天一个智慧用电设备差不多接收 4320 次数据，一个设备每天需要存储的空间是 4.3M 的数据存储空间，那么全省一天的数据存储空间约 1.206T 的设备原始数据，百天数据存储高达 120.6T 设备原始数据，全省一年的数据量达到 440TB 设备监测原始数据存储。

根据全省（含省级、市级、县级）有 94 个消防监管部门，每个单位设置一个监测数据中心节点。那么平均每个感知网分中心需对接 15000*20/94≈3200 台监测设备，每百天需存储 1.3T 的设备监测原始数据，一年差约为 4.7T 的原始数据。根据数据量化可以得到每个感知网分中心 3000 个设备平均每秒有 150 个设备并发量，平均带宽是需要 0.1Mbps 的宽带，峰值带宽为 2Mbps 左右。

按照整体平台设计，数据中心需要为省级平台提供数据支撑，可以实现实时数据流给省级消防平台提供大数据分析或实时流信息，所以分中心的带宽应该大于 5Mbps。

3.7.5. 系统安全需求

智慧消防云平台的系统安全需求，可从两方面进行着重考虑：（1）省级平台自身安全保障需求；（2）省级平台与各感知网分中心之间数据传输的安全保障需求。

3.7.5.1. 省级平台自身安全保障需求

信息安全是系统能够成功运行的基本保证。解决好信息共享与安全、完整性的关系、开放性与保护隐私的关系、互联性与物理、逻辑隔离的关系是系统设计是不是合理、系统运行能不能达到预期效果的基本前提。同时，系统必须备有较强的系统安全性和灾难恢复能力。整体上，本项目的应用系统按安全等级保护三级要求。

除软件应用系统自身应满足计算机信息系统安全等级保护三级的要求外，本次智慧消防平台所依托的省电子政务云平台所提供的虚拟硬件、网络等环境，以及已建成的成套安全防护体系，均已达到等级保护三级要求。

在现在安全防护体系中，防火墙通过 NAT 地址转换和策略，可以在门户上过滤掉部分攻击，WAF 对网络中经过它的流量的请求报文头进行分析，与其规则进行匹配做出阻断访问和通过访问的处理， IPS 对定义已知的攻击模式通过模式的匹配去阻断非法访问。对来自于终端、网络、云和用户内部的攻击，特别是涉及到漏洞（NDAY／ODAY），社会工程学和抵近式物理攻击方法。这些攻击方法的存在一定意义上可以穿透传统的防护机制，防火墙、入侵监测、防病毒软件甚至目前流行的防 APT 的沙箱解决方案都具有相当的局限性。

因此，在网络安全威胁日益倾向于以深度渗透、长期窃密和战略控制为目标的时代里，如何确保福建消防云平台各类系统和终端应用及设备免于这些威胁，也是本次建设重要内容之一。

3.7.5.2. 省级平台与各接入分中心安全保障需求

各接入省级平台的市级、县级感知网分中心，由各市、县自行建设，所采集的原始监测数据自行存储。省级平台提供的 SAAS 软件服务，对接各分中心实时获取数据时，需考虑以下几项数据安全保障要素：

1．各分中心的感知网监测数据（分布式存储），面向省级 SAAS 平台提供数据调取时，须以开放高性能、高稳定性的数据接口形式进行数据，确保数据传输的实时性和不中断。

2．由于省级平台与感知网分中心均部署于政务外网（互联网区）或互联网环境中，为保障数据传输的安全性，须对传输中的部分关键数据进行加密由于传输数据

条数较大，且为实时传输，建议采用硬件 VPN 设备，专用加解密芯片可以有效提高数据加解密处理效率，保证数据传输的时效性同时实现数据传输前的双向校验机制，确保数据不被篡改、不改窃取。

3.8. 项目建设必要性

3.8.1. 项目建设意义及必要性

建设福建省智慧消防云平台，能够有效掌握联网火灾风险单位建筑消防设施底数及运行情况，通过对监测数据进行实时统计和智能分析，实现对问题突出的单位法人、消防安全责任人进行点对点的信息警示和提示，落实单位主体责任，及时消除火灾隐患。本项目的建设对各级政府、各行业主管部门、各级消防救援部门、联网火灾风险单位、乃至社会公众都有着重要而深远的意义，主要体现在：

1．进行全省消防信息化工作统筹、普遍提高全省各地消防信息化应用水平

由于全省各地市、区县经济发展差异，各地财政水平不一，因此在信息化方面的投入也各有不同，每年各地针对消防领域的信息化财政预算投入资金差异也比较明显，从而决定了不同区域的消防信息化，特别是近几年来消防物联网系统、智慧消防平台的发展建设水平参差不齐。从整个福建省范围来看，沿海经济发达地市、区县的地区消防信息化工作开展较早且投入较大，而经济较为落后的内地地市、区县的本地消防信息化规划则较为滞后。因此，要对全省消防安全监管工作进行全省统筹，就必须建成全省智慧消防大平台和大数据中心，让暂未规划建设智慧消防相关应用的各地市、区县消防部门无需投入过多财政投资即可将消防安全监管新理念、新技术快速运用到实际工作中，又普遍提高了全省各地的消防信息化应用水平。

2．构建城市安全智能保障体系、推动智慧城市发展的需要

建设福建省智慧消防云平台是适应城市消防安全管理现状的需要，利用物联网技术提升消防安全管理水平的一项措施和科技手段。从 2006 年开始，公安部在全国推广城市消防安全远程监控技术，并出台了《城市消防远程监控系统技术规范》GB50440-2007，《城市消防远程监控系统》系列标准 GB26875-2011，一些城市通过消防远程监控系统的建设取得了较好的应用成效，积累了一定的建设和管理经验，但该系统也存在着信息采集内容少、电话线传输不稳定、误报误判问题严重、火警核

实工作量大等突出缺陷。通过福建省智慧消防云平台项目的实施，可有效促进省总队、各支队、各大队信息化基础设施和消防物联网应用平台建设，在高层超高层建筑、人员密集场所、城乡结合部、地下建筑等火灾多发区域推广应用智慧消防物联网监控管理系统，形成动态的、智能的火灾隐患监控网络。在城市安全运行和应急管理领域优先开展物联网项目建设和应用，建成覆盖重点区域和场所的火情智能化监测网络，实现建筑消防设施远程智能化监测和报警，能够大力推动构建城市安全智能保障体系，推动智慧城市、智慧消防的发展。

3．提高全省消防安全态势感应、辅助决策分析能力的需要

通过建设福建省智慧消防云平台，进一步提高省总队、各支队、各大队对火灾的感应能力。及早发现、上报火灾隐患，以点带面、以专带群，初步形成火灾隐患动态更新、动态消除，智能分析、精确布警的新型防控模式。为各级领导掌握城市建筑火灾防控整体形势，组织展开一系列有针对性的火灾隐患专项排查清剿行动和联合执法提供科学的依据，同时，也为各级消防部门督促辖区内联网火灾风险单位及时整改消除火灾隐患，加强消防网格化管理提供精确的指导，提升智慧城市运行管理水平。

4．有效落实“预防为主，防消结合”的消防工作方针的需要

通过福建省智慧消防云平台，能接收建筑火灾自动报警系统的火灾报警信息；接收建筑消防设施运行的状态信息，对联网用户消防设施发出巡检测试指令，将巡检测试结果通过监控网络反馈回监控中心；能显示报警用户名称、地址、联系人电话等；能对火灾报警信息进行辨识、核实和确认；能向城市 119 指挥中心或其他接处警中心传送经确认的火灾报警信息。福建省智慧消防云平台的建成可大大加强消防部门对联网建筑各类消防设施的实时监控能力，各级消防部门可以方便对联网火灾风险单位进行消防安全管理、实时消防检查，提高消防监督效率，真正做到“预防为主，防消结合”的工作方针。

5．规范消防安全监督管理工作、提升服务水平、强化应急处置能力等需要

福建省智慧消防云平台中的消防物联网远程监控系统具有实时、完整、准确、不受人为因素影响的技术特点。经过测试，采用宽带互联网的条件下，从火灾探测器报警到信息通过物联网传到监控管理中心的延时不超过 5 秒，不仅可以传报警信息还可以传故障信息和运行状态信息，并对信息进行完全有效的存储，使消防部门

准确全面地掌握单位消防设施的运行情况。如果与建筑平面图和消防设施点位图配合使用，还能精确地定位报警房间的位置。过去当消防设施发生报警时，有的单位因为值班人员脱岗、漏岗，延误了处置时间，导致小火酿成大灾。还有的单位消防设施发生故障后不及时维修，等到消防部门检查发现了就改一改，检查过后又置之不理，导致很多消防设施带病运行，发生火灾时无法发挥应有的作用。如果利用智慧消防物联网监控管理系统进行监测，这些问题都可以及时发现、及时督促整改。

6．落实消防安全责任机制，协助技术人员进行灾后分析的需要

《消防法》《火灾事故调查规定》中明确消防救援部门在火灾事故调查工作中不可回避的法定职责包括：“调查、认定火灾原因”“核定火灾损失”“查明火灾事故责任”。《火灾事故调查规定》对火灾事故责任划分为四种：直接责任、间接责任、直接领导责任和领导责任。而实际操作中许多由多种行为相互作用而导致的火灾事故责任不好区分，弄清谁是前因，谁是后果并不容易，其中消防设施设备状态、维护保养是否及时、安全督查是否到位，也是其中重要的影响因素。通过建设福福建省智慧消防云平台，可以有效地落实消防设备设施管理制度，通过完善的设备台账管理、完整日常巡检记录、维修记录、安全督查记录、设备运行状态的历史趋势和报警记录，可以真实全面地反映火灾事故前消防设施设备的完好情况及维保和监督状况，救灾过程中设施设备的工作状态，这将为灾后责任追查提供有力的证据。

7．提升消防安全业务管理水平，降低消防安全管理工作强度的需要

消防设施设备的维修保养和安全监督主要涉及“消防监督部门”“楼宇业主”和“技术服务单位”，通过福建省智慧消防云平台，可以有效地提升相关单位安全业务管理水平，降低消防安全管理工作强度，具体体现在：

（1）对消防监督部门：利用系统提供的在线监测信息，可全面掌握消防安全管辖区域内设施设备运行整体状态，根据实际情况制定工作规划和管理措施；量化管理消防设施维护工作不到位的单位，加强防火工作的信息处理能力，减轻监督人员工作的劳动强度。利用系统提供的数据分析功能，能够向高层管理者提供更科学的决策依据，对出现的新情况、新问题提供技术参考，有利于找出问题解决对策。并对设施设备维护工作到位和不到位的单位进行量化统计，根据实际情况奖惩。在灾后事故调查过程中，利用系统提供的完整历史记录，可以帮助技术人员获得技术参考数据，帮助责任辨识和责任量化，降低调查的失误可能性和纠纷发生。

（2）对消防设施设备维保方：通过集中的设备远程监控，可快速地判断设备设施问题，协助维修工程师精确地定位设施设备故障，通过维保人员统一调配可以更加高效地利用有限的高级设备维修维护人员，降低人员成本，提升工作效率。通过系统的协助，可以帮助日常运维工作流程化，减少因人为因素导致维护工作不到位的现象，提升客户满意度。

（3）对消防设施设备的业主方：利用系统提供的远程在线监测设施、设备运行状态数据，规避因为消防设施故障给业主方带来的行政成本；利用系统提供的消控室值班查岗和视频联动等功能，规范消防值班纪律，监督值班状况；通过电话确认、语音对讲等功能，快速确认火警信息真伪并组织及时有效的扑救，减少火灾造成的损失。

3.8.2. 项目建设可行性

1．政策可行性

国务院发布的《促进大数据发展行动纲要》提出“2017 年底前形成跨部门数据资源共享共用格局”，“2018 年底前建成国家政府数据统一开放平台”。《福建省促进大数据发展实施方案（2016—2020 年）》也提出“2018 年底前，实现数据融合开放领先目标”。

2018 年 4 月 2 日，福建省发布《2018 年数字福建工作要点》，提出数字福建要深入贯彻落实习近平新时代中国特色社会主义思想和党的十九大提出的“建设网络强国、数字中国、智慧社会，加强信息基础设施建设，推动互联网、大数据、人工智能和实体经济深度融合”的战略部署，按照国家信息化发展战略纲要、国家“十三五”信息化规划和福建省“十三五”数字福建专项规划要求，进一步加快数字基础设施建设、政务数据共享开放和信息资源开发利用，推动数字经济不断发展壮大，推动全省信息化发展水平继续位居全国前列，积极打造数字中国样板区和示范区，为“再上新台阶、建设新福建”提供强有力的信息化支撑。

近年来，福建省消防救援总队信息化建设紧紧围绕习近平总书记建设数字中国、网络强国战略思想，根据《国家信息化发展战略纲要》《“十三五”国家信息化规划》“加快消防领域信息化建设”的要求，认真落实福建省委省政府、原公安部消防局等相关消防信息化部署，充分运用网络技术和现代传播手段，积极探索基于 5G、大

数据、物联网、云计算等新兴技术的现代消防、智慧消防业务开展形式，努力拓展新时代新形势下的消防安全监管手段，不断提高消防安全监管与服务水平，降低消防安全事故率、杜绝消防隐患，切实保障社会及人民群众生命财产安全。

按照《“十三五”国家信息化规划》十大重点任务“支持善治高效的国家治理体系构建”的要求，福建省消防救援总队强化工作落实，结合数字福建和“互联网+”主体思路，规划信息化发展导向，建设福建省智慧消防云平台。

为贯彻落实国家相关政策及福建省委省政府、福建省消防救援总队的总体要求，建设全省统一的福建省智慧消防云平台已是迫在眉睫。

2．技术可行性

福建省智慧消防云平台遵循了统一技术体制、统一标准和统一平台建设。首先，在智慧消防云平台统一的技术体制中提供了从物理层到数据访问层的解决方案，包括：软硬件支撑环境，数据组织与高效检索，多中心虚拟化整合和数据访问与传输服务等，为本系统的数据产品共享与分发、数据可视化以及打通与其他系统的数据链路提供了技术基础。

其次，针对智慧消防云平台大数据汇聚集成、组织管理、数据高效查询检索等技术，已经形成了一定的技术基础，本系统可以借鉴云平台的技术积累；另外，在应用开发层上智慧消防云平台提供了基于插件的二次开发集成框架，在此基础上可以增加应用扩展，为实现不同来源数据的汇聚集成提供了技术基础。

再次，在多源数据的汇聚集成上，依托总队现有的数据资源，能够确保智慧消防云平台大数据中心具有稳定、可靠的数据资源保障。

此外，消防专题数据、消防业务数据、省级基础数据库数据、省公共信息资源数据、国家知网数据、省内重点行业消防数据、消防社情民意数据、互联网数据的时空信息融合技术已经在大数据行业使用多年，能够满足日常业务需求。

3．经济可行性

智慧消防云平台以全省技术业务统一、开放共享、平台灵活拓展、解决消防监管现状问题为目标，通过先进的信息技术、通信技术和科学的管理手段，将消防主体、消防监管服务过程、消防安全监管成果、监管机制等进行有效链接，改变传统思维、突破时空限制，建立符合全省消防安全监管工作特色、满足全省消防工作需求的业务应用系统、信息资源库和计算机网络体系，开辟全省消防安全监管新手段、

新领域、新境界，促进消防各项工作更高效、更开放、更现代，项目在社会经济效益方面也是可行的。

4．建设单位能力可行性

本项目建设主体单位福建省消防救援总队具备丰富的应用需求对接和项目管理能力，具备实现重大系统建设基础和能力。

本项目的省市县三级节点的部署既存在共性，又具有个性，目前全省各级消防救援部门在组织单位人力、技术和设备方面基础良好，具备在全省范围内部署各级消防分节点及应用系统的基础。

第4章 项目目标分析与设计

4.1. 政府职能目标

“智慧消防”作为智慧城市建设的一个重要环节，既是政府推进履行消防安全责任监管、消防安全服务、消防宣传、消防应急救援等工作职责的新型信息化手段，也是政府切实加强保障社会及人民群众生命财产安全的一个重要目标。同时，智慧消防平台与其它政府职能部门之间也存在较多的信息相互依赖和信息共享，建设好福建省智慧消防云平台，对于福建省各级政府部门建设大数据互联互通平台也具有重要的目标意义。

建设福建省智慧消防云平台，是为适应城市消防安全管理现状的需要，利用互联网/物联网技术提升消防安全管理水平的一项措施和科技手段。通过福建省智慧消防云平台项目的实施，可有效促进省消防救援总队及各支队、大队的信息化基础设施和消防物联网应用平台建设，在高层超高层建筑、人员密集场所、城乡结合部、地下建筑等火灾多发区域推广应用智慧消防物联网监控管理系统，形成动态的、智能的火灾隐患监控网络。建成可大大加强消防部门对联网建筑各类消防设施的实时监控能力，消防部门可以方便对联网火灾风险单位进行消防安全管理、实时消防检查，提高消防监督效率，真正做到“预防为主，防消结合”的工作方针。

4.2. 福建省“十四五规划”和“2035 远景目标”

以下列举福建省国民经济和社会发展第十四个五年规划和二〇三五年远景目标纲要中与智慧消防相关的条款说明：

1．建设智慧城市和数字乡村

推进“数字城市大脑”建设，加快城市运行“一网统管”步伐，深化社会治理智慧化应用，实现“观管防”有机统一。加强城市“神经元”感知系统建设，提供城镇交通、给排水、能源、通信、环保、应急、消防、防灾与安全生产等智慧应用

服务。建设数字乡村，推进农村基层政务信息化应用，加快现代信息技术与农村生产生活全面深度融合。推进益农信息社建设。

2．提升城市综合承载能力

统筹城市规划、建设、管理，促进城市更加健康安全宜居。改善城市公用设施，实施老旧小区改造、市政管网建设、智慧设施建设等城市更新重大工程。推动城市生态修复和功能完善，完善绿地系统布局，增加生态休闲空间，提升绿化美化彩化水平。完善绿道网络，建设依山傍水、串联城乡的“万里福道”。提升城市抵御冲击和应急保障能力，加强城市防洪、抗震、人防、消防、排水防涝的设施建设，合理规划应急避难场所、方舱医院等，打造海绵城市、韧性城市。建设智慧城市，大力发展智慧管网、智慧水务等，支持智能停车、智慧门禁、智慧消防、智慧养老等智慧社区应用和平台建设。保护城市历史文化，挖掘底蕴，扩大福州、泉州、漳州、长汀等历史文化名城国内外知名度和影响力。提升建筑业发展质量，发展工程总承包和装配式建筑，培育新时期建筑业产业工人大军。

3．健全救灾体系

提升综合抢险救灾能力，整合优化省级专业应急救援中心，统筹自然灾害、消防、安全生产事故救援等专业力量，健全快速调动机制，增强森林火灾、洪涝灾害、地震灾害等应急处置能力，提高危险化学品、矿山、金属冶炼等重点行业领域专业应急救援能力。实施基层应急能力提升示范点和基层防灾减灾示范工程，推进综合性基层应急队伍建设，完善防灾减灾工作预案，确保预警到乡、预案到村、责任到人，提高农村抵御防范各类灾害能力。完善社会力量参与防灾减灾政策，建立社会力量参与防灾减灾救灾工作平台。

4．加强应急保障能力建设

健全应急管理体制机制，完善标准体系和组织体系，优化风险防控、监测预警、应急联动、应急新闻工作、信息发布、恢复重建等机制。统筹利用社会资源，加快新技术应用，强化应急协同保障能力。完善消防安全共治共享机制，加强城乡公共消防基础设施建设，优化消防救援队伍、森林消防队伍人员及装备配置。健全突发

事件和应急处置风险防控监测预警服务体系，完善应急预案评估与演练机制。加强防汛、抢险、救助物资储备，构建统一应急物资储备信息化管理平台，建立省市县乡四级应急物资储备网络。

5．应急保障重大工程

应急救援体系：推进应急预案体系、应急救援力量、应急救援航空体系等建设。建设感知网络、通信网络、应急指挥视频调度系统、应急数据治理系统、应急管理综合应用平台等。建强国家综合性消防救援队伍，壮大政府专职消防队、志愿消防队、微型消防站等多种形式消防队伍，补充消防救援队伍力量，推进“防消一体化”，实现城乡消防救援力量全覆盖。

公共消防基础设施建设：适应“全灾种、大应急”需要，加强消防救援站、消防供水、消防通信、先进消防装备、消防车通道和省市两级消防训练基地、国家级消防科普教育基地建设。建设“智慧消防”平台。

4.3. 公众服务期望目标

消防安全涉及社会及人民群众的生命财产安全，关系到社会正常生产生活，关系到国计民生，是关系到社会公众切身利益的问题，所以社会公众对于智慧消防云平台所能提供的公众服务（如消防安全宣传、消防救援、消防维保等）是有较强的目标期望。

福建省智慧消防云平台中相关的消防物联网远程监控系统通过物联网信息传感与通讯等技术有机链接，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，增强灭火救援的指挥、调度、决策和处置能力，提升消防安全管理智能化、社会化水平，满足火灾防控“自动化”、灭火救援指挥“智能化”、日常执法工作“系统化”、队伍管理“精细化”的实际需求，实现智慧防控、智慧作战、智慧执法、智慧管理，最大限度做到“早预判、早发现、早除患、早扑救”，打造从城市到家庭的“防火墙”。通过福建省智慧消防云平台项目的实施充实消防信息化建设工作，作为智慧城市安全领域的重要组成部分，已经逐渐成为政府力挺的城市发展模式，成为政府为民服务工作的一项实事工程。

4.4. 信息化愿景目标

福建省智慧消防云平台项目建设的信息化愿景目标，旨在基于全省各级消防部门现有业务、行政监管现状、社会现状的基础上，依托移动互联网、物联网、云计算、大数据、BI 业务分析等先进技术，建立全省性消防物联感知网络，建立全省消防大数据中心，为消防安全管理、社会消防监管火灾风险单位、消防监管与应急救援提供高效的管理工具。同时，通过本次项目建设，建成一套全省性智慧消防协同平台，实现业务协同、技术协同、数据协同。

1．省级主导、市县分工协同

智慧消防平台以省总队主导建设，省级负责基础应用软件开发、大数据中心开发、平台延展性和扩展性开发，开发完成的应用系统可分发至各市县消防部门进行日常使用；市级和县级负责本辖区内的物联感知网络建设，以市县为单位建设成多个感知网分中心，并通过平台实现数据汇聚。

2．提高全省各级消防部门的信息化应用水平

通过本次智慧消防云平台项目的全省统筹，进一步带动各地消防部门的信息化应用水平，将消防信息化建设较为落后、滞后的基层单位，通过全省统筹的方式将信息化水平提升到新的层次。

3．建成全省乃至全国智慧消防、智慧城市建设标杆

截至目前，全国范围内还未有以省级为单位进行全省性的智慧消防平台统筹建设，即一个大平台涵盖省、市、县三级的智慧消防应用。因此，通过本次福建省智慧消防平台建设，以先进的平台技术优势、高效的平台业务逻辑，让智慧消防平台成为全省乃至全国智慧消防、智慧城市建设的先进典型形象标杆。

4.5. 系统建设目标

建设福建省智慧消防云平台，本期的系统建设目标如下：

1．建立全省性的智慧消防建设（特别是消防物联网）技术体系标准；

2．以省级为主导，统筹各地建设，智慧消防平台应用软件（包括物联网远程监控系统、大数据运维管理中心、基础统计分析系统、消防远程培训服务平台、SAAS/PAAS 平台、消防值班运维管理系统、大数据一张图综合应用展示系统）由省

级统建，并分发各基层单位使用；

3．各市、县消防部门自建消防物联网感知网络中心，实现消防基础数据、消防设备设施动态数据采集。根据消防安全监管责任落实主体，全省（含省、市、县）消防物联感知网络分中心约为 94 个，省级消防大数据汇聚中心 1 个。

4．为省总队提供 3 年期的技术和业务运维服务。

5．最大程度上对外开放使用省级平台数据、实现业务共享；

6．针对已建智慧消防或物联网系统的市、县消防部门，要求数据接入和上报汇聚至省级平台；

7．各市、县消防部门在使用省级智慧消防云平台过程中，如有针对本辖区内的一些特色应用需求，可在省级平台提供平台技术架构体系和二次开发工具的基础上进行特色应用开发，开发完成后以应用服务形式挂接于省级智慧消防云平台。

第5章 项目业务分析与设计

5.1. 部门业务域、业务线、业务事项设计

综合福建省消防救援总队和各地市支队、县区大队，进行分类和规整，全省各级消防部门的业务架构有 5 个业务域、11 个业务线和 36 业务事项。

序号	业务部门	序号	业务项	业务服务对象	序号	详细业务事项	业务子事项
1	消防安全宣传（新闻宣传）	1	消防安全知识普及	单位	1	单位消防知识普及	
				个人	2	个人消防知识普及	
		2	消防安全培训	单位	3	消防安全教育培训	
				义务消防队	4	指导培训义务消防队	
2	防火监督管理	3	防火检查	单位	5	防火巡查检查	
				单位	6	消防车通道检查	
				单位	7	消防水源情况检查	
				单位	8	重点工种人员以及其他员工消防知识的掌握情况检查	
				单位	9	消防安全重点部位的管理情况检查	
				单位	10	易燃易爆危险物品和场所防火防爆措施检查	
				单位	11	其他重要物资的防火安全情况检查	
		4	防火责任督促落实	单位	12	火灾风险单位消防责任落实	督促消防安全档案建立健全
				单位			督促建立消防安全管理制度
				单位			督促制定紧急疏散预案
				单位	13	消防责任督促检查	定期督促检查
				单位			不定期督促检查
				个人	14	个人消防责任落实	
		5	防火档案管理	消防技术服务单位			消防设施定期检查记录
				消防技			自动消防设施全

序号	业务部门	序号	业务项	业务服务对象	序号	详细业务事项	业务子事项
				术服务单位	15	防火检查档案管理	面检查测试的报告以及维修保养的记录
				单位			火灾隐患及其整改情况记录
				单位			防火检查和巡查记录
				单位			有关燃气及电气设备检测(包括防雷、防静电)等记录资料记录
				单位	16	防火标志设置	
3	消防监督业务资料档案管理	6	消防基础档案	道路	17	道路资料档案管理	
				水源	18	消防水源资料档案管理	
				单位	19	消防安全火灾风险单位资料档案管理	
				单位	20	重点部位资料档案管理	
				消防部门	21	消防组织机构和队伍情况资料档案管理	组织机构档案管理
							消防队伍档案管理
		7	消防管理档案	单位	22	消防工作计划	
				单位	23	消防制度	
				单位	24	消防检查巡查记录	
				消防部门	25	消防法律文书	
				单位	26	消防宣传教育培训情况	
				单位	27	其他相关的消防情况	
4	消防预案管理	8	消防预案制定	单位	28	消防安全火灾风险单位预案制定	
				单位	29	重点部位的事故处置预案制定	
				消防部门	30	灭火作战预案制定	
		9	消防预案演练	单位	31	督促、指导消防安全火灾风险单位预案演练	
				消防部门	32	灭火作战预案演练	
5	灭火救援指挥	10	火灾现场应急救援	单位	33	火灾扑救	
				单位	34	火灾现场保护	

序号	业务部门	序号	业务项	业务服务对象	序号	详细业务事项	业务子事项
		11	火灾事后责任调查	单位	35	火灾原因协助调查	
				单位	36	火灾事故处理	

5.2. 业务对象设计

根据“部门业务域、业务线、业务事项”，全省消防安全管理领域相关的业务架构可划分为全省各级消防队、消防安全协同单位、火灾风险单位、消防技术服务单位、社会机构及公众雇个人等 5 个业务对象。

系统主要使用人员是全省消防队（省总队、市支队、县大队）单位领导和工作人员；受监管单位（火灾风险单位）消防安全负责人消防技术服务单位工作人员、消防安全协同单位工作人员（如综治、街道、派出所等）、社会公众，为这些工作人员提供方便快捷的应用系统。

5.3. 关键业务活动分析

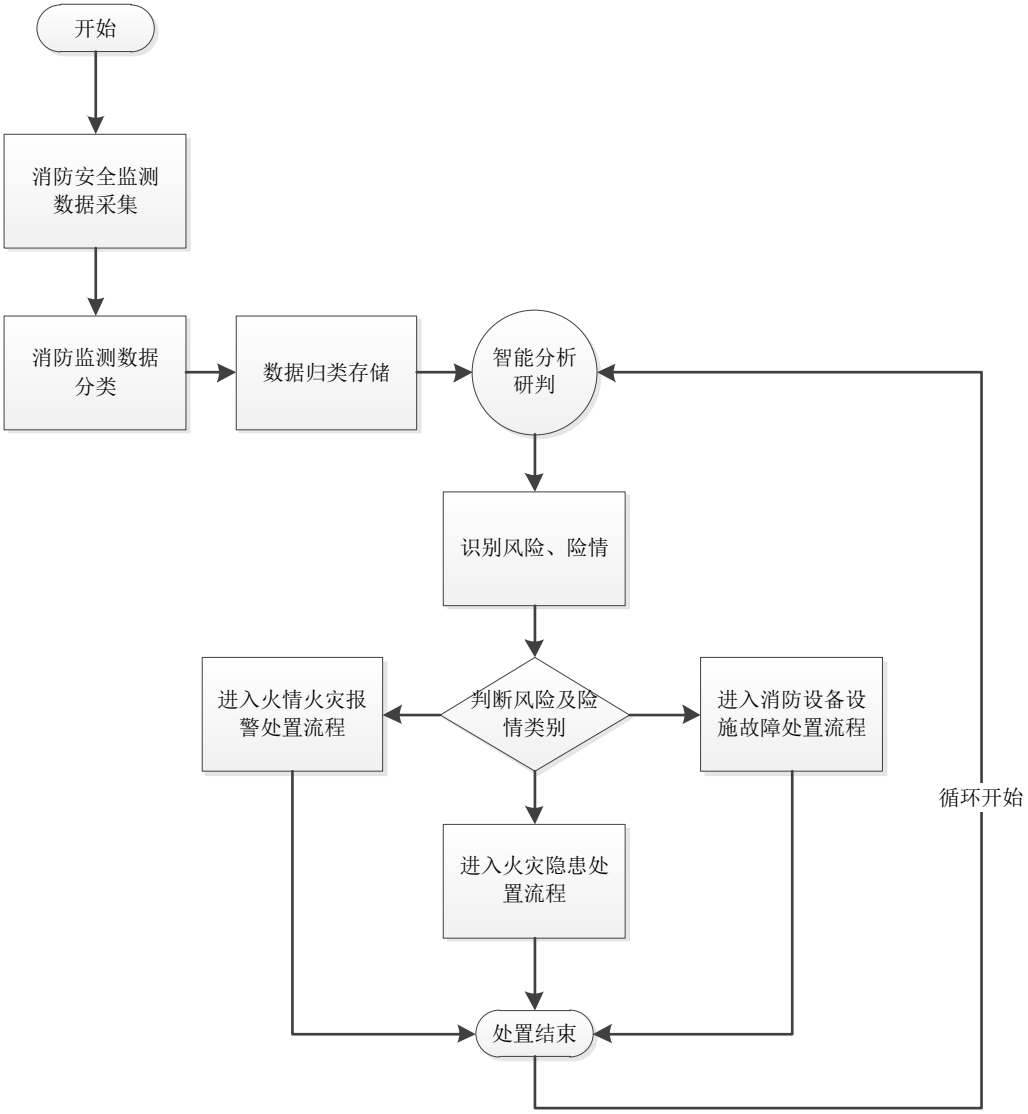
福建省智慧消防平台的关键业务活动，是针对全省（除总队外的二级、三级消防主管部门）消防物联网监测流程进行统一、标准定义。根据省级智慧消防平台的 SAAS 特点以及平台的灵活性与扩展性特点，二级、三级消防主管部门在进行这几项关键业务活动开展时，可根据地区差异性、本单位监督执法特点和特殊需求，对关键业务活动流程中的环节、要素等进行自定义微调，但不可脱离关键业务活动本质。

本次描述的关键业务活动分析主要在于对消防物联网监测要素的实时监测，以及对监测结果的实时分析和分析结果处置流程安排。该项关键活动对于火情、火灾隐患的识别具有重大意义，提高火情、火灾隐患的精准识别度和识别几率，有助于尽早消除火灾隐患或尽早扑灭火情，可极大降低对着火区域及周边的建筑安全、财产安全和人民群众生命安全。

关键业务活动主要针对火情火灾、消防隐患、设备故障等 3 个要点进行分析与设计。

5.3.1. 火灾要素分析与识别流程

在智慧消防体系中极其重要的核心组成部分“消防物联网远程监控系统”，主要的核心业务在于对火灾风险单位的各种消防设备设施、消防安全状态等进行智能设备监测与数据采集，并对采集后的数据进行精准分析、研判和告警。



5.3.2. 火灾火情监测报警处置流程

在消防物联网体系中，火灾报警智能分析判断依据，主要通过消防物联网智能监测设备所采集到的各项要素值进行判断。

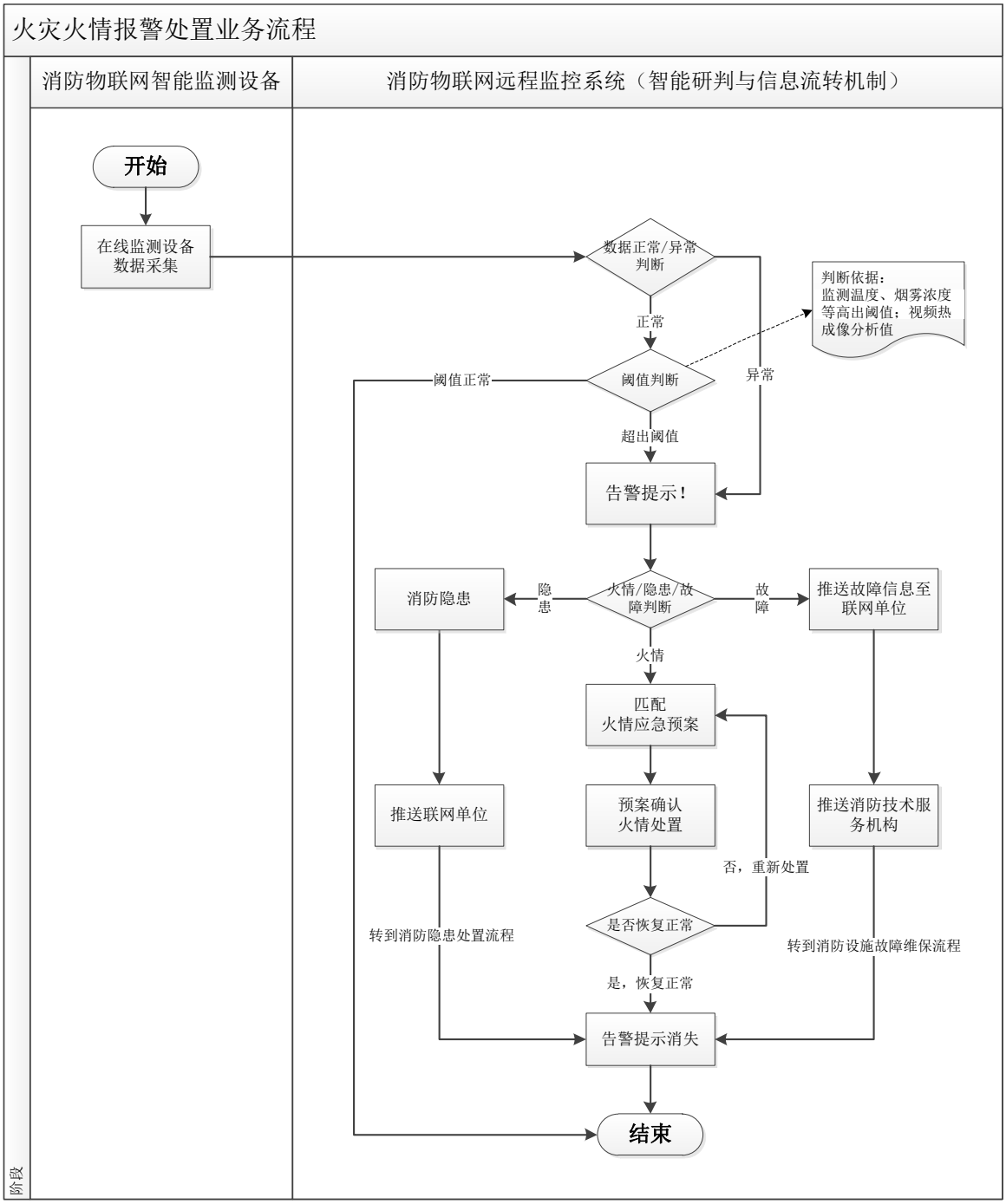
具体判断依据如下：

1．温感监测：空气温度超出阈值；

2．烟感监测：空气烟雾颗粒浓度超出阈值；

3．温度感应器、烟雾感应器等设备出现多点连报（即多个感应器同时采集到数据异常和发出报警信息）；

4．可配合视频热成像技术，探测区域空间内的红外能量辐射，计算生成热图像和温度值，超出温度阈值后发出报警信息。



5.3.3. 火灾隐患监测与处置流程

在消防物联网体系中，火灾隐患监测智能分析判断依据，主要通过消防物联网智能监测设备所采集到的各项要素值进行判断。

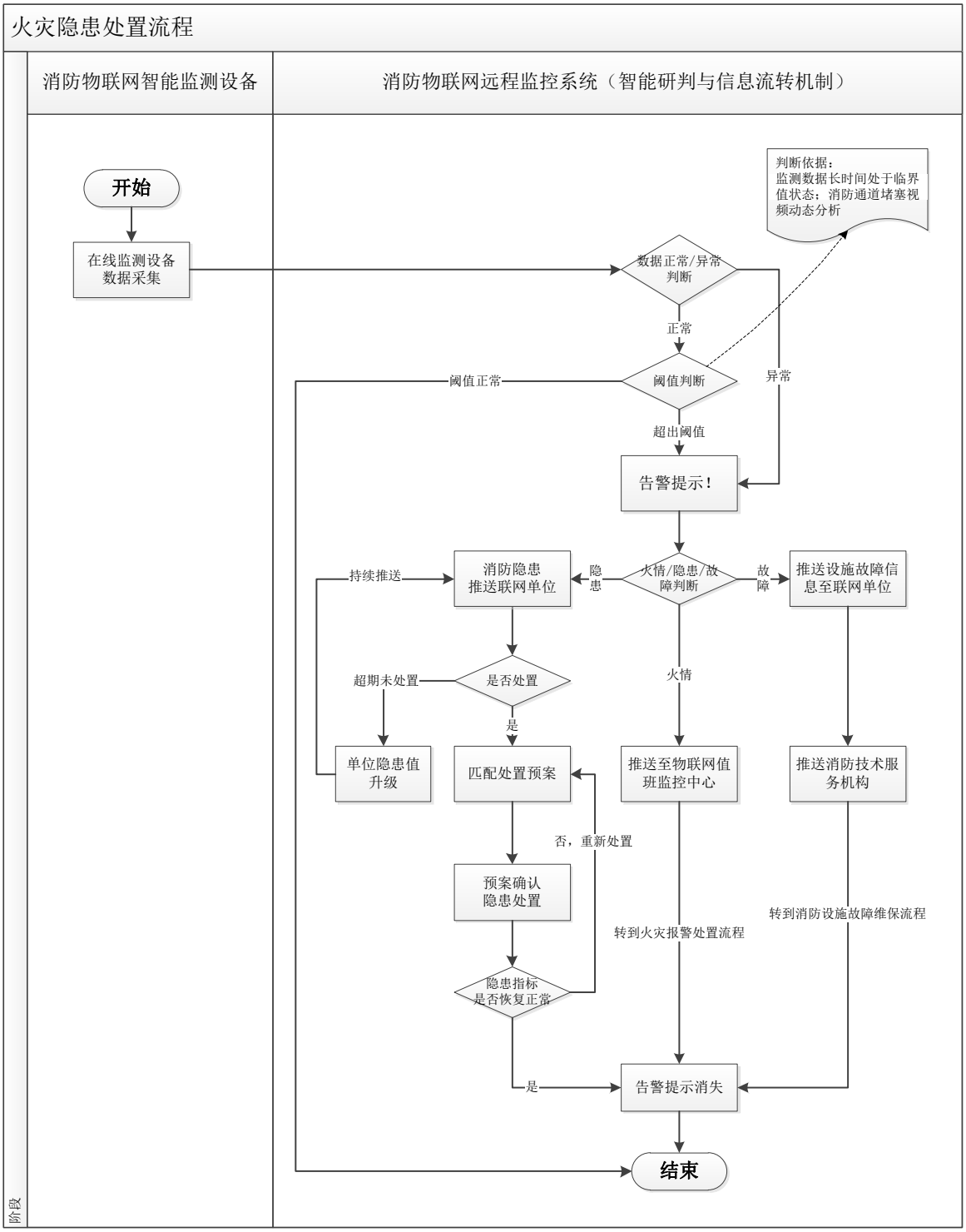
具体判断依据如下：

1．温度感应器监测值，长时间处于阈值临界状态；

2．烟雾感应器检测值，如烟雾固体颗粒浓度、可燃气体浓度长时间处于阈值临界状态；

3．消控室值班人员视频查岗点名时，多次出现不在岗情况；

4．视频巡查时，多次发现消防通道堵塞情况。



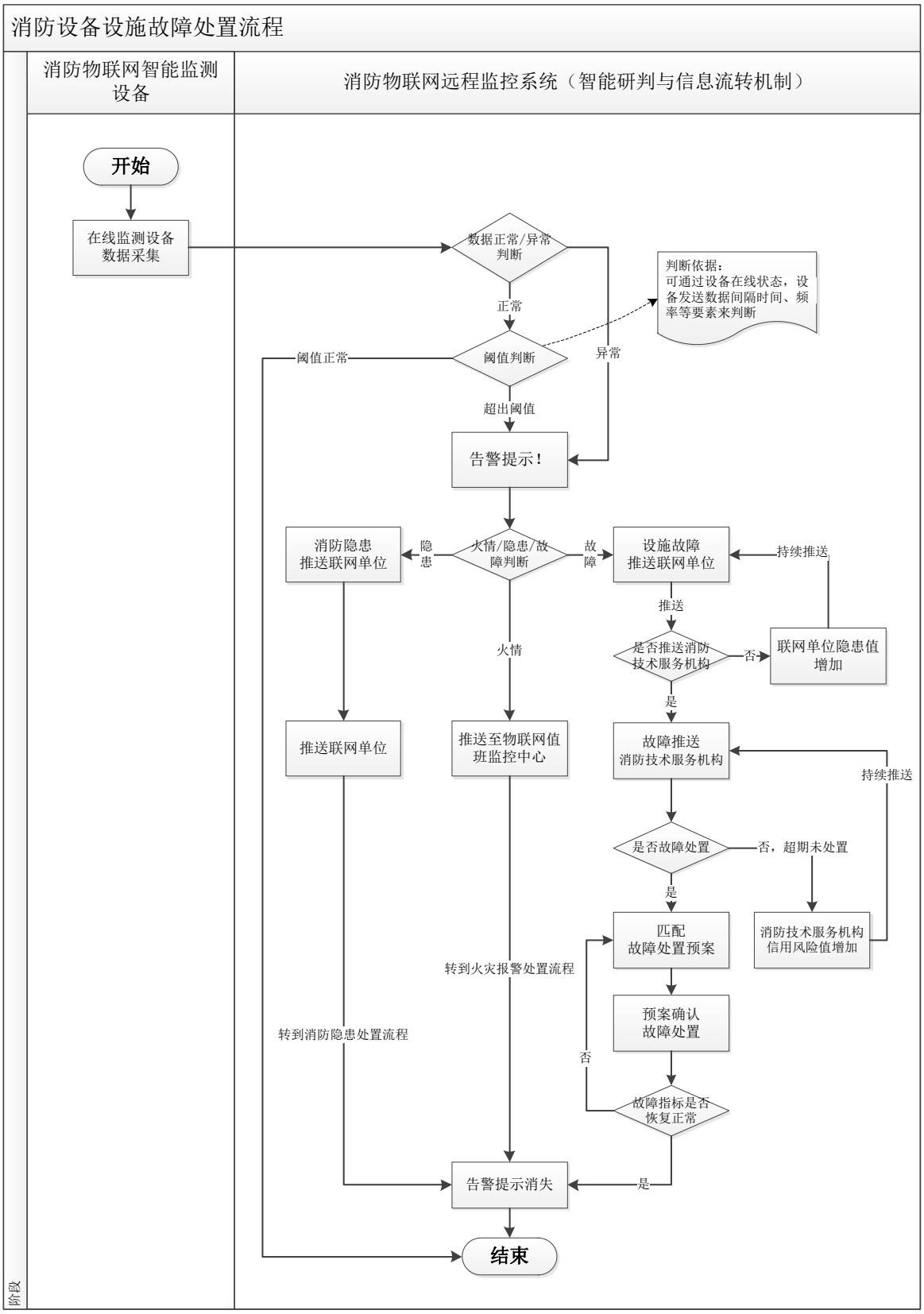
5.3.4. 消防设备设施故障监测与处置流程

在消防物联网体系中，消防设备设施故障智能分析判断依据，主要通过消防物联网智能监测设备所采集到的各项要素值进行判断。

具体判断依据如下：

1．设备通断状态处于“离线”；

2．设备发送数据异常，如“数据格式不完整”“发送频率与预设频率不符”。



5.4. 业务协同关系分析

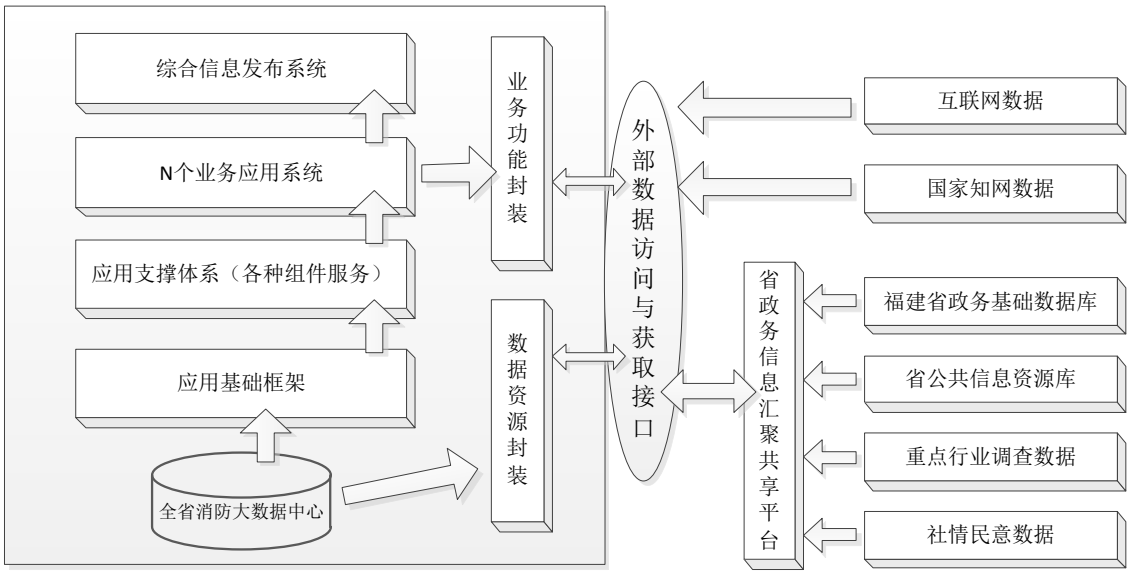
福建省智慧消防云平台业务协同关系主要体现在信息充分共享、业务协同联动。

5.4.1. 信息充分共享

按照“纵向贯通、横向交换、条块融合”的原则，统一数据标准、规范数据来源，对消防内部、外部数据资源进行汇聚和挖掘分析，为火灾风险研判、灭火救援指挥、队伍管理分析、消防宣传服务和领导指挥决策等提供信息支撑。

5.4.2. 业务协同联动

突出消防安全防控治理工作，推进面向政府部门、社会单位、中介组织和社会公众的消防社会化发展进程，创新社会消防安全治理新模式，形成多元共治、齐抓共管、全民参与、全社会共享的社会消防安全治理新格局。



业务协同联动可分为两部分：

（1）对内协同支撑：对内协同主要体现为在整个福建省智慧消防云平台框架下，应用架构层、应用支撑层、业务应用层、数据层等，逐层提供支撑和协同。

（2）对外协同：对外协同主要体现为智慧消防云平台将自身的业务应用、数据资源进行分类、打包、封装，以接口的形式为其他部门提供业务功能调用和数据访问共享。

5.4.3. 应急响应与应急调度协同

智慧消防云平台项目在应急响应和应急调度的业务目标需求上，要进行如下目标设计：

1．应急情况入口：要提供快速、边界的应急情况提交入口和通道，将现有的应急入口和后续设计建设的应急请求入口进行整合，实现多渠道、统一入口。

2．应急响应：应急请求的接收单位（人）、响应对象要明确，通过消防云平台高效的信息传递手段，及时将应急请求主动推送至应急响应机构。

3．应急调度：平台要整合省总队及各支队、大队的应急调度软硬件体系功能，结合消防云平台自身的业务流体系、数据资源体系、消息流转体系等，为消防救援机构提供精准、高效、快速的应急调度方法手段。

5.5. 业务量分析

根据省市县三级消防救援部门、全省各级消防安全协同监管部门、全省火灾风险单位、全省消防技术服务单位、全省众多社会机构和社会民众等不同对象角色的业务管理类型或所关注的业务对象进行划分，主要包括以下几项业务以及对应的业务量分析。

1．用户数。

（1）包括总队在内的省市县三级消防救援部门，单位数量为 94 个，平均每个单位开放账号使用人数为 100 人，合计约为 9400 人。

（2）全省各级消防安全协同监管部门，按照省市县 94 个行政辖区，平均每个辖区开放账号使用人数为 20 个，合计约为 188 人。

（3）全省火灾风险单位，本期按平均每个辖区接入 10 个火灾风险单位，每个单位开放 2 个账号，合计约为 1880 人。后期逐步进行用户扩容。

（4）消防技术服务单位。按照目前全省注册、运营状态正常且未列入黑名单或信用等级 D 级的技术服务单位，均可在平台上进行注册账户，每个技术服务单位的注册用户数可作固定用户量限制。

（5）全省社会机构和社会公众。由于数量众多，因此不进行用户数限制，但必须进行合法性验证，例如社会机构注册时须使用统一社会信用代码进行注册，社会

公众可通过公民身份证（如涉及隐私，可使用手机号码或“闽政通”APP 进行互联授权接入）进行注册。

2．消防物联网监测点接入数。

智慧消防云平台建成后，首先要将全省火灾风险单位的消防物联网监测设备（用户信息传输装置）接入平台，按全省 15000 家火灾风险单位接入，后续持续增加接入。

针对已建成的二级平台智慧消防相关应用（如消防物联网远程监控系统），省级平台不再二次接入已建二级平台对接的物联网监测设备，而由二级平台直接提供监测结果数据即可。

3．感知网络中心接入数。

目前按照各地市、区县自行建设感知网进行规划，全省 85 个县级区划、9 个市级区划，未来将建成 94 个消防物联网感知网络分中心。因此，福建省智慧消防平台需将 94 个感知网络分中心进行分布式管理和接入。

4．消防视频监控接入。

按照全省 15000 家火灾风险单位的消防视频监控接入计算，主要针对火灾风险单位消控室进行视频接入。平台本身不存储视频数据，按需调用本地视频资源数据，功能包括：查岗、查看回放、操作视角等。

5．消防教育培训服务业务。

全省消防教育培训服务业务，主要针对全省所有机构（含党政机关、事业单位、国企、私企）、所有个人进行消防安全知识宣传和防火救援知识的有偿培训和公益培训。培训可通过固定知识库进行宣传培训，也可在线开展专场培训，所产生的业务量也较大。

第6章 总体架构设计

6.1. 设计思想

福建省智慧消防云平台的总体架构设计，基于面向服务的架构（SOA，Service-Oriented Architecture）理论进行开展。

SOA 的实施具有几个鲜明的基本特征，福建省智慧消防云平台实施 SOA 的关键目标是实现消防行业监管数据资产、监管效益、社会效应等方面的最大化作用。

6.2. 设计原则

福建省智慧消防云平台建设的目的是整合利用信息资源，为诸如消防物联网、消防教育培训、消防物联感知网管理、全省消防大数据中心、消防 AI 与 BI 大数据智能分析研判、消防大数据一张图实战指挥、消防值班运维管理福建省智慧消防等相关业务应用系统提供弹性化的信息服务。与此同时，其系统规划和设计与单一系统有很大的不同，本项目总体架构设计必须充分遵循以下原则：

- **完整性**

要全面涵盖福建省智慧消防云平台及后续横向扩展（监管面拓宽，如接入所有重点联网单位和特殊行业单位）和纵向扩展（由省级监管向市级、县级、乡镇、村等行政级别深入拓展）的所有业务要素，保证数据在业务意义上的完整性；

- **合理性**

目前云计算还没有完整的标准可供参考，考虑到技术的延续性，以及系统维护的成本，平台建设应要求采用以业界标准主流的产品为主的建设模式，保证系统架构的合理性。这些技术和产品都是最广泛采用的，将来随着产品的升级，技术和服务也会随之升级扩展。在技术架构升级和系统扩容方面要充分考虑保护现有系统的软硬件投资，既要注意采用先进技术，又要考虑技术对应用的实用性。所有技术的使用必须考虑其业务应用的有效性和风险。

- **先进性**

福建省智慧消防云平台建设采用的产品和技术具有云平台的特征及技术的先进

性，保障平台的资源使用周期最大化。但采用先进的技术也有一定的风险，即可能存在技术不成熟问题。平台建设应要求采用充分论证及测试的方式，在选择先进技术时，把技术风险降低。在实用、可靠的前提下，本平台的设计应尽可能地跟踪国内外先进的软件技术和系统和管理技术，以能够最大限度地适应技术发展变化的需要，确保平台的先进性。

- **高可靠性**

福建省智慧消防云平台服务于整个福建省消防监管、消防服务、消防政策宣传、消防教育服务等业务和广泛的社会用户，有众多任务关键型的应用。每天都交换大量的数据，需进行实时处理，任何的系统故障都可能带来不可估量的损失，这就要求平台具有高可靠性。平台设计应采用成熟、稳定、可靠的软件技术，特别是数据库管理系统等关键系统软件，应优先考虑采用成熟的企业级商业产品，以保证平台长期可靠地运行。

- **可扩展性**

福建省智慧消防云平台容量需要随着形势的发展不断变化或扩充。另一方面，系统平台的计算和存储等资源能力不确定，需要在运行中不断扩充或调整。此外，社会开放服务要求平台逐步演化，不断适应新环境和新的商务、技术要求，不可能以推倒重来的方式进行升级。因此，平台的设计应具备高可扩展性。云计算各层次的设计应保证可平滑扩展与可伸缩。而且在进行扩展和伸缩时，应保证不中断系统业务处理。可实现通过简单的硬件扩容达到系统动态扩容的目的，可动态伸缩，满足应用和用户规模增长的需要。

- **安全性**

福建省智慧消防云平台的开放及广泛连接特性更加凸显信息安全的重要性。因此，平台的设计应建立可靠的安全保障体系，对非法侵入、非法攻击和网络计算机病毒应具有很强的防范能力，所采用的保护措施应能保证整个系统正常高效的运转。

- **开放性**

福建省智慧消防云平台设计应遵循业界统一标准，采用开放结构，具备适配和中介的能力，充分考虑与外部系统的接口，充分利用各层次的开放资源。基于业界开放式标准，对电子政务云平台中的各种网络协议、网关接口、数据接口形式等进行统一规划，为未来的系统扩展奠定基础。

■ **经济性**

福建省智慧消防云平台的技术方案应更加重视能耗与利旧，在性价比最好的情况下尽量做到最低成本，尽可能做到绿色和低碳计算。

6.3. 信息技术及行业标准规范

6.3.1. 引用标准目录

本项目设计所涉及的技术、产品、工程、规范参考国家、福建省及行业相关条例和规范，主要包括：软件工程标准、数据交换标准、软件开发标准、信息安全标准、质量管理标准等几个部分。

6.3.1.1. 软件工程标准

标准号	标准名称
ISO/IEC11801-2017	信息技术互连国际标准
GB/T16260.1-2006	软件工程产品质量 1 部分：质量模型
GB/T16260.2-2006	软件工程产品质量 2 部分：外部度量
GB/T16260.3-2006	软件工程产品质量 3 部分：内部度量
GB/T16260.4-2006	软件工程产品质量第 4 部分：使用质量的度量
GB/T8566-2007	信息技术软件生存周期过程
GB/T18234-2000	信息技术 CASE 工具的评价与选择指南
GB/T18492-2001	信息技术系统及软件完整性级别
GB/T18493-2001	信息技术软件生存周期过程指南

6.3.1.2. 数据交换标准

标准号	标准名称
ISO16022-2006	数据交换标准规范（ISO16022-2000 二维码标准）
GB12904-2008	数据交换标准规范（GB12904-2003 通用商品条码）
EPCC1G2	数据交换标准规范（EPCC1G2（RFID 标准）
GB/T21062-2007	政务信息资源交换体系
GB/T21063-2007	政务信息资源目录体系
	基于 XML 电子文档格式

6.3.1.3. 软件开发标准

分类	标准号	标准名称
软件分析标准	GB/T9385-2008	计算机软件需求规格说明规范
	待定	电子政务业务流程设计方法通用规范
软件开发标准	GB/T19487-2004	电子政务业务流程设计方法通用规范
	GB/T8566-2007	信息技术软件生存周期过程
	GB/T8567-2006	计算机软件文档编制规范
软件测试标准	GB/T9386-2008	计算机软件测试文件编制规范
	GB/T15532-2008	计算机软件单元测试
软件维护标准	GB/T14394-2008	计算机软件可靠性和维护性管理
	GB/T20157-2006	信息技术软件维护

6.3.1.4. 信息安全标准

标准号	标准名称
GB17859-1999	计算机信息系统安全保护等级划分准则
GB/T22240-2008	信息系统安全等级保护定级指南
GB/T22239-2008	信息系统安全等级保护基本要求
信安字[2007]10	信息系统安全等级保护实施指南
信安秘字[2009]059	信息系统等级保护安全设计技术要求
GB/T20282-2006	信息系统安全工程管理要求
GB/T20269-2006	信息系统安全管理要求
GB/T20271-2006	信息系统通用安全技术要求
公通字〔2007〕43 号	公安部、国家保密局、国家密码管理局、国务院信息工作办公室《信息安全等级保护管理办法》
GB/T18336.1 ISO/IEC15408-1	信息技术安全性评估准则：第 1 部分简介和一般模型
GB/T183336.2 ISO/IEC15408-2	信息技术安全性评估准则：第 2 部分安全功能要求
GB/T183336.3 ISO/IEC15408-3	信息技术安全性评估准则：第 3 部分安全保证要求
待定	信息系统安全等级保护测评要求
	信息系统安全等级保护测评过程指南
	“电子政务标准化指南第二版第六部分信息安全”中涉及本次工程的

	标准和规范

6.3.1.5. 质量管理标准

标准号	标准名称
GB/T19001-2008	质量管理体系要求（idtIS09000：2008）
GB/T12504-2008	计算机软件质量保证计划规范
GB/T16260-2015	信息技术软件产品评价质量特性及其使用指南
GB/T13016-2009	标准体系表编制原则和要求
GB/T1.1-2009	标准化工作导则
CMMI-L3	软件能力成熟度集成 CMMI-L3

6.3.2. 新建标准成果

标准体系建设是福建省智慧消防云平台建设中的基础性工作，是实现本项目省、市、县三级各应用类系统互联互通，信息资源交换和共享的关键。

在标准体系建设中，需按照统一标准、统一服务、纵向贯通、横向集成的原则，通过对现有的消防体系相关的标准规范继承、拓展，以及根据需要拟编订新标准规范，来构建统一的、适用性强的福建省智慧消防云平台应用示范标准体系，保证福建省智慧消防云平台项目将来在全省范围内的推广实施。

6.3.2.1. 标准体系建设需求

目前，在消防领域与各行业各自都已具备较为全面的行业或国家标准规范，通过充分调研消防救援部门和消防服务行业方面的标准，结合本示范项目的实际需求和建设目标，发现在原有的标准规范继承基础上，福建省智慧消防云平台应用在数据标准、信息融合共享、交互操作、系统安全管理等表述方面仍存在标准不一，语义混乱等问题。

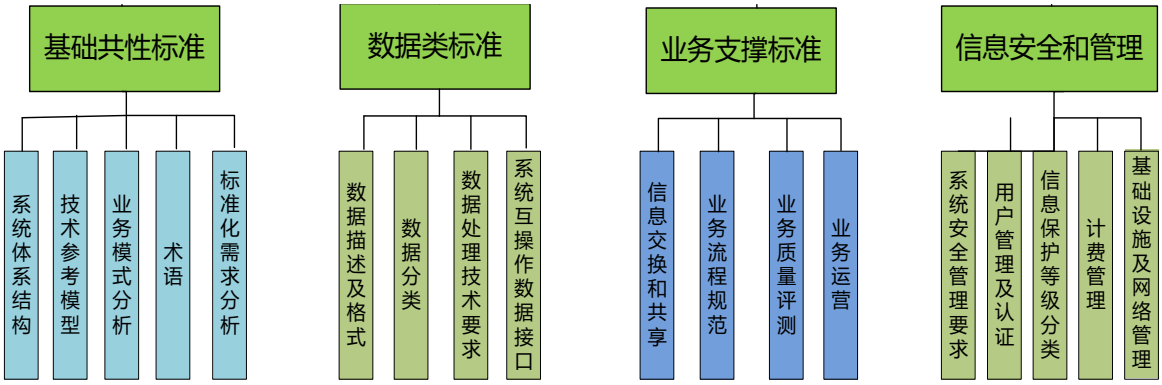
针对上述提出的福建省智慧消防云平台的信息融合与应用方面缺乏统一的标准体系，需按照继承、拓展和新编的原则，在现有标准规范基础之上，针对此项目需求和目标，制定福建省智慧消防云平台应用示范系统统一的技术参考模型、业务运行规则，形成统一的数据描述、数据格式和数据分类、编码、数据处理方法，通过信息交换、业务流程等业务支撑类标准和信息安全、管理类标准研制，实现业务流

程的标准化、规范化，有利于实现应用系统的整合和优化，最大程度实现信息资源的集成与共享，保证各项业务流程的畅通。

6.3.2.2. 标准体系建设内容

6.3.2.2.1. 标准体系总体框架

根据福建省智慧消防云平台《信息化标准体系表》标准体系模型的总体要求，并结合智慧消防云平台应用示范系统项目建设方案，拟提出如下标准体系。



通过本标准体系建设和相关标准制定工作，拟实现如下具体目标：

（1）通过基础共性类标准制定，构建智慧消防领域应用示范的术语、参考体系架构和参考技术体系，实现统一的业务模式分析和标准化需求分析，为实现相关业务的协同开展提供基础支撑。

（2）通过数据类标准制定，打通相关委办厅局数据在智慧消防领域的应用链路，解决行业数据的来源不一、格式不一、描述不一、分类不一等问题，形成面向智慧消防提供专题产品的服务能力，实现不同平台和系统间的互操作接口统一和互联互通。

（3）通过业务支撑类标准制定，为实现各部门业务的协同和信息资源的共享提供标准支撑，实现业务流程规范，业务质量可测，业务运营可控的目标。

（4）通过信息安全和管理类标准制定，提出智慧消防领域应用示范系统中的安全解决方案，规范全过程中的安全管理，实现信息分级保护和对用户授权认证的安全要求，实现对基础设施及网络的严格管理。

6.3.2.2.2. 拟新编的标准规范

虽然在消防监管与服务领域已直接引用了部分相关行业及国家标准，但在交互融合过程中，仍缺少智慧消防云平台应用方面的标准规范，因此结合原有标准，通过拟定新的标准规范，实现各方面服务应用的统一化标准，拟新编的标准规范如下：

1.《福建省智慧消防云平台应用术语》

本标准对福建省智慧消防云平台应用中的专有术语进行规范，以协调福建省智慧消防云平台应用领域不同概念体系间及不同语种术语间的关系，保证术语的一致性和逻辑上的完整性，进而统一指导智慧消防应用的建设、管理和运营。

2.《福建省智慧消防云平台数据资源分类指标体系标准》

定义了智慧消防云平台数据资源体系的数据分类标准，规定了各类数据内容的基本技术指标和要求。本标准综合考虑各级消防监管部门和服务机构的核心需求和数据获取的可行性，遵从数据来源必须是权威可信、共享可得、分享可用的原则，从科学性与系统性、典型性与可操作性、导向性与规范性、特征性与可比性、时效性和互补性、定量与定性相结合等方面进行考虑。对智慧消防云平台获取数据的分类对象定义为：消防专题数据、消防基础业务数据、省基础数据库数据、省公共信息资源数据、国家知网数据、省内重点行业消防调查数据、消防安全社情民意数据、互联网数据等。

3.《福建省智慧消防云平台应用数据描述及格式》

本标准将规定各数据来源域的数据记录存储和通信传输的编排格式。数据描述和格式标准化，可以统一系统数据的内容、结构化、存储地址、内存大小等属性。该标准的目的是在保证记录传输全部信息的同时，提高存储空间的利用率和保证数据来源域之间的数据交换与共享。本标准拟充分利用统计学规则、决策树规则和神经网络规则等规则对系统数据进行分类。该标准的制定目的是为后续的数据处理和数据挖掘提供算法依据，奠定信息共享与交换的源数据基础。

4.《福建省智慧消防云平台应用数据处理技术要求》

本标准对智慧消防云平台应用中数据处理技术要求进行规范。系统中数据处理技术复杂，主要包括数据接入、数据存储、数据同步、数据校验、数据转换、数据清洗、数据融合，数据模糊化等。本标准规定数据处理技术的处理模型、处理流程

和技术要求。该标准的目的是统一系统数据处理技术要求，提高信息交换与共享的效率，为系统的数据处理提供依据。

5.《福建省智慧消防云平台应用体系参考架构》

本标准从系统、通信及信息三个角度对智慧消防应用体系参考架构进行规范，具体包括参考体系总体架构、功能参考模型、实体描述、接口描述等内容。本标准适用于各类智慧消防云平台应用系统的设计，能够为其提供参考依据和架构基础。本标准的目标是保证智慧消防云平台应用系统间的兼容性、互操作性和资源共享性以及为智慧消防云平台应用系统设计者提供一种一致性的系统分解模式和开放性的标准设计框架。

6.《福建省智慧消防云平台应用技术参考模型》

本标准对智慧消防云平台应用技术参考模型进行描述，具体包括系统总体架构技术体系、各平台模块功能、各平台协同流程、组网方式及接口要求等内容。本标准可以为各类智慧消防应用系统的建设提供技术依据。

7.《福建省智慧消防云平台应用系统互操作数据接口》

本标准对智慧消防云平台应用中各系统之间的互操作进行规范，明确各数据接口应符合的统一要求、不同平台和系统间接口的处理原则以及接口的实现方式，对接口中数据内容、数据格式、数据结构、差错控制、接口数据传输方式以及接口间所使用协议包的格式等内容进行统一的规范。

8.《福建省智慧消防云平台应用信息交换和共享》

本标准对智慧消防云平台应用中各类信息的交换和共享进行规范，明确可以交换和共享信息的范围及原则、实现的途径以及数据隐私安全的处理方式，对信息交换和共享业务功能、数据模糊化处理、接口交互实现方式等进行定义。

9.《福建省智慧消防云平台应用系统安全管理要求》

本标准对智慧消防云平台应用中各平台及系统中涉及信息和系统安全的硬件系统安全和软件系统范围进行界定，明确系统安全管理的原则和具体要求。系统安全管理主要包含了对各系统和平台机房访问控制要求、系统和平台登录操作系统的访问控制要求、数据库访问控制要求、应用系统访问控制要求、用户控制要求等。

6.3.2.3. 标准化工作进度安排

根据本项目工程建设对标准化建设的急迫需求，按轻重缓急安排标准研制项目，集中力量解决共性、基础性标准问题，重点解决互联互通、信息共享和系统安全方面的关键问题，现将标准化建设分阶段完成，阶段划分大致如下：

1．设计阶段：完成整体的标准体系框架设计，为后续的标准制定和建设提供基础支撑和制订方向。

2．研制阶段：完成本示范项目的标准体系的初稿，将各种标准按照需求及相应原则制订完成。

3．示范阶段：完成示范项目标准体系的定稿，将制订好的标准体系作为参考应用到示范区中。

4．推广阶段：后续完成示范项目标准体系的内容扩充，试验中依据实际情况不断改进、完善和丰富，最终完成修订、应用和推广。

6.3.3. 消防安全保障行业相关标准规范

GB 51274-2017　《城镇综合管廊监控与报警系统工程技术标准》

GB 14287-2014　《智慧安全用电监控系统》

GB 50116-2013　《火灾自动报警系统设计规范》

GB 50016-2014　《建筑设计防火规范》

GB 28184-2011　《消防设备电源监控系统》

GB 25201-2010　《建筑消防设施的维护管理》

GB 50440-2007　《消防安全远程监控系统技术条件》

GB 16806-2006　《消防联动控制系统》

GB 16806-2006　《消防联动控制系统》

GB 50052　《供配电系统设计规范》

6.4. 福建省智慧消防地方性标准（征求意见稿）

6.4.1. 总则

6.4.1.1. 一般规定

1. “智慧消防”信息平台设计应遵循以下原则：

（1）安全性和可靠性

在设备选择和平台设计中重点考虑安全性和可靠性。平台需具备长期连续稳定工作的能力，满足高可用性设计要求，满足信息技术安全要求，保障平台安全、可靠、稳定。

（2）先进性和实用性

采用成熟先进的技术，技术上要保证一定的前瞻性。总体上保证平台的规范性，按照“业务主导、技术支撑”的定位推进技术与业务深度融合，坚持问题驱动、需求引领，保证平台的实用性。

（3）经济性和合理性

在平台设计中，应在满足当前需求的基础上，确保技术的先进性、可行性和实用性，达到功能与经济相统一的优化设计。尽可能保留和利用原有的硬件、中间件及拥有产权的软件系统，保护已有投资。

（4）集成性和可扩展性

应充分考虑各个子系统的信息共享，确保平台结构的先进性，合理性，可扩展性和兼容性。遵循全面规划的原则，并留有充分的余量，以适应未来发展的需要。

（5）标准性和结构性

应严格按照国家和行业有关标准进行设计和设备配置，保证平台设计的标准化，以及平台结构的合理性。

（6）开放性和自主性

平台设计开放兼容，一方面坚持信息平台接口免费开放，满足各级用户的数据及服务需求；另一方面优先选用自主知识产权的设备和系统，鼓励自主创新，提升自身研发、创新能力，把握发展主导权。

2. 省级层面应统筹“智慧消防”信息平台的规划、设计和建设，统一建设要求

和技术标准，重点实现“智慧消防”信息平台框架搭建、数据支撑能力建立和共性功能应用开发，对市、县（区）级的数据接入、平台应用等工作进行管理和指导。

3．市、县（区）级层面应接入和应用“智慧消防”信息平台，依据省级层面统一技术标准要求和地方标准，重点实现数据接入和平台应用，同时兼顾地域特点和个性需求，开展本级“智慧消防”信息平台的定制化规划、设计和建设，并为各级各类用户提供业务和技术支持。

4．通过“智慧消防”信息平台开展相关业务，不替代社会单位承担消防安全主体责任，不作为追究消防安全执法责任的依据。

5．通过“智慧消防”信息平台开展远程监控相关业务的社会单位，经相关程序审批后，其消防控制室应有至少 1 名持有消防控制室操作职业证书的人员值班。

6.4.1.2. 平台架构

1．“智慧消防”信息平台设计应满足国家应急管理信息化及消防救援信息化相关文件对于体系结构和技术路线的设计要求。

2．“智慧消防”信息平台设计应遵循分层设计原则，包括：感知网络、通信网络、大数据支撑体系、业务应用体系和运行保障体系。平台架构如图 1 所示。

3．感知网络利用智能传感、射频识别、视频图像、红外探测、激光雷达、卫星遥感、航空遥感等感知技术，从多个维度全面感知实体空间信息，为灾害事故发现、研判指挥决策、灾后统计分析、社会单位管理、企业个人服务等具体工作提供客观数据支撑，主要包括：物联感知、卫星感知、航空感知、视频感知、全民感知等。

4．通信网络整合和利用现有的通信设备、通信链路、卫星信道等资源，构建天地一体、全域覆盖、全程贯通的通信网，实现不同类型、不同体制的通信网融合互通，为火灾防控数据采集、应急救援统一指挥提供通信支撑，包括：有线通信网、无线通信网。

5．大数据支撑体系通过汇聚整合各类计算存储资源，提供计算、存储、网络等云资源服务，大数据计算、地图服务、统一认证等通用服务，以及数据接入、清洗、交换共享、管理、分析挖掘等数据处理服务，为业务应用构建和运行提供服务、管理、分析等方面支撑，包括：数据中心、云平台、数据治理、数据交换、数据挖掘。

6．业务应用体系是通过调用数据及服务，集成业务应用系统，构建统一门户，

为政府部门、社会单位、消防技术服务机构、设备厂商、公众个人等各类用户的业务开展提供集成化的应用服务，包括：业务应用系统、统一门户。

7．运行保障体系通过构建安全防护体系和运维管理体系，为信息网络以及应用系统安全、稳定、高效、可靠地运行提供保障，包括：安全防护、运维管理。

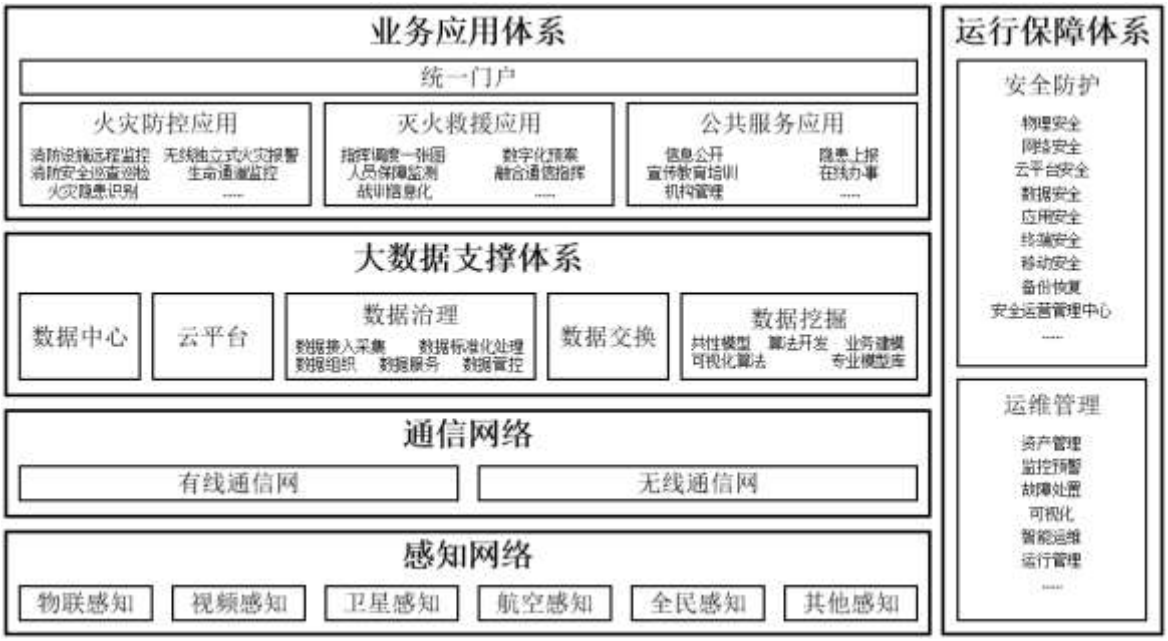


图 “智慧消防”信息平台架构

6.4.1.3. 基本要求

1．“智慧消防”信息平台功能性能设计应符合以下规定：

（1）不得降低原有消防设施的技术性能指标。

（2）不得影响原有消防设施的功能。

（3）不得降低原有消防设施的可靠性。

（4）不得直接对消防设施进行远程控制

2． “智慧消防”信息平台运行环境设置应符合以下规定：

（1）应配备平台运行环境，满足平台性能、环境和信息安全要求。

（2）应具备可靠的平台运行、维护支撑能力。

3．“智慧消防”信息平台支撑保障条件应符合以下规定：

（1）应配备平台运行所需的硬件支撑环境。

（2）应配备平台运维服务所需的人力资源。

6.4.2. 大数据支撑体系

6.4.2.1. 数据中心

1．数据中心应为集中放置计算、存储系统和设备的场所，主要为“智慧消防”信息平台建设提供数据存储、应用部署、安全运维管理等功能。

2. 省级数据中心的机房基础设施应满足《数据中心设计规范》（GB 50174-2017）A 级数据中心标准要求。

3. 省级数据中心灾备系统应满足《信息安全技术 信息系统灾难恢复规范》（GB/T 20988-2013）第 5 级实时数据传输及完整设备支持的要求，生产业务系统和备份业务系统切换时应满足 RPO<30min、RTO<30min 的要求。

4. 市级数据中心的机房基础设施应满足《数据中心电信基础设施标准》（TIA-942）T2 机房标准要求，以及《数据中心设计规范》（GB 50174-2017）B 级数据中心标准要求。

5. 市级数据中心灾备系统应满足《信息安全技术 信息系统灾难恢复规范》（GB/T 20988-2013）第 4 级电子传输及完整设备支持的要求，生产业务系统和备份业务系统切换时应满足 RPO<60min、RTO<60min 的要求。

6．数据中心应具备接入国家电子政务外网和互联网等网络的能力，出口链路带宽应满足业务应用联动和数据汇聚需要，具体性能指标满足《IP 网络技术要求 网络性能参数与指标》（YD/T 1171-2015）要求。

7．数据中心计算资源和网络资源设备应支持通用虚拟化技术。服务器资源设备应支持各项业务应用系统所需的操作系统环境，网络资源设备应支持 IPv6 协议。

6.4.2.2. 云平台

1．云平台应为提供弹性计算服务、存储服务和网络服务的专有云平台，为“智慧消防”信息平台各级用户提供随时、随地、随需、统一的云资源服务。

2．云平台应提供 IaaS 基础设施能力，包括：计算、存储、网络及资源调度管理等基础资源服务。

3．云平台应提供 PaaS 平台服务能力，包括：计算、存储、服务实例、服务资源管理、数据传输交换及作业调度等服务。

4．云平台应具备账号权限管理能力，根据省市区县各级不同需求有针对性提供服务。

5.云平台应满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）中第三级关于安全通用要求、云计算扩展要求等相关内容的要求。

6.云平台应满足《信息安全技术 云技术服务安全能力要求》（GB/T 31168-2014）中关于系统开发、系统通信、访问控制等相关规定的要求。

7.云平台应满足《信息安全技术 大数据服务安全能力要求》（GB/T 35274-2017）中关于数据传输、数据存储、数据交换等规定的要求。

6.4.2.3. 数据治理

1．数据治理应能针对消防业务数据的数据接入采集、数据标准化处理、数据组织、数据服务、数据管控等全生命周期数据整合处理过程提供支撑。

2．数据接入采集应具备数据的获取分发、策略配置、任务配置、任务调度、数据加密、断点续传等能力。

3．数据标准化处理应具备对接入的结构化数据、半结构化数据、非结构化数据等的数据内容进行探查、提取、清洗、转换、脱敏、关联、比对、标识、融合等处理能力。

4．数据组织应按照一定的方式和规则对数据进行归并、存储、处理，形成大数据资源池，包括：原始库、资源库、主题库、专题库等。

5．数据管控应具备对数据资源全生命周期的过程控制和质量监督等能力。

6．数据服务应具备查询检索、数据推送、数据订阅、数据下载、数据可视化、智能标签等数据服务能力。

6.4.2.4. 数据交换

1．数据交换方式应符合以下要求。

（1）数据交换应支持数据库接入、大文件接入和 Web 服务接入。

（2）数据库接入应支持横向表模型和纵向表模型。

（3）大文件接入支持的文件大小应不低于 10MB。

（4）Web 服务接入应提供统一的调用接口。

2．数据交换对象包括政府部门信息系统、社会单位信息系统、消防技术服务机构系统及其他第三方信息系统等，获取的数据资源包括来自政府及其委办局、行业机构、企事业单位及其他主体的数据。各主体应在合法合规的基础上积极开展、配合数据交换相关工作。

3．平台涉及的主要数据交换内容，其内容应满足附录 A 要求。

4．数据交换安全机制应符合以下要求。

（1）应对数据交换的用户身份的真实性进行验证，采用强化管理的口令鉴别、基于令牌的动态口令鉴别、数字证书鉴别等机制进行身份鉴别。

（2）数据传输应采取可靠性协议，保证数据传输的完整性。应能够检测到数据传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

6.4.2.5. 数据挖掘

1．数据挖掘通过构建开放、共享、可扩展、可重构的数据深度分析工具，基于基础数据资源形成主题数据库、专题数据库等，为各类业务应用提供支撑。

2．应支持多源数据的接入，为数据挖掘提供数据支撑。

3．应提供通用的共性模型、算法开发、业务建模、可视化算法等服务。

（1）共性模型宜包括：线性回归、聚类分析、时间序列分析、关联分析、主成分分析、因子分析、逻辑回归、决策树分析、神经网络等。

（2）算法开发应具备用户构建数据集成、预处理、特征工程、算法训练、算法评估等开发流程支撑能力。

（3）业务建模应提供面向火灾防控、应急救援、公共服务等领域业务需求的模型库；应提供用户级业务模型管理，具备多用户的权限管理、协同开发与业务模型共享能力；应具备模型对外的接口，支持业务模型发布。

（4）可视化算法应具备接入数据、模型数据和验证结果数据的多样化展示能力。

（5） 应具备通用服务升级和扩展能力。

4．在通用服务基础上构建专业模型库，为具体业务需求提供数据支撑。专业模型库宜包括：风险评估、隐患识别、事件预警、趋势预测、资源调度等。专业模型库应具备模型升级和规模扩展能力。

6.4.3. 业务应用体系

6.4.3.1. 业务应用系统

1．业务应用系统宜参考业务域开展设计，并应具备拓展能力和演进能力，能够根据业务需求变化和技术发展情况进行迭代升级。

2．火灾防控应用宜包括以下基本功能。

（1）消防设施远程监控应能够对消防设施运行状态信息和消防安全管理信息进行采集、传输、交换、汇聚和处理，为消防部门、社会单位、消防技术服务机构、设备制造商、保险机构等提供数据服务和应用。

（2）无线独立式火灾报警、电动自行车充电桩监控设备、电气火灾预警设备、可燃气体预警设备等应能够为没有设置集中式火灾自动报警系统的小场所提供轻量化火灾报警服务，实现火灾事故的早发现、早报警。帮助消防监管人员决策和治理消防隐患，并为业主、消防责任人、小区物业、消防部门等不同层面用户提供远程预警和管理工具。

（3）消防安全巡查检查应能够为社会单位提供日常消防巡查、故障排查、设备维保等全过程的巡查检查管理功能，并同时提供数据统计、分析、报表生成等功能，实现防火巡查、检查和日常消防安全管理等工作的现场化、移动化、自动化和可溯化，提高巡查检查的质量和效率。

（4）生命通道监控应对消防车道、疏散通道等消防生命通道实时监控，实现目标自动提取、违法行为判定、主动跟踪识别等功能。对发现的封闭、堵塞、占用等异常信息及时报警并推送至相关管理人员，实现消防生命通道畅通的全时监管。

（5）火灾隐患识别应能够基于对多种感知数据的汇聚融合和分析挖掘，智能化识别多种类型的消防安全事件和隐患，实现提前预警和精准定位。

（6）火灾隐患整治应以社会单位火灾隐患排查、防火监督部门火灾隐患核查为主线。对火灾隐患的排查、举报、受理、核实、督办、整改、公布进行全流程精细化管理，实现火灾隐患在举报、核实、排查等环节的社会化协同，社会单位隐患治理能力定量评价，隐患整治任务自动调度等功能。

（7）消防安全评估应能够通过标准化的评价模型和评估方法对基础数据进行规则运算，实时定量评价消防安全风险。计算社会单位的消防安全风险值，确定其风

险等级，发现风险项，指导其改进消防安全管理机制，辅助消防监管部门进行监督管理。

（8） 监督监管机制应能够设置监督监管的抽查范围、抽查事项和抽查细则，合理确定抽查比例和频次，对隐患突出、有严重违法违规记录的单位能够实施重点监督监管。

（9）消防安全社会化服务应能够汇集多个系统模块的相关数据，为个人、社会单位及消防技术服务机构提供信息公开服务、机构管理服务、行政办事服务等一站式、综合性社会化服务。

3．应急救援应用宜包括以下基本功能。

（1）指挥调度一张图应以 GIS 地图为基础，基于统一的底图、统一的图层类型、统一的标注方式、统一的交互逻辑，面向指挥调度展示救援对象、救援力量、周边环境等多方面要素，并可与不同要素间实现通信、指挥、控制、反馈等各种交互操作。

（2）数字化预案应根据突发事件的演化过程，对文本预案进行结构化流程化分解，将事件信息、事件分级、组织机构与职责、监测预警、应急响应、应急资源、应急通讯录等要素与流程关联，并基于二维或三维地图、城市信息建模、建筑信息建模等技术进行可视化展示。

（3）人员保障监测应通过模块化单兵装备采集一线救援人员的位置、体征、周边环境参数、周边音视频、防护设备可用时间等数据，并提供实时监测、时段统计、危险等级分析、危险提示等功能。

（4）融合通信指挥应在一个网络平台上融合电话业务、短消息业务、会议电话、呼叫中心等传统电信业务，即时通信、IP 电话等 IP 类业务，视频监控、信息共享等视频和应用类业务，电子邮件、语音邮件等互联网业务，实现不同模式通信手段的统一化服务支撑。

（5）战训信息化应以受训人员为核心建立电子档案，将人员身体基本情况、机能情况、训练计划、训练科目、训练过程、训练结果等要素电子化、信息化，提供身体状态监测、训练计划管理、训练效能评估等功能。

（6）队伍管理应针对消防部门各类人员、车辆、装备等，采集人员基本信息、车辆基本信息、装备基本信息等静态信息以及人事信息、车辆位置、速度、随车装

备、驾驶人员、周边路况、装备出入库、装备维护保养等动态信息，并基于相关数据提供人员管理、车辆位置追踪、出勤路线规划、装备维保建议等功能。

4．公共服务应用宜包括以下基本功能。

（1）基于多渠道融合进行统一的信息发布，依法依规通过网站、微信、微博、短视频等不同类型平台向公众公开消防安全相关信息。

（2）在网站、微信、微博、短视频等不同类型平台提供隐患上报入口，支持文字、图片、语音、视频、位置等多种类型数据，供公众上报各类火灾隐患情况。

（3）面向公众、社会单位管理人员、消防技术服务机构从业人员、其他技术技能人员等不同类型不同需求受众，通过图文、音视频、文档等多种形式，提供科普知识、基础知识、专业知识等不同深度的宣传教育培训材料。

（4）针对社会单位、消防技术服务机构、设备厂商、公众个人的办事需求，提供各类行政事项的流程化办理入口，并可实时查看办理动态、咨询办理细节、了解办理结果。

（5）针对消防技术服务机构、设备厂商等，提供机构台账、资质管理、从业管理等服务。

6.4.3.2. 统一门户

1．统一门户为管理信息资源并提供有关信息服务的应用系统，用户通过认证，即可获得各项信息及应用的授权访问，由面向政府和面向社会两个部分组成，支持PC 端、移动端、大屏显示终端等多种服务方式。

2．统一门户应采用统一的名称、域名、标识和视觉体系。

3．统一门户应支持自定义门户，可根据需求进行裁剪。

4．统一门户应具备统一认证、统一用户管理等能力。

5．统一门户应具备单点登录能力。

6．统一门户应满足用户正常登录使用要求。

6.4.4. 运行保障体系

6.4.4.1. 安全防护

1．安全防护通过全面落实国家网络安全等级保护制度，建立全面立体的安全防

护体系，为“智慧消防”信息平台的网络信息体系提供多层次、全维度的安全防控。应满足《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）中第三级基本技术的要求，满足国家密码管理局对密码使用和管理的相关要求。

2．安全防护认证授权和密码服务应具备身份管理、PKI/CA 体系、权限管理和密码管理等技术手段进行安全防护。

3. 物理安全应保证省级数据中心机房满足《数据中心设计规范》（GB 50174-2017）A 级数据中心要求，市级数据中心机房不低于《数据中心设计规范》（GB 50174-2017）B 级数据中心要求；应保证设备的防盗和防毁、防止电磁信息泄露、防止线路截获、抗电磁干扰、电源保护等。

4．网络安全应保证网络架构安全；应具备指挥信息网安全防护能力；应具备数据中心边界接入安全和数据交换安全能力；应提供全网流量监测、审计和分析能力。

5．云平台安全应提供云计算平台基础安全加固，云计算平台承载的主机、应用和数据的安全防护，云管理平台安全防护等能力。

6．数据安全基于数据分类分级规范，应具备数据可视、防护、审计和风险分析能力，保障数据全生命周期安全；应具备异地实时数据备份功能；重要数据在传输和存储过程中应采用校验技术或密码技术保证完整性和安全性；应具备数据脱敏能力。

7．应用安全应具备贯穿应用系统全生命周期的安全机制，在应用需求分析、系统设计、功能编码、系统测试、上线部署、运行监视和下线撤销等阶段，应提供应用安全防护能力。

8．终端安全应提供终端基础架构安全、纵深防御安全执行、零信任业务访问授权安全；终端基础架构安全应具备终端软硬件监测、终端准入注册能力；终端纵深防护应具备恶意代码防护、补丁管理、数据防泄漏、威胁分析等能力；业务访问控制应具备安全状态感知、身份识别能力。

9．移动安全应提供移动终端安全、移动网络接入安全、移动数据和应用安全以及移动终端安全管理等能力。

10．备份恢复应能提供重要数据的本地备份恢复功能，应提供异地实时备份功能，应提供重要系统的热冗余。

11．安全运营管理中心应提供安全数据采集、预处理、智能分析、安全应用和

安全可视化等能力；应支持多源异构海量安全数据的收集、汇总、处理、分析、呈现等，提供资产、威胁、脆弱性的相关管理，并能提供对威胁的事前预警、事中发现、事后回溯等能力，通过可视化手段感知全网安全态势及重要安全威胁。

12．应建立安全管理组织机构和人员团队，制定信息基础设施保护、安全审查、安全测评和风险评估等制度，形成由安全策略、安全机构、操作规程、管理制度等构成的安全管理机制

6.4.4.2. 运维管理

1．运维管理通过建立完善的运维管理制度和运维反应机制，构建科学智能的运维管理体系，保障信息网络以及业务应用系统稳定、高效、可靠地运行。

2．资产管理应具备数据中心的物理资源、虚拟资源、软件资源及应用系统等配置信息管理能力。

3．监控预警应具备集中统一的 IT 资源监控管理与告警管理，支持数据中心环境监控、云管理平台监控、应用性能监控等能力。

4．故障处置应具备故障处置能力，支持故障诊断和调度管理。

5. 可视化应具备运维可视化能力，支持多维度资产画像构建、资产可视化分析、运维统计报表可视化管理、单工分析可视化管理等能力。

6．智能运维应具备智能语音交互、告警功能的智能判断与统计分析等智能交互和分析能力。

7．运行管理应建立健全平台运行情况的日报、月报和年报机制。

6.4.5. 附表

6.4.5.1. 单位信息表

字段中文名	类型	是否必填	字段描述
统一社会信用代码	字符串	是	主键
单位名称	字符串	是	
单位地址	字符串	是	
单位类别	对象型	是	包括数据项值、数据项内容
单位属性	对象型	是	包括数据项值、数据项内容、数据项条链
单位概述	字符串	否	

单位概况图	字符串	否	图片 Url
火灾危害性	对象型	否	包括数据项值、数据项内容
火灾隐患性	对象型	否	包括数据项值、数据项内容
经度	浮点型	否	精确到小数点后 6 位
纬度	浮点型	否	精确到小数点后 6 位
单位成立时间	日期型	否	格式：yyyy-MM-dd
通过消防验收时间	日期型	否	格式：yyyy-MM-dd
主要危害	对象型	否	包括危害物质、危害概述、防护要求、存放位置
消防安全责任人	对象型	否	包括人员类型、人员姓名、身份证号、联系电话
消防安全管理人	对象型	否	包括人员类型、人员姓名、身份证号、联系电话
分管等级	对象型	否	包括数据项值、数据项内容
图片信息	字符串	否	包括图片 ID、图片名称（文件名称）、图片后缀（全部大写）、图片描述、图片地址 Url、图片类型 ID、图片类型名称
文本预案	对象型	否	包括预案类型、预案名称、预案文件、URL 地址、存储地址
结构化预案	对象型	否	包括预案类型、预案名称、预案文件、URL 地址、存储地址
数字化预案	对象型	否	包括预案类型、预案名称、预案文件、URL 地址、存储地址
关联建筑情况	对象型	否	包括建筑编号、建筑名称
关联建筑概述	字符串	否	
周边毗邻情况	对象型	否	包括方向类型、方向描述
周边毗邻概述	字符串	否	
灭火演练情况	对象型	否	包括演练时间、演练地点、演练概述、演练文件
灭火演练概述	字符串	否	
灭火逃生疏散预案	对象型	否	包括预案名称、预案概述、预案文件
消防设施情况	对象型	否	包括设施名称、设施位置、设施数量、设施概述
消防设施概述	字符串	否	
执法监督情况	对象型	否	包括监督时间、监督概述、监督文件
执法监督概述	字符串	否	
历史灾情情况	对象型	否	包括灾情编号、发生时间、灾情概述、处置概述、处置文件
历史灾情概述	字符串	否	
灾情处置对策	对象型	否	包括灾情类别、灾情名称、对策概述、对策文件
灾情处置概述	字符串	否	
消防队站	对象型	否	包括消防队站形式、消防队站编号、消防队站名称
所在地消防机构	对象型	是	包括消防机构编号、消防机构名称、消防机构内部编码
所在地行政区划	对象型	是	包括行政区划编号、行政区划名称、行政区划内部编码
维保单位	字符型	是	
维保报告	文件型	是	
下次维保时间	日期型	是	格式：yyyy-MM-dd

记录状态	布尔型	是	
入库人员	字符串	是	
入库时间	日期型	是	格式：yyyy-MM-dd HH:mm:ss
更新人员	字符串	是	
更新时间	日期型	是	格式：yyyy-MM-dd HH:mm:ss

6.4.5.2. 建筑信息表

字段中文名	类型	是否必填	字段描述
建筑编号	字符串	是	主键
建筑名称	字符串	是	
建筑地址	字符串	是	
建筑概述	字符串	否	
建筑概况图	字符串	否	图片 Url
建成日期	日期型	否	格式：yyyy-MM-dd
建筑高度	浮点型	否	单位：米
建筑深度	浮点型	否	单位：米
地上层数	整数型	否	单位：层
地下层数	整数型	否	单位：层
建筑面积	浮点型	否	精确到小数点后 2 位
最大单层面积	浮点型	否	精确到小数点后 2 位
是否大型综合体	布尔型	否	
建筑结构	对象型	否	包括数据项值、数据项内容
建筑类别	对象型	否	包括数据项值、数据项内容、数据项条链
建筑用途	对象型	否	包括数据项值、数据项内容、数据项条链
耐火等级	对象型	否	包括数据项值、数据项内容
图片信息	字符串	否	包括图片 ID、图片名称（文件名称）、图片后缀（全部大写）、图片描述、图片地址 Url、图片类型 ID、图片类型名称
文本预案	对象型	否	包括预案类型、预案名称、预案文件、URL 地址、存储地址
结构化预案	对象型	否	包括预案类型、预案名称、预案文件、URL 地址、存储地址
数字化预案	对象型	否	包括预案类型、预案名称、预案文件、URL 地址、存储地址
经度	浮点型	否	精确到小数点后 6 位
纬度	浮点型	否	精确到小数点后 6 位
外墙保温材料	字符串	否	
保温材料类别	对象型	否	包括数据项值、数据项内容
主要危害	对象型	否	包括危害物质、危害概述、防护要求、存放位置
负责人员	对象型	否	包括人员类型、人员姓名、身份证号、联系电话

入驻重点单位	对象型	否	包括单位编号、单位名称
消防控制室（地下）	对象型	否	包括位置信息、联系人员、联系电话
周边毗邻情况	对象型	否	包括方向类型、方向描述
周边毗邻概述	字符串	否	
灭火演练情况	对象型	否	包括演练时间、演练地点、演练概述、演练文件
灭火演练概述	字符串	否	
灭火逃生疏散预案	对象型	否	包括预案名称、预案概述、预案文件
消防设施情况	对象型	否	包括设施名称、设施位置、设施数量、设施概述
消防设施概述	字符串	否	
执法监督情况	对象型	否	包括监督时间、监督概述、监督文件
执法监督概述	字符串	否	
历史灾情情况	对象型	否	包括灾情编号、发生时间、灾情概述、处置概述、处置文件
历史灾情概述	字符串	否	
灾情处置对策	对象型	否	包括灾情类别、灾情名称、对策概述、对策文件
灾情处置概述	字符串	否	
消防队站	对象型	否	包括消防队站形式、消防队站编号、消防队站名称
所在地消防机构	对象型	是	包括消防机构编号、消防机构名称、消防机构内部编码
所在地行政区划	对象型	是	包括行政区划编号、行政区划名称、行政区划内部编码
记录状态	布尔型	是	
入库人员	字符串	是	
入库时间	日期型	是	格式：yyyy-MM-dd HH:mm:ss
更新人员	字符串	是	
更新时间	日期型	是	格式：yyyy-MM-dd HH:mm:ss

6.4.5.3. 感知信息表－火灾自动报警系统感知

字段中文名	类型	是否必填	字段描述
设备号	整数型	是	
设备名称	字符串	是	
注释	字符串	是	
设备类型	字符串	是	
设备状态	字符型	是	包括正常、故障、报警等
感知上报日期	日期型	是	默认为当前时间

6.4.5.4. 感知信息表－电气系统感知

字段中文名	类型	是否必填	字段描述
设备号	整数型	是	
设备名称	字符串	是	

注释	字符串	是	
设备类型	字符串	是	
设备状态	字符型	是	包括正常、故障、报警等
感知上报日期	日期型	是	默认为当前时间

6.4.5.5. 感知信息表－社会单位消防视频监控感知

字段中文名	类型	是否必填	字段描述
设备号	整数型	是	
设备名称	字符串	是	
注释	字符串	是	
设备类型	字符串	是	
设备状态	字符型	是	包括正常、故障、报警等
感知上报日期	日期型	是	默认为当前时间

6.4.5.6. 感知信息表－消防水系统感知

字段中文名	类型	是否必填	字段描述
设备号	整数型	是	
设备名称	字符串	是	
注释	字符串	是	
设备类型	字符串	是	
设备状态	字符型	是	包括正常、故障、报警等
感知上报日期	日期型	是	默认为当前时间

6.4.5.7. 感知信息表－无人机综合感知

字段中文名	类型	是否必填	字段描述
设备号	整数型	是	
设备名称	字符串	是	
注释	字符串	是	
无人机类型	字符串	是	
感知上报日期	日期型	是	默认为当前时间
可见光数据	浮点型	是	
气体浓度数据	浮点型	是	
三维视频数据	浮点型	是	

6.4.5.8. 感知信息表－值班状态感知

字段中文名	类型	是否必填	字段描述
人员编号	整数型	是	
姓名	字符串	是	
注释	字符串	是	

人员类型	字符串	是	
感知上报日期	日期型	是	默认为当前时间
上岗时间	日期型	是	
下岗时间	日期型	是	
在岗状态	布尔型	是	

6.4.5.9. 感知信息表－装备物资状态感知

字段中文名	类型	是否必填	字段描述
设备编号	字符串	是	
设备名称	字符串	是	
注释	字符串	是	
设备类型	字符串	是	
设备状态	字符型		
感知上报日期	日期型	是	默认为当前时间

6.4.5.10. 感知信息表－公共水资源状态感知

字段中文名	类型	是否必填	字段描述
设备号	整数型	是	
设备名称	字符串	是	
注释	字符串	是	
设备类型	字符串	是	
感知上报日期	日期型	是	默认为当前时间
水源水位	浮点型	是	
水源流速	浮点型	是	
水源流量	浮点型	是	
水源水温	浮点型	是	

6.4.5.11. 感知信息表－救援人员感知

字段中文名	类型	是否必填	字段描述
人员编号	整数型	是	
姓名	字符串	是	
注释	字符串	是	
人员类型	字符串	是	
感知上报日期	日期型	是	默认为当前时间
音视频数据	流媒体型	是	
气象状态数据	字符串	是	
周边物体数据	字符串	是	
生命体征数据	字符串	是	
位置数据	字符串	是	

6.5. 总体架构图

参考《国家电子政务总体框架》的有关要求，结合当前全省消防监管现状的实际情况及发展需求，本项目系统的总体架构采用 SOA（面向服务架构）分层模式进行设计，如下图所示：

第7章 项目数据架构设计

7.1. 数据架构整体设计

7.1.1. 建设目标

基于数字福建总体框架，福建省智慧消防云平台为基础，以“云+集成+服务”为核心，构建全省消防专题数据及全省消防业务数据整体框架，接入省基础数据库数据、省公共信息资源数据、国家知网数据、省内重点行业消防调查数据、消防社情民意数据、互联网数据等八个大类数据资源，构建智慧消防云平台大数据中心，提供多源异构数据的统一接入汇集、组织存储管理、综合处理等功能，能够实现基于智慧消防云平台多源数据服务的共享分发，也能够提供全省各级消防网站分发门户，面向各级消防部门、消防相关单位、社会机构及个人提供更广阔的数据分发服务功能；整体提高智慧消防平台的数据资源应用水平，逐步形成省市县三级覆盖的消防业务数据资源体系。具体建设目标为：

（1）打通多源数据的接入链路，促进多源异构数据资源在智慧消防云平台的应用；

（2）充分利用省消防救援总队现有相关系统的数据资源，促进消防专题数据、业务数据资源的多层次融合分析和共性产品综合处理，进一步提升现有信息资源的使用效能；

（3）形成多源异构数据“数据需求－数据接入－数据存档－数据处理－数据管理－数据分发”在“互联网+消防”应用领域的完整链条，具备消防大数据产品的生产、服务和管理能力，提升智慧消防数据资源应用能力和服务能力；

（4）基于智慧消防资源共享平台，面向消防的政务应用、社会消防服务，构建基于 web 端、移动端及数据大厅的信息分级服务能力，实现消防政务与服务的链接。

7.1.2. 建设任务

1．全省通用消防数据标准规范制定：要实现全省智慧消防的应用统一、数据统一，首先的一项前置条件就是进行全省消防数据统筹，建立全省通用消防数据标准

规范，让所有已建、未建智慧消防系统平台的各级消防主管部门，共同遵守该数据标准规范，有利于后续福建省智慧消防云平台的开发建设、数据汇聚、数据共享，从一开始就消除消防大数据中心的建设壁垒。全省通用消防数据标准规范的制订，属于项目开展建设的一部分，在本可研设计方案中仅提出部分必要的、常用的数据对象和属性字段，详细标准的调研、设计与制订应由项目主办方和承建方根据项目具体情况而具体实施。

2．建立数据获取机制：打通智慧消防云平台大数据中心与福建省相关委办厅局之间的数据传输通道，解决智慧消防的数据来源；

3．研制数据管理应用系统：数据管理系统负责管理各类数据，从现有业务系统获取的智慧消防业务数据，其他部门业务数据以及本系统生产的智慧消防专题产品数据等相关数据资源；

4．建立数据产品分发服务机制：通过消防应急通信网、政务专网或外网，基于数据产品分发系统和网络服务系统的建设，为不同用户提供数据标准化产品和基础专题产品的订阅推送、在线下载以等数据产品共享分发服务；

5、建立信息分级服务体系，面向全省各级消防部门的政务应用、社会消防服务，构建基于 web 端、移动端及数据大厅的信息分级服务能力。

7.1.3. 主要功能

智慧消防云平台大数据中心的具体功能主要包括数据请求审批与管理功能、数据接入功能、数据可视化显示功能、数据处理功能、数据管理与动态融合、数据推送服务功能、数据共享服务功能和产品展示发布功能，具体内容如下：

（1）数据请求审批与管理功能：完成智慧消防大数据中心向相关委办厅局提交数据申请，完成各级消防部门向智慧消防大数据中心提交的数据申请，中心将根据数据请求内容、请求级别等信息进行订单处理、后续跟踪及信息反馈；同时中心将对数据请求工单进行统一的存储、归档管理；

（2）数据接入功能：完成福建省相关委办厅局获取数据及智慧消防云平台相关系统业务数据的统一接入和规范化入库功能；

（3）空间处理功能：对实时在线、定期在线和离线拷贝的结构化、非结构化的时空大数据，序化前的处理工作包括统一格式、一致性处理和空间化。

（4）管理分析功能：包括动态数据获取、数据管理、大数据挖掘、大数据管理等。

（5）数据管理功能：负责管理获取的原始产品数据、现有业务系统获取的智慧消防专题数据、业务数据、专题产品数据等相关数据资源，实现对数据及产品的编目存档、组织管理、更新和维护等内容。通过把多源、多尺度空间数据集成、融合、尺度变换等新技术引入当前智慧消防云平台空间框架建设实践中，系统地研究多尺度和多源空间数据融合与模型同化、多尺度空间数据的智能化生成、多尺度动态空间数据快速变化检测与实时更新方法以及多尺度空间数据的多样化表达等关键技术，解决消防空间数据一体化获取、处理与更新的问题，为智慧消防实现真正的智能打下坚实的物质基础。

（6）数据推送功能：实现向“智慧消防一张图”推送综合专题产品；向现有业务系统推送接入的专题信息产品及数据产品；

（7）数据共享服务功能：实现对外发布各类智慧消防云平台专题产品的服务功能，实现智慧消防平台各类数据产品的统一展现及服务，为行业用户提供一站式的智慧消防专题产品服务，构建“智慧消防一张图”的综合服务体系；

（8）产品展示发布功能：通过与智慧消防云平台的接口实现入库产品的展示、实时发布功能。

7.1.4. 技术指标

（1）存储容量可支持 PB 级，支持数据备份与恢复；

（2）支持用户并发不少于 1000 个；

（3）元数据检索平均响应时间：<3 秒；

（4）访问控制：鉴权性能≥500 次/秒。

7.2. 数据结构设计

7.2.1. 数据设计要求

数据库设计应考虑数据库的转储和恢复，数据库的安全性、完整性控制，数据库性能的监督、分析和改进，以及数据库的重组织和重构造。

（1）主要设计内容

系统数据的逻辑结构共分为两层，即数据库、数据表。数据库包含若干个数据表。

（2）存储、更新机制

信息化工程的数据采用集中的方式进行存储。数据更新机制采用适时更新的方式进行。

（3）主要设计要求

为了提高数据库应用系统的性能，通常以规范化理论为指导，还应该适当地修改、调整数据模型的结构，也就是数据模型的优化。确定数据依赖；消除冗余的联系；确定各关系模式分别属于第几范式；确定是否要对它们进行合并或分解。

7.2.2. 数据库表设计步骤

本项目数据库设计总体分为五个步骤，即：需求分析阶段、概念结构设计阶段、逻辑结构设计阶段、数据库物理设计阶段、验证及优化阶段。详细如下：

（1）需求分析阶段

需求分析阶段需要了解系统的业务流程，从基础信息和业务信息应用的角度考虑需要哪些数据。

（2）概念结构设计阶段

概念结构设计阶段是将需求分析阶段整理的数据需求进行高度抽象，形成独立关系型数据库的概念模型。这些概念模型通常以 E-R 图的形式表现，反映不同系统主体之间存在的各种关系。

（3）逻辑结构设计阶段

逻辑结构设计阶段就是将概念结构设计阶段形成概念模型转化为数据模型。在这个阶段的设计中，经常会使用一些相关的计算机辅助设计工具，如 PowerDesigner 等。在将概念模型转化为数据模型时，需要考虑数据库设计的范式要求，根据数据模型之间的关联关系确立主键和外键。数据模型在包含概念模型的基本属性（最终会对应为数据库表字段）的基础上，应充分考虑横向及纵向的可扩展性，并为此增加数据模型的相应字段。

（4）数据库物理设计阶段

数据库物理设计主要是为逻辑数据模型选取一个最适合应用环境的物理结构。在对数据库进行物理设计时，关键环节在于对数据量的概算，从而确定分区及表空间等的划分原则。

（5）验证及优化阶段

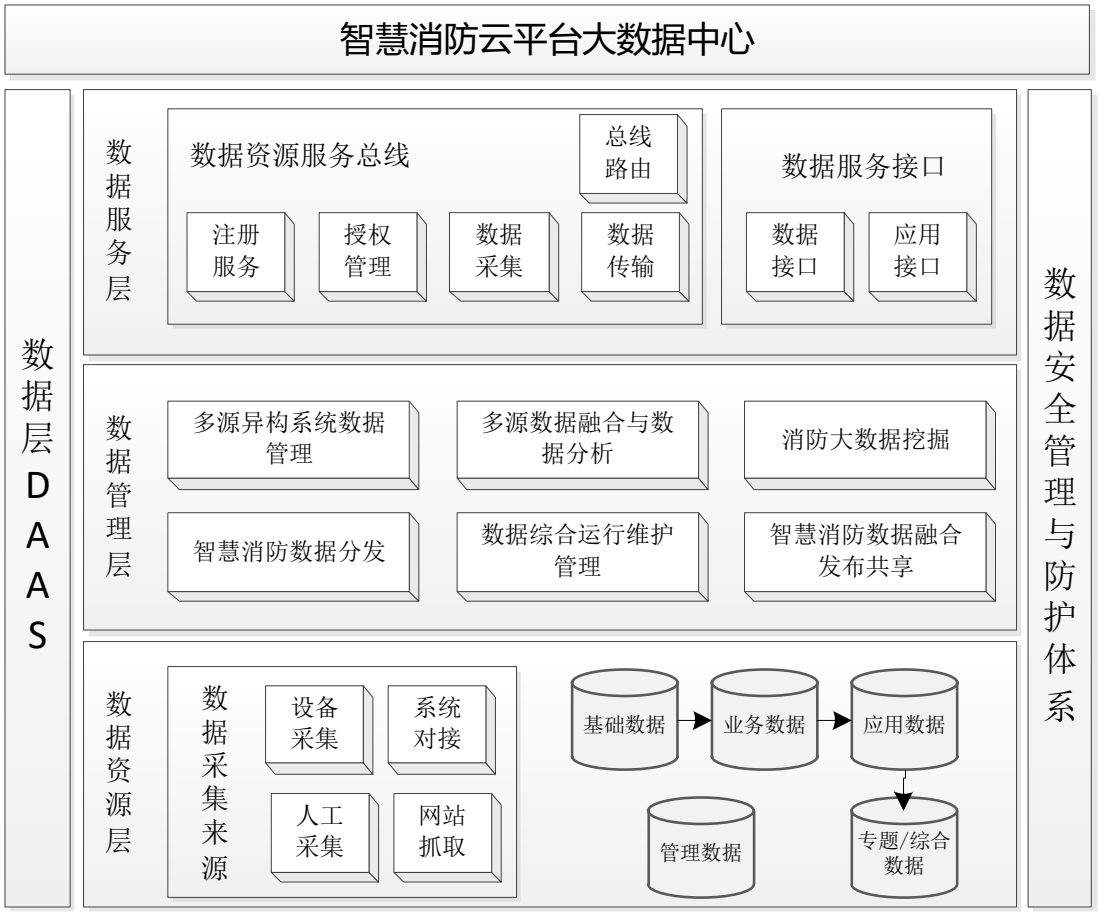
验证及优化阶段是对已经建立好的数据库进行验证和优化。验证主要是测试各部门信息系统中的数据是否可以关联为前期设计好的基础信息和业务信息，关联的过程中是否会造成关键业务环节及其他重要信息的缺失。在验证完成后，针对基础信息和业务信息数据库业务应用的特点以及上层数据库的设计规则优化基础数据库的性能，这些优化主要指数据表的合并与拆分、数据库索引的设计等。

7.2.3. 数据设计思路

按照“统一集中、高度共享”的思路和“一数一源、准确唯一”的原则，建成数据标准统一的数据资源中心，最终实现数据和业务应用的相对分离。通过建立数据资源目录、落实源头数据采集责任，强力推进数据共享，规范经济预测业务应用的数据采集内容和数据标准，确保从源头上避免数据的不一致、重复采集等问题，减轻基层工作人员负担，确保数据鲜活准确。

7.2.4. 数据资源总体架构图

数据资源中心的建设划分为 3 个层次，数据资源层、数据管理层和数据服务层，实现数据与业务应用的相对分离，发挥数据中心资源数据分析和数据挖掘的能力，为后续的大数据分析奠定数据基础。



7.2.5. 数据资源目录体系

数据资源目录体系有 6 个主要功能：资源规划、资源编目、资源注册、资源发布、资源访问、资源维护、资源获取等功能。

7.2.5.1. 资源规划

各部门的提供者按照其管理范围和职责权限梳理、规划信息资源的内容和目录，制定本部门的信息目录体系建设计划。结合本部门信息资源特点定义适合本部门的元数据。依据信息资源分类要求，设计分类方案。各单位应按照主题分类对公共资源和交换资源进行划分，也可以根据需要选用其他一种或多种分类（包括行业分类、服务分类和资源形态分类）。

建立包含但不限于：消防监管执法数据、消防物联网监测数据、技术服务单位数据、消防服务数据、社会消防数据、消防相关政策新闻及宣传信息等一系列资源目录体系。

7.2.5.2. 资源编目

部门的提供者按照规划中设定的元数据标准对共享福建省智慧消防平台数据中心信息资源进行目录编辑、提取元数据，形成目录内容。

1．根据信息资源核心元数据标准对信息资源提取相关特征信息，并在此基础上结合具体业务适当增加所需元数据，形成本部门信息资源元数据；

2．根据信息资源标识符编码标准，向目录管理机构申请本部门信息资源的标识符编码，并对元数据中的标识符信息进行赋值；

3．根据信息资源分类标准对元数据中的分类信息进行赋值；

4．对目录内容设置适当权限。

7.2.5.3. 资源注册

提供者将编目形成的元数据通过元数据注册系统向目录中心的管理机构注册。

1．提交：通过管理机构和提供者之间的网络平台，实现元数据的提交；

2．审核：通过相应的审核系统，管理机构确认提供者提交的信息资源元数据格式及内容是否符合标准要求，未通过审查的元数据返回给提供者修改。对于提供者未对信息资源唯一标识符赋码，由管理者进行赋码。

3．入库：对于通过审核的元数据，实现元数据的入库管理，形成正式目录。这里的库是指管理者向使用者提供信息资源目录服务的元数据库。

7.2.5.4. 资源发布

管理者把目录内容对我发布，目录即可供政务部门和社会公众使用了。目录外部展现方式是一站式服务系统。管理者可以特定的元数据是否可对外服务。面向政务门发布的目录以主题分类为主，面向社会公众发布的目录可以选用服务分类。

经过审核的元数据进入元数据库，各级目录中心管理机构按照规定的核心元数据标准，自动或手动抽取核心元数据放入本级目录中心核心元数据库中，作为目录展现的基础。下级目录中心提取本级中心的核心元数据发布到上级目录中心的核心元数据库中，并且发布目录中心的地址信息，包括目录中心的名称和网络位置标识符 URL（UniformResourceLocator，统一资源定位符）。各级目录中心管理机构根据

已注册的元数据生成、发布并维护目录内容。

7.2.5.5. 资源查询

使用者向一站式服务系统发送目录查询请求，一站式服务系统根据查询条件和用户权限将查询结果返回给使用者。提供多种查询功能：按照主题分类、部门分类等多种方式查询；按照单条件查询；按照组合条件查询。

用户通过消防信息资源目录体系查询系统向目录服务器发送目录查询请求，目录服务器根据查询条件和用户权限将查询结果返回给使用者。

7.2.5.6. 资源维护

对元数据库的建立、更新、备份和恢复；对元数据的修改、删除和注销等；服务监控：监控各种服务器的运行；日志分析：根据查询日志，统计访问系统的次数，统计分析不同信息资源的查询次数等；用户评分与反馈：管理使用者对目录的评分及反馈意见，并与提供者进行协调；辅助管理系统：安全认证服务器，邮件服务器等辅助系统的运行管理。

建立智慧消防云平台数据中心信息资源元数据库、核心元数据库和目录，并进行定时更新、备份与恢复，入库与出库；对目录服务器、消防大数据中心行业信息专网网站的运行进行监控；根据查询日志，统计访问系统的次数，统计分析不同信息资源的查询次数等。

7.2.5.7. 资源获取

使用者根据目录查询得到的定位信息，通过智慧消防云平台数据中心资源数据中心提供的数据共享服务获取信息，用户可以通过网络浏览、查询、交换等各种方式从数据共享服务获取消防信息资源。

7.2.5.8. 目录审核

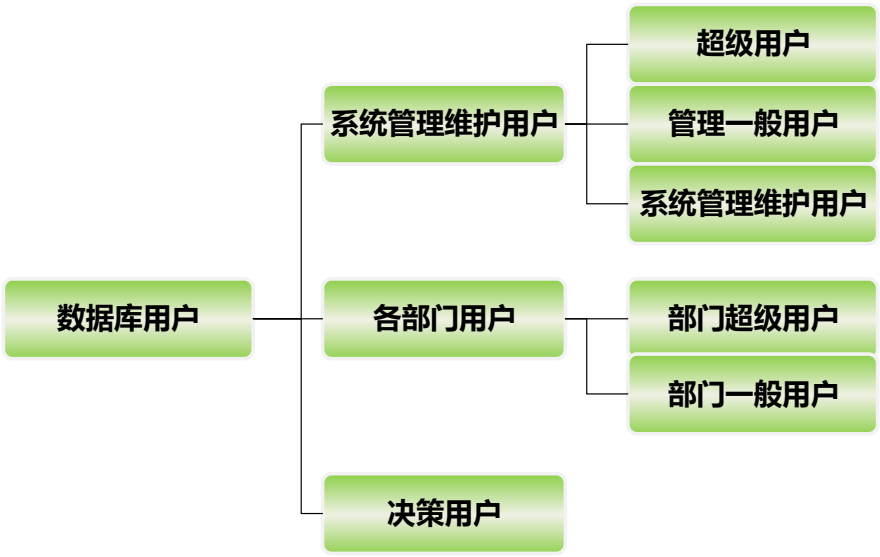
针对新增或规划外的消防数据资源目录要列入平台整体资源目录结构中，必须对新增资源目录进行程序化审核，审核通过后才可建档入库。

7.2.6. 数据库安全管理

核心数据库管理采用 RBAC（角色访问控制）的基本思想，可简单地用用户－－角色－－权限来表示，即把整个访问控制过程分成两步：访问权限与角色相关联，角色再与用户关联，从而实现了用户与访问权限的逻辑分离；由于 RBAC 实现了用户与访问权限的逻辑分离，因此它极大的方便了权限管理。例如，如果一个用户的职位发生变化，只要将用户当前的角色去掉，加入代表新职务或新任务的角色即可，角色/权限之间的变化比角色/用户关系之间的变化相对要慢得多，并且委派用户到角色不需要很多技术，可以由行政管理人员来执行，而配置权限到角色的工作比较复杂，需要一定的技术，可以由专门的技术人员来承担，但是不给他们委派用户的权限，这与现实中情况正好一致。实现权限控制的基本思想是：根据 RBAC 的基本原理，给用户分配一个角色，每个角色对应不同模块的不同权限，同一个用户可属于不同的角色，对模块的操作权限取用户所属几个角色的最高权限。

数据库安全设计通过权限角色管理的方式来实现，权限管理分为数据权限与功能权限，对应角色就有数据管理角色与功能管理角色，不同的角色具有不同的权限，不同的用户根据实际应用情况可以隶属于一个或多个角色，以此来实现用户的权限分配。

根据本项目数据库管理的业务需求，数据库的用户层次主要分为决策用户、各部门用户和系统管理维护用户三个大的类型。每个类型下面根据用户的业务性质和应用的需求，可以分为多级用户，每级用户享有不同的对系统数据库访问和操作的权限。



根据系统用户的划分，基础数据库的用户主要分为三级用户，即超级用户、中级用户和一般用户。

7.3. 数据资源层设计

7.3.1. 数据资源层设计原则

按照“统一集中、高度共享”的思路和“一数一源、准确唯一”的原则，建成数据标准统一的消防资源数据库，建成汇集消防基础数据和业务数据的消防资源数据库，最终实现数据和业务应用的相对分离。通过建立数据资源目录、落实源头数据采集责任，强力推进数据共享，规范消防监管的数据采集内容和数据标准，做到“谁采集、谁录入、谁负责”，确保从源头上避免数据的不一致、重复采集等问题，减轻基层工作人员负担，确保数据鲜活准确。

7.3.2. 数据资源层

本次项目的数据资源主要由基础数据库、业务数据库、应用数据库、综合数据库和管理数据库组成。

7.3.2.1. 基础数据库

7.3.2.1.1. 联网火灾风险单位

序号	数据项	数据类型	长度	说明
1	单位名称	字符型	70	
2	组织机构代码	字符型	9	
3	单位类别	字符型	2	
4	所属区域	字符型	6	
5	单位详址	字符型	40	
6	联系电话	字符型	18	
7	联网状态	字符型	30	
8	邮政编码	数字型	18	
9	消防控制室电话	字符型	18	
10	消防安全责任人姓名	字符型	30	
11	消防安全责任人公民身份号码	字符型	18	
12	消防安全责任人电话	字符型	18	
13	消防安全管理人姓名	字符型	30	
14	消防安全管理人公民身份号码	字符型	18	
15	消防安全管理人电话	字符型	18	
16	专兼职消防管理人姓名	字符型	30	
17	专兼职消防管理人公民身份号码	字符型	18	
18	专兼职消防管理人电话	字符型	18	
19	法定代表人姓名	字符型	30	
20	法定代表人公民身份号码	字符型	18	
21	法定代表人电话	字符型	18	
22	职工总人数	数字型	10	
23	成立时间	日期型	8	
24	上级主管单位名称	字符型	70	
25	管辖单位名称	字符型	70	
26	经济所有制	字符型	3	
27	固定资产	数值型	10	
28	单位占地面积	数值型	10	
29	总建筑面积	数值型	10	
30	入网日期	日期型	8	
31	监管等级	字符型	1	

32	单位总平面图	二进制		
33	单位所属中心名称	字符型	70	

7.3.2.1.2. 建/构筑物

序号	数据项	数据类型	长度	说明
1	建、构筑物名称	字符型	40	
2	建、构筑物类别	字符型	2	
3	建造日期	日期型	8	
4	使用性质	字符型	2	
5	火灾危险性	字符型	1	
6	耐火等级	字符型	1	
7	结构类型	字符型	1	
8	建筑高度	数值型	6	
9	建筑面积	数值型	10	
10	占地面积	数值型	10	
11	标准层面积	数值型	10	
12	地上层数	数值型	3	
13	地上层面积	数值型	10	
14	地下层数	数值型	3	
15	地下层面积	数值型	10	
16	隧道高度	数值型	6	单位：m，精确到小数点后 2 位
17	隧道长度	数值型	10	单位：m，精确到小数点后 2 位
18	消防控制室位置	字符型	50	
19	避难层数量	数值型	3	
20	避难层总面积	数值型	10	单位：㎡
21	避难层位置	字符型	50	
22	安全出口数量	数值型	3	
23	安全出口位置	字符型	50	
24	安全出口形式	字符型	50	
25	消防电梯数量	数值型	3	
26	消防电梯容纳总重量	数值型	10	单位：kg
27	日常工作时间人数	数值型	10	
28	最大容纳人数	数值型	10	
29	储存物名称	字符型	40	

30	储存物数量	字符型	40	
31	储存物性质	字符型	40	
32	储存物形态	字符型	40	
33	储存容积	数值型	10	单位：m^3
34	主要原料	字符型	100	
35	主要产品	字符型	100	
36	毗邻建筑物情况	字符型	500	
37	建筑立面图	二进制		
38	消防设施平面布置图	二进制		
39	建筑平面图	二进制		
40	建筑物所属单位名称	字符型	70	

7.3.2.1.3. 消防设施

序号	数据项	数据类型	长度	说明
1	设施名称	字符型	40	
2	设置部位	字符型	50	
3	设施系统形式	字符型	50	
4	投入使用时间	日期型	8	
5	探测器数量	数值型	5	
6	控制器数量	数值型	5	
7	手动报警按钮数量	数值型	5	
8	消防电气控制装置数量	数值型	5	
9	市政给水管网形式	字符型	1	
10	市政进水管数量	数值型	3	
11	市攻进水管管径	数值型	5	
12	消防水池容量	数值型	10	
13	消防水池位置	字符型	50	
14	消防水箱容量	数值型	10	
15	消防水箱位置	字符型	50	
16	其他水源供水量	数值型	10	
17	其他水源情况	字符型	200	
18	消防泵房位置	字符型	50	
19	消防泵数量	数值型	5	
20	消防泵流量	数值型	6	单位：L/s
21	消防泵扬程	数值型	6	单位：m
22	室外消火栓管网形式	字符型	1	
23	室外消火栓数量	数值型	5	

24	室外消火栓管径	数值型	5	单位：mm
25	室内消火栓管网形式	字符型	1	
26	室内消火栓数量	数值型	5	
27	室内消火栓管径	数值型	5	
28	水泵接合器数量	数值型	5	单位：L/s
29	水泵接合器位置	字符型	50	单位：m
30	稳压泵数量	数值型	5	单位：m^3
31	稳压泵流量	数值型	6	
32	稳压泵扬程	数值型	6	
33	气压罐容量	数值型	10	
34	消防水喉数量	数值型	5	
35	报警阀数量	数值型	5	
36	报警阀位置	字符型	50	
37	水流指示器数量	数值型	5	
38	水流指示器位置	字符型	50	
39	喷头数量	数值型	5	
40	减压阀数量	数值型	5	
41	减压阀位置	字符型	50	
42	竖向分区数量	数值型	5	
43	喷淋系统数量	数值型	5	
44	喷淋泵流量	数值型	6	单位：L/s
45	喷淋泵扬程	数值型	6	单位：m
46	喷淋泵位置	字符型	50	
47	雨淋阀数量	数值型	5	
48	雨淋阀位置	字符型	50	
49	水雾喷头数量	数值型	5	
50	水雾喷头位置	字符型	50	
51	防护区数量	数值型	5	
52	防护区容积	数值型	10	单位：m^3
53	防护区部位名称	字符型	50	
54	防护区位置	字符型	50	
55	灭火剂类型	字符型	50	
56	手动控制装置位置	字符型	50	
57	设施动作方式	字符型	50	
58	瓶库位置	字符型	50	
59	钢瓶数量	数值型	5	
60	单个钢瓶容量	数值型	10	单位：L
61	钢瓶间距	数值型	6	单位：m，精确到小数点后 2 位

62	泡沫泵数量	数值型	5	
63	泡沫泵流量	数值型	6	单位：L/s
64	泡沫泵扬程	数值型	6	单位：m
65	泡沫数值	数值型	5	
66	干粉储罐位置	字符型	50	
67	防烟分区数量	数值型	5	
68	防烟分区位置	字符型	50	
69	风机数量	数值型	5	
70	风机安装位置	字符型	50	
71	风机风量	数值型	6	单位：m^3/h
72	风口设置部位	字符型	50	
73	排烟防火阀数量	数值型	5	
74	排烟绸数量	数值型	5	
75	防火阀数量	数值型	5	
76	正压送风阀数量	数值型	5	
77	防火门数量	数值型	5	
78	防火卷帘数量	数值型	5	
79	防火门设置部位	字符型	50	
80	防火卷帘设置部位	字符型	50	
81	扩音机功率	数值型	5	单位：W
82	备用扩音机功率	数值型	5	单位：W
83	扬声器数量	数值型	5	
84	广播分区数量	数值型	5	
85	广播分区设置部位	字符型	50	
86	消防专用电话数量	数值型	5	
87	消防专用电话位置	字符型	50	
88	应急照明及疏散指示装置数量	数值型	5	
89	消防电源设置部位	字符型	50	
90	消防主电源是否为独立配电柜	字符型	1	1 一是；2 一否
91	备用电源形式	字符型	50	发电机、EPS、蓄电池等
92	灭火器设置部位	字符型	50	
93	灭火器配置类型	字符型	30	
94	灭火器生产日期	日期型	8	表示方法：YYYYMMDD
95	灭火器更换药剂日期	日期型	8	表示方法：YYYYMMDD
96	灭火器数量	数值型	5	
97	设施服务状态	字符型	1	0 一停用；1 一试运行；2 一有效；9 一其他
98	生产单位名称	字符型	70	
99	生产单位电话	字符型	18	

100	维修保养单位名称	字符型	70	
101	维修保养单位电话	字符型	18	
102	设施状态	字符型	2	01 一正常；10 一报警；20 一故障；99 一其他
103	状态描述	字符型	100	
104	状态变化时间	日期时间型	14	表示方法: YYYYMMDDHHmmss
105	火灾自动报警系统图	二进制		
106	消防给水系统平面布置图	二进制		
107	室外消火栓平面布置图	二进制		
108	室内消火栓布置图	二进制		
109	自动喷水灭火系统图	二进制		
110	水喷雾灭火系统图	二进制		
111	气体灭火系统图	二进制		
112	泡沫灭火系统图	二进制		
113	干粉灭火系统图	二进制		
114	防烟排烟系统图	二进制		
115	消防应急广播系统图	二进制		
116	应急照明及疏散指示系统图	二进制		
117	消防设施所属单位名称	字符型	70	

7.3.2.1.4. 消防设施部件

序号	数据项	数据类型	长度	说明
1	设施名称	字符型	40	
2	部件名称	字符型	40	
3	部件型号	字符型	30	
4	部件区号	数值型	4	
5	部件回路号	数值型	4	
6	部件位号	数值型	4	
7	安装位置	字符型	50	
8	部件状态	字符型	2	
9	状态描述	字符型	100	01 一正常；10 一报警；20 一故障；99 一其他
10	状态变化时间	日期时间型	14	

7.3.2.1.5. 消防警力

序号	数据项	数据类型	长度	说明
1	人员姓名	字符型	30	
2	人员电话	字符型	18	
3	人员所属单位名称	字符型	70	

7.3.2.1.6. 救援力量

序号	数据项	数据类型	长度	说明
1	微型消防站名称	字符型	70	
2	微型消防站地址	字符型	100	
3	消控室名称	字符型	70	
4	消控室地址	字符型	100	
5	水源地名称	字符型	70	
6	水源地地址	字符型	100	
7	消防从业人员数量	数值型	4	
8	技术服务单位名称	字符型	70	
9	技术服务单位地址	字符型	100	
10	维保从业人员数量	数值型	4	

7.3.2.1.7. 管理机构

序号	数据项	数据类型	长度	说明
1	管理机构名称	字符型	70	
2	上级机构名称	字符型	70	
3	管理机构地址	字符型	100	
4	管辖范围、内容	字符型	100	

7.3.2.1.8. 水源信息

序号	字段中文名	数据类型	长度	说明
1	水源名称	字符型	70	
2	所在位置	字符型	50	

3	储水量	数值型	4	单位：立方米

7.3.2.1.9. 重点部位

序号	数据项	数据类型	长度	说明
1	重点部位名称	字符型	70	
2	建筑面积	数值型	10	
3	耐火等级	字符型	1	
4	所在位置	字符型	50	
5	使用性质	字符型	2	
6	消防设施情况	字符型	200	
7	责任人姓名	字符型	30	
8	责任人公民身份号码	字符型	18	
9	责任人电话	字符型	18	
10	确立消防安全重点部位的原因	字符型		
11	防火标志的设立情况	字符型		
12	危险源情况	字符型		
13	消防安全管理措施	字符型		
14	重点部位所属单位名称	字符型	70	

7.3.2.2. 业务数据库

7.3.2.2.1. 火警信息

序号	数据项	数据类型	长度	说明
1	中心名称	字符型	50	
2	警情编号	字符型	30	
4	用户编码	数值型	8	
5	联网设备编码	字符型	50	
6	用户名称	字符型	50	
8	转发状态	字符型	4	
9	记录状态	数值型	4	记录状态 0 未处理，1 处理中
10	阶段处理信息	字符型	4000	
11	监控设备类型	数值型	4	监控设备类型(0：GST2000 监控器 1：六防区 2：32

				点 3：GST5000 4：GST1000 5：GST800)
14	所属子系统类型	数值型	4	
15	是否第三方警情	数值型	4	是否第三方警情 0 否 1 是
16	警情类型	数值型	4	警情类型 0，火警；1，故障；2，管理；3，误报；4，测试；5，动环；6，安防；

7.3.2.2.2. 火灾信息

序号	数据项	数据类型	长度	说明
1	单位名称	字符型	70	
2	起火部位	字符型	50	
3	起火时间	日期时间型	14	表示方法：YYYYMMDDHHmmss
4	起火原因	字符型	-	不定长
5	报警方式描述	字符型	40	自动、人工信息
6	过火面积	数值型	10	单位：平方米
7	死亡人数	数值型	6	
8	受伤人数	数值型	6	
9	财产损失	数值型	10	
10	火灾扑救概述	字符型	-	不定长

7.3.2.2.3. 受理信息

序号	数据项	数据类型	长度	说明
1	单位名称	字符型	70	
2	首次报警时间	日期时间型	14	表示方法：YYYYMMDDHHmmss
3	受理时间	日期时间型	14	表示方法：YYYYMMDDHHmmss
4	受理结束时间	日期时间型	14	表示方法：YYYYMMDDHHmmss
5	信息类型	字符型	1	1：火警 2：故障 9：其他
6	信息描述	字符型	100	
7	处理结果	字符型	300	
8	受理员姓名	字符型	30	

9	用户联系人姓名	字符型	30	
10	信息确认	字符型	1	1：误报信息 2：有效信息 9：其他
11	向应急通信指挥中心报告时间	日期时间型	14	表示方法：YYYYMMDDHHmmss
12	应急通信指挥中心反馈确认时间	日期时间型	14	表示方法：YYYYMMDDHHmmss
13	应急通信指挥中心受理员姓名	字符型	30	
14	应急通信指挥中心接警处理情况	字符型	200	

7.3.2.2.4. 消防设施检查信息

序号	数据项	数据类型	长度	说明
1	单位名称	字符型	70	
2	检查日期	日期时间型	8	表示方法：YYYYMMDD
3	检查人姓名	字符型	30	
4	消防安全管理人姓名	字符型	30	
5	检查类别	字符型	1	1：巡查 2：单项检查 3：联动检查 9：其他
6	检查结果	字符型	1	1：正常 2：故障 9：其他
7	检查内容	字符型	-	不定长
8	故障内容	字符型	-	不定长
9	处理情况	字符型	-	不定长

7.3.2.2.5. 消防设施保养信息

序号	数据项	数据类型	长度	说明
1	单位名称	字符型	70	
2	维护保养时间	日期时间型	8	表示方法：YYYYMMDD
3	维护人员姓名	字符型	30	
4	维护保养内容	字符型	-	不定长

5	停用系统消防安全员姓名	字符型	30	
6	维护保养结果	字符型	200	
7	消防安全管理人员姓名	字符型	30	

7.3.2.2.6. 查岗信息

序号	数据项	数据类型	长度	说明
1	查岗发起人姓名	字符型	30	
2	被查岗单位名称	日期时间型	70	
3	发起时间	字符型	14	表示方法：YYYYMMDDHHmmss
4	结束时间	字符型	14	表示方法：YYYYMMDDHHmmss
5	查岗结果	字符型	100	

7.3.2.3. 应用数据库

由省市县各级消防部门内部业务处理结果数据、内部管理数据等组成的应用数据库。

业务库属于生产型数据库，若直接在业务库上进行数据的研判应用，会对业务库产生极大的压力。本项目的设计思路是将业务库的数据同步到应用库中，应用库不仅拥有大量的业务数据，同时也是各类不同渠道数据的汇聚中心。应用库归集了庞大的数据资源，并且这些数据是不会被业务系统所调用，这就使得应用库天然拥有可被数据研判的两大优势：极低的数据被业务锁死概率和海量数据资源。

7.3.2.4. 综合数据库

面向信息全文检索、数据分析应用需求重新构建的综合数据库。应用库经过数据重构后形成综合数据库。综合数据库是基于消防部门管理者的角度提出的，亦有许多业务是想基于海量的数据进行报表分析及趋势分析的需求。

综合数据库的目的是表现业务信息供决策者使用。常见的数据分析方法包括以下几种：

1、预定义报表

该方法是静态的，在 OLTP 系统中取得了较好的应用，在综合数据库系统中可以在一些固定的分析任务中采用。

2、联机分析处理

即 OLAP(OnLine Analysis Process)该技术能够根据操作员的要求，对综合数据库中的数据进行探测分析。

3、数据挖掘(Data Mining)

是从存放在数据库中的大量的数据中获取有效的、潜在有用的、最终可理解的过程。数据挖掘还可创建决策树，用于根据现有数据元素的特性预测将来的数据。

综合数据库中的数据分析技术还有其他种类，但是目前用得最多主要是联机分析处理技术和数据挖掘结合使用。OLAP 是将数据组织为预定义的多维结构以便于探测，而数据挖掘与 OLAP 相反，其目的是执行探测分析并识别信息中有价值的东西，如将数据分组以供分析者或管理人员检查。OLAP 技术使综合数据库能够快速响应重复而复杂的分析查询，从而使综合数据库能有效地用于联机分析。

综合数据库的设计方法是一个逐步求精的过程，在进行设计时，一般是一次一个主题或一次若干个主题的逐步完成的。所以，我们必须对概念模型设计步骤中确定的几个基本主题域进行分析，并选择首先要实施的主题域。选择第一个主题域所要考虑的是：它要足够大，以便使得该主题域能建设成为一个可应用的系统；它还要足够小，以便于开发和较快地实施。

7.3.2.5. 管理数据库

系统管理数据库主要存储系统在运行过程中的日志文件，用户信息、权限信息、系统配置信息等，用于确保系统运行维护和管理。

（1）权限信息：包括用户所属权限的配置信息、权限划分信息、用户和权限之间的映射信息等。

（2）日志记录：包括系统事件、程序错误等，提供系统诊断功能。

（3）安全审计：包括对用户登录审计、指标数据资源、共享数据资源的访问审计信息等，并对审计结果进行统计分析。

7.3.3. 数据管理层

数据管理维护主要包括：数据权限管理、数据更新管理、数据维护和备份、管理工具等。

7.3.3.1. 数据权限管理

数据权限管理需考虑系统功能的使用权限、数据库的使用权限、数据文件的使用权限等方面。

数据库系统的权限管理采用了基于角色的访问控制方法。它的特点是先确定角色对服务所拥有的权限，然后将用户注册到角色中，或者说授予用户适当的角色，从而获得调用服务的权力。当然一个用户可以注册到多个角色中，一个角色也可以授权给多个用户。

7.3.3.2. 数据更新管理

数据的更新是指数据库存储信息的变动，更新操作包括：插入数据、修改数据和删除数据等。数据库的数据一般是不允许随意更新的。但是在数据分析过程中，会根据统计口径变化和具体分析内容的需要对指标数据进行调整、追加、删除及添加新的数据。

数据更新管理主要解决以下问题：

1．基础信息及其相关核心数据同步更新

在系统运行过程中，人员基础信息会发生变更，及时更新变化的数据，使数据能够及时准确的表示信息状态。

2．业务数据和分析型数据的定期更新

分析型数据与其来源的业务数据是紧密关联的，是业务数据加工提取而形成的。基础信息数据变更后，为保证分析数据的完整性、准确性，业务数据、分析数据必须定期更新。

3．基础数据和专题数据集市的同步更新

专题数据集是从内容上是基础数据的一个子集，分析应用要求无论是存储于基础数据、还是存储于专题数据的数据，统一指标内容的数据必须保持全局的、实时的一致性。

4．错误数据追加更新

从理论讲，经过采集处理后入库的数据是稳定的数据，是不能随便更改的；在数据采集交换过程中经常出现由于业务上的不可抗拒的原因导致将错误的数据入库，

在一段时间（一个月）发现错误需要重新修改。此类数据的更新有时既要保持原有错误数据的客观存在，又要及时追加新的数据。

数据更新的技术实现要求有系统自动实时或定期进行，而不需要采用人工方式。用户可以对更新的频率、方式和更新内容做自定义。

数据更新的设置和维护要采用先进的数据管理工具实现。

7.3.3.3. 数据维护和备份

数据维护和备份策略主要包括下列工作：

（1）备份数据信息收集；

（2）完成数据生命周期管理；

（3）定制数据备份策略及定期备份数据；

（4）收集正确的编目信息。

7.3.3.4. 管理工具

提供完备的统一的图形化管理工具，完成对不同平台的数据库的配置，在一个中心管理客户端上就可以对所有的数据库进行集中管理、性能、事务监控，包括元数据管理、数据共享服务、运行监控管理和数据应用服务等功能。管理工具中包含数据库构建向导，索引向导，性能智能向导等多种辅助图形化管理工具，简化数据库的管理，提供数据库的自我管理和资源调度功能，支持部分核心数据库参数由数据库系统自我调节。

7.3.4. 数据服务/共享层

数据共享服务主要是指在系统与其它业务系统对接，提供数据共享服务，基于数据接口的方式提供数据共享服务。为能够直接进行应用对接的外部系统提供统一的应用接口，包括 Web Service 调用方式和接口控件方式，实现与外部系统之间的数据共享服务。

7.3.5. 数据资源指标体系建设

综合考虑省市县各级消防安全监管与服务的核心需求和数据获取的可行性，遵

从数据来源必须是权威可信、共享可得、分享可用的原则，对智慧消防云平台大数据中心获取数据的分类对象定义为：消防专题数据、消防业务数据、省基础数据库数据、省公共信息资源数据、国家知网数据、省内火灾重点行业调查数据、社情民意数据、互联网数据等八部分。

本工程标准体系建设中，《消防数据资源分类指标体系标准》也将遵循以上八类数据进行构建。

序号	数据类别	数据内容
1	消防专题数据	火灾风险数据、火灾趋势专题数据、消防力量统计专题数据、消防资源统计专题数据等
2	消防业务数据	物联感知网监测数据、火灾火警数据、设施检查保养数据、消防教育培训数据、消防宣传数据、值班运维数据等。
3	省基础数据库数据	福建省四大基础数据库数据、公共服务平台数据
4	省公共信息资源数据	安全监管、地理空间、海洋渔业、交通运输、教育文化、财税金融、社保就业、科技创新、工业农业、市场监管、气象服务、生态环境、统计服务、信用服务、医疗卫生、资源能源、闽台合作等
5	国家知网数据	与消防相关文献、法律法规、重大会议、专题、资讯等
6	消防社情民意数据	12345 平台中与消防相关的数据
7	火灾风险重点行业调查数据	生态云数据、河长制数据、自然资源数据等
8	互联网数据	舆情数据、流量数据、聚类数据等

7.3.6. 数据来源

智慧消防大数据中心的数据主要包括内部数据及外部数据。内部数据包括：消防物联网设备自动监测数据、消防基础数据、火灾火警信息、消防监管考核数据、消防服务数据、消防检查巡查数据，系统管理数据、运行日志数据等。外部数据包括：各级消防已建业务系统数据、各委办厅（局）系统共享数据、网站数据、社会调查（公众咨询、投诉举报、主动调查等）数据等。

具体如下表所示：

序号	数据类型	数据来源、内容	获取方式
内部数据			
1	消防物联网设备自动监测数据	全省各级消防物联网感知网的智能设备监测数据	设备采集至感知网分中心服务器，分中心服务器传输至省级平台。
2	消防基础数据	消防资源、消防力量、消防组织机构、火灾风险单位信息	这些纸质档案的信息采集，首先需要将纸质文件进行 OCR 扫描转换成数字字符文档，再将其添加对应的日期、所属行业领域、所属地域区间、文件类型等索引关键字编码信息，再由数据交换平台将文档和其索引信息转换、采集到数据中心库。
3	火灾火警信息	火灾风险单位的隐患、事故、故障信息。	设备采集并传输至省平台大数据中心，由智能分析研判系统加工得出。
4	消防监管考核数据	根据消防检查、巡查、监管、分析数据，进行综合考评得出。	系统生成、系统录入
5	系统运行数据	运行管理参数数据、系统运行日志、用户操作日志等。	系统生成
外部数据			
1	各级消防已建业务系统	市/县消防物联网远程监控系统、福建省消防技术服务平台、消防救援总队实战指挥系统、综合应用系统	数据接口对接
2	各委办厅（局）数据	政务数据、民生服务数据、证照数据、地理数据、行政执法数据等。	数据接口对接
3	互联网数据	互联网信息是当前社会的重要传播途径，它具有信息量大，热点集聚度高，潮汐效应明显，转换响应速度快等特点，其传播载体有：微博、论坛、门户新闻网站、朋友圈、自媒体等。	互联网信息的收集是当前各信息服务商的主攻技术领域，所采用的方式有很多种。但不是所有的技术方式都适合采用，目前相对成熟和适宜的实现方案是采用网络爬虫技术，由大数据中心运营团队，按照当前时期的敏感词、集聚热度、传播链等技术指标，对互联网的候选目标群进行自动筛选；跟踪定位到相应的对象信息源后，抽取对应的信息，经转换处理后，由数据交换平台采集入中心

			数据库。
4	社会调查数据	社会公众咨询数据、投票数据、投诉举报数据、主动调查数据。	纸质获取录入、网站录入

7.4. 数据存储设计

7.4.1. 存储结构

考虑到智慧消防云平台大数据中心是一个行业级的数据中心，在中心的存储设计上充分考虑系统技术的先进性，采用目前先进的云存储架构结合高性能的 NAS 存储实现在线、近线和离线的数据安全存储；同时，充分考虑系统的可扩展性，在设计上充分保障工程建设内中心数据的快速查询检索与管理，能充分处理正常和高峰时期的业务，支持快速扩容；同时，云存储采用分布式方式文件系统，对文件进行备份设计，满足了用户对数据安全性的要求，NAS 具有跨平台、安装及扩充简易、易于管理维护特点，还具备对病毒的免疫能力，因此采用云存储架构结合 NAS 存储的方式能够提供更安全更可靠的数据存储方式。此外，数据是行业级数据中心运行的基础和存在的价值重要体现，在设计上需充分考虑所有可能出现的故障，并考虑中心数据库的便捷式维护和管理。

提供的开放云存储设备主要包括元数据服务器、存储服务器节点等设备。元数据服务器采用主备双机容错的方式管理各个存储节点，文件分散存储在各个存储节点上，负责完成存储节点的虚拟共享，并且在整个网络环境中实现消防数据的全局共享。其中，存储节点采用高性价比的计算机，运用自适应副本管理技术进行容错。所有存储节点同时担任对外服务功能，客户端分别挂载到不同存储节点访问云存储系统。通过增加或减少存储节点的方式，既可以对存储系统进行在线伸缩，由于采用了自适应副本管理技术进行容错，系统在线伸缩的过程中，不影响系统对外提供服务。

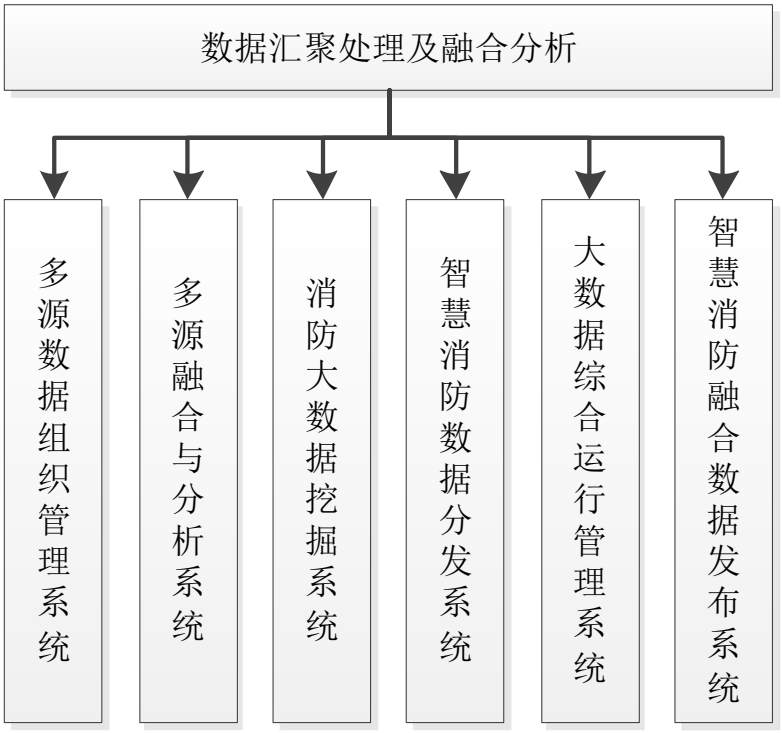
此外，离线数据的存储采用可扩展性较好的 NAS 存储设备进行存储。

7.4.2. 备份与恢复设计

系统利用 Oracle 软件和数据备份软件实现数据库备份与恢复功能。

7.5. 数据汇聚处理及融合分析设计

数据汇聚处理及融合分析由多源数据组织管理系统、多源数据融合与分析系统、消防大数据挖掘系统、智慧消防数据分发系统、消防大数据综合运行管理系统、智慧消防融合数据发布等六个子系统组成。



7.5.1. 多源异构系统数据管理系统

多源异构系统数据管理系统主要实现多源异构数据的存储管理，建立数据字典、提供数据快速查询检索、统计分析，设计高效的数据库存储结构、金字塔结构和数据库索引等，具体功能模块组成如下：

（1）消防数据管理模块：主要是对包括消防专题数据、消防业务数据进行存储管理，并提供数据快速查询检索、统计分析等；

（2）行业业务数据管理模块：主要是对城市环境、楼宇大厦、道路交通、火灾风险单位、特殊产业园区/厂区等行业的视频数据、图像数据和文字信息等进行存储管理，并提供数据快速查询检索、统计分析等；

（3）省 12345 便民服务数据管理模块：主要是对省 12345 便民服务平台的各类应用数据进行存储管理，并提供数据快速查询检索、统计分析等；

（4）支撑部门业务数据管理模块：主要是对引接其他省级单位生产的业务数据进行存储管理，并提供数据快速查询检索、统计分析等；

（5）专题产品数据管理模块：主要是对系统生产各类数据以及其他专题业务产品数据进行存储管理，并提供数据快速查询检索、统计分析等；

（6）系统数据管理模块：主要对系统运行的基础空间数据、智慧消防相关知识数据、标注标绘数据、任务数据、请求数据、系统运行日志数据等进行综合管理；

（7）多源异构数据时空关联模块：主要是对多源异构数据在统一时空框架下的关联组织管理；

（8）数据及数据库备份模块：为全系统数据资源提供备份功能；

（9）数据及数据库恢复模块：提供数据及数据库的恢复功能，以保障在数据及数据库的安全；

（10）备份记录维护管理模块：提供对系统维护记录的备份和记录的恢复功能。

7.5.2. 多源数据融合与分析系统

多源数据融合与分析子系统主要是面向智慧消防云平台的应用级产品需求，开展多源数据融合分析以及综合特征信息的提取，利用多级多类数据以及智慧消防业务数据等多源异构数据的比对分析、测量分析、标注标绘、感兴趣区域选择、空间分析等判读解译工具包。

（1）影像数据与视频数据融合分析模块：提供视频与地理空间数据的坐标统一化处理、视频与影像的对比分析等功能；

（2）实时监测监控数据处理模块：能够支持行业实时监测监控数据的展示与综合处理和分析；

（3）多源异构数据综合特征提取模块：面向智慧消防需求，提供基于影像数据、行业业务数据以及其他辅助支撑数据的关注区域或关注地物的快速特征提取功能；

（4）专题制图模板定制模块：面向智慧消防所需的专题制图共性要求，支持用户根据业务需求实现专题制图模板定制，自定义模板类型、要素和样式等；

（5）信息专题产品制作模块：支持智慧消防通用信息专题产品的快速制作，包括模板与要素快速配置、图幅整饰、模板设置和专题出图等功能。

7.5.3. 消防大数据挖掘系统

（1）基础分析工具模块：包括基础分析开发集成历史推理方法、聚类分析、连接分析、神经网络、判别分析、逻辑分析、人工智能等通用性的挖掘方法，形成基础分析工具包。

（2）空间分布计算模块：计算单一专题数据源的空间粒度，通过地名地址匹配自动化或半自动化将其分布在相应尺度的基础地理信息之上，分析挖掘其空间分布规律。

（3）多因子关联分析模块：将两种及以上专题数据源分布在相应尺度的统一基础地理信息之上，综合运用各种数学模型，探求挖掘专题信息之间的相关性和依赖度。

（4）时空分析模块：将单一或多种带有时间特征的专题信息，分布在相应尺度的统一基础地理信息之上，研究揭示专题信息在时间维度上的演变规律、在空间维度上的分布规律，以及在四维时空中的时空特征。

（5）主题分析模块：面向某一主题，在基础分析工具包和空间分布、多因子关联分析、时空分析的基础上，提炼主题大数据分析的专业模型和业务流程，形成定制化、流程化的知识链，开发高自动化的分析功能，发现潜藏数据背后的知识与规律。

7.5.4. 智慧消防数据分发系统

智慧消防数据分发系统主要功能是实现消防综合数据向各级用户的共享分发；提供数据权限及查询检索等功能，主要包括智慧消防数据产品编目更新发布模块、智慧消防数据产品在线下载模块、智慧消防数据产品订阅推送模块、智慧消防数据产品应急保障模块、数据分发管理模块、数据权限管理模块、虚拟共享目录管理功能模块等。

（1）智慧消防数据产品编目更新发布模块：提供基于目录共享的数据编目更新与发布，实现基于智慧消防综合数据服务的异地数据资源虚拟整合；

（2）智慧消防数据产品在线下载模块：提供在线数据产品的查询浏览、支持用户在浏览器端进行智慧消防数据产品，包括基础数据、部门业务数据以及专题产品

数据的在线查看与下载，提供数据定制和在线下载服务支持，满足多用户并发访问要求；

（3）智慧消防数据产品订阅推送模块：支持用户长期订阅相关数据产品，提供定期推送数据功能；

（4）数据分发管理模块：能够定制数据分发策略，按照用户级别、用户权限、数据区域和时间等关键字段设置数据分发共享的管理机制。提供了基于不同网络链路下各类数据的实时分发服务，针对不同类型保障任务，为用户提供高优先级、快速可靠的数据分发服务；

（5）数据权限管理模块：遵循统一技术体制的用户身份认证与业务授权流程与规范要求，实现用户的同步和内部用户的维护，为全系统提供统一的身份认证、授权与权限控制服务；

（6）虚拟目录管理模块：虚拟目录管理主要提供对各类综合数据产品的目录共享、信息查询浏览服务能力。其主要包括虚拟共享目录构建、虚拟共享目录同步、虚拟共享目录查询三部分，针对系统产品数据库，采用智慧消防综合数据服务的目录整合手段，构建形成虚拟共享数据目录，实时监视变化情况，提供统一查询接口，为系统和用户提供最新的数据产品目录。

7.5.5. 综合运行维护管理系统

实现对系统硬件、软件的全方位状态监控，提供相关图表显示；支持对系统安全和网络安全的监控与防护，提供异常报警；支持系统审计结果、日志信息的管理、统计和成果输出；支持系统用户注册、管理、角色和权限分配等。主要包括系统运行状态监控、数据传输网络状态监控、用户使用状态监控、数据库监控、系统端口防御、系统病毒防御、系统入侵检测、系统运行记录、用户操作记录、系统日志审计、系统日志查询浏览、系统设计结果输出、系统用户注册、系统用户管理、系统角色管理和系统权限管理等功能模块。

（1）用户管理模块：包括省市县各级消防部门的用户组管理、用户信息维护、用户角色授权管理，提供建立用户、删除用户、建立角色、删除角色、机构创建、机构编辑和机构删除以及为用户分配角色等功能，并能按用户分配权限、按角色分配权限以及按数据库表分配权限；

（2）作业任务管理与监控模块：根据数据中心接收的数据请求订单情况，开展任务编制与解析、处理以及跟踪任务情况，支持任务计划编排与优先级定制、任务计划表查询；能够根据任务单标明所需的产品种类、时次以及时间段等任务属性配置作业参数，提交给相关处理单元开展处理；

（3）运行状态监控模块：提供文字报表、统计图表和条目信息等方式实现系统软硬件运行状态监控、用户使用状态监控、归档状态监控、数据查询检索等数据库交互使用效率监控等；

（4）日志管理模块：对服务访问日志、共享管理日志、数据管理日志、安全管理日志、系统监控日志等根据查询条件进行管理；

（5）安全防护模块：提供数据传输加密、端口防御、防病毒防御以及入侵检测等功能；

（6）系统日志安全审计模块：记录和跟踪系统状态的变化，如提供对系统故意入侵行为的记录和对系统安全功能违法的记录，实现对各种安全事故的定位，如监控和捕捉各种安全事件；保存、维护和管理日志。

7.5.6. 智慧消防融合数据发布共享系统

智慧消防融合数据发布共享系统主要是对智慧消防大数据中心获取或生产的数据进行对外发布的平台，建立按需分发、信息发布、订阅提取、在线服务等信息共享机制，通过建立数据共享门户，为用户提供搜索引擎服务，按需组织数据返回用户，为用户提供各类需求的响应和处理服务。实现消防大数据资源在各级消防部门、技术服务单位、社会机构、社会民众间的共享和分发。主要包括：需求受理服务，数据检索引擎，数据传输服务，订阅与分发服务、资源发布管理和数据共享服务、在线浏览、在线服务调度。

（1）需求受理服务：主要是接收来自数据共享门户获取的政府用户、行业用户、公众用户等数据和专题产品需求，对其做出响应，反馈需求执行状态等。

（2）数据检索引擎：主要负责完成各类信息资源的检索查询服务，按照信息资源的种类，检索引擎可以提供基于常规、空间、时间和全文语义等模式的检索服务。

（3）数据传输服务：通过优先级策略管理，任务队列管理和数据传输管理，实现基于数据分类、用户需求、网络性能的数据按需、高效、有序分发。

（4）订阅与分发服务：建立用户订阅机制，维护并管理用户订阅模型，将最新数据向用户进行推送，保证数据推动的按需、准确、及时。根据制定的实时分发策略，如数据推送规则定义、数据优先级定义等，保证数据在网络链路下完成分发服务。

（5）资源发布管理：主要负责对登录用户的权限进行验证，根据用户所拥有的数据权限和操作权限对将要在数据发布门户上进行数据的组织和发布。

（6）数据共享服务：建立数据共享服务，利用门户网站进行资源发布，为用户提供数据检索与下载服务，受理用户提出的专题应用需求，为用户提供专题产品数据的共享服务。

（7）在线数据浏览：提供多种遵循 OGC 等标准规范的多种数据查询检索、数据分析服务。用户可根据不同的查询条件，检索当前数据库中现存的数据信息。

（8）在线服务调度：接收用户提交的各类在线请求，依据计算资源的负载情况，能够将请求下达给负载最少的计算资源，实现系统的负载均衡。能够监视请求的处理进度，即时更新计算资源的负载，为下一次的调度做好准备。

7.6. 关键数据库逻辑设计

7.6.1. 数据表设计原则

1．不应该针对整个系统进行数据库设计，而应该根据系统架构中的组件划分，针对每个组件所处理的业务进行组件单元的数据库设计；不同组件间所对应的数据库表之间的关联应尽可能减少，如果不同组件间的表需要外键关联也尽量不要创建外键关联，而只是记录关联表的一个主键，确保组件对应的表之间的独立性，为系统或表结构的重构提供可能性。

2．采用领域模型驱动的方式和自顶向下的思路进行数据库设计，首先分析系统业务，根据职责定义对象。对象要符合封装的特性，确保与职责相关的数据项被定义在一个对象之内，这些数据项能够完整描述该职责，不会出现职责描述缺失。并且一个对象有且只有一项职责，如果一个对象要负责两个或两个以上的职责，应进行分拆。

3．根据建立的领域模型进行数据库表的映射，此时应参考数据库设计第二范式：

一个表中的所有非关键字属性都依赖于整个关键字。关键字可以是一个属性，也可以是多个属性的集合，不论哪种方式，都应确保关键字能够保证唯一性。在确定关键字时，应保证关键字不会参与业务且不会出现更新异常，这时，最优解决方案为采用一个自增数值型属性或一个随机字符串作为表的关键字。

4．由于第一点所述的领域模型驱动的方式设计数据库表结构，领域模型中的每一个对象只有一项职责，所以对象中的数据项不存在传递依赖，所以，这种思路的数据库表结构设计从一开始即满足第三范式：一个表应满足第二范式，且属性间不存在传递依赖。

5．同样，由于对象职责的单一性以及对象之间的关系反映的是业务逻辑之间的关系，所以在领域模型中的对象存在主对象和从对象之分，从对象是从 1—N 或 N—N 的角度进一步主对象的业务逻辑，所以从对象及对象关系映射为的表及表关联关系不存在删除和插入异常。

6．在映射后得出的数据库表结构中，应再根据第四范式进行进一步修改，确保不存在多值依赖。这时，应根据反向工程的思路反馈给领域模型。如果表结构中存在多值依赖，则证明领域模型中的对象具有至少两个以上的职责，应根据第一条进行设计修正。第四范式：一个表如果满足 BCNF，不应存在多值依赖。

7．在经过分析后确认所有的表都满足二、三、四范式的情况下，表和表之间的关联尽量采用弱关联以便于对表字段和表结构的调整和重构。且数据库中的表是用来持久化一个对象实例在特定时间及特定条件下的状态的，只是一个存储介质，所以，表和表之间也不应用强关联来表述业务（数据间的一致性），这一职责应由系统的逻辑层来保证，这种方式也确保了系统对于不正确数据（脏数据）的兼容性。当然，从整个系统的角度来说我们还是要尽最大努力确保系统不会产生脏数据，单从另一个角度来说，脏数据的产生在一定程度上也是不可避免的，我们也要保证系统对这种情况的容错性。这是一个折中的方案。

8．应针对所有表的主键和外键建立索引，有针对性的（针对一些大数据量和常用检索方式）建立组合属性的索引，提高检索效率。虽然建立索引会消耗部分系统资源，但比较起在检索时搜索整张表中的数据尤其是表中的数据量较大时所带来的性能影响，以及无索引时的排序操作所带来的性能影响，这种方式仍然是值得提倡的。

9．尽量少采用存储过程，目前已经有很多技术可以替代存储过程的功能如“对象/关系映射”等，将数据一致性的保证放在数据库中，无论对于版本控制、开发和部署、以及数据库的迁移都会带来很大的影响。但不可否认，存储过程具有性能上的优势，所以，当系统可使用的硬件不会得到提升而性能又是非常重要的质量属性时，可经过平衡考虑选用存储过程。

10．当处理表间的关联约束所付出的代价（常常是使用性上的代价）超过了保证不会出现修改、删除、更改异常所付出的代价，并且数据冗余也不是主要的问题时，表设计可以不符合四个范式。四个范式确保了不会出现异常，但也可能由此导致过于纯洁的设计，使得表结构难于使用，所以在设计时需要进行综合判断，但首先确保符合四个范式，然后再进行精化修正是刚刚进入数据库设计领域时可以采用的最好办法。

11．设计出的表要具有较好的使用性，主要体现在查询时是否需要关联多张表且还需使用复杂的 SQL 技巧。

12．设计出的表要尽可能减少数据冗余，确保数据的准确性，有效地控制冗余有助于提高数据库的性能。

7.6.2. 实体关系设计（E-R）

E-R 图（实体关系对象图），是数据库设计过程中非常重要的一个环节，通过 E-R 图，可以直观反映出整个智慧消防云平台中各个应用系统的具体实体对象，以及对象中的属性要素、关联关系（依赖/从属、引用）等。

E-R 图的设计准确与否，能够真实反映实际业务逻辑和业务关系，也影响到后续的系统程序逻辑设计开发、代码实现，能否准确支撑业务功能的正常、合理运行。

7.6.2.1. E-R 图的设计原则

1．尽量减小实体集，能作为属性时不要作为实体集。

2．“属性”不能再具有需要描述的性质。“属性”必须是不可分割的数据项，不能包括其他属性。

3．“属性”不能与其他实体具有联系。在 E-R 中所有的联系必须是实体间的联系，而不能有属性与实体之间的联系。

4．针对特定用户的应用，确定实体、属性和实体间的联系，设计该用户视图的局部 E-R 图。

5．综合局部 E-R 图，产生出总体 E-R 图。在综合过程中，同名实体只能出现一次，并去掉不必要的联系，以便消除冗余。一般来说，从总体 E-R 图必须能导出原来的所有局部视图，包括实体、属性和联系。

7.6.2.2. E-R 图的设计方法

在设计 E-R 图时，一般使用先局部后全局的方法。

1．选择局部应用：根据某个系统的具体情况，在多层的数据流图中选择一个适当层次的数据流图作为设计分 E-R 图的出发点 。

2．逐一设计分 E-R 图：将数据字典中的数据抽取出来，参照数据流图，设计出 E-R 图，再做必要的调整。

3．调整原则：为简化图的处置，现实世界中的事物能作为属性对待的，尽量作为属性对待。作为“属性”，不能再具有描述的性质，也不能与其他实体具有联系。

7.6.2.3. E-R 图的设计步骤

（一）设计分 E-R 图

1．首先选择局部应用。根据某个系统的具体情况，在多层的 DFD 中选择一个适当层次的DFD,作为设计分E-R图的出发点。让这组图中每一部分对应一个局部应用。由于高层的 DFD 只能反映系统的概貌，而中层的 DFD 能较好地反映系统中各局部应用的子系统组成，因此人们往往以中层 DFD 作为设计分 E-R 图的依据。

2．选择好局部应用之后，就要对每个局部应用逐一设计分 E-R 图。在前面选好的某一层次的 DFD 中，每个局部应用都对应了一组 DFD，局部应用涉及的数据都已经收集在数据字典中了。现在就是要将这些数据从数据字典中抽取出来，参照 DFD，标定局部应用中的实体、实体的属性、标识实体的主码，确定实体之间的联系及其类型。

3.在实际 E-R 图设计时,实体与属性之间并不存在形式上可以截然划分的界限，现实世界的事物能作为属性对待的尽量作为属性对待，从自然划分的内容出发定义雏形的 E-R 图，再进行必要的调整。例如，图 2-17 所示的是一个有属性上升为用实

体集表示的实例。

（二）分 E-R 图的集成

1．各子系统的分 E-R 图设计好以后，下一步就是要将所有的分 E-R 图集成一个系统的总 E-R 图。一般说来，分 E-R 图的合成有两种方法：第一种方法是多个分 E-R 图一次集成；第二种方法是逐步集成，用累加的方式一次集成两个分 E-R 图。第一种方法比较复杂，做起来难度较大。第二种方法每次只集成两个分 E-R 图，可以降低复杂度。无论采用哪种方式，每次集成分 E-R 图时都需要分两步走：

2．将各分 E-R 图合并起来生成初步 E-R 图

合并时注意解决各分 E-R 图之间的冲突。由于各个局部应用所面向的问题是不同的，而且通常是由不同的设计人员进行不同局部的视图设计，这样就会导致各个分 E-R 图之间必定会存在许多不一致的地方，即产生冲突问题。由于各个分 E-R 图存在冲突，所以不能简单地把它们画到一起，必须先消除各个分 E-R 图之间的不一致，形成一个能被全系统所有用户共同理解和接受的统一的概念模型，再进行合并。合理消除各个分 E-R 图的冲突是进行合并的主要工作和关键所在。

3．消除不必要的冗余，生成基本 E-R 图。

（1）在初步 E-R 图中可能存在冗余的数据和实体间冗余的联系。所谓冗余数据是指可由基本数据导出的数据。所谓冗余的联系是可由其他联系导出的联系。冗余的存在容易破坏数据库的完整性，给数据库维护增加困难，应当加以消除。消除了冗余的初步 E-R 图就称为基本 E-R 图。

（2）常见的消除冗余方法有分析方法和规范化理论方法。

（3）用分析方法消除冗余分析方法是消除冗余的主要方法。分析方法消除冗余是以数据字典和 DFD 为依据，根据数据字典中关于数据项之间逻辑关系的说明来消除冗余的。

7.6.3. 设计说明

该系统使用的数据结构由数据库的表来实现，具体如下：

（1）命名应该使用英文单词，避免使用拼音，特别不应该使用拼音简写。命名不允许使用中文或者特殊字符。

（2）英文单词使用对象本身意义相对或相近的单词，有多个时，最好选择简单

的那个。不能使用毫不相干的单词来命名。

（3）当一个单词不能表达对象含义时，如果有词组就用词组，否则就用多个单词组合，当组合太长时，如果有简写就用简写，如果没有就采用缩写，缩写要基本能表达原单词的意义，不能随意挑。

（4）当出现对象名重名时，是不同类型对象时，通过类型前缀或后缀，加以区别。

（5）数据库对象名称一律大写。

（6）命名的各单词之间必须使用下划线（_）进行分隔。

（7）命名不允许使用 SQL 保留字，如 count。

（8）表名、字段名、视图名等所有数据库对象长度应限制在 30 个字符内（含前缀）。

（9）同一个字段名在一个数据库中只能代表一个意思。

（10）不同的表用于相同含义字段应该采用同样的名称和字段类型定义。

（11）缩写长度应该控制在 2 到 7 字符，缩写一般取每个词元的第一字母作为组合。

7.7. 业务数据量需求分析

根据全省除省级外的 94 个分中心（83 个县级和 10 个地市级），按照向每个感知网分中心、其它渠道（如政务公共信息平台、互联网、行业调查数据）等采集平均（不同地区具有监测对象数量差异）获取约 40TB（循环覆盖获取，数据有一定保管期限）数据计算，以及结合当前全省消防物联网监测数据采集量递增情况，并考虑到今后 8 至 10 年的存储需求，对所需存储资源进行估算。

但由于平台规划设计中，全省各地市、区县自建感知网络分中心，因此感知网分中心的监测数据均自行存储管理，形成全省分布式感知网络分中心。省级或市县两级需要访问数据时，直接调用和访问感知网分中心数据库。

因此，福建省智慧消防平台仅存储省本级的物联网监测数据/视频监控数据、全省消防业务管理数据、全省消防专题数据、福建省政务基础数据库数据、省公共信息资源数据、行业数据、互联网及社会数据等。

数据类型	数据内容	数据量估算（TB）
消防基础数据、日常业务数据	省本级物联网监测数据、全省消防监管考核数据、全省消防巡查数据、省本级消防视频监控数据、消防教育培训数据、消防值班监控运维数据等	20
消防专题数据	火灾风险模型数据、火灾历史统计分析数据、区域火灾隐患数据、区域（或时间段）火灾高发趋势数据等	5
省基础数据库数据、省公共信息资源数据	地理信息数据、人口数据、法人数据、经济数据及公共平台数据等。	10
重点行业调查数据	省级政务数据、城市管理与服务数据、生态云数据、河长制数据、自然资源数据、应急管理数据、审计数据、健康医疗数据、工业数据、农业数据	1
社情民意数据	经济综合、宣传舆论、纪检监察、政法、劳动社保、教育、卫生计生、科技文体、组织人事、交通能源环保、民政、农村农业、国土资源水利林业、城乡建设、信息产业、商贸旅游、企业服务	1
互联网数据	舆情数据、聚类数据、时空数据等，仅考虑保存分析后的结果数据及存储一年内的互联网基础数据。	1

7.8. 云平台/感知网分中心资源需求估算

7.8.1. 省级云平台资源需求估算

福建省智慧消防云平台需要部署应用管理服务器、数据库服务器等基础设施资源。其中应用服务器包括：消息中心服务器、消防数据存储服务器、消防物联网设备接入服务器、视频综合应用服务器、视频设备接入网关、大数据可视化服务器。

系统的部署应充分考虑系统和数据的安全保密性，主机存储系统、应用系统集中部署。因此，采用福建省电子政务外网进行安全访问，考虑利用福建省电子政务云平台资源。

7.8.1.1. 主机计算资源分析

本项目的建设，主机服务器主要用于数据库服务及应用系统服务，其配置设计主要从以下三个方面来考虑：

（1）CPU 性能主要以服务器的 TPM 值（每分钟所处理的平均事务数）和参考 SPEC Web2005 计算出来的请求数来作为选型参考值，在设计服务器处理能力时，需要将一些实际经验值和所计算值综合考虑，设计 CPU 的使用率在 50%以内；SPEC Web2005 标准的衡量结果是一台 Web 服务器能够有效响应客户端的 Web 请求的最大极限个数。因此，测算的结果是一个 Web 请求数字，单位是个。在评估应用服务器的 SPEC Web2005 值时，通常的方法是通过系统的在线用户，结合其并发率估算出并发用户数，在参照日常业务使用场景中可能发起的 http 请求来进行估算。SPEC Web2005 的参考估算公式如下：Web 访问响应能力（SPEC Web2005）＝（在线用户数×并发率×在线用户平均发起 http 请求数）/（1－冗余率）。

（2）内存是所有程序运行的环境，内存设计时需要从不同应用要求的角度来考虑，根据经验分析，不管是 Web 服务器还是数据库服务器对内存和 CPU 的开销相对较大，众多用户在远程访问，对其响应速度比较敏感，应保证有充足的资源。

（3）磁盘 I/O 性能是容易产生瓶颈的地方，在 CPU 处理能力一定的情况下，磁盘 I/O 速度会使服务器的整体性能差异很大，一般磁盘 I/O 选择尽量的大，同时考虑到单个磁盘的 I/O 速度是一定的，需要靠多磁盘的并行读取来提高磁盘 I/O 性能，在容量和性价比容许的情况下，尽量选择容量较小而数量多的磁盘，能大大提高磁盘的 I/O 吞吐性能。

1．应用支撑平台计算资源

应用支撑服务平台，为省智慧消防平台的开发、部署、运行提供所需的公共性、基础性支撑服务。服务器部署应用包括基础平台应用和中间件。

类别	系数	系数描述	用户设定	系数说明	备注
业务基础参数	A	用户数量（个）	15000	应用系统的用户数量	使用需求估算
	B	每日活跃用户比例（%）	60	每日活跃用户占比	
	C	用户平均每日打开次数（次）	20	用户每日访问应用的次数	
	D	用户单次打开请求数量（次）	12	单次访问应用的平均请求数	

	E	每日活跃时段访问数量占比（%）	80	活跃时段的访问数量与访问总量的比值	
	F	用户主要活跃时间段（小时）	8	用户访问应用的主要活跃时段(如集中在上班时间)	
	G	活跃时段平均响应时间（秒）	3	应用系统响应用户访问的平均时长（普通应用一般在0.2~3 秒期间）	
	H	业务访问峰值系数	1.6	较活跃时段平均访问数的倍数（普通应用一般在 1~2 倍期间）	
	I	系统性能冗余系数(%)	25	考虑系统资源的冗余（普通应用一般在 20~30%期间）	
计算资源配置选型参考指标	P	应用访问并发数	800	计算公式：A*(B/100)*C*D*(E/100)/(F*60*60)*G*H/(1-I/100)	
计算资源配置	CPU(核)		4	内存(GB)	16

2．业务应用系统资源计算

（1）物联网感知网管理中心应用服务器

用于接入消防物联网前端设备，对全省所有感知分中心的物联网设备进行统一管理。单台服务器支持接入，支持虚拟化部署。

CPU：系统运行后操作系统占据约 1GHz，其余组件 JDK、Tomcat 预计使用 6.5 GHz，共计 7.5 GHz，按单核 CPU 提供 2.4 GHz 计算，所有 CPU 资源需要 7.5÷2.4≈3.16 核，按冗余计算需要申请 4 核。

内存：centos 根系统占用 0.5G，设备接入和数据采集 4G，消防数据处理 4G，数据自动化检查 4G，数据加密处理 4G，共计 0.5+4+4+4+4=20.5G+8G=16.5G，2 高峰值预留 20%，共计 24G。

（2）消息中心应用服务器

用于对各感知网分中心的消防物联网监测数据监听、采集和传输，以及实现省

平台与各感知分中心之间的消息通讯。单台服务器部署。

CPU：系统运行后操作系统占据约 1GHz，其余组件 JDK、Tomcat 预计使用 12GHz，共计 13 GHz，按单核 CPU 提供 2.4 GHz 计算，所有 CPU 资源需要 13÷2.4≈5.4 核，按冗余计算需要申请 6 核。

内存：centos 根系统占用 0.5G，消防数据监听 4G，消防数据通讯 4G，共计 0.5+4+4=8.5G，2 高峰值预留 20%，共计 16G。

（3）视频接入应用服务器

支持视频接入、视频流媒体转发、视频存储管理等，满足不少于 5000 路前端的管理和应用。

CPU： 系统运行后操作系统占据约 1GHz，其余组件预计使用 6 GHz，共计 7 GHz，按单核 CPU 提供 2.4 GHz 计算，所有 CPU 资源需要 7÷2.4≈2.91 核，按冗余计算需要申请 4 核；

内存：centos 系统占用 0.5G，系统管理模块 1G，视频联动 2G，视频监控 2G，其他功能组件预计 8G，共计 0.5+1+2+2+8=13.5G，高峰值预留 20% 以及考虑冗余，申请 16G。

（4）数据存储服务器

用于物联网监测与分析数据、感知网数据、视频监控分析数据、预警数据、事件处置数据、考核业务数据、值班监控数据、大数据分析、一张图展示数据、消防远程教育培训数据等的存储，以及对数据处理加工管理。多台服务器部署。

CPU：系统运行后操作系统占据约 1GHz，其余组件 JDK、Tomcat 预计使用 6.5 GHz，共计 7.5 GHz，按单核 CPU 提供 2.4 GHz 计算，所有 CPU 资源需要 7.5÷2.4≈3.16 核，按冗余计算需要申请 4 核。

内存：centos 根系统占用 0.5G，设备接入 4G，数据存取 8G，共计 0.5+4+8=12.5G，高峰值预留 20%，共计 16G。

（5）文件存储服务器

用于对省级智慧消防平台各应用子系统的物理文件资料进行统一文件存储、形成文件流机制，提高物理文件资料存取效率。多台服务器部署。

CPU：系统运行后操作系统占据约 1GHz，其余组件 JDK、Tomcat 预计使用 6.5 GHz，共计 13 GHz，按单核 CPU 提供 2.4 GHz 计算，所有 CPU 资源需要 13÷2.4≈3.16 核，

按冗余计算需要申请 6 核。

内存：centos 根系统占用 0.5G，设备接入 4G，数据存取 8G，共计 0.5+4+8=12.5G，高峰值预留 20%，共计 16G。

（6）消防综合业务应用服务器

支持：（1）消防物联网远程监控管理、消防资源数据库的管理、消防数据研判、可视化监管、消防落实管理、灭火救援智能决策分析；（2）消防值班监控业务管理；（3）消防教育远程培训服务平台。满足总队、支队、大队、救援站等各级消防部门的使用，以及满足值班运维单位、相关消防外联机构、社会公众的使用需求。多台服务器部署。

CPU：系统运行后操作系统占据约 1GHz，其余组件 JDK、Tomcat 预计使用 12 GHz，共计 7.5 GHz，按单核 CPU 提供 2.4 GHz 计算，所有 CPU 资源需要 13÷2.4≈5.4 核，按冗余计算需要申请 6 核

内存：centos 根系统占用 0.5G，前端展示 2G，基础信息管理 2G，消防监督业务数据管理 2G，消防研判预警 4G，可视化监管 2G，消防责任落实 2G，消防态势感知 2G，消防智能决策辅助 2G，事件管理 1G，事件响应 1G，系统管理 1G，应用支撑平台组件 1G，共计 0.5+2+2+2+2+2+2+2+2+2+1+1+1+1=22.5G，高峰值预留 20%，共计 24G。

（7）大数据分析及可视化综合展示应用服务器

支持将各类系统的资源和数据进行深度的分析和展示上墙功能，呈现消防设施情况、消防管理数据分析、警情分析、隐患分析、故障分析、天气等情况。单台服务器部署。

CPU：系统运行后操作系统占据约 1GHz，其余组件 JDK、Tomcat 预计使用 6.5 GHz，共计 7.5 GHz，按单核 CPU 提供 2.4 GHz 计算，所有 CPU 资源需要 7.5÷2.4≈3.16 核，按冗余计算需要申请 4 核

内存：centos 根系统占用 0.5G，前端展示 4G，事件管理及调度 4G，系统管理 1G，应用支撑平台组件 1G，共计 0.5+4+4+1+1=10.5G，高峰值预留 20%，共计 16G。

3．数据交换服务计算资源

数据交换服务部署系统的接口服务及政务外网互联网接入区与数据库管理系统的数据转发。单台服务器部署。

CPU：系统运行后操作系统占据约1GHz，其余组件JDK、Tomcat预计使用6.5 GHz，共计7.5 GHz，按单核CPU提供2.4 GHz计算，所有CPU资源需要7.5÷2.4≈3.16核，按冗余计算需要申请4核。

内存：centos根系统占用 0.5G，数据交换4G，数据检查2G，数据处理4G，共计0.5+4+2+4=10.5G，高峰值预留20%，共计16G。

7.8.1.2. 服务器配置清单

在满足福建省智慧消防云平台资源使用需求的基础上，本着节约硬件资源投入的原则，根据信息系统主机计算资源分析可得，本次项目需要的虚拟机计算资源主要由电子政务云平台提供，包括应用服务器和数据库服务器，数量为：18台。

详细规划如下：

编号	项目名称	主要性能指标	单位	数量	部署说明
1	物联网感知网络管理中心服务器	政务云平台虚拟机，4核CPU，24GB内存，WindowsServer2008R2（64 位）操作系统或LINUX操作系统（如已国产化）	台	1	由政务云平台提供
2	消息中心应用服务器	政务云平台虚拟机，6核CPU，16GB内存，WindowsServer2008R2（64 位）操作系统或LINUX操作系统（如已国产化）	台	1	由政务云平台提供
3	视频接入应用服务器	政务云平台虚拟机，4核CPU，16GB内存，WindowsServer2008R2（64 位）操作系统或LINUX操作系统（如已国产化）	台	1	由政务云平台提供
4	文件存储服务器	政务云平台虚拟机，4核CPU，16GB内存，WindowsServer2008R2（64 位）操作系统或LINUX操作系统（如已国产化）	台	1	由政务云平台提供
5	消防综合业务应用服务器	政务云平台虚拟机，6核CPU，24GB内存，WindowsServer2008R2（64 位）操作系统或LINUX操作系统（如已国产化）	台	4	由政务云平台提供
6	大数据分析及可视化综合展示应用服务器	政务云平台虚拟机，4核CPU，16GB内存，WindowsServer2008R2（64 位）操作系统或LINUX操作系统（如已国产化）	台	1	由政务云平台提供

7	数据交换应用服务器	政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）	台	1	由政务云平台提供
8	数据库服务器	政务云平台提供数据库实例 D02（ORACLE，数据库空间大小 80G、归档日志空间大小 16G、用户业务空间 40G、索引表空间（index）16G、回滚表空间（undo）4G、临时表空间（temp）4G、Redo 文件 256MB*6） 政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）	套	8	由政务云平台提供

7.8.1.3. 存储资源计算分析

本项目有大量的基础数据，包括：消防基础数据、消防监督业务数据、物联网接入数据、日志类数据等相关，具体数据存储规模和类型包括如下：

1．消防基础数据：消防基础数据包括联网火灾风险单位信息、建筑物信息、管理机构、消防警力、救援力量、重点部位、消防设施及消防设施部件等基础数据，一次性建库大约需要 3T。

2．消防监督业务及物联网接入数据：消防的业务数据包括巡查、自查自纠、运营服务机构数据接入、以及每日消防巡查业务、视频图像火灾系统等都有产生图片数据，按每日一次巡查及自查自纠数据来计算，一次产生的数据量为 10M。每年产生的数据量预计为 10M*15000*365=3650000M≈52T。（全省首期约 15000 家火灾风险单位）

3．消防物联网接入数据：本次物联网接入的业务数据包括用户信息传输装置、消防电源检测模块、室外消火栓监控终端和消防水监测点等，数据上传周期为 10 秒，合计数据量约为1024字节（1k），每个设备每年产生的数据量为6*60*24*365*1k≈3G，预留全省 6000 家单位的接入能力，即每年产生数据量为 3G*6000=180000G≈180T。根据监测数据的更新周期和监测数据保管期限，按监测数据存储 3 个月计算，消防物联网监测数据所需存储容量为 180T/4≈45T。

综上所述，以上 3 种数据 3 年产生的数据为：（0.3T*10 年）+（52T*10 年）+45T（固定值）≈568T。**考虑到备份数据所占存储空间、缓存数据、日志数据、日常事**

务数据等，系统建设完成后的每年数据量大约为 1.5T。

因此，建议 10 年数据存储量按 100TB 考虑。考虑到部分原始数据的存储保管周期为 2-5 年（取中间值 3 年），因此，向福建省数字办政务云计算平台申请的空间约为 100TB/3 年=33.33TB，取整为 40TB。

7.8.2. 感知网分中心存储容量估算

根据福建省消防情况分析全省总有有 15000 家火灾风险单位，平均每家火灾风险单位接入 20 台设备。以智慧用电为例，智慧用电正常是 20 秒发送一次数据给平台，每次发送约等于 1KB 的数据；那么每天一个智慧用电设备差不多接收 4320 次数据，一个设备每天需要存储的空间是 4.3M 的数据存储空间，那么全省一天的数据存储空间约 1.296T 的设备原始数据，百天数据存储高达 129.6TB 设备原始数据，全省一年的数据量达到 473TB 设备监测原始数据存储。

根据全省（含省、市、县）有 94 个消防监管单位，每个单位设置一个监测数据中心节点。那么平均每个感知网分中心需对接 15000*20/94≈3200 台监测设备，每百天需存储 1.3T 的设备监测原始数据，一年差约为 5T 的原始数据。

按照 10 年存储，每个感知网分中心节点需要 5T*10 年=50TB 的数据存储容量。

本设计方案仅对感知网分中心的数据存储容量进行测算，具体感知网分中心存储设备由各地市、区县自行采购，不计入本次设计方案的存储资源费用计算范畴。

7.9. 业务部署方案（分级/分布式部署）

省智慧消防云平台业务应用系统、数据库存储系统等，部署于上述服务器配置清单中规划的 18 台各类型用途云主机服务器中。

同时由各地市、区县消防部门自建部署的消防物联网感知分中心服务器（分布式），通过政务外网汇聚接入至省智慧消防云平台服务器中。

7.10.云平台费用测算表

7.10.1. 云主机资源费用测算

类目	VCPU（核）		内存（G）		硬盘（G）		操作系统	云负载均衡	公网IP（个）	MYSQL云数据库	ORACLE数据库	云数据	云存储(G)		云备份（实例）	对象存储（G）	物理机租用		
	虚拟机	数据库	虚拟机	数据库	虚拟机	数据库							NAS	备份			通用型	容量型	性能型
数量	82	0	328	0	50000	8000	18	0	0	0	8	0	27000	0	0	0	0	0	0
	82		328		13000								27000						
单价（元/年）	380.1		543		6.516		434.4	760.2	0	15204	27150	15204	5.43		13575	3.6	33120	52992	81696
年预算（元/年）	31168		178104		84708		7819	0	0	0	217200	0	146610		0	0	0	0	0
年预算合计（万元））	≈66 万元/年																		

按照平台软件应用年限至少 8 至 10 年以上，本次福建省智慧消防云平台租赁云

计算平台的年限，按 8 年计，由省财政预算拨付支出。

7.10.2. 云平台安全服务（虚拟化）费用测算

按照计算机信息系统安全等级保护制度（等级：三级），为保障福建省智慧消防云平台软件应用及云计算平台的安全防护措施，须租赁以下几项信息安全及网络安全虚拟化防护应用。

序号	安全区域	产品名称	数量	等保要求	备注
1	核心交换区	1 防火墙	2	网络安全－访问控制－网络边界部署防火墙或网闸 部署在核心交换区的边界 等保三级要求	
		2 入侵防御系统	1	网络安全－入侵防范－入侵防御系统 分别部署在核心交换区的边界	
		3 防毒墙	1	网络安全－而已代码防范－防病毒网关 分别部署在核心交换区的边界 等保三级要求	
		4 下一代防火墙	1	网络安全－结构安全－重要网段之间应采用防火墙进行隔离 部署在外网服务器区边界 等保三级要求	
		5 防火墙	1	结构安全－重要网段之间采用防火墙进行隔离 部署在安全管理区的边界	
2	安全管理区	6 终端安全管理系统	1	非法外联检查与控制、终端软件安装管控	

		7 入侵检测系统	1	网络安全－入侵防范－入侵检测系统 旁路部署在外网核心交换机上	
		8 安全审计系统	1	网络安全－安全审计－网络日志审计	
		9 堡垒机	1	网络安全－安全审计－网络运维管理安全审计	
		10 虚拟化安全管理系统	1		
		11 准入控制系统	1	网络安全－边界完整性检查－采用准入控制系统，实现准入控制	
3	外网服务器区	12 数据库审计系统	1	应用安全－安全审计－数据库安全审计系统	
4	内外网边界	13 安全隔离与信息交换系统	1	网络安全－访问控制－网络边界部署防火墙或网闸 部署在内外网之间	

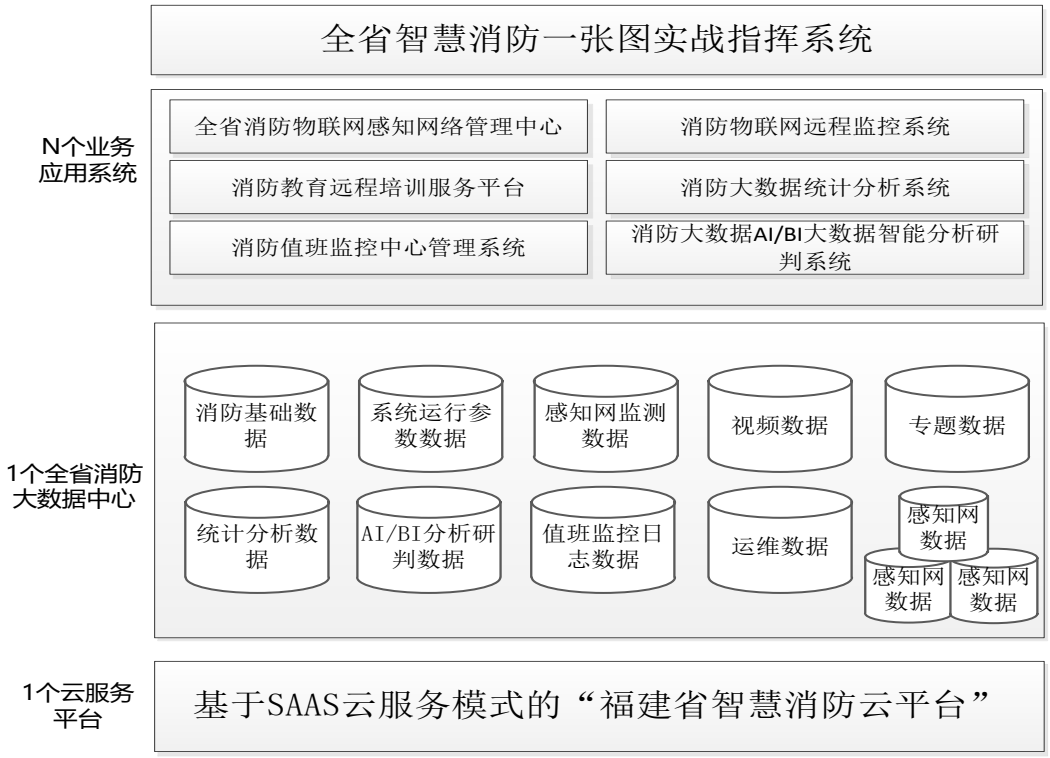
以上属于计算机信息安全等级保护的物理部署清单，可根据电子政务云计算平台的虚拟化安全服务产品，结合三级等保要求进行选择租赁和虚拟化安全部署。

第8章 应用架构设计

8.1. 应用系统总体架构

8.1.1. 1+N 应用设计目标

根据福建省消防救援总队关于智慧消防云平台的总体规划思路，以及符合福建省消防救援总队提出的建立“1 个智慧消防大数据平台，N 个消防应用系统”的智慧消防体系构想，本次将遵循该理念思想进行“1+N”平台应用设计。



8.1.2. 设计原则

为保障和满足系统平台应用软件运行使用的可持续性和跟随业务发展变化的适应性要求，本次福建省智慧消防云平台在软件平台应用架构方面的设计，要求遵循以下几个原则：

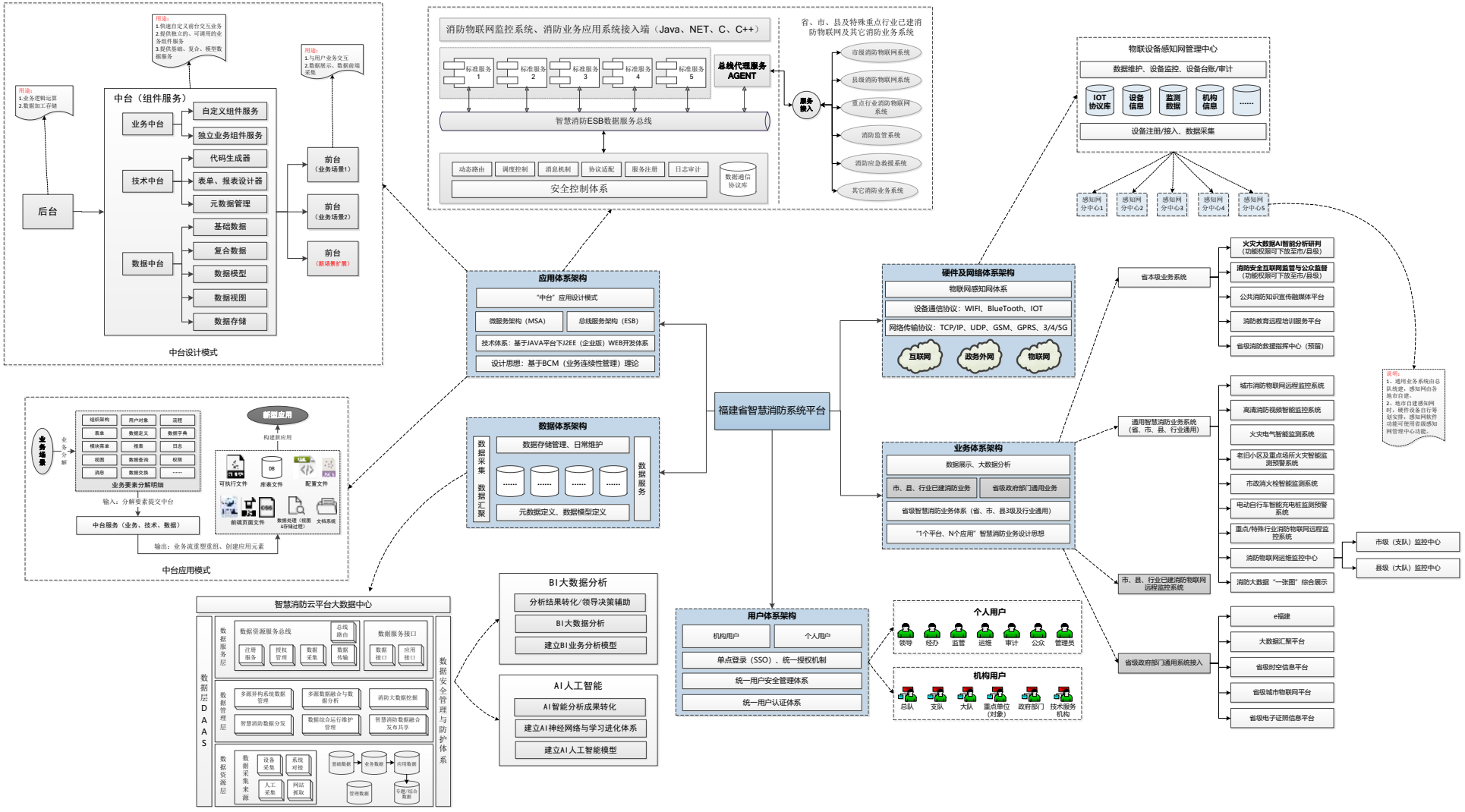
1. 稳定性。软件系统的稳定性主要涉及系统框架设计底层支撑功能的高稳固性、

高并发性等要素特点，能够持续不断地提供功能支撑和并发响应支撑，将平台软件的功能故障率、服务中断率、响应迟滞率等降低到不影响业务连续性的最低水平要求，这样才能极大增强软件系统的生命力和延长系统平台生命周期。

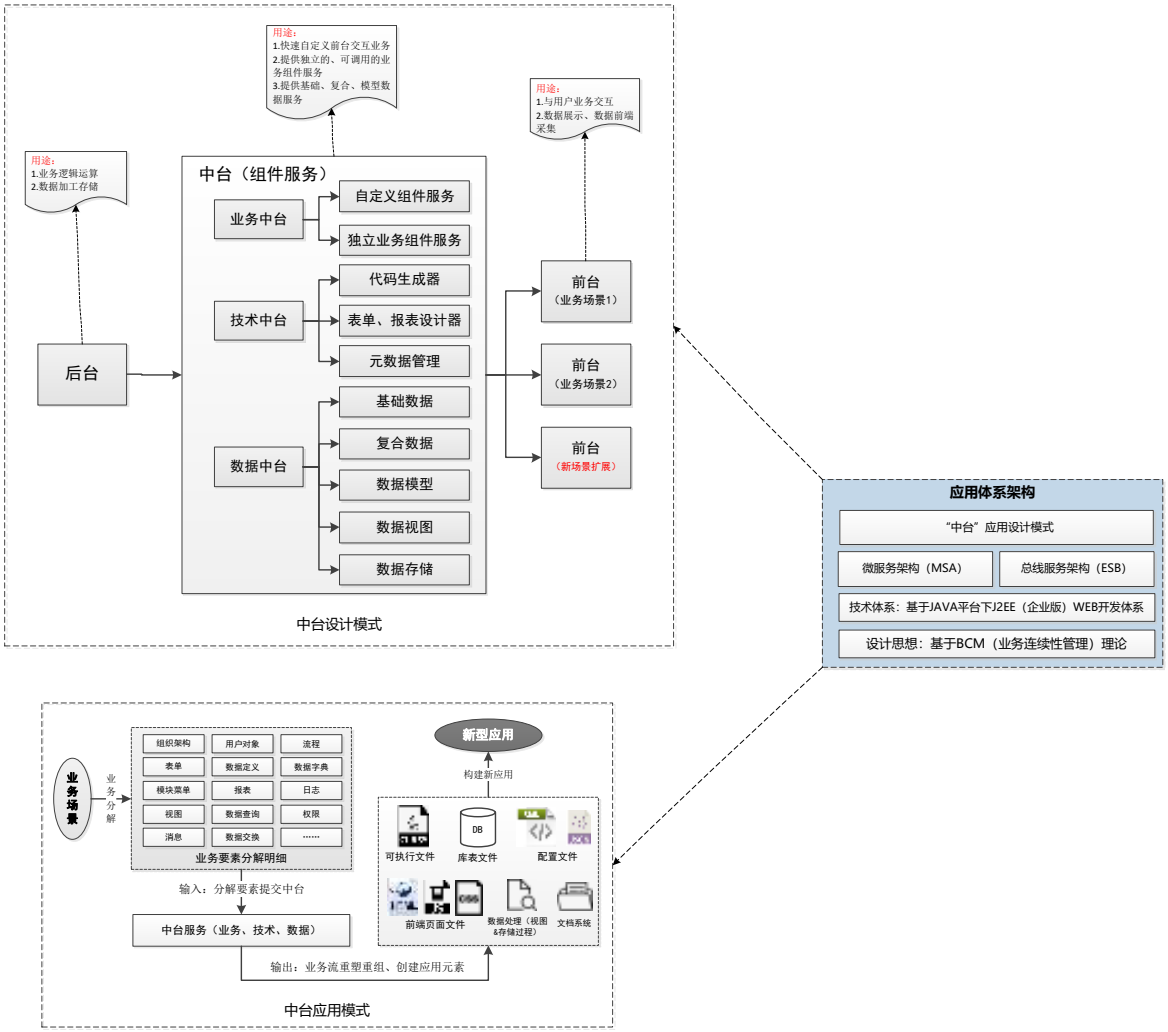
2．连续性与可扩展性。针对业务变化性强的软件系统，必须具备较强的连续性和可扩展性，也就是说，要在已开发完成且在正常运作的软件系统增加或变更业务功能，必须在较短的时间周期内完成业务功能新增或变更，并快速投入使用，且不影响软件系统本身已有功能的正常运作，或将影响运作的周期控制在最低水平。

3．可配置性。通常情况下，许多业务软件系统进行业务功能变更时，可通过两种方式来完成：（1）原生代码二次开发；（2）可视化模块组件配置开发。一个可管理性强、具备可运维管理的平台软件系统，随着业务的发展变化要对业务功能进行新增或变更时，要求不依赖于进行原生代码的修改或重构来完成业务新增变更，而是通过可视化模块配置方式来快速完成业务功能的变更或新增。

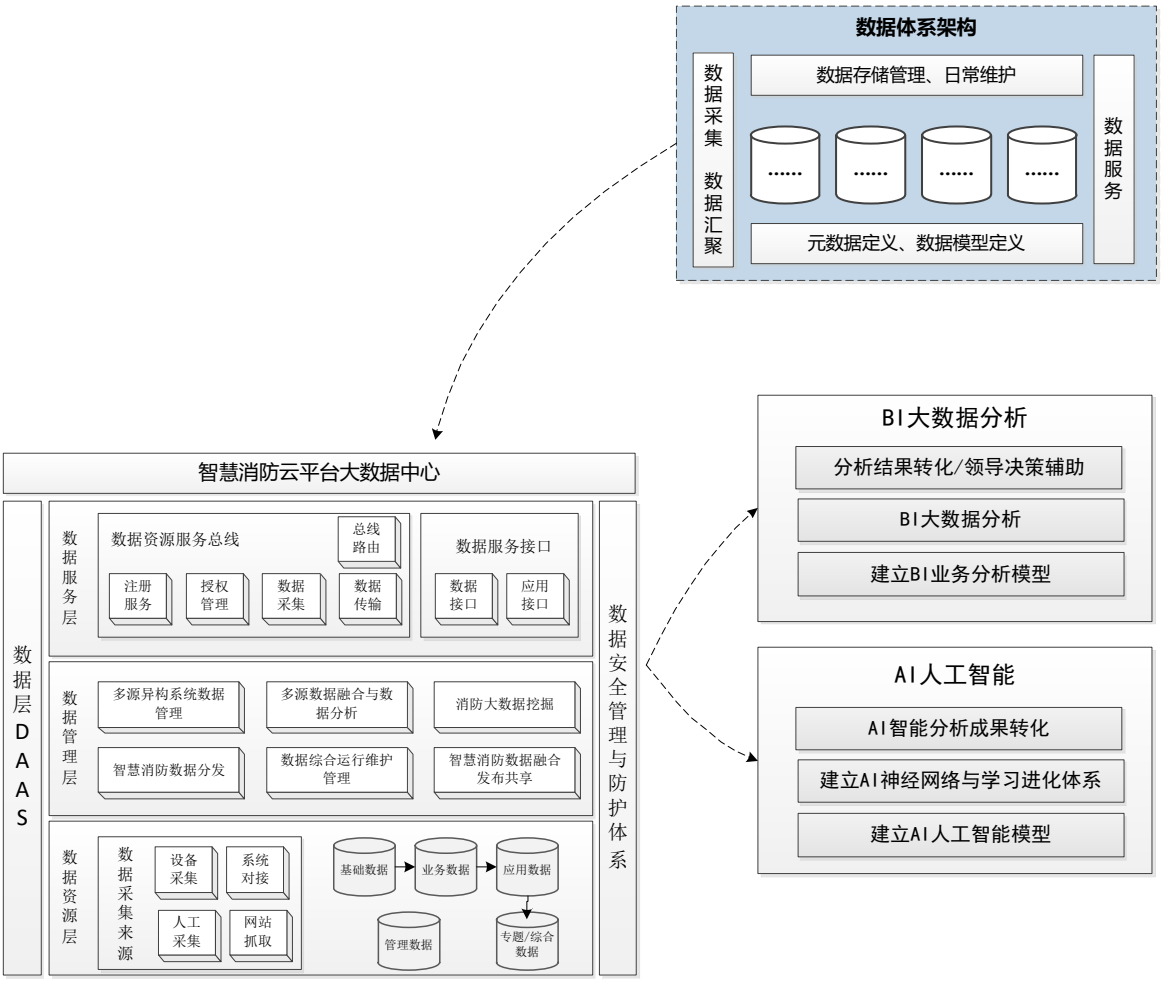
设计思路属于框架性原则，背离该设计思想，将极有可能导致项目建设周期延长、建设成果返工、建设成本增加等，甚至导致项目建设以失败告终。


中台（组件服务）
业务中台
技术中台
数据中台
自定义组件服务
独立业务组件服务
代码生成器
表单、报表设计器
元数据管理
基础数据
复合数据
数据模型
数据视图
数据存储
后台
前台（业务场景1）
前台（业务场景2）
前台（新场景扩展）
中台设计模式
消防物联网监控系统、消防业务应用系统接入端（Java、NET、C、C++）
标准服务1
标准服务2
标准服务3
标准服务4
标准服务5
总线代理服务AGENT
智慧消防ESB数据服务总线
动态路由
调度控制
消息机制
协议适配
服务注册
日志审计
安全控制体系
数据通信协议库
服务接入
省、市、县及特殊重点行业已建消防物联网及其它消防业务系统
市级消防物联网系统
县级消防物联网系统
重点行业消防物联网系统
消防监管系统
消防应急救援系统
其它消防业务系统
物联设备感知网管理中心
数据维护、设备监控、设备台账/审计
IOT协议库
设备信息
监测数据
机构信息
设备注册/接入、数据采集
感知网分中心1
感知网分中心2
感知网分中心3
感知网分中心4
感知网分中心5
应用体系架构
“中台”应用设计模式
微服务架构（MSA）
总线服务架构（ESB）
技术体系：基于JAVA平台下J2EE（企业版）WEB开发体系
设计思想：基于BCM（业务连续性管理）理论
硬件及网络体系架构
物联网感知网体系
设备通信协议：WIFI、BlueTooth、IOT
网络传输协议：TCP/IP、UDP、GSM、GPRS、3/4/5G
互联网
政务外网
物联网
省本级业务系统
火灾大数据AI智能分析研判（功能权限可下放至市/县级）
消防安全互联网监管与公众监督（功能权限可下放至市/县级）
公共消防知识宣传融媒体平台
消防教育远程培训服务平台
省级消防救援指挥中心（预留）
说明：
1、通用业务系统由总队统建，感知网由各地自行建。
2、地市自建感知网时，硬件设备自行筹划安排，感知网软件功能可使用省级感知网管理中心功能。
业务场景
业务分解
组织架构
用户对象
流程
表单
数据定义
数据字典
模块菜单
报表
日志
视图
数据查询
权限
消息
数据交换
……
业务要素分解明细
输入：分解要素提交中台
中台服务（业务、技术、数据）
输出：业务流重塑重组、创建应用元素
中台应用模式
新型应用
构建新应用
可执行文件
库表文件
配置文件
前端页面文件
数据处理（视图&存储过程）
文档系统
数据体系架构
数据采集
数据汇聚
数据存储管理、日常维护
元数据定义、数据模型定义
数据服务
福建省智慧消防系统平台
业务体系架构
数据展示、大数据分析
市、县、行业已建消防业务
省级政府部门通用业务
省级智慧消防业务体系（省、市、县3级及行业通用）
“1个平台、N个应用”智慧消防业务设计思想
通用智慧消防业务系统（省、市、县、行业通用）
城市消防物联网远程监控系统
高清消防视频智能监控系统
火灾电气智能监测系统
老旧小区及重点场所火灾智能监测预警系统
市政消火栓智能监测系统
电动自行车智能充电桩监测预警系统
重点/特殊行业消防物联网远程监控系统
消防物联网运维监控中心
消防大数据“一张图”综合展示
市级（支队）监控中心
县级（大队）监控中心
市、县、行业已建消防物联网远程监控系统
省级政府部门通用系统接入
e福建
大数据汇聚平台
省级时空信息平台
省级城市物联网平台
省级电子证照信息平台
智慧消防云平台大数据中心
数据层DAAS
数据服务层
数据管理层
数据资源层
数据资源服务总线
总线路由
注册服务
授权管理
数据采集
数据传输
数据服务接口
应用接口
多源异构系统数据管理
多源数据融合与数据分析
消防大数据挖掘
智慧消防数据分发
数据综合运行维护管理
智慧消防数据融合发布共享
数据采集来源
设备采集
系统对接
人工采集
网站抓取
基础数据
业务数据
应用数据
管理数据
专题/综合数据
数据安全管理与防护体系
BI大数据分析
分析结果转化/领导决策辅助
BI大数据分析
建立BI业务分析模型
AI人工智能
AI智能分析成果转化
建立AI神经网络与学习进化体系
建立AI人工智能模型
用户体系架构
机构用户
个人用户
单点登录（SSO）、统一授权机制
统一用户安全管理体系
统一用户认证体系
个人用户
领导
经办
监管
运维
审计
公众
管理员
机构用户
总队
支队
大队
重点单位（对象）
政府部门
技术服务机构

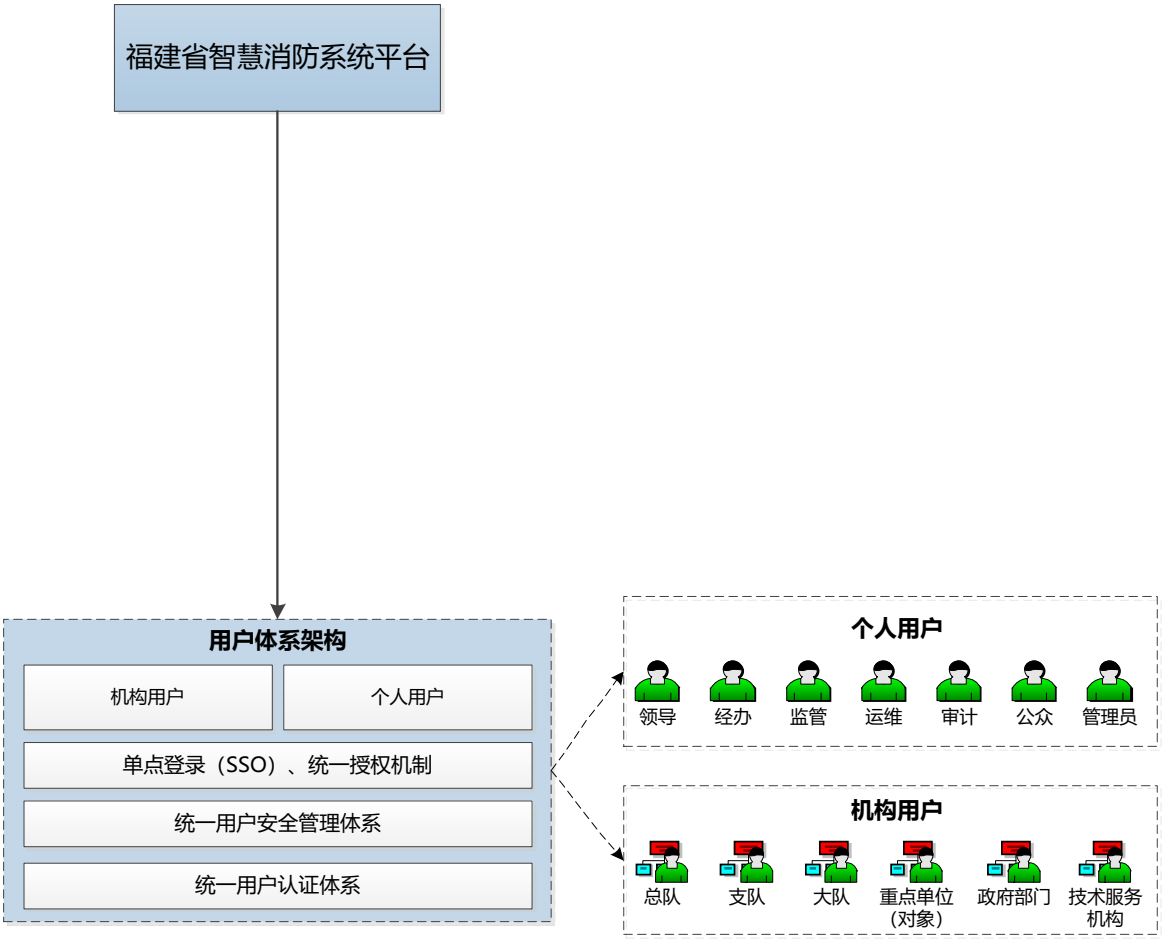
8.1.3. 应用体系架构


用途：
1.快速自定义前台交互业务
2.提供独立的、可调用的业务组件服务
3.提供基础、复合、模型数据服务
用途：
1.与用户业务交互
2.数据展示、数据前端采集
用途：
1.业务逻辑运算
2.数据加工存储
中台（组件服务）
业务中台
自定义组件服务
独立业务组件服务
技术中台
代码生成器
表单、报表设计器
元数据管理
数据中台
基础数据
复合数据
数据模型
数据视图
数据存储
后台
前台
（业务场景1）
前台
（业务场景2）
前台
（新场景扩展）
中台设计模式
应用体系架构
“中台”应用设计模式
微服务架构（MSA）
总线服务架构（ESB）
技术体系：基于JAVA平台下J2EE（企业版）WEB开发体系
设计思想：基于BCM（业务连续性管理）理论
业务场景
业务分解
组织架构
用户对象
流程
表单
数据定义
数据字典
模块菜单
报表
日志
视图
数据查询
权限
消息
数据交换
……
业务要素分解明细
输入：分解要素提交中台
中台服务（业务、技术、数据）
输出：业务流重塑重组、创建应用元素
新型应用
构建新应用
可执行文件
DB
库表文件
配置文件
前端页面文件
数据处理（视图&存储过程）
文档系统
中台应用模式

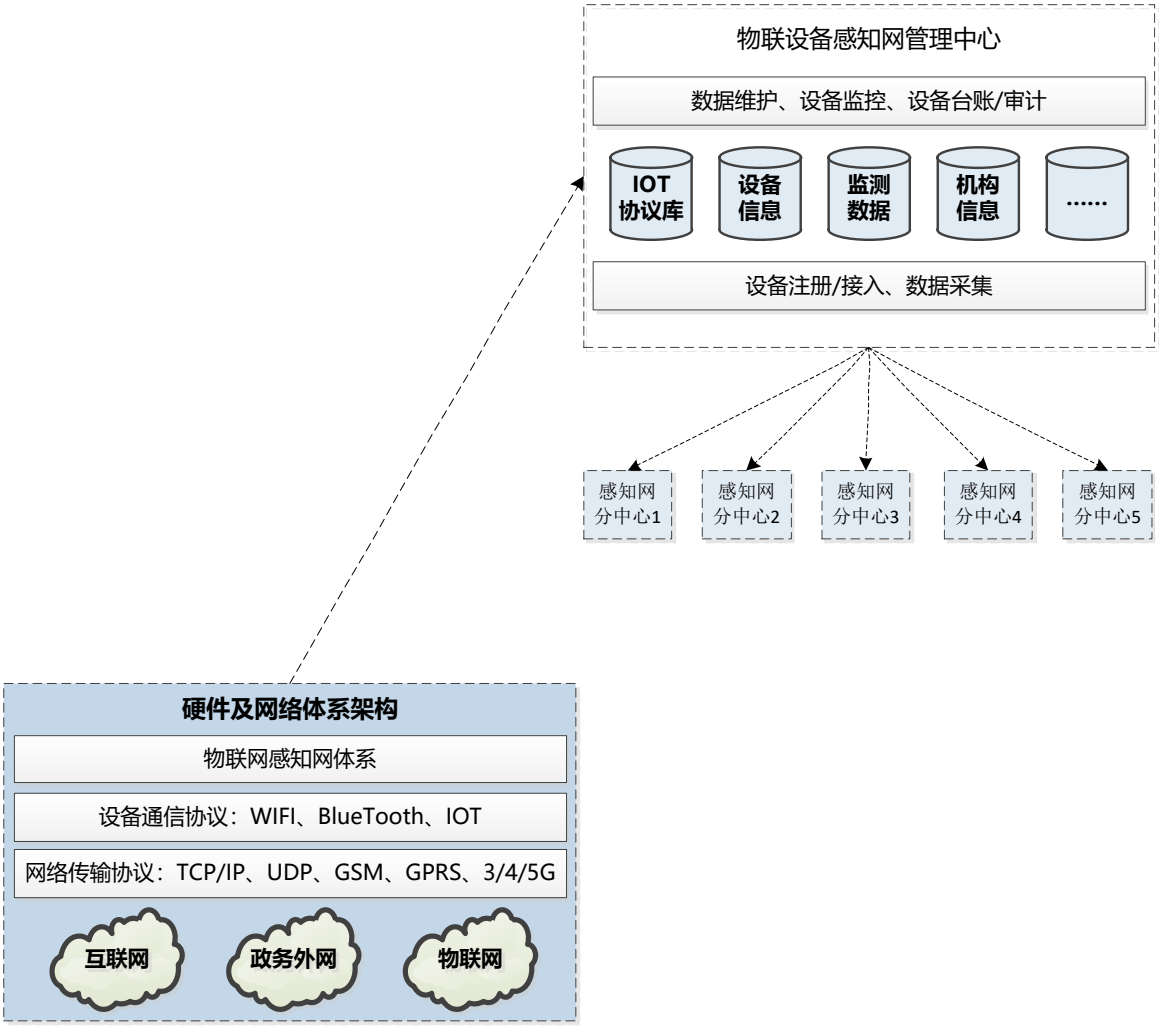
8.1.4. 数据体系架构


数据体系架构
数据采集
数据汇聚
数据存储管理、日常维护
.....
.....
.....
.....
元数据定义、数据模型定义
数据服务
智慧消防云平台大数据中心
数据层DAAS
数据服务层
数据资源服务总线
总线路由
注册服务
授权管理
数据采集
数据传输
数据服务接口
数据接口
应用接口
数据管理层
多源异构系统数据管理
多源数据融合与数据分析
消防大数据挖掘
智慧消防数据分发
数据综合运行维护管理
智慧消防数据融合发布共享
数据资源层
数据采集来源
设备采集
系统对接
人工采集
网站抓取
基础数据
业务数据
应用数据
管理数据
专题/综合数据
数据安全管理与防护体系
BI大数据分析
分析结果转化/领导决策辅助
BI大数据分析
建立BI业务分析模型
AI人工智能
AI智能分析成果转化
建立AI神经网络与学习进化体系
建立AI人工智能模型

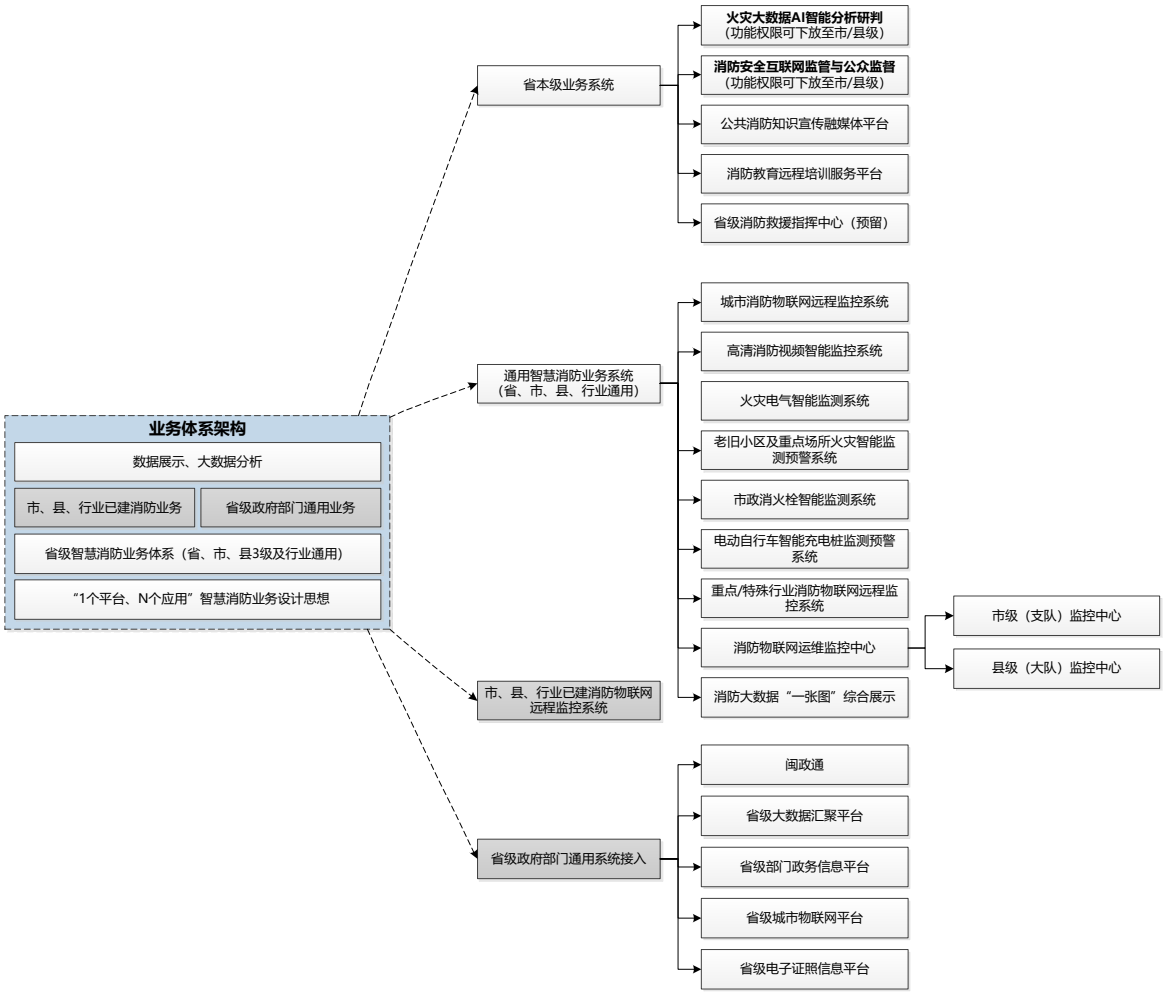
8.1.5. 用户体系架构


福建省智慧消防系统平台
用户体系架构
机构用户
个人用户
单点登录（SSO）、统一授权机制
统一用户安全管理体系
统一用户认证体系
个人用户
领导
经办
监管
运维
审计
公众
管理员
机构用户
总队
支队
大队
重点单位（对象）
政府部门
技术服务机构

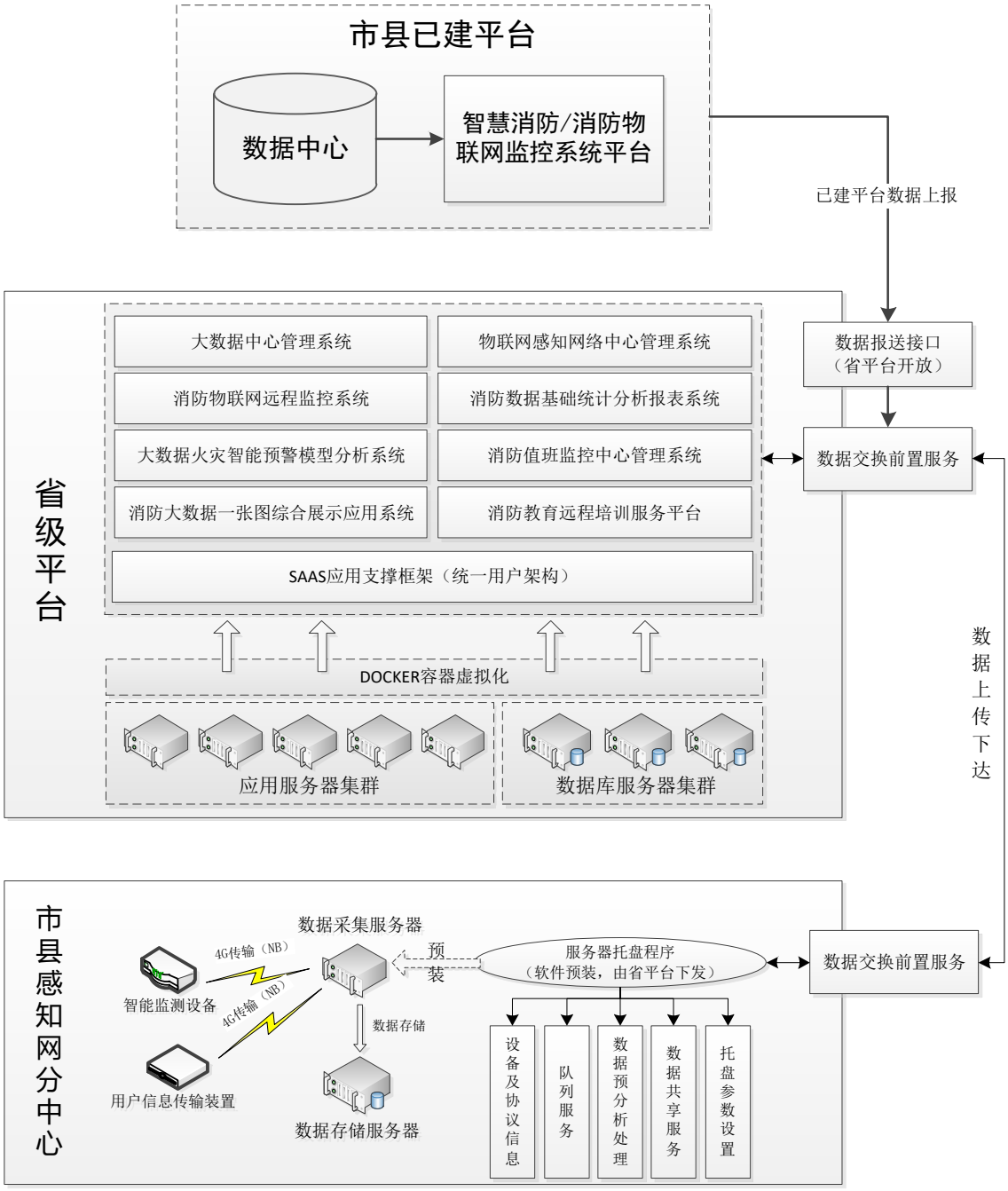
8.1.6. 硬件及网络体系架构



8.1.7. 业务体系架构


业务体系架构
数据展示、大数据分析
市、县、行业已建消防业务
省级政府部门通用业务
省级智慧消防业务体系（省、市、县3级及行业通用）
“1个平台、N个应用”智慧消防业务设计思想
省本级业务系统
火灾大数据AI智能分析研判
（功能权限可下放至市/县级）
消防安全互联网监管与公众监督
（功能权限可下放至市/县级）
公共消防知识宣传融媒体平台
消防教育远程培训服务平台
省级消防救援指挥中心（预留）
通用智慧消防业务系统
（省、市、县、行业通用）
城市消防物联网远程监控系统
高清消防视频智能监控系统
火灾电气智能监测系统
老旧小区及重点场所火灾智能监测预警系统
市政消火栓智能监测系统
电动自行车智能充电桩监测预警系统
重点/特殊行业消防物联网远程监控系统
消防物联网运维监控中心
市级（支队）监控中心
县级（大队）监控中心
消防大数据“一张图”综合展示
市、县、行业已建消防物联网远程监控系统
省级政府部门通用系统接入
闽政通
省级大数据汇聚平台
省级部门政务信息平台
省级城市物联网平台
省级电子证照信息平台

8.1.8. 应用部署架构图



应用部署架构说明：

1. 除了市县已建系统平台外，所有软件应用功能由省级统一建设，并通过 SAAS 模式向省市县三级消防部门用户及其他消防服务机构用户开放账号及权限。

2. 市县消防救援部门自建感知网分中心，并建立本地数据分中心，分中心的数

据及部分应用功能，由省级平台下发并预装于分中心服务器中。

3．省级平台与各感知网分中心通过数据交换前置服务实现数据的上传下达。在福建省智慧消防云平台中，消防物联网智能监测数据约占所有数据的 90%以上，对平台用户而言属于“无感知”数据，可分布存储于各感知网分中心数据库中；余下10%为日常业务数据，对平台用户属于“可感知”数据，存储于省级平台云服务器中。

4．针对市－县已建设完成的智慧消防平台或消防物联网远程监控系统，由省级平台开放数据接口，市县已建系统平台调用该接口进行数据上报。

5．对于未建智慧消防系统的市县消防主管部门，应纳入福建省智慧消防平台的应用下发普及范畴，并针对各级消防主管部门的行政级别与行政管辖特点，可按照不同行政级别的管理需求而开放不同业务权限和数据权限，例如可为市级消防支队开放针对本市各大队的业务管理权限和数据查阅统计权限。

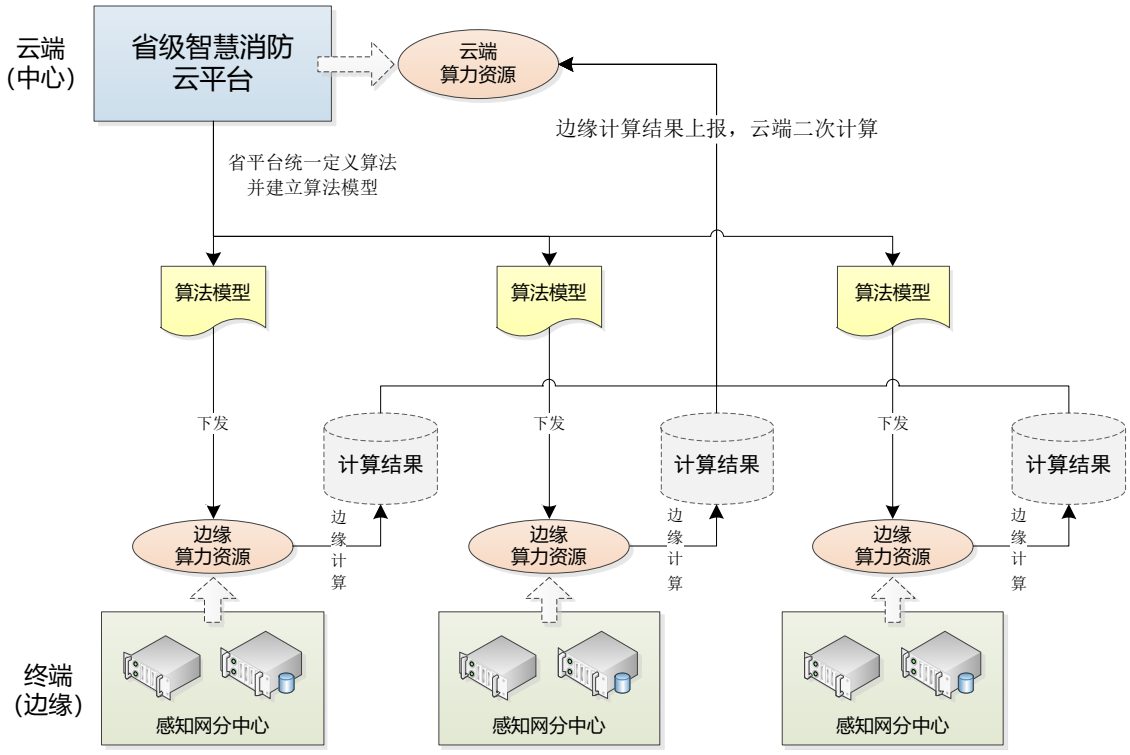
8.1.9. “云边协同”设计

在前面章节提到的由各地市、区县自建物理网感知网分中心，主要功能是用于存储各地市、区县的物联网监测数据、视频监控数据等。感知网分中心除了具有存储功能外，还具有一定的计算能力。为提高整个智慧消防云平台的整体运作性能，可加入“云边协同”设计，通过“边缘计算”降低对云计算的高度依赖性，减轻云计算负担，提高边缘监测分析的时效性。

“云边协同”，是指“云计算”和“边缘计算”的协同，具体应用于“云端”和“终端”同时具有算力资源，且对“实时计算”要求较高的应用场景。通常由于云端算力资源和网络性能的局限性和延迟性，以及终端需要连接众多智能化数据采集设备，为达到“云边”高效协同，可采取中心计算（云）和终端计算（边）相结合的分布式计算方式，充分利用云边各算力资源，实现算力资源负载均衡。

“边缘计算”的算法可通过省平台下发至感知网分中心，算力资源由感知网分中心的服务器资源承担。

具体“云边协同”设计模式见下图：



8.2. 应用系统层设计

8.2.1. 应用系统层模块组件设计

8.2.1.1. 基于云计算架构设计

云计算（Cloud Computing）是当前 IT 领域的热点，它的目的是通过互联网，使用户更加方便、快捷、灵活地使用各种质量保障的 IT 资源，这些资源以服务形式提供。

云计算包括三个主要的层次：基础设施服务（Infrastructure Services）、平台服务（Platform Services）和应用服务（Application Services）。

8.2.1.2. 基于 SOA 的设计理念

面向服务体系结构（service-oriented architecture）简称 SOA，将应用程序的不同功能单元（称为服务）通过这些服务之间定义良好的接口和契约联系起来。接口是采用中立的方式进行定义的，它独立于实现服务的硬件平台、操作系统和编程语言。这使得构建在各种这样的系统中的服务可以以一种统一和通用的方式进行

交互。这种具有中立的接口定义的特征称为服务之间的松耦合。松耦合的好处有两点，一个是它的灵活度，一个是组成整个应用程序的每个服务的内部结构和实现逐渐地发生改变时，他能过继续存在。

8.2.1.3. 基于平台即服务（Platform-As-A-Service, PaaS）

平台即服务（PaaS）将应用运行所需的 IT 资源和基础设施以服务的方式提供给用户，包括了中间件服务，信息服务，连通性服务，整合服务和消息服务等多种服务形式。PaaS 模式，基于互联网提供对应的完整生命周期（包括设计、开发、测试和部署等阶段）的支持，减少用户在购置和管理应用生命周期内所必须的软硬件以及部署应用和 IT 基础设置的成本，同时简化了以上工作的复杂度。为了确保高效地交付具备较强灵活性的平台服务，在 PaaS 模式中，平台服务通常基于自动化的技术通过虚拟化的形式交付，在运行时，自动化，自优化等技术也将被广泛应用，以确保实时动态地满足应用生命周期内的各种 功能和非功能需求。

8.2.1.4. 基于软件即服务（Software-As-A-Service，简称 SAAS）

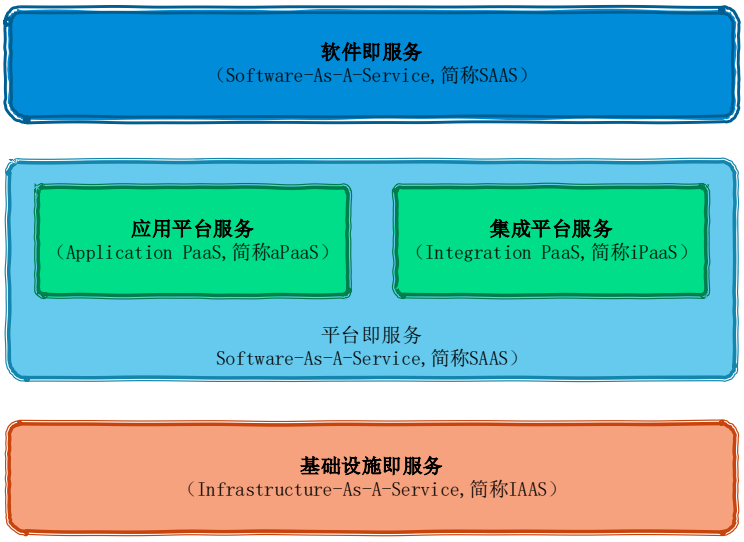
SAAS 是一种将应用软件统一部署在自己的服务器上，通过开放网络（互联网、专用网）向用户提供软件功能服务的租赁，用户无需自建或购买软件系统，无需对软件进行维护，服务商或平台管理单位全权管理和维护软件。服务商或平台管理单位在向客户提供网络应用服务的同时，也提供软件的离线操作和本地数据存储，让用户随时随地都可以使用其租赁的软件和服务。

8.2.1.5. 基于微服务架构（Microservice Architecture）

微服务架构（Microservice Architecture）是一种架构概念，旨在通过将功能分解到各个离散的服务中以实现对解决方案的解耦。把一个大型的单个应用程序和服务拆分为数个甚至数十个的支持微服务，它可扩展单个组件而不是整个的应用程序堆栈，从而满足服务等级协议。围绕业务领域组件来创建应用，这些应用可独立地进行开发、管理和迭代。在分散的组件中使用云架构和平台式部署、管理和服务功能，使产品交付变得更加简单。用一些功能比较明确、业务比较精练的服务去解决更大、更实际的问题。

8.2.2. 应用系统层模块逻辑关系设计

8.2.2.1. 云计算下的服务模型



整个云计算架构分为 3 层：

1. 基础设置即服务层：指把 IT 基础设施作为一种服务通过网络对外提供。在使用模式上，IaaS 与传统的主机托管有相似之处，但是在服务的灵活性、扩展性和成本等方面 IaaS 具有很强的优势。

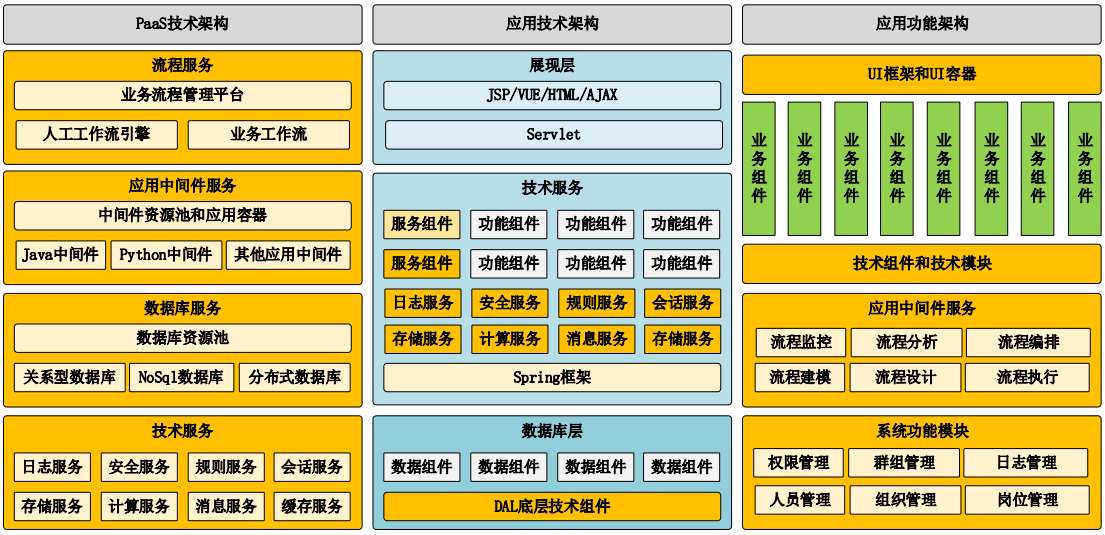
2. 平台即服务层：主要提供 PAAS 技术基础设施和 PAAS 平台服务层。

PaaS 技术基础设施可以理解为 PaaS 底层的技术架构，实现 PaaS 平台的核心技术并和 IaaS 层实现集成。在整个 PaaS 技术架构里面又分为了性能基础能力，云基础能力和管理平台能力三个重要的部分。

3. 软件即服务层：提供平台支撑的、面向终端用户的各个具体应用或业务功能。

8.2.2.2. PAAS 平台总体架构

8.2.2.3. 应用层和 PAAS 平台融合架构图



1. 应用技术架构

在应用的技术架构中，基于传统标准的 J2EE 架构而已，某些组件和能力已经置换为 PaaS 平台已有的组件和能力。其中对于数据层考虑到将 DaaS 进一步封装形成应用技术架构的 DAL 底层技术组件。

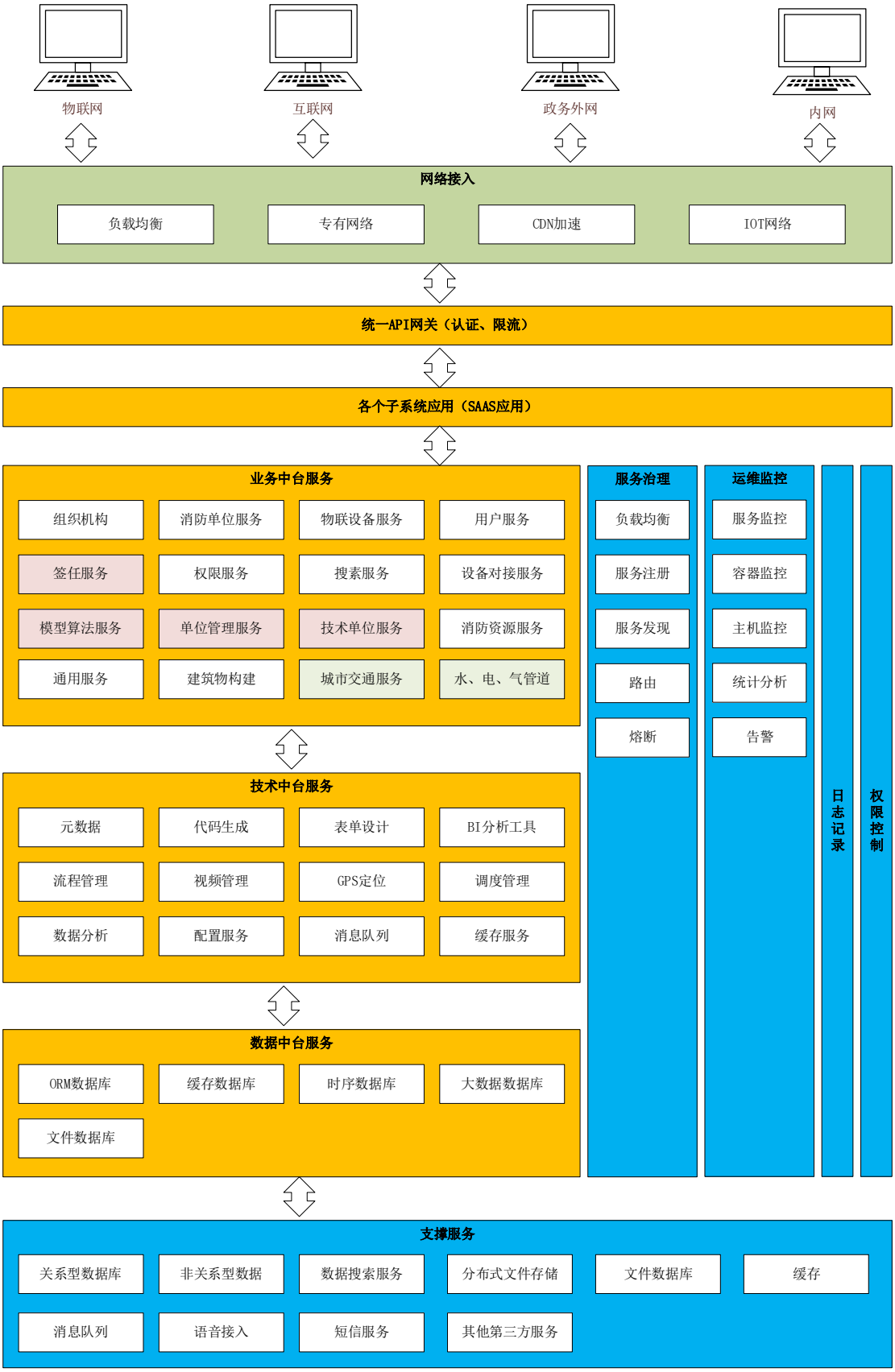
在逻辑层，将考虑引入各种 PaaS 的技术组件，实现日志，缓存，安全，规则，消息，计算等各种技术服务。同时也会引入其他业务组件提供的业务服务。而本身

业务规则层也会暴露相应的业务服务出去。

2. 应用功能架构

在应用功能架构中可以看到对于系统管理，权限管理，工作流管理等平台层功能应该全部由公共的平台层提供相应的能力，这些能力全部集中化提供和存储。业务系统在开发过程中完全不需要开发这部分内容，而仅仅是使用系统管理和流程管理暴露的服务。

8.2.2.4. 应用架构层


物联网
互联网
政务外网
内网
网络接入
负载均衡
专有网络
CDN加速
IOT网络
统一API网关（认证、限流）
各个子系统应用（SAAS应用）
业务中台服务
组织机构
消防单位服务
物联设备服务
用户服务
签任服务
权限服务
搜素服务
设备对接服务
模型算法服务
单位管理服务
技术单位服务
消防资源服务
通用服务
建筑物构建
城市交通服务
水、电、气管道
服务治理
负载均衡
服务注册
服务发现
路由
熔断
运维监控
服务监控
容器监控
主机监控
统计分析
告警
日志记录
权限控制
技术中台服务
元数据
代码生成
表单设计
BI分析工具
流程管理
视频管理
GPS定位
调度管理
数据分析
配置服务
消息队列
缓存服务
数据中台服务
ORM数据库
缓存数据库
时序数据库
大数据数据库
文件数据库
支撑服务
关系型数据库
非关系型数据
数据搜索服务
分布式文件存储
文件数据库
缓存
消息队列
语音接入
短信服务
其他第三方服务

1. 网络接入层接入外部网络和内网络的通讯入口。

2. 统一 API 网关（认证、限流）系统与外界联通的入口，我们在网关进行处理一些非业务逻辑的逻辑，比如权限验证，监控，缓存，请求路由等等。在我们系统中由于同一个接口新老两套系统都在使用，我们需要根据请求上下文讲请求路由到对应的接口。对于鉴权操作不涉及到业务逻辑，那么可以在网关层进行处理，不用下层到业务逻辑。由于网关是外部服务的入口，所以我们在这里监控我们想要的数据，比如入参出参，链路时间。对于流量控制，熔断降级非业务逻辑可以统一放到网关层。

3. 各个子系统应用（SAAS 应用）是网关通过权限过滤到具体的应用系统实体。网关向应用请求具体的应用子系统，由应用子系统针对业务做相应的业务处理和跟平台进行接口对接。

4. 业务中台包含了针对性的业务逻辑整合的业务处理逻辑单元，在各个业务中台服务内运行和存储各个业务中台服务的数据，以实现数据分离和业务重复利用，防止重复造车和快速搭建应用系统的模块。同时平台采用微服务架构可以方便的扩展中台服务。中台包含以下一些常用服务：

（1）用户服务：管理平台系统和应用系统的各种不同类别的用户信息，可以实现用户通过不同的渠道登录到平台上去操作，方便不同的应用子系统之间的用户是互通。

（2）组织结构服务：管理不同应用系统和不同类型的单位的组织架构，在同一个单位内部不同应用子系统跟用户一样实现统一组织结构管理，防止重复录入。

（3）签认服务：主要是用于各个应用子系统之间的系统认证。

（4）权限服务：主要是用于各个应用子系统的权限控制。

（5）消防单位管理：管理全省的各级消防单位基础信息和消防单位的人员配备和装备配备情况，以方便各级消防紧急指挥中心可以第一时间了解管辖范围内的消防力量配备用于提供消防救援第一手资料。省级消防管理单位通过消防单位管理信息可以了解到各级市、县的消防力量配备。

（6）单位管理服务：根据各个行业类别管理各个管理单位的信息，以方便记录很管理各个单位的信息和消防状况记录。

（7）技术单位服务：同一个管理各个技术服务单位的信息，管理技术管理单位的人员配备情况和各类资质管理。方便各级消防管理单位对各个技术服务单位的监管。

（8）物联设备服务：登记各种类别的物联网设备，可以控制设备的状态和下发指令给设备。

（9）设备对接服务：管理各个厂商设备的通讯接口和通讯协议，实现一个协议库方便设备对接。协议库可以实现不同厂商不同型号的数据通讯协议的解析标准，以实现设备采集的数据跟省级平台的大数据平台的数据标准协议进行一层数据转换和清洗。

（10）消防资源服务：主要管理市政消防栓、消防水池、微型消防站等等各类消防资源信息，已方便消防救援时可以统筹消防资源。消防资源包括消防主管单位和各级政府单位、企事业单位等各类社会消防力量，是全民消防的一部分。

（11）建筑物构建：平台提供一套建筑建模管理和城市建模管理的数据模型管理。建筑物数据为以后虚拟现实和数字孪生提供数据支撑。

（12）城市交通服务：主要是对接智慧城市的交通接口，实现实时掌握城市交通情况，实现查看各个街道的交通情况和视频情况统一分配支援，可以实现跨部门的救援协作。

（13）水、电、气等服务：主要是对接第三方平台应用，实现对各种消防民生资源的统筹管理，为消防救援提供救援地点的周边的情况的了解。

5.技术中台主要提供给业务中台和各个应用子系统各种技术点的支撑，以实现一些常用技术或大型技术框架的重复利用。可以通过技术中台和业务中台配合实现快速搭建一个应用子系统或一个业务模块。

（1）元数据是只管理业务模块的各种数据配置，例如：表单、视图、查询配置等。

（2）代码生成是用于基于平台规则生成可执行的代码，方面开发者做二次开发用。

（3）表单设计主要是针对表单的内容设计表单的展示方式和部分逻辑。

（4）BI 分析工具是用来将平台中现有的数据进行有效的整合，快速准确的提供报表并提出决策依据，帮助使用者做出明智的业务决策。BI 分析工具是由

数据仓库（或数据集市）、查询报表、数据分析、数据挖掘、数据备份和恢复等部分组成的、以帮助企业决策为目的技术及其应用。

（5）流程管理主要是管理平台的业务流程的走向的一套完整的流程管理工具，帮助应用子系统快速的搭建流程并应用。流程管理服务包括流程定义、流程发布、流程停止、流程控制等一系列流程管理服务。

（6）视频管理主要管理各个单位对接过来的各个厂商或平台的视频监控信息，方便监管单位或使用单位实时查看视频监控等操作。

（7）GPS 定位主要提供地图引擎和定位服务，方便消防救援和消防防控快速定位报警位置。

（8）调度管理主要是服务应用子系统定时任务的执行情况，主要有创建调度任务、停止调度任务和执行调度任务等。

（9）数据分析主要是提供一系列数据分析模板库，为后面的分析管理和智能分析提供分析算法库；还提供了一系列数据分析的执行过程编排，为数据分析提供算力支撑。

（10）配置服务主要是为平台或 SAAS 应用提供一个统一配置界面，可以指定配置信息分发到具体的应用或局部模块当中去。

（11）消息队列提供系统的队列的支撑，为异步操作或接收数据比较频繁的业务提供一个缓冲区的保障。

（12）缓存服务主要提供一定量的数据缓存，把常用的数据缓存到内存里面以实现加快系统执行速度和反应速度。

6. 数据中台服务主要提供各种类型的数据存储服务，主要包括传统的关系型数据库、非关系性数据库、表格存储、图形数据库、时序数据库等；为平台或应用提供各种类型的数据源分配，以加快系统的访问数据。

7. 支撑服务主要是支撑整个平台的外部的硬件资源和软件资源，如操作系统、数据库资源、分布式是服务资源，计算机资源等等。

8. 服务治理主要是整个平台针对各个服务的管理，主要提供一下主要内容：

（1）负载均衡主要通过一定算法来处理外部请求分布到多台相通服务主机的其中一台，以实现系统的高可用和集群扩容。

（2）服务注册主要是由一个独立的服务 Registrar 负责注册与注销。当服

务启动后以某种方式通知 Registrar，然后 Registrar 负责向注册中心发起注册工作。同时注册中心要维护与服务之间的心跳，当服务不可用时，向注册中心注销服务。

（3）服务发现主要有网关（API gateway）实现服务发现的功能，这样一套语言便可以轻松维护服务发现的功能。

（4）路由是根据请求地址，讲请求分配到对应的处理程序。

服务路由的分组应用场景包括以下几方面：

分组调用：为了保证服务的高可用性，实现异地多活的需求，一个服务往往不止部署在一个数据中心，而且出于节省成本等考虑，有些业务可能不仅在私有机房部署，还会采用公有云部署，甚至采用多家公有云部署。服务节点也会按照不同的数据中心分成不同的分组，这时对于服务消费者来说，选择哪一个分组调用，就必须有相应的路由规则。

灰度发布：在服务上线发布的过程中，一般需要先在一小部分规模的服务节点上线发布服务，然后验证功能是否正常。如果正常的话就继续扩大发布范围；如果不正常的话，就需要排查问题，解决问题后继续发布。这个过程就叫做灰度发布，也叫金丝雀部署。

流量切换：在业务线上运行过程中，经常会遇到一些不可抗力因素导致业务故障，比如某个机房的光缆被挖断，或者发生着火等事故导致整个机房的服务都不可用。这个时候就需要按照某个指令，能够把原来调用这个机房服务的流量切换到其他正常的机房。

读写分离：对于大多数互联网业务来说都是读多写少，所以在进行服务部署的时候，可以把读写分开部署，所有写接口可以部署在一起，而读接口部署在另外的节点上。

（5）熔断为了应付偶尔抖动的情况，以求更多地挽回损失。熔断包含几个方面：

限流：当服务提供者个多个消防者提供服务时，其中一个消防者流量飙升占用服务提供者大部分机器时间导致其他可能更重要的服务消防者不能被正常服务，所以服务提供者根据消防者的重要程度，以及 QPS 大小，给每个服务消费者设置一个流量上限，同一时间内只会给一个消防者提供一定数量的并发请求，超

过限制则等待或者直接拒绝。

资源隔离：服务消费者也需要对调用服务的提供者的线程资源进行隔离。

服务降级：代码或人工根据实际情况进行突发情况的切换。

9．运维监控主要是提供平台日常的管理，包括服务的监控、容器监控、主机监控、统计分析、告警。

10．日志记录主要提供平台或应用的各种日志信息。

11．权限控制主要是控制这个平台的权限，权限包括资源权限、功能权限、业务权限等。

8.3. 应用系统性能需求分析

1．应用性能需求

应用系统的性能应满足业务处理流程的要求，稳定、可靠、实用，人机界面友好，输入输出便捷，查询功能简单明了。

（1)提供丰富的功能和业务组件，保证灵活扩展，相关组件相互调用简单易用。

（2）服务接口：系统采用 WebService 的形式提供数据服务，遵循 OGC 规范的 WMS/WFS 标准。

系统运维管理操作简便，平台监控时效性高，对低质量服务和恶意访问及时提示管理员，并能有效、方便地进行控制和管理。

2．系统响应需求

系统必须具备负载均衡能力，以保证多用户并发访问时的系统的可靠性和系统性能不受到严重影响，具体性能要求如下：

（1）系统应实现 7×24 小时的连续运行；

（2）在多人（1000 人以上）同时使用的情况下（并发数不少于 200），系统需运行流畅、稳定；网络和本地查询响应速度小于 5 秒，影像栅格数据刷新速度小于 5 秒；

（3）单次操作，资源搜索响应时间在 2 秒以内；基于图片引擎地图浏览平滑、不留白；

（4）数据库管理系统操作简便；数据库管理系统可移植性强，配置步骤少；

3．数据准确需求

数据的加载、存储、计算、统计和制表制图等功能必须准确。空间数据的存取准确、无信息遗失，在确保信息安全的情况下，空间数据的显示应体现正确的空间位置关系和拓扑关系。

4．系统容量需求

系统要求采用主流大中型数据库系统，对数据库记录数的增长没有限制，数据管理容量支持 PB 级容量，并且保证大容量数据库的可操作性。

5．查询速度需求

由于本项目涉及数据量大，格式不一，而且数量的增量非常迅速，对于关系数据库和非关系数据库的查询能力及算法是一个非常严峻的挑战。需设计出合理的数据库结构和查询算法，以保证查询的响应速度并不随记录数的增长而急速下降。

6．稳定性指标

系统应实现 7×24 小时的连续运行，平均年故障时间（MTBF）≤5 天，平均故障修复时间（MTTR）≤24 小时。

8.4. 消防大数据中心管理系统

8.4.1. 数据支撑平台

数据中心支撑平台主要包括：数据共享交换子系统、目录管理服务子系统、共享数据管理子系统、共享业务管理子系统、系统配置管理子系统、系统安全管理子系统和数据检索子系统。

8.4.1.1. 数据共享交换

数据共享交换为全省各级消防救援部门和其他各级政府单位提供数据交换服务。

主要功能包括：

1．交换管理

提供交换节点、交换服务和交换桥接的配置、调度和检测功能；提供交换服务和交换桥接的日志查询和统计功能。

2．交换服务

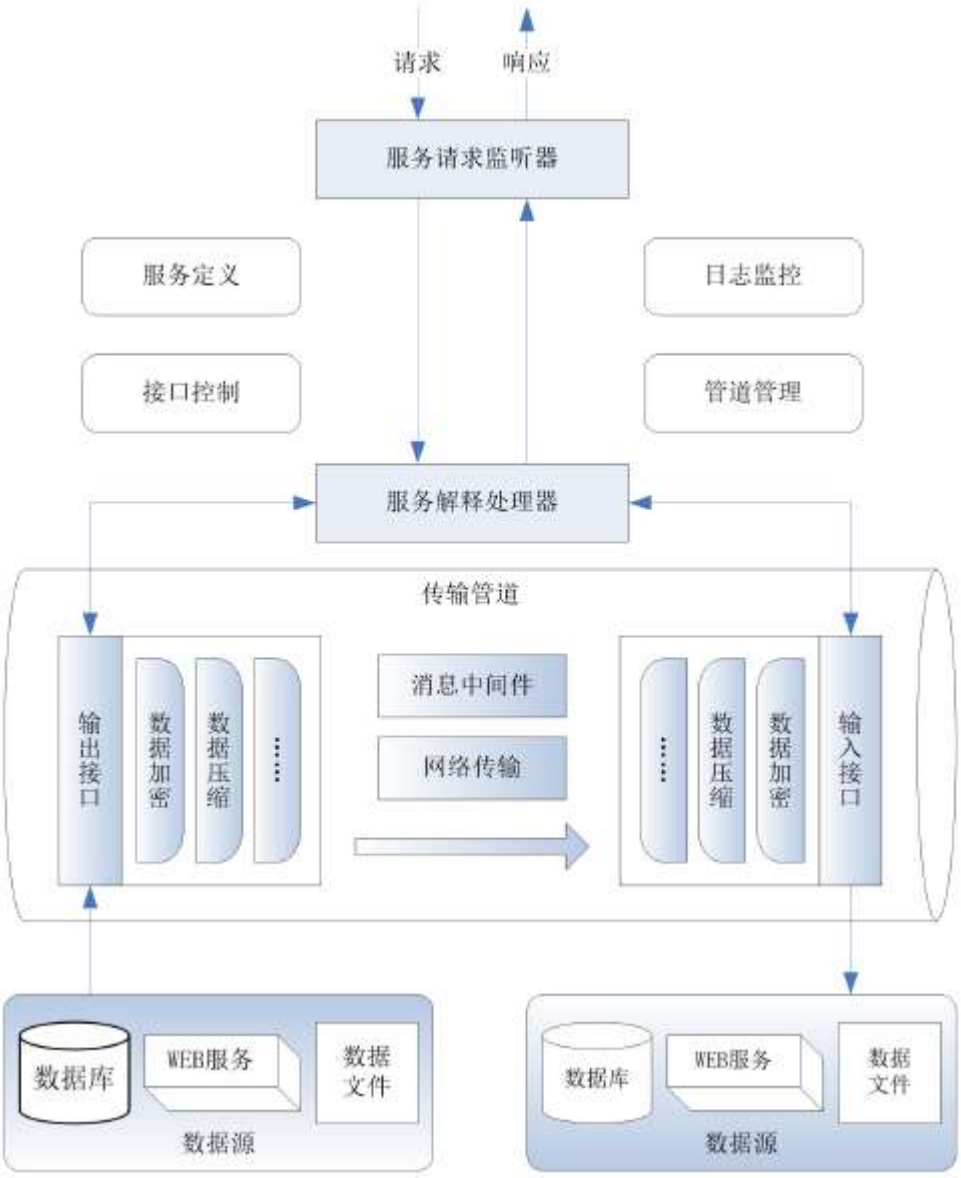
提供共享域内交换节点之间的数据共享交换服务，包括采集、分发、汇总和转

发；提供交换节点与业务系统之间的交换桥接服务，实现数据提供和获取；提供跨域交换服务，实现共享域之间通过对接节点进行数据交换。

数据交换引擎是数据共享交换平台的核心。数据交换引擎主要包括服务处理和数据接口。

（一）服务处理

数据交换引擎运行过程示意图如下：



数据交换引擎接负责收并处理数据交换服务请求，实现数据的交换。主要包括：

1．服务请求监听器

服务请求监听器采用监听机制，实现对服务请求的并发接收。

2．服务解释处理器

服务解释处理器负责解释执行服务请求。服务请求监听器把服务请求转发到解释处理器，服务解释处理器查询所请求的服务定义，根据服务定义产生执行序列并控制各个交换节点实现交换服务。在数据交换压力大的时候，根据服务的优先级高低，控制交换服务的执行顺序，确保高优先级的服务优先执行。

3．服务定义

服务定义记录了服务的项选参数以及设置，描述了服务应该如何解释和执行。交换服务可以定义服务优先级等信息。

4．接口控制

接口控制负责把命令序列发送到各个交换节点，控制交换节点上的数据接口，驱动数据交换的执行。

5．传输管道

数据的交换过程是在传输管道中进行的，传输过程分为三部分，数据输出，网络传输、数据输入。在源节点的数据输出接口把数据由数据源读出，并根据服务配置经过数据加密、数据压缩等过滤器。经数据输出接口输出的数据通过消息中间件传输到目标节点。目标节点的数据接口接收到数据后反向经过各种过滤器把数据还原出来，然后写入到目标数据源。

6．管道管理

管道管理器负责管理数据交换过程中的传输管理，包括管理的创建、动态分配、撤销等操作。

7．日志监控

日志监控按级别记录数据交换引擎在运行过程中的事件记录，提供监控功能。

（二）数据接口

数据共享交换平台支持三种数据接口方式：交换库方式、文件方式以及 Web 服务方式，业务系统通过交换平台进行数据共享交换时，可以根据实际的情况选择合适的数据接口方式接入交换平台。

在接入节点时，根据实际情况选用一种或多种接口类型。对于有业务系统存在，只要求提供或获取共享业务数据的情况，建议采用数据库类型接口；对于需要获取基础数据的情况，以及实时性要求高的情况，建议使用 Web 服务类型接口；文件类型接口根据实际情况决定是否采用。

8.4.1.2. 目录管理服务

目录管理服务功能是支撑平台的核心子系统，提供消防数据资源目录的注册管理以及数据资源的发现定位服务。

主要功能包括：

1．目录管理

提供数据主题的管理功能，数据主题包含了对数据资源的语义信息和规格信息等；提供对目录层次结构的管理，包括系统自动管理以及手工管理两种方式。

2．目录服务

按部门、专项以及分类标签等方式浏览数据资源目录；提供数据资源的检索和统计功能。

8.4.1.3. 共享数据管理

共享数据管理功能是支撑平台的一个基础子系统，是实现数据资源共享交换的基础。

主要功能包括：

1．数据标准管理

提供公共数据元、信息分类和代码的配置管理功能。

2．数据源管理

提供数据源的配置管理功能。

3．数据质量管理

提供对共享数据的质量管理功能，包括问题数据的查询、浏览和统计。

8.4.1.4. 共享业务管理

共享业务管理功能是支撑信息共享申请、授权业务开展的系统。

主要功能包括：

1．共享业务流程

提供对共享业务流程的支撑功能，包括共享业务申请和审核。

2．共享业务统计

提供按部门、业务状态和业务时间等维度对共享业务统计功能。

8.4.1.5. 系统配置管理

系统配置管理功能是支撑平台的一个基础子系统。

主要功能包括：

1．共享域

提供数据资源共享域的信息配置功能。

2．全局配置

提供组织机构、系统信息等全局配置功能。

8.4.1.6. 系统安全管理

系统安全管理功能是支撑平台的一个基础子系统。

主要功能包括：

1．用户管理

提供用户、用户组、角色管理功能。

2．权限管理

提供基于角色（RBAC）的权限管理功能。

3．操作日志

提供用户操作日志的查询和导出功能。

8.4.2. 数据采集基础功能

8.4.2.1. 自动数据采集系统

自动数据采集的主要功能需要从源系统中采集数据到数据资源中心的源系统数据文件落地区。常见的数据采集方法主要有以下几种：

1．通过专用数据同步工具将源系统生产数据实时同步到数据采集区。采用该模式的好处，主要是基于效率以及稳定性考虑，特别适合数据库层次的复制；另外一个好处是，几乎可以适用于任何类型的数据源，包括不同厂商的数据库、文件等。

2．通过存储设备本身的同步复制软件将源系统生产数据同步到数据采集区。该模式实际上和上述专用工具备份方式没有本质上的区别，只不过一个是数据库厂商或其他软件厂商开发的数据备份软件，一个是存储设备厂商（例如 EMC）自行开发的数据备份软件。从效率上来说，存储设备复制技术要优于其他数据备份软件，但同时有一个比较大的缺点，受制于操作系统和数据库系统对存储设备的识别方式；一般情况下，通过存储设备复制的数据库，并不能很快就能使用，需要重新加载数据库设备，重新启动数据库，极端情况下还需要重启操作系统，因此这种存储复制技术更多情况下也是用于灾备。

3．自行开发通用的数据下载平台，将源系统生产数据同步到数据采集区。这种模式常用于增量数据采集。通过该模式基本上能按需要来定制开发数据采集程序，灵活性大，效率也较高，同时还可以集成增量比对、乱码校验及修正、压缩打包、拆分并发处理、传输处理等功能，是一个务实的做法。但该模式也存在一个致命的问题，那就是如何确定增量数据的问题？如果通过数据库日志来获取，难度很大，而且也并不一定可行；如果通过数据库结构的某个字段来识别，这完全取决于源系统最初设计时是否考虑了增量备份的需求；不幸的是，大多数情况下，并没有考虑。于是，不得不采用先全量下载的方式，然后传送到数据采集区，再通过数据采集区来实现增量对比。在这种模式下，全量数据的传输无疑又是一个新的问题。

4．由源系统本身开发数据下载脚本，在本地生成数据，然后通过文件传输工具发送到数据采集区。这种模式常用于源系统数据采集，这主要是考虑其他源系统的数据采集量不大，而且各源系统架构多样化，不适宜采用通用的数据下载工具。这

种模式是一种主动采集模式。

上述四种数据采集模式，均各有特点，各有合适的应用场景。“智慧消防平台”的数据源也是多种多样，不宜采用统一的数据采集模式；应根据采集数据本身的特点，来规划数据采集模式。

本次设计是：若能识别增量数据，尽可能在第 3 种模式；对于数据量大的数据对象，可以考虑使用第 1 种或第 2 种方法，注意对操作系统和数据库软件的限制；在一些特殊日子，可能有些表的数据量会激增，应分析数据量激增的时间窗口，决定是否需要从加载流程上进行调整。

数据采集除了考虑上述采集技术外，还应该设计数据采集区的存储方式。由于“智慧消防平台”的数据是来自于各源系统，不改变源系统的数据表结构，因此无需另外设计独立的数据模型，仅需按一定的规则存储于非同源系统的基础数据即可。

- 自动采集设计

直观地提供对系统运行各方面状态的监控管理功能。

在源系统数据的时间窗口不一致的情况下，提供系统的运行策略，确保系统的正确运行和数据准确性。

提供数据抽取的错误及异常处理机制，增强系统的可靠性。

- 数据抽取策略

本次抽取所涉及外围元业务系统的范围及各系统所涉及的表的大致范围确定以后，就要根据每个系统的具体情况确定抽取策略。数据抽取策略包括数据源连接策略和数据加载策略。

数据源连接策略包括：文件传送方式，直连方式。

数据加载策略包括：增量（通常按照交易日期），全量。增量原则是根据业务系统数据产生或变化为标准，对于“智慧消防平台”而言，每日加载为了提高数据传输和转换的效率和计算性能，尽量选择增量加载。

■ 数据转换策略

自动抽取在把源数据加载到“智慧消防平台”临时数据区以后，对临时数据区的数据进行转换加载到信息数据库基础数据模型中，在该数据转换中需要根据数据的特点选择不同的数据转换策略。数据转换策略包括：

(A)全表覆盖（Delete All and Insert）

全表覆盖策略，是指对整个目标表在抽取加载时，删除目标表中原有数据，从源表中重新抽取、转换数据，并添加到目标表中，从而达到对目标表中数据全部更新的作用。目标表全部更新，适用于存在修改历史的数据并且不用保存历史的数据，同时也基于性能考虑。

(B)增量追加(Add)

增量追加策略，是指按照加载周期，仅仅将源表中加载时间点或加载时间段内的数据 insert 到目标表中。这种抽取加载策略适用于源表中的数据是按照日期的增长，不断增加记录（insert），并且这些增加的数据对原来的数据不发生作用(即没有 delete、update)的情况下，要对目标表进行加载转换的情况。

(C)增量比对（Update and Insert）

增量比对策略，是指按照加载周期，将源表中加载时间点或加载时间段内的数据 insert 到目标表中，因源表中部分并不是完全新增，会有部分数据发生变化，如此，就需要对加载时间点或时间段中的数据与已经加载的数据进行比对，以保证加载的数据是正确的。这种抽取加载策略适用于源表中的数据是不断变化而无法容易的得到增量的情况。这种策略情况下，我们通常将主键字段作为比对条件，但是某些情况下要根据业务含义及源系统数据提供方式来决定。

(D)历史拉链（History Chain）

适用于需要保存数据的连续历史轨迹，用开始时间和结束时间标志数据不同历史时段。历史拉链的算法在数据库实现步骤上通常由如下 2 种方式：

方式 1：

1) 获取当前的数据；

2) 比较当前数据和历史数据，找出新增加的和变化的数据，存放在临时表中，把起始日期置为该数据所对应的日期，结束日期置为最大日期；

3)针对变化的历史数据对结束日期进行更新置为最大日期；

4)从临时表向历史表中插入新增加的和变化的数据。

方式 2：

1) 找出前一日的数据和当前的数据；

2) 比较当前数据和前一日的数据，找出新增加的和更改后的数据；

3) 比较前一日的数据和当前的数据，找出被删除的和更改前的数据；

4) 从历史表中删除被删除的数据和更改前的数据；

5) 向历史表中插入新增加的和更改后的数据，把起始日期置为该数据所对应的日期，结束日期置为最大日期；

6) 向历史表中插入被删除的数据和更改前的数据，并把结束日期置为该数据所对应的日期。

方式 1 与方式 2 比较而言实现上更为简洁，但具体采取何种实现方式需要参考实际数据处理量和数据库性能状况，方式 2 在数据处理量大的情况下效率会较高。

■ 抽取作业调度

抽取任务间关系的最大特点，就是相互依赖性和高度并发性，而抽取作业调度的关键，就是解决好依赖性和并发性二者的统一。

在依赖性方面，作业调度模块要能够识别任务间的依赖关系，优先处理被依赖的任务，滞后并有选择地处理依赖任务。在并发性方面，作业调度模块在处理并发任务时，要顾及系统的资源和处理能力，过高的并发会使处理效率不升反降。

抽取作业调度功能主要由下述模块组成。

(A)流程管理

抽取过程是一个标准的流程作业，因而以流程图的方式来表示抽取过程是最为

直观方便的。流程管理模块通过直观图形化的交互方式，实现抽取流程的定制与维护。

流程管理模块支持对运行中的流程的修订，修订结果不会作用于当前运行中的流程，只有在下一次运行时才会生效。

(B)调度核心

调度核心负责抽取任务间的流转，包括控制任务的并发、检查逻辑依赖关系、实时动态调整系统负载和效率等功能。

调度核心可以同时执行任意多个任务流程，并在多个任务流程间进行协调，使系统资源和效率达到最佳化。调度核心会在必要时，将并行处理的任务自动转为串行处理方式，以防止过高的并发影响系统整体效率。

当抽取任务出现异常时，调度核心会自动设置任务流程的断点，当抽取作业被重新启动时，调度核心会跳过已经成功完成的任务，而从故障断点继续抽取作业的执行，以避免重复的时间开销。

调度核心支持任务流程的启动、停止或删除，能够实时提供各任务流程的当前状况信息。

(C)日志管理

整个的作业调度过程，都被记录在调度日志中，调度日志记录了每个任务、每组任务、每个批次和每个作业的执行时间，可用于对每天的数据处理流程差异进行对比分析，也可为任务流程的优化提供参考数据。

■ 抽取作业监控

抽取作业的监控功能如下。

(A)作业监控

抽取作业的触发有两种方式：自动触发与手动触发。自动触发是在到达指定的时间点时自动启动抽取作业，而手动触发是指由操作人员通过交互操作启动抽取作业。

在通常情况下，抽取作业被配置为自动触发方式，只有当特殊的场合无法确定准确的抽取作业启动时间时，才会采用手动触发方式。此外，当自动触发的抽取作业出现异常故障时，也可以用手动触发方式对抽取作业进行重启和修正。

操作管理人员可以通过监控界面实时监控抽取作业的日程和执行情况，并在必要时手工停止作业的运行。

(B)错误处理

每个抽取任务，都会在任务日志中记录各自的完成情况，包括处理的数据量、异常数据、错误原因等信息。通过查看错误日志，可以快速地定位错误位置，并根据错误原因方便地排查错误。

(C)质量报告

可以通过任务日志，生成数据质量报告，以有利于对源数据质量的改进。

■ 抽取数据质量检核

抽取处理原则：

1．质量检核是数据准确性的外部保证，应尽量提供检核处理；

2．检核处理不能对抽取处理有较大性能上的影响；

3．检核处理不能对时间窗口压力过大。

抽取处理方法：

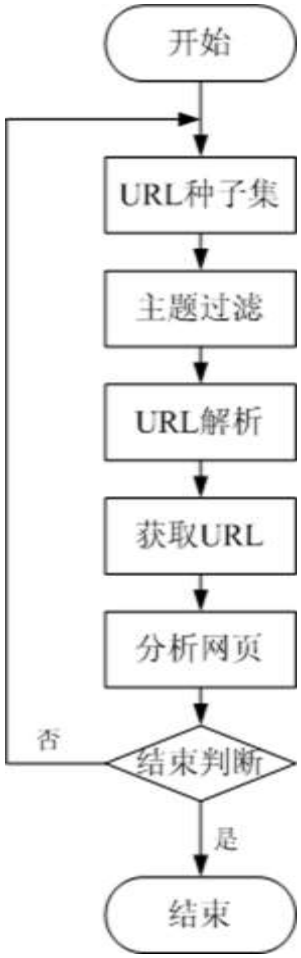
1．检核作业与该表的数据处理作业封装在同一个作业组中。

■ WEB 数据抽取

针对于对方数据库无法开放，无法提供接口的业务数据抽取情况，为了解决上述问题，采用 WEB 数据抽取方式，使用定向抓取相关厅局业务系统网页资源的方式完成数据抽取。WEB 数据抽取程序是一个自动下载网页的程序，它根据既定的抓取目

标，有选择的访问万维网上的网页与相关的链接，获取所需要的信息，将目标定为抓取与某一特定主题内容相关的网页，为面向主题的用户查询准备数据资源。

WEB 数据抽取方式实际上是一个自动提取网页的程序，它的工作流程较为复杂，需要根据一定的网页分析算法过滤与主题无关的链接，保留有用的链接并将其放入等待抓取的 URL 队列。然后根据一定的搜索策略从队列中选择下一步要抓取的网页 URL（或元素），并重复上述过程，直到达到系统的某一条件时停止，如下图所示。



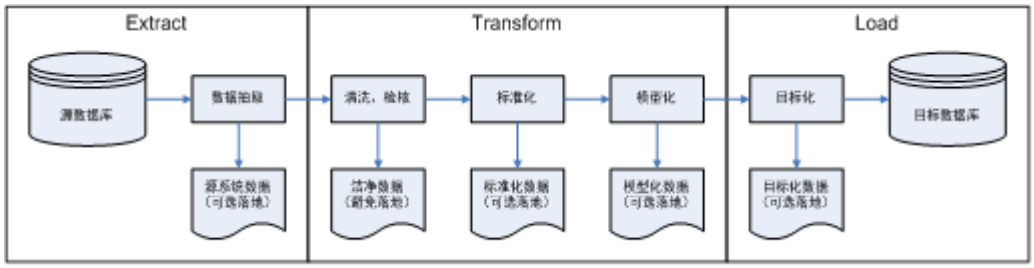
所有被抓取的网页将会被系统存贮，进行一定的分析、过滤，并建立索引，以便之后的查询和检索；这一过程所得到的分析结果还可能对以后的抓取过程给出反馈和指导。

WEB 数据抽取只抓取与某个主题相关的页面，抓取下来一个页面后并不抽取所有的文本内容，而是将主题相关的内容提取出来，一般格式化成有结构的数据，同时

抽取超链接时只选择与某个主题相关的，概括地说就是抽取的范围与内容是受控的。

■ 文件抽取处理

从系统效率的角度考虑，在抽取过程中的所有数据文件，都应该尽可能地避免落地。但是，要使应用成为一个成熟稳定的系统，又应该避免过于复杂的处理流程，应该将冗长的处理过程划分为若干的处理步骤，每个步骤产生各自的稳定结果。因而，抽取过程中数据文件的落地操作，就需要一个折中的解决方案。



在抽取过程的诸多步骤中，如果步骤间输出与输入的衔接是一对一的关系，就应该选择不落地方式，如果步骤间输出与输入的衔接是一对多或多对一的关系，就应该选择的方式。

■ 特殊字符处理

在抽取过程的数据加载阶段，有时候会出现数据无法正常加载的错误。出现这种错误的原因有多种可能，但常见的原因则是由于待加载的数据文件中出现了异常字符，导致加载程序无法按正常逻辑加载。这些字符可能是某个数据项的值中出现了分隔符或换行符，使得某条记录的栏位数与表结构不一致，或者是某个全角字符强制截取成了单字节导致后续的字符出现乱码，根本无法加载等。

在处理这些特殊字符时，一般会在数据抽取、数据清洗、数据转换、数据加载等过程中增加一些特殊处理，避免出现这些字符，或对这些字符进行转码。

在数据抽取的时候，必须确保数据平台环境的字符集与源数据环境的字符集一致，不至于出现字符集不一致导致无法识别。一般情况下，数据的抽取工作是由源数据系统本身完成，采用的是数据库的通用卸数工具。为了确保源数据的真实性，

不建议在数据抽取的时候对特殊字符进行处理，避免出现新的错误。

源数据文件准备好之后，抽取调度程序将启动数据清洗任务。在数据清洗任务过程中，除了对一些不满足业务规则的非法数据进行清洗之外，对这些异常字符的处理也是必须进行清洗，这里的清洗主要是指识别存在异常字符的记录，并做标记。这就需要有专门用于清洗特殊字符的程序。

在数据转换阶段，对那些已经标记出来的含有异常字符的记录按事先约定的规则进行转码处理，用可以识别并且有特定含义的字符串进行替换，确保这些记录能正常加载成功。

经历了前面的处理之后，并不能完全保证不会再出现有非法字符的记录。因此，在数据加载阶段，同样还是必须保留这种特殊字符处理机制。常见的一种方法是：在加载的过程中，若出现了无法加载的异常记录，加载程序会放弃这条记录，转存到一个异常记录日志文件；待全部正常记录加载完成之后，再调用特殊字符处理程序对这些记录进行清洗转换处理。若能自动完成，则系统自动再进行加载；若不能自动完成，则保留这些记录，通过人工方式进行加载。

特殊字符出现的频率也是评价数据质量好坏的一个重要指标。它与业务系统的数据采集处理机制和后台加工处理有直接关系，可以反映出该数据采集功能对应的程序质量。有意识地搜集特殊字符处理信息，可以提高程序开发质量，减少后续的错误出现频率。

- 数据采集日志

本次数据采集的过程中也需要大量日志去监控与管理数据采集过程中发生的事情，故本次项目规划数据采集日志主要功能点如下：

数据库抽取采集日志：针对数据库数据抽取的采集方式，通过采集日志来记录数据库数据采集过程中数据采集情况，是否出现采集异常等问题。

文件数据库采集日志：针对文件数据的采集方式，通过采集日志来记录文件数据采集过程中数据采集情况，是否出现采集异常等问题，采集是否成功，文件数据是否重名等问题。

WEB 抓取采集日志：针对 WEB 抓取数据的采集方式，通过采集日志来记录 WEB 数据采集过程中数据采集情况，是否出现采集异常等问题，采集是否成功，采集页面是否有异常等问题。

8.4.2.2.手动数据采集系统

数据录入是为了弥补数据源缺失或者业务系统建设不完善的情况而设置特殊采集模式。在本方案中数据录入功能采用信息平台的数据录入模块来实现。

数据录入模块的提供是针对不同业务数据库的通用数据录入工具，包括页面录入和模板录入以及数据入库的审批流程。支持对录入数据的事件处理（如新增前进行有效性数据检查、新增后进行数据平衡校验等，使用检核规则来实现）。数据录入工具可服务于各部门、各机构的数据录入人员。

- 检核规则管理

检核规则有两种类型：存储过程、正则表达式，是用于对录入数据进行合法性检核而定义的规则。存储过程类型的检核规则必须要有输入参数和输出字段，其中输入参数得到需要检核的数据的值，输出参数返回检核结果的标志位。

管理员建立录入任务的时候，可以在检核规则设置界面设置录入的数据所对应的检核规则，可以设置数据入库前、入库后、修改前、修改后等各种检核规则。

- 录入任务管理

录入任务是对一项录入工作的总体安排，包括录入的目标表、操作控制信息、使用的检核规则、批量录入模板的管理和权限控制等一系列内容。

- 数据录入界面

录入任务定义好之后，用户可以在录入界面进行具体数据的录入。

用户也可以下载批量录入模板，按模板样式填好数据之后，可以将批量录入文件上传至服务器并导入文件中的数据。

■ 录入任务审批

用于对用户录入的临时表数据进行审核及入库操作。

用户录入的数据存放在临时表中，需要对临时表数据审核之后，才可以正式入库。

■ 数据导入模块

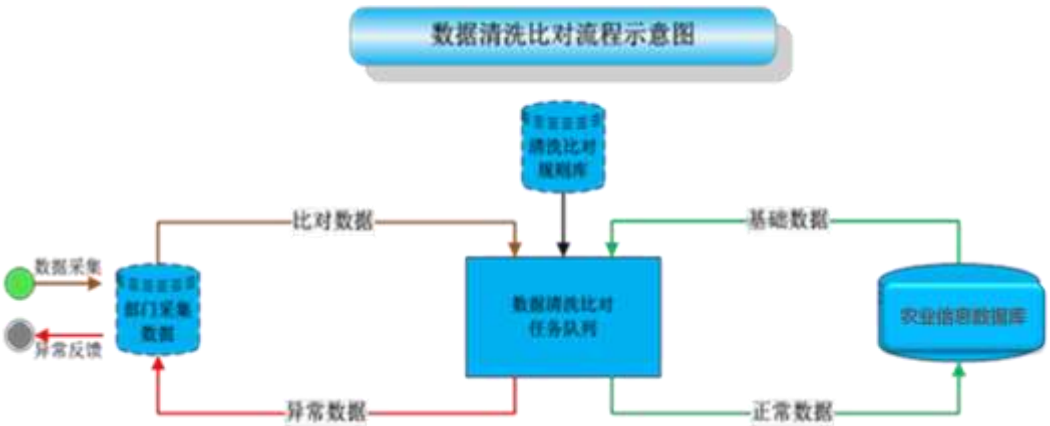
将经过分析的数据导入到系统数据库，实现从网页到数据库的入库转化，包含以下数据的录入。

8.4.2.3. 数据清洗比对系统

数据清洗及比对功能需要数据库和应用程序结合处理，数据清洗比对系统对部门交换的数据进行清洗、比对、整理，过滤出异常数据并反馈给提供部门，并形成消防信息共享数据库。

数据清洗及比对功能需要数据库和应用程序结合处理，由于数据清洗和比对过程中涉及数据批量数据操作，为了提高数据清洗及比对效率，方案设计将数据清洗及比对时的数据处理工作放在数据库中进行，以存储过程和数据库作业来完成。

数据清洗比对业务主要环节有比对规则建立、比对任务建立、数据清洗、数据比对、整合入库、异常反馈等几个环节。比对流程如下图数据清洗比对流程示意图：



数据清洗比对系统主要分为数据清洗、数据比对、数据反馈、清洗比对监控等功能构成。

■ 数据清洗

数据清洗流程：数据质量分析→形成分析报告→确定清洗解决方案→数据清洗系统开发。

1．模型设定

设定清洗的模型，根据清洗解决方案对照设定，为数据清洗提供规则和识别方法。

2．数据清洗

根据清洗任务中设定的各参数，以及模型设定中设定的清洗模型，进行清洗。

3．定时任务

定时实现清洗系统中的各个清洗任务的执行；

4．参数配置

动态配置清洗相关的参数，这些参数包括：参与清洗的部门、参与清洗的字段项、参与清洗的字段质量类型、定时任务增删改及参数配置。

■ 数据比对

数据比对整合的入库流程：

数据进入临时中心库→数据比对→（合格）数据入库→（不合格）数据返回修订→数据比对→（合格）数据入库。

1．规则管理

针对不同数据表定制不同的比对规则，包括规则建立、查询、引用、修改、删除等功能。

2．数据比对

根据比对任务中设定的各参数，调用数据库相关程序、作业，进行比对。

3．定时任务

定时实现比对系统中的各个比对任务的执行，包括任务查询、查看、启动、停止等功能

4．参数配置

动态配置比对相关的参数，这些参数包括：参与比对的部门、参与比对的字段项、定时任务增删改及参数配置。

■ 数据反馈

数据反馈系统是定时将基础信息库中的数据比对过程中的不合格数据和数据清洗的低质量数据，经由系统标识后反馈给原始数据来源部门。

1．异常数据反馈

根据配置的参数，将标识为比对不通过的和数据清洗低质量的数据，经整理后，返回到对应的原始数据来源部门或系统。

2．定时反馈任务

定时实现反馈系统中的各个反馈任务的执行；包括任务的创建，周期的设置，任务的查询、启动、停止等。

3．参数配置

动态配置反馈相关的参数，这些参数包括：本次反馈数据的部门、本次反馈数据的数据项、定时任务增、删、改及参数配置

■ 清洗比对监控

清洗比对监控是对数据交换过程中产生的各类运行过程的监控日志，并以图形化方式反映清洗比对监控的运行状态。

8.4.2.4. ETL 数据抽取工具

系统实现从各消防物联网感知网分中心中抽取前一日产生的新数据，抽取后在某个指定的目录下生成数据库文件，系统通过文件读取功能自动将该数据库文件拷贝到位于智慧消防云平台的服务器的某个指定目录下，该工具自动实现将这些新拷入的数据库文件导入到数据库中，从而实现数据库的同步。

系统管理员再利用数据抽取工具将各消防物联网感知网分中心数据库中前一日获取的外部单位数据导出，并导入智慧消防平台的基础数据库中。

系统分为配置工具和执行工具两个组成部分。

配置工具主要用于配置各种抽取方案，包括数据源配置、映射方案定义、任务调度等。

执行工具用于执行各种抽取方案，包括任务执行引擎、任务执行监控、方案调用接口等功能。

已建消防物联网系统与新系统之间属于异构平台。因此，要实现新旧系统的融合，就需要通过数据采集接口开发技术与 ETL 数据交换技术来实现。

8.4.2.4.1. 数据抽取

数据抽取是从数据源中抽取数据的过程。实际应用中，数据源较多采用的是关系数据库。从数据库中抽取数据一般有以下几种方式。

1．全量抽取

全量抽取类似于数据迁移或数据复制，它将数据源中的表或视图的数据原封不动的从数据库中抽取出来，并转换成自己的 ETL 工具可以识别的格式。全量抽取较为简单。

2．增量抽取

增量抽取只抽取自上次抽取以来数据库中要抽取的表中新增或修改的数据。在 ETL 使用过程中。增量抽取较全量抽取应用更广。如何捕获变化的数据是增量抽取的

关键。对捕获方法一般有两点要求：准确性，能够将业务系统中的变化数据按一定的频率准确地捕获到；性能，不能对业务系统造成太大的压力，影响现有业务。

8.4.2.4.2. 数据转换和加工

从数据源中抽取的数据不一定完全满足目的库的要求，例如数据格式的不一致、数据输入错误、数据不完整等等，因此有必要对抽取出的数据进行数据转换和加工。

数据的转换和加工可以在 ETL 引擎中进行，也可以在数据抽取过程中利用关系数据库的特性同时进行。

(1)ETL 引擎中的数据转换和加工

ETL 引擎中一般以组件化的方式实现数据转换。常用的数据转换组件有字段映射、数据过滤、数据清洗、数据替换、数据计算、数据验证、数据加解密、数据合并、数据拆分等。这些组件如同一条流水线上的一道道工序，它们是可插拔的，且可以任意组装，各组件之间通过数据总线共享数据。

有些 ETL 工具还提供了脚本支持，使得用户可以以一种编程的方式定制数据的转换和加工行为。

(2)在数据库中进行数据加工

关系数据库本身已经提供了强大的 SQL、函数来支持数据的加工，如在 SQL 查询语句中添加 where 条件进行过滤，查询中重命名字段名与目的表进行映射，substr 函数，case 条件判断等等。

相比在 ETL 引擎中进行数据转换和加工，直接在 SQL 语句中进行转换和加工更加简单清晰，性能更高。对于 SQL 语句无法处理的可以交由 ETL 引擎处理。

8.4.2.4.3. 数据装载

将转换和加工后的数据装载到目的库中通常是 ETL 过程的最后步骤。装载数据的最佳方法取决于所执行操作的类型以及需要装入多少数据。当目的库是关系数据库时，一般来说有两种装载方式：

(1)直接 SQL 语句进行 insert、update、delete 操作。

(2)采用批量装载方法，如 bcp、bulk、关系数据库特有的批量装载工具或 api。

大多数情况下会使用第一种方法，因为它们进行了日志记录并且是可恢复的。但是，批量装载操作易于使用，并且在装入大量数据时效率较高。使用哪种数据装载方法取决于业务系统的需要。

8.4.2.4.4. 智能统计与查询

系统引入智能统计与查询功能，用于满足用户对数据中心数据的统计与查询的需求，主要包含功能如下：

- 智能统计

可对相应的输入条件提供相应的数据做统计，并可按饼状图、柱状图等图形展示，主要包含以下三个方式：

1、时间维度统计

通过用户输入的时间区间，统计在这个时间区间内的相应数据，如在 XX 月到 XX 月，有多少笔的农经资讯的信息产生等。

2、区域维度统计

通过用户输入的地区的区间，统计在这个地区区域内的相应数据，如在 XX 区域内，有多少份消防监测数据产生等。

3、消防因素统计

通过用户输入的相关的消防因素，统计出与这个消防因素的相应数据，如输入“XX 火灾风险隐患”，可查询并统计出有关“XX 火灾风险隐患”的相关信息与内容。

- 数据查询

1. 消防监管行业专业数据查询

2. 消防服务行业查询

3．消防物联网专业数据（设备、监测数据）查询

4．消防教育、政策宣传数据

5．消防专题数据查询

6．统计分析数据或智能研判数据查询

8.4.3. 数据共享交换平台

8.4.3.1. 交换网络结构

一般数据交换有两种常见的交换结构：星型交换和网状交换。在星型交换结构中，所有端节点都只与中心节点相关，通过中心实现数据交换；而网状交换结构中，数据可以在任意两个节点之间直接交换。

经过调研和分析，全省各级消防救援部门之间以及消防与各级政府部门之间存在着复杂的数据共享和交换需求，并存在以下特点：

1．同一批共享数据通常需要共享给多个子系统；

2．对同一批数据，不同的子系统应用的需求存在差异；

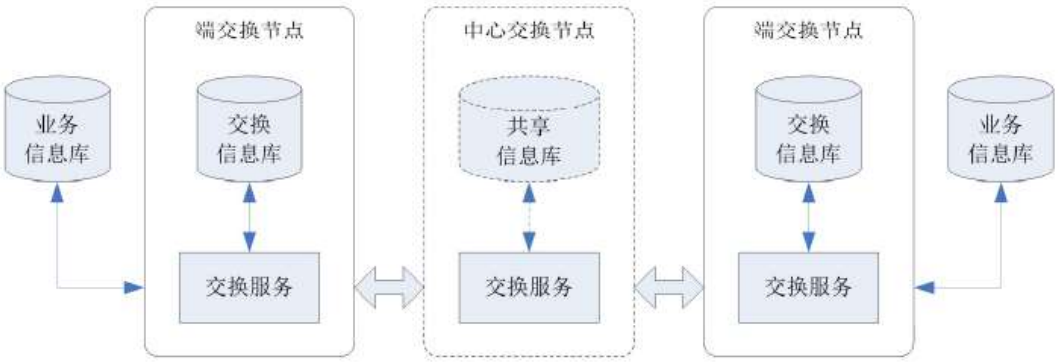
3．各个子系统独自开发，技术平台不一，数据标准不一；

4．数据共享和交换要求进行备案。

8.4.3.2. 交换概念模型

交换概念模型由中心交换结点和端交换结点组成。端交换结点接收和发送政务部门的交换信息。中心交换结点管理交换网络内端交换结点的数据交换服务，并根据需求形成共享信息库。

交换的概念模型如下图所示：



交换概念模型说明如下：

（一）业务信息是由各消防部门产生和管理的消防数据资源；

（二）交换信息是端交换结点用于存付参与交换的消防数据资源；

（三）共享信息库是可以为多个端交换结点提供一致的消防数据资源的信息集中存储区。任意一个端交换结点是可以按照一定的规则访问共享信息库。

（四）端交换结点是消防数据资源交换的起点或终点，完成业务信息与交换信息之间的转换操作，并通过交换服务实现消防数据资源的传送和处理；

（五）中心结点主要为交换信息提供点至点、点到多点的信息路由、信息可靠传送等功能。在两个端交换结点之间可以有 0 个或若干个中心交换结点；

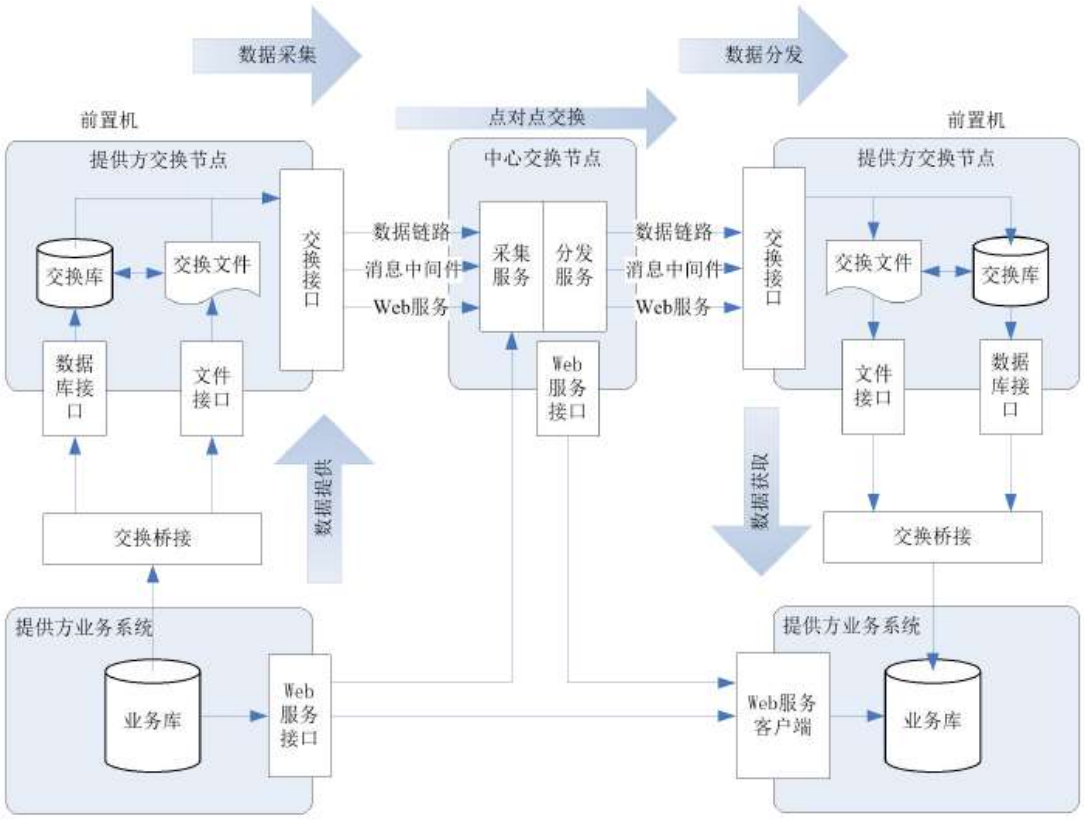
（六）交换服务是交换结点传送和处理消防数据资源的操作集合，通过不同交换服务的组合支持不同的服务模式。交换服务按照数据交换任务的重要性以及时效性要求设置为不同的优先级。一般情况下，交换服务按照预先设定的调度计划执行。在服务器、网络资源紧缺的情况下，高优先级的交换服务可以优先执行，确保满足数据交换的时间要求。

8.4.3.3. 交换体系结构

消防大数据共享交换平台由中心交换节点和端交换节点组成，依托统一的电子政务网，通过采用一致的交换协议，实现跨地区、跨部门应用系统之间的数据交换。

全省消防大数据中心作为中心交换节点，各消防职能部门的前置机作为端交换节点。部门业务系统通过交换桥接实现与前置机互联，接入数据共享交换平台。

数据中心的交换体系架构如下：



业务库是由各政务部门产生和管理的政务数据资源库。交换库是政务部门提供本部门交换数据、获取其他部门交换数据的存储库。交换文件作用与交换库相同，把政务部门提供本部门交换数据、获取其他部门交换数据以文件形式存放在前置机上。

中心交换节点提供交换数据的采集、分发服务，实现交换节点之间的数据路由和传送功能。端交换节点提供交换数据的存储库、数据写入和读取接口以及文件上传和下载接口，业务系统与端交换节点之间通过交换桥接进行交换数据的提供和获取，并实现业务数据和交换数据之间的转换。

端交换节点是交换平台中数据交换的起点或终点。数据交换过程可分为数据提供、数据采集、数据分发和数据获取四个阶段：

（一）数据提供：数据从提供方的业务系统转换并传输到提供方的前置机；

（二）数据采集：数据从提供方的前置机传输到中心节点；

（三）数据分发：数据从中心节点传输到使用方的前置机；

（四）数据获取：数据从使用方的前置机传输并转换到使用方的业务系统。

其中，数据提供和数据获取流程由消防职能部门的交换桥接负责。数据采集和数据分发流程由中心数据共享交换平台负责。

业务系统可以通过公开 Web 服务的方式向数据中心或其他消防部门提供数据。职能部门获取数据时，也可以直接从数据提供方公开的 Web 服务获取数据。

数据中心公开的 Web 服务主要用于共享基础数据，业务系统可以调用数据中心的数据共享服务查询基础数据。

8.4.4. 共享数据管理系统

在没有数据标准的时候，数据中心对同一个数据字段可以从多个数据来源采集数据。对于同一个数据字段，数据中心对于该数据字段保存多个来源的版本。

公共数据维护系统提供工具、服务来展现数据的不一致性，数据管理员根据工作制度，对数据字段进行电话等多种手段核实字段的真实数值，如果在一定的时限内不能解决冲突，则可以发布该数据字段的多个版本，每个版本都标明数据字段的来源，并指示该数据是存在冲突的。

通过数据共享与交换平台以数据服务的方式从各业务部门采集数据，保存到公共数据缓存库，使用公共数据维护系统进行数据比对、冲突检查、数据审核、数据转换。当数据达到一致性、完整性要求时，数据被发布到公共数据发布库，通过数据共享与交换平台以数据服务的形式提供数据使用方访问。

数据管理系统面向数据中心和业务部门的数据管理员，确保数据的一致性、准确性和完整性，为数据质量把关。

8.4.4.1. 功能设计

- 数据管理工作流

实现对数据管理的主要工作流程的管理，方便业务部门提供、使用和交换数据。比如从数据使用方提出申请，然后数据提供方进行审核，然后双方协商数据交换规则到最后配置实现的整个工作过程的管理。

- 数据转换

建立业务部门数据于标准规范数据的转换映射关系和转换规则，将业务部门的数据转换为符合标准规范的数据。

- 数据整理

对缓存数据库中的各业务部门数据进行比对、清洗，检查数据冲突，对数据进行审核校验。确保数据一致性、完整性。

- 数据发布

数据管理系统把经过比对、审核、转换之后的具有完整性、一致性的数据保存到数据中心的发布数据库，经过数据共享与交换平台发布提供各业务部门使用。

- 主题管理

数据中心以主题为单位实现数据采集、数据交换、数据共享、数据比对以及数据发布。因此必须提供主题管理功能。

- 元数据管理

对共享数据进行元数据管理，以主题的方式组织数据资源。

- 数据标准管理

对数据标准的内容、数据标准的版本进行管理，将标准变更对业务系统的影响屏蔽在数据接口系统一级。

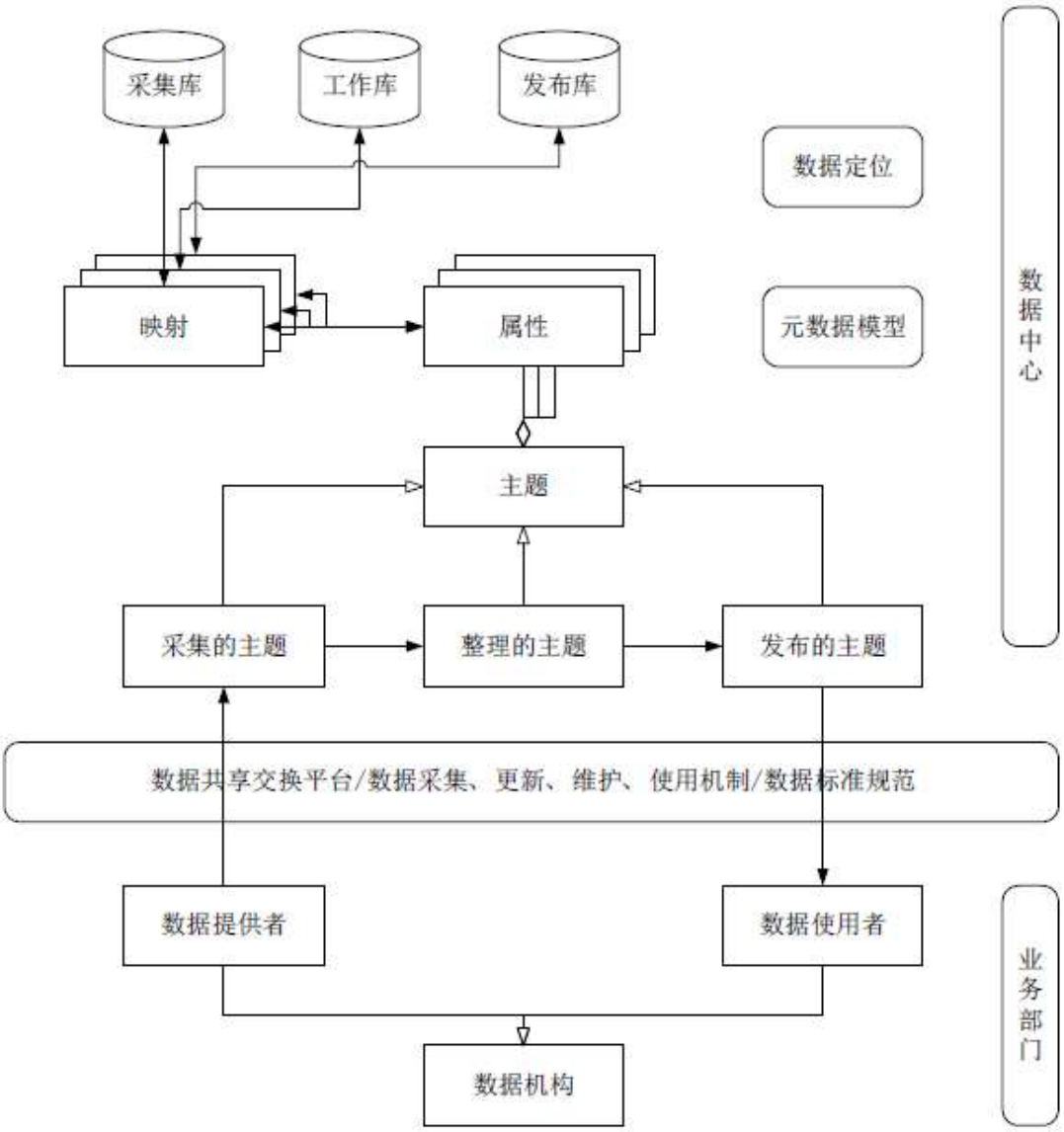
- 数据维护

通过数据管理系统进行日常的数据维护工作，如：数据备份恢复。提供对业务系统的异地容灾数据备份的管理支持。

8.4.4.2. 逻辑结构

数据管理系统以主题的方式组织数据资源，提供元数据管理、数据供需关系管理、数据标准规范管理，与数据共享与交换平台结合，提供数据转换、整理、发布

等功能。



8.5. 应用功能设计

8.5.1. 物联网感知网络中心管理系统

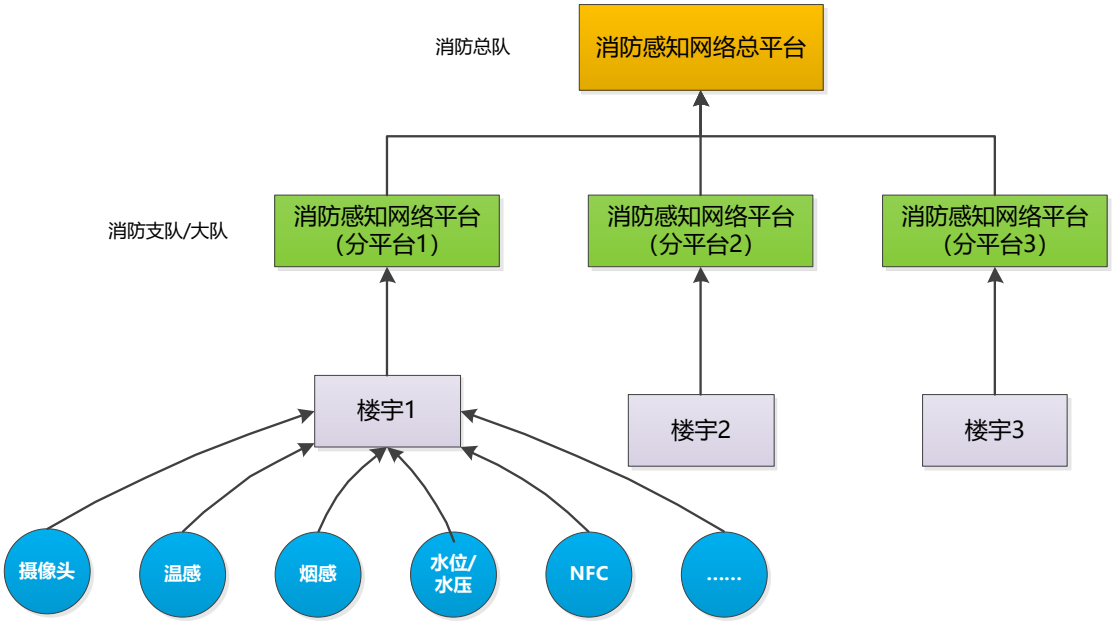
8.5.1.1. 感知网分中心建设模式

在物联网感知网络中心服务器接入物联网前端感知设备，如：火灾探测器、声光警报器、电磁阀、高位水箱、低位水池液位、水压传感器等设备，包含火灾报警监控子系统、建筑消防水监控子系统、消防电源监控子系统、消控室视频监控子系

统、消防电源监控子系统、消防巡查管理子系统等系统中感知数据。

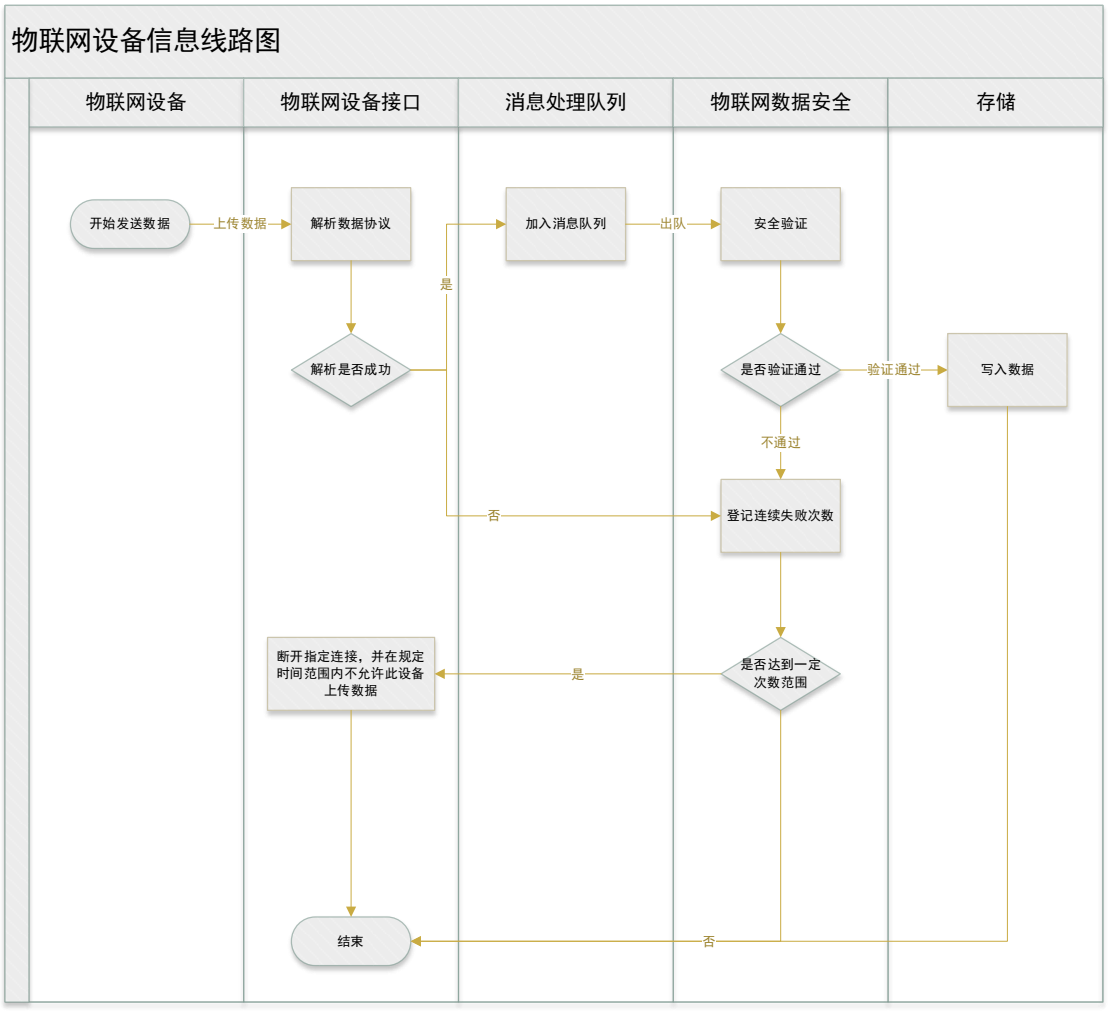
由此可见，消防物联网系统感知网络体系的基础，就是终端的各种环境要素检测感知设备设施，这些终端感知设备又分散于各个重点消防场所中。如何将这些分散的消防场所感知设备进行分类整合，形成完整的“消防感知网络”，这就需要引入“社会网格化”的概念，也就是对消防终端感知设备进行分类、分组、分区域、分监管部门等，实现对终端消防感知设备的层级和精细化管理。

网格化消防感知平台结构如下图：



通过对消防感知网络进行网格化划分，各级政府主管部门、消防监管部门、业主单位、社会公众等，都可通过网格化形式查找对应分类、行政区域、辖区范围内的感知网络分平台对消防设备设施及当前消防安全状态状况进行实时监管。

8.5.1.2. 物联感知安全与研判设计



物联网设备信息流转图

具体说明如下：

1．物联网设备通过探测器把探测的信息内容发送到平台。

2．平台的物联网对接接口通过物联网设备上传的数据的特性找到对应的数据解析协议，通过数据解析协议完成才把解析的数据推送给消息队列去做后续处理。如果解析不成功抛出并记录解析不成功的通道的次数。如果解析不成功达到一定次数的话，可以采取一定策略，使当前的设备连接在一定时间范围内（例如：20 分钟）不允许此对应的 ip 或 mac 地址的设备进行连接。

3．数据入消息队列后，后端的处理程序接收队列信息进行下一步处理。

4．物联网数据安全校验通过一定策略，例如：发送的数据的两次时间间隔、上一次发送数据的路由表信息对比和同一个设备的 IMEI 号对应同时有多个 socket 连

接等分析策略来判定和校验数据的合法性。如是合法数据就直接到下一步，倘若判断数据非法，结束并登记非法数据的通道的连续次数，达到一定次数样系统将自动清洗非法连接并针对 ip 或 mac 地址进行一定时间范围内不允许次对应的 ip 或 mac 地址进行连接。

5．数据通过校验就可以进入数据的存储和后续处理。

8.5.1.3. 感知网络中心基础管理功能

1．设备注册登记。每个火灾风险单位的物联网感知设备要接入到本辖区的感知网络分中心，需要到省平台的感知网络分中心设备接入登记功能中进行注册登记备案，注册信息包括：设备名称、设备编号、设备安装位置、设备用途、设备归属火灾风险单位、厂商信息、出厂日期等。另外注册登记过程中，需要选择设备 NB-IOT 通信协议，便于云平台与设备之间进行数据通信对接。

2．设备解除登记。当物联感知设备损坏无法修复或设备移除时，需要在系统中进行解除登记，避免由于状态变更不及时而导致系统出现火情误报或设备故障误报。

3．设备日常维护管理。包括设备信息的日常抽检、排查、汇总等。

4．设备状态监测。主要针对设备的运行状态、通断状态、故障提示状态等信息进行实时监测，并可形成状态监测报表。

5．设备查询统计。提供多条件要素查询功能，提供汇总统计，以及图表展示。

6．设备运行日志。记录系统日常的运行日志和故障日志。

8.5.1.4. 感知分中心预分析处理功能（边缘计算）

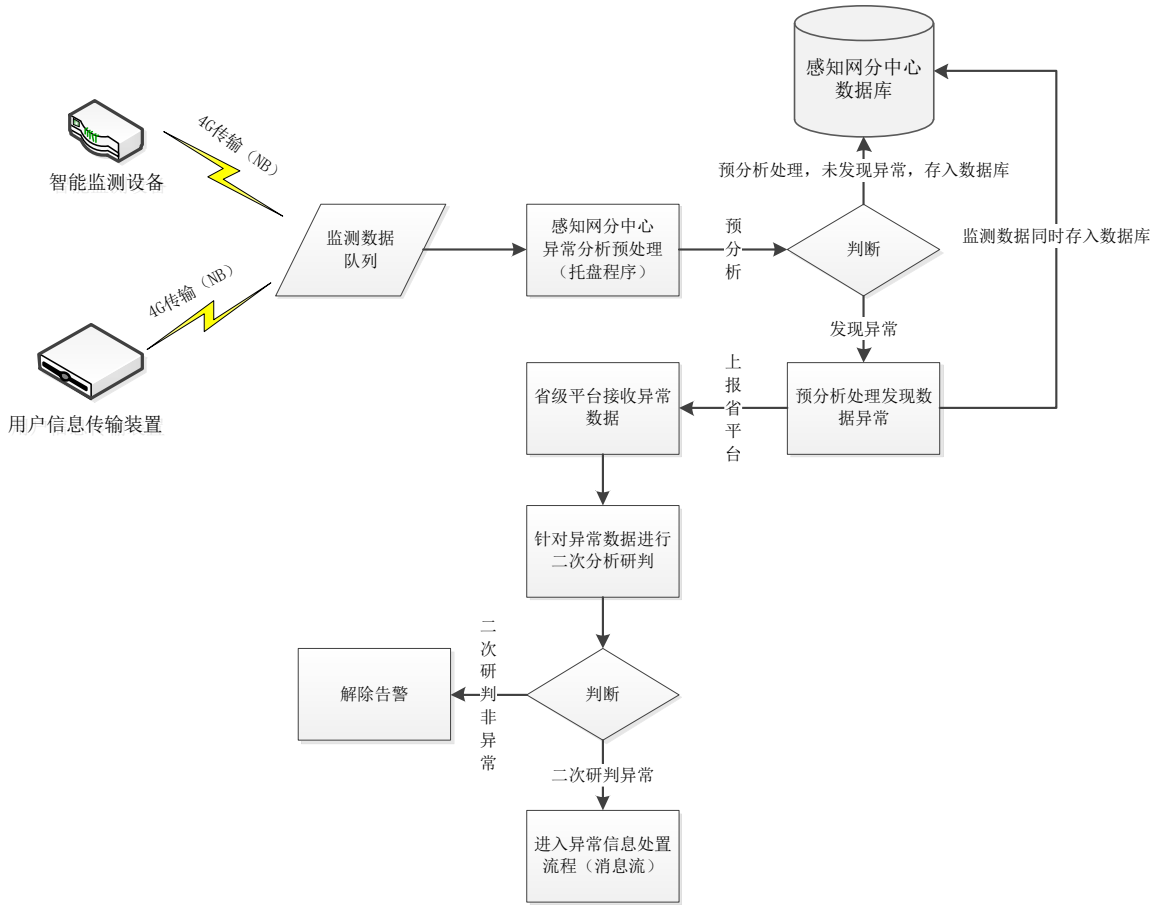
感知网分中心建设完成后，需要预装由省级智慧消防平台下发的前置处理软件，可以以“托盘”小程序的方式进行部署，分中心数据采集存储服务器开机即启动托盘小程序服务。

该方式利用感知网分中心具有的算力资源，实现云平台下各分中心对本地资源的“边缘计算”，将计算结果反馈给云端，从而降低云端对原始数据资源的初始计算压力。

托盘小程序具备消防物联网监测数据的前端预分析处理功能，通过运算规则对监测设备发送的最新监测数据进行异常（火灾、隐患、故障）分析。如果监测数据

预处理发现数据异常，则上报至省平台进行二次分析研判和进入处置流程；如果监测数据预处理分析后，未发现异常的，直接存储至分中心数据库中。

具体的预处理流程如下：



8.5.1.5. 感知网分中心数据共享服务功能（边缘计算）

感知网分中心数据共享服务功能，也是由省平台下发前置软件，也是以托盘小程序的形式，在分中心服务器进行预装，分中心服务器开机即启动。

数据共享服务托盘程序软件安装完成后，可在托盘程序中配置数据源、定义数据格式、配置服务参数、配置指令接收参数（省平台可直接下发指令，直接获取指定数据）。

8.5.2. 消防物联网远程监控系统

针对消防管理中常见的管理需求，结合物联网、大数据等新技术发展，解决传统管理方式的弊端，向科技要效率，实现消防管理工作智能化、可视化、痕迹化。

实现传统消防系统联网监控，并将消防电源监控系统、消防水监控系统、消火栓可视化管理、视频监控、设备设施巡查管理、小微场所火灾预警等通过物联网的方式，将消防基础数据信息化，统一汇聚至系统，将“人防、物防、技防”三结合应用于传统的消防管理和监督。实现对消防核心系统关键信息的感测、分析、整合，从而对消防监督业务活动的各种需求做出智能响应。打破各消防监督业务系统之间的信息壁垒，使消防信息资源更供需对接，推动消防工作模式从传统向现代、被动向主动、单一向综合、人工向智能的发展。

8.5.2.1. 消防基础资源数据采集

系统通过打通各类数据采集平台，避免“信息孤岛”，逐步完善消防资源数据库，为各级响应力量能够及时掌握进行火灾防控提供决策辅助支撑。

主要为建筑物（群）年龄、耐火等级、电气线路、区域内单位火灾隐患危险等级、公共消防设施运行情况、整体建筑火灾负荷等，及外围道路信息、水源信息、消火栓信息、出入口信息、消防通道信息、重点部位信息、消防设备信息等环境数据，结合区域范围内的典型火灾情况、历史重大火灾情况、人员密集场所分布、危化品分布、整体情况、区域群众消防意识情况、天气状况、区域内灭火救援力量等级等相关信息，将影响起火的因素和扩大蔓延趋势的因素建立基础汇总库，并整合地理信息系统统一展现。同时，社区消防站、消防车辆、装备、消防人员等信息均可通过平台进行信息录入、维护。

系统将构建统一消防资源数据库，并通过落地实施后逐渐扩展数据项，完善数据内容。数据来源主要包括消防内部数据、市政面数据、社会面数据三大类，采集方式包括物联网自动采集、街道级平台调用、消防相关人员上报、互联网数据抽取等。

8.5.2.1.1. 建筑物

建筑数据，支持全省各个城市建筑（楼栋）信息采集，建立建筑物台账，并且能对应建筑物经纬度在地图上直观展示。建筑物信息的要素包括建筑物名称、建筑物类别、建造日期、使用性质、火灾危险性、耐火等级、结构类型、毗邻建筑物情况、建筑立面图、消防设施平面布置图、建筑平面图、建筑物所属单位名称、建筑

高度、建筑面积、占地面积、标准层面积、地上层数、地上层面积、地下层数、地下层面积、隧道高度、隧道长度、消防控制室位置、避难层数量、避难层总面积、避难层位置、安全出口数量、安全出口位置、安全出口形式、消防电梯数量、消防电梯容纳总重量、日常工作时间人数、最大容纳人数、储存物名称、储存物数量、储存物性质、储存物形态、储存容积、主要原料、主要产品、建筑在地图经度、建筑在地图纬度等。系统支持根据联网火灾风险单位信息表收集内容导入平台建筑信息、建筑图纸等信息。对建筑消防档案的电子化管理。建筑物信息可以跟联网火灾风险单位信息进行关联管理，并在 GIS 地图上进行标注显示，直观的显示各建筑物的信息状态。

8.5.2.1.2. 联网火灾风险单位

支持入驻的联网火灾风险单位数据采集，以楼栋单位，主要包含一般企事业单位、消防火灾风险单位、物业小区、出租房屋等企业单位信息，建立信息台账，摸清底数。

8.5.2.1.3. 消防设施及部件

消防设施及部件管理主要实现火灾自动报警系统、消防水源、室外消火栓、室内消火栓系统、自动喷水灭火系统、水喷雾灭火系统、气体灭火系统、泡沫灭火系统、干粉灭火系统、防排烟系统、防火门及卷帘、消防应急广播、应急照明及疏散指示标志、消防电源、灭火器的信息管理功能。

消防设施部件信息要素包括部件名称、部件编码、部件类型、部件位置信息、部件区号、部件回路号、部件位号、生产公司、生产日期、报废日期、部件型号、部件规格、部件状态、部件位置（经纬度）、所属报警主机、所属传输装置、所属单位、所属建筑物、所属楼层、图纸等信息。

8.5.2.1.4. 消防警力

1．基础信息采集

支持消防警力数据采集，包括总队、支队、大队、救援站信息，以及大队下的大队领导（大队长姓名、联系电话、副大队长姓名、联系电话、政委姓名、联系电话）、消防救援站（救援站站长姓名、联系电话、副站长姓名、联系电话、政委姓名、联系电话）；街道下的专职消防队、兼职消防队等信息。

2．出警记录采集

对全省各级消防部门消防警力（总队、支队、大队、救援站）的救援出动的时间、地点、报警来源等出警记录进行采集，形成全省各支队、各大队、救援站等消防警力救援出动情况的数据档案库。

8.5.2.1.5. 救援力量

支持救援力量数据采集，包括消防站布点在地图上的位置，以及统计每个消防站的消防人数、消防车总数、灭火类消防车总数、举高类消防车总数、专勤类消防车总数、专勤保障类消防车总数以及特种类消防车总数。

8.5.2.1.6. 管理机构

支持管理机构数据采集，主要包含市消防救援总队、支队、县（市、区）消防救援大队、乡镇（街道）、村（社区）工作站和行业主管部门等，采集管理机构的基本信息。

8.5.2.1.7. 水源信息

实现消防水源分布、市政水源分布、管网压力、消防力量分布管理功能。建立完善消防水源档案，完善消防水源分布图、设置地点、形式、数量、编号等。在地图上展示室外水源的位置和信息。

8.5.2.1.8. 重点部位

支持重点部位数据采集，采集各城市火灾风险单位消防重点部位信息，主要采集重点部位名称、建筑面积、耐火等级、所在位置、使用性质、消防设施情况、责任

人姓名、责任人公民身份号码、责任人电话、确立消防安全重点部位的原因、防火标志的设立情况、危险源情况、消防安全管理措施、重点部位所属单位名称等信息，便于了解辖区内所有重点部位的分布情况。

8.5.2.1.9. 地理编码

地理编码数据应涵盖以下内容：

1．行政区划数据：包括市、县（市、区）、乡镇（街道）、村（社区）；

2．单元网格数据：单元网格数据；

3．地名数据：包括现状地名、历史地名、历史沿革地名、地名别名等数据；

4．道路数据：包括主要道路、现状道路、弄、街等数据；

5．门址院落数据：包括院落名 称、门牌编号等；

6．小区楼座数据：包括小区名 称、楼座名 称等；

7．沿街店面：包括道路两旁商业单位、饭馆、企事业单位、机关等名称。

地理编码数据库以点、线、面方式表现城市地理实体。通过地理编码实现地址空间的相对定位，可以使城市中的各种数据资源通过地址信息反映到空间位置上来，提高空间信息的可读性，在各种空间范围行政区内达到信息的整合。通过地理编码技术对城市部件进行分类分项管理，最终实现社会化消防管理由盲目到精确，由人工管理到信息管理的转变。

8.5.2.1.10. 基础空间

基础空间数据库包括基础地形图、空间数据、行政区划分以及环境、城市建设、历史文化保护、人文、社会经济等众多的基础空间信息和非空间信息。

基础空间数据库是消防物联网远程监控系统的基础。数据分类依据各级部门所管理的数据信息内容进行划分。基础地理数据库可直接对消防管理相关的各部门提供准确实时的基础地理信息，保证了消防管理平台对基础地理信息的需求。

8.5.2.1.11. 建筑消防平面图编辑功能

建筑体内平面图编辑器：开发平面图编辑器，对建筑体内的平面图及消防设备分布情况进行编辑，由用户编辑建筑体内的平面图，并上传到服务器。

平面图编辑器：联网火灾风险单位建筑平面图；联网火灾风险单位消防平面图

建筑消防平面图管理系统：数据采集完成后，要将重要的消防设施按照楼宇编号、楼层编号、分区编码、设施类别编号、设施编号进行统一编码，对上述数据进行录入处理，并与后台数据库关联，在消防设施发生故障时能够即时在平面图上显示出故障点的位置，并发出提示信息。

8.5.2.2. 消防物联网监测数据采集

8.5.2.2.1. 远程联网监测数据

消防远程监控（展示火灾自动报警系统中，所有设备正常、离线、故障、报警的设备总数）、地图（平面图等）报警联动、报警视频联动。立体式监测火灾自动报警系统的运行状态及故障、报警信号基础。

8.5.2.2.2. 智能互联式探测器监测数据

提供对传统消防设备监控盲区的补充覆盖。提供消防无线互联式烟感、燃气探测设备接入渠道。支持报警 APP 通知、电话推送等功能。

说明：该部分内容可放至后续建设规划中，不列入本期概算。

8.5.2.2.3. 水系统液位（压）监测数据

消防水监控系统数据实时监测（展示消防用水系统中，所有设备正常、故障、报警的设备总数）、数据异常报警、显示水系统实时工作状态、环境温湿度实时监测。

支持实时监测室内消火栓和自动喷淋系统水压、高位消防水箱和消防水池水位、消防供水管道阀门启闭状态、弥补消防水监控系统监管空白，推送警情发生时消防

用水系统运转状态。

8.5.2.2.4. 电气火灾监测数据

系统实时监测联网建筑的电气火灾运行状态。能够将监测点剩余电流和温度等的实时变化自动绘成动态曲线，能够真实、直观的显示监测点电气火灾隐患情况。

当工作电流或温度发生异常时，立即发出报警，及早发现火灾隐患，从根本上避免因为电气短路或过载而引发的火灾危险。

8.5.2.2.5. 其他消防监督业务数据

企业单位开展自查自纠和消防安全教育培训数据，消防安全员排查或者抽查数据，行业主管部门监管执法数据，以及物联网故障数据和报警数据，这些消防管理的业务数据，需要统一存储，将作为执法和消防工作考核的有力依据。

8.5.2.2.6. 运营服务机构数据接入

系统支持预留各类对接接口，用于多厂家、多维度消防采集设备的接入，以及各区、街道自建平台的接入，顶层统一平台进行统筹、统展、统管。

整合已有的各运营服务机构监管中心，扩大监控系统的联网用户数量，完善系统报警联动、设施巡检、单位管理、基础数据等功能。配合手机 APP 系统，动态监控、立体呈现联网火灾风险单位消防安全。

8.5.2.3. 视频监控数据采集

“重点部位可视化监管模块”实现对重点部位（消控值班室、疏散通道、防火分区、消防登高操作场地等）的可视化监督。支持可对视频进行抓图、录像、回放、语音对讲的功能。可高效利用单位已装视频监控、社会面监控资源，实现大范围安防资源消防利用，提供多样音视频资源。

通过对消控值班室安装智能高清人脸识别摄像机（可选），可对消控室值班人员进行定时（如以 10 分钟间隔作为识别频率）人脸识别，以此计算出消控室值班人员

的离岗时间，并发出预警提示。通过该方式可以解决消控室值班人员不在岗、擅离职守等问题，加强联网火灾风险单位自身的消防安全管理责任意识，提高联网火灾风险单位建筑场所消防安全防护水平。

8.5.2.4. 监测数据分析与处置

8.5.2.4.1. 火灾报警分析

根据物联网监测数据进行火灾报警分析，主要分析依据为温感监测数据、烟感监测数据，如温度超过阈值、烟雾浓度超过阈值，多种监测数据超出阈值时共同组合成火灾报警分析依据，形成火灾报警即时告警信息和分析报告。

即时告警信息和分析报告推送至消防救援部门。

8.5.2.4.2. 安全隐患分析

安全隐患分析，主要可通过物联设备监测数据多次达到临界阈值、视频监控到通道堵塞情况等，形成安全隐患分析报告。

消防通道堵塞则是通过视频监控图像智能分析得出安全隐患分析报告。

分析报告推送至重点联网火灾风险单位。

8.5.2.4.3. 设备故障分析

根据物联设备、视频监控设备长时间离线状态，或长时间无信号数据上报，或上报数据频次过高等情况进行综合分析，得出设备故障分析报告。

分析报告推送至消防技术服务单位。

8.5.2.4.4. 值班行为分析

根据视频监控智能人脸分析，在间隔时间内进行消控值班室进行值班人员人脸分析扫描，得出值班人员是否存在脱岗行为，也可结合值班打卡信息，得出值班行为异常分析报告。

分析报告推送至重点联网火灾风险单位。

8.5.2.4.5. 事件（任务）生成

事件（任务）来源包括 2 个：

1. 监测数据前置分析形成的事件分析报告，同时作为任务下发；

2. 根据日常或临时巡查任务，自动或手动设置生成巡查任务并下发。

8.5.2.4.6. 事件（任务）下发

事件（任务）生成后，事件处置总调度员通过后台将处置任务下发至各消防责任主体用户的手机 APP 中，用户通过手机 APP 接收处置任务，并进行相应的签到、处置情况反馈、处置结果状态确认等信息的登记。

8.5.2.4.7. 事件（任务）处置跟踪与反馈

事件（任务）处置跟踪与反馈，主要对各消防责任主体的处置任务接收情况、任务执行情况（包括现场定位签到、现场拍照、隐患/故障情况说明、处置过程信息、处置结果状态确认、处置结果现场拍照确认、签字单据确认等）

8.5.3. 消防数据基础统计分析报表系统

消防数据基础统计分析管理主要用于日常的数据查询、汇总、统计，以及报表自定义、报表生成、报表展示、报表输出、报表存储等。

消防数据统计分析系统，提供非模型化的查询条件、汇总条件、统计条件，以及规则化（非模型）的分析条件，辅以高性能的大数据查询检索性能，得出各级消防监管部门、使用部门、服务对象等所需要的日常统计分析报表。

8.5.3.1. 查询统计要素管理

针对平台的基础统计分析功能，首先要针对不同的消防业务类型、消防数据类型进行查询统计要素进行分类建立和分类管理。

查询统计要素主要包括：

1．单一要素：主要针对某个业务属性、业务特征字段等，建立独立的单一查询统计要素。

2．复合要素：主要针对多个业务属性、业务特征字段，进行组合，建立固定的复合查询统计要素。

3．运算要素：通过单个或多个业务属性特征字段，辅以简单或复杂的运算计算规则，实现查询统计。该方式通常以运算视图、数据存储过程等方式实现。

8.5.3.2. 可视化报表自定义

提供“所见即所得”的可视化报表自定义功能，为普通用户提供报表自定义、自建功能。

报表自定义主要包括：

1．表头/表格自定义：用于定义报表呈现的页面格式、样式。

2．表格数据来源选择：选择每行、每列的表格数据来源。

3．表格运算功能选择定义：定义表格行、列的数据运算功能。

4．表格模板生成：报表自定义完成后，生成报表表格模板，并输出为固定模板文件。

8.5.3.3. 统计分析报表展示

统计分析报表通常以二位数据表格、饼状图、柱状图、坐标曲线图、蛛网图（星空图）等形式进行综合展示呈现。

8.5.3.4. 报表性能管理

在海量数据中进行数据报表查询、汇总、统计，必须要具备优越的性能，才能满足快速报表自定义、报表生成展示与报表输出需求。

具体的性能主要通过以下几个方式来实现：

1．SQL 语句优化：减少行计算、减少关联查询和嵌套查询。

2．数据库字段优化：在设计阶段就必须开始进行字段设计优化，如字段长度冗余、数据格式选择等。

3．建立索引：如主键索引、联合索引、针对 SQL 语句单独建立索引等。

4．适当增加冗余字段，采用空间换效率的方式提升 SQL 执行效率。

8.5.3.5. 报表结果存储管理

针对查询统计报表输出的结果，具有静态性质和长期使用价值的，可以将报表结果文件长期保存，并进行归类，便于下一次有相同报表统计需求时，直接调取，降低冗余报表运算请求对服务器资源需求量。

8.5.4. 基于大数据火灾智能预警模型分析系统（BI）

随着消防信息化建设的逐步深入，消防领域积累了海量数据，在融合共享基础上，如何充分挖掘数据价值，使数据转化为“智慧”，是当前和今后一段时期内消防工作的重中之重。通过建设消防安全综合评估模型、隐患趋势分析模型等大数据分析与计算模型，让消防感知数据、业务系统数据等充分发挥其效能，打造消防大数据分析服务体系，为消防事业跨越发展添翼赋能。

大数据火灾智能预警模型分析，须建立在前述消防大数据中心管理系统的 ETL 功能基础之上。在本项目中，要进行消防大数据分析，必须采取专业的可视化 ETL（Extract-Transform-Load）数据抽取工具，对原始数据进行采集、清洗、抽取、转换加工、装载数据服务等一系列过程操作，从而为大数据分析及其它应用功能提供数据服务。

8.5.4.1. BI 基本定义

商业智能（Business Intelligence，简称：BI），又称商业智慧或商务智能，指用现代数据仓库技术、线上分析处理技术、数据挖掘和数据展现技术进行数据分析以实现商业价值。

商业智能通常被理解为将企业中现有的数据转化为知识，帮助企业做出明智的业务经营决策的工具。这里所谈的数据包括来自企业业务系统的订单、库存、交易账目、客户和供应商等来自企业所处行业和竞争对手的数据以及来自企业所处的其他外部环境中的各种数据。而商业智能能够辅助的业务经营决策，既可以是操作层的，也可以是战术层和战略层的决策。为了将数据转化为知识，需要利用数据仓库、

联机分析处理（OLAP）工具和数据挖掘等技术。因此，从技术层面上讲，商业智能不是什么新技术，它只是数据仓库、OLAP 和数据挖掘等技术的综合运用。

可以认为，商业智能是对商业信息的搜集、管理和分析过程，目的是使企业的各级决策者获得知识或洞察力（insight），促使他们做出对企业更有利的决策。商业智能一般由数据仓库、联机分析处理、数据挖掘、数据备份和恢复等部分组成。商业智能的实现涉及到软件、硬件、咨询服务及应用，其基本体系结构包括数据仓库、联机分析处理和数据挖掘三个部分。

因此，把商业智能看成是一种解决方案应该比较恰当。商业智能的关键是从许多来自不同的企业运作系统的数据中提取出有用的数据并进行清理，以保证数据的正确性，然后经过抽取（Extraction）、转换（Transformation）和装载（Load），即 ETL 过程，合并到一个企业级的数据仓库里，从而得到企业数据的一个全局视图，在此基础上利用合适的查询和分析工具、数据挖掘工具、OLAP 工具等对其进行分析和处理（这时信息变为辅助决策的知识），最后将知识呈现给管理者，为管理者的决策过程提供支持。

8.5.4.2. 消防大数据 BI 模型分析目标

基于大数据的火灾智能预警模型分析系统，其主要目标是综合各种火灾要素和周边环境要素的基础上，运用数学、物理、计算机等多门综合学科，针对不同应用场景建立不同的火灾算法模型，并将火灾算法模型应用到具体业务分析中，得出各级消防业务部门所需的分析结果。

具体的模型分析目标包括：

1. 火灾风险/隐患分析
2. 责任落实情况分析
3. 易燃易爆物品管控分析
4. 视频监控分析
5. 火灾预测分析
6. 智能化辅助决策模型
7. 精细化效能评估
8. ……

8.5.4.3. 火灾风险模型设计

1．火灾类型定义（人为火灾、自然火灾、电气线路火灾等）

2．火灾风险因子定义（因子，代表影响火灾风险值变化的各种基本因素）

3．火灾风险因子权重（%）/分值定义

4．火灾风险因子变化规则定义

5．火灾风险模型设计（融合多类型、多因子、权重、规则，形成完整模型，可进行高效海量数据分析，实现精准度较高的模型分析结果输出）

6．模型进化设计（涉及 AI 部分，AI 智能模型，具备自分析、自我学习、不断迭代、人工干预进化、模型自主进化等特点）

8.5.4.4. 消防大数据 BI 智能分析模型（参考）

8.5.4.4.1. 建筑起火频率预测模型

统计分析包括住宅、公共建筑、厂房等场所的历史火灾，根据建筑检查信息等信息预测建筑起火频率，构建建筑起火概率预测模型，并对起火频率进行分级。

8.5.4.4.2. 建筑火灾损失预测分析模型

通过对住宅、公共建筑、厂房建筑历史火灾损失等数据进行分析，构建建筑火灾损失预测模型，并对火灾损失进行分级。

8.5.4.4.3. 区域火灾防控能力评估模型

模型建立可包括消防应急通讯子模型、消防队人员评估子模型、消防站布局评估子模型等模型评估结果为因子项建立模型。

（1）消防应急通讯评估子模型

模型建立包括接处警时间数据等因子的子评估因子项，同时结合福建省应急通讯实际数据情况，建立应急通讯评估子模型。

（2）消防队人员评估子模型

模型建立包括人员配置情况、消防人员战斗能力等因子的子评估因子项，同时结合国内消防员配置情况，以及福建省各市消防站实际情况，建立消防队人员评估子模型。

（3）消防站布局评估子模型

模型建立消防站管辖范围等因子的子评估因子项，根据福建省各市消防站数据情况，建立消防站布局评估子模型。

（4）其他评估 4 个子模型

建立其他区域火灾防控能力的子模型，结合福建省消防的情况，对区域火灾防控评估模型进行完善修正。

8.5.4.4.4. 火灾仿真模拟模型

建立办公、住宅、商业等典型场所的火灾仿真子模型，预测火灾损失。

8.5.4.4.5. 三维区域火灾风险评估模型

根据建筑起火频率预测结果、建筑火灾损失预测结果和消防站火灾防控能力评估模型评估结果等数据，构建三维区域火灾隐患风险评估模型，对区域火灾风险进行综合分析，并根据数据变动情况对模型进行优化。

8.5.4.4.6. 全省消防安全综合评估分析模型

基于城乡人口密度、消防经费投入情况、火灾隐患分布、建筑密度及高危建筑类型比例、重大危险源分布及类型、人员密集场所分布、单位及建筑消防水平、灭火救援能力、社会消防意识、历史火灾事故分布及损失等评估指标基础数据，通过构建评估指标体系和权重分布，利用分析引擎计算层次化消防安全综合评分，并根据后验性数据对指标体系及权重分布进行有人介入的循环链训练提升，使之持续演进，更好适应经济社会条件下消防安全特点。

8.5.4.4.7. 城市消防安全评估分析模型

基于城市地理与自然条件、产业分布、建筑密度及类型分布、重大危险源、人员密集场所、消防系统健康情况、单位消防管理水平、灭火救援机构分布及处置能力、消防安全宣传教育、消防经费预算与投入和历史火灾事故状况等一级指标，通过自顶向下形成指标体系。通过指标体系，确定其权重分布，能够输出多层级城市消防安全评价分值。

8.5.4.4.8. 区域消防安全综合评估分析模型

基于区域建筑分布数据、规模体量数据、建筑消防系统数据、建筑消防管理数据、区域救援力量及救援条件数据，通过构建评估体系、确定指标权重、收集指标数据、计算风险得分，根据历史事件对体系及权重进行动态调整，并以区域消防安全等级及风险得分为输出。

8.5.4.4.9. 隐患趋势分析评估分析模型

基于历史隐患发现处置记录、消防系统运行状态记录、消防管理历史记录等数据，以时间序列分析工具为核心，结合关联分析、聚类分析、拟合分析等其他工具，并以综合隐患发生趋势时间数量曲线为输出。

8.5.4.4.10. 消防水资源健康度评估分析模型

基于消防水资源历史运行状态数据、巡查巡检数据、监测维保数据等，通过构建评估体系、确定指标权重、收集指标数据、计算风险得分，并根据故障、维修等事件对体系及权重进行动态调整，并以水系统健康度为输出。

8.5.4.4.11. 电气火灾风险评估分析模型

基于剩余电流、线缆温度和故障电弧等电气火灾直接特征参数，电流、电压、功率等用电功率特征参数，谐波、浪涌、功率因素等电能质量特征参数，以及大功

率电气用电指纹特征，通过边缘特征智能分析识别和云端多参数统筹分析相结合，研判电气火灾发生风险并提供针对性预警，并初步确定承灾体、致灾因子，用于指导电气火灾隐患排查治理。

8.5.4.4.12. 企业消防安全评估分析模型

旨在通过企业建筑防火设计、消防设施安全状态、消防安全管理制度和日常消防安全管理工作情况等要素及其对消防安全的影响程度，确定指标体系，并建立相关算法，实现对企业消防安全指数的计算。根据分析对象不同，可分为：

（1）一般单位消防安全评估模型

基于企业基础数据、消防系统状态数据、消防管理水平数据、周边救援力量及救援条件数据、企业火灾事故历史数据，综合考虑其对火灾损失指标预期的正向作用与负向作用，形成适用于一般单位的消防安全评估指标体系。

（2）火灾风险单位消防安全评估模型

在一般单位评估模型分析应用设计的基础上，结合火灾风险单位消防安全管理的特殊要求，以及特殊建筑对防火设计和消防设施、系统的管理规定，增补指标项并重新确定各层级指标权重分布，形成适用于火灾风险单位的细粒度消防安全评估模型。

（3）特殊行业火灾风险单位消防安全评估模型

在火灾风险单位评估模型的基础上，根据石油化工、港口和文物古建所独有的重大危险源、危化品、化工反应器、露天堆场、木质建筑，以及动火作业、燃烧香烛等特殊行为，对评估内容、指标体系和评估算法进行调整优化，形成特殊行业火灾风险单位消防安全评估模型。

8.5.4.4.13. 火灾预防策略智能分析

1．电气火灾预防

针对电气火灾频发的原因，根据历史火灾数据及延伸调研大数据分析，提出电气隐患检查策略、内容及解决措施，从根本上减少电气火灾的发生频率。

2．生产作业火灾预防

针对生产作业火灾，分析福建特色产业的生产作业中起火频率较高的关键部位及工序，参考历史火灾数据及延伸调研大数据分析，有针对的提出不同建筑类型生产作业隐患检查策略、内容及日常火灾防控要求，降低生产作业火灾发生频率。

3．用火不慎火灾预防

针对用火不慎的起火原因，根据历史火灾数据及延伸调研大数据分析，提出不同建筑类型用火不慎的预防策略及要点，降低用火不慎火灾发生频率。

4．其他火灾预防策略

8.5.4.4.14. 消防宣传内容及策略分析

为提高公众、单位对火灾隐患的认识，提出针对公众及单位的火灾危险源辨识提出全面及综合的实施体系。

8.5.4.5. 大数据分析模型构建方法

拟采用业内相对成熟完善的分析模型，根据智慧消防建设对智能化应用的实际需求，与相关科研院所和厂商共同发展相关算法。在此基础上，实现智能分析应用服务的构建，包括以下几点。

8.5.4.5.1. 分析算法模型的微服务移植封装

根据微服务开发框架和业务支撑应用技术规范要求，在算法模型基础上进行移植和微服务封装，使之符合 SOA 架构与 Spring Cloud 框架，能够在微服务集群中发布、部署、注册、运行，可被其他应用服务及任务调度机制调用，并被统一监测和管理。

8.5.4.5.2. 分析计算所需专题库数据集构建

根据数据中台整体架构，需将分析算法所依赖的数据集作为库表纳入数据资源池专题库，其建立方式符合专题库设计规范，并确定专题库数据订阅、更新方式。当需要实时分析时，需在专题库建立基于数据变化的触发机制，发起对算法服务的

调用，以随时产生分析结果。

8.5.4.5.3. 分析算法模型效用的追踪与持续演进

随着专题库中数据集的积累，可利用后验性数据与算法结果进行比对，依靠算法内部或外部偏差度分析机制对算法结果质量进行分析，并根据算法运行性能日志和异常日志，形成算法效用评估结果，作为算法进一步改进的依据。

8.5.5. 消防值班监控中心管理系统

8.5.5.1. 值班在岗登记

平台运维值班人员上岗开始工作前，需要进行打卡登记，可通过视频打卡方式、用户登录打卡方式进行在岗登记。

下班后需进行离岗打卡登记。

8.5.5.2. 交接班异常告警

值班人员交接班时，离岗打开时间和上岗打卡时间间隔不能超过 1 分钟（可根据实际情况进行设定），否则系统将发出无人值守告警。

8.5.5.3. 值班报表管理

取代传统值班信息填写表格，采用软件记录方式，对值班过程发生的情况进行记录，例如火灾报警信息、安全隐患信息、设备故障信息、值班来电信息、运维过程异常信息等。

1. 系统自动记录。通过消防物联网远程监控系统对各联网火灾风险单位的监控，自动分析和获取监控对象的异常情况（火灾、隐患、故障等），并进行自动记录和提醒相关责任单位。

2. 人工记录。值班人员记录系统未监控到的其它异常情况或值班来电来访情况。

8.5.5.4. 消防证核实与预警

根据联网火灾风险单位录入的消控室值班人员的“消防证”进行全面检查或抽

检核实，以确定消防证的真实性。

同时，系统根据消防证的到期日期进行监测预警，包括即将到期预警、过期告警等。

8.5.5.5. 联网火灾风险单位消控值班室查岗

随机抽选联网火灾风险单位，联系消控室值班人员进行视频拍照查岗。

8.5.5.6. 即时通讯（IM）

可通过手机 APP 内置的即时通讯软件与消防各级部门、火灾风险单位、技术服务单位、值班运维机构等用户进行在线实时沟通。

8.5.5.7. 值班监控报警

值班监控中心系统获取感知网分中心预分析处理异常报警信息，以及获取省平台消防物联网远程监控系统中的监测数据二次分析结果，并进行大屏展示发出告警。针对二次分析研判结果，为异常的，要进入后续处置流程。

8.5.1. 基于 BIM 的消防应用

8.5.1.1. BIM/CIM 定义

CIM——城市信息模型（City Information Modeling），是三维城市空间模型和城市动态信息的有机综合体，是将微观建筑信息模型（Building Information Modeling，简称 BIM）、宏观地理空间数据（Geo-Spatial Data，简称 GSD）、物联网（Internet of Things，简称 IoT）数据进行统一，形成综合数据处理计算平台。

故：CIM（城市信息模型）= BIM（建筑信息模型）+GIS（地理信息系统）+IoT（物联网）

建设 CIM 城市信息模型群是一项庞大的工程，受限于整体建设成本预算及成本控制，本次福建省智慧消防系统平台建设，将围绕单个或少量 BIM 模型试点进行展开设计，并结合 GIS 系统和 IOT 物联网，实现 BIM 在福建省智慧消防平台的初步应用展示，为后续大规模 CIM 集群建设的开展，奠定良好设计与技术基础。

8.5.1.2. BIM 在消防实战中的应用

BIM 技术是一种三维数字化信息技术，它以建筑工程项目的各相关信息数据为基础进行建模，通过模型整合各种信息，在项目的全生命周期中进行共享和传递。将 BIM 技术应用于消防领域，将在图形可视化、设计方案协调以及火灾场景模拟等方面具有显著优势。

依托三维建筑信息模型（BIM）平台，通过添加消防数据模块，整合建筑构件、消防设备、人员流向和周边环境等信息，构建建筑消防设计图纸审查、建筑防火、灭火应急救援的综合应用平台。与以往的各种消防应用系统相比，基于 BIM 的建筑消防数字化管理平台将更安全、更精细、更高效。

BIM 应用于消防领域的具体实战应用，主要体现以下方面：

1．应用于建设工程消防行政审批图纸的三维可视化数据审查；

2．实现对建筑内部情况数据化管理便于日常防火监督检查；

3．提高灭火救援演练的实战性，保障了实际火场指挥决策的准确性。

8.5.1.3. BIM 下消防安全管理综合应用系统

基于 BIM 技术的消防安全管理综合系统，其主要包括数据库系统、基础平台系统、应用平台系统，还可以进一步细化为 GIS 数据库、BIM 数据库、火灾模型数据库、消防资源数据库。这些数据库是支撑消防安全管理综合应用系统的基础内容。综合应用系统的主要架构与功能包括：消防设计图纸审查系统、防火监督检查系统、火灾救援预案训练系统、应急疏散逃生系统。

8.5.1.3.1. BIM 基础数据库设计

建设基于 BIM 消防安全应用系统，首先要对 BIM 中涉及的消防要素数据进行数据模型定义（包括数据名称、数据类型、数据规范、数据格式、数据释义、数据约束等），通常的 BIM 数据包括：

（1）建筑结构数据；

（2）建筑专业数据；

（3）水暖电专业数据；

基于BIM的消防应用，则需要加入消防安全相关要素数据，包括：

（1）消防基础数据（联网火灾风险单位信息、建/构筑物、消防设施、消防设施部件、消防警力、救援力量、管理机构、水源信息、重点部位）

（2）消防业务数据（火警信息、火灾信息、受理信息、消防设施检查信息、消防设施保养信息、查岗信息）

（3）其它数据（其它特殊或专业应用数据、综合报表数据、系统管理数据、GIS数据、火灾模型数据等）。

以上这些数据库是支撑消防安全管理综合应用系统的基础内容。综合应用系统的主要架构与功能包括：消防设计图纸审查系统、防火监督检查系统、火灾救援预案训练系统、应急疏散逃生系统。

8.5.1.3.2. 消防设计图纸审查系统

消防图纸审查系统主要是采用了电子图纸，是静态平面形式。图纸当中含有消防设计当中的各项参数，但是参数信息非常冗余，审查人员检查参数多有不便。如审查防火分区划分要沿着分区标注线一一检查，才能够掌握分区边界范围。疏散楼梯设置数量与方式等参数信息也要投入大量的时间，个别时间还需要和设计单位多次沟通。而 BIM 下的图纸审查系统，可以动态掌握不同颜色区域的参数，可以更加清楚对消防区域进行划分，包括救援路线、疏散路线等等。再者，在整个 BIM 设计审查系统当中，要结合消防设计图纸审查标准，提供各类测量、查询、标注工具，最大程度上减少图纸审查所需时间，保证设计、审查、修改、施工效率。

8.5.1.3.3. 建筑防火监督检查系统

结合我国消防相关法律法规标准，通过审查的消防系统参数不会有太大差异。如果因为某些因素需要变更消防系统设计功能，要重新展开消防系统设计报批程序。但是很多单位擅自更改消防系统结构或建筑使用功能，从而增加了建筑火灾风险。在BIM防火监督检查系统中,通过BIM平台可以快速查找到工程消防相关文件信息，粪便设计参数、使用功能是否发生了变化。此外，通过在建筑结构模型当中科学设置消防管道，在消防管道周边、建筑控矿位置设置传感器，可以实时传递建筑消防

安全信息，监督人员可以通过网络平台远程监控消防系统日常运行情况，加强对消防安全管理质量，从而实现最终的消防目标。

8.5.1.3.4. 应急疏散逃生指示系统

对于办公楼、写字楼等建筑，由于建筑内部结构简单，发生火灾人员疏散较为简单。但是对于综合性建筑，如商场、歌厅等人员密集场所，由于人员变动大，多数人不熟悉建筑构造、疏散路线，因此需要重点考虑如何安全疏散。采用 BIM 应急疏散逃生系统，主要是应用三维图形形式，辅助动态性图表、声光指示灯，可以有效调整逃生路线，并且结合 BIM 结构图形，找出最佳的逃生路线，结合消防广播指导人员逃生，从而保障人员生命安全。

8.5.2. 消防大数据“一张图”综合展示系统

系统支持将各类系统的资源和数据进行深度的分析和展示上墙功能，有效呈现消防设施情况、消防管理数据分析、警情分析、隐患分析、天气等，形成以业务为导向的大数据指挥作战图墙，直观地了解消防设施实时信息、消防管理情况以及警情的及时汇总情况。消防大数据“一张图”综合展示系统可投放于省市县消防救援部门的应急指挥中心大屏、值班监控中心大屏等，也可在电脑屏幕上进行投放展示。

省市县每个辖区的一张图展示，都只显示本辖区行政区划内地图交通、楼宇建筑、道路、消防资源等情况。

1．多视图整合，探索不同维度的数据关系

通过专业的统计数据分析系统设 计方法，理清海量数据指标与维度。按主题呈现复杂数据背后的联系；将多个视图整合，展示同一数据在不同维度下的规律，帮助用户从不同角度分析数据、缩小答案的范围、展示数据的不同影响，具备显示结果的形象化和使用过程的互动性，便于用户及时捕捉其关注的数据信息。

2．所有数据视图交互联动

每一项数据在不同维度指标下交互联动，展示数据在不同角度的走势、比例、关系。除了原有的饼状图、柱形图、热力图、地理信息图等数据展现方式，还可以通过图像的颜色、亮度、大小、形状、运动趋势等多种方式在一系列图形中对数据进行分析，帮助用户通过交互，挖掘数据之间的关联。并支持数据的多维并行分析，

利用数据帮助决策者做决策。

3．强大的大屏展示效果

支持主从屏联动、多屏联动等大屏展示功能，可支持触控交互，满足用户的不同展示需求。可以将同一主题下的多种形式的数据综合展现在同一个或分别展示在几个高分辨率界面之内，实现多种数据的同步跟踪、切换。

8.5.2.1. 消防地理信息“一张图”

建设消防地理信息“一张图”展示功能，支持显示 2D 地图和卫星地图，地图中能够显示各类设备状态和报警信息、建筑评分、责任网格、网格责任人信息，点击相应图标，可弹出该图标位置的建筑、设备的基本信息。

地理信息“一张图”中显示地理信息监控界面区域概貌地图，在正常监视界面下，可以对地进行浏览、放大、缩小操作。报警状态下，自动定位报警区位置，以红色标识报警点；系统可支持具备条件的单位应能够录入建筑分层图，图中可对各类消防设施、监控摄像头、配电控制箱等设备进行标注。出警线路规划及建筑周边情况显示，在地图中显示火警信息的位置，并能够辅助规划 119 灭火救援的路线。

通过地理信息“一张图”，可全局预览全省联网火灾风险单位消防概况：（1）可在地图上显示所有联网社会单位，可在地图上实现红、黄、绿“消防三色预警机制”显示。（2）通过树状目录按不同辖区选择要显示的社会单位，方便选择和查看各个辖区管理情况。（3）点击单位可显示单位详细信息，包括单位名称、地址、联系人、联系方式、单位灭火设备实施实时状态等。在首页可显示当日报警情况（报警单位总数报警总数及详细信息）。

8.5.2.2. 消防一张图火灾防控

将消防防控元素集中体现在消防专用地图中，每一个元素既与其他元素形成整体性又具有作为个体的单一性。在日常工作中，对单一的元素进行巡检更新，保持数据的准确性。

通过火灾防控管理逐级汇聚至火灾防控“一张图”中，关联作战对象的地理位置、概况、结构、消防设施，以及周边道路、水源、重大危险源等信息，为分析研判作战对象提供立体式支撑。提供火灾数据分析功能，供分析和决策时灵活调用。

主要通过救援力量分析、火灾事件分析两个维度数据分析进行整合决策支持，实现辖区消防队站、多种形式消防队伍、装备器材、保障物资等信息汇总，为科学指挥和力量调度提供准确信息参考。

8.5.2.3. 全国消防“一张图”数据标准规范

福建省智慧消防云平台在进行消防大数据一张图综合展示系统建设时，必须要遵循全国消防“一张图”数据标准规范和服务接口规范，以及按照全国消防一张图的部署建设方案要求进行福建省消防“一张图”的定制开发。

具体参考：

1.《全国消防一张图部署建设方案》

2.《全国消防一张图数据标准规范》

3.《全国消防一张图服务接口规范》

8.5.2.4. 消防一张图提供服务说明

2019 年，消防救援局统一规划地图支撑系统——消防一张图，作为消防救援信息化的基础平台，供各地建设消防救援信息化系统使用。2020 年，消防救援局正式建设消防一张图，主要提供如下三块服务：

1．地图数据更新服务：统一提供地图数据更新服务，包括电子矢量地图与影像地图，其中电子矢量地图提供每年四次的更新服务，影像地图提供每年一次的更新服务（消防救援局只负责提供地图更新数据，具体数据更新和维护由各消防救援总队、支队自行安排）；

2．统一对外接口服务：提供一系列对外的服务，可对第三方业务系统提供相应的地图服务；

3．技术支撑服务：提供全面的技术支撑，协助第三方系统能顺利的调用地图服务。

消防一张图的地图采用 CGCS2000 坐标系，与应急管理部一张图保持同一坐标系，可与其无缝对接。

8.5.2.5. 智慧消防云平台与消防一张图对接

目前在福建省消防救援总队以及各支队、各大队，部署的均是原公安部消防局下发的全国消防一张图系统平台，为避免重复建设，福建省智慧消防云平台与消防一张图系统平台的对接方式，可采取以下方式：

1．由部消防救援局的消防一张图系统平台提供 B/S 模式的 WEB 页面，可直接嵌入至智慧消防云平台中进行展示，并提供部分数据接口供智慧消防云平台进行调用。

2．由部局消防一张图系统平台统一提供数据接口，智慧消防云平台使用公共、社会化的 GIS 电子地图（如百度地图），在布局一张图和社会化电子地图之间进行坐标系转换，实现全国消防一张图系统平台数据在社会化电子地图上的精准展示。

8.5.3. 消防教育远程培训服务平台

8.5.3.1. 培训服务平台建设要点

1．该平台属于“信息发布类、信息服务类”的门户性平台，根据国务院及福建省政府有关门户网站建设的相关要求，除各单位的统一对外官方门户网站外，不得另外申请一级域名和自立网站门户。因此，消防教育远程培训服务平台，必须依托于省消防救援总队的官方门户网站或智慧消防门户，实现平台访问跳转。

2．涉及移动端的政务信息发布，必须对接福建省政府“闽政通”APP，实现政务公开信息统一汇聚于闽政通 APP 进行统一出口发布。

8.5.3.2. 消防行业从业人员职业化培训管理系统平台

8.5.3.2.1. 平台建设目标

通过“消防行业从业人员职业化培训管理系统平台”的建设，加强对消防服务机构从业人员的规范化管理，提高从业人员技术水平，促进消防工程安装、消防设备设施维保等工作的质量提升，消除消防安全隐患，降低消防安全事故率，全面保障社会公共消防安全，保障人民群众及机构单位的人身及财产安全。

8.5.3.2.2. 职业化培训对象

培训对象：消防工程安装、消防维保等机构的相关从业人员

从业要求：持证上岗

8.5.3.2.3. 系统主要功能

系统平台的主要功能分为：培训管理端、消防维保企业端。

（一）培训管理端功能（PC 端）

1．办班管理：包括发布办班计划（培训时间、地点、讲师、培训课程、学时等）、接收消防维保企业报名、培训学员身份信息核对、培训费用收取核对、培训花名册汇总统计。

2．开班管理：包括培训学员签到管理、培训过程现场资料上传、培训课件上传等。

3．考试管理：包括学员考试成绩录入，设定考试评分规则，系统根据评分规则对学员考试成绩进行自动打分和合格情况评定。

4．发证管理：管理员根据考试结果进行发证操作，系统自动进行证书编号和自动生成电子证书格式。

5．异常管理：包括黑名单管理、培训人员异常提醒（例如同个身份证号码从业人员多次参加培训等）。

6．其它功能：如电子通知公告、职业化培训政策信息发布、相关从业规范信息发布、培训电子课件下载等。

（二）消防维保企业端（PC 端、微信端）

1．培训报名：根据培训管理端发布的办班计划，提交从业人员基本信息和上传身份证扫描件信息；可进行在线缴费（需对接微信支付或支付宝等第三方支付通道）

2．成绩查询：查询本机构从业人员的培训过程及考试成绩。

3．证书下载：通过每一期的办班培训计划，下载本机构从业人员的电子证书。

4．通知公告：接收系统发布的各项通知公告信息。

5．其它功能：培训政策信息查询、电子课件下载

8.5.3.3. 消防救援作战人员培训平台

8.5.3.3.1. 建设目标

建设消防救援作战人员培训平台，目的在于罗列社会各种常见的应急救援场景，通过虚拟现实技术（VR）将消防应急救援场景的各要素进行虚拟化，实现仿真沉浸式培训，不受场地等外界条件限制，让救援作战人员身临其境，提高消防救援作战战训效率。

8.5.3.3.2. 培训对象及培训内容

1．培训对象：消防救援作战人员、其它相关机构消防保障人员

2．培训内容：常见救援场景培训，如楼房救火救援、高楼轻生者救援、交通事故车辆移动破拆救援、河流湖泊溺水者救援等。

8.5.3.3.3. 主要技术

运用虚拟现实技术（VR）实现仿真沉浸式培训。

8.5.3.3.4. 系统主要功能

指挥员计划指挥和临机指挥训练

1．力量查询：通过列表、图表、地图、统计数据等方式，快速查询消防应急作战力量的分布和作战实力情况，包括消防作战机构数量、消防设备设施数量、消防人员数量及岗位职责。

2．地理信息测量：在电子地图（2D 或 3D 地图）对救援地点进行快速定位，并连接救援地点周边的消防作战机构，快速规划多条最优的作战行进路线，便于快速指挥调度救援力量前往救援。

3．作战部署标绘：在电子地图上，结合地理信息测量结果，指挥人员可在电子触控大屏上手动进行作战部署标绘，如救援路线标绘，各救援点位作战力量（人员、设备）部署配置，系统提供各种快捷的标绘元素组件在电子地图上以图标状标志显

示。

4．辅助单兵定位：对救援力量的单兵进行现场定位，以及接收现场实时数据反馈（例如视频、语音、环境数据采集等），可更加精准指挥单兵救援和自我安全保护。

作战员业务学习

1．室内熟悉演练：作战人员通过虚拟现实技术（VR）进行仿真演练，所有演练过程环节都会通过系统进行记录和自动评分。

2．战例复盘：对历史演练战例，可实时调取复盘并播放，供所有指挥作战人员进行评价讨论，便于发现演练过程中不足之处。

3．作战指挥推演：将救援配备力量、救援目标、救援等级、道路交通路线、救援障碍等各种要素集中起来，为作战指挥人员提供电子沙盘救援作战推演。

4．三维场景展示：用于展示各种救援场景的 3D 模型，方便作战指挥人员无需经常到实际现场进行考察，加深作战人员对各种应急救援场所环境和救援要点的熟悉程度。

8.5.3.4. 社会化消防培训

8.5.3.4.1. 建设目标

社会化消防培训是为了让广大人民群众学习消防知识，体验消防文化，参加休闲娱乐消防互动，深入了解消防基本共通性，了解防火安全和应对火灾的感受。

8.5.3.4.2. 培训对象

社会公众（包括居民、机构职工、企业职员等）

8.5.3.4.3. 主要功能

1．消防知识宣传：区域消防动态、生活工作消防小技巧、消防案例分析、消防技术创新、最新救援装备等讯息发布探讨。

2．消防公益培训办班：包括发布培训通知、线上接受报名（须提交报名人员基本信息）、现场培训过程及结果上传发布、发放培训电子证书和纸质证书（如初级社

会消防人员证书）、往期培训查询、

3．消防指战员：消防立功或先进事迹人物报道、消防转业人员再就业。

8.5.3.5. 在线教材资源管理

消防教育远程培训服务平台，除了软件自身管理功能外，还包括需要引入的各种教育资源素材。系统平台提供教材资源素材的管理功能，包括：

1．开放性教育资源采集：针对社会上或互联网上那些不具有版权的公共教育资源，可直接采集获取（标注来源），并进行编目存储。

2．教育资源导入：针对自创的、外部采购的教育资源，可按照其格式（如文档格式、视频格式、VR 格式、可执行程序格式等）导入或挂载于教材资源库中，提供授权调用。

3．版权授权到期预警提醒功能：针对外部采购的，具有版权限制、授权期限限制、授权用户数量限制的教材资源，系统根据导入时间、授权时间、授权数量、版权变更情况等，进行定期巡检和预警，避免超期无法使用或侵权。

8.5.3.6. 社会化线上学习管理

针对社会化的线上学习管理，主要结合前述社会化消防培训的多个类型对象（社会公众，包括居民、机构职工、企业职员等）提供线上免费学习教育功能。

1．在线学习：选择专题在线看视频、浏览文档资料（提供下载）、学习后掌握度测评等。

2．在线互动：提供趣味消防小应用，加强社会公众对消防安全意识的培养与理解。

3．学习专题管理：对学习资料内容（视频、文档等）进行分类，也可根据该段时间的政策形势、会议风向、特殊节日等进行消防学习专题自定义。

4．题库管理：针对不同学习专题，可设置在线测评试题及对应答案、解析点评等信息。

5．互动交流：提供非行政管理职能（如投诉、举报）的日常消防知识互动，例如简易的论坛、朋友圈形式发布互动交流主题。

8.6. 平台支撑服务系统

8.6.1. 系统功能概述

平台应用支撑服务系统的主要需求内容包括：

一是通过应用支撑服务系统作为系统的软件运行环境，提供基础的公共功能，支持信息交换、协同工作；

二是通过应用支撑系统作为应用管理和数据管理平台，实现统一的用户管理和权限控制。在此基础上，支持各种具体应用。

三是应用支撑系统基于构件化思想，可以随用户的不同需要提供不同的解决方案。该系统设计的构件化思路是以基础构件为核心、其他构件为业务插件的“主体+插件”形式，搭建出来的各个子系统健壮灵活，从而保证了大型企业级应用的稳定性和高效的可扩展性。

四是应用支撑系统作为系统的中间层构件，它基于跨操作系统平台、数据库平台的中间件软件构建，应具有良好的平台兼容性、部署灵活性、互操作性和标准性等特点，从而达到基于应用支撑平台之上构建的业务应用系统，建设周期短，平台移植性强，系统运行稳定、维护方便的目的。

8.6.2. 软件应用基础支撑功能

业务基础软件支撑平台是指以业务为导向和驱动的、可快速构建应用软件的软件平台。业务基础软件支撑平台功能包括集成应用平台、开发体系两个部分。从技术角度分析，业务基础软件平台为复杂应用软件系统的开发提供了一个基本框架，并有与之相应的、方便易用的开发与维护管理工具。这个框架给出了一些复杂应用软件的基本组成部分和实现方法，并且预置了很多供参考的软件模块。有了这样的准备，在业务基础软件平台之上开发管理软件就可以降低复杂性，省去很多基础性的研发工作，从而大大缩短研发周期，提高研发效率。

软件应用支撑平台功能是用来构建和支撑应用软件的独立软件系统，包含支撑环境和开发体系这两个基本要素，其本质是将复杂应用软件进行系统分层。

目前软件平台可以分为操作系统平台、软件基础支撑系统平台和业务基础软件平台。

基础应用支撑系统是一个信息的集成环境，是将分散、异构的应用和信息资源进行聚合，通过统一的访问入口，提供一个支持信息访问、传递、以及协作的集成化环境，实现个性化业务应用的高效开发、集成、部署与管理；并根据每个用户的特点、喜好和角色的不同，为管理用户提供量身定做的访问关键业务信息的安全通道和个性化应用界面，使其可以浏览到相互关联的数据，进行相关的事务处理。同时应用支撑平台起到同步几个应用系统，避免信息孤岛的关键角色。

8.6.2.1. 统一用户管理服务（SAAS 基础服务）

“统一用户管理服务”是智慧消防云平台 SAAS 应用模式的基础服务之一。

统一用户管理模块是对系统所涉及的单位、人员以及单位和人员之间的关系进行管理，实现单位和人员的层次关系、隶属关系、相关岗位的定义，实现用户身份的认证功能，实现一人多岗、权限及业务职能的继承关系。

8.6.2.1.1. 人员管理

管理维护人员的基本信息、详细信息、登录信息。其中系统要有支持一个用户多账号登录的功能。

8.6.2.1.2. 机构管理

管理维护单位部门的基本信息。包含组的维护，组类型至少要有：成员组、领导组、工作人员组。

8.6.2.1.3. 机构列表与业务关联功能

可以从机构人员树中查看任何单位的人员列表。通过相关的权限查看单位各级别机构的人员的信息。机构人员树可以为所有业务模块提供人员、单位的隶属信息。

8.6.2.1.4. 临时组织机构维护

为了完成某一项临时性的工作，需要成立临时性的部门，系统应该支持对于临时部门的维护、授权、管理。

8.6.2.1.5. 支持机构的管理

把机构作为统一隶属树来管理，并可以设置当前使用单位。

8.6.2.1.6. 机构人员资料变更

一个机构人员可能因为升迁调动等变更，资料的变更包括用户的基本信息、登录信息、其他详细信息，该机构人员相应的权限信息也需要进行调整。

8.6.2.1.7. 机构人员维护树

体现机构的层次关系，把人员定位到机构的每个职务上，通过职务建立人员与机构的关系。单位的关系可以用行政级别的关系来描述实现，人员的关系可以建立领导和工作人员之间的关系。机构人员树满足如下要求：

（1）一个人可以担任多个职务。任何一个用户都可以被设置属于多个部门或者组别。在用户内部可能有部分人员身兼数职。

（2）一个人代替另一个人的职务，则该人具有原来人的所有权限或部分权限。

（3）领导组为成员组的领导。

（4）机构人员可以复制、粘贴。

（5）使用过的机构要适当处理，关联的数据仍可以正确关联。

（6）机构人员树中的人员有在职、离职、离岗三种状态，离岗表示还会回来任职，只是在离岗期间不能登录系统。

（7）人员变更时，应有人员变更记录。

（8）机构人员维护需要有日志记录。

（9）在调用机构人员树时，不显示的人员与单位不能出现，同时要根据不同的

要求，显示不同级别的机构或人员。

（10）支持多单位的机构人员树管理。

8.6.2.1.8. 与其他业务系统关联

（1）提供给其他所有系统的用户登录认证接口。

（2）提供给其他所有系统的机构人员树选择接口。

8.6.2.2. 统一角色权限管理服务（SAAS 基础服务）

“统一角色权限管理服务”是智慧消防云平台 SAAS 应用模式的基础服务之一，和“统一用户管理服务”共同组成整个智慧消防 SAAS 云平台全省分布式应用租赁服务的基础要素。

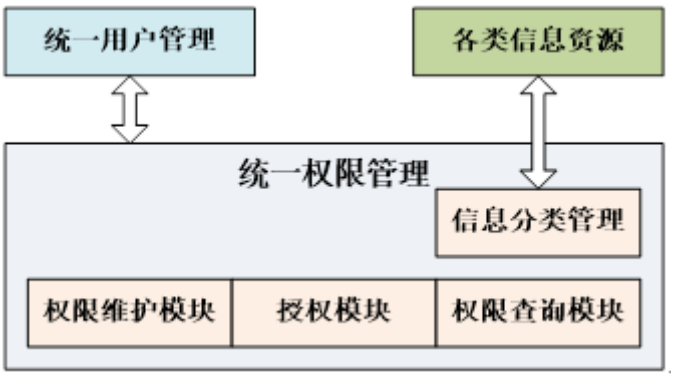
基于角色的访问控制方法的思想就是把对用户的授权分成两部分，用角色来充当用户行使权限的中介。这样，用户与角色之间以及角色与权限之间就形成了两个多对多的关系。系统提供角色定义功能允许用户根据自己的需要（职权、职位以及分担的权利和责任）定义相应的角色。

角色是一组访问权限的集合，一个用户可以是很多角色的成员，一个角色也可以有很多个权限，而一个权限也可以重复配置于多个角色。权限配置工作是组织角色的权限的工作步骤之一，只有角色具有相应的权限后角色分配才能具有实际意义。

利用角色作为平台访问权限分配的中介，作用就是把相关权限集合授予一个或多个用户，其优点是有利于灵活适应用户的变更和进行使用权限的分配调整，但如果临时需要为某个人分配指定的功能权限，就必须先建立一个角色，再为角色配置功能权限，最后还要把角色分配到某个人。反之，如果要收回权限的话，首先必须将角色从某用户上移除，再将这个角色进行删除操作。这样操作就显的比较繁琐，对角色管理也带来了混乱。所以，针对具体人员临时权限的分配，承建方在用户功能临时授权模块中进行实现。

统一权限管理包括两部分：访问控制、权限管理。实现对系统中的所有权限进行维护，并为系统的使用者设置相应的权限。由权限分配策略将信息分类和机构人

员有机挂接，实现对所有用户通过权限分配策略将所有信息有效控制起来。一个单位任何一项工作或全部工作(某一个或全部的信息对象)，均是根据该单位内部职责的分配与指定，由 1-N 个机构的 1-N 个人员在不同时间范围内完成并有多种可能的权限规定。这一权限策略分配体系是由权限分配策略树来穷尽描述。统一权限管理系统把统一用户管理系统与各类信息资源紧密的联系在一起，用户管理系统通过权限管理系统来实现对信息资源的访问控制，如下图所示：



图统一权限管理架构

8.6.2.2.1. 用户角色分类

在智慧消防云平台中，用户根据岗位、职责的不同，角色分类可划分为：

- 超级管理员：具有应用系统最高级别的权限，可进行任何业务操作和系统管理操作。
- 单位管理员：由超级管理员分配部分业务管理权限给单位内部的具体某个业务管理人员，可由其对本单位的其他普通用户进行账户设置、业务授权。
- 普通用户：仅具有应用系统中普通的业务操作权限，不具备管理权限。

8.6.2.2.2. 业务权限控制级别

根据用户在系统中的业务权限级别，具体划分如下：

- 登录权限。该权限为用户的基本权限，也是先决权限，不具备该权限的用户就不具备后续级别的权限分配资格。

- 模块权限。该权限为基本业务功能模块权限，模块权限的分配直接影响到用户的业务模块可视性。
- 操作权限。该权限级别又可划分为：模块操作权限、表单操作权限。模块操作权限的分配与否决定了用户能否进行数据列表操作；表单操作权限决定了用户在打开单条数据记录后能否进行字段数据操作。
- 流程权限。在上述的表单操作权限中，又嵌入了流程权限，若在流程环节的人员参数配置中未配置对应的用户，则在业务的流转过程中，该用户就不具备接收流转数据的权限。

8.6.2.2.3. 用户角色与权限关系

应用信息系统中对用户操作权限的控制是通过建立一套角色与权限对应关系，对用户账号授予某个角色或多个角色的组合来实现的，一个角色对应一定的权限（即应用信息系统中允许操作某功能点或功能点集合的权力），一个用户账号可通过被授予多个角色而获得多种操作权限。

8.6.2.2.4. 系统及业务权限分配设计

本系统将根据每个用户的岗位、职责、职务等要素进行统一的权限划分与分配控制，确保每个用户具备精确的业务操作权限，做到用户在系统内的权责分明。

序号	权限类别	权限名称	分配对象
1	系统权限	数据存取	系统
2		系统运行	系统
3	管理权限	部门管理	超级管理员
4		用户管理	超级管理员、分级管理员
5		角色分配与授权	超级管理员、分级管理员
6		流程配置	超级管理员、分级管理员

7		字典管理	超级管理员
8		系统运行参数配置	超级管理员
9		文件系统管理	超级管理员
10		短信参数配置	超级管理员
11		短信提醒人员配置	超级管理员、分级管理员
12		日志管理	超级管理员

按照角色类型名称划分，主要的系统业务权限分类包括：

序号	角色名称	权限描述
1	普通用户	所有用户的基础权限
2	查看所有文件信息权限	该权限具有查询、删除所有文件的权限，请慎重分配给用户。
3	文件新建权限	该权限可根据需要同时分配给“普通用户”。
4	文件审核审批权限	该权限可根据需要同时分配给“普通用户”，例如 分配给单位一级领导、二级领导，以及其它部门领导主管。
5	消息系统权限	该权限可根据需要同时分配给“普通用户”。
6	分级管理员权限	由系统超级管理员将系统管理权限分配给每个部门的“分级管理员”

8.6.2.2.5. 与其他业务系统关联

（1）为其他系统授权提供授权接口。

（2）为其他系统权限判断提供接口。

8.6.2.3. 中台应用支撑体系

8.6.2.3.1. 业务中台

实现 SAAS 模式下的租户（各级市、县和行业）自定义应用、菜单和鉴权。实现

各个租户的不同应用的数据相互独立又相互关联。

8.6.2.3.2. 技术中台

实现 SAAS 租户的各个应用的元数据的在线设计，包含了表单、菜单、视图、查询功能、流程节点功能函数、按钮功能函数和权限等。实现 SAAS 应用的数据管理、代码在线编辑、在线调试等功能，以方便实现快速搭建应用系统功能，尽量做到无码开发和快速修改和调整业务流程和代码。

8.6.2.3.3. 数据中台

省级智慧消防平台的基础数据、复合数据、数据模型、数据视图、数据存储。以及对内部应用系统和外部应用系统提供各种数据服务。

8.6.2.4. 权限认证体系

权限认证体系，主要包含了用户访问权限、数据存储权限、数据传输权限、加解密权限等多个方面的权限安全体系认证。

其中，身份认证是系统平台对外部访问者进行身份识别的最重要环节，身份权限认证，主要包括了用户密码权限、用户唯一身份码权限、通讯号码验证权限认证、设备唯一码权限认证等。

系统提供足够灵活，可配置的权限管理功能，对用户的系统访问权限进行控制，确保系统和数据的安全。通过权限管理功能，管理员可便捷地授予/收回账户相应的角色或权限。

8.6.2.5. 平台安全组件接入

平台的安全组件体系，主要包括软件安全组件体系、硬件安全组件体系。其中，软件安全组件体系，除了平台自身的安全保障外，还需要通过安装第三方的安全软件组件来保障系统业务层和数据层的安全。另外，在硬件安全组件体系方面，需要通过平台所部署的硬件环境、网络环境等已安装部署的硬件设备来确保网络链路、

底层硬件存储等方面传输和存储安全。

大多数信息化应用有三个基本安全需求。首先，它们要能够认证一个访问者；其次，它们需要有能力对 Web 请求提供安全保证；第三，它们需要有能力对访问者提供安全保证。

安全涉及到两个不同的概念，认证和授权。前者是关于确认用户是否确实是他们所宣称的身份。授权则是关于确认用户是否有允许执行一个特定的操作。

8.6.2.6. 附件管理

平台软件系统运行过程中，除了一些基本的元数据、关系数据或其它数据流外，还涉及到一些物理文件的上传使用，因此对于附件管理，需要提供传输速率高、上传过程稳定、文件保存稳定等一系列功能。

在平台使用过程中，附件上传与下载是系统功能的一个重要组成部分，由于智慧消防平台的网站系统对安全性的要求比较高。上传的附件有一定的格式限制，只上传如 DOC、PPT、PDF、XLS、JPG、BMP 等，上传格式可以管理，不属于上传格式的，不许上传，并且可支持上传多附件形式。

另外，通常情况下，附件文件所占空间较大，在附件的存取过程中，需要耗费较长时间。为避免附件存取过程中长时间占用服务器资源，因此需要单独部署附件管理服务（可单独部署于附件服务器），区分进程服务管理，提高平台整体访问和使用性能。

8.6.2.7. 消息管理体系

消息管理体系，主要用来建立平台对内、对外的消息传播体系，实现平台运行情况的提醒、平台交互过程的消息提醒，使平台的使用者、维护者能够快速收到系统消息，便于对系统进行运行保障和业务操作。

消息管理体系的主要功能包括如下几项：

- 邮件消息：邮件消息方式，只需要配置相应的邮件信息，当有消息产生时，会自动发送消息邮件给邮件接收者。

- 短信消息：实现了邮件消息方式，只需要配置相应的接收人信息，当有消息产生时，会自动发送消息短信给接收者。
- 消息配置：消息的规则、时段、信息、方式等相关消息信息配置的设定。

8.6.2.8. 系统运行参数设置

系统运行参数设置，主要包括系统运行过程所需要的一些运行标准值、阈值、范围值、目录路径、地址参数、多字典参数、模板参数等。

通过系统运行参数设置，可保障系统的基础应用功能支撑和基础业务运行条件。

通过修改系统运行参数值，可改变系统运行目标或系统运行性能。

另外，还可设置系统的一些基本参数，包括上传文件格式限制、敏感字。

8.6.2.9. 多类型信息全文检索

在本次项目建设中，因建设有消防数据中心系统，平台将有大量消防基础数据和平台各系统运行产生的业务数据。因此，建立一套完善的数据检索机制是非常重要的。针对存放于多个不同类型数据表、不同数据格式/文件格式的数据而言，要获取一项查询业务的综合全面数据，就必须通过“全文检索”功能来完成。

全文检索系统的实现技术分为三个方面：关系型全文检索系统、层次型全文检索系统、面向对象的全文检索系统及自动标引技术。

针对全文数据系统的构建，要通过多维度（时间轴、空间区域、属性特性、归属对象单元、存储位置等）进行综合设计，并提出全文检索系统的实现技术，主要分为 5 个步骤。

（1）数据准备：它是指针对计划加载到全文数据库中的数据进行收集、整理、归类等预先处理的过程。加载到全文数据中的数据可以从多种途径获得，常见的数据来源有：电脑打字产生的文件，电子印刷产生的文稿，计算机网上传输的文件，电子出版物，图文处理产生的文件，专门组织人力录入建库。

（2）文本预处理：包括规范格式，当格式多种多样时，应加以整理，使文献的格式规范化；批式标引，文本预处理阶段完成的批式标引，不受全文数据库结构

的限制，效率较高。

（3）数据加载：数据准备好以后，便可以加载（拷入、输入）到数据库文件中去了。加载数据可有单篇方式或批量方式。单篇方式一次加载一篇，适于平时文献随时加载的情况。批量方式一次加载多篇，适于集中大量加载的情况。

（4）数据检索：数据库建立起来之后，便可根据全文检索系统提供的检索功能对数据库进行检索。

（5）数据维护：全文数据建立以后，需要经常对数据库的内容进行索引、更新、追加和清理。

8.7. 区块链应用体系建设

针对省级智慧消防云平台的“总—分”式部署架构，为保障省级平台数据中心与各市、县级感知网分中心数据的同步性、一致性、安全性，可引入区块链应用技术实现省、市、县三级物联感知监测数据、火灾风险隐患与火情分析数据的多中心化数据安全管理。

8.7.1. 区块链概述

区块链技术作为新兴的互联网技术，可作为将来消防物联网大数据体系下的一项数据唯一性和权威性认定与标记的应用。

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。简单来讲，在区块链系统中，每过一段时间，各参与主体产生的交易数据会被打包成一个数据区块，数据区块按照时间顺序依次排列，形成数据区块的链条，各参与主体拥有同样的数据链条，且无法单方面篡改，任何信息的修改只有经过约定比例的主体同意方可进行，并且只能添加新的信息，无法删除或修改旧的信息，从而实现多主体间的信息共享和一致决策。区块链技术具有如下优点：

1．信息不可认篡改

一旦信息经过验证并添加至区块链，就会永久存储起来，单个节点上对数据的

修改是无效的，因此区块链的数据稳定性和可靠性极高，具有不可变性，即写入的数据将“永久”抗干扰。区块链的不可修改/防止篡改通过拜占庭共识算法实现，能够抵抗任何恶意攻击。

2．极强的保密性

匿名性：数据交互是无需信任的，交易双方无须通过公开身份的方式让对方对自己产生信任。

交易数据隐藏：用户可以根据他们的需要选择合适的加密技术加密交易数据。通过隐藏地址技术来保护接受方的数据，通过环签名和零知识证明等隐藏交易发起者和交易数据。

3．重塑信任机制

区块链基于协商一致的规范和协议，使得整个系统中的所有节点能够在去信任的环境自由安全的交换数据，使得对“人”的信任改成对机器的信任，任何人为的干预都不起作用。

4．区块链存证的法律效力

通过为电子操作提供不可抵赖的证据来减少法律纠纷，而且支持把收据、具有法律约束力的合同和认证信息都直接存储到数据库中。区块链存证的数据可以作为监管和责任划分的有力证据。

把区块链技术融入到智慧消防管理系统中，使消防全闭环监管无人为干扰，做到系统的科学与公正，提升系统公信力。

8.7.2. 技术特性

1．防御已知病毒（如勒索病毒）及未知病毒攻击。

2．抵御获得最高控制权的入侵者加载未知病毒、木马。

3．针对内部人员的非法操作，UEBA 技术可快速识别合法用户的异常操作。

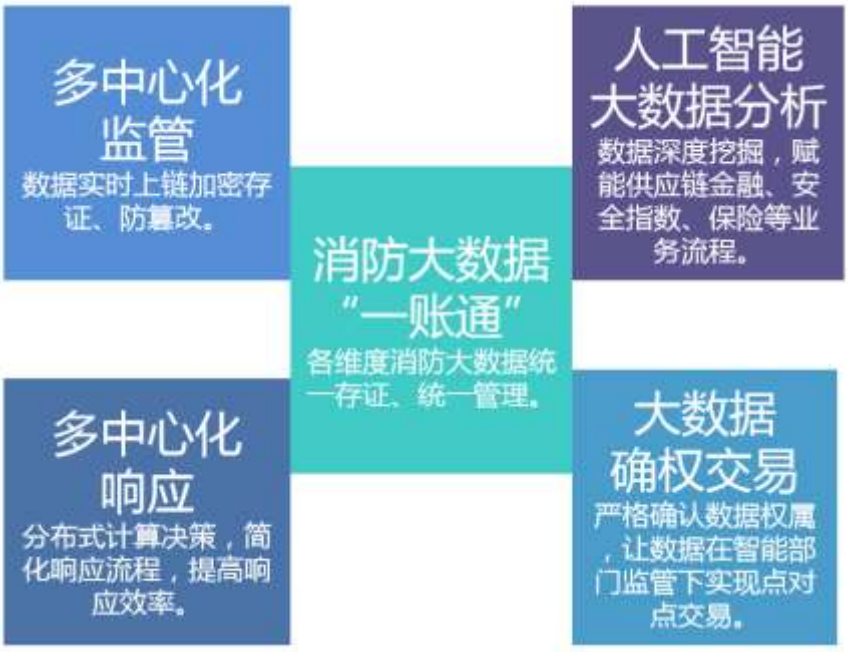
4．对于网络攻击，可运用 AI 预判网络攻击路径、告警阻断攻击，自动建立对抗安全防御策略。

5．对关键数据进行防篡改服务，并实现数据的存证、可追溯和防删除。

6．对被恶意篡改的网页数据文件，可进行毫秒级的自动恢复。

8.7.3. 功能架构

基于区块链技术构建的分布式消防大数据账本“一账通”，可以实现多中心化监管、多中心化响应，结合人工智能、大数据分析、智能合约技术，实现对保险、供应链金融、会员积分等各业务流程的赋能，并且实现大数据在监管之下进行交易。



消防大数据“一账通”：各维度消防大数据统一存证，统一管理

1．多中心化监管：数据实时上链加密存证、防篡改。

2．人工智能大数据分析：数据深度挖掘，赋能供应链金融、安全指数、保险等业务流程。

3．多中心化响应：分布式计算决策，简化响应流程，提高响应效率。

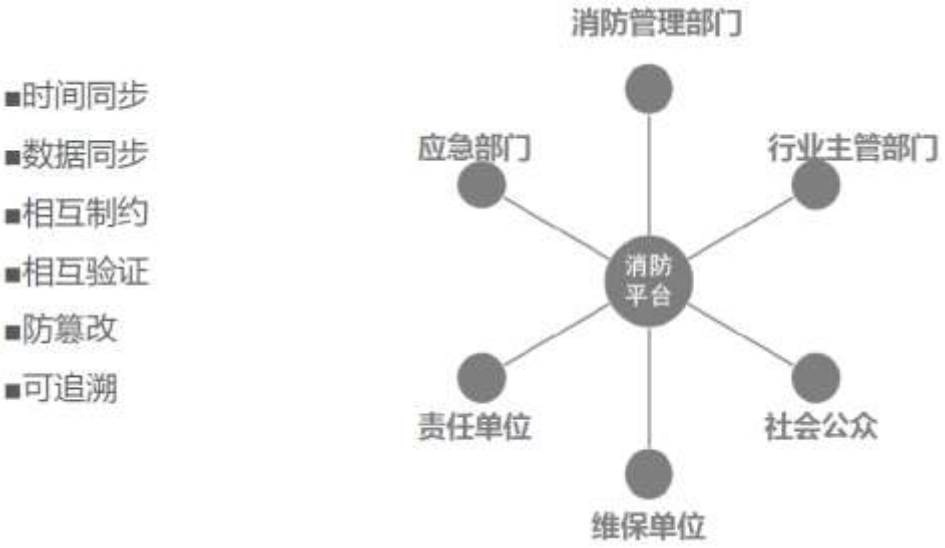
4．大数据确权交易：严格确认数据权属，让数据在职能部门监管下实现点对点交易。

8.7.3.1. 分布式账本“一账通”

建立消防大数据分布式账本“一账通”，坚持共同记账，共同维护，相互监督的原则，各维度消防数据实时同步，共同存证，具有真实客观、防篡改、可追溯的特性。

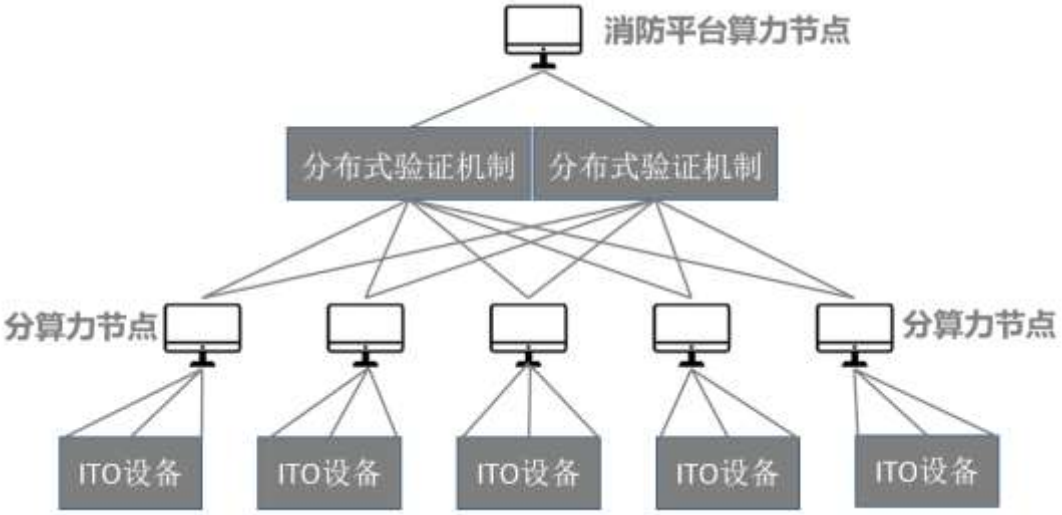
8.7.3.2. 多中心化监管

每个运算中心都是区块链节点，关键数据第一时间上链，实现消防大数据的防篡改处理，从而如实、及时反应各处消防安全状况。



8.7.3.3. 多中心化响应

每个运算中心都可作为应急响应中心，利用智能合约技术确保应急响应流程真实有效不被篡改，运用分布式计算，提高响应效率，第一时间处理危急情况，分算力中心可以是应急部门、消防管理单位、责任单位等主体。



8.7.3.4. 人工智能、大数据分析

“一账通”实现了消防大数据的互联互通，结合 UEBA 人工智能以及大数据分析技术，对责任单位、维保单位及其他相关主体进行科学客观的信用评审、风险评测以及资质审查，全面赋能保险业务流程以及供应链金融业务流程，赋能各单位安全指数的形成。

8.7.3.5. 多场景智能合约

金融增值服务：基于消防平台基础链存证的真实消防大数据，运用供应链金融智能合约、保险服务智能合约，安全指数智能合约，为用户提供相应的资质审查、信用审核、风险评估等服务。

（1）保险服务智能合约：

借助智能合约提供的真实可信的用户（责任单位）安全大数据分析，方便保险公司对企业进行风险评估，有利于用户降低保费支出，达成服务。

（2）供应链金融智能合约：

基于企业的消防大数据存证的供应链金融智能合约，可以向金融机构提供真实可靠的信用审查服务，资质信用链上审核，简便快捷。

（3）安全指数智能合约

基于人工智能评价和大数据分析形成的企业安全指数，可直观、客观地反映出该单位的安全等级，有利于责任单位加强自律、努力做到合法合规。

8.7.3.6. 消防大数据确权交易

金融增值服务：基于消防平台基础链存证的真实消防大数据，运用供应链金融智能合约、保险服务智能合约，安全指数智能合约，为用户提供相应的资质审查、信用审核、风险评估等服务。

（一）消防大数据确权交易增值服务

基于消防平台基础链存证的真实消防大数据，可以严格确认数据的所有权人，并在所有权人授权的情况下，进行可控的有偿使用。

1．整合消防大数据记录

打破健康数据孤岛，并在消防平台大数据账本“一账通”中管理自己所有的消防记录和消防大数据。

2．分享数据 ，获得补偿

数据即资产，资产可变现，如果消防大数据的所有权人同意分享一些消防大数据，提供给研究机构或消防相关机构等买家，可以获得相应的报酬。

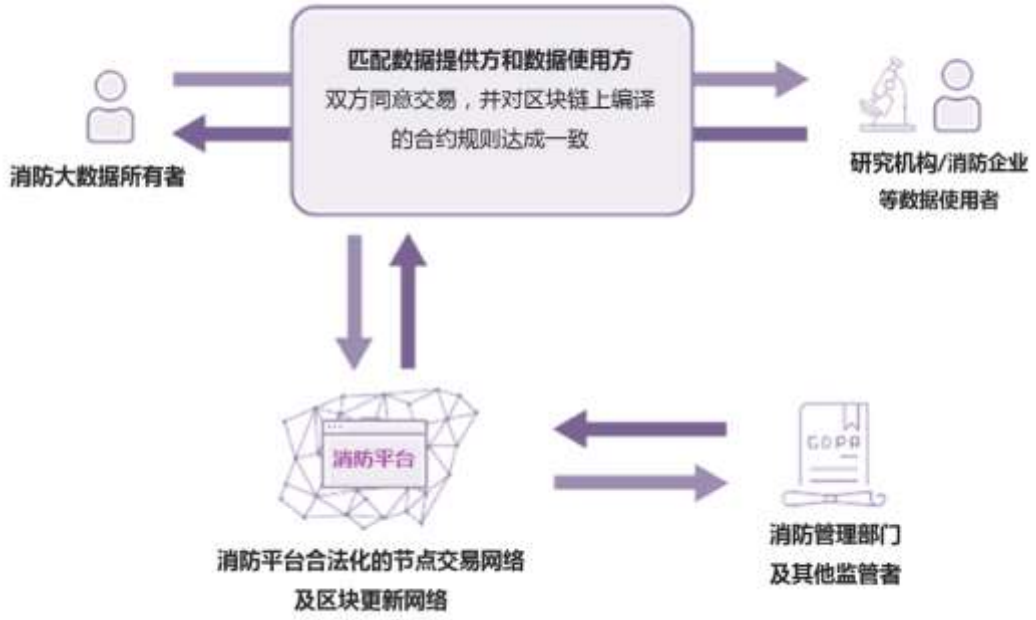
3．访问消防大数据

消防大数据提供者可以访问自己的完整的数据账本，以获得更好的管理和运维成效。

4．最前沿的隐私和安全性

使用基于区块链技术的消防管理平台， 用户可以拥有并完全控制自己的消防大数据， 让其进行安全的存储和经授权的交易。

（二）消防大数据交易体系：对于用户完全拥有所有权的消防数据资产(比如会员积分)， 消防平台的区块链网络允许用户进行点对点的交易，并同时接受相关部门的监管。

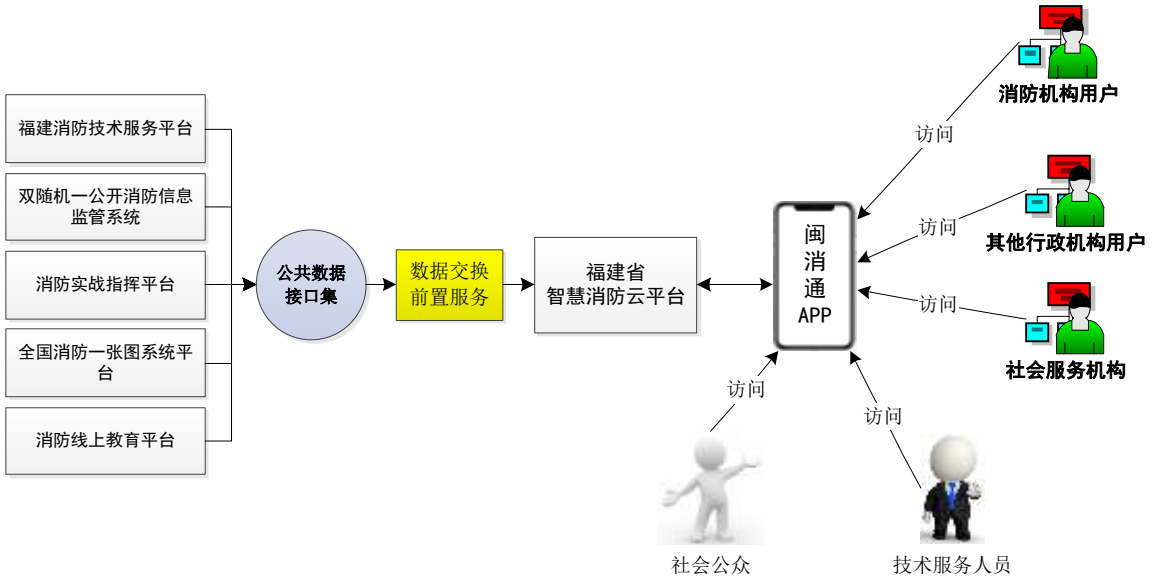


8.8. 手机 APP 建设（闽消通）

福建省智慧消防平台是面向全省消防业务的一个智慧型、综合性平台，为打造全省消防监管及服务业务的统一入口，可参照“闽政通”APP，打造一个属于全省消防领域的“闽消通”平台和 APP 应用。

8.8.1. 建设目的

建设“闽消通”APP 的目的，在于打通全省消防监管业务、消防服务业务、消防公众展示与监督业务等信息应用系统，将各种数据提交入口、数据展示窗口，统一通过一个面向消防全领域、全产业众多消防相关用户的手机 APP 应用通道，来完成各业务系统与业务处理结果受众之间的交互。



8.8.2. 用户对象

“闽消通 APP”的主要用户对象，包括：

1. 全省各级（省、市、县）消防救援机构用户
2. 全省各级非消防行政机构用户
3. 全省消防社会服务机构
4. 全省消防技术服务人员
5. 全省社会公众

所有用户对象使用“闽消通”APP 前，要以单位统一社会信用代码、个人身份证、手机号码等进行身份注册认证。

8.8.3. 监管功能

闽消通 APP 的主要监管功能，是面向消防救援机构、其他行政机构，主要功能包括：

1．消防安全预警通知

2．消防实战指挥信息查询

3．消防一张图综合查询与展示

4．消防监测数据、业务数据基础统计分析展示

5．消防大数据智能分析研判结果展示

6．消防服务机构&技术服务人员信息查询

8.8.4. 服务功能

1．监管信息（双随机、一公开）结果公开公示

2．消防网上办事大厅（入口）：包括资讯发布、结果公示、办事指南、法律法规、表格下载等。

3．网上咨询、网上投诉举报、结果反馈

4．在线宣传、在线教育

5．服务机构信息查询、技术服务人员信息查询

6.公共消防设施查询

8.9. 接口体系建设

8.9.1. 用户信息传输装置对接设计

省级智慧消防云平台中的“消防物联网远程监控系统”由省级统建，并分发至各支队、大队使用。消防物联网远程监控系统的物联网数据监测功能模块与用户信息传输装置（含无线手动火灾报警按钮、NB 无线水位水压监测、室外消防栓监控终端等，下同）之间的通信协议以 RFC 791、RFC 793 和 RFC 768 中规定的 TCP/IP 或 UDP/IP 网络控制协议作为底层通信承载协议，同时考虑到所有联网单位自身网络条件的网络有无、网络稳定性等情况不一，为保障数据传输的不间断性和稳定性，须同时采用 3G/4G/5G 移动网络通信协议作为底层通信承载协议。本部分定义的协议对应于 ISO/OSI 定义的七层协议结构的应用层。因此，不依赖于所选用的传输网络，在基础传输层已经建立的基础上，应用层通信协议与具体传输网络无关。

二者之间的通信方式主要包括控制命令、信息（火灾报警和建筑消防设施运行

状态等信息）上传和信息查询等，均采用发送/确认或请求/应答模式进行通信。

8.9.1.1. 设备产品执行标准（国标）

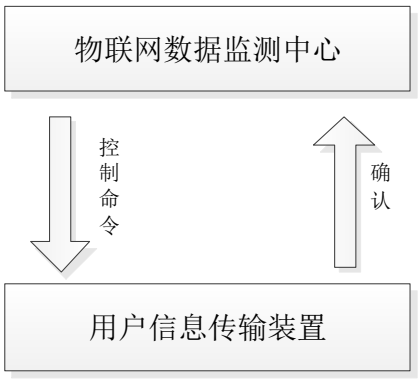
消防物联网用户信息传输装置所遵照执行的国家标准为：

GB 26875.1-2011《城市消防远程监控系统 第 1 部分：用户信息传输装置》

8.9.1.2. 通信协议

8.9.1.2.1. 控制命令

系统向用户信息传输装置发送指令时的控制命令采用发送/确认模式，通信流程如下图所示：



控制命令通信流程示意图

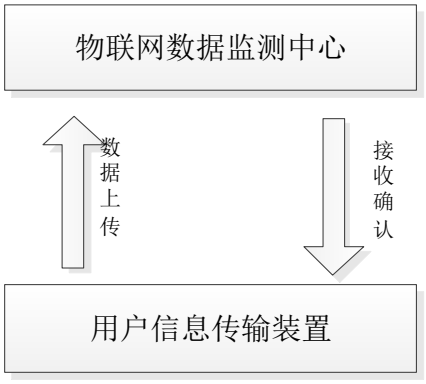
系统向用户信息传输装置发送控制命令，用户信息传输装置对接收到的命令信息进行校验。在校验正确的情况下，用户信息传输装置执行监控中心的控制命令，并向监控中心发送确认命令；在校验错误的情况下，用户信息传输装置舍弃所接收数据并发出否认回答。

系统接收到用户信息传输装置的确认命令后完成本次控制命令传输；系统在规定时间内未收到确认命令或收到否认回答后，启动重发机制。

8.9.1.2.2. 信息上传

用户信息传输装置向系统传输火灾报警和建筑消防设施运行状态等信息时采用

发送/确认模式。通信流程如下图所示：



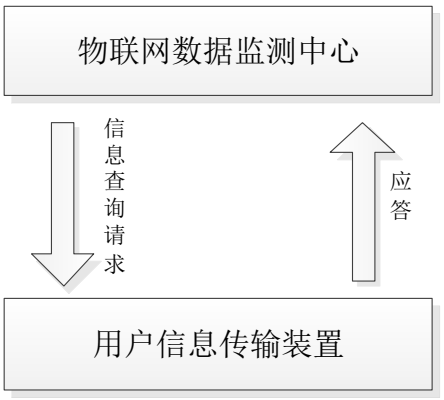
信息上传通信流程示意图

当发生火灾报警或运行状态改变时，用户信息传输装置主动向系统上传信息，系统对接收到的信息进行校验。在校验正确的情况下，系统对接收的信息进行相应处理，并向用户信息传输装置发送确认命令；在校验错误的情况下，系统舍弃所接收数据并发出否认回答。

用户信息传输装置接收到系统的确认命令后完成本次信息的传输；用户信息传输装置在规定时间内未收到确认命令或收到否认回答后，启动重发机制。

8.9.1.2.3. 信息查询

系统向用户信息传输装置查询相关信息时采用请求/应答模式。通信流程如下图所示：



信息查询通信流程示意图

系统向用户信息传输装置发送请求查询命令，用户信息传输装置对接收到的信息进行校验。在校验正确的情况下，用户信息传输装置根据请求内容进行应答；在

校验错误的情况下，用户信息传输装置舍弃所接收的数据并发出否认回答。

系统在接收到正确的应答信息后完成本次信息查询操作；在规定时间内未接收到应答信息、应答信息错误或接收到否认回答后，启动重发机制。

8.9.1.2.4. 重发机制

发送/确认模式下，发送端发出信息后在规定时间内未收到接收端的确认命令或收到否认回答，应进行信息重发，重发规定次数后仍未收到确认命令，则本次通信失败，结束本次通信。

请求/应答模式下，请求方在发出请求命令后的规定的时间内未收到应答信息或收到否认应答，重发请求命令，重发规定次数后仍未收到应答信息，则本次通信失败，结束本次通信。

通信过程中的校验错误包括校验和错误、不可识别的命令字节、应用数据单元长度超限、启动字符和结束字符错误等。

超时时间不宜大于 10s，可根据具体的通信方式和任务性质自行定义。

超时重发次数宜为 3 次，可根据具体的通信方式和任务性质自行定义。

8.9.1.2.5. 数据包结构

每个完整的数据包应由启动符、控制单元、应用数据单元、校验和、结束符组成，其中控制单元包含业务流水号、协议版本号、发送时间标签、源地址、目的地址、应用数据单元长度、命令字节，具体的结构和定义见下表：

表 数据包结构

定义		描述
启动符"@@" (2 字节)		数据包的第 1、2 字节，为固定值 64，64
控制单元	业务流水号 （2 字节）	数据包的第 3、4 字节。发送/确认模式下，业务流水号由发送端在发送新的数据包时按顺序加一，确认方按发送包的业务流水号返回；请求/应答模式下，业务流水号由请求端在发送新的请求命令时按顺序加一，应答方按请求包的业务流水号返回。低字节传输在前。业务流水号是一个 2 字节的正整数，由通信双方第一次建立网络连接

		时确定，初始值为 0.业务流水号由业务发起方（业务发起方指发送/确认模式下的发送端或者请求/应答模式下的请求端）独立管理，业务发起方负责业务流水号的分配和回收，保证在业务存续期间业务流水号的唯一性
	协议号 （2 字节）	协议版本号包含主版本号（第 5 字节）和用户版本号（第 6 字节）。主版本号为固定值 1，用户版本号由用户自行定义
	时间标签 （6 字节）	数据包的第 7~12 字节，为数据包发出的时间。
	源地址 （6 字节）	数据包的第 13~18 字节，为数据包的源地址（监控中心或用户信息传输装置地址）。低字节传输在前
	目的地址 （6 字节）	数据包的第 19~24 字节，为数据包的目的地址（监控中心或用户信息传输装置地址）.低字节传输在前
	应用数据单元长度 （2 字节）	数据包的第25、26字节，为应用数据单元的长度，长度不应大于1024；低字节传输在前
	命令字节 （1 字节）	数据包的第 27 字节，为控制单元的命令字节，具体定义见表 2
应用数据单元 （最大 1024 字节）		应用数据单元，基本格式见图 5，对于确认/否认等命令包，此单元可为空
校验和 （1 字节）		控制单元中各字节数据（第 3~27 字节）及应用数据单元的算术校验和，舍去 8 位以上的进位位后所形成的 1 字节二进制数
结束符“##” （2 字节）		为固定值 35，35

表 数据包结构续表

类型值	命令定义	命令说明
0	预留	
1	控制命令	时间同步
2	发送数据	发送火灾报警和建筑消防设施运行状态等信息
3	确认	对控制命令和发送信息的确认回答
4	请求	查询火灾报警和建筑消防设施运行状态等信息
5	应答	返回查询的信息
6	否认	对控制命令和发送信息的否认回答
7~127	预留	

128~255	用户自行定义	

8.9.1.3. 应用数据单元基本格式

应用数据单元基本格式如下表所示：

表 应用数据单位基本格式

数据单元表示符	类型标志	1 字节
	信息对象数目	1 字节
信息对象 1	信息体	根据类型不同长度不同
	时间标签 1a	6 字节
. . .		
信息对象 n	信息体 n	根据类型不同长度不同
	时间标签 nb	6 字节

a，b 对于某些特殊数据类型，此项可为空。

8.9.1.4. 数据定义

8.9.1.4.1. 数据单元标识符

类型标志为 1 字节二进制数，取值范围 0～255，类型标志见下表。 信息对象数目为 1 字节二进制数，其取值范围与数据包类型相关。

表 数据单元标识符

类型值	说明	方向
0	预留	上行
1	上传建筑消防设施系统状态	上行
2	上传建筑消防设施部件运行状态	上行
3	上传建筑消防设施部件模拟量值	上行
4	上传建筑消防设施操作信息	上行
5	上传建筑消防设施软件版本	上行
6	上传建筑消防设施系统配置情况	上行
7	上传建筑消防设施部件配置情况	上行
8	上传建筑消防没施系统时间	上行

9~20	预图（建筑消防设施信息）	上行
21	上传用户信息传验装置运行状态	上行
22	预留	上行
23	预留	上行
24	上传用户信息传输装置操作信息	上行
25	上传用户信息传输装置软件版本	上行
26	上传用户信息传输装置配置情况	上行
27	预留	上行
28	上传用户信息传输装量系统时间	上行
29~40	预留（用户信息传输装置信息）	上行
41~60	预留（控制信息）	上行
61	读建筑消防设施系统状态	下行
62	读建筑消防设施部件运行状态	下行
63	读建筑消防设施部件模拟量值	下行
64	读建筑消防设施操作信息	下行
65	读建筑消防设施软件版本	下行
66	读建筑消防设施系统配置情况	下行
67	读建筑消防设施部件配置情况	下行
68	读建筑消防设施系统时间	下行
69~80	预留	下行
81	读用户信息传输装置运行状态	下行
82	预留	下行
83	预留	下行
84	读用户信息传输装置操作信息记录	下行
85	读用户信息传输装置软件版本	下行
86	读用户信息传输装置配置情况	下行
87	预留	下行
88	读用户信息传输装置系统时间	下行
89	初始化用户信息传给装置	下行
90	同步用户信息传输装置时钟	下行
91	查岗命令	下行
92~127	预留	
128~254	用户自定义	

8.9.1.4.2. 信息对象

信息对象由信息体和时间标签组成。其中，信息体包括如下：

1、建筑消防设施系统状态

建筑消防设施系统状态数据结构如下图所示，共 4 字节。

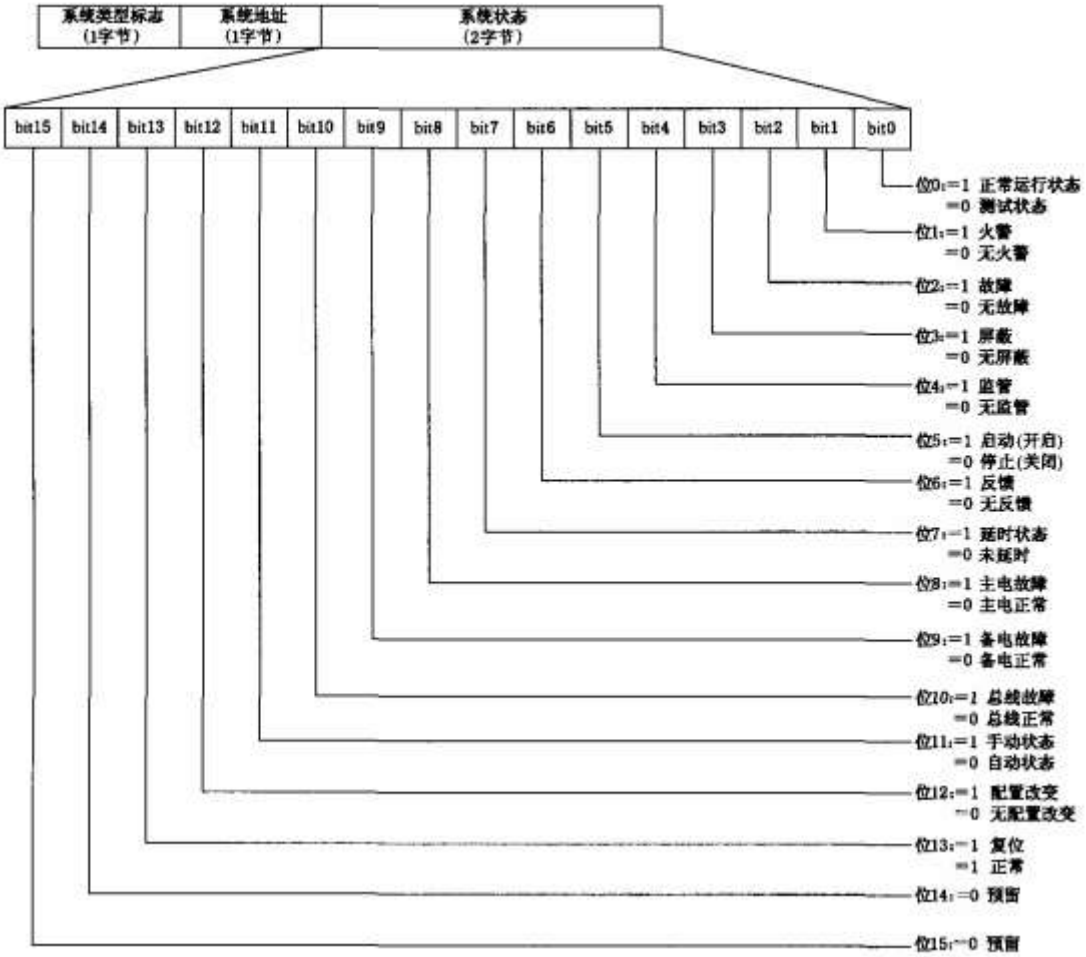


图 建筑消防设施状态数据结构图

系统类型标志符为 1 字节二进制数，取值范围 0～255，系统类型定义如下表所示。系统地址为 1 字节二进制数，取值范围 0～255，由建筑消防设施设定。系统状态数据为 2 字节，低字节传输在前。

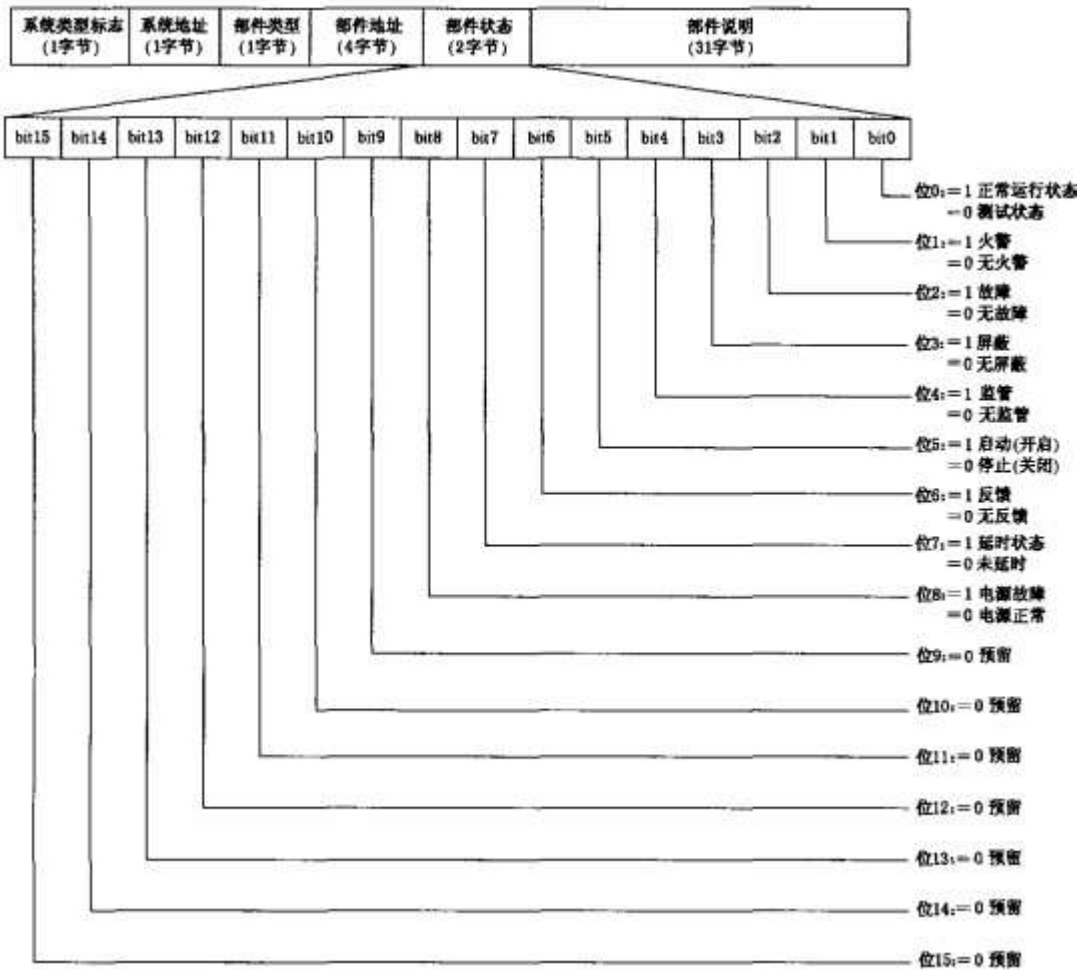
表 建筑消防设施系统状态系统类型定义

系统类型值	说明
0	通用
1	火灾报警系统
2~9	预留
10	消防联动控制器
11	消火栓系统
12	自动喷水灭火系统
13	气体灭火系统
14	水喷雾灭火系统（泵启动方式）

15	水喷雾灭火系统（压力容器启动方式）
16	滤沫灭火系统
17	干粉灭火系统
18	防排烟系统
19	防火门及卷帘系统
20	消防电梯
21	消防应急广播
22	消防应急照明和疏散指示系统
23	消防电源
24	消防电话
25~127	预留
128~255	用户自定义

2、建筑消防设施部件状态

建筑消防设施部件状态数据结构如下图所示，共 40 字节。



建筑消防设施系统类型标志、系统地址分别为 1 字节二进制数。建筑消防设施

部件类型标志符为 1 字节二进制数，定义下表。建筑消防设施部件地址为 4 字节二进制数，建筑消防设施部件状态数据为 2 字节，低字节先传输。建筑消防设施部件说明为 31 字节的字符串，采用 GB 18030-2005 规定的编码。

表 建筑消防设施部件状态系统类型

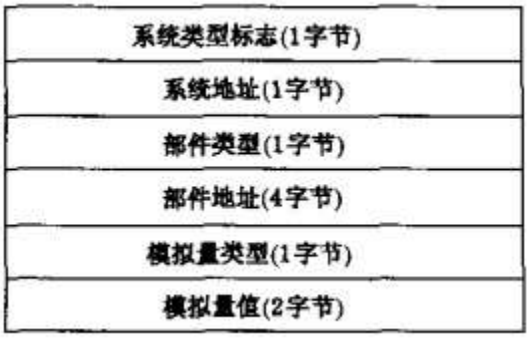
系统类型值	说明
0	通用
1	火灾报警控制器
2~9	预留
10	可燃气体探测器
11	点型可燃气体探测器
12	独立式可燃气体探测器
13	线型可燃气体探测器
14~15	预留
16	电气火灾监控报警器
17	剩余电流式电气火灾监控探测器
18	测温式电气火灾监控探测器
19~20	预留
21	探测回路
22	火灾显示盘
23	手动火灾报警按钮
24	消火栓按钮
25	火灾探测器
26~29	预留
30	感温火灾探测器
31	点型感温火灾探测器
32	点型感温火灾探测器（S 型）
33	点型感温火灾探测器（R 型）
34	线型感温火灾探测器
35	线型感温火灾探测器（S 型）
36	线型感温火灾探测器（R 型）
37	光纤感温火灾探测器
38	预留
39	预留
40	感烟火灾探测器
41	点型离子感烟火灾探测器
42	点型光电感烟火灾探测器
43	线型光束感烟火灾探测器
44	吸气式感烟火灾探测器

45~49	预留
50	复合式火灾探测器
51	复合式感烟感温火灾探测器
52	复合式感光感温火灾探测器
53	复合式感光感烟火灾探测器
54~59	预留
60	预留
61	紫外火焰探测器
62	红外火焰探测器
63~68	预留
69	感光火灾探测器
70~73	预留
74	气体探测器
75~77	预留
78	图像摄像方式火灾探测器
79	感声火灾探测器
80	预留
81	气体灭火控制器
82	消防电气控制装置
83	消防控制室图形显示装置
84	模块
85	输入模块
86	输出模块
87	输入/输出模块
88	中继模块
89~90	预留
91	消防水泵
92	消防水箱
93~94	预留
95	喷淋泵
96	水流指示器
97	信号阀
98	报警阀
99	压力开关
100	预留
101	阀驱动装置
102	防火门
103	防火阀
104	通风空调
105	泡沫液泵
106	管网电磁阀
107~110	预留

111	防烟排烟风机
112	预留
113	排烟防火阀
114	常闭送风口
115	排烟口
116	电控挡烟垂壁
117	防火卷帘控制器
118	防火门监控器
119~120	预留
121	警报装置
122~127	预留
128~255	用户自定义

3、建筑消防设施部件模拟量值

建筑消防设施部件模拟量值数据结构如下图所示，共 10 字节。



系统类型标志、系统地址、部件类型、部件地址的定义同 1。模拟量类型为 1 字节二进制数，取值范围 0～255。模拟量值为 2 字节有符号整型数，取值范围为－32768～+32767，低字节传输在前。模拟量类型和模拟量值的具体定义见下表。

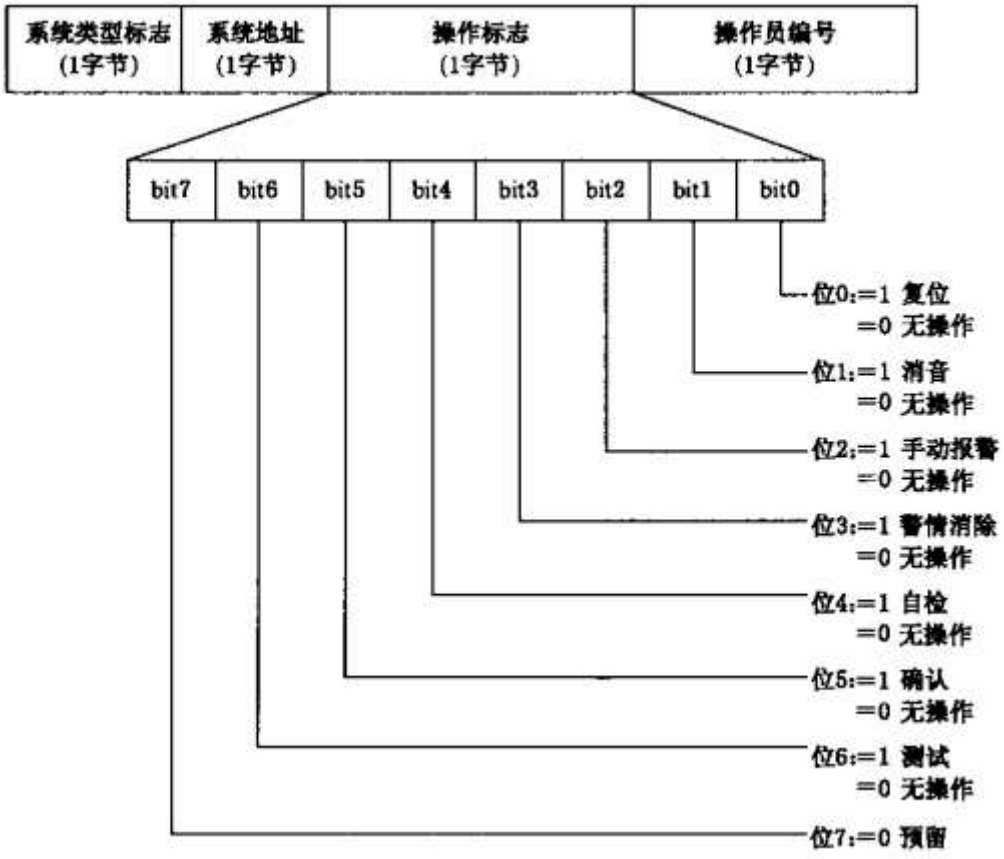
表 建筑消防设施部件模拟量系统类型

模拟量类型值	说明	单位	有效值范器	最小计量单元
0	未用			
1	事件计数	件	0~32000	1 件
2	高度	M	0~320	0.01m
3	温度	℃	-273~+3200	0.1℃
4	压力	Mpa	0~3200	0.1MPa
5	压力	Kpa	0~3200	0.1KPa
6	气体浓度	%LEL	0~100	0.1%LEL
7	时间	S	0~32000	1s
8	电压	V	0~3200	0.1V

9	电流	A	0~3200	0.1A
10	流量	L/s	0~3200	0.1L/s
11	风量	m^3/min	0~3200	o.1m^3/min
12	风速	m/s	0~20	1m/s
13~127	预留			
128~255	用户自定义			

4、建筑消防设施操作信息

建筑消防设施操作信息数据结构如下图所示，共 4 字节。



系统类型标志和系统地址的定义见 1。操作员编号为 1 字节二进制数，由建筑消防设施定义。

5、建筑消防设施软件版本

建筑消防设施的软件版本数据结构如下图所示，共 4 字节。系统类型标志和系统地址定义见 1。主版本号和次版本号分别为 1 字节二进制数，由建筑消防设施定义。

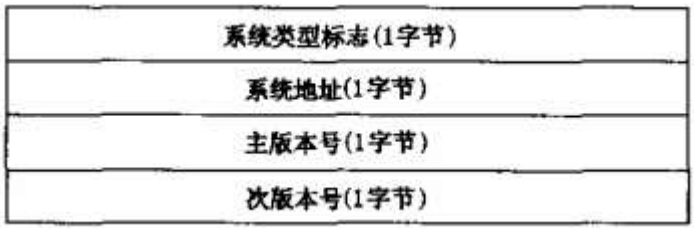


图 建筑消防设施软件版本数据结构图

6、建筑消防设施系统配置情况

建筑消防设施系统配置情况数据格式如下图所示，不定长。系统类型标志和系统地址定义见 1。系统配置说明部分为字符串，采用 GB 18030-2005 规定的编码。

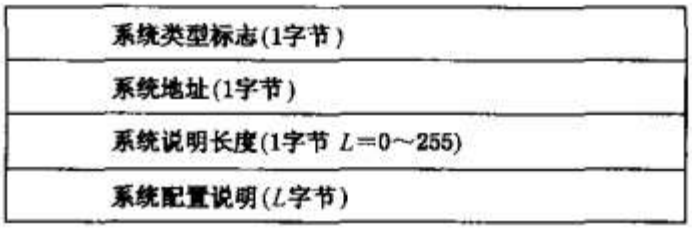


图 建筑消防设施系统配置数据结构图

7、建筑消防设施系统部件配置情况

建筑消防设施系统部件的配置情况数据格式如下图所示，共 38 字节。系统类型标志、系统地址、部件类型、部件地址定义见 2。 部件说明为 31 字节的字符串，采用 GB 18030-2005 规定的编码。

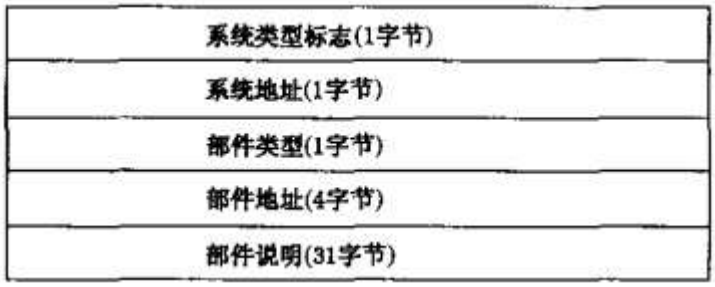


图 建筑消防设施系统部件配置数据结构图

8、用户信息传输装置运行状态

用户信息传输装置运行状态数据定义格式如下图所示，共 1 字节。

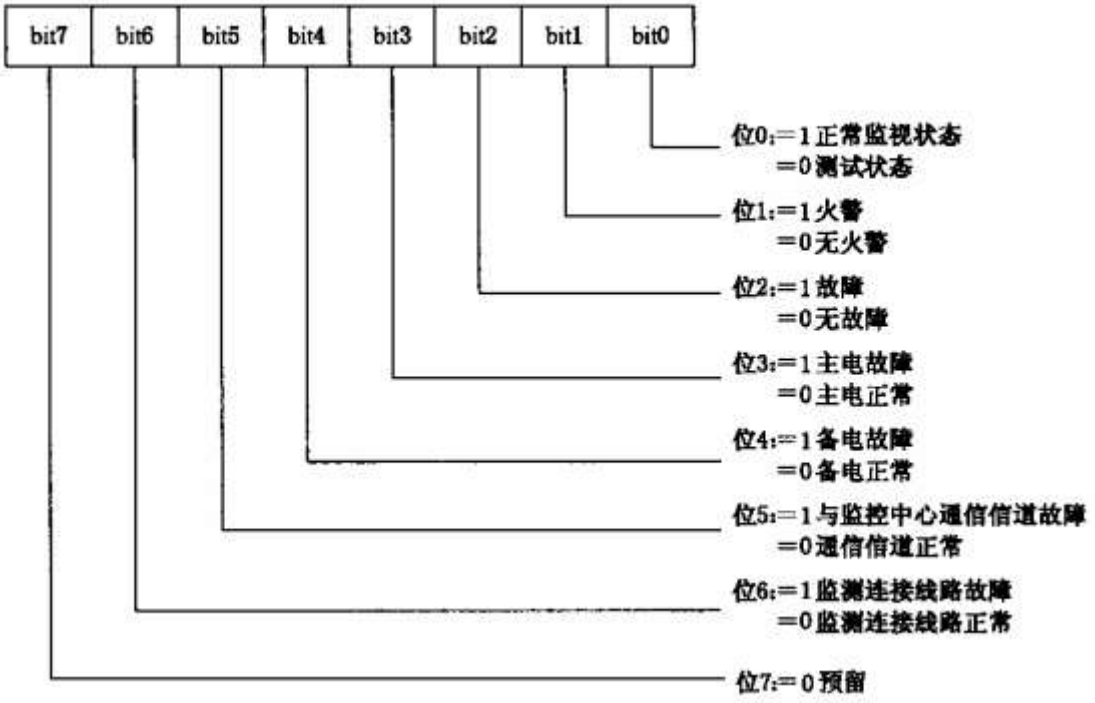


图 用户信息传输装置运行状态数据结构图

9、用户信息传输装置操作信息

用户信息传输装置操作信息数据结构如下图所示，共 2 字节。操作员编号为 1 字节二进制数，由联网用户定义。

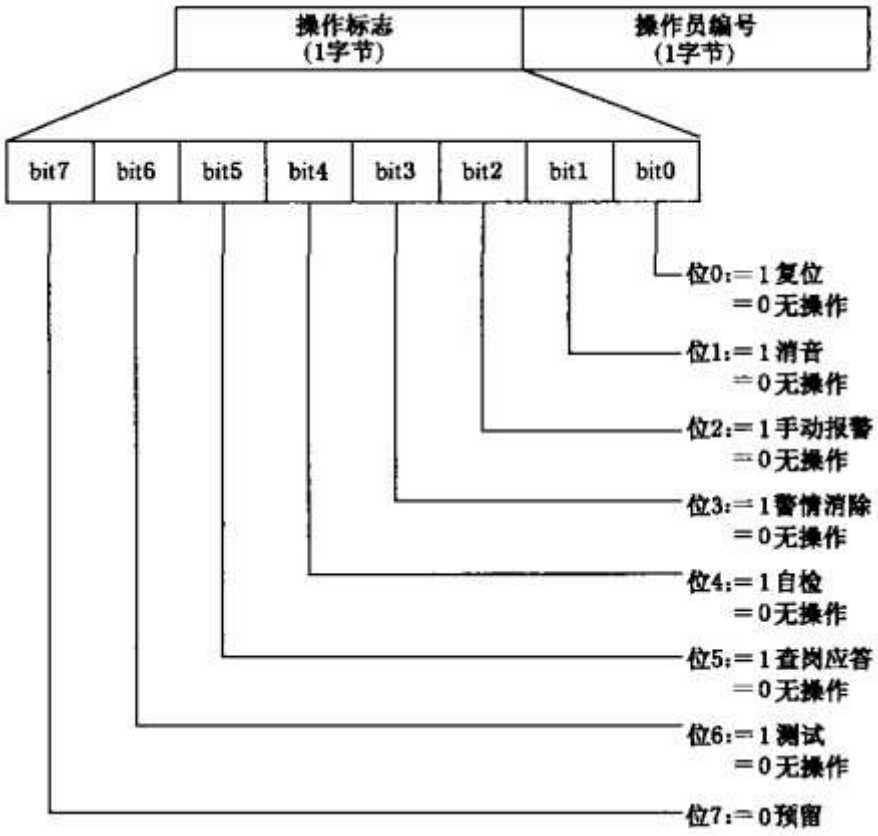


图 用户信息传输装置操作信息数据结构图

10、用户信息传输装置的软件版本

用户信息传输装置的软件版本数据结构如下图所示，共 2 字节。主版本号和次版本号分别为 1 字节二进制数，由制造商自行定义。

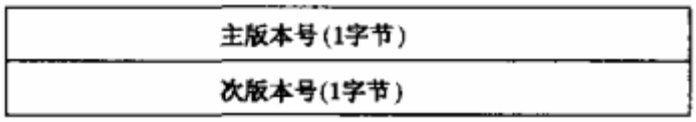


图 用户信息传输装置软件版本数据结构图

11、用户信息传输装置配置情况

用户信息传输装置的配置情况数据结构如下图所示，用户信息传输装置说明为不定长的字符串，采用 GB 18030-2005 规定的编码。

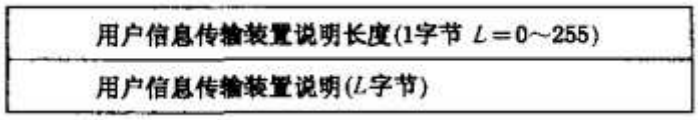


图 用户信息传输装置配置数据结构图

时间标签数据结构如下图：

秒	=0～59
分	=0～59
时	=0～23
日	=1～31
月	=1～12
年	=0～99

图 时间标签数据结构图

8.9.1.4.3. 上行方向数据定义细则

上行方向，即从用户信息传输装置到消防物联网远程监控系统的数据传输方向，数据定义细则如下：

1、上传建筑消防设施系统状态

上传建筑消防设施系统状态的数据格式如下图所示。

类型标志符(1字节)
信息对象数目(1字节)
系统类型1(1字节)
系统地址1(1字节)
系统状态1(2字节)
状态1发生时间(6字节)
系统类型n(1字节)
系统地址n(1字节)
系统状态n(2字节)
状态n发生时间(6字节)

图 上传建筑消防设施系统状态的数据格式图

2、上传建筑消防设施部件运行状态

上传建筑消防设施部件运行状态的数据格式如下图所示。

类型标志符(1字节)
信息对象数目(1字节)
系统类型1(1字节)
系统地址1(1字节)
部件类型1(1字节)
部件地址1(4字节)
部件状态1(2字节)
部件说明1(31字节)
状态1发生时间(6字节)
系统类型n(1字节)
系统地址n(1字节)
部件类型n(1字节)
部件地址n(4字节)
部件状态n(2字节)
部件说明n(31字节)
状态n发生时间(6字节)

图 上传建筑消防设施部件运行状态的数据格式图

3、上传建筑消防设施部件模拟量值

上传建筑消防设施部件模拟量值的数据格式如下图所示。

图 上传建筑消防设施部件模拟量值的数据格式图

4、上传建筑消防设施操作信息记录

上传建筑消防设施操作信息的数据格式如下图所示。

类型标志符(1字节)
信息对象数目(1字节)
系统类型1(1字节)
系统地址1(1字节)
操作信息1(1字节)
操作员编号1(1字节)
操作1的记录时间(6字节)
系统类型n(1字节)
系统地址n(1字节)
操作信息n(1字节)
操作员编号n(1字节)
操作n的记录时间(6字节)

图 上传建筑消防设施操作信息的数据格式图

5、上传建筑消防设施软件版本

上传建筑消防设施软件版本的数据格式如下图所示。

类型标志符(1字节)
信息对象数目(1字节)
系统类型(1字节)
系统地址(1字节)
软件主 版本号(1字节)
软件次版本号(1字节)

图 上传建筑消防设施软件版本的数据格式图

6、上传建筑消防设施系统配置情况

上传建筑消防设施系统配置情况的数据格式如下图所示。

图 上传建筑消防设施系统配置情况的数据格式图

7、上传建筑消防设施部件配置情况

上传建筑消防设施部件配置情况的数据格式如下图所示。

图 上传建筑消防设施部件配置的数据格式图

8、上传建筑消防设施系统时间

上传建筑消防设施系统时间的数据格式如下图所示。

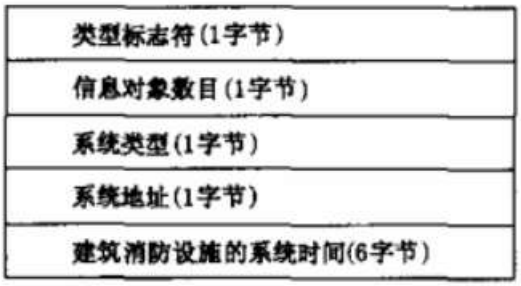


图 上传建筑消防设施系统时间的数据格式图

9、上传用户信息传输装置运行状态

上传用户信息传输装置运行状态的数据格式如下图所示。

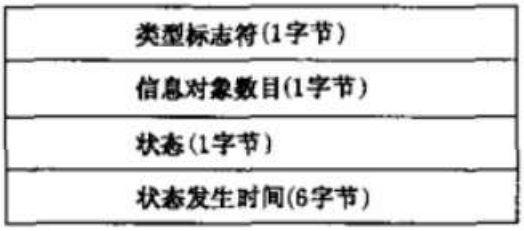


图 上传用户信息传输装置运行状态的数据格式图

10、上传用户信息传输装置操作信息记录

上传用户信息传输装置操作信息的数据格式如下图所示。

图 上传用户信息传输装置操作信息的数据格式图

11、上传用户信息传输装置软件版本

上传用户信息传输装置数据版本的数据格式如下图所示。

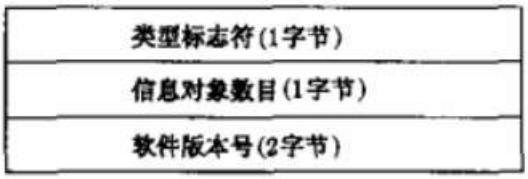


图 上传用户信息传输装置软件版本的数据格式图

12、上传用户信息传输装置配置情况

上传用户信息传输装置配置情况的数据格式如下图所示。

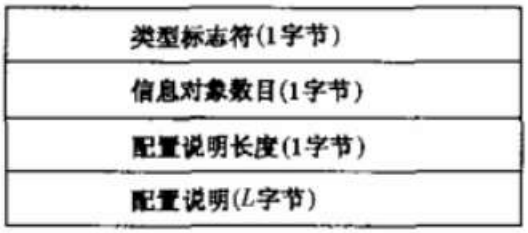


图 上传用户信息传输装置配置的数据格式图

13、上传用户信息传输装置系统时间

上传用户信息传输装置系统时间的数据格式如下图所示。

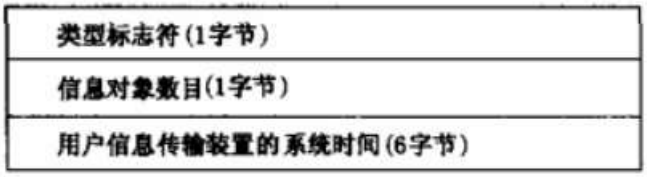


图 上传用户信息传输装置系统时间的数据格式图

8.9.1.4.4. 下行方向数据定义细则

下行方向，即从消防物联网远程监控系统到用户信息传输装置的数据传输方向，数据定义细则如下：

1、读建筑消防设施系统状态

读建筑消防设施系统状态的数据格式如下图所示。

图 读建筑消防设施系统状态的数据格式图

2、读建筑消防设施系统部件状态

读建筑消防设施系统部件状态的数据格式如下图所示

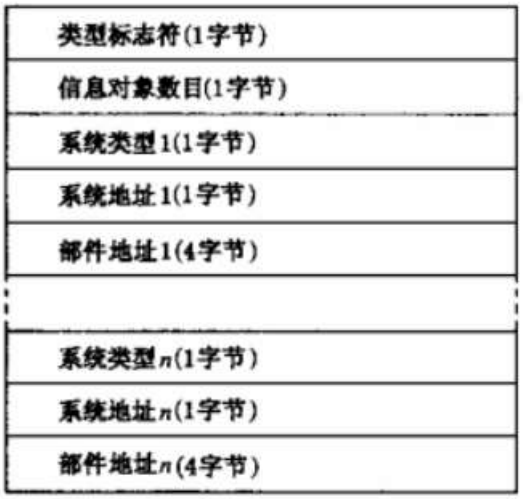


图 读建筑消防设施系统部件状态的数据格式图

3、读建筑消防设施部件模拟量值

读建筑消防设施部件模拟量值的数据格式如下图所示。

图 读建筑消防设施部件模拟量值的数据格式图

4、读建筑消防设施操作信息记录

监控中心请求用户信息传输装置传送建筑消防设施操作信息记录，并指定记录起始时间和记录数目。其数据格式如下图所示。

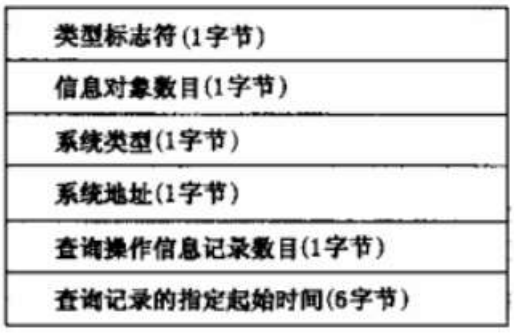


图　读建筑消防设施操作信息的数据格式图

5、读建筑消防设施软件版本

读建筑消防设施软件版本的数据格式如下图所示。

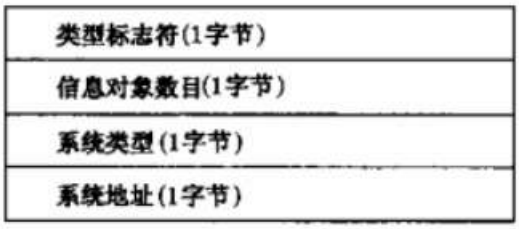


图　读建筑消防设施软件版本的数据格式图

6、读建筑消防设施系统配置情况

读建筑消防设施系统配置情况的数据格式如下图所示。

图　读建筑消防设施系统配置情况的数据格式图

7、读建筑消防设施部件配置情况

读建筑消防设施部件配置情况的数据格式如下图所示。

类型标志符(1字节)
信息对象数目(1字节)
系统类型1(1字节)
系统地址1(1字节)
部件地址1(4字节)
系统类型n(1字节)
系统地址n(1字节)
部件地址n(4字节)

图　读建筑消防设施部件配置的数据格式图

8、读建筑消防设施系统时间

读建筑消防设施系统时间的数据格式如下图所示

类型标志符(1字节)
信息对象数目(1字节)
系统类型(1字节)
系统地址(1字节)

图　读建筑消防设施系统时间的数据格式图

9、读用户信息传输装置运行状态

读用户信息传输装置运行状态的数据格式如下图所示。

类型标志符(1字节)
信息对象数目(1字节)
预留(1字节)

图　读用户信息传输装置运行状态的数据格式图

10、读用户信息传输装置操作信息记录

监控中心请求用户信息传输装置传送操作信息记录，并指定记录起始时间和信息数目。其数据格式如下图所示。

类型标志符(1字节)
信息对象数目(1字节)
查询操作信息记录数目(1字节)
查询记录的指定起始时间(6字节)

图　读用户信息传输装置操作信息的数据格式图

11、读用户信息传输装置软件版本

读用户信息传输装置软件版本的数据格式如下图所示。

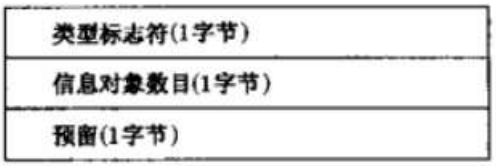


图　读用户信息传输装置软件版本的数据格式图

12、读用户信息传输装置配置情况

读用户信息传输装置配置情况的数据格式如下图所示。

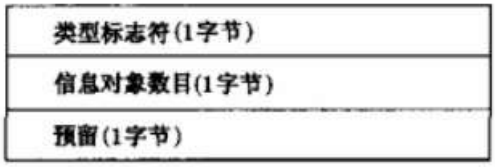


图　读用户信息传输装置配置的数据格式图

13、 读用户信息传输装置系统时间

读用户信息传输装置系统时间的数据格式如下图所示。

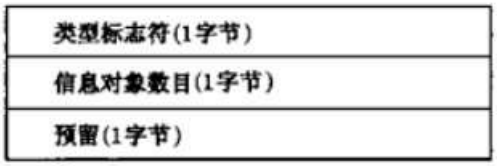


图　读用户信息传输装置系统时间的数据格式图

14、初始化用户信息传输装置

初始化用户信息传输装置的数据格式如下图所示。

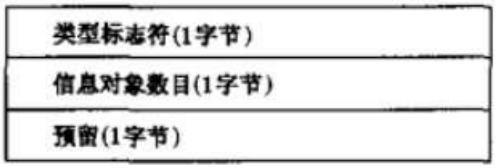


图 初始化用户信息传输装置的数据格式图

15、同步用户信息传输装置时间

同步用户信息传输装置时间的数据格式如下图所示。

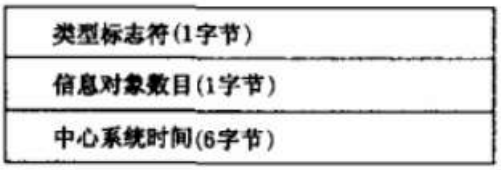


图　同步用户信息传输装置时间的数据格式图

16、查岗命令

监控中心向用户信息传输装置发送查岗命令的数据格式如下图所示。

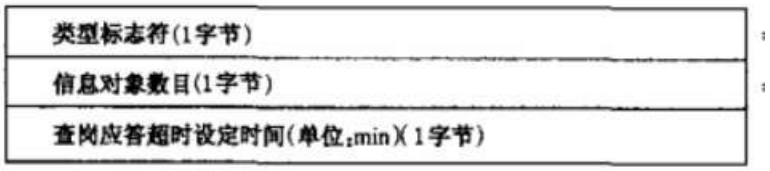


图 查岗命令的数据格式图

8.9.2. 消防物联网智能监测设备对接设计

除火灾风险单位标配使用的用户信息传输装置外，许多火灾风险单位楼宇内、市政设施、经消防安全改造的老旧小区等都有加装智能监测设备，例如智能烟感/温感设备、市政消火栓监测设备、用电监测设备等。

为确保各感知网分中心的物联监测设备顺利注册接入省级智慧消防平台，因此需要采集各种主流消防物联智能监测设备的通信传输协议，分类存储于省级平台中，并对各种通信传输协议进行封装，便于感知设备直接绑定、调用，设备持续接入时的免于二次接口开发对接。

智能监测设备通信传输协议的采集，要能覆盖市面上 90%以上的主流产品和小众产品，并能持续更新设备通信传输“协议库”。

8.9.3. 电子地图对接设计

8.9.3.1. 与政务电子地图对接

由于省级智慧消防云平台覆盖全省各级消防部门、各城市进行应用，因此，本次项目将与省、市、县政务电子地图（例如福州市时空信息公共服务平台，其它城市电子地图也可引入并对接）进行对接，获取基础电子地图服务信息。政务电子地

图提供了多种接口，本项目中使用到的接口有下列几种：

1．地图浏览 API

是一种通过 JavaScript（结合其他语言）将地图嵌入到网页的 API。该 API 提供了大量实用接口用以处理地图，并通过各种服务向地图添加内容，从而使用户能够在其网站上创建功能全面的地图应用程序。地图浏览 API 不仅包含构建地图的基本接口，还提供了诸如地图标绘等服务接口。

2．Web Map Service（网络地图服务）

简称 WMS，由开放地理信息联盟（Open GeoSpatial Consortium，OGC）制定。该规范定义了 Web 客户端从网络地图服务器获取地图的接口标准。一个 WMS 可以动态地生成具有地理参考数据的地图，这些地图通常用 GIF、JPEG 或 PNG 等图像格式，或者 SVG、KML、VML 和 WebCGM 等矢量图形格式来表现。使用者通过指定的参数获取相应的地图图片。WMS 实现规范由三个基础性操作协议(GetCapabilities，GetMap 和 GetFeatureInfo)组成，这些协议共同构成了利用 WMS 创建和叠加显示不同来源的远程异构地图服务的基础。

3．Web Map Tile Service（网络地图瓦片服务）

简称 WMTS，由开放地理信息联盟（Open GeoSpatial Consortium，OGC）制定，是和 WMS 并列的重要 OGC 规范之一。WMTS 不同于 WMS，它最重要的特征是采用缓存技术能够缓解 WebGIS 服务器端数据处理的压力，提高交互响应速度，大幅改善在线地图应用客户端的用户体验。WMTS 是 OGC 主推的缓存技术规范，是目前各种缓存技术相互兼容的一种方法。WMTS 服务支持 RESTful 访问，其接口包括 GetCapabilities、GetTile 和 GetFeatureInfo3 个操作，这些操作允许用户访问切片地图。

4．Web Feature Service（网络要素服务）

简称 WFS，由开放地理信息联盟（Open GeoSpatial Consortium，OGC）制定。该规范主要对 OpenGIS 简单要素的数据编辑操作进行规范，从而使服务器端和客户端能够在要素层面进行“通讯”。其返回结果的是 XML 格式的 WFS 服务元数据文档，通过该文档用户能够了解：WFS 服务器支持的所有操作列表，GetFeature 操作返回的数据格式，可用的坐标参照系统列表，操作异常信息的列表，WFS 服务提供商的相关信息，WFS 服务器的可用要素类列表等。WFS 服务接口规范定义了 GetCapabilities，DescribeFeatureType、GetFeature、Transaction、GetGmlObject 和 LockFeature

一共 6 种操作。其中，前三个 GetCapabilities，DescribeFeatureType 和 GetFeature 为必须实现的操作，也即只要实现了这三个操作的服务均可称为 WFS 服务。

5．地图标绘服务

是遵循 OGC 制定的 WPS 规范开发的功能服务接口。 地图标绘服务为用户提供在地图上添加、删除和移动 POI 及其相关信息的功能，允许用户收集自己关心区域的信息，标注到地图上，方便搜索和利用，满足个性化的需求。标注信息保存提供 2 种方式：上传至平台服务器或保存在客户端。

6．空间分析服务

包括叠加分析、缓冲区分析等，方便用户基于空间数据服务进行空间分析，发掘空间数据中隐含的知识信息，实现满足不同需求的增值服务，为辅助决策提供支持。同时此服务也实现了 OGC 制定的 WPS 规范接口。调用空间分析服务接口获得的响应数据默认以 Json 数据格式组织。空间分析服务目前实现叠加分析、缓冲区分析等空间分析服务。

8.9.3.2. 与互联网商业电子地图对接

与政务电子地图提供的服务基本相同，包括：地图浏览 API、网络地图服务、网络地图瓦片服务、网络要素服务、地图标绘服务、空间分析服务等。

由于政务电子地图的数据涉及范围较广，为城市整体结构和各层面的数据资源信息，具有一定程度的保密性或敏感性，因此其数据资源（如地图数据）面向互联网的开放度存在限制，以及随使用对象的不同而要求的地图数据精度也不同。因此，在面向互联网进行地图数据展示时，需要将政务电子地图信息通过规则算法转换为在互联网商业电子地图上展示的数据。

综合来说，省级智慧消防云平台在使用电子地图时，要根据系统软件使用对象（监管单位、被监管单位、运营单位等）来进行区分调用和对接开发。

8.9.4. 福建消防技术服务信息平台对接设计

福建省消防救援总队在运行的 “福建消防技术服务信息平台”包括维护保养检测机构基本信息、维护保养检测/评估项目信息、违法执业信息、机构黑名单信息等。由于平台软件的分管部门、技术架构、数据权限体系等均不同，因此省级智慧消防

云平台的各子平台、子系统要获取上述消防技术服务信息，须由省消防救援总队开放该技术服务平台的数据接口（如基于 WebService 的 HTTPS 协议接口），实时获取数据。

8.9.5. 与“闽政通”对接设计

8.9.5.1. 闽政通概述

福建省政务服务 APP 统一平台(闽政通 APP)于 2017 年 10 月 20 日上线试运行，整合全省各级政府部门面向公众和企业的服务资源，提供信息服务、办事服务和互动服务，并具有统一支付、统一身份认证功能。公众和企业可以随时随地获取所需服务，变“群众跑腿”为“掌上办事和信息跑路”，变“群众来回跑”为“部门协同办”。闽政通 APP 由福建省经济信息中心负责建设。

“闽政通”系统平台具有以下几项特点：

1．聚合省市两级政府门户网站最新文件、政策解读等政务信息，提供信息共享服务

2．对接全省 12345 政务服务平台，具有随手拍功能，提供互动监督服务

3．接入福建政务服务网（省网上办事大厅）行政审批、公共服务事项，整合政府及第三方可信便民服务事项，提供网上办事服务

4．对接财政非税支付缴费平台、多卡融合公共平台、微信支付和支付宝等多个渠道，提供统一支付服务

5．率先建设省级统一身份认证平台——福建省社会用户实名认证和授权平台，具备安全二维码、人像识别、eID 等多元认证能力，完成与福建政务服务网、福建公安公众服务网、掌上住建 APP、闽税通 APP、e 福州 APP 和 e 龙岩 APP 等政务平台用户体系交叉互认，实现用户信息的平台间共享、“一号通认”

8.9.5.2. “闽政通”资源对接

根据“闽政通”的应用特点，福建省智慧消防云平台与闽政通之间涉及的对接应用设计如下：

1. 基于福建省智慧消防云平台具有“互联网特性”的特点，而且属于智慧城市的一个重要组成部分，为体现其智慧性、城市性、互联网性等特点，在省级智慧消防平台的社会化应用方面，可引入闽政通的“省级统一身份认证平台——福建省社会用户实名认证和授权平台”，社会化用户可通过闽政通直接互联授权登录使用智慧消防云平台的相关应用功能。

2. 省级智慧消防云平台的相关火灾风险监测分析报告、消防安全宣传政策信息、消防教育培训信息、消防安全投诉举报信息反馈等，都可以通过闽政通作为中转渠道发布，或直接在闽政通发布。

8.9.6. 与指挥中心/实战指挥系统对接设计

省级智慧消防云平台建成后，其相应的监测采集数据、大数据智能分析结果数据，都可成为消防应急指挥救援的训练、实战过程等辅助决策分析依据。因此，可由指挥中心管理系统和实战指挥系统开放数据接口，实现数据传递。

目前省总队指挥中心系统和实战指挥系统处于升级改造过程中，待升级完成后提供完整的数据与应用接口。

8.9.7. 与全国消防一张图对接设计

8.9.7.1. 开放服务接口说明

消防一张图为消防的各个业务系统提供高比例尺、高精度的地图服务，整体上可以提供如下三类接口：

渲染引擎（JavaScript SDK）：轻量级的二维地图引擎，采用国内领先的 WebGL 渲染技术。主要包括以下接口：

1. 基础功能接口：提供电子地图的地图缩放、移动、前进、后退、复位等基础操作接口；测距、测面积等测量接口；鹰眼、比例尺、指北针等地图空间接口；坐标转换等接口。
2. 绘制功能接口：支持绘制点、线、面、矩形、扇形、多边形等接口。
3. 图层处理接口：基础数据、业务数据、几何图形、3D 图层等数据上图，以及数据聚合等接口。
4. 服务查询接口：支持 POI、行政区划、道路、路口、水系等数据的关键字查询、矩形查询、不规则区域查询、缓冲区查询等接口。
5. 轨迹服务接口：支持对象追踪、实时轨迹、历史轨迹、以及事件轨迹等上图及查询接口。
6. 路径规划接口：支持距离最短路径规划、添加途径点及避障区域等接口。
7. 数据可视化接口：提供热力图、关系图、台风轨迹等分析上图接口；
8. 覆盖物添加接口：支持添加标记、文本、信息窗体等接口；
9. 路况服务接口：支持添加实时路况、实时路况过滤等接口。

位置服务：地图服务端产品，提供了丰富的基础数据服务（POI, 水系，道路等）

强大的空间（缓冲区）分析，强大高效的展示方式（多样的聚合算法），实时轨迹，历史轨迹场景的接入。

1. 数据管理接口：提供数据的增删改等接口，建立基础数据与业务数据的关联接口等。
2. 查询接口主要包括：
   （1） 业务图层数据的查询接口；
   （2） POI、道路、路口等基础数据的搜索接口；
   （3） 行政区划相关的查询接口；
3. 图层数据删除接口；
4. 正逆地理编码转换接口；
5. 路径规划接口；
6. 坐标转换接口；

地图服务：提供矢量地图服务：采用矢量地图瓦片技术，通过图层叠加的方式进行矢量地图渲染，大大减少了数 据的传输量及服务器压力，方便进行不同风格的地图样式渲染，支持地图无极缩放功能。主要包含以下特性：

1. 高性能、高可用

通过分布式集群、多层次缓存等方案，提高系统容错和负载平衡能力，为用户提供高性能、高稳定性、高可靠性的地图服务器。同时配合矢量配套平台，让地图样式可配置，可修改，打造属于消防的专业风格地图。

2. 遵循标准、开放兼容

是一个开放的 GIS 服务器，在支持 OGC 标准的基础上，能够对接多种第三方服务，实现服务的获取与聚合。

3. 支持多场景适配

根据不同的硬件配置与地图显示需求，为 PC 端、大屏可视化等提供不同应用场景的地图服务，从地图性能与可视化效果为用户定制快速、美观的地图体验。

4. 数据安全性高

通过完善的地图服务鉴权与数据加密机制，有效防止数据爬取，保证数据安全。

具体地图接口详见《附件 3-2 全国消防一张图服务接口标准》文档。

8.9.7.2. 图层字段概要说明

消防灾情图层：灾情名称、地点、类型、等级、出动、时间、死伤情况、过火面积、消防机构等，并制作成消防灾情图层等。

高层建筑图层：建筑地址、建筑结构、建筑高度、建筑层数、建筑面积、耐火等级、外保温、负责人、建成日期、消防机构。

地下建筑图层：建筑结构、建筑高度、建筑层数、建筑面积、耐火等级、外保温、负责人、建成日期、消防机构等。

大型综合体图层：建筑地址、建筑高度、建筑层数、建筑面积、负责人、消防机构、周边等。

石油化工图层：单位名称、地址、单位性质、主要产品、最大产量、负责人、消防机构等。

核电站图层：地址、负责人、电话、机组数、装机容量、年发电量、消防机构。

水电站图层：单位地址、负责人、电话、总库容、装机容量、蓄水位、消防机构。

水库图层：单位地址、负责人、电话、总库容、蓄水位、消防机构。

地震带图层：地震带分布情况及地震带的名称。

防火重点单位图层：建筑名称、建筑地址、建筑类别、成立时间、负责人、消防机构。

灭火重点单位图层：建筑名称、建筑地址、建筑类别、成立时间、负责人、消防机构。

泡沫生产厂图层：公司名称、公司地址、建筑类别、库存容量、日生产量、联系人、电话、消防机构、库存概述。

消防机构图层：机构名称、机构地址、机构类别、机构全称、人员、车辆、联系人、电话、机构描述。

视频会议图层：名称、设备 IP、设备类型、所属单位等信息。

消防队站图层：名称、地址、类别、形式、人员、车辆、联系人、电话。

救灾专业队伍图层：队伍名称、地址、人员、车辆、集结时间、联系人、电话、消防机构、消防装备。

移动设备图层：包括单兵、手机、消防车、通信车辆、无人机、执法记录仪、行车记录仪、平板电脑、对讲机、便携、LTE。

单兵图层：设备的相关信息（设备类型、设备呼号、设备编号、所属单位、更新时间）、持有人信息（持有人编号、持有人名称、持有人类别、所属单位、联系电话）等信息。

手机图层：设备的相关信息（设备类型、设备呼号、设备编号、所属单位、更新时间）、持有人信息（持有人编号、持有人名称、持有人类别、所属单位、联系电话）等信息。

消防车图层：车辆底盘相关信息（包括速度、发动机转速、剩余燃油百分比、总里程、蓄电池电压、机油温度等信息）、车辆上装信息（包括水罐液位、泡沫罐液位、消防水泵出口压力）等信息。

通讯车辆图层：设备的相关信息（内容包括设备类型、设备呼号、设备编号、所属单位、更新时间）、持有人信息（内容包括持有人编号、持有人名称、持有人类别、所属单位、联系电话）等信息。

无人机图层：设备的相关信息（设备类型、设备呼号、设备编号、所属单位、更新时间）、所属单位、联系电话等信息。

执法记录仪图层：设备的相关信息（设备类型、设备呼号、设备编号、所属单位、更新时间）、持有人信息（持有人编号、持有人名称、持有人类别、所属单位、联系电话）等信息。

对讲机图层：设备的相关信息（设备类型、设备呼号、设备编号、所属单位、更新时间）、持有人信息（持有人编号、持有人名称、持有人类别、所属单位、联系电话）等信息。

便携图层：设备的相关信息（设备类型、设备呼号、设备编号、所属单位、更新时间）、持有人信息（持有人编号、持有人名称、持有人类别、所属单位、联系电话）等信息。

LTE 图层：设备的相关信息（设备类型、设备呼号、设备编号、所属单位、更新时间）、持有人信息（持有人编号、持有人名称、持有人类别、所属单位、联系电话）等信息。

特种装备图层：装备名称、存放单位、生产厂家、联系人、电话、消防机构。

消火栓图层：消防栓地址、状态、取水方式、所属管网、管网压力、流量、建成日期、消防机构。

消防水源图层：水源地址、状态、容量、储水量、取水方式、消防机构。

应急保障图层：单位名称、地址、类别、联系人、电话、消防机构、保障能力。

救灾储备物资图层：名称、地址、联系人、电话、描述、所在总队、物资概述。

重大安保涉会场所图层：名称、地址、类型、成立时间、负责人、消防机构。

重大安保驻地图层：名称、地址、类型、联系人、电话、执勤车辆、配套车辆、执勤人数、配套人数。

增援编队图层：增援编队名称、消防机构、队伍人数、联系人、队伍车数、增援情况、编队力量等信息。

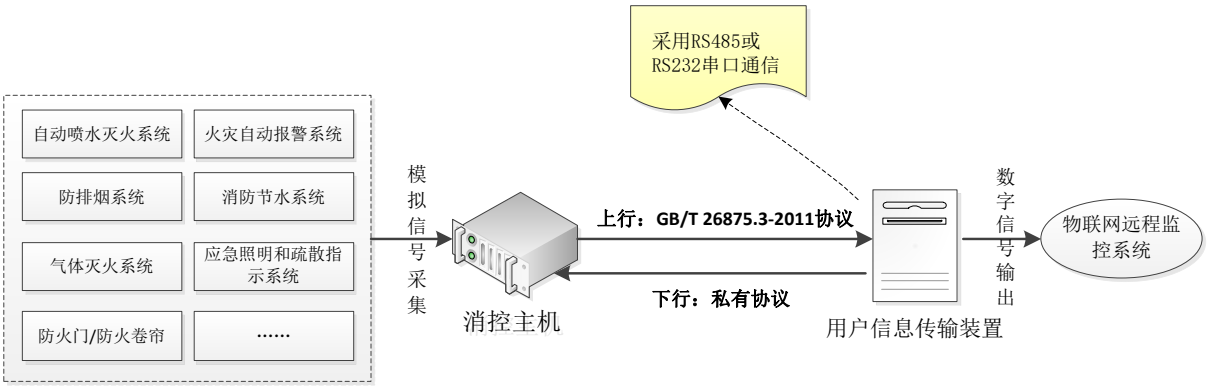
具体各图层的字段规范请参见《附件 3-3 全国消防一张图数据标准规范》。

第9章 技术架构设计

9.1. 物联设备通信协议适配标准设计

智慧消防云平台中的城市消防物联网远程监控系统建设过程中，将涉及多种品牌、类型的物联网监测设备接入，为保障系统平台在设备接入方面的灵活性与可扩展性，解决不同品牌设备、不同类型设备在通信协议接入的不兼容性与排异性等问题，本次设计将建立统一的物联设备通信协议适配标准和机制，各种设备（用户信息传输装置、智能传感终端设备）接入时必须通过协议适配机制进行协议格式转换，以满足统一通信标准的需求。

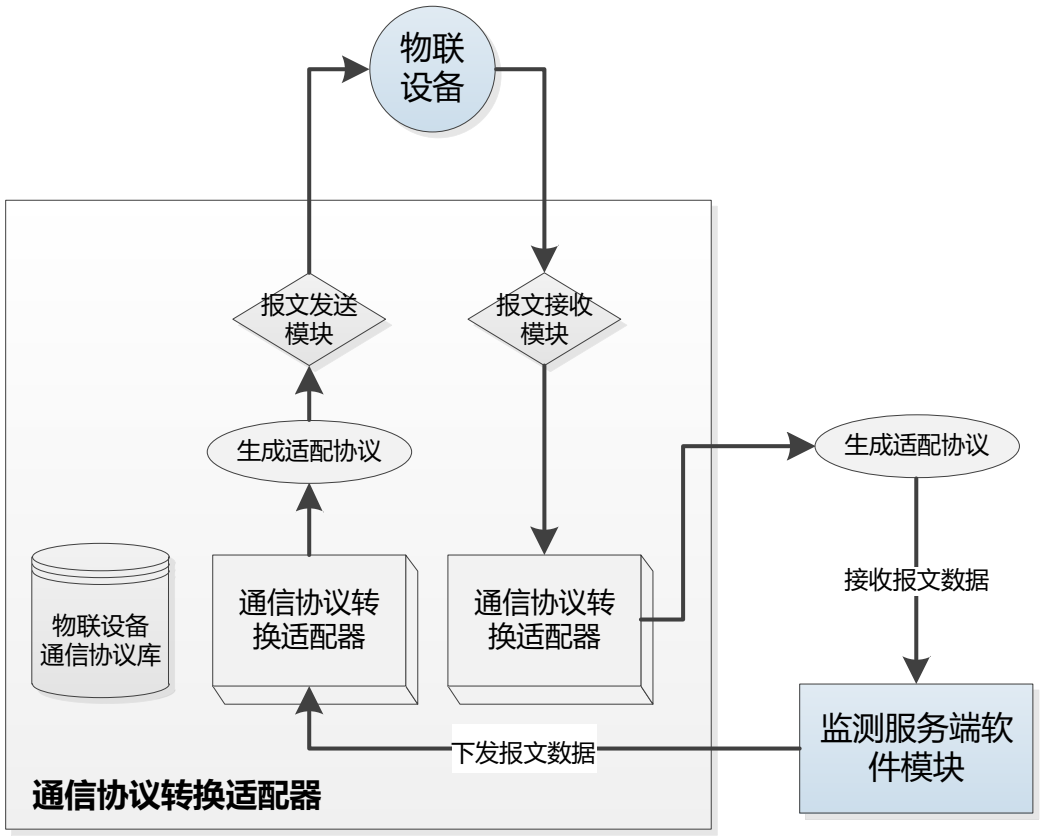
9.1.1. 硬件装置拓扑结构



上图中，消控主机通过有线方式将各种消防设备设施系统连接进来，用户信息传输装置通过 RS485 或 RS232 串口通信标准实现从消控主机获取消控设备各种监测状态数据。目前几乎所有的消防火灾风险单位都建设了消控系统，城市消防物联网远程监控系统，本期智慧消防云平台中城市消防物联网远程监控系统只需通过在消控室架装 1 台或多台（有多个消控室的）采用 GB/T 26875 标准的“用户信息传输装置”，即可实现物联网远程监控系统实时获取火灾风险单位的消防监测数据。

9.1.2. 通信协议适配转换机制

具体通信协议适配转换机制如下图所示：



通过建立通信协议统一转换适配器，当有物联设备（用户信息传输装置、智能传感监测终端设备）接入物联网系统时，系统平台将通过协议转换适配器按照协议转换适配规则，生成标准的设备适配协议（翻译协议），满足物联网设备与监测服务端软件模块之间的快速报文数据通信。

9.1.3. 接入设备规范性要求

为确保物联设备接入消防物联网远程监控系统时设备通信协议适配转换过程的稳定性，要求接入远程监控系统的物联设备产品必须采用国标规范，这样才能确保通信协议转换的机制统一性和标准可循性。

以下为消防物联网接入设备产品的国标规范性要求：

1．火灾报警智能监控设备：GB 20517-2006《独立式感烟火灾探测报警器》、GA 1151-2014《火灾报警系统无线通信功能通用要求》

2．消火栓智能监控设备：GB／T 30269.602-2017 《信息技术 传感器网络 第 602 部分：信息安全：低速率无线传感器网络网》

3．用户信息传输装置：GB 26875.1-2011《城市消防远程监控系统 第 1 部分：

用户信息传输装置》

4. GB/T 26875.3-2011 城市消防远程监控系统 第 3 部分：报警传输网络通信协议

9.1.4. 协议转换适配器实现方式

由于通信协议转换适配器数据较为复杂的一套软硬件及网络装置，且消防物联网远程监控系统接入设备的数据采集具有实时、海量的特点，对于通信协议转换适配器在转换质量、转换性能效率、持续性及稳定等要求较高，因此建议优先选择市面上已有的通信协议转换适配装置产品，确保物联网设备快速接入和通信稳定。若市面无标准产品，则可由后期系统项目承建单位结合本项目特点进行自主开发。

9.2. 数字福建公共平台调用设计

数字福建公共平台调用设计，也可称为福建省级公共支撑平台资源调用设计，调用设计内容如下：

9.2.1. 应用支撑层调用设计

应用支撑层调用优先利用政务外网云平台资源，优先调用数字福建公共平台资源，以达到避免重复建设和投资、提高信息建设效率的目的。

9.2.2. 基础设施层调用设计

基础设施层不另行建设，将利用省电子政务信息网、省政务外网及省电子政务云平台现有资源。

9.2.3. 安全基础平台调用设计

安全设备利用政务外网云平台现有安全资源，并满足计算机信息安全等级保护标准：三级。

9.3. 服务渠道层设计

9.3.1. 接入终端设计

本项目采用基于 Java EE 技术的 B/S 多层应用体系结构设计，通过 PC 浏览器、智能手机客户端访问系统。

1．消防业务部门、消防领导指战员等可采用电脑终端，通过政务信息网接入，开展政务信息网相关业务应用；采用电脑终端、移动终端通过互联网接入省政务外网互联网接入区开展互联网相关业务应用。

2．公众可采用电脑终端、移动终端，通过互联网接入政府门户网站（政务外网互联网接入区），开展查询、查看等应用。

9.3.2. 发布渠道设计

福建省消防救援总队、各支队、各大队，以及智慧消防云平台的相关数据、政策信息、公告信息等均可通过门户网站（含微信公众号、微官网）、APP、小程序等进行发布，采用链接的方式接入，并可通过指挥中心、值班监控中心的 LED 大屏系统进行展示。

9.4. 应用系统层技术路线设计

系统在软件开发、页面设计、主机存储等方面均需较先进的技术路线。

9.4.1. J2EE 与三层构架

本次项目在应用软件开发上考虑到系统存在跨平台部署问题，故建议使用 JEEE 与三层架构的方式，因此本项目建设应用软件开发的技术路线与开发方案主要有：

严格遵循标准：本系统的指标体系、数据接口、信息数据项、信息分类编码标准和有关技术标准与国家标准保持一致。系统采用 B/S 结构，遵从 TCP/IP 协议标准。如与相关部门交换数据时，单位信息以组织机构代码为标准依据，个人信息以公民身份号码为标准依据等。

J2EE 技术框架：三层技术体系结构即采用 J2EE 技术，三层结构的客户/服务器

模型是当前先进的协同应用程序开发模型，它将应用功能分成表示层、功能层和数据层三部分。

9.4.2. 面向服务（SOA）的设计

本次项目软件开发应遵循使用面向服务（SOA）的设计，采用面向服务的体系结构（SOA）的技术路线，通过服务抽象标准化，使用标准的服务契约定义数据格式转换和协议转换，实现服务之间的解耦。

9.4.3. 松耦合的设计

各分系统集成采取松耦合原则，既共享与交换必要的信息，又能相对独立地运行，互不干扰；各系统之间保持相对独立。通过松耦合设计能够使业务应用功能的扩展更新、日常维护、启动/停止服务等变得更加灵活。

9.4.4. 中间件技术

中间件是一种独立的系统软件或服务程序，中间件软件管理着客户端程序和数据库或者早期应用软件之间的通讯。中间件在分布式的客户和服务之间扮演着承上启下的角色，如事务管理、负载均衡以及基于 Web 的计算等。

在本次项目中建议采用成熟、安全、稳定的中间件产品或技术。

9.4.5. GIS 地理信息技术

在福建省智慧消防云平台中，可引入 GIS 地理信息系统，对消防安全监管与消防服务行业领域的各种生产要素、经营管理要素、监管要素、流通要素、监测预警要素等，都可以在 GIS 上进行展现、跟踪和追溯。

9.4.6. 商用密码防伪技术

商用密码产品是指采用密码技术对不涉及国家秘密内容的信息进行加密保护或者安全认证的产品。商用密码技术是商用密码的核心，商用密码技术由国家密码管理局统一管理并发布标准，例如 SM2、SM3、SM4、SMC 算法等。在本项目中的主要应用范围包括了消防安全服务与消防安全溯源 RFID 电子标签、消防物联网监测部分数

据的加密、以及整个系统平台安全身份认证与验证。对于原来通过明文或简单加解密算法的数据与安全防护技术手段，升级到依托国密标准的加密安全防护手段。

9.5. 应用支撑层技术路线设计

9.5.1. MVC 设计模型

系统引入 MVC(ModelViewControl)设计模型,使前台显示与后台业务处理分离，使系统表现层丰富，适应业务需求的变动。

9.5.2. 系统服务组件技术

系统采用组件技术提供系统的快速开发和更新，并将公共的组件封装，可随着业务需求不断的变化快速的重组，建成新的应用，使系统具备较强的可扩展性。

9.5.3. MQ 消息队列技术

消息队列技术是分布式应用间交换信息的一种技术。消息队列为构造以同步或异步方式实现的分布式应用提供了松耦合方法。消息队列可用在应用中以执行多种功能，比如要求服务、交换信息或异步处理等。

9.5.4. Portal 技术

Portal 以用户为中心，提供统一的用户登录，实现信息的集中访问，集成了办公商务一体的工作流环境。

9.5.5. 负载均衡技术

负载均衡（Load Balance）建立在现有网络结构之上，分摊到多个操作单元上进行执行，从而扩展网络设备和服务器的带宽、增加吞吐量、加强网络数据处理能力、提高网络的灵活性和可用性。

9.5.6. RESTful 技术

RESTful 架构是对 MVC 架构改进后所形成的一种架构,通过使用事先定义好的接

口与不同的服务联系起来。在 RESTful 架构中，浏览器使用 POST，DELETE，PUT 和 GET 四种请求方式分别对指定的 URL 资源进行增删改查操作。因此，RESTful 是通过 URI 实现对资源的管理及访问，具有扩展性强、结构清晰的特点。

9.5.7. 缓存技术

缓存就是在内存中存储的数据备份，当数据没有发生本质改变的时候，就不让数据的查询去数据库进行操作，而去内存中取数据，这样就大大降低了数据库的读写次数，而且从内存中读数据的速度比去数据库查询要快一些，这样同时又提高了效率。

9.5.8. 微服务架构

9.5.8.1. 微服务概述

智慧消防云平台采用微服务架构，每个服务运行在其独立的进程中，服务和服务之间采用轻量级的通信机制相互沟通（通常是基于 HTTP 的 Restful API）.每个服务都围绕着具体的业务进行构建，提高系统平台的可维护性、运行持续性，以及提高平台服务性能。

9.5.8.2. 微服务（网关）

实现省级智慧消防物联平台的应用服务入口和应用服务路由和相通服务的分流、流量镜像、应用服务的维护开关和 Api 监控、Api 文档。实现 QPS 和 TPS 双万级别，随着硬件设施和网络环境的改善最高可达百万级别。

9.5.8.3. 微服务（服务治理）

实现服务物框架基础内容，包括：服务目录、注册发现、限流、熔断降级、容错、路由、负载均衡、自动分流、拓扑依赖、配置中心、服务监控、服务告警、认证鉴权

9.5.8.4. 基础组件服务集群

实现 MySQL 集群、Redis 集群、ElasticSearch 集群、RocketMQ 集群、Kafka 集群、FastDFS 集群，以此来实现大数据的存储和容错机制和架构的运行效率，是平台可以日吞吐 PB 级别的海量数据和提供整体的 TPS 的吞吐量。

9.5.8.5. 分布式服务

支撑整个省级智慧消防服务平台的基础服务，例如：分布式日志服务、分布式配置服务、分布式定时任务、分布式监控中心等。

9.5.8.6. 运营服务

数据分类、流程权限、审计、业务策略、消息系统监控、信息系统监管、数据保留规则。

9.5.8.7. 运维服务

故障管理、服务管理、操作警告、运维流程编排、配置任务自动化、策略管控、变更管理和 Docker 容器管理。

9.5.8.8. 流程处理服务

流程编排、规则管理、预测分析、决策表、流程发现及优化。

9.6. 数据层技术路线设计

9.6.1. 数据存储

9.6.2. 业务数据存储

系统的业务数据可选择存储在 Mysql、人大金仓（信创产品）、达梦（信创产品）等成熟的关系型数据库上。

9.6.3. 数据格式类型

本项目的数据格式类型，主要使用结构化查询语言（StructuredQueryLanguage）简称 SQL，是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统；同时也是数据库脚本文件的扩展名。

9.6.4. 大数据存储

HDFS（Hadoop 分布式文件系统）是大数据环境下数据仓库/数据平台最完美的数据存储解决方案，可将设备采集数据及系统运行日志等海量数据存储在 HDFS(Apache Hadoop)。

HDFS 有如下优点：扩容能力强、成本低、高效率、可靠性强。

9.6.5. 数据库开发技术

本项目的数据库操作（存取）主要采取 ORM（对象关系映射 Object Relational Mapping）框架来实现程序类对数据库层的快速开发操作。主要包括：Hibernate，MyBatis，ObjectiveSQL，JDO 以及 JPA 等。

9.7. 基础设施层设计

9.7.1. 网络系统设计

依托政务云平台进行建设，由云平台提供所需交换机及其相关网络设备。

9.7.2. 主机系统设计

主机系统主要可以分为应用服务器和数据库服务器，本次主机系统利用福建省电子政务外网电子政务云平台上资源，不另外新增设备。

数据库服务器是构建各种信息数据库、中间件、应用软件平台的依托，涉及到各种数据库及其应用，存储着所有业务数据、应用系统和信息运行所需的数据，是保证系统正常运作的关键。这些对服务器系统处理能力提出了较高要求，需要高性能 CPU、大容量内存为各类遥感数据应用提供支撑。

根据业务量分析，本项目系统按照最大同时在线用户数 1000 人和并发数 200 计算。

9.7.2.1. 应用服务器

依托政务外网云平台建设，基于电子政务云平台 IaaS 基础设施层，为本项目提供主机资源。虚拟机资源需求如下：

序号	应用名称	数量	操作系统	CPU（核）	内存（GB）	说明
一	政务外网云平台互联网接入区					
1	业务应用服务器	11	WindowsServer 或 Linux	8	32G	云平台提供
2	数据交换服务器	2	WindowsServer 或 Linux	8	32G	云平台提供
3	文件服务器	2	WindowsServer 或 Linux	4	16G	云平台提供

9.7.2.2. 数据库服务器

目前云平台提供的数据库实例资源如下表所示：

序号	数据库规格编号	数据库空间大小	归档日志空间大小	用户业务空间	索引表空间（index）	回滚表空间（undo）	临时表空间（temp）	Redo 文件
1	D01	40G	8G	20G	8G	2G	2G	128MB*6
2	D02	80G	16G	40G	16G	4G	4G	256MB*6

本项目需要基础信息数据库、业务数据库、应用数据库、综合数据库、管理数据库、元数据库，相应的服务器配置如下：

表 数据库服务器设计表

序号	服务器用途	主要性能指标	数量
1	数据库服务器	数据库规格编号 D02	8

9.7.3. 存储系统设计

存储系统利用福建省政务云平台存储资源，根据数据量需求分析，需要申请政务外网电子政务云平台提供 100TB 存储空间。

9.7.4. 备份系统

依托福建省级政务外网电子政务云平台备份系统，由福建省政务外网云平台提供所需的备份空间，数据需永久保存。为了确保数据安全，要求备份数据与生产数据不保存在同一存储设备上。备份系统实现操作系统数据及应用程序、Oracle 或 MySQL 数据库数据、电子文件（报表文件、文书文件等）的数据备份。在备份策略的制定上，需要分析不同的数据源和数据类型来做相应制定，备份容量约为 100TB 左右。

（1）操作系统数据及应用程序

操作系统数据及应用程序只有安装系统软件包或改变一些系统配置时才会改变，对于它备份可以比较灵活，只需要在系统变更后进行一次操作系统全备份即可，也可以定义在备份策略中每个月做一次全备份。该部分备份的技术实现方式可通过电子政务云平台的虚拟机镜像备份机制实现。

（2）Oracle 或 MySQL 数据库数据

作为核心业务数据处理系统，数据量较大，变化比较频繁，建议每天做逻辑增量备份；每周做全库物理热备份。

（3）电子文件

根据电子文件数据量的特点，建议每天做逻辑增量备份；每周做全库物理热备份。

9.7.5. 系统软件

（1）操作系统

操作系统采用 LINUX、WindowsServer，利用云平台已有资源。

（2）数据库管理系统

数据库管理系统采用国产品牌数据库或 ORACLE 企业版，利用云平台已有资源。

9.7.6. 机房及配套设计

本次福建省智慧消防云平台软硬件部署将依托于福建省电子政务云计算平台，所使用云平台虚拟服务器资源等均由省级政务云平台提供分配。

本次项目不再进行机房及相关配套设计。

9.8. 系统物理部署方案

9.8.1. 应用及数据物理部署方案

为符合系统设计的原则和工程投资概算，根据业务和技术要求、设备的性价比、满足项目建设兼容性、整体维护的要求进行选择。相关产品的实际配置待招投标确定；配套设备与其他软件配置依据安全性、稳定性和业务性要求不同分别选用。

本项目以互联网为主要网络环境，将智慧消防云平台应用部署在福建省电子政务外网云平台互联网区。

根据所需要虚拟设备资源及其用途分析，具体部署方案如下：

编号	项目名称	主要性能指标	单位	数量	部署说明
1	网络系统				
（1）	核心交换机	政务云平台网络资源池提供	套	1	由政务云平台提供
（2）	服务器接入交换机	政务云平台网络资源池提供	套	2	由政务云平台提供
2	主机（服务器）系统				
（1）	应用服务器	政务云平台虚拟机，8 核 CPU，32GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）	套	11	由政务云平台提供
（2）	文件服务器	政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）	套	2	由政务云平台提供
（3）	数据交换服务器	政务云平台虚拟机，8 核 CPU，32GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）	套	2	由政务云平台提供
（4）	数据库服务器	政务云平台提供数据库实例 D02（ORACLE，数据库空间大小 80G、归档日志空间大小 16G、用	套	8	由政务云平台提供

		户业务空间 40G、索引表空间（index）16G、回滚表空间（undo）4G、临时表空间（temp）4G、Redo 文件 256MB*6）			
3	存储备份系统				
（1）	虚拟存储系统	政务云平台提供，≥50T。	套	1	由政务云平台提供
（2）	虚拟备份磁带库	电子政务云平台提供，备份策略要求每份数据保留 3 个月，每天一增备、每周一全备（3 个月内），要求备份数据不与生产数据保存在同一存储设备上，确保数据安全，≥50T。	套	1	由政务云平台提供
4	系统软件				
（1）	Windows 操作系统或 LINUX 操作系统（如已国产化）	电子政务云平台提供	套	23	由政务云平台提供
（2）	数据库存储系统	优先选择国产数据库，如政务云平台暂未提供国产品牌数据库，则可选择 ORACLE、MYSQL 等通用数据库。	套	1	由政务云平台提供
（3）	数据库终端管理系统	数据库系统自带数据库管理运维系统，或政务云平台指定专用数据库终端管理系统。	套	1	由政务云平台提供
（4）	备份软件	由政务云平台提供	套	1	
5	虚拟化安全防护系统软件				
（1）	防火墙	由政务云平台提供	套	1	由政务云平台提供
（2）	负载均衡	8 核 CPU；8GB 内存；2 个网卡；≥500G 磁盘空间；Linux 操作系统	套	1	由政务云平台提供
（3）	入侵防御系统（IPS）	由政务云平台提供	套	1	由政务云平台提供
（4）	入侵检测系统（IDS）	由政务云平台提供	套	1	由政务云平台提供
（5）	数据库审计系统	由政务云平台提供	套	1	由政务云平台提供
（6）	日志审计系统	由政务云平台提供	套	1	由政务云平台提供
（7）	漏洞扫描系统	由政务云平台提供	套	1	由政务云平台提供

（8）	终端侦测与响应系统	由总队与支队提供	套	10	由政务云平台提供安装环境
（9）	数字证书系统	由政务云平台提供	套	1	由政务云平台提供
（10）	VPN 加密设备	由 94 家监管单位提供，火灾风险单位可监管单位指定要求自行采购，满足 VPN 对接	套	94	由 94 家监管单位提供

9.8.2. 消防值班监控中心（总队）部署方案

9.8.2.1. 建设背景与需求

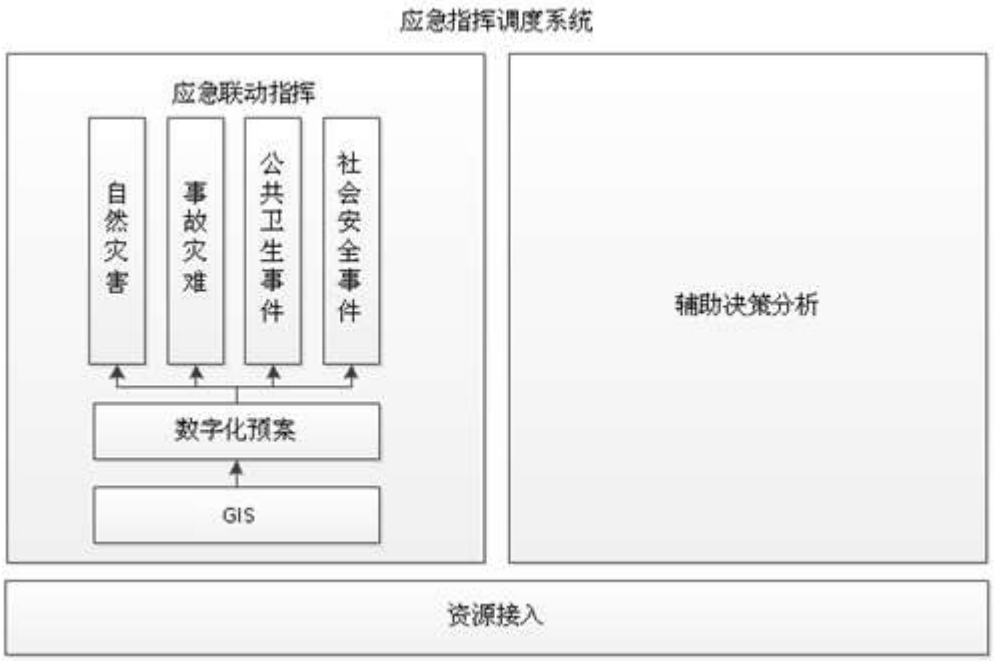
消防值班监控中心，是对省、市、县三级智慧消防相关系统（特别是消防物联网远程监控系统）的监测数据、巡查维护数据、在岗信息进行综合汇总、统计、分析研判、隐患险情报警，以及事件发生后的一系列消息传递与处置流程。

本次福建省智慧消防云平台消防值班监控中心（总队）设计建设，将为福建省消防救援总队应急处理部门提供视频通信与信息保障，结合省消防救援总队的各种指挥系统（如实战指挥系统、属地政府应急联动系统、互联网舆情监控系统、图像综合管理系统、北斗定位导航系统、119 接处警系统等），将各种消防安全监管应急服务资源统一在一套完整的智能化信息处理与通讯方案之中；遇紧急、突发、特殊事件，联动系统即成为消防体系统一的协调、信息的收集与分析、指挥调度中心。

9.8.2.2. 建设依据

包括《国家自然灾害救助应急预案》《国务院关于加强应急管理工作的意见》，并参考《福建省人民政府突发公共事件总体应急预案》，《原公安部消防局有关消防火灾隐患及险情综合应急管理预案》，本方案所称突发事件，是指突然发生，造成或可能危及生命安全、财产损失、生态环境破坏和严重社会危害，危及社会公共安全的紧急事件。

9.8.2.3. 系统组成



消防救援总队值班监控中心系统建设的核心是“普通消防安全隐患及险情事件专业处置，重大消防安全事件协同指挥”的目标。系统在非应急情形下，采用应急指挥中心管理系统及预警管理系统功能，承担系统的维护、预案的管理和常态信息发布的职能。

在应急情况下通过应急联动指挥体系、数字预案管理体系、辅助决策分析体系和资源接入体系，实现人员特别是省消防救援总队领导对各相关机构负责人员的坐镇调度指挥，并借助各机构负责人对下属机构的消防物资、消防人员、消防设施设备实施等进行协同指挥调度。

9.8.2.4. 应急预警体系建立

9.8.2.4.1. 应急联动指挥体系

根据突发公共事件的发生过程、性质和机理，系统需要处理的突发公共事件主要分为以下四类：

（1）自然灾害。主要包括水旱灾害，气象灾害，地震灾害，地质灾害，海洋灾害，生物灾害和森林草原火灾等。

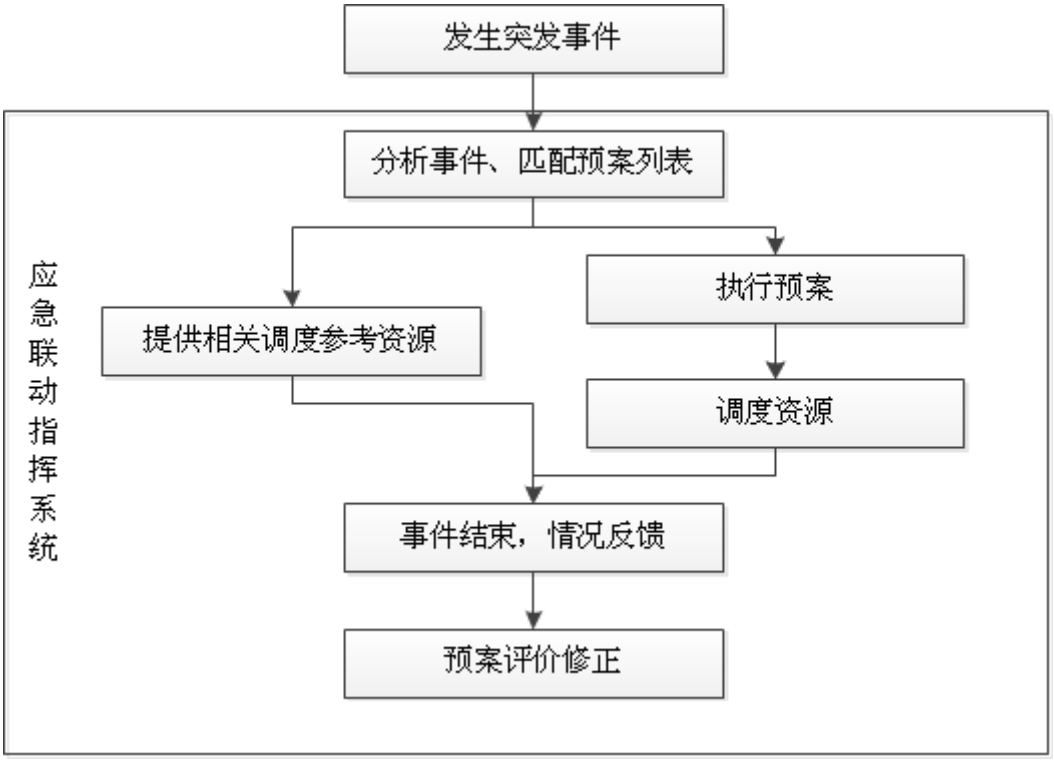
（2）事故灾难。主要包括工矿商贸等企业的各类安全事故，交通运输事故，公共设施和设备事故，环境污染和生态破坏事件等。

（3）公共卫生事件。主要包括传染病疫情，群体性不明原因疾病，食品安全和职业危害，动物疫情，以及其他严重影响公众健康和生命安全的事件。

（4）社会安全事件。主要包括恐怖袭击事件，经济安全事件和涉外突发事件等。

各类突发公共事件按照其性质、严重程度、可控性和影响范围等因素，一般分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）和Ⅳ级（一般）。

针对消防安全事件的应急指挥联动，主要包括了自然灾害、事故灾害、公共卫生事件等三个。



图：应急联动指挥事件处理流程

■ 联动指挥内容

应急联动指挥是应急指挥调度系统的核心业务，当以上提到的各类事件发生时，可以管理调度任务，基于百度或高德 GIS 电子地图进行指挥调度，根据事件的类型、区域、严重程度、影响范围等因素自动推荐最匹配的预案列表，不同类型的突发事件给出不同的应对措施，统一分配应急资源，调度各级消防安全监管部门、消防安

全救援领域专家、消防技术服务单位、火灾风险单位消防工作人员、各种消防救援物资、救援力量等单位，达到资源的“即需、即知、即用”。

- **调度方式**

具体调度方式可分为“电话调度（数字录音）”“短信调度”“传真调度”“350M集群呼叫调度”“卫星通讯车调度”等几种方式，因此应急联动指挥模块需要集成以上调度方式。适当时候可以在应急指挥车上实现与指挥中心的辅助指挥。

- **信息发布**

调度全过程可以直接在大屏上体现，实现指挥的可视化实时协同联动，动态信息实时展示和发布，根据事件的等级，及时对接上一级如市级、省级应急指挥相应部门，做到通信畅通。并向专网、网站、广播、商业通信、官方微博等工具提供动态信息。

9.8.2.4.2. 数字化预案管理体系

数字化预案管理体系包括专家库和预案库。

建立完善、可按需定制的专家库，专家涉及不同突发事件的联系人及电话。针对不同类型的事件建立不同的预案库，每类事件给出关键参数，根据关键参数给出不同的预案等级及应对措施。预案库与应急联动指挥业务紧密关联，当有突发事件发生时预案库可以匹配出最优预案。另外提供调度结束后的任务总结、统计分析功能，并在预案执行完毕后根据预案完成情况对预案评价修正。

9.8.2.4.3. 辅助决策分析体系

辅助决策分析体系的目标是综合利用各种设备和信息资源，为指挥人员了解情况、实战指挥提供决策支持。系统对现有的业务进行交叉分析，利用表格、曲线图、柱状图、饼型图、多维分析、数据挖掘模型等手段为案情分析，数据统计等工作提供分析工具。辅助决策子系统基于数据仓库、数据挖掘技术，通过对消防安全监管服务各业务系统数据的抽取、转换、清洗、加载，形成消防安全行业领域的综合数

据库。

9.8.2.4.4. 资源接入体系

资源接入是辅助决策分析的消防安全监管与服务数据基础，本系统需要接入如下资源：

- 全省各级消防部门的消防物联网设备实时监测采集数据
- 火灾风险单位日常巡查维护数据
- 消控室值班在岗视频信号数据
- 省市县基础业务数据

9.8.2.5. 建设内容

省总队消防值班监控中心拼接大屏显示部分不仅包含用来视频图像显示的大屏显示部分，还包括解码控制等。子系统大屏拼接部分能与视频综合平台无缝对接，获得最佳效果。

LED 显示单元常用的尺寸有 46 寸、47 寸、55 寸、60 寸等，它可以根据客户需要任意拼接，采用背光源发光，物理分辨率可以轻易达到高清标准，LED 屏功耗小，发热量低，且运行稳定，维护成本低。LED 大屏单元组成的拼接墙具有低功耗、重量轻、寿命长、无辐射、安装方便快捷、占用空间较小等优点。

本次项目的大屏显示系统可采用 P1.66 规格（或以上，根据实地情况）LED 屏（像素间距 1.8mm，每平方米的像素点为 308641 点）来显示各类视频信息和 VGA 图像，采用单屏 46 英寸（16:9）的 VGA 显示屏拼接墙系统，以视频矩阵为中心，应急指挥中心的计算机 VGA 图像、视频监控图像、摄像机图像、DVD 视频图像、展示台视频图像、有线电视图像、互联网信息展示图像、养殖场分布信息及现场信息展示图像等，所有视频源均输入视频矩阵，切换输出到大屏幕及各图像系统。

- **扩声系统**

扩声系统以调音台和音频矩阵控制设备为中心，指挥中心的麦克风（包括固定

位有线麦克风、耳夹式麦克风、手持麦克风）、视频会议、计算机、电话、录像机、DVD 机、卡座、有线电视等声音输入输出信号均接入调音台和音频矩阵系统，实现各路音源输入输出的切换控制。经过自动回声消除、反馈抑制、功放等设备处理后通过扬声器放音，实现会场扩音。

- **中央控制系统**

中央控制系统是指操作员可以通过控制面板、触摸屏或无线遥控等方式，通过计算机和中央控制系统软件来控制投影机、音视频矩阵、摄像机、功放、计算机、电动屏幕、灯光、窗帘等设备。

- **供电系统**

指挥中心所有电子设备集中由市电供电，以保证各系统的正常运行。必要时可配备 UPS 电源。

9.8.2.6. 消防值班监控中心大屏建设原则

省总队消防值班监控中心 LED 拼接大屏可采用目前国内主流且先进的 H.265 最新编码格式，并向下兼容 H.264 编码格式。拼接屏采用 9 块 46 英寸 3.5 拼接缝 LED 显示单元，以 3(行)X3(列)拼接方式组成，高清拼接屏由集成一体式拼接控制器控制。本系统可实现远程监控，指挥养猪场视频监控系统。

- **可用性原则**

大屏幕信息显示系统作为综合性信息显示的重要场所，系统必须保证实用并切实满足或高于客户的需求。根据客户应用需求的规模和要求，承建方将选择最合适的 LED 大屏幕拼接单元、最优化的拼接控制系统和外部控制软件环境组成 LED 大屏幕拼接系统。配合信号切换，可以选择任一路信号在大屏幕上的显示；满足不同接入信号的组合显示等需求。通过软件操作控制，快速实现输入信号在 LED 大屏幕拼接系统的独立显示或大屏显示。

- **先进性原则**

LED 大屏幕拼接单元具备大尺寸、显示质量优异、单位面积成本低、使用寿命

长等特点，它已成为最具发展前景的大型显示器件在与 DLP、PDP 的竞争中也占据越来越大优势。

作为LED大屏幕拼接系统的显示单元，能够直接输入 RGB 信号、Video（BNC）信号、YPbPr 信号、S-video 信号、DVI 信号、HDMI 信号，还可以通过拼接控制系统进行多种信号源的拼接显示，若配合矩阵进行信号切换可以实现多路信号的同时输入并可任意选择一路信号在大屏幕上任一单屏的显示。全中文控制界面具有强大的显示控制功能和简易直观的操作界面。

- **可靠性原则**

整个系统可以按照需求全天 24 小时、一年 365 天连续工作，所以整个 LED 大屏幕拼接系统必须具有高可靠性、高稳定性等特点，以保证系统常年连续正常运行。为了满足大屏幕拼接系统长年连续运行，因而其设计必须遵循可靠性的原则，在系统设计时，关键部位选用了高可靠性设备，对于重要的控制节点采用先进的高新技术来保障。

- **标准化原则**

系统在选用控制技术和设备时，符合国际标准，充分利用各种产品的优势，将它们有机地结合起来。也就是说，要求系统的通信环境、硬件环境、软件环境相互间的依赖减至最小，充分发挥自身优势；同时，系统的互联为信息互通和网上控制创造有利条件。

- **经济性原则**

合理的性价比是系统设计中应当考虑的重要内容。因此，所选用的设备在兼顾良好性能的基础上也要考虑经济性，除考虑系统总体造价外，还应当考虑系统长期运行维护成本。

- **可扩充性原则**

随着技术的发展和需求的扩大，系统的扩充是必然的，因而在系统设计时充分考虑未来系统扩充的可行性，在进行扩充时现有设备可得到充分的利用。

■ **兼容性原则**

大屏幕系统项目是一个庞大而复杂的系统，需要实现各种子系统的完美汇接，所以系统的兼容性就显得十分必要。

■ **可维护性、可管理性原则**

承建方从用户角度出发，充分考虑到系统设备的安装、配置、操作方便等需求，提供了强大的系统管理手段，合理配置和调整系统负载、监视系统状态、控制系统稳定运行。

9.8.2.7. 现场勘查情况

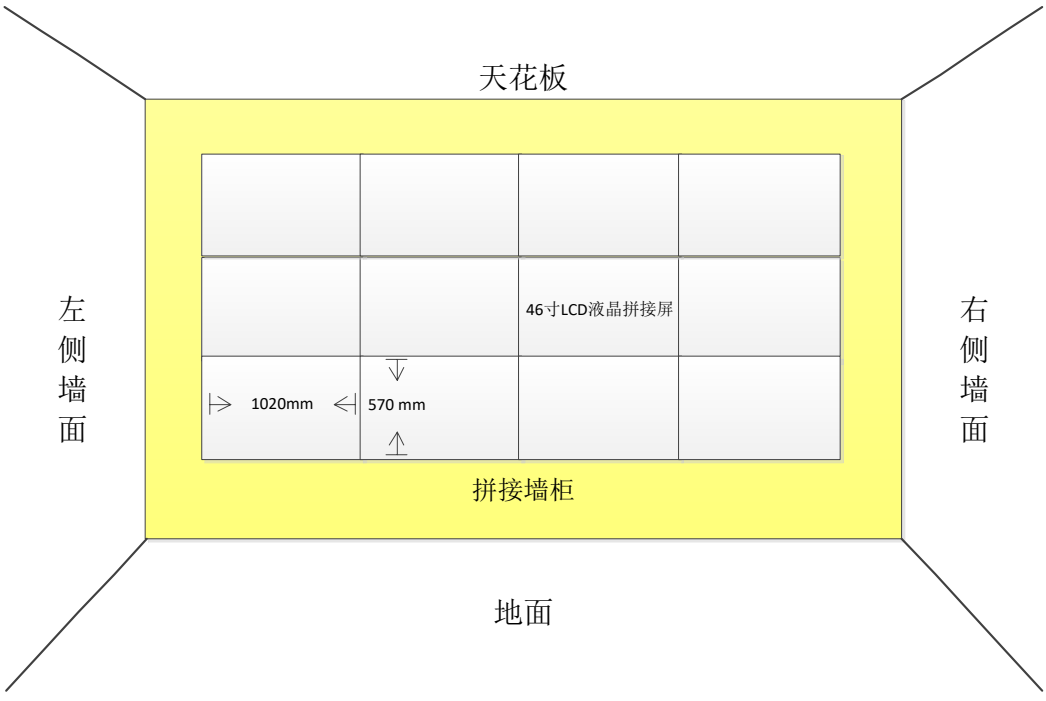
目前省消防救援总队应急指挥中心的升级改造正在进行中，待指挥中心升级改造完成后，智慧消防云平台的消防值班监控中心可与指挥中心同时办公，应急指挥中心可分配 2-3 个座席给智慧消防值班小组进行日常值班使用，智慧消防平台的汇总统计信息，在需要上墙时可借用智慧中心的 LED 大屏。

9.8.2.8. 主要设备及参数（参考）

序号	设备名称	技术参数（参考）	数量
1	宽带线路	承租运营商宽带线路，百兆光纤	1 条
2	46 寸拼接屏	1. 屏幕尺寸 46 寸，LED 光源，分辨率：1920×1080 2. 双边拼缝 3.5mm 3. 亮度 500cd/m2，对比度 3500:1 4. 输入接口可支持：USBx2，HDMI×2，VGA×1，DVI 环入×1，AV,BNC×1，Y(YPbPr)×1，Pb(YPbPr)×1，Pr(YPbPr)×1，音频，RJ45/ISP，输出接口可支持：VGA×1，DVI 环出×1，AV，音频，RJ45，DEBUG/ISP×1； 5. 液晶显示单元金属外壳符合盐雾试验要求； 6. 液晶显示单元金属外壳符合防火试验要求。	12 台
3	解码器	1. 处理器：工业级嵌入式处理器，操作系统：嵌入式 LINUX 操作系统，音频压缩：PCM/G.711/AAC 2. 音视频采集接口：支持 4 路输入，其中 2 路 DVI-I 输入口，2 路 HDMI 输入口，输入采集支持 3840 ×2160、1920 ×1080 、 1600 ×1200 、1280 × 960 、1280 ×720 等分辨率 3. 视频输出接口：9 路 HDMI 4. 解码性能：H.264、H.265 视频解码均支持至少 12 路	1 台

		4000x3000，或 18 路 3840x2160@30fps，或 21 路 3392x2008@25fps，或 32 路 2506x1920@25fps，或 32 路 2688x1520@25fps，或 30 路 2048x1536@30fps，或 42 路 2048x1536@25fps，或 64 路 1920x1080@30fps，或 144 路 1280x720@30fps，或 144 路 960x576@30fps 图像解码输出 5. 每个输出口支持任意开窗、漫游。每个输出口支持 16 路开窗。任意一路信号可在整屏的任意位置上与其它信号源拼接漫游缩放叠加显示，图层可达 18 层 6. 语音对讲接口：1 路输入，1 路输出，3.5mm jack 口，网络接口：2 个 10/100/1000M 自适应以太网口，支持 3 个标准 232 接口（1 个 DB9，2 个 RJ45），1 个 USB 2.0 接口，1 个 USB 3.0 接口，1 个 485 接口	
4	支架	采用铝合金材质	12 个
5	底座	采用铝合金材质	4 个
6	线缆	使用 HDMI 线缆	12 条

9.8.2.9. 消防值班监控中心大屏示例图（参考）



图：示例图（参考）

9.9. 系统性能保障设计

以下将从性能设计概述、数据库性能优化、应用服务器性能优化、应用软件性能优化，数据缓存机制五个方面来阐述系统性能优化设计。

9.9.1. 性能设计概述

智慧消防云平台各子系统的整体性能主要取决于两个主要的方面：应用程序性能和数据访问性能。其中应用程序性能主要需考虑多用户并发的问题和应用集群、反向代理等技术。而数据访问性能则不仅要考虑系统支持大并发访问的能力，而且由于综合数据库数据需要从各业务数据库中进行抽取更新，还需重点考虑跨库数据访问的执行策略、整体数据访问负载的管理与控制等方面的内容。

9.9.1.1. 性能设计目标

任何一个应用系统在大访问量和大数据量的真实环境（即生产环境）下运行，与在此之前的开发状态相比，很多因素都发生了变化。系统要能够在多用户并发查询时提供较短的响应时间，因此系统必须实现负载均衡，以最大程度地提高系统的运行效率。要求在对应用系统的访问量达到峰值时，系统的响应速度不发生明显的波动。为达到这一目的，智慧消防云平台建设中将从后台数据库、应用服务器和应用访问代码三个层面上做性能优化设计。

在大访问量的压力下，位于一线的终端同时向服务器发出申请。在后台数据库连接总数一定且应用服务器端连接池中预置连接不可能突破最大值的情况下，系统必须能有效释放空闲资源，一方面可以提高利用率，另一方面能防止“假死机”现象（即因容易导致用户访问超时，而使用户误以为系统死机）。

智慧消防云平台实际运行环境中的后台数据将是海量的数据。许多事实已经证明，随着系统数据量的提升，应用程序与后台数据库的交互、服务器与终端用户之间的数据吞吐、网络负载、静态数据下载量会发生大的改变。对此，智慧消防云平台需要相应制订有效的优化策略，以避免瓶颈制约，提高运行访问效率。

从终端用户发出访问请求到最终得到页面上的结果集的这段时间称为响应时间。响应时间的最大部分往往出现在应用服务器取得后台数据库连接、访问实体表、组

织结果集到关闭连接这一段。经过分析，后台数据的访问率是不均等的。有些数据属于高访问频率，如应用软件的控制表信息、业务信息代码等，我们称之为“公共数据”。基于公共数据的这一特点，本方案在代码级别上专门设计了缓存机制，在满足用户请求的前提下尽量减少应用程序与后台数据库的交互操作。

性能优化设计是立足于效率、并发度和响应速度最优化，在信息缓存和资源就绪两方面、在应用服务器配置和信息代码两个级别上予以体现。

9.9.1.2. 性能设计原则

智慧消防云平台的性能设计将坚持以下原则：

- 实现系统的负载均衡

快速响应时间和持续有效性将是智慧消防云平台各项应用功能向用户提供有效服务的基本要求，担负业务逻辑运算任务的应用服务器所需要的是这样一种解决方案：在确保可靠的持续性服务前提下，对服务器能力进行动态测试及优化，以保证能够满足用户的使用需求。负载均衡的机制能为网络构架提供应用进程平衡负载的能力，使各应用服务器的效率达到最大化，同时保证高效应用方面的可靠性。

负载均衡意味着在应用系统的业务逻辑层上部署多台主机或虚拟主机。当访问量达到一定程度的时候，应用服务器在多台主机间平衡工作量，使已经部署的多台主机都能够发挥最大潜能。

- 提高资源利用率

在一个需要整合后台数据库的应用系统中，后台数据库的运算能力及数据库连接是至关重要的资源。在使用基于请求服务平台进行查询请求的场合，与消息中间件的连接也是如此。当连接难以取得或获取不到时，与当前主机相连的所有前端用户将陷入无限等待中。而事实证明，在一个特定的时间点上，总有部分连接在连接池中处于闲置状态。本方案在配置和程序中制订周密的资源释放计划，以确保一个用户离线或一次查询请求结束/超时切断后，专属于此范畴之内的相关资源能回归原始状态。

- 减少交互及网络负载

在智慧消防云平台中，一次性查询出的数据量如果过多，查询动作执行的时间势必变长，对后台压力变大，并且导致网络上的传输量增大、应用服务器维护数据的压力加大。

现实情况是过大的结果集对用户的意义并不大，因此本方案设计采取两种解决办法，一是在程序中采用分批、多次的办法加快交互速度，避免因少数用户的查询操作导致数据库服务器性能明显下降；另一种解决办法是由系统管理员设定返回结果集的最大数目，以限制每次查询出的数据量大小。这两种方法可由系统管理员根据需要进行选择。

- 提高访问命中率

提高访问命中率，最根本的途径是调整数据库服务器和应用服务器的运行状态使其运行平稳。但是在同等条件下，可以分析出不同范畴数据的访问频率，容易得到的结论是，消防行业信息代码数据和记载配置信息的元数据的访问概率是最大，几乎任何一个页面、任何一次操作均要访问这些数据；同时，某个登录用户的权限信息，包括账号、密级、入口权限等，虽然不是在全局范围内共享的信息，但在该用户登录之后到其离线之前的时间内仍属于频繁访问的数据。对于以上这些数据，将它们与待查询的业务数据分开存放、另行处理是比较可行的方案，可以明显提高访问命中率。

- 性能曲线平滑

在系统运行的高峰期，要求保证应用系统的响应速度和平时相比不出现明显的波动。

9.9.1.3. 系统性能优化措施

对智慧消防云平台从数据库性能、应用服务器性能、应用软件性能以及数据缓存等方面采取优化措施，应达到以下目标。

- 对于信息检索查询结果，要求查询结果必须与原始业务数据保持一致，主题数据量 100 万条以下，响应时间不超过 3 秒；100 万条以上响应时间不超过 5 秒。

- 对于全文检索查询结果，要求查询结果必须与原始业务数据保持一致，主题数据量 100 万条以下，响应时间不超过 3 秒；100 万条以上响应时间不超过 5 秒。
- 对于多维分析结果，要求分析结果必须与原始业务数据保持一致，主题数据量 100 万条以下，响应时间不超过 3 秒；100 万条以上响应时间不超过 10 秒。
- 页面访问的响应时间在 3 至 5 秒内；
- 系统有效工作时间：99.9%；

9.9.2. 数据库性能优化

针对智慧消防云平台的数据库性能优化主要包括以下三个方面措施：

- 查询 SQL 执行计划优化
- 数据库性能优化
- 数据存储优化

9.9.2.1. 查询 SQL 执行计划优化

应用对数据库操作的方式通过SQL脚本进行,SQL的解析将按照特定的规律进行，不同的执行计划将产生性能差异巨大的结果。所以 SQL 代码优化极为重要。

使用 CBO（基于成本的优化器）对查询 SQL 语句进行优化。基于成本的优化器是一组例程，它有助于选取满足传递给 Oracle SQL 引擎做处理查询所需数据的最佳存取路径。存取路径是 Oracle 根据对象上的索引和相关的统计数据所选取的汇集、组装查询结果的方法。对于处理海量数据的数据库,CBO 是唯一的查询优化方法。Oracle 的 SQL 优化策略分为基于规则、基于成本、选择性三种，在缺省情况下，Oracle 采用选择性优化器， 为了避免那些不必要的全表扫描，必须尽量避免使用选择性优化器，而直接采用基于规则或者基于成本的优化器。

此外，还可使用 Trace（跟踪）手段对 SQL 语句进行动态追踪，以尽量出现避免全表扫描等过于耗费系统资源的动作。

9.9.2.2. 数据库性能优化

数据库级的性能优化是建立在数据库正常营运后，一段时间的性能监控和跟踪基础上的。而对于性能优化来说，最有效的方法是加更多（add more）和使更大(make it bigger)。主要从表空间监测、sga 区监测、I/O 使用情况、redo log 使用情况等方面入手来进行调整。

- **表空间的优化**

表空间优化主要是确保数据文件有足够的剩余空间，对碎片进行定时的清理。

- 经常监控数据文件的使用情况，对于快要写满的数据文件应该及时的增加空间；
- 使用 oracle 对于数据段的自动管理功能，减少碎片产生的机会；
- 经常监测碎片。Oracle 本身由 smon 进程来自动处理碎片。但是运行一段时间后，某些物理文件的碎片是在所难免的。当表空间碎片过多时，可以使用命令 alter tablespacets_qbk coalesce；命令（ts_qbk 是表空间名）或者更好的方法是采取导出数据后重建数据文件再导入的方式来确保碎片的消除；
- 设置足够大的临时表空间和重作表空间（undo_tablespace）。对于重作表空间，应该经常监测。当频繁出现快照过久的错误时，可以增大回滚表空间，或者调大 undo_retention 参数。

- **SGA 区优化**

建立在对空闲内存的监测，数据块存命中率，共享池使用效率及等待事件的监测基础上的。

- 监测 SGA 区中各部分内存的使用情况，对于会经常大量空闲内存的区域，可以将其分配给那些占用比率很高的区域；
- 数据块缓存（data buffer）命中率标示数据库中的数据在内存中的使用效率。为了提高命中率，应该定时的将 DB_CACHE_ADVICE 设置为 true，运行一段

时间后再通过 V$DB_CACHE_ADVICE 视图来获得最佳的数据块缓存大小。另外定时的监控数据块缓存的命中率，当命中率过低时考虑调大数据块缓存；

- 共享池的调整可以参考 V$SHARED_POOL_ADVICE 来进行调整。当字典缓冲区命中率太低时候，可以通过增加共享区内存来提高命中率；
- 经常监测系统中的等待事件，并分析这些等待时间的原因，以调整参数来避免不必要的等待。

➢ I/O 性能优化

I/O 可能是最影响系统性能的因素。合理的布局数据存储，设置表的存储参数，对热点数据固化到内存的处理，以提高 I/O 的性能。

- 合理布局数据存储，尽量保证把可能并发的数据放在不同的物理空间中。例如把索引表空间与数据表空间放在不同的物理磁盘上；
- 跟踪热点数据，将查询经常会用到并且又不是太大的表，可以放在固化的那部分内存中（buffer_pool），或者使用 cache 参数；
- 为避免行迁移和行链接，对于经常可能更新的表设置更大的 pctfree 参数，对于很少用于更新的数据，减少 pctfree 参数。

➢ Redo log 文件的性能优化

当数据库受到日志切换时间影响时，增加 log 文件的大小或者增加 log 文件的成员。这项优化一般在系统安装时进行调整。

➢ Alter.log 文件的整理

Alter.log 文件包含大量数据库的运转信息。应该定时的清理和分析 alter.log，对于严重影响系统及性能方面的问题应该及时给予处理。此外，在处理完成后，应该把 alter.log 删除掉。

9.9.2.3. 数据存储优化

数据存储优化主要从分区存储、合理调整表和索引的存储位置、启用自动回滚段管理、临时段平衡几个方面进行优化。

- **分区存储**

分区存储在管理的方便性和性能的提高上都有较强的实用性，甚至可以认为分区是提高与大型表有关的性能的最佳方法。通过访问一个表或者索引的较小片段，而不是访问整个表或索引，分区可以很好地提高效率。通过将一个表或者索引的分区建在不同的磁盘上可以大大增加数据吞吐量，获得很好的数据库性能。

- **合理调整表和索引的存放位置**

因表和索引的数据块通常是被同时读取的，所以尽量将表和其相关联的索引分别放置在不同的磁盘上，以便减少文件的 I/O 冲突，达到提高数据访问速度的目的。

- **启用自动回滚段管理**

在 Oracle 数据库中，使用自动回滚段管理可以大幅度提高回滚段的管理效率和准确度，而无须关心用户使用回滚段的频度。只需定期或者不定期检查当前回滚段的使用和分配情况即可。

- **临时段平衡**

当初始化参数中定义的 SORT_AREA_SIZE 大小无法满足排序要求的空间，Oracle 数据库系统就会使用临时表空间中的临时段进行排序，磁盘上排序比内存排序要慢 100-10000 倍，所以尽量减少磁盘排序是性能优化工作的重要部分。

临时段平衡就是将临时表空间中的多个临时数据文件分布在不同的磁盘上，以减少排序时可能会产生的磁盘冲突。

9.9.3. 应用服务器性能优化

智慧消防云平台的应用服务器性能优化主要通过在中间件软件服务中进行数据

源连接池、JAVA 虚拟机堆栈、线程池、负载均衡等方面进行优化。

9.9.3.1. 数据源连接池

一个与后台数据库密切相关的应用系统，其最大的系统开销便是频繁地与数据库间连接的取得和断开。通过在应用服务器上建立包含一定数目预置连接的数据库连接池，可以避免频繁创建和关闭数据库连接，提高系统运行效率，特别是在多个用户并发访问的时候。在建立连接池的过程中，本方案尤其重视对参数的有效设置，如连接的最大空闲时间等，力求在应用系统高效运行和后台资源最低浪费之间取得平衡。

9.9.3.2. Java 虚拟机堆栈

由于 Java 程序运行过程中的所有内存均从 Java 虚拟机堆栈中分配得到内存单元，因此要适度地调大默认的 Java 虚拟机堆栈，并且将最大堆栈和最小堆栈设置为同一个值以免在运行期动态增长内存耗费额外的资源。

9.9.3.3. 线程池

智慧消防云平台上各种的程序组件尽可能设计成多线程模式。在应用服务器中由线程池统一管理线程的创建、运行和销毁。线程池是服务器端处理大量客户端访问的时候普遍采用的一种方式，在 Web 容器中表现尤为重要，当一个客户端访问某一 Web 组件的时候，容器就要运行一个线程。当用户多的时候，频繁的线程开启和关闭往往容易引起系统的崩溃，线程池的作用就是线程的预先开启建池，使用的时候分配管理，从而避免了上述问题。

9.9.3.4. 负载均衡

建立集群的作用在于分担大访问量，使得每一台成员服务器（主机或虚拟主机）发挥最大性能，以充分挖掘软、硬件潜力，即实现负载均衡。

9.9.4. 应用软件性能优化

智慧消防云平台的应用软件性能优化主要从关联算法、信息代码和元数据缓存、

控制结果集、多线程机制、运行期参数据调整等方面进行优化。

9.9.4.1. 关联算法的优化

从理论上而言，任意两张表间的关联有多种方法，如常用的 Merge Join、Nested-loop Join、Hash Join 等方法。每种方法均有其适用的环境，各有优缺点，不同的关联方法在实现具体 SQL 功能时，性能可能有数十倍甚至上百倍的差异。如果同时关联的数据表多，关联的先后顺序也将变得很重要，不同顺序所导致的差异更大。因此数据关联方式的选择需要了解待关联表的索引情况、数据分布的统计信息等资料来决定。

9.9.4.2. 信息代码和元数据缓存

元数据是存放管理员配置整个消防行业信息查询系统的信息存放场所，是应用系统基于配置运行的关键。信息代码和元数据虽然也在数据库中的，但是由于它们属于公用信息，访问量很大，改动次数却很少，因此将它们作为系统缓存的一部分，使应用程序在需要用到它们时能直接通过内存来获得，而不必频繁地访问数据库。

9.9.4.3. 控制结果集规模

在显示某用户授权范围内的查询项目，以及对应不同登录用户实现条目密级控制的时候都要涉及到用户权限的校验，若每次都从数据库中读取的话，在用户多的情况下会给数据库带来明显负担，而通过缓存的方式将使访问效率得到提高。

9.9.4.4. 多线程机制

智慧消防云平台上的各项应用功能是基于 J2EE 规范实现的，因此在代码级别上可充分利用 J2EE 平台内置的多线程模式。服务器端程序尽可能实现多线程接口，配合应用服务器的线程池，在运行性能上达到最佳。

9.9.4.5. 运行期参数调整

在系统运行期，需要对某些应用系统参数提供动态调整的机会。例如系统日志输出会占用部分 I/O 资源，所以管理员可视情况进行动态调整。

9.9.5. 数据缓存优化

智慧消防云平台数据缓存优化目的在于提高访问命中率。以下将从数据库、Web服务器、应用软件层面阐述数据缓存优化。

9.9.5.1. 数据库共享池

与数据库共享池相关的几个概念列举如下：

- SHARED_POOL_SIZE：这个参数指定了共享池的大小，单位是字节。
- SHARED_POOL_RESERVED_SIZE：指定了为共享池内存保留的用于大的连续请求的共享池空间。当共享池碎片强制使 Oracle 查找并释放大块未使用的池来满足当前的请求的时候，这个参数和 SHARED_POOL_RESERVED_MIN_ALLOC 参数一起可以用来避免性能下降。这个参数理想的值应该大到足以满足任何对保留列表中内存的请求扫描而无需从共享池中刷新对象。既然操作系统内存可以限制共享池的大小，一般来说，你应该设定这个参数为 SHARED_POOL_SIZE 参数 10% 大小。
- SHARED_POOL_RESERVED_MIN_ALLOC：这个参数的值控制保留内存的分配。如果一个足够尺寸的大块内存在共享池空闲列表中没能找到，内存就从保留列表中分配一块比这个值大的空间。默认的值对于大多数系统来说都足够了。如果你加大这个值，那么 Oracle 服务器将允许从这个保留列表中更少的分配并且将从共享池列表中请求更多的内存。

从理论上讲，对于在共享池中要求大于 100K 连续空间的数据库对象，应考虑是否将其固定在系统全局区域中的共享池中，是的话就将需要频繁使用的表放置到另外一个独立的 Buffer Cache 中。这种设定可以使这些表的数据不至于很快被清除出 Default Buffer Cache。

9.9.5.2. Web 服务器均衡负载

通过增加 Web 服务器数量提高服务的吞吐量，访问请求通过均衡负载器按照设定的负载均衡策略分配到 Web 服务器群，Web 服务器可以实现异构平台的集群，以保

证在 Web 服务层面的高可用性和扩展性。

当一台 Web 服务器或一组服务器的负荷增加时，做为此层面的负载均衡组件——边缘服务器组件会自动重定向新的访问流量到更轻松的或者缓存着请求目标资源的服务器，从而保证了对用户最快速的响应。此外，边缘服务器组件的缓存功能可以用来加速客户响应时间，减轻系统压力。所要求边缘服务器组件应可以支持对不同操作系统下的 Web 服务器的负载平衡。

9.9.5.3. 应用软件的数据缓存设计

智慧消防云平台上各应用功能设计实现中可根据情况采取数据缓存设计来提升应用响应速度，例如：对常用的信息代码、元数据等，这里仅应用软件对查询结果集的缓存设计为例说明。

用户对每次查询之后得到的结果集可能进行分页、分组、排序、过滤等二次操作处理。信息查询功能设计上可采用以一次简要信息查询为单位，将私有于某用户的结果集作为他与服务器建立会话所维护的一种状态信息，存储于 Web 容器之中。这样，用户在对现有结果集进行排序、过滤等操作时将不必再次访问数据库，而只需在内存中进行，这将大大的提高响应速度、节省系统资源。

9.10.防雷、消防设计

本次福建省智慧消防云平台软硬件部署将依托于福建省政务云平台，所使用云平台虚拟服务器资源等均由省级政务云平台提供分配。目前福建省政务云平台已按照国家标准建立计算机专用机房，已考虑防雷和消防设计。

因此，本次智慧消防云平台设计规划不再赘述平台的防雷与消防设计。

9.11.节能措施

福建省智慧消防云平台属于信息系统开发建设项目，项目本身不产生环境污染问题，购置的电子设备的电磁辐射技术指标都要求在国家强制规定范围以内。

本项目配置的软硬件设备在满足系统功能与性能要求的同时，符合国家有关节能政策的规定，并尽量降低设备的功率消耗，优先考虑选用节能型设备，以控制能

耗。

由于计算机机房设施和信息系统为每天 24 小时连续运行，所以机房节能问题较为突出。机房主要节能措施如下：

（1）加强机房门、窗的密封处理；

（2）选用高能效比的机房设备，降低设备电能能耗；

（3）在日常工作中，尽可能减少进出机房的次数，及时关闭机房照明，以减少机房耗能。

9.12.环境评价

1．环境影响分析

本项目的计算机网络建设属于无污染工程，在建设与运行过程中对周围环境基本不造成污染，项目运行过程中没有有害气体、废渣、废水排出，不会污染环境，所采用的设备也不产生超过国家强制规定范围外的电磁污染、设备噪声源。

2．环保措施及方案

本项目建设使用的设备基本属于电子设备，运行无污染且能耗较小。在项目实施中，将严格遵守国家有关规定，选择能耗低、可靠性高的设备，以控制能耗。

3．职业安全和卫生措施

工程应符合国际环保管理标ISO14001及国际职业安全卫生管理标准OHSAS18001两个体系的标准。

第10章　系统安全总体设计

福建省智慧消防云平台安全系统建设的原则，是要从实际工作需求出发，建设符合要求又满足实际需求的安全系统。

10.1.安全域设计

安全域的设计是以信息系统为核心，分析信息系统的存储、交换和使用环境，确定信息的共享范围、交换路径和存储区域，原则上同一类信息存储、交换和使用的信息设备(包括终端设备、存储设备、网络设备和应用服务器等)都应该划分为同一个安全域。所有安全域可以再细分，划分成安全子域。

10.1.1. 安全域设计基本原则

安全域设计的基本原则如下：

（1）业务保障原则：安全域方法在保证安全的同时，还要保障业务的正常和高效运行。

（2）结构简化原则：安全域划分并不是粒度越细越好，否则可能导致安全域的管理过于复杂和困难。

（3）分级保护原则：安全域的划分要做到每个安全域的信息资产具有相同或相近的密级分级、安全环境、安全策略等。

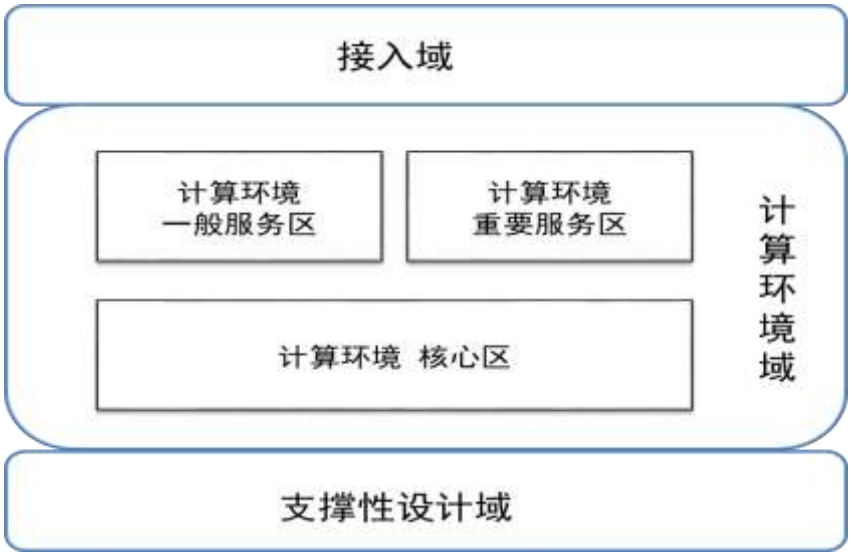
（4）一体化协防原则：安全域的主要对象是网络，但是围绕安全域的防护需要考虑在各个层次上一体化防护，包括物理安全、网络安全、系统安全、防病毒、CA认证、容灾备份等电子政务网络的整体安全环境。

10.1.2. 安全域划分

安全域是指同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络，划分的目的是把一个大规模复杂系统的安全问题，化解为更小区域的安全保护问题，是实现大规模复杂信息系统安全等级保护的有效方法。每一个逻辑区域内有相同的安全保护需求，具有相同的安全访问控制和

边界控制策略。区域间具有相互信任关系，相同的网络安全域共享同样的安全策略。安全域的划分不能单纯从安全角度考虑，而是应该以业务角度为主，辅以安全角度，并充分参照现有网络结构和管理现状，才能以较小的代价完成安全域划分和网络梳理，而又能保障其安全性。

10.1.3. 安全域参考模型



10.2.信息系统安全等级保护

10.2.1. 信息系统安全等级保护概述

信息系统根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高划分为五级。

根据等级保护相关管理文件，信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

10.2.2. 安全体系需求

10.2.2.1. 安全体系需求

由于“黑客”、计算机病毒、信息间谍等对网络安全构成越来越严重的威胁，网络安全也成为网络应用的必需手段，以保护网络传输的数据的安全性和完整性。加强福建省互联网＋大数据辅助领导科学决策的安全建设，以实现对系统实体安全、网络安全、信息安全、系统安全、运行安全实施安全管理。

针对福建省智慧消防云平台信息化应用，主要存在的安全需求包括如下几个方面：

（1）符合相关政策文件安全需求

根据国务院办公厅《国家网络与信息安全事件应急预案》（国办〔2008〕168 号）、省政府办公厅《福建省网络与信息安全事件应急预案》（闽政办〔2010〕19 号），开展网络与信息安全事件应急处置工作，构建福建省消防救援总队中心网络与信息安全应急处置体系，进一步提高福建省消防救援总队信息安全事件的预警、分析和应急处置能力。

《福建省人民政府关于印发加快推进“互联网+政务服务”工作方案的通知》（闽政〔2016〕66 号）中的“继续完善网络与信息安全应急处置平台，开展全省网络安全事件统一监测、通报、响应和处置；扩大政务外网云安全监测平台的监测范围，完成省级、市级和部门政务云平台统一安全监测，扩展和升级云平台脆弱性检测系统和安全监控系统，完善福建省智慧消防云平台安全保障体系”的要求。

（2）符合等级保护基本需求

1）系统的设计不能为病毒提供后门；

2）防止黑客对福建省智慧消防云平台的恶意攻击；

3）需保证网络数据传输的安全性、保密性。

4）系统必须备有较强的系统安全性和灾难恢复能力。

5）解决好信息共享与安全、完整性的关系；开放性与保护隐私的关系；互联性与物理、逻辑隔离的关系。

10.2.2.2. 信息系统安全等级预评估步骤

为确定信息系统的安全保护等级，首先要确定信息系统内各业务子系统在 4 个定级要素方面的分析，然后分别由 4 个定级要素确定业务信息安全性和业务服务保证性两个定级指标的等级，再根据业务信息安全性等级和业务服务保证性等级确定业务子系统安全保护等级，最后由信息系统内各业务子系统的最高等级确定信息系统的安全保护等级。

具体步骤如下图所示：

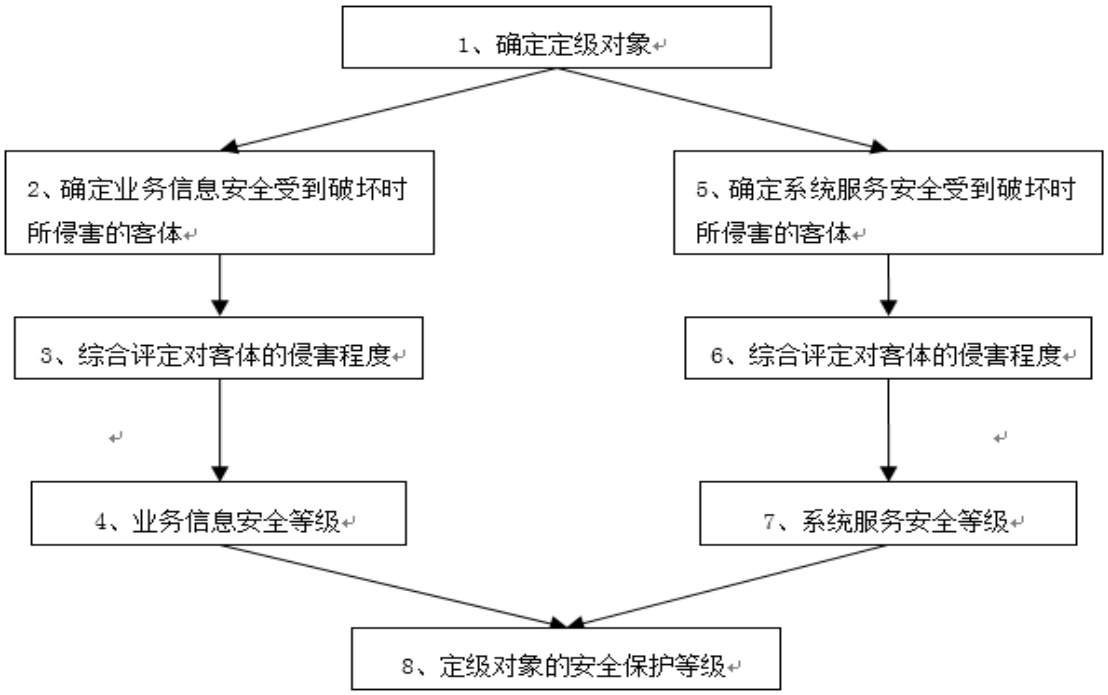


图 等级确定流程

10.2.2.3. 受侵害的客体及对客体的侵害程度

定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。

（1）侵害国家安全主要是指影响国家政权稳固和国防实力、民族团结和社会安定、重要的安全保卫工作、经济竞争力和科技实力等；

（2）侵害社会秩序主要是指影响国家机关社会管理和公共服务的工作秩序、各种类型的经济活动秩序等；

（3）影响公共利益主要是指影响公共设施、公开信息资源、公共服务等方面；

（4）影响公民、法人和其他组织的合法权益是指由法律确认的并受法律保护的公民、法人和其他组织所享有的一定的社会权利和利益。

不同危害后果的三种危害程度描述如下：

（1）一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害。

（2）严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较严重损害。

（3）特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常严重损害。

10.2.2.4. 信息系统安全等级预评估

10.2.2.4.1. 业务信息安全性等级分析

福建省智慧消防云平台各应用系统的数据信息，一旦遭受入侵、修改、增加、删除等不明侵害，可能影响正常工作的开展，造成信息泄露，会对社会秩序、公共利益造成一般损害。

因此，根据业务信息安全性等级矩阵表，业务信息安全性等级为：3 级。

表 业务信息安全性等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
国家安全	第三级	第四级	第五级

10.2.2.4.2. 系统服务安全性等级分析

福建省智慧消防云平台应用被破坏，可能会对社会秩序、公共利益造成一般损害；

根据下列系统服务安全性取值矩阵表，该系统平台的安全保护等级为：3 级。取值矩阵如下表所示：

表 系统服务安全性取值矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

系统的安全保护等级由业务信息安全性等级和系统服务安全性等级较高者决定。

因此，系统的安全保护等级为：三级。

10.2.2.5. 安全等级保护建设需求

为了保证福建省智慧消防云平台的安全，按《信息安全等级保护基本要求》三级系统的安全标准，完善配置并构建成福建省智慧消防云平台统一的信息安全防护系统是必需的。

10.3. 安全体系结构规划

安全系统建设的原则，一是必须符合国家电子政务安全规划及国家的其他相关规定，二是要从网上业务的实际工作需求出发，建设既符合要求又满足实际需求的安全系统。

安全系统建设的重点是，确保信息的安全，确保业务应用过程的安全防护、身份识别和管理。安全系统建设的任务，需从技术和管理两个方面进行安全系统的建设。基本技术要求从物理安全、网络安全、主机安全、应用安全和数据安全几个层面提出；基本管理要求从安全管理制度、人员安全管理、系统建设管理和系统运维管理几个方面提出，基本技术要求和基本管理要求是确保信息系统安全不可分割的两个部分。

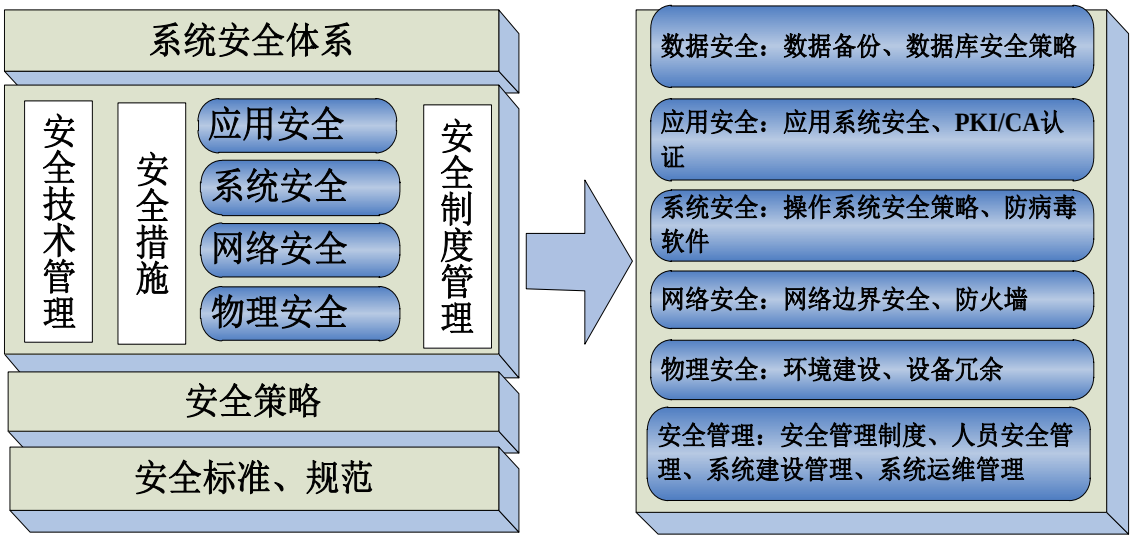


图 系统安全体系结构

10.4.安全等级保护建设要求

为了保证本项目安全稳定运行，根据《信息系统安全等级保护基本要求》中的第三级要求进行设计，提供多层次的全面信息保护与网络安全应用解决方案，安全建设目标划分为技术和管理两部分。

10.4.1. 技术目标

从安全体系上考虑，实现多种安全技术或措施的有机整合，形成一个整体、动态、实时、互动的有机防护体系。具体包括：

（1）本地计算机安全：主机系统文件、主机系统的配置、数据结构、业务原始数据等的保护。

（2）网络基础设施安全：网络系统安全配置、网络系统的非法进入和传输数据的非法窃取和盗用。

（3）边界安全：横向网络接入边界，内部局域网不同安全域或子网边界的保护。

（4）业务应用安全：业务系统的安全主要是针对应用层部分。应用软件的设计是与其业务应用模式分不开的，同时也是建立在网络、主机和数据库系统基础之上的，因此业务部分的软件分发、用户管理、权限管理、终端设备管理需要充分利用相关的安全技术和良好的安全管理机制。

10.4.2. 管理目标

一套完整的安全解决方案必须配备相应的管理制度。因为完美的安全系统是建立在用户特定的管理运行模式中的，没有严格的管理规范和管理制度，再完美的设计和昂贵的设备都没用的。建立全面的安全运行维护服务，以保障系统安全、高效运转的需要。

安全建设管理目标就是根据覆盖信息系统生命周期的各阶段管理域来建立完善的信息安全管理体系，从而在实现信息能够充分共享的基础上，保障信息及其他资产，保证业务的持续性并使业务的损失最小化，具体的目标如下：

（1）定期对局域网网络设备及服务器设备进行安全隐患的检查，确保所有运行的网络设备和服务器的操作系统安装了最新补丁或修正程序，确保所有网络设备及服务器设备的配置安全。

（2）提供全面风险评估、安全加固、安全通告、日常安全维护、安全应急响应及安全培训服务。

（3）对已有的安全制度，进行更加全面的补充和完善。

（4）应明确需要定期修订的安全管理制度，并指定负责人或负责部门负责制度的日常维护。

（5）应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告。

（6）应通过第三方工程监理控制项目的实施过程。

10.5.政务外网/互联网安全需求分析

10.5.1. 系统定级建议

信息系统定级是进行等级保护设计的首要环节，根据国家信息安全等级保护实施指南，信息系统定级阶段的目标是信息系统运营、使用单位按照国家有关管理规范和 GB/T 22240—2008，确定信息系统的安全保护等级，信息系统运营、使用单位有主管部门的，应当经主管部门审核批准。

智慧消防云平台信息安全等级保护的总体思路是：以自身的信息系统特点为核心，结合国家相关标准要求，根据省消防救援总队实际业务需求，和对实际业务的影响来划分安全等级，在确定定级方面更重视系统对消防业务开展的影响性而确定等级，目的只是为体现对不同等级的信息系统，如何加强保护措施方面。而不是根据国家标准，严格地评估信息系统受到破坏后的影响范围和影响程度而确定。

10.5.1.1. 确定定级对象

根据公安部的《信息安全等级保护定级指南》指出作为定级对象的信息系统应具有如下基本特征：

- **具有唯一确定的安全责任单位**

作为定级对象的信息系统应能够唯一地确定其安全责任单位。如果一个单位的某个下级单位负责信息系统安全建设、运行维护等过程的全部安全责任，则这个下级单位可以成为信息系统的安全责任单位；如果一个单位中的不同下级单位分别承担信息系统不同方面的安全责任，则该信息系统的安全责任单位应是这些下级单位共同所属的单位。

- **具有信息系统的基本要素**

作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的有形实体。应避免将某个单一的系统组件，如服务器、终端、网络设备等作为定级对象。

- **承载单一或相对独立的业务应用**

定级对象承载“单一”的业务应用是指该业务应用的业务流程独立，且与其他业务应用没有数据交换，且独享所有信息处理设备。定级对象承载“相对独立”的业

务应用是指其业务应用的主要业务流程独立，同时与其他业务应用有少量的数据交换，定级对象可能会与其他业务应用共享一些设备，尤其是网络传输设备。

对于智慧消防云平台，根据承载业务的独立性，以业务系统为核心来划分定级对象，并针对不同的业务系统来设计保护措施，确定的保护对象分别为：《福建省智慧消防云平台》。

此外，福建省智慧消防云平台中还包括了安全管理区域的安全管理系统和终端办公区域的终端系统，由于福建省智慧消防云平台未来还会增加其他信息系统，而这些终端及安全管理设备会与多个系统相连，无法做到不同的信息系统使用专用的设备，因此建议将安全管理系统和终端系统划分为其他的信息系统，不作为定级对象，但在安全管理服务器区域、终端区域和服务器区域间建立边界保护，并通过身份鉴别和访问控制等措施加以控制。

10.5.1.2. 外网网站防护等级定级

10.5.1.2.1. 福建省智慧消防云平台系统描述

福建省智慧消防云平台是作为福建省消防救援总队面向全省各级消防行政监管部门、消防火灾风险单位、业主单位、社会公众的综合性应用管理与信息发布平台。网站提供权威、准确、全面、快速的信息服务和公众互动功能，起到政策、指令快速发布、下情及时上达的作用。平台主要包括省市县三级通用业务系统、消防物联网感知网设备接入管理系统、消防大数据中心等系统或功能模块。

福建省智慧消防云平台建成后将部署于省电子政务云计算平台，通过政务外网和互联网供消防行政机构人员、消防服务机构人员、社会公众等进行业务操作、数据浏览查询以及互动交流。省电子政务云计算平台，已具备全套完善的网络安全防护设备和安全防护机制，且符合计算机信息系统等级保护（三级）的标准，因此智慧消防云平台除自身软件安全设计与开发须符合等级保护标准外，其余系统层、硬件层、网络层等的安全防护均依托与省电子政务云计算平台现有安全防护体系。

福建省消防救援总队承担着福建省智慧消防云平台的安全防护责任。

10.5.1.2.2. 福建省智慧消防云平台安全保护等级确定

福建省智慧消防云平台系统受到破坏时，对信息安全的危害方式表现为对其业务信息安全的破坏和对信息系统服务的破坏。其中信息安全是指确保信息系统内信息的保密性、完整性和可用性等；系统服务安全是指确保信息系统可以及时、有效地提供服务，以完成预定的业务目标。

由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，分别从业务信息安全和信息系统服务安全两方面评定对客体的侵害程度，确定定级对象的安全保护等级。

（一）业务信息安全保护等级的确定

1、业务信息描述

福建省智慧消防云平台主要处理的业务信息为消防业务长传下达信息、消防业务管理信息、消防专题信息、消防宣传服务信息、消防动态监测信息等。

2、业务信息受到破坏时所侵害客体的确定

福建省智慧消防云平台是面向社会公众提供消防监管和服务相关信息服务，并且作为对外信息发布的窗口，因此其业务信息安全受到破坏时所侵害的客体是社会秩序和公共利益，影响社会成员使用消防相关公共设施、获取消防公开信息资源、接受消防相关服务等，以及其他影响公共利益的事项。

3、信息受到破坏后对侵害客体侵害程度的确定

福建省智慧消防云平台系统业务信息安全受到破坏时，福建省消防救援总队及各支队、大队的工作职能受到严重影响，严重影响其信息获取服务和信息发布，会对全省各级消防监管部门公信度造成负面影响，同时会造成较大范围的社会不良影响。因此确定其侵害程度为严重损害。

4、业务信息安全等级的确定

业务信息安全受到破坏时，受到影响的客体是社会秩序、和公共利益。侵害程度为严重损害，根据表 1，确定该系统的信息安全保护等级为第三级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级

社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

（二）系统服务安全保护等级的确定

1、系统服务描述

福建省智慧消防云平台的服务范围包括内部工作人员、消防服务单位、消防联网火灾风险单位、外部社会公众等，主要作为消防日常业务管理和消防数据采集分析用途以及对外信息发布的平台。

2、系统服务受到破坏时所侵害客体的确定

福建省智慧消防云平台系统是面向内部工作人员、消防服务单位、消防联网火灾风险单位、外部社会公众等提供消防监管、消防服务、消防宣传、消防教育培训等信息查询服务，并且作为对外信息发布的窗口，因此其信息系统服务安全受到破坏时所侵害的客体是社会秩序和公共利益，影响社会成员使用消防相关公共设施、获取消防公开信息资源、接受消防相关信息服务等，以及其他影响公共利益的事项。

3、系统服务受到破坏后对侵害客体的侵害程度

福建省智慧消防云平台系统信息系统服务安全受到破坏时，将会影响各级消防部门内部工作人员、消防服务单位、消防联网火灾风险单位、外部社会公众对系统的使用，影响各项消防相关工作业务信息查询工作、信息发布工作的顺利完成。因此确定其侵害程度为一般损害。

4、系统服务安全等级的确定

信息系统服务安全受到破坏时，受到影响的客体是社会秩序和公共利益。侵害程度为一般损害，根据表 2，确定该系统的系统服务安全保护等级为第二级。

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

（三）安全保护等级的确定

信息系统的安全保护等级由业务信息安全等级和系统服务安全等级较高者决定。根据表 3，最终确定该系统的安全保护等级为第三级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级

福建省智慧消防云平台	第三级	第三级	第二级

最终确定的智慧消防云平台系统保护强度为 3 级，且对应等级保护要求选择措施为：S3A2G3。

10.5.2. 安全需求分析

10.5.2.1. 符合等级保护技术要求的需求

根据确定的定级对象及定级建议，参考《信息系统安全等级保护基本要求》中对各子系统提出的安全建设要求，从符合性的角度福建省智慧消防云平台各应用系统的技术防护需求包括：

10.5.2.2. 智慧城市应用系统

系统定级为 3 级，且等级保护要求选择为 S3A2G3，查找《信息系统安全等级保护基本要求》得到该系统的具体技术要求选择，以及差异性需求包括：

防护层面	要求选择	差异性需求
物理安全	物理位置的选择（G3）	机房建设（应按照 3 级机房标准或达到 GB9361-1988《计算机场地安全要求》中的 A 类机房的指标进行建设）
	物理访问控制（G3）	
	防盗窃和防破坏（G3）	
	防雷击（G3）	
	防火（G3）	
	防水和防潮（G3）	
	防静电（G3）	
	温湿度控制（G3）	
	电力供应（A2）	
	电磁防护（S3）	
网络安全	结构安全（G3）	应实现网络层面的加固，确保网络能够更好地支撑应用系统的运行
	访问控制（G3）	利用访问控制措施实现基于网络 IP 地址、协议、端口的强访问控制，并支持针对用户的访问控制

防护层面	要求选择	差异性需求
	安全审计（G3）	应实现对网络设备的运行状况日志审计、流量审计等，应实现对日志信息的集中记录
	边界完整性检查（S3）	应防范非法的内联和外联
	入侵防范（G3）	应实现有效的网络入侵防范
	恶意代码防范（G3）	应对蠕虫类恶意代码进行过滤防护
	网络设备防护（G3）	网络设备应采取加固措施
主机安全	身份鉴别（S3）	操作系统和数据库应采取加固技术
	访问控制（S3）	操作系统和数据库应进行加固
	安全审计（G3）	应对关键的服务器配置日志审计措施，
	剩余信息保护（S3）	应通过对服务器的核心加固，防范客体重用，实现剩余信息保护
	入侵防范（G3）	通过操作系统加固来实现部分入侵防范
	恶意代码防范（G3）	实现基于主机的防病毒
	资源控制（A2）	实现对主机资源的限制和保护
应用安全	身份鉴别（S3）	应实现高强度的身份认证技术
	访问控制（S3）	应实现针对应用系统的授权和严格的访问控制
	安全审计（G3）	应对应用系统实现有效安全审计，并防范审计记录被非法修改和删除
	剩余信息保护（S3）	应用系统应当对缓存信息和临时信息进行有效保护，在注销当前用户时应当进行有效清除
	通信完整性（S3）	应采用 SSL 协议来实现通信数据的完整性保护
	通信保密性（S3）	应采用 SSL 协议来实现通信数据的保密性保护
	抗抵赖（G3）	应在应用系统中设计实现防范操作抵赖行为
	软件容错（A2）	应用软件对错误的输入有控制
	资源控制（A2）	应针对应用服务器进行连接数的限制
数据安全	数据完整性（S3）	应当保障业务数据在存储和传输过程中的保密性
	数据保密性（S3）	应当保障业务数据在存储和传输过程中的完整性
	备份和恢复（A2）	采用双机热备措施，关键网络设备、通信线路和数据处理系统应有冗余设计

10.5.2.2.1. 二级系统区域

对于定为 2 级的系统区域，等级保护要求选择为 S2A2G2，查找《信息系统安全等级保护基本要求》得到该区域的具体技术要求选择，以及差异性需求包括：

防护层面	要求选择	差异性需求
物理安全	物理位置的选择（G2）	机房建设（按照2级机房标准或达到GB9361-1988《计算机场地安全要求》中的B类机房的指标进行建设）
	物理访问控制（G2）	
	防盗窃和防破坏（G2）	
	防雷击（G2）	
	防火（G2）	
	防水和防潮（G2）	
	防静电（G2）	
	温湿度控制（G2）	
	电力供应（A2）	
	电磁防护（S2）	
网络安全	结构安全（G2）	应实现网络层面的加固，确保网络能够更好地支撑应用系统的运行
	访问控制（G2）	利用防火墙实现基于网络IP地址、协议、端口的强访问控制，并支持针对用户的访问控制
	安全审计（G2）	应对网络的运行状态进行审计，并采取审计平台对记录进行单独保存
	边界完整性检查（S2）	应限制私自外联的行为
	入侵防范（G2）	应实现有效的网络入侵防范
	恶意代码防范（G2）	应在网络边界处对蠕虫类恶意代码进行过滤
	网络设备防护（G2）	网络设备加固
主机安全	身份鉴别（S2）	应进行服务器加固、数据库加固，实现高强度的口令加固
	访问控制（S2）	应进行服务器加固、数据库加固，对登录人员进行访问控制
	安全审计（G2）	应对关键的服务器配置日志审计措施，
	入侵防范（G2）	实现主机入侵防护
	恶意代码防范（G2）	实现基于主机的防病毒
	资源控制（A2）	应对服务器访问数量进行限制
应用安全	身份鉴别（S2）	软件实现身份认证
	访问控制（S2）	软件实现访问控制
	安全审计（G2）	应在应用软件中实现安全审计
	通信完整性（S2）	应在应用软件中对重要数据进行完整性检验
	通信保密性（S2）	应在应用软件中对重要数据机密性传输保护

防护层面	要求选择	差异性需求
	软件容错（A2）	应在应用软件中对输入信息进行控制
	资源控制（A2）	应实现对应用系统的连接控制
数据安全	数据完整性（S2）	应实现对重要数据的机密性保护
	数据保密性（S2）	应实现对重要数据的完整性保护
	备份和恢复（A2）	磁盘备份（数据备份）

10.5.2.2.2. 安全管理系统

福建省智慧消防云平台的安全管理系统包括外网的终端安全管理服务器、网络杀毒管理服务器和网络入侵检测管理服务器组成，其中终端安全管理服务器和网络杀毒管理服务器存在对应用系统的访问。终端安全管理服务器和网络杀毒管理服务器在对应用系统服务器的访问上属于混用模式，无法做到按不同系统进行划分，因此本规划中将安全管理系统视为单独的系统，进行单独的防护，其防护需求包括：

- 对其他系统服务器的访问控制：利用防火墙进行网络层边界防护和访问控制。限制终端安全管理服务器和网络杀毒服务器对应用服务器的访问行为，禁止其他安全管理服务器访问应用服务器；
- 与终端区域之间的访问控制：利用防火墙进行网络层访问控制。限制网络杀毒服务器及终端安全管理服务器与终端区域之间的访问行为，禁止网络入侵检测系统管理服务器对终端区域发起访问；仅允许终端区域的管理维护终端对所有管理服务器的管理访问；
- 对管理服务器的自身防护：应统一部署服务器防病毒系统，并进行管理服务器系统的安全加固配置，提升服务器系统自身的安全性。

10.5.2.2.3. 终端系统

各级消防部门外网的办公终端在对应用系统的访问上属于混用模式，且无专用的管理维护终端（在办公终端上实现管理维护）；无法做到按不同系统使用不同终端进行访问，因此本规划中将终端视为单独的系统，进行单独的防护，其防护需求包括：

- 对其他系统服务器的访问控制：利用现有的防火墙进行网络层访问控制。限制

不同类型的终端对不同的应用服务器进行访问，禁止普通办公终端访问安全管理服务器；对于管理维护终端则在策略上允许对安全管理服务器的维护操作。

- 对应用系统的认证和访问控制：通过应用系统的认证和访问控制功能来实现，根据终端使用者的角色来分配可使用的模块和功能；
- 对终端的自身防护：一方面应统一防病毒系统的型号，改变目前终端防病毒软件不统一，无法进行统一的病毒管理的问题；另一方面利用已部署的北信源终端安全管理平台，来实现终端的健康性检查，包括终端的资产管理、终端自身安全防护、终端行为监管、终端补丁统一升级等，应在现有的终端安全管理平台上安装补丁升级服务器，实现补丁的自动升级；
- 终端的非法接入控制和非法外联控制：利用部署的北信源终端安全管理平台来实现，防止终端私自通过其他方式接入互联网；通过网络设备的端口安全特性结合北信源系统限制非许可的终端接入各级消防部门外网，对消防单位的信息系统造成非法的访问。

10.5.2.3. 符合自身安全防护的需求

各级消防部门外网安全需求可以从管理层、物理层、网络层、系统层、应用层等方面加以分析。

- 在安全管理方面，要考虑政策、法规、制度、管理权限、级别划分、安全域划分、责任认定、安全培训等，制定切实有效的管理制度和运行维护机制；建设支撑安全管理的技术支撑体系；
- 在物理安全方面，要根据实际情况建立相应的安全防护机制；
- 在网络安全方面，要解决各级消防部门外网的安全域划分和逻辑隔离，实现纵深的防御体系；对各个安全域，要防范黑客入侵、身份冒充、非法访问；要解决信息在安全域间传输时的完整性、可用性、保密性问题；要解决移动接入用户身份鉴别和安全传输等问题；
- 在系统安全方面，要解决操作系统安全、数据库安全、病毒及恶意代码防范等问题；
- 从应用安全需求进行分析，要实现全网统一的身份鉴别和授权访问机制；

要解决重要终端用户敏感信息和数据的完整性、可用性、保密性问题，数据的访问控制等问题。

针对福建省智慧消防云平台的安全风险，我们可以得出如下比较详细的安全需求：

10.5.2.3.1. 物理层安全需求

- 应建设安全可靠的机房，提供良好的运行环境，用以支撑重要应用系统的运行，防止电磁信息的泄露、防止设备被盗被破坏；
- 应当评估托管机房的物理安全保障能力，以确保政府网站系统的物理安全防护；
- 建设完备的灾难备份系统，实现系统、数据和应用软件的备份；

10.5.2.3.2. 网络层安全需求

- 实现安全域划分，并在此基础上实现安全、可控的逻辑隔离；
- 对进出各安全域的信息和数据进行严格的控制，防止对安全域的非法访问；
- 对于各个安全域之间交互的信息和数据，保护其完整性、可用性、保密性，防止在传输过程中被窃取、篡改和破坏；
- 在各个安全域内，能及时发现和响应各种网络攻击与破坏行为；
- 升级各类安全系统为最新版本，设置严格的密码策略、用户错误登录次数限制和超时自动退出；
- 设置严格的 IP 访问控制。

10.5.2.3.3. 主机层安全需求

- 建立病毒及恶意代码的预警和响应机制，能及时发现和响应各种病毒及恶

意代码的攻击、破坏和信息泄露行为；

- 使系统内的操作系统能及时升级、安装安全补丁；
- 实现主机操作系统的安全加固；
- 使主机操作系统的内置服务启动最小化 ，应用软件启动账户权限最小化；
- 设置严格的用户登录策略和密码管理策略；
- 使主机操作系统的用户权限最小化，并进行分权管理；
- 启用操作系统的日志审核并进行保存；
- 使用加密通道对主机操作系统进行远程管理，并设置严格的 IP 访问控制策略；
- 设置认证失败处理和超时退出措施；
- 对服务器运行状态进行监控。

10.5.2.3.4. 应用层安全需求

- 对系统、应用、数据库系统进行审计，建立相应的安全审计机制，对引发事件的根源进行责任认定。
- 应用系统应设置登录次数限制，对登录用户进行标识，只允许同一时间同一来源只有该用户登录；
- 应用系统应设置严格的密码管理和访问策略；
- 启用应用系统的日志审核并且进行保存；
- 设置严格的 IP 访问控制策略；
- 设置认证失败处理和超时退出措施；
- 重要应用系统需要设置双因子认证；
- 对应用系统的运行状态进行监控。

10.6.等级保护技术设计解决方案

根据中华人民共和国国家《信息安全技术信息系统安全等级保护定级指南》，福建省智慧消防云平台系统应定级为信息安全等级保护三级。因此下面将根据《信息系统安全等级保护基本要求》，参照《福建省政府信息系统安全等级保护工作实施方案》，并结合福建省消防救援总队应用系统安全的现状，从网络安全、主机安全、应用安全三个方面来设计福建省消防救援总队信息系统等级保护三级技术解决方案。

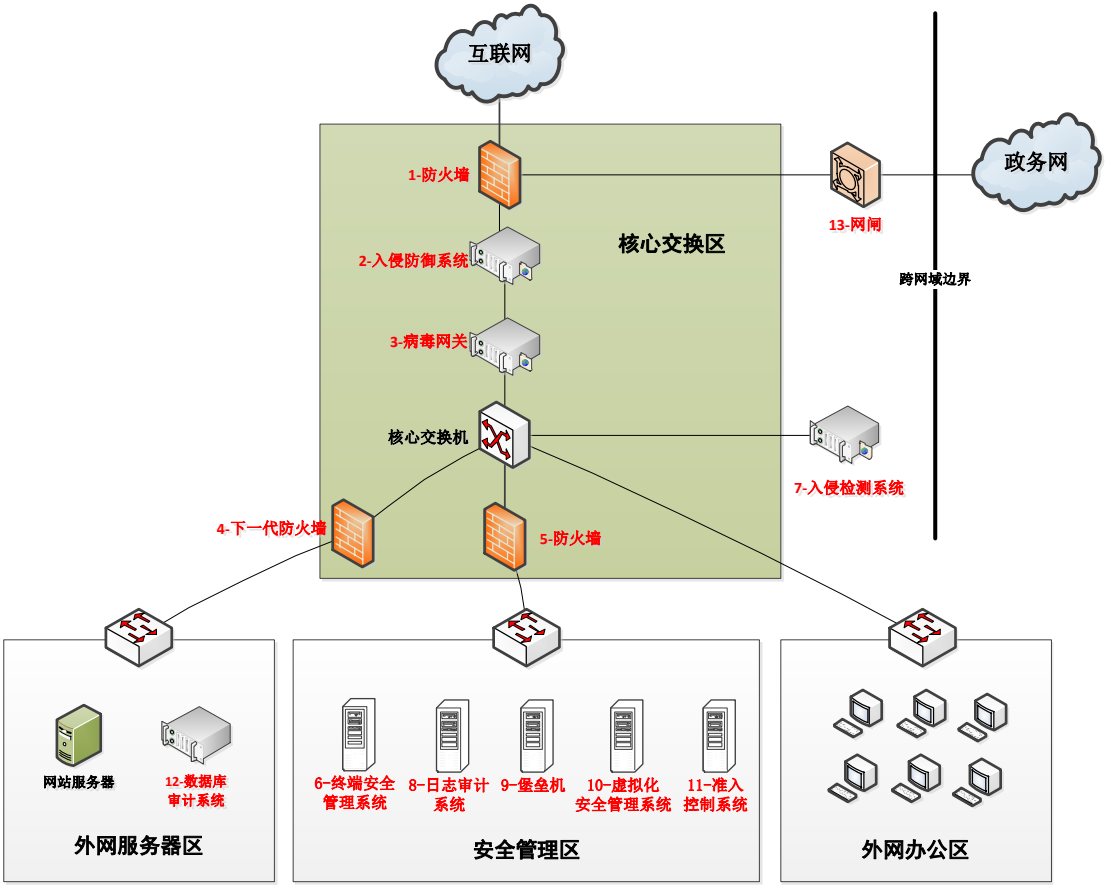
10.6.1. 网络安全域的划分

为实现智慧消防云平台系统的等级化划分与保护，需要依据等级保护的相关原则规划网络的安全区域，并定义各区域的安全级别。对应等级保护的相关要求，按各区域所运行业务系统的安全级别进行对所属网络区域进行定级建设，并在各网络区域中针对业务及应用的类型、特点等因素进行子区域划分，并对各子区域进行分级保护。省总队外网功能区安全等级具体划分如下：

网络区域	功能区	安全等级
省总队外网	核心交换区	3
	外网服务器区	3
	安全管理区	2
	外网办公区	2

10.6.2. 信息系统技术保障体系设计

通过对智慧消防云平台系统的规划，建议按下图所示规划建设智慧消防云平台系统技术保障体系。根据智慧消防云平台系统网络现状的调研以及等保差距分析的结果，结合福建省消防救援总队在网络安全建设的指导意见，安全规划确定总体的安全技术产品包括防火墙、网闸、入侵防御系统、入侵检测、防病毒系统、WEB 应用防火墙、网站安全智能监控系统、运维管控系统、数据库审计系统、日志审计系统。具体如下图所示：



10.6.3. 网络安全建设方案

10.6.3.1. 结构安全

根据各智慧消防云平台系统的重要程度、业务特点以及各处室的工作职能、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，实现对智慧消防云平台系统的安全域划分。不同的安全域之间形成网络边界，通过边界保护，严格规范省总队智慧消防平台各个系统内部之间的访问，防范不同网络区域之间的非法访问和攻击，从而确保智慧消防云平台各个区域的有序访问。

一般来说边界防护采用的主要技术包括防火墙技术、三层交换机技术、流控技术、VPN 技术等。本次方案设计建议在核心交换接入的边界、外网的服务器区以及安全管理区部署防火墙产品，在省消防救援总队外网接入的边界部署网闸产品，实现网络边界以及重要网段的安全隔离。

10.6.3.2. 访问控制

在智慧消防云平台系统网络中，需要部署防火墙或网闸产品在网络边界实行访问控制。对此规划部署的内外网边界防火墙、服务器区防火墙、安全管理区防火墙以及内外网安全隔离网闸可以按照不同安全级别的网络的各自功能和重要程度制定相应的访问控制策略，对经过的数据包进行严格的审查，将不安全或者不合规的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为，保障省消防救援总队内外网的安全。

10.6.3.3. 安全审计

根据等级保护的基本要求：应对信息系统网络中设备运行状况、网络流量、用户行为等进行日志记录，并且审计记录应包括：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。

对此，应采取网络日志审计、网络运维管理安全审计等措施。规划部署的运维审计系统，可根据管理制度制定的相关策略，对运维管理人员进行集中统一管理，并可对所有操作行为进行完整地审计。规划部署的专业日志审计系统，可以对信息系统网络中的主机、服务器、网络设备、安全设备、应用、中间件、数据库等日志进行集中的审计。

10.6.3.4. 边界完整性检查

根据等级保护技术要求，三级系统的边界应当能够有效监测非法外联和非法接入的行为，即应当能够对内部用户未通过准许私自联到外部网络的行为进行检查，同时，也要对非授权设备私自联到内部网络的行为进行检查，并能准确定位。为有效监测非法接入和非法外联，可在接入交换机和边界网关设备上进行 IP/MAC 绑定基础上，规划部署准入控制系统、终端运维管控系统。准入控制系统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。通过终端运维管控系统的非法外联监控管理，可以防止用户访问非信任网络资源，从而避免了访问非信任网络资源而引入安全风险或者导致信息泄密的可能性。

10.6.3.5. 入侵防范

根据等级保护的基本要求，网络边界处监视以下攻击行为并提供报警：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。结合省消防救援总队的实际网络环境，建议在外网安全管理区部署入侵检测系统，在核心交换区边界接入区域部署入侵防御系统，可以对核心区域网中可能潜在的黑客、病毒、蠕虫等实现对各种攻击的检测、告警和记录，同时可以阻断各种入侵行为。

10.6.3.6. 恶意代码防护

根据等级保护的基本要求，应在网络边界处对恶意代码进行监测和清除，应维护恶意代码库的升级和监测系统的更新。通过对病毒在网络中存储、传播、感染的各种方式和途径进行分析，结合当前系统架构特点，本项目需要在核心交换区边界的接入区域部署防病毒网关，与终端检测与响应系统软件形成立体防护，达到“多级防范，集中管理，以防为主、防治结合”的动态防毒策略。

10.6.4. 主机安全建设方案

10.6.4.1. 入侵防范

针对主机的入侵防范，主要是采用操作系统加固技术，除此之外，还可运用漏洞扫描、终端管理等多种技术来实现。

在智慧消防云平台系统服务器区域中，非常有必要部署安全、稳定的主机核心防护系统对系统内关键服务器主机进行安全防护。在服务器中安装部署单机版主机核心防护系统，使用管理员账户在本地登录后，根据服务器的具体业务系统情况配置安全策略，实现对核心数据资产的强制访问控制。通过主机核心防护系统对重要信息资源设置敏感标记，并对敏感标记进行检测与控制。为保障关键服务器的登录安全，通过主机核心防护系统实现认证 Key+密码的双因子认证，将通过在关键主机上绑定认证 key 的方式实现双因子认证。建议后期可规划在重要业务系统的宿主操作系统安装服务器安全加固系统，实现对业务系统的深层防护。

人工安全加固服务是对于系统安全的实现部分，服务的质量直接影响到评估范

围内所有设备的安全性。评估的范围包括项目范围内规定的所有的服务器、网络设备和 PC 机等，以及设备的安全维护手册及建议。服务器加固主要包括对 Windows 服务器和 Unix 服务器的评估，其中还包括对服务器操作系统层面的估和数据库层面的评估。网络设备加固主要包括对路由器，防护墙，交换机的评估。PC 机评估加固主要包括对 Windows 工作站和 Unix 工作站的评估。

漏洞扫描技术是在智慧消防云平台系统网络部署漏洞扫描系统，该系统可以对内部网络进行全面或部分扫描和漏洞分析。然后，根据漏洞扫描的结论来指导系统漏洞的修补，从而达到针对漏洞的入侵防御目的。本次规划在等保安全服务中采用专业漏洞扫描系统对重要的系统进行漏洞扫面并根据扫描结果协助修补漏洞。针对门户网站的高风险性，建议部署网站安全智能监控系统，24 小时不间断检测网站的风险情况。该系统通过旁路获取镜像流量，解析 url。可提取出一级域名作为根节点。一键添加后，能够全面发现 Web 服务器中匹配的站点，进行漏洞检测。除此还可利用域名匹配和 IP 关联做到对未知站点的发现及检测，无需人工持续跟进，减少人工工作量的同时，极大地提升网站的整体安全。

终端管理技术是通过在智慧消防云平台系统部署终端管理系统实现对终端的安全保障，部署说明如下：

1．在安全管理区域部署终端管理中心、补丁分发系统等终端管理系统中心所需插件，使其成为智慧消防云平台系统全网的终端管理中心；

2．通过管理中心实现补丁分发与集中管理，并制定策略，在每一台终端开机时先与终端防护系统管理服务器联系，检查终端上最新的补丁安装情况。

10.6.4.2. 安全审计

针对主机的安全审计可以采用主机审计系统来实现，在安全管理区部署主机审计系统，然后在全网的服务器及办公终端上安装客户端插件，管理中心即可对该主机进行审计。通过安全审计监视终端主机的活动，审计的记录可以作为证据供事后分析调查。

10.6.4.3. 恶意代码防范

恶意代码是一类不必要但却可能带来威胁的代码，通常是指病毒、木马、蠕虫、

后门、逻辑炸弹等。针对主机的恶意代码防范，等级保护要求应安装防恶意代码软件，及时更新防恶意代码软件版本和恶意代码库，并支持防恶意代码的统一管理。

防恶意代码通常采用防病毒软件，但是基于签名式或启发式的防病毒运行机制却无法识别和分析变种恶意代码。而对来自于终端、网络、云和用户内部的攻击，特别是涉及到漏洞（NDAY／0DAY），社会工程学和抵近式物理攻击方法。这些攻击方法的已被证明可以穿透传统的防护机制，防病毒软件甚至目前流行的防 APT 的沙箱解决方案都具有相当的局限性。而终端检测与响应系统作为下一代端点安全防护方案被广泛引用。除了防已知和未知恶意代码（勒索、挖矿、蠕虫等），它也可以有效检测 APT 攻击等恶意行为并予拦截、溯源、审计。

在智慧消防云平台系统的安全管理区域内部署终端侦测与响应分析平台，为省总队所有主机提供恶意程序、恶意代码、恶意行为的检测和防御规则下发服务。同时，通过全网联动功能，实现一处发现全网防护，提高恶意代码防护检测和阻断效率和效果。部署说明如下：

1．在安全管理区域内的云主机安装终端侦测与响应分析平台，使其成为智慧消防云平台系统网络的防恶意代码防恶意行为的监控管理中心；

2．在终端侦测与响应分析平台建立后，通过“WEB 安装”“共享安装”及“本地安装”的方式安装防病毒防恶意行为终端，终端覆盖网内 Windows、Linux 服务器及所有办公用机；

3．智慧消防云平台系统的终端侦测与响应分析平台与 Internet 相连，自动下载恶意行为规则库进行升级，平台服务器升级后自动将升级包推送给下级各终端，如果终端侦测与响应分析平台与互联网物理隔离，也不影响终端对恶意代码、恶意行为的识别和阻断，在断网情况下依然能拦截攻击，并保存拦截记录。

10.6.5. 应用安全建设方案

10.6.5.1. 身份鉴别

等级保护基本要求应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别，这项安全措施一般由应用系统开发商在系统开发阶段完成。围绕应用安全建设思路，构建统一的身份鉴别支撑平台，将数字证书同应用系统结合，实现如

下安全功能：

1、身份认证，以 CA 签发的数字证书认证方式取代原有用户名/口令弱认证方式，为各类应用系统提供统一、高强度的身份认证手段；

2、单点登录，用户仅需登录任意一个应用系统或 Portal 门户系统，即可无需再次登录访问多个应用系统，实现单点登录，全网漫游；

3、网络传输安全，数据加密，为主业务层的信息传递进行保护，保障主业务层的数据传递的安全性，确保用户无法查看未被授权的数据信息；

4、数据签名/签名验证，为主业务层的各项应用提供身份确认和重要数据签名服务，保障主要数据完成性、不可抵赖性；

5、访问控制，为主应用层提供用户在业务系统中权限的权限信息，保障业务信息访问者的权限控制；

6、安全审计，对外提供日志接口，各类系统(包括安全系统或者应用系统)能够通过向安全审计系统发送应用日志或安全日志实现日志信息的统一收集、整理、归档、管理。

10.6.5.2. 安全审计

应用安全的审计一般表现为针对数据库系统的审计。对此，省消防救援总队已在信息系统网络的三级核心交换区部署数据库审计系统，该系统是由软硬件一体化的审计中心和数据库引擎组成。数据库引擎采取旁路监听的方式部署于核心交换机上，数据库审计系统在不影响数据库系统自身性能的前提下，抓取网络中的数据包，并对抓到的包进行分析、匹配、统计，通过特定的协议算法，从数据库访问操作入手，对抓到的数据包进行语法分析，从而审计对数据库中的哪些数据进行操作，同时对数据库的用户事件，系统状态进行审计，对特定的数据操作制定规则，产生报警事件，由审计中心实现报警。

审计的行为应包括数据库的 DDL、DML、DCL，以及其它操作等行为；审计的内容可以细化到库、表、记录、用户、存储过程、函数、调用参数，等等。

10.6.5.3. 应用安全防范

由于智慧消防云平台信息系统包含 web 应用系统，此系统对外发布业务中包含

各级消防部门内部重要信息，必须保证只有业务系统架构内的信息才可以被发布出去，需要采取措施防范非法获取数据的行为，同时需要对 web 应用的可用性进行监控。建议采用本地 web 应用防火墙及网站云监测结合的手段对业务系统进行安全保护和监测。

Web 应用防火墙简称 WAF，可以保护页面内容防篡改、防爬虫、防跨站、防注入等针对 web 应用的攻击行为，可以有效避免“拖库”等依靠 web 应用系统漏洞造成的严重问题。

网站云监测系统主要提供对网站的云端监测功能，对网络提供修补建议，保障本地的网络站安全运维。

10.6.6. 安全管理平台建设

福建省消防救援总队信息化建设具备一定的规模，有大量的网络设备、主机设备、应用系统、服务器等等。随着信息化建设的发展，网络中的设备也随之增多，而随之带来的就是对网络中各种设备的整体管理和运维的困难。网络中对各式网络的设备的管理需要在不同的管理控制平台之间频繁的切换，这对运维管理人员带来很大的不便，而且导致管理的孤岛，每个设备各自为政。为有效地对省总队的 IT 资源进行管理，有必要建立一套 IT 监控运维平台。此外，等级保护也要求对信息系统的重要资源进行监视，最小值进行检测和报警。

安全管理平台围绕用户的业务安全，可全面监控与之相关的网络设备、安全设备、服务器主机、数据库、中间件、通用服务、业务系统等的运行状态，采集它们的安全事件。系统可对各类关键运行指标设置监控阈值，可对采集的事件进行归一化处理和关联分析。当出现运行指标异常，发现攻击行为或违规访问时，可及时进行多种方式的告警，执行预定义的响应动作，帮助管理员迅速定位故障点，发现高危安全事件，及时采取有效措施，保障用户业务连续性。同时，安全管理平台利用所采集的运行指标数据和安全事件数据，能够提供多种类型的统计分析，依照合规要求生成多种审计报表。安全管理平台为持续提高业务系统可用性和提高网络安全预警能力提供了有效的技术平台。

10.7. 等级保护技术设计产品清单

10.7.1. 系统及网络安全虚拟化部署

由于福建省智慧消防云平台拟部署于福建省电子政务云计算平台中，因此在系统和网络安全防护方面，无法挂载和使用物理安全防护设备，必须使用电子政务云平台提供的虚拟化系统及网络安全防护应用软件。

10.7.2. 安全设备配置清单

安全设备配置表

编号	项目名称	主要性能指标	单位	数量	部署说明
（1）	防火墙	电子政务云平台提供	套	1	电子政务云平台提供
（2）	负载均衡	电子政务云平台提供，8 核 CPU；8GB 内存；2 个网卡；≥500G 磁盘空间；Linux 操作系统	套	1	电子政务云平台提供
（3）	入侵防御系统（IPS）	电子政务云平台提供	套	1	电子政务云平台提供
（4）	数据库审计	电子政务云平台提供	套	1	电子政务云平台提供
（5）	漏洞扫描系统	电子政务云平台提供	套	1	电子政务云平台提供
（6）	终端侦测与响应系统（6）	总队和支队提供，免于遭受不限于 APT 攻击、勒索、挖矿、蠕虫等恶意程序的攻击，提供全网联动功能		0	总队和 9 个支队分析中心安装电子政务云平台，客户端部署在各区域的服务器和终端上
（7）	数字证书系统	电子政务云平台提供	套	1	电子政务云平台

(8）	VPN 设备	94 个监管单位提供，支持 IPSEC VPN\ SSL VPN，支持 SM2\SM3\SM4 加密算法	94	提供 部署在 15000 风险单位和 94 个监管单位之间，用于数据完整性、机密性保护，火灾风险单位可按照总队支持的设备功能要求自行采购。

10.8.云计算安全责任划分

本次福建省智慧消防云平台项目的部分主体拟部署于福建省政务外网电子政务云平台。云计算以服务为本质，包括云服务方和云租户两大责任主体，并且包括不同的服务模式和部署模式。云计算环境的安全由云服务方和云租户共同保障。针对不同服务模式，云服务方和云租户的安全责任边界不同，由二者对云服务各组件的管理和控制权限范围决定了各自的安全责任边界。

具体如下图所示：

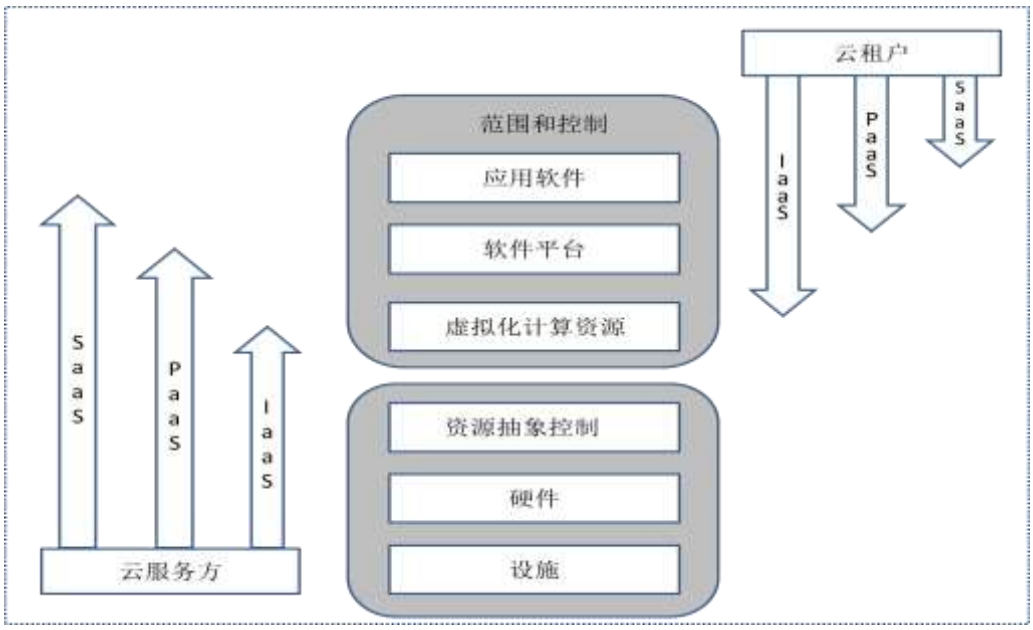


图 云服务模式与资源控制范围的关系

云计算保护环境是云服务方的电子政务云平台，及云租户在电子政务云平台之上部署的软件及相关组件的集合。其中，电子政务云平台的等级保护定级和按照等级的保护工作由云服务方负责，对于大型电子政务云平台可以将云计算基础设施平台及辅助支撑系统划分为不同的等级对象，各自独立定级。如果云租户在电子政务云平台上部署的软件及相关组件可以构成等级保护定级对象，则一般称为云租户信息系统，针对其的具体定级和按等级开展的保护工作由云租户负责。

福建省发改委和公安厅于 2017 年发布了《关于明确福建省级政务云计算服务网络与信息安全管理职责分工的通知》（闽发改数字〔2017〕503 号）要求：“各应用单位负责各自建设使用的应用系统的主机安全、应用安全、数据库安全、数据防泄漏与完整性。首次部署在省级政务云平台的信息系统，各应用单位要明确信息系统安全等级，并通过安全等级测评”。下表为《福建省级政务云计算服务网络与信息安全管理职责表》：

表 10 福建省级政务云计算服务网络与信息安全管理职责表

安全类别	安全项	网安办	应用单位	经济信息中心	空间中心
物理安全	物理位置的选择			责任人	
	物理访问控制			责任人	
	防盗窃和防破坏			责任人	
	防雷击			责任人	
	防火			责任人	
	防水和防潮			责任人	
	防静电			责任人	
	温湿度控制			责任人	
	电力供应			责任人	
	电磁防护			责任人	
	监督、检查	责任人			
网络安全	结构安全与网段划分			责任人	
	网络访问控制			责任人	
	拨号访问控制			责任人	
	网络安全审计			责任人	
	边界完整性检查			责任人	
	网络入侵防范			责任人	
	网络恶意代码防范			责任人	
	网络设备防护			责任人	
	预警、监控	责任人			
	监督、检查	责任人			
数据库安全	承载环境与可用性			责任人	

	管理员身份鉴别			责任人	
	管理员访问控制			责任人	
	管理员安全审计			责任人	
	实例管理员身份鉴别		责任人		
	实例管理员访问控制		责任人		
	实例管理员安全审计		责任人		
	资源控制			责任人	
	预警、监控	责任人			
	监督、检查	责任人			
政务数据汇聚共享平台安全	身份鉴别				
	访问控制				责任人
	应用及数据安全审计				责任人
	资源安全管理				责任人
	平台安全审计				责任人
	安全预警、监控、监督、检查	责任人			
数据备份与恢复	本地备份与恢复			责任人	
	本地备份数据安全			责任人	
	异地灾备与恢复				责任人
	灾备数据安全				责任人
	监督、检查	责任人			
主机安全	虚拟机模块安全			责任人	
	身份鉴别		责任人		
	自主访问控制		责任人		
	强制访问控制		责任人		
	安全审计		责任人		
	系统保护		责任人		
	剩余信息保护		责任人		
	入侵防范		责任人		
	恶意代码防范		责任人		
	资源控制		责任人		
	预警、监控	责任人			
	监督、检查	责任人			
应用安全	身份鉴别		责任人		
	访问控制		责任人		
	安全审计		责任人		
	剩余信息保护		责任人		
	通信完整性		责任人		
	通信保密性		责任人		
	抗抵赖		责任人		
	软件容错		责任人		

	资源控制		责任人		
	代码安全		责任人		
	信息内容安全		责任人		
	预警、监控	责任人			
	监督、检查	责任人			

福建省智慧消防云平台项目的建设依照国家电子政务外网管理中心办公室发布了《国家电子政务外网安全等级保护实施指南》，该指南中对于我国政务外网的等级保护定级对象做了明确的规定：

“政务外网的定级对象为本级政务外网管辖范围内（由边界设备确定）的所有网络、计算、存储和安全防护等各类设备、各种用于网络运维管理、安全保障的应用系统、各种通信线路及支持所有软硬件正常运行的机房等基础环境设施等。

门户网站系统、跨部门的数据共享与交换系统、数据中心内的各业务应用系统以及各级政务部门的各类业务应用系统不包含在政务外网的等级保护范围内，这些信息系统应按国家标准《信息系统安全等级保护基本要求》（GB/T22239-2008）中的规定由信息系统的责任主体单位自行实施定级和保护。”

福建省智慧消防云平台项目的各类业务应用系统不包含在政务外网的等级保护范围内。在等级保护定级范围界定时，可参照政务外网实施指南相关规定执行。

10.9.安全防护设计

10.9.1. 物理安全

物理环境安全策略的目的是保护网络中计算机网络通信有一个良好的电磁兼容工作环境，并防止非法用户进入计算机控制室和各种偷窃、破坏活动的发生。

10.9.1.1.机房选址

机房和办公场地要求选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

10.9.1.2.机房管理

机房出入口要求安排专人值守，控制、鉴别和记录进入的人员；

需进入机房的来访人员须经过申请和审批流程，并限制和监控其活动范围。

对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置过渡区域；

重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

10.9.1.3. 机房环境

要求合理规划设备安装位置，应预留足够的空间作安装、维护及操作之用。房间装修必须使用阻燃材料，耐火等级符合国家相关标准规定。机房门大小应满足系统设备安装时运输需要。机房墙壁及天花板应进行表面处理，防止尘埃脱落，机房应安装防静电活动地板。

机房需安装防雷和接地线，设置防雷保安器，防止感应雷，要求防雷接地和机房接地分别安装，且相隔一定的距离；机房设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。配备空调系统，以保持房间恒湿、恒温的工作环境；在机房供电线路上配置稳压器和过电压防护设备；提供短期的备用电力供应，满足关键设备在断电情况下的正常运行要求。设置冗余或并行的电力电缆线路为计算机系统供电；建立备用供电系统。铺设线缆要求电源线和通信线缆隔离铺设，避免互相干扰。对关键设备和磁介质实施电磁屏蔽。

10.9.1.4. 设备与介质管理

为了防止无关人员和不法分子非法接近网络并使用网络中的主机盗取信息、破坏网络和主机系统、破坏网络中的数据的完整性和可用性，必须采用有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。此外，必须制定严格的出入管理制度和环境监控制度，以保障区域监控系统和环境监控系统的有效运行。对介质进行分类标识，存储在介质库或档案室中。利用光、电等技术设置机房防盗报警系统；对机房设置监控报警系统。

10.9.1.5. 物理安全设计

由于本项目部分应用主体拟部署在福建省级政务外网云平台上，云平台满足上述等保物理安全要求。

10.9.2. 网络安全

10.9.2.1. 网络结构安全

网络结构的安全是网络安全的前提和基础，选用主要网络设备时需要考虑业务处理能力的高峰数据流量，要考虑冗余空间满足业务高峰期需要；网络各个部分的带宽要保证接入网络和核心网络满足业务高峰期需要；按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机；合理规划路由，业务终端与业务服务器之间建立安全路径；绘制与当前运行情况相符的网络拓扑结构图；根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

10.9.2.2. 网络安全审计

实现对用户的网络行为、网络传输内容进行监控；实现对网络行为进行统计分析和事后取证；对网络潜在威胁者予以威慑。对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，能根据记录数据进行分析，并生成审计报表。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。

10.9.2.3. 网络设备防护

为提高网络设备的自身安全性，保障各种网络应用的正常运行，对网络设备需要进行一系列的加固措施，包括：

（1）对登录网络设备的用户进行身份鉴别，用户名必须唯一；

（2）对网络设备的管理员登录地址进行限制；

（3）身份鉴别信息具有不易被冒用的特点，口令设置需 3 种以上字符、长度不

少于 8 位，并定期更换；

（4）具有登录失败处理功能，失败后采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

（5）启用 SSH 等管理方式，加密管理数据，防止被网络窃听。

（6）对于鉴别手段，建议采用 USBkey+密码进行身份鉴别，保证对网络设备进行管理维护的合法性。

10.9.2.4. 网络可信接入

为保证网络边界的完整性，不仅需要禁止非法外联行为，同时对非法接入进行监控与阻断，形成网络可信接入，共同维护边界完整性。通过部署终端安全管理系统可以实现这一目标。此外，还可部署网络准入管理平台，加强和完善基于 DHCP 协议的网络接入控制。

10.9.2.5. 网络安全设计

由于本项目部分应用主体拟部署于福建省级政务外网云平台上，云平台满足上述等保网络安全要求。

10.9.3. 主机安全加固

10.9.3.1. 系统选用

选择自主可控、安全可靠的正版操作系统或借助第三方安全加固工具和服务对操作系统和数据库系统的内核、服务、应用、端口等进行安全加固。

10.9.3.2. 系统设置

10.9.3.2.1. 最小化安装

操作系统和数据库系统遵循最小化安装原则，仅安装业务所需的服务、组件和软件等。

10.9.3.2.2. 身份鉴别

1、可采用用户名/口令等鉴别机制实现服务器操作系统及数据库系统的身份鉴别；

2、口令应由大小写字母、数字及特殊字符组成。

3、普通用户的口令长度不短于 10 位，系统管理员用户的口令长度不短于 12 位，且每 3 个月至少更新一次；

4、应采取措施防范口令暴力破解攻击，应设置登录延时、限制最大失败登录次数、锁定账号等措施，认证失败 3 次锁定 10 分钟，累计认证失败 6 次锁定 30 分钟，累计认证失败 10 次锁定 24 小时；

5、用于身份认证的用户名和口令在传输时应进行加密；

6、存储的用户名和口令应进行加密保护；

7、应当对登录用户开启日志审计功能。

10.9.3.2.3. 访问控制

1、针对服务器操作系统及数据库系统应设置用户访问控制策略，至少分为系统管理员（只能对系统进行维护）、安全管理员（只能进行策略配置和安全设置）、安全审计员（只能维护审计信息）等，为不同用户授予其完成各自承担任务所需的最小权限，限制超级管理员等默认角色或用户的访问权限；

2、应及时清除无用账号、默认账号、过期账号，禁止多人共用同一个系统账号；

3、应限制网站 Web 服务器、数据库服务器等重要服务器的远程管理方式；

4、若需要采用远程管理方式时，宜采用 SSH 等安全方式进行服务器的远程管理，并对远程管理的系统管理员采用数字证书等高强度鉴别方式；

5、应开启业务所需的最少服务及端口；应启用访问控制功能，依据安全策略控制用户对资源的访问；

6、应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；

7、应实现操作系统和数据库系统特权用户的权限分离；

8、应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些账户的默

认口令；

9、应对重要信息资源设置敏感标记；

10、应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

10.9.3.2.4. 安全审计

1、应实现服务器操作系统及数据库系统的安全审计，对系统远程管理、账号登录、策略更改、对象访问、服务访问、系统事件、账户管理等行为及 WWW、FTP 等重要服务访问进行审计，并设置审计日志文件大小的阈值以及达到阈值的处理方式（覆写、自动转存等）；

2、指定独立的安全审计员负责管理审计日志，针对安全审计记录及审计策略设置必要的访问控制，禁止未授权的删除、修改或覆盖等；

3、审计记录应保存于专用的日志服务器上，保存时间不宜少于 6 个月；

4、对审计数据进行分析，包括分类、排序和趋势分析等，支持集中审计和事件关联分析；

5、对特定异常事件进行审计分析，提高实时报警功能，提供自动响应机制，如进行实时报警、终止违例进程、取消异常服务等。

10.9.3.3. 系统更新

1、应统一采购、部署正版软件以及相关服务，并定期开展系统漏洞扫描工作；

2、应通过操作系统软件、数据库系统软件官方网站或其他合法渠道获得补丁程序，并在补丁程序通过安全测试后及时更新。

10.9.3.4. 恶意程序防护

1、防恶意程序软件的部署应该由点及面，全方位进行部署，彻底截断已知和未知病毒入侵的途径；能够识别 ATP 攻击，并给予阻断和溯源。

2、开启实时检测，保障在病毒入侵时可以随时发现并清除；能够实现一处发现，全网联动的防护效果。

3、定期进行检测规则库的升级，在重大病毒事件发生时，做到实时升级，确保系统防恶意程序防恶意行为的规则库是最新的；

4、每月进行服务器和客户端全磁盘查杀病毒；

5、建立恶意程序防范的日常管理机制和审查机制；

6、一旦发现重大恶意程序应立即查杀，并上报主管领导或上级主管部门；

7、对于染毒次数、杀毒次数、杀毒后果应进行详细记录。

10.9.4. 应用安全

10.9.4.1. 身份鉴别

1、应采用数字证书、用户名/口令、短信、动态口令等 2 种以上用户身份认证方式；

2、应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

3、口令应由大小写字母、数字及特殊字符组成，普通用户的口令长度不短于 8 个字符，系统管理员用户的口令长度不短于 10 个字符，且每 6 个月至少修改一次；

4、应采取措施防范口令暴力破解攻击，可采用设置登录延时、限制最大失败登录次数、锁定账号等措施；

5、应提供用户身份标识唯一和鉴别信息复杂度检查功能，可根据安全策略配置相关参数；

6、应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

7、鉴别信息在存储和传输时进行保护。

10.9.4.2. 访问控制

1、应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

2、基于数字证书的访问控制，需先通过验证数字证书来确认是否具有访问系统的权限；

3、支持通过用户名、数字证书方式对系统管理员和操作员进行身份认证，认证支持政务外网数字证书，应通过政务外网现有认证体系进行认证也可离线认证；

4、访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

5、自主访问控制以用户身份标识并控制对客体的访问，阻止非授权用户对客体的访问，可以有多个自主访问控制功能，但其访问控制策略必须具有一致性；

6、自主访问控制策略提供用户按照确定的访问控制策略对自身创建的客体的访问进行控制的功能；

7、应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；

8、应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

10.9.4.3. 安全审计

1、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；

2、应保证无法删除、修改或覆盖审计记录；

3、审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等；

4、当检测到有安全侵害事件时，生成实时报警信息，并根据报警策略在告警事件发生时触发告警。

10.9.4.4. 通信完整性

1、应用系统数据传输可采用数字证书、数字签名等技术方式来保证数据传输的完整性；

2、应采用校验码技术保证通信过程中数据的完整性。

10.9.4.5. 通信保密性

1、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；

2、应对通信过程中的敏感信息字段进行加密；

3、所配置的密码或其他相应的安全机制，对需要进行存储或传输保密性保护的用户数据进行加密。

10.9.4.6. 软件容错

1、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；

2、在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的应急措施。

10.9.4.7. 资源控制

1、当应用系统的通信双方中的一方在 30 分钟内未做任何响应，另一方应能够自动结束会话；

2、应对单个账户的多重并发会话进行限制；

3、应对应用系统的最大并发会话连接数进行限制。

10.9.4.8. 会话管理

1、会话过程中不允许修改的信息，必须作为会话状态的一部分在服务器端存储和维护；

2、禁止使用客户端提交的未经审核的信息来给会话信息赋值，防止会话信息被篡改；

3、用户登录后必须分配新的会话标识，不能继续使用用户登录前所使用的标识；

4、当用户退出时，必须清除该用户的会话信息；

5、会话超时后应清除会话信息且超时时间不超过 30 分钟。

10.9.4.9. 内容安全

1、对外提供应用服务的平台不应向公众发布不良信息；

2、对恶意非法访问统一跳转至报错提示页面；

3、对公众提供应用服务的平台应对向公众发布的各种文本信息内容进行实时的过滤，以阻止不良信息的传播、应采用技术或人工手段有效防止其他类型（图像、音频、视频等）不良信息通过业务网络向公众传播。阻止网页篡改、越权访问信息等各类企图，或者及时发现并恢复受到篡改的网站页面。

10.9.4.10. 敏感数据保护

1、敏感数据（比如密码、密钥等）必须加密存储、加密传输；

2、禁止在隐藏域中存放明文形式的敏感数据。

10.9.4.11.应用安全防护

1、能够根据内容对 HTTP 请求和响应进行过滤；

2、应对 SQL 注入精确报警和主动防御；

3、应对 XSS 攻击精确报警和主动防御；

4、满足策略自定义设置，阻断恶意注入攻击（SQL 注入、XSS 攻击、目录遍历、信息泄漏）；

5、应对侦测到的网络安全攻击具备阻断访问的能力。

10.9.5. 数据库安全控制

10.9.5.1. 访问控制要求

1、用数据库目录表、存取控制表、能力表等确定主体对客体的访问权限；

2、应允许命名用户以用户和（或）用户组的身份规定并控制对客体的共享，并阻止非授权用户读取信息；

3、所有数据库引擎实例都由安装该实例的过程中指定的实例名标识，应用程序必须提供准备连接的计算机的名称和实例名；

4、自主访问控制的粒度应是用户级、表级、记录级、字段级；

5、自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问。

10.9.5.2. 数据库身份认证

1、进入数据库系统的用户，先进行操作系统身份认证；

2、当用户远程直接登录到数据库管理系统或与数据库服务器进行访问连接时，应进行用户认证；

3、数据库管理系统应明确用户标识；

4、操作系统应确保任何用户不能通过数据库以外的使用方式获取和破坏数据库用户的标识和认证信息；

5、鉴别信息应是不可见的，并在存储和传输时有安全保护；

6、数据库系统应保证用户以安全的方式和途径使用数据库系统的标识和认证信息；

7、数据库用户标识信息应在数据库系统的整个生命期有效，被撤销的用户账号的 UID 不得再次使用。

10.9.5.3. 数据库的安全审计

1、安全审计功能的设计应与用户标识与鉴别、自主访问控制等安全功能的设计紧密结合；

2、提供审计日志、潜在侵害分析、基本审计查阅和有限审计查阅、安全审计事件选择以及受保护的审计踪迹存储等功能；

3、能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏，特别要保护审计数据，要严格限制未经授权的用户访问；

4、能够创建并维护一个对受保护客体访问的审计跟踪，保护审计记录不被未授权的访问、修改和破坏。

10.9.5.4. 运行安全

1、系统在设计时不应留有“后门”。即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口；

2、安全结构应是一个独立的、严格定义的系统软件的一个子集，并应防止外部干扰和破坏，如修改其代码或数据结构；

3、应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性进行定义；

4、当数据库管理系统安装完成后，在普通用户访问之前，系统应配置好初始用户、管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制。

10.9.5.5. 数据库备份

数据库应至少每天备份一次。

10.9.6. 数据安全及备份恢复

10.9.6.1. 数据完整性

1、应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中进行完整性检测，及时发现以某种方式传送或接收的用户数据被篡改、删除、插入等情况，并在检测到完整性错误时采取必要的恢复措施；

2、应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

3、应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。

10.9.6.2. 数据保密性

1、对存储的用户的数据，根据不同数据类型的不同保密性要求，进行不同程度的保密性保护，确保除具有访问权限的合法用户外，其余任何用户不能获取该数据；

2、对不同用户间进行传输的用户数据，根据不同数据类型的不同保密性要求，进行不同程度的保密性保护，确保数据在传输过程中不被泄露和窃取；

3、应对重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用协议的攻击破坏数据保性。

10.9.6.3. 数据访问

1、应用程序访问数据须经授权和身份认证；

2、实现控制，以限制对非结构化数据的访问；

3、应保护数据的导出。

10.9.6.4. 数据交换

根据交换对象种类的不同，可分为数据库数据、文件数据、流媒体数据、请求命令与响应数据。可根据业务需要选择数据交换对象及数据交换流向，如单向数据交换、双向数据交换。

10.9.7. 安全管理设计

1、制订安全管理策略和原则

信息安全管理策略：

信息安全管理策略是信息系统安全的最高指导。信息安全领导小组需根据业务信息系统的状况，进行深化、细化，针对信息系统的各个环节制订出相应的安全管理规则，完整的管理框架和有效的过程控制，形成信息安全策略一系列文件，覆盖以下内容：

信息安全的方针政策、整体目标和范围；

对安全管理策略、原则、标准的简介；

各个工作人员在信息安全管理方面的责任和义务，及违反安全管理策略的后果；

支持该安全管理策略的文档，如更详尽的安全管理策略，包括用户授权管理、机房安全管理、设备安全管理、信息安全管理、用户终端管理，安全故障处理流程等各种安全规则等。

信息安全管理策略及安全规则应该简单明了、通俗易懂，有很强的可操作性。用户都要能理解信息安全策略的详细内容，及他们的安全责任与义务，并通过培训使信息安全管理策略真正植根于所有用户的脑海并落实到实际工作中。

信息安全管理原则：

1）多人负责原则

每一项与安全有关的活动，都必须有两人或多人在场。这些人应是系统主管领导指派的，他们忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。

以下各项是与安全有关的活动：

信息处理系统使用的媒介发放与回收；

处理保密信息；

硬件和软件的维护；

系统软件的设计、实现和修改；

重要程序和数据的删除和销毁等。

2）任期有限原则

一般地讲，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

3）职责分离原则

在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。

出于对安全的考虑，下面每组内的两项信息处理工作应当分开。

安全管理和系统管理；

应用程序和系统程序的编制；

计算机操作与信息处理系统使用媒介的保管等。

2、建立健全安全管理制度

1）物理安全管理

物理安全管理是系统安全管理的重要组成部分，它包括网络和基础设施、计算环境设施、支持性基础设施的物理安全。

物理安全管理是为了防止未授权个人或团体以更改、收集或拒绝访问信息为目的，物理上接近网络、系统或设备，破坏、修改或盗窃网络基础设施、业务系统服务器或应用软件，或者窃取各种介质（如磁盘、光盘、硬盘）上的重要数据。还应防止内部人员恶意或无意的攻击。

物理安全管理可以采取以下措施：

规定信息安全区域。应区分公共区域，内部办公人员区域及保护区域。在限制的内部办公人员区域及保护区域设立相应的出入控制制度。在机房等级保护区域的门禁制度应更加严格，可以要求出入人员提供身份证明，并对其出入时间和进入原因、完成什么工作进行记录；

指定专人对机房内各种设备进行管理，列出机房设备清单，对设备进行标注，对各设备的配线连接和配置进行记录；

指定专人负责机密信息和数据的载体，如备份磁盘、光盘、硬盘等的保存、传输和销毁，制订出相应的操作规程。

2）人员安全管理

人员是实现信息的创建、查询、修改、销毁的过程，是信息系统安全使用的决

定因素。人员对信息系统恶意或无意的攻击会对信息系统构成巨大的威胁。比如人员为了方便记忆系统登录口令而粘贴在桌面或计算机屏幕边的一张便条，就足以毁掉花费了大量人力物力建立起来的信息安全系统。对人员的有效管理是实现信息安全的基础。人员管理针对人员不同的角色，如安全管理人员、业务领导、技术管理人员，一般人员等制订不同的安全管理条例。如对一般人员的管理可以从以下方面进行：

在人员工作职责内规定他在信息安全中的安全角色和责任；

制订用户账户管理条例，规定人员不能与他人共享账户或将用户名及口令泄露给他人；

制订用户口令管理条例。规定人员在选择和使用口令时要遵守良好的安全标准。选择的口令应难于猜测，避免使用自己的名字、生日等非保密的个人信息；

制订软件或程序安装管理条例。规定人员不能安装、运行密码猜测软件、网络SNIFFER 软件等非法产品。不能破坏信息服务，滥用系统资源，滥用或错用 EMAIL 等；

制订出现安全问题时的报告程序及应急处理方法。让人员了解会影响机构资产安全的不同类别事件（安全破坏、威胁、弱点或错误工作），并知道如何处理及申报；

制订信息安全操作程序。规定人员必须执行这些安全操作程序，具备正确使用安全设备及安全技术的知识；

明确规定违规处置办法并严格执行。

10.10. 数据分级分类管理及授权应用机制

消防基础管理数据、消防动态监测数据、消防专题数据由福建省智慧消防云平台提供；城市信息服务基础数据库数据、消防监督相关社情民意数据、重点行业消防相关调查数据、公共资源数据由省政务信息汇聚共享平台提供；互联网数据、国家知网数据通过互联网获取，数据进行分级分类管理，授权应用机制如下表所示：

表 10-1：数据分级分类管理及授权应用机制表

序号	类别	数据来源	安全授权
1	消防基础监管数据	应用系统	由平台按使用用户级别授权
2	消防专题数据	应用系统	由平台按使用用户级别授权
3	国家知网数据	接入	根据订购数据库类别由国家知网平台统一授权静态IP，再由智慧消防平台根据用户级别统一授权

4	基础数据库数据	接入	由智慧消防平台向相关业务平台提交数据申请，由相关平台对智慧消防平台进行数据授权接入。再由智慧消防平台根据用户级别统一授权
5	消防监督相关社情民意数据	接入	由智慧消防平台向相关业务平台提交数据申请，由相关平台对智慧消防平台进行数据授权接入，再由智慧消防平台根据用户级别统一授权。
6	重点行业消防相关调查数据	接入	由智慧消防平台向相关业务平台提交数据申请，由相关平台对智慧消防平台进行数据授权接入，再由智慧消防平台根据用户级别统一授权。
7	公共资源数据	接入	由智慧消防平台向相关业务平台提交数据申请，由相关平台对智慧消防平台进行数据授权接入，再由智慧消防平台根据用户级别统一授权。
8	互联网数据	接入	由智慧消防平台向相关业务平台提交数据申请，由相关平台对智慧消防平台进行数据授权接入，再由智慧消防平台根据用户级别统一授权。

10.11. 密码技术方案设计

10.11.1. 密码应用保障框架

10.11.1.1.信息系统密码保护框架

信息系统密码应用总体框架如下：

密码应用保障框架

采用多层次映射方法提出的密码应用框架如图所示，共分为 4 个层次，分别是客观系统层、安全服务层、安全目标层和密码技术层。

（1）客观系统层：包括安全域和密级标识；

（2）安全服务层：不同系统对安全服务需求的划分，包括物理安全服务、密码

机制提供的信息安全服务、信息加密、访问控制、完整性校验、抗抵赖以及其他安全服务等；

（3）安全目标层：包括机密性、认证性、完整性和不可否认性；

（4）密码技术层：包括序列密码、分组密码、数字签名，以及对称密码技术、秘钥管理和非对称密码技术等。

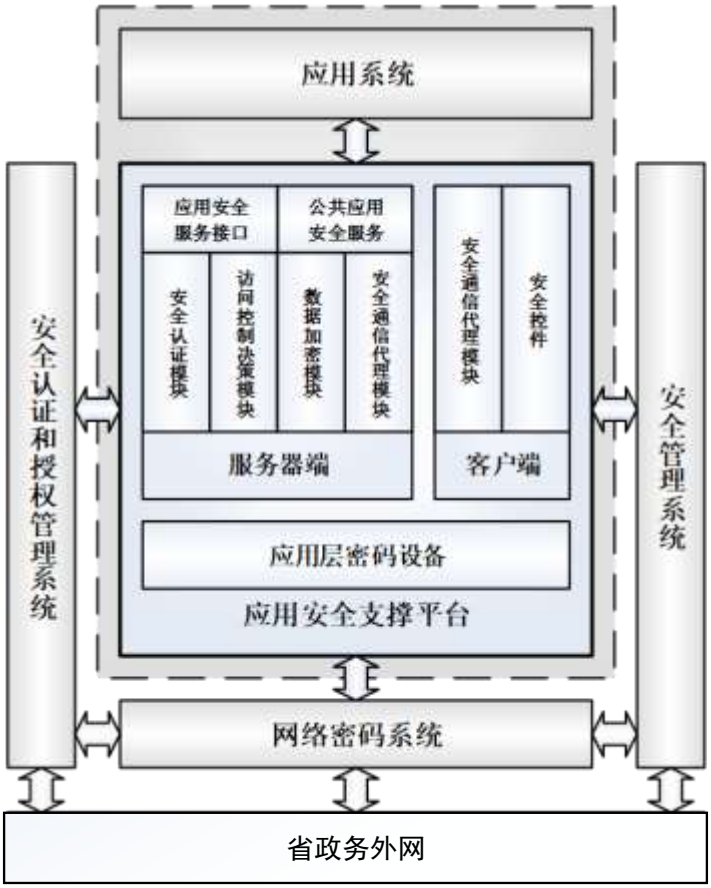
10.11.2. 详细设计

数据加解密是实现数据安全的基础，数据加解密对于大数据管理平台的安全机制具有重要的意义。

数据在系统上的存储和传输都要求要有严格的加解密机制进行保护，如数据传输时，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，并对通信过程中的整个报文或会话过程进行加密以保证通信过程中数据的完整性。数据存储时会采用加密算法以保证系统管理数据、鉴别信息和重要业务数据的存储保密性。

存放在 HDFS 上的数据是密文的，用户即使找到 HDFS 的数据块也不能直接浏览其内容，将数据加密以防止恶意窃取或篡改。并采用加密或其他保护措施实现鉴别信息、系统管理数据、鉴别信息和重要业务数据存储保密性。

根据密码应用保障框架要求，密码技术实现主要是在政务外网的基础设施为依托，网络密码系统、应用密码系统和应用安全支撑平台为骨干，业务应用为主题的一个加密信息系统。其结构如下图所示：

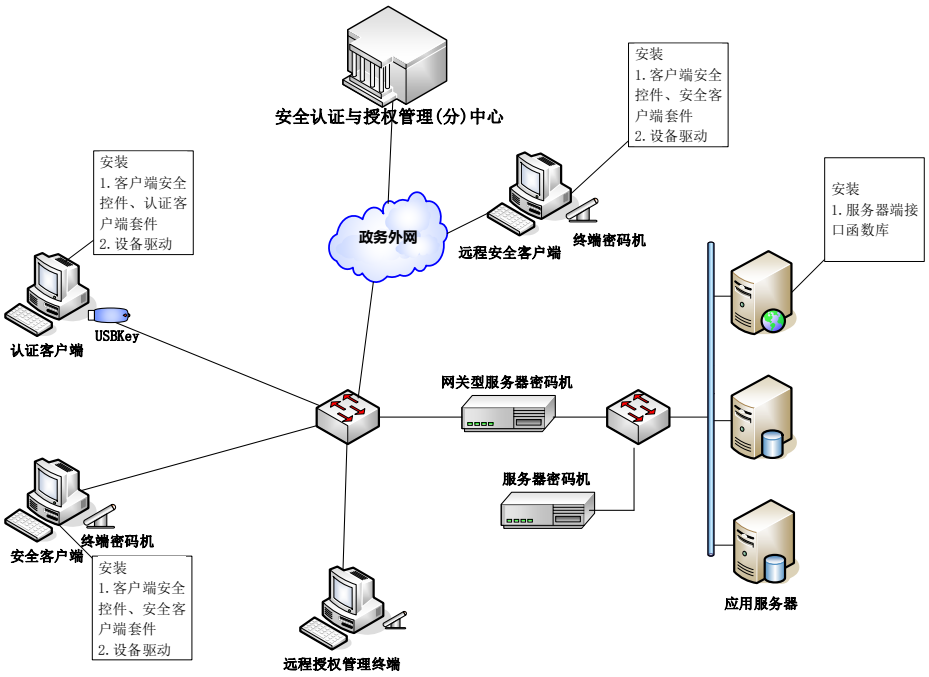


密码技术设计结构图

10.11.2.1.密码子系统

应用安全密码系统的核心是应用安全支撑平台。应用安全支撑平台基于安全认证和授权管理系统提供的身份证书、属性证书、安全认证、访问控制决策等服务，采用密码技术，为各类应用系统提供标准、统一、规范的安全功能支撑，保障整个系统的安全。应用安全支撑平台主要由服务器端和客户端的应用层密码设备、以及安装在应用服务器和客户端的安全软件模块、接口函数库、安全控件等组成，为应用系统提供标准的应用安全开发的接口。应用系统通过对接口的访问，调用应用安全支撑平台提供的安全服务，实现应用层安全。

一个较完整的加密网应用的配置如下图所示：



加密网应用的配置示意图

10.11.2.2.密码产品和密码服务

密码子系统包括了服务端和客户端。本项目主要在应用端部署客户端的安全软件模块、安全控件等部分内容，服务端应用层密码设备和安装在应用服务器的安全软件模块、接口函数库、安全控件等统一由云平台实现。

10.11.2.3.密码协议

- 信息加密可分为：

（1）通信加密：在传输过程中的数据加密；

（2）文件加密：将存储数据进行加密。

- 以加密实现的通信层次来区分，包括：

（1）链路加密；

（2）节点加密；

（3）端到端加密。

- 加密算法主要指：

（1）加密算法是实施具体加密的基础，它决定了加密的强度、运算量以及它的实用性。

（2）密码算法可以看作是一个复杂的函数变换，s=f（m，k）。

s 代表密文，即加密后得到的字符序列，m 代表明文，即待加密的字符序列，k 表示密钥，是秘密选定的一个字符序列。

- 加密算法实现包括软件加密和硬件加密，主要：

（1）软件加密：通过算法的计算机程序实现。

特点：实现简单，成本低；速度比较慢；相对来说，机密性差。

（2）硬件加密：通过具体的电子线路实现加密算法。

特点：实现复杂，成本高；加密速度比较快；相对软件加密算法实现，其机密性更好。

- 根据密码体制可分为对称密码体制和非对称密码体制。

（1）对称密码体制

对称密码体制（私钥）：加密密钥和解密密钥相同，且都需要保密。

1）优点：加密算法比较简便、高效、密钥简短，对方破译极其困难，且经受住时间的检验和攻击；

2）缺点：密钥必须通过安全的途径传送。

3）系统的机密性主要取决于密钥的安全性。

4）加密的方式：

按字符逐位加密（流密码）

将明文消息分组（分组密码）

5）常用算法：DES

6）适用范围：数据加密、消息认证

（2）非对称密码体制

非对称密码体制（公钥）：加密密钥和解密密钥不相同，一个公开，一个保密。

1）优点：可以适应网络的开放性要求，且密钥管理简单。增加数字签名应用。

2）缺点：算法复杂，且加密数据的速率较低。

3）特点：加密和解密功能分开。

4）常用算法：RSA、背包密码、零知识证明和椭圆曲线算法

10.11.2.4.密码应用工作流程

密码学是信息安全等相关议题，如认证、访问控制的核心。密码学的首要目的是隐藏信息的涵义，并不是将隐藏信息的存在。密码学也促进了计算机科学，特别是在于电脑与网络安全所使用的技术，如访问控制与信息的机密性。密码技术主要是加密和解密的过程。

加密与解密总体架构如下：

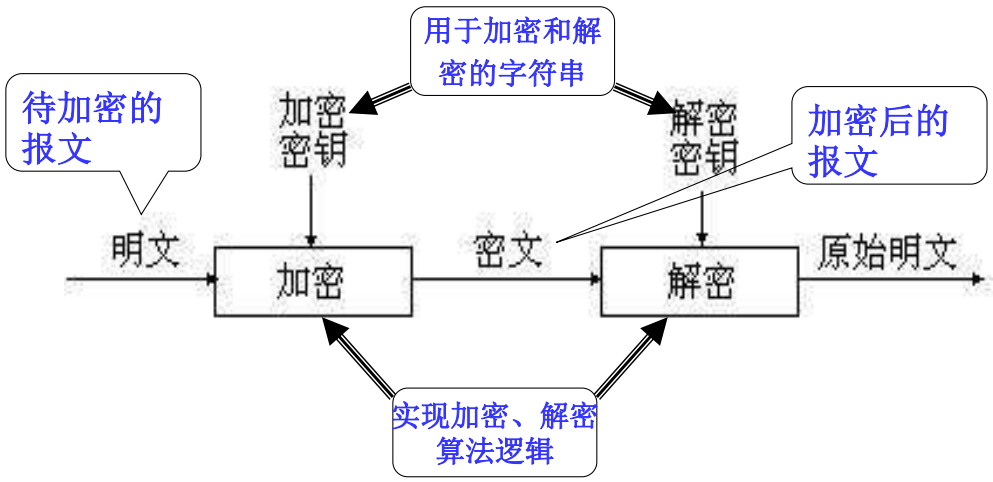


图 10-1：加密解码总体流程图

（1）加密

明文：加密前的数据。

密文：加密后的数据。

作用：防止有价值的信息被拦截和窃取。

加密变换：明文→密文

有两种主要的加密（编码）方法，分别是：

1）换位：将组成信息块的数字位进行交换。

2）置换：将每一个字符或数位替换为其他内容。对文件中的字符或符号进行替换，就能创建一个置换密码。

（2）解密

加密的逆过程称为解密。

解密变换：密文一〉明文

- 加密信息进行解密具备两个条件：

1）解密规则或者算法；

2）解密的密钥。

- 密钥：数据变换所用的独立输入项

1）加密密钥；

2）解密密钥。

10.11.2.5.密钥管理实现

- 一个完整的密钥管理系统应该包括：

（1）密钥管理、密钥分配、计算机网络密钥分配方法、密钥注入、密钥存储、密钥更换和密钥吊销。

（2）密钥管理是处理密钥自产生到最后销毁的整个过程中的关键问题，包括系统的初始化，密钥的产生、存储、备份/恢复、装入、分配、保护、更新、控制、丢失、吊销和销毁等内容。

（3）密钥的管理需要借助于加密、认证、签字、协议、公证等技术。

- 密钥种类很多，主要的密钥包括：

（1）初始密钥：由用户选定或系统分配的，在较长的一段时间内由一个用户专用的秘密密钥。要求它既安全又便于更换；

（2）会话密钥：两个通信终端用户在一次会话或交换数据时所用的密钥。一般由系统通过密钥交换协议动态产生。它使用的时间很短，从而限制了密码分析者攻击时所能得到的同一密钥加密的密文量。丢失时对系统保密性影响不大；

（3）密钥加密密钥（KeyEncryptingKey,KEK）：用于传送会话密钥时采用的密钥；

（4）主密钥（MasterKey）：对密钥加密密钥进行加密的密钥，存于主机的处理器中。

- 根据密钥信息的交换方式，密钥分配可以分成三类：

（1）人工密钥分发；

（2）基于中心的密钥分发；

（3）基于认证的密钥分发。

目前人工密钥分发已经不适应现代计算机网络发展的要求，现主流的密钥分配

主要是基于中心的密钥分发和基于认证的密钥分发。其中基于中心的密钥分发主要利用可信任的第三方，进行密钥分发。基于认证的密钥分发也可以用来进行建立成对的密钥。

10.11.2.6.算法配用

设计上要求系统采用的密码算法为国密算法。

为了保障商用密码安全，国家商用密码管理办公室制定了一系列密码标准，包括 SSF33、SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等等。其中 SSF33、SM1、SM4、SM7、祖冲之密码，是对称算法；SM2、SM9 是非对称算法；SM3 是哈希算法。

目前已经公布算法文本的包括 SM2 椭圆曲线公钥密码算法、SM3 密码杂凑算法、SM4 分组密码算法等。

（1）SM1 对称密码

国密 SM1 算法是由国家密码管理局编制的一种商用密码分组标准对称算法，分组长度为 128 位，密钥长度都为 128 比特，算法安全保密强度及相关软硬件实现性能与 AES 相当，算法不公开，仅以 IP 核的形式存在于芯片中。

采用该算法已经研制了系列芯片、智能 IC 卡、智能密码钥匙、加密卡、加密机等安全产品，广泛应用于电子政务、电子商务及国民经济的各个应用领域（包括国家政务通、地方政务通等重要领域）。

（2）SM2 椭圆曲线公钥密码算法

SM2 算法就是 ECC 椭圆曲线密码机制，但在签名、密钥交换方面不同于 ECDSA、ECDH 等国际标准，而是采取了更为安全的机制。国密 SM2 算法标准包括 4 个部分，第 1 部分为总则，主要介绍了 ECC 基本的算法描述，包括素数域和二元扩域两种算法描述，第 2 部分为数字签名算法，这个算法不同于 ECDSA 算法，其计算量大，也比 ECDSA 复杂些，也许这样会更安全吧，第 3 部分为密钥交换协议，与 ECDH 功能相同，但复杂性高，计算量加大，第 4 部分为公钥加密算法，使用 ECC 公钥进行加密和 ECC 私钥进行加密算法，其实现上是在 ECDH 上分散出流密钥，之后与明文或者是密文进行异或运算，并没有采用第 3 部分的密钥交换协议产生的密钥。对于 SM2 算法的总体感觉，应该是国家发明，其计算上比国际上公布的 ECC 算法复杂，相对来

说算法速度可能慢，但可能是更安全一点。

设需要发送的消息为比特串 M，len 为 M 的比特长度。为了对明文 M 进行加密，作为加密者的用户应实现以下运算步骤：

1）步骤 1：用随机数发生器产生随机数 k∈[1，n-1]；

2）步骤 2：计算椭圆曲线点 C1=[k]G=（X1，Y1），将 C1 的数据类型转换为比特串；

3）步骤 3：计算椭圆曲线点 S=[h]P，若 S 是无穷远点，则报错；

4）步骤 4：计算椭圆曲线点[k]P=（X2，Y2），将坐标 X2，Y2 的数据类型转换为比特串；

5）步骤 5：计算 t=KDF（x211y2，len），若 t 为全 0 比特串，则返回步骤 1；

6）步骤 6：计算 C2=M⊕t；

7）步骤 7：计算 C3=Hash（x211M11y2）；

8）步骤 8：输出密文 C=C111C211C3。

2010 年底，国家密码管理局公布了我国自主研制的“椭圆曲线公钥密码算法”（SM2 算法）。为保障重要经济系统密码应用安全，国家密码管理局于 2011 年发布了《关于做好公钥密码算法升级工作的通知》，要求“自 2011 年 3 月 1 日期，在建和拟建公钥密码基础设施电子认证系统和密钥管理系统应使用 SM2 算法。自 2011 年 7 月 1 日起，投入运行并使用公钥密码的信息系统，应使用 SM2 算法。”近期，人民银行组织召开多次专题会议讨论研究金融领域国产加密算法升级改造的相关工作。

（3）SM3 杂凑算法

又叫文摘算法，也有叫杂凑算法的。功能与 MD5，SHA-1 相同。产生 256 位的编码。该算法位不可逆的算法。具体算法也是保密。SM3 密码杂凑算法给出了杂凑函数算法的计算方法和计算步骤，并给出了运算示例。此算法适用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。在 SM2、SM9 标准中使用。此算法对输入长度小于 2 的 64 次方的比特消息，经过填充和迭代压缩，生成长度为 256 比特的杂凑值，其中使用了异或，模，模加，移位，与，或，非运算，由填充，迭代过程，消息扩展和压缩函数所构成。

SM3 算法包括预处理、消息扩展和计算 Hash 值三部分。预处理部分由消息填充

和消息分组两部分组成。首先将接收到的消息末尾填充一个“1”，再添加 k 个“0”，使得填充后的数据成为满足 length=448mod512bit 的数据长度，再在末尾附上 64bit 消息长度的二进制表示数，然后将消息分成 512bit 的子块，最后将每个 512bit 的消息子块扩展成 132 个字用于 Hash 值的计算。SM3 算法计算流程图如图所示。

SM3 算法的 Hash 运算主要是在压缩函数部分，压缩函数共包含 64 轮，每轮包括 12 步运算，64 轮循环计算结束后，再将计算结果与输入到本轮计算的初始数据进行异或运算，即上一次 Hash 运算的 Hash 值输出与输入到本轮计算的初始数据异或得到本次 Hash 值输出，Hn 即为最终的 Hash 值，H0 为设计者提供的初始值 IV。

（4）SM4 对称算法

此算法是一个分组算法，用于无线局域网产品。该算法的分组长度为 128 比特，密钥长度为 128 比特。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

定义反序变换 R 为：

R（A0，A1，A2，A3）=（A3，A2，A1，A0），Ai∈Z322，i=0,1，2,3。设明文输入为（X0，X1，X2，X3）∈（Z322）4，密文输出为（Y0，Y1，Y2，Y3）∈（Z322）4，轮密钥为 rki∈Z322。则本算法的加密变换为：

Xi+4=F （ Xi,Xi+1,Xi+2,Xi+3,rki ） =Xi⊕T （ Xi+1⊕Xi+2⊕Xi+3⊕rki ），i=0,1,2,3…，31.

（Y0，Y1，Y2，Y3）=R（X32，X33，X34，X35）=（X35，X34，X33，X32）。

本算法的解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序。

加密时轮密钥的使用顺序为：（rk0,rk1,…,rk31）。

解密时轮密钥的使用顺序为：（rk31,rk30,…,rk0）。

SM4 算法的优点是软件和硬件实现容易，运算速度快，但该算法的缺点是消息安全取决于对密钥的保护，泄漏密钥就意味着任何人都能对消息进行密码和解密。由于其加密过程和解密过程互逆，这两个过程均使用相同的保密密钥，使得对称密钥加密体制的适用范围受到了很大限制。

（5）SM7 对称密码

SM7 算法是一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。SM7

的算法文本目前没有公开发布。SM7 适用于非接 IC 卡应用包括身份识别类应用（门禁卡、工作证、参赛证），票务类应用（大型赛事门票、展会门票），支付与通卡类应用（积分消费卡、校园一卡通、企业一卡通、公交一卡通）。

（6）SM9 非对称算法

SM9 是基于对的标识密码算法，与 SM2 类似，包含四个部分：总则，数字签名算法，密钥交换协议以及密钥封装机制和公钥加密算法。在这些算法中使用了椭圆曲线上的对这一个工具，不同于传统意义上的 SM2 算法，可以实现基于身份的密码体制，也就是公钥与用户的身份信息即标识相关，从而比传统意义上的公钥密码体制有许多优点，省去了证书管理等。

双线性对的双线性的性质是基于对的标识密码SM2中的总则部分同样适用于SM9，由于 SM9 总则中添加了适用于对的相关理论和实现基础。

SM9 给出了数字签名算法（包括数字签名生成算法，数字签名验证算法），密钥交换协议，以及密钥封装机制和公钥加密算法（包括密钥封装算法，加密盒解密算法）。数字签名算法适用于接收者通过签名者的标识验证数据的完整性和数据发送者的身份，也适用于第三方确定签名及所签数据的真实性。密钥交换协议可以使用通信双方通过双方的标识和自身的私钥经过两次或者可选三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥。密钥封装机制和公钥加密算法中，利用密钥封装机制可以封装密钥给特定的实体。公钥加密和解密算法即基于标识的非对称秘密算法，该算法使消息发送者可以利用接收者的标识对消息进行加密，唯有接收者可以用相应的私钥对该密文进行解密，从而获取消息。基于对的算法中同样使用了国家密管理局批准的 SM3 密码杂凑算法和随机数发生器，密钥封装机制和公钥加密算法中使用了国家密码管理局批准的对称密码算法和消息认证码函数。

（7）祖冲之对称算法

祖冲之密码算法由中国科学院等单位研制，运用于下一代移动通信 4G 网络 LTE 中的国际标准密码算法。祖冲之密码算法（ZUC）的名字源于我国古代数学家祖冲之，祖冲之算法集是由我国学者自主设计的加密和完整性算法，是一种流密码。它是两个新的 LTE 算法的核心，这两个 LTE 算法分别是加密算法 128-EEA3 和完整性算法 128-EIA3。ZUC 算法由 3 个基本部分组成，依次为：1、比特重组；2、非线性函数 F；3、线性反馈移位寄存器（LFSR）。

10.11.2.7.密码设备提供

根据福建省消防情况分析全省总有有 15000 家火灾风险单位，94 个监管单位，火灾风险单位通过互联网将感知数据传递给监管单位。因为互联网开放的原因，在通信线路传输过程中可能被非法侵袭者攻击、窃取或篡改，为确保业务信息得以保护，需进行网络边界控制和数据传输加密，保证业务信息的机密性、完整性和真实性。

为保障福建消防感知数据的传输安全，防止数据被非法窃取，需通过配备网络密码设备在互联网隔离出福建智慧消防感知数据传输的专用网络。

在 94 家监管单位部署 VPN 设备，15000 家火灾消防单位按照总队的规范自行采购 VPN 设备，需要满足 ipsec\ssl 协议，支持 SM2\SM3\SM4 加密算法，满足与监管单位 VPN 设备对接。通过监管单位与火灾风险单位启用并配置 IPSEC VPN 之间的互通策略，建立传输加密通道，实现对消防感知数据传输加密保护。在总队部署一套 VPN 管理系统，对 94 家监管单位部署的 IPSEC VPN 进行在线管理和监控。

本项目其它软硬件支撑环境依托数字福建电子政务云平台搭建，相关的软硬件密码设备由电子政务云平台提供。

10.11.2.8.密码管理措施

（1）密码设置应具有安全性、保密性，不能使用简单的代码和标记。密码是保护系统和数据安全的控制代码，也是保护用户自身权益的控制代码。密码分设为用户密码和操作密码，用户密码是登录系统时所设的密码，操作密码是进入各应用系统的操作员密码。密码设置不应是名字、生日，重复、顺序、规律数字等容易猜测的数字和字符串；

（2）密码应定期修改，间隔时间不得超过一个月，如发现或怀疑密码遗失或泄漏应立即修改，并在相应登记簿记录用户名、修改时间、修改人等内容。

（3）服务器、路由器等重要设备的超级用户密码由运行机构负责人指定专人（不参与系统开发和维护的人员）设置和管理，并由密码设置人员将密码装入密码信封，在骑缝处加盖个人名章或签字后交给密码管理人员存档并登记。如遇特殊情况需要

启用封存的密码，必须经过相关部门负责人同意，由密码使用人员向密码管理人员索取，使用完毕后，须立即更改并封存，同时在“密码管理登记簿”中登记。

（4）系统维护用户的密码应至少由两人共同设置、保管和使用。

（5）有关密码授权工作人员调离岗位，有关部门负责人须指定专人接替并对密码立即修改或用户删除，同时在“密码管理登记簿”中登记。

管理运维体系是福建省智慧消防云平台网络可靠、稳定运行的实现保障。各级管理部门及接入单位应加强对信息网络的安全管理，设立安全管理组织机构、制订健全安全管理制度，明确人员岗位的职责，加强人员安全管理、安全事件处理流程以及相应的操作规范，加强信息系统应急预案的建设。

1、机构与人员安全管理制度。

2、系统运行环境安全管理制度。

3、硬件设施安全管理制度。

4、网络安全管理制度。

5、数据安全管理制度。

6、技术文档安全管理制度。

7、应用系统开发、运行安全管理制度。

8、操作安全管理制度、应急安全管理制度。

在整个安全系统中最重要的安全保密因素是操作人员，上述有所有安全措施都是操作人员来实现的，因此，必要的安全意识教育与培训和严格的管理制度是系统安全的重要组成部分。

本项目运行维护系统依托福建省级政务外网电子政务云平台运行维护。

10.12. 物联网安全设计

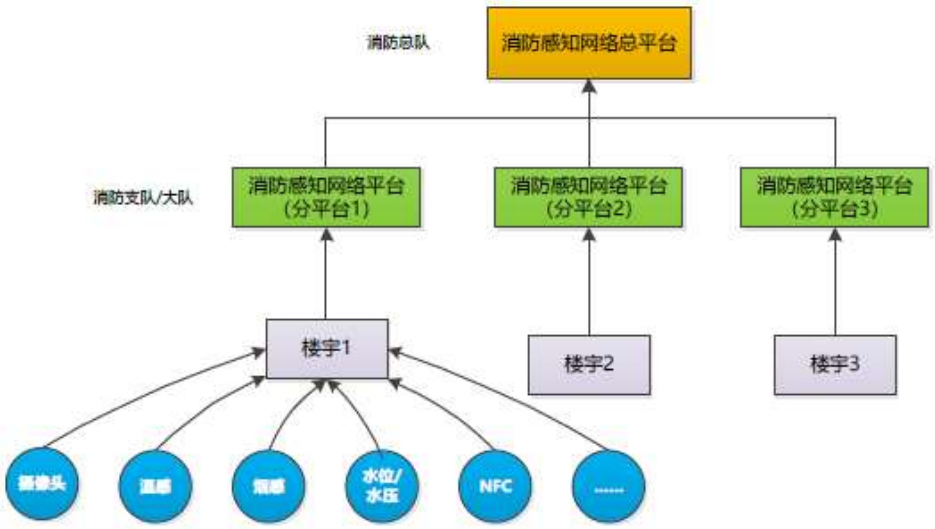
10.12.1. 物联网系统架构

10.12.1.1.物联网感知层

感知层包括感知层网关和传感器、RFID 等感知设备，也包括这些感知设备与感知层网关之间的短距离通信（通常为无线）。感知层网关是将感知设备所采集的数据传输到数据处理中心的关键出口，简单的感知层网关只是对感知数据的转发，而智能的感知层网关可以对数据进行适当处理、数据融合等。

在福建消防云平台感知网络中心服务器接入物联网前端感知设备，如：火灾探测器、声光警报器、电磁阀、高位水箱、低位水池液位、水压传感器等设备，包含火灾报警 监控子系统、建筑消防水监控子系统、消防电源监控子系统、消控室视频监控子系 统、消防电源监控子系统、消防巡查管理子系统等系统中感知数据。 由此可见，消防物联网系统感知网络体系的基础，就是终端的各种环境要素检 测感知设备设施 。

网格化消防感知层结构如下图：



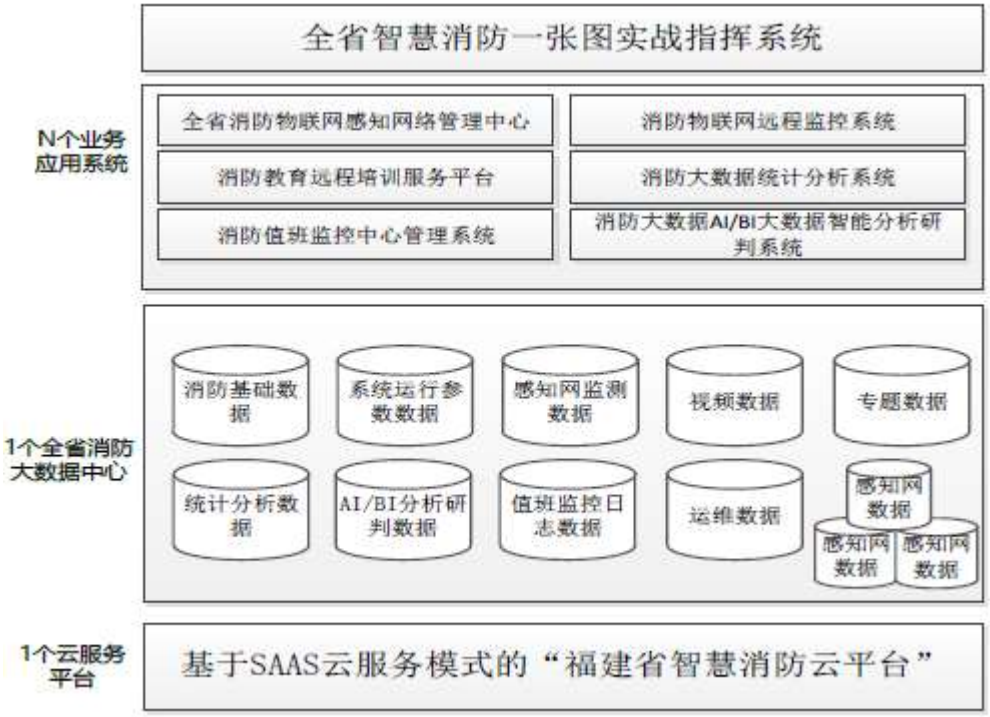
10.12.1.2.物联网网络层

网络层主要实现物联网数据信息和控制信息的双向传递，福建省消防救援总队现有的消防信息网、消防指挥调度网、互联网三张网络之间物理隔离。消防信息网按照属地原则就近接入国家电子政务外网，指挥信息网承载应急决策、指挥调度、协同会商、 态势分析等核心业务系统；国家电子政务外网承载政务办公、风险监测预警等应用；国家电子政务内网用于承载和处理涉密信息；互联网面向社会公众提供信息发布和 政务服务。在本次建设中互联网采集的数据资源以及物联网终端采集的数据通过安全边界进入消防云平台。

10.12.1.3.物联网应用层

应用层指对感知数据进行集中处理的平台，其中应用支撑是为应用服务提供基础支撑服务的系统，包括标识解析、数据存储、数据处理、数据管理等。对大型物联网应用系统来说，应用层一般是云计算平台，该平台的任务包括收集合法感知网络的真实数据，存储并管理这些数据，管理终端用户对这些数据的访问和使用，以及建立审计、授权、访问控制等机制。

根据福建省消防救援总队关于智慧消防云平台的总体规划思路，以及符合福建省消防救援总队提出的建立“1 个智慧消防大数据平台，N 个消防应用系统”的智慧 消防体系构想，本次消防云平台遵循该理念思想进行“1+N”平台应用设计。



针对消防管理中常见的管理需求，结合物联网、大数据等新技术发展，解决传统管理方式的弊端，向科技要效率，实现消防管理工作智能化、可视化、痕迹化。实现传统消防系统联网监控，并将消防电源监控系统、消防水监控系统、消火栓可 视化管理、视频监控、设备设施巡查管理、小微场所火灾预警等通过物联网的方式， 将消防基础数据信息化，统一汇聚至系统，将“人防、物防、技防”三结合应用于 传统的消防管理和监督。实现对消防核心系统关键信息的感测、分析、整合，从而对消防监督业务活动的各种需求做出智能响应。打破各消防监督业务系统之间的信息壁垒，使消防信息资源更有效地实现供需对接，推动消防工作模式从传统向现代、被动向主动、单一向综合、人工向智能的发展。

系统通过打通各类数据采集平台，避免“信息孤岛”，逐步完善消防资源数据库， 为各级响应力量能够及时掌握进行火灾防控提供决策辅助支撑。

主要为建筑物（群）年龄、耐火等级、电气线路、区域内单位火灾隐患危险等 级、公共消防设施运行情况、整体建筑火灾负荷等，及外围道路信息、水源信息、 消火栓信息、出入口信息、消防通道信息、重点部位信息、消防设备信息等环境数 据，结合区域范围内的典型火灾情况、历史重大火灾情况、人员密集场所分布、危 化品分布、整体情况、区域群众消防意识情况、天气状况、区域内灭火救援力量等 级等

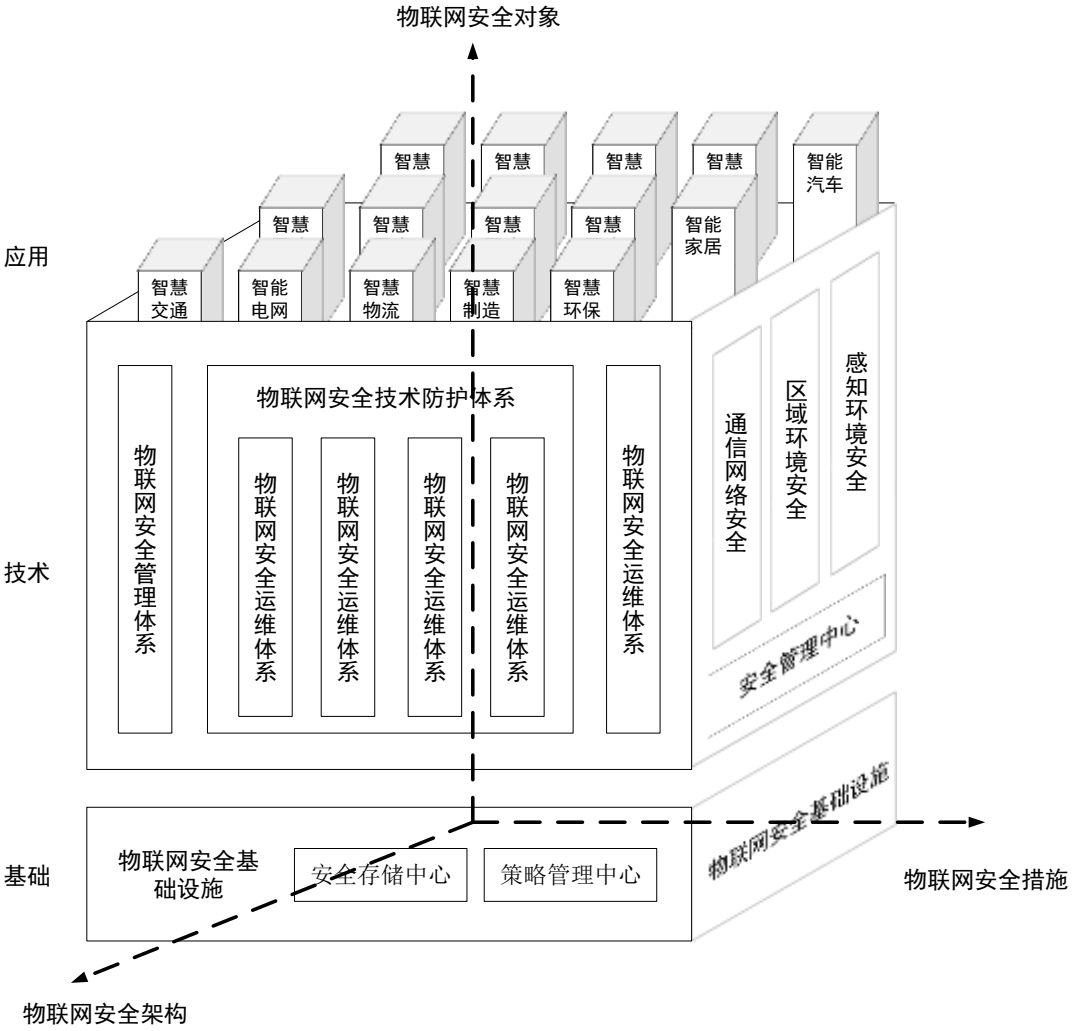
相关信息，将影响起火的因素和扩大蔓延趋势的因素建立基础汇总库，并整合 地理信息系统统一展现。同时，社区消防站、消防车辆、装备、消防人员等信息均 可通过平台进行信息录入、维护。

系统将构建统一消防资源数据库，并通过落地实施后逐渐扩展数据项，完善数据内容。数据来源主要包括消防内部数据、市政面数据、社会面数据三大类，采集 方式包括物联网自动采集、街道级平台调用、消防相关人员上报、互联网数据抽取等。

上述省智慧消防云平台业务应用系统、数据库存储系统等，部署于福建政务云平台上。同时由各地市、区县消防部门自建部署的消防物联网感知分中心服务器（分布式），通过政务外网汇聚接入至省智慧消防云平台服务器中。

10.12.1.4.物联网安全参考模型

福建消防云平台物联网安全参考模型从物联网安全对象、物联网安全架构和物联网安全措施三个维度描述物联网安全保护方法。物联网安全对象规范了物联网最终达到的安全目标，物联网安全架构规范了安全技术防护体系，物联网安全措施规范了具体实施环节的安全要素。



参考标准：

- NIST SP 800-53：《Security and Privacy Controls for Federal Information Systems and Organizations》
- ISO/IEC 20180:2012 Telecommunications and information exchange between systems - Security framework for ubiquitous sensor networks
- IEC 62443-1-1:2009 Industrial communication networks - Network and system security
- ITU-T Y.2060:Overview of the Internet of things
- GB 17859，计算机信息系统安全保护划分准则
- GB/T 18336 信息技术 安全技术 信息技术安全性评估准则

- GB/T 20281 信息安全技术 防火墙技术要求和测试评价方法
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 28448 信息安全技术 网络安全等级保护测评要求
- GB/T 28449 信息安全技术 网络安全等级保护测评过程指南
- GB/T 25070 信息安全技术 网络安全等级保护物联网安全设计技术指南
- YD/T 2437-2012 物联网总体框架与技术要求
- YDB 101-2012 物联网安全需求
- 信息安全技术 网络安全等级保护安全设计技术要求（征求意见稿）
- 信息安全技术 网络安全等级保护测评要求（征求意见稿）
- 信息安全技术 物联网数据传输安全要求（征求意见稿）
- 信息安全技术 物联网感知终端应用安全技术要求（征求意见稿）
- 信息安全技术 物联网感知层网关安全技术要求（征求意见稿）
- 信息安全技术 物联网安全参考模型及通用要求（征求意见稿）
- 《 物联网白皮书（2011 年） 》，工业和信息化部电信研究院
- 《 物联网白皮书（2016 年） 》，CAICT 中国通信院

10.12.2. 物联网安全威胁与需求分析

物联网是一个广义的信息系统，物联网系统安全属于信息系统安全的一个子集，许多传统的信息安全问题在物联网系统中也将面临到，此部分主要阐述福建省智慧消防物联网云平台特有的安全威胁及其安全需求。物联网系统的安全设计主要针对以下安全威胁构建安全防护框架，形成物联网系统安全防护体系。

10.12.2.1.物联网感知层

物联网感知延伸层作为物联网和物理世界交互的边界，该层中的各种信息通信节点具有信息处理和通信能力。物联网感知延伸层中各种信息通信节点的信息处理能力和安全能力强弱依赖于节点类型，如信息采集、标识读取、信息存储、根据网络指示执行特定动作等。需要建立对通信节点本身的安全机制，防止身份假冒，信息截取等常见攻击。保护物联网感知延伸层中各种信息通信节点所支持的通信手段可以有多种形式，如有线、无线、移动通信等方式，通常基于近距离通信技术，安

全方面多采用轻量级安全手段。 物联网感知延伸层中各种信息通信节点之间可以直接交互，也可以连接到物联网网络/业务层，和物联网网络设备、应用服务器、其他感知延伸层节点设备进行所需的交互，每一次交互都需要不同的信息安全技术来保证整个感知延伸层的安全。

10.12.2.1.1. 感知层安全威胁

- **非授权读取设备信息**

对于任意类型的感知设备或感知层网关，包括物联网终端、传感器节点和传感器网关，可能被攻击者物理俘获或逻辑攻破，攻击者可以利用专用工具分析出感知设备所存储的机密信息。

- **拒绝工作**

在感知设备被物理俘获或逻辑攻破后，攻击者可以采用破坏或修改配置的方式造成感知设备不能正常工作。

- **节点欺骗**

攻击者通过假冒网络中已有的感知设备或感知层网关，可以向感知网络注入信息来发动多种形式的攻击，包括监听感知网络中传输的信息，向感知网络中发布假的路由信息，重放已发送过的数据信息，传送假的数据信息等。

- **恶意代码攻击**

木马、病毒、垃圾信息的攻击，这是由于终端操作系统或应用软件的漏洞所引起的安全威胁。

- **隐私泄露**

与用户身份有关的信息泄露，包括个人信息、使用习惯、用户位置等，攻击者综合以上信息可进行恶意目的的用户行为分析。

- **网络中断**

路由协议分组，特别是路由发现和路由更新消息，会被恶意感知设备中断和阻塞。攻击者可以有选择地过滤控制消息和路由更新消息，并中断路由协议的正常工作。

- **网络拦截**

路由协议传输的信息，如“保持有效”等命令和“是否在线”等查询，会被攻击者中途拦截，并重定向到其他感知设备，从而扰乱网络的正常通信。

- **篡改**

攻击者通过篡改路由协议分组，破坏分组中信息的完整性，并建立错误的路由，造成合法感知设备被排斥在网络之外。

- **伪造**

感知层网络内部的恶意感知设备可能伪造虚假的路由信息，并把这些信息插入到正常的协议分组中，对网络造成的破坏。

- **拒绝服务**

拒绝服务主要是破坏网络的可用性，减少、降低执行网络或系统执行某一期望功能能力的任何事件。如试图中断、颠覆或毁坏感知层网络，另外还包括硬件失败、软件 bug、资源耗尽、环境条件等。包括在网络中恶意干扰网络中协议的传送或者物理损害感知设备，消耗感知设备能量。

- **路由攻击**

恶意感知设备拒绝转发特定的消息并将其丢弃，以使得这些数据包不再进行任何传播。另一种表现形式是攻击者修改特定感知设备传送来的数据包，并将其可靠地转发给其它感知设备，从而降低被怀疑的程度当恶意感知设备在数据流传输路径上时选择转发攻击最有威胁。

10.12.2.1.2. 感知层安全需求

- **物理安全防护**

需要采取措施保护感知设备或感知层网关避免失窃，或被攻击者物理上获得或复制。

- **访问控制**

需要采取访问控制的方式，防止末端节点被逻辑攻破，或向其它末端节点或网络设备泄露用户或末端节点信息。

- **身份鉴别**

为确保采集数据来源的合法性及有效性，同时避免非法感知设备接入网络，需

对感知设备进行身份鉴别；为控制合法感知层网关的接入，阻断非法感知层网关的连接，需对感知层网关进行身份鉴别。

- **数据保密性**

感知设备所存储的数据或所传送的数据要加密。

- **数据完整性**

需要采取措施防止感知设备所存储的数据或所传送的数据被篡改。

- **可用性**

需要采取措施保护感知设备，例如采用防病毒软件，防火墙等措施，使之不会被逻辑攻破或被病毒攻击导致不工作。

- **隐私保护**

需要保护感知设备所存储的用户隐私，并防止与用户身份有关的信息泄露。

- **数据源认证**

避免感知设备或感知层网关被恶意注入虚假信息，确保信息来源于正确的物联网设备。

- **新鲜性**

保证接收到数据的时效性，确保没有恶意感知设备重放过时的消息。

10.12.2.2.物联网网络层

物联网网络/业务层主要提供消息的路由寻址和传送功能，可以基于现有或未来的各种网络技术， 并可以有各种消息传送方式，如 IP 方式、短消息方式等。物联网可以是新构建的网络，或者是对现有网络进行功能扩展和能力增强。安全方面与现有网络类似。

物联网网络/业务层应能够获知物联网感知延伸层节点的通信状态。如果需要，物联网网络/业务层 可以提供到物联网感知延伸层节点的管理功能。

对于对消息传送的安全、可靠性、服务质量等有特殊的应用场景，物联网的网络核心应能够提供相 应的机制满足要求。

如果需要，物联网网络/业务层可以向应用层提供必要和所需的能力支持，如网络能力开放、终端能力适配等。 物联网应支持与其他物联网之间的互联互通。 由于不同物联网应用对移动性、通信模式、鉴权、处理模式、数据速率、安全性、可

靠性、交互性等业务交互特征和需求也存在很大差异，因此，物联网架构应具有智能和弹性，应能够通过充分利用各 种网络资源或通过能力增强，来满足不同物联网应用的服务需求，同时应能够实现网络资源和能力的共用。

物联网应具有扩展性，适应物联终端数量和业务种类的增加。

10.12.2.2.1. 网络层安全威胁

- **网络拥塞和拒绝服务攻击**

由于物联网设备数量巨大，如果通过现有的认证方法对设备进行认证那么信令流量对通信网络来说是不可忽略的，尤其是大量设备在很短时间内接入网络，很可能会带来网络拥塞，而网络拥塞会给攻击者带来可乘之机，从而对服务器产生拒绝服务攻击。

- **中间人攻击**

攻击者可以发动中间人攻击，使得物联网设备与通信网络失去联系，或者诱使物联网设备向通信网络发送假冒的请求或响应，从而使得通信网络做出错误的判断而影响网络安全。

- **伪造网络消息**

攻击者可以利用感知层网络的安全性等特点，伪造通信网络的信令指示，从而使得物联网设备断开连接或者做出错误的操作或响应。

10.12.2.2.2. 网络层安全需求

- **组认证**

基于组的形式对感知设备进行认证，避免大规模设备认证造成的网络信令拥塞并防止可能的拒绝服务攻击。

- **身份鉴别**

感知设备、感知层网关与网络的需采用多种鉴别方式实现双向身份鉴别。

10.12.2.3.物联网应用层

典型的物联网应用包括：监控报警类、数据收集类、信息推送类、视频监控类、

远程控制执行器类。从服务范围来看，物联网应用包括：公众服务、行业公众服务、行业专用服务。在应用层上，各自的软件系统，通信系统，数据库系统，管理系统等均需要一定安全手段进行保护，与现有方法类型。

10.12.2.3.1. 应用层安全威胁

- **隐私威胁**

隐私泄漏：隐私泄露是指用户的隐私信息暴露给攻击者，例如用户的病历信息，个人身份信息、兴趣爱好、商业机密等信息。

恶意跟踪：隐私信息的获取者可以对用户进行恶意跟踪。例如，攻击者可以通过标签的位置信息获取标签用户的行踪或者利用标识信息来确定并跟踪贵重物品的数量及位置信息等。

- **业务滥用**

物联网中可能存在业务滥用攻击，例如非法用户使用未授权的业务或者合法用户使用未定制的业务等。

- **身份冒充**

物联网中存在无人值守设备，这些设备可能被劫持，然后用于伪装成客户端或者应用服务器发送数据信息、执行操作。例如针对智能家居场景中，针对自动门禁远程控制系统，通过伪装成基于网络的后端服务器，可以解除告警、打开门禁进入房间。

- **信息窃听/篡改**

由于物联网通讯需要通过异构、多域网络，这些网络情况多样，安全机制相互独立，因此应用层数据很可能被窃听、注入和篡改。

- **抵赖和否认**

通信的所有参与者可能否认或抵赖曾经完成的操作和承诺。

- **重放威胁**

攻击者向目标（感知设备或物联网应用服务器）发送已接收过的消息，来达到欺骗系统的目的。

- **拒绝服务攻击**

目前的认证方式是应用终端与应用服务器之间的 1 对 1 认证。而在物联网中，终端设备数量巨大，当短期内这些数量巨大的终端使用业务时，会与应用服务器之间产生大规模的认证请求消息。这些消息将会导致应用服务器过载，使得网络中信令通道拥塞，引起拒绝服务攻击。

10.12.2.3.2. 应用层安全威胁

- **身份鉴别**

为防止假冒用户使用未授权的业务应用或者合法用户使用未定制的业务应用，用户请求使用业务前必须经过严格的身份鉴别；为防止末端感知设备身份伪造和克隆等攻击，需对感知设备进行身份鉴别。

- **组认证**

物联网应用通常对应大量的末端节点，这些末端节点可能构成一个组，物联网应用服务器需要提供对这些末端节点进行组认证的能力。

- **隐私保护**

保护行为或者通信信息不泄密，这些信息包括通信内容、用户地理位置和用户身份等。

- **数据完整性**

考虑到物联网络中恶意末端节点可能注入、篡改应用层消息。因此，物联网应用层需要避免未授权的删除、插入和复制操作。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的完整性保护。

- **数据保密性**

在物联网络中各种数据和消息只能让授权用户查看。保密性保护可以避免非授权访问和应用层数据内容非授权阅读。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的保密性保护。

- **防抵赖**

提供不可抵赖性机制，保证通信各方对自己行为及对行为发生的时间的不可抵

赖性。例如通过进行身份认证和数字签名，数字时间戳等机制避免对行为发生的抵赖。

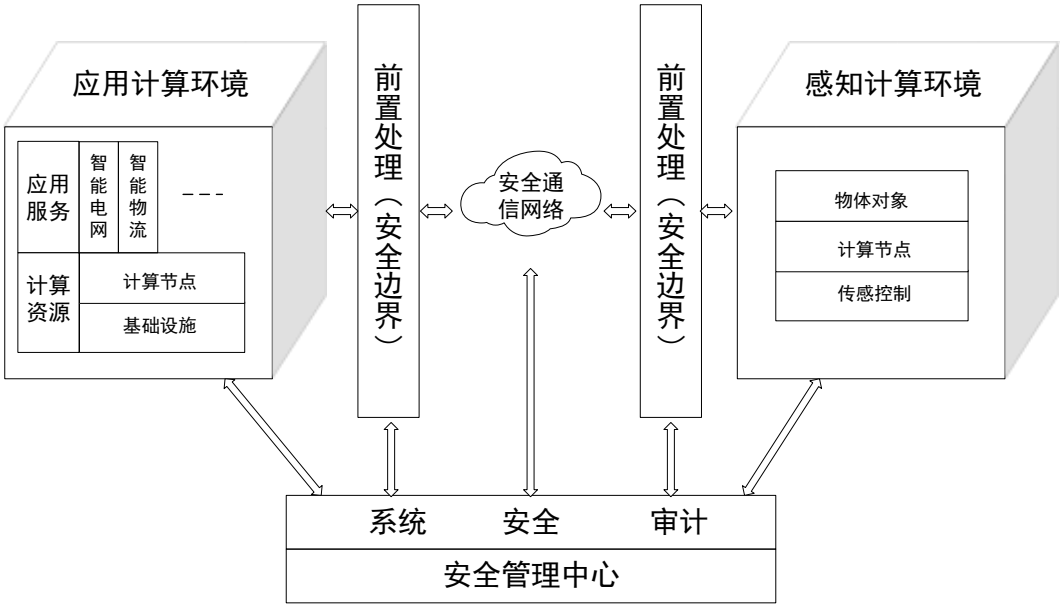
- **抗重放**

提供抵御重放攻击的机制。

10.12.3. 总体设计

10.12.3.1.设计思路

依据 GB/T25070-2010《信息安全技术 信息系统等级保护安全设计技术要求》和 GB/T 22239.4《网络安全等级保护基本要求 第 4 部分：物联网安全扩展要求》（审批搞，待发布），结合物联网系统的特点，构建在安全管理中心支持下的安全计算环境、安全区域边界、安全通信网络三重防御体系。信息系统等级保护物联网安全设计包括各级系统安全保护环境的设计及其安全互联的设计。各级系统安全保护环境由安全计算环境、安全区域边界、安全通信网络和（或）安全管理中心组成，其中安全计算环境、安全区域边界、安全通信网络是在计算环境、区域边界、通信网络中实施相应的安全策略。定级系统互联由安全互联部件和跨定级系统安全管理中心组成。



10.12.3.2.设计原则

福建消防物联网的安全建设基于等保合规和高可用性的特点，应该着重以下几

个方面：

- **高度确定性网络**

福建消防物联网承载了大量的数据信息同时物联网与普通网络的开放性，不确定性不同，核心特征是具有高度的确定性，因此福建消防物联网规划将通过落实高确定性来实现高安全性。物联网网络环境相对清晰明确，网络边界、通信协议、操作行为都可以通过管理制度、强制措施予以明确。物联网的用户身份、终端设备、政务应用、数据资源等安全防护对象是相对有限的，都可以被清晰定义。物联网的网络安全架构、标准、策略是可以被清晰定义，并通过政策、制度予以执行的。

- **网络环境的可信性**

边界可信（物联网所有网络边界都是清晰可描述的，包括互联网的连接、局域网的接入、终端设备的接入以及边界隔离交换设备策略等。）设备可信（物联网所有接入网络的设备都是明确无遗漏的，设备的使用和变更都被管理的，包括网络设备、安全设备、服务器设备和终端设备等。）网络访问可信（物联网所有的网络访问行为都是清晰可信的，包括网络交互的参与方、采取的通信协议、执行的操作行为等。）

- **网络状态的可知性**

设备接入可知（各类设备接入电子政务外网的情况是实时可知的，包括设备数量、设备类型、设备环境等属性）网络访问可知（物联网中各类访问行为是实时可知的，包括用户访问政务应用、政务应用间的连接情况、网络流量情况等。）安全事件可知（物联网的异常网络行为、异常的网络流量是实时可知的，包括对政务应用的攻击、可疑终端设备的接入等。）

- **网络风险的可控性**

控制的完整性（网络安全能力最大化覆盖构成物联网的各个层级以及所有的组成实体。）控制的动态性（能够随着物联网所面临安全威胁的变化动态调整安全防护能力，包括非授权人员的攻击防护和授权人员的异常访问。）控制的有效性（物联网内发现外部攻击行为或内部异常活动后，能够及时采取措施反制，恢复网络安全运行。）

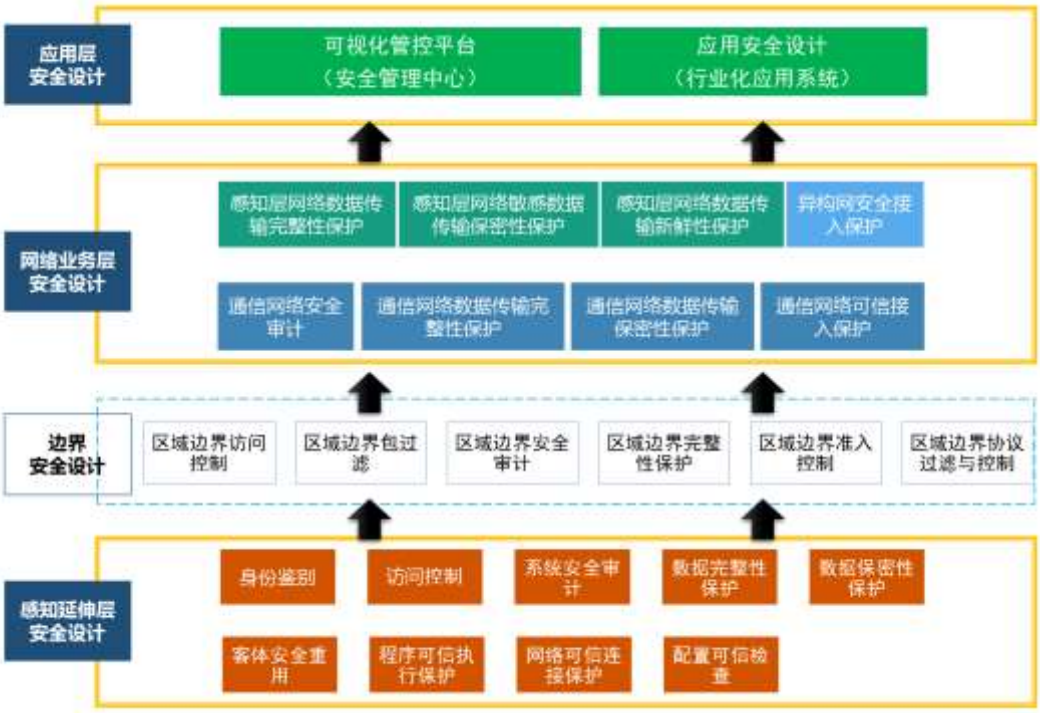
10.12.3.3.设计策略

本方案依据等级保护物联网三级安全要求从感知延伸层、网络业务层、应用层、

边界安全进行规划设计。

第三级系统安全保护环境的设计策略是：遵循 GB/T 22239.4-《网络安全等级保护基本要求 第 4 部分：物联网安全扩展要求》的 6.1 中相关要求，感知层实现感知设备和感知层网关双向身份鉴别；以区域边界恶意代码防范、区域边界访问控制等手段提供区域边界防护；以密码技术等手段提供数据的完整性和保密性保护，以增强系统的安全保护能力。

第三级物联网系统安全保护环境的设计通过第三级的安全计算环境、安全区域边界、安全通信网络以及安全管理中心的设计加以实现。



10.12.3.3.1. 物联网感知层安全设计

- **身份鉴别**

- **用户身份鉴别**

需要支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并

对鉴别数据进行保密性和完整性保护。

- **物联网系统身份鉴别**

（1）感知设备和感知层网关的身份标识和鉴别，安全管理中心对感知设备和感知层网关进行统一入网标识管理和维护，并确保在系统整个生存周期设备标识的唯一性；

（2）感知层网关与感知设备之间应采用受安全管理中心控制的口令、密钥或具有相应安全强度的其他机制实现双向的身份鉴别，并对鉴别数据进行保密性和完整性保护；

（3）应采用密码等技术支持的鉴别机制如国家密码行政主管部门规定的数字摘要算法、签名算法等，对感知设备发送的数据进行鉴别，确保数据来源于正确的感知设备且没有被恶意注入虚假信息；

（4）应采取措施对感知设备组成的组进行组认证，以减少网络拥塞，组认证可通过认证代理来完成，如物联网感知层网关或主设备；

（5）应采用密码等技术支持的鉴别机制如国家密码行政主管部门规定的数字摘要算法、签名算法等，对假冒用户使用未授权的业务应用或者合法用户使用未定制的业务应用进行鉴别，防止末端感知设备身份伪造和克隆等攻击。

- **访问控制**

- **自主访问控制**

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

- **标记和强制访问控制**

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

- **物联网系统访问控制**

（1）通过制定安全策略如访问控制列表，实现对感知设备的访问控制；

（2）感知设备和其他设备（感知层网关、其他感知设备）通信时，根据安全策略对其他设备进行权限检查，只有权限检查通过后，才允许设备间开始通信；

（3）感知设备进行更新配置时，根据安全策略对用户进行权限检查，只有经过授权的合法用户才能通过外部接口对感知设备进行更新配置、下载软件等。

- **区域边界包过滤**

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。

- **区域边界安全审计**

应在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。

- **区域边界完整性保护**

（1）信息系统区域边界完整性保护

应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。

（2）物联网系统区域边界完整性保护

应在区域边界设置轻量级的双向认证机制，能够保证防止数据的违规传输。

- **区域边界准入控制**

（1）应在安全区域边界设置准入控制机制，能够对设备进行认证，保证合法设备接入，拒绝恶意设备接入；

（2）应根据感知设备特点收集感知设备的健康性相关信息如固件版本、标识、配置信息校验值等，并能够对接入的感知设备进行健康性检查。

- **区域边界协议过滤与控制**

应在安全区域边界设置协议过滤，能够对物联网通信内容进行过滤，对通信报文进行合规检查，根据协议特性，设置相对应控制机制。

- **系统安全审计**

应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；确保对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；

对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

- **数据完整性保护**

- **用户数据完整性保护**

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

- **物联网系统数据完整性保护**

应采用密码等技术支持的完整性校验机制如国家密码行政主管部门规定的数字摘要算法、签名算法等，检验感知设备生存信息、鉴别信息、隐私性数据和重要业务数据在存储过程中完整性是否破坏，以及防止被非法复制，且在其受到破坏时能够进行恢复、重传等。

- **数据保密性保护**

- **用户数据保密性保护**

采用密码等技术支持的保密性保护机制，对在安全计算环境中的用户数据进行保密性保护。

- **物联网系统数据保密性保护**

应采用密码等技术支持的保密性保护机制如国家密码行政主管部门规定的对称加密算法、非对称加密算法等，对感知设备生存信息、鉴别信息、隐私性数据和重要业务数据进行保密性保护。

- **客体安全重用**

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

- **程序可信执行保护**

可构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。

- **网络可信连接保护**

应采用具有网络可信连接保护功能的系统软件或具有相应功能的信息技术产品，在设备连接网络时，对源和目标进行平台身份鉴别、平台完整性校验、数据传输的

保密性和完整性保护等。

- **配置可信检查**

应将系统的安全配置信息形成基准库，实时监控或定期检查配置信息的修改行为，及时修复和基准库中内容不符的配置信息。

10.12.3.3.2. 物联网网络层安全设计

- **通信网络安全审计**

应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警。

- **通信网络数据传输完整性保护**

应采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

- **通信网络数据传输保密性保护**

应采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

- **通信网络可信接入保护**

可采用由密码等技术支持的可信网络连接机制，通过对连接到通信网络的设备进行可信检验，确保接入通信网络的设备真实可信，防止设备的非法接入。

- **异构网安全接入保护**

（1）应采用接入认证等技术建立异构网络的接入认证系统，保障控制信息的安全传输；

（2）应采用入侵检测等技术拒绝恶意设备的接入，保证合法设备不被恶意设备攻击而被拒绝接入，保证网络资源的可使用性；

（3）应采用密码等技术支持的保密性保护机制如国家密码行政主管部门规定的数字摘要算法、签名算法、对称加密算法、非对称加密算法等，以实现异构网接入时数据传输完整性和保密性保护；

（4）应根据各接入网的工作职能、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，并采取相应的防护措施。

10.12.3.3.3. 物联网应用层安全设计

◆ 应用系统安全设计

➢ 身份鉴别

（1）应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

（2）应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

（3）应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

（4）应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

（5）应启用身份鉴别、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。

➢ 访问控制

（1）应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

（2）访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

（3）应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；

（4）应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

（5）应具有对重要信息资源设置敏感标记的功能；

（6）应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

➢ 安全审计

（1）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；

（2）应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

（3）审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

（4）应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

- **客体安全重用**

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

- **通信完整性保护**

（1）用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

（2）物联网系统数据完整性保护

应采用密码等技术支持的完整性校验机制如国家密码行政主管部门规定的数字摘要算法、签名算法等，检验感知设备生存信息、鉴别信息、隐私性数据和重要业务数据在存储过程中完整性是否破坏，以及防止被非法复制，且在其受到破坏时能够进行恢复、重传等。

- **通信保密性**

（1）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；

（2）应对通信过程中的整个报文或会话过程进行加密。

- **程序可信执行保护**

可构建从操作系统到上层应用的信任链，以实现系统运行过程中可执行程序的完整性检验，防范恶意代码等攻击，并在检测到其完整性受到破坏时采取措施恢复，例如采用可信计算等技术。

- **软件容错**

（1）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；

（2）应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

- **资源控制**

（1）当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

（2）应能够对系统的最大并发会话连接数进行限制；

（3）应能够对单个账户的多重并发会话进行限制；

（4）应能够对一个时间段内可能的并发会话连接数进行限制；

（5）应能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

（6）应能够对系统服务水平降低到预先规定的最小值进行检测和报警；

（7）应提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源。

◆ **可视化管控平台（安全管理中心）**

➢ **系统管理**

（1）信息系统管理

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，包括用户身份管理、系统资源配置、系统加载和启动、系统运行的异常处理以及支持管理本地和（或）异地灾难备份与恢复等。

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。

（2）物联网系统管理

a、应通过系统管理员对感知层的资源和运行进行配置、控制和管理，包括感知设备身份管理、标识管理、感知节点退出管理等；

b、应通过系统管理员对感知设备状态（电力供应情况、是否在线、位置等）进行统一监测和处理；

c、应通过系统管理员对下载到感知设备上的应用软件进行授权。

➢ **安全管理**

（1）信息系统安全管理

应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置一致的安全策略。

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，并进行审计。

（2）物联网系统安全管理

应通过安全管理员对系统中所使用的密钥进行统一管理，包括密钥的生成、分发、更新、存储、备份、销毁等，并采取必要措施保证密钥安全。

- **审计管理**

（1）应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行处理。

（2）应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

10.12.3.3.4. 物联网安全扩展要求设计

- **安全物理环境**

  - **感知节点设备物理防护**

（1）感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；

（2）感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能安装在阳光直射区域）；

（3）感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；

（4）关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久稳定的电力供应能力）应确保信息来源于正确的感知节点设备。

- **安全区域边界**

  - **接入控制**

应保证只有授权的感知节点可以接入。

  - **入侵防范**

（1）应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击行为；

（2）应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为。

◆ 安全计算环境

➢ **感知节点设备安全**

（1）应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更；

（2）应具有对其连接的网关节点设备（包括读卡器）进行身份标识和鉴别的能力；

（3）应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力。

➢ **网关节点设备安全**

（1）应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力；

（2）应具备过滤非法节点和伪造节点所发送的数据的能力；

（3）授权用户应能够在设备使用过程中对关键密钥进行在线更新；

（4）授权用户应能够在设备使用过程中对关键配置参数进行在线更新。

➢ **抗数据重放**

（1）应能够鉴别数据的新鲜性，避免历史数据的重放攻击；

（2）应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

➢ **数据融合处理**

应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一 个平台被使用。

➢ **安全运维管理**

（1）应指定人员定期巡视感知节点设备、网关节点设备的部署环境，对可能影响感知节点设备、网关节点设备正常工作的环境异常进行记录和维护；

（2）应对感知节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；

（3）应加强对感知节点设备、网关节点设备部署环境的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

10.12.3.4.实现方案

10.12.3.4.1. 物联网整体安全框架

结合上文对物联网环境三大层模型安全能力的论述，将福建消防物联网安全总结为 8 个安全建设维度，分别是物联网基础设施安全、物联网网络安全、物联网账户安全、物联网数据安全、物联网应用安全、物联网终端接入安全、物联网

安全服务、物联网可视化管控 8 个建设维度。方案将首先对这 8 个安全建设维度及其代表的安全能力进行论述，实现对 8 个安全建设能力的交付。

10.12.3.4.2. 物联网安全能力建设

◆ 物联网基础设施安全

在物联网基础设施安全方面，包含如下内容：

➢ 感知环境安全要求

物联网感知延伸层、网络/业务层和应用层由传感器等各类感知终端、路由器、交换机、计算机等物理设备组成，其物理安全是物联网安全的重要方面。

主要包括：

a）应制定物理设备的物理访问授权、控制等制度；

b）应具备可靠稳定的供电要求；

c）应具备防火、防盗、防潮、防雷和电磁防护等物理防护措施。

- **数据采集安全要求**

（1）数据可用性

感知终端在传输其采集到的数据时,应对数据新鲜性做出标识。

（2）数据完整性

感知终端应为其采集的数据生成完整性证据(如：校验码、消息摘要、数字签名等)。

- **安全能力清单**

序号	安全能力需求	安全能力描述
1	物理环境安全	由福建电子政务云机房提供
2	数据采集安全	实现对全类型网络攻击行为的检测与阻断处置

◆ **物联网网络安全**

- **安全能力要求**

- **安全能力清单**

序号	安全能力需求	安全能力描述
1	防火墙	实现基于接口、安全域、IP 五元组，应用的访问控制，支持时间表
2	防病毒网关	实现对病毒在边界的检测与阻断处置。
3	入侵检测\防御	实现对全类型网络攻击行为的检测与阻断处置
4	VPN 设备	实现客户端与服务端的通信，保护数据机密、完整性

◆ 物联网账户安全

➢ 安全能力要求

➢ 安全能力清单

序号	安全能力需求	安全能力描述
1	4A	实现物联网环境下安全能力包括统一的身份管理、统一认证管理和统一授权管理、统一审计管理四个方面
2	堡垒机	实现对运维人员的操作行为审计，及违规行为的阻断

◆ 物联网数据安全

➢ 安全能力要求

➢ 安全能力清单

序号	安全能力需求	安全能力描述
1	数据交换平台	实现物联网跨网数据交换，保证数据传输过程中不被恶意篡改、非授权访问
2	数据库审计	实现对数据库操作行为的审计
3	数据脱敏	对系统敏感数据进行识别、脱敏，防止数据泄露。
4	数据加密	对系统敏感数据进行识别、加密，确保数据完整性及可用性

◆ 物联网应用安全

➢ 安全能力要求

- **安全能力清单**

序号	安全能力需求	安全能力描述
1	WEB 威胁监测	针对 Web 应用系统，提供对各类 Web 应用系统的注入、XSS 等 Web 应用层的攻击识别
2	APP 渠道监测	实现物联网平台中的 APP 应用安全

◆ 物联网终端接入安全

- **安全能力要求**

- **安全能力清单**

序号	安全能力需求	安全能力描述
1	VPN	实现用户远程访问的身份认证和加密传输
2	可信接入网关	对接入的终端进行基于硬件特征的设备认证及基于数字证书的用户身份认证，同时为外网用户访问内网服务器提供访问控制
3	视频安全接入	能够检测针对视频监控网络的攻击行为，并进行拦截，有效保障视频监控网络的安全，除此之外，通过对摄像头、网络链路的状态检测帮助管理人员发现摄像头无法连接及带宽不足带来的网络视频图像卡顿甚至黑屏问题
4	移动 EMM	实现对移动设备的精细化管理，同时对于 APP 的安全检测、加固

5	终端风险管理	实现终端风险管理能力，具备终端威胁分析和溯源取证，资产管理、报表查看等力
6	轻量级加密认证插件	加密认证插件是软件模式的加密认证程序，可安装运行于具有完整操作系统的感知层终端中，该插件不仅需要完成对终端设备接收调度控制命令数据及其他信息进行加解密处理，而且还需要具有严格的防破译、防复制、防篡改等安全措施，确保保密该插件应用程序失控后不与任何非法设备进行信息交互，不对终端、系统的安全造成威胁
7	轻量级加密认证芯片	嵌入式加密认证芯片以硬件方式嵌入终端中，实现终端数据的加密认证和访问控制
8	轻量级加密认证设备	串联式接入专网方案是在感知层终端与网络层之间，以路由透明的模式部署加密认证设备，从而实现感知层终端的数据加密与认证
10	终端侦测与识别	对总队、支队、大队接入云平台的终端进行 ATP 攻击、蠕虫、勒索、挖矿等恶意程序的检测和响应

◆ 物联网安全服务

➢ 安全能力要求

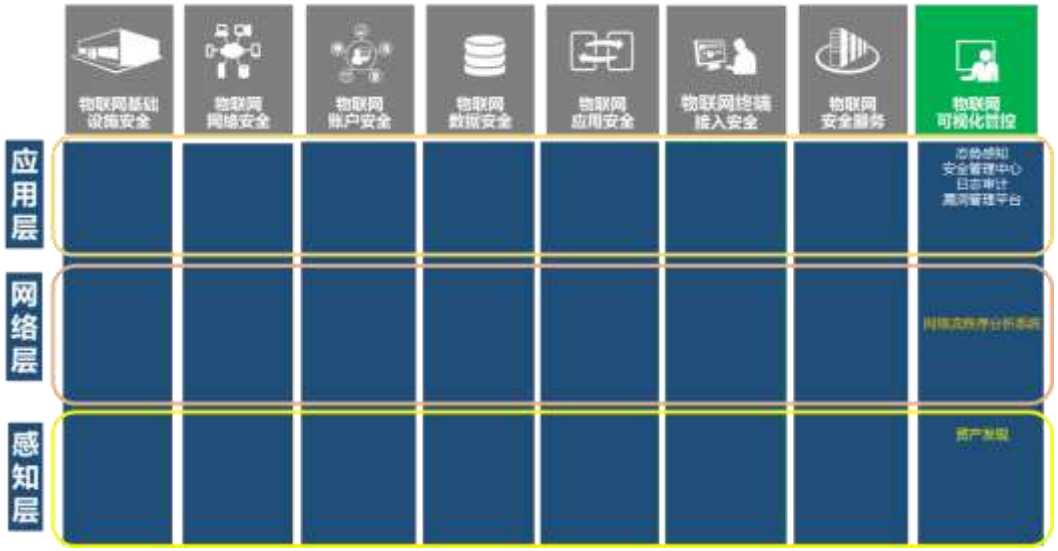
➢ 安全能力清单

序号	安全能力需求	安全能力描述
1	配置核查	基线检查包括应用系统、操作系统和数据库等不同层面的安全配置合规进行检查，要求新上线系统必须满足最基本或要求必须达到的安全性才可上线
2	漏洞扫描\工控漏扫	对评估范围内的系统进行安全扫描，查找对象目标存在的系统漏洞、弱口令、信息泄露及配置不当等脆弱性问题
3	端口扫描	对全网资产进行端口扫描，识别高危风险端口并给出合理化加固建议
4	弱口令扫描	对全网资产进行弱口令描扫，识别网络中存在的弱口令并

		进给出合理化加固建议
5	漏洞挖掘\ 工控漏洞挖掘	通过人工扫描、渗透、逆向分析、黑白盒测试等技术手段对系统进行全方位漏洞挖掘，包括对工控系统漏洞挖掘（需要提前调研研究工控系统的类型与特性，提出针对性测试方案）
6	安全补丁	实现链路负载均衡与应用负载均衡
7	安全加固	对发现的安全性问题进行安全指导、加固
8	系统最小化裁减	对系统最小化安全配置进行合理裁减，实现安全最大化
9	网站安全监测	实现网站实时安全检测与预警
10	网络安全评估	对物联网网络进行安全评估（需要提前调研研究物联网系统的类型与特性，提出针对性测试方案）

◆ 物联网可视化管控

➢ 安全能力要求



➢ 安全能力清单

序号	安全能力需求	安全能力描述
1	物联网安全态势感知	实现物联网环境中各类型多厂商安全监测防护资源的整合，通过现有及待建安全子系统的对接，态势感知系统可覆盖全网攻击行为信息、资产及业务脆弱性信息、异常流量信息、威胁情报及未知威胁等信息，并在此基础上综合分析呈现，形成包括被攻击对象和攻击源识别、脆弱性识别、攻击过程及影响分析、安全风险态势等在内的多视角全方位的态势感知
2	安全管理中心	满足物联网自身安全管理需求，实现整体安全状况、业务安全状况、安全监测、安全预警等能力，可实现与态势感知平台的智能联动和安全态势展现
3	日志审计系统	实现对网络设备、服务器、安全设备的日志收集及分析，可实现与态势感知平台的智能联动和安全态势展现

4	漏洞管理平台	通过漏洞扫描、公网爬虫等技术手段采集漏洞信息并与网内资产进行关联告警，实现漏洞闭环管理，可实现与态势感知平台的智能联动和安全态势展现
5	全流量分析系统	以深度流分析技术（DFI）为基础， 结合 DPI、日志分析等技术以一体化融合的威胁识别技术为客户实现资产持续监测、未知安全威胁检测及告警、合规管理、取证分析等，发现其他解决方案不能发现的入侵和违规行为，保证网络的正常、有序，提升网络安全等级，可实现与态势感知平台的智能联动和安全态势展现
6	资产发现	通过对全网资产扫描、探测，及时发现未知资产并进行告警，能够实时掌握网内资产动态，可实现与态势感知平台的智能联动和安全态势展现。

第11章　项目建设与运行管理

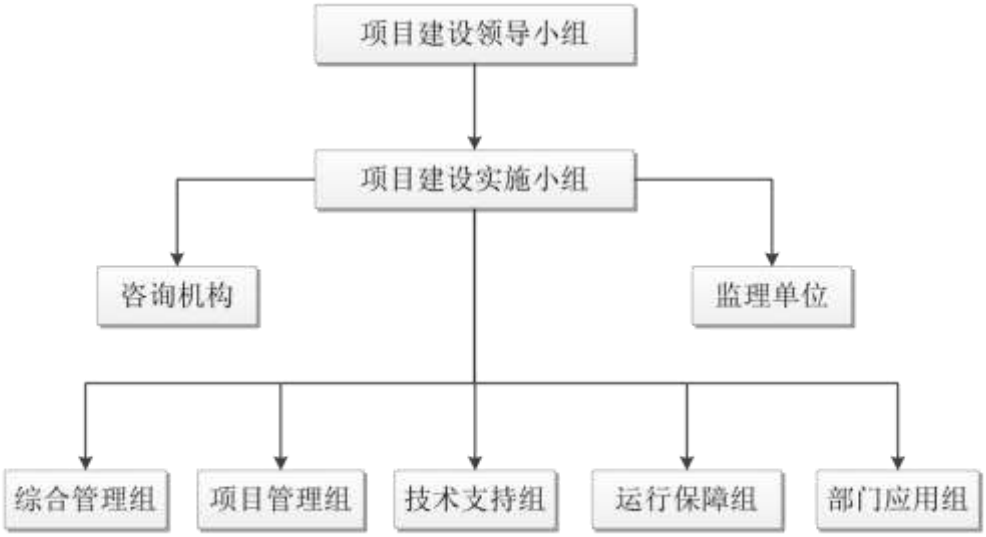
11.1.领导和管理机构

11.1.1. 管理组织机构

一个项目成功，除了优质合理的设计、可靠和高性能的软、硬件，也离不开良好的项目实施和针对项目的必要培训。本章将针对项目实施和培训提出相应建议。

福建省智慧消防云平台项目是一项较大规模的信息化建设系统工程，为了对项目实施能进行有效的管理，使项目参与各方能进行有效的沟通，必须对项目组织机构各方进行明确的职责划分。

为保障工程建设的顺利实施，本项目拟成立“智慧消防”项目建设领导小组。领导小组下设“智慧消防”项目建设实施小组、项目管理咨询机构和监理单位等。领导小组各机构明确职责，分工负责，完成各机构的工作任务。



项目领导小组全面负责项目建设和运行的领导、组织工作，对重大的技术、管理、业务规范和部门关系协调等进行决策，确定建设目标，审查建设方案，按照相关部门批准的建设方案组织实施。

项目领导小组应进一步加强对福建省智慧消防云平台项目的宏观决策和指导，进一步优化“智慧消防”平台建设布局，确保本项目建设沿着科学化、规范化、网络化方向健康发展。

信息化项目建设要接受项目领导小组领导，贯彻落实领导小组的决定，在项目的规划、设计、实施、管理、运行等各个环节中制定规范，组织实施，并协调解决工程建设问题。

11.1.1.1. 项目领导小组主要职责

制定项目的方针及策略，并指导项目实施小组的工作；

批准项目计划，监控项目的进程；

负责调配项目人力和资金；

推动并监管项目培训工作的进行；

审批新系统的工作准则与工作流程，确保项目逐步顺利实施；

解决项目实施小组职权所不能解决的问题。

领导小组每 2 周至少一次例会，领导小组组长应经常关注、参与和指导实施工作，及时处理各种问题。

11.1.1.2. 项目建设实施小组主要职责

负责统筹协调推动福建省智慧消防云平台各应用子系统的联网应用工作；

汇总并通报各、各部门年度工作情况，以及为落实工作任务制定的本地区、本行业、本领域开展消防物联网监测、消防安全监管、消防服务等工作的有关情况；

研究制定推进智慧消防平台相关工作发展的配套政策，加强对各地区、各行业、各领域智慧消防应用子系统联网应用工作的监督、指导和考核；

负责对该项目实施相关职能单位的协调工作；

负责项目经费的管理和监督；

负责承办领导小组交办的其他事项。

11.1.1.3. 综合管理小组主要职责

组织起草建设有关管理制度；

对重大项目进行会审，报“办公室”审批；

组织审核建设项目负责调整项目建设计划；掌握建设进展情况；督促检查项目实施计划的执行情况；组织审核建设项目的标书和合同书；组织开展建设经验交流

和技术交流；

负责建设的标准化管理工作；

负责各部门协调和监督指导工作；

负责各部门工作落实和考核工作。

11.1.1.4. 项目管理小组主要职责

负责申请“智慧消防”建设资金；

组织项目的中期评估和竣工验收工作；

组织项目的招投标、政府采购工作；

组织项目的工程监理工作；对项目建设过程中的立项、设计、签订合同和实施各个环节进行监督；

协调开展对专项资金和项目经费使用情况的内部审计。

组织协调有关单位对建设项目的使用效果和社会经济效益进行评估；

审核项目建设资金。

11.1.1.5. 技术支持小组主要职责

负责编制总体技术方案；

会同有关单位研究、提出业务应用系统的信息采集、数据整合和应用集成的方案，协调推进跨部门信息资源共享和业务系统整合。

负责消防物联网资源数据标准制定、接入和授权规范制定、智慧消防各应用子系统资源应用标准制定、各消防数据资源安全等级规范制定、跨部门消防数据资源共享应用规范等；

负责消防数据资源规范制定，建立统一的数据标准，智慧消防各应用子系统应用标准制定，设计基础设施管理系统、运营管理系统、安全管理系统的功能和实现方案；

推进全省各地市、区县消防物联网数据资源联网整合，实现消防物联网监测数据、分析数据最大限度的共享共用。

11.1.1.6. 运行保障小组主要职责

维护平台正常运行。进行资源管理和授权访问服务。

11.1.1.7. 部门应用小组主要职责

提供各部门的基础消防数据、监测数据、基础分析数据等资源；

维护管理消防物联网感知网络硬件设施；

提供消防物联网数据资源服务等。

根据各自工作需要，建设标准统一的消防物联网远程监控分中心。其他各单位应建设本单位的消防物联网监控室。

11.1.2. 项目管理模式

项目由福建省消防救援总队防火监督处进行项目管理，主要从以下几个方面开展工作：

1.项目启动：启动项目，包括发起项目，授权启动项目，任命项目经理，组建项目团队，确定项目利益相关者。

2.项目策划：包括制定项目计划，确定项目范围，配置项目人力资源，制定项目风险管理计划，编制项目预算表，确定项目预算表，制定项目质量保证计划，确定项目沟通计划，制定采购计划。

3.项目执行：当项目启动和策划中要求的前期条件具备时，项目即开始执行。

4.项目监测：实施、跟踪与控制项目，包括实施项目，跟踪项目，控制项目。

5.项目完成：也叫作收尾项目，包括项目移交评审，项目合同收尾，项目行政收尾。

11.2.项目实施机构

省总队防火监督处负责项目具体实施，并成立项目实施小组，下设技术支持组、建设支撑组，以确保项目按计划、保证质量建设。

针对项目实施过程中遇到的具体技术问题，组织专家咨询。项目实施小组负责项目实施的日常工作，配合工信、数字办等部门和有关部门进行的论证、评审等项

目前期工作，负责项目的立项、经费的申报和计划管理、有关项目的协调、检查监督、人员培训计划以及技术管理等工作。

11.3.项目实施进度

本项目的建设周期包括可行性研究报告暨初步设计方案批复在内为16个月（智慧消防平台建设第一期）。

项目实施进度计划（第一期完成目标）如下：

持续时长1个月：发出招标通知后一个月内完成项目招投标工作。

持续时长1个月：合同签订后，协调相关部门一个月内完成需求调研。

持续时长8个月：项目需求确认后，八个月内完成系统开发及调试。

持续时长 1 个月：系统功能开发完成后，协调相关部门一个月内完成系统对接联调，并初验交付使用。

持续时长3个月：初验完成后，系统试运行三个月。

持续时长1个月：试运行完成后，开展第三方测试。

持续时长1个月：第三方测试完成后，一个月内完成项目终验。

11.4.项目进度、质量、资金管理方案

11.4.1. 项目进度管理方案

本工程工期紧，任务重，为对施工进度进行有效控制，按时按质完成工程，需要有一个简明实用、有效的工程进度控制方案。

工程实施进度的控制是一个计划编制审核、检查分析与反馈调整的动态控制过程。其目标就是实现工程进度控制总目标，主要包含以下内容：

1、工程进度的跟踪检查

对工程进度的执行情况进行动态检查并分析进度偏差产生的原因，为进度计划的调整及实现工程总进度目标提供必要的信息。工程进度的检查包括对各作业项目完成情况的检查和工程总进度完成情况的检查。

2、进度偏差原因的分析

在检查过程中发现进度偏差要及时分析原因，研究相应的对策和解决方法。影

响工程进度的因素很多，除人力、资金等因素处，还包括设计因素、技术因素、组织管理因素、信息沟通、外部环境的影响及各参建单位的协调配合问题等等。

3、工程进度控制计划的调整

在进度计划的实施过程中，常常受各种因素的影响而出现进度偏差。为了保证工期总目标的实现，必须对原计划进行相应的调整。计划的调整有如下原则：

- 计划调整应慎重，能不调的尽量不调，能局部调整的绝不大范围调整；
- 计划调整要及时，一发现有进度偏差，必须及时分析，立即采取相应对策及时解决，问题解决得越早，对整个工程项目的影响和冲击就越小。

11.4.2. 项目质量管理方案

项目质量管理主要通过以下措施实现：

建立完善的质量保证体系，配备高素质的项目管理和质量管理人员，强化“项目管理，以人为本”；

严格过程控制和程序控制，开展全面质量管理；

制定质量目标，将目标层层分解，质量责任、权力彻底落实到个人，严格奖罚制度；

建立严格而实用的质量管理和控制办法、实施细则，在工程项目上坚决贯彻执行；

严格质量检查和审批等制度；

强化质量检测和验收系统，加强质量管理的基础性工作。

11.4.3. 项目资金管理方案

本项目由福建省财政厅拨付项目预算资金，在资金使用过程中严格按照相关规范和制度执行。

11.5.运行维护机构与运行维护管理制度

为保证福建省智慧消防云平台的正常运行，建议组建专门的运维队伍，负责平台的软硬件运行维护以及应用日常运行维护、管理等工作。运维人员由福建省消防

救援总队防火监督处相关人员组成，平台设备与应用软件提供商负责支撑。

福建省消防救援总队防火监督处牵头负责系统平台日常的运行管理、使用维护，硬件系统的维护由设备供应商负责支撑，软件系统由软件提供商负责支撑。

各业务部门承担各自办事项目的流程优化、配置及业务数据维护等工作。

（1）维护和维修内容

维护维修内容	具体说明	提供的人员及方式
应用软件的维护升级	包括政务网应用、外网应用，主要维护内容如下：程序错误的修正，漏洞更新，主要是为了保证系统的功能更完善和性能的进一步改善	系统软件开发商需要负责系统正式验收以后起 3 年的技术支持

（2）设备及软件供应商维护要求

维护维修策略：平台通过验收后，即应履行 3 年的缺陷责任期（质保期）和售后服务保证。

保修和维护保证：对所提供的设备，必须在厂商提供的质保期的基础之上，对整个系统必须提供 3 年的正常运行保证期。在此期间，厂商需要负责整个系统的设备正常运行，并提供专业的技术支持与服务，必须保证一定数量的备品备件，以确保整个系统不会因为维护而影响正常使用。

快速响应：对客户的服务请求，必须在接到报告后两小时内处理。必要时，应赴现场解决问题。

定期维护：必须定期对系统和产品的技术近况进行调查及检验，排除故障隐患，为建设单位安全可靠的使用系统提供有效的保障。

11.6.项目招标方案

11.6.1. 招标范围

考虑到本项目工程技术特点、建设任务的构成及规模，根据《中华人民共和国招标投标法》《中华人民共和国政府采购法》《项目可行性研究报告增加招标内容和核准招标事项暂行规定》（国家发展计划委员会 9 号令）《福建省招标投标条例》《福建省省级政府协议定点采购管理暂行办法》《福建省省级政府集中采购目录及限额标

准》《福建省省级单位委托政府采购代理机构管理办法（试行）》等的相关要求，确定本项目招标范围如下：

（1）系统软硬件采购、开发及集成。

（2）主机及存储系统、终端系统及安全系统等设备的采购。

（3）工程初步设计、工程监理、系统集成等工程咨询服务。

（4）第三方评测费用（软件质量、网络安全）。

11.6.2. 招标方式

依照《招标投标法》的规定和项目建设特点，本项目招标方式拟采取公开招标形式。招标中坚持公开、公平、公正的原则，要求投标人在法律法规的约束条件下进行投标竞争，并使整个过程置于透明的环境之中，选择真正符合要求的供货商、承包单位，使国家利益和社会公共利益得到保护。

11.6.3. 招标组织形式

招标分为招标人自行组织招标和招标人委托招标代理机构代理招标两种组织形式。其中：

自行招标：具有编制招标文件和组织评标能力，并向有关行政监督部门备案的招标人，自行办理招标事宜，组织招标投标活动。

委托招标：招标人自行选择具有相应资质的招标代理机构，委托其办理招标事宜，开展招标投标活动；不具有编制招标文件和组织评标能力的招标人，必须委托具有相应资质的招标代理机构办理招标事宜。

按照相关规定，由福建省消防救援总队委托具有相应资质的招标代理服务机构负责工程的招标组织工作。

11.6.4. 相关工程服务招投标

1、技术总承方的确定

建议通过公开招标方式确定项目的技术总承单位，项目的技术总承单位代表建设方，对项目的技术质量把关。

2、其他研制单位的确定

对于本项目的相关经费，建议由福建省消防救援总队按照有关规定，通过公开招投标方式，确定有关承担单位。

表 11-1：招标内容表

招标类别		招标范围		招标组织形式		招标方式		不采用招标方式	招标估算金额（万元）	备注
		全部招标	部分招标	自行招标	委托招标	公开招标	邀请招标			
工程服务	设计	✓			✓	✓				
	技术总承及系统集成	✓			✓	✓				
	监理	✓			✓	✓				
软件开发	应用软件	✓			✓	✓				
设备购置及安装	设备	✓			✓	✓				
	系统软件和支撑软件	✓			✓	✓				
情况说明：										

第12章　人员配置与培训

为保证项目移交后能有效使用该平台，在项目建设过程中需对相关人员进行应用培训，在以后系统运行过程中亦需根据系统开发、应用的深入针对不同培训对象进行相应内容的培训，以保证系统的管理人员、技术人员和应用人员能够及时、准确地了解和熟练地运行系统。

12.1.人员配置计划

福建省智慧消防云平台的人员配置工作要坚持结构合理，以补充缺额、优化结构为目标，合理布局，促进人员合理分布、均衡支撑，确保在编人员动态平衡的基础上，实现人员队伍可持续发展；坚持以用为本，健全测评、使用和约束机制，提高人员使用效果；建立按岗定责，促进人员有效使用。

福建省智慧消防云平台值班监控中心和运维中心设在福建省消防救援总队指挥中心，指挥中心 24 小时不间断运行值班，值班主任 1 人，值班人员编制 8 人。项目建成后（自竣工验收之日起）3 年内，系统运行维护由项目中标单位组织运营团队，3 年后系统运行维护可采取外包方式。

12.2.人员培训需求和计划

12.2.1. 培训需求

系统培训适应提供以下培训资料，并通过实际操作对相关工作人员进行培训，以可以完成日常运行维护操作为培训完成标准。

- 各系统设计方案
- 各系统操作手册
- 各系统维护手册
- 各类软硬件产品技术手册

- 厂商认证教材

12.2.1.1. 项目管理知识培训

项目管理知识培训的对象是项目管理小组，培训内容包括项目管理知识体系，目前项目管理知识体系的事实标准是美国项目管理协会的 PMBOK，其总结了全世界成功实施项目的方法、技术及经验。内容包括：整体管理、范围管理、时间管理、成本管理、质量管理、风险管理及采购管理等，培训目标是保证项目管理小组的项目管理人员对先进的项目管理知识有比较全面、深刻地了解，并且能把这些知识应用到系统工程的项目管理中。确保工程建设在可控的范围内，提高项目实施成功的可能。

12.2.1.2. 信息技术培训

信息技术培训分为基础知识培训和专业知识培训两种，培训对象分别为项目管理人员和专业技术人员。

基础知识的培训内容包括系统建设的理论、信息系统工程设计方案、信息系统建设项目管理、信息系统建设项目监理等，目的是使项目管理人员从总体技术实现对系统建设有深刻的认识，确保项目质量。专业知识培训主要包括面向对象的分析与设计、中间件产品与技术、数据库技术、计算机网络技术等。通过技术培训和技术交流，提高全体参与系统建设的技术人员的技术水平，为工程的设计、开发、实施和维护奠定坚实的技术基础。

12.2.1.3. 业务及标准培训

培训包括对业务人员和审查人员及主管部门的培训。按照系统工程的要求，将安排对参与开发的技术人员进行业务培训，使之深入理解系统设计方案，为将来的开发打下业务基础。技术人员同时应掌握相关的项目管理工具、技术及方法，能够很好的理解项目进度安排，质量计划，风险应对计划等，从而保证项目的顺利执行。各市属单位信息主管、技术人员应参加接口标准培训，了解系统接入的各种标准，为接口开发做相应的技术准备。接口标准是效能绩效考核管理系统信息共享的保证，严格的按照标准执行的接口接入是保证整个系统有效果、有效益的保证，因此标准

的培训是非常必要且不可或缺的。

12.2.2. 培训计划

在培训的开始，由每期培训班的课堂负责人，负责考勤及活动组织。要求每天的上午、下午正式上课时需要签到。

原则上，在每个培训班上需要安排 3 名培训人员进行培训，其中 1 名为讲师，其余 2 名作为辅导老师，协助培训学员上机操作并答疑。

在培训的过程中，培训讲师要根据课程表的安排进行讲解。每一期培训班的内容将设置多个环节，每一个环节都分为授课和练习两部分，授课部分要按照培训讲义对当期培训班所设置的内容进行详细的介绍，并配有培训教材以做参考。练习部分要求学员按照事先准备好的案例进行实际操作，以加强对所学知识的记忆和理解。

在课堂上，参与培训人员若有疑问，可先记录下来课下交给讲课老师，讲课老师将在练习阶段或下一个培训环节给予答复。

讲课老师及辅导老师每天把培训人员的疑问进行记录下来，汇总并提炼后形成问题集锦，在培训结束时发放给每一位培训人员。

12.2.3. 培训方式

针对不同阶段，不同人群，需采用不同的培训方式，从而使培训更能够针对特定用户需求。

12.2.3.1. 系统管理员培训

在系统正式投入运营后，系统管理员是保证系统长期稳定运行的主要人员，因此系统管理员应掌握系统各方面的知识，从系统构架到操作使用方法，到故障排除，到获取技术支持等。系统管理员从一开始就参与到系统的开发建设中来对于以后的有效维护有着重要作用，是深入理解系统的有效途径。系统在上线运行后要求具有高可靠性，高可用性，因此一旦运行就需要尽量联机，因此对管理员的素质提出了较高的要求，而这些素质必须通过完善的培训得以解决。鉴于系统管理员的培训工作如此重要，应在项目开发建设阶段就做好详细的培训计划，并认真组织实施。

12.2.3.2. 各级管理人员培训

对各级管理人员应采取全面掌握相关技术及操作的原则进行培训，该培训以参与部分开发建设工作的方式展开，从系统建设开发时期便开始进行，从而保证对系统从底层到全局的把握。

12.2.3.3. 业务、审查、主管人员培训

对业务人员、审查人员及主管人员应采取全面掌握操作流程的原则进行培训。

12.2.4. 培训成本估算

表 12－1 培训费用估算

序号	培训对象	参加培训人数	培训内容	培训单位	培训时间	培训费用
1	数据库系统管理和维护人员	10 人	数据库系统培训，包括数据库的使用、开发、管理、规划与日常维护技术。	软硬件厂家	3 天	
2	应用服务器中间件管理和维护人员		应用服务器培训，包括应用服务器启停、优化、管理和日常维护技术。	软硬件厂家		
3	应用系统管理、维护人员		应用子系统的架构和各类功能，具体操作，错误的原因和查找方法，系统日志管理，系统用户管理等。	系统软件开发单位		
4	各地市、区县消防部门（每单位 2 人）	180	消防物联网远程监控系统、消防教育培训服务平台、消防感知网平台等应用系统的基本操作。	软硬件厂家	10 天	

第13章 投资概算和资金来源

13.1.项目总投资及资金筹措方案

本报告方案总投资概算为5834.4万元，其中工程费用5304万元，工程建设其他费用530.4万元。

项目由福建省发改委批准立项，建设资金申请从以下几个渠道综合安排：

1．财政厅年度信息化专项资金。

2．省政府专项经费。

3．“数字福建”建设经费。

4．云资源经费每年单列，不计入建设资金。

项目由福建省消防救援总队负责组织实施，详细预算表格参见“概算编制”“投资概算书”章节。

13.2.概算编制说明

13.2.1. 投资概算范围

本项目投资主要用于福建省智慧消防云平台项目，以及项目系统集成与培训费、信息工程监理费、软件系统测试与网络安全测评费、项目管理和可研报告及初步设计费。

13.2.2. 编制依据

1、国家发展和改革委员会、建设部《工程勘察设计收费标准（2002年修订本）》；

2、国家发展和改革委员会、建设部《项目经济评价方法与参数（第三版）》；

3、国家发改委2007年第55号令《国家电子政务工程建设项目管理暂行办法》；

4、财建[2002]394号《关于印发基本建设财务管理规定的通知》；

5、计价格[1999]1283号《关于印发建设项目前期工作咨询收费暂行规定的通知》；

6、发改价格[2007]670号《建设工程监理与相关服务收费管理规定》；

7、发改高技[2008]2071号《关于加强国家电子政务工程建设项目信息安全风险

评估工作的通知》；

8、计价格[2002]1980 号《招标代理服务收费管理暂行办法》；

9、《中国软件行业协会软件工程定额标准》；

10、《软件开发项目概算指南》；

11、《信息系统工程造价指导》等。

12、福建省发展和改革委员会《福建省数字福建项目管理办法》；

13、“数字福建”的相关标准；

14、通信信息工程建设的有关费率标准；

15、根据以往经验估列。

13.2.3. 费率取定与说明

本工程的投资概算具体的费率取定如下：

1、硬件购置费根据闽数字办技术〔2005〕8 号，并参考市场价格确定，设备安装费已含在设备费中；

2、项目系统集成与人员培训费用按工程费用的 3%取定；

3、项目系统测试与安全测评费用按工程费用的 2%取定；

4、项目系统监理费用按工程费用的 2%取定；

5、项目管理与可研初设费，按 3%取定；

6、不计取预备费；

7、软件开发按 0.8 万元/人月估算，包括前期研发和现场实施的人员工资、补助、税费、管理费等；

8、机房及管理用房不列入本项目的投资范围，机房建设费用仅包括由于本项目建设需要增加的配套设施费用。

13.3.投资概算书

13.3.1. 投资概算总表

编号	项目名称	投资预算 (万元)	备注
一	工程费用	5304	

1	**消防大数据中心建设**	**308**	
1.1	消防数据结构设计开发	16	
1.2	数据资源目录体系建设	72	
1.3	数据库安全管理	16	
1.4	数据资源层建设	80	
1.5	数据资源存储建设	28	
1.6	数据汇聚与融合分析设计开发	48	
1.7	消防大数据中心应用管理系统	48	
2	**智慧消防应用系统建设**	**2140**	
2.1	物联网感知网络管理系统	124	
2.2	消防物联网远程监控系统	336	
2.3	消防数据基础统计分析系统	100	
2.4	基于大数据火灾智能预警模型分析系统	600	
2.5	消防值班监控中心管理系统	112	
2.6	基于 BIM 消防应用系统	300	
2.7	消防大数据一张图综合展示系统	40	
2.8	消防教育远程培训服务平台	508	
2.9	闽消通手机 APP 应用	320	
3	**平台基础应用支撑保障体系建设**	**728**	
3.1	软件应用基础支撑功能	500	
3.2	区块链应用体系建设	76	
3.3	接口应用体系建设	152	
4	**平台运维服务**	**800**	
4.1	业务运维服务（总队）	500	
4.2	技术运维服务（平台）	300	
5	**云计算平台租赁费用**	**1028**	
5.1	基础软硬件（云平台服务器主机）	528	
5.2	平台安全服务（按等保三级配置）	500	
二	**工程配套服务费用**	**530.4**	
1	系统集成与培训费	159.12	（工程费用）×3%
2	信息工程监理费	106.08	（工程费用）×2%
3	系统测试与安全测评费	106.08	（工程费用）×2%
4	项目管理与可研设计费	159.12	（工程费用）×3%
三	**项目总投资：**	**5834.4**	**一+二**

13.3.2. 分项投资概算表

13.3.2.1. 消防大数据中心建设概算表

编号	项目名称	功能说明描述（或参数说明描述）	工作量（人月）	金额(万元)
1	**消防数据结构总体设计**		**20**	**16**
2	**数据资源目录体系建设**		**90**	**72**
2.1	业务数据梳理		10	
2.2	资源规划		10	
2.3	资源编目		10	
2.4	资源注册		10	
2.5	资源发布		10	
2.6	资源访问		10	
2.7	资源维护		10	
2.8	资源获取		10	
2.9	目录审核		10	
3	**数据库安全管理**		**20**	**16**
4	**数据资源层建设（数据库设计）**		**100**	**80**
4.1	数据资源层设计	本次项目的数据资源主要由基础数据库、业务数据库、应用数据库、综合数据库和管理数据库组成。省级平台需对全省消防数据类型和结构进行整体调研、分析和数据基础模型设计。	50	
4.2	数据管理层设计	数据管理维护主要包括：数据权限管理、数据更新管理、数据维护和备份、管理工具等。	15	
4.3	数据服务共享层设计	数据共享服务主要是指在系统与其它业务系统对接，提供数据共享服务，基于数据接口的方式提供数据共享服务。	15	
4.4	数据指标体系设计	智慧消防云平台大数据中心获取数据的分类对象定义为：消防专题数据、消防业务数据、省基础数据库数据、省公共信息资源数据、国家知网数据、省内火灾重点行业调查数据、社情民意数据、互联网数据等八部分。	10	
4.5	数据来源设计	智慧消防大数据中心的数据主要包括内部数据及外部数据。	10	

5	**数据资源存储建设**		**35**	28
5.1	存储架构设计		20	
5.2	备份与恢复设计		15	
6	**数据汇聚与融合分析设计**		**60**	48
6.1	多源异构系统数据管理		10	
6.2	多源数据融合与分析		10	
6.3	消防大数据挖掘系统		10	
6.4	智慧消防数据分发系统		10	
6.5	综合运行维护管理系统		10	
6.6	智慧消防融合数据发布共享系统		10	
7	**消防大数据中心管理系统**		**60**	48
7.1	数据支撑平台		15	
7.2	数据采集基础功能		15	
7.3	数据共享交换平台		15	
7.4	共享数据管理系统		15	
合计				**308**

13.3.2.2. 智慧消防应用系统建设概算表

编号	项目名称	功能说明描述（或参数说明描述）	工作量（人月）	金额(万元)
1	**物联网感知网络中心管理系统**		155	124
1.1	感知网分中心模式设计		20	
1.2	物联网感知安全研判设计		20	
1.3	感知网分中心基础管理功能		20	
1.4	感知分中心预分析处理功能		60	
1.5	感知分中心数据共享服务功能		35	
2	**消防物联网远程监控系统**		**420**	336
2.1	**消防基础资源数据采集**		**185**	148
2.1.1	建筑物数据		15	
2.1.2	联网火灾风险单位数据		15	
2.1.3	消防设施及部件数据		15	
2.1.4	消防警力数据		15	
2.1.5	救援力量数据		15	
2.1.6	管理机构数据		15	

2.1.7	水源信息数据		15	
2.1.8	重点部位数据		15	
2.1.9	地理编码数据		15	
2.1.10	基础空间数据		15	
2.1.11	建筑消防平面图编辑功能		35	
2.2	**消防物联网监测数据采集**		**90**	**72**
2.2.1	远程联网监测数据		15	
2.2.2	智能互联式探测器监测数据		15	
2.2.3	水系统液位（压）监测数据		15	
2.2.4	电气火灾监测数据		15	
2.2.5	其他消防监督业务数据		15	
2.2.6	运营服务机构数据接入		15	
2.3	**消防视频监控数据**	**全省 15000 家火灾风险单位包括消控室视频、重点部位视频等监控数据可实时接入调用，但不存储。**	**20**	**16**
2.4	**监测数据分析与处置**		**125**	**100**
2.4.1	火灾报警分析		20	
2.4.2	安全隐患分析		20	
2.4.3	设备故障分析		20	
2.4.4	值班行为分析		20	
2.4.5	事件（任务）生成		15	
2.4.6	事件（任务）下发		15	
2.4.7	事件（任务）处置跟踪与反馈		15	
3	**消防数据基础统计分析报表系统**		**125**	**100**
3.1	查询统计要素管理		20	
3.2	可视化报表自定义		50	
3.3	统计分析报表展示		20	
3.4	报表性能管理		20	
3.5	报表结果存储管理		15	
4	**基于消防大数据火灾智能预警模型分析系统（BI）**		**750**	**600**
4.1	消防大数据 BI 模型目标设计		20	
4.2	火灾风险模型设计		50	

4.3	消防大数据 BI 智能分析模型	消防大数据 BI 智能分析模型，目前主要方向包括：建筑起火频率预测、建筑火灾损失预测、区域火灾防控能力评估、火灾方针模拟、三维区域火灾风险评估、全省消防安全综合评估、城市消防安全评估、区域消防安全综合评估、隐患趋势分析评估、消防水资源健康度评估、电气火灾风险评估、企业消防安全评估、火灾预防策略分析、消防宣传内容及策略分析。这些智能分析模型涉及多领域、多方向、多学科要素以及复杂精细算法，属于综合/复合型的模型分析体系，根据市场行情，可按照预算选择适合平台使用的智能分析模型。	625	
4.4	大数据分析模型构建方法	包括：分析算法模型的微服务移植封装、分析计算所需专题库数据集构建、分析算法模型效用的追踪与持续演进。	55	
5	**消防值班监控中心管理系统**		**140**	**112**
5.1	值班在岗登记		15	
5.2	交接班异常告警		15	
5.3	值班报表管理		15	
5.4	消防证核实与预警		15	
5.5	联网火灾风险单位消控值班查岗		15	
5.6	即时通讯（IM）		50	
5.7	值班监控报警		15	
6	**基于 BIM 的消防应用**	**本次福建省智慧消防系统平台建设，将围绕单个或少量 BIM 模型试点进行展开设计，并结合 GIS 系统和 IOT 物联网，实现 BIM 在福建省智慧消防平台的初步应用展示，为后续大规模 CIM 集群建设的开展，奠定良好设计与技术基础。**	**375**	**300**
6.1	BIM 基础数据库设计及模型设计	建设基于 BIM 消防安全应用系统，首先要对 BIM 中涉及的消防要素数据进行数据模型定义（包括数据名称、数据类型、数据规范、数据格式、数据释义、数据约束等）	150	

6.2	消防设计图纸审查系统	BIM 下的图纸审查系统，可以动态掌握不同颜色区域的参数，可以更加清楚对消防区域进行划分，包括救援路线、疏散路线等等。再者，在整个 BIM 设计审查系统当中，要结合消防设计图纸审查标准，提供各类测量、查询、标注工具，最大程度上减少图纸审查所需时间，保证设计、审查、修改、施工效率。	75	
6.3	建筑防火监督检查系统	在 BIM 防火监督检查系统中，通过 BIM 平台可以快速查找到工程消防相关文件信息，粪便设计参数、使用功能是否发生了变化。此外，通过在建筑结构模型当中科学设置消防管道，在消防管道周边、建筑控矿位置设置传感器，可以实时传递建筑消防安全信息，监督人员可以通过网络平台远程监控消防系统日常运行情况，加强对消防安全管理质量，从而实现最终的消防目标。	75	
6.4	应急疏散逃生指示系统	采用 BIM 应急疏散逃生系统，主要是应用三维图形形式，辅助动态性图表、声光指示灯，可以有效调整逃生路线，并且结合 BIM 结构图形，找出最佳的逃生路线，结合消防广播指导人员逃生，从而保障人员生命安全	75	
7	**消防大数据一张图综合展示系统**	**按照全国消防“一张图”数据标准规范和提供的数据接口，在智慧消防平台上构建展示平台（非重做），也可按照全国消防一张图系统平台的技术特性，实现页面直接嵌入。**	**50**	40
8	**消防教育远程培训服务平台**		**635**	508
8.1	**消防行业从业人员职业化培训管理系统平台**		**100**	80
8.1.1	培训管理端功能	办班管理、开班管理、考试管理、发证管理、异常管理、其它功能（如电子通知公告、职业化培训政策信息发布、相关从业规范信息发布、培训电子课件下载等）	50	

8.1.2	消防维保企业端（PC 端、微信端）	培训报名、成绩查询、证书下载、通知公告、其它功能（培训政策信息查询、电子课件下载）	50	
8.2	**消防救援作战人员培训平台**	**运用虚拟现实技术（VR）实现仿真沉浸式培训。**	**300**	240
8.2.1	指挥员计划指挥和临机指挥训练	消防力量查询、地理信息测量、作战部署标绘、辅助单兵定位。	150	
8.2.2	作战员业务学习	室内熟悉演练、战例复盘、作战指挥推延、三维场景展示。	150	
8.3	**社会化消防培训平台**		**65**	52
8.3.1	消防知识宣传		20	
8.3.2	消防公益培训办班		25	
8.3.3	消防指战员事迹信息宣传培训		20	
8.4	**在线教材资源管理系统**		**60**	48
8.4.1	开放性教育资源采集	针对社会上或互联网上那些不具有版权的公共教育资源，可直接采集获取（标注来源），并进行编目存储。	25	
8.4.2	教育资源导入	针对自创的、外部采购的教育资源，可按照其格式（如文档格式、视频格式、VR 格式、可执行程序格式等）导入或挂载于教材资源库中，提供授权调用。	20	
8.4.3	版权授权到期预警提醒功能	针对外部采购的，具有版权限制、授权期限限制、授权用户数量限制的教材资源，系统根据导入时间、授权时间、授权数量、版权变更情况等，进行定期巡检和预警，避免超期无法使用或侵权	15	
8.5	**社会化线上学习管理系统**		**110**	88
8.5.1	在线学习	选择专题在线看视频、浏览文档资料（提供下载）、学习后掌握度测评等。	20	
8.5.2	在线互动	提供趣味消防小应用，加强社会公众对消防安全意识的培养与理解。	30	
8.5.3	学习专题管理	对学习资料内容（视频、文档等）进行分类，也可根据该段时间的政策形势、会议风向、特殊节日等进行消防学习专题自定义。	20	

8.5.4	题库管理	针对不同学习专题，可设置在线测评试题及对应答案、解析点评等信息。	25	
8.5.5	互动交流	提供非行政管理职能（如投诉、举报）的日常消防知识互动，例如简易的论坛、朋友圈形式发布互动交流主题。	15	
9	**“闽消通”手机 APP**	**类似闽政通 APP，融合消防领域各业务应用系统，为消防监管机构、监管人员、消防从业人员、社会机构、社会公众等提供综合性监管与服务功能。**	**400**	320
9.1	监管功能	1、 消防安全预警通知 2、 消防实战指挥信息查询 3、 消防一张图综合查询与展示 4、 消防监测数据、业务数据基础统计分析展示 5、 消防大数据智能分析研判结果展示 6、 消防服务机构&技术服务人员信息查询	200	
9.2	服务功能	1、 监管信息（双随机、一公开）结果公开公示 2、 消防网上办事大厅（入口）：包括资讯发布、结果公示、办事指南、法律法规、表格下载等。 3、 网上咨询、网上投诉举报、结果反馈 4、 在线宣传、在线教育 5、 服务机构信息查询、技术服务人员信息查询 6、 公共消防设施查询	200	
合计				**2440**

13.3.2.3. 平台基础应用支撑保障体系建设概算表

编号	项目名称	功能说明描述（或参数说明描述）	工作量（人月）	金额(万元)
1	**平台基础应用支撑保障体系建设**		**910**	

1.1	**软件应用基础支撑功能**		**625**	**500**
1.1.1	**统一用户管理服务（SAAS 基础服务）**		**80**	**64**
1.1.1.1	人员管理		10	8
1.1.1.2	机构管理		10	8
1.1.1.3	机构列表与业务关联功能		10	8
1.1.1.4	临时组织机构维护		10	8
1.1.1.5	支持机构的管理		10	8
1.1.1.6	机构人员资料变更		10	8
1.1.1.7	机构人员维护树		10	8
1.1.1.8	与其它业务系统关联	（1）提供给其他所有系统的用户登录认证接口。 （2）提供给其他所有系统的机构人员树选择接口。	10	8
1.1.2	**统一角色权限管理服务（SAAS 基础服务）**		**50**	**40**
1.1.2.1	用户角色分类管理		10	8
1.1.2.2	业务权限控制级别管理		10	8
1.1.2.3	用户角色与权限关系管理		10	8
1.1.2.4	系统及业务权限分配设计		10	8
1.1.2.5	与其他业务系统关联	(1)为其他系统授权提供授权接口。 (2)为其他系统权限判断提供接口。	10	8
1.1.3	**中台应用支撑体系（PAAS 基础服务）**		**360**	**288**
1.1.3.1	业务中台	实现 SAAS 模式下的租户（各级市、县和行业)自定义应用、菜单和鉴权。实现各个租户的不同应用的数据相互独立又相互关联。	80	64
1.1.3.2	技术中台	实现SAAS租户的各个应用的元数据的在线设计，包含了表单、菜单、视图、查询功能、流程节点功能函数、按钮功能函数和权限等。实现 SAAS 应用的数据管理、代码在线编辑、在线调试等功能,以方便实现快速搭建应用系统功能,尽量做到无码开发和快速修改和调整业务流程和代码。	200	160
1.1.3.3	数据中台	省级智慧消防平台的基础数据、复合数据、数据模型、数据视图、数据存储。以及对内部应用系统和外部应用系统提供各种数据服务。	80	64
1.1.4	**权限认证体系**	**权限认证体系，主要包含了用户访问权限、数据存储权限、数据传输权限、**	**25**	**20**

		加解密权限等多个方面的权限安全体系认证。		
1.1.5	**平台安全组件接入**	**平台的安全组件体系，主要包括软件安全组件体系、硬件安全组件体系。其中，软件安全组件体系，除了平台自身的安全保障外，还需要通过安装第三方的安全软件组件来保障系统业务层和数据层的安全。**	25	20
1.1.6	**附件管理**	**平台软件系统运行过程中，除了一些基本的元数据、关系数据或其它数据流外，还涉及到一些物理文件的上传使用，因此对于附件管理，需要提供传输速率高、上传过程稳定、文件保存稳定等一系列功能。**	25	20
1.1.7	**消息管理体系**	**消息管理体系，主要用来建立平台对内、对外的消息传播体系，实现平台运行情况的提醒、平台交互过程的消息提醒，使平台的使用者、维护者能够快速收到系统消息，便于对系统进行运行保障和业务操作。**	25	20
1.1.8	**系统运行参数设置**	**系统运行参数设置，主要包括系统运行过程所需要的一些运行标准值、阈值、范围值、目录路径、地址参数、多字典参数、模板参数等。**	15	12
1.1.9	**多类型信息全文检索服务**	**建立一套完善的数据检索机制是非常重要的。针对存放于多个不同类型数据表、不同数据格式/文件格式的数据而言，要获取一项查询业务的综合全面数据，就必须通过“全文检索”功能来完成。**	20	16
1.2	**区块链应用体系建设**		**95**	**76**
1.2.1	分布式账本“一账通”		20	16
1.2.2	多中心化监管		15	12
1.2.3	多中心化响应		15	12
1.2.4	人工智能、大数据分析		15	12
1.2.5	多场景智能合约		15	12
1.2.6	消防大数据确权交易		15	12
1.3	**接口应用体系建设**		**190**	**152**
1.3.1	用户信息传输装置对接设计		60	48
1.3.2	消防物联网智能监测设备对接设计		40	32

1.3.3	电子地图对接设计		20	16
1.3.4	与省级政务平台对接设计		15	12
1.3.5	福建消防技术服务信息平台对接设计		10	8
1.3.6	与“闽政通”对接设计		15	12
1.3.7	与指挥中心/实战指挥系统对接设计		15	12
1.3.8	与全国消防一张图对接设计		15	12
合计				**728**

13.3.2.4. 平台运维服务概算表

编号	项目名称	功能说明描述（或参数说明描述）	运维保障期限	金额(万元)
1	业务运维服务（总队）	1、提供 3 年，8 人，24*365 全年运维服务。 2、可由省总队应急救援指挥中心提供运维值班座席。 3、费用支出包括人工成本、网络成本、通讯成本、水电成本、设备耗材成本等	3 年	500
2	技术运维服务（平台）	包括平台架构、基础业务系统的日常维护（故障修复、性能保障、性能调优）、功能升级维护(现有系统功能的二次开发)、服务器及网络硬件的日常维护(故障修复、性能调优、日志追踪报告）。随着平台投入使用和持续应用深入,涉及大量应用拓展和业务扩展,必须有强力的技术开发作为平台长期、稳定、高效运行的服务保障。	3 年	300
合计				**800**

13.3.2.5. 云计算平台租赁概算表

编号	项目名称	功能说明描述（或参数说明描述）	服务租赁保障期限	金额(万元)

1	**基础软硬件（云平台服务器主机）**	**按照平台软件应用年限至少 8 至 10 年以上，本次福建省智慧消防云平台租赁电子政务云计算平台的年限，按 8 年计。每年约 66 万元(见 6.10.1. 云主机资源费用测算)**	8 年	528
1.1	物联网感知网络管理中心服务器	数量：1 台。 政务云平台虚拟机，4 核 CPU，24GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		
1.2	消息中心应用服务器	数量：1 台。 政务云平台虚拟机，6 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		
1.3	视频接入应用服务器	数量：1 台。 政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		
1.4	文件存储服务器	数量：1 台。 政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		
1.5	消防综合业务应用服务器	数量：4 台。 政务云平台虚拟机，6 核 CPU，24GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		
1.6	大数据分析及可视化综合展示应用服务器	数量：1 台。 政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		
1.7	数据交换应用服务器	数量：1 台。 政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		
1.8	数据库服务器	数量：8 台。 政务云平台提供数据库实例 D02（ORACLE，数据库空间大小 80G、归档日志空间大小 16G、用户业务空间 40G、索引表空间（index）16G、回滚表空间（undo）4G、临时表空间（temp）4G、Redo 文件 256MB*6） 政务云平台虚拟机，4 核 CPU，16GB 内存，WindowsServer2008R2（64 位）操作系统或 LINUX 操作系统（如已国产化）		

2	**平台安全服务（按等保三级配置）**		**8 年**	**500**
2.1	防火墙	1 套，电子政务云平台提供		
2.2	负载均衡	1 套，电子政务云平台提供		
2.3	入侵防御系统（IPS）	1 套，电子政务云平台提供		
2.4	数据库审计系统	1 套，电子政务云平台提供		
2.5	漏洞扫描系统	1 套，电子政务云平台提供		
2.6	终端侦测与响应系统	1 套，电子政务云平台提供，总队和 9 个支队分析中心安装电子政务云平台，客户端部署在各区域的服务器和终端上		
2.7	数字证书系统	1 套，电子政务云平台提供		
2.8	VPN 设备	94 套，部署在 15000 风险单位和 94 个监管单位之间，用于数据完整性、机密性保护，火灾风险单位可按照总队支持的设备功能要求自行采购。		
合计				**1028**

13.4.资金使用计划

福建省智慧消防云平台项目按照财务管理要求，专款专用、专帐核算，按概算明目核算，项目资金按项目进度投入。

第14章 项目运行维护经费测算

14.1.测算依据

福建省智慧消防云平台项目投资概算只包括项目建设期的资金投入，建成后对系统进行正常运行和维护更新工作所需的资金，建议有关部门在每年安排项目资金时予以考虑。

运行维护费每年建议按项目工程费用的6%~10%取定。

14.2.运行维护经费及来源

福建省智慧消防云平台项目作为数字福建的电子政务项目，信息化财政性资金是系统运行维护费用的唯一来源。本可研报告投资概算只包括项目建设期的资金投入，系统建设完成后，质保期内不需运维资金投入，质保期以后，运维费用将以外包服务费用形式另行计算。质保期以后系统运行和维护更新工作所需的资金，即系统运行维护费建议有关部门统一纳入项目建设单位部门年度预算，逐年拨付。

14.3.平台运维服务

14.3.1. 业务运维服务（总队）

针对福建省消防救援总队，提供全天候值班运维保障。

1、提供3年，8人，24*365全年运维服务。

2、可由省总队应急救援指挥中心提供运维值班座席。

3、费用支出包括人工成本、网络成本、通讯成本、水电成本、设备耗材成本等。

14.3.2. 技术运维服务

技术运维主要针对平台提供日常技术服务。包括平台架构、基础业务系统的日常维护（故障修复、性能调优）、功能升级维护（现有系统功能的二次开发）、服务器及网络硬件的日常维护（故障修复、性能调优、日志追踪报告）。

第15章　风险和效益分析

15.1.项目风险与风险管理

15.1.1. 风险识别与分析

15.1.1.1. 系统风险

1、各项信息技术的迅速发展和信息化应用的日益普及，各种新兴的信息技术频频出现，为项目建设带来更多可供选择的技术方案，但同时由于技术成熟度、兼容性等原因，也会给项目带来一定的技术风险。

2、随着数据的集中的不断深入，为信息安全和系统运行的稳定性带来更大的考验。

3、本项目系统涉及的业务领域较多，为系统的一体化设计和实施带来难度。

15.1.1.2. 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。

15.1.1.3. 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。

15.1.1.4. 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，项目建设完成后，有可能会失去普遍性，无法与新的技术形成无缝链接等等。这些技术的未来发展前景，在某种程度上很难预测，规避风险很难，无论是哪一个政府部门和企业都无法从根本上解决。

15.1.1.5. 资金风险

本项目建设需要一定的资金投入。项目建设的各个环节紧密相关，需要保证资金投入，任何一个环节的资金提供出现短缺、拖延等问题，都会对项目的顺利建设产生影响。因此，资金的及时到位是保证项目顺利完成的重要条件，也是保证项目建设能获得预期收益的重要条件。

15.1.1.6. 政策风险

我国当前正处在向社会主义现代化建设的发展过程中，全面深化改造的各项新政策在不断地制定和调整中，由于信息系统的调整滞后于政策的变化。因此，也就给项目带来了一定的政策风险。

15.1.2. 风险对策与管理

15.1.2.1. 系统风险对策

1、在系统设计的过程中，以保障稳定科学为原则，继续选用成熟可靠的技术，在大数据、虚拟化计算和人工智能等建设方面成熟的技术框架基础上进行发展和提升，保障系统成熟度。

2、注重信息安全和系统安全建设力度，同时加强安全意识、安全制度建设，建立故障预警和应急响应机制，确保系统安全稳定运行。

3、加强业务管理规范和业务流程优化设计，将管理模式转变与信息化建设融合起来，促进系统的一体化设计和建设。

15.1.2.2. 组织风险对策

项目的重要程度、高要求和复杂性，以及建设单位的多样性决定了项目需要有强有力的项目组织保障，本项目尤其要重点加强相关政务部门的组织管理工作。为

了规避或降低项目的组织风险，建设单位从领导层开始对本项目建设给予高度重视，让相关业务部门共同参与决策项目重大问题。建设部门宜建立相应的信息化组织，参与信息化建设的全过程。这支队伍应该由部门高层领导负责，以信息服务专职人员为主，业务部门、商业公司开发和设计人员为辅。

15.1.2.3. 管理风险对策

在项目建设过程中做好项目计划（应将项目沟通计划纳入项目计划中），及时沟通协调项目各方，加强监控和督促，保障项目实施按计划顺利进行。

为了规避项目实施中的管理风险，充分考虑本项目实际情况，如数据资源需求、资源限制、项目总工期限制等因素，参考同类项目实施的经验，制定切合实际的详细的项目基准计划，制定详细的项目实施方案。同时在项目实施过程中，根据基准计划采取有效措施对项目进行“三控三管一协调”，采用监理例会、专题会议、电话、邮件等方式及时沟通协调项目各方，加强项目的质量、进度、投资等要素进行监控。对于项目实施中出现的非预期情况进行分析，尽快采取恰当的措施进行处理，特别对于变更（项目范围变更、需求变更、方案变更、工期变更等等），应建立完善的变更管理和配置管理程序，确保项目始终处在受控状态。

在项目实施前期，要选择确定经验丰富的实施负责人，合理、明确制定项目的工作计划，落实项目管理的人员和职责，建立建设单位负责人、项目实施负责人、各项任务负责人的长效沟通机制，同时加强对实施方的过程监督管理，在项目实施过程中即时发现问题、解决问题，降低项目管理风险。

在项目管理过程中，将风险计划列入项目计划中，及时动态识别项目风险，定期评估已识别的风险清单和风险应对措施，并建立相应的管理储备对应对未识别出的风险。

15.1.2.4. 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，同时应选择具有相关监理经验的项目监理公司，协助建设单位做好项目管理工作。

项目组一定要本着项目的实际要求，坚持技术的先进性和稳定性相结合，选用

合适、成熟的技术，千万不要无视项目的实际情况而选用一些虽然先进但并非项目所必须且自己又不熟悉的技术。如果项目所要求的技术项目成员不具备或掌握不够，则需要重点关注该风险因素。在项目设计中，要加大对新技术的研究力度，同时充分评估和论证各种技术框架的先进性、成熟性和安全性，有效平衡技术选择的先进性和成熟性，确定技术路线，降低技术风险。

15.1.2.5. 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福建省财政厅财政统一划拨。对于承建单位，一方面要控制需求，另一方面要优化开发方式或创新管理，尽量减低人工成本。

15.1.2.6. 政策风险对策

1、主要涵盖已经明确政策的业务领域，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。

2、充分和业务部门沟通，在系统建设中随时跟踪业务部门业务需求的变更，及时的调整业务需求，做到系统建设也业务需求保持一致。

3、各级应用系统及其数据信息逐步迁移和优化升级，逐步实现统一管理模式和统一解决方案。

15.2. 效益分析

1、经济效益。通过省级统筹全省智慧消防云平台建设，可实现信息化财政投资节约投入，完成信息化应用指标的同时减轻市县财政负担，同时深入至消防产品、消防服务、消防教育宣传等各领域，带动福建省消防全产业链生产、流通、消费、信息服务等环节的经济快速发展。

2、社会效益。平台建成投入应用后，将实现全省和市县消防体系协同，用数据事实来分析研判消防事故原因、消防隐患、消防安全事件发展趋势等，用以指导消防安全监管与服务工作的开展，切实保障社会及人民群众生命财产安全，提高人民群众满意度。

3、政治效益。平台建成后，在全省乃至全国范围内，都将成为智慧消防、智慧

城市建设的一项重要标杆，可直观反映我省在城市治理、社会治理方面的突出成绩，彰显我省各级党委、政府优良的执政能力。