目录

第一章 需求分析

一、 政务职能和政务目标分析

1. 政务职能

（一）区分自然性与社会性紧急事件、综合性与专项性紧急事务，形成集中统一的应急管理职能体系

突发事件不外乎自然性紧急事件和社会性紧急事件两大类。自然性紧急事件不仅本身容易直接造成灾难和严重的被动局面，而且还很容易引起社会紧张而转化为社会性紧急事件。因此，仅有专业处置能力而无综合处置能力作保障，就必定会导致十分严重的现实后果。社会性紧急事件对综合处置能力比对专业处置能力有更高的要求；综合处置能力不到位就将衍生出更广泛、严重的现实危机。

一般而言，两类紧急事件在更具体的类型上需要非常专业化的专项治理，从而构成专项性紧急事务；但一旦事态严重，就特别需要加以综合性的有效应对与处置，进而构成综合性紧急事务。而综合性紧急事务及其处置在应急管理体制中具有最突出的位置和作用，构成应急管理职能的主体和核心。专项性紧急事务及其处置在微观过程中具有不可替代的特殊作用，但在总体上却只构成延伸性的应急管理职能。

（二）系统厘清、大力整合现有的政府应急职能，形成一个相对独立、又与常规管理职能紧密对接和互补融合的应急职能体系。

第一，要把应急管理从常规管理中独立出来，明确其性质、定位、范围，把握其规律、特点、原则和要求，弄清其目标、任务、条件、方式和途径，界定出一个成熟完备、独立专门的应急管理职能领域。只有这样，才能把应急管理职能体系界定和设置得更加科学完备和现实有效。另外，要结合行政改革，把政府应急管理的职能职责从政府常规管理的职能职责中具体、细致而系统地离析出来，加以系统的分类梳理和集中整合，形成专门而独立的应急管理职能职责系统。

第二，要把分散的综合性应急服务职能进行适当的规划、调整、组合和集中，把薄弱和欠缺的综合性应急服务职能大力强化起来，形成一套细致全面的综合性应急服务职能体系。

第三，要在现行配置于各职能部门的专门性应急职能系列的基础上，对专门

性应急管理职能和应急服务职能进行提炼、完善和精专，形成一个高度精确有效的专门性应急处置职能体系；同时，还要使之与综合性应急处置职能体系相互匹配、呼应和协调，形成一个完整完备、规范高效的国家应急处置职能体系。概言之，就是要把大量的专项应急管理职能也加以科学梳理和整饬，确保它们与综合应急职能更加契合，确保整个应急管理职能体系变得更加科学高效。

2. 政务目标

根据《应急管理部科技信息化领导小组办公室关于印发地方应急管理信息化2021年建设任务书的通知》（应急科信办〔2021〕1号）要求，2021年是应急管理系统信息化的应用完成年，要贯彻落实习近平总书记在中央政治局十九次集体学习时的重要讲话精神，以信息化提升五大能力，完成应急管理信息化跨越式发展第一步目标。完成信息化基础建设，信息网络运行可靠畅通，通信基础设施基本建成，信息安全防护能力显著提升。

1、提升应急指挥控制能力

应急指挥控制能力是应急管理部门处置突发事件成功与否的重要因素，是应急管理能力建设的根本保证。通过对应急决策、组织指挥、沟通协调等方面的能力建设，进一步提升应急管理部门应急指挥控制能力，打造出具有统一、灵活、快速、高效的应急指挥控制体系是应急管理能力建设的关键。

2、提高应急快速反应能力

突发性、复杂性、紧迫性是突发事件的典型特征，事态发展的瞬息万变，对应急管理部门应急快速反应能力提出了很高的要求。应急管理能力的强弱，是对应急管理部门法规制度落实、行动预案拟制、日常演练和针对性训练情况的综合演练的综合检验，也是提高应急管理部门快速反应能力必须注重把握的问题。通过快速反应、应急投送等方面的能力建设，打牢日常应急管理工作基础，保持良好的应急状态，加强实战化、实案化演练，对提高应急管理部门平时应急、多能一体、灵活高效的应急快速反应能力，确保事件发生时能快速反应，人员装备能迅速投入行动，都有着十分重要的意义。

3、提高应急协调联动能力

应急管理能力建设是一个由诸多因素构成的复杂系统，这些因素相互依存、相互作用、相互影响，在一定条件下还会相互制约，必须坚持统筹兼顾，协调发

展。应急管理部门应急能力建设处于社会发展和应急管理部门建设发展的大环境中，应急管理能力建设必须与社会环境相适应，与人员装备各项建设相协调。提高应急管理能力，就要按照统筹兼顾、协调发展的要求，科学地指导应急管理能力建设，使应急管理能力建设的各项内容以及人员装备各项建设和谐发展，整体提高，使各项应急工作得到落实，促进人员装备的全面、协调、可持续发展。

二、 业务功能分析

1. 应急响应

应急响应包括启动应急预案响应和突发事件综合研判。在应对突发事件时，根据预案启动应急响应，将事态进展和领导批示分发下级单位和相关部门。基于灾情信息对突发事件发展态势进行分析与研判，辅助制定应急处置决策方案。应急响应要求有据可依、有条不紊、科学及时。

2. 指挥救援

指挥救援包含组织指导协调安全生产类、自然灾害类等突发事件应急救援，衔接解放军和武警部队参与应急救援工作，承担应对重大灾害指挥部现场协调保障工作，综合研判突发事件发展态势并提出应对建议，协助省委省政府指定的负责同志组织重大灾害应急处置工作，会同有关方面组织协调紧急转移安置受灾群众。应急救援要求指挥统一有力、救援方案科学合理、便捷高效、安全保障，特别是在极端灾害条件下保持沟通通畅。

3. 值班值守

值班值守业务主要涉及应急指挥中心，包括政务值班和应急值守两方面，主要任务包括建立值班信息报告制度，应急值守排班制度，保证各类型信息报送及时准确等。

应急指挥中心负责应急值守、政务值班等工作，负责机关应急值守工作，负责举报信息的接收、分转等工作，指导各级应急管理部门应急值守工作。负责机关政务值班工作，负责机关相关专网、机要设备管理以及文电接收、转送工作。

值班值守流程主要包括举报等信息的接收、分转，及文电公文信息的接收、转送。

4. 资源调配

资源调配业务主要涉及灾情核查和物资保障处，包含组织协调重要应急物资的调拨和紧急配送，指导救灾捐赠工作，管理、分配省级救灾款物并监督使用。资源调配业务要求科学合理、信息畅通。

5. 协调联动

协调联动业务涉及应急管理厅应急指挥中心、救援协调和预案管理处、火灾防治管理处、自然灾害救援处、灾情核查和物资保障处、地震灾害防御管理处、调查评估和统计处、危险化学品安全监督管理处、工矿商贸行业安全生产监督管理处、安全生产综合协调处等部门。以及厅外相关行业部门。根据突发事件情况协调各部门及各类应急专业队伍，建立应急协调联动机制，协调推进相关平台对接。拟订应急物资需求计划，组织协调重要应急资源的储备。协调联动要求信息通畅、便捷高效。

三、 系统功能和性能需求分析

1. 系统功能需求

1.3.1.1 指挥场所信息化需求

应急指挥场所是应急值守和指挥会商的办公场所，其建设应满足日常应急管理和突发公共事件应急处置的需求。

按照功能划分，应急指挥场所包括应急指挥大厅、多功能厅（新闻发布厅）、总调度室、防火会商室、防汛会商室、安全生产会商室、办公楼 4 楼会议室、办公楼 6、7 楼会议室、办公楼 8 楼会议室、设备间等区域。

各功能区需具备视频会议联动召开、指挥调度信息大屏共享显示、数字音频扩声等系统功能。同时为满足整个系统的统一控制、互通联动、快速使用启动等需求，部署可视化交互控制系统。

1、图像显示系统

新的应急指挥中心新址根据业务职能规划不同功能用房，对视频图像显示有需求的用房包括指挥大厅、多功能厅、会商室、会议室等，满足应急业务的指挥调度、视频监控融合图像显示、会商研判、多媒体展示等需求。

2、数字音频扩声系统

为保证在指挥大厅、会议室等进行应急指挥会议或进行发言、报告等活动时，发言者的声音能够被每一个与会人员清晰的听到，需配置高灵敏度的拾音及扩声系统。

会议室音频设计采用数字会议系统，要求具有较高的整体化和智能化，且系统需采用标准化接口。采用数字会议设备，包括发言设备、控制设备、扩音设备等。

根据大厅或会议室的使用面积和高度，设计扩声系统，参考国家扩声厅级标准一级进行设计，符合声学特性指标中的语言扩声一级标准演讲时应能达到语音清晰、无失真、声压余量充足、声场分布均匀、无声反馈啸叫、声像定位准确。

3、视频会议系统

黑龙江省应急指挥视频会议系统，采用华为 MCU 设备作为核心控制设备，部署在应急指挥中心设备间，各视频会议分会场部署华为视频会议终端设备与高清云台摄像机，实现远程视频会议功能。由于全省视频会议系统以华为设备搭建，本期项目需求属于会场搬迁及部分会场增设，因此仍建议采用华为设备建设，或采用完全兼容产品，以便于设备兼容、管理及维护。

4、无纸化会议系统

传统会议形式越来越不能满足当代会议需求，会议人数众多，会议资料复杂、会议决策低效等问题成为传统会议的通病。无纸化会议将多种智能化通讯技术、音频技术、视频技术、软件技术融入会议的会前会中会后各个环节，通过文件的电子交换为用户提供极为便捷高效的会议平台，同时也带来全新的会议体验。无纸化会议系统远远不止是实现会议无纸化这么简单，它还要满足传统意义上多功能会议室的各种信号自由交互、互联互通的功能。

5、会议预约

为符合现代信息化的考虑，在视频会议室部署一套多媒体信息显示公告系统，用于显示会议室的使用情况和正在召开会议的相关情况。系统功能应包括会议室的预约管理和发布，支持预约、审核机制等功能。

6、可视化分布式交互系统

指挥中心作为负责安全信息采集、监测、分析和预警的统一平台，需要接入

大量不同类型的信号，因此其指挥调度系统平台需具备超强的信号接入及处理能力，以满足业务需要。

1.3.1.2 基础支撑系统需求

基础支撑系统包括新址视频监控系统、新址楼宇门禁系统、会议室预约系统、WIFI 覆盖等。

1、视频监控

数字视频安防监控系统主要是对项目内公共区域进行全方位 24 小时不间断的视频监控；在监控室通过电视墙实时显示整座大楼内外各个监控区域的现场情况。

本项目为一座连体统合性的大楼，分为办公楼与指挥中心两部分，视频安防监控系统主要是在电梯轿厢、入口大厅、各楼层出入口处、楼道走廊、指挥厅、餐厅等处设置摄像机，既考虑到公共位置的安全，又兼顾到重要位置的隐私，摄像机布置要严密、合理。结合环境部署不同安装方式摄像机，进行全面实时监控。

2、楼宇门禁

门禁系统对重要出入口进行权限控制，授权人员才能够进入。通过对不同人脸信息、指纹权限授权，实现不同人员、不同区域、不同时段的权限管控。

3、WIFI 覆盖

通过统一建设全楼覆盖的 WIFI 网络，杜绝私接无线行为发生，避免网络管理混乱和网络安全漏洞，在集中管控、安全可靠的网络环境下，提供办公人员方便快捷的无线上网环境。

1.3.1.3 网络重构及安全加固需求

1、网络重构

根据不同的网络承载不同的业务，且面向不同的业务终端。目前网络拓扑结构，省级汇聚层三张网络共用核心交换机，存在网络边界融合，网络层次不清晰，网络安全边界模糊等问题，需对网络架构进行梳理，按照单张网络垂直网络出口层、汇聚层、接入层进行网络层次划分，使网络层次更清晰规范，同时三网络汇聚层两两互联，中间部署安全设备套件，实现数据的跨网安全交换。

2、网络安全加固

目前网络安全建设，已经具备关键基础设施安全防护的措施和手段，但随着

新业务系统陆续上线，按照《网络安全法》及等级保护 2.0 等相关法律法规及标准要求还有一定的差距，需要通过本期建设，弥补现有完全漏洞。

2. 系统性能要求

（1）网络性能指标

网络链路：链路通道 ES（误码秒数）≤6 个/2 小时，链路通道 SES（严重误码秒数）≤6 个/2 小时，IP 包丢包率≤1%。

路由节点：交换容量≥110Tbps、包转发率≥24000Mpps。

交换节点：交换容量≥100Tbps，包转发率≥40000Mpps。

（2）视频会议性能指标

支持 30%网络丢包时，语音清晰连续，视频清晰流畅，无卡顿;支持 80%的网络丢包时，声音清晰，不影响会议继续进行。

支持 1Mbps 会议带宽下，实现 4K30fps 帧图像格式编解码；支持 512Kbps 会议带宽下，实现 1080P60 帧图像格式编解码；384Kbps 会议带宽下，实现 1080P30 帧图像格式编解码；256Kbps 会议带宽下，实现 720P30 帧图像格式编解码。

（3）音视频系统性能指标

音响系统主要技术指标频率特性：音响设备重放时的频率范围（频率响应）以及信号幅度随频率的变化关系。幅频特性：幅度的单位是 dB，频率的单位是 Hz。音响系统的频率响应至少达到 32-18000Hz，在此频率范围内信号幅度变化应小于 2dB。信噪比：在同一参考点有用信号、与噪音的比值的对数。在音箱输入点信噪比 70dB，人耳距音箱一米噪音几乎不可闻，Hi-Fi 系统一般达到 100dB 以上。

动态范围：音响设备重放时最大不失真输出功率与静态时系统噪音输出功率之比的对数。Hi-Fi 系统一般达到 100dB 以上。 失真度：音响设备重放时，音源信号的失真程度。有谐波失真、交调失真、瞬态失真。Hi-Fi 系统谐波失真一般小于 1%。 立体声分离度：左右两声道的分离度。反映左右两声道的串扰程度。立体声平衡度：左右两声道的信号增益之差。

四、 信息系统装备和应用现状与差距

1. 装备和应用现状

黑龙江省应急管理厅过渡指挥中心位于哈尔滨市南岗区文化街 24 号，建有 1 个指挥大厅和 5 个视频会商室，涵盖大屏显示系统、扩声系统、会议系统、视频会议系统等；3 个网络机房，分别位于文化街机房、文明街机房、王兆街机房，机房内部署交换机、服务器、存储、网络安全等设备。

2. 装备和应用差距

作为省级应急指挥中心，应对各种常规及突发应急事件，需要收集、汇聚、共享、分发各种应急信息，是全省应急信息的枢纽，因此在信息互通、共享、安全方面要求较高。 现有指挥大厅各系统集成通过混插矩阵设备联通，系统扩展能力差，信息共享能力弱，网络安全防护建设不足，已不能满足省级应急指挥中心的要求。

同时，指挥中心新址位于红旗大街 251 号，为新规划用房，需重新部署信息化系统，在系统种类和数量都有新的增长需求，现有系统也已不满足新址的需求。

现有网络层次不清、边界混乱，安全措施简单，不满足网络安全等保 2.0 三级要求，根据 2021 年建设任务书，需要对网络及安全进行重构加固。

第二章 总体建设方案

一、 设计原则

根据应急管理部相关要求，遵照黑龙江省应急管理厅相关设计及要求，在现有信息化基础设施和资源的基础上，坚持目标导向和问题导向，按照总体设计、分步实施、急用先行、保证质量的原则，高起点、高标准开展规划建设，确保适用实用、整体推进。进一步加强应急管理信息化建设与应用，提升信息共享、监测预警和指挥救援、分析研判等能力。本次信息化规划遵循以下几个原则：

一、统筹规划，统一建设

采用系统工程理念，统筹制定本期项目总体工作计划，利用新理念、新技术、新设备，立足应急管理现状，合理规划设计，本着统筹规划、统一建设原则，开展应急指挥中心场所建设、基础支撑系统、网络搬迁及网络安全加固等工作，满足应急管理厅工作需要。

二、先进实用、适度超前

以落实“安全第一、预防为主、综合治理”方针，建立有效的预防事故发生的信息技术支撑体系为出发点和落脚点，借鉴国内外先进经验，采用先进的成熟的技术和设备，确保本期项目建成后 3-5 年不落后；又要敢于探索，发挥新技术在应急管理方式方法、提高科学施救水平方面的作用。

三、资源整合、充分利旧

统筹现有过渡应急厅系统设备，兼顾新建工程与既有成果，整合优势力量和资源，原则上尽可能的复用利旧，避免系统的多次设计、互不兼容、盲目投资和重复建设，从根本上提高应急信息化建设的效率、效果和效益，降低建设和应用的复杂度。

四、技术保障、安全可靠

在信息系统的建设过程中，必须加强信息安全保护，严格按照国家规定，采用符合当前发展趋势的先进技术，开展信息安全等级保护测评、安全检查、风险评估和涉密信息管理等工作，强化系统设备的可靠性和先进性。同时结合实际情况，应积极采取多种手段，加强系统运维管理，确保系统的正常运转、运行维护

与升级完善。

二、 总体目标

遵循国家应急管理部下发的应急管理信息化规划、地方建设任务书，及原国家安全生产监督管理总局（现应急管理部）下发的安全监管监察执法装备配备标准、安全监管职业能力建设标准要求，依托转隶部门、外联部门已有信息化建设成果，结合黑龙江省应急管理厅信息化要求，参考省级应急管理特点，坚持一切从实际出发，以全面提升综合防灾减灾救灾能力为总目标，以防范安全生产、自然灾害类突发事件为重点，以公共安全科技为支撑，充分整合优化现有资源，夯实信息化建设基础，补齐业务技术短板，全面提高应急管理能力和科学施救水平，满足服务黑龙江省应急管理厅指挥作战需要，为形成“统一指挥、专常兼备、反应灵敏、上下联动、平战结合”的中国特色应急管理体制提供技术保障和基础支撑。

三、 总体建设任务

黑龙江省应急管理厅新址为主楼与副楼连体建筑，主楼作为办公主楼，满足应急管理厅日常办公需求；副楼作为指挥调度中心，满足应急管理厅日常监测及事件调度指挥职责。

本期项目建设方案涉及指挥中心信息化系统、应急指挥基础支撑系统、新址大楼楼宇智能化系统、网络接入、网络安全加固等几方面。

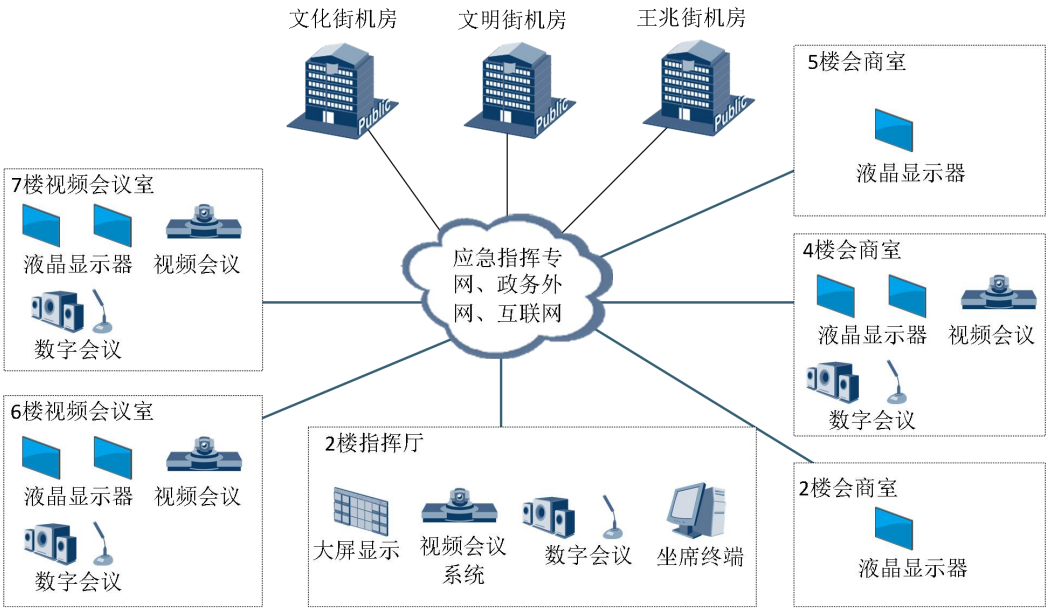
指挥中心信息化系统旨在满足应急指挥中心数据监测、指挥调度、会商研判等职能，在指挥大厅、多功能厅、会商研判室新建显示系统、数字会议、视频会议、无纸化会议等系统。新建系统将采用分布式布局，在系统先进性、扩展性、可靠性等方面满足应急业务的发展需求。

基础支撑系统包括视频监控、WIFI、楼宇门禁等几部分。视频监控系统将对新址布局无死角覆盖、WIFI 实现全楼宇覆盖、门禁系统实现楼宇分区分人分时段出入管控，加强新址的安防保卫工作。

网络接入部分对原接入的指挥信息网、政务外网、互联网三张网络进行整改，由原融合接入整改为分体系隔离，使网络边界更清晰，业务数据边界与流向更清晰。

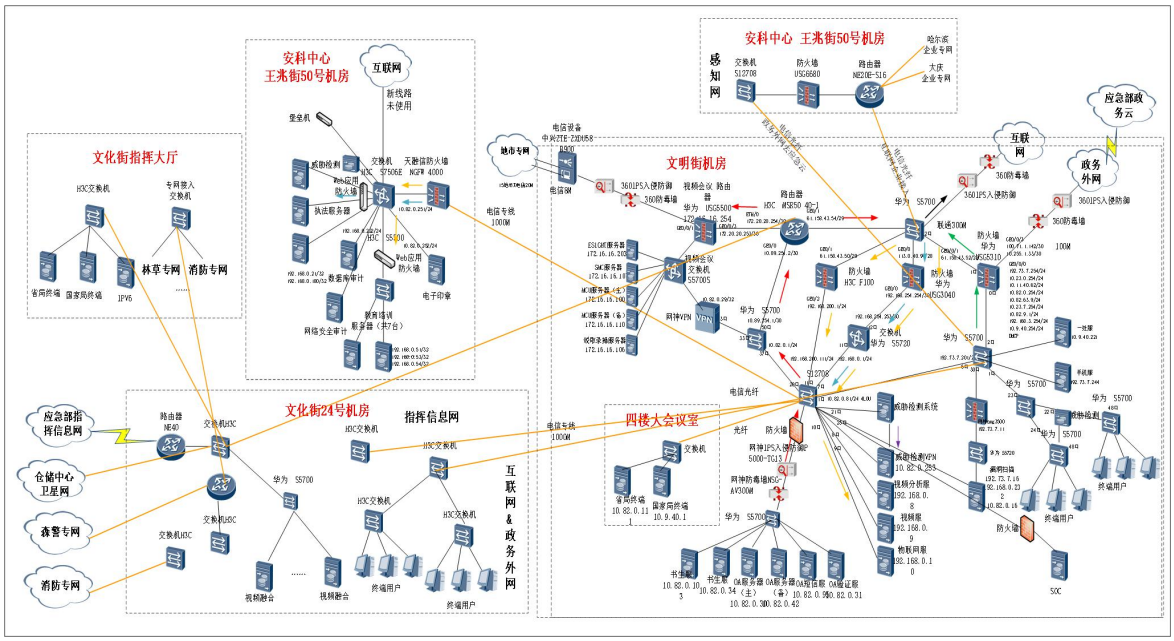
网络安全部分对整改后的网络进行网络安全加固，满足等保 2.0 三级的安全技术要求。

四、 系统现状

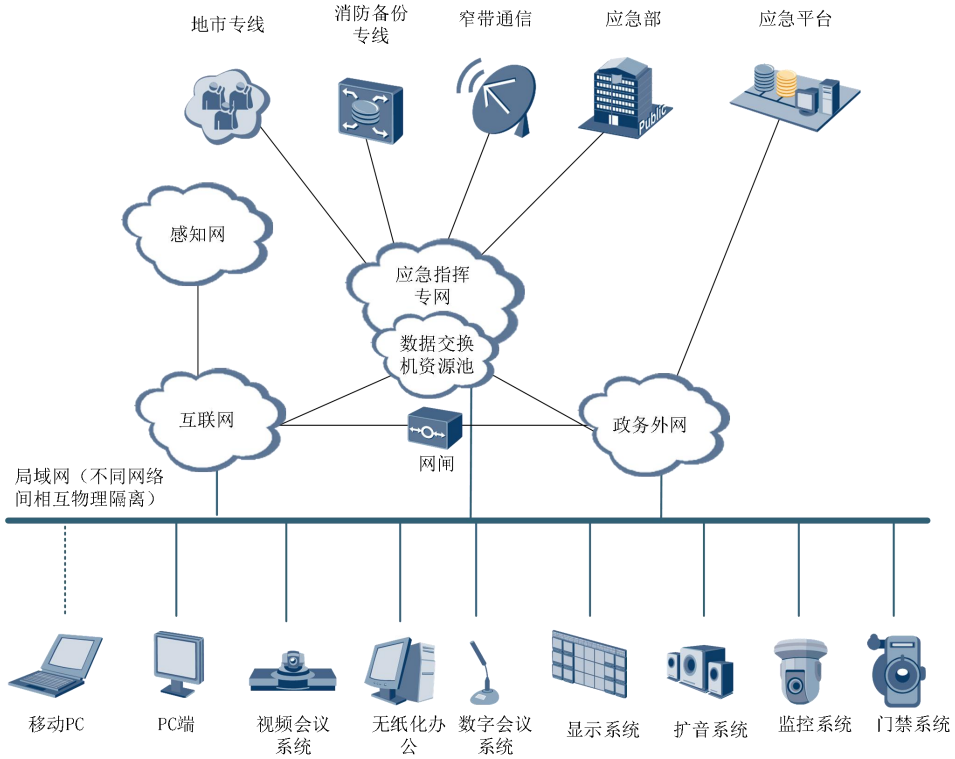


黑龙江省应急管理厅过渡指挥中心位于文化街 26 号，设置 2 楼指挥大厅，2 楼、5 楼设有会商室，4 楼、6 楼、7 楼设有视频会议室。现有指挥中心部署了大屏显示系统、视频会议系统、数字会议系统、终端坐席等设备。

网络传输、视频融合、业务平台、网络安全等设备分布在文化街机房、文明街机房、王兆街机房。文化街机房位于文化街 26 号 3 楼，文明街机房位于文明街 11 号 2 楼，王兆街机房位于王兆街 50 号 2 楼。现有网络结构如下：



五、 总体方案

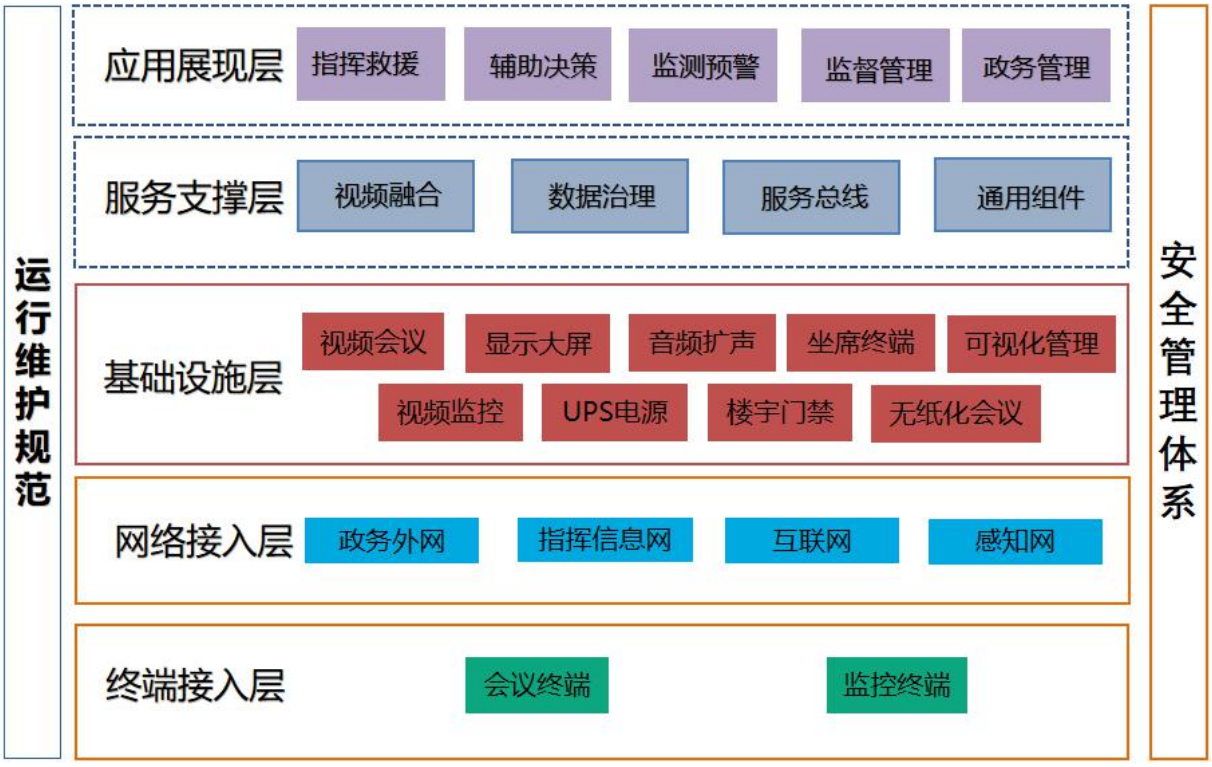


网络及安全部分：应急管理厅将对现有网络进行有效整合。规划后的网络主要由互联网、政务外网和指挥信息网三张网络组成，各网络自成体系，依照出口路由层，核心交换层、接入层，进行分层建设。网络域、安全域、数据业务域，

设备域边界清晰。每张网按照《网络安全法》和等保 2.0 的相关要求进行信息安全防护体系建设。按照等保 2.0 的标准要求，规划后的网络将三张网之间进行网络边界的强隔离，实现三网之间数据和视频传输的安全隔离与安全交互要求。建立统一安全管理中心区，通过三张网边界隔离设备，对三张网进行统一的网络运维和安全运维，并分屏进行可视化呈现，实现可视化运维要求。

信息化及基础支撑部分：各系统通过以太协议接入新址局域网，由分布式控制节点纳入可视化分布式交互控制系统。通过统一的控制，实现图像、音频共享，会议的召开等日常办公需求。视频监控、门禁等系统也通过局域网上联至中心设备。

本期建设后的系统与现有的平台系统、远程终端等部分组成为一个统一的应急指挥信息化体系，形成如下的整体架构：



六、 利旧设备汇总

本期项目建设统筹现有过渡应急厅系统设备，兼顾新建工程与既有成果，整合优势力量和资源，原则上尽可能的复用利旧，避免系统的多次设计、互不兼容、盲目投资和重复建设，从根本上提高应急信息化建设的效率、效果和效益，降低建设和应用的复杂度。

现有可利旧设备汇总如下：

- 现有过渡指挥大厅 LED 拼接显示屏，19.2 ㎡；
- 75 寸液晶显示器，原 4 楼、5 楼、6 楼、7 楼共计 8 台（利旧到餐厅及监控室）；
- 原值班室等场所电视 7 台（利旧到新址值班室等需求场所）；
- 数字音频系统：原 2 楼、7 楼各一套；
- 视频会议系统：原 4 楼、6 楼、7 楼、过渡指挥大厅以及库存共计 6 个视频会议终端和 6 个视频会议摄像机；
- 现有过度指挥大厅可利旧计算机终端 21 台。

除以上可利旧设备外，其余各信息化系统建设需求均为新建。

七、 技术特点及先进性

黑龙江省应急管理厅应急指挥中心信息化建设项目，在信息化系统建设上设计采用了技术先进的可视化分布式系统、数字会议系统、无纸化办公系统等。

1、可视化分布式系统

应急指挥中心音视频系统设备，管理复杂，当决策者下达指令时，往往需要多人操作，如音频、视频、业务系统组合，需要多人切换操作，可视化管理平台的出现解决了这个问题，把各个音视频等子系统的操作归属在一个平台上，利用触摸技术和人机软件界面，把大屏幕显示系统、音响扩声系统、视频会商系统、环境灯光系统集成在一个平台上操作，运用矢量可视化的界面可完成直观可视音视频资源调度，环境资源集中化控制等，解决了要素繁多，信号繁多，设备参数复杂与抽象，专业操控人力资源稀缺等问题。做到全方位无缝人机协作，全力打造节约、友好、可视化的调度管理系统为调度指挥中心的决策者提供了快速、准确、高效、实时的分析决策系统支持，极大的提高了工作效率。

可视化管理平台是融合虚拟现实技术，面向智能控制设计应用，以流程化的方式，快速、方便、准确地实时智能管理调度指挥中心，集合了可视化技术、多点触摸技术、智能控制技术、智能检测技术的立体全智能化闭环控制平台。

应急指挥中心是综合展示、指挥调度及处理应急突发事件的重要场所，调度指挥中心的信号来源于各个业务系统服务器、工作站、大数据分析展示系统、应急

厅的视频/数据以及现场的信息接口插座等，由于输入信号的种类和分辨率各不一样,输出显示设备的分辨率也不一样,同时信号也需要传送到各个显示区域(中心指挥大屏、背面展示大屏、房间外侧引导大屏、交互显示屏等)，传输距离远，显示区域多，显示类型也不一样，传输和管理是个大问题。

根据项目的特点,本项目采用一套分布式交互管理系统可统一完成信号源接入、传输、交换、显示、控制、融合等功能，通过可视化管理平台的统一整理和调用，保证信号的互联互通，满足现场调度的信号分配显示在各个区域、各类屏幕上任意分布和调度的目的。

分布式交互管理系统采用模块化、分布式的组成方式;系统由全高清音视 频输入节点，全高清音视频输出节点、平台服务器以及网络交换机组成。所有设备均通过 CAT6 网线连接至网络交换机。工作人员使用任意一台触摸终端即可：实现对 AV 系统的控制，包括大屏显示图像的切换、强弱电设备控制、系统状态 等信息都能及时反馈到控制界面上，使以往复杂的操控变得简单和直观。

2、数字会议系统

系统包括发言系统、扩声系统和数字音频信号处理系统，负责现场的发言、扩声、视讯音频的输入输出以及对啸叫、音量、视频会商回声和信号路由的各类处理，用数字化方式完成，并与可视化分布式管理平台通讯，由管理人员迅速操控。发言扩声处理系统应实现以下功能：应急指挥中心的内部讨论、汇报、接待讲解；多媒体资料的音频现场扩声播放；与视频会商系统结合，实现与各个分会场进行视频会商时的语音输入和输出；

（1）发言系统

根据调度指挥中心的桌椅布局以及实际使用情况分析,通过会讨主机将麦克风信号接入数字音频处理系统，输出至本地扩声系统和远程视讯会商系统，根据场景模式进行任意摆放和使用。

功能特点如下：

可根据现场建声环境的好坏，灵活调整发言话筒的数量，有效果的避免啸叫产生；

由于数字话筒连接方式为手拉手形式，并且采用网线传输，一根线缆通常可带 30 只以上话筒，所以其它布线简单，且容易扩展；

数字话筒在功能上可选配会议签到、表决等功能，应用上更加完善；

同时，数字会议系统可独立实现语音摄像自动跟踪功能：即某位领导打开话筒发言时，摄像机自动跟踪、拍摄图像。

（2）扩声系统

1）应急指挥中心扩声要求：

有足够的声压级、良好的语言清晰度；同时又能满足声音方向感、空间感、生动感的需要；具有声场均匀、空间方向感强、听众的听觉与视觉一致、直达声强，清晰度好、语言的可懂度高等特点；满足扩声系统声学特性指标GB50371-2006《厅堂扩声系统设计规范》中规定的会议类扩声一级指标为标准。

2）扬声器的布局原则：

扬声器的位置应符合现场的实际安装位置条件，并在建筑上是合理的；扬声器尽量采用隐藏的安装方式，不影响美观；扬声器的重量应符合吊挂点承载的要求；扬声器的布置应避免声反馈和产生回声干扰，以提高传声增益；扬声器的布置保证利用扬声器的指向特性来覆盖观众区，所有听众接收到均匀的声能；来自扬声器的直达声和自然声源的声音方向大致相同、声像一致、空间感好；扬声器均匀覆盖观众区，无辐射死角。

3）扩声形式

对于应急指挥中心的扩声，会场内以人声为主，人声追求的是甜美、饱满，中频突出；因此本次采用主扩全频音箱+辅助环绕音箱的扩声方式，2 只高品质线阵列全频音柱分布在会场前端 LED 大屏左右两侧，2 只高品质线阵列全频音柱分布在指挥后场，满足全场声压覆盖，提高全场的声压级的均匀度。

（3）数字化音频处理

所有信号通过音频处理器内置的 DSP 芯片对音频信号进行路由、分配、均衡、压限、降噪、回声消除、分频等逻辑器件的处理送至重放设备。数字化处理系统应用了 ALC 和 AGC 技术、AEC 回声消除技术、反馈抑制、集成路由分配、音频降噪等技术，抑制了音频系统啸叫，消除了视频会议中的回声，同时降低了系统的噪声，满足调度指挥中心语言扩声清晰度的需求。功能特性如下：

1）ALC 和 AGC 技术

与会者在正常发言过程中容易出现动作幅度的变动，致使发言距离的频繁变

动，导致声音的忽大忽小，而发言者通常为了保持声音的恒定不变，需要长时间保持姿势对准话筒进行发言，极大的影响发言者的发言舒适度和现场发言听音效果；数字音频处理器具备话筒输入通道的 ALC 与 AGC 语音平衡技术功能，提供手动或自动的音频增益补偿，在发言者声音变小时自动于音频电频增加 2-4dB,在发言者声音变大时自动于音频电频减少 2-4dB,实现现场声音始终保持在恒定大小位置，这样高效的系统传声增益功能彻底解决与会者发言过程中的语音不平衡问题，提供舒适的发言功能。

2）AEC 回声消除技术

在召开远程会议时，本地音频与远端相互叠加后重复传输，导致产生回声问题，同时本地大量的音频信号的调度、各种音频传输设备都易产生回声干扰问题，降低语言清晰度。通过 AEC（Acoustic Echo Chancellor）的处理技术，可以对每路输入信号进行独立处理。AEC 对扬声器信号与由它产生的多路径回声的相关性为基础，建立远端信号的语音模型，利用它对回声进行估计，并不断地修改滤波器的系数，使得估计值更加逼近真实的回声。然后将回声估计值从输入信号中减去，从而达到消除回声的目的，AEC 还将音频的输入信号与扬声器过去的值相比较，从而消除延长延迟的多次反射的声学回声。AEC 参考定义了精密的数字模型中统计的重复传输的音频信号，提取相应的频谱（频率和振幅），真正做到精确的回声消除，而不是简单的回声抑制。从而达到非常优秀的回声消除的效果。

3）反馈抑制 AFC

音频发言过程中，由于发言拾音设备和扩声设备较多，与会者的声音经常容易经过扬声器输出后重复拾音，通过反复不断的拾音和扩声，初始音频信号被不断放大而最终产生啸叫，直接影响现场的语音发言效果；数字音频处理器的反馈控制技术，能够精准的捕捉现场多个静态和动态啸叫点，在不影响原声传输的情况下，解决音频产生的啸叫问题。

4）集成路由分配

通过数字音频处理器取代传统的音频周边设备，避免过多的设备连线，系统结构简单，功能强大，提供灵活直观的信号切换处理界面，区别于传统处理设备的信号切换的系统，数字音频处理器的路由切换界面显得更加直观和简便，对于各种输入信号均可以根据需求快速选择对应的输出通道，整个过程简 便快捷，

大大提高会议使用效率。

5）自动音频降噪 ANC

常规音频处理系统中的各种音频设备，包括发言设备、各种音频信号、处理设备等均容易产生噪声干扰，各级的噪声经过累积放大，最终形成对现场音频信号的干扰，数字音频处理器具备的噪声抑制处理模块，从各个阶段设备源头进 行噪声抑制处理，降低噪声的重复产生，同时系统具备的"原音保护"技术，真正将发言者的原声无损的传输到扩声扬声器上，为现场音频发言扩声提供清晰的处理效果。

6）可视化控制

本项目音频系统建设采用分布式网络架构，设备通过网线连接，可任意扩展，满足一根网线联通所有设备和视听场所，实现信息共享、互连互通。分布式音视频系统的优势是以其无限带宽、分散架构、网络化、模块化、高稳定性、高扩展性等特点。

通过可视化分布式控制平台，可以"所见即所得"的在控制界面上"看到"数字音频处理器的通道路由、场景调用以及每个输入/输出通道当前声音的动态电平值。为现场操作提供精准的参考依据。

3、无纸化办公系统

无纸化会议系统根据应急指挥中心使用角度出发，充分了解指挥中心使用需求，根据需求量身定制出一套无纸化会议系统，该系统搭建通用的会议管理模板工具，帮助会议主办方更加电子化、智能化地管理各项会议工作，从而大大减少人工的参与。本系统具有以下特点

纯网络：

无纸化会议系统的设计目标是通过网络，完成单位团体内部会议通知发布、参会人员入场指引、会议室文件的分配与共享，实现无纸化会议，与会人员使用触摸屏或鼠标即可在桌面环境下快捷地审阅查看会议文件，远端加入会议讨论。该系统蕴含的环保、高智能化的理念是系统的价值所在。

多功能：

无纸化会议系统包含了桌牌显示、会议签到、会议投票、会议交流、会议议程查看、会议材料查看、文件批注、投影、同屏分享、电脑操作等会议常用功能

和无纸化交互功能。

可定制：

无纸化会议系统针对不同用户的不同需求，系统可根据用户的实际要求作功能上的相应增减、定制或调整，满足用户的实际使用需求。

可扩展：

为适应无纸化软件系统技术和设备的不断更新与发展，系统具有良好的灵活性和可扩展性，能够根据不同使用需要，兼容不断更新的设备及技术功能，方便扩展。

易操作：

本系统终端界面简洁明了，各个功能一键到位，人性化、可操作性强，能够满足不同层级人员的使用习惯，满足对电子类产品不同使用熟练程度的用户使用需求。

易管理：

采用一台后台管理控制服务器，通过网络对多个终端实现集中有效的管理，操作简单，使用方便。改变了过去电子化会议室中线路布放复杂、硬件设备繁多、系统运行故障率高的弊病。

经济环保：

本系统只需要在一台服务器、多个会议终端上安装无纸化软件，通过有线或无线网络连接，即可实现终端无纸化会议主要功能的操作，后期维护成本低。实现系统的更多环保理念。

安全保密：

所有与会议有关的文件统一保存在服务器，集中管理，终端不保存任何文件。管理人员通过密码进入管理端，实现文件的分发和管理等操作，确保会议的保密性、安全性。

快速组织会议

管理端开启会议后，坐席端自动进入会议

文件分享

在会议开始之前和会议进行中用户都可以随时上传会议所需的资料。

同屏分享

在会议开始时用户可以随时分享自己的桌面，使得和其他与会人的讨论更加高效。

自定义投票

在会议进行时秘书或者主持人可以随时创建一个投票以支持决策。

会议消息

会议期间用户可以随时互发消息进行沟通。

会议功能全面

强大的数据处理能力和文档共享能力，可以协同讨论文件内容并实时圈点批注，批注后的文档可自动上传至服务器保存。

高保密性管理

无纸化智能会议系统，会议通信采取 MD5&DES 加密措施，有效保障会议内容的安全性，从根本上杜绝传统会议方式下的带来安全泄密等各种隐患。

易学易用性

参会者可以在系统中对文件进行亲笔圈阅、批注，从而使不同用户可对所传阅讨论的文件发表各自的意见、相互交流并进行最终的定稿及签署，用户对文件进行的亲笔圈注、签名信息均可被保存，操作简单，界面友好，从而大大减少了培训工作量。

绿色环保低碳、提高工作效率

无纸化智能会议系统被认为是绿色办公的最佳实践者，一方面因其将日常办公资料全部电子化，变成可永久存储、随时调用、无需纸质媒介的数字化形式；另一方面其全程无纸化、低碳办公，符合环保大趋势。通过使用无纸化智能会议系统，避免了政府部门会议过程中文件的大量打印，避免了人力及时间的过多消耗，由此提高了工作效率，加快中央政府部门决策部署的传达、贯彻、落实。

第三章 项目方案

一、 建设目标、规模与内容

1. 建设目标

根据《应急管理部科技信息化领导小组办公室关于印发地方应急管理信息化2021年建设任务书的通知》（应急科信办〔2021〕1号）要求，2021年是应急管理系统信息化的应用完成年，要贯彻落实习近平总书记在中央政治局十九次集体学习时的重要讲话精神，以信息化提升五大能力，完成应急管理信息化跨越式发展第一步目标。完成信息化基础建设，信息网络运行可靠畅通，通信基础设施基本建成，信息安全防护能力显著提升。

1、提升应急指挥控制能力

应急指挥控制能力是应急管理部门处置突发事件成功与否的重要因素，是应急管理能力建设的根本保证。通过对应急决策、组织指挥、沟通协调等方面的能力建设，进一步提升应急管理部门应急指挥控制能力，打造出具有统一、灵活、快速、高效的应急指挥控制体系是应急管理能力建设的关键。

2、提高应急快速反应能力

突发性、复杂性、紧迫性是突发事件的典型特征，事态发展的瞬息万变，对应急管理部门应急快速反应能力提出了很高的要求。应急管理能力的强弱，是对应急管理部门法规制度落实、行动预案拟制、日常演练和针对性训练情况的综合演练的综合检验，也是提高应急管理部门快速反应能力必须注重把握的问题。通过快速反应、应急投送等方面的能力建设，打牢日常应急管理工作基础，保持良好的应急状态，加强实战化、实案化演练，对提高应急管理部门平时应急、多能一体、灵活高效的应急快速反应能力，确保事件发生时能快速反应，人员装备能迅速投入行动，都有着十分重要的意义。

3、提高应急协调联动能力

应急管理能力建设是一个由诸多因素构成的复杂系统，这些因素相互依存、相互作用、相互影响，在一定条件下还会相互制约，必须坚持统筹兼顾，协调发展。应急管理部门应急能力建设处于社会发展和应急管理部门建设发展的大环境

中，应急管理能力建设必须与社会环境相适应，与人员装备各项建设相协调。提高应急管理能力，就要按照统筹兼顾、协调发展的要求，科学地指导应急管理能力建设，使应急管理能力建设的各项内容以及人员装备各项建设和谐发展，整体提高，使各项应急工作得到落实，促进人员装备的全面、协调、可持续发展。

通过本项目的建设，完善应急指挥中心信息化装备，提高信息化应用水平，一个高效集约的信息化应用系统能全面提高政府保障公共安全和处置突发公共事件的能力，最大程度地预防和减少突发公共事件及其造成的损害，保障公众的生命财产安全，维护国家安全和社会稳定，促进经济社会全面、协调、可持续发展。

2. 建设规模

本期项目为黑龙江省应急管理厅新址信息化建设，涵盖网络重构、网络安全、信息化系统、基础支撑系统。

应急指挥中心新址占地面积 4732.17 ㎡，总建筑面积 5525.39 ㎡，包含两栋建筑，分别规划为业务技术楼和办公楼。其中指挥大厅、总调度室、各会商室等功能场所位于业务技术楼，由于业务技术楼场所空间有限，不能满足极端自然灾害和多发安全生产事故救援情况下应急指挥调度场所需求，因此，为办公楼相关场所建设配套信息化系统作为指挥中心的功能扩展。

网络重构及网络安全部分涉及将文化街机房、文明街机房、王兆街机房三处机房设备搬迁至应急指挥中心新址设备间，搬迁设备涉及路由交换设备、网络数据安全设备、服务器设备、存储设备等。

新址信息化系统涉及办公楼 1-8 楼及业务技术楼 1-4 楼的各类大屏显示、音频会议、视频会议、会议管理、无纸化会议、可视化分布式交互系统。

基础支撑系统涉及办公楼 1-8 楼及业务技术楼 1-4 楼的视频监控、楼宇门禁、WIFI 覆盖、全楼广播，基础配套。

3. 建设内容

遵循《应急管理部科技信息化领导小组办公室关于印发地方应急管理信息化 2021 年建设任务书的通知》（应急科信办〔2021〕1 号）、《应急管理部视频会议值班管理制度和视频会议室建设规范（试行）的通知》(应急厅 2019 29 号)等文件中对省级应急指挥中心信息化的总体定位和建设要求，立足黑龙江省应急管

理工作的实际需要，建设满足应急指挥实战需要的指挥场所信息化体系，具体包括内容如下：

网络搬迁重构：对应急指挥信息网、政务外网、互联网设备搬迁，梳理网络边界，重构网络拓扑结构。

网络安全：对网络安全边界、网络安全策略梳理，补缺安全短板，加固网络安全边界。

新址信息化系统：大屏显示、音频会议、视频会议、会议预约、无纸化会议、可视化分布式交互系统。

基础支撑系统：视频监控、楼宇门禁、WIFI 覆盖、全楼广播，基础配套。

二、 标准规范建设内容

总体标准是建设所需的总体性的标准与规范，结合项目建设需求，制定建设总体规范。从工程建设角度看，总体标准的建设内容是根据项目建设总体方案，从框架性思路出发，制定项目所涉及的基本术语、标准化指南、标准编写规则等方面的标准，以保证信息系统的建设工程高效、健康和稳定发展，减少重复投资和互不兼容。此外，总体技术标准中，还应确定项目整体框架，包括信息化相关系统内部结构和与外部系统间的联系，对接系统和新建系统与该平台联系等。

1. 业界开放标准及协议

该类标准通常涉及应用系统的基本构架、软硬件要求、基本功能要求、基本数据要求、基本的业务流程要求等。本项目应用系统标准重点建设各子系统的整合集成、协同工作，数据的访问、设备接口规范等，规定各子系统功能实现、交换接口等多方面要求。规定各项对接系统的容错性、可维护性、可移植性、易安装性、安全性、易用性等。为不同系统间数据共享信息交互、系统对外接口、系统一致性等要求提供指导。

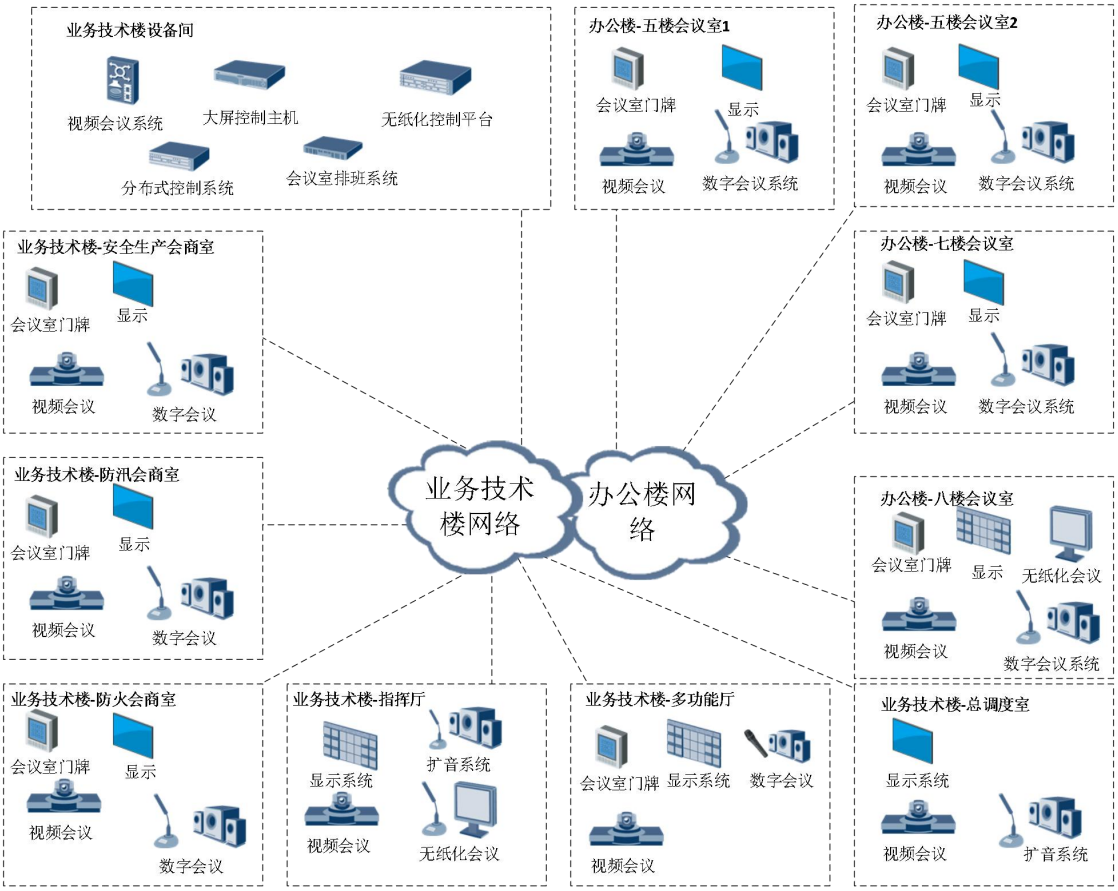
为了避免网络系统、应用系统和数据资源遭受来自系统内外各类主动或被动式的攻击，保障各级系统稳定、有效地运行，本工程将建立完善的安全保障体系。信息安全标准为配套工程建设要求，配套终端安全接入规范，对终端设备安全、应用系统、数据安全、安全管理等方面进行规范。

2. 项目建设行业标准

项目建设依据行业标准参照 1.4.2 技术规范中规定各类规范标准。

三、 信息化系统建设

1. 信息化系统总体方案



根据应急管理厅新址用房规划，业务技术楼设有指挥大厅、多功能厅、会商室、总调度室等，需建设图像显示、视频会议、无纸化会议、数字会议、会议预约等系统；办公楼 4 楼、6 楼、7 楼、8 楼设有会议室，作为指挥中心扩展功能用房，需建设图像显示、视频会议、数字音频会议、会议室预约等系统。同时视频监控和 WIFI 覆盖全楼。

根据房间功能规划：

指挥大厅新建大屏显示、视频会议、数字音频会议、无纸化会议、会议预约等系统；

多功能厅利旧大屏显示、新建视频会议、数字音频会议、会议预约等系统；

总调度室新建图像显示、视频会议、数字音频会议系统；

业务技术楼各会商室新建图像显示、视频会议、数字音频会议、会议室预约等系统；

办公楼 4 楼、6 楼、7 楼、8 楼会议室新建图像显示、视频会议、数字音频会议、会议室预约等系统，其中 8 楼需新建无纸化会议系统。

2. 图像显示系统

3.3.2.1 需求分析

新的应急指挥中心新址根据业务职能规划不同功能用房，对视频图像显示有需求的用房包括指挥大厅、多功能厅、会商室、会议室等，满足应急业务的指挥调度、视频监控融合图像显示、会商研判、多媒体展示等需求。

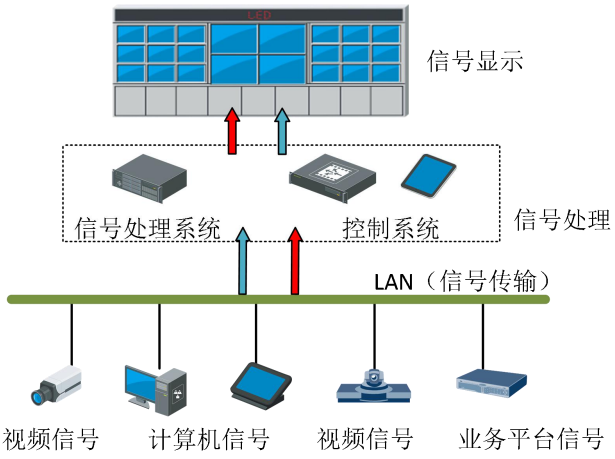
3.3.2.2 建设方案

1、新建 LED 大屏

LED 高清面板电视属国际最领先的 LED 高清晰数码显示技术，融合了高密度 LED 集成技术、多屏幕拼接技术、多屏图像处理技术、网络技术等，整套系统具有高稳定性、高亮度、高分辨率、高清晰度、高智能化控制、操作方法先进的大屏幕显示系统。整套系统的硬件、软件设计上已充分考虑到系统的安全性、可靠性、可维护性和可扩展性，存储和处理能力满足远期扩展的要求。大屏幕由一块块单元板平铺而成，每个单元板上规则布满 LED 颗粒，这些颗粒能够显示发光，是显示图像的基本像素点，一副图像的清晰度就取决于这样的像素点数的多寡，通常用每平米所拥有的像素点数表示。本项目采用≤1.25MM 间距屏幕，每平米像素密度为 640000 点，足以显示高清画质视频，效果更出众。

同时 LED 高清面板电视又区别于市场上一般的 LED 显示屏，具有高密度发光点，黑表面 LED 具有的高对比度，视频处理更高级、呈现效果更多样等特点。

在进行大屏显示系统的设计时，应考虑大厅的现场墙面两柱体间宽度和领导指挥席的位置，合理设计大屏尺寸，使视觉效果达到最好。由于应急指挥工作涉及多部门联动，指挥中心新址指挥大厅、会议室、会商室显示系统可显示同源图像，也可显示自有独立图像。

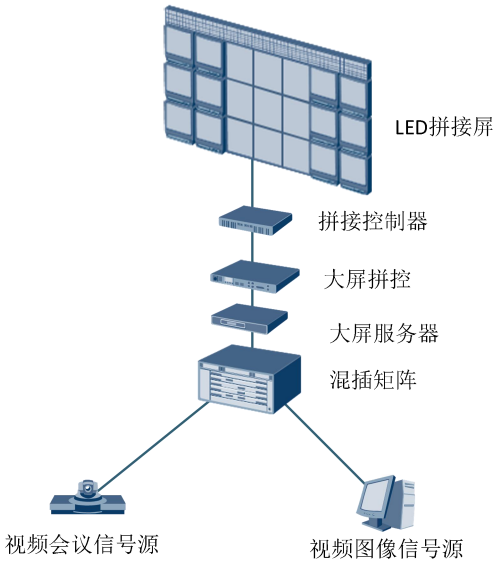


指挥大厅设计采用一块长约为 15.6 米，高约为 3.0375 米，面积为 47.385 平方米的室内 P1.25 小间距全彩曲面显示屏作为主显示屏。主屏两侧设计 2 块侧屏，用于显示天气信息和值班信息等，侧屏尺寸为宽 1.2 米，高为 1.6875 米，单屏面积 2.025 平米。

总调度室设计采用一块长约 6 米，高约 2.025 米，面积为 12.15 平方米的室内 P1.25 小间距全彩显示屏。

2、利旧 LED 大屏

多功能厅显示系统拟利旧过渡厅大屏显示系统。原过渡指挥大厅大屏显示系统为 2019 年建设，为 1.25mm 小间距 LED 大屏，屏幕面积 19.2 平米。



利旧设备如下所示：

序号	设备名称	主要参数	单位	数量
1	小间距显示屏	1.25mm 小间距	平米	19.2
2	拼接控制器	多屏拼接控制器采用分布式、全数字化并行处理结构，服务器基于 PCI-E 总线传输数据，由控制（电脑）、信号采集、输出和信号交换等模块构成,各设备之间通过千兆网络连接。 单机可支持 24 个通道输出，采用 HD15/DVI-I 接口输出，每通道显示内存 256MB 以上，输出 1024×768、1400×1050、1366×768 或 1920×1080 分辨率，输出色彩支持 24 位、32 位颜色。	台	8
3	大屏拼控		台	1
4	大屏服务器		台	1
5	混插矩阵	最大支持 72 路信号输入,72 路信号输出；非 FPGA 架构	台	1
6	混插矩阵万能输入板卡	支持 4 路 CVBS\YPbPr\VGA\HDMI\DVI+AUDIO 信号输入	块	12
7	混插矩阵万能输出板卡	支持 4 路 CVBS\YPbPr\VGA\HDMI\DVI+AUDIO 信号输出	块	3

3、新建 LCD 拼接屏

指挥中心新址内各会议室会商室需近距离观看大屏图像显示,综合考虑图像显示尺寸及观看距离，采用 LCD 拼接屏显示方案。

（1）安全生产会商室根据需求设计 12 块 55 寸 LCD 拼接屏，采用 3 行 4 列拼接，通过分布式控制节点控制。

（2）防火会商室根据需求设计 15 块 55 寸 LCD 拼接屏，采用 3 行 5 列拼接，通过分布式控制节点控制。

（3）防汛会商室根据需求设计 12 块 55 寸 LCD 拼接屏，采用 3 行 4 列拼接，通过分布式控制节点控制。

（4）办公楼四楼会议室一根据需求设计 9 块 46 寸 LCD 拼接屏，采用 3 行 3 列拼接，通过分布式控制节点控制。

（5）办公楼四楼会议室二根据需求设计 9 块 46 寸 LCD 拼接屏，采用 3 行 3

列拼接，通过分布式控制节点控制。

（6）保密会议室根据需求设计 12 块 55 寸 LCD 拼接屏，采用 3 行 4 列拼接，通过拼接控制器单独控制，不接入分布式控制系统。

4、其他显示设备

办公楼六楼、七楼共五个会议室：根据需求各设计一台 65 寸智慧屏，内置视频会议等功能。

业务技术楼 1 楼监控室：根据需求设计利旧 2 台 75 寸液晶显示器，用于指挥中心新址视频监控图像轮回巡视。

办公楼 1 楼监控室：根据需求设计利旧 2 台 75 寸液晶显示器，用于指挥中心新址视频监控图像轮回巡视。

办公楼负一层餐厅：根据需求设计利旧 4 台 75 寸液晶显示器，用于就餐时电视节目播放。

尾矿库预警监测室、危化预警监测室、减灾救灾预警监测室根据需求，共设计 1 台 85 寸触摸屏和 3 台 85 寸液晶电视，供尾矿库、危险化学品、减灾救灾预警监测使用。

展厅：根据需求设计一台 85 寸触摸屏和一台电子展台查询机，用于展厅内容展示和信息查询等。

其他值班室等场所：根据需求设计利旧原有 7 台 75 寸液晶显示器。

3. 音频会议系统

3.3.3.1 需求分析

为保证在指挥大厅、会议室等进行应急指挥会议或进行发言、报告等活动时，发言者的声音能够被每一个与会人员清晰的听到，需配置高灵敏度的拾音及扩声系统。

会议室音频设计采用数字会议系统，要求具有较高的整体化和智能化，且系统需采用标准化接口。采用数字会议设备，包括发言设备、控制设备、扩音设备等。

根据大厅或会议室的使用面积和高度，设计扩声系统，参考国家扩声厅级标准一级进行设计，符合 的声学特性指标中的语言扩声一级标准演讲时应能达到语音清晰、无失真、声压余量充足、声场分布均匀、无声反馈啸叫、声像定位准

确。

顺应时代发展趋势，本项目音频系统建设采用分布式网络架构，设备通过网线连接，可任意扩展，满足一根网线联通所有设备和视听场所，实现信息共享、互连互通。分布式音视频系统的优势是以其无限带宽、分散架构、网络化、模块化、高稳定性、高扩展性等特点，这使其更能适应这个时代的不断的变化发展，所以它能在多个领域中应用起来更具有优势。

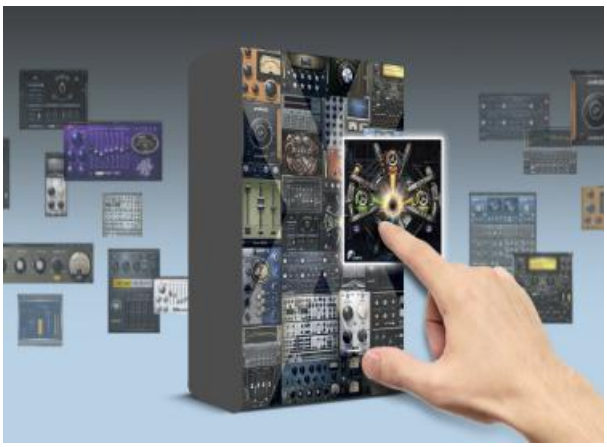
3.3.3.2 建设方案

分布式音频系统是基于网络建设，核心由服务器及各音频节点组成，服务器上运行的是音频处理及控制软件，服务器与云计算技术紧密结合在一起。系统的节点设备（网络处理器或网络音箱）采用网络传输的方式，通过节点设备传输音频信号。接入到分布式音频系统的节点设备可以非常的简单，不需要智能化，只需要把音频模拟量转换成数字的量输入到分布式音频系统中就能完成你所需要的功能，由服务器完成对多点多地信号源进行集中式管理。

分布式音频系统分为以下几部分：

（1）核心设备：分布式网络音频服务器，设备采用开放式处理架构，按需添加插件，1000 多种处理类型，如：混响、均衡、压缩、限幅器、延时器、响度调节器、自动反馈消除器等等。单台设备支持 128x128 矩阵混音，最大可扩容 8000 路音频管理。系统采用主动语音处理技术,无需手动调整,人工智能计算方

式，自动判断啸叫点，自动削减增益，可同时自动控制最多可达 64 通道；支持交叉淡入淡出,过程中不对任何信号进行压缩处理，保证高保真的音质;支持 5.1 和 7.1 环绕声插件处理,可最大组合成 64.1 的环绕声系统;支持先进的侧链处理功能,可消除齿音、调节音色、实现闪避等混音处理；支持 1000 个场景预设。



（2）节点设备：此部分可分为两类，一种是网络终端（无处理能力，如网络话筒、网络音箱），可直接接入网络，由核心服务器统一处理与调度；一种是网络处理节点（有处理能力，如网络数字音频处理器、网络音频节点），些产品用于连接传统的模拟设备，如模拟话筒、DVD、功放音箱等，把模拟信号转换成网络信号进行传输与处理。

（3）控制设备：即系统管理方式，可通过服务器自带的软件进行灵活管理与控制,也可通过第三方控制系统对其进行模式化管理,实现一键切换不同场景、一键恢复最佳状态等。

根据房间的坐席摆放及音频会议功能需求，各功能用房的建设内容如下：

音频会议		
序号	建设地点	建设内容

1	业务技能用房	指挥大厅 72 人	新建有线话筒 51 个+无线话筒 8 个+头戴麦 2 个（不包含无纸化终端 21 个）
2		多功能厅 143 人	新建有线话筒 11 个+无线话筒 8 个+头戴麦 2 个
3		防火会商室 35 人	新建有线话筒 19 个
4		安全生产会商室 25 人	新建有线话筒 25 个
5		防汛会商室 33 人	新建有线话筒 19 个
6		总调度室 19 人	新建有线话筒 19 个
7		保密会议室 21 人	利旧过渡性指挥大厅 2 楼和 7 楼设备 21 个（不接入分布式系统）
8	办公用房	4 楼两个会议室 各 18 人	会议室 1 利旧过渡性指挥大厅 2 楼和 7 楼设备；会议室 2 新建有线话筒 18 个
9		6、7 楼会议室	无
10		8 楼会议室 67 人	无线话筒 8 个+头戴麦 2 个（不包含无纸化终端 43 个）

3.3.3.3 系统特点

数字化处理

本次项目设计，采用数字音频处理技术作为核心处理的技术手段，主要优势在于可提供更为丰富多样化的处理方法，同时数字处理更为高效、快捷；处理能力上，数字处理技术较传统模拟处理方式具备更好的扩展性能，信号接入系统后经过模数转换、采样、量化、编码等一些列的前期转化工作后。信号转化为国际通用标准的数字化音频信号，辅以芯片内的数字算法，配置的核心处理设备可对

信号进行多种方式的转化处理，并且，数字信号很大程度的解决了传输问题，通过 Dante 网络传输协议的携带，可将信号在组网内的任意节点进行自由传输，高效管理。数字处理技术不仅具备处理容量可观、处理手段多样、处理速度高效、扩展能力惊人、产品更新升级便捷等等一系列的优势。

极简系统

分布式音频系统布线较简单，而传统音频系统，设备较多，品牌型号不统一，各个设备间的接口差异巨大，在系统设计初期，要详细考虑到各个设备的数据接口，然后在布线阶段各个设备都需要布多种线材，这不仅仅浪费时间，更加大大的增加了成本。而分布式系统由于采用全网络化设计，各个设备间都只需使用网线连接到交换机即可，无论是在设计还是在布线上都极为简单，这就大大降低了成本费用。系统满足无机柜设计，所有设备均可选用网络型，通过网线连接交换机即可，核心管理服务器放于机房，可远程管理各节点设备，无需在会议室内设置机柜。

易于扩展

分布式音频系统易于扩展，各个多媒体设备相互独立而又紧密相连，各个设备在系统中都是独立的存在的，并不会对其他设备造成影响，而他们又通过交换机间接相连，通过分布式服务器分配其 IP 地址进行数据交换而紧密相连。在会议室应用领域中，由于会议室设计当中我们都会预留网络端口在会议室的桌插或者地插当中，因此需要增加信号时只要把设备通过网络连接到分布式系统的交换机即可，方便扩展。系统便于后期建设扩容，后期增加会议场所，只需增加相应的节点设备，网络联通，即可统一管理。

互联互通

系统采用网络化架构，通过网络可实现所有会议室之间的信号互联互通，既能将 A 会议室的任意音频信号同步到其他所有会议室；也能将其他多间会议室的音频信号同步传输到 A 会议室扩声。满足一对多、多对一实时对讲。通过管理界面可任意切换不同的应用场景，实现不同要求的联席会议。

管理便捷

此次项目建设，共包含不同类型大小会议室 13 间，可在每间会议室配备独立的控制终端，对本房间音频系统进行控制；也可设计 1 套总控终端，支持对所

有房间设备的统一集中管理。

分布式音频系统的远程控制功能，可通过软件客户端、APP、第三方控制平台等实现远程网络化管理与管理，无论身处何处，一切尽在掌控之中。

4. 视频会议系统

3.3.4.1 需求分析

黑龙江省应急指挥视频会议系统，采用华为 MCU 设备作为核心控制设备，部署在应急指挥中心设备间，各视频会议分会场部署华为视频会议终端设备与高清云台摄像机，实现远程视频会议功能。由于全省视频会议系统以华为设备搭建，本期项目需求属于会场搬迁及会场增设，因此仍建议采用华为设备建设，以便于设备兼容、管理及维护。

3.3.4.2 建设方案

现有过渡指挥厅有华为视频会议终端设备 6 台，其中 2 楼指挥大厅 3 台，4 楼会商室 1 台，6 楼视频会议室 1 台，7 楼视频会议室 1 台；现有华为高清云台摄像机 6 台，其中 2 楼指挥大厅 1 台，4 楼会商室 1 台，6 楼视频会议室 1 台，7 楼视频会议室 1 台，仓库存放 2 台。

指挥中心新址需求，如下表：

序号	会场	视频会议终端	视频会议摄像机
1	办公楼 4 楼会议室 1	1	1
2	办公楼 4 楼会议室 2	1	1
3	办公楼 8 楼会议室	2	2
4	业务技术楼 2 楼多功能厅	1	2
5	业务技术楼 2 楼防火会商室	1	3
6	业务技术楼 3 楼总调度室	4	1
7	业务技术楼 3 楼安全生产会商室	1	3
8	业务技术楼 3 楼防汛会商室	1	1
9	业务技术楼 4 楼指挥大厅	5	4
	合计	17	18

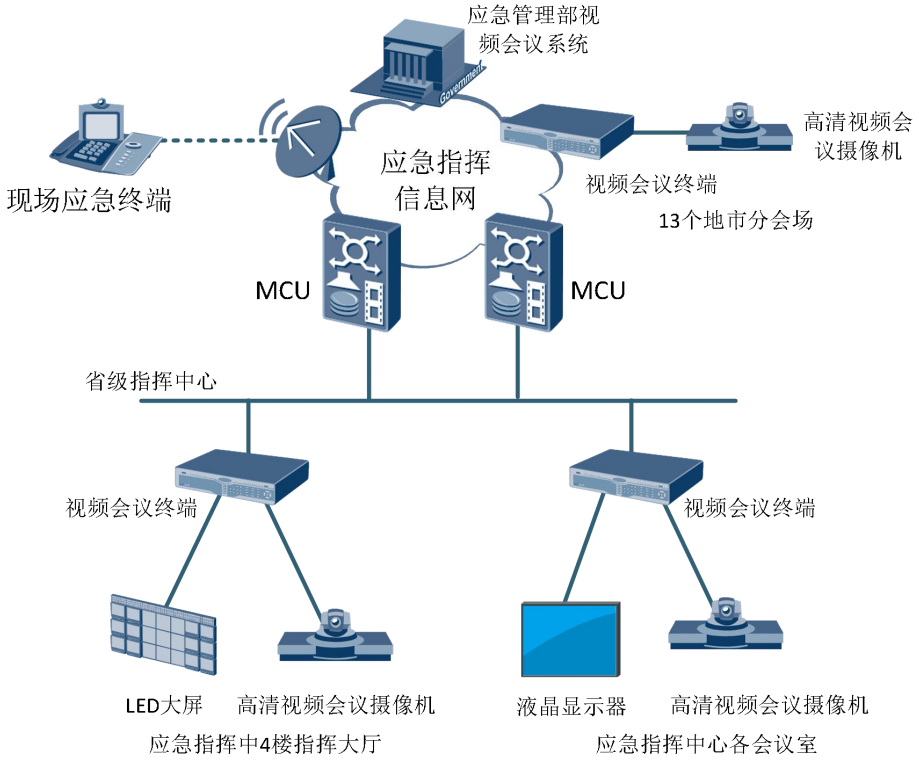
通过设备对比，现有视频会议终端设备 6 台，高清视频会议摄像机 6 台；需求视频会议终端设备 17 台，高清视频会议摄像机 18 台；需新增视频会议终端设

备 11 台，高清视频会议摄像机 12 台。

在指挥大厅、多功能厅和办公楼 8 楼会议室各配置一台会议摄像机控制器，通过 IP 网络控制视频会议摄像机，可瞬时完成多台摄像机的设置，为摄像机的调整节约丰富时间。

由于市、县两级应急管理部门正按省厅要求开展指挥中心建设，从目前调研情况看两级指挥中心配备了不同版本的视频会议系统。为更好提升省级视频会议系统的纳管能力，解决不同版本的视频会议系统图像传输差异，拟升级现有省厅视频会议管理平台进一步保障视频会议系统稳定运行。另外，为指挥大厅配置一套单机版语音识别与转写系统，实现日常会议、报告演讲、指挥调度的实时语音转写文字的能力。上述功能主要包括：会议管理平台、多点控制单元（MCU）、可视化调度级联服务模块、语音转写系统。

视频会议系统拓扑图如下：



现有的高清视频会议系统采用 IP 传输网络，基于标准的 H.323 架构，是一个开放的系统，视频协议采用主流的 H.264 编码同时兼容 H.261、H.263 编码，

可以提供720P高清视频图像。采用H.264编码技术，可以提供图像压缩比，在同样带宽下，能提供更逼真、更清晰、更流畅的画面。通过高清MCU可以兼容4CIF、CIF等高标清视频互译终端接入，支撑高标清视频终端混网融合。

3.3.4.3 系统功能

1、视频会议功能

可召开全网会议、分组会议、多组多点会议同时召开、支持广播会议、支持远程WEB遥控器控制、支持多组多画面、支持一屏多显、支持字幕滚动、支持远程摄像机控制、支撑轮询等功能。

2、远程数据会议（双流）

可将运行的PC界面发送至远端、可将本地计算机幻灯片广播到远端、可连接电子白板、图文摄像机等。

3、多种会议管理方式

BS架构管理，不受地域限制，不管控制中心还是分会场，授权后，都可进行控制。

可通过PAD等无线终端进行控制。

4、备份功能

双台MCU设备组成热备份资源池。

5、统一控制功能

整个会议过程可由主持人控制，画面切换、分屏变化、屏幕视频等功能。

6、支撑高清录制点播

支持会场录制和点播。

5. 无纸化会议系统

3.3.5.1 需求分析

传统会议形式越来越不能满足当代会议需求，会议人数众多，会议资料复杂、会议决策低效等问题成为传统会议的通病。无纸化会议将多种智能化通讯技术、音频技术、视频技术、软件技术融入会议的会前会中会后各个环节，通过文件的电子交换实现会为用户提供极为便捷高效的会议平台，同时也带来全新的会议体验。无纸化会议系统远远不止是实现会议无纸化这么简单，它还要满足传统意义

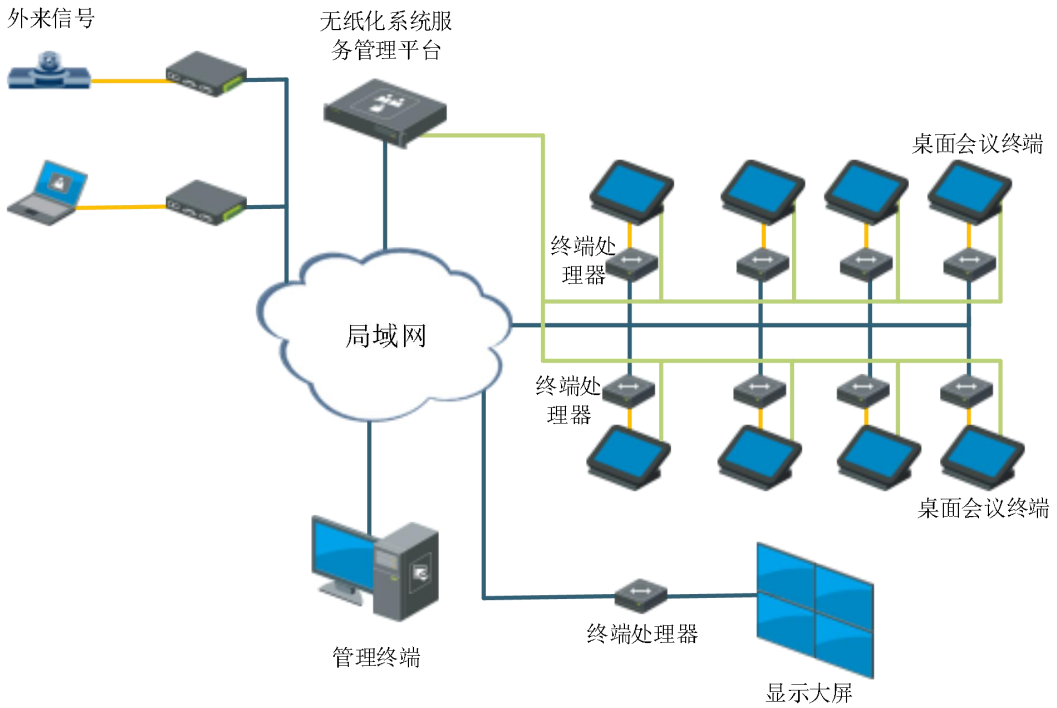
上多功能会议室的各种信号自由交互、互联互通的功能。

3.3.5.2 建设方案

根据使用需求，设计 2 套无纸化会议系统，在每个座位设计 1 台无纸化超薄 17.2 英寸电容液晶屏一体机。各会议室无纸化需求如下表：

无纸化会议			
序号	建设地点		建设内容
1	业务技术用房	指挥大厅	17.2 寸液晶升降式一体机。共 27 套
2	办公用房	8 楼会议室	17.2 寸液晶升降式一体机。共 50 套

整体系统图如下：



触控无纸化智能终端采用超薄 17.2 英寸电容液晶屏，分辨率达到 4K，屏幕

视角为IPS全视角液晶屏，显示效果清晰亮丽。清新显示会议文档，10点触控电容屏设计，触控操作灵敏度非常高，操作方便。超薄设计，铝合金磨砂超薄一体外壳，表面处理为喷砂阳极氧化，宽屏无边框设计，彰显产品高端、尊贵，满足会议室高标准要求。无纸化终端采用分体式设计，由触控显示屏、升降器、无纸化终端组成，方便后期维护和升级更新。系统配置视频编码器，用于无纸化会议系统与外部视频设备的对接，实现视频信号的互联互通。

具体设计如下：

（1）智能会议系统管理服务平台，含系统管理、图像投影管理、流媒体管理等；

（2）无纸化智能终端：指挥大厅需求21个坐席、办公楼8楼会议室需求43个坐席，每个座位席设计1台，用于无纸化会议显示、会议操作；含会议发言升降话筒、智能会议系统终端处理器及终端软件，用于处理无纸化系统的各项功能；

（3）无纸化信号云节点，用于无纸化信号编解码，无纸化会议视频输入/输出等。

（4）在指挥大厅、总调度室、八楼会议室、多功能厅的领导席及无纸化席位使用电子桌牌，共计104个，同时配备7台POE交换机，供电子桌牌使用。

3.3.5.3 系统功能

1、快速组织会议。软件利用Web的优势使得你可以随时使用浏览器访问会议系统组织您的会议。

2、文件分享。在会议开始之前和会议进行中用户都可以随时上传会议所需的资料。

3、同屏分享。在会议开始时用户可以随时分享自己的桌面，使得和其他与会人的讨论更加高效。

4、定义投票。在会议进行时用户可以随时创建一个投票以支持决策。

5、会议消息。会议期间用户可以随时互发消息进行沟通。

6、Windows客户端的分辨率自适应。无纸化智能会议系统，能够让用户在不同的分辨率的设备下舒适的使用系统。支持最小1024*768 到最大2560x1440分辨率的显示设备，兼容Windows各类平板等设备。

7、会议功能全面。大的数据处理能力和文档共享能力，可以协同讨论文件内容并实时圈点批注，批注后的文档可自动上传至主机保存。

8、高保密性管理。无纸化智能会议系统，会议通信采取 MD5&DES 加密措施，有效保障会议内容的安全性，从根本上杜绝传统会议方式下的带来安全泄密等各种隐患。

9、易学易用性。参会者可以在系统中对文件进行亲笔圈阅、批注，从而使不同用户可对所传阅讨论的文件发表各自的意见、相互交流并进行最终的定稿及签署，用户对文件进行的亲笔圈注、签名信息均可被保存，操作简单，界面友好，从而大大减少了培训工作量。

10、绿色环保低碳、提高工作效率。无纸化智能会议系统被认为是绿色办公的最佳实践者，一方面因其将日常办公资料全部电子化，变成可永久存储、随时调用、无需纸质媒介的数字化形式；另一方面其全程无纸化、低碳办公，符合环保大趋势。通过使用无纸化智能会议系统，避免了政府部门会议过程中文件的大量打印，避免了人力及时间的过多消耗，由此提高了工作效率，加快中央政府部门决策部署的传达、贯彻、落实。

6. 会议管理系统

3.3.6.1 需求分析

会议室是楼宇内的公共资源会议室是办公大楼的公共资源，会议室及其附属的设备是召开会议的基础环境。提高会议效率有两个决定性因素：“参会人”和“会议环境”，“参会人”是核心因素，“会议环境”则是基础因素。会议室没有管理，会造成会议室被争抢、重要会议被非重要会议挤占、会议室信息不能及时发布、会议室设备开会时不满足会议要求、会议室设备没有提前调试以及设备因没有及时检修造成故障、会中设备出现故障且没有应急预案等等问题。因此合理的会议规划，信息的提前发布，能有效解决以上问题，提高资源使用率，有助于工组效率的提供。

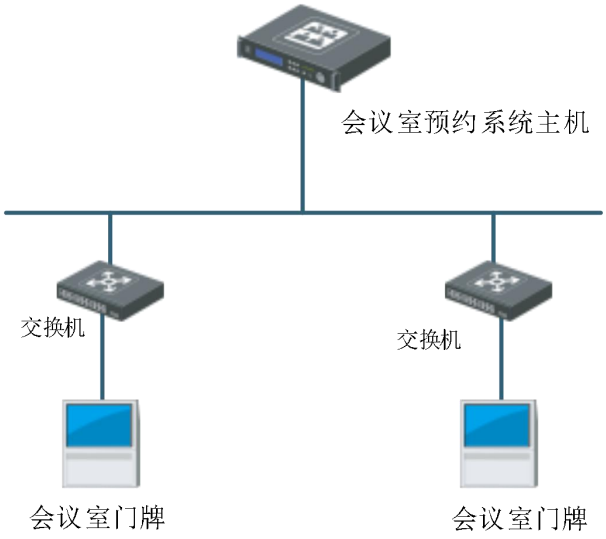
3.3.6.2 建设方案

会议排班系统是利用网络对用户现有会议室使用情况、时间安排、人员安排、

设备安排、会议显示等各种信息的收集与分析，减少工作中，会议室管理混乱，使用不均衡、设备不到位等情况，最大限度的提高工作效率。

联网会议排班系统是用于在网络环境下，对会议信息进行编辑处理和控制发布的专业系统平台。通过平台的操作，实现会议室预定申请，会议室预定审批，会议室状态查询,会议邮件通知，会议室资源管理，会议引导，会议信息显示，会议信息模板编辑等功能；实现会议信息实时显示引导功能，实时动态的将会议室预定信息，传递到每个会议室门口、大厅及楼梯口等公共通道的显示屏上，实现会议信息发布引导功能，会议排班系统由系统管理软件，终端信息显示屏及网络平台等部分构成，结合多媒体信息发布管理系统功能，实现公共多媒体信息实时发布和显示。

应急指挥新址 9 个会议室设计了会议室门牌，业务技术楼包括指挥大厅、多功能厅、总调度室、防火会商室、防汛会商室、安全生产会商室；办公楼包括 4 楼 2 个会议室、8 楼 1 个会议室。会议室门牌通过网络连接至设备间内会议排班系统主机，系统拓扑如下：



3.3.6.3 系统功能

1、会议管理

1）会议预约

通过 web 页面登录会议预约系统，选择预约时间、会议时长，填写会议主题、需参会人员等信息，完成会议预约。

2）会议审核

会议管理人员通过系统完成会议预约的审核，通过或驳回。

3）会议管理

在列表中查看已预约、会议中、已结束的会议等信息，并可查看会议考勤情况等信息。

4）会议签到

通过系统端查看各会议人员签到情况。

5）会议室门禁

人脸识别门禁功能，在会议预约时间内，第一个有权限的人进入后，门禁功能取消，与会人员可自由出入。

2、会议门牌

会议室门牌显示会议名称、会议室状态、日期等信息，可对会议室名称、会议状态、签到二维码、会议列表、门牌背景图案自定义设置大小、颜色、位置等。

3、通知管理

与省厅原有短信平台对接，通过短信方式通知与会人员。

7. 可视化分布式交互系统

3.3.7.1 需求分析

指挥中心作为负责安全信息采集、监测、分析和预警的统一平台，需要接入大量不同类型的信号，因此其指挥调度系统平台需具备超强的信号接入及处理能力，以满足业务需要。

指挥中心提供的大屏幕拼接显控系统可对接入的多路数字 IP 流媒体视频信号进行集中显示。一旦发生紧急 事件，便可实现多部门联合出动，形成“统一指挥、各负其责、快速反应、运转高效”的联合调度指挥体系，更好地保障 的畅通及市民出行的安全。

指挥系统具备以下基本需求：

接入信息量大：系统需要有海量的信号接入能力，实际工程应用中可能需要同时显示几百路视频信号，需要视频信号处理、传输、显示等；

多种格式视频接入：包括网络监控摄像机、高清会议摄像机、席位电脑、视频会议等信号；

方便、快速管理和控制：系统需要快速、随意的调用各种音视频信号；

信息需求点多：所有的信号除了需要在本地显示、存储的需求外，同时满足多场所多点信号的互通和共享；

容易扩展：除了相对固定的信号外，系统需要具备随时接入各种临时和移动信号的能力；

具备特殊信号显示（如超高分辨率、4K 视频源设备接入）和处理功能；

具备远程 KVM 控制功能，可远程管控任意一台电脑；

统一管理：需要一个平台对音频、视频、监控、控制等统一管理，提升智能管理模式，节省人力资源。

传统指挥中心项目建设，各个系统独立运行，信息不能共享，没有关联，形成信息孤岛。现代化的指挥中心是承担多种工作任务的综合型场所，既要担负重大事件、突发事件的现场决策指挥，又要进行日常的办公工作，还要承担会议、访问等接待任务。因此指挥中心建设的指挥调度系统是集多种设备类型和技术门类、多种媒体信息和接口方式、多种通信方式和软硬件平台的多功能综合型平台。

交互式系统是一种新理念的管理控制平台，可对多点多地信号源进行集中式管理，高性能传输的管理控制平台。系统结合了计算机控制技术和网络传输技术，采用网络的控制架构。核心由主机及各节点组成，服务器上运行的是控制软件平台，主机与云计算技术紧密结合在一起。系统的节点设备采用网络传输的方式，通过节点设备控制终端设备和传输音视频信号。接入到交互式管理系统的节点设备可以非常的简单，不需要智能化，只需要把各种量转换成数字的量输入到交互式系统中就能完成你所需要的功能，系统能完成传统集中控制系统所有的控制功能，同时还能把音频和视频信号高保真、高清的格式通过网络传输，把音频、视频、控制和物联网管理等真正意义上结合在一个平台上管理，实现音频、视频及控制同网同步传输。

3.3.7.2 建设方案

为保证系统的稳定性、兼容性和扩展的便利性，核心处理采用网络分布式平台，核心由主机设备组成，具备双机热备份功能，各节点均具备独立 DSP 芯片处

理能力，可完成 AV 系统中的五大工作：控制、传输、处理、管理、存储，要求音视频及控制信号可同网同步传输。

系统支持对接 GB28181、H.323、SIP 协议的监控平台、视频会议平台、可视对讲平台。系统可对接主流 B/S 架构的第三方系统平台，如 OA、无纸化会议、会议预约等。

分布式交互系统采用高清输入输出接口机，取代了传统的拼接处理器，各类视频矩阵以及转换器、网传延长器等。接口机兼容 VGA、HDMI、DVI、SDI、分量等视频信号接入，支持 MIC 以及线路音频信号接入，同时可支持 RS23、485、IO、IR、RELAY、TCP\UDP 等控制方式。

整个分布式音视频管理系统基于 1000M 网络构架，1 个 1000M 网络可同时容纳不少于 1024 路高清信号的接入与传输，可扩展升级。所有的音视频信号经过输入输出节点接入系统，音频、视频和控制在同一个网络内传输，保证音视频及控制的同步性。

分布式架构，单个节点设备故障，不会影响整个系统运行。接口机通过网线连接，布线简单，成本低，维护方便。

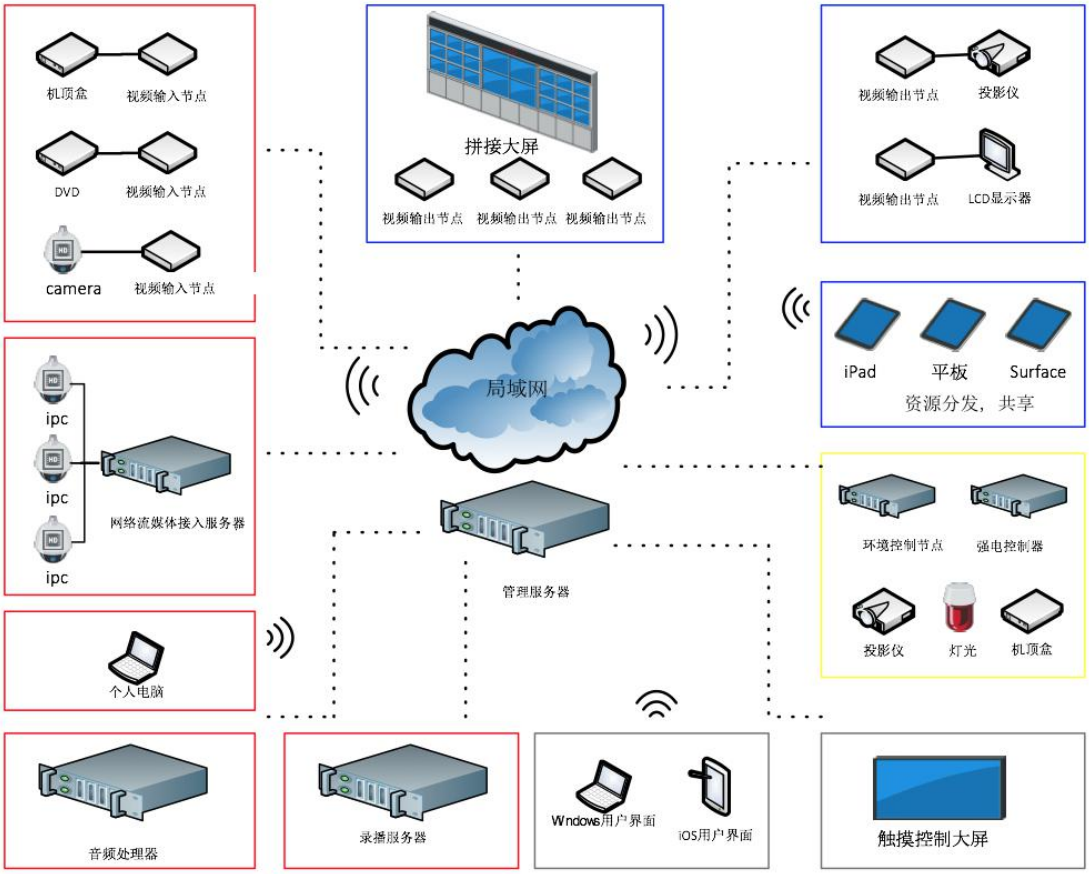
分布式交互系统采用高速图像处理技术，为用户提供可视化超高分辨率信息解决方案，分布式交互系统基于高分显示拼接大屏技术，从统筹、指挥、管理的角度出发，根据指挥决策者的实际需要，整合行业的重点数据信息，快速、精准地在控制中心大屏幕上调用、显示，真正实现辅助决策、业务智能。

它通过良好的高速图像处理技术，真实利用大屏幕整个超高物理分辨率，快速、平滑地显示更加广阔的地理区域；从统筹、指挥、管理的角度，整合海量的行业重点信息，以高分可视化的方式进行组织与分析运算，实现全面掌握行业关键信息动态及趋势，提高总体指挥、决策和管理能力；打通相互独立的业务系统，对海量业务信息的可视化综合，真正的实现辅助决策、业务智能。

分布式交互系统尽量提供模式选择并充分利用功能联动,以降低操作难度，对操作人员来说异常方便。操作界面设置应友善简洁,且通过细致周到的编程考虑对设备起到保护作用等等。对系统的开启、关闭和控制实现快速的响应，确保信号切换、环境控制以及预设程序的连琐反应达到无延时响应。

1、系统组网

系统主要分为五大功能块，媒体前端（图中红框组件），管理主机（图中云朵组件），多媒体终端（图中蓝框组件），用户控制（图中灰框组件），环境中控（图中黄色组件）。



由组网图可以看出，媒体前端并不区分模拟信号还是数字信号，根据媒体前端的信号特点，可以将媒体前端设备变成为交互式系统的媒体源节点。通过解码器，将媒体信号输出到媒体终端，高清输出节高使得大屏幕等媒体终端接入到交互式系统中，成为系统的终端节点。当各个媒体设备成为了交互式系统的节点设备，即被交互式管理主机管控起来。用户可以通过客户端（PC 电脑、智能手机/平板）控制媒体的展示的终端和呈现的方式，实现任何信号，从任何地方来，到任何地方去，以任何想要的方式展示出来。

（1）媒体源前端

媒体源前端（以下简称前端），为交互式管理系统提供了各种各样的媒体信息，其中包括有：个人电脑的屏幕画面、监控平台的视频流、视频会议主辅流、摄像机信号、机顶盒的画面等等。系统提供了多种途径将这些媒体信息接入到交互式管理系统。

（2）媒体终端

媒体终端（以下简称终端），最终呈现给用户的形式，主要以LCD屏幕、拼接屏幕等显示设备为主。媒体终端主要是通过从高清输出节点的音视频输出接口（包括有HDMI音视频输出、DVI-I音视频输出等）获取到媒体数据，来呈现和播放媒体数据。高清输出节点作为交互式管理系统的终端节点，受中心主机管控，换句话说，媒体终端呈现什么样的媒体信息，由中心主机来决定，这就在整个工程应用上具有极大的灵活性。

（2）管理主机

管理主机是系统的大脑，管理主机管理了所有的媒体源节点和终端节点，在这里我们将上图的组网结构，称之为拓扑网络数据，在这个拓扑结构中，各个节点都是拓扑的顶点，而每个顶点之间的通路则由中心主机来决定。比如某个摄像头的信号可以送到某中心的电视墙上显示，某台电脑的桌面可以呈现在培训室的大屏幕上。除此以外，管理主机还承载了系统的所有业务功能，比如说与视频会议系统的信令对接、与监控设备的数据对接等。

（3）网络流媒体接入主机

网络流媒体接入主机是主要是承接的业务是管理和转发外围第三方的媒体流，将第三方的媒体流接入到交互式管理系统中来，并且进行管理。比如监控平台的媒体流需要接入到系统，则可以有两种方法，第一种是在IPCAM的通过DVI-I部署一个编码器，形成媒体源节点，接入到系统中；另外一种方式就是监控平台的媒体流通过流媒体主机的转发，接入到系统中。流媒体主机支持GB28281的协议，即只要是支持GB28281的监控平台都能够通过流媒体主机，都能够纳入到交互式管理系统中来。

（4）录播主机

录播主机是作为系统主机的扩展功能模块，主要是可以将系统的媒体源节点的媒体流录制下来，然后通过系统将录制下来的媒体流再传到解码器，由媒体终端呈现出来。录播主机以场景为单位，最多可以支持32路媒体源节点的媒体录制。

（5）环境控制节点

环境控制节点，顾名思义就是把交互式管理系统周边的环境信号都控制起

来，比如说灯光控制、电动窗帘等环境控制，对于终端设备（如投影机）来说高清输出节点即可对其管控，则不需要环境控制节点管理。

（6）用户控制客户端

用户控制客户端，是作为用户控制系统的唯一入口，支持 WINDOW/IOS 系统，客户端的界面可以根据实际的工程项目的需要，由管理软件来设计生成。并且支持多用户不同权限的控制界面定制，比如说管理员和操作员，由于两人的权限不同，能够控制的范围也是有差异的，那么可以通过设计不同的用户界面支持这两种角色的权限控制范围。所以用户控制客户端是支持完全深度定制化，完整的权限划分。

2、在指挥方面的应用

分布式交互作为建立在标准 1000M 网络上的分布式 DSP 多媒体处理系统，具备处理容量大、系统稳定、使用方便、可视化交互性能强、结构简洁、扩展方便等特点，能够与应急调度指挥系统进行较好的融合，代表着未来指挥系统发展的方向。

- 分布式交互系统主要特点如下：
- 极简人机交互体验.可视化操作界面
- 支持多屏集中管理，全信号源跨墙调度
- 平台支持多个物理隔离网段内计算机桌面视频的采集、调用，甚至广域网，只需提供固定的 IP 地址即可。
- 可对各信号源实时预览
- 多预案设置与自动切换
- 集成各类外设控制，定制化开发
- 支持 PAD 及触控一体机控制
- 屏幕镜像功能，可将指定屏幕内容镜像到另一个或多个任意尺寸的屏幕
- 指挥中心所有信号源、屏幕均通过 1000M 网络统一管理。
- 使用者手持 PAD 即可轻松调取信号源、一键加载场景，分发视频。实时可视化控制，操作直观，简易，便捷。
- 支持指挥大厅内的电气设备，实现对投影显示、音频扩声、会议系统、灯光环境、窗帘等设备进行全面、自动化、智能化控制；

- 实现各子系统的独立操作或模式化操作。
- 屏幕镜像将指定屏幕内容镜像到另一个或多个任意尺寸的屏幕上。即使不在指挥大厅，也能100%同步了解所有中心大屏实况。

3、在视频系统中的应用

分布式交互系统采用高清接口机，取代了传统的拼接处理器，各视频矩阵。每块屏幕单独连接接口机，每块屏幕独立运算，分布式架构，单个节点设备故障，不会影响整个系统运行。接口机通过网线连接，布线简单，成本低，维护方便。整体可实现信号的漫游，堆叠，跨屏等功能。

整个系统操作简单、智能，可使用PAD／笔记本等设备操作实现所有信号的调用及实时预览。可以说一根网线连通所有设备，一切管理尽在指尖操作。

交互式管理系统针对视频信号可完成多方面的无缝对接：

- 与各种视频设备的对接

关于高清摄像机，高清视频会议终端，蓝光播放器等视频设备的对接，分布式交互系统视频接口机支持信号种类包括DVI、 HDMI、YCbCr、VGA、HD-SDI等，可自适应不同的视频设备，无需考虑信号源及显示终端接口等问题。

- 与工作站系统的对接

可实现工作站席位中任意电脑信号，包含任意应用程序，表单文件，视频文件的信号传输至大屏显示系统。

- 与任何移动式笔记本电脑输出信号的对接

可通过无线传输模式，将任意的电脑输出信号传输至大屏拼接或系统中任意显示终端。

- 与监控平台信号的对接

本系统可扩展接入不同品牌、不同网段的IP camera设备等监控信号进入本系统，只需配置一台高清流媒体数据接入主机即可，单台主机最大可输入1024路IPC，支持16路(1080P)或32路(720P)或72路(D1) IP Camera同时输出至大屏。满足指挥中心对网络IP摄像头的调用及监控。其主要特点如下：

- 集成近百种主流IP Camera
- 无需外置H.264解码器以及任何转码设备
- 支持标准及私有协议，可快速添加新型

- 1 个千兆分布式交互网络可同时容纳 1024 路+高清信号的接入
- 将分散的节点通过网络集合成可视化信息至统一管理平台
- 与超高分辨率信号的对接

系统支持动态超高分辨率显示，最大支持 16 个 1920*1080 分辨率的点对点显示，线路运营图、SCADA 图、电网图、精细业务数据图表等均一览无遗，尽收眼底。

4、在管理方面的应用

交互式管理系统结构简单，设有高清输入节点、高清输出节点、控制终端及软件等。功能要求如下：

- 可任意调用各职能部门的席位电脑音视频、视频会议音视频、以及监控摄像机的视频信号本地显示,同时可根据要求开放共享互传资源；
- 系统管理满足室内电脑有线控制或 PAD 无线控制；
- 根据要求可设置不同权限，分级管理；
- 支持一键模式场景调用，音视频联动管理；
- 满足 20 路以上视频信号实时动态回显预览；
- 满足所有音视频节点均带 DSP 模块，可独立完成信号处理；
- 满足音频、视频、控制同网同步传输；
- 系统自带大屏拼接、漫游、叠加等功能，不需要传统拼接处理器；
- 满足拼接大屏开关机管理；
- 高清节点支持远程 KVM 控制；
- 支持监控摄像机直接接入系统，随时大屏调看；
- 支持室内全信号的任意组合录制、直播、点播等功能；
- 满足音频系统的控制：音量大小控制、扩声模式切换等；
- 满足室内灯光开关及多种模式控制；

可实现同一管理平台、同一网络下多用户、多终端、多操作平台下集中控制管理,指挥大厅和 室采用无线触摸屏或有线触摸屏即可实现对整套系统的控制，包括输入输出、环境控制、系统状态等信息都能及时反馈到控制界面上，使以往复杂的操控变得简单和直观。

本期配置分布式输入节点、分布式输出节点、分布式同步输出节点共计 339

个，配备核心交换机 1 台以及普通交换机 45 台，供分布式节点以及无纸化终端等设备连接使用。

3.3.7.3 系统功能

1、数据展示可视化

分布式系统支持音频和视频同时可见功能，可在控制界面上同时反馈每路音频信号实时动态电平及实时动态视频画面，增加了信号的反馈性，减少了控制的失误率。操作员通过控制终端将需要的视频信号快速、准确显示在屏幕上。

分布式系统可提供实时信号预览达 20 路以上，所有操作基于图形化、触摸拖拽式操作，达到人机交互功能，可采用多点触控的方式，实现对信号窗口的放大、缩小、移动、关闭，在控制的同时可实现所见即所得的控制效果。

系统管控界面可根据要求定制，如界面布局风格、控制主题、LOGO 等均可根据需求定制。

2、信息融合平台化

对于指挥中心内音视频信号，涉及业务电脑、摄像机、DVD、视频会议主机等本地模拟音视频信号，以及网络监控信号等，本地模拟音视频信号可通过高清输入接口机专为网络信号接入系统，信号可同时支持 VGA/DVI/HDMI/ YPbPr/SDI 多种常用格式信号。视频编码采用国际标准算法进行编码，通过国际标准 RTSP 传输协议进行音视频传输。对于监控信号，可通过监控融合主机进行转码统一管控，实现海量信息统一平台化调度、管理。

3、功能应用综合化

分布式交互系统采用 IP 网络化架构，平台化管理方式，系统可集成视频监控平台、视频会议平台、超高分展示平台等。实现多平台统一化管控：

支持监控平台无缝数字对接：支持国家标准 GB28181 协议，通过平台强大的解码能力，可把所有的监控系统调至大屏上显示，也可在有线或无线触摸屏上实时预览监控信号

支持视频会议平台无缝数字对接：系统支持视频会议系统信号直接读取、调用，无需视频会议终端，即可召开远程视频会议，支持 SIP/H323 协议，支持从视频会议 MCU 取媒体流直接上墙；支持从分布式管理系统中任意的媒体源提交给视频会议系统。

支持超高分展示平台上屏显示：系统支持超高分辨率显示，可显示指挥中心GIS、SCADA、GPS、TDCS 等超高分辨率信号，在拼接屏上整屏高清显示。也可用于显示超高分数量分析软件等。

电话系统融合：系统音频核心（数字音频处理器）支持电话信号接入、回传，满足市民热线与指挥中心音频系统打通，实现与电话的实时对讲，直观，图形化的电话拨号、接听、挂断界面，支持通话记录查询等功能。

4、业务处理协调化

本系统支持无纸化办化系统接入，支持多人多点互动讨论、桌面共享、白板演示等。

支持人可将多个部门领导、专家等所在屏幕画面拖拽在智能屏幕上进行多方交流。可直接在智能屏幕上写画、同步研讨。可直接通过触摸对摄像信号进行调焦。

会议主持人可以将任意智能交互云会议图像、网络视频图像、本地视频图像分发到每一个移动终端上，让与会者自由地操作切换视频以及材料，并且能够用悬浮窗的方式观看视频，达到真正的双向流动，视频文件两不误。主持人通过手触、笔触、教鞭等，对 PPT 播放、文档翻页、重点标注、视频画面的缩放聚焦等。

会议开始后，无纸化系统可显示当前会议的主题、与会人员、会议资料、议程、公告等信息，参会人员分不同权限查阅此会议授权的所有文档。可任意设置某位参会者为当前发言人，发言人可以将自己对文档操作同步给全体人员。

全体参会者可以在本地无纸化终端界面或者会议室大屏幕中看到当前会议资料，同时展开讨论。会议过程中可以发起投票，全体参会者通过无纸化终端参与投票。同时，可以将会议中的视频、声音、会议议程、资料文档、投票表决、会议考勤等全部内容，统一录制为文件，录制好的文件可以作为会议资料进行存档保管。

系统支持智能会议终端与会议大屏幕联动功能。支持同一文件在多个屏幕上由多人同时修改。屏幕之间不仅支持一对一联动，还支持一对多、多对多协同以完成更为复杂的任务。

系统支持智能会议同步演示功能，会议主持人可通过智能屏幕分享会议材料给所有参会人员，在参会人员的显示屏幕上同步显示主持人正在展示的内容和笔

迹。

系统支持音频随路切换，大屏幕可显示多项会议内容，支持触控某一项内容时，播放音频可立即切换到正在展示内容的随路音频。

5、运营指挥平台化

系统可实现突发事件信息的接报处理、跟踪反馈和情况综合等值守应急业务管理。按照统一格式，通过应急平台报送特别重大、重大突发公共事件信息和现场音视频数据，以及特别重大突发事件预警信息，并向有关部门通报。

利用视频会议、异地和指挥调度等功能，以及移动应急平台，为各级应急管理机构应对突发公共事件提供快捷指挥和对有关应急资源力量的紧急调度等方面的技术支持。

系统支持多项任务联动处理，实时信息反馈，多任务一键式快速响应，系统支持人与数字代码化的指挥内容高度融合，实现“人数合一”：确保使用者能够对指挥内容进行可视化直接操作（即看到什么就可以自然地直接操作什么），系统联合多平台及多套指挥中心的信息，多方联动响应，实现综合管控。

四、 基础支撑系统建设

1. 视频监控系统

3.4.1.1 需求分析

数字视频安防监控系统主要是对项目内公共区域进行全方位 24 小时不间断的视频监控；在监控室通过电视墙实时显示整座大楼内外各个监控区域的现场情况。

本项目为一座连体统合性的大楼，分为办公楼与指挥中心两部分，视频安防监控系统主要是在电梯轿厢、入口大厅、各楼层出入口处、楼道走廊、指挥厅、餐厅等处设置摄像机，既考虑到公共位置的安全，又兼顾到重要位置的隐私，摄像机布置要严密、合理。结合环境部署不同安装方式摄像机，进行全面实时监控。

办公楼与业务技术楼一层各设置 1 个监控室，用于安保工作。

3.4.1.2 布点原则

本项目点位部署主要考虑监控区域的视频图像采集，结合大楼的环境特点与实际应用需求，通过对大楼安全防范区域设置监控设备，为大楼提供安全监视、

证据提取等有效的技术防范手段。本次设计选用的前端摄像机监控图像质量为1080P（1920*1080），以获取更多图像中的关键信息。在针对不同区域进行监控点设计时，主要遵循以下几点原则：

按需确定监控区域：监控点设计首先应根据环境特点与管理需求确定监控区域，如一楼出入口的人流量大，属于安全防范的重点监控区域，设置视频监控点可以记录进出人员的特征，且管理人员可以通过云台控制对异常人员进行跟踪监视，对于不法人员的进出，事后均可进行录像调阅。

根据监控视野选择适用的镜头：在摄像机图像传感器（CCD/CMOS）尺寸确定的前提下，所需监视的场景大小以及监视场景与摄像机的距离，决定摄像机镜头的焦距，在不同距离处需要看清人脸，需选择不同尺寸的焦距。

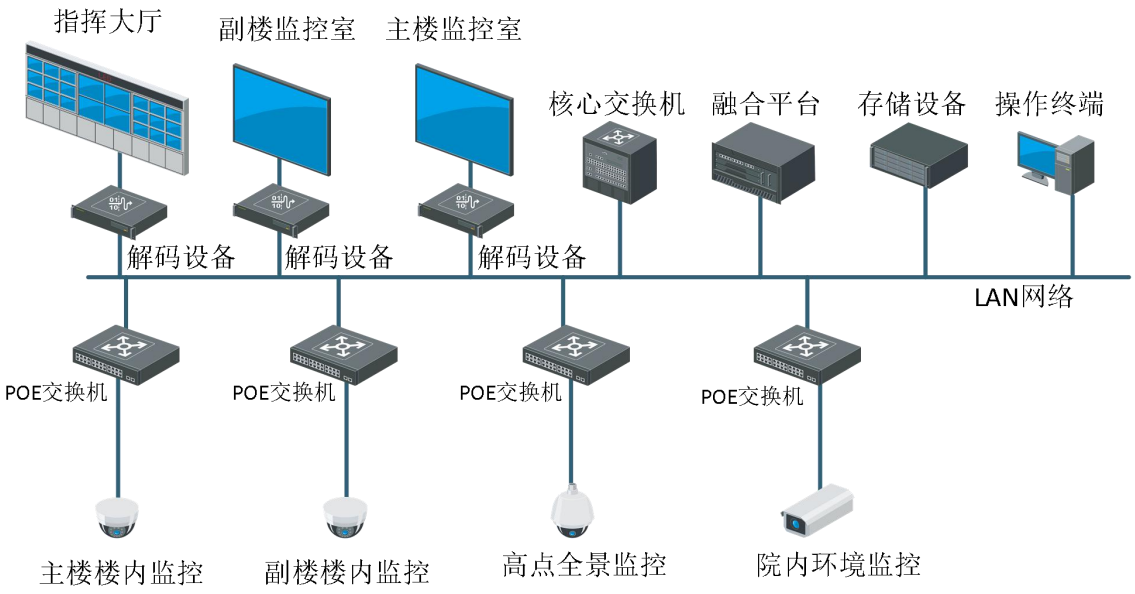
选择合适的外形、尺寸与安装方式：前端监控设备的选择应考虑安装后不影响大楼环境的整体舒适性，同时考虑部分监控设备的隐蔽安装需求，根据监控区域的环境特点选择合适的外形、尺寸，如枪式摄像机、半球摄像机、球型摄像机等，并根据现场安装条件选择便捷合理的安装方式，如室内壁装、吊装，室外立杆安装等。

选择合理的功能配置：根据监控区域的环境特点与安防管理需要，合理选配前端监控点的功能与配置，如办公楼楼道光线较低的环境下，需要看清监视场景的细节，需配置红外灯或选择超低照度摄像机。

选择最佳的安装地点：在监控区域内选取合适的安装点，以满足设备取电与布线的便利性，同时考虑周边昼夜环境对视频采集效果的影响。

3.4.1.3 建设方案

视频监控系统由前端部分、传输部分、控制部分、显示及记录等四大部分组成，控制和记录部分采用 IP 网络化的解决方案。具有图像的显示、切换、控制等功能，硬盘录像机具有画面分割、图像记录、按时间、通道查询及回放等功能。



1、前端监控部分：

楼内：楼内监控摄像机采用半球吸顶式摄像机，安装分布在大厅、楼道、电梯口、食堂等公共活动区域。

室外：院内监控采用枪式一体机，安装在楼体墙壁外侧，实现对院内环境监控。

高点：高点全景摄像机安装在办公楼楼顶，对院内及周边环境实现整幅图像画面监控。

2、传输部分：

办公楼与业务技术楼内各汇聚点设置 POE 交换机，由 POE 交换机通过双绞线与摄像机互联，由 POE 交换机内置的供电模块与前端摄像机供电。

各汇聚点 POE 交换机通过楼宇综合布线网络连接核心交换机，实现图像的汇聚转发。

3、中心端平台部分：

控制中心是整个系统的“心脏”和“大脑”，是实现整个系统功能的项目。

4、中心端存储部分：

中心端配置视频存储系统，将前端重要监控图像经后台编目发布主机（录像发布平台）编目后保存到存储主机。

存储主机建议采用监控专用存储系统，高清监控系统的存储系统需适应大码

流并发写操作，而且是以写为主、以读为辅的应用，应优化资源分配，保障高清监控存储系统能长时间运行在大并发量、大码流的工作环境下。

存储系统建议支持 IPSAN 工作模式，IPSAN 多工作于集中存储或者用于中心备份存储，集中存储是利用 iSCSI 协议透过 IP 网络将视频数据全部集中保存在数据中心，中心备份存储是在 NVR 定时录像的基础上，经编目主机编目后发布并备份保存在中心的 IPSAN 内。

以每台摄像机的码流 2.5M，保存 30 天计算，每个前端存储总容量(TB)＝【2.5Mbps×60 秒×60 分×24 小时×30 天/8】/1024/1024=0.77TB。

本期项目共计布放监控点位 142 个，合计需要存储空间为 109.34TB。

5、显示部分：

视频监控显示部分设置在办公楼一楼监控室，业务技术楼一楼监控室。监控室内各安装 2 台 75 寸液晶显示器用于视频图像显示。

2. 门禁系统

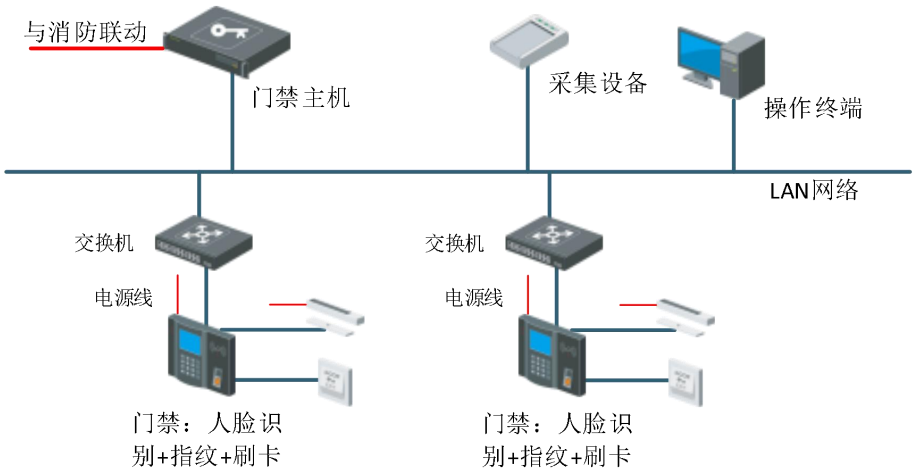
3.4.2.1 需求分析

门禁系统对重要出入口进行权限控制，授权人员才能够进入。通过对不同人脸信息、IC 卡权限授权，实现不同人员、不同区域、不同时段的权限管控。

3.4.2.2 建设方案

整个系统由门禁管理中心、传输网络、门禁一体机、读卡器、开门按钮组成。其中门禁管理中心包含人脸采集注册、卡印刷、卡发行、挂失、注销等功能。本系统只设一个门禁管理中心，通过统一人脸采集、制卡、权限管理等操作，无需再到各子系统进行任何授权操作。

门禁管理中心主机与楼宇消防系统联动，在发生火警时，系统进行 220V 断电，使门禁处于失效状态，便于人员及时逃生。



业务技术楼门禁采用门禁主机+电磁锁形式，门禁主机具备人脸识别、指纹识别、密码及刷卡识别方式。采用 7 英寸 LCD 触摸显示屏，200 万像素双目摄像头，面部识别距离 0.2-3m，支持照片视频防假。

控制中心设置信息采集设备 1 台，支持人脸采集、指纹采集、卡片录入、身份证采集；支持有线网络、无线 WiFi、USB 口通信；支持在线采集，通过网络协议或 USB 口对接到平台，平台进行在线采集，采集信息实时上传。

3. WIFI 覆盖系统

3.4.3.1 需求分析

随着互联网的发展，移动终端的数量呈爆炸式的增长，需求也越发的广泛，极大的推动了无线网络的发展，对于政府单位而言，难免会遇到有人在自己单位私拉乱接无线网络的情形发生，有业务需要的需求背景，也有管理运维的难度问题；时常发生网络地址冲突，私接路由影响业务上线现象，网络产生新的网络边界问题，为此建设一张网络状态可视、身份权限可统一管理、具备内网无线通信管控与防御，能够清晰呈现业务数据、网络状态数据并方便维护与管理，有效发送相关告警提示的无线网络已经成为了大家建设过程中的共性要求。

通过统一建设全楼覆盖的 WIFI 网络，杜绝私接无线行为发生，避免网络管理混乱和网络安全漏洞，在集中管控、安全可靠的网络环境下，提供办公人员方

便快捷的无线上网环境。

3.4.3.2 信道划分

按照 802.11bgn 协议规定，WIFI 工作频段带宽为 83.5MHz，划分为 14 个子频道，每个子频道带宽为 22MHz。在多个频道同时工作的情况下，为保证频道之间不相互干扰，要求两个频道的中心频率间隔不能低于 25MHz。在一个覆盖区内，直序扩频技术最多可以提供 3 个不 重叠的频道同时工作。

因此，频点分配原则如下：

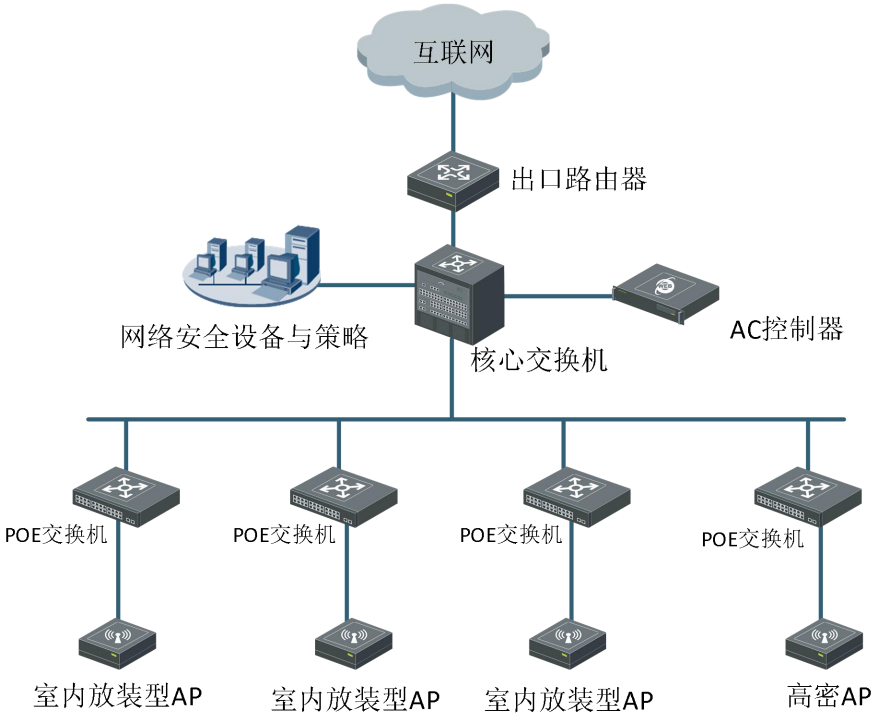
原则上采用同一频点组中的 3 个不重叠频点（如，1、6、11）进行频点规划；

相邻覆盖区域的 AP 不使用相同频点；

相同频点通过间隔较远距离或者建筑隔断增加同频隔离度，避免同频干扰；在容量极高区域，可采用 1、3、6、8、11、13 频点的紧凑复用，提高区域内的承载容量，必须详细提供各个 AP 的覆盖区域以及模测效果，说明已采用避免干扰的布点及规划。

3.4.3.3 建设方案

本设计方案按照 AP+AC 的结构化无线网络解决方案进行设计。网络拓扑原理如下：



办公楼与业务技术楼门厅、走廊、会议室内采用普通室内放装型 AP，内置天线；指挥大厅、多功能厅等人员密集区采用高密度 AP。

各 AP 设备就近接入本楼层 POE 交换机，实现网络接入与设备供电。各楼层 POE 交换机汇聚至核心交换机。中心端 AC 控制器旁挂于核心交换机，实现 WIFI 控制功能。WIFI 系统的安全审计功能依托整体网络安全策略，不再单独建设。

3.4.3.4 系统功能

1、身份统一管理

无线办公网采用 802.1X/Portal/WAPI 认证，外置 AAA 以及 RADIUS+AD 用于存储用户账号密码。

每个账号对应一个员工，包括姓名、部门、手机号等个人信息，保证每个上网的账号都是可寻的，便于安全管理。

用户输入账号密码上网验证时均采用加密传输，防止黑客空中拦截，窃取账号密码等数据，多因子技术有效防盗号。

自动将账号与上网终端的硬件特征码进行绑定，防止员工账号被他人使用或者被盗用。

每台设备的硬件特征码是唯一的，无法通过软件修改。即使通过软件修改仍

然可以识别原始的。每个账号最多可绑定 5 台终端，超过时需要管理员审核。

联动原有业务系统的 Radius 等认证系统实现用户密码管理及自助修改，无需通过管理员即可修改密码，提高效率。

若账号绑定手机号码、口袋助理、钉钉、企业号等移动终端自助修改密码。

二维码审核认证，外来访客连接无线网络后打开浏览器，访问任意网站时，系统将页面重定向到认证页面，认证页面中会显示二维码，具备审批权限的内部接待人员，使用终端扫描访客的认证界面上的二维码，外来访客即可上网。

无线办公网采用 802.1X/Portal/WAPI 认证，外置 AAA 以及 RADIUS+AD 用于存储用户账号密码， portal 认证界面五张大图可以任意上传作为政府单位的党建展示。

2、网络安全管控

接入前&接入时进行身份认证、账号绑定（硬件码+手机号），采取虚假热点检测及防御、网络攻击防护、射频定时关闭及安全加固。

接入后&上网时进行访问权限控制，上网后进行上网行为记录.

防止黑客在窗口业务区附近搭建一个一模一样或者类似的 Wi-Fi 名称，诱使用户连到虚假钓鱼 Wi-Fi 上，黑客利用分析软件从用户上网产生的数据包中分析提取用户隐私信息。

通过 WIPS 无线入侵防御系统实时检测周围无线信号，当检测出来的信号 BSSID、且 AP 源 MAC 地址不在授权列表中时，向对应的 AP 和终端发送解除关联帧，让终端无法连上钓鱼 Wi-Fi。7×24 小时不间断监测网络。

3、无线通信防御

对典型的危险攻击行为进行检测，当超过设定的阈值后自动将攻击者加入到黑名单中，并冻结一定时间，即时发现网络攻击并进行防御。

检测的攻击包括：DDOS 防御、ARP 扫描、IP 扫描、端口扫描防御，禁止客户端私设 IP 以及 ARP、网关欺骗防御、DHCP 请求泛洪防御。

针对网络中存在的横(东西)向流量，针对互访存在的可能潜在的风险进行呈现，当有异常终端在网络中发起不合规的流量请求或扫描时，可通过配置策略第一时间发现潜在网络中的问题终端与病毒，早起发现病毒风险。

通过射频关闭控制策略，可指定某 SSID 网络，定时自动关闭和开启无线网

络射频信号，下班后自动关闭射频信号。

一方面可以节能减排、节省电费支出；另一方面又能防止非法用户利用深夜时间入侵无线网络，做一些非法的操作。

4、业务、数据可视

通过应用识别技术，可以根据应用类型或者具体某一种应用进行封堵，包括视频、论坛、游戏、金融、下载等 5200 多种网络应用。比如上班时间不允许炒股、P2P 下载、外发敏感文件等； 支持主流移动平台，可识别 IM、社交、Mail、新闻、炒股等应用。

网络控制器内置千万级别 URL 分类库，能够对 URL 进行识别，包含新闻、购物、金融、教育等 18 个种类的 URL 地址； 准确识别目前主流网站，识别率高达 99.9%，有效实现网页过滤。

通过基于时间段的访问控制策略，实现不同的时间段不同的访问权限，比如上班时间，禁止访问网上银行、游戏、论坛贴吧等与工作无关的应用。

办公区域内，不同办公部门总会有各自专属的无线网络，并且不希望部门之外的成员使用这个网络。无线网络控制器可以根据用户的属性，限制禁止非本部门的用户接入。

支持对用户的接入认证、访问控制、流量管理、上网行为审计等，并提供统一中文 Web 管理界面，一站式服务，极大降低网络建设成本。可以通过 web 界面查看内网当中的流量访问走势和终端访问情况。

4. 全楼广播系统建设

3.4.4.1 需求分析

广播系统的建设是指挥中心及办公场所必不可少的硬件设施，在应急指挥调度及日常办公上发挥着重要作用。因此，广播系统建设非常重要。系统选型应从实际出发，综合指挥中心建设规划情况，结合广播系统的投资，按照对广播系统使用功能的需求，选择数字 IP 网络广播。

3.4.4.2 建设方案

基本功能

(1) 多音源播放：每分区音频解码终端都具有独立的 IP 地址管理，可实现不同

分区播放不同音乐节目。

(2) 分控站管理：配置好寻呼话筒，无需亲临机房就能对整个学校进行广播，也可实现分控发布学校管理信息。

(3) 背景音乐自动播放：为丰富学校生活，在傍晚的时候可以播放轻柔的音乐，可舒缓气氛，有效改善学校环境。

(4) 时事转播、电台转播：系统可对 AM/FM 调谐器进行定时控制，播放时事政治相关内容。

(5) 声卡采播功能：通过服务器声卡输入，可将 CD、调谐器、卡座等外控音源按编程设置实现单路手动或自动播放输出。

支持实现功能

(1) 外接音源定时采播：采用软件编码终端功能，可把外接 DVD、收音机、卡座等音源设备，馈送到任意终端进行播放。实现外部音源定时自动播放功能。

(2) 支持 U 盘播放：终端具有外接 U 盘插口，具有 MP3 音频解码功能，终端支持读取 MP3 格式音频节目。可通过终端面板或遥控器对 U 盘歌曲进行选择播放，同时支持录音存储功能。

(3) 支持本地话筒\线路输入：系统设有话筒、线路输入口，可将本地话筒或 DVD 等线路信号接入。实现本地无线话筒讲话及本地外接音源播放信号放大功能。

(4) 环境监听：应用网络监听音箱通过 IP 广播服务软件设置，可对任何终端节目流进行监听，监控音频播放输出是否处于正常工作状态；也可在各分区终端上安装微型拾音器，可对现场环境进行实时监听。

(5) 短信广播：在突发紧急事件时，人员可通过编辑短信，实现短信紧急自动广播，可用于自然灾害、求救等紧急广播。（注：需配置 IP 短信猫）

(6) 电话广播：系统可以通过打入电话来控制广播讲话，便于领导即使不在办公室也可以随时发布紧急广播通知。（注：需配置远程 IP 网络电话转接器）

(7) 2.4G 无线模块、蓝牙推送：终端可选配 2.4G 话筒模块、蓝牙模块，可实现学校教室老师讲课以及手机蓝牙播放音乐。（注：应用于学校为主）

系统特点

(1) 全程网络化，数字化通信：系统采用网络数字化架构及网络传输控制管理，

避免了传统音频广播的信号衰减与噪音，提供高保真音质的声音；

(2) 智能化设计，自动化操作：系统通过各项编程实现自动播放，定时播放、循环播放等智能化播放功能，图形菜单化界面设计，操作简单明了，管理方便快捷；

(3) 分布式架构，强大扩展性：系统采用分布式架构建设，施工简单方便。每增设一个 IP 广播点，只需增加网络广播适配器即可。利用内部通信网络，广播系统与计算机网络系统可以共用，减少多网建设投入；

(4) 稳定可靠，零维护运转：系统借助于成熟的以太网络通讯技术，每一台终端设备相当于一台接入学校内部网的终端，系统采用独立网段设计，嵌入式主机等，在网络正常使用的情况下，实现系统零维护。

本期建设包含 93 个扩声喇叭在内的一套全楼广播系统。

5. 基础配套系统建设

3.4.5.1 设备间总体规划

如何使项目的智能化系统的设备在设备间内安全有效地运行，如何保证数据及时有效地满足项目正常运营，很重要的一个环节就是设备间建设。设备间的环境条件，如：温度、湿度、洁净度、噪声、振动、静电、电磁干扰、防雷、接地系统等条件及其控制精度对于设备间中的各类计算机网络、通信、自动化设备的稳定、可靠的运行有着至关重要的作用。

由于分工界面的划分，本期项目只负责设备间的网络机柜和主机机柜的布局、配电系统的建设。其他系统由土建项目弱电部分负责，设备间的承重问题也同土建项目沟通，在其规划设计过程中充分考虑设备间的承重。

由于应急指挥中心新址空间限制，可用于设备间用房为 7 个独立房间，分布在 1-4 层。考虑承重问题，一层设备间作为 UPS 主机及电池组用房。根据用户需求，指挥信息网、政务外网、互联网三网隔离需求，考虑楼宇各设备间需要互联，与办公楼互联，三家电信运营商线路进线等因素，将 4 层大设备间用于指挥信息网设备用房；4 层小设备间用于指挥大厅配套信息化设备用房；3 层大设备间用于政务外网设备用房；3 层小设备间用于配线间，作为整个新址综合布线的枢纽中心；2 层大设备间用于互联网设备用房；2 楼小设备间作为楼宇智能化配套设备用房。

根据需求分析，将 7 间设备间用途进行规划，如下图所示：

3.4.5.2 设备间布局建设

设备间内除网络设备外，还有各类主机、服务器、配线设备等，只有合理的规划设备布局，才能充分发挥各子系统的功能，便于今后的扩充，方便运维人员的管理。

(1)系统主机、存储设备、服务器机柜宜分区布置，主机、存储设备、服务器机柜等设备应按产品要求留出检修空间，允许相邻设备的维修间距部分重叠。

(2)设备之间走道净宽不应小于 1200mm，才可以包装充足的安装检修空间。

(3)划分阶段进入的设备及预留扩充设备的相对位置，既要符合计算机系统的工艺流程，又要方便今后扩充设备的进场就位及线缆的连接。

(4)服务器机柜侧面可无间距排列，并柜，以便于强、弱电线(缆)的敷设。每排机柜之间的距离最好符合地板模数，以避免机柜前后出现小于 300mm 的补边地板。

(5)设备较多的综合布线汇聚建议使用配线柜，使综合布线线缆汇集到配线柜而不是核心柜从而节省双绞线与光纤。

考虑承重因素影响，将指挥中心一层作为 UPS 与电池室用房，电池组采用多

层电池柜安装。

2-4 层房间作为网络设备间使用。机柜采用一字排列，网络机柜作为配线及网络接入层用，操作比较频繁，靠近设备间门口侧布置；设备间业务平台设备及网络安全设备等，在设备间内一字排列。

共配备机柜 54 台、ODF 柜 6 台以及机柜对应的 PDU 电源 162 个。

3.4.5.3 配电系统建设

对于设备间内的各重要设备采用干净、不间断的电源供应是极端重要的。但公用供电系统不可能提供不间断的高质量电源，因此可靠的解决办法是采用不间断电源（UPS），UPS 不仅保证可靠的连续供电，而且 UPS 输出是绝对稳定，没有瞬变和谐波。

原文化街 26 号一楼机房 UPS 电池为 2019 年采购，具备可再利用性，UPS 主机为 60KW，可用于本期工程 4 楼指挥大厅内设备供电。

新址 1-4 楼设备间承载指挥信息网、电子政务外网、互联网及业务平台设备，需新增一套 UPS 供电系统，用于 1-4 楼设备间设备供电保障。

一、设备间设备供电

设备间设备能耗计算：

应急指挥中心新址设备间主要承载应急指挥信息网设备、政务电子外网设备、互联网设备及相关业务平台设备等，通过对搬迁设备及新建设备的统计，应急指挥信息网设备总功耗约 30kw，电子政务外网设备约 19kw，互联网设备约 18kw，其他接入设备约 1kw，合计约 68kw。按照 UPS 冗余量，以及双路供电考虑，本期项目配置双路共两台 100kw UPS 主机。

根据建设单位需求，电池供电时间不少于 8 小时。设备间设备运行功率按照 45KW 计算，单节电池电压 12V

需要电池安时数=45000W×8h÷12v=30000AH

因此本期配置 12v200ah 电池 160 块，总容量 32000ah，满足建设需求。

二、指挥大厅、总调度室设备供电

指挥大厅需要 UPS 供电设备有 LED 显示大屏、数字会议、无纸化会议、坐席电脑等设备，合计约 47kw。

现有过渡厅在用 1 台 60kw UPS 供电系统可支持新址指挥大厅的设备供电，

在考虑主备双路供电的情况下，再新配一台 60KW UPS 主机。

根据建设单位需求，电池供电时间不少于 8 小时。设备间设备运行功率按照 30KW 计算，单节电池电压 12V

需要电池安时数=30000W×8h÷12v=20000AH

本期利旧电池 12v100ah 共 120 块，其中每组 40 块，因此本期需再配置 12v100ah 电池 2 组共 80 块，总容量 20000ah，满足建设需求。

三、主要技术要求

1. 本项目要求 UPS 具有真正无主从自适应并机功能,无需增加并机柜或并机卡，根据业务发展任意进行在线升级或扩容，满足“边成长、边建设”需求，提供国家相关部门专利证明文件。控制软件需为同厂正版,提供著作权登记证书。

2.输入电压范围（V）：380±25%；输入频率范围（Hz）： 50±10%；输出电压范围（V）：380±1%；输出频率范围（Hz）： 50/60±0.5%；直流电压：348V。需提供检测报告。

3. 负载功率因素（带载能力）≥0.8，过载能力：125％满载时维持 10 分钟，150％满载时维持 1 分钟。

4. 主机输出端内置隔离变压器,彻底解决雷击,零地电压,电网的各种脉动和干忧等电力系统问题,保证负载的安全运行。

5. 支持 SNMP 网络管理协议,通过 SNMP 网络适配器,实现网络管理功能.和自动发送手机短信告警，E-mail 告警功能。

6.工作温度（℃）：0～40；环境湿度：0～95%，无冷凝。

7.绿色节能，符合国家标准 EMC 电磁兼容特性（GB7260.2），降低、避免各类辐射、传导干扰，构建纯净电网环境。

8.冷启动、自启动功能：

在无市电状态下，可直接用电池组启动 UPS，满足应急需求，在电池放电到欠压保护后，市电恢复时可以自动启动 UPS，更具有无人值守功能。

9.UPS 面板的开关机键应具备避免误操作的设计，来实现开关机

10. 具备 LCD 中文液晶显示功能，可记录 1000 条保护动作历史记录。

11.具有以下保护功能设计：

• 可设置输出过载保护点

• 可设定电池告警保护点

• 可设定输入频率同步范围，同步速度及超范围告警点

• 可设定市电输入异常（过高/过低）告警点

12.兼容智能化电池监控管理系统,对电池组实行 24 小时无风险电池在线监测功能。

13. 使用工业级可插拔式模块风机，并采用智能变速方式,风扇依据负载量的大小自动调节转速快慢,以达到节能的效果。

14. 电池柜/箱需与主机统一品牌，具有原厂电池管理系统，可对电池电压、电流、内阻进行实时监测。

3.4.5.4 其他配套系统建设

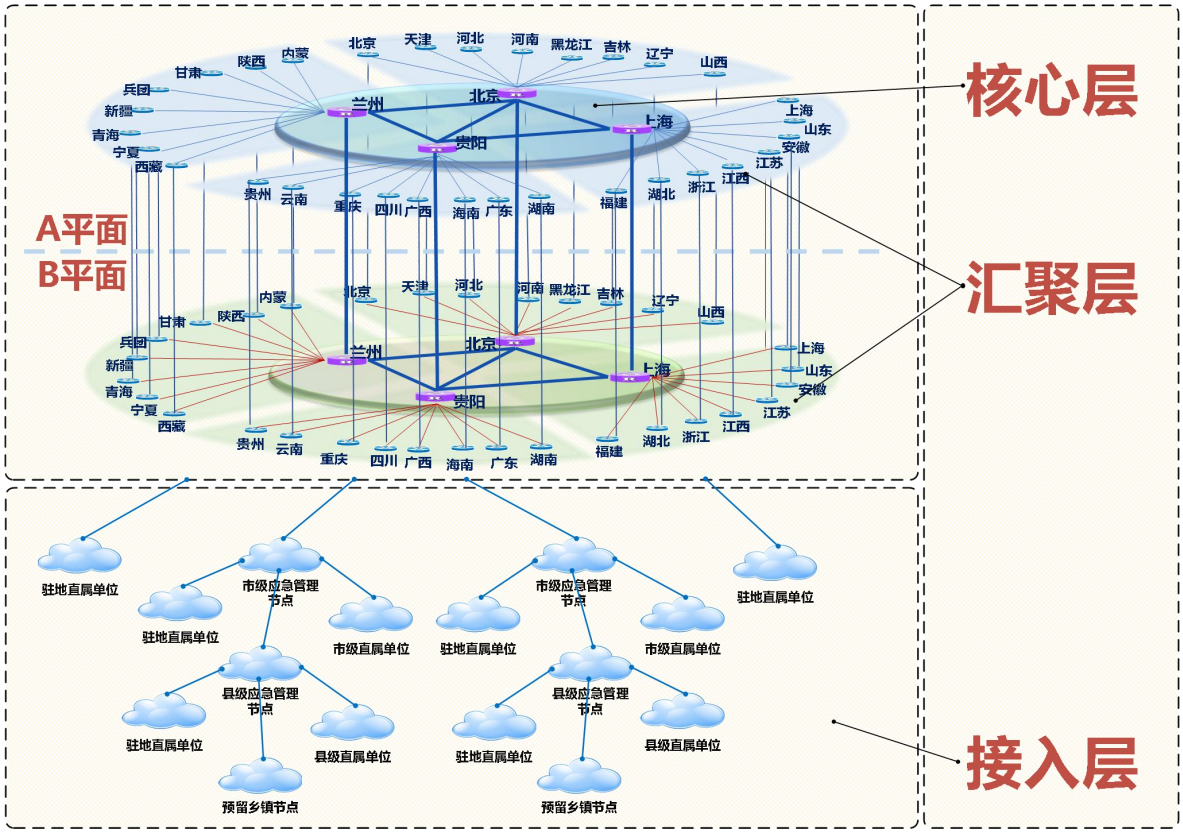
楼宇综合布线、设备间的暖通系统、消防系统、弱电系统、动环监控系统的建设由土建部分弱电专业负责。

五、 网络及安全系统建设

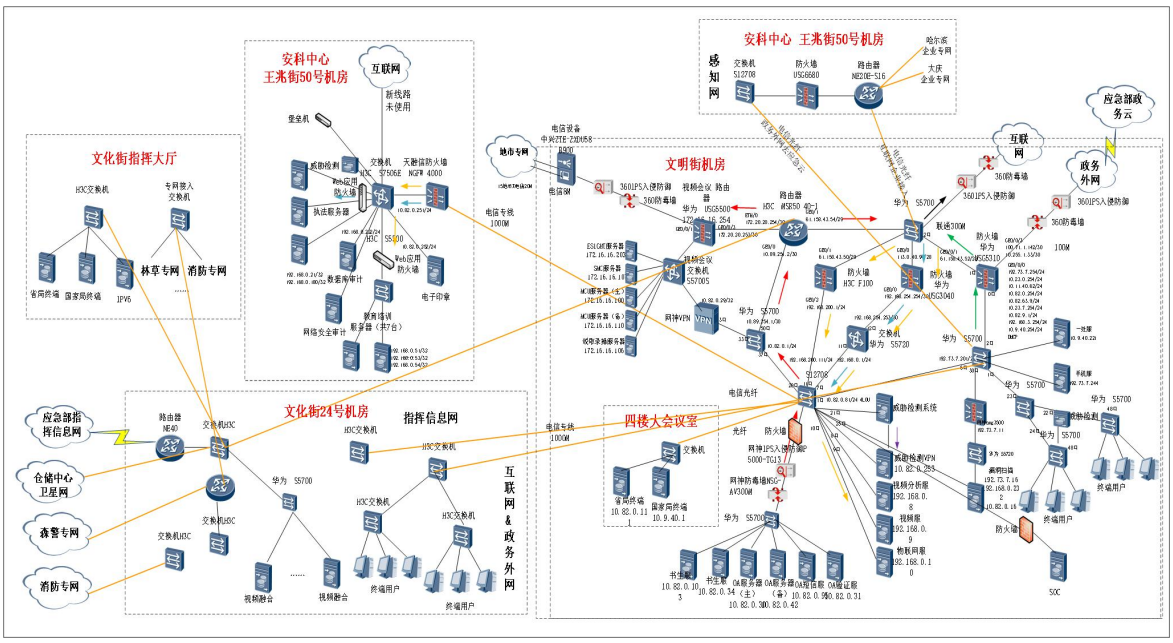
1. 网络现状

目前，我国在安全生产执法与隐患排查治理工作中使用互联网联合指挥调度的网络应用还相对比较薄弱，各地安监部门无法充分整合资源，安全生产业务比较单一，功能较弱。因此，实现省、市、县多级网络安全高效转发，整合各个部门之间的资源，提高创新安全管理水平和提高企业隐患排查治理能力重要方式之一，可实现安全生产的远程、动态、科学监管的有效途径，有力提高事故风险防范能力和增强本质安全水平，有效防范和坚决遏制重特大事故发生。以安全风险分级管控为基础，从源头上对企业安全风险进行辨识，科学评估和分级管控，把各类风险控制在隐患形成之前，以隐患排查治理为手段，及时找出风险管控措施失效或者弱化环节，并有效进行治理，把隐患消除在事故发生之前。

指挥信息网实现部、省、市、县四级应急管理部门立体式全覆盖，为应急管理提供统一高效的网络通信保障。指挥信息网由核心层、汇聚层和接入层组成，采用完全对称的双平面架构，全国网络架构如下图所示：



黑龙江省网的省级核心节点和国家应急骨干网黑龙江落地设备对接，省级网络根据所连接的部门分为应急部分和消防部分。目前黑龙江省应急部分已实现省级节点与地市节点的网络互通，其中应急管理厅已接入应急指挥信息网、政务外网、互联网，整体网络架构如下：



黑龙江省应急管理厅现有网络拓扑图

经过多年信息安全建设已经初步建成较为完善的执法、教育培训和办公 OA 等网络应用系统，为全省应急管理处置与安全宣传提供全面的信息服务，为信息化建设有效开展提供了强有力的支撑，同时，按照应急管理部下发的《应急管理信息化 2019 年第一批地方建设任务书》（应急科信办〔2019〕3 号）的文件要求正在陆续完成网络和应用系统相关体系建设。当前，在信息科技发展的同时，各种黑客手段、病毒技术、木马技术也在飞速发展，信息安全问题在信息化发展的过程中也日益突出，信息系统建设必须面对日益严峻的信息安全问题。目前，现有的信息安全体系功能十分有限，无法预防来自以下几个方面的安全隐患：来自系统软硬件故障造成的服务中止或者数据丢失、来自自然灾害或其他意外事故造成的物理破坏、来自内部或外部的黑客针对网络基础设施、主机系统和应用服务的各种攻击、或者恶意篡改数据、来自有害信息（如病毒等）的传播等。

因此，应遵循各类型系统的保密性、完整性、可用性的原则，做好物理层安全、网络层安全、操作系统安全、内容安全、应用层安全、PKI 体系、安全审计、安全集中管理的建设。在此基础上，同时，做好信息安全管理、技术、运维、知识体系的建设。

按照近期网络安全规划与调整，现有网络主要由互联网、政务外网和指挥信息网三套网络组成，在全网中已进行了检测体系建设（已部署威胁检测系统、漏洞扫描等部分检测设备）、边界防护体系建设（已部署防火墙、入侵防御、防病毒网关和 VPN 等部分设备）、审计体系建设（已部署数据库审计系统、日志审计系统等）和安全管理体系建设（即将上线的安全运营管理平台等），虽然已经完成了上述安全体系建设，但是，随着网络和应用系统不断地增加，业务规模不断地扩大，按照等级保护 2.0 三级的相关标准要求还有一定的差距，需要逐步落实与完善。

2. 需求分析

2018 年 3 月《深化党和国家机构改革方案》通过，正式组建应急管理部，组建应急管理部对防范化解重特大安全风险，健全公共安全体系，整合优化应急力量和资源，推动形成统一指挥、专常兼备、反应灵敏、上下联动、平战结合的中国特色应急管理体制，提高防灾减灾救灾能力，确保人民群众生命财产安全和

社会稳定具有重要意义，其中应急信息的互联互通建设迫在眉睫。

应急管理信息化反战是依托于国家天地一体信息网络重大工程，整合各转隶部门存量通信网络、通信设备、卫星信道等资源，建设“天地一体、全域覆盖、全面融合、全程贯通”的应急通信网络。

3.5.2.1 网络建设需求

（1）指挥信息网

指挥信息网是承载应急管理部核心业务的基础通道，具有高可靠、高稳定、高安全、全覆盖等特点。具备与国家电子政务外网、互联网的安全互联能力。

主要运行应急指挥、大数据分析、视频会议、监测预警等关键应用，面向指挥决策部门、应急救援部门的特定用户。

（2）国家电子政务外网

国家电子政务外网是承载非涉密行政业务的基础通道，具有国家统一建设、免费使用，可跨部门、跨地域信息共享和业务协同等特点。具备经授权访问指挥信息网和互联网的能力。主要运行政务办公和行政执法等应用，面向应急管理全域用户。

（3）互联网

互联网是承载公众服务和监测预警业务的基础通道，具有覆盖面广、传播速度快、互动性强、成本低廉等特点。具备信息获取、信息交换和发布能力。

主要运行信息采集、信息报送、门户网站等应用，面向企事业单位、公众等用户。

根据以上分析，不同的网络承载不同的业务，且面向不同的业务终端。目前网络拓扑结构，省级汇聚层三张网络共用核心交换机，存在网络边界融合，网络层次不清晰，网络安全边界模糊等问题，需对网络架构进行梳理，按照单张网络垂直网络出口层、汇聚层、接入层进行网络层次划分，使网络层次更清晰规范，同时三网络汇聚层两两互联，中间部署安全设备套件，实现数据的跨网安全交换。

3.5.2.2 安全建设需求

目前网络安全建设，已经具备关键基础设施安全防护的措施和手段，但随着新业务系统陆续上线，按照《网络安全法》及等级保护 2.0 等相关法律法规及标准要求还有一定的差距，目前主要安全需求分析如下：

（1）指挥信息网

在指挥信息网第三方接入边界缺少安全访问控制、入侵防御和病毒过滤的措施和手段；

在第三方视频接入线路缺少视频安全防护的措施和手段；

在指挥信息网中缺少对视频安全防护设备进行统一安全管理的措施和手段；

指挥信息办公终端中缺少病毒查杀与过滤的措施和手段；

我厅现网中有安全运营管理平台，原建设已经完成了基础平台建设，本期要求完成三网中分别采集日志与设备性能统一发送至安全运营管理平台中进行统一安全管控及全网态势分析，需要完善增强关联分析、资产建模、基础监控、增强监控、漏洞调度管理、业务管理、历史关联分析和态势感知等功能。为了更好地使用安全运营管理平台各项功能，本项目要求至少提供一名安全工程师驻场服务两年。

由于省厅指挥信息网与十三地市专网带宽升级，原有防毒墙和入侵防御设备无法满足带宽升级需要，因此，在指挥信息网与十三地市网络边界带宽升级后缺少防病毒和入侵防御的措施和手段；

省厅新建视频融合指挥平台，需要接入互联网视频、政务外网视频、第三方专网视频（包括公安等第三方等），目前缺少数据和视频安全接入的强隔离措施和手段；

在指挥信息网与十三地市专网之间访问控制、入侵防御和病毒过滤的措施和手段；

在互联网（办公）的网络中缺少入网终端认证与访问控制的措施和手段；

在政务外网中缺少运维身份鉴别与审计的措施和手段。

（2）国家电子政务外网

按照国家电子政务外网跨网数据交换要求，省厅互联网与政务外网之间缺少针对数据安全交互与安全隔离的强隔离措施和手段；

在省厅互联网和政务外网之间缺少视频安全传输与隔离的措施和手段；

在互联网（办公）的网络中缺少入网终端认证与访问控制的措施和手段；

在政务外网办公区边界缺少访问控制、入侵防御和病毒过滤的措施和手段；

在政务外网中缺少运维身份鉴别与审计的措施和手段。

（3）互联网

在互联网（业务）出口、互联网（业务）服务器区边界及互联网（办公）办公区边界缺少访问控制、入侵防御和病毒过滤的措施和手段；

在互联网（业务）出口边界缺少 DDOS 攻击流量清洗与过滤的措施和手段；

在互联网（办公）的网络中缺少入网终端认证与访问控制的措施和手段；

在互联网（业务）网络中缺少动态行为检测、文件还原、和威胁检测的措施和手段；

按照国家《密码法》要求，在互联网（业务）网络中缺少远程安全运维访问、数据国密算法加密的措施和手段。

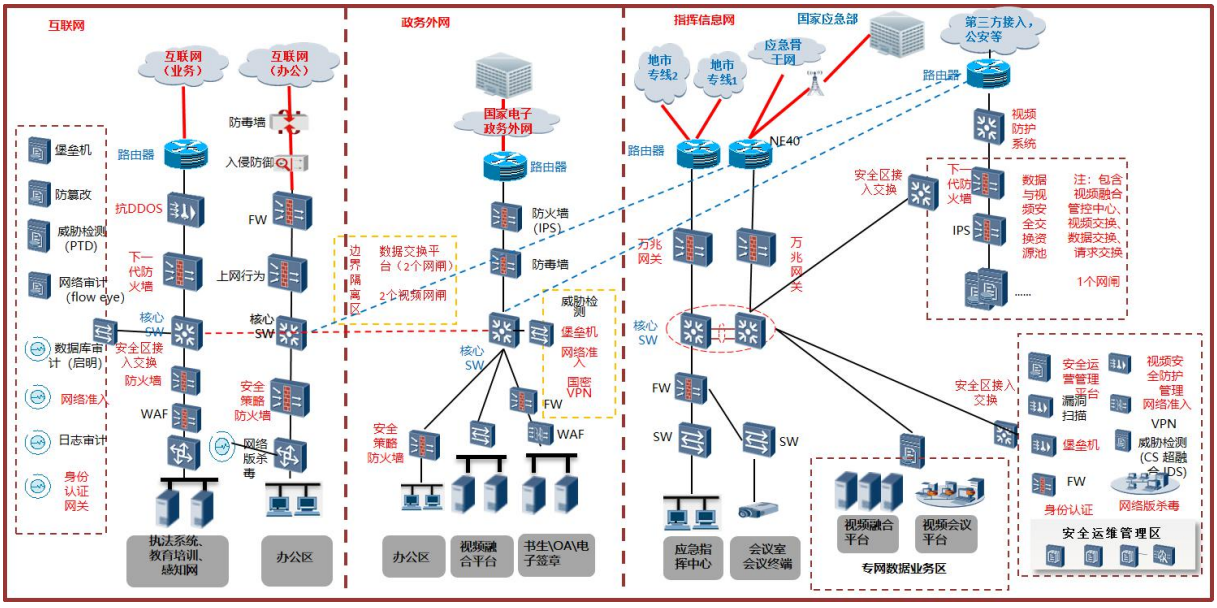
3. 总体方案

省厅现有数据中心机房由王兆街安技中心数据中心机房、省厅文明街数据中心机房和省厅文化街数据中心机房三个机房组成。随着省厅多个新业务陆续上线，业务规模不断扩大，省厅需要对现有数据中心机房进行重新规划。本次网络安全方案设计主要参考了应急管理部整体网络安全规划设计理念，同时，按照国家《网络安全法》和等保 2.0 等法律、法规进行方案顶层设计。

应急管理厅对现有网络进行有效整合。规划后的网络主要由互联网、政务外网和指挥信息网三张网络组成，各网络自成体系，依照出口路由层，核心交换层、接入层，进行分层建设。网络域、安全域、数据业务域，设备域边界清晰。每张网按照《网络安全法》和等保 2.0 的相关要求进行信息安全防护体系建设。按照等保 2.0 的标准要求，规划后的网络将三张网之间进行网络边界的强隔离，实现三网之间数据和视频传输的安全隔离与安全交互要求。建立统一安全管理中心区，通过三张网边界隔离设备，对三张网进行统一的安全运维。

为保证省级与地市级网络的数据通信能力，本期方案将在各地市新增路由器设备，部署在地市网络出口路由层。

总体建设方案效果如下图所示：



4. 网络建设方案

3.5.4.1 建设原则

1、分区分域原则

应急指挥信息网具备与国家电子政务外网、互联网的安全互联能力；主要面向指挥决策部门、应急救援部门的特定建设单位，承载应急指挥、大数据分析、视频会议、监测预警等关键应用。因此需要根据不同网络、不用用途进行分区分域建设，使网络结构与层次清晰健壮。

2、安全可靠原则

应急指挥信息网作为应急通信网络的重要组成部分，是承载应急管理应急救援指挥等关键业务和大容量数据转发的基础通道，具有高可靠、高稳定、高安全等特点。

3、可扩展原则

根据应急管理信息化发展战略规划框架，依托国家天地一体化信息化网络重大工程，整合各转隶部门存量通信网络、通讯设备、卫星信道等资源，建设“天地一体、全域覆盖、全面融合、全程贯通”的应急通信网。

3.5.4.2 建设方案

1、建设思路

将原始拓扑图重新梳理并进行逻辑分区。原采购部分网络设备已经接入现

网，分别替换在安科中心的核心交换机和防火墙及专网核心交换机。同时，部委给省下发一台 NE40E 路由器用作指挥信息网出口，与部委互联，地市/横向单位通过新采购出口路由器与省厅指挥信息网互联。

1、网络分层

（1）将部委下发的 NE40E 路由器（文化街机房）部署在指挥信息网出口。

（2）安科中心单独开通互联网出口，用作后期感知网，前期采购的路由器设备 NE20E-S16 及防火墙设备 USG6680 放在这里，核心交换机暂时与文明街机房互联网出口相连。

（3）指挥信息网新增核心路由器，连接地市专线，按照应急指挥专网建设标准，核心交换机进行双链路冗余。

（4）对接消防部门建立一条独立的专网，连接到指挥信息中心。

（5）指挥信息网、政务外网、互联网新增核心交换机，用于本网内数据转发。核心交换机下挂接入交换机，设接入层，用于终端设备的接入。

（6）按照前面规划思路对现网结构进行优化，对现网设备进行删除或利旧或增补。

2、网络隔离

（1）指挥信息网与办公网进行隔离，办公终端只能通过国家电子政务外网访问应急专网数据。

（2）互联网与政务外网隔离。

（3）指挥信息网与互联网隔离。

（4）对专网、政务外网、互联网进行边界安全防护。

3、业务分区

（1）将 OA 服务器及书生服务器等相关业务系统迁移至电子政务外网。

（2）将视频服务器及物联网服务器等相关业务系统迁移至安科中心。

（3）建立专网数据业务区，主要包括融合指挥平台和视频会议平台。承载的主要业务包括：数据传输，语音通话，视频业务等。

（4）将指挥中心平台及视频会议平台纳管到专网数据中心。

（5）部署安全运维管理区，对整网业务数据进行安全管控。

（6）对安科中心的门户网站进行安全防护。

2、省级汇聚层

配置 3 台省级核心路由器做指挥信息网、电子政务外网和互联网的出口路由器；配置 3 台省级核心交换机做指挥信息网、电子政务外网、互联网核心交换用；

通过省干传输网 GE 链路（带宽 200M）下连至各地市（州）核心路由器；

部署 1 台路由器作为第三方接入路由出口用；

部署 1 台交换机作为视频安全资源池区域数据交换用；

部署 1 台交换机作为安全运维接入区数据交换用；

3.5.4.3 性能指标

1、网络带宽要求

（1）省级网带宽要求

省级驻地单位到省级节点的链路带宽推荐不低于 100Mbps，业务量较大的单位可基于业务量调整。

（2）市级网带宽要求

市级节点接入到省级节点的链路带宽推荐不低于 100Mbps，市级驻地单位接入到市级节点的链路带宽推荐不低于 50Mbps，业务量较大的单位可基于业务量调整。

2、路由器性能要求

（1）省级核心路由器

省级核心层部署 2 台高端路由器,路由器上连冗余资源不少于 50%，以便业务的扩展，设备具备 VLAN 管理、流量控制、访问控制等多种功能，支持 ISIS、OSPF、BGP、MPLS 等多种路由协议，设备还须支持 IPv6、6VPE、SR、SDN 等先进技术。设备在电源、业务板卡、风扇等模块上均具备冗余实现高可用。需具备强大的转发能力（单槽位 2T），预留足够的槽位，以适用未来发展，其他技术参数要求如下：

设备性能	设备性能：支持交换容量≥100Tbps 支持包转发率≥14000Mpps
设备架构	整机业务载板插槽≥8 个（全尺寸业务卡槽位，非子卡槽位）
	带独立交换网板并满配，交换网板总数≥4
	要求设备双主控、双风扇槽位冗余、电源冗余满配置，支持机箱内双主控热备，要求所有业务板卡及电源、风扇模块均可热插拔
	设备散热方式采用前后风道散热方式
路由能力	支持 RIP、OSPF、IS-IS、BGP 等路由协议

	支持 BGP 协议扩展：BGP ADD-Path(BGP Additional Paths)、BMP 和 BGP Best-external 增强功能
	支持并实配 MPLS，MPLS VPN，支持 PIM-SM、IGMP、MBGP、MSDP、MPLS VPN、NG-MVPN 组播协议
	要求设备具备对 VPN 路由的按需管理和控制能力
	支持 VPN ORF（VPN 路由策略），以满足客户对 VPN 路由的按需控制
	支持 VPN 业务保证功能，以满足客户对 VPN 业务的区分管理和控制
	具备快路由收敛性能，以满足应急网络要求
	具备快速 IGP 路由收敛能力，例如 ISIS 路由收敛时间，正切＜300ms，回切不丢包
	具备快速 BGP 收敛能力，正切＜250ms，回切不丢包
	具备快速 IBGP 快速收敛能力，正切≤250ms，回切不丢包
	IPV6 线速转发不丢包，满足国家 ipv6 网络改造要求
	支持按需灵活配置的低时延、低抖动以太场景类 SDH 的 IP 硬管道业务保障能力技术，保障业务带宽
	支持 5 级 H-QoS 调度
高可靠性	具备业界领先的快速故障检测及重路由技术，以保证网元设备或者链路故障时，视频会议等敏感业务的稳定运行 支持硬件 BFD，5ms 发包频率，15ms 故障检测能力 支持单臂 BFD（BFD echo）功能，以解决对端设备不支持 BFD 功能时，部署 BFD 快速检测提高现网可靠性的能力 支持误码倒换功能，以解决传统 BFD 检测技术无法识别由光路抖动、线路老化等原因导致的概率性误码
	支持 FRR 功能：IP/LDP/TE/VPN FRR(提供国际权威或者国家 CMA&CNAS 测试机制提供的第三方测试报告证明)
	支持 IPV6 协议的 FRR 功能，以满足国家 IPV6 改造需要
	IPv6 FRR/VPNv6 FRR，其中 OSPFv3 FRR 收敛时间≤35ms，ISISv6 FRR 收敛时间≤35ms，BGP4+ FRR 收敛时间≤30ms，VPNv6 FRR 收敛时间≤35ms
	支持 RLFA（remote-LFA）技术，以解决 LDP FRR 无法生效的场景
	支持 LDP,VRRP,OSPF,ISIS,BGP,L3VPN,MPLS TE,PIM 的 NSR（不中断路由技术），主备倒换不丢包。
	支持 OSPFv3，ISISv6，BGP4+和 IPV6 VRRP 的 NSR（不中断路由技术），主备倒换不丢包，以满足国家 IPV6 改造需要。
可维护性	支持丰富的网络质量检测技术，包括 支持 ETH OAM 技术，包括 EFM、CFM、Y.1731 支持 MPLS-TP OAM 功能
SDN	支持广域网智能调优
	支持 VXLAN、EVPN、Segment Routing 和 openflow 等 SDN 相关技术
	支持 GMPLS 功能，实现 IP+光的 SDN 场景，充分利用数通和传输资源对用户网络进行智能化应用
安全	支持 CPU 防攻-溯源，可记录攻击报告部分详细字段，有效帮助用户快速定位和解决安全问题
	支持国密算法 IPSec IKE

	支持 IPV6 防攻击
接口类型	设备支持 100GE/40GE/10GE/GE/FE、155M POS，622M POS，155M CPOS，2.5G POS，E1/CE1 等接口模块。
系统管理	支持 Console、Telnet、SSH、SNMP 等管理方式
	支持 Netconf，可以提供配置 API
	支持配置回滚和配置试运行功能，提供智能化维护管理体验
其他	提供工信部入网链接及入网测试报告
	提供工信部抗震检验报告并满足 9 级烈度的抗震等级

3、其他性能要求

各级网络相关链路技术指标和设备指标推荐如下。

序号	类别	功能描述
1	网络链路	链路通道 ES（误码秒数）≤6 个/2 小时。 链路通道 SES（严重误码秒数）≤6 个/2 小时。 IP 包丢包率≤1%。
2	省级节点路由器	用于省级应急管理部门、消防总队、省级地震局等。 设备双主控、独立交换网板、支持双主控热备，支持 IPv6。 性能：交换容量≥110Tbps、包转发率≥24000Mpps。
3	省级节点交换机	用于省级应急管理部门、消防总队、省级地震局等。 设备双主控、冗余独立交换网板、支持业务卡堆叠和扩展，支持 IPv6。 性能：交换容量≥100Tbps，包转发率≥40000Mpps。
4	市级节点路由器	用于市级应急管理部门、消防支队、森林消防支队、市级地震局。 设备双主控、独立交换网板、冗余风扇、冗余电源，支持机箱内双主控热备，支持 IPv6。 性能：交换容量≥70Tbps、包转发率≥24000Mpps。

5. 安全建设方案

3.5.5.1 建设原则

1、分区分域防护原则

任何安全措施都不是绝对安全可靠的，为保障攻破一层或一类保护的攻击行为而不会破坏整个信息系统，以达到纵深防御的安全目标，需要合理划分安全域，综合采用多种有效安全保护措施，实施多层、多重保护。

2、均衡性保护原则

对任何类型网络，绝对安全难以达到，也不一定是必须的，需正确处理安全需求、安全风险与安全保护代价的关系。因此，结合适度防护实现分等级安全保护，做到安全性与可用性平衡，达到技术上可实现、经济上可执行。

3、技术与管理相结合

信息安全涉及人、技术、操作等方面要素，单靠技术或单靠管理都不可能实现。因此在考虑信息安全时，必须将各种安全技术与运行管理机制、人员思想教育、技术培训、安全规章制度建设相结合。

4、动态调整与可扩展

由于网络安全需求会不断变化，以及环境、条件、时间的限制，安全防护一步到位，一劳永逸地解决信息安全问题是不现实的。信息安全保障建设可先保证基本的、必须的安全保护，后续再根据应用和网络安全技术的发展，不断调整安全策略，加强安全防护力度，以适应新的网络安全环境，满足新的信息安全需求。

5、网络安全三同步

信息系统在新建、改建、扩建时应当同步建设信息安全设施，确保其具有支持业务稳定、持续运行性能的同时，保证安全技术措施同步规划、同步建设、同步使用，以保障信息安全与信息化建设相适应。

3.5.5.2 需求分析

我厅经过多年的网络安全建设，已经具备关键基础设施安全防护的措施和手段，但随着我厅新业务系统陆续上线，我厅按照《网络安全法》及等级保护 2.0 等相关法律法规及标准要求还有一定的差距，目前，我厅主要安全需求分析如下：

一、安全技术需求

1、安全物理环境需求

物理和环境安全主要影响因素包括机房环境、机柜、电源、服务器、网络设备和其他设备的物理环境。该层面为基础设施和业务应用系统提供了一个生成、处理、存储和传输数据的物理环境。具体安全需求如下：

由于机房容易遭受雷击、地震和台风等自然灾难威胁，需要通过对物理位置进行选择，及采取防雷击措施等来解决雷击、地震和台风等威胁带来的问题；

由于机房容易遭受水患和火灾等灾害威胁，需要采取防水、防潮、防火措施来解决水患和火灾等威胁带来的安全威胁；

由于机房容易遭受高温、低温、多雨等原因引起温度、湿度异常，应采取温湿度控制措施来解决因高温、低温和多雨带来的安全威胁；

由于机房电压波动影响，需要合理设计电力供应系统来解决因电压波动带来

的安全威胁；

针对机房供电系统故障，需要合理设计电力供应系统，如：购买 UPS 系统、建立发电机机房，铺设双电力供电电缆来保障电力的供应，来解决因供电系统故障带来的安全威胁；

针对机房容易遭受静电、设备寄生耦合干扰和外界电磁干扰，需要采取防静电和电磁防护措施来解决静电、设备寄生耦合干扰和外界电磁干扰带来的安全威胁；

针对机房容易遭受强电磁场、强震动源、强噪声源等污染，需要通过对物理位置的选择、采取适当的电磁防护措施，来解决强电磁场、强震动源、强噪声源等污染带来的安全隐患；

针对利用非法手段进入机房内部盗窃、破坏等安全威胁，需要通过进行环境管理、采取物理访问控制策略、实施防盗窃和防破坏等控制措施，来解决非法手段进入机房内部盗窃、破坏等带来的安全问题；

针对利用工具捕捉电磁泄漏的信号，导致信息泄露的安全威胁，需要通过采取防电磁措施，来解决电磁泄漏带来的安全问题。

2、安全通信网络需求

通信网络是对定级系统安全计算环境之间进行信息传输及实施安全策略的安全部件。是利用网络设备、安全设备、服务器、通信线路以及接入链路等设备或部件共同建成的、可以用于在本地或远程传输数据的网络环境。具体安全需求如下：

针对网络架构设计不合理而影响业务通信或传输问题，需要通过优化设计、安全域改造完成。

针对利用通用安全协议、算法、软件等缺陷获取信息或破坏通信完整性和保密性，需要通过数据加密技术、数据校验技术来保障。

针对内部人员未授权违规连接外部网络，或者外部人员未经许可随意接入内部网络而引发的安全风险，以及因使用无线网络传输的移动终端而带来的安全接入风险等问题，需要通过违规外联、安全准入控制以及无线安全控制措施来解决。

针对通过分布式拒绝服务攻击恶意地消耗网络、操作系统和应用系统资源，导致拒绝服务或服务停止的安全风险，需要通过抗 DDoS 攻击防护、服务器主机

资源优化、入侵检测与防范、网络结构调整与优化等手段来解决。

针对攻击者越权访问文件、数据或其他资源，需要通过访问控制、身份鉴别等技术来解决。

针对利用网络协议、操作系统或应用系统存在的漏洞进行恶意攻击（如碎片重组，协议端口重定位等），需通过网络入侵检测、恶意代码防范等技术措施来解决。

针对利用网络结构设计缺陷旁路安全策略，未授权访问网络，需通过访问控制、身份鉴别、网络结构优化和调整等综合方法解决。

针对众多网络设备、安全设备、通信线路等基础设施环境不能有效、统一监测、分析，以及集中安全策略分发、漏洞补丁升级等安全管理问题，需要通过集中安全管控机制来解决。

3、安全区域边界需求

区域边界包括安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件，区域边界安全即各网络安全域边界和网络关键节点可能存在的安全风险。需要把可能的安全风险控制在相对独立的区域内，避免安全风险的大规模扩散。

各类网络设备、服务器、管理终端和其他办公设备系统层的安全风险。主要涵盖两个方面，一是来自系统本身的脆弱性风险；另一个是来自用户登录帐号、权限等系统使用、配置和管理等风险。具体如下：

针对用户帐号权限设置不合理、帐号暴力破解等等安全风险，需要通过帐号管理、身份鉴别、访问控制等技术手段解决。

针对在网页浏览、文档传递、介质拷贝或文件下载、邮件收发时而遭受恶意代码攻击的安全风险，需通过恶意代码防范技术手段解决。

针对操作用户对系统错误配置或更改而引起的安全风险，需通过安全配置核查、终端安全管控等技术手段解决。

针对设备系统自身安全漏洞而引起被攻击利用的安全风险，需要通过漏洞扫描技术、安全加固服务等手段解决。

针对通过恶意代码或木马程序对主机、网络设备或应用系统进行攻击的安全威胁，需通过恶意代码防护、入侵检测、身份鉴别、访问控制、安全审计等技术

手段解决。

4、安全计算环境需求

计算环境安全涉及业务应用系统及重要数据处理、存储的安全问题。具体安全需求如下：

针对利用各种工具获取应用系统身份鉴别数据，进行分析获得鉴别内容，从而未授权访问、使用应用软件、文件和数据的安全风险，需要采用两种或两种以上鉴别方式来，可通过应用系统开发或第三方辅助系统来保证对应用系统登录鉴别安全；

针对应用系统缺陷、接口设计等导致被恶意攻击利用、数据丢失或运行中断而影响服务连续性的安全风险，需要通过对产品采购、自行软件开发、外包软件和测试验收进行流程管理，同时保证应用软件具备自我容错能力；

针对应用系统过度使用内存、CPU 等系统资源，需要对应用软件进行实时的监控管理，同时对系统资源进行管控来解决；

针对由于应用系统存储数据而引发的数据损毁、丢失等数据安全问题，需通过本地数据备份和异地容灾备份等手段来解决；

针对通过伪造信息进行应用系统数据的窃取风险，需要加强网络边界完整性检查，加强对网络设备进行防护、对访问网络的用户身份进行鉴别，加强数据保密性来解决。

5、安全管理中心需求

安全管理中心能够对网络设备、网络链路、主机系统资源和运行状态进行监测和管理，实现网络链路、服务器、路由交换设备、业务应用系统的监控与配置。

安全管理平台对安全设备、网络设备和服务器等系统的运行状况、安全事件、安全策略进行集中监测采集、日志范式化和过滤归并处理，来实现对网络中各类安全事件的识别、关联分析和预警通报。

针对内部管理员的违规操作行为，需要采取身份鉴别、安全审计等技术手段对其操作行为进行限定，并对其相关操作进行审计记录。

针对众多网络设备、安全设备、通信线路等基础设施环境不能有效、统一监测、分析，以及集中安全策略分发、恶意代码特征库、漏洞补丁升级等安全管理问题，需要通过集中安全管控和集中监测审计机制来解决。

针对应用系统过度使用服务器内存、CPU 等系统资源的行为，需要对应用软件进行实时的监控管理，同时对系统资源进行管控来解决。

二、安全管理需求

1、安全管理制度需求

安全策略和管理制度涉及安全方针、总体安全策略、安全管理制度、审批流程管理和安全检查管理等方面。其安全需求如下：

需要制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

需要建立安全管理制度，对管理活动进行制度化管理，制定相应的制定和发布制度；

需要对安全管理制度进行评审和修订，不断完善、健全安全制度；

需要建立相应的审批部门，进行相关工作的审批和授权；

需要建立协调机制，就信息安全相关的业务进行协调处理；

需要建立审核和检查部门，安全人员定期的进行全面的安全检查；

需要建立恰当的联络渠道，进行沟通和合作，进行事件的有效处理；

需要建立审核和检查的制度，对安全策略的正确性和安全措施的合理性进行审核和检查；

需要建立备案管理制度，对系统的定级进行备案；

需要建立产品采购，系统测试和验收制度，确保安全产品的可信度和产品质量；

2、安全管理机构需求

安全管理机构涉及安全部门设置、人员岗位设置、人员安全管理等方面。其安全需求如下：

需要建立专门安全职能部门，设置安全管理岗位，配备安全管理人员、网络管理人员、系统管理人员；

需要对人员的录用进行必要的管理，确保人员录用的安全；

需要对人员离岗进行有效的管理，确保人员离岗不会带来安全问题；

需要对人员考核进行严格的管理，提高人员安全技能和安全意识；

需要对人员进行安全意识的教育和培训，提高人员的安全意识；

需要对第三方人员进行严格控制，确保第三方人员访问的安全。

3、安全人员管理需求

安全人员管理需求，涉及到人员的岗位设置、职责分工、人员管理等方面，其安全需求如下：

需要对人员的录用进行必要的管理，确保人员录用的安全；

需要对人员离岗进行有效的管理，确保人员离岗不会带来安全问题；

需要对人员考核进行严格的管理，提高人员安全技能和安全意识；

需要对人员进行安全意识的教育和培训，提高人员的安全意识；

需要对外部人员进行严格控制，确保外部人员访问受控区域或接入网络时可控可管，并签署保密协议。

4、安全建设管理需求

安全建设管理涉及定级备案管理、安全方案设计、产品采购和使用、软件开发管理、安全集成建设、测试验收交付、等级测评以及服务商选择等方面。其安全需求如下：

需要建立备案管理制度，对系统的定级进行备案；

需要具有总体安全方案设计、方案评审的流程和管理能力；

产品采购符合国家有关规定，密码算法和密钥的使用需符合国家密码管理的规定；

需要有专人对工程实施过程进行管理，依据工程实施方案确保安全功能的落地，实施过程需要有第三方工程监理来共同控制实施质量；

需要制定软件开发的相关制度和代码编写规范，并对源代码的安全性进行检测；

需要建立产品采购，系统测试和验收制度，确保安全产品的可信度和产品质量；

需要与符合国家的有关规定的服务供应商签订协议

需要定期组织开展等级测评并及时整改；

需要在工程实施过程中做好文档管理工作，并在系统交付时提供完整的资料交付清单，对运维人员进行技能培训。

5、安全运维管理需求

安全运维管理涉及机房运行管理、资产管理、系统安全运行维护管理等方面。其安全需求如下：

需要保证机房具有良好的运行环境；

需要对信息资产进行分类标识、分级管理；

需要对各种软硬件设备的选型、采购、使用和保管等过程进行控制；

需要各种网络设备、服务器正确使用和维护；

需要对网络、操作系统、数据库系统和应用系统进行安全管理；

需要定期地对通信线路进行检查和维护；

需要硬件设备、存储介质存放环境安全，对其使用进行控制和保护；

需要对支撑设施、硬件设备、存储介质进行日常维护和管理；

需要对系统使用手册、维护指南等工具文档进行管理；

需要在事件发生后能采取积极、有效的应急策略和措施。

制定系统安全运维管理制度，指导系统日常安全运维管理、应急响应管理和外包运维管理活动

综上所述，我厅按照国家《网络安全法》和等保 2.0 的法律法规及标准要求，我厅还需要从安全管理和安全技术两方面逐步落实与完善信息安全体系建设。可以根据我厅网络实际安全现状实行分批分阶段建设。

3.5.5.3 建设方案

1、建设思路

参考等级保护三级安全设计要求，本方案的设计思路如下：

根据信息系统的安全定级结果，明确该等级对应的总体防护描述；

根据系统和子系统划分结果、安全定级结果将保护对象归类，并组成保护对象框架；

根据方案的设计目标来建立整体保障框架，来指导整个等级保护方案的设计，明确关键的安全要素、流程及相互关系；在安全措施框架细化后将补充到整体保障框架中；

根据此等级受到的威胁对应出该等级的保护要求（即需求分析），并分布到物理和环境、网络和通信、设备与计算、应用和数据等层面上；

根据由威胁引出的等级保护基本要求、等级保护实施过程、整体保障框架来

确定总体安全策略（即总体安全目标），再根据等级保护的要求将总体安全策略细分为不同的具体策略（即具体安全目标），包括安全域内部、安全域边界和安全域互联策略；

根据保护对象框架、等级化安全措施要求、安全措施的成本来选择和调整安全措施；根据安全技术体系和安全管理体系的划分，各安全措施共同组成了安全措施框架；

各保护对象根据系统功能特性、安全价值以及面临威胁的相似性来进行安全区域的划分；各安全区域将保护对象框架划分成不同部分，即各安全措施发生作用的保护对象集合。

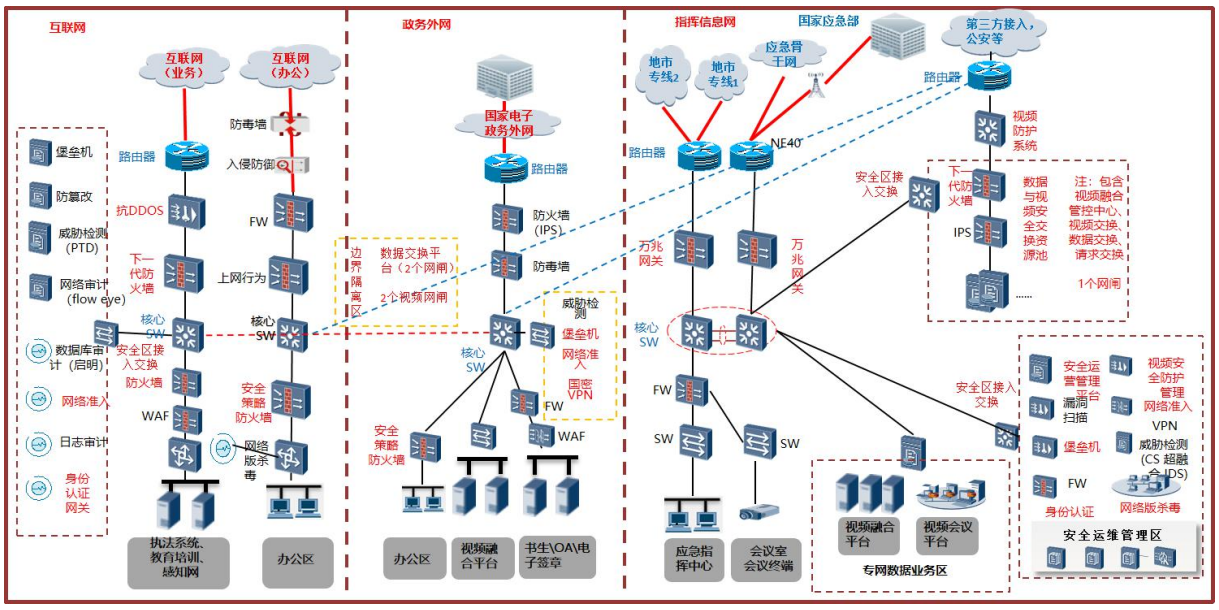
根据选择好的各保护对象安全措施、安全措施框架、实际的具体需求来设计安全解决方案。

省厅现有数据中心机房由王兆街安技中心数据中心机房、省厅文明街数据中心机房和省厅文化街数据中心机房三个机房组成。随着省厅多个新业务陆续上线，业务规模不断扩大，省厅需要对现有数据中心机房进行重新规划。本次网络安全方案设计主要参考了应急管理部整体网络安全规划设计理念，同时，按照国家《网络安全法》和等保 2.0 等法律、法规进行方案顶层设计。

省厅将新建数据中心机房，同时，省厅需要对现有网络进行有效整合。省厅规划后的网络主要由互联网、政务外网和指挥信息网三张网络组成。每张网按照《网络安全法》和等保 2.0 的相关要求进行信息安全防护体系建设。按照等保 2.0 的标准要求，规划后的网络将三张网之间进行网络边界的强隔离，通过两套边界隔离区，实现三网之间数据和视频传输的安全隔离与安全交互要求，其中，第三方专网也通过两套边界隔离区的一套完成数据与视频安全交换。省厅将建立统一安全管理中心区，通过三张网边界隔离设备，对三张网进行统一的网络安全运维，并分屏进行可视化呈现，实现可视化安全运维要求。

另外，参考应急管理部终端方案设计理念，省厅本次方案设计将进行三网一终端设计，实现一个终端通过安全访问控制措施同时访问三张网络的需求。

对优化后的网络进行安全加固，安全加固后的网络符合等级保护三级的安全要求，拓扑图如下：



2、互联网加固建设

1）下一代防火墙

在互联网（业务）出口、互联网（业务）服务器区边界及互联网（办公）办公区边界分别部署下一代防火墙，实现网络边界进出数据的访问控制、入侵阻断和病毒过滤等功能。下一代防火墙可以实现七元组访问控制：以源地址、目的地址、源端口（源安全域）、目的端口（目的安全域）、服务类型、APP 类型及用户为参数的访问许可控制；七元组会话控制：以源地址、目的地址、源端口（源安全域）、服务类型、APP 类型及用户为参数的会话控制；应用行为控制：深入 APP 或各类网络协议的细节参数，实现精细的网络行为管理和日志记录；带宽及 QoS 控制：以源地址、目的地址、服务类型、APP 类型及用户为参数的多层管道嵌套式流量及 QoS 控制。

2）抗 DDOS 设备

在互联网（业务）出口边界部署一台抗 DDOS 设备，实现针对互联网应用系统 DDOS 攻击流量清洗与过滤，保障我厅互联网应用对外发布的安全性与稳定性。支持针对学习周期自定义；支持学习结果自动/手动方式配置防护规则；支持包括但不限于：IP Fragment Flood、ICMP FLOOD、UDP FLOOD、UDP 碎片防护、TCP SYN FLOOD、TCP ACK FLOOD、TCP RST FLOOD、TCP FIN FLOOD、慢速连接耗尽等网络层清洗；支持 HTTP 协议的防护，包括但不限于：HTTP GET FLOOD、HTTP POST FLOOD、HTTP 代理攻击，最少支持 4 种认证算法，包括：重定向、js 重定向、表

单重定向、验证码等；支持基于 IP、TCP、UDP、ICMP、HTTP、HTTPS、DNS、SIP 、NTP、OTHER 等协议的自定义报文特征过滤。

3）网络准入控制系统

在互联网（办公）的网络中部署一台网络准入控制系统，实现能够在不改变网络结构的情况下，对各种复杂网络实现准入控制，在实现准入控制基础上，通过边界探测技术，对全网的网络边界各接入点实现自动探测和防护，加强了网络可视性和可控性。系统内置了 Radius 服务、DHCP 服务、SNMP 服务、Web 服务，从用户、终端、网络、业务四个维度着手进行规范化管理，构建内网规范管理体系，严格审核入网对象的合法性、合规性，同时，我厅可根据定制的管理策略，对于不同的对象采取相应的处理手段，对网络中的用户、终端、网络、应用进行全方位的管控。

4）身份认证网关

在我厅互联网安全管理中心区部署一台身份认证系统，实现登录我厅互联网办公终端访问我厅互联网应用系统的身份鉴别，只有合法获取数字证书的办公终端才允许访问互联网应用系统。系统可以自动更新黑名单、动态更新，不需要重新启动服务；支持 LDAP、HTTP 等多种方式更新；支持 B64、DER 等多种格式。具有快速检索海量数字证书黑名单的功能。系统可以拥有多个站点证书，不同的服务可以拥有不同的站点证书。支持一个 SSL 服务中可同时配置多条证书链，验证不同 CA 的用户证书；支持多种证书支持功能：支持 CFCA、SHECA 及多数省级 CA 中心数字证书。系统可以将用户证书信息包括扩展项信息传送给应用系统。

3、国家电子政务外网加固建设

1）数据交换平台

按照国家《GW0205-2014 国家电子政务外网跨区域的安全数据交换技术要求与实施指南》的标准要求，在互联网与政务外网以及互联网与指挥信息网之间分别设计一套数据交换平台来实现两网之间数据安全交换与隔离访问的需求。支持共享、客户端、FTP、NFS 等多种模式的文件交换服务；实现过滤规则的标准化处理，验证访问控制的有效性，并给出合理的访问控制列表，列表可直接引用；支持平面文件装载到关系型数据库中；支持主流关系型数据库数据交换：Oracle、DB2、SQL Server、GreenPlum、Sybase、MYSQL、Postgresql 的各种版本，及支

持达梦、Gbase、神舟通用、人大金仓等国产数据库，及支持 Cassandra、UDB 等大数据数据库；支持通过解析数据库日志文件的技术原理，在不同类型的数据库之间进行数据同步。无需在数据库中创建触发器、存储过程、临时表等对象，实现低干扰的数据采集。

2）网闸

在省厅互联网和政务外网之间部署 2 台网闸，实现两网之间视频传输的安全隔离与访问等功能。网闸主要由内网主机系统、外网主机系统和隔离交换矩阵三部分构成。内网主机系统与内网相连，外网主机系统与外网相连，内/外网主机系统分别负责内外网信息的获取和协议分析，隔离交换矩阵根据安全策略完成信息的安全检测，内外网络之间的安全交换。支持多网络隔离的体系结构，通过专用硬件完成两侧信息的“摆渡”。支持被隔离网络之间任何时刻不产生物理连接。支持内/外网主机系统之间没有网络协议逻辑连接，通过隔离交换矩阵的全部是应用层数据，也就是 OSI 模型的七层协议全部断开。支持数据交换方式完全私有，不具备可编程性。支持 SQL Server、Oracle、DB2、Sybase 多种大型数据库同步。支持达梦，人大金仓，博阳等国产数据库。支持“多对一”、“一对多”等多网接入功能。支持 NFS、SMBFS、SAMBA、FTP 等文件系统文件安全交换，支持跨系统平台文件同步。

3）安全策略防火墙

在政务外网办公区边界部署一台安全策略控制防火墙，实现网络边界进出数据的访问控制、入侵阻断和病毒过滤等功能。防火墙可以实现七元组访问控制：以源地址、目的地址、源端口（源安全域）、目的端口（目的安全域）、服务类型、APP 类型及用户为参数的访问许可控制；七元组会话控制：以源地址、目的地址、源端口（源安全域）、服务类型、APP 类型及用户为参数的会话控制；应用行为控制：深入 APP 或各类网络协议的细节参数，实现精细的网络行为管理和日志记录；带宽及 QoS 控制：以源地址、目的地址、服务类型、APP 类型及用户为参数的多层管道嵌套式流量及 QoS 控制。

4）堡垒机

在我厅政务外网安全管理中心区部署一台堡垒机设备，实现运维人员通过堡垒机制定严格的特权帐号权限划分与访问认证功能，防止核心数据泄露，并进行

威胁追踪。运维人员通过堡垒机单点登录运维，不必记录设备的 IP 地址、用户名、口令等信息，也避免这些敏感信息的泄露，极大地方便了运维工作，提升运维效率。运维审计系统（堡垒机）对整个运维过程从事前预防、事中控制和事后审计进行全程参与。事前预防：建立“自然人-资源-资源帐号”关系，实现统一认证和授权。事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制。事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定。

5）网络准入控制系统

在政务外网网络中部署一台网络准入控制系统，实现能够在不改变网络结构的情况下，对各种复杂网络实现准入控制，在实现准入控制基础上，通过边界探测技术，对全网的网络边界各接入点实现自动探测和防护，加强了网络可视性和可控性。系统内置了 Radius 服务、DHCP 服务、SNMP 服务、Web 服务，从用户、终端、网络、业务四个维度着手进行规范化管理，构建内网规范管理体系，严格审核入网对象的合法性、合规性，同时，我厅可根据定制的管理策略，对于不同的对象采取相应的处理手段，对网络中的用户、终端、网络、应用进行全方位的管控。

6）国密 VPN

国密 VPN 是集 IPsec、SSLVPN、VPDN 于一身，兼具用户认证、访问控制、传输加密众多功能的综合性 VPN 安全网关，具有安全性高、稳定强、易用强、兼容好、性能高的特点。通过部署 VPN 安全网关构建我厅统一的远程办公安全接入环境，可以统一管理远程用户接入的身份认证、访问权限，实现远程用户在任何时间、任何地点、使用任何终端安全、快速的接入我厅内部业务系统。

4、指挥信息网加固建设

1）下一代防火墙

在指挥信息网第三方接入边界部署一台下一代防火墙，实现网络边界进出数据的访问控制、入侵阻断和病毒过滤等功能。下一代防火墙可以实现七元组访问控制：以源地址、目的地址、源端口（源安全域）、目的端口（目的安全域）、服务类型、APP 类型及用户为参数的访问许可控制；七元组会话控制：以源地址、目的地址、源端口（源安全域）、服务类型、APP 类型及用户为参数的会话控制；应用行为控制：深入 APP 或各类网络协议的细节参数，实现精细的网络行为管理

和日志记录；带宽及 QoS 控制：以源地址、目的地址、服务类型、APP 类型及用户为参数的多层管道嵌套式流量及 QoS 控制。

2）视频安全防护系统

在第三方视频接入线路部署一台视频安全防护系统，实现对视频连接状态监控、视频攻击检测与阻断等功能，保证视频传输的安全性。.支持与在线 GIS 地图的对接，可在地图上展示资产的各种状态，包括在线、离线、非法占用等正常/异常状态；支持集中管理中心，可集中展现视频监控终端和链路质量情况，并支持拓扑展示，通过不同线条和颜色区分链路质量情况；支持视频链路质量监控，针对视频通信线路进行自动化质量探测，帮助管理员及时发现线路异常情况并处理；支持弱口令检测功能，需支持多种网络协议并支持 6 种弱口令检测元素，并支持修改 IPC 设备登录密码，支持逐个/批量改密；能够对视频情报进行收集、分析、分发与整合，对突发热点事件进行监测与告警，自动生成安全运营脚本，实现用例分析、威胁评估与态势预测。

3）视频安全防护管理平台

在指挥信息网中部署一台视频安全防护管理平台，实现省厅所有视频安全防护系统的集中管理、集中监控与集中策略下发等功能，满足等保 2.0 集中管控的标准要求。可对各引擎上报上来的资产状态集中监控，监控内容包括：摄像头状态及详情、非法终端设备详情、唯一性检查详情、脆弱口令详情、异常流量详情。支持安全日志的汇总和查询，并基于威胁等级进行排序，包括：优先级、安全威胁的详细名称、分类和采取的处置措施。支持引擎设备配置回滚功能，集中管理中心通过手动及自动两种方式备份配置文件，并可以选择可回滚的版本。集中管理中心可和第三方管理平台对接，并支持安全事件日志转发功能，可调整日志发送内容的格式。

4）网络版杀毒

在指挥信息网部署一台网络版杀毒软件，实现指挥信息网办公终端的查杀与过滤。可以实现对系统进行实时监控，感知文件存储以及进程启动，并自动检测存储文件以及进程源文件安全性，同时还可以对网络端口进行监控，并提供 STIG 规则检测；针对不能修复的已知漏洞，能够提供虚拟补丁防护策略，在不重启、不更新补丁的情况下让系统具有对指定漏洞的防御能力；可以检测终端访问

URL，自动拦截对恶意 URL 的访问，针对浏览器下载到任务目录的文件主动进行扫描，可禁止端口使用、设置允许访问的 IP 地址和进行网络访问的进程。

5）万兆安全网关

在指挥信息网与十三地市专网之间以及指挥信息网与应急管理部指挥信息网之间分别部署一台万兆安全网关，实现访问控制、入侵行为阻断、病毒过滤和上网行为审计等功能。万兆安全网关可以实现七元组访问控制：以源地址、目的地址、源端口（源安全域）、目的端口（目的安全域）、服务类型、APP 类型及用户为参数的访问许可控制；七元组会话控制：以源地址、目的地址、源端口（源安全域）、服务类型、APP 类型及用户为参数的会话控制；应用行为控制：深入 APP 或各类网络协议的细节参数，实现精细的网络行为管理和日志记录；带宽及 QoS 控制：以源地址、目的地址、服务类型、APP 类型及用户为参数的多层管道嵌套式流量及 QoS 控制。

6）数据与视频安全交换资源池

数据与视频安全交换资源池包含管控中心 1 台、视频交换节点 2 台、数据交换节点 2 台、请求交换节点 2 台和网闸 1 台。数据与视频安全交换资源池采用分布式计算技术，把传统边界接入平台的内外网交换服务器及隔离设备资源池化，随着后期应用规模增加可以无限扩展。管控中心实现各个交换节点设备统一管控，数据交换节点实现文件数据和数据库数据跨网数据交换，视频交换节点实现音视频数据跨网交换，请求交换节点实现请求与响应数据跨网交换。网闸实现网络的强隔离和数据的跨网摆渡。

7）网络准入控制系统

在指挥信息网网络中部署一台网络准入控制系统，实现能够在不改变网络结构的情况下，对各种复杂网络实现准入控制，在实现准入控制基础上，通过边界探测技术，对全网的网络边界各接入点实现自动探测和防护，加强了网络可视性和可控性。系统内置了 Radius 服务、DHCP 服务、SNMP 服务、Web 服务，从用户、终端、网络、业务四个维度着手进行规范化管理，构建内网规范管理体系，严格审核入网对象的合法性、合规性，同时，我厅可根据定制的管理策略，对于不同的对象采取相应的处理手段，对网络中的用户、终端、网络、应用进行全方位的管控。

8）堡垒机

在我厅指挥信息网安全管理中心区部署一台堡垒机设备，实现运维人员通过堡垒机制定严格的特权帐号权限划分与访问认证功能，防止核心数据泄露，并进行威胁追踪。运维人员通过堡垒机单点登录运维，不必记录设备的 IP 地址、用户名、口令等信息，也避免这些敏感信息的泄露，极大地方便了运维工作，提升运维效率。堡垒机对整个运维过程从事前预防、事中控制和事后审计进行全程参与。事前预防：建立“自然人-资源-资源帐号”关系，实现统一认证和授权。事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制。事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定。

9）身份认证系统

在我厅指挥信息网安全管理中心区部署一台身份认证系统，实现登录我厅指挥信息网办公终端访问我厅指挥信息网应用系统的身份鉴别，只有合法获取数字证书的办公终端才允许访问指挥信息网应用系统。系统可以自动更新黑名单、动态更新，不需要重新启动服务；支持 LDAP、HTTP 等多种方式更新；支持 B64、DER 等多种格式。具有快速检索海量数字证书黑名单的功能。系统可以拥有多个站点证书，不同的服务可以拥有不同的站点证书。支持一个 SSL 服务中可同时配置多条证书链，验证不同 CA 的用户证书；支持多种证书支持功能：支持 CFCA、SHECA 及多数省级 CA 中心数字证书。系统可以将用户证书信息包括扩展项信息传送给应用系统。

10）安全运营管理平台

满足《网络安全法》第二十一条相关要求：即“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。”

满足等保 2.0 三级安全管理-集中管控相关要求：即“应划分特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。”

满足应急管理部科技信息化领导小组办公室下发文件要求：即“《关于印发

地方应急管理信息化2021年建设任务书的通知》（应急科信办【2021】1号）文件要求，主要内容为“省级应急管理部门负责数据汇聚处理节点，负责汇聚本瞎区市、区县指挥信息网运维管理数据，采集应用扫描结果，采集全网全要素的安全日志和网络流量，根据部统一数据规范对数据进行处理后上传至应急管理部安全运营管理平台。”

我厅建设省级安全运营管理平台，实现省本级、各（地）市、区县应急局各类型资产日志采集和流量采集等功能，同时，通过省级应急管理平台对各类型安全事件进行分析与处理后将上报至应急管理部安全运营管理平台。同时，省级安全运营管理平台应具备全网安全风险态势感知能力。

安全运营管理平台实现海量信息的采集、分析与展示，多种管理类系统的整合，保证业务信息系统的安全运营，符合并体现信息安全管理体系和等级保护的要求，并能够进行持续运营和改进。

（1）实现海量的分散安全信息采集、汇总、分析和展示

安全运营管理平台为了获悉全网的整体安全态势，就必须从现有的分散的各种安全系统和IT系统中采集相关的安全信息，而这些信息是海量的，每天的数据量可能数以百GB计。

这些海量的安全信息是安全运营管理平台的基础，完整采集、分析并展示这些信息对安全运营管理平台系统来说非常必要且重要。首先，如果不能采集到这些海量信息，分析的准确性就可能打折扣，而安全问题的回溯和取证就可能出现信息缺失。其次，如果不能对海量信息进行快速分析、提取出真正有意义的安全事件，就无法让安全管理人员聚焦到重要的安全事件上，反而陷入到数据的汪洋大海之中。最后，如果不能直观的展示分析结果，并将分析结果与响应处理过程挂钩，也就无法使执行层的安全管理流程运转起来，更无法为管理层提供决策支持。因此，如何采集这些分散在网络各处的海量信息，进行实时不间断的处理、分析，并以客户能够接受的形式有效的展示出来，成为了考验安全运营管理平台技术水平的一把重要标尺。

（2）实现多种管理类系统的整合

通过建设安全运营管理平台，不仅要能够打破安全防御的孤岛，将分散的安全设备和IT系统中的安全机制有效的集合到一起，还要能够与针对不同管理目

标的管理类系统有机的整合到一起，实现与各种管理类系统的协同工作。安全运营管理平台必须厘清与客户现有或待建的安全审计系统、终端/内网安全管理系统、身份管理系统、授权与访问控制系统、网络管理系统、应用服务管理系统、业务管理系统、资产管理系统、IT 服务管理系统之间的关系，在全局性管理体系的指导下，制定好安全运营管理平台与各类管理系统之间的接口和分工界面。否则的话，安全运营管理平台的建设可能会导致“管理孤岛”林立。

（3）保障业务信息系统的安全

对于客户而言，安全运营管理平台建设的根本目标一定要保障客户的核心业务系统的安全，从而有效的保障组织的战略。因此，需要从业务系统的高度去看待安全运营管理平台。安全运营管理平台的功能设计、分析对象以及展示角度都需要考虑到客户业务系统的构成、运行和保护要求。

（4）符合并体现等级保护及信息安全管理体系的要求

随着信息安全的建设以及对安全管理的需求不断提高，信息安全已经逐渐从技术上升到管理的高度，需要形成完整有效的信息安全保障体系和安全管理体系，达到系统地、完整地保障组织的信息安全的目的。等级保护和信息安全管理体系/ISO27000 建设已经成为了安全管理工作中必不可少的职责。安全运营管理平台能否及如何符合和体现等级保护和信息安全管理体系的要求成为了安全运营管理平台面临的重大挑战，这需要对等级保护和 ISO27000 系列标准的深刻理解，以及对安全运营管理平台功能的重新梳理。

（5）建成安全管理的长效机制

通过安全运营管理平台不仅要实现全网的整体安全，还要实现持续的安全运营，成为安全管理长效机制得以落实的关键技术保障。因此，安全运营管理平台必须具备持续监测的能力、安全量化的能力以及安全运维的能力。

安全管理平台详细功能设计如下：

1、综合展示

用户登录即可进入综合展示界面。通过该界面，能够快速的导航到各个功能。用户能够通过仪表板从不同的方面进行一体化安全管控，可以在一个屏幕中看到不同安全域的资产信息、实时安全事件曲线、统计图，以及网络整体运行态势、待处理告警信息等。用户可以自定义仪表板，按需设计仪表板显示的内容和布局，

可以为不同角色的用户建立不同维度的仪表板。用户可以对展示界面进行换肤。

2、工作台

工作台为特定用户提供了一个从其自身业务需要出发使用本系统的快速入口，通过预先配置，工作台集成了当前登录用户有关的日常工作活动，为其提供一站式管理功能。

工作台是与用户相关的，它把系统各功能模块进行有序的联系，形成面向用户的、条理清晰的工作桌面。

用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为不同角色的用户建立不同维度的仪表板。

3、资产管理

用户可以对网络中的管理对象划分安全域，并进行资产化管理，能够维护资产的基本属性、安全属性（CIA 三性）、管理属性等，并可以自定义资产标签，实现资产的动态属性扩展。系统提供基于拓扑的资产视图，可以按图形化拓扑模式显示资产，并可编辑资产之间的网络连接关系，通过资产视图可直接查看该资产的状态、事件、性能、风险、配置及告警信息，并可以通过资产管理界面直接对资产进行配置、监控、审计和管理等，实现了安全管理的统一入口。

用户可以根据自身业务的需求自定义资产类型、子类型，针对每种资产类型，用户都可以自定义资产属性，包括属性名称、类型（字符串、数字、枚举、时间、BLOB 等）。

4、业务安全管理

系统内置业务建模工具，用户可以构建业务拓扑。用户可以自由绘制业务拓扑图，支持多种自动布局方式，支持多种连线方式。业务拓扑支持子图，层次不限。

用户可以对业务拓扑中的每个资产设定关键性能指标及其每个指标的权重，针对用户设定的关键性能指标，系统会自动计算业务的整体性能指数。系统同时会自动计算业务的脆弱性指数和业务的威胁指数，连同业务性能指数，综合计算业务的健康度，并绘制出健康度随时间变化的业务健康曲线。

系统能够协助用户从业务的角度去分析业务可用性、业务安全事件和业务告警。

系统的业务管理模块还为用户提供了一个从业务层透视到资产层的下钻功能。用户选择构成业务的任何一个资产，都能够查看到该资产的相关信息，包括性能信息、安全事件等。

5、网络拓扑管理

系统能够描绘出网络拓扑图，展示 IT 资产之间的逻辑拓扑连接关系，并能够自动进行多种拓扑布局。

通过网络拓扑图，管理人员可以对全网的资产进行可视化的监控。拓扑图具备动态更新能力，能够实时地显示资产的运行状态和安全状态，能够方便地链接到其他功能模块。

系统还提供了机房机架视图，将客户资产设备根据实际机架摆放可视化地展示出设备的物理摆放。管理员透过机架视图可以清楚地知道每个资产的位置。机架视图也具备动态更新能力，能够实时地显示资产的运行状态和安全状态。

6、集中性能监控

系统能够对各种不同厂商的安全设备、网络设备、主机、操作系统以及各种应用系统的性能与可用性进行集中化实时监控。

7、系统智能故障诊断

系统具备基于故障树的网络故障诊断功能，能够根据网络故障沿网络拓扑水平传播的特性，通过对大量网络告警事件在拓扑空间中的分布，以及传播时间上的顺序，自动判别故障源。该技术本质上就是一种基于拓扑的事件关联分析技术。

8、仿真 3D 机房

系统中提供 3D 机房功能。通过 3D 虚拟现实技术，提供了一个完整的、网络化、可视化的三维虚拟环境，以可交互的界面，清晰完整展现整个用户机房的运行状态。包括环境、资产、运行状态等。对于网络、主机等信息实时监测的信息，可通过可视化的方式显示到 3D 机房中，实时反映系统的运行状态和报警信息。

9、性能信息采集

系统能够主动地、周期性地采集各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统的性能与可用性信息，采样周期、采集参数都可以独立配置。 系统支持通过 SNMP、TELNET、SSH、SSH2、ODBC、JMX、协议仿真等方式对 IT 资产进行性能与可用性信息的采集。管理中心内置性能信息采集，也

提供独立安装的性能信息采集器。

10、性能信息转发

管理中心或者性能采集器都具备性能信息转发功能，可以将收集到的性能信息转发给指定的管理中心，或者第三方系统。通过性能信息转发功能，可以实现性能采集器的分布式部署以及系统级联部署。系统支持性能数据的加密压缩转发。

11、IT 系统性能与可用性监控分析

系统对于各种监控对象都能进行全方位细粒度的监控，具有丰富的监控指标。管理员可以通过丰富的可视化图表查看监控指标信息；可以对监控指标设置告警阈值；可以将监控指标的数据保存起来，并进行历史分析。

系统提供各种性能监控指标的对比分析，如某段时间（小时、天、周、月）内某个资产的不同监控指标的对比分析、不同资产的相同监控指标对比分析等等，并能够将分析的结果以折线图和柱状图的形式进行直观展现。横向对比分析会以直观的折线图形式展现，而纵向对比分析则会以时间轴的方式动态展现。

12、性能采集器管理

系统能够对所有外接的性能采集器进行统一管理。用户可以对性能采集器进行登记、注销，进行性能采集参数的配置，设定监控任务、配置信息存储转发的参数。

13、网络故障诊断

系统具备基于故障树的网络故障诊断功能，根据网络故障沿网络拓扑水平传播的特性，通过对大量网络告警事件在拓扑空间中的分布，以及传播时间上的顺序，自动判别故障源。

14、安全事件管理

- 日志采集

系统能够采集各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的日志，通过 Syslog、SNMP、SNMP Trap、FTP、OPSEC LEA、NETBIOS、ODBC、WMI、Shell 脚本、VIP、Web Service 等协议进行采集。客户仅需安装部署审计中心，无需另装采集器，即可实现对日志的采集工作。系统也支持通过日志采集器和日志代理的方式采集日志，完全取决于用户的实际需要。

- 日志范式化与分类

对于所有采集上来的日志，系统自动进行范式化处理，将各种厂商各种类型的日志格式转换成统一的格式。系统提供的范式化字段包括日志接收时间、日志产生时间、日志持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、日志的事件名称、摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等 50 余个字段，并可以支持使用自定义字段。

在进行日志范式化的时候，系统对日志进行了信息补齐，加入了日志类型字段，对日志进行自动分类，为后续日志审计提供了便利条件。与此同时，系统将原始日志都原封不同的保存了下来，以备调查取证之用。

- 日志过滤与归并

系统可以对采集到的日志进行基于策略的过滤和归并，提升日志审计的效率。通过过滤操作，可以剔除掉无用的日志信息，降低日志噪音。通过归并操作，可以把短时间内满足一定条件的多条日志合并成一条日志，减少日志的存储量。日志过滤和合并策略可以用户自定义，系统默认不进行过滤和合并。

- 日志采集器

系统能够对所有外接的日志采集器进行统一管理。用户可以对日志采集器进行登记、注销，进行日志采集参数的配置，设定范式化、过滤、归并、转发的参数。

日志采集器支持分布式部署。

- 日志代理

如果管理中心无法通过远程方式主动或者被动地采集日志，那么系统提供日志代理软件包，通过在被管理对象上安装日志代理，采集相应的日志后，发送给管理中心。

- 日志转发

管理中心或者日志采集器都具备日志转发功能，可以将收集到的日志转发给指定的管理中心，或者第三方系统。通过日志转发功能，可以实现日志采集器的分布式部署以及系统级联部署。

日志支持无条件转发，也支持基于过滤规则的转发。系统支持加密压缩转发，

支持定时转发，支持断点续传。

15、安全事件实时监视

系统提供了实时监视与审计视图，管理员可以根据内置或者自定义的实时监视策略，从日志的任意维度实时观测安全事件的走向，并可以进行事件调查、钻取，并进行事件行为分析和来源定位。管理员可以实时监视防火墙、IDS、防病毒、网络设备、主机和应用的高危安全事件；可以实时监视各个部门、各个安全域、各个业务系统的重点安全事件；可以实时监视全网的违规登录事件、配置变更事件、针对关键服务器的入侵攻击事件等等。

对于实时监视中的日志，用户可以进行追踪调查，进行源/目标 IP 地址世界地图定位，并可以以图形化的方式展示事件之间的拓扑关系以及事件属性之间的聚合关系。

对于关联事件，可以追溯导致该关联事件的原始事件。

针对每条事件，用户都可以手工产生告警或者派发工单。

16、安全事件统计分析

系统提供了实时统计视图和历史统计视图，管理员可以根据内置或者自定义的统计策略，从日志的多个维度实时进行安全事件统计分析，并以柱图、饼图、堆积图等形式进行可视化的展示。管理员可以查看一段时间内的主机流量排行、主机登录失败次数排行、活跃病毒排行、网络设备故障排行、最多访问用户排行等等。

对于统计图表，支持下钻分析，查看相关的详细事件。

17、安全事件查询

系统提供事件和原始日志的查询功能，便于从海量数据中获取有用的事件信息。用户可自定义查询策略，基于时间、名称、地址、端口、类型等各种条件进行组合查询。系统还提供快速查询和模糊查询功能。

对于大时间跨度的查询，系统会自动进行任务调度，用户可以在查出部分结果后再看。

18、事件关联分析

- 规则关联

系统具备事件关联分析功能。通过关联分析规则，系统能够对符合关联规则

条件的日志产生告警。系统提供了可视化的规则编辑器，用户可以定义基于逻辑表达式和统计条件的关联规则，所有日志字段都可参与关联。

规则的逻辑表达式支持等于、不等于、大于、小于、不大于、不小于、位于……之间、属于、包含、FollowBy 等关系、“与或非”逻辑运算符以及关键字。

规则支持统计计数功能，并可以指定在统计时的固定和变动的事件属性，可以关联出达到一定统计规则的事件。

规则支持外部引用，可以引用地址资源、端口资源、时间资源、过滤器、资产分类属性。

系统支持单事件关联和多事件关联。通过单事件关联，系统可以对符合单一规则的事件流进行规则匹配；通过多事件关联，系统可以对符合多个规则（称作组合规则）的事件流进行复杂事件规则匹配。

- 情境关联

系统支持多种基于情境的关联分析：

基于资产的情境关联：分析师可以将事件中的 IP 地址与资产名称、资产价值、资产类型（包括自定义类型）、自定义资产标签进行关联；

基于弱点的情境关联：将安全事件与该事件所针对的目标资产当前具有的漏洞信息进行关联，包括端口关联和漏洞编号关联；

基于网络告警的情境关联：将安全事件与该事件所针对的目标资产（或发起的源资产）当前发生的告警信息以及当前的网络告警信息进行关联；

基于拓扑的情境关联：根据网络故障沿网络拓扑水平传播的特性，通过对大量网络告警事件在拓扑空间中的分布，以及传播时间上的顺序，自动进行网络根本故障源（Root Cause）诊断。

- 行为关联

系统支持多种基于行为的关联分析：

动态基线技术：采用了周期性基线分析的方法。周期性基线根据历史数据计算得出，通常是一个单周期数据库轮廓线。这条曲线由若干数据轮廓点组成。每个轮廓点代表一个采样时点。一个新的实际测量值如果没有超过基线范围，则通过加权平均算法更新旧的轮廓值。如果新的实际测量值超过基线范围则丢弃，不参与新轮廓值计算。如此往复循环，基线始终处于动态变化中。

预测分析技术：采用了基于时间窗置信区间的检测模型和方法。可以在实际运行中不断自我调整和逼近，自动剔除历史时间窗内的异常历史数据，实现历史时间窗数据与网络实际正常流量行为特征的高度吻合，从而提高了对异常行为报警的准确性。

系统采用了基于分析场景的交互模式。系统内置 14 种行为分析场景的模板，用户可以根据自身需求对模板进行实例化，建立任意数量的分析场景实例。

19、事件可视化

系统能够将海量的事件分析结果以可视化的方式形象地展示出来。包括行为分析图、IP 定位图、动态事件图等等。

20、事件存储

系统将收集来的原始日志和事件统一安全存储和备份。系统支持 TB 级的海量数据加密存储，满足合规与内控条款的相关要求。系统支持数据的自动或手动备份，备份数据可手工恢复，用作日志回查。

为了支撑海量事件的存储与分析，系统提供了分布式事件存储器部件，支持分布式事件存储与分析。系统将海量安全事件分布式地存储到多个事件存储器上，通过并行计算、分布式计算、聚合计算技术获得超高速的事件处理能力。管理中心可以对网络中分散的事件存储器进行集中管理。

21、脆弱性管理

系统具有脆弱性管理功能，能够从漏洞、配置弱点两个维度综合计算资产的脆弱性，包括漏洞的脆弱性和配置暴露的脆弱性。系统能够通过多种方式展示资产/安全域/业务系统的弱点信息，支持时间趋势分析和横向对比分析。

- 漏扫引擎调度

系统能够对漏扫引擎进行集中管理，并对漏扫引擎下发扫描任务，收集扫描结果，统一进行漏洞脆弱性分析。

- 漏扫结果导入分析

系统能够导入主流第三方漏洞扫描器对资产的漏洞扫描信息，并与系统的资产信息进行关联，自动计算出资产漏洞的脆弱性。

- 风险评估

系统通过内置的风险计算模型，综合考虑资产的价值、脆弱性和威胁，能够

定期自动地计算出资产的风险可能性和影响性，并通过二者建立了一个风险矩阵，进而计算出资产、安全域和业务系统的风险值，并刻画出资产、安全域和业务系统随时间变化的风险变化曲线。

系统能够形象地展示出安全域的风险矩阵，从可能性和影响性两个维度标注安全域中风险的分布情况，通过风险矩阵法，指导安全管理员进行风险分析，采取相应的风险处置对策。

系统还能以图表的形式可视化地显示每个资产、安全域或业务系统风险的关键因素，便于管理人员理解风险的具体含义。

- 配置核查

系统能够主动地、周期性地采集各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统的配置信息，并与配置基线进行比对。系统支持通过多种协议方式去对核查对象进行配置检查，这些协议包括并不限于：SSH/SSH2、TELNET、JDBC、SMB、核查代理，等等。系统内置了配置核查采集器，通过管理中心即可发起配置核查。系统也支持分布式部署的配置核查采集器，支持分布式配置核查和离线核查。

系统具有配置核查项管理和核查脚本管理功能，用户可以自定义核查脚本和核查项。

配置核查项，也称为检查项，包含了获取并验证某个核查对象某项安全配置的方式、方法、比对标准（基线）的说明。一个配置核查项表明了这个核查对象的安全配置基线是怎样的，这个配置项是如何采集和比对的。

配置核查项是用户配置安全检查规范和标准的落地。通过定义配置核查项，系统能够将用户纸面上的配置安全检查规范变成系统可以执行的配置检查规则，为自动化的配置安全核查奠定了基础。

系统内置了针对 5 大类、30 种设备对象的 1100 多个配置核查项，并支持自定义扩展。配置核查项类型包括帐号类、口令类、授权类、日志类、IP 设置类，以及其它类。

每条配置核查项信息包括并不限于：核查项名称、适用的设备类型、权重、检查脚本、比对脚本（解析规则）、配置基线值，等等。

核查脚本，是指针对核查对象的获取其相关配置项的命令行脚本或者数据库

查询语句。通常，一个核查脚本能够采集一个或多个配置信息。系统内置了 1100 多种检查项。

通常，真实应用场景中的用户不会针对孤立的资产进行配置核查，而是会对网络中重要的资产集合进行统一的核查，并且，针对这个集合中不同的资产有不同的核查标准。进一步地，组织管理机构检查、上级单位巡查以及内部定期检查的时候会存在多重检查标准，不同的业务系统相同设备检查要求也会存在差异。

为此，系统提供了核查策略的功能。通过建立核查策略模版，用户可以为不同的检查规范、不同的业务资产对象设定不同的核查标准和范围，为不同场景的检查制定多重标准。

用户可以基于任意的配置核查项组合出核查策略模版，并且可以修订配置核查项中默认的配置基线值。

借助核查作业功能，系统提供灵活的任务调度和管理功能，支持即时检查、定时检查、周期性检查和离线检查四种模式。

即时检查：直接选择核查对象，指定核查项后，生成即时核查作业，立即进行检查，并返回检查结果；

定时检查：基于核查策略、选定核查对象、建立核查作业，指定任务执行时刻，定时地地进行检查，并保存检查结果；

周期性检查：基于核查策略、选定核查对象、建立核查作业，并对任务进行调度，周期性地进行检查，并保存检查结果；

离线检查：在对不可达的网络进行检查时，系统可以先将核查作业下发给配置核查采集器，然后将配置核查采集器接入不可达网络自动执行检查，最后将配置核查采集器连回系统所在网络，会自动将检查结果回收至管理中心。

核查作业管理结合 PDCA 模型，实现检查作业的全过程管理，并从已创建、正执行、已执行等多个维度，实现对作业自身的监控、展示与统计。提供从计划到结果的全程追踪与展示。

配置核查结果可以导出为 WORD、HTML、EXCEL 等格式的核查报告，给出核查对象的配置符合性评分，并详细说明配置符合情况。历次配置核查的结果都予以保存，随时可以查阅。对于周期性核查结果，可以进行历次结果的比对分析和趋势分析，了解配置安全的改进情况。

22、安全态势呈现

态势感知层基于系统下层安全要素的采集和分析，负责向用户呈现态势感知能力，这里根据安全防护的重点和影响安全态势的几个重要方面，分为了资产态势、攻击态势、运行态势、脆弱性态势、风险态势、威胁态势、网站态势、流量态势。系统将通过这几个维度使用户对网络的安全态势进行把握和感知。

- 总体安全态势

集中全部获取的安全信息进行综合安态势呈现，帮助用户从全局的角度把控全网安全状态。包括攻击态势地图，围绕网络中的资产呈现被防护对象的安全态势，安全威胁趋势，全网告警分布，全网漏洞及配置弱点分布以及业务系统的健康态势等。

- 资产感知

资产感知是态势感知的基础，首先它通过主动发现、导入或创建的方式来识别和梳理目标网络中要被防护的资产及业务对象。所获得并维护的被防护对象信息将在整个态势分析呈现过程中，被其他维度的感知所利用，成为面向安全对象安全态势分析的基础。

在资产发现及安全对象信息维护的基础上，资产感知也会融合平台所收集的各类攻击威胁信息和脆弱性信息，形成被保护资产及业务对象视角的安全态势。

资产视角的安全态势将从资产类型、安全域角度和业务系统角度来审视资产的整体安全防护状态。从每个视角维度都可以提供资产受危害概览、资产弱点情况、资产受攻击情况以及资产风险的相关态势信息。

- 运行感知

运行态势基于各类信息资产和业务系统的性能与可用性信息，通过对各种监控对象进行全方位细粒度的监控，提供丰富的可视化图表；系统会自动计算业务的整体性能指数，系统同时会自动计算业务的脆弱性指数和业务的威胁指数，连同业务性能指数，综合计算业务的健康度，并绘制出健康度随时间变化的业务健康曲线。

- 攻击感知

攻击感知基于汇总全网相关的攻击行为相关信息，通过统计分析、关联融合等手段对攻击信息进行处理，从而获得全景式的攻击态势监视。攻击感知从遭受

攻击、攻击的类型、分布、攻击关系、趋势、攻击结果等维度进行攻击态势的呈现。包括分别从内部和外部的视角监视受攻击和发起攻击的态势，攻击在网络、主机、应用、数据层面上的分布和趋势，攻击的源目关系态势，攻击类型在不同安全域及业务系统或资产类型上的分布，攻击成功与否的结果态势等。

攻击感知通过对全网攻击相关信息的整合分析，用户可以从 6 个基础的维度来感知攻击行为，这 6 个维度分别是发起攻击维度、遭受攻击维度、攻击关系维度、攻击类型维度、攻击结果维度和攻击趋势维度。

- 发起攻击维度

  感知攻击来源的分布，包括外部发起的攻击或是内部安全域发起的攻击。

- 遭受攻击维度

  感知攻击目标在内部区域的分布。

- 攻击关系维度

  感知攻击来源和目的之间的关系，感知攻击类型与安全域的关系。

- 攻击类型维度

  感知攻击类型在安全域的分布，在业务系统的分布和在资产类型的分布。

- 攻击结果维度

  从被阻断和未被阻断的角度感知攻击结果。

- 攻击趋势维度

  感知网络层、系统层、网络层和数据层的攻击趋势。

通过这几个维度的攻击相关信息的感知，用户可以进一步了解获取全网范围内的攻击态势情况，所获得的攻击态势可以划分为 4 个方面，分别为攻击来源态势、遭受攻击分布态势、攻击规律和趋势态势以及攻击结果态势。

- 攻击来源态势

通过攻击来源态势，用户首先可以了解网络中所遭受的攻击哪些来自于内网，哪些来自于外网。对于来自外网的攻击，用户可进一步了解哪些是被监测到的具体攻击行为，而哪些是基于威胁情报感知到的外部攻击威胁。对于来自内网的攻击，用户可进一步了解发起的攻击在安全域或具体资产上的分布。

- 遭受攻击分布态势

在遭受攻击分布态势中，用户可以从多个维度了解掌握各类攻击行为所针对

目标对象的分布。从对象集合的维度来看，可以呈现被攻击目标在安全域、资产类型和业务系统上的分布；从网络分层的维度来看，可以呈现被攻击目标在网络层、主机层、业务层以及数据层的分布。

- 攻击规律和趋势态势

通过攻击规律和趋势态势，用户可以综合各类攻击信息从多个方面了解攻击的攻击规律和趋势情况。攻击规律方面，用户可以了解攻击源与攻击目标的一个汇总抽象关系，监视安全域、攻击类型、资产类型之间的对应关系及规律，以及掌握当前受攻击最严重的安全域、资产类型和具体资产等信息。趋势态势方面，用户可以从网络、主机、业务、数据 4 个维度了解攻击数量的发生趋势。

- 攻击结果态势

通过对攻击信息中有关攻击结果信息的抓取和分析，可以为用户呈现攻击结果的态势。这里首先为用户提供两个基本维度的攻击结果监视，分别是被阻断攻击态势和未被阻断的攻击态势。被阻断攻击态势包括各区域被防护的攻击、被防护的针对业务系统的攻击、内部发起被防护的攻击、外部发起被防护的攻击。未阻断攻击态势包括各区域未阻断的攻击、未被阻断的针对业务系统的攻击、内部发起未被阻断的攻击、外部发起未被阻断的攻击。

- 脆弱性感知

综合漏洞扫描、基线核查所扫描的全网漏洞弱点进行弱点态势呈现，使用户统一把控全网各区域各资产业务类型的弱点暴露。所呈现的态势包括漏洞的分布统计、影响的资产范围、长时间未处理高危漏洞情况、破坏及影响最高的安全弱点、漏洞及配置弱点在全网的风险态势、漏洞的综合处置情况等。

漏洞感知的信息来源自各类脆弱性扫描器的扫描结果信息，包括系统漏洞扫描器、应用漏洞扫描器、配置核查扫描器以及外部的漏洞情报信息。经过对各类脆弱性信息的分析处理，结合安全对象信息，漏洞感知可以从资产类型、安全域和业务系统维度进行漏洞态势的呈现。基于不同的维度可以展现如下的漏洞态势信息：

- 漏洞概要统计信息

包括当前发现漏洞的总数量、高危漏洞数量、新增漏洞数、漏洞影响的资产范围以及长期未处理的漏洞情况。

- 高危漏洞监视

通过高危系统漏洞、高危应用漏洞和高危配置弱点几个方面监视高危漏洞情况。

- 漏洞发现态势

包括系统漏洞的发现率、配置弱点的发现率以及扫描发现漏洞最多的资产情况。

- 漏洞总体安全态势

以漏洞风险矩阵的形式，分别从资产类型、安全域、业务系统的视角呈现漏洞的整体安全态势。

- 漏洞分布态势

包括漏洞和配置弱点在资产类型上的分布态势，漏洞和配置弱点在安全域上的分布态势，漏洞和配置弱点在业务系统上的分布态势。

- 漏洞数量趋势

反映一定时间范围内全网安全漏洞的数量变化趋势，也可烦展示不同等级漏洞的数量变化趋势。

- 细粒度监视

分别从资产类型、安全域、业务系统的视角，通过更丰富的字段信息呈现较为详细的漏洞统计信息，包括各严重等级的漏洞数量、出现漏洞的资产占比以及漏洞存在的时间等。

- 漏洞处置态势

从漏洞扫描、处置过程中各漏洞状态视角呈现漏洞的处置态势，包括漏洞消除的态势、新发现漏洞的态势、遗留未处理漏洞的态势和复现漏洞的态势。

- 威胁感知

威胁感知主要是通过收取对接来自于外部的威胁情报信息，经过比对分析来发现对网络及安全对象可能的潜在威胁，包括潜在的漏洞威胁和潜在的攻击威胁。

威胁感知包括态势信息的获取和针对自身网络情况的威胁分析。态势感知可分别对获取到的威胁情报信息和威胁分析后的结果进行呈现。

- 态势信息的获取

系统能够自动同步/导入/抓取来自内外部的威胁情报和漏洞情报并予以利用，提高威胁分析的实效性和准确性。威胁情报主要包括恶意 IP、恶意 URL 和一些互联网漏洞信息，可通过对接公开的外部安全机构、社区和合作的商业威胁情报厂商来获取。

- 威胁比对分析

通过数据关联，能实现将用户的资产与安全威胁相关联，来深度挖掘用户资产所面临的安全隐患、判断威胁的严重程度。

- 风险感知

风险感知综合资产价值、安全属性、脆弱性、攻击威胁等风险要素，基于风险模块内置的风险计算模型，进行全网、各安全域及各业务系统的风险量化评估和风险赋值。风险感知是从风险的角度来衡量被防护对象的安全态势，在平台的态势呈现过程中，风险感知存在于资产感知、漏洞感知和态势总揽当中，通过在各维度中为对应的目标给定风险值来帮助用户把握安全态势，例如在资产感知中，通过风险视图呈现各资产类型、安全域及业务系统的风险值，在态势总揽中通过风险视图给出全网的风险等级。

- 网站感知

网站感知主要从网站的脆弱性、被攻击情况、可用性、脆弱性等因素出发，利用内置的统计分析模型，对网站安全态势进行量化的分析呈现。以网站安全为中心，通过对网站的挂马、篡改、漏洞、敏感词的统计进行风险评估，通过被攻击详细信息、漏洞等级分布，敏感词的详情信息进行威胁的判断，脆弱性的排名，同时对网站的可用性进行实时监测呈现。

- 流量感知

借助创新的 vFlow 流描述语言，采用基于行为的分析方法，对流信息建立行为轮廓模型，通过流量的访问关系，流量大小，各协议流量分布和流量趋势等因素进行进行可视化呈现，掌控实时的流量态势，及时对网络连接的合规情况进行判定，实现对未知攻击行为的感知研判。

23、威胁态势分析

威胁态势（威胁 KPI）分析：系统通过对一组关键威胁指标（KPI）计算得到一个威胁指数，并以此随时间描述出一条威胁指数曲线，从而表征一段时间内、

某个网络区域的网络安全威胁状态及其发展趋势。系统建立了一套动态的多维威胁指标体系，通过帕累托分析法，协助管理员对当前的威胁成因进行辨别，实现对关键威胁因素从宏观到中观，再到微观的层层下钻，直至定位到导致威胁态势异常的关键安全事件。

24、热点事件分析

热点事件分析：系统采用聚类算法持续地从事件的源 IP、目的 IP、资产类型、事件等级、事件数目 5 个维度（向量）朝终端、网络和应用三个群组进行聚类运算，找到当前一段时间的事件热点，从而实现对海量事件的实时宏观分析。系统能够在群组标靶上动态显示事件热点，点击每个热点都能够进行钻取分析，显示产生该热点的相关安全事件。系统还支持历史事件的回放分析。

25、安全管理关键指标分析

系统通过对一组表征某个安全域或者业务系统安全管理建设水平的层次化指标的计算，得到该安全域或者业务系统的安全管理建设水平评级，以此来表明该安全域或业务系统的信息安全管理体系的建设成熟度。

系统将表征安全管理建设水平的这套层次化指标称作关键管理指标，每个指标项都建立了一个针对某类安全事件的度量标准。

系统能够可视化的展示出每个安全域或业务系统随时间变化的安全管理评估曲线，并能够进行环比分析，以及跨安全域或业务系统的同比分析。对于每个关键管理指标都支持指标项的下钻，实现从宏观到微观的聚焦。

26、告警管理

系统的告警功能包括告警设置和告警管理两个部分。

用户可以通过性能监控的监控指标阈值，或者安全事件的关联规则设置告警，包括告警触发条件和告警响应动作。系统的告警响应动作支持事件属性重定义、弹出提示框、发送邮件、发送 SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送 MSN、发送 Syslog、派发工单等方式。

告警管理则包括对告警信息的查看、处理和统计分析。系统提供快捷的告警响应处理流程，可记录告警信息的处理过程和处理结果，并能够与工单管理模块联动。

27、预警管理

用户可以通过预警管理模块发布内部及外部的早期预警信息，分析可能受影响的资产，提前了解业务系统可能遭受的攻击和潜在的安全隐患。

用户既可以手工产生内部预警，也可以设定内部预警规则，系统自动产生内部预警；用户可以发布的外部预警包括安全通告、攻击预警、漏洞预警和病毒预警等。

系统能够对预警信息进行生命周期管理，预警信息包括预备预警、正式预警和归档预三个状态。

预警信息能够与网络中的 IP 相关联，进行影响性分析。

28、威胁情报

威胁情报是一种基于证据的知识，包括了情境、机制、指示器、隐含和实际可行的建议。威胁情报描述了现存的、或者是即将出现针对资产的威胁或危险，并可以用于通知主体针对相关威胁或危险采取某种响应。

系统加入了威胁情报管理模块，利用开源以及威胁情报提供商的威胁情报系统，对整个系统的安全情况和网络上以及系统内部的威胁情报进行比对，更准确的分析以及预警安全事件。

获取组织内部的资产数据，以资产库的形式对资产进行管理；同时对组织对外的域名以及可探测到的对外服务进行收集，形成组织的资产数据。并对资产进行重要性赋值，为不同重要级别的资产提供对应的情报收集策略和关注度。

- 配置数据

获取组织资产的配置数据，包括终端、服务器、网络设备、安全设备的具体软硬件配置情况，如具体的软件版本、审核策略、安装软件、开放端口和开放服务等信息。

- 漏洞数据

对组织资产进行漏洞扫描，获取漏洞数据，与资产数据形成关联。

- 流量数据

通过实时实时镜像核心设备端口，获取网络流量数据和摘要数据。

- 日志数据

获取组织内部相关资产的日志数据。

- 外部威胁情报

本项目可以整合外部威胁情报提供商提供的外部威胁情报，根据项目建设提出的要求提供以下信息内容：

网络安全威胁信息：当前互联网爆发的安全威胁信息数据，如：APT 攻击、勒索软件等

病毒库：与当前爆发的病毒木马相关的信息，如病毒木马的各类指示器、威胁源、目标、所属团体、利用手段等威胁信息。

whois 库：域名 whois 信息与近 3 年内历史 whois 数据。

IP 库：包含 IP 地理位置信息（精确到区县级），AS 域信息，IP 反向解析记录信息，关联样本信息等。

傀儡机库：网络中监控到的被僵尸网络控制的 IP 信息。

行业资讯：当前热点的安全行业资讯信息。

安全漏洞：与企业自身 IT 资产相关的安全漏洞情报，如防火墙、网络设备、网站、操作系统、常用软件等企业自身内部 IT 基础设施资产的漏洞信息。

另外提供如下类型的威胁情报资源。

序号	情报类型	分类描述	分类示例
1	盗版软件	与企业应用软件盗版、仿冒相关的资产情报	如软件盗版（正版破解）、软件抄袭、仿冒 APP 等信息
2	钓鱼网址	与仿冒企业网站应用的非法钓鱼活动相关的威胁监测情报	如仿冒银行、公检法机关等的网站的 IP、域名等信息
3	钓鱼访问记录	钓鱼网站访问记录的威胁监测情报	如钓鱼网站访问用户身份、访问时间、银行账户、手机号、是否输入过密码/验证码、邮箱或其他身份信息等威胁信息
4	资产信誉	与企业 IT 资产被恶意利用导致资产信誉下降相关的资产情报	企业 IT 资产与恶意网络节点信誉库(如 C&C、垃圾邮件、域名等）比对命中后的反馈结果，如 IP、URL、域名、邮件等信息
5	社会舆论	与企业信息安全相关的社会舆论事件情报	如对其企业信息安全相关产品、服务、项目、人员等进行恶意炒作和网络水军攻击等事件

序号	情报类型	分类描述	分类示例
6	数据泄露	与企业内部数据泄漏相关的事件情报	如企业的员工账户数据、用户账户数据、内部文件、网络拓扑、财务报表、核心技术资料等敏感数据被公开外泄，或进行过地下交易等事件信息
7	资产发现	与企业外网 IT 资产暴露面相关的资产情报	外网 IT 资产探测数据与企业外网 IT 资产进行比对后的反馈结果，如 IP、域名、URL、端口、组件、版本等信息
8	安全漏洞	与企业自身 IT 资产相关的安全漏洞情报	如防火墙、网络设备、网站、操作系统、常用软件等企业自身内部 IT 基础设施资产的漏洞信息
9	内容篡改	与企业网络站点内容被篡改相关的事件情报	通过对企业网站内容的监控，发现的页面文字、图片等被篡改事件，如文字链接、图片链接等信息
10	网页木马	与企业网络站点存在的网页木马相关的事件情报	监测发现存在网页木马的具体事件信息，如木马类型、木马样本 MD5 值等
11	网页暗链	与企业网络站点存在的网页暗链相关的事件情报	与黄、赌、毒、传销等相关的网页暗链植入的具体事件信息，如暗链类型、URL 等
12	WEBSHELL	与企业网络站点存在的 WEBSHELL 相关的安全事件情报	监测发现存在 WEBSHELL 后门的具体事件信息，如 WEBSHELL 名称、上传路径、源 IP 等
13	病毒木马	与当前爆发的病毒木马相关的威胁情报	如病毒木马的各类指示器、威胁源、目标、所属团体、利用手段等威胁信息
14	勒索软件	与当前爆发的勒索软件相关的威胁情报	如勒索软件的各类指示器、威胁源、目标、所属团体、利用手段等威胁信息
15	APT 情报	与 APT 攻击事件相关的威胁情报	如 APT 事件涉及的指示器、威胁源、目标、利用手段、利用漏洞等威胁信息

序号	情报类型	分类描述	分类示例
16	指示器集合	与威胁相关的指示器集合情报	如恶意 IP、恶意域名、恶意 URL、VPN 节点、IP 地理位置、C&C 节点、TOR 节点、僵尸网络、IDC 节点、VOS 节点等

29、工单管理

工单即任务单，是安排安全管理运维人员解决或者完成某项任务的指令，包含有工作内容描述，完成该项工作的人，以及工单的流转和完成状态等。

系统支持通过告警自动派发一次性告警工单，也支持用户手工派发周期性任务工单。指定的工单处理人在接收到工单后可以记录工单的流转信息和状态信息。管理员可以查看所有的工单及其流转的全过程。系统能够对工单的数量、状态（处理情况）等进行统计分析。

30、报表管理

系统内置了丰富的报表模板，包括统计报表、明细报表、综合审计报告，审计人员可以根据需要生成不同的报表。系统内置报表生成调度器，可以定时自动生成日报、周报、月报、季报、年报，并支持以邮件等方式自动投递，支持以 PDF、Excel、Word 等格式导出，支持打印。

系统还内置了一套报表编辑器，用户可以自行设计报表，包括报表的页面版式、统计内容、显示风格等。

31、知识管理

系统提供开放的知识管理功能，内置了大量的安全知识，同时也允许用户在系统使用过程中不断丰富和完善。用户可以对所有的知识点进行基于关键字的全文检索，操作界面类似百度搜索或者 Google 搜索。

系统预先建立的知识包括：案例库、漏洞库、事件库、文档库、字典库等。

32、级联管理

系统允许上级管理中心对下级管理中心的节点进行集中管理和展示，上级管理中心可以访问下级管理中心，上级管理中心可以集中将系统泛化策略规则下发给下级管理中心。在上级管理中心，可以对下级管理中心的节点进行配置和监控。

33、权限管理

系统应采用基于角色的访问控制机制（RBAC），在该机制中，权限与角色相

关联，用户通过成为适当角色的成员而得到这些角色的权限。这就极大地简化了权限的管理。在一个组织中，角色是为了完成各种工作而创造，用户则依据它的责任和资格来被指派相应的角色，用户可以很容易地从一个角色被指派到另一个角色。角色可依新的需求和系统的合并而赋予新的权限，而权限也可根据需要而从某角色中回收。系统提供三权分立的设计，内置系统管理员、用户管理员和审计管理员三种角色。

系统提供用户集中管理的功能，对不同的角色赋予不同的访问权限，对角色可以访问的资源进行细致的权限划分，通过将用户赋予不同的角色来赋予不同的功能。系统具备安全可靠的分级及分类用户管理功能，支持用户的身份认证、授权、用户口令修改等功能。不同的操作员具有功能操作权限。

34、系统管理

系统具有丰富的自身配置管理功能，包括自身安全配置、系统运行参数配置等。系统具有自身运行监控与告警、系统日志记录等功能。

安全运营管理平台方案建设的收益如下：

- 四维一体的全网安全管理与运维

安全运营管理平台以客户的业务信息系统安全为保障目标，从监控、审计、风险、运维四个维度对全网的整体安全进行集中化的管理与运维，为用户建立起了一个可视、可查、可度量与可持续的安全管理新平台。

借助安全运营管理平台，用户可以获得对全网安全的可视化，洞悉业务信息系统的运行状况与安全状况；可以对全网的安全事件进行综合分析与审计，识别

和定位外部攻击、内部违规；可以进行业务系统的安全风险度量、安全态势度量和安全管理建设水平度量；可以进行持续的安全巡检、应急响应与知识积累，不断提升安全管理的能力。

- 日常安全运维工作的有力工具

对于日常安全运维而言，核心的工作内容就是对 IT 网络及重要业务系统进行持续监测，确保网络、主机、应用、业务、重要信息和人员资产的安全。更具体地说，就是要持续监测并识别针对网络、主机、应用、业务、重要信息和人员资产性能故障、非法访问控制、非法或不当操作、恶意代码、攻击入侵、违规与信息泄露行为。

借助安全运营管理平台，客户能够统一收集来自网络中 IT 资产的运行信息和日志信息，通过分析这些数据，识别各类性能故障、非法访问控制、不当操作、恶意代码、攻击入侵，以及违规与信息泄露等行为，协助客户安全运维人员进行安全监视、审计追踪、调查取证、应急处置、生成各类报表报告，成为客户日常安全运维的有力工具。

- 遵照等级保护的技术要求

安全运营管理平台在设计之初就充分考虑的国家制定的信息系统等级保护制度中对于安全管理中心的安全设计技术要求。系统能够帮助客户更好地遵从等级保护的基本安全要求和安全设计技术要求。

GB/T 22239-2008《信息安全技术信息系统安全等级保护基本要求》对定级信息系统提出的基本安全要求覆盖面广、安全措施分散，安全运营管理平台能够对基本安全要求中涉及物理、网络、主机、应用和数据相关的安全机制的有效性进行集中的审计。系统对这些分散的安全机制产生的安全日志进行统一的采集和存储，协助客户对安全记录数据进行统计、查询、分析，并生成审计报表。

与此同时，针对基本安全要求中涉及系统运维管理的基本管理要求，安全运营管理平台从资产管理、设备管理、监控管理、网络安全管理、系统安全管理、恶意代码防范管理、安全事件处置等方面为客户提供了一个多角色的运维支撑的技术平台。

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》明确指出在对定级系统进行等级保护安全技术方案进行设计和实施的时候，对于二级

（含）以上的定级系统必须设计安全管理中心，实现对定级系统的安全策略和安全机制的统一管理。安全运营管理平台符合相关的设计技术要求，能够对定级系统中涉及安全计算环境、安全区域边界、安全通信网络的安全信息进行集中化的安全信息与事件采集、分析、响应、处置，监测与分析系统的运行状态、用户行为，为定级系统信息安全管理体系的实施、检查和改进过程提供支持。

- 契合信息安全管理体系的监测与评审要求

信息与网络安全建设的复杂性决定了企业和组织需要建立和维持一套信息安全管理体系。为此，ISO 颁布了信息安全管理体系的系列标准（ISO27000 系列）。越来越多的企业和组织开始采用 ISO27000 的最佳实践来指导自身的安全管理体系建设。

ISO27001 强调通过 PDCA 的方式来持续建设安全管理体系。其中，作为 C（Check，检查）的监测与评审环节十分重要，它要求客户“对照信息安全管理体系的方针、目标和实践经验，评估并在适当时测量过程的执行情况，并将结果报告给管理者以供评审”。

安全运营管理平台为客户提供了一个对信息安全管理体系进行持续监测与评审的技术支撑平台，协助客户通过对安全日志的持续采集与分析以及安全风险的持续评估，最终达到对信息安全管理控制措施的持续改进。

六、 其他终端等建设

在指挥大厅和总调度室新建 2 套一机三屏计算机。一机三屏的主要目的是将工作中的工作信息、辅助工具和内容输出显示在三台显示器上，以方便并行开展工作，达到快速了解各项资讯和决策处置的目的。

新增加一套触摸屏通信调度台。

新址计算机需求为 106 台，现有可利旧数量为 21 台（放总调度室），需要新建 85 台。

根据需求，为政务外网、互联网、指挥信息网设备间共配备了 3 套 KVM、3 台扫地机器人和 3 台自动鞋套机。

根据各处室应急指挥和办公需求，配置电话 114 部、IP 电话 21 部、可视电话 1 部。

七、 原有系统搬迁方案

本着经济节约、能用尽用的原则，根据新址的信息化系统建设方案，将可用设备搬迁至新址，以重复利用；不满足建设需求的设备，盘点整理后入库，以做备件使用。对网络、安全设备，需要关注业务使用情况，搬迁割接过程尽量避开业务使用时段。

1、网络及安全设备：指挥中心新址网络经过重新组网架构，现有系统中部分低端交换机将整改出网络，此部分交换机可作为接入层交换机使用，也可以作为备品备件。

重构后的网络中，核心网络设备和安全边界设备均为新购置的设备，因此，在新址网络设备环境搭建完成后，再将可利旧设备搬迁至新址，搬迁时间点设在网络使用率最低的时间。

2、业务平台设备：本项目不涉及业务平台的变动，原有相关业务平台设备直接搬迁至指挥中心新址，搬迁时间点设在业务使用率最低的时间。

机房内的网络设备、安全设备、业务平台设备搬迁至新址后的机柜立面图见附图。

3、显示大屏系统：过渡指挥厅的 LED 显示大屏系统，整体搬迁至新址业务技术楼 2 层多功能厅，利旧使用。大屏搬迁时间在新址指挥大厅建设完成并投入使用后，不影响指挥中心指挥调度。

5、音频会议系统：过渡指挥厅的音频会议系统，搬迁至新址业务技术口保密会议室和办公楼 4 楼会议室，利旧使用。在新址指挥大厅建设完成并投入使用后，不影响指挥中心指挥调度。

6、视频会议系统：过渡厅的视频会议系统搬迁至新址，利旧使用，与新建视频会议系统一同上线使用。

7、LED 液晶显示器：过渡厅多台 75 寸 LED 显示器设备，根据现场尺寸需求，可搬迁至主业务技术楼监控室、餐厅等处利旧使用。直接搬迁安装即可，不影响使用。

8、其他设备搬迁：其他可利旧设备均可在新址建设完成后统一搬迁，不影响指挥中心指挥调度。

八、 软硬件选型原则及配置清单

1. 选型原则

一、标准性与兼容性

系统的设计应遵循国家标准和行业标准，采用标准化设计，对外提供统一标准的接口，供其他业务系统调用。所有技术与业务标准完全符合有关标准要求，对于尚无全国统一标准的部分，支持自定义与扩展。

二、先进性与适用性

采用科学的、主流的、符合发展方向的技术、设备和理念。设计合理，架构简洁，功能完备，切合实际，能有效控制和提高效率，满足各项应用需求。系统的技术性能和质量指标达到国际领先水平；同时，系统的安装调试、软件操作使用又应简便易行，容易掌握。

三、经济性与实用性

在先进、可靠和充分满足系统功能的前提下，体现高性价比。采用经济实用的技术和设备，充分利用现有资源，综合考虑系统的设计、建设、升级和维护。充分考虑实际需要和信息技术发展趋势，根据用户使用环境及相关资源配备，设计选用功能和符合用户要求的系统配置方案，实现最佳的性能价格比，以便节约项目投资。

四、可靠性与安全性

系统采用成熟的、稳定的、完善硬件设备，系统具有一致性、升级能力，能够保证全天候长期稳定运行。在系统故障或事故造成中断后，能确保数据的准确性、完整性和一致性，并具备迅速恢复的功能，同时系统具有一整套完成的系统管理策略，能够符合 365*7*24 运行的需要，可以保证系统的运行安全。同时具有可靠的备份方案，在系统发现严重故障后，备份的数据可以正确恢复。

系统采取必要的安全保护措施，防止病毒感染、过载、断电和人为破坏，具有高度的安全和保密性。对用户权限分级管理，用户所有操作通过日志存档记录。

五、开放性与便捷性

系统设计坚持开放式架构，可随着存储空间增加的需求，在现有的设计架构下，实现业务功能的不断发展与完善。系统需要支持各个开放性标准，包括跨平台及支持各种数据库与应用中间件等。

2. 配置清单

详见附表。

九、 环保、消防、职业安全和节能措施的设计

1. 环境影响分析和环保措施

建设任务属于无污染工程，设备电磁辐射值在国家规范允许范围内，不会对环境造成污染。系统建设和运行过程中没有有毒、有害废水和气体排出，主要排放物为生活污水。建设过程中，严格按照国家颁发的有关环境保护法规和要求进行文明施工，设置在室外的风机采用高效低噪声设备，以降低室外噪声。

（1）施工期分析

施工期的水污染主要为施工人员生活污水；大气污染物主要为施工扬尘；固废污染则是建筑垃圾，包括包装袋、废包装箱、废砖块、废木料、废水泥制品、弃土、生活垃圾等。

（2）营运期分析

营运期项目将会对周围环境产生一定影响。影响环境的因素主要有：

1）扩声系统、动力设备、空调系统等设备产生的噪音。

2）电磁辐射。

3）激光打印机硒鼓、喷墨打印机墨盒的污染。

4）计算机、激光打印机排放出的有害气体。

5）营运期项目产生废水主要为生活污水，包括厕所污水和盥洗污水等。

6）固体废弃物主要是生活垃圾，有果皮、果壳、饮料罐、包装袋、废纸等。

针对上述影响环境的因素，必须考虑使用符合国家环保要求的设备和技术，保护系统使用人员的身体健康。具体的环保措施为：

（1）项目建设期环保措施

项目建设期中尽可能选择先进的施工工艺和低噪声的施工设备；在施工现场设置临时的生活污水处理措施；对施工材料及废弃物加强管理，防止雨水冲刷污染水体；尽量使用能够循环的材料，避免浪费、重复建设、重复返工等现象发生。建筑垃圾及时由环卫部门清运。

（2）项目运行期环保措施

针对上述影响环境的因素，必须考虑使用符合国家环保要求的设备和技术，保护系统使用人员的身体健康。具体的环保措施为：

1）计算机、网络及相关硬件设备要满足 TCO99 和 FCC-B 低电磁辐射标准认证，设备外壳采用绿色阻燃可回收环保材料。

2）计算机屏幕采用液晶显示屏幕，保护工作人员视力，满足人体工程学、生态学方面的要求。同时室内必须安装必要的空调、空气加湿/去湿设备，保证空气的流通。

3）激光打印机要控制粉尘污染，硒鼓、墨盒要考虑回收利用或鼓粉分离。

4）室内设备的噪音应当低于 50 分贝；合理布置扩声系统，采用适宜的声学处理措施。选用低噪声的空调机、冷冻机、冷却塔、水泵等设备。空调送风口设消音器和消声弯头，管道出入口接软接头；易产生振动的设备，采取减震措施。

5）项目产生的生活污水，生活污水经化粪池经过处理达到排放标准后排至城市污水管网，由城市污水处理厂统一处理。

6）固体废弃物：室内外设垃圾筒、垃圾箱，生活垃圾及时由环卫部门清运。

2. 消防措施

在项目建设过程中，遵循“预防为主，消防结合”的方针，严格贯彻执行国家《建筑设计防火规范》，设计中采取一下措施：

（1）消防措施

消防设备、器材的配备型号和功率要满足消防需要，并随时进行检查和保养，使其始终处于良好的待命状态，并确保消防水源充足和供水系统工作正常。

设置火灾自动报警系统、消防电话通信系统、建筑设备（通风、空调、给排水、供电）自动系统等，并自动连锁，构成一套完整的火灾报警即自动灭火体系。

定期进行防火安全检查。

（2）配套设施

计算设备间内的主要出入口设置出入口指示灯，室内需设置人员疏散用的事故照明和应急报警灯，疏散标志。

设备间内电源切断开关靠近工作人员的操作位置或主要出入口。

3. 职业安全和卫生措施

3.9.3.1 成立安全防护领导小组

项目实施阶段，安全防护领导小组设组长 1 名，成员若干名。组长由项目经理担任，成员由项目主管工程师、项目部成员组成。

3.9.3.2 健全各项安全制度

本项目为信息化项目，实施中遵守国家关于信息化工程的相关标准规范、信息安全等级保护相关标准规范、软件研发相关标准规范等，并针对安全管理制定具体制度规范。

3.9.3.3 职业卫生措施

本项目将贯彻“以人为本”的原则，根据国家和有关部门的规范和标准，采取的主要职业安全和卫生措施有：

（1）所有用电设备的金属外壳、金属底座、电缆金属铠装层、电缆保护管以及所有金属支架均与接地装置连接，设有安全接地，配电系统设有安全短路保护、过流保护装置，保证用电安全。

（2）选购计算机设备时，考虑防辐射问题，以利于操作人员的身体健康。

（3）选用低噪声设备，保证业务域噪声小于 60db。

4. 节能措施

3.9.4.1 用能标准及节能设计规范

本项目建设方案的编制和实施，严格按照发改委【2006】2787《国家发展改革委要求加强固定资产投资项目节能评估和审查工作》、国发【2006】28 号《国务院关于加强节能工作的决定》的要求进行，依据国家和行业有关节能的标准和规范，合理设计，注重节约，提高了能源利用效率，贯彻了生态和可持续发展原则。

本项目相关的节能设计规范有；

1《中华人民共和国节约能源法》；

2《中华人民共和国可再生能源法》；

3《国家鼓励发展的资源节约综合利用和环境保护技术》（国家发改委〔2005〕

第65号）；

4《民用建筑节能管理规定》（建设部部长令第76号）；

5《节能中长期专项规划》（发改环资〔2004〕2505号）；

6《中国节能技术政策大纲》（2006年修订）；

7《国务院关于加强节能工作的决定》（国发〔2006〕28号）；

8《关于加强固定资产投资项目节能评估和审查工作的通知》（发改投资〔2006〕2787号）；

9《国家发展改革委员会关于印发固定资产投资项目节能评估和审查指南（2006）的通知》（发改环资〔2007〕21号）；

10《国务院关于进一步加强节油节电工作的通知》（国发〔2008〕23号）；

11《国务院办公厅关于深入开展全民节能行动的通知》（国办发〔2008〕106号）；

12《用能单位能源计量器具配备和管理通则》；

13《国家发改委等部门关于贯彻实施〈中华人民共和国节约能源法〉的通知》（发改环资〔2008〕2306号）；

14《综合能耗计算通则》（GB/T 2589－2008）；

15《工业企业能源管理导则》（GB/T 15587－2008）；

16《企业能耗计量与测试导则》（GB/T 6422－2009）；

17《企业能源计量器具配备和管理通则》（GB/T 17167－2006）；

18《评价企业合理用电技术导则》（GB/T 3485－1998）；

19《节水型企业评价导则》（GB/T 7119－2006）；

20《用能单位能源计量器具配备与管理通则》（GB/T 17167－2006）；

21《采暖通风与空气调节设计规范》（GB 50019－2003）；

22《节电技术经济效益计算与评价方法》（GB/T 13471－2008）；

23《公共建筑节能设计标准》（GB 50189－2005）；

24《建筑照明设计标准》（GB 50034-2004）；

25《采暖通风与空气调节设计规范》（GB 50019－2003）。

3.9.4.2 项目能源消耗种类和数量分析

政府工作报告提出将全面加强管理，把节能降耗纳入经济社会发展的统计、

评价考核体系，建立信息发布制度。

本项目为信息工程，主要能源消耗为电力资源，电力资源消耗主要由网络设备、服务器设备、安全设备、终端电脑、显示设备、扩声设备、制冷设备等产生的能源消耗。

本项目能耗分析根据新建内容建设规模及用电设备配置情况选择合理的计算方法，根据用电设备功率、需要系数及设备负荷率等相关参数计算项目年电能消耗量。

本项目用电主要包括设备间的网络、安全设备及服务器设备，指挥大厅及其他场所的信息化设备，年电能消耗量约为32万度，折合标准煤约39.33吨。项目年电能消耗量汇总如下表所示：

表　项目年电能消耗量汇总表

序号	耗能设备	单位	数量	标称功率（瓦）	同时系数	年运行时间	负荷率	年用电量
						小时		万度
1	设备间（网络、安全设备及服务器等）	台	50	500	0.9	8760	70%	13.8
2	指挥大厅耗电设备	项	1	23500	0.9	8760	60%	11.1
3	其他	项	1	15000	0.9	8760	60%	7.1
	合计							32

3.9.4.3 项目所在地能源供应状况分析

本项目的基础硬件设施，主要将布置在哈尔滨市红旗大街251号主楼及副楼，部署系统及设备主要依靠该大楼的电力能源供应系统来运行。现有的电力供应能力能够满足本项目设备的运行。

3.9.4.4 节能措施和节能效果分析

在设备采购和组织管理方面加强管理力度，采取切实有效的节能措施，使本项目以最小的能源消耗取得最大的经济效益，达到国家相关节能要求。

（1）设备采购

本工程项目所有电气设备采用国家推荐的高效节能设备，严禁使用落后淘汰

产品。本工程项目所安装的电气设备功率很小，负荷电流也很小，电缆线路按经济电流密度选择，可降低线路损耗，可实现节电。

（2）组织管理

在能源管理制度建设方面，加强节能管理机构，制定完善从能源采购、计量、统计、管理和定额考核等一系列的能源管理制度，把能耗指标细化、量化，落实好能源管理经济责任制的考核，促进各项节能工作的有效展开，为取得好的节能降耗效果，做好组织和管理工作。

建立专职能源计量机构，加强能耗设备的能耗计量管理工作，配备相应的仪表和设备，定期对计量器具进行检查维护，达到计划用能、节约用能的目的。

针对本项目的具体情况，经过分析、比较，制定合理利用能源及节能的技术措施，有效的降低了各类能源的消耗。

十、 施工工艺要求

1. 施工技术总则

1、施工单位严格按照批准后施工图进行施工。

2、接到任务书制定详细的施工方案、计划和进度，确保按时完成任务。

3、审核施工图后，组织相关的施工人员、技术人员，讲解本次施工的要点、要求和注意事项，使施工人员明确施工性质、内容和任务。更好的按期、按质、按量完成施工任务。

4、遵守国家和部委颁发的法规、标准和规范。

5、严格执行国家或部委颁发的工程施工验收技术规范或工程及验收暂行技术规定。

6、以施工质量第一为宗旨，加强施工现场的管理和施工监督，严格执行施工规范。做到施工工艺精良，各种测试项目齐全、记录清楚、文字端正、数据准确。符合相关技术要求。

7、严格按施工操作程序施工，做到文明施工、文明生产。施工中做好防火、防电、防雷、防化学气体、防事故等预防性的工作，做到施工人员的安全及设备材料的安全。

2. 材料、设备、器具要求

1、设备选型及验收

设备、材料应根据合同及设计要求选型，设备、材料进场验收，并填写验收记录。设备应有产品合格证、检测报告、安装及使用说明书、认证标识等。如果是进口产品，则需提供原产地证明和商检证明，配套提供的质量合格证明，检测报告及安装、使用、维护说明书的中文文本。设备安装前，应根据说明书进行全部检测，合格后方可安装。

2、其他材料

镀锌材料、镀锌钢管、镀锌线槽、金属膨胀螺栓、金属软管、塑料软管、机螺钉、平垫圈、弹簧垫圈、接线端子、绝缘胶布、各类接头等。

3、安装器具

手电钻、电锤、电烙铁、电工组合工具、对讲机、RJ45 专用压线钳、尖嘴钳、剥线钳、脚手架、梯子等。

4、测试工具

万用表、工程宝、测线仪、兆欧表、水平尺、钢尺、小线、线坠等。

3. 作业条件

1、建筑内土建工程、内装修完毕，门、窗、门锁装配齐全完整。

2、设备间、弱电竖井、建筑物其他公共部分线缆沟、槽、管、箱、盒施工完毕。

3、设备间内防雷接地、保温层、处理完毕后。

4、施工方案编制完毕并经审批。

5、施工前，应组织施工人员熟悉图纸、方案及专业设备使用说明，并进行有针对性的培训及安全、技术交底。

4. 线缆布放及连接

1、线路布放标准

线缆完好无损，外皮完整，中间严禁有接头和打结的地方；

线缆布放时，连接正确，保持其顺直、整齐，布放时线缆按一定顺序；

线缆拐弯应均匀、圆滑一致，弯弧外部保持垂直或水平成直线；

每条线缆两端有明显标志，以便于连接和检查，线缆标签应贴（绑）于线缆两端的明显处且不易脱落；

信号线与电源线分开敷设，不相互缠绕，平行走线，并避免在同一线束内。信号线及电源线在机架内布放时，分别在两侧走线。在同一线槽内走线时，间距不小于 200mm；

线缆穿越上、下层或水平穿墙时，用防火封堵材料将洞孔堵实。

2、线路绑扎标准

对于插头处的线缆绑扎应按布放顺序进行绑扎，防止电缆相互缠绕，电缆绑扎后应保持顺直，水平电缆的扎带绑扎位置高度应相同，垂直线缆绑扎后应能保持顺直，并与地面垂直。

选用扎带时应视具体情况选择合适的扎带规格，尽量避免使用多根扎带连接后并扎，以避免绑扎后强度降低。扎带扎好后应将多余部分齐根平滑剪齐，在接头处不得带有尖刺。

电缆绑扎成束时，一般是根据线缆的粗细程度来决定两根扎带之间的距离。扎带间距应为电缆束直径的 3-4 倍。

绑扎成束的电缆转弯时，扎带应扎在转角两侧，以避免在电缆转角处用力过大造成断芯的故障。

3、信号线的布放及连接标准

信号线缆的规格、位置、路由和走向符合施工图的规定，线缆排列必须整齐，外表无损伤。

信号线缆绑扎在垂直桥架上。绑扎后的线缆相互紧密靠拢，外观平直整齐，线扣间距均匀，松紧适度。

在水平桥架内布放信号线不绑扎，线缆应顺直，尽量不交叉。在线缆进出线槽部位和转弯处应绑扎或用塑料扎带捆扎。

静电地板下布放的线缆，注意顺直不凌乱，避免交叉，并且不得堵住空调送风通道。

电缆的弯曲半径不小于电缆外径的 15 倍，避免不必要的信号损失。

4、电源线布放及连接标准

根据实际情况利用设备自带的电源线。当设备电源引入线孔在机顶时，电源

线沿机架顶上顺直成把布放。

电源线芯线对地的绝缘电阻符合国家对电缆的相关技术要求。

设备间内的交直流电源线和接地线采用防火阻燃电缆，交、直流电源线不绑扎在一个线束内。

交直流电源线的连接牢固，接触良好，电压降指标及对地电位符合设计的要求。

电源线的接头使用铜鼻子时，进行适当的防腐蚀处理，与设备连接用的螺栓紧固件必须加装弹簧片。电源线与铜鼻子连接采用压接方式。

沿地槽布放电源线时，线缆不直接与地面接触，宜采用橡皮垫子或横木条垫底。

十一、 安全生产措施

1. 工程安全管理组织

1、建设单位要根据《安全生产法》等有关法律规定，设置安全生产管理机构或者配备专职（或兼职）安全生产管理人员。

2、新建、改建、扩建工程的安全生产设施必须要与主体工程同时设计、同时施工、同时投产使用。

3、工程监理要严格按安全生产专篇要求实施安全监督和管理

4、工程施工要严格按安全生产专篇要求，对施工人员要进行安全教育和培训，落实安全防护措施和安全经费，加强施工现场安全管理和检查。

5、施工现场有两个以上施工单位交叉作业时，建设单位应明确各方的安全职责，对施工现场实行统一管理。

6、依法进行工程招标投标的建设项目，招标方或委托的招标代理机构编制招标文件时，应当单列安全生产费用项目清单，并在招标文件中明确。

7、建设单位与施工单位应当在施工合同中明确安全生产责任、安全生产计划；明确安全生产费用的数额、支付计划、使用要求、调整方式等条款。建设单位对安全防护、安全施工有特殊要求需增加安全生产费用的，应结合工程实际单独列出安全生产增加项目清单。

2. 安全施工基本要求

1、施工单位应当按照国家有关规定配备专职安全生产管理人员，施工现场必须有专职安全生产管理人员。

2、施工单位应根据施工现场情况编制应急预案。发生任何事故，应迅速采用有效措施，积极组织救护、抢险、减少人员伤亡和财产损失，防止事故继续扩大，并立即报告安全生产管理部门。

3、施工单位在施工前应对施工作业环境进行检查和评估，制定相应的安全生产、文明施工措施。施工现场工作人员必须严格按照安全生产、文明施工的要求，积极推行施工现场的标准化管理，按施工组织设计、科学组织施工。

4、施工单位必须严禁使用未取得有关部门颁发的《特种作业人员岗位操作证》的人员从事特种作业；禁止使用未经上岗培训的人员上岗作业。

施工单位必须保证施工现场安全措施费用和施工人员的安全生产用品的落实。

5、如果在施工过程中可能会出现与设计文件不符的地方，需进行适当的修改或调整时需要施工方、设计方、建设方和各单位安保部门等共同协商，按最佳方案实施。

6、对涉及在线扩容、割接和带电作业的工程，施工企业必须与维护部门商定实施方案，保护措施，应急方案，做好安全防范措施，保证工程顺利进行。

7、施工作业区内严禁一切非工作人员进入。严禁非作业人员接近和接触正在施工运行中的各种机具与设施。

8、施工单位应为从事高空、高压、易燃、易爆、剧毒、放射性、高速运输、野外作业的施工人员办理团体人身意外伤害险或个人意外伤害险。