姚明织带工业园区信息化建设设计方案

XXXXXXX 有限公司

2019 年 7 月

目录

1. 概　述 4
1.1 背景介绍 4
1.2 需求分析 4
1.2.1 设计依据 4
1.3 设计原则 8
1.4 设计目标 9
2. 整体设计框架 10
2.1 整体网络设计拓扑 10
2.2 分区分域详细说明 11
3. 云数据中心&容灾备份方案规划 13
3.1 云数据中心设计思路 13
3.2 云数据中心设计功能说明 15
3.3 云数据中心建议清单 16
4. 安全建设方案规划 20
4.1 建设思路 20
4.2 安全建设设计功能说明 21
4.2.1 安全物理环境 21
4.2.2 安全通信网络 24
4.2.3 安全区域边界 25
4.2.4 安全计算环境 28
4.2.5 安全管理中心 32
4.3 安全建设建议清单 35
5. 安防系统工程 37
5.1 视频监控系统 37
5.1.1 园区视频监控总体设计思路 37
5.1.2 视频系统总体架构设计 39
5.1.3 系统安全设计 39
5.1.4 系统组成 40
5.1.5 各部分系统详细设计 44
5.1.6 监控平台功能介绍 52
5.2 巡更管理子系统 55
5.2.1 系统概述 55
5.2.2 系统设计说明 55
5.2.3 功能功能介绍 56
5.3 周界防入侵报警系统 57
5.3.1 概述 57
5.3.2 系统需求分析 57
5.3.3 系统组成 57

5.3.4 周界防入侵报警系统配置 *61*
5.3.5 系统功能点 *61*
6. 基础网络传输系统 **63**
6.1 基础网络规划 63
6.1.1 核心层交换机设计 *64*
6.1.2 汇聚层交换机设计 *64*
6.1.3 接入层交换机设计 *65*
6.1.4 无线 AP 设计 *65*
6.2 网络建设建议清单 70

1. 概　述

1.1 背景介绍

需要补充

1.2 需求分析

该工程由于委托进行建设，本次项目名称为新建园区项目。

信息化系统建设分为以下几大部分：

1、 **安防系统工程**

2、 **网络安全系统**

3、 **数据中心超融合系统**

4、 **园区无线及数据交换系统**

1.2.1 设计依据

园区信息系统的建设依据国家相关法律规章、国家和行业相关标准、相关研究成果等资料进行规划设计，具体如下：

- **法规政策**
  - 《中华人民共和国网络安全法》（2017 年 6 月 1 日起施行）
  - 中办[2003]27 号文件（关于转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知）
  - 中办[2003]27 号文件（关于转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知）
  - 公通字[2004]66 号文件（关于印发《信息安全等级保护工作的实施意见》的通知）
  - 公通字[2007]43 号文件（关于印发《信息安全等级保护管理办法》的通知）
  - 公信安[2009]1429《关于开展信息安全等级保护安全建设整改工作的指导意见》
  - 国发[2012]23 号《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》

- 公信安[2014]2182 号《关于加强国家级重要信息系统安全保障工作有关事项的通知》（ 公信安[2014]2182 号）

- **国际标准**
  - ISO27000 系列标准
  - ISO/IEC 13335 信息安全管理标准
  - SSE-CMM 安全系统工程能力成熟度模型
- **国家标准**
  - GB/T25066-2010 信息安全产品类别与代码
  - GB/T17900-1999 网络代理服务器的安全技术要求
  - GB/T20010-2005 包过滤防火墙评估准则
  - GB/T20281-2006 防火墙技术要求和测试评价方法
  - GB/T18018-2007 路由器安全技术要求
  - GB/T20008-2005 路由器安全评估准则
  - GB/T20272-2006 操作系统安全技术要求
  - GB/T20273-2006 数据库管理系统安全技术要求
  - GB/T20009-2005 数据库管理系统安全评估准则
  - GB/T20275-2006 入侵检测系统技术要求和测试评价方法
  - GB/T20277-2006 网络和终端设备隔离部件测试评价方法
  - GB/T20279-2006 网络和终端设备隔离部件安全技术要求
  - GB/T20278-2006 网络脆弱性扫描产品技术要求
  - GB/T20280-2006 网络脆弱性扫描产品测试评价方法
  - GB/T20945-2007 信息系统安全审计产品技术要求和测试评价方法
  - GB/T 21028-2007 服务器安全技术要求
  - GB/T25063-2010 服务器安全侧评要求
  - GB/T 21050-2007 网络交换机安全技术要求（EAL3）
  - GB/T28452-2012 应用软件系统通用安全技术要求
  - GB/T29240-2012 终端计算机通用安全技术要求与测试评价方法
  - GB/T28456-2012 IPsec 协议应用测试规范
  - GB/T28457-2012 SSL 协议应用测试规范
  - GB/T20269-2006 信息系统安全管理要求

- GB/T28453-2012 信息系统安全管理评估要求
- GB/T20984-2007 信息安全风险评估规范
- GB/T24364-2009 信息安全风险管理指南
- GB/T20985-2007 信息安全事件管理指南
- GB/T20986-2007 信息安全事件分类分级指南
- GB/T20988-2007 信息系统灾难恢复规范

- **行业标准**
  - 《商业银行信息科技风险管理指引》
  - 《股份制商业银行风险评级体系（暂行）》
  - 《网上银行系统信息安全保障评估准则》

园区视频监控技术要求：

《关于 XX 区视频监控及安保设计要求》

《XX 区生产保安视频监控技术要求》

安防视频监控系统设计方面：

《安全防范工程程序与要求》（GA/T75-1994）

《安全防范工程技术规范》（GB50348-2004）

《中华人民共和国治安部行业标准》（GA70-94）

《视频安防监控系统技术要求》（GA/T367-2001）

《民用闭路监视电视系统工程技术规范》(GB50198-94）

《工业电视系统工程设计规范》（GBJ115-87）

《安全防范系统通用图形符号》（GA/T75-2000）

治安部《警用地理信息系统系列标准规范》

《安全防范系统验收规则》（GA308-2001）

《安全防范系统通用图形符号》（GA/T74-2000）

《安全防范系统雷电浪涌防护技术要求》（GA/T 670-2006）

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《安全防范工程技术规范》(GB 50348-2004）

《安全防范系统验收规则》（GA308-2001）

《电子计算机机房设计规范》(GB50174-93）

视频监控图像质量方面：

《电视视频通道测试方法》（GB3659-83）

《彩色电视图像质量主观评价方法》（GB7401-1987）

视频系统网络设计方面：

《信息技术开放系统互连网络层安全协议》（GB/T 17963）

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《计算机信息系统安全》（GA 216.1－1999）

《计算机软件开发规范》（GB8566-88）

视频系统工程建设方面

《建筑物防雷设计规范》(GB50057-94）

《建筑物电子信息系统防雷技术规范》(GB50343-2004）

《安全防范系统雷电浪涌防护技术要求》(GA/T670-2006）

《民用建筑电气设计规范》(JGJ/T16-92）

《电气装置安装工程电缆线路施工及验收规范》（GB 50168-92）

《电气装置安装工程施工及验收规范》（GBJ 232-92）

《工业企业通讯接地设计规范》

《治安交通管理外场设备基础施工通用要求》（GA/T652-2006）

《通信建设工程安全生产管理规定》 （工信部 [2008]111 号）

《工程建设标准强制性条文》（建标 [2000]259 号）

《电信专用房屋设计规范》（YD/T 5003-2005）

《电信设备安装抗震设计规范》（YD/T 5059-2005-I）

《光同步传送网技术体制》（YDN 099-1998）

《电磁辐射防护规定》(GB8702-88)

3GPP2 标准、CWTS 公布的有关 cdma2000-1X 及相关升级标准；

除上述规范以外的遵循相关地方规范与标准以及国家、省市、相关行业的技术要求及规范。

1.3 设计原则

本系统的方案应体现“总体规划、统一设计、分步实施”的原则。

1）总体规划

在系统规划时，整个系统应总体规划，分步实施。园区监控系统的建设考虑与海关、海事和边检等口岸单位的监控需求，预留光纤节点。

2）统一设计

本方案设计时，考虑系统的可扩充性，充分考虑园区的建设和发展。前端点位和分控系统可以分步实施，分控可以逐步建成。整个系统提供扩展接口，为以后前端点的扩充，为传送到各口岸单位的图像预留好相应的接口。

3）分步实施

在系统实施时，我们考虑分步实施，根据“分步实施、急用先上”的原则。系统的具体设计应以“实用、可靠、先进、经济”为指导思想。

4）实用性

在工程设计和实现的过程中，始终要把园区的实际需求放在首位，做到灵活、好用。选择实用性强的系列产品，模块化结构设计，既满足当前的需要又为今后系统发展留有余地。

5）先进性

在系统总体方案设计时，总体规划采用先进技术。先进性是指关键设备采用国内的先进设备，以确保 3-5 年内不落后。

6）经济性

系统尽量采用性能、价格比好的产品，既能满足实际需要，又可尽量降低费用，同时在系统化的设计过程中，进行优化设计，便于今后维护，大大降低系统费用。

1.4 设计目标

以科技与信息化为支撑，加强信息化基础设施建设，初步建立起园区管理信息系统，推进园区建设，提升园区现代化管理服务水平创建新一代“智慧园区”。

2. 整体设计框架

2.1 整体网络设计拓扑

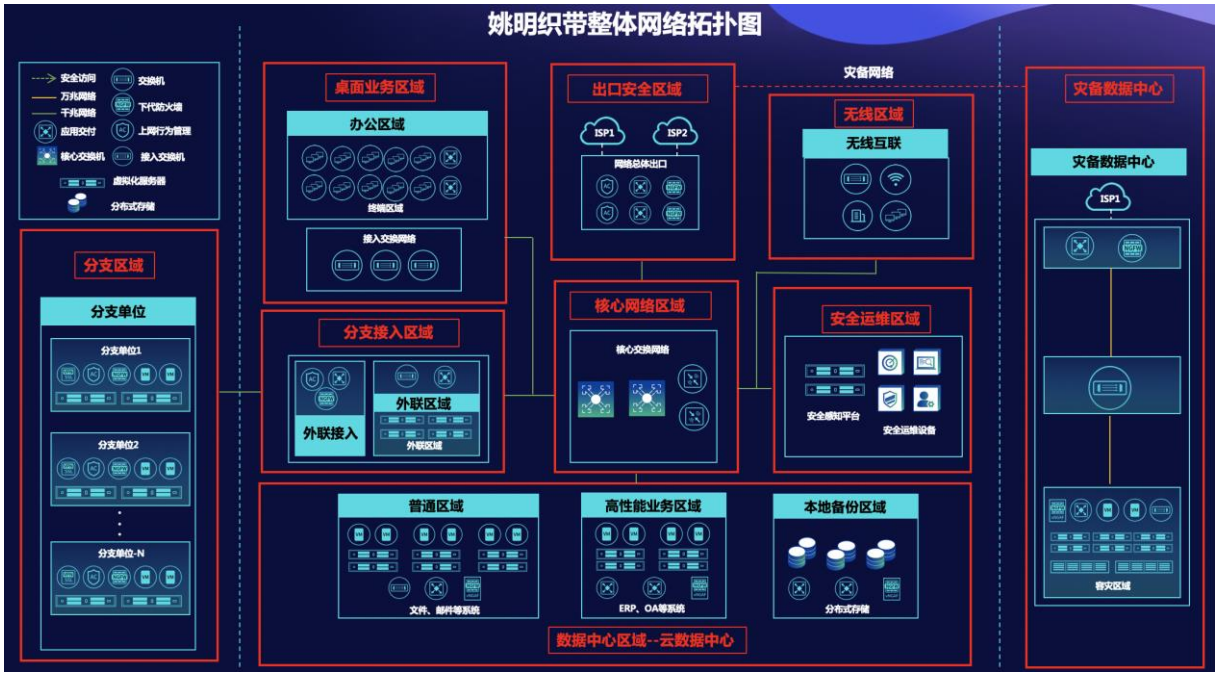


图 整体设计网络框架

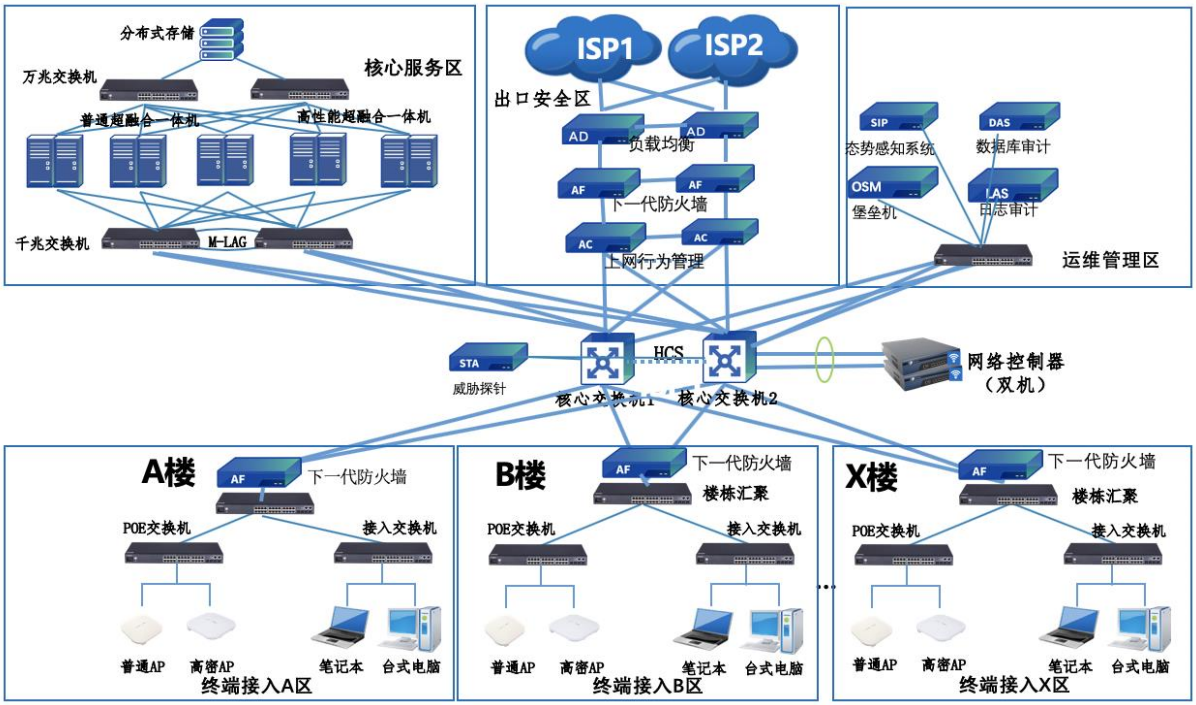


图 主数据中心拓扑设计

图为姚明织带整体网络设计规划，主要包含数据中心业务区域、数据中心业务备份区域、边界安全区域、安全运维区域、分支接入区域、桌面办公系统区域、无线接入区域、异地容灾区域和连接所有区域的网络设计。

2.2 分区分域详细说明

（1）数据中心业务区域：

根据当前数据中心调研，目前姚明织带机房已经使用了虚拟化技术，建议新工业园区可以借鉴虚拟化的方式进行数据中心规划，可以使用完整的超融合方案分别规划高性能业务区域和普通业务区域，承载 ERP、OA 或文件、邮件等系统；同时在计算、存储和网络虚拟化技术之上，建议规划云平台，满足后续分支单位按需分配资源的需求。

（2）数据中心业务备份区域：

数据中心业务规划完整后，为了保障本地数据安全，建议规划本地备份设备，需要同时满足定时备份和连续数据保护功能，可以按照业务的重要程度选择合适的备份策略。

（3）异地容灾区域：

考虑到姚明织带业务的安全性，可以在异地机房规划完整的灾备中心，当主机房出现故障时，可以在异地机房快速的拉起并恢复业务，满足园区工作和生产的需求。

（4）边界安全区域：

边界防护是安全保障体系中最基础的第一道门槛，考虑到姚明织带每个网络区域业务的安全性，需要把风险和威胁抵御在边界外部，保障内部资产的安全。同时也满足等级保护 2.0 基于边界防护的要求；

（6）安全运维区域：

考虑到姚明织带业务的安全性以及为了提高企业 IT 运维人员的效率。需要部署一个安全运管理域，负责主要的安全运维、安全审计和管理中心。

（7）无线接入区域：

根据现场环境选择适当 AP 类型进行部署，包括高密、普通、面板等，所有 AP 均通过接入 POE 交换机供电供网，节省布线施工成本；同时在部署无线 AP 时需考虑无线的信道规划，避免相互干扰，并设置安全可靠的接入认证方式；

（8）网路框架设计：

为满足整网高可靠及高吞吐需求，本次核心层采用万兆核心进行堆叠部署，核心区到楼栋汇聚间采用万兆光口级联实现数据信息的汇集，楼栋汇聚与楼层接入间采用千兆光纤互联；

3. 云数据中心&容灾备份方案规划

在数据中心规划过程中，建议采用云计算方式进行方案设计，应用在 IT 的不同层面，从逻辑层将物理层抽象出来意味着逻辑组件会得到更一致的管理。

从安全监督来看，云计算提升了服务器的可靠性、可用性，从基础架构层面获得了原先单机系统无法想象的功能，大大提高了业务连续性的级别，降低了故障率、减少了系统宕机的时间。

从服务器的角度来看，云计算让每台设备都能托管多套操作系统，最大化了利用率，降低了服务器数量。

从存储的角度来看，云计算可网络化、整合磁盘设备，并让多个服务器共享磁盘设备，从而提高了利用率。

从网络角度来看，云计算可实现托管应用基于虚拟网络进行通信，简化数据中心网络架构。

从应用的角度来看，云计算将应用计算从用户设备中分离出来，并在数据中心对应用及相关数据进行整合，通过集中化技术改善了管理和系统的安全性。

信息化经过多年的发展，数据中心在基础设施和应用系统方面取得了很大的成绩，随着业务规模的不断扩张，数据中心已出现瓶颈，若继续采用传统架构进行建设，从成本、管理、运维等角度已不符合公司发展需求，从长远策略出发，考虑经济效益，建设云化数据中心势在必行。

3.1 云数据中心设计思路

在规划云计算数据中心过程中，整体规划思路如下图，主要包括：

（1）物理层：

通过标准的服务器+存储+网络的方式进行搭建，沟通硬件资源池，对虚拟化层进行直接交付，可以按照业务需求规划普通硬件和高性能硬件；

（2）资源池层：

基于标准的硬件资源，通过计算虚拟化构建计算资源池，存储虚拟化构建存储资源池，网络虚拟化构建虚拟网络设备资源池，安全虚拟化构建安全资源池，并且在此基础

上，可以向业务层分别交付块、文件和对象存储，可以直接在 IAAS 层之上扩展交付 PAAS 解决方案和桌面云解决方案；

（3）IAAS 资源：

平台提供云管理平台功能，或者其提供标准接口，被第三方云管（Openstack 等）接管和运维；

（4）服务目录：

基于云平台提供的计算、存储和网络资源池，可以按照需要提供云主机、云硬盘、VPC、弹性 IP、vGPU、虚拟防火墙、虚拟 SSL VPN、备份、容灾、块存储等服务内容，满足后续业务使用过程中，按需获取需求，同时也可以满足姚明织带未来几年发展过程中，对于底层架构资源的诉求；

（5）应用中心：

为了实现部分 PAAS 层的需求，云平台需要提供容器、微服务、代码仓库、大数据服务和中间件等功能，匹配公司业务的快速发展；

（6）运营：

为了保障姚明织带集团云的规划需求，可以按需给分支公司分配云资源满足其使用，云平台需提供多租户管理、自助服务门户、流程工单审批、报表中心的等功能，从而实施真正的姚明集团云的使用和运维；

（7）混合云：

平台需要提供接口，满足未来和混合云对接需求；

（8）智能运维

为了保障整个云平台的的运维，平台需支持虚拟机监控、数据库监控、业务监控、主机监控、存储监控、集中告警等等功能，保障业务上云后可以通过运维工具实时了解数据中心业务状态；

（9）本地备份&异地容灾：

为了保障数据安全，备份规划备份资源池，可以按照需要将业务定时或者实施备份到本地区域，本地集群数据故障时，可以直接从本地备份中加载数据恢复业务；为了避免机房性故障，在异地规划灾备业务区域，本地故障后，可以在异地将业务拉起，提供业务服务，本地恢复后，可以将异地数据回迁至本地；

（10）平台安全：

姚明云平台建设完毕，需要持续关注平台本地安全，虚拟化本身需要提供安全防护解决方案，虚拟机之前需要提供安全隔离解决方案，平台出口也需要提供相应的安全防护解决方案，从而满足数据中心安全合规的需求。

3.2 云数据中心设计功能说明

序号	组件	功能
1	服务器	提供运行业务系统所需计算资源、存储资源等；规划不同的服务器以区分不同的性能的业务区域
2	存储	提供存储资源

3	交换机	网络连接设备
4	计算虚拟化	安全分配虚拟机并实现虚拟机全生命周期管理
5	存储虚拟化	存储虚拟化，规划分布式存储资源
6	网络虚拟化	简化网络运维
7	安全虚拟化	提供虚拟安全资源，保障平台业务安全
8	云管理平台	租户管理、资源分配、流程工单、自主门户运维等功能
8	定时备份和连续数据保护功能	保障数据和业务安全
9	异地容灾软件功能	业务异地接管
10	提供 PAAS 功能	提供容器、微服务等功能
11	提供块、对象和文件存储	提供不同的存储方式，满足虚拟机、文件和视频等存储需求

3.3 云数据中心建议清单

序号	型号	描述	数量	单位
姚明织带新建园区业务区域				
1	普通性能服务器	CPU 2 颗 Xeon Gold 6132,256G 内存，12*SATA/SAS 盘位，缓存盘 2*960 SSD，数据盘 4*4T STA，6 个 GE 接口，2 个万兆光口	7	台
2	高性能服务器	CPU 2 颗 Xeon Gold 6132,256G 内存，12*SATA/SAS 盘位，数据盘 6*1.9 SSD，6 个 GE 接口，2 个万兆光口	3	台

3	计算服务器虚拟化软件	务器虚拟化，虚拟机生命周期管理， HA 高可用，虚拟机备份，一键故障检测。	20	CPU
4	虚拟存储软件	存储虚拟化，存储多副本，高性能读写缓存，存储弹性扩展，数据故障切换，磁盘故障告警。	20	CPU
5	网络虚拟化软件	网络虚拟化，快速网络部署，虚拟交换机，虚拟路由器，分布式防火墙，应用监控。	20	CPU
6	云计算管理软件	云管平台，含工单审批，多租户管理，自服务页面等云功能。	20	CPU
7	持续数据保护软件	CDP 功能必备，至少提供 30 个台虚拟机的 CDP 授权	1	套
8	容灾备份软件	容灾备份软件功能，至少提供 10 个台虚拟机的异地容灾授权	1	套
9	PAAS 平台授权	支持容器、微服务等功能	1	套
10	虚拟防火墙	带宽性能:400M;新建会话/秒（七层）:50000;并发会话数（七层）:2000000;推荐虚拟机配置:4 核 CPU,8G 内存;	2	套
11	虚拟负载均衡	授权带宽:3G;并发连接:2000000;L4 新建性能 CPS:120000;L7 新建性能 RPS:35000;最低要求 4 核 CPU、8G 内存;	2	套
12	存储交换机	下一代智能光交换机，48 个 10G SFP+光口,6 个 40G SFP+光口；支持全端口线速转发；支持 NAC 统一管理、统一查看状态、VLAN 等配置管理；支持胖瘦一体化	2	台
13	业务交换机	下一代智能万兆交换机，48 个 1G 电口,4 个 10G SFP+光口;，支持全端口线速转发；支持 NAC 统一管理、统一查看状态、VLAN 等配置管理；支持胖瘦一体化	4	台
14	硬件质保	三年硬件质保	3	年
15	软件升级	三年软件升级	3	年
备份业务区域				

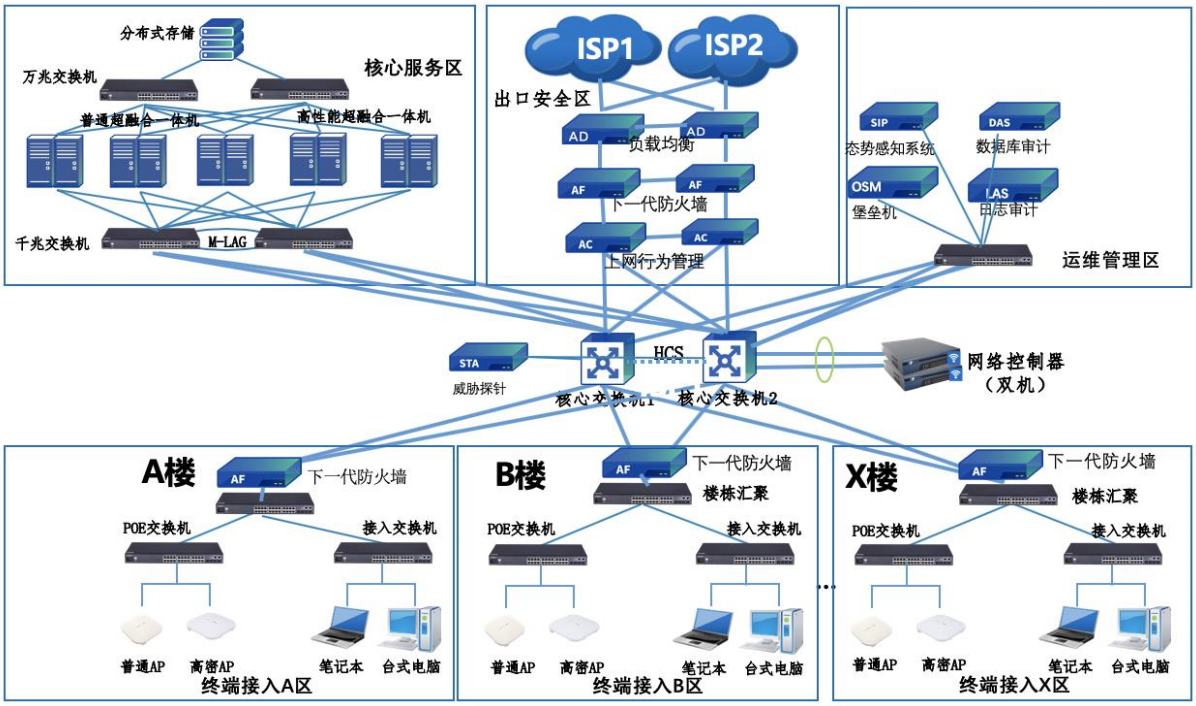
1	分布式存储	存储一体机，高度 4U，128G 内存，36 个 3.5 寸盘位，2x1G+4x10G 网口，双电源，2*960T SSD 缓存盘，10*6T 数据盘	3	台
2	企业级分布式存储授权软件	软件功能：快照、配额、拓扑管理、智能缓存、智能分层，桶管理、用户管理。总共包含 180T 容量授权。	1	套
3	万兆光模块	SFP+万兆多模	24	个
4	存储交换机	下一代智能光交换机，15 个 10G SFP+万兆光口，1 个 SFP 千兆光口，8 个千兆电口，支持全端口线速转发；支持 NAC 统一管理、统一查看状态、VLAN 等配置管理；支持胖瘦一体化。	2	台
5	硬件质保	三年硬件质保	3	年
6	软件升级	三年软件升级	3	年
容灾业务区域				
1	普通性能服务器	CPU 2 颗 Xeon Gold 6132,256G 内存，12*SATA/SAS 盘位，缓存盘 2*960 SSD，数据盘 6*4T STA，6 个 GE 接口，2 个万兆光口	3	台
2	计算服务器虚拟化软件	服务器虚拟化，虚拟机生命周期管理， HA 高可用，虚拟机备份，一键故障检测。	6	CPU
3	虚拟存储软件	存储虚拟化，存储多副本，高性能读写缓存，存储弹性扩展，数据故障切换，磁盘故障告警。	6	CPU
4	网络虚拟化软件	网络虚拟化，快速网络部署，虚拟交换机，虚拟路由器，分布式防火墙，应用监控。	6	CPU
5	云计算管理软件	云管平台，含工单审批，多租户管理，自服务页面等云功能。	6	CPU
6	PAAS 平台授权	支持容器、微服务等功能	1	套
7	虚拟防火墙	带宽性能:400M;新建会话/秒（七层）:50000;并发会话数（七层）:2000000;推荐虚拟机配置:4 核 CPU,8G 内存;	1	套

8	虚拟负载均衡	授权带宽:3G;并发连接:2000000;L4 新建性能 CPS:120000;L7 新建性能 RPS:35000;最低要求 4 核 CPU、8G 内存;	1	套
9	存储交换机	下一代智能光交换机，48 个 10G SFP+光口,6 个 40G SFP+光口；支持全端口线速转发；支持 NAC 统一管理、统一查看状态、VLAN 等配置管理；支持胖瘦一体化	2	台
10	业务交换机	下一代智能万兆交换机，48 个 1G 电口,4 个 10G SFP+光口;，支持全端口线速转发；支持 NAC 统一管理、统一查看状态、VLAN 等配置管理；支持胖瘦一体化	2	台
11	硬件质保	三年硬件质保	3	年
12	软件升级	三年软件升级	3	年

4. 安全建设方案规划

4.1 建设思路

在规划新园区安全建设过程中，整体规划思路如下图：



安全域划分

安全域是指同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络，每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略，区域间具有相互信任关系，而且相同的网络安全域共享同样的安全策略。一个安全域内可进一步被划分为安全子域，安全子域也可继续依次细化。根据新建园区业务访问的需要，结合信定级对象分等级保护的思想，将新园区安全整体网络分为出口安全区域、分支接入区域、内网办公区域、数据中心域、运维管理区域等。安全域具体划分如上图所示。

互联网出口域，该区域说明如下：需在互联网出口边界进行隔离和访问控制，保护内部网络，从 2-7 层对攻击进行防护，实现对入侵事件的监控、阻断，保护整体网络各个安全域免受外网常见恶意攻击，主动扫描 web 和电子邮件流量、阻止恶意软件到达并感染网络上主机等防护功能；需对互联网出口流量进行识别并对流量进行管控，提高带宽利用率的同时保障用户上网体验，并按相关法律法规进行上网行为审计。

核心服务器域，该区域说明如下：该安全域内主要承载业务服务的服务器等，需在区域边界设置访问控制策略，对这些业务信息系统提供 2-7 层安全威胁识别及阻断攻击行为的能力，如 SQL 注入、XSS（跨站脚本攻击）、CSRF（跨站请求伪造攻击）、cookie 篡改等；主要存储业务信息系统产生的数据；

运维管理区域：该区域负责主要的安全运维、安全审计和管理中心。需要通过运维审计系统（堡垒机）对日常网络设备和资产登录进行身份认证和操作纪律审计，并实现对网络设备的防护；通过日志审计系统搜集分析各类网络设备、安全设备及操作系统等日志，综合分析并存储及事后追溯；主要存储业务信息系统产生的数据，需对这些数据库的访问权限进行划分，并对数据库的相关操作进行审计；主要存储业务信息系统产生的数据，需对这些数据库的访问权限进行划分，并对数据库的相关操作进行审计；通过安全感知实现统一安全管理中心，满足等级保护 2.0 中技术要求新增的安全管理中心相关要求，提供应急响应与处置、监测预警等新技术要求。

终端接入区域：该区域主要是针对边界进行防护，从 2-7 层对攻击进行防护，实现对入侵事件的监控、阻断，保护整体网络各个安全域免受外网常见恶意攻击，主动扫描 web 和电子邮件流量、阻止恶意软件到达并感染网络上主机等防护功能；

4.2 安全建设设计功能说明

4.2.1 安全物理环境

对于不同安全保护等级子系统各自独立使用机房或独立使用某个部分（区域）的情况，其独立部分可根据不同安全保护等级的要求和需求独立设计。对不同安全保护等级子系统共用机房或共用某些部分（区域）的情况，其共用部分按照最高原则进行设计，也就是就高不就低的原则。在安全物理环境建设方面，参考 GB 50174-2017《数据中心设计规范》，机房物理安全标准遵循国家等级保护三级要求进行防护，具体设计如下：

（1）物理位置选择

机房场地选择在具有防震、防风和防雨等能力的建筑内，机房和办公场地场所在建筑物具有建筑物抗震设防审批文档；避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

（2）物理访问控制

二级系统要求机房出入口安排专人值守或配置电子门禁系统，三级系统要求机房出入口配置电子门禁系统物理机房，控制、鉴别和记录进入的人员，从物理访问上加强对机房的管理。

（3）防盗窃和防破坏

将机房设备或主要部件进行固定，并设置明显的不易除去的标记；通信线缆铺设在隐蔽处，可铺设在地下或管道中；机房配备防盗报警系统或设置有专人值守的视频监控系统。

（4）防雷

各类机柜、设施和设备等要通过接地系统安全接地并采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

（5）防火

配备火灾自动消防系统，自动检测火情、自动报警，并自动灭火。机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料同时对机房划分区域进行管理，区域和区域之间设置隔离防火措施。

（6）防水和防潮

有措施防止雨水通过机房窗户、屋顶和墙壁渗透，防止机房内水蒸气结露和地下积水的转移与渗透同时安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

（7）防静电

安装防静电地板并采用必要的接地防静电措施，防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

（8）温湿度控制

配备温、湿度自动调节设施（空调系统），使机房温、湿度的变化在设备运行所允许的范围之内。

（9）电力供应

配备稳压器和过电压防护设备，配备 UPS 系统，设置冗余或并行的电力电缆线路为计算机系统供电。

（10）电磁防护

电源线和通信线缆隔离铺设，避免互相干扰。对关键设备实施电磁屏蔽。

技术措施实现或涉及产品：

分类	安全控制点	对标产品	技术措施
安全物理环境	**物理位置选择**		1、机房选址：机房场地建筑应具有防震、防风和防雨等能力 2、机房选址：机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施
	物理访问控制	电子门禁系统	
	防盗窃和防破坏	防盗报警系统 / 视频监控系统	1、设备固定+设备标签 2、通信线缆铺设在隐蔽安全处
	防雷击	防雷保安器或过压保护装置	1、电路设计：各类机柜、设施和设备等通过接地系统安全接地
	防火	火灾自动消防系统	1、机房建设-耐火材料 2、机房划分区域进行管理，区域和区域之间设置隔离防火措施
	防水和防潮	防水检测、报警设备	1、窗户、屋顶、墙壁的防水方法 2、防地下积水的转移与渗透：排水沟
	防静电	静电消除器、防静电手环	防静电地板，并设备接地
	温湿度控制	机房空调/精密空调	

分类	安全控制点	对标产品	技术措施
	电力供应	稳压器、UPS	冗余或并行的电力电缆线路为计算机系统供电（三级要求）
	电磁防护	屏蔽柜、屏蔽机房	电源线和通信线缆应隔离铺设

4.2.2 安全通信网络

安全通信网络从网络架构、通信传输和可信验证三个方面进行设计和安全防护。

（1）网络架构

网络结构是网络安全的前提和基础，对信息系统合理规划网络，绘制与当前运行情况相符的网络拓扑结构图，通信线路、关键网络设备的硬件冗余，保证系统的可用性，网络结构设计时应重点关注的方面；根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN，业务终端与业务服务器之间建立安全路径；存放重要业务系统及数据的网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域；通过网络设备流量控制等技术手段保证重要业务不受网络拥堵影响，保证网络设备的业务处理能力满足业务高峰期需要及各个部分的带宽满足业务高峰期需要；

（2）通信传输

使用 VPN 设备或采用 PKI 体系中的完整性校验功能进行完整性检查，保障通信完整性及通信过程中敏感信息字段或整个报文的保密性。

（3）可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

技术措施实现或涉及产品：

分类	安全控制	对标产品	技术措施

	点		
安全通信网络	**网络架构**	负载均衡，上网行为管理、综合网管系统 下一防火墙/路由器/交换机	1、干路设备、边界设备、汇聚层以上的设备、安全设备等设备性能冗余空间充足（路由器、交换机和防火墙提供网络通信功能的设备） 2、带宽在设计要求上满足需求上要有一定比例的冗余 3、划分 VLAN 4、关键网络设备及安全设备要求冗余配置（如核心交换机、AD、AF、AC 等）
	通信传输	VPN	客户端到服务器、服务器到服务器之间要使用 SSL 等通信
	可信验证		此要求项为“可”而非“应。用户可根据实际需要选择性确认实现此安全要求。如使用可信服务器，可信操作系统等

4.2.3 安全区域边界

（1） 边界防护

部署访问控制设备，保证跨越边界的访问和数据流通过边界防护设备提供的受控接口进行通信；部署准入设备或其他安全措施对非授权设备私自联到内部网络的行为进行限制或检查以及对内部用户非授权联到外部网络的行为进行限制或检查对使用无线网络时在边界部署下一代防火墙等安全设备保证无线网络通过受控的边界防护设备接入内部网络。

（2） 访问控制

信息系统边界是安全域划分和明确安全控制单元的体现。在网络边界部署防火墙，对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为，基于应用协议及应用内容进行访问控制。

针对网络内部各区域之间的访问，采用防火墙及 VLAN 划分进行控制。在核心交换机上设置访问控制列表策略，禁止终端用户对安全管理区的直接访问。重要网段及设备进行 IP 与 MAC 地址绑定。

采用安全认证网关结合信任服务系统对访问应用系统提供访问控制和身份鉴别；具有登录失败处理功能，失败后采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施。

（3） 入侵防范

通过在出口边界部署入侵防御设备，利用入侵防御设备的深度检测功能，对网络中的威胁流量进行识别，及时发现并阻断网络中的异常入侵行为。

通过在核心交换机旁路部署入侵检测设备，利用入侵检测设备的动态检测功能，对网络中的流量进行监测，并定期对入侵检测设备的特征库进行升级，及时发现网络中的异常行为。

（4） 恶意代码防范和垃圾邮件防范

部署网络版防病毒软件，及时进行升级更新；进行漏洞扫描，及时进行系统补丁更新。部署防病毒网关，对网络中的恶意代码进行查杀，同时和主机防病毒使用不同的特征库。

部署防垃圾邮件系统保障在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。

（5） 安全审计

通过部署网络审计系统，对网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录的留存时间 6 个月以上且不中断。对远程访问的用户行为、访问互联网的用户行为通过 AC、SSL VPN 等设备单独进行行为审计和数据分析。

（6）可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

技术措施实现或涉及产品

分类	安全控制点	对标产品	技术措施
安全区域边界	**边界防护**	下一防火墙、网闸、路由器和交换机	端口级访问控制
		上网行为管理、终端管理系统、安全感知平台、	1、控制非法联入内网（可使用安全设备满足或技术措施如 MAC 绑定） 2、控制非法联入外网 3、无线网络通过受控的边界设备接入内部网络

分类	安全控制点	对标产品	技术措施
	访问控制	下一代防火墙、网闸、路由器和交换机 WEB 防护防火墙、上网行为管理	1、边界访问控制策略（网闸、防火墙、路由器和交换机等提供访问控制功能的设备） 2、对进出网络的数据流实现基于应用协议和应用内容的访问控制。（传统的防火墙无法满足，必须使用 WAF）
	入侵防范	下一代防火墙、IPS、安全感知平台、抗 APT 攻击、抗 DDoS 攻击和网络回溯等系统	1、关键网络节点双向（外部发起攻击和内部发起攻击行为）网络攻击行为检测、防止或限制 2、实现对网络攻击特别是新型网络攻击行为的分析
	恶意代码和垃圾邮件防范	下一代防火墙+AV 模块 \ 防毒墙网关 ； 邮件安全网关	1、防御网络恶意代码 2、垃圾邮件进行检测和防护
	安全审计	日志审计系统、堡垒机、上网行为管理、下一代防火墙、SSL VPN	1、（综合安全审计系统、路由器、交换机和防火墙等设备）启用日志功能 2、应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖 3、对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析
	可信验证		此要求项为“可”而非“应。用户可根据实际需要选择性确认实现此安全要求。如使用可信服务器，可信操作系统等

4.2.4 安全计算环境

计算环境对定级对象中的服务器、终端、网络安全设备等设备及数据进行安全防护，从身份鉴别、访问控制、安全审计、可信验证、入侵防范、恶意代码防范、数据完整性、数据保密性、数据备份恢复、剩余信息保护及个人信息保护等几个方面进行防护。

（1）身份鉴别

通过部署 CA 认证系统（或其他双因素鉴别产品）或进行主机配置项，对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换（如配置用户名/口令，口令采用 3 种以上字符、长度不少于 8 位并定期更换，启用登录失败处理功能，登录失败后采取结束会话、限制非法登录次数和自动退出等措施）；通过部署 SSL VPN 或堡垒机等安全防护保证进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听。

（2）访问控制

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

在交换机和防火墙上设置不同网段、不同用户对服务器的访问控制权限。

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

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

（3）安全审计

日志审计系统、数据库审计、上网行为审计等安全设备的部署实现设备和计算的安全审计，同时对主机系统、安全设备、交换机等根据需求开启设备自身审计功能，审计设备连接至单位 NTP 服务器保证了审计记录产生时的时间由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计日志保存 6 个月以上，应对审计进程进行保护，防止未经授权的中断。

（4）入侵防范

针对信息系统的主机系统入侵防范采取操作系统遵循最小安装的原则，仅安装需要的组件和应用程序，关闭不需要的系统服务、默认共享和高危端口；终端安全管理系统或设备配置项设置对终端接入范围进行限制。并通过设置升级服务器或通过补丁分发系统保持系统补丁及时得到更新，增强抵御入侵的防护手段。EDR（终端检测响应系统）或网络防病毒系统的部署能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

（5）恶意代码防范

在所有终端主机和服务器上部署网络防病毒系统，加强终端主机的病毒防护能力并及时升级恶意代码软件版本以及恶意代码库。

部署防病毒网关，对网络中的恶意代码进行查杀，同时和主机防病毒使用不同的特征库。

（6）可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

（7-8）数据完整性、保密性

在数据完整性和保密性方面，通过部署 VPN 实现网络传输层数据的完整性和保密性防护，如通过 VPN 设备实现同城/异地备份中心的传输加密；对于特别重要的数据，使用数据加密系统实现关键管理数据、鉴别信息以及重要业务数据存储的完整性和保密性。

对鉴别信息、重要业务数据进行加密传输和存储，即确保传输的数据是加密后传输和存储。用户名和密码及填报数据需要加密后再存储到数据库，以防获取系统重要信息，避免造成信息泄露。

通过链路加密设备对数据进行保密性防护；应用系统在设计时，需要充分考虑抗抵赖要求。

（9）数据备份与恢复

数据备份是指为防止系统出现操作失误、系统故障或人为因素而破坏数据的可用性和完整性，而将全系统或部分数据集合复制到其它的存储介质的过程。数据恢复则是根据需要，利用有效备份数据把数据还原到指定时间点的过程。

在数据备份和恢复方面，提供重要数据的本地备份和恢复功能，异地实时备份；提供重要数据处理系统（包括边界交换机、边界防火墙、核心路由器、应用服务器和数据库服务器等）的热冗余，保证系统的高可用性；通过部署备份和恢复系统，建立备份中心，利用通信网络将重要数据实时备

份至备份场地,实现数据的备份和恢复。重要应用系统每天进行一次完全数据备份，备份介质场外存放，指定备份恢复策略；对主要网络和安全设备的策略，定期导出进行备份。

可以在系统管理运维域部署数据备份恢复系统，实现对核心生产系统和 DMZ 区域的重要数据资源实现不同安全策略的备份，并制定定期恢复测试计划，实现定期恢复测试，验证备份数据的完整性。

（10）剩余信息保护

对残余信息的风险进行防范，保证用户的残余信息所在的存储空间在退出时被释放或再分配给其他用户前得到清除。

在设备更换时，对数据完全擦除，对单个文件、文件夹以及磁盘剩余空间做清除。

（11）个人信息保护

确保仅采集和保存业务必需的用户个人信息；通过 AC 等设备的部署或应用配置项，通过访问控制限制对用户信息的访问和使用进行限制，实现对禁止未授权访问和非法使用用户个人信息。

技术措施实现或涉及产品

分类	安全控制点	对标产品	技术措施
安全计算环境	**身份鉴别**	VPN、运维堡垒主机 CA 证书	1、主机配置项：设备设置登录认证功能；用户名不易被猜测，口令复杂度达到强密码要求（对象：终端和服务器等设备中的操作系统、数据库系统和中间件等系统软件及网络设备和安全设备。） 2、主机启用设备自身策略：密码策略、用户管理、登录失败处理功能，启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施 3、远程管理时，使用 SSH、HTTPS 加密 4、双因素认证（用户名口令、动态口令、USBkey、生物特征等鉴别方式）

分类	安全控制点	对标产品	技术措施
	访问控制	下一代防火墙，VPN 运维堡垒主机，WAF 水印系统	1、主机配置项：登录的用户账户和权限合理分配 2、重命名或删除默认账户，修改默认账户的默认口令 3、及时删除或停用多余的、过期的账户，避免共享账户的存在 4、最小权限，管理用户的权限分离（三权分立） 5、合理分配访问控制策略：访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；设置安全标记
	安全审计	下一代防火墙、日志审计系统	启用安全审计
	入侵防范	下一代防火墙、IPS、堡垒机、漏洞扫描系统 上网行为管理、安全感知平台、EDR 主机 IPS	1、操作系统遵循最小安装原则，仅安装需要的组件和应用程序 2、关闭不需要的系统服务、默认共享和高危端口 3、配置终端接入方式、网络地址范围 4、系统配置项（如登录对输入框输入的内容进行长度、位数及复杂度验证等） 5、及时发现并修复已知漏洞 6、能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
	恶意代码防范	EDR 杀毒	安全杀毒软件并及时更新库
	可信验证		此要求项为“可”而非“应。用户可根据实际需要选择性确认实现此安全要求。如使用可信服务器，可信操作系统等

分类	安全控制点	对标产品	技术措施
	数据完整性	VPN、CA	系统使用 HTTPS，SSL
	数据保密性	VPN、数据加密软件	
	数据备份恢复	数据备份软件、容灾备份系统	双活热备（三级要求）
	剩余信息保护		应用配置项
	个人信息保护	上网行为管理	应用配置项

4.2.5 安全管理中心

（1） 系统管理

通过系统管理员对系统的资源和运行进行配置、控制和可信及密码管理，包括用户身份、可信证书及密钥、可信基准库、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

配备集中系统和设备管理功能的工具或平台，进行系统管理操作 ，对系统管理操作进行审计；系统或平台需要有三权分立，使用系统管理员对系统的资源和运行进行配置、控制和管理 。（如运维堡垒机、SOC 平台、CA 认证服务器等）

（2） 审计管理

通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行处理。对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

配备集中系统和设备管理功能的工具或平台，系统或平台需要有三权分立，审计管理员是否通过管理工具或平台进行安全审计操作 。（如运维堡垒机、日志审计系统等）

（3） 安全管理（三级及以上系统要求）

通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置可信验证策略，维护策略库和度量值库。应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

配备集中系统和设备管理功能的工具或平台，系统或平台需要有三权分立。设立安全管理员，安全管理员不能兼任其他岗位（如系统管理员、审计管理员、机房管理员等）。

（4） 集中管控（三级及以上系统要求）

安全运维区的划分，保证了对分布在网络中的安全设备或安全组件进行集中管控；通过堡垒机实现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。APM 或安全管理平台的部署对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测，日志审计系统部署实现分散在各个设备上的审计数据进行收集汇总和集中分析。检测探针+安全感知平台应能对网络中发生的各类安全事件进行识别、报警和分析。网络防病毒系统及补丁分发系统的部署应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

技术措施实现或涉及产品：

分类	安全控制点	对标产品	技术措施
安全管理中心	**系统管理**	运维堡垒机、网管系统等	
	审计管理	数据库审计、日志审计、运维堡垒机	
	安全管理	运维堡垒主机等	
	集中管控	运维堡垒机、BBC 集中管理平台、网管平台 数据库审计、日志审计系统、安全感知平台 EDR 管理平台、补丁分发系统	1、划分运维管理域，安全设备或安全组件集中管理 2、建立一条安全的信息传输路径 3、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 4、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 6 个月以上； 5、对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理 6、能对网络中发生的各类安全事件进行识别、报警和分

分类	安全控制点	对标产品	技术措施
			析。

4.3 安全建设建议清单

序号	产品名称	描述	数量	单位
互联网出口域				
1	下一代防火墙	三层吞吐量 4G，应用层吞吐量 600M， 硬件参数：1U，4G 内存，SSD 64G 硬盘，单电源，4 个千兆电口+4 个千兆光口；	2	台
2	上网行为管理	推荐带宽性能 200Mb， 支持用户数 1400；硬件指标：1U，4G 内存，1TB 硬盘， 单电源，2 对 ByPass 口，4 个千兆电口+2 个千兆光口 ，1 个串口(RJ45) ，2 个 USB2.0	2	台
3	负载均衡	吞吐量 5Gbps， 并发连接数 3,000,000 4 层新建连接数 CPS150000 7 层新建连接数 RPS70,000 内存 4GB，硬盘 SSD 128GB 6 个千兆电口，2 个千兆光；	2	台
核心业务域				
4	下一代防火墙	三层吞吐量 4G，应用层吞吐量 600M，并发连结数 180W，新建连接数（CPS）40000 个， 硬件参数：1U，4G 内存，SSD 64G 硬盘，单电源，4 个千兆电口+4 个千兆光口；	3	台
分支接入区域				
7	下一代防火墙	三层吞吐量 4G，应用层吞吐量 600M，并发连结数 180W，新建连接数（CPS）40000 个，SSL VPN 接入数（最大）1000 个，IPSec VPN 隧道数（最大）1000 个，硬件参数：1U，4G 内存，SSD 64G 硬盘，单电源，4 个千兆电口+4 个千兆光口；	1	台
8	上网行为管理	推荐带宽性能 200Mb，支持用户数 1400；硬件指标：1U，4G 内存，1TB 硬盘， 单电源，2 对 ByPass 口，4 个千兆电口+2 个千兆光口 ，1 个串口(RJ45) ，2 个 USB2.0	1	台
运维管理域				

9	安全感知平台	2U，96G 内存，SSD 128G 系统盘、SATA 32T 存储、双电源，RAID50、标配 4 个千兆电口； 安全感知平台基于海量的安全数据，通过机器学习、UEBA、关联分析等智能技术，帮助客户看清业务、感知威胁、及时预警、快速响应。	1	台
10	堡垒机	含 150 个运维资源授权，提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护三级建设要求	1	台
11	数据库审计	单向数据库流量 400M 硬件指标：1U，单电源，6 个千兆电口+2 个千兆光口，2TB SATA 硬盘	1	台
12	日志审计	含 150 个主机审计许可证书,配备 2*1T 的硬盘,采用 raid1 的技术，实际可用是 1T，6 个千兆电口，接口可扩展；支持获取各种主流网络及数据库访问行为，支持 Syslog、WMI、OPSEC Lea、SNMP trap 和 LAS-1000 专用协议等协议事件日志，支持通过 Http、Https、FTP、SFTP、SMB 等协议获取各类文件型日志，支持基于 SQL/XML 标准内容获取；	1	台
13	潜伏威胁探针	性能指标：3Gbps，硬件指标：2U，SATA 1T、双电源，标配 6 个千兆电口+4 个千兆光口+2 个万兆光口； 潜伏威胁探针主要通过旁路部署方式对全流量信息进行采集	1	台
内网办公区域				
15	下一代防火墙	三层吞吐量 4G，应用层吞吐量 600M，并发连结数 180W，新建连接数（CPS）40000 个，； 硬件参数：1U，4G 内存，SSD 64G 硬盘，单电源，4 个千兆电口+4 个千兆光口；	1	台

5. 安防系统工程

为了保证生产管理的安全，本次将在新建园区设计安防系统。系统包含：

1.1 视频监控系统

1.2 电子巡查系统

1.3 周界防入侵报警系统

5.1 视频监控系统

园区视频监控前端的布控点主要是对园区内的办公区域、生产区域、车间、厂房等办公场所进行部署设置。

5.1.1 园区视频监控总体设计思路

园区监控覆盖的范围广，监控点多且分散。包括、泊位、堆场、仓库、航道、区内的区道路、路口、卡口通道等重点区域，主要涉及陆路货物运输体系监控、作业体系监控、堆场仓库作业体系监控、区周界安防、区楼宇监控及区区道路监控六大监控体系，对园区生产要素（堆存、集装箱、装卸机械、车辆、人员）及周界进行可视化管理和防控。从上述六大监控体系建设实际需求出发，我司对于园区视频监控总体设计思路如下：

1）立足于园区监控建设现状及需求的，基于高起点的监控系统设计，建设统一的区综合视频监控平台。园区综合视频监控平台实现所有图像资源的集中管理，保证联网视频传输的质量，提供一个视频信息资源的统一监控检索系统，充分发挥园区综合视频监控系统在加强园区运营管理，提高园区生成效率、确保作业质量和作业安全等方面的作用。

2）强调系统全局实时监控性，实时可视化直观显示作业机械（岸桥、场桥、叉车/正面吊、内部拖车）的位置/状态、外部拖车的预定位置、堆场、集装箱、仓库、闸口、建筑、灯塔、区道路、交通标志、前沿、缆桩、泊位、船舶等各要素。

3）强调系统的实战性，一切围绕区管理与服务对于视频图像应用的业务需求，实现系统的日常监控管理、应急指挥调度；

4）强调系统的联动，实现区综合视频监控系统与区监控中心各个信息系统之间的互联互通，真正实现园区的全局视频图像资源的联网共享，建立全方位的、立体的、多层次的高清智能综合视频监控系统，实现“上下一盘棋”；

5）强调系统的兼容性、可靠性、可扩展性，提升系统的可靠性也可以实现将来与多级第三方系统互联互通的要求。

6）整合各类不同来源、不同格式的图像资源，实现视频图像信息系统的数字化、网络化和智能化，具备信息资源管理、设备管理、用户管理、网络管理、安全管理等功能；

7）以园区个业务单位监控业务需求为导向，依托系统之间的有效关联和对接以及系统平台的业务开发能力，为各园区业务部门提供实战支撑。

8）建设统一的园区视频图像信息数据库，该视频图像数据库是园区各业务单位防控、应急和园区经营管理的核心视频图像库，是园区视频监控与报警的数据中心。分级建立视频图像信息数据库，对各园区业务部门关注的视频图像信息进行整理、分类存储，通过视频图像信息与园区各业务单位所关注的事件、人员进行有效关联，方便园区各业务部门进行情报分析研判且视频图像信息数据库采取动态管理方式，以确保入库信息的及时性、准确性和有效性。

5.1.2 视频系统总体架构设计

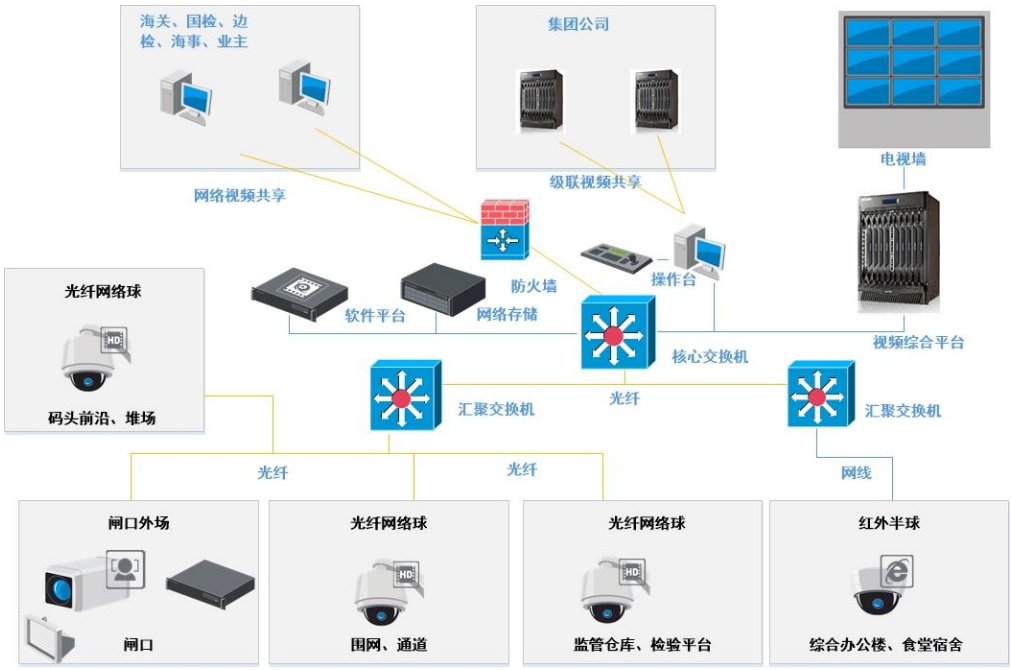


图1. 系统组成结构图

1）系统将查验站、集装箱货运站、、重箱/空箱堆场、变电所、仓库等室外 IP 监控点（或高清监控点）、办公大楼监控点、食堂宿舍楼、闸口高清抓拍监控点接入统一平台；

2）系统采用视频综合平台实现数字视频信号、IP 视频信号的统一切换、控制、输出显示、级联共享；

3）系统采用网络磁盘阵列实现录像数据的集中存储和录像取证保存；

4）系统采用视频监控软件平台实现系统集中管理、可视化应用等。

5）系统支持公司、海关、海事、边检等多个交叉部门共享视频资源，并支持统一协调和应急指挥。

5.1.3 系统安全设计

1）设备安全

本安防系统使用电气设备和主机的电气安全和防雷安全指标符合国家和行业的相关标准，为确保使用人员和设备的安全可选用先进的防雷设备（可选），整体防雷设施建议采用三级防雷方式，即：前端设备防雷、大楼电源防雷、机房电源与设备防雷。

2）数据安全

建立完善的数据备份与恢复机制。保证数据不因物理介质的损坏丢失。数据采取有效的加密保护措施，确保数据的安全。

3）系统安全

监控系统软件和存放监控系统信息的所有主机和系统应的严格的身份认证机制，防止对系统的非法侵入。监控主机的操作系统和软件系统建立完善的备份和灾难恢复机制，确保系统被损坏后的快速恢复。由系统需要采用远程监控,建议采用防病毒措施，安装杀毒功能强大的正版杀毒软件，并及时升级。

5.1.4 系统组成

园区综合监控系统主要包括高清视频监控子系统、区道路监控子系统、出入口子系统和周边防范子系统、其中高清视频监控子系统包括各监管场景，包括、堆场、仓库、办公区、园区水域等。

5.1.4.1 实时监控

实时监控是整个监控系统最基本的功能，在用户的日常安全管理中，也是最基本的监控模式。本系统的实时监控功能提供了全方位的操作体验，能够满足用户各种实时监控需求。

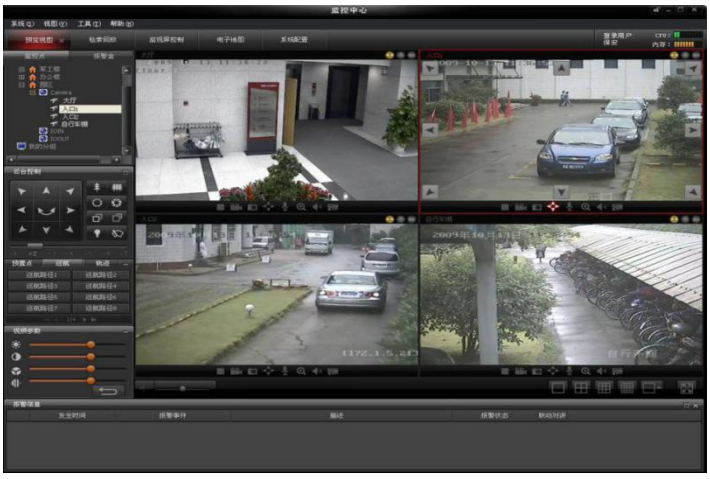


图2. 实时监控界面

1）高清监视：支持显示 1280*720、1280*960、1600*1200、1920*1080 等多种高清分辨率图像，并向下兼容 4CIF/DCIF/CIF/QCIF 等标清格式；

2）多级监控：支持多级视频监控，并可实现跨部门、跨业务单位视频资源共享；

3）PTZ 控制：支持无延时切换显示模拟视频信号和高清数字视频信号，支持低延时切换显示 IP 视频信号。

5.1.4.2 存储回放

系统采用的是录像集中存储管理策略，既考虑到视频资源的集中管理，同时也支持各个子系统对中心存储的录像文件的灵活共享，做到了资源的有机整合和高效利用。

检索回放功能能够帮助用户追溯历史事件，在日常安全事件的查找、处理和取证中发挥着重要的作用。

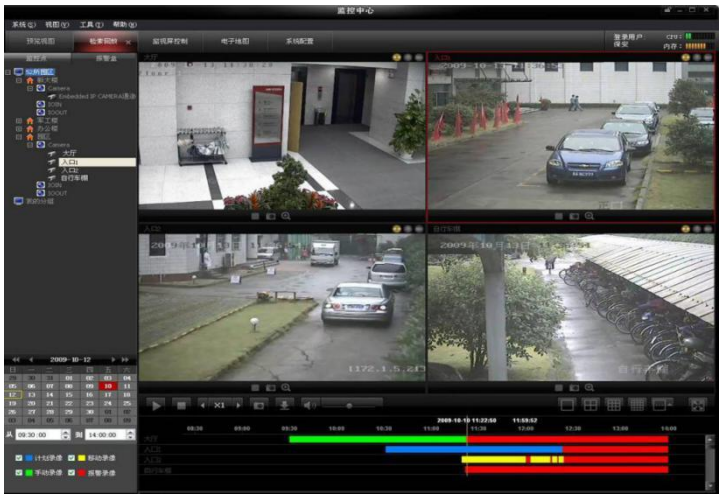


图3. 视频回放界面

1）视频录像：同时保存标清视频录像和高清视频录像，支持 NAS/IPSAN/SDK 等多种存储技术，支持定时录像、手动录像、报警录像等多种存储方式；

2）检索回放：支持手动检索、智能检索等；

3）取证迁移：支持将人工浏览确认的录像文件截取保存，保存周期一般为 1-3 年。

5.1.4.3 电子地图

该功能将系统的抽象信息和真实的现场环境有效的结合在一起，能够更好的帮助用户理解系统的实际结构，指导其处理日常的事务。

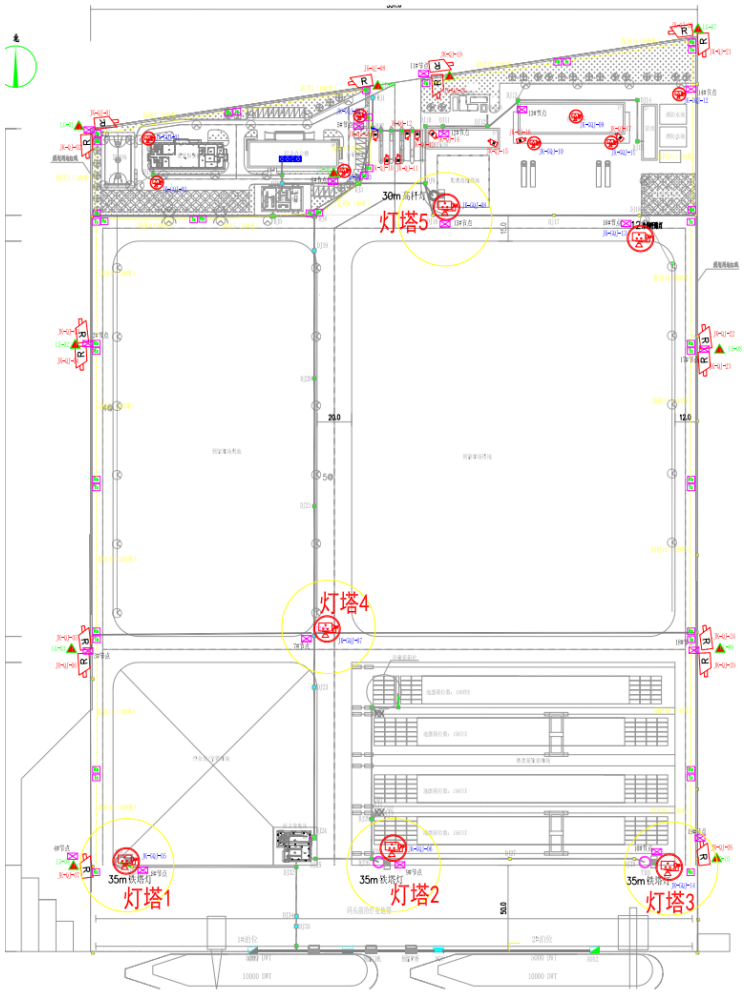


图4. 电子地图

1）可视操作：将实时监控、录像检索、报警联动都集成在电子地图上，支持按区域、按分中心管理系统；

2）联动提示：报警系统、智能分析系统产生的报警信息在电子地图上闪烁提示，并自动弹出报警联动图像。

5.1.4.4 报警联动

系统根据园区作业的多样化提供了丰富的报警类型和报警联动策略，优化了报警信息传递和处理流程，保障了能够对安全事件进行及时的响应和联动。

支持红外报警系统、光纤震动报警系统与视频监控系统互联互动；

支持智能视频分析与视频监控系统互联互动；

支持多种报警类型，包括硬盘满报警，硬盘出错报警，视频丢失报警，视频遮挡报警，移动侦测报警、IO 报警、智能分析事件报警，服务器异常状态报警；

支持多种报警联动策略，联动方式有客户端联动（视频图像、声光显示、信息叠加）、云台联动、通道录像、报警输出联动、EMAIL 通知、短信发送、电子地图、通道抓图、执行预案等方式。

5.1.4.5 运行维护

设备检测：系统支持网管功能，可全面监测节点设备工作状态；

远程升级：系统支持网管中心集中维护和远程升级；

配置管理：系统支持远程修改和配置设备参数。

5.1.5 各部分系统详细设计

视频系统是跨学科跨行业的系统工程，由以下几部分构成：

1） 前端摄像部分

2） 传输部分

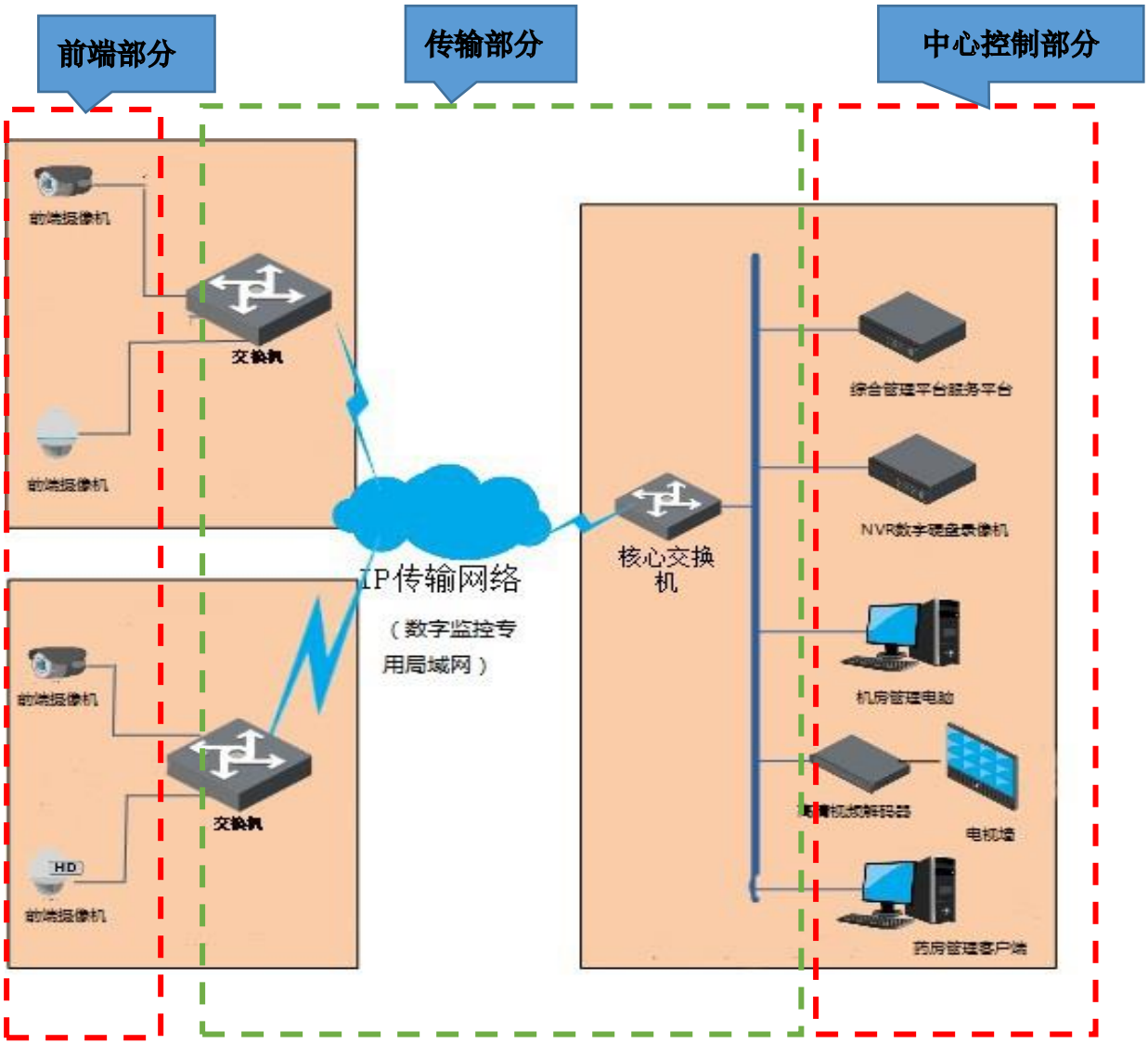
3） 中心控制部分

前端摄像部分是电视监控系统的前沿部分，是整个系统的“眼睛”，它把监视的内容变为图像信号，传送控制中心的监视器上，摄像部分的好坏及它产生的图像信号质量将影响整个系统的质量。

传输部分是系统的图像信号通道。

中心控制部分是整个系统的“心脏”和“大脑”，是实现整个系统功能的指挥中心。

系统拓扑图：



5.1.5.1 前端部分设计

根据摄像机使用环境，选用红外枪机、红外高速球 2 种类型的摄像机，具体分布如下：

序号	位置	变焦枪机	枪机	半球	高速球	双光谱全彩摄像机
1	西北围墙角	2				
2	西面围墙角 1	2				
3	西面围墙角 2	2				
4	西南围墙角	2				
5	值班室	6	1	1	1	
6	中心变电所		6			4
7	灯塔 4				2	
8	灯塔 1				2	
9	灯塔 2				2	
10	前方变电站		3			
11	灯塔 3				2	
12	机修车间		11			
13	查验仓库	2	2		3	
14	灯塔 5				1	
15	东面 12 米路灯				1	
16	东北面围墙	2			1	
17	北面出入口围墙角	2				
18	东面围墙角 1	2				
19	东面围墙角 2	2				
20	东南围墙角	2				
21	办公楼 1 楼机房		2	23	1	
22	食堂宿舍楼 2 楼备份机房		3	7	3	
23	**合计**	**26**	**28**	**31**	**19**	**4**

前端监控点主要分为两类，一类是室内监控点，一类是户外监控点。

5.1.5.1.1 室内监控点

室内监控点主要根据室内装潢和监控功能进行摄像机选型。根据本项目的实际情况，共选用以下 4 款摄像机：

1）200 万像素星光级高清红外网络智能球：安装于综合办公楼大厅，监控范围广，可根据管理人员监控需求进行巡检监控；

2）200 万像素高清红外枪网络摄像机：用于室内没有吊顶部分的监控，采用壁挂安装，满足实际监控安装高度，具有强光抑制功能，夜间监控效果佳；

3）200 万像素星光级高清红外半球网络摄像机：用于室内有吊顶部分的监控，采用吸顶安装，整体美观；

4）双光谱全彩摄像机：配合轨道自动化，用于监控配电柜内的具体情况，满足管理人员远程监视配电柜。

5.1.5.1.2 户外监控点

户外监控点安装相对复杂，根据现场物理环境选择吊装或壁装，需考虑光纤和电源线走线，同时考虑防雷接地和户外抱杆机柜。

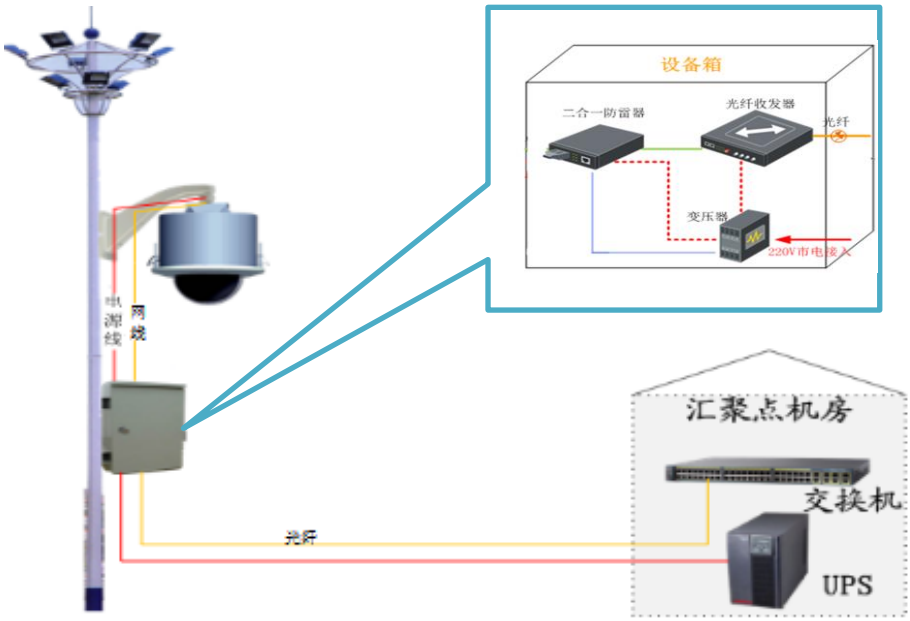


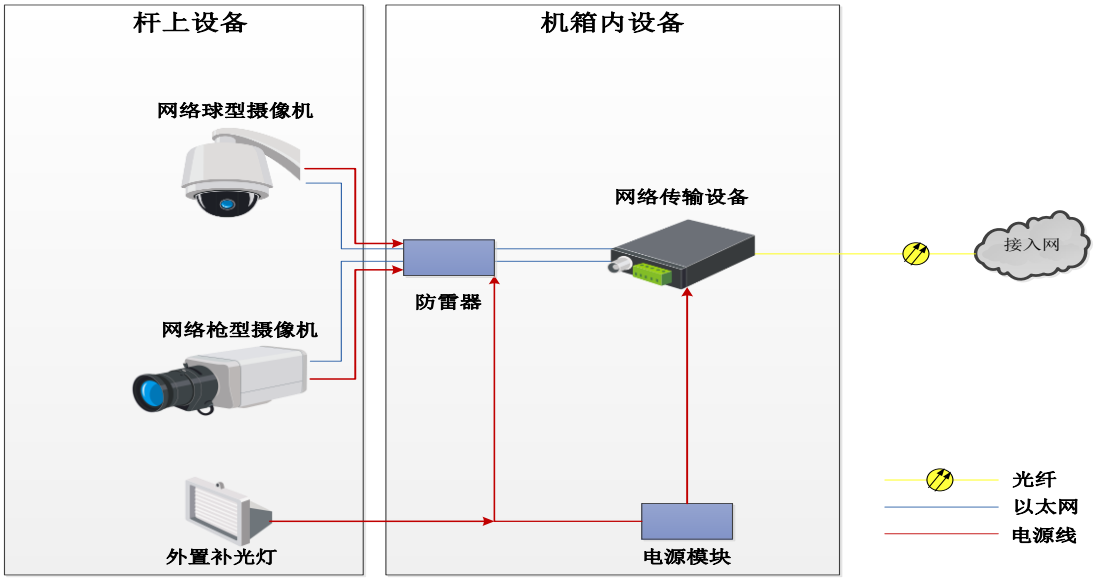
图5. 室外监控点典型连线图

抱杆机箱内部包含防雷器、开关电源、交换机、风扇等等。同时需防雷接地。

5.1.5.2 外场监控设计

5.1.5.2.1 监控点设计

针对具体监控点位的实际情况，摄像机设备、补光灯部署于监控立杆，网络传输设备、光纤盒、防雷器、电源等部署于室外智能机箱。监控网络摄像机前端部署架构图如下图所示：



监控点部署架构图

5.1.5.2.2 监控杆件

监控点根据区道路现场实际情况，可采用立杆安装方式。监控立杆设计考虑整体杆件的设计、立杆材质、杆型、焊接工艺、表面处理以及杆体颜色等。

立杆为 304 不锈钢立杆（大头Φ200，小头Φ120），高度为 8m。根据项目点位分布共设置 10 根立杆，其余均利用路灯杆和灯塔。

采用立杆固定时，杆底端焊接固定法兰盘，预留拉线孔，地基应是硬质，同时根据现场安装点的地质的实际情况，调整相应的尺寸。立杆的安装应牢固，不得歪斜，需用水平仪来测定；制作要美观，其顶部应做防水帽。立杆应有较高强度，抗台风、防腐蚀、防摄像机抖动、防攀爬、防腐。立杆基础规格按不同的杆体进行分别设计。

5.1.5.2.3 室外机箱

1）通过对运行维护需求、实际地理环境和气候、安全性、稳定性分析新建室外机箱应采用智能机箱。根据各监控点位摄像机数量和其他接入设备要求在箱体内部应配置相应的电源配电模块、防雷模块、绕纤盘、接地铜排、散热风扇、防雷插座、以及其他配套模块并预留网络传输设备放置空间。

2）分析其他配套设备的数量和尺寸，保证箱体内部充足空间方便设备安装和维护，同时应与杆体大小协调。

3）用于箱体的金属材料应具备抵抗腐蚀、电化学反应、防酸雨能力，监控箱结构为露天环境使用设计，应具有良好的防水、防尘、散热、防盗、防寒、防曝晒结构。

5.1.5.2.4 防雷接地

为保护摄像机不受到直接雷击而在立杆上设计安装避雷针，并和立杆一次成型。在设备箱内我们对电源、信号线安装相应的防感应雷措施，采用二合一防雷模块。

本方案严格执行国家的有关标准和规范，立杆防雷接地电阻≦10Ω。

接地网布置依据地形进行设计。立杆的基础由钢筋网加混凝土构成，首先用四根Φ50 毫米的钢管或 50×50×5㎜ 的角钢作为接地极，同时用镀锌扁钢把四根接地极焊接形成接地网的一部分，再此接地网与法兰盘进行焊接，钢管或角钢需经过热镀锌工艺处理，以增加抗腐性能和提高其导电性能。当土壤电阻率太高而不能满足要求时，采用垂直接地极＋减阻剂的方法使地网接地电阻符合要求。

5.1.5.3 传输部分设计

中间传输部分主要分为前端供电和网络传输 2 部分。

5.1.5.3.1 前端供电

系统前端设备视工程实际情况，采用集中供电。集中式供电：适用于前端监控点在一个区域内相对比较集中的情况采用集中供电具有电源质量相对稳定，产权分界明晰和易于维护的优点，也是前端感知系统主要采用的供电方式。

（1）主干电源：由中心机房的 UPS 配电箱引主干电源 YJV3*4 至 13 个光纤汇聚点和 1 个备用机房汇总点的配电箱。

（2）分支电源：由光纤汇聚点配电箱引 RVV3*2.5 给光纤节点供电，再经 RVV3*1.0 给前端摄像机供电。

5.1.5.3.2 传输网络设计

四级网络结构，监控点—前端光纤节点—前端汇聚点—中心交换，并预留海关、还是、边检及综合布线工程的主干光纤，实现公司、海关、海事、边检的可光纤互联互通；满足后期扩容需求。

视频监控系统信号线缆传输分为数字信号传输和光信号传输 2 部分，系统利用络线将摄像机的视频信号传输至各个光节点，再通过分支光纤和主干光纤将光信号传输至监控中心。

（1）数字信号传输

采用六类网络线进行传输；

（2）光信号传输

分为主干光传输和分支光传输 2 部分：

1）主干光纤：设置 13 个光纤汇聚点和 2 个光纤汇总点，采用 12 芯、24 芯和 48 芯光缆作为主干；

2）分支光纤：由汇聚点引 4 芯或 8 芯单模光纤至每个分节点。

主干光纤传输分布如下：

光纤编号	位置点	汇聚点编号	光纤芯
办公楼机房至前端汇聚点			
G1	办公楼 2 楼弱电间	1#	12 芯
G2	办公楼 4 楼弱电间	2#	12 芯
G3	闸口	3#	12 芯
G4	仓库	4#	24 芯
G5	左侧围墙	5#	24 芯
G6	灯塔 5	6#	12 芯
G7	右侧围墙	7#	24 芯
G8	灯塔 4	8#	24 芯
G9	灯塔 1	9#	12 芯
G10	灯塔 2	10#	24 芯
G11	灯塔 3	11#	12 芯
G12	备份机房	12#	48 芯
备份机房至前端汇聚点			
G13	宿舍楼 2 楼弱电间	11#	12 芯
G14	宿舍楼 4 楼弱电间	12#	12 芯
G15	闸口	3#	12 芯
G16	仓库	4#	12 芯
G17	灯塔 5	6#	12 芯
G18	灯塔 1	9#	12 芯
G19	灯塔 3	11#	12 芯

5.1.5.4 监控中心

监控中心分为数据中心、管理中心和分控中心三部分。

5.1.5.4.1 数据中心

数据中心设置于综合办公楼数据中心机房，用于放置视频监控中心的核心设备，保障监控数据的稳定。

在数据中心机房设计以下设备：

1）1 台视频综合管理平台：为系统提供平台支撑，保障系统稳定运行；

2）2 台网络存储服务器和 59 块 6T 企业级硬盘：满足视频监控系统图像存储的 90 天的要求；

3）1 台核心交换机、1 台汇聚交换机和 3 台接入层交换机：为智能化系统建设智能专网。

5.1.5.4.2 管理中心：

管理中心位于综合办公楼消防监控室，中心设计 1 台控制键盘、1 台 4 路高清解码器、1 台管理客户端（甲供）和 1 套由 4 台 75 寸液晶大电视拼接成 2x 2 液晶大电视墙（甲供）。满足管理人员能够在液晶拼接墙上显示超高分辨率的应用程序，高清视频等的综合显示，形成一个查询准确、显示全面、操作便捷、管理高效、美观实用的综合系统，实现对图像的显示管理，满足项目的需求。

5.1.5.4.3 分控中心：

系统在综合办公楼 4 楼中控室，系统配备 1 台 4 路高清视频解码器、1 套管理客户端（**甲供**）和由 2 台 75 寸液晶大电视拼接成 1x1 液晶电视墙（**甲供**），满足分控中心对前端视频监控图像显示、控制和管理的功能。

5.1.6 监控平台功能介绍

5.1.6.1 视频监控与存储

视频监控为 IP 网络监控组成结构，前端高性摄像机的视频信号进行数字转换与存储，再通过专线 IP 网络联网到监控中心的集控平台，各个监控终端可以通过客户端软件在电子地图或树形目录上实现网络监控，进行录像检索，实现在中心以及领导办公室等多级管理。

5.1.6.2 电视墙管理

通过视频解码设备将网络视频信号解码后送上电视墙，指挥中心负责监控的工作位，在客户端计算机上实现对指定区域电视墙的控制和管理。

电视墙上所有屏幕可独立进行显示计划的编程设定，包括显示方式（单屏、四分屏……）、显示顺序、显示位置、解码码流、切换时间等，实现多种模式的图像浏览、分组轮切，并可实现批量图像分组轮切，实现不同的监控模式。（如上班时间模式、下班时间模式、深夜时间模式等等）。

电视墙可设定前端触发联动，比如在夜间探测到有人进出的信号，就可以触发中心在电视墙相应监视器上显示视频图像并录像，同时提醒值班人员的注意，在设定延迟的一段时间之后自动关闭视频连接同时保存报警记录，电视墙恢复到正常状态。而如果是来自报警系统的触发，则在联动图像样的同时，还同时执行报警预案，警情未处理，电视墙不会恢复到正常状态。

5.1.6.2.1 调阅管理

完善的调阅管理功能，调阅权限是经过严格的授权管理的，同时所有的录像数据查看、下载及复制操作都有详细记录，并将相关录像数据保存在专门的服务器上统一管理。

5.1.6.2.2 防盗报警

在现场通过专业的报警主机进行布防、撤防等操作管理。同时报警主机通过专线 IP 网络联网到监控中心的集控平台。

平台具有可视化、智能化管理功能，前端防区发生报警时，中心自动弹出对应的电子地图，实时显示报警区域和报警信息，在电视墙上显示预先关联的视频图像并录像、声光报警同时弹出报警处理预案窗体。接警员选择输入处理方案之后，电视墙视频恢复

到正常状态，同时将处理方案保存下来方便以后查询，如果接警员没有选择处理方案，系统将一直保持现状直接处理为止。

系统可以指定一个或多个监视器用来处理接警视频，并设置处理方案。报警时电视墙将按预先设置好的方案显示视频图像。

因为中心资源有限，所以当多个前端同时报警时，中心采用先入先出排队处理方式处理警情，排队等待处理警情会显示在列表中，操作员可以根据实际选定比较重要的警情优先处理。

5.1.6.2.3 **授权管理**

系统针对每个操作员分配各种功能的操作权限，并对每个功能指定有效操作时间段，只有在有效时间内并具有相关功能操作权限的操作员才可使用相应功能。

系统可设置每个操作员对前端每个摄像机的查看、调阅、下载的权限及时间段。

权限可设置多级优先级，当视频图像访问数大于设置值时，新客户端将无法继续访问该视频图像，如果新客户端的级别比原来访问的客户端级别高，系统将停止级别低的客户端访问该网点视频图像来保证级别高的客户端正常访问。出现紧急事件时，高级领导通过输入用户名和密码在任意一个网点都可以方便的建立起紧急处理中心对突发事件进行即时处理。

系统可按操作员、权限或者摄像机查看方式显示详细的权限信息。

5.1.6.2.4 **操作日志**

可以对系统登陆、设备登陆（如硬盘录像机）、数据下载、报警信息（布、撤防、复位等）等各项目的操作做详细的记录管理。所有用户在登陆系统时要以用户名和密码或刷卡等形式进入，日志会记录登陆人员的姓名、时间、地点、设备和该用户登陆后在系统中所做的重要操作。所有的重要操作日志（包括数据下载、报警信息、系统设置等）都不可以删除。

5.1.6.2.5 **报表功能**

根据用户的实际需求可生成各种记录、统计报表，报表格式可根据用户需求进行定制。生成的报表可以是 Excel、PDF 文件，并且可以直接通过打印机输出。

5.2 巡更管理子系统

5.2.1 系统概述

巡更系统的覆盖面全部涵盖视频安防监控系统的防范死角，在技防的基础上辅以必要的人防，加强人们的安全防范意识，对于小区来说主要是针对保安人员巡查工作的管理，只有建立行之有效的保安管理措施，才能最大限度地发挥技术防范系统的作用。因此通过配置电子巡更子系统，规范保安人员的工作模式，实现“人防”与“技防”的有机结合。

5.2.2 系统设计说明

根据项目特点及实际情况，系统采用离线式巡更系统，由电脑集中管理，同时集合物业管理系统，实现对巡更保安的严格管理，人防与技防高效结合。

系统由巡更点和中心设备统两个部份组成。

5.2.2.1 巡更点设置

✧ 针对本项目食堂宿舍楼和综合办公楼的各个楼层等处设置巡更点，共设置 18 个巡更点，并结合巡更点划分巡更线路。

5.2.2.2 巡更线路设置

✧ 智能化控制中心配置 2 根保安巡更采集器，保安人员携带巡更棒进行巡逻。

✧ 巡更点和巡更线路的设置可具体根据管理要求进行调整。

5.2.2.3 中心管理

✧ 系统中心与综合视频管理平台共用。通讯数据线可将巡更采集器与管理客户端（与视频监控系统共用）连接，在接收巡更棒传送来的信息后，通过软件将对保安人员巡逻情况进行显示、统计并根据需要产生不同的报表。

✧ 监控中心设置交接班 4 个按钮，保安人员巡更前和巡更后在监控中心交接班。

5.2.3 功能功能介绍

✧ 实现对保安巡逻工作的有序管理，合理分配人力。

✧ 帮助管理人员全面掌握保安人员的巡查状况。

✧ 安装使用简便性，便于系统的扩容及操作者的使用。

✧ Windows 操作系统便于管理者的使用，通过软件设置实现各种系统功能。

5.3 周界防入侵报警系统

5.3.1 概述

微电子计算机技术高速发展的今天，应用于防盗报警系统中的技术越来越多，各种设备日趋先进和完善。对于设计者来说最重要的一点是如何将先进的技术和设备有机地加以结合，根据用户的实际情况使系统切实地发挥出安全防范的威力，以达到安全有效防范的目的。

安全防范领域的设备器材品种繁多，性能、价格差别很大。在首先确保系统先进、可靠性的基础上，我们还应该本着为用户负责的原则，使系统具有较高的性能价格比。同时各种功能都应具有其经济实用性，减少浪费投资。

5.3.2 系统需求分析

设置周界防入侵报警系统的目的是：建立安全可靠的生产区域，加强周界的管理，防范区外闲杂人员非法进入，同时防范非法翻阅围墙或栅栏，在防区内出现意外情况时发出报警通知保安部门，满足海关、边检等监管部门的监管要求。

因此，本次周界防入侵报警采用前端探测器配合围网来实现防入侵。由于本项目围墙范围大，为了能够快速的对外来入侵进行及时响应并制止，本系统在周界报警系统设计增加了声光报警联动和视频监控联动。

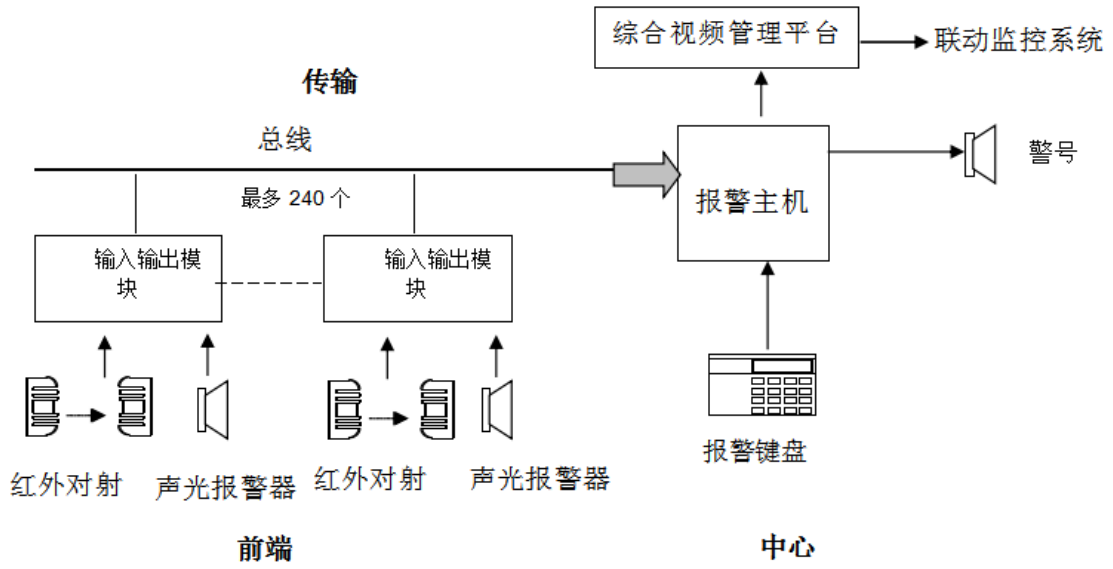
5.3.3 系统组成

周界防入侵报警系统是利用主动红外移动探测器将科技中心的周界控制起来，并连接到保安室的报警监控主机，当外来入侵翻越围墙、栅栏时，探测器会立即将报警信号发送到保安室报警中心，同时启动联动装置和设备，对入侵者进行阻吓，并联动闭路监控系统进行录像存证。

根据扩建货运的实际情况设计如下：

总线制的报警产品，为本项目量身定做了一套周界防范系统。前端红外对射的点位设置主要根据围墙的特点进行点位设置，20 对对射式红外报警探测器，主要用于防止非法人员的侵入。在消控室设立报警监控中心,中心配置报警主机、报警打印机、警号等，并将系统接入综合视频管理平台

周界防入侵报警系统由前端、传输、中心三部分组成，以下就这三部分分别进行阐述。



系统原理图：

5.3.3.1 前端

前端是由周界报警探测器组成，本项目的周界防护采用三光束主动红外对射探测器。

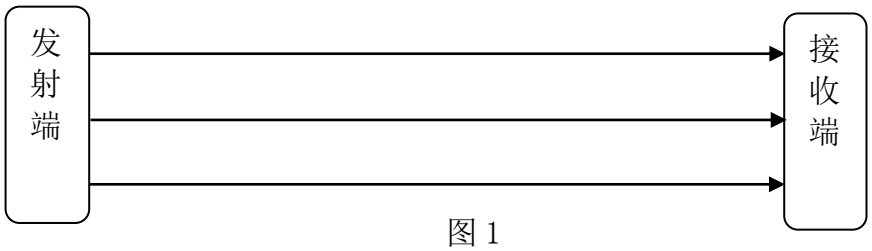


图 1

主动红外对射探头由一个发射端和一个接收端组成。发射端发射经调制后的三束红外线，这三束红外线构成了探头的保护区域（图 1）。如果有人企图跨越被保护区域，则两条红外线被同时遮挡，接收端输出报警信号，触发报警主机报警（图 2）。如果有飞禽（如小鸟、鸽子）飞过被保护区域（图 3），由于其体积小于被保护区域，仅能遮挡一条红外射线，则发射端认为正常，不向报警主机报警。

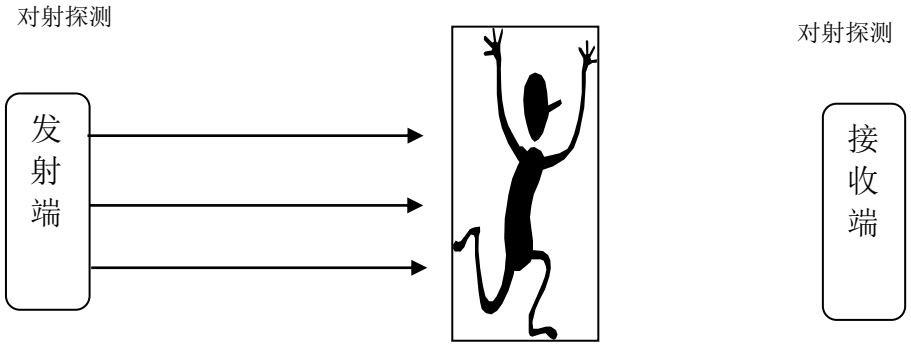


图 2

经过调制的红外线光源是为了防止太阳光、灯光等外界光源干扰，也可防止有人恶意使用红外灯干扰探头工作。

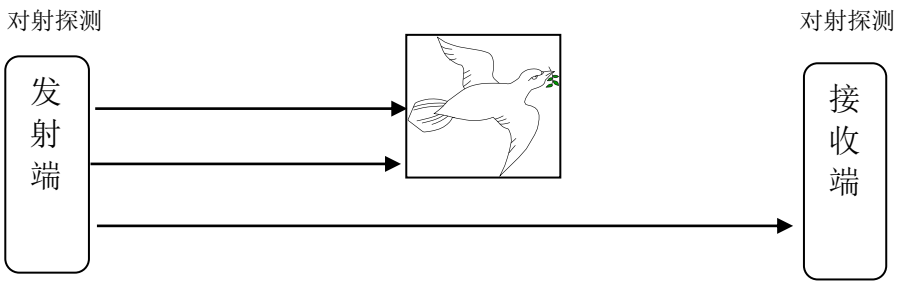


图 3

5.3.3.2 传输

报警信息传输采用双绞屏蔽线 RVV2*1.0，传输到报警监控中心的报警主机。

监控中心集中 220V 强电至前端电源箱，再供电+12V 到前端报警探头（RVV2*1.0）。

周界接收的各种报警信息利用通讯总线传输到报警监控中心主机的报警主机，整个报警系统采用独立开发的通信编码格式，并为其进行了适当地加密，从而保证整个系统在通信上的安全与可靠，防止恶意的复制与侦测，并保证本项目周界报警信号有效、快速的传输到监控中心。前端设备应用地址编码，方便布线。

5.3.3.3 控制中心

控制中心同样设在综合办公楼的消控室，控制中心控制主机及键盘组成。通过键盘或管理软件对前端设备进行布/撤防，在布防期间，若发生非法入侵，当报警被触发时，键盘显示具体报警点，同时键盘和警号开始报警，发出声音告警，提示值班人员注意。加上报警联动，就可将各防区的报警输入同时提供给视频监控系统，视频监控系统根据报警区域位置进行联动自动弹出报警图像，监控中心第一时间查看警情发生区域。本系统可进行报警中心报警状态、报警时间记录。可通过于基于 PC 机上的报警控制软件，直观的显示警情确切位置于报警类型，可记录各种警情，并可将警情详细内容选择性打印出来。

在布防期间，若发生非法入侵，当报警被触发时，显示具体报警点，同时键盘和警号开始报警，发出声音告警，提示值班人员注意。并通过继电器输出模块连接报警输出，联动前端探声光警号开启，视频监控系统根据报警区域位置进行联动摄像机对准警情发生区域，并且相应图像自动在监控中心监视器弹出；同时进行报警中心报警状态、报警时间记录。

5.3.4 周界防入侵报警系统配置

探测器设立：

在围墙上设立 20 对三光束红外对射，其中 100 米 18 对，50 米 2 对。

控制中心：综合办公楼 1 层消控室。

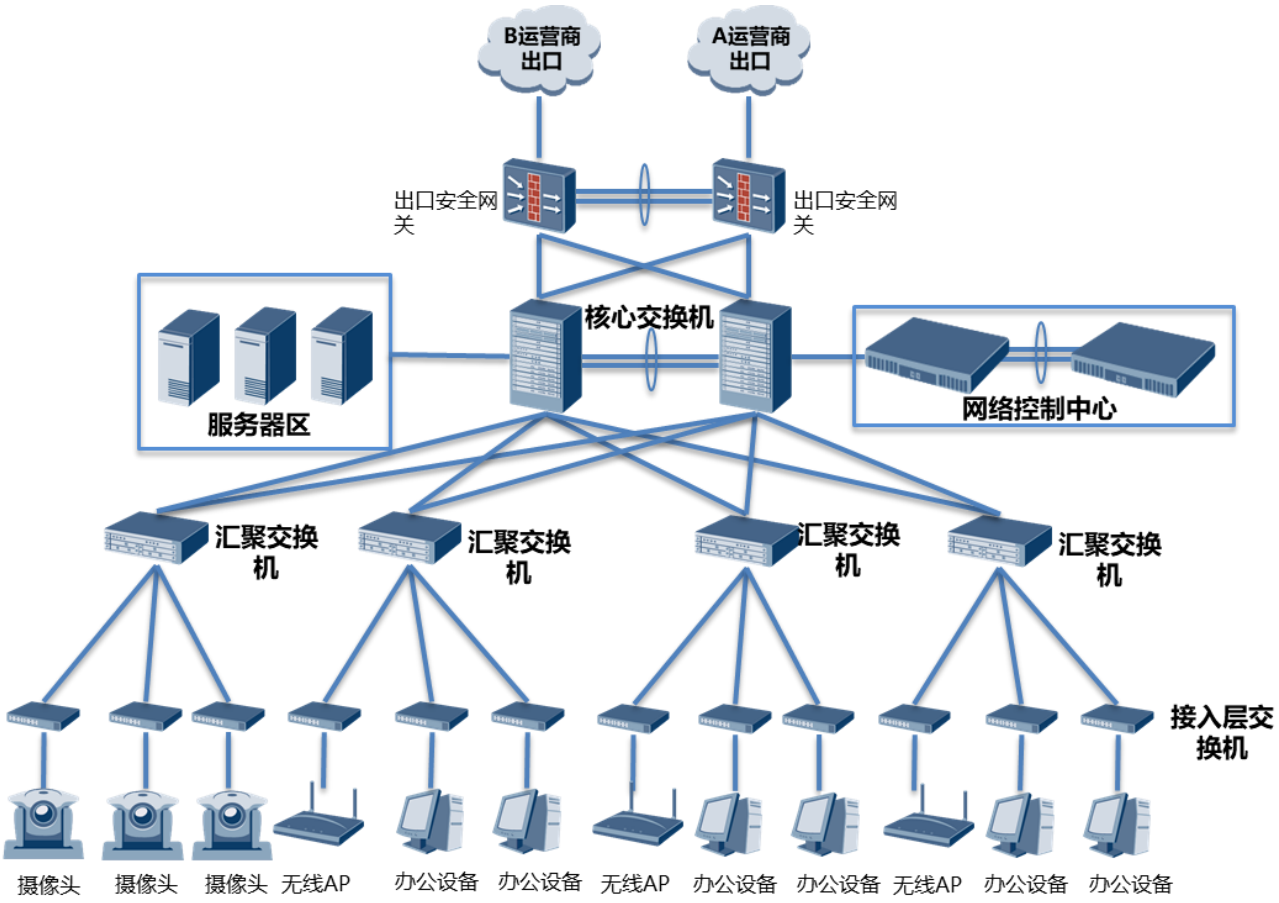
5.3.5 系统功能点

- 防区管理：对防区进行设置，从空间上区分方位区域，发生报警后可以迅速定位具体的物理位置，快速查看和排查警情。
- 防区布防：使防区处于报警防卫状态，有报警信息产生即发生报警，上送平台进行相关处理。
- 防区撤防：使防区处于报警撤防状态。
- 报警预案维护：发生报警时的报警处理预案，可以用文字描述处理步骤，可以自动联动上墙、联动手机短信、EMAIL 等，使得报警的处理及时准确。

- 报警信息实时监控，对防区进行视屏监控。
- 报警相关视频、录像、图片等信息展示，发生报警后，可以调取报警时的视频录像以及图片，可以预览报警防区的实时视频。
- 报警信息查询，对历史报警信息进行相关查询。
- 报警相关处理，发生报警后的人工处理动作，系统记录处理方式，处理人，处理时间等等相关信息。
- 报警记录查询与统计，对报警记录以各种方式进行汇总统计，生成相关报表。
- 报警级别设置，用户可以自定义报警事件的报警级别，并可以按照报警级别来自定义该报警产生后所提示出的背景颜色。
- 紧急联系人管理，可以维护多个报警的紧急联系人，以便及时的通知到相关人员警情。
- 报警预处理,有些报警需要经过一段时间的核实或者处理,这会需要一段时间，为了标注该报警相关人员已经知晓并正在处理，但还没处理完成，需要预处理这个中间状态。
- 设备巡检，系统可以出发对各个报警主机进行巡检，查看设备运行情况，从而保障各个防区工作正常，减少不报以及误报的发生。

6. 基础网络传输系统

6.1 基础网络规划



结合本次建设网络基础需求，现对整网提出以下网络设计原则：

为简化整体网络管理节点，本次设计将汇聚、接入交换机及 AP 等设备统一采用网络控制中心进行接入管理控制，把数据转发及设备管理切割开来，提高整网传输利用率。

有线网络：为满足整网高可靠及高吞吐需求，本次核心层采用万兆核心进行堆叠部署，核心区到楼栋汇聚间采用万兆光口级联实现数据信息的汇集，楼栋汇聚与楼层接入间采用千兆光纤互联；

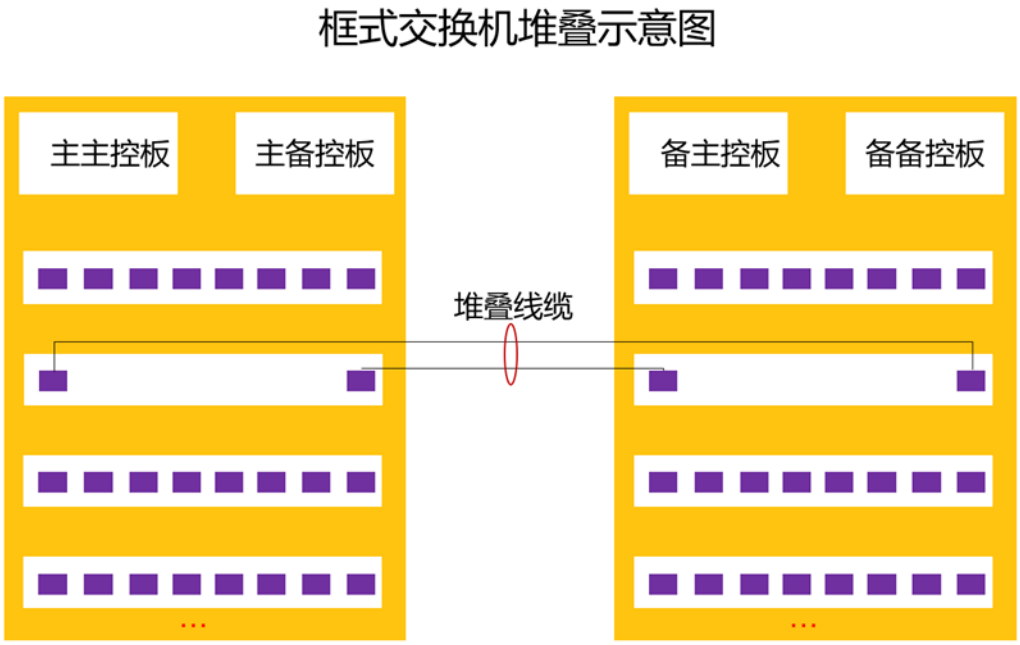
无线网络：根据现场环境选择适当 AP 类型进行部署，包括高密、普通、面板等，所有 AP 均通过接入 POE 交换机供电供网，节省布线施工成本；

6.1.1 核心层交换机设计

核心层是部署在机房中的网络核心交换机设备，连接所有的汇聚交换机，汇聚各楼栋/区域/部门之间的流量，提供三层交换机的功能。它承担了网络内部数据流量和对外的数据流量，因此核心交换机必须能够提供高速的数据转发性能、高稳定性，达到高带宽、高转发性能的效果。

同时核心层交换机系统需要支持各部件冗余，以免单点故障导致整个核心系统宕机的问题，因此需要核心层交换机支持电源、风扇等重要部件采用冗余设计。

为了保障核心系统的高可靠性，采用双机 HCS 虚拟化部署，实现核心系统互为冗余。单台设备故障的时候，可以 ms 级切换，实现业务双重高可靠性。



6.1.2 汇聚层交换机设计

汇聚层是各楼栋/区域/部门的核心，汇聚来自接入层设备的流量。转发用户业务间的“横向流量”，同时它又需要提供到核心层的“纵向流量”，因此汇聚层的设备要去也是比较高的，汇聚层与核心层共同组建成网络核心骨干网。因此汇聚层需要提供高密度的 GE 接口，汇聚接入交换机流量，用于支撑汇聚交换机下各业务，通过 10GE 接口接到核心交换机。

6.1.3 接入层交换机设计

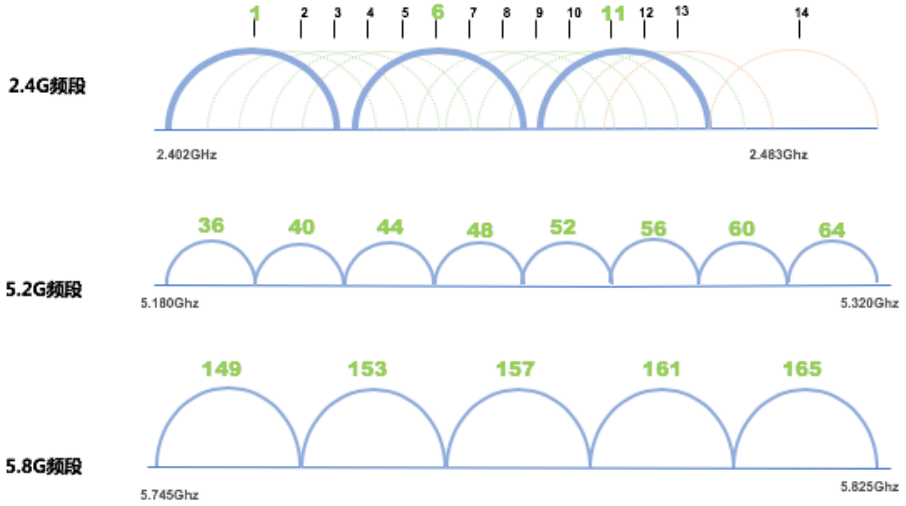
接入层是直接接入用户的终端，提供各种接入方式，这里通常部署一些弱三层层设备即可，除了能够提供丰富的二层交换机的功能之外，又能提供简单的三层功能满足业务安全的需要（例如 QOS/ACL 等），降低网络设备部署成本。接入层交换机一般需要提供高密度的 GE 接口，能够支持更多的终端接入有线网络，同时双归属到两台汇聚交换机。

6.1.4 无线 AP 设计

姚明织带网络项目，覆盖范围广、AP 数量多，WLAN 信道规划的好坏，直接影响到各部门无线网络的带宽、无线网络的性能、无线网络的扩展以及无线网络的抗干扰能力，也必将直接影响到无线网络的用户上网。

6.1.4.1 频段划分

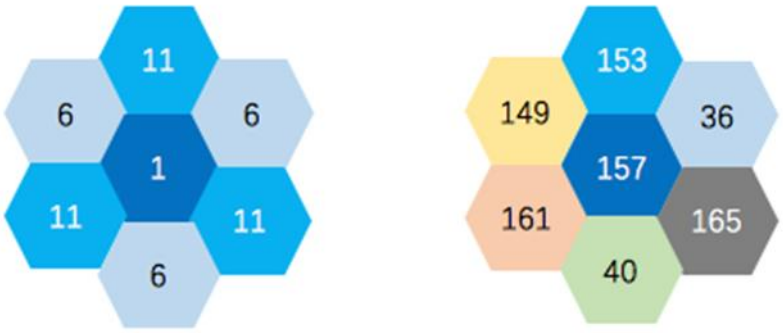
为保证信道之间不相互干扰，各部门无线政务外网对 WLAN 信道进行统一规划并实施。此次 WLAN 系统主要应用两个频段：2.4GHz 和 5.0GHz。2.4G 频段具体频率范围为 2.4～2.4835GHz 的连续频谱，信道编号 1～14，非重叠信道共有三个，我们选取 1、6、11 这三个非重叠信道。5.0G 频段分配的频谱并不连续，主要有两段：5.15～5.35GHz、5.725GHz～5.85GHz。不重叠信道在 5.15～5.35GHz 频段有 8 个，分别为 36、40、44、48、52、56、60、64；在 5.725GHz～5.85GHz 频段有 4 个，分别为 149、153、157、161，根据实际部署情况，选择相应的非重叠信道。



6.1.4.2 信道覆盖

WLAN 信道规划需遵循两个原则：蜂窝覆盖、信道间隔。根据覆盖密度、干扰情况、选择 2.4G/5G 单频或双频覆盖。AP 交替使用 2.4G 的 1、6、11 信道及 5.8G 的信道，避免信号相互干扰；此次项目都采用双频 AP，可以启用双频进行覆盖，以便提供更好的接入能力。单频覆盖和双频覆的示意图如下图所示。

6.1.4.3 漫游规划



为保证姚明织带办公网络的使用体验，需要无线网络保证良好的漫游效果，漫游是指用户在部署了 WLAN 网络的场所移动时，用户终端可以从一个 AP 的覆盖范围移动到另一个 AP 的覆盖范围，用户无需重新登录和认证，即“一次认证，多次有效；一地认证，多地有效”

可以有效的保证用户在同一栋大楼上无线信号的漫游切换。

同时也提供三层漫游功能，保证用户进行跨区域、跨网段的漫游。

6.1.5 用户认证

针对企业使用无线网络的办公人员，推出内部员工使用的认证方式，并且通过逻辑隔离手段，使办公网络和访客网络分开。

支持和企业内部的用户认证服务器进行身份认证，只需要在配置页面上配置对接信息即可以和 LDAP、AD 域、Radius 等企业内部的用户身份数据库进行快速的身份校验，既安全且可靠。

企业认证支持本地内部数据库服务器，本地数据库支持认证终结到控制器上，可满足没有内部身份认证服务器的中小型企业。

首次连接无线网络认证时，用户名和终端可以实现自动绑定，帮助企业快速完成身份绑定，若用户拥有多个上网终端，管理员也可以灵活的手动审批后续新加入终端的绑定。因此企业可根据用户组织结构划分不同的访问权限，避免越权访问问题的发生。

（1）802.1X 认证

本次无线建设需支持 802.1X WEP 认证方式，并且提供企业级安全隧道认证方式，在保证认证安全的同时，在一些特殊场景，比如没有 radius 服务器时可直接与 AD 域对接，用 AD 域里面的用户名直接认证，省去部署 radius 服务器的成本和麻烦。

使用 802.1X 认证，可以有效保证企业的信息安全，在用户认证和数据传输两个过程均进行加密，避免黑客通过无线抓包窃取用户名密码以及用户传输的机密数据信息。

控制器支持 EAP 终结，自带服务器证书，账号认证时，连接无线网络无须提前安装服务器证书，只需要提示是否信任无线网络时，点击连接即可，简化了 802.1x 的认证流程。

（2）人脸识别认证

互联网正在悄然改变人们的日常生活模式，购物、乘车、餐饮等消费付款方式已经被“人脸支付”这种新型的潮流方式所渠道，显然这种方式已经得到了商用验证。

当前企业网络登录认证方式，当采用较为安全的认证方式时，不可避免的相对其它认证方式就会显得有些复杂。因而一种便捷性、安全性的认证方式就成为了企业认证方式的一种新需，显然人脸识别认证具备这两种特征。

人脸识别认证优势说明

1）便捷

人脸识别可以在秒级时间内快速完成终端登录认证的过程，极大的提升了认证效率

2）安全

在人脸比对的过程中，认证系统会自动完成 802.1x 的认证交付过程，从而最大限度实现安全认证的级别

（3）OA 认证及账号自主管理

为简化无线网络的认证及管理，要求本次无线网络建设可支持如口袋助理、钉钉、微信企业号等移动 OA 软件平台与 Wi-Fi 员工上网管理相结合做上网认证，实现对接口袋助理、钉钉、微信企业号做企业认证。这里的企业认证，我们可以简单理解为账号密码认证。

OA 认证可以帮助企业省去人力物力搭建其他系统来管理员工、部署维护接入认证服务器，并且可以通过使用这些移动办公平台统一管理实现员工的上网信息，并实现接入认证。

Wi-Fi 智能考勤

相比较于传统的指纹考勤、打卡考勤、有源 RFID 考勤等传统考勤系统来说，利用办公 OA 软件口袋助理适合考勤系统更加精准、人性化，而且无需排队；每天上班前口袋助理会准时提醒上班考勤打卡，员工只需要打开软件此时口袋助理会自动识别进行考勤打卡签到。

（1）点击 APP 签到考勤按钮，APP 将终端 WI-FI 连接信息（连接的 SSID、连接的 AP 位置名称、AP MAC 地址、终端 MAC 地址等信息）传递给 APP 服务器。

（2）办公 OA 联动无线控制器进行校对终端 WI-FI 连接信息，若校对成功则返回信息给终端“签到成功”；若信息不匹配则返回“请连接公司 WI-FI 进行签到”。

6.1.6 应用缓存节流

企业中，往往经常会在互联网上面去下载 APP 或者其他文件（视频、办公软件等），那么无线控制器能够缓存 APP 和文件，只要某用户第一次下载过该文件过后，第二个用户若要下载，直接从本地控制器上面取即可，无需到互联网上面再次下载，不但节约了互联网的带宽，也能够提升下载速度。

6.1.7 APP 管理

随着移动互联网的发展，在无线管理方面，当下已经不再只满足于传统的 web 页面进行管理，通过移动端手机 APP 进行管理，管理员随时随地通过手机就能进行远程管理及运维，确保在网络出现问题时第一时间能了解到问题所在并进行排查处理。

6.2 网络建设建议清单

序号	产品名称	描述	数量	单位
有线网络				
1	核心交换机	框式核心交换机，支持 18 个总槽位（12 个业务槽位，2 个主控槽位，4 个独立交换网板槽位）；7 个电源槽位； 4 个风扇框）	2	台

		1、交换容量≥85.2Tbps/307.2Tbps、包转发率≥10080Mpps/86400Mpps； 2、支持横向 N:1 虚拟化（N≥2）； 3、支持 ISSU 业务不中断系统升级、静态路由、RIP v1/v2、OSPF、BGP、策略路由 4、支持 IPv6 静态路由、RIPng、OSPFv3、BGP4+ 5、支持 EAPS 环网保护技术、VRRP 冗余技术		
2	汇聚交换机	48 个 10G SFP+万兆光口，6 个 40GE QSFP+光口，交换容量≥2.56Tbps/40.96Tbps，包转发率≥1080Mpps，支持全端口线速转发；支持网络控制中心统一管理	待定	台
3	接入交换机	24 个 10/100/1000Base-T 自适应电口，4 个万兆 SFP+光口，交换容量≥336Gbps/3.36Tbps，包转发率≥108Mpps/126Mpps，支持全端口线速转发，支持网络控制中心统一管理；	待定	台
4	POE 交换机	24 个千兆 POE 电口，4 个 1G/2.5G SFP 光口；交换容量≥336Gbps/3.36Tbps，包转发率≥108Mpps/126Mpps，支持全端口线速转发；支持 IEEE 802.3af/at 供电标准，单端口最大输出 PoE 功率 30W，整机最大输出 PoE 功率 370W；支持网络控制中心统一管理	待定	
无线网络				

5	高密 AP	室内高性能 11ac wave2 三频 AP，采用创新的三频设计，支持 2.4G、5G、5G 三频并发，整机最高速率可达 3Gbps，支持双电口上联，支持 USB 口	待定	台
6	普通 AP	室内智能 11ac wave2 无线接入点，支持 MU-MIMO，内置智能天线，支持 2.4G 和 5G 同时工作，整机最大接入速率 1167Mbps；千兆口上联；	待定	台
7	室外 AP	室外型 11ac wave2 无线接入点，内置定向天线；支持 2.4G 和 5G 同时工作，整机最大接入速率 1267Mbps；一个 SFP 光口和两个千兆电口；内置天馈防雷器；支持蓝牙串口管理；支持 POE 供电	待定	
管理中心				
8	一体化网络控制器	推荐千兆电口≥6 个，千兆 SFP 光口≥4 个，最大支持 AP 管理数≥3840 台，最大支持交换机管理数≥3120 台，支持在线用户数 75K，支持身份认证、应用层流控、IPsec VPN、AP 管理、交换机管理等，可支持纵向集群父子级管理，内置 1TB 硬盘	2	台