招 标 文 件

采购方式：公　开　招　标

项目编号：HNJY-2022-088

项目名称：海口综合保税区智慧园区建设项目

采 购 人：海口综合保税区管理委员会

采购代理：海南简一项目咨询管理有限公司

2022 年 11 月

目　录

第一章　招标公告.....1
第二章　用户需求书.....5
第三章　投标人须知.....693
第四章　合同文本（仅供参考）.....709
第五章　投标文件格式.....726
第六章　评审办法和程序.....749

第一章　　招标公告

项目概况

海口综合保税区智慧园区建设项目招标项目的潜在投标人应在登录海口市公共资源交易网（http://ggzy.haikou.gov.cn）网站主页,选择“政府采购-交易公告”专栏获取招标文件，并于 2022 年 12 月 16 日 09 点 00 分（北京时间）前递交投标文件。

一、项目基本情况

1.项目编号：HNJY-2022-088

2.项目名称：海口综合保税区智慧园区建设项目

3.预算金额：109811337.48 元

4.最高限价：109811337.48 元

5.采购需求：项目建设主要内容包括：（1）园区智慧基础设施建设；（2）园区网络及计算资源平台建设；（3）园区数据资源及开放能力建设；（4）园区应用系统建设；（5）信息安全建设内容，详见采购需求。

6.合同履行期限：19 个月

7.本项目不接受联合体投标。

二、投标人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求： /

3.本项目的特定资格要求：

3.1、满足《中华人民共和国政府采购法》第二十二条规定细化为：（1）、在中华人民共和国注册的、具有独立承担民事责任能力的法人【提供营业执照副本复印件、组织机构代码证副本复印件、税务登记证副本复印件或改革后的“三证合一”或“多证合一”营业执照复印件；根据《<政府采购法实施条例>释义》，银行、保险 、石油石化、电力、 电信运营商等有行业特殊情况的，其分支机构可参与投标。采购文件中涉及要求提供“法定代表人”相关证明材料的，提供分支机构“负责人”的相关证明材料】

（2）、具有良好的商业信誉和健全的财务会计制度【提供 2021 年度经会计

师事务所审计的财务审计报告或2021年至今任意三个月财务报表（财务报表至少应包含资产负债表、利润表、 现金流量表），复印件加盖公章，投标人注册成立时间不足三个月的，从注册时间起算。】

（3）、具有依法缴纳税收和社会保障资金的良好记录【提供2021年至今任意三个月的依法缴纳税收和社保的相关材料 ，复印件加盖公章，投标人注册成立时间不足三个月的，从注册时间起算】

（4）、参加政府采购活动前三年内，在经营活动中没有重大违法记录【提供声明函,投标人注册成立时间不足三年的，从注册时间起算，加盖公章】

（5）、被中国执行信息公开网列入失信被执行人的供应商;或被信用中国网站(www.creditchina.govcn)列入重大税收违法失信主体的供应商;或被中国政府采购网(www.ccgp.gov .cn)列入政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商 (处罚决定规定的 时间和地域范围内)，无资格参加本项目的采购活动【提供查询结果网页截图加盖公章】

3.2、法定代表人身份证明及授权书【按招标文件格式提供法定代表人身份证明及授权委托书原件】

3.3、按照招标文件要求缴纳投标保证金【提供投标保证金缴纳凭证或银行保函】。

三、投标程序及采购文件获取办法

1.查看采购公告及下载采购文件。登录海口市公共资源交易网（http://ggzy.haikou.gov.cn）网站主页,选择“政府采购-交易公告”专栏查看采购公告，免费下载项目采购文件。

2.市场主体登记。新用户在海南省公共资源交易中心按照要求登记注册（http://zw.hainan.gov.cn/ggzy/ggzy/jyzn/63369.jhtml），已经在海南省或海口市公共资源交易网登记过的，无须再登记。

3.投标申请并获取保证金账号。提交市场主体登记信息后，在海口市公共资源交易网主页,进入交易系统选择“我要投标”，提交项目投标申请后获取投标保证金账号,如未在规定时间内提交投标申请者,视同放弃参与本项目采购活动。

四、提交投标文件截止时间、开标时间和地点

1.递交投标文件截止时间：2022年12月16日09时00分 （北京时间）

2.开标时间：2022 年 12 月 16 日 09 时 00 分（北京时间）

3.递交投标文件及开标地点：海口市公共资源交易中心开标会议室（海口市海甸五西路 28 号建安大厦副楼 203 开标室）（详见会议室门前标识），如有变动另行通知；

4.逾期送达或者未送达指定地点的投标文件，视为无效投标文件不予接收。

五、采购信息发布媒体

1.本项目采购信息指定发布媒体为海南省政府采购网 https://www.ccgp-hainan.gov.cn/ 和海口市公共资源交易网（http://ggzy.haikou.gov.cn）。

2.采购文件下载网址海口市公共资源交易网（http://ggzy.haikou.gov.cn）。

3.有关本项目采购文件的补遗、澄清及变更信息以上述网站公告与下载为准，采购代理机构不再另行通知，采购文件与更正公告的内容相互矛盾时，以最后发出的更正公告内容为准。 其他补充事宜

六、公告期限、确认投标期限和投标保证金到账截止日期

1.本项目采购公告及确认投标期限不少于 5 个工作日，2022-11-25 零时至 2022-12-1 二十四时止。

2、投标保证金到账截止日期：2022 年 12 月 16 日 09 时 00 分（北京时间）；

七、其他补充事宜

7.1 在开标时提交电子版、纸质版投标文件；

7.1.1 电子版投标文件（PDF 格式）的递交：电子版投标文件（PDF 格式）密封，随纸质版投标文件一起递交，否则视为无效投标。

7.1.2 投标人提供的电子版投标文件（PDF 格式）必须与纸质版投标文件的正本保持一致，否则自行承担由此带来的一切风险。

7.2 报价保证金：￥500000.00 元（大写：伍拾万元整）。

7.3 本项目支持节能产品管理、环境标志产品管理、进口产品管理、中小企业发展等相关政策。

八、对本次招标提出询问，请按以下方式联系。

1.采购人信息

名 称：海口综合保税区管理委员会

地址：澄迈县老城开发区南一环路 69 号

采购项目联系人：符先生

联系方式：0898-67205016

2.采购代理机构信息

名 称：海南简一项目咨询管理有限公司

地　址：海口市龙华区龙昆南路延长线保明新村 7 号

联系人：陈工

联系方式：0898-65327762

3.项目联系方式

项目联系人：陈工

电　话：0898-65327762

第二章　用户需求书

采 购 需 求

第一部分：项目概述

项目概述

项目名称

海口综合保税区智慧园区建设项目

第二部分：设计依据

设计依据

政策文件

1、中共中央、国务院印发《海南自由贸易港建设总体方案》；

2、《智慧海南总体方案（2020-2025 年）》；

3、《习总书记 4 月 13 日在庆祝海南建省办经济特区 30 周年大会上的重要讲话》；

4、《中共中央国务院关于支持海南全面深化改革开放的指导意见》；

5、《国务院办公厅关于进一步优化营商环境更好服务市场主体的实施意见》（国办发【2020】24 号）；

6、中国（海南）自由贸易试验区总体方案（国发【2018】34 号）；

7、《国家政务信息化项目建设管理办法》（国办发【2019】57 号）；

8、《海关总署关于印发〈直属海关口岸监管业务运行监控指挥中心工作方案（试行）〉的通知》（署监发【2018】198 号）；

9、《海关总署关于发布〈海南自由贸易港交通工具及游艇“零关税”政策海关实施办法（试行）〉的公告》（海关总署公告 2021 年 1 号）；

10、《财政部 海关总署 税务总局关于海南离岛旅客免税购物政策的公告》（财政部 海关总署 税务总局公告 2020 年第 33 号）；

11、《海关总署关于印发〈海关总署完善进出口商品质量安全风险预警和快速反应监管体系工作实施方案〉的通知》（署检发〔2019〕153 号）；

12、《海南自由贸易港进口“零关税”原辅料海关监管办法（试行）》（公告〔2020〕121 号）；

13、《关于海南自由贸易港原辅料“零关税”政策的通知》（财关税【2020】42 号）；

14、《关于海南自由贸易港交通工具及游艇“零关税”政策的通知》（财关税【2020】54 号）；

15、《海关总署关于综合保税区验收有关工作的通知》署贸函〔2019〕209 号；

16、《综合保税区基础和监管设施设置规范》（2019）；

17、《中华人民共和国海关监管区管理暂行办法》海关总署令第 232 号；

18、海关总署关于印发《海关特殊监管区域设立审核办法（试行）》；

19、《海关总署关于综合保税区验收有关工作的通知》（署贸函〔2019〕209 号）；

20、《全国海关监控指挥中心基础设施建设指导方案》（署科发 56 号）；

21、《关于出口加工区有关检验检疫问题的通知》；

22、《出口加工区检验检疫监督管理办法》；

23、《中华人民共和国海关监管场所管理办法》232 号令；

24、《海关监管作业场所（场地）监控摄像头设置规范》（海关总署公告 2019 年第 69 号令）；

25、《综合保税区基础和监管设施设置规范》署贸函〔2019〕209 号。

26、《海南省信息化条例》海南省人民代表大会常务委员会公告第 12 号（2020 修订版）；

27、《海南省政务信息化项目建设管理办法》琼府办〔2020〕38 号；

28、《海南省公共信息资源管理办法》海南省人民政府公告 琼府〔2018〕39 号；

29、《中共海南省委关于贯彻落实党的十八届三中全会精神推动海南全面深化改革的实施意见》（琼发〔2014〕1 号）；

30、2017 年海南省人民政府文件《海南省人民政府关于印发海南省政务信息整合共享专项行动实施方案的通知》（琼府〔2017〕77 号）；

31、海南省人民政府办公厅文件《海南省人民政府办公厅关于印发海南省 2017 年促进大数据发展工作要点的通知》（琼府办〔2017〕107 号）；

32、《海南省信息化建设领导小组办公室关于尽快谋划重大 5G 应用信息化项目的通知》（琼信组办〔2020〕12 号）。

标准规范

1、《电子政务标准化指南》（第一版）；

2、《计算机软件需求说明编制指南》（GB9385-1988）；

3、《功能建模方法 IDEF0》（IEEE 1320.1-1998）；

4、《信息建模方法》（IEEE 1320.2-1998）；

5、《计算机软件产品开发文件编制指南》（GB/T 8567-1988）；

6、《信息技术开放系统互联高层安全模型》（GB/T 17965-2000）；

7、《信息技术开放系统互联基本参考模型》（GB/T 9387）；

8、《信息技术开放系统互联应用层结构》（GB/T 17176-1997）；

9、《信息技术开放系统互联开放系统安全框架》（GB/T 18794）；

10、《中华人民共和国标准—集装箱安全智能锁通用技术规范》（GB/T29752-2013）；

11、《中华人民共和国海关行业标准—海关物流监控前端集成系统建设》（JGS/T 14-2015）；

12、《海关金关工程二期工程标准－海关智能云卡口前端设备技术选型规范》（JGS/T 15—2015）；

13、海关总署（关于修订《海关监管作业场所（场地）设置规范》《海关监管作业场所（场地）监控摄像头设置规范》和《海关指定监管场地管理规范》的公告）（公告〔2021〕4 号）；

14、《海关总署关于印发〈进出口商品质量安全风险监测工作规范（试行）〉等 4 个工作规范的通知》（署检发〔2019〕256 号）；

15、信息安全技术 《信息系统安全等级保护基本要求》（GB/T22239-2019）；

16、信息技术 《云计算 概览与词汇》（GB/T32400-2015）；

17、物联网 《术语》（GB/T33745-2017）；

18、智能传感器 第 2 部分：《物联网应用行规》（GB/T33905.2-2017）；

19、物联网总体技术 《智能传感器接口规范》（GB/T34068-2017）；

20、物联网总体技术 《智能传感器特性与分类》（GB/T34069-2017）；

21、物联网 《电流变送器规范》（GB/T34070-2017）；

22、物联网总体技术《智能传感器可靠性设计方法与评审》(GB/T34071-2017)；

23、信息技术大数据 《术语》（GB/T35295-2017）；

24、《数据中心设计规范》（GB 50174-2017）；

25、《综合布线系统工程设计规范》（GB 50311-2016）；

26、《智能建筑设计标准》（GB 50314-2015）；

27、《安全防范工程技术规范》（GB 50348-2018）；

28、《通信管道与通道工程设计规范》（GB 50373-2006）；

29、《通信管道工程施工及验收技术规范》（GB 50374-2006）；

30、《移动通信室内信号覆盖系统设计与验收规范》(DG/TJ08-1105-2010)；

31、《民用建筑电气设计规范》（JGJ 16-2016）；

32、《电缆桥架》（QB/T 1453-2003）；

33、《电信基础设施共建共享工程技术暂行规定》（YD/T 5124-2015）；

34、《无线局域网工程设计规范》（YD 5191-2009）；

35、《海南省信息化项目文档编制规范》琼工信信推〔2018〕231 号；

36、《海南省大数据开发应用条例》海南省人民代表大会常务委员会公告第37 号；

37、《海南省公共建筑节能设计标准》（DBJ 46-03-2017）；

38、《海南省信息化管理条例》；

39、《海南省大数据局管理暂行办法》（海南省人民政府令 第 284 号）；

40、《海南省政务信息化工程建设管理办法》（海南省人民政府令 第 190 号）。

第三部分：总体目标与建设成效

总体目标与建设成效

一、近期目标

强化基础平台，升级改造监管配套的平台、场地和设备，完善仓储、物流等供应链业务，优先解决“离岛免税”政策实施后，进口免税品供应链服务需求激增的问题，构建自由贸易港和综保区政策创新背景下核心的消费品（免税品）国际供应链仓储配送中心，通过聚集品牌商、供应链服务商和免税店等服务侧数据

资源，满足地方政府和监管部门、业务管理部门监管侧的工作需要，丰富监管测手段，结合政府、园区、机场、港口、码头、船舶、车辆等公共数据资源，形成满足服务侧对于供应链可视化、可追溯、可预测的业务管理的现实需求，降低企业供应链管理成本，同时降低监管侧信用管理和监管成本，为政府和监管部门的制度创新和业务创新提供支撑和保障，打造海南自贸港贸易便利和风险防控“双创双赢平台”。

二、中期目标

结合海南自贸港产业政策，瞄准国内产业龙头企业，对标相关产业链和供应链需求，补短板，强优势。运用自贸港“一线放开，二线管住”、“加工增值30%”等政策优势，提前规划全岛封关后岛内加工企业合规管理格局，参考以企业为单元的加工贸易保税管理体系，智慧协同地方政府和监管部门，优化业务、通关流程，完善设施建设，满足政务服务需求、产业链配套需求、交通物流需求和园区运营管理需求，创新构建海南自贸港“双向服务平台”。

三、远期目标

借力国际国内双循环和区域经济合作伙伴关系协定（包括 RCEP 和东盟自贸协定），将海南自贸港产业发展融入国际产业链分工，用足用好原产地规则，以5G、物联应用等信息科技手段为抓手，打通生产要素有序流动的堵点和痛点，为探索全岛封关运行积累实践经验和可复制可推广的能力，力争将海口综保区打造成为国内自由贸易政策“先行先试”示范区。

四、本期目标

打造一个整合多方资源、打通各类平台功能的园区监管、服务体系——智慧园区。搭建系统、科学、闭环的服务、监管体系，提供更合理、更有效的园区监管服务，为园区企业提供全链条的服务支撑，为管理者实施精确监管、掌控园区全局提供手段。

一、在行业及园区监管方面，能够协同海关、外汇、工商、税务等管理部门，在作业操作、业务流程优化等方面，完善设施建设，高效完成监管作业任务；实现对园区内企业一企一帐管理，提高监管质量和效率，加快企业物流运转速度、缩短运转周期，优化园区营商环境。

二、在产业服务方面，能够结合全岛产业政策，面向园区政务服务需求、产业链配套需求、交通物流需求等，向园区企业提供一站式服务；做好招商工作，吸引外部投资；评估区内经济运行情况，及时了解企业经营状况，帮助园区企业

解决在实际经营方面遇到的问题；

三、在综保区管理方面，实现综保区公共设施的建设、管理和服务等基础设施的智慧化运行、管理和维护，实现园区全方位智慧安防和企业安全生产管理，有效防范重大安全事故；实现一人一码，一车一册的精细化、个性化管理，更加高效地服务于园区企业和员工。

综保区运营方以驱动产业协同为核心提升综保区整体运营能力，促进园区内产业可持续发展，助力园区内业务创新和经营创新，探索可复制的能力并加以推广。

基础设施建设广泛采用云计算、5G 通信、物联网等新兴技术，全面接轨新基建要求，衔接智慧海南总体设计，保障海口综保区信息化建设整体规划。满足未来 10 年的信息化建设需要，为海南自贸港整体封关运作奠定基础。

第四部分：总体建设思路

总体建设思路

指导思想

海口综合保税区充分利用国际和国内两个市场、两种资源，重点打造“四中心两基地一总部”的布局指引，积极推进六大产业的业务发展，以物流汇聚商流、信息流和资金流，以供应链融合产业链、创新链和消费链，快速发展成为海南开放型经济集聚发展的重要园区。对标国际一流自由贸易区，不断提升投资和贸易便利化水平，优化国际营商环境，并以开放促进产业聚集和创新，将海口综合保税区打造成连接全球的资源要素配置中心，全国自由贸易港建设先行区，海南发展核心引擎和全国全国综保区高质量发展示范区。

总体定位

海口综保区数字智慧园区项目以信息化管理为基础，以先进科技装备应用为手段，实施多手段、少手续的安全隐性监管和低干预、便利化的高效精准监管。另外，实现管理机构、监管部门间数据交换、信息共享及协同按。因此海口综保区数字智慧园区平台将与海南省国际贸易单一窗口、海南省社会信息管理平台、

海关监管系统、港口管理系统等在数据共享、业务协同上进行深度对接。

海口综合保税区智慧园区平台是服务于园区管理、监管单位、园区相关企业的智慧园区平台。

与海南单一窗口、海南大数据管理局、海口海关等省级管理单位的公共服务平台（海南单一窗口、海南公共服务平台、海关监管系统）实现数据交换、数据共享、服务集成等功能，形成省级平台和园区平台的两级应用建设互补互助的生态优势。

与园区相关的仓储企业、物流企业、生产制造企业、园区运营企业等信息化系统互联互通。促进工单核销、仓储联网、监装监卸等创新业务有效落地，形成外贸数据的联盟链。

第五部分：建设架构

建设架构

总体框架

海口综保区的管理及业务的开展需要通过本项目建设的综保区智慧辅助监管平台，分别与海关端、相关企业端、商务厅公共服务平台、海南大数据平台、公安对接进行工作联动、数据互联互通，进行数据交换与共享。

企业服务相关平台通过综保区智慧监管平台与企业自有的 ERP 集成系统对接，在企业进行作业申请时，企业的数据通过综保区智慧监管平台进行初步的审核后，将数据推送到相关政务、监管、管理平台，并通过各政务、监管、管理平台向审核通过后，将企业作业申请审核结果通过本项目建设的辅助监管平台反馈到企业服务平台。

园区管理平台包含智慧安防系统、物联网平台、智慧路灯等系统，园区管理平台需要支持园区内各个系统之间的视频、地理位置、设备信息、人员信息数据的整合和交换，快速实施应用程序节点部署以及各子系统之间的协同。在园区系统中的各子系统中，比如智慧安防、智慧路灯、智慧消防、智慧环境、智慧能耗等，传递和展现整个管理过程中的相关信息，可为海口综合保税区管委会打造一体化的运营管理，提升园区精细化运营、信息化管理水平，通过综保区智慧监管平台将采集的仓储物流数据和监控图像、卡口数据等数据经过审核、统计分析后传送到海关监管端。

打造园区综保区监控中心，统一展示园区运行全貌，采集园区各运行节点的传感、采集、收发，将各个设备设施运行效率和异常情况，实现智能化的故障报警和运行效能监测，并提供管理者手机远程监控功能，提高处理故障的反应速度和应急指挥。形成充分的“可视”、“可控”和“可管”。

结合海口综合保税区的总体规划，本方案采用一个平台、多种应用、差异化服务、智能联动性的智慧园区方案。

总体架构

本项目将以“1 个方向、2 个看齐、3 个目标”服务六大产业建设海口综合保税区智慧园区：

1 个方向：建设智慧海口综合保税区智慧园区，对接智慧海南，按照“统一架构、统一标准、集约建设、长效发展”的设计思想，以“大连接”、″大平台”、″大数据”为核心，坚持综保区统筹规划、统筹布局、集约部署，自上而下构建体系优化、资源共享、功能强大、应用丰富、管理高效的智慧园区。

2 个看齐：看齐试点建设全时空智慧园区；智慧赋能，看齐吸取上海洋山综保区成功经验，打造生态环境和营商环境双一流的智慧综保区。通过构建综保区物理世界与网络虚拟空间的对应、相互映射、协同交互的复杂矩阵系统，在计算机世界再造一个与之匹配、对应的孪生园区，实现园区的全要素数字化和语义化、全状态实时化和可视化、管理决策协同化和智能化。

3 个目标：建设智慧监管，智慧协同海关等管理部门，优化营商环境、通关流程，完善设施建设，高效完成通关任务，实现对园区内企业管理，对接智慧海南“一人一码、一物一链、一企一账”实现海关对监管对象精准监管；建设智慧综合保税区管理，建设基础公共设施，管理、服务、运行、维护基础市政设施，优化营商环境，全方位安防管理，企业安全生产、重大安全事故等管理；建设智慧产业服务，满足产业链配套、政务服务、交通物流需求等；做好招商投资；评估区内经济运行情况，及时了解企业经营状况。

第六部分：用户需求

用户需求

建设内容

实现对综保区全流程海关监管，实现对综保区产业服务、管理服务、经营服务的一体化管理；遵循智慧海南、海南自由贸易港总体规划以及相关行业信息技术标准规范体系，推进园区信息化系统建设的规范化、集约化、集成化发展。

基于“总体规划、分阶段实施”的原则，本项目建设开发任务应在 19 个月的工期内完成，具体划分为三个阶段完成。

投标人须为完成各阶段目标提供进度计划横道图。

总体的建设内容如下：

一、园区智慧基础设施建设

基于先进的感知及信息传输处理技术，控制视频、路灯、消防、能源等基础设施设备，通过有线、5G、WIFI 等通信技术手段加以连接成网，形成园区内部的“万物互联”，同时整合这些终端及边缘基础设施的管理，实现智慧化的园区基础设施管理，建设园区的智慧安防、智慧能源、智慧消防等管理体系，从而提高园区管理效率、减少管理成本、提升管理水平，构建绿色生态园区。

具体建设内容如下：

1、园区智慧管理平台建设

整合园区各类基础设施的管理，构建园区基础设施管理的全景业务视图，实现园区基础设施管理“一张图”。

2、园区智慧安防系统建设

是园区智慧管理平台下属的子系统，以覆盖园区的视频监控网络为基础，以智能视频分析为技术依托，实现面向人员、车辆、区域、事件为对象的全方位的园区安全防护体系。具体包括：

（1）视频监控子系统

（2）报警子系统

（3）智能巡查子系统

（4）园区一脸通子系统

（5）车辆通行管理子系统

（6）园区交互会议子系统

（7）防疫绿码管理子系统

（8）一键报警子系统

（9）无人机远程监控系统

（10）园区电子围栏子系统

（11）卡口 LED 屏升级改造

（12）安防综合管理平台

3、智慧路灯系统建设

面向智慧路灯基础设施，实现路灯的智能管理，并构建覆盖园区的道路 WIFI 服务能力，提供由路灯承载的视频监控以及后台的各种智能分析以及资源监测的能力。通过统一路灯的承载与服务方式，成为园区的物联网体系的重要构成。

具体包括：

（1）园区道路路灯控制管理子系统

（2）视频监控子系统（预留园区室外道路监控位置并提供摄像头及其附加装置的安装接入方式，与智慧安防系统中的视频监控子系统统一整合管理，是整个园区视频监控子系统的重要组成）

（3）园区室外环境监测子系统

（4）园区音乐广播子系统

（5）一键告警子系统

（6）通信子系统

4、智慧消防系统建设

主要包括火灾报警系统、消火栓系统、自动喷水(喷淋)灭火系统以及疏散系统。其中消火栓系统、自动喷水(喷淋)灭火系统属于消防给水系统的重要组成部分。

根据消防相关的国家标准，火灾报警系统与消防给水系统均是建筑消防最核心的系统，火灾报警系统保证了火灾发生时第一时间发出警报，消防给水系统属于灭火系统，应始终处于持续稳定的预定压力状态，要保证在发生火灾时可以第一时间快速出水和有充足的水量。

具体建设内容如下：

（1）监控中心大屏显示子系统

（2）消防综合管理控制子系统

（3）消防给水监测子系统

（4）火灾联网报警子系统

（5）移动应用客户端子系统

5、智慧能效监测系统建设

实时监测能耗数据,洞悉园区能耗走向，建立园区能耗模型,挖掘节能潜力，积累能耗数据,为后续决策提供依据。

具体包括：

（1）能耗数据采集子系统

（2）能耗分类、分项计量子系统

（3）电能质量监测子系统

6、智慧查验系统

具体包括：

（1）5G 智能单兵查验

（2）VR 全景查验监控系统

（3）海关侧国产化云节点

二、园区网络及计算资源平台建设

一是充分利用现有海南省政务云的云计算资源,将园区规划建设的与园区行政管理和园区运营管理等相关的应用软件系统部署到到海口市电子政务云进行管理。

二是面向园区智慧化建设的计算需求，建设园区的云计算中心，包括园区机房全面升级改造、新增机房计算和存储设备以及相关的网路和安全设备，按照云计算技术架构构建园区计算和存储资源的管理和服务,以满足园区智慧化管理的计算和存储需求、网络带宽需求以及安全管理需求。升级改造现有园区的网络平台，包括园区局域网重构、新建园区物联网，打通国际互联网数据专用通道等，为满足海口综保区智慧园区建设提供网络环境。

三是面向园区海关监管的需求,升级改造园区海关主机房和配套的卡口机房。建立海关专网接入，便于部署海关监管信息系统、视频监控系统等，为海关监管服务的智慧化建设提供基础环境。

具体建设内容如下：

1、园区网络系统

（1）园区局域网建设

（2）园区海关专网建设

（3）园区物联网建设

（4）园区 5G 专网建设

（5）园区国际互联网数据专用通道建设

2、园区计算资源系统

（1）园区机房建设

（2）海关专用机房

（3）监控中心建设

（4）服务器建设（包括本地机房服务器建设和电子政务云服务器租赁）

（5）存储系统建设

三、园区数据资源及开放能力建设

基于园区业务管理范围，按照数据治理标准规范，从园区各个业务信息化系统中采集数据，构建园区数据资源池，并按照大数据局的要求以及数据开放权责的要求，纳入大数据局数据资源开放目录中，供相关人员和机构使用。

具体建设内容如下：

1、建立园区信息数据资源分类目录；

2、实施数据治理，建立园区数据资源池；

3、建立园区信息数据资源开放目录，并纳入到大数据局数据资源开放目录中，从而形成园区数据资源开放能力；

4、结合园区业务需求，从大数据局数据资源开放目录中引入园区业务开展需要的外部数据。

四、园区应用系统建设

结合智慧海南、海南自由贸易港总体建设方案的总体规划和整体部署，实现园区内部各业务系统的全要素数字化、全状态实时化、管理决策协同化和智能化。同时根据智慧海南、海南自由贸易港总体建设方案的要求对接海南省和海口市相关的统一平台，同时与海关相关业务系统及平台建立紧密的协同工作机制。

通过展销类、作业类、监管服务类、园区经营管理类等各类应用系统的建设，为园区内企业提供统一的业务运营支撑服务，同时实现园区内各业务之间的协同，充分利用智能技术实现园区供应链管理的智能化。

具体包括：

1、园区公共服务平台

（1）统一门户

（2）智能园区服务系统

（3）访客管理系统

2、园区运营管理平台

（1）园区智慧党建系统

（2）园区决策分析系统

（3）安全生产管理系统

3、展销综合服务平台

（1）云展综合服务系统

（2）宝玉石交易服务系统

（3）资源云交易系统

4、作业综合服务平台

（1）一体化 ERP 云服务系统

（2）智慧云仓服务系统

（3）物流运输管理系统

（4）供应链金融服务系统

（5）融资租赁管理系统

（6）免税交通工具管理系统

（7）冷链协同管理系统

（8）跨境电商新零售管理系统

（9）溯源采集管理系统

5、辅助监管业务服务平台

（1）智能场站管理系统

（2）多式联运服务系统

（3）跨境电商园区服务系统

（4）免税品辅助管理系统

6、应用支撑平台

（1）统一用户/权限管理系统

（2）数据交换系统

（3）订阅分发系统

（4）统一 API 管理系统

7、智慧海南对接体系

（1）与海南省大数据管理局对接

（2）与一线口岸对接

（3）与二线口岸对接

四、信息安全建设内容

智慧园区安全保障体系框架包括园区安全保障体系、安全管理体系和安全运营体系。以园区安全保障体系为支撑，整合 “技术、管理、运营”所需各类安全技术资源，为智慧园区提供安全基础能力支撑。在保障体系的建设上，根据智慧园区的层次模型，针对“园区感知、云基础设施、数据资源以及应用安全”分别进行针对性的安全保障。

通过归集智慧园区安全相关基础设施、安全保障体系、平台、系统以及主题应用等的日志及情报数据，汇总多家安全服务商及厂商安全情报数据，由建立统一的安全保障体系，将原本零散的安全数据变成统一规范的安全数据资源并对外提供数据服务，使得这些数据可以有效支撑安全运营管理及常态化的威胁发现和应急处置，提高安全管理者决策的科学性和精准性，将智慧园区的安全管理单位及各个业务部门组织联动起来，避免多头管理，形成一体化的运营中心管理机制。补齐风险源登记制度短板，对责任主体、风险指数、应对措施做到“底数清”“情况明”，实现智慧园区安全运行风险的全面辨识、超前预测、科学预警、动态防御，有效控制风险源。

结合智慧园区具体建设情况，安全保障体系建设内容主要包括：

密码基础设施：建设包含智慧园区密码基础设施；从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出密码应用技术要求，保障信息系统实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性；并从信息系统的管理制度、人员管理、建设运行和应急处置四个方面提出密码应用管理要求，为信息系统提供管理方面的密码应用安全保障。

网络边界安全防护：建设智慧园区云平台上联至市级政务网络，以及互联网出口边界安全防护措施；通过在安全域边界均部署安全网关设备进行隔离和访问控制，严格控制外部网络对业务系统信息资源的访问，确保虚拟化数据中心和信息系统自身的安全。

安全管理中心：建立安全数据中心，全面收集信息系统内部和外部的安全要素，实现对安全要素的体系化、集中化管理。通过建立体系化的管理方式，方便运维人员对安全要素集中管理，并能够及时感知资产风险，提升智慧园区的网络

安全自主可控能力。对多源安全告警进行关联分析、规则分析、情报分析等，发现潜伏的高级持续性威胁。结合安全事件检测结果，梳理内网资产互访关系，基于攻击链阶段推导事件发展过程，分析历史数据实现逆向溯源。帮助安全分析人员梳理安全事件发生链路，并进一步研判安全威胁扩散情况，及时阻断威胁蔓延。对接联动安全防护设备，在安全事件发生时自动下发阻断策略，并在必要时下发通知预警，及时完成安全闭环。

物联网安全：建设物联网安全监测平台设备，实时或周期性对物联网进行安全摸底检查，从网络资产快速摸底、设备弱口令及漏洞检测、网络边界检测以及异常行为检测等几个方面，对网络进行快速的扫描检测，及时发现存在的各类安全隐患，比如系统漏洞、弱口令、敏感服务端口等安全弱点，摸清物联网整网的安全现状，排查并督促整改重要网络安全隐患、风险和突出问题。

安全运营体系：建设智慧园区安全运营体系，在流程机制方面采用自上而下进行合理的责任划分，用数据分析问题、预判问题、验证问题、协调资源解决问题并持续迭代优化。利用安全运营中心为安全运营工作提供技术支撑，提供态势感知、通报预警、应急处置等运营手段。安全运营团队可以利用安全运营中心相关技术及数据，对智慧园区的安全问题进行统一分析，及时将预警信息同步给支撑单位做好提前防范，加强整改，预防发生更多安全事件发生。以此促进安全事件应急响应时效性，提升安全事件处置水平。对发现安全问题的场景及系统进行处置结果的跟踪，掌握其整改结果是否达标，是否引入新的安全问题，从而形成事前预警通报，事中防护应急，事后监督整改的应用安全运营保障闭环。

业务需求分析

园区公共服务平台

统一门户需求分析

门户是园区信息发布的总平台，也是集中对外提供服务的总平台， 可以将各种应用系统、数据资源和互联网资源集成到该信息管理平台上，并以统一的用户界面提供给用户，并建立园区对客户、企业、内部员工和园区对相关部门的信息通道，使企业能够释放存储在企业内部和外部的各种信息。主要业务需求如下：

前台展示：前台主要是信息发布展示与所集成业务办理系统的入口，构成门户主体结构内容包括导航栏、门户首页、子页面三大块。导航栏贯穿首页及各子页面，实现全网的功能导航，并集中展示关键核心的内容。

内容管理：通过文章管理、资源管理、信息内容管理、问卷管理和链接管理模块，实现对各频道上信息的管理。

资讯展示：跨境电商园区门户实现园区的信息发布展示，按照不同的资讯信息类型，在门户中分模块、分区域进行不同类型资讯信息的展示与公告。

业务集成：跨境电商产业园门户平台通过办事平台实现在线业务办理功能，在门户实现对于当前业务办理系统的集成

后台发布管理：跨境电商产业园门户平台后台发布管理功能实现对整个门户平台前台页面展示信息的后台维护管理，实现敏感词维护、信息编辑、敏感词自动监测预警、权限管理等功能。

信息发布系统：为使网站结构在统一的规划和标准下管理实施，需要建设统一的信息发布系统，实现分布式信息发布功能，加强网站信息管理，避免重复投资。

智慧园区服务系统需求分析

主要是为园区管理提供统一的应用治理平台，使整个园区互通互联，为合作伙伴提供技术、产品和智慧服务，提供统一的物业管理、运营管理、实现人员、资产、设备的统一运营、维护、管理，形成信息汇集、资源共享及优化管理等综合功能的服务系统。

招商管理可为园区提供详细招商信息，包括招商计划编号、招商计划名称、招商企业类型、规模、招商企业行业等信息。系统可根据后台运算自动提示贴合度更高的企业，直观的判断出招商的匹配情况，方便招商对口的企业。

租赁管理可为园区提供办公用房、设备的管理和租赁的管理功能。当产生租赁业务时，可对园区内办公房屋、设备租赁合同进行维护及归档，提高管理效能。

物业管理为园区企业提供物业费缴纳、水电费缴纳等相关服务，进行自动催缴。园区可在后台进行物业信息的维护，制定规范化的费用计算方式。

资产管理主要是维护管理园区内资产，可登记所有资产的信息，包括时间、所属部门、资产编号、资产类别、所属部门以及折旧信息和入账信息等。当资产

信息发生转移时，系统提供产权发生转移时的登记台账，详细维护资产转移后的信息、数量、转入转出单位及转移和接收的原因、时间等，方便查找资产变动情况。

访客管理系统需求分析

访客管理系统是一个集智能卡、信息安全、软件、网络及机械为一体的智能化管理系统。通过在园区出入口设置通道闸机，配合出入口控制系统，对进入园区的外部来访人员及车辆进行出入管理的自动化系统。

访客管理系统可对进出访客人员进行全面数字化管理，替代管理者完成传通手工登记工作，并能高效准确的对外来访客人员登记、信息录入、确认及授权等，便于异常情况发生后查询，提高园区的安全防范等级，提高了安保工作效率、安全性和物业管理形象

车辆管理需求：

为规范海口综合保税区卡口行政通道管理，优化园区营商环境，切实提升行政通道通行效率，进入园区的小型汽车、大巴车、施工车辆必须提前进行备案，否则不能通行。行政车辆备案分为长期备案、短期备案、快速入园备案。一定时期内需要经常进出综保区的行政车辆可以申请办理长期备案，偶尔进出园区的行政车辆一般申请短期备案，临时入园车辆扫码登记后即可快速入园。

申请长期备案和短期备案的企业，需在平台填写申请信息并提交以下材料：

（一）《机动车行驶证》复印件；

（二）车辆使用人身份证正反面复印件；

（三）租用仓库的区内单位提供仓储服务合同或房屋租赁合同复印件（只需提供合同首页、带合同有效期页及双方盖章页）。

以上材料均加盖申请单位的公章。

长期备案和短期备案车辆发生员工离职、客户终止合作等情形的，原备案的企业应在平台申请撤销车辆备案资格。

人员需求：

由于目前新冠疫情反复，综保区受疫情影响，需要对园区进行静态管理，为方便静态管理时提前了解企业入园人员信息，减少人员前往卡口聚集登记，需通过线上方式进行预约登记。预约数据需要园区管理方进行审核通过后，方可生效，

人员可进入园区。

为方便企业办理车辆及人员备案，便于园区管理方审核并长期留存车辆、人员入园历史数据，需建设系统进行管理。

园区运营管理平台

园区智慧党建系统需求分析

为进一步提升园区党建工作水平，充分发挥党员职工的先锋模范作用，全面提升基层党组织的战斗堡垒作用，通过党建引领作用，实现党建引智助推发展、党建引资助推发展、党建聚力助推发展的作用以党建高质量发展推动园区经济社会发展。主要业务需求如下：

党务管理系统主要包括党员管理、党籍管理、党费管理、三会一课管理等功能，可对党员电子档案的维护，实现对党员大会、党支部会议、党小组会议、党课情况的管理。动态维护党员党籍变化，实现系统内部全程跟踪管理。进行主题党日活动的策划，搭建党组织基础信息库。

党建服务系统可为党员定制和发送政治生日贺卡、礼物、祝福语，体现组织和党员的温暖关怀。收集党员意见或建议、解答党员疑问、处理举报投诉，并进行满意度评分，促进良性互动。在线发起爱心公益，并对公益活动进行排行展示。实现对困难党员的关爱帮扶。

监督考评系统需通过清单式量化考评，常态化开展党建督查，梳理细化出园区党建工作的重点督查内容，明确了重要工作落实情况、非公企业党组织班子运行情况、打造党建综合示范点、党建工作特色亮点做法、党建问题整改情况等，逐级传导工作压力，推动从严治党向园区党支部和党员延伸。

园区决策分析系统需求分析

园区决策分析不仅有很强的数字感知能力，汇集传导融合能力，还有快速反应能力，凝聚了从数据的提取、关联分析、指标的生成、数据统计、预警分析，趋势判断等等各项功能，从功能应用上，分为以下几个主要方面：

统计管理：统计管理涵盖的数据范围包括宏观上的主要业务数据、生产动态数据统计，如集装箱吞吐量、快件邮包吞吐量、玉宝石/免税品吞吐量、货种统计等。现有模式下，数据的统计和整理往往由完全人工采集，或人工+系统采集

后，最终由人工验算得出统计结果。占用大量人工、时间和精力，计算成本高且由于疏忽导致的错误，统计时效和统计结果都尽如人意，而且往往计算量越大越容易出错。同时，统计效率限制也导致了统计业务及类型较少，仅能满足基础需求，难以拓展且难以进行多维度的分析，找到精确的影响因素和结果。因此，亟需智能手段实现自动计算、统计模式，实现由传统向数字化、智能化的转变。

综合管理：综合管理涵盖的数据范围包括一般政务管理、备案数据以及其他数据，如备案企业信息、经营企业信息、仓库/场站经营单位基本数据、制度规章查询等，综合管理类的数据大多以静态数据为主，随着时间线的发展变化波动较小，但是相关数据的重要程度并不低，综合管理主要面向政务人员、管理人员提供服务，以自动化数据导出、报表等方式替代绝大部分人工记录工作。通过全便利化方式满足相关人员汇总统计使用需求。

通关时效：通关时效是指相关于综保区监管单位，海关等部门的各类关键性数据的统计和分析，现有模式下，由于受到政策不透明，需求没有完全共享的限制，监管类数据与物流类数据没有很好的结合，形成合力。通关环节是综保区的重要业务环节，很多关键性指标能够体现一个园区的“健康”程度与发展程度，这些指标包括：进出口通关时长，进口放行统计、出口放行统计、免税品申报统计、车辆进出区统计等，系统将通过对数据资源的发掘、整合，改变传统模式下物流环节数据与监管环节数据相互独立的现状，形成平行联动的有机数据整合模式，为推动口岸通关效率的提升提供重要支撑。

物流管控：物流管控数据是有着数据量大，分类庞杂，涵盖内容多的特点，每个物流节点完成斗可能意味着下一个、或者多个新节点的开始，业务的涵盖范围包括：综保区关键性物流节点数据、存储数据、放货数据、堆存数据、电子单据动态数据等，以出口运抵动态为例，传统模式下，报关企业需要通过电话、微信、QQ 等主动的、反复的跟踪运抵审核状态，在审核通过后，才能进行下一步的出口报关工作。本次系统建设拟提供一站式全程查询，帮助企业提升效率，有效降低沟通成本。

指标分析：指标分析是对综保区经营性、管理维度的重要指标进行数据综合服务管理的功能。传统模式下，由于数据提困难，没有设定科学的指标管理科体系，而往往忽略，或者省去了大部分指标分析。本次园区决策分析系统的建设将打造科学的指标管理体系，制定严谨的数据统计过程和推算依据，利用系统优势帮助用户实现各项指标的分析和比对。并以此为基础不断完善、发展指标分析体

系，适应新形势下业态不断增长的需求。

预警管理：预警管理是安全管理的重要支撑功能，通过园区决策分析对历史数据进行挖掘和统计，辅以人工经验生成的预警规则，实现对预警管理功能进行可持续的配置和优化，在对相关数据采集分析后，系统根据预判规则自动生成的预警提示，起到了重点监督，快速分析的作用，为整个口岸安全生产、安全管理保驾护航。

产业分析主要用于分析园区产业现状，通过对企业数据、行业数据、经济数据进行分析，了解园区企业发展趋势、园区产业分布、产业链分布，优化园区产业结构，调整产业政策，促进园区产业发展。

智能报表：是以互联网为基础设施和创新要素，利用大数据、云计算等技术，为在海口综保区内注册的企业提供生产经营情况、建设投资情况、财务状况报表的填写及上报。企业需按要求向海口综保区经济发展局提供统计资料，通过对上报的材料数据进行综合分析，让园区更好的了解和掌握海口综合保税区各产业及综保区企业的发展状况。为指导、引导园区及企业发展，为各级政府和各有关部门制定相关政策、实施管理与调控提供参考依据。

安全生产管理系统需求分析

针对园区安全生产管理，需建设安全生产管理系统，满足园区安全管理需求，结合园区视频监控系统、消防监控系统、弱电集成系统等园区现有的必要设备情况，对园区公共区域和入驻企业开展安全生产巡查，及时消除事故隐患，并对公共设施、设备进行日常检查和维护。以企业重大危险源管理、应急资源管理等业务为主，主要包括安全生产一张图、园区封闭管理一张图、园企信息管理、园区风险隐患双控、教育培训管理、日常安全管理等模块，实现安全生产综合管理。

安全生产一张图功能汇聚安全生产数据资源，对安全生产风险进行标准化、流程化评估，可快速、全面、准确地掌握辖区内企业安全风险分布和变化情况、隐患排查治理情况及重大危险源监管情况，对当前安全生产工作的工作量和工作压力进行初步判断，确保安全生产监管工作有的放矢。

园区封闭管理一张图功能结合园区人员、车辆定位信息、电子围栏数据、出入卡口数据、高点监控视频等感知手段和信息资源，确保园区各项流动性因素得到有效管控，为园区企业提供安全可控的封闭化管理环境。

园企信息管理主要是采集、掌握企业安全生产信息，实现对园区内企业单位的基本信息、机构信息、安全管理人员、特种作业人员、伤亡事故、设备设施和作业情况、评审情况、证照情况、安全生产制度、危化品等情况的普查、登记和查询、统计、分析。

园区风险隐患双控功能指针对企业安全生产风险分级管控与隐患排查治理，风险分级管控首先进行风险辨识、分级并采取管控措施，再根据各风险点的管控措施是否到位、各项管理制度等基础管理情况制定隐患排查治理清单。

教育培训管理可为园区相关业务人员增强危机意识和责任意识，提高突发事件防范能力，并提高应急救援人员的应急能力，从而保证应急防控方案贯彻实施。

日常安全管理功能包括特殊作业管理、特种设备管理、安全生产责任网格管理及履职考核管理，加强事前防控，为园区安全生产提供保障，企业端实时和及时更新有关涉及生产安全的信息数据。

为实现和辅助海口综合保税区管理部门及相关政府单位对海口综保区的贸易情况进行监测，需对现有信息资源进行深入广泛研究和充分整合。

建立全景展示管理子系统，逐步实现数据共享、数据查询、数据统计、分类布控和解控等功能，为政府和外贸企业提供功能强大的外贸互动工具。政府管理决策部门、口岸职能部门、外贸进出口企业等综保区业务相关方甚至全社会各部门、机构、个人，均可以通过全景展示管理系统获取其所需要的信息资源，因此全景展示管理系统建设对于口岸来说非常重要。

展销综合服务平台

云展综合服务系统需求分析

常规的线下展示，受到疫情、宣传、运输、布展、设备调试等多方面的障碍因素，展示的效果难以预计与把控。随着全球经济的数字化转型，为综保区内企业提供线上展览服务，解除空间、时间限制，成为促进企业形象展示、商品展示的新途径。云展综合服务系统主要从线上展览展示系统、主办营销推广系统、线上商贸洽谈系统以及线上展览管理系统展开。主要业务需求如下：

线上展览展示系统：展会主办方可以采用虚拟数字场馆模拟线下办展的全流程，有真实的带入感和场景感，在线上呈现看得见的服务，使观众和展商获得良好体验。

主办营销推广系统：可以实现短信、邮件、微信公号、海报、视频直播和图片直播等统一账号，统一平台和数据的营销推广。基于主办营销推广系统，可以激活参展商和采购商历史数据，数据标签化管理，实现针对性的招商招展工作。

线上商贸洽谈系统：基于预约洽谈工具、在线直播系统以及即时通讯工具实现参展商、采购商在线洽谈和询盘，实现买卖双方的云上交流和对接，促进买卖双方的商贸合作。洽谈结束后可通过问卷进行调研，并对洽谈质量进行打分。

线上展览管理系统：通过对主办方、参展商、展厅的管理，实现对展览的统一管理，提高展览运营管理效率。并通过对数据分析、展示、预警实现对品牌传播的量化和效果的转化，便于会展后的复盘和跟踪。

宝玉石交易服务系统需求分析

为中外珠宝玉石企业提供一站式信息化服务。需构建以宝玉石“身份证”为载体的追溯体系，集宝玉石跨境交易、竞价拍卖、评估鉴定、保税仓储物流、政策指引等核心环节为一体的交易生态圈，打造一个全生态链的宝玉石交易平台，提升宝玉石行业的诚信度。主要业务需求如下：

商品展示销售：展示所有商品，包括自有商品和联盟商家商品，并实时更新，买家可通过该平台购买商城的商品。要求前台设计以用户为中心，方便简捷的实现用户购物流程。同时可以实现与主流社区、微信、微博等分享互通。

支付结算模块：对商品订单进行在线支付，支付方式包括积分支付、网银支付、支付宝支付、微信支付等，并进行宝玉石支付鉴定。

后台管理子系统：对商城网站所有的信息进行后台管理和维护，包括进销存管理、用户管理、订单管理、商品管理、营销管理、财务管理、数据分析、权限管理、宝玉石加工管理等功能。

资源云交易系统需求分析

近年来，因边角料管理违规被海关处罚的企业屡见不鲜，企业容易出现诸多问题，除了一些企业别有用心故意逃避监管的做法外，很多企业在理解海关对边角料的管理及处理问题上存在误区：边角料处理必须等到手册核销时才能进行；实际损耗与合同备案损耗不一致时，简单地以合同备案的损耗数量报税；不同材料的边角料混在一起，因无法区分而认为可以不做记录。

同时，企业内部对于处理边角料也存在诸多不透明，企业无法及时找到最合适、最高价的交易对象。导致边角料低价处理或者质押库存等成本浪费，并且影响到企业资金流转，更可能导致企业内部非法交易等腐败现象的产生。

在以上误区以及风险的影响之下，参与加工贸易的企业以及其监管单位急需一个公平公正、透明安全、实时交易的在线交易平台来处理企业内部因加工而产生的边角料，层挖掘边角料的可用价值。

随着海南自由贸易港的发展，酒类、腕表等高奢产品的交易随之增加，为了提升海口综合保税区的发展，充分发挥综合保税区的业务价值，需增加高奢品的交易模块建设，以对业务进行支持。

作业综合服务平台

一体化 ERP 云服务系统需求分析

根据园区的发展要求，需对园区的基建项目、物业管理、防疫风险进行管理，主要用户为规建局、园管局、社事局。一体化 ERP 云服务系统主要包含基建项目管理子系统、物业管理子系统、防疫风险预警子系统，基建项目管理子系统主要用于规建局对园区开展的基建项目进行全方位管理，物业管理子系统主要用于园管局对园区的物业服务进行管理；防疫风险预警子系统主要用于社事局对园区的疫情防控进行预防管理。

智慧云仓服务系统需求分析

海口综合保税区作为全省最大的免税品分拨和仓储物流中心，全省最大的跨境电商的局聚集地，还拥有高附加值的免税加工政策，建设智慧云仓服务以满足监管、统筹利用、为入驻企业打造全流程的仓储物流服务。保证货物仓库管理各个环节数据输入的速度和准确性，确保管委会及时准确掌握库存真实数据。同时可实现对园区自有仓库、企业自建仓库的全方位的管理工作，包括仓库类别（冷冻库、危险品库、普通库等）、仓库余量、仓库温度监控等；还可对仓库租赁期限、租赁费用进行管理，提高管理效率。

整个系统分为仓储服务子系统、云仓联网辅助监管子系统、仓库租赁管理子系统、视频管理子系统，通过业务的有效集成，为仓储人员、运输管理人员、移动端操作人员以及客户等不同角色的参与方提供服务。

物流运输管理系统需求分析

物流运输管理系统主要包含物流服务子系统、简化进出区管理子系统、分类监管辅助管理子系统，主要用于物流服务和各大园区主要业务物流申报管理支撑。利用物流信息建设实现物流交易信息化平台，让找车找货更放心，让发车发货更简单。通过系统建设集理货、委托、竞价、合同、结算、保险、担保、运输跟踪、数据接口等一系列的电子交易流程和交易体系，让商流和资金流立足于线上，基于线上来落实线下的物流服务。通过交易监控，用户管理，运营推广等增加平台的粘性，活跃园区的交易，促进物流产业在园区整个生态链的良性发展，最终达到以下目标：

（一）搭建车主与货主的信息交流桥梁

基于信息化的沟通手段，提供无时不在的连接服务，让信息的发布与广播更方便与快捷。替代以前以前人工打电话咨询、报价的费时费力的方式，提供整个交易的沟通效率。

（二）实现交易的安全保障，由园区背书加交易保障金机制降低了虚假信息的发布，减少了交易纠纷的产生，促进交易的良性发展

园区目前无物流资源交易信息平台，交易管理体制呈现条块分割的模式，这使得园区物流交易难以整合全部资源，造成物流交易发展规模不大重要原因。物流交易资源交易信息平台涉及诸多行业和部门，这些条块分割的部门都有各自的监管体系，而各个地方也都有自己的势力范围和控制范围，统一规划欠缺。一个统一的物流资源信息交易信息平台，需要将这些环节打通并整合，对存在着资金瓶颈、平台建设和推广应用进展缓慢、交易难、运营难、监管不清晰等问题，通过物流资源交易信息平台功能来系统化的解决。通过整合信息资源和市场资源形成区域内的统一网络平台，活跃交易，吸引区域资源聚集，做大做强物流经济。

简化进出区管理子系统的建设便于总署、直属海关、隶属海关各层级对空港综合保税区简化进出区、飞机维修、一般纳税人业务进行线上管理、监控分析以及内控管理，有利于提升美兰机场海关特殊监管区域信息化管理水平和监管效能；促进监管模式和监管资源配置的优化，更好地适应和促进美兰机场海关特殊监管区域及其承载的新兴业务发展。

分类监管辅助管理子系统主要功能是对非保业务及新兴业态等特殊业务进行管理与监控。系统以企业为单元，以账册和业务单证作为基础，贯彻总署相关

要求，对特殊监管区域业务进行一体化规划与作业流程设计。全面支持与覆盖非保及特殊业务，将特殊监管区域内的货物流、单证流与信息流有机结合，实现数据智能化管理，对进出特殊监管区域的分类监管货物的进、出、转、存等环节实施全方位监管，构建统一、完整、分层级管理的分类监管辅助管理系统。

供应链金融服务系统需求分析

整合园区在投资建设、物流贸易、综合运输等方面的资源，集中优势打造功能清晰、主业突出、特色鲜明、充满活力的核心企业，建立架构灵活、扩张性强、支持多元化业务拓展的供应链金融信服务，为资产方、资金服务商、银行合作方、增值服务方等提供前台撮合交易服务和后台 SAAS 管理服务，助力综合保税区内中小企业的高速发展。

主要业务需求如下：

客户管理：进行客户基本信息维护、客户拜访记录维护，然后对客户基本信息、证照信息、股东信息等进行审查。根据客户提供的资料，对客户进行信用评级，确定客户可以开展的业务品种以及融资额度等信息。

应收账款融资：支持应收账款借贷额度的管控，能保存额度批复编号；能够依照应收账款合同，完成各业务品种的额度授信管理，在系统内实现对卖方、买方、担保方等各方授信额度的管控，同时也支持额度的组合控制，所有额度品种都可以通过配置方式来实现。完成额度授信后，银行按照额度进行放贷评估，完成应收账款融资业务。

订单融资：围绕核心企业订单信息。对订单的真实性、准确性、合法性进行综合判断。从而完成订单授信。系统需与报关系统、企业生产系统做对接。完成信息流的有效验证，从而确定订单的有效性。最终实现额度授信。

融资租赁管理系统需求分析

以承租人、供应商、融租企业、保险公司等角度出发，需基于融资租赁风控模型，为融资租赁企业提供全业务周期“一体化”。系统主要业务需求如下：

平台介绍、企业注册、企业准入要求描述、政策法规讲解、融资产品介绍、新闻资讯浏览、企业资质查询、可进行融资申请、企业还款、逾期信息提醒、欠款追回、对接保险系统完成投保操作，进行投保信用融资审核、保单管理、保单

赔付、补贴审批、补贴发放、追还欠款返还、银行资质管理、产品管理。需要支持直租、回租、经营性租赁等多种业务模式，实现可视化高效管理。兼具以运营管理为基础，以决策分析为核心的企业管理模式。使得决策层和运营层紧密结合，提高企业管理水平和增加企业经济效益。支持对接银行风控体系介入系统帮助企业完善承租人准入标准、合理规划承租人授信管理、进行智能风控识别、减少贷款坏账率，提高工作效率，降低工作成本。

免税交通工具管理系统需求分析

免税交通工具是综保区试点业务，服务免税交通工具全产业链服务能力，并为其认定和管理的会员企业提供通关手续、仓储物流、展示销售、售后服务、 金融支持等一站式服务的企业。免税交通工具管理系统是服务免税交通工具产品质量追溯、通关协调为目标综合服务平台，要按照“一品（交通工具）一档” 的原则建立应用系统。系统支持多种贸易方式和物流作业方式，打造海关监管、物流作业、车辆检测、车辆保存的综合性监管和服务平台等功能。主要业务需求如下：

（一）先入区后检测模式：

1.企业申报免税交通工具清单，与转关申报单比对后形成物流底账；

2.企业发起调拨申请，将整车集装箱从口岸场站调拨至检测线场站；

3.企业发起拆箱申请，海关审批通过后，在检测线场站进行拆箱作业；

4.在拆箱作业完成后，进行贴标、理货、安全检测等作业；

5.开展保税业务的免税交通工具，在理货、检测通过后，由特殊区域系统发起调拨申请，通过一体化系统发送至整车系统，运输至特殊区域开展保税业务。

（二）先入区后检测模式：

1.企业申报免税交通工具清单，与转关申报单比对后形成物流底账；

2.企业发起调拨申请，将整车集装箱从口岸场站调拨至特殊区域进行保税业务；

3.企业发起拆箱申请，在特殊区域监管场所进行拆箱作业；

4.在特殊区域监管场所内完成贴标、理货作业；

5.车辆检测由企业在特殊区域系统发起调拨申请，将整车调拨至检测线场所进行安全检测作业；

6.检测报告合格、报关单放行后企业方可申请提免税交通工具，并在海关审批通过后可提免税交通工具出场。

冷链协同管理系统需求分析

扎实推进新冠肺炎疫清防控工作基础上，充分做好冷链货物消毒、检测、溯源必要措施；有效防范新冠肺炎疫情通过进口货物输入风险，实现“安全、有效、快速、经济”的整体防控目标。构建一个追溯可视化体系，汇集单一消杀作业现场或不同消杀作业业务现场各个消杀设备在作业过程中产生的数据，并对数据进行分析、处理、存储和展示，实现对消毒作业的存证、生成二维码、消毒证明及扫码追溯等功能，同时监控大屏可与作业现场进行远程可视化交互。主要从四个环节进行协调：主要业务需求如下：

1.口岸环节。进口企业如实申报进口冷链货物的相关信息，平台根据冷链货物入境信息、提运信息等相关信息，制定检测、消杀、监测计划。对于检测为高风险货物（即新冠监测为“阳性”）的，根据相关要求进行退运或销毁处理。平台实现相关人员、运输工具以及污染环境全面跟踪。对于检测为低风险货物，指导督促查验场地经营者或进口企业，对进口货物的集装箱内壁、货物外包装实施消毒。消毒完成后，消毒单位出具该批货物业经消毒的证明。未在口岸环节消毒的进口冷链食品按规定放行后。在后续环节予以消毒。全程托运、理货、进出口岸等相关信息传输至平台。

2.货物运输和出入库环节。进口冷链货物在从集装箱卸货换装至国内运输工具时，货主或其代理人对货物包装实施消毒。进口货物运输过程中，承运企业不得开箱，在国内运输段交通运输管理部门要督促指导落实运输车辆船舶等装载运输装备消毒和一线工作人员个人防护等措施。仓库接受进口货物时，应如实记录并核对集装箱号及消杀信息，做好货物的出入库记录，相应数据信息传输至该平台。

3.流通环节。对从口岸放行的进口冷链货物，在社会库房或企业库房倒箱过车、入库存储前，相关生产经营单位查验货物所附的消毒证明，如未消毒，则在掏箱卸货时，对该批货物的渠装箱内壁、货物外包装实施消毒。消毒完成后，消毒单位出具该批货物业经消毒的证明。生产经营单位对需打开外包装的货物的内包装实施消毒。相关信息记录至平台。

4.市场环节。进口冷链货物销售市场要加强管理，规范市场卫生环境，做好销售场所的日南消毒工作。要严格落实防控要求，加强进口货物溯源工作，防止未经过预防性全面消毒处理的进口货物进入市场。做到所有进入市场的进口货物来源可查去向可追。

跨境电商新零售管理系统需求分析

海口综合保税区开展跨境电商新零售业务，在区内开设跨境电商新零售店铺，游客可入区选购跨境电商商品。为帮助开展跨境电商新零售业务的企业完成售出商品的通关申报，实现综合保税区对出区跨境电商商品的溯源管理，需建设跨境电商新零售管理系统。

系统主要实现跨境电商核注清单、核放单的自动申报，并生成溯源二维码供企业贴于货物包装上，供买家进行溯源。系统提供接口供人行闸机调用，进行清关后商品的出闸验核。

溯源采集管理系统需求分析

溯源采集系统核心需采集的数据如下：

1.生产加工环节：生产企业生产信息；生成溯源二维码，以身份证的形式贯穿货物流通始终。

2.口岸通关环节：外贸企业货物信息采集；口岸监管三证信息采集；进境货物若无生产加工环节信息，可在本环节生成溯源二维码。

3.交通运输环节：运输车辆及司机信息备案；货物运抵地信息备案。

4.贮存转运环节：仓储信息采集；场所信息采集；检验检疫信息采集；流通下一环节运抵地采集。

5.销售使用环节：销售使用去向信息采集。商品进入流通环节后，消费者、企业及监管部门通过溯源码或网页查询快速获取全链条溯源信息及特殊状态提醒，同时可进行咨询、举报或投诉，动员全社会质量相关方通过信息反馈参与质量管理。

6.其他信息采集：第三方检测机构信息采集。

辅助监管业务服务平台

智能场站管理系统需求分析

货运场站是综保区内口岸物流的延伸。货物在综保区进行集拼、分拨、通关的主要场所。需要对场所内的计划、实际业务操作、结费等方面进行全方位的业务管理，同时，还需要在统一服务接口的支撑下，与单一窗口等系统进行数据互动，构建一套及客户服务、计划制定、实际操作、动态监控等为一体的综合场站信息管理系统。

智能场站信息管理系统需包括预确报管理、货运计划管理、装卸作业跟踪、换装管理、堆场管理、堆场终端应用、仓库管理、仓库终端应用费收管理、综合查询统计等九大子系统模块。

多式联运服务系统需求分析

货物托运人或其代理人为了进出口货物，通过系统向相关外贸企业提交电子化的委托、订舱、班列管理、集装箱管理、在线报关、财务结算等，承接方在接收到申请后给予回执并制定相关电子单证的一整套完整的电子化标准化流程，以整合资源，促进多方联动，协同发展。主要业务需求如下：

货代进入委托书录入页面，填写订舱申请、租箱信息以及其他委托申请并提交至陆港审核，陆港审核通过后，将结果回传。

系统根据委托书审核结果自动生成订舱回单，供货代在单证下载模块进行下载和导出。

箱管部接收到箱属为 COC 的委托书后，对于提箱地为北站的订舱回单，进行确认放箱操作，系统自动生成放箱令供货代下载；对于提箱地非北站的订舱回单，上传对应放箱令后供货代下载。

订舱接单后，系统根据箱量自动生成对应数量的清单数据，货代进行清单详细信息的补录后提交至汉欧审核，陆港操作部接单后可对清单进行发运前的部分信息上传，确认发运后，清单信息不可修改。

清单确认发运后生成对应的发运数据，操作部可对发运清单进行运踪的导入和添加，货代也可实时跟踪集装箱物流信息。

清单确认发运后自动生成对应的提货通知书以及提箱密码，供货代在单证下

载页面进行下载和导出。

清单确认发运后，对于箱属为 COC 的发运清单，箱管部进行还箱确认后系统自动生成对应的还箱令和还箱台账，供货代在还箱令页面进行下载和导出。

根据放箱结果，在系统上，填制报关单，同时将填制后的报关单发送至中国或合肥单一窗口，进行报关作业。对于涉税报关单，系统对接单一窗口税费支付功能。报关结束后，根据退税需要，通过系统与单一窗口对接，完成出口退税申报。

清单确认发运后，系统根据已维护的运费标准自动生成发运清单的铁路运费数据，财务根据已生成的运费信息以及其他杂费生成对账单并提交至商务部以及货代确认，两方确认后生成开票申请单，后续财务操作流程沿用现行程序。对运踪实时跟踪，全流程查询。

园区跨境电商服务系统需求分析

海口综保区抢抓跨境电商业务发展机遇，充分发挥海关通关一体化政策红利，积极发展跨境电商业务，目前已有 50 多家跨境电商企业入驻园区开展 9610 跨境直购与 1210 保税备货业务，创新推出跨境电商线上线下融合模式，国内知名电商唯品会在区内建设面积为 7 万平方米的跨境电商亚洲物流中心，海南新毅国际、海南高培乳业、海南君和君美等企业、海南优选、黑虎科技、海南适成等跨境电商企业在海口、三亚等商圈设立线下体验店，给市民及游客带来了更好的消费体验。

为进一步服务区内企业，加大跨境电商招商力度，吸引更多国内外知名电商平台入驻园区，园区复制推广跨境电子商务综合试验区“六体系两平台”等成熟经验做法，建设跨境电商线上综合服务和线下产业园区“两平台”。目前海南单一窗口已集成国口办跨境电商线上综合服务平台，需要进一步建设线下产业园区平台，为入驻企业提供信息化服务，降低跨境电商企业开展业务的信息化成本，既满足企业的业务需求和园区的监管需求。

业务需求主要包括开展跨境电商的各个角色的企业信息备案、开展保税业务的账册备案、9610、1210、9710、9810 业务模式下的订单、运单、支付单清单数据查询、业务支撑和辅助申报功能。

免税品辅助管理系统需求分析

为满足海口综合保税区免税品出入区货物的管理，园区卡口进行自动抬杆并在区内设立监控设备，可实现保税品货物出入时实行虚拟过卡，将最大限度地提高园区内的工作的效率，促进园区的业务发展。为实现区内免税品出入管理的信息化建设，需要建立配套的免税品辅助管理系统对出入园区的免税品进行记账式管理。园区的业务需求主要包括开展业务时的账册备案、货品出入区时对账册进行核增核减、各企业的信息备案、核放单申报及数据查询功能。海口综合保税区免税品辅助管理系统主要分为企业端及监管端。

海口保税区免税品辅助管理系统企业端主要是为了满足企业用户的需要，通过该系统可完成企业的账册备案、免税品核放单（出、入）区申报、区内保税品转免税品入区申报、区内保税品转免税品出区申报、区内免税品转保税品入区的申报、账册调整、调整单申报、（出、入）库准单绑定、核注清单（进口、出口）申报、核注清单变更、核注清单核查、综合查询等要求，为企业提供便捷的对接途径。

海口保税区免税品辅助管理系统监管端主要是为加强简化海关作业审批手续以及对企业用户申报数据进行审核，包含账册审核、调整单审核、免税品核放单人工审核、人工过卡、核放单预警处置等使货物在园区内自由流转。

支撑平台需求

统一用户/权限管理系统需求分析

为智慧园区平台提供统一身份认证，实现不同系统和用户一点接入进行统一身份认证，同时使用户在权限范围内进行合法操作，提供身份认证功能和权限管理。主要业务需求如下：

统一身份认证：对园区统一门户所集成业务系统用户身份进行统一认证管理，包括用户基本身份信息管理、业务系统访问授权管理。用户通过单点登录进入业务系统，系统对其登录人员身份信息，所授权访问的业务系统进行认证管理，控制用户只允许访问已被授权的业务系统。

单点登录：实现用户对所集成的业务系统的一点登录，业务用户登录成功即可访问经统一身份认证授权的业务系统，在已授权的业务系统之间进行切换时不

再需要进行登录操作。使用户方便、快捷的进行业务操作。

数据交换系统需求分析

基于智慧园区建设的成果，需构建统一的数据交换系统，实现园区与大数据局之间、监管单位之间、管理单位之间、企业之间的交互标准，实现对基础数据的统一管理，构建统一的数据主索引，打造统一数据枢纽，实现各系统之间数据的规范、集散，并为大数据展示及数据挖掘奠定基础。通过数据交换系统也可以将数据服务扩展到整个海口，为企业提供数据查询。

订阅分发系统需求分析

随着各类业务系统的上线，系统之间的交互也越来越频繁，数据访问、订阅、分发的业务也变得错综复杂。为减少数据孤岛产生的数据搬运问题，减少系统运行压力，降低系统安全风险，增强系统可扩展性，建设数据统一管理、高效服务、安全稳定的订阅分发平台。系统采用事件触发器的方式，需提供业务数据的订阅和分发，通过格式化的数据订阅的申请、审核、触发、接收和回执流程，标准化的管理数据的订阅和分发工作。

统一 API 管理系统需求分析

为了更好的发挥数据中心的作用，需将平台运行时产生的大量多数据源的实时数据接入实时数据中心对应的实时数据库。在接收数据时，每种数据源都需要对应的数据接口，由于接口实现方式、源系统厂商等都不一样，随着接口数量的增加，势必增加运维和管理难度，需实现对所有数据接入和访问接口的统一管理。

智慧海南体系对接需求

与海南省大数据管理局对接

海口综合保税区智慧园区建设项目将通过与与海南省大数据管理局进行平台对接，传输海口综保区内的基础设施数据与业务开展数据，为智慧海南能力中台提供数据基础，为构建海南自由贸易港智慧大脑添砖加瓦。另外也将通过大数据管理局数据平台订阅园区开展的业务相关数据，打通园区与其他管理机构的信

息壁垒，辅助海关对园区开展业务进行监管，简化企业的申报流程，减少信息录入。

需对接数据包含海南单一窗口、海南公共服务平台、国际贸易投资单一窗窗口、海口海关监管系统的报关单表头数据、验放指令、仓库实时视频、跨境电商清单、人员健康码数据等。需预留与统计局的接口，传输报表统计数据；预留与海口海关的数据接口，传输核注清单、核放单数据。

与一线口岸对接

目前，海南省设立 8 个对外开放口岸，为满足全岛封关运作“一线”进出需要，设立 10 个“二线口岸”保障“二线”进出需要。海口综合保税区作为特殊监管区域，区内会开展 “一线、二线”业务，为了区内“二线”业务的健康发展，本项目需预留与“一线口岸对接 ”模块，与航空、水运、铁路等“一线口岸”进行信息对接，获取报关数据、订舱数据、航空舱单、船舶舱单、铁路舱单、一线检疫结果等数据，完善出入区货物的业务流、数据流、物流。

与二线口岸对接

目前，海南省设立 8 个对外开放口岸，为满足全岛封关运作“一线”进出需要，设立 10 个“二线口岸”保障“二线”进出需要。海口综合保税区作为“一线放开、二线管住”的重点区域，需预留与其他 10 个“二线口岸”的对接接口。通过预留接口传输相关货物到达海口综合保税区后的流转及处置，获取货物在其他“二线口岸”的相关数据，完善货物的物流链条，保证票票货物可追踪、可溯源。

信息交换与共享需求

下图为业务对象分析示意图。

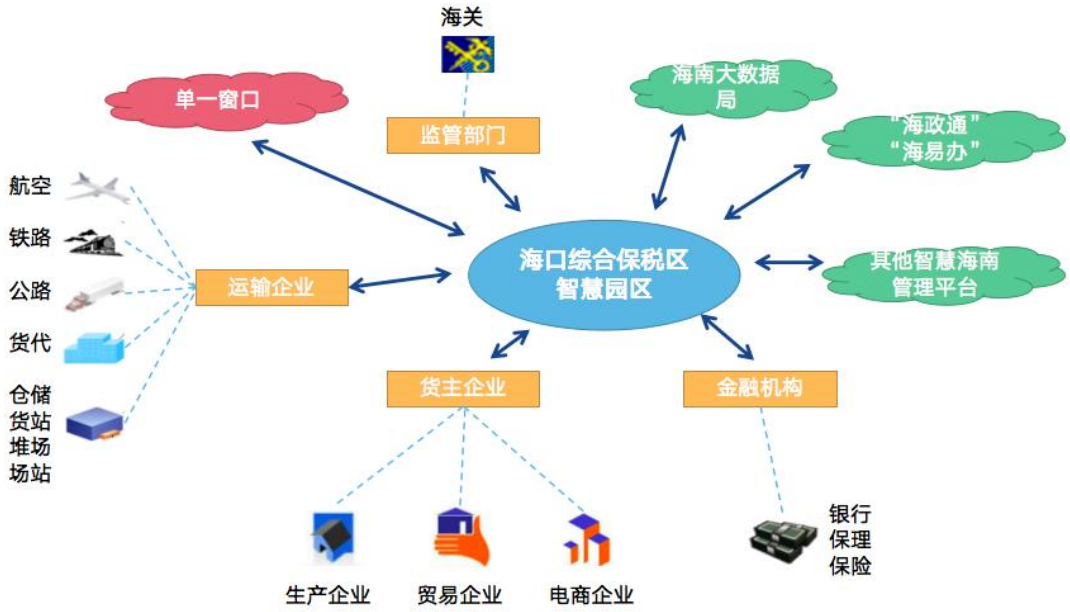


图 4- 2 项目业务对象分析示意图

针对业务对象下面进行简要分析。

与海关监管平台共享需求

实现海口综合保税区与海关辅助管理系统等业务和监管数据的协同，实现企业相关业务的快速办理。

共享数据包括报关单、海关报关状态信息、原始舱单、装载舱单、预配舱单、分拨舱单、装箱清单、转关单、海关放行、查验指令、出库指令、入库指令、理货报告、运抵报告、舱单回执、账册数据、手册数据、监管仓库出库信息、监管仓库入库信息。

与海南国际贸易单一窗口共享需求

信息交换和共享的范围包括但不限于跨境进出口物流单、订单、支付单、清单、回执等信息、企业的基本信息、企业的海关注册信息、企业的资质申请及备案信息、企业的信用评价信息、企业的风险信息、企业违法信息等。

与其他口岸共享需求

与整车口岸系统进行接口对接，以实现车辆信息、理货信息、车辆订单信息、堆场集装箱位置数据、电子提货单数据、查验集装箱数据、运抵报告数据的接收。

与其他口岸港口共享数据，如车辆信息、企业信息、过卡信息、调拨信息、

进出区信息等，做到卡口联动，数据共享。

与外贸企业共享需求

智慧口岸项目需要实现对企业财务信息以及有关进出保税港区货物的库存、转让、转移、销售、加工和使用等信息的全程跟踪。

与政府管理部门的共享需求

各个政府部门间需要高度业务协同参与，实施联合监管。而联合监管的基础，就是智慧口岸平台与各政府部门的系统打通接口，形成各政府部门的协同流程与审批闭环，全面落实企业、区内管理机构、海关等监管部门间的协同监管。满足海南省、社会管理信息化平台、海南省物联感知设施管理平台的管理要求，实现数据信息的交换和共享需求。

与大数据局共享需求

目前，信息共享交换主要是通过省大数据管理局数据共享交换平台实现，按照省、市县、以及单位主管部门级别进行分类，向相关单位共享企业信息、单证信息、车辆信息、跨境业务情况以及园区经营等相关数据。

数据资源建设与开放能力需求

数据资源建设需求

在海口综保区中，所有进出口企业与执法单位、政府管理部门之间的数据往来与共享通过该系统进行交换、处理、转发，根据调研结果与需求分析结果有数据交换需求的有：海关、交通海洋局、海南省单一窗口、大数据管理局等多家单位及平台对接；平台交换、处理、转发数据内容分别有：舱单、报关单、通关状态数据、卡口进出门信息、账册数据、装卸信息、承运资质、在途信息、堆场信息、危运信息、船舶信息等多类数据。

主要数据量估算如下：

（1） 用户量测算：每天用户量为 1000 人次，同时在线为 300 人次，并发用户数最多支持 3000 人次。

（2） 企业备案信息：企业共 3000 家。

（3） 进出口业务量测算：年进出口业务总量 200 万单。

（4） 商品信息量测算：商品总数量 50 万。

（5） 物流业务量测算：物流笔数 10 万。

（6） 展销类平台业务量：交易笔数 15 万。

（7） 应用系统查询频率：每 2 分钟一次。

（8） 数据交换接口对接数据交换频率：实时。

（9） 短信的发送频率：实时。

（10） 与海关的接口数据交互频率：实时。

（11） 与海南省大数据管理局对接接口数据交互频率：每日。

（12） 与“海政通”“海易办”平台对接接口数据交互频率：实时。

（13） 与其他智慧海南管理平台对接接口数据交互频率：实时。

（14） 文件交互频率：每日。

因此，需要依托本项目建设的信息化系统建设海口综保区数据资源库。

开放能力建设需求

按照大数据局要求，将园区的数据资源纳入统一的数据资源共享目录中，供社会公众、企业以及相关管理机关应用。

园区建设面向企业的服务体系，包括覆盖供应链各节点的服务能力，包括仓储、运输等方面的资源或平台服务可按照园区的发展规划，进一步延伸到区外的企业。

园区设施智慧管理建设需求

随着园区信息化进程的演进，以及物联网等系统产品与技术的逐渐成熟，园区整体管理逐渐由传统粗放型向现代集约型转变，提升安全工作管理水平，并逐步成为管理部门决策分析、调度指挥的主要平台之一。主要体现在产业园区的“三位一体”的主体需求，包含政府部门对园区的建设、管理规划的需求，园区内企业对园区服务的需求（包括金融服务，人才服务，培训服务等等个配套服务）以及园区内的人员对在园区中吃穿住行的便捷需求。

下面是整个园区“三位一体示意图”：

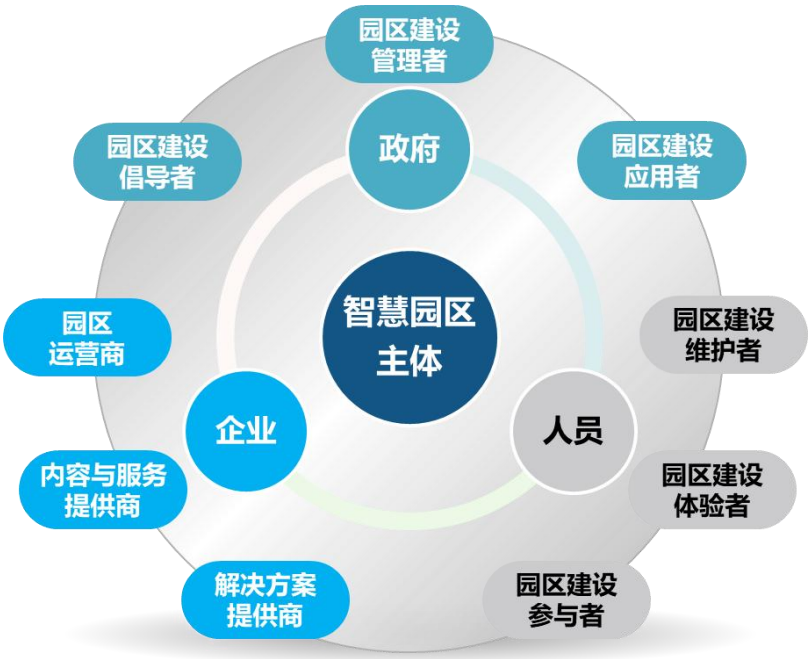


图 4- 3 园区三位一体安防体系

从园区的整个发展阶段来看，园区的需求也有比较大的变化，从最开始的自然资源驱动，到社会资源驱动以及到现在信息和智力资源驱动，不仅在互动模式上从传统的一对一变化为现在的多对多，在整个业务服务内容上也从简单的“土地出让、房屋出租、金融孵化”到现在的“文化塑造、信息融合以及数据分析预判”，让整个产业园区不再是简单的产业聚集，而是一个更加统一的整体。

园区管理逐渐以数字化的方式由传统粗放型向现代集约型转变，提升管理水平，并逐步成为管理部门决策分析、生产调度指挥的主要平台之一。

主要体现在以下几点的业务需求：

1、拉近管理距离需求

打通各自独立的系统、最大可能地消除信息孤岛的需求

实现园区与各企业的统一视频管理的需求

建立数据中心，通过数据中心大屏等形式，监控管理企业运行并可及时处理异常情况。出现异常状况和突发事件时，可以及时报警，提醒管理人员及时处理的需求

对整个企业园区的安防、消防、能耗等各类数据的集中展示的需求

对分散的车间、仓库进行远程统一管理的需求，避免使用人力频繁的去现场监管、检查，减少人员管理成本，提高工作效率

由生产的物理驱动（资源驱动）和管理的流程驱动变为数据驱动的需求

提供远程管理手段提升管理效率的需求

2、提升业务效率需求

对企业园区内人、车运行的有序、可靠、可管理的需求

园区内各地的人员进出权限管控、工作秩序有条理可管理的需求

员工管理科学高效，考勤、进出权限、食堂消费等智能便捷的需求

对资源紧张的物流月台的利用效率的管理提升需求

对作业过程实时监测，辅助产线岗位优化的需求

提升能源运营效率，持续改进能源绩效的需求

对提升巡检效率和密度的需求

提升资产盘点效率，降低人工计数误差，规避漏报瞒报事件的需求

规范作业行为需求

规范作业行为标准化，保障园区和生产规范安全，提升作业质量和生产效率的需求

对不规范的行为（人员动作、穿戴等）进行自动检查和报警的需求

对制造过程的的关键环节进行质量追溯的需求

3、防范安全隐患需求

对整个企业园区（包括周界、人车出入口、公共区域、道路、厂房、办公楼、研发楼等）的人、车、物的安全防范管理的需求

需要对车间、仓库等高价值区域、易燃区域有较高的防火需求，需提前预警火灾隐患。并且可以对环境的温湿度、粉尘、噪音进行监测与超阈值报警。

需要对企业物流车辆进行园区内安全管理。

访客管理需要科学高效，可控可查可管。访客来访后可自助登记，并且可自助达到等待区域，进入非授权区域报警等需求。

对 EPA 区域的安全保护需求。

园区安防的系统设计以增强其科技功能和提升应用价值为目标，以其功能类别、管理需求及建设投资为依据，以结构化、模块化和集成化的方式实现组合，应集系统、服务、管理及其优化组合为一体，为用户提供安全、高效、便捷、健康的生产生活环境。主要考虑以下需求：

（1）子系统的融合

信息孤岛问题一直是困扰客户的最大难题，如果能够将各接入子系统看作是平台的管理模块，实现平台的统一管理、各接入子系统的协调运行，进行整套系统的有机结合，才符合客户的真正期望。

（2）智能化的运行管理

庞大的系统建设随之带来的就是运维的人员成本增加;同时也会影响系统的使用，直接导致使用效率低下；另一方面，随着行业技术的进一步发展，平台的智能化运行管理应用越来越被客户认可，已成为行业的一种趋势。

（3）业务能力平滑扩展

以往一般通过在平台中增加功能模块,或依赖于一个平台去接入其它业务系统。由于整体的复用性较差，带来了相当高的开发维护成本。同时，也影响了产品品质，已经越来越不能适应发展需要。

（4）智能化的应用

安防产品“智能化”的概念提出多年，传统的图像识别和图像处理算法仍然存在着识别准确率低、环境适应性差、识别种类少等问题，严重限制了智能应用的普及。

（5）开放的对接模式

项目运作中，经常会遇到不同品牌之间的合作共建一套智能化弱电系统。第三方业务系统的数据交互、资源共享等问题成为系统集成的一个瓶颈，平台的集成与被集成成为难题，客户希望得到一个非常顺畅的资源交互环境。

通过帮助企业拉近管理距离、提高管理效率、规范作业行为、防范安全隐患来帮助企业提高生产效率、提升产品质量，帮助企业实现工厂全面透明化管控，深入实施智慧企业园区的数字化工程。使管理层明确了解企业业务进展的实时情况，将管理做到“看得见，管得着”。并进一步完善企业园区安全防范功能，提高企业园区运行的便捷性和有序性，加快对企业园区异常事件处理的速度，提高企业园区的综合管理水平。

（6）子系统统一集成

数字化企业运行指挥中心平台（或称为智慧企业园区平台，以下简称为“数企平台”）对各子系统进行统一的管理和控制，实现将分散的、相互独立的子系统用相同的环境、相同的软件界面进行集中管理。提供人员、组织、资源等基础数据的统一管理，保证同一个物理资源在一个产品或者多个产品中的唯一性，可关联并实现一处录入多处使用，为产品互相集成提供机制保障。

（7）平台运行统一监控

数企平台运行管理中心，给系统交付及维护人员提供一站式安装、运行、维护的服务。通过运行管理中心，可实时获知软件的运行状态，根据运管中心提供

的信息方便地定位并解决问题，保障系统的正常运行。

（8）业务弹性扩展

数企平台基于组件化设计，以新增组件的方式满足业务的横向扩展。只需在一套软件下通过增加相应的业务组件即可实现复杂项目的需求，避免以往一个项目部署多套平台的冗杂情况，彻底解决一线人员的痛点。

（9）智能化的应用

数企平台以各类功能与应用整合和集成为核心，实现单纯的图像监控向基于深度学习算法的车牌识别、人脸识别等智能应用领域的广泛拓展与延伸。

（10）应用接口开放

数企平台基于软件集成框架和统一规范，通过 Web Service 及 http 接口提供基础服务，实现应用接口的开放，支持第三方应用快速集成，接口遵循 RESTful 规范。平台通过动态新增设备接入驱动，实现对第三方设备的接入。

（11）通过综合安防与扩充应用提高快速反应能力

大多数企业的组织结构是建立在专业化分工基础上的“金字塔”型组织结构，横向沟通困难，导致对过程变化反应迟缓等，逐渐难以适应日益复杂、变化多端的市场环境。而在信息技术的支持下，综合安防管理可帮助企业优化传统安防管理方式，减少中间环节和中间管理人员，从而建立起精良、敏捷、具有创新精神的“扁平”型组织结构。这种组织形式信息畅通、及时，使信息反馈更加迅速，提高了企业对安全隐患及生产现场问题的快速反应能力，从而更好地适应竞争日益激烈的市场环境。

指挥中心需求

指挥中心是智慧园区中枢大脑，本项目需通过大屏展示系统、集成平台、数据平台、可视化平台等建设以实现统一指挥调度，并可对园区视频、运营数据等实时直观展示，对设备集中监控，对生产统一指挥。

需通过对接园区相关业务系统，如安防、消防、招商、场站、物流、辅助监管等系统，对接园区业务核心呈现和分析数据，实现园区运行数据的可视化展示、智能监测与预警，实现整体运行态势，指挥中心大屏可视化专题页面需包括：园区总览、安防监测、便捷通行、设施管理、敏捷招商、党建管理、数字化运营态势、数字物流运营、业务运营可视化等模块。

指挥中心作为保税区管理的决策辅助系统，平台需以三维模型/实景为载体，将园区运行核心系统的各项关键数据进行综合展现，支持从综合保税区未来规划、基础设施、园区数字运营、数字贸易管理、预警分析管理，智慧物联及企业画像等多个维度进行日常运行监测与管理，以及突发事件的应急指挥调度管理，提供一个集保税区规划、园区生产、园区运营、园区决策多维一体的智能指挥、运营管理平台，为保税区管理者提高园区运行效益以及园区管理效率，并提供数据决策支撑。

智慧安防需求

网络高清视频联网：通过视频监控联网，可为各级管理人员按权限分配各环节现场图像信息，避免现场状况信息汇报的延时，出差在外的管理人员甚至可通过移动网络了解现场实际情况以参与应急决策；

报警联动策略：可设计通过视频分析、人脸识别、黑名单识别等技术进行实时侦测，当有非法入侵等异常行为时，推送报警信息、现场图片等至管理人员手机、邮件以及时响应；

制造过程可视化追溯：MES 信息触发、条码扫描（或 RFID 信息读取等）形成关键岗位生产及操作过程的起始标签，事后可根据条码、货品信息等快速追溯，提高生产管理、售后服务等部门后期问题分解与追查的工作效率；

报警预案：可设置多种报警预案以提高警情发生时的处理速度；

联动策略：门禁、车辆出入口设备等与消防系统联动，消防报警时自动打开消防通道；

移动单兵在线巡查：通过单兵设备巡查，当发生异常情况时可将现场状态以视音频方式及时记录，并通过移动网络传输至中心进行预览，管理人员可及时进行工作调度。

（1）优化人车物管理流程促进企业提高管理水平

系统与管理的有机结合，把先进的管理理念、管理制度和方法引入到管理流程中，进行管理创新，以此实行科学管理，提高企业的整体管理水平。

以下抽取本方案设计部分应用进行说明：

一键巡查：通过车牌登记与识别减少车辆进出验证时间，免刷卡无停留方便快捷；通过车位摄像机，实现停车引导与反向寻车，可在较大型以上停车场降低

员工停车消耗的时间；

车牌识别：通过车牌登记与识别减少车辆进出验证时间，免刷卡无停留方便快捷；通过车位摄像机，实现停车引导与反向寻车，可在较大型以上停车场降低员工停车消耗的时间；

优化访客预约管理流程：结合一卡通与数企平台优化访客从预约、申请至授权进出的整个流程管理，减少员工接待的无效工时，提升企业的对外形象。

（2）辅助业务管理有效地降低企业成本

企业的成本来自于生产经营和管理的各个环节，安防系统应用，特别是基于视频监控系统的可视化管理系统与基于一卡通系统的人员管理系统，多年来通过系统单一建设满足各部门某一具体场景的应用需求，零散的与生产经营管理的各个环节产生关系，本方案实施建设后，通过数企平台建设，可为企业降低运营管理成本提供多种辅助手段。以下抽取本方案设计部分应用进行说明：

视频远程联网：通过视频对员工工作状态与现场生产经营状况的远程监督指导，降低管理人员的出差、现场巡视产生的成本；

车载监控、GIS 定位辅助物流管理：通过在物流车实施车载监控系统，可实时了解物流运输情况，按需进行视音频远程调度；分析历史数据，结合降低成本、提高效率要求进行排班、优化物流路线规划等；

仓库管理：对仓储环境变量进行实时采集与联动，提防环境变化对原材料、半成品、成品质量的影响而导致浪费。

热成像防火管理：对仓库、车间的防火管理，相比传统的温感、烟感的探测方式，热成像防火管理方式可以及早发现火情或火险隐患，及时处理，闭门企业的重大损失。

（3）提高企业决策的科学性、正确性

完备的信息是经营决策的基础。基于综合安防系统的众多应用可改善企业获取信息、收集信息和传递信息的方式，减少决策过程中的不确定性、随意性和主观性，增强决策的理性、科学性及快速反应，提高决策的效益和效率。以下抽取本方案设计部分应用进行说明：

物流过程可视化：可在车载视频、GIS 路线回放的基础上为研究物流策略提供数据基础。

（4）标准作业可视化监督提升企业人力资源素质

企业的竞争是人才的竞争，是人员素质的竞争，人员素质在企业竞争优势中

极为重要。企业可视化管理，可以加速标准作业在企业中的传播，使企业领导、全体员工知识水平、信息意识与信息利用能力提高，提升了企业人力资源的素质及企业文化的环境。以下抽取本方案设计部分应用进行说明：

工位监控：利用高清网络视频监控，对关键工位操作过程进行抽查筛选，结合电子看板播放最佳实践范例，引导员工操作标准；

流程监督：可视化远程监督与视音频调度，有利于约束员工实施工作规范；

智慧灯杆需求

通过建设智能路灯为基础，解决道路亮化照明，同时，通过智慧路灯的建设，实现园区基础设施建设。园区的建设中，智慧路灯不仅仅是灯，也是智能感知和网络服务的节点。它像园区的神经网络一样，是整个智慧园区的触角，可实现以下建设目标：

建设以节能照明为理念的亮化工程。整个规划道路全部采用 LED 路灯建设，实现路灯的智能调光、统一管理、节能照明，为整个规划区照明建设节省开支；

建设园区信息发布系统。通过集成在智慧路灯杆上的 LED 显示屏，相关部门能够实现相关政策在线宣传及突发事件即时消息推送等，能够实现广告营销，能够随时随地了解最新资讯，享受智慧园区带来的各类服务；

建设智慧园区安防监控系统。通过 360°无死角摄像头实现园区无死角安防监控。

建设智慧园区信息采集分析系统。通过摄像头采集园区公共设施和道路运行情况，各类传感器采集园区环境信息，集中控制器采集所有智能路灯的运行状况，无线 WiFi 网络了解民生关注需求，通过智慧路灯网络平台，统一传送至云平台，获取园区道路管理、资产管理、环境管理的数据，实现园区的信息化建设。同时可以搭载不同功能摄像机实现不同功能的智能分析，通过分析做出决策。

智慧消防需求

为了充分发挥系统及时发现、预测、预警的重要功能，物联感知终端应尽可能提高覆盖面，系统应能够涵盖整个企业园区，作为传统消防的补充，增加智慧“烟、点、水、气”等智能化检查，减少监测盲区，实现全天候监管模式，防范于”未然”。

针对园区，应将消防、安防系统融为一体，统一建设，安消一体化，达到及时感知，及时预警，防患于未然，防患于未“燃”，鉴于如此，大型商业综合体安消一体化系统应包括如下功能；

1、 消防物联网实时在线监管

结合物联网、云计算等新技术发展，解决传统管理方式的弊端，实现消防管理工作智能化、可视化、痕迹化。将电气火灾系统、消防水系统、消火栓、燃气、烟雾等通过物联网的方式进行可视化管理，实时在线监测，将火灾隐患消灭在萌芽状态。

2、 火灾火情高清视频监控联动

融合高清视频技术，将消防物联系统与视频监控全面融合联动，通过视频查看和监测火灾现场情况，准确判断火灾事故现场，提供更好的应急救援依据。

3、 消防管理体系化建设

建立消防工作信息化的标准化流程，强化单位消防巡查等单位主体责任的落实，提高单位消防自主管理能力，解决单位消防管理无人管、不会管的局面。通过消防预案演练、消防培训、消防设施管理、消防巡查等手段，建立完善的消防管理体系。

4、 高清视频监控系统

在传统视频监控基础上，结合最新 AI 技术，增加周界防范、AR 全景监控、视频结构化等智能化应用，做到实时分析、及时预警、事后取证，提高安防等级，保障文物安全。

智慧能耗监测需求

1．能耗监测

对园区办公大楼配电箱每个用电回路的空开设备进行改造，替换成智能空开，对用电回路的详细能耗指标数据进行采集，实时监测不同回路不同场景用电信息。

2．空调节能

对园区办公大楼不同楼层的空调外机进行智能化改造，通过对空调进行不同模式控制，实现对空调用电进行智能化管控。

3．照明管控

通过对不同场所的照明灯光进行人体感应式控制，使大量无人使用的时间段

内灯光处于熄灭状态，最大程度节约用电量。

4．用电管理

能对回路开关状态进行实时监测，方便对用电环境进行集中管理；根据实际使用需要设置分控管理终端，方便人员巡检与管理。

5．电气火灾风险排查

对园区大楼内原有用电回路进行电气火灾风险检查，对发现的问题进行记录，方便进行整改。对原有回路需要重新进行测量和明确标识，以便完成回路改造规划。

6．电气火灾预防

对回路电气参数进行实时监测，包括电压、电流、温度、漏电等，对异常情况进行预警，包括过压报警、欠压报警、过载报警、过流报警、过温报警、漏电报警、用电量统计功能。能监测回路电火花和电弧现象，防止插座插排及用电设备出现高强度频率打火，避免引发火灾，减少火灾隐患。

智慧查验系统需求

为进一步满足海关监管需求，本项目需通过建设 5G 智能单兵查验系统及 VR 全景查验监控系统，以进一步提高园区智慧查验水平。

5G 智能单兵查验系统的用户主要包括在综保区海关查验场执行查验作业的海关一线关员，该用户需要使用 AR 眼镜、查验 Pad 和执法记录仪，并进行系统日常操作。一线关员在查验作业中遇到无法识别的商品、无法判断的风险情况，需要远程求助业务专家进行求助。系统应用功能需包括智能辅助查验、单兵后台协同、单兵录证关联三种基础应用能力，并基于业务开发的算法实现 AI 分析能力。充分提高海关一线关员查验能力。

此外，需在海口综保区海关查验现场及公共区域，部署 VR 全景摄像机，通过内部网络进行视频回传，保障视频传输的稳定性和视频清晰度。在综保区监控中心可以通过大屏幕以及 VR 眼镜播放现场 360° 全景摄像机拍摄的视频画面，360° 查看查验现场的实况，实现沉浸式指挥。

信息化基础设施和能力需求分析

机房及配套设施需求

现有机房及配套设施已经不能满足综保区改造升级的需求，需要进行改建和扩建。

根据按照国家 C 类机房建设标准设计、建设，依据 GB50174-2008《电子信息系统机房设计规范》和 GB2887-2000《电子计算机场地通用规范》、《海关网络安全管理规定》（署科发[2018]194 号）中的有关要求，按照既要满足目前使用要求，又适应远期发展的需要。弱电机房在环境装修质量、供电电网的稳定、空气的洁净度、环境的温湿度、噪音的控制、防静电防雷击上都能达到如下指标，既为该项目信息化设备提供一个良好的、稳定的、高效的、管理方便的集中设备运行区域，也是信息化建设成果对外的一个形象窗口。

机房装饰工程是一项系统工程，是现代科学技术和装饰艺术的综合体现。不仅要满足工作人员的人体工学效果，更重要的是为机房设备提供一个良好的运行环境。随着现代科技的发展，室内环境的设计已经不满足传统的简单、生硬的设计，现代空间设计不仅在视觉上加以延伸，而且根据弱电工程独有的工作性质及特点，除注重环境装饰外，更注重于内部全系统的建设。以技术数据为依据建造一个符合特定环境的空间，突出空间的舒适、相对独立，并体现了现代科技的巨大发展和装饰文化的精神内涵。

对于机房来说，电力保障是基础设施建设中的重中之重，数据中心机房具有设备密集、耗电量极大、发热量大、可靠性要求极高、安全性要求极高等特点，机房一旦运转起来，就不能有哪怕是 0.1 秒钟的停电时间，并且要求具有极高品质的电源质量，因此机房的建设必须要建立一个可靠性强的供配电系统，在这个系统中不仅要解决大量机柜以及计算机设备的用电问题，还要解决保障计算机设备正常运行的其它附属设备的供配电问题。如：恒温恒湿专用空调，照明系统用电，安全消防系统用电等，以保证数据中心能够安全稳定地运行。

云服务和服务器需求

政务云服务器资源细项

此类应用为园区公共性平台，均依托省大数据局政务云资源。所需政务云资

源需满足等保三级安全测评要求及三级密码测评要求。

一、园区公共服务平台

序号	系统	服务器类型	虚拟机	虚拟机 CPU		虚拟机内存		虚拟硬盘	
			数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
1	园区统一门户	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	2	4	8	16	300	600
		数据库服务器	2	4	8	16	32	500	1000
2	智慧园区服务系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	2	4	8	16	300	600
		数据库服务器	2	4	8	16	32	500	1000
3	访客管理系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	2	4	8	16	300	600
		数据库服务器	2	4	8	16	32	500	1000
小计			**18**		**48**		**192**		**6600**

二、园区运营管理平台

序号	系统	服务器类型	虚拟机	虚拟机 CPU		虚拟机内存		虚拟硬盘	
			数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
1	园区智慧党建	Web 服务器	2	2	4	8	16	150	300
		应用服务	2	2	4	8	16	150	300

	系统	器							
		数据库服务器	2	4	8	16	32	300	600
2	园区决策分析系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
3	安全生产管理系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
小计			**26**		**216**		**288**		**9600**

综上统计，本期项目政务云建设需求为 44 台虚拟机、264vCPU、480GB 内存、16200GB 存储资源、备份存储需求 27994GB（按存储年增长率 20%，三年增长量）。

国产化本地云一区服务器资源细项

此类应用为满足监管要求以及企业商业机密，部署在海口综保区机房，与海关机房形成信息化闭环。

一、展销综合服务平台

系统	服务器类型	虚拟机	虚拟机 CPU		虚拟机内存		虚拟硬盘	
		数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
云展综合服务系统	应用服务器	3	8	24	16	48	500	1500
	Web 服务器	1	4	4	8	8	500	500
	数据库服务器	1	8	8	16	16	1000	1000
宝玉石交易系统	应用服务器	3	8	24	16	48	500	1500
	Web 服务器	1	4	4	8	8	500	500
	数据库服务器	1	8	8	16	16	1000	1000
资源云交易系统	应用服务器	3	8	24	16	48	500	1500
	Web 服务器	1	4	4	8	8	500	500
	数据库服务器	1	8	8	16	16	1000	1000
小计：		**15**		**108**		**216**		**9000**

二、、作业综合服务平台

系统	服务器类型	虚拟机	虚拟机 CPU		虚拟机内存		虚拟硬盘	
		数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
一体化ERP云服务系统	应用服务器	2	8	16	16	32	500	1000
	Web服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
智慧	应用服务器	2	8	16	16	32	500	1000

云仓服务系统	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
物流运输管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
供应链金融服务系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
溯源采集管理系统	应用服务器	1	8	8	16	32	500	500
	Web 服务器	1	8	8	16	32	500	500
	数据库服务器	1	8	8	16	16	500	500
融资租赁管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
跨境电商	应用服务器	2	8	16	16	32	500	1000

新零售管理系统	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
免税交通工具管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
冷链协同管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
源数据库集群	服务器	2	8	8	16	16	500	500
存储/备份服务器	服务器	1	8	8	16	16	500	500
文件服务器	服务器	1	8	8	16	16	500	500
小计		47		368		768		23000

三、辅助监管业务服务平台

系统	服务器	虚拟机	虚拟机 CPU	虚拟机内存	虚拟硬盘

	类型	数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
智能监管场站系统	应用服务器	1	8	8	16	16	300	300
	传输服务器	1	8	8	16	16	300	300
保税业务辅助管理系统	应用服务器	8	8	64	16	128	300	2400
	传输服务器	4	8	32	16	64	300	1200
多式联运服务系统	应用服务器	4	8	32	16	64	300	1200
	传输服务器	2	8	16	16	32	300	600
跨境电商服务系统	应用服务器	2	8	16	16	32	500	1000
	传输服务器	2	8	16	16	32	500	1000
	接口服务器	2	8	16	16	32	300	600
应用支撑	应用服务器	2	8	16	16	32	300	600
	传输服务器	2	8	16	16	32	500	1000
小计		**30**		**240**		**480**		**10200**

四、园区应用数据库集群

系统	服务器类型	虚拟机	虚拟机	内存	存储磁盘

		数量	CPU	小计	内存(GB)	小计	容量(GB)	小计
园区数据库集群	数据库集群服务器	1	4	4	128	128	10000	10000
	数据库集群服务器	1	4	4	128	128		
海关数据库集群	数据库集群服务器	1	4	4	128	128	10000	10000
	数据库集群服务器	1	4	4	128	128		
小计：		**4**		**16**		**512**		**20000**

五、对外接入网数据交换集群

系统	**服务器类型**	**虚拟机**	**虚拟机**		**内存**		**磁盘**	
		数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
数据交换系统	数据交换服务器	1	32	32	128	128	500	500
	数据交换服务器	1	32	32	128	128	500	500
	集群域控	1	32	32	128	128	500	500
	集群控制台	1	32	32	128	128	500	500
小计		**4**		**128**		**512**		**2000**

六、园区智慧管理平台

需求	**场景**	**数量**	**部署方式**	**规格**
园区安防体系平台	应用服务器	1	VM	CPU：>=16 核，内存：>=64GB，硬盘：>=500GB
	Web 服务器	1	VM	CPU：>=16 核，内存：>=64GB，硬盘：>=500GB

	数据库服务器	1	VM	CPU：>=16 核，内存：>=64GB，硬盘：>=500GB

综上本地云服务器所需资源汇总如下表：

系统分类	应用场景	VPU	内存（G）	存储（T）
国产化本地云一区	展销综合服务平台	108	216	9
	作业综合服务平台	368	768	23
	辅助监管业务服务平台	240	480	10.2
	园区应用数据库集群	16	512	20
	对外接入网数据交换集群	128	512	2
	园区智慧管理平台	48	192	1.5
合计		908	2680	65.7

国产化本地云二区服务器资源细项

为满足智慧园区集成平台、智慧园区数据平台、媒体转码组件、地理信息数字系统、运营指挥可视化平台、物联网平台等工具软件部署，支撑智慧园区指挥管理平台和可视化应用的数据汇集、呈现、管理，根据各模块所需资源进行此部分服务器资源评估。本次项目中的国产化服务器资源需求如下：

系统分类	应用场景	VPU	内存（G）	存储（T）
国产化本地云二区	园区集成平台	120	544	13.5
	物联网平台	16	128	3
	园区数据平台	152	640	12.5
	GIS 平台	16	64	2.5
	可视化平台	96	192	2

	视频转码	24	96	1
合计 2		**424**	**1664**	**34.5**

存储备份需求

充分考虑海口综保区现有业务和未来 5 年内业务发展的整体规划。现有信息化系统和将来上线的新信息化系统，以及来自海关的数据都将参与数据分析与计算，而各业务系统中大概有 40%的数据需要参与数据分析与计算，具体数据量测算（取系统中主要数据表进行测算），数据主要分为静态数据（基础数据库）与动态数据（业务库数据、主题库数据、交换与共享库）。按照静态数据永久保存，业务数据在线保存 5 年，视频数据保存 2 个月进行数据量估算。基础数据、业务数据、主题数据、交换数据的数据量分别为 352.77、1746.34、2134.4 和 64.47 GB，共计约 4.2TB；考虑到数据空间及日志空间、临时表空间的占用，以及空间预留，通常取数据量的 3 倍，即所需数据存储空间为 4.2TB×3=12.6TB，按照每年 30%的增长量，三年备份服务所需云端备份资源量为向上取整【12.6TB*1.3^3】=30TB。

初步的数据量估算如下表。

序号	数据类型	分析存储量	设计存储量
1	基础数据	352.77GB	1,058.31GB
2	业务数据	1746.34GB	5,239.02GB
3	主题数据	2134.4GB	6,403.20GB
4	交换数据	64.47GB	193.41GB
5	视频数据	166.3TB	200TB
合计			212TB

根据对园区云上业务存储备份需求统计分析，项目将租赁三年 30TB 公有云

备份服务对基础数据、业务数据、主题数据、交换数据进行云端备份。

针对本地云关键应用系统的容灾，考虑采用租赁公有云实现应用级容灾服务。通过对本地云承载业务系统的分析，大部分虚拟机采用的规格为：8 核 CPU、16G 内存、500G 数据盘，因此在公有云上租赁 5 台同等规格的备用虚拟机用于对关键应用的容灾热备服务；本地云与公有云容灾服务之间采用 CDP 持续数据保护的方式进行数据复制，考虑到 CDP 技术复制过程中存在全量镜像数据、CDP 连续复制每日增量数据、容灾恢复预留空间要求，灾备云 CDP 复制所需存储资源为 5 台虚拟机数据盘规格的 3 倍，即容灾 CDP 所需存储资源=0.5TB*5*3=7.5TB。

其他基础硬件设备需求

本项目规划的智慧园区各平台或系统需要大量的计算和存储资源，一部分使用电子政务云的资源，另外有相当一部分不适宜使用电子政务云的资源，尤其是本项目中规划的园区智慧安防等系统或平台，一方面数据量巨大（视频图像数据），另一方面需要本地高强度计算（图像识别与分析等），因此需要在园区建设数据中心用于存储海量的视频图像数据以及园区各基础设施上采集到的数据，需要建立本地的计算能力对这些数据进行分析。

系统及工具软件需求

本项目中规划的平台和系统将统一地采用基于 J2EE 技术体系，同时应尽可能地按照国产化的要求进行建设，因此存在对操作系统、数据库系统、中间件、以及其他工具软件等使用国产软件的需求。

操作系统需求

根据平台应用与网络安全要求，规划采用开源操作系统与商用操作系统两种。

表 4- 1 操作系统

序号	类别	单位	数量	参考品牌
1	操作系统	套	1	开源/国产，Linux 系列；参考品牌：CentOS/中标麒麟 Linux
2	操作系统	套	6	Windows 2012。

				与海关对接的前置系统，按照海关要求部署。

数据库需求

根据平台应用要求，规划采用关系型数据库、内存数据库以及 NOsql 数据库。

表 4- 2 数据库

序号	类别	单位	数量	参考品牌
1	关系型数据库	套	1	开源/国产，参考品牌：MySQL/达梦
2	其他数据库	套	1	开源/国产，参考品牌：MangoDB 等

中间件需求

根据平台应用需求，规划中间件分别有商用与开源两种。具有可伸缩性、集群可用性、web 服务、事务支持、消息支持、安全性。

表 4- 3 中间件

序号	类别	单位	数量	参考品牌
1	中间件	套	1	开源/国产，参考品牌：Tomcat/东方通
2	数据交换系统	套	1	采购商业数据交换系统，并在此基础上进行二次开发。

网络建设和部署需求

一、园区局域网建设需求

海口综合保税区目前覆盖三个园区，分别是海口园区、老城园区、空港园区，未来还将新增海口客运港园区。

目前海口园区和老城园区现有网络已经使用十年以上，存在设备老化、容量不足、网络拓扑不合理等问题，因此亟待升级改造；与此同时，空港园区也必须纳入到整个海口综保区统一的网络规划、设计中。因此，需要针对现有的三个园区以及未来新增园区的角度，对海口综保区的园区局域网络进行重新规划和设计，搭建覆盖海口园区、老城园区、空港园区三个园区的局域网络，同时考虑为新增

的海口客运港园区进行设计预留。

二、园区海关专网建设需求

由于综保区属于特殊监管区域，因此在园区内需要设计为海关监管作业的封闭区域，例如卡口区域、检验检疫区域、查扣库区域等等，在这些区域应建立海关专网接入，便于部署海关监管信息系统、视频监控系统等供海关监管机构工作人员使用。因此，在目前海口综合保税区目前覆盖的三个园区以及未来新增园区均有该项建设需求。

三、园区物联网建设需求

以智慧园区为本项目的建设目标，园区物联网的建设需求成为必然。园区物联网络的建设包括有线、5G、WIFI、NFC 等多种接入方式，以适应不同的智能终端设备的入网要求。园区物联网用于连接园区安防、消防、照明、能效等各类终端设备。

四、园区 5G 专网建设需求

5G 专网主要是用于连接那些必须以 5G 通信方式接入园区信息系统平台的设备，特别是在一些不便于采用有线方式接入的场所，一方面可以节约初期布线的成本，另一方面也可以减少设备运维的成本。

五、园区国际互联网数据专用通道建设需求

由于园区的核心业务是国际贸易，因此入住园区的企业中有大量的企业需要与国外的客户或供应商、国外企业总部进行线上的业务往来，通过园区国际互联网数据专用通道进行线上的业务往来将极大地提高这些企业的运营效率。

性能和其他需求

本项目涉及到园区运行管理、针对园区企业的业务服务以及针对海关监管的要求，因此对平台或系统的提出了较高的性能、稳定性和可靠性要求。

机房和网络

本地机房的建设以及相关的设施例如网络接入、电力接入等应采用双路冗余设计，本地机房建设 UPS 后备电源系统，机房内服务器、存储、网络等的设计应采用双路冗余设计，Web 服务器、应用服务器、数据库等应采用双机热备架构，保证平台或系统 7×24 小时不间断服务。

硬件平台建成后将采用虚拟化部署，需要满足平台基础设施的规模随业务量的增加而快速增加的能力。

应用软件系统

系统架构需具备高度可移植性，保证与硬件平台的无关性，以及与系统软件平台的低耦合，在设计上必须具有适应业务变化的能力。

一、展销综合服务类应用软件系统

最大并发人数：2000 人；

响应时间：秒级响应；

服务时间：7×24 小时不间断服务；

普通应用查询：平均 3 秒，最长 5 秒；

单个事务速度：400 毫秒内；

统计分析类查询：平均 5 秒，最长 10 秒；

系统备份在 30 分钟内完成。

二、作业类和监管服务类应用软件系统

最大并发人数：200 人；

响应时间：秒级响应；

服务时间：7×24 小时不间断服务；

普通应用查询：平均 3 秒，最长 5 秒；

单个事务速度：400 毫秒内；

统计分析类查询：平均 5 秒，最长 10 秒；

系统备份在 30 分钟内完成。

三、园区管理类应用软件系统

最大并发人数：50 人；

响应时间：秒级响应；

服务时间：7×24 小时不间断服务；

普通应用查询：平均 3 秒，最长 5 秒；

单个事务速度：400 毫秒内；

统计分析类查询：平均 5 秒，最长 10 秒；

系统备份在 30 分钟内完成。

网络安全建设需求分析

网络安全基础设施建设需求

合法合规性建设需求

近年来网络与信息技术高速发展，移动互联网、云计算、大数据、区块链、人工智能、工业互联网、物联网、智能制造、智慧园区等新兴基础设施和应用不断出现，网上购物、无卡支付、自动驾驶、共享经济在网络与信息技术的发展驱动之下成为现实并快速普及，人们在享受着网络与信息技术所创造新经济奇迹的同时已经悄然进入了万物互联的 IoT 时代。

国家网络安全主管部门陆续印发文件，对信息安全体系建设指导和推进形成了很好的指导作用，特别是对于基础安全防护系统建设提供重要参考和规划设计方向。部分政策文件摘要如下：

一、《国家信息化领导小组关于安全保障工作的意见》从国家战略高度提出了加强我国信息网络安全的方针；明确加强网络安全保障工作的主要原则是“立足国情，以我为主，坚持管理与技术并重；正确处理安全与发展的关系，以安全保发展，在发展中求安全；统筹规划，突出重点，强化基础性工作；明确国家、企业、个人的责任和义务，充分发挥各方面的积极性，共同构筑国家网络安全保障体系”；确定加强网络安全保障工作的总体要求是“坚持积极防御、综合防范方针，全面提高网络安全防御能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全”；明确提出“要重视网络安全风险评估工作，对网络与信息系统安全的潜在威胁、薄弱环节、防护措施等进行分析评估，综合考虑网络与信息系统的重要性、涉秘程度和面临的网络安全风险等因素，进行相应等级的安全建设和管理”。

二、《网络安全等级保护工作的实施意见》、《网络安全等级保护管理办法》等多个文件完善了我国信息系统等级保护的政策体系，相关文件中明确阐述了网络安全等级保护建设的重要意义。

三、《关于开展全国重要信息系统安全等级保护定级工作的通知》明确了定级范围，其中明确规定“铁路、银行、海关、税务、民航、电力、证券、保险、外交、科技、发展改革、国防科技、公安、人事劳动和社会保障、财政、审计、商务、水利、国土资源、能源、交通、文化、教育、统计、工商行政管理、邮政

等行业、部门的生产、调度、管理、办公等重要信息系统。市（地）级以上党政机关的重要网站和办公信息系统”必须进行等级保护。

四、《国务院关于大力推进信息化发展和切实保障网络安全的若干意见》中对信息化安全给出了以下意见：

强调了确保重要信息系统和基础信息网络安全的重要性。要求对涉及国计民生的重要信息系统和基础信息网络，要同步规划、同步建设、同步运行安全防护设施，强化技术防范，严格安全管理，切实提高防攻击、防篡改、防病毒、防瘫痪、防窃密能力。加强互联网网站、地址、域名和接入服务单位的管理，完善信息共享机制，规范互联网服务市场秩序。强调了加强政府和涉密信息系统安全管理的必要性。

五、《中华人民共和国网络安全法》更是通过立法的方式对建设、运营网络或者通过网络提供服务的单位建立和维护网络安全提出了明确的要求：

应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

六、《中华人民共和国数据安全法》在“数据安全制度”明确提出了：

第二十一条　国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

七、GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》中针对共性安全保护需求提出安全通用要求，针对云计算、移动互联、物联网、工业控制和大数据等新技术、新应用领域的个性安全保护需求提出安全扩展要求，形成新的网络安全等级保护基本要求标准。

《中华人民共和国网络安全法》以及《网络安全等级保护基本要求》（等保2.0）都明确要求加强关键信息基础设施等级保护安全防护能力建设，落实国家

网络与信息安全信息通报工作规范和信息化考核要求。新的网络安全形势和信息化考核要求推网络安全建设提出了新的建设需求。

一是继续深入贯彻落实《网络安全法》和等保 2.0 条例的相关要求，强化安全制度体系的建设，确保网络安全各项工作的部署和落实，强化组织领导，把网络安全工作做细、做实；

二是强化网络安全顶层设计，提高网络安全战略能力，这是一个基础工作，也是一项长期工作。持续优化和改进网络安全管理机制，加大信息安全投入，推动信息安全人才队伍建设，都是提升网络安全管理水平的必要措施；

三是定期开展信息安全监督检查，推动全行业的信息安全风险评估，逐步形成常态化的安全检查和评估机制；

四是推进网络安全综合防御技术体系建设，全面梳理现有的安全防御技术，重点关注互联网接入区域的防御，建立严密的外网安全防护系统，提升网络安全威胁的检测、分析和预警能力，将安全威胁拒之门外。

安全管理和防控仍是一项艰巨但重要的工作，需要不断改进和提升，可谓任重而道远。

等级保护建设需求

架构设计以等级保护“一个中心、三重防护”为核心指导思想，构建集防护、检测、响应、恢复于一体的全面的安全保障体系。以全面贯彻落实等级保护制度为核心，打造科学实用的信息安全防护能力、安全风险监测能力、应急响应能力和灾难恢复能力，从安全技术、安全管理、安全运维三个维度构建安全防护体系，切实保障信息安全总体防护水平。

安全管理体系：为保障信息安全而采取的一系列管理措施的总和，内容主要包括建立健全信息安全组织体系和信息安全策略体系。

安全技术体系：为保障信息安全而采取的一系列技术措施的总和，内容主要包括安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全物理环境等。

安全运维体系：为保障管理措施和技术措施有效实现信息安全而采取的一系列活动的总和，内容主要包括安全加固、渗透测试、应急演练及应急响应、安全管理制度编制及完善等内容

安全通信网络

数据中心安全首先应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。应利用访问控制、入侵检测等技术手段对不同区域之间的互相访问进行控制和流量检测。

进行远程业务数据通讯时，必须确保数据的秘密性和完整性，防止数据在传输通讯过程中被窃听和篡改，在没有采取其他可靠的数据传输加密机制的情况下，可采用在 IP 或传输层建立虚拟专用网的机制来实现对重要应用数据的远程传输加密保护。

安全区域边界

本项目网络系统以澄迈园区为中心，辐射海口园区和空港园区，海口园区和空港园区通过租用运营商专线连接至澄迈园区。同时需要通过专线连接至海口市电子政务外网、海口市电子政务外网互联网区和海关专网网络；边界安全防护设施具体包括：

在安全域边界均需要采用安全网关设备进行隔离和访问控制，严格控制外部网络对业务系统信息资源的访问，确保虚拟化数据中心和信息系统自身的安全。

需要在安全域出口分别部署多功能的安全网关设备，集成网络入侵防御功能、病毒检测功能、恶意代码检测功能等，对进出网络及访问重要业务系统的数据流进行黑客攻击、蠕虫、木马、病毒等非法流量的检测和拦截，并提供日志审计和报警机制，确保通信网络和业务系统不会因为外界攻击而无法正常工作。

通过对内部网络流量进行抓包分析，捕获高危攻击行为，实现安全风险预警。在检测过程中会分离流量中的各种协议的文件，对文件进行检测。发现文件中的恶意代码，并及时进行预警。

在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

电子政务外网区和海关专网边界部署网闸系统进行隔离，确保数据交换安全。

在安全域边界均需要采用防火墙进行隔离和访问控制，严格控制外部网络对业务系统信息资源的访问，确保虚拟化数据中心和信息系统自身的安全。

需要在安全域出口分别部署多功能的安全网关设备，集成网络入侵防御功能、病毒检测功能、恶意代码检测功能等，对进出网络及访问重要业务系统的数据流

进行黑客攻击、蠕虫、木马、病毒等非法流量的检测和拦截，并提供日志审计和报警机制，确保通信网络和业务系统不会因为外界攻击而无法正常工作。

通过对内部网络流量进行抓包分析，捕获高危攻击行为，实现安全风险预警。在检测过程中会分离流量中的各种协议的文件，对文件进行检测。发现文件中的恶意代码，并及时进行预警。

在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

安全计算环境

重要业务系统需要建设数据库审计能力，实现对数据库访问的详细记录、监测访问行为的合规性，针对违规操作、异常访问等及时发出告警，将安全风险控制在最小的范围之内。

需要对云平台中的云主机实施主机安全管理，加强对网络接入、访问情况进行统一授权和管理，更加有效地防范各类违规、泄密事件的发生，提高网络的整体维护效率和管理力度。

安全管理中心

信息要素多种多样，除了资产的基本信息之外，还包括各资产和应用的弱点漏洞、来自系统外部的攻击威胁、内外交互的流量数据、设备运行的日志告警、云端和本地积累的威胁情报等异构数据。以上各种信息要素数据来源多样，数据结构各不相同，传统的安全检测与防护设备各自为战互不协同，在产生更多安全要素数据的同时，并不能对这些数据进行有效的集中化管理。

因此需要建立安全数据中心，全面收集信息系统内部和外部的安全要素，实现对安全要素的体系化、集中化管理。通过建立体系化的管理方式，方便运维人员对安全要素集中管理，提升企业的网络安全自主可控能力。

通过建立安全数据中心，可以统一管理安全要素、集中监控安全风险、及时处置安全威胁、提升安管协作效率。

集中监控。需采集流量、日志等多源异构数据，统一管理安全要素，覆盖云、数据、应用、网络、边界和终端等 6 大维度，集中监控全网安全风险。

威胁发现。需融合海量异构安全数据和全流量，对安全事件进行智能分析，

发现高级潜伏威胁，实现精准告警。

智能研判。需对网络访问关系进行可视化呈现，能够重点标注高风险资产，并对资产进行风险评分；需对攻击流向、攻击趋势、攻击链阶段等进行分析，帮助用户快速研判安全事件，

响应处置。实现自动化安全处置联动，发生安全事件时自动化下发安全策略，快速阻断威胁，完成安全运营闭环。

安管协作。发生安全威胁后，可生成工单，指派威胁处置人员，通过工单流转，快速形成处置闭环。

云安全防护体系建设需求

本项目除了政务云上的两个业务系统除外，其余的业务系统均部署于本地数据中心云平台中，而不法分子会通过对云平台的网络、主机、应用和数据层面进行攻击，对云上的业务系统的安全造成威胁。因此，本地数据中心云平台上的业务系统有等保二级安全能力的建设需求，以满足国家对于合规性的要求。

攻击预警平台建设需求

APT 攻击特点

1） 近年来国内的诸多单位遭受到的高级威胁 APT 攻击越来越多，通过传统的安全工具不能很好的发现此类攻击，导致无法从源头上得到处理；

2） 高级威胁 APT 攻击具备了国家和组织的背景，导致攻击手段复杂，更加难以被发现，隐藏的更深，潜伏的时间更长，网络窃密和网络破坏程度持续加剧；

3） APT 攻击，采用的攻击手法和技术都是未知漏洞（Oday）、未知恶意代码等未知行为，在这种情况下，依靠已知特征、已知行为模式进行检测的 IDS、IPS 在无法预知攻击特征、攻击行为模式的情况下，理论上就已无法检测 APT 攻击；

攻击预警平台

APT 攻击通常都会在内网的各个角落留下蛛丝马迹，真相往往隐藏在网络的流量中。传统的安全事件分析思路是遍历各个安全设备的告警日志，尝试找出其中的关联关系。但依靠这种分析方式，传统安全设备通常都无法对 APT 攻击的各个阶段进行有效的检测，也就无法产生相应的告警，安全人员花费大量精力进

行告警日志分析往往都是徒劳无功。如果采用全流量采集的思路，一方面是存储不方便，每天产生的全流量数据会占用过多的存储空间，组织通常没有足够的资源来支撑长时间的存储；另一方面是全流量数据包含了结构化数据、非结构化数据，涵盖了视频、图片、文本等等多种格式，无法直接进行格式化检索，安全人员也就无法从海量的数据中找到有价值的信息。所以我们可知通过传统的安全手段无法有效的查出 APT 的攻击行为，需要借助更加专业的安全设备才能捕抓到 APT 攻击，攻击预警平台就是针对此种场景研发出来的安全工具。

安全态势感知能力建设需求

1） 安全要素集中管控需求

IT 系统的信息要素多种多样，除了资产地基本信息之外，还包括各资产和应用的弱点漏洞、来自系统外部的攻击威胁、内外交互的流量数据、设备运行的日志告警、云端和本地积累的威胁情报等异构数据。以上各种信息要素数据来源多样，数据结构各不相同，传统的安全检测与防护设备各自为战互不协同，在产生更多安全要素数据的同时，并不能对这些数据进行有效的集中化管理。

因此需要建立安全数据中心，全面收集信息系统内部和外部的安全要素，实现对安全要素的体系化、集中化管理。通过建立体系化的管理方式，方便运维人员对安全要素集中管理，提升企业的网络安全自主可控能力。

2）安全威胁检测与分析需求

现有的安全设备如 IDS 和 WAF 等，可以基于内置的静态规则分析发现简单的安全入侵与非法访问，但仍然存在其局限性。近年来不断增长的账户安全和数据安全问题，让静态分散的安全检测和防护手段越来越 显示其局限性。一方面基于不同设备静态规则的事中检测，针对同一安全事件会触发大量的重复告警。另一方面，缺乏对多个设备的告警日志进行实时关联分析，难以发现 APT 攻击等高级威胁行为，无法实现基于时间轴进行清晰的事后溯源分析。

针对安全事件的事中检测，一方面需要全面收集现有的安全检测设备产生的告警，剔除误报提高告警准确率；另一方面需要关联不同来源的安全告警并进行建模分析，发现潜藏的高级持续性威胁。

针对安全事件的事后溯源分析，需要梳理内外资产的互访关系，并按照攻击链阶段推导整个事件的发展过程，分析历史数据达到逆向溯源的目的。

3）安全事件处置响应需求

安全事件爆发之后，有多方面原因导致事件的处置响应滞后。一是海量的告警将安全运维人员淹没，难以将有效告警迅速识别出来；二是识别出有效告警之后，需要手动操作去对应的安全防护设备上下发策略；三是缺乏有效的安全事件突发预案管理，导致在面对突然发生的事件告警时应对失措。如果不能在安全事件被发现的第一时间进行妥善处置，势必会对企业的信息资产造成更大范围的破坏。

事件处置响应滞后的主要原因，是安全检测系统发现安全事件生成告警之后，需要人工识别有效告警并在对应的安全防护设备下发策略，实现安全事件的处置。告警筛选和手动策略下发的时间肯定落后于安全事件发生的时间，无法实现真正及时的闭环联动。

4）安全态势监测需求

网络安全威胁态势复杂多样，因此需从多维度多视角对安全态势进行分析监测并可视化呈现，才能在总览全局态势的同时，以业务系统-安全域-资产的视角逐级放大，保证全面多方位的展示安全态势。安全态势呈现应包括但不限于以下几个维度。

数据流向视角：不同的安全事件数据流向各不相同，网络攻击事件的方向是外对内，勒索病毒回连或者受控挖矿的方向是内对外，木马蠕虫的扩散是系统内的横向蔓延，因此根据不同的数据流方向需要都分别独立的可视化呈现界面。

业务系统视角：针对易受攻击的重点业务系统，例如对外部直接提供访问的web 系统等，需要将其单独呈现作为重点关注对象，监测其数据流量趋势，当有恶意攻击之类的安全事件发生时第一时间发现，应当具有独立的可视化监测页面。

信息资产视角：资产是安全攻击作用的对象，安全运维人员通过观察资产安全态势可以直观地知晓哪些资产上面告警较多，哪些资产日志数据异常，事件处置更具针对性。

事件溯源视角：安全事件发生后从海量的告警日志中人工梳理溯源工作量巨大，应提供直观的安全事件溯源可视化页面，基于事件发生的时序，从攻击者、被攻击资产、资产横向互访关系的角度进行溯源呈现。

物联网安全建设需求

本项目涉及的物联网终端种类繁多，如智慧路灯、人脸识别门禁、高清摄像机、物联网网关等，设备采用 WIFI、4G/5G、NB-IoT 等传输协议入网，设备数量多，分布广，同时支撑的上层智慧应用系统多样。

物联网是指以视频监控为代表的一系列安全终端设备所组成的网络，视频专网是实现园区安全和稳定的重要基础，是“智慧园区”的重要载体，它不仅可以满足治安管理、园区管理、交通管理、应急指挥等需求，在预防、发现、控制、打击违法犯罪，提供破案线索，固定违法犯罪证据等方面也发挥人防、物防所不可替代的作用。

物联网设备的特征主要有以下几点：

特点 1-资产数量特别多：一般都是数十万的量级—管理难度大，各级区域数量都非常多—投入规模大；

特点 2-网络边界不清晰：都是由中心统一接入—难以权限控制，各区域没有明确隔离—无法逻辑隔离；

特点 3-网络关系复杂：设备类别、型号多—统一管控难，网络协议类型特有—检测审计难；

特点 4-终端极易遭受攻击：终端分布分散—攻击面广，内部易被控制—敌我难辨；

因此新的物联网设备的覆盖引入了新的安全隐患，现有的措施无法保障，主要的隐患有前端风险、边界风险、以及管控中心风险组成：

1）前端风险

频监控前端设备含有大量的数据信息，其中包括治安监控的视频图像数据、卡口/电警的过车图片数据等信息，同时设备的弱口令、不安全的配置、不完善的补丁策略、未关闭的端口等都可能导致未授权的用户接入，以及物理上的违法私接、非法仿冒行为都会造成视频专网敏感图像、视频数据泄露。

2）网络攻击入侵风险

由于物联网终端的计算资源有限，当终端遭遇一些资源消耗型攻击行为时，例如 DDoS 攻击行为，会直接让终端中断服务甚至死机。网络入侵行为会直接应用终端及所支撑平台应用的稳定性与连续性。

3）网络链路数据劫获风险

物联网终端接入的方式多样，有有线，也有无线，如果传输过程没有足够的安全防护，在网络传输链路上的数据流量就存在被劫获、监听的风险，甚至可以篡改其传输的数据。

密码应用建设需求

《中华人民共和国密码法》中强化了密码应用要求，突出密码应用监管，重点面向关键信息基础设施和网络安全等级保护第三级以上系统，落实密码应用安全性评估和国家安全审查制度。

《信息安全技术网络安全等级保护基本要求》2.0 版本的新标准中强调了密码技术对物理环境安全、网络和通信安全、设备和计算安全、应用数据安全、密钥管理等方面的重要应用性。并规定第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。

根据《关于进一步明确省政务信息化项目建设密码应用有关要求的通知》琼国密局字[2021]2 号要求：《海南省信息化项目建议书网络安全部分编制规范(试行)》《海南省信息化项目可行性研究报告网络安全部分编制规范(试行)》《海南省信息化项目初步设计网络安全部分编制规范(试行)》《海南省购买信息化服务方案网络安全部分编制规范(试行)》中涉及密码应用的编制要求可由密码应用方案统一替代。

因此本项目“密码应用建设方案”单独进行编制，详见《海口综合保税区智慧园区建设项目密码应用方案》。

网络安全等保/密评/分保工作需求

安全等级保护定级

定级情况说明

根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019)、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）和《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）等标准，本项目安全包括业务信息安全和系统服务安全，与之相关的受到破坏所侵害的客体和对客体的侵害程度可能不同，因此，本项目定级也应由业务信息安全和系统服

务安全两方面确定。从业务信息安全角度反映的信息安全保护等级称业务信息安全保护等级。从系统服务安全角度反映的信息系统安全保护等级称系统服务安全保护等级。

业务信息安全保护等级的确定

本项目其业务信息安全受到破坏时，所侵害的客体属于社会秩序、公共利益。

本项目业务信息安全受到破坏时，其侵害程度为一般损害。

根据或者业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据业务信息安全保护等级矩阵表，即可得到或者业务信息安全保护等级为第二级。

表 4- 1 业务信息安全保护等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

系统服务安全保护等级的确定

业务信息安全保护等级确定

海口市综合保税区智慧园区应用包含：园区公共服务平台、园区运营管理平台、展销综合服务平台、作业综合服务平台、辅助监管业务服务平台和应用支撑平台。

园区公共服务平台：

对公民、法人和其他组织的合法权益的侵害程度属于特别严重损害，对社会秩序、公共利益的侵害程度属于严重损害，对国家安全一般损害。

园区运营管理平台：

对公民、法人和其他组织的合法权益的侵害程度属于严重损害，对社会秩序、公共利益的侵害程度属于严重损害。

展销综合服务平台：

对公民、法人和其他组织的合法权益的侵害程度属于严重损害，对社会秩序、公共利益的侵害程度属于一般损害。

作业综合服务平台：

对公民、法人和其他组织的合法权益的侵害程度属于严重损害，对社会秩序、公共利益的侵害程度属于一般损害。

辅助监管业务服务平台：

对公民、法人和其他组织的合法权益的侵害程度属于严重损害，对社会秩序、公共利益的侵害程度属于一般损害。

应用支撑平台：

对公民、法人和其他组织的合法权益的侵害程度属于严重损害，对社会秩序、公共利益的侵害程度属于一般损害。

业务信息安全保护等级矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

安全保护等级的确定

本项目的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。所以，最终确定本项目安全保护等级为第二级。

按照以上定级指南要求，结合本项目情况，特列出项目中需定级系统清单。

表 4- 3 定级系统清单

序号	名 称	部署位置	等保级别	备注
1	园区公共服务平台	政务云	三级	互联网区域
2	园区运营管理平台	政务	三级	电子政务

		云		外网区
3	展销综合服务平台	本地云	二级	
4	作业综合服务平台	本地云	二级	
5	辅助监管业务服务平台	本地云	二级	
6	应用支撑平台	本地云	二级	

等保测评需求

本项目依据《中华人民共和国网络安全法》，国家实行网络安全等级保护制度。网络运营者按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。网络安全等级保护工作包括信息系统定级、备案、建设整改、等级测评、监督检查五个阶段。

本项目相关信息系统将按系统级别对应的等保基本要求开展等级测评。测评的内容包括但不限于以下内容：

安全技术测评：包括安全物理环境、安全通信边界、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；

安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

网络安全服务需求

本项目旨在落实《中华人民共和国网络安全法》和国家网络安全等级保护制度，做好单位网络安全保障工作，提升信息系统安全防护水平，避免发生重大网络安全事故。根据当前网络安全工作存在的差距和不足，通过采购网络安全服务

的形式，为信息系统网络安全保障工作提供可靠保障。

本次网络安全服务，主要是针对园区公共服务平台、园区运营管理平台、展销综合服务系统、作业综合服务平台、辅助监管业务服务平台、应用支撑平台6个应用系统平台，在其开发阶段及正式上线发布前，为避免带“病”上线情况，需开展相应的安全服务评估及加固工作，具体服务需求如下：

编号	系统名称	安全服务内容
1	园区公共服务平台	安全代码审计服务 入网安全评估服务 渗透测试服务 计算环境安全加固服务
2	园区运营管理平台	
3	展销综合服务平台	
4	作业综合服务平台	
5	辅助监管业务服务平台	
6	应用支撑平台	

网络安全运营需求

依据《中华人民共和国网络安全法》、国家网络安全等级保护制度、贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见、以及相关法律法规、政策、行业标准。夯实项目网络安全底座，筑牢网络安全防线，通过运营服务团队、标准化运营流程及配套的运营支撑平台来构建网络安全运营中心，持续优化和输出安全能力，最大程度杜绝发生安全事件，保证网络和业务的稳定、可续化运行。

按照本项目信息系统安全保护最高级别拟定的网络安全三级等保级别，结合当前网络安全建设现状与不足，从建设网络安全运营中心的角度分析需求如下：

1）网络安全运营团队建设需求

安全运营网络安全的本质是人与人的对抗。对于安全运营中心来说，专业安全人员在安全运营体系中占据核心地位，合理地配置专业人员能够保证策略可有效执行、安全运营管理平台可有效使用、产品可合理管理、流程可正常运转。

2）运营组织构架需求

海口市综合保税区网络安全信息化和网络安全领导小组为决策层，中心管理团队、安全专家、项目经理为管理层，各单位安全运营支撑团队下分风险评估组、

威胁监测组、应急处置组、安全合规组、安全情报组、安全建设组等负责安全运营工作的具体执行。

决策层、管理层与执行层应做到信息共享，决策层、管理层对于执行层有指挥职权，双方应共同配合做好网络安全运营工作。安全专家组为整体全线网络安全工作提供技术支撑，辅助决策层、管理层开展网络安全运营体系规划建设、重大决策过程中提出专业的建议，指导执行层高效开展安全运营工作，跟进最新技术发展趋势，攻关解决重大、疑难技术难题。

3）运营职责分工需求

岗位职责		岗位描述
决策层		网络安全运营体系决策层为信息化和网络安全领导小组，其职责同时聚焦安全运营整体战略和安全运营重大决策的制定
管理层		工作职责为聚焦推动安全运营体系建设和安全运营整体的指挥、调度、协调工作，参与安全运营重大决策，保障安全运营工作顺利开展
安全专家组		工作职责为协助管理层在安全决策、指挥、调度、执行时提供技术支持
执行层	风险评估组	负责探查全网资产并进行弱点检测，从网络、主机、系统、策略、用户等方面对网络安全现状进行评估，并指导各安全响应组进行加固处置
	威胁监测组	负责对全网的安全威胁进行集中式分析研判，给出专业的处置建议，指导安全响应组进行加固处置
	应急处置组	负责定期开展应急演练工作，一旦发生网络安全事件，进行应急快速恢复，并对事件进行审计取证
	安全情报组	负责收集与企业网络安全相关的威胁情报，根据网络安全实际情况进行场景的推演判定，实现风险态势预测和通报
	建设与加固组	负责承建安全建设、安全设备维护和安全策略优化及安全加固处置等工作

4）网络安全运营流程建设需求

安全运营中心建设不仅要考虑到运营人员的组织分工，还要融合业务发展、

适配管理要求，制定和完善统一化、标准化、高效化的运营流程，形成和落实日常安全运营机制，规范安全运营操作环节、步骤、工具和方法，提高安全运营的工作效率，保证运营操作的一致性、服务交付的统一性和服务质量的稳定性。

安全运营流程设计以网络安全业务为导向，旨在促进安全运营团队工作标准化、体系化，并为安全运营流程通过安全运营管理平台数字化管理、执行以及KPI 评估打下顶层设计基础。流程执行期间，安全运营团队可针对初始流程设计进行评估，并根据实际安全业务需求持续优化、迭代改进。

安全运营流程分为三类：管理类流程、调度类流程、运行类流程，其中管理类流程应用于平台、服务、保护对象、网络安全能力中心的管理以及网络安全工作的绩效考核；调度类流程应用于安全运营管理平台，运营团队通过平台对安全运营工作进行安排调整以及调度，实现对保护对象的看与管；运行类流程应用于安全运营及运维服务，运行团队在保障安全运行工作时，通过该类流程提供标准化、高效率安全服务。

5）网络安全运营支撑平台需求

安全运营支撑平台应基于数据中心业务网络安全底座技术体系实现安全能力平台的无缝集成、安全数据的纳管和共享，通过梳理安全运营的日常业务场景，借助技术手段将组织、流程、工具有机结合实现业务表单化、流转数据化、流程自动化、管理可视化，并提供一个集中式、一体化的安全管理界面为不同层级用户分配多视角、多视图的运营管理视图。

为安全运营团队提供资产风险管理、边界防御、威胁检测、应急响应、运营管理五大核心能力基础承载平台，实现精准化的安全运营执行和精细化的安全运营管理，有效地提高安全运营工作的输出质量和工作效率，持续优化和输出安全能力，最大程度杜绝发生安全事件，保证网络和业务的稳定、可续化运行。

用户需求分析

海口综保区管理委员会

根据海口综保区管理委员会管理职责，通过该平台促进地区物流资源的集约化整合发展，增加园区物流聚集、税收收入。以海口综保区为辐射区，构建覆盖区域内的智慧园区平台，与地方汽运物流企业（平台）、铁路货运部门、港口合作，拓展线上园区业务的开展。同时通过智慧园区平台实现园区信息化生产作业

及安全管理，执行并持续完善园区运营作业规范，公平公正的开展跨境贸易业务，以促进区域内各地区各类优质运力资源的集约化发展，增加货运量。

提供全面了解园区生产作业、调度管理、安防监控等情况，通过数据挖掘、数据分析、智能报表、地理服务、大数据等信息化技术，实现多维度、多口径的统计数据分析，进而为行业管理决策提供辅助支撑。

园区运营作业人员

一站式办理客户发布的展销需求需求，与加工、仓储协同作业，完成全程物流组织与交付。

为保障顺利开展园区跨境业务，园区运营作业人员需要一套完善的内部作业综合服务系统、辅助日常集生产作业、生产管理、经营分析等为一体的实时系统，满足作业过程中堆场、装卸、统计为业务需要，还需考虑现场作业与调度中心联合作业的实时数据传输问题，保障园区内集装箱作业处理和运输组织业务的顺利展开。

为了提升园区出入口的智能化管理，需要实现对出入联运中心的车辆、集装箱等相关业务数据实现自动采集和逻辑校验，辅助无人职守出入联运中心大门的高效管理。

针对园区仓储需要实时掌握仓储位置信息、仓储租赁状态、仓储利用率、园区运力信息、调度信息、相关交易信息等海量数据，对线上、线下各类仓库进行整合管理，实施统一调度、智能分仓、智能调拨，实现库存数量预测预警，从而能够更快处理物流业务，充分发挥仓储利用效率并提高管理水平。

需要保障园区及生产作业安全，对园区不同的区域按照相应的防护要求，实现安全监控，有效处理突发事件及采取相应的应急处置。

园区企业用户

根据园区企业用户发货需求，系统自动提供线上推介全程物流解决方案，实现园区从发货到交付全过程的一体化管理。对大客户主要按协议制定运输解决方案；对于零散客户，主要采取展示展销（直播等）营销模式，促进线上线下业务融合，满足货物销售、物流运输的一站式办理、一单制结算、全程担保、全程跟踪的便捷化服务。根据商品特性、园区企业用户规模、风险防范规则等因素，合

理定制满足不同行业、不同消费群体的线上展销服务平台。

海关监管部门

按照海口综合保税区业务发展特点。海关监管单位对创新业务，新业务应加强安全监管。因此在发展业务的同时，致力于服务海关、海事等监管部门。通过信息化建设实现对钻石珠宝产业、免税交通工具、跨境电商等特殊业务得信息化监管服务。保证货物快速通关的同时，满足严守国门的需求。

项目工期和地点

项目的建设任务主要包括应用系统的需求调研、设备安装、软件开发、测试集成，以及整个系统的测试验收。根据项目组织形式以及工程建设复杂程度、工程量和施工条件，本项目的建设工期（从项目开工到竣工验收）总计为 19 个月。

第一阶段（2022 年 12 月-2023 年 1 月）：本阶段主要目标是完成园区基础设施建设以及部分园区业务急需的应用系统的建设。

第二阶段（2023 年 2 月-2023 年 12 月）：本阶段主要目标是完成园区核心业务应用系统的建设。本阶段结束后，园区业务的主体基本完成。

第三阶段（2024 年 1 月-2024 年 6 月）：本阶段主要目标是完成园区运营、管理、监管等各个业务方向的高层应用需求，面向园区管理者提供基于大数据、人工智能等技术支撑的智慧决策和指挥系统。

地点：用户指定。

项目交付要求

1、投标人须按照计算机工程规范的国家标准分阶段提交相应纸质文档和电子文档。

2、投标人的交付物包括但不限于如下表：

交付物名称	交付物名称	交付物名称
项目相关文档	包括但不限于项目相关的需求规格说明书、概要设计说明书、详细	光盘＋电子文档＋纸质文档

	设计说明书、测试计划及方案、系统使用手册、系统维护手册、培训计划和培训资料、验收相关文档等。	

项目售后服务要求

本项目要求投标人对**所有硬件设备免费提供 3 年维保，软件开发免费提供 1 年维保和 3 年驻场运维服务，自项目通过验收之日起算。**项目维保期内，投标人应提供所有硬件产品原厂质保服务，保障所有软件应用系统的各项业务功能正常运行；软件产品免费提供软件升级、版本更换和技术支持，保障应用系统配套的硬件设备、运行环境、中间件及服务的正常运行；运维期内提供包括巡检、维护、维修、故障排除、系统优化、应急服务在内的各项服务。

1、硬件部分

免费提供操作培训；定期回访以及对设备维护；提供 7x24 原厂售后服务。3 年维保期内定期对设备进行免费保养和维护（免费维修或更换配件），保修期内出现故障，需派出技术工程师到达现场处理故障，并承担一切费用，维保期外发生维修只收材料成本费。

每季度不少于 1 次设备巡检、维护，并在完成后 3 日内提供巡检报告。

2、软件部分

免费维保期内，中标人必须配备一支稳定的专业技术服务队伍，负责系统的一切维护工作，负责为软件提供免费升级服务及系统免费维护服务。免费驻场运维期内，中标人至少派出 4 名技术服务人员驻场，负责本项目运维的一切工作。

培训要求

为确保项目后期的可靠运行，需要配置业务人员、值守人员以及应用系统和数据维护人员，保证中心的持续正常运转。在项目建设期，本项目应用系统开发及软件支撑平台建设，将通过招标选定技术实力强、经验丰富的专业公司完成，开发建设所需技术力量由中标单位自行组织。培训准备阶段，主要通过需求的了解来制定培训的策略，耗时，根据授课对象的不同与培训内容的不同，来定制具体的培训实施方案。将提供：

1、培训大纲：其中应注明每次课程的内容和目的；

2、培训计划：其中应注明每次培训课程的时间、地点及课时；

3、培训内容：系统的性能、相关技术原理和操作使用方法，维护管理的技术，实际的操作练习；

4、课程的文件和资料。

培训内容包括但不限于：计算机应用基础培训、系统管理培训、应用系统操作培训、系统维护培训。

培训方式主要包括以下几种模式：现场培训、集中培训、补训和二次培训、一对一培训、版本升级培训。

培训费用：投标人应将所有培训费用（含培训教材费），计入投标总价；实际培训时间、地点按中标单位与项目业主商定的为准。

培训人数：本项目建设后，系统用户包括业务涉及到的人员，需培训管理和值守人员 20 人。

第七部分：建设方案

建设方案

应用系统建设方案

园区公共服务平台

园区统一门户

各功能模块定义

首页

提供用户登录入口，并可通过平台的用户管理系统注册，同时调用标准版提供的服务，通过标准版验证以及地方验证后成功注册账号。

1、用户注册

用户注册该模块用户可在园区统一门户平台进行注册。

2、系统集成

该模块主要用于各业务系统集成后的登录，业务系统完成集成后，可通过单点登录进行统一登录。

3、单点登录

该模块满足用户登录时可通过同一个账号，使用园区统一门户多个平台业务。

园区概况

1、园区机构

园区机构版块介绍园区内机构的设置与机构职能信息，主要显示综合办公室的主要职责，负责园区日常事务和内部科室组织协调工作，负责园区人事、组织、政务、宣传等相关内容。园区机构模块包含机构概括、领导信息、各内部领导简历、机构所属职能、机构建设方针。

2、园区企业介绍

园区企业介绍主要用于介绍园区入驻企业信息。

3、基础设施介绍

基础设施介绍模块主要用于介绍园区的基础设施。

4、园区优势介绍

该模块主要用于介绍园区的优势，充分体现园区“自贸港+综保区”叠加优势。

5、优惠政策介绍

该模块主要用于介绍园区的优惠政策，点击查看全部跳转至优惠政策详情页。

6、高效率审批

该模块主要用于园区管理模块进行快速审批数据信息，可在审批管理模块进行参数调整。

我要投资

1、招商引资

招商引资版块介绍了用地项目和非用地项目的入园流程，通过点击我要入园进行项目入园申请。同时在页面中展示了产业定位、招商方向、招商政策、园区比较发展等内容。

我要咨询

1、在线交流

在线交流版块是结合小图标的方式列举展示咨询中心提供的咨询、投诉、领导信箱等交流服务，主要包含常见问题、留言查询。将咨询相关的各种在线业务

集中汇总到咨询中心平台中。使用户能够更加快速、准确的定位所需的资讯服务。

2、互动交流

该模块主要用于管理员对企业提问的问题进行答复，支持对问题进行删除、隐藏等管理。

我要投诉

该模块主要用于园区企业进行投诉，主要包含在线投诉、投诉管理两个模块。

案例展示

该模块主要用于向社会及企业展示成功案例详情。

园区动态

1、园区动态

园区动态版块展示的是园区新闻、国务院新闻、省府新闻和媒体报道。

2、专题解读

专题解读版块包含了最新解读、回应关切及新闻发布会，发布对政策的图文解读及召开的新闻发布会的详细信息，回应关切公示了政府或专家对热点问题的回应，展示当前新闻热点或者社会聚焦关注的资讯信息。

信息公开

信息公开版块设立了政府信息公开专栏，对政府信息、人事信息、财政信息、行为规范性文件及中央文件、权责清单等内容进行公开展示。

数说园区

数说园区版块统计近 12 个月的企业注册、跨境申报、营业收入、进出口货值、工业总产值和税收收入的统计结果展示发布。

政务服务

该模块为门户后台管理模块，可管理前台页面展示的主要信息。主要用于发布人才服务、党建党史、投资服务、机构介绍、园区企业、数说园区等。

联系我们

公布了海口综合保税区的联系电话与联系地址、邮政编码、机构网址、电子

邮箱、办公时间，方便相关人员使用。

系统管理

1、文章管理

该模块主要用于园区发布门户相关新闻及文章，并对文章进行管理。

2、友链管理

该模块主要用于维护友情链接，友情链接主要包含六大模块，分别为国家部委、省直部门、市县政府、新闻媒体、保税区、重要部门等。

3、栏目管理

该模块主要用于对门户的栏目进行管理。

4、关于我们

该模块主要用于维护关于我们的信息，点击关于我们进入关于我们详情页信息。

5 、园区跨境溯源查询

该模块主要用于查询跨境电商产品溯源信息。

6、资源管理

该模块主要用于园区的已有资源进行登记管理，可查看不同模块下所有资源讯息。

集成对接

1、系统集成

（1）已规划业务系统

该模块主要用于系统后台集成，对平台内规划的子系统进行集成。

（2）预留业务系统集成

该模块主要用于预留后期接入业务系统的集成。

2、政务服务对接

该模块主要用于对接政务服务系统。

3、第三方服务对接

该模块主要用于与其他第三方服务进行对接，传输数据。

各功能模块定义

数字招商管理子系统

1、系统首页

该模块为招商管理的首页，主要提供系统导航栏、招商热点、政策文件、招商服务、案例、在线互动等模块的入口，并对重要模块进行简单展示。

2、待办事项

该模块为管理模块，企业与招商管理人员可查看不同页面，主要用于查看需要办理的事项，主要包含待我办理、我已办理、招商审核、协调处理模块。

3、招商项目管理

可根据招商工作要求对项目信息进行相应调整或扩展，主要包括项目信息审核、重新修改审核、到资凭证审核、协调事项处理模块。

4、招商项目展示

提供移动版招商项目查询展示功能，可展示 PC 版招商项目所有信息，包括招商项目查询、招商项目列表、招商项目详情、个人收藏功能。

5、招商统计报表

根据管理要求设计报表维度，进行统计。

6、产业链招商

产业链招商通过建链、补链、强链，提升园区产业链核心竞争力。

7、产业服务

产业服务对接园区服务平台，提供产业的服务资源，对企业的财税审计、项目申报、申报管理、政策解读、知识产权等提供相应培训。

园区客服管理子系统

1、客户资料自动弹出（SCF）

呼叫中心来电同步自动弹出客户详细资料及历史服务记录并提供客户资料保护设定功能。

2、自动话务分配

呼叫中心系统智能识别来电，自动将来电分配给相应的座席、队列或语音信箱来处理。

3、电话排队管理

呼叫中心软件可提供智能、高效的队列管理功能。

4、通话录音

无需添加任何专用录音设备，呼叫中心即可实现对所有来电、去电实时录音并可设定录音策略。对电话录音可以方便的备份、下载、回放等。

5、智能话务管理

呼叫中心可灵活实现来电转接、通话保持/恢复、点击拨号、三方通话、通话监听、强插、强拆、示忙/示闲、呼出 DID 号码设定等通讯控制功能。

6、通话详细报告

实时提供通话详单，并针对各分机、队列提供详细的话务分析报告和图表，使您对整个呼叫中心系统的使用情况及坐席绩效一目了然。

7、工作流程

呼叫中心系统内置工作流模块，可根据客户需要，轻松定制企业内部的服务流程，坐席人员可以高效受理客户的服务请求并将服务请求第一直接转化为工作事件。

8、报表统计

通过系统提供的日/周/月/年等对客户服务评价统计和话务统计分析报表数据，为企业领导的业务调整等决策提供强有力的依据。

9、CRM 客户管理功能

支持 Excel 表格的客户信息列表导入，可以分别导入客户名称和客户地址。

会议管理子系统

1、多种移动终端接入功能

系统支持利用 5G、4G、WIFI、普通 ADSL 有线网络，实现对 PC 电脑、笔记本电脑、平板电脑、智能手机等多类型移动终端的接入，支持 IOS，MAC OS X，Android，Windows XP、Windows7、Windows8 等不同版本的操作系统。

2、会议管理功能

会议系统具有方便、高效的会议管理特性：支持同时召开多个会议.不同的会议室可以根据需要进入不同的会议模式,并且可以根据用户需要增加会议室数量，单个会议室支持多个分组会议，可分别进行分组讨论。

3、会议录制和回放功能

会议系统可将会议过程中所有的音视频信息、屏幕信息如电子白板、文档共享、协同浏览等实时录制下来，最真实的再现会议的实际状况，可进行会后录像回放。..

4、电子白板协同操作功能

会议系统支持电子白板，其中包括放大缩小、翻转、捕捉窗口等。电子白板可以授权多人进行控制,也可以锁定白板只有自己可以控制，系统可对电子白板进行保存。

5、桌面及程序的共享功能

会议系统支持屏幕共享、屏幕选定区域共享、应用程序共享，此外，在主席共享桌面时，其他与会者可申请远程操作，主席同意后申请人便可远程控制主席的电脑，实现远程的会议支持。

6、同步播放多媒体文件功能

会议系统支持同步播放任意标准格式的多媒体文件给其他与会者,效果清晰流畅,丰富了会议的表达方式，提升了视频会议的功能和市场价值。

7、文件分发功能

会议系统支持在视频会议过程中将需要分发的文件下发给与会者,同时系统还能根据情况随时灵活添加文件进行共享，方便了会议的应用.

园区服务子系统

1、租赁管理

方便园区内管理办公用房、设备的管理和租赁，对各办公用房进行划分登记房屋信息，以及对繁杂设备的登记，包括种类、数量、名称、型号、购买情况、使用情况等。

2、营销管理

园区会根据实际生产情况，进行营销活动，如一些运营活动、市场活动、推送活动，包括标题、内容、时间、通知人和通知信息等。

3、物业管理

园区的物业信息在此维护，区内企业可查看自己的物业费用、水电费用等相关金额，可进行线上缴费，管理人员可手动录入区内企业的物业费用，必要时可发送信息进行催缴。

4、资产管理

维护管理园区内资产，可登记所有资产的信息，包括时间、所属部门、资产编号、资产类别、所属部门以及折旧信息和入账信息等。

5、停车场管理

规范化管理园区停车场，提供园区内停车场车辆停放信息，作为停车场展示地图的区域信息参数。

6、企业经营情况申报

园区内企业可申报某一时间段内的经营情况，可对企业信息审核，然后返回审核状态。

7、设施设备

（1）As-ls 被动响应

员工电话或 APP 报修、巡逻故障上报、服务热线创建维修单、统一提交维修单。

（2）To-Be 主动维护

巡逻故障自动上报、GIS 地图可视化故障位置、自动触发维修工单上报。

8、政务服务

整合企业监控设备通过大数据技术，对园区内的人、车、货、仓的信息进行数据采集，按业务特性进行数据抽取和清洗后，汇集到数据池中做分析建模透视。

9、投诉建议

园区内企业或者从业人员可对园区的管理单位提出建议，管理单位根据投诉内容给出不同的处理意见。

10、综合查询

对园区内所有业务模块的综合查询功能，可根据不同的查询条件筛选信息。

11、统计分析

通过数据清洗分析提供报表，可根据需求提供不同报表体现，也可展示不同企业、不同时间或不同类型的数据情况。

访客管理系统

各功能模块定义

访客管理子系统

1、访客人员预约

访客管理子系统拟提供网页方式进行预约，访客来访前可在网页提交预约信息。

2、二代身份证阅读

采用 TypeB 非接触 IC 卡阅读技术，对第二代身份证读卡识别。

3、证件扫描识别

证件专用扫描仪，能够扫描身份证、驾驶证等各种证件，生成证件图片，并能对证件做 OCR 识别，有效地保证登记信息的正确性。

4、摄像图片保存

在访客登记过程中，通过摄像头对访客进行拍照，并将拍摄照片与访客身份信息等进行绑定存储，做到人员、证件、照片三者统一。

5、证件图片保存

扫描名片、工作证等一般证件的图片并进行保存，最大限度保存来访人员的信息，确保信息的完整性，方便后续进行统计、查询等。

6、登记数据查询统计

用户可自行设定查询、统计的条件，对以往登记数据进行快速查询、统计。

7、数据海量保存

访客登记所有数据完全存入数据库，同时访客管理子系统对业务系统访客人员数据和闸口系统访客行程轨迹进行同步、保存。

8、登记数据检索

用户可以按照自身需要，自行设定各种查询条件，对以往的登记数据进行快速检索，定位到所查询的数据。

9、数据网络共享

对于多个访客易（多门进出）同时登记的情况下，所有登记数据可以通过网络与闸口系统进行实时共享，方便来访人任意选择进出口。

10、黑名单处理

为了加强对来访者身份管理，系统还可以用证件 ID 对某些身份进行黑名单管理。

11、闸口系统链接

人员识别登记时，可直接选择主要通道门禁进行通行授权，并能通过门禁电子地图实现访客通行轨迹查询。

12、对接业务系统

业务人员进入园区前需在业务系统进行备案、绑定人员、车辆信息等。业务系统备案数据会同步到访客管理子系统。

车辆管理子系统

1、企业信息登记

该模块主要用于企业用户登记企业信息，上传营业执照，支持对企业信息进行修改。

2、备案管理

（1）车辆备案

该模块主要用于园区企业对出入园区的车辆进行长期、短期备案，填写信息后，可提交审核。

（2）临时车辆备案

该模块主要用于临时入园车辆进行临时备案，系统生成填写临时入园的二维码，用户通过扫描二维码进行信息登记，登记后提交审核。

（3）人员入园预约（疫情管理）

该模块主要用于用户在疫情管控期间，提前进行入园人员预约报备。

3、备案审核管理

（1）车辆备案审核

该模块主要用于园区管理方对企业提交的车辆备案信息进行审核，可选择同意、拒绝。

（2）临时入园审核

该模块主要用于园区管理方对临时入园车辆进行审核，可选择同意、拒绝操作，支持管理方对申请进行批量通过、拒绝操作。

（3）预约人员审核

该模块主要用于园区管理方对企业提交的预约入园人员信息进行审核。

4、租仓合同提交

该模块主要用于仓储企业用户提交租仓合同，提供图片上传功能。

5、备案信息查询

该模块主要用于查询信息，包含全部车辆查询、已备案车辆查询、未通过备案车辆查询、预约人员查询。

6、抬杆记录

该模块主要用于查询行政通道抬杆记录，可查看出入园区的车辆记录及其备案信息，用户可通过各类查询条件对车俩出入记录及其备案信息进行查询。

7、车辆类型核对

该模块主要用于园区管理方对车辆类型异常的数据进行修改，对需要修改的车辆进行查询，定位相关车辆后将车辆类型修改为正确类型。

8、基础设置

（1）基础参数

该模块主要用于管理员对系统的参数数据进行管理，用户可在该模块新增相关参数，用于系统表单中填报使用，规范填写标准。

（2）菜单管理

该模块主要用于管理系统的菜单功能，可新增菜单模块，修改菜单名称、增加下级，亦可对菜单进行删除操作。

园区运营管理平台

园区决策分析系统

各功能模块定义

综合管理

综合管理涵盖的数据范围包括一般政务管理、备案数据以及其他数据，服务各类政务及管理人员，提供友好的、全自动及自助式的系统服务，主要包含、经营企业信息库、仓库信息库、资质信息库、自定义查询、报表导出、数据下载、报告自动生成、可视化图表。

通关时效

通关时效是指相关于口岸监管单位海关等部门的各类关键性数据的统计和分析，主要包含进出口通关时长、通关效率分析、海关查验时长分析、进出口放行时长分析、邮件包裹通关时长。

物流管控

物流管控数据业务的涵盖范围包括货种流向、放货数据、堆场数据、集装箱动态数据、电子单据动态数据、指标分析、仓库占有率、货物进出流量、车辆平

均在区时长。

预警管理

预警管理功能主要是对生产安全信息进行阈值比对，采集分析后，系统根据预判规则自动生成的预警提示，为整个口岸安全生产、安全管理保驾护航，主要包括的功能有：货物疫情预警、车辆预警、隐患随手拍等。

产业分析

产业分析主要用于分析园区产业现状，通过对企业数据、行业数据、经济数据进行分析，了解园区企业发展趋势，主要功能包含数据采集、分析建模、产业分析、分析应用。

智能报表

1、企业信息管理

该模块主要包含企业信息登记、企业信息查询，企业信息登记主要用于企业进行企业信息的完善，管理方可在该模块进行企业纳统授权。

2、报表申报管理

该模块主要包含园区企业人才调查表、园区工业企业主要指标调查表、园区工业企业主要产品产销量调查表、园区第三产业企业（单位）主要指标调查表的申报，企业可在该模块进行报表的填写并提交审核。

3、报表审核管理

该模块主要包含园区企业人才调查表、园区工业企业主要指标调查表、园区工业企业主要产品产销量调查表、园区第三产业企业（单位）主要指标调查表的审核，管理方可在该模块对报表进行审核，可通过或退回企业。

4、历史报表管理

该模块主要包含园区企业人才调查表查询、园区工业企业主要指标调查表查询、园区工业企业主要产品产销量调查表查询、园区第三产业企业（单位）主要指标调查表查询、综合报表查询、漏报查询。

5、报表期限管理

该模块主要用于管理方对各类报表的报表期进行设置，设置后企业可在报表期内进行报表的申报。

6、预警参数管理

该模块主要用于管理方对各类报表的预警期进行设置，设置后系统可在设置期限对未申报企业进行申报预警，可设置多个预警参数，进行多次预警。

7、系统管理

该模块主要用于对系统的用户信息、角色信息、菜单信息、数据字典等信息进行管理，可在该模块对用户进行授权操作。

园区智慧党建系统

各功能模块定义

党建管理子系统

1．党员管理

维护党员电子档案库,操作留痕，信息校核准确性,快速查找党员；对党员关键信息进行加密保存。

2．党籍管理

动态维护党员党籍变化，实现系统内部全程跟踪管理。

3．发展管理

扎实做好入党申请人培养，把发展重心放到企业生产第一线，实现对发展党员五大阶段 25 个发展环节的管理，规范发展流程，实现发展党员的电子化管理。

4．组织管理

搭建党组织基础信息库，实现对组织基本信息、单位信息的维护、换届选举、班子成员任免等。

5．主题党日管理

贯穿主题党日活动的策划发起、通知、开展、活动总结等各环节需求，支持活动报名、签到、请假、自动考勤统计等，提高主题党日管理效率。

6．民主评议管理

在线管理民主评议会议信息，实现会议考勤管理，可对党员评定结果进行录入，实现民主评议线上管理全纪实。

7．党费管理

实现党费标准设置、收缴、统计全流程的规范化管理。

8．在线学习

由党员根据个人需求进行自主选学。

9．在线考试

党员在学习结束后，可以通过考试检验学习效果。

党务服务子系统

- 政治生日

“政治生日”激发先锋活力，定制和发送政治生日贺卡、礼物、祝福语，支持图文结合展现形式，体现组织和党员的温暖关怀，能够重温入党誓词，体现党员不忘初心牢记使命。

- 支部信箱

支持收集党员意见或建议、解答党员疑问、处理举报投诉，可匿名公开常见问题与回复问题。党员对答复内容进行采纳与满意度评分，促进良性互动。

- 投票问卷

自主设置题型、题目及选项等多类属性，一键发送问卷提醒，支持匿名投票的管理。党员参与投票，系统自动统计结果并生成统计报表，公开又便捷。

- 三会一课管理

实现对党员大会、党支部会议、党小组会议、党课情况的管理。支持线上录入会议，发送会议通知、签到、请假、纪要上传、统计、查询等功能，同时也支持会议数据的补录，实现对三会一课的全方位管理。

- 爱心公益

党员可以发起爱心公益，经过党委审核后，可对外展示，系统内所有用户都可以报名参加，活动结束后可获得爱心积分。

- 关爱帮扶

实现对困难党员的关爱帮扶，实现对困难党员信息的线上管理工作，便于对困难党员信息的实时掌握，也为后续困难党员慰问活动开展提供数据参考依据。

- 党员服务窗口

建设党员服务窗口，实现对园区企业和党员的反馈问题的受理，畅通企业遇困的诉求渠道，促进企业良性发展。

监督考评子系统

通过清单式量化考评，常态化开展党建督查，梳理细化出园区党建工作的重点督查内容。

■ 党组织考核

对党组织的考核过程、考核结果、奖惩情况进行综合性的管理，对考核结果进行公示。

■ 党员考核

对党员的考核过程、考核结果、奖惩情况进行综合性的管理，对考核结果进行公示。

安全生产管理系统

各功能模块定义

安全生产一张图

全面汇聚安全生产数据资源，对安全生产风险进行标准化、流程化评估，采用美观清晰的可视化图标方式对安全生产风险分析结果、隐患排查治理信息及重大危险源监管信息进行展示，可快速、全面、准确地掌握辖区内企业安全风险分布和变化情况、隐患排查治理情况及重大危险源监管情况，对当前安全生产工作的工作量和工作压力进行初步判断，辅助制定下一阶段的工作计划，确保安全生产监管工作有的放矢。包括风险云图、风险点分布图、风险排名、行业风险分析、风险变化趋势、隐患统计分析、隐患排查治理信息、重大危险源监管信息。

园区封闭管理一张图

园区封闭管理模块结合园区人员、车辆定位信息、电子围栏数据、出入卡口数据、高点监控视频等感知手段和信息资源，实现对出入园区的内部和外部人员、车辆进行精细管理，对危化品运输车辆等重点监管车辆实行严格的全流程动态管控，确保园区各项流动性因素得到有效管控，为园区企业提供安全可控的封闭化管理环境。系统实现园区出入卡口监管信息、电子巡查监管信息、园区全景监控等信息在地图上的综合展示。

园企信息管理

通过整合园区企业档案管理、园区信息管理、公共设施管理信息，实现园区企业安全生产、环境信息、应急信息、消防设施台账、园区基础信息和公共设施一表清，便于园区管理者快速、全面地掌握上述各类信息，为安全生产管理和应

急提供数据支持，包括园区信息管理、公共设施管理、企业档案管理功能。

园区风险隐患双控

风险隐患双控包含风险分级管控及隐患排查治理两部分。风险隐患双控系统是指针对企业安全生产风险分级管控与隐患排查治理，风险分级管控首先进行风险辨识、分级并采取管控措施，再根据各风险点的管控措施是否到位、各项管理制度等基础管理情况制定隐患排查治理清单。系统分为企业端和管委员端的两个方面的应用，包括风险分级管控、隐患排查治理功能。

教育培训管理

教育培训管理可为园区相关业务人员增强危机意识和责任意识，提高突发事件防范能力，并提高应急救援人员的应急能力，从而保证应急防控方案贯彻实施。

日常安全监管

日常安全监管包括特殊作业管理、特种设备管理及履职考核管理，加强事前防控，为园区安全生产提供保障，企业端实时和及时更新有关涉及生产安全的信息数据。

全景展示管理子系统

（1） 园区业务总览

园区业务总览展示海口综合保税区运营的主要信息

（2） 园区成绩及发展

园区成绩及发展主要展示历年园区贸易额统计、历年园区贸易量统计、历年园区入驻企业量统计。

（3） 跨境电商版块

跨境电商版块主要展示 1210、9610、9810、9710 业务数据量及跨境电商场站货物吞吐量。

（4）园区车辆吞吐版块

园区车辆吞吐版块主要展示出入园区行政车辆统计数据。

（5） 简化进出区版块

简化进出区版块主要展示园区简化进出区、货物维修、一般纳税人业务开展情况。

（6）分类监管版块

分类监管版块主要展示园区分类监管业务开展情况。

（7）仓储版块

仓储板块主要展示园区仓储业务现状。

（8）企业版块

企业版块主要展示园区入驻企业情况。

展销综合服务平台

云展综合服务系统

各功能模块定义

线上展览展示子系统

不管是线上和线下，展示、洽谈、对接的需求是不会变的。在线上，我们依然要实现买卖双方对接和洽谈的需求，这是永远不会变的，技术只是更好的解决效率和效益问题。展会主办方可以采用虚拟数字场馆模拟线下办展的全流程，有真实的带入感和场景感，呈现看得见的服务，使观众和展商获得良好体验。主要包含虚拟登录大厅、虚拟展馆和展台、展品展示中心、移动端展销助手。

线上活动直播子系统

1．线上直播巡管管理

通过自动设定巡管路线，建立直播巡查路线，主要包含涉政视频识别、色情视频识别、暴恐视频识别、广告视频识别、未成年人识别。

2．主分论坛等活动直播

采用 3D 虚拟直播室或者实景直播间，支持单人及多人直播会议，可以借助同传、字幕和速记等功能，支持国内外嘉宾远程参与，支持 PC 端与移动端同步观看，支持全程录制。

线上商贸洽谈子系统

参展商和采购商双方之间需要精准、高效配对和洽谈。在买卖双方预约成功后，会自动开启在线洽谈直播间，双方实现云洽谈，洽谈结束后可通过问卷进行调研，并对洽谈质量进行打分。

线上展览管理系统

1．智慧宣传中心：通过 B 端和 C 端渠道，吸引高质量的观众；

2．智慧邀约中心：包含定向邀约系统和非定向邀约系统；

3．智慧展览运营中心：包含展商和观众服务、活动运营以及商务洽谈等；

4．线上展览大数据：可以实时统计在线观众流量、观众停留时间等相关数据，可以展现同比增长人数及展位热度排名等内容。

5．管理中心主要包含登录大厅、主办方中心、参展商中心、云展厅、站台搭建、数据统计。

宝玉石交易服务系统

各功能模块定义

商品展示销售

1、宝玉石展示

宝玉石交易服务系统对宝玉石商品信息进行分类展示，支持通过营销管理设置区别化展示宝玉石的商品信息。

2、收藏家社区

宝玉石交易服务系统的收藏家社区支持内容发布、交友、聊天、社区论坛、社区活动、社群管理等功能。

3、用户中心

管理用户的用户名、密码、头像、历史浏览信息、自我介绍信息、个人标签、个人收藏、个人二维码等信息。

4、订单中心

管理用户的订单信息，支持订单的列表展示和搜索查询，并根据待付款、待发货、待收货、待评价的订单状态进行订单的分类展示。

支付鉴定

1、购物车

用户可将意向购买的宝玉石商品加入购物车，支持商品的选择支付、删除、移入收藏夹。

2、溯源管理

用户通过溯源管理功能，可对宝玉石原料采购、设计、生产、仓储、物流、销售信息进行查看，帮助用户掌握宝玉石产品的全生命流程。

3、支付

用户可在宝玉石交易服务系统对选定的商品进行微信支付、支付宝支付、网银支付并支持支付信息的查询。

4、鉴定管理

用户支付环节可自选宝玉石的鉴定服务，通过鉴定管理功能可以查询商品的鉴定证书、鉴定机构、鉴定时间等信息。

5、撤销和退款

支持用户撤销支付申请和退款申请，支持对撤销支付及退款信息进行查询管理。

6、短信验证

短信验证功能旨在确保支付安全，用户通过短信验证可增强支付安全性并体现用户在支付、商品鉴定方面的自助行为。

后台管理子系统

1、进销存管理

进销存管理支持批发销售零售销售，供货商往来帐务管理，客户往来帐务管理，支持销售换货，支持财务管理功能，支持库存盘点功能，支持分销。包含库存管理、采购管理、销售管理。

2、用户管理

用户管理支持对用户账号进行管理，包含对用户账号的列表展示、添加、删除、禁用、启用、编辑和查询；支持对使用该系统的用户进行查询。

3、权限管理

支持对后台管理子系统的操作权限进行设置。包含身份认证管理，功能操作权限的管理，数据获取权限的管理。

4、财税管理

支持对采购、运输、生产加工、仓储、销售的财务数据进行统计分析、生成报表，支持成本、利润、税收、退税数据的统计分析，支持财税凭证的管理。

5、订单管理

订单管理与进销存管理、用户管理、财税管理实现数据互通，支持对用户下

达的订单进行管理及跟踪。

6、宝玉石加工管理

宝玉石加工管理功能包含生产设备管理，物料管理，生产技术文件管理，工艺数据管理，装置开停工方案管理，临时工艺、临时标准管理，统计报表管理，综合查询管理，加工增值内销货物计税管理。

7、商品管理

商品管理支持商品信息的录入、导入、上架、下架、删除的批量操作，支持对商品按照类目、监管政策进行分类管理。

8、政策指引

支持海关监管政策、园区管理规范、贸易享惠政策、税收减免政策、其它政策法规的动态维护与解读。

9、营销管理

营销管理功能支持促销、满减、满赠等营销活动的管理，优惠券管理，折扣管理，捆绑销售管理，营销数据跟踪分析及报表自定义等。

10、数据分析

数据分析功能支持数据的整合，包含数据抽取、数据清洗、数据转换、数据调度、运行监控等，支持数据建模，支持数据分析展现。

资源云交易系统

各功能模块定义

买/卖方交易子系统

1、卖方交易管理

（1）我的发布

可以自行决定是否需要发布产品信息，若委托交易中心发布产品信息，需要向交易中心递交产品相关纸质材料。

（2）我的交易

我的交易包括发布的交易信息详情、交易信息状态组成。

（3）历史交易

历史交易包括查询历史交易记录，可根据具体交易信息进行查询。

（4）查询统计

查询统计模块主要统计日报表、周报表、月报表、年报表，企业根据统计表分析主要数据，提升分析工作效率。

（5）会员基本资料维护

会员完成注册之后即可获得平台提供的会员账号和登录密码，可以登录系统。

（6）企业诚信管理修改

交易中心工作人员在“诚信管理”页面中可设置不同等级的诚信意向金修改。

2、买方交易管理

（1）查询统计

查询统计模块主要统计日报表、周报表、月报表、年报表，企业根据统计表分析主要数据，提升分析工作效率。

（2）交易列表

交易列表模块主要查询交易信息，点击交易数据局可跳转至交易列表详情页。

（3）我的报名

该模块主要满足招标事前报名，对用户的报名记录进行后期查询，根据关键字筛选报名数据。

（4）我的交易

我的交易包括发布的交易信息细节、交易信息状态组成。

（5）历史交易

历史交易包括查询历史交易记录，可根据具体交易信息进行查询。

（6）合同打印

合同打印模块可以根据卖家提交的纸质合同的内容，将多笔交易信息同时打印。

（7）查询统计

查询统计模块主要统计日报表、周报表、月报表、年报表，企业根据统计表分析主要数据，提升分析工作效率。

（8）会员基本资料维护

会员完成注册之后即可获得平台提供的会员账号和登录密码，可以登录系统。

（9）密码修改

买卖双方可对自己的密码进行修改，无需交易中心审核。会员在输入旧密码，同时两次输入相同的新密码即修改密码成功。

（10）诚信意向金管理

交易中心工作人员在“诚信管理”页面中可设置不同等级的诚信意向金，诚信意向金要用于在使用交易系统过程中根据是否遵守交易规则，在交易过程中的每一个环节对交易参与者进行考查并赋予相应的分数，并根据不同的分数段给予相应的等级。

交易控制子系统

1、会员管理

（1）会员信息管理

会员信息主记录是指存放在系统中的所有有效会员的正式记录，根据主记录的状态变化来反映本模块对其他模块的影响。

（2）企业诚信管理

在使用交易系统过程中根据是否遵守交易规则，在交易过程中的每一个环节对交易参与者进行考查并赋予相应的分数，并根据不同的分数段给予相应的等级。

（3）监管管理

该模块所有的企业有一个“监控等级”属性，该属性有三个等级：正常企业、重点监控企业、黑名单企业，默认值为“正常企业”。

（4）屏蔽清单

屏蔽清单包含拉黑、解除拉黑，交易中心工作人员根据需要进行屏蔽拉黑角色。

（5）会员信息管理

会员信息管理通过会员注册申请审核通过后方能生成，修改需要会员信息修改申请审核通过后方完成修改，删除需要会员正式退出平台方可标记删除。

2、交易管理

（1）交易信息发布

交易信息发布包括发布的交易信息细节、交易信息状态组成。新增：需要通过发布申请经过交易中心安排之后方能生成。

（2）买方报名

该模块主要满足招标事前报名，对用户的报名记录进行后期查询，根据关键字筛选报名数据。

（3）交易控制

该模块交易信息发布之后不能进行修改，交易信息不可随便删除。若加贸企

业选择自行发布产品，需要在平台中填写产品发布申请，同时准备产品的相关纸质材料，提交交易中心工作人员。

3、财务管理

（1）诚信意向金管理

诚信意向金管理主要用于在使用交易系统过程中根据是否遵守交易规则，在交易过程中的每一个环节对交易参与者进行考查并赋予相应的分数，并根据不同的分数段给予相应的等级。

（2）会员费管理

会员费管理包含有效会员的续费正式记录，企业注册成为交易系统会员之后需要缴纳会员费。

（3）交易服务费管理

交易中心工作人员在“交易服务费折扣率”页面中修改交易服务费折扣率。

（4）招标代理服务费管理

该模块招标代理服务费管理包含收费、打印缴费等功能。

4、汇总统计

（1）出货备案统计

汇总统计模块核心功能为信息登记汇总、出货备案统计表、财务出货记录账单统计表、招标工作表等交易中心内部用户无法访问。

（2）信息登记统计

信息登记统计根据所有的交易信息进行登记统计，根据加贸企业、回收企业等进行数据筛选。

（3）财务出货记录统计

适用于招标交易，以每笔议价每次实际出货来计算成交金额和交易服务费。交易手续费是按照含税价计算，即便该招标是完税价格交易。

（4）招标统计

招标统计该模块按照卖方与买方关于某商品的实际成交及出货数量的关系，来统计招标合同、议价周期及出货情况。

5、基本情况管理

（1）商品类别维护

该模块主要用于对需要交易的商品类别进行提前维护，后期企业进行交易时无需重复录入。

（2）海关代码维护

该模块主要用于海关编码类别进行提前维护，后期企业进行交易时无需重复录入。

（3）商品编码维护

该模块主要用于商品编码进行提前维护，后期企业进行交易时无需重复录入。

（4）工作日管理

工作日志管理该模块主要用于查询工作日志，便于交易中心工作人员对工作日志的查看。

（5）评标规则

评标规则模块是运用评标标准评审、比较投标的具体方法。该模块可对评标规则进行查询，搜索评标关键词，系统根据关键词进行检索筛选，查询评标信息。

6、系统管理

用户管理、角色管理、权限分配、日志管理、CA 证书管理。

信息发布子系统

1、交易信息

该模块主要用于交易信息查询，主页面显示“序号”、“交易类型”、“招标企业性质”、“回收企业服务类型”、“交易服务费折扣率”和“生效时间”、“操作”等字段。

2、政策公告

政策公告模块主要用于最新政策显示，可进入政策公告详情页，进行政策公告查询。

3、通知公告

通知公告模块主要用于公告通知展示，可进入通知公告详情页，进行通知公告及历史查询。

4、价格指数

以后各个时期平均价格同基期价格相比计算出的百分数。编制比较系统的价格指数。

5、图片定制新闻

该模块可用于定制大屏展示新闻图片。发布的信息可以根据配置选择，实现在内网、外网和大屏幕上的发布显示。

作业综合服务平台

一体化 ERP 云服务系统

各功能模块定义

基建项目管理子系统

基建项目管理系统到目前已经成为中国经济发展的重要保障，特别是政府投资的基建项目，在加速建立社会经济基础，促进科学文化教育发展、提高人民生活水平，促进社会和谐和经济持续稳定发展方面发挥着至关重要的作用，基建项目管理系统是项目成果资料的积累，是项目管理工程师对项目过程规范严格要求确保项目进度与质量规范达标的标准。主要包括项目申报管理、项目受理管理、项目分送管理、项目审批管理、项目报价查询、项目汇总管理、资金计划管理、资金计划调整、项目库管理、系统对接。

物业管理子系统

物业管理系统是现代园区不可缺少的一部分。一个好的物业管理系统可以提升园区的管理水平，使园区的日常管理更加方便。将计算机的强大功能与现代的管理思想相结合，建立现代的智能园区是物业管理发展的方向。重视现代化的管理，重视细致周到的服务是园区工作的宗旨。主要包含客户服务、收费管理、资源管理、OA 办公、业主管理、安保消防、报事报修、物料设备、财务管理。

防疫风险预警子系统

防疫风险预警子系统主要用于疫情防控期间对出入园区人员的健康状况、核酸检测情况进行跟踪及预警，系统数据主要来自于园区人员通道闸机设备及园区企业自行上报数据。主要包含闸机数据采集、临时进出人员分析、企业人员维护、人员健康信息报备、企业人员出入园区记录、临时出入人员记录、预警信息管理、风险参数设置、系统设置。

智慧云仓服务系统

各功能模块定义

仓储服务子系统

1、入库管理

入库管理主要对货物的入库过程进行管理，主要包含申报信息反馈、入库计划、入库准备、卸货记录、入库理货、面单打印。

2、出库管理

出库管理主要对货物的出库过程进行管理，主要包含出库计划、出库准备、货物分拨、装车出库。

3、库存管理

该模块主要对库存进行管理，主要包含库存管理、库位转移、仓库架管理、动态盘点、库存调整审批。

4、报表管理

该模块主要用于进行报表统计，主要包含入库统计、出库统计、库存统计、商品统计。

5、订单管理

（1）订单查询

订单查询是根据不同维度，对订单进行综合查询，如商品类型等。

（2）订单维护

订单维护是维护新增订单，根据实际情况可修改、删除订单号，货物名称，数量，类型等数据，完善订单信息。

6、费用管理

费用管理是系统可对仓库作业过程中产生的费用进行统计、查询以及费用类型维护。

7、仓库管理

该模块主要用于设置仓库的基础信息，包含仓库设置、库区设置、库位设置。

8、综合查询

该模块主要用于查询，主要包含入库明细查询、出库明细查询、库存调整查询。

9、系统管理

系统用户管理功能通过对接统一权限单点登录进行同步，主要包含用户管理、角色管理、授权管理、资源管理。

10、云仓储移动端

主要用于库内上下架操作，主要包含微信绑定、指令推送、装卸记录、单据查询、库存查询、报表查询、在线提问、常见问题。

云仓联网辅助监管子系统

1、仓库可视化统计

主要利用可视化方式对全省各特殊监管区域仓储位置、仓储面积、仓库个数、企业数进行展示，便于海关查看各特殊监管区域的仓储情况，主要包含全部仓库、特殊区域仓库、非特殊区域仓库。

2、仓库总览

对各特殊监管区域的仓储进行分区管理，可通过仓库数据对各仓库的商品类型进行统计排名，可查看各园区的主要储存商品及开展业务，主要包含综保区管委会自有仓库、嘉城国际物流中心仓库、菜鸟物流中心仓库、中免国际物流中心仓库。

3、仓储企业信息

对各特殊监管区域的企业信息进行管理，可根据不同园区查看所属企业信息及其仓库信息，主要包含全部企业信息、海口综保区企业信息、空港综保区企业信息、洋浦保税港区企业、三亚保税物流中心企业、区外企业信息。

4、仓库信息

对各特殊监管区域的仓库信息进行管理，可根据不同园区查看所属仓库信息及其商品信息，主要包含全部仓库信息、海口综保区仓库、空港综保区仓库、洋浦保税港区仓库、三亚保税物流中心仓库、区外仓库信息。

5、商品信息

对各特殊监管区域下仓库储存的商品信息进行管理，可根据不同园区查看所属仓库的商品信息及其库存、出入库信息，主要包含商品列表、商品库存。

仓库租赁管理子系统

1、园区租赁资源展示

实现园区仓库资源、叉车、吊车、电动平衡重力叉车、高位液压叉车等园区仓库相关租赁资源的展示，并实现企业在系统上的仓库相关资源租赁记录查询智能租仓推荐、订单管理等功能，包含仓库租赁设备资源查询、地图选仓、订单管理、智能推荐。

2、资源租赁交易记录查询

该模块实现设备资源、仓库租赁的交易记录查询，包含支付记录管理、账单记录管理等功能。

3、企业闲置资源展示

该模块实现企业的闲置设备等资源的展示，并提供其它企业在系统上的企业闲置资源查询、闲置资源展示、订单管理、智能推荐。

4、闲置交易

该模块主要用于实现企业闲置资源的交易，包含支付管理、账单管理等功能。

5、后台管理

后台管理该模块主要实现园区对仓库租赁资源及企业闲置设备资源的综合管理，实现对园区资源的监控及安全管理。主要功能模块包括基础信息管理、仓储设置、仓库楼设置、场所租赁清单管理、设备租赁清单管理、租赁平面图、租赁费用维护管理、预警处置跟踪、统计分析、闲置资源清单管理、闲置费用维护管理、订单管理、用户管理。

视频管理子系统

1、全部视频展示

该模块主要用于查看园区仓库重点位置视频接入，便于管理层对园区内部进行统一管理、及时掌控工作的进度状况，重点位置的视频展示可让相关人员直观查看仓库重点管理范围，仓库视频接入管理可有效提升园区生产安全。

2、A 仓库接入视频

该模块主要用于查看 A 仓库重点位置视频，实时监测、警报，大程度的降低人力成本，实时进行画面保存，随时查看回放录像，能够及时发现工作错误，减少误差。

3、B 仓库接入视频

该模块主要用于查看 B 仓库重点位置视频，实时监测、警报，大程度的降低人力成本，实时进行画面保存，随时查看回放录像，能够及时发现工作错误，减

少误差。

4、C 仓库接入视频

该模块主要用于查看 C 仓库重点位置视频，实时监测、警报，大程度的降低人力成本，实时进行画面保存，随时查看回放录像，能够及时发现工作错误，减少误差。

5、D 仓库接入视频

该模块主要用于查看 D 仓库重点位置视频，实时监测、警报，大程度的降低人力成本，实时进行画面保存，随时查看回放录像，能够及时发现工作错误，减少误差。

6、后续接入仓库视频

该模块提供后续入驻企业仓库重点位置视频接入，接入视频后便于管理层对仓库内部进行统一管理、及时掌控仓库的使用状况，更高效完成监督管理。

物流运输管理系统

各功能模块定义

运输服务子系统

1、物流运输管理

（1）基础信息管理

对物理运输管理系统的项目信息和用户信息进行维护，便于订单的生成和流转。

（2）开单

在运输业务的第一阶段，通常以开单的方式提出用车需求。开单包含许多其他功能，如信息关联、地图定位、里程预估、上下游价格预估等，具体的内容根据用户需求而定。

（3）订单管理

订单创建成功后，进入运输业务的第二阶段，运营商按照一定的规则处理订单，并将订单推送给合适的承运商。

（4）智能调度

物流运输管理系统订单体量大，协调资源多，纯人力调度效率低、成本高，

难以满足配送需求。智能调度针对以上痛点，利用算法围绕人、车、路线合理规划调度策略，实现最优资源分配方案，高效完成调度工作。

（5）订单跟踪

订单跟踪进入运输业务第三阶段,承运商开始执行配送任务,实时跟踪订单状态，并将状态信息回传给运营商，再由运营商回传给货主。订单跟踪可使货主实时获取当前订单状态，也方便平台管控司机，保障订单任务顺利完成。实现订单跟踪的方式有两种——人工更新、电子围栏。

（6）签回单管理

判断一个运输任务是否完成，以货主是否签收订单为准。货主签收订单后，承运商需上传回单并更改订单状态以完结一个订单。

2、价格管理

（1）计价方式

运输业务常用的计价方式有以下五种：单一计价、分段计价、梯度计价、比价计价、分段+梯度计价。

（2）价格模板维护

对于不同商家、承运商，甚至于不同货物，运输的计价方式不同，根据不同的需求需要维护不同的价格模板，方便使用和管理。价格模板分为上游价格模板和下游价格模板两种，上游价格模板是对商家进行收款的计价规则，下游价格模板是对承运商进行付款的计价规则。

3、结算管理

在结算管理中，完成对订单费用的调整和审核工作，然后由财务人员对照账单进行上下游的收款和付款。

4、异常管理

在订单创建之后，签收之前，都可上报异常，上报异常时需对异常情况进行说明。

5、2C 业务

对于 2C 的运输业务，除了以上的功能模块，还需要有司机管理模块，与上面描述的用户管理的不同之处是，司机管理只需对用户信息进行维护，无需绑定合作关系。

6、物流运输全流程跟踪

通过结合海关监管平台信息化平台的数据、海关数据、视频监控数据、地图、

GPS、RFID 的数据信息，实时监控货物从入港、装车、运输、入园、入库、出库的全流程跟踪。

7、车辆无感进入园区

通过结合海关监管平台信息化平台数据、园区卡口监控及智能诱导屏，智能识别对应车辆，实现车辆无感进入园区，根据诱导屏行驶到相应的货物存放仓、车辆自主备案。

8、车辆自主备案

建立综保区智慧园区 APP，企业/报关员/司机可以登陆下载 APP，在 APP 上完成车辆自主备案。

9、智能化行政卡口

车辆通过卡口时，硬件设备进行相关车辆信息的采集，包含：车牌、车重、外观图片、集装箱尺寸与备案车辆进行比对，如车辆未进行备案，则系统不完成抬杆动作。

10、卡口临时登记

企业/报关员/司机可以登陆下载 APP，在 APP 上完成卡口临时登记。企业在手机端提交样品、工具、治具等临时进区申请，要求录入货物信息（需上传照片）、收发货企业名称、携带货物的人员（身份证、联系电话）及车辆信息。

11、卡口分流、司机引流

卡口自动分流，司机自动引导，将报关单的布控查验信息推送给智慧查验管理系统的海关端及客户端，进行分流。

12、园区物流路线智能规划（区内区外线路规划）

通过企业服务平台与货代/报关行进行对接，获取货代/报关行空运、海运、路运线路，并对线路进行整合，串联，作为基础资料，为其余相关同航线货代/报关行提供成本低、时间短的多式联运、港到港等国际物流运输方案。

13、对接建设海关智慧物流辅助管理系统

前期建设海关智慧物流辅助管理系统，后期对接统一的海南海关智慧物流辅助管理系统，数据落地园区。

在途监管子系统

在途监管子系统主要用于园区管理方对物流交易的运输过程进行监管，可对运输车辆的轨迹进行监控，查询车辆的实时定位，并以地图的方式进行可视化展

示。

1、轨迹回放

车辆的轨迹回放是车辆监控的重要组成部分，用来追踪车辆，预测货物的送达时效，计算车辆的运力等。主要包含轨迹信息管理、轨迹地图。

2、常停地址

根据 GPS 采集车辆的停靠地址信息，聚合出车辆经过的地址列表，为车辆的线路管理提供数据支撑，指引司机行驶最优线路，来降低物流成本，提高运输效率。

3、危情报警

支持对于突然的地质灾害的预警提醒，通过获取车辆经过的区域的信息，经过大数据搜索影响该区域的地质灾害信息，自动通知公司做好人员、车辆、货物的防控措施。主要包含报警查询、报警处置管理、电子围栏预警管理、天气预警管理、超速预警管理、地图管理。

4、用户管理

该模块主要用于对从用户中心登录的用户进行管理，可查询用户信息，亦可对用户进行导出。

5、里程统计

根据查询的车辆，检索出系统从 GPS 上采集到的车辆里程数，生成汇总的里程数清单。

6、实时监控

系统支持灵活配置 GPS 的采集参数，根据业务要求灵活采集需要车辆数据，主要包含车辆定位信息管理、监控信息管理、运输全流程管理、监控地图坐标管理、历史路线信息管理。

7、 电子围栏

防止车辆进入非安全区域，系统支持通过建立电子围栏来限制车辆驶入特定的区域，坐标化管理来实时监控车辆，避免管理的失控，主要包含围栏设置、围栏限速、围栏边界、围栏监控、围栏报警、围栏预警处置。

简化进出区管理子系统-企业端

1、企业中心

该功能主要用于企业对企业基础信息进行登记，主要功能包含企业信息登记、

企业信息查询、维修人员登记。

2、商品中心

该模块主要用于企业进行区内流转业务时，对流转商品进行备案，主要包含商品信息登记、商品信息查询。

3、资质登记

实现仓储企业、物流企业、加贸企业、经营企业等，向海关申请可开展业务类型资质的功能，包含资质登记、资质注销、资质查询。

4、账册备案

实现海关对特殊监管区域内开展业务企业的电子账册备案联网管理功能，包含、账册备案、账册变更、账册查询。

5、维修账册管理

该模块主要用于管理货物维修出入区记录，账册内容根据飞机维修核放单放行状态自动更新。

6、简化进出区核放单

该模块主要用于企业对简化进出区类型物品的出入区核放单进行申请，主要功能包含核放单申请、作废申请、核放单查询。

7、货物维修核放单

该模块用于维修企业申请飞机出入区核放单，企业端提交核放单申请，海关端审核，维修核放单不能进行负数库存操作，主要功能包含核放单申请、作废申请、核放单查询。

8、一般纳税人核放单

该模块主要用于企业对一般纳税人类型物品的出入区核放单进行申请，主要功能包含核放单申请、作废申请、核放单查询。

9、库存管理

该模块主要用于企业进行库存的调整，海关审核通过后，调整成功，主要功能包含调整单申报、调整单查询。

10、区内流转管理

该模块主要用于企业进行货物区内流转，通过转入企业与转出企业的流转申请，进行库存的转移，海关审核通过后，转入转出企业账册自动核增核减。主要功能包含：转入申请管理、转入查询、转出申请管理、转出查询。

11、综合查询

提供分类监管核放单的审批进度综合查询功能，能够按照企业权限进行数据展示。

12、统计分析

对系统的企业量、业务量、商品库存、主要商品进行统计，供园区管理员方查看。

13、基础设置

该模块主要提供菜单管理、参数管理功能，用于对企业端的系统参数进行配置。

简化进出区管理子系统-监管端

1、资质审核

该模块主要用于海关对仓储企业、物流企业、加贸企业、经营企业等提交的简化进出区、货物维修、一般纳税人资质信息进行审核，主要功能包含资质登记初核、资质登记复核、资质注销初核、资质注销复核、资质登记管理、资质登记查询。

2、账册审核

该模块主要用于海关对仓储企业、物流企业、加贸企业、经营企业等企业提交的简化进出区、货物维修、一般纳税人账册信息进行审批，账册生效后应根据各企业进出区申请自动核算，一种业务类型一家企业只能有一本账册，账册编号为唯一标识。主要功能包含账册初审、账册复审、账册查询。

3、简化进出区审核

该模块主要用于海关对企业提交的简化进出区核放单进行审批，系统可根据设置的风险参数和自动审批开关，对核放单进行自动放行、布控查验、人工受理等操作，主要功能包含人工核验、核放单作废、人工过卡口、核放单查询。

4、货物维修审核

该模块主要用于海关对企业提交的货物维修核放单进行审批，系统可根据设置的风险参数和自动审批开关，对核放单进行自动放行、布控查验、人工受理等操作，主要功能包含人工核验、核放单作废、人工过卡口、核放单查询。

5、一般纳税人审核

该模块主要用于海关对企业提交的一般纳税人核放单进行审批，系统可根据设置的风险参数和自动审批开关，对核放单进行自动放行、布控查验、人工受理

等操作，主要功能包含人工核验、核放单作废、人工过卡口、核放单查询。

6、账册管理

该模块主要用于海关查看各类业务的账册库存，包含简化进出区账册、一般纳税人账册、维修账册，账册根据核放单进行自动核增核减，海关可查看各类商品的账册核增核减明细。

7、库存管理

该模块主要用于海关审核企业提交的库存调整单，主要功能包含库存调整核验、库存调整查询。

8、区内流转审核

该模块主要用于同一业务场所两家不同企业之间的货物流转管理，实现转入企业转入申请单以及转出企业转出申请单审核、查询以及逻辑比对功能，主要功能包含转入核验管理、转出核验管理、区内流转查询。

9、抽查管理

该模块主要用于对布控数据进行管理，在核放单审核模块被布控的核放单将流转至该模块，海关可在该模块对处置结果进行选择，放行的车辆可出入区，移交至其他部门的需人工放行。

10、预警管理

该模块主要用于对预警核放单进行处置，触发预警的核放单将从审核模块流转至当前模块。

11、风险参数

针对分类监管业务数据进行预警参数管理，该模块可对风险参数进行维护。

12、综合查询

提供分类监管核放单审核后的综合查询功能，所有申报、审核过的核放单可在此菜单查询。

13、统计分析

对系统的企业量、业务量、商品库存、单量、主要商品进行统计，供海关查看。

14、基础设置

该模块主要提供菜单管理、基础参数维护、场站通道号维护等功能，用于对监管端的系统参数进行配置。

15、系统对接

（1）H4A 对接

该系统监管端需要与海关 H4A 系统进行对接，获取用户及角色权限。

（2）智能卡口对接

该系统需要与空港综合保税区智能卡口系统进行对接，根据卡口返回车辆信息下发卡口抬杆指令。

分类监管辅助管理子系统-企业端

1、企业中心

该功能主要用于企业对企业基础信息进行登记，主要功能包含企业信息登记、企业信息查询。

2、商品中心

该模块主要用于企业进行区内流转业务时，对流转商品进行备案主要功能包含商品信息登记、商品信息查询。

3、分类监管资质登记

实现仓储企业、物流企业、加贸企业、经营企业等，向海关申请可开展业务类型资质的功能，企业可通过系统接收海关的审批结果，该模块主要功能包含资质登记、资质注销、资质查询。

4、分类监管账册备案

实现海关对特殊监管区域内开展业务企业的电子账册备案联网管理功能，主要功能包含账册备案、账册变更、账册查询。

5、分类监管核放单

该模块主要用于企业对分类监管类型物品的出入区核放单进行申请，主要功能包含核放单申请、作废申请、核放单查询。

6、分类监管库存管理

该模块主要用于企业进行库存的调整，海关审核通过后，调整成功，主要功能包含调整单申报、调整单查询。

7、区内流转管理

该模块主要用于企业进行货物区内流转，通过转入企业与转出企业的流转申请，进行库存的转移，海关审核通过后，转入转出企业账册自动核增核减。主要功能包含：转入申请管理、转入查询、转出申请管理、转出查询。

8、综合查询

提供分类监管核放单的审批进度综合查询功能，包含核放单查询、车辆查询。

9、统计分析

对系统的企业量、业务量、商品库存、主要商品进行统计，供园区管理员方查看。

10、基础设置

该模块主要提供菜单管理、参数管理功能，用于对企业端的菜单及系统参数进行配置。

分类监管辅助管理子系统-监管端

1、分类监管资质审核

该模块主要用于海关对仓储企业、物流企业、加贸企业、经营企业等提交的资质信息进行审核，主要功能包含资质登记初核、资质登记复核、资质注销初核、资质注销复核、资质登记管理、资质登记查询。

2、分类监管账册审核

该模块主要用于海关对仓储企业、物流企业、加贸企业、经营企业等企业提交的账册信息进行审批，账册生效后应根据各企业进出区申请自动核算，一种业务类型一家企业只能有一本账册，账册编号为唯一标识。主要功能包含账册初审、账册复审、账册查询。

3、核放单审核

该模块主要用于海关对企业提交的分类监管核放单进行审批，系统可根据设置的风险参数和自动审批开关，对核放单进行自动放行、布控查验、人工受理等操作，主要功能包含人工核验、核放单作废、人工过卡口、核放单查询。

4、分类监管账册管理

该模块主要用于海关查看分类监管业务的账册库存，账册根据核放单进行自动核增核减，海关可查看各类商品的账册核增核减明细。

5、分类监管库存管理

该模块主要用于海关审核企业提交的库存调整单，主要功能包含库存调整核验、库存调整查询。

6、区内流转审核

该模块主要用于同一业务场所两家不同企业之间的货物流转管理，实现转入企业转入申请单以及转出企业转出申请单审核、查询以及逻辑比对功能，主要功

能包含转入核验管理、转出核验管理、区内流转查询。

7、抽查管理

该模块主要用于对布控数据进行管理，在核放单审核模块被布控的核放单将流转至该模块。

8、预警管理

该模块主要用于对预警核放单进行处置，触发预警的核放单将从审核模块流转至当前模块。

9、风险参数

针对分类监管业务数据进行预警参数管理，该模块可对风险参数进行维护。

10、综合查询

提供分类监管核放单审核后的综合查询功能，所有申报、审核过的核放单可在此菜单查询海关审批进度、操作日志等信息。

11、统计分析

对系统的企业量、业务量、商品库存、单量、主要商品进行统计，供海关查看。

12、基础设置

该模块主要提供菜单管理、参数管理功能，用于对监管端的系统参数进行配置。

13、系统对接

（1）H4A 对接

该系统监管端需要与海关 H4A 系统进行对接，获取用户及角色权限。

（2）智能卡口对接

该系统需要与海口综合保税区智能卡口系统进行对接，根据卡口返回车辆信息下发卡口抬杆指令。

供应链金融服务系统

各功能模块定义

企业信息注册

企业信息注册园区内外贸中小微企业提供基本信息注册为系统用户。

企业信息验真

企业信息验真指平台自行抓取有关政府机构数据，对企业信息进行验真。

企业融资申请

企业融资申请是企业在线提交融资请求后，平台向银行等多方金融机构推送实时融资需求，进行撮合交易。

金融融资验真

银行或金融机构可以借助平台上政府部门信息的真实性和权威性，利用大数据为企业信用把脉，充分了解外贸中小微企业主体的经营状况，降低金融机构业务成本，减少由于信息不对称而导致的风险问题。

金融融资放款

金融融资放款是金融机构根据平台信息进行企业资质审核和风控评估后，审核通过即可放款。非银行金融机构利用其吸收的外汇资金或自筹外汇资金对自行审定的企业或项目发放的贷款。

金融融资还款

金融融资还款是企业融资还款后，在线提交融资还款结果，金融机构确认，完成融资业务单，直接偿还现有负债，包括融资负债和利息费用等。

数据统计公开

该模块主要用于统计系统的业务数据，主要统计类别包含融资量统计、申请量统计、放款量统计。

应收账款融资申请

该模块主要用于企业进行应收账款融资申请，通过上传应收账款记录。

应收账款融资审核

该模块主要用于管理方对应收账款融资申请进行审核，可填写相关审核意见。

订单融资申请

该模块主要用于企业进行订单融资申请，通过上传订单记录，填写订单详细

信息，申请订单融资。

订单融资审核

该模块主要用于管理方对订单融资申请进行审核，可填写相关审核意见，反馈企业，对于审核通过的企业，可进行后续放款操作。

库存融资申请

该模块主要用于企业进行库存融资申请，通过上传库存商品信息，填写库存数量等详细信息，申请库存融资。

库存融资审核

该模块主要用于管理方库存融资申请进行审核，可填写相关审核意见，反馈企业，对于审核通过的企业，可进行后续放款操作。

后台管理

该模块主要用于融资类型管理、风险预警管理、放款风险防控、还款期限预警，通过对融资类型、风险预警等参数设置，实现系统的预警及风险防控。

风控模型

该模块主要用于后台设置企业财务风控模型、放款风控模型、还款风控模型，通过不同算法对各类风控类型进行建模，实现风控。

银行数据接口

该模块主要用于对接银行，获取银行放款及还款数据，实现放款、还款数据核对，完成融资管理。

单一窗口数据接口

该模块主要用于对接单一窗口，获取货物舱单、报关单等企业进出口贸易数据，实现数据核碰，完成企业申请数据的可信度匹配。

融资租赁管理系统

各功能模块定义

首页

1．平台介绍

阐述该融资租赁平台的产品定位、核心价值、核心业务、行业背景及平台功能、平台类型。

2．企业准入要求

对于需要进行融资租赁业务的企业，进行企业准入要求规则说明和限制条件说明。

资讯发布

1、政策法规

通过收集国家部委、省市、行业官网等融资租赁相关政策法规，及时发布至系统后台，推送至资讯发布前台，使得有业务需求的企业及租赁企业员工学习了解行业资讯。

2、融资产品介绍

对于融资租赁相关产品信息通过资讯发布后台进行维护，推送至资讯发布前台，为企业查阅、获取产品信息提供精准、便捷的介绍说明，

3、新闻资讯

通过对各大新闻资讯平台有关融资租赁行业新闻的收集整理，展示至资讯发布前台

企业服务

1、企业注册

企业客户通过企业注册申请前台进行企业注册，。

2、企业资质

业务人员收集承租企业拥有的相关行业资质证书正副本复印件，并上传图片、文件至系统中。

3 企业融资申请

企业注册完成后进行企业融资申请填写承租企业需要的固定资产设备，型号、

同时选择需要进行融资租赁业务的类型，融资金额填写完成后进行租赁公司内部申请审批审批。

4、 企业还款

企业根据实际租金支付表要求，在指定的还款日期进行款项归还，归还至融资租赁公司在银行的指定账户。

5、逾期提醒

对承租人企业的合同执行情况、项目的进展情况和经营情况进行跟踪调查，提醒借款人及时筹备资金按时还本付息，对逾期贷款本息进行催收工作。

6、欠款追回

通过银行系统监管承租人账户，若对方账户有资金流入，立即进行清偿请求。申请保险公司进行保险赔付从而追回欠款。

保险服务

1、企业注册

通过接口对接形式，将承租人企业企业注册信息，推送至保险系统进行承租人企业注册、判断是否保险机构“黑白名单客户，进行业务开展初期筛选”

2、信用融资审核

对接保险系统，进行保险机构对于承租人企业提供的信息进行信用融资审核。

3、保单管理

对接保险系统，融资租赁业务开展至合同签订时，与保险机构签订保险合同、包括合同内容、赔付情况说明、可赔付的金额范围，可赔付的情况描述。

4、保险赔付

保险机构根据实际业务情况，包括租赁设备损坏、承租人企业未还款情况进行保险赔付确认，同时推送保险赔付相关信息至融资租赁系统后台。

5、欠款追回

通过银行系统监管承租人账户，若对方账户有资金流入，立即进行清偿请求。申请保险公司进行保险赔付从而追回欠款。

银行服务

1、企业注册

通过接口对接形式，将承租人企业在融资租赁管理系统进行企业注册的信息，

推送至银行系统进行承租人企业注册、判断是否银行“黑白名单客户，进行业务开展初期筛选。

2、银行授信

对接银行系统，进行银行授信生成风控信用评分，同时推送至银行进行授信额度审批并提供银行可授信的确认额度。

3、贷款发放

租赁企业落实企业放款前提条件，推送信息至银行，银行进行款项支付至租赁设备供应商指定账户。

4、企业逾期

未按照实际租金支付表进行款项支付的承租企业，进行企业逾期记录，包括：实际还款时间、逾期时间、逾期本金、逾期利息、逾期天数。

5、补贴管理

融资租赁企业依据租赁设备优惠政策补贴为承租人企业进行政策补贴申请，推送数据至相应政策补贴审核平台，审核通过后，推送审核信息至银行系统银行进行补贴款项发放至承租人企业账户，

6、欠款追回

通过银行系统监管承租人账户，若对方账户有资金流入，立即进行清偿请求。申请保险公司进行保险赔付从而追回欠款。

资金管理

1、补贴审批

融资租赁企业依据租赁设备优惠政策补贴为承租人企业进行政策补贴申请，推送数据至相应政策补贴审核平台。

2、补贴发放

补贴审批通过后，推送审核信息至银行系统银行进行补贴款项发放至承租人企业账户。

3、追还欠款返还

对于企业逾期中含有未归还的贷款金额进行追偿、追偿后及时归还至银行资方。

4、银行资质管理

对于提供资金的银行方进行管理，包括银行名称、机构、所属地区、可提供

的业务类型，合作期限等

5、产品管理

对于融资租赁企业可进行的租赁产品进行设置包括：直租、回租、经营性租赁等多种业务模式的设置。

统计分析

1、贷款规模统计

根据市场融资租赁申请规模对比该融资租赁企业业务规模情况：统计企业的贷款情况统计包括：现有市场规模占比、当地市场规模占比情况，各行业融资租赁占比等。

2、贷款发放统计

统计累计贷款金额的发放统包括：贷款年度、季度、月度、本周发放金额的统计。

3、贷款回收统计

累计贷款回款金额情况统计、包括：贷款年度、季度、月度、本周回款金额的统计。

4、企业逾期统计

累计企业逾期金额情况统计、包括：逾期年度、季度、月度、本周逾期情况、逾期金额、逾期时长。

5、贷款企业统计

贷款企业个数、租赁企业申请个数、承租人企业类别、承租人企业分布情况等对贷款规模进行统计。

免税交通工具管理系统

各功能模块定义

清单管理

1、综保区备案

提供综保区基础信息备案功能，备案完成后代理企业可对应选择保税区。

2、检测线备案

安全检测监管场所设为场所，并设立场所代码，提供检测线基础信息备案功

能，备案完成后代理企业可对应选择检测线。

3、收发货人备案

针对有进口免税交通工具进出口资质的企业综合管理，包含资质的认定、审批、开展业务许可等方面的管理功能。

4、交通工具清单

提供交通工具清单录入功能。

通关管理

1、通关管理

根据免税交通工具实际进境口岸，制定通关流程。同时完成报关单证（报关单、核放单等）申报功能。与海关辅助系统对接，实现卡口的自动抬杠。

2、集装箱调拨

通过铁路/船舶运输的进口交通工具到达铁路/水运口岸后，企业通过系统向口岸主管海关发起集装箱调拨，申请一体化核放单，核放单放行后，由企业将整车/飞机/船舶集装箱自行运输至安全检测监管场所。

3、一体化核放单

开展保税仓储的一般贸易进口车辆/其他交通工具，由仓储企业在系统中发起集装箱调拨，申请入区核放单，经主管海关审核通过后，通过一体化系统发送至整车系统，由企业将整车集装箱自行运输至综保区（中心）进行保税仓储。

4、空箱出场

集装箱卸货后可通过系统向主管海关申请空箱出场申请，申请通过后，由运输企业将空箱运输出场。

5、退运申请

整车/飞机/船舶检测不通过，需由代理企业向主管海关发起退运申请，将交通工具退运至境外。

6、底账管理

针对进口免税交通工具建立数据底账，高效记录免税交通工具的进出转存，如交通工具进场时间、拆箱申请时间、海关审核时间、检测时间以及提车时间等，确保流程可追溯。

7、报关单比对

企业申报整车车辆/其他交通工具清单，与转关申报单、报关单比对后形成

物流底账。

8、交通工具放行管理

检验合格的交通工具或可以进行整改的交通工具入指定场地进行保税仓储，由代理企业向主管海关发起放行出场申请，海关审核通过后交通工具放行出场，系统记录申请时间和出场时间等。

物流作业

1、卸场作业

集装箱进场后，企业发起拆箱申请，海关审批通过后，在检测线场站进行拆箱作业，企业发起申请后，海关可进行指定地点进行查看；

2、在场作业

拆箱作业完成后，进行贴标、理货、安全检测等作业，并在指定场所进行信息登记，以及安全检测等流程。

3、提货管理

检测报告合格以及报关单放行后企业可申请提货，在海关审批通过后可提车出场/通关手续齐全，可放行。

检测作业

1、上线检测

交通工具入区后，综保区（中心）主管海关对交通工具开展一般项目检疫、安全基本项目检疫，对检疫不符合要求且无法整改的交通工具作退运或销毁处理；检验合格的交通工具或可以进行整改的交通工具入指定场地进行保税仓储。

2、检测报告

对销售免税交通工具进行质量检测，并根据检测结果记录其质检报告，质检报告支持下载和导出。系统实现“一品一侧”的同时建立其对应检测管理体系。

电子地图

1、可视化管理

依托成熟的 GIS、移动互联网和三维等技术，建设形成统一的业务展示系统，将所有飞机、船舶、整车等交通工具在地图上进行二维和三维展示，让管理人员更快捷方便的查看和管理。

2、在场交通工具查询

为监管单位提供可视化的查询展示界面，直观展示现有综保区数量、检测场地数量，运往综保区、检测线交通工具数量、送检合格数量、送检不合格数量、退运数量等。

统计查询

1、通关物流查询

提供车辆、船舶、飞机等交通工具的通关物流查询，可按照按区域、按状态、按贸易方式、以及按经营单位等统计。

2、业务情况统计

提供业务情况查询统计功能，可交通工具生命周期履历查询统计，展示现有综保区数量、检测场地数量，运往综保区、检测线交通工具数量、送检合格数量、送检不合格数量、退运数量等。

3、在场检测统计

提供在场车辆/其他交通工具的检测情况，即送检交通工具数量、送检合格数量、送检不合格数量以及退运数量等。

冷链协同管理系统

各功能模块定义

信息登记

提供进口货物相关的信息登记功能，包含企业信息登记、消杀报告登记、运输车辆登记等相关功能。

货物监管

实现海关等口岸部门对进口货物监管的通关环节的消杀及货物检验环节的抽样、采样以及全程流转跟踪管理的全程监管，系统实现进口货物的口岸消杀，防止逃检和漏消、流转，主要包含货物进出申请、货物进出审批、货物流转跟踪。

风险预警

风险预警管理子系统实现货物监管风险预警的智能化管理，建立动态风险评估模型，系统自动评估货物业务情况，在严格监管的前提下，加快企业物流速度，为企业节约成本，创造效益。建立基于疫情风险等级管理，实现按货物来源国、

途径国、接触人员、消杀情况建立相关风险预警管理，主要包含预警参数、预警规则设定。

运输管理

运输管理通过对车辆运输人员的信息登记，运输路线登记，确保运输人员新冠检测，运输途径地管理，主要包含司机信息登记、运输路线登记。

库存管理

库存管理子系统通过出入库时选择对应进口报关单实现关联比对，在分批出库时，分批核销进口货物信息，系统可以追溯每批出库货物信息的进口信息及余量信息，实现关联报关单货物的分批核销，主要包含出入库记录、库存量查询。

销售溯源管理

销售溯源是对货物在销售环节流转备案的核心系统，通过建立销售台账、销售记录等添加销售环节的溯源信息，形成进境环节到销售环节的闭环管理，主要包含货物进出区记录、货物采购方记录。

货物流向管理

根据进口货物入境的运输方式，货主/货代及时向口岸监管部门申报货物最终流向信息。

溯源移动应用

溯源移动应用提供移动端业务登记、提货预约、提货完成、溯源码打印一系列操作流程，主要包含信息登记、提货预约、溯源打印、溯源查询。

数据分析管理

平台备案登记信息，对各地市货物存量增量及轨迹信息进行统计分析，对流入我货物分布、组成、体量进行综合分析，为掌握货物市场流通情况提供数据支撑，对同批次检测呈阳性国家货物流入分布情况进行研判分析，主要包含消杀记录统计、货物流向统计、综合数据分析。

各功能模块定义

企业信息管理

该模块主要用于登记企业基本信息，并提供查询。

电商账册管理

开展保税进出区业务时，需提前进行物流账册的建立，通过进出区操作实现对物流账册的核销。

保税进口清单管理

1、邮寄清单管理

该模块主要用于显示通过接口传输的跨境邮寄清单数据。

2、自提清单管理

该模块主要用于显示通过接口传输的跨境自提清单数据。

保税进口报关管理

1、邮寄核注清单申报

该模块主要用于申报跨境邮寄业务核注清单。

2、自提核注清单申报

该模块主要用于企业查看自动申报的核注清单数据。

物流管理

1、邮寄核放单申报

该模块主要用于企业申报跨境邮寄核放单。

2、自提核放单申报

该模块主要用于企业查看跨境自提核放单。

综合查询

1、清单查询

该模块主要用于查询清单，并生成溯源二维码，提供二维码接口及闸机放行接口供企业系统调用。

2、核注清单查询

该模块主要用于企业查询核注清单，主要查询条件包含清单编号、电商清单编号、数据状态、录入日期等。

3、核放单查询

该模块主要用于企业查询核放单、重发卡口报文。

系统设置

1、用户管理

该模块主要用于管理系统用户，可通过企业名称查询企业用户信息，并通过勾选角色，赋予用户权限。

2、角色管理

该模块主要用于创建角色权限，可新增不同角色，对角色可见菜单及数据进行配置，通过该模块对系统权限进行设置。

3、菜单管理

该模块主要用于新增菜单，对菜单的名称、排序、链接、下级菜单等信息进行维护，可对菜单进行隐藏或显示设置。

客户端设置

该模块主要用于设置客户端的收发路径，用户在 PC 端对客户端创建收发路径后，可在该模块对回执路径、报文发送路径进行配置，配置成功后可进行核注清单、核放单申报。

客户端

客户端主要用于传输核注清单、核放单、卡口过卡报文，接收海关返回的报文回执，企业需要安装客户端后进行相关单证的申报及回执查看，主要包含基础配置管理、监控服务管理、数据落地管理、申报异常管理、资源监控管理。

系统对接

1、溯源码接口

系统提供二维码接口供企业系统调用，企业可内部生成，简化贴码流程。

2、闸机放行接口

该二维码可根据核注清单、核放单申报状态改变显示内容，提供放行接口供

闸机调用，顾客出园区时可在闸机扫该二维码出区。

3、金二对接

该模块主要用于与海关金二系统进行对接，传输核注清单、核放单的报文信息，并通过该接口接收海关返回的回执信息。

4、卡口对接

该模块通过与卡口对接，实现虚拟报文的传输，通过核放单报文信息，获取卡口虚拟报文内容进行填充，经过该接口传输卡口 X81 报文，实现虚拟过卡。

溯源采集管理系统

各功能模块定义

货物信息管理

1、运抵确认

针对口岸环节的进口货物货主代理企业进行基本信息填报，方便后续信息溯源。

2、消杀登记

货物货主代理企业根据运抵确认的货物相关信息进行口岸环节消杀信息登记。

3、核酸登记

货物货主代理企业根据运抵确认的货物相关信息进行口岸环节核酸检测登记。

风险预警管理

1、应急处置

展示各环节未消杀信息和各环节未核酸信息。

2、异常预警

异常类型包含人员异常、货物异常、运输工具异常、场所异常。

3、预警管理

分为疫区国预警和目的地预警。

运输及库存管理

1、入库确认

进境货物信息运抵确认完成后，进行货物去向确认，精准记录各个节点的信息。

2、货物流出

交接给销售使用单位时，在货物流出模块登记流出信息，可将库存货物信息流转至销售使用环节。

3、出库转运

用于出库转运时，在出库转运模块登记流出信息，可将库存货物信息流转至销售使用环节。

4、自用耗损

产生货物损耗时，可在本模块进行登记。

5、信息补录

对企业存量货物或外省报关运输至本企业的货物于此页面进行信息登记。

销售溯源

1、销售入库

销售企业接收到货物后，在本模块登记入库入库件数、入库净重等信息，并根据实际的消杀、核酸检测情况登记对应的消杀记录和核酸检测报告。

2、销售流通

进境货物完成口岸通关、交通运输、贮存转运环节后，进行的货物销售去向登记，精准记录各个节点的信息。根据不同的出库件数、出库重量及收货方信息录入数据。

3、损耗报备

货物销售耗损至此模块进行货物信息报备。

4、信息补录

对企业存量货物或外省报关运输至本企业的货物进行信息登记。

信息登记管理

1、备案管理

对企业、车辆、监管场所、场所、人员信息进行备案，展示企业已备案的信

息。

2、备案审核

所有企业信息提交后同步展示在备案管理模块，初始备案信息直接同步至备案管理。

货物流向管理

1、提货预约

进行口岸通关环节的提货，填写流通信息后，按照口岸填报信息、消杀信息、核酸信息加上流通信息更新溯源码。

2、提货完成

提货预约信息填写完成后，数据流转至提货完成页面，需在页面进行提货完成确认操作更新溯源码流通信息。

数据分析

1、提货量统计分析

该页面以口岸环节的车牌数量统计，对应的统计区域为各监管场所，时间按照已提货完成时间年月分组。

2、放码量统计分析

该页面按照已提货完成的分运单数量对应的各初始溯源码，统计区域为各监管场所，已提货完成时间的年月分组。

3、消杀量统计分析

该页面统计口岸环节已消杀记录，及对应的各监管场所，按照货物运抵确认时间年月分组。

4、进境口岸统计分析

该页面统计货物监管-运抵确认环节的记录的进境口岸，对应提(运)单号，以到货确认时间年月分组。

5、货物类型统计分析

该页面统计货物监管-运抵确认环节的记录的货物类型，以提(运)单号记录，以到货确认时间年月分组。

6、目的地统计分析

该页面统计口岸环节分运单对应的省市区统计，以提货完成时间查询。

溯源移动应用

1、个人中心

用户未登录显示为游客，不显示所属企业信息，无法点击具体系统信息，提示用户注册登录。

2、注册登录

用户首次访问系统，需先填写注册资料，输入用户账号（手机号）、密码、确认密码以及短信验证码，完成注册。

3、信息登记

货主代理企业、监管场所、消杀单位、核酸检测机构、仓储企业、物流企业进行企业备案和备案查询，审核端对企业信息进行审核。

4、货物管理

登记运抵确认信息、消杀信息、核酸检测报告、人员健康码等信息，方便后续信息溯源。

5、货物流向

根据进口货物基本信息、消杀登记、核酸登记、业务人员健康码信息申报，形成口岸环节信息，按照货物流转轨迹进行交通运输环节提货预约。

6、运输库存

运输库存管理分为入库确认、出库转运、货物流出、接收确认、耗损报备。

7、销售溯源

销售溯源分为：销售入库、销售流通、货物流出、接收确认、自用报备等模块。

8、溯源码

溯源码一码通行，可从口岸环节到最后的销售流通环节，货物的每一个流通环节，都使用溯源码将货物流转信息串联成唯一追溯链条。用户可扫码查询溯源信息。

辅助监管业务服务平台

智能场站管理系统

各功能模块定义

货运管理子系统

货运管理子系统是整个系统的业务核心，主要包括计划受理、资料管理、作业管理、集装箱装卸作业、业务查询等子模块；货运管理主要完成要车计划编制、货运计划编制、发送与交付管理，并管理与货物有关的发送作业、装卸作业、到达作业、安全作业、集装箱作业、篷布作业等货运组织工作，对货运装卸工作、计划指挥、货物内勤、货物外勤进行统计分析等。主要功能包含集装箱装卸作业、装卸作业跟踪、现车管理、货运计划管理、作业管理。

预确报管理子系统

主要是对车辆抵达、离开场站的预报、确报信息进行管理，需要与前后站进行数据互通，对车辆运行状态进行自动预判和处理，主要包含车辆抵达预报、车辆抵达确保、车辆离场预报、车辆离场确保。

换装管理子系统

完成对换装计划编制、对换轮作业进行监控及信息的录入，对轮对履历进行管理、对换装清单进行管理，主要包含换装计划编制、换轮作业监控、换装清单管理。

堆场管理子系统

堆场管理是为了集装箱顺利装车，充分利用堆场容量，减少翻箱率，根据按贝位箱区的堆放方法，考虑集装箱的提运作业和转堆作业，力求减少各种堆场作业的相互影响，能在最短时间内完成装车工作，主要包含落箱单打印、落箱确认、移箱管理、提箱单打印、提箱确认。

堆场终端应用子系统

主要为堆场的现场理货、作业机械、堆场现场人员等提供实时移动信息化数据处理手段，主要包括：收箱确认、发箱确认、移箱确认、装车确认、卸车确认

等。

仓库管理子系统

主要为场站仓库提供全面的业务管理，包括货物进出管理、暂存仓储管理、理货管理、普货单证管理、普货底账管理、暂不放行货物管理、风险预警。

费收管理子系统

场站财务人员在费用结算部分可以设置费用标准、为单独企业设置费用、按照货物运输业务类型分别进行费用设置，并且根据场站的各项操作自动计算每家企业需要缴纳的场站费，在实际收取后可在系统中设置结费操作，并打印相关的财务报表。主要功能包含标准费用设置、协议企业费用设置、费用清单管理、月结账单管理。

场站可视化管理子系统

结合 GIS 技术，对整个场站提供可视化的货物查询功能，以图形化手段对货物库存信息进行监控与管理。

1、库场管理

主要是完成集装箱场、散装货物场、成件货物场等场地规划、运用计划，实时监控应用状况，并根据具体情况，调整计划，并下发给现场作业人员。

2、可视化作业监控

主要是图形化手段对作业进行监控管理，主要功能包括堆场监控、货场监控及仓库监控，为堆场企业提供可以同时管理多个不同堆场与仓库的信息化管理平台。

综合查询子统计

1、集装箱统计

根据进口拆箱作业、出口拼箱作业统计每年不同月份的进口集装箱数量和出口集装箱数量，默认统计当前年份每月的进出口集装箱数量，也可选择进口和出口以及不同年份分别统计。

2、进口货物统计

以报关单+提单为最小单位，根据时间条件和企业名称统计查询场所每月入库、出库和库存的重量、件数、体积。

3、出口货物统计

以批次号为最小单位计算，根据时间条件和企业名称统计查询场所每月入库、出库和库存的重量、件数、体积。

多式联运服务系统

各功能模块定义

委托书管理子系统

该系统主要用于各类企业进行不同委托信息委托及审核，面向非货代公司、货代公司及业务销售人员。非货代公司可以通过在平台注册获取登录权限后，通过委托书管理系统的委托单申报模块，进行不同类型委托业务的委托申报。企业可以选择货代公司，将本公司的货物信息以委托单方式提交给指定的货代公司，待货代公司审核通过后，将货物配送给货代公司代为处理；货代公司可以结合接单的委托单数据，主要包含委托单填报、委托单审核、制单、委托单查询、物流跟踪。

订舱管理子系统

该系统主要用于订舱申报及审核，设计业务为铁路订舱与海铁联运订舱。系统主要服务对象为货代公司、业务人员、舱位管理人员，业务人员通过结合订舱委托书信息（已完成审核的）进行舱位申请，由舱位管理员进行审核，审核通过并安排舱位后，通知相关人员进行线下舱位确认，并由舱位管理人员对确认的舱位进行线上记录操作等。订舱成功（即舱位已确认）之后，数据进入订舱管理模块，接下来业务销售人员可在此提交报关申请。主要包含订舱申请、订舱审核、订舱查询功能。

单据管理子系统

主要用于管理运费补贴申请及审计中所需的各类单据，用户对象主要是报关人员、运费补贴审核人员、审计人员、委托企业等。主要包含补贴申请、补贴审核、补贴参数维护、审计资料上传、审计资料比对、单据信息查询。

集装箱管理子系统

主要用于管理集装箱，主要实现境内集装箱运踪查询、运费查询功能；实现

对陆港自有集装箱进行箱务管理，包括但不限于备箱、租赁、调运、保管、交接、发放等管理功能；系统预留集装箱 GPS 定位系统接口。主要包含用箱申请、用箱审核、放箱审核、费用统计、还箱申请、验箱审核、综合查询。

8、集装箱管理

该模块主要用于对集装箱进行管理，通过记录集装箱的编号、大小、体积等信息，对集装箱进行归档管理，便于后续对集装箱的收费及调度进行联动管理。

9、集装箱调度

该模块主要用于集装箱调度，通过查询集装箱的装载状态，对集装箱进行调度。

10、GPS 信息管理

该模块主要用于管理集装箱的 GPS 信息，通过对接 GPS 硬件定位模块，获取集装箱的定位信息，从而对集装箱的位置进行更新。

11、数据统计分析

该模块主要用于系统进行数据统计分析，可对集装箱的使用率、空置率、常用定位、装载货物等数据进行分析，便于集装箱的运营管理。

用户管理子系统

该系统主要对整个平台的用户进行集中管理，管理内容包括需要使用系统的相关用户的详细信息、秘钥，以及用户角色的设定、角色权限的设置等管理，另外支持对用户的统计分析。主要包含权限管理、角色管理、用户管理。

园区跨境电商服务系统

各功能模块定义

事前备案

1、企业中心

用于电商企业、电商平台企业、物流企业、支付企业、仓储企业、报关行等企业用户在企业端录入企业信息并向海关提出企业信息备案、变更、注销等申请，系统进行基础数据校验。

2、商品中心

通过该功能，企业用户可录入将要开展跨境业务的商品信息，并提出企业信息备案、变更、注销等申请，系统进行基础数据校验。

3、海外仓报备

该模块主要用于开展 9810 出口海外仓业务的企业对开展业务的海外仓进行登记报备，主要用于后续业务申报填充信息。

账册管理

建立料号级电子账册，管理保税进出口跨境货物。根据入区、出区单证进行账册货物库存的核增、核减，实现库存管理。主要包含账册备案、账册查询。

计划管理

物流企业将直邮进口、一般出口进出库业务计划，提前向场站管理系统申报进出库计划，该模块主要包含了进口到货计划管理、出口到货计划、进口出库计划、出口出库计划。

交易单据管理

三单数据查询：对企业提供订单、运单、支付单/收款单三单数据查询功能。同海南省单一窗口跨境综服平台对接，传输三单数据，数据本地留存。

入库明细单查询：对企业提供入库明细单查询功能。同海南省单一窗口跨境综服平台对接，接收入库明细单数据回执，数据本地留存。

B2C业务

1、直购进口

直购进口模块将订单、支付、物流数据实时传送给省公服平台，境外商品通过邮件、快件等物流运输方式进口至跨境电商专门的监管场所。

2、一般出口

一般出口模块将订单、收款单、物流数据实时传送给省公服平台，境内商品通过邮件、快件等物流运输方式出口至跨境电商专门的监管场所。

3、网购保税进口

网购保税进口是一种“先备货后接单”的模式，国外商品整批抵达国内监管场所和保税监管场所，消费者下单后商品从保税区直接发出，在监管部门的监管下实现快速通关。

4、特殊区域出口

特殊区域出口模块将订单、收款单、物流数据实时传送给省公服平台，境内商品通过邮件、快件等物流运输方式出口至跨境电商专门的监管场所。

B2B业务

1、直接出口

B2B 业务主要是直接出口、出口海外仓，开展跨境电子商务直接出口业务的电商企业、物流企业、代理企业在该模块下，按照不同身份类型对订单、运单、收款单、清单等数据进行申报。

2、出口海外仓

B2B 业务主要是直接出口、出口海外仓，开展跨境电子商务出口海外仓业务的电商企业、物流企业、代理企业在该模块下，按照不同身份类型对订单、运单、收款单、清单等数据进行申报。

查询统计

1、进口数据管理

该模块主要用于对进口业务的各类单据进行查询统计，包含进口的订单查询、运单查询、支付单查询、清单查询、入库明细单查询等。

2、出口数据管理

该模块主要用于对出口业务的各类单据进行查询统计，可查询所有单证信息以及状态统计，可进行清单查询、订单查询、支付单查询、运单查询、运单状态查询、运抵报告查询等。

免税品辅助管理系统

各功能模块定义

企业端

1、企业中心

（1）个人资料

个人资料模块中可修改企业的营业执照信息。

（2）企业信息查询

用于企业信息查询。

2、账册备案

（1）账册备案

该模块用于企业进行账册备案，账册审核通过后即可开展区内免税品业务。

（2）账册变更

该模块用于企业发起账册变更申请，企业对账册中的仓库信息进行修改，账册变更后需要申报至监管端审核。

3、免税品核放单

（1）核放单申报

核放单申报模块主要用于系统核放单的新增、申报、删除、编辑等。

（2）核放单作废

该模块主要用于核放单的作废，选中需要作废的核放单，点击作废后数据传至监管端通过作废或不通过作废生成回执至企业端。

（3）核放单查询

该模块提供查询、重置、刷新等操作，根据核放单编号、账号编号、出入区类型、车牌号、创建时间等筛选项对各类核放单的数据进行查询。

4、账册管理

（1）账册查询

该模块主要用于查询企业的账册信息，系统根据同步后的准单信息进行账册库存的核增、核减，实现账册管理，企业通过账册查询模块可查询出本企业的库存信息。

5、入库准单绑定

（1）入库准单绑定

入库准单绑定该模块自动录入核放单信息，该模块提供查看、绑定入库准单、日志、同步数据、查询、重置等操作。

6、账册调整

（1）调整单申报

用户可在该模块对账册进行库存调整，填写库存调整单提交至监管端审核通过后，账册库存变更。

（2）调整单查询

该模块提供查询、重置、刷新等操作，根据核放单编号、账号编号、主管海

关、仓储企业名称、创建时间等条件进行查询。

7、核注清单

（1）核注清单申报（进口）

该模块主要用于区内免税品转保税品业务报关使用，用户可在该模块填写核注清单进行申报，通过单一窗口客户端，将报文传输至金二。

（2）核注清单申报（出口）

该模块主要用于区内保税品转免税品业务报关使用，用户可在该模块填写核注清单进行申报，通过单一窗口客户端，将报文传输至金二。

（3）核注清单变更

该模块对于发起核放单变更的数据时需给出提示，是否进行变更，如果变更，当前数据自动变为变更类型。

（4）核注清单删除

该模块发起删除申请的数据，申报后，数据类型即为删除。

（5）核注清单核查

核注清单核查页面该模块提供通过、退回、查询、重置、日志、查看功能。

（6）核注清单查询

该模块主要用于查询区内保税转免税、区内免税转保税业务数据使用，用户可在该模块查看核注清单详情信息。

8、综合查询

（1）免税品核放单查询

该模块仅提供免税品的核放单查询。

（2）核注清单查询

该模块主要用于查询区内保税转免税、区内免税转保税业务数据使用，用户可在该模块查看核注清单详情信息。

（3）核放单查询

该模块提供保税核放单查询。

9、统计分析

（1）企业统计

企业统计该菜单统计企业进区与出区数据总和。该模块提供导出、查询、重置功能。

（2）业务统计

该模块按照业务类型对进区、出区单量进行统计，查询条件为（创建时间、企业名称）。

（3）商品库存统计

该模块按照商品编码统计所有商品现有库存数，可以按照企业名称、业务类型、主管关区进行统计，导出时将页面的查询结果全部导出。

（4）主要商品统计

该模块主要统计主管关区下各类业务的主要商品类型，统计商品的前十进行显示。

监管端

1、企业信息

用于查询各企业的企业信息，可查询企业基本信息如：企业名称、主管海关、企业海关编码、统一社会信用代码等。

2、账册备案

（1）账册审核

在该模块对企业申报的账册备案信息进行审核，海关可对账册进行通过、不通过操作，审核意见为不通过的企业可根据不通过意见进行修改后，再次进行申报。

（2）账册（备案）查询

该模块提供查看、日志、重置、查询、刷新等操作，根据账册编号、主管海关、企业名称、创建时间等筛选项根据不同的查询条件对各类账册的数据进行查询定位。

3、账册管理

账册查询页面主要用于海关人员对企业的账册库存进行查询。

4、调整单管理

（1）调整单审核

在该模块对企业在企业端填写的库存调整单进行审核，审核通过后，账册库存可变更。

（2）调整单查询

该模块主要用于查询企业需要的调整单。

5、免税品核放单

（1）人工审核

该模块主要用于审核企业申报的核放单，审核不通过的核放单直接退单，审核状态显示为退单，企业可进行再次申报核放单。

（2）作废审核

作废审核页面主要用于核放单作废申请，可进行通过、不通过操作，不通过需要填写不通过的原因。核放单作废成功不可进行恢复。

（3）人工过卡

人工过卡页面主要用于核放单人工过卡，对过卡异常情况可进行人工过卡，海关人员可根据查询条件对需要过卡的数据进行查询。

（4）核放单查询

该模块提供核放单查询。

6、预警管理

（1）核放单预警处置

核放单预警处置页面点击查询根据用户实际输入的查询条件，显示符合条件的信息进行处置。

（2）核放单预警查询

该页面用于查看核放单的预警数据。系统提供功能有查看、日志、查询、重置等操作。点击查看系统跳转至准单信息详情页面。

7、查验管理

（1）核放单抽查处置

该模块主要用于处置核放单，状态为抽查的核放单对其处置处理。点击处置，弹出处置信息录入。

（2）核放单处置查询

该模块主要用于查询处置后的核放单数据，列表数据筛选功能分为核放单编号、账册编号、出入区类型、车牌号等。查询的处置结果为放行或退单。

8、风险参数

（1）预警参数

预警参数模块主要用于设置预警参数，可根据各关区设置预警参数。

（2）布控参数

该模块主要用于设置布控参数，可根据各关区设置抽查率。

（3）审单参数

该模块主要用于设置审单参数，可针对不同关区设置自动审单及转人工审单率。

9、统计分析

（1）企业统计

企业统计该菜单统计企业进区与出区数据总和。该模块提供查询、重置功能。查询条件为。

（2）业务统计

该模块按照业务类型对进区、出区单量进行统计，查询条件为。

（3）单量统计

该模块按照业务类型对进区、出区单量进行统计，查询条件为。

（4）主要商品统计

该模块主要统计主管关区下各类业务的主要商品类型，统计商品的前十进行显示。

（5）商品库存统计

该模块按照商品编码统计所有商品现有库存数，可以按照企业名称、业务类型、主管关区进行统计，导出时将页面的查询结果全部导出。

10、综合查询

（1）免税品核放单查询

免税品核放单查询模块用于查询免税品核放单。

（2）核放单处置查询

核放单处置查询该模块主要用于海关人员对核放单处置情况进行查询，可通过不同查询条件筛选。

11、基础设置

（1）基础参数

该模块主要提供查询、新增、导入、删除功能。根据用户实际输入的查询条件，以列表显示符合条件的记录信息。

（2）角色管理

在角色管理页面用户勾选需要授权的角色进行授权后，系统判断选择的数据若能够授权的情况下提示授权成功。

（3）用户管理

在用户管理页面设置新增、删除、查询、重置、编辑、删除功能。点击新增

后弹出新增页面，可直接新增监管端用户并赋予角色。

（4）菜单管理

在该页面中用户若主要添加下级记录，点击添加下级后，系统判断选择的信息是否允许添加下级添加成功修改记录状态，并提示添加下级添加不成功则异常提示。

系统对接

1、H4A 对接

该系统监管端需要与海关 H4A 系统进行对接，获取用户及角色权限。

2、智能卡口对接

该系统需要与智能卡口系统进行对接，根据卡口返回车辆信息下发卡口抬杆指令。

3、大数据局报关单对接

该系统需要与大数据局开放的海关系统数据接口进行对接，获取报关单数据，进行出入区核碰。

4、装卸监控设备对接

该系统需要与监管仓卸货月台监控设备进行对接，获取车辆到达卸货月台时间数据，进行准单录入判断。

应用支撑平台

统一用户/权限管理系统

各功能模块定义

登录管理

所有用户都可以访问登录首页，登录管理模块包括登录、注册、忘记密码功能。

区域管理

区域功能用于维护权限平台控制的所有地区，用户可维护地区名称、代码和是否有效的状态。维护完成后用于分配不同地区的功能权限，主要包含地区维护、区域权限。

菜单管理

菜单功能可管理所有功能菜单，用户可查看和修改功能次序、页面是否展示等主要包含功能菜单管理、子系统菜单管理。

数据管理

数据管理可维护不同区域的所能用的不同业务数据库，分配后的区域业务数据都将保存在所属的数据库中，数据可进行分类、分时查看主要包含业务数据库维护、业务数据库管理。

企业管理

企业管理用于维护区域所有企业信息，可新增、修改、删除、查看企业信息，主要包含企业信息维护、企业授权、企业状态维护。

部门管理

部门管理可对同一企业设置不同的业务部门，可新增、修改、删除、查看部门信息，主要包含新增部门、删除部门。

角色管理

角色管理是为了解决维护用户较多时耗时的问题，对权限表中的记录进行分组，将相关的一些权限分配为同一角色，主要包含角色维护、角色权限管理。

用户管理

用户管理可创建系统登录账号，用户可新增、修改、删除、查看、禁用、启用用户账号，主要包含用户信息管理、用户权限设置。

信息查询

登录用户可以通过点击页面左侧的目录树，查看系统中的人员信息。目录树按部门的隶属关系和级别展开，点击某个部门节点，在右侧列出该部门的人员列表，系统管理员可以设置人员列表里显示的信息条目，主要包含用户查询、角色查询、子系统查询。

数据交换系统

各功能模块定义

系统仪表盘

在系统仪表盘中查看到当前接收数据数量、发送数据数量、接收数据容量、发送数据容量、当前数据监控、流量监控以及系统占用监控。

用户管理

1、用户管理

用户在系统中指能操作该系统的人员所拥有的用户名和所设置的密码，用户名设置不做限制，系统只保证所设置的用户名全局唯一。

2、角色管理

管理可对拥有相似权限的用户进行分类管理，例如系统管理员、管理员、用户、访客等角色。可以编辑角色信息、搜索分配用户、配置权限功能。

3、组织机构

组织机构管理主要提供对系统中的组织部门的信息进行维护。

4、功能权限

管理员可在功能权限模块中维护管理系统全部功能权限树，定义功能名称，功能编码、功能地址等信息。

系统管理

1、基本信息管理

系统管理员可以对本系统的版本信息、名称信息和系统唯一标识信息做管理维护。主要功能包含添加、删除、修改、查询。

2、配置模板管理

对当前配置模板进行添加、查询、删除、修改操作。

3、系统参数管理

系统参数指的是本系统运行过程中所必备的参数信息，参数主要分为两大类：一类为开关类参数，另外一类是值设置参数。

4、系统代码管理

对当前系统代码进行添加、查询、删除、修改操作。

5、组件实现管理

管理员能在组件管理模块下对组件、进行增加、删除、修改、查询操作。

资源管理

1、连接池管理

管理员能在连接池管理模块下对连接配置、进行增加、删除、修改、查询操作。

2、责任链管理

管理员能在责任链管理模块下对责任链以及责任链下关联组件进行增加、删除、修改、查询操作。

终端管理

1、对接终端管理

对当前接入终端的终端标识、终端名称、审批状态进行添加、查询、修改操作。

2、节点用户管理

对当前节点用户进行添加、查询、删除、修改操作。

路由管理

1、消息路由

通过对消息接收者列表进行用户分组和动态路由配置，实现通讯消息的动态转发和分发。

2、静态路由管理

对当前静态路由进行添加、查询、删除、修改操作。

3、动态路由管理

对当前动态路由进行添加、查询、删除、修改、更新操作。

监控管理

1、线程状态管理

系统运行时根据为了达到系统性能的最优，系统将接收、发送、交换和共享四大类的场景分开处理，不同的场景根据单据量的多少自动开辟多个线程处理。

2、资源监控管理

用于查看当前资源使用情况。

3、报文异常管理

系统异常管理分为系统异常和阻塞异常，系统管理员可以根据异常时间范围，线程名称，和异常信息等条件进行检索查询，即可清晰了解到当前系统出现的问题的原因。

4、报文阻塞监控

系统异常管理分为系统异常和阻塞异常，系统管理员可以根据异常时间范围，线程名称，和异常信息等条件进行检索查询，即可清晰了解到当前系统出现的问题的原因。

5、资源预警监控

系统管理员可以根据资源名称，协议类型，时间范围等条件进行检索查询，即可清晰了解到当前系统出现资源预警问题的原因。

6、暂存落地管理

由于系统原因和阻塞原因造成的信息发送失败，在该模块下可以将失败的信息批量查询出来，并提供重新发送的机制对发送失败的信息重新发送。

7、数据落地管理

通过该模块利用所提供的查询条件查询出符合要求的历史记录。查询出来的历史记录可以选中查看详细内容，在该模块也提供了重发功能选中需要重发的数据进行重发操作。

8、消息安全

可与安全认证设备集成，通过数据签名、数据加密、数字信封等安全加密手段实现文档数据传输安全。

数据订阅

1、业务预定策略管理

管理员能在业务预定策略管理模块下，维护从业务系统预定数据的规则策略，业务系统预定规则配置方面包括预定的业务数据类型、业务数据项、业务数据查询条件、业务接收时间、地点、方式等等，

2、数据订阅下发管理

管理员能在数据订阅下发管理模块下将根据其他业务系统订阅需求维护数据订阅策略。

3、格式转换

数据交换系统将消息发送前，会检查消息发送者和接收者设置的消息格式转换的情况，并依次调用发送者和接收者消息转换规则，对消息进行格式转换处理。转换成功后的消息内容作为最终消息发送至接收者。

日志管理

1、交互日志管理

管理员可在交互日志管理模块下查看系统用户页面交互层面的操作日志。

2、服务日志管理

管理员可在服务日志管理模块下数据交换系统后台系统服务的调用日志。

3、登录日志管理

系统将自动采集操作人员登录和登出系统的日志信息。

各系统间接口

Websphere MQ 具有统一接口，可以跨越 IBM 和非 IBM 平台的特性。WebSphere MQ 目前支持 40 种系统平台，包括各种 IBM 和非 IBM 平台，具体接口如下：

序号	对接系统
1	与货物申报接口开发
2	与舱单申报接口开发
3	与金二核注清单接口开发
4	与核放单接口开发
5	与加贸账册接口开发
6	与加贸手册接口开发
7	与运输工具申报申报接口开发
8	与货物申报接口开发
9	与监管场动态管理系统接口开发
10	与智能卡口散货杂货接口开发
11	与港航 EDI 轨迹数据采集接口开发
12	与码头装卸动态接口开发
13	与堆场管理系统接口开发
14	与港航场站管理系统接口开发

15	与集装箱管理系统接口开发
16	与多式联运接口开发
17	与电商平台接口开发
18	与支付企业接口开发
19	与物流企业接口开发
20	与洋浦公服接口开发
21	与金税平台接口开发
22	与外汇管理平台接口开发
23	与海南政务平台接口开发
24	与仓储企业接口开发
25	与贸易企业采购平台接口开发
26	与公安平台接口开发
28	与商务厅数据接口开发
29	与质检数据接口开发

订阅分发系统

各功能模块定义

数据订阅

1.订阅事件申请

通过事件方式，提供数据订阅的申请、审核及相关管理工作，订阅事件包含发起端信息，订阅目标端信息及订阅数据内容、接收和分发方式、目标地址，以及更新频度等。

2.订阅事件解析及管理

采用结构化的方式存储订阅事件的要素，对订阅事件进行管理，记录系统日志，解析订阅事件要素，实现动态监控和执行，获取被订阅端系统的数据变化情况，同时支持被订阅端系统的插件植入方式，即动态监控获取和被订阅端主动触发两种模式。

3.订阅事件的监控和预警

动态监控数据预定事件的执行情况，支持事件异常的提醒和处置，管理事件

的订阅和接收结果，按一定时间段保存订阅数据的报文内容，以支持数据补发和排查工作。

4.订阅事件的统计分析

以订阅事件为单位，统计本事件历史接收次数、历史接收数据总量、数据分布情况、历史数据接收时间统计（日/月/年）。

数据分发

1.数据订阅式分发

根据数据预定事件的要素，主动获取被订阅端的数据变化情况，动态监控数据变化并获取数据信息，将数据变更情况和数据内容进行报文打包，在本地系统留存底账。

2.数据触发式分发

根据数据预定事件的要素，建订阅触发器插件部署至被订阅系统，被订阅系统在指定环节触发数据预定事件，主动打包数据报文并发送至分发端，分发端留存，并留存报文结果和分发事件执行情况，对回执结果进行监控和管理，支持分发异常情况下的补发操作，记录系统执行日志。

3.分发事件的统计分析

对所有订阅数据的分发情况进行记录、展示和统计分析。包括分发次数、订阅系统数、接收情况、数据量和异常情况等。

统一 API 管理系统

各功能模块定义

接入平台管理

可以对接入的系统基本系统进行标识化管理，用于后期子系统对接越来越多，解决个性化接入的管理。避免特殊接口修改影响全局。主要提供查询，新增，修改，删除功能。

协议管理

对于每个接口所使用的通信协议进行单独灵活配置，便于系统对接适应不同的网络协议环境，统一管理快速部署，降低开发成本。

接口管理

提供各接口在使用层面灵活配置调入参数和返回参数的名称，个数，数据类型等，做到千人千面的使用。降低了开发为适应业务发展而改底层逻辑的成本。便于后期运维的管理。

日志管理

将用户配置接口的结果集中记录，用于用户行为的监控，对可疑或错误操作，进行追溯分析。便于事后的安全责任认定。主要为开发人员对接口操作的记录。

接口统计

对系统中以及开发的接口进行汇总统计，避免接口重复开发，对取消或开发未发布使用的接口进行标记归档。提供查询，导出功能。

路由分发

支持接口的路由配置管理，为接口配置多个路由通道，当系统接口出现负载过重时，自动或人工切换到其他渠道，保证接口的稳定运行。主要提供查询，新增，修改，删除等功能。

连接设置

支持调用接口的 IP 和端口等信息变更，方便系统迁移以及网络部署等环境变更导致接口的逻辑修改风险，主要提供查询，新增，修改，删除等功能。

单边地址维护

把系统的接口提供方的 IP 地址设置为常量，进行手工灵活配置，避免网络断网或专线断线导致网络传输中断引起的系统接口调用失败情况产生，主要提供查询，新增，修改，删除等功能。

地址过滤

支持人工隔离或系统隔离非法服务访问接口获取数据的情况发生，通过设置 IP 地址或域名限制未进允许的服务访问接口数据。

配置推送

运维人员将开发完成的接口，经过配置推送后自动部署到服务器进行服务调

用。减少了人工部署繁琐操作。

日志记录

该模块主要用于记录各接口的接入状态及其异常日志、运维日志，通过接口名称、时间等条件可对日志记录进行查询。

智慧海南对接体系

促进政务数据共享是提升政府治理能力、促进经济转型升级的有效途径和重要手段，推动政务数据共享是我国深化改革、转变职能、创新管理的重要举措。随着《智慧海南总体方案（2020-2025 年）》及《“十四五”大数据产业发展规划》的发布，以及海南省大数据管理局各项工作的落实与推进，为加快推动海南省大数据产业高质量发展，全面推进大数据与经济社会深度融合，海口综合保税区智慧园区建设项目将与智慧海南的数据共享平台进行园区公共服务、运营管理、展销综合服务、作业综合服务、辅助监管业务数据的传输共享。

智慧海南总体架构包括“四梁八柱”和“地基”。“四梁”指国际信息通信开放试验区、精细智能社会治理样板区、国际旅游消费智能体验岛、开放型数字经济创新高地四个战略定位；“八柱”包括打造 5G 和物联网等新型基础设施、提升国际信息通信服务能力、创新现代化治理和智慧监管新模式、构建立体防控智慧生态治理体系、优化国际旅游消费服务智慧化体验、推动数字政府和智能公共服务创新、加快优势产业数字化转型、数字新产业做优做强等内容。“地基”包括智慧大脑、能力中台、支撑体系以及机制体制等共性设施，通过构建智慧大脑和能力中台，形成智慧海南“内核”和技术创新“引擎”，通过健全运营、标准、安全一体化支撑体系，形成多主体高效配合、多要素有力支持的资源中心和生态体系。

与海南省大数据管理局对接

海口综合保税区智慧园区建设项目将通过与与海南省大数据管理局进行平台对接，传输海口综保区内的基础设施数据与业务开展数据，为智慧海南能力中台提供数据基础，为构建海南自由贸易港智慧大脑添砖加瓦。另外也将通过大数据管理局数据平台订阅园区开展的业务相关数据，打通园区与其他管理机构的信息壁垒，辅助海关对园区开展业务进行监管，简化企业的申报流程，减少信息录

入。

主要对接数据包含海南单一窗口、海南公共服务平台、国际贸易投资单一窗口、海口海关监管系统的报关单表头数据、验放指令、仓库实时视频、跨境电商清单、人员健康码数据等。预留与统计局的接口，传输报表统计数据；预留与海口海关的数据接口，传输核注清单、核放单数据。对接内容包含园区公共服务平台数据对接、园区运营管理平台数据对接、展销综合服务平台数据对接、作业综合服务平台数据对接、辅助监管业务服务平台数据对接。

与一线口岸对接

目前，海南省设立 8 个对外开放口岸，为满足全岛封关运作“一线”进出需要，设立 10 个“二线口岸”保障“二线”进出需要。海口综合保税区作为特殊监管区域，区内会开展 “一线、二线”业务，为了区内“二线”业务的健康发展，海口综合保税区智慧园区建设项目需预留与“一线口岸对接 ”模块，与航空、水运、铁路等“一线口岸”进行信息对接，获取报关数据、订舱数据、航空舱单、船舶舱单、铁路舱单、一线检疫结果等数据，完善出入区货物的业务流、数据流、物流。

与二线口岸对接

目前，海南省设立 8 个对外开放口岸，为满足全岛封关运作“一线”进出需要，设立 10 个“二线口岸”保障“二线”进出需要。海口综合保税区作为“一线放开、二线管住”的重点区域，需预留与其他 10 个“二线口岸”的对接接口。通过预留接口传输相关货物到达海口综合保税区后的流转及处置，获取货物在其他“二线口岸”的相关数据，完善货物的物流链条，保证票票货物可追踪、可溯源。

园区智慧管理平台建设方案

园区智慧管理体系总体设计

一、总体概述

结合海口综保区的实际需求，满足智慧园区的多应用整合多个异构子系统，同时以网络通讯及数字化技术为基础，为多个“信息孤岛”提供协同合作的统一平台，建立一套高集成、高智能化的管理机制，满足统一的配置管理、数据共享、功能联动和业务优化等系统需求，形成有智慧园区特色的场景应用。

鉴于系统接入的复杂性与多样性，在该系统架构规划设计时，采用全网络的架构，各个子系统最终通过网络连接到中心，通过建设智慧园区管理平台进行统一集成与管理，同时能够面向园区企业、园区管理方以及园区公众。

二、系统拓扑

智慧园区管理系统的建设，绝不应该是对各个子系统进行简单堆砌，而是在满足各子系统功能的基础上，寻求内部各子系统之间、与外部其它智能化系统之间的完美结合。系统主要依托于智慧园区管理平台对众多安防子系统的统一管理和控制，通过智慧园区管理平台建设，实现统一数据库、统一管理界面、统一授权、统一权限卡、统一安防管理业务流程等，同时考虑将各安防系统资源作为信息化基础数据，满足部分生产运营管理的业务需求，辅助业务流程优化。

三、重点应用设计

智慧园区综合解决方案从基础的园区整体安全防护需求做为切入点，利用用户对视频安防的依赖，扩展并引导用户采用一系列可视化智能应用，从而更好的帮助用户通过视频可视化方案实现智慧园区减员增效降成本的需求，同时能够通过大数据分析为用户提升招商能力，企业服务能力，继而提升园区内受众的整体体验，以下是整个综合方案的应用集划分：智慧园区解决方案的应用介绍如下：

1、智慧物联应用包含安全管理、智慧消防、安消一体和能耗管理四个智能应用。

2、科技服务应用包含招商管理、园区办公、人员管理和车辆管理四个子智能应用。

3、运营支撑应用包含物业巡检管理、电瓶车充电管理、运营服务应用三个智能应用。其中运营服务应用是由第三方生态合作伙伴提供。

4、数字化运营应用包含 AR 实景指挥应用、数据看板应用和 3D 指挥视图应用。

系统基于智慧园区管理平台对多个子系统的业务整合，实现了高效的人员管理机制，为产业园区内人员提供了便捷、安全的环境，为管理人员提供了高效的管理手段。

（1）无纸化访客管理，提升园区安全及访客来访便捷性，并提升产业园区形象；配合人员定位管理大大提升访客人员管理的精细度，真正起到分级分区的人员管控，对高涉密、高危区域形成有效的保护。

产业园区智能一脸通提供便捷、安全的人员管理；人员精确管理，授权通过，省管理人力。

人员进出数据可查、管、追溯。

（2）可靠的车辆管理

系统实现了高效的车辆管理机制，提供了产业园区内车辆有序运行、以及产业地产开发商或运营商自有物流车辆的可靠管理手段。

园区车辆出入口、园区内卡口管理让车辆有序规范运行。

物流可视化子系统让园区自有特殊车辆处于可靠的管理之下。

车辆进出数据可查、管、追溯。

（3）统一的管理平台

综合安防系统通过智慧园区管理平台可将若干子系统进行统一配置与管理：

统一数据库，内部信息相互联通，有利于信息传递。

通过软件设计实现的业务联动，简化系统联动设计。

智能网管实时监测系统运行数据，方便运行维护。

统一界面、控制逻辑与配置方式等，提升管理效率。

（4）多方位的系统联动

系统基于智慧园区管理平台对传统定义的多个子系统进行业务整合，实现丰富的功能联动机制，通过多个子系统功能互补避免安防疏漏，提高安防管理的业务自动化程度，对安防事件防患于未然，对安防警情及时响应。

全面的联动触发事件设计。

可配置多种联动结果响应警情。

支持短信、电子邮件等远程告警。

可设置软硬件联动输出，与周边设备联动。

（5）便捷的功能设计

系统从终端用户的角度出发，考虑日常应用的便捷与合理性进行业务流程设计，同时从管理方的角度出发，为管理业务提供更多高效的自动化管理手段：

可配置全局预案实现管理业务自动化。

全局电子地图监管功能，为管理员提供直观的图形化监控界面。

功能全面的大屏幕显示方案。

支持手机、Pad 等远程客户端访问。

（6）灵活的系统扩展

系统基于模块化设计，可根据后期需求进行灵活扩展而不影响整体软硬件框架，同时支持多种标准接口。

基于以太网 TCP/IP 通讯，同时兼容 RS-485 等其它通讯方式接入；

提供 SDK/OPC/Web Service 等多种标准接口。

指挥中心建设

大屏显示系统

系统概述

考虑到综合指挥中心空间跨度窄的特点以及屏幕的亮度，对比度和视角范围，建议采用间距小于或等于 1.25mm 的 LED 产品作为本项目的显示主体。

大屏规划建设尺寸如下：

三面墙体安装 p1.25 屏幕，主屏幕长 7m，高 2.3625m，分屏幕长：4m，高 2.3625m,总面积为：7m*2.3625m+4m*2.3625m*2=35.4375 ㎡。大屏两边采用不锈钢封边，防火板封口。

系统架构

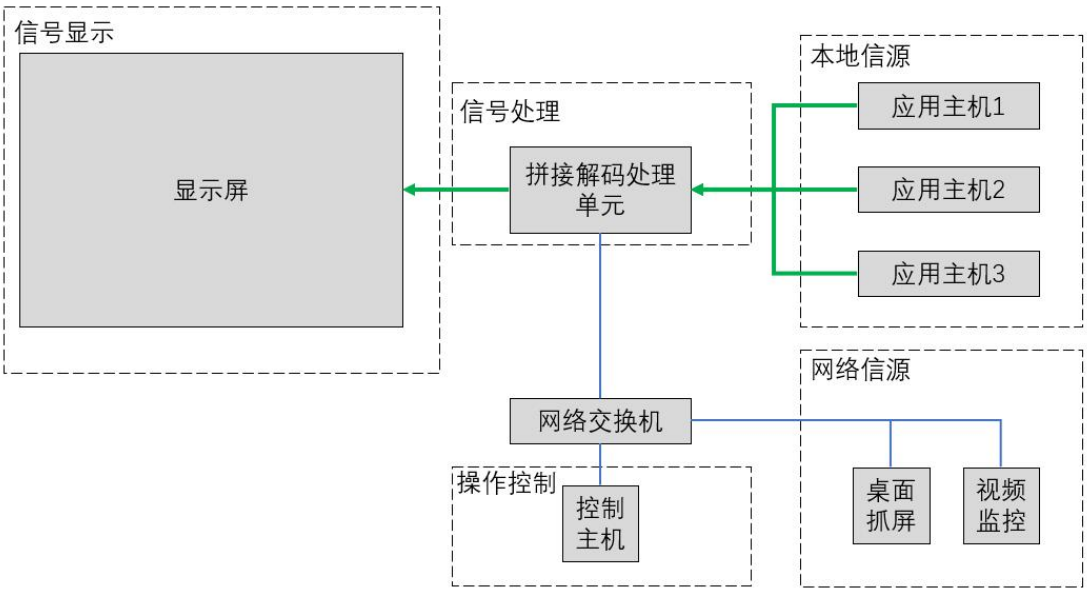


图 1- 48 大屏业务系统架构图

操作控制

电脑登录客户端或 web 界面，通过网路向拼接解码处理单元发送控制指令。

信号处理

本地输入信号和网络输入信号通过拼接解码处理单元的输出端口通道输出，输出端口通道可自定义多个独立的组，每个组输出的分辨率可以相同或不同。用户根据现场需要配置相应的分辨率，为系统控制及管理多组分辨率提供解决方案。为保证高速运动的画面在虚拟墙的各个物理显示器上能达到同帧播放的效果，避免不同步造成的不同屏运动、画面错位和追赶现象造成的横切纹问题。支持画面全系统同步技术和双缓冲技术，保证了全虚拟屏的帧同步和无追赶，为用户提供流畅、连贯、实时的高清运动画面。

信号显示

显示屏 HDMI 视频输入接口接收拼接解码处理单元的视频信号进行画面显示，RS232 接口接收开关机信号控制开关机。

功能框架图

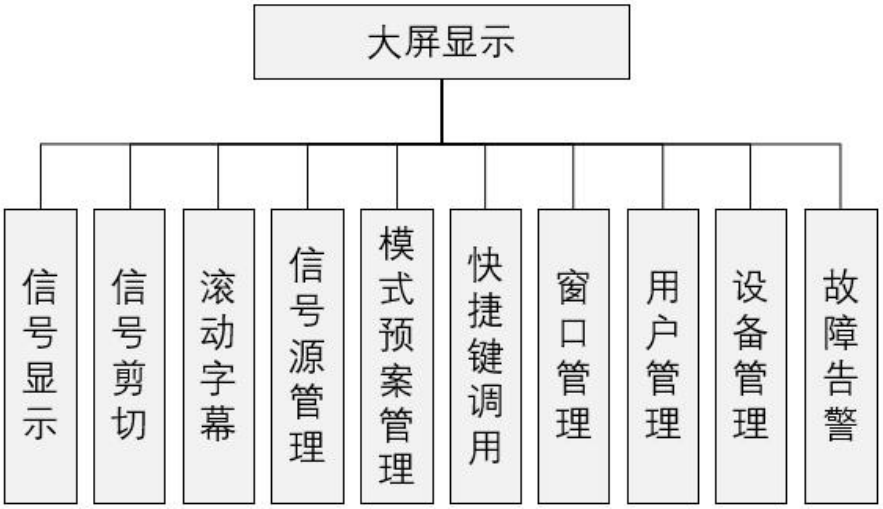


图 1- 49 业务功能结构示意图

指挥中心配套设备

操作设备

配置2台具备独立显卡的图形工作站和2台采用集成显卡的管理工作站用与值班人员日常使用。

配套 1 台对讲求助接收主机，可接收对讲求助呼叫。

配置 1 台总线网络报警主机及声光警号，配置报警联动，高危报警是现场声光提示。

操作台

在指挥中心配备操作台，主要用于值班人员及操作人员办公。操作台采用钢木结构，尺寸定制,造型简单约实用。

地板装修

指挥中心也有较多的线缆，设计采用 OA 网络活动地板，指挥中心敷设活动地板可形成隐蔽空间，可以在地板下敷设电源线管、线槽、综合布线、消防管线等以及一些电气设施（插座、插座箱等），方便今后线缆设备检修；在活动地板上安装地毯，既整洁，又显得高档大气。地板安装高度约 5-10cm，不占用过多

的地面空间，保证指挥中心高度。静电地板与墙边采用不锈钢踢脚线收边，美观大方。

配电照明

指挥中心照明灯具采用不频闪光源，度尽量采用漫的射照明，指挥中心区照度 500Lx 1x，灯光色温为 4300K，，指挥中心内要考虑应急照明、疏散照明和安全出口标志灯：应急照明按一般照明的 1/10 考虑。应急灯和安全出口标志灯照度不低于 501X。应急照明及出口指示灯内置电池供电。

照明灯具控制方式：灯具采用分区分散控制的原则，以利于节能。应急照明单独走管穿线并由墙面荧光显示跷板开关单独控制。主要照明采用控制箱控制，局部用跷板式暗开关，安装在墙上距地 1.4m 处。

指挥中心配套设备

操作设备

配置 2 台具备独立显卡的图形工作站和 2 台采用集成显卡的管理工作站用与值班人员日常使用。

配套 1 台对讲求助接收主机，可接收对讲求助呼叫。

配置 1 台总线网络报警主机及声光警号，配置报警联动，高危报警是现场声光提示。

操作台

在指挥中心配备操作台，主要用于值班人员及操作人员办公。操作台采用钢木结构，尺寸定制,造型简单约实用。

地板装修

指挥中心也有较多的线缆，设计采用 OA 网络活动地板，指挥中心敷设活动地板可形成隐蔽空间，可以在地板下敷设电源线管、线槽、综合布线、消防管线等以及一些电气设施（插座、插座箱等），方便今后线缆设备检修；在活动地板上安装地毯，既整洁，又显得高档大气。地板安装高度约 5-10cm，不占用过多

的地面空间，保证指挥中心高度。静电地板与墙边采用不锈钢踢脚线收边，美观大方。

配电照明

指挥中心照明灯具采用不频闪光源，度尽量采用漫的射照明，指挥中心区照度 500Lx 1x，灯光色温为 4300K，，指挥中心内要考虑应急照明、疏散照明和安全出口标志灯：应急照明按一般照明的 1/10 考虑。应急灯和安全出口标志灯照度不低于 501X。应急照明及出口指示灯内置电池供电。

照明灯具控制方式：灯具采用分区分散控制的原则，以利于节能。应急照明单独走管穿线并由墙面荧光显示跷板开关单独控制。主要照明采用控制箱控制，局部用跷板式暗开关，安装在墙上距地 1.4m 处。

智慧园区集成平台

智慧园区集成平台概述

集成平台定位为智能子系统、数据和各种应用提供通用核心能力，打破平台、云、网络、地域边界，连接烟囱应用，消灭信息孤岛，打通业务流，实现业务数字化全联接协同。

集成平台对外统一提供标准化的 API，上层应用可以基于平台快速构建业务应用，当下层集成的系统有所变动，可以在平台进行适配和服务编排，避免上层应用的改动。

集成平台需要具备基本的大数据处理能力，包括数据清洗治理、实时流服务、数据仓库建模、数据存储等功能。

集成平台旨在提供便捷的线上开发&编排能力，提供快速的行业套件开发定制能力，使能客户不断沉淀综保区场景行业资产，促进业务持续高效创新，加速应用开发和创新，打造百花齐放的开放应用系统。

1.1.1.1.1 集成架构设计

智慧综保区涉及到多个智慧化应用，系统之间涉及到大量的集成与互联等需求。智慧综保区主要通过部署园区集成平台应子系统较多、数据类型复杂、通信

模式多样、系统跨建筑等挑战况。除视频流以外，所有系统间的数交换必须通过场馆集成底座进行。整体集成策略如下：

1．通过集成平台为大多数业务应用软件提供系统集成支撑

2．通过大数据分析平台支撑海量数据的汇聚、存储和分析，为跨系统、跨业务的应用提供数据分析支撑能力

3．通过集成平那台，为综保区内外各应用搭建数据和信息交换的桥梁。

各子系统集成架构如下：

通过网联网与集成平台统一接入到数据平台，各种数据在此进行清洗治理，然后形成 IOC、智慧安防等应用所需的主题库、专题库，供智慧化应用使用。

其他系统的数据，比如海关相关的综合作业数据，智慧化应用可直接通过集成平台中的 Restful API，或者 MQS 消息队列等调取。

视频监控系统的视频数据通过转码器进行格式和分辨率的转换，供 IOC、手机等终端使用；视频算法使用的，

实时数据可直接通过集成平台中的 Flink 组建直接提供给智慧化应用。

智慧园区数据平台

数据平台概述

智慧园区数据平台作为综保区园区园区管理类应用的数据底座，主要负责完成各异构子系统（安防管理、人员通行、一卡通、停车管理、消防管理等）的数据集中建模管理和使用，实现园区数据的基础数据整合，统一规划数据语言，向下通过集成平台或直接提供已接入子系统应用的数据集成接口，把对应的源数据转换成为结构化数据，保存在数据使能组件的相应主题库中；向上提供数据服务、计算能力接口给智慧应用系统，以供智能运营中心、GIS、物联网等调用数据接口，消费相关数据。

数据平台架构

园区数据平台作为智慧综保区的物联数据底座，主要负责完成各异构子系统（综合安防、人员通行、一卡通、停车管理、能耗管理等）的数据集中建模管理

和使用，实现园区数据的基础数据整合，统一规划数据语言，向下通过融合集成平台或直接提供已接入子系统应用的数据集成接口，把对应的源数据转换成为结构化数据，保存在数据使能组件的相应主题库中；向上提供数据服务、计算能力接口给智慧应用系统，以供智能运营中心、GIS、物联网等调用数据接口，消费相关数据。

媒体转码组件

媒体转码概述

媒体网关是一套集视频采集，视频管理、视频存储、视频转码、视频直播、视频点播、智能调度于一身的视频云平台：

系统能够支持分布式架构，采集、编辑、存储、转码、分发和管理均可灵活配置。

系统支持集群负载均衡和自动容灾机制，保障内容生产正常运行。

系统均采用标准的协议和机制构建，保证系统的开放性和通用性

网络架构应体现高性价比的原则，同时要求保证网络的安全性、可用性、稳定性和前瞻性，要求提供清晰的网络架构和性能指标设计。

能够提供完善的系统管理功能，可以对系统进行灵活配置等操作。

媒体转码组件架构

主要模块和能力

集成开放网关:集成 eSDK 并以 restFul 形式开放接口;支持对转码分发系统进行控制调度;

AllMedia 媒体子系统：从 VCN 获取 RTSP 流按照转码模板进行转码压缩，并以 FLV、RTMP、HLS 形式输出。

5.4.1.12.5. 地理信息数字系统 GIS

海口综保区地理信息子平台是一个二、三维一体化的地理信息服务平台，支持对海口综保区空间静态数据的采集、储存、管理、运算、分析、显示，并支持

与定位子平台集成，实现室内的人员定位与导航基本功能，提供 SDK 和 REST 接口（或者 OGC），供上层应用如运行指挥中心等应用集成，实现统一视图的可视化的综保区管理。突破以人工管理为主的常规综保区管理模式，解决传统模式中信息孤立、流通不畅、缺乏综合分析、难以共享、应对突发事件反应迟缓、安全隐患较大等问题，实现物联网时代全面感知综保区各种信息，让综保区管理更加智能和便捷。

5.4.1.12.6. 可视化平台

本平台通过对接园区相关业务系统，如安防、消防、招商、场站、物流、辅助运营系统等，对接园区业务核心呈现和分析数据，实现园区运行数据的可视化展示、智能监测与预警，实现整体运行态势，可视化专题页面包括：园区总览、安防监测、便捷通行、设施管理、敏捷招商、党建管理、数字化运营态势、数字物流运营、业务运营可视化。

作为保税区管理的决策辅助系统，平台以三维模型/实景为载体，将园区运行核心系统的各项关键数据进行综合展现，支持从综合保税区未来规划、基础设施、园区数字运营、数字贸易管理、预警分析管理，智慧物联及企业画像等多个维度进行日常运行监测与管理，以及突发事件的应急指挥调度管理，提供一个集保税区规划、园区生产、园区运营、园区决策多维一体的智能运营管理平台，为保税区管理者提高园区运行效益以及园区管理效率，提供数据决策支撑。

智慧安防系统

视频监控子系统

系统设计

视频监控子系统的设计思路如下：

前端设备均采用全高清的前端智能摄像机，具备按需定义场景的特点，根据不同的场景按需加载不同的软件和算法,通过多样的组合来快速适配实际需求，采用精准判断的方式，以全特征和多信息的方式提高准确率、降低误判；同时，通过端云间的协同进行联合判断，提高分析准确率，支撑实战。

采用云计算、云存储、大数据等核心技术，构建硬件资源集成度更高的机器视觉云解决方案，适用于智慧园区应用场景，为用户提供大容量、高并发的视频接入、存储、转发和视频分析、视频检索能力。通过软件服务化，实现软件弹性部署，按需定义云节点；南向接口支持多种场景算法，算法按需加载，实现业务弹性； 统一 API 接口，服务上层应用开发。

部署模块化、集成化的视频综合平台，结合高清显示大屏实现视频图像、电子地图、电脑信号的上墙显示、拼接控制等功能。

建立统一的综合管理平台，实现对系统的统一管理；同时引入视频质量诊断技术，保障系统稳定运行。

充分考虑原有系统利旧，实现新老系统的无缝对接，降低成本，减少资源浪费。

系统采用高清视频监控技术，实现视频图像信息的高清采集、高清编码、高清传输、高清存储、高清显示；系统基于 IP 网络传输技术，提供视频质量诊断等智能分析技术，实现全网调度、管理及智能化应用，为用户提供一套“高清化、网络化、智能化”的视频图像监控系统，满足用户在视频图像业务应用中日益迫切的需求。

前端摄像机部署在两个园区，分别为澄迈保税区园区和海口保税园区，点位图如下所示：

点位名称	需求摄像机类型								点位数量汇总	立杆要求
原保税区	网络球机		网络枪机		网络半球		其他类			
戊号路和三号路交汇处	网络球机	2	网络枪机	1					3	新建 1 根
戊号路和四号路交汇处	网络球机	2	网络枪机	1					3	新建 1 根
戊号路金星药业旁	网络球机	1	网络枪机	1					2	新建 1 根
金盘路康宁旁	网络球机	1	网络枪机	1					2	新建 1 根
金盘路越阳生物旁	网络球机	1	网络枪机	1					2	新建 1 根
金盘路美大制药旁	网络球机	1	网络枪机	1					2	新建 1 根

金盘路恒远泰富旁	网络球机	1	网络枪机	1					2	新建 1 根
五号路康宁旁			网络枪机	2					2	新建 1 根
五号路美兰克史旁			网络枪机	2					2	新建 1 根
五号路新世通旁			网络枪机	4					4	新建 2 根
六号路新世通旁			网络枪机	4					4	新建 2 根
丁号路新世通旁	网络球机	1	网络枪机	1					2	新建 1 根
丁号路与六号路交汇处	网络球机	1	网络枪机	1					2	新建 1 根
丁号路惠普森			网络	2					2	新建 1 根

旁			枪机							
乙号路均达汽车旁	网络球机	1	网络枪机	3					4	新建 2 根
均达汽车旁小路			网络枪机	4					4	新建 2 根
乙号路全兴工业旁	网络球机	1	网络枪机	3					4	新建 2 根
全兴工业与联顺金属中间			网络枪机	4					4	新建 2 根
威昌汽车旁道路			网络枪机	6					6	新建 3 根
威昌汽车旁路口	网络球机	1							1	新建 1 根
瑞利工业和宇傲汽车中间			网络枪机	4					4	新建 2 根

全兴工业和宇傲汽车中间	网络球机	1	网络枪机	3					4	新建 2 根
六号厂房旁			网络枪机	6					6	新建 3 根
五号厂房与七号厂房间			网络枪机	2					2	新建 1 根
际中药业旁			网络枪机	2					2	新建 1 根
华夏消声器门前	网络球机	1	网络枪机	1					2	新建 1 根
金盘电气			网络枪机	2					2	新建 1 根
八号路			网络枪机	2					2	新建 1 根
海卡后门处路	网络	2							2	新建 2 根

段	球机									
保税区大楼门前			网络枪机	4					4	新建 2 根
周界围墙							周界防护摄像机	46	46	新建 13 根及 10 根围墙支架
澄迈保税区									0	
联检大楼 1 楼大厅	网络球机	7	网络枪机	18	网络半球	8			33	不涉及
联检大楼 2 楼			网络枪机	2	网络半球	8			10	不涉及
联检大楼 3 楼			网络枪机	7	网络半球	8			15	不涉及
联检大楼 4 楼			网络枪机	8	网络半球	8			16	
联检大楼 5 楼			网络	6	网络	1			7	

			枪机		半球				
联检大楼6楼			网络枪机	6	网络半球	1		7	不涉及
联检大楼7楼			网络枪机	5	网络半球	1		6	不涉及
联检大楼8楼			网络枪机	5	网络半球	1		6	不涉及
联检大楼9楼			网络枪机	8	网络半球	1		9	不涉及
商务中心			网络枪机	10	网络半球	30		40	不涉及
展销中心					网络半球	23		23	不涉及
园区内部道路	网络球机	20	网络枪机	160				180	复用灯杆

园区高点							全景摄像机	10	10	不涉及
综保区人才公寓									0	
室外					网络半球	6			6	新建 6 根
室内					网络半球	11			11	不涉及
地下室					网络半球	6			6	不涉及
电梯					网络半球	4			4	不涉及
高空抛物							高空抛物专用摄像机	4	4	不涉及
汇总		45		304		117		210	676	

系统架构

前端设备

前端支持多种类型的摄像机接入，系统可配置高清网络枪机、球机、智能网络摄像机等，按照标准的音视频编码格式及标准的通信协议，通过网络进行视频图像的传输。

传输网络

采用视频专网的形式搭建整个监控网络，专网专用，保证安防视频的稳定性与安全性。

监控中心

监控中心配置视频云平台，完成视频的解码、拼接，通过部署拼接大屏用来将视频进行上墙显示等。系统可将局域网内的网络摄像机都接入到视频综合平台，实现统一的管理、统一的切换控制和统一的显示，实现对整个系统的统一配置和管理。

视频云平台部署在视频存储服务器以及视频解析服务器上，可以对视频监控设备和用户进行统一管控，并实现浏览、回放、下载等视频应用。

功能设计

1.视频云监控架构，99.999%电信级可靠性

视频监控的核心是在确保视频监控数据存储的安全，视频云监控存储通过如下设计确保系统的电信级可靠性：

分布式全对称架构，高可靠性，部署维护简单；

视频云节点关键部件全冗余设计，采用双网络接口，冗余电源、散热风扇；采用双系统盘并进行 Raid1 保护，更换故障部件不中断业务；

支持按需冗余、RAID 失效后仍然可读可写、RAID 在线扩容；

N+0 云化集群部署，故障自动迁移恢复，单点故障不中断业务；

磁盘碎片避免设计，通过核心专利视频流动态块控制技术、视频块连续写入技术和合理空间回收技术相结合，对视频数据存储进行优化，既保证了数据的连续性，又避免了磁盘空洞；

2.全天候场景自适应的软件定义摄像机

确保各场景下优异的低照度、宽动态、强光抑制的成像效果：

先进芯片内嵌图像处理算法。

三帧超宽动态技术、基于点光源曝光的强光抑制算法、专用图像透雾算法。

基于 H.265 的 Extra265 专利编码技术，更低码率，更高的图像质量。

3.经过实战检验的园区人脸识别系统

针对园区人流量大，出入口进出方向不固定、外来人员身份复杂、抓拍环境复杂的特点，针对该场景下的人脸识别进行了专门优化：

支持实时布控告警、静态库\路人库以图搜图检索、轨迹查询、1:1 和 1：N 比对分析，

摄像机支持侧脸 60 度抓拍，抓拍率可达 99%，重复率低于 3%，误抓怕率小于千万分之一。

人脸黑名单比对准确率大于 85%，黑名单告警响应时间低于 3s，实时声音提示，亿级路人库数据，秒级返回检索结果。

4.先进的车辆违停识别

超星光违停检测系统，全智能车辆违停管理，防止进入园区车辆长期占用主干道、消防通道等。

5.智能行为分析提高安防效率

前端摄像机和后端系统均支持智能分析能力，提高了安防效率，如通过入侵检测，有效制止安全事件。

6.开放架构，易于集成

视频云监控解决方案通过 eSDK 提供开放接口和开发套件，分为南向接口和北向接口。

南向接口负责接入前端设备、接入第三方平台、接入第三方算法；

北向接口负责向上层业务应用开放视频图像及结构化数据等。

监控中心部署

监控中心建设内容具体包括视频云平台、视频解码器、拼接大屏、客户端软件等。 本次所规划的前端点位均存储于澄迈园区机房。

结构设计

监控中心系统架构图如下所示：

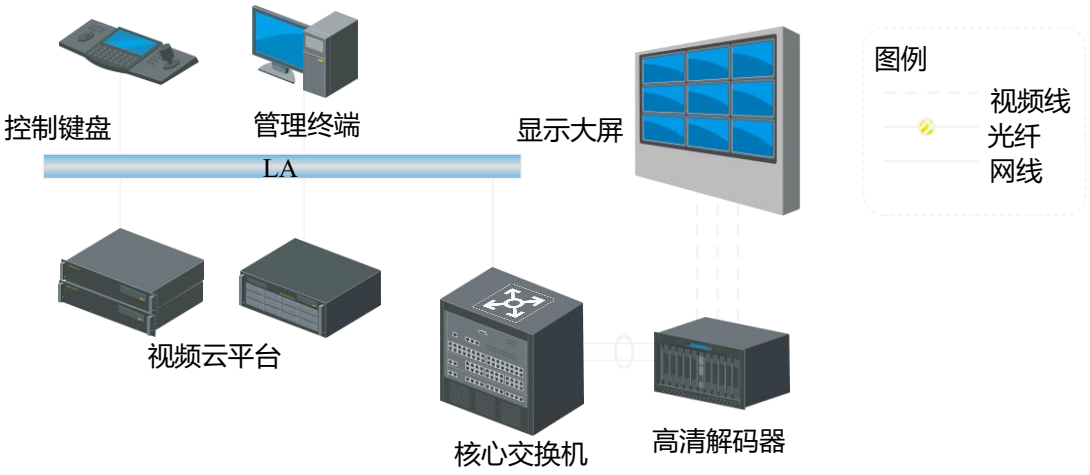


图 5-32 监控中心系统架构图

监控中心是整个视频监控系统的核心，实现视频图像资源的汇聚，并对视频图像资源进行统一管理和调度。其中，视频云平台实现视频图像资源的存储及调用解析；高清解码器完成视频解码上墙和图像的拼接控制，并通过网络键盘进行视频切换和控制，通过高清大屏对高清视频进行精彩展现。

视频存储平台

视频存储平台是上级业务应用系统的主要数据来源。传统分布式存储为主的“小而散”的智能安防方案，对建设单位的场地、运维、人员等诸多因素带来了越来越多的挑战和问题，诸如机房建设标准、布线、系统的维护等问题日益突出。

当前智能安防的“智能化”发展已经得到了社会各界的普遍认同，智能应用得以快速发展，而传统使用“一体机”软硬件绑定的烟囱式建设模式，分散的数据存储都给智能安防智能化发展带来了巨大的困扰。

➢ 本次建设的视频存储平台在物理服务器操作系统之上，直接通过轻量化容器技术部署和运行业务应用，以保持系统所具有的弹性扩容、自动化部署升级等特性。系统采用容器化微服务部署和本地硬盘可靠存储，基于高性能的容器网络、高可靠的容器存储和轻量级的无损计算性能，实现了基于容器的应用生命周期管理机制。

后端视频云存储

视频数据量估算

视频存储资源计算

视频格式与视频码率对照表如下：

H.264/H.265				
视频格式	默认码率（Mbps)	码率取值范围（Mbps)	备注	路数
900W	12	12-16	分辨率 4096*2160	
4K（800W）	12	12-16	分辨率 3840*2160	
600W	8	8--12	分辨率 3072*2048	
500W	8	8-10	分辨率 2688*1944	726 路
400W	8	8-10	分辨率 2688*1944	
300W	8	6-8	分辨率 2048*1536	
1080P（200W）	4	4-16	分辨率 1920*1080，全高清	

计算视频裸存储容量

全量录像存储容量 =（录像路数×码率×录像天数×24×3600×CBR）÷8÷1024÷1024；此处码率以 Mbps 为单位，录像存储容量以 TB 为单位。

视频裸存储容量为：

=（676 路）×8M×60 天×24×3600×1.1÷8÷1024÷1024≈3677TB。

备注：

1、CBR 为码率波动系数，取值范围为 1.0 ~ 1.3，可根据项目调整，一般项目中推荐使用 1.1；

2、存储裸容量按照全天 24 小时不间断存储进行计算；

3、码率按 8M 取值.

本次视频存储硬盘推荐采用企业级 16TB SATA 硬盘，减少所需硬盘位空间，考虑硬盘格式化损耗和厂商标称的容量换算，实际有效数据可用容量

=16*（7/8）（硬盘利用率）≈14TB

考虑到监控系统整体存储空间冗余，配置 1 台视频存储服务器，每台配置 38 块硬盘，每台可用磁数为 35 块（1 块校验盘，2 块热备盘），实际可用磁盘数为 35 块，则所需的视频存储服务器的台数为=总存储容量

/35/14=3677/14/35=7.5≈8 台。

所需的硬盘数为=总存储容量/硬盘实际可用容量+（服务器数量*（校验盘数量+热备盘数量）=（3677/14）+（8*2）=280 块。

同时考虑到硬盘损耗，建议 10 块作为备件盘。

则本次配置需要 8 台视频存储服务器以及 290 块 16TB 硬盘。

视频存储设备

设备名称	功能参数	数量
磁盘阵列	1)操作系统：嵌入式 LINUX 系统； 2)主处理器≥64 位高性能多核处理器； 3)高速缓存：标配 8GB，可扩展至 64GB； 4)电源冗余：1+1 冗余电源； 5)网络接口：1 个千兆管理电口，2 个千兆数据电口； 6)硬盘个数：≥38 块硬盘； 7)硬盘兼容性: 1TB、2TB、3TB、4TB、5TB、6TB、8TB、10TB、12TB、14TB、16TB，支持 SATA 盘混插支持 SSD 硬盘支持 2.5、3.5 英寸硬盘支持 SATA 盘； 8)支持视频流和图片流直存：最大不少于支持 2048 路前端接入、1560Mbps 存储、1024Mbps 转发，512Mbps 网络回放； 9）支持单台服务器起配，管理和业务服务共享统一的虚拟化资源；在一台实体服务器虚拟化后的多台逻辑服务器上，支持部署不同功能以及数量的存储、转发、智能分析、检索服务模块；	8
企业级硬盘	16TB 企业级硬盘,SATA 6Gb/s,7.2K rpm,3.5-Inch(3.5-Inch Drive Bay)	290

智能行为分析服务器	支持 32 路前端实时视频流接入，通过配置一定的智能分析规则，输出异常事件报警及分析数据，其中异常事件检测包括绊线入侵检测、区域入侵检测、人群聚集检测、物品检测、未带安全帽、烟雾明火识别、离岗检测、跌倒检测等事件类型。	2
视频分析服务器	1)处理器：2 颗多核处理器，主频≥2.2GHz，缓存≥35MB； 2)单台配置不少于 2 张 GPU 卡，最大可支持 6 块 GPU 卡； 3)内存：不低于 128GB,采用 DDR4、2666MHZ 及以上规格，支持内存扩展； 4)配置≥2 块 1.2TB 硬盘 5)≥2 个万兆/千兆自适应网口 6)支持人脸图片流检测分析，支持性别、年龄段、表情、眼镜、胡子、口罩等属性 7)支持 200 张/秒人脸小图。 8)支持按性别、年龄段、抓拍时间等对历史抓拍人脸图片进行检索与导出。 9)支持 200 万黑/白名单库总容量。 10)单台支持 20 亿条目标/车辆/人体特征数据存储，检索响应时间不大于 3 秒；支持 40 亿条目标/车辆/人体结构化数据存储和检索；单台支持对 2 亿条目标/车辆/人体特征数据进行检索，检索响应时间小于 3 秒；11)支持对历史录像进行分片并行分析； 12)分析业务包括：目标特征识别、车辆特征识别； 13)管理和业务服务共享统一的虚拟化资源;在一台实体服务器虚拟化后的多台逻辑服务器上,支持部署不同功能以及数量的存储、转发、智能分析、检索服务模块；	2

报警子系统

系统设计

报警子系统由前端、报警主机及辅助设备、传输网络和综合管理平台组成。整体的系统架构示意图如下：

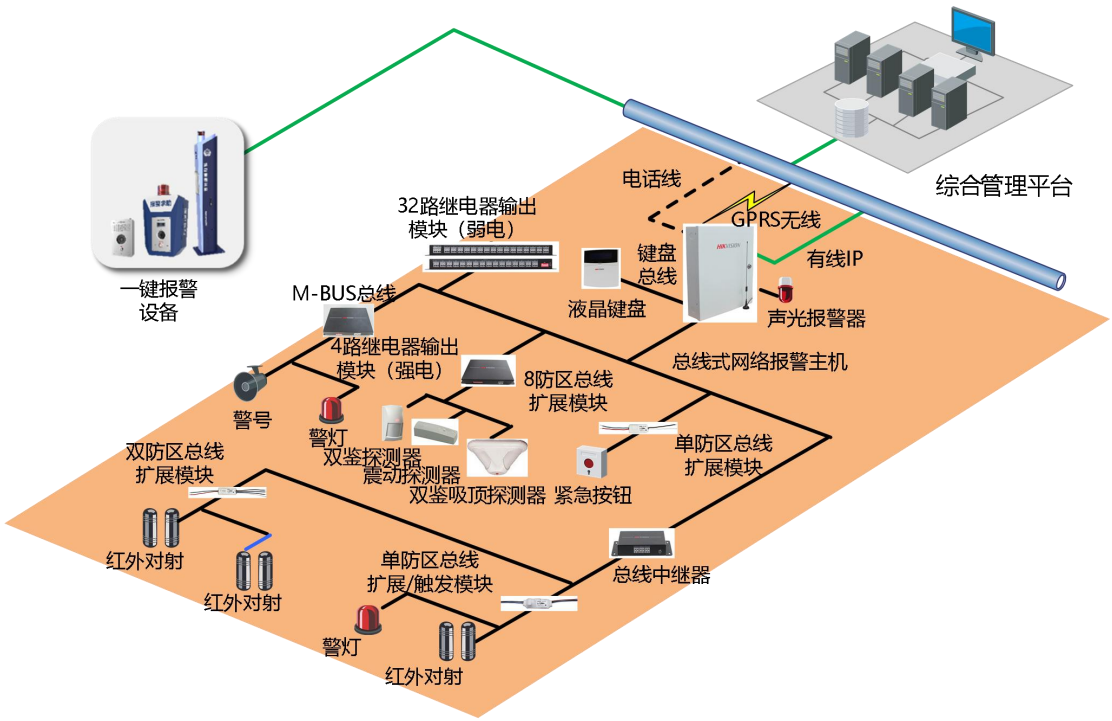


图 5- 64 报警子系统架构示意图

前端：

报警前端设备主要包括各类探测传感器、紧急报警设备等，主要用于探测和触发开关量报警信息，并将该信息传输至报警主机。

1、探测传感器

主要包括双鉴探测器、震动探测器、红外对射探测器、被动红外探测器、玻璃破碎探测器、紧急按钮、烟感应探测器、燃气探测器和其他探测器等。

2、紧急报警设备

主要包括、一键报警箱、一键报警盒等设备，通过按下紧急按钮实现报警信息上报。

报警主机及辅助设备

报警主机一般包括总线制网络报警主机、网络报警主机和视频报警主机，可根据当前防区回路电压范围以及布防情况，分析判断是报警或故障，并对事件进行标记，形成的 CID 格式信号，并传输至综合管理平台。

报警主机辅助设备主要包括报警键盘、继电器、防区扩展模块、遥控器、打印机等。

传输网络

传输网络是支撑整个系统运行的重要要素，负责把前端探测器采集到的报警信号上传到接处警中心。通常采用的传输网络类型包括公共电话交换网（PSTN）、无线网络（GPRS/3G/4G/WIFI）和 Internet 网络等。

综合管理平台

综合管理平台的报警子系统功能模块可实现接警处理、报警设备配置管理、报警信息查询管理等功能，并能与视频监控子系统、可视对讲子系统以及智能一脸通子系统集成联动。

系统功能

报警设备接入管理

系统支持主流报警主机设备接入，并对报警系统硬件设备和报警防区进行设置，自动接收并提示报警事件。

视频复核功能

报警信息上报到平台，平台第一时间显示收到的报警信息，同时按照用户预先定义的报警联动视频关系设置，自动弹出报警发生所在区域的现场图像（包括报警前 N 秒的录像，N 的大小可设定），并进行实时录像。

报警联动上墙显示

根据用户实际应用需要，通过软件配置，可联动报警图像上墙显示，可设置具体哪一路或几路图像上墙显示、上墙画面分辨率、上墙的具体位置等参数。当报警发生时，相关图像自动在显示屏上的指定位置进行实时显示，监控中心工作人员可实时掌握报警点的视频图像信息，或者是报警点周围的环境信息。

报警联动对讲

系统可设置特定点位的报警与附近摄像机（带对讲功能）进行对讲联动，实现监控中心与前端基于音视频的连接。

报警联动声音

系统支持本地语音输出，即在报警发生时，可触发监控中心本地输出多种不同的报警声音或警铃，声音文件可自行设定或录制，在监控中心使用声音提醒，效果会更好。

报警联动电子地图

本平台支持高德、谷歌电子地图系统，可添加用户点、视频监控点、防区点，当收到报警信息后可自动弹出报警所在点位，并以动画形式闪烁提示。

事件查询

系统可根据事件类型、事件源以及时间段等条件对报警事件进行查询，查询结果包含准确的事件发生时间和详细的事件描述信息。

智能巡查子系统

系统设计

巡查管理子系统主要由以下几个模块组成：

1、组织资源模块：

可对巡查设备和巡查区域进行导入和管理，通过场景元素与设备元素的后台软件关联结合，将场景与设备进行有机展示。

2、人员管理模块：

可自由对人员进行添加、修改、删除，并且可添加人员基本信息，部门属性等。可对人员进行角色分配，以确定不同人员的权限。

3、任务管理模块：

可根据日常巡查流程，生成定制化巡查模板；可对巡查任务按状态进行分类，并与巡查人员智能关联；可将巡查设备与巡查任务关联，自动保存上传的巡查数据，并智能表单输出。

4、巡查管理模块：

可对巡查地图进行可视化管理，地图可添加巡查设备、摄像机、传感器等实物元素，并融合属性数据在地图上直观显示；可在巡查地图上直观查看巡查任务状态、巡查设备信息等。

系统功能

巡查任务定制管理

管理人员可根据实际巡查任务情况通过巡查模板创建巡查任务，巡查任务可分为多种：如抢修模式，多人任务模式，单人任务模式等。另外还可指定巡查路线和巡查人员，优化巡查线路，提高巡查效率。

巡查任务自动下发

巡查任务可自动下发到对应人员账号，在移动单兵手持终端 APP 内自动生成巡查任务。

园区一脸通子系统

系统设计

园区一脸通子系统将人脸与园区考勤、访客、门禁、消费、轨迹等子模块有机结合，进而由人脸代替钥匙、卡片、RFID 设备，配合电脑，实行智能化管理，有效的解决了传统业务的多种不足，其强大的扩展功能更是会给人们带来意想不到的方便。本系统的实施将有效保障智慧产业园区内的人、财、物的安全以及内部工作人员免受不必要的打扰，提高园区管理的安全可靠性，并且提升生产效率，为智慧园区建立了一个安全、高效、舒适、方便的环境。

系统主要由前端设备、后端设备、传输网络与管理中心设备组成。

前端设备由人脸门禁设备、人脸抓拍相机、门禁控制器、后端人脸比对服务器、通用服务器、传输网络层、综合管理平台软件等组成，主要负责采集与判断人脸身份信息与相应权限，结合各子系统对人脸信息的权限设置，如进出、考勤、消费、黑名单布控、轨迹定位等。传输网络主要负责数据传输，前后端设备与管理中心之间的数据通讯。管理中心负责系统配置与信息管理，实时显示系统状态等，主要由管理服务器与管理平台组成。

系统功能

园区一脸通子系统实现一张人脸通行整个园区的功能，脱离了传统的卡、RFID 等。可实现无纸化访客、巡查地图任务显示、图片/视频附件上传、实时视频语音对讲、任务自动刷新提醒等功能

园区交互会议子系统

建设内容

本次项目，拟新建 1 套高清视频会议系统，建设需求如下：

1. 统一核心设备（视频会议管理平台、视频会议多点控制器 MCU、视频会议终端）的品牌，实现灵活、便捷的会议管理，提高会控效率，减小多级会议管理员的运维压力；

2. 多点控制单元 MCU 具备混速、混协议、混图像格式的全适配功能，具备大容量接入能力，满足现有不同会场终端接入，实现全网高清视频会议的召集；

3. 整套视频会议系统采用国际标准、国家标准通信标准，须保证行业内设备的兼容互通，采用保持国际、国内的领先性，并且支持未来相关业务的拓展需求。

4. 统一会控管理平台，可将新增视频会议终端同时管控。

系统应具备较强的互通兼容能力，能够在不增加设备的条件下与国内主流厂商实现高清音视频、双流互通。

大型会议室设备部署

本次项目后续根据实际情况建设多个会议室会场，比如通过澄迈综保区主会场与金盘多个分会议场进行联通，为视频会议网络质量，采用园区之间的专线网络环境。

本次在澄迈综合保税区和金盘综合保税区建立 2 间大型会议室。

根据本次视频会议系统的建设，为大型会议室部署 1 台超清分体式终端用于视频编解码；部署 1 台高清摄像机用于拍摄会场整体画面，可搭配三角摄像机支架或者壁挂支架使用，部署 1 台阵列麦克风级联，用于捕获会议发言人语音及环境声音；同时单位根据需要自行配置大屏幕液晶电视、双屏电视（支架）、投影仪等设备。

所配分体式超清终端具备 H.265 编解码能力，支持 H.264 HP、H.264 BP 等技术；SRTP、TLS、HTTPS 等多重安全加密措施；抗网络丢包，在网络丢包率高达 20%情况下，能够确保良好的视频图像效果。

所配全高清 PTZ 摄像机,需支持 12 倍光学变焦，支持 HDMI2.0 视频传输。

所配阵列麦克风，支持 360° 6 米拾音，内置噪声抑制、自动增益处理和回

声处理技术，48KHz 采样率，全频语音，支持双声道立体声，可高清晰记录和传播全程音频信息。

小型会议室终端部署

根据本次视频会议系统的建设，考虑到会议室的场景构造，为各个分会场配置会议一体机智慧屏。

智慧屏需具备集智能书写、极清投屏、视频 会议、开放办公应用为一体的智能终端产品；设备由编解码器、内置摄像机、阵列麦克风、扬声器、65 寸触控屏组成。内置电子白板，支持本地和远端双向远程协作；选配 OPS 模块，可扩展 Windows 操作系统；设备支持 HarmonyOS 或 Android，内置云会议，硬编解码，一键激活，支持 H.265 高清视频会议，4K 数据辅流，60fps 超高帧率，支持网络自适应，视频 30%、音频 80%抗丢包。智能导播功能：支持发言人跟踪，自动显示发言人特写画面，自动呈现最佳会议视角。内置高频应用，支持自定义首页应用，应用市场等，满足大屏应用适配。内嵌加密芯片，支持 H.235、STARTTLS、TLS 和 SRTP 加密，支持国密、安全启动、TEE（可信执行环境）。

系统设计原则

1、先进性原则

- 系统严格遵循国际标准、国家标准和国内通信行业的规范要求；
- 需符合视频技术以及通信行业的发展趋势，并确保采用当前成熟的产品技术；
- 所有的系统采用最先进的技术，确保今后相当长的时间内技术上不会落伍。

2、开放性原则

- 必须完全符合H.323和SIP标准框架协议；必须采用业界标准的视音频编解码协议；
- 必须采用开放式标准设计，兼容标准的视讯系统和设备，确保可与其他厂家标准的产品有效互通；
- 满足今后的发展，留有充分的扩充余地；
- 建议选择国内主流通信厂家的设备，确保产品得到持续的技术支持和可

靠的服务。尽可能避免选择小厂家的以及采用非标准协议的设备。

3、可靠性原则

- 确保系统具有高度的安全性，不易感染软件病毒；
- 对工作环境要求较低，环境适应能力要强；
- 系统设备安装使用简单，无需专业人员维护；
- 系统需要满足7×24小时无人职守方式稳定的工作。

4、投资最优化原则

综合考虑视讯系统的性能和价格，最经济最有效地进行建设，性能价格比在同类系统和条件下达到最优。

系统要求

安全性

网络安全

随着网络技术的发展，互联网攻击也变得越来越频繁。如何在频繁复杂的网络攻击下，保证视频会议系统的安全性，成为客户在购买视频会议系统时需要重点考虑的一方面。视频会议系统应针对不同类型的网络攻击给出完整的安全解决方案。

系统安全

为保证视频会议系统解决方案的安全性，应满足国内和国外的安全标准，如TCSEC、ITSEC、ISO 17799、ITU X.805等，并借助在成功运作的网络和设备的安全运营经验，针对系统分层提供安全解决方案。

多重加密

在H.323组网时，系统支持H.235信令加密与AES媒体流加密技术，在SIP组网时，支持TLS信令加密和SRTP媒体流加密技术，提供端到端、端到系统侧、多点会议等全网全业务信令，媒体流的加解密方案，极大的保证了会议的安全性，充分保障用户使用安全。系统需支持第三方加密机方式，支持防火墙加密，支持路由器和交换机加密。

稳定性

成熟的协议标准

本次项目所采用的产品，应采用成熟的协议框架及标准视音频编解码协议。

成熟的平台产品

本次采用电信级产品设计原理。

完善的备份机制

结合多种先进技术、充分利用网络和软硬件资源，提供多种系统应急备份方案供。优秀的应急备份方案，体现在备份切换智能化、执行自动化、端口资源颗粒化，具有无需人工干预、资源充分共享、会议状态可恢复、切换时间短等特点。多种应急备份机制完全可以应对视频会议中 MCU 和终端侧可能出现的各种类型的故障和问题，为会议应用保驾护航。

车辆通行管理子系统

方案概述

企业园区停车场服务是服务的重要组成部分，是企业园区综合管理运营的难点问题。目前，驾驶人员具备停车难、体验差的痛点，运营企业成本高、效益低，需要通过无人值守、智慧运营的方式，提高整个停车场的管理效率。

建设出入口停车场管理系统具备对临时车辆进行权限放行和对固定用户进行认证管理的功能。系统采用视频识别进出场管理方式，由抓拍相机、道闸、停车场管理平台、云平台、管理电脑等组件构成。

方案架构

通过前端抓拍摄像机采集识别获取车辆信息（车牌、车型、车系、车标），利用网络将车辆信息数据发送至后端管理中心，对理出场车辆信息数据比对，确保车辆的进出有据可查、进出可控，确保停车位的合理利用，加强出入口的高效和安全管理。

系统功能

出入口管理系统

出入口管理系统采用视频识别进出场管理方式，出入口管理系统通常设置在地面车场出入口、地下车库出入口等处，对所有临时和固定车辆开放。通过前端车牌识别相机抓拍车辆图片及识别车辆车牌号，利用网络将车辆图片及车牌号等数据发送至后端管理中心进行存储，及车牌号比对，确保车辆的进出有据可查，确保车辆的进出可控，确保停车位的合理利用，加强出入口的高效和安全管理。

系统应用流程

入场流程

车主驶近停车场附近区域，查看余位指示屏，有足够车位时，车主驶向停车场入口；车辆驶入入口抓拍识别区域，触发车牌识别相机抓拍车辆图片，及识别车辆车牌；车牌识别相机将抓拍图片及识别的车牌号等信息上传管理平台，实现车辆入场管理

支付功能

本次系统围绕停车场出入口无人值守收费进行设计，系统建成后可大大减少停车场人工管理成本，及提升车主停车支付体验，具体实现功能如下：

自助缴费机支付

APP/微信公众号支付

支付宝 APP 支付

出口自助扫码支付

中央服务台人工收费

车位引导及反向寻车系统

新建系统包括车位引导和反向寻车两大业务部分：

车位引导：车位引导系统是通过部署车位检测器，检测车位的状态，并同步给管理平台；车位引导屏从管理平台获取关联区域相关车位检测器检测信息实时更新区域余位信息，实现车位引导；针对部署有车位指示灯的室内停车场，指示灯可通过车位状态显示红绿色，车位指示灯显示红色时，表示车位检测器所覆盖范围内无空车位，显示绿色时，表示车位检测器所覆盖范围内有空车位。

反向寻车：反向寻车系统通过部署视频车位检测器识别车牌确定车辆位置，并在停车场内的各个重点人行出入口部署反向寻车机，车主可在寻车机上通过车牌号、车位号、停车时间段、无牌车四种查询方式查找自己的车辆，系统会基于地图模式为车主实时规划出寻找爱车的最优路线。车主也可以通过手机 APP 或微信公众号，在手机端实现室内停车场一键寻车、实时导航。

蓝牙定位导航寻车系统

蓝牙定位寻车系统凭借强大的技术实力，创造性地采用了新型系统架构；整个系统由视频车位检测器、车位引导屏、终端管理盒、反向寻车机、蓝牙定位模块、手机客户端、控制电脑和管理平台组成，大大简化了系统组件，防止了组件过多来带来的系统臃肿问题，又降低了系统对管理中心的依赖程度，使系统的应用更为灵活多变。其中视频车位检测器根据不同型号可以分别同时管理 2、3、6 车位，适用于地下停车场不同车位场景，同时，检测器采用创新型的网络级联供电，极大程度的节省了系统建设成本。

立体车库车位引导及反向寻车系统

室内车位引导及反向寻车系统凭借强大的技术实力，创造性地采用了新型系统架构；整个系统由前端检测设备（视频车位检测器、停车场终端管理设备、立体车库无线超声波探测器、立体车库超声波节点控制器、立体车库无线车位指示灯）、诱导及寻车设备（室外余位显示屏、室内车位引导屏、、反向寻车机、蓝牙定位模块、云端定位服务、手机客户端）、以及后端管理设备（控制电脑和管理平台）组成，大大简化了系统组件，防止了组件过多来带来的系统臃肿问题，又降低了系统对管理中心的依赖程度，使系统的应用更为灵活多变。其中视频车位检测器根据不同型号可以分别同时管理 2、3、6 车位，适用于地下停车场不同车位场景，同时，检测器采用创新型的双网口手拉手接线及 POE 供电，极大程度的节省了系统建设成本。

室外车位引导系统

车位引导系统是通过部署地磁车位检测器，检测车位的状态，并同步给管理平台；车位引导屏从管理平台获取关联区域相关车位检测器检测信息实时更新区域余位信息，实现车位引导。

防疫绿码管理子系统

方案概述

随着疫情防控进入常态化，工作生活节奏越来越快，“健康码”也愈发成为大家日常出行的标配。在疫情防控和复产复工中，“健康码”可以实现高效率的人员流动管理，在办公楼、商场、地铁、火车站等人流密集的地点提高过检效率，

避免过多的人员接触和聚集。

本次项目通过安装人脸测温门禁一体机、人行通道闸机（可选）、人证核验一体机、综合管理平台等设备，当人员出入时，人脸测温门禁一体机实时抓拍人脸建模比对、上报人员信息到综合管理平台，综合管理平台调用健康码数据接口实时获取健康码状态，下发人脸测温门禁一体机显示健康码信息，实现绿码通行，红黄码禁行功能。

系统功能

无感测温

利用红外非接触式体温检测+人脸识别，降低交叉感染风险，提升通行效率，节省人力、物力。

健康码筛查

平台软件对接当地健康码数据库，可实现快速健康码筛查，有效杜绝健康码冒用、截图等行为，实现自动预警机制。

全天候监测

全天候实时监测体温、健康码状态数据，适用于企业、社区、学校、医院等出入口多种场景。

过程数字化

结合管理平台，实现全过程体温、人脸、健康码数据上报，助力监管部门疫情防控。

快速回溯

通过平台软件可实现对体温、人脸、健康码历史检测记录回溯，潜在病患大数据分析。

一键报警子系统

方案概述

1、一键报警应急系统由前端一键报警设备、监控管理中心和传输网络构成。

2、前端一键报警设备主要包括报警箱、报警盒及联动摄像机，报警立柱可

以扩展球机、雷达测速提醒、无线等模块，根据每个现场不同的环境选择不同的设备和模块。

3、监控管理中心配置有报警应急指挥平台、大屏显示系统等系统核心部分。通过报警应急指挥平台终端，采用大屏显示的方式，对监控点位的视频图像进行轮巡和切换显示。收到报警时能够联动声音报警，同时在客户端或大屏上弹出报警人视频图像和周边视频图像，处警人员可通过麦克风和音箱设备与前端一键报警设备进行语音对讲，对警情进行及时有效的处理。

4、前端报警设备可通过网络进行 24 小时存储，可对报警对讲过程全程录像录音，监控管理中心可以查询查看历史视频图像资料。

系统功能

在一张图上展示摄像头、报警设备等资源位置信息，并支持事件上图、资源图上搜索，资源图上调取等功能。

本产品支持谷歌、高德、天地图、PGIS、百度地图、ArcGIS 平面地图等 4 种底图方式，可根据项目情况进行合理选择底图形式。

基于一张图以分图层的形式展示摄像头、报警设备等位置信息。

图上视频预览：支持图上调取摄像头实时视频画面；

事件定位及处理

实现事发地点在 GIS 地图上的定位，提供单事件、多事件定位功能。有助于调度人员了解事发地点周围信息。

指挥联动

支持报警联动抓图、报警可视对讲、报警视频联动弹窗、语音提醒、短信提醒等报警联动功能；

地图资源搜索

支持根据输入名称和地图图层搜索地图上资源点位信息。

支持搜索结果的分类列表展示。点击搜索到的相关资源，即可查看相关资源的详细信息；

支持对搜索的视频类资源一次打开多路视频。

地图基本操作

提供测距、测面积、框选、自定义标绘、地图配置管理、地图基础操作、图层控制、综合标绘等地图操作小工具。

视频调度

支持主流视频厂家标准的平台对接和级联能力，可汇聚下级平台或汇聚入上级平台，满足建设共享平台的场景。支持以国标（GB/T 28181）、ONVIF 等标准协议接入 IPC、DVR/NVR 等监控视频资源。实现所有视频资源的统一管理与视频点播。具备视频调取、录像、录像下载、上墙、轮巡、语音对讲、设备报警、智能报警、地图、视频分享等功能；

呼叫转移

可提供呼叫转移功能： 遇忙转移、无人应答转移 、无条件来电转移 、不在线转移。

忙音提醒

支持接警中心的调度台处于通话中时系统可进行忙音提示，具体为"接警中心忙，请等待“，播放时长 30 秒，直至接听或前端主动挂断。

报警联动

支持报警柱、报警盒等告警终端报警；

将报警源与视频监控绑定后，支持 1-4 路视频监控绑定。绑定视频后，收到配置的报警源后，能够联动弹窗，弹出的视频窗口中能够自动播放配置的视频；

报警管理

支持本级及下级报警前端的报警记录、任一报警记录音视频查阅及同步回放，支持按照报警开始时间、前端报警设备名称进行报警查询；

支持历史报警列表展示，内容包含平台所有的历史报警，能够查询到报警对应的操作：接警和消警；消警操作可以查询到消警原因。

支持查看事件列表，查看事件中的音视频和聊天记录；

报警回溯

支持对报警进行录像、抓图回溯，对前端报警设备的视频进行全程录像，可实现调度过程中语音文件的存储、查询等管理服务。

无人机远程监控系统

系统概述

结合海口综保区园区车辆多，管理手段少等现状，按照好用管用实用并重的原则，在园区的围网，海关监管区域，根据敏感区域管控的核心，结合无人机巡检功能，实现对查验货运车辆超时停留的异常行为智能管控以及相关场所无人机巡检可视化展示。

建设目标

本项目租赁无人机自动飞行并提供远程喊话能力，为实时监控及后续处置提供智能手段，创新场所监控和处置情况的展示方式，从而有效提升场所管控的精准性和有效性，防范执法和廉政风险，化解内外矛盾，实现管得住、通的快，营造良好的内外执法环境。核心目标有以下几点：

1．无人机自动巡检

可设置无人机巡检路线，针对综保区围网区域进行自动巡航并实时回传现场高清视频画面。

2．无人机定点监控

出现中控车辆或者堵车等异常事件，系统可设置或者手动输入坐标参数，无人机自动飞抵现场进行实时监控。

3．查验车辆管控

监控指挥中心发现货运车辆超时停留，后台可以设置无人机飞行路线，无人机飞抵现场后加强监控并可喊话驱离。

园区电子围网子系统

系统设计

本方案通过在周界围墙部署智能警戒摄像机，当检测到异常情况时，前端摄像机声光报警进行威慑，同时将报警信息传送至监控中心，提高保安处理效率，保障安全，减轻管理人员的工作负担。

点位部署：

点位名称	需求摄像机类型								点位数量汇总	立杆要求
澄迈保税区									0	
周界围墙	周界防护摄像机							150	150	新建 75 根
汇总								150	150	

系统特点

深度智能，精准检测

前后端产品均采用深度学习算法，相比传统绊线、区域入侵报警，能准确过滤因动物经过、光影变幻等造成的环境干扰因素，进一步降低误报率。

实时警戒，声光告警

当发生异常情况时，联动声光告警震慑入侵者，同时利用客户端弹窗、抓图等功能，将报警信息同步监控中心，便于保安及时采取措施，阻止危险事件发生。

远程对讲，化解险情

当发生异常情况时，保安人员通过双向语音对讲功能，对非法闯入人员远程喊话示警驱离，在确保社区安全的同时，减轻保安的工作负担，提高安保效率。

一键撤防，消除告警

当告警事件解决后，需及时消除告警声音，尤其在夜间会存在噪音扰民现象。智能警戒产品可通过 APP 一键远程撤防并消除告警，简单便捷，降低安保人员的操作门槛，减少因夜间突发报警引起的业主投诉。

卡口 LED 屏升级改造

对现有电子卡口 LED 屏升级改造

海口综合保税区目前主卡口的基本情况：

1）4 进 4 出 8 条货车通道；

2）1 进 1 出 2 条行政通道；

3）1 条查验通道。

保税区主卡口

针对以上需求，需要对目前主卡口 LED 屏进行升级，详细如下表：

海口综合保税区主卡口改造设备需求

序号	设备名称	设备型号	参数	数量	单位
1	通道 LED 引导大屏	P10 户外屏	1、驱动器件：恒流 IC 2、驱动方式： 1/4 3、刷新频率：≥380Hz；帧频： ≥60Hz 4、灰度/颜色：显示 66536 颜色；亮度：≥5000cd/m2 5、亮度调节方式：软件 16 级可调 6、显示内容：文字、图片、视频、时钟、日期、温度、	台	10

			湿度等 7、控制系统采用：网口或USB传输（可选） 8、平均无故障时间：≥10000小时；寿命：5万小时 9、平整度：任意相邻像素间≤0.5mm；模组拼接间隙＜1mm ； 10、均匀性：像素光强、模组亮度均匀；盲点率：＜0.0002 11、开关电源负荷：5V/40A、5V/30A 12、计算机显示模式：1024×768 13、有效通讯距离：网线100m（无中继），多模光纤500m，单模光纤20km		
2	通道LED引导大屏安装杆件及基础笼	定制	镀锌圆钢/方钢定制； 管壁：≥3mm； 基础笼：定制；	套	10
3	LED引导屏管理软件	PF-ICEDA V1.0	1、编辑LED引导屏显示内容； 2、控制LED引导屏显示编辑好的内容。	1	1

安防综合管理平台

园区安全保卫涵盖园区内部人员和园区基础设施等多种元素，因此，如何集合所有相关信息和数据，做出最有效的保卫园区安全和顺利运行的决策，园区管

理部门需要最先进和创新的多层次安全监控和管理情报系统，而且要实时跟进所有环境和元素的变化。智慧园区综合安防管理系统，其核心就是通过创建园区全境安防智能整体解决方案，使园区主管部门具备实时、准确的情境意识，实现先进的园区安全集成。安防系统集成并融合不同类型的实时传感器和数据采集子系统，可在固定和移动等各种模式下运行并适应各种环境条件，为所有的使用者和相关方提供实时的动态数据信息和决策操作平台。

1)系统可通过一套统一的综合管理平台，将不同功能的安防子系统进行系统融合，可实现对各类系统监控信息资源的共享和优化管理，具有对各子系统进行数据通信、信息采集和综合处理的能力，可生成优化管理所需的相关信息分析和统计报表。

2)视频调阅是安全防范和生产监控体系的基础，可有效对各区域实行实时监控，整个安防监控系统的重点在于对人员、车辆、物品、产线、实验室等的实时监控，防患于未然。

智慧路灯系统

面向智慧路灯基础设施，实现路灯的智能管理，并构建道路 WIFI 服务能力，提供由路灯承载的视频监控+各种智能分析以及资源监测的能力。通过统一路灯的承载与服务方式，实现园区的物联网体系的建设。

建设园区信息化网络管理平台，为后续无线园区奠定基础。以节能照明为基础，进行园区亮化工程建设，实现道路路灯智能控制管理。建设园区信息发布系统，通过智慧路灯上的 LED 显示屏与音柱，实现相关资讯信息的推送与发布。通过视频监控以及物联网信息采集设备，对视频图像以及环境数据等信息，进行采集，通过不同的算法对数据资源加以分析，实现园区的智能化。

施工要求

施工原则

1、质量：严格按照设计要求，严把质量关，保证在项目施工过阶段的质量要求。

2、安全：安全包括人身安全和设备安全，要求施工人员在施工过程中注意安全，遵守各项安全操作程序，在施工中选用的电气设备和材料要能满足设计要

求。

3、可靠：不仅要求设计时采取必要措施，而且在施工时必须保证各个环节的可靠性。

4、便利：在安装施工中，要考虑以后运行和维修的便利，并考虑到有发展和更新的可靠性。

5、经济：施工中在能满足设计要求的前提下，保证系统安全可靠地运行，要注意推广使用新技术、新工艺、新材料、新机具、提高安装质量，提高效率，提高经济效益。

6、美观及工艺：施工中每种设备的安装要和周边整体环境相互衬托，使之尽可能保持协调、对称和美观。

施工工艺及设备安装

工程中各专业交叉施工，合理安排专业施工工序，缩短工期，提高施工质量，保证安全生产。

（1）基础制作

基础严格按照设计方案进行，横竖必须要正，水平居中，防雷接地系统阻值小于 10 欧。

（2）灯杆安装

每根灯杆配备编号，灯杆水平牢固安装。灯杆的安装需要吊车来配合安装，然后底部装上法兰盘加上螺丝来固定，还可以根据螺丝垫圈等来调节灯杆的水平位置。

（3）设备安装

安装时，设备要注意水平安装，不能斜放，要按设备厂家的安装规范去施工；设备应与地面平等高度符合人体学，如已安装但无法固定，特殊情况下可安装额外订制的固定架。

智慧路灯系统布局原则

智能 LED 路灯按照中华人民共和国行业标准，《CJJ45-2015 道路照明 LED 应用技术规范》进行布置。灯杆间隔按照 30 米一个进行部署。

级	道	路面亮度	路面照度	眩	环境比

别	路类型	平均亮度 L_{av}（cd/m^2）维持值	总均匀度 U_0 最小值	纵向均匀度 U_L 最小值	平均照度 $E_{h,av}$（lx）维持值	均匀度 U_E 最小值	光限制阈值增量 TI（%）最大初始值	SR 最小值
	快速路主干路	1.50/2.00	0.4	0.7	20/30	0.4	10	0.5
II	次干路	1.00/1.50	0.4	0.5	15/20	0.4	10	0.5
III	支路	0.50/0.75	0.4	—	8、10	0.3	15	—

本次智慧路灯全部布建在老城园区，替换原有灯杆为智慧灯杆共计 200 套，详见下表：

海口综合保税区-老城园区智慧灯杆布建表					
安商路 436m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
1	智慧灯杆	套	18	8	
亲商路 436m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
2	智慧灯杆	套	18	8	
乐商路 436m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
3	智慧灯杆	套	18	8	

海澄二路（西）1385m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
4	智慧灯杆	套	55	20	
惠商路 706m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
5	智慧灯杆	套	28	10	
旺商路 270m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
6	智慧灯杆	套	11	6	
富商路 436m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
7	智慧灯杆	套	18	8	
强商路 706m					
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
8	智慧灯杆	套	28	12	
序号	名称	单位	现有灯杆数量	替换为智慧灯杆数量	备注
10	合计	套	469	80	

另外新增 4 个 12 米智慧灯杆满足全景拍摄的需要。

智慧消防系统

在移动互联网、大数据、云计算等科技不断发展的背景下，通过建立“智慧消防物联网云平台”，将企业所管理的建筑楼宇的消防设施实现远程联网监控，提高消防监督和灭火救援效能，提高企业的消防安全管理水平。

本系统能将消防设施在运行过程中出现各类故障和告警信息及时发送给维保人员，以便维保人员及时上门维修，消除安全隐患，确保消防设施正常运行。

同时，系统记录了消防设备各类故障和告警信息，以及消防设备的维修信息，联网单位能够查看维保工作的统计信息，如维保的次数（可以按时间段统计）、当前消防设备的完好率、维保工作的及时性分析等，通过这些数据，可以对维保工作进行客观公正的评价，通过量化指标实现对维保工作的监督管理，也可以对消防设施的产品质量做出客观评价。

将消防联网系统的信息在一张总图上显示，使公司领导、各级消防主管人员对所管理的楼宇建筑物内的消防设备运行情况能一目了然。包括火灾报警控制器数量、各类消防部件（烟感、手报等）总数、当前设备完好率、完好率趋势分析图、告警趋势图等，在提供大屏可视化渲染效果的同时，为用户的业务决策提供有力支撑。

系统主要功能

物联网云平台软件功能

物联网云平台软件基于 WEB，功能主要包括如下：

消防系统运行情况一览图

将消防联网系统的信息在一张总图上显示，使公司领导、各级消防主管人员对所管理的楼宇建筑物内的消防设备运行情况能一目了然。包括火灾报警控制器数量、各类消防部件（烟感、手报等）总数、当前设备完好率、完好率趋势分析图、告警趋势图等，在提供大屏可视化渲染效果的同时，为用户的业务决策提供有力支撑。

实时报警功能

系统收到报警信息后，显示报警点信息（编号、名称、报警类型、位置、时间等），通过声光告警提示值班操作人员，并对报警点进行定位，在楼层布局图中显示具体的报警对象，也可以将建筑物位置在 GIS 地图上定位。

应急预案管理

可以根据发生事件的具体条件，直接调用预案系统的预案信息，从而实现预

案与应急事件处理的联动。在联动过程中，预案系统可以根据事件响应级别及类型，自动匹配相关预案，然后启动相关预案。

消防给水监测

消防给水监测采用图形化的监测表单样式，实时展现每个压力变送器、液位变送器当前的数值，并在二级页面展现变送器历史趋势图，可以针对每个变送器设置上下限阈值，超出阈值即触发报警。

火灾联网报警子系统

火灾报警系统利用用户信息传输装置实时监测消防主机运行状态，系统可以支持 200 余中消防主机品牌类型，实时监测消防主机运行状况，将火警、故障、反馈、监管远传至监控中心。

联网单位资料数据管理功能

对联网单位的基础数据进行管理和维护：

（1）联网单位基本信息：

联网单位联系人基本信息，包括联系人姓名，联系人身份，手机号，其他联系方式；

建筑物信息，包括建筑名称，建筑结构，楼层数；

（2）消防设备基本信息：

每个种类的消防设备的主机型号、生产厂家，消防部件（烟感、温感等）的数量，以及消防部件的类型、编号、名称等；

（3）消防图纸：

楼层编号，楼层名称；房间编号，房间名称，描述信息等。

消防设备（包括消防主机系统和消防部件）在建筑物楼层布局图上安装位置等；

图形制作功能

系统中包括大量的消防设备楼层布局图，系统设计了图形制作工具，完成图形数据输入

安全管理

（1）操作人员账号管理

根据企业的管理模式，将操作人员分成不同的组，具有不同的权限。每个人都建立账号和密码。

（2）权限管理

对不同的角色分配不同的权限，角色权限包括菜单权限、功能按钮权限和数据权限。菜单权限是允许用户是否能看到某一菜单；功能按钮权限是指增加、删除、修改、查看等按钮操作权限；数据权限是指能看到的数据范围。

数据分析

通过对数据库的各类信息进行数据分析，为单位领导、消防主管人员提供信息查询服务，为单位领导分析企业消防安全水平和进行决策提供依据。统计分析有三类数据展现形式，即：汇聚分析、列表、图表，具体包括如下：

提供任意时间段内告警信息如火警、误报、故障、动作、隔离等信息的统计，报表打印。

可以按每日、每月显示告警信息总数、设备完好率等指标，以评估本企业的消防安全水平。

根据消防设备的完好率、告警信息等，对消防维保工作进行评价；

视频联动监控功能

可实现与视频监控系统的联动，当联网单位发生报警时，可以自动切换到相应的摄像机，直接获得现场的图像，效果直观，可实现全方位消防监控管理，极大地提高了报警效率和监管水平。

系统自身运行状况监控功能

系统由运行于不同地理位置的物联网设备、通信网络多个功能设备组成，因此，系统除了要自动监测各联网单位的消防设备外，对自身的运行情况也能进行自动检测，才能保障系统的安全、连续运行。为了进一步提高系统的可靠性，使得相关人员能够及时知道系统中运行设备出现的故障，发现问题及时处理。这些功能包括：对联网终端工作状态的监测、对通信线路工作状态的监测。

手机微信服务功能

通过手机微信，为联网单位各级管理人员、维保人员等提供各类信息服务功能。可根据管理级别和权限，为不同的用户提供所需的信息。

巡检系统功能

巡检系统由以下几部分组成：巡检点标签、手机 app 软件和服务器端管理软件。

手机app软件

（1）标签读取功能：巡检人员通过账号，登录系统后，直接读取标签。

（2）巡检提示功能：对每个需要巡视设备的巡检路线以及巡视点都进行了详细的标注，巡检人员可以根据提示巡检路线完成巡检工作。巡视提示功能与数据库服务器进行实时通讯，可以实时下载巡检路线表，即时反映巡检点对应设备的工作状态。

（3）设备巡检记录功能：巡检人员可以根据不同的需求，填写设备实际情况，是否故障、故障内容等，上传至服务器。

（4）拍照上传功能：可以将巡检现场拍照，上传至中心。

服务器端管理软件

实现对巡检工作的集中管理，包括增减巡检人员、人员权限分配、巡检点设置、巡检点内容设置、巡检记录查询等功能。用户可以通过互联网访问 Web 站点，为了提高系统的安全性，在操作时，用户必须要通过用户身份确认。

智慧能耗监测系统

通过建设智慧用电云平台，兼顾用电安全和能耗管理要求，实现如下目标：

（1）用电安全隐患监管

对引起电气火灾的主要因素（线缆温度、负载电流、剩余电流等）进行实时在线监测，及时处理电气线路运行中存在的用电安全隐患，预防火灾发生，提高企业用电安全管理水平。

（2）能耗管理

通过合理采集分类、分项能耗数据，准确掌握重点区域以及重要用能设备的能耗以及运行状况；有效指导园区能源管理以及安全运行，从而在业务不断增长的同时，更合理控制能源的使用，提高能源管理水平，为园区节能改造提供科学依据。

系统主要功能

数据采集功能

用电安全数据采集

实时采集用电安全报警数据（漏电、电缆温度等），并将数据上传到云服务中心。

能耗数据采集

能耗数据包括各类智能设备（智能电表、电气综合监控装置等）的遥测量、遥信量、电度量、智能水表等数据。

遥测量（模拟量）主要包括：有功功率、无功功率、电流、电压、功率因素、频率、谐波等。遥信量(状态量)主要包括：断路器位置、事故总信号、刀闸位置信号等。

原始数据的加工处理

数据采集的结果只是反映现场运行状况的基本数据，一般称为生数据，它既缺乏与其它数据之间的联系，也缺乏与同一数据其它采样值之间的联系。系统对接送到的数据进一步加工处理，具体如下：

数据状态的判别，如测量值是否有效、是否超过合理范围、状态是否发生变化等等，并将判别的结果加以保存。

数据计算功能。对于一些有明确计算方法的计算，系统定时对系统中有计算要求的数据点完成这些计算，并保存计算结果。

数据采样间隔

数据采集的时间间隔可以设置，最短时间间隔为 1 分钟。对于具有不同采样周期要求的数据点，在明确了采样周期及采样范围之后，由系统根据要

求完成采样工作，并保存到数据库中。

实时监控

实时能耗数据查看

提供给用户各种实时数据查看方式

实时告警数据查看

查看到本单位所有的实时报警数据数量以及详细报警信息，以便值班人员及时处理，每个告警数据需要操作人员进行确认，也可以一键确认所以告警数据。

历史数据查询

可显示当前存在的遥测点的告警数据、可选择性显示用能设备在某一个时间段中的电能参数的历史曲线。

能耗数据统计

可以按日、月、年统计本单位的用电用水数据，也可以显示某一时间段内的用能数据。

能耗分析

（1）电能数据时比

某个电能数据在不同时间的数据比较

（2）电能数据类比：不同设备的相同类型的电力数据在选择的时间段内的数据比较

基础信息管理

对系统的基础数据进行管理和维护：

（1）基本信息：

- 单位基本信息，包括名称、地址、电话号码、联系人、责任人等；

- 单位联系人基本信息，包括联系人姓名，联系人身份，手机号，其他联系方式；
- 建筑物信息，包括建筑名称，建筑结构，楼层数；

（2）物联网设备信息：

对物联网设备（包括电气综合监控装置、通信网关等）进行管理，包括这些设备的名称、型号、地址编码、通信方式、安装位置等。

对每个物联网设备能够采集的信息点进行管理，包括信息点的名称、量纲、上下限等。

操作人员管理

（1）操作人员账号管理

根据企业的管理模式，将操作人员分成不同的组，具有不同的权限。操作人员包括系统管理员（权限较高，可以看所有的数据）、一般操作人员等。每个人都建立账号和密码。

（2）权限管理

采用不同角色不同权限的方式，角色权限包括菜单权限、功能按钮权限和数据权限。菜单权限是允许用户是否能看到某一菜单；功能按钮权限是指增加、删除、修改、查看等按钮操作权限；数据权限是指能看到的数据范围。

（3）日志管理

对操作人员进行的关键操作，记录进数据库，以便追溯。

智慧查验系统

5G 智能单兵查验

主要包含智能辅助查验、单兵后台协同、单兵录证关联三种基础通用能力，以及基于三种能力基础上构建的货车查验和客车通道查验 APP 应用：

智能辅助查验：提供风险地址识别、违禁物品识别、应税商品识别、外来物种识别、货物标签识别和货物识别六种智能识别能力；

单兵后台协同：单兵指挥调度（基于移动音视频平台、融合通讯调度平台和地理信息平台，提供执法单兵的定位、融合通讯、组呼等能力，让后台监控指挥

人员可以调度现场人员完成应急事件处理），远程查验作业（基于 AR 眼镜提供第一视角视频，海关执法关员通过单兵设备和现场人员互动共同完成查验工作）；

单据录证关联：提供单据视频关联和证据回看功能。

VR 全景查验监控系统

在海口综保区海关查验现场以及公共区域，部署 VR 全景摄像机，通过内部网络进行视频回传，保障视频传输的稳定性和视频清晰度。在综保区监控中心可以通过大屏幕以及 VR 眼镜播放现场 360° 全景摄像机拍摄的视频画面，360° 查看查验现场的实况。同时，配备 VR 眼镜观看现场实况画面，实现沉浸式指挥。

国产化云节点

计算资源需求

海关侧计算资源需求均需要使用国产化硬件，用于满足海关自主可控要求。

系统名称	VCPU	内存/GB	磁盘空间/GB	数量
底座管理面	16	32	600	3
底座数据面	16	32	600	3
应用编排	16	64	400	4
Web 服务	8	16	300	4
微服务	16	32	600	2
集成中枢	16	64	100	2
数据编排	16	32	100	2
流处理	8	16	100	2
数仓服务	16	64	100	2
AI 训练推理	16	32	200	2
AI 接口服务	8	16	600	2
查验辅助	8	16	600	2
电子证据管理	16	64	800	1

充分考虑当前海关、政府针对信息化项目需要充分考虑国产化和维护底层技

术**自主可控、数据安全、资源统一管理和运维**的要求，综合海关侧的网络、安全以及计算存储资源情况，海关基础设施采用全国产化的技术路线，本项目新建边缘超融合一体机基础设施，需要与海口海关中心基础设施云平台形成中心-边缘多级设计。

为满足海关总署基础设施管理规定，海口海关中心通用算力将与海关总署的基础设施云有机融合，将纳入总署统一监管，接受总署统一运维支持。形成总署-海口海关-马村港海关（隶属关）多级计算基础设施体系，系统数据层、应用层实现互联互通，管理层实现上下统一。

本次项目海关侧海口中心通用算力具体对接要求为：作为总署基础设施云平台下属分节点，以资源池的方式接入到总署，接受总署的资源管理和监控。要能实现总署及直属关可调用到资源池中的资源，包括物理资源，虚拟资源的监控和控制，资源下发和回收，资源故障处理等。

服务器存储方案

1)查验超融合服务器：通过计算、存储、网络高度融合的一体机，部署简单，占地面积小，交付快，一体化提供超融合，为马村港海关部署三大应用和视频转码等业务提供虚拟机业务。

从计算维度看，本期通用算力资源需求为 31 台虚拟机，共 416 个 vCPU，计算资源按照 3:1 的复用比进行计算，单台超融合节点配置 2 路自主可控的芯片架构 32 核服务器可提供 2（CPU 数量）*32（单 CPU 核数）*3（超分比）=192vCPU 计算能力，按照 80%的资源利用率（含硬件利用率、虚拟化软件开销、分布式存储软件开销），本期需要超融合节点数量=416/(192*80%)≈3 台。

基于计算存储融合节点数据可靠性考虑，需要做多副本或者 EC 校验，至少需要部署 3 台。因此，海关侧 5G 单兵智能查验系统需要 3 台计算存储融合节点可满足平台对算力资源和可靠性的需求。计算节点部署虚拟化软件，为平台提供计算资源；计算存储节点配置本地硬盘及高速缓存盘，部署虚拟化软件及块存储软件，为平台提供计算资源及存储资源。

2)AI 服务器：通过专用 AI 服务器，提供高性能灵活可配置的 AI 计算能力，对接 5G 智能单兵装备快速实现实时视频流的 AI 分析，并将分析结果实时上报到智慧应用，实现视频从接入到 AI 应用的一站式流转。

本项目需要建设 2 台 AI 推理服务器和 1 台 AI 训练服务器，用于满足 5G 智能单兵查验所需的 AI 算力资源。

网络方案

海关网络系统主要组成内容分为业务网和视频网，综保区海关查验系统建设，需要马村港海关虚拟化基础网络展开相应建设。

1）马村港海关管理网

马村港海关管理网主要包括 2 台业务接入交换机、1 台BMC带外接入交换机、1 台数据视频网闸、若干台超融合节点服务器。

2）马村港海关对外接入局域网

马村港海关对外接入局域网络主要包括 2 台视频业务交换机、2 台视频接入交换机，2 台视频管理存储平台设备等。

信息化基础设施和能力建设方案

机房及配套设施方案

本工程中配套机房工程是整个项目重要基础设施，承担着除部署于省电子政务云之外的、需要在园区内部部署运行的系统及数据，为确保为各类系统、众多设备提供良好的机房环境，根据现有机房情况及整个项目的需求，尽量利旧现有资源进行建设。本工程配套机房工程主要为升级改造，其中升级改造的为“管委会中心机房、海关中心机房及监控指挥中心三大部分”。

根据建设目标，本次 IT 机房优化参考 GB50174 的准 C 级标准进行新机房建设，一方面解决现有机房存在问题，另一方面考虑未来发展。

机柜建设标准及规模

机柜建设是机房建设的核心，也是所有其它设备测算的起点，其它设备测算均依赖于机柜建设的数量和功率。

根据当前机房的情况、海南机房建设普遍功率情况，并考虑未来发展需求，本次机房建设拟建 5KW 机柜 40 个。具体如下：

机房	位置	面积（平	参考建	可提供机	机柜规格

		方米）	设标准	柜数量	（kVA）
管委会中心机房	联检大楼三楼现管委会中心机房	99	准 C 级	20	5
海关中心机房	联检大楼三楼现海关中心机房	75	准 C 级	20	5
合计		164		40	

UPS 方案

本项目中 UPS 服务对象为新建三个机房机柜。其中管委会机房与海关机房各 20 个 5KW 机柜采用模块化 UPS 主机加 12V200AH 电池方式提供服务。安检一机房由于面积受限，选用微模块 10KW 型 DPS 主机提供服务。

暖通方案

因机柜采用封闭冷通道的设计方案，所以对于空调制冷量 Q 需求为室内设备负荷（设备额定功率×同时系数×功率因数）。

空调总制冷量计算 Qt=Q1+ Q2

——Qt 为主机房总热负荷(kW)

——Q1 室内 IT 设备负荷(考虑到设备的同时使用率，Q1=IT 设备总功率×0.8~1)。如果给 UPS 房间配置空调，设备负荷 Q1=UPS 名义功率*0.04+UPS 输出功率*0.06。

——Q2 建筑环境热负荷(考虑太阳辐射、围护结构传热、新风及空气渗透、人员、照明等散热量，取 0.14～0.18kW/m2×机房面积）。

---Qups 为带电池 UPS 的热负荷(kW)Qups=0.04W1+0.06W2

---Qp 为配电系统的热负荷(kW)Qp=0.02(W1+W2)

确定机房的总负荷之后，选择合适的空调容量和台数，使合计总制冷量大于机房总负荷。根据业主要求我们设计在设备服务器主机房配置房间 3 套 80KW 精密空调。

3、设备选型

主机房：Qt=Q1 ×（1+X）+Qups+Qp ；（X 取 10%~20%）

主机房：Qt=Q1 ×（1+X）+Qups+Qp ；（X 取 10%~20%）

Q1 设备总功率 (1+X) Q2 建筑环境热负荷 Q ups 带电池 UPS 的热负荷(Kw Qp 为配电系统的热负荷(kW) QT 为主机房总热负荷(kW)。

所以管委会机房的制冷量 Q1=5*20*0.7*0.95=66.5kw,考虑 10%冗余,取 70kw。海关机房的制冷量 Q1=5*20*0.7*0.95=66.5kw，考虑 10%冗余，取 70kw。

检验一机房的制冷量 Q1=4*4*0.7*0.95=10.64kw，考虑 10%冗余，取 12kw。

根据 n 设计方案，管委会机房的空调设计为 2 台制冷量为 70kW 风冷机房精密空调。海关机房空调设计为 2 台 70kW 的风冷机房精密空调。安检一机房 2 台 12KW 风冷空调

空调为机房精密空调静音型，下送风，单冷功能，压缩机位于室内。

主机房要求完全封闭，不能长时间开门（一般不超过 3 秒）。每个机房设计空调带除湿功能，除湿要求每天除湿量不小于 30L，使用三相电源。

防雷接地方案

本项目采用保护性接地和功能性接地共用一组接地装置的方式,在静电地板下围绕机柜支撑架构建等电位联结带，再将等电位连接带与建筑物接地相连，其中等电位连接带采用截面积不小于 25 平方毫米的铜排。

将机柜、ups 设备等的金属外壳与等电位连接带联结接地。

消防方案

系统构成：本系统由火灾自动报警系统、柜式灭火装置组成。火灾自动报警系统由火灾探测器、气体灭火控制器、声光报警器、紧急启停按钮、防火指示灯及系统布线组成。灭火装置由柜体和灭火药剂组成。

系统工况：系统设计为自动、电气手动、机械手动三种工况

自动工况：即自动探测报警，发出火警信号，自动启动灭火系统进行灭火

电气手动工况：即自动探测报警，发出火警信号，经人工电气手动启动烈火系统执行灭火，该操作在灭火控制盘上实现

机械手工状况:探测报警发出火警信号后,电气系统故障不能执行灭火指令，在七氟丙烷瓶站进行，首先拔去启动装置电磁阀手动启动器的保险，拉下启动手柄，执行灭火

机房智能系统方案

机房智能系统包括 3D 可视化监控和设备能耗管控两部分

改造机房及配套设施方案

根据需求，本次对如下机房进行改造，解决目前机房存在的问题：

机房	位置	面积（平方米）	参考建设标准	现有机柜数量	机柜规格（KW）	建设方式	备注
机房	跨境二期机房	30	准 C 级	8	保持现有不变	整改	
机房	卡口机房	60	准 C 级	11	保持现有不变	整改	

根据现场勘查情况，现有机房改造主要包括如下方面：

1. 走线方式改为上走线，并对现有线缆进行整理
2. 机房监控接入新的智慧机房系统

利旧原有机柜、机房配电、UPS、消防设施。

走线方案

序号	位置	走线方案
1	跨境二期机房	增加部分吊顶走线架
3	卡口机房	机柜顶添加 W 槽作为柜顶走线架，与 W 槽垂直方向采用双层走线架

监控测点方案

序号	位置	测点	备注
1	跨境二期机房	8 个机柜电流电压温度测点，6 个温湿度测点，4 个摄像头	2 个温湿度监控点，4 个摄像头；每个机柜测量电流、电压及机柜出风口温度；
2	卡口机房	11 个机柜电流电压温度测点，2 个温湿度测点，4 个摄像头	2 个温湿度监控点，4 个摄像头；每个机柜测量电流、电压及机柜出风口温度

服务器系统方案

服务器配置原则

服务器设备应满足本项目建设需求，在满足平台建设需求的前提下，尽量采用优化设计，使服务器资源能够满足用户的高性能、高安全可靠、可扩展、可管理等需求。服务器设备应满足以下配置原则：

（1）高性能原则

本项目拟采用的服务器设备，应达到当前服务器设备主流高端性能标准、技术先进，在运行速度、磁盘读写、容错能力、稳定性、监测功能及电源能效等方面具有较高的性能指标。

（2）安全可靠性原则

本项目拟采用的服务器设备，应具有可靠性，满足大型的、有大量处理要求的、需要长期运行的系统部署，并且性能稳定，整体故障率低。

（3）可扩展性原则

本项目拟采用的服务器设备，应具有优秀的可扩展性原则。能及时调整配置来适应业务的发展，使服务器随负荷的增加而平稳升级，保证服务器工作的稳定性和连续性。

（4）可管理性原则

本项目拟采用的服务器设备，应易于操作和管理，对支持标准的管理系统进行有效的管理，实现较低的维护成本。

服务器配置选型

经过对本项目的需求进行分析，可以疏理出本项目中所承载的应用系统主要包括二层架构（应用层－数据库层）和三层架构（接入层－应用层－数据库层）的应用系统。两种应用系统架构在部署时，各层分别需要一个或多个虚拟服务器来承载，虚拟服务器的配置和数量依赖于各层应用的特性来决定。在所有的应用系统中，根据所承载的应用系统分为大访问量应用系统、大计算量应用系统、大数据量应用系统三类。

1、基于 Web 的大访问量、简单处理型应用系统

大访问量应用系统如 WWW 网站等 web 类应用系统，这类应用的特点是业务逻辑简单，不同业务请求互不关联，但请求的并发量根据业务特点不同可能很大。

大访问量应用系统要求对大量互不关联的并发请求进行快速响应。这种情况

下，需要应用服务器有足够数量的线程响应请求，而单个线程计算量不大，因而对单个 CPU 处理性能要求不高，可通过提供足够 CPU 数量或应用服务器数量来满足需求。通过虚拟化技术为大访问量应用系统部署是大量小配置的虚拟机作为应用服务器，多应用服务器工作在负载均衡模式，提升用户使用体验。大访问量应用系统对数据库要求不高，配置一般虚拟机即可满足要求。

2、大计算量的应用系统

大计算量应用系统，这类应用的特点是计算量较大、运算复杂、内存需求大，应用逻辑对服务器计算性能要求高。这种应用系统由于通常应用逻辑的串行性不能实现分布式设计，对于单一应用层服务器要求高，体现为需要配置较高的单一个虚拟服务器，建议配置单一高性能虚拟服务器。因而，该种应用需求的虚拟化技术支撑点是配置较高性能的应用层虚拟机，接入层、数据库层作常规配置。

3、大数据量处理的应用系统

大数据量应用系统，根据数据存储模式不同，可分为文件型和数据库型的系统。

数据库型大数据量应用系统要求较高性能数据库服务器。建议配置强大的数据库服务器，提供足够的 CPU、Memory 及 IO 性能来处理大量的数据，根据应用系统重要级别，数据库服务器可以选用虚拟物理器，应用服务器业务逻辑简单，对配置要求不高，配置一般虚拟机即可满足要求。

文件型大数据量应用系统基础数据量大，通过传统的集中存储方式，存储并发读写 IO 能力无法满足计算资源要求，建议通过并行计算模型实现。根据业务计算特点，服务器可灵活选择虚拟机。

本项目拟采用超融合服务器，超融合服务器提供了便捷的部署方式，计算资源、网络资源、存储资源的融合架构，使得用户可以按需灵活调整虚拟资源池以满足园区相关业务的需求。

服务器配置方案

政务云服务器资源细项

此类应用为园区公共性平台，均依托省大数据局政务云资源。所需政务云资源需满足等保三级安全测评要求及三级密码测评要求。

一、园区公共服务平台

序号	系统	服务器类型	虚拟机	虚拟机 CPU		虚拟机内存		虚拟硬盘	
			数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
1	园区统一门户	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	2	4	8	16	300	600
		数据库服务器	2	4	8	16	32	500	1000
2	智慧园区服务系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	2	4	8	16	300	600
		数据库服务器	2	4	8	16	32	500	1000
3	访客管理系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	2	4	8	16	300	600
		数据库服务器	2	4	8	16	32	500	1000
小计			**18**		**48**		**192**		**6600**

二、园区运营管理平台

序号	系统	服务器类型	虚拟机	虚拟机 CPU		虚拟机内存		虚拟硬盘	
			数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
1	园区智慧党建系统	Web 服务器	2	2	4	8	16	150	300
		应用服务器	2	2	4	8	16	150	300

		数据库服务器	2	4	8	16	32	300	600
2	园区决策分析系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
3	安全生产管理系统	Web 服务器	2	2	4	8	16	300	600
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
		应用服务器	2	8	16	8	16	300	600
		数据库服务器	2	16	32	16	32	600	1200
小计			**26**		**216**		**288**		**9600**

综上统计，本期项目政务云建设需求为 44 台虚拟机、264vCPU、480GB 内存、16200GB 存储资源、备份存储需求 27994GB（按存储年增长率 20%，三年增长量）。

国产化本地云一区服务器资源细项

此类应用为满足监管要求以及企业商业机密，部署在海口综保区机房，与海关机房形成信息化闭环。

一、展销综合服务平台

系统	服务器类型	虚拟机	虚拟机 CPU	虚拟机内存	虚拟硬盘

		数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
云展综合服务系统	应用服务器	3	8	24	16	48	500	1500
	Web 服务器	1	4	4	8	8	500	500
	数据库服务器	1	8	8	16	16	1000	1000
宝玉石交易系统	应用服务器	3	8	24	16	48	500	1500
	Web 服务器	1	4	4	8	8	500	500
	数据库服务器	1	8	8	16	16	1000	1000
资源云交易系统	应用服务器	3	8	24	16	48	500	1500
	Web 服务器	1	4	4	8	8	500	500
	数据库服务器	1	8	8	16	16	1000	1000
小计：		**15**		**108**		**216**		**9000**

二、、作业综合服务平台

系统	**服务器类型**	**虚拟机**	**虚拟机 CPU**		**虚拟机内存**		**虚拟硬盘**	
		数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
一体化ERP云服务系统	应用服务器	2	8	16	16	32	500	1000
	Web服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
智慧云仓服务系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000

	数据库服务器	1	8	8	16	16	500	500
物流运输管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
供应链金融服务系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
溯源采集管理系统	应用服务器	1	8	8	16	32	500	500
	Web 服务器	1	8	8	16	32	500	500
	数据库服务器	1	8	8	16	16	500	500
融资租赁管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
跨境电商新零售管	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000

理系统	数据库服务器	1	8	8	16	16	500	500
免税交通工具管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
冷链协同管理系统	应用服务器	2	8	16	16	32	500	1000
	Web 服务器	2	8	16	16	32	500	1000
	数据库服务器	1	8	8	16	16	500	500
源数据库集群	服务器	2	8	8	16	16	500	500
存储/备份服务器	服务器	1	8	8	16	16	500	500
文件服务器	服务器	1	8	8	16	16	500	500
小计		47		368		768		23000

三、辅助监管业务服务平台

系统	服务器类型	虚拟机	虚拟机 CPU		虚拟机内存		虚拟硬盘	
		数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计

智能监管场站系统	应用服务器	1	8	8	16	16	300	300
	传输服务器	1	8	8	16	16	300	300
保税业务辅助管理系统	应用服务器	8	8	64	16	128	300	2400
	传输服务器	4	8	32	16	64	300	1200
多式联运服务系统	应用服务器	4	8	32	16	64	300	1200
	传输服务器	2	8	16	16	32	300	600
跨境电商服务系统	应用服务器	2	8	16	16	32	500	1000
	传输服务器	2	8	16	16	32	500	1000
	接口服务器	2	8	16	16	32	300	600
应用支撑	应用服务器	2	8	16	16	32	300	600
	传输服务器	2	8	16	16	32	500	1000
小计		**30**		**240**		**480**		**10200**

四、园区应用数据库集群

系统	**服务器类型**	**虚拟机**	**虚拟机**		**内存**		**存储磁盘**	
		数量	CPU	小计	内存(GB)	小计	容量(GB)	小计

园区数据库集群	数据库集群服务器	1	4	4	128	128	10000	10000
	数据库集群服务器	1	4	4	128	128		
海关数据库集群	数据库集群服务器	1	4	4	128	128	10000	10000
	数据库集群服务器	1	4	4	128	128		
小计：		**4**		**16**		**512**		**20000**

五、对外接入网数据交换集群

系统	**服务器类型**	**虚拟机**	**虚拟机**		**内存**		**磁盘**	
		数量	内核(个)	小计	内存(GB)	小计	容量(GB)	小计
数据交换系统	数据交换服务器	1	32	32	128	128	500	500
	数据交换服务器	1	32	32	128	128	500	500
	集群域控	1	32	32	128	128	500	500
	集群控制台	1	32	32	128	128	500	500
小计		**4**		**128**		**512**		**2000**

六、园区智慧管理平台

需求	**场景**	**数量**	**部署方式**	**规格**
园区安防体系平台	应用服务器	1	VM	CPU：>=16 核，内存：>=64GB，硬盘：>=500GB
	Web 服务器	1	VM	CPU：>=16 核，内存：>=64GB，硬盘：>=500GB
	数据库服务器	1	VM	CPU：>=16 核，内存：>=64GB，硬盘：>=500GB

综上本地云服务器所需资源汇总如下表：

系统分类	应用场景	VPU	内存（G）	存储（T）
国产化架构	展销综合服务平台	108	216	9
	作业综合服务平台	368	768	23
	辅助监管业务服务平台	240	480	10.2
	园区应用数据库集群	16	512	20
	对外接入网数据交换集群	128	512	2
	园区智慧管理平台	48	192	1.5
合计		**908**	**2680**	**65.7**

综合考虑 vCPU、内存、存储资源需求，服务器数量取最大值 10 台。因考虑系统预留 30%的资源量，故配置 12 台国产化架构的超融合服务器。

国产化本地云二区服务器资源细项

为满足智慧园区集成平台、智慧园区数据平台、媒体转码组件、地理信息数字系统、运营指挥可视化平台、物联网平台等工具软件部署，支撑智慧园区指挥管理平台和可视化应用的数据汇集、呈现、管理，根据各模块所需资源进行此部分服务器资源评估。本次项目中的国产化服务器资源需求如下：

系统分类	应用场景	VPU	内存（G）	存储（T）
国产化架构	园区集成平台	120	544	13.5
	物联网平台	16	128	3
	园区数据平台	152	640	12.5
	GIS 平台	16	64	2.5

	可视化平台	96	192	2
	视频转码	24	96	1
合计 2		**424**	**1664**	**34.5**

综合考虑 vCPU、内存、存储资源需求，取 11 台。因此建议配置 11 台国产化架构超融合服务器。

存储备份方案

整个项目的备份方案主要从两个层面来进行设计，一是园区数据中心，二是电子政务云。

园区数据中心存储系统采用结构化数据非分结构化数据隔离存储架构。在老城园区部署一套超融合架构的云平台，该云平台提供的分布式云存储服务作为园区数据中心虚拟化平台的核心存储，统一为园区核心生产和运营管理的各类业务系统提供存储资源空间使用。部署一套分布式非结构化存储，用于存储监控视频资源。同时，园区数据中心通过专线或互联网与省内公有云服务商进行连接，将关键数据灾备到公有云，通过购买服务方式实现园区业务的灾备。

对于部署在政务云上的应用，通过电子政务云现有的存储备份方式实现数据存储备份。

园区本地云上的业务系统采用公有云备份、政务云上业务采用政务云备份，可利用线上及线下的管理联动，实现高效的问题解决及运行维护体系构建，降低整体安全可靠上的建设成本，提升园区全业务的数据备份和恢复能力。

存储灾备容量分析

充分考虑海口综保区现有业务和未来 5 年内业务发展的整体规划。现有信息化系统和将来上线的新信息化系统，以及来自海关的数据都将参与数据分析与计算，而各业务系统中大概有 40%的数据需要参与数据分析与计算，具体数据量测算（取系统中主要数据表进行测算），数据主要分为静态数据（基础数据库）与动态数据（业务库数据、主题库数据、交换与共享库）。按照静态数据永久保存，业务数据在线保存 5 年，视频数据保存 2 个月进行数据量估算。基础数据、业务数据、主题数据、交换数据的数据量分别为 352.77、1746.34、2134.4 和 64.47

GB，共计约 4.2TB；考虑到数据空间及日志空间、临时表空间的占用，以及空间预留，通常取数据量的 3 倍，即所需数据存储空间为 4.2TB×3=12.6TB，按照每年 30%的增长量，三年备份服务所需云端备份资源量为向上取整【12.6TB*1.3^3】=30TB。

初步的数据量估算如下表。

序号	数据类型	分析存储量	设计存储量
1	基础数据	352.77GB	1,058.31GB
2	业务数据	1746.34GB	5,239.02GB
3	主题数据	2134.4GB	6,403.20GB
4	交换数据	64.47GB	193.41GB
5	视频数据	166.3TB	200TB
合计			212TB

根据对园区云上业务存储备份需求统计分析，项目将租赁三年 30TB 公有云备份服务对基础数据、业务数据、主题数据、交换数据进行云端备份。

针对本地云关键应用系统的容灾，考虑采用租赁公有云实现应用级容灾服务。通过对本地云承载业务系统的分析，大部分虚拟机采用的规格为：8 核 CPU、16G 内存、500G 数据盘，因此在公有云上租赁 5 台同等规格的备用虚拟机用于对关键应用的容灾热备服务；本地云与公有云容灾服务之间采用 CDP 持续数据保护的方式进行数据复制，考虑到 CDP 技术复制过程中存在全量镜像数据、CDP 连续复制每日增量数据、容灾恢复预留空间要求，灾备云 CDP 复制所需存储资源为 5 台虚拟机数据盘规格的 3 倍，即容灾 CDP 所需存储资源=0.5TB*5*3=7.5TB。

存储架构选择

本次项目所进行存储备份的数据类型包括结构化数据及非结构化数据两类，

目前主流的存储架构主要分为分布式存储与集中式存储两大类，两种架构的主要对比如下：

分布式存储架构，是将数据分散存储在多台独立的通用服务器上，通过通用的存储协议 iSCSI、NFS、 CIFS、FTP、S3 等对外提供服务，每个存储服务器节点既能够进行数据存放和性能加速，也同时提供数据控制和存储接口对接，没有单点故障，每个节点都可以对外提供数据吞吐，性能随着存储节点的增多会线性上升，分布式存储系统采用可扩展的系统结构，利用多台存储服务器分担存储负荷，它具有高扩展性、高性价比的优点，但数据存储分散，维护复杂，适合大容量、并发量大及 WEB 类数据存储。分布式存储系统的多节点并行恢复数据不小于 1 Tb/h：存储系统的容量、性能随节点增加而线性增长，平均响应时间不大于 3 ms；存储系统的节点扩容时间不大于 1 min/节点，数据可靠性指标≥ 99.9999999%。

集中式存储架构，是指由一台或多台主控制器组成中心节点，各数据设备级联部署，数据集中存储于这个中心节点中，并且整个系统的所有业务单元都集中部署在这个中心节点上，系统所有的功能均由其集中处理，中心节点统一对外提供 FC、ISCSI 存储接口。集中式系统中，每个终端或客户端及其仅仅负责数据的录入和输出，而数据的存储与控制处理完全交由主机来完成。集中式系统最大的特点就是部署结构简单，具有高可靠和稳定性，技术成熟，维护管理难度小但扩展性相对较差，需要额外配置光纤交换机，适合核心业务及数据库类存储。集中式存储数据可靠性指标≥99.99%，单设备的读写次 IOPS 不小于 10 万，数据访问时延≤0.5ms，但由于集中式存储不具备分布式存储多节点并发读写访问、横向扩容的能力，随着应用系统的增加，读写能力及存储容量将成为设备的瓶颈。

基于上述技术对比以及智慧园区各业务系统对存储系统电信级高可靠、容量横向弹性扩容、数据零丢失的需求特点，本次建设本地云平台拟采用分布式存储，用于存储本地云上部署的展销综合服务平台、作业综合服务平台、辅助监管业务服务平台、园区应用数据库集群、对外接入网数据交换集群、园区智慧管理平台结构化及非结构化数据；对于园区的视频监控的非结构化数据，则利用磁盘阵列进行集中存储，此部分详见视频监控子系统建设方案一节。

容灾类型选择

系统故障时，可以在规定时间内完成整体容灾切换，前台业务系统基本不受影响。容灾主要针对数据和应用两大类，根据提供基本的数据保护和提供不间断的应用服务来区分，一般情况下容灾体系可以分成数据级容灾、应用级容灾和业务级容灾三个级别。

一、数据级容灾

数据级容灾是指通过建立一个异地数据系统作为本地数据的远程备份，能够保证业务数据的完整性、可靠性和最终一致性。数据级容灾的关注点在于数据本身，当本地系统由于意外停止工作时，确保原有的数据不会丢失或者遭到破坏，不过，在数据级容灾级别上，当本地发生灾难时，因相应的信息系统自身没有备份，用户的服务请求在灾难中可能会中断，单纯的数据容灾无法保证业务持续性。

在数据级容灾方式下，所建立的容灾中心可以简单地理解成一个远程的数据备份中心。数据级容灾的恢复时间比较长，但是其建设费用比较低，而且构建实施和运行维护也相对简单。

二、应用级容灾

应用级容灾是在数据级容灾基础上的升级，通过在备份站点构建一套相同或缩小比例的应用子系统，在本地系统由于意外而停止工作时，可以及时启用备用应用子系统，保证关键应用在允许的时间范围内恢复运行，尽可能的减少因灾难带来的损失。应用级容灾一般在生产中心和容灾中心之间采用同步或异步的数据传输，但容灾中心也需要具有和生产中心类似的外部广域网资源，应用级容灾涉及到需要通过更多的软硬件来实现，可以使多种应用在灾难发生时进行快速切换，确保业务的连续性。

三、业务级容灾

业务级容灾是在数据级容灾和应用级容灾基础之上的一个更高级别的容灾，是应用级容灾的最高标准，生产中心和容灾中心对业务请求可以同时提供服务，在某一方灾难发生时，另一方可以保证所有的业务都是正常运行并可访问，用户感受不到灾难影响，因此既能实现业务服务冗余分担，又能够确保业务持续可用。

实现业务级容灾，不仅需要确保两地数据一致，还需要在数据管理层面、应用程序层面、访问通道层面都能够平滑切换，数据中心之间的距离也有较大限制，甚至主备中心最好具备对称的基础设施，以便一旦原有的办公场所遭到破坏，在

备份场所也能正常的开展业务。

为保障综保区业务的安全，有效应对自然灾害、人为破坏造成的灾难，避免单点故障，确保各业务系统的高可用性和业务连续性。

本项目考虑建设相应的灾备体系，以实现系统的应用级容灾，以确保灾难发生时，实现关键服务在允许的时间范围内恢复运行，数据不会丢失或者遭到破坏，应用级容灾的 RPO≤5 分钟，RTO≤15 分钟。

除了数据复制和应用自动切换外，同时需要把数据中心的所有数据，包括数据库、应用环境、文件、操作系统等进行统一的备份，防止逻辑故障，同时作为容灾系统的最后一道防线。

容灾级别选择

国家标准《信息系统灾难恢复规范》GB/T20988-2007 规定了六个级别的容灾，下表分别针对每个级别的内容要求给出了相应的应对措施。

容灾级别分类表

级别	内容	RTO 要求	RPO 要求	措施
Level 6	数据零丢失和远程集群支持	数分钟	0	实现远程数据实时备份，实现零丢失；备用与生产系统处理能力一致；应用软件可以实现无缝切换；远程集群系统的实时监控和自动切换能力。
Level 5	实时数据传输及完整设备支持	数分钟到2天	0 到 30 分钟	实现远程数据实时复制技术；配置所需要的全部数据和通讯线路及网络设备，并处于就绪或运行状态；备用网络也具备自动或集中切换能力。
Level 4	电子传输及完整设备支持	数小时到2天	数小时到 1 天	配置所需要的全部数据和通讯线路及网络设备，并处于就绪状态；更高的技术支持和运维

				管理。定时通过网络自动得把备份数据复制到异地。
Level 3	电子传输和部分设备支持	12 小时以上	数小时到 1 天	配置部分数据通信线路和网络设备； 每天实现多次定时的数据传送； 有备用场地。
Level 2	备用场地支持	24 小时以上	1 天到 7 天	配置部分或预定时间内可调配数据通信线路和网络设备； 有备用场地； 设备及网络紧急供货协议。
Level 1	基本支持	2 天以上	1 天到 7 天	每周至少做一次完全数据备份； 有存放备份设备的场地。

遵循科学先进、实用高效、安全可靠、节能环保的设计理念，按照国家关于灾备系统能力的 6 级标准，结合本项目实际情况，数据和应用恢复整体满足《信息系统灾难恢复规范》（GB/T20988-2007）的第 5 级要求。如果数据中心出现重大灾难性损失，可以达到信息系统数据基本不丢失。同时容灾中心建设在充分考虑可扩展性的条件下，与主数据中心设计能力相匹配，在主数据中心暂停服务期间，容灾中心能够提供基本的应用系统服务和数据查询工作。

容灾备份技术选型

针对项目中部署在政务云中的平台和系统，考虑采用电子政务云系统进行灾备份，针对部署在本地云中的平台和系统，考虑采用省内公有云服务商有提供的灾备服务。

容灾备份技术的核心是实现数据的实时复制，目前主流的数据复制技术可以从信息系统的 4 个层次：应用软件、数据库、操作系统、存储系统来实现。

一、基于应用的数据复制技术

基于应用的数据复制是指由应用软件来实现数据的远程复制和同步，当主中

心失效时，灾备中心的应用软件恢复运行，接管主中心的业务。这种数据复制技术需要在软件开发时，在存储、操作系统、数据库等层面进行定制开发，维护人员需要了解各个层面上的工作状况，还要熟悉应用程序本身，复杂度极高，稳定性较差。

二、基于数据库的数据复制技术

基于数据库的数据复制是由数据库系统软件来实现数据库的远程复制和同步。支持异构数据库、异构网络、异构操作系统，对网络带宽的消耗也不大，在灾难发生时能够进行热切换，因此应用较为广泛。缺点是数据库容灾仅支持结构化数据（数据库数据），不支持系统数据、逻辑卷信息、非结构化数据的容灾恢复，对于结构化、非结构化数据混合的环境有一定的局限性。

三、基于操作系统的数据复制技术

基于操作系统的数据复制需要在每台参与复制的服务器上部署多个软件，如磁盘卷管理软件、磁盘卷复制管理软件等，磁盘卷复制管理软件将主节点系统的卷上每次 I/O 的操作数据实时（准实时或延时）复制到远程节点的相应卷上，从而实现两个卷之间的数据同步（或准同步）。该类数据复制一般与物理存储系统设备无关，对物理存储系统自身的管理功能要求不高，有较好的可管理性，也便于主、备用系统的扩充和发展；同时，也可方便地做多对一或者一对多的远程数据复制。缺点是需要对操作系统、文件系统作修改，数据存放过程中需要进行本地和远程两次 I/O 操作，对服务器的性能影响较大，实现过程复杂且不够稳定。

四、基于存储的数据复制技术

基于存储的数据复制是在存储区域网络内部实现数据快照、数据复制的技术。它由存储系统自身实现数据的远程复制和同步，并保持数据的一致性。在这种方式下，数据复制软件运行在存储系统内部，比较容易实现主中心和备份中心数据的实时拷贝维护能力，一般不会影响主中心主机系统的性能。并且上层应用的变化对于存储系统本身及数据远程复制过程没有影响，具有简单、高效的特点，能较好地保证数据的完整性和一致性，数据的复制备份过程不占用主机资源，操作控制比较简单，对结构化、非结构化数据提供良好的支持，因此应用最为广泛。综上所述，基于应用的数据复制技术需要大量的定制开发，目前在业界使用较少；基于服务器操作系统的数据复制技术需要改变现有操作系统对存储逻辑卷的管理，实现过程比较复杂，风险大。基于数据库的数据复制技术和基于存储的数据复制技术对现有信息系统的冲击比较小，比较适合现有成熟应用系统使用，因此

结合园区业务实际情况，本项目的容灾备份核心技术应优先采用基于数据库的数据复制和基于存储的数据复制两种技术。

备份建设方案

备份架构设计

备份系统架构总体划分为三大技术层面：备份数据源层、备份系统实现层、备份管理平台层；

1、备份数据源层需覆盖各类系统的备份数据类型，主要包括：数据库、文件系统、操作系统、虚拟机等；

2、备份系统实现层为备份系统主要构成组件，包括：各类备份客户端、备份系统架构类型、备份系统功能和模块等；

3、备份管理平台层为备份系统的整体管理平台，包括：配置管理、多租户管理、监控管理、报表统计、流程审批、日志管理和权限管理等模块。

备份技术策略

数据备份方式包括本机备份、LAN 备份、LAN-Free、SERVER-Free 备份等。不同的备份方法，其效果不同，主要表现在性能、自动化程度、对现有系统应用的影响程度、管理、可扩展性等方面。分别说明如下：

1. 本机备份：本地服务器硬盘上的数据直接备份到与服务器直接相连的磁带库（磁带机）或其它存储设备上，而不经过网络。这种方式操作维护最为简单，对于主机数量少，并且数据量小的系统较为适用。

2. LAN 备份：通过一台备份服务器控制需要备份的设备，利用 LAN 传递备份数据。这种方式会对 LAN 产生较大的压力，因此适合主机数量较多但数据量相对较小的系统。

3. LAN-Free 备份：基于 SAN（存储局域网）的备份方案，备份设备直接连接到 SAN 网络中，备份数据的传送不需要通过 LAN 实现，因此对 LAN 不会产生压力，这种方式适合大数据量的系统。

4. SERVER-Free 备份：大量数据流无需流过服务器，则可以极大降低备份操作对生产系统的影响，对数据库服务器的压力很小，但这种方式对技术要求高，

需要磁盘阵列额外的空间以及配置特殊的备份管理软件，成本也更高。

5.云备份：在公有云上及客户本地部署备份软件，本地业务服务器部署备份客户端，通过客户端获取数据，去重加密后经专线/公网写至云端存储，轻松满足客户异地备份、低成本、高可靠的需求。

综合考虑，本项目拟采用云备份方式，通过购买省内公有云服务商的云备份服务，实现数据不出省、异地备份的需求。

备份保护策略

备份方案采用的底层存储技术方面，综合考虑到项目备份数据所需的存储可靠性较高、备份数据未来增长量、建设成本，将采用省内公有云服务商提供的分布式存储服务。

对数据进行备份保护的原则是保证数据的安全性、保证操作系统的安全性，在灾难发生时恢复系统等多方面考虑的。需要完整的保留历史数据，并且确定指定时间范围历史数据保留的周期，确保特定情况下恢复特定时期的数据，还要保证数据的完整性和可靠性，就需要保证数据备份的频率、备份的方法、备份介质选择、以及备份介质上数据的保存时间符合预期设计的目标。目前，成熟的备份平台对资源数据的备份都是每天进行一次，并且采用完全备份和差量备份结合的方式，给数据恢复带来便利。由于采用了先进的软、硬件配置，这种日常备份操作都可以在晚间系统负载较轻时定时、自动、快速进行，对系统日间使用不会造成任何额外影响。

随着业务系统的不断发展、数据量不断增大、恢复的级别要求不断提高；数据恢复对“恢复时间点目标”（Recovery Point Objective）和“恢复时间目标”（Recovery Time Objective）的要求也越来越高，结合业务应用特点的不同，对数据在应用系统中的表现进行了分析，以下是具体的备份保护策略：

1. 数据库服务器的备份：作为重要的运营系统和宝贵的信息库，承担着日常的网络与数据中枢的角色，其长期运行过程中积累下来的数据具有重要的价值。基于此，对于这些服务器的备份，应从整体、系统、长期的角度来制定备份策略，做到既能快速的进行日常备份，又能完备的保留一定历史时期内的数据的目的；建议使用每周全备份，每天增量备份的方式。

2. 文件方式的备份：建议采用全备份、增量备份和合成备份结合的方式，

初始做一次全备份，每天增量备份，每周进行一次合成备份由于系统中的每台服务器数据交换和信息更新都极为频繁，每天都有大量的信息数据、那么做每日备份，记录每日系统的最新信息是极为必要的。同时为了提高恢复的速度，采用合成备份，能尽量将全备份数据合成到 1 盘磁带或者存储介质上，提高恢复速度。

3. 操作系统和文件系统的备份：建议初始做一次全备份。当有应用程序变更（如 Oracle 增加 Patch 等操作后），再进行一次全备份；保证操作系统和文件系统备份能准确恢复要业务需要的应用程序状态。

类型	说明	备份策略
操作系统备份	实现服务器的操作系统的备份，操作系统覆盖现网的 windows、Linux 等各类操作系统，解决服务器未做操作系统备份存在重大安全隐患的问题	操作系统 OS 备份，按业务需求制定，通用策略为每两周全备，保存两个月
数据库数据备份	对现网使用最多的 ORACLE、MySQL、PostgreSQL 等数据库的在线热备份、连续日志备份和增量备份，把数据 RPO 时间由每天、小时降低至秒级，提高数据安全的等级	按业务需求制定，通用策略针对 ORACLE、MySQL、PostgreSQL 提供全量备份、增量备份、日志备份，备份策略为每周全备、每日增备、每 4 小时日志备份，保存周期为一个月
数据库合成备份与即时挂载恢复	支持数据规模在 TB 级别、恢复时间用十几小时甚至几天时间的数据库，通过合成备份功能，把备份数据实时挂载可用，实现 TB 级别的数据库即时挂载恢复，同时满足数据分析、数据报表、数据共享等方面的功能需要	按业务需求制定，通用策略针对 ORACLE、MySQL 提供数据库合成备份和即时挂载恢复，备份策略为每日合成备份，保存周期为一个月
重要应用系统文件和数据库	定期对重要业务系统的文件和数据库进行备份，保证业务数据的历史多副本的可恢复能力与数据安全性	按业务需要恢复不同操作系统平台文件（LINUX/WIN）和不同数据库（Oracle、MySQL、

备份		MSSQL 、 Sybase 、 PostreSQL、MongoDB、国产数据库等),按业务需求制定，通用策略为每周全备份、每日增量备份，保存周期为一个月
虚拟机和云主机备份	对虚拟化和云平台采用无代理备份，通过资源层快照方式保护虚拟机和云平台整机系统和数据	针对不同虚拟化和云平台（VMWARE、Hyper-V、H3C CAS 、华为 FusionSphere 、FusionCloud 、RedHat KVM、OpenStack 等）按业务需求制定，通用策略为每周全备份、每日增量备份，保存周期为一个月
定期灾备恢复演练	定期进行数据灾备恢复演练，验证灾备的有效性，以及恢复演练操作手册、恢复演练报告等	按业务需要进行应用系统灾备应急演练，验证恢复接管能力

备份窗口策略

备份时间窗和业务忙时错开。由于备份系统对虚拟机进行备份期间会占用网络带宽，故备份窗口设置为凌晨业务闲时。首次备份的数据量大，一般在用户将业务部署到数据中心后，选在周末统一对一批次数据进行备份。

根据现网的网络和业务情况，备份时间窗内能将当天需要执行的备份数据全部备份完毕。由于备份时，会对虚拟机所在存储进行大量读操作，备份时间窗最好和其他存储消耗型的应用执行时间错开。

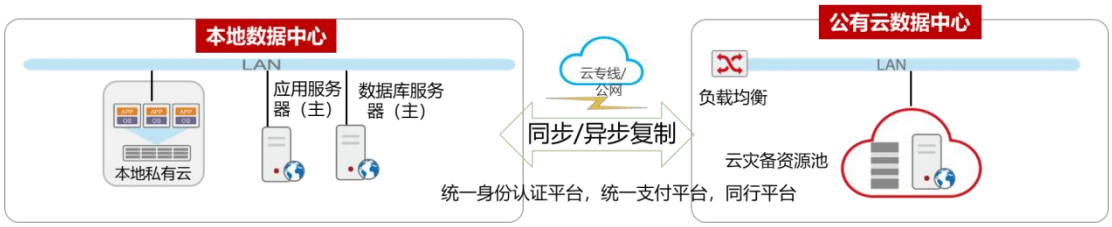
备份周期为 7 天（周天全备份，周一至周六增量备份），数据保留一个半月，

为不影响业务正常运行，每天备份的时间窗口如下：每日 22:00－次日 6:00，共 8 小时。

容灾建设方案

容灾系统设计

本项目采用省内公有云对本地云平台业务系统进行灾备，本地数据中心通过专线或公网与省内云服务商的公有云互联，通过云端部署的灾备软件及本地业务系统部署的灾备客户端实现灾备上云。



根据本地云平台部署的业务系统特点，并结合不同的业务系统保护要求、业务重要程度不同，对业务灾备大致分为三类：

A 类，数据丢失<1 秒，业务中断<5 分钟；

B 类，数据丢失<1 秒，业务中断<1 小时；

C 类，数据丢失<1 秒，业务中断<1 天。

云灾备提供梯度化的 SLA 服务，多种灾备技术根据业务场景（定时备份、CDM、CDP）组合，全面保护所有工作负载，业务 SLA 匹配对应成本的灾备技术，全面优化 TCO。同时结合现有环境情况，通过多重灾难恢复手段和常规演练制度，包括本地日常恢复演练、灾备中心灾难恢复等多成保障机制，确保出现灾难时能在最短时间内完成灾难恢复和故障切换。

1. 针对 A 类系统：采用双活/CDP 秒级保护

持续的纪录并备份数据变化，在特定的情况下可以做到 RPO≈0，而且仅仅当灾难发生后，只需要简单的选择要恢复到的时间点即可实现数据快速恢复使用。

持续数据保护技术根据其实现的原理可以分为：应用级持续数据保护，文件级持续数据保护，块级持续数据保护。应用级持续数据保护是在应用层基于应用的相关技术特性（比如说各种数据库的日志数据）实现应用级持续数据保护。文件级持续数据保护是在对应的文件系统层 IO 链路上增加旁路监听机制，实现实时监控并保护文件系统的 IO 变化。块级持续数据保护是在对应的分区或者磁盘

的 IO 链路上增加旁路监听机制，实现实时监控并保护对应分区或者磁盘上的 IO 变化。

2. 针对 B 类系统：采用 CDM 副本数据管理保护

一般来说，传统备份方案备份 10TB 数据需要 5.5 小时，且每个月需要执行一次完全备份，备份时间较长，如果设备在备份过程中出现故障，势必对数据的完整性和安全性造成重大影响。而采用 CDM 的永久增量备份，每次只需要备份增量的数据，整体备份效率提升 90%，且每个增量时间点均为完整副本，任意增量时间点损坏，不影响其他时间点的恢复。

在此期间，设备资源占用也较多，因此需要通过高效的恢复技术，在确保数据快速恢复的基础上，减轻在此期间的资源消耗。即时恢复技术可实现 5 分钟内恢复所需数据，RTO<5 分钟，无论数据量有多大。

3. 针对 C 类系统：定时备份保护

定时备份提供集中全面保护主流操作系统、主流虚拟化平台、主流数据库，实现虚拟、物理、云环境的统一保护和集中运维，降低管理复杂度和成本投入，有效避免单点方案难管理、成本高等问题。防止各种病毒的勒索，数据由于各种原因的损坏，人为误删除或者或者有意删除，逻辑炸弹或者 BUG，程序出错或者问题，软件出现错误以及断电，爆炸，火灾，洪水，闪电，电涌，静电，偷窃，黑客和红客以及国际攻击等。

容灾资源配置

本项目实现业务系统的应用级容灾，实现关键服务在允许的时间范围内恢复运行，RPO（数据丢失量）≤5 分钟，RTO（业务中断时间）≤15 分钟。省内公有云作为园区本地云的灾备中心，在灾害发生时要有能接管关键业务及数据的能力，因此对灾备云的容灾计算、存储等资源采用 1：1 镜像配置。

容灾切换方案

容灾系统的建设目标是对数据平台进行完整保护，同时对部分（或全部）关键业务种类所依赖的业务平台和接入平台进行保护。在生产中心发生严重故障，系统无法在业务可以容忍的中断时间内予以恢复的情况下，将生产中心系统切换至灾备中心，使关键业务能够在灾备中心及时地被接管，并继续正常的运行。对

容灾备份系统而言，切换工作是将处于保护状态的灾备中心系统变更为生产状态的过程。另外，当发生灾难的原生产中心的运行环境恢复后，还要将关键业务由灾备中心回切到原生产中心，使得业务系统又回复到灾难前的状态。

一、系统切换

系统切换是指在主生产中心发生计算机系统严重故障或灾难时，为了尽可能减少对业务造成的损失，而制定的故障定位与隔离措施、灾备中心接管步骤和方法等。系统切换是控制风险的一种有效方法，是容灾备份系统的一个重要组成部分。系统切换的内容应尽量详尽，易于操作。

1.切换原则

当主生产中心发生的故障或灾难影响到业务系统的正常运行时，应首先对业务系统的受影响程度进行检查，尽可能快速定位业务系统的故障部位。分别对机房受损程度、机房电源、计算机网络、系统硬件、操作系统、数据库、应用系统等进行检查，评估恢复时间，然后由相应人员决策是否进行系统切换，应考虑以下因素和原则：

- 故障影响程度，可以分为两大类：

业务停顿，但故障范围明确，并且可在可忍受的时间内修复，不需要灾备中心切换。例如：电源发生故障、软硬件故障、消防系统和空调系统等机房环境告警、人为因素误操作的情况，应建立相应的本地高可用性系统、备份策略，管理流程，采用专业服务支持、基础设施的防护等措施，来预防和避免故障对业务系统连续性运行的影响。

数据中心系统在可忍受的时间内无法恢复或彻底破坏，必须进行容灾切换。

- 优先选择本地恢复原则

当无法判定生产中心的业务系统修复所需时间时，应在继续恢复生产中心的系统的同时，在容灾中心开始进行切换的准备工作。只要生产中心的业务系统在可容忍时间内有恢复的可能，就应优先选择本地恢复。

- 优先恢复关键性业务原则

对于各个系统，根据停机时间所造成的影响和损失的大小的不同，优先恢复关键性核心业务。当生产中心的主机、网络等资源不足时，优先提供给关键性核心业务使用。

2.切换必要性确认

应分别对原生产中心的机房环境、计算机网络、系统硬件、操作系统、数据

库、应用系统等方面的损害程度和可恢复程度进行评估，当原生产中心不可恢复或恢复时间超过了业务系统停机所能承受的范围，就应采取切换措施。

例如以下情况需要执行系统切换:

- 机房环境：灾难导致机房内部无法进行工作，如火灾、水灾、地震；
- 机房电源：电源故障导致机房没有电源供应，备用发电系统不能工作；
- 计算机网络：主数据中心和外部系统之间的所有通信链路全部中断；
- 系统硬件：运行业务系统主机、存储硬件及其备用系统同时发生严重损坏；
- 操作系统、数据库、应用系统：同时被破坏，且需要的恢复时间过长等。

3.切换可行性确认

在进行切换必要性确认的同时，必须进行切换可行性确认。切换可行性确认的工作包括：

- 明确需要切换的业务种类。
- 在灾备中心标识为需切换业务种类提供支持的系统业务平台、数据平台和接入平台。
- 确认数据平台保护的 RPO 指标满足容灾备份系统设计的要求。
- 确认业务平台冗余配置的正确，评估其处理能力满足容灾备份系统设计要求。
- 确认接入平台的连接正确。

二、回切

当主生产中心的系统恢复以后，就应将业务系统由容灾中心回切到主生产中心。回切过程中要保证两中心的数据的一致性。

1. 回切原则

- 业务影响最小原则

系统回切不同于系统切换，由于灾难发生的随机性和不确定性，系统切换都是在被动的情况下发生的，有可能造成业务数据的丢失和切换时间较长，对业务的正常进行会造成严重影响。而系统的回切是可以按照事先的计划来实现的，因此在系统回切计划中，应选择业务量较小时候，采用最简化的步骤回切；

- 及时性原则

业务系统由主数据中心切换到备份中心后，核心数据不再有容灾保护，因此应尽快恢复主数据中心，并将业务系统回切到主中心，使核心数据重新得到容灾

保护；

- 数据一致性原则

系统回切前需将数据由容灾中心复制到生产中心，并保持严格的一致性。

2.回切可行性确认

应分别对生产中心的机房环境、机房电源、计算机网络、系统硬件、操作系统、数据库、应用系统等方面的恢复程度进行评估，当生产中心已经完全具备生产条件，就要制定回切计划并启动回切流程。

三、业务连续性管理

应当建立业务连续性管理和应急响应体系，包括应急架构及职责、应急响应流程、应急场景和资源管理、应急预案管理、灾备演练管理、灾备切换与回切流程、业务恢复相关的各种内外流程，建立日常应急监测与预警机制。对制度、人员、流程、平台、工具等多方面进行规范化管理从而保障灾难恢复的有效性，确保业务连续性。

容灾演练方案

针对容灾演练和维护，可通过容灾演练、测试确保灾难恢复预案的有效性。灾难恢复预案的维护包括日常计划维护、根据容灾演练结果的维护、由于各项变更产生的维护。

为保证容灾恢复演练的正常进行，在备用数据中心计划预留容灾恢复所需支撑资源，为灾备的恢复提供足够的演练空间的同时，节约容灾成本，提高灾备系统使用效率。

系统及工具软件方案

操作系统

根据平台应用与网络安全要求，规划采用开源操作系统与商用操作系统两种。

表 5- 1 操作系统

序号	类别	单位	数量	参考品牌
1	操作系统	套	1	开源/国产,Linux 系列； 参考品牌：CentOS/中标

				麒麟 Linux
2	操作系统	套	6	Windows 2012。 与海关对接的前置系统，按照海关要求部署。

数据库

根据平台应用要求，规划采用关系型数据库、内存数据库以及 NOsql 数据库。

表 5- 2 数据库

序号	类别	单位	数量	参考品牌
1	关系型数据库	套	1	开源/国产，参考品牌：MySQL/达梦
2	其他数据库	套	1	开源/国产，参考品牌：MangoDB 等

中间件

根据平台应用需求，规划中间件分别有商用与开源两种。具有可伸缩性、集群可用性、web 服务、事务支持、消息支持、安全性。

表 5- 3 中间件

序号	类别	单位	数量	参考品牌
1	中间件	套	1	开源/国产，参考品牌：Tomcat/东方通
2	数据交换系统	套	1	采购商业数据交换系统，并在此基础上进行二次开发。

网络建设方案

立足海南自贸港的战略目标，按照智能物联网应用、5G 新技术应用、海量数据传输处理以及园区作业不同业务类型数据采集共享等多种新型需求，建设由业务网、物联专网以及无线接入网组成的海口综保区网络系统。

外网和园区之间联网

根据网络带宽测算及园区实际需求，综合考虑数据备份容灾等场景，本项目网络专线拟设置如下：

1. 老城园区拟设置 2 条 1Gbps 带宽互联网链路，用于互联网业务开展和园区内互联网访问。

2. 老城园区与海口园区、老城园区与空港园区互联链路拟设置 2 条 1000Mbps 带宽专线，用于园区之间业务数据互通。

3. 老城园区设置 1 条 100Mbps 带宽 VPDN 链路，用于物联网业务开展。其他业务外联也通过老城园区统一出口。

针对海关专网，老城海关与空港海关互联链路拟设置 2 条 1000Mbps 带宽专线，用于园区之间业务数据互通。

园区与政务网

园区内部网络与政务网系统关系：

园区内部网络与电子政务外网通过防火墙进行安全互联，实现综合保税区与电子政务外网业务数据安全交互。

园区内部网络与电子政务专网通过网闸隔离设备进行物理安全隔离，实现综合保税区与电子政务专网涉密业务数据安全交互。

IP 地址规划

IP 地址规划原则

唯一性原则

唯一性是 IP 地址在 TCP/IP 协议中最基本的要求，是 IP 地址的基本特征和 IP 地址编制的重要依据。网络中每一网络所使用的 IP 地址的网络地址字段必须是唯一的，在同一网络中所使用的 IP 地址中包含的主机地址字段也必须是唯一的，这是实现 IP 网络互联互通的基本条件。

连续性原则

在层次化结构的网络中为各个节点划分连续的 IP 地址区间，便于实现路径叠合（Route Summarization）等优化 IP 地址的分配技术，简化路由表数据，提高路由算法的计算效率和动态路由的快速收敛，能有效利用地址空间。

扩展性原则

IP 地址编制要兼顾网络规模扩展的需求，为各个节点预留足够的 IP 地址扩展区间时，应考虑对网络在用地址的继承性，满足路由协议的要求、实现 IP 地址编用的平滑连接等，这是保证网络扩展和有序管理的重要条件。

规范性原则

网络各节点的网络互联设备和局域网内主要设备等采用规范的地址编制技术和方法，是网络互联互通和提高网络管理效率的有效措施。

标准化原则

遵循有关 TCP/IP 协议标准来规划 IP 地址，是网络建设的重要原则。

IP 地址编制方法

完全二叉树分配法

网络中各级子网 IP 地址的编制，是从完全二叉树地址空间中某一子树的根开始，逐级向下地将该子树下的从属子树分配给各级子网和其下级子网，同级子网均以同样方法分配同根的二叉子树。网络互联 IP 地址和用户主机 IP 地址，都是从本级子网的从属子树地址空间中分配。采用这一 IP 地址的编制技术，既避免了各级子网 IP 地址的重叠，又保证了各级子网 IP 地址空间的连续性。

分布的地址空间预留技术

分布的地址空间预留技术是指给按层次划分的各级子网 IP 地址预留空间，当由于网络扩展需要 IP 地址扩展时，可使扩展的 IP 地址空间与在用的 IP 地址空间连续，使网络继续保持其最简的路由表数据结构，保证了 IP 地址的平滑扩展。

无类域间路由（CIDR）编址技术

无类域间路由 CIDR（Classless Interdomain Routing）编址技术使用了可变长子网掩码 VLSM（Variable-Length Subnet Mask）技术和完全二叉树地址分配技术，可根据网络和主机的分布状况，灵活地选择不同的子网掩码屏蔽位长度，动态地分配网络地址标志位和主机地址标志位长度，不仅能有效地提高 IP 地址空间利用率，而且使路由表数据更加简化。

老城园区网络

根据海口综合保税区的业务需求，提供园区管理委员会和所有入住企业的互

联互通，承载视频监控、协同办公、云计算等业务。建设内容包括路由器、交换机、防火墙、安全设备、WIFI6、园区敷设光缆等建设内容。

综保区内部局域网的规划。在海口综合保税区内组建一个万兆光纤内部局域网，局域网划分为核心层、汇聚层、接入层。核心层为汇聚层提供数据的高速转发，与国际互联网数据专用通道、电信运营商互联提供高速出口，并对接政务外网；汇聚层对接入层接入的业务进行汇聚，提供流量控制和用户管理；接入层提供各种类型用户的快速接入。海口综合保税区内部局域网各层网络之间均采用万兆链路通过裸光纤互联，防火墙、安全设备提供内部局域网的网络及信息安全。

802.11ax 协议（WIFI6）作为有线宽带网络的延伸，是业界最新的主流无线网络，通过靠物理层和链路层的优化实现了更多用户并发效率，同时在速率上也比 802.11ac 有了更进一步的提升，最大理论速率可达 9.6Gbps。

园区局域网建成后可为海口综合保税区内的企业及各类应用提供高速率、高带宽、安全可靠的无缝网络连接。

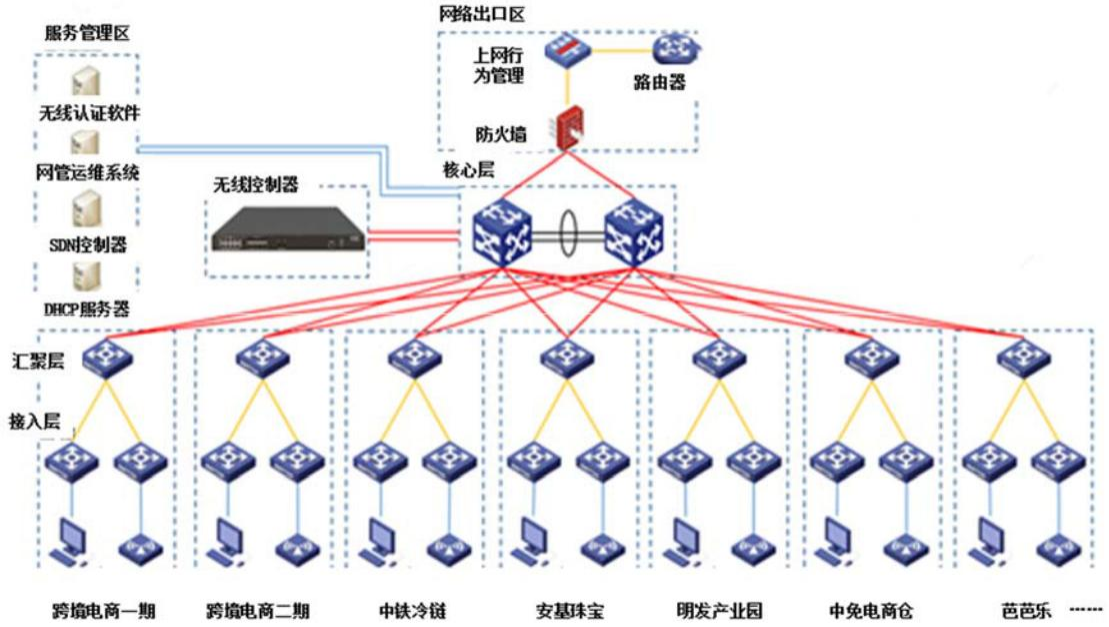


图 5- 121 智慧园区局域网组网图

综保区内部光网络的建设。根据保税区内的规划，结合入住企业的分布，在保税区主干道和主要路口规划光交箱，利用园区内管道、线路资源，规划建设园区光缆覆盖网络，满足入驻企业、园区管理的就近接入。

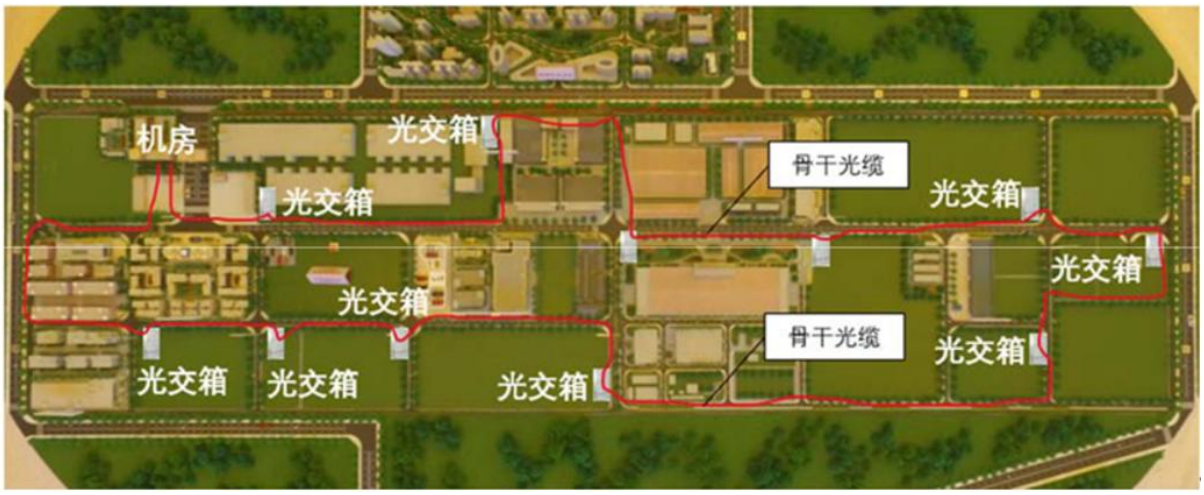


图 保税区园区光缆网络覆盖示意图

园区物联网系统

概述

园区物联网终端感知系统包括终端感知设备和物联感知平台的部署。通过园区的光纤和室内高速宽带，实现全区室内、室外 WIFI 全覆盖，连接智慧环保、污水排放监测、智能停车、智能照明、三表集抄、联网车辆、人流分析，在园区安全监测、信息化管理、配套管理等领域实现相关对象的实时监控与管理，有助于完善园区新型基础设施建设，提高智慧园区的服务水平。

物联网架构

物联网管理平台将网络连接管理、设备接入、设备管理、设备数据解析转发等能力进行整合、封装、管理，并统一对外提供服务。通过物联感知平台的能力集成，快速实现城域物联感知终端的部署接入管理。平台采用开放的企业私有云技术方案设计，是基于 Docker 容器技术的 PaaS 云平台。包含抽象出可以复用的业务能力和技术能力公共组件，以及承载这些组件的弹性计算平台。这些能力组件化、服务化、资源化、透明化，均可以被上层应用以标准化的服务调用方式使用，并支持按需弹性伸缩水平扩展，为应用开发提供平台化能力支撑。

物联感知平台设计

海口综合保税区园区物联感知平台是海南省省级平台的重要组成部分之一，

平台基于园区元素连接、采集园区物联边缘设备的运行数据并进行数据汇集，同时充分利用省级平台提供的强大计算引擎、智能的 AI 分析引擎，动态分析园区内各类物联网感知终端数据，对园区智能设施状态能够实时感知，加快园区反应速度，监测预警园区异常事故，提供应急处置能力。平台向下接入分散的物联网传感器，汇集传感数据；向上面向应用层服务提供应用开发的基础性平台和面向底层网络的统一数据接口。

物联感知平台具备物联感知能力、海量物联设备全生命周期管理能力、安全能力、海量感知设备高并发处理能力。

物联管理平台设计

系统管理

1、配置管理

支持结合统一权限平台进行管理。支持基于权限的远程设备状态数据监测功能、基于权限的远程控制功能，根据需要使用配置工具远程操控现场终端设备，支持单一设备、分组设备、顺序控制等配置方式进行参数调整等功能。

2、设备注册

提供设备注册模块，完成注册的设备支持根据业务需求及场景需要下的逻辑组态功能配置，提供通用配置算法，或支持第三方专用算法，组态输出逻辑，根据实时性与复杂性的要求不同，由平台或远程下载到现场的产品中执行。

支持通过软件定义的方式实现部署和配置功能。支持通过软件定义的方式实现部署和配置。

数据采集管理

1、协议管理

协议解析

为支持创建标准化数据，使得各厂商能按统一的方式对相同的事物进行抽象，从而使得不同厂家的设备能按相同的方式进行访问和控制。

在接入平台创建产品的时候，平台提供可视化配置界面来定义设备功能模型。支持根据设备的感知、属性、状态、事件定义设备功能点。功能点用来描述设备的特性，并作为设备协议模型定义的基础。支持基础功能点、组合功能点和固定

上报功能点。基础功能点支持设备功能和系统功能，组合功能点满足将多个独立功能点组合，进行上报或者下发。针对全局功能点，设置固定上报后，每次上报都会上报一次全局功能点，方便对需要固定上传类型的功能点实现快速配置。

设备功能点定义支持包含设备的功能点名称、字段名称、数据类型、传输类型等字段的收集。同时，系统针对功能点的类型，提供多种数据类型，包括布尔型、数值型、枚举型、故障型、字符型、透传型。支持多种数据传输类型，包括可上报、只上报、只下发，满足不同场景需求。

协议适配

平台支持多种协议将设备接入平台。设备通过搭载平台提供的基础通信套件SDK，实现与平台对接。接入套件屏蔽终端厂商之间的私有协议差异，根据业务需求灵活适配本地、远程、有线、无线等网络通信通道，完成任意设备、任意网络形式的海量设备接入无关性以及安全可信接入。

平台支持多种方式进行设备接入。终端设备可通过搭载预集成平台协议的SDK 快速完成平台的对接；设备也可通过统一接入一个云网关的方式，由云网关实现将设备数据上传到平台；针对已完成开发的设备，平台支持设备数据通过自有平台进行对接。

平台支持终端通过无线、有线等多种网络连接方式接入，可以同时接入固定，移动（4G/5G/NB-IoT）的通信方式。支持丰富的协议适配能力，支持授权频谱（NB-IoT/LTE-M 等）与非授权频谱（LoRaWAN、Sigfox、Weightless、HaLow、RPMA 等）融合，支持多样化频谱。支持通用协议（HTTP、CoAP、LwM2M）等差异性设备接入。支持设备的批量导入、支持海量多样化终端设备接入。支持 TCP 协议透传，根据需要动态协议扩展，实现新协议和私有协议的对接和转换，可屏蔽各类终端厂家的开发差异性，屏蔽各种复杂设备接口差异性，实现终端设备的快速接入。支持设备接入认证功能、设备数据传输加密功能等安全机制。

2、设备管理

平台提供设备全生命周期管理、群组管理能力、批量处理能力、拓扑关系管理、地图服务、文件管理、设备影子、数据存储等设备管理能力。

3、接入管理

智慧物联平台接入适配系统通过内置标准协议，以及提供 SDK 等方式适配各种通信协议，实现碎片化市场中设备统一接入；通过设备管理系统的物模型管理功能定义设备数据模型，统一各个行业终端的数据标准，实现对设备数据的统一

管理。

平台支持三种方式接入，包括终端设备直接接入、设备网关接入和第三方平台接入，解决设备接入复杂多样化和碎片化难题；提供基础的设备管理功能，实现设备的快速接入。

4、传输管理

通过设备通信管理功能，平台为终端设备与平台之间的双向数据传输建立传输链路。平台支持设备通过不同类型的通信模块（包括 NB-IoT、4G、5G、蓝牙、WIFI 等）将数据上报到平台。设备数据以“数据流-数据点模型”将数据上传至平台并进行存储，设备可以通过数据点 Topic 簇调用数据点存储服务存储数据，可以通过订阅系统 Topic 获取数据处理结果通知。平台接收到数据并下发确认消息 ACK，通知用户设备上传数据是否成功，设备接收到 ACK 确认发送成功，完成数据上报工作。当设备需要执行命令时，平台支持应用通过 API 直接向设备发送单播命令，设备可以通过设备命令 Topic 簇获取消息并进行消息应答。平台下发数据到传感模块，模块接收到下行命令后对下发命令应答，用户设备收到下发命令后执行命令，平台会记录命令状态，并反馈用户完成命令下发流程。用户可通过南向设备侧或北向 API 接口方式实现设备数据上报、命令下发功能，极大提高应用开发效率。

平台支持设备通过不同类型的通信模块将数据上传到平台。平台通过数据流与数据点来组织设备上行数据，支持用户以数据流-数据点模型将数据上传至平台并进行存储，设备可以通过数据点 TOPI Topic 簇调用数据点存储服务存储数据，可以通过订阅系统 Topic 获取数据处理结果通知，如下图所示：

平台支持命令下发功能。支持应用通过 API 直接向设备发送命令数据，设备可以通过设备命令 Topic 簇获取消息命令并进行消息命令应答，完成数据下发流程。

5、数据转换

物联网设备接入后的数据通过对接园区数据，实现数据转换和加工处理。

运行管理

1、链接检测

平台提供对设备在线监控管理功能。平台实时发送心跳与设备保持连接，并实时监控设备的在离线状态、运行情况并记录，用户可通过平台页面、API 接口、

人工巡检上报、异常告警消息推送、拨打市民热线（400）等方式实时查看物联网设备的在/离线状态及故障情况，以便用户即时获取设备异常状态，方便用户定位、检测设备问题，减少因设备问题造成的损失，提高对设备管理维护的效率。另外，运维人员通过工单管理系统和人员账号/权限管理系统，对终端设备运维进行统一调度、分层派单管理。

平台提供根据数据情况定位设备在离线状态功能。提前置设备正常运行指标，预测设备故障点，降低设备误报率。通过高效的数据分析处理能力，提供自定义设备数据流类型和数据模板，采用实时数据流跟踪可视化方法，支持物联网数据高并发读、写操作，实现离线\实时数据的分析，从而实现设备在离线状态监控。

2、预警管理

支持通过自动记录故障发生前后一段时间内所有相关日志数据查看功能，以方便分析故障发生的原因。

支持在大屏监视器上全局性显示设备的运行情况和告警情况，支持通过实时预警、邮件、短信等多种方式提供设备告警。

3、运维管理

平台提供统一的设备统计信息概览页面，用户可以通过页面展示情况查询设备、API、推送消息以及下发命令情况整体接入和使用情况。

在设备统计报表上点击某个设备点位可以直接查看该设备最近一天的数据，可展示设备型号中的功能定义，展示对应的属性的值（以曲线或者表格的方式进行展示）。

用户也可以检索到对应设备，查看设备详情，大致分为两部分信息，一类是设备的基本信息（例如设备 ID、设备状态、设备类型、设备型号、供应商、权属机构、部署区域、地理位置、设备激活凭证等），一类是设备的动态实时数据，这是设备传输到云端的实时数据。

5G 专网建设方案

本项目中对于数据安全性以及网络通信稳定性的需求较高，但从需求上分析，所建设的基站在满足专网业务需求的同时，也要满足公众用户访问公网的需求，因此基站采用公有化部署方式。

同时综合考虑造价和园区业务需求对网络中断的容忍性，在园区内部署控制

面网元的需求性并不突出，只需讲用户面网元 UPF 下沉即可，因此本项目采用混合组网模式

本项目覆盖范围为物流通道和园区内 5G 覆盖

一、站点部署

马村港 - 综保区道路和园区内实现 5G 网络全覆盖，规划在马村港 - 海口综合保税区物流通道建设 7 个 5G 基站，物理围网内建设 8 个 5G 基站，后期在综合大楼仓库建设室内覆盖，详细情况如表。

图 5- 130　5G 站点分布示意图

具体部署站点如下：

序号	站址名称	配套	经纬	纬度
1	澄迈保税安基公司	共享铁塔（楼面）	110.044749	19.939453
2	澄迈上海家化日用品灯杆	共享铁塔（地面）	110.04883	19.94282
3	澄迈老城国社灯杆	共享铁塔（地面）	110.03562	19.94307
4	澄迈老城港航	共享铁塔（地面）	110.023887	19.945615
5	澄迈马村港泊口灯杆	共享铁塔（地面）	110.012722	19.957973
6	澄迈老城南一环路口灯杆	新建 25 米灯杆（地面）	110.041658	19.942671
7	澄迈老城白山路口灯杆	新建 25 米灯杆（地面）	110.029006	19.943519
8	澄迈马村港派出所	新建 6 米楼面抱杆（楼面）	110.022994	19.95097

9	澄迈海口保税区沙汀宁	新建 6 米楼面抱杆（楼面）	110.060401	19.940603
10	澄迈保税区中铁冷链南	新建 6 米楼面抱杆（楼面）	110.054473	19.939748
11	澄迈保税区大宗仓储园	新建 6 米楼面抱杆（楼面）	110.04912	19.94077
12	澄迈保税区跨境电商 C 座	新建地面 25 米灯杆	110.04538	19.937207
13	保税区 5G 规划站 1	新建地面 25 米灯杆	110.0532	19.95213
14	保税区 5G 规划站 2	新建地面 25 米灯杆	110.0571	19.95832
15	保税区 5G 规划站 3	新建地面 25 米灯杆	110.05965	19.962182

此外还需对海口综合保税区管委会大楼和园区内自有和企业仓库通过室内5G分布系统建设，进行信号的覆盖。

二、传输方案

沿园区管线敷设20公里24芯光缆，建成环状光缆网，对各站点AAU、RRU进行接入，实现AAU、RRU与BBU的光纤连接。新增2台MAR传输设备成组环形网，保证一侧光缆中断情况下基站仍能正常运行。

需要部署设备如下：

序号	设备名称	规格	单位	数量
1	传输设备	MAR	台	2
2	光缆	24芯管道	公里	20

5G边缘云建设方案

部署一套5G边缘云，具体包括1套用户面网元（UPF）和一套MEC，并部署相应的网元管理软件和边缘云管理软件，实现园区的5G业务数据的本地分流卸载，并承载园区的部分应用。

5G 边缘云部署方案

一、部署地点

在海口综合保税区主机房内部署 1 套 MEC，同时安装 2 个标准化机柜用于安装本次新增的设备。

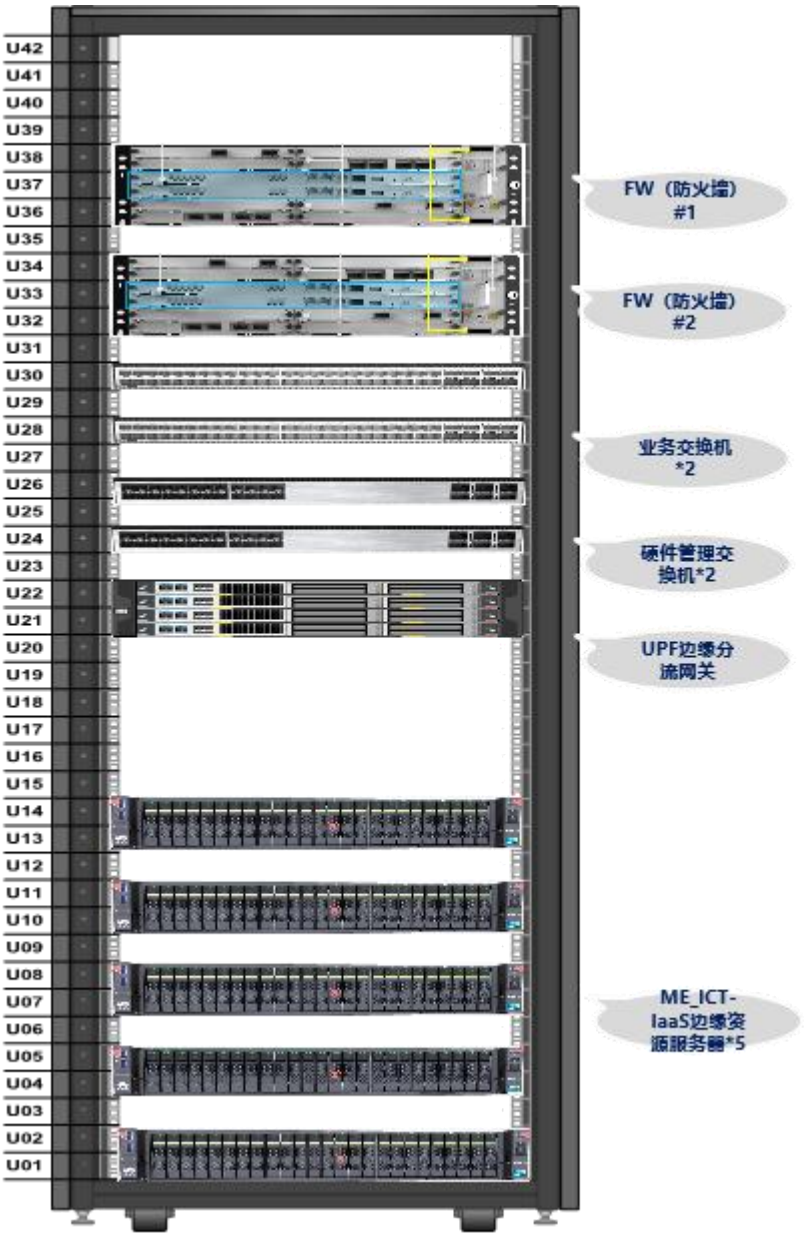
部署设备规模如下：

序号	设备类型	类型	数量
1	UPF 设备	硬件+软件	1
2	MEC 服务器	硬件	5
3	边缘云虚拟化软件	软件	1
4	MEC 防火墙	硬件	2
5	行业专网防火墙	硬件	2
6	业务交换机	硬件	2
7	管理交换机	硬件	2
8	标准化机柜	硬件	2

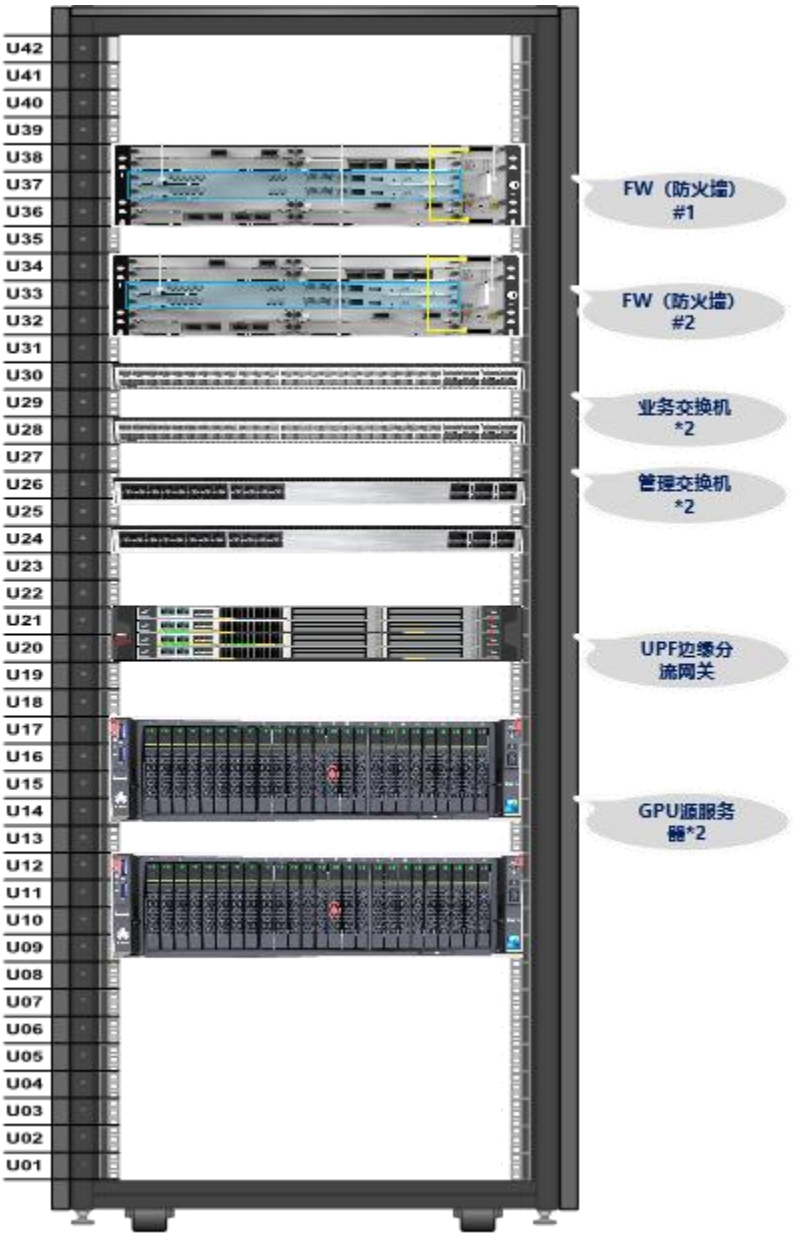
三、设备安装部署

本项目新增标准化机柜 2 个，用于安装本项目新增 5G 边缘云的服务器和交换机、防火墙等设备。设备安装如如下：

机柜 1：


U42
U41
U40
U39
U38
U37
U36
U35
U34
U33
U32
U31
U30
U29
U28
U27
U26
U25
U24
U23
U22
U21
U20
U19
U18
U17
U16
U15
U14
U13
U12
U11
U10
U09
U08
U07
U06
U05
U04
U03
U02
U01
FW（防火墙）#1
FW（防火墙）#2
业务交换机*2
硬件管理交换机*2
UPF边缘分流网关
ME_ICT-IaaS边缘资源服务器*5

机柜 2：



二、机柜配电要求：

本项目新增的设备采用交流供电方式，每个机柜输入电流 32A。机柜从 UPS 列头柜中引接电源，每个机柜从列头柜引接两路电源，分被连接到列头柜内 UPS 两路电源的电源端子上。每个机柜的功耗情况如下：

机柜 1

设备	单台功耗（W）	数量	功耗（W）
UPF 服务器	550	1	550
边缘云平台服务器	550	2	1100
业务交换机	350	2	700

管理交换机	150	2	300
边缘云服防火墙	350	2	700
	合计	12	5000
机柜标准	尺寸：深*宽*高（mm）	1000*600*2200mm/1200*600*2200mm	
	承重要求（KG）	270G	

机柜 2

设备	单台功耗（W）	数量	功耗（W）
UPF 服务器	550	1	550
GPU 服务器	1200	2	2400
业务交换机	350	2	700
管理交换机	150	2	300
行业专网防火墙	350	2	700
	合计	9	4650
机柜标准	尺寸：深*宽*高（mm）	1000*600*2200mm/1200*600*2200mm	
	承重要求（KG）	270G	

国际互联网数据专用通道工程

为保障顺畅的跨境互联网数据互通，有海南省工信厅和海南省通信管理局联合组织申报海南自贸港国际互联网数据专用通道，为海南自由贸易港建设国际合作平台、扩大产业开放提供高质量的通信基础设施，助力海南自由贸易港建设。

本工程由电信运营商根据，海口综合保税区有偿使用。国际互联网数据专用通道以园区为接入单位，服务于外向型企业、直达我国北上广国际通信出入口的专用链路。根据工信部批复，海南自由贸易港国际互联网数据专用通道主要覆盖海口综合保税区在内的 9 个园区，2020 年底前建成，2021 年 5 月正式投入使用。

根据工信部的批复，本项目在海口综合保税区设置国际专用通道节点，在园区机房设置汇聚交换机，上行链路接入波分节点，通过波分网络，接入电信运营商的核心路由器。核心/汇聚层利用 ASON 机制提供多重路由保护，接入层可提供

双路由的光通道保护。

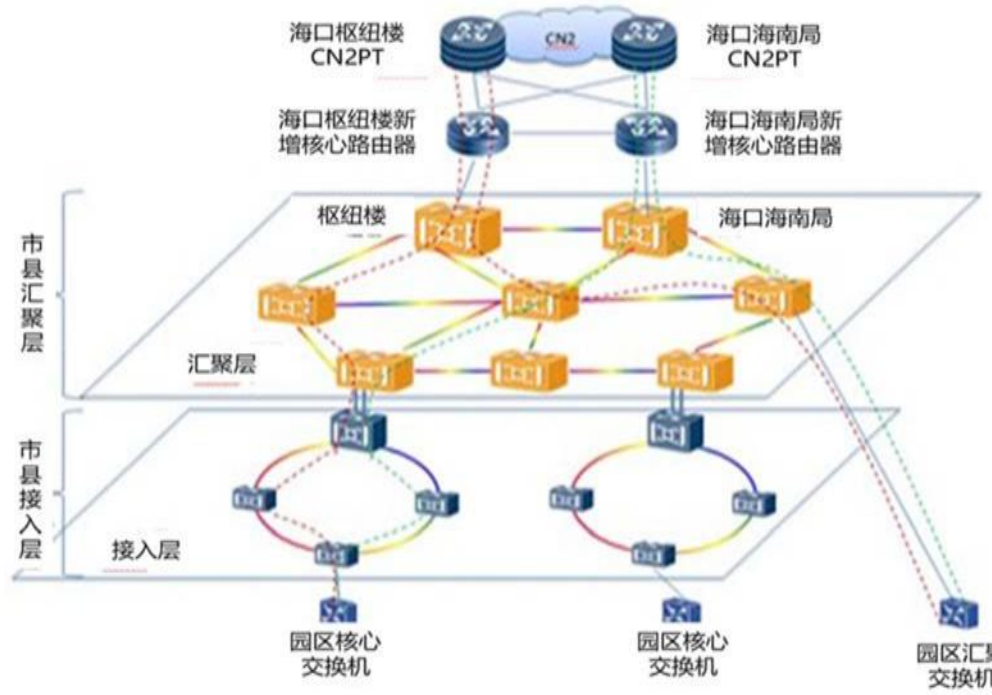


图 5- 134 园区互联网数据专用通道组网示意图

1、物理安全

多家主流电信运营商的光纤接入，选取两个以上物理路由，从路由上保证进入保税区的光缆物理路由安全。

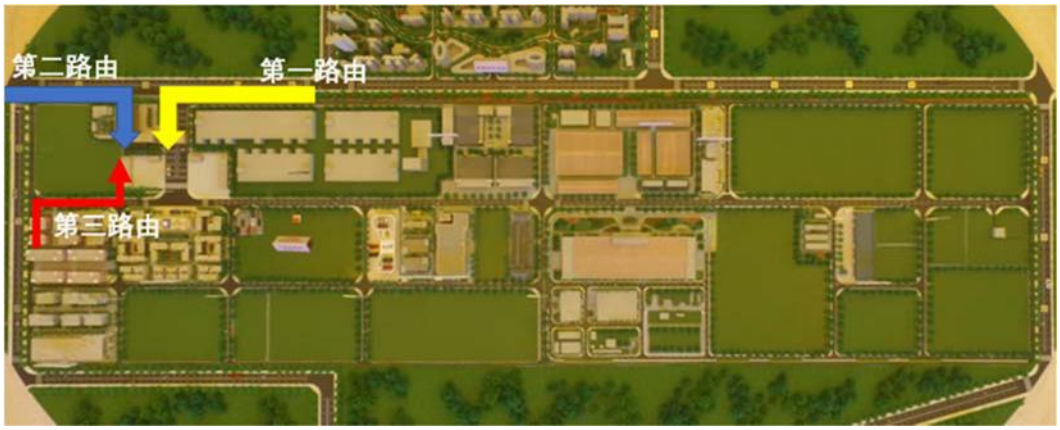


图 5- 135 保税区光缆接入路由示意图

保税区传输设备和服务器机房电力供应需要满足市电+后备电源的方案。

2、设备安全

获得主管部门认证的主流设备，设备性能满足现有业务和潜在业务的需求，并做好以下措施：

1)重要传输、路由器、服务器设备 1+1 备份；

2)各重要设备主控、业务板卡 1+1 备份。

国际互联网数据专用通道供园区企业客户接入专用，采用先进路由器设备和路由分离技术，对访问互联网资源的流量进行有效分流，充分保证重点大客户国际、国内互联网访问质量。同时考虑业务重要性和安全性，网络节点相关重要部件和模块配置均有冗余，确保国际互联网通信专用通道的网络和信息安全。

信息资源共享方案

共享原则

按照谁建设系统、谁负责对接的原则，各级政务部门要加快改造自有的跨层级垂直业务信息系统，并与智慧园区平台对接，实现跨层级、跨地域、跨系统、跨部门、跨业务数据互联互通，避免数据和业务“两张皮”，减少在不同系统中重复录入，提高基层窗口工作效率。

共享与交换模式

本项目应遵循统一的数据交换标准，交换数据统一封装、统一标识，实现系统之间、不同网络之间、异构系统之间的数据共享与交换。数据共享与交换模式包括定时交换、实时交换与应用集成。

●数据交换

采用数据共享与交换的方式实现本项目内数据的共享与交换。内、外网数据交换服务器之间的数据交换，通过硬盘等介质进行人工的方式交换数据。数据交换软件分别部署在内网和外网，各部门和地方需要交换的数据通过数据共享与交换服务器进行交换。

数据交换文件的类型有：文本、音频、视频等文件类型（实时图像采集、视频会议不是通过数据交换软件进行交换）。数据交换软件提供数据接入、数据适配、数据传输、数据转换和路由、交换过程监控、平台配置管理、日志管理等功能。

1)数据加载:采用多种数据加载方式,推荐 XML 文件格式和数据库加载方式。

2)数据适配：提供针对不同数据源数据的数据适配功能，包括文本、音频、视频等独立文件数据和异构数据库数据源等。

3)数据传输：提供数据传输的通道，并为数据传输的完整性、安全性提供保证，提供对大数据传输的支持。

4)数据转换与数据路由：提供配置数据转换规则及路由规则功能，可以根据用户的需求进行相应的定义。

5)交换过程监控：支持对整个数据交换软件中的交换过程进行监控，以保证交换的完整执行，同时在出现异常的情况下进行异常处理，保证数据交换的正确性。

6)配置管理：为数据交换软件提供配置管理功能，包括交换通道的建立、交换策略的选择等。

●数据共享

业务数据共享通过信息资源目录和服务总线等技术实现，资源目录采用轻量级目录访问协议(LDAP)。

按照统一的标准和规范，建设信息资源目录体系。根据业务需求，对相关的信息资源进行编目，生成信息资源目录：对共享信息资源的目录信息进行统一管理，提供准确的应急信息资源的发布、发现和定位服务，以及信息资源目录的访问控制。

数据提供单位根据共享交换系统确定的信息资源目录体系结构及注册机制，在数据共享交换系统上进行目录内容注册，并负责以后的维护工作。信息使用单位调用数据共享交换系统提供的目录服务，查找信息资源目录，定位目录内容相关联的信息资源，从相关系统中获得信息，从而实现信息共享。

数据接口要求

需采集不同的业务数据，集中大数据也需要共享给不同的业务系统，为保证数据查询完整性和有效性，需开发针对不同系统的数据接口。

- 基于 Web Service 方式：

Web Service 使用标准技术，应用程序资源在各网络上均可用。因为 Web Service 基于 HTTP 、XML 和 SOAP 等标准协议，所以即使以不同的语言编写并且在不同的操作系统上运行，它们也可以进行通信。

- 基于消息中间件：

消息中间件能够在任何时刻将消息进行传送或者存储转发，不会占用大量的网络带宽，可以跟踪事务，并且通过将事务存储到磁盘上实现网络故障时系统的恢复。

➢ 基于数据文件：

文件接口不需要其它软件支持，只要接口双方约定好路径、格式、处理方式即可，实现简单、传输批量数据效率较高。

➢ 基于数据中间库：

中间库接口不需要其它软件支持，只要接口双方做好相关约定即可；但接口没有统一标准，而且需要开放数据库权限，安全性差。

系统接口采用开放式的接口管理技术。系统提供了丰富的接口以及接口的参数定义描述，便于和其它系统进行数据交换，凡是基础数据库定义的信息项都必须有相对应的数据接口。提供接口数据交换管理平台对各类信息交换接口进行有效的管理。

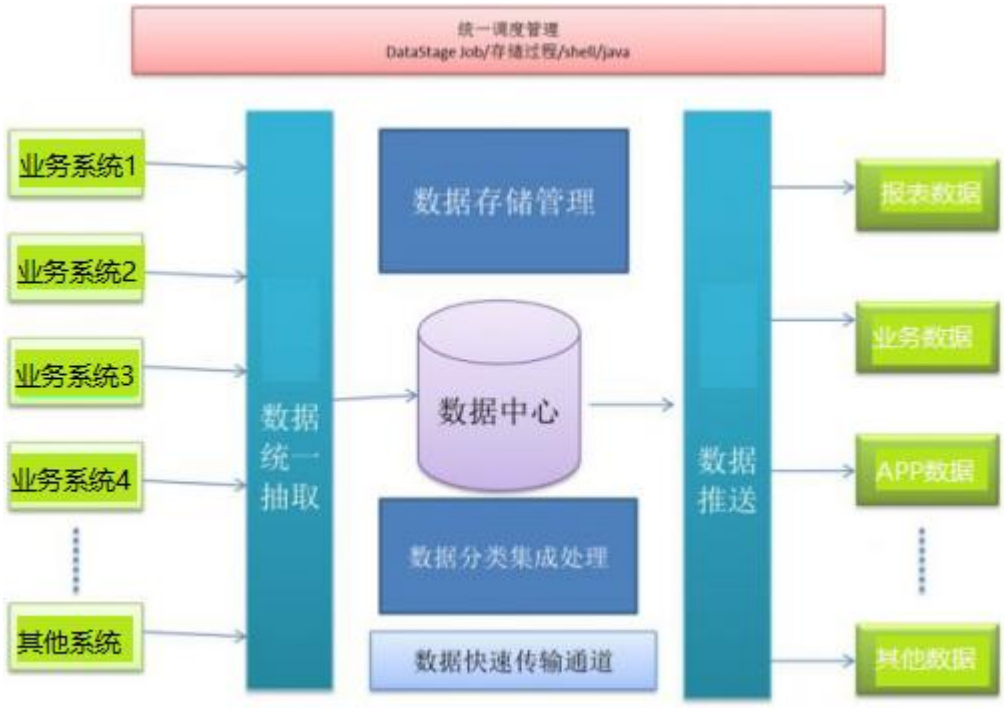


图 5- 4 数据接口示意图

开放式接口技术主要应用于如下场景：

➢ 统一应用接口

平台需要集成多种应用服务，同时满足不同业务需要，必须要实现基于国家规定的相关信息标准，实现统一的应用接口实现系统的集成与扩展应用能力。

➢ 集成方式与接口

平台需要和不同系统进行数据交换，既有可能是现有应用集成提供的服务，又有可能是第三方开发的系统服务，系统必须要实现这些应用服务中使用数据的转换与映射，从而提供多应用集成的交互功能。

系统提供了数据集成接口、身份认证集成接口、消息集成接口等大量集成接口，可无缝的完成与后续建设的数据交换系统、身份认证平台、消息集成平台进行对接，实现数据的共享、身份信息的统一认证、单点登录、一站式的消息推送服务等。

- 接口类型

包括身份信息数据接口、组织机构信息数据接口、系统交互数据接口、资源同步及备份接口、权限信息数据接口等。

- 集成提供方式

集成提供方式包括表数据集成、视图集成、存储过程与快照集成、格式化数据文件集成等。

- 集成接口

JMS 消息、Webservice 接口、SOA 数据总线、数据视图、数据订阅、数据文件、Hadoop 大数据同步接口等。

- 应用的二次开发能力

根据《海南省政务信息整合共享专项行动实施方案》（琼府〔2017〕77 号）政府文件的规定，本项目不再单独建设独立的信息共享交换平台，统一利用省信息共享交换平台及部门和市县节点进行数据共享交换，利用省政务大数据公共服务平台进行行业大数据的采集和挖掘应用，依托省政务数据开放平台开放政务数据，向公众提供数据查询、数据下载、应用接口等服务。

信息共享方案

在智慧园区中，所有进出口企业与执法单位、政府管理部门之间的数据往来与共享通过该系统进行交换、处理、转发，根据调研结果与需求分析结果有数据交换需求的有：海关、交通海洋局、海南省单一窗口、大数据管理局等多家单位及平台对接；平台交换、处理、转发数据内容分别有：舱单、报关单、通关状态数据、卡口进出门信息、账册数据、装卸信息、承运资质、在途信息、堆场信息、危运信息、船舶信息等多类数据。

与海南省政务服务网对接

海口综保区智慧园区平台需要实现与海南政务服务网对接，与海南省政务服

务网中海口综保区的数据同源整合管理，面向智慧政务服务需求，对实现对海口综保区所有事项清单展示、政务服务办事指南、政务服务政策解读、热点政务服务、政务服务事项在线申报、政务服务事项审批公示、办理进度、结果查询等。

一、“海易办”

1、依托“一人一码、一企一码”的一码通平台，提供个人数字空间、法人数字空间，关联各类电子证照，提供亮证办、亮码办等服务。

2、提供政务办事掌上预约、掌上查询、掌上办事等服务。

3、提供各类便民、便企的公共服务、自贸港服务，包括老年证申领、高龄老人补贴申领、社保查询、公积金查询、中小学学位申请、电子证照查询服务。

二、“海政通”

1、移动协同即时通讯服务，包括文字通讯、语音通讯、视频会议等，各级政府机关单位组织通讯录。

2、海政通集成应用上线服务，包括移动 OA 办公系统应用服务、省府办网上督察系统应用服务、省财政厅公务报账系统应用服务、应急厅救灾物资查询服务、省市监局（综合查询系统服务、移动监管系统服务、移动执法系统服务）、疫情防控共享信息查询服务、精准扶贫专题分析服务等各类集成应用服务，实现各级机关办公、协同应用统一入口及单点登录。

3、机关内部办事统一入口，实现跨层级、跨地域、跨部门、跨系统、跨业务的协同管理与服务。

与海南省行政审批系统对接

通过与海南省行政审批系统对接，基于统一数据接口，获取申报人及申报材料信息，实现管理局各项行政审批事项线上一窗受理。同时，智慧园区需要通过数据接口，向海南省行政审批系统共享各类行政审批结果数据，包括用地许可、规划许可等信息，供其他相关部门及社会公众使用。

与海南省 “ 多规合一 ” 信息综合管理平台对接

海口综保区智慧园区平台需要实现与省级“多规合一”信息管理平台对接，调用“多规合一”规划数据，获取园区上位规划要求及与周边规划衔接性要求，

从而支撑园区领导者管理决策。

与海南省大数据公共服务平台对接

海南省大数据公共服务平台是海南省大数据管理局的政务大数据中心，承担着海南省各省级部门业务数据的汇集和管理工作，是全省政务数据的数据中台和数据仓库，大数据公共服务平台扮演着省内各个厅局的数据共享和交换的枢纽角色。需要通过基于统一的平台服务及数据接口，对接海南省大数据公共服务平台，实现省级与园区政务服务数据的共享交换，实现省区信息数据共享。

需求的数据服务：

序号	服务类别	服务名称	服务内容
1	基础库服务（Daas 层）	人口基础库	1.提供婚姻家庭方面的婚姻和户籍等信息； 2.提供教育就业方面的学籍、学历、就业、职业资格等信息； 3.提供行政执法方面的行政处罚、行政确认、行政强制等信息； 4.提供社会保障方面的参保、五险、低保等信息； 5.提供信用评价方面的失信、限高等相关不良信息； 6.提供资产负债方面的个人不动产、动产等相关信息。
2	基础库服务（Daas 层）	法人基础库	1.提供企业登记信息和企业法定代表人信息； 2.提供社会保障方面的企业法人参保等信息； 3.提供资产负债方面的法人不动产、动产等相关信息； 4.提供生产经营方面的法人生产经营等方面信息； 5.提供行政执法方面的企业法人相关行政

			处罚、行政确认、行政强制等信息； 6.提供信用评价方面的企业法人失信、限高、黑名单等相关不良信息。
3	基础库服务（Daas 层）	社会信用库	1.提供基本信息方面的信用主体基本状况信息； 2.提供业务信息方面的信用主体经营状况、司法、行政执法等信息； 3.提供公用事业方面的司法机关、行政机关和公用事业机构等单位的履职过程产生的有关各类市场主体的信用信息； 4.提供信用评价信息方面的依法行使公共职能的部门履职过程产生的有关各类市场主体的信用评价信息，以及信用主体保护自身合法权益产生的其他信用信息。
4	基础库服务（Daas 层）	电子证照库	1.向符合应用场景的部门提供营业执照、结婚证、食品生产许可证等 67 类电子证照接口服务； 2.提供电子证照制证服务，如集成电子印章，可对外提供电子证照制证接口生成 OFD 电子证照，支持电子证照制发、预览、打印、下载； 3.提供电子证照用证服务，包含电子证照信息列表、电子证照照面信息、OFD 电子证照文件、PDF 电子证照文件、电子证照预览验证等。
5	基础库服务（Daas 层）	空间地理库	1.提供电子地图、专题地图、地名地址等 220 项数据及功能接口服务，已覆盖全岛的标准地名地址数据 150 万条。 2.可提供道路卡口、电子地图等 66 个目录，供各省直单位进行数据交换，实现业

			务协同。

与 “ 电子政务+ + 监管 ” 系统对接

本项目需与海南省相关“互联网+监管”系统对接，具体监管内容及接口建设如下：

1、办件过程数据采集相关接口：

办件受理信息采集接口

办件受理信息批量采集接口

办件过程信息采集接口

办件过程信息批量采集接口

办件结果信息采集接口

办件结果信息批量采集接口

特别程序信息采集接口

特别程序信息批量采集接口

材料目录信息采集接口

材料目录信息批量采集接口

办件补正信息采集接口

办件补正信息批量采集接口

领取登记信息采集接口

领取登记信息批量采集接口

2、咨询投诉数据相关接口

诉求人信息接口

话务信息接口

工单信息接口

政务服务应用诉求内容信息接口

政务服务大厅诉求内容信息接口

工单关联信息接口

撤单申请信息接口

延期申请信息接口

处理反馈信息接口

办结信息接口

好差评信息接口

3、运行指标相关数据接口

效能考核信息接口

效能考核申诉信息接口

与商务厅外综服平台等对接

一、外综服平台

外综服与电子口岸的接口主要功能是满足平台在线报关和无纸化通关的需求，基于这个需求，接口应该包含三个主要功能：

（1）报关申报数据推送，由外综服平台向电子口岸推送报关申报数据，内容主要包括下列数据项：

出口报关单表头：申报单位代码、申报单位名称、批准文号、提单号、合同号、录入单位代码、录入单位名称、主管海关（申报地海关）、征免性质、数据来源、报关/转关关系标志、装货港、境内目的地、报关标志、海关编号、报关单类型等。

报关单表体：归类标志、商品编号、备案序号、申报单价、申报总价、征减免税方式、货号、版本号、申报计量单位与法定单位比例因子、第一计量单位（法定单位）、第一法定数量、申报计量单位（成交计量单位）、商品规格、型号、境内货源地等。

报关单集装箱：集装箱号、集装箱规格、集装箱自重

随附单证：单证代码、单证编号

（2）节点状态返回：电子口岸向外综服平台返回报关各节点的状态，内容主要包括下列数据项。

报关信息推送时，单一窗口接口返回信息回执：接收成功、重传文件、上载失败等；

海关审核过程中，单一窗口接口返回各节点的审核状态：申报成功、上载未申报、上载申报失败、海关已接收、担保放行、不被受理、需手工申报、退回修改、报关单已审结、放行交单、需交税费、申报失败、海关删单、报关单重审、

已结单等

（3）结关数据返回：电子口岸向外综服平台返回最终结关数据，内容主要包括下列数据项。

出口报关单表头：申报单位代码、申报单位名称、提单号、合同号、主管海关（申报地海关）、征免性质、装货港、境内目的地、报关标志、海关编号、报关单类型等。

报关单表体：归类标志、商品编号、备案序号、申报单价、申报总价、征减免税方式、货号、版本号、申报计量单位与法定单位比例因子、第一计量单位（法定单位）、第一法定数量、申报计量单位（成交计量单位）、商品规格、型号、境内货源地等。

二、EDI 交换平台

本项目从 EDI 获取以下数据：

序号	功能组件名称	功能简述	共用共享实现方式
1	船舶服务信息	船舶基本信息、船舶靠泊计划、拖轮、引航计划、船舶作业动态、在港动态、船舶轨迹、船舶数据	API
2	码头社区信息	进出闸、装卸船动态，提还箱动态、堆存动态、残损、码头作业动态、箱量、吞吐量等	API
3	场站信息	提送货委托、拆装箱委托，拆装箱和提送货作业动态	API
4	货物信息	放货信息：船公司船代允许换单指令、放货指令、费用查询等；放箱信息：船公司船代用箱期查询、放箱指令、协议车队查询、电子 EIR 确认等	API
5	车辆信息	车辆备案信息、车辆跟踪、车号识别信息、车辆证书信息、检验信息	API
6	人员信息	司机信息、证件信息	API
7	基础信息	港口信息、泊位信息、仓库信息、锚地信息、岸线信息	API

8	资质及诚信信息	港口经营企业资质、水路动输企业资质、车辆运输企业资质、仓储企业资质、船舶服务企业资质，企业诚信评价等	API
9	环保信息	岸电使用信息	API
10	防疫信息	船舶、货物、人员防疫管理信息	API
11	司机作业信息	电子小票、核放单申报	API/EDI
12	全口径舱单信息	内外贸舱单信息、理货信息、运抵信息等	API/EDI
13	物流信息	单票货物串联的全流程物流动态信息及业务办理动态信息	API

三、国际贸易（海南）单一窗口等

本期系统数据共享及需求如下：

业务		所需数据	来源系统	对外提供数据内容
基础通关服务	贸易便利化服务	企业装箱单、合同、发票等信息	企业 erp	报关单信息
	跨境电商公共服务	订单、运单、支付单、清单、报关单	单一窗口	
	启运港退税			
通关增值服务	外贸综合服务			
	数字贸促	/	/	企业信息、项目信息、商品信息
	金融结算便利化系统	1、报关单数据； 2、核注清单数据； 3、结算结果数据；	1、海南国际贸易单一窗口 2、国家外汇管理局跨境区块链平台	1、结算验证结果数据； 2、结算数据(报关单&核注清

				单)数据。
	口岸检测技术服务协同	相关政策信息 客户需求 检测资源 检测报告	第三方检测机构 海关实验室	政策信息 检测资源
智能监管		码头装卸数据、堆场进出数据、场站出入数据	港航 EDI	/
进口高风险货物管理		舱单数据、报关单数据、消杀证明	单一窗口或海关	通关节点
物流协同		查验放行信息 通关物流单证信息（如提单、舱单、设备交接单、装箱单、提货单） 单证节点信息 物流节点信息 集装箱在场信息	单一窗口 港航 EDI 海关 船舶公司（船代） 货主（货主、报关行）	通关信息 节点信息
多式联运公共服务		船期数据	港航 EDI	联运节点信息
		舱单数据	港航 EDI	同船信息
通关时效		船舶申报信息、码头社区信息、货物申报及回执信息、场站信息	港航 EDI、单一窗口或海关	

与其他相关省市委办局信息系统对接

在海口综保区业务事项办理及管理过程中，需要基于统一的平台服务及数据接口，与发改、工商、税务等部门进行信息互通共享。如面向园区企业财政奖励，需要通过对接工商、税务部门相关系统，获取企业营收、税收相关信息，辅助园区企业管理。

园区智慧消防系统与省消防管理平台对接，实现消防报警、消防巡检、重大消防事件等相关数据的上传下达、消防救援的联动指挥。

园区应急管理系统与省应急管理平台对接，实现应急预案管理、应急资源管理、重大应急事件等相关数据的上传下达、重大应急救援的联动指挥。

数据资源建设与数据开放应用（服务）方案

数据资源规划

智慧园区平台的信息资源规划与数据库建设主要实现本项目业务范围内各类信息资源的科学组织和综合管理，为各个应用系统提供集成的数据处理环境，并为部省之间、省市之间提供可靠的数据交换服务。

数据资源规划思路

主要通过整合省内各园区信息资源、园区运行基本数据，以及对数据的统计和分析，形成综保区智慧园区平台数据库。

数据资源内容类别分析

智慧园区平台信息资源包括：基础数据、业务数据、动态监测数据、空间信息数据资源、主题数据资源、共享数据资源等六大类，具体分类如下：

资源分类	具体内容
基础数据资源	园区运行基础信息数据、行政基础数据、生产经营单位基础数据、从业人员基础数据、建设项目基础数据等
业务数据资源	园区生产、物流等业务数据，审批业务数据、监督考核数据等
动态监测数据资源	包括储存货物信息、视频监控信息等
空间信息数据资源	包括数字线划图、高清影像、数字高程模拟、储罐三维模型、压力管道三维模型、其他附属设施三维模型等
主题数据资源	包括流量统计分析、安全隐患分析决策、事故统计分析、安全业态综合分析、行业信用统计分析等
共享数据资源	包括共享基础数据、业务协同数据、应急资源共享数据、园区从业企业、从业人员的基础数据和信用数据等

数据资源采集及共享

本项目的数据采集方式主要包括：人工录入、数据交换、数据导入、数据接口调用、现场勘测等 5 种方式获得。根据园区现有各类数据资源采集情况，结合各类数据源的特点及数据更新及交换要求，综合考虑网络条件，确定不同类型的数据采用不同的数据采集方式。

基础数据

基础数据主要采集园区基础数据，系统将主要通过人工录入、数据对接导入、数据整理抽取的方式进行采集。

业务数据

业务数据主要采集省厅各业务系统的业务数据、行政审批业务数据等，以及监管企业的数据，系统将主要通过人工录入、数据对接及导入的方式进行采集。

动态监测数据

物流数据主要采集从事货物储存运行的企业的动态信息数据，数据将主要通过 WebServcie 等数据接口方式进行采集。

视频监控数据主要采集园区视频监控数据，数据将通过平台提供的 SDK 开发工具和 API 接口实现管理、调看、控制等业务。

空间信息数据数据

数字线划图数据和高清影像数据主要采集空间信息，数据将通过 WebService 等服务接口方式从地理信息服务平台进行采集。

主题数据

主题数据主要通过建立数据分析处理模型，对基础数据、业务数据、动态监测数据及空间信息数据等进行统计查询分析、形成一个个主题数据分析结果。

共享数据

共享数据主要充分调研考虑平台各系统之间、平台与外部之间的数据交换共享需求，根据数据交换共享需求实现将所需数据进行抽取整理，统一推送到数据交换共享平台进行数据共享。

数据库设计方案

一个完整的数据库解决方案的系统体系架构中主要包括数据采集层、数据整合层、数据存储和管理层、数据服务层。对于平台的数据库逻辑结构建设架构如下图所示：

数据库逻辑架构示意图

一、数据采集层

对应数据采集层存在形式的数据，本项目在数据采集层主要围绕基础数据的生产对象，进行对数据的采集。

数据采集主要基于互联网、Web 技术、数据接口、移动互联网、三维图像绘制技术等有效采集高质量的基层统计数据，实现以网上直报为主的多种方式的数据采集管理，通过多元化的采集手段全面采集各类数据。

二、数据整合层

数据整合层对通过上述方式采集到的数据进行整合，具体过程包括数据处理、数据融合。数据整合层首先对采集的数据进行处理，过滤掉无效数据，调整数据结构；然后，按照数据库的统一需求对数据进行融合；最后将采集到的数据载入相应的库。

三、数据存储与管理层

数据存储与管理层构建满足项目需求的数据库，是整个数据库的核心，用于存储和管理来自各种源数据的基础数据和指标。在数据资源存储与管理层，由数据采集层采集的数据按照主题进行组织、重构和存放，包括当前数据和较长时期

的历史数据。

四、数据服务层

该层基于数据库中数据资源，为用户访问数据库提供各种方式的服务，从而实现访问方式的多样化和信息存取的透明化。根据各项应用所需数据资源的属性和使用要求，并按照相关技术要求，确定本工程将建设基础数据库、业务数据库、动态监测数据库、空间信息数据库、主题数据资源和共享数据库。

基础数据库

基础数据库是独立于具体的业务应用，为行业多种业务提供支撑，有较强共享需求的数据库。本工程新建或完善以下基础数据库：

（1）园区管理机构与职责基础数据库

通过人工整理数据录入的方式，建设覆盖园区管理职责的各级组织机构信息，主要包括机构名称、管理职责、基本情况、从属关系、主要岗位等。

（2）生产经营单位基础数据：包括企业名称、统一社会信用代码、企业所属领域、企业类型、法定代表人；企业资质信息、企业良好信息、企业不良信息等

（3）从业人员基础数据：包括主要负责人基础数据、法定代表人基础数据、主要技术负责人基础数据、安全管理人基础数据等。内容包括从业企业名称、姓名、身份证号；人员执业资格信息、人员良好信息、人员不良信息等。

业务数据库

业务数据库是与某一业务应用相联系，在该项业务生产活动中产生、存储和动态更新的数据库。

主题数据资源

主题数据库来源于基础数据库和业务数据库，采用面向主题的方式，对原始数据进行清洗、抽取、转换、加载，形成针对某一主题的综合数据支持库，主要用于运行分析、辅助决策等综合性应用。

（1）园区运行主题数据库

本工程将建设完善园区运行主题数据库主要包括园区生产主题数据、园区运行主题数据、园区服务主题数据与规划辅助决策主题数据等。

（2）综合信息服务主题数据库

主要数据内容包括政务公开信息(包括全国政务公开信息、省级政务公开信息、工专题信等)、投诉举报信息等。

（3）园区运行信息资源目录

按照相关要求，梳理本工程所形成的需共享的数据资源，通过对接省市级信息资源共享交换平台，注入政务信息资源目录。

园区数据资源目录

序号	类型	数据	是否可公开
1	基础设施	仓库基础信息	可以公开
2		停车场信息	可以公开
3		物业管理信息	不可公开
4		园区电子地图	可以公开
5		视频监控	有条件公开
6		虚拟展馆和展台	可以公开

7		门店信息	可以公开
8		园区租赁资源	有条件公开
9	货物及商品	商品基础信息	不可公开
10		车辆备案信息	不可公开
11		车辆轨迹	不可公开
12		到货商品信息	不可公开
13		艺术品鉴定信息	不可公开
14		商品出入库信息	不可公开
15		订单信息	不可公开
16		商品归类预裁定信息资源库	不可公开
17		商品物流信息	不可公开
18	人员	党员信息	不可公开
19		访客信息	不可公开
20		区内工作人员信息	不可公开
21	企业	企业基础信息	不可公开
22		企业金融授信额度	不可公开
23	单证	跨境电商订单、清单信息	不可公开
24		订单物流节点	不可公开
25	园区运营管理	视频数据	有条件公开
26		消防数据	有条件公开
27		能效数据	有条件公开
28		应急数据	有条件公开

29		管理数据	有条件公开
30		运营数据	有条件公开
31		统计信息	有条件公开

数据迁移设计方案

本项目原先采用省统计局系统报送的数据及纳统企业数据需要进行迁移到新建系统中。迁移方式采用数据库迁移，因系统安全问题无法采用接口等方式与统计局系统进行直连，需要当前新建系统给出数据库表结构模板，由用户方进行旧数据填充，拿到旧数据表后，在数据库进行导入。

主要迁移数据包含：企业信息、纳统数据（园区单位人才调查表、园区工业单位主要指标调查表、园区工业单位主要产品产销量调查表、园区第三产业企业单位主要指标调查表）。

企业信息主要包含：企业名称 、统计员 、办公电话、 手机、 备注、其他联系人、 社会信用代码 、组织机构代码、 地址、 填报类别、 所属片区、 行业分类、 高新技术企业、 外资企业 、规上企业。

园区单位人才调查表主要包含：从业人员人数（人）、中专学历、高中学历、大专学历、全日制本科学历、硕士研究生学历、博士研究生学历、中级专业技术资格、高级专业技术资格、中级技师职业资格、高级技师职业资格、外籍人员人数（人）、A 类、B 类、C 类、高层次人才人数（人）、柔性引进的高层次人才。

园区工业单位主要指标调查表主要包含：工业总产值、工业销售产值、出口交货值、进口货值、资产总额、固定资产原价、本年折旧、营业收入、主营业务收入、营业成本、主营业务成本、营业税金及附件、主营业务税金及附件、销售费用、管理费用、财务费用、投资收益、营业利润、利润总额、实际上缴费总额、

应付职工薪酬、应交增值税。

园区工业单位主要产品产销量调查表主要包含：主要产品一产量、主要产品二产量、主要产品三产量、主要产品一销量、主要产品二销量、主要产品三销量。

园区第三产业企业单位主要指标调查表主要包含：商品销售额、仓储收入、技术服务收入、进出口总额、出口总额、进口总额、从业人员期末人数、海外留学归国人数、外籍常驻人员、资产总额、固定资产原价、本年折旧。

云服务方案

作为未来海口综合保税区信息化建设、数据资源融合、管理、调度的基础和枢纽，将根据前面业务应用的建设，建成以物联网管理、视频智能分析、GIS、统一认证和鉴权以及大数据处理服务、信息资源共享交换为主要构成的海口综合保税区“智慧园区”数字平台，以支撑保税港区未来发展对信息化的需求。同时，按照海南省发布的《智慧海南总体方案（2020-2025》的总体规划，预留、开放与海关总署、省级、市级监管中心和管理平台的对接接口，形成基础架构一次成型，未来业务快速上线，构筑未来“基础平台平滑扩容，业务系统持续叠加”的建设模式。

依托上级大数据云平台，充分利用本地边缘计算和存储资源，支持根据业务应用的不同特点分配不同的计算资源，包括采用合理的物理服务器和虚拟服务器。能根据业务应用的特点对服务器或存储进行配置满足应用对计算和存储需要（CPU、内存、网络 I/O、存储 I/O）。计算平台需要和管理平台联动实现对虚拟计算资源的部署和分配。

总体架构

按照业务职能，构建自治、灵活集成的功能中心。功能架构如下：

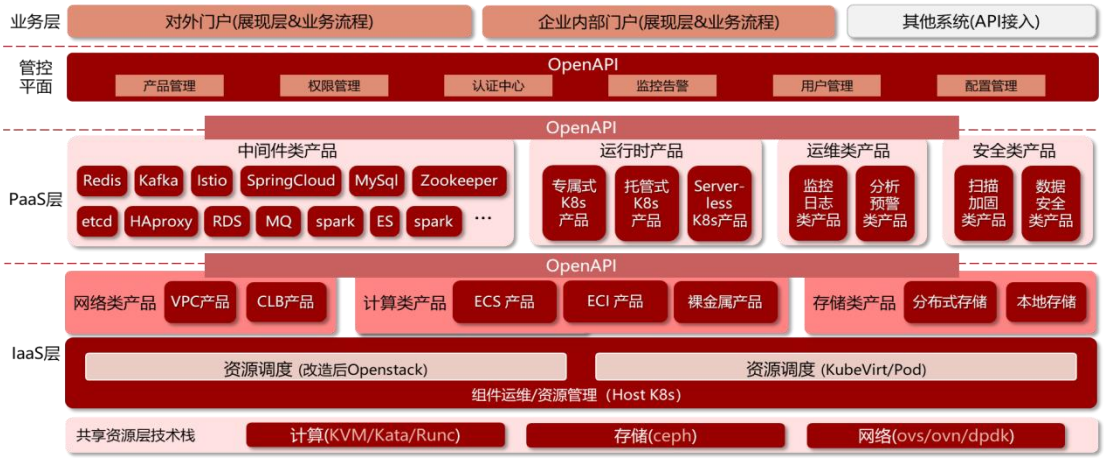


图 云数据技术架构图

云服务资源规划

本项目应用软件开发与系统部署需新增部分信息化设备、系统软件，本项目的系统开发与设备选型应坚持项目的建设目标符合海口综保区及海关监管技术要求与业务要求的原则，同时应在充分利用现有的软硬件设备基础上，考虑业务和技术要求以及设备性价比，依据安全性、稳定性和业务实际要求等原则分别选用配套的软件、硬件。

架构设计

服务器虚拟化技术很好地解决了传统服务器系统建设的问题，通过提高物理服务器利用率大幅度削减物理服务器购置需求、数量和运维成本；通过利用服务器虚拟化中 CPU、内存、IO 资源的动态调整能力实现对业务应用资源需求的动态响应，提升业务应用的服务质量；通过在线虚拟机迁移实现更高的可用性和可靠性以及各种基于资源优化或节能减排策略的跨物理服务器的调度等等。因此，服务器虚拟化技术是新一代数据中心最理想的解决方案。

服务器虚拟化架构设计是服务器虚拟化技术运用的核心。服务器虚拟化架构设计直接决定了整个服务器资源体系对应用系统的承载能力、运行效率以及可靠性。必须根据行之有效的设计方法从多个方面和维度进行综合考虑而得出。服务器虚拟化架构设计方法如下：

1、所承载的应用系统架构的疏理；

2、充分分析所承载的应用系统的特性，根据应用特性疏理虚拟化支撑关键点；

3、分析服务器虚拟化技术的性能、可靠性、可扩展性、成本，对关键点的满足能力；

4、综合各种服务器虚拟化技术对关键点的支持能力，得出虚拟化技术的选择以及应用方式；

5、根据总体的性能、可靠性、统一管理原则，构造统一的服务器虚拟化体系。

承载应用系统类型分析

经过对本项目的需求进行分析，可以疏理出本项目中所承载的应用系统主要包括二层架构（应用层－数据库层）和三层架构（接入层－应用层－数据库层）的应用系统。两种应用系统架构在部署时，各层分别需要一个或多个虚拟服务器来承载，虚拟服务器的配置和数量依赖于各层应用的特性来决定。在所有的应用系统中，根据所承载的应用系统分为大访问量应用系统、大计算量应用系统、大数据量应用系统三类。

1、基于 Web 的大访问量、简单处理型应用系统

大访问量应用系统如 WWW 网站等 web 类应用系统，这类应用的特点是业务逻辑简单，不同业务请求互不关联，但请求的并发量根据业务特点不同可能很大。

大访问量应用系统要求对大量互不关联的并发请求进行快速响应。这种情况下，需要应用服务器有足够数量的线程响应请求，而单个线程计算量不大，因而对单个 CPU 处理性能要求不高，可通过提供足够 CPU 数量或应用服务器数量来满足需求。通过虚拟化技术为大访问量应用系统部署是大量小配置的虚拟机作为应用服务器，多应用服务器工作在负载均衡模式，提升用户使用体验。大访问量应用系统对数据库要求不高，配置一般虚拟机即可满足要求。

2、大计算量的应用系统

大计算量应用系统，这类应用的特点是计算量较大、运算复杂、内存需求大，应用逻辑对服务器计算性能要求高。这种应用系统由于通常应用逻辑的串行性不能实现分布式设计，对于单一应用层服务器要求高，体现为需要配置较高的单一

个虚拟服务器，建议配置单一高性能虚拟服务器。因而，该种应用需求的虚拟化技术支撑点是配置较高性能的应用层虚拟机，接入层、数据库层作常规配置。

3、大数据量处理的应用系统

大数据量应用系统，根据数据存储模式不同，可分为文件型和数据库型的系统。

数据库型大数据量应用系统要求较高性能数据库服务器。建议配置强大的数据库服务器，提供足够的 CPU、Memory 及 IO 性能来处理大量的数据，根据应用系统重要级别，数据库服务器可以选用虚拟物理器或物理服务器，应用服务器业务逻辑简单，对配置要求不高，配置一般虚拟机即可满足要求。

文件型大数据量应用系统基础数据量大，通过传统的集中存储方式，存储并发读写 IO 能力无法满足计算资源要求，建议通过并行计算模型实现。根据业务计算特点，服务器可灵活选择虚拟机或物理服务器。

云计算服务

计算服务

弹性计算服务

弹性计算服务为用户提供的一种可随时自助获取，按需租用虚拟计算资源的云服务。用户开通的云服务器实例是一个虚拟的计算环境，包含了 CPU、内存、操作系统、磁盘、带宽等最基础的服务器组件。一个实例就是一台虚拟机。对自己创建的实例，租户拥有管理员权限，可以进行多项基本操作，如挂载磁盘、添加网卡、创建镜像、部署环境等。

弹性计算服务提供了多层次的安全防护和保障，包括主机操作系统安全、虚拟机隔离、安全组等。通过从虚拟机到主机再到整个组网的整体安全设计，为用户打造安全可靠、灵活高效的应用环境。

镜像服务

镜像是一个包含了软件及必要配置的云服务器模版，包含操作系统，还可以包含各种预装的应用软件（例如，数据库软件）。镜像分为公共镜像、私有镜像和共享镜像。公共镜像是为操作系统提供的标准镜像，私有镜像是用户自行创建的镜像，共享镜像是用户自己定义并分享给其他用户的镜像。

弹性伸缩

弹性伸缩服务是用户根据业务需求，通过其预先定义的伸缩配置和伸缩策略自动按需调整资源的服务。弹性伸缩服务在运行中无需人工干预，就可使资源使用量符合业务当前的需求。在业务增长时实现应用系统自动扩容，业务下降时实现应用系统自动减容。从而既能帮助用户节约计算资源和人力成本，又能保证其业务平稳健康运行。弹性伸缩服务对执行计算资源调配和管控策略的自动化特性有助于避免资源争夺类攻击或租户管理人员在调配资源时人为操作失误所造成的安全风险。

存储服务

云硬盘服务

云硬盘是一种基于分布式架构的，可弹性扩展的虚拟块存储设备。可以在线进行操作，使用方式与传统服务器硬盘完全一致，可以对挂载到云服务器上的云硬盘做格式化、创建文件系统等操作，并对数据持久化存储。同时，云硬盘具有更高的数据可靠性，更高的 I/O 吞吐能力和更加简单易用等特点，适用于文件系统、数据库或者其他需要块存储设备的系统软件或应用。

对象存储服务

对象存储服务（Object Storage Service，OSS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。

OSS 系统和单个桶都没有总数据容量和对象/文件数量的限制，为用户提供了超大存储容量的能力，适合存放任意类型的文件，适合普通用户、网站、企业和开发者使用。OSS 是一项面向 Internet 访问的服务，提供了基于 HTTP/HTTPS 协议的 Web 服务接口，用户可以随时随地连接到 Internet 的电脑上，通过 OSS 管理控制台或各种 OSS 工具访问和管理存储在 OSS 中的数据。此外，OSS 支持 SDK 和 OSS API 接口，可使用户方便管理自己存储在 OSS 上的数据，以及开发多种类型的上层业务应用。

云备份

云服务器备份可为弹性云服务器创建备份（备份内容包括弹性云服务器的配置规格，系统盘和数据盘的数据），利用备份数据恢复弹性云服务器业务数据，最大限度保障用户数据的安全性和正确性，确保业务安全。

网络服务

虚拟私有云

虚拟私有云是通过逻辑方式进行网络隔离，提供安全、隔离的网络环境，提供与传统网络无差别的虚拟网络。

弹性公网 IP

弹性 IP 是可以独立申请和持有的公网 IP 地址资源，通过绑定弹性 IP 到云上的资源，云上的资源就可以与 Internet 上的资源进行通信。

弹性负载均衡

弹性负载均衡将访问流量自动分发到多台弹性云服务器，扩展应用系统对外的服务能力，实现更高水平的应用程序容错性能。

虚拟防火墙

提供 IaaS 层基础安全访问控制能力，能覆盖 Network ACL 的功能需求，为租户提供基于虚拟机端口和 Subnet 子网多层次、灵活的网络 ACL 功能。

安全组

安全组是一个网络安全服务，用户可以将一组具有相同安全组要求的云服务器划分到一个安全组中，提升云服务器的安全性。安全组是一个逻辑上的分组，为同一个项目内具有相同安全保护需求并相互信任的云服务器提供访问策略，支持白名单（指允许策略）。

云专线

云专线服务提供云上子网和云外子网直接路由互访，不需要做地址转换，网络带宽时延有保障，配置和维护简单。

NAT 网关

NAT 网关能够为虚拟私有云内的云主机，提供网络地址转换服务，使多个云主机可以共享弹性公网 IP 访问 Internet 或使云主机提供互联网服务。

共享带宽服务

共享带宽提供主账号下虚拟私有云内的带宽共享和复用能力，支持同一区域下多个弹性 IP 共同使用一条带宽，实现已绑定弹性公网 IP 的弹性云主机、裸金属、弹性负载均衡等实例共用带宽资源，帮助用户降低公网访问成本。

管理与部署服务

云监控服务

云监控服务为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。云监控提供实时监控告警、通知以及个性化报表视图，精准掌握业务资源状态。云监控的监控对象是基础设施、平台及应用服务的资源使用数据，不监控或触碰租户数据。

编排管理及自动化部署服务

编排管理服务提供面向应用的自动化交付能力，可实现应用所需的多个节点的基础设施（计算，网络和存储等）和基础软件（数据库、中间件等）环境的端到端一键自动化部署，最大限度地降低手工操作，减少跨部门的工单流转，标准化、规范化基础软硬件安装配置，从而提高整个 IT 的敏捷性。

自动化部署服务是部署工程师利用定制化的工具或脚本实现批量的安装服务器操作系统和软件，以达到快速、高效、方便的集成符合用户自身需求的一系列技术服务。

多租户管理服务

多租户管理服务支持对多租户环境下的用户安全隔离，云平台中每个租户对所申请的云防火墙、云负载均衡、云网络、云主机、云数据库具有编排、配置和管理的权限。云平台上的租户具有云资源的完全控制权，租户可以将云防火墙、云负载均衡、云网络、云主机进行自由地编排以搭建虚拟数据中心，虚拟数据中心所用虚拟资源完全是租户独享的，从而保证租户业务、数据的安全。

资源配额管理服务

配额管理服务对租户资源进行控制以及相关成本管理，通过配额的分配和管理，有效控制资源的使用率，避免资源浪费，同时也通过配额也可以深入挖掘用户实际需求以及实际使用情况。

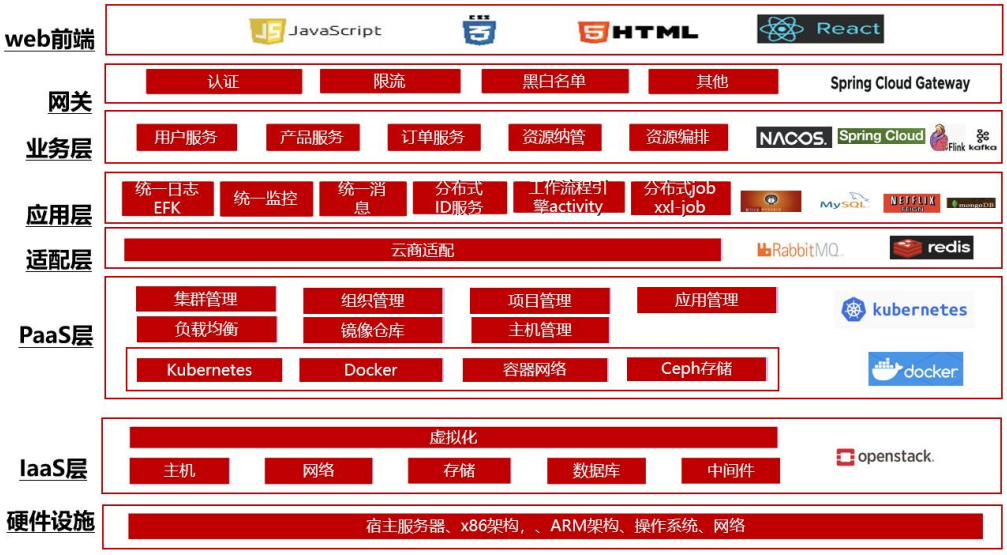
统一云管理平台设计

整体架构设计

统一云管理平台作为整个园区本地云平台的管理、调度和运维中心，对多朵云的计算、存储、网络、安全资源池进行统一管理和监控运维。

统一云管理平台架构应包含云治理、云资源、云服务、云成本、云运维、云适配等服务，助力组织企业上云和数字化转型。

统一云管理平台系统架构图



平台技术架构

平台技术架构分成 8 层，硬件设施、IaaS 层、PaaS 层、适配层、应用层、业务层、网关层、web 前端。

硬件设施层支持国产化服务器、操作系统、网络等基础设施。

IaaS 层由 openstack 技术提供虚拟化能力，提供虚机、网络、存储、数据库、中间件资源。

PaaS 层由 k8s,docker 技术提供集群管理、组织管理、项目管理、应用管理、负载均衡、镜像仓库等能力。

适配层由 RabbitMQ、redis 技术提供云商适配能力。

应用层由 mysql、netflix、mongodb 技术提供应用层的数据服务。

网关由 spring Cloud GateWay 提供认证、限流、黑白名单等功能。

Web 前端 由 javaScript 、html、CSS、React 负责前端页面开发。

功能设计

功能模块	功能说明
云治理	帮助管理员定义角色和权限层次结构，与企业和公有云目录和身份验证服务集成，搭建企业的组织机构管理体系，实现多级组织的精

	细化控制。支持设置配额限制和工作流，实现企业内部的流程管理体系。
云资源	作为核心模块之一，对多层资源进行整合，支持跨公有云和私有云平台管理各种计算、存储、网络以及 PaaS 资源，同时服务资源全生命周期。能够对企业 IT、IP 等基础硬件设施进行整合管理。
云服务	支持将资源以服务的方式，通过自定义流程控制提供给最终用户申请与使用。动态配置各类资源服务及应用，创建和管理多云应用和基础架构模板。提供各类统计分析，如资源统计、容量和利用率统计、告警统计等，帮助企业优化正在进行的统一云管理。
云成本	以数据可视化的方式，全面展现企业在公有云、私有云以及虚拟化环境等资源池中的各类资源用量及费用，各组织机构和项目的费用分摊，并通过横向和纵向的深入成本分析，帮助企业了解实际使用情况。基于资源负载分析，为用户提供成本优化建议，降低和优化云成本，实现降本增效。
云运维	提供全面覆盖的监控范围，对各系统告警进行统一标准化，多种告警提醒，高性能告警处理。提供指令/脚本批量执行、批量文件分发与采集等多种自动化运维方式，实现“主动监控、集中管理、统一运维”的目标。
云适配	混合多云整合能力，跨公有云、私有云、虚拟化和容器的云环境。支持联通云、阿里云、华为云、华三云、VMware 等多家云服务商，不同类型和版本的资源池。提供各级企业云资源环境账号信息配置接入，各环境资源信息同步及管理功能。

网络安全建设方案

网络安全基础设施建设方案

建设目标

通过安全保障体系建设，实现园区安全治理能力现代化和安全治理体系现代化，让园区安全决策科学化、安全治理现代化、安全服务集约化、应急处置协同化。实现园区已知威胁联动处置，未知威胁分析预判。通过数据融合创新，赋能网络安全治理数字化、园区安全管理精细化。

安全保障体系以园区数字基础设施、重要数字资产和信息系统为保护对象，以大数据和人工智能为核心技术，以网络安全态势感知、通报预警和协同联动为安全手段，以安全资源的集约化利用为重要原则，以生态化的服务为安全中心运行模式，利用“实时”、“全样”、“精准”的安全大数据建立全程在线、全域覆盖、实时反馈的“园区网络安全态势地图”，从而快速有效的感知、预警、调度、处置全区网络安全风险，提高管理决策的科学性和精准性，提升园区管理效率和应急响应能力，助力园区的数字化转型和数字经济发展。

构建数字资产安全监管图谱，快速形成园区信息资产底图，快速区分信息资产的类别，对发现的信息资产进行分类管理，并针对所有资产进行安全监测，针对外部威胁及资产自身存在的漏洞进行总体的风险监测，形成园区可视化安全风险热点分布。无缝对接安全大数据监测结果，实现园区安全协同指挥能力，提升突发安全事件的应对能力。

构建园区云端安全防御能力，对园区云平台及云上业务提供主动安全防御能力，构建集约化的安全防御体系，强化园区应急联动处置能力、重大活动安保能力和综合安全管理能力，为园区数字化发展提供强有力的安全保障。

助力园区传统产业转型升级、促进新旧动能转换是园区网络完全中心建设的初衷；通过以建促产、以产促城的创新驱动发展，提升本地数字经济指数，通过产业数字化、数字产业化发展，逐步形成园区数字化，逐步提升数字经济在经济总量中的占有率，助力产业转型。

设计原则

以习近平新时代中国特色社会主义思想特别是网络强国思想为指导，运用大数据解决安全问题，坚持底线思维，基于大数据、人工智能和云边融合的现代技术开展安全工作，助力园区治理能力的持续提升，助力营商环境的不断改善。安全体系设计遵循以下原则：

（1）联动协同，同步管理

项目建设坚持“保障业务、服务大局，筑牢底线、依法合规，体系防护、开放兼容，统一监管、全面审计”的理念，在部门的共同协作下，开展安全保障体系的建设。

（2）管理与技术并重

安全保障体系的安全建设不仅要重视安全技术体系的构建，更加要重视安全运营管理体系的构建。用先进的技术手段来保障安全能力，用先进的管理机制体制来保障安全效率。做到“安全能做到，安全能做好”。

（3）风险与事件共抓

安全保障体系既要重视监管监测体系的构建，也要重视保障体系的构建，实现防护与监管监测一体化，通过一体化的防护机制来保障系统防御外部攻击的能力，一旦发生安全事件，能够有效控制影响范围，避免发生次生损失。

（4）开放、迭代、创新

打破传统被动防御的观念，主动出击、持续改进、开放生态、创新技术，通过泛在感知、大数据分析、一体化运营服务等多种手段感知、发现、应对潜在和已经发生的威胁。在破坏发生之前，主动完成系统加固整改，避免产生实际损失；在问题发生之后，能够通过最新技术手段感知并自动化分析和处理，将问题产生的损失和持续时间降至最低，并追踪问题源头。

安全保障体系建设框架

安全保障体系框架包括网络安全基础设施、物联网安全、安全管理运营中心、安全管理体系和安全运营体系。以数据中心安全保障体系为支撑，整合智慧园区“技术、管理、运营”所需各类安全技术资源，为智慧园区提供基础能力支撑。在保障体系的建设上，根据园区的层次模型，对“园区感知、云基础设施、数据资源、数据资源开放平台以及应用”进行针对性的安全保障。具体设计内容包括：

网络边界安全防护：建设智慧园区云平台上联至政务云网络、互联网出口边界、园区之间、澄迈园区与海关专网之间、园区与 5G 边缘云之间的安全防护能力；通过在安全域边界部署安全网关设备进行隔离和访问控制，严格控制外部网络对业务系统信息资源的访问，以及内部终端访问外网合规管控；在政务云政务外网区与澄迈园区之间、澄迈园区与海关专网之间部署网闸系统进行物理隔离，确保数据交换安全合规，确保虚拟化数据中心和信息系统自身的安全。

安全管理中心：建立安全数据中心，全面收集信息系统内部和外部的安全要素，实现对安全要素的体系化、集中化管理。通过建立体系化的管理方式，利用资产探测实现对网络空间资产的识别发现与安全排查，方便运维人员对安全要素集中管理，并能够及时感知资产风险，提升智慧园区的网络安全自主可控能力。

针对 web 服务，自动化完成“目标侦查、暴露面检测、渗透利用”完整攻击链流程和事件调查的溯源取证，发现潜伏的高级持续性威胁，及时发现和应对网络安全风险。结合安全事件检测结果，梳理内网资产互访关系，基于攻击链阶段推导事件发展过程，分析历史数据实现逆向溯源。帮助安全分析人员梳理安全事件发生链路，并进一步研判安全威胁扩散情况，及时阻断威胁蔓延。对接联动安全防护设备，在安全事件发生时自动下发阻断策略，并在必要时下发通知预警，及时完成安全闭环。

物联网安全：建设物联网安全监测平台，实时或周期性对物联网进行安全摸底检查，利用网络资产快速摸底、设备弱口令及漏洞检测、网络边界检测以及异常行为检测等技术，及时发现目标中存在的各类安全隐患，比如系统漏洞、弱口令、敏感服务端口等，呈现物联网整体的安全现状，从而指导排查并督促整改。

安全运营体系：建设智慧园区安全运营体系，在流程机制方面自上而下进行合理的责任划分，用数据分析问题、预判问题、验证问题、协调资源解决问题，并持续迭代优化。利用安全运营中心为安全运营工作提供技术支撑，提供态势感知、通报预警、应急处置等运营手段。安全运营团队可以利用安全运营中心相关技术及数据，对智慧园区的安全问题进行统一分析，及时将预警信息同步给支撑单位，做好提前防范，加强整改，预防更多安全事件发生，以此促进安全事件应急响应时效性，提升安全事件处置水平。对发现安全问题的场景及系统进行处置结果的跟踪，掌握其整改结果是否达标，是否引入新的安全问题，从而形成事前预警通报，事中防护应急，事后监督整改的应用安全运营保障闭环。

标准规范：重点实现对数据资源采集、汇聚、共享、开放和应用的管理和标准化建设，让数据共享、应用、公开、保密等工作有据可依、有规可循，明确数据提供方、数据使用方、数据管理方、平台运营方、服务提供方的安全职责和义

务。

安全组织与人员：明确各组织机构的职责与分工，落实安全责任制。建立融合的联动工作机制，建立智慧园区安全监测预警、信息通报和应急处置机制，制定全市安全应急预案，加强日常监测预警和联合应急演练，确保安全管理工作协同共治。

总体安全网络拓扑设计

网络结构的安全是网络安全的前提和基础，选用主要网络设备时需要考虑业务处理能力的高峰数据流量，要考虑冗余空间满足业务高峰期需要；网络各个部分的带宽要保证接入网络和核心网络满足业务高峰期需要；按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要主机；合理规划路由，业务终端与业务服务器之间建立安全路径；绘制与当前运行情况相符的网络拓扑结构图；根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

根据海口市综合保税区整体信息系统实际情况，整体网络架构划分为互联网出口区、5G专网区、核心交换区、电子政务网络区（含政务云政务外网区和互联网区）、数据中心区（云平台和物理集群区）、办公接入区、物联网区、外联区（海口园区、空港园区、海关接入区）和安全管理区。

安全技术体系设计

安全物理环境设计

安全物理环境主要涉及的方面包括环境安全（防火、防水、防雷击等）设备

和介质的防盗窃防破坏等方面。具体包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等十个控制点。

1） 机房选址

机房和办公场地选择在具有防震、防风和防雨等能力的建筑内。机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

2） 机房访问控制

机房出入口安排专人值守，控制、鉴别和记录进入的人员；需进入机房的来访人员须经过申请和审批流程，并限制和监控其活动范围。对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；

3） 设备与介质管理

为了防止无关人员和不法分子非法接近网络并使用网络中的主机盗取信息、破坏网络和主机系统、破坏网络中的数据的完整性和可用性，必须采用有效的区域监控、防盗报警系统，阻止非法用户的各种临近攻击。

4） 防雷接地

为了保证海口综合保税区机房的各种设备安全，要求机房设有四种接地形式，即计算机专用直流逻辑地、配电系统交流工作地、安全保护地、防雷保护地。

5） 温湿控制

为了保证海口综合保税区网络的各种设备安全，要求机房配备温湿控制系统来对机房内温湿度进行控制，保障设备安全。

6） 消防报警及自动灭火

为实现火灾自动灭火功能，在海口综合保税区网络机房的各个地方，还应该

设计火灾自动监测及报警系统，以便能自动监测火灾的发生，并且启动自动灭火系统和报警系统。

7） 门禁

海口综合保税区网络机房应建立实用、高效的门禁系统，门禁系统需要注意的原则是安全可靠、简单易用、分级制度、中央控制和多种识别方式的结合。

8） 监控

海口综合保税区的监控包括几个系统的监控：闭路监视系统、通道报警系统和人工监控系统。

9） 供配电系统

海口综合保税区的供配电系统要求能保证对机房内的主机、服务器、网络设备、通讯设备等的电源供应在任何情况下都不会间断，做到无单点失效和平稳可靠，这就要求两路以上的市电供应，N+1 冗余的自备发电机系统，还有能保证足够时间供电的 UPS 系统。

10）电磁防护

铺设线缆要求电源线和通信线缆隔离铺设，避免互相干扰。对关键设备和磁介质实施电磁屏蔽。

安全通信网络设计

网络结构安全

根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

根据海口市综合保税区整体信息系统实际情况，整体网络架构安全域划分为

互联网出口区、5G 专网区、核心交换区、电子政务网络区（含政务云政务外网区和互联网区）、数据中心区（云平台和物理集群区）、办公接入区、物联网区、外联区（海口园区、空港园区、海关接入）和安全管理区。

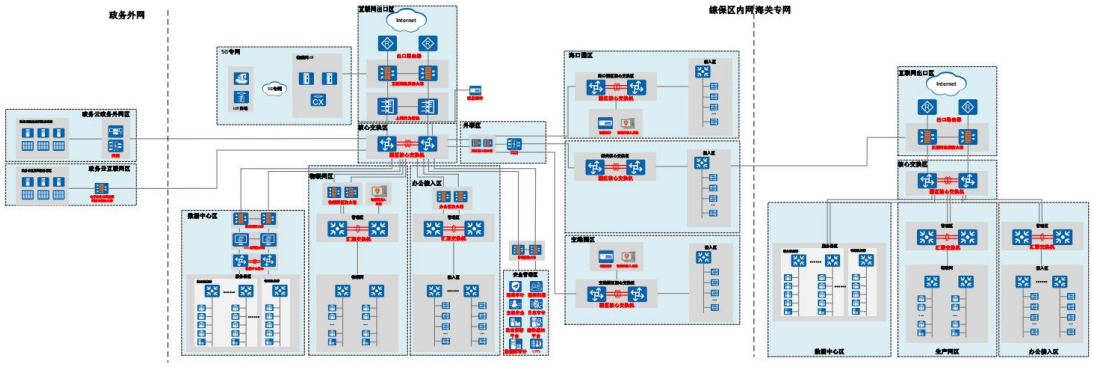


图5-67 本项目网络安全组网拓扑图

政务云电子政务网互联区边界防护新增安全技术措施如下：

在政务云电子政务网互联区部署一台专线防火墙，通过防火墙安全域划分提供基础安全隔离，把安全信任网络和非安全网络进行隔离；并提供从数据链路层、网络层到传输层的安全，包括 ARP 欺骗、扫描攻击、多种畸形报文攻击、端口过滤、抗 IP 分片攻击和防病毒等基础防御，同时应用 NAT 隐藏数据中心网络拓扑结构。

在政务云电子政务网政务外网区部署一台网闸，通过网闸将政务外网区与澄迈园区做物理隔离，确保数据交换安全合规。

外联区、安全管理区、物联网区、办公接入区边界防护新增安全技术措施如下：

在外联区部署两台园区接入防火墙，将澄迈园区与海口园区、空港园区、海关园区做逻辑隔离，通过策略放通相关的合规流量；在物联网区、办公接入区各部署两台防火墙，将物联网区与核心交换区、办公接入区与核心交换区做逻辑隔

离，通过策略放通相关的合规流量；在安全管理区与核心交换区之间部署两台防火墙，通过策略放通相关的合规流量。以上安全区域边界通过防火墙安全域划分提供基础安全隔离，把安全信任网络和非安全网络进行隔离；并提供从数据链路层、网络层到传输层的安全，包括 ARP 欺骗、扫描攻击、多种畸形报文攻击、端口过滤、抗 IP 分片攻击和防病毒等基础防御，同时应用 NAT 隐藏数据中心网络拓扑结构。

在外联区部署一台网闸，通过网闸将澄迈园区与海关接入区做物理隔离，确保数据交换安全合规。

数据中心区边界防护新增安全技术措施如下：

在数据中心区边界部署两台防火墙，将数据中心区与核心交换区做逻辑隔离，通过策略放通相关的合规流量。

在数据中心区边界部署两台web应用防火墙，可以有效地缓解网站及Web应用系统面临如OWASP TOP 10中定义的常见威胁；可以快速地应对恶意攻击者对Web业务带来的冲击，让网站免遭Web攻击侵扰并对网站代码进行合理加固。

互联网出口区边界防护新增安全技术措施如下：

在互联网出口区部署两台防火墙和两台上网行为管理，将互联网与澄迈园区做逻辑隔离，通过策略放通相关的合规流量，对内网业务系统形成有效的安全防护，以满足外网对业务系统的访问；上网行为管理主要是针对内网终端对外访问的行为有效的控制，将不合规连接外网的异常行为进行阻断，以提升内网终端设备的安全性。

物联网区、海口园区接入区、空港园区接入区网络安全新增安全技术措施如

下：

在老城园区核心交换机、海口园区核心交换机、空港园区核心交换机处各部署一台流量探针和一台物联网终端准入设备，通过流量探针检测、筛查出网络流量当中是否存在威胁攻击的行为，将检测数据推送到态势感知平台做综合的分析研判，从而发现内网整体的攻击态势；终端准入设备则是通过IP、MAC绑定、打标签等方式判断前端接入节点是否能安全合规的接入到内网当中，从而规避一些非法终端接入内网，对内网造成网络威胁。

安全管理区新增安全技术措施如下：

在安全管理区部署一套态势感知平台结合智能检测算法可进行多维度海量数据关联分析，主动实时的发现各类安全威胁事件，还原出整个 APT 攻击链攻击行为。同时可采集和存储多类网络信息数据，帮助用户在发现威胁后调查取证以及处置问责。以发现威胁、阻断威胁、取证、溯源、响应、处置，完成全流程威胁事件闭环。

部署一套运维审计系统，通过集中管理、监控与审计所有运维人员的操作行为，有效降低网络设备、服务器、数据库、业务系统等资源的内部运维风险，完善 IT 管理体系，同时满足相关法规、标准要求。

部署一套漏洞扫描系统，智能主机服务发现，智能化爬虫和 SQL 注入状态检测等技术，并以智能便利规则库为基础，深度主机服务探测、Web 智能化爬虫、SQL 注入状态检测、主机配置检查以及弱口令检查等方式相结合的技术，实现 Web 漏洞扫描、系统漏洞扫描、数据库漏洞扫描、基线安全检查与口令猜解五大扫描能力，深度掌握漏洞风险评估。

部署一套攻击预警平台，汇集流量传感器、文件威胁鉴定器、邮件告警、等多种告警数据，基于多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁情报；同时结合部署在客户本地的软、硬件设备，能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源；

部署一套主机安全系统，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，通过防病毒、漏洞管理、运维管控、基线合规检查、网络准入、终端检测与响应（EDR）、终端数据防泄漏（EDLP）等安全功能，为业务终端提供体系化安全防护能力。

部署一套日志审计系统，作为一个统一日志收集与分析平台，能够实时不间断地将企业和组织中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合安全审计。系统能够实时地对采集到的不同类型的日志和事件信息进行标准化（归一化）和实时关联分析，通过统一的仪表板进行实时动态、可视化的呈现，协助安全管理人员迅速准确地识别安全事故，消除了管理员在多个控制台之间来回切换的烦恼，同时提高工作效率，降低工作强度。

部署一套 VPN 系统，可以保障企业移动信息化安全，在满足客户的身份认证、传输加密、访问授权、日志审计等多种基础安全需求基础上，更加保护了移动终端设备的接入安全、移动应用自身安全、移动应用数据安全。

部署一套数据库审计系统，对审计和事务日志进行审查，从而跟踪各种对数据库操作的行为，主要记录对数据库的操作、对数据库的改变、执行该项操作的人以及其他的属性。这些数据被记录到数据库审计与防护系统独立的平台中，并

且具备较高的准确性和完整性。针对数据库活动或状态进行取证检查时，审计可以准确的反馈数据库的各种操作历史，对分析数据库的各类正常、异常、违规操作提供证据。

安全防护措施合规说明

根据安全通信网络等级保护的基本要求，结合本次项目采取的安全防护措施如下：

网络安全等级保护基本要求通用要求—安全通信网络		
控制点	安全通用要求	安全防护措施
网络架构	a）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；	根据网络区域承担功能和部署设备的不同，划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址。
	b)应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；	在边界新增部署防火墙，重要网络区域与其他网络区域之间采取防火墙进行网络隔离。

安全区域边界设计

安全区域边界是对内部应用系统计算环境进行安全防护和防止敏感信息泄露的必经渠道。通过区域边界的安全控制，可以对进入和流出应用环境的信息流进行安全检查，既可以保证应用系统中的敏感信息不会泄漏出去，同时也可以防止应用系统遭受外界的恶意攻击和破坏。区域边界的安全主要包括：边界防护、访问控制、入侵防范、恶意代码防范、边界安全审计等方面。

在网络层进行访问控制需部署防火墙产品，可以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。

各安全区域边界已经部署了相应的安全设备负责保障区域边界的安全。对于流经各主要边界（服务器区域、外部连接边界）需要设置必要的审计机制，进行数据监视并记录各类操作，通过审计分析能够发现跨区域的安全威胁，实时地综合分析出网络中发生的安全事件。根据审计策略进行数据的日志记录与审计。同时审计信息要通过安全管理中心进行统一集中管理，为安全管理中心提供必要的边界安全审计数据，利于管理中心进行全局管控。边界安全审计和日志审计等一起构成完整的、多层次的审计系统。

边界防护

根据GB/T 22239-2019 网络安全等级保护基本要求中对边界防护的要求：应能够对非授权设备私自联到内部网络的行为进行检查和控制。

本项目在在老城园区物联网汇聚交换机、海口园区核心交换机、空港园区核心交换机处各部署一台物联网终端准入设备，对视频终端和网络终端私自联到内部网络的行为进行检查和控制。主要实现功能如下：

准入技术：支持旁路镜像准入技术；支持设备识别自动过滤阻断技术，通过数据智能分析，能够自动判定设备的合法性并进行放行或阻断操作；

准入管理：支持与管理平台心跳连接，管理平台可以配置准入设备的准入网段、准入防护开启、准入黑白名单；IP过滤规则：

边界管理：提供自定义设置网络边界，准入控制IP网段地址、部署模式及被阻断的计算机重定向引导页面；

设备发现与识别：内置设备类型特征库，支持常见设备的识别，如：IPC摄像机、NVR录像机、PC终端、网络交换、服务器设备等，不断完善的特征库，可满足非正常设备的识别需求；提供IPC摄像机、NVR录像机、PC终端、网络交换、服务器设备的识别，后续可根据需求满足非正常设备的识别；

访问控制

通过对边界访问控制需求分析，在网络层进行访问控制需部署防火墙产品，可以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。为网络创造全面纵深的安全防御体系。

防火墙：在各安全域边界部署防火墙产品，并配置入侵防御模块、防病毒模块，部署效果如下：

1） 访问控制策略：防火墙工作在不同安全区域之间，对各个安全区域之间流转的数据进行深度分析，依据数据包的源地址、目的地址、通信协议、端口，进行判断，确定是否存在非法或违规的操作，并进行阻断，从而有效保障了各个重要的计算环境。

2） 会话监控策略：在防火墙配置会话监控策略，当会话处于非活跃一定时间或会话结束后，防火墙自动将会话丢弃，访问来源必须重新建立会话才能继续访问资源。

3） 网络防攻击控制策略：防止 ARP 欺骗等。

本项目规划在互联网出口区、电子政务外网互联网区、核心业务服务器区、外部接入区（海口园区接入、空港园区接入、海关接入）、终端接入办公区、物联网区和安全管理区边界，各部署下一代防火墙（NGFW），通过在重要的安全域边界应采用边界访问控制技术保证安全区域之间进出的数据进行访问控制，防止

未授权访问发生。

在数据中心服务器区边界部署两台web应用防火墙，可以有效地缓解网站及Web应用系统面临如OWASP TOP 10中定义的常见威胁；可以快速地应对恶意攻击者对Web业务带来的冲击，让网站免遭Web攻击侵扰并对网站代码进行合理加固。

在电子政务网政务外网区部署一台网闸，通过网闸将政务外网区与澄迈园区做物理隔离，确保数据交换安全合规。在外联区部署一台网闸，通过网闸将澄迈园区与海关接入区做物理隔离，确保数据交换安全合规。

入侵防范

本项目在各安全域边界部署防火墙产品，防火墙开通入侵防御功能模块，部署效果如下：

1） 防范网络攻击事件：入侵防护系统采用细粒度检测技术，协议分析技术，误用检测技术，协议异常检测，可有效防止各种攻击和欺骗。针对端口扫描类、木马后门、缓冲区溢出、IP 碎片攻击等，入侵防护系统可在网络边界处进行监控和阻断。

2） 防范拒绝服务攻击：入侵防护系统在防火墙进行边界防范的基础上，工作在网络的关键环节，能够应付各种 SNA 类型和应用层的强力攻击行为,包括消耗目的端的各种资源如网络带宽、系统性能等攻击，主要防范的攻击类型有 TCP Flood，UDP Flood，SYN Flood，Ping Abuse 等。

3） 审计、查询策略：入侵防护系统能够完整记录多种应用协议（HTTP、FTP、SMTP、POP3、TELNET 等）的内容。记录内容包括，攻击源 IP、攻击类型、攻击目标、攻击时间等信息，并按照相应的协议格式进行回放，清楚再现入侵者的攻击过程，重现内部网络资源滥用时泄漏的保密信息内容。同时必须对重要安

全事件提供多种报警机制。

4） 网络检测策略：在检测过程中入侵防护系统综合运用多种检测手段，在检测的各个部分使用合适的检测方式，采取基于特征和基于行为的检测，对数据包的特征进行分析，有效发现网络中异常的访问行为和数据包。

5） 异常报警策略：入侵防护系统通过报警类型的制定，明确哪类事件，通过什么样的方式，进行报警，可以选择的包括声音、电子邮件、消息。

6） 阻断策略：由于入侵防护系统串联在保护区域的边界上，系统在检测到攻击行为后，能够主动进行阻断，将攻击来源阻断在安全区域之外，有效保障各类业务应用的正常开展，这里包括数据采集业务和信息发布业务。

此外，在安全管理中心区部署攻击预警平台，基于关键区域入口的旁路镜像流量分析，可以实现 WEB、邮件、文件三个维度多个层次的 APT 攻击检测，主要包含：WEB 层面的 APT 攻击检测（包含各种已知 WEB 攻击特征检测、WEBSHELL 检测、WEB 行为分析、异常访问、C&C IP/URL 检测等），邮件层面的 APT 攻击检测。

恶意代码

本项目在各安全域边界部署防火墙产品，防火墙开通入侵防御功能模块，处进行集中防护，对夹杂在网络交换数据中的各类网络病毒进行过滤，可以对网络病毒、蠕虫、混合攻击、端口扫描、间谍软件、P2P 软件带宽滥用等各种广义病毒进行全面的拦截。阻止病毒通过网络的快速扩散，将经网络传播的病毒阻挡在外，可以有效防止病毒从其他区域传播到内部其他安全域中。功能策略如下：

1） 病毒过滤策略：对 SMTP、POP3、IMAP、HTTP 和 FTP 等应用协议进行病毒扫描和过滤，通过恶意代码特征过滤，对病毒、木马、蠕虫以及移动代码进行过滤、清除和隔离，有效地防止可能的病毒威胁，将病毒阻断在敏感数据处理区域之外。

2） 恶意代码防护策略：支持对数据内容进行检查，可以采用关键字过滤，URL 过滤等方式来阻止非法数据进入敏感数据处理区域，同时支持对 Java 等小程序进行过滤等，防止可能的恶意代码进入敏感数据处理区；此外，也支持对移动代码如 Vbscript、JAVA script、ActiveX、移动终端 let 的过滤，能够防范利用上述代码编写的恶意脚本。

3） 蠕虫防范策略：可以实时检测到日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止信息网络因遭受蠕虫攻击而陷于瘫痪。

安全审计

根据 GB/T 22239-2019 网络安全等级保护基本要求中安全区域边界中安全审计的要求：应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

本项目通过在澄迈园区核心交换机、海口园区汇聚交换机、空港园区汇聚交换机旁路部署流量分析探针，具备流量威胁深度检测能力，支持异常会话检测、WEB 攻击检测、挖矿行为检测、僵木蠕检测、Webshell 文件检测、异常文件检测、漏洞利用检测等；具备流量协议内容深度还原，包括 http、dns、smb、ftp、smtp 等协议；具备网络入侵攻击报文检测引擎，触发告警，记录入侵攻击事件，记录：事件名称、来源 IP、来源端口、目的 IP、目的端口等。

通过在互联网边界防火墙处部署上网行为管理功能，实现对访问互联网的用户行为等单独进行行为审计和数据分析。

通过在安全管理区部署 SSL VPN 网关配合运维审计系统，确保登录系统重要设备的身份鉴别和访问控制，对远程访问的用户行为进行行为审计和数据分析。

安全防护措施合规说明

根据安全区域边界等级保护的基本要求，结合本次项目采取的安全防护措施如下：

信息安全技术网络安全等级保护基本要求—安全区域边界		
控制点	安全通用要求	安全防护措施
边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；	在边界新增部署防火墙。通过防火墙可保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信。
访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；	边界新增部署防火墙。通过防火墙，可在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
	b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；	在边界新增部署防火墙。 通过防火墙，可删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。
	c）应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据	在边界新增部署防火墙。 通过防火墙可对源地址、目的地址、源端口、目的端口和协议等

信息安全技术网络安全等级保护基本要求—安全区域边界		
控制点	安全通用要求	安全防护措施
	包进出；	进行检查，以允许/拒绝数据包进出。
	d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；	在边界新增部署防火墙。 通过防火墙可根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力。
入侵防范	a）应在关键网络节点处监视网络攻击行为；	在边界新增部署防火墙（内置入侵防御模块）。通过防火墙（内置入侵防御模块），可在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。	在边界新增部署防火墙（内置防病毒模块）。通过防火墙（内置防病毒模块），可在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

安全计算环境设计

身份鉴别

身份鉴别可分为主机身份鉴别和应用身份鉴别两个方面：

主机身份鉴别：

为提高主机系统安全性，保障各种应用的正常运行，对主机系统需要进行一系列的加固措施，包括：

- 对登录操作系统和数据库系统的用户进行身份标识和鉴别，且保证用户名的唯一性。
- 根据基本要求配置用户名/口令；口令必须具备采用 3 种以上字符、长度不少于 8 位并定期更换；
- 启用登陆失败处理功能，登陆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。
- 远程管理时应启用 SSH 等管理方式，加密管理数据，防止被网络窃听。
- 对主机管理员登录进行双因素认证方式进行身份鉴别。

应用身份鉴别：

为提高应用系统系统安全性应用系统需要进行一系列的加固措施，包括：对登录用户进行身份标识和鉴别，且保证用户名的唯一性。

根据基本要求配置用户名/口令，必须具备一定的复杂度；口令必须具备采用 3 种以上字符、长度不少于 8 位并定期更换；

启用登陆失败处理功能，登陆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。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

本项目通过在安全管理区部署 SSL VPN 网关配合运维审计系统，确保登录系统重要设备的身份鉴别和访问控制，通过集中管理、监控与审计所有运维人员的操作行为，有效降低网络设备、服务器、数据库、业务系统等资源的内部运维风险，完善 IT 管理体系，同时满足相关法规、标准要求。

访问控制

自主访问控制实现：在安全策略控制范围内，使用户对自己创建的客体具有各种访问操作权限，并能将这些权限的部分或全部授予其他用户；自主访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；强制访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级。

由此主要控制的是对应用系统的文件、数据库等资源的访问，避免越权非法使用。采用的措施主要包括：

启用访问控制功能：制定严格的访问控制安全策略，根据策略控制用户对应用系统的访问，特别是文件操作、数据库访问等，控制粒度主体为用户级、客体为文件或数据库表级。

权限控制：对于制定的访问控制规则要能清楚的覆盖资源访问相关的主体、客体及它们之间的操作。对于不同的用户授权原则是进行能够完成工作的最小化授权，避免授权范围过大，并在它们之间形成相互制约的关系。

账号管理：严格限制默认账户的访问权限，重命名默认账户，修改默认口令；及时删除多余的、过期的账户，避免共享账户的存在。

访问控制的实现主要采取两种方式：采用安全操作系统，或对操作系统进行安全增强改造，且使用效果要达到以上要求。

本项目通过在安全管理中心部署运维审计系统（堡垒机），通过运维审计可对登录的用户分配账户和权限。可授予管理用户所需的最小权限，实现管理用户

的权限分离。

入侵防范

针对主机和网络的入侵防范，可以从多个角度进行处理：

本项目在安全管理区新增部署一台漏洞扫描系统；可定期对海口综合保税区网络的网络、服务器、重要终端中存在的已知安全漏洞进行扫描和评估，并及时封堵漏洞，做到防患于未然。功能策略如下：

1）资源管理：对主机信息、网站信息进行增、删、改操作，同时可对属性进行维护，包括责任人、责任部门、漏洞状态等。在资源管理模块中实现漏洞整改单下发、一键扫描、脆弱性账号展示等功能。资源管理包括资产管理和网站管理、属性管理。

2）漏洞扫描：包括扫描器管理、扫描任务管理、漏洞整改管理、漏洞整改单。

恶意代码防范

各类恶意代码尤其是病毒、木马等是对网络的重大危害，病毒在爆发时将使路由器、3 层交换机、防火墙等网关设备性能急速下降，并且占用整个网络带宽。

针对病毒的风险，建议是将病毒消灭或封堵在终端这个源头上。本项目通过在安全管理区部署一套主机安全系统，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，通过防病毒、漏洞管理、运维管控、基线合规检查、网络准入、终端检测与响应（EDR）、终端数据防泄漏（EDLP）等安全功能，为业务终端提供体系化安全防护能力。

功能及策略

主机杀毒客户端采用轻量级客户端安装，同时支持虚拟主机以及终端部署，

部署防病毒系统后，可以给最终用户带来的安全防护效果如下：

支持对终端设备/虚拟主机内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力。并具备空闲查杀、断点查杀、后台查杀等功能支持扫描和清除各种广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等等。能够实时监控和清除来自各种途径的病毒、木马、恶意程序。

支持病毒自动隔离功能，对于暂时无法清除的被感染文件或者可疑文件，防病毒软件的客户端能自动将其隔离到本地隔离区。

支持未知病毒、恶意代码的防范能力，支持基于行为的检测和防护技术：智能识别蠕虫木马，无需提示用户操作判断。支持注册表病毒、内存或服务类病毒的查杀，提高终端安全防护等级，对已经运行的病毒进程可以执行关闭。

支持多防护资产类型，包括：客户端 agent 支持虚拟主机、终端 PC、物理服务器等多种资产；管理端支持传统服务器以及虚拟部署模式。

安全防护措施合规说明

根据安全计算环境等级保护的基本要求，结合本次项目采取的安全防护措施如下：

信息安全技术网络安全等级保护基本要求—安全计算环境		
控制点	安全通用要求	安全防护措施
身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；	新增部署运维审计系统（堡垒机），通过运维审计可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。

信息安全技术网络安全等级保护基本要求—安全计算环境		
控制点	安全通用要求	安全防护措施
	b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；	新增部署运维审计系统（堡垒机），运维审计具有登录失败处理功能，并配置启用结束会话、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
	c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	新增部署 VPN 系统，当进行远程管理时，通过 VPN 系统可防止鉴别信息在网络传输过程中被窃听。
访问控制	a）应对登录的用户分配账户和权限；	新增部署运维审计系统（堡垒机），通过运维审计可对登录的用户分配账户和权限。
	b）应重命名或删除默认账户，修改默认账户的默认口令；	新增部署运维审计系统（堡垒机），通过运维审计可重命名或删除默认账户，修改默认账户的默认口令。
	c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；	新增部署运维审计系统（堡垒机），通过运维审计可及时删除或停用多余的、过期的账户，避免共享账户的存在。
	d）应授予管理用户所需的最小权限，实现管理用户的权限分离；	新增部署运维审计系统（堡垒机），通过运维审计可授予管理用户所需的最小权限，实现管理用户的权限

信息安全技术网络安全等级保护基本要求—安全计算环境		
控制点	安全通用要求	安全防护措施
		分离。
入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；	通过部署漏洞扫描系统，管理端和客户端遵循最小安装的原则，仅安装需要的组件和应用程序。
	b）应关闭不需要的系统服务、默认共享和高危端口；	关闭不需要的系统服务、默认共享和高危端口。
	c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；	通过 VPN、堡垒机接入终端或通过限制只有堡垒机的 IP 能对终端进行远程运维。
	e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；	通过部署漏洞扫描系统，可以发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。
恶意代码防范	应采用免受恶意代码攻击的技术措施或配置具有相应功能的软件，并定期升级和更新恶意代码库。	部署主机安全管理系统，通过终端杀毒可及时识别服务器、PC 终端、虚拟机的入侵和病毒行为，并将其有效阻断。
数据备份恢复	a)应提供重要数据的本地数据备份与恢复功能；	具有本地数据备份与恢复功能。

安全管理中心设计

安全管理中心主要涉及系统管理、审计管理等方面的建设。

系统管理

通过在安全管理区新增部署运维审计系统（堡垒机），通过堡垒机授权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。功能策略如下：

1）单点登录：堡垒主机提供了基于 B/S 的单点登录系统，用户通过一次登录系统后，就可以无需认证的访问包括被授权的多种基于 B/S的应用系统。

2）账户管理：集中帐号管理包含对所有服务器、网络设备帐号的集中管理，是集中授权、认证和审计的基础。集中帐号管理可以实现将帐号与具体的自然人相关联，从而实现针对自然人的行为审计。

3）身份认证：堡垒主机为用户提供统一的认证界面。采用统一的认证接口不但便于对用户认证的管理，而且能够采用更加安全的认证模式，包括静态密码、双因素、一次性口令和生物特征等多种认证方式，而且可以方便地与第三方认证服务对接，提高认证的安全性和可靠性，同时又避免了直接在业务服务器上安装认证代理软件所带来的额外开销。集中身份认证建议采用基于静态密码+数字证书的双因素认证方式。

4）访问控制：堡垒主机系统能够提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，可以是一组可执行命令，也可

以是一组非可执行的命令，该命令集合用来分配给具体的用户，来限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。

5） 操作审计：主要审计操作人员的帐号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的帐号、资源进行标识后，操作审计能更好地对帐号的完整使用过程进行追踪。为了对字符终端、图形终端操作行为进行审计和监控，内控堡垒主机对各种字符终端和图形终端使用的协议进行代理，实现多平台的操作支持和审计，例如Telnet、SSH、FTP、Windows平台的RDP远程桌面协议，Linux/Unix平台的X Window图形终端访问协议等。

审计管理

通过日志审计和数据库审计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。

日志审计：现网已部署日志审计系统，已部署日志审计系统 CPU 使用率大于 80%，需新增一台日志审计。实现信息资产（网络设备、安全设备、主机、应用及数据库）的日志收集与处理，通过预置的解析规则实现日志的解析、过滤及聚合，构建全面的风险管理和内控体系提供必要的支撑。功能策略如下：

1．日志收集：收集用户内、外网的网络设备、安全设备、服务器、数据库以及各类应用系统，进行统一集中存储和汇总，并提供给系统管理人员进行进一步的分析和查询。

2．日志查询：支持对海量日志信息进行组合条件检索查询，查询结果根据归一化后的格式展现给管理者，便于管理者事后追溯。支持多条件日志检索查询；支持原始日志全文检索。查询结果支持 word、pdf 等多种格式导出；支持将备份日志数据进行还原检索查询；支持查询结果二次查询。

数据库审计：实现对关系型数据库和分布式数据库的访问和操作行为进行审计，记录相关日志。并且对数据库攻击行为进行检测与告警。对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握数据库系统的整体安全。数据审计功能策略如下：

1)数据审计工作主要是审查数据库的安全策略、安全保护措施及故障恢复计划等对系统的各种操作，如访问、查询、修改等，尤其是对一些敏感操作进行记录、对用户的行为进行有效的监控和记录，及时发现威胁数据库的操作企图，采取相应措施，保证数据库的安全。

2)支持数据库部署 agent 以及旁路镜像方式获取流量的方式。

3)支持主流数据库审计，包括：Oracle， SQLServer，DB2，Infomix，Sybase、Cache、Mysql，PostgreSQL、人大金仓、达梦、南大通用、MongoDB、TeraDATA、神通 OSCAR 等。

4)SQL 操作审计：支持对 SQL 语句的解析、SQL 语句的操作类型、操作字段和操作表名等的分析。

5)业务关联分析：通过对浏览器与 Web 服务器、Web 服务器与数据库服务器之间所产生的 HTTP 事件、SQL 事件进行业务关联分析，管理者可以快速、方便的查询到某个数据库访问是由哪个 HTTP 访问触发，定位追查到真正的访问者，从而将访问 Web 的资源账号和相关的数据库操作关联起来。包括访问者用户名、源 IP 地址、SQL 语句、业务用户 IP、业务用户主机等信息。

攻击预警平台

攻击预警平台汇集流量传感器、文件威胁鉴定器、邮件告警等多种告警数据，基于自有的多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁情报；同时结合部署在客户本地的软、硬件设备，能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源；支持运用 SOAR 编排技术，实现对确定的威胁进行多种类型的响应处置，真正实现监测预警、威胁检测、溯源分析和响应处置的威胁监测与分析系统。

安全态势感知管理中心建设

态势感知平台建设

（一）产品设计背景

从国家的整体安全战略出发，中共中央总书记、国家主席、中央军委主席、中央网络安全和信息化领导小组组长习近平在北京主持召开网络安全和信息化工作座谈会并发表重要讲话指出“网络安全和信息化是相辅相成的，安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”

同时在最新颁布的《网络安全法》中指出“负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息”，“建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件”。政府单

位作为国家重要的关键信息基础设施部门，建立整体的网络安全态势感知势在必行。

（二）技术框架

态势感知平台是本期项目安全防护体系核心，系统按照一体化、标准化、智能化、可视化要求进行建设。可实现对网络安全的态势觉察、跟踪、预测和预警，全面、实时掌握网络安全态势，及时掌握网络安全威胁、风险和隐患，及时监测漏洞、病毒木马、网络攻击情况，及时发现网络安全事件线索，及时预警通报重大网络安全威胁，及时处置安全事件，有效防范和打击网络攻击等违法犯罪活动，达到实时态势感知、准确安全监测、及时应急处置等目标，提升安全风险发现能力，加快风险解决速度。

设计包含四个层次，分别为采集探针层、存储计算层、业务处置层、业务展示层。具体如下：

1）数据收集层：负责包括安全检测/安全监测探针、安全防护系统、安全审计系统、日志探针等设备的各类数据的统一收集；

2）存储计算层：负责数据汇入、转换、存储、基础分析功能，数据转换支持的数据类型包括结构化、半结构化、非结构化的数据转换，提供的转换方式包括去隐私、归一化、过滤、归并、打标签等；存储计算引擎提供的存储功能包括分布式文件存储、数据仓库、分布式检索、分布式计算框架、关系数据等，实现对事实数据、结果数据、知识数据的存储；

3）分析处置层：包含态势分析、安全监测、安全处置、安全对象管理、深度分析等子系统，负责通过攻击检测、情报关联、态势统计、画像分析等模型并匹配输入输出、记录处置、集合处置、聚类处置、分类处置等算子库实现数据深度挖掘分析。提供基于资产、日志、情报的信息检索机制；提供基于任务、操作

的探索分析功能。提供基于安全事件的发布通报、处置管理、工作分析、事件确认等通报处置功能。另外提供威胁情报管理功能；

4）业务展示层：面向主管领导、安全管理员、安全运维人员、安全审计人员提供安全业务功能展现，包括全网综合态势、资产态势、漏洞态势、全网病毒态势等功能上层展示模块。

（三）系统部署说明

本项目在在安全管理区部署态势感知系统，可实现对安全态势觉察、跟踪、预测和预警，全面实时掌握网络安全态势，及时掌握网络安全威胁、风险和隐患，及时监测漏洞、病毒木马、网络攻击等情况。

（四）管理对象范围说明

态势感知系统是一套定位于面向安全相关人员、设备、安全事件等多方面因素的综合性安全运管平台，面向的安全对象如下：

1）平台使用方：用户领导层、安全管理人员、安全运维人员、安全审计人员等；

2）设备：含安全设备、网络设备、服务器设备、边界设备等。

- 安全设备：包括但不限于防火墙、流量检测探针、终端杀毒系统、日志审计、网络安全审计、数据库审计、运维审计等；
- 网络设备：包括但不限于交换机、路由器等；
- 服务器设备：包括但不限于数据挖掘服务器、存储服务器等；
- 边界设备：包括但不限于网闸等。

3）安全事件：含特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件四个等级。

（五）平台功能实现

1、 大数据分析展示

1）全网综合态势

➢ 功能说明

全网综合态势感知通过攻击行为统计和挖掘等大数据分析技术，基于监测类系统监测结果、知识库数据建立模型进行关联分析，针对分析结果进行展示能够帮助用户发现全网安全问题。

全网综合态势是面向组织内安全监控的管理人员，从安全事件、脆弱性、组织架构、业务和操作系统等多个维度进行安全事件类型、风险趋势、安全对象的操作系统类型、安全对象的脆弱性、安全报表等监视主题提供具体的风险评估参数，可作为管理人员监控、指定策略、降低网络安全风险的依据和工具。

全网综合态势展示当前网络中风险资产，从安全事件、脆弱性、部门、业务、操作系统不同维度来呈现风险的分布情况，如受风险业务系统排名等等。态势展示的主题包括：全局安全事件趋势、全局风险趋势、安全域风险趋势、业务风险趋势、风险安全对象 TOP10、脆弱性安全对象 TOP10。

2）全网攻击态势

➢ 功能说明

攻击态势是通过与威胁检测探针联动分析并监控网络内部和外部攻击行为，支持多维度展示网络攻击的情况。支持对安全攻击事件进行分类展示，具体包括事件类别、攻击来源、攻击手段、攻击时间、攻击目标 IP、攻击源 IP、攻击次数等。支持图形化展示攻击类型的分布、占比，支持列表下钻展示攻击类型统计详情等。

对于外部的安全攻击事件，提供攻击地图展示功能，以地理地图为底图，可图形化呈现来自区域外的攻击现象，支持攻击数据的实时展现和按时间周期统计

展现。对于内部的安全攻击事件支持以组织机构分布的展示视角。

3）全网资产态势

- **功能说明**

依托分布式主动信息探测引擎、扫描技术和爬虫技术，探测全网 IP 地址和域名的分布情况。通过态势感知平台提供的知识库针对主动扫描和爬虫技术获取全网在线设备资产。通过大数据统计分析，快速掌握单位网络在线设备总数、设备分布、质保期等信息。

4）漏洞分布态势

- **功能说明**

当有漏洞威胁发布时，通过资产摸底的结果，借助态势感知大数据分析可快速定位漏洞威胁影响的资产，以及资产 IP 地址等详细信息，为通报预警和快速处置提供强有力的支撑。

5）全网病毒态势

- **功能说明**

通过实时收取网络防病毒、终端杀毒等系统安全防护日志信息并进行大数据分析，可视化展示全网病毒态势，同时为管理人员提供预警信息。

6）威胁情报态势

- **功能说明**

威胁情报态势支持对威胁情报数据的分类展示，支持包括 IP 类、域名类、漏洞类、网站类、恶意样本等威胁情报的展示。同时通过与威胁检测探针联动分析出本地安全威胁事件并展现，支持安全威胁事件展示内容包含但不限于：时间、源 IP、资产 IP、资产名称、资产所属业务系统等。

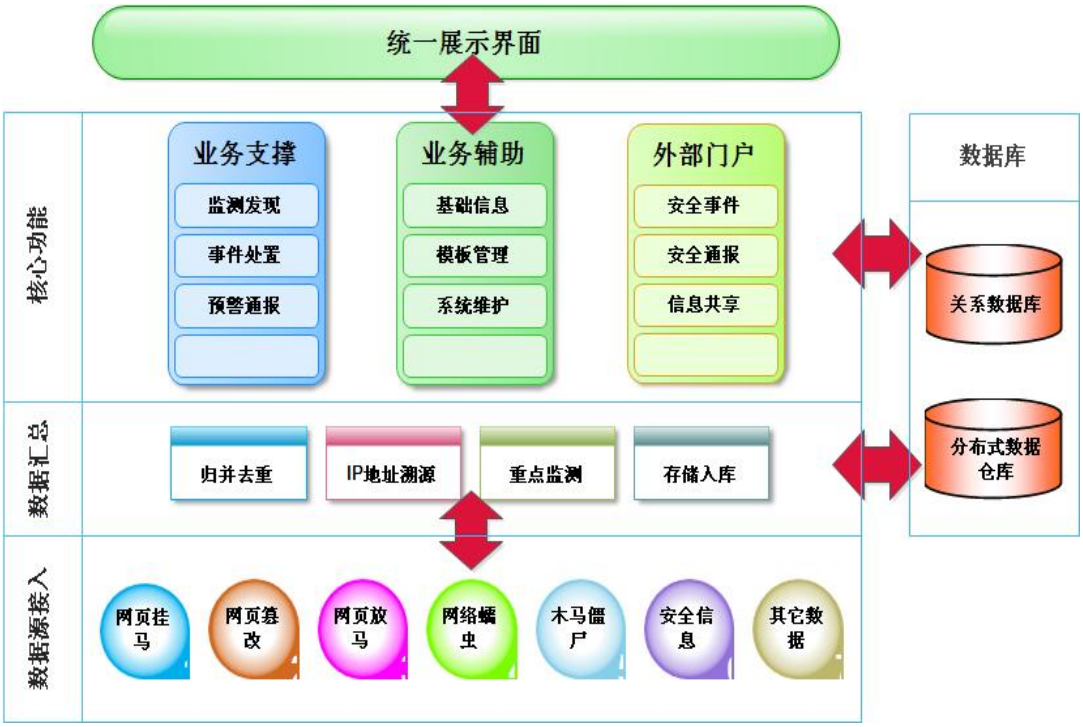
安全事件处置

态势感知平台具备通报预警与联动处置能力，具体功能如下：

1）通报预警

态势感知平台安全主要针对重大安全事件和协作单位信息进行通报。包括：支持通报模版、支持通报任务化、支持第三方通报、支持预警通报、支持通报平台发布和支持通报统计等。

功能模块流程如下图所示：



通报预警功能模块示意图

2）模板管理

支持模板的上传、下载、删除等操作。

3）任务管理

态势感知系统提供通报预警任务管理功能用于定期生成综合通报文档。该功能的主要目标是定时去驱动通报预警引擎执行指定的通报文档模板，引擎将会自动解析模板，根据模板的数据驱动部分自动获取平台中已存储的已采集和分析数据，再根据模板的数据布局部分自动生成相应的通报预警文档。该功能支持任务

的添加、删除、修改等操作。

4）联动处置

根据实际安全规范要求及安全业务需求设计了较多的安全产品，涵盖访问控制、入侵防范、防病毒、威胁检测、主机防护等，设计的安全产品在行使自身主体安全功能的同时，并不是作为孤立的安全资产存在，通过安全产品之间联动，可实现组合防御功能，在保证网络性能不牺牲的情况下实现安全闭环管理。

5）追踪溯源

通过实时获取各安全设备日志信息，基于大数据检索查询、挖掘分析、关联分析等技术对安全威胁源进行目标定位。支持基于攻击状态机模型的关联检测技术，支持图形化方式表示攻击回放，支持用户自定义关联分析场景，对于关联分析确认的攻击事件，采取预设响应处理。

2、 安全运维管理

1）安全策略管理

态势感知平台支持对安全设备（包括但不限于防火墙、入侵防御、网络防病毒、终端杀毒、日志审计、网络审计、数据库审计、运维审计、威胁检测探针等）、网络设备（包括但不限于交换机、路由器）、服务器设备（包括但不限于数据挖掘服务器、存储服务器）、边界设备（包括但不限于可信边界安全网关、隔离网闸）等进行集中管理、策略配置。

针对安全防护类设备（如防火墙、网络防病毒等）支持设备配置集中保存、查看、导出、更新和比较。能够查询、接收并保存设备配置信息，并为设备提供查看、导出和配置更新服务。可以为一个设备保存多个配置，并在更新时由管理员进行选择。设备配置应用后需要提示保存，可定期获取设备配置信息，可定期检查设备配置是否被私自修改，可显示配置变化状态。

支持防火墙、威胁检测探针、终端杀毒等安全设备策略编辑和下发，支持包过滤策略、访问控制策略、NAT 策略、内容过滤策略、带宽控制策略。防病毒策略参数、反垃圾邮件策略参数和防火墙参数的统一配置，支持策略分组管理。

支持防火墙、威胁检测探针、终端杀毒等安全设备策略集中编辑和下发，集中策略可以手工创建策略。策略按域制定，可将策略下发并应用到所选设备（可多台）或域，支持定期将指定的设备（可多台）进行下发。

支持将防火墙、威胁检测探针、终端杀毒等安全设备纳入态势感知平台实现以上安全策略管理功能。

2）边界集中监控审计

态势感知平台支持对边界平台进行集中监控与审计，实现如下功能要求：

a）设备控制，对接入平台内的多种关键设备进行控制；

b）平台监控，监控设备的实时状态信息、平台中链路与业务系统流量变化。捕获业务异常及各链路产生的告警信息，监视在线用户及其访问结果、访问量、所用终端等信息；

c）业务审计，审计接入平台内各个业务的历史运行状态并提供相应的统计报表；

d）自动报警，实时地将平台内各种设备产生的报警信息，通过短信方式或邮件的方式发送给指定的管理人员；

e）自动备份，自动地进行数据备份。能将数据远程备份到数据中心；

f）远程升级，能通过 WEB 浏览器以远程的方式对监管系统（包括系统内的各个模块）进行升级。

3）运行监控

态势感知平台支持针对各类型安全设备（防火墙、入侵防御、网络防病毒、

日志审计、网络安全审计、数据库审计、运维审计、流量检测探针等）运行状态监控。监控信息包含但不限于：设备 CPU 使用情况、内存使用情况、存储空间使用情况等，并在态势感知进行集中可视化展示。可设置各类资源告警阀值，自动对超过既定阀值的资源使用进行告警提醒，提醒管理员关注此安全对象的安全风险，以采取必要的手段。

4）安全拓扑

态势感知平台需支持安全拓扑功能，能够通过直观、友好的安全设备管理界面，实现对各安全设备的综合管理与监控。对网络中的安全节点进行拓扑管理，将安全资源进行细致的分类，对每类资源提供相应的管理功能。设置告警门限，管理网络告警和事件，以及监测周期设置，链路流量、颜色设置等。以及包括根据设备物理位置构建的物理视图和根据网络结构构建的安全视图管理等。

5）报表管理

态势感知平台需预置丰富的系统报表，可以充分满足用户的需求。报表支持多种格式的显示包括：pdf、html、excel、rtf 等。报表的生成方式分为手工报表和自动报表两种，手工报表支持根据用户输入的统计参数立即生成报表，自动报表可以按照每小时、每天、每周、每月、每年等周期的方式定时生成报表。

6）工单管理

态势感知平台需支持工单管理功能。管理员可以手工创建和派发工单，也可以设定规则由系统在一定条件下自动创建/派发工单。

支持安全管理员选择一个或多个关注的安全事件添加到指定的工单。并对工单进行派发，通过短信/邮件提醒功能以及工单超时处理的功能来提高工单处理的及时性；提供了工单处理过程的监控的功能，系统支持通过图形化的方式展示工单的处理阶段。

3、 态势平台扩展性

态势感知平台支持全面的系统扩容能力，扩容能力包括方面包括数据存储能力、分布式计算能力、数据分析能力。

数据存储能力扩容能够在要求存储的数据容量增大时进一步提高平台的存储能力。态势感知平台通过增加综合数据分析基础架构集群中服务器数量的方式来增加数据存储能力，每增加一台服务器所增加的数据存储容量由服务器配置的存储容量决定，整个平台支持千台以上服务器的集群存储空间。

数据分析能力扩容包括两个方面：分析性能扩容、分析场景扩容。分析性能扩容能够在分析数据量增大、分析任务增多、分析速度要求提高时进一步提高平台的分析性能，平台通过增加大数据基础架构集群中服务器数量和监测分析子系统服务器集群的方式来增加数据分析性能。分析场景扩容能够在分析需求增加时，针对新的分析需求建立新的分析场景来进行支持，平台通过在系统中新建场景的方式来进行分析场景扩容。本项目为了使安全态势感知平台能够尽可能采集全网更多的数据，拟采用平台加流量采集探针的部署方式。

流量采集探针

一、系统部署

本项目设计在澄迈园区物联网汇聚交换机、海口园区汇聚交换机、空港园区汇聚交换机处，分别部署 1 台流量采集探针，采集网络中的流量，输送到态势感知平台上，进行网络风险智能联动风险，感知发现网络中的威胁。

二、功能策略

1）攻击检测：支持对扫描探针攻击、缓冲区溢出攻击、拒绝服务攻击、漏洞扫描攻击、蠕虫病毒攻击、后门木马攻击、文件漏洞攻击等常见攻击行为检测。具有防逃逸检测能力，做到从根源上检测逃逸行为攻击。通过弱口令字典和口令

强度双种模式实现对邮件、LDAP、RDP 等协议的弱口令攻击检测。同时支持对邮件、TELNET、FTP 等协议的口令暴力破解攻击行为检测；

2）僵木蠕检测：支持对僵尸网络行为、木马控制行为、蠕虫活动行为、勒索病毒行为、移动端木马控制行为等多种僵尸主机行为检测。对被检测到的僵尸主机异常行为，支持对异常行为报文取证、事件记录，事件记录包括攻击源信息、事件应用协议、事件描述等信息；

3）DDos 检测：支持对 IP 扫描攻击、TCP 扫描攻击、端口扫描攻击等多种扫描类的 DDoS 攻击检测。支持对 ICMP FLOOD、TCP FLOOD、UDP FLOOD、SYN ACK FLOOD、FIN FLOOD、RST FLOOD、DNS FLOOD、HTTP FLOOD、HTTPS FLOOD 等多种 FLOOD 攻击行为检测；

4）恶意程序检测：支持对压缩类型、Windows 可执行类、Lunix 可执行类型、移动端类、文档类、JAR 类、加壳类的病毒文件检测。同时，支持对被检测文件进行样本还原和留存，对留存样本文件支持用户本地下载和加密外发；

5）APT 检测：可依靠威胁情报检测已知 APT 事件，依靠恶意程序检测未知 APT 事件，依靠僵尸行为规则库检测已知 APT 组织；

6）WEB 安全检测：支持对 SQL 注入攻击、跨站攻击、URL 跳转攻击、WEB 缓冲区溢出攻击、WEB 漏洞及越权攻击、Webshell 上传攻击、WEB 口令暴力破解攻击等多种类型的 WEB 攻击检测；

7）虚拟沙箱：虚拟沙箱中的系统环境中具有文件系统、注册表系统、窗口系统等多种操作系统核心机制，到达高度仿真效果。实现对恶意代码进行通用脱壳、深度扫描、动态行为分析等深度检测；

8）威胁情报：对网络数据流深入解析，解析出 IP、URL、域名、文件 MD5 值等多种信息放入威胁情报库匹配，并能够对恶意威胁样本还原捕获，发现当前网络所面临的现有或潜在威胁及风险；

9）威胁处置：持对入侵攻击、僵木蠕行为、恶意程序传播、APT 攻击、WEB 攻击、访问非法 URL/域名、恶意 IP 通信等安全事件进行阻断处置，支持旁路阻断处置和防火墙联动阻断处置两种方式；

流量分析：支持对所有网络流量从应用维度详细分析，记录统计各应用的总流量消耗、上下行流量消耗、当前上下行速率、连接总数等。并能分析记录应用的主机访问详情，包括主机 IP、总流量消耗、连接数等信息。

安全防护措施合规说明

根据下述安全管理中心等级保护的基本要求，结合本次项目采取的安全防护措施如下：

信息安全技术网络安全等级保护基本要求—安全管理中心		
控制点	安全通用要求	安全防护措施
系统管理	a）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；	部署运维审计系统（堡垒机），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。
	b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身	部署运维审计系统（堡垒机），系统管理员通过运维审计可进行配置、控制和管理，包括用户身份、

信息安全技术网络安全等级保护基本要求—安全管理中心		
控制点	安全通用要求	安全防护措施
	份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。	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。
审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；	部署运维审计系统（堡垒机），可对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。
	b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。	部署运维审计系统（堡垒机），可对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；	划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
	b）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	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；

信息安全技术网络安全等级保护基本要求—安全管理中心		
控制点	安全通用要求	安全防护措施
	管理；	
	c）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；	通过日志审计对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
	d）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；	通过日志审计可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
	e）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；	通过漏洞扫描发现威胁，并提供安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
	f）应能对网络中发生的各类安全事件进行识别、报警和分析。	通过部署态势感知平台，对网络中发生的各类威胁安全事件进行识别、报警和分析。

物联网安全防护体系建设

物联网安全设计是依据相关安全建设要求，遵循“重点保障，适度防护、体系防御”原则，围绕物联网场景的全生命周期设计安全防护方案，构建集防护、检测、响应于一体的全面的安全保障体系，在入侵行为对物联网信息系统发生影响之前，能够及时精准预警，实时构建弹性防御体系，避免、转移、降低物联网

信息系统面临的风险。针对用户物联网业务体系，为用户提供感知层防护、网络层防护、应用层防护以及数据安全防护等差异化安全防护手段，满足等保 2.0 以及物联网安全国家标准的要求。

本项目主要通过建设物联网安全感知与管理平台、物联网监管系统和物联网准入系统，形成整体物联网安全解决方案，有效保障园区物联网终端层、网络层和平台层安全。

物联网安全感知与管理平台

为构建统一物联网安全感知与管控能力，可通过采用物联网安全感知与管理平台实现。物联网安全感知与管理平台主要从安全监测和分析防护两个方面解决视频监控设备的安全问题，对物联网终端各类关键数据的采集，进行数据汇总、数据处理、数学建模分析等，整体功能主要包含态势感知、资产管理、威胁管理、加密管理、审计管理、准入管理和引擎管理等功能，实现对管辖范围内用户物联网终端资产分布、资产状态、非法接入、威胁统计、漏洞统计等管控能力。支持基于轻量化国密 TLS 协议的安全数据采集，支持系统级别态势信息收集。

平台通过行为分析和关联分析，可以识别非法接入、网络质量和异常攻击等多种场景下的异常威胁，包含各种系统入侵、对外 DDOS 攻击、资源耗尽、异常访问、在线离线等数十种类型的异常威胁分析。及时发现威胁并预警，推进安全管控处置。物联网安全感知与管理平台主要有如下 9 大功能子系统：

大数据分析子系统

大数据分析子系统是整个平台建设的中枢，是物联网场景下专用大数据实时数据系统。分析引擎构建于大数据平台之上，为威胁分析模块封装高效易用的分析工具，目前支持四类引擎：规则引擎支持对数据进行正则匹配、阈值计算、数

值对比等处理；关联引擎支持不同数据间聚合碰撞，如碰撞情报库，提取出有价值的告警；统计引擎通过统计指标的数据量，来确定一些高危动作，比如暴力破解；算法模型使用数据挖掘算法，提供复杂场景分析能力。

大数据分析子系统提供数据存储、数据处理、数据分析、数据服务的系统级能力和支撑。支持灵活的数据清洗编排，提供快速响应异构数据解析能力。

- 通过流式计算引擎，提供实时数据处理、分析能力；
- 提供 MPP 计算框架，支持实时数据 OLAP 能力；
- 提供全文搜索引擎；
- 支持物联数据时序存储；
- 采用统一的通信协议数据对外服务。

物联网接入网关子系统

物联网应用层网关是物联网平台侧的 IOT 接入管理系统，支持多种物联网设备接入场景，如直连设备接入，网关子设备级联接入，第三方平台对接（云云对接）等。

网关提供 MQTT、HTTP、COAP、Syslog 等标准协议的连接和通信，以及对连接通信的安全管理，包括设备认证鉴权和会话管理，对传输的数据进行加解密等。

安全感知子系统

根据资产、隐患、告警以及整体安全情况等维度分析安全态势，并对每个维度进行可视化展示。

■ **总体态势**

支持对资产信息进行实时威胁感知，总体态势大屏展示当前资产安全，同时可切换至其他分析维度的可视化大屏，客户通过大屏一览安全问题及时告警，帮

助客户快速响应。

■ **物联资产**

以资产维度，对客户当下资产所有情况、资产状态、高中低风险资产分布、资产整体防护情况、资产品牌类型分布、以及以安全域为维度的资产统计，客户通过该大屏可以更加快速直观的了解所管理的资产情况，帮助客户定位物联资产安全问题。

■ **威胁告警**

以告警维度展示包括告警数量、告警类型、最新告警、告警趋势、以及最多告警资产 top 等，为客户实时分析告警趋势，帮助客户及时发现告警资产。

■ **资产分析**

对资产进行资产画像分析，包括资产基本信息、危险等级打分、资产安全状态、网络进程关系以及状态性能趋势等。客户可通过此页面明确每个资产的安全情况。

资产管理子系统

■ **资产概览**

可视化展示年度月增长资产数量，资产在线离线状态、风险资产占比、资产类型分布、资产安全域分布，一览资产情况。

■ **资产列表**

资产管理页面统一展示和管理整网资产，支持资产 IP、资产所属区域、资产类型、资产状态、资产型号以及 CPU 和内存等资产信息展示。

■ **资产画像**

针对每个资产形成资产画像，从资产基本信息包括品牌、终端类型、系统信息、内存 CPU、型号，资产风险信息包括隐患、告警，资产访问关系，进程关系，

开放端口等维度为每个资产形成资产画像。

■ **资产安全域**

支持自定义安全域，根据实际业务情况将资产划分到不同安全域中，可以按照安全域的维度，去对应监管资产，更利于多资产的区域划分及管理。

隐患管理子系统

■ **隐患概览**

可视化展示漏洞及弱口令的分布情况及趋势，一览隐患、弱点整体的变化及分布情况。

■ **漏洞管理**

以漏洞为视角，展示漏洞最新发现时间、漏洞类型、漏洞等级、以及影响的资产数量和资产所在安全域等信息，在漏洞详情中展示更多漏洞信息包括漏洞基本信息、漏洞简介以及修复建议等，并展示当前漏洞所影响的所有资产，支持资产多条件检索。

■ **弱口令管理**

展示弱口令资产信息，包括资产的类型、所属品牌等以及弱口令的用户名和密码。及时为客户发现弱口令资产，进而提醒用户及时采取安全加固措施。

威胁分析子系统

■ **威胁概览**

以威胁总体概览形式，直观展示当前整网资产受威胁情况，包括告警总数、违规外联告警数、不同告警等级分布、告警类型分布、告警资产所属安全域、告警趋势等。

■ **安全告警**

以类型和告警名称聚合展示，支持合规缺陷、进程异常、网络扫描、终端认证变更、网络攻击、安全隐患以及配置风险等告警类型；每个告警类型展示最新发现的时间、告警等级、累计发生数量、告警详情等信息。

安全监测子系统

支持对监测平台的登录管控、状态监控和一键管理。从而达到对监测平台中可识别资产脆弱性、恶意 代码、风险漏洞等信息的监管。

数据加密子模块

■ **加密设置**

可对资产进行加密设置，支持批量和单个资产配置，在配置项中可选择关闭或开启加密，同时可以选择加密服务器，保障终端数据安全。

■ **密钥设置**

支持加密配置，支持新增和删除密钥服务器，同时支持密钥周期的修改和配置。

物联网安全监测平台

为形成面向物联网终端的安全监测评估机制，可通过采用物联网安全监测平台实现，物联网安全监测平台包含 9 大子系统。

网络空间测绘子系统

基于网络空间测绘技术对物联网专网信息资产进行纵深探测，对数量大、多元的信息数据，进行时间、空间、类型等一体化组织，基于统一的空间基准数据模型和资源标识,对数据进行有效关联组织和可视化表达,对网络空间资源的分布、状态、发展趋势等进行全方位动态展示，形成网络空间测绘拓扑图，为掌握在网资产在网络空间的位置提供可视化支撑,实现网络资产空间的可查、可定位，解决未知边界节点、未知资产发现和防护不足的难题。

■ **网络空间拓扑**

基于资产大数据库信息，以全网资产的网络路径为线，形成网络空间测绘拓扑图，标注全网关键路由节点，提供依据不同角度、不同层面的统计分析数据。

■ **网络空间路径查询**

支持对全网任意 IP 的网络路径查询,展现从顶级节点到目标 IP 的完整网络路径。

■ **网络空间异常分析**

通过网络空间测绘拓扑图进行全网节点、路由合规性梳理，发现异常节点、异常路由问题，包括：高危互联网路由、其他专网路由、私网路由、过长路由、

环线路由等。

资产安全监测子系统

基于资产遥感技术，对专网中接入的资产进行识别，自动获取厂商品牌、设备类型、操作系统类型、协议、平台等信息。根据识别的资产建立设备指纹库，实现资产智能检索和资产统计，对资产非法接入、非法占用、非法替换等安全行为进行监测告警。

■ **资产识别**

对全网资产进行识别，提供以下资产信息：

（1）设备类型，品牌型号，系统版本，固件版本。

（2）应用名称，品牌，版本。

（3）服务类型，端口等信息。

■ **资产大数据库**

基于识别的资产信息建立资产大数据库。

■ **资产统计**

统计识别的资产总数，在线数，空闲数，类型，厂家，位置等资产信息。

■ **资产检索**

对全网资产进行多维度检索，关联分析。

边界安全监测子系统

基于多风险场景建模，对专网边界安全进行监测，主动监测专网内存在的违规和非授权网络边界，发现不受控隐蔽的跨边界数据传输和网络访问通道，以及监测外部设备非授权入网和内部用户违规外联外部网络等高危风险行为，从而预防专网络资源被不法人员利用，造成网内资源被破坏、数据被泄露以及非法入侵

等安全事件。

■ **违规外联节点**

对违规外联互联网、违规外联视频网以及其他专网等私自连接不受控网络的违规外联节点进行监控。

■ **违规边界通道**

对违规的搭建网闸设备、WIFI 路由设备、交换机串线、DHCP 服务、网络代理服务、可解析互联网域名的 DNS 服务等违规网络边界通道行为进行监控。

■ **私网与专网连接**

对私自搭建网中网、多网卡跨网、私网 IP 入网访问等行为进行监控。

■ **不受控入网设备**

定位网络中存在的非授权设备接入，包括非授权登记设备、移动设备等，掌握全网入网资源情况。

■ **异常边界节点**

对全网资产空间路径节点监测，及时发现专网中未知的第三方网络路由节点以及未知的第三方边界节点接入等安全行为。

网络攻击监测子系统

基于安全分析框架对专网内网络通信行为进行大数据建模分析，对网内网络攻击行为进行实时监测。

■ **入侵渗透**

对黑客入侵攻击行为进行分析和监测，包括：定向探测、恶意扫描、端口试探、敏感端口扫描、失败连接等。

■ **漏洞利用**

从行为特征角度对利用设备漏洞的入侵攻击进行分析和监测。

■ **僵木蠕病毒**

基于传播行为特征对网内存在的病毒传播进行监测。

■ **数据窃取**

对可疑的数据传输和异常数据库访问进行监测。

异常访问监测子系统

基于大数据建模分析技术，主动监测网内异常访问，对重要或敏感业务、应用、数据、资产的访问行为实时监测。包含以下内容：

■ **异常访问设备/应用**

监测网内设备对业务系统或应用进行大规模的异常访问连接，定位设备地址以及连接总数等信息。

■ **数据异常访问**

监测网内设备对特定数据库端口进行高频密/异常的访问，定位访问源的地址、归属以及会话总数等信息。

■ **跨域异常访问**

基于完整的安全域策略，确定访问逻辑关系，监测全网异常的跨域访问行为，实现全网全量访问行为审计。

违规行为监测子系统

依据国家/单位的管理条例和相关规定，基于违规行为特征建立模型，通过正则方式匹配网络行为，对专网内出现的各类违规行为进行监测并告警，并定位违规主机，减少安全隐患，提升安全考核。

■ **违规入网**

保护内部网络资源不被外部非授权用户使用，监测非合规终端入网、非授权

终端入网以及移动设备入网等行为，提供入网设备的地址、所在位置等信息。

■ **游戏行为**

监测范围内的联网游戏行为，提取游戏主机、位置、游戏端口、游戏名和游戏版本等相关游戏特征信息。

■ **违规站点**

监测网络中未授权违规搭建的域名服务站点、FTP 站点、WEB 站点、论坛站点，提供服务器地址、访问方式、所在位置等信息。

■ **违规通讯**

监测网络中违规启用的非合规通讯系统和通讯工具，定位设备地址、位置和工具类型等相关信息。

■ **违规传输**

监测网络中存在的病毒文件传输、娱乐影音文件违规传输以及敏感信息文件传输等行为，进一步避免数据信息被泄露、病毒传染源和木马扩散。

安全隐患监测子系统

对全网设备节点进行扫描，针对开放的端口进行识别，实时分析端口、服务开放详情，及时发现网内自身存在脆弱性的资产设备、易被内外威胁利用或被当做攻击载体的设备，避免设备被恶意控制，引发各类安全事件。

■ **异常端口开放**

监测网络中开放敏感端口、全端口开放的设备，提供设备地址、信息等信息。

■ **可匿名登陆 FTP 服务器**

监测网络中无需输入用户名密码即可登录匿名 FTP 服务器，提供 FTP 服务器地址、信息等信息。

信令安全监测子系统

基于信令行为特征建模分析，对通过信令进行的网络攻击、黑客入侵、设备破坏、数据窃取等行为进行有效监测，持续监测可疑信令源、异常信令交互、高危控制信令，定位网络中存在的高危控制信令以及可疑访问源，保障设备和数据安全。

- **可疑信令源**

监测网络中信令源设备对网内目标设备发出可疑操控信令行为，提供可疑信令源的地址、位置、发起时间等信息。

- **异常信令交互**

监测网络设存在的异常信令交互、跨域信令交互以及频密信令请求等行为，提供信令源的地址、位置、发起时间等信息。

- **高危控制信令**

监测网络中基于信令协议对设备进行关闭、删除、修改等高危行为，提供信令源的地址、位置、时间以及操作类型等信息。

- **信令审计**

对全流量信令通信行为进行安全审计，获悉网络中信令的行为轨迹，为事后的问题分析和调查取证提供必要的信息。

安全数据取证子系统

为快速研判和查处各类内部安全事件和外部入侵案件提供充足的数据证据，避免出现证据不足遇到蓄意抵赖导致无法有效的查处和侦办，通过网络定位技术以及全网访问关系，对各种安全事件提供电子数据取证，包括设备地址对应关系、明细行为记录以及原始数据包通信记录，协助对安全事件的追查、核实与取证。

- **行为取证**

对专网行为进行取证留存，包括状态跟踪、访问行为、文件传输行为、传输指令等。

■ **网络原始数据包**

在网络异常产生时，提供最原始的通信记录数据，为安全行为分析等提供证据。

■ **交换机 IP-MAC 追踪**

通过交换机的 SNMP 协议,定位资产 IP-MAC 信息以及冒用或替换的 IP 和 MAC 的对应关系。

物联网准入系统

本项目设计在澄迈园区核心交换机、海口园区汇聚交换机、空港园区汇聚交换机处，分别部署 1 台网络准入系统，系统不但可以实现摄像头和打印机等 IoT 设备无代理端口级接入控制，还可以实现资产、资产风险、网络异常行为的统一管理。可广泛应用于视频专网管控、IoT 风险管控、内网资产统一管理等场景，是防范勒索病毒、发现威胁、识别风险和安全合规的最佳选择。

基于海口综合保税区当前网络终端资产数量、物联网终端数量，以及未来扩展接入需求，本次规划的网络准入系统授权为 5000 个点。

设备资产可视化管理

通过系统自动发现和功能，可以快速发现识别分布在网络中的摄像机、硬盘录像机、流媒体等视频语音设备，识别 PC 电脑、服务器、网络设备、安全设备等类型设备资源，并收集设备的 IP、MAC、开放端口、协议、在线时间、是否在线、所在交换机及物理端口、流量信息、会话信息、安全状态信息，通过流量识别技术可以发现设备的物理地址、设备的操作系统指纹、设备的流量行为模式等

信息。

同时提供网络管理功能，对感知网进行拓扑发现和展示拓扑图等，如果有设备通过 HUB 接入到感知网中也能进行快速定位，如果设备通过路由器等 NAT 方式接入亦可进行检测和定位。

IP地址使用情况可视化管理

终端准入系统系统会记录已经分配的 IP 地址、设备在线信息、历史 IP 使用记录。并对每个网络的可用地址进行计算，给管理员提供准确的参考。通过图表的不同颜色对不同接入状态的 IP 使用进行直观、可视化的表示，有效简化管理人员的 IP 地址及时更新与维护问题。

网络控制权限精细化到IP及协议和端口

系统以旁路方式部署在被管网络的核心交换设备上，通过端口镜像进行流量监听，不需要调整网络结构，可适应各类组网方式的网络。针对违规接入网络的终端进行自动阻断隔离，禁止接入网络。

针对已经发现的摄像机实现动态 ACL 网络权限控制，仅允许摄像机访问必要的网络，合理的设置设备的网络访问权限，将风险降到最低。

同时，针对发现网内存在设备伪冒、异常访问和异常攻击行为的终端，在发现之后可通过准入控制手段进行阻断隔离。

网络访问控制权限可以精确到 IP、协议、端口，并根据不同分组分配不同的 ACL 访问权限。

前端视频设备流量与行为仿冒检查与防护

系统对摄像机的 IP、MAC、硬件信息等形成的指纹信息生成免检设备列表和采用流量来识别摄像机的行为最终形成设备防伪冒列表，可以清晰的定位到所有

的摄像机的接入状态和接入位置。一旦出现摄像机被恶意人员替换为电脑或路由器等设备进行入网行为，将被及时发现和进行处理，并通过 Web 浏览器实施警告，控制+警告的方式提醒违规接入人员。系统后台提供仿冒设备的详细审计信息。

同时，当网内摄像头被恶意攻击者利用漏洞等方式进行控制后从事非法活动，系统能够第一时间通过流量异常方式进行感知、告警、阻断、取证：系统管理员可定义前段视频设备在安全合规状态下只与指定服务器如硬盘录像机、流媒体服务器等进行通信。终端准入系统能够通过流量进行监测，利用大数据机器学习，生成网络访问行为画像，一旦发现前端视频设备的访问流量超出了画像范围，能够在第一时间进行发现、告警、阻断。

合规遵从管理

入合规性检测：支持准入颗粒度检查，发现用户帐号使用多个终端登录、终端未使用规定的认证方式、未使用特定的接入控制点设备、未使用指定的 WIFI 进行准入认证给予阻断，并通知管理员进行审批。

软件合规性检测：支持发现未安装防病毒软件的终端设备，支持发现未安装企业合规的软件或者安装违规软件的设备，发现软件违规的设备立即告警或者阻断。

配置合规性检测： 支持发现未关闭 guest 帐号的终端设备；支持发现未加入域的设备；支持发现开启共享目录的终端设备；支持发现未开启屏保，或屏保设置不合规的终端设备；支持发现存在可疑文件的终端设备；发现配置违规的设备立即告警或者阻断。

日志外部推送

系统提供 SYSLOG、SNMP Trap 日志推送功能，支持日志级别设定，可将日志

便捷地推送给视频平台等系统。

云平台安全建设

设计原则

1. 符合等级保护原则

私有云承载了用户大量重要信息系统，其安全建设不能忽视国家相关政策要求，在安全保障体系建设上最终所要达到的保护效果应符合《信息系统安全等级保护基本要求》以及最新发布的《信息安全技术 信息系统安全等级保护 第二分册 云计算安全技术要求》。

2. 体系化的设计原则

安全系统设计应充分考虑到各个层面的安全风险，构建完整的安全防护体系，充分保证系统的安全性。同时，应确保方案中使用的信息安全产品和技术方案在设计和实现的全过程中有具体的措施来充分保证其安全性。

3. 系统的先进性原则

客户业务系统及云平台对所需的各类安全系统提出了很高的要求，必须认真考虑各安全系统的技术水平、合理性、先进性、安全性和稳定性等特点，共同打好工程的技术基础。

4. 安全可视化原则

随着平台的不断成熟，云上各类业务系统的不断迁入，安全能力的不断增加，整个平台的安全会变得越来越复杂。所以安全平台要能够全局观察整个平台的安全态势，实现安全拓扑、业务风险、安全合规等可视化管理，让安全运维管理变得更加简单。

云平台安全能力建设

数据中心云平台在构建本地化安全能力这块，围绕着等保合规“一个中心、三重防护”的安全建设理念给数据中心云平台上的业务系统提供符合等保三级的安全能力，如在数据中心云平台的边界处部署防火墙、web 应用防火墙等设备，提供对应的安全防护能力，且构建本地集中的安全管理中心，统一为数据中心云平台环境提供本地化的安全能力。安全管理中心提供完善的安全能力，包括数据传输安全类的 VPN 安全能力，事前监测类的漏洞扫描、主机安全防护、攻击预警平台等安全能力，事后审计类的堡垒机、日志审计、数据库审计等安全能力。集中化的安全能力结合态势感知系统可为用户提供全局安全视角和安全态势感知能力，打造面向云环境的动态安全防御体系。

通过业界成熟可靠的安全技术及安全产品，结合专业技术人员的安全技术经验和能力，系统化的搭建安全技术体系，确保技术体系的安全性与可用性的有机结合，达到适用性要求。

安全软硬件设备清单

根据上述方案，本项目建设的网络安全软硬件如下表：

表 5- 45 网络安全软/硬件清单

1	互联网边界防火墙	台	2
2	服务器区防火墙	台	2
3	电子政务外网互联网区专线防火墙	台	1
4	园区接入防火墙	台	2
5	管理区防火墙	台	2
6	办公区防火墙	台	2
7	物联网区防火墙	台	2
8	上网行为管理	台	2
9	日志审计	台	1
10	运维审计系统	台	1
11	漏洞扫描系统	台	1
12	主机安全管理系统	台	1
13	攻击预警平台	台	1
14	网闸	台	2
15	SSL VPN	台	1

16	数据库与防护系统	台	1
17	web 应用防火墙	台	2
18	态势感知平台	套	1
19		台	3
20	流量探针 （5G-综保区）	台	1
21	流量探针 （3G-金盘园区&空港园区）	台	2
22	物联网安全感知与管理平台	套	1
23		台	1
24	物联网监管系统	套	1
25		台	1
26	网络准入控制系统	台	3

等级保护安全管理体系详细设计

安全管理制度

安全策略和制度体系

设计目标

安全技术措施的有效实施需要安全管理制度的助力，同样，安全管理制度的落实也常常需要技术措施的支撑，两者是相辅相成，相互关联的。等级保护对于海口综合保税区网络安全制度体系的建设要求参照了 ISO 27001 的相关标准，即安全管理制度体系自上而下分为安全策略、管理制度和操作规程、记录表单，海

口综合保税区需要建设符合实际情况的安全管理制度体系，应覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容，并对管理人员或操作人员执行的日常管理操作建立操作规程。

设计实现

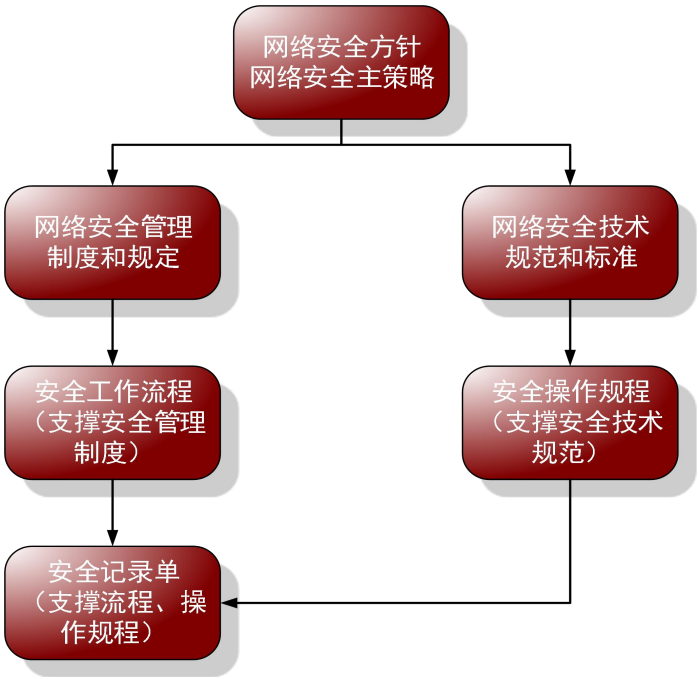


图 5- 87 安全管理制度示意图

（1）安全方针和策略。

最高方针，纲领性的安全策略主文档，陈述本策略的目的、适用范围、网络安全的管理意图、支持目标以及指导原则，网络安全各个方面所应遵守的原则方法和指导性策略。

（2）安全管理制度和规范

各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是必须具有可操作性，而且必须得到有效推行和实施的。

技术标准和规范，包括各个安全等级区域网络设备、主机操作系统和主要应用程序的应遵守的安全配置和管理的技术标准和规范。技术标准和规范将作为各个网络设备、主机操作系统和应用程序的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，不允许发生违背和冲突。

表 5- 48 安全管理制度和规范表

序号	类型	制度组成
1	总体方针、安全策略	《网络安全总体方针和安全策略》
2	安全管理机构	《网络安全组织及职责管理规定》
3		《重大事项授权和审批管理规定》
4	安全制度管理	《网络安全制度管理规定》
5	人员安全管理	《内部人员安全管理规定》
6		《外部人员安全管理规定》
7	信息系统建设管理	《信息系统建设安全管理办法》
8	系统运维管理	《机房环境安全管理规定》
9		《办公环境安全管理办法》
10		《信息资产安全管理办法》
11		《介质管理办法》
12		《信息资产运行维护安全管理办法》
13		《网络安全管理规定》
14		《系统安全管理规定》
15		《防病毒管理办法》
16		《口令管理办法》
17		《信息系统变更管理规定》

序号	类型	制度组成
18		《备份与恢复管理规定》

（3）安全流程和操作规程

为网络安全建立相关的流程，保证安全运营可以遵照标准流程制度执行，主要的内容包括：

流程制定：建立健全流程管理制度，主要包括的流程有：安全事件处置流程、安全风险评估流程、安全事件应急响应流程、安全事件溯源取证流程、安全设备上线交割流程等；

流程变更维护：定期的维护和修订相关的管理制度；

流程发布：根据需要，定期发布变更后的全套流程到相关的组织范围内，并对发布的流程进行相关的培训。

（4）安全记录单

安全记录单是落实安全流程和操作规程的具体表单，根据不同等级信息系统的要求可以通过不同方式的安全记录单落实并在日常工作中具体执行。主要包括日常操作的记录、工作记录、流转记录以及审批记录等。

制度文件管理

设计目标

制度文件需要正式发布并进行定期评审修订和版本控制。网络安全管理制度应该得到海口综合保税区管理中心负责人的签发和认可，只有被正式发布并真正落实的管理制度才能促使海口综合保税区管理中心安全管理能力的提升和安全技术措施的有效运行。

设计实现

网络安全管理制度体系是不断改进和完善的过程，包括以下：

（1）制定和发布

安全制度系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到管理层的大力支持和推动外，还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

安全制度在制定和发布过程中，应当实施以下安全管理：

安全管理制度应具有统一的格式，并进行版本控制；

安全管理职能部门应组织相关人员对制定的安全管理制度进行论证和审定；

安全管理制度应通过正式、有效的方式发布；

安全管理制度应注明发布范围，并对收发文进行登记。

（2）评审和修订

网络安全领导小组应组织相关人员对于网络安全制度体系文件进行评审，并确定其有效执行期限。同时应指定网络安全职能部门每年审视安全策略系列文档，具体检查内容包括：

网络安全策略中的主要更新；

网络安全标准中的主要更新。网络安全标准不需要全部更新，可以仅对因变更而受影响的部分进行更新；如果必要，可以使用年度审视／更新流程对网络安全标准做一次全面更新。

安全管理组织机构和人员的安全职责的主要更新；

操作流程的主要更新；

各类管理规定、管理办法和暂行规定的主要更新；

用户协议的主要更新等。

安全管理机构

网络安全组织机构及职责

设计目标

网络安全管理机构是行使海口综合保税区管理中心网络安全管理职能的重要机构，一般由网络安全管理领导机构和执行机构构成，网络安全领导机构需确保整个组织贯彻海口综合保税区管理中心的网络安全方针、策略和制度等。等级保护制度中明确规定“应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由主管领导担任或授权。”并设立网络安全管理的职能部门。

设计实现

海口综合保税区管理中心应根据管理工作需要设立安全管理机构，但至少应包括网络安全领导小组和网络安全管理职能部门，其工作职责分工如下：

一、网络安全领导小组

网络安全领导小组是海口综合保税区管理中心网络安全工作的最高领导决策机构，负责海口综合保税区管理中心网络安全工作的宏观管理，其最高领导由海口综合保税区管理中心主要负责人担任或授权，职责如下：

(1)贯彻执行国家关于网络安全工作的方针、政策，组织落实海口综合保税区管理中心网络安全体系建设工作的目标、方针、政策。

(2)审定网络安全相关策略、规范及管理规定。

(3)监督、检查网络安全相关制度的落实与执行情况。

(4)协调指挥网络安全重大突发事件的应急处理。

(5)完成上级单位交办的有关工作。

二、网络安全管理部门

网络安全管理部门负责落实网络安全领导小组各项决策，协调组织海口综合保税区管理中心各项网络安全工作，具体职责如下：

(1)负责网络安全日常工作的协调和处理。

(2)负责网络安全总体规划设计与实施。

(3)组织网络安全管理规定的编制；

(4)督促网络安全重大突发事件应急预案的落实。

(5)组织网络安全培训的相关工作。

(6)完成网络安全领导小组交办的有关事项。

岗位职责及授权审批

设计目标

网络安全管理应落实岗位安全责任，网络安全组织机构及职责明确了组织层面的管理职责，但管理职责的落实需要层层落实到人，等级保护中明确要求要“设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责”，并设立系统管理员、审计管理员和安全管理员，并明确岗位工作职责。

设计实现

根据海口综合保税区管理中心实际情况，设立相关的网络安全管理岗位，但至少应包括安全主管以及“三员”（系统管理员、审计管理员和安全管理员），且“三员”工作职责需分工明确，互相监督，安全管理员需专职，不得兼任其他岗位工作。

三员的岗位职责建议如下：

（1）安全管理员

安全管理员不能兼任网络管理员、系统管理员，其职责是：

组织信息系统的安全风险评估工作，并定期进行系统漏洞扫描，形成安全现状评估报告；

定期编制网络安全状态报告，向网络安全领导小组报告海口综合保税区业务系统的网络安全整体情况；

负责核心网络安全设备的安全配置管理工作；

编制网络安全设备和系统的运行维护标准；

负责信息系统安全监督及网络安全管理系统、补丁分发系统和防病毒系统的日常运行维护工作。

负责沟通、协调和组织处理网络安全事件，确保网络安全事件能够及时处置和响应。

（2）系统管理员

系统管理员不能兼任安全管理员，其职责是：

负责网络及网络安全设备的配置、部署、运行维护和日常管理工作；

负责编制网络及网络安全设备的安全配置标准；

能够及时发现、处理网络、网络安全设备的故障和相关安全事件，并能根据流程及时上报，减少网络安全事件的扩大和影响；

负责服务器的日常安全管理工作，确保服务器操作系统的漏洞最小化，保障服务器的安全稳定运行；

负责编制服务器操作系统的安全配置标准；

能够及时发现、处理服务器和操作系统相关安全事件，并能根据流程及时上报，减少网络安全事件的扩大和影响。

（3）安全审计员

安全审计员的职责是：

定期审计网络安全制度执行情况，收集和分析信息系统日志和审计记录，及时报告可能存在的问题；

对安全、网络、系统、应用、数据库管理员的操作行为进行监督，对安全职责落实情况进行检查。

信息中心可根据实际管理需要进行岗位职责的细化，如将系统管理和网络管理工作分别由不同的人负责，对重要的应用系统设置业务系统管理员，对机房、数据库、信息资产进行专门的管理，设置机房管理员、数据库管理员、信息资产管理员等，并明确岗位职责。

在明确岗位职责过程中，信息中心需梳理在网络安全管理过程中需要授权审批的事项，并根据各个部门和岗位的职责明确授权审批部门和批准人等，对于系统变更、重要操作、物理访问和系统接入等重要事项建立审批程序，按照审批程序执行审批过程， 对重要活动建立逐级审批制度，并定期审查，及时更新相关信息。

内部沟通和外部合作

设计目标

网络安全管理工作不是孤立的，在海口综合保税区业务系统管理工作中离不开安全管理中心工作的保障，同样，网络安全管理中心工作也离不开海口综合保税区业务系统部门的配合，要使网络安全管理工作顺利开展，需“加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题”，加强内部沟通。

同时，海口综合保税区管理中心的网络安全工作也需要得到外部专家和技术力量的支持，包括监管部门、供应商、业界专家及其他安全组织等。

设计实现

聘请专家和外部顾问成员，这些成员需要对网络安全或相关领域有丰富地知识和经验，如安全技术、电子政务、等级保护或质量管理等。专家和外部顾问负责对网络安全重要问题的决策提供咨询和建议。

同时加强与供应商、业界专家、专业的安全公司等安全组织的合作和沟通。建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

安全审核与检查

设计目标

网络安全管理工作是否有效，安全制度和规范是否得到落实需要海口综合保税区管理中心网络安全管理部门定期进行检查，以便及时发现问题，持续改进和提升网络安全管理能力。按照等级保护的要求，海口综合保税区业务系统网络安全检查可分为定期常规安全检查和定期全面安全检查，安全检查工作需进行认真准备，保留记录。

设计实现

海口综合保税区管理中心可根据实际情况，进行安全检查工作安排。包括：

（1）定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

（2）定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；由于海口综合保税区管理中心人员及安全技术能力有限，全面安全检查可请专业的安全厂商协助完成。

（3）制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。海口综合保税区管理中心也可参照上级监管单位或自行制定安全检查评价指标，以便量化考核安全工作的执行情况。

安全管理人员

内部人员安全管理

设计目标

人是网络安全工作的主体，也是网络安全威胁的主要来源，调查发现，越来越多的网络安全事件是由内部人员的恶意或工作疏忽导致，因此，加强人员安全管理是网络安全管理工作的重中之重，其中，尤其需要加强对内部人员的安全教育和审核。

设计实现

针对内部人员的安全管理需从人员的录用、安全培训和教育、技能考核和调用、离岗审核等全过程进行安全管理，具体管理要求包括：

（1）录用前

a.指定或授权专门的部门或人员负责人员录用；

b.应对被录用人员的身份、安全背景、专业资格或资质等进行审查， 对其所具有的技术技能进行考核；

c.与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

（2）工作期间

a.对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；

b.针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；

c.定期对不同岗位的人员进行技能考核；

（3）调离岗

a.及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

b.办理严格的调离手续，并承诺调离后的保密义务后方可离开。

外部人员安全管理

设计目标

在日常业务工作中，海口综合保税区管理中心越来越多地与外部单位人员进行业务合作和往来，外部人员包括指软件开发商，硬件供应商，系统集成商，设备维护商和服务提供商，以及实习生、临时工、调用人员等。这些人员由于工作需要需临时或短期访问海口综合保税区管理中心内部网络，进出海口综合保税区业务系统工作场所，非内部人员由于流动性强，背景情况不明，给海口综合保税区业务系统的安全带来较大隐患，必须建立严格的物理和网络访问授权审批制度，并有效执行。

设计实现

海口综合保税区管理中心应制定外部人员物理访问和网络接入的管理制度，并记录相关内容，具体要求如下：

（1）在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；

（2）在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；

（3）外部人员离场后及时清除其所有的访问权限；

（4）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

安全建设管理

系统定级和备案

设计目标

根据新等级保护制度的要求，二级以上（含二级）信息系统在定级工作中需要组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定，新建信息系统在规划阶段就可根据信息系统将承载的业务的重要程度对信息系统进行定级，按照相应等级进行等级保护安全体系设计和建设，对二级以上（含二级）信息系统还需按照公安机关的要求进行备案。本项目海口综合保税区对 4 个信息系统按照等保三级进行设计和建设。

设计实现

为了进一步明确信息系统定级、备案的相关责任和流程，应明确系统定级、备案和系统测评流程，包括以下内容：

（1）明确定级备案责任部门和责任人；

（2）跟公安部门沟通明确定级备案相关材料要求和格式；

（3）制定系统定级和备案工作的时间计划；

（4）定级评审相关单位和专家联系和确定；

（5）组织定级评审工作，并获得上级或相关部门的批准。

为确保系统等级保护定级备案工作的规范性和专业性，可选择专业的等级保护咨询服务完成相关工作。

系统安全方案设计

设计目标

按照“三同步”的原则，网络安全需要与信息化建设同步规划、同步建设、同步使用，在系统建设规划阶段需明确安全建设的目标和建设需求并进行安全规划方案的设计，安全方案应经过评审，经过批准后才能实施。

设计实现

安全方案设计需根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

安全方案应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

安全建设项目根据实际建设阶段需设计不同的安全方案，包括总体建设规划方案、详细设计方案、建设实施方案等，安全方案需组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

安全产品采购管理

设计目标

网络安全产品的采购和使用应符合国家的有关规定，对于密码产品的采购和使用需符合国家密码主管部门的要求，并预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

设计实现

针对海口综合保税区业务系统中安全设备采购，需严格按照设备采购管理流程和政府设备采购目录来采购相应的安全产品；并且在搭建的模拟系统中对这些安全设备和软件进行测试和试运行验证，以防止产生对系统产生不可预见的影响。

外包软件开发管理

设计目标

对于外包软件开发由于开发过程可控，在系统上线后可能引发各种安全问题，且难以从源头解决，因此，在等级保护制度中，对于外包软件开发明确要求应在软件交付前检测其中可能存在的恶意代码，并要求开发单位提供软件设计文档和使用指南，对于三级系统的外包软件开发还要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

设计实现

针对外包软件开发建议可选择专业的安全公司作为第三方进行开发过程的安全管理，包括协助开发单位建立安全开发制度和流程，并在软件开发的关键节点进行代码检测，代码检测采用自动化工具+专家审核的检测方式，既提高检测准确性和效率，又能发现系统逻辑错误等问题。

工程实施管理

设计目标

信息系统安全建设过程中，涉及产品安装部署、功能启用、策略配置、与应用系统集成等各方面工作，安全工程建设整个过程本身还需要安全可控，需要由专门的部门或人员负责工程实施过程的管理，并制定安全工程实施方案，控制工程实施过程。对于三级信息系统，等级保护还明确要求需通过第三方工程监理控制项目的实施过程。

设计实现

海口综合保税区业务系统实施周期较长，在实施过程中指定监理作为项目第三方监控单位，并指定了专门的项目安全工作负责人，制定了项目管理制度和项目实施方案。

测试及交付管理

设计目标

项目建设完成后在正式上线前应进行系统测试，应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告，按照等级保护的要求，应进

行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

在系统交付时，应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，对负责系统运行维护的技术人员进行相应的技能培训，提供建设过程文档和运行维护文档。

设计实现

由于海口综合保税区业务系统的复杂性，在系统及各子系统交付时，要制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；对负责运行维护的技术人员进行相应的技能培训；确保提供建设过程中的文档和指导用户进行运行维护的文档。

系统安全性测试建议选择专业的安全公司进行系统上线前安全检测，并针对安全风险及时采取措施整改。

系统等级测评

设计目标

在系统建设完成后，按照等级保护的要求必须选择国家认可的测评机构对信息系统进行等级测评，并在系统运行过程中定期进行测评，对于三级系统要求每年测评一次，对发现不符合相应等级保护标准要求的及时整改，并在发生重大变更或级别发生变化时进行等级测评。

设计实现

系统上线运行后，选择经过国家认可的等级保护测评机构进行测评，由于测评工作的专业性和复杂性，建议选择专业安全厂商协助海口综合保税区管理中心进行测评工作，如在正式测评前协助海口综合保税区管理中心进行自测和整改等。

服务供应商选择

设计目标

来自供应链的安全威胁已经越来越引起人们的关注，加强对供应链的管理是新等级保护制度的变化之一，等级保护制度规定要确保服务供应商的选择符合国家的有关规定；与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；并定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

设计实现

确保选择有相应资质的安全服务商、安全集成商、系统集成商和软件开发商，并与其签订协议，明确相关安全义务和责任。

安全运维管理

按照等级保护要求，日常安全运维管理主要从环境管理、资产管理、介质管理、资产维护管理、漏洞和风险管理、网络和系统安全管理、防病毒管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置管理、应急预案管理、外包运维管理几个方面进行考虑。

环境管理

设计目标

环境是指信息系统所处的物理环境，包括机房、配线间、办公场所等，加强对环境的安全管理主要是为了防止非授权物理访问导致的对信息系统的破坏，一般来说，机房作为重要信息设备集中放置的场所应重点加强防护，重要办公区域也需要加强物理防护。

设计实现

所有的服务器和核心网络设备均按照要求放置在机房中，指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；

制定机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；

制定办公环境安全管理制度，并对以下方面进行规定：办公室的网络安全要求；办公终端网络安全保密要求；办公终端使用规范等。

资产管理

设计目标

信息资产是构成网络和信系统的基础，是系统各种服务功能实现的提供者和信息存储的承载者，应明确海口综合保税区业务系统信息资产的种类、数量、责任人等，并建立清单，定期盘点，对重要信息资产应重点保护。

设计实现

编制并定期更新与被保护对象相关的资产清单，包括各类硬件、软件、数据、介质、文档等，确定并标识资产责任部门、重要程度和所处位置等内容；

根据资产的重要程度对资产进行标识管理，针对重要信息资产制定专门的管理措施；

对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

介质管理

设计目标

介质作为信息的载体，在信息的存储、传递过程中发挥着重要作用，同时，也是恶意代码传播的重要手段、且容易导致信息泄露。

海口综合保税区管理中心需要制定严格的介质管理制度，规范介质的使用行为，对个人介质更加需要严格的管理。

设计实现

需制定介质安全管理制度，规定介质的使用范围、介质标识、介质保存等方面的内容。

对于海口综合保税区管理中心介质，需将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；

对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

设备维护管理

设计目标

信息设备在日常工作中存储和处理业务信息，设备的可用性和安全性对网络安全至关重要，要加强对信息设备日常的管理，包括设备日常维护、外带、报修、报废等。

设计实现

对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

对配套设施、软硬件维护管理做出规定，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；

信息处理设备必须经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据必须加密；

含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

漏洞和风险管理

设计目标

网络安全漏洞是信息系统脆弱性的主要表现，易被攻击者利用进而入侵系统进行破坏，对漏洞的发现和修补除了需采取必要的技术措施外，加强对系统的日常安全评估，并及时进行整改修复，也是降低网络安全风险的重要手段。

设计实现

定期开展安全评估，形成评估报告，对发现的漏洞等安全问题及时通报，并限定整改时间；

定期开展安全测评，形成安全测评报告，对发现的问题制定整改方案，采取措施应对发现的安全问题，相关内容形成记录。

网络和系统安全管理

设计目标

网络和系统作为信息系统的基础性设施，为各个业务系统和办公应用提供连通和数据传输，实现信息共享，网络和系统应进行更细分更专业的管理，对重要的业务系统还需要指定专门的管理人员。

设计实现

按照等级保护的要求，对网络和系统的安全管理包括：

（1）划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。可以指定专门的网络管理员、系统管理员、数据库管理员等，对网络设备、操作系统、数据库等进行专业化管理。

（2）指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制。对重要服务器、数据库、业务应用等的管理账户应更加严格管理。

（3）建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、 日志管理 、日常操作、升级与打补丁、口令更新周期等方面作出规定；

（4）制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；

（5）详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；

（6）指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；

（7）严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；

（8）严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。

（9）严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；

（10）保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

防病毒管理

设计目标

对于病毒的防范需要采取必要的安全技术措施，但技术措施的有效性需要安全管理制度进行保障，病毒防范作为海口综合保税区管理中心重要的网络安全基础性工作，必须确保提高全员的防病毒意识，确保技术手段的有效落实。

设计实现

（1）制定防病毒管理办法，明确防恶意代码软件授权使用、恶意代码库升级、定期汇报等流程，明确对外来计算机或存储设备接入系统前进行恶意代码检查。

（2）定期验证防范恶意代码攻击的技术措施的有效性；

（3）组织全员的网络安全意识培训，提高全员对病毒的防范意识。

配置管理

设计目标

信息系统的配置基线管理是重要的日常运维管理工作，良好的配置管理是系统安全可靠运行的基础，配置基线应结合等级保护的要求，进行相关配置信息的保存、更新和变更控制。

设计实现

海口综合保税区管理中心日常配置管理包括：

（1）记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；

（2）将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

（3）建立安全配置基线，对设备、操作系统、数据库等制定安全基线，并定期维护安全基线。

密码管理

设计目标

根据等级保护的要求，海口综合保税区管理中心在网络安全建设过程中需遵循密码相关国家标准和行业标准，使用国家密码管理主管部门认证核准的密码技术和产品。

设计实现

确保在系统中使用的密码相关产品获得有效的国家密码管理主管部门规定的检测报告或密码产品型号证书。

变更管理

设计目标

网络安全风险是“动态”的主要因素之一，就是网络和信息系统是会发生变化的，为了加强防范由于网络和系统变化对整体安全现状的影响，规避变更产生的风险，需进行变更管理。

设计实现

变更管理建设的内容包括：

（1）明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；

（2）建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；

（3）建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

备份与恢复管理

设计目标

按照等级保护要求，三级信息系统需具备实时的数据备份能力，并能进行异地备份，对于海口综合保税区业务系统信息系统容灾备份能力的建设，除了建设

备份与恢复技术措施外，对备份策略的制定和管理，备份与流程的制定以及备份恢复能力的演练是海口综合保税区业务系统实现高可用的重要保证。

设计实现

制定海口综合保税区管理中心备份与恢复管理制度，体现的内容包括：

（1）指定责任部门，识别需要定期备份的重要业务信息、系统数据及软件系统等；

（2）定义备份信息的备份方式、备份频度、存储介质和保存期等；

（3）根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

（4）建立备份和恢复流程，对备份过程进行记录，所有文件和记录应妥善保存；

（5）建立演练流程，定期对恢复程序进行演练，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

安全事件处置和应急管理

设计目标

新等级保护制度强调了海口综合保税区管理中心对于网络安全事件处置能力和应急管理的能力，在当前网络安全威胁形势下，各类安全事件频发，网络安全保障的思路已经从传统的以防为主，转换为更加关注海口综合保税区管理中心中心威胁检测能力以及快速的响应和处置能力。

设计实现

针对网络安全事件需要建设以下内容：

（1）及时向安全管理部门报告所发现的安全弱点和可疑事件；在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

（2）制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

（3）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

此外，对海口综合保税区业务系统中心应急管理需要从总体制度层面加以规范和明确，并按照国家应急管理的相关规定明确流程，定期演练，包括：

（1）规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。

（2）制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

（3） 定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；

（4）定期对原有的应急预案重新评估，修订完善。

外包运维管理

设计目标

针对目前普遍存在的信息系统运维工作外包的现状，新等级保护明确了对外部管理的相关要求，海口综合保税区业务系统中心选择外包服务商应符合国家相关制度规范，并需明确外部服务商的责任。

设计实现

对于外包服务商的管理包括以下：

（1）确保外包运维服务商的选择符合国家的有关规定，与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

（2）保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

（3）在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

密码应用建设方案

根据《关于进一步明确省政务信息化项目建设密码应用有关要求的通知》琼国密局字[2021]2 号要求：《海南省信息化项目建议书网络安全部分编制规范(试行)》《海南省信息化项目可行性研究报告网络安全部分编制规范(试行)》《海南省信息化项目初步设计网络安全部分编制规范(试行)》《海南省购买信息化服务方案网络安全部分编制规范(试行)》中涉及密码应用的编制要求可由密码应用方案统一替代。

因此本项目“密码应用建设方案”单独进行编制，详见《海口综合保税区智慧园区建设项目密码应用方案》。

网络安全等保/密评/分保工作方案

本项目涉及众多业务应用系统，整体上按照等级保护三级和二级要求提出工作方案。

项目依据

1、 实施依据

在本次项目中，我方项目组将依据国家等级保护相关标准开展工作，依据标准包括但不限于如下国家标准：

- 《信息安全等级保护管理办法》（公通字[2007]43 号）；
- GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》；
- GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》；
- GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》；
- GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》；
- 适用于被测评方的行业法律法规；
- 其他相关法律法规要求。

2、 实施原则

根据对业主的需求分析，在整个项目的设计与实施过程中将严格遵循国家关于信息安全等级保护测评的相关标准。同时遵循如下原则：保密性、可用性、安全性、规范性。

1）规范性

在本项目的设计与实施过程中，我方项目组将保证相关工作的规范性。测评工作将严格符合国家等级保护相关标准要求，同时符合电力行业等级保护的相关行业标准，以期能够交付一个合规、合理的优质项目。

2）保密性

对业主敏感信息保密非工作常重视，业主敏感信息视为最重要商业机密，针对本项目将实施相应的保密措施以保证业主相关敏感信息。

3）可用性

对测评过程中出具的相关建设报告中所提出的整改措施力求切实可用，对于目前网络安全领域不能实现的技术手段或因业主行业特殊原因无法实现的整改措施应进行相关说明，保证所提出的整改建议具有可用性。

4）安全性

为保证本项目的实施过程中不影响原业务系统的可用性、实时性，应在进行工具测试等环节与业主进行充分沟通，在业主许可及技术准备充分的前提下进行相关测评以保证本项目实施过程的安全性，若业主不同意进行工具测试，项目组需与业主签署《自愿放弃工具测试声明》，由业主方签字并盖章。

3、 实施步骤

1）系统定级备案

重要信息系统的定级备案工作，是开展等级保护的首要环节，是进行信息系统建设、整改、测评、备案、监督检查等后续工作的前提。

2）差距分析

差距分析工作内容就是根据网络和信息系统的安全保护等级，根据国家等级保护相应等级的技术和管理要求，分析评价网络和信息系统当前的安全防护水平和措施与相应等级要求之间的差距。

3）等保建设整改

等级保护建设整改是根据信息系统差距分析结果，对信息系统所依赖的服务器操作系统、数据库、网络及安全设备进行配置安全加固，安装和实施各项新增安全设备，保障信息系统的安全稳定性。

4）等保管理制度建设

等级保护管理制度建设是根据信息安全等级保护安全管理的要求，编写符合等级保护要求的信息安全管理规范和制度，通过安全管理的加强来规避管理风险。

定级备案

1. 工作目的

协助客户完成安全等级保护的定级与备案。依据 GBT 22240-2020 《信息安全技术 网络安全等级保护定级指南》，对未定级、备案信息系统进行梳理，完成信息系统安全等级保护的定级与备案工作。

2. 工作方式

在定级咨询过程中，咨询顾问将通过现场调研的方式来全面了解主要信息系统的基本情况，如数量、类别、名称、承载业务、服务范围、用户数量、部署方式，以进行汇总分析，初步进行系统归类、重要性划分，为下一步确定定级对象、确定级别、形成定级报告做准备。

现场信息资料收集，以及对系统管理员进行访谈及信息确认，是现场调研的主要工作。通过现场的了解，可以较深入理解信息系统的重要程度，重要信息的分类情况，以及用户分布情况。一般系统的定级结果，不依赖于现有保护措施，所以通过现场的工作，可以基本准确理解信息系统及承载重要信息的侵害客体以及侵害程度，从而为进一步定级报告的编写打下良好基础。

3. 工作内容

1) 协助定级

如果信息系统只承载一项业务，可以直接为该信息系统确定等级，不必划分业务子系统。如果信息系统承载多项业务，应根据各项业务的性质和特点，将信息系统分成若干业务子系统，分别为各业务子系统确定安全保护等级，信息系统

的安全保护等级由各业务子系统的最高等级决定。信息系统是进行等级确定和等级保护管理的最终对象。

现场调研后，咨询顾问会准备《信息系统安全等级保护定级报告模板》，给出定级报告示例。信息管理部门和业务部门依据定级报告模板，起草各信息系统安全等级保护定级报告，咨询顾问根据已经掌握的信息系统情况，对各信息系统定级报告的合理性进行初步研究和审核把关，请相关单位派人共同讨论，按照系统类别梳理定级报告，对照国家对不同等级的要求，在报告内容、行文格式、定级准确性等方面给出修改意见。根据讨论的定级报告修改意见，统一汇总、整理后，形成定级报告的专家评审稿。

2）专家评审

咨询顾问还将根据需要协助聘请等级保护专家、行业专家、主管机关领导等外部专家，召开信息系统定级评审会，对定级报告进行外部评审，形成评审意见。

咨询顾问将参考专家定级评审意见，最终协助确定信息系统等级，协助将各信息系统安全保护等级定级报告报经上级主管部门审批同意。

最后，咨询顾问将协助填写《信息系统安全等级保护备案表》，若经过专家评审目标系统为第三级，还需要提供协助客户提供《系统拓扑结构及说明》、《系统安全组织机构及管理制度》、《系统安全保护设施设计实施方案或改建实施方案》、《系统使用的安全产品清单及认证、销售许可证明》。并由咨询顾问在对接当地公安局网安支队时提供必要的支持，了解当地公安政策，依据当地条例住准备定级资料，最终完成目标系统备案工作。

4. 提交成果

《信息系统安全等级保护备案表》

《信息系统安全等级保护定级报告》

《专家评审意见》

《系统拓扑结构及说明》（三级系统提交）

《系统安全组织机构及管理制度》（三级系统提交）

《系统安全保护设施设计实施方案或改建实施方案》（三级系统提交）

《系统使用的安全产品清单及认证、销售许可证明》（三级系统提交）

以及当地公安局要求提供的相关资料。

5. 输出成果

公安局网安部门发放的《XX 信息系统备案证明》

差距分析

根据国家等级保护政策法规和标准规范，确定安全保护等级的信息系统应该具有相应级别的安全防护能力，其中主要是根据 GBT22239-2019《网络安全技术网络安全等级保护基本要求》来分析承载于互联网和综合安防网上的业务应用系统目前的安全防护能力与基本要求中相应级别之间的差距。

1. 工作目的

根据国家等级保护要求，对于确定了安全保护等级的信息系统规定了基本的安全保护要求，规定了应该具有的防护措施，以确保信息系统具有相当水平的安全防护能力。

差距分析就是根据 GBT22239-2019《网络安全技术网络安全等级保护基本要求》，结合本项目的业务情况和行业要求，从安全技术和安全管理两个方面，全面分析信息系统现有防护措施和能力与相应等级基本要求之间存在的差距，用以为等级保护建设提供客观依据并指导信息系统等级保护体系设计。

2. 工作方式

业务系统差距分析工作计划通过以下方式进行。

1）访谈

访谈是指评估人员与信息系统有关人员就差距分析所关注的问题进行有针对性的询问和交流的过程，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

访谈深度（即访谈内容的详细程度）以及访谈的广度（即对被评估组织中员工角色类型以及每种类型中人数的覆盖程度）由评估人员依据不同的评估需要进行选择和判断。

2）检查

检查是指对评估对象（如规范、机制或行为）进行观察、调查、评审、分析或核查的过程。与访谈类似，该过程可以帮助评估者了解现状、澄清疑问或获得证据。

比较典型的检查行为包括：对安全配置的核查、对安全策略的分析和评审等。

3）测试

测试是指在特定环境中运行一个或多个评估对象（限于机制或行为）并将实际结果与预期结果进行比较的过程。测试的目标是判定对象是否符合预定的一组规格。测试过程可以帮助评估者获得证据。

4）调查表

根据系统业务情况和系统现状，制定详细的调查表，并由相关人员进行填写，以获得业务系统基础数据。具体包括应用信息系统调查表、物理资产调查表、软件资产调查表、各相关设备资产调查表。

3. 工作内容

按照等级保护实施要求，不同安全等级的信息系统应该具备相应等级的安全防护能力，部署相应的安全设备，制定相应的安全管理机构、制度、岗位等。差距分析就是依据等级保护技术标准和管理规范，比较分析信息系统安全防护能力与等级要求之间的差距，为等级化体系设计提供依据。

4. 提交成果

差距分析过程中将产生众多文档，其中包括过程文档和结果文档，过程文档用以支持咨询人员进行差距分析，并形成结果文档《等级保护差距分析报告》。

信息系统等级保护差距分析报告主要内容：差距分析是以现场调查和测试所收集的信息为依据，满足等级保护要求为目标，对现有系统安全做出的一种客观的、真实的评价。报告内容包括对各信息系统现有安全防护水平与相应等级之间差距的描述和整改建议等。差距分析是制定信息系统安全等级保护体系设计方案前的一个非常关键的环节，为信息系统安全等级保护体系设计方案的撰写提供参考。

等保建设整改

1. 工作目的

根据前期等级保护整改、差距分析结果，结合项目的业务需求，对信息系统的服务器、网络设备、安全设备、数据库进行安全策略加强、调优等，加强网络、系统和设备抵御攻击和威胁的能力，整体提高网络安全防护水平。

2. 工作方式

安全加固与优化将采用如下工作方式：

会议交流：项目组将根据脆弱性检测结果，提出安全加固与优化建议，并通

过组织交流会的形式，与相关负责人就每台主机、网络与安全设备的具体加固内容进行协商，明确操作风险，探讨利害关系，确定加固方式，最终确定安全加固方案；

现场实施：项目组将赴现场，以安全加固方案为依据，协助和指导系统运维人员进行加固与优化操作，逐项实施每台设备的安全加固项目。

3. 工作流程

系统相关网络设备、安全设备、服务器操作系统以及数据库等配置安全加固与优化的工作流程如下图所示：

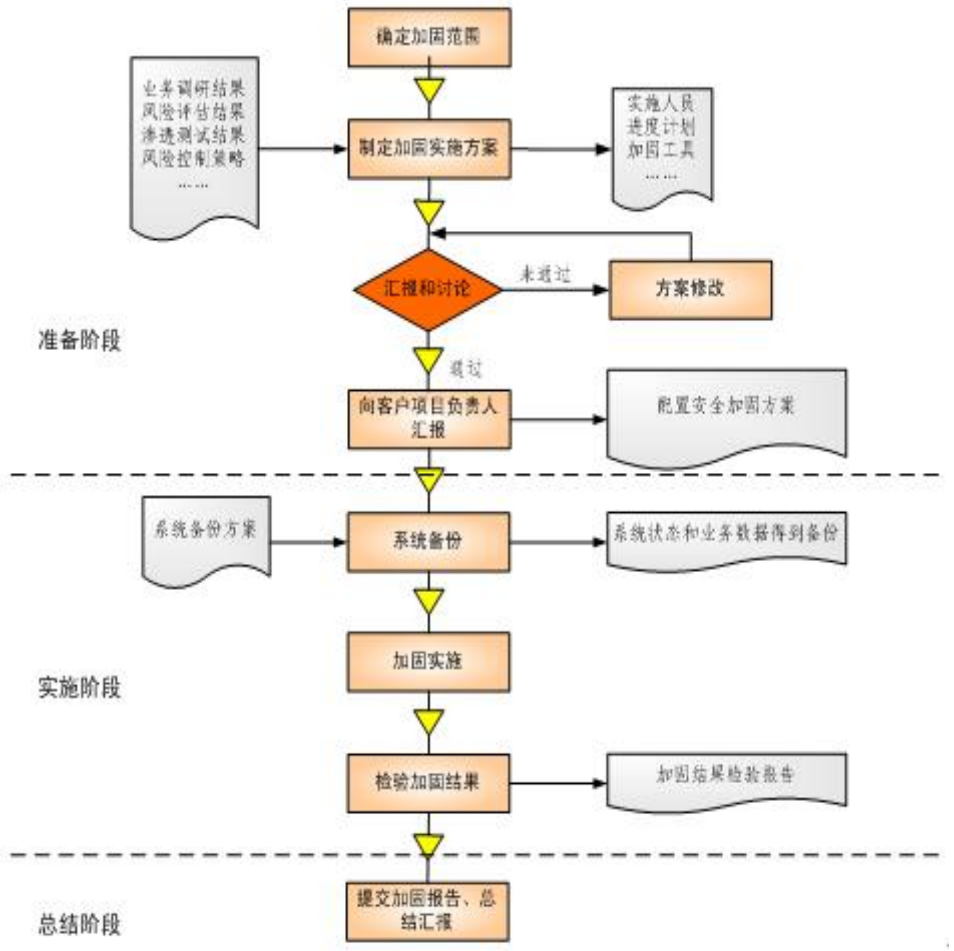


图 5- 5

图 5- 6 工作流程图

配置加固流程描述如下（项目实施中，可以根据实际情况需要，对流程进行调整、合并和展开等）：

确定加固范围：确定实施范围，如应用系统、资产等；

制定加固实施方案：确定实施人员、加固工具、进度计划等，为实施提供指导；

向项目负责人汇报：就配置加固实施方案向项目负责人汇报，并得到同意；

系统备份：对配置加固涉及的系统和数据进行备份；

加固实施：根据配置加固实施方案进行加固实施；

检验加固结果：验证配置加固的有效性；

提交加固报告、总结汇报：总结配置加固实施情况，并进行汇报。

4. 提交成果

《系统安全扫描人工分析报告》、《安全配置检查和加固建议报告》、《系统主机设备加固报告》、《网络设备加固实施报告》。

通过对系统相关主机、网络与安全设备配置的加固与优化，将会减少安全漏洞和设备配置策略的不合理性，提高系统抗攻击的能力，从而可有效防范攻击、限制危害蔓延，充分发挥各项安全措施的作用，增强系统的安全性和稳定性。

等级保护管理制度建设

1. 工作目的

以等级保护差距分析结果为依据，依照安全保障体系设计所提及的建设内容，按照等级保护标准要求，制定等级保护管理体系框架，明确管理方针、策略，以及相应的规定、操作规程、业务流程和记录表单；从贴合业务流程的原则出发，

指导系统运维方按照等级保护三级系统的管理标准，编写管理制度文件，并进行反复沟通和修订，确保所制定的文件的适用性，且满足各系统相应保护等级的安全管理要求。通过制定和完善管理制度，明确责任权力，规范操作，加强对人员、设备和业务系统的管理，完备应急响应机制，将显著提升信息安全管理水平，有效控制信息系统所面临的安全风险，从而确保业务系统的安全、稳定运行。

2. 工作方式

等级制度建设的工作方式主要如下：

调研访谈：采用定制的调研问卷进行访谈，了解本项目的详细情况，如组织机构（部门设置、人员职务、外部联系和接口）、业务流程（目标、流程、人员、物理位置、外部联系和接口）、信息资产（网络拓扑、主机和设备资料）、内部文件（运维程序、安全管理制度、建设方案）、原有管理相关文件及需遵守的法律法规文件等。

项目会议：召开会议，以调研访谈记录和差距分析结果为依据，研究制定安全管理制度框架和编写相应的管理制度。

交流：与相关人员就管理制度框架、管理制度内容进行反复的沟通、讨论和修订，确保安全管理制度贴合业务实际，并满足等级保护标准和相关政策要求。

3. 工作内容

制定和本项目相关的安全保护等级相适应的配套管理制度，制度相关内容如下：

安全管理机构：加强和完善安全机构的建设，设立指导和管理信息安全工作的信息安全领导小组，设立安全主管、安全管理各个方面的负责人，明确定义各个工作岗位的职责。建立各种安全管理活动的审批程序，明确对内对外的沟通协作方式，建立对各项安全管理活动的监督审核机制。

安全管理制度：在差距分析的基础上，建立信息安全工作总体方针、安全策略，以方针策略为依据建立配套的安全管理制度及流程规范，由专门的组织机构负责管理制度的制订、发布和贯彻落实。定期对制度进行评审和修订，确保安全管理制度的适用性。

人员安全管理：主要涉及两方面，对内部人员的安全管理和对外部人员的安全管理。具体包括人员录用、人员离岗、人员考核、安全意识教育和培训和外部人员访问管理等方面。

系统建设管理：为了建设符合安全等级保护要求的信息系统、系统建设管理主要关注的是信息系统生命周期中的前三个阶段（即设计、采购、实施）中各项安全管理活动，实现信息系统的安全管理贯穿系统的整个生命周期。系统建设管理分别从工程实施建设前、建设过程以及建设完毕交付等三方面考虑，具体包括系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评和安全服务商选择等方面。

系统运维管理：系统运行涉及到很多管理方面，要保证系统始终处于相应安全保护等级的安全状态中。要监控系统发生的重大变化，以便修改对应的安全措施。系统运维管理主要包括环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等方面。

4. 工作成果

依照等级保护标准，综合考虑安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理各方面的具体要求，建立安全管理框架，如图所示：

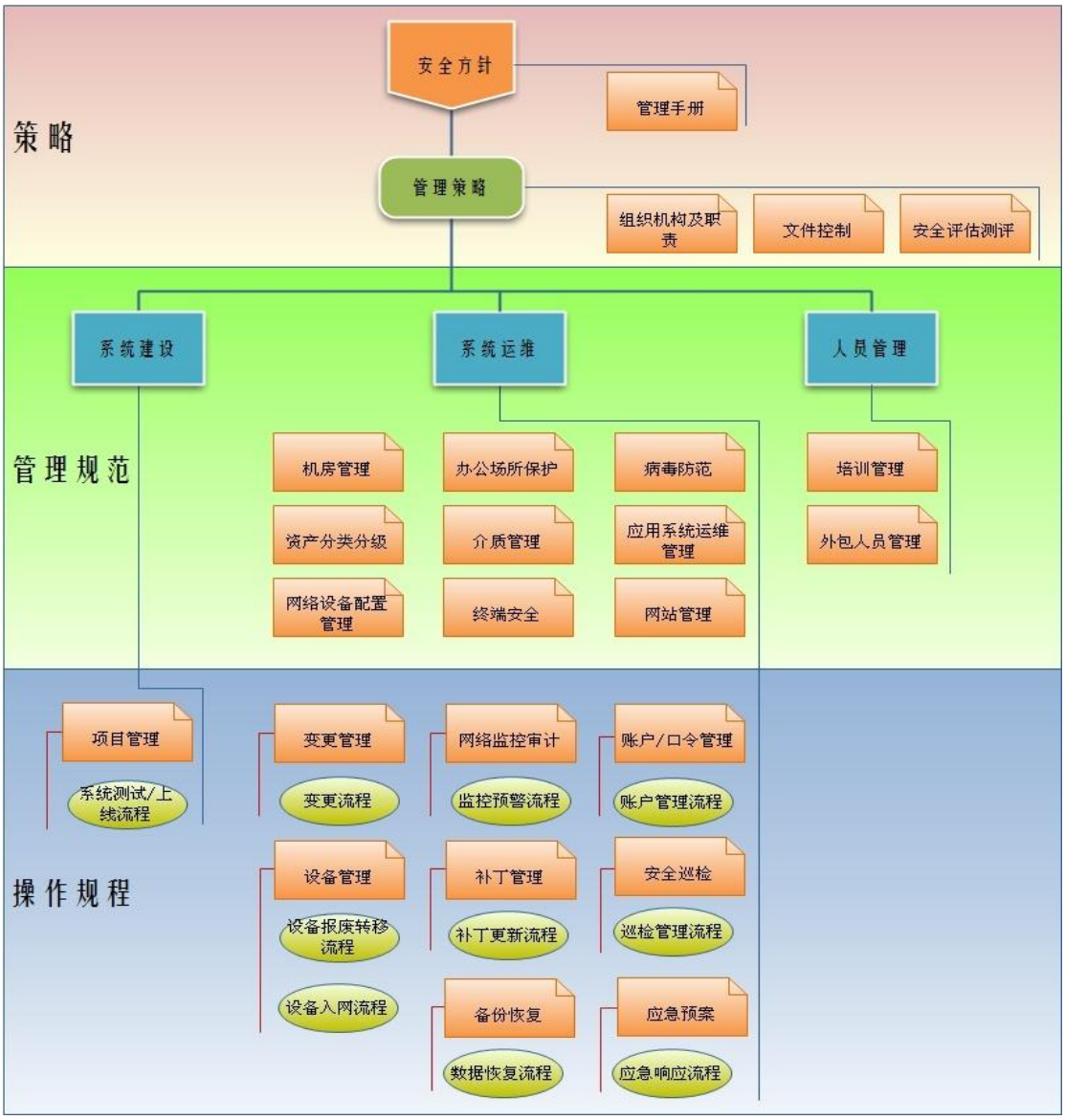


图 5- 1 安全管理框架图

以安全管理框架为基础，本次制度建设具体内容包括（不限于以下文件）：

1）《信息安全管理手册》：规定了本项目安全管理的方针、目标和策略，明确应采取的相应控制措施，并对整套文档进行解释说明。

2）《组织机构及职责》明确安全管理机构及各成员职责，规定机房管理员、系统管理员、网络管理员、数据库管理员和安全管理员的岗位职责，并对单位对内对外的沟通等方面作出要求。

3）《机房管理》对机房环境要求、人员与设备进出、工作人员管理、日常监控管理、系统上线及变更管理等做出明确规定。

4）《办公场所保护》对办公场所安全管理和消防安全进行规定，以加强办公场所的防火、防盗、防信息泄露等工作。

5）《病毒防范》对防病毒的控制措施和操作程序制定管理规范，以预防病毒与各种恶意软件的入侵，提高对病毒的防御能力，保障本项目和日常工作的正常进行。

6）《资产分类分级》对资产进行分类和统一化标识，使本项目的资产受到有效的保护。

7）《介质管理》为加强对介质的使用控制和物理上的保护，防止其承载的敏感信息遭泄漏、篡改、丢失或破坏，对介质的处置做出明确规定。

8）《应用系统运维管理》对应用系统日常维护所涉及的巡检、配置管理、故障处置、系统优化、软件维护等工作进行相应规定，并明确考核措施。

9）《网络设备配置管理》对网络、安全设备配置的管理，以及配置变更所涉及的申请、审批和实施等事项作出明确规定。

10）《终端安全》规范终端的应用，对终端的使用和联网进行明确规定，以防止病毒、网络攻击及失泄密事件的发生。

11）《网站管理》对网站建设、信息发布、网站监控与维护作出明确规定，确保网站的安全性与可靠性。

12）《培训管理》要求定期开展培训，并对培训流程进行规范，对培训效果进行考核，确保人员的安全意识和技术水平得以有效提升。

13） 《外包人员管理》对外包服务人员的派遣、监督和考核作出明确规定，确保外保服务质量。

14） 《系统安全建设》以等级保护要求为依据，对信息系统建设的各阶段作出了相应规定，以提高本项目的安全保障能力和水平，保障并促进信息化建设。

15） 《变更管理》明确需要执行申报审批手续的重要变更事项，如补丁更新、软件升级、设备更换等，并对变更的执行流程进行规定。

16） 《设备管理》对设备的获取、接收、入账、维护、用途变更、报废处理等环节做出明确规定，防止因资产的丢失、损坏、失窃、使用不当而导致业务系统正常运行的中断。

17） 《网络监控审计》监控网络运行状况，对安全审计、IDS 等设备的使用作出明确规定，以保云平台网络安全、高效运行。

18） 《补丁管理》对服务器操作系统、小型机操作系统、终端计算机操作系统、应用中间件和数据库软件的补丁更新要求和操作流程进行规范，确保系统防御病毒和网络攻击的能力。

19） 《备份恢复》确定业务数据的备份策略，并从数据恢复的申请、申请的审批、实施数据恢复、结果检查等方面做出明确规定，以保证业务系统数据的完整性和可用性。

20） 《帐户/口令管理》明确帐户的角色及权限管理，并对口令的设置、保管与更新进行了明确规定，以防止非授权访问。

21） 《安全巡检》对网络与安全设备、服务器、应用系统和机房基础环境的巡检工作进行规范，以保证本项目业务应用系统的安全运行，有效消除安全隐患。

等级测评

等级测评过程中将对系统的技术体系和管理体系进行全方位的安全测评。其中，技术体系包含：物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复 5 个方面安全测评。管理体系包含：安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理 5 个方面的安全测评。

本期测评对象包括：

表 1 测评对象

序号	名 称	部署位置	等保级别	备注
1	园区公共服务平台	政务云	三级	互联网区域
2	园区运营管理平台	政务云	三级	电子政务外网区
3	展销综合服务平台	本地云	二级	
4	作业综合服务平台	本地云	二级	
5	辅助监管业务服务平台	本地云	二级	
6	应用支撑平台	本地云	二级	

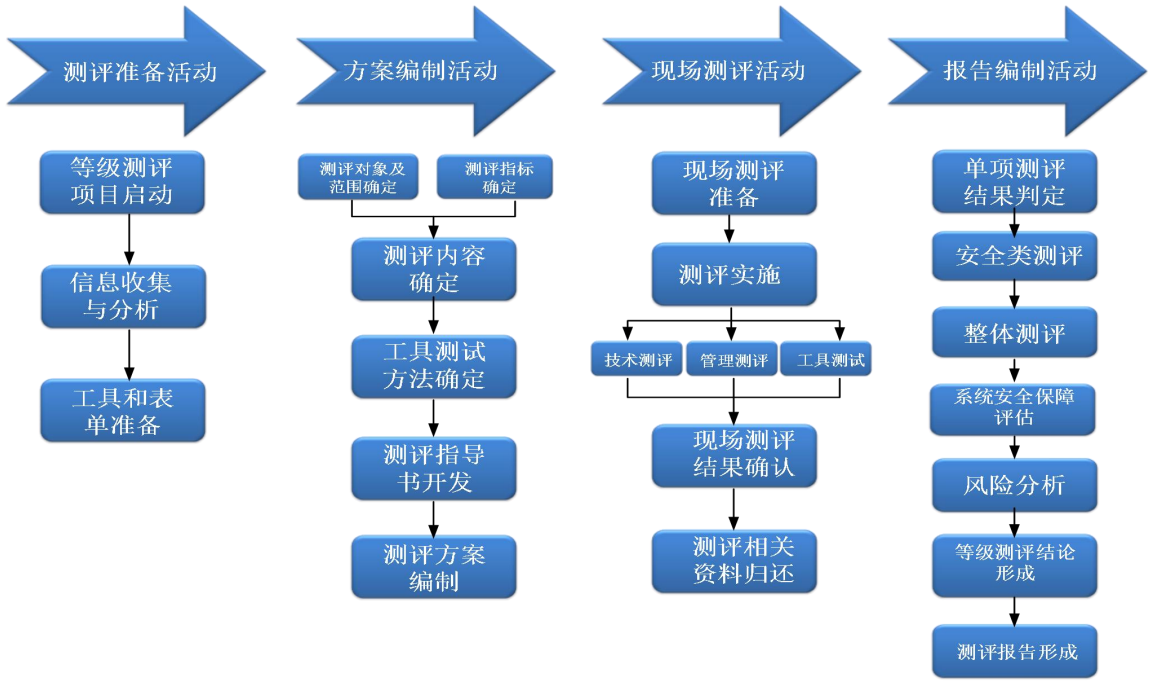
1. 测评流程

依据国家等级保护相关政策标准及行业相关政策要求，测评过程按如下思路进行：

收集被测系统信息，识别信息系统结构、业务、边界、区域等内容。了解信息系统定级情况，根据《基本要求》的要求，选择测评指标，并根据《测评要求》的要求，选择测评对象，对系统实施安全测评。制定测评方案，并实施现场测评活动。通过现场测评收集的证据，进行单项测评、单元测评和整体测评，并对测评结果进行分析，得出信息系统安全现状与《基本要求》的差距，对于不达标项目，进行风险分析，评估当前安全保护能力是否会造成信息系统面临较高的风险。最终形成等级测评结论。

本项目的测评过程主要分为测评准备、方案编制、现场测评、报告编制 4 个阶段进行。详细过程依照 GB/T28449-2018《信息安全技术 网络安全等级保护测评过程指南》以及公司制度《等保测评管理制度》执行。

本次项目工作流程图如下所示：



1）**测评准备活动：**等级测评项目确定后双方成立测评项目组，双方协同梳理信息系统基本要素，完成客户单位信息系统基本要素和定级情况。

2）**方案编制活动：**在获取客户单位信息系统基本要素和定级情况后，电子项目组明确项目内容、实施安排、人员配备、配合内容、注意事项、材料准备、测评指导书等内容完成测评方案编制，并与客户确认测评方案和测评时间安排，确认正式现场测评步骤。

3）**现场测评活动：**通过项目启动会议，双方人员准备相关材料、工具等，进入信息系统现场进行信息系统调查；根据各信息系统现场调查的结果，分别对各信息系统的物理、主机、网络、应用、数据、管理等方面进行安全测评，并且通过技术手段对信息系统测评对象实施安全测试和扫描，获取信息系统最真实的数据。此外利用风险评估的方法对信息系统进行合理的信息系统风险分析。针对测评过程中的问题，我方项目组向用户提交《不符合项及整改建议》，用户整改完成后，我方项目组进行问题整改确认。

4）**报告编制活动：**根据现场测评实施获取的材料、信息、记录等进行统一汇总，分析得到单项测评结果，根据得到的单项测评结果计算得到安全类测评结果。在安全类测评的基础上，进一步分析信息系统已有安全措施的整体相关性，对信息系统实施整体测评，主要包括安全控制点间、安全类间和区域间相互作用的安全测评，并且结合标准和行业特殊需求合理分析相关数据形成最终的等级测评结论，出具符合信息系统安全等级保护要求的信息安全等级保护测评报告（提交成果《测评报告》）。

2. 测评方法

安全测评的主要方式包括：访谈、检查和测试。

1）访谈

访谈是指测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据表明信息系统安全保护措施是否落实的一种方法。在访谈的范围上，应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

2）检查

检查是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在检查范围上，应基本覆盖所有的对象种类（设备、文档、机制等），数量上可以抽样。

3）测试

测试是指测评人员通过对测评对象按照预定的方法/工具使其产生特定的响应等活动，查看、分析响应输出结果，获取证据以证明信息系统安全等级保护措施是否得以有效实施的一种方法。在测试范围上，应基本覆盖不同类型的机制，在数量上可以抽样。

表 2 测评方式

管理测评	☑ 访谈	☑ 文档审核	☑ 实地察看	
安全物理环境测评	☑ 访谈	☑ 文档审核	☑ 实地察看	
安全区域边界测评	☑ 访谈	☑ 文档审核	☑ 配置检查	☑ 工具测试
安全通信网络测评	☑ 访谈	☑ 文档审核	☑ 配置检查	☑ 工具测试
设备计算环境测评	☑ 访谈	☑ 文档审核	☑ 配置检查	☑ 工具测试

安全管理中心测评	☑ 访谈	☑ 文档审核	☑ 配置检查	

安全运维

主要工作为推动安全管理制度的落实工作，包括但不限于以下工作内容：

- 定期安全漏洞扫描工作；
- 定期进行设备安全基线核查工作；
- 组织安全整改工作；
- 组织安全培训；
- 其他安全管理工作。

项目管理与控制

1. 项目质量保证与管理

根据项目的具体需要，本项目的整个管理过程将参考美国项目管理协会 PMI 提出的项目管理方法学、我方项目组项目管理办法、ISO9000 体系以及一些顾问管理规范实施。通过规范化的项目管理，保证项目过程的质量。

2. 配置管理

在项目进程中的项目组将维护一个项目文档输出的基线。所有的文档的版本修改和更新将在配置管理的版本控制和变更控制之下，并将所有文档的最新版本维护在基线中。

3. 变更控制管理

不受控制的项目变更，包括目标变更、范围变更、人员变更、环境变更、文档修改等等是对项目质量的重大威胁。

在项目中，将围绕实施方案和计划的维护为核心，对实施方案和计划及其衍生文档进行正规的变更控制管理。

4. 风险与应对措施

不同类型的项目有不同类型的风险，安全项目实施的风险同样有其特殊性。本项目中信息安全等级保护项目实施及安全评估过程中的主要风险管理措施如下。

5. 项目进度的风险

我方项目组将充分考虑各种潜在因素，适当留有余地；任务分解详细度适中，便于考核；在执行过程中，强调项目按进度执行的重要性，在考虑任何问题时，都将保持进度作为先决条件；同时，合理利用赶工及快速跟进等方法，充分利用资源。

6. 项目人力资源的风险

人力资源将是信息安全等级保护项目中最为关键的资源。保证合适的人员以足够的精力参与到项目中来，是项目成功实施的基本保证。我方项目组在此项目实施中将调动公司骨干服务人员和工程技术人员，保证进入到项目中并承担角色的各类人员满足项目要求。同时，保证项目人员对项目的投入程度。将参与本信息安全等级保护项目人员的业绩评估与该项目实施的状况相关联，明确本信息安全等级保护项目是在该阶段项目相关人员最重要的本职工作。

7. 对实际环境存在不熟悉的风险

1）可能存在的风险

对用户现场不熟悉，可能误动设备。

2）规避措施

制定详细的实施方案，经用户同意后方可实施。

配置核查命令在测评师指导下，由甲方指定人员输入，测评师不直接接触被测系统。

放弃工具测试或选择在离线环境下测试，避免影响正线运行系统安全稳定运行。

8. 项目实施中的风险监控

我方项目组采取以下措施对本信息安全等级保护项目实施中的风险进行监控，以防止危及项目成败的风险发生。

1）建立并及时更新项目风险列表及风险排序。项目管理人员随时关注与关键风险相关因素的变化情况，及时决定何时、采用何种风险应对措施；

2）风险应对审计：随时关注风险应对措施（规避、减轻、转移）实施的效果，对残余风险进行评估；

3）建立报告机制，及时将项目中存在的问题反映到项目经理或项目管理层；

4）定期召集项目相关人员召开项目会议，对风险状况进行评估，并通过各方面对项目实施的反馈来发现新风险。

9. 系统备份与恢复措施

为防止在测评过程中出现的异常的情况，所有被测评系统均应在被测评之前作一次完整的系统备份或者关闭正在进行的操作，以便在系统发生灾难后及时恢复。

操作系统类：停止前台的应用操作，制作系统应急盘，对系统信息，注册表，sam 文件，/etc 中的配置文件以及其他含有重要系统配置信息和用户信息的目录和文件进行备份，并应该确保备份的自身安全。

数据库系统类：停止数据库系统的运行，然后对数据库系统进行数据转储，并妥善保护好备份数据。同时对数据库系统的配置信息和用户信息进行备份。

网络应用系统类:停止网络应用服务的运行,对网络应用服务系统及其配置、用户信息、数据库等进行备份。

网络设备类：对网络设备的配置文件进行备份。

桌面系统类：关闭正在运行的前台应用，备份用户信息，用户文档，电子邮件等信息资料。

10. 项目保密措施

我方项目组对客户敏感信息保密非工作常重视,客户敏感信息视为我方项目组最重要商业机密。我方项目组针对项目实施保密措施如下：

- 项目实施测评师与我方项目组签署《保密协议》、《测评师声明》，约束测评师相关行为，同时为了加强员工保密工作和意识，我方项目组制度内部保密制度，并且每年落实保密培训工作。此外，我方项目组所有测评师已经向公安部和省公安厅备案；

- 从技术上，我方项目组使用商业软件加密软件对测评师测评计算机文件进行加密，文件被非法窃取也无法进行解密。同时在项目实施过程中，测评师主机禁止对 Internet 网络访问；

- 在日常工作中，实施人员涉及文件未经项目经理许可禁止相互之间传输敏感资料，与其他人员沟通禁止泄露客户敏感信息；

双方签署项目合同时，我方项目组要求与客户签署《保密协议书》，明确双方保密职责。

网络安全服务方案

为保障新建设的园区公共服务平台、园区运营管理平台、展销综合服务系统、监管指挥平台、跨境电商园区服务平台、应用支撑平台安全稳定运行,避免带“病”

上线情况。在其开发测试时开展安全开发培训，规范开发编码安全；通过代码审计、渗透测试等安全管控措施，提升系统平台自身健壮性和稳定性。系统正式上线前完成安全评估和加固，修复所有高危漏洞后才可正式上线。应对 APP 移动终端，应按照国家相关法律法规开展 APP 客户端、服务端、敏感数据等专项测试、加固。正式交付使用后，由安全运营中心定期或者在重大变更后进行安全性评估并依据评估建议进行加固。

安全代码审计服务

源代码审计，在新系统或新版本上线前，从安全角度对应用系统的所有逻辑路径进行测试，通过分析源代码，充分挖掘代码中存在的安全缺陷、规范性缺陷。找到普通安全测试所无法发现的如二次注入、反序列化、xml 实体注入等安全漏洞。尽可能识别全部潜在的 bug 和漏洞，保证系统本身的安全性，避免因漏洞而直接造成不必要的损失。

服务描述

代码审计（Code Audit）是由具备高技能和高素质的安全服务人员发起，检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。

代码审计服务的目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。信息安全问题时刻都有新的变化，新的攻击方法层出不穷，攻击者攻击的方向越来越侧重于利用软件本身的安全漏洞，例如 SQL 注入漏洞、跨站脚本漏洞、CSRF 漏洞等，这些漏洞主要由不良的软件架构和不安全的编码产生。

开展源代码审计能够降低源代码出现的安全漏洞，构建安全的代码，提高源代码的可靠性，提高应用系统自身安全防护能力。源代码安全检测能够帮助开发人员提高源代码的质量，从底层保障应用系统本身的安全，从早期降低应用系统的开发成本。

代码组件安全检测，对系统开发所采用的第三方组件信息进行采集、维护及时发现组件存在的已知风险，定位受影响的开发项目，避免因引入存在安全风险组件导致的系统性风险发生。

服务内容

代码审计服务主要对象包括并不限于对Windows和Linux系统环境下的以下语言进行审核：java、C、C#、ASP、PHP、JSP、.NET全面测试。

代码审计服务的主要内容包括但不限于：

- OWASP WEB TOP 10漏洞
- Web应用程序的权限架构
- Web应用通信安全
- 数据库的配置规范
- SQL语句的编写规范
- Web应用框架安全性

代码审计服务主要分为四个阶段，包括测试前期准备阶段、检测阶段实施、复测阶段实施以及成果汇报阶段：

- 前期准备阶段

在实施源代码安全检测工作前，负责项目实施的技术人员会和系统负责人对源代码安全检测服务相关的技术细节进行详细沟通。由此确认源代码安全检测的

方案，方案内容主要包括确认的源代码安全检测范围、最终对象、检测要求的时间等内容，系统负责人签署源代码安全检测授权书。

在测试实施之前，会做到让系统负责人对安全测试过程和风险的知晓，使随后的正式测试流程都在系统负责人的控制下。

- 检测实施阶段

在检测实施过程中，测试人员首先进行环境部署，源代码调试，然后使用专业的代码安全检测工具扫描，完成初步的源代码安全检测测试执行工作。

然后由人工的方式进行确认和分析，对安全扫描的结果进行检测和验证，从而对源代码安全漏洞进行定级，测试人员需整理源代码安全检测服务的输出结果并编制源代码安全检测报告，最终提交系统负责人和对报告内容进行沟通。

- 回归测试阶段

在经过初次源代码安全检测报告提交和沟通后，等待系统负责人针对源代码安全检测发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给系统负责人复测报告和对复测结果进行沟通。

- 成果汇报阶段

根据初次源代码安全检测和二次复测结果，整理源代码安全检测服务输出成果，最后汇报项目领导。

序号	服务名称	服务说明	服务对象	服务频率	服务类型

1	代码审计服务	源代码审计：在新系统或新版本上线前，从安全角度对应用系统的所有逻辑路径进行测试，通过分析源代码，充分挖掘代码中存在的安全缺陷、规范性缺陷。找到普通安全测试所无法发现的如二次注入、反序列化、xml 实体注入等安全漏洞。尽可能识别全部潜在的 bug 和漏洞，保证系统本身的安全性，避免因漏洞而直接造成不必要的损失。 组件安全检测：对系统开发所采用的第三方组件信息进行采集、维护及时发现组件存在的已知风险，定位受影响的开发项目，避免因引入存在安全风险组件导致的系统性风险发生。	园区公共服务平台、园区运营管理平台、展销综合服务系统、监管指挥平台、跨境电商园区服务平台、应用支撑平台	一年期内 1 次	远程服务 现场服务

服务成果

交付物资料包括不限于如下内容：

1 《代码审计服务服务方案》

2 《系统源代码缺陷分析报告》

3 《系统源代码缺陷溯源分析报告》

入网安全评估服务

服务概述

网络安全评估是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施；为防范和化解信息安全风险，将风险控制在可接受的水平，从而最大限度地为保障信息安全提供科学依据。

通过开展网络安全评估服务，对信息系统的网络安全、主机安全（WINDOWS、Linux 等操作系统，Oracle 及 SQL Server 等数据库，Windows 终端等）、应用安全（Weblogic、Tomcat 等）、数据安全等开展安全评估，形成网络安全整体分析报告，清晰呈现信息系统的整体信息安全状况。

通过安全评估及时发现网络安全短板，提供风险安全所需的技术服务支持，对主机、网络设备、数据库、中间件、应用系统等从技术等层面提供专业的安全整体规划方案、提供整改建议、并协助实施合理的风险控制措施，将系统的安全风险控制在可接受的范围内，最大程度的防止各类安全事件的产生，保障业务网络与信息系统的安全、稳定运行。

服务内容

针对收集的信息系统资产，需要进行安全评估以发现当前业务系统存在的安全脆弱性及薄弱点。安全评估主要有三个层面：

通过大数据漏洞扫描技术，及时发现计算环境存在的系统、中间件、数据库、大数据平台等应用环境存在的漏洞与各类安全隐患，并持续跟踪漏洞修复情况。

评估系统、数据库、账号配置存在的风险点，包括服务和应用程序设置、操

作系统组件的配置、权限和权利分配、管理规则等，以最小权限原则规范计算环境安全基线。

弱口令专项监测，包括云基础平台弱口令、管理平台弱口令、系统远程登陆弱口令、中间件后台弱口令、数据弱口令、组件弱口令、业务应用弱口令及未授权等。

序号	服务内容	服务说明	服务对象	服务频率	服务类型
1	入网安全评估服务	计算环境漏洞评估：针对业务计算环境，在系统正式上线前，通过大数据漏洞扫描技术，及时发现计算环境存在的系统、中间件、数据库、大数据平台等应用环境存在的漏洞与各类安全隐患，并持续跟踪漏洞修复情况。 计算环境安全基线评估：针对业务计算环境，在系统正式上线前，评估系统、数据库、账号配置存在的风险点，包括服务和应用程序设置、操作系统组件的配置、权限和权利分配、管理规则等，以最小权限原则规范计算环境安全基线。 计算环境弱口令专项检测：针	园区公共服务平台、园区运营管理平台、展销综合服务系统、监管指挥平台、跨境电商园区服务平台、应用支撑平台	一年期内1次	远程服务/现场服务

序号	服务内容	服务说明	服务对象	服务频率	服务类型
		对业务计算环境，在系统正式上线前，开展弱口令专项监测，包括云基础平台弱口令、管理平台弱口令、系统远程登陆弱口令、中间件后台弱口令、数据弱口令、组件弱口令、业务应用弱口令及未授权等。			

服务成果

《系统网络安全评估报告》。

计算环境安全加固服务

计算环境漏洞加固，系统正式上线前，采用系统补丁、版本升级、策略配置等技术手段，对计算环境发现的中高危漏洞进行安全加固。

计算环境安全基线加固，系统正式上线前，修改操作系统安全策略，以提高主机操作系统安全性；启用操作系统安全审计，以追踪操作系统运行状况、登录事件等各类安全事件；修改数据库安全策略，以提高数据库系统安全性；启用数据库安全审计，以追踪数据库登录事件、修改事件等各类安全事件。

业务系统加固整改支撑，系统正式上线前，结合应用系统相关业务流程的实际情况，并在不影响系统稳定运行的前提下，指导优化业务应用安全策略，以提高应用系统的安全性；指导优化及完善应用系统安全审计，以追踪应用系统的登

录事件、修改事件等各类安全事件；对 WEB 应用系统的代码规范安全加固进行指导。

弱口令加固支撑，系统正式上线前，针对发现的业务逻辑层弱口令，根据业务协助制定口令加固方案，并对其身份认证体系，协助优化加固整改。

业务运行环境部署安全组件，系统正式上线前，针对业务系统发布环境，协助安装部署云平台安全组件，包括：云安全终端、EDR、防篡改 Agent 等安全组件。

服务概述

随着信息化的不断推进，业务应用持续增加，基础设施的架构越来越复杂，面临的安全威胁越来越多，信息系统是否能够正常运行直接关系到业务或生产是否能够正常运转维系，信息系统的任何安全问题如果没有及时得到妥善处理都将会导致很大的影响，甚至会造成可怕的政治事件。

当前运行的信息系统或多或少发现存在相应的安全漏洞及隐患，为了有效促进信息系统的安全稳定运行，将依据国家及行业信息安全等级保护的相关标准及法规的要求，从网络安全、主机安全、应用安全和数据安全的角度，结合多种技术手段为信息系统提供信息安全等级保护加固服务，逐步构建动态、完整、高效的信息安全技术体系，提高信息系统的整体技术防护能力，从整体上促进信息系统的安全稳定运行。

服务内容

主要服务内容如下：

（一） 计算环境漏洞加固

系统正式上线前，采用系统补丁、版本升级、策略配置等技术手段，对计算环境发现的中高危漏洞进行安全加固。

（二） 计算环境安全基线加固

系统正式上线前，修改操作系统安全策略，以提高主机操作系统安全性；启用操作系统安全审计，以追踪操作系统运行状况、登录事件等各类安全事件；修改数据库安全策略，以提高数据库系统安全性；启用数据库安全审计，以追踪数据库登录事件、修改事件等各类安全事件。

（三） 业务系统加固整改支撑

系统正式上线前，结合应用系统相关业务流程的实际情况，并在不影响系统稳定运行的前提下，指导优化业务应用安全策略，以提高应用系统的安全性；指导优化及完善应用系统安全审计，以追踪应用系统的登录事件、修改事件等各类安全事件；对 WEB 应用系统的代码规范安全加固进行指导。

（四） 弱口令加固支撑

系统正式上线前，针对发现的业务逻辑层弱口令，根据业务协助制定口令加固方案，并对其身份认证体系，协助优化加固整改。

（五） 业务运行环境部署安全组件

系统正式上线前，针对业务系统发布环境，协助安装部署云平台安全组件，包括：云安全终端、EDR、防篡改 Agent 等安全组件。

序号	服务内容	服务说明	服务对象	服务频率	服务类型

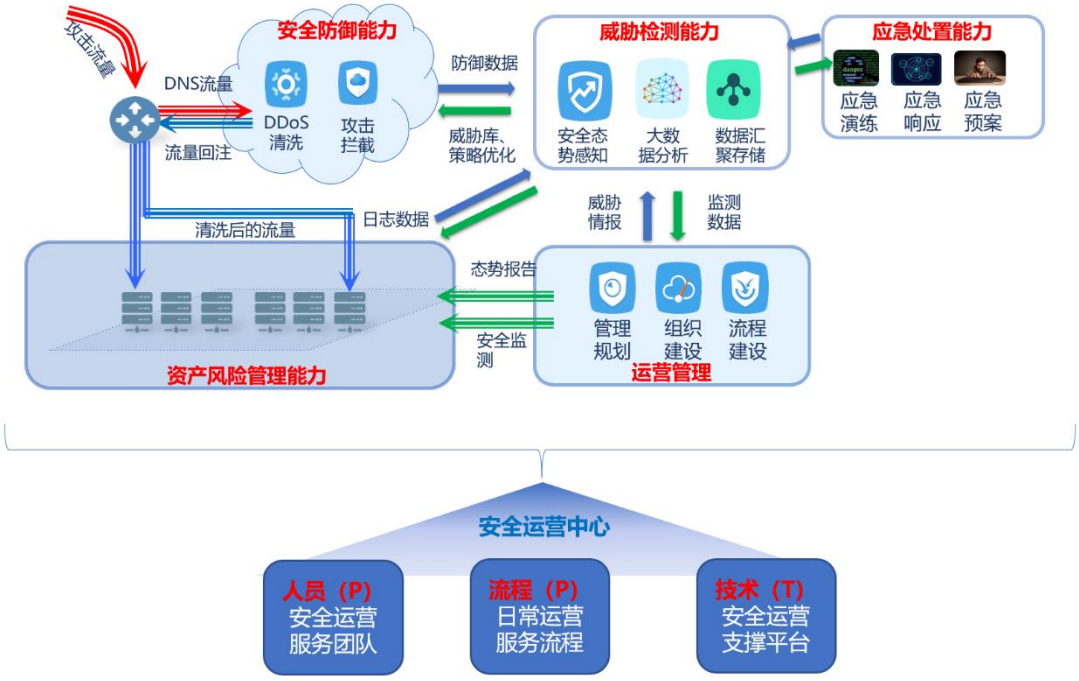
1	安全加固指导服务	计算环境漏洞加固：系统正式上线前，采用系统补丁、版本升级、策略配置等技术手段，对计算环境发现的中高危漏洞进行安全加固。 计算环境安全基线加固：系统正式上线前，修改操作系统安全策略，以提高主机操作系统安全性；启用操作系统安全审计，以追踪操作系统运行状况、登录事件等各类安全事件；修改数据库安全策略，以提高数据库系统安全性；启用数据库安全审计，以追踪数据库登录事件、修改事件等各类安全事件。 业务系统加固整改支撑：系统正式上线前，结合应用系统相关业务流程的实际情况，并在不影响系统稳定运行的前提下，指导优化业务应用安全策略，以提高应用系统的安全性；指导优化及完善应用系统安全审计，以追踪应用系统的	园区公共服务平台、园区运营管理平台、展销综合服务系统、监管指挥平台、跨境电商园区服务平台、应用支撑平台	一年期内1次	现场服务

服务成果

通过对信息系统进行网络安全加固、主机安全加固及应用安全加固指导，以提高信息系统的整体技术防护能力，输出《安全加固指导报告》。

网络安全运营方案

安全运营中心提供覆盖了资产风险管理能力、安全防御能力、威胁检测能力、应急响应能力、运营管理能力等全面的安全管控界面，通过标准化的安全运营流程（SOP）将组织、流程、技术的有机结合，充分利用用户现有基础安全资源，从五大核心攻防对抗域进行重新设计和编排，持续开展常态化、一体化、专业化的安全运维服务，快速提升和迭代优化攻击防御能力、风险检测能力、威胁分析能力、应急响应能力和业务恢复能力，构建整体联动的动态、主动、积极、纵深、精准、整体的安全防御体系，实现全链路的安全管理闭环，最大限度上将风险降低到可接受的范围，有效地保障用户各项业务的可用性和连续性，遵循 PDCA 循环模型（Plan-Do-Check-Action），持续提升和改进用户的安全管理水平，最终实现安全管理的智能化分析、数据化决策、自动化联防、闭环化管理、可视化展示，一站式解决安全建设过程中存在的管理工作无头绪、服务流程不规范、安全决策无数据、安全分析难度大、事件处置不闭环、服务成果不显著等问题。



核心能力	能力域描述	运营团队
资产风险管理能力	绘制资产图谱，发现敏感信息泄露，评估暴露面现状，收敛攻击面，消除资产风险	风险评估组，安全建设与加固组，安全专家组
安全防御能力	构建纵深防御体系，全路径管控风险，并通过技术手段查找控制缺陷，验证防御措施的有效性	安全建设与加固组，安全专家组
威胁检测能力	深度发现未知威胁，结合主动诱捕方式，锁定攻击源，还原攻击链，定位失陷主机	威胁监测组，安全专家组
应急响应能力	安全事件分级分类，及时止损，控制影响，查找原因，消除隐患，恢复业务	应急处置组，安全专家组
运营管理能力	开展安全运维，组织安全培训，评估安全风险，闭环安全管理，通过红蓝对抗验证	管理组，风险评估组，安全专家组

核心能力	能力域描述	运营团队
	安全能力	

资产风险管理能力建设

互联网暴露面监测，借助互联网暴露面监测平台周期对互联网的网站、管理系统、VPN 系统、邮件系统等目标系统的互联网暴露面进行周期性检测，检测包括但不限于子域名、C 段 IP、邮箱、Github 敏感信息、管理后台/控制台、隐藏目录、微信公众号、App 资产、Web 指纹（如开发框架、第三方组件/插件、Waf/云 Waf、可用性状态等）、OS 指纹、DB 指纹、主机端口服务、系统版本及补丁等敏感信息，发现资产风险后，将通过安全运营管理平台进行通报预警、风险处置和风险管理。

互联网区脆弱性管理，针对互联网区资产，检测发现弱点后，安全运营人员将通过资产 CIA 级别、漏洞级别、暴露面等多维度评估弱点的风险值及定义弱点级别和修复次序，开展漏洞通报预警工作，根据资产 CIA 级别、业务特性、漏洞风险级别等维度进行综合考虑，指导安全管理员有序进行风险规避、漏洞修复、安全配置等安全加固工作，以达到最大限度从根源上消除或降低系统的安全风险，提升系统的自身安全防护能力。

政务外网脆弱性管理，针对互联网区资产，检测发现弱点后，安全运营人员将通过资产 CIA 级别、漏洞级别、暴露面等多维度评估弱点的风险值及定义弱点级别和修复次序，开展漏洞通报预警工作，根据资产 CIA 级别、业务特性、漏洞风险级别等维度进行综合考虑，指导安全管理员有序进行风险规避、漏洞修复、安全配置等安全加固工作，以达到最大限度从根源上消除或降低系统的安全风险，提升系统的自身安全防护能力。

安全防御能力建设

安全域规划，通过现场调研、报告整理、工具测试等技术手段，梳理并分析业务系统的访问关系、数据流向、防护措施、传输安全、隐私安全，对现有网络安全保障体系进行审视，从攻击者视角全面评估业务系统的安全威胁，找到存在的安全能力建设差距，补全安全建设的防御短板，指导用户通过基于最小权限原则通过架构设计、分区分域、分层防御、深度检测、访问控制、人员安全、管理安全、数据安全等手段构建纵深、动态、联动的防御体系。根据业务发展周期性开展优化更新。

互联网边界策略优化，根据提供安全监测和防护策略信息，梳理互联网边界防火墙、VPN、堡垒机、WAF 等安全设备的策略配置，检查项包括策略控制粒度、特征库升级、帐号口令、日志记录等，检验策略是否遵循“最小原则”，关闭不必要的服务和端口。

安全域边界策略优化，根据提供安全监测和防护策略信息，梳理安全域边界防火墙、VPN、堡垒机、WAF 等安全设备的策略配置，检查项包括策略控制粒度、特征库升级、帐号口令、日志记录等，检验策略是否遵循“最小原则”，关闭不必要的服务和端口。

专线接入边界策略优化，根据提供安全监测和防护策略信息，梳理专线接入边界防火墙、VPN、堡垒机、WAF 等安全设备的策略配置，检查项包括策略控制粒度、特征库升级、帐号口令、日志记录等，检验策略是否遵循“最小原则”，关闭不必要的服务和端口。

边界设备运行维护，期对安全设备、安全产品的软件版本、策略版本进行备份和更新，提升安全设备自身安全的同时，最大限度上发挥安全设备的安全能力。在安全设备版本维护过程中，所有的服务记录可通过安全运营管理平台进行工单

管理及事后追责追溯。

区域边界防御能力评估，通过模拟黑客攻击的手法，对目标实战检查区域边界防御能力情况，是即没有源代码和服务器权限的情况下，从互联网资产边界入侵到内网资产（由外到内）、内网边缘资产漫游入侵内网核心资产（由内到内）、在内网建立外网连接的隐秘隧道（由内到外）等方面进行全方位安全渗透。

区域边界访问权限评估，采用灰盒测试的模式，对区域网络内部网络的访问控制策略进行识别和梳理，分析在不同权限场景下访问控制策略的有效性和合理性，发现现有的访问控制策略存在的不足与风险点。通过渗透测试等手段充分发掘访问控制策略的缺陷造成的威胁深度，降低因网络权限配置不合理引起的内部网络风险。

威胁检测能力建设

网络威胁检测分析，借助威胁建模、机器学习、AI 技术发现主机失陷后的攻击者发起的安全事件，如横向漫游攻击、非法外联、非法内联、数据越权访问、拖库等，通过钉钉、短信、邮件、语音电话、安全运营管理平台发布等方式将安全事件告警通知运营处置人员及用户相关责任人。

数据泄露分析，基于全流量大数据分析，识别内部员是否合法访问内部数据的权限，因其账号被冒用/盗用/借用或主观恶意操作的行为，定位和发现数据泄露事件，避免造成检测安全欺诈、敏感数据泄露、敏感数据非法访问等新型安全问题。

系统运行环境威胁分析，对系统运行环境开展：APT、僵尸、木马、蠕虫、病毒分析排查；发现网络中存在的高级安全威胁并查杀。 查找 web 站点中以各种形式存在的 webshell，使用 webshell 专杀工具对全站进行排查。

系统失陷检测，安全运营管理平台借助威胁建模、机器学习、AI 技术发现主机失陷后的攻击者发起的安全事件，如横向漫游攻击、非法外联、非法内联、数据越权访问、拖库等，通过钉钉、短信、邮件、语音电话、安全运营管理平台发布等方式将安全事件告警通知运营处置人员及用户相关责任人。

应急响应能力建设

安全应急预案编制，参照国家标准和行业最佳实践，并根据数据中心业务场景制定分类分级的应急处置预案，建立和保障应急处置架构，提升应急处置的沟通效率，明确应急处置的环节、步骤、工具、方法及工作岗位，并定期组织应急预案的宣贯、学习、考核，不定期开展流程执行的审计，以便不断迭代优化应急预案，提升应急预案的适用性和科学性。

安全应急演练，根据场景和安全现状，设计相应应急演练方案，组织安全应急演练活动，检验应急预案的有效性，验证相关组织和人员应对突发安全事件的组织指挥能力和应急处置能力，保证各项应急指挥调度工作迅速、高效、有序地进行，满足突发情况下网络与信息系统运行保障和故障恢复的需要，确保信息系统安全运行。在安全应演练服务过程中，所有的应急预案、演练方案、演练成果可通过安全运营管理平台进行管理、检索、查阅、归档等操作。

应急响应处置，由丰富安全攻防经验、分析经验的安全专家组成本地专属 7*24 小时安全应急团队，对发生的信息安全事件进行应急处置工作，配置应急处置技术工作，分析总结信息安全事件成因，还原攻击链，定位安全漏洞，锁定攻击者及攻击手法，开展补救和反制措施，消除安全隐患，控制安全风险。

运营管理能力建设

安全规划优化，基于风险评估结果和监管合规要求所提出的信息安全保障体系设计规划需求，为数据中心运营方提供专业咨询服务，立足于数据中心信息处理设施和信息安全管理现状，依据信息安全相关的国际国内标准规范、协助数据中心建立信息安全保障的建设目标，选择和组合信息安全控制措施，完成信息安全保障体系架构设计，并合理规划信息安全保障体系的建设步骤和资源投入，最终达成满足合法合规要求、有序提升信息安全风险管控能力、保障信息系统安全运行的目标。

安全意识培训，对数据中心工作人员、城市运营中心人员、上云委办厅局人员开展网络安全意识培训，提升全员网络安全素质，降低由人为因素导致的网络安全事件发生。

流程规范管理编排，通过成立流程规范梳理及制定小组，参考国家、地方和行业标准，结合用户安全现状和行业安全建设最佳实践，制定和完善相关标准、流程和制度，形成科技有效的安全运行机制，实现安全管理依法合规、有章可循，安全工作可度量，安全效果可验证。在安全管理过程中，所有的交付成果可通过安全运营管理平台进行管理、检索、查阅、归档等操作。

网络安全制度机制编排，针对网络安全制度管理场景，基于安全运营平台，根据数据中心实际业务情况，编排工作机制，落地责任到人，实行基于平台的全方位监管、工作扭转机制，实现高效协同、人机共智的网络安全运营能力。

数据安全制度机制编排，针对数据安全管理场景，基于安全运营平台，根据数据中心实际业务情况，编排工作机制，落地责任到人，实行基于平台的全方位监管、工作扭转机制，实现高效协同、人机共智的网络安全运营能力。

系统上线安全评估制度编排，针对系统上线安全评估场景，基于安全运营平

台，根据数据中心实际业务情况，编排工作机制，落地责任到人，实行基于平台的全方位监管、工作扭转机制，实现高效协同、人机共智的网络安全运营能力。

安全运营团队

数据中心网络安全信息化和网络安全领导小组为决策层，中心管理团队、安全专家、项目经理为管理层，各单位安全运营支撑团队下分风险评估组、威胁监测组、应急处置组、安全合规组、安全情报组、安全建设组等负责安全运营工作的具体执行。

决策层、管理层与执行层应做到信息共享，决策层、管理层对于执行层有指挥职权，双方应共同配合做好网络安全运营工作。安全专家组为整体全线网络安全工作提供技术支撑，辅助决策层、管理层开展网络安全运营体系规划建设、重大决策过程中提出专业的建议，指导执行层高效开展安全运营工作，跟进最新技术发展趋势，攻关解决重大、疑难技术难题。

岗位职责	岗位描述	人员规划
决策层	网络安全运营体系决策层为信息化和网络安全领导小组，其职责同时聚焦安全运营整体战略和安全运营重大决策的制定。	由信息化负责人牵头
管理层	工作职责为聚焦推动安全运营体系建设和安全运营整体的指挥、调度、协调工作，参与安全运营重大决策，保障安全运营工作顺利开展。	信息化小组成员担任 安全运营供应商提供安全管理经理 1 名，常驻
安全专家组	工作职责为协助管理层在安全决策、指挥、	安全运营供应商

岗位职责		岗位描述	人员规划
		调度、执行时提供技术支持。	提供安全专家组团队（4 人，非常驻）
执行层	风险评估组	负责探查全网资产并进行弱点检测，从网络、主机、系统、策略、用户等方面对网络安全现状进行评估，并指导各安全响应组进行加固处置。	安全运营供应商提供（1 人，非常驻）
	威胁监测组	负责对全网的安全威胁进行集中式分析研判，给出专业的处置建议，指导安全响应组进行加固处置。	安全运营供应商提供（1 人，常驻）
	应急处置组	负责定期开展应急演练工作，一旦发生网络安全事件，进行应急快速恢复，并对事件进行审计取证。	安全运营供应商提供（1 人，常驻）
	安全情报组	负责收集与企业网络安全相关的威胁情报，根据网络安全实际情况进行场景的推演判定，实现风险态势预测和通报。	安全运营供应商提供（1 人，非常驻）
	建设与加固组	负责承建安全建设、安全设备维护和安全策略优化及安全加固处置等工作。	安全运营供应商提供（1 人，常驻）

。

利旧方案

硬件设备利旧清单：

现有硬件部分			
序号	硬件设备名称	数量	是否利旧
1	老城园区监控数量	384	利旧
2	金盘园区监控数量	18	
3	路由器	8	
4	交换机	163	
5	防火墙（及网络安全设备）	11	
6	服务器	12	
7	网管专用电脑	2	
8	网络流量控制与认证管理设备	1	
9	入侵检测	2	
10	网管软件	2	
11	磁盘阵列	1	
12	磁带库	1	
13	磁带备份管理软件	1	
14	安全隔离与信息交换系统	1	

业务应用系统利旧清单：

现有业务应用部分			
序	种类	系统名称	是否利旧

号			
1	海关监管	智能卡口系统	无法利旧，建议更新
2	业务管理	关务辅助管理系统	
3	数据交换	数据交换三级节点	
4	门户网站	综保区门户网站	
5	网上办公	党政集成办公系统	上级管理部门统一建设，可以利旧
6	网上申报	海口市联网直报统计系统	

部署方案

服务器存储部署方案

本地云平台资源池采用分布式超融合架构，通过分布式超融合架构充分保障业务的稳定性，方便云资源池快速扩容部署，简化管理，降低建设成本。

在园区核心交换机侧串联部署等保安全接入设备，如防火墙、上网行为管理等；在核心交换机侧旁挂安全管理区，部署态势感知、堡垒机、VPN 等安全设备。

网络安全部署方案

根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的网段或 VLAN。保存有重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分区域。

根据海口市综合保税区整体信息系统实际情况，整体网络架构划分为互联网接入区、5G 接入网络区、核心交换区、电子政务网络接入区（含电子政务外网接入和电子政务外网互联网数据专线接入）、服务器区（云平台和物理集群区）、终端接入区、海口园区接入区、空港园区接入区、海关接入区和安全管理区。

电子政务网互联区边界防护新增安全技术措施如下：

在电子政务网互联区部署一台专线防火墙，通过防火墙安全域划分提供基础安全隔离，把安全信任网络和非安全网络进行隔离；并提供从数据链路层、网络层到传输层的安全，包括 ARP 欺骗、扫描攻击、多种畸形报文攻击、端口过滤、抗 IP 分片攻击和防病毒等基础防御，同时应用 NAT 隐藏数据中心网络拓扑结构。

在电子政务网政务外网区部署一台网闸，通过网闸将政务外网区与澄迈园区做物理隔离，确保数据交换安全合规。

外联区、安全管理区、物联网区、办公接入区边界防护新增安全技术措施如下：

在外联区部署两台园区接入防火墙，将澄迈园区与海口园区、空港园区、海关园区做逻辑隔离，通过策略放通相关的合规流量；在物联网区、办公接入区各部署两台防火墙，将物联网区与核心交换区、办公接入区与核心交换区做逻辑隔离，通过策略放通相关的合规流量；在安全管理区与核心交换区之间部署两台防火墙，通过策略放通相关的合规流量。以上安全区域边界通过防火墙安全域划分提供基础安全隔离，把安全信任网络和非安全网络进行隔离；并提供从数据链路

层、网络层到传输层的安全，包括 ARP 欺骗、扫描攻击、多种畸形报文攻击、端口过滤、抗 IP 分片攻击和防病毒等基础防御，同时应用 NAT 隐藏数据中心网络拓扑结构。

在外联区部署一台网闸，通过网闸将澄迈园区与海关接入区做物理隔离，确保数据交换安全合规。

数据中心区边界防护新增安全技术措施如下：

在数据中心区边界部署两台防火墙，将数据中心区与核心交换区做逻辑隔离，通过策略放通相关的合规流量。

在数据中心区边界部署两台 web 应用防火墙，可以有效地缓解网站及 Web 应用系统面临如 OWASP TOP 10 中定义的常见威胁；可以快速地应对恶意攻击者对 Web 业务带来的冲击，让网站免遭 Web 攻击侵扰并对网站代码进行合理加固。

互联网出口区边界防护新增安全技术措施如下：

在互联网出口区部署两台防火墙和两台上网行为管理，将互联网与澄迈园区做逻辑隔离，通过策略放通相关的合规流量，对内网业务系统形成有效的安全防护，以满足外网对业务系统的访问；上网行为管理主要是针对内网终端对外访问的行为有效的控制，将不合规连接外网的异常行为进行阻断，以提升内网终端设备的安全性。

物联网区、海口园区接入区、空港园区接入区网络安全新增安全技术措施如下：

在老城园区核心交换机、海口园区核心交换机、空港园区核心交换机处各部署一台流量探针和一台物联网终端准入设备，通过流量探针检测、筛查出网络流量当中是否存在威胁攻击的行为，将检测数据推送到态势感知平台做综合的分析研判，从而发现内网整体的攻击态势；终端准入设备则是通过 IP、MAC 绑定、打

标签等方式判断前端接入节点是否能安全合规的接入到内网当中，从而规避一些非法终端接入内网，对内网造成网络威胁。

安全管理区新增安全技术措施如下：

在安全管理区部署一套态势感知平台结合智能检测算法可进行多维度海量数据关联分析，主动实时的发现各类安全威胁事件，还原出整个 APT 攻击链攻击行为。同时可采集和存储多类网络信息数据，帮助用户在发现威胁后调查取证以及处置问责。以发现威胁、阻断威胁、取证、溯源、响应、处置，完成全流程威胁事件闭环。

部署一套运维审计系统，通过集中管理、监控与审计所有运维人员的操作行为，有效降低网络设备、服务器、数据库、业务系统等资源的内部运维风险，完善 IT 管理体系，同时满足相关法规、标准要求。

部署一套漏洞扫描系统，智能主机服务发现，智能化爬虫和 SQL 注入状态检测等技术，并以智能便利规则库为基础，深度主机服务探测、Web 智能化爬虫、SQL 注入状态检测、主机配置检查以及弱口令检查等方式相结合的技术，实现 Web 漏洞扫描、系统漏洞扫描、数据库漏洞扫描、基线安全检查与口令猜解五大扫描能力，深度掌握漏洞风险评估。

部署一套攻击预警平台，汇集流量传感器、文件威胁鉴定器、邮件告警、等多种告警数据，基于多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁情报；同时结合部署在客户本地的软、硬件设备，能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源；支持运用 SOAR 编排技术，实现对确定的威胁进行多种类型的响应处置，真正实现监测预警、威胁检测、溯源分析和响应处置的攻击预警平台。

部署一套主机安全系统，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，通过防病毒、漏洞管理、运维管控、基线合规检查、网络准入、终端检测与响应（EDR）、终端数据防泄漏（EDLP）等安全功能，为业务终端提供体系化安全防护能力。

部署一套日志审计系统，作为一个统一日志收集与分析平台，能够实时不间断地将企业和组织中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合安全审计。系统能够实时地对采集到的不同类型的日志和事件信息进行标准化（归一化）和实时关联分析，通过统一的仪表板进行实时动态、可视化的呈现，协助安全管理人员迅速准确地识别安全事故，消除了管理员在多个控制台之间来回切换的烦恼，同时提高工作效率，降低工作强度。

部署一套 VPN 系统，可以保障企业移动信息化安全，在满足客户的身份认证、传输加密、访问授权、日志审计等多种基础安全需求基础上，更加保护了移动终端设备的接入安全、移动应用自身安全、移动应用数据安全。

部署一套数据库审计系统，对审计和事务日志进行审查，从而跟踪各种对数据库操作的行为，主要记录对数据库的操作、对数据库的改变、执行该项操作的人以及其他的属性。这些数据被记录到数据库审计与防护系统独立的平台中，并且具备较高的准确性和完整性。针对数据库活动或状态进行取证检查时，审计可以准确的反馈数据库的各种操作历史，对我们分析数据库的各类正常、异常、违规操作提供证据。

运行维护方案

运行管理单位

运行管理分为三种模式：

第一种模式是由业主单位自行成立运维机构对系统平台相关的软硬件进行运行维护。此种模式的优点是安全程度高、人员成本低，缺点是对人员专业技术水平要求高、人员数量需求比较大，当前业主人员组织难以满足；

第二种模式聘请专业第三方企业进行系统平台软硬件的运维工作，第三方企业主要负责区域内所有设备及系统的正常运行维护工作。此种模式的优点是专业性较高，缺点是运维资金成本高；

第三种模式是业主单位负责已建系统的运维工作，第三方企业负责新建系统的运维工作。此种模式既降低了运维成本，同时又保障了系统运维的专业性。 通过对三种模式的衡量分析，我们建议业主单位选择第三种模式进行运维。

一、本项目选择运维管理方式：自运维；

二、运维管理单位名称：智慧口岸运营服务单位；

项目建成后，智慧口岸运营服务单位协同项目建设单位共同负责运行管理，全面负责系统的运行、维护和组织管理；协调系统内部有关系统运行的工作。

项目的免费运维期以通过业主组织的专家综合验收为起始时间，通过最终验收后，即进入系统的运维期。从这个阶段开始，系统正式进入使用阶段，承担起运载各项业务的重任，因而这一阶段将成为整个系统维护的工作中心和重点。

运维管理规范

为了使系统运营始终处于一个最佳状态，有必要制作一套完整的系统运营管

理指南向各组织成员派发，让他们在实际业务操作过程中做到心中有数。作为系统运营最重要的参考资料，指南不仅囊括了运营管理方面的帮助内容，还包括诸如各类系统设计书、试运营计划书与结果报告、各种教材以及与系统软、硬件的使用手册等丰富的内容。以期望在这些运营管理指南的帮助下系统能够实现不间断安全稳定运行目标。

1、针对各个系统分别提出维修响应时间、故障排除时间、人员组织、交通工具、通信工具、检测仪器、维修设备以及长期技术支持等方面的要求。

2、提出定期检修计划、定期清洁卫生计划、系统设备运行状态记录制度。

3、针对本单位工作的行业特殊性提出安全保卫工作制度。

4、提出设备及设施被盗、被毁或其他不可抗拒力造成损坏的报案报告制度。

5、提出技术文件等文档资料的管理制度。

通过执行管理制度，可以明确系统管理员的工作内容和工作职责，使系统维护工作日常化、制度化。对操作系统、数据库系统、应用系统和网络设备设置权限，阻止非授权用户读取、修改、破坏或窃取数据。由于系统中包含了大量的基础数据和业务数据，不同用户在系统中操作的内容不同，所以要通过系统用户管理，对不同用户对数据的操作方式进行严格控制。另外，还要利用操作系统、数据库、网络设备等提供的安全管理功能，配置合适的系统安全策略。同时，需要制定有效的备份制度管理，及时备份各类基础数据和业务数据。

运维服务内容

本期项目通过验收后，实施单位至少提供两年信息化运维服务，提供的运维服务内容包括日常管理、定期检查、巡检保养、服务咨询、应急管理、培训管理、运维服务报告、客户满意度调查。

1、日常管理

为软件平台建立软件定期定时备份计划，指定数名管理人员，定期定时查看计划备份的数据信息是否已经备份，并对查看的情况通过书面的形式记录案，定期巡视设备运行状况。

2、定期检查

组织专职人员对设备、系统进行检查；形成定期检查。对重要设备、系统进行重点、详细检查；按各项指进行检查，做好记录。对各设备、系统填写运行情况表，形成定期报告。对表、报告进行归档，形成历史记录。

3、巡检保养

实施单位应安排定期对系统各组成部分进行定期巡检和定期抽检服务，以确认所有设备及系统工作正常。在每次进行系统巡检之前实施单位应向采购人提交本次巡检的内容、人员构成和日程安排的书面请求，在采购人批准后，严格按照提交的巡检内容、构成人员和日程安排对系统进行巡检。在系统巡检完毕后的2-4 个工作日内实施单位应向采购人提交相关表格及书面报告，并须经采购人签字确认。如果在巡检的过程中发现系统存在隐患，实施单位应向采购人提交系统隐患情况分析、解决方案等文档作为系统巡检报告的附件，并按照采购人要求及时对发现的隐患进行排除。

4、服务咨询

(1)实施单位应设立专门的服务咨询中心，接受系统故障申告、使用帮助

要求、业务和技术咨询、服务投诉等。服务咨询中心应 7x24 小时全天候正常运行，提供的 7*24 小时热线电话，配备足够的咨询人员或技术工程师，热线电话的接通率达到 90%以上(报障指引如下)。在热线电话发生故障的情况下，实施单位提供接口人作为应急备份联系人。

实施单位提供的热线电话如发生变更，需提前 15 个工作日以书面形式告知采购人，经采购人同意后方可更换；实施单位提供的接口人及联系方式如发生变更，需提前 5 个工作日以书面形式告知采购人，经采购人同意后方可更换。

(2)实施单位应提供包括远程技术指导、现场技术支持等在内的多种有效的咨询服务；采购人如有需要，实施单位还应提供工程师常驻服务，即派出与采购人系统技术要求相适应的工程师常驻采购人系统设施所在地，为采购人提供全日制的相关运维服务工作，以保证系统保持良好的工作状态和实现最佳的运行效率。

5、应急管理

成立应急管理小组，负责制定应急方案、方案实施及方案评估重点做好以下已知的应急方案：断电应急，在电供应充足的情况下保证 UPS 充满电，应对突然停电，保证数据库正常关闭；火灾应急，做好消防设施，争取时间，保证数据库正常关闭；数据库瘫痪，平时做好冷热备份。条件允许的情况下，让数据库运行在归档模式下。这样数据库可以恢复到某个时间点。

6、培训管理

根据政策调整和业务调整制定培训计划。定期组织本系统技术人员进行软件硬件安装、操作及维护培训，以提高本系统的技术水平。

组织所有业务人员进行新政策、业务系统进行培训，提高业务人员的业务水平，计算机操作水平。每次培训后，对参与培训的人进行考核，评估培训效果。

7、运维服务报告

在整个运维服务周期内，实施单位应与采购人建立完善的沟通协调机制，实施单位应及时提供运维服务的各种报告，包括重大故障维修报告、每月故障总结报告、每季度的设备和系统管理报告、每季度的系统维护总结报告，有针对性的系统优化方案报告等。此外采购人还可根据实际情况需要，要求实施单位提交每

日运维服务日志或就特定事件提交说明报告。

实施单位应提供各种设备管理的原始数据(包括设备故障数据)，接受采购人或采购人委托的第三方的独立检查。实施单位应保证系统所有设备维护数据的真实，没有被篡改或删除。采购人及其委托方可以随时检查、使用实施单位的设备管理系统获取设备管理信息。

8、客户满意度调查

实施单位应至少每季度针对包括故障受理、故障处理、技术支持等在内的、涉及到运维服务的各方面内容进行满意度调查，调查对象应包括系统涉及的采购人各级单位，并在每季度结束后的 10 个工作日内将调查结果报送采购人。满意度调查包括上门走访和电话故障回访两个部分。每季度到各个监控中心走访 1 次，电话故障回访按照故障总量的 3%进行。

运维服务提供方式

表 5- 13 运维提供方式

项目组职位	运维时间（现场）	运维地点	应急响应时间（现场）	电话响应时间	短信响应时间	邮件响应时间
值守人员	每周 7*24 小时日常工作	机房、监控室、值班室	10 分钟	1 分钟内	5 分钟内	2 小时内
承建商技术服务工程师	每周 7*24 小时待命	机房、监控室、值班室	4 小时内到现场	10 分钟内	20 分钟内	24 小时内

应急措施

1、突发事件的前提条件

系统运维服务小组可从以下途径得知故障的发生：

1) 运维服务中心通过网管告警发现故障；

2) 维护站点通过维护巡检发现故障；

3)用户发现故障，报给呼叫中心；

4)驻场工程师发现故障。

2、突发事件的应急流程

1) 报障受理

监控系统运维服务小组得知系统故障发生后，立即响应，并向报障人或单位详细了解系统故障情况。

2) 信息研判

运维服务小组根据了解到的系统故障情况进行分析判断，以确定采用一般故障处理流程还是立即启动系统突发故障应急处理预案。

3) 预案启动

如需启动应急预案，则立刻通知系统突发故障应急领导小组，由领导小组启动应急预案，对系统突发故障应急事件进行全面管控处理。

4) 资源确认

系统突发故障应急预案启动后，首先是根据现场突发故障实际状况、紧急程度、技术难度、备品备件等情况对相关资源(主要是参与人员)依据经验进行调度和确认，主要有公司技术支持人员、相关厂家技术支持人员。

5) 预案执行

按照既定的预案进行突发故障抢修，如遇到问题及时向系统突发故障应急领

导小组汇报。

6) 预案终止

预案的终止时间由故障现场技术人员根据现场的实际进展情况，在与用户单位有关部门协调后报系统突发故障应急领导小组决定。

7)结果上报

预案中止后，相关预案参与人员将整个事件过程中的经验和教训，修改、完善事件应急预案。然后集中上报至系统突发故障应急领导小组。

3、突发事件的职责分工

1) 故障应急领导小组:掌握系统故障发生情况，监督预案执行。

2)运行维护小组:受理故障，并对故障进行信息研判。

3) 公司技术支持人员、相关厂家技术支持人员:配合执行预案。

4、突发事件的应急策略

1) 居安思危，预防为主。实行突发事件统一管理、统一指挥、各级负责的原则。

2) 统一领导，分级负责，全面规划、及时发现、快速反应、措施果断的原则对突发事件进行分级管理，并按照事件级别迅速上报相关领导和责任人。

3) 制度规范，加强管理，使突发应急的工作规范事件化、制度化。

4) 快速反应，协同应对。当突发事件发生时，立即按应急预案，投入应急工作；加强各个部门配合协作。形成统一指挥、反应灵敏、功能齐全、协调有序、运转高效的应急管理机制。

5) 主动报告原则:当突发事件发生后，要及时报告应急预案实施情况。

运维服务质量与考核

质量计划编制

质量计划编制就是确定与项目相关的质量标准并决定达到标准的方法。在项目的每个阶段，针对不同的项目内容，制定相应的质量标准。

质量保证

质量保证是在质量体系中实施的全部有计划、有系统的活动，以提供满足项目相关标准的信心。在本项目中质量保证的提供对象是项目管理班子以及项目的专家验收评审班子。质量保证的一个循环过程是：质量保证的输入、质量保证的方法和技术、质量保证的输出。

1. 质量保证的输入是指将质量管理计划、质量控制测量结果、各功能的操作定义以文字的方式提交。

2. 质量保证的方法和技术是指根据质量保证的输入实施并评审质量保证的方法和技术。

3. 质量保证的输出是指：对质量保证的方法和技术评审结果进行审核，并由项目管理班子提供质量提高的方法和途径，并对先前的方法和技术进行改进。

质量控制

质量控制是监控具体项目结果以决定是否符合相关的质量标准以及确定排除不满意结果的方法。质量控制贯穿于整个项目的全过程。在本项目中，项目的质量控制采用的方法主要有：

检查：在项目运维的各个阶段普遍使用检查的方法以确定结果是否符合需求。

控制图:用来监控任何类型的输出变量,也用于监控系统成本和进度的偏差、项目文档中的错误或其他管理结果。

帕雷托图：帕雷托图是一种按发生频率排序的直方图，显示了可识别原因的种类和所造成的结果的数量。该图可用于指导纠正项目团队采取的错误措施。

统计抽样：统计抽样的方法能够经常用于系统质量控制的过程，同时可以有效地降低质量控制成本。同时，该方法要求项目管理班子熟悉各种抽样技术。

流程图：在质量控制中流程图用来帮助分析问题的产生原因。

运维服务工作考核

建设单位会每个季度对运维单位进行一次考核，一年四次。考核内容分两个部分：一是硬性指标；二是客户评价。对合格的运维单位继续提供服务，对不合格的单位则通知整改，连续两次考核不通过的则终止合同。

考核输入文档：维护单位提供的月度总结、信息中心的故障记录表、用户满意度记录。

考核输出文档：季度考核表。

表 5- 15 系统维护工作月度总结报告

定性工作内容		
巡检内容	巡检次数	发现故障次数
应用系统巡检		
数据库巡检		
服务器及存储设备巡检		
日常备份巡检		

故障处理		
日期	巡检故障	处理情况
突发性工作内容		
次数		
日期	突发性原因	处理情况

表格 5- 16 故障记录表

日期	
发现人	
联系方式	
故障开始时间	
故障描述	
故障等级	
维护单位响应时间	

故障处理时间	
故障原因	
故障处理	
事后分析	
改进意见	

软件开发清单

软件开发清单

序号	名　称	子　项	模　块
1	园区公共服务平台	园区统一门户	首页（用户注册）
2			首页（系统集成）
3			首页（单点登录）
4			园区概况-园区机构（机构概况）
5			园区概况-园区机构（领导信息）
6			园区概况-园区机构（机构职能）
7			园区概况-园区企业介绍
8			园区概况-基础设施介绍
9			园区概况-园区优势介绍
10			园区概况-优惠政策介绍
11			园区概况-高效率审批
12			我要投资-招商引资（入区流程）

13			我要投资-招商引资（产业定位）
14			我要投资-招商引资（招商方向）
15			我要投资-招商引资（比较发展）
16			我要咨询-在线交流（常见问题）
17			我要咨询-在线交流（留言查询）
18			我要咨询-互动交流（提问管理）
19			我要投诉-在线投诉
20			我要投诉-投诉管理
21			案例展示
22			园区动态（园区新闻）
23			园区动态（国务院新闻）
24			园区动态（省府新闻）
25			园区动态（媒体报道）
26			专题解读（最新解读）
27			专题解读（回应关切）
28			专题解读（新闻发布会）
29			信息公开
30			数说园区（企业注册数据采集）
31			数说园区（跨境申报数据采集）
32			数说园区（营业收入数据采集）
33			数说园区(进出口货值数据采集)
34			数说园区（工业总产值和税收收入数据采集）

35			政务服务（人才服务）
36			政务服务（党建党史）
37			政务服务（投资服务）
38			联系我们
39			系统管理-文章管理
40			系统管理-友链管理
41			系统管理-栏目管理
42			系统管理-关于我们
43			系统管理-园区跨境溯源查询
44			系统管理-资源管理
45			集成对接-系统集成（已规划业务系统）
46			集成对接-系统集成（预留业务系统集成）
47			集成对接-政务服务对接
48			集成对接-第三方服务对接
49		智能园区服务系统	数字招商管理子系统-系统首页（导航栏）
50			数字招商管理子系统-系统首页（招商热点）
51			数字招商管理子系统-系统首页（政策文件）
52			数字招商管理子系统-系统首页

			（招商服务）
53			数字招商管理子系统-系统首页（招商案例）
54			数字招商管理子系统-系统首页（在线互动）
55			数字招商管理子系统-待办事项（待我办理）
56			数字招商管理子系统-待办事项（我已办理）
57			数字招商管理子系统-待办事项（招商审核）
58			数字招商管理子系统-待办事项（协调处理）
59			数字招商管理子系统-招商项目管理（项目信息审核）
60			数字招商管理子系统-招商项目管理（重新修改审核）
61			数字招商管理子系统-招商项目管理（到资凭证审核）
62			数字招商管理子系统-招商项目管理（协调事项处理）
63			数字招商管理子系统-招商项目展示（招商项目查询）

64			数字招商管理子系统-招商项目展示（招商项目列表）
65			数字招商管理子系统-招商项目展示（招商项目详情）
66			数字招商管理子系统-招商项目展示（个人收藏）
67			数字招商管理子系统-招商统计报表（项目进展报表）
68			数字招商管理子系统-招商统计报表（项目质量报表）
69			数字招商管理子系统-招商统计报表（新开工招商项目一览表）
70			数字招商管理子系统-招商统计报表（新签约招商项目一览表）
71			数字招商管理子系统-招商统计报表（新投产招商项目一览表）
72			数字招商管理子系统-招商统计报表（新落地招商项目一览表）
73			数字招商管理子系统-招商统计报表（双促项目报表）
74			数字招商管理子系统-产业链招商（全国企业库）
75			数字招商管理子系统-产业链招

			商（智能推荐）
76			数字招商管理子系统-产业链招商（园区产业链全景展示）
77			数字招商管理子系统-产业链招商（企业画像）
78			数字招商管理子系统-产业服务（财税审计服务）
79			数字招商管理子系统-产业服务（项目申报服务）
80			数字招商管理子系统-产业服务（申报管理服务）
81			数字招商管理子系统-产业服务（政策解读服务）
82			数字招商管理子系统-产业服务（知识产权服务）
83			数字招商管理子系统-产业服务（推广培训活动）
84			园区客服管理子系统-客户资料自动弹出
85			园区客服管理子系统-自动话务分配
86			园区客服管理子系统-电话排队管理

87			园区客服管理子系统-电话录音
88			园区客服管理子系统-智能话务管理
89			园区客服管理子系统-通话详细报告
90			园区客服管理子系统-工作流程
91			园区客服管理子系统-报表统计
92			园区客服管理子系统-CRM 客户管理
93			会议管理子系统-多种移动终端接入
94			会议管理子系统-会议管理
95			会议管理子系统-会议录制和回放
96			会议管理子系统-电子白板协同操作
97			会议管理子系统-桌面及程序共享
98			会议管理子系统-同步播放多媒体文件
99			会议管理子系统-文件分发
100			园区服务子系统-资产管理
101			园区服务子系统-停车场管理

102			园区服务子系统-企业经营情况申报
103			园区服务子系统-投诉建议
104			园区服务子系统-综合查询
105			园区服务子系统-统计分析
106			园区服务子系统-设施设备
107			园区服务子系统-政务服务
108			园区服务子系统-租赁管理
109			园区服务子系统-营销管理
110			园区服务子系统-物业管理
111		访客管理系统	访客管理子系统—访客人员预约
112			访客管理子系统—二代身份证阅读
113			访客管理子系统—证件扫描识别
114			访客管理子系统—摄像图片保存
115			访客管理子系统—证件图片保存
116			访客管理子系统—登记数据查询统计
117			访客管理子系统—数据海量保存
118			访客管理子系统—登记数据检索
119			访客管理子系统—数据网络共享
120			访客管理子系统—黑名单处理
121			访客管理子系统—闸口系统连接

122			访客管理子系统—对接业务系统
123			车辆管理子系统—企业信息登记
124			车辆管理子系统—备案管理（车辆备案）
125			车辆管理子系统—备案管理（临时车辆备案）
126			车辆管理子系统—备案管理（人员入园预约）
127			车辆管理子系统—备案审核管理（车辆备案审核）
128			车辆管理子系统—备案审核管理（临时入园审核）
129			车辆管理子系统—备案审核管理（预约人员审核）
130			车辆管理子系统—租仓合同提交
131			车辆管理子系统—备案信息查询（全部车辆查询）
132			车辆管理子系统—备案信息查询（已备案车辆查询）
133			车辆管理子系统—备案信息查询（未通过备案车辆查询）
134			车辆管理子系统—备案信息查询（预约人员查询）

135			车辆管理子系统—抬杆记录
136			车辆管理子系统—车辆类型核对
137			车辆管理子系统—基础设置（基础参数)
138			车辆管理子系统—基础设置（菜单管理)
139	园区运营管理平台	园区决策分析系统	综合管理（场站信息库）
140			综合管理（经营企业信息库）
141			综合管理（仓库信息库）
142			综合管理（报表导出）
143			综合管理（数据下载）
144			综合管理（自定义查询）
145			综合管理（报表导出）
146			综合管理（报告自动生成）
147			综合管理（可视化图表）
148			通关时效（进出口通关时长）
149			综合管理（通关效率分析）
150			综合管理（海关查验时长分析）
151			综合管理(进出口放行时长分析）
152			综合管理（邮件包裹通关时长）
153			物流管控(货种流向)
154			物流管控(放货数据)
155			物流管控(堆场数据)

156			物流管控(集装箱动态数据)
157			物流管控(电子单据动态数据)
158			物流管控(指标分析)
159			物流管控(仓库占有率)
160			物流管控(货物进出流量)
161			物流管控(车辆平均在区时长量)
162			预警管理(货物疫情预警)
163			预警管理(车辆预警)
164			预警管理（隐患随手拍）
165			产业分析（数据采集）
166			产业分析（分析建模）
167			产业分析（产业分析）
168			产业分析（分析应用）
169			智能报表-企业信息管理
170			智能报表-报表申报管理
171			智能报表-报表审核管理
172			智能报表-历史报表管理
173			智能报表-报表期限管理
174			智能报表-预警参数管理
175			智能报表-系统管理
176		园区智慧党建系统	党建服务系统
177			政治生日
178			支部信箱

179			投票问卷
180			爱心公益
181			关爱帮扶
182			党员服务窗口
183			监督考评系统
184		安全生产管理系统	安全生产一张图（风险云图）
185			安全生产一张图(风险点分布图)
186			安全生产一张图（风险排名）
187			安全生产一张图(行业风险分析)
188			安全生产一张图(风险变化趋势)
189			安全生产一张图(隐患统计分析)
190			安全生产一张图（隐患排查治理信息）
191			安全生产一张图（重大危险源监管信息）
192			园区封闭管理一张图（出入卡口监管）
193			园区封闭管理一张图（电子巡查监管）
194			园区封闭管理一张图（园区全景监控）
195			园企信息管理（园区信息管理）
196			园企信息管理（公共设施管理）

197			园企信息管理（企业档案管理）
198			园区风险隐患双控（风险分级管控）
199			园区风险隐患双控（隐患排查治理）
200			教育培训管理
201			日常安全监管（特殊作业管理）
202			日常安全监管（物流安全）
203			日常安全监管（特种设备管理）
204			日常安全监管（履职考核管理）
205			全景展示管理子系统(园区业务总览)
206			全景展示管理子系统(园区成绩及发展)
207			全景展示管理子系统(跨境电商版块)
208			全景展示管理子系统(园区车辆吞吐版块)
209			全景展示管理子系统(简化进出区版块)
210			全景展示管理子系统(分类监管版块)
211			全景展示管理子系统(仓储版块)

212			全景展示管理子系统(企业版块)
213	展销综合服务平台	云展综合服务系统	注册
214			登陆
215			审核管理
216			客服中心
217			展馆介绍
218			展会日程
219			展板信息
220			企业信息
221			在线客服
222			预约洽谈
223			展品详情
224			展商管理
225			名片管理
226			询价询盘
227			个人微页（小程序）
228			展商小站（小程序）
229			线上巡管直播连接
230			论坛
231			直播会议
232			直播录制
233			在线洽谈直播间
234			洽谈问卷调研

235			宣传中心
236			邀约中心
237			展览大数据
238			展览运营
239			订单和发票管理
240		宝玉石交易服务系统	宝玉石展示
241			收藏家社区
242			用户中心
243			订单中心
244			帮助中心
245			关联算法
246			购物车
247			社交分享
248			积分兑换
249			互动
250			签约
251			解约
252			支付
253			结算
254			鉴定管理
255			撤销
256			退款
257			收货地址管理

258			短信验证
259			进销存管理
260			用户管理
261			权限管理
262			订单管理
263			宝玉石加工管理
264			后台商品管理-商品信息
265			后台商品管理-分类管理
266			后台商品管理-商品资质
267			后台商品管理-商品图片
268			后台商品管理-商品库存
269			后台商品管理-属性管理
270			后台库存管理
271			后台备货管理
272			后台发货管理
273			内容管理
274			财务管理
275			营销管理
276			智能推荐算法
277			数据分析
278		资源云交易系统	买卖方交易子系统-买方交易管理（交易列表）
279			买卖方交易子系统-买方交易管

			理（我的报名）
280			买卖方交易子系统-买方交易管理（我的交易）
281			买卖方交易子系统-买方交易管理（历史交易）
282			买卖方交易子系统-买方交易管理（合同打印）
283			买卖方交易子系统-买方交易管理（查询统计）
284			买卖方交易子系统-买方交易管理（会员基本资料维护）
285			买卖方交易子系统-买方交易管理（密码修改）
286			买卖方交易子系统-买方交易管理（诚信意向金管理）
287			买卖方交易子系统-卖方交易管理（我的发布）
288			买卖方交易子系统-卖方交易管理（我的交易）
289			买卖方交易子系统-卖方交易管理（历史交易）
290			买卖方交易子系统-卖方交易管理（查询统计）

291			买卖方交易子系统-卖方交易管理（会员基本资料维护）
292			买卖方交易子系统-卖方交易管理（密码修改）
293			交易控制子系统-会员管理(会员信息管理）
294			交易控制子系统-会员管理(企业诚信管理）
295			交易控制子系统-会员管理(监控管理）
296			交易控制子系统-会员管理(屏蔽清单）
297			交易控制子系统-会员管理(会员信息管理）
298			交易控制子系统-会员管理(会员信息管理）
299			交易控制子系统-交易管理(交易信息发布）
300			交易控制子系统-交易管理(交易信息主记录）
301			交易控制子系统-交易管理(买方报名）
302			交易控制子系统-交易管理(交易

			控制）
303			交易控制子系统-财务管理（诚信意向金管理）
304			交易控制子系统-财务管理（会员费管理）
305			交易控制子系统-财务管理（交易服务费管理）
306			交易控制子系统-财务管理（招标代理服务费管理）
307			交易控制子系统-汇总统计（出货备案统计）
308			交易控制子系统-汇总统计（信息登记汇总）
309			交易控制子系统-汇总统计（财务出货记录统计）
310			交易控制子系统-汇总统计（招标统计）
311			交易控制子系统-基本情况管理（商品类别维护）
312			交易控制子系统-基本情况管理（海关代码维护）
313			交易控制子系统-基本情况管理（商品编码维护）

314			交易控制子系统-基本情况管理（工作日管理）
315			交易控制子系统-基本情况管理（评标规则）
316			信息发布子系统（交易信息）
317			信息发布子系统（政策公告）
318			信息发布子系统（通知公告）
319			信息发布子系统（价格指数）
320			信息发布子系统(图片定制新闻)
321	作业综合服务平台	一体化 ERP 云服务系统	基建项目管理子系统-项目申报管理
322			基建项目管理子系统-项目受理管理
323			基建项目管理子系统-项目分送管理
324			基建项目管理子系统-项目审批管理
325			基建项目管理子系统-项目报价查询
326			基建项目管理子系统-项目汇总管理
327			基建项目管理子系统-资金计划管理

328			基建项目管理子系统-资金计划调整
329			基建项目管理子系统-项目库管理
330			物业管理子系统-客户服务
331			物业管理子系统-收费管理
332			物业管理子系统-资源管理
333			物业管理子系统-OA 办公
334			物业管理子系统-业主管理
335			物业管理子系统-安保消防
336			物业管理子系统-报事报修
337			物业管理子系统-物料设备
338			物业管理子系统-财务管理
339			物业管理子系统-仓库资源管理
340			物业管理子系统-仓库资源维护
341			物业管理子系统-仓库租赁发布
342			物业管理子系统-仓库资源发布审核
343			物业管理子系统-仓库资源申请审核
344			物业管理子系统-仓库租赁合同管理
345			物业管理子系统-房屋资源管理

346			物业管理子系统-房屋资源维护
347			物业管理子系统-房屋租赁发布
348			物业管理子系统-房屋资源发布审核
349			物业管理子系统-房屋资源申请审核
350			物业管理子系统-房屋租赁合同管理
351			物业管理子系统-房屋水电费用管理
352			物业管理子系统-租金、管理费管理
353			物业管理子系统-房屋维修管理
354			物业管理子系统-房屋租赁记录管理
355			物业管理子系统-费用维护
356			物业管理子系统-仓库资源展示
357			物业管理子系统-房屋资源展示
358			物业管理子系统-空车资源展示
359			物业管理子系统-仓库资源申请
360			物业管理子系统-房屋资源申请
361			物业管理子系统-空车资源发布
362			物业管理子系统-我的租赁

363			防疫风险预警子系统-闸机数据采集
364			防疫风险预警子系统-临时进出人员分析
365			防疫风险预警子系统-企业人员维护
366			防疫风险预警子系统-人员健康信息报备
367			防疫风险预警子系统-企业人员出入园区记录
368			防疫风险预警子系统-临时出入人员记录
369			防疫风险预警子系统-预警信息管理
370			防疫风险预警子系统-风险参数设置
371			系统设置
372		智慧云仓服务系统	仓储服务子系统-申报信息反馈
373			仓储服务子系统-入库计划
374			仓储服务子系统-入库准备
375			仓储服务子系统-自动备库算法
376			仓储服务子系统-三维电子仓库
377			仓储服务子系统-所有对外标准

			接口
378			仓储服务子系统-接口监控
379			仓储服务子系统-卸货记录
380			仓储服务子系统-入库理货
381			仓储服务子系统-面单打印
382			仓储服务子系统-出库计划
383			仓储服务子系统-出库准备
384			仓储服务子系统-货物分拨
385			仓储服务子系统-装车出库
386			仓储服务子系统-库存管理
387			仓储服务子系统-库位转移
388			仓储服务子系统-仓库架管理
389			仓储服务子系统-动态盘点
390			仓储服务子系统-库存调整审核
391			仓储服务子系统-入库统计
392			仓储服务子系统-出库统计
393			仓储服务子系统-库存统计
394			仓储服务子系统-商品统计
395			仓储服务子系统-订单查询
396			仓储服务子系统-订单维护
397			仓储服务子系统-费用管理
398			仓储服务子系统-仓库设置
399			仓储服务子系统-库区设置

400			仓储服务子系统-库位设置
401			仓储服务子系统-入库明细查询
402			仓储服务子系统-出库明细查询
403			仓储服务子系统-库存调整查询
404			仓储服务子系统-资源管理
405			仓储服务子系统-用户管理
406			仓储服务子系统-角色管理
407			仓储服务子系统-授权管理
408			云仓联网辅助监管子系统-全部仓库
409			云仓联网辅助监管子系统-特殊区域仓库
410			云仓联网辅助监管子系统-非特殊区域仓库
411			云仓联网辅助监管子系统-综保区管委会自有仓库
412			云仓联网辅助监管子系统-嘉城国际物流中心仓库
413			云仓联网辅助监管子系统-菜鸟物流中心仓库
414			云仓联网辅助监管子系统-中免国际物流中心仓库
415			云仓联网辅助监管子系统-全部

			企业信息
416			云仓联网辅助监管子系统-海口综保区企业信息
417			云仓联网辅助监管子系统-空港综保区企业信息
418			云仓联网辅助监管子系统-洋浦保税港区企业
419			云仓联网辅助监管子系统-三亚保税物流中心企业
420			云仓联网辅助监管子系统-区外企业信息
421			云仓联网辅助监管子系统-全部仓库信息
422			云仓联网辅助监管子系统-海口综保区仓库
423			云仓联网辅助监管子系统-空港综保区仓库
424			云仓联网辅助监管子系统-洋浦保税港区仓库
425			云仓联网辅助监管子系统-三亚保税物流中心仓库
426			云仓联网辅助监管子系统-区外仓库信息

427			云仓联网辅助监管子系统-商品列表
428			云仓联网辅助监管子系统-商品库存
429			仓库租赁管理子系统-仓库租赁设备资源查询
430			仓库租赁管理子系统-园区租赁资源展示
431			仓库租赁管理子系统-地图选仓
432			仓库租赁管理子系统-园订单管理
433			仓库租赁管理子系统-智能推荐
434			仓库租赁管理子系统-支付记录管理
435			仓库租赁管理子系统-账单记录管理
436			仓库租赁管理子系统-企业闲置资源查询
437			仓库租赁管理子系统-闲置资源展示
438			仓库租赁管理子系统-订单管理
439			仓库租赁管理子系统-智能推荐
440			仓库租赁管理子系统-订单管理

441			仓库租赁管理子系统-支付管理
442			仓库租赁管理子系统-账单管理
443			仓库租赁管理子系统-基础信息管理
444			仓库租赁管理子系统-仓储设置
445			仓库租赁管理子系统-仓库楼设置
446			仓库租赁管理子系统-场所租赁清单管理
447			仓库租赁管理子系统-设备租赁清单管理
448			仓库租赁管理子系统-租赁平面图
449			仓库租赁管理子系统-租赁费用维护管理
450			仓库租赁管理子系统-预警处置跟踪
451			仓库租赁管理子系统-统计分析
452			仓库租赁管理子系统-闲置资源清单管理
453			仓库租赁管理子系统-闲置费用维护管理
454			仓库租赁管理子系统-订单管理

455			仓库租赁管理子系统-用户管理
456			视频管理子系统-全部视频展示
457			视频管理子系统-A 仓库接入视频
458			视频管理子系统-B 仓库接入视频
459			视频管理子系统-C 仓库接入视频
460			视频管理子系统-D 仓库接入视频
461			视频管理子系统-后续接入仓库视频
462		物流运输管理系统-运输服务子系统	基础信息管理
463			开单
464			订单管理
465			派单管理
466			智能调度
467			路径规划
468			订单跟踪
469			签回单管理
470			价格管理
471			价格模板维护
472			结算管理

473			费用清单管理
474			异常管理
475			2C 业务
476			车辆备案
477			智能放行
478			卡口临时登记
479			园区物流智能规划
480			物流协同管理
481			系统对接
482			数据报表
483			人员管理
484			数据接口
485			后台管理
486		物流运输管理系统-在途监管子系统	轨迹回放-轨迹信息管理
487			轨迹回放-轨迹地图
488			常停地址
489			危情报警-报警查询
490			危情报警-报警处置管理
491			危情报警-电子围栏预警管理
492			危情报警-天气预警管理
493			危情报警-超速预警管理
494			危情报警-地图管理
495			用户管理

496			里程统计
497			实时监控-车辆定位信息管理
498			实时监控-监控信息管理
499			实时监控-运输全流程管理
500			实时监控-监控地图坐标管理
501			实时监控-历史路线信息管理
502			电子围栏-围栏设置
503			电子围栏-围栏限速
504			电子围栏-围栏边界
505			电子围栏-围栏监控
506			电子围栏-围栏报警
507			电子围栏-围栏预警处理
508		物流运输管理系统-简化进出区管理系统子系统	企业端-企业中心（企业信息登记）
509			企业端-企业中心（企业信息查询）
510			企业端-企业中心（维修人员登记）
511			企业端-商品中心（商品信息登记）
512			企业端-商品中心（商品信息查询）
513			企业端-资质登记（资质登记）

514			企业端-资质登记（资质注销）
515			企业端-资质登记（资质查询）
516			企业端-账册备案（账册备案）
517			企业端-账册备案（账册变更）
518			企业端-账册备案（账册查询）
519			企业端-维修账册管理
520			企业端-简化进出区核放单(核放单申请)
521			企业端-简化进出区核放单(作废申请)
522			企业端-简化进出区核放单(核放单查询)
523			企业端-货物维修核放单(核放单申请)
524			企业端-货物维修核放单(作废申请)
525			企业端-货物维修核放单(核放单查询)
526			企业端--一般纳税人核放单(核放单申请)
527			企业端--一般纳税人核放单(作废申请)
528			企业端--一般纳税人核放单(核放

			单查询）
529			企业端-库存管理（调整单申报）
530			企业端-库存管理（调整单查询）
531			企业端-区内流转管理(转入申请管理）
532			企业端-区内流转管理（转入查询）
533			企业端-区内流转管理(转出申请管理）
534			企业端-区内流转管理（转出查询）
535			企业端-综合查询（核放单查询）
536			企业端-综合查询（车辆查询）
537			企业端-统计分析（企业量）
538			企业端-统计分析（业务量）
539			企业端-统计分析（商品库存）
540			企业端-统计分析（主要商品）
541			企业端-基础设置（用户管理）
542			企业端-基础设置（角色管理）
543			企业端-基础设置（菜单管理）
544			企业端-基础设置（参数管理）
545			监管端-资质审核（资质登记初核）

546			监管端-资质审核（资质登记复核）
547			监管端-资质审核（资质注销初核）
548			监管端-资质审核（资质注销复核）
549			监管端-资质审核（资质登记管理）
550			监管端-资质审核（资质登记查询）
551			监管端-账册审核（账册登记初审）
552			监管端-账册审核（账册登记复审）
553			监管端-账册审核（账册查询）
554			监管端-简化进出区审核(人工核验）
555			监管端-简化进出区审核(作废审核）
556			监管端-简化进出区审核(人工过卡口）
557			监管端-简化进出区审核(核放单查询）

558			监管端-货物维修审核（人工核验）
559			监管端-货物维修审核（作废审核）
560			监管端-货物维修审核(人工过卡口）
561			监管端-货物维修审核(核放单查询）
562			监管端-一般纳税人审核(人工核验）
563			监管端-一般纳税人审核(作废审核）
564			监管端-一般纳税人审核(人工过卡口）
565			监管端-一般纳税人审核(核放单查询）
566			监管端-账册管理(简化进出区账册）
567			监管端-账册管理(一般纳税人账册）
568			监管端-账册管理（维修账册）
569			监管端-库存管理（库存调整核验）

570			监管端-库存管理（库存调整查询）
571			监管端-区内流转管理(转入核验管理）
572			监管端-区内流转管理(转出核验管理）
573			监管端-区内流转管理(区内流转查询）
574			监管端-抽查管理
575			监管端-预警管理
576			监管端-风险参数
577			监管端-综合查询（核放单查询）
578			监管端-综合查询（车辆查询）
579			监管端-统计分析（企业量）
580			监管端-统计分析（业务量）
581			监管端-统计分析（商品库存）
582			监管端-统计分析（主要商品）
583			监管端-基础设置（用户管理）
584			监管端-基础设置（角色管理）
585			监管端-基础设置（菜单管理）
586			监管端-基础设置（参数管理）
587			监管端-系统对接（H4A 对接）
588			监管端-系统对接（智能卡口对

			接）
589		物流运输管理系统-分类监管辅助管理子系统	企业端-企业中心（企业信息登记）
590			企业端-企业中心（企业信息查询）
591			企业端-商品中心（商品信息登记）
592			企业端-商品中心（商品信息查询）
593			企业端-分类监管资质登记(资质登记）
594			企业端-分类监管资质登记(资质注销）
595			企业端-分类监管资质登记(资质查询）
596			企业端-分类监管账册登记(账册备案）
597			企业端-分类监管账册登记(账册变更）
598			企业端-分类监管账册登记(账册查询）
599			企业端-分类监管核放单(核放单申请）

600			企业端-分类监管核放单（作废申请）
601			企业端-分类监管核放单（核放单查询）
602			企业端-分类监管库存管理（调整单申报）
603			企业端-分类监管库存管理（调整单查询）
604			企业端-区内流转管理（转入申请管理）
605			企业端-区内流转管理（转入查询）
606			企业端-区内流转管理（转出申请管理）
607			企业端-区内流转管理（转出查询）
608			企业端-综合查询（核放单查询）
609			企业端-综合查询（车辆查询）
610			企业端-统计分析（企业量）
611			企业端-统计分析（业务量）
612			企业端-统计分析（商品库存）
613			企业端-统计分析（主要商品）
614			企业端-基础设置（用户管理）

615			企业端-基础设置（角色管理）
616			企业端-基础设置（菜单管理）
617			企业端-基础设置（参数管理）
618			监管端-分类监管资质审核（资质登记初核）
619			监管端-分类监管资质审核（资质登记复核）
620			监管端-分类监管资质审核（资质注销初核）
621			监管端-分类监管资质审核（资质注销复核）
622			监管端-分类监管资质审核（资质登记管理）
623			监管端-分类监管资质审核（资质登记查询）
624			监管端-分类监管账册审核（账册登记初审）
625			监管端-分类监管账册审核（账册登记复审）
626			监管端-分类监管账册审核（账册查询）
627			监管端-核放单审核（人工核验）
628			监管端-核放单审核（作废审核）

629			监管端-核放单审核（人工过卡口）
630			监管端-核放单审核（核放单查询）
631			监管端-分类监管库存管理(库存调整核验）
632			监管端-分类监管库存管理(库存调整查询）
633			监管端-区内流转管理(转入核验管理）
634			监管端-区内流转管理(转出核验管理）
635			监管端-区内流转管理(区内流转查询）
636			监管端-抽查管理
637			监管端-预警管理
638			监管端-风险参数
639			监管端-综合查询（核放单查询）
640			监管端-综合查询（车辆查询）
641			监管端-统计分析（企业量）
642			监管端-统计分析（业务量）
643			监管端-统计分析（商品库存）
644			监管端-统计分析（主要商品）

645			监管端-基础设置（用户管理）
646			监管端-基础设置（角色管理）
647			监管端-基础设置（菜单管理）
648			监管端-基础设置（参数管理）
649			监管端-系统对接（H4A 对接）
650			监管端-系统对接（智能卡口对接）
651		供应链金融服务系统	企业信息注册
652			企业信息验真（政府数据抓取）
653			企业信息验真（个人实名验证）
654			企业信息验真（企业信息验证）
655			企业融资申请
656			企业融资推送
657			企业融资撮合
658			金融融资验真
659			金融融资放款（资质审核）
660			金融融资放款（风控评估）
661			金融融资放款（发放贷款）
662			金融融资还款（还款申请）
663			金融融资还款（还款审核）
664			数据统计公开（融资量统计）
665			数据统计公开（申请量统计）
666			数据统计公开（放款量统计）

667			应收账款融资申请
668			应收账款融资审核
669			订单融资申请
670			订单融资审核
671			库存融资申请
672			库存融资审核
673			后台管理（融资类型管理）
674			后台管理（风险预警管理）
675			后台管理（放款风险防控）
676			后台管理（还款期限预警）
677			风控模型（企业财务风控模型）
678			风控模型（放款风控模型）
679			风控模型（还款风控模型）
680			银行数据接口
681			单一窗口数据接口
682		融资租赁管理系统	平台介绍
683			企业准入要求
684			政策法规
685			融资产品介绍
686			新闻咨询
687			企业注册
688			企业资质
689			企业融资申请

690			企业还款
691			逾期提醒
692			欠款追回
693			信用融资审核
694			保单管理
695			保险赔付
696			银行授信
697			贷款发放
698			企业逾期
699			补贴管理
700			后台功能
701			融资产品介绍
702			补贴审批
703			补贴发放
704			追回欠款返还
705			银行资质管理
706			产品管理
707			数据接口
708			贷款规模统计
709			贷款发放统计
710			贷款回收统计
711			企业逾期统计
712			贷款企业统计

713		免税交通工具管理系统	清单管理（综保区备案）
714			清单管理（检测线备案）
715			清单管理（收发货人备案）
716			清单管理（交通工具清单）
717			通关管理（通关管理）
718			通关管理（集装箱调拨）
719			通关管理（一体化核放单）
720			通关管理（空箱出场）
721			通关管理（退运申请）
722			通关管理（底账管理）
723			通关管理（报关单比对）
724			通关管理（交通工具放行管理）
725			物流作业（卸场作业）
726			物流作业（在场作业）
727			物流作业（提货管理）
728			检测作业（上线检测）
729			检测作业（检测报告）
730			电子地图（可视化管理）
731			电子地图（在场交通工具查询）
732			统计查询（通关物流查询）
733			统计查询（业务情况统计）
734			统计查询（在场检测统计）
735		冷链协同管理系统	信息登记（企业信息登记）

736			信息登记（消杀报告登记）
737			信息登记（运输车辆消杀登记）
738			货物监管（货物进出申请)
739			货物监管（货物进出审批）
740			货物监管（货物流转跟踪）
741			风险预警（预警参数）
742			风险预警（预警规则设定）
743			运输管理（司机信息登记）
744			运输管理（运输路线登记）
745			库存管理（出入库记录）
746			库存管理（库存量查询）
747			销售溯源管理(货物进出区记录）
748			销售溯源管理(货物采购方记录）
749			货物流向管理
750			溯源移动应用（信息登记）
751			溯源移动应用（提货预约）
752			溯源移动应用（溯源打印）
753			溯源移动应用（溯源查询）
754			数据分析管理(消杀记录统计)
755			数据分析管理(货物流向统计)
756			数据分析管理(综合数据分析)
757		跨境电商新零售管理系统	企业信息管理-企业信息登记
758			企业信息管理-企业信息查询

759			电商账册管理
760			保税进口清单管理-邮寄清单管理
761			保税进口清单管理-自提清单管理
762			保税进口报关管理-邮寄核注清单申报
763			保税进口报关管理-自提核注清单申报
764			保税进口报关管理-核注清单报文生成
765			保税进口报关管理-核注清单打印
766			保税进口报关管理-核注清单导出
767			物流管理-邮寄核放单申报
768			物流管理-自提核放单申报
769			物流管理-核放单报文生成
770			物流管理-核放单打印
771			物流管理-核放单导出
772			综合查询-清单查询
773			综合查询-溯源二维码
774			综合查询-核注清单查询

775			综合查询-核放单查询
776			综合查询-核放单查询（重发卡口报文）
777			系统设置-用户管理
778			系统设置-角色管理
779			系统设置-菜单管理
780			系统设置-客户端设置
781			系统设置-客户端（基础配置管理）
782			系统设置-客户端（监控服务管理）
783			系统设置-客户端（数据落地管理）
784			系统设置-客户端（申报异常管理）
785			系统设置-客户端（资源监控管理）
786			系统对接-溯源码接口
787			系统对接-闸机放行接口
788			系统对接-金二对接
789			系统对接-卡口对接
790		溯源采集管理系统	货物信息管理子系统(运抵确认)
791			货物信息管理子系统(消杀登记)

792			货物信息管理子系统(核酸登记)
793			风险预警管理子系统（应急处置）
794			风险预警管理子系统（异常预警）
795			风险预警管理子系统（预警管理）
796			运输及库存管理子系统（入库确认）
797			运输及库存管理子系统（货物流出）
798			运输及库存管理子系统（出库转运）
799			运输及库存管理子系统（自用耗损）
800			运输及库存管理子系统（信息补录）
801			销售溯源子系统（销售入库）
802			销售溯源子系统（销售流通）
803			销售溯源子系统（损耗报备）
804			销售溯源子系统（信息补录）
805			信息登记管理子系统（备案管理）
806			信息登记管理子系统（备案审核）
807			货物流向管理子系统（提货预约）
808			货物流向管理子系统（提货完成）
809			数据分析（提货量统计分析）

810			数据分析（放码量统计分析）
811			数据分析（消杀量统计分析）
812			数据分析（进境口岸统计分析）
813			数据分析（货物类型统计分析）
814			数据分析（目的地统计分析）
815			溯源移动应用（个人中心）
816			溯源移动应用（注册登录）
817			溯源移动应用（信息登记）
818			溯源移动应用（货物管理）
819			溯源移动应用（货物流向）
820			溯源移动应用（运输库存)
821			溯源移动应用（销售溯源）
822			溯源移动应用（溯源码）
823	辅助监管业务服务平台	智能场站管理系统	货运管理子系统-集装箱装卸作业
824			货运管理子系统-装卸作业跟踪
825			货运管理子系统-现车管理
826			货运管理子系统-货运计划管理
827			货运管理子系统-作业管理
828			确报管理子系统-车辆抵达预报
829			确报管理子系统-车辆抵达确报
830			确报管理子系统-车辆离场预报
831			确报管理子系统-车辆离场确报

832			换装管理子系统-换装计划编制
833			换装管理子系统-换轮作业监控
834			换装管理子系统-换装清单管理
835			堆场管理子系统-落箱单打印
836			堆场管理子系统-落箱确认
837			堆场管理子系统-移箱管理
838			堆场管理子系统-提箱单打印
839			堆场管理子系统-提箱确认
840			堆场终端应用子系统-收箱确认
841			堆场终端应用子系统-发箱确认
842			堆场终端应用子系统-移箱确认
843			堆场终端应用子系统-装车确认
844			堆场终端应用子系统-卸车确认
845			仓库管理子系统-货物进出管理
846			仓库管理子系统-暂存仓储管理
847			仓库管理子系统-理货管理
848			仓库管理子系统-普货单证管理
849			仓库管理子系统-普货底账管理
850			仓库管理子系统-暂不放行货物管理
851			仓库管理子系统-风险预警
852			费收管理子系统-标准费用设置
853			费收管理子系统-协议企业费用

			设置
854			费收管理子系统-费用清单管理
855			费收管理子系统-月结账单管理
856			场站可视化管理子系统-库场管理
857			场站可视化管理子系统-可视化作业监控
858			综合查询子系统-集装箱统计
859			综合查询子系统-进口货物统计
860			综合查询子系统-出口货物统计
861		多式联运服务系统	委托书管理子系统-委托单填报
862			委托书管理子系统-委托单审核
863			委托书管理子系统-制单
864			委托书管理子系统-委托单查询
865			委托书管理子系统-物流跟踪
866			订舱管理子系统-订舱申请
867			订舱管理子系统-订舱审核
868			订舱管理子系统-订舱查询
869			单据管理子系统-补贴申请
870			单据管理子系统-补贴审核
871			单据管理子系统-补贴参数维护
872			单据管理子系统-审计资料上传
873			单据管理子系统-审计资料比对

874			单据管理子系统-单据信息查询
875			集装箱管理子系统-用箱申请
876			集装箱管理子系统-用箱审核
877			集装箱管理子系统-放箱申请
878			集装箱管理子系统-费用统计
879			集装箱管理子系统-还箱申请
880			集装箱管理子系统-验箱审核
881			集装箱管理子系统-综合查询
882			集装箱管理子系统-集装箱管理
883			集装箱管理子系统-集装箱调度
884			集装箱管理子系统-GPS 信息管理
885			集装箱管理子系统-数据统计分析
886			用户管理子系统-权限管理
887			用户管理子系统-角色管理
888			用户管理子系统-用户管理
889		跨境电商园区服务系统	事前备案（企业中心）
890			事前备案（商品中心）
891			事前备案（海外仓报备）
892			账册管理（账册备案）
893			账册管理（账册查询）
894			计划管理（进口到货计划）

895			计划管理（出口到货计划）
896			计划管理（进口出库计划）
897			计划管理（出口出库计划）
898			交易单据管理（三单数据查询）
899			交易单据管理(入库明细单查询)
900			B2C 业务（直购进口-订单管理）
901			B2C 业务（直购进口-运单管理）
902			B2C 业务（直购进口-支付单管理）
903			B2C 业务（直购进口-清单管理）
904			B2C 业务（一般出口-订单管理）
905			B3C 业务（一般出口-运单管理）
906			B2C 业务（一般出口-收款单管理）
907			B2C 业务（一般出口-清单管理）
908			B2C 业务（网购保税进口-订单管理）
909			B2C 业务（网购保税进口-运单管理）
910			B2C 业务（网购保税进口-支付单管理）
911			B2C 业务（网购保税进口-清单管理）

912			B2C 业务（特殊区域出口-订单管理）
913			B3C 业务（特殊区域出口-运单管理）
914			B2C 业务（特殊区域出口-收款单管理）
915			B2C 业务（特殊区域出口-清单管理）
916			B2B 业务（直接出口-订单管理）
917			B2B 业务（直接出口-运单管理）
918			B2B 业务（直接出口-收款单管理）
919			B2B 业务（直接出口-清单管理）
920			B2B 业务（出口海外仓-订单管理）
921			B2B 业务（出口海外仓-运单管理）
922			B2B 业务（出口海外仓-收款单管理）
923			B2B 业务（出口海外仓-清单管理）
924			查询统计（进口数据管理-订单查询）

925			查询统计（进口数据管理-运单查询）
926			查询统计（进口数据管理-支付单查询）
927			查询统计（进口数据管理-清单查询）
928			查询统计（进口数据管理-入库明细单查询）
929			查询统计（出口数据管理-订单查询）
930			查询统计（出口数据管理-运单查询）
931			查询统计（出口数据管理-收款单查询）
932			查询统计（出口数据管理-运抵单查询）
933		免税品辅助管理系统-企业端	个人资料
934			企业信息查询
935			账册备案
936			账册变更
937			核放单申报
938			核放单作废
939			核放单查询

940			账册查询
941			入库准单绑定
942			调整单申报
943			调整单查询
944			核注清单申报（进口）
945			核注清单申报（出口）
946			核注清单变更
947			核注清单删除
948			核注清单核查
949			核注清单查询
950			免税品核放单查询
951			核注清单查询
952			核放单查询
953			企业统计
954			业务统计
955			商品库存统计
956			主要商品统计
957		免税品辅助管理系统-监管端	企业信息-企业信息列表
958			账册备案-账册审核
959			账册备案-账册（备案）查询
960			账册管理-账册查询
961			调整单管理-调整单审核
962			调整单管理-调整单查询

963			免税品核放单-人工审核
964			免税品核放单-作废审核
965			免税品核放单-人工过卡
966			免税品核放单-核放单查询
967			预警管理-核放单预警处置
968			预警管理-核放单预警查询
969			查验管理-核放单抽查处置
970			查验管理-核放单处置查询
971			风险参数-预警参数
972			风险参数-布控参数
973			风险参数-审单参数
974			统计分析-企业统计
975			统计分析-业务统计
976			统计分析-单量统计
977			统计分析-主要商品统计
978			统计分析-商品库存统计
979			综合查询-免税品核放单查询
980			综合查询-核放单处置查询
981			基础设置-基础参数
982			基础设置-角色管理
983			基础设置-用户管理
984			基础设置-菜单管理
985			系统对接-H4A 对接

986			系统对接-大数据局报关单对接
987			系统对接-智能卡口对接
988			系统对接-装卸监控设备对接
989	应用支撑平台	统一用户/权限管理系统	登录管理
990			区域管理
991			菜单管理
992			数据管理
993			企业管理
994			部门管理
995			角色管理
996			用户管理
997			信息查询
998		数据交换系统	数据接入
999			数据处理
1000			数据共享
1001			数据质量管理
1002			数据服务管理
1003			异步传输
1004			加密压缩
1005			流量控制
1006			安全通道
1007			链接控制
1008			访问授权

1009			传输管理
1010			监控报警
1011		订阅分发系统	订阅事件申请
1012			解析及管理
1013			监控预警
1014			订阅式分发
1015			触发式分发
1016			统计分析
1017		统一 API 管理	接入平台管理
1018			协议管理
1019			接口管理
1020			日志管理
1021			接口统计
1022			路由分发
1023			连接设置
1024			单边地址维护
1025			地址过滤
1026			配置推送
1027			日志记录
1028	智慧海南对接体系	与海南省大数据管理局对接	
1029		一线口岸对接	
1030		二线口岸对接	

硬件设备采购清单

序号	名称	技术参数要求	单位	数量
一	园区智慧安防系统			
1.1	视频监控子系统			
1	网络半球摄像机	1）传感器类型 1/2.7 英寸 CMOS； 2）像素不低于 400 万； 3）最低照度≤0.002Lux(彩色模式)；≤0.0002Lux(黑白模式)；0Lux(补光灯开启)； 4）最大补光距离 30m（红外）； 5）镜头类型定焦（2.8mm、3.6mm、6mm 等可选）； 6）区域入侵； 7）视频压缩标准 H.265；H.264； 8）宽动态 120dB； 9）内置 MIC； 10）支持报警事件：网络断开；IP 冲突；非法访问；动态检测；	台	117

		11）视接入标准 ONVIF、GB/T28181； 12）供电方式 DC12V/POE； 13）工作温度：-30℃~60℃，工作湿度：5%~95%(无冷凝)； 14）防护等级 IP67。		
2	智能网络球机	1)内置 GPU 芯片，支持深度学习算法，有效提升检测准确率 2)支持视频结构化功能：支持机动车抓拍、机动车属性提取，支持非机动车抓拍、非机动车属性提取，支持人体抓拍、人体属性提取，支持人脸抓拍、人脸属性提取； 3)支持人脸检测；支持人脸优选抓拍；支持人脸属性提取；最多可同时检测、跟踪、抓拍≥40 个运动人脸目标； 4)支持绊线入侵、区域入侵、穿越围栏、徘徊、快速移动、停车、人员聚集检测；支持人车分类报警； 5）采用开放架构，支持快速集成智能算法或应用 APP，智能算法或 APP 可以独立升级；支持智能算法模块动态加载，加载过程中，视频业务不中断； 6)一体化设计，兼顾全景与细节，达到单个产品既能看全也能看清的优势，全景和细节镜头都采用 400 万像素 1/1.8 英寸 CMOS 传感器，支持≥25 倍光学变倍，≥16 倍数字变倍； 7)支持 H.265 编码，实现超低码流传输 8)全景相机内置≥30 米白光灯补光，采用暖色调和柔化处理，有效降低炫目程度；细节相机内置≥100 米红外灯补光，	台	45

		可根据被摄物的距离自动调节补光灯的功率，补光效果更均匀 9)细节相机：水平范围：0°～360°，垂直范围： -20°～90，预置位最大速度 200°/s； 10)支持 300 个预置位，不低于 8 条巡航路径、5 条巡迹路径 11)工作温度:-40℃~60℃,工作湿度:5%~95%(无冷凝)； 12)防护等级:IP67		
3	智能网络枪机	1）内置 GPU 芯片，支持深度学习算法，有效提升检测准确率 2）支持六种智能资源切换：通用行为分析、人脸检测、视频结构化、客流统计、人脸识别、道路监控 3）支持视频结构化：支持机动车、非机动车、人脸、人员等目标的抓拍和属性识别；支持人脸检测;支持跟踪;支持优选;支持抓拍;支持上报最优的人脸抓图;支持人脸增强,人脸曝光;支持人脸属性提取。最多可同时检测、跟踪、抓拍≥20 个运动人脸目标； 4）支持客流统计：支持排队管理；支持区域内人数统计，进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用 5）支持绊线入侵，区域入侵，快速移动，物品遗留，物品搬移，徘徊检测，人员聚集，停车检测 6）采用开放架构，支持快速集成智能算法或应用 APP，智能算法或 APP 可以独立升级；支持智能算法模块动态加载，加	台	76

		载过程中，视频业务不中断； 7）采用超星光超低照度 400 万像素 1/1.8 英寸 CMOS 图像传感器，低照度效果好，图像清晰度高） 8）支持 H.265 编码，压缩比高，实现超低码流传输 9）支持走廊模式，宽动态，3D 降噪，强光抑制，背光补偿，数字水印，适用不同监控环境 10)工作温度:-30℃~60℃,工作湿度:5%~95%(无冷凝) 11)防护等级:IP67		
4	高清网络枪机	1)传感器类型 1/3 英寸 CMOS,像素不低于 400 万 2)工作温度：-30℃~60℃，工作湿度：5%~95%(无冷凝)； 3)最大分辨率≥2688×1520； 4)最低照度≤0.002Lux(彩色模式)；≤0.0002Lux(黑白模式)； 5)最大补光距离小于等于 120m（红外）； 6)镜头类型定焦,3.6/6mm 等可选； 7)支持人群态势分析、目标检测和目标属性检测、支持最佳人脸筛选。 8)通用行为分析绊线入侵；区域入侵； 9)视频压缩标准 H.265；H.264； 10)宽动态≥120dB； 11)报警事件无 SD 卡；SD 卡空间不足；SD 卡出错；网络断开；IP 冲突；非法访问；动态检测； 12)接入标准:ONVIF；GB/T28181；	台	228

		13)最大 MicroSD 卡 256GB； 14)供电方式 DC12V/POE； 15)防护等级≥IP67		
5	全景球机	1)传感器类型≥1/1.8 英寸 CMOS； 2)双镜头一体化像素≥400 万（全景）+200 万（球机）； 3)最大分辨率≥2560×1440； 4)最低照度：全景：≤0.001Lux（彩色模式）；≤0.0001Lux（黑白模式）；细节:≤0.001Lux（彩色模式）；≤0.0001Lux（黑白模式）；0Lux（补光灯开启）； 5)最大补光距离：球机：≥200 米（红外补光）； 6)镜头类型：全景：定焦 5mm，镜头细节 40 倍变焦，焦距≥6-240mm； 7)支持车辆识别、车辆事件检测、交通数据统计、人群态势分析、全结构化、通用行为分析：区域入侵；绊线入侵； 8)支持机动车、非机动车、行人混合检测抓拍，支持将人脸与人体、车牌与车辆进行关联；支持人脸、人体、车辆检测抓拍及属性提取。 10)视频压缩标准：H.265；H.264； 11)宽动态：120dB; 12)报警事件：无 SD 卡；SD 卡空间不足；SD 卡出错；网络断开；IP 冲突；非法访问；动态检测； 13)接入标准：ONVIF；GB/T28181； 14)工作温度:-40℃~60℃,工作湿度:5%~95%(无冷凝)；	个	10

		15)防护等级:IP67		
6	高空抛物专用摄像机	1)算力:1 TOPS;1/2.7″,像素不低于 400 万 2)镜头焦距≥2.8-12mm; 3)最低照度:彩色:0.005Lux(F1.6,AGC ON),黑白:0.0025Lux(F1.6,AGC ON),0Lux(红外开启); 4)红外补光:50m; 5)压缩编码:H.264/H.265; 6)行为分析;支持目标检测，支持 7)以太网络接口:1 个 RJ45 10M/100M 以太网口; 8)DC12V,PoE(IEEE 802.3af);最大功耗:12.2W,典型功耗:3.2W; 9)工作温度:-30℃~60℃; 10)防护等级≥IP67。	个	4

7	周界警戒摄像机（海口园区）	1)传感器类型 1/2.7 英寸 CMOS；像素不低于 400 万； 2)最低照度≤0.002Lux(彩色模式)；≤0.0002Lux(黑白模式)；0Lux(补光灯开启)。 3)最大补光距离 50m（红外视频监控距离）30m（暖光视频监控距离） 10m（暖光人脸检测距离）； 4)镜头类型定焦；镜头焦距 3.6mm（6mm 等可选）； 5)周界防范绊线入侵；区域入侵；快速移动；徘徊检测；人员聚集；停车检测；支持人脸检测； 6)视频压缩标准 H.265；H.264； 7)报警事件无 SD 卡；SD 卡空间不足；SD 卡出错；网络断开；IP 冲突；非法访问；动态检测； 8)灯光报警；声音报警（内置语音可选，支持用户自定义语音导入）； 9)接入标准 ONVIF；GB/T28181；GA/T1400； 10）工作温度：-30℃~60℃，工作湿度：5%~95%(无冷凝)； 11）防护等级 IP67。	个	46
8	全景球机支架	不锈钢重载支架	个	10
9	智能网络枪机支架	壁装支架/铝合金	个	76

10	枪机支架	壁装支架/铝合金	个	228
11	球机支架	铝合金；最大承重 9.0kg；立杆支架装；	个	45
12	监控立杆	立杆高度 6 米，悬臂长度按现场环境 1-3 米定制，热镀，一杆一横臂	个	73
13	外加横杆	悬臂长度按现场环境 1-3 米定制，热镀	个	73
14	立杆底座基础	摄像机立杆基础底座尺寸为 1.2mX1.2mX1.2m，包含地锚、基础、开挖、回填、机械费、人工费、垃圾外运等	套	73
15	立杆地笼	与立杆大小配套	个	73
16	磁盘阵列	1)操作系统：嵌入式 LINUX 系统； 2)主处理器≥64 位高性能多核处理器； 3)高速缓存：标配 8GB，可扩展至 64GB； 4)电源冗余：1+1 冗余电源； 5)网络接口：1 个千兆管理电口，2 个千兆数据电口； 6)硬盘个数：≥38 块硬盘； 7)硬盘兼容性：1TB、2TB、3TB、4TB、5TB、6TB、8TB、10TB、12TB、14TB、16TB，支持 SATA 盘混插支持 SSD 硬盘支持 2.5、3.5 英寸硬盘支持 SATA 盘；	台	8

		8)支持视频流和图片流直存：最大不少于支持 2048 路前端接入、1560Mbps 存储、1024Mbps 转发，512Mbps 网络回放； 9）支持单台服务器起配，管理和业务服务共享统一的虚拟化资源；在一台实体服务器虚拟化后的多台逻辑服务器上，支持部署不同功能以及数量的存储、转发、智能分析、检索服务模块；		
17	企业级硬盘	16TB 企业级硬盘,SATA 6Gb/s,7.2K rpm,3.5-Inch(3.5-Inch Drive Bay)	块	290
18	HDMI 线	HDMI 高清数据线，15m	条	20
19	输入板卡	4 路 HDMI 编码卡音频输入接口：无接口，HDMI 接口自带音频编码格式：H.264/MPEG4 编码能力：单板 4 路 1080P，支持 1080P/720P/UXGA/SXGA+ /SXGA/XGA/SVGA/VGA 分辨率	块	1
20	输出解码板卡	6 路 HDMI 增强型解码卡，支持 8 路 4096*2160@25fps，8 路 3840*2160@30fps ，32 路 1080p@30fps（H.264、H.265），72 路 720p@30fps，150 路 D1 解码； 支持 8 路 1080P 的 SVAC 解码；支持 24 路非标 D1 码流解码； 1/4/6/8/9/16/25/36 画面分割，自由分割	块	4
21	网络键盘	10.1 英寸电容触摸屏,分辨率不低于 1280*800 支持 H.265、H.264、H264H、H264B 等；最大 16 画面分割 支持在触屏观看图像或通过 HDMI 将图像投到屏幕上 支持最大 2 万路设备控制	台	1

		支持支持抓图、录像功能，文件保存至U盘 USB2.0和USB3.0各2个 4路报警输入，高低电平可调 4路报警输出，3路继电器，1路12V_1A可控″		
22	安防综合管理平台	基础平台，包含视频监控系统、报警管理系统、门禁管理系统、车辆管理系统、停车管理系统、设备运维系统的接入； 系统功能包括： 1）作业中心：告警处置系统、安防巡逻系统（视频巡更+电子巡更模式）、视频实景查看与调阅、布防管理（人员与车辆布防与检索、人脸布控、人脸轨迹、以图搜图）； 2）人员通行管理：访客预约、出入口管理、通行权限、通行记录、疫情防控管理； 3）安防综合管理：园区安防态势（人员、车辆、安防设备、告警事件、支持多园区接入和选择）、运营态势（人员通行画像、车辆通行画像、告警事件画像、工单任务画像、运营指标）	套	1
23	流媒体服务器	Intel Xeon 4108 1.8G 9.6UPI 11M 8C 85W*2/16GB*4/2T 3.5吋 7200转 6Gb SATA硬盘*2/LSI3008 SAS卡*1/8千兆网口/冗余电源/2U机架式	台	1
24	视频诊断服务	支持对视频模糊、高亮异常、低亮异常、偏色、低对比度异常、视频抖动运动、噪声过大、条纹干扰、视频丢失、视频冻结、视频遮挡和场景变化等异常现象进行报警统计；支持	台	1

	器	3000 路视频质量诊断授权 1 颗 IntelXeonE3-1275V5，3.6GHz，4C/8T|1 根 16GBDDR4 内存条|1 块 3.5 寸 1T 硬盘|2 个千兆以太网电口|单电源		
25	智能行为分析服务器	支持 32 路前端实时视频流接入，通过配置一定的智能分析规则，输出异常事件报警及分析数据，其中异常事件检测包括绊线入侵检测、区域入侵检测、人群聚集检测、物品检测、未带安全帽、烟雾明火识别、离岗检测、跌倒检测等事件类型。	台	2
26	视频分析服务器	1)处理器：2 颗多核处理器，主频≥2.2GHz，缓存≥35MB； 2)单台配置不少于 2 张 GPU 卡，最大可支持 6 块 GPU 卡； 3)内存：不低于 128GB,采用 DDR4、2666MHZ 及以上规格，支持内存扩展； 4)配置≥2 块 1.2TB 硬盘 5)≥2 个万兆/千兆自适应网口 6)支持人脸图片流检测分析，支持性别、年龄段、表情、眼镜、胡子、口罩等属性 7)支持 200 张/秒人脸小图。 8)支持按性别、年龄段、抓拍时间等对历史抓拍人脸图片进行检索与导出。 9)支持 200 万黑/白名单库总容量。 10)单台支持 20 亿条目标/车辆/人体特征数据存储，检索响应时间不大于 3 秒；支持 40 亿条目标/车辆/人体结构化数据存储和检索；单台支持对 2 亿条目标/车辆/人体特征数据	台	2

		进行检索，检索响应时间小于 3 秒； 11)支持对历史录像进行分片并行分析； 12)分析业务包括：目标特征识别、车辆特征识别； 13)管理和业务服务共享统一的虚拟化资源；在一台实体服务器虚拟化后的多台逻辑服务器上，支持部署不同功能以及数量的存储、转发、智能分析、检索服务模块；		
27	网线	超 5 类 4 对（每个摄像头预估 50 米）	米	19237
28	主电源线	RVV3*2.5 （每个摄像头预估 35 米）	米	13466
29	壁挂机柜	24U	个	75
30	PVC 线管	PVC 管 25mm	米	52

				500
31	插排插座	8位5孔	个	385
32	辅材		批	1
	小计1			
1.2	**报警子系统**			
1	总线报警主机	支持本地16路报警输入，最大可扩展到256路；支持接入常开或常闭型探测器;支持探测器防拆、防短、防遮挡功能;1支持本地4路报警输出，最大可扩展到256路；支持强制开启、强制关闭、自动控制功能，支持报警联动;支持即时防区、延时防区、24小时无声等多种防区类型;1 支持报警输入输出接口电路保护功能;	台	12
2	单防区扩展模块	单防区扩展；常开、常闭类型探测器可选；最大级联数240；通信协议Mbus	个	150

3	双鉴探测器	探测器探测距离 6m、8m 可选，探测角度 15° 报警输出 NC/NO 可选，适应不同项目需求 探测器内置防拆开关，防拆报警输出，更加安全可靠 支持双向数字温度补偿技术，确保高温环境下探测距离不衰减 支持数字抗白光技术，专用滤光镜片，抗白光等级 20000Lux	个	150
4	双鉴探测器支架	探测器配套支架	个	150
5	报警键盘	LCD 屏幕，报警对应防区号显示，报警布撤防，支持通讯状态查询	个	12
6	蓄电池	市电断电给报警主机供电，上传断电报警信号	个	12
7	声光警号	报警中心联动报警，声光一体式	个	12
	小计 2			
1.3	**智能巡查子系统**			
1	移动	CPU：8 核 1.8G/4GBLPDDR3+64GBeMMC；操作系统：	台	2

	手持巡更终端	Android9.0,64bit；SD 卡：支持一个 TF 卡扩展,最大支持 256GB；网络：4G 全网通，双卡,nanoSIM 卡,DSDS，支持双 4G；屏幕尺寸/分辨率：5.7 英寸/FHD+(2160*1080)（18：9）；主摄像头/副摄像头：1600 万像素/800 万像素；电池容量：4600mAh,4.35V，充电时间小于 4 小时；指纹识别：带指纹识别前置式，具备 HOME 键（触摸式）功能；Wi-Fi：802.11a/b/g/n/ac,2.4GHz;蓝牙:BT4.2;NFC:NFC13.56MHz；感应器：光敏/距离/指南针/陀螺仪/重力 G-Sensor；GPS：支持 GPS/北斗，精度 3 米以内；喇叭：1 个，单体防水，功能 2W；视频压缩格式：兼容 H.265、H.264；侧键：实体按键：音量+、音量-、开关机、自定义 Fn2、自定义 Fn1、PTT、SOS；防护等级：IP68，跌落 1.5 米；工作/存储温度：-20℃~+60℃/-30℃~+70℃；外部扩展接口顶部接口：可锁定 Type-C，连接头戴式摄像头、肩夹式摄像头；背部 pogpin 接口：8pin，可以连接充电底座，3.5mm 耳机接口；标配配件：电池、充电器、数据线各一个；		0
2	巡更点标签	支持国际标准 IEC/ISO14443A 13.56MHz 工作频段； 读取距离 0～3m（与信息采集设备有关） 数据存储时间长达 10 年	个	300
	小计 3			
1	**园区**			

.4	**一脸通子系统**			
1	人脸门禁一体机	采用 7 寸 TFT 液晶屏，屏幕显示分辨率达到 1024×600 摄像头采用 200 万 CMOS，支持真实宽动态 工作温度支持-30 至 60℃，可适应各种环境 支持 IP65 防护等级（需要点胶，详见操作手册） 支持自动补光，可有效降低环境光污染 支持 10 万个用户、10 万张人脸、1 万枚指纹、10 万张卡、10 万个密码、50 个管理员、30 万条记录 支持人脸、指纹、IC 卡、密码、二维码等多种识别方式，并支持多种组合识别鉴权方式 支持显示人脸框，并实时检测最大人脸，支持识别区域及人脸目标大小设置 支持面部识别距离 0.3m-2.0m;适应 0.9m～2.4m 身高范围(镜头安装高度 1.4 米) 基于深度人脸识别算法，精准定位目标人脸 360 个以上关键点位置	台	10
2	双开门磁力锁	铝合金；电镀拉丝；锁体尺寸：长 500x 宽 47x 厚 26(mm)；吸板尺寸：长 180x 宽 38x 厚 11(mm)；280kg*2(600Lbs*2)直线拉力；锁状态信号输出；断电开门；适用木门\玻璃门\金属门\防火门等；工作温度：-20℃-+60℃，工作湿度：≤95%；	个	10

3	磁力锁支架	磁力锁支架（ZL 型）	个	20
4	磁力锁电源	DC12V2A	个	10
5	开门按钮	塑料外壳 86*86*25mm 工作温度：-30℃-+60℃，工作湿度：≤95%；	个	10
6	闭门器	最大门重:80KG 最大门宽:1100MM 关门力度:EN4 开门角度:180 度 定速功能:有 定位功能:有 使用寿命:100 万次 适用范围:工作温度：-20℃-+55℃， 工作湿度：≤95%；	个	20
7	单机芯左边道	产品尺寸 1500mm×200mm×980mm（长×宽×高）；外壳材料 SUS304；驱动电机直流无刷伺服电机；电机使用寿命 500 万次；摆臂材料不锈钢/亚克力；通道宽度 600mm；最大定制通道宽度 1100mm；红外对射 12 对；通行速度 20 人~60 人/min；开闸时间 0.5s；开门模式刷卡/人脸识别；输入接口 RS232 串口/RS485 接口；功耗≤10W（待机），≤130W（工作）；工作温度-25℃~+70℃；使用环境室内、室外	台	2

8	单机芯中间道	产品尺寸 1500mm×200mm×980mm（长×宽×高）；外壳材料 SUS304；驱动电机直流无刷伺服电机；电机使用寿命 500 万次；摆臂材料不锈钢/亚克力；通道宽度 600mm；最大定制通道宽度 1100mm；红外对射 12 对；通行速度 20 人~60 人/min；开闸时间 0.5s；开门模式刷卡/人脸识别；输入接口 RS232 串口/RS485 接口；功耗≤20W（待机），≤260W（工作）；工作温度-25℃~+70℃；使用环境室内、室外	台	2
9	单机芯右边道	产品尺寸 1500mm×200mm×980mm（长×宽×高）；外壳材料 SUS304；驱动电机直流无刷伺服电机；电机使用寿命 500 万次；摆臂材料不锈钢/亚克力；通道宽度 600mm；最大定制通道宽度 1100mm；红外对射 12 对；通行速度 20 人~60 人/min；开闸时间 0.5s；开门模式刷卡/人脸识别；输入接口 RS232 串口/RS485 接口；功耗≤10W（待机），≤130W（工作）；工作温度-25℃~+70℃；使用环境室内、室外	台	2
10	摆臂	摆闸不锈钢门翼-1100mm	个	8
11	人脸识别模块	采用 7 英寸 LCD 屏，分辨率 1024*600 支持人脸、密码、二维码等多种识别认证方式，支持分时段开门 支持显示人脸框，并实时检测最大人脸，支持识别区域及人脸目标大小设置 采用 200 万广角宽动态双目摄像头，支持自动开启补光灯以及手动调节补光灯亮度	台	6

		支持面部识别距离 0.3m-2.0m，适应 0.9m～2.4m 身高范围 基于深度人脸识别算法，精准定位目标人脸 360 个以上关键点位置 人脸验证准确率高达 99.5%，1：N 比对时间 0.35 秒/人，识别速度快，准确率高 适应侧脸，支持人脸识别角度 0~90° 设置 设备支持 50000 个用户，50000 张卡，50000 个密码，50000 个人脸，50 个管理员 支持活体检测功能，支持手机照片、打印照片和视频防假 支持胁迫报警、 防拆报警 支持来宾用户下发、巡逻用户下发、黑名单用户下发、VIP 用户下发、普通用户下发、特殊用户 支持 4 种识别提示模式及多种语音提示信息，方便用户选择		
12	遥控器	接收器：电压 DC 24V；电流 0.1A；接收灵敏度-107dBm；四路继电器输出，信号互锁、信号非锁、信号自锁、信号两路自锁和两路非锁并存；遥控器：电压：DC12V（10 号干电池）；电流：38mA（待机为 0）；输出功率 16dBm；按键数量：4 个；塑料；工作温度：-10℃-+70℃， 工作湿度：≤93%；包含一个接收器、两个遥控器（含干电池）	个	4

13	访客设备	主屏：采用 15.6 英寸触摸显示屏，分辨率 1920(H)*1080(V)； 辅屏：采用 11.6 英寸显示屏，分辨率 1366(H)*768(V)； 采用 200 万高清单目摄像头；摄像头角度可调，可适应不同身高访客登记； 支持发卡功能； 支持人脸活体检测，照片视频有效防假； 支持脱机运行，事件记录存储功能； 支持身份证、二维码、IC 卡等多种签离方式； 支持图片、视频广告播放功能； 支持语音提示功能； 支持访客信息打印功能； 支持双网口网络通信； 支持 2 路 USB2.0、2 路 RJ45；	台	2
14	人脸采集摄像机	外观 USB；像素 200 万；镜头焦距 2.8mm；传感器类型 1/2.9 英寸 CMOS；镜头类型定焦；供电方式 USB5V	台	1
	小计 4			
1.5	**园区交互会议子系**			

	统			
1	会议管理平台	1）采用国产自主的操作系统和数据库软件。独立硬件部署（非 MCU 内置模块），基于容器的服务化架构，支持将不同功能的业务部署在不同的容器内运行，避免应用对资源抢占和相互影响。 2）支持 H.323 Gatekeeper、Sip Server、SIP Proxy 等功能。 3）支持会议终端、MCU、呼叫注册网守、穿越网关、网络地址本服务器、录播服务器等统一设备管理功能。本次配置 50 个硬件设备管理 License,50 个硬件设备注册 License 4）支持会议锁定功能，管理员锁定会议后不允许其他终端主动加入会议，保障会议私密性 5）支持系统三员账号管理，支持系统管理员、安全管理员、安全审计员权限隔离。 6）支持 MCU 资源池备份功能，当某台 MCU 发生故障时，管理平台自动将会议调度在其他 MCU，无需断会及手动更改配置，业务恢复时间<10S； 7）支持即时会议、预约会议、周期会议、永久会议等会议模式，支持一键静闭音、广播/选看会场、辅流加入多画面、设置多画面、锁定会议演示、指定会场发送辅流、声控切换、设置主席、点名等功能。 8）▲支持 SM2、SM3、SM4 国密算法加密会议.（提供具有 CNAS 或 CMA 机构认可的第三方检测机构出具的检测报告复印件并	台	1

		加盖厂家公章或投标专用章） 9）支持 NAPT/HTTP 反向代理及 Web 数据业务代理，实现内外网终端网络地址本访问、数据共享、白板共享、多方批注等功能； 10）支持 IPv4 和 IPv6 双协议栈，支持 IPv4 和 IPv6 混合组网.		
2	MCU	1）采用国产自主嵌入式操作系统，非 Windows、非 Android 系统。 2）支持 ITU-T H.323、IETF SIP 协议，支持 ITU-T H.239、IETF BFCP 双流协议，具备良好的兼容性。支持 64Kbps-8Mbps 呼叫带宽。 3）支持 4K30fps、1080p30/60fps、720p30/60fps、4CIF 分辨率的活动视频。 4）在全编全解模式下，单台 MCU 最大支持≥16 个 4K30fps 视频端口或者 32 个 1080P60fps 视频端口或者 64 个 1080P 30fps 视频端口.本次 MCU 配置 10 个 1080P 30fps 会场并发端口。 5）▲支持全编全解技术，确保每个接入的会场均能以任意不同的协议、带宽、格式、帧率参加同一组会议；支持 AVC/SVC 混合会议，以适应不同线路带宽、不同设备能力、不同网络	台	1

		环境下的组网要求；（提供具有 CNAS 或 CMA 机构认可的第三方检测机构出具的检测报告复印件并加盖厂家公章或投标专用章） 6）支持 MCU 资源池备份功能，当某台 MCU 发生故障时，系统自动将会议调度在其他 MCU，无需手动配置，会议切换时间<10S； 7）支持断线重呼功能，MCU 可自动重邀掉线或断电的终端再次入会 8）支持 SIP(TLS/SRTP)信令和媒体流加密、AES 加密算法、H.235 媒体流加密、H.235 认证和信令完整性校验； 9）支持 IPv4 和 IPv6 协议下的会议和设备管理；为降低网络带宽支出，以 512Kbps 带宽实现 1080P60fps 会议效果；以 384Kbps 带宽实现 1080P30fps 会议效果； 10）支持 30%网络丢包下，语音清晰连续，视频清晰流畅，无卡顿、无马赛克；80%网络丢包下，声音清晰，不影响会议正常进行；支持≥7×24 小时连续正常工作 11)支持 SM2、SM3、SM4 国密加密算法。支持 SIP(TLS/SRTP)信令和媒体流加密、AES 加密算法、H.235 媒体流加密、H.235 认证和信令完整性校验 12)支持≥7×24 小时连续正常工作 13)支持会议中每个会场观看独立的多画面，每个会场的多画面模式及多画面中所有分屏会场可设置，最大可设置 25 多画面		

3	高清视频会议终端	1）与 MCU 同品牌，采用国产自主编解码芯片，采用分体式结构，嵌入式操作系统，非 PC 架构、非工控机架构。 2)支持 4K30fps、1080P50/60fps、1080P25/30fps、720P50/60fps、720P25/30fps 等分辨率。本次项目配置 1080P30fps 对称编解码能力。支持后续升级至 4K30fps 分辨率。 3)支持 H.265、H.264 HP、H.264 BP 等图像编码协议，支持 ITU-T H.239、IETF BFCP 双流协议。 4）支持 1Mbps 会议带宽下，实现 4K30 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； 5)提供至少 4 路高清视频输入接口、至少 3 路高清视频输出接口；支持≥5 路音频输入接口、≥5 路音频输出接口，至少具备卡侬头、RCA 等音频接口。 6)支持 IPV4 和 IPV6 双协议栈；支持在 H.323 协议下，H.235 信令加密； 支持在 SIP 下，TLS、SRTP 加密；支持 AES 媒体流加密算法，保证会议安全。 7）标配触控终端，触控屏尺寸≥10 英寸，分辨率≥1280×800；支持终端休眠和唤醒、创建会议、静音/闭音、音量调节、摄像机 PTZ 控制、预置位调用、双流共享、呼叫/挂断会场、添加/删除会场、观看/广播会场、多画面设置、声控切换、结束会议等功能。	台	2

4	高清摄像头	1）须与终端同一品牌，支持图像倒转功能，方便摄像机安装在天花板上。 2）支持≥851 万像素 1/2.5 英寸 CMOS 成像芯片，支持 WDR 图像数字宽动态功能。 3）支持 4K30fps、1080P60fps、1080P30fps 等视频输出格式。 4）支持≥12 倍光学变焦；水平转动范围：≥+/-110°，垂直转动范围：≥+/- 30°。 5）支持≥254 个预置位；支持≥1 路高清视频输出接口。。 6）支持≥2 个 RS-232 控制接口，支持标准 VISCA 控制协议；支持红外透传功能，实现终端遥控器通过摄像机控制机房内会议终端，方便调试； 7）支持自动白平衡（AWB）、自动曝光（AE）、自动聚焦（AF）功能。	个	4
5	麦克风	1）须与终端同一品牌。 2）数字阵列麦克风，支持 360° 全向拾音，拾音距离≥6 米。 3）支持终端供电，不需要额外电源。 4）支持回声抵消、自动增益控制、自动噪声抑制。	个	2
6	投影仪	投影技术 3LCD 显示芯片 0.76 英寸芯片 亮度 5500 流明 对比度 15000:1 标准分辨率 WUXGA（1920*1200）	个	1

		扫描频率水平：15-92kHz 垂直：50-85Hz 光源参数 光源类型超高压汞灯 光源功率 300W 光源寿命正常模式：5000 小时，经济模式：10000 小时 投影参数 变焦方式手动变焦 聚焦方式手动聚焦 变焦比 1.6X 光圈范围 F=1.5-2.0 实际焦距 f=23-38.4mm 投射比 1.38：1(变焦：广角) 2.28：1(变焦：长焦) 投影距离 1.46-8.95m（变焦：广角） 2.43-14.79m（变焦：长焦） 投影尺寸 50-300 英寸 屏幕比例 16:10 色彩数目 10.7 亿色 画面调节水平：±30 度 垂直：±30 度 投影方式正投，背投，吊顶 系统参数		

		无线功能 WIFI 扬声器 16W 其它系统参数智能设备投影，网络 4 画面投影，网络监控 接口参数 输入接口 2×HDMI（HDMI 1 兼容 MHL） 1×视频输入：RJ45 1×视频输入：RCA 2×音频输入：RCA（白 x1，红 x1） 2×视频输入：D-sub 15 针 1×视频输入：HD-BaseT 2×音频输入：迷你立体声 输出接口 1×视频输出：D-sub 15 针（与计算机 2 接口兼容，仅输出 Computer1 信号） 1×音频输出：迷你立体声 控制接口 1×USB A 型 1×RS-232C（D-sub 9 针） 1×USB B 型 规格参数 产品噪音经济模式：29dB 电源功率正常模式：425W，经济模式：323W，待机功率：0.31W 电源性能 AC100-240V，50/60Hz，4.5-2.0A 适用环境工作温度：5-40℃ 工作湿度：20%-80%（未结露）		

		存储温度：-10-60℃ 存储湿度：10%-90%（未结露） 其它参数开关机功能：直接开关机，开机 LOGO 自定义，自动监测信号源开机 技术功能：快速四角调节，Home Screen，演示手势，高海拔模式，自动信号源搜索，日程管理，聚焦帮助，Screen Fit，双画面并列投影		
7	会议室智慧屏（86寸）	1）采用一体化设计，具备内置摄像头、麦克风、扬声器、触摸屏等，外部无任何可见内部功能模块及连接线； 2)液晶屏显示尺寸≥86 英寸，采用 A+规屏；显示比例 16:9；分辨率≥3840*2160，可视角度≥178°，屏幕显示灰度分辨率等级达到 256 级以上灰阶； 3）采用红外感应技术，在双系统下均支持不少于 20 点触控，触摸分辨率≥32768（W）*32768（D）；触摸精度≤±1mm；触摸高度≤2mm；最小识别直径≤2mm； 4）屏体采用硬件防蓝光设计，无需通过按键操作，默认达到防蓝光效果。 5）▲采用国产化的主要元器件，包括但不限于音视频硬件编解码单元、CPU 处理单元、可编程逻辑芯片、摄像机镜头等。（提供具有 CNAS 或 CMA 机构认可的第三方检测机构出具的检测报告复印件并加盖厂家公章或投标专用章） 6）内置一体化摄像头，像素≥800 万，镜头水平视角≥80°、垂直视角≥50°，可拍摄不低于 4K 30fps 的高清视频画面。	台	2

		6）提供内置嵌入式国产操作系统或 Android11 系统，ROM≥64GB，RAM≥8GB，支持在线升级，系统主页面提供≥6 个应用程序，并可以根据使用需求随意替换，内置≥6 个非独立外扩展的麦克风，支持前向≥180°拾音，拾音距离≥12 米； 7）嵌入式操作系统下须内置电子白板，书写延时≤25ms，支持通过自定义书写颜色，使用者可进行手写、绘制、擦除、标注、保存、翻页、白板缩放、白板锁定等功能。 8）支持语音及人脸图像跟踪功能，自动切换发言人特写画面，无需人工干预，声源定位精度≤1 度，跟踪定位后可进行不小于 2 倍的画面放大； 9）支持 ITUT H.323 和 IETF SIP 通信协议，支持音视频会议，具备自主发起多方会议的功能、可实现广播会场、观看会场、添加/删除会场、静闭音、结束会议等功能，可同时显示远端图像、本端图像和辅流图像。 10）支持音视频会议，采用硬件编解码方式，非 PC 结构，稳定可靠。支持 4K、1080P、720P 视频解码能力，非安装第三方 APP 功能。 11）具有良好的视频处理能力，呼叫带宽范围支持 1Mbps - 8Mbps。在 384Kbps 带宽下可实现 1080P 30fps 图像格式编解码，在 256Kbps 带宽可下实现 720P 30fps 图像格式编解码，最大限度节省用户网络资源。。 12）内置无线投屏接收器，可选择配套同品牌智慧投屏器进行匹配，匹配完成后 PC 画面及音频可通过接入智慧投屏器		

		传输到设备上显示，且支持通过触摸屏反向控制 PC 的共享桌面； 13）带落地支架		

8	会议室智慧屏（65寸）	1)采用一体化设计，具备内置摄像头、麦克风、扬声器、触摸屏，整体美观、大方，可以提供统一的维保和服务。 2)一体化设计，高度集成化，采用全包裹设计， 标配不少于 1 个全高清红外触控显示屏，显示屏尺寸不低于 65 英寸。显示器物理分辨率 3840*2160,显示比例 16:9。可视角度≥178°。 3)采用红外感应技术，在双系统下均支持不少于 20 点触控，触摸分辨率≥32768（W）*32768（D）；触摸精度≤±1mm；触摸高度≤2mm；最小识别直径≤2mm。 4)支持电子白板实现手写、绘制、擦除、标注、截图、背景颜色自定义、白板缩放/锁定等功能。 5)内置摄像机支持 4K 视频输出格式，水平视角不低于 80°，垂直视角不低于 50°。 6)内置扬声器支持 100HZ-20KHZ 频域，2 个全频单元和 2 个高频单元，支持立体声， 7)内置内置≥6 个非独立外扩展的麦克风，可用于音频进行采集，拾音角度≥180°，拾音距离≥10 米。 8)内置无线模块，双 WI-F 模块，频率 2.4GHZ+5GHZ,嵌入式 Android 操作系统下，内置互动白板须支持 2 种以上书写笔头，书写延时≤25ms，支持 8 种以上书写颜色，使用者可对书写内容进行选择，移动，缩放，删除。 9)采用国产化的主要元器件，包括但不限于 CPU 处理单元、可编程逻辑芯片、时钟芯片等。	台	2

		10)内置安卓系统， ROM≥32GB，RAM≥4GB，系统版本≥Android 9.0，支持在线升级；安卓主页面提供≥6 个应用程序，并可以根据使用需求随意替换。 11)前置接口：≥2 个 USB，侧置接口：USB≥2 个，HDMI IN≥2 个，HDMI OUT≥1 个， 12)支持多种投屏方式，须包括但不限于 APP 投屏、智慧投屏器、NFC 一碰投屏、手机下拉菜单软投屏等方式。 13)支持断点续传功能，终端升级过程中发生网络中断、断电重启，恢复后可断点续传，避免升级失败。		

9	各部门智慧屏（65寸）	1)采用一体化设计，具备内置摄像头、麦克风、扬声器、触摸屏，整体美观、大方，可以提供统一的维保和服务。 2)一体化设计，高度集成化，采用全包裹设计， 标配不少于 1 个全高清红外触控显示屏，显示屏尺寸不低于 65 英寸。显示器物理分辨率 3840*2160,显示比例 16:9。可视角度≥178°。 3)采用红外感应技术，在双系统下均支持不少于 20 点触控，触摸分辨率≥32768（W）*32768（D）；触摸精度≤±1mm；触摸高度≤2mm；最小识别直径≤2mm。 4)支持电子白板实现手写、绘制、擦除、标注、截图、背景颜色自定义、白板缩放/锁定等功能。 5)内置摄像机支持 4K 视频输出格式，水平视角不低于 80°，垂直视角不低于 50°。 6)内置扬声器支持 100HZ-20KHZ 频域，2 个全频单元和 2 个高频单元，支持立体声， 7)内置≥6 个非独立外扩展的麦克风，可用于音频进行采集，拾音角度≥180°，拾音距离≥10 米。 8)内置无线模块，双 WI-F 模块，频率 2.4GHZ+5GHZ,嵌入式 Android 操作系统下，内置互动白板须支持 2 种以上书写笔头，书写延时≤25ms，支持 8 种以上书写颜色，使用者可对书写内容进行选择，移动，缩放，删除。 9)采用国产化的主要元器件，包括但不限于 CPU 处理单元、可编程逻辑芯片、时钟芯片等。	台	10

		10)内置安卓系统， ROM≥32GB，RAM≥4GB，系统版本≥Android 9.0，支持在线升级；安卓主页面提供≥6 个应用程序，并可以根据使用需求随意替换。 11)前置接口：≥2 个 USB，侧置接口：USB≥2 个，HDMI IN≥2 个，HDMI OUT≥1 个， 12)支持多种投屏方式，须包括但不限于 APP 投屏、智慧投屏器、NFC 一碰投屏、手机下拉菜单软投屏等方式。 13)支持断点续传功能，终端升级过程中发生网络中断、断电重启，恢复后可断点续传，避免升级失败。		
10	办公电脑	I5-10400 2.9GHz 6 核 12 线程；内存：8GB/2666 DDR4；硬盘：256GB M.2 SSD；显卡：集成；蓝牙+WiFI6;WIN10，23.8 寸显示器	台	4
	小计 5			
1.6	**车辆通行管理子系统**			
1	出入	杆件类型直杆；支持杆长 4 米；起杆速度 2S；RS-485 接口 1	台	6

	口道闸	个；I/O 接口 5 个（升、降、地感 1、地感 2、防砸）；状态输出 3 路（开到位、关到位、红绿灯）；防砸功能支持：压力波防砸、雷达防砸、线圈防砸、红外防砸；远程遥控支持遥控器远程开关，最大距离 50m；防护等级 IP54；供电方式 AC186~264V		
2	道闸杆件	颜色红白相间；外壳材料铝合金	根	6
3	防砸雷达	检测目标人、车；在线调试支持（串口、APP 通过 wifi 进行调试）；升级功能支持（串口、APP 通过 wifi 在线升级）；检测区域 0.3~6m（可调）；防砸区域 0~2m（可调）	个	6
4	电源适配器	AC220V 转 DC12V 电源适配器，可用于给雷达	个	6
5	雷达调试线	USB 转 RS-485/422 转换器-UT-891	条	1
6	杆式抓拍一体机	显示屏 LED 屏（4 行 4 字，支持红绿黄三色显示）；显示屏亮度≥5000cd/㎡，可调并可根据环境亮度自适应；显示屏分辨率 4096Dots（64x64，4 行 4 字），点间距 4.0mm；传感器类型 1/2.8 英寸 CMOS；镜头标配 2.7~13.5mm 电动变焦镜头；补光灯数量 3 颗（暖光灯，色温为 3000K，亮度可自动调）；图像分辨率 1920×1080（不包含 OSD 黑边）；视频压缩标准 MJPEG;H.264H;H.264M;H.264B;H.265；抓拍距离	个	6

		2.5~8m；二维码显示支持；语音功能支持语音播报；屏幕坏点检测支持；除雾功能支持自动除雾；触发方式支持视频检测、I/O 线圈、雷达三种触发方式；车辆识别支持车型、车标、车系、车身颜色、车牌颜色、车牌号码、车牌类型、无牌车、新能源车牌识别 车牌识别率≥99.9%，车辆特征识别率≥95%；车辆检测车辆捕获率≥99.9%；视频结构化支持；OSD 信息叠加支持叠加时间、地点、车牌、车身颜色、防伪码、车标、触发源、车牌类型、车辆颜色、车辆类型、卡口方向、车系、置信度、车头朝向、自定义信息；防护等级 IP54		
7	出入口管理终端	USB 接口 4 个,2 个前置 USB3.0、2 个后置 USB3.0；操作界面本地 GUI 操作；操作系统 windows 操作系统；多路回放 25 路 1080P；解码能力 25 路 1080P；视频输出 1 路 VGA 输出，2 路 HDMI 输出；网络接口 2 个 RJ-45，10/100/1000Mbps 自适应以太网口（千兆电口）；网络协议 HTTP、HTTPS、TCP/IP、IPv4、UDP；主处理器工业级嵌入式微控制器	台	4
	小计 6			
1.7	**防疫绿码管理子系统**			

1	测温健康码核验一体机	1、7 寸触摸屏 2、100000 张人脸底库 3、二维码扫码 4、支持健康码展示和语音提示 5、支持体温异常报警信息及语音提示 6、支持未戴口罩提醒或未戴口罩拦截 7、支持测温功能，温度范围：30℃~45℃，测温误差≤±0.5℃；	台	5
2	安装支架	立式落地支架	个	5
	小计 7			
1.8	**一键报警子系统**			
1	一键报警盒	采用铝合金面板 采用 200 万像素低照度 CMOS 摄像头、星光级图像传感器； 支持自动补光，夜视； 支持双向语音对讲； 支持一键报警，紧急求助； 支持语音播放； 支持明装装；	台	66

2	报警对讲管理机	采用 10 寸全玻璃触摸显示屏，屏幕分辨率 1024*600 支持和报警柱、紧急求助终端的双向实时对讲 支持同时监视 4 路 VTA、IPC 的画面 支持 SD 卡扩展，在报警柱、紧急求助终端对讲和监视时进行录像和抓拍图片 支持免提、听筒和鹅静麦自由切换。 支持桌面安装，支架 0°～45°可调。 支持 HDMI 输出，最大分辨率 1024*600 支持管理机之前的实时双向可视对讲。 管理机可独立管理前端报警柱和紧急求助终端，独立管理能力 120 路	台	1
	小计 8			
1.9	**无人机远程监控系统**			
1	无人机远程监控系统	租用	年	3

	小计9			
1.10	**园区电子围网系统**			
1	周界警戒摄像机（澄迈园区）	1)传感器类型 1/2.7 英寸 CMOS；像素不低于 400 万； 2)最低照度≤0.002Lux(彩色模式)；≤0.0002Lux(黑白模式)；0Lux(补光灯开启)。 3)最大补光距离 50m（红外视频监控距离）30m（暖光视频监控距离） 10m（暖光人脸检测距离）； 4)镜头类型定焦；镜头焦距 3.6mm（6mm 等可选）； 5)周界防范绊线入侵；区域入侵；快速移动；徘徊检测；人员聚集；停车检测；支持人脸检测； 6)视频压缩标准 H.265；H.264； 7)报警事件无 SD 卡；SD 卡空间不足；SD 卡出错；网络断开；IP 冲突；非法访问；动态检测； 8)灯光报警；声音报警（内置语音可选，支持用户自定义语音导入）； 9)接入标准 ONVIF；GB/T28181；GA/T1400； 10）工作温度：-30℃~60℃，工作湿度：5%~95%(无冷凝)； 11）防护等级 IP67。	个	150
2	监控	立杆高度 3 米，悬臂长度按现场环境 1-3 米定制，热镀，一	个	7

	立杆	杆一横臂		5
3	外加横杆	悬臂长度按现场环境 1-3 米定制，热镀	个	75
4	立杆底座基础	摄像机立杆基础底座尺寸为 1.2mX1.2mX1.2m，包含地锚、基础、开挖、回填、机械费、人工费、垃圾外运等	套	75
5	立杆地笼	与立杆大小配套	个	75
6	8 口接入交换机	8 个百兆电口	个	75
7	室外智能设备箱	1.防雨户外箱体：一体化模具成型。 2.维护终端：220VAC 输入，5 路 220V 远程可控输出，3 路 12V 远程 可控输出，2 路干节点输入，支持后备电源输入、RS485、RS232 扩 展接口。 3.配电模块：2 路 220V 输出，2 路光端机供电输出，3 路摄像机供电输出，额定电流 10A. 4.微型断路器：2P 导轨式空开，额定电流 16A， 5.电源防雷：单 AC220V 电源防雷，支持远程状态检测，标称放电	个	75

		电流：20KA，最大放电电流：40KA，最大持续运行电压：385V，额 定电压：220V，2P DIN35mm 标准导轨安装		
8	自动重合闸	工作电压：220V AC 工作电压可变范围：85-300V AC 额定负载电流：10A 抗雷击能力：10kA 漏电不动作电流：15mA 漏电动作电流：30mA 过流动作时间：2S 短路动作时间：30MS 漏电不动作电流：≤15MA	个	75
9	避雷针	定制、长度：1 米	个	75
10	信号防雷器	V2/RJ45，可防感应雷和直击雷（球机、枪机）	个	75
11	防雷插座板	8 插位	个	75
12	接地铜线	2.5mm2	项	75

13	镀锌圆钢	Φ12	项	75
14	扁钢	4X40mm	项	75
15	角铁	5X50X2000mm	项	75
16	主干电源线	主干电源线 RVV3*4mm2（每个监控立杆点取电平均按照 250 米计算）	米	18750
17	支路电源线	支路电源线 RVV3*1.0mm2（每个监控点取电平均按照 20 米计算）	米	15000
18	PVC管	PVC25 主干电缆敷设管	米	18750
19	PVC管	PVC20 支杆电缆敷设管	米	150

				0
20	过路钢管	SC50 过路钢管（开挖及回填）	米	1000
21	拖拉管	定向顶管 1xΦ110(PE)	米	1500
22	超五类屏蔽双绞线	超 5 类 4 对室外阻水电缆，每个点以 20 米估算	米	1500
23	水晶头	RJ45 水晶头	个	300
	小计 10			
1.11	**卡口 LED 引导屏升级改**			

	造			
1	通道LED引导大屏	1、驱动器件：恒流 IC 2、驱动方式： 1/4 3、刷新频率：≥380Hz；帧频： ≥60Hz 4、灰度/颜色：显示 66536 颜色；亮度：≥5000cd/m2 5、亮度调节方式：软件 16 级可调 6、显示内容：文字、图片、视频、时钟、日期、温度、湿度等 7、控制系统采用：网口或 USB 传输（可选） 8、平均无故障时间：≥10000 小时；寿命：5 万小时 9、平整度：任意相邻像素间≤0.5mm；模组拼接间隙＜1mm ； 10、均匀性：像素光强、模组亮度均匀；盲点率：＜0.0002 11、开关电源负荷：5V/40A、5V/30A 12、计算机显示模式：1024×768 13、有效通讯距离：网线 100m（无中继），多模光纤 500m，单模光纤 20km	台	2
2	LED引导屏管理软件	1、编辑 LED 引导屏显示内容； 2、控制 LED 引导屏显示编辑好的内容。	套	1
	小计11			

二	**园区智慧路灯系统**			
1	园区智慧路灯平台软件	照明控制系统，广告发布，视频监控，环境监测系统，wifi管理，充电桩管理系统，广播系统，紧急呼叫系统	套	1
2	单灯控制器	IP65 防水,一路调光输出，一路单灯电流、电压、功率、坏灯检测功能;输入电源：AC 85～265V 50/60Hz;输出电源：AC 85～265V 50/60Hz;具有电流、电压、功率、用电能耗检测功能;1 路开关和 0～10V 或 PWM 调光信号输出的功能;监控灯具工作状态，异常情况输出报警;单灯自定义分组控制;本地定时、经纬度控制功能;具有过流保护、灯具状况检测、缺省亮灯等功能;适用于 LED 灯、高压钠灯、金卤灯等灯具的开关和调光使用;基于安全的过载保护设计;无线频点：ZIGBEE/LORA/NB--IOT/4G;工业级工作温度范围：-40℃～+85℃;安装简单方便，能在几秒钟内响应中心发送的指令。	台	84
3	集中管理器	三相统计，回路控制，策略,定时，含三年流量，每个月流量 30M;通信上行 4G，下线 ZIGBEE，采集三相电压、电流和功率；支持本地经纬度或定时策略控制回路开光，支持传感器和智能电表接入；工作电压 85V-420V,整机功耗 2W，防浪	台	5

		涌等级 6KV，支持 8 路		
4	智慧灯杆（8 米）	灯杆高度：8M（壁厚 5MM）单灯头，表面镀锌喷塑;选材：Q235 或 Q345 钢材;地笼按尺寸定制、外形按尺寸定制、预留智能设备安装位置/可集成灯控、一键报警、广播、摄像机、信息发布、环境监测、充电桩等模块	套	80
5	智慧灯杆（12 米）	灯杆高度：12M（壁厚 5MM）单灯头，表面镀锌喷塑;选材：Q235 或 Q345 钢材;地笼按尺寸定制、外形按尺寸定制、预留智能设备安装位置/可集成灯控、一键报警、广播、摄像机、信息发布、环境监测、充电桩等模块	套	4
6	LED 光源	功率 120W，二模，显色指数≥Ra70,光效≥110LM/W，色温 2800K-6500K	套	84
7	驱动电源	保护功能：输出短路、输出过压、过温等三重保护;智能控制方式：0-10V 调光;防护等级：IP67;工作温度：-40℃-+60℃;工作湿度：10%RH-95%RH 无冷凝	台	84
8	IP 音柱	1. 一体化壁挂式设计、整合网络音频解码，数字功放及音箱。2. 采用高速工业级双核(ARM+DSP)芯片、启动时间≤1 秒。3. 内置高真保线性阵列扬声器和立体声 D 类功率放大器。4. 内置回路检测功能、可远程监听扬声器工作状态、轻松维护。5. 终端支持服务软件远程控制方式调节音量。6. 标准 RJ45 网络接口、有以太网口的地方即可接入、支持跨网段和跨路由。电源、功耗 DC48V/2.7A，≤30W;网络通讯协议 TCP/IP、UDP、ARP、ICMP、IGMP;音频编码 MP2/MP3/PCM/ADPCM;音频采样、位率 8kHz～44.1kHz，	台	20

		16bit， 8kbps-320kbps;信噪比、频响 ≥90dB，50Hz-15KHz(±3dB);内置功放功率 2x30W(8Ω定阻);工作温度、湿度 -10℃～50℃，≤90%RH（无结露）		
9	LED全彩显示屏	点间距：3.57mm，像素组成：SMD 1919 定制，分 辨 率：168*336，亮 度：≥ 7000nit，模组尺寸：200mm*200mm，平均功率：170W/台，工作温度：-40℃~+80℃，RH=10~90%，工作湿度：10～90%（无凝结），智能风冷	套	54
10	物联网网关	智能外设供电及通讯设备，强弱电一体，空开，智慧灯杆智能网关，用于灯杆上智能设备汇聚，并将其信号转化为网络信号上传平台，只支持 RJ45 电口接入网络，适用于灯杆位置离网络接入点位置较近，距离不超过 100 米的场景使用	台	84
11	光模块	工业级千兆光模块，单模双纤 LC 模口 20KM 及光纤跳线	个	84
12	配件/辅材	电源、防雷模块、连接网线、电源线、辅材	套	84
13	电力电缆	1.名称:低压电缆。2.规格:YJV22-1KV-5X16	米	2520
14	配管	1.名称:PVC 管。2.材质:塑料。3.规格:Φ75。	米	2520

15	超五类屏蔽双绞线	超5类4对室外阻水电缆，每根灯杆以30米估算	米	2520
	小计12			
三	**园区智慧消防系统**			
1	智慧消防系统平台软件	实时报警功能：系统收到报警信息后，显示报警点信息（编号、名称、报警类型、位置、时间等），通过声光告警提示值班操作人员，并对报警点进行定位，在楼层布局图中显示具体的报警对象，也可以将建筑物位置在GIS地图上定位。 消防系统运行情况一览图：将消防联网系统的信息在一张总图上显示，对所管理的楼宇建筑物内的消防设备运行情况能一目了然。包括火灾报警控制器数量、各类消防部件（烟感、手报等）总数、当前设备完好率、完好率趋势分析图、告警趋势图等。 应急预案管理：可以根据发生事件的具体条件，直接调用预案系统的预案信息，从而实现预案与应急事件处理的联动。在联动过程中，预案系统可以根据事件响应级别及类型，自动匹配相关预案，然后启动相关预案。	套	1

		楼宇资料数据管理：联系人基本信息；建筑物信息，包括建筑名称，建筑结构，楼层数；消防设备基本信息： 每个种类的消防设备的主机型号，消防部件（烟感、温感等）的数量，以及消防部件的类型、编号、名称等； 图形制作功能：提供图形制作工具，完成图形数据输入，包括编制各类图元，分别表示各类消防设备部件（感烟探测器、感温探测器、防火门等）；楼层图制作； 操作人员账号权限管理：将操作人员分成不同的组，具有不同的权限。每个人都建立账号和密码。 数据分析：通过对数据库的各类信息进行数据分析，提供信息查询服务，为单位领导分析企业消防安全水平和进行决策提供依据。		
2	手机微信服务软件	报警信息实时推送：微信用户可实现分级管理，将火警、故障等各类报警信息实时推送到有管理权限的相关人员手机上，也可以根据需要设置推送的信息。 消防设备的告警信息汇总：查看该微信用户有权限管理的消防设备的运行信息汇总。包括联网单位（建筑物）的总数、消防设备部件总数（烟感、温感、手报等），以及当前存在的各类告警分类汇总，包括火警总数、故障总数等。 查询统计功能：显示消防部件的完好率和当日、最近 7 天、30 天的各类告警信息总数和具体报警内容	套	1
3	传输设备	有 3C 认证证书，支持以太网或 4G 通信，具有主备电源 传输时间：≤10S	台	25

		故障报警时间：小于等于 100S 备电工作时间：≥8h		
4	消防水系统数据采集终端	8 路模拟量，16 路状态量，4G 无线通信 模拟量输入：支持 8 路 开关量：最大 16 路。	台	25
5	压力变送器	测量消防水管水压，4~20ma 信号输出 补偿温度：-10~70℃ 工作温度：-10~70℃。 综合精度：0.5 级 零点温度漂移：±1.5%FS/℃ 长期稳定性：≤0.2%FS/年	个	50
6	无线水压采集终端	测量最不利点水压，NB 或 4G 无线通信 参数配置：支持本地蓝牙，远程。 工业时钟：内置，自动校时。 防护等级：IP65，防爆。 精度：0.5 级 工作电流：低功耗待机<45uA，发送平均电流 60mA。	个	25
7	无线液位采集	测量消防水池液位，NB 或 4G 无线通信 参数配置：支持本地蓝牙，远程。 工业时钟：内置，自动校时。	个	25

	终端	防护等级：IP65。 精度：0.5 级 工作电流：低功耗待机<45uA，发送平均电流 60mA。		
8	防排烟系统数据采集终端	8 路状态量，4G 无线通信 模拟量输入：支持 4 路 开关量：最大 8 路。	台	25
9	辅材	包括三通、阀门、线缆等辅材,以及安装施工	套	25
	小计 13			
四	**园区智慧能耗监测系统**			
1	智慧能效监测系统平台	电能数据实时监测和报警：电能数据包括电流、电压、电度、有功功率、无功功率、频率等，对每个电能数据可设置合理的数值范围，当超出这个范围后（如电流过大、电压偏高、功率因素过低。），则有报警提示。 用电安全数据实时监测和报警：实时采集用电安全报警数据	套	1

	软件	（漏电、短路、电缆温度等），并将报警信息实时显示在监控界面上，通过声光告警提示操作人员。 水表数据实时监测：实时采集水表数据。 能耗统计：可以对用能对象按不同统计粒度的统计，并能生成多种能耗信息统计图形、曲线和报表。统计粒度有按年、按月、按天、指定日期、按小时、指定小时段等。 能耗分析：提供各种的能耗分析方式，相同能耗参数不同时间段的数据对比；不同能耗参数在相同时间段的数据对比；可以对多个电能参数的变化趋势进行分析、对比。		
2	手机微信服务软件	报警信息推送功能：当发生数据异常、故障报警时能够及时自动将信息推送到手机上。 数据实时查询：实时查看现场设备采集的各类用电安全数据（漏电、电缆温度等）、电能参数（包括电压、电流、电度、有功功率、无功功率、功率因素等）、水表数据。 查看各类统计信息，包括提供选定时间段内用电安全告警信息如漏电报警、电流过载等信息的统计；各类能耗数据的排名等。	套	1
3	智慧用电监控装置	测量三相电流、电压、频率、功率因数、有功、无功、电能、剩余电流、温度等，具有漏电、温度、过压、欠压、过流报警功能,RS485 通信。	套	100
4	智能水表	RS485 通信，防护等级:IP68。 计量等级：2 级。	台	60

		电池寿命：>6 年。		
5	通信网关	支持以太网、4G 通信	台	20
6	辅材	包括线缆、管线等辅材,以及安装施工	套	20
	小计 14			
五	**智慧查验系统**			
1	**AR 查验单兵装备**			
1.1	AR 眼镜	1、一体机眼镜，可作为查验 PAD 配置使用； 2、采用光波导成像显示，拥有摄像头、麦克风、九轴、光感等传感器，提供第一视角视频，具备手势、语音交互功能； 3、支持独立的电池盒供电，电池容量≥4800mAh； 4、支持业务信息回显，显示分辨率不低于 1920×1080； 5、支持 Wifi direct 无线协议连接查验 PAD； 6、视频分辨率≥1200 万像素。	台	10

1.2	查验PAD	1、屏幕尺寸≥10 寸； 2、支持全网通； 3、内存≥4GB； 4、存储空间≥64GB； 5、可支持部署总署查验 APP（安卓版）及移动辅助查验 APP（安卓版），支持查验作业，查验单管理，查验作业记录，单兵后台协同（音视频通讯）。	套	10
1.3	执法记录仪	1、支持 5G 网络； 2、支持 4K 高清实时视频回传； 3、支持专业防抖，摄录稳定； 4、支持 125 度水平广角，几何失真≤10°，支撑视频取证拍摄大视野画面； 5、具备红外夜视功能； 6、具有电信设备入网证； 7、支持 IP68 防护等级。 8、支持音视频通讯，一键呼叫，群组呼叫，AI 识别（车牌识别、人脸识别）	套	10
1.4	执法记录仪采集站	1、支持≥20 口并发采集； 2、支持 4K 高清播放； 3、支持≥8T 存储空间； 4、支持全自动采集充电; 5、支持自主设置优先采集口，数据安全保护； 6、支持 Type-c 与 Mini USB 双接口。	套	1

		7、支持离线视频回传、对接电子证据管理系统		
2	**AR 查验分析服务器**			
2.1	AI 推理服务器	1、国产品牌； 2、CPU：配置 2 颗国产 CPU，单 CPU 主频≥2.2GHz，物理核心数≥32； 3、内存：配置≥256GB DDR4 内存； 4、硬盘：配置≥6 块 1.92TB SSD 硬盘； 5、Raid 卡：配置 1 张磁盘阵列卡，支持 RAID 0/1； 6、网卡：配置≥4 个千兆 GE 网口和 4 个 10GE 光口（含光模块）； 7、AI 加速卡：配置≥4 个 AI 加速卡； 8、电源：配置冗余电源； 9、 ▲管理：内置国产化管理芯片，支持远程管理，投标时需提供相关芯片型号资料证明，并加盖厂家公章或投标专用章；	台	2

2.2	AI 训练服务器	1、国产 AI 训练服务器，设备高度≤4U，单台设备最高支持≥2 PFLOPS FP16 算力； 2、 CPU：配置 4 颗国产架构 CPU，单 CPU 物理核心数≥48，主频≥2.6GHz； 3、 内存：配置≥256GB DDR4 内存； 4、 硬盘：配置≥2 块 960GB SSD 硬盘； 5、 网卡：配置≥2*100Gb 光口（含光模块）； 6、 AI 加速卡：配置≥4 个 AI 加速卡或 AI 处理器，单卡或者单 AI 处理器提供算力≥256TFLOPS； 7、 管理：内置国产化管理芯片，支持远程管理。 8、 电源：配置冗余电源；	台	1
3	**AI 训练平台**			

3.1	AI 训练平台	一、支持通过 AI 推理，解决综保区海关查验的 AI 模型或镜像的管理、服务发布、资源统一调度管理的问题；支持通过 AI 训练，解决口岸监管的 AI 模型基于现场图形数据的训练调优工作； 1）实时消息：通过 Rest 接口，对海关侧智能分析算法对现场视频识别的异常事件实时采集，利用 Flink、策略编排等进行预处理后传递给上层事件中心； 2）批量接入：通过批量数据采集，将海口海关可共享的业务系统数据及部分口岸侧提供到海关使用的结构化数据进行接入； 3）轻量化数据存储：根据 5G 智能单兵查验业务需求，构建的轻量化 OLAP 数据仓库，支持基于 Docker 容器的轻量化部署方式，提供高性能的数据查询和加载能力，提供轻量化数据存储对口岸数据进行数据集中处理、统计计算，生成口岸统计指标； 4）轻量化消息总线：消息总线基于开源 Kafka 架构实现，可为海口综保区(海关侧)的 AR 全景和 5G 智能单兵提供智能分析实时告警数据交互； 5）数据编排：提供图形化编排能力，对 5G 单兵智能查验需要集成的事件消息数据、结构化离线数据进行统计计算，包括轻量化 ETL 和流处理引擎； 6）数据接口：通过 Rest 接口和 JDBC 接口分别将处理的异常事件和海关统计指标共享到上层应用使用；	套	1

		7）数据集成与运营服务：针对 5G 智能单兵涉及的海关数据集成服务： 1、海口海关本地数据平台共享的口岸通关数据集成服务 2、单一窗口或综保区共享到海关的数据集成服务 3、海关侧监控视频涉及的智能分析识别的异常告警数据集成服务 AI 推理底座：主要解决综保区海关查验的 AI 模型或镜像的管理、服务发布、资源统一调度管理的问题。 AI 训练底座：主要解决口岸监管的 AI 模型基于现场图形数据的训练调优工作。 二、部署对接与运维要求： 1、AI 底座要求国产化且支持国产 NPU 服务器，提供模型运行环境 2、支持国产 AI 框架； 3、支持货物标签识别应用服务，提供算法将现场货物标签图片通过 AR 眼镜或 PAD 拍照后回传后台，移动辅助查验 APP 上显示识别出的文字信息； 4、支持车牌识别服务，进行车牌识别返回车牌结构化结果。 5、支持对边缘设备统一运维管理，支持对国产 NPU 边缘智能服务器的设备纳管、设备配置、固件升级、设备监控、OS 部署等全生命周期的管理能力，有效帮助运维人员提高运维效率、降低运维成本		

3.2	数据库	产品需为国产集中式关系型数据库，具有跨操作系统平台的能力 1、支持 Linux、麒麟、统信 UOS 等操作系统等； 2、支持 INTEL、鲲鹏、飞腾等处理器； 3、支持 PL/pgSQL 过程语言；支持 JDBC/ODBC 标准接口； 4、支持 number、date、blob/clob、varchar2 等数据类型； 5、支持序列与自增列，支持事件触发器； 6、支持 connect by 层次查询； 7、支持 Package、物化视图； 8、支持 B-TREE 索引、GIN 倒排索引、Gist 空间索引等多种索引访问方式； 9、支持并配置 HA 故障转移集群和主备同步技术，并且能够支持故障转移功能，支持主从、一主多从等架构，从库能设置延迟复制和优选提交复制； 10、支持逻辑备份恢复、物理备份恢复，物理备份支持增量备份和联机热备份技术，逻辑和物理备份均支持本地和远程备份； 11、过程性语言支持自治事务，包括存储过程、自定义函数、触发器以及匿名块。存储过程支持自治事务的嵌套调用； 12、支持系统性能监控动态视图，TOP SQL 信息、内存管理信息、事务信息、线程信息、操作历史等信息； 13、支持创建表分区，包括 range、list、hash、interval 间隔，支持两级分区方式；	套	2

		14、支持自主访问控制、基于安全标签的强制访问控制、用户角色三权分立、审计、加密、身份识别与验证等安全功能； 15、支持安全管理功能和审计功能； 16、支持全密态等值查询功能和动态脱敏功能； 17、需兼容 MySQL 常用数据类型，特色函数，常用语法，数据类型包括 Tinyint、Bit、Datetime、LONGTEXT、LONGBLOB 等，语法包括表字段 AUTO_INCREMENT 属性、REPLACE INTO、SELECT INTO OUTFILE、DISTINCT 列可使用非 ORDER BY 列、SELECT 字段列表可以使用非 GROUP BY 列； 18、内置内存引擎，能够实现在同一个实例中内存表跟普通的磁盘表的共存，内存表支持 ACID、常用 SQL 语法、存储过程和数据持久化等功能特性，支持 Masstree 索引的优化技术； 19、支持行存表和列存表，要求行存表和列存表支持在同一个事务内增删改查，并且支持在同一个查询命令中进行多表关联； 20、支持 AI 功能，能够根据数据库访问负载分析并且自动调整数据库参数以优化性能，能够根据数据库访问特征智能推荐索引； 21、支持通信和存储加密功能，支持字段级别和库级别的磁盘文件级加密，支持多种加密算法； 22、支持基于成本的全局优化功能，实现基于成本的查询机制，能够选择合适的查询计划；数据库内核支持并行查询技		

		术，且能够完全自动化启动并行查询，无需人工启动或干预		
	小计 15			
4	5G 智能单兵查验平台软件			

4.1	5G 智能单兵查验平台	包含 AR 眼镜前端控制、移动辅助查验前端、移动辅助查验后台、电子证据管理系统、智能识别算法等功能模块： 1、支持调用基于国产化软硬件的 AI 平台的智能辅助识别服务（货物标签识别、车牌识别）； 2、支持和电子证据管理系统交互，传递查验单号，并从电子证据管理系统读取执法录证视频； 3、支持根据查验单号检索执法录证视频，并提供下载能力； 4、支持执法记录仪视频的集中回传； 5、支持控制 AR 眼镜与查验 Pad 无线连接，支持稳定传输业务数据、图片、视频； 6、支持调用后台货物识别服务，进行货物的智能归类，返回货物的海关编码、税号和监管条件。	套	1
	小计 16			
5	**VR 硬件**			
5.1	VR 全景摄像机	1、4 镜头直播设备； 2、支持输出 4K/8K 直播码流； 3、支持 H.264/H.265 视频编码技术； 4、内置≥521G 固态存储； 5、内置≥2 个小型收声硅麦； 6、电池容量≥6800mAh； 7、支持轴陀螺仪+光流混合视频防抖技术；	台	2

		8、WIFI 遥控与图传距离≥30 米； 9、防护级别≥IP65； 10、支持全密封无风扇内置铜管制冷液体被动散热 含基座、杆件和安装		
5.2	VR 流媒体服务器	1.软硬一体化设备，内存≥ 32GB，硬盘≥ 512GB SSD； 2.支持 SRT 低延迟技术； 3.支持相机端及眼镜端语音双向对讲； 4.支持≥ 200 路直播机位； 5.支持最大观看终端数量≥ 1000 路；	台	1
5.3	VR 眼镜	1.支持 rtmp 流媒体协议 2.支持 srt 低延迟协议 3.支持 8k 分辨率解码 4.支持双向语音对讲 5.主体双眼分辨率≥ 3664*1920 6.连接方式：Wi-Fi 7.屏幕精细度≥ 773ppi，刷新率≥ 120Hz，屏幕材质：LCD； 8.视场角≥ 98 度 9.操作系统：Android10 10.机身存储≥ 128GB 11.运行内存≥ 6GB	台	2
	小计			

	17			
6	海关侧国产化云节点			
6.1	业务交换机	1、交换容量不少于 4.8Tbps，包转发率不少于 1600Mpps； 2、标准 1U 机架式设备； 3、提供不少于 48 个万兆光口，不少于 6 个 40G/100G 光口； 4、设备提供 1+1 冗余备份电源模块、3+1 冗余风扇模块； 5、整机可用缓存不少于 36MB； 6、CPU、LSW 均为国产化芯片； 7、支持 Access、Trunk 和 Hybrid 三种模式； 8、支持 M-LAG 或 vPC 或 DRNI 等跨机箱链路捆绑技术； 9、支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议； 10、支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议； 11、支持 IP 报文分片重组； 12、支持 L2 协议头、L3 协议和 L4 协议等的组合流分类； 13、支持微分段（IPv4 和 IPv6）； 14、支持防止 DOS、arp 攻击和 ICMP 攻击 15、配置：双电源，12 个万兆多模模块 16、支持硬件双向转发检测 BFD 协议，使得链路故障可以实	台	2

		现毫秒级的检测，提高设备的可靠性； 17、支持基于真实业务流的实时检测技术，可实时准确的进行网络故障检测； 18、支持 Netstream、sflow 流量分析功能； 19、支持 VxLAN OAM: VxLAN ping, VxLAN tracert；		
6.2	BMC 带外管理接入交换机	1、交换容量不少于 750Gbps，包转发率不少于 250Mpps； 2、标准 1U 机架式设备； 3、提供不少于 48 个千兆电口，不少于 4 个万兆光口； 4、提供冗余备份电源模块，冗余风扇模块； 5、支持 Access、Trunk 和 Hybrid 三种模式； 6、支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议； 7、支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议； 8、支持集群或堆叠多虚一技术，实现单一界面管理多台设备； 9、支持防止 DDOS、ARP 攻击和 ICMP 攻击； 10、支持 OPS 功能、Netstream 流量分析功能； 11、支持 IP、MAC、端口和 VLAN 的组合绑定； 12、支持端口隔离； 13、支持 ERPS 以太环保护协议（G.8032）； 14、支持配置回滚；	台	1

		15、配置：双电源，2 个万兆多模模块		
6.3	数据视频网闸	内网接口：6 个 10/100/1000Base-T 端口，4 个 SFP 插槽,2 个 SFP+插槽，1 个 Console 口，2 个 USB 口；≥64G 硬盘; 外网接口：6 个 10/100/1000Base-T 端口，4 个 SFP 插槽,2 个 SFP+插槽，1 个 Console 口，2 个 USB 口，≥64G 硬盘；应用层吞吐≥5Gbps ，应用层并发连接≥15 万条；功能模块：数据库同步、文件交换、数据库访问、视频模块、邮件访问、安全浏览、安全 FTP、定制模块、工控访问等；提供三年硬件维保。 支持文件同步，文件同步支持 FTP、SFTP、SMB、NFS 等协议； 支持 MySQL、ORACLE、ORACLE_RAC、SQLServer、DB2、SYBASE、POSTGRESQL 等常见数据库，支持神通、达梦、人大金仓、南大通用等国产数据库同步； 支持 MySQL、ORACLE、SQLServer、DB2、SYBASE、POSTGRESQL、达梦、神通、人大金仓等数据库的访问； 支持视频访问，支持 28181、DB33 标准。	台	1

6.4	查验超融合服务器	硬件配置参数： 1、 处理器：配置 2 颗国产 CPU，单 CPU 物理核心数≥32，主频≥2.2GHz； 2、 内存：配置≥512GB DDR4 内存； 3、 硬盘：系统盘配置≥2*1.2TB SAS 硬盘，缓存盘配置≥1*3.2TB NVMe SSD 硬盘，数据盘配置≥12*2.4TB 10K SAS 硬盘； 4、 Raid 卡：配置独立 RAID 卡，链路支持 12G，支持 RAID0、RAID1、RAID10 等以及磁盘直通； 5、 网卡：提供不少于 4 个千兆电口、4 个万兆光口（含光模块）， 6、 其它：冗余交流电源、风扇； 三、软件功能： 7、 设备须提供与硬件配置相对应的分布式块存储软件、超融合管理软件的授权，支持在统一个管理界面中监控和管理计算、存储、交换机、虚拟化平台等； 8、支持磁盘拔出和换位的容错功能，2 块磁盘被拔出，能够产生自动告警，5 分钟内互换槽位插入，系统不发生数据重构。 9、快速重构：磁盘故障时，系统能自动进行数据快速重构，1TB 重构时间≤15 分钟。 10、支持 EC 缩列功能，当节点故障时，自动调整 EC 配比，	台	3

		确保数据可靠性不降级。 11、 超融合存储系统支持重删压缩功能，压缩比≥10，性能下降≤15%； 12、 支持 Call Home 功能，可通过管理界面配置 7*24 小时自动将系统告警信息发送给原厂商，便于及时处理系统告警； 13、 系统健康巡检功能：支持对系统服务器、系统 OS、分布式存储、管理系统的健康状态检查，识别系统的风险和异常，支持定时系统巡检		

6.5	虚拟化软件套件	1.国产自主品牌虚拟化软件，基于 KVM 架构，可直接安装在国产化的物理服务器上，提供 6 个物理 CPU（单 CPU≥32 核）的虚拟化软件授权，至少包含虚拟化软件、虚拟化管理平台软件、虚拟化备份软件等授权； 2.支持虚拟机规格的在线或离线调整，包括 CPU、内存、硬盘、网卡等资源，支持重启生效； 3.提供虚拟机基本生命周期管理功能，支持删除、移动、克隆、迁移、VNC 登录、快照、导出、重启、关闭、强制重启、强制关闭等操作； 4.支持虚拟机的 CPU 的 Qos，支持控制虚拟机获得的最低/最高 CPU 计算能力； ▲5.支持虚拟机 HA，允许配置集群内 HA 预留的主机数量，以保证在虚拟机故障时有足够的资源进行切换，支持配置存储故障后是 HA 虚拟机还是不处理(提供产品彩页或功能截图并加盖厂家公章或投标专用章)； 6.支持虚拟机启动阶段的负载均衡策略，虚拟机启动时根据集群内主机的实时 CPU、内存负载情况动态选择运行的主机； 7.支持通过文件夹对虚拟机进行分组，不同类型的虚拟机实现逻辑分组管理，方便运维，文件夹深度最多可以支持 5 层，并可以对分组虚拟机批量进行关闭、启动、克隆等操作； 8.虚拟化平台使用存储设备时，须支持本地存储、IP-SAN、FC-SAN、NAS 等不同类型的存储设备，支持这些存储资源的添加、删除、查询、扫描；	台	1

		9.支持虚拟机离线或关机状态下，从一个存储设备迁移到另一个存储设备中，迁移过程中指定目的磁盘置备格式并指定迁移速率控制，并且可以支持带快照的虚拟机磁盘迁移； 10.支持虚拟交换机，通过对接受和发送的流量进行整形保证网络质量，至少支持平均带宽、峰值带宽、突发大小、优先级、DHCP 隔离、广播抑制、TCP 校验和的设置； 11.为保证业务连续性，虚拟化软件在 x86 和 ARM 场景支持与双活存储配合，实现本地存储高可用和同城双活容灾； 12.支持记录操作维护人员通过运维管理系统进行的操作日志。系统操作维护人员可以在运维管理系统中筛选并查看、导出、操作日志，不允许删除日志。		
	小计 18			
六	**机房及配套设施**			
6.1	**管委会机房改造**			

1	拆除原有地板原地面找平防尘处理	拆除原有地板，清理地面垃圾，地面找平，	m2	110
2	机房区原顶面防尘处理	基础凿平、刷水泥砂浆防水涂料	m2	200
3	顶面橡塑保温层	橡塑绝热材料、B1 级、厚度 20mm	m2	200
4	机房区铝合金天花板	乳白色烤漆、600mm*600mm*0.8mm、1.8 微孔	m2	200
5	配电	乳白色烤漆、600mm*600mm*0.8mm、1.8 微孔	m	1

	房铝合金天花板		200	
6	墙面橡塑保温层20mm厚	橡塑绝热材料、B1级、厚度20mm	m2	240
7	墙面彩钢板龙骨及附材	75mm*50mm*0.6mm	m2	240
8	主机房区域墙面彩钢板	1200mm*3000mm*13mm	m2	240
9	不锈钢地脚线	304哑光磨砂不锈钢板,高度80mm，厚度1.2mm	m	120

	80mm 高			
10	防火玻璃隔断	12mm 厚防火玻璃	m2	100
11	玻璃隔断上下支架	40 角钢，支架不锈钢包边	m	30
12	双开钢质防火门及安装	2200mm*1500mm 不锈钢	樘	2
13	防火玻璃平开门及安装	12mm 厚防火玻璃	樘	2
14	机房区及配电区抗	防静电地板 600mm（长）*600mm（宽）*32mm(厚)	m2	110

	静电地板			
15	配电柜、UPS承重安装钢支架	40角钢	个	12
16	机柜承重安装钢支架1000宽×500高	40角钢	个	20
17	安装挡鼠板	不锈钢	个	2
18	踏步	40mm*4mm角钢支架、304哑光磨砂不锈钢板	个	1

19	斜坡	铝合金花纹板	个	2
20	排水管	¢40PP-R 热熔管及配件	项	1
21	精密列头柜	标准列头柜，总市电输入开关：250A/3P*1，市电分配：插座 32A40 个、预留前端市电维修旁路接入孔位，保障可靠的维修特性；	台	2
22	IT 机柜	1、尺寸：600*1200*2000（42U），标准 19″机柜， 2、前门单开，后门双开，含顶底板(顶板两侧带走线孔，毛刷密封处理)，方孔条，横梁等； 3.通孔率＞80%，静态承重不少于 2500kg； 4、配置 2 对 PDU 安装板，2 条 100mm 宽垂直绑线板，左右安装；前后门配接地线，含并柜件、50 套卡扣螺母螺丝； 5.优质冷轧钢板：型材框架≥1.5mm；立柱≥2.0mm，方孔条≥2.0mm，横梁≥1.5mm；前后门板≥1.2mm； 6、前后门配置隐藏式走线槽； 7、木托运输，纸箱包装 ； 8、表面处理，环保纳米陶瓷技术和静电粉末喷涂，颜色黑色 RAL9005；	架	20
23	1U 盲面板	配 19”安装机架，机柜漏空挡板,塑料材质，阻止冷气流旁通，美观防尘，高度 1U，卡扣式安装	副	400
2	600	适用 600 宽机柜，单通道走线槽，强弱电分离则需要配置 2	个	4

4	机柜走线槽	个		0
25	冷仓门	适配双排通道宽度 1200mm，配套 1200mm 深机柜使用，含声光告警安装辅件；	套	2
26	有框门配套机柜侧门	适用用微模块最外侧侧门，带显示屏和读卡器孔位，带通道照明控制开关，配套 10 寸触摸屏使用，配套 1200mm 深机柜使用	个	8
27	有框门配套机柜侧门	适用用微模块最外侧侧门，带读卡器孔位，带通道照明控制开关，配套 1200mm 深机柜使用	副	18
28	LED 照明灯	安装在通道的两侧顶部。	套	2
29	天窗控制盒	集成控制盒，含翻转天窗控制，含烟感消防接口，可为 LED 灯，翻转天窗电磁锁以及全自动双开门电机供电。	个	2
30	应急开关	防止门禁失灵，应急出门使用	个	4

	附件			
31	标准天窗	尺寸：用于600mm宽机柜，1200mm宽通道；功能：可固定、可翻转（由电磁锁自动控制开启）。天窗开启实现与通道内消防告警信号联动，在消防状态下电磁锁打开，旋转天窗在重力作用下自动打开，保证灭火气体进入密封冷通道。天窗开启后冷通道的净高不小于2米，不影响日常维护工作和维护人员安全。	批	18
32	电缆	ZR-RVV 3*4，列头柜到机柜PDU	米	900
33	电缆	ZR-RVV3*25+1*16　空调电源线	米	100
34	电缆	120平方单芯电缆　　电池到UPS主机	米	150
35	电缆	ZR-RVV 4*95　UPS输出柜到列头柜	米	160
36	PDU电源	铝合金外壳 单路32A输入/10A国标12口 16A国标4口输出（带接线盒,带指示灯,垂直安装,面对机柜后门左、右侧安装）	套	40

37	UPS	1、功率模块 50KVA 1.0 功因 380Vac/50Hz,3U.1 块。200KW 机柜， 2、系统效率可达：96%； 3、电源制式：3Ph+N+PE，三相输入、三相输出； 4、输入电压：138～485VAC； 5、输入功率因数≥0.99； 6、UPS 功率模块内一个风扇异常时，模块可以继续工作，并可带 50%负载； 7、UPS 应采用集中控制的逻辑，集中控制单元需要 1+1 冗余； 8、机主支持锂电或铅酸，支持电池输入电压：360～528Vdc ； 9、抗震性能：满足 YD 5096-2005《通信用电源设备抗震性能检测规范》的要求 10、模块化不间断电源（UPS）厂商入选国家绿色数据中心先进适用技术产品目录，	个	2
38	电池组	12V 100AH 阀控式密封铅酸蓄电池组，含配套每套 176 节电池	套	2
39	精密空调	行级精密空调 室内机 制冷量 60kW 风冷型 水平前送风 含加热加湿 直流变频压缩机 EC 风机 电子膨胀阀 彩色触摸屏 柜体尺寸（W*D*H）600*1200*2000mm，配套 1200mm 深拼装机柜使用	台	1
40	机房消防	柜式七氟丙烷灭火，含报警配套	套	1

41	机房安防	安防设备：满足国密要求门禁系统：5 套处理器：32 位处理器　刷卡读卡器:读卡频率：13.56MHz 按键方式：触摸按键.可识别卡：国密 CPU 卡,卡片发卡器,支持发卡类型：ID 卡、Mifare 卡、身份证物料卡号（序列号）、普通 CPU 卡、国密 CPU 卡；USB2.0 接口；具有 2 个 Sim 卡尺寸的 PSAM 卡座；,通讯方式：RS485+Wiegand 工作电压：DC 12V 功耗：≤2W 管控门数:2 门　包括门磁与所有配件通讯方式:上行 TCP/IP 读卡器接口：RS485 和 Wiegand 双通讯接口 存储容量：10 万张卡和 30 万记录存储 工作电压：自带机箱和供电电源（AC220V 输入），工作电压 DC 12V，功耗≤4W（不带负载） 支持蓄电池（303700655 OT7-12 蓄电池）接入，设备本身不含蓄电池； 支持消防功能，支持蓄电池功能主机应能对门的开启方式，卡的各种使用权限进行组合设置，实现不同场景的权限管理，故应具有以下功能：反潜回（防跟随）功能；多重卡认证开门功能；多重卡+中心远程开门功能；多重卡+超级密码开门功能；多重卡+超级卡开门功能；超级权限开门；中心远程开门；支持身份证开门；支持银行卡开门；支持单向刷卡（指纹）和双向刷卡（指纹）开门。 主机应具有丰富的通讯接口、控制接口及拓展接口：TCP/IP 接口 1 个；上行 RS485 通讯接口 2 个；下行 RS485 通讯接口	套	1

		2 个；wiegand 通讯接口 2 个；可接入最多读卡器数量 4 个，其中 2 个 RS485 读卡器和 2 个 wiegand 读卡器；报警输入接口 4 个；事件输入接口 2 个；门磁输入接口 1 个；开门按钮接口 1 个；电锁输出接口 1 个；报警输出接口 2 个。 主机应具防区报警功能，有 4 个防区输入端口，具有防短、防剪功能，能够联动报警输出。视频设备：400 万 1/3″CMOS 白光全彩筒型网络摄像机智能侦测：支持越界侦测，区域入侵侦测 1 个内置麦克风，高清拾音白光/红外双补光，白光最远可达 30 m，红外最远可达 50 mm 最低照度：彩色：0.005 Lux @（F1.2，AGC ON），0 Lux with IR 宽动态：120 dB 焦距&视场角：2.8 mm，水平视场角：97°，垂直视场角：52.3°，对角线视场角：114.3° 4 mm，水平视场角：78.8°，垂直视场角:40.5°，对角线视场角：93.9° 6 mm，水平视场角：49.1°，垂直视场角：26.3°，对角线视场角：57.2° 8 mm，水平视场角：37.5°，垂直视场角：20.7°，对角线视场角：43.3° 12 mm，水平视场角：23.4°，垂直视场角：13.3°，对角线视场角：26.88° 补光灯类型：默认白光，可切换红外补光 补光距离：红外光最远可达 50 m，白光最远可达 30 m 波长范围：850 nm 防补光过曝：支持最大图像尺寸：2560 × 1440 视频压缩标准：主码流：H.265/H.264 音频：1 个内置麦克风网络：1 个 RJ45 10 M/100 M 自适应以太网口启动及		

		工作温湿度：-30 ℃~60 ℃，湿度小于 95%（无凝结）供电方式：DC：12 V ± 25%，支持防反接保护；PoE：802.3af，Class 3 电流及功耗：DC：12 V，0.75 A，最大功耗：9.0 W；PoE：802.3af，36 V~57 V，0.29 A~0.18 A，最大功耗：10.5 W 在彩色模式下，当照度降低至一定值时，可自动开启补光灯补光，在白天夜晚均可输出彩色视频图像。录像机：名单库比对报警（8 路人脸分析比对（图片流），或 2 路人脸抓拍（视频流）） 录像机：12U 标准机架式 2 个 HDMI，2 个 VGA9 盘位，已内置 8 块 8T 盘 2 个 RJ45 10M/100M/1000M 自适应以太网口 2 个 USB2.0 接口、1 个 USB3.0 接口 1 个 eSATA 接口报警 IO：16 进 9 出支持 DC 12V，ctrl 12V 反向供电软件性能：输入带宽： 160Mbps 输出带宽：160Mbps16 路 H.264、H.265 混合接入最大支持 12×1080P 解码支持 H.265、H.264 解可同时显示输出 12 路 H.265 编码、30fps、1920×1080 格式的视频图像，或同时输出 3 路 H.265 编码、25fps、4096×2160 或者 3840×2160 格式的视频图像，或同时解码 2 路 H.265 编码、20fps、4000×3000 格式的视频图像。输出 1 路 H.265 编码、25fps、8160×3072 格式的视频图像；开启视频流智能分析，NVR 解码性能不会降低 具有 2 个 HDMI 接口、2 个 VGA 接口、2 个 RJ45 网络接口、2 个 USB2.0 接口、1 个 USB3.0 接口、1 个 RS232 接口、1 个 RS485 接口、1 个 eSata 接口、1 路音频输入接口、2 路音频		

		输出接口；16 路报警输入接口、9 路报警输出接口、具有 2 路直流 DC 12V 输出接口（其中 1 路为 Ctrl 报警输出口）；可内置 9 个 SATA 接口硬盘 支持周界报警过滤 2 功能，对 IPC 上报的越界侦测报警和区域入侵报警进行去误报，可去除由树叶、灯光、车辆、阴影以及小动物引起的误报；最大支持 16 路		
42	动力环境监控	双 AC220V 输入电源 ， Intel®2.0GHZ 四核处理器，4G 内存，6 路 DI，2 路 DO,2 个 232 串口，6 个 485 串口，1 路 VGA 接口，1 路 HDMI 接口，有 1 个插槽，可 1U 标准机架或者壁挂安装。含监控系统软件，组态软件，可 IE 和客户端查看数据；包括机房水电暖通监控组件	套	1
43	机房智能系统	3D 可视化监控和设备能耗管控两部分	套	1
4	安装	包含机房强弱电线缆、管材等	套	1

4	配件及材料			
45	安装调试	设备系统安装调试	项	1
46	现有搬迁	现有机房搬迁	项	1
	小计19			
6.2	**海关机房改造**			
1	拆除原有地板原地面找平防尘处理	拆除原有地板，清理地面垃圾，地面找平，	m2	90
2	机房区原顶面	基础凿平、刷水泥砂浆防水涂料	m2	200

	防尘处理			
3	顶面橡塑保温层	橡塑绝热材料、B1 级、厚度 20mm	m2	200
4	机房区铝合金天花板	乳白色烤漆、600mm*600mm*0.8mm、1.8 微孔	m2	200
5	配电房铝合金天花板	乳白色烤漆、600mm*600mm*0.8mm、1.8 微孔	m2	100
6	墙面橡塑保温层 20mm 厚	橡塑绝热材料、B1 级、厚度 20mm	m2	240
7	墙面	75mm*50mm*0.6mm	m	2

	彩钢板龙骨及附材		2	400
8	主机房区域墙面彩钢板	1200mm*3000mm*13mm	m2	2400
9	不锈钢地脚线80mm高	304 哑光磨砂不锈钢板,高度 80mm，厚度 1.2mm	m	120
10	防火玻璃隔断	12mm 厚防火玻璃	m2	1000
11	玻璃隔断上下支架	40 角钢，支架不锈钢包边	m	30
12	双开钢质	2200mm*1500mm 不锈钢	樘	2

	防火门及安装			
13	防火玻璃平开门及安装	12mm 厚防火玻璃	樘	2
14	机房区及配电区抗静电地板	防静电地板 600mm（长）*600mm（宽）*32mm(厚)	m2	90
15	配电柜、UPS 承重安装钢支架	40 角钢	个	12
16	机柜承重	40 角钢	个	20

	安装钢支架1000宽×500高			
17	安装挡鼠板	不锈钢	个	2
18	踏步	40mm*4mm 角钢支架、304 哑光磨砂不锈钢板	个	1
19	斜坡	铝合金花纹板	个	2
20	排水管	Φ40PP-R 热熔管及配件	项	1
21	精密列头柜	标准列头柜，总市电输入开关：250A/3P*1，市电分配：插座 32A40 个、预留前端市电维修旁路接入孔位，保障可靠的维修特性；	台	2
22	IT 机柜	1、尺寸：600*1200*2000（42U），标准 19″机柜， 2、前门单开，后门双开，含顶底板(顶板两侧带走线孔，毛刷密封处理)，方孔条，横梁等； 3.通孔率＞80%，静态承重不少于 2500kg；	架	20

		4、配置 2 对 PDU 安装板，2 条 100mm 宽垂直绑线板，左右安装；前后门配接地线，含并柜件、50 套卡扣螺母螺丝； 5.优质冷轧钢板：型材框架≥1.5mm；立柱≥2.0mm，方孔条≥2.0mm，横梁≥1.5mm；前后门板≥1.2mm； 6、前后门配置隐藏式走线槽； 7、木托运输，纸箱包装 ； 8、表面处理，环保纳米陶瓷技术和静电粉末喷涂，颜色黑色 RAL9005；		
23	1U 盲面板	配 19”安装机架，机柜漏空挡板,塑料材质，阻止冷气流旁通，美观防尘，高度 1U，卡扣式安装	副	400
24	600 机柜走线槽	适用 600 宽机柜，单通道走线槽，强弱电分离则需要配置 2 个	个	40
25	冷仓门	适配双排通道宽度 1200mm，配套 1200mm 深机柜使用，含声光告警安装辅件；	套	2
26	有框门配套机柜侧门	适用用微模块最外侧侧门，带显示屏和读卡器孔位，带通道照明控制开关，配套 10 寸触摸屏使用，配套 1200mm 深机柜使用	个	8
2	有框	适用用微模块最外侧侧门，带读卡器孔位，带通道照明控制	副	1

7	门配套机柜侧门	开关，配套 1200mm 深机柜使用		8
28	LED 照明灯	安装在通道的两侧顶部。	套	2
29	天窗控制盒	集成控制盒，含翻转天窗控制，含烟感消防接口，可为 LED 灯，翻转天窗电磁锁以及全自动双开门电机供电。	个	2
30	应急开关附件	防止门禁失灵，应急出门使用	个	4
31	标准天窗	尺寸：用于 600mm 宽机柜，1200mm 宽通道；功能：可固定、可翻转（由电磁锁自动控制开启）。天窗开启实现与通道内消防告警信号联动，在消防状态下电磁锁打开，旋转天窗在重力作用下自动打开，保证灭火气体进入密封冷通道。天窗开启后冷通道的净高不小于 2 米，不影响日常维护工作和维护人员安全。	批	18
32	电缆	ZR-RVV 3*4，列头柜到机柜 PDU	米	900
3	电缆	ZR-RVV3*25+1*16　空调电源线	米	1

3				00
34	电缆	120 平方单芯电缆　　电池到 UPS 主机	米	150
35	电缆	ZR-RVV 4*95　UPS 输出柜到列头柜	米	160
36	PDU 电源	铝合金外壳 单路 32A 输入/10A 国标 12 口 16A 国标 4 口输出（带接线盒,带指示灯,垂直安装,面对机柜后门左、右侧安装）	套	40
37	UPS	1、功率模块 50KVA 1.0 功因 380Vac/50Hz,3U.1 块。200KW 机柜， 2、系统效率可达：96%； 3、电源制式：3Ph+N+PE，三相输入、三相输出； 4、输入电压：138～485VAC； 5、输入功率因数≥0.99； 6、UPS 功率模块内一个风扇异常时，模块可以继续工作，并可带 50%负载； 7、UPS 应采用集中控制的逻辑,集中控制单元需要 1+1 冗余； 8、机主支持锂电或铅酸,支持电池输入电压:360～528Vdc ； 9、抗震性能：满足 YD 5096-2005《通信用电源设备抗震性能检测规范》的要求，	个	2

		10、模块化不间断电源（UPS）厂商入选国家绿色数据中心先进适用技术产品目录，		
38	电池组	12V 100AH 阀控式密封铅酸蓄电池组，含配套每套 176 节电池	套	2
39	精密空调	行级精密空调 室内机 制冷量 80kW 风冷型 水平前送风 含加热加湿 直流变频压缩机 EC 风机 电子膨胀阀 彩色触摸屏 柜体尺寸（W*D*H）600*1200*2000mm，配套 1200mm 深拼装机柜使用	台	1
40	机房消防	柜式七氟丙烷灭火，含报警配套	套	1

41	机房安防	安防设备：满足国密要求门禁系统：5 套处理器：32 位处理器　刷卡读卡器:读卡频率：13.56MHz 按键方式：触摸按键.可识别卡：国密 CPU 卡,卡片发卡器,支持发卡类型：ID 卡、Mifare 卡、身份证物料卡号（序列号）、普通 CPU 卡、国密 CPU 卡；USB2.0 接口；具有 2 个 Sim 卡尺寸的 PSAM 卡座；,通讯方式：RS485+Wiegand 工作电压：DC 12V 功耗：≤2W 管控门数:2 门　包括门磁与所有配件通讯方式:上行 TCP/IP 读卡器接口：RS485 和 Wiegand 双通讯接口 存储容量：10 万张卡和 30 万记录存储 工作电压：自带机箱和供电电源（AC220V 输入），工作电压 DC 12V，功耗≤4W（不带负载） 支持蓄电池（303700655 OT7-12 蓄电池）接入，设备本身不含蓄电池； 支持消防功能，支持蓄电池功能主机应能对门的开启方式，卡的各种使用权限进行组合设置，实现不同场景的权限管理，故应具有以下功能：反潜回（防跟随）功能；多重卡认证开门功能；多重卡+中心远程开门功能；多重卡+超级密码开门功能；多重卡+超级卡开门功能；超级权限开门；中心远程开门；支持身份证开门；支持银行卡开门；支持单向刷卡（指纹）和双向刷卡（指纹）开门。 主机应具有丰富的通讯接口、控制接口及拓展接口：TCP/IP 接口 1 个；上行 RS485 通讯接口 2 个；下行 RS485 通讯接口	套	1

		2 个；wiegand 通讯接口 2 个；可接入最多读卡器数量 4 个，其中 2 个 RS485 读卡器和 2 个 wiegand 读卡器；报警输入接口 4 个；事件输入接口 2 个；门磁输入接口 1 个；开门按钮接口 1 个；电锁输出接口 1 个；报警输出接口 2 个。 主机应具防区报警功能，有 4 个防区输入端口，具有防短、防剪功能，能够联动报警输出。视频设备：400 万 1/3″CMOS 白光全彩筒型网络摄像机智能侦测：支持越界侦测，区域入侵侦测 1 个内置麦克风，高清拾音白光/红外双补光，白光最远可达 30 m，红外最远可达 50 mm 最低照度：彩色：0.005 Lux @（F1.2，AGC ON），0 Lux with IR 宽动态：120 dB 焦距&视场角：2.8 mm，水平视场角：97°，垂直视场角：52.3°，对角线视场角：114.3° 4 mm，水平视场角：78.8°，垂直视场角:40.5°，对角线视场角：93.9° 6 mm，水平视场角：49.1°，垂直视场角：26.3°，对角线视场角：57.2° 8 mm，水平视场角：37.5°，垂直视场角：20.7°，对角线视场角：43.3° 12 mm，水平视场角：23.4°，垂直视场角：13.3°，对角线视场角：26.88° 补光灯类型：默认白光，可切换红外补光 补光距离：红外光最远可达 50 m，白光最远可达 30 m 波长范围：850 nm 防补光过曝：支持最大图像尺寸：2560 × 1440 视频压缩标准：主码流：H.265/H.264 音频：1 个内置麦克风网络：1 个 RJ45 10 M/100 M 自适应以太网口启动及		

		工作温湿度：-30 ℃~60 ℃，湿度小于 95%（无凝结）供电方式：DC：12 V ± 25%，支持防反接保护；PoE：802.3af，Class 3 电流及功耗：DC：12 V，0.75 A，最大功耗：9.0 W；PoE：802.3af，36 V~57 V，0.29 A~0.18 A，最大功耗：10.5 W 在彩色模式下，当照度降低至一定值时，可自动开启补光灯补光，在白天夜晚均可输出彩色视频图像。录像机：名单库比对报警（8 路人脸分析比对（图片流），或 2 路人脸抓拍（视频流）） 录像机：12U 标准机架式 2 个 HDMI，2 个 VGA9 盘位，已内置 8 块 8T 盘 2 个 RJ45 10M/100M/1000M 自适应以太网口 2 个 USB2.0 接口、1 个 USB3.0 接口 1 个 eSATA 接口报警 IO：16 进 9 出支持 DC 12V，ctrl 12V 反向供电软件性能：输入带宽： 160Mbps 输出带宽：160Mbps16 路 H.264、H.265 混合接入最大支持 12×1080P 解码支持 H.265、H.264 解可同时显示输出 12 路 H.265 编码、30fps、1920×1080 格式的视频图像，或同时输出 3 路 H.265 编码、25fps、4096×2160 或者 3840×2160 格式的视频图像，或同时解码 2 路 H.265 编码、20fps、4000×3000 格式的视频图像。输出 1 路 H.265 编码、25fps、8160×3072 格式的视频图像；开启视频流智能分析，NVR 解码性能不会降低 具有 2 个 HDMI 接口、2 个 VGA 接口、2 个 RJ45 网络接口、2 个 USB2.0 接口、1 个 USB3.0 接口、1 个 RS232 接口、1 个 RS485 接口、1 个 eSata 接口、1 路音频输入接口、2 路音频		

		输出接口；16 路报警输入接口、9 路报警输出接口、具有 2 路直流 DC 12V 输出接口（其中 1 路为 Ctrl 报警输出口）；可内置 9 个 SATA 接口硬盘 支持周界报警过滤 2 功能，对 IPC 上报的越界侦测报警和区域入侵报警进行去误报，可去除由树叶、灯光、车辆、阴影以及小动物引起的误报；最大支持 16 路		
42	动力环境监控	双 AC220V 输入电源 ， Intel®2.0GHZ 四核处理器，4G 内存，6 路 DI，2 路 DO,2 个 232 串口，6 个 485 串口，1 路 VGA 接口，1 路 HDMI 接口，有 1 个插槽，可 1U 标准机架或者壁挂安装。含监控系统软件，组态软件，可 IE 和客户端查看数据；包括机房水电暖通监控组件	套	1
43	机房智能系统	3D 可视化监控和设备能耗管控两部分	套	1
4	安装	包含机房强弱电线缆、管材等	套	1

4	配件及材料			
45	安装调试	设备系统安装调试	项	1
46	现有搬迁	现有机房搬迁	项	1
	小计20			
6.3	**跨境一期机房改造**			
1	现有搬迁	现有机房搬迁	项	1
	小计21			
6.4	**跨境二期机房改造**			
1	配电柜、	40 角钢	个	1

	UPS 承重安装钢支架			
2	精密空调	行级精密空调 室内机 制冷量 30kW 风冷型 水平前送风 含加热加湿 直流变频压缩机 EC 风机	台	1
3	走线改造	重新制作桥架与整理原有走线	批	1
	小计 22			
6.5	**卡口机房改造**			
1	配电柜、UPS 承重安装钢支架	40 角钢	个	4
2	机柜承重	40 角钢	个	12

	安装钢支架1000宽×500高			
3	踏步	40mm*4mm 角钢支架、304 哑光磨砂不锈钢板	个	1
4	排水管	¢40PP-R 热熔管及配件	项	1
5	电缆	ZR-RVV 3*4，列头柜到机柜 PDU	米	200
6	600机柜走线槽	适用 600 宽机柜，单通道走 W 型线槽，强弱电分离则需要配置 2 个	个	24
7	UPS	功率模块 50KVA 1.0 功因 380Vac/50Hz,3U.1 块。100KW 机柜	个	1
8	电池组	12V 200AH 阀控式密封铅酸蓄电池组，含配套每套 64 节电池	套	1
9	LED照明	安装在通道的两侧顶部。	套	1

	灯			
10	机房安防	利旧原有监控及配套，门禁系统等	套	1
11	动力环境监控	双 AC220V 输入电源 ， Intel®2.0GHZ 四核处理器，4G 内存，6 路 DI，2 路 DO,2 个 232 串口，6 个 485 串口，1 路 VGA 接口，1 路 HDMI 接口，有 1 个插槽，可 1U 标准机架或者壁挂安装。含监控系统软件，组态软件，可 IE 和客户端查看数据；	套	1
12	安装配件及材料	线缆、管材等	套	1
13	安装调试	设备系统安装调试	项	1
14	现有搬迁	现有机房搬迁	项	1
	小计 23			
6.6	**监控指挥中心**			

1	LED 大屏	1. 点间距≤1.25mm；像素密度：≥640000 点/㎡ 2. 显示屏尺寸：≥15000W*2362.5Hmm，显示屏宽高尺寸可正偏离，且显示屏宽高尺寸偏 离误差≤2%。 3. LED 封装：SMD 表贴三合一；采用国星、日亚或亿光等同等品牌金线封装； 4. 防护等级：IP30； 5. 亮度：≥600cd/㎡； 6. 箱体平整度：≤0.1mm； 7. 色温：3200K-9300K； 8. 水平视角和垂直视角：水平视角≥140°，垂直视角≥140°； 9. 刷新率： ≥3840Hz； 10. 最大对比度：≥3000:1； 11. 换帧频率：50/60Hz； 12. 亮度/颜色校正：亮度均匀性：＞97%； 13. 供电要求：AC 100-240V（50/60Hz）；平均功耗：≤250W/㎡；发光点中心距偏差＜ 3%；驱动方式：恒流驱动；	㎡	35.4375
2	接收卡	内置箱体内，1 箱体 1 个	张	144
3	4K 发送卡	输入有 HDMI，输出接口有网口；	张	3
4	集中	DVI/HDMI-集中式输入	路	1

	式拼接器1			2
5	集中式拼接器2	HDMI(4K@60Hz)-集中式输入	路	4
6	集中式拼接器3	DVI/HDMI-集中式输出	路	3
7	配电柜	1.功率≥40 kw，输入电压 380VAC±5% 2.具备防雷、过压、过流、欠压、短路、断路以及漏电保护措施； 3.具有漏电保护开关、空气开关、熔断器、延时启动接触器、电源防雷器等； 4.配电柜门上具有配备各支路手动开关和状态指示灯等； 5.具备远程智能控制功能，手动，自动，定时控制等功能 6、提供 PLC 软件著作权证书并加盖厂家公章或投标专用章	台	1
8	控制电脑	CPU：i7-10700 处理器及以上 内存：16GB 及以上 硬盘：1TB+256GB SSD 及以上 显卡：独立显卡，显存 2GB 及以上	台	1

		显示器：LCD 21.5″及以上		
9	机柜	黑色，2000*600*600	台	2
10	百兆交换机	用于发送卡间互联用交换机	台	1
11	钢结构及包边	钢结构及包边	㎡	25.92
12	线缆	通信线及电源线	套	1
13	86 寸触控一体机	屏幕显示尺寸 86 寸。 显示比例 16:9，亮度>320cd/m2，对比度>1200:1，可视角度>178° 整机具备 Windows 和 Android 双系统。 悬浮菜单:悬浮菜单可通过单指或多指调用到屏幕任意位置，可根据需要设置常用菜单;悬浮菜单可自行开启或关闭。 摄像头像素:800 万，支持拍照以及扫描功能，整机内置拾音麦克风。 整机接口至少 1 路 HDMT、1 路 USR-TOUCH、至少 3 路前置 USB30 同时支持在 Windows 和 Android 在 VGA 或 HDMI 通道下外接设备实现交互时，前置 USB 接口	台	1

		可实现自由读取 U 盘功能。 低蓝光保护，可有效过滤 LED 光源发出的可见光中含有的大量有害蓝光，保护视力健康。 CPU:INTELI7;内存:>8G;固态硬盘:>128G;内置 WIFI 模块。 整体通过 3C 检测		
14	PAD 平板	≥10.8 英寸全面屏 2560*1600,8 核 CPU，支持多点触控，运行内存 8G,256GB 内存	台	1
15	可视化渲染工作站	CPU：8 核及以上，主频在 3.0GHz 以上 内存：DDR4 240 0 32G 及以上， 显卡：图形工作站专用显卡， 显存 48GB DDR6、显存频率达到 16Gbps、带宽 768 GB/s 硬盘：不低于 1T SSD 存储空间 操作系统：windows 10 64 位专业版 千兆有线网卡 含视频线 3m USB 延长线 无线鼠标	台	1

16	智慧园区集成平台	一、园区接入服务：预集成市面主流安消、通行、设施、能耗、环境空间等不同种类接入设备和系统，提供设备/子系统的接入标准，接入标准包括物模型和协议类型等，符合标准的南向子系统可直接对接，无需项目定制开发；支持通过定义综保区设备/子系统的集成标准，自行定制开发属于项目自有的设备和子系统接入，从而在架构上保持整体的接入标准化。 二、园区事件服务：支持园区事件能力以 API 服务等形式开放，支持创建多个事件中心，可预定义事件/告警模型库，完成典型系统预集成；支持灵活的模型设计，通过配置新增事件规格、事件转发动作等，实现新的业务事件和业务告警的接入、呈现和处理；提供的事件能力以服务形式开放，支持各开发厂家基于场景创建多个事件中心，围绕综保区场景预定义事件/告警模型库，并完成典型系统预集成。 三、园区设备服务：提供统一设备服务或标准的设备物模型库，包含设备规格的定义，设备实例数据的管理，可基于物模型标准化不同厂家设备的管理和控制服务；提供设备主数据应用进行设备实例的查看和管理；提供设备规格的定义，设备实例数据、基于设备的触发器管理、设备的关联关系管理、设备组管理能力。 四、园区运维服务：对智慧综保区的平台组件以及智慧化应用实现统一部署、系统状态可视、统一巡检等功能，提供统一的监控和告警上报能力，能够自动完成监控数据采集、查	套	1

		询、告警通知和告警总览；提供内置监控指标，形成系统运维监控标准，可以从资源、设备、应用层等方面全方位提供运维监控能力 五、系统集成功能： 1、数据集成： ▲支持多种异构数据源间的同步：如 DB2、Oracle、MySQL、SQLServer、Kafka、Hive、IBM MQ、Redis、API、ActiveMQ、FTP、Websocket 等读取和写入；提供产品彩页或功能界面截图并加盖厂家公章或投标专用章 支持 MySQL、文本文件、消息、API 等多种数据的分片读取和写入。 支持自定义及自动映射两种方式关联数据源字段与目标数据源字段 支持对创建的数据集成任务进行启动、停止、修改等管理操作； 支持任务调度：按照时间（实时、定时），数据量（增量、全量）等来调度任务。 支持任务监控：可以对创建的数据集成任务的运行情况进行监控，并对异常的任务进行处理，保证业务正常运行； 支持基于数据库日志的增量数据同步能力 支持服务中断后，修复后自动修复任务； 支持用户自定义需要集成的数据库表及数据库字段； 2、消息集成		

		支持消息的 topic 发布与订阅、支持消息 topic 的管理； 支持 Kafka 1.1.0 和 2.3.0 等版本； 兼容开源 Kafka 的 API，具备原生 Kafka 的所有消息处理特性，兼容 Java、python、Go 多语言客户端。 支持消息数据高可靠：支持消息持久化，多副本存储机制。可选择副本间消息同步、异步复制，数据同步或异步落盘等多种方式。 细粒度权限控制：基于 APP 的权限，控制 Topic 消息的订阅和发布权限； 支持消息查询：通过指定时间和位置，查询具体消息的内容； 3、应用集成 支持 HTTP/HTTPS（实例域名访问），websocket（数据 API），SOAP（函数 API）访问 ▲API 网关支持 API 生命周期管理：从 API 新建、发布、编辑、调试、授权、下线、删除等生命周期管理能力；提供产品彩页或功能界面截图并加盖厂家公章或投标专用章 把自定义 JS 脚本函数定义为后端服务，把函数的能力以 API 的形式对外发布。 提供 API 策略后端配置能力，支持配置协议与请求方式、重试次数等参数来定制 API 接口的后端； 支持秒级 API 流控，针对不同的业务等级、用户等级，可实施 API 级别的精细流控，保护集成业务的稳定运行		

		API 协议&数据格式转换， Rest 转 soap， Json 转 Xml 等； 安全认证，支持 app key&app Secret 对应用进行认证，用户可编写自定义脚本对接第三方认证； 支持 API 安全管理：统一的认证模式、支持 SSL 加密， 支持 API 的在线调试 支持数据库到 API 的转换发布能力，降低应用开发的用数难度，支撑应用快速创新，SQL->RESTful API 4、系统包含含边缘自治形态专业版软件授权许可（80 个连接） 六、系统部署：通过安装工具链流水线方式完成所有满足规范的系统的安装；提供基础的安全容器镜像（容器化部署），确保操作系统级底层安全；应用基于安全容器镜像进行打包；提供灵活的安装入参，支持快速完成平台及应用安装；		
17	K8S 容器编排软件	商用 K8S 集群软件，支持平台组件的容器化部署的调度和管理，包含一年保修，提供 7x24 小时的在线维护支持服务，含软件补丁升级，现场问题解决。	套	1

18	智慧园区数据平台	一、数据库： 1）采用国产关系型数据库，具有跨操作系统平台的能力，建设主备模式 2）支持 Linux、麒麟、统信 UOS 等操作系统等， 3）支持 INTEL、鲲鹏、飞腾等处理器； 4）支持 PL/pgSQL 过程语言；支持 JDBC/ODBC 标准接口； 5）支持 number、date、blob/clob、varchar2 等数据类型 6）支持序列与自增列，支持事件触发器 7）支持 connect by 层次查询 8）支持 Package、物化视图 9）支持 B-TREE 索引、GIN 倒排索引、Gist 空间索引等多种索引访问方式。 10）支持并配置 HA 故障转移集群和主备同步技术，并且能够支持故障转移功能，支持主从、一主多从等架构，从库能设置延迟复制和优选提交复制； 11）支持逻辑备份恢复、物理备份恢复，物理备份支持增量备份和联机热备份技术，逻辑和物理备份均支持本地和远程备份； 12）过程性语言支持自治事务，包括存储过程、自定义函数、触发器以及匿名块。存储过程支持自治事务的嵌套调用。 13）支持系统性能监控动态视图，TOP SQL 信息、内存管理信息、事务信息、线程信息、操作历史等信息； 14）支持创建表分区，包括 range、list、hash、interval	套	1

		间隔，支持两级分区方式； 15）为满足园区多维数据建模，需支持空间数据功能，支持丰富的原生几何数据类型，包括点、线、面、多点、多线、多面、几何集合等；支持 EWKT、EWKB 和 Canonical 格式的几何对象；支持 2D/3D 坐标系、坐标系转换·和球体长度计算；支持空间数据分析函数和聚合函数，包括 Area、Length、Distance、Extent、ST_3DLineInterpolatePoint 等；支持二元谓词如如 Union 和 Difference，空间操作符如 Contains、Within、Overlaps、Touches 等； 16）支持行存表和列存表，要求行存表和列存表支持在同一个事务内增删改查，并且支持在同一个查询命令中进行多表关联； 17）内置内存引擎，能够实现在同一个实例中内存表跟普通的磁盘表的共存，内存表支持 ACID、常用 SQL 语法、存储过程和数据持久化等功能特性，支持 Masstree 索引的优化技术； 18） 支持基于成本的全局优化功能，实现基于成本的查询机制，能够选择合适的查询计划；数据库内核支持并行查询技术，且能够完全自动化启动并行查询，无需人工启动或干预； 19）支持提供专业的迁移工具自动将数据库的 DDL 包括存储过程转换至本数据库，迁移工具能够提供全面的迁移评估功能，给出迁移成功率和工作量报告，支持 DDL 和数据的迁移，		

		支持迁移后的数据校验功能 20）满足 ITSS 信息技术服务标准三级。 二、具备园区数据管理功能： 1）提供园区范畴的专题库（DM）、主题库（DWR）、数据湖（DWI）三层模型及架构能力，使用融合集成平台中的数据集成和消息集成组件完成贴源层数据的采集汇聚，数据集成完成批量数据采集的调度处理，消息集成使用消息队列的方式进行实时数据采集； 2）提供数据加工工具和方法论，满足园区定制数据采集、数据处理、数据分析等端到端全流程的需要；可针对贴源层汇聚的数据，根据业务服务需要的数据分析服务需求，对数据进行清洗，加工以及计算，将数据转换成主题层或专题层的的数据模型并存储；提供 Flink 的实时流处理能力； 3）提供已预置的人员、组织、设备、车辆、时空、资产、事件、资源、工单等主题库内容，满足园区常见业务的主要分析诉求，并可根据需要进行定制； 4）提供已经预置开发的关于人员、组织、设备等相关的主题服务 API，支撑项目快速开发各大专题应用数据分析的需求。		

19	地理信息数字系统GIS	地理信息服务： 1、系统支持多数据源融合、支持二三维一体化，支持2D和3D地图，兼容多种地图引擎，建议不少于三种厂家； 2、提供统一的地图组件，支持各类园区数据（设备、告警、热力图等）的叠加展示。支持对接多种数据存储介质，包括文件型数据源，Oracle、SQLServer、Kingbase、HDFS分布式文件系统、MongoDB分布式数据库以及Postgres-XL数据库集群、Elasticsearch、MySQL等数据库； 3、易定制、可扩展，提供统一的SDK，可以通过开放的JS API，快速定制地图应用；对接web数据源（Google Map、天地图，百度地图，BingMaps、OpenStreetMap等在线地图）、 OGC地图服务，并支持在二维地图及三维场景中叠加显示 4、支持对接多种主流BIM类型数据的加载； 5、支持以服务的形式对接各类GIS标准数据； 6、二维数据加工：基于倾斜摄影或CAD的二维矢量数据采集，制作园区矢量图，并构建园区环境渲染后的高清图片，增强地图美感.二维数据加工范围需包括澄迈老城区园区、金盘保税区、空港保税区等区域，面积不低于6平方公里。	套	1
20	3D建模	地面建模：根据CAD图纸等资料，通过3DMax进行建模，利用高清材质贴图，提供包括园区内道路、绿化等设施的三维建模服务。	平方公里	6
2		单栋楼外景建模：根据CAD图纸等资料，通过3DMax进行建	栋	1

1		模，利用高清材质贴图，真实还原建筑的内外部结构细节。		00
22	媒体转码组件	1、转码任务管理：并发转码视频 16 路，支持转码模板配置管理、转码任务管理、转码任务监控等功能 （含交付服务：系统安装部署调测、用户培训、项目技术方案现场支持） 2、转码格式管理：支持高码率、高分辨率视频转换为低码率、低分辨率视频，包含且不限于:将 4K/1080P/720P/D1 码流等降码率、降分辨率的能力，可根据需求灵活设置转换后视频的码率、分辨率。	套	1
23	可视化平台	一、可视化引擎：大数据可视化平台用完全自主可控的国产化引擎，适配国产化芯片、操作系统、数据库，支持大场景下大数据量的流畅、稳定运行，支持集中式及分布式部署，应用开发采用 B/S 模式： 1）▲平台二三维一体化能力：基于数字地球，将园区周边地理信息与三维场景进行无缝的融合技术，实现园区场景远、中、近三个层次穿透式查看；宏观对园区全景进行完整、鲜活的呈现，中景查看楼宇建筑轮廓及布局，微观查看建筑构造、每层的内部设施等精细场景。提供产品彩页或功能界面截图并加盖厂家公章或投标专用章 2）支持各类地图影像的渲染呈现；如政区图、卫星影像、高程影像、DLG 矢量数据、倾斜摄影、房屋轮廓面等多种数据源混合叠加综合展示。 3）多模式切换渲染能力：支持多种渲染展示模式的实时切	套	1

		换，突出关注信息；比如虚幻模式、实景模式、夜景模式、重要关注物突出显示；针对特殊的位置及数据，采用模型局部消隐、半透显示、内部轮廓、灯带等多种渲染方式，对楼体进行数据叠加，搭配园区场景进行可视化展示。 4）▲重点楼宇可视化表达能力：支持对园区外部环境、楼宇建筑到建筑内部结构以及房间内设备设施进行真实展现；基于 3dmax 及 BIM 模型对重点楼宇进行半透及分层着色渲染，可对楼宇进行单层抽出或分层展开，展示各楼层企业分布情况、楼宇空间闲置情况、人流监控情况及物联设施分布运行情况，实现微观场景的可视化业务表达。提供产品彩页或功能界面截图并加盖厂家公章或投标专用章 5）地上、地下一体化展示能力：支持对数字园区地面进行剖切，查看地下管线分布；支持以地块抬起方式将地面半透，以地上、地下一体化方式查看地下管线的空间走向分布。 6）具备漫游操作，可在场景中通过路线设置进行漫游线路的自定义，可实现漫游路线的自动播放，可以全方位、多视角、立体化地观察场景及信息。 7）支持时间、空间、属性等多维度呈现和查询能力，支持空间量算功能。 二、数据对接与专题开发： 对接园区相关业务系统，比如安防、消防、招商、场站、物流、辅助运营系统等，对接园区业务核心呈现和分析数据，		

		实现园区运行数据的可视化展示、智能监测与预警，实现整体运行态势，可视化专题页面包括：园区总览、安防监测、便捷通行、设施管理、敏捷招商、党建管理、数字化运营态势、数字物流运营、业务运营可视化 1）园区安防监测展示内容：通过集成智慧安防系统的视频监控系统、电子巡更系统、卡口系统等园区安全防范管理系统数据，需支持对园区重点部位、人员、车辆、告警事件等要素进行实时监测，实时呈现园区安全态势监测一张图。 2）便捷通行监测展示内容：需实现园区人员监测、车辆监测、交通诱导、物流管理态势，展现园区人员流动及报警信息，各视频监控实画面及各类报警分析，实现园区人员、车辆、交通、物流管理流动的可观、可视、可控。 2.1）人员态势：汇集园区人员日常流动数据及信息。同时可按照时间、类型、空间维度进行数据分析，辅助值班人员进行管理。 2.2）车辆态势：汇聚园区车辆道闸及视频监控对园区车辆通行情况、车位情况、车辆告警等进行分析，辅助值班人员及时了解园区的车流情况。 2.3）交通诱导：汇聚园区内交通相关数据，对交通运行态势及交通诱导设备情况，对数据进行多维度分析，展示园区内交通运行情况。 2.4）物流管理：汇集物流相关数据，呈现园区物流管理日常人车流数据及信息，呈现物流管理整体态势。〞		

		3）设施管理监测展示内容：需实现基于地理信息系统，通过三维建模，对设备的外观进行三维仿真呈现，支持对园区供水、供电、供热、空调、新风、照明等设备要素进行实时监测，实时呈现园区设施管理监测一张图。 4） 敏捷招商监测展示内容：需实现通过智慧园区服务系统的招商管理版块的招商数据，整合招商业务类型、招商项目、项目分布以及流程、招商企业行业等要素进行实时监测，实时呈现园区招商一张图 5）园区总览展示内容：园区总览专题需实现整合园区经济发展、政务服务、安全监管等相关各领域数据，通过对跨部门、跨业务的数据及业务进行融合，围绕经济发展、资源概况、园区服务和安全监管等领域，结合物联感知监测设备数据，形成“园区运行全景图” 6）党建管理展示内容：全力提升园区党建工作水平，充分发挥党员职工的先锋模范作用，全面提升基层党组织的战斗堡垒作用，通过党建引领作用，实现党建引智助推发展、党建引资助推发展、党建聚力助推发展的作用以党建高质量发展推动园区经济社会发展。 7）数字化运营透视展示内容：企业数字化运营透视专题对园区、企业、人员的运营数据进行管理和分析。收集企业生产、经营、环境、能耗等数据，通过统计分析形成直观的报表，自动对问题、风险预警、告警。 8）数字物流运营展示内容：数字物流专题包括数字仓储、		

		数字场站、数字堆场等。通过收集智慧物流、仓储、场站、堆场等数据，通过可视化对对仓储、场站、堆场的运营数据进行管理和分析。实时呈现数字仓储、数字场站及数字堆场态势 9）业务运营展示内容：聚焦园区业务运营情况，展示园区内场站业务、跨境业务等业务的运营情况，并对于园区门户使用情况进行监测，展示系统集成量、注册企业数量、访问量等指标，反映智慧园区信息化建设成功。通过数据的融合，并提供历史及同期业务数据分析、对比、统计呈现，为园区管理者提供可视化的经营辅助手段。 三、可视化呈现与渲染： 包括大屏导航面板、 数据呈现、基础效果、虚实切换及仪表与 场景联动交互等功能。大屏导航面板，支 持对展示内容进行解析、对所展示的要素 进行组态配置。 1）大屏导航面板，支持对展示内容进行解析、对所展示的要素进行组态配置。 2)）数据呈现，支持包括根据 布局配置，实现支持指标数据在大屏的呈 现。支持从仪表和三维可视化场景两个角 度对指标进行钻取分析。支持实时数据动 态刷新。 3）基础效果，支持提供常用的基础效果库，包含色块图，二维柱状图，弹出式标牌，道路线效果，投影线，广告牌，楼宇虚化，镂空，模型标注，屏幕图片，屏幕文字，普通区		

		域线，迁移线，热力图，视频标牌，贴地线，贴图标牌，贴图线，线上文字，相机服务，圆柱标注，圆锥标注，空间文字，空间线效果，扩散环效果、火焰、爆炸、云、雾、雨、雪、水浪等三维特效。 4）虚实切换，支持宏微观场 景的一体化显示、虚实结合和无缝切换。 5）仪表与场景联动交互，支持仪表的交互操 作自动传递给可视化场景。 6）大屏渲染增强 ：支持丰富的可视化三维特效，包含建筑物科技蓝，建筑物虚化，调整楼层颜色，建筑边框，楼宇抽屉式查看，楼宇分层查看，电梯移动，流动管线效果，轨迹图，扫光，扫描光圈，物体移动 ，池火灾控制，灯带，地质效果，毛玻璃，喷泉，逃生路线 ，监控扫描，空间菜单，动态光圈，动态光影，动态水面，动态图片，动态拖尾，三维柱状图等三维特效。		
24	坐席	CPU：I5-10400 2.9GHz 6 核 12 线程；内存：16GB/2666 DDR4；硬盘：512GB M.2 SSD；显卡：集成；蓝牙+WiFI6;WIN10 家庭版；23.8 寸显示器	台	13
25	装修工程	包含拆除及脚手架工程、指挥中心整体装修、强弱电工程、消防工程、空调工程等（面积根据实勘）	套	1
26	配套桌椅	指挥中心坐席配套桌椅	套	1
	小计			

	24			
七	服务器及存储			
7.1	国产化云平台一区			
1	超融合服务器	1、支持部署虚拟化、分布式存储和管理软件，同一节点内实现计算存储融合，不需要外置 SAN 存储 2、处理器：配置 2 颗国产 CPU，单 CPU 物理核心数≥32，主频≥2.0GHz； 3、内存：配置≥512GB DDR4 内存； 4、硬盘：系统盘配置≥2*960GB SSD 硬盘，缓存盘配置≥2*3.2TB NVMe SSD 硬盘，数据盘配置≥10*8TB 硬盘； 5、Raid 卡：配置独立 RAID 卡，链路支持 12G，支持 RAID0、RAID1、RAID10 等以及磁盘直通； 6、网卡：提供不少于 2 个千兆电口、4 个万兆光口（含光模块）， 7、其它：冗余交流电源、风扇；	台	12

2	接入交换机	1、交换容量不少于 2.56Tbps，包转发率不少于 1600Mpps； 2、支持万兆光口不少于 48 个，40GE 光口（可升级 100GE）不少于 6 个； 3、为了提高设备可靠性，支持可插拔的双电源； 4、为了提高设备散热性能，支持可插拔风扇框； 5、支持 MAC 表项≥128K； 6、支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN； 7、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 8、支持真实业务流实时检测技术，能实时检测网络故障 9、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 10、配置：双电源，48 个万兆多模光模块，6 个 40G 上联端口及多模光模块。	台	2
3	IPMI 交换机	1、交换容量不少于 750Gbps，包转发率不少于 250Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 48 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个； 4、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 5、支持静态路由、RIPv1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+； 6、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、	台	1

		IS-IS、Static Route； 7、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 8、支持真实业务流实时检测技术，实时检测网络故障 9、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 10、配置：双电源。		
4	虚拟化管理软件	1.云平台须采用国产化平台，采用基于 openstack+KVM 的技术路线实现，具备自主知识产权且获得软件著作权登记。 2.支持虚机开通、安全组管理、资源编排、平台备份、CMDB、审批流程管控、私有网络管理、块存储、镜像、快照、资源监控预警等功能。 3.云主机、块存储的业务可用性≥99.95%，对象存储的业务可用性≥99.98%，通过可信云认证。 4.云主机、块存储数据存储持久性≥99.9999999%，对象存储数据存储持久性≥99.9999999999%，通过可信云认证. 5.弹性云主机可绑定的网卡数量（主网卡+辅助网卡）不小于 15 块。 6.支持 TCP、UDP 协议的四层负载均衡和 HTTP、HTTPS 协议的七层负载均衡，支持至少两种负载均衡策略，支持超过 10 万 QPS。 7.支持 VPC 的安全组和网络访问控制列表等高级安全功能，	套	1

		可以在实例级别和网络级别控制进出流量。 ▲8.云平台须具备零信任安全能力，通过可信云认证，满足用户零信任访问场景的需求，需提供证书复印件或官网截图并加盖厂家公章或投标专用章。 9.提供 24 个国产化架构物理 CPU（单 CPU≥32 核）的虚拟化软件授权		
	小计			
7.2	**国产化云平台二区**			
1	超融合服务器	硬件配置参数要求： 1、 处理器：配置 2 颗国产 CPU，单 CPU 物理核心数≥32，主频≥2.6GHz； 2、 内存：配置≥512GB DDR4 内存； 3、 硬盘：系统盘配置≥2*1.2TB SAS 硬盘，缓存盘配置≥1*3.2TB NVMe SSD 硬盘，数据盘配置≥12*2.4TB 10K SAS 硬盘； 4、 Raid 卡：配置独立 RAID 卡，链路支持 12G，支持 RAID0、RAID1、RAID10 等以及磁盘直通； 5、 网卡：提供不少于 4 个千兆电口、4 个万兆光口（含光	台	11

		模块）， 6、 其它：冗余交流电源、风扇； 软件功能要求： 1、 设备须提供与硬件配置相对应的分布式块存储软件、超融合管理软件的授权，支持在统一个管理界面中监控和管理计算、存储、交换机、虚拟化平台等； 2、支持磁盘拔出和换位的容错功能，2 块磁盘被拔出，能够产生自动告警，5 分钟内互换槽位插入，系统不发生数据重构。 3、快速重构：磁盘故障时，系统能自动进行数据快速重构，1TB 重构时间≤15 分钟。 4、支持 EC 缩列功能，当节点故障时，自动调整 EC 配比，确保数据可靠性不降级。 5、 超融合存储系统支持重删压缩功能，压缩比≥10，性能下降≤15% 6、 支持 Call Home 功能，可通过管理界面配置 7*24 小时自动将系统告警信息发送给原厂商，便于及时处理系统告警； 7、 系统健康巡检功能：支持对系统服务器、系统 OS、分布式存储、管理系统的健康状态检查，识别系统的风险和异常，支持定时系统巡检		

2	接入交换机	1、交换容量不少于 2.56Tbps，包转发率不少于 1600Mpps； 2、支持万兆光口不少于 48 个，40GE 光口（可升级 100GE）不少于 6 个； 3、为了提高设备可靠性，支持可插拔的双电源； 4、为了提高设备散热性能，支持可插拔风扇框，风扇框个数≥4； 5、支持 MAC 表项≥128K； 6、支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN； 7、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 8、支持真实业务流实时检测技术，能实时检测网络故障 9、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 10、配置：双电源，48 个万兆多模光模块，6 个 40G 上联端口及多模光模块。	台	4
3	IPMI 交换机	1、交换容量不少于 750Gbps，包转发率不少于 250Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 48 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个； 4、支持 MAC 地址不少于 256K，ARP 表项不少于 128K，IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K 5、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN；	台	1

		6、支持静态路由、RIPv1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route； 8、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 9、支持真实业务流实时检测技术，实时检测网络故障 10、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 11、配置：双电源。		
4	虚拟化管理软件	1.国产自主品牌虚拟化软件，基于 KVM 架构，可直接安装在国产化的物理服务器上,提供 22 个物理 CPU（单 CPU≥32 核）的虚拟化软件授权，至少包含虚拟化软件、虚拟化管理平台软件、虚拟化备份软件等授权； 2. 通过国产化服务器节点构建，同一节点内实现计算存储融合，不需要外置 SAN 存储，存储系统为分布式 Server SAN 架构，可配置副本或 EC（纠删码），满足不同可靠性要求的业务场景。 3. 支持在统一界面上扩容节点，在界面可将待扩容节点自动发现，完成相应的系统配置，包括：IP 地址、主机名、网关、存储池等参数，校验后进行系统扩容操作，将待扩容节点加入系统集群中。 4. 支持在统一界面上进行超融合组件升级，在界面上可以通过系统升级功能完成虚拟化、分布式存储等组件的升级。	台	1

		5. 支持资源以虚拟数据中心 VDC 维度划分，支持多租户，VDC 管理员可对资源池自助管理。 6. 支持以集群为单位设置跨代 CPU 虚拟机热迁移属性. 支持同一 CPU 厂商不同 CPU 型号服务器组建在同一逻辑集群中,并且支持虚拟机在不同 CPU 型号服务器之间进行业务不中断热迁移。 7.▲支持虚拟机的 CPU 、内存、存储 的 QoS 设置，满足不同应用的性能需求。需提供产品彩页或软件功能界面截图并加盖厂家公章或投标专用章；； 8. 支持创建精简配置卷，系统应该根据精简配置卷的实际使用情况动态分配空间，提供存储资源利用率。 9. 支持卷的 IOPS、带宽的上限设置，可设置卷的总 IOPS 和带宽，也可以设置每单位容量的 IOPS 与带宽，用户可指定 Qos 策略的运行周期为单次、每天、每周或始终执行。 10. 支持虚拟交换机，通过对接受和发送的流量进行整形保证网络质量，至少支持安全组、平均带宽、峰值带宽、突发大小、优先级、DHCP 隔离、广播抑制、TCP 校验和的设置。 11. 支持虚拟机 HA，允许配置集群内 HA 预留的主机数量，以保证在虚拟机故障时有足够的资源进行切换，支持配置存储故障后是 HA 虚拟机还是不处理。 12. 兼容性要求：虚拟化平台需支持异构多类型 CPU 集群混合部署，包括但不限于鲲鹏、飞腾、海光；		
	小计			

	26			
7.3	**云资源租用**			
1	云容灾3年服务	容灾高可用主机：8核CPU，16G内存，500G数据盘，10M公网带宽	台	5
		容灾管理控制器：8核CPU，16G内存，100G数据盘	台	1
		容灾CDP主机：8核CPU，32G内存，7500G数据盘	台	1
		租户安全等保二级服务：含云防火墙、云主机安全、云Web应用防火墙、云综合日志审计、云堡垒机	套	1
		容灾HA高可用授权（容灾源端、目标端节点均需授权）	个	10
		容灾CDP授权(含5台私有云源端授权及1台目标端容灾CDP主机授权）	个	6
2	云备份服务3年	租用海南省内云服务商的云备份服务，支持文件备份、数据库备份、虚机备份。备份存储容量30T。	套	1
	小计27			
7.3	**统一云管理平**			

	台			
1	统一云管理平台	1.云资源管理：云资源概览、基础资源管理、分布式服务管理、分布式网络管理、多云多基础设施编排 2.云服务：云平台统计分析、云平台大屏展示服务、消息中心服务 3.云运维：告警管理、监控管理、日志管理、工单管理、云平台备份管理 4.多云适配管理：纳管资源池的增/删/改/查、主流云平台的纳管适配 5.云治理：权限管理、配置管理、服务目录管理 6.云成本管理：统一计量管理、成本分析、账单管理 7.支持私有云资源管理、分布式资源管理、运维中心管理、运营中心管理、应用集成、配置管理、资产管理等功能 8.提供混合多云统一管理能力，支持纳管第三方私有云，支持纳管阿里云、华为云、腾讯云、华三云、VMware 等云服务商的私有云产品。	项	1
	小计 **28**			
八	**系统软件**			
1	操作系统	开源/国产	套	13

2	数据库	开源/国产	套	1
3	中间件	开源/国产	套	13
4	数据交换平台	采购商业数据交换系统，并在此基础上进行二次开发	套	1
	小计29			
九	**园区网络系统**			
9.1	**网络设备**			
1	出口路由器（澄迈园区）	1、采用无阻塞交换架构，支持多核 CPU ▲2、设备关键芯片采用国产化，包括 CPU 芯片和 NP 芯片。提供第三方测试报告并加盖厂家公章或投标专用章； 3、业务插槽不少于 10 个（主控、风扇、电源、其他扣卡等槽位不及入业务槽位之内）； 4、所有业务板卡支持直接热插拔； 5、整机交换容量不少于 640Gbps； 6、转发性能不少于 60Mpps；	台	2

		7、万兆光口（可自适应千兆）不少于 4 个，千兆电口不少于 10 个； 8、支持 DHCP server/client/relay，PPPoE server/client，NAT，子接口管理； 9、支持 IEEE 802.1P，IEEE 802.1Q，IEEE 802.3 ，VLAN 管理，VLAN 聚合，MAC 管理，STP/RSTP/MSTP，SEP 等； 10、支持静态路由，路由策略，RIP，OSPF，IS-IS，BGP，RIPng，OSPFv3，IS-ISv6，BGP4+等路由协议； 11、支持 IPv6 ND，IPv6 PMTU，IPv6 FIB，IPv6 ACL，ICMPv6，DNSv6，DHCPv6； 12、支持 IPsec VPN，GRE VPN，DSVPN，A2A VPN，L2TP VPN，L2TPv3 VPN； 13、支持 LDP，MPLS L3 VPN，VLL，PWE3，静态 LSP，动态 LSP，MPLS TE，IP FRR，LDP FRR，TE FRR； 14、支持 IPsec 国密算法，SAC 应用阻断，URL 过滤，防火墙功能。 15、配置：双电源，4 个万兆多模模块。		

2	园区核心交换机（澄迈园区核心交换区）	1、交换容量不少于 512Tbps，包转发率不少于 28000Mpps； 2、主控引擎与交换网板物理分离；主控引擎不少于 2 个；独立交换网板不少于 4 块；整机业务板槽位数不少于 8 个，主控槽位与业务线卡槽位宽度相同，为全宽槽位； 3、采用信元交换架构； ▲4、支持每槽位单向转发 能力≥2.4Tbps，提供第三方测试报告并加盖厂家公章或投标专用章； 5、支持颗粒化电源，支持 M+N 电源冗余（AC 和 DC 均支持），电源插槽个数不少于 4 个； 6、支持独立的硬件监控板卡，控制平面和监控平面物理槽位分离，支持 1+1 备份，能集中监控风扇、电源等模块，能调节能耗； 7、支持 VxLAN 功能，支持 VxLAN 二层网关、三层网关，支持 BGP EVPN，支持分布式 Anycast 网关，支持 VxLAN Fabric 的自动化部署； 8、支持交换机作为认证策略实施点，对有线、WLAN 无线用户，进行 802.1x、MAC、Portal 认证； ▲9、支持 ARP 表项≥256K；提供第三方测试报告并加盖厂家公章或投标专用章； 10、支持 4K VLAN，支持 1：1、N：1 VLAN mapping，支持端口 VLAN，支持 Voice VLAN； 11、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；	台	2

		12、支持 PQ、WRR、DRR、PQ+WRR、PQ+DRR 等调度方式； 13、支持真实业务流的实时检测技术，实现对 IP 网络的精确丢包监控和快速故障定界能力； 14、支持硬件 BFD/OAM，3.3ms 稳定均匀发包检测，故障倒换时间小于 50ms； 15、配置：双主控，双电源，满配网板，48 万兆光接口，48 个万兆多模模块。		
3	接入交换机（澄迈园区）	1、交换容量不少于 750Gbps，包转发率不少于 220Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 24 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个。支持 802.3at POE+功能，单端口最大输出 30W，24 端口 POE+满供； 4、支持 MAC 地址不少于 256K,ARP 表项不少于 128K,IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K； 5、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 6、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route； 8、支持多个物理端口的流量镜像到一个端口； 9、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL；	台	10

		10、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机； 11、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 12、支持真实业务流实时检测技术，实时检测网络故障； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块。		
4	24 口 POE 接入交换机（澄迈园区 WIFI 部分）	1、交换容量不少于 750Gbps，包转发率不少于 220Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 24 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个； 4、支持 MAC 地址不少于 256K,ARP 表项不少于 128K,IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K； 5、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 6、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route； 8、支持多个物理端口的流量镜像到一个端口； 9、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL； 10、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast	台	5

		网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机； 11、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 12、支持真实业务流实时检测技术，实时检测网络故障； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块； 15、支持 802.3at POE+功能，单端口最大输出 30W，24 端口 POE+满供		
5	无线控制器（澄迈园区）	1、最大管理 AP 数量不少于 256 个； 2、最大接入用户数量不少于 4K 个； 3、三层转发吞吐量不少于 10Gbps； 4、提供不少于 2 个 10GE 光口，不少于 8 个 GE 电口； 5、支持静态路由，RIP-1/RIP-2，OSPF，BGP，IS-IS，路由策略、策略路由； 6、支持 MAC 地址认证、802.1x 认证（EAP-PAP、EAP-MD5、EAP-PEAP、EAP-TLS、EAP-TTLS）、Portal 认证、MAC+Portal 混合认证、WAPI 认证； 7、支持基于 802.11k 和 802.11v 协议的智能漫游，使低漫游灵敏度的客户端能漫游到最佳 AP； 8、支持 VIP 用户识别和优先调度，VIP 用户可无视任何限速策略，并可获得空口报文的优先级提升； 9、支持定时开关 SSID 功能，在规定的时间内自动关闭指定	台	2

		SSID 的发射信号，方便网络控制； 10、支持广域认证逃生，在 CAPWAP 链路故障后，MAC 或者 802.1x 认证逃生到本地认证 11、支持可视化端到端的故障诊断，显示用户、AP、AC 连接图，呈现故障根因 12、配置：72 个无线管理授权。		
6	面板 AP（澄迈园区）	1、采用 802.11ax 标准，2.4GHz/5GHz 双频段； ▲2、总空间流数不少于 4 条；整机速率不少于 2.9Gbps，提供官网链接及截图并加盖厂家公章或投标专用章； 3、上行不少于 1 个 GE 自适应以太口，下行不少于 1 个 GE 自适应以太口； 4、内置智能天线； 5、支持蓝牙串口无线运维； 6、支持 telemetry，配合服务器可以高速采集 Wi-Fi 的数据； 7、支持 AP 零配置，AP 可以通过 DHCP、DNS 方式自动注册到无线控制器 AC； 8、支持频谱分析功能，对蓝牙设备、数字无绳电话、无线音频发射等干扰源进行识别；	台	25

7	放装AP（澄迈园区）	1、采用802.11ax标准，2.4GHz/5GHz双频段； 2、总空间流数不少于4条；整机速率不少于2.9Gbps； 3、支持不少于1个GE自适应以太口； 4、内置智能天线； 5、支持蓝牙串口无线运维； 6、支持telemetry，配合服务器可以高速采集Wi-Fi的数据； 7、支持AP零配置，AP可以通过DHCP、DNS方式自动注册到无线控制器AC； 8、支持频谱分析功能，对蓝牙设备、数字无绳电话、无线音频发射等干扰源进行识别；	台	32
8	高密AP（澄迈园区）	1、采用802.11ax标准，2.4GHz/5GHz双频段； 2、总空间流数不少于6条；整机速率不少于5Gbps； 3、支持不少于2个GE自适应以太口； 4、内置智能天线； 5、支持蓝牙串口无线运维； 6、支持telemetry，配合服务器可以高速采集Wi-Fi的数据； 7、支持AP零配置，AP可以通过DHCP、DNS方式自动注册到无线控制器AC； 8、支持频谱分析功能，对蓝牙设备、数字无绳电话、无线音频发射等干扰源进行识别；	台	10

9	24 口 POE 接入交换机（澄迈园区监控部分）	1、交换容量不少于 750Gbps，包转发率不少于 220Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 24 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个； 4、支持 MAC 地址不少于 256K,ARP 表项不少于 128K,IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K； 5、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 6、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route； 8、支持多个物理端口的流量镜像到一个端口； 9、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL； 10、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机； 11、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 12、支持真实业务流实时检测技术，实时检测网络故障； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块； 15、支持 802.3at POE+功能，单端口最大输出 30W，24 端口	台	7

		POE+满供。		
10	24口接入交换机（澄迈园区监控部分）	1、交换容量不少于336Gbps，包转发率不少于50Mpps； 2、千兆电口不少于24个，千兆光口不少于4个； 3、支持MAC地址不少于32K，ARP表项不少于2K； 4、支持4K个VLAN，支持Voice VLAN，基于端口的VLAN，基于MAC的VLAN，基于协议的VLAN； 5、支持 1:1 和 N:1 VLAN Mapping 功能； 6、支持静态路由、RIP、RIPng、OSPF等路由协议； 7、支持IPv4 FIB表项不少于4K； 8、支持VLAN内组播转发和组播多VLAN复制； 9、支持防止DOS、ARP攻击功能、ICMP防攻击； 10、支持CPU保护功能； 11、支持以太网环网保护协议ERPS，故障倒换时间小于50ms； 12、支持SP、WRR、SP+WRR等队列调度算法； 13、支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；	台	7

		14、采用静音无风扇设计，环保无噪声； 15、配置：4 个千兆单模模块。		
11	8 口 POE 接入交换机（澄迈园区监控部分）	1、交换容量不少于 336Gbps，包转发率不少于 27Mpps； 2、千兆电口不少于 8 个，千兆光口不少于 4 个，支持 802.3at POE+功能； 3、支持 MAC 地址不少于 32K，ARP 表项不少于 2K； 4、支持 4K 个 VLAN，支持 Voice VLAN，基于端口的 VLAN，基于 MAC 的 VLAN，基于协议的 VLAN； 5、支持 1:1 和 N:1 VLAN Mapping 功能； 6、支持静态路由、RIP、RIPng、OSPF 等路由协议； 7、支持 IPv4 FIB 表项不少于 4K； 8、支持 VLAN 内组播转发和组播多 VLAN 复制； 9、支持防止 DOS、ARP 攻击功能、ICMP 防攻击； 10、支持 CPU 保护功能； 11、支持以太网环网保护协议 ERPS，故障倒换时间小于 50ms； 12、支持 SP、WRR、SP+WRR 等队列调度算法； 13、支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；	台	6

		14、采用静音无风扇设计，环保无噪声； 配置：4 个千兆单模模块		
12	汇聚交换机（海口园区）	1、交换容量不少于 2.5Tbps，包转发率不少于 1600Mpps； 2、支持万兆光口不少于 48 个，40GE 光口（可升级 100GE）不少于 6 个； 3、为了提高设备可靠性，支持可插拔的双电源； 4、为了提高设备散热性能，支持可插拔风扇框，风扇框个数≥4； 5、支持 MAC 表项≥128K； 6、支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN； 7、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 8、支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式，支持对用户进行分组/分域/分时的管理，用户、业务可视可控； 9、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关，支持 VxLAN 的自动化部署；	台	2

		10、支持横向堆叠，主机堆叠数不小于 9 台； 11、支持真实业务流实时检测技术，能实时检测网络故障； 12、支持纵向虚拟化，作为父节点将下联交换机、AP 纵向虚拟为一台设备管理； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块。		
13	接入交换机（海口园区）	1、交换容量不少于 750Gbps，包转发率不少于 220Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 24 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个。支持 802.3at POE+功能，单端口最大输出 30W，24 端口 POE+满供； 4、支持 MAC 地址不少于 256K,ARP 表项不少于 128K,IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K 5、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 6 支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route； 8、支持多个物理端口的流量镜像到一个端口；	台	2

		9、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL； 10、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机 11、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 12、支持真实业务流实时检测技术，实时检测网络故障； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块。		
14	24 口接入交换机（海口园区监控部分）	1、交换容量不少于 336Gbps，包转发率不少于 50Mpps； 2、千兆电口不少于 24 个，千兆光口不少于 4 个； 3、支持 MAC 地址不少于 32K，ARP 表项不少于 2K； 4、支持 4K 个 VLAN，支持 Voice VLAN，基于端口的 VLAN，基于 MAC 的 VLAN，基于协议的 VLAN； 5、支持 1:1 和 N:1 VLAN Mapping 功能； 6、支持静态路由、RIP、RIPng、OSPF 等路由协议； 7、支持 IPv4 FIB 表项不少于 4K； 8、支持 VLAN 内组播转发和组播多 VLAN 复制； 9、支持防止 DOS、ARP 攻击功能、ICMP 防攻击； 10、支持 CPU 保护功能； 11、支持以太网环网保护协议 ERPS，故障倒换时间小于 50ms； 12、支持 SP、WRR、SP+WRR 等队列调度算法； 13、支持通过命令行、Web、中文图形化配置软件等方式进	台	10

		行配置和管理； 14、采用静音无风扇设计，环保无噪声； 15、配置：4 个千兆单模模块。		
15	汇聚交换机（空港园区）	1、交换容量不少于 2.5Tbps，包转发率不少于 1600Mpps； 2、支持万兆光口不少于 48 个，40GE 光口（可升级 100GE）不少于 6 个； 3、为了提高设备可靠性，支持可插拔的双电源； 4、为了提高设备散热性能，支持可插拔风扇框，风扇框个数≥4； 5、支持 MAC 表项≥128K； 6、支持 4K 个 VLAN，支持 Guest VLAN、Voice VLAN，支持基于 MAC/协议/IP 子网/策略/端口的 VLAN； 7、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 8、支持统一用户管理功能，支持 802.1X/MAC/Portal 等多种认证方式，支持对用户进行分组/分域/分时的管理，用户、业务可视可控； 9、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关，支持 VxLAN 的自动化部署； 10、支持横向堆叠，主机堆叠数不小于 9 台；	台	2

		11、支持真实业务流实时检测技术，能实时检测网络故障 12、支持纵向虚拟化，作为父节点将下联交换机、AP 纵向虚拟为一台设备管理； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块。		
16	接入交换机（空港园区）	1、交换容量不少于 750Gbps，包转发率不少于 220Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 24 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个。支持 802.3at POE+功能，单端口最大输出 30W，24 端口 POE+满供； 4、支持 MAC 地址不少于 256K,ARP 表项不少于 128K,IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K； 5、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 6、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route； 8、支持多个物理端口的流量镜像到一个端口； 9、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL； 10、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast	台	2

		网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机； 11、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 12、支持真实业务流实时检测技术，实时检测网络故障； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块。		
17	园区核心交换机（海关核心交换区）	1、交换容量不少于 75Tbps，包转发率不少于 8600Mpps； 2、主控引擎不少于 2 个；整机业务板槽位数不少于 6 个； 3、为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，独立风扇框数不少于 2 块； ▲4、支持颗粒化电源，整机电源槽位数不少于 4 个，实配电源不少于 3000W；提供产品彩页并加盖厂家公章或投标专用章 5、支持独立的硬件监控板卡，控制平面和监控平面物理槽位分离，支持 1+1 备份 6、支持 VxLAN 功能，支持 VxLAN 二层网关、三层网关，支持 BGP EVPN，支持分布式 Anycast 网关，支持 VxLAN Fabric 的自动化部署； 7、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持路由协议多实例；	台	2

		8、支持基于第二层、第三层和第四层的 ACL； 9、支持真实业务流的实时检测技术，秒级快速故障定位； 10、支持硬件 BFD/OAM，3.3ms 稳定均匀发包检测，提高设备的可靠性； 11、支持 DHCP Snooping trust，防止私设 DHCP 服务器； 12、支持 PQ、WRR、DRR、PQ+WRR、PQ+DRR 调度方式； 13、支持 MPLS L3VPN、MPLS L2VPN(VPLS，VLL)、MPLS-TE、MPLS QoS； 14、支持能效以太网功能，IEEE 802.3az； 15、配置：双主控，双电源，48 万兆光接口，48 个万兆多模模块。		
18	接入交换机（海关）	1、交换容量不少于 750Gbps，包转发率不少于 220Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 24 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个。支持 802.3at POE+功能，单端口最大输出 30W，24 端口 POE+满供； 4、支持 MAC 地址不少于 256K，ARP 表项不少于 128K，IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K； 5、支持 4K VLAN，支持 QinQ，灵活 QinQ、支持端口 VLAN、协议 VLAN、IP 子网 VLAN； 6、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、	台	2

		IS-IS、Static Route； 8、支持多个物理端口的流量镜像到一个端口； 9、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL； 10、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机； 11、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS； 12、支持真实业务流实时检测技术，实时检测网络故障； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块。		
19	园区核心交换机（管理区数据中心业务交换区）	1、交换容量不少于 387Tbps，包转发率不少于 115000 Mpps； 2、业务槽位数不少于 4 个。交换网板插槽数量不少于 6 个，且支持网板 N+M 冗余； 3、风扇框冗余设计，要求风扇框个数不少于 3 个 4、支持 RIP、OSPF、ISIS、BGP 等 IPv4 动态路由协议； 5、支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议； 6、支持 IP 分片和重组； 7、支持 PQ、DRR、PQ+DRR 等队列调度方式； 8、支持 BFD for M-LAG，支持 BFD 3.3ms 检测间隔； 9、支持集群或堆叠多虚一技术，实现单一界面管理多台设备；	台	2

		10、支持 Vxlan 协议，且支持 BGP EVPN 协议； 11、配置：双主控，四电源，满配交换网板，24 个 40GE 光接口，48 个万兆光接口，12 个 40GE 多模模块，48 个万兆多模模块		
20	接入交换机（安全管理中心）	1、交换容量不少于 750Gbps，包转发率不少于 220Mpps； 2、为了提高设备可靠性，支持模块化可插拔双电源； 3、支持千兆电口不少于 24 个，万兆光口不少于 4 个，业务扩展插槽数不少于 1 个。支持 802.3at POE+功能，单端口最大输出 30W，24 端口 POE+满供； 4、支持 MAC 地址不少于 256K,ARP 表项不少于 128K,IPv4 路由表不低于 512K，IPv6 路由表不低于≥64K； 6、支持静态路由、RIP V1/2、URPF、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6； 7、支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route； 8、支持多个物理端口的流量镜像到一个端口； 9、支持基于第二层、第三层和第四层的 ACL、支持双向 ACL； 10、支持 VxLAN 功能，支持 BGP EVPN，支持分布式 Anycast 网关；支持控制器基于 WEB 界面进行 VxLAN Fabric 配置并下发给交换机，； 11、支持 MPLS L3VPN、MPLS L2VPN(VPLS/VLL)、MPLS-TE、MPLS QoS；	台	2

		12、支持真实业务流实时检测技术，实时检测网络故障； 13、支持 SNMPv1/v2c/v3，支持 RMON、WEB 网管特性； 14、配置：双电源，4 个万兆多模模块。		
21	物联网平台	设备统一接入：平台支持海量设备连接上云，设备与平台通过 IoT Hub 进行稳定可靠地双向通信。支持主流通信协议及行业协议，支持蜂窝、非蜂窝网络设备接入，支持各种物联网接入协议类型，包括 MQTT、CoAP、LwM2M、HTTP 等常见接入协议 ； 设备统一管理：提供丰富的行业标准物模型，赋能设备行业属性，提供精细化的设备生命周期管理，包括设备注册、数据查询、文件管理、泛协议服务、设备授权； 行业应用赋能：通过平台开放 API 接口、SDK 对接、消息队列、规则引擎、场景联动，支持行业标准应用打造； 可视化呈现：通过物模型采集生产过程中的大量数据，使数据结构化，便于平台进行数据分析和数据展示。 自动化运维：平台提供了设备的实时数据查询、远程控制、远程升级、告警处理、日志查询等功能，为客户提供自动化的设备监控运维能力 网络故障定位：平台与物联网卡连接管理平台实现联动，为	套	1

		客户提供蜂窝设备的网络状态查询和故障定位、设备位置服务、设备低功耗配置等能力		
22	物联网网关	网络制式：4G 、3G、2G 内存：128M CPU：ARM9 高速微处理器 接口类型：2 个蜂窝网天线接口（MAIN+AUX） 、1 个 LAN 接口（10/100Mbps自适应） 、1 个 USB2.0 接口 、1 个 RS232 接口、1 个 RS485 接口 、2 个 Mini SIM 卡（单 3.0V/1.8V） 南向对接：透传、TCP 客户端/服务器、UDP、Modbus RTU 网关 4G 频段：1880-1900MHz、2320-2370MHz、2575-2635MHz 北向对接：支持 PPP、 PPPoE、 TCP、 UDP、 DHCP、 ICMP、 NAT、 HTTP、 HTTPs、DNS、 ARP、 RIP、 OSPF、 NTP、 SMTP、 Telnet、 VLAN 等网络协议	台	100
23	园区光纤网络	园区内部光纤网络实施，含光电转换器等配套；国产	点	120

24	网管软件	1、硬件要求：2 块 4210-10Core/2.2GHz CPU,2 条 32GB 内存,2 块 1200GB SAS HDD,(2G cache)Raid 卡+电容,4 块 2 个 GE 接口,2 块 900W AC； 2、系统使用 B/S 架构，支持 IE、Firefox、Chrome 等主流浏览器； 3、支持完全自主的操作系统、数据库，并能集成交付； 4、支持多种设备的管理，包括交换机、路由器、防火墙、WLAN、服务器、存储、IP 话机、摄像头、eLTE、GPON 设备； 5、支持资源分组管理：按照设备名称、类型、子网、厂商、IP 地址自定义设备分组，设备增加完成后能够按照预置和自定义设备分组自动分组； 6、支持以拓扑图的方式直观显示被管网元及其之间的连接关系和状态，提供左树右图的拓扑展现方式，对拓扑对象通过子网进行分层展示； 7、支持将有线、无线设备虚拟成一台设备进行管理，接入交换机、AP 无须配置单独的管理地址，所有接入设备的管理均通过管理设备实现，支持通过查看管理设备的面板来查看整个网络的状态。 8、支持告警信息中包含与故障关联的信息（如端口故障需关联呈现端口信息、故障信息、链路拓扑信息、历史流量信息、维护经验等）。 9、提供告警、性能、有线无线资源、用户终端定位信息等报表管理能力；	台	1

		10、提供交换机、WLAN、路由器、防火墙设备的软件和补丁升级能力，支持防火墙的特征库升级； 11、支持区域内用户的网络使用质量分析能力，并以区域维度进行信息汇聚（如区域内低速率用户占比、高丢包率 AP 占比、高掉线率 AP 占比等）在拓扑上呈现。 12、支持基于真实流的 IP 网络实时监测能力（非模拟报文监测或者探针式监测），监测结果可实时在拓扑上显示。 13、支持不同维度（设备、接口、应用、DSCP、主机、会话、接口组、IP 组、应用组、DSCP 组）的流量图表查看功能，并支持下钻一层深入详细分析流量数据； 14、配置：100 个网络设备管理授权，72 个无线设备管理授权，硬件 3 年维保服务。		
25	网管专用终端	I5 /8G DDR4/1TB/HDD/集成显卡/有线键盘/有线鼠标/PCI-E X 16 插槽*1/PCI-E X 1 插槽*2/UDIMM 插槽*2/支持 USB 端口安全管控/显示器 23.8 英寸（黑色）全面屏高清办公显示器	台	1
26	配套辅材	线缆、光模块、尾纤等；国产	批	1
27	综合布线施工	综合布线施工与改造	批	1
	小计 30			
9	**5G 边**			

.2	**缘云**			
1	UPF（核心网边缘用户面网元硬件+软件）	1、吞吐能力（Gbps）：15； 2、会话处理能力（万 PDU）：3.5； ▲3、UPF 设备支持极简组网，支持免 EOR 方式部署，软硬件均满足 1+1 冗余要求；需提供产品彩页并加盖厂家公章或投标专用章； 4、设备具备转发增强能力，单套 UPF 可最大扩展至 100Gbps 能力，100Gbps 规格下，UPF（含 EOR）可实现共柜部署； 5、设备支持 NFV 虚拟化平台，支持 N-WAY 冗余，支持热插拔功能； 6、单套设备满配支持最大同时附着 20 万用户数； 7、支持远程集中运维和本地运维； 8、支持基于业务感知的带宽管理； 9、支持内置 IPSec 业务能力，支持 N3/N4/N9/N6 接口数据加密保护。 10、支持 HTTP/DNS 计费防欺诈、支持 HTTP/HTTPS/RTSP 头增强、支持 HTTPS/HTTP2.0 业务识别和策略控制、支持 HTTP/IP 重定向； 电源：220V 交流。	套	1

2	边缘云平台服务器	1、CPU：主频≥2.4Ghz 核数≥16 核 个数≥2 3、内存：512GB； 4、磁盘：≥300GB、≥SAS 硬盘*3；≥10TB【6Gbps sata,7200rpm】*6 5、HBA 卡：≥16Gb 光纤通道卡*2（需配备相应模块及线缆）； 6、网卡：万兆 SFP+网卡*2（配备相应模块及线缆）*2、千兆网口≥2； 7、≥1.3TB NVMe PCIe ssd 固态盘 *1； 8、RAID 卡：配置 RAID 控制器，支持 RAID 0，1，5； 9、配置冗余电源； 10、配置冗余风扇； 11、管理口（全功能授权）：配置 IPMI（平台管理接口）。监视服务器的物理健康特征，如温度、电压、风扇工作状态、电源状态等；故障日志记录和 SNMP 警报发送；访问系统事件日志（System Event Log ,SEL）和传感器状况；控制包括开机和关机。 12、售后服务：所有硬件包含 3 年 7*24 原厂售后服务。	台	3
3	GPU 服务器	图像和图形相关运算工作，支持远程管理、远程安装操作系统、冗余电源冗余风扇；同时支持视频流解析；不低于配置 16 张 P4 卡 GPU 服务器的处理性能。	台	1
4	边缘云计算虚	边缘云计算虚拟化、终端接入安全管控应用软件、客户边缘数据服务平台应用软件	套	1

	拟化软件			
5	边缘云平台防火墙	网络处理能力≥40G，并发连接≥460 万，每秒新建连接≥28 万/秒， 冗余电源，配置≥6 个 10/100/1000M 自适应电口，配置≥4 个 SFP+插槽（含万兆光模块）， 含三年硬件维保服务。含 3 年病毒防护特征库升级服务，3 年入侵防御特征库升级服务 防火墙产品通过中国国家信息安全产品认证； 防火墙产品获得公安部《计算机信息系统安全专用产品》销售许可证； 防火墙产品经中国泰尔实验室检验通过。	台	2
6	业务交换机	24 口 10GE 光交换机，配 10 个多模 10GE 光模块	台	2
7	管理交换机	24 口 GE 电口交换机	台	2
8	5G CPE	支持 5G 接入	台	60
	小计 31			
1	**网络**			

0	**安全设施**			
10.1	**网络基础安全设备**			
1	互联网边界防火墙	标准配置≥6 个 10/100/1000M 自适应电口，≥4 个 SFP 插槽或接口，1 个 Console 口；多核架构，网络处理能力≥10G，并发连接≥260 万，每秒新建连接 18 万/秒。配置三年防火墙功能模块授权（包含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务），提供三年硬件维保服务。 支持本地的威胁情报对可疑行为进行深入分析，阻断病毒扩散、漏洞入侵，并实时预警； 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索。可在策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项； 支持恶意行为的审计，包括攻击、病毒防护、木马防护等。 支持将恶意源地址加入或批量导入到黑名单的操作； 支持对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀；本地病毒库规模大于 500 万。 ▲提供基于云构筑的安全分析 SaaS 服务能力，无需在客户	台	2

		处部署任何软件平台，SaaS 服务基于安全防御节点上送的安全日志能够进行日志的聚合、分析、判定动作，去除安全日志的噪音，可在安全日志分析后标注为“确认为攻击”、“已下发告警”等状态，在用户授权下为用户提供精准的安全威胁事件展示和自动进行外部攻击者 IP 的封禁。提供产品彩页或功能截图并加盖厂家公章或投标专用章；		
2	服务器防火墙（物理机集群区）	配置≥8 个千兆电口，≥8 个 SFP 插槽或接口，大于等于 4 个万兆 SFP+插槽或接口，1 个 Console 口 、1 个 HA 接口，1 个 MGT 接口。多核架构，网络层吞吐量≥30G，并发连接≥400 万，每秒新建连接数 28 万。配置三年防火墙功能模块授权（包含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务） ，提供三年硬件维保服务。 支持本地的威胁情报对可疑行为进行深入分析，阻断病毒扩散、漏洞入侵，并实时预警； 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索。可在策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项； 支持恶意行为的审计，包括攻击、病毒防护、木马防护等。 支持将恶意源地址加入或批量导入到黑名单的操作； 支持对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀；本地病毒库规模大于 500 万。	台	2

3	电子政务外网互联网区专线防火墙	配置≥6 个 10/100/1000M 自适应电口，另有≥1 个接口板卡扩展插槽，1 个 Console 口。多核架构，网络层吞吐量≥6G，并发连接≥200 万，每秒新建连接数≥6 万。配置三年防火墙功能模块授权（包含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务），提供三年硬件维保服务。 支持本地的威胁情报对可疑行为进行深入分析，阻断病毒扩散、漏洞入侵，并实时预警； 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索。可在策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项； 支持恶意行为的审计，包括攻击、病毒防护、木马防护等。 支持将恶意源地址加入或批量导入到黑名单的操作； 支持对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀；本地病毒库规模大于 500 万。	台	1
4	园区接入防火墙	配置≥6 个 10/100/1000M 自适应电口，≥2 个 SFP 插槽或接口，1 个 Console 口。多核架构，网络处理能力为 10G，并发连接≥260 万，每秒新建连接 18 万/秒。配置三年防火墙功能模块授权（包含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务），提供三年硬件维保服务。 支持本地的威胁情报对可疑行为进行深入分析，阻断病毒扩	台	2

		散、漏洞入侵，并实时预警； 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索。可在策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项； 支持恶意行为的审计，包括攻击、病毒防护、木马防护等。 支持将恶意源地址加入或批量导入到黑名单的操作； 支持对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀；本地病毒库规模大于 500 万。		
5	管理区防火墙	配置≥6 个 10/100/1000M 自适应电口，≥2 个 SFP 插槽或接口，1 个 Console 口。多核架构，网络处理能力为 10G，并发连接≥260 万，每秒新建连接 18 万/秒。配置三年防火墙功能模块授权（包含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务），提供三年硬件维保服务。 支持本地的威胁情报对可疑行为进行深入分析，阻断病毒扩散、漏洞入侵，并实时预警； 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索。可在策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项； 支持对最多 6 级的压缩文件进行解压查杀； 支持恶意行为的审计，包括攻击、病毒防护、木马防护等。	台	2

		支持将恶意源地址加入或批量导入到黑名单的操作； 支持对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀；本地病毒库规模大于 500 万。		
5	办公区防火墙	配置≥6 个 10/100/1000M 自适应电口，≥2 个 SFP 插槽或接口，1 个 Console 口。多核架构，网络处理能力为 10G，并发连接≥260 万，每秒新建连接 18 万/秒。配置三年防火墙功能模块授权（包含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务），提供三年硬件维保服务。 支持本地的威胁情报对可疑行为进行深入分析，阻断病毒扩散、漏洞入侵，并实时预警； 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索。可在策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项； 支持对最多 6 级的压缩文件进行解压查杀； 支持恶意行为的审计，包括攻击、病毒防护、木马防护等。 支持将恶意源地址加入或批量导入到黑名单的操作； 支持对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀；本地病毒库规模大于 500 万。	台	2

6	物联网区防火墙	配置≥6 个 10/100/1000M 自适应电口，≥2 个 SFP 插槽或接口，1 个 Console 口。多核架构，网络处理能力为 10G，并发连接≥260 万，每秒新建连接 18 万/秒。配置三年防火墙功能模块授权（包含威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务），提供三年硬件维保服务。 支持本地的威胁情报对可疑行为进行深入分析，阻断病毒扩散、漏洞入侵，并实时预警； 支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索。可在策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项； 支持对最多 6 级的压缩文件进行解压查杀； 支持恶意行为的审计，包括攻击、病毒防护、木马防护等。 支持将恶意源地址加入或批量导入到黑名单的操作； 支持对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀；本地病毒库规模大于 500 万。	台	2

7	上网行为管理	标配≥6 个千兆电接口；≥2 个万兆 SPF+光口；≥1 个管理接口。最大并发连接数为≥60 万;最大新建连接数为 4 万/秒；含网页过滤、用户认证、应用控制、内容审计、带宽管理、行为监控分析等功能；提供新版本功能优化与性能提升，URL 库、应用协议库定期更新;含一年硬件质保服务 支持 IPv6 环境下的网址访问审计、生成分析报表等功能； 支持标准 IPSec 协议的 VPN 功能,能够实现隧道建立于配置、隧道状态监视、证书管理等内容； 可集中呈现上网行为风险等级和状态； 支持行为风险等级包括安全等级、效率等级、合规等级和管控等级； 支持行为状态包括管控效果、运行状态、安全状态、泄密风险状态、合规状态和应用使用状态；点击页面数值可直接跳转查询详情。； 支持自动识别网络中终端的 IP 地址、MAC 地址、终端类型、操作系统、终端厂商和网卡厂商等信息； 支持自动发现网络中通过无线上网的热点和移动终端的 IP 和终端类型，支持移动终端型号识别，至少识别不少于 10 种移动终端型号； 对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等，支持查看终端类型，以及厂商、系统、端口等详细信息； 支持自动扫描发现网络中已占用的 IP 地址，支持图形化展	台	2

		示某个 IP 地址的在线状态、当前使用者、MAC 地址和活跃时间； 支持本地中英文 Web 界面管理及命令行管理，支持基于 SSL 协议的远程安全管理。		
8	日志审计	≥6 个千兆电口，≥1 个 Console 接口。包含三年硬件标准维保，三年软件升级服务；资产授权数≥250； 支持无需另外安装软件组件，管理中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、文件\文件夹、WMI、FTP、SFTP、NetBIOS 等多种方式完成日志收集功能；可灵活定制不支持的数据源采集，而无须改动代码； 支持无需另外安装软件组件，审计中心即可实现新增 Oracle 数据库自身日志的采集任务、新增 SQL Server 数据库自身日志的采集任务、新增 Apache 服务器日志的采集任务； 系统具有资产管理的功能，能够将被审计资产进行分组、分域 的统一维护。支持对资产增删改查以及批量导入导出； 工作台为用户提供了一个从用户自身业务需要出发使用本系统的快速入口。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；	台	1

		支持可以对选中的日志进行事件拓扑分析，并可视化的展示一幅描述日志之间的行为相关关系的事件拓扑图。		
9	运维审计系统	支持 6 个千兆电口；支持 2 个接口扩展槽位；内置≥2TB 硬盘；冗余电源；采用专用千兆多核硬件平台和安全操作系统；最大支持≥200 路图形会话或≥350 路字符会话并发；配置 600 个授权许可，20 个 USBKey。提供三年标准售后服务。 支持多因子认证，方式包括手机令牌、手机短信、动态令牌等多因子认证方式； 支持自定义角色权限，支持角色权限细粒度划分，包括安全配置、网络配置、端口配置、认证配置、告警配置等权限划分； 支持使用浏览器通过H5方式即可直接运维SSH、RDP、Telnet、VNC、SFTP 资源，支持的运维协议包含 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server 等； 支持使用 XShell、Putty、SecureCRT、MSTSC、PLSQL 等客户端访问资源； 支持双因素组合认证，可以将两种认证方式自定义组合为全新的认证方式 支持按不同属性对资产进行多级分类并自动生成树状结构的资源视图	台	1

		针对基于云盘模式的文件传输操作：用户将文件暂存在系统上，然后一键上传到目标系统或者一键下载到用户本地，同时可通过文件分享功能以URL链接的方式将文件分享给其他用户		
10	漏洞扫描系统	标准配置6个10/100/1000M自适应电口,2个USB口，1个Console口，单电源。Web扫描域名≥200，Web扫描任务并发数为5个域名。系统扫描IP地址支持≥1000个，支持扫描A类、B类、C类地址，系统扫描支持50个IP地址并行扫描。配置三年漏洞特征库升级，提供三年硬件维修服务. 支持同时下发系统扫描、Web扫描、弱口令扫描任务，无需单独下发扫描任务，扫描目标可以是IP、域名、URL的任一格式； 支持扫描国产系统、数据库扫描。国产操作系统包括中兴新支点、中标麒麟等，国产数据库包括神通、人大金仓、南大通用、达梦； 支持对系统存在的弱口令做检测，支持知名的协议、数据库、中间件、HTTP服务、HTTPS服务如TELNET、FTP、SSH、POP3、RDP、SMTP、Oracle、MySQL、PostgreSQL、MsSQL、Sybase、Informix、HTTP等。 网络配置需提供快速配置向导，支持快速部署上线 支持检测的漏洞数大于65000条以上，涵盖漏洞标准包含	台	1

		CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq6 种，CVSS 覆盖 CVSS2 和 CVSS3 版本；		
11	主机安全管理系统	包含一套管理中心系统软件，支持主流 Windows Server 及 Linux 操作系统。 配置 500 点客户端授权，包含防病毒、补丁管理、主机防火墙、终端管控、终端数据防泄漏功能。支持主流 Windows PC 客户端操作系统，提供三年更新服务。 支持展示在线终端详细信息。 支持终端进程黑名单、白名单功能。 支持对终端各种外设、接口设置使用权限，并支持生效时间设置。 支持对互联网出口地址探测。 ▲具备人工智能引擎，人工智能引擎支持 PE/OFFICE/PDF 常见文件类型威胁检测,提供功能截图并加盖厂家公章或投标专用章； 支持 ARP 欺骗防御，支持网关和 DNS 绑定。 支持扫描过程中动态切换扫描速度，支持多核极速、多核高速、单核节能三种工作模式。	台	1

12	攻击预警平台	配置 6 千兆网口，包含基础系统软件一套，包括网页漏洞利用检测、webshell 上传检测、网络攻击检测、威胁情报检测功能。吞吐 1Gbps；配置高级扩展功能模块，包括威胁感知，响应处置，态势大屏等高级功能；配置恶意文件分析功能模块,对流量中还原的文件进行检测，并支持云查杀。配置文件动态检测功能模块。提供三年威胁情报与检测引擎规则升级授权，三年产品标准维保服务。 支持检测多种网络协议中的攻击行为，提供 ids、webids、webshell、威胁情报多种维度的告警展示，支持检测如多种网络应用、木马、广告、exploit 等多种网络攻击行为，支持检测如 sql 注入、跨站、webshell、命令执行、文件包含等多种 web 攻击行为，支持检测 php 后门并记录相关信息，拥有威胁情报实时匹配能力，能发现恶意软件、APT 事件等威胁，产生的多种告警都会加密，并传输给分析平台进行统一分析管理； 支持多种攻击检测，能更全面的从流量中发现威胁，如：信息泄露、间谍软件、协议异常、网络欺骗、代码执行等； 支持提供多种报表模版，模版包括告警、受害资产、日志、威胁分析等等，支持与云端安全运营中心联动。设备能连接互联网时，安全专家在云端分析并撰写威胁分析报告下发到设备上共用户查阅；设备离线时，可将关键数据离线导出上传到云端安全运营中心，安全专家进行分析撰写威胁分析报告；	台	1

		支持根据威胁等级、攻击结果、威胁类型、网络日志筛选并通过 syslog 发送威胁告警，告警包含网页漏洞利用、webshell 上传、网络攻击、威胁情报和恶意文件等。		
13	网闸	内网接口：6 个 10/100/1000Base-T 端口，4 个 SFP 插槽,2 个 SFP+插槽，1 个 Console 口，2 个 USB 口；≥64G 硬盘; 外网接口：6 个 10/100/1000Base-T 端口，4 个 SFP 插槽,2 个 SFP+插槽，1 个 Console 口，2 个 USB 口，≥64G 硬盘;应用层吞吐≥5Gbps ，应用层并发连接≥15 万条；功能模块：数据库同步、文件交换、数据库访问、视频模块、邮件访问、安全浏览、安全 FTP、定制模块、工控访问等；提供三年硬件维保。 支持文件同步，文件同步支持 FTP、SFTP、SMB、NFS 等协议； 支持 MySQL、ORACLE、ORACLE_RAC、SQLServer、DB2、SYBASE、POSTGRESQL 等常见数据库，支持神通、达梦、人大金仓、南大通用等国产数据库同步； 支持 MySQL、ORACLE、SQLServer、DB2、SYBASE、POSTGRESQL、达梦、神通、人大金仓等数据库的访问； 支持视频访问，支持 28181、DB33 标准。	台	2

14	SSL VPN	接口配置≥6 个千兆电口，≥2Combo（含一个管理口）。含链路加密、访问控制、门户式单点登录、日志追溯等功能； 配置≥300 个 SSL VPN 授权，提供三年硬件质保服务; SSL VPN 支持页面定制功能特性，包括登录页面、交互信息、提示信息的定制功能； 支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的自动批量和手动逐条策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略	台	1
15	数据库与防护系统	接口配置≥6 个千兆自适应电口，≥1 个 Console 口。SQL 审计处理能力（速率）≥34000SQL/S，硬盘总容量≥2TB，提供三年软件升级，三年硬件维修服务。 支持针对 IPv6 协议的审计，通过 IPv6 的地址检索事件； 支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase、神舟通用、Cache 等； 支持白名单管理，根据白名单支持数据库操作命令，支持对系统语句的过滤； 支持对 HTTP、FTP、TELNET、SMTP、NFS 协议的审计； 支持将多个数据库 IP 绑定为一个业务系统，后期的数据分析如流量、用户数和操作行为等，均以业务视角的方式分析展示	台	1

16	web 应用防火墙	接口配置≥6 个千兆自适应电口（含 2 组 bypass），≥8 个千兆 SFP 插槽或接口，≥1 个 Console 口，≥2 个 USB 口，网络吞吐量≥6Gbps，应用层吞吐量≥1Gbps，HTTP 并发连接数≥80 万。提供三年 WAF 软件特征库服务，三年硬件维修服务。 支持 Web 业务控制防御功能，提供针对爬虫、黑链等防护功能； 支持 SQL 注入、XSS 跨站攻击防御策略，支持特征检测与语义算法检测； 支持防护 SQL 注入、XSS 攻击、Web 漏洞攻击等； 支持 HTTP 访问控制，可根据实际网络状况自定义请求方法等参数的访问控制规则； ▲支持防护资产安全状态展示，可针对资产的 TCP,UDP,ICMP/ICMP6,RAW-IP,HTTP,DNS 等数据进行统计，提供具有 CNAS 或 CMA 机构认可的第三方检测机构出具的检测报告复印件并加盖厂家公章或投标专用章）	台	2
	小计 32			
10.2	**安全管理中心**			

1	态势感知平台	1、支持异常流量检测，包括：网络层、应用层 Flood 检测，恶意扫描检测、异常包攻击检测等； 2、支持支解析多种协议，包括：HTTP、DNS、FTP、ICMP、IMAP、POP3、RIP 等，可针对协议类型检测攻击事件、恶意文件等； 3、支持漏洞自动关联到受影响的资产，支持漏洞标签功能，支持标签的添加、删除、编辑、检索，支持批量添加漏洞标签信息； 4、支持识别网络威胁数据：失陷检测、入侵检测、病毒检测、异常流量、DDoS 攻击、应用识别等 5、支持威胁场景分析，覆盖网络流量传感器、Windows、Linux、防火墙、VPN 等多类数据源，预置关联分析规则； 6、支持使用多种逻辑运算和关系运算进行复杂搜索的能力，支持对展示字段数据范围快捷操作。	套	1
2		CPU:≥2 颗 10 核 主频≥2.0GHz 内存≥256G（总容量）DDR4；12*4TB 企业级 SATA 3.5 寸硬盘，总容量 48T； 网口≥4*GE 管理电口、≥2*SPF+插槽（含两个多模光模块）；	台	3
3	流量探针（7G）	流量采集探针： 1、支持开启网络流量采集、威胁数据采集和日志上报功能情况下混合流吞吐量≥7Gbps HTTP 并发连接数 700 万 HTTP 新建连接速率 25 万/秒；≥标准配置 1 个 10/100/1000M 专用管理接口 1 个 Console 口，≥4 个千兆光口，≥2 个万兆光口，≥4 个接口扩展板卡插槽，提供三年全功能特征库升	台	1

		级服务，包括三年硬件维修服务。 2、支持通过流量镜像的方式旁路部署在虚拟化网络中，实现网络流量数据采集、威胁检测和日志外发，支持通过流量被动识别资产； 3、支持自定义解析流量，支持基于正则表达式对应用流量解析； 4、支持本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于 100 万； 5、系统需具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报；		
4	流量探针（3G）	流量采集探针： 1、支持开启网络流量采集、威胁数据采集和日志上报功能情况下混合流（模拟企业级网络真实场景流量）吞吐量≥3Gbps，HTTP 并发连接数 400 万，HTTP 新建连接速率 15 万/秒；2U 机箱，单电源，标准配置 6 个 10/100/1000M 自适应千兆电口，1 个 Console 口，2 个接口扩展板卡插槽，提供三年全功能特征库升级服务，包括三年硬件维修服务。 2、支持通过流量镜像的方式旁路部署在虚拟化网络中，实现网络流量数据采集、威胁检测和日志外发，支持通过流量被动识别资产； 3、支持自定义解析流量，支持基于正则表达式对应用流量解析； 4、支持本地集成威胁情报库，支持实现基于威胁情报的失	台	2

		陷主机检测，情报不少于 100 万； 5、系统需具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报；		
	小计 33			
10.3	**物联网安全管理**			
1	物联网安全感知与管理平台	1、终端采集数据接收：无缝对接终端防护系统及物联网安全监管系统上报终端数据及安全数据，并支持关联处置。 2、威胁分析：支持针对物联网常见安全威胁进行大数据分析，包括不限于以下威胁：设备状态异常、ARP 扫描、敏感端口扫描、IP 地址嗅探、异常失败连接、暴力破解攻击、ARP 欺骗、专网渗透、远程异常连接、违规外联等 3、资产管理：支持按照年度月增长资产数量，资产在线离线状态、风险资产占比、资产类型分布、资产安全域分布，一览资产概况。 4、隐患管理：针对安全隐患、漏洞、告警、弱口令从多维度进行统计分析，支持各类告警的安全验证。帮助用户了解整网潜在安全威胁。以漏洞为视角，展示漏洞最新发现时间、漏洞类型、漏洞等级、以及影响的资产数量和资产所在安全	套	1

		域等信息，在漏洞详情中展示更多漏洞信息包括漏洞基本信息、漏洞简介以及修复建议等，并展示当前漏洞所影响的所有资产，支持资产多条件检索。 5、威胁告警：展示所有的告警情况，包括告警等级、告警名称、最新发现时间等信息，点击告警管理+安全告警进入安全告警页面；支持针对安全告警威胁等级分布情况了解整网安全防护状态以及薄弱环节，针对性发现薄弱点设备类型、厂商、安全域分布，便于用户执行针对性修复方案。 6、提供物联网资产状态、漏洞状态、攻击威胁及非法接入等维度发现能力，提高安全运营效率，实现全网资产（可管、可控、可知）集中管控、终端隐患实时监测、终端安全威胁实时感知。		
2		专用硬件服务器：网口类型：2 个千兆电口\电源：双电源\CPU： 6 核 6 线程\规格：2U\内存：64G\硬盘：2*4T	台	1

3	物联网监管系统	1、设备安全监测：可进行自定义监测频率设置，并对全网设备进行安全检测。 能够对在网资产的设备类型、品牌型号、操作系统、应用名称、版本、端口等信息进行识别。可对资产的在线状态、资产变更进行监测。可对视频设备进行安全漏洞扫描检测，分析设备安全风险状况。 2、信令安全监测：支持对设备进行视频信令安全检测 3、边界安全监测：实现不间断对全网进行边界安全检测。可显示网闸设备、小型路由器、代理服务器等边界安全设备的监测信息。 4、网内攻击监测：实现对网络中存在的网内攻击行为进行检测，包括： 恶意扫描——监测网络中频繁或大规模的访问其它主机设备、服务端口的行为，提供发起扫描的设备地址、被扫描最多主机、被扫描最多端口等详细信息。 5、异常行为监测：实现对网络中存在的异常行为进行监测，包括：频繁访问业务系统——监测对特定业务系统的进行频繁访问的异常行为，提供频繁访问业务系统的终端设备地址、所在位置、被访问系统的地址、端口、名称等详细信息。 6、安全隐患监测：实现对网络中存在的安全隐患进行监测，包括： 脆弱性——对使用弱口令、设备端口的安全风险隐患进行监测和发现。用户可以自定义扫描目标、类型、扫描时间策略。	套	1

		系统会根据设备类型进行漏洞扫描。 7、违规行为监测：实现对网络中存在的违规行为进行监测，包括：监测网络违规设备（移动设备/Windows 8 系统）接入，提供设备接入地址、设备类型、所在地市位置等信息。 8、数据取证：支持对发现的监测告警行为提供数据取证功能： 9、报表功能：提供报表自动生成功能。提供灵活的报表策略管理，可根据策略自动生成报表，并自动通过邮件发送给接收者。 10、告警管理：提供告警事件类型、类别、等级、内容、告警时间、持续等告警事件管理。提供告警事件名称、类型、状态、级别、告警时间、签收时间、处理时间、处理人、处理结果等告警事件处置管理。 11、用户管理：提供用户的增删改查等管理功能。 12、日志管理：提供系统操作的操作人、时间、类型、事件、访问地址等在内的日志记录。 13、探测策略管理：提供可自定义配置的探测策略管理。		
4		专用硬件服务器：最大资产识别数：≥5000；网口类型： ≥2*千兆电口+≥2*千兆光口；内存：≥96G 硬盘：≥2T	台	1
5	网络准入控制系统	1）硬件规格：硬件服务器品牌工控机、规格 2U、CPU4 核 4 线程、内存 16G、硬盘≥1T、6 千兆口； 2）最大支持 5000 台无代理软件设备安全管理（支持瘦终端、IoT 设备）；	台	3

		3）支持策略路由； 4）支持系统内置帐号认证、AD/LDAP 帐号认证、邮件帐号认证等多种身份认证方式； 5）支持入网安全状态检查、网络访问权限控制、仿冒发现控制、违规外联发现控制、访客外协准入管理等； 6）提供三年维保服务		
	小计34			
10.4	**密码应用**			
1	密码安全	与海南省云密码平台对接	套	1
	小计35			
	合计			

注：上述硬件平台若涉及品牌、型号等，并不是采购人拟指定该品牌、型号的意思表示，而是为了更好的表述技术要求，各投标人可投报产品技术性能相当于或高于所列品牌、型号的产品，但必须保证系统正常运行且符合国家现行标准。

通信服务清单

序号	名称	相关指标或用途说明	单位	数量
一	**链路费**			
1	园区 100M 云专线	园区老城中心机房至电子政务云，100M 专线两条，两年服务费	条/年	4
2	园区骨干互联专线	园区老城中心机房至海口园区机房、空港园区机房，1000M 专线，各两条，两年服务费	条/年	8
3	园区 100M 云专线	园区 100M 云专线 园区老城中心机房至省内云服务商机房 100M 专线 2 条，两年服务费	条/年	4
4	园区互联网专线	园区老城中心机房至互联网，作为园区互联网统一出口，1000M 两条，两年服务费	条/年	4
5	园区 100M 云联网	园区老城中心机房至云服务商云平台，100M 云联网 2 条，两年服务费	条/年	4
6	海关骨干互联专线	海关老城中心机房至空	条/年	4

		港园区机房，1000M 专线两条，两年服务费		
7	国际互联网专线	海南自贸港国际互联网数据专用通道（20M）	条/年	1
8	物联网流量费	物联网设备流量使用费，按 1.5 万 GB/年预估，两年服务费	GB	3750
9	短信费用	为园区管理、园区服务等场景提供短信通知服务，每年预估 60 万条，两年服务费	条	150000

演示清单

系统演示清单

序号	名　称	子　项	模　块
1	园区公共服务平台	园区统一门户	首页（用户注册）
2			首页（系统集成）
3			首页（单点登录）
4			园区概况-园区机构（机构概况）
5			园区概况-园区机构（领导信息）
6			园区概况-园区机构（机构职能）
7			园区概况-园区企业介绍
8			园区概况-基础设施介绍

9			园区概况-园区优势介绍
10			园区概况-优惠政策介绍
11			园区概况-高效率审批
12			我要投资-招商引资（入区流程）
13			我要投资-招商引资（产业定位）
14			我要投资-招商引资（招商方向）
15			我要投资-招商引资（比较发展）
16			我要咨询-在线交流（常见问题）
17			我要咨询-在线交流（留言查询）
18			我要咨询-互动交流（提问管理）
19			我要投诉-在线投诉
20			我要投诉-投诉管理
21			案例展示
22			园区动态（园区新闻）
23			园区动态（国务院新闻）
24			园区动态（省府新闻）
25			园区动态（媒体报道）
26			专题解读（最新解读）
27			专题解读（回应关切）
28			专题解读（新闻发布会）
29			信息公开
30			数说园区（企业注册数据采集）
31			数说园区（跨境申报数据采集）

32			数说园区（营业收入数据采集）
33			数说园区（进出口货值数据采集）
34			数说园区（工业总产值和税收收入数据采集）
35			政务服务（人才服务）
36			政务服务（党建党史）
37			政务服务（投资服务）
38			联系我们
39			系统管理-文章管理
40			系统管理-友链管理
41			系统管理-栏目管理
42			系统管理-关于我们
43			系统管理-园区跨境溯源查询
44			系统管理-资源管理
45			集成对接-系统集成（已规划业务系统）
46			集成对接-系统集成（预留业务系统集成）
47			集成对接-政务服务对接
48			集成对接-第三方服务对接
49		访客管理系统	车辆管理子系统—企业信息登记
50			车辆管理子系统—备案管理（车辆备案）
51			车辆管理子系统—备案管理（临时车辆备案）
52			车辆管理子系统—备案管理（人员入园预约）
53			车辆管理子系统—备案审核管理（车辆备案审核）
54			车辆管理子系统—备案审核管理（临时入园审核）

55			车辆管理子系统—备案审核管理（预约人员审核）
56			车辆管理子系统—租仓合同提交
57			车辆管理子系统—备案信息查询（全部车辆查询）
58			车辆管理子系统—备案信息查询（已备案车辆查询）
59			车辆管理子系统—备案信息查询(未通过备案车辆查询）
60			车辆管理子系统—备案信息查询（预约人员查询）
61			车辆管理子系统—抬杆记录
62			车辆管理子系统—车辆类型核对
63			车辆管理子系统—基础设置（基础参数)
64			车辆管理子系统—基础设置（菜单管理)
65	园区运营管理平台	园区决策分析系统	智能报表-企业信息管理
66			智能报表-报表申报管理
67			智能报表-报表审核管理
68			智能报表-历史报表管理
69			智能报表-报表期限管理
70			智能报表-预警参数管理
71			智能报表-系统管理
72		安全生产管理系统	全景展示管理子系统(跨境电商版块)
73			全景展示管理子系统(园区车辆吞吐版块)
74	作业综合	智慧云	云仓联网辅助监管子系统-全部仓库

75	服务平台	仓服务系统	云仓联网辅助监管子系统-特殊区域仓库
76			云仓联网辅助监管子系统-非特殊区域仓库
77			云仓联网辅助监管子系统-综保区管委会自有仓库
78			云仓联网辅助监管子系统-嘉城国际物流中心仓库
79			云仓联网辅助监管子系统-菜鸟物流中心仓库
80			云仓联网辅助监管子系统-中免国际物流中心仓库
81			云仓联网辅助监管子系统-全部企业信息
82			云仓联网辅助监管子系统-海口综保区企业信息
83			云仓联网辅助监管子系统-空港综保区企业信息
84			云仓联网辅助监管子系统-洋浦保税港区企业
85			云仓联网辅助监管子系统-三亚保税物流中心企业
86			云仓联网辅助监管子系统-区外企业信息
87			云仓联网辅助监管子系统-全部仓库信息
88			云仓联网辅助监管子系统-海口综保区仓库
89			云仓联网辅助监管子系统-空港综保区仓库
90			云仓联网辅助监管子系统-洋浦保税港区仓库
91			云仓联网辅助监管子系统-三亚保税物流中心仓库
92			云仓联网辅助监管子系统-区外仓库信息
93			云仓联网辅助监管子系统-商品列表
94			云仓联网辅助监管子系统-商品库存
95		物流运输管理系统-简	企业端-企业中心（企业信息登记）
96			企业端-企业中心（企业信息查询）
97			企业端-企业中心（维修人员登记）

98		化进出区管理系统子系统	企业端-商品中心（商品信息登记）
99			企业端-商品中心（商品信息查询）
100			企业端-资质登记（资质登记）
101			企业端-资质登记（资质注销）
102			企业端-资质登记（资质查询）
103			企业端-账册备案（账册备案）
104			企业端-账册备案（账册变更）
105			企业端-账册备案（账册查询）
106			企业端-维修账册管理
107			企业端-简化进出区核放单（核放单申请）
108			企业端-简化进出区核放单（作废申请）
109			企业端-简化进出区核放单（核放单查询）
110			企业端-货物维修核放单（核放单申请）
111			企业端-货物维修核放单（作废申请）
112			企业端-货物维修核放单（核放单查询）
113			企业端--一般纳税人核放单（核放单申请）
114			企业端--一般纳税人核放单（作废申请）
115			企业端--一般纳税人核放单（核放单查询）
116			企业端-库存管理（调整单申报）
117			企业端-库存管理（调整单查询）
118			企业端-区内流转管理（转入申请管理）
119			企业端-区内流转管理（转入查询）
120			企业端-区内流转管理（转出申请管理）

121			企业端-区内流转管理（转出查询）
122			企业端-综合查询（核放单查询）
123			企业端-综合查询（车辆查询）
124			企业端-统计分析（企业量）
125			企业端-统计分析（业务量）
126			企业端-统计分析（商品库存）
127			企业端-统计分析（主要商品）
128			企业端-基础设置（用户管理）
129			企业端-基础设置（角色管理）
130			企业端-基础设置（菜单管理）
131			企业端-基础设置（参数管理）
132			监管端-资质审核（资质登记初核）
133			监管端-资质审核（资质登记复核）
134			监管端-资质审核（资质注销初核）
135			监管端-资质审核（资质注销复核）
136			监管端-资质审核（资质登记管理）
137			监管端-资质审核（资质登记查询）
138			监管端-账册审核（账册登记初审）
139			监管端-账册审核（账册登记复审）
140			监管端-账册审核（账册查询）
141			监管端-简化进出区审核（人工核验）
142			监管端-简化进出区审核（作废审核）
143			监管端-简化进出区审核（人工过卡口）

144			监管端-简化进出区审核（核放单查询）
145			监管端-货物维修审核（人工核验）
146			监管端-货物维修审核（作废审核）
147			监管端-货物维修审核（人工过卡口）
148			监管端-货物维修审核（核放单查询）
149			监管端-一般纳税人审核（人工核验）
150			监管端-一般纳税人审核（作废审核）
151			监管端-一般纳税人审核（人工过卡口）
152			监管端-一般纳税人审核（核放单查询）
153			监管端-账册管理（简化进出区账册）
154			监管端-账册管理（一般纳税人账册）
155			监管端-账册管理（维修账册）
156			监管端-库存管理（库存调整核验）
157			监管端-库存管理（库存调整查询）
158			监管端-区内流转管理（转入核验管理）
159			监管端-区内流转管理（转出核验管理）
160			监管端-区内流转管理（区内流转查询）
161			监管端-抽查管理
162			监管端-预警管理
163			监管端-风险参数
164			监管端-综合查询（核放单查询）
165			监管端-综合查询（车辆查询）
166			监管端-统计分析（企业量）

167			监管端-统计分析（业务量）
168			监管端-统计分析（商品库存）
169			监管端-统计分析（主要商品）
170			监管端-基础设置（用户管理）
171			监管端-基础设置（角色管理）
172			监管端-基础设置（菜单管理）
173			监管端-基础设置（参数管理）
174			监管端-系统对接（H4A 对接）
175			监管端-系统对接（智能卡口对接）
176		物流运输管理系统-分类监管辅助管理子系统	企业端-企业中心（企业信息登记）
177			企业端-企业中心（企业信息查询）
178			企业端-商品中心（商品信息登记）
179			企业端-商品中心（商品信息查询）
180			企业端-分类监管资质登记（资质登记）
181			企业端-分类监管资质登记（资质注销）
182			企业端-分类监管资质登记（资质查询）
183			企业端-分类监管账册登记（账册备案）
184			企业端-分类监管账册登记（账册变更）
185			企业端-分类监管账册登记（账册查询）
186			企业端-分类监管核放单（核放单申请）
187			企业端-分类监管核放单（作废申请）
188			企业端-分类监管核放单（核放单查询）
189			企业端-分类监管库存管理（调整单申报）

190			企业端-分类监管库存管理（调整单查询）
191			企业端-区内流转管理（转入申请管理）
192			企业端-区内流转管理（转入查询）
193			企业端-区内流转管理（转出申请管理）
194			企业端-区内流转管理（转出查询）
195			企业端-综合查询（核放单查询）
196			企业端-综合查询（车辆查询）
197			企业端-统计分析（企业量）
198			企业端-统计分析（业务量）
199			企业端-统计分析（商品库存）
200			企业端-统计分析（主要商品）
201			企业端-基础设置（用户管理）
202			企业端-基础设置（角色管理）
203			企业端-基础设置（菜单管理）
204			企业端-基础设置（参数管理）
205			监管端-分类监管资质审核（资质登记初核）
206			监管端-分类监管资质审核（资质登记复核）
207			监管端-分类监管资质审核（资质注销初核）
208			监管端-分类监管资质审核（资质注销复核）
209			监管端-分类监管资质审核（资质登记管理）
210			监管端-分类监管资质审核（资质登记查询）
211			监管端-分类监管账册审核（账册登记初审）
212			监管端-分类监管账册审核（账册登记复审）

213			监管端-分类监管账册审核（账册查询）
214			监管端-核放单审核（人工核验）
215			监管端-核放单审核（作废审核）
216			监管端-核放单审核（人工过卡口）
217			监管端-核放单审核（核放单查询）
218			监管端-分类监管库存管理（库存调整核验）
219			监管端-分类监管库存管理（库存调整查询）
220			监管端-区内流转管理（转入核验管理）
221			监管端-区内流转管理（转出核验管理）
222			监管端-区内流转管理（区内流转查询）
223			监管端-抽查管理
224			监管端-预警管理
225			监管端-风险参数
226			监管端-综合查询（核放单查询）
227			监管端-综合查询（车辆查询）
228			监管端-统计分析（企业量）
229			监管端-统计分析（业务量）
230			监管端-统计分析（商品库存）
231			监管端-统计分析（主要商品）
232			监管端-基础设置（用户管理）
233			监管端-基础设置（角色管理）
234			监管端-基础设置（菜单管理）
235			监管端-基础设置（参数管理）

236			监管端-系统对接（H4A 对接）
237			监管端-系统对接（智能卡口对接）
238		跨境电商新零售管理系统	企业信息管理-企业信息登记
239			企业信息管理-企业信息查询
240			电商账册管理
241			保税进口清单管理-邮寄清单管理
242			保税进口清单管理-自提清单管理
243			保税进口报关管理-邮寄核注清单申报
244			保税进口报关管理-自提核注清单申报
245			保税进口报关管理-核注清单报文生成
246			保税进口报关管理-核注清单打印
247			保税进口报关管理-核注清单导出
248			物流管理-邮寄核放单申报
249			物流管理-自提核放单申报
250			物流管理-核放单报文生成
251			物流管理-核放单打印
252			物流管理-核放单导出
253			综合查询-清单查询
254			综合查询-溯源二维码
255			综合查询-核注清单查询
256			综合查询-核放单查询
257			综合查询-核放单查询（重发卡口报文）
258			系统设置-用户管理

259			系统设置-角色管理
260			系统设置-菜单管理
261			系统设置-客户端设置
262			系统设置-客户端（基础配置管理）
263			系统设置-客户端（监控服务管理）
264			系统设置-客户端（数据落地管理）
265			系统设置-客户端（申报异常管理）
266			系统设置-客户端（资源监控管理）
267			系统对接-溯源码接口
268			系统对接-闸机放行接口
269			系统对接-金二对接
270			系统对接-卡口对接
271		溯源采集管理系统	货物信息管理子系统(运抵确认)
272			货物信息管理子系统(消杀登记)
273			货物信息管理子系统(核酸登记)
274			风险预警管理子系统（应急处置）
275			风险预警管理子系统（异常预警）
276			风险预警管理子系统（预警管理）
277			运输及库存管理子系统（入库确认）
278			运输及库存管理子系统（货物流出）
279			运输及库存管理子系统（出库转运）
280			运输及库存管理子系统（自用耗损）
281			运输及库存管理子系统（信息补录）

282			销售溯源子系统（销售入库）
283			销售溯源子系统（销售流通）
284			销售溯源子系统（损耗报备）
285			销售溯源子系统（信息补录）
286			信息登记管理子系统（备案管理）
287			信息登记管理子系统（备案审核）
288			货物流向管理子系统（提货预约）
289			货物流向管理子系统（提货完成）
290			数据分析（提货量统计分析）
291			数据分析（放码量统计分析）
292			数据分析（消杀量统计分析）
293			数据分析（进境口岸统计分析）
294			数据分析（货物类型统计分析）
295			数据分析（目的地统计分析）
296			溯源移动应用（个人中心）
297			溯源移动应用（注册登录）
298			溯源移动应用（信息登记）
299			溯源移动应用（货物管理）
300			溯源移动应用（货物流向）
301			溯源移动应用（运输库存)
302			溯源移动应用（销售溯源）
303			溯源移动应用（溯源码）
304	辅助监管	跨境电	事前备案（企业中心）

305	业务服务平台	商园区服务系统	事前备案（商品中心）
306			事前备案（海外仓报备）
307			账册管理（账册备案）
308			账册管理（账册查询）
309			计划管理（进口到货计划）
310			计划管理（出口到货计划）
311			计划管理（进口出库计划）
312			计划管理（出口出库计划）
313			交易单据管理（三单数据查询）
314			交易单据管理（入库明细单查询）
315			B2C 业务（直购进口-订单管理）
316			B2C 业务（直购进口-运单管理）
317			B2C 业务（直购进口-支付单管理）
318			B2C 业务（直购进口-清单管理）
319			B2C 业务（一般出口-订单管理）
320			B3C 业务（一般出口-运单管理）
321			B2C 业务（一般出口-收款单管理）
322			B2C 业务（一般出口-清单管理）
323			B2C 业务（网购保税进口-订单管理）
324			B2C 业务（网购保税进口-运单管理）
325			B2C 业务（网购保税进口-支付单管理）
326			B2C 业务（网购保税进口-清单管理）
327			B2C 业务（特殊区域出口-订单管理）

328			B3C 业务（特殊区域出口-运单管理）
329			B2C 业务（特殊区域出口-收款单管理）
330			B2C 业务（特殊区域出口-清单管理）
331			B2B 业务（直接出口-订单管理）
332			B2B 业务（直接出口-运单管理）
333			B2B 业务（直接出口-收款单管理）
334			B2B 业务（直接出口-清单管理）
335			B2B 业务（出口海外仓-订单管理）
336			B2B 业务（出口海外仓-运单管理）
337			B2B 业务（出口海外仓-收款单管理）
338			B2B 业务（出口海外仓-清单管理）
339			查询统计（进口数据管理-订单查询）
340			查询统计（进口数据管理-运单查询）
341			查询统计（进口数据管理-支付单查询）
342			查询统计（进口数据管理-清单查询）
343			查询统计（进口数据管理-入库明细单查询）
344			查询统计（出口数据管理-订单查询）
345			查询统计（出口数据管理-运单查询）
346			查询统计（出口数据管理-收款单查询）
347			查询统计（出口数据管理-运抵单查询）
348		免税品	个人资料
349		辅助管	企业信息查询
350		理系统-	账册备案

351		企业端	账册变更
352			核放单申报
353			核放单作废
354			核放单查询
355			账册查询
356			入库准单绑定
357			调整单申报
358			调整单查询
359			核注清单申报（进口）
360			核注清单申报（出口）
361			核注清单变更
362			核注清单删除
363			核注清单核查
364			核注清单查询
365			免税品核放单查询
366			核注清单查询
367			核放单查询
368			企业统计
369			业务统计
370			商品库存统计
371			主要商品统计
372		免税品	企业信息-企业信息列表
373		辅助管	账册备案-账册审核

374		理系统-	账册备案-账册（备案）查询
375		监管端	账册管理-账册查询
376			调整单管理-调整单审核
377			调整单管理-调整单查询
378			免税品核放单-人工审核
379			免税品核放单-作废审核
380			免税品核放单-人工过卡
381			免税品核放单-核放单查询
382			预警管理-核放单预警处置
383			预警管理-核放单预警查询
384			查验管理-核放单抽查处置
385			查验管理-核放单处置查询
386			风险参数-预警参数
387			风险参数-布控参数
388			风险参数-审单参数
389			统计分析-企业统计
390			统计分析-业务统计
391			统计分析-单量统计
392			统计分析-主要商品统计
393			统计分析-商品库存统计
394			综合查询-免税品核放单查询
395			综合查询-核放单处置查询
396			基础设置-基础参数

397			基础设置-角色管理
398			基础设置-用户管理
399			基础设置-菜单管理
400			系统对接-H4A 对接
401			系统对接-大数据局报关单对接
402			系统对接-智能卡口对接
403			系统对接-装卸监控设备对接

注：1、演示需要各投标人自备演示所需电脑；2、评标区域没有网络，请各投标人自备联网设备（手机不能带入评标区，联网不能使用手机热点）。

系统验收要求

1 系统部署

1）投标人应提供软硬件设备统一调试、配置的解决方案。

2）投标人应向采购人提供产品和服务，承担方案中的所有设备及软件的集成责任，无论该设备或软件是由投标人采购的还是由采购人提供的。承诺与采购人进行积极主动的合作。

3）投标人应在中标后负责在项目规定的时间内完成应用系统开发、系统安装调试、验收测试等系统集成部署任务。

4）投标人应提供应用系统的运行维护深化方案。

5）有关系统集成服务的全部费用包含在总价中。

2 验收进程

项目的初验，由中标人提供验收测试方案及大纲，经采购人会同相关验收部门确认后进行系统集成初验，根据系统相关技术要求，提交系统初验报告。项目

完成初验后进入系统试运行期，试运行期为 3 个月，试运行期间，中标人应积极配合采购人处理或整改系统出现的问题，试运行期满后，采购人向海南省大数据管理局（或其他主管部门）申请进行系统终验，海南省大数据管理局会（或其他主管部门）同省委网信办、省发展改革委等部门组织验收。

3 验收测试

1）投标人应在中标后根据招标文件采购需求、投标文件技术方案、合同协议书等技术文件编写关于本项目的系统验收测试大纲，并交采购人审核确认。

2）投标人应在验收测试前两周提供详细的验收测试大纲，大纲应提供所有验收的细则，细则指定的实验项目以及达到的性能指标和功能不得低于招标文件的要求。

3）本项目的验收分为初验和终验两个阶段。系统初验包括系统功能测试和系统稳定性测试，初验后系统进入试运行期，试运行期结束后进行系统终验，终验主要包括系统功能测试。

4）在现场安装、调试、投运及验收测试过程中，中标单位应对损坏的设备负责。

第八部分：其他要求

一）、项目其他要求

1）在平台开发建设过程中使用的开发平台由投标人自行解决，与此有关的知识产权方面的纠纷由投标人负责，采购人不另外支付该方面的费用。在系统的开发和验收测试期间，所有费用均由项目实施单位自行承担。

2）本项目中标人应保证本系统建成后，拥有系统的全部权限，以便于项目

的后期维护或升级并确保系统的安全。

3）项目实施单位应保证，采购人在使用该系统或系统的任何一部分时，免受第三方提出的侵犯其专利权、商标权、 著作权或其它知识产权的起诉。项目实施单位应承担由此可能产生的一切法律责任和费用。

4）系统建设最终验收合格，交付采购人使用后，该系统软件全部产权（包括源代码）属采购人所有。

5）本项目付款方式：

合同签订生效后，支付签约合同价款的 30%作为预付款，项目总体进度达到 50%付合同总金额的 20%；项目初验完成进入试运行期后，付合同价款的 35%，项目最终验收完成后，付项目款的 10%，剩余 5%作为质量保证金，3 年维保期结束后，无息付清。

6）投标人拟在中标后将中标项目中的非主体，非关键性工作分包给第三方完成的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。

7）招标文件中，报价要求、建设周期（含阶段工期）要求、免费维保期（质保期）要求、付款方式、资格性审查要求、符合性审查要求为本项目的实质性要求，不允许负偏离，否则按无效投标文件处理。

8）本项目硬件部分核心产品为“可视化平台”。

9）投标人提供的产品或产品有关技术参数，涉及国家强制性要求的，应保证符合国家强制性要求，不得负偏离，供应商应提供承诺函（格式自拟），否则按无效投标文件处理。

10）除非另有说明，本项目适用所有现行有效的相关国家、行业以及地方规范、规程和标准。上述规范、规程和标准均指它们各自的最新版本。如果上述规

范、规程和标准之间出现矛盾或与合同其他内容存在不一致，按其中最高的要求或最严格的标准执行。适用本项目的上述规范、标准和规程的具体编号和名称则在本文件中若有空缺，由成交供应商依据上述原则自行收集。

第三章　　投标人须知

一、总则

1. 名词解释

1.1 采购人：海口综合保税区管理委员会

1.2 采购代理机构：海南简一项目咨询管理有限公司

1.2 投标人：系指获取招标文件拟参加投标和拟向采购人提供货物及相应服务的投标单位。

2. 适用范围

本招标文件仅适用于采购人或者采购代理机构组织的本次招标投标活动。

3. 合格的投标人

3.1 凡有能力按照本招标文件规定的要求交付货物、工程和服务的投标单位均为合格的投标人。

3.2 投标人参加本次政府采购活动应当符合《中华人民共和国政府采购法》第二十二条的规定并具备招标文件第一章“投标人资格条件”规定的条件。

3.3 投标人应遵守中华人民共和国的有关法律、法规。

3.4 单位负责人为同一人或者存在直接控股、管理关系的不同投标人，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的投标人，不得再参加该采购项目的其他采购活动。

4.本项目不接受联合体投标。

5. 投标费用

无论招标投标过程中的做法和结果如何，投标人均自行承担所有与参加投标有关的全部费用。

6. 现场考察、答疑会

6.1 现场考察（如有），采购单位应在规定的时间、地点组织已报名的潜在投标人进行现场考察。（组织时间、地点、联系人、联系电话：遵照招标公告或更正公告的相关约定。）

6.2 答疑会（如有），采购单位在规定的时间、地点组织已报名的潜在投标人召开答疑会。（组织时间、地点、联系人、联系电话：遵照招标公告或更正公告的相关约定。）

6.3 潜在投标人现场考察和参加答疑会所发生的费用自理。

6.4 除采购单位的原因外，投标人自行负责在现场考察中所发生的意外伤害和财产损失。

6.5 采购单位在现场考察和答疑会中所提供的信息，供潜在投标人在编制投标文件时参考。采购单位不对潜在投标人现场考察做出的判断和决策负责。

7. 法律适用

本次招标活动及由本次招标产生的合同受中华人民共和国的法律制约和保护。

8. 招标文件的约束力

8.1 本招标文件由采购人或者采购代理机构负责解释。

二、招标文件

9. 招标文件的组成

9.1 招标文件由六部分组成，包括：

第一章 招标公告

第二章 用户需求书

第三章 投标人须知

第四章　合同文本

第五章　投标文件格式

第六章　评审方法和程序

附表 1 资格审查表

附表 2 符合性审查表

附表 3 技术商务评分表

请仔细检查招标文件是否齐全，如有缺漏，请立即与招标人联系解决。

9.2 投标人被视为充分熟悉本招标项目所在地的与履行合同有关的各种情况，包括自然环境、气候条件、劳动力及公用设施等，本招标文件不再对上述情况进行描述。

9.3 投标人必须详阅招标文件的所有条款、文件及表格格式。投标人若未按招标文件的要求和规范编制、提交投标文件，将有可能导致投标文件被拒绝接受，所造成的负面后果由投标人负责。

10. 招标文件的澄清

采购人或者采购代理机构可以对已发出的招标文件进行必要的澄清或者修改。澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构应当在投标截止时间至少 15 日前，以书面形式通知所有获取招标文件的潜在投标人；不足 15 日的，采购人或者采购代理机构应当顺延提交投标文件的截止时间。

11. 招标文件的更正

11.1 当招标文件与更正公告的内容相互矛盾时，以采购人或者采购代理机构最后发出的更正公告为准。

11.2 投标人在收到更正公告后，应于一个工作日内正式书面回函采购人或者采购代理机构。逾期不回的，采购人或者采购代理机构视同投标人已收到更正公告。

11.3 为使投标人有足够的时间按招标文件的更正要求修正投标文件，采购人或者采购代理机构有权决定推迟投标截止日期和开标时间，并将此变更书面通知所有购买了同一招标文件的投标人。

三、投标文件

12. 投标文件的语言及度量衡

12.1 投标文件以及投标人与采购人或者采购代理机构之间的所有书面往来都应用简体中文书写。

12.2 投标人已印刷好的资料如产品样本、说明书等可以用其他语言，但其中要点应附有中文译文。在解释投标文件时，以译文为准。

12.3 除在招标文件第五章中另有规定外，度量衡单位应使用国际单位制。

12.4 本招标文件所表述的时间均为北京时间。

13. 投标文件的组成

13.1 投标文件应包括下列部分（目录及有关格式按招标文件第五章“投标文件格式”要求）：

13.1.1 投标函、投标报价及相关证明文件。

13.1.2 投标人资格证明文件。

13.2 若投标人未按招标文件的要求提供资料，或未对招标文件做出实质性响应，将导致投标文件被视为无效。

14. 投标报价

14.1 本项目招标采购预算金额（最高限价）为：109811337.48 元，各投标人投标报价超过投标最高限价的视为无效投标。

投标人不能低价恶意竞标，降低货物及服务质量。如果投标人的报价过低（低于采购预算金额的 80%），有可能影响产品质量或者不能诚信履约，其中标后招标人有权要求其在签订采购合同前提供采购合同金额的 4.9%作为履约保证金，同时预付款比例调整为 0%，结算方式改为项目最终验收合格后一次性结算。如中标人在实施过程中偷工减料、不按质按量完成本项目，则招标人有权终止合同，没收履约保证金，并报主管部门严肃处理。

14.2 投标人的投标报价应是包括全部平台建设开发、配套硬件设备、运输、辅助材料、安装、调试，以及人工、机械、运输、仓储、运费、各种税费、劳保、专利技术及质保期（免费运行服务期）间一切费用的总报价，在项目实施过程中，如发现有漏项，中标单位应无条件、无偿补齐，所发生的费用，视为已包含在投标人的报价之中，且并不因此影响项目进度。

14.3 采购人或者采购代理机构不接受任何有选择的报价。

15. 投标货币

投标报价均须以人民币为计算单位。招标文件另有规定的，从其规定。

16. 投标保证金

16.1 投标保证金是参加本项目投标的必要条件，保证金金额：￥500000.00 元（大写：伍拾万元整））。

16.2 投标保证金缴纳方式：

投标保证金的形式：银行转账、银行保函、电子保函等。银行转账应当从其基本账户中转出。 银行转账投标申请并获取保证金账号。提交市场主体登记信息后，在海口市公共资源交易网主页,进入交易系统选择“我要投标”，提交项

目投标申请，获取投标保证金账号，如未在规定时间内提交投标申请同时获取保证金账号者，视同放弃参与本项目采购活动。用途注明：（项目编号）保证金投标保证金截止时间：同递交投标文件截止时间；投标保证金账户：交易系统随机分配的唯一账号；注：投标保证金以转账方式提交的要求：1、仅接受投标单位以系统注册的银行账户使用转账的方式一次性提交，投标保证金交纳时间以保证金到帐时间为准。2、不符合以上要求的保证金缴纳情形视为不合格，投标人自行承担由此产生的风险。

16.3 若投标人不按规定提交投标保证金，或提交保证金而未注明所报价的项目编号的，其投标文件将被拒绝接受。

16.4 投标保证金的退还

16.4.1 中标人的投标保证金在其与采购人签订了采购合同后 5 个工作日内无息退还（除有特殊情况外）。

16.4.2 未中标的投标人的投标保证金将在招标人发出中标通知书 5 个工作日内无息退还。

16.5 发生下列情况之一，投标保证金将不予退还：

（1）投标人在投标有效期内撤回投标；

（2）中标人不按第 31 条规定签订合同；

（3）投标人提供虚假材料谋取中标的；

（4）采取不正当手段诋毁、排挤其他投标人的；

（5）与采购人、其他投标人或者采购代理机构恶意串通的；

（6）向采购人、采购代理机构行贿或者提供其他不正当利益的

17．投标有效期

17.1 投标有效期为从开标截止之日起计算的一百二十天，有效期短于此规定的投标文件将被视为无效。

17.2 在特殊情况下，采购人或者采购代理机构可于投标有效期满之前，征得投标人同意延长投标有效期，要求与答复均应以书面形式进行。投标人可以拒绝接受这一要求而放弃投标，投标保证金将尽快无息退还。同意这一要求的投标人，无需也不允许修改其投标文件，但须相应延长投标保证金的有效期。受投标有效期制约的所有权利和义务均应延长至新的有效期。

18．投标文件的数量、签署及形式

18.1 投标文件一式柒份，固定胶装。其中正本壹份，副本陆份，副本可以是正本的复印件。

18.2 投标文件须按招标文件的要求执行，每份投标书均须在封面上清楚标明“正本”或“副本”字样，“正本”和“副本”具有同等的法律效力；“正本”和“副本”之间如有差异，以正本为准。

18.3 投标文件正本中，文字材料需打印或用不褪色墨水书写。投标文件的正本须按照招标文件格式要求经法定代表人或授权代表签署和加盖投标人公章。

四、投标文件的递交

19．投标文件的密封及标记

19.1 投标人应将投标文件正本和所有副本分别密封在两个投标专用袋（箱）中（正本一包，副本一包），并在投标专用袋（箱）上标明“正本”、“副本”字样，封口处应加盖投标人公章并经法定代表人或被委托人签字。

19.2 投标人提交投标文件时应单独备有一个“唱标信封”，并将下列内容单独密封入该信封，封口处应加盖投标人公章并经法定代表人或被委托人签字：

（1）从投标文件正本中复印的开标一览表；

（2）交纳投标保证金证明文件的复印件；

（3）投标函。

（4）提供与正本一致的电子文件（应提供U盘）1份，电子介质的投标文件与纸质投标文件应具有同等的法律效力。

19.3 投标专用袋（箱）和“唱标信封”上须按招标人提供的格式注明：

（1）项目编号及项目名称；

（2）分包号（如有的话）；

（3）投标人的名称、地址、联系人、联系电话

19.4 投标文件未按第 19.1、 19.2 及 19.3 条规定密封和标记的投标人，采购人或者采购代理机构应当拒收。

19.5 唱标信封未按照招标文件要求提供的投标人，投标无效。

20. 投标截止时间

20.1 投标人须在招标文件第一章规定的投标截止时间前将投标文件送达采购人或者采购代理机构规定的投标地点。

20.2 若采购人或者采购代理机构按 11.3 条规定推迟了投标截止时间，采购人或者采购代理机构和投标人受投标截止时间制约的所有权利和义务均应以新的截止时间为准。

20.3 逾期送达的投标文件，采购人或者采购代理机构应当拒收。

21. 投标文件的修改和撤回

21.1 投标人在提交投标文件后可对其进行修改或撤回，但必须使采购人或者采购代理机构在投标截止时间前收到该修改的书面内容或撤回的书面通知，该书面文件须由法定代表人或被委托人签署。

21.2 投标文件的修改文件应按第 19 条规定签署，正、副本分别密封，并按第 19.2、19.3 条规定标记，还须注明“修改投标文件”和“开标前不得启封”字样。修改文件须在投标截止时间前送达采购人或者采购代理机构规定的投标地点。上述补充或修改若涉及投标报价，必须注明“最终唯一报价”字样，否则将视为有选择的报价。

21.3 投标人不得在投标截止时间以后修改投标文件。

21.4 投标人不得在投标截止时间起至投标有效期满前撤回投标文件，否则投标保证金将被没收。该投标人的投标文件不予退还。

五、开标及评标

22. 开标

22.1 采购人或者采购代理机构按招标文件第一章规定的时间和地点开标。采购人有关工作人员参加。政府采购主管部门、监督部门、国家公证机关公证员由其视情况决定是否派代表到现场进行监督。

22.2 投标人应委派授权代表参加开标活动，采购人或者采购代理机构有权要求参加开标的代表持本人身份证件签名报到以证明其出席。未派授权代表或不能证明被委托人身份的，采购人或者采购代理机构对投标文件的处理不承担责任。

22.3 开标时，采购人或者采购代理机构、公证员（如有）或投标人代表将查验投标文件密封情况，确认无误后拆封唱标，公布每份投标文件中“开标一览表”的内容，以及采购人或者采购代理机构认为合适的其他内容，采购人或者采购代理机构将作开标记录。

22.4 按照第 21 条规定，同意撤回的投标文件将不予拆封。

23. 评标委员会

评标委员会由采购人代表 2 名和从海南省综合评标专家库中随机抽取的评

审专家 5 名共 7 人单数组成，其中，评审专家人数不得少于成员总数的 2/3。该评标委员会独立工作，负责评审所有投标文件并确定中标侯选人，提交评标报告。

24. 对投标文件的资格审查和符合性审查

24.1 资格审查的内容包括：

详见附表 1

24.2 符合性审查的内容包括：

详见附表 2

以上资格审查和符合性审查的内容只要有一条不满足，则投标文件无效。

24.3 所谓偏离是指投标文件的内容高于或低于招标文件的相关要求，各投标人应在“商务、技术响应偏离表”中如实填列，对招标文件实质性要求负偏离的，按无效投标文件处理。

24.3.1 判断投标文件的响应与否只根据投标文件本身，而不寻求外部证据。

24.4 评标委员会在初审中，对算术错误的修正原则如下:

24.4.1 开标一览表内容与投标文件中明细内容不一致的，以开标一览表为准

24.4.2 投标文件的大写金额和小写金额不一致的，以大写金额为准；

24.4.3 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

24.4.4 单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价。

24.4.5 若投标人不同意以上修正，投标文件将视为无效。

25. 投标文件的澄清

25.1 在评标期间，评标委员会有权要求投标人对其投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容进行澄清。投标人应派授权代表和技术人员按评标委员会通知的时间和地点接受询标。

25.2 评标委员会认为有必要，可要求投标人对某些问题作出必要的澄清、说明和纠正。投标人的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，并不得超出投标文件的范围或者改变投标文件的实质性内容。投标人的书面澄清材料作为投标文件的补充，

25.3 投标人不按评标委员会规定的时间和地点作书面澄清，将视为放弃该权利。

25.4 并非每个投标人都将被询标。

26. 评标及定标

26.1 评标委员会分别对通过资格性审查和符合性审查的投标文件进行评价和比较。

26.2 评标委员会按招标文件“附则”中的评标办法对每份投标文件进行评审，确定中标候选人。最低投标价等任何单项因素的最优不能作为中标的保证。

26.3 关于政策性优惠

根据财政部、工业和信息化部《政府采购促进中小企业发展管理办法》[财库(2020)46号]的规定，政府关于强制采购节能产品、信息安全产品和优先采购环境标志产品的实施意见，以及根据《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》和《财政部、民政部、中国残疾人联合会关于促进残疾人就业政府采购政策的通知》[财库(2017)141号]的相关规定，本项目相应的政府采购政策优惠条件及要求如下:

节能环保清单

26.3.1 所投分包(如不分包则指本项目)的所有投标产品进入当期节能清单的，其评标价=投标报价*(1-2%)；投标人所投产品满足此规定的，必须提供声明函并提供相关证明文件。

26.3.2 所投分包(如不分包则指本项目)的所有投标产品进入当期环保清单的，其评标价=投标报价*(1-1%)；投标人所投产品满足此规定的，必须提供声明函并提供相关证明文件。

监狱企业

26.3.3 监狱企业视同小型、微型企业，享受相同的价格扣除优惠政策监狱企业属于小型、微型企业的，不重复享受政策。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参加政府采购活动时，应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件，否则不得享受相关扶持政策。

残疾人福利性单位

26.3.4 残疾人福利性单位视同小型、微型企业，享受相同的价格扣除优惠政策;残疾人福利性单位属于小型、微型企业的，不重复享受政策。残疾人福利性单位的具体标准及要求见“关于促进残疾人就业政府采购政策的通知[财库(2017)141 号]”。属于残疾人福利性单位的，投标时需按照有关要求提供规定的《残疾人福利性单位声明函》[规定格式见“财库(2017)141 号”附件]，并对声明的真实性负责，否则不得享受相关扶持政策。

中小企业

26.3.5 中小企业的认定标准:

1)中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业;

2)本规定所称中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准(工信部联企业(2011)300号);本项目所属行业为：软件和信息技术服务业。

3)在政府采购活动中，投标人提供的货物、工程或者服务符合下列情形的，享受[财库(2020)46 号]规定的中小企业扶持政策：（1）在货物采购项目中，货物由中小企业制造，即货物由中小企业生产且使用该中小企业商号或者注册商标；（2）在工程采购项目中，工程由中小企业承建，即工程施工单位为中小企业；（3）在服务采购项目中，服务由中小企业承接，即提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员。（4））在货物采购项目中，投标人提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受[财库(2020)46 号]规定的中小企业扶持政策。以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业。其中，联合体各方均为小微企业的，联合体视同小微企业。

26.3.5.1 具体评审价说明:

1)投标人符合[财库(2020)46 号]规定的小微型企业报价给予 10%(工程项目为 3%)扣除，用扣除后的价格参加评审。

适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，评标时在采用原报价进行评分的基础上增加其价格得分的

3%作为其价格分。

26.3.5.2　投标人为小型和微型企业(含监狱企业和残疾人福利性单位)的情况:

1）接受大中型企业与小微企业组成联合体或者介许大中型企业向一家或者多家小微企业分包的采购项目，对于联合协议或者分包意向协议约定小微企业的合同份额占到合同总金额 30%以上的，对联合体或者大中型企业的报价给予4%(工程项目为 1%)的扣除，用扣除后的价格参加评审。

2）适用招标投标法的政府采购工程建设项目，采用综合评估法但未采用低价优先法计算价格分的，评标时在采用原报价进行评分的基础上增加其价格得分的 1%作为其价格分。

3）组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。

4)投标人为工信部联企业(2011)300 号文规定的小型和微型企业(含联合体)的，必须如实填写“中小企业声明函”(内容、格式见“财库(2020)46 号”附 1)，否则不得享受相关中小企业扶持政策。

26.3.6 如有虚假骗取政策性优惠， 将依法承担相应责任。

27. 评标过程保密

27.1 在宣布中标结果之前，凡属于审查、澄清、评价、比较投标文件和中标意向等有关信息，相关当事人均不得泄露给任何投标人或与评标工作无关的人员。

27.2 投标人不得探听上述信息，不得以任何行为影响评标过程，否则其投标文件将被作为无效投标文件。

27.3 在评标期间，采购人或者采购代理机构将有专门人员与投标人进行联络。

27.4 采购人或者采购代理机构和评标委员会不向未中标的投标人解释未中标原因，也不对评标过程中的细节问题进行公布。

六、授标及签约

28. 定标原则

评标委员会将严格按照招标文件的要求和条件进行评标,根据评标办法推荐3名中标候选人，并标明排列顺序。采购人将确定排名第一的中标候选人为中标人并向其授予合同。中标人拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标人，也可以重新开展政府采购活动，中标结果将在与招标公告发布相同媒介公告。

29. 质疑处理

29.1 接收质疑函方式：投标人认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的,可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人或者采购代理机构提出质疑；潜在投标人对招标文件提出质疑的，应当在获取招标文件之日起7个工作日内提出。

29.2 联系部门、联系电话和通讯地址详见本采购文件中第一章招标公告。

29.3 投标人应在法定质疑期内一次性提出针对同一采购程序环节的质疑。

30. 中标通知

30.1 采购人或者采购代理机构应按评审报告的评审结果向中标人发出中标通知书。

30.2　中标人收到中标通知书后，须立即以书面形式回复采购人或者采购代理机构，确认中标通知书已收到，并同意接受（若到采购人或者采购代理机构领取则无需回复）。

30.3 中标通知书将是合同的一个组成部分。

31．签订合同

31.1 中标人应按中标通知书规定的时间、地点与采购人签订中标合同，否则投标保证金将不予退还，给采购人造成损失的，投标人还应承担赔偿责任。

31.2 招标文件、中标人的投标文件及评标过程中有关澄清文件均应作为合同附件。

31.3 签订合同后，中标人不得将货物、工程及其他相关服务进行转包。未经采购人同意，中标人不得采用分包的形式履行合同。否则采购人有权终止合同，中标人的履约保证金（如有）将不予退还。转包或分包造成采购人损失的，中标人还应承担相应赔偿责任。

32．采购代理服务费

本次招标服务费根据发改价格〔2015〕299 号文收费标准规定，本次招标服务费以采购预算金额为基数，按百分之一点五的费率向中标人收取。

中标人应在领取中标通知书的同时向海南简一项目咨询管理有限公司一次性付清招标服务费。

第四章　　合同文本（仅供参考）

海口综合保税区智慧园区建设项目

合同

项　目　名　称：

委托方　（甲方）：

受托方　（乙方）：

签　订　时　间：　202X 年　月

签　订　地　点：

委托方 （甲方）：

办 公 地 址：

法定代表人/负责人：

项 目 联 系 人：

联 系 方 式：

受托方 （乙方）：

办 公 地 址：

法定代表人/负责人：

项 目 联 系 人：

联 系 方 式：

甲乙双方根据 202X 年 X 月 X 日海口综合保税区智慧园区建设项目（项目招标编号:_____）招标结果及招标文件的要求，本着平等互利的原则，经协商一致，签订以下合同：

第一条 适用法律

本合同适用法律为：《中华人民共和国民法典》、《中华人民共和国政府采购法》、《中华人民共和国著作权法》和《中华人民共和国计算机软件保护条例》等有关国家法律法规。

第二条 合同范围

乙方负责完成海口综合保税区管理委员会海口综合保税区智慧园区建设项目建设工作。建设内容详见《附件 1 建设内容》、招标文件技术规范书、技术应答及附件、招投标文件、中标通知书、本合同附件及乙方所提供的商业文件与技术文件均作为本合同的有效部分。合同范围包括基础软硬件采购、软件开发、集成及服务。

第三条 合同金额

合同总金额为人民币（大写）_____（小写：￥_____元），合同总金额包括但不限于乙方为履行本合同约定、完成符合甲方要求而产生的费用及相关税费等一切费用，甲方支付合同总金额后，无须再向乙方或任何第三人担负任何形式的义务，乙方也不得以任何理由要求甲方承担任何义务。

合同总金额中，包括软硬件采购费人民币_____（￥_____元）；服务费用人民币_____（￥_____元）；软件开发费人民币_____（￥_____元）；集成费人民币_____（￥_____元）。具体详见《附件 2 采购清单和费用明细》。

第四条 费用及支付方式

4.2 甲方开票信息如下：

单位名称：海口综合保税区管理委员会

纳税人识别号：

甲方保证所提供的开票信息准确有效，如果提供的开票信息有误导致所开具的发票无效的，乙方重新开具发票的费用由甲方承担。甲方每次付款前，乙方应开具合规的增值税普通发票，乙方不提供合格发票或逾期提供发票的，甲方有权拒绝付款且不承担逾期付款违约责任，若给甲方造成损失的（包括但不限于税务风险），乙方应赔偿甲方损失，并承担法律责任。

4.5 支付方式：甲方依照本合同向乙方支付的所有款项均以转账方式支付到乙方指定的以下银行账户：

开户户名：

开户银行：

开户账号：

乙方保证以上收款信息准确无误，若由于乙方提供信息有误导致未能及时收到款项的，甲方无需承担逾期付款的违约责任。

第五条 实施地点

项目实施地点为甲方指定地点。

第六条 建设周期

6.1 项目建设周期：签订合同之日起____个月。

质保（维保）期限：　　。

6.2 乙方应在签订合同后 15 个工作日内提交详细的《项目实施计划》，并通过甲方签字确认。

6.3 乙方应在合同签订后 1 个月内，提交本项目《需求规格说明书》，并通过甲方签字确认。

6.4 乙方应在合同签订后 2 个月内提交《详细设计说明书》，并通过甲方签字确认。

6.5 乙方应在签订合同之日起___个月内完成所有软硬件内容的建设，并通过甲方组织的初步验收。

6.6 项目整体试运行不少于___个月，按照项目初步验收意见，乙方完成本合同中要求的所有建设内容的试运行和整改调试工作后，向甲方提交《项目竣工验收申请》及相关验收文档申请项目竣工验收，由甲方提请政务信息化行业主管部门组织项目竣工验收。

第七条 责任和义务

7.1 双方共同责任：

7.1.1 双方根据本合同规定的内容进行实施，并协商解决合作中出现的有争议的问题。

7.1.2 甲乙双方应各派 1 名工作人员负责整个项目建设过程中的协调、安排,以保障工作顺利进展。

7.2　甲方的责任和义务：

7.2.1 按本合同的付款条款按时支付所需款项。

7.2.2 负责项目中的组织和协调工作。

7.2.3 负责提供场地、人员等，协助乙方做好系统建设工作。

7.3 乙方的责任和义务：

7.3.1 按期完成项目软件采购，软件开发以及整个系统的安装、调试、初验、试运行、项目测评、竣工验收，和对甲方相关人员的培训工作，负责确保项目按技术规范和项目质量要求通过运行测试及验收。

7.3.2 在满足各阶段付款条件后，乙方要及时向甲方提出付款申请并出具正式有效发票。

7.3.3甲方允许乙方可通过公开招标方式与具备相应资格条件的合作伙伴共同开展非核心主体功能部分的项目建设，具体合作建设方案见附件三。乙方应要求合作建设单位不得再次分包。对于合作建设部分，乙方应配合监理单位对合作建设单位资格进行复核。

7.3.4 乙方应文明施工，确保施工安全，因乙方安全生产不当造成的损失由乙方承担全部责任。

7.3.5 乙方应根据项目实施计划、进度以及甲方的合理要求，按照培训计划及时安排对甲方的相关人员进行培训。

7.4 保密与数据安全条款

7.4.1 乙方应与甲方签订保密协议，承诺不将任何涉及本项目的信息向外界泄露，该保密义务在合同终止后继续有效；签订保密协议人员范围：项目组所有

成员。

7.4.2 乙方不得把从甲方获得的与本项目有关或因项目产生的任何文字、图片或其他资料泄露给第三方。

7.4.3 乙方应设置专人在项目建设期间对文档进行检查和管理，形成规范的文档体系，项目最终验收后全部移交给甲方，不得私自留存或擅自处理。

7.4.4 在项目建设或者维保过程中，乙方严格遵守甲方安全保密有关规定。

7.4.5 乙方应与甲方签订数据安全协议，乙方及其员工要按照《中国人民共和国网络安全法》等有关规定，落实数据安全管理相关要求，不得违反规定查询、收集、存储或公开相关数据，不得窃取或者以其他非法方式获取项目相关数据。除甲方授权外，乙方不得以任何形式将数据提供给第三方使用。

7.4.6 如果发现乙方违反以上条款要求，甲方将依法追究其责任，由此造成的一切损失由乙方承担。

第八条 安装、调试、初验、试运行和竣工验收

8.1 乙方应按照项目实施计划完成项目涉及的软硬件安装、软件开发、系统集成、售后维护等工作，并负责把软件部署到相应的环境或者经甲乙双方确定的其他环境上，完成软件系统测试，并按要求向甲方提交软件系统测试报告。

8.2 乙方完成系统部署、调试和集成工作后的 工作日内，应向甲方提出项目初步验收的书面申请。

8.3 甲方收到乙方的初步验收的书面申请后，在___工作日内组织完成项目初步验收工作，并根据初步验收结果要求乙方在双方协商整改时限内完成整改。

8.4 甲方在项目初验合格后，协助乙方做好项目系统试运行工作。试运行期间，甲方按照相关技术规范对系统进行测试和试用，在使用过程中出现异常，需记录故障现象，及时与乙方取得联系，并要求乙方在规定的期限内完成整改；乙

方配合甲方完成第三方软件测试、网络安全等级保护测评、密码应用安全测评等工作。

8.5 乙方收到甲方的整改通知后，应及时完成整改，整改期限不得超过双方协商的整改时限的时间要求，造成工期延误的，按照 11.5 条承担违约责任。

8.6 系统试运行通过的条件为系统无重大故障连续运行 3 个月以上，如发生重大故障，试运行终止，整改完成后重新开始试运行，直至试运行通过。

8.7 试运行通过后的 10 日内，乙方书面向甲方提请进行项目竣工验收。甲方在收到乙方书面的竣工验收申请后 15 工作日内向政务信息化行业主管部门提请项目竣工验收。如系统竣工验收第一次不通过，乙方应按照甲方要求在规定的时间内完成整改并再次书面提请竣工验收。因乙方原因导致项目竣工验收不能按期完成，造成工期延误的，乙方须承担违约责任。

8.8 在项目竣工验收通过后，乙方必须向甲方递交竣工资料和相关技术文档，如系统安装和管理手册、系统使用和维修说明书、第三方软件授权书、系统管理员权限、调试验收资料等，并保证上述文档清晰、完整和正确。

第九条 售后服务与技术支持

9.1 项目质保期从项目通过竣工验收之日起算，本项目要求硬件设备免费提供 3 年维保期，软件开发免费提供 2 年维保。若软硬件原厂商提供免费保修服务期长于本合同约定，以原厂商规定为准。

9.2 乙方应针对本项目成立专门的运维服务团队，由驻场（运维主管、现场值守服务人员、项目管理人员）和后台（二线支持）两部分构成，人员数量及质量满足甲方的要求，驻场人员___人。在质保期内，向甲方提供上门指导、培训及运行维护服务。派驻具备相应运维管理能力的工程师，提供每周 5*8 小时的驻场运维服务和每周 7*24 小时的远程运维服务管理支持。

9.3 在质保期内，乙方提供多种即时通讯方式服务及时响应需求，提供每周 7×24 小时电话支持服务，并在 1 小时内响应甲方报告的故障、缺陷，2 小时内

到达指定现场，提供现场技术支持。对系统不稳定的情况，乙方在被告知起 24 小时内提交分析报告。如果缺陷因乙方原因引起，乙方应在与甲方商定的时间内完成整改。

9.4 在质保期内出现影响用户使用的安全管理软件、应用软件故障或者发现软件安全漏洞等系统及软件故障，乙方应在被告知时起 24 小时内整改并重新部署完毕；其他暂不影响用户使用的系统及软件故障，乙方应在与甲方商定的时间内修复。系统及软件故障修复完毕，应在 3 个工作日内提交系统及软件故障处理报告，说明故障种类、故障原因、故障解决中使用的方法及造成的损失等情况。

9.5 在质保期内，乙方负责免费升级系统中需要升级或更新的系统软件、安全管理软件、应用软件等。

9.6 质保期满，如果甲方继续聘请乙方对本合同所规定的系统进行维护，双方另行签署维护协议。

第十条 事故处罚措施

10.1 项目通过竣工验收后，乙方提供的信息系统产生故障或没有及时排除故障（含主观和客观因素，不可抗拒因素除外），导致系统或平台不可访问、数据丢失、数据泄露等，则定义为事故。

10.2 系统或平台产生故障原因是电子政务云故障或网络故障，责任不在乙方，乙方需配合解决；系统或平台产生故障原因是软件系统本身或乙方人为原因的，责任在乙方。

10.3 事故评估工作由甲方根据系统的监控数据及使用单位反馈等信息进行分析及鉴定，定义事故等级。若经鉴定事故成因在于乙方或者乙方未能及时处理的，乙方需要承担因乙方主观或客观因素引发事故所造成的所有直接经济损失。由战争、严重火灾、水灾、台风和地震以及其它经双方同意属于不可抗力（以下简称：不可抗力）的原因或甲方原因造成的事故除外。

10.4 事故处罚规则如下：

事故等级	事故定义	事故处理要求	处罚规则
特级事故	100% 系统功能中断，或者数据全部丢失且无法恢复。	处理时间要求：远程响应时间＜10 分钟；非正常上班时间响应＜15 分钟；正常上班响应时间＜10 分钟；事故解决时间＜1 小时	1 小时候内解决不予处罚；如 1 小时内无法解决，每增加 1 小时扣除已累计支付合同款 0.5‰，每次事故罚款上限为已累计支付合同款的 1.5‰。
一级事故	50% 以上系统功能中断，或者 50% 以上数据丢失且无法恢复。	处理时间要求：远程响应时间＜10 分钟；非正常上班时间响应＜0.5 小时；正常上班响应时间＜10 分钟；事故解决时间＜1 小时	如 1 小时内事故无法解决，每增加 1 小时则扣除已累计支付合同款的 0.4‰，每次事故罚款上限为已累计支付合同款的 1.2‰。
二级事故	30% 以上和 50%以下系统功能中断，或者 30%以上和 50%以下数据丢失且无法恢复。	处理时间要求：远程响应时间<20 分钟；非正常上班时间响应＜0.5 小时；正常上班响应时间＜20 分钟；解决时间＜2 小时	如 2 小时内事故无法解决，每增加 2 小时则扣除已累计支付合同款的 0.3‰，每次事故罚款上限为已累计支付合同款的 0.9‰。

事故等级	事故定义	事故处理要求	处罚规则
三级事故	10%以上和30%以下系统功能中断，或者10%以上和30%以下数据丢失且无法恢复。	处理时间要求：远程响应时间＜20分钟；非正常上班时间响应＜0.5小时；正常上班响应时间＜20分钟；解决时间＜2小时	如2小时内事故无法解决，每增加2小时则扣除已累计支付合同款的0.2‰，每次事故罚款上限为已累计支付合同款的0.6‰。
四级事故	10%以下系统功能中断，或者10%以下数据丢失且无法恢复。	处理时间要求：远程响应时间＜30分钟；非正常上班时间响应＜0.5小时；正常上班响应时间＜30分钟；解决时间＜2小时	如2小时内事故无法解决，每增加2小时则扣除已累计支付合同款的0.1‰，每次事故罚款上限为已累计支付合同款的0.3‰。

第十一条 违约责任

11.1 双方均应严格遵守本合同条款，若未按本合同执行则将视作违约。任何一方不履行义务或者履行义务不符合约定的，应当承担继续履行、采取补救措施或者赔偿损失等违约责任。

11.2 双方均不应擅自提前解除本合同，除非依据法律法规应当解除或双方另行协商一致解除。

11.3 如甲方逾期付款，甲方应就迟延支付部分按日0.1‰的标准向乙方承担违约金，违约金累计最高不应超过合同总价的5%。

11.4 在项目建设过程中，乙方未按照本合同及附件约定提供服务或交付成

果的，乙方应按合同总价款每日 0.1‰的标准向甲方支付违约金，乙方逾期超过 30 日，甲方有权解除合同，不再向乙方支付合同款，并要求乙方返还甲方已支付的合同价款，同时乙方应向甲方支付合同总金额的 20%作为违约金，违约金不足以弥补甲方因此造成的损失的，甲方有权继续追偿（但确因甲方原因造成的，乙方不承担责任）。由此给甲方造成其他直接损失的，乙方仍应赔偿，赔偿金额最高不应超过合同总价的 10%。

11.5 在项目建设过程中，甲方认为乙方需要整改的，甲方有权要求乙方在 3 日内整改，乙方逾期未整改的，乙方应按合同总价款每日 0.1‰的标准向甲方支付违约金，乙方逾期超过 30 日，甲方有权解除合同，不再向乙方支付合同款，并要求乙方返还甲方已支付的合同价款，同时乙方应向甲方支付合同总金额的 20%作为违约金，违约金不足以弥补甲方因此造成的损失的，甲方有权继续追偿（但确因甲方原因造成的，乙方不承担责任）。。由此给甲方造成其他直接损失的，乙方仍应赔偿，赔偿金额最高不应超过合同总价的 10%。

11.6 本协议任何一方违约，违约方需向守约方支付守约方的经济损失及实现合法权益的必要支出，包括但不限于律师费、差旅费、诉讼费、鉴定费等。

11.7 在任何情况下，乙方在本合同项下所累计承担的违约、损失赔偿责任总额不超过索赔发生前乙方依据本协议向甲方收取的费用总额。

第十二条 知识产权

12.1 乙方为甲方开发的海口综合保税区智慧园区建设项目产权归甲方所有，乙方为实施项目提供的资料及全部项目工作成果（包括项目计划、需求规格说明书、概要设计说明书、详细设计说明书、测试报告、安装手册、操作手册、培训方案、试运行报告、前台页面及后台接口源代码、项目验收文档等资料）的知识产权权利归甲方所有，乙方提供的具备知识产权的产品或采购具备知识产权的成

熟产品（包括硬件产品和软件产品），知识产权仍归产品提供方所有；基于成熟产品进行二次开发的系统及成果的知识产权归甲方所有。

12.2 乙方保证对其销售产品/服务拥有完全的所有权/处置权或已取得相关授权，不侵犯任何第三方的专利、商标、著作权和其他合法权利，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由乙方承担所有相关责任的同时不得耽误本项目进度。

12.3 乙方保证其提供的软件及服务不含有任何旨在破坏最终用户计算机信息系统和/或获取最终用户隐私信息的恶意代码。

12.4 乙方应在项目完成时，将本项目所有文档汇集成册交付甲方。技术文档（光盘与纸质）及为本项目开发的软件系统（光盘形式，包括注释清晰明了的源代码）各两份。

第十三条 合同的生效和终止

13.1 本合同自双方签字并加盖公章或合同专用章之日起生效，至乙方完成本合同约定的全部义务之日止。

13.2 如果发生以下情况，可以视为合同解除或终止，相关方承担相应责任（如有）：

13.2.1 任一方进入解散或清算阶段；

13.2.2 任一方被判为破产或其它原因致使资不抵债；

13.2.3 本合同已有效、适当、全面得到履行；

13.2.4 双方共同同意以书面文件提前解除合同；

13.2.5 根据仲裁机构的生效裁决或司法机关的生效判决，本合同解除。

13.3 由于乙方原因，导致系统连续出现两次以上特级事故，甲方有权终止合同。

第十四条 不可抗力

14.1 如任何一方由于不可抗力而无法全部或部分履行其在本合同项下的任何义务，则该义务应在受不可抗力影响期间内在受影响的范围内中止履行。根据本条主张不可抗力的一方在必要时有权根据实际情况合理延期履行该义务。

14.2 本合同所述之不可抗力是指不能预见、不能克服、不能避免且对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、瘟疫流行等以及社会事件如战争、动乱、政府行为、电信主干线路中断、黑客、网路堵塞、电信部门技术调整和政府管制等。

14.3 遭受不可抗力的一方应在不可抗力事件发生后三日内通知另一方，并采取合理措施减轻损害的发生，同时向另一方提交有关部门出具的证明文件。在可能的情况下,遭受不可抗力的一方应在不可抗力结束后十日内恢复履行本合同。如果因不可抗力致使任何一方延迟履行本合同超过三十日，另一方有权向其发出书面通知后，终止本合同。

第十五条 争议解决以及适用法律

15.1 本合同之订立、效力、解释、执行应适用中华人民共和国法律（不包括香港特别行政区、澳门特别行政区、台湾地区法律）。

15.2 本合同履行过程中产生的争议由双方协商解决，协商不成的，提交甲方所在地有管辖权的人民法院提起诉讼,败诉方应向另一方支付由此所产生的一切费用，该费用包括但不限于诉讼费、保全费、聘请律师费用、调查取证费、差旅费、执行费及在执行过程中发生的一切费用等。

第十六条 其他

16.1 除甲乙双方协商一致或本合同另有约定外，任何一方不得擅自修改、终止本合同。

16.2 本合同所载任何内容不应被解释为在甲乙双方间创设合资、合伙、代理或任何其他本合同目的以外的关系。

16.3 本合同的所有附件、本项目可行性研究报告、初步设计文档、招投标文件、中标通知书、补充协议、保密协议、乙方提供的商业文件与技术文件均构成本合同的有效组成部分，并具有与合同同等法律效力。

16.4 任何一方未能或延迟行使其在本合同项下的权利，不能解释为对该权利的放弃。

16.5 本合同未尽事宜，双方在不违背项目初步设计文档、招投标文件、中标通知书及本合同附件的原则下，协商解决，并签订补充协议。

16.6 若本合同中任何条款因任何原因而被认定无效，此无效条款不影响其他条款的有效性，且此无效条款应自始视为不存在。

16.7 本合同一式捌份，中文书写。甲方执肆份、乙方执贰份、招标代理机构壹份，另外壹份由招标代理机构报政府采购主管部门备案。

（以下无正文）

甲方(盖章)： **乙方(盖章)：**

法人/授权代表（签名）： **法人/授权代表（签名）：**

日期： **日期：**

采购代理机构声明：本合同标的经海南简一项目咨询管理有限公司依法定程序采购，合同主要条款内容与招标响应文件的内容一致。

招标代理机构：海南简一项目咨询管理有限公司（盖章）

经办人：

时间：　　年　　月　　日

附件 1：建设内容

附件 2：采购清单和费用明细

序号	名　称	项目内容	单位	数量	单价	小计
一、软硬件采购						
总计		（小写）	¥00000.00			
		（大写）	人民币零万零仟零佰零拾零元整			

附件 3：中标通知书

【以下无本附件正文】

备注：1、合同格式为参考格式，甲乙双方可根据实际情况另行确定合同格式，但相关合同条款不得背离本次招标的实质性内容；2、合同未尽之处，由甲乙双方协商确定；

第五章 投标文件格式

注：请投标人按照以下文件的要求格式、内容，顺序制作投标文件，并请编制目录及页码，否则可能将影响对投标文件的评价。

投标文件格式要求

_____（项目名称）

项目编号：

投

标

文

件

投标人名称：_____（盖章）

法定代表人或被委托人：_____（签字或盖章）

年 月 日

1、投标报价

1.1 开标一览表

项目名称：

项目编号：

列名称	列内容
投标单位名称	
投标报价（大写）	
投标报价（小写）	
合同履行期限	
是否享受政策性优惠	□否 □是，我单位属于：　　（填写“小型企业或微型企业或监狱企业或残疾人福利性单位”）

投标单位：　　（公章）

法定代表人（或被委托人）：（签字或盖章）

日期：　年　月　日

注:1、各投标人的投标报价应是包括全部平台建设开发、配套硬件设备、运输、辅助材料、安装、调试，以及人工、机械、运输、仓储、运费、各种税费、劳保、专利技术及质保期（免费运行服务期）间一切费用的总报价，在项目实施过程中，如发现有漏项，中标单位应无条件、无偿补齐，所发生的费用，视为已包含在投标人的报价之中，且并不因此影响项目进度。

1.2 分项报价明细表

项目名称：_____ 招标编号：____

一、软件部分							
序号	名称	子项	模块	数量及单位	单价	单项总价	备注
1							
2							
.....							
软件部分报价合计： 元							
二、硬件部分							
序号	名称	品牌	型号	数量及单位	单价	单项总价	备注
1							
2							
.....							
硬件部分报价合计： 元							
三、集成部分							
序号	服务名称	服务内容概述		数量及单位	单价	单项总价	备注
1							
2							
.....							
集成部分报价合计： 元							
总计： 元							

投标单位：_____（公章）

法定代表人（或被委托人）：（签字或盖章）

日期：年 月 日

注:1、各投标人的投标报价应是包括全部平台建设开发、配套硬件设备、运输、辅助材料、安装、调试，以及人工、机械、运输、仓储、运费、各种税费、劳保、专利技术及质保期（免费运行服务期）间一切费用的总报价，在项目实施过程中，如发现有漏项，中标单位应无条件、无偿补齐，所发生的费用，视为已包含在投标人的报价之中，且并不因此影响项目进度。

2、本表格为参考格式，因各投标人技术特点、实际情况不尽相同，各投标人可对表格进行调整，但报价明细表中必须包括但不限于“项目类别/名称”、“服务内容/品牌型号/技术参数”、“单位”、“数量”、“单价”、“合价”必备信息

3、合计总价应与总报价表中的总报价一致

2、投标函

致：海口综合保税区管理委员会、海南简一项目咨询管理有限公司

根据贵方_____（项目编号为：_____）的投标邀请函，正式授权下述签字人___（姓名）_____代表投标人____（投标单位名称）____，提交投标书正本 1 份，副本 6 份，唱标信封 1 份，电子版一份。根据此函，我们宣布同意如下：

1. 我方接受招标文件的所有的条款和规定。
2. 我方同意按照招标文件第二章“投标人须知”的规定，本投标文件的有效期为从投标截止日期起计算的____天，在此期间，本投标文件将始终对我方具有约束力，并可随时被接受。
3. 如果在开标后规定的投标有效期内撤回投标，我方的投标保证金可被贵方没收。
4. 我方完全理解贵方不一定要接受最低价的投标。
5. 我们同意提供贵单位要求的有关本次投标的所有资料或证据。
6. 如果我方中标，我们将根据招标文件的规定严格履行自己的责任和义务。
7. 如果我方中标，我方将支付本次招标的服务费。
8. 如果我方中标，我方将根据招标文件的规定递交履约保证金（如需）。

投标人名称：_____（公章）

地址：_____.

邮编：_____.

电话：_____.

传真：_____.

开户名：_____.

开户行：_____.

账户：_____.

被委托人（签字或盖章）：_____.

职务：_____.

日期：_____年____月____日

3、法定代表人身份证明

单位名称：_____

地　　址：_____

姓　　名：_____　性别：_____　职务：_____

身份证号码：_____系_____的法定代表人。

特此证明。

附法定代表人身份证人面像复印件	附法定代表人身份证国徽面复印件

投标人名称（加盖公章）：_____

日 期：_____年_____ 月_____日

4、授权委托书

致：

本授权委托书声明：我 （姓名） 系 （单位名称） 的法定代表人，现授权委托 （被授权人姓名及身份证号码） 为我公司的代理人，以本公司的名义参加海南简一项目咨询管理有限公司组织的海口综合保税区智慧园区建设项目（项目编号：HNJY-2022-088 ）的投标活动，处理与本项目有关的一切事务。被授权人在投标过程及合同签订中所签署的一切文件，我均予以承认。

与本项目有关的质疑、投诉事项，我将亲自处理或另行特别授权。

本授权委托书的效力自签署日起至合同履行完毕止。

被授权人无转委托权。特此委托。

本授权书于_____年___月___日签字生效，特此证明。

附被委托人身份证人面像复印件	附被委托人身份证国徽面复印件

投标人（盖章）：

年 月 日

授权委托人（签字或盖章）：

年 月 日

5、联合投标协议书（本项目不接受联合体）

6、投标保证金缴付凭证

注：附投标保证金缴付凭证复印件，加盖公章；如为保函，附保函复印件加盖公章。

7、投标人诚信承诺书

我单位在参加_____项目的投标活动中，郑重承诺如下：

1、我方在此声明，本次招标投标活动中申报的所有资料都是真实、准确完整的，如发现提供虚假资料，或与事实不符而导致投标无效，甚至造成任何法律和经济责任，完全由我方负责；

2、我方在本次投标活动中绝无资质挂靠、串标、围标情形，若经贵方查出，立即取消我方投标资格并承担相应的法律责任；

3、我方在以往的招标投标活动中，无重大违法、违规的不良记录；我方人员没有重大违法记录；

4、我方未被地市级及其以上行政主管部门做出取消投标资格的处罚且该处罚在有效期内的；

5、我方一旦中标，将严格按照投标文件中所承诺的报价、质量、建设周期、项目负责人等内容组织实施；

6、我方一旦中标，将按规定及时与采购人签订合同。

投标人名称：　　（盖公章）

法定代表人（或被委托人）：　　（签字或盖章）

日期：　　年　　月　　日

8、投标人类似项目业绩一览表

序号	项目名称	业主名称	完成情况	合同金额	签订日期	联系方式	备注

注： 按招标文件要求，在表格后附相关业绩证明材料

投标人名称： （盖章）

日期： 年 月 日

9、投标人基本情况

<table>
<tr><td>投标人名称</td><td colspan="9"></td></tr>
<tr><td>注册地址</td><td colspan="4"></td><td>邮政编码</td><td colspan="3"></td></tr>
<tr><td rowspan="2">联系方式</td><td>联系人</td><td colspan="3"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>传真</td><td colspan="3"></td><td>网址</td><td colspan="3"></td></tr>
<tr><td>组织结构</td><td colspan="9">附后</td></tr>
<tr><td>法定代表人</td><td>姓名</td><td></td><td>技术职称</td><td></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>技术负责人</td><td>姓名</td><td></td><td>技术职称</td><td></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>成立时间</td><td colspan="3"></td><td colspan="6">员工总人数：</td></tr>
<tr><td>企业资质等级</td><td colspan="3"></td><td rowspan="6">其

中</td><td>注册工程师</td><td colspan="3"></td></tr>
<tr><td>营业执照号</td><td colspan="3"></td><td>高级职称人员</td><td colspan="3"></td></tr>
<tr><td>注册资金</td><td colspan="3"></td><td>中级职称人员</td><td colspan="3"></td></tr>
<tr><td>开户银行</td><td colspan="3"></td><td>初级职称人员</td><td colspan="3"></td></tr>
<tr><td>账号</td><td colspan="3"></td><td>技工</td><td colspan="3"></td></tr>
<tr><td>经营范围</td><td colspan="9"></td></tr>
<tr><td>备注</td><td colspan="9"></td></tr>
</table>

附：营业执照副本或事业单位法人证书复印件加盖公章。

10、参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明（格式）

参加政府采购活动前三年内，在经营活动中没有重大违法记录的声明

致：海口综合保税区管理委员会、海南简一项目咨询管理有限公司

我公司在参加本次政府采购（海口综合保税区智慧园区建设项目，项目编号:　　）活动近三年内（成立不满三年的，从成立之日起计算），在经营活动中无重大违法行为记录。

特此声明。

投标人名称：_____（盖公章）

法定代表人或被委托人：_____（签字或盖章）

日　　期：_____年_____月_____日

11、项目管理机构表

职务	姓名	职称	从业时间	执业或职业资格证明				从事过类似业绩	备注
				证书名称	专业	级别	证号		

投标人名称：（盖章）

日期: 年 月 日

11.1 项目负责人简历表

姓名		性别		年龄
职务		职称		学历
参加工作时间		从事 工作年限 年		
拟在本项目中担任的职务				
参与项目情况				
业主方	项目名称	规模	工程质量	业主联系人及方式

按招标文件要求，后附项目负责人相关材料。

11.2 项目管理机构主要人员简历表

姓名		性别		年龄
职务		职称		学历
参加工作时间		从事 工作年限 年		
拟在本项目中担任的职务				
参与项目情况				
业主方	项目名称	规模	工程质量	业主联系人及方式

按招标文件要求，后附项目管理机构人员相关材料。

12、相关证明材料

1、**资格证明文件：**

按招标公告申请人的资格要求提供

2、评分有关证明材料（按招标文件相关要求提供）

3、招标文件规定的或其它投标人认为需要提供的内容

备注：本小节要求的相关证明材料，如果招标文件给定的投标文件格式中已经涉及相关材料，无需再重复提供。

13、中小企业声明函（服务）

本公司郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司参加_____（单位名称）的（项目名称）采购活动，服务全部由符合政策要求的中小企业承接。相关企业的具体情况如下：

1._____（标的名称），属于（采购文件中明确的所属行业）行业；承建（承接）企业为（企业名称）_____，从业人员_____人，营业收入为_____万元，资产总额为_____万元[1]，属于_____（中型企业、小型企业、微型企业）；

2._____（标的名称），属于（采购文件中明确的所属行业）_____行业；承建（承接）企业为_____（企业名称）_____，从业人员_____人，营业收入为_____万元，资产总额为_____万元，属于（中型企业、小型企业、微型企业）；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情 形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

① 从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报

14、监狱企业证明文件

享受政策优惠的监狱企业须提供由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具的属于监狱企业的证明文件。

15、残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　期：

16、商务、技术响应偏离表

说明：请投标人对应招标文件中对商务内容、技术内容的相关要求，如实填写该表。

序号	名称	招标文件要求	投标文件响应情况	偏离
1				
2				
3				
4		……		

投标单位全称（公章）： 法定代表人（或被委托人）：（签字或盖章）

注： 1、此表为样表，行数可自行添加。

2、各投标人无需对招标文件中商务内容、技术内容的相关要求逐条进行填列，如有负偏离只填列相关负偏离的条款即可；如完全响应招标文件，则可对单元格进行合并后填列“完全响应招标文件各项要求，无负偏离”

3、各投标人应如实填写本表，如有弄虚作假，一切后果自负。

17、技术方案

（格式自定）

第六章 评审办法和程序

一、评标办法

（一）评审规则

1.评标办法采用综合评分法。

2.综合评分法评标步骤：先进行初步评审，再进行技术、商务的详细评审。只有通过初步评审的投标人才能进入详细的评审。

3.综合评分及其统计：按照评标程序、评分标准以及分值分配的规定，评标委员会成员分别就各个投标人的技术、商务状况，其对招标文件要求的响应情况进行评议和比较，评出各投标人的总分，评分的算术平均值即为该投标人的合计得分。合计得分与投标报价分（投标报价的分值计算由招标人工作人员负责计算）相加得出综合得分。综合得分相同的，按投标报价由低到高顺序排列。综合得分和投标报价均相同的，按技术指标由优至劣顺序排列。综合得分最高的投标人为第一中标候选投标人，综合得分次高的投标人为第二中标候选投标人，以此类推，评标委员会推荐出一至三名中标候选投标人。

（二）初步评审

1.招标人或者采购代理机构应当根据“资格审查表”对投标文件的资格进行评审，评标委员会根据“符合性审查表”对投标文件的符合性进行评审，只有对“资格审查表”和“符合性审查表”所列各项作出实质性响应的投标文件才能通过初步评审。对是否实质性响应招标文件的要求有争议的投标内容，评标委员会将以记名方式表决，得票超过半数的投标人有资格进入下一阶段的评审，否则将被淘汰。

2.无效投标的认定

投标文件出现但不限于下列情况的将被认定为无效投标

（1）未按照招标文件的规定提交投标保证金的；

（2）投标文件未按招标文件要求签署、盖章的（投标文件中对招标文件实质性要求不得有负偏离，对实质性要求的响应须经投标人的受托人逐页签字）；

（3）不具备招标文件中规定的资格要求的；

（4）报价超过招标文件中规定的预算金额或者最高限价的；

（5）投标文件含有采购人不能接受的附加条件的；

（6）法律、法规和招标文件规定的其他无效情形。

（三）详细评审

本项目采用如下综合打分法，总分为 100 分，具体打分方法如下：

项目评定标准及评分表见**评审评分表**

评分项目	技术商务评分	价格评分
权　　重	80%	20%

1、价格占 20 分：将所有通过初步评审的有效投标单位中价格扣除后报价的最小值为评标基准价，其价格分为满分。其他投标人的报价得分=（评标基准价/价格扣除后的投标报价）*100*报价分值权重。

2、整个项目的技术商务分占 80 分，具体由评委根据投标人的投标文件评比。

其中价格评审按如下方法处理：

（1）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

（2）投标报价有计算上或累加上的算术错误，修正错误的原则如下：

a 开标一览表内容与投标文件中明细表内容不一致的，以开标一览表为准

b 投标文件的大写金额和小写金额不一致的，以大写金额为准；

c 总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

d 单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价。

e 若投标人不同意以上修正，投标文件将视为无效。

附表 1

（HNJY-2022-088）资格审查表

序号	评审因素	评审标准
符合《中华人民共和国政府采购法》第二十二条规定的条件		
1	在中华人民共和国注册的、具有独立承担民事责任能力的法人	提供营业执照副本复印件、组织机构代码证副本复印件、税务登记证副本复印件或改革后的“三证合一”或“多证合一”营业执照复印件；根据《<政府采购法实施条例>释义》，银行、保险 、石油石化、电力、电信运营商等有行业特殊情况的，其分支机构可参与投标。采购文件中涉及要求提供“法定代表人”相关证明材料的，提供分支机构“负责人”的相关证明材料。
2	具有良好的商业信誉和健全的财务会计制度	提供2021年度经会计师事务所审计的财务审计报告或2021年至今任意三个月财务报表（财务报表至少应包含资产负债表、利润表、 现金流量表），复印件加盖公章，投标人注册成立时间不足三个月的，从注册时间起算。
3	具有依法缴纳税收和社会保障资金的良好记录	提供2021年至今任意三个月的依法缴纳税收和社保的相关材料 ，复印件加盖公章，投标人注册成立时间不足三个月的，从注册时间起算。
4	参加政府采购活动前三年内，在经营活动中没有重大违法记录	提供声明函,投标人注册成立时间不足三年的，从注册时间起算，加盖公章，格式详见第五章
5	被中国执行信息公开网列入失信被执行人的供应商;或被信用中国网站列入重大税收违法失信主体的供应商;或被中国政府采购网列入政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商（处罚决定规定的 时间和地域范围内），无资格参加本项目的采购活动	根据财政部《关于促进政府采购公平竞争优化营商环境的通知》（财库〔2019〕38 号）“对于采购人、采购代理机构可以通过互联网或者相关信息系统查询的信息，不得要求供应商提供”之规定，投标人无需就此项要求提供任何材料，由采购人、采购代理机构进行资格审查时查询。
本项目的特定资格要求		

6	法定代表人身份证明及授权委托书	按招标文件格式提供法定代表人身份证明及授权委托书原件
7	按照招标文件要求缴纳投标保证金	提供投标保证金缴纳凭证或银行保函

附表 2

（HNJY-2022-088）符合性审查表

序号	审查项目	评议内容
1	投标文件的有效性、完整性	是否符合招标文件的式样和签署要求
2	投标有效期	是否满足招标文件要求
3	报价	是否满足招标文件要求
4	合同履行期限	是否满足招标文件要求
5	其他	不存在其他无效投标认定条件
结　　论		

附表 3

（HNJY-2022-088）技术商务评分表

评选因素		评审标准	分值
投标人商务能力要求	投标人开发、集成与服务能力	1、投标人具备： （1）GB/T19001-2016/ISO9001:2015（质量管理体系认证） （2）GB/T24001-2016/ISO14001:2015（环境管理体系认证） （3）GB/T45001-2020/ISO45001:2018（职业健康安全体系认证） （4）ISO/IEC20000-1:2018（信息技术服务管理体系认证） （5）ISO/IEC27001:2013（信息安全管理体系认证） 资质证书 以上证书每个证书 1 分，最高 5 分 2、投标人具备： （1）信息安全服务资质-软件安全开发服务（满足三级及以上） （2）信息通信网络系统集成企业服务能力（甲级） （3）信息系统服务交付能力等级证书（满足四星级及以上级别） （4）信息系统建设和服务能力等级证书（满足 CS3 及以上级别） （5）ITSS 信息技术服务标准符合性证书(运行维护服务一级) 以上证书每个证书 1 分，最高 5 分。 注：以上证书需提供加盖投标人公章的复印件，证书均应在有效期内，否则视为无效证书，不予认可。	10
	相关业绩	投标人 2019 年 1 月 1 日以来承担的与本项目类似的案例，并且项目已经完成实施。具备一项合同案例得 2 分，此项最高得 6 分。具体要求如下： （1）投标人提供的案例为 2019 年 1 月 1 日以来，且项目案例为独立承接（非联合体），时间以合同签订时间为准； （2）以上案例要求提供合同清晰的复印件，内容须包含合同名称、双方签字印章、签订时间等合同关键信息，并加盖投标人公章。 （3）以上案例要求提供业主方盖章的验收证明（验收证明可以是复印件，加盖投标人公章）。 （4）不满足以上要求视为无效案例。	6
投标	技术指标响应情况	投标人针对招标文件第三章采购需求中的要求进行响应，带“▲”号的指标全部满足得满分 20 分，带“▲”	20

人技术要求		号的指标每有一项不满足扣 1 分，扣完为止。此项最高得 20 分。	
	技术服务方案	投标人提供的技术服务方案应包括对项目应用系统和数据共享交换实施方案；信息基础设施建设及管理方案；网络安全实施方案；海关及政务平台核心业务对接方案（包含 H4A、金关二期、智能卡口、海南大数据共享平台等内容）；质量控制方案；应急保障方案；软、硬件部署方案；功能测试方案；试运行方案及验收方案。 （一）、投标人提供的技术方案没有缺项，得基本分 3 分，每缺少一项方案扣 0.3 分，扣完为止。 （二）、评标委员会根据各投标人提供的各项技术方案进行评审 1、投标人提供的各项方案均完全满足或优于招标文件的要求，得 5 分； 2、投标人提供的各项方案中，有 3（含）项以内不能满足招标文件要求的，得 3 分； 3、投标人提供的各项方案中，有 3（不含）项以上不能满足招标文件要求的，得 1 分； 未提供技术方案的，本项不得分。	8
	项目实施进度保障方案	因本项目实施时间紧，投标人应为本项目提供完整的项目实施进度保障方案，以确保项目有序推进实施。 （1）投标人提供的项目实施进度保障方案，在满足招标文件要求的建设总工期及各阶段建设内容的基础上，可以保证各阶段建设内容及阶段工期均能优于招标文件要求，得 5 分。 （2）投标人提供的项目实施进度保障方案，在满足招标文件要求的建设总工期及各阶段建设内容的基础上，有 2 个阶段的建设内容及阶段工期能优于招标文件要求，得 3 分。 （3）投标人提供的项目实施进度保障方案，在满足招标文件要求的建设总工期及各阶段建设内容的基础上，只有 1 个阶段的建设内容及阶段工期能优于招标文件要求，得 1 分。 未提供项目实施进度保障方案或提供的项目实施进度保障方案不满足招标文件要求的，本项不得分。	5
	培训方案	投标人应为本项目提供完整的培训方案，以确保项目后期的可靠运行。 （1）投标人提供的培训方案涵盖内容齐全，完全满足招标文件要求，得 3 分。 （2）投标人提供的培训方案中，有 1（含）项以内缺项或不能满足招标文件要求的，得 2 分。 （3）投标人提供的培训方案中，有 1（含）项以上缺	3

		项或不能满足招标文件要求的，得 1 分。 未提供培训方案的，本项不得分。	
	现场演示	本次项目要求各投标人进行部分核心软件的现场功能演示，具体演示内容见《系统演示清单》。此项最高得 10 分。 1、具体评分标准如下： （1）采用软件系统（含 DEMO）进行演示，演示内容完整全面，各个子系统（或者模块）有完整的页面和功能展示、数据流转展示，完全满足或优于全部采购需求，得 10 分； （2）采用软件系统（含 DEMO）进行演示，演示内容覆盖不全，在单独子系统（或者模块） 内有完整的页面和功能展示、数据流转展示，满足部分采购需求，得 6 分； （3）采用软件系统（含 DEMO）进行演示出现错误，或采用 PPT、视频、截图等材料进行演示，得 2 分； （4）不能提供演示的，不得分； 2、演示要求： 演示时间 30 分钟，演示超时不得分。	10
投标人项目组实力要求	项目实施团队要求-项目经理资质	投标人需委派专业的项目经理 1 名，项目经理具有以下证书： （1）信息系统项目管理师 （2）信息安全工程师 （3）系统架构设计师 （4）系统规划与管理师 每有一个得 1 分，满分 4 分。 注：项目经理必须为本单位员工。需提供有效期内人员证书复印件，以及人员与投标单位签署的劳动合同和在投标单位 2022 年 1 月以来任意三个月的社保证明。以上证明材料需加盖投标人公章。	4
	项目实施团队-技术负责人	投标人需委派专业的技术负责人 1 名，承担项目技术总负责的职责。此项最高得 4 分。技术负责人能力资质要求如下： （1）信息系统项目管理师 （2）信息安全保障人员认证（CISAW，认证方向：包括但不限于风险管理、安全软件、安全运维其中之一） （3）ITIL EXPERT （4）注册信息安全专业人员 (CISP 或 CISO) 每有一个得 1 分，满分 4 分。 注：技术负责人必须为本单位员工。需提供有效期内人员证书复印件，以及人员与投标单位签署的劳动合同和在投标单位 2022 年 1 月以来任意三个月的社保证明。以上证明材料需加盖投标人公章。	4

	项目实施团队-技术团队成员（不含项目经理和技术负责人）	投标人需成立项目团队，承担项目具体实施和服务职责。此项最高得 10 分。具体要求如下： 1、项目团队人员能力要求： （1）具备由中华人民共和国人力资源和社会保障部等官方认证的系统集成项目管理工程师证书，每提供 1 人得 0.2 分，满分 2 分； （2）具备由中华人民共和国人力资源和社会保障部等官方认证的软件设计师证书，每提供 1 人得 0.5 分，满分 2 分； （3）具备由中华人民共和国人力资源和社会保障部等官方认证的网络工程师证书，每提供 1 人得 0.5 分，满分 2 分； （4）具备由中国信息安全测评中心认证的注册信息安全专业人员证书，每提供 1 人得 0.4 分，满分 2 分； （5）具备由工业和信息化部官方机构认证的的系统分析师资格证书，每提供 1 人得 1 分，满分 2 分； 以上证书的人员不能复用，若人员同时满足多个资质，只计算 1 个。 注：项目团队人员必须为本单位员工，需提供有效期内人员证书复印件和在投标单位 2022 年 1 月以来任意三个月的社保证明。以上证明材料需加盖投标人公章。	10
报价得分	报价得分	报价得分=（评标基准价/价格扣除后的投标报价）*100*报价分值权重；评标基准价等于有效投标单位中价格扣除后报价的最小值。	20

为了便于评委对投标文件内容的审核，投标人可针对本投标文件第六章中“技术商务评分表”编写响应页码索引表，即该评分项目内容在投标文件中的页码。