

DB4403

深 圳 市 地 方 标 准

DB4403/T 418—2023

口岸边检信息化建设规范

Specification of information construction for Port and Border inspection

2023-12-27 发布

2024-02-01 实施

深圳市市场监督管理局 发布

目 次

前言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 2

4 缩略语 2

5 总体建设原则与要求 3

 5.1 总体建设原则 3

 5.2 安全建设要求 3

 5.3 智慧建设要求 3

6 总体构成 3

7 机房 4

 7.1 机房规划 4

 7.2 建设内容 5

 7.3 机房管理 7

8 供电系统 7

 8.1 站级机房和设备间供电系统构成 7

 8.2 站级机房供电 9

 8.3 设备间供电 9

 8.4 配电柜 9

 8.5 UPS 供电 10

 8.6 通道供电 10

 8.7 设备供电 10

9 综合布线 11

 9.1 机柜 11

 9.2 布线 11

 9.3 强电 13

 9.4 弱电 13

10 网络系统 14

 10.1 总体要求 14

 10.2 口岸网络建设要求 17

 10.3 口岸网络链路传输指标 18

 10.4 口岸内设备要求 18

10.5 网络边界原则 19

11 通信系统 19

11.1 系统构成及基本要求 19

11.2 有线通信系统建设 20

11.3 无线通信系统建设 20

11.4 有线和无线通信系统互联互通的技术要求 24

12 查验系统 25

12.1 总体要求 25

12.2 系统架构 25

12.3 数据中心 26

12.4 设备间 29

12.5 查验现场 29

12.6 辅助设备 33

12.7 登机口人脸识别系统 34

12.8 梯口智能管控系统 34

12.9 应急系统 34

13 视频监控系统 35

13.1 总体要求 35

13.2 系统构成 35

13.3 功能性要求 36

13.4 业务要求 37

14 报警系统 40

14.1 一般要求 40

14.2 有线报警模块 40

14.3 无线报警模块 40

14.4 系统要求 40

14.5 其他建设要求 40

15 指挥系统 41

15.1 总体要求 41

15.2 系统构成 41

15.3 数据要求 42

15.4 硬件要求 43

15.5 系统功能要求 43

15.6 电子地图 44

15.7 定位系统 45

16 会议室及会议系统..... 46

 16.1 总体要求..... 46

 16.2 信息化建设组成..... 46

 16.3 场地基础设施建设..... 47

17 其他辅助部分..... 51

 17.1 配套系统建设..... 51

 17.2 培训室..... 51

 17.3 执法记录仪和采集工作站..... 51

18 信息安全系统..... 52

 18.1 总体要求..... 52

 18.2 物理环境安全..... 52

 18.3 网络安全..... 52

 18.4 数据安全..... 54

 18.5 个人信息安全..... 55

 18.6 密码应用安全..... 55

 18.7 视频安全..... 56

 18.8 供应链安全..... 56

 18.9 安全运营..... 57

19 安全防护..... 57

 19.1 总体要求..... 57

 19.2 防雷与接地..... 57

 19.3 机房防水..... 58

 19.4 电磁兼容性..... 58

20 系统运行与维护、保养..... 58

 20.1 一般要求..... 58

 20.2 运维管理平台..... 59

 20.3 运维保养管理要求..... 59

 20.4 维护保养工作程序..... 60

 20.5 工作内容与要求..... 60

 20.6 维护评价..... 61

参考文献..... 62

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由深圳出入境边防检查总站提出并归口。

本文件起草单位：深圳出入境边防检查总站、深圳市智慧安防行业协会、深圳市中安测标准技术有限公司、深圳市特种证件研究制作中心、深圳市华正联实业有限公司、华为技术有限公司、深圳北斗应用技术研究院有限公司、广东公信智能会议股份有限公司、中国移动通信集团广东有限公司深圳分公司、浙江大华技术股份有限公司、北京天融信网络安全技术有限公司、深圳市星火电子工程公司、深圳市航通智能技术有限公司、深圳市雄帝科技股份有限公司、海能达通信股份有限公司、杭州海康威视数字技术股份有限公司深圳分公司、奇安信安全技术（深圳）有限公司、中国电信股份有限公司深圳分公司、中国联合网络通信有限公司深圳市分公司。

本文件主要起草人：徐晓伟、褚邦恒、郭俊辉、何慧、张汉杰、刘卫、宋思缘、关世龙、李佳、马冬冬、傅源、刘凯、曾令楚、梁那日苏、李旻、赖子亮、许程、张毅、景发俊、吴金平、王榜金、钟善戈、张寒、张帆、陶丹、郭宇、梁宏霞、凌育杰、王学军、杨凡、唐合宾、彭德芳、吴轩、刘冬、蒋芯鹏、徐凯圆、邢越、吴乃星、赵宇芬、林淑娟、陈在杰。

口岸边检信息化建设规范

1 范围

本文件规定了口岸边检信息化建设的总体建设原则与要求、总体构成、机房、供电系统、综合布线、网络系统、通信系统、查验系统、视频监控系统、报警系统、指挥系统、会议室及会议系统、其他辅助部分、信息安全系统、安全防护和系统运行与维护、保养等要求。

本文件适用于深圳出入境边防检查总站（以下简称“深圳边检总站”）所辖口岸及口岸边防检查管理限定区域、深港边界过境耕作口、流动渔船停靠点、台轮停靠点、沙头角边境特别管理区等场地的边检信息化建设，是上述场地新建、改建、扩建的基本依据。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 3836.1 爆炸性环境 第1部分：设备 通用要求
- GB/T 4208—2017 外壳防护等级（IP代码）
- GB/T 7251.1 低压成套开关设备和控制设备 第1部分：总则
- GB/T 7251.2 低压成套开关设备和控制设备 第2部分：成套电力开关和控制设备
- GB/T 7260.1—2008 不间断电源设备 第1-1部分：操作人员触及区使用的UPS的一般规定和安全要求
- GB/T 7260.4—2008 不间断电源设备 第1-2部分：限制触及区使用的UPS的一般规定和安全要求
- GB/T 14048.1 低压开关设备和控制设备 第1部分：总则
- GB/T 15408 安全防范系统供电技术要求
- GB 15763.1 建筑用安全玻璃 第1部分：防火玻璃
- GB/T 18883 室内空气质量标准
- GB/T 19115.1 信息技术 无中断电源（UPS）的安全要求 第1部分：总则
- GB/T 20984—2022 信息安全技术 信息安全风险评估方法
- GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南
- GB/T 22080 信息技术 安全技术 信息安全管理体系 要求
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求
- GB/T 30148 安全防范报警设备电磁兼容抗扰度要求和试验方法
- GB/T 32581 入侵和紧急报警系统技术要求
- GB 35114 公共安全视频监控联网信息安全技术要求
- GB/T 37078 出入口控制系统技术要求
- GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
- GB 50052 供配电系统设计规范
- GB 50054 低压配电设计规范

GB 50057 建筑物防雷设计规范
GB 50174—2017 数据中心设计规范
GB 50222 建筑内部装修设计防火规范
GB 50311 综合布线系统工程设计规范
GB 50343 建筑物电子信息系统防雷技术规范
GB 50371 厅堂扩声系统设计规范
GB 50394 入侵报警系统工程设计规范
GB 50464 视频显示系统工程技术规范
GB 50635 会议电视会场系统工程设计规范
GB/T 50719 电磁屏蔽室工程技术规范
GB/T 51409 数据中心综合监控系统工程技术标准
GB 55037 建筑防火通用规范
GA/T 1056—2013 警用数字集群（PDT）通信系统 总体技术规范
GA/T 1057—2013 警用数字集群（PDT）通信系统 空中接口物理层及数据链路层技术规范
GA/T 1058—2013 警用数字集群（PDT）通信系统 空中接口呼叫控制层技术规范
GA/T 1059—2013 警用数字集群（PDT）通信系统 安全技术规范
GA/T 1127 安全防范视频监控摄像机通用技术要求
GA/T 1260 人行出入口电控通道闸通用技术要求
GA/T 1364—2017 警用数字集群（PDT）通信系统 互联技术规范
GA/T 1366—2017 警用数字集群（PDT）通信系统 移动台技术规范
GA/T 1400.4 公安视频图像信息应用系统 第4部分：接口协议要求
GA/T 1788（所有部分） 公安视频图像信息系统安全技术要求
DB4403/T 234—2022 公共安全视频监控建设联网共享技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

视频专网 video private network

采用专线方式或非公共网络基础上的虚拟专用网（VPN）方式建设的、用于支撑视频图像服务和汇聚对接各层级视频图像信息系统的传输网络。

[来源：DB4403/T 234—2022，3.4]

3.2

网络安全 cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.3

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

4 缩略语

下列缩略语适用于本文件。

ATS: 自动转换开关 (Automatic Transfer Switching)
 CMOS: 互补金属氧化物半导体 (Complementary Metal Oxide Semiconductor)
 HDMI: 高清多媒体接口 (High Definition Multimedia Interface)
 KVM: 多计算机切换器 (Keyboard Video Mouse)
 IAD: 综合接入设备 (Integrated Access Device)
 OCR: 光学字符识别 (Optical Character Recognition)
 PDU: 电源分配单元 (Power Distribution Unit)
 POE: 以太网供电 (Power Over Ethernet)
 PDT: 警用数字集群 (Police Digital Trunking)
 SIP: 会话初始协议 (Session Initiation Protocol)
 UPS: 不间断电源系统 (Uninterruptible Power Systems)
 UWB: 超宽带 (Ultra Wide Band)
 VPN: 虚拟专用网 (Virtual Private Network)
 WebGL: Web图形库 (一种3D绘图协议) (Web Graphics Library)

5 总体建设原则与要求

5.1 总体建设原则

坚持数字化、智能化、体系化、自主化发展原则,基于绿色环保低碳要求,规划边检查验管理体系,广泛运用现代信息科技和现代管理服务手段,提供系统完备、功能完善、安全可靠的科技支撑保障,使得口岸边检具备防灾减灾救灾和应对重大突发公共事件处置保障能力。

5.2 安全建设要求

应保障边检查验全过程顺畅、无盲区监管、数据信息安全,并满足以下要求:

- a) 陆路口岸,单场地查验不应中断 15 min 以上;
- b) 海港码头,视频监控不应中断 15 min 以上;
- c) 数据信息安全应符合 GB/T 22080、GB/T 22239 的相关规定,以及国家和公安部对口岸边检信息化安全建设的规定。

5.3 智慧建设要求

智慧建设宜满足以下要求:

- a) 通过视频监控、雷达感知、传感器收集等技术应用,确保辖区海洋与陆地监管区域视频全覆盖、陆路口岸各场地及周边区域的人员与车辆可定位、室内区域单个人员可定位、人员密集区域可感知和异常事件能预警;
- b) 通过新型生物特征识别、非接触式识别、通关预约、智能感知等技术应用,优化出入境人员、交通运输工具的通关流程;
- c) 通过建设合作查验、“一站式”查验、无人驾驶车辆查验系统等查验模式的创新应用,促进人员、货物、资金、科技、信息等要素跨境流动、区域融通。

注:口岸边检信息化智慧建设原则依据《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》和《“十四五”移民管理事业发展规划》的要求。

6 总体构成

口岸边检信息化建设主要由基础部分、功能部分、其他辅助部分和运维部分构成，见图1，各部分信息化建设内容如下：

- a) 基础部分包含机房、供电系统、综合布线、网络系统、通信系统、信息安全系统和安全防护等；
- b) 功能部分包含查验系统、视频监控系统、报警系统、指挥系统、会议室及会议系统等；
- c) 其他辅助部分包含配套系统建设、培训室、执法记录仪和采集工作站等；
- d) 运维部分包含系统运行与维护、保养等。

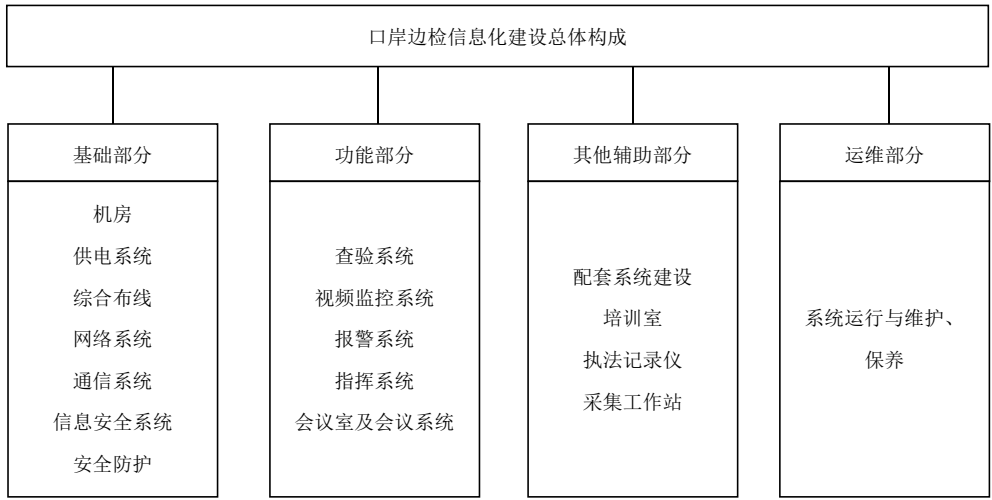


图 1 口岸边检信息化建设总体构成示意图

7 机房

7.1 机房规划

7.1.1 机房分类

机房进行以下分类：

- a) 机房按承担功能应分为主机房、灾备机房、监控机房、场地机房，以及供会议系统、显示大屏使用的专用功能机房等；
- b) 主机房、灾备机房及监控机房属于站级机房；场地机房、专用功能机房等属于设备间。

7.1.2 机房区域划分

机房区域进行以下划分：

- a) 站级机房区域应划分以下区域：
 - 1) 核心区：安装 IT 机柜、制冷等设备；
 - 2) 功能区：安装供配电、空调外机间和消防等设备；
 - 3) 辅助区：配置机房监控区、操作区、缓冲区等。
- b) 设备间区域的划分根据实际使用面积宜按照站级机房的区域划分要求进行。

7.1.3 面积规划

机房面积规划满足以下要求：

- a) 设计流量大于 1000 万人次/年的新建口岸，站级机房核心区域面积不应小于 80 m²，功能区域和辅助区域应按照核心区域的大小配套建设，并应适当留有扩容空间；
- b) 其他口岸站级机房面积不宜小于 80 m²，设备间面积不宜小于 30 m²。

7.1.4 机房选址

机房的选址应符合GB 50174的相关规定，并满足以下要求：

- a) 电力供给应稳定可靠，交通、通信应便捷，自然环境应清洁；
- b) 应远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的场所；
- c) 应远离水灾和火灾隐患区域；
- d) 应远离强振源和强噪声源；
- e) 应避开强电磁场干扰；
- f) 站级机房位于多层或高层建筑物内的，在确定主机房的位置时，应满足以下要求：
 - 1) 设备运输、管线敷设、雷电防护和结构荷载等方面应具备建设条件；
 - 2) 安装机房专用空调的机房设备间，应具备安装空调室外机的建筑条件；
 - 3) 机房位置上方不应存在卫生间、淋浴房、蓄水池等或存在下沉式蓄水空间建筑设施。

7.1.5 设备间

设备间建设满足以下要求：

- a) 查验场地设备间应设置在临近查验现场位置；
- b) 旅客查验场地应设置两个或两个以上数量的设备间进行保障；
- c) 建设面积充足的情况下，设备间的功能区域应按照站级机房标准划分；
- d) 信息点离机房设备间较远时应根据实际需求建设必要的网络汇聚点，网络汇聚点可参照设备间标准建设；
- e) 各类机房、设备间用房面积可根据口岸实际情况进行调配，房间面积调配应符合 GB 55037 中防火分区的相关规定。

7.2 建设内容

7.2.1 通则

机房的建设内容应包括基础装修、恒温恒湿、消防、综合监控系统、照明、供电（市电供配电与UPS等）、综合布线、KVM、机柜、新风等。受客观条件限制，供电、恒温恒湿等由口岸服务单位管理的机房，应配置保障机房设备最小化运行的应急设备。

注1：KVM（多计算机切换器）以多主机切换技术为依据，通过直接连接键盘、视频或鼠标端口，访问和控制计算机，完成多台服务器之间的切换，实现系统和网络的集中管理。

注2：供电（市电供配电与UPS等）、综合布线的内容见本文件中第8章、第9章的内容。

7.2.2 基础装修

7.2.2.1 机房室内装修设计选用材料应符合 GB 50222 的相关规定。

7.2.2.2 铺设防静电活动地板的地面，满足以下要求：

- a) 活动地板的高度应根据电缆布线和空调送风要求确定；
- b) 活动地板下的空间只作为电缆布线使用时，地板高度不宜小于 250 mm；
- c) 活动地板下的地面和四壁装饰，可采用水泥砂浆抹灰，地面材料应平整、耐磨；
- d) 活动地板下的空间既作为电缆布线，又作为空调静压箱时，地板高度不宜小于 500 mm；
- e) 活动地板下的地面和四壁装饰应采用不起尘、不易积灰、易于清洁的材料；

f) 楼板或地面应采取保温、防潮措施，一层地面垫层宜配筋，围护结构宜采取防结露措施。

7.2.2.3 当主机房内设有用水设备时，应采取防止水漫溢和防止渗漏的措施。

7.2.2.4 门窗、墙壁、地（楼）面的构造和施工缝隙，均应采取密闭措施。

7.2.3 恒温恒湿

恒温恒湿建设满足以下要求：

- a) 站级机房应按不低于 800 W/m^2 、设备间应按不低于 400 W/m^2 的标准估算本机房所需制冷量；
- b) 恒温恒湿系统制冷总量除应满足本机房所需制冷量外，另需配备至少一台同规格的精密空调运行作为冗余；
- c) 恒温恒湿系统中精密空调应接入市电配电系统，并满足以下要求：
 - 1) 内、外机之间应满足设备高差要求，距离过长应加装增压设备；
 - 2) 排水管道应避免穿过 IT 机柜区、供配电区等，排水管道应汇入建筑物整体排水系统；
 - 3) 精密空调应至少具备回风温度、回风湿度、高温报警、高湿报警、低温报警及低湿报警等基础监测功能，并应纳入机房综合监控系统。

7.2.4 消防

消防建设满足以下要求：

- a) 站级机房及设备间内应配置边检机关独立使用的气体自动灭火消防系统，应对机房内温度、室内烟雾浓度等情况进行实时监测，遇有紧急情况能够及时自动处置；
- b) 应根据实际需求选择管网式、柜式或悬挂式等建设模式，其中管网式气体自动灭火消防系统必须设置独立的气瓶间，机房应作为独立的防护区，单独设置钢瓶和灭火剂；
- c) 气体自动灭火消防系统控制主机、灭火指示灯应安装在机房外，墙面应设置泄压口，控制主机处应粘贴紧急启停等重要操作的操作方法；
- d) 采用管网式气体灭火系统或细水雾灭火系统的主机房，应同时设置两组独立的火灾探测器，且火灾报警系统应与灭火系统和视频监控系统联动；
- e) 设置气体灭火系统的主机房，应配置专用空气呼吸器或氧气呼吸器；
- f) 机房宜配置外开甲级防火门，宽度不宜小于 1400 mm ，当主机房面积超过 120 m^2 时，宜设置两个或两个以上防火门，应保证任何情况下均能从机房内开启；
- g) 当机房采用防火玻璃时，防火玻璃应符合 GB 15763.1 的相关规定，且耐火隔热性时间不宜小于 2 h ，耐火完整性时间不宜小于 2 h ；
- h) 机房位于其它建筑物内时，机房与建筑内其它功能用房之间应采用耐火极限不低于 2.0 h 的防火隔墙和 1.5 h 的楼板隔开，隔墙上开门应采用甲级防火门；
- i) 机房的耐火等级不应低于二级。

7.2.5 综合监控系统

综合监控系统建设应符合 GB/T 51409 的相关规定，系统主要监测对象应包括市电配电柜、UPS 主机、UPS 配电柜、后备电池、通道配电柜、精密空调、温湿度、漏水、新风机、图像监控、门禁等，并满足以下要求：

- a) 站级机房及设备间内均应安装综合监控系统对机房环境进行实时监测，应能够随时观察到机房的情况，及时地发出预防性报警，通知值班人员采取措施，防止事故发生；
- b) 机房视频监控应覆盖机房所有区域，针对安全服务器等特殊区域应设置专用镜头监控，视频录像画质不应低于 1080 P ，存储时间不应少于 180 天；

- c) 系统应提供数字化查询接口，用于机房综合监控或智能分析等，并纳入总站机房综合监控系统平台统一监控；
- d) 系统的设计应保证信息安全性，并满足以下要求：
 - 1) 系统宜采用专用传输网络，有线公网传输和无线公网传输应具有信息加密措施；
 - 2) 根据安全管理需要，系统宜对重要数据进行加密存储；
 - 3) 应具有防病毒和防网络入侵的措施；
 - 4) 应对用户和设备进行身份认证，应对用户和设备基本信息、属性信息以及身份标识信息等进行管理；
 - 5) 当基于不同传输网络的系统和设备联网时，应采取相应的网络边界安全管理措施。

7.2.6 照明

站级机房及设备间照明满足以下要求：

- a) 一般照度标准值不应低于 500 lx；
- b) 常规照明应接入市电供电系统，应急照明应接入 UPS 供电系统，均应使用独立开关控制；
- c) 应设置通道疏散照明及疏散指示标志灯，主机房通道疏散照明的照度值不应低于 5 lx；
- d) 主要照明光源宜采用高效节能荧光灯或者 LED 灯；
- e) 电池间宜使用防爆灯；
- f) 灯具应采用分区、分组的控制措施；
- g) 灯具不宜布置在设备的正上方；
- h) 站级机房的照明线路宜穿钢管暗敷或在吊顶内穿钢管明敷。

7.2.7 辅助系统

- 7.2.7.1 应根据实际情况安装新风系统，保持机房内的正常压强，维持机房内恒定、洁净的空气环境。
- 7.2.7.2 根据实际需求可配置 KVM，通过管理控制服务器对主机系统进行集中控制，支持本地管理和异地管理方式，方便对主机的监控，缩短故障响应时间。
- 7.2.7.3 新风系统抽、进风口应远离核心设备机柜，同时不应位于 UPS 及电池柜（或电池架）上方。

7.3 机房管理

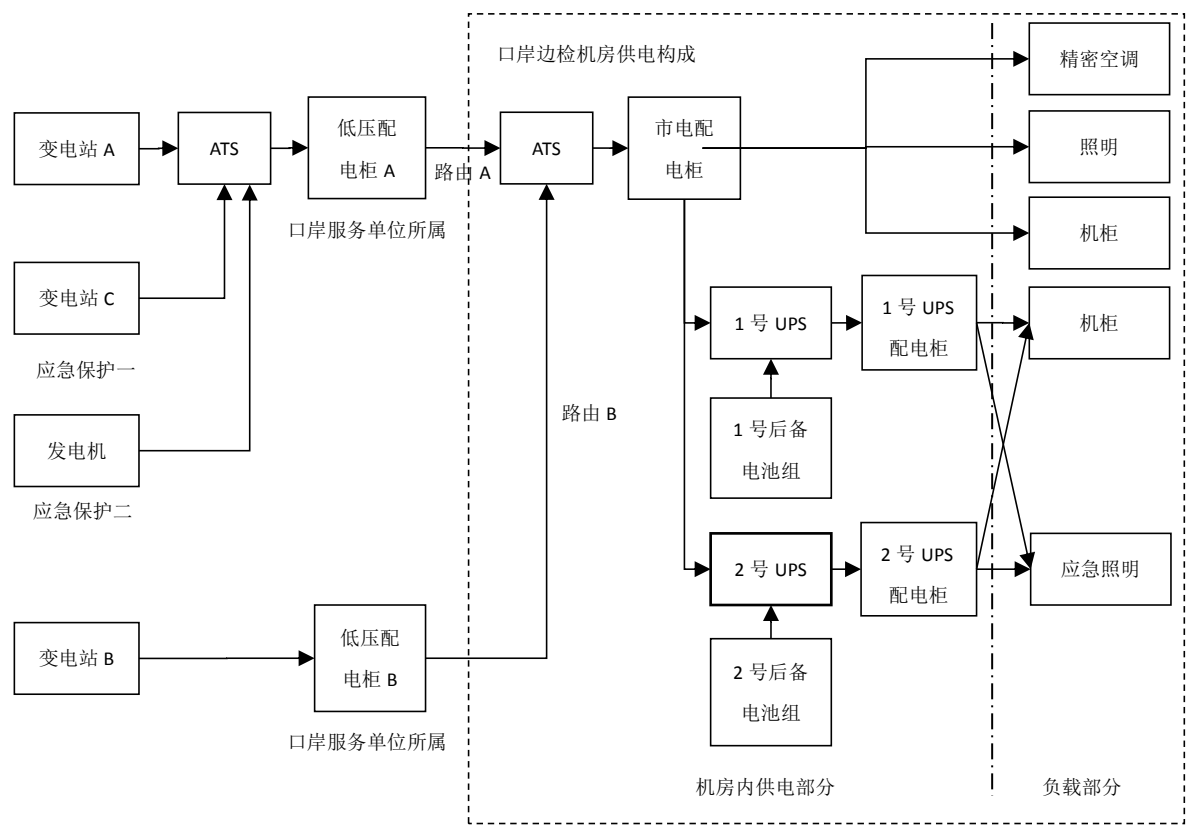
机房、设备间宜由边检机关单独管理，不宜与其他单位共用，并满足以下要求：

- a) 非本单位人员或非授权人员应无权限接触机房内网络、信息系统服务器等核心设备；
- b) 无人值守的机房外墙不应采用玻璃隔断；
- c) 所有出入口应安装出入口控制系统及设备，管理人员出入，并应安装机械锁、指纹解锁、面相识别解锁、密码解锁、IC 卡解锁等不同类型的锁具，保证出入口具备至少两种门禁管理方式；
- d) 当须与其他单位共同使用共享机房时，应在共享机房内设立边检机关独立管理和使用的区域。

8 供电系统

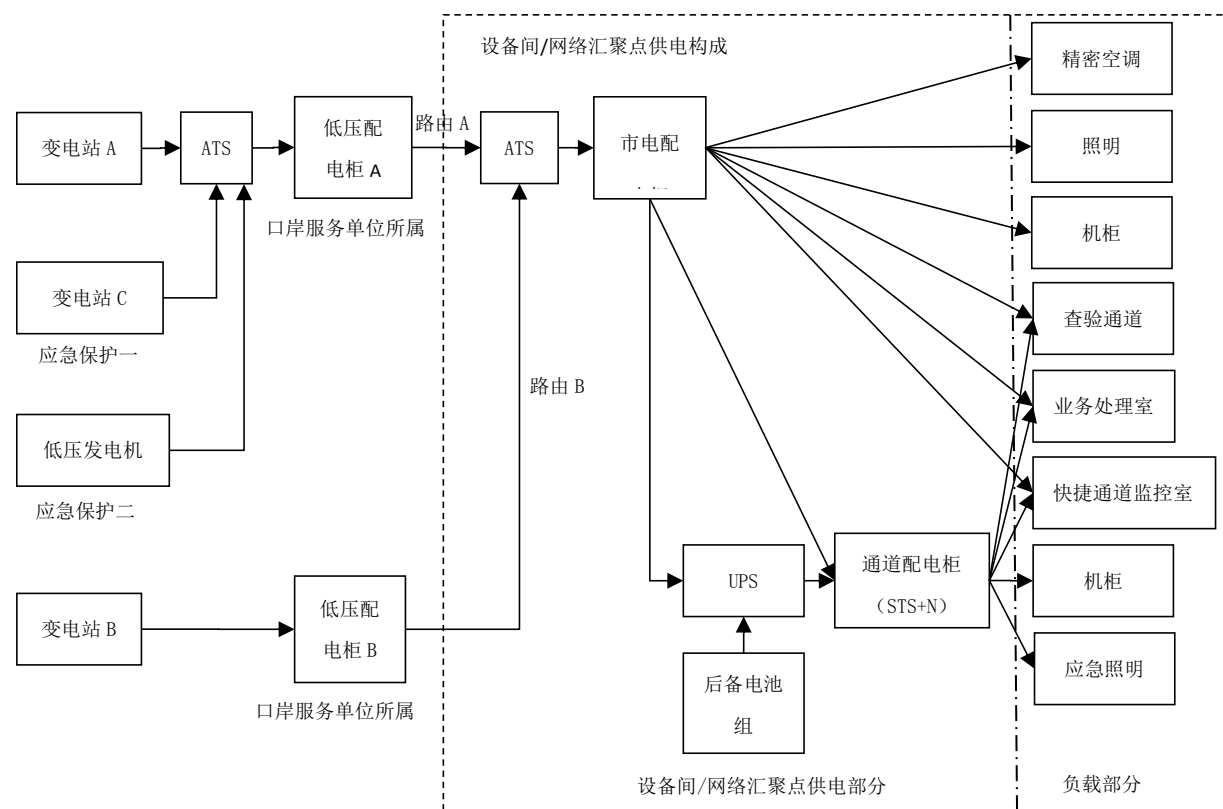
8.1 站级机房和设备间供电系统构成

根据口岸边检信息化建设的空间分布特点、供电条件和安全保障需求，口岸边检的站级机房、设备间/网络汇聚点供电系统构成分别见图2、图3。



注：应急保护一和应急保护二至少具备一种。

图 2 站级机房供电系统构成示意图



注：应急保护一和应急保护二至少具备一种。

图 3 设备间/网络汇聚点供电系统构成示意图

8.2 站级机房供电

站级机房供电满足以下要求：

- a) 应有两路以上从不同变电站供给的多回路三相电源，其中至少一条回路电源应配置应急供电保护或应急低压发电机；
- b) 电源线路应从不同路由铺设进入机房；
- c) 应设置独立使用的市电配电柜，多路电源应通过多电源切换装置完成自动切换，给机房供电；
- d) 机柜和应急照明应配备 UPS 电源。

8.3 设备间供电

设备间供电满足以下要求：

- a) 应至少配置一路主电源和一路应急电源，或其中主路电源应配置应急供电保护；
- b) 电源线路应从不同路由铺设进入设备间；
- c) 应设置独立使用的市电配电柜，双路电源通过双电源切换装置完成自动切换后，给设备间供电；
- d) 查验通道、业务处理室、快捷通道监控室、机柜和应急照明应配备 UPS 电源。

8.4 配电柜

市电配电柜、UPS 配电柜和通道配电柜满足以下要求：

- a) 采用空气开关，应按照 20%冗余数量配置，其下方应安装承重架，并采用母排配线方式接入配电柜；

- b) 应具备对每条输入输出回路的电压、电流、负载等情况进行监测统计等功能;
- c) 应具备数字化查询接口;
- d) 安装应符合 GB 50054 的相关规定;
- e) 选型的配电柜及其配套的设备及辅件应符合 GB/T 7251.1、GB/T 7251.2 和 GB/T 14048.1 的相关规定。

注: GB/T 7251 适用于交流不超过 1000 V, 直流不超过 1500 V 的成套设备; GB/T 14048 适用于(当有关产品标准有要求时)低压开关设备和控制设备, 该电器用于连接额定电压交流不超过 1000 V 或直流不超过 1500 V 的电路。

8.5 UPS 供电

8.5.1 总体要求

- 8.5.1.1 站级机房应至少配置双 UPS 系统, 设备间应至少配置一路 UPS 系统, 保障设备供电。
- 8.5.1.2 初始建设时, 负载量不应超过主机容量的 25%, 并应按照主机满载、后备时间不少于 2 h 标准配置后备电池组。
- 8.5.1.3 机房设置的 UPS 配电柜满足以下要求:
 - a) 每台 UPS 主机应配置一套独立使用配电柜或配电模块, 其线路应与其他电源线路相绝缘;
 - b) 配电柜内的输入、输出线路、空气开关应标签清晰, 对应明确;
 - c) 对于三相输出的 UPS, 应遵循平衡负载接入原则, 避免偏相。
- 8.5.1.4 UPS 电源满足以下要求:
 - a) 选型使用应符合 GB/T 19115.1 的相关规定;
 - b) 操作人员触及区使用应符合 GB/T 7260.1 的相关规定;
 - c) 限制触及区使用应符合 GB/T 7260.4 的相关规定。

8.5.2 后备电池组

后备电池组供电满足以下要求:

- a) 应安装在开放式电池架内, 下方应安装有承重架;
- b) 电池接头应配备绝缘胶套;
- c) 电池架顶部应配置透明绝缘板;
- d) 电池组应通过直流开关与 UPS 主机相连, 电池架应做接地处理;
- e) 机房空间充足的条件下, 应与机房其他设备分开独立放置。

8.6 通道供电

通道供电满足以下要求:

- a) 查验场地设备间应配备专用的通道配电柜;
- b) 通道配电柜应支持双路电源输入、包含多组支持热插拔的双电源自动静态切换模块、每组模块切换时间不高于 8 ms、输出端口可快速插拔等功能。

8.7 设备供电

设备供电满足以下要求:

- a) 机房设备间内用于保障公安网、业务网、视频专网上各应用系统运行设备以及查验电脑、证件阅读机、快捷通道等各类前台查验设备, 应使用 UPS 系统电源;
- b) 打印机、碎纸机等办公设备以及取暖机、电风扇等生活设备不应接入 UPS 系统电源;
- c) 制冷、新风、维修电源、通道电动门、通道增强照明等辅助系统及设备应接入市电供电系统;

- d) 视频监控系统、报警系统和门禁系统等供电要求应符合 GB/T 15408 的相关规定。

9 综合布线

9.1 机柜

机房内应根据需求规划配置服务器机柜、专用网络机柜以及非标准机柜等，并满足以下要求：

- a) 机房内应设置专用网络机柜，作为机房弱电线路的核心汇聚点。初始建设时，机柜内空间使用率不宜超过 50%；
- b) 机柜内宜设上、下走线槽，每排机柜之间设横向走线槽，用于机柜间电源线和数据线等内部走线，并配备相应数量的理线架。

9.2 布线

9.2.1 基本要求

基本要求包括以下内容：

- a) 机房内宜采用上走线方式开展综合布线系统建设；
- b) 使用独立的强、弱电金属桥架和专用 ABS 光纤槽道，宜预留 50%的空余空间；
- c) 暂无业务需求的区域，宜规划备用线槽；
- d) 综合布线选型应符合 GB 50311 的相关规定。

9.2.2 工作区布线

9.2.2.1 工作区信息插座

工作区信息插座的安装满足以下要求：

- a) 暗装在地面上的信息插座盒应满足防水和抗压要求；
- b) 宜具备保护壳体；
- c) 暗装或明装在墙体或柱子上的信息插座盒底距地高度宜为 300 mm；
- d) 安装在工作台侧隔板面及临近墙面上的信息插座盒底距地高度宜为 1000 mm；
- e) 信息插座模块宜符合标准 86 系列面板安装要求，安装光纤模块的底盒深度不应小于 60 mm。

9.2.2.2 工作区电源插座

工作区电源插座的安装满足以下要求：

- a) 每个工作区宜配置不少于两个单相交流 220V/10A 电源插座盒；
- b) 应选用带保护接地的单相电源插座，接在漏电保护开关下端；
- c) 宜嵌墙暗装，电源插座盒底距地高度宜为 300 mm，高度应与信息插座一致。

9.2.3 导管与桥架安装

布线导管与桥架的安装满足以下要求：

- a) 材质、性能、规格以及安装方式的选择应满足敷设场所的温度、湿度、腐蚀性、污染以及自身耐水性、耐火性、承重、抗挠、抗冲击等因素对布线的要求；
- b) 缆线敷设在建筑物的吊顶内时，应采用金属导管或槽盒；
- c) 建筑物室外引入管道设计应满足建筑结构地下室外墙的防水要求，引入管道应符合 GB 50311 的相关规定。

9.2.4 线缆敷设

建筑物内线缆的敷设方式应根据建筑物构造、环境特征、使用要求、需求分布以及所选用导体与线缆的类型、外形尺寸及结构等因素综合确定,并满足以下要求:

- a) 水平缆线敷设时,宜采用穿干管、桥架的方式,并满足以下要求:
 - 1) 墙体内宜采用穿干管方式敷设;
 - 2) 吊顶内宜采用金属托盘、槽盒的方式敷设;
 - 3) 吊顶或地板下缆线引入至办公家具桌面宜采用垂直槽盒方式及利用家具内管槽敷设;
 - 4) 大开间地面布放缆线时,根据环境条件宜选用架空地板下或网络地板内的托盘、槽盒方式敷设;
 - 5) 从槽盒、托盘引出至信息插座,宜采用金属导管方式敷设。
- b) 干线子系统垂直通道宜选用穿楼板电缆孔、导管或桥架、电缆竖井三种方式敷设;
- c) 建筑群之间的缆线宜采用地下管道或电缆沟方式敷设;
- d) 明敷缆线除了满足室内或室外敷设场所环境特征要求外,应符合 GB 50311 的相关规定。

9.2.5 设备安装设计(机柜)

机柜的选择与安装满足以下要求:

- a) 综合布线系统宜采用标准 19" 机柜,安装满足以下要求:
 - 1) 机柜数量规划应计算配线设备、网络设备、电源设备及理线等设施的占用空间,以及设备安装的空间冗余和散热需求;
 - 2) 机柜单排安装时,前面净空不应小于 1000 mm,后面及机列侧面净空不应小于 800 mm;多排安装时,列间距不应小于 1200 mm。
- b) 在公共场所安装配线箱时,暗装箱体底边距地面不宜小于 1.5 m,明装式箱体底面距地面不宜小于 1.8 m;
- c) 机柜、机架、配线箱等设备的安装宜采用螺栓固定,在抗震设防地区,设备安装应采取减震措施,并应进行基础抗震加固。

9.2.6 标签

综合布线的标签要求见表1。

表 1 综合布线的标签要求

序号	用途	公安专网	视频专网	边检专网	其他网
1	双绞线跳线	橙色	蓝色	灰色	蓝色
2	BMC 管理电口	灰色	灰色	灰色	灰色
3	多模光纤跳线	浅绿色	浅绿色	橙色	橙色
4	单模光纤跳线	黄色	黄色	黄色	黄色
5	标签	红底黑字	蓝底黑字	白底黑字	蓝底黑字
6	管理口标签	白底黑字	白底黑字	白底黑字	白底黑字
注:公安专网、视频专网标签定义有统一的标准规范,边检专网和其他专网与公安专网及视频专网区分开。					

9.3 强电

9.3.1 站级机房

站级机房应符合本文件中 8.2 的规定，综合布线满足以下要求：

- a) 站级机房的机柜应至少配有三路电源，两路 UPS 电源、一路市电；
- b) 机房建设时，应在墙面规划设置市电、UPS 电源插座，电源线路应采用 3 芯电缆；
- c) 市电插座与 UPS 插座应采用不同颜色区分，市电宜采用白色插座、UPS 电源宜采用红色插座。

9.3.2 设备间

设备间满足以下要求：

- a) 站级机房的机柜至少应配有两路电源，一路 UPS 电源、一路市电；
- b) 机房建设时，应在墙面规划设置市电、UPS 电源插座，电源线路应采用 3 芯电缆；
- c) 市电插座与 UPS 插座应采用不同颜色区分，市电宜采用白色插座、UPS 电源宜采用红色插座。

9.3.3 机柜

机柜满足以下要求：

- a) 机柜中应配有市电 PDU 和 UPS 电源 PDU，机柜数量较多的机房内应设置列头柜，负责机柜 PDU 供电控制，其参数要求与 UPS 配电柜一致；
- b) 宜采用模块化机柜。

9.3.4 执勤场地使用的设备间

执勤场地使用的设备满足以下要求：

- a) 应分别从每条查验通道铺设 1 条 UPS 电源线路至通道配电柜；
- b) 每 2 条旅客查验通道应铺设 1 条市电线路至市电配电柜；每条车辆查验通道应铺设 1 条市电线路至市电配电柜；
- c) 电源线路应采用 3 芯电缆，通道端市电插座与 UPS 插座应采用不同颜色区分：
 - 1) 通道端市电应采用白色插座；
 - 2) UPS 电源应采用红色插座。

9.4 弱电

9.4.1 口岸内

口岸内满足以下要求：

- a) 通信光缆应整缆铺设，中间不应做接头，不应与其他光缆续接混用；
- b) 应采用 LC 型连接器接口；
- c) 网线应使用标准六类及六类以上网线，应采用 RJ45 接口。

9.4.2 机房内

机房内应从核心网络机柜向其他机柜铺设 12 芯单模光缆和 12 条六类及六类以上网线并成端。

9.4.3 执勤场地使用的设备间

执勤场地使用的设备间满足以下要求：

- a) 每条旅客查验通道应铺设 4 条六类及六类以上网线和 2 芯单模光纤至网络机柜；
- b) 每条车辆查验通道应铺设 2 条六类及六类以上网线和 8 芯单模铠装光缆至网络机柜；

- c) 每条船舶或其他交通运输工具查验通道宜铺设 2 条六类及六类以上网线和 8 芯单模铠装光缆至网络机柜。

9.4.4 业务用房

业务用房满足以下要求：

- a) 旅客查验场地的业务处理室宜铺设不少于 4 条旅客查验通道布线的标准铺设强弱电线路；
- b) 车辆查验监控室宜铺设不少于 4 条车辆查验通道的布线标准铺设强电线路，每条车辆查验通道宜敷设 2 条六类及六类以上网线和 2 芯光纤标准的弱电线路；
- c) 查验场地较大的业务处理室和车辆查验监控室宜根据实际情况建设网络电源汇聚点。采集点、查询点等业务区域宜参照查验通道标准铺设强弱电线路。

9.4.5 内部光缆

内部光缆满足以下要求：

- a) 口岸内应使用单模铠装光缆搭建主干网络；
- b) 站级机房之间应铺设光缆相连，每条光缆纤芯数量不应少于 48 芯；
- c) 主机房、灾备机房应与每个设备间之间铺设光缆相连，每条光缆纤芯数量不应少于 24 芯；
- d) 设备间与临近设备间之间应铺设光缆，每条光缆纤芯数量不应少于 24 芯；
- e) 连接主机房、灾备机房的光缆应采用不同路由铺设。

9.4.6 外部光缆

外部光缆满足以下要求：

- a) 主机房应分别铺设与临近两个或两个以上其他口岸主机房的光缆，并应根据实际需求铺设主机房与总站机房的通信光缆；
- b) 光缆应使用单模铠装光缆，纤芯数量不应少于 48 芯。

10 网络系统

10.1 总体要求

10.1.1 网络规划原则

各口岸边检网络系统主要由边检公安信息网、边检业务网、边检视频专网、政务外网、互联网五张独立网络构成，网络系统总体构成示意图见图4。

注1：政务外网即国家电子政务外网，按照中办发〔2002〕17号文件和〔2006〕18号文件要求建设的我国电子政务重要公共基础设施，是服务于各级党委、人大、政府、政协、法院和检察院等政务部门，满足其经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络，用于实现政府内部信息交流和公共服务的提供；它属于互联网，是国家政务内网互联网区域，即政务对外服务的业务专网，与互联网通过防火墙逻辑隔离。

注2：互联网是常用的公共网络环境。

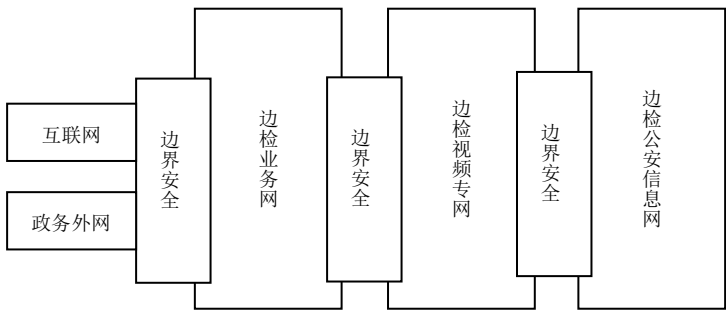


图 4 各口岸边检网络系统总体构成示意图

10.1.2 网络总体架构

各口岸边检公安信息网、边检业务网、边检视频专网应与深圳边检总站及比邻口岸边检站互联互通，网络总体架构示意图见图5。

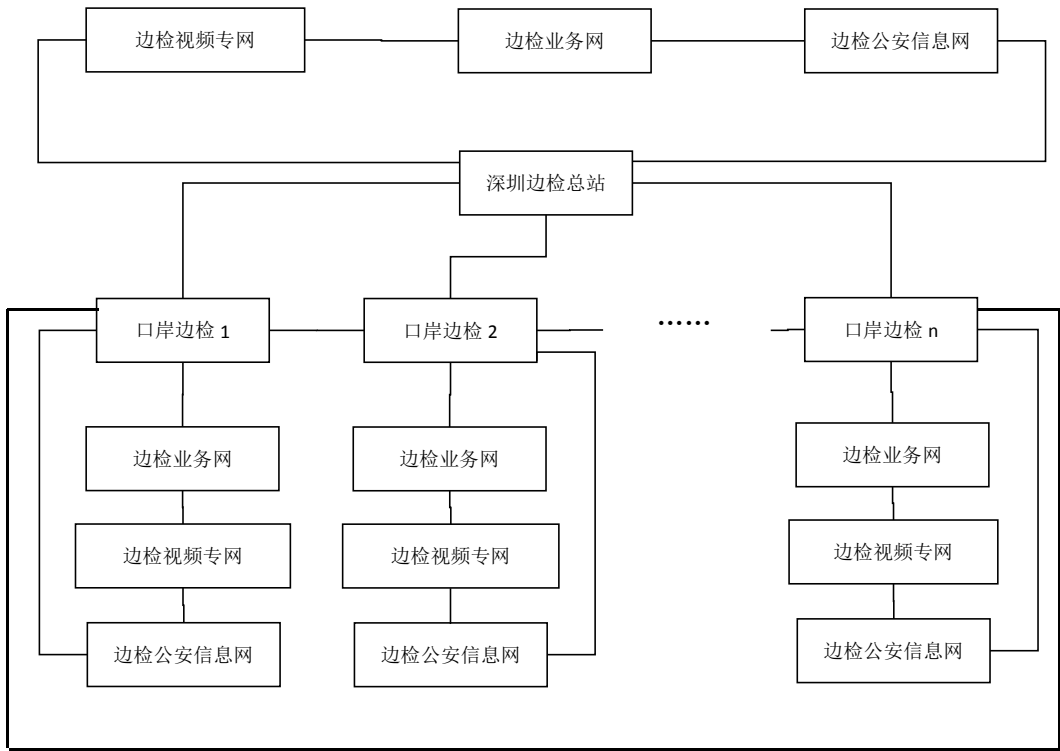


图 5 口岸边检网络总体架构示意图

10.1.3 口岸内网络架构

口岸内网络架构满足以下要求：

- a) 各口岸内部网络应按照核心层和接入层两层架构部署，其中网络核心层交换机应按冗余模式部署 3 层高性能交换机；
- b) 各口岸内边检视频专网摄像头应连接到部署在口岸边检的光传送网设备；
- c) 口岸边检公安信息网、边检业务网和边检视频专网网络架构分别见图 6、图 7 和图 8。

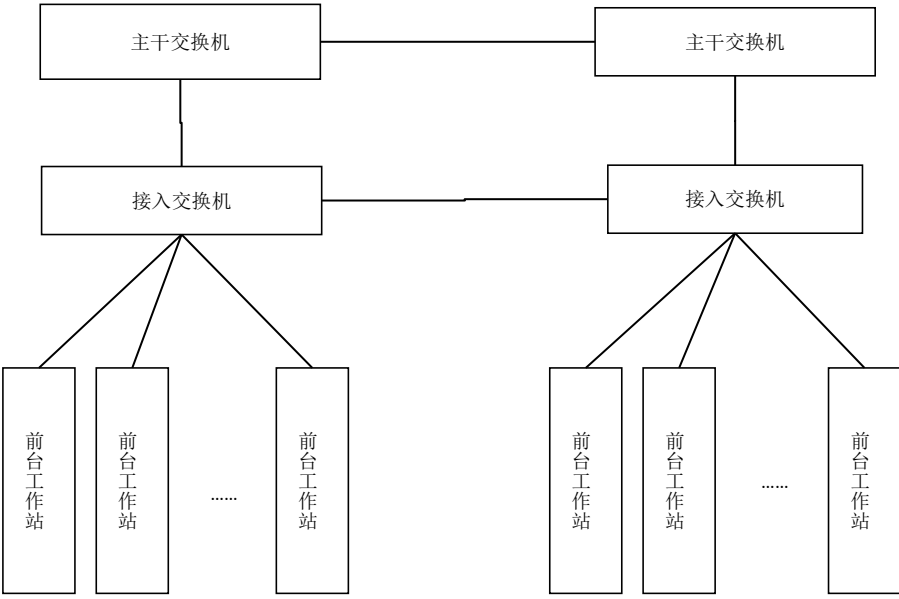


图 6 边检公安信息网网络架构示意图

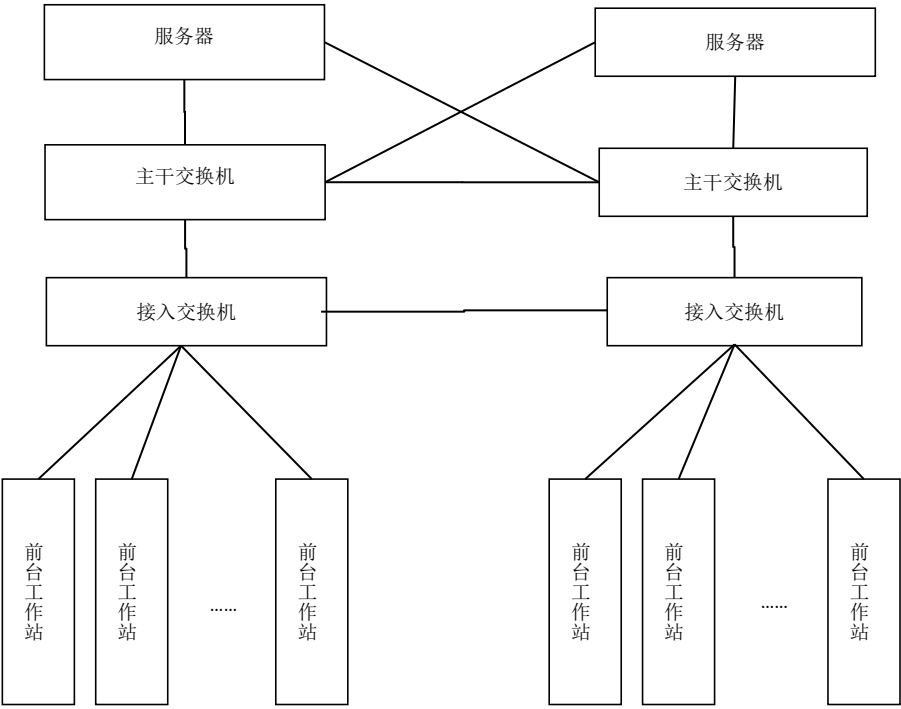


图 7 边检业务网网络架构示意图

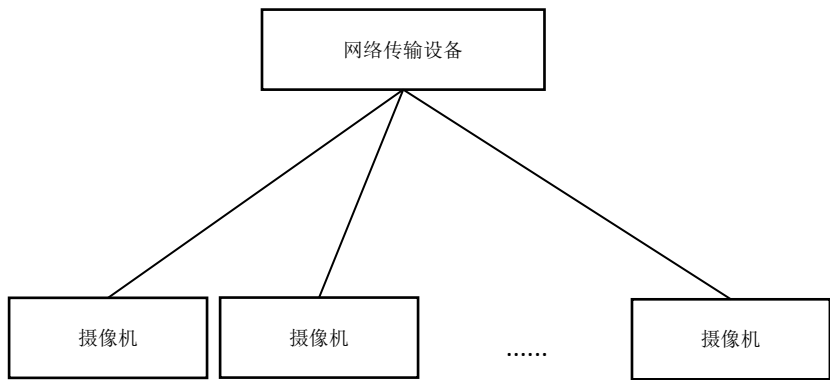


图 8 边检视频专网网络架构示意图

10.2 口岸网络建设要求

10.2.1 口岸承载网建设原则

口岸承载网建设原则包括以下内容：

- a) 各口岸边检公安信息网、边检业务网、边检视频专网宜通过传输链路与深圳边检总站及比邻口岸边检站互联互通；
- b) 传输链路宜采用 OTN、MSTP 等链路类型，通过独立时隙进行物理隔离传输，传输过程应具备防篡改、防窃听措施；
- c) 口岸边检承载网构成见图 9。

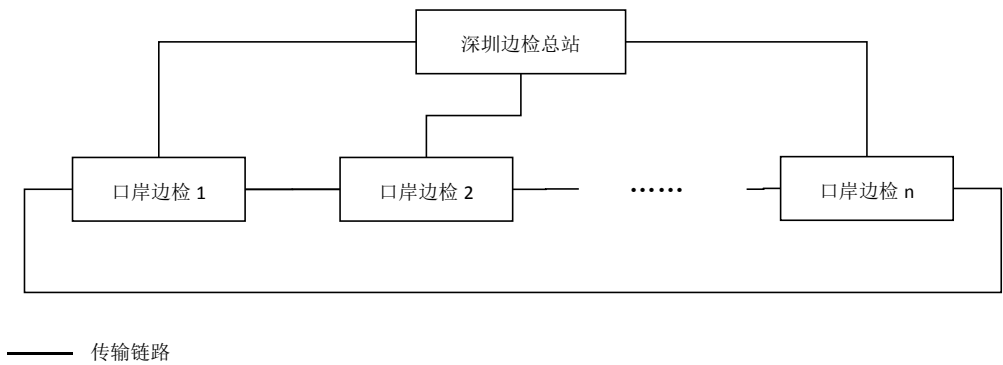


图 9 口岸边检承载网络示意图

10.2.2 边检视频专网建设原则

边检视频专网建设原则包括以下内容：

- a) 口岸摄像机视频图片流传输链路宜采用 OTN、MSTP 链路类型独立时隙回传至深圳边检总站视频云平台，满足边检视频流和图片流等敏感数据高安全传输的要求；
- b) 边检视频专网构成见图 10。

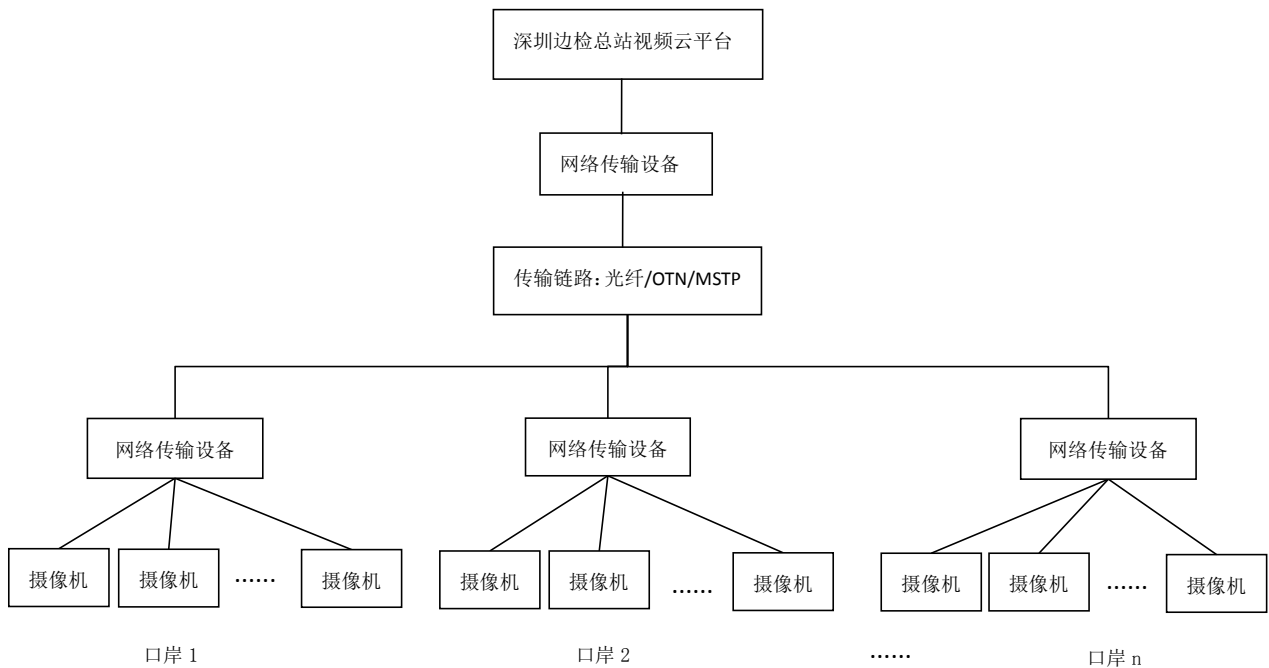


图 10 边检视频专网构成示意图

10.3 口岸网络链路传输指标

10.3.1 边检公安信息网传输指标

边检公安信息网传输指标满足以下要求：

- a) 网络带宽：各口岸间横向传输链路带宽不应小于 1 Gbps，纵向至深圳边检总站传输链路带宽不应小于 2 Gbps；
- b) 传输质量：网络时延不应超过 100 ms，时延抖动不应超过 50 ms，丢包率不应大于 1×10^{-3} 。

10.3.2 边检业务网传输指标

边检业务网传输指标满足以下要求：

- a) 网络带宽：各口岸间横向传输链路带宽不应小于 4 Gbps，纵向至深圳边检总站传输链路带宽不应小于 2 Gbps；
- b) 传输质量：网络时延不应超过 100 ms，时延抖动不应超过 50 ms，丢包率不应大于 1×10^{-3} 。

10.3.3 边检视频专网传输指标

边检视频专网传输指标满足以下要求：

- a) 网络带宽：对于前端采集点位链路带宽，单个监控采集点位不应小于 100 Mbps；
- b) 传输质量：网络时延不应超过 50 ms，时延抖动不应超过 20 ms，丢包率不应大于 1×10^{-3} 。

10.4 口岸内设备要求

交换机配备满足以下要求：

- a) 业务网核心层交换机应配备双机冗余，其他网络核心层交换机应根据口岸业务量的冗余能力、可靠性、传输速率、吞吐量、带宽等因素进行配备；

- b) 业务网接入层交换机应配备双电源、双机热备+单机冷备、双上行路由（“门”字结构或“口”字结构）；
- c) 每个交换机 RJ45 接口实际接入数量不应超过交换机的 75%。

10.5 网络边界原则

口岸边检公安信息网、边检业务网、边检视频专网不应建设与互联网联接的边界区域或设备，并应严格遵循“与互联网物理隔离”原则，任何单位和个人不应建立公安网与其它网络的直接联接，不应将公安网延伸到非公安机关单位；如果公安信息网、业务网、视频专网之间因业务需要进行联网时，应报深圳边检总站批准实施。

11 通信系统

11.1 系统构成及基本要求

通信系统主要由有线通信、无线通信、应急通信等系统构成，各系统满足以下要求：

- a) 有线通信系统包括内线语音通信系统等，通过固定线路完成日常性高、保密性强、场所固定的指挥调度通话需要，并满足以下要求：
 - 1) 语音通信系统包含国家移民管理局机关至深圳边检总站、深圳边检总站至其他总站、深圳边检总站至各站级单位语音等具备统一通信协议的网络通信系统，应确保内部专网电话、传真等畅通；
 - 2) 语音通信系统应由深圳边检总站统一架构，使用统一信令，应采用 SIP 协议的接入设备，网络层应接入边检视频专网；
 - 3) 语音通信系统的各用户节点宜根据办公环境使用模拟电话线路，集中至语音 IAD 设备后分配用户话号入网；宜使用视频专网网络，采购 IP 电话入网。
- b) 无线通信系统主要包括警用数字集群（PDT）对讲通信系统和普通无线对讲通信系统，完成户外作业、移动作业等点对点或点对多点的指挥调度通话需要，并满足以下要求：
 - 1) 警用数字集群（PDT）对讲通信系统应符合 GA/T 1056—2013、GA/T 1059—2013 的相关规定；
 - 2) 警用数字集群（PDT）对讲通信系统应使用口岸驻地公安机关的 PDT 核心网，应支持属地化 PDT 数字集群“一张网”运行；边检的 PDT 基站能直接接入属地公安局的 PDT 系统；

注1：PDT系统由PDT核心网与PDT基站组成；PDT核心网包含了中控服务、网管服务、加密鉴权服务、调度服务、录音服务等硬件服务器和软件系统，是警用数字集群PDT对讲通信系统的控制中心；PDT核心网与PDT基站之间通过专用链路有线连接，组成的网络叫PDT专用网络。

注2：“一张网”是指边检的PDT基站接入属地公安局的PDT核心网（即属地公安局的PDT对讲机系统控制中心），所有对讲机终端都在属地公安局的PDT对讲通信系统下管理。

注3：口岸规划建设时，当地政府（市人民政府）协助口岸建设单位对接驻地公安机关，完成PDT系统的安全接入。
 - 3) 多种制式下的无线通信系统应互联互通，包括窄带无线通信系统和宽带无线通信系统。基于全国边检 PDT 系统网络(对讲机通信网络)，能支持包含国家移民管理局机关至深圳边检总站、深圳边检总站至其他总站、深圳边检总站至各站级单位等语音通信的通信系统。

注：多种制式一般是指常规对讲通信、集群对讲通信、模拟对讲通信、数字对讲通信、公网专用通信、窄带通信、宽带通信等多种通信的模式。

- c) 应急通信系统包括卫星通信、应急通信车、单场地局域网应急组网通信等，支持应急情况下的通信通话需要。

11.2 有线通信系统建设

有线通信系统建设满足以下要求：

- a) 有线软交换机通信系统接入方式：有线软交换机(SS)应通过 IP 网络接入到边检系统，应支持 SIP 协议的终端和中继设备通过 IP 网络接入，SIP 设备 IP 地址应采用统一规范的全国行政纵向业务系统 IP 地址；
- b) 有线程控交换机通信系统接入方式：有线程控交换机(PBX)能通过中继网关转换后接入到边检系统网络；
- c) 有线通信网与公网的互联互通满足以下要求：
 - 1) 有线软交换机(SS)通过 SIP 中继网关，应支持采用 SIP 协议与公网(PSTN)互联，支持与市话、手机的互联互通；
 - 2) 有线程控交换机(PBX)通过中继网关，应支持 No. 7 信令与公网(PSNT)互联，支持与市话、手机的互联互通；
 - 3) 有线通信系统的网络带宽要求：采用不同的语音编码技术，有线通信系统的网络带宽要求见表 2。

表 2 有线通信系统的网络带宽要求

编码器	网络带宽需求	备注
G. 711	环回延时<120 ms，带宽需求90.4 kbps	单路呼叫
G. 729a	环回延时<150 ms，带宽需求34.4 kbps	单路呼叫
G. 723.1	环回延时<200 ms，带宽需求22.9 kbps	单路呼叫

11.3 无线通信系统建设

11.3.1 无线通信系统

无线通信系统建设满足以下要求：

- a) 无线通信系统采取以下接入方式：
 - 1) 无线通信系统的各个网络设备之间均应采用 IP 网络接入边检系统网络；
 - 2) 无线通信系统的核心网通过网间接口应支持国家移民管理局机关至深圳边检总站、深圳边检总站至其他总站、深圳边检总站至各站级单位无线系统的互联互通。
- b) 无线通信系统的网络带宽要求见表 3。

表 3 无线通信系统的网络带宽要求

编码器	网络带宽需求
窄带系统	延时<10 ms，抖动<10 ms，带宽大于32 kbps/呼叫，组呼建立延时<500 ms
宽带系统	延时<50 ms，抖动<10 ms，带宽大于100 Mbps，组呼建立延时<500 ms

11.3.2 警用数字集群（PDT）无线对讲通信系统

11.3.2.1 一般要求

系统主要由PDT数字集群基站、手持对讲机终端、车载/固定对讲机终端等组成，满足以下要求：

- a) 应支持在口岸限定区域范围、边防检查机关工作执勤点以及各工作场地之间的单呼、组呼、紧急呼叫、动态重组、短信等功能，支持口岸在日常工作及动态指挥调度情况下无线语音通信和调度功能；
- b) 应符合 GA/T 1056—2013、GA/T 1059—2013 的相关规定。

11.3.2.2 PDT 数字集群基站

基站应采用有线方式通过IP传输链路与深圳边检总站的数字集群交换中心互联，并满足以下要求：

- a) 根据通信业务量的需要，基站应支持载波的扩容；
- b) 基站在可靠性方面应支持基站控制器和信道机电源冗余备份；
- c) 口岸内，信号覆盖及场强要求达到-90 dBm以上的面积覆盖率不应小于98%；
- d) 基站工作频段应为PDT系统频段要求，载波输出功率应小于50 W（可调），接收灵敏度不应大于-118 dBm（误码率为5%）。

11.3.2.3 手持对讲机终端

手持对讲机终端应符合GA/T 1056—2013、GA/T 1059—2013的相关规定，并满足以下要求：

- a) 工作模式应支持数字集群、数字常规和模拟常规；
- b) 工作频段应为 PDT 系统频段要求；
- c) 设备通信应加密，并应符合 GA/T 1059—2013 的相关规定；
- 注：PDT 对讲机要进行加密通信，主要采用公安部规定的加密设备进行通信加密。
- d) 应支持北斗定位；
- e) 应支持蓝牙功能；
- f) 声码器应采用 NOVC；

注：为贯彻落实公安部《关于推进公安信息化发展若干问题的意见（公通字〔2017〕7号）》，公安部明确指出“统一国产终端声码器安装要求”，国内警用对讲机系统的声码器目前都统一为国产“NOVC”。

- g) 电池平均工作时间（5-5-90 工作循环，高功率发射）不应小于 24 h；
- h) 数字静态接收灵敏度不应大于-124 dBm。

11.3.2.4 车载/固定对讲机终端

车载/固定对讲机终端应符合GA/T 1056—2013、GA/T 1059—2013的相关规定，并满足以下要求：

- a) 工作模式应支持数字集群、数字常规和模拟常规；
- b) 工作频段应为 PDT 系统频段要求；
- c) 设备通信应加密，并应符合 GA/T 1059—2013 的相关规定；
- 注：PDT 对讲机要进行加密通信，主要采用公安部规定的加密设备进行通信加密。
- d) 应支持北斗定位；
- e) 应支持蓝牙功能；
- f) 声码器应采用 NOVC；
- g) 噪声抑制能力不应小于 30 dB；
- h) 集群模式下应具备根据当前信号强度自动调节发射功率、信号较强时降低发射功率、信号较弱时增大发射功率等功能。

11.3.3 公网专用视音频通信平台

11.3.3.1 一般要求

平台主要由视音频集群通信系统、公网对讲终端和多模智能终端组成，满足以下要求：

- a) 应保证口岸 PDT 通信系统网络覆盖盲区，支持 PDT 对讲机、公网对讲终端、多模智能终端等多类型终端之间不限距离、不限地域的通信，同时应构建多媒体数据、移动视频能力；
- b) 应符合 GA/T 1057—2013、GA/T 1058—2013、GA/T 1059—2013、GA/T 1364—2017 和 GA/T 1366—2017 的相关规定。

11.3.3.2 视音频集群通信系统

视音频集群通信系统满足以下要求：

- a) 应支持P-SIP与PDT通信系统实现系统级互联，支持为公网专用视音视通信平台提供视音频通信服务、调度服务、媒体服务、录音录像服务等基础服务；
- b) 应接入多类型终端，具备宽、窄带终端之间的跨系统的语音组呼、语音单呼、短消息、状态消息、紧急呼叫、广播呼叫、统一定位等互联功能；
- c) 跨系统语音组呼建立时间不应大于700 ms；
- d) 跨系统话权申请时间不应大于650 ms；
- e) 跨系统语音传输时间不应大于500 ms。

11.3.3.3 公网对讲终端

公网对讲终端应符合GA/T 1056—2013、GA/T 1366—2017的相关规定，并满足以下要求：

- a) 工作频段应包括2G/3G/LTE，宜包括5G；
- b) 设备通信应加密，并应符合 GA/T 1059—2013 的相关规定；
注：PDT 对讲机要进行加密通信，主要采用公安部规定的加密设备进行通信加密。
- c) 应支持GPS、北斗双定位；
- d) 应支持室内、室外全覆盖精准定位；
- e) 应支持蓝牙、Wi-Fi等功能；
- f) 电池平均工作时间（5-5-90工作循环，高功率发射）不应小于24 h。

11.3.3.4 多模智能终端

多模智能终端应符合GA/T 1056—2013、GA/T 1366—2017的相关规定，并满足以下要求：

- a) 应支持融合PDT数字集群和2G/3G/LTE/5G/WLAN等宽带通信；
- b) 应支持PDT集群业务、PDT语音室内通信；
- c) 设备通信应加密，并应符合 GA/T 1059—2013 的相关规定；
注：PDT 对讲机要进行加密通信，主要采用公安部规定的加密设备进行通信加密。
- d) 应支持NVOC声码器；
- e) 数字静态接收灵敏度不应小于-124 dBm；
- f) 应支持GPS、北斗双定位；
- g) 应支持室内外精准定位；
- h) 应支持智能降噪；
- i) 应支持视音频通信、采集及传输等多种业务。

11.3.4 应急通信系统

11.3.4.1 一般要求

一般要求包括以下内容：

- a) 系统主要由窄带自组网、宽带自组网、专网 LTE 基站、宽带集群对讲系统、应急指挥调度系统、多模智能终端、执法记录仪等组成；
- b) 系统应具有组网灵活、部署便捷、覆盖广、传输带宽高等特点，应能结合口岸应急通信需求，支持现场音频、视频和关键数据等信息实时、稳定地回传至各级指挥中心，通过多媒体通信网络，支持统一的可视化调度指挥。

11.3.4.2 窄带自组网

窄带自组网满足以下要求：

- a) 应支持灾害现场语音无线信号覆盖，用于灾害现场语音信号的接力传输及信号延伸，每一跳中继之间应至少保证穿透地下 2 层、水平 5 km 的传输距离；
- b) 语音通信设备满足以下要求：
 - 1) 应具备无线自组网功能，支持级联多跳自组网模式组建网络，具备大范围的语音业务覆盖功能；
 - 2) 应兼容 PDT 系统频段的终端，具备数字业务覆盖功能；
 - 3) 应具备开机一键式使用功能；

注：一键式使用无需配置和更改参数，无需人工干预，短时间内即可完成组网。
 - 4) 应具有整机一体化设计、便携、防灾抗毁、快速投放延伸覆盖等特点；
 - 5) 应支持车载使用、单兵便携移动部署。

11.3.4.3 宽带自组网

宽带自组网满足以下要求：

- a) 应支持快速部署宽带数据链路，具备灾害现场宽带视频采集及视频实时传输功能，具备灾害现场到前方指挥部的宽带信号自动覆盖功能；
- b) 应支持多种灵活组网模式，在全向天线情况下，空旷地不应小于 10 km，城市建筑群不应小于 2 km，大型场馆、地下停车场等密闭场所不应小于 800 m；
- c) 应支持蓝牙、Wi-Fi 等多类型接口；
- d) 应支持背负、车载、便携多种携装方式。

11.3.4.4 专网 LTE 基站

专网 LTE 基站满足以下要求：

- a) 应支持事故现场外围信息的采集，应具备多方位观察现场形势为应急救援提供更多现场信息的功能，同时满足现场集群业务需求；
- b) 设备应采用 LTE 专网信号的覆盖，应允许专网终端接入；
- c) 基站内部应集成 BU、RRU、核心网功能，应能快速处理数据，便于现场部署和携带。

11.3.4.5 宽带集群对讲系统

宽带集群对讲系统满足以下要求：

- a) 应支持向应急现场终端提供音视频对讲、多媒体信息传输、定位服务以及与现场应急指挥调度员的互联互通功能；
- b) 应具备语音、视频、短消息、定位等基本功能；
- c) 应具备专网特殊业务功能，包括 PDT 拨号规则、强插强拆、遥晕、遥毙、分级组以及一键视频回传等功能。

11.3.4.6 应急指挥调度系统

应急指挥调度系统满足以下要求：

- a) 应具备对现场终端设备的定位、对全网设备的录音录像的功能，具备与窄带自组网络语音互联互通、与现场音视频终端互通与调度功能；
- b) 应具备调度和统一管理现场各类图像、语音、数据的功能，支持集成核心网、网管模块，具备多媒体集群对讲功能；
- c) 支持融合语音调度、视频调度以及数据调度等多种业务，并支持统一呈现和统一管理功能。

11.3.4.7 多模智能终端

多模智能终端满足以下要求：

- a) 应具有公网4G/5G、Wi-Fi、PDT等常规配置，并支持宽带集群对讲系统软件；
- b) 应支持灾害现场、事故外围的图像、数据、语音等多媒体信息的传输；
- c) 应支持窄带语音、宽带语音，以及宽带视频和图像传输；
- d) 应支持宽窄带统一UI界面，操作方便；
- e) 宽窄带两个系统的程序运行及数据分离满足以下要求：
 - 1) 应保证当一方被破坏或宕机时，另一方应能正常工作；
 - 2) 宜支持单独关闭宽带系统，满足窄带超长时间工作。

11.3.4.8 执法记录仪

执法记录仪满足以下要求：

- a) 应具有公网4G/5G、Wi-Fi等配置，以及支持宽带集群对讲系统软件；
- b) 应支持灾害现场、事故外围的音视频或图像数据的摄录与传输；
- c) 应具备宽带语音和视频通信功能，可进行宽带视频及图像回传。

11.3.5 卫星通信系统

11.3.5.1 一般要求

一般要求包括以下内容：

- a) 应不受时间、距离和地域的限制；
- b) 应支持现场与后方指挥中心的语音、视频图像、公安网数据、传真、图文、短信等双向信息传输畅通以及公安网相关应用系统的通信畅通；
- c) 系统应包括卫星电话设备。

11.3.5.2 卫星电话设备

卫星电话设备满足以下要求：

- a) 应支持接入卫星系统，卫星通信可在任何时间、任何地点（含无公网信号区域），保障与各级指挥中心电话、窄带数据；
- b) 应具备GPS、北斗双模定位模块。

11.4 有线和无线通信系统互联互通的技术要求

有线和无线通信系统互联互通满足以下要求：

- a) 号码统一编址要求：有线和无线通信系统均应采用统一号码段编址，支持同一号接入到有线通信系统和无线通信系统；

- b) 互联互通要求：有线通信系统终端之间应支持不基于网关方式的互联互通，互通的路数和方式不应受技术体制的限制；

注：技术体制是指保证通信网正常运行所作的技术规定的总和。

- c) 业务融合要求：应采用类 IMS 交换控制系统，支持有线和无线通信系统的业务级融合；
- d) 安全性要求：有线和无线通信系统之间通信应具备消息机密性与完整性保护；
- e) 接入方式满足以下要求：

- 1) 应使用统一的用户归属服务器 HSS；
- 2) 应统一编制有线用户、无线用户、无线群组、IP 用户；
- 3) 有线终端和无线终端应接入到同一个交换系统，应支持有线用户和无线用户的互联互通；
- 4) 对于无线和有线系统的相同业务应支持完全融合。

注：相同业务包括会议、优先级呼叫、视频调度等功能。

12 查验系统

12.1 总体要求

查验系统通过综合运用信息化手段和传统手段相结合的方式，对口岸边检的人、车、物等进行查验，是支撑出入境边防检查业务的核心系统，满足以下要求：

- a) 应支撑系统运行的操作系统、数据库和应用软件；
- b) 应具备服务器、工作站、旅客快捷通道、车辆查验通道等核心硬件；
- c) 应具备生物特征采集一体机、OCR 证件阅读机等外接设备；
- d) 应支撑出入境边防检查站的日常查验、移动查验、应急查验等业务；
- e) 应在查验前端加入必要的辅助设备，利用后台管理系统，进行设备和数据管理，并提供标准接口调用数据，保证业务快速便捷的开展；
- f) 应具有高可靠性和迭代升级能力。

12.2 系统架构

查验系统架构见图11。

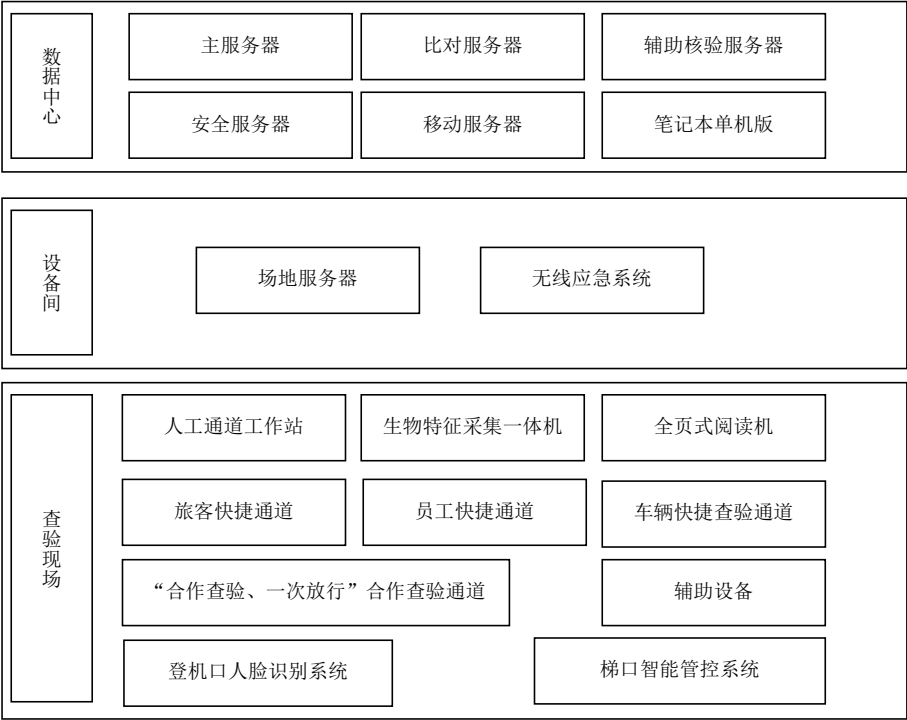


图 11 查验系统架构示意图

12.3 数据中心

12.3.1 服务器总体要求

应采用国产化服务器，操作系统、数据库、中间件等基础软件应通过国家相关机构的检测认证，宜为国产软件。

注1：国产软件的检测认证包含安全要求，安全要求遵照相关的国家安全标准。

注2：国产设备通过相关国家安全标准的认证。

12.3.2 性能要求

查验系统应配套后端服务程序和不同类型的服务器，其核心部件CPU、内存、硬盘、电源等应满足日常业务开展要求，并保证业务稳定流畅运行，满足以下要求：

- a) 高性能：应具有快速处理和响应各种计算任务和数据请求的能力，支持高效率处理复杂的应用场景和大规模的数据；
- b) 高可靠性：应具有高度的可靠性和稳定性，支持长时间的高负载运行，并应具有较强的故障恢复能力，能应对各种异常情况；
- c) 安全稳定：应具有高度的安全防护能力，能抵御各种网络攻击和安全威胁，保证数据的安全性和保密性，并应具有较高的系统稳定性，避免因安全问题而导致的系统崩溃或数据损失；
- d) 弹性扩展：应具有良好的弹性扩展能力，能够根据业务需求进行灵活的升级和扩展，支持横向和纵向的扩展，满足不同阶段的应用需求；
- e) 高效管理：应具有高效的管理和运维能力，能通过集中化的管理平台进行批量管理和监控。

12.3.3 服务器类别划分及部署要求

服务器类别划分及部署要求包括以下内容：

- a) 根据作用或业务功能宜分为主服务器、场地服务器、移动服务器、采集服务器、辅助查验服务器、电子出入境证件数字安全系统安全服务器（以下简称“安全服务器”）、生物特征识别比对服务器和其他与边检查验业务相关联的服务器；
- b) 应部署主服务器和移动服务器（特殊情况下主服务器可作为虚拟服务器在异地或其他口岸集中部署）；
注：移动服务器通过无线网络连接，将移动设备变为小型服务器，提供远程访问和数据传输服务。用于紧急环境搭建和数据访问。
- c) 其他类型服务器宜根据口岸规模和业务需要视情部署。

12.3.4 主服务器

各口岸按规范部署查验系统主服务器，并满足以下要求：

- a) 流量大于1000万人次/年的口岸，应部署4台查验系统主服务器；
- b) 其他口岸应部署2台查验系统主服务器，其中无旅客查验业务的海港口岸，主服务器可以以虚拟化服务器的形式部署；
注：根据建标 185—2017《国家口岸查验基础设施建设标准》，口岸主要分为水运口岸、航空口岸、铁路口岸、公路口岸。
- c) 口岸分为三级，分别是Ⅰ级、Ⅱ级、Ⅲ级，对应为大、中、小口岸。根据口岸大小，主服务器配置数量应满足表4的要求；
- d) 主服务器应采用经边检测试通过、符合边检查验系统使用的主流高性能国产化服务器，主服务器部署应具有防范风险措施，增加灾备管理；
- e) 新建口岸以及流量满足特大型口岸标准的，应根据实际情况增加主服务器数量，见表4，按照技术形势发展，支持主流国产化操作系统，加入虚拟化部署、云计算等。

表 4 主服务器配置数量

口岸类型	数量	单位
Ⅰ级/大	4	台
Ⅱ级/中	2	台
Ⅲ级/小	2	台

12.3.5 移动服务器

各口岸根据口岸规模和应急处置需要部署查验系统移动服务器，配置数量不应小于1台，并满足以下要求：

- a) 硬件配置：应具有较强的计算能力和内存空间，足够的硬盘空间存储应用程序和数据，并支持高速移动互联网连接，足够的电池寿命以保持长时间的使用，以及轻便、易携带和耐用的外观设计等特点；
- b) 操作系统配置：应选择具有性能稳定、安全可靠等特点的操作系统；
- c) 网络环境：应支持高速移动互联网连接、4 Gbps 及以上链路接入和快速数据传输和处理；
- d) 安全管理：应采取一系列的安全管理措施，包括访问控制、加密技术、防火墙等，确保移动服务器的数据安全；
- e) 电源管理：应考虑到电源的问题，使用 UPS 不间断电源等，确保移动服务器在断电的情况下能够继续运行。

12.3.6 安全服务器

各口岸根据口岸规模和业务需要部署安全服务器，满足以下要求：

- a) 流量大于 1000 万人次/年的口岸，部署 3 台安全服务器，其他有旅客查验业务的口岸部署 2 台；海港口岸统一使用总站安全服务器；
- b) 安全机柜和所在机房应满足国家移民管理局对电子出入境证件数字安全系统安全服务器的管理要求，每 2 台安全服务器配备 1 个安全机柜（不足 2 台的以 2 台计），并应额外配备用于存放安全服务器管理员卡、安全服务器机箱钥匙、安全机柜钥匙等配件的密码柜；
- c) 安全服务器系特定专用安全设备，应选购经边检测试通过、符合边检查验系统使用要求的国产化定制安全服务器，安全服务器配置数量见表 5。

表 5 安全服务器配置数量

口岸类型	数量	单位
I 级/大	3	台
II 级/中	2	台
III 级/小	2	台

12.3.7 比对服务器

各口岸根据业务需要部署生物特征识别比对服务器，满足以下要求：

- a) 流量大于 1000 万人次/年的口岸，应部署 4 台比对服务器，其他有旅客查验业务的口岸应部署 2 台；海港口岸应统一使用总站服务器；
- b) 大、中、小口岸配置比对服务器时，应充分考虑负载均衡，应按虚拟化、黑盒子及其他云服务器计算等形式部署，比对服务器配置数量见表 6。

表 6 比对服务器配置数量

口岸类型	数量	单位
I 级/大	4	台
II 级/中	2	台
III 级/小	2	台

12.3.8 辅助核验服务器

辅助查验服务器、采集服务器等服务器应根据口岸实际情况另行规划。

12.3.9 笔记本单机版

各口岸根据口岸规模和应急处置需要在主机房部署笔记本（单机版），配置数量不应小于 2 台，并包括以下内容：

- a) 高性能笔记本；
- b) 14 寸显示器以上；
- c) 内存大于 16G DDR4；

- d) 1T 固态硬盘以上；
- e) 宜配备 2 套作为配件。

12.4 设备间

12.4.1 概述

边检设备间应用于存放包括服务器、存储设备、网络设备等边检设备的房间或空间，应支持边检业务的处理和运行。

12.4.2 场地服务器

各口岸根据口岸规模和旅客通道数量及其他查验设备数量，结合标准服务器算力和旅客通关时间，配置场地服务器数量，并满足以下要求：

- a) 查验场地远离主服务器机房，存在与主机房网络中断风险的场地，根据需要在场地设备间部署场地服务器，其中有旅客快捷通道的场地服务器应存储旅客证件签发信息；
- b) 场地服务器性能应支持边检前端业务流畅运行；
- c) 网络安全性：应具备安全防护措施，包括防火墙、入侵检测、数据加密等方面的安全设备，确保数据安全和业务稳定；
- d) 数据备份和恢复：应具备完善的数据备份和恢复机制，确保数据不会因意外情况而丢失，同时在需要时快速恢复数据；
- e) 电力供应：应具备稳定的电力供应，并配备 UPS 不间断电源等设备，避免因断电而导致服务器停机和数据丢失；
- f) 灾备方案：应制定完善的灾备方案，以应对各种意外情况，确保业务连续性和数据安全性。

12.4.3 无线应急系统

12.4.3.1 部署要求

按照以下要求部署：

- a) 各口岸应在技术值班室、各旅检场地部署 1 套无线应急系统；
- b) 无线应急系统主要由笔记本工作站、无线上网卡、SIM 卡组成；
- c) 宜配备 2 套作为配件。

12.4.3.2 性能要求

性能满足以下要求：

- a) 无线上网卡应支持高速无线接入、内置 SIM 密码算法硬核、端到端数据加密传输、公网安全传输，并支持 4G LTE 网络制式；
- b) SIM 卡应为互联网卡；
- c) 笔记本工作站应为 X86 架构且不应低于 2 核 3.5 GHz，内存不应低于 8 G，并配置千兆网口。

12.5 查验现场

12.5.1 人工通道工作站

12.5.1.1 部署要求

按照以下要求部署：

- a) 各口岸应在人工查验通道、后台处理、海港办理等区域配置高性能台式工作站用于日常查验；

- b) 旅客查验工作站应配备生物特征采集一体机、OCR 证件阅读机等外接设备；
- c) 宜按通道数量 10% 配备配件。

12.5.1.2 性能要求

性能满足以下要求：

- a) CPU 不应低于 2 核 3.5 GHz；
- b) 内存不应低于 16 G；
- c) 网卡应至少含 2 个千兆网口，2 个千兆口可同时使用；
- d) 串口不应少于 3 个；
- e) 硬盘应至少 1T 固态硬盘；
- f) 电源应至少 350 W。

12.5.2 生物特征采集一体机

12.5.2.1 部署要求

按照以下要求部署：

- a) 根据出入境业务需求，每条人工查验通道和每个后台处置电脑部署一台；
- b) 应支持人脸识别、四指指纹采集、虹膜识别等其他必要生物特征；
- c) 设备整合指纹采集、可见光人脸抓拍、显示指引、控制器、音频处理等硬件模块以及实现相应功能的软件部件，可满足口岸出入境检查通道开展生物特征采集工作的需要；
- d) 应部署在口岸边检查验台上（或台外），旅客可按照采集终端的人机交互提示（屏幕显示和声音提示）在终端上自主完成指纹图像、可见光人脸图像采集，同时终端应与口岸边检查验工作站通过软件接口进行交互；
- e) 宜按通道数量 10% 配备配件。

12.5.2.2 性能要求

性能满足以下要求：

- a) 彩色双目摄像头不应小于 300 万像素；红外摄像头不应小于 200 万像素；
- b) 应支持虹膜识别、人脸识别、多模态面部融合的识别方式；
- c) 识别距离应为 40 cm~70 cm（虹膜人脸同时捕捉距离）；
- d) 应具备假体攻击报警功能；
- e) 有效采集窗口尺寸不应小于 15.24 mm×0.32 mm；
- f) 图像大小不应小于 300 pixel×400 pixel；
- g) 图像分辨率不应小于 500 dpi；
- h) 指纹存储容量不应小于 2000 枚。

12.5.3 全页式阅读机

12.5.3.1 部署要求

按照以下要求部署：

- a) 根据出入境业务需求，每条人工查验通道和每个后台处置电脑部署一台；
- b) 应具备护照的全量采集、证件自动翻转和校正、人像裁切、图像保存、机读区阅读、芯片读写、证件真伪鉴别等功能；
- c) 宜按通道数量 10% 配备配件；

- d) 应具备护照读取、证卡识别、电子签证、证件/文件拍照留存、数字签名等功能；
- e) 证照识别范围满足以下要求：
 - 1) 应符合国际民航组织 ICAODOC 9303 的电子护照、电子回乡证、电子台胞证等国内外旅行证件；
 - 2) 应识别身份证、驾驶证、行驶证、港澳通行证、台湾通行证等几十种身份证件。
- f) 部署模式应支持常规部署以及移动部署；
- g) OCR 证件阅读机应具备资料页采集、证件自动翻转和校正、人像裁切、图像保存、机读区阅读、芯片读写、证件真伪鉴别等功能。

12.5.3.2 性能要求

性能满足以下要求：

- a) 多光谱图像采集，应支持输出可见光、红外光、紫外光图像；
- b) CMOS1200 万像素及以上，500DPI 及以上，证件色彩不失真，消除防伪膜和反光的影响，保证证件色彩不失真；
- c) 应支持护照、签证、海员证、港澳台往来通行证、中国二代身份证等证件的图像采集与全页识别，拍照识别速度应小于 1 s；
- d) 应支持证件人像提取裁切、机读码解析、证件照片及电子照片比对、个人资料页信息和电子芯片内容比对鉴别的功能；
- e) 应支持符合 ICA09303 标准的电子证件（如带电子芯片的护照和往来港澳通行证）及二代身份证电子芯片读卡，护照读卡时间应小于 2 s，身份证读卡应小于 1 s；
- f) 应支持 ISO14443 Type A/B 类型卡片读卡；
- g) 应支持 BAC、EAC、PACE、PA、AA 等芯片通信及认证技术。

12.5.4 快捷通道

12.5.4.1 基本要求

快捷通道的系统及设备提供商或厂家应提供符合口岸边检针对出入境边防检查自助通道查验系统建立的技术规范的检测报告，或者针对通道设备提供符合GA/T 1260相关要求的检测或认证报告。

12.5.4.2 旅客快捷通道

旅客快捷通道满足以下要求：

- a) 应支持旅客证件核验、指纹识别、人脸识别等识别功能，以及其他必要生物特征识别功能；
- b) 应支持智能卡技术、OCR 技术、防尾随技术等；
- c) 应支持计算机智能控制、通道安全管理、状态检测、运行状态集中监控等功能，并应快速读取、对比、识别人员证件信息、生物特征信息、自动完成人员出入验放；
- d) 根据技术发展形势，可加入虹膜识别等其他必要生物特征识别，以及通道双向使用、非接触无感通关等技术；
- e) 旅客创新查验模式下可采用单一识别或其他快速验证方式，实现“常旅客”快速通关。

注：旅客创新查验模式是指经常往来通关旅客，往来频率符合政策标准的，采取快速通关模式。

12.5.4.3 员工快捷通道

员工快捷通道满足以下要求：

- a) 根据口岸实际要求配置功能,应支持口岸工作人员工作证/身份证/出入境证件等多类证件核验、指纹识别、人脸识别、虹膜识别、RFID卡识别等识别功能,以及其他必要生物特征识别功能;
- b) 应支持智能卡技术、OCR技术、防尾随技术;
- c) 应支持计算机智能控制、通道安全管理、状态检测、运行状态集中监控等功能,并应快速读取、对比、识别人员证件信息、生物特征信息、自动完成工作人员出入验放;
- d) 宜支持生物特征识别,以及通道双向使用、非接触无感通关等功能;
- e) 应支持单门双向/双门双向等通行方式,并配套管理软件系统及管理电脑。

12.5.4.4 “合作查验、一次放行”合作查验通道

12.5.4.4.1 部署要求

按照以下要求部署:

- a) 新建、改建、扩建口岸应配套建设独立的内地与港方合作查验场地的机房、设备间和网络通信、视频监控、显示引导等系统;
- b) 一地两检模式下的旅客快捷通道应具备证件识别、凭条打印、闯关报警、护照阅读、防尾随等功能,双方查验应配置数据交换设备、安全边界等网络设备。

12.5.4.4.2 性能要求

性能满足以下要求:

- a) 平均通行频率应为 10 人/min;
- b) 极限开关门时间应小于 0.5 s/次;
- c) 通道闸机平均无故障周期 MCBF 不应小于 500 万次;
- d) 平均修复时间 MTTR 不应大于 30 min;
注:特指核心部件的更换时间,包括主控设备和闸机机芯更换时间。
- e) 冲撞侦测:遇撞击时,闸门停止运行,避免伤人;
- f) 总体人工干预率:异常报警等人工干预率不应大于 0.5%;
- g) 尾随告警响应时间应小于 1 s,即当尾随人员进入尾随监测区域开始至客户端发出报警提示时间应小于 1 s;
- h) 尾随检测的误报率应小于 0.1%。

注:通道查验系统所选用的人行出入口电控通道闸需获得公安部的检测认证后投入市场,检测标准为 GA/T 1260《人行出入口电控通道闸通用技术要求》。

12.5.4.5 车辆快捷查验通道

12.5.4.5.1 部署要求

按照以下要求部署:

- a) 新建、改建、扩建口岸应配套建设独立的口岸联检单位共同使用的机房、设备间和网络通信、视频监控、显示引导、通道管控等系统;
- b) 应支持自动识别车牌、自动侦测车辆高度、自动调节操作面板高度、证件识别、生物特征识别;
注:生物特征识别包含人脸识别、指纹识别及其他必要生物特征识别。
- c) 应支持机械自动化技术、超声波雷达等定位技术,应智能识别捕捉乘客位置、抓拍人脸、核验信息;

- d) 应具备车辆防冲关、车体人员检测、双向对讲、远程控制、通道状态检测等功能；
- e) 支持“一站式”查验模式：在车辆快捷通道的基础上进行功能扩展，支持车辆及驾驶人在一条通道内自助完成边检与海关两个单位查验手续并通关。

12.5.4.5.2 性能要求

性能满足以下要求：

- a) 适用对象：完成信息备案采集的驾驶人及车辆；
- b) 车牌识别类型：包括内地车牌、香港车牌、澳门车牌、特种车牌等；
- c) 车辆通行效率：平均核验时间不应大于 30 s；
- d) 防护等级不应小于 IP54。

12.6 辅助设备

各口岸应根据业务实际，配置前置采集机、签证/签注查询机、自助采集机等一体化便民设备，以及查验系统智能手机、移动警务终端、移动查验终端、智能手持核验终端、证卡销毁等其他移动设备，并满足以下要求：

- a) 前置采集机/自助采集机（外国人生物特征采集）满足以下要求：
 - 1) 用于出入境外国旅客按照提示自助操作完成出入境证件、十指指纹、可见光人脸等信息的采集核验，为外国人提供便捷服务；
 - 2) 设备应集成证件阅读器、四指指纹仪、高速热敏打印机、面相采集摄像头等部件，与边检查验工作站无缝对接；
 - 3) 设备应为可移动式柜体设备，并按照模块化、标准化、人性化原则设计。
- b) 签证/签注查询机：应包含电子往来港澳通行证、电子往来台湾通行证再次签注、证件信息读取、现场人像拍摄、银联卡支付、出入境申请表格打印、出入境记录查询等功能一体化的自助设备；
- c) 查验系统智能手机：应支持基于梅沙网开展边检业务的智能手机；
- d) 移动警务终端：应支持基于公安网开展业务的智能手机；
- e) 移动查验终端：应支持出入境业务需求证卡读取、人脸识别、四指指纹采集、电子签证、数字签名等多功能于一体的移动终端设备；
- f) 智能手持终端：应具备高清摄像头、证件读取、二维码读取、人脸识别、红外测温等其他必要信息采集功能，支持高负荷工作8 h以上，待机时长应达300 h以上；
- g) 证卡销毁设备：应具备卡表面信息识别、芯片信息读取、打孔作废、核验卡片作废等功能与一体的全自动证卡销毁设备；
- h) 应根据新建口岸类型，配置相关辅助设备，见表7。其中查验系统智能手机、移动警务终端、智能手持核验终端数量应根据口岸业务民警人数的10%配置。

表 7 相关辅助设备配置数量

口岸类型	前置采集机/自助采集机	签证/签注查询机	移动查验终端	证卡销毁	其他移动设备
I 级/大	4	10	20	10	X
II 级/中	2	5	10	5	X
III 级/小	1	2	6	2	X

12.7 登机口人脸识别系统

空港口岸登机口人脸识别系统应支持出境旅客在登机口的人脸核验比对功能，系统部署满足以下要求：

- a) 应在登机口处部署专用网络和人脸采集识别设备；
- b) 应在边检机房部署数据库服务器和应用服务器，并配套部署防火墙、网闸设备、前置服务器及文件传输、日志审计等软硬件；
- c) 系统软件应由国家移民管理局统一发布。

12.8 梯口智能管控系统

12.8.1 配置要求

配置要求包括：

- a) 应根据具体码头泊位数量进行配置，宜为 1:1 配置，配置数量满足表 8 的要求；
- b) 高速组网设备应结合现场架设环境设置点位和距离，以保证网络能高速运行。

表 8 海港口岸建设梯口智能管控系统配置数量

口岸类型	数量	单位
I 级/大	10	套
II 级/中	6	套
III 级/小	4	套

12.8.2 海港口岸梯口智能管控系统

海港口岸梯口智能管控系统满足以下要求：

- a) 应具备证件识别、人脸识别、无线通信、视频监控、条码扫描、声光报警、智能统计、行为分析等功能；
- b) 应在码头配套部署供电及网络接口；
- c) 应在后端配套部署高速无线自组网设备、网络通信设备及管理软件；高速无线自组网设备满足以下要求：
 - 1) 应具有高速组网功能，点间距离不应小于 200 m，带宽不应小于 200 Mbps；
 - 2) 应带有定向或全向天线，并具备无线分布式视频、对讲、广播、无线覆盖、智能组网等功能；
 - 3) 设备应自带电池，满负荷工作不应小于 8 h。
- d) 系统宜接入深圳边检总站指挥系统，支持视频预览、回放以及实时报警等功能；
- e) 前端设备应具备防水、防尘和防腐蚀能力；
- f) 无线通信功能应符合边检业务网络安全要求。

12.9 应急系统

12.9.1 部署要求

按照以下要求部署：

- a) 边检站技术值班室应配备一套国家移民管理局专用无线数据传输网络连接设备和专用工作站；

- b) 有旅客查验业务的每个查验场地应配备一套国家移民管理局专用无线数据传输网络连接设备和专用工作站；
- c) 各口岸应按人工查验通道数量的 20%配置笔记本（单机版），且最低数量不少于 6 台；
- d) 旅检口岸应具备独立查验能力的移动应急查验台；
- e) 移动应急查验台满足以下要求：
 - 1) 应具备集成查验工作站、应急网络连接设备、移动式监控镜头、UPS 独立供电等装备；
 - 2) 应采用便携式拉箱设计；
 - 3) 应支持指纹采集、人脸识别、个人信息采集等功能，以及其他必要生物特征信息采集功能；
 - 4) 应支持可调节摄像头、证卡读取、电子签证等多种功能；
 - 5) 应支持离线采集、物理拷贝、有线/无线实时传输；
 - 6) 应支持 SDK 二次开发等。

12.9.2 性能要求

性能满足以下要求：

- a) 4G 专用上网卡：应符合国家移民管理局无线 4G 接入标准；
- b) 4G 接入设备应包括以下内容：
 - 1) 高性能笔记本；
 - 2) 14 寸显示器以上；
 - 3) 内存大于 8 G；
 - 4) 500 G 固态硬盘以上。
- c) 笔记本（单机版）应包括以下内容：
 - 1) 高性能笔记本；
 - 2) 14 寸显示器以上；
 - 3) 内存大于 16 G；
 - 4) 1T 固态硬盘以上。

13 视频监控系统

13.1 总体要求

总体要求包括以下内容：

- a) 应采用网络高清建设方案规划建设，系统应接入国家移民管理局视频综合应用管理平台，通过设备的统一管理实现国家移民管理局、深圳边检总站、边检站三级单位对口岸限定区域的全面管控；
- b) 所有设备均运行在边检专用的视频专网内；
- c) 视频监控系统的建设应符合 GB 50395 的相关规定，并满足国家移民管理局边检机关对于视频监控系统的建设要求。

13.2 系统构成

视频监控系统主要由前端接入区（摄像机、拾音器、NVR）、核心区（硬件服务器、软件平台等）、集中存储区（CVR、EVS等）、显示设备区（LED显示屏、视频矩阵等）和网络传输设备等组成，见图12。

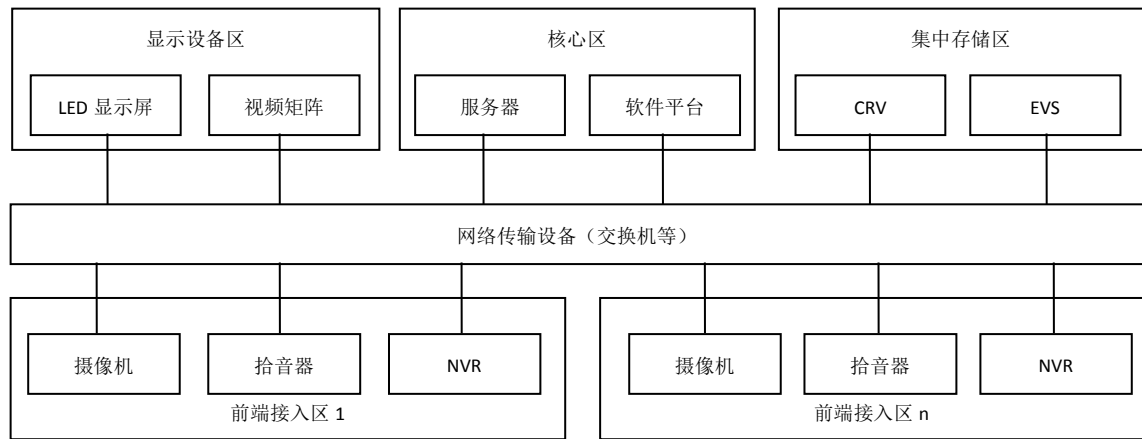


图 12 视频监控系统

13.3 功能性要求

13.3.1 一般要求

一般要求包括以下内容：

- 摄像机应按照点、线、面的覆盖要求进行布设；口岸建设单位应向边检站提供符合规范的电子地图/三维图/平面图，接入深圳边检总站视频综合应用管理平台、深圳边检指挥系统，支持布点图上可视化；
- 摄像机应支持网络高清制式，不应少于 300 万像素；
- 摄像机应满足 GA/T 1127 的相关规定，音视频传输协议应符合 GB/T 28181 的相关规定，并支持 H.264、H.265 视频编码格式；
- 摄像机应支持智能分析功能，具备根据不同场景支持前端智能检测分析功能，数据传输协议应符合 GA/T 1400.4 的相关规定，具备通过 SDK 接口上传智能分析数据的功能。

13.3.2 详细要求

13.3.2.1 前端接入区

前端接入区满足以下要求：

- 像素数量：不应少于 300 万像素；
- 帧率：不应低于 25 帧/秒；
- 视频压缩标准：应支持 H.265/H.264；
- 应具备宽动态能力；
- 叠加信息不应遮挡视频图像上重要目标和关注区域；
- 采集设备宜支持电动变焦功能，支持在线调整；
- 设备需具备校时功能；
- 截图要求：查验通道的视频采集设备，应支持通过接口实现截图功能，并保存截图至视综平台；
- 物理安全要求：采集设备防破坏能力满足以下要求：
 - 室内使用的设备，其外壳防护能力应符合 GB/T 4208—2017 中 IP20 的规定；
 - 室外使用的设备，其外壳防护能力应符合 GB/T 4208—2017 中 IP66 的规定；
 - 在沿海室外环境运行的摄像机应具备防水防腐能力；
 - 在易燃易爆等危险环境（如化工码头）下运行的摄像机设备应有防爆能力，并应符合 GB/T 3836.1 的规定。

- j) 拾音器应自带降噪功能，人声清晰；
- k) 拾音器的信噪比不应小于 70 dB；
- l) 前端存储应采用硬盘录像机，至少支持 8 盘位，本地存储时长不应少于 1 年。

13.3.2.2 核心区

核心区满足以下要求：

- a) CPU：不应低于 20 核 2.4 GHz；
- b) 内存：不应低于 128 G；
- c) 网卡：应至少含 2 个千兆网口；
- d) 硬盘：应至少不低于 2 块热插拔 1.2 T 硬盘，并构建 RAID 组（基于模式 1、5、6）提供冗余保护；
- e) 关键模块如电源、风扇，应支持热插拔并配备冗余；
- f) 宜规划 3 台服务器用于部署视综平台，最低不应少于 2 台；
- g) 所有数据口支持接入交换机，管理口宜接入交换机；
- h) 数据口应设置聚合模式，单台服务器数据口上联宜接入不同交换机。

13.3.2.3 集中存储区

集中存储区满足以下要求：

- a) 应采用视频存储阵列，所有监控点存储时长不应少于 1 年；
- b) 中心存储设备应由平台直接接管，应具备存储空间管理、视频存储计划下发、自行完成视频录像取流存储及响应平台录像片段查询、录像调阅、播放控制等功能；
- c) 集中存储阵列所用硬盘宜提供 5%冗余备件。

13.3.2.4 显示设备区

显示设备区满足以下要求：

- a) 站级单位的指挥中心应部署视频矩阵及大屏显示系统；
- b) 视频矩阵应能对接视频综合管理平台的资源，支持资源自动同步、视频解码上墙等功能；
- c) 输入口不应少于 8 路 HDMI 接口；
- d) 输出口除输出给大屏外，至少应预留 4 个 HDMI 输出口备用；
- e) 大屏应采用 LED 显示屏，室内 LED 显示屏像素中心间距不大于 2.5 mm，室外 LED 显示屏像素中心间距不大于 4.0 mm；LED 显示屏宜采用独立的拼控设备，规模与指挥中现场拟安装大屏的墙面（或横截面）匹配，大屏面积不应少于墙面（或横截面）面积的 80%。

13.4 业务要求

13.4.1 点位监控

13.4.1.1 点位监控位置

点位监控位置见表9。

表 9 点位监控位置

序号	点位监控的位置	序号	点位监控的位置
1	出入境记录凭证打印点	13	船舶梯口

表9 点位监控位置（续）

序号	点位监控的位置	序号	点位监控的位置
2	出、入境查验现场	14	咨询台
3	查验台（含船舶报检台）及通道	15	询问室
4	码头泊位（船舶内、外档）	16	监管室
5	入境检查前与出境检查后的所有出入口关键节点	17	旅客疏导处
6	出入境礼遇专办处窗口报检区	18	证件办理处
7	旅客登车登船处	19	监控室
8	工作人员通道查验点	20	值班室
9	口岸限定区域出入口	21	岗亭
10	生物信息采集点	22	填卡处
11	边检防爆设备摆放处	23	检查室
12	验讫章存放调校地	24	枪库
注：点位监控指人员及交通运输工具出入境过程中关键位置的监控。			

13.4.1.2 点位监控布设

点位监控布设满足以下要求：

- 每条人工查验通道应部署 1 个摄像机（旅客正面）；
- 每 2~4 条人工查验通道前面（检查员正面）应部署 1 个摄像机；
- 每 4~6 条旅客查验通道应部署 1 个摄像机；
- 每条车辆查验通道应部署 3 个摄像机（车牌、前后全景）；
- 每个海港泊位应部署 3 个摄像机（全景摄像机、灵活部署的梯口摄像机、船舶外档摄像机），全景摄像机光学变焦不应少于 25 倍，补光不应少于 200 m；
- 为防止断网断电导致监控失效，每个海港口岸应至少部署一套自带无线组网和电源的应急监控设备。

13.4.2 路线监控

人员及交通运输工具出入境时途经的路线监控包括以下方面：

- 人员及交通运输工具进入口岸（含深港两地的边民通道）后至离开口岸或国（边）境的沿途路线；
- 执勤人员在室内执勤场所押送监管人员或验讫章携带使用及保管的路线；
- 工作人员通道及沿线、口岸监管区的围墙围网边界及所管辖两翼地区等。

13.4.3 场所监控（特定区域的监控）

13.4.3.1 口岸限定区域管理及海港锚地管控相关场所

口岸限定区域管理及海港锚地管控相关场所包括：

- a) 人员及车辆检查场地及前后区域；
- b) 口岸管理区的公共场所；
- c) 口岸限定区域警戒巡查场所；
- d) 交通运输工具监护场所；
- e) 口岸出入口结合部；
- f) 口岸内外人员密集处；
- g) 封闭隔离场所；
- h) 港区海面；
- i) 入海口、锚地；
- j) 特殊查验场所（车体检查、行李物品、枪支弹药、外事礼遇检查）。

13.4.3.2 口岸限定区域管理及海港锚地管控技术要求

口岸限定区域管理及海港锚地管控满足以下要求：

- a) 有条件的陆路口岸、空港口岸、海港口岸，应选择制高点，安装高倍数监控云台摄像机或球机，用于监控口岸全景；
- b) 海港口岸应在制高点安装带夜视功能的远程光电摄像机，用于监控港区海域和锚地；
- c) 设备应具备全天候监控能力，满足以下要求：
 - 1) 摄像机应具备全天候监控能力，在光线不足、天气恶劣或夜间等条件下也能提供可靠的图像；
 - 2) 摄像机应具备防水、防尘和抗腐蚀等特性，以保护设备并保持稳定的性能；
注：海港口岸区域经常面临恶劣的气候条件和潮湿环境。
 - 3) 宜具备低光和红外功能。

13.4.3.3 执勤保障场所的监控

应包括以下执勤保障场所的监控：

- a) 指挥调度；
- b) 证件鉴别；
- c) 重点核查；
- d) 防疫装备装脱；
- e) 验讫章保管；
- f) 警械装备存放；
- g) 枪支弹药存放；
- h) 卡片档案存放；
- i) 收缴物品存放等。

13.4.3.4 专门办案场所和现场执法场所的监控

包括行政案件办理、违法违规嫌疑人监管、法制监督审核、遣返审查、等候处置、询问、候问、临时监管等场所的监控，并满足以下要求：

- a) 专门办案场所应按照人身安全检查、信息采集、询问、等候、辨认等流程，设置满足人身安全检查、信息采集、询问、等候等功能；
- b) 现场执法场所应在出入境边防检查执法执勤现场，设置满足当场盘问检查、出入境人员人身检查、行李物品检查以及现场办理行政案件等执法需求的功能；
- c) 执法办案场所音视频监控应独立存储。

13.4.3.5 对外窗口报检场所的监控

应包括以下对外窗口报检场所的监控：

- a) 报检中心；
- b) 办证中心；
- c) 手续办理处；
- d) 信息采集。

13.4.3.6 其他监控

其他重点场所及其他因工作开展需要设置的监控，包括为应对发生口岸闯关事件等突发事件而预设的监控镜头等。

14 报警系统

14.1 一般要求

一般要求包括以下内容：

- a) 应根据场地及具体业务需求，选择报警方式及部署相应报警系统；
- b) 应支持多种网络上传报警信息，分为有线报警和无线报警，包括如下内容：
 - 1) 至少支持以电话线作为上报方式；
 - 2) 宜支持以太网、互联网上传报警信息；
 - 3) 宜支持无线通信方式上传报警信息。
- c) 应支持通过网络获取前端主机状态并进行远程控制；
- d) 报警系统应符合 GB/T 32581 的相关规定，系统建设应符合 GB 50394 的相关规定。

14.2 有线报警模块

有线报警模块主要由报警主机、报警按钮、扩展模块、蓄电池、报警键盘等组成。

14.3 无线报警模块

无线报警模块主要由报警主机、无线报警按钮、无线转网络扩展模块、蓄电池、报警键盘等组成。

14.4 系统要求

根据边检口岸的实际场景选择适宜的报警终端，如集对讲、报警、可视摄像头于一体的报警终端，满足以下要求：

- a) 应支持键盘、WEB 多种配置方式，支持快速配置向导；
- b) 应支持键盘/遥控器平台等多种布撤防方式；
- c) 应支持一键报警功能，保证用户在危险或紧急情况下能快速求助报警；
- d) 对外观要求不高、布线方便的场所应设置有线报警；
- e) 在布线困难、对美观程度要求较高的场所宜设置无线报警；
- f) 应支持触发报警后快速建立语音和视频通信；
- g) 应具备实时感知和信息反馈功能；
- h) 终端数据应能通过相应的软件模块，通过接口协议、规定的格式要求，接入口岸指挥系统和深圳边检总站总指挥系统。

14.5 其他建设要求

14.5.1 重点人员布控预警

重点人员布控预警满足以下要求：

- a) 应具备对重点防控人员出入境行为的监测和报警功能，结合边缘采集设备采集的人脸、身份证等数据信息，比对重点人员库的特征信息，实现重点人员的及时报警；
- b) 宜形成人员报警台账记录，支持对记录的查询查看以及统计功能。

14.5.2 风险感知报警

口岸密集人群场景下，应具备基于多元传感器的风险行为智能分析和报警技术，实现可疑尾随、徘徊、翻越围栏等不少于4种人员异常行为的识别和报警。

14.5.3 短临综合流预测报警

应支持高准确率口岸综合流短临预测的智能分析及大客流、车流的报警。

14.5.4 报警信息自适应关联匹配

应具备基于异构多传感器的自适应结果关联及自动判决技术功能，构建“人、车、地、事、物、组织”等全要素多元特征时空数据资源库，实现多元特征数据与口岸通关对象间的自适应关联匹配。

14.5.5 报警事件通知和分发

报警事件通知和分发满足以下要求：

- a) 应支持可灵活配置、自定义各类报警事件的消息内容；
- b) 应具备报警流程、感知设备的配置功能，具备多感知设备的多重验证预警能力，提供更精确的报警服务；
- c) 应支持实时接收报警信息，分级分类形成报警台账；
- d) 应具备口岸区域网格化处理能力，根据区域岗位职责划分网格，实现报警信息统一分拨至报警所在的网格区域所有职责部门/人员。

15 指挥系统

15.1 总体要求

总体要求包括：

- a) 应具备应急指挥调度、组织协调、决策支持、执行能力和监督能力；
- b) 应符合一网统管、一图感知、一图可视的需求，汇聚和统计展示对讲、电话、广播、电子地图、边检查验系统、视频监控系统和和其他业务系统的相关业务数据，实现与其他业务系统的数据对接共享服务。
- c) 应兼容国产化操作系统及国产化数据库。

15.2 系统构成

指挥系统主要由各业务系统数据可视化、人员车辆设备指挥调度等功能、电子地图、定位系统、短临综合流以及第三方系统/数据接入组成；各子系统宜通过接口、网闸、边界服务器等形式接入指挥系统，见图13。

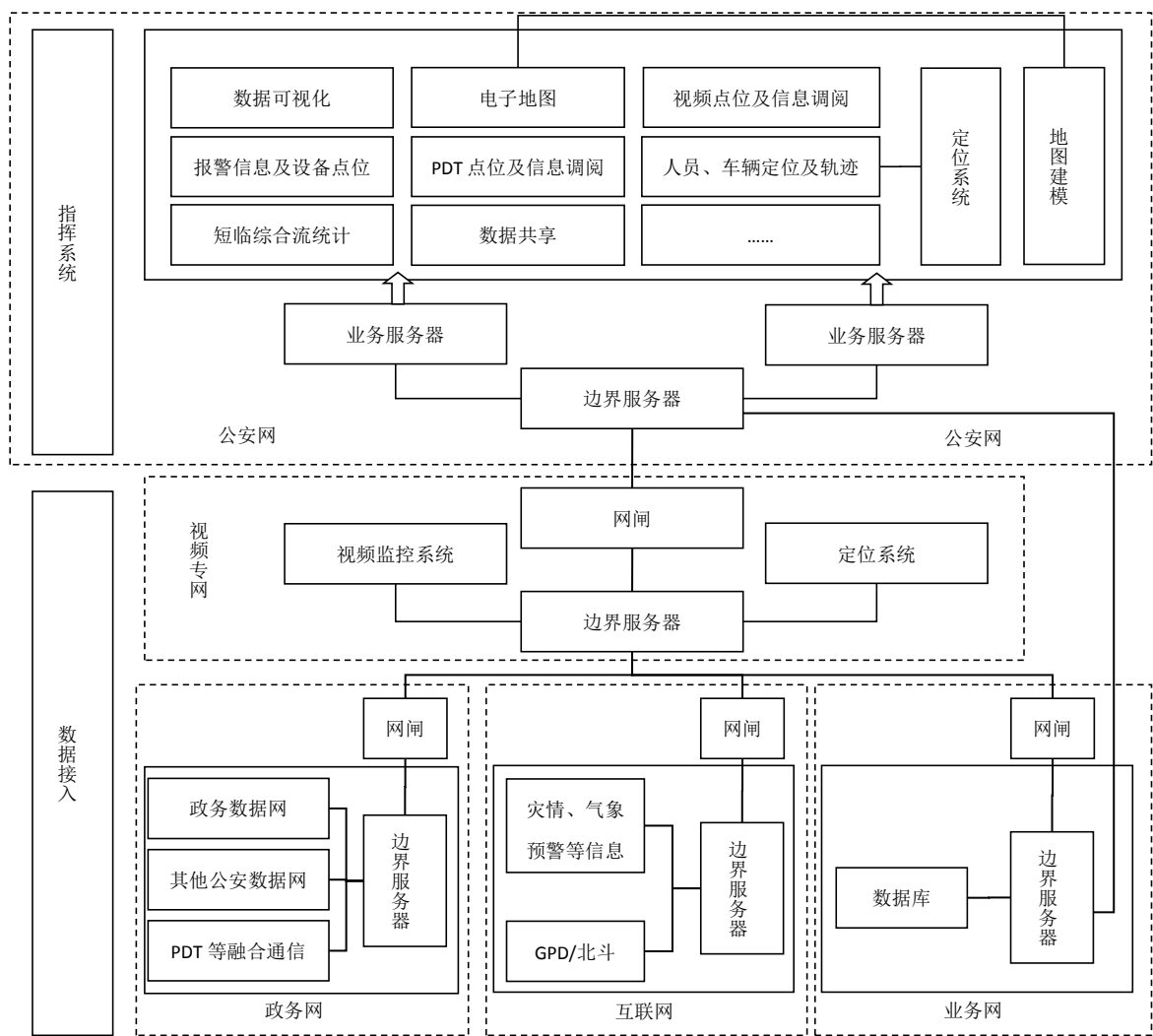


图 13 指挥系统构成示意图

15.3 数据要求

15.3.1 数据对接

数据对接满足以下要求：

- a) 在不同网络业务系统对接指挥系统时，应按照同网同接口、统一数据格式的规范将业务数据传输至指挥系统；
- b) 不同网趋向通用接口规范，满足指挥系统对接的通用性及扩展性，具体格式可由口岸指挥系统制定。

15.3.2 数据接入

应根据指挥系统的业务数据需求，满足对以下各网端的相关系统数据的接入：

- a) 监控网的视频监控系统、定位系统的相关数据的接入；
- b) 梅沙网的数据库中相关所需数据信息的接入；
- c) 政务网的数据、其他公安系统以及包括 PDT 在内的融合通信的相关所需数据的接入；
- d) 互联网的舆情、气象预警等信息以及 GPS 北斗信息的接入；

- e) 新建数据汇聚节点要与原有的数据接入能力兼容，应适配国产化操作系统及国产化数据库。

15.3.3 数据跨网传输

数据跨网传输满足以下要求：

- a) 业务网、梅沙网、政务网、互联网与公安网进行数据跨网传输，应遵守“与互联网物理隔离”的原则，通过各类数据接口、边界服务器、网闸，将数据经由视频监控外网，再传输至公安网中；
- b) 各口岸单位如涉及跨网业务，应报深圳边检总站批准，按照相关标准规范实施；
- c) 数据跨网传输应满足公安网的数据安全要求。

注：参照《中华人民共和国网络安全法》第37条、《中华人民共和国数据安全法》第31条及《中华人民共和国个人信息保护法》第40条，CII0及处理个人信息达到国家网信部门规定数量的个人信息处理者，将在境内收集和产生的个人信息和重要数据存储在境内，确需向境外提供的，通过国家网信部门组织的安全评估。

15.4 硬件要求

15.4.1 服务器要求

指挥系统应配套后端服务程序和不同类型的服务器，其核心部件CPU、内存、硬盘、电源等应满足日常业务开展要求，保证指挥系统稳定流畅运行。服务器主要性能满足以下要求：

- a) 高性能：应具备快速处理和响应各种计算任务和数据请求的能力，支持高效率处理复杂应用场景和大规模的数据；
- b) 高可靠性：应支持长时间高负载运行，具有较强的故障恢复能力，能够应对各种异常情况；
- c) 安全稳定：应具有高度的安全防护能力，能抵御各种网络攻击和安全威胁，保证数据的安全性和保密性；并应具有较高的系统稳定性，避免因安全问题而导致的系统崩溃或数据损失；
- d) 弹性扩展：应具有良好的弹性扩展能力，能根据业务需求进行灵活的升级和扩展，支持横向和纵向的扩展，满足不同阶段的应用需求；
- e) 高效管理：应具有高效的管理和运维能力，能通过集中化的管理平台进行批量管理和监控，提高管理效率和操作便捷性；
- f) 其他子系统的服务器应按照公安信息安全标准部署，并按照数据跨网传输的方法与指挥系统对接。

15.4.2 数据安全传输设备

数据安全传输设备满足以下要求：

- a) 指挥系统在跨网传输时应配套数据安全传输设备，并应按照口岸实际需求和数据量情况进行合理配置；
- b) 数据安全传输设备类型主要应包含：边界服务器、安全隔离网闸、VPN网关、边界服务器、数据摆渡机、扫码机等。

15.5 系统功能要求

系统功能满足以下要求：

- a) 应具备关键点位监控、路线监控、场所监控的布点可视化的功能，并应支持查看实时视频及历史视频；
- b) 应具备对讲系统的设备及数据进行可视化展示的功能，包括对讲设备实时位置、点对点、点对多集群对讲、信息发送等功能；

- c) 应具备报警设备可视化、实时报警信息联动以及报警区域视频联动的功能;
- d) 应根据实际业务需求对各系统相关数据信息进行统计, 并应通过图表可视化形式进行展示, 包括舆情信息、气象预警信息、预警信息等;
- e) 应基于电子地图、定位技术, 具备人员车辆的实时定位和历史轨迹可视化的功能;
- f) 应具备对短临综合流情况进行监测和标记的功能, 包括历史大客流区域、实时大客流区域、报警高发区域等;
- g) 应具备指挥中心业务子系统、数据研判中心等其他日常必要的业务功能;
- h) 应具备视频点位可视化的功能;
- i) 应具备对接一体化指挥平台的功能;
- j) 应支持本系统各类数据共享上传, 并应具备对共享数据资源进行监控的功能。

15.6 电子地图

15.6.1 地图建模要求

地图建模满足以下要求:

- a) 应根据口岸和所有涉及边检执勤场地的施工图或竣工图, 制作室内框架三维模型, 包含墙体、地板、天花、楼梯、电梯等空间白模;
注: 所有涉及边检执勤场地包括出入境大厅楼层、室外区域、船舶停靠点、过境耕作口、边境特别管理区、边检巡逻区域等。
- b) 应根据制图区域的范围及 POI 的疏密程度确定图幅的范围及比例尺, 确保主要数据清晰显示;
- c) 地图制作精度应小于 0.1 m, 室内三维地图应支持分层展示室内模型;
- d) 应支持包括摄像头、闸机、指示牌等设施设备的空间位置标定、基础信息绑定及查询展示等地图动态要素信息接口服务;
- e) 应采用轻量化方案, 主要用于 PC 端以 Web 网页访问, 基于 WebGL 绘制显示站点三维地图, 便于与现有 BS 架构的业务系统进行整合和实时交互;
- f) 应采用平面图、2.5D 或 3D 视觉效果, 平面坐标系统应采用 2000 国家大地坐标系或可与 2000 国家大地坐标系转换的坐标系;
- g) 室内地图比例尺不宜高于 1:200, 室外地图比例尺不宜高于 1:2000。口岸或场地内的主体要素发生重大变化时, 应及时提供更新的电子地图。

15.6.2 地图应用要求

地图应用满足以下要求:

- a) 可与总站总指挥系统打通, 满足对口岸模型的调取要求, 新建的电子地图应具备兼容性, 与口岸现有的平台实现无缝对接, 指挥系统与地图效果具备整体性, 统一风格样式;
- b) 应具备与报警系统、查验系统的接口对接能力, 实现要素设备数据信息的对接以及基于位置的动态信息呈现(报警信息等);
- c) 应支持室内地图和室外地图的无缝数据管理和切换, 室外地图应支持高德、谷歌等主流互联网地图厂商以及自定制的地图数据;
- d) 应支持各类电子地图交互操作, 包括 2D/3D 切换、放大缩小旋转、多楼层全部展示和切换等操作, 支持模型缓存;
- e) 应具备添加各类要素的功能, 提供地图控件服务;
- f) 地图数据安全应采用加密方式, 支持地图限制域名运行, 防止拷贝地图;
- g) 地图管理应具备二三维的地图数据加载、地图浏览、图层管理、地图查询、属性查询、地图定位等功能, 支持模型缓存。

15.7 定位系统

旅检口岸或室内场地占比达到50%以上的口岸，应基于室内三维地图及室外区域的室外电子地图搭建定位系统。

注：室外区域包括船舶停靠点、过境耕作口、边境特别管理区、边检巡逻区等。

15.7.1 定位设备

定位设备包含定位标签、室内外定位基站、后台服务器、定位标签充电器、定位标签个性化打印机，应采用 UWB 定位技术。

15.7.1.1 定位标签

定位标签满足以下要求：

- a) 接收（通信）距离不应小于 60 m；
- b) 无遮挡平均定位精度不应大于 20 CM，一般遮挡下平均定位精度不应大于 1000 px；
- c) 单次收发时间不应大于 0.7 ms；
- d) 防护等级应为 IP68；
- e) 内置充电锂电池，续航能力（UWB-1Hz）不应少于 3 个月；
- f) 接收灵敏度不应大于-100 dBm；
- g) 内置加速度计，应支持惯导模块与 UWB 信号融合定位；
- h) 电池容量不应小于 600 mah；
- i) 充电时间不应大于 1.2 h；
- j) 定位标签充电器要求：单台充电器同时支持充电标签数不应小于 10 个。

15.7.1.2 定位基站

定位基站的要求见表10。

表 10 定位基站要求

类别	具备无线通信核准证	定位精度	同步模式	接口速率	供电模式	传输间距	防护等级
室内基站	是	≤20 cm	无线同步	≥100 Mbps	标准 POE	≥100 m	—
室外基站	是	≤50 cm	无线同步	≥100 Mbps	标准 POE	≥100 m	IP67 以上

15.7.1.3 后台服务器要求

后台服务器的配置满足以下要求：

- a) CPU 不应低于 20 核 2.4 GHz；
- b) 内存不应低于 128 G；
- c) 网卡应至少含 2 个千兆网口；
- d) 硬盘不应低于 2 块热插拔 1.2T 硬盘，并构建 RAID 组（基于模式 1、5、6），提供冗余保护；
- e) 关键模块电源、风扇应支持热插拔，并应配备冗余。

15.7.2 业务要求

15.7.2.1 室内定位服务

室内定位服务满足以下要求：

- a) 室内部分应涵盖边检机关执勤的全部场地，包括出入境人员候检区、查验通道、人员完成查验至离开口岸的线路区域、卡口哨位和巡逻区域等；
- b) 室内定位服务应采用基于 UWB 协议通信的定位基站和定位终端，定位精度不应高于 20 cm。

15.7.2.2 室外定位服务

室外定位服务满足以下要求：

- a) 室外部分应包含边检机关管理的口岸限定区域；
- b) 室外定位宜采用基于 GPS 信号、5G/4G 信号或 UWB 协议通信的定位技术，对执勤人员、执勤车辆和关注交通工具等进行定位，定位精度不应低于 50 cm。

15.7.2.3 公安网接入

基于UWB协议通信的定位系统应建设于边检视频专网，GPS或5G/4G终端应按公安信息安全标准接入公安网。

15.7.2.4 系统对接

定位系统须提供后台服务程序和部署后端服务程序的服务器，并应根据深圳边检总站指挥系统架构进行数据对接。

15.7.2.5 定位数据跨网传输

数据需要跨网传输时，应同时提供符合公安信息安全标准的数据跨网传输设备。

16 会议室及会议系统

16.1 总体要求

16.1.1 会议室信息化建设总体要求包括以下内容：

- a) 应满足口岸单位日常办公会议的需要；
- b) 应满足日常工作交流讨论会、报告会、培训学习会、党委会、远程视频会等各种会议的需求；
- c) 应具有良好的会议管理、用户管理、设备管理和系统集中控制等功能。

16.1.2 每个口岸应至少配备一间会议室，会议室席位数不应少于该口岸单位编制人数的三分之一，并应根据业务需要配备相应的会议信息化设备。

16.1.3 会议室所配备的设备应支持 7×24 h 不间断运行，系统内核心设备应支持热备份能力。

16.1.4 每个口岸的会议室应配备视频会议系统，以及配套使用的显示设备和扩声设备；对于执勤点分散、距离会议室较远的场地，应配置移动式视频会议系统。

注：配置移动式视频会议系统，用于非固定场地的视频连线。

16.1.5 除视频会议系统以外的其它类型会议系统设备，宜根据口岸单位对会议应用需求和会议室建设规划选择性配置。

16.2 信息化建设组成

16.2.1 信息化建设组成见图 14。

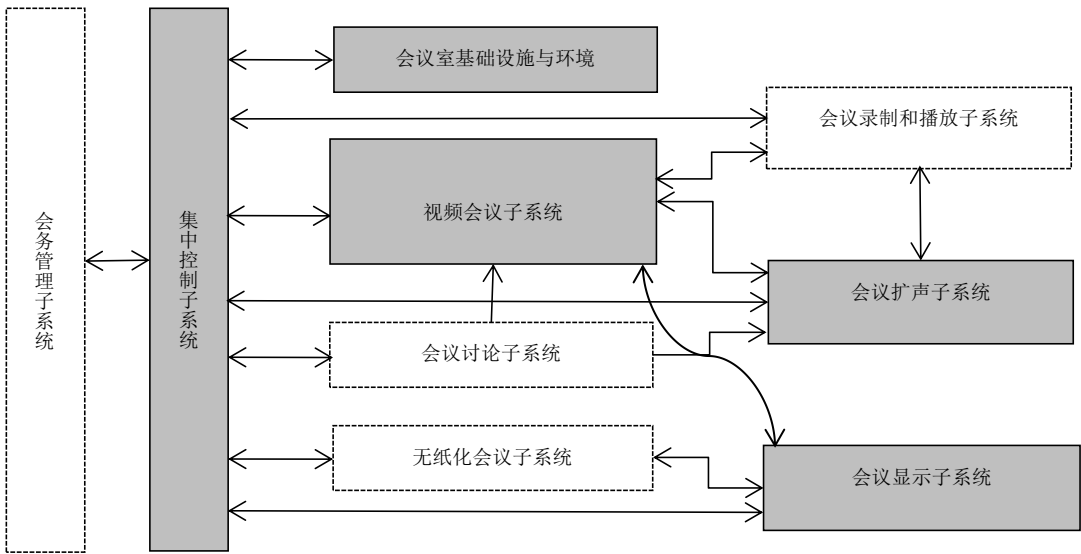


图 14 信息化建设组成示意图

16.2.2 会议室信息化是将信息技术与音视频、网络融合而成的软硬一体化会议系统，为组织会议者和参与会议者提供高效和便捷的实用会议平台。会议室信息化建设满足以下要求：

- a) 会议室基础设施与环境：主要包含会议室物理空间的装修以及空调、灯光等；
- b) 视频会议子系统：主要由视频会议 MCU、视频会议终端以及配套的摄像机、麦克风等设备组成，具备远程音、视频互联互通功能；
- c) 会议扩声子系统：一般包含音频处理器、功放、扬声器等，保证会议中音频播放应清晰、响亮；
- d) 会议显示子系统：一般包含传输路由设备、视频处理器、显示器等，支持会议中视频、图像、文字等信息显示功能；
- e) 集中控制子系统：一般由会议控制软件或集中控制系统完成，具备会议室信息化设备管理、设备控制、会议组织和会议管理等功能；
- f) 其他会议子系统：主要包括会务管理、会议讨论、无纸化会议、会议录播录制和播放等专用子系统，口岸单位宜根据会议室建设目标以及视频会议功能需求选择配备。

16.3 场地基础设施建设

16.3.1 装修环境要求

装修环境满足以下要求：

- a) 会议室温度宜为 18℃～26℃，相对湿度宜为 30%RH～80%RH；
- b) 会议室通风满足以下要求：
 - 1) 应有与室外空气直接对流的窗户、洞口或可自然通风的通风器；
 - 2) 当建筑条件不具备时，应设置机械通风设施；
 - 3) 采用自然通风的会议室，其通风开口面积不应小于会议室地板面积的 1/20。
- c) 会议室内空气质量各项指标应符合 GB/T 18883 的规定。

16.3.2 建筑声学要求

建筑声学满足以下要求：

- a) 建筑声学设计应满足语言清晰度的要求,声场环境应采取声扩散措施,应避免产生声聚焦、共振、回声、多重回声、颤动回声等缺陷;
- b) 对附着于墙体和楼板的传声源部件应采取防止结构声传播的措施;
- c) 总体噪声不应大于 40 dB(A 声级);
- d) 会议室选址应远离外界噪声干扰,无法避免时,应采取隔声和隔振措施;
- e) 会议室与相邻房间之间的空气声隔声标准不应小于 50 dB(计权标准化声压级差)

16.3.3 供电与接地要求

供电与接地满足以下要求:

- a) 对于大型和重要会议系统,其供电负荷等级应符合 GB 50052 中划分的一级负荷的规定;小、中型会议系统供电负荷等级应符合 GB 50052 中划分的二级负荷的规定;
- b) 会议室的会议系统及设备供电应采用 UPS 电源,供电不应低于 2 h;
- c) 保护地线应采用三相五线制中的地线,与交流电源的零线应严格分开,接地电阻值不应大于 4 Ω ;
- d) 位于建筑最高层的会议室,应设置浪涌保护器。

16.3.4 保密要求

口岸单位宜根据会议保密级别需求,采取相应的信息防护措施,满足以下要求:

- a) 应设置电磁屏蔽、防止电磁泄露的防护措施;
- b) 应设置防止窃听、录音的设备或设施;
- c) 会议系统数据、软件应进行加密处理;
- d) 会议室计算机系统、会议系统宜采用国产化设备。

16.3.5 会议控制室设计要求

会议控制室设计满足以下要求:

- a) 应以会议室为中心,与会议室相邻布置,宜设置在便于观察到会议室全景的位置;
- b) 环境温度宜为 18 $^{\circ}\text{C}$ ~26 $^{\circ}\text{C}$,相对湿度宜为 30 %RH~80 %RH;
- c) 消防设施不宜采用水剂喷淋装置;
- d) 宜设置双层单向透明玻璃观察窗,观察窗高度宜为 800 mm,宽度不宜小于 1200 mm,窗底距离地面宜为 900 mm;
- e) 面积、地板敷设、噪声、电磁干扰、振动、接地及装修应符合 GB 50174 的相关规定。

16.3.6 视频会议子系统

16.3.6.1 总体要求

总体要求包括:

- a) 应与深圳边检总站现有的视频会议系统相互兼容;
- b) 应依托于口岸现有公安信息网络,支持音视频会议信息互通,视频会议系统不应独立建设网络;
- c) 应支持深圳边检总站与各区口岸单位、口岸单位与口岸单位之间召开高清视频会议,分辨率应在 1080 P、帧率 30 fps 以上;
- d) 应支持 H.323、SIP 协议、H.264、H265 等视频编解码标准,以及 G.711、G.722、G.722.1.C 等音频标准;
- e) 应支持双流,且应具备单屏双显或双屏双显,主辅双流分辨率均应达到 1080 P 和 30 fps;
- f) 应支持系统设置任意会场为主会场;

- g) 带宽应支持位于 64 Kbps~8 Mbps 之间。

16.3.6.2 视频会议 MCU

视频会议MCU满足以下要求：

- a) 宜选择具有自主知识产权、稳定和成熟的国产设备；
- b) 设备架构宜采用嵌入式实时操作系统，不宜采用 Windows 等非实时操作系统；
- c) 宜支持级联控制功能，不宜少于 3 级以上的级联和控制能力。

16.3.6.3 视频会议终端

视频会议终端满足以下要求：

- a) 视频接口满足以下要求：
 - 1) 应支持不少于 3 路高清视频输入、不少于 2 路高清视频输出接口；
 - 2) 应支持 HDMI、SDI、DVI、VGA、YPbPr 中的一种或几种。
- b) 音频接口满足以下要求：
 - 1) 应支持不少于 1 路麦克风、1 路线路音频输入、不少于 1 路线路音频输出接口；
 - 2) 应支持 3.5 mm、卡侬头、RCA 中的一种或几种。
- c) 控制接口满足以下要求：
 - 1) 应支持至少 1 路用户控制接口；
 - 2) 应支持 USB、蓝牙、红外、Wi-Fi/LAN、串口中的一种或几种。
- d) 内置麦克风的会议终端应具备音频声学回声消除 AEC、声学降噪 ANS、自动增益控制 AGC 功能，能自动适应会议室声学环境，满足视频会议系统对回声消除、语音清晰、拾音范围的要求；
- e) 内置摄像机的会议终端应具备图像自动聚焦 AF、自动曝光 AE 和自动白平衡 AWB 功能，能自动适应会议室光照环境，满足视频会议系统对视频画面清晰度的要求；
- f) 内置音响的会议终端宜支持双声道。

16.3.6.4 会议摄像机

会议摄像机满足以下要求：

- a) 应与视频会议终端同一品牌或兼容使用；
- b) 应根据会场空间结构尺寸布置合理数量的摄像机，每个会议室不宜少于两台会议摄像机；
- c) 应支持图像倒转功能；
- d) 分辨率应在 1080 P、帧率 30 fps 以上；
- e) 应支持不少于 2 路视频输出接口，视频接口应支持 HDMI、SDI、DVI、VGA、YPbPr 中的一种或几种；
- f) 应具备图像自动聚焦 AF、自动曝光 AE 和自动白平衡 AWB 功能，能自动适应会议室光照环境，满足视频会议系统对视频画面清晰度的要求；
- g) 应支持 H.281 协议、预置位、PTZ 控制，预置位调用偏差不应大于 0.1° ；
- h) 应支持本地控制和远程控制；
- i) 小、中型会议室的摄像机应支持至少 5 倍以上光学变焦，大会议室的摄像机应支持 12 倍以上光学变焦；
- j) 宜搭配会议讨论系统使用，支持摄像自动跟踪，摄像机云台水平最高旋转速度不宜低于 $260^\circ/\text{s}$ ，垂直最高旋转速度不宜低于 $100^\circ/\text{s}$ ；
- k) 云台机械噪声不宜大于 50 dB。

16.3.6.5 会议麦克风

会议麦克风满足以下要求：

- a) 每台会议终端应配备至少 1 台带控制功能的全向会议麦克风；
- b) 应与视频会议终端同一品牌或兼容使用；
- c) 应支持不小于 6 m 拾音距离、360° 全向拾音；
- d) 应支持采样率 48 KHz、频响 100 Hz~20 kHz；
- e) 应支持音频声学回声消除 AEC、声学降噪 ANS、自动增益控制 AGC 功能，能自动适应会议室声学环境，满足视频会议系统对回声消除、语音清晰、拾音范围的要求；
- f) 应采用不少于 4 单元麦克风阵列，宜选用 6 单元麦克及以上的；
- g) 应具备多台级联功能；
- h) 应具有直观的工作状态指示灯和操控按键装置。

16.3.7 会议扩声子系统

会议扩声子系统满足以下要求：

- a) 应与会议室的建筑设计、建筑声学设计和其他有关工程设计专业密切配合；
- b) 应具有保证会议语音清晰度的建声设计和电声设计；
- c) 应具有计算机仿真的声学预测设计；
- d) 应满足与其他子系统的联动功能；
- e) 应符合 GB 50371 的相关规定；
- f) 扬声器应根据会议室面积和与会人员座席人数、空间高度、容积、混响时间等因素进行设计，可选择性采用集中、分散或集中分散相结合的分布方式；
- g) 应配置数字、模拟调音台或音频处理设备，其输入通道总数不应少于最大使用输入通道数；
- h) 音频处理器、调音台、功放等扩声设备应具有串口或以太网通信接口。

16.3.8 会议显示子系统

会议显示子系统满足以下要求：

- a) 功能设计应符合 GB 50464 和 GB 50635 的相关规定；
- b) 传输路由设备主要包括矩阵切换、分布式系统等设备，信号输入及输出通道应根据实际需求进行通道扩展，输出通道之间彼此独立；
- c) 视频传输路由设备满足以下要求：
 - 1) 应具有断电路由设置信息保护功能；
 - 2) 随机信噪比不应低于 60 dB；
 - 3) 微分增益不应大于 $\pm 1\%$ ，微分相位不应大于 1° ，幅频特性不应小于 $6\text{ MHz} \pm 0.5\text{ dB}$ 。
- d) 视频信号处理设备满足以下要求：
 - 1) 应能同时接受并处理多种不同视频图像信号；
 - 2) 应支持实时视频、计算机显卡信号的随意缩放、漫游、拖动、叠加等功能，画面应快速、流畅。
- e) 会议显示器满足以下要求：
 - 1) 物理分辨率不应低于会议室内视频、计算机显卡信号源分辨率；
 - 2) 屏前亮度宜高于会场环境光产生的屏前亮度 $100\text{ cd/m}^2 \sim 150\text{ cd/m}^2$ ；
 - 3) 表面应具有耐磨、抗冲击性能，屏幕抗冲击压力不应小于 90 MPa。
- f) 系统各类设备应具有串口或以太网通信接口。

16.3.9 集中控制子系统

集中控制子系统主要由中央控制主机、触摸屏、电源控制器、灯光控制器、红外发射器、音量控制器等设备组成，满足以下要求：

- a) 应具有开放式的可编程控制平台和控制逻辑，以及人性化的图形控制界面；
- b) 可根据会议室设备情况，控制管理会议室灯光、音响音量、设备电源、空调、电动窗帘等设施；
- c) 应具有场景预设存储和场景调用功能；
- d) 应具有多路控制接口，可控制 RS232/RS485 和 TCP/IP 协议设备。

16.3.10 其他会议子系统

其他会议子系统满足以下要求：

- a) 会务管理子系统：应具备会议筹备、会议室资源管理、会议召开、会议资料分发管理、会后决议执行跟进、会议设备运维管理等功能；
- b) 会议讨论子系统：中、大会议室应支持对会场发言严格秩序管理要求的会议场景，应根据会议室座席布局配置相应数量的会议讨论系统，并可根据会议室结构选择有线或无线系统；
- c) 无纸化会议子系统：应具备会议文件电子化浏览、电子书写批注、屏幕同屏共享、电子白板、电子表决等功能；
- d) 会议录播子系统：应具备会议音视频信号存储、点播、直播等功能。

17 其他辅助部分

17.1 配套系统建设

根据需要，各口岸顺畅运行应建设门禁系统、广播系统等配套系统，系统建设应根据口岸实际选择先进的技术方式，并满足以下要求：

- a) 门禁系统建设应符合不低于 GB/T 37078 中等级 3 规定的要求，人行出入口通道控制设备应符合 GA/T 1260 的相关规定；
- b) 广播系统建设应保证在口岸边检人能到达的任何区域能清晰听到广播系统的语音播报。

17.2 培训室

培训室满足以下要求：

- a) 新建口岸应配建 1 个培训室，席位不少于编制人数的四分之一，用于业务培训、业务考试；
- b) 每个席位应配备 1 台国产化电脑，配套建设教学软件、电子白板、音响设备、显示设备等。

17.3 执法记录仪和采集工作站

执法记录仪和采集工作站满足以下要求：

- a) 执法记录仪及采集工作站应能接入国家移民管理局执法记录仪管理系统，并实现所有功能；
注：执法记录仪及采集工作站遵照国家移民管理局内部对其的规范要求。
- b) 执法记录仪满足以下要求：
 - 1) 应建设执法记录仪存储和管理系统，存储容量应支持执勤民警按照一人一机配备的标准；
 - 2) 应支持拍照、录音、视频，视频清晰度应达到 4 K，内存不应小于 64 Gbps，电池应支持不间断摄录 6 h。
- c) 采集工作站满足以下要求：
 - 1) 应支持一执勤单元一台配备的标准；
 - 2) 接口不应少于 22 个，每台采集站的内部存储不应少于 32 T。

18 信息安全系统

18.1 总体要求

口岸边检信息安全整体建设满足以下要求：

- a) 建设范围应覆盖口岸边检信息化建设所涉及的各类信息系统资产、网络、应用及数据等；
- b) 系统应符合 GB/T 22239—2019 中第三级的安全要求以及 GB/T 39786—2021 中第三级密码应用的基本要求；
- c) 应加强数据安全以及个人信息安全保障能力,重点提升关键信息基础设施领域的安全水平。

18.2 物理环境安全

机房场地的建设应符合GB/T 22239—2019、GB 50174—2017的相关规定，并满足以下要求：

- a) 场地选址应充分考虑安全、自然环境、设备运输、通信和交通、管线敷设、雷电防护、结构荷载、水患及空调系统室外设备的安装位置等进行位置确定，避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区；
- b) 场地应具备出入人员访问控制、防盗窃、防破坏、防雷击、防火、防水、防潮、防静电、温湿度控制、冗余电力供应和电磁防护等安全措施。

18.3 网络安全

18.3.1 网络安全管理

网络安全管理应符合 GB/T 22239、GB/T 22080 的相关规定，并满足以下要求：

- a) 安全管理制度满足以下要求：
 - 1) 应制定网络安全工作的总体方针和安全策略，明确机构安全工作的总体目标、范围、原则和安全框架等；
 - 2) 应对安全管理活动中的各类管理内容建立安全管理制度，并定期对安全管理制度进行修订。
- b) 安全管理机构满足以下要求：
 - 1) 应设立网络安全管理工作的职能部门，设立安全负责人、系统管理员、审计管理员和安全管理员等岗位；
 - 2) 应明确各个部门和岗位的职责和授权审批流程，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。
- c) 安全人员管理满足以下要求：
 - 1) 应与被录用人员签署保密协议和岗位责任协议，加强在岗和离岗过程的权限管理；
 - 2) 应对各类人员进行安全意识教育和岗位技能培训，并制定人员考核制度。
- d) 安全建设管理满足以下要求：
 - 1) 各口岸建设信息系统时，应遵循“同步规划、同步建设、同步运行”的原则，参照上级单位相关要求，同步规划信息安全建设资金，不宜低于信息化建设总资金盘的 10%，保障口岸信息系统的安全稳定运行；
 - 2) 系统上线前应通过等级保护测评和商用密码应用安全性评估。

18.3.2 网络通信安全

网络通信安全应符合GB/T 22239—2019中8.1.2安全通信网络的规定。

18.3.3 边界区域安全

边检公安信息网、边检业务网、边检视频专网的建设应符合GB/T 22239—2019中8.1.3安全区域边界的规定，应采取边界防护、访问控制、入侵防范、恶意代码防范、安全审计等措施保证边界区域安全，并满足以下要求：

- a) 边检公安信息网、边检业务网、边检视频专网之间应相互独立、保持物理隔离；
- b) 边检公安信息网接入应严格限定在公安部允许的范围之内；
注：安全保障工作按照公安信息网相关规范及技术执行。
- c) 边检公安信息网、边检业务网、边检视频专网之间确因业务需要进行联网，应报深圳边检总站批准；并应采取安全隔离单向导入、安全边界接入平台等物理隔离手段控制安全访问。口岸边检信息资源联网安全架构见图 15。

注：参照口岸边检内部对边界安全规定相关标准规范实施。

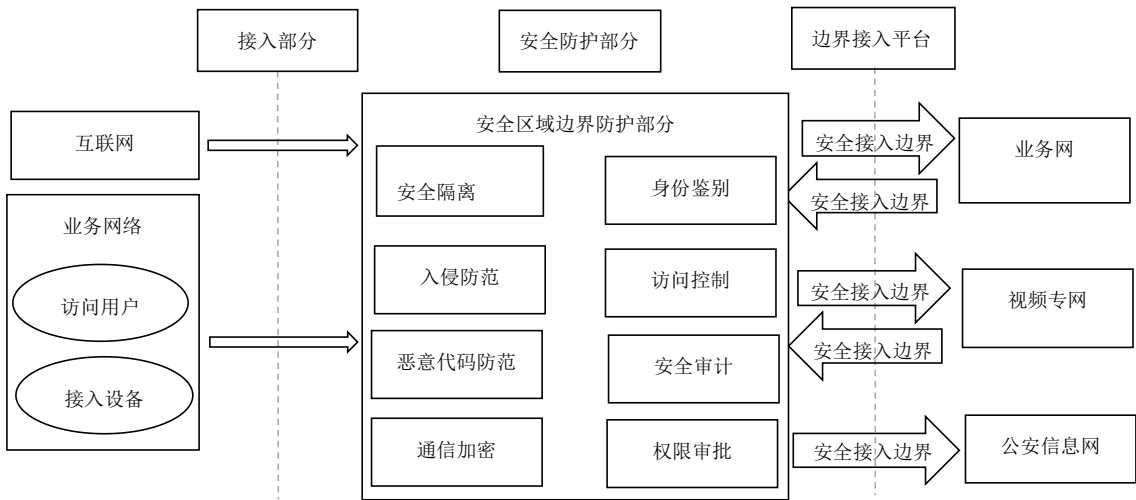


图 15 口岸边检信息资源联网安全架构示意图

18.3.4 计算环境安全

计算环境安全建设应符合GB/T 22239—2019中8.1.4安全计算环境的规定，并满足以下要求：

- a) 身份鉴别：应对登录网络、服务器、中间件、数据库、终端及应用等计算环境的用户采用密码技术身份标识和鉴别，并应设置口令强度、认证失败后锁定时间等策略；
- b) 访问控制：应对登录网络、服务器、中间件、数据库、终端及应用等计算环境的用户分配独立的账户，并应根据用户角色进行分组，按照最小必要的权限进行资源访问授权；
- c) 安全审计：应启用网络、服务器、中间件、数据库、终端及应用等计算设备安全审计功能或采用第三方审计产品，对重要的用户行为和重要安全事件进行审计。涉及重大事件的日志存储时间不应少于 12 个月；
- d) 入侵防范和恶意代码防范满足以下要求：
 - 1) 应将服务器、终端等遵循最小安装的原则，仅安装需要的组件和应用程序，并应定期开展漏洞扫描和漏洞修复工作；
 - 2) 应具备系统主动防护能力，及时识别并阻断入侵和病毒行为。

18.3.5 安全管理中心

安全管理中心的安全建设应符合GB/T 22239—2019中8.1.5安全管理中心的规定，并满足以下要求：

- a) 系统管理：应对系统管理员、审计管理员、安全管理员进行身份鉴别，只允许其分别通过特定的命令或操作界面分别进行系统资源配置、安全审计、安全策略配置操作，并应对这些操作进行审计；
- b) 集中管控满足以下要求：
 - 1) 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分析，对异常情况进行监测；
 - 2) 应使用自动化工具支持系统账户、配置、漏洞、补丁、病毒库等的管理。漏洞、补丁应在经过验证后及时修补。

18.4 数据安全

18.4.1 通则

各口岸建设信息系统时，应满足以下要求：

- a) 向深圳边检总站信息科技处申请配套数据安全体系建设，并使用商用密码技术对数据进行加密；
- b) 具备数据脱敏、数据水印、数据防泄漏、API 监测等数据安全能力，保证数据在数据采集、数据传输、数据存储、数据共享、数据使用、数据销毁的全生命周期安全可控。

18.4.2 基本要求

基本要求包括以下内容：

- a) 进行数据处理活动的基础网络环境以及承载业务数据的应用系统应具备等级保护三级安全防护能力；
- b) 在中华人民共和国境内采集和生成的各类数据应在境内存储。因业务需要，确需向境外提供的，应获得数据所有者同意，并应进行出境安全评估和审批；
注：出境安全评估和审批要遵循国家和有关部门的相关规定和技术标准。
- c) 应识别业务活动涉及的数据，形成数据保护目录，并对数据进行分级分类保护。

18.4.3 数据生命周期安全

数据生命周期安全满足以下要求：

- a) 数据采集阶段：数据采集应当遵循合法、正当、必要原则，按照法定范围和程序，明确采集数据的范围、目的和用途，规范数据格式，同时应采取必要措施，保证采集数据的真实性、准确性、时效性、完整性、可用性和可追溯性；
- b) 数据传输阶段：应采取链路冗余、密码技术、校验技术、审计技术等保证数据传输过程中机密性、完整性、可用性及可追溯性。针对重要数据应采用国家密码管理部门核准的密码技术，保证数据传输的机密性；
- c) 数据存储阶段：应根据数据安全等级采取分级分域的存储处理策略，采取必要的认证、防泄漏、加密、容灾备份等措施保证数据存储安全；
- d) 数据处理阶段：数据处理应遵循必要性和合法性，以确保数据正当使用。应保证在安全的环境下开展数据处理活动，加强对数据处理过程风险监测及处理，采取审核、脱敏、审计等手段保证数据处理阶段安全；
- e) 数据交换阶段：应在安全的环境下开展数据交换活动，数据交换过程中，应采取审核、加密、脱敏、容灾备份、审计等措施保证安全；
- f) 数据销毁：应制定数据清理和过期数据销毁流程。针对数据销毁，应采取技术手段防止溯源，且应针对数据销毁过程进行审计及记录；

18.4.4 数据安全

数据安全满足以下要求：

- a) 应加强对数据资源的安全分类分级管理，落实数据收集、存储、提供、使用等环节的安全管理责任，防范数据被泄露、滥用和篡改；
- b) 应明确数据资源管理各环节安全责任主体，建立数据安全评估机制、数据备份恢复机制、数据安全应急预案、安全责任认定机制和重大安全事件及时处置机制；
- c) 应加强对第三方技术服务单位、供应商的管理，要求其依法履行数据资源安全保护义务，防止数据资源泄露；
- d) 应当建立安全检查机制，定期检查数据资源的收集、汇聚、共享、开放、应用等情况，对发现的问题及时整改；
- e) 应针对定期组织相关人员进行应急演练，保障数据安全。

18.5 个人信息安全

18.5.1 个人信息和个人敏感信息识别

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息，满足以下要求：

- a) 个人信息的处理应包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等功能；
- b) 个人信息的识别应符合 GB/T 35273—2020 中附录 A 中的规定，个人敏感信息识别应符合 GB/T 35273—2020 中附录 B 的规定。

18.5.2 个人信息安全保障

个人信息安全保障满足以下要求：

- a) 个人信息控制者应建立适当的安全保障能力，落实必要的管理和技术措施，防止个人信息的泄露、损毁、丢失、篡改；
注：个人信息控制者的安全保障能力建设可以参照有关国家标准的要求。
- b) 应设置指导和管理个人信息保护的工作机构，明确机构的职责，配备个人信息保护专岗人员明确岗位职责，针对岗位人员的背景、专业技能等进行审查，并应签订保密协议；
- c) 应设立制定个人信息保护的总体方针和安全策略等相关规章制度和文件，包括个人信息管理操作规程、安全策略、管理制度和记录表单，并应确保个人信息管理的制度和文件执行落实；
- d) 应加强对第三方涉及个人信息处理活动的人员，如技术服务单位、供应商的管理，签订保密协议，加强第三方人员涉及个人信息过程的监督和审计，防止个人信息泄露；
- e) 应当建立安全检查机制，定期针对个人信息处理活动流程、个人信息管理制度执行、个人信息岗位人员情况进行检查，对发现的问题及时整改；
- f) 应建立健全网络安全风险评估机制，定期对个人信息处理活动进行风险评估，对发现的问题及时整改，修订完善个人信息处理活动流程。

18.6 密码应用安全

密码应用安全建设应符合 GB/T 39786—2021 中第三级密码应用的规定，并满足以下要求：

- a) 在系统规划阶段应同步设计商用密码应用方案，同步开展密码应用安全建设，并加强与等级保护建设和测评工作的衔接；

- b) 应用系统建设完成后，应委托国家密码管理部门认定的商用密码应用安全性评估机构对系统开展商用密码应用安全性评估，将应用系统通过商用密码应用安全性评估作为项目验收的必要条件；
- c) 重要业务系统应每年至少开展一次商用密码应用安全性评估。

18.7 视频安全

视频安全满足以下要求：

- a) 视频专网总体安全建设应符合 GB/T 28181、GB 35114、GA/T 1788（所有部分）和 DB4403/T 234—2022 的相关规定；
- b) 每个口岸应部署一套准入安全管控设备；服务器区应增加防火墙；访问客户端应部署具备防病毒、接口管控功能的安全系统；
- c) 应按实际需要部署视频单向传输网关设备，方便接入外单位共享镜头；
- d) 跨网平台级联应部署视频边界接入平台；
注：按照国家移民管理局边检机关对视频监控系统的建设规范要求部署视频边界接入平台。
- e) 应通过采取资产识别、资产管理、准入控制、异常告警、攻击防护、安全接入等措施保证视频专网的安全，并满足以下要求：
 - 1) 资产识别：应通过主动探测、被动监测、手工设置等方式识别和采集前端视频设备的属性信息，建立有效合法的资产库。采集信息包括但不限于 IP 地址、MAC 地址、设备厂商、设备类型、厂商视频协议等；
 - 2) 资产管理：应具有一机一档功能，能通过一机一档属性对终端进行认证，支持对一机一档属性配置不匹配的终端进行阻断和告警提示；
 - 3) 准入控制：应采用基于设备的 IP/MAC 信息、资产属性、视频协议中的一种或多种进行资产信息校验，设置准入控制策略，支持对未校验通过的设备实时生成告警信息；
 - 4) 异常告警：应采用主动探测、流量监测等技术，针对前端视频非法接入、弱口令、网中网、漏洞攻击、DDoS 攻击、病毒攻击等异常行为实时预警；
 - 5) 攻击防护：应采用旁路阻断、交换机联动阻断等有效防护方式，支持对病毒攻击、僵尸网络、蠕虫、木马、DDoS、APT 等攻击行为及时阻断；
 - 6) 安全接入：前端视频设备接入视频专网，应通过专用线路的方式或采用符合商用密码技术的虚拟专用网（VPN）技术进行链路加密通信，涉及到视频专网和其他网络之间的互联，应按照本文件中 18.3.2 的要求进行建设。

18.8 供应链安全

供应链安全满足以下要求：

- a) 应建立供应链安全管理策略，降低供应链安全风险；
- b) 采购网络关键设备和网络安全专用产品目录中的设备产品时，应采购通过国家检测认证的设备和产品；
- c) 采购、使用的网络产品和服务应通过国家相关机构的检测认证；可能影响国家安全的，应通过国家网络安全审查；
- d) 应保证产品服务的持续性，确保在产品的使用周期内，能提供稳定的原厂技术支持服务和硬件质保服务；
- e) 应自行或委托第三方网络安全服务机构对定制开发的软件进行源代码安全检测，或由供应方提供第三方网络安全服务机构出具的代码安全检测报告；

- f) 使用的网络产品和服务存在安全缺陷、漏洞等风险时，应及时采取措施消除风险隐患，涉及重大风险的应按规定向相关部门报告。

18.9 安全运营

18.9.1 安全运营建设

安全运营建设满足以下要求：

- a) 安全运营建设整体目标是持续优化网络安全能力，满足安全监管要求，保障业务持续发展；
- b) 深圳边检总站应建设统一的网络安全态势感知和应急处置平台，支持集约化安全管理，建设7×24 h集中化安全运营体系；
- c) 应配备安全专职人员，并应向深圳边检总站信息科技处报备，对新建的安全设备设计预留接口，全量接入总站一体化安全管理平台，支持安全运营和网络运维一体化。

18.9.2 业务功能

业务功能满足以下要求：

- a) 应建立安全运营制度，明确信息资产风险管理、人员日常运营、团队协作和应急响应等流程；
- b) 资产管理和风险评估：应建立资产台账，定期梳理资产清单，明确资产关联关系，对资产进行分类；
- c) 风险评估及加固：应符合 GB/T 20984—2022 和相关合规要求，定期开展风险评估活动，及时修复存在的安全问题；
- d) 安全监测及处置：应通过采集事件日志和系统网络流量的状态，实时监测网络安全风险态势，并进行深入分析，及时进行通报预警和事件处置；
- e) 应急响应：应根据 GB/T 20986—2023 进行安全事件风险级别判定是否需要进行应急处置，在判断需要处置安全事件后，对事件进行详细分析，提供事件处置建议，在事后进行复盘归档；
- f) 安全协同：应建立应急指挥协同机制，加强各个边检站之间的安全事件协同预警、协同防御能力，提高安全事件预警和处置的时效性。

19 安全防护

19.1 总体要求

总体要求包括：

- a) 应根据所处深圳市各区域的雷电灾害风险等级情况，采用等电位连接与共用接地系统的设计原则，信息化系统的防雷建设应满足 GB 50343 的相关规定；
- b) 当信息化建设场地作为独立建筑时，其建筑物的防雷应符合 GB 50057 的相关规定；
- c) 机房的防雷应满足 GB 50174 的相关规定。

19.2 防雷与接地

应防止雷击损害信息化系统及设备正常运行的影响，满足以下要求：

- a) 机房位于其建筑物内时应做防雷处理，场地应采取有效隔离和防雷保护的措施，满足不限于以下的要求：
 - 1) 机房内所有设备的金属外壳、各类金属管道、金属线槽、建筑物金属结构等必须进行等电位联结并接地；

- 2) 电子信息设备等电位联结方式应根据电子信息设备易受干扰的频率及机房的等级和规模确定,可采用 S 型、M 型或 SM 混合型;
 - 3) 采用 M 型或 SM 混合型等电位联结方式时,机房应设置等电位联结网络,网络四周应设置等电位联结带,并应通过等电位联结导体将等电位联结带就近与接地汇流排、各类金属管道、金属线槽、建筑物金属结构等进行连接;
 - 4) 等电位联结网络应采用截面积不小于 25 mm^2 的铜带或裸铜线,并应在防静电活动地板下构成边长为 $0.6\text{ m}\sim 3\text{ m}$ 的矩形网格。
- b) 各信息化系统的接地母线应采用铜导体,接地端子应有接地标识,并满足以下要求:
 - 1) 采用共用接地装置时,共用接地装置电阻值应满足各种接地最小电阻值的要求。
 - 2) 采用专用接地装置时,专用接地装置电阻值不应大于 $4\ \Omega$;安装在室外前端设备的接地电阻值不应大于 $10\ \Omega$;在高山岩石的土壤电阻率大于 $2000\ \Omega\cdot\text{m}$ 时,其接地电阻值不应大于 $20\ \Omega$ 。
 - c) 进出建筑物的电缆,在进出建筑物处应采取防雷电感应过电压、过电流的保护措施;
 - d) 重要设备应安装电涌保护器。电涌保护器接地端和防雷接地装置应作防雷等电位连接,防雷等电位连接带应采用铜导体,其截面积不应小于 16 mm^2 ;
 - e) 架空电缆吊线的两端和架空电缆线路中的金属管道应接地;
 - f) 光缆金属加强芯、架空光缆金属接续护套应接地。

19.3 机房防水

机房防水满足以下要求:

- a) 机房应防止结构渗水、墙面凝水、外部漫水;
- b) 不宜采用暖气取暖,取暖设备、空调不应漏水凝水;
- c) 与机房无关的水管不宜从机房内穿过;核心机房宜设置漏水报警系统;
- d) 采用水冷系统时,宜采用低压力的供水系统,并应采取有效的防护措施。

19.4 电磁兼容性

电磁兼容性满足以下要求:

- a) 应综合考虑现场的电磁环境、系统电磁敏感度、电磁骚扰和周边其他系统的电磁敏感度等因素;
- b) 所用设备的静电放电抗扰度、电快速瞬变脉冲群抗扰度、浪涌(冲击)抗扰度应符合信息化系统及设备相应的国家及行业标准,例如安全防范系统符合 GB/T 30148 的相关要求;
- c) 各信息化系统线缆宜单独管槽敷设,可与相同信号电压等级的其他线路合用管槽;
- d) 220 VAC 以上的供电电缆与信号传输电缆宜分开敷设,当受条件限制必须并行靠近敷设时,应采取屏蔽或隔离措施;
- e) 室内信号传输线缆、系统专用电缆宜采取屏蔽措施;
- f) 电源线进入屏蔽空间时应设置电源滤波器,控制线和信号线进入屏蔽空间时应设置信号滤波器,滤波器性能参数应符合 GB/T 50719 的要求。

20 系统运行与维护、保养

20.1 一般要求

各口岸边检的信息化系统运维保养工作满足以下要求:

- a) 各口岸信息化建设应规划和具体部署时明确要求：各信息化系统及设备、电源等提供商或厂家，应在系统及设备运行生命周期内提供售后维护和保养服务；
- b) 各口岸边检应建立信息化系统使用、管理和日常运行维护（以下简称“运维”）监督管理的规章制度，包括监控值班、值机巡检、安全保密、内部监督、运行环境检查，以及第三方运维监督管理、服务评价与考核等制度，建立系统运维管理和监督保障长效机制；
- c) 信息化建设工程竣工移交后，应根据系统竣工文件，确认各系统及设备的配置和参数，及时编制该项目系统运行维护计划；
- d) 应提供有利于系统维护保养工作开展的技术资料及清单；
- e) 应在信息化建设项目的财务预算中安排用于系统在免费维护保养期限后的专项经费；
- f) 应对自有的系统管理及使用人员进行培训，持证上岗。

20.2 运维管理平台

运维管理平台满足以下要求：

- a) 应具有对信息系统、设备、用户、网络、业务等进行综合维护管理的功能；
- b) 应支持设备信息管理、设备/软件/链路监测、质量检测、用户和日志管理；
- c) 应支持对设备接入率/在线率/完好率、故障排除率、系统链路可用率、运行维护日志完整率等指标的统计分析，并生成相应报表。

20.3 运维保养管理要求

运维保养管理满足以下要求：

- a) 应建立完善的维护保养服务体系，包括但不限于维护保养管理制度、维护保养服务规程、质量管理要求、安全生产要求等；
- b) 应建立系统设备台账，并对信息化系统和设备的全生命周期进行有效维护和管理；
- c) 应设立备品备件库，对于常见故障的设备和易损坏的材料进行储备；
- d) 应根据系统情况组建系统维护工作团队，维护工作团队应由维护服务单位、口岸边检的相关人员组成，包括维护服务单位的管理人员、技术人员、维护人员等；
- e) 应根据系统运行情况及业务管理需要，维护保养单位向口岸边检（自行开展维护保养工作时，由口岸边检自行）提出关于系统设备升级、改造的合理化建议，并应具有协助口岸边检建立、完善系统运行应急预案的能力；
- f) 应加强对系统运行维护管理人员岗前和在岗培训，熟练掌握系统设备使用、分布情况、基本操作技能、常见设备故障规律和处置技巧；
- g) 维护保养单位应与口岸边检签订相关保密协议，落实保密责任与措施；
- h) 应规范系统维护保养服务管理，包括明确的岗位设置、职责分工、值班安排，健全的维护保养服务管理制度，详实的维护、维修、保养服务记录等；
- i) 维护保养单位应具备固定的客服电话，保持每周 7×24 h 接听，处理口岸边检的技术咨询、沟通和服务支持，反馈服务信息；
- j) 日常技术咨询、技术支持等应在 2 h 内响应；应急维护响应时间不应超过 1 h；
- k) 系统或设备发生故障时，维护保养单位应在与口岸边检约定的时间内恢复系统、设备正常运行。一般情况下故障响应时间应符合下列规定：
 - 1) 一级故障：指系统崩溃导致大范围系统和设备停止运行、数据丢失等故障。接到通知，应在 0.5 h 内响应；
 - 2) 二级故障：指部分系统和设备失效、系统性能下降，但仍能运行。接到通知，应在 1 h 内响应；

- 3) 三级故障：指系统和设备报错或告警，但系统和设备能继续运行且性能不受影响。接到通知，应在 2 h 内响应。

20.4 维护保养工作程序

- 20.4.1 项目交付使用后，应及时提出维护保养需求，制定系统维护保养规划。
- 20.4.2 宜委托维护保养单位或自行开展维护保养工作。
- 20.4.3 在开展维护保养工作前，应对各信息化系统进行现场勘察，分析评估故障风险，并编制系统勘察报告。
- 20.4.4 根据各信息化系统的系统特征及运行情况，结合系统勘察报告编写维护保养方案，维护保养方案应至少包含以下内容：
- a) 维护保养对象和周期；
 - b) 系统与设备故障风险分析与评估；
 - c) 维护保养内容及要求，系统维护工作的受理、响应、回访、用户满意度调查等服务机制；
 - d) 维护保养实施组织方案、维护团队、管理制度、技术支撑系统和评价考核方法；
 - e) 维护保养备品备件配置、管理、替代方案；
 - f) 特殊时期的系统保障措施，突发事件处置预案；
 - g) 重大故障(一、二级)应急抢修预案；
 - h) 维护保养的费用预算等。
- 20.4.5 维护保养方案应经口岸边检和维护保养单位共同确认，应至少包含以下内容：
- a) 维护保养服务期限、内容要求及故障响应与维修处理时间限定；
 - b) 维护保养工程所需相关资料；
 - c) 维护所需的设备材料供应方式；
 - d) 维护保养服务验收规范；
 - e) 双方的责任、权利、义务与争议、违约及违约责任，违约处理方式；
 - f) 维护保养费用及支付方式；
 - g) 双方具体负责人的姓名、联系电话；
 - h) 保密约定。
- 20.4.6 维护保养人员应按照维护保养方案开展维护保养工作。
- 20.4.7 口岸边检应按约定周期或合同要求对维护保养工作进行验收、评价。

20.5 工作内容与要求

20.5.1 基本要求

基本要求包括以下内容：

- a) 应编制维护保养报告，定期统计系统设备的在线率和可用率；
- b) 应对系统维护的过程进行详细记录；对出现的问题，应根据维护方案要求进行处理和调整，并经相关方确认后存档；
- c) 各系统维护保养应符合维护保养方案。

20.5.2 日常巡查

日常巡查满足以下要求：

- a) 维护保养单位应定期巡查系统设备在线、运行情况，并对关键技术指标及功能运行质量进行检测。发现系统设备存在故障，应及时组织维修；

- b) 口岸边检和维护保养单位应共同做好系统设备日常巡查工作，重点巡查系统设备在线率和完好率，并做好系统设备巡查日志。

20.5.3 各信息化系统及设备的保养

各信息化系统及设备的保养满足以下要求：

- a) 应针对各信息化系统及设备的技术特征、使用场景及环境等因素，制订相应的技术保养规范；
- b) 应严格按照技术保养规范的要求对各信息化系统及设备执行保养工作，确保系统及设备处于良好的运行状态，发挥其最佳使用效果；
- c) 各信息化系统及设备的维护保养工作频次按合同要求进行，并建立维护保养记录表。

20.5.4 故障维修

故障维修满足以下要求：

- a) 应对系统和设备故障进行分级；
- b) 应优先对高等级故障进行处理；
- c) 维修或协同维修恢复后，应及时报口岸边检确认；
- d) 应对故障维修情况进行详细记录，并对故障设备后续运行情况进行跟踪，对于重大故障抢修恢复应编制故障处理报告；
- e) 应建立系统故障维修程序，并按照该程序执行；
- f) 应详细记录故障现象、故障原因、维修记录等情况。

20.6 维护评价

20.6.1 评价指标包括但不限于对系统维护工作团队维护工作质量的评价。

20.6.2 评价方法包括但不限于对所维护系统设备的现场抽检、统计系统设备的在线率和可用率以及维护管理制度的执行情况。

20.6.3 维护保养单位应根据系统维护工作情况，优化其管理制度和工作程序，并可根据监测数据、工作经验，向建设/使用单位提出系统设备的优化、改造建议。

参 考 文 献

- [1] GB/T 35273—2020 信息安全技术 个人信息安全规范
 - [2] 建标 185—2017 国家口岸查验基础设施建设标准
 - [3] 中共中央办公厅, 国务院办公厅. 国家信息化领导小组关于我国电子政务建设指导意见: 中办发〔2002〕17号. 2002年
 - [4] 中共中央办公厅, 国务院办公厅. 国家信息化领导小组关于推进国家电子政务网络建设的意见: 中办发〔2006〕18号. 2006年
 - [5] 中华人民共和国公安部. 关于推进公安信息化发展若干问题的意见: 公通字〔2017〕7号. 2017年
 - [6] 新华社. 中华人民共和国网络安全法: 第十二届全国人民代表大会常务委员会第二十四次会议. 2016年
 - [7] 新华社. 中华人民共和国数据安全法: 第十三届全国人民代表大会常务委员会第二十九次会议. 2021年
 - [8] 新华社. 中华人民共和国个人信息保护法: 第十三届全国人民代表大会常务委员会第三十次会议. 2021年
 - [9] 新华社. 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要: 2021年
 - [10] 国家移民管理局. “十四五”移民管理事业发展规划: 2021年
-