

文件编号：NT/SSD/OSSP-16231

版 本：V1.0

修订状态：新建

**国内系统方案事业部**

**毫米波集中查验**

**总体设计说明书**

**编制：**

**审核：**

**批准：**

2019-09-12发布 2019-08-18实施

版 本 历 史

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 版本 | 状态 | 作者 | 参与者 | 起止日期 | 描述 |
| V1.0 | 新建 | 张爱春 |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

状态：新建，增加，修改，删除

目录

[1 引言 5](#_Toc453078909)

[1.1 项目名称 5](#_Toc453078910)

[1.2 项目背景 5](#_Toc453078911)

[1.3 参考资料 5](#_Toc453078912)

[1.4 名词解释 5](#_Toc453078913)

[2 总体设计 5](#_Toc453078914)

[2.1 系统概述 5](#_Toc453078915)

[2.2 系统拓扑图 6](#_Toc453078916)

[2.3 基本设计思想及处理流程 6](#_Toc453078917)

[2.4 技术方案选择 6](#_Toc453078918)

[2.5 系统架构 7](#_Toc453078919)

[2.6 采购及复用分析 7](#_Toc453078920)

[2.7 人工处理过程 8](#_Toc453078921)

[3 接口设计 8](#_Toc453078922)

[3.1 外部接口描述 8](#_Toc453078923)

[3.2 内部接口描述 8](#_Toc453078924)

[4 系统数据结构和算法设计 8](#_Toc453078925)

[4.1 逻辑结构设计要点 8](#_Toc453078926)

[4.2 物理结构设计要点 9](#_Toc453078927)

[4.3 主要算法设计 9](#_Toc453078928)

[5 系统故障处理设计 9](#_Toc453078929)

[5.1 故障信息和处理措施 9](#_Toc453078930)

[6 安全保密设计 10](#_Toc453078931)

[7 系统维护设计 10](#_Toc453078932)

[8 系统可靠性设计 10](#_Toc453078933)

[9 系统可扩展性设计 10](#_Toc453078934)

[10 系统性能设计 10](#_Toc453078935)

# 引言

## 项目名称

项目名称为毫米波集中查验产品。

## 项目背景

## 参考资料

《毫米波集中查验需求模型》

## 名词解释

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名词/缩略语** | **释义** | **备注** |
| 1 |  |  |  |
| 2 |  |  |  |

# 总体设计

## 系统概述

MW1000人体安检仪，是一款新型人体安检产品，能够进行快速、非接触式检查并发现藏匿于被检人衣物之下的各种违禁品。

这款产品使用可复用多通道毫米波收发阵列，采用双面联动方式实现快速平面扫描，利用基于精确重建的近场毫米波全息成像算法和高性能硬件加速计算技术，快速得到全息毫米波图像，并通过基于深度学习的智能识别算法，自动给出被检人携带违禁品的信息。产品具有检查全面、方便、快捷、人性化等优势，且不存在电离辐射风险。

该系统提供了一套基于MW1000人体安检仪，配合该安检仪的设备端、远程判图站、手检端形成的人体安检整体解决方案，可实现快速高效的多通道分级查验。

本系统主要分为集中管理、后台服务模块。

集中管理包括图像管理、数据统计、日志管理、设备管理、黑名单管理、用户管理、维保管理等子模块；

后台服务包括图像存储、智能分发、存储空间监控、命令转发等子模块。

## 部署拓扑图



部署架构图

**部署说明：**

1. 本部署方案的设计思想：核心服务避免单点故障，提高系统的整体性能；
2. 后续部署优化内容：应用服务的集中管理、后台数据服务科根据实际需要进行分离部署，提高应用服务的性能；
3. 数据库服务器、文件服务器采用双机热备方式部署。
4. 后台数据服务与设备端、判图站、手检站之间的接口：消息通过MQ通信，文件通过FTP通信。

## 基本设计思想及处理流程

**设计思想：**

本系统根据前后台分离的设计思想，集中管理模块分为前台、后台两大子模块，前后台之间通过Restful接口和json数据结构进行交互，实现前后台的开发和部署完全分离、平台无关、技术无关等，使前后台的开发充分发挥各自的优势，进行专业分工。

后台数据服务主要负责判图任务调度、数据存储、命令转发等功能，与设备端、手检站、判图站主要通过MQ消息队列进行数据交互。

**主要处理流程:**

本系统支持多种工作模式：单机模式、联机模式，联机模式流程包括单设备端、设备端+ 判图站+ 手检站、设备端+ 判图站、设备端+ 手检站，各模式业务流程请具体如下：

1. **单机模式：**

设备端无法连接至数据服务，使用自动判图，旅客在设备端接受手检。



1. **联机模式**
   1. **单设备端：**

使用设备端自动判图，旅客在设备端扫描完成后，数据上传服务器，继续在设备端进行手检。



* 1. **设备端+远程端+手检站：**

常规集中查验工作模式，旅客在设备端扫描后，等待数据服务分配的远程端判图结果，判图结束后， 旅客到数据服务分配的手检站接受手检。



* 1. **设备端+远程端：**

旅客在设备端完成扫描后，在设备端等待，收到数据服务分配的远程端判图结果后，旅客在设备端接受手检。



* 1. **设备端+手检站：**

常见工作模式，设备端使用自动判图，旅客在设备端完成扫描后，到数据服务分配的手检站接受手检。

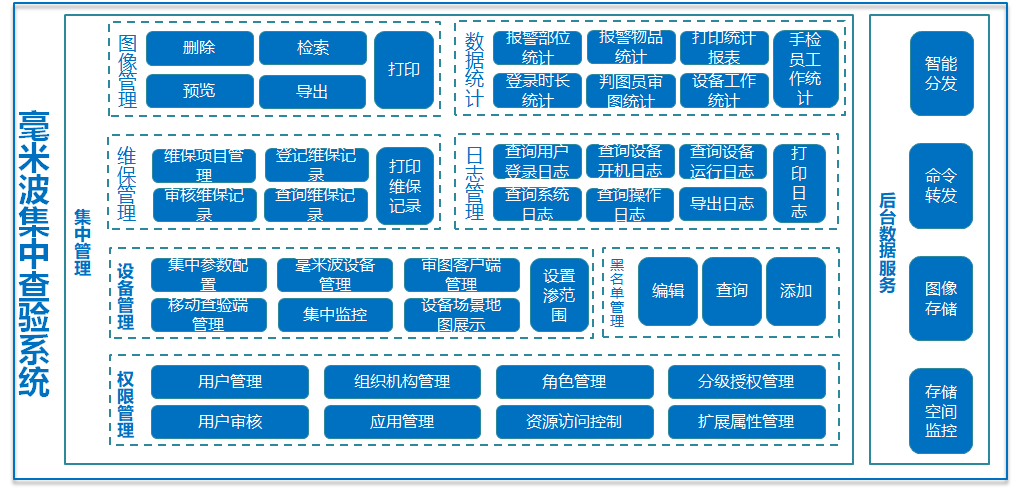


## 技术方案选择

* 采用SpringMVC+ VUE来实现前后台分离的架构
* 采用SpringMVC，容易上手，后期可根据业务的扩展平滑的过渡到微服务架构，整合到Spring Cloud系统框架下，满足产品未来的扩展需求
* 以ActiveMQ作为统一的数据总线
* 持久层用JPA方式，实现了业务与Hiberbate等其他持久层框架的解耦，便于后续持久层技术的升级或调整
* 缓存采用SpringCache，实现了业务与常见缓存技术的解耦，支持本地、远程等常用的缓存技术，如guava、redis等

## 系统架构

### 功能架构



功能架构图

### 技术架构



技术架构图

**本系统技术架构整体分为五层:**

**第一层**是数据采集层，主要负责数据的采集和预处理，采集毫米波安检门的查验图像、人脸抓拍图像、性别等信息，进行智能调度分发给相关的远程判图站或手检站，并接收远程判图站或手检站的处理结果。

**第二层**为存储层，根据各业务模块的数据分类，满足结构化、非结构化、等多种形式的数据的一定年限的存储要求：查验信息、配置信息等结构化数据存储在SQL Server数据库服务器上，查验相关的非结构化数据据存储在文件服务器上。

**第三层**是业务层，主要提供集中管理、后台数据服务相关的业务服务，配合设备、判图站、手检站完成人体查验的采集、判图、处置等服务；

**第五层**是接口层，提供基于应用需求解析出来的接口服务：图像管理、设备管理、数据统计、维保管理等业务的Rest服务；

**第六层**是应用层，提供图像管理、设备管理、数据统计、维保管理应用管理功能。

## 功能模块描述

### 集中管理

#### 图像管理

1. 删除图像

管理员可根据检索出的图片批量或单独删除。

1. 检索图像

按照设备编号、通道号、设备组、时间、判图结果、手检结果、用户检索历史图像。

1. 预览图像

根据检索条件可以单独预览选中的某一张图片的全部信息。

1. 导出图像

导出加密数据包括但不限于：原始图、原始数据、卡通图、各个节点工作人员信息、各个节点设备信息（设备型号，设备编号、位置等）、日期、判图结论、处理结论、旅客信息。

1. 打印图像

打印内容包括但不限于：卡通图、各个节点工作人员信息、各个节点设备信息（设备型号，设备编号、位置等）、日期、判图结论、处理结论、旅客信息。

1. 图像处理

图像预览时具备以下图像处理功能：图像亮度、图像对比度、图像伪彩、图像反色、图像增强、图像边缘、图像还原。

1. 图像标签管理

可以增加、删除图像标签,提供给手检站选择使用。

#### 数据统计

1. 报警部位统计

统计指定时间范围的报警中各个部位所占百分比，图表展示。

1. 报警物品统计

统计指定时间范围的报警中各物品种类所占百分比，图表展示。

1. 打印统计报表

根据不同的统计类型，输出其符合条件的全部信息。

1. 登录时长统计

统计指定多个用户指定时间范围的在线工作时间，图表展示。

1. 判图员审图统计

统计指定多个用户指定时间范围的判图总数、扣留计数、放行计数、判图时间（平均最值），图表展示。

1. 设备工作统计

统计指定多个设备指定时间范围的开机时长、扫描次数、报警次数，无效扫描次数，漏报率、误报率，图表展 示，统计时间粒度：小时、天、周、月、季度，年。

1. 手检员工作统计

统计指定多个用户指定时间范围的手检总数、查获计数、放行计数、手检时间（平均最值），图表展示。

1. 图像统计

图像统计结果分别以表格和柱状图的形式显示，其中表格具体显示：设备组、旅客总数、放行旅客数、报警旅客数、报警率；柱状图具体显示各设备组的旅客总数和报警旅客数。

1. 统计报表导出到Excel

根据不同的统计类型，导出其符合条件的全部信息。

#### 维保管理

1. 维保项目管理

基本的维护保养管理功能，主要包括：添加、编辑、删除等操作。维护保养项主要包括：维保项编号、维保名 称、描述、设备类型、设备位置、执行时间或周期、激活状态等。 维保项目类型包含：单次维保项、周期维保项。

1. 登记维保记录

维护员通过后台维保管理页面进行查询抵达指定节点，完成保养工作后，进行维保记录登记确认工作。登记内 容包括但不限于：维保人员信息（姓名、编号），维保时间，备注信息，支持上传 图片附件。

1. 审核维保记录

用户提交的维保记录，必须由管理员进行审核，审核通过后方可发布生效。

1. 查询维保记录

用户可以通过设备类型，设备编号，维保人员信息（姓名、编号），维保日期等多种组合条件，方便地查询维 保记录。

1. 打印维保记录

将目标维保记录输出到打印机或打印到文件。输出内容包括但不限于：维保项信息，维保人员信息（性名 、编 号），维保时间，备注信息，附件。

#### 日志管理

1. 查询用户登录日志

查询整个系统各节点指定用户指定时间范围的登录/ 注销记录。

1. 查询设备开机日志

查询指定设备指定时间范围的开机/ 关机记录。

1. 查询设备运行日志

查询指定设备的系统运行日志，来自设备端。

1. 查询系统日志

根据时间、节点类型、节点名称查询对应系统运行中产生的所有日志信息。来自所有节点。

1. 查询操作日志

整个系统运行过程中，用户在各个节点的所有操作活动将被记录入日志，这些操作信息可用于操作事故跟踪调查。可根据时间、节点类型、节点名称、操作员信息查询对应节点产生的所有操作日志信息。

1. 导出日志

对查询出的日志内容进行导出。

1. 打印日志

对查询出的日志内容进行打印。

#### 设备管理

1. 设备组管理
   1. 添加设备组

可以在系统中添加设备组, 添加信息包括但不限于：设备组名称、备注。默认有一个未分组的组别。

* 1. 删除设备组

支持单独设备数据删除、批量设备数据删除。删除设备组后，组内的设备进到未分组中。

* 1. 重命名设备组

支持修改组名。

1. 集中参数配置
   1. 设备端参数
      * 本机手检

配置设备端为本机手检模式。

* + - 自动识别配置

辅助识别开关- A T R 识别的嫌疑框；辅助识别等级- A T R 识别灵敏度，低中高三档；辅助识别嫌疑框颜色- A T R 识别的嫌疑框颜色；记录删除的嫌疑框开关- 是否记录判图站删除的A T R 识别嫌疑框，已删除用蓝色表示。

* + - 工作模式

0 - 单设备端，1 - 设备端+ 判图站， 2 - 设备端+ 手检站， 3 - 设备端+ 判图站+ 手检站。

* + - 模糊处理

面部模糊处理，胸部模糊处理，臀部模糊处理，腹股沟模糊处理。

* + - 设备端待机时间

设备端登陆后无操作超过此时间，退回登陆界面。

* + - 数据保存

硬盘空间扫描任务周期，磁盘空间报警，历史图像自动删除时间间隔，设备端是否保存历史图像，设备端仅保存嫌疑图。

* + - 提示声音开关

通过提示声音开关、 报警提示声音开关、站姿错误提示声音开关、开始扫描提醒声音开关、扫描过程声音开关 、扫描完成提示声音开关。

* + - 罩板校正时间

自动校正时间。

* + - 流量参数设置

可设置在一定时间内所有人体成像设备的中等和高等客流量阈值。

* 1. 审图端参数
     + 单幅图审图时间

对审图员单幅图审图时限进行设置, 超出此时间自动提交结论（放行/ 嫌疑）。

* + - 累计工作时长提醒阈值

对审图员疲劳提醒的时间阈值设置。

* 1. 手检站参数
     + 累计工作时长提醒阈值

对手检员疲劳提醒的时间阈值设置。

* 1. 后台数据服务
     + 存储空间阈值

设置磁盘剩余空间不足预警阈值。

* + - 跳过黑名单图检任务

对于黑名单审图任务在进行调度审图端时是否直接跳过审图流程, 直接提交手检站手检。

* + - 图像存储方式配置

数据保存形式可以灵活配置：不存储、卡通图、裸图（jpg）、原始数据。

1. 毫米波设备管理
   1. 添加毫米波设备

可以在系统中添加毫米波设备, 添加信息包括但不限于：设备型号、设备编号、设备描述、设备I P 、通道、设备 组别、备注。

* 1. 编辑毫米波设备

可以在系统中编辑毫米波设备, 可编辑信息包括但不限于：设备描述、设备I P 、通道、设备组别、备注。

* 1. 删除毫米波设备

支持单独设备数据删除、批量设备数据删除。

1. 审图客户端管理
   1. 添加审图客户端

可以在系统中添加审图客户端, 添加信息包括但不限于：设备型号、设备编号、设备描述、设备I P 、备注。

* 1. 编辑审图客户端

可以在系统中编辑审图客户端, 可编辑信息包括但不限于：设备描述、设备I P 、备注。

* 1. 删除审图客户端

支持单独审图客户端数据删除、批量审图客户端数据删除。

1. 移动查验端管理
   1. 添加移动查验端

可以在系统中添加手检站客户端, 添加信息包括但不限于：设备型号、设备编号、设备描述、设备I P 、备注。

* 1. 编辑移动查验端

可以在系统中编辑手检站客户端, 可编辑信息包括但不限于：设备描述、设备I P 、备注。

* 1. 删除移动查验端

支持单独移动查验端数据删除、批量移动查验端数据删除。

1. 集中监控
   1. 卡片式显示所有毫米波设备

小卡片显示所有设备（设备名、位置、组别、用户、状态（故障状态），以不同颜色区分高中低流量）

* 1. 卡片式显示所有审图客户端

小卡片显示所有审图客户端（设备名、用户、状态（故障状态），以不同颜色区分高中低流量）

* 1. 卡片式显示所有移动查验端

小卡片显示所有手检站客户端（设备名、用户、状态（故障状态），以不同颜色区分高中低流量）

#### 黑名单管理

1. 编辑黑名单人员

通过人员信息（姓名、身份证号、性别）、录入日期、查验等级查询、激活状态。

1. 查询黑名单人员

对被查获的人员进行黑名单信息录入，信息包括单不限于：人员信息（姓名、身份证号、人脸图像等）、查验 等级，激活状态。

1. 添加黑名单人员

可以修改指定黑名单人员的查验等级及激活状态。

#### 调度策略管理

能直观显示所以节点关系，并且可以编辑，同时可以配置调度相关的一些其他参数（比如男/女，超时提交什么结论等）

#### 权限管理

复用UPMS公共模块，具体实现内容见UPMS相关文档。

##### 用户信息导出

可以导出用户信息到Excel。

##### 打印用户

可以打印选中的用户的全部信息。

##### 用户快速定位

快速定位栏里输入英文或数字关键词，将自动筛选出用户名、用户描述、用户角色或部门中包含所输入关键词的用户，并以当前用户列表的排序情况进行排序。输入中文并点击空格键/回车键功能也相同。

##### 角色权限配置

**角色权限做到可自由配置配置项可分为：**

1. 图像管理子功能使用权限
2. 数据统计子功能使用权限
3. 日志管理子功能使用权限
4. 设备管理子功能使用权限
5. 黑名单子功能使用权限
6. 用户管理子功能使用权限
7. 维保管理子功能使用权限
8. 设备端使用权限
9. 手检端使用权限
10. 判图站使用权限

**角色默认权限：**

1. 设备引导员- 设备端使用权限
2. 手检员- 手检端使用权限
3. 判图员- 判图站使用权限
4. 管理员- 集中管理软件使用权限
5. 维保员- 维保登记功能使用权限

##### 角色管理

默认角色有：设备引导员、审图员、手检员、管理员、维保员。

##### 帐号管理

帐号信息包括：登录名字、姓、名、性别、 电话、邮箱、密码、用户组、状态等。

### 后台数据服务

#### 图像存储

图像存储时间不少于半年；

图像存储可配置为四种模式：不存储、卡通图、裸图(jpg)、原始数据。

#### 命令转发

#### 智能分发

扫描设备与远程判图站客户端允许多对多关系，判图任务派发具有智能分发机制。

#### 存储监控监控

磁盘空间不足时进行图像导出提醒，磁盘空间不足时自动循环删除。

#### 第三方系统集成

预先设计对外接口。

## 采购及复用分析

复用及采购准则：为了更好得分享项目经验，组件/模块要尽可能复用，做到标准化，参考《系统方案事业部可复用标准组件及模块清单》，如果能全部复用的直接全部复用，可以部分复用的则部分复用。为了节省成本，不允许做重复开发。基于工期和成本考虑，如果采购更合适，可以做采购。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **模块名称** | **部分复用/全部复用/采购** | **原因分析** | **备注** |
| **1** | 权限管理 | 全部复用 | 提供用户、角色等权限管理的功能 |  |
| **2** |  |  |  |  |
| **3** |  |  |  |  |
| **4** |  |  |  |  |
| **5** |  |  |  |  |

## 人工处理过程

# 接口设计

## 外部接口描述

### 与设备端接口

1. 图像上传：
   1. 接口类型：FTPS/MQ
   2. 接口描述：首先，设备扫描完成后无论扫描是否有效都将图像通过FTPS上传至后台服务端（图像、人脸等文件）；其次把上传的文件路径以及查验人性别等信息通过MQ上传到后台服务器，后台数据服务器把相关查验信息保存到关系数据库，并返回是否保存成功（成功返回数据id）。
2. 判图任务调度：
   1. 接口类型：MQ
   2. 接口描述：按照任务智能分配的调度策略，选择一个空闲的判图站或手检站（若没有空闲的，则默认选择设备端，即地手检站），发送一条判图任务的消息
3. 判图结果推送：
   1. 接口类型：FTPS/MQ
   2. 接口描述：把判图结果（文字结论、相关图片URL等）推送到设备端
4. 查验数同步：
   1. 接口类型：FTPS/MQ
   2. 接口描述：把脱机的查验数据、判图结果、手检结果等相关数据批量保存到后台服务器

### 与远程判图站接口

1. 判图任务通知：
   1. 接口类型：MQ
   2. 接口描述：推送查验任务的通知消息到判图站（查验数据id）
2. 查验数据获取：
   1. 接口类型：FTPS/MQ
   2. 接口描述：先根据查验数据ID查询需要审图的相关数据（图片、性别、数据ID，图片是文件URL），再从FTP服务器下载相关图像文件
3. 判图结果保存：
   1. 接口类型：FTPS/MQ
   2. 接口描述：首先把相关图片结论文件FTP到服务器，再把文字结论等信息保存到后台服务器，并与查验数据相关联

### 与手检站接口

1. 判图结果保存：
   1. 接口类型：FTPS/MQ
   2. 接口描述：首先把相关拍照记录的照片文件FTP到服务器，再把反馈结论（放行/扣留）、文字备注等信息保存到后台服务器，并与查验数据相关联
2. 判图任务推送：
   1. 接口类型：FTPS/MQ
   2. 接口描述：推送判图任务（查验数据ID、卡通图，判图结论，人脸图片，查验等级，图像编号、性别等，图片是文件URL）到手检站

## 内部接口描述

**集中管理前后台之间的交互接口，采用Restful方式**：

1. 图像管理：提供图像的增删改查，以及导出、打印等功能
2. 数据统计：提供报警部位统计、报警物品统计、登录时长统计等功能
3. 维保管理：提供维保项目的登记、审核、查询等功能
4. 日志管理：提供登录日志、运行日志、操作日志、系统日志等管理功能
5. 设备管理：提供参数配置、集中管理、设备管理等功能
6. 黑名单管理：提供黑名单的增删改查等功能
7. 权限管理：提供用户、角色、权限等管理功能

# 系统数据结构和算法设计

## 逻辑结构设计要点

### 集中管理子系统

主要是设备管理、数据统计、日志管理、维保管理等相关数据表，权限管理数据库的设计参见用户权限管理模块UPMS。

### 后台数据服务子系统

本子系统主要是读写集中管理维护的相关配置库表，自身暂无数据库表。

## 物理结构设计要点

### 数据分布设计

* 因为各子系统中数据库的访问压力均不大，因此所有子系统中的数据库均建立在同一台物理服务器上面（双机热备）;
* 所有图片，文件等数据都保存在同一个文件服务器上面（双机热备）;

### 安全模式设计

#### 系统安全设计

* SQL Server
  + 操作系统级别: 对于SQL Server数据库，建议采用WINDOWS认证模式以提高系统的安全性, 即使用Windows账号及登录机制。在这种情况下，需要保留NT AUTHORITY\NETWORK SERVICE和NT AUTHORITY\SYSTEM这两个默认账户来分别支持网络及本地登录过程；
  + 服务器级别:
    - 在数据库服务器级别，因为超级用户SA拥有所有操作权力并无法删除，应将密码设置尽可能复杂，并应由数据库管理员妥善保管；
    - 应为客户的数据库管理员创建一个属于sysadmin级别的本地管理员账户如”ADMIN”，直接使用默认账户BUILTIN/administrator并由对方系统管理员设定密码；
    - 另外，应另外创建一个属于sysadmin级别的本地管理员账户，例如”NUCTECH\_MAINTENANCE”, 由系统维护人员或者开发人员保存密码并使用；
  + 数据库级别:
    - 在数据库级别，因为dbo用户拥有数据库的超级权限，同样建议将密码设置尽可能复杂，并由数据库管理员妥善保管；
    - 不建议启用默认建立的guest用户。相反，应建立一个数据库的日常使用账户，如”DB\_QUERY”，此账户应对数据库只有查询权限但没有修改权限；
    - 系统使用应用程序角色来访问数据库；

#### 数据安全设计

系统采用权限管理来保证数据安全。

## 主要算法设计

### 智能分发的调度策略

**调度策略：**

调度策略主要考虑三条因素：节点关系（分组）、男/女性别、空闲/非空闲。，当设备端扫描完成后，调度服务在节点关系内根据被检旅客性别，根据配置的性别策略（**男查男，女查女、女查全部等**）选择空闲的远程判图站和手检站。当有多个符合条件的选项时，**随机分配**一个。

注意：在工作模式（设备-远程-手检）和（设备-手检）下，设备端可以配置为本地手检模式，此时设备端同时作为手检站使用，在无可用手检站情况下，通知设备端有手检任务，收到设备端可用反馈后，集中查验手检站调度服务可以将手检任务分配到该设备端。在此期间，如果手检任务已经分发到其他手检站，需要通知该设备端任务取消。

远程判图站获取图像为请求模式，手检站图像由集中查验服务推送。

以下图为例，中间为毫米波设备，左侧为手检站，右侧为远程判图站。将三台毫米波设备分为三组，每一组各对应数台手检站和数台远程判图站。当AM\_2扫描一个女性旅客后，调度策略需要在R\_2和R\_4当中选择空闲的远程判图站，如果R\_2和R\_4都空闲，则随机从R\_2和R\_4中选取一个。手检站则需要从PAD\_2和PAD\_4中选取，方式同理。



# 系统故障处理设计

## 故障信息和处理措施

### 故障编码规则

|  |  |  |  |
| --- | --- | --- | --- |
| **故障分类** | **故障信息记录方法** | **解决方案** | **备注** |
| RUN0001 | 服务响应超时 | 弹窗提示服务响应超时 |  |
| SYS0001 | 数据新增失败 | 消息栏提示数据新增失败 |  |
| SYS0002 | 页面不存在 | 跳转异常页面，提示页面不存在 |  |

**故障分类代码缩写：**

* 系统故障：SYS，是指系统内部服务相关的故障，如数据基本操作异常（增删改查）等
* 运行故障：RUN，是指系统运行相关的故障，如服务响应超时、数据库连接池已满等
* 网络故障：NET，是指网络通信相关的故障，如网络连接超时，队列数据发送失败等

**异常编码规则：**

故障分类代码缩写+四位数字编号

### 故障处理要求

通过异常处理，我们可以对用户在程序中的非法输入或者使用进行控制和提示，以防程序崩溃

**异常处理的主要原则如下：**

* 优先模块内处理解决
* 其次是异常转换为容易理解的信息并抛出
* 重新抛出异常
* 不捕获异常：并不是无视异常，而是流程需要交由上层进行捕获处理

**异常处理要求：**

* 捕获了异常就一定要处理
* 尽量进行特定异常处理，不同异常会有不同的处理方式与流程，防止异常改变了正常的处理流程
* 异常中处理好资源释放，保证所有资源都被正确释放，防止资源泄露（内存、数据库连接等）：可与finally结合处理
* 异常需要输出日志时，要提供适量的错误原因信息，以及其他辅助信息等，组织错误信息使其易于理解和阅读，有助于解决问题时了解异常发生时的情况
* 尽量减小try块的体积：全面考虑可能出现的异常以及这些异常对执行流程的影响，有利于分析程序异常的原因，也要防止程序的崩溃

# 安全保密设计

**本系统安全保密设计：**

* 完整性

系统对于关键信息进行加密存储（含数据库敏感信息、配置里的敏感信息）、加密传递（对于所有经外网传输的通信都采用安全协议如Https和FTPS），保障信息存储、信息传递的完整性，如用户密码不能明文保存，通过加密方式存储到数据库。

* 可用性

系统采用应用服务器、数据库服务器的集群部署方案，以保障系统的不间断服务能力。

* 真实性

系统采用实体鉴别（身份认证）和信息源鉴别技术来保证信息的真实性。

* 可控性

系统采用用户授权机制来控制用户能访问的功能和数据，最小授权原则，保证系统使用的严格可控。

* 可审查性

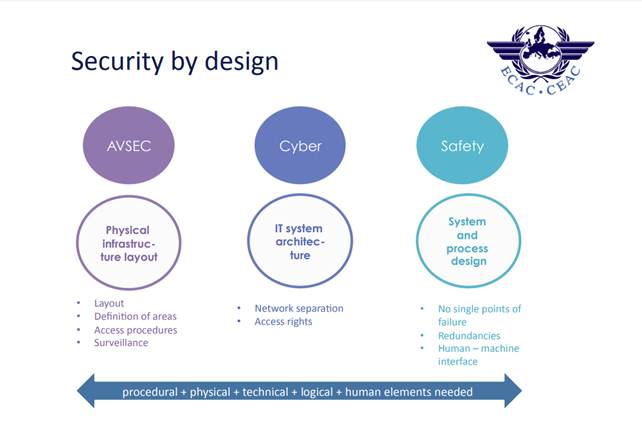
系统采用日志记录方式，记录所有的引起数据改变的业务操作，以保障所有事件的可追溯性，可审查性。

* 容错性

系统在遇到网络故障时各节点需能做出应对,尽量保证业务继续运行并在恢复后将数据同步。某节点出现异常时当前正在进行的任务应能够转移至其他节点，从而保证业务能正常运行。

**网络安全设计：**

参考欧洲民航的Cyber Security（网络安全）相关的东西，系统必须合规。网上部分资料，大致如下图：



# 系统维护设计

* 模块化设计

集中管理前、后台独立部署，后台数据服务模块也可以独立部署，也可集成部署。

* 参数配置

针对不同客户对于参数可能存在不同定义的情况，可通过系统业务参数配置功能定制，从而达到不修改程序的前提下满足客户的个性化需要。

* 系统审计

操作人员所做的任何引起数据变化的操作，在系统中都会被详细记录，具有相应权限的人可以跟踪、统计每一个操作人员在系统中的操作，监控系统是否被合法使用。

# 系统可靠性设计

**数据传输可靠性：**

* 从MQ收到的消息先放到到远程缓存（处理完毕后清除），防止当前模块的异常造成的数据丢失

**运行稳定性：**

* 数据库服务、文件服务器均采用双机策略
* 反向代理、系统应用服务均采用集群策略

# 系统可扩展性设计

* 接口化设计

采用面向接口的编程思想，来降低模块之间的耦合度

* 插件化设计

功能设计上，充分利用插件化设计思想，使程序功能可以自由拼装组合。通用功能插件尽量避免对其它插件的依赖

* 模块化设计

要求在系统设计时，要遵循模块化设计原则，合理地划分功能模块，有效地组织程序结构。模块与模块之间的交互抽象为接口之间的交互，要有效降低模块之间的耦合度

* RESTful

对于客户端和服务器交互类的软件，遵顼RESTful原则

* 支持离线工作模式

当集中查验系统故障时系统可以暂时切换为离线以，并可以在查验系统恢复后同步故障期间的缓存数据

* 灵活部署

支持多种工作模式：

* + 单机模式
  + 联机模式：1 .单设备端；2 .设备端+ 判图站+ 手检站；3 .设备端+ 判图站；4 .设备端+ 手检站

# 系统性能设计

本系统性能设计要求：

* 常用操作无明显延迟感

常规操作响应时间不超过1秒，网络操作响应时间不超过2秒，数据库操作响应时间不超过7秒。

* 高稳定性

4 0 年中故障停机时间不超过2小时。

* 其他要求

集中审图允许接入毫米波设备要大于等于200台，扫描完成调度加传输时间小于等于1秒。

