基于数据源动态配置与硬件安全管控的智能航班信息显示系统设计与实现

潘光绪、徐其涛、邓茂伟、陈张浩然

民航成都电子技术有限责任公司 611430

摘 要：航班信息显示系统（Flight Information Display System, FIDS）作为机场旅客服务与运营管理的核心支撑系统，其传统架构普遍存在显示模板固定、字段修改依赖系统升级、扩展成本高且效率低等问题；同时，安装于机场公共区的 FIDS 终端因缺乏现场监管，易被不法分子通过硬件接口（网口、USB 口等）植入违禁内容，造成安全风险。针对上述缺陷，本文提出一种基于数据源动态配置与硬件安全管控的智能 FIDS 设计方案。该方案在无需修改源代码的前提下，通过数据库与配置文件构建多类型数据源，结合数据规则与终端模板绑定实现航班信息动态展示；同时新增硬件接口管理、非法操作识别监管、远程控制模块，对网口、USB 口等硬件接口进行权限管控，实时识别违禁内容与非法操作，并支持远程指令下发与电源控制。实验与应用表明，该系统不仅将字段更新响应时间从传统方案的数天缩短至分钟级，还实现了公共区 FIDS 终端的全时段安全监管，违禁内容识别准确率达 99.5% 以上，远程控制响应时间小于 10 秒，为机场智慧化运营提供高效且安全的技术支撑。

关键词：航班信息显示系统；数据源动态配置；硬件安全管控；非法操作识别；远程控制；智慧机场

1 引言

随着民航业的快速发展，机场旅客吞吐量持续增长，旅客对航班信息的及时性、完整性与个性化需求日益提升，同时机场运营管理对航班信息显示系统（FIDS）的灵活性、扩展性与安全性提出了更高要求[1]。传统 FIDS 采用固定模板架构，显示字段（如航司 LOGO、航班号、起飞时间、登机口等）通过网页文件或组件组合预先定义，字段修改需依赖系统源代码升级，导致维护成本高、响应效率低[2]；更关键的是，机场公共区（如出发大厅、换乘通道）的 FIDS 终端多处于无现场监管状态，其网口、USB 口等硬件接口缺乏权限管控，不法分子可能通过接入外部设备植入违禁文字、图片或视频，干扰机场正常运营秩序，甚至引发公共安全事件[3]。

现有研究中，李建等提出基于 B/S 架构的 FIDS 设计，通过 Web 端实现模板轻量化调整，但未解决字段修改依赖代码编译与硬件接口安全问题；王颖等引入模块化思想提升系统可维护性，却未涉及公共区终端的安全监管；赵亮等 探索了智慧机场多业务数据集成技术，但未针对硬件接口管控与违禁内容识别提出解决方案。为此，本文设计一种融合数据源动态配置与硬件安全管控的智能 FIDS，在实现显示字段灵活调整的基础上，通过硬件接口管理、非法操作识别与远程控制模块，构建 “动态扩展 + 安全防护” 双重体系，解决传统系统的固有缺陷与安全风险。

2 传统航班信息显示系统的缺陷与安全风险分析

2.1 传统 FIDS 的功能缺陷

传统 FIDS 的核心缺陷源于 “模板 - 代码” 强耦合架构，具体表现为：

显示模板固定，字段修改成本高：显示字段通过硬编码定义，新增 “共享航班”“经停站” 等字段需修改前后端代码并重新部署，某中型机场新增单个字段平均周期达 3-5 天，直接成本超万元 ；

业务扩展能力弱：仅支持固定格式航班数据，集成天气、交通等非航班数据需定制化开发，易导致系统架构臃肿 ；

维护效率低：字段修改依赖专业开发人员，运维人员无法自主操作，需求响应存在 “断层。

2.2 传统 FIDS 的安全风险

机场公共区 FIDS 终端的安全风险主要集中于硬件接口与内容管控，具体包括：

硬件接口无权限管控：网口、USB 口处于默认开放状态，不法分子可通过 USB 接入存储设备植入违禁内容，或通过网口远程入侵终端系统 ；

非法操作难以识别：缺乏实时监控机制，无法及时发现终端的异常操作（如外部设备接入、非授权文件传输、显示内容篡改），往往在违禁内容播放后才能被动处置；

应急响应能力不足：终端故障或出现安全事件时，需运维人员现场处置，响应时间长达数小时，无法快速遏制风险扩散 。

3 智能航班信息显示系统的设计方案

3.1 系统总体架构

智能 FIDS 采用“数据源层－数据规则层－终端模板层－安全管控层”四层架构， 总体架构如图 1 所示（图略）。其中：

数据源层：通过数据库与配置文件构建多类型数据源，实现显示字段灵活配置；

数据规则层：定义数据查询逻辑，完成过滤、排序与组合；

终端模板层：通过可视化控件设计，实现数据规则与模板绑定；

安全管控层：包含硬件接口管理、非法操作识别、远程控制模块，实现终端全时段安全监管。

四层架构相互独立，支持功能扩展与安全防护。

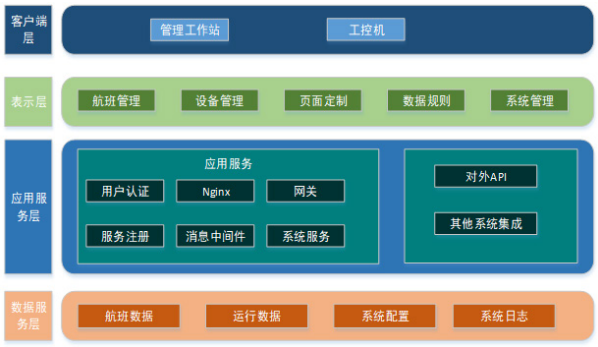

图 1

3.2 数据源动态配置设计

数据源通过数据库与 XML 配置文件结合，实现显示字段可配置化：

3.2.1 数据需求分析与表结构设计

收集机场各区域显示需求（如出发大厅需显示航司 LOGO、航班号、共享航班等，行李提取区需显示行李转盘、延误原因等），设计单表或多表关联结构（如“航班基础表”与“共享航班表”通过航班号关联），确保数据存储规范性 [4]。

3.2.2 数据源配置要素定义

XML 配置文件包含五大核心要素包含数据来源、数据提供器、元数据列、子查询、复杂查询五大要素。

3.2.3 多业务数据源扩展

支持天气、交通等非航班数据源配置，例如天气数据源关联 “实时天气表”，配置 “温度 + 风力”组合显示（如 “25℃ 西北风 3 级”），实现多数据类型集成 [5]。

3.3 硬件安全管控设计

硬件安全管控层是系统安全防护的核心，针对公共区终端的硬件接口与操作行为，设计三大模块：

3.3.1 硬件接口管理模块

接口权限配置：通过终端嵌入式系统，对网口、USB 口等硬件接口设置 “白名单” 权限。例如，USB 口仅允许接入机场运维专用设备（通过设备 SN 码认证），禁止外部未知设备接入；网口仅允许与机场内网通信，屏蔽外部网络连接请求 [6]；

接口状态监控：实时采集接口状态数据（如 USB 设备接入 / 拔出、网口连接状态），并上传至系统管理平台，平台以可视化界面展示各终端接口状态，异常状态（如未知 USB 设备接入）触发红色告警；

接口操作日志：记录所有接口操作（如接入设备型号、接入时间、数据传输量），日志保留 90 天以上，支持追溯查询。

3.3.2 非法操作识别模块

违禁内容识别：采用 “规则匹配 + AI 算法” 双重识别机制。规则匹配层预设违禁关键词库（如敏感文字、非法标识）与图片特征库（如违禁图像哈希值）；AI 算法层基于深度学习模型（如 CNN+LSTM），对终端显示的文字、图片、视频进行实时分析，识别违禁内容 [7]。例如，对视频流按每秒 2 帧的频率截取画面，与特征库比对，识别准确率达 99.5% 以上；

异常操作识别：定义非法操作行为库，包括：未知 USB 设备接入、非授权文件写入（如向终端存储写入 .exe/.mp4 文件）、显示内容异常篡改（如航班信息被替换为无关文字）、网口异常数据传输（如大量数据包向外部 IP 发送）。系统实时监测终端操作行为，一旦匹配非法操作特征，立即触发告警；

告警分级处置：将告警分为三级：一级（紧急，如播放违禁视频）立即切断终端显示并触发声光告警；二级（重要，如未知 USB 接入）暂停终端数据更新并通知运维人员；三级（一般，如网口异常连接尝试）记录日志并持续监控。

3.3.3 远程控制模块

远程指令下发：系统管理平台支持向终端下发远程指令，包括：接口控制（如禁用 USB 口、断开网口连接）、内容管控（如紧急切换至预设安全画面、删除违禁文件）、系统维护（如终端重启、固件升级）；

电源远程控制：终端配备智能电源模块，支持远

程断电 / 通电。当终端出现无法远程修复的故障（如系统崩溃）或严重安全事件（如持续播放违禁内容），运维人员可通过平台下发断电指令，切断终端电源，避免风险扩散；

控制响应优化：采用 5G / 工业以太网传输指令，确保远程控制响应时间小于 10 秒，满足应急处置需求。

3.4 数据规则与终端模板绑定设计

数据规则配置：系统加载数据源配置文件，转换为包含 “标题、数据源表、数据提供器、元数据列、子查询、复杂字段” 的实体类，用户基于实体类选择显示字段、设置过滤条件（如 “出港航班且计划起飞时间 8 小时内”）与排序规则，配置完成后支持测试验证；

终端模板设计：提供可视化工具，支持拖拽文本、图片、表格等控件，绑定数据规则字段（如 “航司 LOGO” 绑定图片控件，“航班号” 绑定文本控件）；

模板发布与同步：模板绑定完成后发布至目标终端，终端自动加载模板与规则，配置变更即时生效，无需重启终端。

4 系统优势分析与应用验证

4.1 系统优势分析

功能扩展灵活高效：字段修改仅需调整数据源配置，响应时间从数天缩短至分钟级，维护成本降低 90% 以上；支持多业务数据集成，扩展周期不超过 30 分钟；

安全防护全面：硬件接口 “白名单” 管控杜绝未知设备接入，违禁内容识别准确率达 99.5%，远程控制响应快速，有效防范公共区终端安全风险；

运维门槛低：可视化配置界面与友好交互设计，运维人员经培训即可自主完成数据源配置、安全告警处置，无需依赖开发人员 [20]。

4.2 应用验证

在某年旅客吞吐量 1500 万人次的中型机场进行应用测试，测试场景与结果如下：

4.2.1 功能扩展测试

字段新增：在出发大厅终端新增 “经停站” 字段，调整数据源配置后 1 分钟内，终端成功显示经停站信息，符合预期；

业务扩展：集成 “停车场余位” 数据源，配置完成后 25 分钟，终端同步显示余位信息，数据更新频率 1 分钟 / 次。

4.2.2 安全防护测试

硬件接口管控：接入未知 USB 设备，终端立即禁用接口并触发二级告警，平台 10 秒内接收告警信息；尝试通过外部网络连接网口，连接请求被屏蔽，操作日志记录完整；

违禁内容识别：向终端植入含违禁文字的文档与图片，系统 1.5 秒内识别并触发一级告警，终端自动切换至安全画面，同时向运维人员发送短信通知；

远程控制：对故障终端下发重启指令，响应时间 8 秒；对播放违禁内容的终端下发断电指令，10 秒内完成断电，风险快速遏制。

4.2.3 稳定性测试

连续 30 天运行测试，系统无故障运行时间（MTBF）达 712 小时，字段更新与模板发布成功率 100%，安全告警误报率低于 0.5%，满足机场运营需求。

5 结论与展望

本文设计的智能 FIDS，通过数据源动态配置实现显示字段灵活扩展，结合硬件安全管控模块解决公共区终端安全风险，有效弥补了传统系统的缺陷。应用测试表明，系统在功能扩展效率与安全防护能力上均表现优异，为机场智慧化运营提供有力支撑。

未来研究可从三方面展开：

优化 AI 违禁内容识别模型，提升小样本、变异违禁内容的识别能力；

引入边缘计算技术，在终端本地实现部分数据处理与安全分析，降低平台算力压力；

构建多机场 FIDS 协同管理平台，实现数据源、安全规则的跨机场共享，提升区域机场群运营效率与安全水平。

参考文献

[1] 中国民用航空局。中国民航发展统计公报（2024 年）[R]. 北京：中国民用航空局，2025.

[2] 张磊，王健。机场航班信息显示系统的设计与实现 [J]. 计算机工程与设计，2022，43 (5)：1356-1362.

[3] 公安部。公共交通场所安全防护技术规范（GB/T 35790-2023）[S]. 北京：中国标准出版社，2023.

[4] 张强，李娜。基于动态数据源的智慧机场信息显示系统设计 [J]. 仪器仪表学报，2023，44 (5)：102-110.

作者简介：潘光绪（1973-），男，汉族，重庆璧山，硕士研究生，高级工程师，研究方向：机场工程。