ICS 35.240.60
V 07

MH

中华人民共和国民用航空行业标准

MH/T 0054.1—2015

民用机场离港前端系统指南
第1部分：系统安全

The guide to the front-end system of the departure control of civil aviation airport—
Part 1：System security

2015－07－15 发布　　2015－10－01 实施

中国民用航空局　发布

前　言

MH/T 0054《民用机场离港前端系统指南》分为四个部分：

——系统安全；

——运行维护；

——应急响应与处置；

——应急预案与演练。

本部分为MH/T 0054的第1部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国用航空局人事科教司提出。

本部分由中国民航航空局航空器适航审定司批准立项。

本部分由中国民航科学技术研究院归口。

本部分起草单位：中国民航信息网络股份有限公司、中国民航大学。

本部分主要起草人：李响、程忠锋、杨宏宇、成翔、王信元、睦永波。

民用航空机场离港前端系统指南
第1部分：系统安全

1 范围

MH/T 0054的本部分规定了民用航空机场离港前端系统的建设原则、安全审查要求、等级保护要求、备份机制、机房与设备安全要求、离港网络安全要求、系统安全要求、数据安全要求，以及信息安全管理制度要求。

本部分适用于民用航空运输机场离港前端系统的安全建设与安全管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 9361 计算机场地安全要求

GB/T 20988-2007 信息系统灾难恢复规范

GB/T 22239 信息系统安全等级保护基本要求

GB/T 22240 信息系统安全保护等级定级指南

MH/T 5103 民用机场信息集成系统技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

离港系统 departure control system

提供旅客值机、配载平衡、登机控制、联程值机等信息服务，能满足值机控制、配载控制、登机控制等机场旅客服务所需功能的计算机信息系统及终端设备。

[MH/T 5103-2004，定义3.4]。

3.2

离港前端系统 front-end system of departure control

支持离港主机服务，当与离港主机连接中断时仍能在机场本地提供旅客值机、配载平衡、登机控制等备份信息服务的计算机信息系统。

3.3

离港网络 network of departure control system

机场离港业务的网络承载平台，由机场本地离港局域网和离港主干接入网络组成。

4 建设原则

4.1 安全性和可控性

应确保机场离港业务数据的保密性和完整性，保证离港前端系统的安全性、可靠性和业务连续性，确保对离港业务资源、数据和服务的自主可控。

4.2 开放性

机场离港前端系统应易于与机场其他业务系统相融合，应为机场其他信息系统提供标准的数据接口。

4.3 接入安全

其他应用服务接入机场离港前端系统时，应符合统一的安全策略规范。

4.4 可扩展性

离港前端系统应具备扩展能力，可支持值机、登机、控制、配载等业务终端的扩展和系统业务功能的扩展。

5 安全审查要求

机场离港前端系统的技术产品供应商、技术产品和技术服务应符合系统设计要求，并事先通过我国国家级信息安全权威机构的信息安全审查和安全测评。对未通过我国信息安全审查或信息安全测评的技术产品和技术服务，不得在中国境内使用。

6 等级保护要求

6.1 应确定机场离港前端系统的边界和范围。
6.2 应依照国家有关管理规范和 GB/T 22240 的要求，确定机场离港前端系统的安全等级。
6.3 应按照 GB/T 22239 对机场离港前端系统持续开展等级保护工作。

7 备份机制

7.1 网络备份

7.1.1 机场离港网络核心设备、接入设备和线路应具备冗余备份机制，应能保证网络的连通性和数据传输的连续性。
7.1.2 机场离港前端系统与其他信息系统的数据交换应具备冗余机制。

7.2 系统备份

7.2.1 机场离港前端系统的应用服务器、数据库服务器、接口服务器、数据存储设备等核心硬件应采用热备份冗余机制，应确保备份冗余机制的有效性。

7.2.2 机场离港前端系统软件应具备本地备份机制和服务应急机制，应确保备份机制和服务应急机制的有效性。

7.2.3 机场离港前端系统的本地备份机制和服务应急机制应能在短时间内实现切换和启动，应能避免离港业务中断。

7.2.4 应按照 GB/T 20988 的第 5 级灾难恢复技术要求，为机场离港前端系统建立灾难备份和恢复机制。

8 机房与设备安全要求

8.1 机场离港前端系统的机房环境建设应首先满足 GB/T 9361 和 MH/T 5103 对机场离港前端系统主机房、中央控制室及电源设备间的环境要求，并宜符合附录 A 的技术指标要求。

8.2 应按照 GB/T 9361 要求建设和完善机场离港前端系统设备的物理防护措施。

8.3 应部署各服务器、存储设备、应用软件和接口软件的实时监控技术措施，具备对软硬件运行异常情况的实时报警能力。

8.4 离港前端系统的服务器、存储设备、网络设备等重要系统设备应配备 UPS 设备进行供电。

9 网络安全要求

9.1 机场内应具备两家以上电信运营商的离港主干接入网络，并经不同物理链路和物理管井接入。

9.2 机场离港前端系统核心交换机至离港系统主机的离港主干接入网络应具备冗余物理路由，应具备端到端的保障机制。

9.3 机场离港网络的重要网络设备应采用双机热备份冗余配置，并应满足分接 UPS 双路供电要求。

9.4 机场离港网络应避免与其他网络直接互联或混用，应根据访问控制策略部署网络访问控制和业务隔离等技术手段。

9.5 应部署网络监控系统，实时监控离港网络状态和设备运行状况，应具备对机场离港网络各种异常状况的告警、记录和审计能力。

9.6 应具备网络设备用户的安全管理措施，对离港网络设备用户进行鉴别和限制，并支持身份验证。

9.7 应具备网络权限管理、接口访问和数据访问的安全控制措施。

9.8 机场离港网络安全策略应只开通与生产及维护相关的访问控制策略。

9.9 机场离港网络应与其他非生产网络进行安全隔离，如有网络互联需求，应通过必要的安全设备或安全访问策略进行控制与防护。

9.10 远程维护应采用专用终端并安装管理工具和安全防护软件，及时更新系统补丁和安全资源库。

9.11 远程维护终端应具备在本地业务部门许可前提下的远程接入机制。

10 系统安全要求

10.1 应具备对机场离港前端系统的值机、登机、控制等终端和用户进行标识和识别的技术措施，拒绝非法用户使用。

10.2 宜通过第三方授权或认证方式验证用户登录访问、权限分配、操作执行等的合法性。

10.3 机场离港前端系统的服务器应采用本地备份冗余配置。

10.4 应具备系统操作工作日志的自动记录和分析措施，并具有日志分析处理机制。

10.5 机场离港前端系统用户安全策略应只涉及与生产及维护相关用户，并授予相应权限。

10.6　其他信息系统与机场离港前端系统进行交互作业时，机场离港前端系统应对其进行安全验证并保存验证日志与记录。

10.7　应对操作系统和应用服务默认的配置进行安全审计和加固，应及时更新操作系统和应用服务的安全补丁，保证系统无高危漏洞。

10.8　机场离港前端系统投入使用前，应对硬件、软件以及应用进行连通性测试、性能测试、安全性测试和压力测试。

10.8.1　机场离港前端系统测试通过后，应删除测试数据、账号和口令，回收超级用户权限。

11　数据安全要求

11.1　应具备数据操作日志记录和分析措施。

11.2　应具备数据安全防护措施，确保信息不被非法查看、复制、修改、转录和删除。

11.3　应具备对离港数据存储和传输的加密能力。

11.4　应具备对数据进行备份和介质转存能力。

12　信息安全管理制度要求

12.1　应制定并严格执行机场离港前端系统的信息安全管理制度。

12.2　应制定并严格执行机场离港前端系统的网络和系统设备安全管理规范。

12.3　应制定并严格执行机场离港前端系统信息通报管理规范。

12.4　应制定并严格执行机场离港前端系统数据存储及介质安全管理规范。

12.5　应制定并严格执行机场离港前端系统的应急响应、处置与定期演练规范。

附 录 A
（资料性附录）
离港前端系统机房环境技术要求

见表A.1。

表A.1

技术指标	技术要求			备注
	枢纽机场	大中型机场	其他机场	
环境要求				
机房温度控制范围（机柜进风口工况 °C）	18 °C～27 °C			不得结露
机房相对湿度控制范围（机柜进风口工况）	20%～80%			
温度变化率	3 °C/h			
湿度变化率	6%/h			
建筑结构				
机房活荷载	不小于 8 kN/m²			根据机房设备布局和摆放密度确定荷载值
空气调节				
机房面积小于 50 m² 机房空调	应按 N+1 冗余		宜按 N+1 冗余	—
机房空调	大于 50m² 应按照《电子信息系统机房设计规范》GB50174 相关规定执行			—
机房设置采暖散热器	不应		不宜	—
电气技术				
后备发电机电源	应具备	宜具备	不间断电源系统的供电时间满足信息存储要求时，可不设置柴油发电机	—
不间断电源系统配置	2N	2N 或 N+1	根据实际需要确定	—
不间断电源系统电池备用时间	根据实际需要确定			—

表 A.1(续)

技术指标	技术要求			备注
	枢纽机场	大中型机场	其他机场	
机房布线				
布线方式	电气线路宜地板下布线，通信线路宜机柜上端布线		根据实际需要确定	—
环境和设备监控系统				
机房空调	宜设置		根据实际需要确定	—
供配电系统	宜设置		根据实际需要确定	—
不间断电源系统	应设置，并具备远程监控功能		根据实际需要确定	—
集中控制和管理	宜设置		根据实际需要确定	机房区域大于100㎡
安全防范系统				
机房出入口	应设置		宜设置	—
视频监控	应设置		根据实际需要确定	—
给水排水				
与机房无关的给排水管道穿越主机房	不应			—
机房地面设置排水系统	应			用于冷凝水排水
消防				
机房设置洁净气体灭火系统	应		宜	采用洁净灭火系统