ICS 35.020
V 07

MH

中华人民共和国民用航空行业标准

MH/T 0051—2015

民用航空信息系统安全等级保护实施指南

Implementation guide to information system security classified protection of civil aviation

2015－04－08 发布　　2015－08－01 实施

中国民用航空局　发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国民用航空局人事科教司提出。

本标准由中国民航航空局航空器适航审定司批准立项。

本标准由中国民航科学技术研究院归口。

本标准起草单位：中国民航大学、中国民航科学技术研究院。

本标准起草人：谢丽霞、刘晓杰、熊育婷、钟安鸣、赵宏旭、成翔、杨宏宇、杜伟军、王信元、王冲。

民用航空信息系统安全等级保护实施指南

1 范围

本标准规定了民用航空信息系统安全等级保护工作的对象、目标，定义了民用航空信息系统安全等级保护工作的实施流程，涉及的各类角色及职责，以及等级保护实施各阶段的主要任务和工作流程。

本标准适用于民用航空信息系统安全等级保护工作。

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 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

GB/T 28448 信息安全技术 信息系统安全等级保护测评要求

3 术语和定义

3.1

网络与信息安全 network and information security

依靠网络进行的信息交互活动中的信息安全性，以及网络与信息系统自身的安全可靠性，特指网络和信息系统的保密性、完整性和可用性，以及信息的可认证性、可核查性、不可抵赖性和可靠性。

[MH/T 0035—2012，定义3.1]

3.2

民用航空重要网络与信息系统 important network and information system of civil aviation

安全保护等级为二级以上的民用航空网络和信息系统，包括民航各级行政管理机构、直属单位、民用航空运输机场、航空公司、空管部门和航空运输保障单位的基础网络和核心业务系统等。

[MH/T 0035—2012，定义3.4]

3.3

安全等级保护 classified security protection

依照信息系统安全保护等级要求，对网络与信息系统实施的安全防护、技术保障和安全管理等行为。

3.4

等级保护对象 target of classified security

信息安全等级保护工作直接作用的具体的网络与信息系统。

3.5

等级测评　classified security testing and evaluation

确定信息系统安全保护能力是否达到相应等级基本要求的过程。

[GB/T 25058-2010，定义3.1]

4　安全等级保护概述

4.1　等级保护对象

民用航空信息系统安全等级保护对象为民用航空网络与信息系统。

4.2　安全等级保护目标

安全等级保护的目标是通过对民用航空重要网络与信息系统进行安全等级划分，按照本标准中的安全等级保护要求进行规划、建设、运维、管理和监督，从而加强民用航空信息系统的安全防护能力，确保其安全性和可靠性。

5　信息系统安全等级保护实施流程

信息系统安全等级保护实施的总体流程见图1，安全等级保护实施工作各阶段活动流程参见附录A。各阶段的主要任务应包括：

a) 信息系统定级：民航各企事业单位应按照国家有关管理规范，识别信息系统的范围，进行信息系统分析并确定信息系统安全保护等级；
b) 信息系统等级备案：民航各企事业单位应整理需要备案的信息系统的等级保护报告和备案表，形成完整的备案材料并办理备案手续；
c) 安全规划设计：民航各企事业单位应根据相应等级的信息系统等级保护基本要求，对信息系统的安全保护措施进行总体规划设计；
d) 安全建设与实施：民航各企事业单位应根据通过评审的方案，选择和使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设和实施；
e) 安全等级测评：民航各企事业单位应选择符合条件的信息安全服务机构，依据 GB/T 28448 定期对信息系统安全等级状况开展系统安全等级测评和风险评估；
f) 系统建设与整改：完成系统测评和风险评估后，应依照报告内容对系统进行安全措施整改和安全加固，完善信息系统的安全保护措施；
g) 安全运行与管理：在运行期间应依照等级保护要求做好系统安全运行、变更、安全状态监控、安全事件处置、安全审计和检查等方面的相关工作；
h) 系统终止：应妥善处理系统内的残余信息，确保民航信息资产得到安全控制。

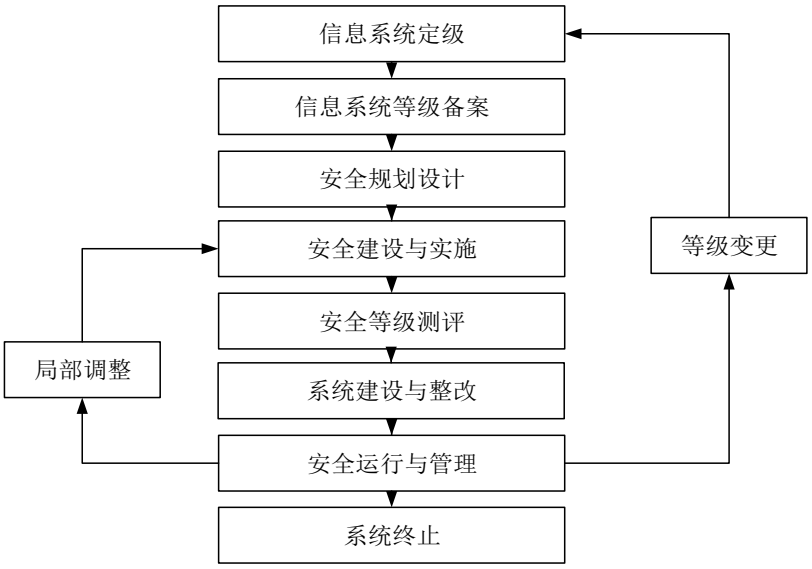

图1 安全等级保护系统实施的总体流程

6 信息系统定级

6.1 信息系统定级阶段的工作流程

民航信息系统运营、使用单位应按照国家有关管理规范和信息系统等级保护定级指南的要求，确定信息系统的安全保护等级。本阶段的主要工作应包括：

a) 信息系统分析：应确定信息系统的边界和范围，形成信息系统总体描述文件；
b) 安全保护等级确定：应依照信息系统等级保护定级指南的要求，确定信息系统的安全保护等级，形成定级报告和备案表；
c) 专家评审：应针对信息系统的总体描述材料、信息系统的定级报告和备案表，聘请专家对定级的准确性、合规性进行评审。

6.2 信息系统分析

应从信息系统运营、使用单位相关人员处收集有关信息系统的信息，并对信息进行综合分析和整理，依据分析和整理的内容形成本单位的信息系统总体描述性文档。

6.3 安全保护等级确定

信息系统运营、使用单位应按照GB/T 22239和GB/T 22240的要求，确定信息系统的安全保护等级，并对定级结果进行审核和批准，保证定级结果的准确性。应对定级过程中产生的文档进行整理，形成定级报告和备案表。

6.4 专家评审

信息系统运营、使用单位应组织专家对定级报告进行评审。评审通过后，应由信息系统运营、使用单位按要求向公安机关备案。

6.5 定级审核

信息系统运营、使用单位应向民航行政管理机构提供三级以上（含三级）的民用航空重要网络与信息系统的安全保护定级报告及备案材料，民航行政管理机构应根据定级报告视情况聘请专家对定级报告进行审核。

7 信息系统等级备案

信息系统运营、使用单位应根据国家信息安全管理部门对信息系统等级备案的要求，整理相关备案材料，并向公安机关提交备案材料，获得公安机关出据的信息系统安全保护等级备案证明。应将备案证明和材料向民航行政管理机构备案。

8 安全规划设计

应根据民航信息系统的等级保护定级情况、系统承载的业务情况，明确已定级的民航信息系统的安全需求，设计合理的、满足等级保护要求的安全方案，并制定安全实施计划。应包括：安全需求分析、安全总体设计、安全建设项目规划、安全建设内容规划、形成安全建设项目计划等部分。

9 安全建设与实施

应该根据建设目标和建设内容，将信息系统安全总体方案中要求实现的安全策略、安全技术体系结构、安全措施和要求落实到产品功能或物理形态上，提出能够实现的产品或组件及其具体规范，并将产品功能特征整理成技术措施落实方案。主要应包括：安全方案详细设计、管理实施实现内容设计、安全实施过程管理等部分。

10 安全等级测评

10.1 测评机构选择

信息系统运营、使用单位应严格按照国家和民航相关规定选择具有资质的信息安全测评机构。

10.2 测评实施

信息安全测评机构应依据GB/T 28448，对信息系统进行等级保护测评和风险评估。

10.3 测评报告提交

测评结束后，信息安全测评机构应向系统运营、使用单位提交测评报告和风险评估报告。

11 系统建设整改

11.1 制定整改方案

应根据测评报告和风险评估报告，确定与安全保护等级相适应的安全整改方案。

11.2 测试与验收

应检验系统是否严格按照方案进行建设，是否实现了设计的功能和性能。在安全控制实施工作完成后，应对整个系统进行集成性安全测试。

11.3 文件和制度修订

按照安全整改方案实施各项补充的安全措施后，应调整和修订相关技术文件和管理制度，保证信息安全体系的完整性和一致性。

12 安全运行与管理

12.1 运行管理过程控制

应通过制定运行管理操作规程，确定并实施安全运行与维护阶段的运行管理和控制、安全状态监控、安全事件处置和应急预案、安全检查和持续改进等过程，确保对操作过程实施有效控制。

12.2 定期测评

应由具备资质的信息安全服务机构按照GB/T 28448，对已经完成等级保护建设的信息系统定期进行等级测评，确保信息系统的安全保护措施符合相应等级的安全要求。

12.3 监督检查

应由民航各级行政管理机构对系统运营、使用单位的信息系统定级、规划设计、建设实施和运行管理等过程进行监督检查，确保其符合信息系统安全保护相应等级的要求。

12.4 持续改进

应根据测评和检查结果、对系统的安全技术措施和管理措施进行局部调整或安全等级变更。

13 系统终止

应参照国家有关标准，在民航信息系统终止阶段实施信息的转移、暂存或清除，设备迁移或废弃，存储介质的清除或销毁等工作。

附 录 A
（资料性附录）
安全等级保护实施工作各阶段活动流程

表A.1中标注“*”的完成文档为比较重要的文件。

表A.1

主要阶段	主要过程	工作内容	准备文档	完成文档
信息系统定级	信息系统分析	系统识别和描述	信息系统的立项、建设、管理文档	信息系统总体描述文件
		信息系统划分	信息系统总体描述文件	*信息系统详细描述文件
	安全保护等级确定	定级、审核和批准	信息系统总体描述文件 信息系统详细描述文件	定级结果
		形成定级报告	信息系统总体描述文件 信息系统详细描述文件 定级结果	*信息系统安全保护等级定级报告
	专家评审	信息安全主管部门审核,并示情请专家审核	信息系统的总体描述报告信息系统的定级报告	*民航重要网络和信息系统安全保护等级定级专家评审意见 *民航重要网络和信息系统安全保护等级定级报告” *民航重要网络和信息系统安全保护等级备案表”
信息系统备案	备案材料整理	针对提交备案材料进行整理	信息系统安全保护等级定级专家评审意见 信息系统安全保护等级定级报告 信息系统安全保护等级备案表	整体性备案材料。
	备案材料提交	办理定级备案手续，提交备案材料，公安机关审核	整体性备案材料	信息系统备案证明

表 A.1(续)

主要阶段	主要过程	工作内容	准备文档	完成文档
安全规划设计	安全需求分析	基本安全需求确定	信息系统详细描述文件 信息系统安全保护等级定级报告 信息系统安全等级保护基本要求 信息系统相关的其它文档	基本安全需求
		额外/特殊安全需求的确定	信息系统详细描述文件 信息系统安全保护等级定级报告 信息系统相关的其它文档	重要资产的特殊保护要求
		形成安全需求分析报告	信息系统详细描述文件 信息系统安全保护等级定级报告 信息系统安全等级保护基本要求 基本安全需求 重要资产的特殊保护要求	*安全需求分析报告
	安全总体设计	总体安全策略设计	信息系统详细描述文件 信息系统安全保护等级定级报告 安全需求分析报告	总体安全策略文件
		安全技术体系结构设计	总体安全策略文件 安全需求分析报告 信息系统安全等级保护基本要求	安全技术体系结构文档
		安全管理体系结构设计	总体安全策略文件 安全需求分析报告 信息系统安全等级保护基本要求	安全管理体系结构文档
		设计结果文档化	安全需求分析报告 信息系统安全技术体系结构 信息系统安全管理体系结构	*信息系统安全总体方案
	安全建设项目规划	安全建设目标确定	信息系统安全总体方案 单位信息化建设的中长期发展规划	信息系统分阶段安全建设目标
		安全建设内容规划	信息系统安全总体方案 信息系统分阶段安全建设目标	安全建设内容

表 A.1(续)

主要阶段	主要过程	工作内容	准备文档	完成文档
安全规划设计	安全建设项目规划	安全建设项目计划设计	信息系统安全总体方案 信息系统分阶段安全建设目标 安全建设内容	*信息系统安全建设项目计划
安全建设与实施	安全方案详细设计	技术措施实现内容设计	信息系统安全总体方案 信息系统安全建设项目计划 各类信息技术产品技术白皮书 各类信息安全产品技术白皮书	技术措施实现方案
		管理措施实现内容设计	信息系统安全总体方案 信息系统安全建设项目计划	管理措施实现方案
		设计结果文档化	技术措施落实方案 管理措施落实方案	*安全详细设计方案
	管理措施落实	管理机构和人员的设置	本单位现有相关管理制度和政策 安全详细设计方案	*角色与职责说明书
		管理制度的建设和修订	安全组织结构表 角色与职责说明书 安全详细设计方案	*各项管理制度和操作规范
		人员安全技能培训	系统/产品使用说明书 各项管理制度和操作规范	培训记录及上岗资格证等
		安全实施过程管理	安全技术建设各阶段相关文档	各阶段管理过程文档
	技术措施落实	信息安全产品采购	安全详细设计方案、相关产品信息	已采购信息安全产品清单
		安全控制集成	安全详细设计方案	安全控制集成报告
		系统验收	安全详细设计方案 安全控制集成报告	*系统验收报告
安全等级测评	测评机构选择		信息安全服务机构选择规定 信息安全服务机构清单 信息安全服务机构资质	*信息安全服务合同
	测评实施		等级保护测评标准 风险评估标准	等级保护测评方案 风险评估方案

表 A.1(续)

主要阶段	主要过程	工作内容	准备文档	完成文档
安全等级测评	测评报告提交		系统等级保护测评数据 系统风险评估数据	*信息系统安全等级测评报告 *信息系统安全风险评估报告
系统建设与整改	制定整改方案		信息系统安全等级测评报告 信息系统安全风险评估报告	安全整改方案
	安全方案实施控制		安全整改方案 安全产品文档	安全加固技术文档 安全建设文档
	测试与验收		安全建设文档	*测试报告 *验收报告
	文件和制度修订		原技术文档 原安全管理制度文件	*技术文档 *安全管理制度文件
安全运行与管理	运行管理和控制	运维管理职责确定	安全详细设计方案 安全组织机构表	*运行管理人员角色和职责表
		运维管理过程控制	运行管理需求 运行管理人员角色和职责表	*各类运行管理操作规程
	等级测评		信息系统安全保护等级定级报告 系统验收报告 测试或验收报告	*安全等级测评报告
	监督检查		备案材料	*监督检查结果报告
系统终止	信息转移、暂存和清除		信息系统信息资产清单	信息转移、暂存、清除处理记录文档
	设备迁移或废弃		信息系统硬件设备清单	设备迁移、废弃处理记录文档
	存储介质的清除或销毁		信息系统存储介质清单	存储介质清除、销毁处理记录文档