2017 年第 4 期　总 127 期
ISSN 1674-9804　CN 31-1614/V

DOI: 10.19416/j.cnki.1674-9804.2017.04.008

民用飞机电传飞控系统功能危害性评估方法研究

Functional Hazard Assessment Methods of Fly-by-wire Flight Control System for Civil Aircraft

王晓梅　龚孝懿　李　棋 / WANG Xiaomei　GONG Xiaoyi　LI Qi
（上海飞机设计研究院，上海 201210）
（Shanghai Aircraft Design and Research Institute, Shanghai 201210, China）

摘　要：
民机系统级功能危害性评估（Functional Hazard Assessment，简称 FHA）是指对系统功能进行系统性的综合分析过程，即依据系统功能失效状态对飞机安全性影响严重程度进行评估，从而实现对功能的等级进行识别和分类的过程，是系统顶层关键的设计过程。在分析大量相关资料和实际型号经验的基础上，得出适用于民机电传飞控系统的功能定义、功能失效状态分析和确定功能失效影响等级并对其进行确认的思路和方法，以及保证民机电传飞控系统级 FHA 正确性和完整性的具体可行的措施等，该方法已应用到某民机电传飞控系统级 FHA 的评估工作中，取得了良好的效果。
关键词：民机；电传飞控系统；功能危害性评估；失效状态；功能失效影响分级
中图分类号：V249.1　　**文献标识码：**A
[**Abstract**] Civil aircraft system functional hazard assessment refers to the process of systematic comprehensive analysis of the system function, namely according to system function failure condition to evaluate severity influence on the safety of aircraft, so as to realize the function of the level of recognition and classification process, which is the top key system design process. Based on the analysis of a large number of relevant materials and practical experience, this article gives the ideas and methods which applies to commercial fly-by-wire flight control system's function definition, function of failure condition, analysis and validation of the functional failure affect level, and makes sure that correctness and completeness of fly-by-wire flight control system FHA. The method has been applied to a commercial fly-by-wire flight control system of the evaluation work of FHA.
[**Keywords**] civil aircraft; flight control system; functional hazard assessment; failure condition; classification of failure condition

0　引言

功能危害性评估（Functional Hazard Assessment，简称 FHA）是检查分析飞机及系统功能，以确定潜在的功能失效，并根据具体的失效状态对功能危害进行分类的安全性评估方法。民机电传飞控系统级 FHA 是开发飞控系统架构，驱动系统设计的最为关键的安全性需求源之一，也是进行系统安全性评估过程及系统研制过程的重要输入。如何保证 FHA 功能定义、功能失效状态分析和功能失效影响分级的正确性和完整性，是系统构架及满足适航安全性要求的关键。

1　民机电传飞控系统的功能定义

系统级功能来源于飞机级功能分解，系统功能的准确定义和层级的合理划分是建立飞控系

统级 FHA 的先决条件，是飞控系统危害分析的关键。

依据型号经验，进行民机电传飞控系统功能定义时，主要步骤为：1）为每项已经能明确的系统级功能需求生成一项功能；2）构建功能架构和功能框图（包括外部接口）；3）生成符合功能逻辑层次和功能流程图的功能；4）创建功能文件；5）进行概念设计，在系统级确认子系统；6）分配功能给子系统，定义产品分解结构（PBS）。

按照上述步骤，民机电传飞控系统功能定义应遵循的原则为：1）按照逐步展开的方式进行相应的功能分析，找出所有工作状态和模式下可能的所有功能或子功能，包括功能的定义、所处的工作状态或飞行阶段描述等；2）在进行功能分析时应充分考虑飞机系统间的界面关系；3）只针对分析对象的功能展开分析，而不涉及完成功能的具体设备、系统或结构；4）按照飞机级-系统级进行功能的划分；5）功能定义综合分析系统在功能、性能、物理、人机、安全等各方面的需求，应使所有的需求信息通过功能组织架构进行表达。

民机电传飞控系统功能由软硬件共同实现，进行系统级 FHA 设计分析时，既要考虑硬件功能又要考虑软件功能。功能通常包括内部功能和交互功能两大类。如果功能之间存在相互补充或相互冗余的关系，需考虑功能之间的耦合和组合失效情况。表 1 为民机飞控系统按不同层级展开的横滚控制功能清单示例。确定系统功能定义时要选取合适的层级，具体的技术实现层级和过高层级都应在系统功能定义中避免。表 1 中：功能层级 1 属于飞控系统级功能，层级太高；功能层级 2 属于飞控子系统级功能，功能失效对系统运行的影响可直接分析形成；功能层级 3 属于具体的技术实现层级，层级太低，若对该层级进行失效分析需考虑过于细节的系统运行情况，难以分析出这些功能失效对系统的危险影响。因此将展开的功能层级 2 作为系统级功能清单更为合适。

表 1　民机飞控系统的横滚控制功能清单示例

顶层功能	展开的功能层级 1	展开的功能层级 2	展开的功能层级 3
横滚控制功能	副翼横滚控制功能	提供横滚操纵输入功能	实现横滚左/右控制功能
			横滚控制左/右驾驶互联功能及相应脱开及反馈功能
			提供驾驶盘横滚控制的电信号输出功能
			为飞行员提供操纵阻尼力、摩擦力和人工感觉力功能
			……
		通过动力装置提供副翼舵面控制功能	提供左或右副翼舵面运动功能
			为左或右副翼舵面提供余度颤振抑制功能
			提供精确的作动器状态反馈功能
			……
		提供副翼 PCU 控制指令功能	……
	MFS 辅助横滚功能	……	……

2　功能失效状态分析

2.1　建立完整功能失效状态的系统方法

为确保 FHA 中功能失效状态的完整性，分析过程全面考虑了系统功能所有可能的失效状态、功能接口、失效状态的通告状态、工作阶段及失效状态场景/紧急情况等情况，其流程如图 1 所示。具体分析过程如下：

1）可能的失效状态

（1）失控（全部或部分）、卡阻或游离；

（2）功能完全失效、部分失效、功能不稳定或降低工作功效；

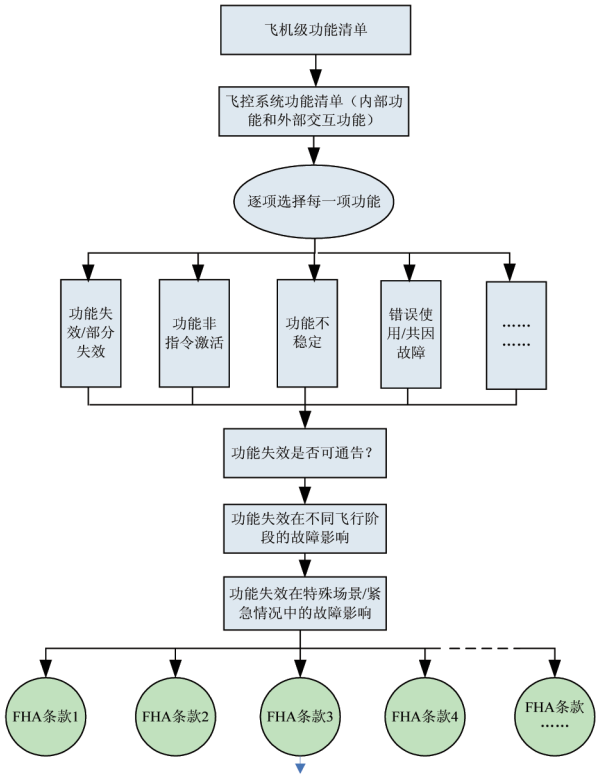

图 1　建立 FHA 失效状态的基本流程图

（3）意外工作或非指令地工作；

（4）特性改变（载荷、速率、刚性、延迟、振荡等）；

（5）无失效指示/警告或有害的失效指示/警告；

（6）错误的数据输出或数据显示；

（7）其它。

失效状态是否通告对某些失效条件影响分级有较大影响。另外，指示系统的错误指示通常比指示系统故障或失效的影响更为严重。

2）飞行阶段及失效状态场景

在失效影响分析时，应考虑不同的飞行任务和可能的飞行场景等。民机的飞行任务一般分七个阶段，如图 2 所示。另外，还有复飞、中断起飞等飞行阶段。

功能失效在不同飞行阶段产生的影响不同时，要对不同飞行阶段的同一功能失效分别进行分析。例如某民机飞控系统级 FHA 条目“非指令性打开两块地面扰流板的地面破升功能”，对于不同的飞行阶段，其失效状态影响等级是不同的。

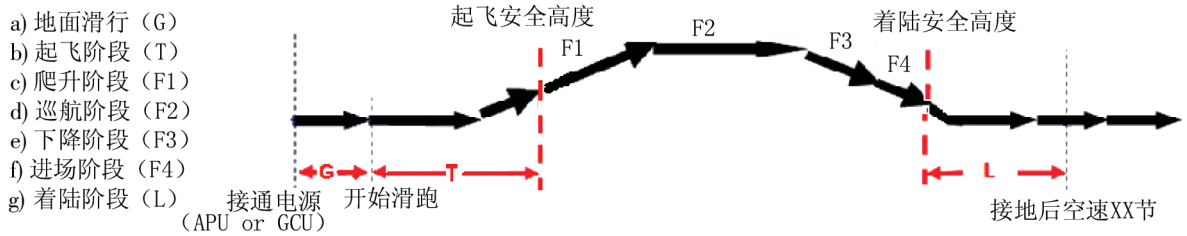

图 2　民机的飞行阶段示例

另外，失效状态应考虑特殊场景和紧急情况，例如某民机丧失减速板功能为 IV 类故障，但是当考虑到飞机紧急下降的场景，其失效状态影响等级评估为 II 类。对于民机电传飞控系统，考虑的故障特殊场景和紧急情况至少包括如下情况：①中断起飞；②紧急下降；③液压系统失效；④单发失效；⑤飞控系统进入降级模式；⑥共模故障；⑦失效状态的通告性。

2.2　确保 FHA 失效状态完整的其他措施

1）相似性

在形成飞控系统级 FHA 失效状态清单后，可与相似机型或系列机型进行对比确认，明确飞控系统级 FHA 与相似/系列机型 FHA 之间的差异，分析存在的差异是否合理、可信。不同机型 FHA 的差异性主要来源于飞机构型的差异，如系统架构、舵面布置、系统所实现的功能差异等。

2）追溯性

飞机级 FHA 来源于飞机级功能分解，系统级 FHA 来源于系统级功能分解。由于系统级功能来源于飞机级功能分解、定义，因此飞机级 FHA 与系统级 FHA 之间必定存在联系。通过系统级功能清单建立的飞控系统级 FHA 应能有效覆盖飞机级 FHA 中与飞控系统相关的部分，通过对比分析的方法，可从侧面检查飞控系统功能分解是否完整。

3）工程评审

邀请本专业和相关专业及适航等方面的若干资深专家对系统的 FHA 进行工程评审，依据专家

丰富的经验对系统级 FHA 中失效状态的完整性进行判定，这是工程活动中较为常用和适用的确认方法。

3　系统级 FHA 失效状态影响等级的判定原则和方法

3.1 判定原则

根据 AC25.1309-1B，故障危害程度与定性、定量要求成反比。对于越严重的故障状态，要求故障发生的概率越小；反之亦然。故障状态影响等级分为灾难性的、危险的、较大的、较小的和无安全性影响五类。

等级 I—灾难性的：失效情况妨碍继续安全飞行，造成多个人员死亡和（或）系统破坏。发生概率要求低于1E-9。

等级 II—危险的：失效情况导致安全裕度和性能大大降低；飞行机组人员身体受伤或负担大大增大，使得他们不能准确和完善地执行任务；对乘客产生有害影响，可能发生某些人员严重的或许是致命的伤害。发生概率要求在1E-9～1E-7。

等级 III—较大的：失效情况导致安全裕度和性能显著降低；由于工作载荷的增加或由于损害操作者效率情况的出现；使操作者处理不利工作情况的能力有所下降；乘客感到不舒服，可能发生人员受伤的情况。发生概率要求在1E-7～1E-5。

等级 IV—较小的：失效情况对安全性没有显著的影响，所要求的任何操作安全在操作人员的能力之内。例如，稍微降低飞机的安全裕度和性能，飞行机组的负担稍微增加、航线飞行计划改变或乘客感到有些不方便。发生概率高于1E-5～1E-3。

等级 V—无安全性影响：对飞机运行能力、安全性和人员无影响。

3.2 判定方法

系统级 FHA 中失效状态影响等级一般可通过分析、计算、风洞试验、工程模拟器试验以及工程评审等方法，由于飞机研制的成熟度的增加，在飞机设计具有足够数据后，可进一步对影响等级进行分析和确认，并可通过飞行员在环试验进行评估和确认。

3.2.1 分析

在项目早期，一般通过桌面仿真的方法对系统失效状态影响等级进行评估。另外，还可借鉴相似机型的相关经验对失效状态影响等级进行确认，如相似/系列机型定义的“单个升降舵失效”在不同飞行阶段的影响等级均为 III 类，可在初步建立 FHA 中失效状态影响等级时，将其影响等级初步定义为 III 类。

3.2.2 计算

当飞机气动数据分析完成后，对影响操稳、性能的失效状态进行计算确认；当载荷、强度分析完成后，亦对影响结构的失效状态进行计算确认。如某民机飞控系统失效状态“襟翼/缝翼的单个操纵面偏斜超出结构限制”通过载荷强度计算，评估该失效状态影响等级为 I 级。

3.3 风洞试验

项目早期通过风洞试验对部分飞控系统级 FHA 中失效状态的影响等级进行评估。如某民机在一期风洞试验中规划了“地面扰流板在空中对称打开”失效状态的试验，正常情况地面扰流板在空中是不允许打开的，如果地面扰流板因故障非指令全部打开，其中升力系数和俯仰力矩均明显增加，在正常的飞行迎角范围内，将产生负升力和低头力矩，这在起飞和着陆阶段有安全隐患。根据风洞试验得出的升力系数和俯仰力矩变化，在飞机不同形态下对飞行高度变化和飞行迎角变化进一步分析，地面扰流板空中打开在起飞和着陆阶段是灾难级的，定为 I 级，在襟翼收起的巡航状态是危险的，定为 II 级。

3.4 工程评审

邀请本专业和相关专业及适航等方面的若干资深专家对系统的 FHA 进行工程评审，依据专家丰富的经验对系统级 FHA 中失效状态影响等级的正确性进行判定，这是工程活动中较为常用和适用的确认方法。

3.5 工程模拟器试验

飞控系统级 FHA 中失效状态的影响等级可通过工程模拟器试验进行确认，随着项目进展，参数和模型、气动数据得到了调整、修正和优化后，通过工程模拟器试验对系统级 FHA 失效状态的影响等级进行最终确认。其试验项目可覆盖系统失效状态影响等级为 II、III、IV 类。图 3 为通过模拟器试验方法对失效状态影响等级进行评定的流程图。

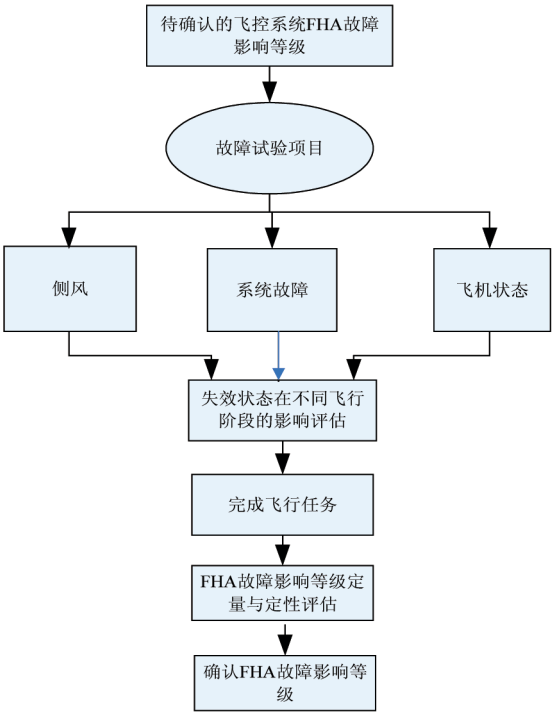

图 3　风挡玻璃夹角和上下边界示图

3.5.1 定量评估

当某一功能失效发生后，飞机可能出现不安全的姿态变化及响应。因此，在充分考虑飞行员延迟时间的基础上，需要在飞控系统失效状态影响等级判定的定量因素方面引入飞机姿态变化等作为对失效状态影响等级细分的定量指标评判依据。

进行 FHA 影响分析时需考虑飞行员延迟时间，飞行员延迟时间应包括意识时间加反应时间加脱开操作的时间。故障试验时，意识时间为故障出现到飞行员感知应当采取行动的时间，识别故障可能是通过飞机的表现或通过可靠的故障警告系统进行的。反应时间为飞行员感知应当采取行动的时间点到飞行员开始采取动作抵消故障影响的时间。反应时间一般如表 2 所示。

表 2　飞行员反应时间参考

飞行条件	反应时间
在地面	1s(＊)
在空中(＜1 000 ft AGL)	1s(＊)
手动飞行	1s(＊)
自动飞行(＞1 000 ft AGL)	3s

注：(＊) 如果需在飞行员之间转换控制权反应时间为 3s。

试验通过在某一飞行阶段下模拟某功能失效且等待一定延迟时间后，对飞机姿态的变化按图 4 流程进行影响等级细分的定量判断。评判方法为：将某一飞行阶段下的滚转角、过载、俯仰角、空速、高度损失、攻角、下沉率等参数，与对应飞行阶段各类影响等级(IV—I 类)的定量判断指标比较，确定该失效状态在某飞行阶段的影响等级。最终按最严酷的飞行阶段影响对该失效状态的影响等级进行确认。

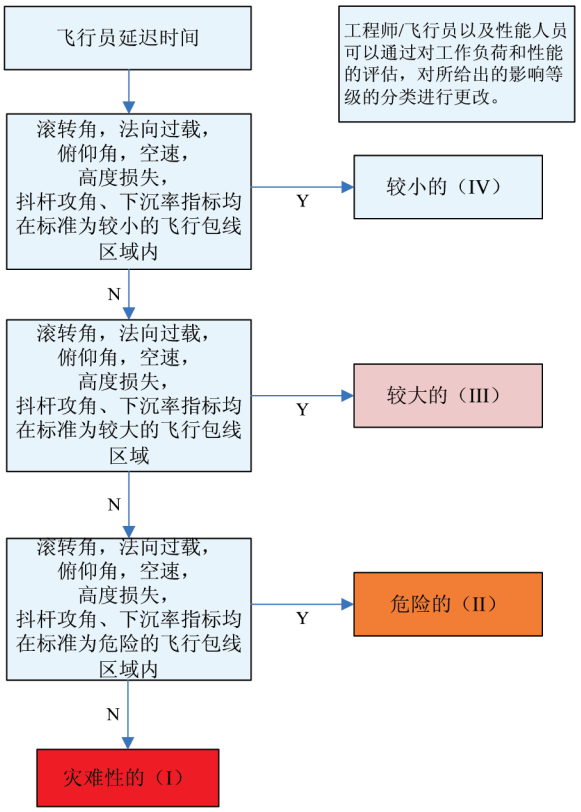

图 4　失效状态影响等级分析定量判断流程

3.5.2 飞行员定性评估

每项试验中，通过模拟发生功能失效且经过延迟时间后，飞行员对飞机姿态变化进行纠正，并通过执行坡度转弯、推拉杆操作、侧风下操作等机动动作，从瞬态响应、操纵性、操纵力、飞机剩余操纵能力、工作负担等方面以检查单形式评估飞机继续安全飞行和着陆的能力，评估该功能失效状态对飞机和机组的影响。系统功能失效状态的影响要结合多次试验的结果、多名飞行员的评价，以及通过工程人员对飞机剩余飞行能力的数据判定综合考虑。

4　案例分析

如某型民机在工程模拟器上进行单块副翼的舵面卡阻试验，对飞控系统级 FHA 中“丧失单个副翼滚转控制功能”失效状态的影响等级进行确认，该条失效状态影响等级为 III 级。飞机以不同指定构型分别在爬升、巡航、下降阶段选取了状态点进行了试验，现以飞机在特定构型要求的下降阶段试验为例，表明该状态点下的评定过程。在飞机特定重量重心，襟缝翼放下，起落架收起，1.23VSR，高度 5 000 ft，下滑状态时，对机组进行该试验点的试验要求为：

1）在飞行员操作飞机下降过程中，在后台注入左侧副翼舵面卡阻故障，使左侧副翼卡阻至某一位置，出现“副翼不工作”EICAS 信息后飞行员等待 1s，进行飞机姿态控制；

2）飞行员按照 AFM“副翼不工作”的非正常程序操纵飞机；

3）飞行员对飞机姿态进行修正，待飞机配平后，进行 60°滚转机动操纵；

4）飞行员操纵飞机，模拟飞机进场-复飞-巡航-进场-着陆的全过程。

该试验点的时间历程曲线图如图 5 所示。

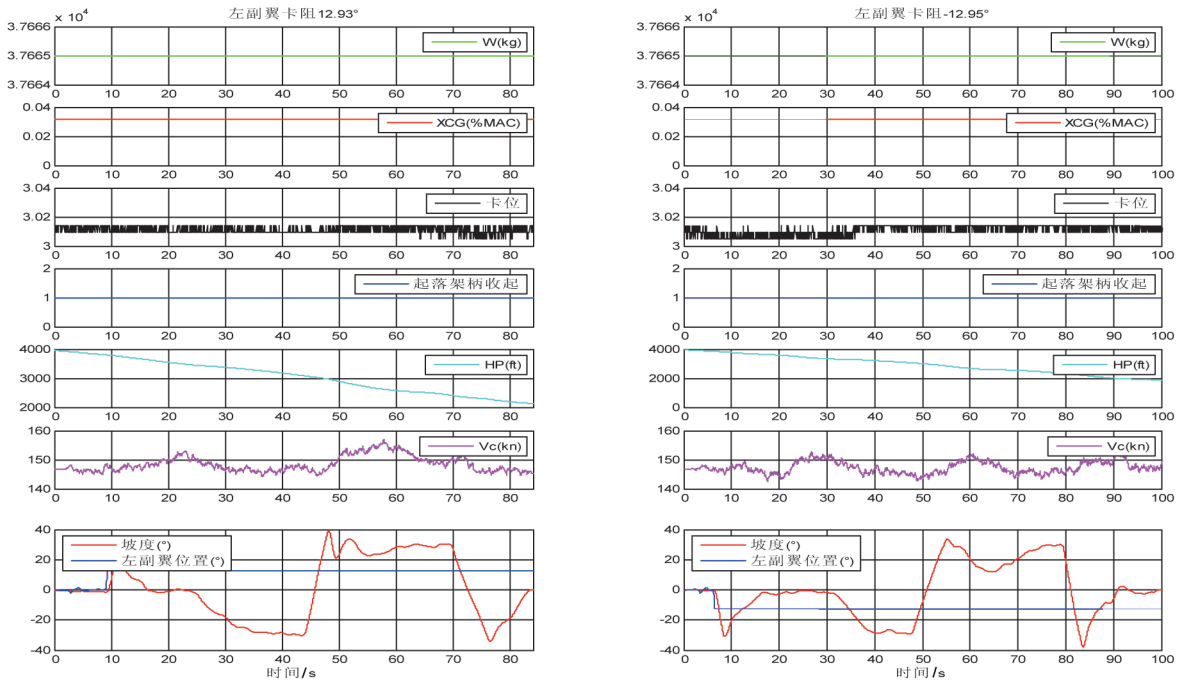

图 5　左副翼舵面卡阻，滚转机动时间历程曲线图

通过对图 4 的具体下降阶段的定量判断流程对该状态点副翼舵面卡阻发生后的飞机姿态变化进行分析，可得出该功能失效状态在下降阶段发生时，对飞机的影响属于较大的（III 级）。

飞行机组对单块副翼舵面卡阻试验的定性评估结果为：

1）故障发生后，可通过剩下的滚转操纵面克服失效带来的影响，飞机仍能继续安全飞行和着陆；

2）单侧副翼漂浮或卡阻以及单侧驾驶盘卡阻后，飞机在后续飞行中具备向左或向右 30°坡度转弯的能力，60°滚转机动时间可接受；

3）为保持飞机正常滚转姿态，明显的增加了飞行员的工作负担，能完成进场 - 复飞 - 巡航 - 进场 - 着陆的全过程；

4）飞行员对该失效状态影响等级的评分为 IV 级。

综合所有试验状态下定量判断和定性评估的结果，FHA 中给出的“丧失单个副翼滚转控制功能”失效状态影响等级为 III 级是正确的，即完成了对其的工程模拟器试验确认工作。在飞机后续的研发飞行试验中，也对该失效状态的影响等级进行了试飞验证，其结果与 FHA 中所定义的等级一致，最终获得了局方认可。

5　结论

本文在实际型号经验并分析了大量相关资料

的基础上,整理得出适用于民机电传飞控系统的功能定义、功能失效状态分析和确定功能失效影响等级并对其进行确认的思路和方法,以保证民机电传飞控系统级 FHA 正确性和完整性。该方法已应用到某民机电传飞控系统级 FHA 的设计及评估工作中,取得了良好的效果,并获得了适航审定方的认可。

参考文献:

[1] SAE ARP4754A Guidelines for Development of Civil Aircraft and System[S]. SAE,2010,12.

[2] SAE ARP 4761 Guideline and Methods for Conducting the Safety Assessment Process on Civil Airborne System and Equipment[S]. SAE,1996,12.

[3] AC/AMJ 25. 1309-1B System Design and Analysis[S]. USA: FAA, 2002.

[4] AC25-7C Flight Test Guide For Certification Of Transport Category Airplanes[S]. USA: FAA, 1998.

[5] AC25. 672-1 Active Flight Controls[S]. USA: FAA, 1983.

[6] 孙泽鹏,张昊. 民用飞机的功能定义及方法研究[J]. 广东科技,2015,24(10):46 -49.

[7] 李亚男,金平,王兴波. 民用飞机飞行控制系统失效状态等级确认方法分析[J]. 民用飞机设计与研究, 2013(S2):77.

[8] 孙有朝,刘建军,梁力,等. 功能危险分析在民机安全性设计中的应用研究[C]//. 中国航空学会,中国工程院机械与运载工程学部. 大型飞机关键技术高层论坛暨中国航空学会,2007 年学术年会论文集,2007,7.

作者简介

王晓梅　女,工程硕士,高级工程师。主要研究方向:民机系统功能危害性评估和飞控系统需求确认;E-mail:wangxiaomei@comac.cc

龚孝懿　男,硕士,高级工程师。主要研究方向:民机飞控系统安全性分析;E-mail:gongxiaoqi@comac.cc

李　棋　男,硕士,工程师。主要研究方向:飞控系统模拟器试验和试飞运营保障;E-mail:liqi5@comac.cc