DOI：10.19416/j.cnki.1674－9804.2016.03.017

民机电传飞控系统安全性设计与验证

The Safety Design and Verification of Fly by Wire Flight Control System for Civil Aircraft

唐志帅　刘兴华 / TANG Zhishuai　LIU Xinghua
（上海飞机设计研究院，上海 201210））
（Shanghai Aircraft Design and Research Institute，Shanghai 201210，China）

摘　要：
目前 CCAR25 部的规章要求主要针对传统机械操纵飞机，随着电传飞控系统（Fly by Wire，以下简称 FBW）在现代民机上的广泛应用，在控制指令的数字信号完整性、AC 25.1309 等效安全等方面产生了一些新的适航要求，以达到传统设计相同的或等效的安全水平。介绍了民机电传飞控系统安全性评估过程，然后针对电传飞控系统安全性设计特点，总结了适用的适航要求和符合性验证方法。

关键词：电传飞控系统；安全性评估；适航；验证
中图分类号：V249.1　　**文献标识码：**A

[**Abstract**] The regulations and requirements of current CCAR 25 aim at the traditional aircrafts which use mechanical flight control system. With the widespread use of Fly-by-Wire (FBW) flight control system, some new airworthiness requirements are generated about the integrity of digital signals, and AC 25.1309 provisions, in order to achieve the same or equivalent safety level of traditional design. This paper introduces the FBW safety assessment process of civil aircraft, and the applicable airworthiness requirements and verification methods were presented based on the features of FBW safety design.

[**Keywords**] fly-by-wire flight control system；safety assessment；airworthiness；verification

0　引言

民机的发动机除了为飞机提供正/反推力外，还为飞机上的液压、气压等次级功率系统提供源动力。多种次级功率的存在造成飞机上接口繁多，可靠性、维修性较差，使用成本增高。因此多电飞机技术的研究成为飞机发展的重要方向，目前国内外最新的民用飞机（例如 A320/A350/A380/波音 777/波音 787 等）大多安装了电传飞控系统，不仅驾驶舱操纵设备和飞控电子设备实现了多电或全电，作动系统也越来越多地使用机电作动器（Electromechanical Actuator，以下简称 EMA）替换之前的液压作动器。例如 A380 飞机的副翼/方向舵/升降舵/平尾，均采用了电备份，当丧失所有液压源时，仍可通过 EMA 完成俯仰和滚转方向的控制。

对于采用 FBW 飞控系统的安全性设计，需捕获飞机级和适航规章中的安全性需求，通过功能危险性评估（Functional Hazard Assessment，以下简称 FHA）和初步系统安全性评估（Preliminary System Safety Assessment，以下简称 PSSA）等安全性评估过程将定性和定量的需求分解到飞控系统各软硬件[1]。然而，针对传统机械操纵飞机所制定的适航规章要求（例如 CCAR 25.1309）已不能完全适用于电传飞控系统。根据近年来国内外适航当局的研究成果，针对 FBW 的特点也产生了一些新的适航要求，这些新的适航要求及其符合性验证方法成为了当前研究的热点。

1　FBW 安全性评估过程

飞控系统设计中的安全性工作是飞机级安全性工作的继续。SAE ARP4761 提供了民用飞机机载系统和设备在合格审定过程中进行安全性评估的指南和方法，其主要用于表明对 25.1309，25.671 等适航条款的符合性[2]。

安全性评估内容主要包括 FHA、PSSA 和系统安全性评估(System Safety Assessment,以下简称 SSA),其分析方法包括故障树分析(Fault Tree Analysis,以下简称 FTA)、失效模式与影响分析/摘要(Failure Modes and Effects Analysis/Summary,以下简称 FMEA/FMES)和共因分析(Common Cause Analysis,以下简称 CCA)。图 1 给出了飞机研制周期内安全性评估与系统研制过程的关系。

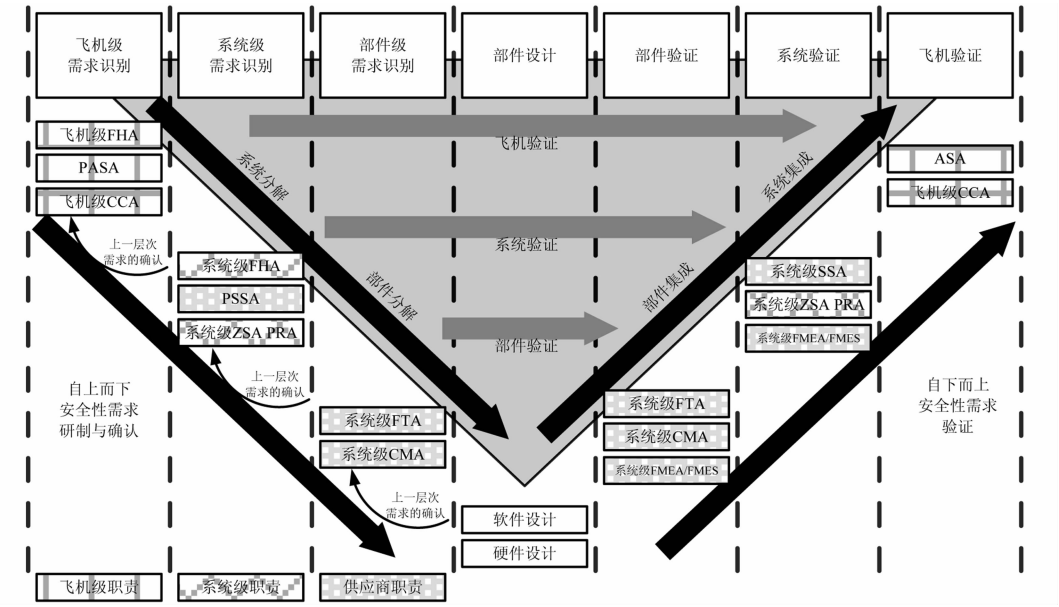

图 1　安全性评估与系统研制过程的关系

FHA 在飞机/系统研制开始时进行,此工作应识别功能及功能组合相关的失效状态并进行影响等级分类,建立相应的安全性目标。FHA 的目的在于识别所有失效状态,明确其影响等级和进行等级分类的基本理由,它的输出是 PSSA 的起点。

飞机级/系统级功能定义是飞机级/系统级 FHA 的重要输入。一般情况下飞机级功能可划分为飞机基础功能(外部功能)、功能和子功能等三个或四个功能级别。系统级功能可分为一个或两个层级,第一层级为系统功能,可根据飞机级子功能完成定义;第二层为系统级子功能,可根据系统复杂程度确定是否需要定义。图 2 给出了功能层级划分的说明。

飞机级 FHA 可选择图 2 第二/三层功能定义,这样能将 FHA 的失效状态总数控制在一个合适的量级,同时兼顾组合失效的影响。如果选择第四层功能开展 FHA,由于这一层飞机级子功能已涉及到具体的系统功能,因此难以覆盖各系统之间组合失效的情况。

PSSA 对所建议的系统架构进行系统性检查,建立系统的安全性要求,并确定所建议的系统架构能够满足 FHA 识别的安全性目标。SSA 是对所实现的系统进行系统性和全面的评价,以表明满足从 FHA 得到的安全性目标以及从 PSSA 得到的衍生安全性要求。

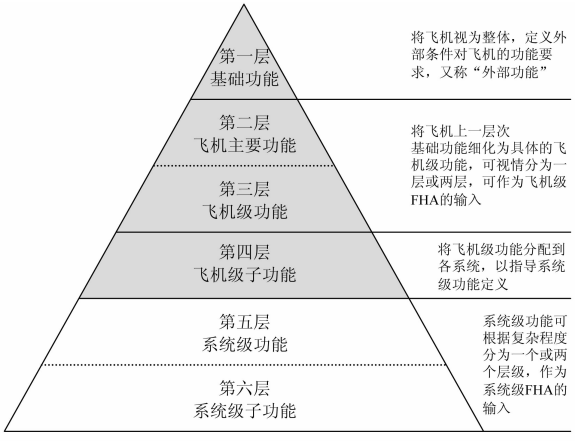

图 2　飞机和系统功能层次与 FHA 的关系

CCA 应通过评价整个架构对共因事件的敏感度,支持系统架构的设计。这些共因事件通过完成下列分析来进行评价:特定风险分析(Particular Risk Analysis,以下简称 PRA),共模分析(Common Mode Analysis,以下简称 CMA)和区域安全性分析(Zonal Safety Analysis,以下简称 ZSA)。

当为 PSSA 或 SSA 进行 FTA 时,维修任务相关的故障检测方法和暴露时间必须与飞机级规定的维修任务和时间间隔相一致。安全性评估过程不

只是定量的，也包括研制保障等级、HIRF/Lighting要求等定性内容。

2 FBW 安全性设计的特点

2.1 飞控系统数字信号完整性问题

传统的飞控系统采用机械或液压－机械方式将指令信号传输到各控制舵面。其失效模式数量有限且相对简单(如卡阻、脱开等)，因此能够相对直接地确定干扰指令传输的原因。但电传飞控系统包含数字设备、软件和电子接口，可能受到来自内/外部的干扰源的影响(例如数据位的丢失、传输延迟、电磁干扰等)。同时考虑到 FBW 系统设备的复杂性，失效模式也不像传统机械控制系统那样，容易被分析和处理。

现行 CCAR25.671 和 25.672 等条款没有对指令信号完整性做出专门要求[3]。因此为了保持与现行 CCAR25 部等效的安全水平，适航当局通常会要求 FBW 在设计时，应该使用特殊的设计手段使系统完整性保持在至少等效于传统的液压－机械设计所具有的安全水平。

2.2 25.671 条款的修正案

25.671 条款用于确保飞控系统的基本完整性和可用性，确保服役过程中发生的任何失效都是飞行机组能处理的，并不会妨碍飞机持续安全飞行和着陆。但其要求主要针对传统机械操纵飞机，部分要求对于 FBW 不能完全适用。

2002 年，FAA 下属的一个飞控协调工作小组递交了关于 25.671 条款修订的新提案以及相关的 AC 咨询材料。对飞机非正常姿态恢复、防止维修差错、飞控卡阻和失控、所有发动机失效情况下的可控性、操纵权限极限位置的飞行机组告警等提出新的适航要求[4]。

例如修正案中提出当已存在单个卡阻情况下，任何额外的、能够妨碍持续安全飞行和着陆的失效状态，其组合概率应小于 1/1 000；飞机必须设计成所有发动机在飞行中的任何点全部失效的情况下仍可操纵。这些新的适航要求应落实到系统安全性分析和架构设计中去。

2.3 25.1309 的等效安全说明

FAA 于 2003 年 4 月 29 日在《联邦注册报》上刊登了一则关于 FAA 的航空规章制定咨询委员会的建议稿(针对 25.1301 和 25.1309 条拟议的改动)的通告。此建议稿被认为是一种对现有的 25.1301 条和 25.1309 条的改善，不会显著地增加申请人额外的符合性验证成本，并且有益于 FAA/EASA 清晰的协调指南。

鉴于当前 CCAR 25.1309 与 FAA 的 ARAC 建议的规章 FAR 25.1309 修订稿和 EASA 现行规章 CS 25.1309 中的要求存在差异，为了同时符合 FAA/EASA/CAAC 关于系统安全性的规章要求，可使用以下等效安全说明[5]。

1)飞机的设备和系统必须设计及安装成：

①那些型号合格审定或运行规则所要求的，或者其功能不正常将降低安全性的系统或设备能在飞机运行和环境条件下执行预定功能；

②其它设备和系统不会对飞机或其乘员，或者对 1)①中所覆盖系统或设备的正常工作造成不利的安全性影响。

2)飞机系统和相关组件，在单独考虑或与其它系统一起考虑时，必须设计和安装成：

①每一个灾难性的失效条件

i. 是极不可能的；并且

ii. 不会由单个失效造成；并且

②每一个危险的失效条件是极小可能的；并且

③每一个重大的失效条件是很小可能的。

3)有关系统不安全工作情况的信息必须提供给机组，以使得他们能够采取适当的纠正行动。如果需要立即采取纠正行动，则必须提供警告指示。包括指示和通告在内的系统和控制必须设计成尽量使可能导致额外危险的机组错误降至最低。

3 FBW 的符合性验证

针对本文第二节 FBW 特点提出的新的设计要求，应建立相应的符合性验证方法。

3.1 飞控系统数字信号完整性问题

采用 FBW 的飞机，在系统架构和监控设计时，应充分考虑“指令信号完整性”问题所带来的挑战。在进行符合性验证时，可对系统架构设计进行安全性分析，表明设备故障、内部和外部干扰导致的系统失效可满足相应的概率要求。

同时有必要通过鉴定试验、铁鸟试验等表明飞控系统在预期环境下均可正常工作。结合铁鸟试验、飞行试验和模拟器试验的分析结果表明其符合性。

3.2 25.671 条款的修正案

对于“25.671 条款的修正案”的符合性验证，可采用描述和分析的方法，表明飞控系统操纵器件操作简便，相应的机组告警设计符合要求；飞控系统

的零部件在设计上采取措施能有效防止维修差错。

可通过描述分析和模拟器试验的方法，表明飞控系统在所有发动机都失效情况下的电源/液压源/作动器配置，仍可提供操纵能力。

3.3 25.1309 的等效安全说明

对于“25.1309 等效安全说明”各条款，可通过系统描述来表明飞控系统的设计能够保证在飞机运行和环境条件下完成预定功能，系统故障后可通过简图页、EICAS 信息、PFD 信息将系统的不安全工作情况提供给机组，系统已根据故障的紧急程度设置不同的告警级别。

可通过安全性分析的方法来表明飞控系统发生灾难性失效条件的概率为极不可能（≤1E-9/FH），发生危险失效条件的概率是极小可能的（≤1E-7/FH），发生重大的失效条件是很小可能的（≤1E-5/FH）。

4 结论

本文介绍了民机电传飞控系统的安全性评估过程，重点说明了需开展的安全性活动及飞机/系统功能层级划分原则。然后针对 FBW 安全性设计特点，总结了适用的适航要求及对应的符合性验证方法。

参考文献：

[1] Society of Automotive Engineers. ARP4754A Guidelines for Development of Civil Aircraft and Systems [S]. 2010.

[2] Society of Automotive Engineers. ARP4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment [S]. 1996.

[3] 中国民用航空局. CCAR25-R4 运输类飞机适航标准 [S]. 北京：中国民用航空局，2011.

[4] Federal Aviation Administration. FAR/JAR 25.671 FCHWG-ARAC Report (Includes Rule, Advisory Material, & Alternate Recommendations) [R]. 2011.

[5] Federal Aviation Administration. AC 25.1309-1A-System Design and Analysis [R]. 1988.

（上接第 35 页）

离散程度），而 9 名航线飞行员的平均工作负荷为 46.7（SD = 20.8）。从统计结果可以看出，航线飞行员评估的机组工作负荷要大于试飞员。又如，在评估场景“人工手动飞行”中，传统杆飞行员认为评估机型杆力适中，略微偏重；而侧杆飞行员则认为评估机型杆力偏重，工作负荷较大。

通过评估结果可以发现，各类飞行人员因其背景和经历的差异，其工作负荷也存在差异，这就意味着在选择评估机组时，为更准备地体现设计机型在相应场景下的机组工作量，需要同时考虑选择试飞员和航线飞行员，同时他们的人数也应该相近，这样才能代表完整的飞行员群体。同时，最小机组工作量评估中各类飞行员所反映的问题和意见，对于机组操作程序和飞行员培训手册等的改进和完善都是重要的参考。

4 结论

本文针对民用运输类飞机机组工作量评估中的评估机组选取问题展开研究。重点讨论了各类飞行人员的服役经历和资质的差异，分析了其在最小机组工作量评估中的作用和差异。同时，针对规章所要求的“能够反映中等技巧的飞行机组的工作量水平”，提出了一套切实可行的评估机组选取原则和方法。该方法对于最小机组工作量型号审查活动的开展，以及后续的机组操作程序、飞行员培训手册等的改进和完善都具有较好的指导作用。

参考文献：

[1] J. C. Geddie, L. C. Boer, R. J. Edwards, and et al., NATO Guidelines on Human Engineering Testing and Evaluation [S]. North Atlantic Treaty Organization, RTO-TR-021, 2001.

[2] 中国民航局. CCAR-61-R4 民用航空器驾驶员和地面教员合格审定规则[S]. 北京：中国民航局，2014.

[3] C. D. 威克斯，J. G. 霍兰兹. 工程心理学与人的作业 [M]. 朱祖祥，等译. 上海：华东师范大学出版社，2003.

[4] 中国民航局. CCAR-25-R4 中国民用航空规章第 25 部：运输类飞机适航标准[S]. 北京：中国民航局，2011.

[5] Federal Aviation Administration. Minimum Flight Crew, AC25.1523－1[S]. US：FAA，1993.

[5] Federal Aviation Administration. Minimum Flight Crew, AC23.1523[S]. US：FAA，2005.

[6] William H. Corwin, and et al.. Assessment of crew workload measurement methods, techniques and procedures：AD-A217-699, Vol. I[S]. 1989.