机载设备研制阶段的适航性分析与验证*

Airworthiness Analysis and Compliance for Airborne Equipment Development

空军北京局125厂代表室　于　静
空军工程大学装备管理与安全工程学院　郑　磊　胡剑波　张　磊

于　静
空军北京局125厂军事代表，从事装备质量、安全与检验等研究工作。

机载设备适航性就是将机载设备安装在军用航空器上时要保证航空器能够适合飞行、保证航空器飞行安全性的能力，是验证机载设备确保航空器具有安全飞行能力的检验准则。

机载设备适航性的分析与验证是为了检验机载设备是否满足航空器对机载设备的技术性能和安全性要求，既要保证其分析方法正确有效，更要保证其验证方法可靠、结论可信。事实上，航空器为了提高其飞行性能经常要采用一些新技术、新工艺、新材料或者新理论，有些会落实到具体的机载设备上，如全球定位系统、高性能数据链设备等。我们注意到尽管这些设备是为了提高航空器的性能指标，但其同样关系到航空器的飞行安全，如全球定位系统的故障可导致飞机偏离航线、数据链设备故障可导致飞机引导能力降低，危及航空器的生存能力。为此，必须深刻思考机载设备的适航性，这也反应了机载设备对保障飞行安全的重要性。

航空器机载设备一般要求能够适应航空器运行所处环境因素的极限条件，包括载荷、耐热度、温湿度、恶劣天气以及复杂电磁环境等，即航空器首先要求其机载设备具有满意的适航性，以使航空器满足其安全基线要求。本文将重点研讨机载设备适航性的分析与验证等问题，并就如何开展其分析与验证工作进行研讨。

* 工业控制技术国家重点实验室项目（ICT1447）资助。

机载设备适航性的基本内涵

1 适航性

依据牛津词典的解释，适航性（Airworthiness）即适于飞行。美国科学院在1980年出版的《改进航空安全性》一文中指出：适航性是“在预定的使用环境中和在经申明并被批准的使用限制之内运行时，航空器（包括其部件和子系统、性能和操纵特点）的安全性和物理完整性”。中国民用航空局发布的CCAR-25部中也定义了适航性[1]：“民用航空器的适航性是指该航空器包括其部件及子系统整体性能和操纵性能在预期的使用环境和使用环境下的安全性和物理完整性的一种品质。这种品质要求航空器应始终处于保持符合其型号设计和始终处于安全运行状态。”可见，适航性要求从飞机级的

角度提出以安全为向导的设计与验证要求，其确定的是飞机级的适航性基线，形成的是型号的适航性审查基础，同时，适航性要求还需分解落实到相关的系统研制要求中，作为系统的适航性验证技术依据[2]。

综上所述，适航性是航空器的固有特性，必须通过其全寿命周期内设计、制造、使用和维护等各个环节来实现和保持，同时，适航性也是民用航空器安全性的代名词，是航空安全技术发展的产物。

2 机载设备适航性及其分类

机载设备具有适航性是航空器适于飞行的前提。机载设备适航性就是将机载设备安装在军用航空器上时要保证航空器能够适合飞行、保证航空器飞行安全性的能力，是验证机载设备确保航空器具有安全飞行能力的检验准则。机载设备满足适航性要求就是要保证机载设备具有良好的工作性能和安全性设计，使其在恶劣的环境条件下能够维持良好的性能和安全性水平。可见，合理的设计、制造以及安全验证方法选择等均是保证机载设备适航性的重要基础，也是适航管理核心和审查准则。

机载设备适航管理主要包括全寿命管理、全领域管理、全过程管理、全方位管理等，机载设备适航性贯穿其整个寿命周期，各个性能参数都必须满足适航要求，且必须经过适航审查确认满足相应的适航标准后，方可获得使用方认可。机载产品适航管理分为初始适航和持续适航[3]两大类。

机载设备初始适航是对机载设备设计和制造的控制，是在机载设备交付使用之前，使用方依据各类机载设备适航标准和规范，对其设计和制造进行的型号合格审查、生产许可审查，以确保机载设备的设计、制造是按照机载设备适航性要求的规定进行的。

机载设备持续适航是对机载设备使用和维修的控制，是在机载设备满足初始适航标准和规范、满足机载设备设计要求，符合审查基础，投入运行后，为保持它在设计制造时的安全基准或适航水平，为保证机载设备能够始终处于安全运行状态而进行的管理，初始适航和持续适航是密不可分的一个整体。

机载设备研制阶段适航性分析与验证的基本流程

图 1 为机载设备研制阶段适航性分析与验证的基本流程，反映了机载设备在研制阶段中所开展的适航性工作内容。机载设备适航性工作从航空器的构型、用途和使用环境条件等需求分析开始，需要经历适航性分析、适航准则剪裁、适航性要求生成、适航性设计和适航性验证等过程，并且伴随着适航审查工作，不断地进行适航性分析、设计和验证的迭代，直至机载设备满足其适航性要求。

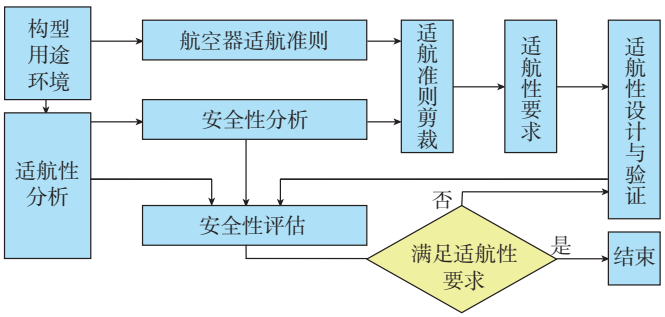

图1 机载设备研制阶段适航性分析与验证的基本流程

从图 1 所示的适航性分析与验证流程可见：该流程的输入是航空器构型、用途和环境等需求，输出为适航符合性结论。首先，需求一方面对照相关的适航性准则，获取适航性的基线要求；另一方面进行机载设备适航性分析，通过机载设备的安全性分析和安全性评估，获取适航性的具体要求。进一步，便可依据适航性基线要求、安全性分析结果和安全性评估结论，得到机载设备适航性要求。之后，研制单位将适航性要求转化为设计要求和验证方法，开展机载设备适航性设计和适航符合性验证。此后，由适航审查人员对机载设备进行适航性审查，如果审查结果存在不符合项目，需要研制单位采取技术手段进行重新设计和验证，直到满足适航性要求为止。

值得注意的是，审查人员不只是对适航性设计及验证结果进行审查。在整个适航准则剪裁、安全性分析与评估和适航性要求生成等各个环节，均要开展相应的适航性取证、评审和考核等适航审查工作。

机载设备适航性分析

在研制阶段，机载设备适航性分析是指利用系统安全性分析方法，识别并评估机载设备在运行环境、使用条件和自然环境下的各种危险源，开展功能危险分析、故障树分析和区域风险分析，进而得到适航性要求。可见，适航性分析是机载设备适航性工作的重要基础，而其核心在于安全性分析和安全性评估。

1 安全性分析

在机载设备安全性分析中，经常用到以下 4 种安全性分析方法：功能危险分析（FHA）、故障模式及影响分析（FMEA）、故障树分析（FTA）和共因故障分析（CCA），这 4 种方法密切联系，相互补充。

（1）功能危险分析（FHA）：系统、综合地检查机载设备的各种功能，识别各种功能故障状态，并根据其严重程度对其进行分类的一种安全性分析方法（或过程）。FHA 用来

从系统的角度来确定机载设备安全性设计目标，帮助决定设计方案的可接受性，发现潜在的问题和所需的设计更改，确定所需的进一步分析的要求及范围。FHA 在安全性分析工作的前期进行，用于建立机载系统总体安全性要求，需要考虑系统功能、功能失效模式、危险组成、工作状态、系统外部交联和人为因素等诸多要素。

（2）故障模式与影响分析（FMEA）：在产品的设计过程中，通过对产品各组成单元潜在的各种故障模式及其对产品功能的影响进行分析，提出可以采取的预防改进措施，以提高产品可靠性的一种设计方法。FMEA 是一种系统地、自下而上的识别系统、单元与功能的故障模式并确定其对上层影响的方法。FMEA 可以在系统的任一层次上进行（如零件、功能等）。通过 FMEA 可以确保所有零部件的各种故障模式及影响都经过周密考虑，找到对系统故障有重大影响的零部件和故障模式并分析其影响程度，提出各类危险的预防措施。通常 FMEA 用来分析单一故障的故障影响。由于进行 FMEA 分析需考虑产品结构、组成等因素，因此 FMEA 在系统的详细设计阶段方能进行。

（3）故障树分析（FTA）：在系统设计过程中，通过对可能造成系统故障的各种因素进行分析，画出逻辑框图，从而确定系统故障原因的各种可能组合方式并计算系统故障概率，采取相应的纠正措施，以提高系统可靠性的一种设计分析方法。FTA 是一种自上而下的分析方法，其可以分析不可预见的硬件故障、人为差错有关的故障事件，以及由此导致的不希望发生的其他相关事件。FTA 既可用于定性分析又可用于定量分析。通过 FTA 可以确定系统故障原因或原因组合，获得系统故障发生概率（定量分析时），求得组成系统的各个零部件的重要度。与 FMEA 相比，FTA 可以对组合失效进行分析。

（4）共因故障分析（CCA）：用于分析复杂系统的共因故障及造成的危害。CCA 包括特殊风险分析（PRA）、共模故障分析（CMA）与区域安全性分析（ZSA）3 种分析方法。

特殊风险分析：PRA 主要是分析系统外部的事件或因素对飞机或系统的影响，如泄漏物、飞禽撞击、雷电、高强度辐射等，这些事件是造成共因失效的重要原因。PRA 总体分析过程是逐个为被研究的特定风险建立一个合适的失效模式，确定受影响的区域以及评审特定风险的后果。共模故障分析：CMA 是分析共因事件对余度设计影响的重要方法，其主要分析故障树分析中“与门”输入事件的独立性，CMA 分析内容涵盖了设计、制造和维修失误以及相同软硬件故障等方面。区域安全性分析：ZSA 主要是分析设备安装、故障对邻近系统或结构的影响，避免相邻系统之间相互干涉以保证系统达到安全要求。ZSA 是抑制共因失效产生的重要措施，由于要判断系统各区域物理功能上是否相关，必须明确系统的组成与结构，因此 ZSA 在详细设计阶段才能进行。

2 安全性评估

在研制阶段，安全性评估就是要评估安全性分析的各种危险源影响程度，将安全性评估过程分为 3 个步骤 [4]：功能危险分析（FHA）、初步系统安全性分析（PSSA）和系统安全性分析（SSA）。

（1）功能危险分析：这里将功能危险分析作为安全性评估过程中的一个子过程来看待。在该过程中需要借助 FHA、PRA 和定性 FTA 安全分析方法。FHA 的特点是在系统设计的初期便可以进行，并且一般作为民机设计评估的第一步。在飞机 / 系统研制周期的初始要进行一次功能危险分析（整机级 FHA），查明与飞机功能及功能组合相关联的故障状态并对其进行分类。PRA 则作为 FHA 的补充，对 FHA 分析不到的特殊风险进行分析。随着设计过程中飞机的功能被分配到各个系统，可利用 FTA 自上而下的分析特点，将整机级的安全性要求分配到系统级，并利用 FHA 检查每一个综合了多项功能的系统（系统级 FHA）。此时的 FHA 应调整为考虑分配到该系统的单个功能或其组合。系统级 FHA 的输出将成为 PSSA 的起始点。

（2）初步系统安全性评估：该步骤主要用到定性 FTA 和 CMA。同样利用 FTA 自上而下的分析特点，将系统级的安全性要求分配到各分系统。CMA 则用以分析冗余系统的共模故障情况。PSSA 是对初步拟定的系统结构进行的一次系统的检查，以便判明故障是如何引起 FHA 所确定的功能危险的。PSSA 的目标是建立系统的安全性要求并判断拟定的系统结构是否有足够的理由表明它可以满足 FHA 提出的安全性目标。

（3）系统安全性评估：该步骤主要用到 FMEA、定量 FTA、CMA 及 ZSA 安全性分析方法。SSA 综合各种分析结果用以确认整个系统的安全性，SSA 要求把所有的在 PSSA 中识别的具体安全性要求都考虑进去。SSA 文档包括相关分析结果和必要的说明，通常包括外部事件概率、系统描述、故障状态及分类、故障状态定性及定量分析、共因分析等信息。

单元 FMEA 实施并总结为故障模式与影响摘要（FMES），用以支持在单元 FTA/CCA 中考虑的对应于故障模式的故障率。系统级 FMEA 总结为系统级 FMES，用以支持在系统级 FTA 中考虑的对应于故障模式的故障率。通过与整机级 FHA 相比较，整机级 FTA/CCA 被用来建立与整机级故障状态和故障概率的相符和一致性。安全性评估各步骤、各阶段的分析成果需要形成文档。这些文档可以作为适航符合性验证的重要支

撑材料。

机载设备适航性验证

在研制阶段，验证就是对适航条款中要求的“失效”、“故障影响”、“概率极小”、“危害最小”等要求进行验证。从前面的介绍可以看出，安全性分析、评估主要用于确定系统的危险源及其影响，而验证选择要进一步确认实际系统的安全性水平是否符合适航条款的要求，三者之间显然有共通之意，是一种递进关系。符合性验证是指采用各种验证手段，以验证的结果证明所验证的对象是否满足航空器适航审查基础要求[5]。一般地，型号审查基础由必要的、足够的且适用的航空器适航准则和该型号设计增加的专用条件组成。

1 验证方法

在研制阶段，出于航空器型号审查需要，研制方必须获得所需的证据资料以向审查方表明产品对于适航条款的符合性，可以采用不同的方法进行说明和验证，这些方法统称为符合性验证方法[6]。

常用的符合性验证方法可根据实施的符合性工作的形式分为四大类[7]：工程评审、试验、检查和设备鉴定。根据这四大类方法再具体进行细化，最终形成了常用的、经实践检验的、适航部门认可的10种符合性验证方法，常用的符合性方法表1所示。

2 验证任务

在研制阶段，适航符合性验证围绕着设计验证、制造检查、产品验证3个基本阶段来展开[2]。根据各阶段验证工作需要，可以采取多种不同方法来实施适航验证任务。

（1）设计验证：设计验证阶段的主要任务是验证设计（方案、原理、功能等）是否满足适航性要求，其验证结果可以判断设计符合性。

（2）制造检查：检查产品制造与设计的一致性，采用的方法主要是产品检验、重要工序的检查以及机上检查等，各项检查工作的结果表明的是制造符合性。

（3）产品验证：验证产品（试验机/试验件）是否满足适航性要求，采用的方法主要有试验室试验、机上试验、飞行试验、模拟器等。与设计验证不同，产品验证阶段的符合性验证是针对实体产品进行，验证结果表明产品的符合性。

结论与建议

（1）加强安全性分析与评估工作，固化适航性要求生成机制。随着型号研制适航工作的不断深化和有序推进，机载设备适航性要求的生成已经成为型号研制的强制性工作。为此，需要加强系统安全性分析和评估工作，固化适航性要求生成机制，使适航审查准则编制、适航性要求编制以及适航审查等均可做到“有理有据、有章有法”。

（2）深化适航理论研究、优化和重组航空主干专业设置。机载设备种类多、数量多，其适航性工作必然带来大量的审查工作。尽管目前机载设备的适航审查任务日益艰巨，但是能担当适航审查任务的人员较少。为此，需要加强适航理论研究，深刻领会适航理念对机载设备适航性的挑战、优化和重组航空主干专业设置，满足机载设备适航工作不断推广的需求。

（3）统筹适航验证资源，加强机载设备适航符合性验证条件建设。适航符合性验证需要试验设备、场地和基础设施的支撑。目前，机载设备适航验证资源有限，还不能满足适航符合性验证任务的需要。一方面要统筹验证资源，充分发挥现有资源的利用率；另一方面要科学论证适航符合性验证需求，加强投入，建设一批急需的机载设备适航符合性验证试验室。

（4）加强与国外适航机构的交流，培养机载设备适航审查和验证专业人才。机载设备适航与验证专业人才是推进适航工作的重要力量。目前，我国航空适航工作不但需要大量的适航审查人员，更需要优秀的适航性验证人才。为此，急需加强与国外适航机构的交流，总结借鉴国外的先进适航理念、技术和经验，建设完善的适航人员培养渠道，加强机载设备适航审查和验证专业人才建设。

表1 适航验证方法

符合性工作	方法编码	符合性验证方法	相应文件
工程评审	MC0	符合性声明 ----- 引用型号设计文件 ----- 公式、系数的选择 ----- 定义	型号设计文件 符合性记录单
	MC1	说明性文件	说明、图纸、技术文件
	MC2	分析/计算	综合性说明和验证报告
	MC3	安全评估	安全性分析
试验	MC4	试验室试验	试验任务书
	MC5	地面试验	试验大纲
	MC6	试飞	试验报告
	MC8	模拟器试验	试验结果分析
检查	MC7	航空器检查	观察/检查报告 制造符合性检查记录
设备鉴定	MC9	设备合格性	设备鉴定过程可能包括前面所有的符合性验证方法

本刊共有参考文献7篇，因篇幅所限未能一一列出，如有需要请向本刊编辑部索取。

（责编 小城）