飞机系统安全评估技术的发展

Overview of Aircraft System Safety Assessment Technique

西北工业大学自动化学院　李爱军　武　坚　王长青

随着科学技术的发展，飞行器的复杂性大大提高，飞机系统越来越复杂，各系统间的交叉关联也越来越多，飞机系统的安全性和适航性愈加受到重视。飞机系统的安全性评估不再仅限于完成基本评估内容，还要考虑由于系统的高度综合、系统的复杂性、软硬件的相互作用而产生的新问题。

李爱军

工学博士，西北工业大学自动化学院教授，2005 年和 2007 年分别在美国伊利诺伊大学（UIUC）和加州大学（UCSB）做访问学者。2008 年 6~12 月，在中国商飞工作，参与了大型客机 C919 电传飞行控制系统的论证设计工作。主持“863”创新项目 2 项，航空基金项目 1 项，参与科研项目 10 多项，现已发表学术论文 60 余篇，其中 EI 索引 15 篇，出版教材和专著 4 部，编写讲义 2 本。目前主要研究领域包括航空飞行器控制系统设计与仿真、智能控制理论及应用、自适应控制等。

安全性是通过设计赋予的一种产品特性，是航空航天飞行器设计必须满足的首要特性。“系统安全”概念于 20 世纪 60 年代正式引用，它要求在系统的寿命周期中都应识别、分析和控制危险，强调在系统设计阶段应把可接受的安全性水平设计入系统中，以保证系统在以后的试验、制造、使用、保障和退役处置中都是安全的。现行的美军规范“MIL-S-38130 军用规格系统，次系统级装备的一般安全需求”提出：系统安全是在有限的时间、成本以及操作环境中，运用工程与管理的原理、原则以及技术使系统达到最佳的安全境界，最终足够安全投入使用（Release To Service）[1]。

飞机系统安全评估是对系统存在的危险进行定性和定量的分析，得出系统发生危险的可能性及其程度的评估，以寻求最低事故率、最少损失和最优安全投入收益。对于民机来说，要求安全、舒适、经济、环保，其中安全始终是第一位的，适航标准就是国家对民用航空产品制定的最低安全标准[2]。为了使民机在设计过程中同时满足安全舒适的要求，以及在适航审定过程符合要求，国外已经提出了相应的适航符合性验证流程来评估飞机的安全性。

飞机系统安全评估技术的发展

航空航天飞行器安全性技术的发展大致可划分为如下 4 个阶段。

1　20 年代初期至 40 年代前期：飞行安全概念形成阶段

早期的飞机主要追求飞行系统的完备性与适航性，虽然事故频繁，但由于飞行速度低，造成灾难性事故并不多，美国陆军航空兵在 1908~1914 年间共发生 11 次灾难性事故。20 年代初，美英军方开始记录飞行事故，统计飞机的飞行事故率。随着飞机设计、制造和飞行训练水平的提高，飞行事故率呈逐年下降的趋势[3]。在 30 年代之后，美英都进一步加强重大飞行事故的记录和调查。与此同时，对飞机的发动机、无线电台、空速表等系统采取了冗余设计，但在飞行操纵、螺旋桨、发动机失火、有害的环境条件等方面仍存在问题。

2 20世纪40年代中期至60年代中期：事故预防阶段

飞行安全机构的建立及飞行安全大纲的实施，使飞行事故率继续下降，1946年美英军用飞机的灾难性事故率分别为每10万飞行小时发生44次和40次灾难事故。二次大战结束后，美英空军都把工作重点从事故记录和调查转向事故预防。一方面不断完善事故的调查、报告和分析研究方法；另一方面利用事故调查和分析得到的信息，找出引发事故的各种重复的和共同的原因，采取纠正措施以防止类似事故的发生，并强调在飞机和系统的设计和制造中考虑安全性问题。在此期间，飞机的安全性前进了一大步。工业界和美国政府部门一起于1945年开会并制定了“单故障理念”，即假设每次飞行期间至少发生一个故障，而不管其概率大小。这个概念对减少单故障型事故产生了重要影响[4]。

3 60年代末期至80年代中期：系统安全实施阶段

1969年7月，美国国防部在空军发布的军用规范MIL-S-38130的基础上，制定了军用标准MIL-STD-882“系统及其有关的分系统、设备的系统安全大纲要求”，规定了系统安全管理、设计、分析和评价的基本要求，作为国防部范围内武器系统研制必须遵循的文件。随后，美国空军的F-15、F-16战斗机、B-1战略轰炸机等的研制都开展系统安全工作，包括制定系统安全大纲、确定安全性设计要求、进行系统安全分析、开展安全性设计与验证、进行系统安全培训等。同时，在民用领域也吸取了系统安全分析技术进行民用飞机安全性评定，以确定是否满足适航当局提出的安全性要求。

4 80年代末期至今：系统安全综合性设计阶段

为了进一步提高航空航天飞行器的安全性，80年代中期以来，除了进一步加强安全性分析、设计和验证工作外，还综合运用人为因素分析、软件安全性、风险管理和定量风险评估等各种先进技术来预防事故发生。从飞行器的故障与操作人员的人为因素、设备的硬件与软件、安全性设计与风险管理、定性分析与定量风险评估等各个方面对飞行事故进行综合预防。

在应用该理念设计的第三代商用喷气式飞机上正式使用功能危害性评估（FHA）、故障模式及其影响分析（FMEA）、故障树分析（FTA）[4]。同时NASA加强定量风险评估，进一步改进航天飞机的设计工作，更重视定量风险评估，并发现各分系统间的相互影响、确定人员活动和环境条件的影响，以及发现共因故障等方面，概率风险评估优于面向设计的定性分析技术。NASA及其他有关研究机构都相继研究和开发各种有效的概率风险评估方法，例如，以可靠性为基础的概率风险评估和贝叶斯概率风险评估等定量风险评估方法。

飞机系统安全评估的目标

飞机系统安全评估要达到以下目标[5]：（1）飞机系统具有及时有效的安全设计。（2）飞机各个子系统可能出现的故障均被定义、追踪、评估和消除或降低至一个可接受的程度。（3）各个系统的历史安全数据（包括系统的安全信息）可以使用。（4）可以在新的技术、材料、设计和产品，测试或可行技术中检测出来可能存在的最小风险。（5）记录下所有将风险降至可接受范围所采取的措施。（6）设计、制图或任务要求中的变化将以一种把故障风险降至可接受范围的方式来完成。（7）定义用来支持和维护系统安全的损耗，并声明程序性和培训的要求。（8）重新审阅针对安全的过度限制性和非充分性要求的设计标准，同时推荐使用研究分析结果与测试数据支持的设计标准。（9）避免无授权的复杂性设计和新颖设计。

对于安全评估的进一步标准，美国FAA在AC25.1309-1A中从定性和定量两个方面进一步定义了安全性指标，其中定性的安全指标包括四类：可能的、极少的 、极端少的和不可能的。以上定性的安全指标分别对应一个以发生概率表征的定量指标[6]：（1）可能的失效状态的定量指标是，每飞行小时平均概率高于1×10^{-5}。（2）极少的失效状态的定量指标是，每飞行小时平均概率低于1×10^{-5}但高于1×10^{-7}。（3）极端少的失效状态的定量指标是，每飞行小时平均概率低于1×10^{-7}但高于1×10^{-9}。（4）极不可能的失效状态的定量指标是，每飞行小时平均概率低于1×10^{-9}。

目前，在国际民用航空工业中，实施系统/设备安全性的评估方法普遍遵循4部适航当局认可的指导材料：SAE ARP4761（对民用机载系统和设备进行安全性评估过程的指导和方法）、SAE ARP4754（关于高度综合或复杂的飞机系统的合格审定考虑）、RTCA DO178B（机载系统设备审定软件考虑因素）、RTCA DO254（机载电子硬件设计保证指南）。

飞机系统安全评估流程

一个好的制定评估计划的策略应该能够考虑到以下因素[2]。

（1）利益相关者：一个成功的评估要求一个紧密合作并且相互理解的团队。

（2）安全/风险标准：合适的标准应该能够给出顶级系统的安全要求，给出具体术语的定义并且分配出合理的解决措施。

（3）系统等级：对需要评估的系统划分等级，并且根据等级的高低制定相应的评估计划。

（4）系统描述：考虑到系统的操作模式（包括操作环境与适宜波段

区）并修改现有系统内容中不恰当的地方。

（5）系统验证：需要设计者来决定采用何种最适合的方法来组成一个逻辑性的论证过程以验证系统的安全性。

飞机系统安全评估的流程可用图1表示[7]。系统安全评估过程包括安全性评估与安全性验证两个方面，其中同时包括定性评估和定量评估。整个安全性分析过程应该从飞机最初始的设计阶段开始做起，一直持续到整个系统的实现过程[8]。

飞机研发伊始就要进行飞机级的功能危害性评估（Functional Hazard Assessment，FHA），是对飞机各项功能进行的一次系统、全面的检查，用以明确各项功能的失效状态和产生的影响，并根据影响的严重程度划分等级，它是一种自上而下的评估方法。随后在了解飞机的基本参数以及功能要求的基础上再对各个分系统进行系统级FHA，定性的分析顶层失效故障的情况、影响和概率。

做完功能危害性评估之后，进行初级系统安全性评估（Preliminary System Safety Assessment，PSSA），PSSA的目的是明确硬件失效影响，硬件和软件的设计误差影响，允许的最大发生概率和设计保证等级，然后根据分析结果确定为满足安全目标需要采取的防范措施和设计构型[9]。PSSA可以从定性、定量两个方面对系统进行评估，最常采用的分析方法是故障树分析法，有时也会用到相关性图表法（Dependence Diagram，DD）或马尔科夫分析法（Markov Analysis，MA）。该流程本质上是一个反复的过程，随着设计工作的进行，所做出变更和修改的设计必须按流程再次评估。

一旦完成设计和定型，就会进行系统安全性评估（System Safety Assessment，SSA），SSA是对已设计定型的系统（包括其构型、安装）进行的一次系统地、全面地评估，用以表明由FHA拟定的安全目标和由PSSA给定的安全要求都得到了满足。通过进行零部件失效模式及其影响分析（Failure Modes and Effects Analysis，FMEA）来计算各个硬件的实际失效率，同时对整个系统进行共因分析（Common Cause Analysis，CCA）用以验证功能、系统和组件之间的独立性，并确保这种独立性的存在处于可以接受的状态以满足安全性要求[9]。根据不同的分析角度和分析对象，CCA分为：区域安全性分析（Zonal Safety Analysis，ZSA）、特定危险分析（Particular Risks Analysis，PRA）和共模分析（Common Mode Analysis，CMA）[9]。

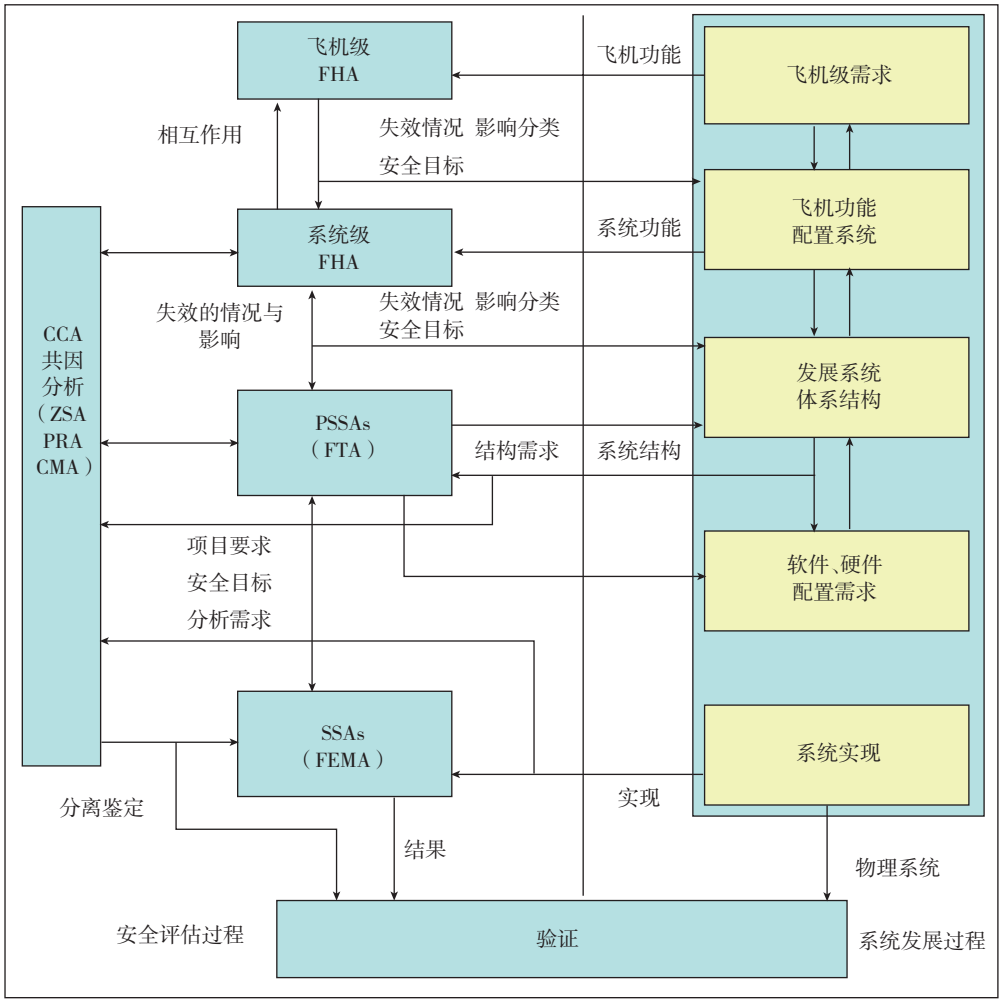

图1 飞机系统安全评估流程

飞机系统安全评估常用方法

对飞机系统进行安全性评估的方法可以分为以下3类：

（1）定性评估方法[8,10]。

主要包括故障模式与影响分析（FEMA）方法、故障树分析（FTA）方法和共因分析（CCA）方法。

故障模式与影响分析方法是1950年美国古拉曼公司为了研究飞机主操纵系统可靠性而提出的一种自下而上的方法，由系

统内所有部件的一个详细的列表开始，一次一个部件地分析整个系统。FMEA 简单易行，适用于发现问题，是一种系统化的技术，易于推广到各级产品设计师中并得到普遍应用。该方法的局限性在于不能识别造成严重失效的复合失效或共因失效。由于它针对每一个部件，而每个部件都被看作是独立的，所以复合失效无法处理。同时，运行和维修失效一般也不能通过 FEMA 检测出来。所以运用该方法，部件的所有失效模型都必须已知。

故障树分析方法是由贝尔实验室 H.A.waston 于 1961 年提出的一种自顶向下识别系统故障的方法。其后的 3 年里，FTA 技术被美国波音公司接受，并成功地应用于安全性分析。后来，FTA 技术被推广应用到航天部门及核能、化工等许多领域，成为复杂系统可靠性和安全性分析的一个有力工具，也是事故分析，特别是航天事故分析的一个重要手段。故障树分析主要是帮助人们发现复杂系统中的设计问题，追溯系统失效的根源，深入到故障组合关系，是对 FEMA 的很好补充，它非常适合找出造成问题的多个故障。FTA 方法描述了各种故障条件下系统会发生什么状况，为更详细的可靠性和安全性分析提供了必要的文件。

共因分析方法对灾难的和严重的失效状态进行独立性分析，以确保故障树中“与门”事件和“与门”事件下的组合失效是满足独立性要求的，确保由于彼此之间存在关联而可能导致的危害一定是在可接受的范围之内 [11]。由环境引起的共因风险，与区域安全性分析（ZSA）对应；由事件引起的共因风险，与特定风险分析（PRA）对应；由差错引起的共因风险，与共模分析（CMA）对应。

（2）定量评估方法 [8,10]。

主要包括定量概率评估方法、模拟仿真法、排队论方法和马尔科夫分析（MA）方法。

模拟仿真法主要是用蒙特卡洛方法对实际系统多个部件和在多个阶段可能引起不安全性的情况加以模拟，通过方法可得到传统的性能指标而且能得到动态的仿真结果，为设计飞控系统提供了动态参数。能够更真切地模拟飞控系统的工作环境，从中得到所需要的多种故障和安全的有关指标。该方法比概率方法能考虑的因素要多得多，但花费计算机时间较长。

排队论方法将多种故障看作是一个顾客流，将各种应急措施、修复故障看成是服务，这样整个航天系统就可看作一个极为复杂的并串联服务系统。根据流和服务分布的规律及排队服务的不同规则可以计算各种安全性指标。由于计算公式过于复杂，该方法一般很难得到切合实际的计算结果，但可以得到一些近似结果。

马尔科夫分析方法主要用来求解系统失效状态的发生概率。它通过分析系统的组成，准确定义系统的运行状态，列出系统的状态转移图和方程式并求解来计算失效概率。与 FTA 相比，MA 方法的定量精确度更高，并克服了 FTA 静态分析特性的缺点 [12]。

（3）综合评估方法 [10]。

主要包括风险评估复验技术（Venture Evaluation Review Technique，VERT）和概率风险评估（Probabilistic Risk Assessment，PRA）方法。

VERT 方法的优点是对整个项目可以分阶段、分部件来描述，逻辑功能强，同时可以利用计算机仿真反复模拟，得到的结果主要以概率分布形式表示。VERT 主要分 3 类指标来考虑风险，即时间、成本费用、性能指标，其中性能指标最为复杂。国际上尤其在美国，不少型号研究应用该法，我国也有人用于飞机、舰炮武器、飞船方案论证等。

PRA 方法是定性、定量相结合，以定量为主的安全性分析方法，是对复杂系统进行定量风险评估的一种重要工具。通过应用 PRA 方法，可以使安全工程师对复杂系统的特性有全面深刻的了解，有助于找出系统的薄弱环节，提高系统的安全性；并可以在概率的意义上区分各种不同因素对风险影响的重要程度，为风险决策提供有价值的定量信息。

结束语

随着科学技术的发展，飞行器的复杂性大大提高，飞机系统越来越复杂，各系统间的交叉关联也越来越多，飞机系统的安全性和适航性愈加受到重视。飞机系统的安全性评估不再仅限于完成基本评估内容，还要考虑由于系统的高度综合、系统的复杂性、软硬件的相互作用而产生的新问题。如何对复杂系统进行系统的评估，如何在设计周期中兼顾软硬件的潜在故障，成为飞机系统安全十分关注的问题。与此同时还需要关注系统的组成以及系统与环境之间的关系。仅仅用试验或分析的方法已经不能覆盖系统安全评估中需要考虑的所有问题，或者即使可能，也因试验数量太大而无法实行。以试验或数据分析为主体的传统验证方法已逐步朝着兼顾结构化的设计保证方法和严格的过程控制方法发展，对飞机系统的安全性评估需要设计者在飞行器的整个设计阶段，从多个角度考虑飞机系统的安全性能，通过安全性分析、设计、验证和优化等方面全方位的保证飞机系统安全性能，相应的安全性能评估才能够有效地减小故障发生的概率。

本文共有参考文献 12 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　良辰）