航空科学技术
Aeronautical Science & Technology
Aug. 15 2014 Vol. 25 No.08 23-26

军用飞机安全性设计方法研究

乔卫华*，胡宝雷
西安航空计算技术研究所，陕西 西安 710119

摘　要：随着军用飞机的不断发展，安全性问题日益突出，传统的安全性技术不能满足军用飞机系统研制的需要。本文从安全性标准、风险评定和安全性分析三个方面对军用飞机与民用飞机的安全性工作进行比较，论证了将民用飞机安全性开发过程吸纳到军用飞机研制中的可行性，可以作为国内军用飞机安全性设计的参考。

关键词：军用飞机；安全性设计；民用飞机；风险评定；安全性分析

中图分类号：V221　　**文献标识码**：A　　**文章编号**：1007-5453（2014）08-0023-04

随着军用飞机的不断发展，系统变得更加复杂，安全性问题日益突出。军用飞机发生事故将会造成己方人员的伤亡和设备的损失，严重影响战斗能力的发挥。在预期军事用途和使用条件下的安全运行能力势必成为军方研究的主要问题之一。

在国外军用飞机的研制中都明确要求应用安全性技术，将安全性作为军用飞机研制的一项要求，但在实际应用中如何贯彻、执行这些要求却仍是一个需要研究的问题。美军标MIL-STD-882D是世界上许多国家开展安全性的引用标准，由于保密的原因，美军在其军用飞机的研制过程中如何进行系统安全性分析尚无从知晓，能够查询资料如AD报告、PB报告等都只有一些类似于MIL-STD-882D标准的文献。而在民用飞机工程中早已具备健全的安全性标准体系，可以为军用飞机借鉴，从民用飞机采用的安全性流程及其方法出发，把民用飞机的安全性设计逐步纳入军用飞机的安全性设计中来研究安全性问题，通过安全性分析、设计、试验和优化技术的应用，找到最佳的减少和控制风险的措施，从而在使用有效性、费用和进度等限制条件下，确保系统达到最佳的安全程度。

1 军用飞机与民用飞机的安全性比较

军用飞机与民用飞机在设计、制造、使用等方面有较大的差异，军用飞机更加注重操纵性，而民用飞机更加注重安全性，在设计过程中始终把保证乘客与机组的人身安全放在首要位置。下文将从安全性标准、风险评定、安全性分析方法三个方面对军用飞机和民用飞机的安全性内容进行比较，分析两者差异，进而找出借鉴民用飞机安全性体系的可能性。

1.1 安全性标准

GJB900-1990和MIL-STD-882D是指导武器装备安全性工作，尤其是研制阶段安全性工作的通用要求和重要依据；SAE ARP4761是民用飞机机载系统和设备安全性评估过程的指南和方法，这两种标准或指南在国内外飞机安全性领域被广泛应用和研究，区别如下：

（1）面向的对象不同。GJB900-1990和MIL-STD-882D是军用标准，是面向所有武器装备的通用性标准，而不是专门针对军用飞机的安全性标准；而SAE ARP4761是专门针对民用飞机机载系统和设备安全性评估的方法与指南。

（2）参考依据不同。GJB900-1990和MIL-STD-882D的依据是系统安全工程的原理和方法，本质上是属于系统工程技术和管理的范畴；而SAE ARP4761是对机载系统的安全性分析与评估，并没有体现系统安全工程的思想，系统安全性评估的“系统安全性”是指“系统的安全性”，与系统安全标准的“系统安全”是两个不同的概念。

（3）在全寿命周期中适用的阶段不同。GJB900-1990和MIL-STD-882D是用于产品整个生命周期的安全性工作；而SAE ARP4761只针对飞机的研制过程。

收稿日期：2014-06-19；　退修日期：2014-07-06；　录用日期：2014-07-10
*通讯作者．Tel.：029-89186296 E-mail：qwhdp0@163.com
引用格式：QIAO Weihua,HU Baolei. Study on the safety design method of military aircraft[J].Aeronautical Science & Technology, 2014,25(08):23-26.乔卫华,胡宝雷.军用飞机安全性设计方法研究[J].航空科学技术,2014,25(08):23-26.

(4) 包含的内容与层次不同。GJB900-1990和MIL-STD-882D对产品的承制方和订购方提出了全寿命周期内的安全性工作要求，不仅包括了具体的工程和技术工作，还包括了对管理工作的要求，如制定系统安全大纲、开展安全培训等内容；而SAE ARP 4761的系统安全性评估只是对机载系统的安全性评估方法及过程提供了指南，主要目的是通过定性和定量的方法确定系统、设备以及硬件和软件安全性要求并进行验证，基本上是技术层面的问题，没有管理工作等的要求。

1.2 风险评定

风险评定指的是按危险严重性和可能性划分等级，对风险进行评价，并根据有关风险的评定决定对已判定的危险提出处理的方法。

1.2.1 危险严重性等级

在军用飞机中危险严重性等级根据人为差错、环境条件、设计缺陷、规程缺陷、系统及分系统或部件故障等引起的事故提供了定性度量，通常划分为灾难的(Ⅰ级)、严重的(Ⅱ级)、轻度的(Ⅲ级)和轻微的(Ⅳ级)等四个等级。具体说明如表1所示。

表1 军用飞机危险严重性等级

Table 1 Military aircraft hazards level

等级	等级说明	事故后果说明
Ⅰ级	灾难的	人员伤亡或系统报废
Ⅱ级	严重的	人员严重受伤、严重职业病或系统严重损坏
Ⅲ级	轻度的	人员轻度受伤、轻度职业病或系统轻度损坏
Ⅳ级	轻微的	人员受伤和系统损坏轻于Ⅲ级的损伤

民用飞机根据要求将危险严重性划分为五个等级，具体说明如表2所示。

表2 民用飞机危险严重性等级

Table 2 Civil aircraft hazards level

等级	等级说明	事故后果说明
Ⅰ级	灾难的	妨碍飞机继续安全飞行，导致多数人员致命或飞机坠毁
Ⅱ级	危险的	导致安全裕度显著降低，工作量明显增加，少数人员可能严重受伤或致命
Ⅲ级	主要的	导致安全裕度降低，机组人员工作量显著增加，降低机组人员的效率，使机组人员感觉不适，造成乘客身体伤害
Ⅳ级	次要的	对安全性没有显著影响，机组人员工作量轻微增加，人员有一些身体不适
Ⅴ级	无影响	对飞机运行能力、安全性和人员无影响

1.2.2 危险可能性等级

在系统寿命期内造成危险的可能性可用单位时间(或事件、活动等)可能发生的事故数来描述。在设计初期，定量的危险概率数据不可能获得，一般可通过分析、研究相似系统的安全性信息获得。

军用飞机危险可能性通常分为频繁发生(A级)、很可能发生(B级)、有时发生(C级)、极少发生(D级)和不可能发生(E级)等5个级别。具体说明如表3所示。

表3 军用飞机危险可能性等级

Table 3 Military aircraft failure probability level

等级	等级说明	个体发生情况	总体发生情况
A	频繁	频繁发生：在某一项目寿命中可能经常发生，在寿命中发生的概率超过10^{-1}	连续发生
B	很可能	在寿命期内会发生若干次：在某一项目寿命中可能发生一些次，在寿命中发生的概率超过10^{-2}低于10^{-1}	经常发生
C	有时	在寿命期内可能有时发生：在某一项目寿命中可能发生几次，在寿命中发生的概率超过10^{-3}低于10^{-2}	发生若干次
D	极少	在寿命期内不易发生，但有可能发生：在某一项目寿命中不易发生但可能发生，在寿命中发生的概率超过10^{-6}低于10^{-3}	不易发生，但有理由预期可能发生
E	不可能	很不容易发生，以至于可以认为不会发生：如此不可能，可以被假定发生没有历史性经验，在寿命中发生的概率低于10^{-6}	不易发生，但有可能发生

民用飞机的危险可能性等级也分为频繁发生(A级)、很可能发生(B级)、有时发生(C级)、极少发生(D级)和不可能发生(E级)等5个级别。但是其在寿命中发生的概率则与军用飞机有很大差异，民用飞机的故障发生概率要求随着飞机类型有不同的规定。如23部小型飞机定义E级故障发生概率为10^{-6}，而25部大型飞机为10^{-9}。表4所示为25部飞机的危险可能性等级。

表4 民用飞机危险可能性等级

Table 4 Civil aircraft failure probability level

等级	等级说明	个体发生情况	总体发生情况
A	频繁	频繁发生：在某一项目寿命中可能经常发生，在寿命中发生的概率超过10^{-3}	连续发生
B	很可能	在寿命期内会发生若干次：在某一项目寿命中可能发生一些次，在寿命中发生的概率超过10^{-5}低于10^{-3}	经常发生
C	有时	在寿命期内可能有时发生：在某一项目寿命中可能发生几次，在寿命中发生的概率超过10^{-7}低于10^{-5}	发生若干次
D	极少	在寿命期内不易发生，但有可能发生：在某一项目寿命中不易发生但可能发生，在寿命中发生的概率超过10^{-9}低于10^{-7}	不易发生，但有理由预期可能发生
E	不可能	很不容易发生，以至于可以认为不会发生：如此不可能，可以被假定发生没有历史性经验，在寿命中发生的概率低于10^{-9}	不易发生，但有可能发生

1.3 安全性分析方法

为了使系统具有最佳的安全性，技术人员必须采用系统

的分析方法，主要包括定性分析和定量分析两大类。当对具体的系统进行分析时，根据系统的特点以及用户的要求可采用各种具体的定性及定量分析方法。定性分析用于检查、分析和确定可能存在的危险、危险可能造成的事故以及可能的影响和防护措施。定量分析用于检查、分析并确定具体危险、事故及其影响可能发生的概率，比较系统采用安全措施或更改设计方案后概率的变化。定量分析目前主要用于比较和判断不同方案的系统所达到的安全性水平，作为对有关安全性更改方案决策的基础。定量分析必须以定性分析作为依据。

军用飞机常用的定性分析方法有：故障危险分析(FHA)、故障模式及影响分析(FMEA)、故障树分析(FTA)、潜在通路分析(SCA)、事件树分析(ETA)、意外事件分析(CA)、区域安全性分析(ZSA)、接口分析(IFA)、电路逻辑分析(CLA)、环境因素分析(EFA)等；常用定量分析方法有故障模式、影响及危害性分析(FMECA)、故障树分析(FTA)和概率估算等。

民用飞机常用的定性分析方法有：FTA、FMEA、故障模式及影响摘要(FMES)、相关性图表分析(DD)、马尔可夫分析(MA)、ZSA、特定风险分析(PRA)、共模分析(CMA)；常用定量分析的方法有FMECA、FTA和PRA等。

在军用飞机和民用飞机设计中所采用的定性和定量的分析方法有很多相同的方法，最常见有FTA、故障模式及影响分析等。

2 军用飞机安全性设计思路

军用飞机研制引入适航是充分借鉴民用飞机适航的理念，将系统安全性开发过程吸纳到型号研制中来，为型号的安全性设计提供了捷径。安全性是系统级属性，而非单个部件的属性。即安全性问题是系统级的问题，而非部件级问题。因此安全性必须在系统级进行控制，而不是在部件级。相应的安全性分析也应该是一个从系统整体到部分的演绎过程。SAE ARP 4761的系统安全性分析与要求的确认就很好地体现了这一思想。

机载系统的开发是一个多阶段反复迭代、交互的过程，如图1所示。图中左半部分为安全性分析活动，图中右半部分为设计实现活动。系统安全性评估过程主要包括功能危害性分析(FHA)、系统安全性预见分析(PSSA)、系统安全性分析(SSA)和共因分析(CCA)等。系统设计活动从飞机级需求开始，其后是飞机的各项功能确定，系统结构设计、定义软件需求以及系统实现。

系统设计工作与安全性评估以渐进方式相互作用，首

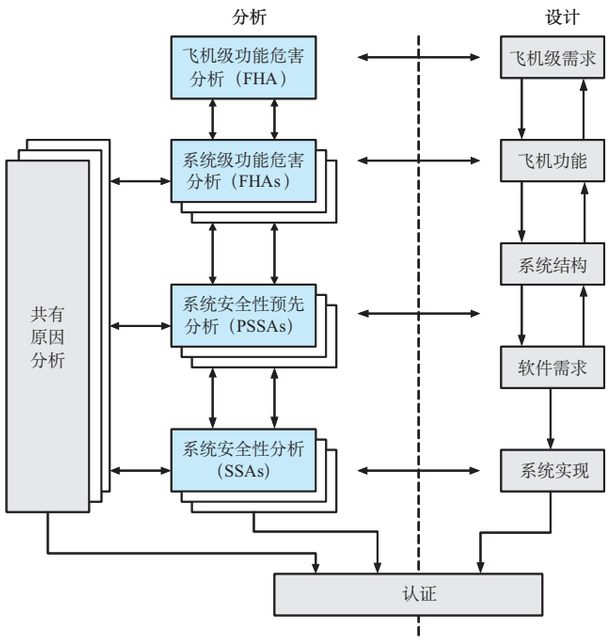

图1 典型系统开发过程

Fig. 1 Airborne system development process

先针对飞机平台进行需求分析，定义出航空电子系统的各主要功能，其次通过FHA分析发现系统中的薄弱环节，考虑上述因素后设计出初步系统架构，再由PSSA分析进一步改进系统架构设计，待系统样机实现后经SSA分析再次验证系统安全性或提出改进方法，共因分析可以发现系统中导致主备份单元同时故障的因素，经过多次迭代最终设计出满足所有安全性要求的系统。

飞机的整机级功能是由不同的系统通过一定的联系和交互作用来实现的，而系统级功能是由组成系统的各种设备和部件通过一定的联系和相互作用来实现的。因此，对于系统安全性评估来说，从功能危险分析入手，便是从飞机整体或系统整体入手，来分析具有整体性质的功能危险，再以功能危险为顶事件，通过故障树分析得到整机级或系统级功能危险的具体的系统或设备失效原因。通过以上的分析可知，军用飞机研制虽然在安全性标准、风险评定、安全性分析方法上与民用飞机有所区别，但安全性评估方法的要求是一致的，即完全可以采用SAE ARP 4761所提供的系统安全性评估方法，开展军用飞机的系统安全性分析与评估工作。

3 结论

军用飞机研制的安全性工作应在GJB 900–1990和MIL–STD–882D确定的系统安全工程的框架内，充分借鉴SAE ARP 4761民用飞机安全性评估的流程与方法，将适应型号

特点的适航要求纳入到安全性设计当中来，并应用民用飞机系统安全性评估的方法确定定性和定量的安全性要求，进行要求的确认与验证。通过应用系统安全工程方法，进行先导式的危险识别，确定出由新颖设计和先进技术引入的风险，通过危险消除和风险控制，将安全风险控制在可接受的范围之内。 AST

参考文献

[1] 系统安全性通用大纲,中华人民共和国军用标准,GJB 900-1990[S]. 北京：国防工业出版社，1998.
General program for system safety, National Standard of People's Republic of China. GJB900-1990[S]. Beijing: National Defense Press,1998. (in Chinese)

[2] 可靠性维修性保障术语,中华人民共和国军用标准,GJB 451A-200 [S]. 北京：国防工业出版社，2002.
Reliability, maintainability and supportability terms, National Standard of People's Republic of China. GJB451A-200[S]. Beijing: National Defense Press,2002. (in Chinese)

[3] 系统安全工程手册，中华人民共和国军用标准,GJB/Z99-97[S]. 北京：国防工业出版社，1998.
Engineering handbook for system safety, National Standard of People's Republic of China, GJB/Z99-97[S]. Beijing: National Defense Press,1998. (in Chinese)

[4] Certification consideration for highly integrated or complex aircraft systems, SAE ARP4754[S]. The Engineering Society For Advancing Mobility Land Sea Air and Space, 1996.

[5] Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, SAE ARP4761[S]. The Engineering Society For Advancing Mobility Land Sea Air and Space, 1996.

作者简介

乔卫华(1979—) 男，本科，工程师。主要研究方向：军用飞机机载电子设备五性设计。
Tel：029-89186296
E-mail：qwhdp0@163.com
胡宝雷(1987—) 男，本科，助理工程师。主要研究方向：军用飞机机载电子设备五性设计。
Tel：029-89186295
E-mail：hubl@163.com

Study on the Safety Design Method of Military Aircraft

QIAO Weihua*, HU Baolei

Aeronautics Computing Technology Research Institute, Xi'an 710119, China

Abstract: With the development of military aircraft, security issues have become increasingly prominent, the traditional security technology can not meet the development needs of military aircraft. This paper compared work safety of military aircraft and civil aircraft from security standard, risk assessment and safety analysis three aspects, demonstrated the feasibility of absorbing the civil aircraft safety development process into military aircraft development, can be used as a reference of military aircraft safety design.

Key Words: military aircraft, safety design;civil aircraft; risk evaluation; safety analysis

Received: 2014-06-19; **Revised:** 2014-07-06; **Accepted:** 2014-07-10

***Corresponding author. Tel. :** 029-89186296 **E-mail:** qwhdp0@163.com