* 1

飞机整机级系统安全性指标分析

宗蜀宁[1]，端木京顺[1]，王　青[1]，赵瑞贤[2]，汪建华[2]
(1. 空军工程大学工程学院,陕西西安,710038;2. 北京航空工程技术研究中心,北京,100076)

摘要　针对整机级系统安全性评估中安全性指标的选择与确定问题,分析对比了国内常用安全性参数之间的区别,指出了其在系统安全性评估应用中的缺点;根据系统安全性的特点,提出了飞机整机级系统安全性指标的要求和维度;借鉴国外系统安全性评估的成功经验,结合可靠性,提出了指标选择和量化的具体方法,并举例说明安全性指标的应用时机和使用方法。研究表明,将安全性与可靠性相结合,选择影响飞机安全性的可靠性指标进行机整机级系统安全性评估,可以解决传统安全性参数量化困难、不适用等问题,是一种可行并且合理的方法。

关键词　飞机;整机级;系统安全性指标;系统安全性评估
DOI　10.3969/j.issn.1009-3516.2012.01.003
中图分类号　V27;X949　　**文献标识码**　A　　**文章编号**　1009-3516(2012)01-0010-05

安全性指标是飞机整机级安全性的度量,是系统安全性工作的基础和重要参考标准。当前民用飞机必须具备所要求的适航性[1],即满足适航条令或适航规章对飞机设计、制造、飞行和空中交通管制等规定的最低要求,其中包括定性要求和定量要求2部分[2],可选取不同的安全性参数进行表述。飞机安全性指标不仅是新型飞机研制的依据和标准,也是后期系统安全性分析、验证工作的基础。目前国内全面飞机安全性工作刚刚起步,对系统安全性指标的研究方面还不足,尤其是整机级指标参数的选取和确定,急需开展研究。

1　安全性参数体系

1.1　常用安全性参数

安全性参数表示系统的安全性的度量[3],在评估飞机安全性时,参数的选择尤其重要。目前我国常用的安全性参数有:平均事故间隔时间 T_{BA}、事故率或事故概率 P_A、安全可靠度 R_S 和损失率或损失概率 P_L。这4个参数相互联系,但侧重点不同:R_S 不同于事故概率,R_S 关注灾难性事故,不考虑其他严重等级的事故,并且衡量的时间范围为系统的工作时间,而不是系统的寿命;P_L 是 P_A 的特例,前者只关注的是灾难性事故,而后者包括所有类型的事故。对于同一个系统或部件,通常情况下 $P_L \leqslant P_A$。

1.2　安全性风险度量

安全性与事故的风险密切相关。事故的风险包括事故严重性和事故概率,根据文献[4]中的方法可定性、定量地确定事故严重性和事故概率。其中事故严重可分为灾难的(I类)、严重的(II类)、轻度的(III类)和轻微的(IV类),事故概率可分为频繁的(A等)、很可能的(B等)、有时的(C等)、极少的(D等)和不可能的(E等)。能否接受事故的风险不仅取决于事故的严重性,还取决于事故的概率。通过绘制风险评估指数矩阵,可以帮助人们判断该类事故风险是否可以接受。表1为风险评估指数矩阵的一种范例。矩阵中,1-5为高风险,6-9为严重风险,10-17为中等风险,18-20为低风险。能否接受各个等级的风险,需要由相应级别的管理方或者使用方人员来决定。

*　**收稿日期**:2011-07-12
基金项目:国家自然科学基金资助项目(71171199)
作者简介:宗蜀宁(1983-),男,重庆江津人,博士生,主要从事装备安全评价、预测与决策研究.
E-mail:shuninging@vip.qq.com

表 1　风险评估指数矩阵

Tab. 1　Mishap risk assessment values

事故概率	灾难性的	严重的	轻度的	轻微的
频繁	1	3	7	13
很可能	2	5	9	16
有时	4	6	11	18
极少	8	10	14	19
不可能	12	15	17	20

1.3　与安全性相关的可靠性指标参数

安全性与可靠性密切相关[1],可靠性低的系统会经常出现失效事件,致使系统处于故障状态,很可能影响系统的安全。与安全性有关的可靠性参数有故障率、失效率。

故障率或故障概率(fault rate or fault probability),指在规定时间或规定的期间内,产品的故障总数与寿命单位总数之比:

$$P_F = \frac{N_F}{N_T} \tag{1}$$

式中:P_F 为故障率或故障概率,单位为次/小时或次/飞行次数;N_F 为故障次数;N_T 为寿命单位总数。

失效率(failure rate),指在规定的时间或规定的期间内,所有由该硬件出现的失效总数与总的运行时间单位之比(失效函数呈指数分布时)[5]:

$$R_F = \frac{N_{F1}}{O_T} \tag{2}$$

式中:R_F 为失效率,单位为次/飞行小时;N_{F1} 为失效次数;O_T 为运行时间。

故障是对可修复系统或部件未能完成规定功能的统称,失效是对不可修复系统或部件未能完成规定功能的统称,两者本质一样,但存在细微差别:故障通常是产品本身失效后的状态,但也可能在失效前就存在;失效是一个事件,是故障的具体体现,当出现故障时可能产生失效。在国外的系统安全评估过程中[5],故障与失效是 2 个不同的概念,使用时机也不同,故障通常用于飞机系统级安全性评估中,而失效常用于整机级,因此要区别对待。

2　系统安全性指标的要求

根据系统安全的依据和要求,飞机的整机级系统安全性评估指标的总体要求为:①综合性:即指标应该充分考虑可靠性、维修性、保障性和测试性,甚至可以用其中部分指标作为安全性指标。②通用性:即系统、分系统、部件使用统一指标来表示,或各指标间可以通过简单运算相互转换。③阶段性:即在寿命期不同阶段,应提出相应的门限值(或最低可接受值)与目标值(或规定值)。

安全性风险要求即使用方和社会可接受的风险程度。虽然使用方和承制方对飞机和设备都有一个基本的安全性目标,但其安全性水平不一定都会让人满意。因此,系统安全性指标必须明确提出社会或双方共同认可的具体的风险要求。

3　系统安全性指标的维度

维度是确定系统安全性指标的具体依据,指标的选取和量化应在维度范围内进行,且应当满足使用方和承制方要求。排除外在和人为因素,飞机的安全性是由系统、分系统共同保证的。因此,飞机整机级系统安全性评估指标应该分层次考虑,即 S。

安全性指标与风险的 2 个决定性因素密切相关——危险可能性和危险严重性。因此飞机整机级系统安全性评估指标应考虑风险等级,即 $L = (P_r, C)$,其中 L 为风险等级,P_r 为危险可能性,C 为危险严重性。

在不同的使用效能、时间和费用等约束条件下,可以选择不同的风险类型 T,如可接受的、可控制的、不可接受的等。

以上构成了飞机整机级系统安全性评估指标的维度,见图 1。

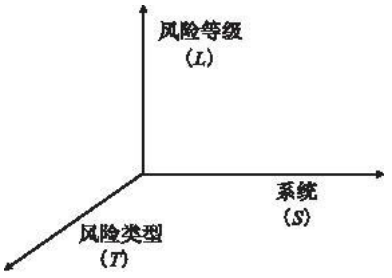

图 1 飞机整机级系统安全性评估指标维度

Fig. 1 System safety assessment index dimensionality in aircraft level

例如:某型飞机发动机系统的作用是产生推力以提供使飞机前进的动力,飞行时可能会出现丧失全部或部分推力导致推力不足或严重不对称的危险事件(或失效状态)。评估前应首先确定研究对象,然后判断危险事件的风险和风险等级,最后确定风险类型。发动机系统发生此类失效状态将会导致灾难性的事故,因此为 I 等,且允许概率不能大于 10^{-6}。现假定该事故概率为 10^{-7},根据表 1 可知该类事故的风险评估指数为 12,属于中等风险。若经使用方和承制方商量认定发动机系统以中等风险导致事故是可接受的,则该风险的类型为可接受的风险。综上,S = 发动机系统,$L = (10^{-7}, I)$,T = 可接受的风险,指标为事故概率 = 10^{-7}。由于指标满足维度要求,因此可以使用该指标对发动机系统进行系统安全性评估。

4 确定系统安全性指标的方法

4.1 参数的确定

我国安全性参数均以事故作为研究对象,因此参数不容易衡量,且直接测量系统的安全性成本高。本文所列出的 4 种常用安全性参数均为统计参数,如果限制其统计范围,则可以提供最顶层的安全性要求。例如通过统计运输类飞机的损失率,可以得出该类飞机在其寿命范围内发生灾难性事故的可能性为 $P1$,因此可以要求设计方在设计运输类飞机时将 $P1$ 作为安全性评估的参考值。传统安全性参数较适用于整体的、顶层的安全性评估,而不适合分系统、部件。众所周知,飞机的零部件种类繁多,数量巨大,若采用事故率、损失率等参数来计算分系统、部件的安全性水平,不仅难度大,而且数值太小,有的数据无法获得。因此传统安全性参数不适用于除顶层以外层次的安全性评估。

鉴于传统安全性参数的局限性,可尝试借鉴国外较为先进的系统安全性思想学,用故障率、失效率等指标来代替。在已经确定某一可能导致事故(可以是顶层事故)的失效模式前提下,运用 FMEA 等方法绘制功能故障树,找出引发该失效模式的相关系统。故障树内所有元素都将分配可接受的失效率,当分配到部件级时,失效率基本等于故障率。因此,可以在已有基础上增加的故障率、失效率等可靠性范畴的参数,通过运算获得飞机整机级系统安全性。

4.2 参数的量化

系统安全性参数量化十分复杂。系统安全性指标过高将影响研制周期、费用以及其他战术技术指标,指标过低又将难以保证安全,造成生命财产的重大损失,因此可以借鉴和吸收飞机可靠性、维修性指标确定的经验,即:在统计分析飞行事故的基础上,确定各种风险等级的整机级安全性指标,然后分配至各系统。精确确定飞机整机级系统安全性指标十分困难,一般只给出水平量级。以事故、故障和失效作为研究对象,统计民航资料,依据文献[6]中的假设确定飞机系统安全性参数的量值。

民用飞机对能够引发灾难性事故的系统失效模式的发生概率为 10^{-9}次/飞行小时。相应严重程度的可接受的失效模式发生率见表 2。

表 2 整机级系统安全性评估指标量化

Tab. 2 quantitative index of system safety assessment in aircraft level

失效严重程度	无影响	轻微的	轻度的	严重的	灾难性的
失效率(次/飞行小时)	$\geqslant 10^{-3}$	$10^{-5}-10^{-3}$	$10^{-7}-10^{-5}$	$10^{-9}-10^{-7}$	$\leqslant 10^{-9}$

综合以上要求,可绘制飞机整机级系统安全性评估参考图,见图 2。这些系统安全性指标是系统安全性评估中的最低要求,实际的评估值不应低于此指标。

5 应用举例

某型飞机起落架控制系统提供收起和放下起落架的能力,并向驾驶员指示起落架的收放状态功能[7]。

若在近进阶段出现“全部起落架不能放下或放下未锁定但误指示已放下锁定”的失效模式,则会导致灾难性的事故[8]。运用故障树进行系统安全性评估,功能故障树见图 3,图中 G1 – G4 是逻辑门。

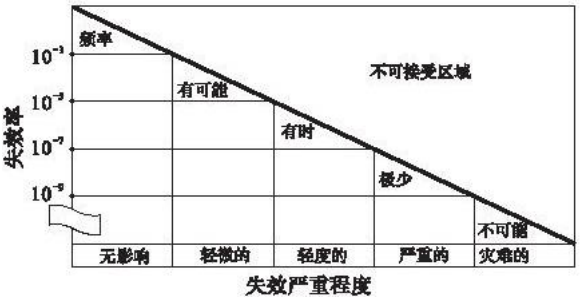

图 2　飞机整机级系统安全性评估指标(单位:次/飞行小时)

Fig. 2　System safety assessment index in aircraft level (unit: per flight hour)

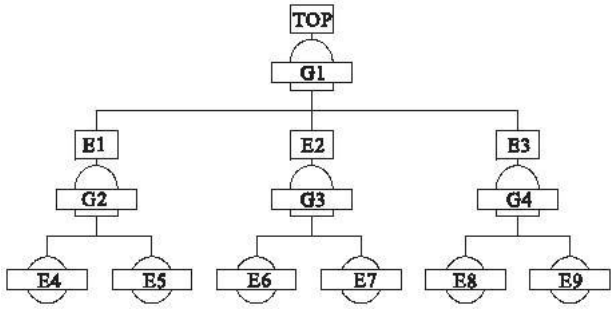

图 3　功能故障树

Fig. 3　Functional fault tree

TOP 为顶层失效模式即:“全部起落架不能放下或放下未锁定但误指示已放下锁定”。E1 – E9 为其他失效模式。文献[4]规定了失效模式 TOP、E1 – E9 应满足的安全性要求。通过系统安全性评估,可得出各失效模式的实际失效率,见表 3。

表 3　失效模式意义及失效概率

Tab. 3　Failure modes and failure probability

失效模式	失效模式意义	严重程度	指标要求失效概率	实际失效概率
TOP	全部起落架不能放下或放下未锁定但误指示已放下锁定	灾难的	$\leqslant 10^{-9}$	5.2×10^{-33}
E1	前起落架不能放下或放下未锁定但误指示已放下锁定	灾难的	$\leqslant 10^{-9}$	3.6×10^{-11}
E2	左主起落架不能放下或放下未锁定但误指示已放下锁定	灾难的	$\leqslant 10^{-9}$	1.2×10^{-11}
E3	右主起落架不能放下或放下未锁定但误指示已放下锁定	灾难的	$\leqslant 10^{-9}$	1.2×10^{-11}
E4	前起落架不能放下或放下未锁定	严重的	$10^{-9}-10^{-7}$	4×10^{-6}
E5	误指示前起落架已放下锁定	轻度的	$10^{-7}-10^{-5}$	9×10^{-4}
E6	左主起落架不能放下或放下未锁定	严重的	$10^{-9}-10^{-7}$	4×10^{-7}
E7	误指示左主起落架已放下锁定	轻度的	$10^{-7}-10^{-5}$	3×10^{-5}
E8	右主起落架不能放下或放下未锁定	严重的	$10^{-9}-10^{-7}$	4×10^{-7}
E9	误指示右主起落架已放下锁定	轻度的	$10^{-7}-10^{-5}$	3×10^{-5}

表中假设飞机飞行时间为 1 h,失效概率 = 失效率 × 飞行时间。实际失效率不是真实值,仅为说明指标的使用方法而举例。TOP 和 E1 – E3 是根据 E4 – E9 推算而得出。虽然顶层失效模式远远小于要求值,但是 E4 未达到要求,因此需要将此信息反馈给设计方以改进设计方案,或与使用方协商能否接受该失效模式的风险。从此例可以看出整机级系统安全性指标的使用时机和方法。同时也证明了其对保证飞机安全性和保障使用方利益所做的贡献。

6　结束语

如今,新型军民用运输机正处在研制时期,研究整机级系统安全性指标并将其运用在该型飞机的系统安全性评估之中,可在一定程度上保证飞机的安全性。同时,飞机整机级系统安全性评估指标还可为使用方(特别是军方)合理、具体的安全性要求提供定性和定量的依据,从而在型号研制中获得主动权[9]。更重要的是,若将系统安全性指标合理转化为设计指标,指导承制方的研制工作,可直接、有效地提升飞机安全性水平。

参考文献(References):

[1]　逯军. 民机飞行控制系统的安全性评估和分析研究[D]. 天津:中国民航大学,2009.

LU Jun. Study on system aafety assessment and analysis of flight control system of civil aircraft[D]. Tianjin: Civil aviation university of China, 2009. (in Chinese)

[2] 杨祯梅,孙安宏. 对民用飞机整机级安全性评估依据和方法的探讨[C]//第二届中国航空维修工程学术研讨会论文集. 南昌:中国航空学会,2005:72 - 76.
YANG Zhenmei, SUN Anhong. Discussion on basis and method system safety assessment on aircraft level[C]//The 2nd national aviation maintains engineering academic seminar. Nanchang:Chinese society of aeronautics,2005:72 - 76. (in Chinese)

[3] 端木京顺,常洪,雷洪利,等. 航空装备安全学[M]. 北京:国防工业出版社,2010:198 - 199.
DUANMU Jingshun,CHANG Hong,LEI Hongli, et. al. Aviation materiel safety science[M]. Beijing: National defense industry press,2010:198 - 199. (in Chinese)

[4] Department of Defense. MIL - STD - 882D, standard oractice for system safety [S]. 2000.

[5] Society of automotive engineers inc. ARP 4761, guideline and methods for conducting the safety assessment process on civil airborne systems and equipment[S]. 1996.

[6] 中国民航总局航空器适航审定司. 飞机系统安全性设计与评估[R]. 北京:中国民航总局,2007.
Aircraft airworthiness certification department of CAAC. Aircraft system safety design and assessment[R]. Beijing:CAAC,2007. (in Chinese)

[7] 王丰. 前起落架系统的系统安全性分析方法研究[D]. 天津:中国民航大学,2009.
WANG Feng. Study on system safety analysis of nose gear[D]. Tianjin: Civil aviation university of China,2009. (in Chinese)

[8] 王玉鑫. 主起落架系统的系统安全性分析方法研究[D]. 天津:中国民航大学,2009.
WANG Yuxin. Study on system safety analysis method of the main landing gear system[D]. Tianjin:Civil aviation university of China,2009. (in Chinese)

[9] Department of defense. MIL - STD - 882E, draft standard practice for system safety [S]. 2005.

(编辑:徐敏)

System Safety Index Analysis in Aircraft Level

ZONG Shu - ning[1], DUANMU Jing - shun[1], WANG Qing[1], ZHAO Rui - xian[2], WANG Jian - hua[2]
(1. Engineering Institute, Air Force Engineering University, Xi'an 710038, China; 2. Beijing Aeronautical Technology Research Center, Beijing 100076, China)

Abstract: System safety index in aircraft level is analyzed to solve the problem of index selection and quantization in this paper. The flaws of the safety parameter application in system safety analysis are indicated through the analysis and comparison of domestic safety parameters. Based on characteristic of system safety, the requirment and dimensionality of index are proposed. Using the experience on system safety assessment of foreign countries for reference, and considering reliability, methods to select and quantify safety index in aircraft level is started, and one example is given to illustrate when and how to apply safety index. Research shows, combining safety and reliability, selecting indexes having effect on aircraft safety to conduct system safety assessment in aircraft level, can be a practical and reasonable way to solve problems of traditional safety parameters such as the difficulty of quantification and inapplicability.

Keywords: aircraft; aircraft Level; system safety indexes; system safety assessment