一种基于事故树的安全风险定量评估方法

Security Quantitative Assessment Based on Fault Tree

空军工程大学工程学院　李　琳　陈云翔　刘　源

[摘要] 针对目前安全风险评估方法的不足，提出了基于事故树的飞机部件安全风险定量评估方法。首先采用布尔代数理论对事故树进行逻辑表述，通过概率重要度表示部件故障的后果严重度，在此基础上对飞机部件的危险度进行计算，解决了当前安全风险定量评估的难题。实例证明，该方法能够较为准确地检验飞机部件对飞行安全的影响。

关键词：风险定量评估　事故树　危险度　概率重要度

[ABSTRACT] To improve the existing assessment methods on security risk, a new method based on the fault tree is proposed, which can be used in security quantitative assessment of the component for aircraft. Firstly the fault tree is denoted by probability importance degree, and the effect parameter of fault is obtained by using probability importance degree. And then the hazard degree of component for aircraft is calculated. The difficult problem on security quantitative assessment is also solved primarily. Its application is shown that the approach can fully verify the risk of component effect on flight security.

Keywords: Security quantitative assessment Fault tree Hazard degree Probability importance degree

随着军用航空装备复杂程度的不断提高和飞行部队执行作战任务的复杂化，安全保障问题变得非常突出[1]。飞行事故的发生不仅会造成人员的极大伤亡，也给国家带来了巨大的财产损失，严重阻碍了部队武器装备建设的发展及战斗力的提高。如何应用系统的、有效的方法定量评估飞机部件的安全风险，对高危部件加以有效的预防，是飞机安全保障工作中必须解决的重要问题。

本课题在深入分析风险评估过程的基础上，针对当前风险参数表示方法的不足，提出了基于事故树原理的后果严重度表示方法，在此基础上可对风险因素进行准确的量化评估。以某型飞机电传操纵系统为例，对影响飞行安全的部件进行辨识并予以量化评估，旨在为飞机安全保障与事故预防工作提供基本依据。本课题提出的方法同样适用于其他危险因素的定量风险评估。

1　风险评估的一般方法

美国国防部将风险定义为：风险指在规定的费用、进度和技术的约束条件下不能实现整个项目目标的可能性的一种度量，它包含 2 个方面的含义，一是不能实现具体目标的概率；二是因不能实现该目标所导致的后果[2]。可用公式（1）予以表示：

$$R=f(p,c)\ , \qquad (1)$$

式中，R 表示危险度，p 表示不利事件发生的概率，c 表示该事件发生的后果。

安全性风险评估一般由 3 个步骤构成，如图 1 所示。

（1）辨识潜在的危险源，即判断严重影响军用飞机飞行安全的关键部件。

（2）确定危险源故障概率 p 及故障所导致的后果严重度 c。

（3）计算危险度[2]，即：

$$R=p+c-pc\ , \qquad (2)$$

其中：R 为危险度，即标识危险源安全性风险的定量度量。

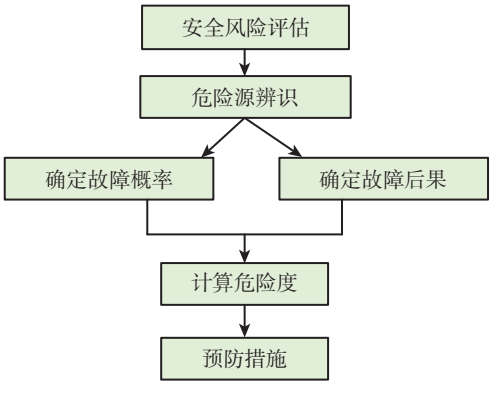

图1　风险评估过程

Fig.1　Risk assessment process

2　飞机部件的安全风险评估方法

军用飞机由成千上万个部件组成，有些部件对于军用飞机的安全性能起到了至关重要的作用。因此对安全性关键部件的确定，是军用飞机保障维护过程中安全性研究工作的第一步。对于不同的机型，飞机的安全性关键部件往往也不相同。常用的危险部件识别方法有检查表法、故障树分析法、专家调查法、流程图法、功能

风险分析法以及模糊识别法等[3]。为了有的放矢地对部件安全性进行评估，提高工作效率，本课题拟对飞机部件采用统一的安全性风险量化标准，帮助机务人员有针对性地对安全性风险量化值高的部件进行重点安全保障维护，以减少其发生故障的可能性，确保飞机飞行安全。

2.1 基于事故树的安全性风险参数定量表示方法

事故树分析是美国贝尔实验室于 20 世纪 60 年代提出的一门技术，通过该方法可对各种系统的危险性进行识别评估，具有简明、形象化的特点，目前已得到国内外的公认和广泛采用。

飞机部件安全度的准确性取决于安全性风险参数的取值。目前国内外文献主要通过权重的大小来表示故障所导致的后果，而在采用层次分析法确定权重的过程中，由于专家经验的不同，导致权重的取值在一定程度上具有主观性、模糊性。针对这个问题，可采用事故树方法对部件安全性风险参数进行定量表示，具体步骤如下。

假设以某型飞机电传操纵系统为例说明基于事故树的部件安全风险评估方法，根据该系统结构工作原理，绘制该系统事故逻辑图，如图 2 所示，其中 X_i 表示该系统部件 i 出现故障。

（1）通常根据系统结构绘制的事故树较为复杂，为了对该事故树进行深入直观的定量分析，首先运用布尔代数法对其进行描述，经简化得到该系统的故障逻辑表达式：

$$T = X_2X_3X_4X_5 + X_2X_3X_4X_6 + X_1X_2X_5 + X_1X_2X_6 \quad (3)$$

根据表达式（3）的构成，我们不难得出此系统故障

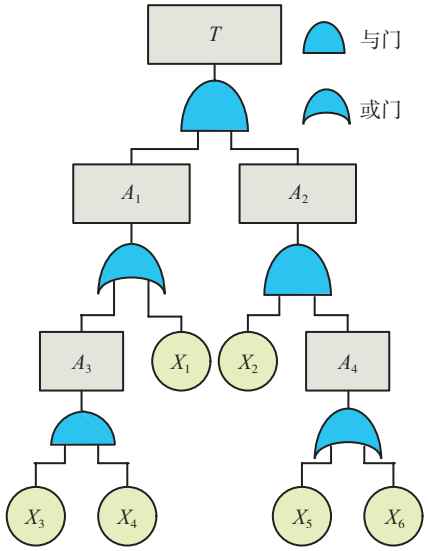

图2 某型飞机电传操纵系统事故树

Fig.2 Fault tree of fly-by-wire flight control system in a certain type of aircraft

数的所有最小割集，即 $\{X_2X_3X_4X_5\}$、$\{X_2X_3X_4X_6\}$、$\{X_1X_2X_5\}$ 和 $\{X_1X_2X_6\}$，其中每一个最小割集代表一条能导致事故发生的事故链，也是一种事故致因模式。

这里采用逆向思维对问题进行分析：系统故障的发生是各个最小割集基本元素之间相互作用的结果，若 X_i 在所有最小割集中重复出现的次数越多，由部件 i 故障导致该系统故障的可能性也就越大；相应的若 X_i 所在的割集中其他部件的故障率乘积的数值越大，由部件 i 故障导致该系统故障的危险性也就越高。因此，一个部件对所在系统安全性能的影响与该部件所在最小割集中其他部件的故障率乘积的大小及它在各个最小割集中重复出现的次数密切相关。

（2）求出顶上事件发生概率的表达式，即该系统失效的概率表达式：

$$P = p_2p_3p_4p_5 + p_2p_3p_4p_6 + p_1p_2p_5 + p_1p_2p_6 \quad (4)$$

其中 p_i 表示某部件 i 发生故障的概率。在这里引入概率重要度的概念：

$$I_i = \partial P/\partial p_i \quad (5)$$

I_i 直观的物理意义是该系统对于部件 i 的敏感程度。然而通过对公式（4）的深入分析，我们不难发现一个部件 i 的概率重要度如何，并不取决于部件本身的故障率的大小，而取决于该部件所在最小割集中其他部件的故障率积的大小及它在各个最小割集中重复出现的次数。因此可采用公式（5）作为部件后果严重度评判的依据。

需要指出的是，不少文献将危险严重度、危险关联度和危险可能度作为安全性评估的标准，而通过对表达式（4）的深入分析可知最小割集中其他因素的概率积正是危险关联度的定量表示。

2.2 基于事故树的飞机部件安全风险评估

通过公式（2）对各部件的危险度进行定量计算，其中 p 表示部件发生故障的概率。c 通过事故树计算该部件概率重要度而获得，它代表该部件出现故障所导致的事故后果。部件的危险度越大，它对系统安全性影响越大，即该部件损坏所导致事故的可能性也就越高。

3 案例分析

电传操纵系统目前在各类先进飞机中得到了普遍应用，不仅使飞机具有高度灵活性，容易实施复杂的控制，还可以改善飞机飞行可靠性。在飞行中，电传操纵系统完成改变飞机姿态和飞行轨迹的主要任务，可靠性直接影响飞行安全。电传操纵系统发生故障，会导致重大飞行事故[4-5]。

下面以某型飞机为例，对该飞机电传操纵系统部件进行安全风险评估。根据该飞机电传操纵系统的结构

原理，绘制事故树逻辑图，如图 3 所示。

将表 1 中的数据结合事故树结构函数得此操纵系统发生故障的概率为 1.5547E-08。通过公式（5）对各部件后果严重度展开计算，为减少数值大小对评估结果的影响，对部件故障概率和后果严重度进行归一化处理，将处理后数据代入公式（2）计算各部件的危险度，根据各部件危险度数值的大小可对各部件进行安全风险排序，如表 2 所示。

根据各部件的危险度可知，此系统各部件的安全风险排序为：$X_2>X_5>X_6>X_1>X_3>X_4$。通过与该型飞机操纵系统部件所导致事故征候的比重数值相比较（如图 4 所示），不难发现通过该方法计算所得到的部件危险度数据与实际情况有轻微偏差，但大体符合基本情况。因此，采用此种方法可有效定量评估飞机部件的安全风险，对危险度大的部件要进行重点维护，确保飞机飞行安全。

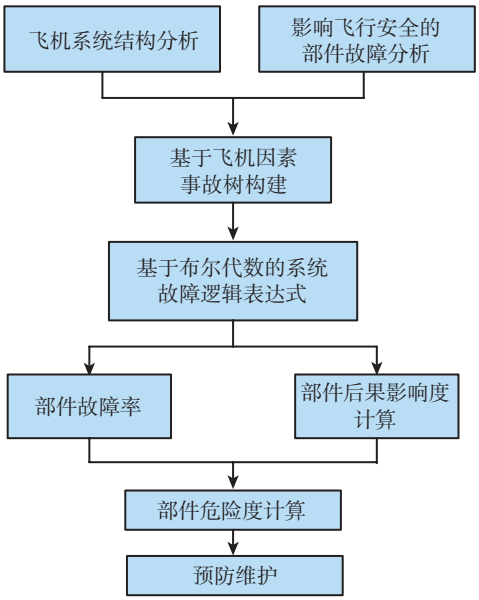

图3　基于事故树的飞机部件安全风险评估步骤

Fig.3　Security risk assessment process of component for aeroplane based on fault tree

表1　某型飞机电传操纵系统部件故障概率

部件	故障原因	概率
X_1	机载计算机故障	2.65E-03
X_2	飞控系统电源失效	3.70E-04
X_3	传感组件失效	4.32E-03
X_4	飞行控制板故障	6.40E-04
X_5	复合舵机不工作	8.21E-03
X_6	操纵液压系统故障	7.63E-03

表2　部件故障后果严重度与危险度

部件	后果严重度	危险度
X_1	5.8608E-06	0.217 8
X_2	4.2020E-05	0.861 4
X_3	1.9282E-08	0.181 7
X_4	2.5319E-08	0.027 4
X_5	1.0308E-09	0.344 7
X_6	9.8152E-07	0.334 0

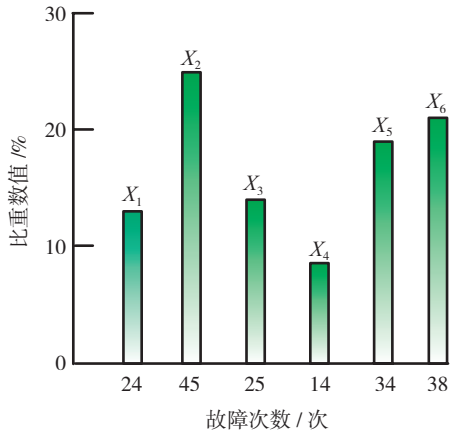

图4　部件故障导致的事故征候统计结果

Fig.4　Statistic analysis of aviation incidents resutted from components failure

4　结论

基于事故树的安全风险评估方法可对飞机部件进行有效评估，可帮助机务人员对飞机部件进行有针对性的重点维护，还可对高危部件展开进一步的事故树分析，查找问题的根源。相比其他方法，该方法解决了飞机部件的定量评估问题，具有显著的便捷性与准确性。

通过该方法计算得到的部件危险度与实际情况大体符合，但存在轻微偏差，究其原因主要是由于航空事故的发生不是飞机本身单一作用的结果，影响飞机飞行任务的多种因素包括机组成员、飞机本身、环境、地面保障与指挥等素。因此，如何在“人－机－环”系统下对飞机部件安全风险展开进一步评估，是下一步的重点研究方向。

参 考 文 献

[1]　陆惠良．军事飞行安全．北京：国防工业出版社，2003.

[2]　Department of Defense. Risk management guide for DOD acquisition（Fourth Edition）. Defense Acquisition University, Defense Systems Management College, 2001.2. 14-15.

[3]　马占新，任慧龙．船舶综合安全评估中的评估方法研究．系统工程与电子技术，2002（10）:57-62.

[4]　顾诵芬．飞机总体设计．北京：北京航空航天大学出版社，2001.

[5]　葛志浩，徐浩军，胡飞．电传操纵系统可靠性分析及飞行安全评估．火力与指挥控制，2005，3（31）:28-31.

（责编　泰山）