一种改进的系统安全性分析方法

李大伟[1],陈云翔[1],徐浩军[2],张 蓉[1]

1. 空军工程大学装备管理与安全工程学院,西安 710051
2. 空军工程大学航空航天工程学院,西安 710038

摘要 系统安全性分析方法是目前广泛采用的飞机安全性设计方法。由于在分析中缺乏对系统整体动态特性的检查,在设计中可能存在可靠性指标分配的不合理。通过面向安全性的风险评估,能够实现系统动态特性的综合验证。提出了一种基于割集和重要度的故障树可靠性指标分配方法,以某型飞机横向电传操纵系统安全性设计为例对顶事件不可靠度指标进行分配,然后结合基于极值理论的飞行风险评估实现了部分底事件可靠性指标的修正。

关键词 系统安全性;指标分配;风险评估;极值理论;综合验证

中图分类号 V22 **文献标识码** A **doi** 10.3981/j.issn.1000-7857.2012.34.005

Improved Method for System Safety Analysis

LI Dawei[1], CHEN Yunxiang[1], XU Haojun[2], ZHANG Rong[1]

1. *Material Management and Safety Engineering Institute, Air Force Engineering University, Xi'an 710051, China*
2. *Aeronautics and Astronautics Engineering Institute, Air Force Engineering University, Xi'an 710038, China*

Abstract The system safety analysis is widely used in the safety design of an aircraft. For lack of checks for dynamic characteristics of the whole system, the distribution of some reliability indexes may not be reasonable. A comprehensive verification of system dynamic characteristics can be realized through the safety-oriented risk assessment. This paper proposes a new method of distributing the reliability index for Fault Tree Analysis (FTA), based on the cut sets and the importance measure. With the safety design of the Fly-By-Wire (FBW) system for an aircraft's rolling channel as an example, the fallibility index of the top event is distributed. Then the distributed reliability indexes are modified, combined with the flight risk assessed by the Extreme Value Theory (EVT), which plays an important role in the system safety analysis.

Keywords system safety; index allocation; risk assessment; EVT; comprehensive verification

0 引言

飞机安全性是制约航空业发展的主要问题。安全性分析是飞机适航合格审定的重要部分[1]。美国机动车工程师学会颁布了 SAE ARP4761 和 SAE ARP4754 等系统安全性分析标准,可以作为飞机设计中安全性分析指南和适航符合性验证方法的参考[2-3]。Burdun 等[4-5]提出了一种基于"人-机-环"复杂系统行为特性仿真的飞机适航性验证方法。熊峻江[6]和李晓磊[7]等对系统安全性分析与设计方法进行了改进。然而,SAE ARP4761 中描述的安全性分析方法侧重从可靠性出发分析系统的安全性,没有考虑诸如控制率、飞行品质等系统特性对安全性的影响。本文通过系统安全性分析方法对可靠性指标进行分配,然后结合面向安全性的风险评估对系统可靠性指标再次分配,能够实现安全性的综合验证。

1 系统安全性分析方法概述

系统安全性分析的基本思想是识别风险并将风险控制在可接受的范围之内[2]。系统安全性分析方法主要包括安全性分析的程序和基本方法两部分。与飞机研发过程相关的系统安全性分析流程可用图 1 表示。

1.1 系统安全性分析的过程

系统安全性分析的过程可分为 FHA (功能危险分析)、PSSA(初步系统安全性分析)和 SSA(系统安全性分析)。

FHA 是系统安全性分析的起点,用于对功能面临的危险的识别和分类。PSSA 是对提出的系统结构进行系统检查,以

收稿日期:2012-09-11;修回日期:2012-10-24
基金项目:国家自然科学基金项目(61074007);国防项目(51327020104)
作者简介:李大伟,博士研究生,研究方向为飞机可靠性安全性保障性建模、装备发展战略与管理决策,电子信箱:lidaweitg@163.com

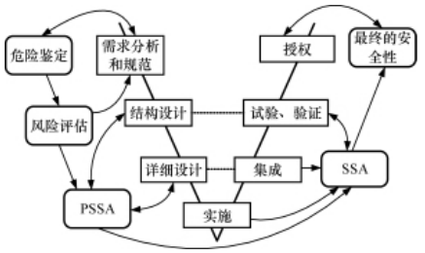

图 1　寿命周期相关的安全评估过程

Fig. 1　Safety analysis during system lifecycle

确定失效是如何引起 FHA 确定的功能危险的。SSA 是系统、综合地评估完成的系统,以验证 FHA 的安全目标和 PSSA 中的安全要求是否得到了满足。

1.2　安全性分析的基本方法

系统安全性分析的方法包括 FTA/关联表法(DD)/马尔科夫分析 (MA)、故障模式及影响分析 (FMEA) 和共因分析(CCA),CCA 又包括区域安全性分析 (ZSA)、特殊风险分析(PRA)和共模分析(CMA)。

2　基于极值理论的小概率事件安全性评估方法

飞行事故的发生是小概率事件。小概率事件具有重尾分布特征,对于有限样本量,采用一般的数理统计很难进行小概率事件的评估。极值理论是次序统计的一个分支,主要研究随机样本以及随机过程中极值的概率值以及统计推断,能够用于拟合样本数据序列分布的尾部特征。

2.1　面向安全性评估的系统建模

建立“人-机”系统模型是风险评估的基础,在 Matlab 环境下可以实现模型的建立。故障模型可根据 FMEA 和工程经验建立。

2.2　极值分布模型

将评估飞行安全中具有决定性的参数称为决定性参数[8]。常见的决定性参数包括迎角、过载、高度、表速、马赫数等。每个决定性参数都有其极限值限制。假设特殊情况下,最先达到极限值的决定性参数为临界参数 x, 当临界参数值超过极限值 (x_{li}) 后, 发生飞行事故。决定性参数有规定的允许值(x_{av}),允许值都小于极限值,如图 2 所示。

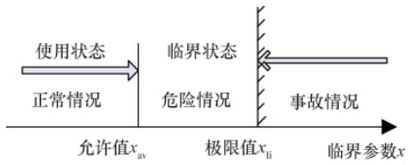

图 2　飞行状态与临界参数关系

Fig. 2　Safety state vesus the critical parameter

设随机量 $Y=\{Y_1,Y_2,\cdots,Y_k\}$是灾难性事件决定性参数的一组样本极值。把 Y 按照递增排列, 可以求取序列 $Y'=\{Y'_1,Y'_2,\cdots,Y'_k\}$。

定义累积概率:$F(Y'_n)=n/k+1$。累积概率序列为

$$F(Y')=\{F(Y'_1),F(Y'_2),\cdots,F(Y'_k)\} \tag{1}$$

设 Y'与累积概率 $F(Y')$近似存在映射

$$f(\cdot):Y'_i\in Y'\mapsto F(Y'_i)\in F(Y') \tag{2}$$

用非线性函数 $f^*(\cdot)$逼近映射 $f(\cdot)$,随机量的极限值为 x_{li},则事故风险发生概率为

$$P_x=P(x<x_{li})=1-f^*(x_{li}) \tag{3}$$

$y=f^*(x)$具有下面性质:(1) $F(Y'_n)\approx f^*(Y'_n)$;(2) $\forall y\in R$, $\exists 0\leqslant x\leqslant 1$;(3) $x_1<x_2$,则 $y_1<y_2$。性质(1)保证了模型的准确性,性质(2)是计算小概率事件发生概率的必要条件,性质(3)属于累积概率的性质。

极值理论涉及极大值和极小值(统称为极值)的极限分布问题。考虑到极值的限制值,将极值分布类型分为 I 型、II 型和 III 型。II 型考虑了存在下限值的情况,III 型考虑了存在上限值的情况。渐进分布类型如图 3 所示。

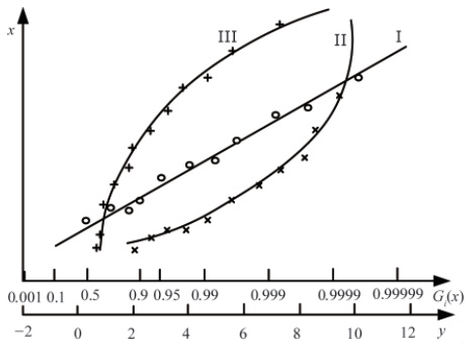

图 3　渐进分布类型

Fig. 3　Asymptotic distribution type

Gumbel 给出了其分布形式[8]。I 型分布为

$$G_1(x)=\exp\{-\exp[-a(x-u)]\} \tag{4}$$

其中,$-\infty<x<+\infty$;$a>0$ 为极值强度函数;u 为特征最大值。

II 型分布为

$$G_2(x)=\exp\left[-\left(\frac{u-a}{x-a}\right)^k\right] \tag{5}$$

其中,$a<x<+\infty$,a 为极限下限;k 为形状参数。

III 型分布为

$$G_3(x)=\exp\left[-\left(\frac{b-x}{b-u}\right)^k\right] \tag{6}$$

其中,$-\infty<x<b$,b 为极限上限。

3　基于割集和重要度的 FTA 可靠性指标分配模型

目前, 工程上采用的可靠性分配方法有考虑重要度、复杂度的分配法、拉格朗日乘数法、动态规划法和直接寻查法等[9-11]。本文提出一种在飞机初步设计阶段,故障树底事件发生概率未知的条件下,基于割集和重要度的 FTA 不可靠度指标快速分配模型。

(1) 系统中最小割集的可靠性分配

假设顶事件所能允许的最大不可靠性为 F,共有 m 个最小割集,分别为 $X_1,X_2,\cdots,X_m$。则最小割集所能容忍的不可靠性为

$$F_{X_i} \leqslant \frac{F}{m} \qquad i=1,2,\cdots,m \tag{7}$$

(2) 基于重要度的可靠性指标二次分配

假设割集 X_i 共包括 n 个底事件,分别为 $y_1,y_2,\cdots,y_n$。在底事件发生概率未知的情况下,用结构重要度表征底事件的重要程度。假设底事件 $y_1,y_2,\cdots,y_n$ 的结构重要度系数分别为 $c_1,c_2,\cdots,c_n$,则对于重要度大的底事件分配低的不可靠度,即

$$F_{y_1}:F_{y_2}:\cdots:F_{y_n}=\frac{1}{c_1}:\frac{1}{c_2}:\cdots:\frac{1}{c_n} \tag{8}$$

并且满足条件

$$F_{y_1}F_{y_2}\cdots F_{y_n} \leqslant F_{X_i} \tag{9}$$

如果最小割集中存在交集,即某个底事件 y_i 的 F_{y_i} 有 j 个值,设为 $F_{y_{i1}},F_{y_{i2}},\cdots,F_{y_{ij}}$。那么

$$F_{y_i}=\min(F_{y_{i1}},F_{y_{i2}},\cdots,F_{y_{ij}}) \tag{10}$$

4　实例

以某型飞机横向电传操纵系统安全性设计为例,从 FHA 出发,经 PSSA 建立了系统级 FTA 作为系统安全性分析的基础。选取系统级 FTA 的部分子树(图 4)研究 PSSA 阶段可靠性指标的综合分配方法。G0(飞控系统控制失效)为顶事件,其不可靠性要求为 1.725×10^{-8}。

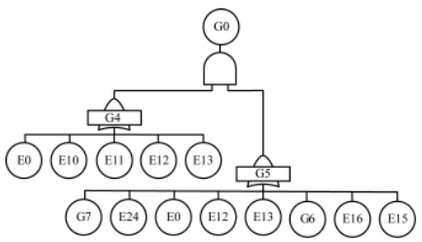

图 4　飞控系统控制失效的故障树

Fig. 4　FTA of flight control system failure

4.1　基于 BBD 方法的底事件重要度计算

如何对 G0 的可靠性指标进行有效分配,是系统安全性设计中重点研究的问题。于捷[10]和徐亨成[11]等研究表明,对于大型复杂故障树,将 FTA 转化为 BDD(二元决策图),利用 BDD 求解底事件重要度能够避免求最小割集和不交化运算,并且得到的结果是精确解,不存在近似。本文采用此方法将图 4 所示的故障树进行转化,得到的 BDD 结构如图 5 所示。

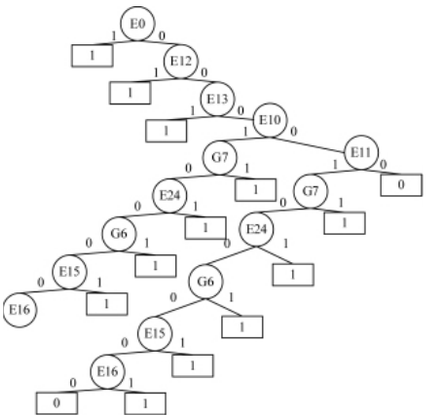

图 5　飞控系统控制失效的 BDD

Fig. 5　BDD of flight control system failure

在系统设计的初始阶段,用结构重要度来表征底事件重要度的大小。基于 BDD 方法计算底事件结构重要度,并与传统 FTA 计算结果进行对比,见表 1。可以看出,传统 FTA 法与 BDD 法计算得到的底事件结构重要度有一定误差。因为 BDD 法能够避免求最小割集和不交化运算,得到的是精确解。

表 1　BDD 法和 FTA 法求解的重要度对比

Table 1　Comparisons of importance measures based on BDD and FTA

编号	底事件	结构重要度		编号	底事件	结构重要度	
		FTA 法	BDD 法			FTA 法	BDD 法
E0	27V 电源完全丧失	0.0141	0.0684	G7	倾斜计算机失效	0.0094	0.0059
E12	迎角测量失效	0.0141	0.0684	E24	倾斜阻尼电门断开	0.0094	0.0059
E13	动压测量失效	0.0141	0.0684	G6	滚转角速度测量失效	0.0094	0.0059
E10	平尾差动计算机失效	0.0235	0.0605	E16	5 号表决器失效	0.0094	0.0059
E11	1 号表决器失效	0.0235	0.0605	E15	静压测量失效	0.0094	0.0059

4.2　基于割集和重要度的系统可靠性指标分配

对于图 4 所示故障树,共有 13 个最小割集,分别为{E0}、{E12}、{E13}、{E10,G7}、{E10,E24}、{E10,G6}、{E10,E15}、{E10,E16}、{E11,G7}、{E11,E24}、{E11,G6}、{E11,E15}、{E11,E16}。

根据式(7)可以求出割集不可靠度要求为 1.3269×10^{-9}。对于含有 2 个底事件的最小割集,根据式(8)和式(9),结合表 1 中的结构重要度进行不可靠度指标的二次分配,最终分配的底事件不可靠度指标如表 2 所示。

表 2　基于割集和重要度分配的底事件不可靠度指标

Table 2　Fallibility of events distributed based on cut sets and importance measures

编号	不可靠度	编号	不可靠度
E0	1.3269×10^{-9}	G7	1.1665×10^{-4}
E12	1.3269×10^{-9}	E24	1.1665×10^{-4}
E13	1.3269×10^{-9}	G6	1.1665×10^{-4}
E10	1.1375×10^{-5}	E16	1.1665×10^{-4}
E11	1.1375×10^{-5}	E15	1.1665×10^{-4}

4.3　基于风险评估的指标综合验证

以底事件 G6 为例。滚转角速度故障服从(-60,60)之间的均匀分布。采用 Monte Carlo 法对系统进行仿真,得到滚转角速度 ω_x 的 30 个样本。横向操纵时,决定性参数选 ω_x,认为 ω_x 超过 90°/s 即发生飞行事故。分别以累积概率及其双负对数为横坐标,ω_x 的极值样本为纵坐标,得到滚转角速度传感器故障后的样本极值分布图,见图 6。采用基于极值分布的最小二乘法估计分布参数,计算得到滚转角速度传感器故障后驾驶员不能排除该故障的概率为 $P_{eG6}=2.4\times10^{-3}$。

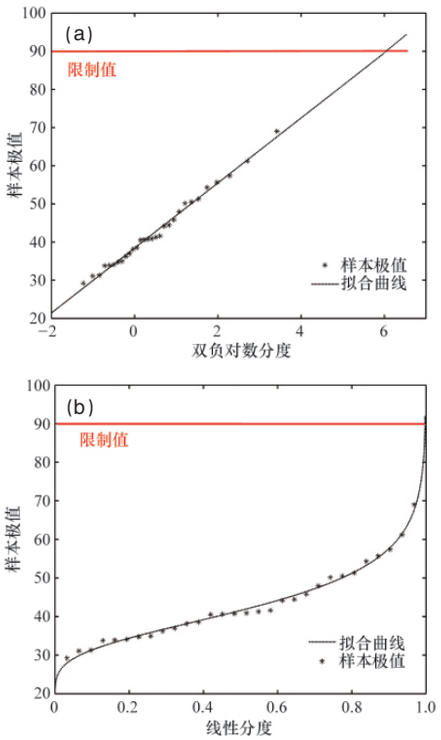

图 6　双负对数分度(a)和线性分度(b)下的样本极值分布

Fig. 6　Extreme-value distribution on double negative logarithm scale (a) and linear scale (b)

同理,计算得 E12,E13 和 E15 条件下驾驶员不能排除该故障的概率分别为 2.1×10^{-7},7.9×10^{-8},4.8×10^{-8}。

对表 2 中分配的底事件不可靠度指标进行再次验证。对于底事件 G6,经重要度分配后的不可靠度指标为 $P_{fG6}=1.1665\times10^{-4}$,驾驶员不能排除底事件 G6 引起飞行事故的概率为 $P_{eG6}=2.4\times10^{-3}$。于是,由底事件 G6 引起的飞行风险概率为 $P(G6)=P_{fG6}P_{eG6}=2.7996\times10^{-7}$,而根据系统安全性标准,I 级飞行事故的发生概率不能高于 1.5×10^{-9}。因此,经系统安全性分析分配的底事件 G6 的不可靠度指标不能满足安全性要求。综合考虑系统整体特性,在系统设计中,G6 的不可靠度指标应该降为 6.27×10^{-7}。同理,对于底事件 E12,E13,E15,经综合验证其不可靠度指标能够满足安全性要求。横向操纵中,滚转角速度测量元件(G6)是影响飞行安全的关键部件。面向安全性的风险评估表明,给 G6 分配的不可靠度指标过高,需要降低其指标值。

5　结论

(1) 通过基于重要度的 FTA 不可靠度指标分配方法,可以实现 FTA 不可靠度指标的快速、合理分配。

(2) 实例研究表明,基于极值理论的飞行风险评估方法可以作为系统安全性分析方法的有效补充。

参考文献(References)

[1] FAA. Advisory Circular AC 23.1309-1C Equipment, systems, and installations in part 23 airplanes[S]. Washington DC: Federal Aviation Administration, 1999.

[2] SAE. SAE ARP4761 Guidelines and methods for conducting the safety assessment process on airborne systems and equipments [S]. Detroit, Michigan: The Engineering Society For Advancing Mobility Land Sea Air and Space, 1996.

[3] SAE. SAE ARP4754 Certification considerations for highly-integrated or complex aircraft systems [S]. Detroit, Michigan: The Engineering Society for Advancing Mobility Land Sea Air and Space, 1996.

[4] Burdun I Y, De Laurentis D A, Mavris D N. Modeling and simulation of airworthiness requirements for an HSCT prototype in early design [R]. AIAA-98-4936, Washington DC: American Institute of Aeronautics and Astronautics, 1998.

[5] Burdun I Y, Mavris D N. A technique for testing and evaluation of aircraft flight performance during early design phases [R]. AIAA-97-5541, Washington DC: American Institute of Aeronautics and Astronautics, 1997.

[6] 熊峻江, 刘宝成, 高宏. 系统安全性分析与设计方法研究[J]. 北京航空航天大学学报, 2002, 28(2): 141-143.
Xiong Junjiang, Liu Baocheng, Gao Hong. *Journal of Beijing University of Aeronautics and Astronautics*, 2002, 28(2): 141-143.

[7] 李晓磊, 田瑾, 赵廷弟. 改进的区域安全性分析方法 [J]. 航空学报, 2008, 29(3): 622-626.
Li Xiaolei, Tian Jin, Zhao Tingdi. *Acta Aeronoutica et Astronautica Sinica*, 2008, 29(3): 622-624.

[8] 葛志浩, 徐浩军, 孟捷. 一种基于最优化的极值分布建模方法[J]. 系统工程与电子技术, 2007, 29(11): 1877-1879.
Ge Zhihao, Xu Haojun, Meng Jie. *Systems Engineering and Electronics*, 2007, 29(11): 1877-1879.

[9] 曾声奎. 任务可靠性指标分配的比例组合法及评分分配法[J]. 航空学报, 1995, 16(S1): 15-19.
Zeng Shengkui. *Acta Aeronoutica et Astronautica Sinica*, 1995, 16(S1): 15-19.

[10] 于捷, 孙立大, 石耀霖, 等. 基于 BDD 技术的数控机床故障树重要度分析[J]. 机床与液压, 2008, 36(12): 186-189.
Yu Jie, Sun Lida, Shi Yaolin, *et al. Machine Tool & Hydraulics*, 2008, 36(12): 186-189.

[11] 徐亨成, 张建国. 基于 BDD 技术下的故障树重要度分析 [J]. 电子机械工程, 2003, 19(6): 1-3.
Xu Hengcheng, Zhang Jianguo. *Electro-Mechanical Engineering*, 2003, 19(6): 1-3.

(责任编辑　安莹,吴晓丽)