基于故障树与马尔科夫分析模型的发动机系统安全性评估

Engine System Safety Analysis Based on Fault Tree and Markov Models

孙杨慧 / Sun Yanghui
（中航商用航空发动机有限责任公司，上海 201108）
（AVIC Commercial Aircraft Engine Co., Ltd., Shanghai 201108, China）

摘　要：
安全性评估是发动机适航验证的重要方法之一，故障树与马尔科夫分析方法是安全性评估常用的方法，两种方法在安全性评估的不同时机具有各自的特点。针对故障树与马尔科夫在安全性评估中的应用时机进行了深入的研究，分析结果表明：对于失效率为常数的顺序相关的系统，若部件是主动失效部件（即 λ×t 较小），应用故障树与马尔科夫分析方法均可准确评估系统的失效概率，采用故障树可以减少运算的复杂性；若部件是潜在失效部件，由于部件暴露时间较长（即 λ×t 较大），使用马尔科夫的分析方法可以更精确的评估系统的安全性。

关键词：发动机；安全性评估；故障树；马尔科夫；定量重要度分析

[**Abstract**] Safety analysis is one of the most important means of compliance demonstration for airworthiness regulation. Fault tree analysis (FTA) and Markov (MA) models are widely used in safety analysis. In this paper, we address the application of FTA and MA model in failure sequence dependent event. The results of FTA are compared with that of MA model. It shows that if the system is composed of items with active failure (λ×t is minor), using either FTA or MA model, we can correctly obtain system failure probability. In addition, we find using FTA analysis could reduce the calculation complexity. However, if the system is composed of items with potential failure, due to the long exposure time (λ×t is major), MA model could be used to analyze system safety more accurately. More detailed analysis indicates that the quantitative analysis of the degree of importance for the top event can be used to establish the system repair method.

[**Key words**] Engine; Safety Analysis; Fault tree; Markov; Quantitative Importance Analysis

0　引言

航空发动机是飞机的心脏，担负着为飞机提供推力与反推力、为机载系统提供输出功率等重要功能，对飞机的安全性有着极为重要的影响，与飞机其他系统相比，对安全性和可靠性有着更高的要求。现代航空发动机系统一般都是由机械、电子、电气、液压等部件组成的典型大型复杂系统，对于此类系统，基于试验的符合性验证方法无法验证系统的所有危险状态，安全性评估方法已成为航空发动机系统不可或缺的适航符合性验证方法，也是CCAR33.75 条款最主要的符合性方法[1]。通过安全性分析能够确保所有发动机失效状态对飞机造成的危险减小到可接受的程度。同时CCAR33.75条款明确提出要对发动机所有的失效可能带来的后果进行分析，这就要求对所有的主动失效部件以及潜在失效部件都要进行安全性分析[1]。

SAE ARP 4761“民用机载系统和设备安全性评估过程的指南和方法”[2]为安全性评估提供了方法，同时也是 33.75 条款咨询通告指定的参考工业标准[1]。在 SAE ARP 4761 标准中，介绍了故障树（FTA）与马尔科夫（MA）分析方法。FTA 分析方

法,具有直观、逻辑性强等特点,与 MA 分析方法相比,FTA 方法计算相对简单,然而这种方法也存在弊端,例如 FTA 方法很难对同时发生的耦合故障、瞬态故障和间歇故障以及动态故障进行有效的建模,同时在处理失效顺序相关的事件时,还存在运算不精确的问题[3]。MA 方法作为另一种安全性评估方法,是对 FTA 分析方法的有效补充,它对动态、可修复系统能够进行有效、精确的建模,同时对于失效顺序相关事件的处理也相当的精确。然而,MA 模型的规模随着系统部件数量的增加呈指数式增长,求解状态微分方程非常繁琐,给安全性分析带来了困难[3]。基于上述两种方法的特点,有必要对 FTA 分析方法以及 MA 分析方法的应用时机展开研究。

本文结合 CCAR33.75 条款的要求,以失效顺序相关系统为分析对象,并充分考虑系统的组成部件(即主动失效部件与潜在失效部件),利用 FTA 方法与 MA 方法分析了在不同暴露时间下系统的失效概率,以及系统组成部件对顶层事件的定量敏感度分析,系统地比较了两种分析方法的仿真结果,并得出了若干有价值的研究成果,该成果可以用来指导安全性分析,保证在最低时间成本条件下实现最精确的安全性分析。

1 FTA 和 MA 分析方法介绍

1.1 失效顺序相关事件 FTA 分析方法的建模过程

在 SAE ARP 4761 标准中[2],给出了处理失效顺序相关事件的故障树分析方法,它是在与门的输入事件中引入失效顺序要求系数,作为一项独立的输入事件,相关失效顺序要求系数计算过程如下:

$$P_{seq}=k/n! \quad (1)$$

式中:n! 表示 n 个输入事件可能发生的顺序;k 表示导致顶层事件发生的输入事件发生顺序。

1.2 失效顺序相关事件 MA 方法的建模过程

基于 MA 方法对系统进行失效概率分析的一般过程为[2,4,5,6]:

(1)分析系统的状态以及系统的组成;

(2)准确定义系统状态,确定不同状态间的状态转移率;

(3)根据系统的运行状态,画出状态转移图;

(4)将状态转移图分解成若干条状态转移链,根据不同链长,推导出计算公式;

(5)对导致系统故障的不同马尔科夫链的概率进行求和,即得到系统的失效概率。

2 FTA 和 MA 方法的建模

为了研究故障树和马尔科夫分析的特点,本文采用失效顺序相关系统作为故障树和马尔科夫的建模对象,以探讨这两种方法在安全性评估中的应用时机。

2.1 系统失效的描述

某一系统的顶层事件,有三个基本输入事件分别为 A、B、C,当三个输入事件同时失效且输入事件 C 发生在 A、B 之前,顶层事件才发生(即系统失效)。其中,三个基本输入事件的失效率分别为:$\lambda_A = 0.000\ 3$;$\lambda_B = 0.000\ 88$;$\lambda_C = 0.001\ 28$。

2.2 基于定性 FTA 的建模分析

根据系统描述,构建故障树,并确定失效顺序相关系数。根据(1)式的计算准则,$P_{seq}=k/n!$,对于研究的系统,导致系统失效的基本事件发生顺序有两种,分别为:CAB、CBA,即(1)式中 k=2;三个基本输入事件发生故障的所有可能顺序有:ABC、ACB、BAC、BCA、CAB、CBA,即(1)式中 n! =6,带入(1)式可以得到 $P_{seq}=k/n! = 2/6 = 1/3$。将失效顺序相关概率作为一项独立与门输入事件,可以构建出顺序相关的顶事件故障树,如图 1 所示。

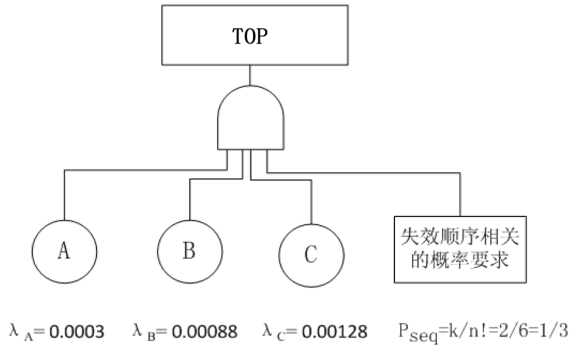

图 1 顶层事件的故障树分析

根据与门的概率计算公式,可以得到基于故障树建模的顶事件的发生概率:

$$P_{top}(t)=\frac{1}{3}(1-e^{(-\lambda_A t)})\times (1-e^{(-\lambda_B t)})\times(1-e^{(-\lambda_C t)}) \quad (2)$$

式中,λ_A、λ_B、λ_C 分别表示部件 A、B、C 的失效率;t 为输入事件的暴露时间。

2.3 基于 MA 的建模分析

依照上述 MA 分析的步骤,并根据系统故障描述,可以得到系统的状态转移图,如图 2 所示。

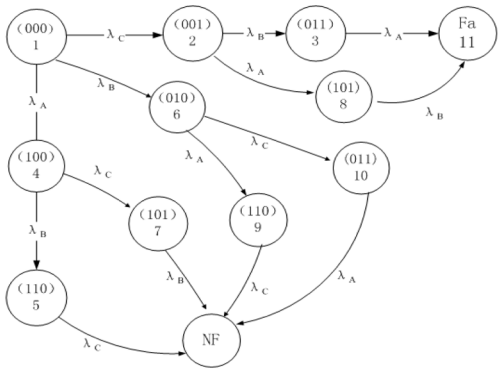

图 2　系统的状态转移图

图 2 中圆圈内三元组分别表示系统组成单元 A、B、C 的状态，0 表示单元正常工作，1 表示单元失效，例如(001)表示单元 A、B 正常，C 失效。根据状态转移图可以得到导致系统故障的马尔科夫链共有两条，如图 3 所示。

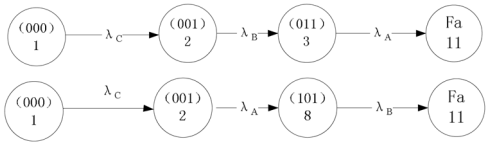

图 3　导致系统故障的马尔科夫链

对于图 4 中链长为 n 的状态转移链 Tn 的概率计算公式由(3)式给出[6]。

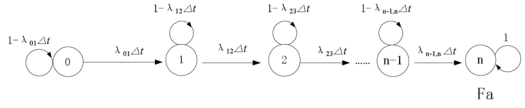

图 4　n 次马尔科夫转移链图

$$p^{T^n}(t)=\prod_{i=1}^{n}\lambda_{i-1,i}\left[\prod_{i=1}^{n}\frac{1}{\lambda_{i-1,i}}-\sum_{i=1}^{n}\frac{e^{-(\lambda_{i-1,i})t}}{\lambda_{i-1,i}\prod_{\substack{i=1\\ j\neq 1}}^{n}(-\lambda_{i-1,i}+\lambda_{j-1,j})}\right] \tag{3}$$

对于所研究的系统，只需计算出上述两条马尔科夫链的转移概率，它们的和即为系统失效的概率：

$$p_1^{T^3}(t)=\lambda_A\lambda_B\lambda_C\left[\frac{1}{\lambda_A\lambda_B\lambda_C}-\frac{e^{-\lambda_C t}}{\lambda_C(-\lambda_C+\lambda_A)(-\lambda_C+\lambda_B)}-\frac{e^{-\lambda_B t}}{\lambda_B(-\lambda_B+\lambda_A)(-\lambda_B+\lambda_C)}-\frac{e^{-\lambda_A t}}{\lambda_A(-\lambda_A+\lambda_B)(-\lambda_A+\lambda_C)}\right] \tag{4}$$

$$p_2^{T^3}(t)=\lambda_A\lambda_B\lambda_C\left[\frac{1}{\lambda_A\lambda_B\lambda_C}-\frac{e^{-\lambda_C t}}{\lambda_C(-\lambda_C+\lambda_A)(-\lambda_C+\lambda_B)}-\frac{e^{-\lambda_A t}}{\lambda_A(-\lambda_A+\lambda_B)(-\lambda_A+\lambda_C)}-\frac{e^{-\lambda_B t}}{\lambda_B(-\lambda_B+\lambda_A)(-\lambda_B+\lambda_C)}\right] \tag{5}$$

$$P_{top}(t)=p_1^{T^3}+p_2^{T^3} \tag{6}$$

3　FTA 和 MA 分析结果的比较

3.1　对于主动失效部件的分析

对于所研究的系统，若三个输入事件均为主动失效部件，则暴露时间即为飞行时间，定义一次飞行时间为 5 小时，取部件的失效率分别为：λ_A = 0.000 3；λ_B = 0.000 88；λ_C = 0.001 28，并将数据带入式(2)与式(6)，利用 MATLAB 软件进行分析，可以得到顶层事件的发生概率随时间的变化曲线，如图 5 所示。

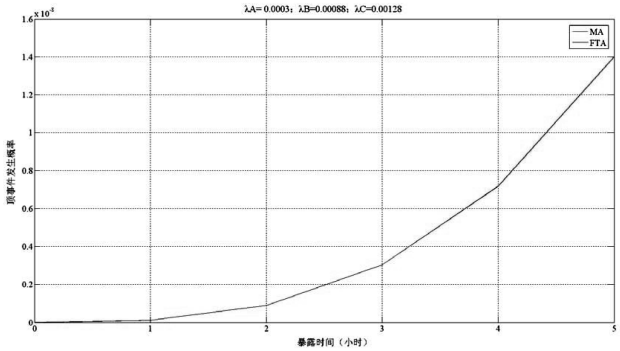

图 5　顶事件的发生概率随时间的变化图

从图中可以得到对于主动失效的部件，即部件的暴露时间较短，利用 FTA 建模与 MA 建模得到的顶层事件的发生概率完全吻合，基于计算的复杂程度，建议使用 FTA 分析方法。

进一步对所分析的系统开展重要度分析，通过改变部件 A、B、C 的失效率，分析了部件失效率的变化对顶事件发生概率的影响。图 6 给出了利用 FTA 方法，得到的部件失效率的变化对顶层事件失效概率的影响，从图中可以获得部件 A 对系统安全性起到关键的作用，其次为 B，最后为 C 为，因此在系统维护过程中应当加强对部件 A 的维护。

3.2　对于潜在失效部件的分析

对于分析的系统，若三个输入事件均为潜在失效部件，即部件的暴露时间较长，一般视为系统的维修时间间隔[2]，取 T = 1000 h。同样取 λ_A = 0.000 3；λ_B = 0.000 88；λ_C = 0.001 28，并将数据带入(2)式与(6)式，利用 MATLAB 软件进行分析，可以得到顶层事件的发生概率随时间的变化曲线，如图 7 所示，从图中可以看出，对于给定的部件失效率，当部件的暴露时间大于 400 h，利用 FTA 与 MA 方法得到的顶事件的发生概率存在较大的差异，运用 FTA 分

（下转第 39 页）

3 结论

根据 t 分布理论,按一定置信度和误差度要求,给出确定最少试件个数的判据。在进行疲劳试验时,可以先进行少数试验然后根据最少试件个数判据确定试验试样是否足够,如果不满足最少试件个数判据则继续试验直至满足最少试件个数判据。如果考虑经济问题,时间成本,并且试件个数 n 不满足估计基值的最少试件个数判据的要求时,则可借助单侧容限系数 k,给具有置信度 γ 的百分位值。最少试件个数的判据法和单侧容限系数法,可以节省试验中大量试验件,减少试验成本。

参考文献:

[1]Federal Aviation Administration. Metallic Materials Properties Development and Standardization (MMPDS). April 2011.

[2]高镇同,熊峻江. 疲劳可靠性[M]. 北京:北京航空航天大学出版社,2000.

(上接第 31 页)

析方法得到的系统失效概率过于保守,鉴于计算的精度,应当采用 MA 分析进行建模计算,以确保系统失效的发生概率满足最低的安全要求。

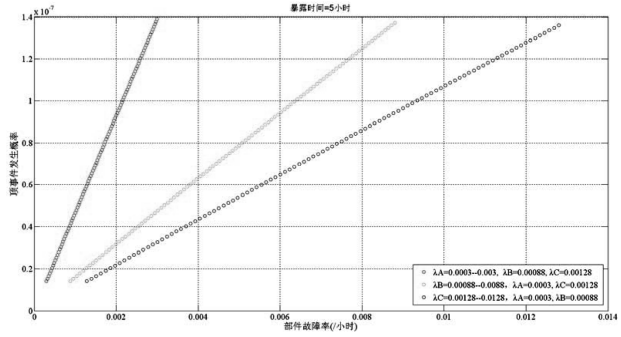

图 6 基于 FTA 方法得到的部件失效率的变化对顶事件发生概率的影响

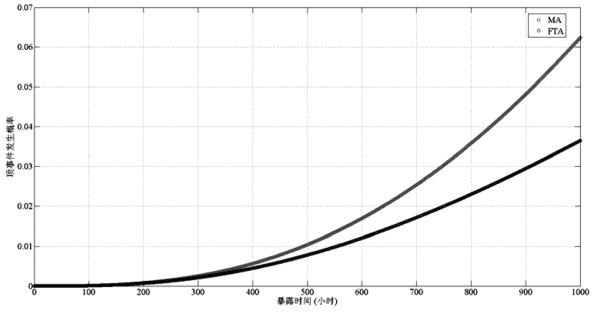

图 7 基于 FTA 与 MA 方法分析潜在失效系统的发生概率随暴露时间的变化

4 结论

本文系统研究了故障树分析与马尔科夫分析在发动机系统安全性评估中的应用时机,研究结论有:

(1)对于所研究的系统,若 λ * t 较小(一般小于 10^{-2}), 则可以采用 FTA 或 MA 方法对系统展开安全性分析,并可以得到相同的分析结果,其中包括系统的失效概率以及部件的重要度;若 λ * t 较大(一般大于 10^{-2}),则应当采用 MA 方法展开分析,若采用 FTA 方法处理这类问题将会导致计算结果过于保守,很难准确的反映系统的安全性。

(2)通过对部件重要度的定量分析,可以得到相关的维修任务,比如维修的优先顺序,系统设计的薄弱环节等信息。

通过对安全性分析方法的系统研究表明,MA 方法与传统的静态 FTA 方法相比,能够更加精确的反映失效顺序相关系统的安全特征。该方法将在发动机系统安全性评估中有非常大的应用前景和优势。

参考文献:

[1] AC33. 75 - 1A. GUIDANCE MATERIAL FOR 14CFR §33.75. SAFETY ANALYSIS [G]. 2007. 9.

[2] SAE ARP4761. The Society of Automotive Engineering. Aerospace Recommended Practice: Guideline and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment[S]. U.S., 1996, 12.

[3] 赵廷弟. 安全性设计分析与验证[M]. 北京: 国防工业出版社, 2011: 158- 159.

[4] 罗云林, 张巨联, 杨剑忠. 基于马尔可夫方法的飞控系统安全性评估[J]. 中国民航大学学报, 2011, 4: 16-19.

[5] Y. Ren, J. B. Dugan., Design of Reliable Systems Using Static & Dynamic Fault Tree [J]. IEEE Trans on Reliability, 1998, 47 (3): 234- 244.

[6] 朱正付, 李长福, 等. 基于马尔科夫链的动态故障树分析方法[J]. 兵工学报, 2008: 1104-1107.