文章编号：2095-2163(2020)03-0138-05 中图分类号：V228.1 文献标志码：A

基于动态故障树的民机燃油系统安全性评估

张 洋[1]，陈志雄[2]，王 烨[3]，蔡 景[4]
（1 上海工程技术大学 机械与汽车工程学院，上海 201620；2 上海工程技术大学 航空运输学院，上海 201620；
3 中国民航上海航空器适航审定中心，上海 200335；4 南京航空航天大学 民航学院，南京 211106）

摘 要：针对民用飞机燃油系统故障的发生具有动态性以及故障发生的概率具有模糊不确定性的问题，提出了一种把模糊理论和 Markov 模型与动态故障树相结合的方法，通过动态故障树得到二元决策图和模糊 Markov 模型分别从定性和定量方面对民机燃油系统进行安全性评估，解决了不确定条件下的民机燃油系统安全性评估问题，并以民机燃油系统的泵丧失向左发动机供油功能为例进行分析，获得了顶事件发生的最小割集以及失效概率曲线，为民机燃油系统的检修与维护提供了理论支撑。

关键词：民机燃油系统；安全性评估；动态故障树；马尔科夫模型；二元决策图；模糊理论

Safety assessment of civil aircraft fuel system based on dynamic fault tree

ZHANG Yang[1], CHEN Zhixiong[2], WANG Ye[3], CAI Jing[4]
(1 School of Mechanical and Automotive Engineering, Shanghai University of Engineering Science, Shanghai 201620, China;
2 School of Air Transportion, Shanghai University of Engineering Science, Shanghai 201620, China;
3 Shanghai Aircraft Certification Center of China Civil Aviation, Shanghai 200335, China;
4 College of Civil Aviation, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

【Abstract】 According to the dynamic characteristic of the fault occurrence and the fuzzy uncertainty of the failure incidence rates of civil aircraft fuel system, fuzzy theory and Markov model are combined with the dynamic fault tree. In the process, make safety assessment of civil aircraft fuel systems from qualitative and quantitative aspects by binary decision diagram and fuzzy Markov model of the dynamic fault tree, solving the safety assessment of civil aircraft fuel system under uncertain conditions, take the pump of the civil aircraft fuel system to lose the fuel supply function to the left engine as an example, obtain the minimum cut set and failure probability curve of the top event. The paper provides theoretical support for the maintenance of the civil fuel system.

【Key words】 civil aircraft fuel system; safety assessment; dynamic fault tree; Markov model; binary decision diagram; fuzzy theory

0 引 言

C919 大型客机试飞工作的加快以及北京大兴机场的投入运营标志着我国自主研制大飞机进程又向前跨越一大步。在民机的设计过程中，公众最为关心的就是其安全性。因此，各飞机制造商越来越注重飞机的系统安全性评估工作，作为安全性评估主要方法之一的故障树分析也得到了充分的研究与发展。民机燃油系统作为高度集成化的复杂系统，集多功能于一体，对整机的安全性影响极大。以往的飞机事故调查表明，燃油系统的故障失效所导致的飞机事故占比很高，迫切需要对民机燃油系统进行有效的安全性评估，降低风险发生的概率。

故障树分析（Fault Tree Analysis，FTA）是一种定性和定量的安全性评估方法，通过以图形的形式显示了导致不希望发生的事件（顶事件）的所有故障原因[1]。故障树常用与门和或门。总地来说，与门相当于所有输入串联的模式；或门相当于所有输入并联的模式。故障树分析针对某一顶事件，建立定性模型，并进行自上而下的分析，一层层向下细化分解，直到得到导致该顶事件的所有最小原因为止[2]。

研究可知，传统的故障树不能评估分析复杂系统的动态故障事件，也难以表示具有冗余和备件的复杂系统[3]。因此，故障树衍生出了各种新的分支，并尤以动态故障树的应用最为广泛。动态故障树分析（Dynamic Fault Tree Analysis，DFTA）是在故障树中引入动态逻辑：例如优先与门（PAND）、顺序相关门（SEQ）、备件门（CSP、WSP、HSP）和功能相关门（FDEP）[4-10]。

1999 年，Dugan 教授结合 Markov 理论和组合数

基金项目：民用飞机专项科研（工信部联装[2016]37 号）；国家自然科学基金（51465047）；航空科学基金（2014ZD56009）。

作者简介：张 洋（1995- ），男，硕士研究生，主要研究方向：安全性评估、持续适航；陈志雄（1977- ），男，博士，副教授，主要研究方向：发动机状态监控与故障预测、航空维修工程。

通讯作者：陈志雄 Email：chenzhixiong1000@ hotmail.com

收稿日期：2019-11-16

学方法建立了动态故障树模型。国内学者结合二元决策图和马尔可夫链应用于动态故障树，对复杂系统做了相关研究。其中，通过二元决策图（BDD）求最小割集，通过模糊马尔科夫模型求解动态故障概率，丰富了传统故障树[11]。作为民机高度集成复杂系统之一的燃油系统，动态故障树方法适用于对其进行安全性评估。

1　理论简介

1.1　动态逻辑门

动态逻辑门包括：优先与门（PAND）、顺序相关门（SEQ）、功能相关门（FDEP）和备件门（CSP、WSP、HSP），见表 1[12]。

表 1　动态逻辑门

Tab. 1　Dynamic logic gate

序号	图形	说明
1.优先与门	PAND A B C	当优先与门的输入事件按顺序发生时，就会导致输出事件发生
2.功能相关门	FDEP T A B C	当功能相关门的触发事件T发生时，就会导致全部相关事件相应发生
3.冷备件门	CSP A S	当冷备件门的主设备失效时，备件开始由未接通状态转为工作状态，主设备与备件均失效时，输出事件发生

1.2　二元决策图

二元决策图（binary decision diagram，BDD）是一种基于 Shannon 分解的有向无环图。BDD 可以简化分析故障树得到最小割集的过程。与门和或门可转化为 BDD，如图 1 所示[13]。

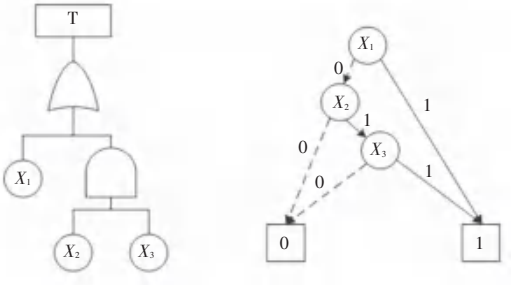

图 1　逻辑与门转化为 BDD

Fig. 1　Logic AND gate transformed into BDD

1.3　Markov 模型

1907 年，Markov 提出 Markov 链，其特点是：系统下一个状态与过去的状态无关，只与系统当前的状态有关。在动态故障树中，割集的发生概率不仅仅与事件的组合有关，还与事件发生的时间节点密切相关。因此选用 Markov 模型处理动态故障树中的割集发生概率问题[14]。

假设 T 为无限实数集，若对每一个 $t \in T$，$X(t)$ 都是一个随机变量，则称 $\{X(t),\ t \in T\}$ 为随机过程。当已知的随机过程在时刻 t_i 处于 x_i 状态的条件下，过程在时刻 $t(>t_i)$ 所处的状态与 t_i 之前的状态无关，而仅和过程在 t_i 所处的状态有关，则该随机过程被称为 Markov 过程。对应的数学公式可写为：

$$P\{X(t_n)=x_n \mid X(t_1)=x_1, X(t_2)=x_2, \ldots, X(t_{n-1})=x_{n-1}\}, \tag{1}$$

其中，$x_i \in S$，S 是随机过程的状态空间。

2　基于模糊 Markov 模型的 DFTA

建立民机燃油系统的动态故障树模型，将其转化为 Markov 模型[15]。状态之间的转移率用模糊数表示，模型的模糊状态转移率矩阵为：

$$\tilde{\boldsymbol{A}} = (\tilde{\lambda}_{i,j}) = \begin{pmatrix} \tilde{\lambda}_{1,1} & \tilde{\lambda}_{1,2} & \cdots & \tilde{\lambda}_{1,n} \\ \tilde{\lambda}_{2,1} & \tilde{\lambda}_{2,2} & \cdots & \tilde{\lambda}_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ \tilde{\lambda}_{n,1} & \tilde{\lambda}_{n,2} & \cdots & \tilde{\lambda}_{n,n} \end{pmatrix}, \tag{2}$$

模糊状态转移图如图 2 所示。图 2 中，S_1 表明系统处于正常状态，$S_i(i=2,\cdots,n-1)$ 表明系统处于存在失效但仍能工作的中间状态，S_n 表明系统处于失效状态。

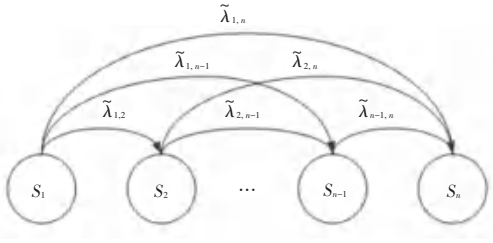

图 2　模糊状态转移图

Fig. 2　Fuzzy state transition diagram

根据模糊转移率得到马尔科夫模型对应的微分方程为：

$$\begin{cases} \dfrac{\mathrm{d}\tilde{p}_1(t)}{\mathrm{d}t} = -\tilde{p}_1(t)\sum\limits_{j=2}^{n}\tilde{\lambda}_{1,j}, \\ \dfrac{\mathrm{d}\tilde{p}_i(t)}{\mathrm{d}t} = \sum\limits_{j=1}^{i-1}\tilde{p}_j(t)\,\tilde{\lambda}_{j,t} - \sum\limits_{j=i+1}^{n}\tilde{p}_i(t)\,\tilde{\lambda}_{i,j}, \\ \dfrac{\mathrm{d}\tilde{p}_n(t)}{\mathrm{d}t} = \sum\limits_{j=1}^{n-1}\tilde{p}_j(t)\,\tilde{\lambda}_{j,n}, \\ 1 < i < n, t \geqslant 0. \end{cases} \tag{3}$$

初始条件 $\tilde{p}_1(0)=1$，$\tilde{p}_i(0)=0(i\neq 1)$，对方程

(3)进行拉普拉斯变换,得线性方程组:

$$\begin{cases} s\,\tilde{p}_1(s) - 1 = -\tilde{p}_1(s)\sum_{i=2}^{n}\tilde{\lambda}_{1,i}, \\ s\,\tilde{p}_i(s) = \sum_{j=1}^{i-1}\tilde{p}_j(s)\,\tilde{\lambda}_{j,i} - \sum_{j=i+1}^{n}\tilde{p}_i(s)\,\tilde{\lambda}_{i,j}, \\ s\,\tilde{p}_n(s) = \sum_{j=1}^{n-1}\tilde{p}_j(s)\,\tilde{\lambda}_{j,n}, \\ 1 < i < n. \end{cases} \tag{4}$$

计算求解上述方程组得到关于 s 的函数 $\tilde{p}_n(s)$,对其作拉普拉斯反变换,求解得到系统状态关于时间的概率分布 $\tilde{p}_n(t)$,带入不同的时间 t 以及底事件的失效模糊概率,得到相应时间系统的失效模糊概率。

3 算例分析

3.1 建立燃油系统动态故障树模型

以"泵丧失向左发动机供油功能" E_1 为顶事件建立动态故障树,其中"泵控制失效" A_1 为静态模块,"泵传感器失效" G_2 和"泵失效" G_3 为动态模块。建立的动态故障树模型如图 3 所示。在此基础上,得到的事件名称以及事件模糊失效率见表 2。结合历史数据、技术手册、统计数据以及行业工作人员经验,得到事件失效率的模糊均值,设定模糊区间为 11%,得到事件的模糊失效率,用三角模糊数表示事件的失效率。

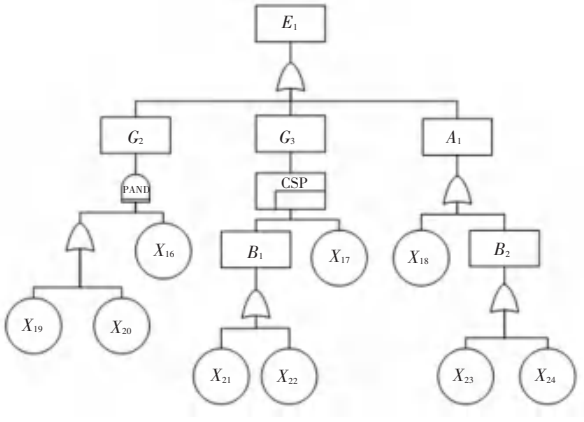

图 3 泵丧失向左发动机供油功能故障树

Fig. 3 The pump loses its fuel supply to the left engine

3.2 基于 BDD 的静态子树分析

将动态故障树转为 BDD 图,详见图 4,由此可以求出顶事件 E_1 的最小割集。

经过 BDD 分析,得到 E_1 故障失效的最小割集为 $\{G_2\}$、$\{G_3\}$、$\{X_{18}\}$、$\{X_{23}\}$、$\{X_{24}\}$。

3.3 基于模糊 Markov 模型的动态子树分析

以"泵丧失向左发动机供油功能" E_1 的子动态故障树"泵传感器失效" G_2 为例,将其转化为模糊马尔科夫模型,如图 5 所示。

表 2 E_1 故障树事件描述以及模糊失效率

Tab. 2 E_1 fault tree event description and fuzzy failure rate

事件	事件描述	模糊失效率 $\tilde{\lambda}(10^{-6}\cdot h^{-1})$
B_1	泵失效	-
B_2	泵电源丧失	-
X_{16}	压力继电器故障	(0.374, 0.420, 0.466)
X_{17}	备用泵失效	(0.570, 0.640, 0.710)
X_{18}	泵控制面板开关故障	(0.463, 0.520, 0.577)
X_{19}	启动异常故障	(0.316, 0.355, 0.394)
X_{20}	关闭异常故障	(0.263, 0.296, 0.329)
X_{21}	泵失去流量或流量减少	(0.401, 0.450, 0.500)
X_{22}	泵供油单向阀不能打开	(0.169, 0.190, 0.211)
X_{23}	泵 SSPC 失效	(0.196, 0.220, 0.244)
X_{24}	泵电源失效	(0.320, 0.360, 0.400)

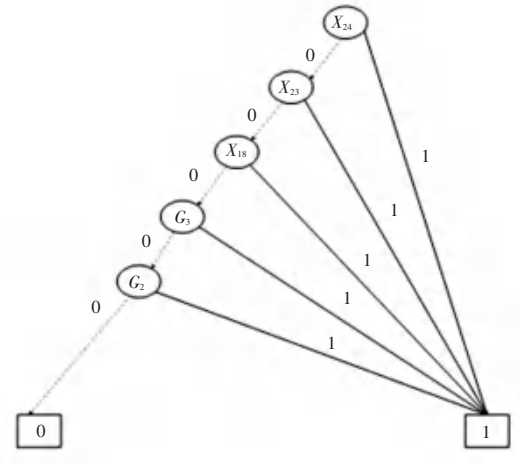

图 4 E_1 转化为 BDD 图

Fig. 4 E_1 transformed into BDD

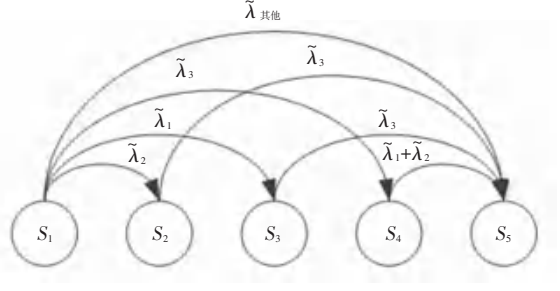

图 5 泵丧失向左发动机供油功能状态转移图

Fig. 5 Status transition diagram of pump losing oil supply to left engine

图 5 中,S_1 表示系统处于正常状态;S_2 表示关闭异常故障导致系统部分故障状态;S_3 表示启动异常故障导致系统部分故障状态;S_4 表示压力继电器故障导致系统部分故障状态;S_5 表示系统处于完全

失效状态。这里，由图 5 可推得：$\tilde{\lambda}_{其他} = \tilde{\lambda}_4 + \tilde{\lambda}_5$，$\tilde{\lambda}_{总} = \tilde{\lambda}_{其他} + \tilde{\lambda}_1 + \tilde{\lambda}_2 + \tilde{\lambda}_3$。其中，$\tilde{\lambda}_1$ 表示 X_{19} 启动异常故障的模糊失效率，$\tilde{\lambda}_2$ 表示 X_{20} 关闭异常故障的模糊失效率，$\tilde{\lambda}_3$ 表示 X_{16} 压力继电器故障的模糊失效率，$\tilde{\lambda}_4$ 表示 G_3 泵失效的模糊失效率，拟定 $\tilde{\lambda}_4$ 为 (0.490,0.550,0.611)，$\tilde{\lambda}_5$ 表示 A_1 泵控制失效的模糊失效率，$\tilde{\lambda}_5 = \tilde{\lambda}_{X_{18}} + \tilde{\lambda}_{X_{23}} + \tilde{\lambda}_{X_{24}}$，经计算，$\tilde{\lambda}_5$ 为 (0.979,1.100,1.221)。

结合状态转移图和各基本事件的模糊失效率得到模糊状态转移率矩阵为：

$$\tilde{\boldsymbol{A}} = \begin{pmatrix} -\sum_{i=1}^{5}\tilde{\lambda}_i & \tilde{\lambda}_2 & \tilde{\lambda}_1 & \tilde{\lambda}_3 & \tilde{\lambda}_{其他} \\ 0 & -\tilde{\lambda}_3 & 0 & 0 & \tilde{\lambda}_3 \\ 0 & 0 & -\tilde{\lambda}_3 & 0 & \tilde{\lambda}_3 \\ 0 & 0 & 0 & -\tilde{\lambda}_1 - \tilde{\lambda}_2 & \tilde{\lambda}_1 + \tilde{\lambda}_2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad (5)$$

状态转移图对应的微分方程为：

$$\begin{cases} \dfrac{\mathrm{d}\tilde{p}_1(t)}{\mathrm{d}t} = -\tilde{p}_1(t)\sum_{i=1}^{5}\tilde{\lambda}_i; \\ \dfrac{\mathrm{d}\tilde{p}_2(t)}{\mathrm{d}t} = \tilde{p}_1(t)\tilde{\lambda}_2 - \tilde{p}_2(t)\tilde{\lambda}_3; \\ \dfrac{\mathrm{d}\tilde{p}_3(t)}{\mathrm{d}t} = \tilde{p}_1(t)\tilde{\lambda}_1 - \tilde{p}_3(t)\tilde{\lambda}_3; \\ \dfrac{\mathrm{d}\tilde{p}_4(t)}{\mathrm{d}t} = \tilde{p}_1(t)\tilde{\lambda}_3 - \tilde{p}_4(t)(\tilde{\lambda}_1 + \tilde{\lambda}_2); \\ \dfrac{\mathrm{d}\tilde{p}_5(t)}{\mathrm{d}t} = \tilde{p}_1(t)\sum_{i=1}^{5}\tilde{\lambda}_i + (\tilde{p}_2(t) + \tilde{p}_3(t))\tilde{\lambda}_3 + \\ \qquad \tilde{p}_4(t)(\tilde{\lambda}_1 + \tilde{\lambda}_2). \end{cases} \quad (6)$$

初始条件为：

$$\begin{cases} \tilde{p}_1(0) = 1, \\ \tilde{p}_i(0) = 0 (1 < i \leqslant 5). \end{cases} \quad (7)$$

利用 Matlab 求解上述微分方程，可以得到系统处于状态 S_5 的概率关于时间的函数，也就是“泵丧失向左发动机供油功能” E_1 的模糊故障概率函数。计算得到 E_1 在不同时间的失效模糊概率。得出不同时间 E_1 的失效模糊概率的隶属函数图。

例如，t = 2 000 h 时，失效模糊概率的隶属函数如图 6 所示，其模糊概率为(0.004 8, 0.005 4, 0.006 0)，表示系统运行至 2 000 h 时，失效概率的最大可能值为 0.005 4。

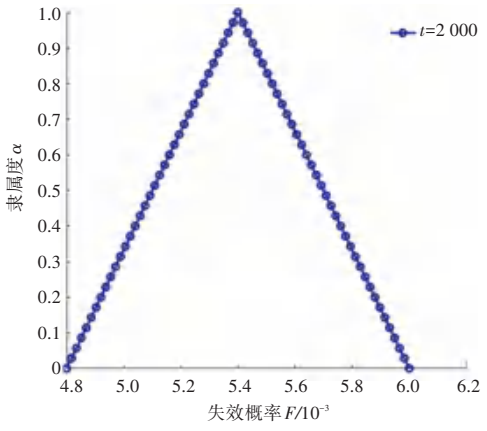

图 6　t=2 000 h，失效模糊概率的隶属函数图

Fig. 6　Membership function graph of failure fuzzy probability when t=2 000 h

4　结束语

本文以民机燃油系统“泵丧失向左发动机供油功能”为顶事件，建立动态故障树模型，结合模糊理论、二元决策图、马尔科夫模型，对其进行定性与定量分析评估，通过二元决策图优化了最小割集的求解方法，通过马尔科夫模型求解出子故障随时间的模糊失效率。为民机燃油系统安全性评估方法做了推进，有利于后续对具有动态特征的民机复杂系统安全性评估工作的开展。

参考文献

[1] CHANG S Y, LIN C R, CHANG C T. A fuzzy diagnosis approach using dynamic fault trees[J]. Chemical Engineering Science, 2002, 57(15): 2971.

[2] SAE APR4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment[S]. USA: The Engineering Society for Advancing Mobility Land Sea Air and Space, 1996.

[3] 韦家增. 故障树分析和模糊理论在机械故障诊断中的应用研究[D]. 合肥：合肥工业大学，2002.

[4] RAUZY A B. Sequence algebra, sequence decision diagrams and dynamic fault trees[J]. Reliability Engineering &System Safety, 2011, 96(7): 785.

[5] GUO Lijie, KANG Jianxin. An extended HAZOP analysis approach with dynamic fault tree[J]. Journal of Loss Prevention in the Process Industries, 2015, 38: 224.

[6] 朱慧慧. 基于改进 FMECA 与 DFTA 的带式输送机可靠性分析[D]. 广州：华南理工大学，2017.

[7] 李彦锋. 复杂系统动态故障树分析的新方法及其应用研究[D]. 成都：电子科技大学，2013.

[8] 杨玲. 基于模糊动态故障树分析法的地铁隧道施工风险分析[D]. 石家庄：石家庄铁道大学，2016.

[9] 徐璇. 面向适航的民机系统动态故障树分析方法研究[D]. 南京：南京航空航天大学，2017.

(下转第 145 页)