http：//myfj. cnjournals. com　myfj_sadri@comac. cc　(021)20866796

DOI：10. 19416/j. cnki. 1674 -9804. 2021. 04. 011

离散时间 T-S 动态故障树在民用飞机辅助动力装置系统安全性评估中的应用研究

陶文操 *　王　栋

(上海飞机设计研究院,上海 201210)

摘　要：辅助动力装置(APU)是安装于飞机上的、用于提供辅助动力源的、自成体系的小型发动机。在民用飞机 APU 系统安全性评估过程中,逐步采用动态故障树对传统故障树进行优化,使故障树分析结果能够更加精确地体现系统失效的动态特性。不同于传统故障树可以根据布尔逻辑求解,动态故障树一般需要转化为同构的状态空间模型才能求解。这种求解过程欠缺通用性,并且存在指数爆炸问题。采用离散时间 T-S 动态故障树计算方法,计算了 APU 系统故障树中的一段子树的顶事件的失效概率,并与使用马尔可夫模型计算的结果进行比较。计算结果发现随着任务时间分段的增加,相对误差单调下降。当任务时间分段大于 5 时,相对误差小于 1%,在计算精度满足要求的情况下能够显著降低计算成本。

关键词：民用飞机;辅助动力装置(APU);系统安全性评估;T-S 动态故障树

中图分类号：V228　　**文献标识码**：A　　**OSID**：

0　引言

故障树分析(Fault Tree Analysis)作为一种故障分析手段,揭示了各个失效事件与其所能导致的上层事件失效状态的关系[1]。传统故障树分析已经广泛应用于复杂系统的安全性与可靠性分析[2-3]。但是对于各个事件之间的交互关系,例如事件的先后发生顺序、动态冗余关系、功能相关性等,都无法在传统故障树中被分析到[4]。基于以上缺陷,动态故障树应运而生并有效解决了传统故障树中失效时序相关、功能冗余等问题。

辅助动力装置(APU)是安装于飞机上的、用于提供辅助动力源的、自成体系的小型发动机[5],其安全性和可靠性指标对全机指标的贡献度较高。在民用飞机 APU 系统安全性评估过程中,也逐步将动态故障树分析应用于安全性定量分析中[6],用于更精确地反映事件失效的动态关系。不同于传统故障树可以应用布尔运算求解,动态故障树的求解有赖于开发新的算法。目前对于动态故障树求解办法的研究非常丰富,包括马尔可夫链法[7]、动态贝叶斯网络法[8]、蒙特卡洛仿真法[9]和多值决策图法[10]等。

本文采用了离散时间 T-S 动态故障树分析方法[11],对民用飞机辅助动力装置(APU)系统故障树分析中的一段子树进行分析,并与马尔可夫链分析的方法进行对比,以确认离散时间 T-S 动态故障树法在辅助动力装置系统安全性分析过程中的有效性和精确度,对 APU 系统的研制和适航取证工作起到积极作用。

1　离散时间 T-S 动态故障树分析

动态故障树是指将动态门引入静态故障树结构而产生的能够表征系统动态特性的故障树[5]。动态门包括“优先与门(PAND)”、“功能相关门(FDEP)”、“顺序相关门(SEQ)”、“冷备件门(CSP)”、“温备件门(WSP)”、“热备件门(HSP)”、“延时门(TD)”等,如图 1 所示,对于各个动态门的解释可参考文献[12]。

* **通信作者**. E-mail：taowencao@comac. cc

引用格式：陶文操,王栋. 离散时间 T-S 动态故障树在民用飞机辅助动力装置系统安全性评估中的应用研究[J]. 民用飞机设计与研究,2021(4):67-72. TAO W C, WANG D. Application of discrete-time T-S dynamic fault tree on safety assessment of auxiliary power unit (APU) system for civil aircraft[J]. Civil Aircraft Design and Research,2021(4):67-72(in Chinese).

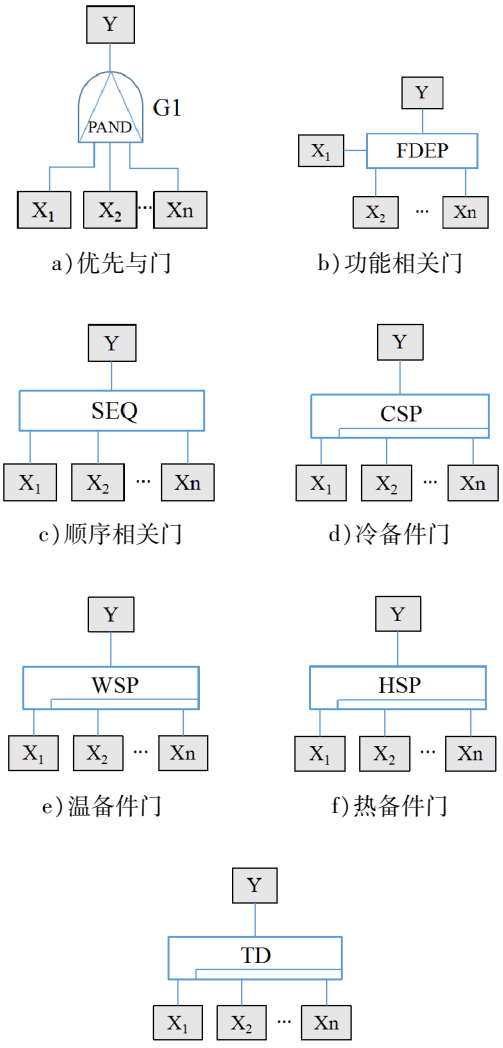

图 1　动态门

离散时间 T-S 动态故障树则将连续的任务时间分割为有限的小段，再根据每个事件在各个时间小段的发生情况建立“离散时间 T-S 动态门规则”，最后依据每一条规则进行计算求得上级事件的失效率。

假设任务时间 t 划分为 m 段，则每一段的时间间隔为 $\Delta = t/m$，假设下级事件数量为 n，则 *T-S* 动态门规则数量为 $l = (m+1)^n$。以功能相关门举例，假设下级事件数量为 $n = 3$，任务时间 t 划分为 $m = 2$ 段，则 T-S 动态门规则数量为 $l = 27$。功能相关门如图 2 所示，当事件 X_1 失效或者 X_2 和 X_3 同时失效时导致上级事件 Y 失效。任务时间分段为 $[0,\Delta]$、$(\Delta, 2\Delta]$ 和 $(2\Delta,\infty)$，事件 $X_i(i \in \{1,2,3\})$ 在时间段 $j(j \in \{1,2,3\})$ 内的失效状态为 $S_{X_i}^{[j]}$，同理上级事件 Y 的失效状态为 $S_Y^{[j]}$。图 2 功能相关门的离散时间 T-S 动态门规则见表 1 所示，其中下级事件 X_i 下的数字表示事件发生的时间段，$P_{(l)}(Y^{[i]})$ 表示上级事件 Y 在规则 l 下在时间段 i 的失效状态为 $S_Y^{(b_Y)}$ 的概率。

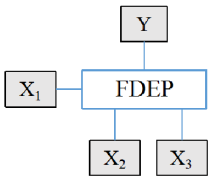

图 2　功能相关门

表 1　离散时间 T-S 动态门规则(功能相关门)

规则 l	X_1	X_2	X_3	$Y = S_Y^{(b_Y)}$		
				1	2	3
1	1	1	1	$P_{(1)}(Y^{[1]})$	$P_{(1)}(Y^{[2]})$	$P_{(1)}(Y^{[3]})$
2	1	1	2	$P_{(2)}(Y^{[1]})$	$P_{(2)}(Y^{[2]})$	$P_{(2)}(Y^{[3]})$
3	1	1	3	$P_{(3)}(Y^{[1]})$	$P_{(3)}(Y^{[2]})$	$P_{(3)}(Y^{[3]})$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
10	2	1	1	$P_{(10)}(Y^{[1]})$	$P_{(10)}(Y^{[2]})$	$P_{(10)}(Y^{[3]})$
11	2	1	2	$P_{(11)}(Y^{[1]})$	$P_{(11)}(Y^{[2]})$	$P_{(11)}(Y^{[3]})$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
26	3	3	2	$P_{(26)}(Y^{[1]})$	$P_{(26)}(Y^{[2]})$	$P_{(26)}(Y^{[3]})$
27	3	3	3	$P_{(27)}(Y^{[1]})$	$P_{(27)}(Y^{[2]})$	$P_{(27)}(Y^{[3]})$

2　离散时间 T-S 动态故障树计算

对于每一条离散时间 T-S 规则 l，对应的执行可能性为：

$$P_{(l)}^{*} = \prod_{i=1}^{n} P_{(l)}(X_i^j) \tag{1}$$

其中，$P_{(l)}(X_i^j)$ 表示事件 X_i 在时间段 j 的故障概率。

$P_{(l)}(X_i^j)$ 的计算方法为事件 X_i 的故障概率密度函数在对应时间分段内的积分：

$$P_{(l)}(X_i^j) = \int_{(j-1)\Delta}^{j\Delta} \lambda_i e^{-\lambda i t} \mathrm{d}t \tag{2}$$

上级事件 Y 在时间段 j 的故障状态 $Y^{[j]}$ 为 $S_Y^{(b_Y)}$ 的概率为：

$$\begin{cases} P(Y^{[j]} = S_Y^{(1)}) = \sum_{l=1}^{r} P_{(l)}^{*} P_{(l)}(Y^{[j]} = S_Y^{(1)}) \\ P(Y^{[j]} = S_Y^{(2)}) = \sum_{l=1}^{r} P_{(l)}^{*} P_{(l)}(Y^{[j]} = S_Y^{(2)}) \\ \vdots \\ P(Y^{[j]} = S_Y^{(b_Y)}) = \sum_{l=1}^{r} P_{(l)}^{*} P_{(l)}(Y^{[j]} = S_Y^{(b_Y)}) \end{cases} \tag{3}$$

其中,$P(Y^{[j]}=S_Y^{(b_Y)})$ 为上级事件 Y 在时间段 j 的故障状态 $Y^{[j]}$ 为 $S_Y^{(b_Y)}$ 的概率。

3　离散时间 T-S 动态故障树在辅助动力装置系统中的应用

辅助动力装置(APU)是一台安装于飞机上的、为飞机提供辅助动力源的燃气涡轮发动机。而安全性评估过程是安全性需求捕获、分配、确认、设计、实现和验证的过程,贯穿整个 APU 系统的研制过程。传统故障树作为安全性定量分析的重要手段已经被应用于 APU 系统安全性工作。但是 APU 系统中存在着功能冗余、时序相关等场景无法用传统故障树精确表达,例如 APU 系统具有两个通道的超速保护机制,超速保护功能失效具有功能冗余性。因此引入动态故障树表现 APU 系统动态特性无论是对 APU 系统的研制还是对适航取证工作都能起到积极作用。

APU 系统故障树分析中常有动态门与静态门组合的情况,如图 3 所示。该故障树为“APU 丧失停车功能”故障树中的一段子树。其中 G_1 为优先与门,当“APU 丧失主数据接口单元全部数据”先于“未探测到的备用数据接口单元产生错误的数据”发生或同时发生时才会导致上级事件“ECU 使用备份数据接口单元产生的错误数据”发生。这是由于 ECU 优先使用来自主数据接口单元传输的数据,只有当主数据接口单元失效时才会采用备用数据接口单元传输的数据。G_2 为或门,当“未探测到的主数据接口单元产生错误的数据”或“ECU 接收来自航电的错误信号”发生时顶事件发生。底事件 X_1、X_2、X_3 的失效率如表 2 所示,任务时间按照中型客机单次平均飞行时间 $t=3$ h 计算。

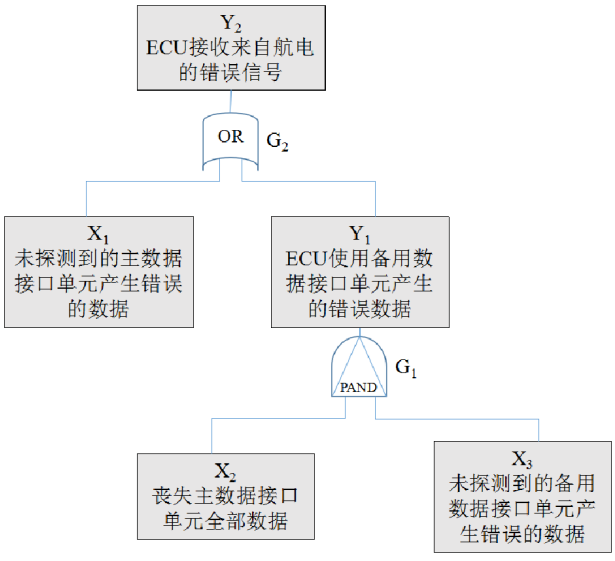

图 3　APU 丧失停车功能的一段子树

表 2　底事件失效率

底事件	失效率符号	失效率/h
X_1	λ_1	1×10^{-6}
X_2	λ_2	8×10^{-4}
X_3	λ_3	4×10^{-5}

3.1 采用马尔可夫链方法求解

采用马尔可夫链方法可以求得动态故障树的解析解。根据图 3 故障树分析失效路径,可以获得马尔可夫状态转移图,如图 4 所示。其中的指代关系见表 3 所示。

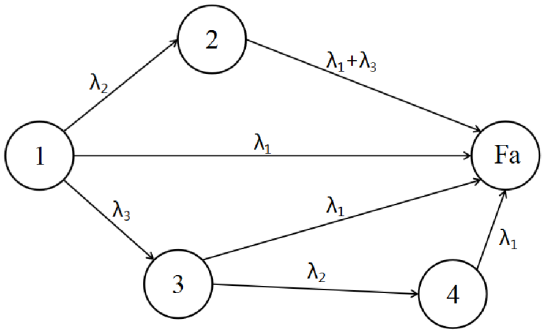

图 4　马尔可夫状态转移图

表 3　马尔可夫链状态指代表

状态	说明	发生概率
1	系统正常状态	$P_1(t)$
2	X_2 失效且系统正常	$P_2(t)$
3	X_3 失效且系统正常	$P_3(t)$
4	X_3 先于 X_2 失效,事件 Y_1 正常,系统正常	$P_4(t)$
Fa	系统失效	$P_5(t)$

由马尔可夫状态转移图可得到状态转移速率矩阵 T 如下:

$$T=\begin{bmatrix} -(\lambda_1+\lambda_2+\lambda_3) & \lambda_2 & \lambda_3 & 0 & \lambda_1 \\ 0 & -(\lambda_1+\lambda_3) & 0 & 0 & \lambda_1+\lambda_3 \\ 0 & 0 & -(\lambda_1+\lambda_2) & \lambda_2 & \lambda_1 \\ 0 & 0 & 0 & -\lambda_1 & \lambda_1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \tag{4}$$

状态转移速率矩阵中第 i 行,第 j 列表示由状态 i 向状态 j 转移的速率,其中 i, j 为自然数,且 i,

$j\in[1,5]$。当 $i=j$ 时，由于状态向外转移，因此转移速率为负。由此列出马尔可夫链微分方程如下：

$$\frac{dP(t)}{dt}=T^{T}P(t) \tag{5}$$

代入马尔可夫状态速率转移矩阵 T 得：

$$\begin{bmatrix}\frac{dP_1(t)}{dt}\\ \frac{dP_2(t)}{dt}\\ \frac{dP_3(t)}{dt}\\ \frac{dP_4(t)}{dt}\\ \frac{dP_5(t)}{dt}\end{bmatrix}=\begin{bmatrix}-(\lambda_1+\lambda_2+\lambda_3) & 0 & 0 & 0 & 0\\ \lambda_2 & -(\lambda_1+\lambda_3) & 0 & 0 & 0\\ \lambda_3 & 0 & -(\lambda_1+\lambda_2) & 0 & 0\\ 0 & 0 & \lambda_2 & -\lambda_1 & 0\\ \lambda_1 & \lambda_1+\lambda_3 & \lambda_1 & \lambda_1 & 0\end{bmatrix}\cdot\begin{bmatrix}P_1(t)\\ P_2(t)\\ P_3(t)\\ P_4(t)\\ P_5(t)\end{bmatrix} \tag{6}$$

根据边界条件 $P(t=0)=[1\quad 0\quad 0\quad 0\quad 0]^{T}$ 求解微分方程组，可得到 $P_1(t)\sim P_5(t)$ 的解析解如下：

$$\begin{aligned}P_1(t)&=e^{-(\lambda_1+\lambda_2+\lambda_3)t}\\ P_2(t)&=e^{-(\lambda_1+\lambda_3)t}-e^{-(\lambda_1+\lambda_2+\lambda_3)t}\\ P_3(t)&=e^{-(\lambda_1+\lambda_2)t}-e^{-(\lambda_1+\lambda_2+\lambda_3)t}\end{aligned} \tag{7}$$

$$P_4(t)=\frac{\lambda_3}{\lambda_2+\lambda_3}e^{-\lambda_1 t}-e^{-(\lambda_1+\lambda_2)t}+\frac{\lambda_2}{\lambda_2+\lambda_3}e^{-(\lambda_1+\lambda_2+\lambda_3)t}$$

$$P_5(t)=\frac{\lambda_3}{\lambda_2+\lambda_3}e^{-(\lambda_1+\lambda_2+\lambda_3)t}-e^{-(\lambda_1+\lambda_3)t}-\frac{\lambda_3}{\lambda_2+\lambda_3}e^{-\lambda_1 t}+1$$

将失效率 $\lambda_1\sim\lambda_3$ 和任务时间 $t=3$ h 分别代入，可得顶事件的失效率 $P_5(t=3)=3.143\,87\times10^{-6}$

3.2 采用 T-S 动态故障树方法分析

将任务时间划分为 $m=2$、3、5、10、20、30、50、100 段，则每段任务时间的长度 $\Delta=T/m$。此处以 $m=2$ 为例，其他任务分段数的计算方法类似。当 $m=2$ 时，$\Delta=1.5$ h，任务时间段为[0，1.5 h]、(1.5 h，3 h]和(3 h，∞)。中间事件 Y_1 和顶事件 Y_2 的发生情况如表 4 和表 5 所示。

表 4　优先与门 G_1 发生规则

规则 l	X_2	X_3	$Y_1=1$		
			1	2	3
1	1	1	1	0	0
2	1	2	0	1	0
3	1	3	0	0	1
4	2	1	0	0	0
5	2	2	0	1	0
6	2	3	0	0	1
7	3	1	0	0	1
8	3	2	0	0	1
9	3	3	0	0	1

表 5　或门 G_2 发生规则

规则 l	X_1	X_1	$Y_2=1$		
			1	2	3
1	1	1	1	0	0
2	1	2	1	0	0
3	1	3	1	0	0
4	2	1	1	0	0
5	2	2	0	1	0
6	2	3	0	1	0
7	3	1	1	0	0
8	3	2	0	1	0
9	3	3	0	0	1

在建立 T-S 发生规则之后，按照公式(1)～(3)计算顶事件 Y_2 的失效率，得到的离散时间 T-S 动态故障树求解结果如表 6 所示。可以看出随着任务时间分段数的增加，T-S 动态故障树的求解结果越来越逼近利用马尔可夫链求得的解析解，相对误差逐渐缩小，证实了离散时间 T-S 动态故障树分析方法的可行性。同时相比马尔可夫链等状态空间模型方法，T-S 动态故障树法采用数值计算方法，显著降低了计算成本。

表 6　动态故障树求解结果

马尔可夫链求解	T-S 动态故障树求解		相对误差/%
	任务分段数 m	T-S 动态故障树结果	
$3.143\,87\times10^{-6}$	2	$3.215\,40\times10^{-6}$	2.275 42
	3	$3.191\,44\times10^{-6}$	1.513 23
	5	$3.172\,27\times10^{-6}$	0.903 41
	10	$3.157\,89\times10^{-6}$	0.446 00
	20	$3.150\,70\times10^{-6}$	0.217 29
	30	$3.148\,30\times10^{-6}$	0.141 05
	50	$3.146\,39\times10^{-6}$	0.080 05
	100	$3.144\,95\times10^{-6}$	0.034 31

4　结论

研究离散时间 T-S 动态故障树在民用飞机辅助动力装置(APU)系统中的应用,本文采用上述计算方法,计算了 APU 系统故障树分析中的一段子树的顶事件的失效率,并与使用马尔可夫模型计算的结果进行比较,得到的结论如下:

1)随着任务时间划分段数的增加,离散时间 T-S 动态故障树分析方法求解的结果与马尔可夫链求解的结果相对误差逐渐减小。当任务时间分段数大于 5 时,相对误差小于 1%,计算精度可接受;

2)相比于状态空间模型方法,离散时间 T-S 动态故障树采用数值计算方法,在保证计算精度的前提下显著降低计算成本,在工程领域具有应用价值。

参考文献:

[1] LEE W S, GROSH D L, TILLMAN F A, et al. Fault tree analysis, methods, and applications-a review[J]. IEEE Transactions on Reliability, 1985, 34(3):194-203.

[2] 廖柯熹, 姚安林, 张淮鑫. 长输管道失效故障树分析[J]. 油气储运, 2001(1):27-30;57.

[3] 陈朝阳,张代胜,任佩红,等. 基于故障树分析法的汽车故障诊断专家系统[J]. 农业机械学报, 2003, 34(5):130-133;118.

[4] CEPIN M, MAVKO B. A dynamic fault tree[J]. Reliability Engineering & System Safety, 2002, 75(1):83-91.

[5] 李东杰. 辅助动力装置的应用现状和发展趋势[J]. 航空科学技术, 2012,(6):7-10.

[6] 王栋. 基于动态故障树分析的民用飞机辅助动力装置系统安全性评估[J]. 民用飞机设计与研究,2014(3):48-52.

[7] 朱正福, 李长福, 何恩山,等. 基于马尔可夫链的动态故障树分析方法[J]. 兵工学报, 2008(9):1104-1107.

[8] 周忠宝, 马超群, 周经伦,等. 基于动态贝叶斯网络的动态故障树分析[J]. 系统工程理论与实践, 2008, 28(2):35-42.

[9] 戴志辉, 王增平, 焦彦军. 基于动态故障树与蒙特卡罗仿真的保护系统动态可靠性评估[J]. 中国电机工程学报, 2011, 31(19):105-113.

[10] 王斌,吴丹丹,莫毓昌,等. 基于多值决策图的动态故障树分析方法[J]. 计算机科学,2016,43(10):70-73;92.

[11] 姚成玉,饶乐庆,陈东宁,等. T-S 动态故障树分析方法[J]. 机械工程学报, 2019, 55(16):17-32.

[12] 饶乐庆. T-S 动态故障树分析方法及在液压系统中的应用[D]. 秦皇岛:燕山大学,2018:11-13.

作者简介

陶文操　男,硕士,助理工程师。主要研究方向:APU 系统集成设计。E-mail: taowencao@comac.cc

王　栋　男,硕士,高级工程师。主要研究方向:APU 系统集成设计。E-mail: wangdong@comac.cc

Application of discrete-time T-S dynamic fault tree on safety assessment of auxiliary power unit (APU) system for civil aircraft

TAO Wencao *　WANG Dong

(Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

Abstract: Auxiliary power unit (APU) is a small-sized engine installed on the aircraft which is used to provide auxiliary power resource. In the process of APU system safety assessment of civil aircraft, dynamic fault tree is gradually used to optimize the traditional fault tree, so that the fault tree analysis results can more accurately reflect the dynamic characteristic of system failure. Different from the traditional fault tree, it can be solved by Boolean logic; dynamic fault tree usually needs to be transformed into isomorphic state space model to solve. This kind of solution process lacks generality and has the problem of exponential explosion. In this paper, the discrete-time T-S

dynamic fault tree calculation method was employed to calculate the failure probability of the top event of a subtree in APU system fault tree, and the results were compared with those calculated by Markov model. The results show that the relative error decreases monotonously with the increase of task time segments. When the task time segment is more than 5, the relative error is less than 1%, which can significantly reduce the calculation cost when the calculation accuracy meets the requirements.

Keywords: civil aircraft; auxiliary power unit(APU); system safety assessment; T-S dynamic fault tree

* Corresponding author. E-mail: taowencao@comac.cc