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

Safety Assessment of Auxiliary Power Unit (APU) System for Civil Aircraft Based on Dynamic Fault Tree Analysis (DFTA)

王　栋 / Wang Dong
(上海飞机设计研究院,上海 201210)
(Shanghai Aircraft Design and Research Institute, Shanghai 201210, China)

摘　要:
在民用航空工业领域,传统的故障树分析方法广泛运用于系统安全性评估。然而,包含系统/子系统运行的时序阐述以及备份、冗余表达在内的动态特性不能通过传统故障树呈现。另一方面,民用飞机辅助动力装置(APU)经常作为一个冗余系统运作,因而其行为可以通过运用动态故障树进行适当的描述。所以 APU 的这种特性激发了动态故障树分析在 APU 系统安全性评估上应用的关注。首先介绍了两种动态门(优先与门和冷备件门),其定量计算通过施用马尔可夫模型来呈现;然后分别通过传统故障树以及动态故障树分析了 APU 系统安全性评估的两个典型案例;最后进行了两种故障树分析(FTA)的比较,其结果显示出通过合理的应用,动态故障树(DFTA)方法达到了对于真实情况来说相当高的精度,并且对指数分布函数施用二阶近似后,其运算成本也是可以接受的。

关键词:民用飞机;辅助动力装置(APU);系统安全性评估;动态故障树分析(DFTA)
中图分类号:V228　　**文献标识码:**A

[**Abstract**] Traditional fault tree analysis method is widely used for system safety assessment in civil aviation industry, but dynamic characteristics of systems/subsystems, including operational sequencing interpretation, spare and redundancy expression cannot be represented by traditional fault trees. On the other hand, civil aircraft auxiliary power unit (APU) often operates as a redundant system and its behavior can be described by using dynamic fault tree appropriately. As a result, the interest of DFTA application is focused on APU system safety assessment. In this paper, two kinds of dynamic gates (PAND and CSP) were introduced firstly. Their quantitative calculations were presented by applying Markov model. Then two typical cases with auxiliary power unit (APU) system safety assessment were analyzed by traditional fault tree and dynamic fault tree respectively. Finally the comparison between two kinds of Fault Tree Analysis (FTA) was provided and the result indicates that Dynamic Fault Tree Analysis (DFTA) method based on proper application reaches remarkable accuracy, and the calculation cost is acceptable when second-order approximation of exponential distribution function is applied.

[**Key words**] Civil Aircraft; Auxiliary Power Unit; System Safety Assessment; Dynamic Fault Tree Analysis

0　引言

故障树分析(FTA)是一种演绎分析方法[1],该方法与相关图(Dependence Diagram)、马尔可夫分析(Markov Analysis)一并收录于 SAE ARP 4761[2],作为一种标准化工具广泛应用于民机系统安全性评估领域。然而,传统的故障树分析是一种基于静态逻辑和静态故障模式的分析方法,它对具有动态

随机性故障的容错系统、具有冗余的可修系统、具有公用资源库的系统以及具有顺序相关性的可靠性分析是不适用的[3]。为使其适用,在安全性评估的工程实践上,常忽略系统的动态特性而只考虑其静态特性,由此得到的分析结果存在一定的误差。在安全性要求日趋严格、营运人和乘客对民机安全性日益关注的背景下,通过应用动态故障树得到更为准确的分析结果将对飞机适航取证工作以及提高飞机竞争力有一定的帮助。

辅助动力装置(APU)是安装在飞机上的小型动力装置,其核心类似于涡轮轴发动机[4]。APU 主要功能是向飞机提供辅助电源和气源,与动力装置不同,在实际运营中 APU 往往扮演着公共资源的备份或冗余系统的角色;另外,APU 具有自动停车功能,在遇到紧急情况如 APU 超转发生时可以自动关闭燃油切断阀使 APU 停车,因此对于 APU 不可控超转这项失效状态来说,其下层事件的发生具有时序特性,即自动停车功能的失效必须先于超转的发生才会导致 APU 不可控超转的发生。类似的例子还有很多,本文将取其中两个较为典型的失效事件进行分析。总之对于 APU 系统安全性评估,其动态特性是值得关注的。

国内外许多研究人员对 DFTA 进行了理论研究以及应用[5-7],指出了 DFTA 求解较繁琐[5]并且存在状态空间爆炸问题[6-7],但是对于 APU 系统安全性评估来说,并不会存在非常复杂的马尔可夫链,一般链长为 2 的故障树结构,即双输入的优先与门和冷备件门就足够了。而对于求解较繁琐的问题,本文对上面提及的这两种动态门进行了解析求解,然后对指数项施用了二阶近似法,在保证精确度的前提下得到了简单易用的计算式,可用于工程实践。

1 动态故障树的定性分析

所谓动态故障树,是指将动态门(dynamic gates)引入静态故障树结构而生成的一种可以表征系统动态特性的故障树。对动态故障树进行定性分析和/或定量计算的活动便称为动态故障树分析(DFTA)。与静态门施用布尔逻辑(Boolean logic)就可以完成分析任务不同,动态门需要施用马尔可夫模型(Markov models)进行分析。关于动态门的详细描述可参看文献[3],本文仅给出对 APU 系统安全性评估影响比较大的两种动态门——优先与门(PAND)与冷备件门(CSP)的定性分析与定量计算。

1.1 优先与门的定性分析

优先与门是与门的拓展,它在与门的基础上增加了一个约束条件,该条件要求输出事件必须按顺序依次发生。例如,要使图 1 中的输出事件 S 发生,需要满足以下两个条件:① 输入事件 A 和输入事件 B 都发生;② 输入事件 A 先于输入事件 B 发生。其对应的马尔可夫链如图 2 所示。

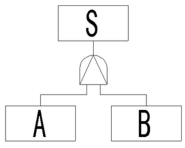

图 1 优先与门

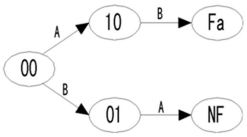

图 2 优先与门的马尔可夫模型

1.2 冷备件门的定性分析

当一个活动系统的功能可由另一个备份系统的功能代替,并且仅在活动系统失效时备份系统才开始工作的情况下,可以用冷备件门来描述其动态特性。冷备件门是与门的另一种拓展形式,具有输入事件依次工作的动态特性。冷备件门的结构示意图及其对应的马尔可夫模型如图 3、图 4 所示。

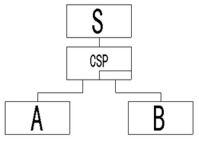

图 3 冷备件门

图 4 冷备件门的马尔可夫模型

2 动态故障树的定量计算

布尔逻辑不适用于动态故障树的计算,对于简单的树形结构可以在将其转化为马尔可夫模型之后求得其解析解。

2.1 优先与门的定量计算

以图 2 所示的马尔可夫模型为例,各状态的发生概率的字母指代见表 1,输入 A 与输入 B 的转移率(即故障树中事件 A 与事件 B 对应的失效状态的失效率)的字母指代见表 2。

表 1　发生概率的字母指代

状态	发生概率
00	P_1
10	P_2
Fa	P_3
01	P_4
NF	P_5

表 2　转移率的字母指代

输入	转移率
A	λ_1
B	λ_2

根据表 1 与表 2 写出状态“00”的微分方程组：

$$\left\{\begin{array}{l}\dfrac{\mathrm{d}P_1(t)}{\mathrm{d}t}=-(\lambda_1+\lambda_2)P_1(t)\\ P_1(0)=1\end{array}\right\} \tag{1}$$

解得：

$$P_1(0)=\mathrm{e}^{-(\lambda_1+\lambda_2)t} \tag{2}$$

类似地，写出状态“10”的微分方程组：

$$\left\{\begin{array}{l}\dfrac{\mathrm{d}P_2(t)}{\mathrm{d}t}=\lambda_1P_1(t)-\lambda_2P_2(t)\\ P_2(0)=1\end{array}\right\} \tag{3}$$

解得：

$$P_2(t)=-\mathrm{e}^{-(\lambda_1+\lambda_2)t}+\mathrm{e}^{-\lambda_2t} \tag{4}$$

类似地，写出状态“Fa”的微分方程组：

$$\left\{\begin{array}{l}\dfrac{\mathrm{d}P_3(t)}{\mathrm{d}t}=\lambda_2P_2(t)\\ P_3(0)=0\end{array}\right\} \tag{5}$$

解得：

$$P_3(t)=\frac{\lambda_2}{\lambda_1+\lambda_2}e^{-(\lambda_1+\lambda_2)t}-\mathrm{e}^{-\lambda_2t}+\frac{\lambda_1}{\lambda_1+\lambda_2} \tag{6}$$

这样就得到了图 2 上半部分各状态的失效概率，对于下半部分，根据对称性原则，易得到：

$$P_4(t)=-\mathrm{e}^{-(\lambda_1+\lambda_2)t}+\mathrm{e}^{-\lambda_1t} \tag{7}$$

以及，

$$P_5(t)=\frac{\lambda_1}{\lambda_1+\lambda_2}\mathrm{e}^{-(\lambda_1+\lambda_2)t}-\mathrm{e}^{-\lambda_1t}+\frac{\lambda_2}{\lambda_1+\lambda_2} \tag{8}$$

最后回到图 1 的优先与门，其输出 S 发生的概率便可以通过式(6)来求得。

2.2　冷备件门的定量计算

以图 4 所示的马尔可夫模型为例，各状态的发生概率的字母指代见表 3，输入 A 与输入 B 的转移率(即故障树中事件 A 与事件 B 对应的失效状态的失效率)的字母指代见表 4。

表 3　发生概率的字母指代

状态	发生概率
00	P_1
10	P_2
Fa	P_3

表 4　转移率的字母指代

输入	转移率
A	λ_1
B	λ_2

根据表 3 与表 4 写出状态“00”的微分方程组：

$$\left\{\begin{array}{l}\dfrac{\mathrm{d}P_1(t)}{\mathrm{d}t}=-\lambda_1P_1(t)\\ P_1(0)=1\end{array}\right\} \tag{9}$$

解得：

$$P_1(t)=\mathrm{e}^{-\lambda_1t} \tag{10}$$

类似地，写出状态“10”的微分方程组：

$$\left\{\begin{array}{l}\dfrac{\mathrm{d}P_2(t)}{\mathrm{d}t}=\lambda_1P_1(t)-\lambda_2P_2(t)\\ P_2(0)=0\end{array}\right\} \tag{11}$$

解得：

$$P_2(t)=\frac{\lambda_1}{\lambda_2-\lambda_1}(\mathrm{e}^{-\lambda_1t}-\mathrm{e}^{-\lambda_2t}) \tag{12}$$

特别地，当 $\lambda_2=\lambda_1$ 时，需要对式(4)求极限，施用洛必达法则，得到：

$$\lim_{\lambda_2\to\lambda_1}P_2(t)=\lambda_1t\mathrm{e}^{-\lambda_1t} \tag{13}$$

类似地，写出状态“Fa”的微分方程组：

$$\left\{\begin{array}{l}\dfrac{\mathrm{d}P_3(t)}{\mathrm{d}t}=-\lambda_2P_2(t)\\ P_3(0)=0\end{array}\right\} \tag{14}$$

解得：

$$P_3(t)=1+\frac{\lambda_2}{\lambda_1+\lambda_2}\mathrm{e}^{-\lambda_1t}+\frac{\lambda_1}{\lambda_2+\lambda_1}\mathrm{e}^{-\lambda_2t} \tag{15}$$

$$\lim_{\lambda_2\to\lambda_1}P_3(t)=1-\mathrm{e}^{-\lambda 1t}(1+\lambda_1t) \tag{16}$$

最后回到图 3 的冷备件门，其输出 S 发生的概率便可以通过式(15)或(16)来求得。

2.3　计算式的一阶近似

对 $f(t)=\mathrm{e}^{-\lambda_1t}$ 进行泰勒展开，得到：

$$f(t)=\mathrm{e}^{-\lambda_1t}=1-\lambda t+\frac{1}{2}\lambda^2t^2-\frac{1}{6}\lambda^3t^3\cdots\cdots+R_n \tag{17}$$

式中 R_n 为余项。

在传统故障树分析中，常采取式(17)的一阶近

似，即 $e^{-\lambda_1 t} \approx 1-\lambda t$ 来简化计算，在文献[1]和[2]中也都认可了这种近似（前提是 $\lambda t \leqslant 0.1$）。但是对式(6)或式(15)施用一阶近似后求得 $P(3)=0$，显然该结果误差较大。因此需要采用更高阶的近似值。

对式(17)取其二阶近似，得到：

$$e^{-\lambda_1 t} \approx 1-\lambda t+\frac{1}{2}\lambda^2 t^2 \tag{18}$$

将式(18)分别代入式(6)、(15)，得到了动态门的二阶近似计算式（优先与门和冷备件门的近似式相同）：

$$P_{3\_PAND}(t)=P_{3\_CSP}(t)=\frac{1}{2}\lambda_1\lambda_2 t^2 \tag{19}$$

假设 $\lambda_1=2\times10^{-3}/h$、$\lambda_2=7\times10^{-4}/h$，图5给出了顶事件发生概率与系统工作时间的关系，实线代表优先与门的解析解，双画线代表冷备件门的解析解，点画线代表二阶近似解。两个解析解都通过使用 Reliability workbench 软件的 Markov 模块进行了验证，结果是符合的。图5表明：当系统工作时间为10h，其误差不超过1.2%，即使工作时间达到100h，误差也不超过12%。不过对于隐蔽失效来说，其失效暴露时间往往比较长（超过100h），近似式可能不再适用，文献[8]对这种情况进做了定量分析，因此对于隐蔽故障来讲，不论是静态还是动态故障树的计算都不能采用近似式。对于显性失效来说，式(19)是合理、可行的。

3 案例分析

通过传统故障树进行 APU 系统安全性评估时，无法表达 APU 的动态特性。下面对两个比较典型的故障树案例改用动态门进行分析并与原先的静态门进行比较。

3.1 优先与门案例

图6是 APU 系统安全性评估中的一个典型事件“APU 超速（APU over speed）”的一段子树，当 APU 的转速传感器产生出错误的转速信号，且电子控制单元（ECU）的信号处理模块未能探测该错误时，ECU 就会判断该信号有效，并控制燃油模块维持这个“错误”的转速，最终可能导致实际转速过快。从动态特性上来讲，只有信号处理模块失效的发生先于转速传感器失效的发生才会导致顶事件发生。

将图6中的与门改成优先与门，其余不变，便得到了一个动态子树。假设两个底事件的失效率分别为 $\gamma_1=5.1\times10^{-3}/h$ 和 $\gamma_1=2.6\times10^{-4}/h$，工作时间为2h，分别对两种故障树进行计算，得出的结果如表5所示。

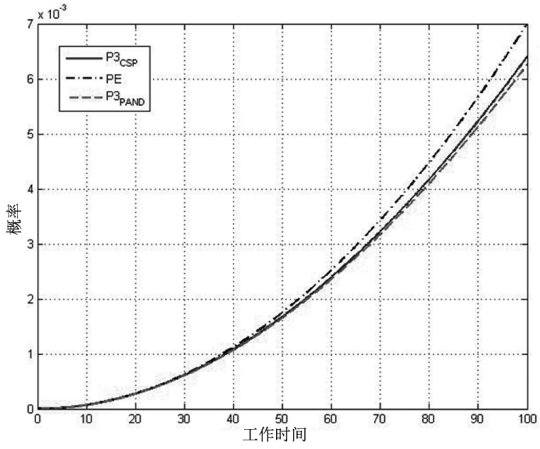

图5 二阶近似式的误差检查

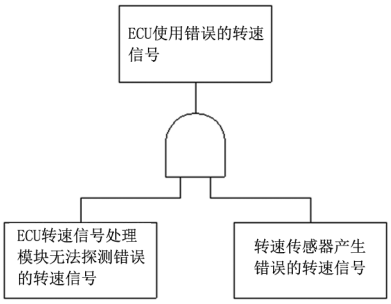

图6 APU 超速故障树的一段子树

表5 优先与门案例的计算结果

方法	传统故障树解析解	动态故障树解析解	动态故障树二阶近似解
顶事件发生概率	5.28×10^{-6}	2.64×10^{-6}	2.65×10^{-6}

3.2 冷备件门案例

图7是飞机级的一个典型事件“丧失交流供电功能”的一段子树，民机通常备有多套交流电源，一般情况下由主发动机驱动交流发电机为飞机提供交流电源，APU 与 RAT（冲压空气涡轮）作为冷备份待机。把图7顶事件下面的与门换成图3所示的冷备件门后就可以表达出冷备份这一动态特性。

底事件的失效率假设见表6，分别为 $\gamma_1=5.1\times10^{-3}/h$ 和 $\gamma_1=2.6\times10^{-4}/h$，飞行时间设为4h，分别对两种故障树进行计算，得出的结果如表7所示。

3.3 结果分析

从两个案例的结果来看，传统故障树不能表达系统动态特性，即使求出了解析解，其误差虽然偏保守，但是相当大。相比较之下，动态故障树的二阶近似解与解析解误差很小且偏保守，计算过程则相当简易、快捷，对于工程实践上的大批量计算来说，成本也是可以接受的。

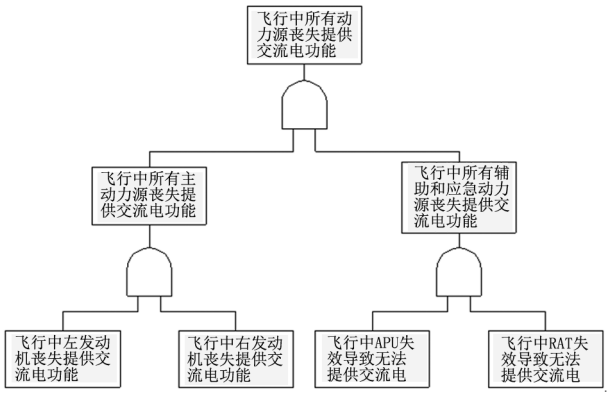

图 7　APU 丧失交流供电功能故障树的一段子树

表 6　底事件的失效率

	飞行中左发动机丧失提供交流电功能	飞行中右发动机丧失提供交流电功能	飞行中 APU 失效导致无法提供交流电	飞行中 RAT 失效导致无法提供交流电
失效率（/h）	2.2×10^{-3}	2.2×10^{-3}	7.5×10^{-2}	3.6×10^{-2}

表 7　冷备件门案例的计算结果

方法	传统故障树解析解	动态故障树解析解	动态故障树二阶近似解
顶事件发生概率	2.67×10^{-6}	1.65×10^{-6}	1.67×10^{-6}

4　结论

动态故障树作为传统故障树的拓展，具有两个优点：定性分析方面，由于可以表达出系统的动态特性，因此对系统的描述更为全面，有助于分析人员进一步理解系统架构。定量计算方面，通过施用马尔可夫模型求解，可以得到更准确的数值。但同时也有一个缺点，即马尔可夫模型的建立和计算都比较复杂。本文对双输入的动态逻辑门的计算式进行了理论推导，然后对解析解施用了二阶近似，得出的计算式在保证一定精度的前提下较大幅度地简化了计算，其运算成本几乎与传统故障树分析相同，所以保证了工程实践上大批量计算的可行性，有一定的应用前景和价值。

参考文献：

[1] 美国原子能委员会. 故障树手册[M]. 1987：6.
[2] SAE. ARP 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment[S]. 1996.
[3] 高顺川. 动态故障树分析方法及其实现[D]. 长沙：国防科学技术大学，2005.
[4] 赵运生，胡骏，吴铁鹰，陈娟娟. 大型民用飞机辅助动力装置性能仿真[J]. 航空动力学报，2011，26：1590.
[5] 朱正福，李长福，何恩山，杨春华. 基于马尔可夫链的动态故障树分析方法[J]. 兵工学报，2008，29：1104.
[6] 王波，刘东，李艺. 基于顺序失效符的动态故障树形式规约[J]. 北京航空航天大学学报，2012，38：1255.
[7] K. Dura Rao，V. Gopika，V. V. S. sanyasi Rao，H. S. Kushwaha，A. K. Verma，A. Srividya. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliability engineering and system safety[J]. 2009，Vol. 94：872.
[8] 孙杨慧. 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[J]. 民用飞机设计与研究，2013，增刊第 2 期：29.

（上接第 4 页）

为了将系统的民机试飞规划与管理研究成果应用于实际试飞工作，使用计算机辅助和人工干预相结合的方式是必然的途径。

在上述民机试飞规划和管理研究成果和方法的基础上，上海飞机设计研究院已开发出一套适用于民机试飞的 FTCS 软件平台，且已在 ARJ21-700 飞机型号项目取证试飞工作中得到了验证和应用。

5　结论

本文梳理了民机试飞需求类型，讨论了民机试飞任务分工和试飞计划制订原则，分析了民机试飞科目特点和逻辑关系，研究并提出了一种民机试飞任务单优化方法，阐述了一套国际先进水平的试飞规划与管理体系，实现了民机试飞的闭环控制，解决了国内试飞规划中未能系统研究的问题，并创建了一套具有国际先进水平的 FTCS。

本文所得出的研究成果和方法已在实际型号试飞工作中得到了应用和验证，起到了减少试飞架次、提高试飞效率、缩短型号试飞周期和降低成本投入的作用，具有实际的工程应用意义。

参考文献：

[1] Marle D. Hewett，David M. Tartt etc. The development of an automated flight test management system for flight test planning and monitoring [J]. ACM，1988，324-333.
[2] Victor W，Bender，Gerald Cahill etc. Automating the flight test planning process [C]. Digital Avionics Systems Conference，1994，14th DASC：83-88.
[3] 沈宏良，余勇军，刘旭，等. 试飞科目的最优排序问题研究[J]. 南京航空航天大学学报，2000，32(3)：312-317.
[4] 周自全. 飞行试验工程[M]. 北京：航空工业出版社，2010.