第 43 卷第 9 期　　机 械 工 程 学 报　　Vol.43 No.9
2007 年 9 月　　CHINESE JOURNAL OF MECHANICAL ENGINEERING　　Sep. 2007

故障树分析的等效失效概率计算方法*

裴　扬　宋笔锋
(西北工业大学航空学院　西安　710072)

摘要：在故障树分析中，系统的失效概率及部件重要度函数并不能全面考虑所有部件所有状态对系统可靠性的影响，为弥补这一不足，提出等效失效概率的概念及其计算方法。利用概率分解法来分析部件及系统所有的存在状态，采用马尔可夫链法及概率论知识计算系统的期望工作次数，进而获得等效失效概率。应用中表明，等效失效概率能够完全考虑所有部件关键状态及非关键状态对系统可靠性的影响。在于系统失效概率相同的情况下，可以利用等效失效概率来比较不同系统的可靠度。该方法是对目前部件重要度函数的扩展，具有一定的实用价值。

关键词：故障树　等效失效概率　重要度　马尔可夫链　期望
中图分类号：V221

0　前言

在故障树分析中，经常要计算部件重要度和系统失效概率，以便发现系统的薄弱环节，从而指导可靠性设计。目前已经发展了多种重要度函数，例如 Brinbaum 重要度、结构重要度、关键重要度、联合重要度等[1-4]，主要用于分析单独部件以及结构拓扑对系统可靠性的影响[3]。然而，重要度函数并不能全面考虑所有部件所有状态对系统可靠性的影响。系统的失效概率计算只能反映部件处于关键状态下对系统的贡献，而不能全面反映非关键状态对系统的贡献。为了反映所有部件关键状态及非关键状态对整个系统失效概率的影响，本文提出了等效失效概率概念及其计算方法。

假设系统以若干状态存在，将导致系统失效的状态定义为系统的“失效状态”，无任何部件失效的状态定义为“无部件失效状态”，其余状态为系统的“中间状态”。从上面定义可以看出，“中间状态”和“无部件失效状态”均是系统的非失效状态。通常，故障树只给出失效状态(部件关键状态)对应的概率，但实际情况是，中间状态(部件非关键状态)对系统的失效也有很大影响，原因就在于影响系统中间状态的部件可能处于某个或某几个最小割集中，本文所提出的“等效失效概率概念”的实质就是研究如何将中间状态对应的概率等效到系统的失效概率中去，等效的关键在于计算导致系统失效的期望工作次数。对于只有非余度部件组成的系统来说，系统的失效概率与等效失效概率在理论上应是相等的，对应的期望工作次数为 1；对于复杂的系统(例如故障树由若干与门、或门、表决门等组成)来说，其期望工作次数就需要详细的计算得出。

* 中国博士后基金(20060400301)和西北工业大学青年科技创新基金(W016218)资助项目。20060711 收到初稿，20070416 收到修改稿

1　等效失效概率计算的基本原理

设系统以 N 个状态存在，$\boldsymbol{S}$ 为状态矢量，令 $\boldsymbol{S}_1$ 表示系统的“失效状态”，$\boldsymbol{S}_N$ 为系统的“无部件失效状态”，$\boldsymbol{S}_2$～$\boldsymbol{S}_{N-1}$ 为系统的“中间状态”。设 P_w 为第 w 个状态的存在概率，则式(1)表示所有存在状态对应的存在概率之和应为 1。通常，系统失效概率 P_{F} 即为系统“失效状态”对应的概率，如式(2)所示

$$\sum_{w=1}^{N} P_w = 1 \tag{1}$$

$$P_{\mathrm{F}}=P_1 \qquad w=1 \tag{2}$$

根据飞机作战生存力分析中计算“等效单一易损面积”的思路[5-6]，提出以下“系统等效失效概率”的计算方法。设 E 为导致系统失效的期望工作次数，系统的等效失效概率 P_{EF} 计算公式为

$$P_{\mathrm{EF}} = \sum_{w=1}^{N-1} P_w / E \tag{3}$$

从式(3)可以看出，等效失效概率关键在于计算系统各个状态的存在概率以及期望工作次数。计算方法为：首先利用概率分解法确定系统的存在状态及对应的存在概率；其次，利用马尔可夫链方法计算若干工作次数后系统的累积存在概率；再次，利用累积存在概率，并根据数学期望理论推导导致系统失效的期望工作次数，进而根据式(3)计算等效失效概率。具体的流程如图1所示，下面介绍该流程的有关说明。

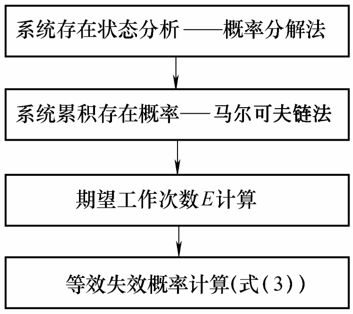

图 1 等效失效概率计算流程图

1.1 确定系统存在状态的概率分解法

假设系统中每个部件有两个存在状态(正常工作或失效)，则系统的存在状态便可以根据部件状态及其组合状态给出。

例如，设系统具有 N_0 个非余度部件(x_1, x_2, ···, x_{N_0})和 L 组余度部件(第 i 组余度部件组共有 n_i 个部件，记为 Y_i)。令 $y(i_p)$ 表示第 i 个余度部件组中的第 p 个部件，$P_{k/h_{yi}}$ 表示第 i 个余度组的失效概率，表达式为

$$P_{k/h_{yi}}=\prod_{p=1}^{n_i}P_{k/h_{y(i_p)}} \tag{4}$$

式中 $P_{k/h_{y(i_p)}}$ 表示第 i 个余度部件组中第 p 个部件的失效概率。令集合 Ω 为所有余度组部件组成的集合，记为 $\Omega=(U_1，U_2，\cdots，U_R)$，$R$ 为 Ω 的元素个数。表1列出了分析系统存在状态及对应存在概率的概率分解方法。

表 1 系统存在状态分析的概率分解法

存在状态	对应的存在概率	
非余度部件或余度部件组失效 ($x_1+x_2+\cdots+x_{N_0}+Y_1+Y_2+\cdots+Y_L$)	$\sum_{q=1}^{N_0}\left[P_{k/h_q}\prod_{i=1}^{q-1}(1-P_{k/h_i})\right]+\prod_{w=1}^{N_0}(1-P_{k/h_w})\cdot\sum_{r=1}^{L}\left[P_{k/h_{yr}}\prod_{s=1}^{r-1}(1-P_{k/h_{ys}})\right]$	
Ω 中只有第 i_1个部件失效	$\prod_{i=1}^{N_0}(1-P_{k/h_i})\cdot\prod_{q=1}^{1}P_{k/h_{y(i_q)}}\cdot\prod_{r=1,\ r\neq i_1}^{R}(1-P_{k/h_{yr}})$	$\forall\ 1\le i_1\le R$
Ω 中只有第 i_1，i_2个部件失效，且事件 $U_{i_1}U_{i_2}$ 不造成系统失效	$\prod_{i=1}^{N_0}(1-P_{k/h_i})\cdot\prod_{q=1}^{2}P_{k/h_{y(i_q)}}\cdot\prod_{r=1,\ r\neq i_1,i_2}^{R}(1-P_{k/h_{yr}})$	$\forall\ 1\le i_1<i_2\le R$
Ω 中只有第 i_1，i_2，i_3个部件失效，且事件 $U_{i_1}U_{i_2}U_{i_3}$ 不造成系统失效	$\prod_{i=1}^{N_0}(1-P_{k/h_i})\cdot\prod_{q=1}^{3}P_{k/h_{y(i_q)}}\cdot\prod_{r=1,\ r\neq i_1,i_2,i_3}^{R}(1-P_{k/h_{yr}})$	$\forall\ 1\le i_1<i_2<i_3\le R$
$\vdots$	$\vdots$	
Ω 中只有第 i_1，i_2，i_3，$\cdots$，$i_{(R-1)}$个部件失效，且事件 $U_{i_1}U_{i_2}\cdots U_{i_{(R-1)}}$ 不造成系统失效	$\prod_{i=1}^{N_0}(1-P_{k/h_i})\cdot\prod_{q=1}^{R-1}P_{k/h_{y(i_q)}}\cdot\prod_{r=1,\ r\neq i_1,i_2,\cdots,i_{(R-1)}}^{R}(1-P_{k/h_{yr}})$	$\forall\ 1\le i_1<i_2<\cdots<i_{R-1}\le R$
Ω 中只有第 i_1，i_2，i_3，$\cdots$，i_R 个部件失效，且事件 $U_{i_1}U_{i_2}.\cdots U_{i_{(R-1)}}U_{i_R}$ 不造成系统失效	$\prod_{i=1}^{N_0}(1-P_{k/h_i})\cdot\prod_{q=1}^{R}P_{k/h_{y(i_q)}}$ $\quad i_1=1,i_2=2,\cdots,i_R=R$	

概率分解法确定系统的存在状态不仅适用于只由余度和非余度部件组成的系统，该方法可以扩展到任意的故障树模型(含若干与门、或门、表决门等逻辑门)，其基本步骤为：首先将所有部件按照组合原理，列出所有的存在状态；然后确定存在状态的性质并对性质相同的状态进行合并；最后确定每个独立存在状态对应的概率数值。

1.2 累积失效概率计算

马尔可夫链(Markov chain)法，又称状态转换矩阵法，计算系统多次工作后累积失效概率的基本思路是将系统多次工作模型化为一个马尔可夫过程[7-8]。在马尔可夫过程中，系统被定义成它能以若干独立状态存在，并且系统由于第 $j+1$次工作引起的失效概率就是系统从第 j 次工作下的非失效状态转换为失效状态的概率。设矢量 $\boldsymbol{S}^{(j)}$表示系统第 j 次工作后各状态的累积存在概率矢量，则第 $j+1$次工作后各个状态的概率矢量为

$$\boldsymbol{S}^{(j+1)}=\boldsymbol{TS}^{(0)} \tag{5}$$

式中，矢量 $\boldsymbol{S}^{(0)}$表示系统未工作前各状态的存在概率矢量；$\boldsymbol{T}$ 为状态转换矩阵。系统第 j+1 次工作后的累积失效概率可根据累积存在状态概率矢量 $\boldsymbol{S}^{(j+1)}$ 的失效状态概率给出。

在系统工作之前，系统的“无部件失效状态”的存在概率为 1，而其他状态对应的存在概率为 0，此时

$$\boldsymbol{S}^{(0)}{}_w=\begin{cases}0 & w=1,\ 2,\cdots,N-1\\ 1 & w=N\end{cases} \tag{6}$$

因此，系统在工作前的累积失效概率为

$$\overline{P}_{\mathrm{F}}^{0}=\boldsymbol{S}^{(0)}{}_1=0 \tag{7}$$

从式(5)可以看出，马尔可夫链法的关键在于如何确定状态转换矩阵。由于 $\boldsymbol{T}$ 的元素 $\boldsymbol{T}_{iq}$ 反映了系统从第 q 个存在状态转换到第 i 个状态的概率，故

$$\boldsymbol{T}_{iq}=\sum_{w=1}^{N}P_w \qquad \boldsymbol{S}_q\cup\boldsymbol{S}_w=\boldsymbol{S}_i \tag{8}$$

这样，系统在第 j+1次工作后的累积失效概率为

$$\overline{P}_{\mathrm{F}}^{\,j+1}=\ \boldsymbol{S}_1^{(j+1)} \tag{9}$$

1.3　期望工作次数计算

令随机变量 Z_N 为

$$Z_N=\begin{cases}1 & N\text{ 次工作后系统未失效}\\ 0 & N\text{ 次工作后系统失效}\end{cases} \tag{10}$$

则随机变量

$$Z=\sum_{N=0}^{+\infty}Z_N=Z_0+Z_1+Z_2+\cdots \tag{11}$$

表示系统失效时的工作次数。设系统在经过 N 次工作后的累积失效概率为 $\overline{P}_{\mathrm{F}}^{N}$，由于

$$P(Y_N)=\begin{cases}1-\overline{P}_{\mathrm{F}}^{N} & Z_N=1\\ \overline{P}_{\mathrm{F}}^{N} & Z_N=0\end{cases} \tag{12}$$

根据数学期望的性质[9]，有

$$E=\mathrm{E}(Z)=\mathrm{E}(Z_0+Z_1+\cdots)=\mathrm{E}(Z_0)+\mathrm{E}(Z_1)+\cdots \tag{13}$$

从而

$$E=\sum_{N=0}^{+\infty}1\times(1-\overline{P}_{\mathrm{F}}^{N})+0\times\overline{P}_{\mathrm{F}}^{N}=\sum_{N=0}^{+\infty}(1-\overline{P}_{\mathrm{F}}^{N}) \tag{14}$$

由于 $\overline{P}_{\mathrm{F}}^{N}$ 满足 $\overline{P}_{\mathrm{F}}^{0}=0$、$\overline{P}_{\mathrm{F}}^{N+1}\geqslant\overline{P}_{\mathrm{F}}^{N}$、$\overline{P}_{\mathrm{F}}^{+\infty}=1$。即 $\overline{P}_{\mathrm{F}}^{N}$ 随着工作次数 N 的增大而逐渐增大，并逐渐趋于 1，因此计算过程中，可以利用式(15)计算 E

$$E=\sum_{N=0}^{N_{\mathrm{end}}}(1-\overline{P}_{\mathrm{F}}^{N}) \tag{15}$$

式中 N_{end} 可以由式(16)确定

$$1-\overline{P}_{\mathrm{F}}^{N_{\mathrm{end}}}<\varepsilon \tag{16}$$

式中　ε——无穷小量

2　等效失效概率计算算例

假设有三个系统的故障树(T_1、T_2、T_3)如图 2 所示，每棵树都含有 5 个底事件，底事件的发生概率如表 2 所示。下面以 T_3 为例来说明等效失效概率的计算过程。

表 2　底事件发生概率

故障树编号	1	2	3	4	5
T_1	0.000 906	0.000 906	0.000 903	0.000 902	0.000 902
T_2	0.006 500	0.006 500	0.006 500	0.035 800	0.035 800
T_3	0.080 000	0.080 000	0.080 000	0.050 000	0.050 000

2.1　确定存在状态及概率值

故障树 T_3 共有 5 个部件，共有 2^5=32 个存在状态，根据表 1 并经过状态合并，可知该系统共有 13 个独立存在状态，如表 3 所示。

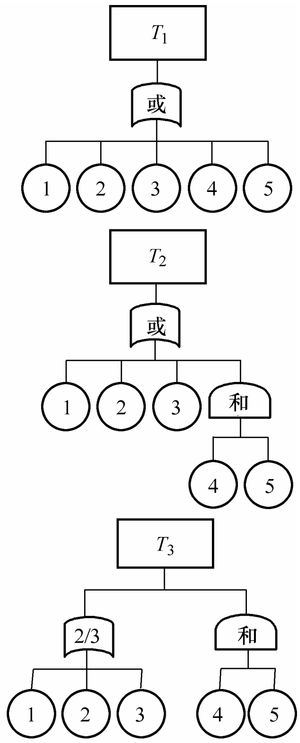

图 2　算例故障树

表 3　系统存在状态分析

状态编号	存在状态	对应的存在概率
1	系统失效状态	0.020 630 56
2	只有部件 1 失效	0.061 110 08
3	只有部件 2 失效	0.061 110 08
4	只有部件 3 失效	0.061 110 08
5	只有部件 4 失效	0.036 987 68
6	只有部件 1 和 4 失效	0.003 216 32
7	只有部件 2 和 4 失效	0.003 216 32
8	只有部件 3 和 4 失效	0.003 216 32
9	只有部件 5 失效	0.036 987 68
10	只有部件 1 和 5 失效	0.003 216 32
11	只有部件 2 和 5 失效	0.003 216 32
12	只有部件 3 和 5 失效	0.003 216 32
13	无任何部件失效	0.702 765 92

2.2　马尔可夫链计算累积失效概率

根据表 3，并结合式(8)，可以建立 13×13 的马尔可夫链状态转换矩阵。根据式(5)、(6)、(9)可以计算系统工作 N 次后的累积失效概率 $\overline{P}_{\mathrm{F}}^{N}$，根据公式(16)确定 N_{end}，本例取 $\varepsilon=10^{-5}$。

2.3　计算期望工作次数及等效失效概率

表 4 列出了利用所提出的方法计算的原始失效概率、等效失效概率及各个系统的期望工作次数。

表 4　算例计算结果

故障树编号	P_{F}	E	P_{EF}	可靠度排序
T_1	0.020 63	1.000 00	0.020 63	1
T_2	0.020 63	2.242 63	0.039 39	2
T_3	0.020 63	2.757 79	0.107 78	3

从表 4 可以看出以下几点。

(1) 三个系统的原始失效概率均为 0.020 63，这个结论并不能比较三个系统可靠性的高低。

(2) 每个系统的等效失效概率完全不同，利用等效失效概率可以确定系统 3 的可靠性最低，其次为系统 2，系统 1 可靠性最高。

(3) 系统 1 完全由或门组成，组成的部件均为非余度部件，因此该系统的期望工作次数理论上应为 1。系统 2、3 除了非余度部件外，还存在余度部件，因此系统的独立存在状态中会包含余度部件的非关键状态及其组合状态，期望工作次数理论上应该比 1 大一些。表 4 中期望工作次数 E 的计算结果与理论分析一致。

3 结论

(1) 等效失效概率不仅可以考虑所有部件关键状态对系统可靠性的影响，而且可以考虑部件非关键状态对系统可靠性的影响，是目前部件重要度函数的扩展，具有明确的物理意义。

(2) 可以利用等效失效概率来比较不同系统的可靠性。

(3) 等效失效概率可以全面考虑部件的存在状态，对于系统可靠性的改进具有参考价值。

参 考 文 献

[1] KUO W, ZUO M J. Optimal reliability modeling principles and applications[M]. Hoboken：John Wiley & Sons, Inc., 2003.

[2] HWANG F K. A new index of component importance [J]. Operations Research Letters, 2001, 28(2)：75-79.

[3] WU Shaomin. Joint importance of multistate systems [J]. Computers & Industrial Engineering, 2005, 49(1)：63-65.

[4] RAMIREZ-MARQUEZ J E, ROCCO C M, GEBRE B A, et al. New insights on multi-state component criticality and importance [J]. Reliability Engineering and System Safety, 2006, 91(8)：894-904.

[5] Survivability aircraft nonnuclear general criteria[S]. Dept. of Defense, MIL-HDBK-336-1, Washington DC, 1982.

[6] PEI Y, SONG B F, QIN Y. Aircraft equivalent vulnerable area calculation methods [C]// ICAS 2004 Proceedings on Disc [CD], ICAS 2004-5.6 (St.).R.2, Optimage Ltd, Edinburgh, UK, 2004.

[7] BALL R E. The fundamentals of aircraft combat survivability analysis and design [M]. 2nd edition. Reston：American Institute of Aeronautics and Astronautics, Inc., 2003.

[8] BALL R E. 飞机作战生存力分析与设计基础[M]. 林光宇，宋笔锋，译. 北京：航空工业出版社，1998.

[9] MILLER I, MILLER M, JOHN E. Freund’s mathematical statistics with application [M]. 7th edition. Beijing：Tsinghua University Press，2005.

EQUIVALENT FAILURE PROBABILITY CALCULATION METHOD FOR FAULT TREE ANALYSIS

PEI Yang SONG Bifeng
(*College of Aeronautics*, *Northwestern Polytechnical University*, *Xi’an 710072*)

Abstract：In fault tree analysis, the system failure probability and the component importance measures cannot totally include the contribution of all the component existing states to system reliability. Hence, an equivalent failure probability concept and calculation method is proposed. First, the system existing states are analyzed by probability decomposition method. Markov chain method and the expectation theory are used to calculate the expected number of working circle. And the equivalent failure probability is finally attained. Analysis shows that, equivalent failure probability not only includes the contribution of the critical states of component to system reliability, but also considers the non critical states of component, the equivalent failure probability may compare the relative reliability when different systems have the same failure probability, and the concept of equivalent failure probability is an important extension of current component importance measures and is useful for reliability design.

Key words：Fault tree Equivalent failure probability Importance measure Markov chain Expectation

作者简介：裴扬，男，1978 年出生，博士后。主要研究方向为飞行器可靠性、维修性和生存性。

E-mail：peiyang_yang@163.com