

基于等效失效率的动态故障树分析

李振, 孙新利

(第二炮兵工程学院, 陕西 西安 710025)

摘 要: 运用动态故障树对动态系统进行可靠性定量分析, 当动态子树规模较大时, 直接运用马尔可夫理论的难度较大。在综合运用模块化、等效失效率方法的基础上, 提出了一种动态故障树顶事件发生概率的近似算法: 首先通过深度优先最左遍历来搜索独立模块; 接着, 对时间域进行不等距划分, 将动态门下的子模块看作“准底事件”, 利用其在各区间内的等效失效率来逐步求取整个动态故障树顶事件的发生概率。通过对实例的求解, 验证了此方法的有效性。

关键词: 动态故障树; 深度优先最左遍历; 等效失效率; 马尔可夫理论

中图分类号: TB114.3 **文献标识码:** A **文章编号:** 1672-5468 (2007) 04-0026-04

Dynamic Fault Tree Analysis Based on Equivalent Failure Rate

LI-Zhen, SUN Xin-li

(The Second Artillery Engineering Institute, Xi'an 710025, China)

Abstract: In case of applying the dynamic fault tree to the quantitative analysis of dynamic system, it is difficult to use Markov theory directly when the dynamic sub-tree is very complex. Based on modularization and equivalent failure rate, an approximate algorithm for top-event occurrence rate of dynamic fault tree was introduced. At first, independent modules are recognized through the depth first left most ergodic algorithm. Then, the time domain is divided into non-equidistant intervals. A submodule included in the dynamic gate is considered as an approximate base event and its equivalent failure rate in each interval is used to obtain the top-event occurrence rate of the whole dynamic fault tree step by step. The effectiveness of the algorithm is demonstrated with an practical example.

Key words: dynamic fault tree; depth first left most ergodic algorithm; equivalent failure rate; Markov theory

1 引言

为了将故障树技术用于容错计算机和控制系统的可靠性分析, Dugan 等人提出了动态故障树的概念 (DFT)^[1]。DFT 是一种在一般故障树的基础上,

通过引进动态逻辑门来表述系统动态性的分析方法。由于它对动态子树和静态子树采取了不同的处理方法, 由此既克服了直接应用马尔可夫理论导致状态过多的困难, 又解决了传统静态故障树无法对动态系统建模的问题。

收稿日期: 2007-06-15

作者简介: 李振 (1983-), 男, 山东枣庄人, 第二炮工程学院硕士研究生, 研究方向为导弹战斗部毁伤效应与可靠性研究。

顶事件发生概率作为动态故障树定量分析的重要指标, 其求解一直是研究的热点之一。1997年, Gulati 利用马尔可夫状态转移图来求解动态子树, 用 BDD 算法来求解静态子树, 最后将两者进行综合^[2]; 2003年, Amari 直接分析故障树模块, 得到顶事件发生概率的近似值^[3]; 2006年, 高顺川等人在此基础上研究了几种常用动态门的相应算法^[4]。

传统方法通过区分动态模块和静态模块, 在一定程度上减小了计算规模, 但当动态模块过于庞大时, 仍会面临所转化的马尔可夫状态转移图中状态过多的困难。将动态模块中的子模块进一步分割出来, 视为“准底事件”进行处理, 可以大大减少马尔可夫状态转移图中的状态, 使分析过程不易出错。动态门的输出状态不仅和“输入事件”的状态有关, 还和发生时刻有关, 一般需用马尔可夫理论进行分析, 因此, 需要求取子模块的等效失效率。

2 用深度优先最左遍历来寻找动态故障树的独立模块

动态故障树分块的算法基于以下规则^[5]: 对动态故障树进行两次深度优先最左 (DFLM-Depth First Left Most) 遍历。第一次对搜索到的动态故障树中的底事件和中间事件设置3个标记, 标记1表示第一次搜索到该事件所用的步数; 标记2表示第二次搜索到该事件所用的步数; 标记3表示最后一次搜索到该事件所用的步数。然后再对动态故障树进行第二次搜索, 对每一个中间事件, 计算与其相连接的所有下层事件中, 标记1的最小值和标记3的最大值, 分别用 min 和 max 表示。当满足下述条件时, 节点 N 是独立模块:

- 1) 与其相连接的所有下层事件中, 标记1的 min 比节点 N 的标记1的值大;
- 2) 与其相连接的所有下层事件中, 标记3的 max 比节点 N 的标记2的值小。

3 动态故障树顶事件的发生概率

求 T 时刻顶事件的发生概率, 对于搜索到的独立模块, 如果位于静态门下, 只需求取该子模块中 T 时刻“顶事件”的发生概率, 将它作为上层静态门的输入; 若位于动态门下, 即动态模块中的子模块, 因动态门的输出状态不仅与输入事件的状态有关, 还与发生时刻有关, 需要求出子模块的等效失效率, 将其视为“准底事件”, 与其它输入事

件一起构成动态模块的状态转移图。但子模块中“顶事件”的发生概率一般不再服从指数分布, 不能直接应用马尔可夫理论, 可将时间域进行分割, 在很小的区间内, 认为仍服从指数分布。一般情况下, 子模块中“顶事件”的等效失效率在刚开始时变化比较大, 随着时间的推移, 会逐渐趋近于某个常数。在计算量相同的条件下, 为提高计算精度, 这里对时间域进行非等距划分; 随着时间的推移, 间距逐渐增大。具体的计算步骤如下:

a) 将时间域 $[0, T]$ 分为 N 个区间, 分别编号为 $1, 2, L, n, L, N$, 区间长度分别为 $M^1dt, M^2dt, L, M^ndt, L, M^Ndt$, (其中 M 为大于1的数), 则

$$dt = \frac{T(1-M)}{M(1-M^N)} \quad (1)$$

b) 判断子模块是位于静态门下还是动态门下。若位于动态门下, 转向步骤 c); 若位于静态门下, 求取该子模块中 T 时刻“顶事件”的发生概率, 将它作为上层静态门的输入。

c) 判断动态门 G 下的子模块 S 是动态子模块还是静态子模块。若为动态子模块, 转向步骤 d); 若为静态子模块, 该子模块中“顶事件”在第 n ($n=1, 2, L, N$) 个区间内的等效失效率 $\lambda_s(n)$ 为:

$$\lambda_s(n) = \frac{1}{1-h_s(n)} \left. \frac{d(h_s(t))}{dt} \right|_{t=T_n} \quad (2)$$

式 (2) 中: $h_s(n)$ 和 $\left. \frac{d(h_s(t))}{dt} \right|_{t=T_n}$ 分别为该静

态子模块中“顶事件”在 T_n (T_n 为第 n 个区间右端点的时刻, $n=1, 2, L, N$) 时刻的发生概率及其一阶导数值, 可用 BDD 理论求取。

d) 设动态门 G 下的动态子模块 S 对应的马尔可夫链共有 m 个状态, 对应的转移矩阵为 $A_s(t)$, 在各区间内分别取作 $A_s(1), A_s(2), L, A_s(n), L, A_s(N)$ (如 S 下的输入事件均为底事件, 则 $A_s(1) = A_s(2) = L = A_s(n) = L = A_s(N)$), 对于第 n 个区间, 状态的概率分布行向量为 $P_s(n) = [p_1(n), p_2(n), L, p_i(n), L, p_m(n)]$, 则

$$P_s(n) = P_s(n-1) \exp^{(M^n dt) A_s(n)} \quad (3)$$

式 (3) 中: T_{n-1}, T_n 分别为第 $(n-1)$ 个, 第

n 个区间右端点的时刻;

$\exp[(M^ndt) A_s(n)]$ ——矩阵函数^[6]。

设列向量 $Q_s = [q_1, q_2, L, q_i, L, q_m]'$, 若 p_i 表示的状态代表顶事件发生, 则对应的 Q_s 的第 i 个元素 $q_i=1$; 否则, $q_i=0$ 。S 在 T_n 时刻“顶事件”的发生概率 $h_s(n)$ 和第 n 个区间内的等效失效率 $\lambda_s(n)$ 分别为:

$$h_s(n) = P_s(n) Q_s \quad (4)$$

$$\lambda_s(n) = \frac{P_s(n) A_s(n) Q_s}{1 - h_s(n)} \quad (5)$$

e) 求出所有动态门 G 下子模块的等效失效率, 进而构成动态门 G 对应的动态模块的转移矩阵 $A_G(t)$ 在各区间内的取值 $A_G(1), A_G(2), L, A_G(n), L, A_G(N)$ 。

f) 转向步骤 b), 逐步求取整个故障树顶事件的发生概率。

计算的流程如图 1 所示。

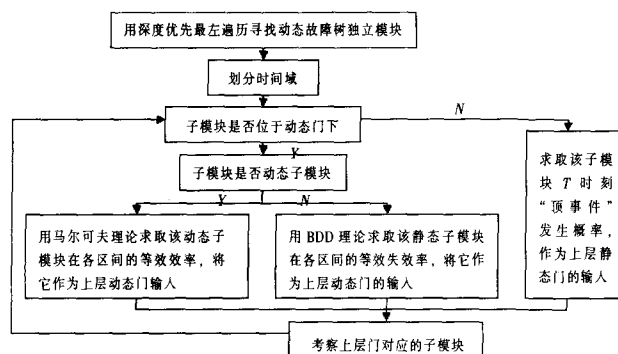


图 1 计算流程图

4 实例分析

以一个带开关的冷储备系统为例进行分析。系统 T 由一个主件 A 和两个冷备件 B 、 C 组成。当发生故障时, B 工作, 当 B 又故障时, C 工作。部件之间的切换通过开关 S 实现。若 S 失效, 则不能实现部件的切换, 因此, S 的可靠性对系统的可靠性影响较大。为了提高其可靠性, 转换开关 S 也是一个冷储备系统, 由一个主件 a 和两个冷备件 b 、 c 组成, 部件之间的转换不需要开关。假设各部件失效率如表 1 所示。

系统对应的动态故障树如图 2 所示, T 、 S 、 a 、 b 、 c 、 A 、 B 、 C 分别代表事件 T 故障、 S 故障、 a 故障、 b 故障、 c 故障、 A 故障、 B 故障、 C 故障。

表 1 各部件的失效率

部件	失效率/($\times 10^{-4} \cdot h^{-1}$)
a	1
b	2
c	3
A	0.4
B	0.8
C	0.9

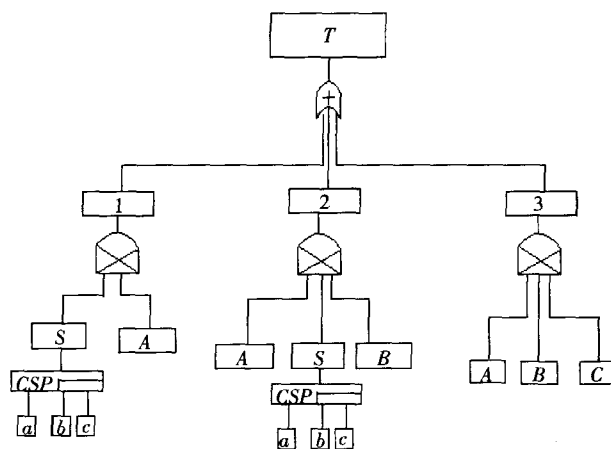


图 2 带开关的冷储备系统对应的动态故障树

模块 S 为动态独立模块, 且位于优先与门下面, 可将其视为“准底事件”。将时间域 $[0, 500\ 000]$ 分为 5 个区间, 取 $M=1$, 算得的系统不可靠度如图 3 所示的曲线 1, 取 $M=2$ 算得的结果如曲线 2 所示; 将时间域分为 50 个区间, 取 $M=1$ 算得的结果如曲线 3 所示。直接将马尔可夫理论应用于整个动态故障树, 算得的结果如曲线 4 所示。

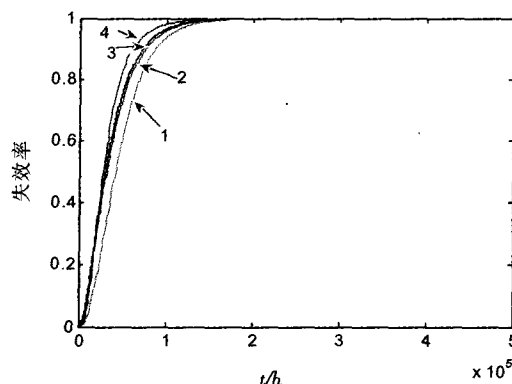


图 3 系统不可靠度和时间的关系

从图中可以看出, 曲线 3 比曲线 1 更靠近真实曲线 4, 说明区间划分的越多, 精度越高。另外,

曲线2和曲线3是比较接近的,说明在划分区间数一定的前提下,适当地控制 M 的取值,可以提高计算的精度。

5 结束语

通过深度优先最左遍历来寻找动态故障树的独立模块,将位于动态门下的独立模块视为“准底事件”,可以解决直接将马尔可夫理论应用于整个系统而带来的“组合爆炸”问题。将时间域进行不等距划分,在每一个小区间内,将“准底事件”的等效失效率视为常数,用马尔可夫理论进行分析,与等距划分时间域的方法相比,在同样的计算量下,能获得更高的精度。

参考文献:

[1] JOANNE BECHTA DUGAN, SALVATORE BAVUSO, MARK

BOUD. Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems [J]. IEEE Transactions on Reliability, 1992, 41 (3): 363-377.

[2] ROHIT GULATI, JOANNE BECHTA DUGAN. A Modular Approach for Analyzing Static and Dynamic Fault Trees [C] // Proceedings Annual Reliability and Maintainability Symposium, 1997: 57-63.

[3] SUPRASAD AMARI. A New Approach to Solve Dynamic Fault Trees [C] // Proceedings Annual Reliability and Maintainability Symposium, 2003: 374-379.

[4] 高顺川, 周忠宝, 郑龙, 等. 一种动态故障树顶事件发生概率的近似算法 [J]. 微计算机信息, 2006, 22 (6-1): 209-211.

[5] 闫剑平. 一种故障树模块的划分方法 [J]. 北方交通大学学报, 2000, 5: 63-66.

[6] 程云鹏. 矩阵论 [M]. 西安: 西北工业大学出版社, 1989: 171-174.

信息与动态



软通动力公司荣获“杰出软件外包服务贡献奖”

北京软通动力信息技术有限公司是中国领先的IT外包服务提供商,为欧美、日韩及中国的客户提供端到端的全面IT外包服务,并具有强大的海内外业务拓展和服务实施能力。目前已整体通过CMMI 5、ISO 9001及ISO 2700 (BS 7799)等标准的信息安全认证。该公司在不断强化ITO领域业务能力的同时,还将业务进一步扩展至业务流程外包(BPO)领域。

软通动力公司最近荣获“2007年第三届中国软件和信息服外包贡献奖”之“杰出软件外包服务贡献奖”。这是该公司自2005年以来第3次获得这个奖项。

“中国软件和信息服外包贡献奖”由中华人

民共和国商务部主办,是目前国内唯一对外包领域企业的业界贡献进行确立和评定的奖项,旨在对企业在服务外包领域所作的贡献予以总结和表彰。“中国软件和信息服外包贡献奖”创建于2005年,由“杰出外包战略解决方案贡献奖”、“杰出IT外包服务贡献奖”、“杰出软件外包服务贡献奖”、“杰出商业流程外包服务贡献奖”、“最佳外包合作关系贡献奖”5大类组成。评审时,评选专家委员会除了要考察企业的规模和盈利能力之外,还要根据科学严谨的评审标准,从外包、服务、合作、成效4个方面进行综合审议和评价后,才能最终确定获奖企业。

(本刊讯)