

基于离散时间贝叶斯网络的动态故障树分析方法

周忠宝, 周经伦, 孙权, 金光, 董豆豆
(国防科技大学信息系统与管理学院, 410073, 长沙)

摘要: 提出了一种基于离散时间贝叶斯网络的动态故障树分析方法. 首先给出优先与门、顺序相关门、备件门、功能相关门等动态逻辑门向离散时间贝叶斯网络的转化方法, 在得到动态故障树对应的离散时间贝叶斯网络之后, 再利用贝叶斯网络推理算法计算、诊断和预计顶事件概率、重要度等常规分析结果. 对数字飞控计算机系统进行的分析表明, 该方法能够保证较高的求解精度, 其相对误差均保持在 0.4% 以内, 而且易于扩展到多态和非确定性逻辑关系的情形.

关键词: 动态故障树; 离散时间贝叶斯网络; 数字飞控计算机系统; 可靠性分析

中图分类号: TB114.3 **文献标识码:** A **文章编号:** 0253-987X(2007)06-0732-05

Dynamic Fault Tree Analysis Method Based on Discrete-Time Bayesian Networks

Zhou Zhongbao, Zhou Jinglun, Sun Quan, Jin Guang, Dong Doudou

(School of Information System and Management, National University of Defense Technology, Changsha 410073, China)

Abstract: A new dynamic fault tree analysis method based on discrete-time Bayesian networks is proposed. The conversion of the dynamic logic gates, such as priority and gate, sequence enforcing gate, spare gate and functional dependency gate to discrete-time Bayesian networks is studied. The top-event probability, importance measures and other diagnosis and prediction results can be obtained subsequently using the classical algorithms based on Bayesian networks. The comparison with Markov chain method is carried out by means of the digital aviation control computer system, and the results show that the proposed method can guarantee high accuracy, and the relative errors are no more than 0.4%. In addition, the proposed method can be easily extended to multi-state systems with non-determinate logic relations.

Keywords: dynamic fault tree; discrete-time Bayesian network; digital aviation control computer system; reliability analysis

传统的故障树分析方法是一种基于静态逻辑和静态故障机理的分析方法, 对于解决动态随机性故障的容错系统、顺序相关性冗余系统、公用资源库系统等问题却无能为力. 为此, 维吉尼亚大学 Dugan 教授领导的研究小组通过对空间站以及空中交通控制等复杂系统的深入研究, 结合 Markov 理论和组合数学方法建立了动态故障树模型^[1]. 传统的动态故障树求解均是基于 Markov 模型的, 但 Markov 模型的组合爆炸缺陷, 使得其难以应用于大型动态故障树的分析. Amari 等人给出了一种基于梯形公

式的顶事件概率近似计算方法^[2], 但该方法仍然存在组合爆炸问题, 而且精度较低.

近年发展起来的贝叶斯网络技术, 承继了故障树的状态描述及推理方式, 而且还具备描述事件多态性和故障逻辑关系非确定性的能力, 既能用于推理, 也可用于诊断, 非常适合于可靠性、安全性分析^[3-4]. 例如, 静态故障树向贝叶斯网络的转化方法^[3], 基于贝叶斯网络的最小路(割)集及重要度求解算法^[5], 优先与门、温备件门、概率依赖门向动态贝叶斯网络的转化方法^[6], 以及将冷备件门转化为

离散时间贝叶斯网络(DTBN)的方法^[7]等.

本文基于上述方法,进一步研究了基于 DTBN 的动态故障树分析方法.

1 离散时间贝叶斯网络

一个具有 N 个节点的 DTBN 可用 $N = \langle \langle V, T_n, E \rangle, P \rangle$ 来表示,其中包括以下 2 个部分.

(1) 一个具有 N 个节点的有向无环图 G , 用 $\langle V, T_n, E \rangle$ 表示. 其中: 节点集合 $V = \{V_1, \dots, V_N\}$ 中的元素代表变量, 它可以是部件、系统状态等问题的抽象; $T_n = \{[t_0, t_1), \dots, [t_{i-1}, t_i), \dots, [t_{n-1}, t_n), [t_n, \infty)\}$ 是对时间轴的一个划分, 其元素表示变量发生时刻所在的区间(如部件、子系统、系统在各个区间内失效等), 所有节点的状态空间均为 T_n ; E 是节点间的有向边, 代表了变量间的关联关系.

$\langle V, T_n, E \rangle$ 蕴含了条件独立性假设, 即在给定 V_i 的父节点 $pa(V_i)$ 的条件下, V_i 与非后代节点 $A(V_i)$ 独立, 即

$$P(V_i | pa(V_i), A(V_i)) = P(V_i | pa(V_i))$$

(2) 一个与每个节点相关的条件概率分布用 P 表示. 由贝叶斯网络的条件独立性假设可知, 条件概率分布可以用 $P(V_i | pa(V_i))$ 来描述, 它表达了节点与其父节点的定量关联关系.

2 动态逻辑门向 DTBN 的转化

2.1 优先与门

优先与门及对应的 DTBN 如图 1 所示. 对于根节点 X , 其概率分布

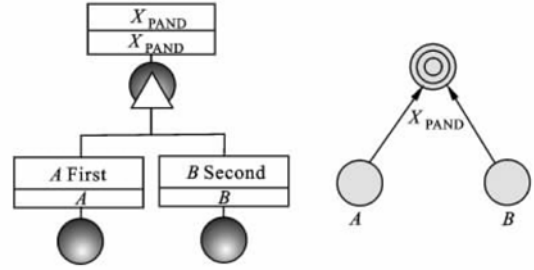
$$P(X = [(x-1)\Delta, x\Delta]) = e^{-\lambda_X x \Delta} (e^{\lambda_X \Delta} - 1) \quad (0 < x \leq n) \quad (1)$$

$$P(X = [T, \infty)) = \int_T^\infty \lambda_X e^{-\lambda_X t} dt = e^{-\lambda_X T} \quad (2)$$

式中: $X = [(x-1)\Delta, x\Delta]$ 表示 X 在 $[(x-1)\Delta, x\Delta]$ 区间内失效; $X = [T, \infty)$ 表示 X 在任务时间 T 内未发生失效; λ_X 为 X 的失效率(在动态故障树分析中, 一般均假设底事件服从指数分布^[1,6-7], 即失效率为常数, 本文仍然沿用这一假设).

需要特别指出的是: 如果节点 A 、节点 B 同时出现, 本文认为优先与门的输出事件发生. 节点 X_{PAND} 的条件概率分布为

$$P_{x,y,z} = P(X_{PAND} = [(z-1)\Delta, z\Delta] | A = [(x-1)\Delta, x\Delta], B = [(y-1)\Delta, y\Delta]) = \begin{cases} 1 & (0 < x \leq y = z \leq n) \\ 0 & (0 < y \leq x \leq n) \end{cases} \quad (3)$$



(a) 优先与门 (b) 优先与门对应的 DTBN

图 1 优先与门及对应 DTBN

$$P_{x,\infty,\infty} = P(X_{PAND} = [T, \infty) | A = [(x-1)\Delta, x\Delta], B = [T, \infty)) = 1 \quad (4)$$

$$P_{\infty,y,\infty} = P(X_{PAND} = [T, \infty) | A = [T, \infty), B = [(y-1)\Delta, y\Delta]) = 1 \quad (5)$$

$$P_{\infty,\infty,\infty} = P(X_{PAND} = [T, \infty) | A = [T, \infty), B = [T, \infty)) = 1 \quad (6)$$

2.2 顺序相关门

顺序相关门及对应的 DTBN 如图 2 所示. 节点 B 的条件概率分布为

$$P_{x,y} = P(B = [(y-1)\Delta, y\Delta] | A = [(x-1)\Delta, x\Delta]) = \begin{cases} 0 & (0 < y < x \leq n) \\ 1 - \frac{\lambda_a (e^{\lambda_a - \lambda_b} \Delta - 1)}{(\lambda_a - \lambda_b) (e^{\lambda_a \Delta} - 1)} & (0 < y = x \leq n) \\ \frac{\lambda_a e^{-(\lambda_a - \lambda_b)(y-x)\Delta} (e^{\lambda_a - \lambda_b} \Delta - 1) (e^{\lambda_a \Delta} - 1)}{(\lambda_a - \lambda_b) (e^{\lambda_a \Delta} - 1)} & (0 < x < y \leq n) \end{cases} \quad (7)$$

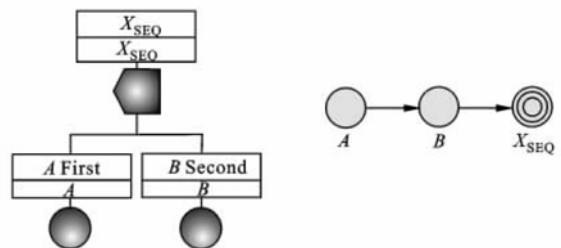
$$P_{x,\infty} = P(B = [T, \infty) | A = [(x-1)\Delta, x\Delta]) = 1 - \sum_{0 < y \leq n} P_{x,y} \quad (8)$$

$$P_{\infty,\infty} = P(B = [T, \infty) | A = [T, \infty)) = 1 \quad (9)$$

节点 X_{SEQ} 的条件概率分布为

$$P_{y,y} = P(X_{SEQ} = [(y-1)\Delta, y\Delta] | B = [(y-1)\Delta, y\Delta]) = 1 \quad (10)$$

$$P_{\infty,\infty} = P(X_{SEQ} = [T, \infty) | B = [T, \infty)) = 1 \quad (11)$$

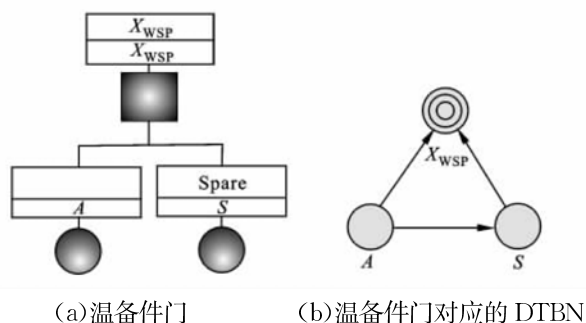


(a) 顺序相关门 (b) 顺序相关门对应的 DTBN

图 2 顺序相关门及对应的 DTBN

2.3 温备件门

温备件门及对应的 DTBN 如图 3 所示. 假设主部件 A 和备份部件 S 的失效率均为 λ , 则节点 S 的



(a) 温备件门 (b) 温备件门对应的 DTBN
图 3 温备件门及对应的 DTBN

条件概率分布为

$$P_{x,y} = P(S = [(y-1)\Delta, y\Delta] | A = [(x-1)\Delta, x\Delta]) = \begin{cases} e^{-\beta\lambda y\Delta} (e^{\beta\lambda\Delta} - 1) & (0 < y < x \leq n) \\ \frac{e^{-\beta\lambda y\Delta}}{e^{\lambda\Delta} - 1} \left(e^{(1+\beta)\lambda\Delta} - \frac{1+\beta}{\beta} e^{\beta\lambda\Delta} + \frac{1}{\beta} \right) & (0 < x = y \leq n) \\ \frac{e^{\beta\lambda\Delta} - 1}{\beta} e^{\lambda(x-y)\Delta} & (0 < x < y \leq n) \end{cases} \quad (12)$$

$$P_{x,\infty} = P(S = [T, \infty) | A = [(x-1)\Delta, x\Delta]) = 1 - \sum_{0 < y \leq n} P_{x,y} \quad (13)$$

$$P_{\infty,y} = P(S = [(y-1)\Delta, y\Delta] | A = [T, \infty)) = e^{-\beta\lambda y\Delta} (e^{\beta\lambda\Delta} - 1) \quad (14)$$

$$P_{\infty,\infty} = P(S = [T, \infty) | A = [T, \infty)) = 1 - \sum_{0 < y \leq n} P_{\infty,y} \quad (15)$$

节点 X_{WSP} 的条件概率分布为

$$P_{x,y,z} = P(X_{WSP} = [(z-1)\Delta, z\Delta] | A = [(x-1)\Delta, x\Delta], S = [(y-1)\Delta, y\Delta]) = \begin{cases} 1 & (z = \max(x, y)) \\ 0 & (z \neq \max(x, y)) \end{cases} \quad (16)$$

$$P_{\infty,y,\infty} = P(X_{WSP} = [T, \infty) | A = [T, \infty), S = [(y-1)\Delta, y\Delta]) = 1 \quad (17)$$

$$P_{x,\infty,\infty} = P(X_{WSP} = [T, \infty) | A = [(x-1)\Delta, x\Delta], S = [T, \infty)) = 1 \quad (18)$$

$$P_{\infty,\infty,\infty} = P(X_{WSP} = [T, \infty) | A = [T, \infty), S = [T, \infty)) = 1 \quad (19)$$

文献[7]中的冷备件的情形可作为特例, 即 $\beta \rightarrow 0$ 时的极限值.

2.4 功能相关门

功能相关门及对应的 DTBN 如图 4 所示. 节点

A 的条件概率分布为

$$P_{x,y} = P(A = [(y-1)\Delta, y\Delta] | Tr = [(x-1)\Delta, x\Delta]) = \begin{cases} e^{-\lambda_A y\Delta} (e^{\lambda_A\Delta} - 1) & (0 < y < x \leq n) \\ 1 - \sum_{y < x} P_{x,y} & (0 < y = x \leq n) \\ 0 & (0 < x < y \leq n) \end{cases} \quad (20)$$

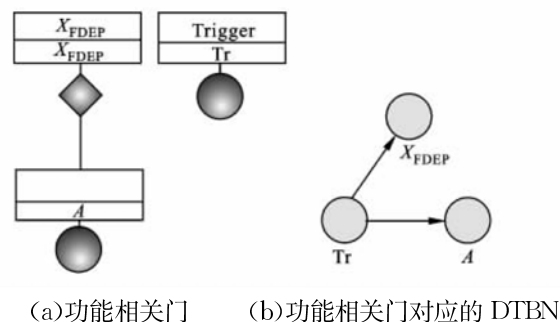
$$P_{\infty,y} = P(A = [(y-1)\Delta, y\Delta] | Tr = [T, \infty)) = e^{-\lambda_A y\Delta} (e^{\lambda_A\Delta} - 1) \quad (21)$$

$$P_{\infty,\infty} = P(A = [T, \infty) | Tr = [T, \infty)) = 1 - \sum_{0 < y \leq n} P_{\infty,y} \quad (22)$$

节点 FDEP 的条件概率分布为

$$P_{x,x} = P(X_{FDEP} = [(x-1)\Delta, x\Delta] | Tr = [(x-1)\Delta, x\Delta]) = 1 \quad (23)$$

$$P_{\infty,\infty} = P(X_{FDEP} = [T, \infty) | Tr = [T, \infty)) = 1 \quad (24)$$



(a) 功能相关门 (b) 功能相关门对应的 DTBN
图 4 功能相关门及对应的 DTBN

3 基于 DTBN 的动态故障树分析

3.1 顶事件概率

若顶事件 E_T 在任务时间 T 内发生, 则 E_T 的发生时刻必定在 $[0, \Delta), [\Delta, 2\Delta), \dots, [(n-1)\Delta, n\Delta)$ 中的一个区间之内, 因而 E_T 在任务时间 T 内的发生概率

$$P(T) = \sum_{0 < x \leq n} P(E_T = [(x-1)\Delta, x\Delta]) \quad (25)$$

而 $P(E_T = [(x-1)\Delta, x\Delta])$ 可以通过联合概率分布直接计算, 即

$$P(E_T = [(x-1)\Delta, x\Delta]) = \sum_{E_1, \dots, E_{M-1}} P(E_1 = e_1, \dots, E_{M-1} = e_{M-1}, E_T = [(x-1)\Delta, x\Delta]) \quad (26)$$

式中: 事件 $E_i (1 \leq i \leq M-1)$ 对应于 DTBN 中的非叶节点 (即动态故障树中的中间事件和底事件); M 为节点数目; $e_i \in \{[0, \Delta), [\Delta, 2\Delta), \dots, [(n-1)\Delta, n\Delta), [T, \infty)\}$ 用来表征 E_i 的发生区间.

由式(25)、式(26)可以得到 E_T 在任务时间 T 内的发生概率,即

$$P(T) = \sum_{0 < x \leq n} \sum_{E_1, \dots, E_{M-1}} P(E_1 = e_1, \dots, E_{M-1} = e_{M-1}, E_T = [(x-1)\Delta, x\Delta)) \quad (27)$$

3.2 重要度

分析动态故障树的底事件重要度是非常困难的,目前只能采用基于 Markov 模型的近似算法.文献[7]在任务时间内假设部件各个区间出现故障的概率相同,然后计算重要度,这一假设往往与实际不符,因而计算结果存在较大偏差.下面给出一种新的

$$\frac{P(E_i = [(y-1)\Delta, y\Delta) \mid E_j = [(x-1)\Delta, x\Delta)) = \sum_{E_1, \dots, E_{i-1}, E_{i+1}, \dots, E_{j-1}, E_{j+1}, \dots, E_M} P(E_k = e_k, E_i = [(y-1)\Delta, y\Delta), E_j = [(x-1)\Delta, x\Delta), 1 \leq k \leq M, k \neq i, k \neq j)}{P(E_j = [(x-1)\Delta, x\Delta))} \quad (28)$$

$$P(E_i = [T, \infty) \mid E_j = [(x-1)\Delta, x\Delta)) = 1 - \sum_{0 < y \leq n} P(E_i = [(y-1)\Delta, y\Delta) \mid E_j = [(x-1)\Delta, x\Delta)) \quad (29)$$

(30)

利用这些信息,可以进行预计或诊断,因而转化后的 DTBN 具有更强的建模分析能力.

4 实例分析

某数字飞控计算机系统^[8]的动态故障树如图5所示,其中包括了3个动态逻辑门,即1个功能相关门和2个温备件门 S1、S2. 在底事件的代码上方标注了各部件的失效率,其中温备件 S1 和 S2 的休眠因子 $\beta=0.2$,在事件代码下方标注了任务时间 $T=$

E_i 概率重要度计算方法,即

$$I_i^{\text{Pr}}(T) = \frac{P(E_T = [T, \infty) \mid E_i = [T, \infty)) - \sum_{0 < x \leq n} P(E_T = [T, \infty), E_i = [(x-1)\Delta, x\Delta))}{1 - P(E_i = [T, \infty))} \quad (28)$$

对于关键重要度、结构重要度等也可以采用类似的方法得到,在此不再赘述.

3.3 其他分析结果

利用 DTBN 还能得到更加丰富的信息,比如 E_j 在区间 $[(x-1)\Delta, x\Delta)$ 内发生之后, E_i 发生的后验概率

50 h 时的各事件发生的概率.

利用第3节中的转化算法,可以得到该动态故障树对应的 DTBN,如图6所示,其中静态逻辑门向 DTBN 的转化方法见文献[7]. 底事件发生的先验概率和系统 10 h 失效条件下的后验概率的直方图如图7所示. 取 $\Delta=1$,利用贝叶斯网络工具箱(BNT)^[9]可计算得到顶事件概率 $P(T)$,与 Markov 链分析的结果对比如表1所示.从表中可以看出,二者计算的相对误差均保持在0.4%以内,这说明基

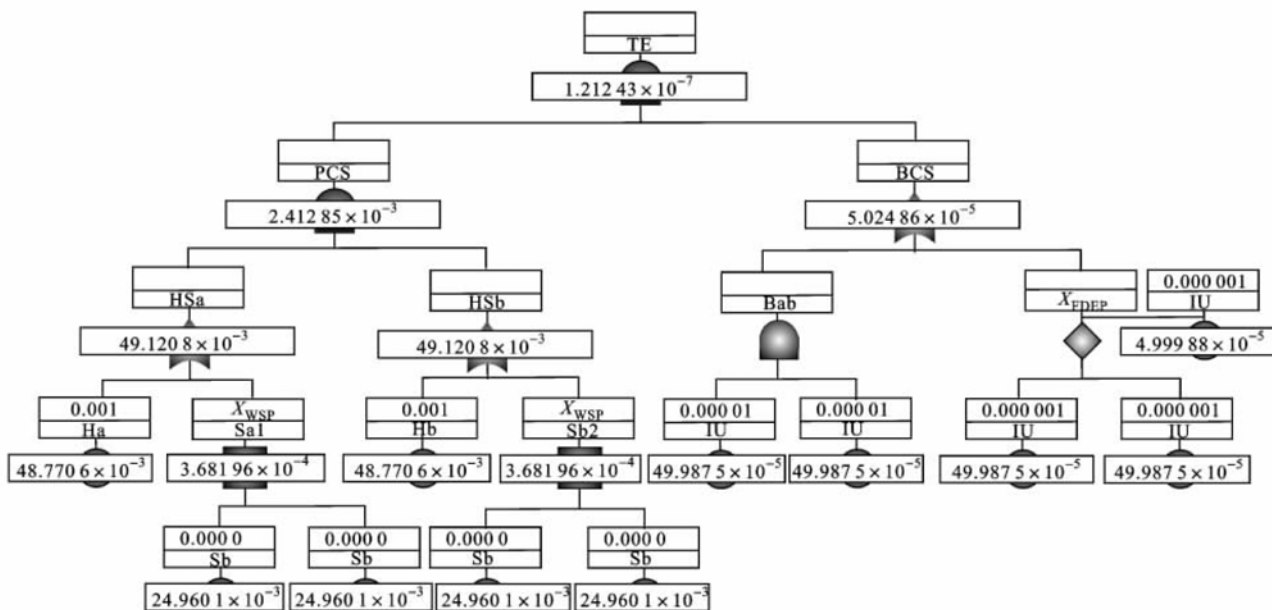


图5 数字飞控计算机系统动态故障树

表1 Markov链与DTBN计算结果比较

任务时间 /h	$P(T)$		$10^3 \times$ 相对误差
	Markov	DTBN	
5	$1.246\ 25 \times 10^{-10}$	$1.248\ 02 \times 10^{-10}$	1.420 0
10	$9.939\ 93 \times 10^{-10}$	$9.948\ 08 \times 10^{-10}$	0.819 9
15	$3.344\ 58 \times 10^{-9}$	$3.345\ 32 \times 10^{-9}$	0.221 3
20	$7.903\ 85 \times 10^{-9}$	$7.900\ 87 \times 10^{-9}$	0.377 0
25	$1.539\ 02 \times 10^{-8}$	$1.537\ 52 \times 10^{-8}$	0.974 7
30	$2.651\ 32 \times 10^{-8}$	$2.647\ 14 \times 10^{-8}$	1.577 0
35	$4.197\ 30 \times 10^{-8}$	$4.188\ 19 \times 10^{-8}$	2.170 0
40	$6.246\ 11 \times 10^{-8}$	$6.228\ 83 \times 10^{-8}$	2.767 0
45	$8.865\ 98 \times 10^{-8}$	$8.836\ 18 \times 10^{-8}$	3.361 0
50	$1.212\ 43 \times 10^{-7}$	$1.207\ 63 \times 10^{-7}$	3.959 0

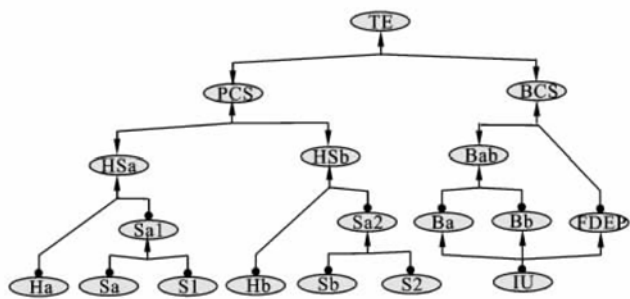
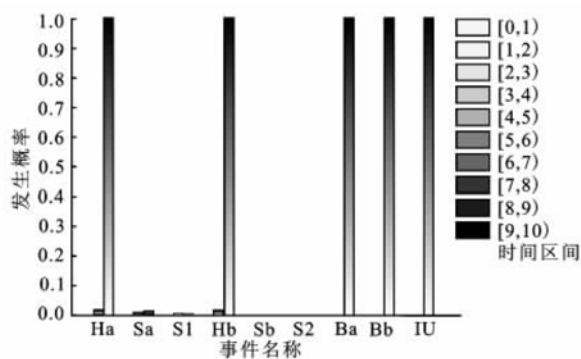


图6 数字飞控计算机系统离散时间贝叶斯网络



左柱:先验概率;右柱:后验概率

图7 数字飞控计算机系统在10 h失效时各部件发生故障的后验概率与先验概率对比直方图

于DTBN的分析方法能够保证较高的求解精度。

从图7可以看出,Ha、Hb、Ba、Bb和IU的后验概率最大,这说明系统一旦失效,很有可能是这些部件造成的.如果采用Markov链分析,则不会得到这样的信息.另外,DTBN在表达事件多状态、不确定信息方面的先天优势,是传统Markov链分析方法所无法比拟的。

5 结束语

本文研究了基于DTBN的动态故障树分析方

法,包括常用的动态逻辑门向DTBN的转化方法,以及基于DTBN的可靠性分析方法.本文的方法不仅能够得到常规的可靠性分析结果,而且便于预计和诊断.由于DTBN具有描述事件多态性和非确定性逻辑关系的能力,所以本文的方法非常适用于动态复杂系统的可靠性、安全性分析。

参考文献:

- [1] Dugan J B, Bavuso S J, Boyd M A. Dynamic fault-tree models for fault-tolerant computer systems [J]. IEEE Transactions on Reliability, 1992, 41(3):363-377.
- [2] Amari S, Dill G, Howald E. A new approach to solve dynamic fault trees [C]//Proceedings of Annual Conference on Reliability and Maintainability. Piscataway, USA: IEEE, 2003:374-379.
- [3] Bobbio A, Portinale L, Minichino M, et al. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks [J]. Reliability Engineering and System Safety, 2001, 71(3):249-260.
- [4] Langseth H. Bayesian networks with applications in reliability analysis [D]. Trondheim, Norway: Department of Mathematical Sciences, Norwegian University of Science and Technology, 2002.
- [5] 周忠宝,董豆豆,周经伦. 贝叶斯网络在可靠性分析中的应用 [J]. 系统工程理论与实践, 2006, 26(6): 95-100.
Zhou Zhongbao, Dong Doudou, Zhou Jinglun. Application of Bayesian networks in reliability analysis [J]. System Engineering Theory & Practice, 2006, 26(6): 95-100.
- [6] Montani S, Portinale L, Bobbio A. Dynamic Bayesian networks for modeling advanced fault tree features in dependability analysis [C]//European Safety and Reliability Conference. Leiden, Netherlands: Balkema Publishers, 2005:1414-1422.
- [7] Boudali H, Dugan J B. A discrete-time Bayesian network reliability modeling and analysis framework [J]. Reliability Engineering and System Safety, 2005, 87(3):337-349.
- [8] 程明华,姚一平. 动态故障树分析方法在软、硬件容错计算机系统中的应用 [J]. 航空学报, 2000, 21(1): 34-37.
Cheng Minghua, Yao Yiping. Application of dynamic fault tree analysis to software and hardware fault-tolerant control computer systems [J]. Acta Aeronautica et Astronautica Sinica, 2000, 21(1): 34-37.
- [9] Murphy K P. The Bayes net toolbox for Matlab [J]. Computing Science and Statistics, 2001, 33:331-351.

(编辑 苗凌)