doi:10.11959/j.issn.1000-436x.2017156

# 针对扩展动态故障树的约束分析方法

吴奇烜[1]，马建峰[1]，孙聪[1]，张帅[1]，张双[2]，郑涛[2]
（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；
2. 中国航空工业集团公司西安航空计算技术研究所，陕西 西安 710068）

**摘 要**：提出延时门机制对动态故障树进行扩展，用于对子系统失效延时传播到上层系统进行建模，并通过扩展动态贝叶斯网络对包含延时门的动态故障树进行求解。还提出并实现了一种基于可满足性模理论的扩展动态故障树求解算法，支持由非确定性的基本事件概率范围约束求解系统的最优化失效率。通过对实际系统的分析、求解及与现有工具的对比，说明分析方法的有效性，并通过对实际系统的分析给出了基本事件概率约束和延时门参数对系统整体失效率的影响。

**关键词**：延时门；动态故障树；动态贝叶斯网络；可满足性模理论
**中图分类号**：TP311.5 **文献标识码**：A

# Constraint analysis for extended dynamic fault tree

WU Qi-xuan[1], MA Jian-feng[1], SUN Cong[1], ZHANG Shuai[1], ZHANG Shuang[2], ZHENG Tao[2]
(1. School of Cyber Engineering, Xidian University, Xi'an 710071, China;
2. Aeronautical Computing Technique Research Institute, Aviation Industry Corporation of China, Xi'an 710068, China)

**Abstract:** As a new extension of dynamic fault trees, time delay gate was proposed. This new mechanism can be used to model the time delay on the fault propagation from the lower level subsystems to the higher level system. The dynamic Bayesian networks was extend to solve the dynamic fault trees containing time delay gates. An algorithm based on SMT to support the optimized failure distribution under the nondeterministic range constraint of basic events was also proposed. The effectiveness is shown by comparison with existing tools on analyzing and solving real systems, and the effects of range constraints and gate parameter on the failure distribution of systems is illustrated.

**Key words:** time delay gate, dynamic fault tree, dynamic Bayesian network, satisfiability modulo theory

## 1 引言

动态故障树[1]通常用于组件失效时对系统风险进行建模，不仅可以表示系统组件间的与、或、表决关系，也能对可靠性分析中常见的冗余管理、功能依赖和有序依赖进行建模。动态故障树的叶节点描述基本事件（BE, basic event），代表具体的组件失效，每个基本事件对应一个概率分布；非叶节点上的基本门结构描述失效如何在系统中传播；故障树的根节点又称顶层事件（TE, top-level event），通常表示整体系统的危害。

动态故障树的扩展和求解方法是近年研究的热点。Mo[2]针对不含容错机制的动态故障树提出了一种多值的基于决策图的求解方法。Ge 等[3]提出一种改进的有序二叉决策图算法，使用启发式索引保证产生的切割序列规模尽可能小。Zhu 等[4,5]分别针

**收稿日期**：2016-12-13；**修回日期**：2017-03-30
**基金项目**：国家自然科学基金资助项目（No.61303033, No.U1405255）；国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA017203）；陕西省自然科学基础研究计划基金资助项目（No.2016JM6034）；航空科学基金资助项目（No.20141931001）；工信部某专项科研基金资助项目（No.MJ-2014-S-37）
**Foundation Items:** The National Natural Science Foundation of China (No.61303033, No.U1405255), The National High Technology Research and Development Program of China (863 Program) (No.2015AA017203), The Natural Science Basis Research Plan in Shaanxi Province of China(No.2016JM6034), The Aviation Science Foundation of China (No.20141931001), The Special Research Foundation of MIIT( No.MJ-2014-S-37)

对含有 PAND 门和 SP 门的动态故障树，提出一种高效的随机计算方法，并针对组件失效率分布为非指数分布的情况给出了解决方案。针对动态故障树中的功能依赖部分，Xing 等[6]提出一种基于分治范式的可组合、可分离的动态故障树计算方法。Guck 等[7]实现了一个用于量化分析含修复策略的动态故障树的工具，其通过随机模型检查交互式马尔可夫链实现量化分析。Bäckström 等[8]提出了一种 SD 故障树，结合了静态故障树和动态故障树的特点，其核心在于使用了面向基础动态行为的边界逼近。Volk 等[9]提出了一种新的状态空间生成动态故障树的方法，大幅提升了动态故障树的生成效率。徐丙凤等[10]为构件化系统失效时间特性的分析提供了一种状态事件故障树的时间特性分析方法，精化了交互马尔可夫链的交互动作，并使用弱互模拟对状态空间进行约简。Bobbio 等[11]对动态故障树的扩展引入了修复盒（RB, repair box）的概念，用于对含有可修复组件的系统进行建模。引入修复盒后，动态故障树能够描述组件由失效状态转换为正常状态的情况。修复率不同，系统对外表现出的失效率也不同，修复率越高，系统总体危险概率越低。近年来，含修复盒的动态故障树已应用于系统脆弱性的恢复过程进行建模[12,13]。

含修复盒的动态故障树存在以下两方面局限性。1) 在建模的表达能力方面，实际系统的修复过程往往受修复时间的约束[14]。组件的失效如果可以在某时限内被修复，则视为组件仍正常工作；而失效时长超过时限约束的修复被认为无效。现有动态故障树建模机制中，尚无具体方法能够对此类修复时限约束进行描述。2) 在求解算法方面，现有求解算法均由确定的基本事件概率求解确定的顶层事件概率，当仅能对基本事件概率指定范围约束而无法指定具体值时，尚无算法能够求出顶层事件的最优化概率。

针对以上问题，本文提出一种延时门机制对动态故障树进行扩展，延时门能够延缓组件或子系统的失效向上层传播的时间，从而对包含可修复组件和具体修复时间约束的系统，实现精确的动态故障树建模和分析。本文通过扩展动态贝叶斯网络[15]（DBN, dynamic Bayesian network）对含延时门的动态故障树进行建模。在此基础上，提出并实现了一种基于可满足性模理论（SMT, satisfiability modulo theory）的动态故障树求解算法，该算法首次支持基本组件失效参数为范围约束的情况下求解顶层事件的最优化概率。通过对多种实际系统的建模和分析求解，得出延时门机制在修复时间约束下可有效分析系统的整体失效率分布；通过与现有工具比较，说明了基于 SMT 的求解算法的准确性；通过典型实例分析说明了最优化概率求解方法的有效性。

## 2 基本知识

动态故障树是由特定门结构组合而成的树状结构，包含一个或多个输入和一个输出，通过输入与输出之间的逻辑关系描述系统故障之间的传播与影响。动态故障树的基本门结构包括与门（AND）、或门（OR）、优先与门（PAND）、备件门（SP）、概率功能依赖门（PDEP）和修复盒（RB）。各基本门结构均具有图形化表示。当且仅当所有输入事件都发生且优先事件首先发生，PAND 门表示输出事件发生。SP 门将输入分为一个主输入和若干替补输入，仅当所有输入事件均发生时输出事件才发生，其中，替补输入事件在主输入事件尚未发生时的发生概率，是其在主输入事件已发生时的发生概率的 $\alpha$ 倍（$0\leqslant\alpha\leqslant1$）。PDEP 门的输入由一个触发事件（基本事件或门事件）及多个相关基本事件组成，输出为不相关事件。其逻辑关系为触发事件的发生将导致相关基本事件以概率 $\pi$ 发生（$0\leqslant\pi\leqslant1$）。修复盒（RB）的使用条件是系统组件具有可修复性。基本事件或门事件的发生将触发 RB 的运作，使 RB 由正常变为修复状态，RB 对组件的修复有特定的概率分布，当 RB 由修复状态变为正常状态时，其所修复的基本组件也恢复正常。

利用动态贝叶斯网络求解动态故障树，是当前动态故障树求解的主流方法。动态贝叶斯网络支持离散时态维度，每个时间片中的节点表示随机变量，节点间的有向边表示相邻时刻随机变量间的依赖关系。通常情况下，组件的失效率服从参数为 $\lambda$ 的指数分布。针对系统基本组件，动态贝叶斯网络通过状态迁移表示从 $t$ 时刻到 $t+\Delta t$ 时刻组件失效概率的变化。假定不可修复的基本组件 $A$ 在 $t$ 时刻和 $t+\Delta t$ 时刻的失效事件分别由 $A$ 和 $A\#$表示，组件 $A$ 在 $t+\Delta t$ 时刻的失效率 $P(A\#=1)$可由式(1)计算。

$$P(A\# = 1) = P(A = 1) + (1 - P(A = 1))F(\Delta t, A) \quad (1)$$

其中，$F(\Delta t, A)$为组件 $A$ 在 $\Delta t$ 时间段内由正常状态变为失效状态的概率，即 $F(\Delta t, A)=P(A\#=1|A=0)$。

对于不可修复组件，有 $P(A\#=1|A=1)=1$。

表 1 给出了各种门结构的输出事件概率计算式，其中，$A$、$B$ 为输入事件。对于 RB，假定由组件 $A$ 的失效触发修复并用于修复组件 $A$。$t+\Delta t$ 时刻组件 $A$ 处于失效状态且正在修复的概率（$P(RB\#=1)$）等于组件 $A$ 新增的失效概率（$P(A\#=1)-P(RB=1)$）与组件 $A$ 在 $\Delta t$ 时间内未被修复的概率（$P(RB=1)(1-R(\Delta t, A)P(trigger))$）之和，其中 $P(trigger)$为触发对组件 $A$ 修复的概率，$R(\Delta t, A)$表示组件 $A$ 在 $\Delta t$ 时间内由修复盒修复的概率。组件 $A$ 在 $t+\Delta t$ 时刻失效的概率（$P(A\#=1)$）为上一时刻修复盒工作之后依然失效的概率（$P(RB=1)$）与新增失效概率（$P(A=0)F(\Delta t, A)$）之和。

如果组件可修复且存在修复机制，则系统失效率将降低。假定系统 $A$ 与系统 $B$ 为同构系统，$A$ 与 $B$ 的组件失效率相同，但 $A$ 中组件可修复而 $B$ 中组件不可修复，则在 $t+\Delta t$ 时刻，$B$ 的失效率 $P(B\#=1)=P(B=1)+(1-P(B=1))F(\Delta t,B)$，$A$ 的失效率 $P(A\#=1)=P(A=1)+(1-P(A=1))F(\Delta t, A)-P(A=1)$。$R(\Delta t, A)P(trigger)$。由于系统 $A$ 与系统 $B$ 的组件失效率相同，故 $F(\Delta t, A)=F(\Delta t, B)$，在第 0 时刻 $P(A=1)=P(B=1)$的前提下，易知对任意 $t\geqslant 0$ 有 $P(A\#=1)\leqslant P(B\#=1)$。所以，存在修复机制能够降低系统失效率。

**表 1　各种功能门的动态贝叶斯网络上层事件条件概率计算式**

| 门结构 | 门输出概率计算式 |
|---|---|
| AND | $P(\text{AND}\#=1)=P(A\#=1)P(B\#=1)$ |
| OR | $P(\text{OR}\#=1)=1-(1-P(A\#=1))(1-P(B\#=1))$ |
| PDEP | $P(X\#=1)=\pi P(Tr\#=1)+P(Tr\#=0)(P(X=0)F(\Delta t,X)+P(X=1))$，其中，$X=A,B$ |
| SP | $P(B\#=1)=(P(A=0)\alpha+P(A=1))P(B=0)F(\Delta t,B)+P(B=1)$<br>$P(SP\#=1)=P(A\#=1)P(B\#=1)$ |
| PAND | $P(\text{PAND}\#=1)=P(\text{PAND}=1)+\dfrac{P(A\#=1)+P(A=1)}{2(P(B\#=1)}-P(B=1))$ |
| RB | $P(RB\#=1)=P(A\#=1)-P(RB=1)+P(RB=1)(1-R(\Delta t,A)P(trigger))$<br>$P(A\#=1)=P(A=0)F(\Delta t,A)+P(RB=1)$ |

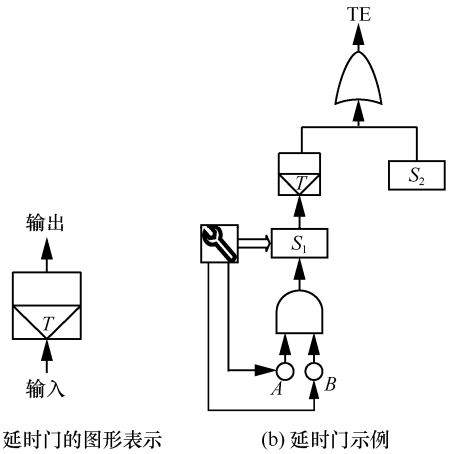
## 3　延时门

### 3.1　延时门定义

在实际系统中，某些失效组件如能在某时限内被修复，则可视为组件仍正常工作。而失效时长超过时限约束的组件被认为修复无效。现有修复盒建模机制无法对此类修复时限约束进行描述，为此，本文提出延时门（TD, time delay gate）建模机制。

**定义 1**　延时门是一种使用时间参数 $T$ 描述单一输入事件对单一输出事件影响延迟的动态故障树门结构。其语义为：输入事件的发生触发计时，若在 $T$ 时间内输入事件未能恢复到未发生状态，则输出事件发生；若在 $T$ 时间内输入事件恢复到未发生状态，则计时器清零且输出事件保持未发生状态。其图形表示如图 1(a)所示。

延时门的使用条件即系统存在某些组件或子系统，其失效在一定时间内不影响系统正常运行。当构成系统的组件可修复时，修复机制可看作将输入事件恢复到未发生状态的机制，因而，延时门通常与修复盒配合使用。图 1(b)中的动态故障树示例简要说明延时门的含义和用法，系统顶层事件 TE 依赖于 $S_1$ 或 $S_2$ 的发生。$S_1$ 为接受 2 个基本事件 $A$、$B$ 的与门的输出，$S_1$ 的发生会触发修复盒对 2 个基本事件的修复，若修复在时间 $T$ 内完成，则 $S_1$ 不影响顶层事件；若修复在时间 $T$ 内未完成，则顶层事件发生。




(a) 延时门的图形表示　　(b) 延时门示例

图 1　延时门的图形表示及示例

### 3.2　通过扩展动态贝叶斯网络求解延时门

由于一般动态贝叶斯网络推理遵循一阶马尔可夫过程，即在时间片段 $T$ 的状态仅与时间片段 $T-\Delta t$ 的状态有关，而与 $T-\Delta t$ 以前的时间片段的状态无关。这一要求使动态贝叶斯网络无法直接用于求解延时门。需对动态贝叶斯网络做出扩展以支持对延时门的输出条件概率进行计算。扩展后的动态贝叶斯网路转换图如图 2(a)所示。其中，$A$ 表示带有修复机制的基本组件或子系统。假定延时门参数 $T$ 与动态贝叶斯网络时间间隔 $\Delta t$ 的关系为 $T=n\Delta t$，将延时门转换为包含 $n+1$ 个状态 $FO_i$（$0\leqslant i\leqslant n$）之间转移的动态贝叶斯网络。其中，$FO_0\#=1$ 的概率与延时门的输入事件发生概率相

等，而 $FO_i$#=1 的概率为 $FO_{i-1}$=1 的概率与该子系统在 $\Delta t$ 时间内未能修复的概率（对于给定的子系统，此概率为定值 $C$）之积。输出事件 *TD*#发生概率即为 $FO_n$#=1 的概率，计算式见表 2。图 2(a)的简化表示如图 2(b)所示，其中，方形节点表示由多个状态组成的抽象状态。

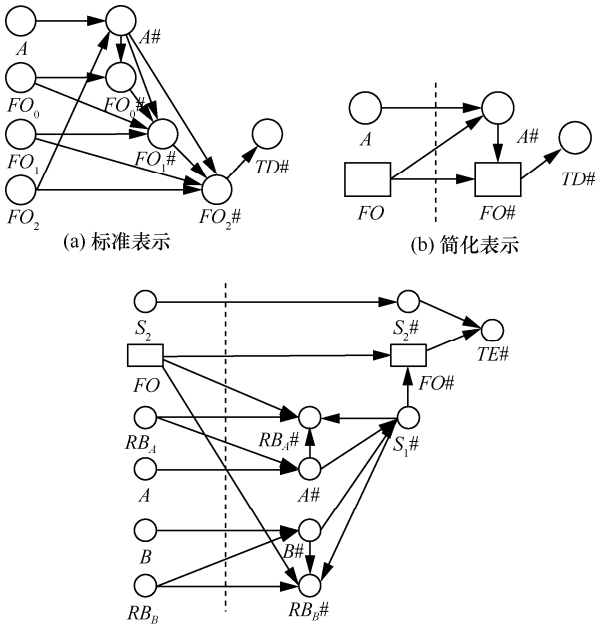



图 2　延时门的扩展动态贝叶斯网络转换图及示例

延时门对修复盒的作用体现在：若修复盒不能在给定的时间 $T$ 内完成对基本组件的修复使子系统恢复正常，则子系统将会失效，因而一旦子系统事件已经发生，即 *TD*#=1，则可视为修复盒停止修复工作，故修复盒可正常进行修复工作的概率为 1−$P$(*TD*#=1)，在 $\Delta t$ 时间内所修复组件 $A$ 的修复概率变为 $R(\Delta t, A)(1-P(TD\#=1))P(trigger)$，因而，在含有延时门的子系统中对 $P(RB\# = 1)$的计算应修正为表 2 中的 $RB'$。

**表 2　延时门的上层事件条件概率计算式及对修复盒概率式的修正**

| 门结构 | 门输出概率计算式 |
|---|---|
| $RB'$ | $P(RB\# = 1) = P(A\# = 1) - P(RB = 1) + P(RB = 1) \cdot (1 - R(\Delta t, A)(1 - P(TD\# = 1))P(trigger))$<br>$P(A\# = 1) = P(A = 0)F(\Delta t, A) + P(RB = 1)$ |
| TD | $P(FO_0\# = 1) = P(A\# = 1)$<br>$P(FO_i\# = 1) = P(FO_{i-1} = 1)C,\ 0 \leqslant i \leqslant n$<br>$P(TD\# = 1) = P(FO_n\# = 1)$ |

将图 1(b)示例中的动态故障树转换为扩展的动态贝叶斯网络如图 2(c)所示，相应的顶层事件概率计算式如下

$$\begin{cases} P(S_2\#=1) = P(S_2=1) + P(S_2=0)F(\Delta t, S_2) \\ P(FO_0\#=1) = P(S_1\#=1) \\ P(FO_i\#=1) = P(FO_{i-1}=1)C \\ P(X\#=1) = P(X=0)F(\Delta t, X) + P(RB_X=1), \\ \qquad\qquad\qquad\qquad \text{其中，}\ X = A, B \\ P(RB_X\#=1) = P(X\#=1) - P(RB_X=1)R(\Delta t, X)\cdot \\ (1 - P(FO_n\#=1))P(S_1\#=1),\ \text{其中，}\ X = A, B \\ P(S_1\#=1) = P(A\#=1)P(B\#=1) \\ P(TE\#=1) = 1 - (1 - P(S_2\#=1)(1 - P(FO_n\#=1))) \end{cases} \tag{2}$$

给定组件 $A$ 和 $B$ 的失效率、修复盒 $RB_A$ 和 $RB_B$ 的修复率、子系统 $S_2$ 的失效率以及延时门参数 $T$ 的值，即可以求得顶层事件 *TE* 随时间的发生概率。

## 4　基于可满足性模理论的扩展动态故障树求解算法

虽然本文能够列出与 3.2 节的扩展动态贝叶斯网络对应的概率计算式，但由于延时门的存在导致时间片段 $T$ 的系统状态会受前 $n$ 个时间片段的影响，传统动态贝叶斯网络求解方法由于仅能在相邻时间片间做推理计算，因而无法求解扩展后的动态贝叶斯网络，不支持对含延时门的动态故障树的求解。本文提出基于 SMT 的动态故障树求解算法，通过在 SMT 求解器中记录多个时间间隔前的延时门失效率，逐步递推实现跨时间片的概率计算，从而求解出含延时门的动态故障树的顶层事件失效率分布。另一方面，现有算法也无法计算基本事件概率不确定的情况，而本文基于 SMT 的求解算法能够通过向求解器中增删逻辑约束来解决这一问题。因此，本文基于 SMT 的求解算法进一步拓展了动态贝叶斯网络的分析求解能力。

算法 1 中，$S$ 为一系列约束的集合，SMT 求解器能够自动检验 $S$ 中的约束是否可满足。*S.add*()即向求解器中添加约束；对于动态贝叶斯网络 $G$=$\{V,E\}$，整个网络含有限个时间片段，每个时间片段由一个有向无环图 $G_T$=$\{V_T,E_T\}$和节点需满足的条件概率分布 $P(V_T)$组成，其中，$V_T$ 和 $E_T$ 分别是第 $T$ 个时间片段的节点集合和有向边集合；对于每一个时间片，算法调用 *S.check*()检验求解器中约束的可满足性，并生成一个可满足实例 *S.model*，该可满足实例包含当前时间片各个节点的失效率。*update*($M$)根据上一可满足实例 $M$ 更新当前时间片

段节点失效率。当叶节点存在约束时，*SearchMin*(*TE*)用于求出当前最优的系统失效率，具体算法为：先根据当前 *S.model* 中 *TE* 值进行无界搜索，锁定最优值的上界与下界，然后使用二分查找得到允许误差下的最优值。

**算法 1**　基于 SMT 的动态故障树求解算法

**输入**　$G=\{V,E\}$为由动态故障树转化得到的动态贝叶斯网络；$\lambda_v$为基本组件的失效参数（确定值或范围约束）；$\mu$ 为修复盒修复率（如果修复盒存在）

**输出**　$List_{TE}$ 为各时刻顶层事件发生故障的概率序列

Begin

1) 初始化 SMT 求解器：$S\leftarrow\varnothing$;

2) $List_{TE}[0]\leftarrow 0$;

3) *S.add*($P(V_T)$);

4) for　$v \in V_0$　do /*初始化节点参数及失效率应满足的条件*/

5)　　*S.add*($\lambda_v$, $\mu$); /*仅基本组件*/

6)　　*S.add*( $P(v=0)+P(v=1)=1$);

7)　　*S.add*($P(v=0)\geqslant 0$ && $P(v=0)\leqslant 1$);

8)　　*S.add*($P(v=1)\geqslant 0$ && $P(v=1)\leqslant 1$);

9) $i\leftarrow 0$ ; /* $i$ 为时间片计数*/

10) *S.check* ( );

11) $M\leftarrow$ *S.model* ;

12) while $List_{TE}[i]<1$ do

13)　　for　$v\in V_i$　do

14)　　*update*(*M*);

15)　　*SearchMin*(*TE*);

16)　　$List_{TE}[i]\leftarrow M[TE]$;

17)　　*S.check*() ;

18)　　$M\leftarrow$ *S.model* ;

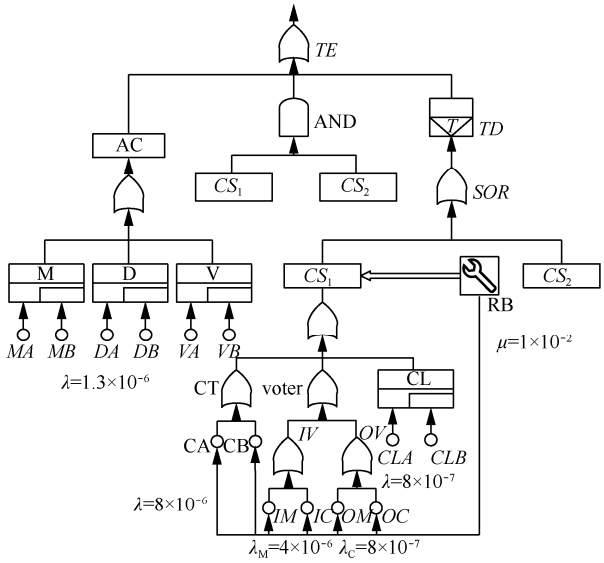
19)　　$i\leftarrow i$+1;

20) Return $List_{TE}$

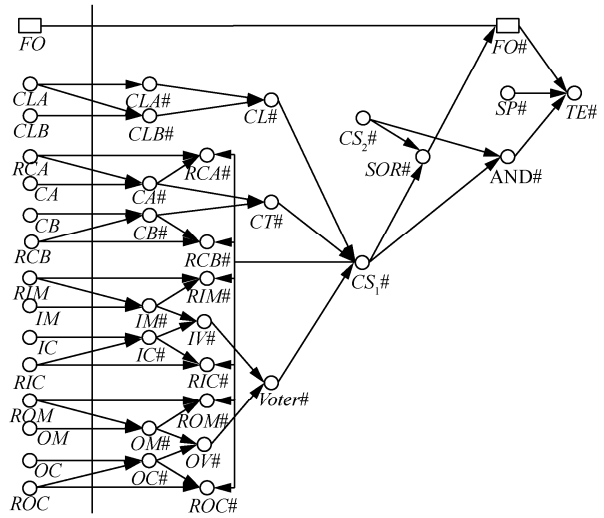
End

## 5　方法评价及应用

本节通过与动态故障树分析工具 RADYBAN[16] 的对比说明本文方法的有效性。通过求解分析实际系统的延时修复及求解基本事件概率约束下的顶层事件最优化概率，说明本文方法的特性。实验使用的SMT求解器为$Z_3$，实验环境为Intel(R) Xeon(R) E5-2640 v3 (32 Core@2.6 GHz)、128 GB RAM、Ubuntu Server 14.04。本文所用系统的动态故障树实例包括：心脏辅助装置、多处理器计算系统、攻击树模型及图 3(a)所示的飞控计算机系统动态故障树。




(a) 动态故障树




(b) 动态贝叶斯网络

图 3　飞控计算机系统动态故障树及其动态贝叶斯网络

飞控计算机系统由数据采集模块和双余度计算机组成。对模拟量（M）、离散量（D）和数字量（V）的采集模块由备件门描述。任一数据量的采集失效均导致整个数据采集模块 AC 失效。结构相同的计算机 $CS_1$ 与 $CS_2$ 共同构成双余度系统。每个余度的计算系统包含交叉传输（CT），输入/输出表决（voter）和控制率计算（CL）模块。交叉传输模块由 RAM 组件 *CA* 和 *CB* 构成，输入表决 *IV* 和输出表决 *OV* 组件分别由用于记录上次

表决结果的存储器 *IM*、*OM* 和表决控制器 *IC*、*OC* 组成；当 $CS_1$ 与 $CS_2$ 之一出现故障时，触发修复盒对其相关基本组件进行修复，此时，整个双余度系统可依靠另一计算系统正常工作一段时间 *T*，可用延时门表示这一时间约束，而当 2 个计算系统同时出现故障时，整个系统将不能正常工作，用 AND 门表示这一逻辑关系。将此动态故障树转换为动态贝叶斯网络，如图 3(b)所示。参照文献[14]中对飞机系统失效率的要求（$10^{-7}$ 数量级）和文献[17]中对嵌入式系统关键组件的失效参数取值（$10^{-6}$ 数量级），结合相关领域专家的建议，将本文飞控计算机系统的组件参数按图 3(a)中的失效参数进行赋值。

为了说明本文提出的基于 SMT 的扩展动态故障树求解算法的有效性，分别使用 RADYBAN 与本文算法对上述 4 个含修复盒的动态故障树实例进行计算（所有节点的失效参数均依据文献[13,15,18]进行赋值），计算结果如图 4 所示。可以看出通过 2 种方法所得的系统失效率曲线趋近一致。差别的原因在于对修复盒的定义，RADYBAN 仅支持对单个基本节点进行修复，而本文定义的修复盒支持对整个子系统修复。可见，本文算法可以有效地对故障系统进行定量的分析求解。

与其他方法相比，本文方法首次支持：1）由非确定性的基本事件概率范围约束求解顶层事件的最优化概率；2）对于含延时门的动态故障树的求解。本文方法能够描述以上 2 种情况对系统可靠性评估结果的影响。

对图 3(a)所示的飞控系统，不考虑修复机制的情况下，设置交叉传输模块基本组件 *CA* 的失效参数 $\lambda_{CA}$ 在$[6\times10^{-6}, 9\times10^{-6}]$，然后计算此时系统顶事件能取到的极值，即分析系统最低失效率。如图 5 所示，$\mathrm{BOUND_{up}}$ 与 $\mathrm{BOUND_{low}}$ 曲线分别为 $\lambda_{CA}$ 取 $9\times10^{-6}$、$6\times10^{-6}$，$\lambda_{CB}$ 取 $8\times10^{-6}$ 时系统的失效率分布，而 $\mathrm{CONSTR_{single}}$ 则为 *CA* 处于约束状态下得到的系统失效率。可以看到 $\mathrm{CONSTR_{single}}$ 基本与 $\mathrm{BOUND_{low}}$ 重合，即约束条件下，系统最优化失效率即为 $\lambda_{CA}$ 取得 $6\times10^{-6}$ 时的失效率。本文方法还支持多个节点带约束的情况，图 5 中 $\mathrm{CONSTR_{multiple}}$ 为组件 *CA* 的失效参数 $\lambda_{CA}\in[6\times10^{-6}, 9\times10^{-6}]$、组件 *CB* 的失效参数 $\lambda_{CB}\in[2\times10^{-6}, 5\times10^{-6}]$的情况下，系统顶事件失效率分布曲线，可以看出系统失效率明显低于上述任何一条曲线。本文算法可得出，此种情况下的系统最优化失效率为 $\lambda_{CA}$ 取 $6\times10^{-6}$ 且 $\lambda_{CB}$ 取 $2\times10^{-6}$ 时的失效率。

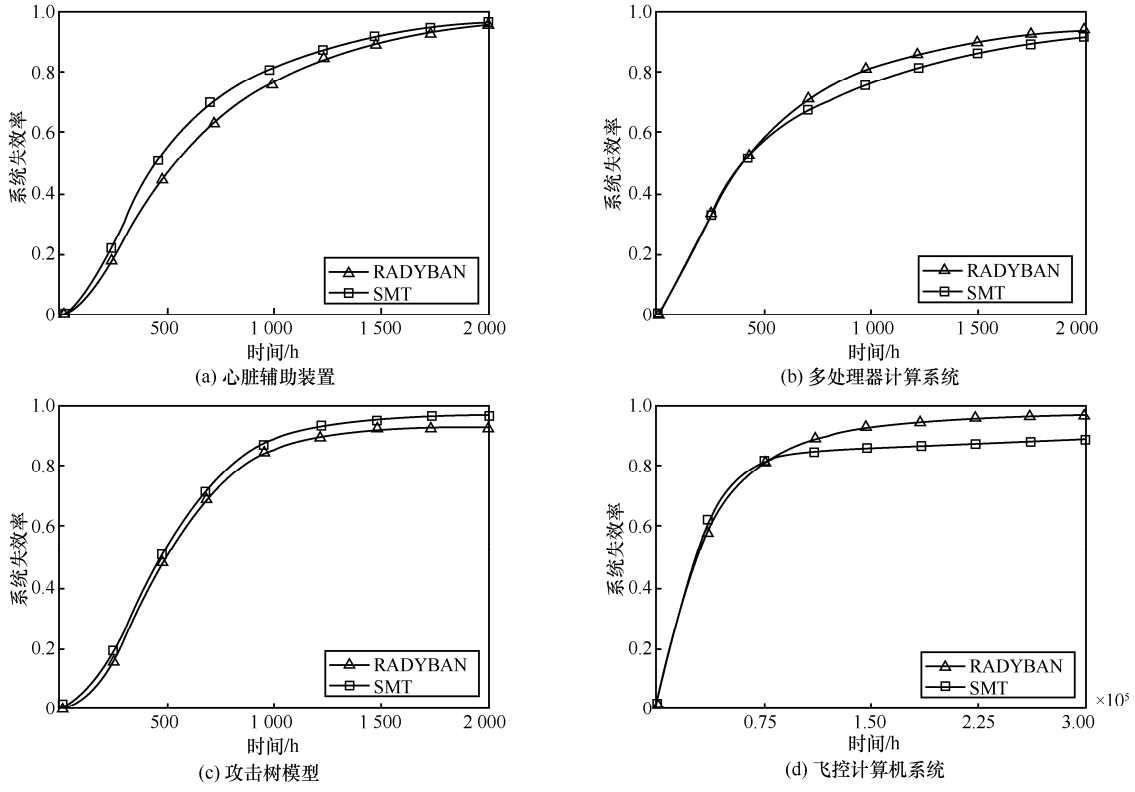



图 4　各系统失效率分布

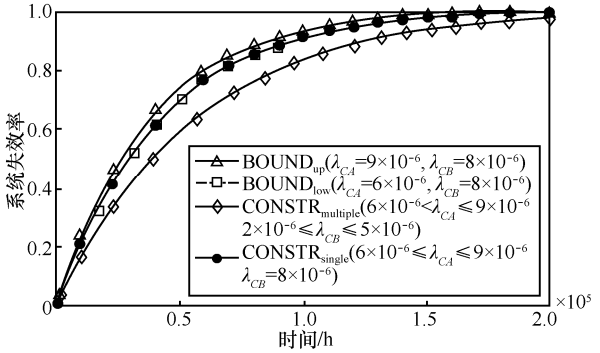



图 5　基本组件失效参数为范围约束对系统失效率的影响

图 6 为飞控计算机系统在 $T$ 值为 0、60 000 h、100 000 h、140 000 h 下的系统失效率分布结果。可以看出，在任意特定时刻系统的失效率随 $T$ 的增大而减小，当 $T$ 增大到 140 000 h 时，系统的失效率下降明显。因此，在含有容错机制的系统中，容错机制的改进会放宽修复时间限制并提升系统健壮性，使用延时门能够正确描述这种健壮性的提升。

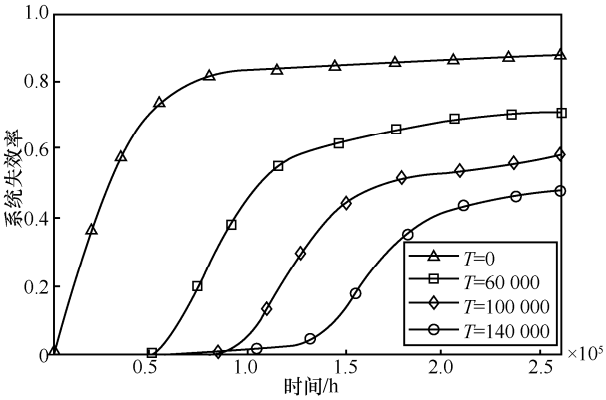



图 6　延时门参数对失效率的影响

## 6　结束语

本文提出了延时门机制扩展动态故障树，并针对此机制，提出了通过扩展动态贝叶斯网络对动态故障树进行求解的方法——基于 SMT 的求解算法，以支持基本事件概率为非确定性范围约束时的系统失效率求解。未来将考虑改进求解算法效率并将扩展动态故障树应用于系统脆弱性恢复过程的建模与分析。

## 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] MO Y C. A multiple-valued decision-diagram-based approach to solve dynamic fault trees[J]. IEEE Transactions on Reliability, 2014, 63(1): 81-93.

[3] GE D C, LIN M, YANG Y H, et al. Quantitative analysis of dynamic fault trees using improved sequential binary decision diagrams[J]. Reliability Engineering & System Safety, 2015: 289-299.

[4] ZHU P C, HAN J, LIU L B. A stochastic approach for the analysis of fault trees with priority AND gates[J]. IEEE Transactions on Reliability, 2014, 63(2): 480-494.

[5] ZHU P C, HAN J, LIU L B, et al. A stochastic approach for the analysis of dynamic fault trees with spare gates under probabilistic common cause failures[J]. IEEE Transactions on Reliability, 2015, 64(3): 878-892.

[6] XING L D, MORRISSETTE B A, DUGAN J B. Combinatorial reliability analysis of imperfect coverage systems subject to functional dependence[J]. IEEE Transactions on Reliability, 2014, 63(1): 367-382.

[7] GUCK D, SPEL J, STOELINGA M, et al. DFTCalc: reliability centered maintenance via fault tree analysis (tool paper)[C]//International Conference on Formal Engineering Methods. 2015

[8] BÄCKSTRÖM O, BUTKOVA Y, HERMANNS H, et al. Effective static and dynamic fault tree analysis[C]//International Conference on Computer Safety, Reliability and Security. 2016: 266-280.

[9] VOLK M, JUNGES S, KATOEN J P. Advancing dynamic fault tree analysis-get succinct state spaces fast and synthesise failure rates[C]// International Conference on Computer Safety, Reliability, and Security. 2016: 253-265.

[10] 徐丙凤, 黄志球, 胡军, 等. 一种状态事件故障树的时间特性分析方法[J]. 软件学报, 2015, 26(2): 427-446.
XU B F, HUANG Z Q, HU J ,et al. Time property analysis method for state/event fault tree[J]. Journal of Software, 2015, 26(2):427−446.

[11] BOBBIO A, RAITERI D C. Parametric fault trees with dynamic gates and repair boxes[C]//The 2004 Annual Symp on Reliability and Maintainability. 2004: 459-465.

[12] CODETTA-RAITERI D. A preliminary application of generalized fault trees to security[C]//International Conference on Security and Cryptography. 2013.

[13] CODETTA-RAITERI D. Generalized fault trees: from reliability to security[C]//International Workshop on Quantitative Aspects in Security Assurance, 2013.

[14] BISHOP P. Does software have to be ultra reliable in safety critical systems[C]//Computer Safety, Reliability, and Security. Berlin: Springer, 2013: 118-129.

[15] MONTANI S, PORTINALE L, BOBBIO A. Dynamic Bayesian networks for modeling advanced fault tree features in dependability anal-

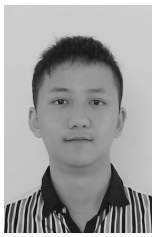
ysis[C]//16th European Conference on Safety and reliability. 2005: 1415-1422.

[16] MONTANI S, PORTINALE L, BOBBIO A, et al. Automatically translating dynamic fault trees into dynamic bayesian networks by means of a software tool[C]//First International Conference on Availability, Reliability and Security (ARES'06). 2006: 6.

[17] YUGE T, YANAGI S. Dynamic fault tree analysis using bayesian networks and sequence probabilities[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2013: 953-962.

[18] CODETTA-RAITERI D. Integrating several formalisms in order to increase fault trees' modeling power[J]. Reliability Engineering & System Safety, 2011, 96(5): 534-544.

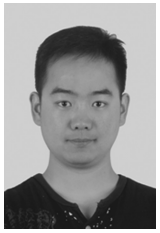
**作者简介：**



**吴奇烜**（1992-），男，陕西商洛人，西安电子科技大学硕士生，主要研究方向为系统可靠性分析、信息流安全。

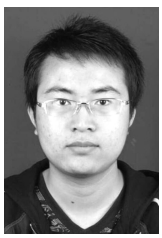
**马建峰**（1963-），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线和移动安全等。

**孙聪**（1982-），男，陕西兴平人，博士，西安电子科技大学副教授，主要研究方向为信息流安全、可信软件。



**张帅**（1990-），男，江苏沛县人，西安电子科技大学硕士生，主要研究方向为大型富媒体系统架构的设计。

**张双**（1976-），男，陕西汉中人，中国航空工业集团公司西安航空计算技术研究所研究员，主要研究方向为计算机网络与机载信息安全技术。



**郑涛**（1988-），男，陕西岐山人，中国航空工业集团公司西安航空计算技术研究所工程师，主要研究方向为计算机网络与机载信息安全技术。