文章编号:1001 - 2486(2004)02 - 0100 - 06

动态系统可靠性分析的新概念*

金　光

(国防科技大学人文与管理学院,湖南 长沙　410073)

摘　要:传统可靠性分析的概念只能描述静态逻辑关系,不能满足现代复杂动态系统可靠性分析的需要。在给出动态系统状态空间结构和结构函数的基础上,提出失效序列和失效丛的概念描述动态系统的故障模式,这一概念扩展了传统可靠性分析的概念,将割集、蕴含集等作为其在静态情形的特例。给出动态系统部件的概率重要度、结构重要度以及关键重要度的概念,用实例对提出的有关概念进行了说明。

关键词:动态系统;可靠性;失效序列;失效丛

中图分类号:O213.2　　文献标识码:A

New Concepts for the Dynamic System Reliability Analysis

JIN Guang

(College of Humanities and Management, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: The traditional reliability concepts aim at static logic, which are no longer satisfy the requirement of the modern complex dynamic system reliability analysis. This article provides a different state space and structural function for describing dynamic system reliability. Then concepts of failure sequence and failure cluster are defined for characterizing dynamic systems' failure mode. They are extensions of the traditional static reliability concepts such as cut set and implication set, which are the special example of the provided concepts. The analog concepts including probability importance degree, structural importance degree and critical importance degree are also put forward. At last the relative concepts are illustrated using a simple example of dynamic system.

Key words: dynamic system; reliability; failure sequence; failure cluster

随着科学技术特别是计算机技术的发展,各种控制和容错技术广泛应用,现代系统越来越复杂,人—机—环境以及系统硬件和软件之间相互作用、相互影响,系统可靠性表现出动态性、非单调性、多态性、相关性和随机性等特征,由此也导致了一些特殊的可靠性问题,如故障安全性、维修有序性(如液位调节系统[12])、隐含相依性结构(如人机故障[10])、状态依赖性(即事件影响与其发生时过程或系统状态及其持续时间有关[11])等。

在动态系统可靠性描述与分析方面,虽然没有必要在所有情况下对影响系统可靠性的所有因素都进行详尽的描述,但是在许多情况下,如果忽略这些因素的影响,或者对所有因素都采用过于简单(如忽略相关性等)的方式进行处理,将导致不可接受的误差。更重要的是,软件、人员等硬件以外的因素对现代系统可靠性的影响越来越大,提供一种可以描述影响系统可靠性的各种因素的方式是非常重要的。传统的系统可靠性建模与分析方法在描述时间、过程和人的因素的影响方面存在困难,在模型精化方面的困难也使得它们在动态系统可靠性设计分析中存在局限性。另外,更根本的是,传统的可靠性分析主要采用割集(单调系统)或蕴含集(非单调系统)的概念描述静态逻辑或静态故障模式,对具有隐含相依性或状态依赖性等特点的系统,不能提供合适的定性概念,也不能准确处理部件对系统可靠性的定量影响。对具有动态随机性故障的容错系统、冗余可修系统、公用资源库系统等采用静态近似处理,经常导致计算的可靠性指标与实际情况相差甚远,不能满足高度复杂的现代系统可靠性分析的需要。所以,针对现代复杂系统可靠性特征,从基本概念、建模方法以及定性定量分析方面提出新的可靠性分析途径,是一项非常有意义的工作,也是系统可靠性理论发展的要求[10]。

* 收稿日期:2003 - 09 - 03

作者简介:金光(1973—),男,讲师,博士。

静态系统可靠性分析是建立在组合函数理论基础之上的,与之对应则有时序函数理论,用于处理输出量与输入变量现在及过去的状态都有关的问题,但是如何将其用于动态系统可靠性分析还需要做进一步研究。Petri 网及其扩展在描述顺序、并发、不对称事件结构等方面具有很强建模能力,并且建立了极其丰富的理论分析体系[4~7],适合于从基本概念、可靠性模型及定性定量分析方法方面建立一套比较完整的动态系统可靠性分析框架。

1　动态系统可靠性基本概念

在系统可靠性分析中,除了关心一个事件组合是否会导致不期望事件的发生以外,对动态系统,确定事件组合如何导致不期望事件的发生(比如控制系统的操作顺序错误会导致严重后果),对指导设计和制定维修方案也是非常有意义的。前者对应于故障树分析中割集和蕴含集的概念,可以采用传统故障树分析方法计算单调或非单调关联故障树的割集和蕴含集 ;对于后者,包括故障树分析在内的传统的可靠性分析没有提供有效的描述。

动态系统可靠性分析与静态系统可靠性分析的最大区别在于,前者不希望事件(如系统失效)的发生可能不仅仅是由基本事件的静态逻辑组合导致的,基本事件对不希望事件的影响可能依赖于其他事件是否发生(如贮备系统)以及发生的时序(如人机系统)等。为此,本文提出‘失效序列’的概念。所谓失效序列,是指在一个(预先给定或缺省的)初始状态(比如‘所有事件都没有发生’)下,一个基本事件序列的时序描述,出现在该事件序列中的事件按时间先后顺序发生,并导致不希望事件的发生。为了给出用失效序列描述动态系统故障模式的形式化描述,首先定义几个符号。

$E=\{e_1,e_2,\cdots,e_n\}$:基本事件集合。这里基本事件可能是部件的故障或修复事件、人员操作、软件处理以及环境激励事件等。

x_i :基本事件 e_i 的状态变量,若 e_i 发生,则 $x_i=1$,否则 $x_i=0$.

X :E 中所有事件的状态构成的状态空间,即 $\forall\, \boldsymbol{x}\in X$ 描述 E 中事件是否发生的状态,而与事件发生的时序无关。

对任一状态向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in X$,其中

$$x_{i_j}=1,\ j=1,2,\cdots,m\ ;\ x_k=0,\ k\in\{1,2,\cdots n\}-\{i_1,i_2,\cdots,i_m\}$$

定义集合 $S(\boldsymbol{x})$为

$$S(\boldsymbol{x})=\{\boldsymbol{x}(\Pi(\{i_1,i_2,\cdots,i_m\}),\Pi(\{1,2,\cdots,n\}-\{i_1,i_2,\cdots,i_m\}))\}$$

其中,$\boldsymbol{x}(\Pi(\{i_1,i_2,\cdots,i_m\}),\Pi(\{1,2,\cdots,n\}-\{i_1,i_2,\cdots,i_m\}))$表示已发生事件是按照排列 $\Pi(\{i_1,i_2,\cdots,i_m\})$的次序发生的,而未发生事件将按 $\Pi(\{1,2,\cdots,n\}-\{i_1,i_2,\cdots,i_m\})$的次序发生。比如 $\Pi(\{i_1,i_2,\cdots,i_m\})=i_1,i_2,\cdots,i_m$ 表示事件按 $e_{i_1},e_{i_2},\cdots,e_{i_m}$ 顺序发生,$\Pi(\{i_1,i_2,\cdots,i_m\})=i_m,\cdots,i_2,i_1$ 表示事件按 $e_{i_m},\cdots,e_{i_2},e_{i_1}$顺序发生。显然 $|S(\boldsymbol{x})|=m!(n-m)!$. 定义状态空间

$$\tilde{X}=\bigcup_{\boldsymbol{x}\in X}S(\boldsymbol{x})=\{(\Pi_i:m)\}_{i=1,2,\cdots,n!,m=0,1,\cdots,n}$$

每个状态$(\Pi_i:m)$的含义为 :Π_i 表示 $\{1,2,\cdots,n\}$的某个排列,m 表示该排列中前 m 个事件发生。显然 $|\tilde{X}|=n\cdot n!+1$. 假设系统状态仅取决于已发生事件发生的顺序,而与未发生事件未来发生的顺序无关。不失一般性,假设系统状态在 $\{0,1\}$取值,则可以定义系统结构函数 $\varphi:\tilde{X}\to\{0,1\}$. 设事件 e_i 发生的概率为 p_i,若$(\Pi_i:m)\in S(\boldsymbol{x})\subset\tilde{X}$,设 $\{i_{m+1},i_{m+2},\cdots,i_n\}=\{1,2,\cdots n\}-\{i_1,i_2,\cdots,i_m\}$,则近似地(准确计算需要事件发生时间的分布和事件发生顺序的约束条件)有

$$P((\Pi_i:m))=\frac{\prod_{k=1}^{m}p_{i_k}\prod_{l=m+1}^{n}(1-p_{i_l})}{m!(n-m)!}$$

对于静态系统,设传统结构函数为 Φ,则对任意$(\Pi_i:m)\in S(\boldsymbol{x})$,都有

$$\varphi((\Pi_i:m))=\Phi(\boldsymbol{x}),P((\Pi_i:m))=\frac{P(\boldsymbol{x})}{m!(n-m)!}$$

所以传统的静态系统可靠性模型可以看做是上述描述在静态情形的特例。

按照假设,还可以定义系统状态空间为 E 中所有事件序列的集合,即设 $A=\{e_{i_1},e_{i_2},\cdots,e_{i_m}\}\in 2^E$, $\Pi(A)$为非空集合 A 中基本事件的排列的集合,定义

$$K=\varnothing\bigcup\bigcup_{A\subseteq E,A\neq\varnothing}\Pi(A)$$

以 $\pi(A)$ 表示 A 中事件的一个排列,定义结构函数 φ' 为:$\forall P=\pi(\{e_{i_1},e_{i_2},\cdots,e_{i_m}\})\in K,\varphi'(P)=\varphi((\Pi_i:m))$. 其中$(\Pi_i:m)\in S(x)$ 且 x 对应于A 中事件的状态变量为1,其余状态变量为0;$(\Pi_i:m)$ 中前 m 个事件的排列顺序与 $\pi(A)$ 相同。于是 φ' 与 φ 是等价的,并且 $|K|=n!\sum_{m=0}^{n}\frac{1}{m!}<|\tilde{X}|$。

采用 $\tilde{X}$ 而不用 K 的好处是状态计数方便,并且基于 $\tilde{X}$ 能够得到一种有效的定量计算方法。为方便,记 $P=(\Pi_i:m)\in S(x)$为 $P=\{A;\pi\}$,其中 A 是已发生事件集合,π 表示已发生事件发生顺序,即 $\pi=\Pi(\{i_1,i_2,\cdots,i_m\})$. 为定义系统的单调性,首先定义 $\tilde{X}$ 上的一个偏序关系如下:$\forall P_1=\{A_1;\pi_1\}$, $P_2=\{A_2;\pi_2\}\in\tilde{X}$,若 $A_1\supseteq A_2$,并且排列 π_1 的开始部分为 π_2,则 $P_1\geqslant P_2$;进一步,若还有 $A_1\supset A_2$,则 $P_1>P_2$.

定义1 称系统 φ 是单调的,如果对任意 $P_1\geqslant P_2$,有 $\varphi(P_1)\geqslant\varphi(P_2)$. 反之称系统是非单调的。

显然,对静态系统,上述定义与传统的概念是一致的。

定义2 称 $P\in\tilde{X}$ 是一个失效序列(failure sequence—FS),若 $\varphi(P)=1$ 称 $P=\{A;\pi\}\in\tilde{X}$ 是一个最小失效序列(minimum failure sequence—MFS),如果对任何 $P'\in\tilde{X},P'<P$,都有 $\varphi(P')=0$。

设 $\Sigma=\bigcup_{x\in\tilde{X}}2^{S(x)}$. $\forall\kappa\in\Sigma$ 称为丛,简记为 $\kappa=\{A;\pi_1,\cdots,\pi_m\}$. 定义 Σ 上的结构函数 $\phi:\Sigma\to\{0,1\}$ 如下:

$$\phi(\kappa)=1-\prod_{(\Pi_i:m)\in\kappa}(1-\varphi(\Pi_i:m)),\forall\kappa\in\Sigma$$

定义3 称 $\kappa\in\Sigma$ 是一个失效丛(failure cluster—FC),若 $\phi(\kappa)=1$ 称 $\kappa=\{A;\pi_1,\cdots,\pi_m\}\in\Sigma$ 是不完全最小失效丛,如果 $\forall P\in\kappa$ 都是最小失效序列,即 κ 是由相同事件构成的最小失效序列的并。称 $\kappa=\{A;\pi_1,\cdots,\pi_m\}\in\Sigma$ 是最小失效丛(minimum failure cluster—MFC),如果 κ 包含所有由集合 A 中元素构成的最小失效序列。

(1)可以将失效序列或失效丛想像成一个顺序发生的导致系统不希望事件的条件事件序列。比如,失效序列$(\{e_1,e_2\};1,2)$可以解释为"在事件 e_1 发生后,如果事件 e_2 发生,则系统不希望事件发生"。基于此,为了使用方便,可以进一步采用类似于条件事件的格式描述失效序列,比如$(\{e_1,e_2\};1,2)$可以表示为 $\{e_1|e_2\}$,$(\{e_1,e_2\};2,1)$表示为 $\{e_2|e_1\}$。进一步,可以用条件事件的格式描述失效丛,比如 $\kappa=(\{e_1,e_2,e_3\});1,2,3\}\cup(\{e_1,e_2,e_3\};1,3,2)$可以表示为 $\{e_1|e_2,e_3\}$,其含义可以解释成"在事件 e_1 发生后,如果事件 e_2、e_3 都发生,则系统不希望事件发生"。

(2)对于单调关联故障树,最小失效丛的定义与最小割集是一致的。也就是说,比如 $C=\{e_1,e_2,\cdots,e_k\}$是一个最小割集,则根据最小割集的定义,$e_1,e_2,\cdots,e_k$ 的任意一个排列是最小失效序列,C 中所有事件的排列的集合是一个最小失效丛。

(3)显然,失效序列的概念也能够描述故障部件修复后对系统状态影响,所以可以描述非单调关联系统的维修有序性。结构函数 φ 的定义已经可以描述某些类型的非单调性,比如静态非单调系统以及不发生事件的影响不依赖于时序的情形。但是失效序列中没有显式的关于"事件未发生"的状态信息,所以对于非单调系统,有时显式提供失效序列导致系统不希望事件发生的初始条件是必要的。

对于失效序列和失效丛的求解,一种方式是建立某种系统可靠性模型,然后模拟事件的顺序并预计该事件序列对系统的影响。但是当系统规模较大时,可能的事件序列是很多的,需要研究有效的模型与求解方法。另外,在静态系统可靠性分析中,常常采用分而治之即模块化算法来降低算法的复杂性。对于故障树模型来说,模块是至少两个底事件的集合,这些事件向上可到达同一逻辑门(称为模块的输出或模块的顶点),且必须经过此门才能到达顶事件。模块没有来自其余部分的输入,也没有与其余部分相重复的事件。所以对于静态系统,模块中底事件对顶事件状态的影响仅与其对模块状态的影响有关,

即具有传递性。对于动态系统,可以根据结构函数 φ 给出类似的定义。仅考虑二元情形,设 $E_0 \subset E$, $\tilde{X}_0$ 是 $\tilde{X}$ 在 E_0 上的限制, φ_0 是 $\tilde{X}_0$ 到 $\{0,1\}$ 上的映射,则 φ_0 也可以认为是事件, $\varphi_0 = 0$ 表示对应事件未发生, $\varphi_0 = 1$ 表示对应事件发生。如果 E_0 对 φ 的影响仅通过 φ_0 是否发生以及发生时序,则称 E_0 是一个模块。设 E_0 是一个模块,则关于失效序列,有如下结论。

命题 1　设 $E_0 = \{e_1, \cdots, e_m\}$. 设 $p' = \{e_{i_1}, e_{i_2}, \cdots, e_{i_l}\}$ 是 φ 定义在 $(E - E_0) \cup \{\varphi_0\}$ 上的一个失效序列, $p_0 = \{e_{j_1}, e_{j_2}, \cdots, e_{j_k}\}$ 是 φ_0 定义在 E_0 上的失效序列,设 $1 \leqslant s \leqslant l$ 使得 $e_{i_s} = \varphi_0$,并且 $1 \leqslant t \leqslant l$ 满足

$$\varphi_0\{e_{j_1}, e_{j_2}, \cdots, e_{j_t}\} = 1, \varphi_0\{e_{j_1}, e_{j_2}, \cdots, e_{j_{t-1}}\} = 0$$

则 $(\{e_{i_1}, e_{i_2}, \cdots, e_{i_{s-1}}\} \sqcup \{e_{j_1}, e_{j_2}, \cdots, e_{j_t}\}) \neq (\{e_{i_{s+1}}, e_{i_{s+2}}, \cdots, e_{i_l}\} \sqcup \{e_{j_{t+1}}, e_{j_{t+2}}, \cdots, e_{j_k}\})$ 都是 φ 定义在 E 上的失效序列。这里 $A_1 \sqcup A_2$ 表示将 A_2 中元素按原来顺序插入到 A_1 元素之间, $A \neq B$ 表示将集合 B 中的元素按原来顺序添加到 A 中元素的后面。

2　重要度

重要度在可靠性工程中是一个重要的概念,对于可靠度分配和系统优化设计、指导运行和维修具有重要意义。传统故障树分析提出了概率重要度、结构重要度、关键重要度和相关割集重要度等概念,这里给出它们在动态系统中的对应概念。为叙述简便,以下仅讨论两状态单调系统。

定义 4　临界状态 :当且仅当某一部件失效,系统即失效,则称系统处于一种临界状态。

定义 5　概率重要度 :部件 e 的概率重要度定义为当且仅当部件 e 失效,系统即失效的概率,或系统处于部件 e 为关键部件状态的概率。

定义 6　结构重要度 :部件 e 的结构重要度定义为以部件 e 失效为临界状态的系统微观状态数 N_e 与除 e 以外的所有部件构成的微观状态数 $N_{\bar{e}} = (n-1)\cdot(n-1)!+1$ 之比。

定义 7　关键重要度 :部件 e 的关键重要度定义为部件 e 的故障变化率导致的系统故障变化率。

这里需要说明的是,虽然表面上定义 4 ~ 7 与其在描述静态系统时是相同的,但是对于动态系统却有不同的内涵。对于静态系统,系统状态仅与当前系统微观状态有关,而与系统的历史状态无关,即无论当前状态是如何达到的,系统状态变化方向是一样的(从这个意义上讲,即使是目前认为属于动态故障树的功能依赖门,在定性描述方面也属于静态逻辑范畴,只是在定量计算时会有很大区别) 对于动态可靠性分析来说,系统状态不仅与当前的微观状态有关,而且与系统的历史状态有关,或者说部件状态变化的时序对系统状态也会产生影响。

关于重要度的计算,由于动态系统与静态系统中部件对系统状态产生影响的机制是不同的,所以不能套用静态系统重要度分析方法。对于静态系统,概率重要度可以解释为 :部件 e 的概率重要度等于部件 e 状态取 1 时顶事件概率和部件 e 状态取 0 时顶事件概率的差。对于动态系统,虽然可以使用相同的解释,但是由于部件 e 状态变化时序对系统状态是有影响的,需要对部件 e 在所有状态变化时序情形下的影响进行计算,得到条件概率重要度,然后对条件概率重要度按每种可能发生的概率求期望。对于 n 部件系统,考虑部件 e 状态变化与其他部件状态变化之间的时序关系,则共有 $C_{n-1}^0 + C_{n-1}^1 + C_{n-1}^2 + \cdots + C_{n-1}^{n-1} = 2^{n-1}$ 种可能,每种可能以 $(x;e)$ 表示,其中 $x \in X$, e 是 x 中最后一个状态变化部件,设在状态 x 下

$$x_{i_j} = 1, j = 1,2,\cdots,m; x_k = 0,\ k \in \{1,2,\cdots n\} - \{i_1, i_2, \cdots, i_m\} - \{e\}$$

为了计算 $(x;e)$ 的概率,一般需要关于事件发生时间的分布。但是在假设事件发生的时间服从指数分布的情况下,如果所有事件在 $[0,T]$ (T 是任意一个大于 0 的实数) 上都是活动的,利用部件不可靠度也可以经过简单的计算得到

$$P(x;e) = \prod_{j=1}^{m} P(e \succ i_j) \prod_{k \in \{1,\cdots,n\} - \{i_1,\cdots,i_m\} - \{e\}} (1 - P(e \succ k))$$

其中 $P(e \succ\!- i)$ 是事件 e 先于 i 发生的概率，并且

$$P(e \succ\!- i) = p_e - \frac{\ln(1-p_e)}{\ln(1-p_e)+\ln(1-p_i)}(p_e + p_i - p_e p_i)$$

其中 p_e 和 p_i 分别是部件 e 和部件 i 的不可靠度。特别地，若 $\forall\, i$ 都有 $p_i = p_e \equiv p$，则

$$P(\boldsymbol{x}\,;e) = q^m \cdot (1-q)^{n-m-1},\ q = \frac{p^2}{2}$$

在每个 $(\boldsymbol{x}\,;e)$ 下计算条件概率重要度后求期望，就得到概率重要度。计算条件概率重要度时，除 e 外的其他部件仍从初始状态开始计算系统在 e 状态为 0 和为 1 时状态变化的概率，而不假定比 e 先失效的部件已经失效。显然，对于静态系统，由于每种可能下的条件概率重要度是相同的，所以利用该方法得到的概率重要度与其在静态处理方法得到的结果是相同的。不过，该方法计算量太大，可以代之而用的一种简单的近似处理方式，即假设部件 e 状态是在初始时刻确定并在此条件下计算，得到条件概率重要度作为近似。对高可靠度系统，由于一个或多个部件失效的概率与所有部件都不失效的概率相比小得多，所以误差可以接受。对于结构重要度和关键重要度，可以根据定义直接计算。

对于静态系统，几种重要度是有密切联系的，比如部件 e 的结构重要度等于所有部件故障概率为 0.5 时该部件的概率重要度。对于动态系统，这种关系可能不再成立，因为此时关于结构函数的分解公式不再存在。另外，对于静态系统的重要度分析，可以采用模块化算法简化有关的计算。对于动态系统可靠性来说，也有如下结论。

命题 2 设 $E_0 \subset E$ 是一个适当定义的子系统，$e \in E_0$. 关于重要度，有如下结论：

(1) 设 e 对于 φ_0 的概率重要度为 I_0^{Pr}，φ_0 对于系统的概率重要度为 I_m^{Pr}，则 e 对于系统的概率重要度为 $I^{Pr} = I_0^{Pr} \cdot I_m^{Pr}$.

(2) 设 e 对于 φ_0 的关键重要度为 I_0^{Cr}，φ_0 对于系统的关键重要度为 I_m^{Cr}，则 e 对于系统的关键重要度为 $I^{Cr} = I_0^{Cr} \cdot I_m^{Cr}$.

证明 对于(1)，根据临界状态的定义知，若 e 处于 φ_0 的临界状态，而 φ_0 处于 φ 的临界状态，则 e 处于 φ 的临界状态，即

$$P\{e \text{ 处于 } \varphi \text{ 的临界状态}\} = P\{e \text{ 处于 } \varphi_0 \text{ 的临界状态，且 } \varphi_0 \text{ 处于 } \varphi \text{ 的临界状态}\}$$

由于给定 ϕ_0 状态后系统状态与 E_0 无关，所以

$$P\{e \text{ 处于 } \varphi \text{ 的临界状态}\} = P\{e \text{ 处于 } \varphi_0 \text{ 的临界状态}\} \times P\{\varphi_0 \text{ 处于 } \varphi \text{ 的临界状态}\}$$

即

$$I^{Pr} = I_0^{Pr} \cdot I_m^{Pr}$$

对于(2)，利用复合函数求导的链式法则，容易证明其正确性。

对于结构重要度，由命题 1 知，没有类似静态系统的简单的计数关系，所以基于模块的结构重要度计算方法，即是否有部件 e 对于系统的结构重要度 I^{St} 等于其对模块 φ_0 的结构重要度 I_0^{St} 与 φ_0 对系统的结构重要度 I_m^{St} 的乘积：$I^{St} = I_0^{St} \cdot I_m^{St}$，还需要进一步研究。

3 实例分析

在某些可靠性要求较高的系统中，往往采用热备件提高系统可靠性。热备件是当系统部件失效后切换到工作状态的部件，并且不论其处于运行或储备状态，失效率都是相同的。设系统由部件 $P1$、$P2$ 和 S 组成，假设工作部件 $P1$ 与 $P2$ 都失效，且 $P1$ 比 $P2$ 先失效时，系统失效。S 是 $P1$ 和 $P2$ 的公用备件，该部件可以代替 $P1$ 和 $P2$ 中的任意一个。采用热备件逻辑门(Hot Spare Pool—HSPP)和优先与门的动态故障树如图 1 所示。

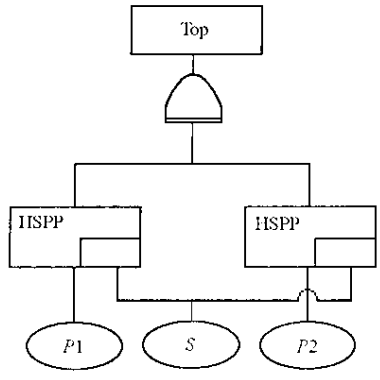

图 1 动态故障树

Fig. 1 A dynamic fault tree

可以枚举系统所有故障模式为 $\{P1, S \mid P2\}$、$\{P2, P1 \mid S\}$。设 $P1$、$P2$ 和 S 的失效概率都为 0.1，则可以计算得到系统不可靠度为 2.22×10^{-4}，若不考虑部件失效顺序的影响，则系统不可靠度为 $1 \times$

10^{-3}，相差 4.5 倍。这说明，对于动态系统，简单采用静态系统的处理方式会导致相当大的误差。表 1 给出了三个部件的概率重要度、结构重要度和关键重要度，其中，动态情形重要度计算采用近似方式处理 静态情形采用三部件并联方式处理，即静态逻辑为“ 系统失效当且仅当所有部件失效 ”。由表 1 看出，如果采用静态近似进行处理，得到的结果是所有部件具有相同的重要度，这与实际情况显然是不一致的。利用本文提出的关于动态系统部件重要度的概念，能够对不同部件的重要程度做出区别。由结果还可以看出，对于动态系统，使用单一的重要度概念不足以刻画部件的重要程度，比如 $P1$ 的结构重要度为 0，并不表明它不重要，因为它的概率重要度是最大的。

表 1　部件的重要度

Tab.1　Importance degree of the components

部　件	概率重要度		结构重要度		关键重要度	
名　称	动态	静态	动态	静态	动态	静态
$P1$	1×10^{-2}	1×10^{-2}	0	1/4	1	1
$P2$	5×10^{-3}	1×10^{-2}	2/5	1/4	1	1
S	5×10^{-3}	1×10^{-2}	2/5	1/4	1	1

4　小 结

由讨论及实例分析可以看出，动态系统与静态系统可靠性分析确实存在不同之处，完全套用静态系统可靠性分析方法或采取静态近似，无法满足动态系统可靠性分析的要求。提出了动态系统可靠性分析的一些新的概念，如何将这些概念用于工程实践，如发动机的潜通路分析、运行状态被用冗余系统的可靠性分析等，还需要进一步研究。作者已经就采用 Petri 网和适当定义的诱导模型，基于 Petri 网可达树分析，得到求解一类动态系统失效路径和失效簇的方法 在动态系统可靠性定量分析方面，也得到了一种优于 Markov 过程分析的序贯破坏法。限于篇幅，在此不便展开讨论。

参 考 文 献：

[1] Murata T. Petri Nets：Properties, Analysis and Applications[J]. Proc. IEEE, 1989, 77(4)：541 – 580.

[2] Liu T S, Chiou S B. The Application of Petri Nets to Failure Analysis[J]. Rel. Eng. Sys. Saf., 1997,57：129 – 142.

[3] Leveson N G, Stolzy J. Safety Analysis Using Petri Nets[J]. IEEE Trans. Soft. Eng., 1987, SE – 13(3)：386 – 397.

[4] Baldan P, Corradini A, Montanari U. Contextual Petri nets, Asymmetric Event Structures and Process[R]. Technical Report, Dipartmento Di Informatica, Universitù di Pisa, October 04, 1999.

[5] Devillers R. The Semantics of Capacities in P/T Nets[J]. Advances in Petri Nets 1989, Lecture Notes in Computer Science, Vol. 424, Springer-Verlag.

[6] Janicki R, Koutny M. Semantics of Inhibitor Nets[J]. Information and Computation, 1995, 123：1 – 16.

[7] Busi N, Pinna G M. Process Semantics for Place/Transition Nets with Inhibitor and Read Arcs[J]. Fundamenta Informaticae, 1999, 40：165 – 199.

[8] Dugan J B, Bavuso S, Boud M. Dynamic Fault Tree Models for Fault Tolerant Computer Systems[J]. IEEE Trans. Rel., 1992, 41(3)：363 – 377.

[9] Fishman G S. A Comparison of Four Monte Carlo Methods for Estimating the Probability of s-t Connectedness[J]. IEEE Trans. Rel., 1986, R – 35(2)：145 – 154.

[10] Labeau P E, Smidts C, Swaminathan S. Dynamic Reliability：towards an Integrated Platform for Probabilistic Risk Assessment[J]. Rel. Eng. Sys. Saf., 2000(68)：219 – 254.

[11] Siu N. Risk Assessment for Dynamic Systems：An Overview[J]. Rel. Eng. Sys. Saf., 1994(43)：43 – 73.

[12] 梅启智，廖炯生，孙惠中. 系统可靠性工程基础[M]. 北京 科学出版社. 1992.