https://doi.org/10.1051/jnwpu/20203840846

基于随机 Petri 网的机载系统动态可靠性建模

庄露, 陆中, 张子文

(南京航空航天大学 民航学院, 江苏 南京 210016)

摘 要:机载系统的可靠性对飞机的安全性有重大影响,现代飞机的机载系统自动化与集成化程度高,导致其失效特性具有显著的动态性,即系统失效不仅取决于单元失效的组合方式,还与单元失效顺序相关。提出了一种基于随机 Petri 网的机载系统的动态可靠性建模方法,针对温储备、冷储备、载荷共担等典型动态结构,构建了随机 Petri 网模型以表征其动态(时序)失效行为。在所构建的随机 Petri 网模型的基础上,提出了基于蒙特卡罗仿真的可靠性分析方法,以用于生成系统寿命样本、进行可靠性参数的计算。最后,以某飞机交流电源系统为例给出了应用实例,结果表明:所提方法与传统解析法的误差在 2×10^{-7} 以内,能够满足工程应用的需要。

关 键 词:机载系统;动态可靠性建模;随机 Petri 网;蒙特卡罗仿真;系统安全性
中图分类号:V240.2 **文献标志码**:A **文章编号**:1000-2758(2020)04-0846-09

现代民用飞机机载系统如飞行控制系统、环境控制系统、动力装置等均是由机械、电子、电气、液压等单元组成的高集成复杂系统,对飞机的安全性有重要影响,美国联邦航空局(Federal Aviation Administration,FAA)与欧洲航空安全局(European Aviation Safety Agency,EASA)在它们各自颁布的咨询材料中均指出,系统故障导致的飞机顶层灾难性失效状态大约在 100 个以上,要远远高于飞机结构失效导致的灾难性失效状态,目前飞机机载系统故障已经成为仅次于人为因素的第二大空难原因。

民用飞机机载系统具有组成单元数量众多、自动化与集成化程度高、各单元间交联关系复杂等特点,由此导致其失效特性具有显著的动态性,即状态依赖行为。静态系统的故障完全由其单元故障的组合决定。而动态系统是否失效不仅取决于单元失效的组合方式,还与单元失效顺序相关[1-2]。如对于三余度的液压系统,如果自测系统(built-in test equipment,BITE)先于主用单元失效,则当主用单元失效时,系统失效;反之,系统仍能正常工作。

故障树分析(fault tree analysis,FTA)、依赖图分析(dependence diagram analysis,DDA)和马尔可夫分析(Markov analysis,MA)是目前应用最广泛的机载系统可靠性建模和安全分析工具。FTA 是一种演绎分析方法,它关注于一个特定的不希望发生的事件,用于确定导致该事件的故障原因并提供了计算该事件发生概率的方法。DDA 等价于可靠性工程中的可靠性框图(reliability block diagram,RBD)法,是描述系统故障逻辑的另一种图示方法。在 MA 中,马尔可夫链被用来表示各种系统状态及其之间的关系。从一种状态到另一种状态的转移率是单元的故障率或修复率。状态发生概率由求解马尔可夫过程对应的微分方程组得到[3-4]。在这 3 种方法中 FTA 和 DDA 都是静态工具,它们不能捕获系统故障机制中的状态依赖行为[5]。虽然 MA 可以处理状态依赖行为,但当系统规模较大且复杂时,它将面临状态空间爆炸问题。此外,马尔可夫链微分方程的求解是一项繁琐的工作,且 MA 只能处理其寿命服从指数分布的情况[6]。

Petri 网作为一种离散事件系统仿真工具,在可靠性工程中得到了广泛的应用[7-11]。Hura 和 Atwood 提出了一种用 Petri 网表示故障树的方法,他们认为这种方法可以更深入地解释系统的故障行为[7]。Malhotra 和 Trivedi 利用随机 Petri 网(stochastic Petri net,SPN)和随机回报网建立可靠性

收稿日期:2019-10-14 **基金项目**:国家自然科学基金(U1733124)及航空科学基金(20180252002)资助
作者简介:庄露(1998—),女,南京航空航天大学硕士研究生,主要从事适航符合性验证及系统安全性评估研究。

模型,并考虑了不同的维修方案[8]。Liu 和 Chiou 使用 Petri 网表示不同类型的逻辑操作,并使用梯形图方法来描述故障场景[9]。Schneeweiss 为多种可靠性场景开发了 Petri 网模型,并在研究中考虑了维护成本和效益[10]。Volovoi 将时效令牌应用于基于 Petri 网的可靠性模型中,并通过与经典可靠性工具的比较,说明了该方法的优越性[11]。Katsigiannis、Georgilakis 和 Tsinarakis 提出了一种基于随机流体 Petri 网的小型孤立电力系统可靠性建模的新方法[12]。Robidoux 等提出了一种将 RBD 模型自动转换成颜色 Petri 网的算法,并验证了该方法的有效性[13]。Wu 等利用故障树和模糊推理 Petri 网建立了太阳能电池组机械系统的可靠性模型,其方法可用于确定故障机理[14]。Chu 等利用广义 SPN 建立了射流管伺服阀的可靠性模型,并与马尔可夫模型进行了比较,说明了该方法的有效性[15]。近年来,Petri 网的应用已经扩展到其他领域的可靠性和安全工程,其中包括综合模块航电设备的可靠性分析[16],多任务分阶段系统的可靠性建模[17],基于模型的安全性分析[18],安全关键实时系统的可靠性分析[19]等等。

Petri 网在可靠性和安全性建模方面显示出强大的能力,本文将提出一种基于 SPN 的动态系统可靠性建模方法,在此基础上提出了一种基于蒙特卡罗仿真的可靠性分析方法用于生成系统寿命样本,以进行系统可靠性参数的计算。最后,结合某型民用飞机交流电源系统给出了应用实例。

1　随机 Petri 网的相关定义

1.1　随机 Petri 网

1 个 SPN 被定义为 1 个七元组:$\sum = (\boldsymbol{P},\boldsymbol{T},\boldsymbol{F},K,W,\boldsymbol{M}_0,\boldsymbol{\Lambda})$,其中[20-21]:

1) $\boldsymbol{P} = \{p_1,p_2,\cdots,p_n\}$ 是库所的有限集合;

2) $\boldsymbol{T} = \{t_1,t_2,\cdots,t_m\}$ 是变迁的有限集合;

3) $\boldsymbol{F} \subseteq (\boldsymbol{P} \times \boldsymbol{T}) \cup (\boldsymbol{T} \times \boldsymbol{P})$ 是弧的有限集合;

4) K: $\boldsymbol{P} \to \{1,2,3,\cdots\}$ 是库所容量函数;

5) W: $\boldsymbol{F} \to \{1,2,3,\cdots\}$ 是权函数;

6) M: $\boldsymbol{P} \to \{0,1,2,\cdots\}$ 是网的标识,且 $\forall p \in \boldsymbol{P}$: $M(p) \leqslant K(p)$,$\boldsymbol{M}_0$ 是初始标识;

7) $\boldsymbol{\Lambda} = \{\lambda_1,\lambda_2,\cdots,\lambda_m\}$ 是变迁引发速率集合,$\lambda_i(i = 1,2,\cdots,m)$ 表示第 i 个变迁的引发速率。

1.2　前置集和后置集

$\forall\ x \in \boldsymbol{P} \cup \boldsymbol{T}$,$x$ 的前置集与后置集分别记为 $\cdot\boldsymbol{x}$ 与 $\boldsymbol{x}\cdot$,定义 $\cdot\boldsymbol{x} = \{y \mid (y \in \boldsymbol{P} \cup \boldsymbol{T}) \cap ((y,x) \in \boldsymbol{F})\}$,$\boldsymbol{x}\cdot = \{y \mid (y \in \boldsymbol{P} \cup \boldsymbol{T}) \cap ((x,y) \in \boldsymbol{F})\}$。

1.3　触发规则

当且仅当满足(1)式时,变迁 $t \in \boldsymbol{T}$ 是使能的

$$\begin{cases} \forall p \in \cdot\boldsymbol{t}:\ M(p) \geqslant W(p,t) \\ \forall p \in \boldsymbol{t}\cdot - \cdot\boldsymbol{t}:\ M(p) + W(t,p) \leqslant K(p) \\ \forall p \in \boldsymbol{t}\cdot \cap \cdot\boldsymbol{t}: \\ \qquad M(p) + W(t,p) - W(p,t) \leqslant K(p) \end{cases} \tag{1}$$

当变迁 t 被触发后,标识将根据(2)式规则进行变化

$$\forall p \in \boldsymbol{P}:\ M'(p) = \begin{cases} M(p) - W(p,t), & p \in \cdot\boldsymbol{t} - \boldsymbol{t}\cdot \\ M(p) + W(p,t), & p \in \boldsymbol{t}\cdot - \cdot\boldsymbol{t} \\ M(p) + W(t,p) - W(p,t), & p \in \cdot\boldsymbol{t} \cap \boldsymbol{t}\cdot \\ M(p), & \text{otherwise} \end{cases} \tag{2}$$

1.4　状态方程

当若干个变迁被触发后,Petri 网的系统标识可根据(3)式所示的状态方程计算求得

$$\boldsymbol{M}' = \boldsymbol{M} + \boldsymbol{C} \times \boldsymbol{U} \tag{3}$$

式中:$\boldsymbol{U} = [U_j]$,$U_j = 0$ 表示变迁 t_j 未被触发;$U_j = 1$ 表示变迁 t_j 已经被触发;$\boldsymbol{C} = [C_{ij}]$ 为关联矩阵,$\boldsymbol{C}_{ij} = W(t_j,p_i) - W(p_i,t_j)$;$\boldsymbol{M}$ 为变迁触发前的系统标识,$\boldsymbol{M}'$ 为变迁触发后的系统标识。

2　基于 SPN 的动态系统可靠性模型

民用飞机机载系统通常由串联系统、并联系统、表决系统、储备系统、载荷共担系统等结构组成。其中串联、并联(热储备)、表决系统属于静态系统,可以用故障树、可靠性框图等典型二元静态方法进行建模。而温储备、冷储备和载荷共担系统是典型的动态系统,在这类系统中,系统失效不仅仅取决于单元失效的组合,还与单元失效的时间顺序密切相关,对于这类系统,传统的二元静态建模方法不再适用。本文将利用 SPN 针对上述动态结构建立相应的可靠性模型。

2.1　基于 SPN 的储备系统可靠性模型

储备系统由 1 个主用单元和 1 个或多个储备单元组成。1 个传感开关机构用于检测主用单元的故

障,并在主用单元发生故障时立即激活储备单元。储备单元可分为 3 种类型,分别是热储备、温储备和冷储备。热储备类似于并联结构,单元在储备状态的故障率与主用状态相等。冷储备系统中,通常认为单元在储备状态不会发生故障。温储备系统中,通常认为单元在储备状态的故障率要远小于其在主用状态的故障率[22]。

基于 SPN 的由 n 个单元组成的温储备系统的可靠性模型如图 1 所示。

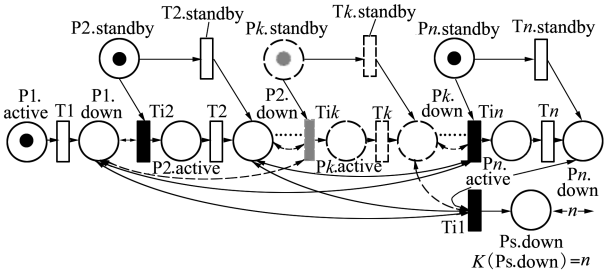

图 1 温储备系统的可靠性模型

图中,Pk.active、Pk.down 和 Pk.standby 分别表示第 k 个单元的主用状态、失效状态和储备状态。它们的容量函数为 1,因此

$$\begin{cases} K(\mathrm{P}k.\mathrm{avtive}) = 1 \\ K(\mathrm{P}k.\mathrm{down}) = 1 \\ K(\mathrm{P}k.\mathrm{standby}) = 1 \end{cases} \quad (k = 1,2,\cdots,n) \tag{4}$$

当有 1 个令牌在 Pk.active、Pk.down 或 Pk.standby 里时,意味着单元 k 分别处于主用、失效、储备状态。库所 Ps.down 表示系统故障状态,其容量函数为 n,即 $K(\mathrm{Ps.down}) = n$。当 Ps.down 内的令牌数为 n 时,系统失效。

时间变迁 Tk 表示第 k 个单元在其主用状态下发生故障,其触发时间等于第 k 个单元的故障前时间。时间变迁 Tk.standby 表示第 k 个单元在储备状态失效,其触发时间等于第 k 个单元在储备状态的故障前时间。变迁 Ti1 到 Tin 为瞬时变迁。每个 Tik 通过一个双箭头弧连接所有的 Pl.down(l<k),这意味着从单元 1 到单元 k−1 的失效是使变迁 Tik 触发的必要条件,库所 Pl.down(l<k) 在被触发之后将仍然有一个令牌。由 Ps.down 出发的弧的权值为 n,其他所有弧的权值为 1。图 2 给出了由 n 个单元组成的冷储备系统基于 SPN 的可靠性模型,在冷储备系统中,库所 Pn.down 就是库所 Ps.down。

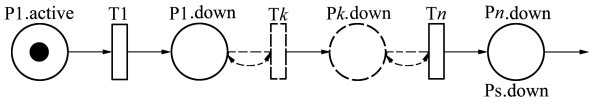

图 2 冷储备系统的可靠性模型

2.2 基于 SPN 的载荷共担系统可靠性模型

在载荷共担系统结构中,单元之间存在依赖关系。如果 1 个单元发生故障,其他单元的故障率会由于负载的增加而升高。基于 SPN 的三单元载荷共担系统结构的可靠性模型如图 3 所示。

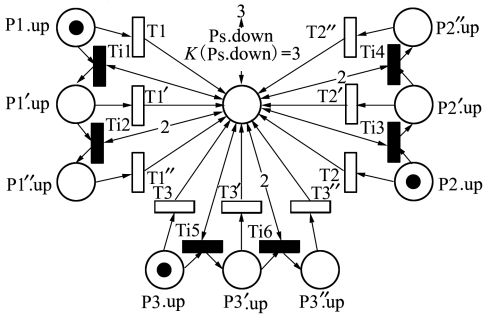

图 3 三单元载荷共担结构的可靠性模型

在图 3 中,Pk.up 为 3 个单元全部正常工作时,第 k 个单元的运行状态。Pk'.up 表示当其他 2 个单元之一失效时,第 k 个单元的状态。Pk''.up 表示当其他 2 个单元都失效时,第 k 个单元的状态。Pk.up,Pk'.up 和 Pk''.up 的容量函数等于 1,即

$$\begin{cases} K(\mathrm{P}k.\mathrm{up}) = 1 \\ K(\mathrm{P}k'.\mathrm{up}) = 1 \\ K(\mathrm{P}k''.\mathrm{up}) = 1 \end{cases} \quad (k = 1,2,3) \tag{5}$$

Ps.down 表示载荷共担系统的失效状态。当且仅当 3 个单元都失效时,载荷共担系统才会失效。因此,当系统失效时,Ps.down 内将有 3 个令牌,Ps.down 的容量函数等于 3,即

$$K(\mathrm{Ps.down}) = 3 \tag{6}$$

Tk 表示当所有 3 个单元都在工作时,第 k 个单元失效。Tk'表示当其他 2 个单元之一失效时,第 k 个单元失效。Tk''表示当其他 2 个单元都失效时,第 k 个单元失效。Tk、Tk'和 Tk''的触发时间等于第 k 个单元分别在全部单元都工作、1 个单元失效、2 个单元都失效的情况下的故障前时间。Ti1 到 Ti6 都是瞬时变迁。由 Ps.down 出发的弧的权值为 n;Ti2 和 Ps.down、Ti4 和 Ps.down、Ti6 和 Ps.down 之间的弧的权值都等于 2;其他所有弧的权值都等于 1。

图 4 在图 3 的基础上进行了简化,给出了两单元载荷共担系统基于 SPN 的可靠性模型。

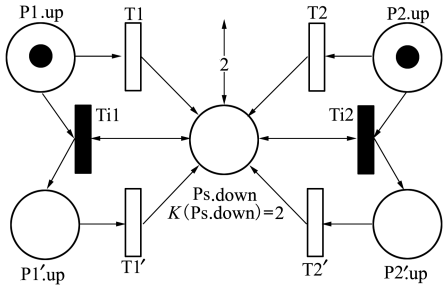

图 4　两单元载荷共担结构的可靠性模型

2.3　基于 SPN 的层次可靠性模型

为大型复杂系统构建基于 Petri 网的可靠性模型是一项繁琐的工作。为简化大型系统的可靠性建模过程,提出了一种基于 Petri 网的层次可靠性模型,可以在一定程度上避免状态空间爆炸问题。在模型中,1 个变迁可以表示 1 个子网,这种变迁称为可替换变迁。因此,1 个大型 Petri 网可以用可替换变迁来表示子网以简化网络结构。本文用正方形来表示可替换变迁。当用可替换变迁表示子网时,应该添加 2 个瞬时变迁,一个连接到库所 Ps.down,另一个连接到初始标记中具有令牌的库所。以图 4 所示的载荷共担结构为例,可替换变迁所表示的子网如图 5 所示。

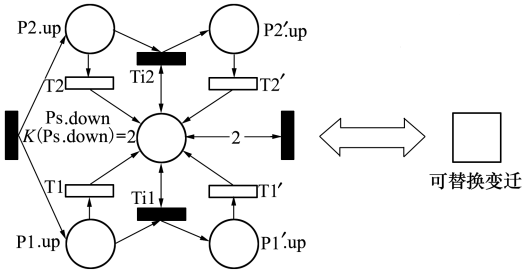

图 5　用可替换变迁表示的载荷共担结构

3　基于 SPN 蒙特卡罗仿真的可靠性评估

本节提出了一种基于 SPN 的蒙特卡罗仿真方法,用于生成系统寿命样本,以进行系统可靠性参数的计算。本算法的基本思想为:用随机数表示 Petri 网模型中各个变迁的触发时间,即相应部件在不同状态下的失效时间;通过触发规则确定哪些变迁会被触发,即哪些部件会在何种状态失效;通过(3)式所示的状态方程确定变迁发生后系统所处的状态,并记录此刻的时间;当系统由初始状态演变到失效状态(Ps.down 中令牌的数量达到其容量函数的值)时,则得到一个寿命样本;多次仿真后可以得到多个寿命样本。通过这些寿命样本进行参数估计与拟合优度检验,求得系统寿命分布,从而可进行可靠性分析与评估。

3.1　基于 SPN 的蒙特卡罗仿真程序

蒙特卡罗仿真流程如图 6 所示。通过一次仿真可以得到系统寿命的一个样本。

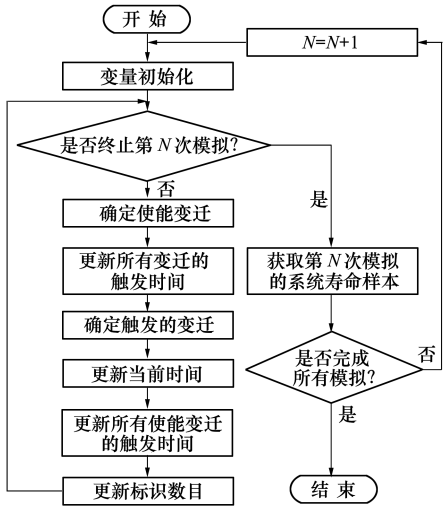

图 6　SPN 的蒙特卡罗仿真步骤

蒙特卡罗仿真的输入项包括:

1) 输入关联矩阵 $\boldsymbol{W}^- = [W(p_i,t_j)]$;

2) 输出关联矩阵 $\boldsymbol{W}^+ = [W(t_j,p_i)]$;

3) 初始标识 $\boldsymbol{M}_0$;

4) 各库所的容量函数 $K(\cdot)$;

5) 变迁的触发速率集 $\boldsymbol{\Lambda} = \{\lambda_1,\lambda_2,\cdots,\lambda_m\}$ 或触发时间分布;

6) 蒙特卡罗仿真的最大次数 $N_{\max}$。

蒙特卡罗仿真的具体步骤如下。

步骤 1　令 $N = 1$,并开始第 N 次仿真。

步骤 2　变量初始化。令 $\boldsymbol{M}_{\text{current}} = \boldsymbol{M}_0$,$\pi_{\text{current}} = 0$,$\pi_j = 0(j = 1,2,\cdots,m)$。式中,$\boldsymbol{M}_{\text{current}}$ 为模型的当前标识,π_{current} 为当前时间,π_j 为变迁 t_j 的触发时间。

步骤 3　决定是否可以终止第 N 次模拟。当 $M(\text{Ps.down}) = K(\text{Ps.down})$,即 Ps.down 中令牌的数量达到其容量函数的值,模拟终止。如果 M(Ps.

down) = K(Ps.down), 前往步骤 10; 否则前往步骤 4。

步骤 4 确定使能变迁。布尔变量 E_j 用于判断变迁 t_j 是否使能。当 $E_j = 1$ 时, t_j 使能; 否则, t_j 非使能。令 $E_j = 0$, 可以通过(1)式确定哪些变迁是使能的。如果 t_j 是使能的, 令 $E_j = 1$。

步骤 5 更新所有变迁的触发时间。对于每个非使能变迁($E_j = 0$), 令其触发时间为 0($\pi_j = 0$)。对于每个使能变迁($E_j = 1$), 如果其初始触发时间为 0($\pi_j = 0$), 则根据其触发速率 λ_j 生成一个随机变量作为其新的触发时间; 否则, 其触发时间不变。

步骤 6 确定触发的变迁。在所有使能的变迁中, 有最小触发时间($\pi_{\min}$) 的变迁将被触发, 如果多个变迁同时具有最小的触发时间, 则随机选择其中一个进行触发。布尔变量 U_j 用于表示变迁 t_j 是否是被触发。如果 U_j 等于 1, 则 t_j 是使能的; 否则, t_j 不是使能的。

步骤 7 更新当前时间 π_{current}。当前时间将更新为 $\pi_{\text{current}} + \pi_{\min}$, 即 $\pi_{\text{current}} = \pi_{\text{current}} + \pi_{\min}$。

步骤 8 更新所有使能变迁的触发时间。所有使能变迁 t_j 的触发时间 π_j 将更新为 $\pi_j - \pi_{\min}$, 即 $\pi_j = \pi_j - \pi_{\min}$。

步骤 9 更新标识数。标识数将由 Petri 网的状态方程进行更新, 即令 $\boldsymbol{M} = \boldsymbol{M} + \boldsymbol{C} \times \boldsymbol{U}$。布尔变量 U_j 为 $\boldsymbol{U}$ 的第 j 个元素。前往步骤 2。

步骤 10 获取系统寿命样本。当前时间 π_{current} 将是系统寿命的一个样本。

步骤 11 确定是否完成所有的仿真。如果 $N = N_{\max}$, 则表示所有模拟都已完成, 程序将结束; 否则, 令 $N = N + 1$, 开始下一次仿真(回到步骤 2)。

3.2 基于系统寿命样本的可靠度计算

威布尔分布是可靠性中常用的失效分布, 可以描述失效率递增、恒定、递减等多种情况下的寿命分布类型, 被广泛应用于各种寿命数据的建模。本节以威布尔分布为例, 说明如何利用寿命样本进行可靠度计算。威布尔分布的可靠度函数为[22]

$$R(t) = \mathrm{e}^{-\left(\frac{t}{\eta}\right)^m} \tag{7}$$

经变换可得

$$\ln\ln\frac{1}{R(t)} = m\ln t - m\ln\eta \tag{8}$$

假设通过 3.1 节得到的 $N_{\max}$ 组有序寿命样本为 $t_1 \leqslant t_2 \leqslant \cdots \leqslant t_{N_{\max}}$, 则在 $t_i (i = 1, 2, \cdots, N_{\max})$ 时刻, 对应的可靠度估计值可表示为 $\hat{R}(t_i) = (N_{\max} - i)/N_{\max}$。将寿命样本及对应的可靠度估计值做如下变换

$$\begin{cases} x_i = \ln t_i \\ y_i = \ln\ln\dfrac{1}{\hat{R}(t_i)} \end{cases} \tag{9}$$

如果 (x_i, y_i) 在普通坐标轴上描点连线后是一条直线, 则说明样本服从威布尔分布。

通过极大似然估计或者最小二乘估计可得参数 η 与 m 的估计值, 再通过 Kolmogorov-Smirnov(K-S) 检验可以判断是否接受该寿命样本服从该分布的假设。

4 实例分析

4.1 系统描述

本节以某飞机交流电源系统为例给出了应用实例。该交流电源系统由主电源、辅助电源与应急电源等部分组成。

主电源是由 2 个发动机分别驱动的 2 个集成驱动发电机(integrated drive generators, IDG), 在飞行中为所有用电设备提供电力。2 个 IDG(GEN1 和 GEN2)都正常时, 两者共同供电, 故障率相同。当其中一个失效时, 另一个可独自为飞机供电, 但其故障率增加。2 个 IDG 为载荷共担关系。主电源失效时, 辅助动力装置(auxiliary power unit, APU)驱动辅助发电机(APU GEN)工作, 它可以取代任意一个 IDG(GEN1 或 GEN2)工作; 且辅助发电机在储备状态时故障率低于工作状态的故障率, 与主电源形成温储备结构。当主电源和辅助电源全部失效时, 使用应急电源; 通常认为应急电源在储备状态下不会发生故障, 即与主电源、辅助电源形成冷储备结构。

4.2 结果及分析

整个交流电源系统的可靠性模型如图 7 所示, 其中 T1 为表示主电源子系统的可替换变迁。其对应的子网如图 5 所示。

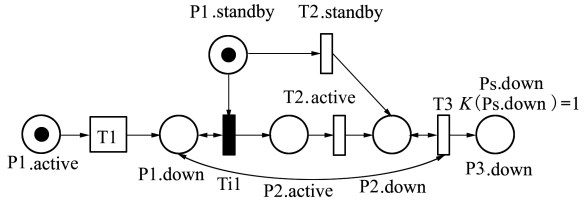

图 7 交流电源系统结构的可靠性模型

交流电源系统各个单元的故障率见表 1。表 1 中,λ_M 为主电源子系统中 2 个 IDG 都正常工作时的故障率。当其中一个 IDG 失效时,另一个 IDG 独自为飞机供电,但其故障率增加,此时的故障率为 λ_M^+。λ_A 为 APU GEN 工作状态下的故障率,λ_A^- 为 APU GEN 在储备状态下的故障率。λ_B 为应急电源的故障率。

表 1　交流电源系统各单元故障率　　h^{-1}

主电源	APU	应急电源
$\lambda_M = 1 \times 10^{-6}$	$\lambda_A = 2 \times 10^{-6}$	$\lambda_B = 1 \times 10^{-7}$
$\lambda_M^+ = 1.5 \times 10^{-6}$	$\lambda_A^- = 0.6 \times 10^{-6}$	

令 $N_{\max} = 1\ 000$,通过蒙特卡罗仿真可以得到该电源系统的 1 000 个寿命样本。由(9)式进行变换后,在普通坐标系描点连线,如图 8 所示,可以看出 x_i 与 y_i 近似满足线性关系,因此可初步确定系统寿命样本服从威布尔分布。

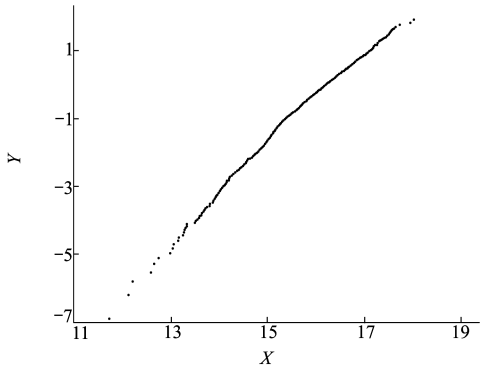

图 8　寿命样本及对应可靠度估计值变换后的线性拟合

采用极大似然估计法拟合两参数威布尔分布表达式,可得形状参数 $m = 1.219\ 1$,尺度参数 $\eta = 1.148\ 2 \times 10^7$。通过 K-S 检验,接受寿命样本符合威布尔分布。

因此,该交流电源系统的可靠度函数的表达式为

$$R(t) = \mathrm{e}^{-\left(\frac{t}{1.148\ 2\times 10^7}\right)^{1.219\ 1}} \tag{10}$$

(10)式给出的可靠度曲线见图 9 中虚线。本实例中单元寿命服从指数分布,且所有故障率均为常数,因此,同可以利用马尔可夫过程求解。该交流电源系统的马尔可夫状态转移图如图 10 所示,图中 M_1,M_2 分别表示主电源的 2 个 IDG 正常,A 表示 APU GEN 正常,B 表示应急电源正常。$\overline{M}_1$,$\overline{M}_2$,$\overline{A}$,$\overline{B}$ 分别表示相应部件失效。根据状态转移图列出的微分方程见(11)式,可靠度函数的解析表达式可表示为 $R(t) = 1 - P_{12}(t)$。由马尔可夫过程解析法求得的可靠性曲线见图 9 中实线。由图 9 可知,本文方法求得结果与马尔可夫过程方法求得结果非常接近。

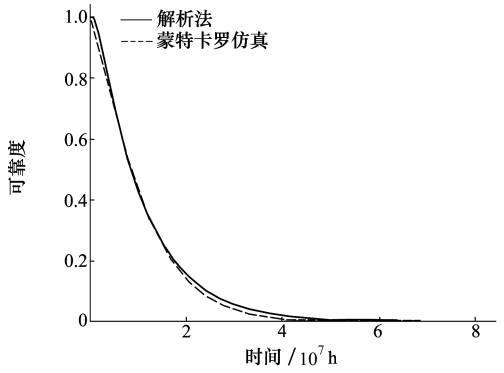

图 9　不同方法得到的交流电源系统的可靠度曲线

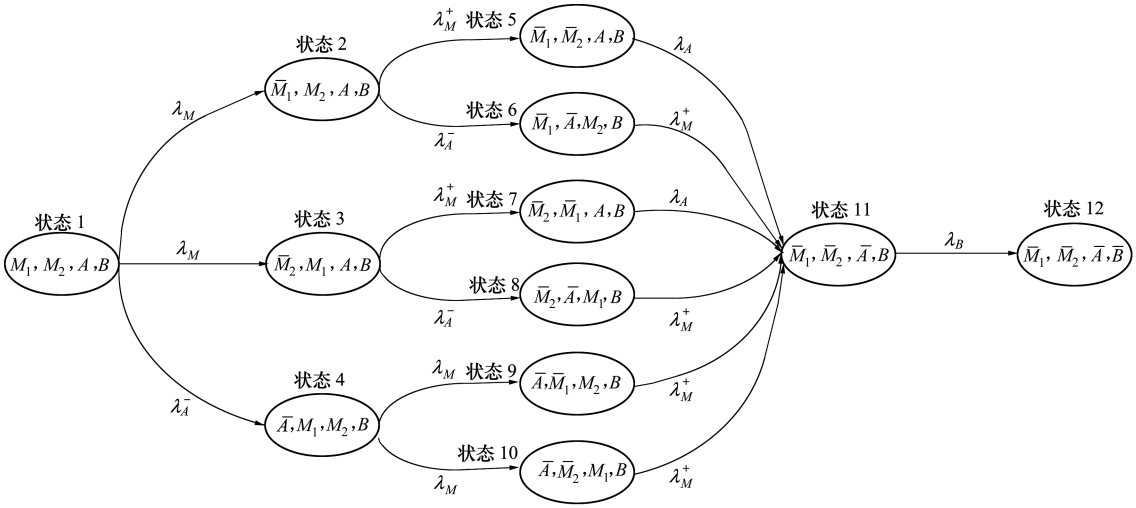

图 10　交流电源系统的马尔可夫状态转移图

图 11 为解析法(马尔可夫过程)求得的可靠度曲线与基于 SPN 的蒙特卡罗数值仿真求得的可靠度曲线之间的误差,误差最大值为 0.045 8。

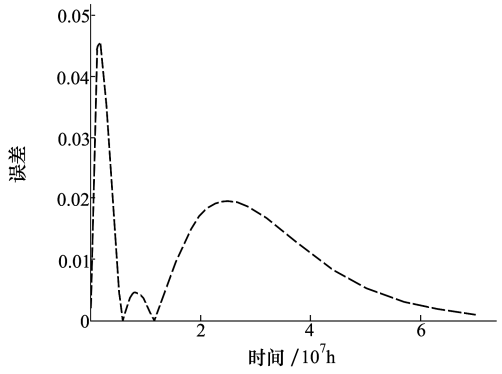

图 11 解析法曲线与蒙特卡罗数值仿真曲线之间的误差

对于民用飞机系统,我们通常关心的是平均航段时间内的任务可靠性,一般民用飞机的平均航段时间从几小时到十几小时不等。取平均航段时间为 15 h,在该时间内,由解析法得到的可靠度曲线和由基于 SPN 的蒙特卡罗数值仿真求得的可靠度曲线如图 12 所示,该时间段内可靠度均大于99.999 9%。

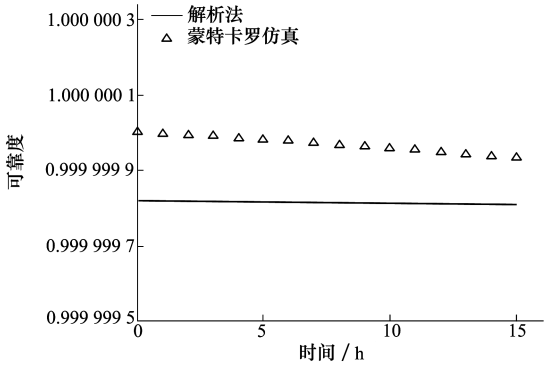

图 12 平均航段时间内交流电源系统的可靠度曲线

在平均航段时间内,解析法求得可靠度曲线与基于 SPN 的蒙特卡罗数值仿真求得可靠度曲线最大误差为 $1.779\ 1\times10^{-7}$,最小误差为$1.212\ 9\times10^{-7}$。

$$\frac{\mathrm{d}P_1(t)}{\mathrm{d}t} = -(\lambda_M + \lambda_M + \lambda_A^-)P_1(t)$$

$$\frac{\mathrm{d}P_2(t)}{\mathrm{d}t} = \lambda_M P_1(t) - (\lambda_M^+ + \lambda_A^-)P_2(t)$$

$$\frac{\mathrm{d}P_3(t)}{\mathrm{d}t} = \lambda_M P_1(t) - (\lambda_M^+ + \lambda_A^-)P_3(t)$$

$$\frac{\mathrm{d}P_4(t)}{\mathrm{d}t} = \lambda_A^- P_1(t) - (\lambda_M + \lambda_M)P_4(t)$$

$$\frac{\mathrm{d}P_5(t)}{\mathrm{d}t} = \lambda_M^+ P_2(t) - \lambda_A P_5(t)$$

$$\frac{\mathrm{d}P_6(t)}{\mathrm{d}t} = \lambda_A^- P_2(t) - \lambda_M^+ P_6(t)$$

$$\frac{\mathrm{d}P_7(t)}{\mathrm{d}t} = \lambda_M^+ P_3(t) - \lambda_A P_7(t)$$

$$\frac{\mathrm{d}P_8(t)}{\mathrm{d}t} = \lambda_A^- P_3(t) - \lambda_M^+ P_8(t)$$

$$\frac{\mathrm{d}P_9(t)}{\mathrm{d}t} = \lambda_M P_4(t) - \lambda_M^+ P_9(t)$$

$$\frac{\mathrm{d}P_{10}(t)}{\mathrm{d}t} = \lambda_M P_4(t) - \lambda_M^+ P_{10}(t)$$

$$\frac{\mathrm{d}P_{11}(t)}{\mathrm{d}t} = \lambda_A P_5(t) + \lambda_M^+ P_6(t) + \lambda_A P_7(t) + \lambda_M^+ P_8(t) + \lambda_M^+ P_9(t) + \lambda_M^+ P_{10}(t) - \lambda_B P_{11}(t)$$

$$P_1(0) = 1,\ P_i(0) = 0(i = 2,3,\cdots,12) \quad (11)$$

本例中,利用前述的冷储备、温储备和载荷共担 3 种结构对交流电源系统进行可靠性建模,克服了传统故障树方法和可靠性框图法无法表征系统失效的时序特性的缺点。同时,本例中各部件的寿命均服从指数分布,可以通过马尔可夫过程进行建模求解;但是,当存在寿命不服从指数分布的部件时,马尔可夫模型无法使用。本文利用 SPN 提出的基于蒙特卡罗仿真的可靠性评估方法则不存在此项缺陷,在已知部件寿命分布的前提下,可以通过生成服从该分布的随机数进行仿真,从而能够求得各种寿命分布类型下的系统可靠性参数。此外,利用马尔可夫过程进行建模时,对于新系统,需要设计人员根据自己经验重新构建马尔可夫模型,对设计人员有较高要求;而利用本文方法建模时,对于新系统,可利用前述的各种基于 SPN 的动态系统可靠性模型进行组合,建模过程简洁方便。

5 结 论

本文针对温储备、冷储备、载荷共担等典型机载系统动态结构,建立了基于 SPN 的可靠性模型。并针对 SPN 可靠性模型,提出了一种蒙特卡罗仿真的可靠性评价方法。与传统可靠性建模工具相比,本

文方法具有以下优点:

1) 与 RBD(DDA)、FTA 等静态可靠性建模工具相比,本文提出的基于 Petri 网的建模方法能够表示失效特征的时序特性,描述系统失效之间的依赖关系;

2) 与 MA 方法相比,基于蒙特卡罗仿真的模拟方法适用于各种寿命分布,克服了马尔可夫模型中所有单元寿命必须服从指数分布的局限性;

3) 对于新系统,利用马尔可夫模型进行可靠性分析需要重新构建新模型,本文只需利用已有的各种动态模型进行组合重构,避免了繁琐的建模过程。同时,本文仿真方法得到的可靠度误差在 2×10^{-7} 以下,能够满足工程需要。

参考文献:

[1] DISTEFANO S, PULIAFITO A. Dependability Evaluation with Dynamic Reliability Block Diagrams and Dynamic Fault Trees [J]. IEEE Trans on Dependable & Secure Computing, 2009, 6(1): 4-17

[2] MERLE G, ROUSSEL J M, LESAGE J J. Algebraic Determination of the Structure Function of Dynamic Fault Trees[J]. Reliability Engineering & System Safety, 2011, 96 (2): 267-277

[3] SAE International S-18 Committee. Guidelines for Development of Civil Aircraft and Systems[S]. ARP4754A, 2010

[4] SAE International S-18 Committee. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne System and Equipment[S]. ARP4761, 1996

[5] RAO K D, GOPIKA V, RAO V V S S, et al. Dynamic Fault Tree Analysis Using Monte Carlo Simulation in Probabilistic Safety Assessment[J]. Reliability Engineering and System Safety, 2017, 94(4): 872-883

[6] LU Z, ZHOU J, LI X. Monte Carlo Simulation Based Time Limited Dispatch Analysis with the Constraint of Dispatch Reliability for Electronic Engine Control Systems[J]. Aerospace Science and Technology, 2018, 72 (1): 397-408

[7] HURA G S, ATWOOD J W. The Use of Petri Nets to Analyze Coherent Fault Trees[J]. IEEE Trans on Reliability, 1988, 37 (5): 469-474

[8] MALHOTRA M, TRIVEDI K S. Dependability Modeling Using Petri-Nets[J]. IEEE Trans on Reliability, 1995, 44(3): 428-440

[9] LIU T S, CHIOU S B. The Application of Petri Nets to Failure Analysis[J]. Reliability Engineering and System Safety, 1997, 57(2): 129-142

[10] SCHNEEWEISS W G. Tutorial: Petri Nets as a Graphical Description Medium for Many Reliability Scenarios[J]. IEEE Trans on Reliability, 2001, 50(2): 159-164

[11] VOLOVOI V. Modeling of System Reliability Petri Nets with Aging Tokens[J]. Reliability Engineering and System Safety, 2004, 84(2): 149-161

[12] KATSIGIANNIS Y, GEORGILAKIS P, TSINARAKIS G. A Novel Colored Fluid Stochastic Petri Net Simulation Model for Reliability Evaluation of Wind/PV/Diesel Small Isolated Power Systems[J]. IEEE Trans on Systems Man and Cybernetics-Part A: Systems and Humans, 2010, 40(6): 1296-1309

[13] ROBIDOUX R, XU H, XING L, et al. Automated Modeling of Dynamic Reliability Block Diagrams Using Colored Petri Nets [J]. IEEE Trans on Systems Man and Cybernetics-Part A: Systems and Humans, 2010, 40(2): 337-351

[14] WU J, YAN S, XIE L. Reliability Analysis Method of a Solar Array by Using Fault Tree Analysis and Fuzzy Reasoning Petri Net [J]. Acta Astronautica, 2011, 69(11): 960-968

[15] CHU Y B, YUAN Z H, CHEN J. Research on Dynamic Reliability of a Jet Pipe Servo Valve Based on Generalized Stochastic Petri Nets[J]. International Journal of Aerospace Engineering, 2015(5): 1-8

[16] WANG Y S, LEI H, HAN X. The Stochastic Petri Net Based Reliability Analysis for Software Partition Integrated Modular Avionics[J]. IEEE Aerospace and Electronic Systems Magazine, 2015, 30(4): 30-37

[17] WU X Y. Mission Reliability Modeling and Evaluation of Multi-Mission Phased Mission System Based on Extended Object-Oriented Petri Net[J]. Eksploatacja i Niezawodnosc-Maintenance and Reliability, 2017, 19 (2): 244-253

[18] WU D H, ZHENG W. Formal Model-Based Quantitative Safety Analysis Using Timed Coloured Petri Nets[J]. Reliability Engineering and System Safety, 2018, 176(8): 62-79

[19] SINGH L K, RAJPUT H. Dependability Analysis of Safety Critical Real-Time Systems by Using Petri Nets[J]. IEEE Trans on Control Systems Technology, 2018, 26(2): 415-426
[20] DAVID R, ALLA P H. Discrete, Continuous, and Hybrid Petri Nets[M]. 2nd Edition, Berlin, Germany: Springer, 2010
[21] LOUCHKA P Z. Time and Petri Net[M]. Berlin, Germany: Springer, 2013
[22] KAPUR K C, PECHT M. Reliability Engineering[M]. New Jersey, USA: John Wiley & Sons, Inc, 2014

Dynamic Reliability Model for Airborne Systems Based on Stochastic Petri Net

ZHUANG Lu, LU Zhong, ZHANG Ziwen
(College of Civil Aviation, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: The reliability of the airborne systems have a significant influence on the safety of aircraft. The modern airborne systems have a high degree of automation and integration, which lead to obvious dynamic failure characteristics. Namely, system failure is not only dependent on the combination of units' failures but also related to their sequence. A dynamic reliability method for modeling airborne systems is proposed based on the stochastic Petri nets. Stochastic Petri nets are applied in reliability modeling for typical dynamic structures including warm standby, cold standby and load sharing, which are widely used in airborne systems. In this way, the dynamic (time-dependent) failure behaviors of the airborne system can be represented. In terms of the stochastic Petri net based reliability model, a reliability analysis method based on Monte Carlo simulation is proposed by generating system life samples for system reliability parameter calculation. Finally, an electrical power system is used as a case to illustrate the application and effectiveness of the present approaches. The results show that the difference by using the present method and the analytical method is below 2×10^{-7}, which can be neglected in practice.

Keywords: airborne systems; dynamic reliability modeling; stochastic Petri nets; Monte Carlo simulation; system safety