复杂系统可靠性

Petri网建模及其智能分析方法

原菊梅◎著

复杂系统可靠性 Petri 网建模及其智能分析方法

原菊梅 著

国防工业出版社

·北京·

图书在版编目(CIP)数据

复杂系统可靠性 Petri 网建模及其智能分析方法/原菊梅著. —北京:国防工业出版社,2011.9

ISBN 978-7-118-07644-8

Ⅰ.①复… Ⅱ.①原… Ⅲ.①Petri 网 Ⅳ.①TP393.12

中国版本图书馆 CIP 数据核字(2011)第 172941 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

天利华印刷装订有限公司印刷

新华书店经售

*

开本 850×1168 1/32 印张 5⅜ 字数 140 千字

2011 年 9 月第 1 版第 1 次印刷 印数 1—3000 册 定价 26.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)68428422 发行邮购:(010)68414474

发行传真:(010)68411535 发行业务:(010)68472764

前　言

由于系统可靠性分析技术的重要性，自20世纪50年代以来，已经形成了许多可靠性模型分析技术和方法，并不断的发展和完善。如故障模式、影响和危害性分析法（FMECA）、可靠性框图法（RG）、故障树分析法（FTA）、事件树分析法（ETA）、运行危险分析方法（HAZOP）、潜通电路分析法（SCA）和Markov模型法等方法。

复杂系统是指通过对一个系统分量部分（子系统）的了解，不能对系统的性质作出完全的解释，即系统的整体性质不等于部分性质之和。这是1999年4月2日美国《科学》杂志出版的《复杂系统》专辑上编者Richand Callagher和Tim Appence的解释。把现有可靠性技术应用于复杂系统可靠性分析中会存在描述能力不足的问题，并且复杂系统可靠性评价不可能采取类似元器件可靠性评价的抽样统计方法。

Petri网是由联邦德国的Carl Adam Petri于1962年在他的博士论文“用自动机通信”中提出，使用网状结构模拟通信系统。Petri网早期的应用主要涉及计算机科学的相关领域，如通信网络的协议验证与分析、操作系统的Petri网描述、分布式数据库系统、实时系统等。近些年来，Petri网的应用渗透到许多新的研究领域，如自动化、机械制造、军事指挥等领域。一个复杂的离散事件系统的动态行为可以通过Petri网清楚地表示，Petri网可以仿真系统的运行过程，分析系统的同步性，描述系统的并发性，通过数学方法证明一个状态的可达性，除了作为建模工具具有以上特性外，还可以用于对系统进行定性的、定量的性能分析。因而为可靠性分析提供了新的思路和方法。目前，在可靠性分析中主要用于可

修系统的可靠性建模与分析、冗余系统的可靠性分析、故障分析等方面。在可靠性工程实践中，Petri 网已被应用于实时控制系统的维修性分析，核电厂保护系统的软件维修性、保障性分析，制造系统的连续故障分析，人造卫星的可靠性建模与仿真等。

本书以 Petri 网为主要建模工具，介绍了一系列新的复杂系统可靠性形式化建模方法及其智能求解算法。全书共 8 章。第 1 章是 Petri 网基本概念及其对典型系统的可靠性建模。首先对 Petri 网的基本概念及其图形表示和分析方法进行了介绍；其次介绍了随机 Petri 网及其分析方法，并就其在可靠性分析中的应用及其他扩展 Petri 网在可靠性分析中的应用进行了综述；最后给出了典型系统的可靠性分析 Petri 网模型。第 2 章是基于模糊 Petri 网的复杂系统可靠性分析。首先讨论了现有模糊 Petri 网对模糊规则的表示及其模糊推理算法；其次分析了可靠性分析中模糊知识库的表示方法；在此基础上介绍了一种适用于复杂系统可靠性估计的模糊神经 Petri 网，并给出一种学习算法；最后介绍了一种收敛速度较快的基于粒子群优化算法的模糊 Petri 网学习方法。第 3 章是基于随机 Petri 网的可修系统可靠性模糊评价。在分析基于模糊数的系统可靠性估计及可修系统可靠性的 $\lambda-\tau$ 理论局限性基础上，把随机 Petri 网中的常数变迁率扩展为模糊数，利用模糊代数运算规则求解由随机 Petri 网得到的状态可达图的稳定状态概率模糊方程组，然后通过解模糊得到系统的可靠性指标；最后就非马尔可夫可修系统的可靠性随机 Petri 网建模进行了讨论，介绍了基于补充变量的非马尔可夫并行系统的可靠性建模方法。第 4 章是基于混合 Petri 网的分布式系统可靠性建模与分析。首先讨论了产品的环境适应性模型建立问题，着重介绍了基于云理论的产品环境适应性模型；然后结合混合 Petri 网的描述能力和部件的环境适应性模型，介绍了考虑环境因素的分布式系统可靠性建模及分析的受控混合随机 Petri 网方法。第 5 章是多状态系统可靠性分析的粗糙 Petri 网方法。首先介绍了一种从知识库中获得系统状态对各部件状态的依赖度和各部件状态对系统状态的重要度并

提取出决策规则的算法;在此基础上定义了带有权重的状态向量范数和状态距离,以此来确定 Petri 网的弧权值和变迁阈值函数;其次给出一种基于粗糙 Petri 网模型的蒙特卡罗仿真算法;最后就属性依赖度问题进行了讨论,介绍了一种基于包含度理论的属性重要性度量方法,并将其应用于软件可靠性多模型综合动态预计中。第 6 章是多任务可重构实时系统可靠性建模与分析。在分析复杂系统可靠性计算基本方法基础上,介绍了基于具有记忆标识的有色 Petri 网分层建模的思想,并给出这种模型的可靠性估计方法;最后就分布式系统的实时性评价问题进行了讨论,介绍了一种时序着色模糊时间 Petri 网,用时序逻辑公式来限制着色 Petri 网的变迁引发行为,用模糊时间来表示各工作过程的时延特性和降级工作问题,通过估计在规定的时间内标识从任务开始状态到达任务完成状态的概率来评价系统的任务实时性。第 7 章是复杂系统可靠性智能分配与优化。介绍了系统可靠性分配原则、常用分配方法和可靠性成本函数,最后将一种改进型粒子群优化算法应用于复杂系统可靠性分配中。第 8 章是软件可靠性综合智能分析方法。首先介绍了软件可靠性的模型组成、基本假设和软件可靠性模型分类,然后介绍了四种典型软件可靠性模型,接着讨论了基于 Kohonen 网络的软件可靠性模型选择方法,最后讨论了软件可靠性多模型综合预测的神经网络方法和基于粒子群优化的自适应方法。

在本书的写作过程中,参考了大量的文献,在此,向这些作者表示衷心的感谢!

由于作者水平有限,书中难免存在不少错误与不妥之处,恳请读者给予批评指正。

作　者

2011 年 1 月

目　录

第 1 章　Petri 网基本概念及其对典型系统的可靠性建模

1.1　Petri 网及其在可靠性分析中的应用

1.1.1　Petri 网基本概念

Petri 网是一种网状信息流模型，包括条件和事件两类节点，在条件和事件为节点的有向二分图的基础上加上表示状态信息的托肯(token)分布，并按一定的引发规则使得事件驱动状态演变，从而反映系统的动态运行过程。通常情况下，用小矩形表示事件节点，称为变迁；用小圆圈表示条件节点，称为库所。两个变迁节点之间和两个库所节点之间不能有有向弧相连，而变迁节点和库所节点之间可以有有向弧连接，由此构成的有向二分图称为网。网的某些库所节点中标上若干个黑点表示托肯，从而构成 Petri 网[1,2]。其形式化描述如下。

定义 1.1　满足下列条件的三元式 $N=(P,T;F)\sum_{i=1}^{n}$ 称为有向网：

(1) $P\cup T\neq\Phi, P\cap T=\Phi$；

(2) $F\subseteq(P\times T)\cup(T\times P)$；

(3) $\mathrm{dom}(F)\cup\mathrm{cod}(F)=P\cup T$。

式中：$\mathrm{dom}(F)=\{x\mid\exists y:(x,y)\in F\}$，$\mathrm{cod}(F)=\{y\mid\exists x:(x,y)\in F\}$ 分别为 F 的定义域和值域。P 和 T 分别称为网 N 的库所(Place)集和变迁(Transition)集，F 为流关系(Flow relation)。

定义 1.2 设 $x \in P \cup T$ 为 N 的任一元素，令 ${}^*x = \{y \mid (y \in P \cup T) \wedge ((y,x) \in F)\}$ 和 $x^* = \{y \mid (y \in P \cup T) \wedge ((x,y) \in F)\}$，称 ${}^*x$ 和 x^* 分别为 x 的前置集和后置集。

定义 1.3 满足下列条件的四元式 PN $= (P, T; F, M_0)$ 称为 Petri 网

(1) $N = (P, T; F)$ 是一个网；

(2) $M: P \to Z$（非负整数集）为标识（也称状态）函数。其中，M_0 是初始标识；

(3) 引发规则：

①变迁 $t \in T$，当 $\forall p \in {}^*t: M(p) \geqslant 1$ 时，称变迁 t 是使能的，记作 $M[t>$；

②在 M 下使能的变迁 t 可以引发，引发后得到后继标识 M'，则

$$M'(p) = \begin{cases} M(p) + 1, & p \in t^* - {}^*t \\ M(p) - 1, & p \in {}^*t - t^*, \\ M(p), & \text{其他} \end{cases} \quad \text{记作 } M[t>M'$$

PN 的标识 M 可以用一个非负整数的 m 维向量表示，记作 M。式中：$M(i) = M(p_i), i = 1, 2, \cdots, m$。

定义 1.4 设 Petri 网 PN $= (P, T; F, M_0)$，M 是 PN 的一个标识，若 $\exists t_1, t_2 \in T$ 使得 $M[t_1> \wedge M[t_2>$，则当

(1) $M[t_1> M_1 \to M_1[t_2> \wedge M[t_2> M_2 \to M_2[t_1>$ 时，称 t_1, t_2 在 M 下并发；

(2) $M[t_1> M_1 \to \neg M_1[t_2> \wedge M[t_2> M_2 \to \neg M_2[t_1>$ 时，称 t_1，t_2 在 M 下冲突。

定义 1.5 设 Petri 网 PN $= (P, T; F, M_0)$，若 $\exists M_1, M_2, \cdots, M_k$，使得 $\forall 1 \leqslant i \leqslant k$，$\exists t_i \in T: M_i[t_i> M_{i+1}$，则称变迁序列 $\sigma = t_1 t_2 \cdots t_k$ 在 M_1 下是使能的，M_{k+1} 从 M_1 是可达，记作 $M_1[\sigma> M_{k+1}$。

定义 1.6　设 Petri 网 PN = $(P,T;F,M_0)$，令 $R(M_0)$ 为满足下列条件的最小集合：

(1) $M_0 \in R(M_0)$；

(2) 若 $M \in R(M_0)$，且 $t \in T$ 使得 $M[t>M'$，则 $M' \in R(M_0)$。则称 $R(M_0)$ 为 Petri 网 PN 的可达标识集合。

Petri 网的状态空间可以用可达树或可达图的形式来表示。

定义 1.7　设 Petri 网 PN = $(P,T;F,M_0)$，若 $M[\sigma>M', M, M' \in R(M_0), \sigma \in T^*]$，则称 $M' = M + CX$ 为 Petri 网 PN 的状态方程。

1.1.2　Petri 网的图形表示[1,2]

Petri 网是一种图形化和形式化的建模工具，为了便于理解，在此给出 1.1.1 中形式化定义的图形表示。设有如图 1－1 所示的简单 Petri 网，则初始标识 $M_0 = [11000]^T$；${}^*t_1 = \{p_1, p_2\}$，$p_4^* = \{t_3\}$ 等；$\forall p \in {}^*t_1 : M_0(p) \geqslant 1$，则 $M_0[t_1>$，记作 $M_0[t_1>M_1$，其中 $M_1 = [00110]^T$，变迁 t_2 和 t_3 在标识 $M_1 = [00110]^T$ 处于并发关系，而变迁 t_4 和 t_5 在标识 $M_3 = [00101]^T$ 处于冲突关系；该 Petri 网的状态可达图如图 1－2 所示，其可达标识集合为 $R(M_0) = \{[11000]^T, [00110]^T, [10010]^T, [00101]^T, [10001]^T, [01100]^T\}$。

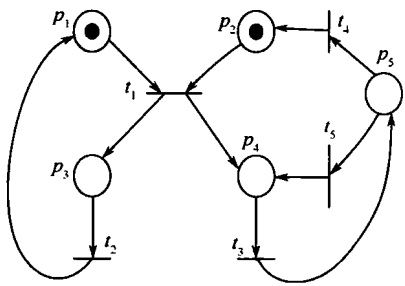

图 1－1　一个简单的 Petri 网

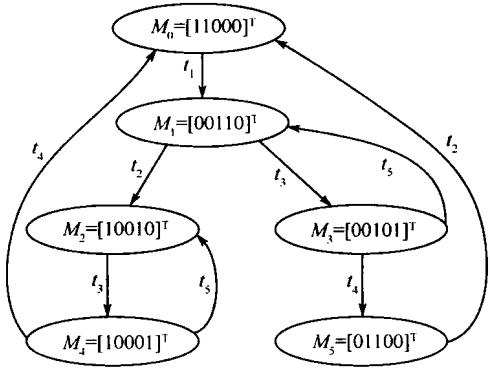

图 1－2　图 1－1 中 Petri 网的状态可达图

1.1.3　Petri 网在可靠性分析中的应用

Petri 网的性质有两大类：动态性质和结构性质。动态性质依赖于网的初始状态，而结构性质与网的初始状态无关，仅仅取决于网的拓扑或结构。Petri 网的性质主要有可达性、有界性、安全性、可覆盖性、可逆性和守恒性等。系统的可靠性分析主要利用 Petri 网的动态性质进行系统的动态行为分析，利用 Petri 网的可达性可以确定在给定的初始状态下，系统是否可能运行到指定状态。利用 Petri 网的活性分析可以确定系统中是否存在死锁问题，从可靠性的角度出发，死锁也是一种故障等。

目前，在可靠性分析中应用较多的是利用 Petri 网的逻辑描述能力代替故障树进行系统的可靠性分析建模。常用的逻辑关系“与、或、非”的 Petri 网表示如图 1－3 所示，从而，可以方便的将故

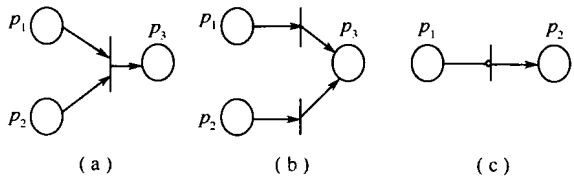

图 1－3　逻辑“与、或、非”的 Petri 网表示

(a)逻辑“与”；(b)逻辑“或”；(c)逻辑“非”。

障树模型转换为相应的 Petri 网模型。故障树的与门采用多输入变迁代替,或门采用多个变迁代替,如此可以很方便地将故障树转变为基本 Petri 网。根据得到的 Petri 网,可以写出关联矩阵,通过关联矩阵,可以快速得到故障树的最小割集[3]。G. S. Hura 等用 Petri 网表示故障树后,利用 Petri 网的可达性及状态方程对系统的动态特性进行了分析,并对故障检测和故障传播方法进行了讨论,证明了 Petri 网是一种比故障树更紧凑的可靠性模型工具[4]。Liu T. S. 等给出了各种复杂故障树关系的 Petri 网表示方法,并利用 Petri 网的简化规则,给出了有效获得最小割集的方法,并通过一个具有 5 层 7 个底事件的故障树实例,说明通过故障树传统方法得到最小割集需要 8 步,而使用 Petri 网方法只需 3 步就可以完成,从而说明 Petri 网是比故障树更加有效的分析工具[5]。金光等在把单调关联系统故障树转化为 Petri 网后,首先构造其逆网,并证明了所得到的逆网是树形网,然后从逆网得到一种求解单调关联系统最小割集的方法[6]。这种方法的定量计算方法与故障树的计算方法相同。

1.2　随机 Petri 网及其在可靠性分析中的应用

进入 20 世纪 80 年代后,由于大型计算机等复杂动态系统性能评估的迫切需要,随机 Petri 网(Stochastic Petri Net,SPN)理论诞生并发展起来。随机 Petri 网最早是由 D. Shadiros 提出(1979,1981),此后许多结合随机过程理论和 Petri 网理论的各具特色的随机 Petri 网被提出,其中 Molloy 提出的理论[1981,1982]影响最大。SPN 的基本思想是:对每一个变迁 t,从其被使能开始到引发的时间是一个连续的随机变量 λ,可以具有不同的分布。用随机 Petri 网对动态系统性能评估、分析和模拟,实质上是给出离散随机过程的一个图形化描述。在 Molloy 提出的随机 Petri 网中,相关于每个变迁的分布函数定义成一个指数分布函数,可以证明,两个变迁在同一时刻实施的概率为零,SPN 的状态可达图同构于一个齐次马尔可夫链,从