(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103823748 A
(43)申请公布日 2014.05.28

(21)申请号 201310153548.5

(22)申请日 2013.04.28

(71)申请人 电子科技大学
地址 610000 四川省成都市高新区(西区)西源大道2006号

(72)发明人 王运盛 雷航 韩炫 张靖

(74)专利代理机构 成都华典专利事务所(普通合伙) 51223
代理人 徐丰 杨保刚

(51)Int.Cl.
G06F 11/36(2006.01)

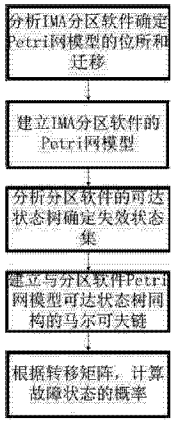
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种基于随机Petri网的分区软件可靠性分析方法

(57)摘要

本发明公开了一种采用随机Petri网(SPN)对综合模块化航空电子系统(IMA)中分区软件的可靠性分析方法。该方法首先参考ARINC653中的分区状态定义,分析并确定分区软件的Petri网的位所和迁移,将“故障状态”作为位所之一,建立IMA分区软件的Petri网模型,进而分析分区软件的可达状态树,确定失效状态集,对变迁的实施速度进行分析,利用SPN的可达状态树可以推导其同构的马尔科夫链(MC),求出稳态分布,系统处于故障状态的稳态概率也就软件发生故障的概率,确定分区软件处在故障状态的稳态概率与内核操作系统的可靠性指标、分区调度周期、系统恢复时间之间的函数关系,从而定量的分析IMA分区软件的可靠性。



CN 103823748 A

1. 一种基于随机 Petri 网的分区软件可靠性分析方法，包括以下步骤：

步骤一：确定 Petri 网模型的位所集 M={M_1, M_2, M_3...M_i}和变迁集 T={T_1, T_2, T_3....T_n}，i 为位所数量，n 变迁数量；

步骤二：根据步骤一变迁集 T 获得各个相关联的实施速率$\lambda=\{\lambda_1,\lambda_2,\lambda_3...\lambda_n\}$；

步骤三：结合子系统的 SPN 模型的可达树，确定子系统的失效状态集；

步骤四：根据所述可达树构造出随机 Petri 网同构的马尔可夫链(MC)；

步骤五：计算稳态下分区软件处于故障状态的概率；

5-1：构造 MC 的 n 阶的转移矩阵 Q=[q_{ij}](1<=i，j<=n)，具体地：在同构的 MC 中，从状态 M_i 到状态 M_j 的转移率 q_{ij}，也就是从状态 M_i 到状态 M_j 的执行比例，如果没有从状态 M_i 到状态 M_j 的弧，则 q_{ij}=0；如果有从状态 M_i 到状态 M_j 的弧，则 q_{ij} 取值等于从状态 M_i 输出的各条弧上标注实施速率λ_i之和的负值；

5-2：根据分区软件 Petri 网模型结合航空电子领域的设计规范和可靠性指标，确定平均无故障工作时间(MTBF)以及相应的实施速率，具体地：操作系统的故障概率与运行操作系统的硬件模块故障率相同，且概率分布服从指数分布：

$$F_x(x)=P_r[X\le x]=1-e^{-\lambda_i x}$$

平均的延时既平均无故障时间(MTBF)为：

$$\bar{d}=\int_0^{\infty}[1-F_x(x)]dx=\int_0^{\infty}e^{-\lambda_i x}dx=\frac{1}{\lambda_i}$$

其中的λ_i也就是变迁 T_i 对应的实施速率；

步骤六：根据步骤五的各项指标以及公式，根据稳态概率由以下线性方程组：

$$\begin{cases} XQ=0 \\ \sum x_i=1,\ 1\le i\le n \end{cases}$$

得出每个可达状态的稳态概率为 P[M_i]=x_i，从而得出系统处于失效状态的稳态概率。

2. 根据权利要求 1 所述基于随机 Petri 网的分区软件可靠性分析方法，其特征为面向综合模块化航空电子系统中的分区软件，定义 IMA 中分区在 Petri 网的位所包含：初始(initial)、空闲(idle)、正常(normal)、等待(waiting)和故障(error)；变迁包含：T1: 初始变迁为空闲，T2: 空闲变迁为正常，T3: 正常变迁为故障，T4: 正常变迁为等待，T5: 等待变迁为正常，T6: 故障变迁为等待，T7: 等待变迁为故障，T8: 错误变迁到空闲，并建立了分区软件的 Petri 网模型。

3. 根据权利要求 2 所述基于随机 Petri 网的分区软件可靠性分析方法，其特征在于：根据分区软件的 Petri 网模型确定系统的失效状态为 M_3，根据同构的 MC 结合航空电子系统中现场可更换单元(LRU)的典型可靠性指标(10^{-5}/ 飞行小时)，确定相关变迁的实施速率，具体地：$\lambda 3=\lambda 7=\lambda=10^{-5}$，分区的周期：t 秒，实施速率是$^1/_t$：$\lambda 4=\lambda 5=1/t$，加载、初始化和启动某个分区的时间时随机变量平均时间：T，相关联的实施速率是：$1/T$；$\lambda 2=\lambda 8=1/T$；根据稳态概率公式可得到各可达状态的稳态概率：

$$\begin{cases} x_0 = 0 \\ x_1 = \dfrac{T\lambda}{2T\lambda + 1} \\ x_2 = \dfrac{(1 + t\lambda)}{(2 + t\lambda) \times (2T\lambda + 1)} \\ x_3 = \dfrac{\lambda}{2T\lambda + 1} \\ x_4 = \dfrac{1}{(2 + t\lambda) \times (2T\lambda + 1)} \end{cases}$$

其中所述失效状态集 M_2 的稳态概率为 $P[M_3]-x_3$。

一种基于随机 Petri 网的分区软件可靠性分析方法

技术领域

[0001] 本发明属于航空电子软件可靠性设计领域，是一种基于随机 Petri 网的 IMA 分区软件可靠性分析方法。

背景技术

[0002] 随着计算机系统使用的日益广泛，信息技术在生活中无处不在，应用软件所提供的服务使的人们越来越依赖它，目前在航空航天、核电技术等许多重要的特殊工程领域中，软件的使用越来越频繁，在这些领域里，软件的故障可能造成巨大的损失，同时目前软件系统的结构越发复杂，功能越来越多，因此软件使用者对可靠性的要求也愈加迫切。

[0003] 软件可靠性是指在规定条件下，在规定的时间内，软件不引起系统失效的概率。

[0004] Petri 网模型就是一种形式化描述模型，着眼于系统中可能发生的各种状态变化及变化之间的关系。Petri 网模型由位所(Place)、变迁(Transition)、弧(Arc)构成。位所用于描述可能的状态，变迁用于描述修改系统状态的事件，弧通过其指向规定了局部状态和事件之间的关系。在 Petri 网模型中，令牌(Token)包含在位所中，它们在位所中的动态变化表示系统的不同状态。

[0005] 一个 Petri 网是一个 5 元的数学模型，即 PN=(P，T，F，W，M_0)，其中：

$P=\{p_1, p_2, \cdots, p_m\}$ 是有限的位所集合，

$T=\{t_1, t_2, \cdots, t_m\}$ 是有限个变迁的集合，

$F \subseteq (P \times T) \cup (T \times P)$ 是有向弧的集合，

$W: F \rightarrow \{1,2,3, \cdots\}$ 是权重的标识，

$M_0: P \rightarrow \{0,1,2,3, \cdots\}$ 是有限的令牌标识，

$P \cap T = \emptyset$ 并且 $P \cup T \neq \emptyset$ P 和 T 非空并且公共元素。

[0006] 标准的 Petri 网 N= (P，T，F，W) 可以简写为 N，给定初始状态的令牌标识的 Petri 网可以表示为(N，M_0)。随机 Petri 网(StochasticPetriNet，SPN)中，与变迁关联的实施速率是服从指数分布的随机变量，表示从变迁触发到开始执行的“延时”，被称为实施速率(fire rate)。如果多个变迁同时触发，系统将执行实施速率最短的变迁。这个与变迁相关的延时，实际上也隐含该变迁相对于其他变迁发生概率。

[0007] 现代航空电子系统采用了综合模块化航空电子系统(Integrated Modular Avionics，IMA)架构，IMA 可以看作是嵌入式系统环境下的集中式分时共用系统，各种驻留功能应用(Hosted Applications，HA)运行在公共计算资源(Common Computing Resources，CCR)板卡上，其基本特点表现为高性能公共处理资源、高速通用数据网络和开放式的软硬件体系结构。按照相关航空电子的行业规范，IMA 中的应用软件需要进行空间和时间隔离，通过采用两级调度和内存管理的“分区技术”(Partitioning)来防止软件之间的相互干扰，从而提供系统的容错能力。分区技术在给系统设计和实现带来方便的同时，也使得软件系统设计工作变得更加复杂。目前与 IMA 相关的软件可靠性分析主要存在以下几个问题：

[0008] 1) IMA 软件组成部分和状态复杂。按照 ARINC653 规范的定义，IMA 软件包括分区软件、内核操作系统、应用程序执行（APEX）接口以及特定系统功能，操作系统、分区软件和应用程序本身均有自己的状态定义。

[0009] 2) 影响软件可靠性的设计因素繁多。IMA 中的软件设计除了软件自身的可靠性问题，还涉及到周期、主时间框架、持续时间、操作系统、故障恢复等众多因素，这些都会直接影响 IMA 中分区软件可靠性。

[0010] 3) 软件相互作用过程复杂。IMA 中的时间和空间隔离由内核操作系统完成，分区软件的创建和初始化需要内核操作系统调度，正常运行后只有在得到处理器资源后才开始执行，这些调度和切换过程可能会发生故障，此外分区软件在发生故障后可以由内核操作系统重新启动进入正常运行状态。这些过程也使得软件的可靠性分析复杂化。

发明内容

[0011] 本发明针对 IMA 软件组成部和状态复杂、相互作用过程复杂的问题，提供了一种基于随机 Petri 网的分区软件可靠性分析方法，主要采用随机 Petri 网对分区软件进行建模和分析，使其克服现有技术的缺陷，可以准确反映操作系统调度等外部事件对分区软件的影响，并定量分析分区软件的可靠性指标与 IMA 其他组成部分可靠性指标和设计考虑因素之间的关系。

[0012] 为了实现上述发明目的，本发明采用以下所述的技术方案：

一种基于随机 Petri 网的分区软件可靠性分析步骤，特征包括以下步骤：

步骤一：确定 Petri 网模型的位所集 $M=\{M_1, M_2, M_3 \ldots M_i\}$ 和变迁集 $T=\{T_1, T_2, T_3 \ldots T_n\}$，i 为位所数量，n 变迁数量；

步骤二：根据步骤一变迁集 T 获得各个相关联的实施速率 $\lambda=\{\lambda_1, \lambda_2, \lambda_3 \ldots \lambda_n\}$；

步骤三：结合子系统的 SPN 模型的可达树，确定子系统的失效状态集；

步骤四：根据所述可达树构造出随机 Petri 网同构的马尔可夫链（MC）；

步骤五：计算稳态下分区软件处于故障状态的概率；

5-1：构造 MC 的 n 阶的转移矩阵 $Q=[q_{ij}]$ $(1<=i, j<=n)$，具体地：在同构的 MC 中，从状态 M_i 到状态 M_j 的转移率 q_{ij}，也就是从状态 M_i 到状态 M_j 的执行比例。如果没有从状态 M_i 到状态 M_j 的弧，则 $q_{ij}=0$；如果有从状态 M_i 到状态 M_j 的弧，则 q_{ij} 取值等于从状态 M_i 输出的各条弧上标注实施速率 λ_i 之和的负值；

5-2：根据分区软件 Petri 网模型结合航空电子领域的设计规范和可靠性指标，确定平均无故障工作时间（MTBF）以及相应的实施速率。具体地：操作系统的故障概率与运行操作系统的硬件模块故障率相同，且概率分布服从指数分布：

$$F_x(x) = P_r[X \le x] = 1 - e^{-\lambda_i x}$$

平均的延时既平均无故障时间（MTBF）为：

$$\bar{d} = \int_0^\infty [1 - F_x(x)]dx = \int_0^\infty e^{-\lambda_i x} dx = \frac{1}{\lambda_i}$$

其中的 λ_i 也就是变迁 T_i 对应的实施速率。

步骤六：根据步骤五的各项指标以及公式，根据稳态概率由以下线性方程组：

$$\begin{cases} XQ = 0 \\ \sum x_i - 1,\ 1 \le i \le n \end{cases}$$

得出每个可达状态的稳态概率为 $P[M_i]=x_i$，从而得出系统处于失效状态 M_3 的稳态概率。

[0013] 基于随机 Petri 网的分区软件可靠性分析方法：所述步骤四中构造 Petri 网 MC 的方法为：将可达树中相同的标识合并，计算每条弧上标注的实施变迁用该变迁的平均实施速率并替换，即得到同构想的有限状态 MC，MC 的状态空间就是 SPN（N,M_0）可达树的状态集合 R（M_0）。

[0014] 基于随机 Petri 网的分区软件可靠性分析方法，其特征为定义 IMA 中分区在 Petri 网的位所包含：初始（initial）、空闲（idle）、正常（normal）、等待（waiting）和故障（error）；变迁包含：T1：初始变迁为空闲，T2：空闲变迁为正常，T3：正常变迁为故障，T4：正常变迁为等待，T5：等待变迁为正常，T6：故障变迁为等待，T7：等待变迁为故障，T8：错误变迁到空闲；所述失效状态集为 M_3。

[0015] 所述基于随机 Petri 网的分区软件可靠性分析方法，其特征在分区软件的 Petri 网模型以及同构的 MC，结合航空电子系统中现场可更换单元（LRU）的典型可靠性指标（10^{-5}/ 飞行小时），确定相关变迁的实施速率，具体地：$\lambda 3 = \lambda 7 = \lambda = 10^{-5}$，分区的周期：t 秒，实施速率是 $1/t$：$\lambda 4 = \lambda 5 = 1/t$，加载、初始化和启动某个分区的时间时随机变量平均时间：T，相关联的实施速率是：$1/T$：$\lambda 2 = \lambda 8 = 1/T$；根据稳态概率公式可得到各可达状态的稳态概率：

$$\begin{cases} x_0 = 0 \\ x_1 = \dfrac{T\lambda}{2T\lambda + 1} \\ x_2 = \dfrac{(1 + t\lambda)}{(2 + t\lambda) \times (2T\lambda + 1)} \\ x_3 = \dfrac{\lambda}{2T\lambda + 1} \\ x_4 = \dfrac{1}{(2 + t\lambda) \times (2T\lambda + 1)} \end{cases}$$

其中所述失效状态集 M_3 的稳态概率为 $P[M_3]-x_3$。

[0016] 使用的 Petri 网的位所和变迁均来在相关标准和规范，贴近真实的 IMA 分区软件的实际运行情况；过 Petri 网建模，将原本复杂的 IMA 中软件相互作用过程清晰化、简单化，使得与分区软件可靠性相关的因素及其作用更加清晰；算分区软件可靠性的相关输入数值均来自实际系统和经验数据，易于获得，并且计算简便；

附图说明

[0017] 图 1 为一种基于随机 Petri 网的分区软件可靠性分析方法流程；

图 2 为分区软件状态（即 Petri 网对应位所）；

图 3 为分区软件的 Petri 网模型；

图 4 为分区软件的可达状态树；

图 5 同构的马尔科夫链；

图 6 为用方程组求出稳态分布及软件发生故障的概率。

具体实施方法

[0018] 所述的一种基于随机 Petri 网的分区软件可靠性分析方法，采用随机 Petri 网对分区软件进行建模和分析，可以准确反映操作系统调度等外部事件对分区软件的影响，并定量分析分区软件的可靠性指标与 IMA 其他组成部分可靠性指标和设计考虑因素之间的关系，具体步骤如下：

1）分析 IMA 分区软件确定 Petri 网模型的位所和迁移

在 ARINC653 定义的分区环境中，驻留应用程序的分区状态包括空闲（IDLE）、正常（NORMAL）、冷启动（COLD_START）、热启动（WARM_START）。其中，空闲状态表示分区的时间和空间资源已经分配，但是驻留的应用程序并不运行；正常状态表示分区资源被占用并且驻留应用程序正常运行；冷启动状态是正在初始化分区和应用程序，分区正在启动；热启动状态表示分区初始化已经完成，应用程序正在启动。

[0019] 为了对方便可靠性分析建模，参考以上的状态，定义 IMA 中分区软件在 Petri 网中的位所，如图 2。为了区分驻留应用启动前后的空闲状态，引入了等待（waiting）位所，则分区在 Petri 网中的位所分别为初始（initial）、空闲（idle）、正常（normal）、等待（waiting）和故障（error），增加了故障（error）位所。其中，初始状态对应于 ARINC653 规范中的冷启动状态，即资源还未分配，分区还未启动；空闲对应于热启动状态和空闲，分区已经启动，但应用程序没有运行；正常状态对应于 ARINC653 规范中的空闲状态；等待状态是在运行过程中分区未获得处理器的时间片，才处于等待；故障状态是运行过程中发生故障而失效。

[0020] 为了更加真实的体现实际软件设计，同时简化 Petri 网模型，对 IMA 中分区的位所的转移路径做了一些假设和限制，如下：

1）分区与操作系统内核、系统特定功能相互独立，分区之间相互独立，各种故障模式相互独立；

2）分区从初始状态开始，经过资源分配和初始化，只能进入空闲状态；

3）空闲状态的分区只能通过驻留应用程序加载和启动进入正常状态；

4）正常状态下的分区不会直接进入空闲状态，只有在故障后才会重新启动分区；

5）在分区发生故障后，只能进入空闲状态重新启动驻留功能软件，进行故障恢复，即故障不会在分区内部自动恢复；

6）不区分冷启动和热启动状态下的分区空闲状态，即驻留应用都要重新初始化。

[0021] 2）建立 IMA 分区软件的 Petri 网模型

按照以上假设条件，可以给出 IMA 中单个分区软件 Petri 网的模型，如图 3 所示。

[0022] 分区变迁和变迁的功能描述如表 1 所示。表中同时说明了执行该变迁的主体，即在 ARINC653 规范中参与变迁的组件，这些组件直接决定了 SPN 网络中与变迁 T_i 相关联的实施速率 λ_i

表 1IMA 中分区变迁表

变迁	描述	实施速率	关联的参考数值
T_1	创建分区，分配资源	λ1	系统初始化延时
T_2	加载应用，启动进程	λ2	分区初始化延时
T_3	系统调用及应用内部错误	λ3	平均无故障时间
T_4	调度分区进入等待时间	λ4	分区周期
T5	调度分区进入运行时间	λ5	分区周期
T6	调度分区进入等待时间	λ6	分区周期
T7	调度分区进入运行时间	λ7	平均无故障时间
T8	重新加载，启动进程	λ8	分区初始化延时

[0023] 3）分析分区软件的状态可达树

结合子系统的SPN模型的可达树，确定子系统的失效状态集。对于单个分区，可以认为在IMA分区Petri网的令牌为1。此时可以得出其对应的系统可达树，如下图4示。在此可达状态树中，状态M3表示系统发生故障，即分区软件的失效状态。

[0024] 4）推导与分区软件Petri网模型可达状态树同构的马尔科夫链

将可达树中相同的标识合并，然后将每条弧上标注的实施变迁用该变迁的平均实施速率替换，即可得到同构的有限状态MC，MC的状态空间就是SPN（N，M_0）可达树的状态集合R（M_0）。分区软件Petri网同构的MC如图5所示。

[0025] 5）确定转移矩阵求解稳态下分区软件处于故障状态的概率

从状态M_i到状态M_j的转移率如图中q_{ij}，也就是从状态M_i到状态M_j的执行比例，

相应的该MC的转移矩阵如下所示。

$$Q=\begin{bmatrix} -\lambda 1 & \lambda 1 & 0 & 0 & 0 \\ 0 & -\lambda 2 & \lambda 2 & 0 & 0 \\ 0 & 0 & -\lambda 4-\lambda 3 & \lambda 3 & \lambda 4 \\ 0 & \lambda 8 & 0 & -\lambda 8-\lambda 6 & \lambda 6 \\ 0 & 0 & \lambda 5 & \lambda 7 & -\lambda 5-\lambda 7 \end{bmatrix}$$

[0026] 令每个可达状态的稳态概率为$P[M_i]=x_i$，稳态概率可以由以下线性方程组确定：

$$\begin{cases} XQ=0 \\ \sum x_i=1,\ 1\le i\le n \end{cases}$$

要求解各可达状态的稳态概率，必须确定转移矩阵Q中与各变迁相关的实施速率。

[0027] 根据航空领域的设计规范和目前航空电子领域的LRU可靠性指标，平均无故障工作时间（MTBF）是100,000小时，即出现故障的概率是10^{-5}/飞行小时。假设操作系统的故障概率与运行操作系统的硬件模块相同，并且概率分布服从指数分布：

$$F_x(x)=P_r[X\le x]=1-e^{-\lambda_i x}$$

平均的延时，既平均无故障时间MTBF可以表示为：

$$\bar{d}=\int_0^\infty [1-F_x(x)]dx=\int_0^\infty e^{-\lambda_i x}dx=\frac{1}{\lambda_i}$$

其中的λ_i也就是变迁 T_i 对应的实施速率。

[0028] 按照航空电子相关的工业规范和当前航空电子设备的可靠性指标，平均无故障时间大约是 100,000 小时，即发生故障的概率是 10^{-5}/ 飞行小时，假设操作系统内核以及驻留应用的故障概率与 LRU 的可靠性指标相同则 T_3 和 T_7 对应的实施速率为：

$$\lambda 3 = \lambda 7 = \lambda = 10^{-5}$$

尽管分区的周期是一个相对固定的值，但是这个值依旧是与硬件执行和上下文相关的随机变量，假设这个事件是 t 秒，，则与 T_4 和 T_5 相关的实施速率是 1/t 即：

$$\lambda 4 = \lambda 5 = 1/t$$

显然，加载、初始化和启动某个分区的时间时随机变量，假定这个事件也符合指数分布，平均时间是 T，则 T_2 和 T_g 相关联的实施速率是：

$$\lambda 2 = \lambda 8 = 1/T$$

根据以上条件解方程组（1）可得各可达状态的稳态概率为：

$$\begin{cases} x_0 = 0 \\ x_1 = \dfrac{T\lambda}{2T\lambda+1} \\ x_2 = \dfrac{(1+t\lambda)}{(2+t\lambda)\times(2T\lambda+1)} \\ x_3 = \dfrac{\lambda}{2T\lambda+1} \\ x_4 = \dfrac{1}{(2+t\lambda)\times(2T\lambda+1)} \end{cases}$$

由此可以计算出不同的初始化时间、不同的周期以及不同的 LRU 可靠性指标下的稳态故障概率 x_2，图 6 所示。

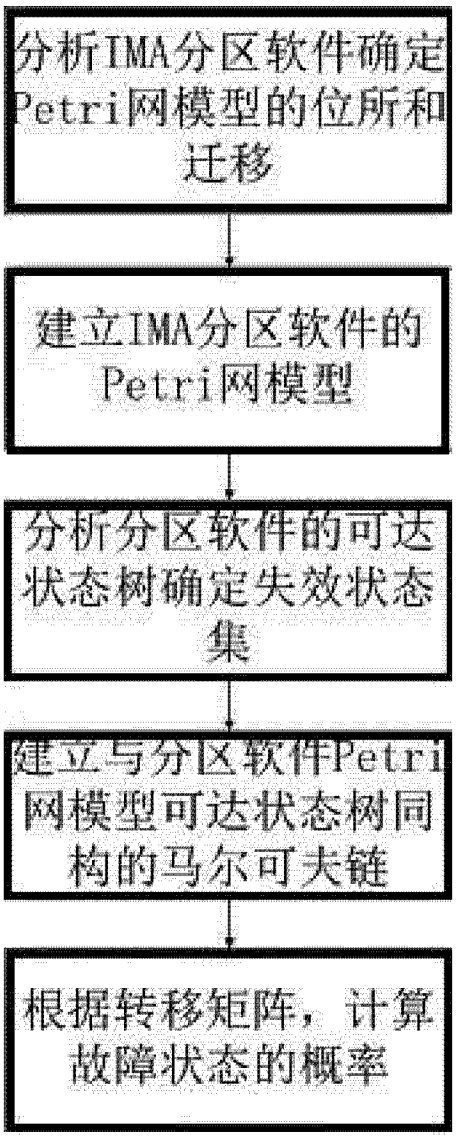

分析IMA分区软件确定Petri网模型的位所和迁移
建立IMA分区软件的Petri网模型
分析分区软件的可达状态树确定失效状态集
建立与分区软件Petri网模型可达状态树同构的马尔可夫链
根据转移矩阵，计算故障状态的概率

图 1

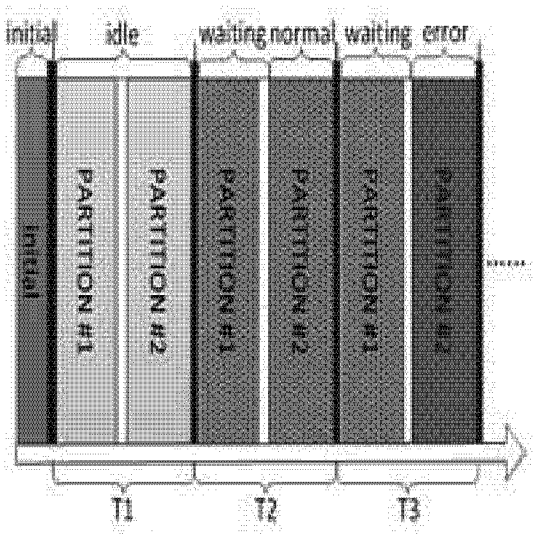

initial
idle
waiting
normal
waiting
error
PARTITION #1
PARTITION #2
PARTITION #1
PARTITION #2
PARTITION #1
PARTITION #2
T1
T2
T3

图 2

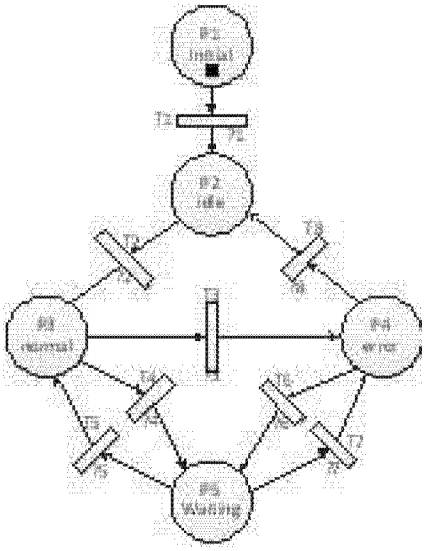


图 3

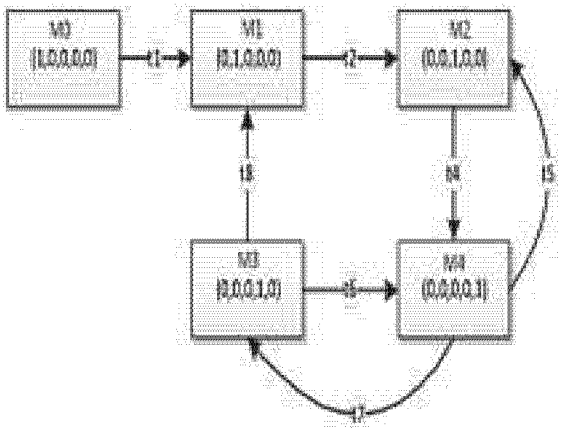

M0
(1,0,0,0,0,0)
t1
M1
(0,1,0,0,0)
t2
M2
(0,0,1,0,0)
t8
t4
t5
M3
(0,0,0,1,0)
t6
M4
(0,0,0,0,1)
t7

图 4

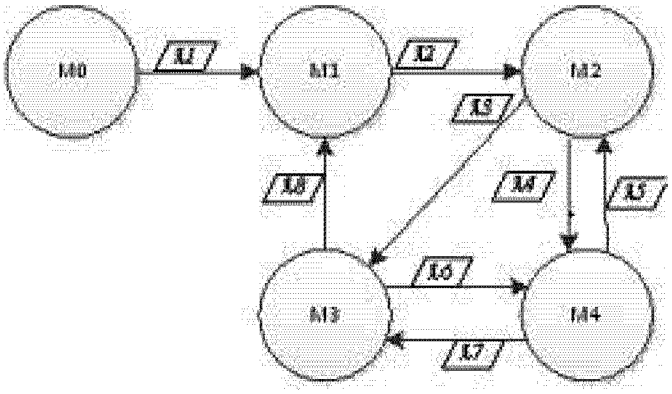

M0
M1
M2
M3
M4
M5
M6
M7
M8

图 5

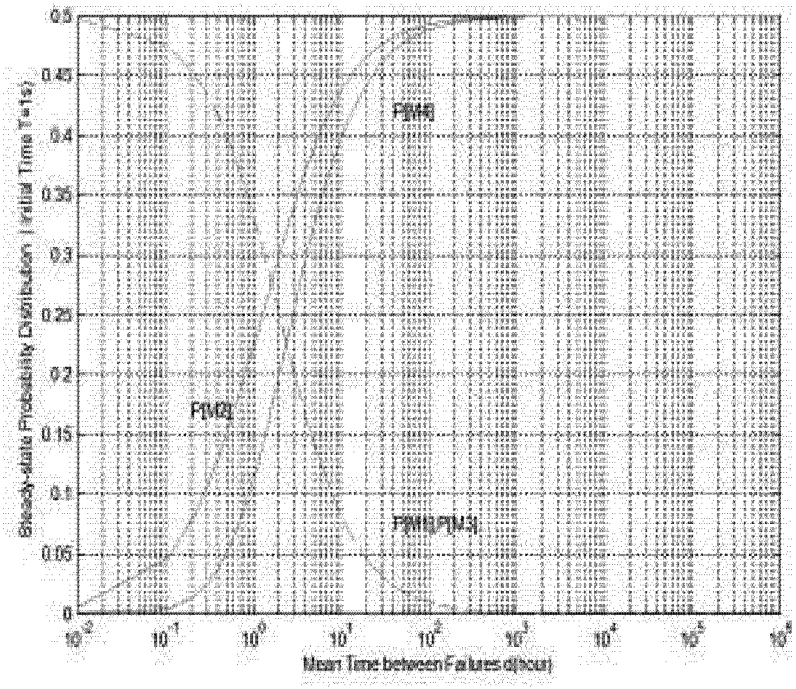

Steady-state Probability Distribution (Initial Time T=1s)
Mean Time between Failures d(hour)

图 6