文章编号: 1001-0920(2005)10-1173-04

基于 Petri 网的非相似余度飞控计算机可靠性分析

秦旭东, 陈宗基
(北京航空航天大学 自动化科学与电气工程学院, 北京 100083)

摘 要: 应用混合 Petri 网建立故障诊断模型, 应用广义随机 Petri 网建立 Boeing 777 非相似余度飞控计算机故障行为模型. 描述了非相似余度系统的结构以及故障的产生和传播的动态过程, 分析了该系统的可靠度和容错度, 并有效地消除了瞬态故障对分析系统可靠性的影响.

关键词: 混合 Petri 网; 广义随机 Petri 网; 非相似余度; 可靠性
中图分类号: TP206.3 **文献标识码**: A

Reliability Analysis of Dissimilar Redundant Flight Control Computers Based on Petri Nets

QIN Xu-dong, CHEN Zong-ji
(School of Automation Science and Electrical Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083, China. Correspondent: QIN Xu-dong, E-mail: qinxudong@buaa.edu.cn)

Abstract: Hybrid Petri nets(HPN) is adopted to develop the model of failure detection and identification(FDI), and generalized stochastic Petri nets(GSPN) is applied to describe and analysis the dissimilar redundant flight control computers of Boeing 777. By using Petri nets, static architectures of the dissimilar redundant system and dynamic behaviors of fault generation and promulgation are properly described. And the effect of transient error on reliability analysis of redundant system can also be eliminated. GSPN model is converted to Markov chain to calculate the reliability of the system, and the incidence matrix is used to compute the ability of fault-tolerance.

Key words: Hybrid Petri nets; Generalized stochastic Petri nets; Dissimilar redundancy; Reliability

1 引 言

在飞控计算机设计的前期, 可靠性建模分析是必要阶段, 有助于设计者从备选的结构方案中挑选出可靠性和结构最为理想的方案[1]. 人们通常采用故障树分析法(FTA)和马尔可夫链等方法确定余度系统的可靠度[2,3]. 但 FTA 方法很难反应出飞控计算机系统的动态特性和余度管理中的排序过程. 马尔可夫链虽然能够建立各种动态系统的模型, 但正确地建立复杂系统的模型非常困难, 也不能准确地描述余度飞控计算机系统的结构, 以及系统内各部分并发等相互关系. 文献[4]应用 Petri 网评价余度系统的可靠性, 但仅使用离散 Petri 网不能有效地消除瞬态故障对系统可靠性的影响, 不能描述连续系统的演变过程.

本文应用混合 Petri 网(HPN)建立了故障诊断(FDI)模型, 应用广义随机 Petri 网(GSPN)建立了 Boeing777 的主飞控计算机的可靠性模型, 应用 GSPN 与马尔可夫链同构性质对系统进行了可靠性计算, 利用 GSPN 的关联矩阵对系统的容错度进行了分析.

2 Petri 网基础

自从德国学者 Petri 于 1962 年提出 Petri 网以来, Petri网已经成为在逻辑层次上对离散事件动态

收稿日期: 2004-10-26; **修回日期**: 2004-12-31.
基金项目: 国家自然科学基金重大研究计划项目(90205011).
作者简介: 秦旭东(1976—), 男, 湖北宜昌人, 博士生, 从事非相似余度飞控计算机及虚拟样机技术研究; 陈宗基(1943—), 男, 上海人, 博士生导师, 从事自适应控制、飞行控制等研究.

系统进行建模和分析的主要方法之一. 近年来, 人们已从不同侧面和不同角度对基本形式的 Petri 网进行了扩展, 导出了不同特点和形式的多种 Petri 网. GSPN 是 Petri 网的扩充, GSPN 中的变迁分为两个子集: 时间变迁集和瞬时变迁集. 瞬时变迁实施延迟为零, 时间变迁的时延参量为按指数分布的随机变量. HPN 是在离散 Petri 网基础上发展形成的, 其位置和变迁区分为连续或离散两种类型, 以表征连续变量过程和离散事件过程.

3 非相似余度飞控计算机系统建模

3.1 Boeing 777 的 3×3 余度主飞控计算机

Boeing 777 主飞控计算机系统(PFC)为非相似 3 余度系统. 系统有 3 个完全相同的数字式主飞控计算机通道, 每个通道有 3 个非相似的支路, 分别采用 AMD 29050, MOTOROLA 68040, INTEL 80486 处理器, 整个 PFC 共使用了 9 个 CPU, 各通道之间采用 ARINC 629 数据总线通讯. PFC 的结构如图 1 所示[5], 3 个支路的硬件接口及其外围电路不相同, 每个支路的软件采用了非相似的编译器, 这就避免了由于使用相同厂家生产的硬件设备和使用相同版本的软件而带来的同态故障.

PFC 和总线被分为左、中、右 3 组. PFC 同时监听 3 组总线, 但只能够向同组的总线传送数据, 当一组的总线出现传送错误或发生故障时, 不会影响另外两组的正常工作. PFC 全部投入工作, 每个 PFC 的 3 个支路被分配为指令支路、备用支路和监控支路. 指令支路将全部作动器控制和系统状态数据传送到它指定的 ARINC 629 总线, 而其他 2 个支路则主要执行监控功能和支路余度管理任务, 一旦指令支路失效, 其任务由备用支路取代. 剩下 2 个支路任意一个再次发生故障都将导致 PFC 输出断开.

3.2 故障诊断的建模

在余度飞控计算机中, 故障的发生是驱动系统状态发生跃变的基本因素, 是研究整个余度飞控系统稳定性的主体. 故障可分为两类: 一类是永久性故障, 另一类是瞬态故障. 瞬态故障的发生率远远大于永久性故障的发生率, 在具有多数表决功能的余度容错系统中, 瞬态故障对系统可靠性的影响大大低于永久性故障对系统可靠性的影响. 有效地区分瞬态故障和永久性故障是提高系统可靠性的有效方法. 在余度计算机运行过程中, 始终启动着故障诊断(FDI). 故障发生后, FDI 在连续 3 个周期中都检测到故障的情况下, 才可判定该故障为永久性故障; 反之判定该故障为瞬态故障. FDI 模块具有如下特征: 一部分是连续的(飞机动力学方程), 另一部分是离散的(故障事件); 一部分是确定的(诊断周期), 另一部分是随机的(故障发生的时间间隔). 因此不能用单一的离散 Petri 网或连续 Petri 网描述.

FDI 模型如图 2 所示. 由 FDI 模型可以看出, 系统有效地消除了瞬态故障的影响. 假定系统出现永久性故障的平均时间间隔为 $1/\lambda$, 则 FDI 模型可以简化为图 3 所示的 GSPN 模型, 其中 T 为服从参数 λ 的指数分布的时间变迁. 在后面的建模中, 可用图 3 所示的简化模型描述单位模块永久性故障的发生.

3.3 Boeing 777 PFC 的建模

777 的 PFC 由并行的多个支路和通道构成, 用 Petri 网对整个系统建模时, 首先是建立单个支路的模型, 而对于多通道的建模则是每个通道内各个支路模型的组合以及通道间的相互关系构成.

每个支路包括 3 个 PCB 模块, 即处理器模块、输入/输出模块和电源模块. 假定每个模块发生故障的时间服从指数分布, 支路的 GSPN 模型如图 4 所示.

Boeing 777 在常规任务期间, 要求 3 个通道都能够正常工作或允许一个通道失效; 在自动着陆时, 允许一个通道失效, 其余两个正常的通道内允许各有一个支路失效[5]. 当 3 个通道有 2 个通道失效时, 认为不能满足飞行任务期间的可靠性要求. PFC 可靠性模型如图 5 所示, 初始时刻左、中、右 3 个通道正常运行, p_1 含有令牌时, 表示系统不能满足飞行任务期间的可靠性. 模型中构造抑制弧的目的是为了

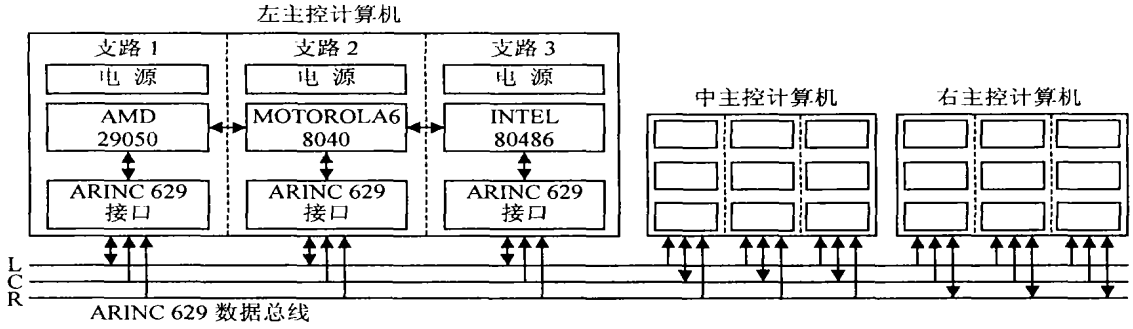

图 1 Boeing 777 主控计算机结构图

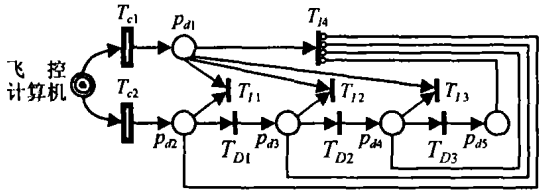

图 2　FDI 的 HPN 模型

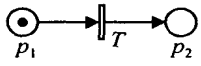

图 3　FDI 的简化模型

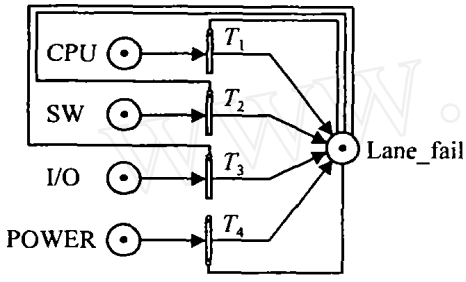

图 4　单支路的 GSPN 模型

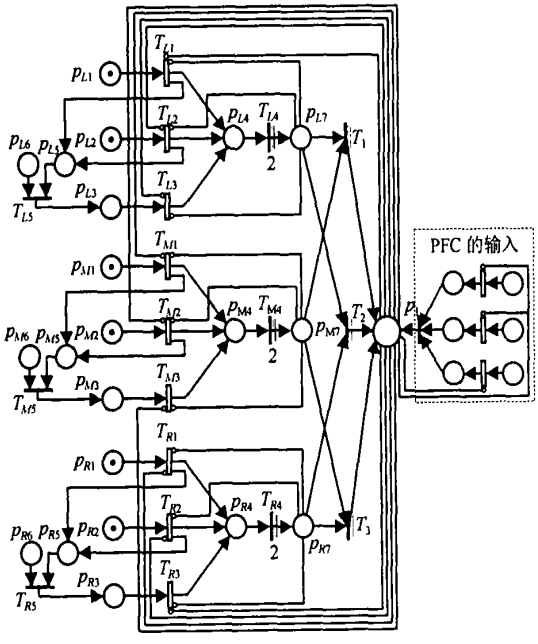

图 5　PFC 故障行为的 GSPN 模型

防止系统失效后, 其他可运行的部件再次发生故障而产生不必要的状态标识, 减少了系统状态的数量, 在与马尔可夫链同构时, 缩短了时间, 减少了存储空间, 从而使可靠性的计算更有效率

4　系统可靠度和容错度的分析

4.1　可靠性分析方法

对于给定的 GSPN 模型, 在初始状态标识 M_0 下按以下步骤可得到其可达集 $P(N, M_0)$:

Step 1: 确定初始标识分布 M_0, 求关联矩阵 D;

Step 2: 在标识分布 $M_k (k = 0, 1, 2\cdots)$ 下, 确定使能变迁序列 X, 由矩阵方程 $M_{k+1} = M_k + XD$ 求出系统新的状态标识 M_{k+1};

Step 3: 判断状态标识 M_{k+1} 下是否使能变迁, 若没有, 系统达到稳态; 否则取 $k = k + 1$, 然后返回 Step 2;

GSPN 和连续时间马尔可夫链是同构的, 可采用同构法对系统的可靠度进行分析. 文献[6] 应用 GSPN 与马尔可夫同构求解了 GSPN 的稳定状态概率. 设 GSPN 的可达集为 R, 按特性可分为两个集合 M_T 和 M_V. 其中: M_T 为显状态, 显状态下不能使能瞬态变迁; M_V 为隐状态, 隐状态下使能瞬态变迁. 系统状态转化过程中, 隐状态不会耗费时间, 因此隐状态可以从可达集 R 中消去, 将它们对系统的影响转移到显状态之间考虑. 对所有的状态进行重新排列, 所有隐状态在前, 显状态在后, 则 GSPN 各状态之间相应的概率转移矩阵为

$$U' = A + B = \begin{bmatrix} P^{VV} & P^{VT} \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ P^{TV} & P^{TT} \end{bmatrix}. \quad (1)$$

式中: 矩阵 A 反映了 GSPN 使能瞬时变迁的情况下, 系统由 M_V 转移到 $M_V (P^{VV})$ 或 $M_T (P^{VT})$ 的转移概率; 矩阵 B 反映了使能时间变迁的情况下, 系统由 M_T 转移到 $M_V (P^{TV})$ 或 $M_T (P^{TT})$ 的转移概率. 系统显状态之间的转移概率矩阵为

$$U = P^{TT} + P^{TV}(I - P^{VV})^{-1}P^{VT}. \quad (2)$$

由 U 可以构造连续时间马尔可夫链的转移速率矩阵, 或称转移密度矩阵. 定义

$$q_{ij} = \begin{cases} \lim\limits_{\Delta t \to 0} \dfrac{u_{ij}(\Delta t)}{\Delta t}, & i \neq j; \\ \lim\limits_{\Delta t \to 0} \dfrac{u_{ij}(\Delta t) - 1}{\Delta t}, & i = j. \end{cases} \quad (3)$$

则称 q_{ij} 为由显状态 M_i 到显状态 M_j 的转移速率, 其中 $i, j \in [1, l], l = |M_T|$. Q 阵是以 q_{ij} 为元素的矩阵.

概率向量 $P(t) = (p_1(t), p_2(t), \cdots, p_l(t))$, 其中 $p_i(t)$ 为系统处于显状态 M_i 的瞬时概率, 则有如下微分方程成立:

$$\begin{cases} P'(t) = P(t)Q, \\ P(0) = [p_1(0), p_2(0), \cdots, p_l(0)]. \end{cases} \quad (4)$$

系统在初始时刻的令牌分布为 M_i 的概率为 $p_i(0)$, 可以由系统的结构以及初始时刻的条件确定, 从而得出 $P(0)$. 求解式(4) 便可得出每个显态的瞬态概率. 若系统状态为 M_f 时系统失效, 其中 $f \in [1, l]$, 则系统的失效概率

$$Q(t) = \sum_{M_f \in M_T} p_f(t),$$

系统的可靠度

$$R(t) = 1 - Q(t) = 1 - \sum_{M_f \subseteq M_T} p_f(t).$$

4.2 容错度分析方法

失效状态集合$M_f = [M_{f1}, \cdots, M_{fk}] \subseteq M_T$, 其中$k = |M_f|$ 模型中所有变迁集合$T = [T_1, T_2, \cdots, T_m]$, 其中$m = |T_t| + |T_i|$ 构造列向量$e = [e_1, e_2, \cdots, e_m]^{\mathrm{T}}$, 其中

$$e_j = \begin{cases} 1, T_j \in T_t; \\ 0, T_j \in T_i \end{cases} \tag{5}$$

引入整数N 表征系统的容错度 下面建立分析余度系统容错度的方法:

Step 1: 求解矩阵方程$M_{fi} = M_0 + X_i D$, $i \in [1, k]$;

Step 2: 计算$N_i = X_i e$;

Step 3: 计算N, $N = \min(N_i - 1)$;

N 的数值越大, 系统的容错度越高 特别的, 当$N = 3$ 时, 系统具有 FO/FO/FS 能力.

4.3 结果分析

假定支路中各部件的故障率如表 1 所示 系统的运行时间为 1 h, 则系统各部分和整个系统的失效概率如表 2 所示 表中分析结果与应用 FTA 分析得出的结果相同, 这表明 Petri 网分析法是对余度飞控计算机系统进行建模和分析的有效方法 以要求两个通道正常工作为准, 计算出 PFC 的容错度N 为 3, 满足 FO/FO/FS 容错准则 如果通道内各支路相同, 当发生同态故障时, 3 个支路同时失效, 此时系统的可靠性会降低到单个支路的级别, 这表明非相似余度技术的应用, 提高了 777 主飞控计算机系统的可靠度和容错度

表 1 系统各部件的故障率

模 块	CPU	I/O	软件	电 源
故障率/(10^{-4}/h)	1.2	1.0	6.0	1.0×10^{-3}

表 2 系统各部分和整个系统的失效概率

系统名称	支 路	通 道	PFC(以要求 2 个通道正常工作为准)
失效概率	8.2×10^{-4}	2.0×10^{-6}	1.2×10^{-11}

5 结 语

本文在建立 Boeing 777 主飞控计算机系统故障行为模型时引入了故障诊断模型, 有效地屏蔽了瞬态故障对分析系统可靠性的影响 提出了应用马尔可夫链与 GSPN 同构的方法来计算余度飞控计算机系统的可靠性, 用关联矩阵的方法分析系统的容错度, 提供了一种适用于余度飞控计算机系统性能评估的通用方法 分析结果表明, 在飞控计算机中引入非相似余度技术, 使系统的失效概率得到了很大程度的降低.

参考文献(References)

[1] Huszerl G, Majzik I. Modeling and Analysis of Redundancy Management in Distributed Object-oriented Systems by Using UML Statecharts [A]. *Euromicro Conf Proc 27th* [C]. Budapest, 2001: 200-207.

[2] 胡谋. *计算机容错技术*[M]. 北京: 中国铁道出版社, 1995.
(Hu M. *Computer Fault Tolerant Techniques* [M]. Beijing: China Railway Publishing House, 1995.)

[3] Yao Y P, Cheng M H. The Application on Dynamic Fault tree Analysis for Dissimilar Fault-tolerant Flight Control System [A]. *AIAA/IEEE Digital Avionics Systems Conf Proc* [C]. St Louis, MO, 1999, 1: 3.B.1-1-3.B.1-6.

[4] Ereau J F. Petri Nets for the Evaluation of Redundant Systems [J]. *Reliability Engineering & System Safety*, 1997, 55(2): 95-104.

[5] Yeh Y C. Triple — Triple Redundant 777 Primary Flight Computer [A]. *Aerospace Applications Conf* [C]. Aspen, Co, 1996, (1): 293-307.

[6] 林闯. *计算机网络和计算机系统的性能评价*[M]. 北京: 清华大学出版社, 2001.
(Lin C. *Computer Network and Computer System Performance Evaluation* [M]. Beijing: Tsinghua University Press, 2001.)

下 期 要 目