# 带马尔可夫参数容错控制系统的可靠性分析

高 飞 张洪钺

(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**: 带马尔可夫参数的容错控制系统 (FTCSMP, Fault Tolerant Control System with Markovian Parameters)作为一种描述主动容错控制系统 (AFTCS, Active Fault Tolerant Control System)的模型,在一些文献中被用于系统稳定性分析. 然而很少有文章研究 FTCSMP的可靠性问题. 以故障检测与隔离 (FDI, Fault Detection and Isolation)装置监视下的冗余传感器组为研究对象,建立了其 FTCSMP模型,进而研究该传感器/FDI装置的可靠性. 在该模型中,用 2个定义在不同状态空间中的齐次马尔可夫随机过程分别表示系统元件的故障过程和 FDI装置的决策过程. 基于马尔可夫理论,研究了传感器/FDI装置的可靠性和安全性. 当 FTCSMP中的系统故障过程和 FDI过程为生灭过程时,将故障检测延迟时间分为"有效"和"无效"2种类型,分析了这 2种延时对传感器/FDI装置可靠性、安全性的影响. 以双余度惯导系统为例,给出了仿真例子.

**关 键 词**: 故障检测; 控制系统分析; 可靠性; 延迟; 冗余; 传感器

**中图分类号**: TP 202$^{+}$. 1

**文献标识码**: A **文 章 编 号**: 1001-5965(2007)03-0302-05

## Reliability of fault tolerant control system with Markovian parameters

Gao Fei Zhang Hongyue

(School of Automation Science and Electrical Engineering, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract: Fault tolerant control system with Markovian parameters (FTCSMP), as a model of active fault tolerant control system (AFTCS), was used to analyze the system stability in several papers. However, little research was on the reliability of FTCSMP. FTCSMP model was used to evaluate the reliability of redundant sensors monitored by fault detection and isolation (FDI). In this model, two homogeneous Markov stochastic processes with different state spaces were defined: one represented system components failures and the other represented the decisions of the FDI process. Based on Markov theory, the reliability and safety of the sensor/FDI unit were studied. When system fault process and FDI process of FTCSMP were both birth and death process, fault detection delay was divided into two kinds: effective and ineffective. The influence of both kinds of delay to the unit reliability and safety was analyzed. A numerical example of dual redundant inertial navigation system was given to show the usefulness of the proposed theoretical results.

Key words: error detection; control system analysis; reliability; delay; redundancy; sensor

主动容错控制系统 (AFTCS, Active Fault Tolerant Control System)的控制方式是用故障检测与隔离 (FDI, Fault Detection and Isolation)装置监视整个系统,如果检测到系统发生了故障,就根据所判断出的故障类型重构控制律,以保证系统的性能. 现代容错技术大量使用冗余技术来提高可靠性,但同时也对 FDI的性能提出了更高的要求. 因此在 AFTCS中, FDI具有十分重要的作用. 选择哪类 FDI装置,如何确定 FDI装置的具体参数等都是系统设计时必须解决的问题.

为了准确地描述 AFTCS, R. Srichander和 B. K Walker在 1993年提出了一类系统模型带马尔

**收稿日期**: 2006-04-03

**基金支持**: 自然科学基金资助项目 (60572185); 自然科学基金重点资助项目 (60234010); 航天科技创新基金资助项目

**作者简介**: 高 飞 (1976 - ),男,内蒙古包头人,博士生, gaofei_nas@21cn. com.

可夫参数的容错控制系统 (FTCSMP, Fault Tolerant Control Systems with Markovian Parameters)[1]. 文献[2]研究了环境噪声对 FTCSMP性能的影响. 文献[3]研究了 FDI检测延迟、误警和漏检对系统的影响. 文献[4]用 FTCSMP模型对延时系统进行了稳定性分析. 然而当前对 FTCSMP模型的研究都集中于对其稳定性的分析,并没有扩展到其它方面. 现有的对 AFTCS的可靠性分析往往将 FDI假设为一个可靠性元件或仅考虑 FDI的误警率和漏检率[5],无法充分反应出 FDI动态特性. 可靠性分析依赖于系统可靠性模型,与系统动态模型不同,这一特点也决定了在现有工作中,系统的可靠性分析与稳定性分析是分开进行的,不能完全同步设计.

本文的目标是利用 FTCSMP模型,对 AFTCS的可靠性进行分析,进而研究 FDI检测延迟时间对系统可靠性的影响,将 FTCSMP的应用从稳定性分析扩展到可靠性分析.

## 1　FTCSMP的定义

现实世界的控制系统中故障发生的时间、位置、幅值大小都具有随机性,可以使用随机过程来描述故障过程. 同样,系统可以有多种故障状态,故障诊断装置能否发现系统发生了故障以及能否判断出系统处于哪种故障状态也是随机的,它的决策过程也可以看作一个随机过程. 因此在 FTCSMP中用一个随机过程 $\eta(t)$来表示系统的发生故障和从故障中自动恢复工作的过程,用另外一个随机过程 $\psi(t)$表示 FDI决策过程.

定义 $\eta(t)$的状态空间为 $S=\{1, 2, \cdots, s\}$. 该空间共有 $s$个离散状态,表示系统正常状态和所有可能的故障状态,用"1"表示系统处于正常状态. 状态间转移的概率可表示为[2]

$$\left.\begin{aligned} p_{ij}(\mathrm{d}t) &= \alpha_{ij}\mathrm{d}t + o(\mathrm{d}t) && i \neq j \\ p_{ii}(\mathrm{d}t) &= 1 + \alpha_{ii}(\mathrm{d}t) + o(\mathrm{d}t) && i = j \end{aligned}\right\} \quad (1)$$

式中,$p_{ij}(\mathrm{d}t)$表示系统在 $\mathrm{d}t$时间内,由状态 $i$转移到状态 $j$的概率; $o(\mathrm{d}t)$表示 $\mathrm{d}t$的二阶及二阶以上无穷小项的总和;

$$\alpha_{ii} = -\sum_{j\neq i,\, j=1}^{s} \alpha_{ij} \qquad i, j \in S \quad (2)$$

定义 $\eta(t)$的转移率矩阵为

$$\Pi = [\alpha_{ij}]_{i,\, j=1,\, 2,\, \cdots,\, s} \quad (3)$$

定义 $\psi(t)$的状态空间为 $R=\{1, 2, \cdots, r\}$,该空间共有 $r$个离散状态,表示 FDI装置判断当前系统所处于的可能状态 (正常状态或某一种故障状态)的集合. 本文假设 $R=S$,因此 $r=s$ $\psi(t)$当前处于哪个状态,就表示 FDI装置判断当前系统处于哪个状态. 因为 FDI的决策过程与当前系统实际所处的状态密切相关,因此用条件概率来表示 FDI状态转移的概率. 在系统实际状态为 $k$的情况下, FDI状态转移的概率可表示为[2]

$$\left.\begin{aligned} p_{ij}^{k}(\mathrm{d}t) &= q_{ij}^{k}\mathrm{d}t + o(\mathrm{d}t) && i \neq j \\ p_{ii}^{k}(\mathrm{d}t) &= 1 + q_{ii}^{k}\mathrm{d}t + o(\mathrm{d}t) && i = j \end{aligned}\right\} \quad (4)$$

式中,$p_{ij}^{k}(\mathrm{d}t)$为系统实际处于状态 $k$的情况下,在 $\mathrm{d}t$时间内,$\psi(t)$由状态 $i$转移到状态 $j$的概率;

$$q_{ii}^{k} = -\sum_{j\neq i,\, j=1}^{r} q_{ij}^{k} \qquad i, j \in R,\ k \in S \quad (5)$$

定义 $\psi(t)$的转移率矩阵为

$$\Theta_k = [q_{ij}^{k}]_{i,\, j=1,\, 2,\, \cdots r} \qquad i, j \in R,\ k \in S \quad (6)$$

系统的实际运行过程,就是发生故障的过程以及从故障中恢复正常的过程,即 $\eta(t)$在集合 $S$中跳变的过程, FDI的决策过程就是 $\psi(t)$在集合 $R$中跳变的过程. 如果 $\psi(t)$状态的变化与 $\eta(t)$状态的变化一致并且同步,那么 FDI装置就可以准确、快速地检测出系统的故障;而实际上,由于噪声、模型不确定、传输延时等因素的影响, FDI过程不可避免地存在漏检、误警、检测滞后等现象,即 $\psi(t) \neq \eta(t)$.

系统正常情况下, FDI装置做出"系统故障"的判断的概率,即误检率为

$$P_{\mathrm{F}} = \sum_{i=2}^{r} P(\psi(t) = i \mid \eta(t) = 1) \quad (7)$$

系统故障情况下, FDI装置做出"系统正常"的判断的概率,即漏检率为

$$P_{\mathrm{M}} = \frac{\sum_{i=2}^{s} P(\psi(t) = 1) \mid \eta(t) = i)\, P(\eta(t) = i)}{\sum_{j=2}^{s} P(\eta(t) = j)} \quad (8)$$

## 2　可靠性分析

首先给出可靠性和安全性的定义[6]:

可靠性:系统输出是正确的概率.

安全性:系统输出是正确的,或者输出中的错误是可检测的概率.

本文考虑功能相同的传感器冗余安装组成传感器组,使用 FDI监视传感器组模块,进行故障诊断,隔离故障的传感器,保证输出数据的正确性. 文中假设同一时刻不会同时发生多个传感器故障,传感器组处在第 $i$种状态 ($\eta(t)=i$)的概率为

$$P_{\mathrm{S},\, i}(t) = P(\eta(t) = i) \quad (9)$$

定义

$$P_S(t) = [P_{S,1}(t), P_{S,2}(t), \cdots, P_{S,s}(t)] \quad (10)$$

由文献[7]可知

$$dP_S(t)/dt = P_S(t)\Pi \quad (11)$$

式中,$P_S(t)$在 $t=0$时的初始概率分布为 $P_S(0)$,因为一般系统开始运行时是正常的,因此取 $P_S(0)$中 $P_{S,1}(0)=1$,其它元素为0.

当使用 FDI来检测传感器组的故障时,若 $\eta(t)=k$,FDI判断系统为状态 $i$的概率为

$$P^k_{FDI,i}(t) = P(\psi(t)=i \mid \eta(t)=k) \quad (12)$$

FDI能够正确检测和隔离当前故障的概率,即 $\psi(t)=\eta(t)=i$的概率为

$$P^i_{FDI,i}(t) = P(\psi(t)=i \mid \eta(t)=i) \quad (13)$$

定义

$$P^i_{FDI}(t) = [P^i_{FDI,1}(t), P^i_{FDI,2}(t), \cdots, P^i_{FDI,s}(t)] \quad (14)$$

可知

$$dP^i_{FDI}(t)/dt = P^i_{FDI}(t)\Theta_i \qquad i \in S \quad (15)$$

式中 $P^i_{FDI}(t)$在 $t=0$时的初始概率分布为 $P^i_{FDI}(0)$.

对本文中的例子来说,全部的传感器功能相同,冗余安装,整个传感器组/FDI模块的安全度就是下面2个事件概率的和:

1) 所有传感器全部正常(即 $\eta(t)=1$);

2) 传感器故障时,FDI装置正确隔离故障.

因此整个模块安全度 $S(t)$可以表示为

$$S(t) = P(\eta(t)=1) + \sum_{i=2}^{s}[P(\eta(t)=i)\,P(\psi(t)=i \mid \eta(t)=i)] \quad (16)$$

整个传感器组/FDI模块的可靠度就是能够输出正确测量数据的概率,即下面2个事件概率的和:

1) 所有传感器全部正常(即 $\eta(t)=1$);

2) 在有传感器正常工作的情况下,存在传感器故障,FDI装置正确隔离故障.

本例中"所有传感器都故障"(状态 $s$)为吸收态,如果假设吸收态的恢复率为0,即从状态 $s$到其它状态的转移率为0,即 $\alpha_{s,i}=0\,(i=1\sim s-1)$,就可以用式(17)来计算整个装置的可靠性:

$$R(t) = P(\eta(t)=1) + \sum_{i=2}^{s-1}[P(\eta(t)=i)\cdot P(\psi(t)=i \mid \eta(t)=i)] \quad (17)$$

现考虑一个简化情况,当 $\eta(t)$和 $\psi(t)$是如图1、图2所示的生灭过程时($|i-j|>1$时,$\alpha_{ij}=q^k_{ij}=0$)[8],稳态系统状态分布概率与系统初始状态无关,为

$$\lim_{t\to\infty} P(\eta(t)=1) = \left(1 + \sum_{j=2}^{s}\frac{\alpha_{j-1,j}\cdots\alpha_{2,3}\alpha_{1,2}}{\alpha_{j,j-1}\cdots\alpha_{3,2}\alpha_{2,1}}\right)^{-1} \quad (18)$$

$$\lim_{t\to\infty} P(\eta(t)=i) = \frac{\alpha_{i-1,i}\cdots\alpha_{2,3}\alpha_{1,2}}{\alpha_{i,i-1}\cdots\alpha_{3,2}\alpha_{2,1}} \lim_{t\to\infty} P(\eta(t)=1) \quad (19)$$

$$\lim_{t\to\infty} P(\psi(t)=1 \mid \eta(t)=i) = \left(1 + \sum_{j=2}^{s}\frac{q^i_{j-1,j}\cdots q^i_{2,3}q^i_{1,2}}{q^i_{j,j-1}\cdots q^i_{3,2}q^i_{2,1}}\right)^{-1} \quad (20)$$

$$\lim_{t\to\infty} P(\psi(t)=i \mid \eta(t)=i) = \frac{q^i_{i-1,i}\cdots q^i_{3,4}q^i_{2,3}q^i_{1,2}}{q^i_{i,i-1}\cdots q^i_{4,3}q^i_{3,2}q^i_{2,1}} \lim_{t\to\infty} P(\psi(t)=1 \mid \eta(t)=i) \quad (21)$$

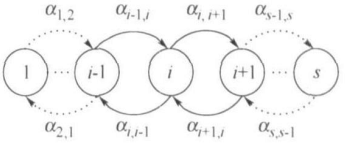



图1 系统故障过程 $\eta(t)$

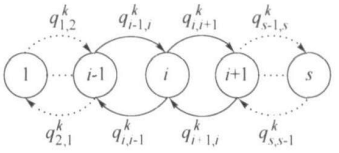



图2 $\eta(t)=k$情况下的系统 FDI过程 $\psi(t)$

## 3 故障检测延迟时间的表达式

任何一种 FDI方法都有一定的检测延时,检测延时表示的是从系统发生故障到 FDI过程做出判断之间的时间间隔.检测延时与 FDI方法、系统的动力学、噪声情况以及故障的发生情况有关.

下面给出检测延迟时间的表示方法[3]:

假设 $\tau$是 FDI决策过程(式(4))保持某种状态的时间;$F^k_{ij}(t)$是在故障过程处于状态 $k$的前提下,当 FDI过程离开状态 $i$,进入状态 $j$之前,在状态 $i$保持时间的概率分布函数;$f^k_{ij}(t)$是 $F^k_{ij}(t)$的概率密度函数.其中 $k\in S$, $i$, $j\in R$.

FDI过程在时间 $t$之前发生状态转化的概率为

$$F^k_{ij}(t) = P(\tau \le t) \quad (22)$$

而在时间 $t$之内不发生状态转化的概率,就可以表示为可靠度 $R^k_{ij}(t)$:

$$R^k_{ij}(t) = P(\tau > t) = 1 - F^k_{ij}(t) \quad (23)$$

FDI过程在时间 $t$之前不发生状态转化,在时间 $t+\Delta t$之前发生转化的概率可表示为

$$F^k_{ij}(t+\Delta t \mid \tau > t) = \frac{P(\tau \le t+\Delta t, \tau > t)}{P(\tau > t)} =$$

$$\frac{P(t < \tau < t+\Delta t)}{P(\tau > t)} = \frac{F_{ij}^k(t+\Delta t) - F_{ij}^k(t)}{1 - F_{ij}^k(t)} \tag{24}$$

$q_{ij}^k(t)$的定义为

$$q_{ij}^k(t) = \lim_{\Delta t\to 0}(F_{ij}^k(t+\Delta t \mid \tau > t)/\Delta t) \tag{25}$$

将式 (24)代入式 (25)可得到:

$$q_{ij}^k(t) = \lim_{\Delta t\to 0}\frac{F_{ij}^k(t+\Delta t \mid \tau > t)}{\Delta t} = \frac{f_{ij}^k(t)}{1 - F_{ij}^k(t)} \tag{26}$$

对于单样本检验等 FDI方法, FDI过程不需要使用历史数据,具有无记忆性, FDI过程的检测延迟时间分布函数可用指数分布来描述;对于序贯概率比等依赖历史数据的 FDI方法,可以使用 Gamma分布来描述其检测延迟时间分布[3].

如果检测延迟时间服从指数分布,即

$$f_{ij}^k(t) = \lambda_{ij}^k \exp(-\lambda_{ij}^k t) \qquad t \geq 0$$

代入式 (26)可得

$$q_{ij}^k(t) = \frac{\lambda_{ij}^k \exp(-\lambda_{ij}^k t)}{\exp(-\lambda_{ij}^k t)} = \lambda_{ij}^k = \frac{1}{T_{ij}^k} \tag{27}$$

式中, $T_{ij}^k$表示在故障过程处于状态 $k$的前提下,当 FDI过程离开状态 $i$,进入状态 $j$之前,在状态 $i$保持时间的期望值,也就是故障检测的延迟时间的期望值.

如果检测延迟时间服从 Gamma分布,即

$$f_{ij}^k(t) = \frac{\lambda_{ij}^k}{\Gamma(r_{ij}^k)}(\lambda_{ij}^k t)^{r_{ij}^k - 1}\exp(-\lambda_{ij}^k t) \qquad t \geq 0$$

代入式 (26)可得

$$q_{ij}^k(t) = \frac{(\lambda_{ij}^k)^{r_{ij}^k} t^{r_{ij}^k - 1}}{(r_{ij}^k - 1)!\sum_{m=0}\frac{1}{m!}(\lambda_{ij}^k t)^m}$$

可见 $q_{ij}^k(t)$是时变的,考虑在很短的时间范围内,可以把 $q_{ij}^k(t)$近似为常数. 当时间趋于无穷大时可得 $q_{ij}^k(t)$的极限为

$$\lim_{t\to\infty} q_{ij}^k(t) = \lambda_{ij}^k = \frac{1}{T_{ij}^k} \tag{28}$$

由此可见, FDI算法的服从 Gamma分布的检测延迟在一定条件下可以用指数分布来近似.

## 4　故障检测延迟时间与可靠度关系

将式 (27)和式 (28)代入式 (20)和式 (21),可得

$$\lim_{t\to\infty} P(\psi(t) = 1 \mid \eta(t) = i) = \left(1 + \sum_{j=2}^{s}\frac{T_{i,j-1}^i \cdots T_{3,2}^i T_{2,1}^i}{T_{j-1,,j}^i \cdots T_{2,3}^i T_{1,2}^i}\right)^{-1} \tag{29}$$

$$\lim_{t\to\infty} P(\psi(t) = i \mid \eta(t) = i) = \frac{T_{i,i-1}^i \cdots T_{4,3}^i T_{3,2}^i T_{2,1}^i}{T_{i-1,i}^i \cdots T_{3,4}^i T_{2,3}^i T_{1,2}^i}\lim_{t\to\infty} P(\psi(t) = 1 \mid \eta(t) = i) \tag{30}$$

利用式 (16)～式 (19),以及式 (29)和式 (30),就可以分析故障检测延迟时间对系统可靠性和安全性的影响.

用 $T_{ij}^k$代替 $q_{ij}^k$,可以得到图 3所示的系统 FDI过程与故障检测延迟时间的关系图. 通过观察图中状态变化的方向可以看出,当系统故障状态为 $i$的时候, FDI过程的跳变可以分为 2大类:趋近状态 $i$的运动和远离状态 $i$的运动. 趋近状态 $i$方向的检测延迟时间有 $T_{1,2}^i$, …, $T_{i-1,i}^i$以及 $T_{s,s-1}^i$, $T_{s-1,s-2}^i$, …, $T_{i+1,i}^i$,在图 3中用粗连结线表示,趋近状态 $i$表示 FDI有正确检测并隔离故障的趋势,在本文中,称作有效检测延迟时间;远离状态 $i$的检测延迟时间有 $T_{2,1}^i$, …, $T_{i,i-1}^i$以及 $T_{s-1,s}^i$, $T_{s-2,s-1}^i$, …, $T_{i,i+1}^i$,在图 3中用细连结线表示,远离 $i$表示 FDI有无法正确诊断故障的趋势,在本文中,称作无效检测延迟时间.

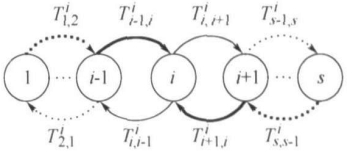



图 3　系统 FDI过程 $\psi(t)$与故障检测延迟时间的关系

下面进行定量分析. 由式 (29)和式 (30)可得

$$\lim_{t\to\infty} P(\psi(t) = i \mid \eta(t) = i) = \frac{T_{i,i-1}^i \cdots T_{4,3}^i T_{3,2}^i T_{2,1}^i}{T_{i-1,i}^i \cdots T_{3,4}^i T_{2,3}^i T_{1,2}^i}\left(1 + \sum_{j=1}^{s}\frac{T_{i,j-1}^i \cdots T_{3,2}^i T_{2,1}^i}{T_{j-1,j}^i \cdots T_{2,3}^i T_{1,2}^i}\right)^{-1} \tag{31}$$

分子分母同乘以 $T_{s-1,s}^i \cdots T_{3,4}^i T_{2,3}^i T_{1,2}^i$,式 (31)变为

$$\lim_{t\to\infty} P(\psi(t) = i \mid \eta(t) = i) = \frac{T_{i,i-1}^i \cdots T_{4,3}^i T_{3,2}^i T_{2,1}^i T_{s-1,s}^i \cdots T_{i,i+1}^i}{T_{s-1,s}^i \cdots T_{3,4}^i T_{2,3}^i T_{1,2}^i + \sum_{j=2}^{s} T_{j,j-1}^i \cdots T_{3,2}^i T_{2,1}^i T_{s-1,s}^i \cdots T_{j,j+1}^i} \tag{32}$$

为了便于分析,将分母中 $j = 2 \sim s$的连加项分为 $(j = 2 \sim i)$和 $(j = i+1 \sim s)$ 2部分,并将分子部分化为 1可得如下形式:

$$\lim_{t\to\infty} P(\psi(t) = i \mid \eta(t) = i) = \frac{1}{\frac{T_{i-1,i}^i \cdots T_{34}^i T_{23}^i T_{12}^i}{T_{i,i-1}^i \cdots T_{43}^i T_{32}^i T_{21}^i} + \sum_{j=2}^{i}\frac{T_{i-1,i}^i \cdots T_{i,i+1}^i}{T_{i,i-1}^i \cdots T_{j+1,j}^i} + \sum_{j=i+1}^{s}\frac{T_{i,j-1}^i \cdots T_{i+1,j}^i}{T_{j-1,i}^i \cdots T_{i,i+1}^i}} \tag{33}$$

分析式(33)可知,有效检测延迟时间都位于分母表达式的分子位置,当有效检测延迟时间减小时,即FDI的故障检测性能提高,整个式(33)的值增大,综合考虑式(16)和式(17)可知,系统的安全度和可靠度提高,即有效检测延迟时间越短,就越有利于故障的快速检测和隔离;同样,无效检测延迟时间都位于分母表达式的分母位置,当其增大时,即FDI发生误检的时候,反应迟缓,这将使FDI误检的可能性减小,式(33)的值也会相应地增大,系统安全度和可靠度提高.

## 5 仿真实例

考虑图4所示的双余度惯导系统,正常情况下测量装置1工作,测量装置2处于冷备份状态,使用FDI装置进行故障诊断,保证正确的输出.

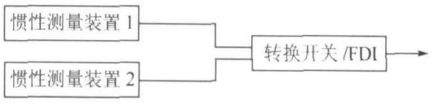



图4 双余度惯性测量装置

假设转换开关完全可靠,定义系统的状态空间 $S=\{1$(2个测量装置都正常);2(测量装置1故障,测量装置2正常);3(2个测量装置都故障)$\}$.定义FDI的状态空间 $R=S$.假设系统故障和从故障中恢复的过程不会同时发生,因此系统状态变化过程和FDI过程满足生灭过程,其中 $\alpha_{1,2}=3.334\times10^{-2}\ h^{-1}$, $\alpha_{2,3}=1.667\times10^{-2}\ h^{-1}$, $\alpha_{2,1}=\alpha_{3,2}=0.1\times10^{-2}\ h^{-1}$.考虑下面3种情况:

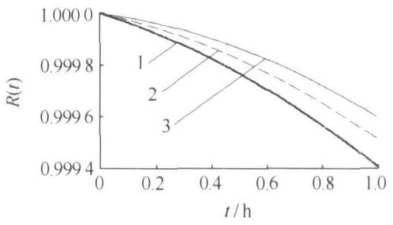
1) $q^1_{1,2}=q^1_{2,3}=0.6\ h^{-1}$, $q^1_{2,1}=q^1_{3,2}=q^2_{1,2}=120\ h^{-1}$, $q^2_{2,3}=q^2_{2,1}=0.6\ h^{-1}$, $q^2_{3,2}=q^3_{1,2}=q^3_{2,3}=120\ h^{-1}$, $q^3_{2,1}=q^3_{3,2}=0.6\ h^{-1}$,即有效检测时间为0.0083 h,无效检测时间为1.6667 h;

2) $q^1_{1,2}=q^1_{2,3}=1\ h^{-1}$, $q^1_{2,1}=q^1_{3,2}=q^2_{1,2}=300\ h^{-1}$, $q^2_{2,3}=q^2_{2,1}=1\ h^{-1}$, $q^2_{3,2}=q^3_{1,2}=q^3_{2,3}=300\ h^{-1}$, $q^3_{2,1}=q^3_{3,2}=1\ h^{-1}$,即有效检测时间为0.0033 h,无效检测时间为1 h;

3) $q^1_{1,2}=q^1_{2,3}=0.6\ h^{-1}$, $q^1_{2,1}=q^1_{3,2}=q^2_{1,2}=300\ h^{-1}$, $q^2_{2,3}=q^2_{2,1}=0.6\ h^{-1}$, $q^2_{3,2}=q^3_{1,2}=q^3_{2,3}=300\ h^{-1}$, $q^3_{2,1}=q^3_{3,2}=0.6\ h^{-1}$,即有效检测时间为0.0033 h,无效检测时间为1.6667 h.

为求取可靠度,定义状态2)为吸收态,即 $\alpha_{3,2}=0$.根据式(11)、式(15)和式(17),通过Matlab数值计算,得出3种情况下,系统可靠度随时间的变化曲线如图5所示.

图5可见,有效检测延迟时间越长,系统可靠度越低;无效延迟时间越短,系统可靠度越低.




1—有效检测延迟为0.0083 h,无效检测延迟为1.6667 h;
2—有效检测延迟为0.0033 h,无效检测延迟为1 h;
3—有效检测延迟为0.0033 h,无效检测延迟为1.6667 h.

图5 系统可靠度随时间变化的情况

## 6 结束语

对FTCSMP已有的研究大多集中在稳定性方面,本文首次将该模型用于传感器组/FDI装置的可靠性分析,在系统故障过程和FDI过程是生灭过程的情况下,定义了"有效"和"无效"2种故障检测延迟时间,进一步研究了2种故障检测延迟时间对可靠性和安全性的影响.本文的意义在于将FTCSMP的研究从稳定性分析推广到可靠性分析.以FTCSMP为桥梁,可以同时进行系统稳定性和可靠性研究,为实际工程中可靠性与稳定性的同步设计和分析提供了理论依据.

### 参考文献 (References)

[1] Srichander R, Walker B K. Stochastic stability analysis for continuous time fault tolerant control systems[J]. International Journal of Control, 1993, 57(2): 433 - 452

[2] Mahmoud M M, Jiang J, Zhang Y M. Stochastic stability analysis of fault tolerant control systems in the presence of noise[J]. IEEE Trans on Automatic Control, 2001, 46(11): 1810 - 1815

[3] Mahmoud M M, Jiang J, Zhang Y M. Effects of fault detection and isolation to the stability of fault tolerant control systems[C]//Proceedings of the American Control Conference. Arlington: IEEE, 2001, 4: 2676 - 2681

[4] 高飞,张洪钺. 带马尔可夫参数的延时容错控制系统稳定性研究[J]. 北京航空航天大学学报, 2006, 32(5): 566 - 570
Gao Fei, Zhang Hongyue. Stability of time-delay fault tolerant control systems with markovian parameters[J]. Journal of Beijing University of Aeronautics and Astronautics, 2006, 32(5): 566 - 570 (in Chinese)

[5] Patton J R, Frank P, Clark R. Issues of fault diagnosis for dynamic systems[M]. London: Spring-Verlag, 2000: 219 - 244

[6] Vaidya N H, Pradhan D K. Fault-tolerant design strategies for high reliability and safety[J]. IEEE Trans Computers, 1993, 42(10): 1195 - 1206

[7] Stewart W J. Introduction to the numerical solution of Markov chains[M]. Princeton, NJ: Princeton University Press, 1994

[8] Kuo W, Zuo M J. Optimal reliability modeling, principles and applications[M]. New York: John Wiley & Sons Inc, 2002: 50 - 58

(责任编辑:文丽芳)