DFTA 在软硬件相关故障诊断中的应用研究

熊 斌[1],张 力[1],王 珊[2]
XIONG Bin[1],ZHANG Li[1],WANG Shan[2]

1.第二炮兵工程学院 401 教研室,西安 710025
2.西安电子科技大学 机电工程学院,西安 710071
1.Xi'an Research Inst. of Hi-Tech,Xi'an 710025,China
2.School of Electro-mechanical Engineering,Xidian University,Xi'an 710071,China
E-mail:xiongbin122@Yahoo.com.cn

XIONG Bin,ZHANG Li,WANG Shan.DFTA based fault diagnosis of correlative fault between software and hardware. Computer Engineering and Applications,2008,44(35):217-219.

Abstract: Because of the existence of a great deal of imbedded software,the fault model of software-intensive system is changed,and a new correlative fault between software and hardware appears.This paper analyses the characteristics of the correlative fault between software and hardware firstly,and then a DFTA based fault diagnosis method is proposed.The analyzing process is also present in the paper.In the end,the feasibility of this method is proved by an example.
Key words: correlative fault between software and hardware;Dynamic Fault Tree Analysis(DFTA);fault diagnosis

摘 要:软件密集型系统中由于有大量软件的嵌入,其故障模式发生了变化,产生了新的软硬件相关的故障模式。在分析软硬件相关故障特征的基础上,提出了一种基于动态故障树分析方法的故障诊断方案,并给出了分析方法和步骤。最后通过实例分析,证明了这种方法的可行性。
关键词:软硬件相关故障;动态故障树;故障诊断
DOI:10.3778/j.issn.1002-8331.2008.35.065 **文章编号**:1002-8331(2008)35-0217-03 **文献标识码**:A **中图分类号**:TP206+.3

1 概述

随着计算机系统的广泛使用,软件密集型系统与人们的日常生活越来越密切。软件密集型系统(Software-Intensive System)即软件对系统研制发展、任务完成起主要作用,或者是软件在系统开发、运行或演化中起着关键作用的系统。

在软件密集型系统中有大量软件程序的嵌入,而现有的开发手段和测试技术不能保证软件不发生错误, 软件错误可以通过和硬件的交互作用传递给硬件,并最终导致系统失效;同时,由于软件设计的不完善,硬件故障也能引起软件的失效。这些新的软硬件相关的故障模式给软件密集型系统的故障诊断和维修保障带来了困难, 研究它们的故障诊断方法具有重要的意义。

2 软硬件相关故障

软件密集型系统中由于有软件程序的嵌入,并和硬件系统起着同样重要的作用。因此其故障模式不仅包括软件、硬件自身的故障模式, 而且还包括软硬件结合所带来的新的问题,这些新的故障模式即软硬件相关故障模式。它既有软件故障的特点又有硬件故障的特点,但并不是软件故障和硬件故障的简单组合,而是在软件和硬件相结合的情况下产生的故障,既影响系统软件又作用于系统硬件,一般有如下 3 种类型:(1)软件程序发生错误,这些错误通过软件和硬件的相互作用,传递给硬件并引起硬件的失效;(2)硬件发生损坏或故障,并对与之相关的软件产生影响,导致软件发生错误;(3)软件和硬件都不存在独立的错误或故障,但当它们发生联系时,发生系统失效,或者不能完成预定功能。

软硬件相关故障的主要故障特性如下:(1)相关性:即当一个元素或联系发生故障后,可能导致同它相关的元素或联系的状态发生变化,进而引起相关元素或联系也发生故障。某一故障可能对应若干征兆,而某一征兆可能对应若干故障,它们之间存在着错综复杂的关系,造成故障诊断困难。故障的相关性使得许多的故障现象可以归根于同一个故障,从而可以从不同的角度对同一个故障进行诊断;(2)时序性:即一个故障只有在其故障因素按照一定时序关系发生时,这个故障才会产生。这主要是因为在软件密集型系统中,许多功能都是通过软件和硬件的相互作用完成的, 控制流和数据流通过软件传递给硬件,只有按照特定的顺序传送特定的数据,系统才能完成其正确的功能,当时序发生改变时,系统就会产生故障。

基金项目:国家部委预研课题。
作者简介:熊斌(1984-),男,硕士,主研领域为指挥自动化;张力,女,博士,副教授,主研领域为指挥自动化;王珊,女,硕士,主研领域为微波非线性。
收稿日期:2008-06-03 **修回日期**:2008-08-21

3 基于 DFTA 的软硬件相关故障诊断方法

故障树分析方法(FTA)是可靠性分析和故障诊断的传统技术工具。它是一种图形演绎方法,用一种特殊的倒立树状逻辑因果关系图,清晰地说明系统是怎样失效的。故障树分析方法可以同时用于硬件和软件的故障诊断,具有直观的分析效果。动态故障树(DFTA)是至少包含一个动态逻辑门的故障树,具有动态的系统性能,能对具有顺序相关、资源共享、可修复和冷热备份的系统进行故障分析。根据软件密集型系统软硬件相关故障的故障特性和动态故障树分析方法的优点,考虑将动态故障树分析方法用于软硬件相关故障诊断。

软硬件相关故障诊断就是从系统的一个软硬件相关故障事件开始,找出导致故障的软、硬件因素。通过对软件密集型系统进行研究可以发现,通常情况下,软硬件相关故障事件有如下几种类型:(1) 包含有嵌入式计算机系统的模块出现故障;(2)包含有常规计算机系统的模块出现故障;(3)包含配置信息的模块出现故障;(4)需要有软件控制或提供数据的硬件模块不能完成预定功能。

动态故障树分析方法用于软硬件相关故障诊断,关键在于动态故障树的构造,一般可以采用和建立硬件故障树类似的演绎法,软硬件相关故障的顶事件可以是上述的 4 种软硬件相关事件。在构建软硬件相关故障动态故障树的过程中,通常需要用到如下几种动态逻辑门:

(1)优先与门:具有两个输入事件,并且输入事件必须以指定顺序发生才会引发输出故障事件,如图 1 所示,即输入事件 A 和 B 必须都发生,并且 A 在 B 之前发生才会产生输出事件 C;

(2)顺序相关门:如图 2,具有 3 个以上输入事件,并且要求输入事件要按指定顺序发生,由此可知,优先与门是顺序相关门的一个特例。软硬件相关故障中与数据流、控制流有关的故障事件一般可以由用顺序相关门或优先与门表示,这样可以描述它们的时序关系, 如显示驱动程序错误使显示器出现故障,最终导致显示器不能正常工作。

(3)功能相关门:系统中某个部件发生故障(称其为激发事件)会导致与其相关的其他部件无法进入工作状态或者发生故障。如图 3,功能相关门由一个输入激发事件(可以是一个基本事件或故障树中某一个门的输出事件)和一个以上的相关基本事件组成。相关基本事件在功能上依赖于激发事件:激发事件发生时,相关事件一定发生,但是任何单个相关基本事件的发生对激发事件的发生并不产生影响。它一般可以描述软硬件相关故障中具有包含关系和转化关系的事件,如通信系统中线路出错导致它的两个信道故障。

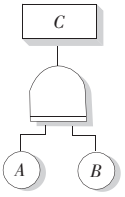

图 1 优先与门

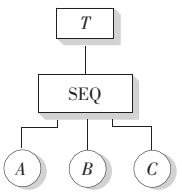

图 2 顺序相关门

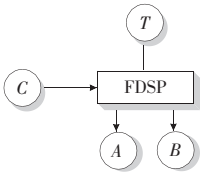

图 3 功能相关门

4 软硬件相关故障的动态故障树分析

软硬件相关故障的动态故障树在建立以后,就需要对其进行分析,以便找出导致故障的原因。在动态故障树中,由于有动态逻辑门的引入,传统的定性定量分析方法已经不能满足分析的需要,而 Markov 过程有利于分析动态问题,利用 Markov 方法,可以有效地分析动态故障树的可靠性参数。

4.1 定量分析

利用 Markov 方法分析动态故障树的可靠性参数, 它的实质就是把具有动态特性的逻辑门转化为故障状态转移子链,然后根据 Markov 链的特性来求解, 所以把动态逻辑门转化为故障状态转移子链是利用 Markov 方法求解动态故障树的关键所在。所举的典型动态逻辑门的故障状态转移子链如图 6 所示(其中 0 表示部件处于正常状态,1 表示部件处于故障状态,p 表示转移概率)。

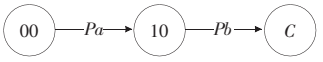

图 4 优先与门的状态转移链

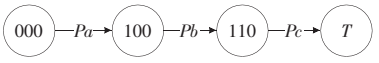

图 5 顺序相关门的状态转移链

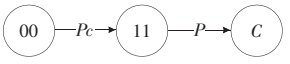

图 6 功能相关门的状态转移链

把动态故障树的动态逻辑门转化为故障状态转移子链以后,可以得到系统的故障状态转移图。设在状态转移图中,系统从正常状态 $S0$ 转移到故障状态 $S1$ 的状态转移子链共有 n 条:$L_1, L_2, \cdots, L_n$,则系统在 t 时刻处于故障状态 $S1$ 的概率为:$P(t)=\sum_{i=1}^{n} p_i^{Li}(t)$,$p_i^{Li}(t)$,是 $p_i(t)$在状态转移子链 Li 上的分量。

设故障状态转移子链 Li 的链长为 m,即 Li 分量由 m 个转移状态组成,则故障状态转移子链是一个时间连续状态离散的 Markov 过程,根据切普曼–柯尔莫哥洛夫(Chapman–Kolmogorov)方程,其状态转移概率函数之间具有关系式:

$$p_{ij}(s+t)=\sum_r p_{ir}(s)p_{rj}(t), i,j=0,1,2,\cdots$$

即由状态 i 出发经过 $s+t$ 时间到达状态,j 必须先经过 s 时间到达任意状态 r,然后再经 t 时间由状态 r 转移到状态 j。

系统经过故障状态转移子链 Li 从正常工作状态 0 到故障状态 1,有:

$$p_{01}=p_{0r}\cdot p_{r1}=(p_{0i}\cdot p_{ir})\cdot(p_{rj}\cdot p_{j1})=$$

$$p_{0,s1},p_{s1,s2}\cdots p_{si,sj}\cdots p_{sn,1}=\prod_{k1}^{m} q_k(t)$$

即对每条状态转移子链,其转移概率函数为:$p_i(t)=\prod_{k=1}^{m} q_k(t)$,$q_k(t)$是状态转移子链 Li 上的每个基本事件的发生概率。由此可得:$P(t)=\sum_{i=1}^{n}\prod_{k=1}^{m} q_k^{Li}(t)$。

在初始状态下,$P(0)=\sum_{i=1}^{n} q_i^{Li}(0)$,设系统故障的修复率为 1, 则系统从正常状态 $S0$ 转移到故障状态 $S1$ 的一步转移矩阵为:$\begin{bmatrix}1-P_{(0)} & P_{(0)}\\ 1 & 0\end{bmatrix}$,经过 n 步达到平稳状态,设平稳状态行向量为$[y_1 \quad y_2]$,根据 Markov 链的遍历性,有:

$$\begin{cases}y_1=(1-P_{(0)})\cdot y_1+y_2\\ y_2=P_{(0)}\cdot y_1\\ y_1+y_2=1\end{cases}$$

由此解得:$y_1=\frac{1}{1+P_{(0)}}$,$y_2=\frac{P_{(0)}}{1+P_{(0)}}$,这样就可以求出系统的失效率和可靠度,在系统经过长时间运行后,系统的可靠度为 y_1,系统的失效率为 y_2。

4.2　定性分析

在系统的故障状态转移图中,n 条状态转移子链 L_1,L_2,…,L_n 中的任何一条 Li,都可以使系统从正常状态 $S0$ 转移到故障状态 $S1$,所以可以认为每一条故障子链中基本事件构成的序列都是系统的一个顺序割集,记为:$\overrightarrow{X_j^{Li}}$,$j=1,\cdots,l$,其中 X_j^{Li} 为故障子链 Li 的第 j 个基本事件,→表示基本事件的一个有秩序的排列,l 为故障子链 L_i 中基本事件的数量。通过遍历系统的状态转移图可以找出系统的所有顺序割集,这些顺序割集就是导致系统故障的基本事件序列。

设有顺序割集 $\overrightarrow{X_1X_2\cdots X_n}$,若 $\exists\{X_i|i\in n\}\Rightarrow\overrightarrow{X_1X_2\cdots X_n}$,⇒表示其左事件可以导致右事件发生,并且使 $\mathbb{R}X_i$ 最小,$\mathbb{R}X_i$ 指 X_i 的个数,则称集合 $\{X_i|i\in n\}$ 为顺序割集 $\overrightarrow{X_1X_2\cdots X_n}$ 的最小原事件集。顺序割集的最小原事件集是顺序割集基本事件的一个子集,它是顺序割集所对应的故障状态转移子链上,导致系统故障的最小基本事件集合。通过分析系统的所有最小原事件集,就能找到导致系统故障的根本原因,达到故障诊断的目的。

5　实例分析

某通信设备具有通信控制和信息保障能力,根据分析,该通信设备属于典型的软件密集型系统,在使用过程中曾发生线路数据不通的系统故障。根据本文的诊断方法建立的软硬件相关故障树中,动态子树如图 7 所示,其中:X_1:软件错误;X_2:软件错误引起线路板故障;X_3:信道 1 故障;X_4:信道 2 故障。

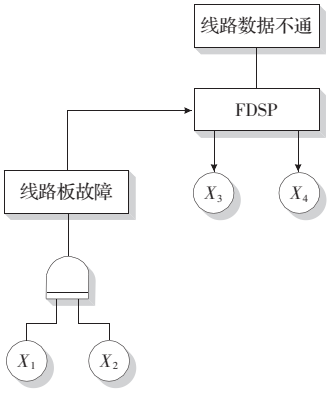

图 7　软硬件相关故障子树

根据动态故障树分析步骤,把上述故障子树转化为Markov状态转移链如图 8 所示,其中 $S0$ 表示系统正常;$S1$ 表示 X_1 故障;$S2$ 表示 X_2 故障;$S3$ 表示顶事件"线路数据不通";$\lambda_1\sim\lambda_4$ 表示 $X_1\sim X_4$ 的故障率。

用 Markov 方法求解其故障参数,设失效模块经过故障排除转移到正常状态的概率为 1,不能修复的概率为 0,则由上图可知,系统由正常状态 $S0$ 转移到故障状态 $S3$ 的一步转移矩阵为 $\begin{bmatrix}1-(\lambda_3+\lambda_4)(1+\lambda_1\lambda_2) & (\lambda_3+\lambda_4)(1+\lambda_1\lambda_2)\\ 1 & 0\end{bmatrix}$,经过 n 步到达平稳状态,设稳态概率行向量为 $[y_1\ \ y_2]$,则可得方程组:

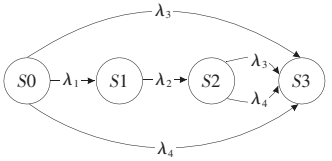

图 8　故障子树转化的 Markov 状态转移图

$$\begin{cases}y_1=[1-(\lambda_3+\lambda_4)(1+\lambda_1\lambda_2)]y_1+y_2\\ y_2=(\lambda_3+\lambda_4)(1+\lambda_1\lambda_2)y_1\\ y_1+y_2=1\end{cases}$$

解得 $y_1=\frac{1}{1+(\lambda_3+\lambda_4)(1+\lambda_1\lambda_2)}$,$y_2=\frac{(\lambda_3+\lambda_4)(1+\lambda_1\lambda_2)}{1+(\lambda_3+\lambda_4)(1+\lambda_1\lambda_2)}$

假定,$\lambda_1=0.05$,$\lambda_2=0.06$,$\lambda_3=0.04$,$\lambda_4=0.08$ 可求得 $y_1=0.892\,5$,$y_2=0.107\,5$ 即系统处于 $S3$ 失效状态的概率为 0.107 5,系统正常工作的概率为 0.892 5。

在状态转移图中,系统的状态转移子链共有 4 条,它们分别对应的基本事件序列为:$\overrightarrow{X_1,X_2,X_3}$,$\overrightarrow{X_1,X_2,X_4}$,$\overrightarrow{X_3}$,$\overrightarrow{X_4}$ 这 4 个基本事件序列是导致系统故障的原因。结合本通信设备分析这 4 个基本事件序列,可以发现事件 $\{X_1\}$ 是事件序列 $\overrightarrow{X_1,X_2,X_3}$,$\overrightarrow{X_1,X_2,X_4}$ 的最小原事件集,$\{X_3\}$、$\{X_4\}$ 是其本身的最小原事件集。由此可得,导致系统线路数据不通故障的根本原因是:X_1 软件错误,或 X_3 信道 1 故障,或 X_4 信道 2 故障。

6　结束语

软硬件相关故障是软件密集型系统中出现的一类新的故障模式,经过分析可知,动态故障树分析方法是进行软硬件相关故障诊断的有效工具,利用 Markov 方法对建立的软硬件相关故障动态故障树进行分析,可以得到系统的故障参数。通过分析系统的故障状态转移图,可以寻找系统的最小原事件集,从而得出导致系统故障的原因,达到故障诊断的目的。但是由于软件密集型系统的复杂性和故障树分析方法的局限性,要建立整个系统的动态故障树是相当困难的,所以一般只利用动态故障树对系统关键部位的软硬件相关故障进行故障诊断。

参考文献:

[1] 高顺川.动态故障树分析方法及其实现[D].长沙:国防科学技术大学,2005.
[2] 刘延夫.基于马尔可夫分析方法的软件系统可靠性研究[D].长春:长春理工大学,2004.
[3] 余爱华.基于 FTA 的液压系统故障诊断与维护[J].铜陵学院学报,2006.
[4] 王世明.故障树分析法在工程机械发动机故障诊断中的应用[J].机床与液压,2007,35(9).
[5] 浣上.磁浮列车故障诊断技术研究[D].长沙:国防科学技术大学,2004.
[6] 张超.基于 BDD 的动态故障树优化分析研究[D].西安:西北工业大学,2002.
[7] Assaf T,Dugan J B.Approximation of diagnostic importance factors using Markov models for diagnostic test sequencing[C]//Pro of IEEE AUTOTESTCON,2004.
[8] Finlay S S,Shen Q.Fault identification through the combination of symbolic conflict recognition and Markov chain-aided belief revision[J].IEEE Transactions on Systems.Man.Aand Cybernetics,part A:Systems and Humans,2004,34(5).