故障树模块化分析系统可靠性

陈光宇，黄锡滋，唐小我

(电子科技大学管理学院 成都 610054)

【摘要】针对软硬件复合计算机系统的可靠性分析，提出了相应的模块化分解模型，采用动态和静态相结合的方法分析系统可靠性。通过分析案例系统的可靠性和部件的重要度，揭示在软硬件复合计算机系统中软件子系统是系统可靠性增长的重要因素，说明软件可靠性分析和设计技术的研究和应用对系统可靠性的整体提高亦十分重要。

关 键 词 可靠性； 故障树分析； 模块化； 失效率； 重要度
中图分类号 N945 文献标识码 A

Modular Solutions for Fault Tree Analysis of Reliability of Systems

CHEN Guang-yu，HUANG Xi-zi，TANG Xiao-wo

(School of Management, Univ. of Electron. Sci. & Tech. of China Chengdu 610054)

Abstract Accounting for reliability analysis of computer systems with hardware and software, a dynamic and static Fault Tree model is presented to analyze reliability of systems. Analyzing reliability and components' importance of a sample of computer systems, this paper is focused on software reliability increment as the most crucial component for increasing system reliability effectively, and thus the importance of software reliability analysis and design is illustrated to increase the global reliability of systems distinctly.

Key words reliability; fault tree analysis; modularization; failure rate; importance

1996年6月，欧洲航天局研制的“阿丽亚娜5型火箭”发射失败，根本原因在于火箭设计师重硬件可靠性设计，轻软件可靠性设计，导致火箭惯性制导系统软件出现规格和设计错误。由此看出，复合计算机系统软件可靠性分析至关重要。

源于20世纪70年代的故障树分析方法(FTA)，以其严整的逻辑结构和形象的树状图形，以及强大的揭示故障根源和定量计算失效概率的功能，深受可靠性工程界的欢迎[1]。传统的FTA方法以系统的各种基本事件是否发生作为故障分析的依据，没有考虑各种基本事件在时间变化过程中的相互依存关系，是一种静态的基本事件组合关系的图形化分析方法。而动态FTA分析方法是传统(静态)FTA的扩展集，即在传统故障树逻辑门的基础上，新设计了若干能够反映系统动态特征(时序活动)的逻辑门[1]。

1 复合计算机系统的FTA模块化分解模型

假定复合计算机系统是串联结构，由相互独立的硬件子系统和软件子系统组成，可得到系统的FTA模块化分解模式，如图1所示。

静态故障树采用图形化的方法表示基本事件的组合关系。组合关系可用布尔函数表达，通过最小割集、不交化方法等求解事件的失效概率。但是，计算量随着故障树逻辑门和基本事件数目的增加而呈指数增长，产生组合爆炸问题。另外，可利用早期逻辑简化、早期模块分解和早期不交化的“三早”简化技术对故障树进行综合简化处理[2]。类似的还有二元决策图(Binary Decision Diagram，BDD)[3]、GA(Genetic algorithms)等算法。BDD是一种紧凑、规范的布尔函数表示法，没有重复的子树或冗余节点，能为系统庞大的组合结构提供有效方案，是一种不需要找割集或对偶树的算法[4]。BDD的缺点是在故障树转化过程中，不能保证结果最优，不利于被广泛使用。

收稿日期：2004 - 06 - 21
作者简介：陈光宇(1969 –)，男，博士，讲师，主要从事系统可靠性和安全性方面的研究.

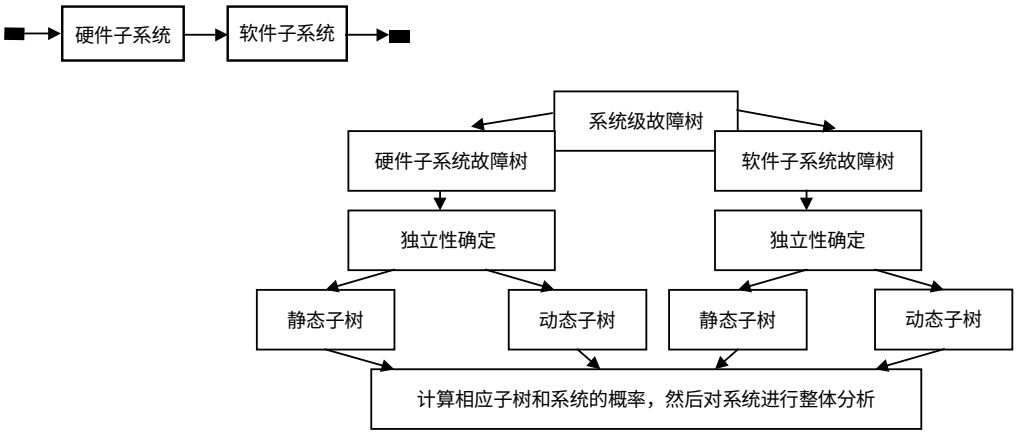

图1 系统模块化分解模型

动态故障树模型能有效地表示基本事件的失效顺序性、功能相关性和储备件分配等相互依存关系。马尔科夫链的状态可以完整地描述部件的失效行为、部件的失效时序和储备件分配等，马尔科夫链模型可用于分析动态故障树[5]。

蒙特卡罗仿真法可用于故障树评价。对于完全接受任何失效分布的模型和无法采用分析方法解决的模型，模型仿真是一种可选方案。而且，模型仿真对于解决高度冗余的情况是非常有效的方法。例如，*k*/*m*表决门的*k*、*m*值很大，且部件不同型。在这种情况下，模型分析会产生组合爆炸，采用模型仿真将优于模型分析。模型仿真方法需要很长的运算时间才能得到所需要的高精度结果，同时采用变量减少的方法，可明显地减少运算时间。

常用的部件分布函数有固定的失效概率、失效率为常数的指数分布、威布尔分布和对数正态分布等。固定概率常常用于描述软件设计故障[4]，指数分布常常用于描述物理随机故障。假如比较复杂的增长模型的数据得不到时，常常容易将固定失效概率应用到计算机应用软件的建模中[4]。不过，在具有实际数据支持的条件下，建议采用由相应的软件可靠性数学模型确定的失效概率进行建模。关于硬件的物理失效和系统软件的随机失效较准确的建模，则常常采用指数分布。

2 案例系统分析统

基于HECS[3-5]的假定通用计算机系统如图2所示，为阐述FTA模块化分解方法，本文建立相应的静态和动态子树。

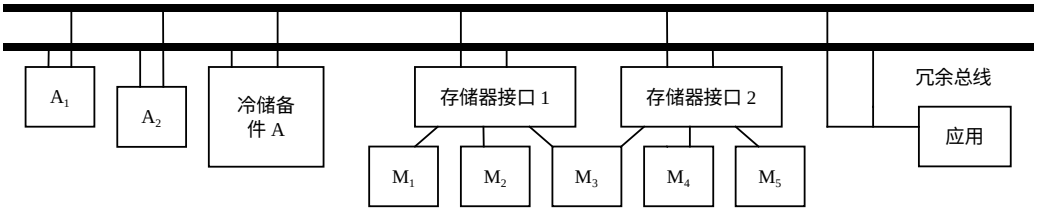

图2 假定的通用计算机系统

HECS由双重冗余的处理器A_1、A_2和可以替代它们的一个冷储备件组成。冷储备件在使用前不会失效。HECS有5个存储器，为保证正常工作需要至少3个部件。存储器之间通过存储器接口互连。如果存储器接口失效，连接其上的存储器就不能使用。存储器M_3是冗余件，与存储器接口连接。因此M_3在任意一个存储器接口正常的情况下，其工作状态都是正常的。此外，还有一个应用软件和系统连接。HECS能正常工作的要求是：(1) 3个处理器中至少有1个工作正常；(2) 5个存储器中至少3个工作正常；(3) 2条总线至少1条正常；(4) 软件运行正常。运用上述的模块化分解方法可构造相应的故障树，如图3所示。

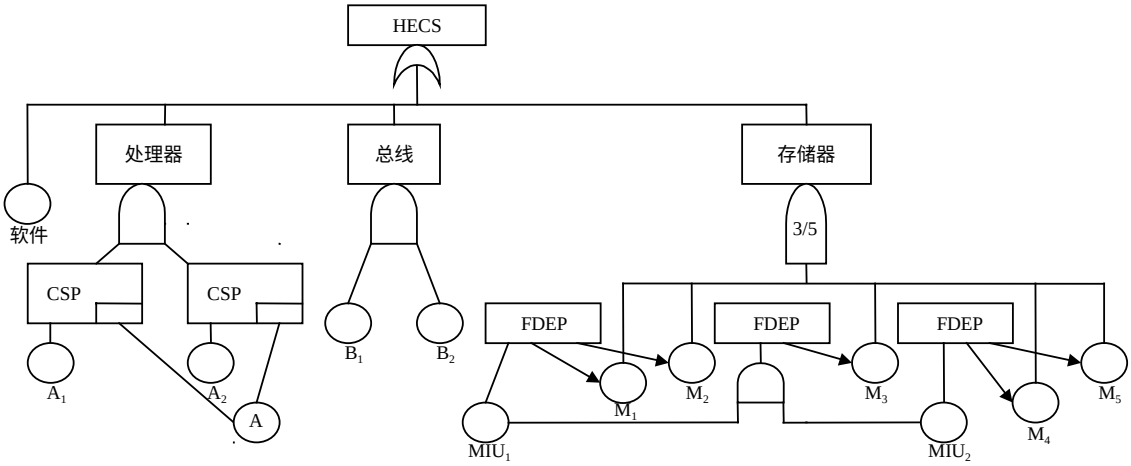

图3　针对HECS的故障树

系统故障树可分解为软件故障子树和硬件故障子树，硬件故障子树包括处理器、存储器、总线部分。软件子树和总线子树分析采用静态故障树的分析方法。总线子树是两个基本事件的并集，其中一条总线是冗余的。

关于处理器模块的分析采用冷储备门CSP。冷储备件A在储备条件下，既不失效也不退化。无论处理器A_1或A_2失效，冷储备件A都可以替代它们。冷储备门CSP左边的输入是冷储备门的初始输入，其余的输入在初始输入失效后，逐个依次替补。依赖于失效的数据和活动，储备件的失效分布可假设为指数分布(失效率为常数)或者是威布尔分布(失效率随时间变化)。马尔科夫链不适宜冷储备件的失效率为WEIBULL的动态模型。这是因为在状态转移时，失效率是多少并不清楚。换句话说，如果在时间t切换，失效率可为$\lambda(0)$或$\lambda(t)$，完全依赖于对储备件在切换时的假设状态是初始的新状态还是剩余的时间状态。

当存储器单元通过工作的存储器接口与系统的其他部分连接时，存储器模块的分析采用功能相关门FDEP。存储器接口MIU_1、MIU_2作为触发器，必须保证5个存储器中至少有3个是正常的，即5个存储器中若有3个或多于3个失效会引起系统失效。

HECS系统级故障树的模块化分解明确了每一个独立的子树是静态模块或动态模块。根据不同的参数和条件，对静态模块或动态模块各自采用有效的解法。

下面假设HECS中各个部件的寿命分布函数服从指数分布，失效率为常数。指数分布是唯一的故障率为常数的连续分布。指数分布简单性和无记忆性的特点，使其被广泛应用于描述部件失效行为。

从图3的故障树，可以看到软件子系统和硬件子系统都是系统故障树的一阶最小割集。分析Birnbaum概率重要度[6-7]可知，失效概率越大的子系统，对系统失效概率的影响越大。对软件和处理器进行对比分析，因处理器在动态故障树中，可选择FUSSELL-VESELY重要度[6]I_i^{FV}作为分析指标。

本文有如下的一些假定。

1) 失效率参数为[1]：

(1) 处理器1.1×10^{-4}/h；(2) 存储器1.1×10^{-4}/h；(3) 存储器接口0.17×10^{-4}/h；(4) 总线0.01×10^{-4}/h。

2) 软件失效率分为4种情况：

(1) 5.0×10^{-4}/h；(2) 1.0×10^{-4}/h；(3) 0.5×10^{-4}/h；(4) 0.3×10^{-4}/h。

处理器、存储器和软件的失效率相差不多。但是，由于系统结构的原因，它们对系统的影响是不同的。表1的数据表明，软件子系统的FUSSELL-VESELY重要度远大于处理器，软件子系统的失效概率对系统的失效概率的贡献最大。显然，系统的失效概率主要是由软件子系统的失效概率确定的，原因是HECS系统仅仅重视了硬件子系统可靠性的提高，而忽视了软件子系统可靠性的提高，致使软件子系统成为系统整体可靠性提高的瓶颈。这种现象提示，对于高可靠计算机系统，不仅要重视硬件子系统的可靠性的提高，而且要重视软件可靠性的提高，才能实现系统可靠性指标的整体提高。

表**1** 软件失效率为表2中的情况**(2)**时，不同时间条件下的**FUSSELL-VESELY**部件重要度

系统运行时间/h	系统失效概率	软件失效概率	$I_{\text{soft}}^{\text{FV}}$	处理器子树失效概率	I_{A}^{FV}
200	0.020 4	0.019 8	0.971 9	0.000 5	0.023 2
400	0.064 4	0.058 2	0.904 4	0.004 1	0.063 3
1 000	0.113 8	0.095 2	0.835 9	0.010 9	0.095 3

表**2** 软件失效率的变化对系统失效率的影响

失效率情况	系统运行时间/h	系统失效概率	软件失效概率	$I_{\text{soft}}^{\text{FV}}$
(1)	1 000	0.406 0	0.393 5	0.969 2
(2)	1 000	0.113 8	0.095 2	0.835 9
(3)	1 000	0.068 4	0.048 8	0.713 5
(4)	1 000	0.049 6	0.029 6	0.596 8

表2的数据表明：

1) 当软件失效率增加时，软件失效率对系统失效概率的贡献增大，逐渐向成为系统整体失效概率的决定因素的趋势发展，软件失效率对系统整体可靠性提高的瓶颈作用变得更强；

2) 当软件失效率减少时，软件的失效概率逐渐降低，软件的FUSSELL-VESELY重要度逐渐减小，系统整体可靠性的增幅逐渐减缓，软件失效率对系统整体可靠性提高的瓶颈作用逐渐减弱。

4 结 束 语

FTA模块化分解模型和重要度分析方法有助于系统设计师分析软硬件复合计算机系统的可靠性。案例分析提示，在目前硬件可靠性技术相对较完善的情况下，应该更加重视对软件可靠性技术的研究和应用，从而有效地提高软件子系统的可靠性，实现系统可靠性水平的整体提高。

参 考 文 献

[1] 黄锡滋. 动态故障树FTA方法的新进展[J]. 装备质量, 2003, 1: 34-43.
[2] 曾声奎. 系统可靠性设计分析教程[M]. 北京: 北京航空航天大学出版社, 2000.
[3] Dugan J B, Coppit D. Developing a low-cost high-quality software tool for dynamic fault-tree analysis[J]. IEEE Transaction on Reliability, 2000, 49(1): 49-59.
[4] Manian R, Dugan J B, Coppit D, et al. Combining various solution techniques for dynamic fault tree analysis of computer system[C]// Third IEEE International High-Assurance System Engineering Symposium, Washington D C., 1998.
[5] Dugan J B, Bavuso S, Boyd M. Dynamic fault tree models for fault tolerant computer systems[J]. IEEE Transaction on Reliability, 1992, 41(3): 363-377.
[6] Henly E J, Kumamoto H. Reliability engineering and risk assessment[M]. Englewood Cliffs: Prentice-Hall, 1981.
[7] 曹晋华, 程 侃. 可靠性数学引论[M]. 北京: 科学出版社, 1986.

编 辑 熊思亮