

国外计算机技术发展动向

一九八一年六月

出版说明

一九八〇年十月，我部以中国宇航学会陕西微电子学研究所代表小组的名义，派出沈绪榜、杨樱华二同志出席了在日本京都举行的第十届容错计算机会议和第八届世界计算机大会。

在容错计算机会议上，杨樱华同志宣读了一篇题为“阈值集中注入逻辑完全自检线路”的论文，受到与会者的好评。容错技术委员会负责人 W. C. Carter 博士，邀请杨樱华同志列席容错技术委员会，并邀请她为第十一届国际容错计算会议的联络委员。

代表小组通过会议和考察，对国外容错计算技术及电子计算机重要性、应用技术水平有较深入的了解，收获很大。回国后，他们进行了认真细致的技术总结，并写出了总结报告，为了促进科研，并为广大计算机爱好者提供一些重要资料，现编辑出版，供各部门有关同志参阅。

目 录

一、容错计算技术.....	1
二、计算机技术概况.....	16

容 错 计 算 技 术

杨 樱 华

一、第十届国际容错计算会议概况

一九八〇年十月一日至十月三日在日本京都举行了国际容错计算会议，也是首次在亚洲地区举行。主办单位为：美国 IEEE 计算机学会容错计算技术委员会、日本电子与通讯工程师学会电子计算机专业组和日本电子与通讯工程师学会可靠性专业组。参加举办本会议的日本单位还包括教育、科学、文化部、国际商务与工业部、邮电部，以及日本科学协会、日本电气工程师学会、日本信息处理学会、日本仪器与控制工程师学会、IEEE 日本分会等单位。

参加会议的人数共二百三十二人，会议从十七个国家送去的 188 篇论文中，选取了十三个国家的 73 篇论文，其中美国占 32 篇，日本 16 篇，法国 13 篇，意大利及加拿大各两篇，我国、西德、波兰、挪威、英国、苏联、澳大利亚、马来西亚各一篇。

会议期间，分两组同时进行。全部论文安排在二十一个分组中宣读。论文的内容以测试和系统诊断为主要课题，共有十八篇，其中四篇是论述微处理机和 PLA 的测试。自检也是个大课题，共七篇文章，包括评估与设计。用各种方法和概念来评估系统的可靠性和性能的论文共十四篇。有关存储器编码有七篇，验证硬件设计的正确性有三篇，其它内容包括线路与系统的容错设计，采用软件手段改进系统的可靠性，提高软件本身的可靠性等。

二、容错计算系统

随着计算机在各个领域里被广泛应用，计算机在各种军事系统、工业系统和经济机构中都起了关键的作用。在一些实时系统中，如果计算机因故障而停止工作或者出现了差错，都会引起严重的后果，如经济损失甚至人的生命危险等。因此要求计算系统有高度可用性和高度可靠性。

由于计算系统的功能不断提高，系统的规模庞大，结构复杂，特别是用大规模集成和超大规模集成电路实现的计算系统，维护这样的系统，和

维护由中小规模集成电路实现的规模较小的系统相比，显然困难得多，因此要求有高水平的维护人员，工作量也很大。由于计算系统的维护费用大幅度的提高，使人们不得不重视计算系统的可维护性。

总的来说，对计算系统提出了新的要求——可用性、可靠性和可维护性。会议上介绍的容错计算系统的设计，都很重视这种新的要求，尽量使系统能够自动处理更多的故障。允许人工维护的系统，应为维护人员提供更多的数据，协助他们进行维护。意大利的语音和数字网的数字电子交换机AFDTI的可用性要求是0.999985。第一台在1976年安装，以后有三台陆续在罗马、尼普斯和米兰安装投入使用。

这次会议上有一个关于商业容错计算系统的分组，说明容错计算技术发展的程度，足以应用到商业容错计算系统中。因为宇航、军用系统为了达到高可靠性，是愿意付出很高的代价采用容错计算技术的。但投入市场上的通用计算系统，肯定是经过仔细的调查研究，认为容错性能即使提高了产品的价格，但在商业竞争中还是处于很有利的地位的。

下面介绍几个商业容错计算系统以及其它的容错计算系统。

(一) Sperr univac 1100/60 信息处理系统

该信息处理系统是中型的通用机，已生产100台。据说我国已订购2台。处理机及快速存贮器用ECL线路，每台机器采用36套MOTOROLA 10800 ECL位片式高速微处理机，输入输出采用TTL线路，16K主存采用MOS。

指令处理机是微程序控制的，特点是由大量的4位片微处理机构成，采用了美国Carnegie Mellon大学Siewiorek教授的多处理机容错计算系统的设计思想。系统的设计很重视并且兼顾了可用性、可靠性和可维护性。系统中有一个系统维持处理机SSP (System Support Processor)。

1. 系统维持处理机SSP负责的功能是：

- (1) 管理系统的划分；
- (2) 当发现控制存贮器出现故障，将正确的微程序重新装入；
- (3) 注入故障以检测关键部件，如检测故障的部件和负责系统恢复的部件，以保证这些部件能够正常工作。系统设有注入故障的指令。

2. 这个系统的维护手段分成四级:

(1) 自动登记错误。

(2) 诊断程序。

(3) 扫描比较——执行子程序将测试数据送入扫描网络, 扫出结果与表格中的正确结果进行比较。

系统内有逻辑分析器, 在每个微指令周期内, 重复两次取样并自动保存任何 16 个点上的 1024 个相继的状态。

(4) 人工维护——与远距离的维护中心连接, 可得到有经验的维护人员的协助。

3. 故障的检测在不同的部件采用不同的方法:

(1) 算术运算和控制部分用双重冗余和比较的方法。双重冗余使用两条数据线, 四个处理机。四个处理机分为两组, 每一组由一个主处理机及一个副本处理机组成。主处理机(主数据线)的结果与副本处理机(副本数据线)的结果相比较; 结果不符时换另一组处理机。

(2) 主存用检错/纠错编码。

(3) 控制存储器存放微程序用奇偶校验。数据通路中 100% 的单个故障以及控制逻辑中相当多的单个故障能被检测。检测故障的线路, 占处理机中线路的 15%。

4. 系统设计的特点:

(1) 失效率最高的存储器和利用率最高的数据总线均有检测故障的功能。

(2) 微程序存放在 LSI 存储器内, 因对 LSI 存储器来说, 采用检错/纠错编码, 附加线路的代价不大。

(3) 大量使用微处理机。

(4) 功能逻辑的设计与检测故障的线路设计是结合起来考虑的。

5. 从错误中恢复的过程:

当发现故障时, 通过硬件强迫连续执行“不操作”微指令, 使瞬态的失效消失。

执行“恢复”微子程序, 以分析失效原因, 给系统软件送去故障状态字, 使判断能否恢复系统的状态并重新执行。不能恢复时, 向系统支持处理

机发中断。

如属于控制存贮器的失效，重新装入正确的微程序（也可以反码形式装入正确微程序，读出时取反），或将指令处理机的状态移植到另一处理机。

（二）日本电气的 ACOS 800/900 (ACOS S800/900) 系统

该系统是大型通用机，截止 1979 年年底，已安装 30 台。用 ECL 的大规模集成电路，门数多于二十万。最大的系统包括有 CPU 2 台；IOP—输入输出处理机 2 台，以及外围设备和通讯设备。每台 CPU 由一至二台 EPU (Execution Processing unit 执行处理机) 及系统控制部件 (SCU) 组成。每台执行处理机 (EPU) 由控制存贮器 (CS—Control Storage)、快速存贮器及 2 台执行部件 (Eu—Execution unit) 组成。

系统通过双重冗余来实现容错性能，每个周期内，两个执行部件进行比较，两个输入输出处理机 (IOP) 也进行比较。

克服间断失效的措施是：处理机可重新执行指令，外围设备可重新执行输入输出命令。输入输出处理机除了控制输入输出命令以外，还起可用性、可靠性、可修理性处理机的作用。它的软件实现以下功能：

- (1) 重新执行指令；
- (2) 卷回；
- (3) 存贮器的重构；
- (4) 登记错误；
- (5) 诊断；

输入输出处理机的软件存放在局部存贮器内，出现故障时可从磁盘重新装入输入输出处理机软件。

系统中可恢复的故障为 80%，不可恢复的故障为 20%，主要由主存贮器及通讯部件所引起。

（三）AMDAHL 470 V/6 计算机

1. 该系统包括：

- (1) 指令部件——9 级流水线，控制指令的执行。
- (2) 执行部件——2 级流水线，对数据进行运算主存、高速存贮器；

通道。

(3) 诊断处理机——小型计算机。

(4) 通道诊断处理机。

主要用 ECL 大规模集成电路，外部接口逻辑以及部分存贮器用中规模集成电路，主存用动态 MOS。

由诊断处理机执行检查程序，以监督和控制计算机的状态。检查程序是用数据序列将主机从任何状态重置在确定的起始状态。在这个起始状态中，大部分点上以及存贮器的值是已知的。用序列重置计算机时，每执行一步，扫出并观察分析各点上的值，事实上只观察那些已取了已知值的各点。对全部要被扫出的点的值取异和，每次 16 位以形成 16 位的检查和，再与予期的值比较，不相符时说明硬件出了故障。这种测试可看成是几千条线的逻辑分析器，最后一步扫出的值约有八千个。

2. 重置序列可以两种方式执行：

(1) 检测方式——在执行重置完成一个功能后，比较检查和，不相符时，以隔离方式执行重置序列。

(2) 隔离方式——每个周期比较检查和，由脱机计算机利用磁带上数据库（约 10 兆字节）的数据进行分析，以找出故障出现的位置。

在诊断控制台上，还允许提供屏蔽字，即将各点的值扫出形成检查和时，可将某些点上的值屏蔽。

（四）日本铁路技术研究所的失效安全与容错计算机

该计算机将用来替换目前用继电器组成的时序机，以控制铁路上的信号灯。

对铁路信号来说，红灯是安全的输出，因为不会引起撞车事故。所谓失效安全，就是计算机的任何失效，不会发出不正确的“绿灯”信号，而只发出红灯信号。

采用三重冗余在总线级表决，来实现容错性能。也是采用了 Carnogie-Mellon 大学 Siewiorek 教授的基本思想，即在总线级表决的三重冗余多处理机系统。

采用三个同步的处理机，三个表决线路，三个存贮器；信号送出以前，再由外部表决路线进行表决，表决在每个微指令中进行，其特点如下：

(1) 表决线路有所谓“与”工作方式。当处理机从存储器取出最关键的数据时,这种工作方式可以防止由于双重故障而发出不正确的绿灯信号。

(2) 采用失效安全的比较线路。

(五) 计算机网中可重构的前端处理机

美国 Ohio 州大学用片式计算机模块 (SCM·Sliced Computer Module) 作为基本模块,来设计用于计算机网和分布处理系统中的可重构的前端处理机 (FEP—Front End Processor)。主要功能是在计算机网的主机之间,处理信息的交换和文件的转移等工作。

基本思想是将计算机分为完全等同的几块,称为片式计算机模块,每一块是完整的计算机。例如一个 8 位的计算机可以由两个四位的 AM2900 电路组成,可采用位片处理方式,即新的微程序算法,协同系统中各基本模块的信息处理。系统有一个监控处理机,若干个通讯处理机、作业处理机和若干备分。当相继出现了故障后再没有备分来替换出了错的模块时,系统可在降低了性能的情况下工作,也就是使字长缩短。

(六) 容错多处理机系统的一致性单元

一致性单元可作为各处理机之间的总线接口,使各处理机交换信息时,能保证数据的一致性。即用硬件来实现 SIFT 系统的系统软件的数据一致性算法。

设 n 是系统中处理机的个数,如果允许系统中同时有 m 个处理机出现故障,为了保证数据的一致性, n 必须大于 $3m$ (即 $n=3m+1$),信息应按算法经过 $(m+1)$ 次的交换。

设计了包括四个处理机的容错系统的一致性单元。共有四个控制器和四条总线。四位字长的控制器用 MNOS 在一块尺寸为 100 平方密耳 (mil^2) 的芯片上实现。

三、容错计算系统的操作系统

(一) SIFT 的系统设计与实现

SIFT 容错计算系统用于控制节约燃料的新型飞机的飞行过程,主要由软件实现系统的容错性能。有关这个系统在两个会议上都有论文。

SIFT 系统的可靠性指标是 10 小时飞行中,失效几率少于每小时 10^{-10} ,也就是每次飞行的失效几率少于 10^{-9} 。

系统用八个 Bendix 公司的空间计算机 BDX 930 按星型连接起来 (32K 16位 CMOS 存贮器, 每秒百万次), 各个计算机之间的信息交换由广播式的通信接口处理。原来的硬件设计, 各处理机之间的数据, 是通过特别设计的总线, 按需求方式传送的。经过对系统进行模拟的结果, 证明用一套分时的总线来传送各处理机之间的数据, 在最坏的情况之下延迟太长, 不能满足要求, 因此对原设计进行修改。新的设计是各处理机直接连接, 采用广播方式传送数据。

各处理机在 50 微秒内同步, 由软件负责周期性的重新同步。

操作系统的功能包括作业调度, 处理机同步, 输入数据的一致性, 处理机之间的通讯, 掩盖错误, 检测错误, 系统重构, 输入输出等。有以下的特点:

1. 适应性表决——按作业的不同要求, 选择三个或五个处理机做相同的运算, 然后表决。

2. 时钟同步算法——用 $3N+1$ 个时钟, 可以掩盖同时在 N 个时钟中出现的故障。

为了验证系统的设计能否满足这样高的可靠性要求, 必须通过严格的分析, 用数学证明。系统尽量使用最简单的硬件, 经过大量的工作, 用 PASCAL 语言编制的系统软件不超过一千行。

SIFT 系统用分层结构, 分层结构如下:

1. 最低层是硬件。

2. 最低层的上面是由四个模块共同实现的 SIFT 虚拟机, 提供每个处理机中的局部容错性能即检测错误、数据 (缓冲区) 管理、表决和局部的作业调度。

3. 虚拟机上面的一层提供全局的容错性能, 如同步和系统的重构。SIFT 有八个处理机, 相应有八套预先计算好的表格, 可根据出现故障的部件的各种组合, 按这些表格分配和调度任务。

4. 在操作系统的上面是应用作业, 如飞行控制、导航等。

对系统设计的验证是首先建立失效的数学模型, 采用分离事件的马可夫模型。各个状态的转换对应于处理机的随机失效 (包括永久性和瞬态失效) 和容错措施。如果要用一般方法验证设计与模型相符, 需要处理的信

息太多，也太复杂。因此引用分层的模型（即不同程度的抽象），只要证明每层是上一层的进一步精细化，就能证明实现的系统和可靠性模型是一致的。

模型中由于出现故障而引起的状态转换的几率，是根据标准部件的可靠性数据得来，由于容错措施而引起的状态转换的几率以及延迟，是通过在另一计算机上进行实验，得出对这些量的比较符合实际的估计。实验时用 Data General S230 计算机来模拟由 SIFT 系统控制的美国空军 T 39 型飞机，通过将数据送入 SIFT 的存储器来模拟故障。

这种验证的途径，虽然仍有一定的限制，但还是能作为进行分析的基础。SIFT 系统的硬件、测试设备等已在 80 年 5 月调试完毕，各个模型规格和执行软件的工作等也已完成，预计在 80 年 10 月完成综合整个系统以及测量、证明等工作。

（二）容错“限期机构”在卫星上计算机的应用

卫星上计算机实现各种功能，其中最复杂、在时间上要求最严格的是飞行高度的控制。控制环节的失效将使卫星晃动而最后失去控制。可用“限期机构”来实现实时系统的容错软件，以提高系统的可靠性，防止由于意外、破坏事件或硬件/软件设计中余留下来的故障引起系统的失效。

实时系统提供的功能必须满足某些时间上的限制。“限期机构”方法与“恢复块”方法都是实现容错软件的方法，也有相似的地方，即对每一单元的计算，都提供两种可能的算法，但“限期机构”能满足实时系统中的时间限制，而“恢复块”只处理一般的软件故障，包括逻辑错误。

在“限期机构”方法中，第一种算法提供质量较好的结果，第二种算法是比较简单的确定性的算法，可保证在限定时间内提供可以接受的结果。执行过程中，调度程序将先安排第二种算法的执行，然后执行第一种算法。如果第一种算法能够在限定时间内执行完毕，便选用第一种算法的结果，否则用第二种算法的结果。

“限期机构”方法采用路径 PASCAL (PATH PASCAL) 语言，因为用高级语言书写的程序，正确性的验证较为简单。有利于提高软件的可靠性。“限期机构”方法被用到模拟的卫星上控制飞行高度的子系统。卫星上计算机 (OBC—On Board Computer) 的模型是根据美国宇航局八十

年代很多项围绕地球运行的任务的标准卫星，即MMS (MaTtimissio Modular Spacecraft) 卫星研制的。

这种方法是在PASCAL 程序语言的基础上增加一些语句和短语。可以定义限期进程 (Process)；定义第一种和第二种算法，能规定某种运算在特定的时间开始，在规定的时间内作出响应等。

四、其它容错计算技术

(一) 自 检

会议上有关自检方面的论文，包括自检线路的设计，如非同步自检时序线路，阈值集成注入逻辑安全自检线路。也有关于自检部件的设计，如自检的检测处理机和多微计算机系统自检的总线集中控制器的设计。这些设计是以自检模块作为基本模块，相互连接的自检模块又由自检的检查线路去观察和监控。

评估自检线路的论文，是对不同方案的自检线路作定量的评估，进行比较后作出选择。日本工业大学当麻教授等的论文，是在Sum和Avizienis提出用信号可靠性对自检线路作定量评估的基础上，改进了原来的算法。对于大的线路，用原来的算法，计算很复杂。改进为较快的递推方法，更适合用计算机进行运算。这种算法的应用范围更广，可以适用于自检的系统，即包括了自检的功能线路和自检的检查线路。按三个参数，即信号掩盖性、信号检测性和信号不可靠性对自检系统进行评估。

斯坦福大学Lu的工作，是评估两种不同实现方式的自检反馈移位寄存器，两种不同的实现方法是：

1. 双重冗余；

2. 奇偶预测；

评估时作为依据的两个参数是：

1. 测试输入比 (TIF-Testing Input Fraction)；

即可检测故障集合中某个故障的那一部分输入编码字。

2. 安全输入比 (SIF-Secure Input Fraction)；

即当故障集合中某个故障出现，而仍不产生不正确输出编码字的那一部分输入编码字。

将对应于某个故障的上述参数与该故障出现的几率相乘，并取对应于

全部故障的累加和（即权和，以故障出现的几率为权）。用 PASCAL 语言编制的程序来计算两种移位寄存器的 $\overline{TIF}$ 值和 $\overline{SIF}$ 值，比较结果指出，第一种实现方式的线路自检效果较好。

法国 Viaud 等的工作，提出了串行自检线路，是从理论上对完全自检线路的概括。

（二）大规模集成电路的测试

HAYES 教授针对大规模及超大规模集成电路很复杂的特点，引进称为矢序列的 $n \times m$ 矩阵，以表示相继 m 个周期出现 n 位总线上的信号。再对矢量序列定义一些操作，也就是建立数学方法，以表示复杂数字系统的测试。换句话说，可以用很简单的形式来表示 LSI 及 VLSI 电路的输入/输出测试数据。

ROBACH 等的论文针对微处理机的测试，利用应用程序作为微处理机的测试程序，但编制该程序时，必须相应分析两个流图，即表示应用程序的控制流图和表示应用程序所用到的硬件的数据图。以 Z80 微处理机作为试验性的系统，处理法国电话交换系统中的记数脉冲。另一篇论文是有关位片式微处理机的测试，以 AM 2903 电路为例。

（三）新的电路设计方法

由于大规模集成及超大规模集成电路的密度很高，芯片上的线路很复杂，引出腿又少，要按线路所实现的功能来产生测试序列是很困难的。会议上有三篇论文提出新的电路设计方法，使测试电路时，不再产生测试序列。

美国 IBM 的 S·J·HONG 及大阪大学的藤原等，独立地进行了基本上是相同的工作，得出了相似的结果。即怎样设计 PLA（可编程序逻辑阵列）使可以用通用的测试序列来测试实现任何功能的 PLA，也就是不再需要按 PLA 实现的不同功能来产生不同的测试序列。基本思想在于增加一些线路，包括增加译码器的控制信号，增加一个移位寄存器，在“与”阵列中增加一行，在“或”阵列中增加一行作为奇偶校验，和增加奇偶校验的线路。

美国斯坦福大学的 E·J·Mcclusky 等提出结构式的利于测试的设计方法。即在片上增加一些线路，主要是多路开关，将组合线路分解为多个

子线路。分解以后，每个子线路的输入端比较少，可用输入信号的全部可能组合，来测试每个子线路。以划分TTL 74181 运算器/功能发生器的电路为例，附加的线路为30%，划分以后可用 2^{10} 个输入图形对电路进行测试，没有划分以前，需用 2^{14} 个输入图形，图形数减少了16倍。这种设计方法的缺点是，由于增加了两层门，也相应增加了延迟时间，延迟时间约增加30%。

(四) 编码理论

1. 算术码对单方向两列错误的检测性

USAS 曾推导出两个邻近列的单方向错误的检测性公式是：

$$\text{检测性} = \frac{\text{能被编码检测的错误图形数}}{\text{全部可能出现的错误图形数}}$$

他推导的公式只适用于两类算术码，即：

- (1) 检查和码 (Checksum Code);
- (2) 低成本余码 (Low Cost Residue Code);

当数据块的长度较长时，必须通过大量的数字运算，才能估计这些表达式的渐近值。日本 Goto 的论文推导出适合于任何类型算术码的两列错误的检测性公式，渐近值的估计也比较方便。

2. 磁带上的随机双道错误纠正

磁带上的信息密度愈高，失效出现的几率也愈高。例如同样一块损坏的面积，在信息密度高的磁带上，受影响的位数就愈多。目前国际上的磁带信息密度一般是1600 bpi (每英寸的位数)或6250 bpi, 但已陆续有更高信息密度的磁带如3M890 磁带机的信息密度为34400bpi。今后还将推向50000 bpi的目标。因此要求有功能更强的编码，论文以九道和十道信号为例，讨论了随机双道纠错码。

3. 适用于移位寄存存贮器的单方向错误的编码

大规模集成电路存贮器的失效，具有单方向错误的特点，即在一个信息字里，有多个位向同一个方向失效，如几位同时固定是1或固定是0。从存贮器的某一地址取出数据时，取出失败或者错误地从多个地址一起取出，都引起单方向的错误。因此大规模集成电路存贮器的失效特点，促使

编码理论向新的方向发展。

论文用算术冗余的检查码 (ARC—Arithmetic Redundancy Check) 来代替循环冗余检查码 (CRC—Cyclic Redundancy Check)，但所用的模底要满足一定的条件。适用于磁泡存贮器，电荷耦合器件存贮器和磁带等，即较长的字符块里任何一道中的多个单方向错误，信息率也高于 CRC 编码。

五、日本大学里的容错计算工作

在日本的大学里进行的容错计算工作，主要是理论工作。我们在大阪大学参观期间，和工学部电子工程系的藤原、工学部通讯工程部的中野进行了座谈。他们的研究课题主要是系统诊断，大规模集成电路的测试，编码理论，自动机理论，程序的测试等。特别是藤原，先后发表了不少论文。广岛大学正在试制一台自诊断容错计算系统，其它大学正在进行的课题如下表所示：

学 校	负 责 人	课 题
东京工业大学 东京大学	当麻教授 INOSE教授	自检线路，纠错编码 测试的产生，利于设计的测试方法
京都大学	三根教授 矢岛教授	可靠性，评估，多值逻辑 系统诊断，程序测试
广岛大学	树下教授 尾崎教授	系统诊断，自动机理论 可靠性理论，冗余理论
九州大学	香田教授	三值逻辑，Petri 网等

这次在参观东京大学、大阪大学和理化学研究所的过程中，看到他们比较好的条件，例如东京大学的计算机中心规模很大，难波教授的光学实验室和离子注入设备等的条件都是很好的。也看到他们的研究工作深入，科研成果比较多。这和他们选择研究课题时能够抓住关键的问题分不开的。即使是理论课题，往往是实际工作中提炼出来的重大问题，因此研究成果对工业和其它领域起到比较大的促进作用。例如容错计算工作中的计算复

杂性结合系统的诊断,新的电路设计方法结合大规模集成和超大规模集成电路的测试,图的表示结合多故障的诊断,图像的分析结合血管的图像,立体的断层像结合神经细胞,人工智能探讨一些最基本的概念等。同时也看到了研究生在科研工作中起到了骨干的作用。

六、收获和几点建议

这次参加第十届国际容错计算会议,代表我国宣读了论文,促进了这方面的科学工作的交流;对于国际上容错计算技术的重要性、应用、水平和最新发展,有了比较深入的了解。归纳起来有以下的收获:

(一)更加具体的认识到容错计算技术的重要性

1. 随着计算机在各个领域的广泛应用,特别是控制一些关键性的工业和机构的计算系统,必须在可用性、可靠性和可维护性三个方面都满足很高的要求,容错计算技术愈来愈引起人们的重视。

2. 随着大规模和超大规模集成技术的发展,计算系统硬件的价格下降,使容错计算系统的实现更切实可行,这就为容错计算技术的发展提供了很有利的条件。目前除了宇航、空间计算机等必须采用容错技术以外,应用在很广泛领域里的计算系统都包括容错性能,就是市场上能买到的计算系统也都采用了容错技术。今后各种类型的计算系统的设计,都会更多的采用容错计算技术。

3. 由于大规模集成和超大规模集成电路的集成密度很高,芯片上的线路很复杂,采用一般的方法进行测试非常困难。因此提出了新的电路设计方法,使超大规模集成电路和系统的测试比较方便。过去要按电路的不同功能,产生不同的测试序列去测试这些电路,虽然是用计算机产生这些序列,但产生这些序列的程度的难度大,工作量也很大。采用新的设计方法,就不再需要产生这些序列,可以用通用的测试序列去测试不同功能的大规模集成或超大规模集成电路。

4. 超大规模集成技术和容错计算技术之间的密切关系已经是相互依存的关系。例如超大规模集成电路中出现的故障,简单的故障模型已经不适用,因此促进了检测故障的功能更强的编码技术的发展,而新的设计方法、新的编码等使超大规模集成电路的使用比较方便。会议上介绍的容错计算系统,大部分是以微处理机作为基本模块实现的。最近看到10月1

日至3日在美国纽约省举行的集成电路与计算机会议 (ICCC 80) 的报导, 这是第一届关于大规模系统中线路与计算机的国际会议, 论文包括大规模集成电路实现的大型系统 (TBM)、容错计算技术及超导等。可以看到, 超大规模集成技术与容错计算技术之间是相互促进、相互依存的关系。

(二) 对于当前已成熟的几种容错技术, 可逐步应用到我们的工作中去, 以改进可靠性。

1. 动态冗余技术;
2. 多处理机容错系统;
3. 双重冗余与比较;
4. 在不同级别上卷回以克服瞬态故障;
5. 存贮器采用检错/纠错编码。

(三) 对于当前正在发展和研究中的新课题的发展趋势有了初步的认识, 为我们在这方面赶超世界先进水平进行予研工作打下基础。

1. 各种新的冗余方案;
2. 新的电路设计方法;
3. 功能较强的编码;
4. 容错软件;
5. 按定量参数对自检线路或系统进行评估;
6. 系统的评估。

我们对集成电路和计算系统的可靠性要求很高, 应该加强容错计算的研究工作。对于我们的工作提出以下几点具体建议:

1. 对77-II型机考虑加上容错性能, 以提高可靠性。

2. 我们要利用和学习国际上新型的16位微计算机如Z8000和M68000的特点, 研制军用微计算机, 研制中尽量采用一些已经成熟的容错技术。因为存贮部件的失效率是最高的, 主存贮器可以采用检错/纠错编码, 即使主存贮器单元里出现特定的故障, 仍不影响系统的正常工作。研制微计算机的PLA电路时, 可以考虑采用新的设计方法, 使PLA电路的测试标准化。有利于提高系统的可靠性。可以增加快速存贮器来保留机器的状态, 在出现了故障以后, 在微程序一级卷回, 这样可以克服瞬态故障的干扰。

3. 根据目前国际上容错计算技术的发展新动向, 安排少数人力, 做一些和我们的工作关系比较密切的容错计算研究课题。例如考虑适合于我们任务的容错计算系统的冗余方案。设计 PLA 来实现给定功能时, 通过软件提高 PLA 的设计自动化。由于我们的任务, 对可靠性的要求很高, 也有必要开展对计算系统的评估工作, 以验证系统能否满足可靠性的要求。