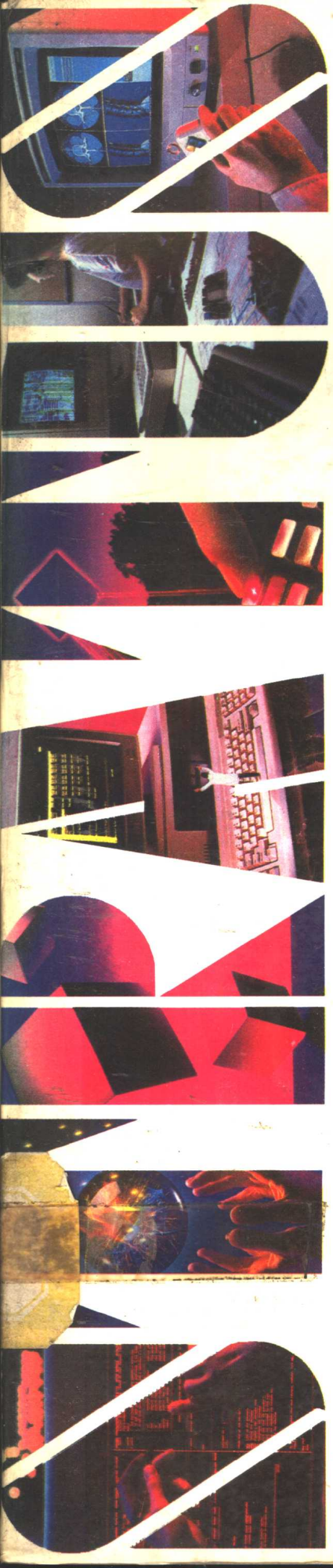


# 容错技术与STRATUS容错计算机

杨孝宗 编著

哈尔滨工业大学出版社

# 容错技术与STRATUS容错计算机

杨孝宗 编著

哈尔滨工业大学出版社

（黑）新登字第4号

## 内 容 提 要

本书从内容上可以分为两个部分。第一部分为对容错计算技术有关内容的阐述，包括容错技术的基本概念、可靠性的估算、实现容错的基本方法，诸如硬件冗余、软件冗余、检测技术。第二部分提供一个典型的容错系统的实例——美国的STRATUS容错机。以此实例为依据说明容错系统的具体实现。这部分从原理上介绍了STRATUS机的基本构成、容错设计、系统软件以及使用原理，通过介绍，将为读者展现一个较为完整的容错系统，从而加深对第一部分内容的理解。

本书是对容错计算技术原理的介绍，可以作为大学计算机专业本科生的教材，也可作为研究生及工程技术人员的参考资料。

**容错技术与STRATUS容错计算机**

杨孝宗 编著

哈尔滨工业大学出版社出版

新华书店首都发行所发行

黑龙江省绥棱县印刷厂印刷

开本787×1092 1/16 印张 18.5 字数424千字

1993年8月第1版 1993年8月第1次印刷

印数 1-1500

ISBN 7-5603-0439-7/TP·38 定价：精18.00元 平12.00元

## 作者简介

杨孝宗 1939 年生，辽宁人，现为哈尔滨工业大学计算机系教授、计算机研究所副所长、中国计算机学会容错计算专业委员会副主任、硬件容错学组组长、哈尔滨市政府咨询顾问专家委员会成员。

杨教授 1964 年毕业于哈尔滨工业大学计算机专业。毕业后留校任教，并从事计算机系统结构、并行处理、Ada 语言应用技术等方面的研究。自 1973 年以来，一直从事容错计算技术的研究、容错计算机的研制，以及软件容错的研究，取得了多项成果，在国内外发表了多篇论文，曾获部级科技进步奖。在哈工大 1973 年开始的“部件级协同二模容错系统”研制中曾任调机组组长。

自 1982 年到 1984 年曾在美国卡内几－梅隆大学 Carnegie－Mellon University）计算机系与 D. P. Siewiorek 教授合作从事容错技术以及 Ada 语言的研究，提出了软件方法实现的容错系统设计。回国后继续从事硬件容错和软件容错的研究以及容错教学工作，编写了全国高校统编教材《Ada 语言》一书，曾多次出任国内外容错计算学术研讨会的程序委员和分组主席。

从 1988 年开始，杨孝宗教授开始了对美国 STRATUS 容错机的研究和应用，带领研究小组从事了 STRATUS 的应用工作。

目前，杨孝宗教授同时在辅导多名博士生和硕士生，在容错技术研究中作更深入的研究。

# 编　者　的　话

在社会进入到信息时代的今天，到处都可以看到计算机的应用。但是，当计算机进入到关键部门的时候，它的可靠性问题将变得异乎寻常的重要。人们宁愿花更多的经费来得到高可靠的计算机，而不愿看到因计算机的失效而造成无法估量的生命和财富的损失。利用传统的办法可以提高计算机的可靠性，像严格挑选元器件、改善工艺条件等等。但是，这种可靠性的提高局限性很大。在这种情况下，容错技术逐渐地被人们所认识，而且迅速地发展起来了，以致于大量的容错计算机进入了国防市场。与此同时，研究和应用容错技术的专业队伍也得到了迅速地壮大，有关容错技术的大量书籍和资料也不断地介绍给读者。

作者期待着通过这本书能为容错技术的应用、普及、发展贡献一份力量。在编写过程中，作者把授课的讲义集中成一个初稿，又补充进了一些作者的科研成果，并参考了国内外同行专家所做的工作，最后形成了这本书。

本书以原理性介绍为主。第一部分包括容错技术的基本概念、可靠性的基本估算、硬件冗余、软件冗余、检测技术等内容的介绍。在这一部分，主要论述了容错技术的基本原理和主要实现方法。为了加深对这些内容的理解，本书在第二部分（从第七章开始到最后）介绍了一个典型的容错系统实例——STRATUS容错计算机。考虑到集中并深入地介绍一个系统，可使读者易于建立一个完整的容错系统的概念，因此，作者选择了STRATUS进行分析。当然，目前在国际市场上出现了多种容错计算机，像Tendam，VAX-ft3000等，它们各自都有不同的特色，也都集中了各家技术人员的才能和智慧。因篇幅所限，这里仅选择了STRATUS一种容错机。该机的容错设计方案与作者科研中所采用的技术途径颇为相似，写起来也较为方便。在这一部分中，包括了STRATUS机的系统介绍，容错设计原理，系统软件和使用原理。

如用作教材，本书的授课时数可在40学时到50学时之间。

本书承蒙董浩教授担任了主审，为本书提出了许多宝贵的意见。

郭威编写了第九章、第十章、第十一章、第十二章。张淑敏翻译了与第一章和第六章有关的英语资料。刘英贤参加了第五章的编写。张勤也参加了本书的部分编写。其余章节由杨孝宗编写，并由他对全书进行了统编。

作者在编写本书的过程中得到了国内同行专家的热情帮助和鼓励，得到了陈光熙先生的热心指点。尤其是傅佩琛教授、杨士元教授、邮萌教授、孟永炎教授、徐拾义教授及时地向作者赠送了各位所编著和翻译的容错书籍。作者还得到了美国D·P·Siewiorek教授、Fernandaz教授、日本的藤原英二教授和当麻喜弦教授送来的书籍和文章。作者向以上各位先生表示衷心地感谢。我们还要特别感谢的是美国STRATUS容错电脑公司的各位先生们，陈源瀚先生、陈恒先生、张大虎先生、梁栋材先生、凌英祥先生以及丁晓娟小姐热情地支持本书的编写并及时地向作者提供有关资料和技术等各方面的帮助，李泊澍先生、廖广廉先生以其熟练的技术给予了作者以极大的帮助。杨平先生、林海先生也为此书提出了宝贵的意见。作者向各位先生深表谢意。

因水平所限，本书难免有错，敬希广大读者指正。

作　者

# 序　言

容错计算技术随着计算机可靠性需求而产生，随着关键应用的普遍而发展。尤其是计算机被广泛地应用在各行业的情况下，高可靠性技术变得越来越重要，成为计算机应用是否成功的关键，使得容错技术得到了飞速发展。今天，容错技术已经不仅是一门学院内的研究技术，而是已经走向了市场的成熟产品，事实上，各种不同型号的容错计算机产品正纷纷投向市场。

美国 Stratus 容错电脑公司适应这种发展形式，1982年推出了第一台紧偶合体系结构的硬件容错计算机，以后不断地更新换代，现在已经成为国际上在金融业、通信业、交通旅游业、生产企业管理和信息处理等领域中很受欢迎的主要机种之一。

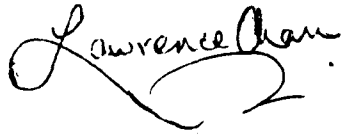
近几年来，Stratus容错计算机在中国普遍使用，在中国1990年第十一届亚运会获得好评的影响下，各行业如银行、通信、交通、旅游等方面纷纷采用并发挥良好效果。美国Stratus容错电脑公司与中国有着十分密切的关系，尤其是与中国的企业家、部门负责人、科学家一直保持着非常好的合作关系。

杨孝宗教授等先生们编写的“容错技术与Stratus容错机”一书就是这种合作的结晶。在这本书中，首先从容错技术的基本概念开始，对容错技术的基本理论和实现原理进行较为全面的阐述，第二部分选用了 Stratus 容错计算机作为容错实现的具体实例，介绍了Stratus的系统结构、容错设计原理和软件系统的构成原理。它将会给读者一个完整的容错系统的概念，并进一步加深对容错实现的理解。

中国的科学技术发展非常快，水平也非常高，在研究和应用中做了卓有成效的工作。杨孝宗教授等各位先生集中了多年的研究成果和教学实践，并得到了国内外同行们合作，写出了这本书。它对中国以及国际容错计算技术的研究人员和教学人员来说，将是一本很好的参考书，对从事计算机设计和应用的人员也将是很有价值的。我相信，它将会受到海内外有关学者、技术员、计算机企业家的欢迎。

祝贺中国的计算机科学与工程技术，尤其是容错技术将得到迅速的发展并不断取得辉煌成就。

美国容错电脑有限公司



远东区总裁

**陈源瀚**

**1992年9月**

# 目　　录

# 第一章 绪 论

## 第一节 容错的概念及容错技术的重要性

容错（Fault Tolerance），顾名思义是“容忍出错”之意。对于任意一个系统而言，都希望在内部出错的情况下，系统的功能仍能保持正常。因此，容错是一个具有广泛意义的概念。本书集中研究的是计算机系统的“容错技术”（Fault Tolerant Computing），严格地讲，计算机容错的含意应该是具有“在内部出现故障的情况下，计算机仍能正确地运行程序并给出正确结果”的能力。这里所指的内部故障，既包括硬件故障、软件故障，又包括环境和操作人员误动作引起的故障。

计算机的容错能力，直接反映了计算机系统的可靠性，是人们最为关心的问题，也是计算机系统最重要的技术指标。然而，在目前情况下，计算机的可靠性还不很高，这严重地影响着计算机的应用。另外，在计算机的许多技术指标中，都有一个比较明确的数值来衡量，如内存容量等，而唯独可靠性这一栏却几乎是空白的，这说明可靠性的研究还有相当艰苦的工作等待人们去做。

可以说，可靠性问题在计算机一问世就被提出来了。世界上第一台计算机ENIAC使用了18 000只电子管，当时电子管的失效率是$10^{-4}$/小时，这样，该机的平均无故障运行时间只有30分钟左右，对于如此的可靠程度，这台机器几乎无法使用。早年的Bell Relay计算机，为了能正常工作，提高可靠性，采用了两次计算并比较其结果、检错编码等技术。

早期计算机对可靠性的要求尚且如此，当代计算机自然就更加迫切了，其原因可以归纳为如下几方面：

①随着计算机技术及应用的飞速发展，计算机的功能越来越强，规模越来越大，复杂性也越来越高，这本身意味着系统的出错概率必然要增大，因此，不采取一定的措施来提高计算机的可靠性是不行的。

②当今社会已经进入了信息时代，大量的信息需要进行处理、传递和存贮。计算机作为信息系统的关键设备，担负着社会的重任，特别是随着计算机应用领域的不断扩大，使越来越多的部门，尤其是关键部门，对计算机呈现出了很强的依赖性。象金融系统、航空、宇航、国防、工业控制等领域，一旦计算机发生故障，那将会带来无可估量的生命和财产的损失。

③计算机的工作环境已经从特定条件下的机房，转移到了条件较为恶劣的场所。如车载、机载、野外以及加工车间等。计算机要承受强烈的振动及温度和湿度的波动，还有强电及核幅射的干扰等各因素的影响，这极大地增大了计算机出错的概率。

④计算机用户的总费用基本上包括两大部分：设备购置费和维修服务费。随着硬件技术的飞速发展，使得硬件的价格下降很快，但是，复杂性的提高，又使得维修费用提高了。经验表明，系统可靠性越高，则维修次数越少，而且维修的难度也越低，这三者的关系可由图1-1来表示。由图可看出，可靠度越低，维修费越高，甚至高得无法承受。

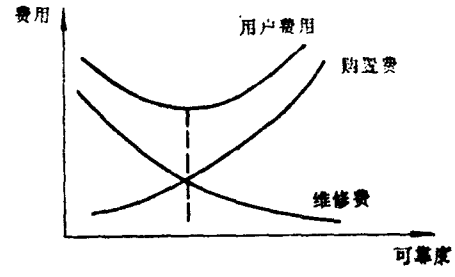


图1-1 费用与可靠度的关系曲线

⑤计算机软件技术的发展十分迅速，其规模和复杂程度越来越高，这样，软件本身的出错率也在增大，因此，软件系统的可靠性问题十分突出。

⑥随着计算机应用的不断普及，形成了一个庞大的计算机用户队伍。在这个队伍里，既包括系统开发人员，也包括操作人员。在这些人员中，技术水平的差异非常悬殊，这样，来自人的差错而造成的计算机故障概率也在不断地增大。这就要求对计算机系统的设计应尽量做到使用户方便，这就会对用户水平的要求越来越低。

由以上分析可以看出，计算机系统的可靠性问题变得越来越迫切，已达到了不解决，计算机就无法使用的地步。假定一个系统某时刻的可用性为99%，看起来已经足够高了。仅有1%的不可用概率，差不多每个月中有1/8停机时间。假定这个系统为ATM（自动提款机）服务的话，如果该1%的时间出在用户取款高峰期，那么影响就大得不能忽视了。

1979年11月9日，设在美国科罗拉多州的北美防空司令部，由于其计算机系统出错，而错误地发出了“敌人导弹袭击美国”的警报，造成了极大的混乱。不仅经济上造成了很大损失，政治上也受到了极大的影响。

在美国的军事演习和武器实验中，多次因计算机失误而造成了很大的损失。例如，60年代美国的空军中心就因为计算机出错，而多次使导弹发射失败。在1979年美国的一次军事演习中，由于计算机的失灵而打乱了演习的秩序。

在宇宙飞行方面，也曾因计算机的错误造成飞行失败，经济乃至时间上的损失是巨大的。

金融界使用计算机是比较早的，现在一些国家的经济命脉几乎建立在计算机系统上了。计算机的多次失误以及不法人员利用计算机作案，都曾造成过巨大的经济损失。例如，1989年东南亚某地区的股票交易市场计算机出错，使系统停止工作30分钟之久，造成交易市场的一片混乱。

数据库是社会最基本最重要的信息中心，它的规模也越来越大，因此，它的破坏对社会的影响是非常严重的。例如，意大利国家数据库在短短6秒钟内所破坏的数据，经过6年之久的时间才得到恢复。

目前，工业控制系统的自动化程度越来越高。计算机在这些实时系统中往往是一个中心环节。它的错误要么使整个系统瘫痪，要么使系统发生重大偏离而造成生命和财产的巨大损失。例如，炼钢高炉系统的失误会使整个高炉报废，联合钢带轧钢机也会因计

算机的错误使钢带拉断，或在瞬间突然堆积，或钢带指标不合格。由此使这一批钢材不得不拉回切割再次回炉。这里还可能包含着人身伤亡，也可能造成产品质量的下降，同时也直接影响了炼钢的产量。

在上述各种情况中，计算机往往工作于实时系统，这就不允许出错或尽可能少地出错。

从另一方面来看，即使是一个非实时系统中的计算机，因它的错误而造成的损失也是不容忽视的。尤其是可靠性本身意味着维修的频繁程度和困难程度。这是决定系统维修费用的关键因素。特别是当今维修费用很高，这笔开支往往高得使用户难以维持。如图1-1曲线所示。

总之，计算机的应用免不了要伴随着计算机的出错，它所造成的损失和影响是巨大的。人们不惜高昂的代价来换得可靠性的提高。在权衡由于可靠性的提高所增加的开支远远低于因计算机的失误所造成的巨大经济损失以后，人们更加充分地认识到了可靠性的迫切程度。

可以说，在任何时刻，人们都没有忘记计算机的可靠性问题。归纳起来，大体上可以分为两类问题：第一类是通过对计算机元、器件的严格挑选，提高老化筛选的阈值，提高制造工艺的质量等等，使系统尽量少出错，从而提高可靠性。系统不允许有故障的发生，我们称这样的技术为“避错设计技术”。但是，任何一个系统很难做到绝对不发生故障，对元、器件挑选的严格程度又不能无限地高。因此，避错设计技术对系统可靠性的提高将会受到很大限制。第二类是允许系统内部有故障的存在。通过容错设计技术消除故障的影响，使系统最终仍能给出正确的结果。这种高可靠性技术不是建立在严格要求元、器件和生产工艺的质量上，而是建立在“冗余”的设计上，实践证明，容错设计对计算机可靠性的提高是十分有效的。它的效果远远超过了第一类

计算机的容错设计技术已经被人们深深地认识到了，至少在目前，它是提高计算机可靠性的希望之所在。容错技术的研究已经形成了计算机科学的一个重要分支。

## 第二节　容错计算技术的发展历史

计算机的产生与发展的历史也就是容错计算技术的历史。从对容错技术的需求及其理论上的研究到各种容错技术的研究与应用，从专用容错机的研制到商品化的通用容错机打入市场，从容错机的研制到系列产品的批量生产，经历了差不多半个世纪的时间。目前容错计算技术渐渐地成熟起来，成为一种较为通用的计算机设计技术。

### 一、早期的容错计算技术

可靠性理论及其应用的研究早从第二次世界大战时就开始了，它是因战争的需要而提出来的。计算机容错技术的研究则从1945年世界上第一台计算机问世时就开始了。

第一台计算机ENIAC因其可靠性过低而无法使用。1951年世界上第一台商用计算机UNIVAC采用了奇偶检测技术和匹配比较、双重运算线路，提高了系统的可靠性，从而开始了计算机的实际应用。世界上第一台容错机SAPO是50年代初在捷克斯洛伐克

研制的，该机处理器采用三模表决工作方式（TMR），在存储器中使用了奇偶校验和比较的方法，发现故障后可自动进行重试。

随着晶体管计算机的发展，元、器件可靠性提高很快，但是，冗余硬件和故障恢复使系统的成本增加很多。当时，自动故障恢复被认为是不太合算的，只好把重点放在设计阶段采用故障检测进而完善诊断的手段上。60年代初，出现了较为有效的组合电路测试算法——D算法。此时开始采用了微程序设计，用微码写诊断程序，对内部逻辑可进行更有效的测试和诊断。许多机器开始采用故障检测逻辑、单指令重试及微诊断。

## 二、60年代的专用容错系统

由于载人航天器需要有非常高的可靠性，美国NASA（美国国家航空和航天管理局）于1961～1965年研制了第一台星载容错机，其指标要求在一年运行期中可靠度为95%。该机采用晶体管元件，在关键部分采用四倍级冗余，即四只晶体管代替原来的一只，其中一只失效，其他三只可继续工作，使逻辑维持正常。存贮单元采用三模表决方式。

NASA支持的第二台容错机用于APOLLO登月飞船的制导系统，是1962～1969年完成的，其可靠性指标为250小时运行时间可靠度为99%，其处理器系统采用三模表决方式，三个处理器执行相同的程序。两个磁芯存储器同时读写数据，并采用了检测编码。该系统的研制成功为宇航飞行器采用容错机创造了十分有利的条件。

NASA研制的第三台容错机是用于喷气推进实验室的自测试与自修复(STAR)计算机。它是为深空间任务而开发的，要求运行寿命至少10年。该机由若干个存储器、一个运算协处理器、一个控制处理器、I/O处理器和测试与修复处理器等组成，各部件具有自检测能力，系统可动态重组。STAR基本上属于混合冗余结构。

60年代使用较为广泛的容错机是Bell电话公司的ESS，其可靠性指标为40年运行期内，系统不能工作的时间不能超过2小时。ESS所有关键部件都是双份的。有专门完成故障检测、定位和隔离的硬件与软件，并允许人工干预。该系统现在一直在应用。

到60年代末，几种主要的容错计算技术差不多走出了实验室，变为较为成熟的应用技术，例如TMR（三模冗余系统）、双模系统、自检测等等。

## 三、70年代的发展

70年代，容错计算机系统有较大的发展，出现了许多极有意义的研究性系统和应用系统。在NASA的支持下，斯坦福研究所(SRT)和MIT的实验室分别研制了FTMP(容错多处理器系统）和SIFT（软件方法实现的容错），用于商务飞机的大型飞行控制系统，可靠性目标是10小时运行的失效率小于$10^{-9}$。以上两个系统均在不同的硬件中执行一个程序的三份拷贝，并对结果进行表决以屏蔽故障，只是它们使用的方法不同。FTMP的所有处理器按时钟同步，表决器由硬件实现；SIFT的各处理器使用独立的时钟，表决和同步由软件来实现。

70年代末，还出现了为商用目的而研制的并直接支持Ada语言的Intel432容错机和Tandem/Nonstop系统。Intel432多处理器系统的设计水平是非常高的，但因其设计

复杂，价格高昂，使用不方便，在市场竞争的大潮中未能得以广泛应用。而Tandem系统在此期间却得到了广泛的应用，在联机事务处理方面（如在金融行业中），在市场上很占优势，这是一台在多处理器系统中以软件方法为主来实现容错的机器，它比较注意资源的利用率。它的广泛应用表明了容错计算机已经从特殊应用领域走向通用的应用领域。从少量的研制到有一定批量的生产，是容错计算机系统的一大进展。

除了容错计算机系统之外，在一般的通用计算机中也广泛地采用了容错技术。像IBM的308X系列和4300系列，Cray公司的Cray-1，DEC公司的VAX-11系列，Honeywell公司的Level/DPS系列都不同程度地采用了检错/纠错码、重试、自检测和恢复、维修诊断处理器、多机体系结构等容错技术，已经使容错成为计算机系统不可缺少的重要功能。

在这一期间，由于美国Algirdas Avizienis教授等人的努力，在IEEE学会下成立了容错计算学术委员会（TCFTC），并且从1971年开始每年都要举办一届国际性高水平的容错学术讨论会。

在中国，首先在哈尔滨工业大学于1973年开始，在陈光熙教授、李仲荣教授、胡铭曾教授等人领导下，开展了对容错技术、容错机系统的研究。他们从编码检测（奇偶编码）和系统冗余技术的研究开始，先后提出了可靠性理论、奇偶预测法、自检测及切换法以及各种冗余方案的比较等等。并用了6年的时间研制了带自检测的部件级协同的双模协同实验系统（RCJ-1），取得了较好的实验结果。但因受当时元、器件质量和工艺水平等等各方面不利因素所限，该机未能推广应用。天津某研究所利用了RCJ-1设计方案，自行设计并研制了容错微型机，于1983年成功地应用到了舰艇的控制系统上。

航空航天部的631所也较早地开展了容错技术的研究，研制的专用容错机也应用得很好。在此期间，北京自动控制研究所对容错技术，尤其是实用化，开展了较多的研究，多台专用容错机发挥了很成功的作用。

中国的学术研究也很活跃，一大批学者从国外进修容错技术或参加国际性的容错研究以后回国，与国内学者们共同努力，极大地推动了中国容错技术的研究。从1987年开始，每两年召开一次全国性的容错学术讨论会，从1989年开始，每两年召开一次中日联合容错技术研讨会。1989年，在魏道政研究员等人的努力下，在中国成立了容错计算专业学组。后来发展为中国计算机学会容错计算专业委员会。美国、日本等国家的容错计算机产品开始进入中国市场。中国的计算机用户开始注重并使用容错机。中国自行研制的专用容错机开始发挥越来越大的作用。

从事容错研究的单位十分普遍，许多研究所、大学都不同程度地进行着这个专题的研究工作。

## 四、80年代的发展现状

到了80年代，容错技术的发展形势非常好。归纳起来有以下几个特点：

1．商用容错计算机市场的出现

以往的容错机大多专用性很强，而且结构特殊，使得容错机的代价过高，这就限制了它的推广和应用。进入80年代以后，VLSI技术的迅速发展，使元、器件的价格成倍地

下降，这就为各种硬件冗余提供了最基本的保证。这样，容错机所增加的代价降至极小的比例，使用户感觉不到沉重的负担。加上ASIC技术的使用，使体系结构更加合理紧凑，这就为容错机产业的形成和迅速扩大奠定了基础。尤其是市场上对容错机的需求量极剧增加，使容错机从以往的“宣传阶段”进入到“深入人心”的地步。于是，容错计算机产业也就应运而生了。几乎是使用计算机的领域都有使用容错机的要求。各大公司纷纷推出容错机产品，争先恐后地打入市场。

Tandem-nonstop容错机是比较早打入市场的商品。紧接着，发展很快的美国STRATUS容错机公司推出了基于硬件冗余兼顾软件容错的StratusFT250、XA2000系列产品，它是包括小型、大型的通用系列机，采用了“带自检测的部件级协同的双模冗余”技术。因其设计与生产上的成功以及具有便于维修和良好的服务系统，使该产品成了目前容错市场上的一支劲旅。本书的后一部分将详细介绍这套系统。

IBM公司的IBM-system/88容错机，DEC公司的VAX FT-3000/310，Concurrent公司的3200系列，Parallel公司的Parallel XR 系列，Tolerant公司的 Eternity 系列，Data General公司的MV等等都是已进入市场的容错机。

这一时期各种容错机的基本方案，见附表1所示。

容错机产业以惊人的速度发展起来了。

2．分布式计算机系统的容错设计

计算机已经开始从第四代向新一代前进了。从系统结构和思维逻辑方面向非冯·诺伊曼方式转化。多机、多处理器和网络系统很快将成为计算机的主要结构形式。这样的系统模块化程度高，比较复杂，不仅强烈地要求容错的支持，而且也具备十分有利的容错设计条件，于是系统设计者很自然地加进了容错技术，一改过去由容错专题研究人员进行容错设计的局面，几乎计算机设计者都懂得如何选取容错方案。这样，针对分布式系统而出现了许多新的容错技术。

3．VLSI技术为容错技术提供了新的内容

以超大规模集成电路作基本元件，使故障模式发生了变化，从而要求人们去考虑更多更新的容错技术，如重点解决“全1”错和“全0”错的问题就属于这种情况。

与此同时，系统可靠性指标不得不分出一部分放在芯片里。因此，这个时期开始了VLSI容错设计的研究和应用，产生了RVLSI技术（可重构VLSI）。研究内容包括电路内部自检测和自诊断的算法和实现。

另外，国际上迅速发展的多值逻辑器件，可把纠错码固化在器件中，纠错码的许多成熟理论可直接应用到多值逻辑器件的计算机设计中。

80年代的容错产业呈现一派迅猛发展的趋势。

## 五、对容错计算技术未来发展的估计

根据当前的状况，可以对未来的容错技术发展趋势，作出如下几点估计：

1．软件容错技术将有比较大的进展

软件系统发展到今天，规模之大，复杂性之强有目共睹，软件可靠性之低也令人十分

担心。有很多人已经从理论上开始了对软件可靠性的研究，也提出了一些算法。从需要和已取得的成果来看，用不了多久，将会出现初级的容错软件的设计方法，有可能首先在易于实现的数据库方面有较大的发展。应用软件方面的容错设计将会产生实用的工具。

2．软件、硬件相结合的容错设计方法将倍受重视

硬件冗余的容错机不会有那么大的系统开销，纠错速度比较快，但是资源利用不太合理，对软件故障处理能力很低。而软件方法实现的容错，对硬件不提过高的要求，系统灵活，资源利用比较合理，但系统开销过大。取长补短，形成一个软、硬件相结合的容错方法，将会出现在新的容错机设计中。这种方法将会受到很大的重视。

3．VLSI的容错设计技术将发挥巨大作用

目前在进行的电路内部的自检测、自重构研究，不仅要解决电路本身可靠性和合格率的问题，更重要的是它将解决子系统的可靠性设计问题。发展的结果将会出现“容错的VLSI芯片”及可直接支持系统容错设计的“可容错设计芯片”，为系统设计者提供一个具有透明性的容错设计元、器件。可以说，进入到芯片内部的容错技术的研究，将会取得重大的成果，将成为容错研究的一大分支。

4．系统容错设计的应用目标

系统容错设计将在分布式系统、阵列机系统投入更大的力量。计算机发展的趋势决定了在阵列机系统、分布式系统中采用各种容错技术。根据这样系统的特点，必将会出现许多新的容错设计方法。

5．容错技术朝向智能化发展

故障检测方法、诊断方法将会采取人工智能的处理途径，以专家系统的各种智能工具来支持故障检测和诊断。利用专家的知识，借助推理机构，迅速而准确地提供诊断结果。系统的动态重构、故障恢复等功能，都将在智能化的支持下得以实现。容错技术的发展将向前迈进一大步。

6．容错技术的发展前景

现有容错技术会更趋完善，应用更广泛，商品化的容错机将发挥更大的作用，容错市场将迅速扩大。

经过若干次循环，早年提出的处于冷门的容错技术，在当今时代却成了热门技术（如四个CPU两组比较），早年受到欢迎的技术，现在有的已被打入冷宫（说不定哪一年又成为受欢迎的技术）。循环利用技术的结果不是一个淘汰另一个，而是各种技术都得到不断发展，技术更趋完善和成熟，生命力会更强。例如，现在市场上受欢迎的几种容错机，所采用的技术都不是什么新的发明，但是效果非常好。现有的技术将仍然会受到极大重视，在相当长的时间内仍会发挥重要作用。

未来的容错机种类会越来越多，容错机的数量会越来越大，在计算机系统不断更新换代的潮流中，将会有大量的容错机充当替换者的角色。有人估计，10年后将有90％的计算机是容错机或具有某种容错功能的机器。

# 第二章　系统可靠性的基本概念与分析

本章将对系统可靠性的基本概念作集中介绍，包括可靠度、可用度、可维修度等概念，也将对失效率的度量作一定的理论上的推导。

## 第一节　可靠度的定义

当前，数字系统的规模和复杂程度正在迅速提高。尽管元器件可以尽量地可靠，但是，不出错几乎是不可能的。因此，对于系统设计者和用户来说，可靠性仍然是一个十分重要的问题。为了定量地描述可靠性，这里将提出可靠度的概念。建立可靠度的基本依据是在给定的时间间隔内，在给定的环境下，系统是否仍然能正常执行其功能。它取决于许多因素，例如系统的设计、元件和部件的设计、环境等等。在给定的时间间隔内及给定的条件下，一个给定系统的执行可以认为是一个随机事件，即只有当其实际发生才存在的事件。所以，可靠度这个概念可以认为是“在给定的时间间隔内，在给定的条件下，系统仍然能正常执行其功能的概率”。

可靠度的提高，可以通过最坏情况设计、选用高质量元器件以及最佳的制造工艺等方面的工作来实现。当然，这将要提高系统的造价，而且可靠度的提高是很有限的，因此，对于一个可靠的系统设计者来说，一个比较好的办法是加冗余，以掩盖故障的影响。这种方法不一定要求高质量的元器件，因此，采用冗余技术来设计可靠的系统并不很贵。

冗余技术通常指硬件冗余、软件冗余和信息冗余，即编码技术。当代的高可靠性设计，往往采用综合性的冗余技术。

## 第二节　可靠度与失效率

假定在相同条件下有$N$个样品元件。设$S(t)$为残留元件数，即从实验开始后$t$时刻仍在正常工作的元件数，$F(t)$为到$t$时刻的失效元件数。这样，元件的残留概率，亦即可靠度$R(t)$为

$$R(t)=\frac{S(t)}{N}$$

失效元件的概率，亦即不可靠度$Q(t)$为