面向21世纪课程教材
Textbook Series for 21st Century

计算机应用系统的故障诊断与可靠性技术基础

邹逢兴 主编
邹逢兴 张湘平 编著

高等教育出版社
HIGHER EDUCATION PRESS

面向21世纪课程教材
Textbook Series for 21st Century

计算机应用系统的故障诊断与可靠性技术基础

邹逢兴 主编
邹逢兴 张湘平 编著

高等教育出版社
HIGHER EDUCATION PRESS

(京) 112号

内容提要

本书是教育部“高等教育面向21世纪教学内容和课程体系改革计划”的研究成果，是面向21世纪教材。

本书总结了作者多年来进行有关教学、科研的经验并结合国外有关的最新技术和发展方向，系统介绍了计算机应用系统的故障诊断与可靠性分析、设计的基本理论和主要方法、技术，包括可靠性与可靠性技术概论、可靠性编码技术、故障自检测与自诊断技术、故障屏蔽技术、动态冗余技术、可测性设计技术、软件可靠性技术、失败安全设计、容错系统的可靠性分析评估和高可靠性计算机应用系统的设计等内容。全书贯彻了原理、技术和应用并重、软硬结合、以硬为主的原则，注重选材的科学性、实用性和先进性。

本书可作为高等院校有关专业的研究生和高年级本科生的教科书使用，也可供从事故障诊断与可靠性技术研究和应用的工程技术人员参考。

图书在版编目(CIP)数据

计算机应用系统的故障诊断与可靠性技术基础 / 邹逢兴主编. -北京：高等教育出版社，1999

ISBN 7-04-007926-7

I. 计… II. 邹… III. ① 计算机系统-故障诊断②计算机系统-系统可靠性 IV. TP30

中国版本图书馆 CIP 数据核字(1999)第 70133 号

计算机应用系统的故障诊断与可靠性技术基础

邹逢兴 主编

出版发行	高等教育出版社		
社　　址	北京市东城区沙滩后街55号	邮政编码	100009
电　　话	010-64054588	传　　真	010-64014048
网　　址	http://www.hep.edu.cn		
经　　销	新华书店北京发行所		
印　　刷	中国科学院印刷厂		
纸张供应	山东高唐纸业集团总公司		
开　　本	787×960　1/16	版　　次	1999 年12月第 1 版
印　　张	27.5	印　　次	1999 年12月第 1 次印刷
字　　数	520 000	定　　价	30.00元

凡购买高等教育出版社图书，如有缺页、倒页、脱页等质量问题，请在所购图书销售部门联系调换

前　言

当前，数字化的浪潮正在迅猛地席卷全球，人们对数字化仪表、数字化设备、数字化家电、数字化地球等名词早已耳熟能详。一个数字化时代正在伴随着21世纪钟声的敲响而悄然到来。

数字化的主要特征就是数字电子计算机的应用，就是用计算机来获取、处理、利用、控制各种信息，辅助人类解决社会、经济活动中的各种问题。所以，数字化也就是信息化、计算机化。

确实，现在计算机的应用非常广泛，已经渗透到社会的各个领域、各个层面，包括普通家庭，并且应用的规模越来越大，开始形成了迅速发展中的社会经济活动全面依赖于计算机的局面。在这种情况下，对于计算机系统的可靠性要求也必然越来越高。试想，一个核反应堆和化工、冶炼等生产过程的实时计算机控制系统突然控制失灵；一个空中、铁路、高速公路等交通计算机管制调度系统在交通繁忙时突然失控；一个计算机实时监控和机器人操作的大型手术正在进行时突然动作出错；一个联机银行业务系统的存、贷款信息突然丢失；一个证券交易市场管理信息系统正在营业时突然瘫痪；一个社会保障/社会保险网络信息管理系统突然崩溃；一个计算机控制的战略导弹综合防御系统突然无中生有的报警；一个自动军事指挥控制系统在战争正激烈进行时突然决策失误……其后果会怎样呢？这是不言自喻的。因此，实现计算机应用系统的高可靠性是实现社会信息化、数字化的关键，是人们能够无忧虑地使用计算机的基础。没有高可靠性，计算机推广应用非但不是好事，反而是人类的灾难。正因为这样，所以近几年来，热心于计算机系统可靠性技术研究的人员越来越多，开设可靠性技术方面课程和研究生研究方向的高校和专业也越来越多。本书正是作者在多年来从事这方面的研究和研究生教学的基础上，参考国内外有关最新技术和发展动向编著而成的。

实现高可靠性计算机应用系统的技术途径从根本上说只有两条：一条是避错，一条是容错。为了实现这两条，需要得到许多技术的支持，其中故障检测与诊断技术是基础。围绕计算机系统的故障诊断与可靠性技术，人们进行了长期的卓有成效的研究，有关论文层出不穷，有关著作也有不少。与目前所见的国内外同类著作相比，本书的主要特点如下：

(1) 基于可靠性系统主要是设计出来的，而不是分析出来的这一认识，在可靠性分析和可靠性设计两者中，本书坚持了以可靠性设计为主的原则，主要介绍有关可靠性设计的各种技术，对可靠性分析内容的介绍是为可靠性设计服

务的。

(2) 从计算机应用的观点出发，把故障诊断和避错、容错的主要目标定位在可更换模块级上。更精细地将故障定位到逻辑门级以下，对计算机应用人员来说是没有实际意义的，也与集成电子技术和计算机技术的发展现状不相适应（除非要进行专用集成电路的设计和测试）。

(3) 在硬件实现技术与软件实现技术的关系上，坚持了软硬结合、以硬为主的原则，着重介绍故障诊断与可靠性设计的硬件实现技术和方法。

(4) 在理论与实践的关系上，贯彻了原理、技术和应用并重、以技术和应用为主的原则。对必要的数学、理论基础，尽量用通俗易懂的语言深入浅出地描述和说明，而绝不使本来易于理解的原理反而抽象化、数学化。

(5) 在学术著作和教材的关系处理上，突出了本书的教材特征，努力按照“基础性、科学性、系统性、实用性和先进性”统一的原则选取内容，按照教育、教学规律组织内容，阐述内容。

本书共分十章。第一、二章介绍可靠性技术的基本理论基础；第三章至第八章介绍计算机应用系统高可靠性设计的主要技术，包括故障自检测与自诊断技术、故障屏蔽技术、动态冗余技术、可测性设计技术、软件可靠性技术、失败安全设计技术等；第九章介绍容错系统的可靠性分析评估方法；第十章介绍高可靠性计算机应用系统的一般设计方法及若干实例。为便于教学和扩展研究，各章有习题，书末有参考文献。

本书第一、二、三、五、八章由邹逢兴编写，第六、九、十章由张湘平编写，第四、七章由两人合编。全书由邹逢兴主编和统稿。

国防科技大学计算机学院杨晓东教授应高等教育出版社之邀，担任本书主审。他曾担任银河Ⅰ型、Ⅱ型和Ⅲ型巨型计算机的主要设计师、副总设计师和技术顾问，在计算机系统的故障诊断与可靠性分析设计方面有很深的理论造诣和丰富的实践经验。他对本书书稿进行了认真审阅，提出了许多十分宝贵的修改意见。在此对杨教授表示衷心感谢。国防科技大学教材建设委员会、自动控制系学术委员会和学校各级领导及机关工作人员对本书的编著自始至终给予了很大关怀、推动和帮助，高等教育出版社则对本书的出版给予了热情支持和厚爱，在此一并致以深深谢意。

由于作者水平和经验有限，加上时间仓促，书中难免有疏漏和不足之处，敬请读者指教。

作者

1999 年 9 月于长沙

责任编辑　何新权
封面设计　张　楠
责任绘图　吴文信
责任印制　宋克学

第一章　可靠性与可靠性技术概论

1.1　计算机系统的可靠性技术及其发展过程

目前，计算机已广泛应用于各行各业、各个领域，渗透到了社会活动的方方面面，并且其规模越来越大，正在形成当今社会全面依赖计算机的局面。这种局面的形成，将给现代人带来极大的便利。与此同时，人们对各类计算机应用系统的可靠性要求也越来越高。在许多应用领域，如航空、航天、金融、保险、核反应堆、水电工程、交通管制、输油管线以及冶金、化工等众多的工业过程控制中，如果计算机系统不能在规定的时间内稳定可靠地工作，将会造成巨大的损失，甚至导致灾难性后果。这类恶性事故在国内外都屡见不鲜，例如：

1962 年，美国宇航局发往金星的“水手 1 号”宇宙探测器，由于计算机系统发生故障，发射后不久即坠毁，几亿美元倾刻间化为灰烬。

1979 年，新西兰航空公司一架客机，因飞行计算机控制系统发生故障，撞到阿尔卑斯山上，机上 257 名乘客全部罹难。

1980 年，北美战略防空司令部由于其计算机系统中一个小元件的故障，竟错误地引发了“苏联带核弹头的导弹已飞临美国”的战争警报，致使美空军司令部和核轰炸部队进入紧张的一级核战准备状态，连位于华盛顿安德鲁斯空军基地的“总统空中司令部”也已经发动。这场虚惊不仅给美国经济上造成了很大损失，而且差点把世界推向了核战争的边缘，政治上造成了很坏影响。

1981 年，日本川崎重工公司发生了一起机器人杀人事件。被害人是该公司的一名机器修理工，当时他维修好机器后正在接通电源准备试车，没想到机器人因电脑故障也随之启动，从背后用两只手将该修理工紧紧抓住，把他夹紧在机器上活活压死了。

1983 年，美国科罗拉多河水泛滥，由于计算机监控系统对天气形势预测出错，致使水库未及时泄洪，造成巨大损失。

1989 年，东南亚某地区的股票交易市场计算机出错，使系统中断工作半小时，造成交易市场一片混乱。

在英阿马岛战争中，英国一艘驱逐舰因舰上计算机控制的防御系统出故障，将对方发射来的导弹错误地识别为友军武器，未将它击落，结果反被它击

沉。

在美国空军的一次编队飞行中，因火控计算机故障，竟向己方部队发射了导弹，造成了严重后果。

意大利国家数据库曾因计算机故障而受到破坏，短短 6 s 内破坏的数据，后来经过 6 年之久才得到恢复。

……

这一个个触目惊心的例子清楚地说明了计算机故障所造成的严重后果。因此，人们希望自己所依赖的计算机应用系统是个高度可靠的系统，最好不发生故障，能“健康”地工作“一辈子”；即使发生了故障，也能正常或基本正常地工作，或者至少不产生严重后果，同时尽量缩短系统维修和恢复时间。这就要求工程设计师们在设计各种重要的计算机应用系统时，不仅要追求高速度、高性能，而且尤其要追求高可靠性，将可靠性设计放在第一位。

计算机系统的可靠性技术正是在这种需求的牵引下产生和发展起来的。

事实上，从世界上第一台计算机问世时（1946 年）起，人们就开始了计算机系统可靠性技术的研究，后来随着计算机技术的发展和计算机应用领域的不断拓宽，计算机系统可靠性技术也不断发展，而且基本上与计算机的发展是同步的，大体经历了四个阶段：

第一阶段：20 世纪 50 年代。这一阶段，计算机以电子管和继电器为主要元件，元件的失效率很高，并且易受瞬时故障的影响，造成系统的平均无故障时间很短，一般只有几分钟至几十小时，因此迫切需要采用故障检测与恢复技术。但当时这方面的技术水平还很低，一般只能采用特别设置的硬件故障检测和人工恢复手段来尽量提高系统的可用性。不过这种状况激励科学家和工程师们从理论上和实践上对计算机系统的可靠性技术开展研究。其中以冯·诺依曼（John Von Neumann）及其同事们的研究最具有代表性和开创性。他从 1952 年起作了一系列关于用重复逻辑模块改善系统可靠性的报告，并于 1956 年发表了题为《概率逻辑及用不可靠的元件设计可靠的结构》的论文。文中提出并证明了高可靠性网络的存在定理，即：将足够多的不可靠元件按适当方式联结，总可以组成一个可靠性达到任意高的电路系统。文中还具体提出了多数表决的概念，并分析了这种结构对系统产生错误结果的概率可能造成的影响。在高可靠性网络存在定理的推动下，20 世纪 50 年代中后期开始出现了少数早期的容错计算机，如世界上第一台容错计算机 SAPO 就于 1956 年在前捷克斯洛伐克研制成功并投入运行。该机处理器采用三模冗余、多数表决方式工作；存储器采用奇偶校验；发现故障后可通过重试（指令复执）来加以恢复。但总的说来，这一阶段属于可靠性和容错计算理论的奠基阶段。

第二阶段：20 世纪 60 年代。这一阶段的计算机以晶体管为主要元件，可

靠性和容错计算理论研究渐趋活跃。这一阶段在校验技术、编码理论与技术、诊断理论与技术以及冗余技术等方面的研究和实践取得了很大成果，并将这些成果向技术化、产品化方向发展，研制出了许多专用容错计算机系统。其中最有代表性的专用容错系统是美国国家航空航天管理局（NASA）主持研制出的土星 V 号运载火箭导航计算机系统（1964 年）、阿波罗登月飞船制导计算机系统（1969 年）和用于喷气推进实验室的自测试与自修复计算机系统 STAR（1969 年）。它们均采用了三模冗余和检测编码等技术来实现容错。STAR 系统为了满足运行寿命至少 10 年的可靠性指标要求，还使用了一个专门的检测与修理处理机负责监控系统其余部分的工作，发现故障时可进行程序卷回复执；故障定位后，可用电源切换方式自动更换部件；为了保证检测与修理处理机本身的可靠性、可信性，该机采用了三模表决加备份的混合冗余结构，并用算术检错码和双机比较来检测故障。

这一阶段另一个采用容错技术的重要领域是电话交换机系统。1965 年，美国贝尔实验室研制成功 1 号 ESS 系统，该系统所有关键部件都是双份的，有专门的硬件和软件进行故障的检测、定位与隔离，对隔离出的故障部件采用人工修理。该系统的可靠性指标是 40 年运行期内不能工作时间不超过 2 小时，至今仍在使用。

第三阶段：20 世纪 70 年代。这一阶段的计算机进入以集成电路为主要元件的发展时期，元件的失效率明显降低，可靠性和容错计算理论与技术的研究更加活跃，容错技术的应用范围大大拓宽。这一阶段，有关容错计算、故障测试与诊断以及设计自动化等方面的各种国际性学术会议开始出现，并逐渐成为国际上可靠性技术研究领域的主要讲坛。如 1971 年以来，IEEE 计算机学会容错计算技术委员会每年召开一次国际容错计算学术会议。当今有关可靠性和容错计算的最具影响的论文和成果大多是在这些会议上发表的，如以软件冗余为主导、用解析冗余代替硬件冗余的故障检测与诊断理论和技术就是 1971 年由麻省理工学院的 Beard 在国际会议上首先提出的。理论研究的成果推动了许多极有意义的研究性和应用性容错系统的出现，应用范围由原来的航天飞行器控制及电话交换机领域扩展至银行事务处理及各种实时控制系统，甚至许多通用计算机系统也采用了容错技术，使容错计算机从特殊应用领域走向了通用应用领域，从少量的研制进入到有一定批量的生产。例如，1975 年美国贝尔实验室的 3A 号 ESS 处理机投入运行。同年，美国出现了 TANDEM 16 容错事务处理系统。1976 年，美国 AMDAHL 470 V/6 容错通用计算机系统研制成功。1978 年出现了容错空间计算机 FTSC。1980 年，在 NASA 支持下由斯坦福研究所研制的容错多处理机系统 FTMP 和由 MIT 实验室研制的软件实现的容错计算机系统 SIFT 问世，均应用于商务飞机的大型飞行控制系统。这期间，许多公

司还先后推出了容错的通用计算机系统，像 IBM 公司的 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 系列等，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，使容错成了计算机系统不可或缺的重要功能。

第四阶段：20 世纪 80 年代以来。这一阶段的计算机进入了以大规模、超大规模集成电路为主要元件的发展时期，计算机性能极大地提高，多处理机计算、分布式计算、网络计算等新的计算技术不断出现。这些反过来使可靠性和容错计算的研究更加深入，为之提供了许多新的研究内容和研究手段，同时也推动容错技术的应用范围进一步扩大。这一阶段，故障的检测手段和冗余技术在改进的基础上更新换代，新的学术研究和探讨更加频繁活跃（如开始了 VLSI 容错设计的研究和应用，产生了可重构 VLSI 技术和将纠错码理论应用于芯片内部的多值逻辑器件设计技术等），容错计算机产业初步形成，计算机网络的容错、数据库的容错、软件的容错以及人工神经网络的容错等新研究领域不断涌现。

迄今为止，经过半个世纪的发展，可靠性和容错计算研究已形成了计算机学科和自动化领域中一个新的、独立的分支，正受到国内外越来越多的计算机和计算机应用系统设计人员的重视。目前，国内外许多重点大学普遍开设了相应的课程，并建立了相关研究生培养方向。有关的学术会议不仅国际上许多学术组织每年都要举办一次以上，而且许多国家和地区还要举办，比如我国从 1985 年起，也是每一二年召开一次相关会议，与国际年会相呼应，并于 1991 年 7 月中国计算机学会在上海成立了容错计算专业委员会，使我国可靠性与容错计算领域的发展走上了更加正规化、组织化的道路。

随着超大规模集成电路技术和计算机技术的进一步发展，必将对计算机系统可靠性的研究带来新的机遇、内涵和挑战。可以预见，可靠性和容错计算理论及可靠性设计技术在 21 世纪将有一个更大、更快的发展。20 世纪 90 年代初期，美国国家科学院计算科技委员会在对美国计算机企业状况进行了评估后，发表了一份正式报告，明确指出了今后研究工作最有希望的几个领域，并建议支持一些高层次的大课题，以便在各个领域中起推动作用。委员会提出了六大课题，其中第二大课题就是研究可靠性极高的计算机系统（即容错能力极强的系统）。日本和西欧一些发达国家也正在组织力量，将容错计算的研究放在极重要的地位来推进，普遍意识到高可靠性理论和技术将对未来的国防、民用工业，对空间技术的发展和对社会公用事业的发展起着难以估量的作用。我国也不例外，近几年来，国家 863 计划的自动化领域和信息技术领域、国家自然科学基金、国防预研计划等都明显加大了对故障检测与诊断、容错计算、冗

余控制等可靠性技术的立项支持，对推动我国可靠性技术的发展和应用将发挥重要作用。

1.2　可靠性技术研究的范畴

提高计算机应用系统可靠性的技术途径很多，但归纳起来大体上可分为两大类：一是提高元部件本身可靠性的技术，即避错技术；二是用给定元部件构成高可靠性系统的技术，即容错技术。除此之外，还有两个与实现高可靠性系统紧密相关的方面也是可靠性研究的重要内容，这就是可测性设计和失败安全设计。前者是加快故障诊断速度，从而加速修复过程，提高系统可用性的重要途径；后者则是当系统万一出现恶性故障时作为保证系统安全可靠的最后一道防线。

1.2.1　提高元部件可靠性的技术——避错技术

一个典型的计算机应用系统一般是由计算机、模拟或（和）数字 I/O 通道、传感器、执行机构和测控对象等各子系统组成的，各子系统又由众多的元部件组成。因此，计算机应用系统的可靠性在很大程度上取决于组成系统的元部件的可靠性。而且可以说，提高元部件本身的可靠性是提高系统整体可靠性的基础。提高元部件可靠性的主要技术途径有：

- 高可靠性元部件的研制、选择和降额使用。一般说来，提高元件的集成度有利于提高元件的可靠性；将系统中由若干元器件构成的硬件电路和某些应用软件、标准子程序库做成专用大规模集成电路芯片，有利于提高系统的可靠性。
- 环境防护设计。包括电磁兼容性设计、机械应力防护设计、热设计、气候环境“三防”（防潮湿、防烟雾、防霉菌）设计等。
- 质量控制。主要指对元部件在实际使用前要进行老化试验和筛选。

1.2.2　使用给定器件构成高可靠性系统的技术——容错技术

一个系统，无论采用多少避错设计方法，总不能保证永远不出错。实践证明，利用避错技术来提高系统的可靠性，一般最多使系统的平均无故障时间增加一个数量级，超过这个限度会使成本急剧上升。因此，要想进一步提高可靠性，就必须采用容错技术。容错是靠资源的冗余和对资源的精心组织来实现的。容错技术的优越性在于，使用线性增加的冗余资源可换取指数增长的可靠

性，它不仅能补偿因系统的规模增大而造成的可靠性损失，而且能使系统的可靠性极大提高，既适用于恶劣环境，又降低成本性能比。

容错技术主要包括下列三方面的内容：

(1) 冗余技术

冗余技术是通过增加冗余资源的方法来换取可靠性，使系统在出故障时仍能维持正常功能。根据冗余资源的不同，通常有硬件冗余、软件冗余、信息冗余、时间冗余之分。硬件冗余是通过硬件的重复使用来获得容错能力，常用的方法有堆积冗余、备份冗余和堆积、备份结合运用的混合冗余等。软件冗余的基本思想是用多个不同软件程序执行同一功能，利用软件设计差异来实现容错。信息冗余是通过在数据中附加多余的信息位来构成检错/纠错码而达到容错的目的。时间冗余则是通过消耗时间资源来实现容错的，其基本思想是重复运算以检测故障。按照重复运算是在指令级还是程序段级，时间冗余可分为指令复执和程序卷回。实际应用中，这几种冗余方法可以单独使用，也可以混合使用。

冗余技术实质上就是利用冗余资源将故障影响掩盖起来，所以也叫故障屏蔽技术或屏蔽冗余技术。这种技术主要用于可靠性要求极高且在一段时间内既要保持连续运行又无法修理的地方，如航空航天、核电站、化工冶金过程控制等应用场合。但是，单纯的故障屏蔽技术只能容忍故障，不能给出故障告警，且故障容忍能力受到本身静态冗余配置的限制，当系统中的冗余因故障增加而耗尽时，再发生故障将使系统失效，产生错误输出。

屏蔽冗余技术的研究内容主要有 N 模表决冗余、纠错码、屏蔽逻辑等。

(2) 故障检测与诊断技术

故障检测的目的是回答系统是否发生了故障。故障诊断则是在故障检测的基础上进一步回答系统中哪里发生了故障、发生了什么性质的故障，实现故障定位和定性。

故障检测和诊断不提供对故障的容忍，只提供对故障的告警。故障检测与诊断可以联机进行，也可以脱机进行。

故障检测与诊断技术主要包括检错码、二倍仿作、自校验、监视定时器、一致校验与权限校验等。

(3) 系统重组与恢复技术

重组是指在检测、诊断出故障后，用后援备份模块替换掉失效模块，或者切除失效模块，改变拓扑结构，实现系统重新组合。重组的基本方法有后援备份、缓慢降级和自适应表决等。

恢复则是在重组后，使系统操作回到故障检测点或初始状态重新开始。如果是回到初始状态从头开始运行则叫重新启动，简称为“重启”。常用的恢

复算法有重试、检测点、记日志、恢复块等。

对重组时切除或替换掉的失效模块，往往要联机或脱机进行修理使之复原（称为修复）。将修复了的模块重新加入系统则称为重构。修复和重构也属于系统重组与恢复的范畴。

利用上述三种容错技术，可构成四类不同的高可靠性计算机应用系统：

(1) 单独用故障检测与诊断技术可构成联机监控系统。这种系统虽然只能提供故障告警与定位的手段，不能容忍故障以直接改善系统可靠性，但利用它可以自动监视系统的运行状态，当系统发生某些局部故障时，可以迅速报警并分离出发生故障的部位，以帮助维修人员快速查明故障源予以排除，防止局部故障在系统中传播而导致更严重故障的发生。其结果不仅提高了系统的可用性，也间接提高了系统的可靠性。

(2) 单独运用故障屏蔽技术可构成具有故障容忍能力的静态冗余系统。这种系统在故障效应尚未到达输出端之前即可通过隔离或校正来消除其影响，达到提高可靠性的目的。值得注意的是，由于单纯的屏蔽技术并不给出故障告警，所以这种系统当其配置的冗余因故障增加而耗尽时，再发生故障将产生错误输出。

(3) 将故障检测与诊断技术同故障屏蔽技术结合运用可构成既有故障容忍能力，又有故障告警能力的静态冗余系统。当这种系统中发生了故障时，系统可一方面带故障正常运行，一方面根据故障告警和定位信息，实行联机或脱机修复。只要在系统提供的冗余配置耗尽之前能将故障排除，系统就能不中断的正常运行。可见系统可靠性得到了提高。在这种系统中，一般只要增加很少的冗余就能达到高可靠性的目的，前提是具有及时而有力的维修保障。

(4) 将故障检测与诊断技术、故障屏蔽技术、系统重组与恢复技术三者综合运用，可构成性能更高的动态冗余系统。当这种系统发生故障时，通过内部的重组可切除或替换掉故障模块，恢复正常工作，而且这种重组可推迟到耗尽屏蔽冗余时再进行，这样，重组实际上起着补充冗余、延长寿命的作用，显然有利于进一步提高系统的可靠性。

上述四方面都是针对硬件而言的，统称为硬件容错技术。为了构建高可靠性的容错计算机应用系统，除了硬件容错外，还应该采用以下两方面的容错、保护技术：

- 软件容错技术。随着计算机应用技术的不断发展，软件系统的规模和复杂程度持续增长，软件故障已成为各类计算机系统的主要不可靠因素。因此采用一些行之有效的软件容错技术来提高软件可靠性就显得越来越重要。当然，为了提高软件可靠性，像硬件可靠性技术一样，软件可靠性技术也有避错和容错两类，从这两方面都要采取措施。

• 信息保护技术。目的是使计算机系统中正在处理/传输的信息和存储着的信息不被破坏和泄漏。

1.2.3 可测性设计技术

过去，传统的做法是将系统设计和系统测试分离，即由设计人员根据功能、性能要求设计电路和系统，而由测试人员根据已经设计或研制完毕的电路和系统来制定测试方案、研究测试方法、开发测试设备。这种做法在早期以分立元件和小规模集成电路为组件的系统研制中还可以，随着元件集成度越来越高，PCB 板的规模和基本功能单元的规模越来越大，功能越来越复杂，这种做法的弊端日益明显，不仅测试效率显著降低、测试开销急剧增加，而且测试难度太大。据美国一些公司统计，按这种做法，PCB 板的测试开销已占其整个生产过程总开销的 50%以上。说起来更使人难以置信的是，如果用传统的办法测试一块有 100 个输入端的普通 VLSI 芯片，所花的时间可能要上亿年！因此，老办法已不适应计算机系统设计、制造现实的需要。这就需要系统设计人员在设计电路和系统的同时就充分考虑到测试的要求，即用故障诊断的理论、方法和技术去指导系统设计，实现功能设计与测试设计的统一。衡量一个系统和电路的标准，不仅看其功能的强弱、性能的优劣、所用元件的多少，而且要看其是否可测试和测试是否方便。这就是所谓的可测性设计。

可测性设计的核心思想是提高系统的可控制性和可观测性。可控制性是指通过对系统输入端产生并施加一定的测试矢量，使系统中各节点的值易于控制（故障易于敏化）的程度。可观测性则是使故障信号易于传输至可及端，便于观察和测量的性能。

可测性设计要研究的主要问题是：什么样的结构容易作故障诊断；什么样的系统测试时所用的测试矢量集既小而全，又便于产生；测试点和激励点设置在什么地方、设置多少，才使得测试比较方便而开销又比较少；等等。

可测性设计一般都是通过增加硬件资源来实现的，所以从广义上说，它也属于一种硬件冗余设计。

1.2.4 失败安全设计技术

在一些要求安全性特别高的计算机应用系统中，不仅要求容错，而且要求万一系统中的故障超出了系统容错能力时，应能做到失败安全，不会造成灾难性后果。这类系统称为失败安全系统。在失败安全系统中，系统的失败被区分为危险失败和安全失败两种状态。前者是指对人身或设备造成危害的失败状态，而后者是指不会对人身或设备造成危害的失败状态。失败安全设计的目标

是确保系统失败时进入安全失败状态，相应的技术称为失败安全设计技术。

可见，通过失败安全设计可使系统失败时的损失减到最小，起码不出安全事故，所以说它是防卫系统故障、确保系统安全可靠的最后一道防线。失败安全设计技术主要是研究失败安全设计的条件和方法。

综上所述，计算机应用系统的可靠性设计技术的研究范畴如表 1.1 所示。由于本书主旨是讨论计算机应用系统的高可靠性技术，所以不涉及第一方面（避错）的内容，而专门介绍后几方面的内容，其中又以容错技术为主。因可靠性设计过程中也离不开可靠性分析和评价，故对此也专列一章予以阐述。

表 1.1　可靠性设计技术的研究范畴

分类	研究范畴	技术
避错技术（提高元部件可靠性技术）	高可靠性元部件	提高元件集成度；研制专用集成电路芯片；元部件降额使用
	环境防护	电磁兼容性设计；应力防护设计；热设计；“三防”设计
	质量控制	老化试验；筛选
容错技术	故障检测与诊断	检错码；完全自校验和部分自校验；双模冗余比较检测；对偶互补比较检测；自对偶交替逻辑检测；监视定时器检测；一致校验检测；软件检测与诊断
	故障屏蔽冗余（静态冗余）	纠错码；交织逻辑；编码状态机逻辑；NMR 模型；TMR 与三模-单模自净
	动态冗余	故障检测与诊断；重组；可重组的 N 模冗余；恢复
	软件容错	多版本程序设计（NVP）；软件故障检测；恢复块技术；自检程序设计；一致性恢复块；接收表决；相异性设计准则
	信息保护	编码化与密码化；资格检查；存储保护；防火墙；公钥加密；Java 沙箱
可测性设计技术	组合逻辑易测性设计	改善可控性；改善可观性；易测性结构设计；测试码生成；测试响应分析
	时序逻辑易测性设计	
	PCB 板易测性设计	
	内建自测试	
失败安全设计技术	失败安全与失败安全设计的条件	基于检错码原理的设计；分块法设计；二重冗余-与（或）逻辑设计
	输出失败安全设计	
	系统失败安全设计	

1.3　可靠性研究的四层次结构模型

为了便于研究，同时消除可靠性研究领域中许多含混不清的概念，人们常将一个复杂的计算机应用系统（即信息处理系统）从内到外分为四个层次，将它看作一个四层次结构模型，如图 1.1 所示。其中每一层次都包含各自的一组基本概念、模型和术语，然后根据不同的研究目的，在不同的层次上来研究、讨论可靠性问题。所以也将这种四层次结构模型称为可靠性研究的四论域（物理域、逻辑域、信息域、用户域）信息模型。物理、逻辑、信息三层（论域）位于系统内部，统称为内部层（论域），用户层（论域）则为外部层（论域）。

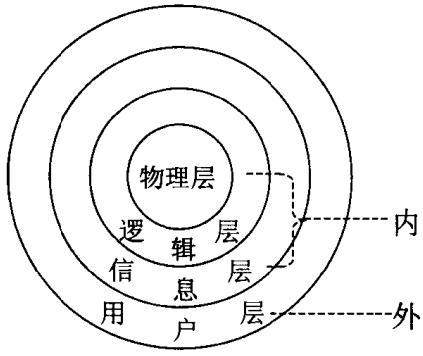

图 1.1　四层次结构模型

采用这种模型，系统的设计要求、性能度量、正确特性样式、测试方法和概念规范等都可通过给定的论域来描述，在给定论域上的一个系统是较高（较外）论域上的一个子系统。在每个论域中，都可以想像按该论域的正确特性标准和时间约定把它的所有状态划分为正确和不正确的两个集合。正确集合代表正常功能，不正确集合代表对正常功能的破坏。引起对正常功能破坏的事件叫不希望事件 UE（Unexpectant Event）。不希望事件 UE 从内部物理域到外部用户域依次称为：

失效 —— 故障 —— 差错 —— 失败
（物理域）（逻辑域）（信息域）（用户域）

一般说来，UE 都是起源于一个内部的论域中，且从低论域到高论域的 UE 构成一个因果链，即物理域失效了，引起逻辑域故障，逻辑域故障引起信息域差错，信息域差错引起用户域失败。图 1.2 给出了这种因果关系和为防止 UE 从低向高传播而在各论域中可采取的 UE 防卫技术。其中避错技术是防卫系统故障的第一道防线，以防止物理失效；故障屏蔽技术是防止故障在该系统的信

息域中产生差错的各种措施；动态冗余技术是防止系统中的差错导致系统失败的各种措施；失败安全技术则是在系统万一出现失败时，确保处于安全失败状态的有关措施。

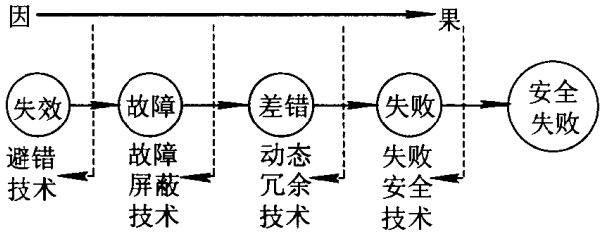

图 1.2　各论域 UE 因果关系与 UE 防卫技术

采用四论域信息模型后，所谓高可靠性的容错系统，就是在计算机应用系统中可能发生 UE 的情况下仍能正确执行所规定的算法和功能，即系统能容忍 UE。容忍 UE 技术的基础包括：

• UE 检测。为了容忍系统中的一个 UE，其后果应当首先被检测到。当一个失效（或故障）不能由系统直接检测时，它往往表现为系统中信息域的某些差错，因此容错技术通常的出发点是错误状态的检测与错误造成的系统损坏程度的评估。

• UE 恢复。其目的是把目前的错误系统状态转换成一个确定的无错系统状态，以便继续正常的系统操作。

• UE 处理与继续服务。尽管 UE 恢复阶段可能已使系统恢复到无 UE 状态，但仍需一种技术确保已被恢复了的 UE 效应不会立即再现，以使系统继续提供规定的服务。UE 处理包括 UE 定位、UE 隔离、系统修复或系统重组等。

信息处理系统三个内部论域中实现 UE 容忍的防卫方案的一个简单抽象模型如图 1.3 所示。图中，环绕正确行为的防卫圈 A 由各种避错技术组成；标号为 $D_1 \sim D_n$ 的圆环表示 n 个不同的 UE 检测算法；带箭头直线 UE(1)～UE(n)表示由这些算法检测的 *UE*；带箭头弧线 $R_1 \sim R_n$ 表示由检测算法所调用的恢复算法的成功作用。A 和 D_n 之间的面积表示可恢复的不正确特性，而 D_n 之外的区域表示内部论域中不可恢复的不正确特性。

图中示出的检测和恢复发生在 *UE* 存在的内部论域中，因此这些 *UE* 的出现在所属论域中被有效屏蔽，从而达到容忍 *UE* 的目的。图中 *UE*(x) 则表示一个不可能被任何检测算法所检测并在内部论域中产生了一个不可恢复的不正确行为的 *UE*。它不能被屏蔽，并且将在外部论域中产生一个 *UE*（失败），甚至可能导致灾难性后果。