名师策划 名师主理 教改结晶 教材精品

普通高等教育“十一五”国家级规划教材

新世纪电子信息与自动化系列课程改革教材

丛书主编 邹逢兴

计算机应用系统的故障诊断与可靠性技术基础

（第二版）

邹逢兴 主 编

邹逢兴 张湘平 龙志强 李 迅 编 著

中国水利水电出版社
www.waterpub.com.cn

普通高等教育“十一五”国家级规划教材

新世纪电子信息与自动化系列课程改革教材

计算机应用系统的故障诊断与可靠性技术基础

（第二版）

邹逢兴　主　编

邹逢兴　张湘平　龙志强　李　迅　编　著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书是普通高等教育“十一五”国家级规划教材，是对1999年12月出版的同名国家“面向21世纪课程教材”的修订版。

本书凝炼了作者及所在单位多年来从事有关教学、科研的成果经验，融入了国内外有关领域的最新发展，系统介绍了计算机应用系统的故障诊断与可靠性设计、分析的基本理论和主要方法、技术。全书包括可靠性与可靠性技术概述、避错技术之电磁兼容设计、避错技术之热兼容设计、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、软件可靠性技术、容错控制技术、失败安全设计技术、系统可靠性设计与分析等11章内容。

全书贯彻了原理、技术与应用并重、软硬兼顾以硬为主的原则，注重内容选取的基础性、实用性、先进性和内容组织的科学性、严谨性、教学适用性。

本书可作为高等学校信息类、控制类各专业的本科高年级学生和研究生的教科书使用，也可供从事故障诊断与可靠性技术研究、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. -- 2版. -- 北京 : 中国水利水电出版社, 2011.12

普通高等教育“十一五”国家级规划教材 新世纪电子信息与自动化系列课程改革教材

ISBN 978-7-5084-9300-8

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

中国版本图书馆CIP数据核字(2011)第267398号

策划编辑：杨庆川　　责任编辑：李　炎　　封面设计：李　佳

书　名	普通高等教育“十一五”国家级规划教材 新世纪电子信息与自动化系列课程改革教材 **计算机应用系统的故障诊断与可靠性技术基础（第二版）**
作　者	邹逢兴　主　编 邹逢兴　张湘平　龙志强　李　迅　编　著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	北京蓝空印刷厂
规　格	184mm×260mm　16开本　25.5印张　660千字
版　次	1999年12月第1版第1次印刷 2011年12月第2版　2011年12月第1次印刷
印　数	0001—3000册
定　价	42.00元

第二版前言

本书是普通高等教育“十一五”国家级规划教材，是对1999年12月出版的同名国家“面向21世纪课程教材”的修订版。

原书（《计算机系统的故障诊断与可靠性技术》）主要是针对研究生编写的。随着计算机在社会的各领域、各层面的日益广泛的应用，目前迅速发展中的社会经济活动，乃至每个家庭的日常生活，已越来越全面地依赖计算机了。在这种情况下，对于计算机的可靠性也提出了越来越高的要求。为此，国内有越来越多的理工科院校/理工科专业已经或将要面向本科生开设相关课程（本人也强烈呼吁各有关院校/专业应该这样做）。尤其在全国工科院校、工科专业普遍以教育部“卓越工程师计划”为牵引，高度重视工程教育的今天，让学生从本科甚至专科开始就认识“可靠好用”是任何工程的第一要务，就掌握必要的可靠性技术基础和技能，是非常重要的、必要的。

为了更好地适应本科生的教学特点及要求，本书在保持原有体系结构和总体编写原则基本不变的情况下，主要在以下方面对内容作了一定的增删、修改、更新：

（1）适当强调了避错技术在提高计算机系统可靠性方面所起的基础性作用，为此专门增加了避错技术中相对最重要的两种技术——电磁兼容设计和热兼容设计，将它们分别专列为一章，作为本书的第2章、第3章。前者包括电磁兼容技术概述、电磁兼容设计、电磁干扰抑制技术（屏蔽技术、滤波技术、接地与搭接技术）等内容；后者包括热兼容技术概述、防热设计、统计信号处理和温度补偿等内容。

（2）考虑到故障诊断与冗余容错技术在控制工程中的应用已越来越广泛深入，并且实际上已融合催生出控制领域一个新的学科分支——容错控制，而计算机控制系统显然又是本书定位的计算机应用系统的一个最重要的方面，所以新增了一章“容错控制技术”，将它放在讲完了各种避错、容错技术以后的第9章。

（3）为了更好地突出本书“设计与分析结合，以设计为主，分析为设计服务”的编写思想，将原书最后两章（“容错系统的可靠性分析评估”和“高可靠性计算机应用系统设计”）合并为一章“容错系统的可靠性分析与设计”。合并时，对可靠性分析部分，只保留对主要分析方法的介绍，而略去对不可维修系统、可维修系统和与预维修系统的可靠性分析的具体介绍。

（4）为了更好地反映软件可靠性技术的发展和体现可靠性技术“软硬结合”的特点，对原书第3章3.3节“以软件为主导的故障检测与诊断技术”（本书调整为第5章5.3节）进行了充实加强，介绍了计算机应用系统特别是计算机控制系统的故障检测与诊断技术中，目前常见或正在发展中的一些以软件为主导的方法技术，并结合科研实践介绍了基于状态观测器、基于卡尔曼滤波器和基于强跟踪滤波器的三种实用故障检测与诊断方法。同时，为更好地实现先进性和实用性的统一，对“软件可靠性技术”一章（原书第7章，本书调整为第8章）内容，也做了适当更新改造，删除了原书“软件可靠性模型”这节（原7.5节），而新增了“容错软件设计的其他常用技术”（现8.3.4节）和“虚拟化技术”（现8.4节）两小节。

（5）为篇幅所限，对原书中与故障诊断和可靠性技术的关系不很直接的“可测性设计技术”一章（原第6章）和“信息保护技术”一节（原7.4节），予以删除。

这次对全书内容进行增删、修改、更新，对全书体系结构进行优化调整，目的是想更好地突出故障诊断与可靠性技术的概念性、基础性及先进性、实用性内容，使之模块化特性更好，以更利于适应不同学校，不同层次教学的需求。但能否达到目的，有待于实践的检验和读者的评判。

本书凝炼了作者及所在单位多年来从事有关教学、科研的成果经验，融入了国内外有关领域的最新发展，系统介绍了计算机应用系统的故障诊断与可靠性设计、分析的基本理论和主要技术。经过修订后的本书，包括可靠性与可靠性技术概述、避错技术之电磁兼容设计、避错技术之热兼容设计、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、软件可靠性技术、容错控制技术、失败安全设计技术、应用系统的可靠性分析与设计等11章内容。全书贯彻了原理、技术与应用并重、软硬兼顾以硬为主的原则，注重内容选取的基础性、实用性、先进性和内容组织的科学性、严谨性、教学适用性。

本书修订改编工作仍主要由原书作者邹逢兴、张湘平负责完成。新编和主要更新/改编部分，第2、3、11章和8.4节由邹逢兴完成，张湘平参与了第2章的整理；龙志强主笔编写了第9章和5.3节，龙志强和李迅参与更新了第11章中两个高可靠性系统设计实例，结合自己科研实践成就了11.4.2节和11.4.3节。全书由邹逢兴主编，在申请并获批“普通高等教育‘十一五’国家级规划教材”之后，策划、提出了修订思想，确定了全书内容及组织结构，撰写了三级目录，交稿后审读修改、协调统一了全部书稿。

本书配有电子教案和素材文件，读者可以从中国水利水电出版社网站和万水书苑免费下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com。

衷心感谢中国水利水电出版社万水公司杨庆川总经理、雷顺加总编辑和李炎责任编辑在本书申报“普通高等教育‘十一五’国家级规划教材”及随后的修订出版过程中付出的辛勤劳动！

本书可作为高等学校信息类、控制类各专业的本科高年级学生和研究生的教科书使用，也可供从事故障诊断与可靠性技术研究、应用的工程技术人员参考。欢迎读者、专家随时指出书中可能存在的不足和错误！

邹逢兴

2011年6月于长沙

第一版前言

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？这是不言而喻的。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的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：

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。

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）。

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。

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。

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型巨型计算机的主任设计师、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

目　录

第1章

可靠性与可靠性技术概论

本章首先以国内外若干计算机系统故障引发的恶性事故为例，说明可靠性技术研究的必要性及其发展简况；然后，相继对可靠性技术研究的范畴，可靠性研究的四层次结构模型，故障与故障模型，表征系统可靠性的常用参数指标，以及串联、并联、串并联、并串联等简单结构系统的可靠性分析计算方法，进行概略性介绍，作为学习、理解后面各章内容的基础和前提。

1.1 可靠性技术研究的必要性

随着计算机应用的日益广泛、深入，现代社会对计算机的依赖程度越来越高，而且许多计算机应用系统，如卫星、飞船等航天系统，原子能反应堆，核电站，航空、列车等交通调度管制系统，金融股市管理系统，冶金、化工等过程控制系统等等，必须长时间连续运行，这些系统一旦发生故障而无法工作，将会造成重大经济或军事损失，甚至导致灾难性后果。实际中，因计算机系统不可靠而引发的恶性事故在国内外均屡见不鲜，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。受害人是该公司一名机器修理工，当时他维修好机器后正在按通电源准备试车，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。

1982 年，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。相反，在美国空军的一次编队飞行中，因火控计算机故障，竟向己方部队发射导弹，造成了自相残杀的严重后果。

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。

1991 年 6 月 18 日，载有美国航天局和几所大学的 10 个科学实验仪器的“探索者”号火箭在发射后不久由于导航系统故障导致迷失方向而坠毁。

1992 年 3 月 22 日，中国用“长征二号 E”火箭发射澳星，由于拧动点火控制器时，从螺钉上旋下一点点金属屑，使电路短路，火箭发动机熄火，发射没有成功。

1995 年 1 月 26 日，中国用“长征二号 E”发射亚太 2 号卫星时，由于美方没有告之卫星的谐振频率，而凑巧卫星的谐振频率与火箭整流罩的谐振频率相同，由于高空切变风对火箭的作用，引起共振，造成星箭爆炸。

1996 年 2 月 15 日，中国西昌卫星发射中心用新研制的“长征三号乙”运载火箭发射国际通信 708 卫星，火箭起飞后飞行姿态因故出现异常，飞行 22 秒后，火箭坠地发生爆炸，星箭俱毁。

1996 年 5 月 14 日，俄罗斯“联盟-U”号运载火箭装载一颗“宇宙”系列地形测绘卫星，从拜科努尔航天发射场发射升空 6 分钟后，因故障与地面失去联系，杳无音讯。

1998 年 9 月 10 日，乌克兰一枚天顶 II 型火箭在发射 12 颗商业卫星时于起飞后 272 秒出现计算机故障，导致星箭坠地。

2003 年 8 月 14 日，因计算机电力控制系统出现软件错误，导致了美国及加拿大部分地区的史上最大停电事故。

2004年12月22日，英国就业和养老金部正在执行每周例行的软件升级工作时，系统突然发生故障，全国1000多处办公室的80%的台式机停止工作或完全陷入瘫痪，受影响的8万多公职人员只能“望屏兴叹”。

2008年11月8日，俄罗斯“海豹”号核潜艇因计算机故障引发鱼雷舱的灭火系统意外启动，导致了20名官兵死亡和38人不同程度受伤的恶性事故。

近年来各地由于计算机控制的交通信号灯错误指示而引发十字路口车辆相撞的严重交通事故，由于银行ATM机发生故障而导致恶意取款的案例，更是常见于各种媒体报道中。

……

这一个个触目惊心的事例，促使人们不得不面对一个严峻的问题：计算机纵有多强的功能、多好的计算性能，如果不能可靠地工作，对人类到底是福还是祸？为了使计算机能真正造福于人类，人们显然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。

可见，研究、掌握可靠性技术并付诸于工程实施，对现在和未来从事计算机系统和计算机应用系统设计开发的科学技术人员来说，不仅是非常必要的，而且是一种崇高的责任。

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。

迄今为止，经过六十多年的发展，可靠性研究已成为计算机、自动化等学科领域中一个新的、独立的分支，正受到国内外越来越多的计算机、计算机应用系统和自动控制系统设计人员的重视。有关的学术会议不仅国际上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，每一两年都会召开一次相关会议，与国际年会相呼应。1991年7月，中国计算机学会还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、组织化的轨道。国家863计划、自然科学基金计划、国防预研计划、航空航天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研究及应用的立项支持，对推动我国可靠性技术的发展和应用发挥了重要的作用。

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：一是避错技术；二是容错技术。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 避错技术

避错技术实际上也就是提高元部件本身可靠性的技术。

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。包括电磁兼容设计、机械应力防护设计、热兼容设计、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 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。容错技术的基本思想是通过资源（给定元部件）的冗余和对资源的精心组织来实现容错，构成高可靠性系统，所以也常将它称为使用给定器件构成高可靠性系统的技术。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，而且能使系统的整体可靠性极大提高。

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，当系统中的冗余资源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。

故障检测与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或定位的手段，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。

上面所述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，软件故障在一定程度上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。

若将上述容错技术应用于计算机控制系统，与控制理论相结合，便形成了可靠性和控制两大领域的一个交叉学科分支——容错控制。

1.2.3 可测性设计

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的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、制造的现实。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少而全，又方便产生；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

在一些安全性要求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。

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（提高元部件可靠性的技术）	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	电磁兼容设计；应力防护设计；热兼容设计；“三防”设计
	质量控制	老化试验；筛选
容错技术（使用给定器件构成高可靠性系统的技术）	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 与三模一单模自净
	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