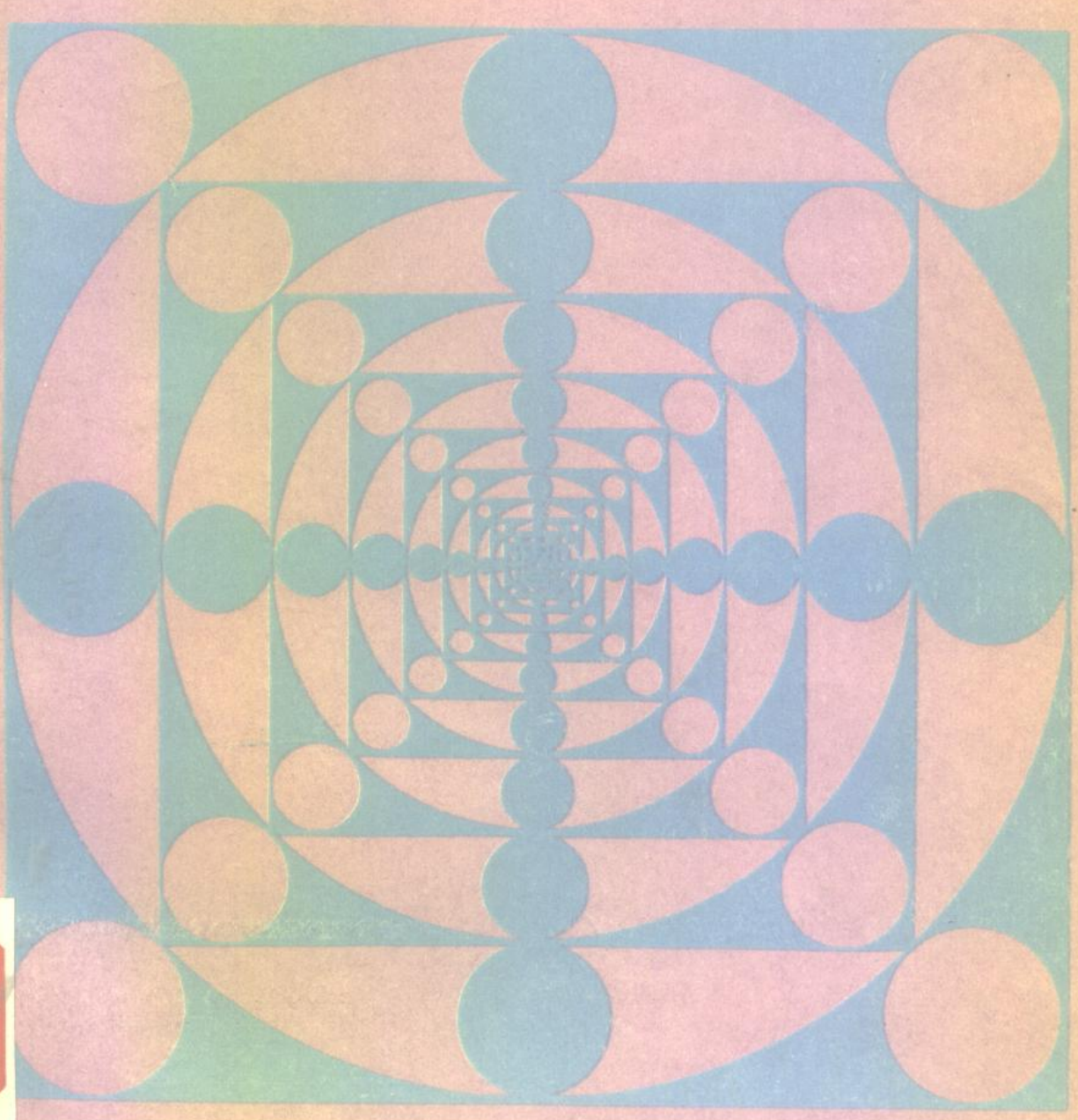
电子计算机应用系列教材

容错与避错技术及其应用

袁由光　陈以农 编著



科学出版社

电子计算机应用系列教材

容错与避错技术及其应用

袁由光　陈以农　编著

科学出版社

1992

（京）新登字 092 号

内 容 简 介

本书是“电子计算机应用系列教材”之一. 书中从理论和实践两个方面系统地介绍了各种容错和避错技术. 全书共九章，首先从故障的来源、表现及分布规律出发，简明地介绍了避免故障发生的各种避错技术，然后详细地阐述了发生故障后确保系统正常运行的各种容错技术，最后给出了高可靠系统的若干评价方法，并结合具体实例说明了如何利用各种容错技术来构造满足多种设计目标的容错系统.

本书可供从事可靠性技术研究和应用的工程技术人员及高等院校的有关专业师生参考.

电子计算机应用系列教材

容错与避错技术及其应用

袁由光　陈以农 编著

责任编辑　章安齐

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100707

武汉市华中电子产业开发集团公司激光照排

天津市静一胶印厂 印刷

新华书店北京发行所发行　各地新华书店经售

*

1992 年 2 月第 一 版　开本：787×1092 1/16

1992 年 2 月第一次印刷　印张：14 1/2

印数：0001—4300　字数：329 000

ISBN7-03-000905-3/TP·60

定价：9.50元

“电子计算机应用系列教材”主持、组织编著单位

主持编著单位：

国务院电子信息系统推广应用办公室

组织编著单位(按笔划顺序排列)：

广东、广西、上海、山东、山西、天津、云南、内蒙古、
四川、辽宁、北京、江苏、甘肃、宁夏、江西、安徽、
河北、河南、贵州、浙江、湖北、湖南、黑龙江、福建、
新疆、广州、大连、宁波、西安、沈阳、武汉、青岛、
哈尔滨、重庆、南京等35省、市、自治区、计划单列市

电子振兴
计算机领导小组办公室
科技工作

“电子计算机应用系列教材”联合编审委员会名单

(以姓氏笔划为序)

主编审委员：

王长胤* 苏世生 何守才 陈有祺 陈莘萌* 邹海明* 郑天健
殷志鹤 童 颋 赖翔飞 (有“*”者为常务主编)

常务编审委员：

于占涛 王一良 冯锡祺 刘大昕 朱维华 陈火旺 陈洪陶 余 俊
李 祥 苏锦祥 佟震亚 张广华 张少润 张吉生 张志浩 张建荣
钟伯刚 胡秉光 高树森 徐洁盘 曹大铸 谢玉光 谢育先 韩兆轩
韩培尧 董继润 程慧霞

编审委员：

王升亮 王伦津 王树人 王振宇 王继青 王翰虎 毛培法 叶以丰
冯鉴生 刘开瑛 刘尚威 刘国靖 刘晓融 刘德镇 孙令举 孙其梅
孙耕田 朱泳岭 许震宇 何文兴 陈凤枝 陈兴业 陈启泉 陈时锦
邱玉辉 吴宇尧 吴意生 李克洪 李迪义 李忠民 迟忠先 沈林兴
肖金声 苏松基 杨润生 闵福德 张志弘 张银明 张 勤 张福源
张翼鹏 郑玉林 郑 重 郑桂林 孟昭光 林俊伯 林钧海 周俊林
赵振玉 赵惠溥 姚卿达 段银田 钟维明 袁玉馨 唐肖光 唐楷全
徐国平 徐拾义 康继昌 高登芳 黄友谦 黄 侃 程锦松 楼朝城
潘正运 潘庆荣

秘 书 组：

秘 书 长：胡茂生
副秘书长：何兴能 林茂荃 易 勤 黄雄才

序

当代新技术革命的蓬勃发展，带来社会生产力新的飞跃，引起整个社会的巨大变革. 电子计算机技术是新技术革命中最活跃的核心技术，在工农业生产、流通领域、国防建设和科学研究方面得到越来越广泛的应用.

党的十一届三中全会以来，我国计算机应用事业的发展是相当迅速的. 到目前为止，全国装机量已突破三十万台，十六位以下微型计算机开始形成产业和市场规模，全国从事计算机科研、开发、生产、应用、经营、服务和教学的科技人员已达十多万人，他们在工业、农业、商业、城建、金融、科技、文教、卫生、公安等广阔的领域中积极开发应用计算机技术，取得了优异的成绩，创造了显著的经济效益和社会效益，为开拓计算机应用的新局面作出了重要贡献. 实践证明，人才是计算机开发应用的中心环节. 我们必须把计算机应用人才的开发与培养放在计算机应用事业的首位，要坚持不懈地抓住人才培养这个关键.

从目前来看，我国计算机应用人才队伍虽然有了很大的发展，但是这支队伍的数量和质量还远不适应计算机应用事业发展的客观需要，复合型人才的培养与教育还没有走上规范化、制度化轨道，教材建设仍显薄弱，培训质量不高. 因此，在国务院电子信息系统推广应用办公室领导、支持下，35 个省、市、自治区、计划单列市计算机应用主管部门共同组织 118 所大学和科研单位的 400 多位专家、教授编写了全国第一部《电子计算机应用人才培训大纲》以及与之配套使用的“电子计算机应用系列教材”，在人才培训和开发方面做了一件很有意义的工作，对实现培训工作规范化、制度化将起到很好的推动作用.

《电子计算机应用人才培训大纲》和“电子计算机应用系列教材”贯穿了从应用出发、为应用服务，大力培养高质量、多层次、复合型 应用人才这样一条主线. 这部培训大纲总结了近几年各地计算机技术培训正反两方面的经验，提出了计算机应用人才的层次结构、不同层次人才的素质要求和培养途径，制定了一套必须遵循的层次化培训办学规范，编制了适应办学规范的“课程教学大纲”. 这部培训大纲为各地方、各部门、各单位制定人才培养规划和工作计划提供了原则依据，为科技人员、管理人员以及其他人员学习计算机技术指出了努力方向和步骤，为社会提供了考核计算机应用人才的客观尺度. “电子计算机应用系列教材”是培训大纲在教学内容上的展开与体现，是我国目前规模最大的一套计算机应用教材. 教材的体系为树型结构，模块化与系统性、连贯性、完整性相兼容，教学内容注重实用性、工程性、科学性，并具有简明清晰、通俗易懂、方便教学、易于自学等特点，是一套很好的系列教材.

这部培训大纲和系列教材的诞生是各方面团结合作、群策群力的结果，它的公开出版和发行，对计算机应用人才的培训工作将起到积极的推动作用. 希望全国各地区、各部门、各单位广泛运用这套系列教材，发挥它应有的作用，并在实践中检验、修改、补充和完善它.

通过培训教材的建设，把培训工作与贯彻国家既定的成人教育、函授教育、电视教育和科技人员继续工程教育等制度相结合，逐步把计算机应用人才的培训工作引向规范化、制度化轨道，为培养和造就大批高素质、多层次、复合型计算机应用人才而努力奋斗，更好地推动计算机应用事业向深度和广度发展.

李祥林

1988年10月17日

前　言

随着计算机速度的提高、容量的增大和应用的推广，系统的可靠性问题越来越受到人们的重视.

容错和避错技术是提高计算机系统可靠性的两种主要手段. 尤其是容错技术，它是构造高可靠、超高可靠系统的强有力手段，也是当今十分活跃的一个研究领域，它已在国防、航空、航天等领域以及危险或恶劣环境、银行事务处理、工厂实时控制和医院病人监护等这些可靠性敏感的场合得到了广泛的应用.

本书从理论和工程实践两个方面系统地介绍了各种容错和避错技术. 本书首先从故障的来源、表现及分布规律出发，简明地介绍了避免故障发生的各种避错技术，然后详细地介绍了发生故障后确保系统正常运行的各种容错技术，包括故障检测、诊断、屏蔽、动态冗余和软件可靠性技术，最后给出高可靠系统的若干评价方法，并结合具体实例说明了如何利用各种容错技术来构造满足多种设计目标的容错系统.

本书在编写时注意了以下两点：一是把各种容错技术统一在编码理论之下，即把容错技术看成是对编码理论的实现，这对于系统地掌握容错技术，了解各种容错技术间的联系十分重要；二是理论联系实际，既强调基础理论，又注重实例介绍，特别注意近年来的新成果介绍，这样不仅可以深化读者对理论知识的理解，也可以对工程技术人员的实践提供指导.

本书可以作为从事可靠性技术工作的工程技术人员的培训教材，也可以作为有关专业的大学生、研究生的教材或教学参考书. 本书按 60 学时编写.

本书由陈廷槐教授审阅. 李卫华、王微、余长芬参加了本书的部分整理工作，王微和袁由光验算了本书的全部习题.

由于作者水平有限，错误和不妥之处在所难免，恳请读者批评指正.

编著者

目　录

第一章 绪 论

采用容错和避错两种技术可提高计算机系统和数字系统的可靠性.尤其是容错技术,它是构造高可靠系统的最有力手段,也是当今最活跃的一个研究领域.本章简要地回顾了可靠性技术的研究历史,概括地叙述了可靠性技术研究的各个方面及未来研究的广阔前景.

1.1 容错和避错技术的产生及发展

1.1.1 历史的回顾

性能、价格和可靠性是评价一个系统的三大要素.为了提高数字系统和计算机的可靠性,人们进行了长期的研究,总结出了两种方法.一种方法叫做避错,试图构造出一个不包含故障的"完美"系统,其手段是采用正确的设计和质量控制方法尽量避免把故障引进系统.要绝对做到这一点实际上是不可能的.一旦系统出了故障,则通过检测和核实来消除故障的影响,进而自动地或人工地恢复系统.第二种方法叫做容错,所谓容错是指当出现某些指定的硬件故障或软件错误时,系统仍能执行规定的一组程序(或算法),或者说程序不会因系统中的故障而中止或被修改,并且执行结果也不包含系统中故障所引起的差错.容错的基本思想是在系统体系结构上精心设计,利用外加资源的冗余技术来达到掩蔽故障的影响,从而自动地恢复系统或达到安全停机的目的.要达到高可靠性的目标,必须综合应用避错和容错两种方法.

人们对避错方法的研究与应用从计算机问世之日就开始了,为了使早期的电子管计算机能满足实际应用的要求,人们在机器的设计和生产过程中,对元器件进行严格的老化和筛选、实行减额使用,并对工艺生产过程严格把关,以使产品能满足设计任务书所规定的可靠性标准.计算机的发展经历了从电子管到晶体管,从晶体管到集成电路,直至目前的大规模集成电路和超大规模集成电路的更新换代,但无论在计算机发展的哪个时代,避错方法都是提高计算机可靠性的基本方法.时至今日,这门技术有了很大的发展,在计算机的研制过程中应用得十分广泛.美国的几家军用计算机公司,如 NORDEN 公司、EMM 公司、ROLM 公司和 MILTOPE 公司等,他们的基本策略就是瞄准当今流行的商用机,研究和利用各种避错技术,使这些计算机具有抗恶劣环境的能力,从而发展系列化、标准化的军用计算机.目前已推入市场的 PDP-11M,VAX-11M,SECS 军用微机模块系列及军用微机(加固 Intel 公司微机产品),MV 系列等就是其中的典型代表.我国已于 1986 年研制出了自己的抗恶劣环境计算机系列(980JX),并通过了国家级鉴定,目前正用于军事和工业控制领域.

人们对容错技术的研究也开始得很早，1952 年冯·诺依曼(Von. Neuman)就在美国加利福尼亚理工学院作过五个关于容错理论研究的报告，他的精辟论述成为以后容错研究的基础.

最初，人们从用四个二极管进行串并联代替单个二极管工作可以提高可靠性这一事实得到了启发，研制出了四倍冗余线路；从多数元件表决的结果较为可靠这一事实总结出了三模冗余和 N 模冗余结构；在通信中发展起来的纠错码理论也很快地被吸收过来以提高信息在传送、存储以及运算中的可靠性. 60 年代末，出现了以自检、自修计算机 STAR 为代表的容错计算机，标志着容错技术从理论上和实践上进入了一个新时期.

70 年代是容错技术研究蓬勃发展的时期，应用和研究范围迅速从宇航领域扩大到交通管制，工厂自动化，电话开关，医院病人监护，银行资金管理，空港管理，潜艇导航，边界、海岸及领空的保安、监护，战略防卫的控制和数据处理等领域，主要的成果有电话开关系统 ESS 系列处理机，软件实现容错的 SIFT 计算机，容错多重处理机 FTMP，表决多处理机 C. vmp 等.

80 年代是 VLSI 和微计算机迅速发展和广泛应用的时代，容错技术的研究也随着计算机的普及而深入到整个工业界，许多公司生产的容错计算机，如 Stratus 容错计算机系列，IBM System88，Tandem16 等已商品化并推入市场. 人们普遍认为：把容错作为每个数字系统的一个主要特征的时代已经到来.

国际电机和电子工程师学会(IEEE)从 1971 年起每年召开一次“国际容错计算年会(FTCS)”，并出版论文集，迄今开了 21 届，会议规模越来越大，近几年来，我国学者也陆续有论文在年会上宣读. 此外，我国科技工作者在诊断和容错理论的研究方面，在建造实际的容错计算机系统和应用容错技术方面也取得了不少成果.

1.1.2 展望

随着计算机的进一发展，特别是第五代计算机(FGCS)的发展，可靠性设计必将变得越来越重要，其原因如下：

(1)计算机性能的增高(即功能的完备和速度的加快)使系统的复杂性增加，主频加快，也将使系统更容易出错. 为了使系统的可靠性不随性能的增高而急剧下降，必须进行精心的可靠性设计.

(2)计算机走向社会，为各行各业所应用，计算机的使用者不再是计算机专业人员，这就要求计算机能够容许各种操作错误.

(3)计算机已从具有良好环境条件的机房迁移到各种应用现场，各种环境因素，如温度、湿度、电磁干扰、机械冲击和振动、盐雾、霉菌等施加于计算机上，使计算机更容易出错，这就要求计算机具有抗恶劣环境的能力.

(4)计算机硬件成本日益降低，维护成本相对增高，则需提高系统的可靠性能以降低维护成本.

由于上述原因，目前和将来的可靠性技术研究将向下面几个方向发展：

(1)瞄准优秀系列结构的商用机，走与商用机兼容的道路，研究和利用各种避错技术，发展抗恶劣环境计算机.

目前世界各国研制军用计算机的许多公司，为了减少重复开发的费用，他们根据商用

机与军用机在体系结构、计算类型、数据传输率、响应时间等没有本质差别的特点，瞄准当前的主流商用机，在逻辑和软件上全盘翻版，集中力量在计算机的结构组装、系统工艺、质量控制上下功夫，使研制出的计算机能在恶劣环境条件下稳定可靠地工作. 这种计算机在工业控制等民用部门也有着广泛的应用.

(2)随着 VLSI 线路复杂性增高，故障埋藏深度增加，发现故障难度增大，为增加芯片可控性和可观测性的可测试性研究已成为重要课题. 同时，随着整片集成 WSI(Wafer Scale Integration)技术的提出，硅片容错技术应运而生. 将动态冗余技术用于 VLSI 的设计，产生了称为 RVLSI(Restructurable VLSI)的技术. 用 PLA 进行容错设计是实现硅片容错的另一途径. 由于多值逻辑器件的出现，又提出了一种新的研究方向，即用冗余的逻辑值来实现容错. 这些思想和研究课题在五代机的可靠性研究中特别重要.

(3)在容错系统结构方面，已由单机向分布式系统发展，并尽量采用目前通用的微处理器以及微计算机来实现高性能的分布式容错系统，这已成为目前的主要趋向.

由于分布式系统具有模块性、并行性和自治性三大特征，它与集中式系统相比具有可靠、坚固，快速响应，易于修改、扩充，资源共享等明显的优点，因此容错系统结构已由单机向分布式系统发展. 利用局部网络的研究成果，采用现有的微处理器及微计算机，在局部网络中注入全局管理、并行操作、自治控制、冗余和错误处理是研究高性能、高可靠的分布式容错系统的便利途径. 在理论方面，至今还缺乏对分布式系统的形式描述和程序在分布式环境下的行为特性的研究和理解；在实际应用方面，实现冗余管理和错误处理方面还有许多困难. 总之，要建造一个完全分布容错的计算机系统，无论在理论方面还是在实际应用方面都有许多工作要做.

(4)对软件可靠性技术将进行更多的研究.

随着计算机硬件技术的飞速发展，软件开发的低效率与不可靠性已成为阻碍计算技术继续发展的主要障碍. 而软件领域中的可靠性技术研究，虽然也有 10 多年的历史，但进展却非常缓慢，只是到了近几年才受到普遍重视.

提高软件可靠性也有避错和容错两种方法. 避错法主要研究生产高可靠软件产品的程序设计方法和软件验证技术，容错法是指开发容错软件的适宜环境和系统方法，其主要目的是提供足够的冗余信息与算法程序，使系统在实际运行中能够及时发现程序设计错误，采取补救措施，保证整个计算机系统的正常运行. 目前对软件容错的研究还远不成熟.

(5)在容错性能评价方面，分析法和实验法并重，同时不惜花费昂贵的代价制作试验样机以获得满意的容错系统.

对高可靠系统性能的评价是一项重要而困难的工作. 例如对 SIFT 可靠性的评估是基于软件正确运行的假定，由于没有一种满意的方法用来估价软件出错的概率，因此唯一的方法是给出软件正确性的严格的数学证明. 尽管 SIFT 系统的软件设计采用了层次结构设计，但这一证明却花了 10 年以上的时间. 因此，研究有效的可靠性评估方法就十分迫切了.

为了获得建造一个容错系统的可靠数据，在部分容错系统的研制过程中，不惜花费高昂的代价先建立一个实验系统，通过实测数据确认该容错系统能达到的可靠性目标. 自检、自修计算机 STAR 就是为了验证待命储备冗余系统可能得到比单份无冗余系统高达 10 倍以上的寿命增益的预测而研制的实验样机.

为了对高可靠系统进行正确而有效的评估，分析法和实验法的研究都同等重要.

(6)在理论研究方面，人们企图建立包含“故障”状态的计算机模型，并提出一套容错系统的综合方法论，建立一个广泛的故障病理学和相应的故障防护学. 这是一项正在探索的困难的研究课题.

1.2 容错计算的特征及定义

1.2.1 可靠性研究的四论域信息模型

数字计算机系统极其复杂，为了便于研究，同时清除可靠性研究领域中许多含混不清的概念，可以按照物理的、逻辑的、信息的(统称内部的)、用户的(或称外部的)这样一个递增顺序构造一个层次结构模型来描述一个信息处理系统. 层次结构模型中的每一层次都包含各自的一组基本概念、模型和术语. 采用这个模型，设计要求、性能度量、正确特性样式、测试方法和概念规范都可以通过给定的论域描述. 系统由确定的原子元件以层次的、递归的方式来构造，在给定论域上的一个系统是较高论域上的一个子系统，等等. 在每一论域中，我们可以想象一个所有状态的划分，即系统可分为正确的和不正确的两个集合，这个划分借助给定论域的正确特性来获得. 此外，每个论域都有一个定时约定，它确定为考察和解释表示信息结构和控制信号的变量的合法的时间间隔. 系统的正常功能可由一个不希望事件 UE(Unexpectant Event)(失效，故障，错误，失败)而被破坏，这个不希望事件起源于一个内部的(物理的，逻辑的，信息的)论域，然后在上述论域中产生破坏作用. 容错系统的属性和实现它的方法论就可通过四论域，它们的不希望事件，不希望事件的检测算法和恢复算法来解释. 因此，我们可以把容错计算定义为当系统出现不希望事件时仍能正确地执行所规定的算法. 在这个意义上，所谓容错应当叫做容忍不希望事件，或容忍 UE.

1.2.2 不希望事件 UE 的分类

已经指出，四论域中的每一个都有各自的基本术语. 发生在物理域的不希望事件称为失效. 同样，从逻辑域到外部域我们依次把它们的不希望事件叫做故障，差错或错误，以及失败，其因果关系为失效→故障→错误→失败. 对于每一个论域，我们都可以根据原因，时间间隔，值和范围对该域的不希望事件进行分类. 由于逻辑域的变量只有两个值(不正确值和正确值，两者相反)，表现出固有的简单性，分析起来要方便得多，因此人们期望把其他论域中极其复杂和丰富多样的不希望事件等价在逻辑域来描述，并都把它归纳在简单的术语“故障”之下，这就需要建立所谓“故障模型”，然而这不是一件容易的事. 实践证明，对于有些物理失效和信息错误是很难找到其等价的逻辑故障的，尤其是随着技术的进步和不断更新许多具有新的特征的不希望事件不断出现，这样做就更加困难. 但是，这毕竟是把复杂的事物简化处理的行之有效的方法. 因此，我们主要讨论逻辑域中不希望事件(故障)的分类，当不能把其他论域中的不希望事件等价成逻辑论域中的“故障”时，或需要严格的分析讨论时，应就每个论域来讨论，但其方法是类似的.

(1)按时间间隔分为“永久故障”和“瞬时故障”.

永久故障是由元件中的不可逆变化引起的，如固定故障、二极管短路故障等，它永久地将原逻辑变成一个新逻辑.

瞬时故障是持续时间不超过一个确定的最大时间长度的故障.例如短时的外界干扰，α粒子对存储单元的影响(由温度和寄生电容引起的)，元件参数的暂时变化或程序员的误操作.这类故障只引起元件当前值的变化而不导致不可逆变化.

间歇故障(或伪瞬时故障)是由元件失效、不正确的设计或恶劣环境所引起的，当出现若干逻辑变量的组合时，这类故障才发生.如半导体存储器中的图形敏感故障，由边缘定时和未发现的竞争条件可引起这类故障.

(2)按值分为"确定值故障"和"非确定值故障".

确定值故障的故障变量保持在许可的一个恒定值上，例如引线开路，而非确定值故障允许故障变量在可能的值之间不断改变，如振荡故障.

(3)按范围分为"局部故障"和"分布式故障".

局部(单)故障是只影响局部逻辑线路(单逻辑变量)的故障，而分布式故障(相当于多故障)是包含有两个，三个，多个变量，一个子系统或整个系统的故障，分布式故障可能造成灾难性后果.

物理故障是由物理系统内部的(如半导体结的破坏)或外部的(电磁辐射等)原因引起的发生在逻辑域的故障.而人为错误(不正确的设计和误操作)是由设计人员或操作人员

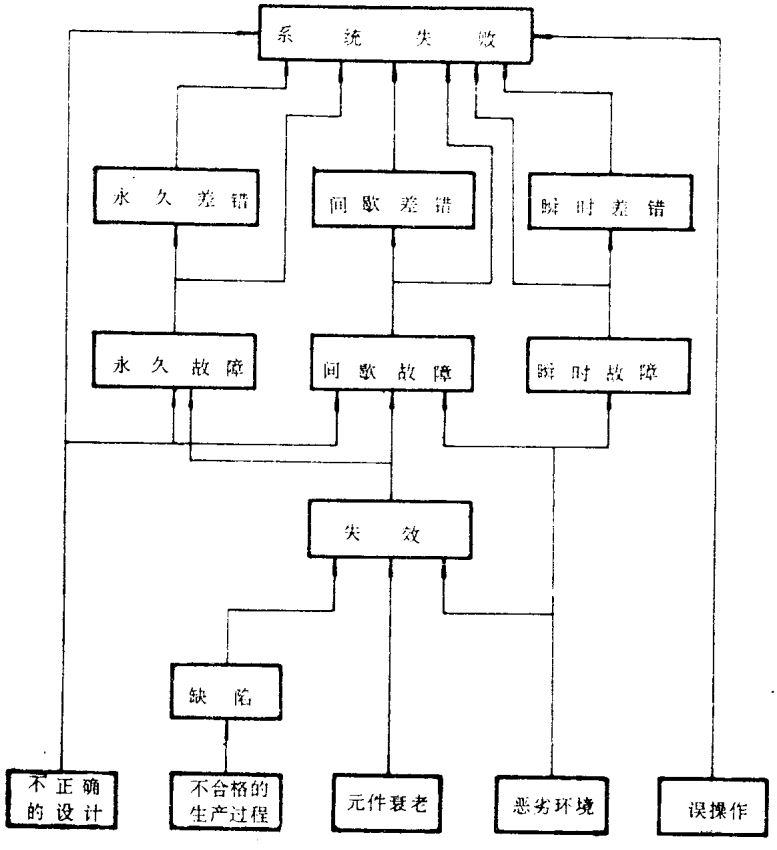


图 1.1 不希望事件及其原因

引起的错误.

值得指出的是,发生在逻辑域中的许多故障的起源点是物理域中的元件失效.

不希望事件及其原因可以简略地用图 1.1 表示.

1.2.3 容忍不希望事件 UE

已经指出,有两种基本的方法可获得可靠的信息处理.第一种叫做避错法,第二种叫做容错法.无论哪种方法,其目的都是控制系统中可能发生的不希望事件.要实现容错法,首先应确认被容忍的不希望事件的规范,其次要选择与该不希望事件的类别相匹配的检测算法,并在此基础上设计出恢复算法,以便由选定的检测算法所调用,并使系统回到正确操作的某个级或者安全停机(系统恢复).实现方法选定之后,应对其性能进行数量估价(容错性能评价)以确定其有效性并使设计精确化(设计精加工).

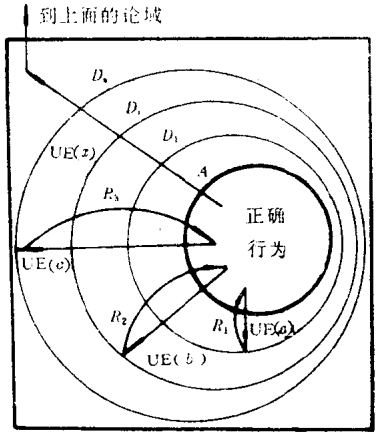


图 1.2 内部论域的防卫结构

信息处理系统三个内部论域(物理的,逻辑的,信息的)中的防卫方案的一个简单抽象模型如图1.2所示.图中所有避错技术形成一个环绕正确行为的防卫圈 A,n 个不同的不希望事件的检测算法由标号为 $D_1,D_2,\cdots,D_i,\cdots,D_n$ 的环来表示,箭头 UE(a),UE(b),UE(c)表示由这些算法检测的 UE,而弧 $R_1,R_2,\cdots,R_i,\cdots,R_n$ 表示由检测算法所调用的恢复算法的成功作用.A 和 D_n 之间的弧表示可恢复的不正确特性,而 D_n 之外的面积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不希望事件 UE(失效,故障,错误)存在的内部论域中,因此,这些 UE 的出现在所论域中被有效屏蔽,从而达到容忍 UE 的目的.图中 UE(x)表示一个 UE,它不可能由 n 个检测算法中的任何一个检测,并且在内部域中产生了一个不可恢复的不正确行为.该 UE 不能被屏蔽,且将在外部论域中产生一个不希望事件,很可能导致灾难性后果.

1.2.4 容错计算四要素

实现容错计算包括下面四个主要方面:

(1)UE 的检测:为了容忍系统中的一个 UE,其后果应当首先被检测.当一个失效(或故障)不能由系统直接检测时,该失效(或故障)往往表现为系统中某些地方的错误(信息域),因此,容错技术通常的出发点是错误状态的检测.

(2)损坏估价:当检测出一个错误时,系统的许多状态都可能被怀疑,而不只是怀疑初始发现的错误状态.由于一个失效(或故障)的出现和它的错误结果之间可能存在延迟,错误的信息可能已经传播到该系统的其他地方,导致错误的扩大.因此,在作出一个被检测的错误有关的任何决定之前,有必要鉴定系统已被破坏的程度.这就依赖于系统设计者的策略和已有的探测技术.

(3)UE 的恢复:在 UE 检测和损坏估价之后,应采用 UE 恢复技术,其目的在于把目

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. 否则，系统损坏可能继续发生.

(4)UE 处理和继续服务：尽管 UE 恢复阶段可能已使系统回到无 UE 状态，仍旧需要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 处理的第一步是试图精确地定位 UE，紧接着是恢复 UE 或重新配置其余的系统以避免发生 UE.

这四个方面形成所有容错技术的基础，从而也是设计和制造容错系统的基础. 各个阶段之间可能有很大的互相影响，导致一个具体系统中这几个阶段识别的模糊. 例如，保护机构常常提供一种形式的错误检测，并可能在设计和实现损坏估价阶段也起着重要作用. 类似地，对一个系统的损坏估价将利用探测方法来识别可能的破坏，测量本身也采用 UE 检测技术，等等.

1.2.5 实现容错计算的主要方法

容错计算是依靠外加资源的方法来换取可靠性的. 外加资源的方法很多，主要的有外加硬件，外加信息，外加时间和外加软件，这些方法往往要合理使用才能达到高可靠性的目标.

1. 硬件冗余

广泛应用的硬件冗余之一是硬件堆积冗余，在物理级可通过元件的重复而获得(如相同元件的串、并联，四倍元件等). 物理域的恢复作用是自动的，即不需单独的检测，但每一次失效将削弱防卫. 在逻辑域可采用多数表决方案，如三模冗余、N 模冗余、分段冗余、修复机构等.

另一硬件冗余方法叫做待命储备冗余. 该系统中共有 $m+1$ 个模块，其中只有一块处于工作状态，其余 m 块都处于待命接替状态. 一旦工作模块出了故障，立刻切换到一个待命储备模块，当换上的储备模块发生故障时，又切换到另一储备模块，直至资源枯竭. 显然，这种系统必须具有检错和切换装置.

将堆积冗余和待命储备冗余结合运用构成所谓混合冗余系统. 当堆积冗余中有一个模块发生故障时，立即将其切除，并代之以无故障的待命模块. 这种冗余方式既可达到较高的可靠度，又可达到较长的无故障运行时间.

上述三种容错基本结构统称为 K 出自 N 结构. 该结构中共有 N 个相同的模块，其中至少有 K 个是正常的，系统才能运行. 这种结构能容忍分别出现在 $N-K$ 个模块中的 $(N-K)$ 个独立的故障，或称其容忍故障能力为 $t=N-K$.

对有人维修的系统，一有故障就能排除，两模块就能起到多模块的作用，因此可构成双模冗余系统. 在部件级和整机级可实现双模结构. 在整机级可采用双机交替工作，双机协同工作和修理不停机等工作方式.

近年来，随着线路密度的大大增加，自动生成测试模式和利用这些测试模式进行故障模拟的能力急剧减弱. 解决这个问题的中心思想是提高系统的可控制性和可观测性，人们把对它的研究归纳在“可测试性设计”这个技术范畴之中，并受到普遍重视. 其中大多数是通过增加硬件资源来达到目的的.

可测试性设计可分为两类. 第一类是针对一个具体的设计，提出一个适合于提高该设计的可控性和可观测性的一个特殊方法，该方法没有普遍意义，如划分、增加测试点、总线结构、特征分析等. 第二类叫做构造法，它具有通用性，一般包括一组设计规则. 构造法的目的是减少一个网络的时序复杂性，往往把一个时序网络当作组合网络来处理，诸如级敏感扫描设计，扫描通路，扫描/置位逻辑，随机访问扫描等.

2. 时间冗余

时间冗余是通过消耗时间资源来达到容错的. 时间冗余的一个应用是程序卷回. 这种技术用来检验一段程序完成时的计算数据，如有错，则卷回重算那个部分. 如果一次卷回不解决问题，还可多次卷回，直到故障消除或判定不能消除故障为止.

指令复执是时间冗余的又一应用. 所谓指令复执就是重复执行已发现错误的指令，如果故障是瞬时的，在指令复执期间，有可能不再出现，程序就可继续向前运行，如果在指令复执期间不能解除故障，则需通过人工干预或调用诊断程序来消除故障.

利用诊断程序对系统进行初始检查、联机检查、周期性检查都可看作是时间冗余的应用. 人们对故障的检测与诊断方面的研究，历史悠久，成果显著，例如 D 算法、布尔差分法、星算法、多值算法、因果分析法、图论法等都是产生故障检测和诊断测试集的有效方法.

3. 信息冗余

信息冗余是靠增加信息的多余度来提高可靠性的. 这些附加的信息位具有如下功能：当代码中某些信息位发生错误(包括附加位本身的错误)时能及时发现错误(检错)，或者能恢复原来的信息(纠错). 一般而言，附加的信息位越多，其检错纠错能力越强. 在数字系统中的信息传送，算术逻辑运算中广泛使用的奇偶码、海明码、乘积码、循环码，各种算术误差码都有很强的检错、纠错能力.

信息冗余的优点是增加的冗余度比别的方法低，而且许多码的信息位和校验位在运算中可统一处理. 此外，它还能纠正瞬时错误，提供故障的自检测、自定位、自纠错能力，其缺点是产生时延，难于纠正编码器和译码器本身的错误.

4. 软件冗余

提高软件的可靠性有两种方法. 一种是研究无错软件，另一种是研究容错软件.

无错软件曾经是过去有关容错的许多文章研究的课题. 通常假定，一个可靠的软件一经产生，它在以后的运行中仍保持是可靠的. 当然，这个假定取决于使用软件的正确性，支撑软件的系统的正确性，软件维护的正确性等. 因此，在上述条件下，无错软件就是在软件的使用时间中无错的软件.

无错软件的研究主要包括三方面的内容：

(1)寻求导致高可靠软件产品的程序设计方法. 目前已为人们广泛接受的结构化程序设计方法就是一例.

(2)软件测试技术. 该方法是在软件设计完成后，交付用户之前施行的. 如验收测试技术等.