计算机系统硬件软件可靠性理论及其应用

傅佩琛　赵　霖　张军英　编著

国防工业出版社

计算机系统硬件软件可靠性理论及其应用

计算机系统硬件软件可靠性理论及其应用

傅佩琛　赵　霖　张军英　编著

国防工业出版社

内 容 简 介

全书共分十一章，主要内容包括：绪论；可靠性的基本概念及其数量特征；系统可靠性数学模型与分析；检错和纠错码理论与应用；系统的可靠性设计与维修性设计；系统硬件的冗余结构设计；计算机系统的故障诊断；软件可靠性的基本概念；软件错误及其分类；软件可靠性模型及其应用；计算机安全保密问题等。

本书可供高等院校计算机专业本科生和研究生使用，也可供从事计算机系统研制、设计、生产和使用维修人员阅读。

计算机系统硬件软件可靠性理论及其应用

傅佩琛 赵 霖 张军英 编著

*

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号)

(邮政编码 100044)

新华书店北京发行所发行 各地新华书店经售

西安电子科技大学印刷厂印装

*

787×1092 1/16 印张 19 436 千字

1990 年 4 月第一版 1990 年 4 月第一次印刷 印数: 0001—2200 册

ISBN 7-118-00613-0/TP·79 定价: 8.60 元

序　言

信息社会化是不可逆转的历史潮流。1957 年苏联发射第一颗人造卫星，标志着全球信息革命的开始。这是人类历史上的新的重大转折，它标志着工业革命的终结和"信息社会"开始。信息革命就是第四次产业革命，即以微电子技术为先导和为核心的新技术革命。新技术革命将把人们带入信息社会。

所谓信息社会是把计算机、软件技术、通信系统、无线广播、电视和自动化系统组成一个完整的信息系统的社会。简而言之，信息社会就是计算机与通信相结合的社会。

随着科学技术的进步，特别是以电子计算机和现代通信设备为代表的信息技术的发展，使社会面貌发生了根本的变化。过去，人们靠机械能只可延伸人的体力，当今，电子计算机等信息技术已成为延伸人的脑力的有力工具，人类将以空前的规模从事信息的采集、储存、传输、处理、利用和管理，信息已成为与能源和原材料并驾齐驱的重要资源。这种变化将深刻地影响着科技、经济和社会的发展，将使产业结构、就业结构重新排列组合。在这一变革中信息业将迅猛发展，信息业、信息部门在国民经济中不断壮大的过程，也就是社会信息化的过程。社会的信息化和信息社会的到来是不可避免的，是必然的。现在发达国家从事信息工作的人员已超过劳动力总数的 60%，总产值占国民生产总值的比重为 40～65%，而我国信息部门的劳力只有 9%，信息部门的产值所占比例仅为 15% 。这说明我国的信息化程度与日本和美国相比分别要差 30 和 60 余年。

在社会信息化的过程中，电子计算机具有十分重要的地位。当前，计算机已广泛用于国防、工农业生产、科研教学、交通、银行、商店、医院等各个行业做为指挥、控制、自动化、事务与金融管理和医疗诊断的重要手段。电子计算机的研制、生产能力、使用状况、装机台数和从业人员数标志着一个国家现代化的水平。在这许多方面我国与技术先进国家相比有较大差距，电子计算机技术领域的科技人员面临的任务是十分艰巨的。

为了迎接新技术革命的严重挑战，制定我们的对策，国务院技术研究中心和中国科协联合开展了 2000 年的研究。中国电子学会印发了"中国电子科学技术国内外水平和差距"一书，指出了电子各学科赶超世界先进水平的具体措施和建议。电子部还召开了厅局长会议，提出了到 2000 年的奋斗目标和发展规划。到 2000 年电子工业总产值要比 1980 年翻三番，要狠抓以大规模集成电路和计算机为重点的基础产品。

此外，科学技术的进步和电子计算机的广泛应用又对电子计算机的性能和可靠性提出了更高的要求。要求计算机系统能够不断地为用户提供服务，要求运算、处理结果正确无误，同时也要求数据、信息存取和传输的正确。随着计算机更广泛更深入到社会，便形成了生产活动、经济活动和社会活动全面依赖于计算机的局面。在这种情况下，如果计算机质量低劣、可靠性差、经常发生故障，则其经济效益和社会效益必然大幅度地下降，以至丧失其功能，从而使生产、经济和社会活动陷入混乱状态。显然，计算机系

统的可靠性是实现信息化社会的技术关键．人们预言，到公元2000年世界上95%的计算机将是高可靠的容错计算机，因此对计算机高可靠性和容错计算机的研究更具有深远的重要意义．

编著者多年来从事电子设备可靠性工程、计算机系统可靠性、计算机安全保密和故障诊断的教学与科研工作．近几年以来又同张泽增教授一起开展了软件可靠性的科研工作，为计算机软件专业研究生开设了软件可靠性课程．编写过程中，在原有讲稿的基础上又补充了大量资料．为迎接信息社会和我国电子计算机事业大发展的到来，特编成此书以供本专业大学生和研究生使用．同时可供从事计算机系统研制、设计、生产和使用维修人员阅读．书中列举了一些计算实例和实际的系统结构，因而便于自学．

全书共十一章．第一至六章和九、十章由傅佩琛编写，第七章由张军英编写，第八和十一章由赵霖编写．第一章绪论、第二至六章内容为：硬件可靠性的数量特征、数学模型、检错与纠错码及可靠性与维修性设计，其中第六章着重研究系统硬件冗余结构设计，第七章为计算机系统的故障诊断，第八到十章叙述软件可靠性的基本概念、理论及其应用技术，第十一章为计算机的安全保密问题．

在计算机系统硬件可靠性设计中，除可靠性指标预计与分配等设计基础和冗余结构设计之外，对于其他保障系统可靠性的设计技术，本书未具体涉及，读者可参阅电子设备与系统可靠性著作．

本书承蒙西安电子科技大学计算机系赵树芗教授和张泽增教授分别对硬件可靠性和软件可靠性进行了全面而详细的审核与校对，提出了宝贵的意见，给编者以积极的支持和帮助．孙青教授和赖金福副研究员对本书的出版给予积极支持并做了大量工作，在此，表示衷心感谢．

编者于西安电子科技大学

1989年10月

目　录

第五章 系统的可靠性设计与维修性设计

第六章 系统硬件的冗余结构设计

第七章 计算机系统的故障诊断

第八章 软件可靠性的基本概念

第九章 软件错误及其分类

第十章 软件可靠性模型及应用

第十一章 计算机安全保密问题

第一章 绪 论

§1.1 研究计算机系统可靠性的重要性

被人们广泛誉为世界上第一台电子计算机 ENIAC 中使用了 1800 只电子管，总重达 30t，耗电量为 100kw，要占用 30m 长的机房。由于当时电子管的失效率只有10^{-4}／小时，所以整机的平均故障间隔时间只有 30min，这是无法满足实际使用要求的。1944 年的计算机 Bell relay 为了能正常运行，除了对每一计算都要执行两次之外，还采用检错码。第一台用于商业的计算机 Univac I （1951 年）中广泛采用了奇偶校验码，此外还用两个运算逻辑部件，以匹配——比较方式工作。四十年来电子计算机经历了电子管、晶体管、小规模集成电路的三代，现已发展到采用超大规模集成电路的第四代计算机，当前一些技术发达国家已着手研制第五代计算机。自计算机问世之日起，可靠性一直是计算机系统设计必不可少的重要指标。尤其是晶体管发明以后，由于半导体技术的飞速发展使计算机的基本元素——器件的可靠性迅速提高，此外由于在计算机系统可靠性设计方面采用了冗余技术、差错控制、故障的自动诊断、定位以及恢复方面的可靠性技术的发展才使它以强大的生命力和适应性广泛应用于各个领域。在国外，计算机系统大约在五～七年内更换一代，经过六年时间运算速度提高十倍，存储容量增加二十倍，可靠性提高十倍，价格降低到四十分之一。由此可以说，计算机产生、发展及实际应用的历史，即使说成是可靠性技术发展的历史并非言过其实。

计算机作为信息工业的基础，新技术革命的带头产品必将大力发展，而且随着科学技术及其应用的大发展也将对计算机系统的可靠性提出更高的要求。亦即计算机系统的可靠性将变得越来越重要。其原因是：

(1) 随着计算机功能的日益完备和运算速度的加快，其组成日益复杂、所使用的元器件日益增加、装配密度日益加大，这都将使计算机系统发生故障的概率增大。

(2) 由于计算机系统的应用日益广泛，计算机的使用场所将不只是有空调、屏蔽，无冲击、无振动的试验室，而将可能是高低温、高湿、电磁或核辐射干扰、冲击、振动等恶劣的环境之中，这些恶劣的环境都将产生硬设备、软件、数据、信息的故障或错误。

(3) 随着大规模集电路和超大规模集成电路的社会化大生产，使得计算机硬件的研制和生产成本日益降低，而维护使用的成本相对提高。事实告诉人们，只有提高计算机系统的可靠性，减小发生故障的概率才可以降低维护使用成本。

(4) 还由于计算机系统的广泛应用，计算机操作使用人员日益增多，这就要求计算机系统必须能够防止或容忍人为的操作失误。

(5) 随着计算机为政府机关、军事机关、企业，以至个人处理越来越多的更为重要以至机密的重要信息，人们将更加担心信息的破坏、信息的被窃取以至信息被恶用等事故的发生。

(6) 随着计算机大型系统或应用软件的研制，软件可靠性又成为人们广泛关注的十

分重要问题.

计算机实际应用的历史同时也是计算机可靠性发展的历史，计算机可靠性是计算机应用实践的要求，在当前还可能不能被所有从事计算机科研、生产、使用，以至教学人员所接受．为了说明这个问题可以举以下事例.

设在科罗拉多州夏延山洞内的北美防空司令部中的大型电子计算机系统同导弹防御网相连．司令部声称，当敌人向美国发射导弹时，计算机系统能立即发出警报．1979年11月9日，计算机突然发出警报信号，指出从美西海岸上一艘潜艇发射的一枚导弹正向美国袭来，在场的工作人员被吓得目瞪口呆．紧接着，指示板宣布进入低级"核战争状态"．几分钟内，十架喷气式截击机从美、加的空军基地起飞，分布在美国本土上的一千多个民兵导弹地下井进入警戒状态．与此同时，联邦航空局所属的各交通管制中心发出了刺耳的笛声，负责官员向各民航班机发出准备着陆的信号．但是，在警报发出后的六分钟，人们才发现这是由于计算机出故障而造成的事故．同类事件，在1980年1月3日和6月6日还发生过两次.

美国曾向火星发射"水手一号"火箭，仅仅因计算机的程序脱落一个字符而宣告失败，造成重大的政治和经济损失.

60年代后期，在国外常因软件错误而使整个计算机系统陷于瘫痪状态．美国范登堡空军中心在此期间多次发生导弹发射试验失败的重大事故，都是因计算机软件错误造成的.

在布鲁塞尔召开的一次国际博览会上，吃饭是由电子计算机来安排的，由于计算机出了故障，造成五千人没有吃上饭.

1979年，美军使用计算机指挥一次军事演习，由于计算机失灵，使进攻与撤退的部队次序颠倒，造成了极大的混乱.

美空军的一次编队飞行，因火控计算机的故障竟向本军方飞机发射了导弹，造成了极严重的后果.

1987年12月9日，布鲁塞尔《晨报》报社的计算机出了故障，报社无足够的打字机来承担报纸的排版，只好用手写制版印刷发行.

在冶金系统采用计算机后可大大提高生产效率．如带钢热轧机采用计算机控制以后，轧速可从每分钟20 m提高到1500 m，提高工效75倍．可是如果计算出故障，在短时间内就会造成数万米钢带的报废，损失是极其严重的.

意大利国家数据库曾遭到破坏，在6 s时间内被破坏的数据，经过长达六年时间才重新恢复起来.

在计算机网络出现之后，计算机和通讯系统组合成大而复杂的系统，如果没有有效的可靠性保证措施，或不进行严谨地可靠性设计的话，是很难完成其预期功能的．同时也要求信息得以迅速而可靠的传输，于是提出了信息保护以免遭破坏的问题．但是，时至今日世界上还没有十分有效的解决信息保护的问题．人们还在深入探索与研究之中.

60年代初，由于计算机在微电子电路的迅猛发展的条件下，其硬件功能以惊人速度发展且硬件成本不断降低，软件的开发费用就已超过了硬件的开发费用．到80年代中后期，软件开发费就已占总费用的85～90%,硬件和软件开发费的变化情况如图1-1

所示。此外，到 60 年代的中后期，由于计算机及其软件的发展，在国外就已进入了所谓软件危机时期。如，60 年代 IBM 公司生产的 OS／360，花费了五千人一年的巨大代价，其软件在平均每修改后仍大约存在一千个左右的错误，交付使用的软件也因软件故障使系统陷于瘫痪。范登堡空军中心多次因软件故障导致导弹发射试验失败就是突出的事例。这就迫使人们认识到研究软件可靠性的重要性和迫切性。自 60 年代以来相继召开了一系列软件可靠性研究的重要会议，大大促进了软件可靠性研究的发展。

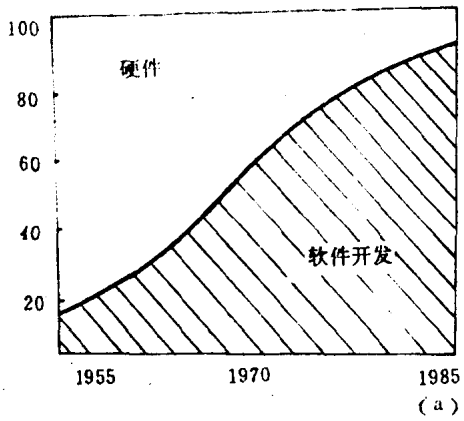

图 1-1 硬件、软件费用发展变化趋势

软件维护费用，尤其是大型复杂软件的维护费用已大大超过了软件研制费用。1985 年的软件维护费已达到或超过硬件软件总费用的 60%。软件维护费与软件可靠性有极为密切的关系，提高软件可靠性就可以大大降低软件维护费。从而也就降低了计算机系统的全寿命周期费用。

在过去的十五年内计算机的功能差不多增加一万倍，而每个功能单元的价格下降了十万倍。图 1-2 上示出了在一块微电子电路片上电子元件数即集成度随年度增加速度。60 年代中期一片电路上的元件数为 256 个，十年后增大了一千倍。1963 年一台计算机需要连接几万个接头，每一个接头（即焊点）都有发生故障的可能。而现在在大规模集成电路板上要接的元件不到十个，其焊点数大大减少。这个趋势仍在继续发展。

图 1-3 为几代随机存储器（RAM）电路每位存储费用下降的曲线。1983 年与 1975 年相比，其价格下降了八倍多，其性能却提高了许多。

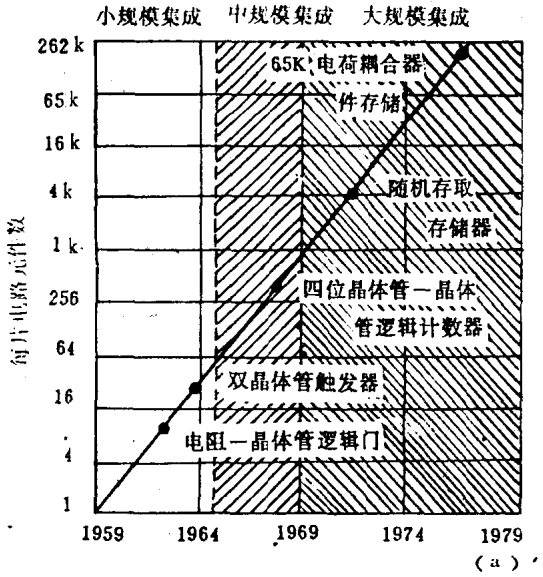

图 1-2 集成电路集成度的演变

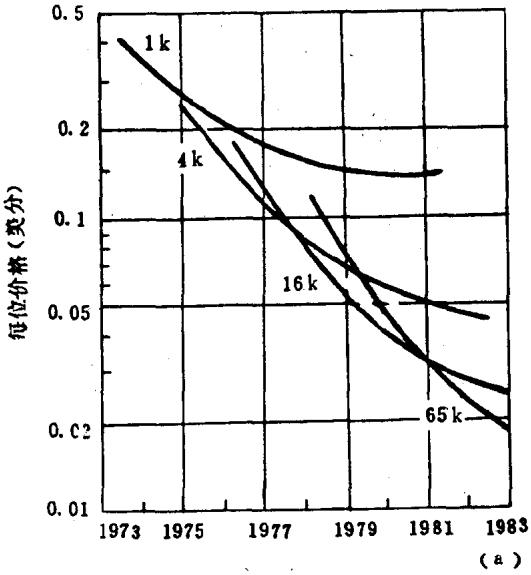

图 1-3 几代 RAM 每位存储费用

图 1-4 分别描绘出作逻辑门的真空管、分立晶体管、小规模集成电路、大规模集成电路情况下的每门相对价格下降情况。其中 LSI 的价格随时间下降最为迅速。而图 1-5 示出了这四种元器件故障率下降即可靠性增大的情况。

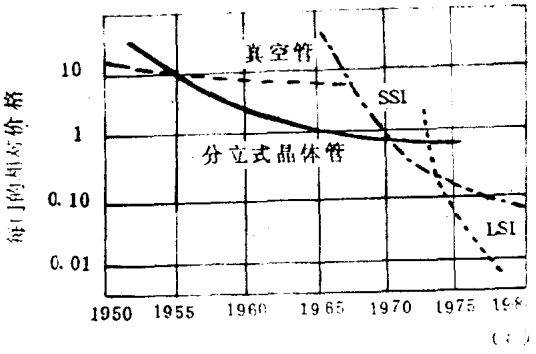

图 1-4 各种逻辑门价格下降情况

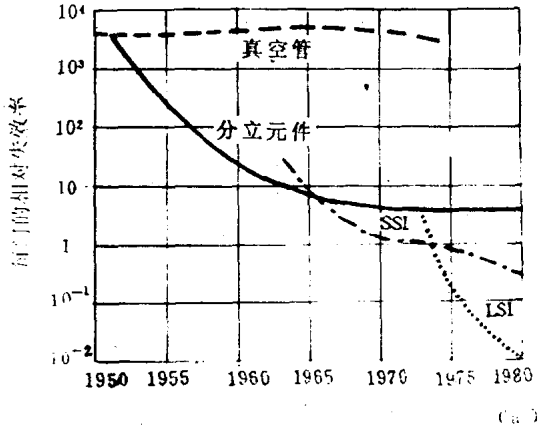

图 1-5 各种电子元件可靠性增大情况

以上各图的情况说明计算机系统硬件成本逐年下降，性能逐年提高，可靠性逐年提高。

软件可靠性，尤其是大型计算机系统的软件更为重要。因为它直接关系到政治、经济、军事的战略决策以及大型科学试验或武器试验的成败。若是因软件故障而导致重大事故将给国家政治、经济和生命财产安全造成重大损失。

硬件可靠性、软件可靠性、信息可靠性以及人员操作的可靠性都属于计算机系统可靠性所要研究的内容。它们对于计算机系统来说，都是十分重要的问题。

§ 1.2 计算机可靠性的简要发展历史

可靠性理论及其应用技术的研究起始于第二次世界大战。在大战中希特勒德国研制并使用了 V-1 和 V－2 火箭，根据故障率高和命中率低的实际情况需要出发便开始了对可靠性的研究工作，后因失败而告终。

在二次世界大战中，雷达等电子设备发展很快，其中最主要的构成单元——电子管经常发生故障，所以美国当时可靠性的研究工作的重点是研究故障占大多数的电子管。研究长寿命电子管时，不仅重视其电性能，而且十分重视耐震、耐冲击等方面的因素。此时都是定性的研究。

系统的定量的研究工作是从朝鲜战争中开始的，并应用了概率论和数理统计这一强有力的数学工具。大约用十年时间完成了对可靠性的基本研究，而后又从使用的角度考虑可靠性，从经济的角度考虑可维修性和从成本费用方面来研究。再就是对元器件进行失效机理的研究，形成了可靠性工程中的一个重要分支——故障物理学，或称做可靠性物理。

日本是从美国引进可靠性技术的，1956 年成立了长寿命电子管专门小组，电子学

会于 1960 年成立了可靠性及质量控制专门机构，在年会上经常进行可靠性学术交流。当前日本在许多方面处于领先地位，大规模集成电路的可靠性水平都优于美苏两国，有的产品已经达到可以在美国建厂的水平。

人们通常把可靠性工程三十余年的发展历史大体分成以下四个阶段：50～57 年的调查研究阶段；195 7～1962 年的统计试验阶段；1962～1967 年的可靠性物理研究阶段；自 1967 年开始的可靠性保证阶段。在当前这一阶段中，在电子元器件的失效率为 10^{-9}／h（相当于 MTTF＝10^{9} h，即 114156 年）的基础上是加强整机高可靠性的实现和可靠性保证、管理、认证制度，以及数据和技术标准的新技术研究，并引用其他学科的新成果，向更高的目标前进。

电子计算机，作为电子设备中极其重要的一类，其可靠性技术的发展基本上也是同上述各发展阶段同步发展的。电子计算机硬件的可靠性是电子设备可靠性理论的具体应用。电子计算机发展的最初阶段，即电子管时代，尽管采用了初步的硬件冗余技术和奇偶校验的时间或信息冗余方式，其可靠性还是比较低的，很难满足实际使用的要求。

1947 年晶体管的发明，以及以后 1958 年集成电路 1967 年大规模集成电路、1978 年超大规模集成电路的相继研制成功，才使得电子计算机在小型化、性能、可靠性、节能耗以及价格方面一次次地取得进步．微电子技术的突飞猛进使得电子计算机的最主要的构成元素——器件可靠性迅速提高，为计算机系统的高可靠性打下了坚实的物质基础。此外，在整机系统可靠性方面，由于采用了电路、部件及系统级的冗余技术、差错控制技术、故障的自动诊断等可靠性技术，于是计算机整机的可靠性也在不断提高，计算机系统的可靠性每经过六年时间 MTBF 就要提高 10 倍。

近几年来，国外计算机学术界纷纷探讨并已开始研制新一代即第五代计算机．第五代计算机将主要有以下特点：① 具有听说看的高度智能性质，有学习、联想、推理及解决问题的多种功能；② 改善软件环境、减轻软件负担，可用自然语言实现人一机对话；③ 大容量、高速、高适应性、高可靠性和保密性．第五代计算机的研制成功，将在计算机系统高可靠性方面取得更大的进展。

尽管在计算机可靠性应用理论方面与其他电子设备（如，雷达、通讯、电视机等）有许多相似之处，也有许多不同的特点．在计算机系统的可靠性技术中，一方面是在硬件研制中选用高可靠的元器件，对元器件进行 100%的老化与筛选及认真的布线、热设计等尽量减少故障出现的概率．这就是所谓有的避错（fault avoidance）技术．此外，是利用冗余提供的信息来掩盖错误的影响，其中包括额外的硬件或额外的时间．即所谓硬件冗余和时间冗余。硬件冗余是利用额外的电路、逻辑门、存储单元、分机或整机等来掩盖故障的影响；同一计算任务执行两次的结果进行比较和采用检测与纠错编码都属于时间（或信息）冗余。利用硬件和时间冗余来掩盖故障的影响，就是所谓容错技术．

容错与非容错的区别在于：容错系统自身包含部分或全部故障处理设备，而非容错系统是所有故障的处理均由系统外部提供．容错技术多用于高可靠性的计算机系统，这就是所谓容错计算机。容错计算机是按容错设计思想设计的计算机。它是以投入超过常规设计所需的资源来换取更高的可靠性的一种设计方法。

容错技术，根据对故障处理的不同方式可分为故障检测、故障屏蔽和动态冗余三

种．故障检测只能发出故障发生的报警，而不能容忍故障．屏蔽技术可容忍故障但不能实现发生故障的报警．动态冗余技术通过动态的改变以消除故障并补充系统的冗余．动态冗余技术的综合性较强，既可实现故障检测，消除故障影响，又可通过诊断实现故障定位，而后采取切换或替换措施，以提高计算机系统的可靠性。

自 1969 年 STAR 容错计算机研制成功以后，容错技术才广泛为人们所重视，成了容错计算技术研究的开端．IEEE 协会于 1970 年建立了容错计算委员会，国际容错计算会议自 1971 年起每年召开一次，至今已召开了十七次会议．

在我国，首先是哈尔滨工业大学在陈光熙教授领导并参加下于 1975 年进行了 NOVA 机的容错化试验．之后航空航天部 631 所于 1978 年，502 所于 1982 年，重庆大学于 1982 年、北京航空航天大学于 1983 年，清华大学于 1984 年先后开展了容错计算技术的研究工作．有的科研成果已展出，有的参加了国际容错会议，发表了论文．国防科技大学在研制大型机和高性能巨型机〔银河〕过程中广泛采用了容错技术，进行了比较严谨的可靠性分析和设计，以保证了高可靠性的实现。

软件可靠性与硬可靠性相比较，既有数学理论上的相类似之处，又有它自己的特点．软件与硬件的主要区别是：软件在反复操作的过程中是不可改变的，软件一旦交付使用不会因疲劳而发生软件故障，它不论存储在磁盘上还是磁带上，或是纸带上，指令和控制的软件及应用的程序，直到发生软件故障都是不变的．复制的软件也是如此．在磁盘或磁带上由于受到随机性的磁场影响，磁场可能损害已存储的软件，这不属于软件故障，而是磁记录设备的硬件故障．而硬件故障是因构成计算机的元器件、零部件的损坏、老化、磨损、以至寿命衰竭造成的．产生软件故障的根源是软件设计阶段人为的因素所产生的缺陷或错误所造成的．即主要区别于故障机理。

由于故障机理的不同，硬件故障只发生在元器件损坏、失效的局部地方，一般来说不波及其他部位；而软件设计上的缺欠一旦被测试出来，一般说来凡是在它出现的地方都必须进行相应的修改．在保持原程序设计或测试该程序的特定环境时，软件故障就不会发生，只有使用环境改变时软件故障才会发生．尽管软件与硬件故障机理不同，但是它们对于计算机系统的影响及其后果却是相同的．所以软件可靠性理论可以用类似于硬件可靠性理论来进行分析研究．但是也应牢记：研究软件可靠性时要时时注意到软件所具有的特殊性，强调它们不同的特点，切忌使自己在研究中过于注意两者的共同之处．一切都借鉴于硬件可靠性理论是错误的．近年来有些软件可靠性的研究者已感到在软件可靠性的研究中过多的依赖于硬件可靠性理论，提出了异议．此种见解已得到了一些学者的赞同．这样，对软件可靠性的研究工作可能会在不久的将来取得突破性的进展。

软件可靠性研究的兴起，是计算机系统应用实践的要求．在 60 年代中后期进入软件危机时期以后，人们便开始了软件可靠性的研究工作．最早是 G.R.Hudson 在杂志上发表文章．他把软件的开发过程用马尔柯夫过程来描述，在做了一些假设以后得到了一个故障间隔的威布尔分布的模型．此后将收集到软件测试的数据按测试阶段三个子阶段来进行分析研究，得出一些结论．Hudson 的工作始于 1967 年。

之后，Z.Jelinski 和 P.B.Moranda 于 1971 年的工作对软件可靠性研究的发展起了重要作用．他们假设故障率为分段的常数，且正比于软件内剩余的错误数．在每次软件

错误的排错时都以一个常量发生改变，在两次错误（相邻）改正中间故障率为常数．即故障率以阶梯形式下降．他们进而用最大似然法判定了隐藏于软件内的总错误数、残留错误数与故障率之间的比例系数。与此同时，M.Shooman 提出一个很类似的模型．他给出了一些不同的错误改正曲线，以根据不同的开发项目采用不同的改正曲线．Shooman 还同 S.Natarajan 合作提出了软件错误发生与排错过程的软件可靠性模型．

在由 G.J.Schick 和 R.W.Wolverton 提出的模型中，假定故障与软件内残留错误数和排错所用时间的乘积成正比．故障间的排错时间在数量上服从瑞利分布．因而故障率变化的大小随排错时的增加而增加． Schneidewind 建议用指数、正态、伽玛、威布尔等分布函数对软件可靠性进行分析研究，以针对不同的开发项目选用符合实际的软件可靠度的数学模型．他本人还收集实测数据加以实施．

J.D.Musa 就软件执行阶段的软件可靠性模型进行了研究，1975 年发表了他的研究成果．他提出软件可靠性的研究应以软件执行时间为基础，而不是日历时间．执行时间包括软件开发过程中测试时间和程序装入、传送和维护等过程在内的累积执行时间．在软件测试的排错过程中，软件可靠度是增长的，而在执行过程中，故障率是不随时间变化的，其常数值是随残留错误数的变化．这样，在分析过程中可避免用比较复杂的分布函数，从而大大减化了软件可靠性理论的分析过程．

在软件可靠性研究中，也有人采用另外一种方法；那就是 B.Littlewood 采用贝叶斯方法所进行的研究．他是把故障率看作是已发生故障的随机过程，并以此来建立数学模型．Littlewood 给出了许多不同的函数形式．这样就可以对比较适合的函数形式加以判定，通过比较就可以挑选出最合适的形式．B.Littlewood 于 1980 年又提出了微分模型．

A.L.Goel 和 K.Okumoto 于 1978 年提出了一个不完善的在排错阶段的可靠度模型．他们把排错过程看成是马氏过程，用状态转移概率进行分析，推导出一些很有用的结论．而后他们二人又用与 Jeliski 和 Moranda 相类似的假设，经过分析认为故障的发现是一个非齐次泊松过程（Nonhomogeneous Poisson Process，简称 MHPP)，他们认为发现了的软件错误数和残留的错误数的分布数都是泊松分布．这种软件可靠度模型是排错阶段的可靠度增长模型（SRGM)．近年来日本学者尾崎俊治、山田茂、山根勉和大场充等人在此基础上并结合实测数据对可靠度增长模型进行了研究，发表了他们的论文．

目前，还有不少的人对程序的输入空间进行研究，枚举程序的所有可能的输入状态集合，进而判断它们产生成功操作的概率．这种研究方法理论性较强，也比较抽象，在实际研究中也存在许多困难，但是从理论上来看还是有价值的．

在国内，软件可靠性的研究现在还不象硬件可靠性那样引人注目．着手对软件可靠性进行研究的单位和人员都不多．与国外的差距还是比较大的．在硬件可靠性方面，国外已经历了四个发展阶段，我国要跨跃这四个发展阶段是有很多困难的．目前，我们建立了有关学会，在国防科工委的直接领导下成立了许多专门机构，广泛开展了可靠性研究工作，取得了很好的效果．

§1.3 提高计算机系统可靠性的方法和途经

已成为未来信息社会核心物质基础的计算机，已远不是原来意义的"计算的机器"，而已从科学计算发展到信息处理、知识加工、工业生产及航天控制、指挥调度、交通管制、金融业务等等方面。这样，要求系统不但要有良好的技术性能、较优良的性能价格比和安全保密性能，同时也要求长寿命高可靠。

因可靠性理论及其应用技术的研究已有40余年的历史，并已发展到可靠性保证阶段。所以实现硬件高可靠性计算机的方法和技术途径是比较多的。这些方法和技术途径大体可以分为两类：提高计算机所用元器件、零部件的可靠性；在给定元器件、零部件的条件下，采用构成高可靠计算机系统的技术。也就是从高可靠元器件研制生产和系统可靠性设计以及生产过程中的可靠性与质量保证上下功夫。

电子元器件在国外已达到了Fit（10^{-9}/h）量级，有些电子元件的失效率可以达到0.1～0.01Fit的高可靠水平。目前，我国的电子元器件多数也只有七级，与国外相比要差两个数量级。1978年底召开的第四次可靠性工作会议，即第一次"七专"工作会议，从此使我国元器件可靠性工作进入了新的阶段。所谓"七专"即专批、专人、专料、专机、专技、专检、专卡。电子元器件可靠性工作走"七专"的道路是符合我国国情，是符合我国实际情况的捷径。从1978年起算到1984年为止解决了许多电子元器件生产中的技术关键，其可靠性水平提高了1～2个数量级。电子元器件可靠性工作从73年开始现已经历两个阶段，在七五计划期间已开始了第三阶段。这一阶段的任务是进一步提高可靠性，逐步贯彻军标，使元器件满足整机的需要。当前开展的元器件"七专"高可靠工作将为实现计算机系统的高可靠打下坚实的物质基础。

提高元器件可靠性的技术是：进行失效分析查明失效机理，通过信息反馈以改进生产工艺，制造出高可靠元器件；通过元器件模型的建立，拟定加速寿命试验方法，以便为整机的系统设计提供元器件的失效率数据及筛选条件和方法；改善元器件生产中的环境条件；明确规定元器件的使用条件；培训生产和使用人员的可靠技术；利用大规模、超大规模集成电路构成子系统或部分单元电路，以提高整机系统的可靠性。提高电子元器件的可靠性是元器件生产厂家的中心任务，不是本书所研究的内容。

本书着重研究在给定元器件的条件下，如何构成高可靠计算机系统的理论与技术。其中主要包括：采用冗余技术延续正常工作时间，提高系统的可靠性；研究提高软件可靠性理论及方法；增加信息多余性和复杂程度的检错与纠错编码以提高信息的可靠性；采用多数表决方式以提高系统输出信息的可靠性。此外，还有以缩短维修时间为目的的故障自动检测技术；使系统从故障状态转移到正常工作状态的恢复（维修）技术；保护系统中正在处理或存储着的信息免遭破坏或泄漏的信息保密等等。由于时间和篇幅所限有些内容只能做简要介绍。

在给定电子元器件的条件下，只要能够采用提高系统可靠性的各种方法进行精心设计，是可以设计出高可靠的系统的。苏联有一度认为用可靠性不太高的元器件照样可以研制出高可靠的系统。这当然是傻大黑粗的产品。当然，既有高可靠的元器件又采用提高系统可靠性的技术是最有效的。被称为美国导弹之父的原德国专家布劳思是从民兵导