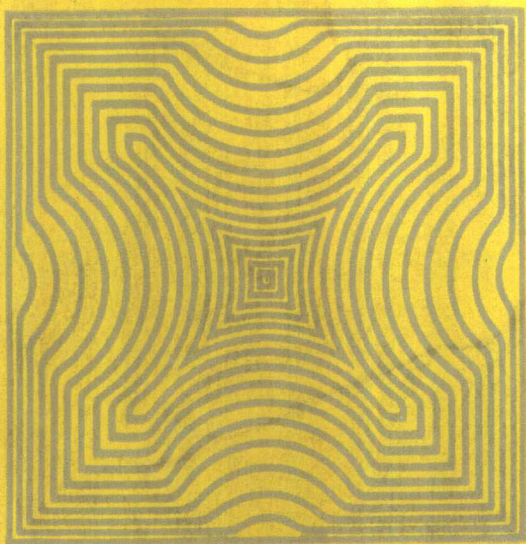




[美] D. P. 西沃赖克 著  
R. S. 斯沃兹

# 可靠系统的设计理论与实践

上 册

科学出版社

# 可靠系统的 设计理论与实践

上册

[美] D. P. 西沃赖克 著  
R. S. 斯沃兹

袁由光 曹泽翰 等译  
刘志模 陈以农

陈廷槐 陈以农 校

科学出版社

1988

## 内 容 简 介

可靠性是系统设计最重要的目标之一。本书全面地介绍构成高可靠数字系统中所涉及的各种问题。

全书分上下两册。上册为可靠系统的设计理论,下册为可靠系统的设计实践。上册共分六章。第一章介绍基本概念;第二章探究了失效的机理、故障的表现及其分布规律;第三、四章全面介绍了可靠性设计中的各种技术,重点讨论容错技术;第五章给出了可靠性的评价标准;第六章通过建立费用模型,讨论了系统可靠性与费用的关系及综合平衡等问题;附录给出了编码理论和可测试性设计等补充材料。

本书可供计算机专业的大学高年级学生、研究生以及从事系统工程设计、半导体器件可靠性分析的工程技术人员参考。

D. P. Siewiorek, R. S. Swarz

## THE THEORY AND PRACTICE OF RELIABLE SYSTEM DESIGN

Digital Press, 1982

## 可靠系统的设计理论与实践

上册

[美] D. P. 西维奥克 著  
R. S. 斯瓦兹

袁由光 等译  
刘志模 等译

陈廷槐 陈以农 校  
责任编辑 黄岁新

科学出版社出版

北京朝阳门内大街 137 号

中国科学院印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

1988 年 9 月第 一 版 开本: 787×1092 1/16

1988 年 9 月第一次印刷 印张: 25 1/4

印数: 0001—2,530 字数: 581,000

ISBN 7-03-000428-0/TP·25

定价: 9.00 元

## 作者简介

D. P. 西沃赖克 (Daniel P. Siewiorek) 于 1968 年在美国安阿伯的密执安大学获得电气工程科学学士学位, 并分别于 1969 年和 1972 年在斯坦福大学获得电气工程 (辅修计算机科学) 科学硕士和哲学博士学位。西沃赖克博士于 1972 年起在卡内基-梅隆大学的计算机科学与电气工程系任教。

在卡内基-梅隆大学, 西沃赖克博士协助开创并负责指导 Cm\* 研究项目, 参加了美国陆军/海军的“军事计算机之家”研究课题, 而且还领导了 C.vmp 计算机的研制工作。

西沃赖克教授曾担任几个商业机构和政府机构的顾问, 而且还获得过好几种奖励。

他当前的研究方向包括计算机体系结构、可靠性模型、容错计算、模块设计以及设计自动化。西沃赖克博士还担任过 IEEE 容错计算技术委员会主席。

R. S. 斯沃兹 (Robert S. Swarz) 于 1967 年获得美国纽约大学电气工程科学学士学位, 1969 年获得伦塞勒尔工艺学院工程科学硕士, 1973 年获得纽约大学哲学博士, 并于 1981 年获得波士顿大学的 M.B.A 学位。从 1967 年至 1976 年, 斯沃兹博士在普拉特-惠特尼航空公司开发了专用测量设备系统。从 1976 年至 1981 年他在数字设备公司的研究开发部门担任某些职务。目前他受雇于普莱门计算机公司, 并在该公司的调查与高级系统部领导一个可靠性与可服务性工程小组。他还在沃斯特多科性工学院任教。

## 译 者 的 话

随着计算机的广泛使用,计算机系统的可靠性愈来愈受到人们的关注。容错技术是建造高可靠系统最有效的方法。在国外,容错计算机已广泛用于国防、工业控制、病人监护和银行事务处理等领域。我国航空工业部计算技术研究所从1979年开始研制机载容错计算机。中国船舶工业总公司数字工程研究所与重庆大学协作,于1983年开始了舰载分布式容错计算机系统研究。天津第一石油化工厂在航天工业部的帮助下已将三模冗余计算机应用于炉温控制,使可靠性增加了几个数量级,赢得了工人信任。全国第一届容错计算会议已于1985年10月在北京召开,第二届会议又于1987年12月在上海召开,并出有会议论文集。然而,由于缺少一本这方面的综合性书籍,容错技术在国内至今还是鲜为人知。因此,本书中译本的公开出版,将促进国内容错计算的教育、研究与应用的发展。

本书在国外也是第一本容错计算的系统专著。在此之前,美国各大学也只是汇总许多论文作为教材,本书出版后,美国容错计算的教育大为改观。本书从1984年起即被重庆大学作为研究生的教材,内容十分丰富,能将研究生引到科研第一线。

重庆大学陈廷槐教授与本书作者西沃赖克教授1980年就已认识,以后又多次在国际容错计算会议上见面。西沃赖克高超的学术见解以及作为IEEE容错计算技术委员会主席所表现出的干练令人钦佩,他十分关心中译本的出版,还特别为此写了前言,在此谨表谢意。

本书的翻译是许多同行共同完成的。上册中,前言由陈廷槐译,第一章由黄开源译,第二章由陈以农译,第三、四章由袁由光译,第五、六章由曹泽翰译,附录A、B、C由刘志模译,附录D、E由陈以农译。第一至六章由陈以农初校,附录由诸义新初校。下册引言、第九、十、十一、十二、十三章由杨孝宗译,第七、八、十六章由袁由光译,第十四、十五、十七、十八章由陈以农译,名词索引由杨孝宗初译,刘志模参加了引言和十四章的翻译。下册由诸义新校。陈廷槐对全书作了最后校阅。

尽管译校者们都是从事容错计算研究的,特别是杨孝宗、诸义新曾在卡内基-梅隆大学听过此课、陈以农在重庆大学讲授此课,然而由于内容很新、专门术语太多,加之译校者水平有限,错误在所难免,敬希广大读者指正。

## 中 译 本 序

1980年9月在陕西微电子研究所副所长黄敞教授和西安交通大学几位教授的安排下,七位世界知名专家组成的代表团在中华人民共和国陕西省临潼县陕西微电子研究所举办的一个为期四天的容错计算报告会上作了报告。有一百多位中国学者参加了这个报告会。作为代表团团长的我,对中华人民共和国在容错计算领域的强烈兴趣产生了深刻的印象。在这个报告会上进行了许多卓有成效的讨论并结识了许多朋友。在那段难忘的日子里,我会见了陈廷槐教授。报告会后不到两年,杨孝宗作为专攻容错计算的访问学者来到了卡内基-梅隆大学。

在本书(可靠系统的设计理论与实践)编写期间,容错计算已经明显地成为一个发展迅速,且具有商用潜力的领域。自1980年开始,容错计算的研究与发展步伐就加快了。美国计算杂志(IEEE 计算机学会的主要出版物)1984年8月号出版了容错计算专辑。Omri Serlin 在一篇文章里总结了不少于11个商业公司的产品经验。这些公司的主要产品是容错计算机。随着高性能微处理器的出现,它的性能是“超级小型计算机”的竞争对手,现在已有可能在单个箱体内组装有16到64个处理器的多处理器系统。将多处理器系统固有的冗余与当代的操作系统和容错概念相结合已产生出整个这种容错系统,其性能、可用性和从开始到失效的平均时间等均比超级小型计算机和主计算机要好几个数量级而成本只有它们的几分之一。

随着计算机的普及使用,原则上容错计算的重要性将会继续增长。我坚信中华人民共和国的研究人员和系统设计师将作出无数贡献并将把容错计算机设计的前沿向前推进。

D. P. 西沃赖克

1984年11月

# 目 录

|      |   |
|------|---|
| 译者的话 |   |
| 中译本序 |   |
| 前言   | 1 |

## 第一部分 可靠系统的设计理论

|                              |    |
|------------------------------|----|
| <b>第一章 基本概念</b>              | 7  |
| 1.1 可靠性的重要性                  | 7  |
| 1.2 数字系统的层次                  | 8  |
| 1.3 系统寿命期的各个阶段               | 9  |
| 1.4 容错计算的特性及其定义              | 10 |
| 1.4.1 可用度                    | 10 |
| 1.4.2 可靠度                    | 10 |
| 1.5 制造阶段                     | 11 |
| 1.5.1 设计成熟性测试                | 11 |
| 1.5.2 进料检验                   | 12 |
| 1.5.3 工艺成熟性测试                | 15 |
| 1.6 运行阶段                     | 16 |
| 1.7 拥有费用                     | 17 |
| 1.8 模型系                      | 18 |
| 1.9 可设计的参量                   | 19 |
| 参考文献                         | 20 |
| <b>第二章 故障及其表现</b>            | 21 |
| 2.1 引言                       | 21 |
| 2.2 故障的表现                    | 23 |
| 2.2.1 物理缺陷                   | 23 |
| 2.2.2 逻辑级故障的类别               | 29 |
| 2.2.3 系统级的抽象                 | 29 |
| 2.3 故障的分布                    | 32 |
| 2.3.1 概率复习                   | 32 |
| 2.4 样本数据与数学分布的拟合             | 35 |
| 2.4.1 极大似然估计法                | 35 |
| 2.4.2 韦伯参数的极大似然估计            | 36 |
| 2.4.3 线性回归分析                 | 36 |
| 2.4.4 置信区间                   | 37 |
| 2.4.5 符合良度检验                 | 37 |
| 2.5 永久故障的分布: MIL-HDBK-217 模型 | 41 |

|                                             |     |
|---------------------------------------------|-----|
| 2.5.1 寿命期测试和现场数据 .....                      | 40  |
| 2.5.2 永久失效数据的分析: 估计分布及其参数 .....             | 47  |
| 2.6 自动失效率计算 .....                           | 52  |
| 2.7 瞬时错误和系统错误的分布 .....                      | 53  |
| 2.7.1 数据收集 .....                            | 53  |
| 2.7.2 图形化数据分析 .....                         | 54  |
| 2.7.3 参数的置信区间 .....                         | 61  |
| 2.7.4 符合检验 .....                            | 61  |
| 2.8 小结 .....                                | 61  |
| 参考文献 .....                                  | 63  |
| 习题 .....                                    | 63  |
| <b>第三章 可靠性和可用性技术 Steven A. Elkind</b> ..... | 64  |
| 3.1 避错技术 .....                              | 68  |
| 3.1.1 环境变化 .....                            | 68  |
| 3.1.2 质量控制 .....                            | 71  |
| 3.1.3 元件集成度 .....                           | 75  |
| 3.2 故障检测技术 .....                            | 77  |
| 3.2.1 二模冗余 .....                            | 78  |
| 3.2.2 检错码 .....                             | 82  |
| 3.2.3 自校验、故障保险和失效-安全逻辑 .....                | 101 |
| 3.2.4 监视计时器和超时 .....                        | 107 |
| 3.2.5 相容性检验和权力检验 .....                      | 108 |
| 3.3 屏蔽冗余 .....                              | 110 |
| 3.3.1 N 模表决冗余 .....                         | 110 |
| 3.3.2 纠错码 .....                             | 118 |
| 3.3.3 屏蔽逻辑 .....                            | 128 |
| 3.4 动态冗余 .....                              | 135 |
| 3.4.1 可重组的二模冗余 .....                        | 136 |
| 3.4.2 可重组的 NMR .....                        | 140 |
| 3.4.3 后援备件 .....                            | 147 |
| 3.4.4 缓慢降级 .....                            | 151 |
| 3.4.5 重组 .....                              | 153 |
| 3.4.6 恢复 .....                              | 161 |
| 3.5 小结 .....                                | 166 |
| 参考文献 .....                                  | 166 |
| 习题 .....                                    | 167 |
| <b>第四章 可维护性和测试技术</b> .....                  | 174 |
| 4.1 生产阶段 .....                              | 175 |
| 4.1.1 参数测试 .....                            | 175 |
| 4.1.2 验收测试 .....                            | 177 |
| 4.1.3 可测试性设计 .....                          | 182 |
| 4.2 现场操作 .....                              | 186 |
| 参考文献 .....                                  | 190 |

|                                                            |     |
|------------------------------------------------------------|-----|
| 习题 .....                                                   | 190 |
| <b>第五章 评价标准</b> Stephen McConnel Daniel P. Siewiorek ..... | 191 |
| 5.1 评价标准概述 .....                                           | 191 |
| 5.1.1 硬件评价 .....                                           | 191 |
| 5.1.2 软件评价 .....                                           | 196 |
| 5.2 模型技术 .....                                             | 201 |
| 5.2.1 组合模型 .....                                           | 201 |
| 5.2.2 马尔柯夫模型 .....                                         | 235 |
| 5.2.3 系统可用性模型 .....                                        | 264 |
| 5.2.4 建立冗余影响性能的模型 .....                                    | 271 |
| 5.3 系统设计的综合分析 .....                                        | 275 |
| 5.3.1 设计实例: PDP-8/e .....                                  | 276 |
| 5.3.2 实例分析 .....                                           | 281 |
| 5.4 小结 .....                                               | 285 |
| 参考文献 .....                                                 | 286 |
| 习题 .....                                                   | 286 |
| <b>第六章 财经考虑</b> .....                                      | 295 |
| 6.1 引言和基本概念 .....                                          | 295 |
| 6.1.1 定义 .....                                             | 295 |
| 6.1.2 维护费用 .....                                           | 296 |
| 6.1.3 用户拥有费用 .....                                         | 298 |
| 6.2 现场服务概观和费用模型 .....                                      | 300 |
| 6.2.1 维护费用模型 .....                                         | 300 |
| 6.2.2 寿命期费用 LCC (Life-Cycle Cost) 模型 .....                 | 303 |
| 6.2.3 具有综合数据成分的 LCC 模型 .....                               | 307 |
| 6.3 结论 .....                                               | 311 |
| 参考文献 .....                                                 | 311 |
| 习题 .....                                                   | 311 |
| <b>附录 A 差错控制的编码技术</b> D. T. Tang R. T. Chien .....         | 313 |
| A.1 基本定义 .....                                             | 313 |
| A.1.1 冗余 .....                                             | 313 |
| A.1.2 源码 .....                                             | 314 |
| A.1.3 分组码 .....                                            | 314 |
| A.1.4 二源码 .....                                            | 314 |
| A.2 数字数据信道中的差错 .....                                       | 314 |
| A.2.1 传送与存储 .....                                          | 314 |
| A.2.2 源编码 .....                                            | 314 |
| A.2.3 调制与解调 .....                                          | 315 |
| A.3 差错源 .....                                              | 315 |
| A.3.1 差错统计 .....                                           | 315 |
| A.3.2 存储 .....                                             | 316 |

|                            |     |
|----------------------------|-----|
| A.3.3 信道模型.....            | 316 |
| A.4 编码中的数学结构.....          | 316 |
| A.4.1 线性分离码.....           | 317 |
| A.4.2 多项式循环码.....          | 318 |
| A.5 对编码与译码的一般要求.....       | 318 |
| A.5.1 差错症候.....            | 318 |
| A.5.2 条件极大似然译码.....        | 319 |
| A.5.3 极大似然译码.....          | 319 |
| A.5.4 最小距离译码.....          | 319 |
| A.6 线性开关线路与移位寄存器.....      | 320 |
| A.6.1 使用延迟算子 $D$ 的多项式..... | 320 |
| A.7 编码器和译码器.....           | 323 |
| A.8 差错控制码的功能分类.....        | 325 |
| A.9 编码策略.....              | 325 |
| A.9.1 差错检测.....            | 326 |
| A.9.2 部分纠正.....            | 327 |
| A.9.3 抹除.....              | 327 |
| A.9.4 自适应编码方案.....         | 328 |
| A.9.5 顺序译码法.....           | 328 |
| A.10 某些差错控制的应用.....        | 328 |
| A.10.1 数据通信.....           | 328 |
| A.10.2 数据存储器.....          | 329 |
| A.10.3 辅助存储器.....          | 329 |
| A.10.4 数字多分支型差错控制.....     | 330 |
| A.11 结束语.....              | 330 |
| 附录1 线性码的结构.....            | 331 |
| 附录2 多项式码的结构.....           | 332 |
| 附录3 求生成多项式的方法.....         | 333 |
| 附录4 特殊的差错控制码.....          | 337 |
| 附录5 循环冗余校验.....            | 343 |
| 参考文献.....                  | 344 |

## 附录B 算术差错码: 在数字系统设计中应用的代价和效果的研究 Algirdas Avižienis

|                           |     |
|---------------------------|-----|
| .....                     | 345 |
| B.1 码评价方法论.....           | 345 |
| B.1.1 问题的范围.....          | 345 |
| B.1.2 代价准则.....           | 346 |
| B.1.3 效果准则.....           | 346 |
| B.1.4 逻辑故障分类.....         | 348 |
| B.2 二进制算术处理器中的故障后果.....   | 349 |
| B.2.1 并行算术运算中的基本故障.....   | 349 |
| B.2.2 二进制处理器中的重复使用故障..... | 351 |
| B.3 低代价以2为基数的算术码.....     | 352 |

|             |                                                           |            |
|-------------|-----------------------------------------------------------|------------|
| B.3.1       | 算术差错码的实现.....                                             | 352        |
| B.3.2       | 低代价校验算法.....                                              | 353        |
| B.3.3       | 故障效果：一次使用故障.....                                          | 354        |
| B.3.4       | 故障效果：确定性重复使用故障.....                                       | 354        |
| B.3.5       | 故障效果：非确定性重复使用故障.....                                      | 355        |
| B.3.6       | 剩余码中的重复使用故障.....                                          | 356        |
| B.4         | 多重算术差错码.....                                              | 357        |
| B.4.1       | 多重低代价码.....                                               | 357        |
| B.4.2       | 多重码的“混合代价”形式.....                                         | 359        |
|             | 参考文献 .....                                                | 360        |
| <b>附录 C</b> | <b>可测试逻辑设计理论和实践的最新进展 R. G. Bennetts R. V. Scott .....</b> | <b>361</b> |
| C.1         | 引言.....                                                   | 361        |
| C.2         | 理论方面的进展.....                                              | 362        |
| C.2.1       | 组合线路.....                                                 | 362        |
| C.2.2       | 时序线路 .....                                                | 370        |
| C.2.3       | 重复阵列.....                                                 | 377        |
| C.3         | 可测试逻辑设计的实践情况.....                                         | 378        |
|             | 结论 .....                                                  | 382        |
|             | 参考文献 .....                                                | 383        |
| <b>附录 D</b> | <b>MIL-HDBK-217B 可靠性模型梗概 .....</b>                        | <b>384</b> |
|             | 参考文献 .....                                                | 387        |
| <b>附录 E</b> | <b>MIL-HDBK-217C 可靠性模型梗概 .....</b>                        | <b>388</b> |
| E.1         | 217C 模型 .....                                             | 388        |
| E.2         | 217C 1 号公报模型 .....                                        | 389        |
|             | 参考文献 .....                                                | 392        |

## 前 言

自从电子数字计算机时代开始以来,系统的可靠性一直是一项主要关注的问题。最早的计算机是用继电器和电子管一类元件构成的,这些元件由正常工作转为失效的频繁度达到了每十万周期或每百万周期出现一次的程度。为了保证正确完成哪怕是只需千万次级运算周期的中等计算,这种出错率也远嫌过大。Bell 继电器计算机(1944)每一计算执行两次并比较其结果,而且还使用了纠错码。第一台商用计算机 UNIVAC (1951) 采用了大量的奇偶校验和用匹配-比较方式工作的两个算术逻辑单元(ALU)。今天,对可靠性的兴趣已遍及整个计算机工业,从大的主机制造商到半导体制造厂,他们不仅生产可靠性的专用元件(例如用于纠错码),而且也生产整个系统(例如 Intel 432)。

计算机的设计者必须学习可靠性技术,计算机系统的用户也应如此。目前我们对计算系统的依赖程度已经增长到如此之大,以至要想退回到使用从前不那么复杂的机构已变得很难,或者根本不可能。例如当航空公司的一台订座用的计算机“崩溃”了,航空公司就不能再根据人工的登记表来恢复订座功能;由于增加了往返票的登记服务,如果不询问计算机就无法知道哪些座位已经分配给哪些尚未办理登记手续的旅客了。最后的结局将是认为所有的票都未被预订,向蜂涌而至的旅客们敞开售票。计算机系统的用户必须懂得当代可靠性设计的优点与限制;能确定这些优点与限制对于应用(即是要进行的计算)的影响范围,并且明确对系统可靠性的要求,以便使应用或计算能成功地完成。

可靠性这门学问的进展曾是相当缓慢的。在二十世纪五十年代可靠性属于工业领域,而且设计的质量经常依赖于个别工程师的智慧,但香农(Shannon) [1948] 和海明(Hamming) [1950] 关于经过有噪声通道(于是产生差错)的通讯,以及莫尔(Moore)与香农于1956年和冯·诺依曼(Von Neumann)于1956年关于在部件失效时尚能生存的冗余技术等著名工作例外。香农与海明开辟了编码理论的领域,这是当代系统设计理论的奠基石。莫尔、香农和冯·诺依曼给冗余技术的发展和数学化评价打下了基础。

六十年代可靠系统的设计在工业中得到了系统化的处理。贝尔电话实验室设计并建成电子开关系统 ESS, 其目标是使四十年中停机维修的时间只占两个小时 [Downing, Nowak, and Tuomenoksa, 1964]。IBM 系统/360 计算机系列具有很好的可服务性 [Carter 等, 1964]。可靠性设计在航天工业中也找到越来越多的用途,一台三模冗余计算机帮助人类登上了月球 [Cooper, Chow, 1967; Dickinson, Jackson and Randa, 1964]。有关这方面的文献也增加了。1962年一次冗余技术的报告会在华盛顿特区召开,出版了这一课题的第一本综合书籍 [Wilcox and Mann, 1962]。稍后,皮尔士(Pierce)于1965年出版了一本概括和分析四重冗余技术的书,该技术是由喘昂(Tryon)提出并于1962年在 Wilcox 和 Mann 书中作了报道。可靠性的理论家和实际工作者之间的交流也在发展之中。

七十年代对系统可靠性的兴趣爆炸性地膨胀。以可靠系统(例如 Tandem)为主要产品的各个公司也已形成。由于 A. 阿维齐尼斯(Algirda Avizienis)和其它先驱者的努

力,一个容错计算的技术委员会 (TCFTC) 已在美国电气和电子工程师协会 (IEEE) 内部组成。从 1971 年起, TCFTC 每年举行一次国际容错计算会议。于是,为可靠计算结构的设计编写一书籍的时机已就成熟。

这本书的读者对象有三类。第一类对象是对可靠性设计有兴趣的本科高年级学生,但他们必须修满先修课程,如像程序设计导论、计算机组成结构、数字线路设计以及概率论。这本书的第一部分(上册),第二部分(下册)的部分章节和章末的习题,足够组成一个学季或学期的课程,正如表 P-1 所建议的那样。

表 P-1 对本科课程结构的建议

| 章 目             | 注 解                                        |
|-----------------|--------------------------------------------|
| 1 基本概念          | 一个适当的子集,例如一组课题(即故障避免 故障检测、屏蔽技术、动态冗余)中的一个分支 |
| 2 故障及其表现        |                                            |
| 3 可靠性及可用性技术     |                                            |
| 4 可维护性和测试技术     | 直到马尔柯夫模型,但不包含它                             |
| 5 评价标准          |                                            |
| 6 财经考虑          | 若时间允许可附加其它例子                               |
| 7 C. vmp (第二部分) |                                            |
| 18 Intel 432    |                                            |

第二类对象是研究生,本书可作为他们在可靠性设计方面的第二课程,或许作为他们从事研究工作的前奏。第一部分的较深部分以及第二部分的系统例子必须增补其它书籍和最新的研究文献,如表 P-2 所示。一个课程设计(例如设计一个双倍系统使得平均无失效时间\* (MTTF) 增长 20 倍,同时使寿命期费用最小)可以帮助学生巩固所学得的知识。本书提供了一个丰富的文献目录,可用来查找所需的文献资料。

表 P-2 对研究生课程结构的建议

| 章 目         |                                                                                                                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 基本概念      |                                                                                                                                                                                                                                                      |
| 2 故障及其表现    | Ross [1972]和/或 Shooman [1968] 对于随机变量、统计参数的估计<br>ARINC [1964] 的数据收集与分析                                                                                                                                                                                |
| 3 可靠性与可用性   | 附录 A, Peterson and Weldon [1972] 的编码理论<br>Sellers, Hsiao and Bearnson [1968b] 的故障检测技术<br>IEEE 历年的国际容错计算会议论文集<br>IEEE 计算机汇刊容错计算专辑(例如 1971 年 11 月,1973 年 3 月,1974 年 6 月,1975 年 5 月,1976 年 6 月,1980 年 6 月,1982 年 7 月)<br>Computer 杂志的容错计算专辑(1980 年 3 月) |
| 4 可维护性和测试技术 | Breuer and Friedman [1976] 的测试部分<br>Cherry Hill 测试会议公报                                                                                                                                                                                               |
| 5 评价标准      | Ross [1972], Howard [1971], Shooman [1968], Craig [1964] 的马尔柯夫模型及其解法                                                                                                                                                                                 |
| 6 财经考虑      | Phister [1979]                                                                                                                                                                                                                                       |
| 第二部分        | IEEE 进展公报 1978 年 10 月专辑                                                                                                                                                                                                                              |

\* 平均无失效时间 (Mean Time To Failure) 也常译为平均无故障时间。——译者注

第三类对象是从事实工作的工程人员。本书的主要目标之一是提供足够的概念使得从事实际的工程人员能将本书的可靠性技术应用到他或她的下项设计中去。第一部分提供了一组可靠性技术以及用来评价它们的数学模型。第二部分的一系列章节阐明了设计技巧,描述了可靠计算机的实际实现方法,这些章节是系统设计人员撰写的。最后一章提供了可靠系统设计的方法论并且阐明了这个方法论是怎样应用于实际设计(Intel 432)中的。

本书分为两个部分。第一部分(上册)涉及可靠设计的理论,第二部分(下册)涉及可靠设计的实践。诸附录提供了编码理论、可测试性设计以及 MIL-HDBK-217 器件可靠性模型的详细信息。

作者们希望对容错计算领域中的许多同事表示深切的感谢。没有他们的投稿和协助,这本书是不可能写成的。我们特别感谢所有论文的作者,他们让我们分享了他们的设计见解。特别向 Sudhir Bhagwani 和 Justin Rottner 对第十八章的帮助致以谢意。John Shebell 提供了第六章的材料和深刻的见解。

Xavier Castillo 和 Vittal Kini 分别提供了数学模拟材料和计算机辅助工具。Ashok Ingle 协助完成了初稿并在各章末准备了一些习题。某些评阅人和学生的补充意见是特别有益的。

十分感谢卡内基-梅隆大学以及 DEC 数字设备公司的同事们,因为他们提供了有助于产生和检验某些想法的环境。数字印刷公司的所有职工为及时出版本书付出了辛勤的劳动。

没有 Dorothy Josephson 夫人的耐心和勤奋,这本书是不可能完成的。她打印和重新打印了原稿的许多次草稿。

D. P. 西沃赖克

R. S. 斯沃兹

### 参 考 文 献<sup>1)</sup>

ARINC [1964]; Breuer and Friedman [1967]; Carter et al. [1964]; Cooper and Chow [1976]; Craig [1964]; Dickinson, Jackson, and Randa, [1964]; Downing, Nowak, and Tuomenoksa [1964]; Hamming [1950]; Howard [1971]; Moore and Shannon [1956]; Peterson and Weldon [1972]; Phister [1979]; Pierce [1965]; Ross [1972]; Sellers, Hsiao, and Bearnsen [1968b]; Shannon [1948]; Shooman [1968]; von Neumann [1956]; Wilcox and Mann [1962].

---

1) 每章之末缩写的参考文献的全称可参看书末的总参考文献目录。



# 第 一 部 分

## 可靠系统的设计理论

---

本书第一部分引入了许多构造可靠计算系统所需的基本技术。第一章对设计可靠系统的根据予以说明,并且提供其设计、制造、维护的理论模型。首先,我们考察设计可靠系统的重要性。其次,我们给出通常用以划分计算机系统的层次结构,以便工程技术人员能有效且高效率地讨论计算机系统;此外,对将计算机系统生存期划分为若干阶段的理由也给予了解释说明。在定义了一些对容错计算很重要的名词术语与度量标准后,第一章深入地讨论了系统生存期的两个阶段,即制造与运行阶段。最后,该章还介绍了某些用于计算机系统设计的数学模型并且给定了工程技术人员可控的参量。

第二章讨论计算机系统故障:失效机理,对应于层次结构(物理、逻辑及系统)各级的故障表现形式,故障预测以及故障测度。本章还回顾了应用概率论以帮助理解各种故障分布的数学基础。对一些用以将经验数据与故障分布相匹配的公共技术,例如极大似然估计法、线性回归、 $\chi^2$  符合良度检验等均作了讨论。

第二章引入了估计固定失效率的一些方法,包括 MIL-HDBK-217 过程——一个在电子设备中广泛使用的固定故障的数学模型和寿命期测试以及数据分析方法。然后,通过对卡内基-梅隆大学四台分时主机的现场数据的分析来讨论如何寻求适合瞬时故障的分布函数。

第三章论述可靠性技术,即提高平均无故障时间的方法。对可靠性与可用性技术作了易于理解分类,且提供了各种技术及评价标准的一览表。

第四章论述可维护性技术,即改善有故障计算机系统平均修复时间的方法。该章提供了一系列测试与维护技术,并且描述了在计算机寿命期各阶段差错源的检测与纠正的方法。对制造阶段的特殊试验策略作了讨论。对许多逻辑级的验收测试,如异或测试、特征分析、布尔差分、通路敏化法、D-算法等均作了解释。该章还引入了一个称作可测试性设计的研究分支,试图确定易测系统的特性。

如何数学化地评价一个可靠系统或可维护系统呢?即是说,假定一个系统在四十年中故障时间不超过两小时,用什么方法可以不必等那么长的时间就能证实系统设计的成功呢?第五章定义了许多评价标准,奠定了数学基础,并给出了一些确定性模型与模拟技术。引入了简单的串-并模型作为评价非冗余系统与备份系统的工具。其次,描述了组合(故障穷举)模型。该章还引入了简化非串非并模型为易处理形式的方法。

第五章介绍马尔可夫模型,该模型定义各种系统状态并反映从一状态到它状态的概率。在此模型中,概率仅取决于现状态而与现状态是如何达到的无关。在描述了其它一些模拟与模型化技术后,本章最后以利用第三章介绍的技术来提高 PDP-8/e 可靠性的尝

试作为实例讨论而进入高潮。

最后,第六章涉及有关计算机系统的设计、购置、运行所固有的经济因素。讨论是从两个主要角度进行的,即维护者的角度与系统所有者/操作者的角度。在对维护费用的各种因素,如劳力与材料作了说明后,概述了现场维修服务业务。提供了一些维护费用模型以及估计可维护性的方法。对于拥有和运行一个计算机系统的寿命期费用模型化的众多方法,本章只选择两种予以介绍;这些费用模型对帮助系统设计者了解买主的经济动机是有实质作用的。