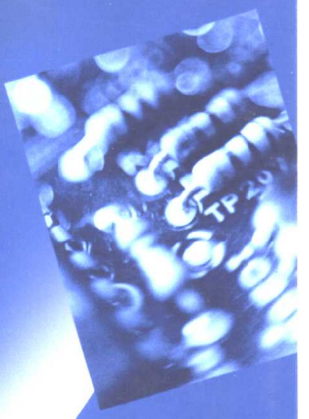
系统可靠性分析与设计



李海泉 李 刚 编著

科学出版社
www.sciencep.com

系统可靠性分析与设计

李海泉　李　刚　编著

科学出版社

北京

内 容 简 介

本书全面、系统地介绍了系统可靠性分析与设计。书后附有元器件降额标准、系统可靠性设计准则和武器装备可靠性设计准则三个附录。每章前有内容提要，每章后有本章小结和习题及思考题，书后有参考文献和附录，可供读者复习巩固和深入研究。本书所介绍的理论、方法具有一定的普遍性、先进性和适用性，所述实例具有一定的典型性、代表性和实用性。本书内容丰富，简明易懂，注重实用，详略得当，具有一定的理论水平和很高的实用价值。

本书可作为计算机工程、信息工程、通信工程、电子工程、自动控制、系统安全和保护等专业的科技人员的参考书，也可供航空、电子、航天、核控制及石油勘探系统研制等领域的工程技术人员参考。同时，还可作为大专院校相关专业的本科生和研究生教材或参考书。

图书在版编目(CIP)数据

系统可靠性分析与设计/李海泉，李刚编著. —北京：科学出版社，2003
ISBN 7-03-012041-8

Ⅰ. 系… Ⅱ. ①李…②李… Ⅲ. ①系统可靠性-系统分析②系统可靠性-系统设计 Ⅳ. N945.17

中国版本图书馆 CIP 数据核字(2003)第 069281 号

责任编辑：陈晓萍 陈砺川/责任校对：钟 洋
责任印制：吕春珉 /封面设计：王 浩

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销

2003 年 10 月第 一 版 开本：787×1092 1/16
2003 年 10 月第一次印刷 印张：31 1/4
印数：1－5 000 字数：720 000

定价：45.00 元
(如有印装质量问题，我社负责调换〈环伟〉)

前　言

随着计算机通工程、信工程、信息工程、电子工程、自动控制、航空、航天、核控制、石油勘探、仪器仪表等领域的应用，其应用系统的可靠性和安全性显得越来越重要，可靠性及安全性成了系统的生命线，成为系统能否推广应用的关键因素之一。在系统研制开发过程中，必须重视可靠性分析与设计。许多系统只注意其功能的完善，而忽视可靠性设计，导致其产品可靠性不高。不可靠系统的应用会造成巨大的经济损失，甚至导致灾祸的发生，丧失信誉，失去市场，其教训是沉痛的。目前，国内每年有大批的计算机应用系统通过鉴定，然而真正推广应用的却很少，其重要原因之一就是系统不可靠，无法投入实际应用。

可靠性是一门涉及面很广的交叉学科，世界各发达国家均给予高度重视。日本人把可靠性当作"国家兴亡"的大事，其产品因高可靠性而赢得了市场，成为经济强国。美国国防部从 1957 年就给予可靠性极大的重视。1965 年国际电工技术委员会可靠性专业委员会成立，表明可靠性工程已成为一门国际性技术。在我国，据 1978 年测试，国产电视机平均无故障工作时间(MTBF)还不到 500 小时，年返修率高达 95%以上，国产计算机的 MTBF 到 1980 年仅 50 小时。20 世纪 80 年代后，我国狠抓了产品可靠性，颁布了一系列可靠性技术标准和管理规定，在现代化武器装备等大型工程研制中，全面推行可靠性工程技术，使我国的可靠性工程得到了迅速发展。目前，国产名牌彩电的 MTBF 均达到了 3 万小时以上，计算机的 MTBF 也得到了很大提高，有的已经远销国外。国内在型号可靠性工程方面已经积累了丰富的经验，研制出可靠性预计、评估、可靠性设计方面的软件。目前，国内已经出版了一些可靠性工程的论著，但是缺少既全面、系统介绍可靠性设计理论、方法和技术，又有可供操作使用的可靠性设计工具软件的专著或教材。本书编著的目的就是努力填补这一空白。

本书作者对可靠性工程已做了几十年系统、深入的研究，进行了系统可靠性工程设计、可靠性工程评估和计算机设备可靠性评估软件的研制，本书是作者在编著并出版了《微机系统的 RAS 技术》(清华大学出版社) 的基础上，总结多年实践经验，优选成熟的、效果明显的可靠性分析与设计方法，并参考国内、外的有关著作、资料后编著出本书。本书所介绍的理论、方法具有一定的普遍性、先进性和适用性，所举实例具有一定的典型性、代表性和实用性。本书内容丰富，简明易懂，注重实用，详略得当，具有一定的理论性和很高的实用价值。

本书共 12 章，分别介绍了可靠性的基本概念和可靠性模型，提高系统可靠性的方法和途径，元器件的可靠性及其选择，半导体元器件的性能及其选择，系统失效分析，系统可靠性预计与指标的分配，系统可靠性设计，冗余设计，电磁兼容性设计，防电磁泄漏设计，数据传输可靠性设计，软件可靠性设计，系统可测试性设计。书后附有元器件降额标准、计算机设备可靠性设计准则和武器装备可靠性设计准则 3 个附录。每章前有内容提要，每章后有本章小结和习题及思考题，书后有参考文献和附录，可供读者复习巩固和深入研究。

本书在编写过程中得到了中国计算机学会理事郝克刚教授的支持；中国电子学会专业委员会原主任、中国软件总公司任公越教授，中国计算机学会专业委员会原主任、中国科学院软件所黄昌夺教授和西安交通大学博士生导师郑守琪教授审阅了编写大纲；西安电子科技大学计算机系陈家正教授、西北大学计算机科学系卞雷教授分别审阅了本书手稿，提出了宝贵的意见。李海泉编著了第一、四、五、六、七、八、九、十一、十二章，李刚编著了第二、三、十章。李健、王志均、张莉芳、李良等16位同志分别帮助描图和打印了部分手稿。此外，本书的编写还得到我院、系有关领导的支持和关心。在此，一并表示衷心的感谢。

本书可作为计算机工程、信息工程、通信工程、电子工程、自动控制、系统安全和保护等专业的科技人员的参考书，航空、航天、电子、核控制及石油勘探系统研制等领域的工程技术人员也可参考，另外，本书还可作为上述专业本科生和研究生的教材或参考书。

由于本书涉及面广，加上时间仓促及作者水平有限，错误之处在所难免，欢迎读者批评指正。

李海泉　李　刚
西安石油学院
西安交通大学
2002年10月10日

目　录

第一章　绪论 …… 1
1.1　系统可靠性分析与设计的意义 …… 1
1.2　系统可靠性的基本概念 …… 3
1.2.1　可靠性与可靠度及可靠度函数 …… 3
1.2.2　故障率 …… 4
1.2.3　平均故障间隔时间 …… 8
1.2.4　可维性和可用性的概念 …… 9
1.2.5　安全性的基本概念 …… 10
1.3　系统的寿命分布 …… 10
1.4　系统可靠性模型 …… 15
1.4.1　建立可靠性模型的目的和用途 …… 16
1.4.2　串联系统的可靠性模型 …… 17
1.4.3　并联系统的可靠性模型 …… 18
1.4.4　混联系统的可靠性模型 …… 21
1.4.5　表决结构系统的可靠性模型 …… 23
1.4.6　非工作储备模型(旁联模型) …… 24
1.5　可维修系统的马尔可夫模型 …… 25
1.5.1　马尔可夫过程的基本概念 …… 25
1.5.2　可维修系统的马尔可夫模型 …… 26
1.6　提高系统可靠性的途径 …… 29
1.6.1　系统可靠性设计 …… 29
1.6.2　系统容错设计 …… 32
1.6.3　加固设计 …… 35
1.6.4　避错技术 …… 36
1.7　系统可靠性分析与设计的内容 …… 38
本章小结 …… 39
习题与思考题一 …… 40
第二章　元器件的可靠性及其选择 …… 41
2.1　元器件的失效特征 …… 41
2.2　元器件的失效机理 …… 43
2.3　元器件的选择 …… 45
2.4　元器件的筛选 …… 49
2.4.1　元器件筛选的基本概念 …… 49

2.4.2 元器件的筛选方法 …… 50
2.5 电阻器的性能及其选择 …… 52
2.5.1 电阻器的种类和性能 …… 52
2.5.2 电阻器的选择 …… 55
2.5.3 使用电阻器时应注意的事项 …… 56
2.6 电容器的性能及其选择 …… 57
2.6.1 电容器的主要性能 …… 57
2.6.2 电容器的等效电路 …… 58
2.6.3 电容器的选择 …… 59
2.6.4 电容器使用时应注意的事项 …… 61
2.7 继电器的选择 …… 62
本章小结 …… 63
习题与思考题二 …… 64
第三章 半导体元器件的性能及其选择 …… 65
3.1 半导体元器件的性能及选择要求 …… 65
3.1.1 半导体元器件的分类、性能和应用 …… 65
3.1.2 半导体元器件的应用要求 …… 66
3.1.3 半导体分立元器件的选择要求 …… 67
3.1.4 半导体分立元器件的选择 …… 69
3.2 二极管的性能及其选择 …… 69
3.2.1 二极管的种类 …… 69
3.2.2 二极管的选择 …… 69
3.3 晶体管的性能及其选择 …… 72
3.3.1 晶体管的种类 …… 72
3.3.2 功率晶体管的选择 …… 72
3.3.3 小功率晶体管的选择 …… 73
3.4 场效应管的性能及其选择 …… 73
3.4.1 场效应管的类型 …… 73
3.4.2 场效应管的选择 …… 74
3.4.3 微波场效应管的选择 …… 74
3.4.4 双栅场效应管的选择 …… 75
3.5 数字集成电路的性能及其选择 …… 75
3.5.1 数字集成电路的类型 …… 75
3.5.2 数字集成电路的特点 …… 76
3.5.3 数字集成电路的选择 …… 78
3.6 模拟集成电路的类型及其选择 …… 79
3.6.1 模拟集成电路的类型 …… 79
3.6.2 运算放大器的性能及其选择 …… 79

3.6.3 线性放大器的选择 …… 80
3.6.4 非线性电路的选择 …… 81
3.6.5 稳压器的选择 …… 82
3.7 微处理器、存储器的选择 …… 83
3.7.1 微处理器的选择 …… 83
3.7.2 存储器的选择 …… 83
3.8 外围接口电路的选择 …… 84
3.8.1 外围接口电路的类型及选择 …… 84
3.8.2 D/A 与 A/D 转换器的选择 …… 85
3.8.3 电平转换器与电压比较器的选择 …… 86
3.8.4 驱动器的选择 …… 86
本章小结 …… 87
习题与思考题三 …… 88
第四章 系统失效分析 …… 89
4.1 系统失效分析的概念 …… 89
4.2 失效分析的意义、思路与方法 …… 90
4.3 失效分析的一般过程 …… 92
4.4 失效分析仪器设备 …… 93
4.4.1 失效分析仪器设备的分类 …… 93
4.4.2 几种主要的功能测试分析仪器 …… 93
4.4.3 几种性能分析测试仪器 …… 99
4.4.4 表面分析仪器 …… 102
4.5 故障模式影响分析 …… 103
4.5.1 概述 …… 103
4.5.2 故障模式分析 …… 104
4.5.3 分析的方法及其必须掌握的资料 …… 105
4.5.4 故障影响分析 …… 106
4.5.5 FMEA 工作步骤 …… 107
4.6 故障模式、影响及危害性分析 …… 109
4.6.1 概述 …… 109
4.6.2 进行 FMECA 的步骤 …… 109
4.6.3 危害性分析法 …… 110
4.6.4 FMECA 的过程 …… 115
4.6.5 应用 FMECA 时应注意的问题 …… 117
4.7 故障树分析 …… 117
4.7.1 概述 …… 117
4.7.2 故障树的基本概念及其符号 …… 118
4.7.3 故障树的建立 …… 119

4.7.4 故障树定性分析 …… 121
4.7.5 故障分析中应注意的问题 …… 123
4.8 事件树分析 …… 124
4.8.1 概述 …… 124
4.8.2 事件树的建造 …… 125
4.8.3 事件树的定量分析 …… 126
4.8.4 事件树与故障树两种分析方法的综合应用 …… 127
本章小结 …… 127
习题与思考题四 …… 129
第五章 系统可靠性预计与指标的分配 …… 130
5.1 系统可靠性要求的确定 …… 130
5.1.1 可靠性定性要求 …… 130
5.1.2 可靠性定量要求 …… 131
5.1.3 可靠性要求的确定 …… 132
5.2 系统可靠性模型的建立 …… 132
5.3 电子设备的可靠性预计 …… 135
5.3.1 可靠性预计的目的和程序 …… 135
5.3.2 电子设备的可靠性预计的特点 …… 136
5.3.3 电子设备的可靠性预计方法 …… 136
5.3.4 CRT 显示器的可靠性预计实例 …… 145
5.4 机械产品的可靠性预计 …… 147
5.4.1 机械产品可靠性预计的特点 …… 147
5.4.2 机械产品的可靠性预计方法 …… 147
5.4.3 机械产品的可靠性预计实例 …… 148
5.5 系统的可靠性预计 …… 149
5.5.1 系统可靠性预计的目的 …… 149
5.5.2 系统的可靠性预计方法 …… 149
5.5.3 系统研制阶段可靠性预计方法的选择 …… 157
5.5.4 进行系统可靠性预计时应注意的问题 …… 157
5.6 系统的可靠性分配 …… 158
5.6.1 系统可靠性分配的目的 …… 158
5.6.2 可靠性分配的准则 …… 158
5.6.3 无约束条件的系统可靠性分配方法 …… 159
5.6.4 有约束条件的系统可靠性分配方法 …… 172
5.6.5 不同研制阶段可靠性分配方法的选择和使用时应注意的问题 …… 175
5.7 计算机设备可靠性评估软件 …… 175
5.7.1 计算机设备可靠性评估软件的功能 …… 176
5.7.2 计算机设备可靠性评估软件的特点 …… 179

5.8 计算机设备可靠性评估软件的应用 …… 179
5.8.1 CRT 显示器可靠性评估 …… 179
5.8.2 计算机系统可靠性评估 …… 185
本章小结 …… 186
习题与思考题五 …… 187
第六章 系统的可靠性设计 …… 189
6.1 系统可靠性设计的内容及其设计准则 …… 189
6.2 元器件的降额设计 …… 192
6.3 元器件的容差和漂移设计 …… 195
6.3.1 容差和漂移设计的概念 …… 195
6.3.2 容差和漂移设计的方法 …… 197
6.3.3 最坏情况法 …… 197
6.3.4 蒙特卡罗法 …… 198
6.3.5 其他容差和漂移设计方法 …… 200
6.4 环境保护设计 …… 201
6.4.1 环境保护设计的内容 …… 201
6.4.2 环境因素对系统可靠性的影响 …… 201
6.4.3 环境防护原则 …… 203
6.4.4 耐环境设计措施 …… 204
6.5 系统的热设计 …… 204
6.6 系统的三防设计 …… 209
6.7 系统抗振动冲击设计 …… 210
6.8 印制板的可靠性设计 …… 213
6.8.1 印制电路板可靠性设计的目的 …… 213
6.8.2 覆铜箔印制板的选择 …… 214
6.8.3 印制板上元器件的布局 …… 215
6.8.4 元器件的安装技术 …… 216
6.8.5 表面贴装技术的应用 …… 217
6.8.6 印制板的布线原则与印制导线设计 …… 217
6.9 可维性和可用性设计 …… 218
6.9.1 可维性设计 …… 218
6.9.2 可用性设计 …… 224
本章小结 …… 227
习题与思考题六 …… 228
第七章 冗余设计 …… 229
7.1 冗余设计的基本概念 …… 229
7.1.1 冗余设计的概念 …… 229
7.1.2 本章介绍的冗余结构 …… 230

7.1.3 冗余系统处理故障的方式 …… 230
7.2 冗余设计要考虑的主要问题 …… 231
7.3 电路冗余设计 …… 234
7.3.1 二倍冗余电路 …… 234
7.3.2 四倍冗余电路 …… 235
7.4 静态冗余设计 …… 236
7.4.1 三模冗余(TMR) …… 237
7.4.2 表决技术 …… 238
7.4.3 三模表决系统的典型应用 …… 240
7.4.4 自动重构容错系统 …… 241
7.5 动态冗余设计 …… 242
7.5.1 双机比较 …… 242
7.5.2 并联结构 …… 244
7.5.3 其他动态冗余技术 …… 247
7.6 动态冗余中的可重组技术 …… 247
7.6.1 重组技术 …… 247
7.6.2 后援备份重组 …… 247
7.6.3 缓慢降级重组 …… 248
7.7 双机容错设计的应用 …… 249
7.7.1 二模协同冗余模式在 Bell ESS-2 和铁路交通控制中的应用 …… 249
7.7.2 双机系统在石油测井控制与数据处理中的应用 …… 251
7.7.3 双机系统在过程控制监测中的应用 …… 253
7.8 三模冗余系统设计的应用 …… 254
7.8.1 航天系统中的三模冗余结构的应用 …… 254
7.8.2 航空系统中应用的三模冗余结构的应用 …… 256
7.8.3 工业过程控制与监测系统中的三模冗余结构的应用 …… 259
本章小结 …… 261
习题与思考题七 …… 262
第八章 系统的电磁兼容性设计 …… 264
8.1 电磁兼容性的基本概念 …… 264
8.2 系统的电磁干扰 …… 268
8.3 电磁干扰的耦合方式 …… 271
8.4 电磁兼容性标准 …… 276
8.5 滤波和屏蔽技术 …… 278
8.5.1 滤波器 …… 278
8.5.2 铁氧体磁珠滤波器 …… 284
8.5.3 电磁屏蔽 …… 285
8.6 电磁干扰的隔离和控制 …… 289

8.6.1 光电隔离 …… 289
8.6.2 继电器隔离 …… 292
8.6.3 变压器隔离 …… 292
8.6.4 布线隔离 …… 293
8.7 雷击与静电的危害及其防护 …… 294
8.7.1 雷击危害及其防护 …… 294
8.7.2 静电危害及其防护 …… 296
8.8 系统的接地技术 …… 299
8.8.1 接地的基本概念 …… 299
8.8.2 接地干扰的产生原因及其危害 …… 300
8.8.3 工作地 …… 302
8.8.4 安全地 …… 303
8.8.5 屏蔽地 …… 305
8.8.6 微机应用系统接地技术 …… 307
本章小结 …… 309
习题与思考题八 …… 310
第九章 系统的防电磁泄漏设计 …… 312
9.1 计算机应用系统的电磁泄漏 …… 312
9.2 系统的电磁泄漏特性 …… 313
9.3 系统辐射信息的接收与测试 …… 317
9.3.1 对计算机应用系统辐射信息的接收与恢复 …… 317
9.3.2 测试计算机应用系统泄漏电磁信息的仪器 …… 317
9.3.3 对计算机应用系统设备辐射泄漏的测量 …… 319
9.3.4 对计算机应用系统设备传导泄漏的测量 …… 320
9.4 TEMPEST 技术 …… 321
9.5 计算机的防电磁泄漏设计 …… 322
9.6 外围设备的防电磁泄漏设计 …… 324
9.7 计算机设备的电磁辐射标准 …… 325
9.8 发展我国 TEMPEST 技术的措施 …… 329
本章小结 …… 330
习题与思考题九 …… 331
第十章 系统数据传输的可靠性设计 …… 333
10.1 数据传输差错的自检与校正 …… 333
10.1.1 数据传输的主要故障 …… 333
10.1.2 传输故障的解决办法 …… 335
10.1.3 编码检错与纠错的有关概念 …… 335
10.2 系统信息的差错自检与校正装置 …… 337
10.2.1 自检校验装置 …… 337

10.2.2 编码检错与纠错能力 …… 339
10.2.3 奇偶校验树 …… 339
10.3 奇偶校验错及纠错 …… 340
10.3.1 奇偶校验在计算机系统中的应用 …… 340
10.3.2 自动定位纠错功能的扩充 …… 342
10.4 多重校验检错及校正 …… 343
10.4.1 多重校验的原理 …… 343
10.4.2 多重校验的应用 …… 344
10.5 海明校验检错及校正 …… 348
10.5.1 海明校验的原理 …… 348
10.5.2 海明校验的实现 …… 352
10.5.3 海明校验的应用 …… 353
10.6 循环冗余校检错与纠错 …… 354
10.7 数字传输信道的抗干扰设计 …… 357
10.7.1 开关触点抖动的抑制 …… 357
10.7.2 负逻辑传输数字信号 …… 359
10.7.3 提高输入端门限电压 …… 360
10.7.4 线间串扰的抑制 …… 360
10.7.5 提高数字信号的电压等级 …… 361
10.8 容错条件下的故障处理 …… 362
10.8.1 计算机中的校错中断 …… 362
10.8.2 容错情况下的故障处理 …… 364
本章小结 …… 365
习题与思考题十 …… 366
第十一章 软件可靠性设计 …… 367
11.1 软件可靠性的概念与软件可靠性技术 …… 367
11.1.1 软件危机 …… 367
11.1.2 软件可靠性的概念 …… 368
11.1.3 软件可靠性技术 …… 370
11.2 软件可靠性设计技术 …… 371
11.2.1 软件的一般研制过程 …… 371
11.2.2 软件可靠性设计技术 …… 373
11.2.3 汇编语言程序设计技巧和避错方法 …… 375
11.2.4 软件的设计管理技术 …… 376
11.3 软件正确性验证 …… 377
11.4 软件容错设计技术 …… 379
11.4.1 软件容错的概念及基本原理 …… 380
11.4.2 软件容错设计基本技术 …… 381

11.4.3 容错算法的设计 …… 383
11.4.4 接口软件的容错设计 …… 384
11.4.5 容错软件常用方法 …… 386
11.5 信息保护技术 …… 387
11.5.1 信息保护技术概述 …… 387
11.5.2 内存和外存的保护 …… 387
11.5.3 身份鉴别与口令 …… 390
11.5.4 信息编码与加密 …… 395
11.6 防火墙技术 …… 395
11.6.1 设置防火墙的目的和作用 …… 395
11.6.2 防火墙的类型 …… 396
11.6.3 防火墙的安全体系结构 …… 397
11.6.4 防火墙的发展趋势 …… 401
11.7 软件可靠性模型 …… 402
11.7.1 概述 …… 402
11.7.2 杰林斯基-莫洛达模型 …… 403
11.7.3 葛尔-奥肯莫特的 NHPP 模型 …… 405
11.7.4 Little Wood 贝叶斯排错模型 …… 408
11.7.5 软件可靠性模型的应用 …… 410
11.8 软件的错误分析及其测试 …… 410
11.8.1 软件错误的特征 …… 410
11.8.2 软件错误的分类 …… 411
11.8.3 软件错误测试方法 …… 414
11.8.4 软件错误测试工具 …… 415
11.9 软件可维性设计 …… 417
11.9.1 软件的可维性 …… 417
11.9.2 改正性维护设计 …… 419
11.9.3 改造性维护设计 …… 419
本章小结 …… 420
习题与思考题十一 …… 422
第十二章 系统可测试性设计 …… 423
12.1 系统可测试性的概念 …… 423
12.1.1 计算机应用系统的测试 …… 423
12.1.2 故障可测试性 …… 424
12.1.3 系统故障的诊断测试 …… 425
12.1.4 测试的评价 …… 427
12.2 逻辑模拟与故障辞典 …… 427
12.2.1 逻辑模拟 …… 428

12.2.2 故障模拟 …… 431
12.2.3 数字模拟 …… 433
12.2.4 故障辞典 …… 436
12.3 改善系统可测试性的基本方法 …… 438
12.3.1 改善逻辑的可控性 …… 439
12.3.2 改善电路故障的可观性 …… 441
12.3.3 改善系统和电路可测性 …… 443
12.4 通路敏化与故障定位测试法 …… 443
12.4.1 通路敏化的概念 …… 444
12.4.2 测试码的生成 …… 445
12.4.3 故障定位测试方法 …… 446
12.5 临界通路敏化法 …… 451
12.6 *D* 算法 …… 454
12.6.1 *D* 算法的原理 …… 454
12.6.2 *D* 算法的过程 …… 457
12.6.3 *D* 算法的应用 …… 460
12.7 因果函数分析法 …… 463
12.7.1 因果函数及其主要性质 …… 463
12.7.2 Paoge 法 …… 464
12.7.3 Bossen 法 …… 465
12.8 机内自测试设计 …… 467
12.8.1 内建自测试设备 …… 468
12.8.2 BITE 的结构 …… 468
12.8.3 测试点的选择和评价 …… 471
本章小结 …… 472
习题与思考题十二 …… 473
附录 …… 475
附录一 元器件降额标准 …… 475
附录二 计算机设备可靠性设计准则 …… 479
附录三 武器装备可靠性设计准则 …… 482
主要参考文献 …… 485

第一章 绪 论

内容提要

本章为绪论，介绍系统可靠性分析与设计的概述和基本知识。它主要包括：

- 系统可靠性分析与设计的意义；
- 系统可靠性的基本概念；
- 系统的寿命分布；
- 系统的可靠性模型；
- 可维修系统的马尔可夫模型；
- 提高系统可靠性的途径；
- 系统可靠性与加固设计的内容。

1.1 系统可靠性分析与设计的意义

随着计算机日益广泛的应用，其可靠性和安全性已成为一个十分突出的问题。许多应用场合都要求计算机必须长期稳定、可靠、安全地运行，否则就无法进行工作。在航空、航天、导弹系统、过程控制和金融及交通管理等应用领域，计算机哪怕有一个微小的故障，都可能造成巨大损失，甚至会导致一场灾难的发生。

1962 年 6 月，美国宇航局发往金星的第一个宇宙探测器——水手 1 号，由于其计算机系统的一个故障，在发射后不久就坠毁了，数亿美元倾刻间化为乌有，也造成了严重的政治影响。

1979 年，美军使用计算机应用系统指挥一次军事演习，由于计算机失灵，使进攻与撤退的次序颠倒，造成了极大的混乱。

1979 年，新西兰航空公司的一架客机，因计算机控制的飞行系统出错而撞在 Erebus 山上，机上 257 名乘客遇难身亡。

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，将飞来的导弹误认为是友军武器，没有将它击落，结果该舰被击沉。

在美国空军的一次编队飞行中，因火控计算机故障，竟向本军发射了导弹，造成了严重的后果。

1981 年 7 月 4 日，在日本兵库县的川畸重工公司发生了一起机器人杀人的事件。被害者叫酒田宽二，男，37 岁。这一天，该厂汽车传动车间的机器发生了故障，修理工酒田宽二前去修理。当他修好机器，接通电源准备试车时，由于电脑发生故障，机器人也随之动作起来。它从酒田宽二的背后过来，用两只手紧紧抓住酒田宽二，把他放在机器上活活地压死了。像这样，由于电脑故障而发生机器人杀人的事件在日本川畸重工公司近两年中就发生过三起。

1980 年 6 月 2 日午夜前不久，北美战略防空司令部发出了“苏联发起核进攻”的战争

警报，司令部值班室内的一块计算机屏幕上突然出现这样惊人的信息：苏联洲际导弹和带有核弹头的潜艇导弹已飞临美国！数秒钟后，值班将军理查德·艾黎斯接到了通知。顿时，1/3的核轰炸部队和约100架安装有8台发动机的B-52飞机已经发动，准备升空，153个火箭分队的发射员的手已经按摸在发射按钮上待命，1054枚“民兵”和“大力神”导弹和24艘装有氢弹头的导弹潜艇已经准备随时出发。一架经过改装的有4台发动机的运输机已经在夏威夷起飞，准备接替可能被摧毁的战略防空司令部作为空军指挥所。在华盛顿的安德鲁斯空军基地上，卡特总统的“空中司令部”已经发动。世界面临着一场核战争的严重威胁。可谁知道，这个系统的计算机中的一个小小的元件故障，竟是造成这场虚惊的罪魁祸首。像这样由于计算机应用系统故障而误发核战争警报的事件，从1977年到1980年6月竟发生过151次。这些故障，不仅造成巨大的损失，引起人们的极大恐慌，也使计算机系统中存储的机密信息严重泄漏和破坏。

近10年来出现和传播的计算机病毒，不仅严重干扰计算机应用系统的工作，而且严重威胁计算机及应用系统的安全。这些病毒，有的只干扰屏幕，有的封锁打印机，有的则修改或破坏软、硬盘上的数据或引导扇区和文件分配表，有的驻留内存，修改中断向量表或格式化硬盘，更有甚者则使系统瘫痪。

1987年12月，美国IBM公司邮电通信网中的数万台计算机因感染圣诞树“蠕虫”病毒而瘫痪，35万台终端因被圣诞树“蠕虫”病毒堵塞而被迫关闭。

1988年11月2日，美国康奈尔大学计算机系研究生罗伯特·莫里斯的一项病毒程序试验，竟使美国国防部远景规划署的APARNET网上的6000多台计算机突然停止工作。该网连接着全国300所大学、研究中心、军事基地和国防部科研机构及私人公司。东起麻省理工学院、哈佛大学、马里兰海军实验室，西到加利福尼亚大学、斯坦福大学国家研究所以及费古尼亚的太空总署研究中心和兰德研究中心，整个网络瘫痪了24个小时，造成的经济损失近1000万美元。

这些事件，都是由于系统可靠性问题造成的，如元器件故障或软件故障，或是机械故障，或是暂时故障或人为故障。它涉及到工艺、设计、制造、使用等多个环节。因此，如何保证计算机及其应用系统的可靠性、安全性就成为一个亟待解决的问题。这是因为：

1）随着计算机及应用系统功能的日益完善，运算速度的日益加快，其组成日益复杂，元器件装配密度日益加大，这就使得计算机及其应用系统的故障率增大。

2）由于计算机应用日益广泛，人们对计算机及其应用系统的依赖性也越来越强。许多国家的重要部门、经济命脉、军事部门、国防工程都由计算机控制。这些领域的计算机及其应用系统可能随时遭受病毒的攻击，重要的信息可能被窃取，甚至被破坏。这就可能导致灾难性后果，必须采用有效措施，进行有力地防护。

3）随着计算机应用队伍的迅速扩大，用户对计算机及其应用系统一时难以全面、深入地了解。这就要求计算机及其应用系统必须能够防止或容忍人为操作的失误。因此，提高计算机及其应用系统的可靠性及安全性就成为人们日益关注的重要问题。

4）随着大规模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不断下降，而使用、维护和管理的成本相对提高。只有提高计算机的可靠性，才能减少出现故障的概率，降低使用、维护和管理的成本。

5）由于计算机应用日益广泛，使用场所逐渐从条件优越的机房转到工厂、野外、海