装备科技译著出版基金

· 国外技术研发成功经验总结
· 产品研发与管理宝典
· 国外技术类畅销书

Assurance Technologies Principles and Practices

A Product, Process,and System Safety Perspective

保证技术原理与实践

产品、过程和系统安全性观点

【美】Dev G.Raheja,Michael Allocco 著

梅文华 罗乖林 侯建 章珂 丁利平 吴文婷 译

国防工业出版社
National Defense Industry Press

WILEY

装备科技译著出版基金

Assurance Technologies Principles and Practices

保证技术原理与实践

产品、过程和系统安全性观点

A Product, Process, and System Safety Perspective

[美] Dev G. Raheja, Michael Allocco 著

梅文华 罗乖林 侯 建
章 珂 丁利平 吴文婷 译

国防工业出版社

著作权合同登记　图字:军-2008-000 号

图书在版编目(CIP)数据

保证技术原理与实践:产品、过程和系统安全性观点/(美)拉赫贾(Rahe ja, D. G.),(美)阿罗科(Allocco, M.)著;梅文华等译. —北京:国防工业出版社,2014.6

书名原文:Assurance technologies principles and practices (Second Edition):a product, process, and system safety perspective

ISBN 978-7-118-09439-8

Ⅰ.①保… Ⅱ.①拉…②阿…③梅… Ⅲ.①软件质量-质量管理 Ⅳ.①TP311.5

中国版本图书馆 CIP 数据核字(2014)第 060796 号

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

※

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 100048)
北京嘉恒彩色印刷有限公司
新华书店经售
*
开本 710×1000　1/16　印张 25　字数 480 千字
2014 年 6 月第 1 版第 1 次印刷　印数 1—3000 册　定价 98.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776
发行传真:(010)88540755　　发行业务:(010)88540717

译 者 序

装备可靠性工程理论和技术从国外引进已有 30 余年，翻译出版了大量书籍，并且通过消化吸收和创新研究，国内专家也编著出版了大量书籍。但是，这些书籍主要局限于可靠性、维修性和保障性的范围。随着技术的发展，近年来逐步重视测试性和安全性的研究。但是，对于装备安全性的研究非常之少，以至于目前在型号研制中，订购方不知如何提出安全性要求、如何进行验证与评价；在研制过程中，研制方不知如何开展安全性设计与分析工作。

《保证技术原理与实践》一书是作者长期研究的总结，在全面阐述装备共性技术及其相互关系方面非常有特色，既有理论深度，又有实践经验，对国内科研、生产和教学，有重大参考应用价值。第一作者 Dev Raheja（德夫·拉赫贾）是世界上系统保证技术领域的领军人物。作为“按竞争力进行设计”的创始人和主席，他主要与通用电气、通用汽车、西门子、尼桑、波音、NASA、福特、英特尔、摩托罗拉和 IBM 等一些大公司负责研发的经理和工程技术人员合作，就如何运用创新和创造力来降低新产品的费用开展培训。他曾经担任通用电气公司执行董事，在加州大学、华盛顿大学和威斯康星大学开办过可靠性与系统安全性培训班，并在马里兰大学任教授，负责可靠性工程专业的博士学位课程教学。他曾获得多项奖励，包括系统安全性学会授予的科学成就奖。他出版的《保证技术原理与实践》第一版曾列入技术类畅销书。第二作者 Michael Allocco（米歇尔·阿罗科）在安全性工程、系统安全性和安全性管理方面有 30 多年的经验，主要从事民用、军用、航空航天和医疗领域的产品、过程和系统的危险分析、风险评估和事故调查。他是系统安全性学会的会员，曾任该学会执行副主席。他发表了很多关于系统安全性技术和方法的论文。他还在 3 所重点大学开设了系统安全性工程方面的研究生课程。

《保证技术原理与实践》由梅文华、罗乖林、侯建、章珂、丁利平、吴文婷翻译，由梅文华统稿。梅文华翻译第 3，7，11，13 章；罗乖林翻译第 5，8，10 章；侯建翻译第 9，14 章；章珂翻译第 1，2，6 章；丁利平翻译第 4 章和术语；吴文婷翻译第 12 章和附录。

《保证技术原理与实践》的翻译出版得到了总装备部装备科技译著出版基金资助，空军装备研究院张福泽院士、武汉理工大学罗帆教授高度评价和热情推荐了该书，在此一并表示衷心的感谢。

译者期望《保证技术原理与实践》的翻译出版对我国军工产品研制过程中贯彻落实可靠性、维修性、测试性、保障性、安全性等专门工程工作能起到促进作用。

由于译者水平有限，译文中难免出现错误和不足，敬请批评指正。

译　者

前　言

复杂系统中超过60%的问题是由内容不完整、描述不清晰、文字水平不高的规范所引起的。一个好的规范将减少至少80%的风险，这就是我们编写本书的目的。要确保规范的质量，就应该完整地读完这本书。每一章都揭示规范的一个不同方面。比如你建造一栋新房，仅描述前边的墙面是不够的，必须仔细关注每一堵墙面，否则，大家可能会对一栋各边失调、墙地不合的房子感到纠结。同样，我们必须从各个方面如系统安全性、可靠性、维修性、人机工程、后勤保障、软件完整性和系统集成等方面描述产品，确保各方面之间匹配良好。

大家都对安全性倾注了大量心血。我们无法忍受重大事故和每年大约125次汽车安全性召回。太多的人徒然丧命，无数家庭遭受痛苦。这就是为什么本书每一章都要描述确保我们所做每一件事情的安全性的方法。

本书强调的安全性工作不仅仅是一项像大多数人出于无知认为的必要开支，而是一项出色的投资。2004年，仅在车祸中就死亡120万人，经济损失达到2300亿美元，预防事故的成本肯定比这要低得多。

本书第一版1991年由McGraw－Hill出版社出版，书名《保证技术：原理与实践》，曾连续两年列入技术类畅销书。后来，由于McGraw－Hill停止出版工程管理类图书，导致印刷中断。作者感谢John Wiley & Sons出版社鼓励我们写作本书并将安全性作为本书的坚实基础。也感谢我们的读者，正是你们让第一版成为畅销书。

Dev G. Raheja

Michael Allocco

目　录

第 1 章　保证技术、利润及与安全性相关的风险管理 …… 1

1.1　引言 …… 1
1.2　更省、更好和更快的产品 …… 2
1.3　什么是系统保证 …… 4
1.4　关键的管理责任 …… 4
1.4.1　集成 …… 4
1.4.2　制定与目标相符的预算 …… 5
1.4.3　管理风险 …… 5
1.5　系统保证是一个过程 …… 7
1.6　系统保证大纲 …… 8
参考文献 …… 8
补充读物 …… 9

第 2 章　统计概念简介 …… 10

2.1　概率设计 …… 10
2.2　用于可靠性、安全性和维修性的概率计算 …… 10
2.2.1　直方图的结构和经验分布 …… 10
2.2.2　可靠性计算 …… 12
2.2.3　故障率和危险函数 …… 13
2.3　正态分布 …… 13
2.4　对数正态分布 …… 18
2.5　指数分布 …… 20
2.6　威布尔分布 …… 24
2.7　威布尔分布的数据分析 …… 26
2.8　离散分布 …… 29

2.8.1 二项分布 …… 30
2.8.2 泊松分布 …… 31
2.9 学生项目和论文选题 …… 32
参考文献 …… 32
补充读物 …… 32

第3章 可靠性工程及与安全性相关的应用 …… 34

3.1 可靠性原理 …… 34
3.2 设计阶段的可靠性 …… 36
3.2.1 编写可靠性规范 …… 37
3.2.2 进行设计评审 …… 37
3.2.3 可靠性分配 …… 40
3.2.4 可靠性建模 …… 41
3.2.5 可靠性预计 …… 43
3.2.6 故障模式影响及危害性分析 …… 45
3.2.7 最坏情况分析 …… 51
3.2.8 其他分析技术 …… 52
3.2.9 设计改进方法 …… 52
3.3 制造阶段的可靠性 …… 55
3.4 试验阶段的可靠性 …… 56
3.4.1 可靠性增长试验 …… 56
3.4.2 耐久性试验 …… 59
3.4.3 低故障率试验 …… 64
3.4.4 老练和筛选 …… 69
3.5 使用阶段的可靠性 …… 73
3.6 可靠性和安全性的共同点 …… 73
3.6.1 共同的系统目标 …… 74
3.6.2 不可靠性和危险 …… 74
3.6.3 复杂风险 …… 74
3.6.4 潜在系统事故 …… 75
3.6.5 软件可靠性与安全性 …… 75
3.6.6 可靠性与安全性权衡 …… 76

3.6.7 有关可靠性和安全性的错误认识 …… 76
3.7 学生项目和论文选题 …… 85
参考文献 …… 85
补充读物 …… 86

第4章 维修性工程及与安全性相关的应用 …… 88

4.1 维修性工程原理 …… 88
4.2 设计阶段的维修性 …… 90
4.2.1 制定维修性规范 …… 90
4.2.2 维修性设计评审 …… 91
4.2.3 维修性分析 …… 92
4.2.4 维修性的 FMECA …… 93
4.2.5 维修性预计 …… 94
4.2.6 寿命周期费用分析 …… 96
4.2.7 可达性设计 …… 98
4.2.8 维修方便性设计 …… 98
4.2.9 测试的 MM 设计 …… 101
4.3 制造阶段的维修性 …… 105
4.3.1 现有设备的维修性 …… 105
4.3.2 新设备的维修性 …… 106
4.4 试验阶段的维修性 …… 108
4.4.1 维修性试验的前提条件 …… 109
4.4.2 设备固有的停机时间试验 …… 109
4.4.3 人的差异试验 …… 109
4.4.4 修理级别试验 …… 109
4.5 使用阶段的维修性 …… 109
4.5.1 预计和减少有寿件 …… 110
4.5.2 监控和预计使用可用度 …… 111
4.5.3 降低保障费用 …… 112
4.6 维修性与系统安全性 …… 113
4.6.1 远程维修的安全性和保密性 …… 114
4.6.2 系统健康监控与维修 …… 115

4.6.3 利用模型来开发维修诊断和监控 …… 115
4.6.4 支持维修的危险分析 …… 117
4.7 学生项目和论文选题 …… 123
参考文献 …… 124
补充读物 …… 124

第5章 系统安全性工程 …… 125

5.1 系统安全性原理 …… 125
5.1.1 系统安全性过程 …… 127
5.1.2 风险评价 …… 128
5.1.3 技术风险分析 …… 129
5.1.4 残余风险 …… 129
5.1.5 应急预案 …… 130
5.2 设计阶段的系统安全性 …… 130
5.2.1 安全设计准则 …… 130
5.2.2 安全性工程任务 …… 132
5.2.3 初步危险分析 …… 133
5.2.4 分系统危险分析 …… 136
5.2.5 故障树分析 …… 137
5.2.6 割集分析 …… 140
5.2.7 故障模式、影响及危害性分析 …… 141
5.2.8 维修工程安全性分析 …… 141
5.2.9 事件树 …… 143
5.2.10 使用与保障危险分析 …… 143
5.2.11 职业健康危险评估 …… 145
5.2.12 潜在电路分析 …… 145
5.2.13 系统危险分析 …… 147
5.3 制造阶段的系统安全性 …… 147
5.3.1 确定安全关键项目 …… 147
5.3.2 制造安全性控制 …… 148
5.4 试验阶段的系统安全性 …… 149
5.4.1 试验原理 …… 149

5.4.2 进行正确试验的先决条件 …… 150
5.4.3 产品鉴定试验 …… 151
5.4.4 生产试验 …… 151
5.4.5 人为差错试验 …… 151
5.4.6 设计更改的安全性试验 …… 152
5.4.7 规程试验 …… 152
5.4.8 试验数据分析——正确的方法 …… 153
5.4.9 多少试验足够? …… 153
5.5 使用阶段的系统安全性 …… 153
5.5.1 闭环危险管理(危险追踪和风险解决) …… 153
5.5.2 规程的完整性 …… 154
5.5.3 更改控制 …… 154
5.5.4 事故/事件调查 …… 154
5.6 分析系统危险和风险 …… 155
5.6.1 SDHA 过程的研发 …… 156
5.6.2 设计事故 …… 157
5.7 危险识别 …… 160
5.7.1 情景主题 …… 160
5.7.2 主要危险 …… 161
5.7.3 诱发因素 …… 162
5.7.4 贡献因素 …… 163
5.7.5 交叉危险 …… 164
5.8 学生项目和论文选题 …… 164
参考文献 …… 165
补充读物 …… 166

第 6 章 质量保证工程和潜在安全隐患预防 …… 168

6.1 质量保证原理 …… 168
6.2 设计阶段的质量保证 …… 169
6.2.1 产品设计质量评审 …… 170
6.2.2 为质量和产量的工艺设计评审 …… 173
6.2.3 对健壮性的设计优化 …… 175

6.2.4 过程 FMECA …… 179
6.2.5 设计阶段的采购和过程控制质量保证计划 …… 182
6.3 制造阶段的质量保证 …… 183
6.3.1 对试运行的评价 …… 183
6.3.2 过程控制 …… 184
6.3.3 对于世界级质量的 ppm 控制 …… 189
6.3.4 与供货商一道工作 …… 191
6.3.5 ppm 评估 …… 192
6.4 试验阶段的质量保证 …… 193
6.4.1 鉴定试验与生产试验 …… 193
6.4.2 工业标准 …… 194
6.5 使用阶段的质量保证 …… 194
6.6 学生项目和论文选题 …… 194
参考文献 …… 194
补充读物 …… 195

第 7 章 后勤保障工程与系统安全性考虑 …… 197

7.1 后勤保障原理 …… 197
7.2 设计阶段的后勤工程 …… 197
7.2.1 现役产品的后勤规范 …… 198
7.2.2 新产品的后勤规范 …… 199
7.2.3 设计评审 …… 200
7.2.4 后勤保障分析 …… 200
7.2.5 为后勤保障分析进行 FMECA …… 201
7.2.6 时间线分析 …… 203
7.2.7 修理级别分析 …… 203
7.2.8 后勤保障分析文档 …… 203
7.3 制造阶段的后勤工程 …… 204
7.4 试验阶段的后勤工程 …… 204
7.4.1 R&M 特征试验 …… 205
7.4.2 使用程序试验 …… 205
7.4.3 应急预案试验 …… 205

7.5 使用阶段的后勤工程 …… 205
7.5.1 以可靠性为中心的维修 …… 205
7.5.2 测量后勤工程的效能 …… 208
7.6 后勤保障工程和系统安全性 …… 209
7.6.1 产品、普通大众和专家的责任 …… 209
7.6.2 变化风险分析 …… 209
7.6.3 寿命周期后勤和系统安全性 …… 210
7.7 学生项目和论文选题 …… 216
参考文献 …… 216
补充读物 …… 217

第8章 人因工程和系统安全性考虑 …… 218

8.1 人因工程原理 …… 218
8.2 设计阶段人的因素 …… 218
8.2.1 在规范中使用检查单和标准 …… 219
8.2.2 人机接口设计评审 …… 221
8.2.3 利用过去的教训 …… 222
8.2.4 危险分析评审 …… 222
8.3 生产阶段人的因素 …… 223
8.3.1 生产错误的类型和控制 …… 223
8.3.2 防止检验错误 …… 224
8.4 试验阶段人的因素 …… 225
8.4.1 针对习惯行为的试验 …… 225
8.4.2 应急准备试验 …… 226
8.4.3 补救试验 …… 227
8.4.4 人－机接口试验 …… 228
8.5 使用阶段人的因素 …… 228
8.6 涉及人因和系统安全性的其他考虑 …… 229
8.6.1 人的个体差异 …… 229
8.6.2 人因工程复杂性 …… 229
8.6.3 人是机器 …… 229
8.6.4 人的行为 …… 230

8.6.5 人的动机 …… 230
8.6.6 动机和安全文化 …… 230
8.6.7 人为差错 …… 230
8.7 实时错误和潜在错误 …… 231
8.8 人因和系统安全性支持分析 …… 231
8.8.1 人的接口分析 …… 231
8.8.2 链路分析 …… 231
8.8.3 严重事故技术(CIT) …… 232
8.8.4 行为抽样 …… 233
8.8.5 程序分析 …… 234
8.8.6 生命保障/生命安全分析 …… 235
8.8.7 工作安全性分析 …… 235
8.8.8 人的可靠性 …… 235
8.8.9 错误率预计技术(THERP) …… 236
8.8.10 人的事件分析技术(ATHEANA) …… 237
8.8.11 人为差错关键度分析(HECA) …… 238
8.8.12 工作量评估 …… 238
8.9 学生项目和论文选题 …… 239
参考文献 …… 239
补充读物 …… 240

第9章 软件性能保证 …… 241

9.1 软件性能原理 …… 241
9.1.1 软件质量 …… 242
9.1.2 软件可靠性 …… 242
9.1.3 软件系统安全性 …… 244
9.1.4 软件可维护性 …… 245
9.1.5 软件保障工程 …… 245
9.1.6 一些重要定义 …… 245
9.2 设计阶段的软件性能 …… 247
9.2.1 设计中的软件质量保证 …… 247
9.2.2 设计中的软件可靠性 …… 247

9.2.3 设计中的软件可维护性 …… 251
9.2.4 设计中的软件系统安全性 …… 252
9.2.5 软件综合保障工程 …… 255
9.2.6 软件系统故障模式和影响分析 …… 256
9.2.7 软件性能规范 …… 259
9.2.8 软件设计评审检查单 …… 264
9.3 编码和集成阶段的软件要求 …… 271
9.3.1 编码错误 …… 271
9.3.2 量化软件错误 …… 272
9.3.3 编码错误的预防 …… 274
9.4 软件测试 …… 275
9.4.1 质量测试 …… 275
9.4.2 可靠性测试 …… 276
9.4.3 可维护性测试 …… 276
9.4.4 软件安全性测试 …… 276
9.4.5 全面合格测试 …… 277
9.5 使用阶段的软件性能 …… 277
9.6 学生项目和论文选题 …… 278
参考文献 …… 279

第 10 章 系统效能 …… 280

10.1 概述 …… 280
10.2 系统效能原理 …… 281
10.3 贯彻大纲 …… 284
10.4 寿命周期费用管理 …… 287
10.5 系统效能模型 …… 288
10.6 作者建议 …… 288
10.7 系统风险及其对系统效能的影响 …… 289
10.7.1 系统事故 …… 289
10.7.2 复杂的系统风险 …… 289
10.7.3 相关风险 …… 290
10.7.4 采用有效的系统安全性要求和标准控制风险 …… 290

10.7.5 有效的系统安全性要求和标准 …… 291
10.7.6 其他的系统效能模型 …… 295
10.7.7 系统效能或成功的其他指标 …… 295
10.8 学生项目和论文选题 …… 296
参考文献 …… 296
补充读物 …… 297

第 11 章 管理与安全性相关的风险 …… 298

11.1 制定适当的安全性大纲以管理风险 …… 298
11.2 针对产品、过程和系统的安全性大纲 …… 298
11.2.1 产品安全性管理 …… 298
11.2.2 过程安全性管理 …… 300
11.2.3 系统安全性管理 …… 303
11.3 安全性管理的资源分配和费用分析 …… 308
11.4 学生项目和论文选题 …… 308
参考文献 …… 309
补充读物 …… 309

第 12 章 统计概念、损失分析以及与安全性相关的应用 …… 310

12.1 与安全性相关的分布和统计应用 …… 310
12.2 安全性分析中采用的统计分析技术 …… 310
12.3 在安全性决策中运用统计控制 …… 312
12.4 行为抽样 …… 314
12.5 计算人身系统受到的危险 …… 315
12.6 学生项目和论文选题 …… 317
参考文献 …… 318
补充读物 …… 318

第 13 章 模型、概念和实例:应用情景驱动危险分析 …… 319

13.1 不利序列 …… 319
13.1.1 安全性分析中的情景 …… 319
13.1.2 安全性分析中的建模 …… 319

13.1.3 分析信息的综合和表示 …… 322
13.1.4 叙述报告与表列格式 …… 322
13.2 为进行分析和报告结果设计格式 …… 323
13.3 记录报告 …… 325
13.4 概念模型 …… 326
13.4.1 Hammer 模型 …… 326
13.4.2 复杂情景模型 …… 326
13.4.3 鱼骨图 …… 327
13.5 系统事故的寿命周期 …… 328
13.5.1 复杂的交互作用 …… 329
13.6 使用与保障危险分析案例 …… 329
13.7 学生项目和论文选题 …… 336
参考文献 …… 336
补充读物 …… 336

第 14 章 自动化、计算机和软件复杂性 …… 338

14.1 复杂系统分析 …… 338
14.2 系统概述 …… 338
14.3 理解不利序列 …… 339
14.3.1 失灵和故障模式 …… 339
14.3.2 理解系统功能 …… 339
14.3.3 理解概念过程 …… 340
14.4 其他的软件安全性分析技术 …… 340
14.4.1 软件失灵 …… 341
14.4.2 与软件相关的风险的表现形式 …… 342
14.4.3 理解异常 …… 342
14.4.4 复杂性、理解风险、系统状态 …… 342
14.4.5 系统状态 …… 343
14.4.6 诱发因素、贡献因素和系统事故的复杂性 …… 343
14.4.7 功能的抽象和域 …… 343
14.4.8 寿命周期内的潜在危险 …… 343
14.4.9 模型使用和开发中的错误 …… 344