

高等学校通用教材

# 系统可靠性 设计分析教程

曾声奎 赵廷弟 张建国 康锐 石君友 编著

北京航空航天大学出版社

<http://www.buaapress.com.cn>

# 系统可靠性设计分析教程

曾声奎 赵廷弟  
张建国 康锐 石君友 编著

北京航空航天大学出版社

<http://www.buaapress.com.cn>

## 内容提要

本书在跟踪国内外可靠性工程技术发展的基础上,结合国内型号可靠性工作经验,优选成熟且效果明显的系统可靠性设计分析技术,以型号可靠性设计分析工作流程为主线,进行了系统的整理、编写。

本书共分 11 章。在阐述现代系统设计思想转变和系统可靠性设计分析流程的基础上,讲述了可靠性建模、可靠性要求制定与分配、可靠性预计、故障模式影响和危害性分析、故障树分析、事件树分析等内容,并针对电子产品与机械产品的特点,对其可靠性设计方法分别专章进行了论述。最后,对一些前沿的可靠性设计分析技术,如软件可靠性、功能可靠性仿真技术等作了简要介绍。

本书强调了基本理论技术的系统性与工程实用性的结合,并提供了丰富的工程案例。可供大专院校本科生及研究生学习使用,也可供工程技术人员学习和参考。

### 图书在版编目(CIP)数据

系统可靠性设计分析教程/曾声奎. —北京:北京

航空航天大学出版社,2001.1

ISBN 7-81077-015-2

I. 系… II. 曾… III. ①系统可靠性-系统设计-高等学校-教材②系统可靠性-系统分析-高等学校-教材  
IV. N945.17

中国版本图书馆 CIP 数据核字(2000)第 50219 号

### 系统可靠性设计分析教程

曾声奎 赵廷弟 编著  
张建国 康锐 石君友

责任编辑 王晓梅

北京航空航天大学出版社出版发行

北京市学院路 37 号(100083) 发行部电话(010)82317024

<http://www.buaapress.com.cn>

E-mail: [pressell@publica.bj.cninfo.net](mailto:pressell@publica.bj.cninfo.net)

河北省涿州市新华印刷厂印制 各地书店经销

\*

开本:787×1092 1/16 印张:17.125 字数:438 千字

2001 年 1 月第 1 版 2001 年 1 月第 1 次印刷 印数:3000 册

ISBN 7-81077-015-2/TB·001 定价:20.00 元

# 前 言

可靠性工程是研究产品全寿命过程中故障的发生、发展规律,达到预防故障、消灭故障,提高产品效能之目的的工程技术。

可靠性工程作为一门独立的工程学科,率先在美国形成。从1957年美国国防部电子设备可靠性顾问团(AGREE)报告发表以来,至今已40余年,可靠性工程经历了萌生、发展、成熟的过程。1965年国际电工委员会(IEC)可靠性专业委员会的成立,标志着可靠性工程成为了一门国际化的技术。

20世纪60年代我国就在电子工业部门进行了可靠性工程技术的开拓性工作。进入80年代以后,我国颁布了一系列的可靠性工程技术标准和管理规定,在现代武器装备等大型系统的研制中全面推行可靠性工程技术,使我国工程型号的可靠性工作进入规范化的轨道,并得到迅速的发展。国内外可靠性工程技术的快速发展,特别是国内开展型号可靠性工作所积累的丰富经验,都需要很好的总结与推广。近年来,国内出版了不少关于可靠性工程技术的论著,然而却缺少随着可靠性设计分析技术进步而更新的本科生及研究生的教材。本书编写的目的就是努力填补这一空缺。

本书编写的指导思想是:全面追踪国内外可靠性工程技术的发展,结合近十年来国内型号可靠性工作中的经验,优选成熟的、效果明显的可靠性设计分析技术,以型号可靠性设计分析工作流程为主线,总结多年的教学经验,进行系统的整理并组织教材的编写。编写中强调了基本理论与技术的系统性和工程实用性的结合,强调案例,强调教学法,以满足教学的需求。

本书共分11章,在阐述现代系统设计思想转变和系统可靠性设计分析流程的基础上,讲述了可靠性建模、可靠性要求的制定与分配、可靠性预计、故障模式影响和危害性分析、故障树分析、事件树分析等内容,并针对电子产品与机械产品的特点,对其可靠性设计分析方法分别专章进行了论述。最后,对一些前沿的可靠性设计分析技术,如软件可靠性、功能可靠性仿真技术等进行了简要介绍。

本书可供大专院校本科生及研究生学习使用,也可供工程技术人员学习和参考。由于水平有限,错误之处在所难勉,望读者指正。

参加编写工作的有:曾声奎副教授(第1、2、3、9章),赵廷弟副研究员(第4、5、11章),康锐研究员(第6、8章),张建国讲师(第7、10、11章),石君友讲师(第9章及附录)。全书由曾声奎主编,屠庆慈教授、李沛琼教授主审。

作者

2000年5月

# 目 录

## 第 1 章 引 言

1.1 现代质量观念与设计思想转变 .....	1
1.2 系统可靠性设计分析流程 .....	3
1.3 系统可靠性设计分析的基本内容 .....	8
习 题 .....	8

## 第 2 章 可靠性基本概念和参数体系

2.1 可靠性基本概念 .....	9
2.1.1 可靠性及故障 .....	9
2.1.2 寿命剖面与任务剖面 .....	10
2.1.3 可靠度函数、累积故障分布函数及故障密度函数 .....	12
2.1.4 故障率与浴盆曲线 .....	13
2.1.5 平均故障前时间与平均故障间隔时间 .....	16
2.1.6 产品的寿命特征 .....	17
2.1.7 常用分布 .....	17
2.2 可靠性参数体系 .....	18
2.2.1 可靠性参数的分类 .....	18
2.2.2 常用可靠性参数 .....	19
2.2.3 可靠性参数间的相关性 .....	20
2.2.4 可靠性参数指标的特点 .....	21
习 题 .....	22

## 第 3 章 系统可靠性模型建立

3.1 概 述 .....	23
3.2 系统功能分析 .....	26
3.2.1 功能的分解与分类 .....	27
3.2.2 功能框图与功能流程图 .....	27
3.2.3 时间分析 .....	29
3.2.4 任务定义及故障判据 .....	30
3.3 典型可靠性模型 .....	31
3.3.1 串联模型 .....	31

3.3.2	并联模型	32
3.3.3	$r/n(G)$ 模型	33
3.3.4	非工作贮备模型(旁联模型)	34
3.3.5	桥联模型	35
3.4	不可修系统可靠性模型	36
3.4.1	虚单元	36
3.4.2	复杂系统任务可靠性模型	37
3.5	系统可靠性建模示例	42
	习 题	45

#### 第4章 可靠性要求制定与分配

4.1	可靠性要求	46
4.1.1	可靠性定性要求	46
4.1.2	可靠性定量要求	47
4.2	可靠性要求的制定	48
4.2.1	可靠性定量要求的制定	48
4.2.2	可靠性定性要求的制定	51
4.3	可靠性分配	51
4.3.1	可靠性分配的原理和准则	52
4.3.2	无约束条件的系统可靠性分配方法	53
4.3.3	有约束条件的系统可靠性分配方法	64
4.3.4	不同研制阶段可靠性分配方法的选择	67
4.3.5	进行可靠性分配时的注意事项	67
4.4	应用示例	68
4.4.1	可靠性参数选择与指标确定	69
4.4.2	可靠性分配	71
	习 题	72

#### 第5章 可靠性预计

5.1	概 述	75
5.1.1	可靠性预计的目的和用途	75
5.1.2	可靠性预计的分类及程序	75
5.1.3	可靠性预计与可靠性分配的关系	76
5.2	单元可靠性预计方法	76
5.2.1	相似产品法	76
5.2.2	评分预计法	77
5.2.3	应力分析法	79
5.2.4	故障率预计法	81
5.2.5	机械产品可靠性预计方法	82

5.3 系统可靠性预计	84
5.3.1 基本可靠性预计	84
5.3.2 任务可靠性预计	86
5.3.3 不同研制阶段可靠性预计方法的选取	97
5.3.4 进行可靠性预计时的注意事项	98
习 题	98
<b>第 6 章 故障模式影响及危害性分析</b>	
6.1 概 述	101
6.2 故障模式影响分析	103
6.2.1 故障模式分析	103
6.2.2 故障原因分析	104
6.2.3 故障影响分析	105
6.2.4 故障检测方法分析	107
6.2.5 补偿措施分析	107
6.2.6 FMEA 的实施	107
6.3 危害性分析	108
6.3.1 风险优先数法	109
6.3.2 危害性矩阵法	110
6.3.3 危害性分析的实施	113
6.4 FMECA 结果	114
6.5 FMECA 应用示例	114
6.6 应用 FMECA 应注意的问题	115
习 题	116
<b>第 7 章 故障树分析</b>	
7.1 概 述	117
7.2 建造故障树	117
7.2.1 基本概念及符号	117
7.2.2 故障树建造的步骤和注意事项	120
7.3 故障树的定性分析	121
7.3.1 基本概念	121
7.3.2 求最小割集的方法	122
7.3.3 最小割集的定性分析	124
7.4 故障树的定量计算	125
7.4.1 故障树的数学描述	125
7.4.2 单调关联系统	127
7.4.3 通过底事件发生的概率直接求顶事件发生的概率	128
7.4.4 通过最小割集求顶事件发生的概率	129

7.4.5	故障树的简化 .....	133
7.4.6	对偶树和成功树 .....	135
7.4.7	重要度分析 .....	136
7.4.8	故障树分析中应注意的问题 .....	138
7.5	滑油告警系统 FTA 示例 .....	139
	习 题 .....	144
<b>第 8 章 事件树分析</b>		
8.1	概 述 .....	146
8.2	事件树建造 .....	147
8.2.1	连续运转部件组成的系统事件树 .....	147
8.2.2	有备用或安全装置的系统事件树 .....	148
8.2.3	考虑人为因素的事件树 .....	149
8.3	事件树的定量分析 .....	149
8.3.1	确定初因事件与后续事件的发生概率 .....	149
8.3.2	计算后果事件的发生概率 .....	150
8.3.3	后果事件的风险评估 .....	153
8.4	事件树分析与故障树分析方法的综合应用 .....	154
8.4.1	综合应用的原理 .....	154
8.4.2	综合应用的实例 .....	154
	习 题 .....	157
<b>第 9 章 电子产品可靠性设计分析方法</b>		
9.1	概 述 .....	158
9.2	电子元器件的选用 .....	158
9.2.1	电子元器件的质量等级 .....	159
9.2.2	电子元器件的选择 .....	163
9.2.3	电子元器件的正确使用 .....	165
9.3	降额设计 .....	166
9.3.1	降额基准与降额等级 .....	167
9.3.2	降额准则示例 .....	167
9.4	容差分析 .....	169
9.4.1	容差分析的重要性 .....	169
9.4.2	容差分析方法 .....	169
9.4.3	最坏情况分析法 .....	170
9.4.4	蒙特卡罗分析 .....	173
9.5	潜在通路分析 .....	176
9.5.1	潜在通路的产生原因及主要表现形式 .....	176
9.5.2	潜在通路分析的基本步骤 .....	176



9.5.3	潜在通路分析示例	178
9.5.4	潜在通路分析的特点	180
9.6	热设计热分析技术	180
9.6.1	热设计方法	180
9.6.2	热分析手段	183
9.7	电磁兼容设计	185
9.7.1	电磁干扰源	185
9.7.2	电磁干扰传播途径	186
9.7.3	抗电磁干扰的措施	187
9.8	耐环境设计技术	189
9.8.1	环境条件及其对产品可靠性的影响	189
9.8.2	环境保护原则	192
9.8.3	耐环境设计措施	193
	习 题	194

## 第 10 章 机械产品可靠性设计分析方法

10.1	概 述	196
10.1.1	机械产品可靠性的特点	196
10.1.2	机械产品可靠性工作的特点	196
10.2	应力和强度的随机特性	198
10.2.1	应力和强度随机性的影响因素	198
10.2.2	确定应力和强度随机性分布的方法	198
10.3	干涉理论及可靠度计算	199
10.3.1	应力-强度干涉模型	199
10.3.2	可靠度的计算方法	201
10.3.3	一次二阶矩法	202
10.4	静强度概率设计方法	207
10.5	疲劳与断裂可靠性分析设计方法	208
10.5.1	疲劳可靠性设计分析	208
10.5.2	断裂及其可靠性设计	214
10.6	磨损和腐蚀的概率计算	216
10.6.1	磨损的基本概念	216
10.6.2	给定寿命下的耐磨可靠度计算	217
10.6.3	给定耐磨可靠度时可靠寿命的计算	218
10.6.4	腐蚀的概率计算	218
10.7	机构功能可靠性	219
10.7.1	机构的基本概念	219
10.7.2	机构功能可靠性分析的基本方法	219
	习 题	221

## 第 11 章 其他可靠性设计分析方法

11.1 概 述	222
11.2 可靠性设计准则	222
11.2.1 可靠性设计准则的结构和内涵	223
11.2.2 可靠性设计准则的制定程序	225
11.2.3 可靠性设计准则的贯彻实施	226
11.3 余度设计与容错技术	227
11.3.1 余度设计	227
11.3.2 余度设计程序	231
11.3.3 容错技术	233
11.4 软件可靠性	237
11.4.1 基本概念	237
11.4.2 软件可靠性特征	238
11.4.3 软件可靠性设计分析方法	239
11.5 健壮设计	248
11.5.1 质量功能展开	249
11.5.2 三次设计	252
11.6 功能可靠性分析	255
11.6.1 功能可靠性分析的发展概况	255
11.6.2 存在的问题	257
11.6.3 发展趋势	258
习 题	258

## 附 录

A 大型网络系统最小路集的计算机算法	259
B 歼六飞机主起落架故障树分析	262

## 参考文献

# 第1章 引言

## 1.1 现代质量观念与设计思想转变

现代质量观念认为,质量包含了系统的性能特性、专门特性、经济性、时间性、适应性等方面,是系统满足使用要求的特性总和(如图 1-1 所示)。系统的性能特性,可以用性能指标来描述,如发动机的输出功率;系统的专门特性,描述了系统保持规定性能指标的能力,包括系统的可靠性、维修性、保障性、安全性、测试性等,如发动机能连续工作若干小时并保证在此期间输出功率不低于规定的值;经济性即系统的寿命周期费用,指在系统的整个寿命期内,为获取并维持系统的运营所花费的总费用;时间性指的是系统的按期交付,它也影响系统的寿命周期费用(费用的时间性);适应性反映了系统满足用户需求、符合市场需要的能力。

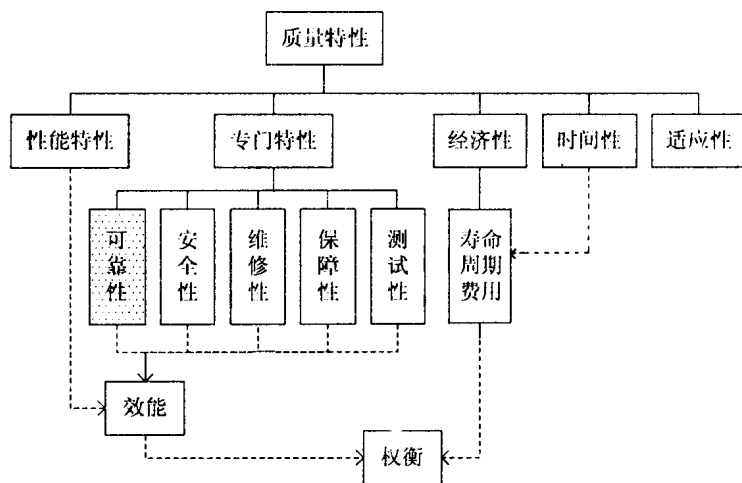


图 1-1 性能特性、专门特性及其权衡

随着现代工程系统的复杂化,系统的专门特性显得更加重要。例如:①工程系统日益庞大和复杂,带来了系统可靠性和安全性的下降,投资增大,研发周期加长,风险增加。②工程系统的应用环境更加复杂和恶劣。从陆地、海洋到天空、太空,工程系统的使用环境不断地扩展和更加严酷。严酷的环境对系统高可靠性、高安全性等综合特性的实现提出了挑战。③系统要求的持续无故障任务时间加长。如太空探测器的长时间无故障飞行要求、通信网络的关键任务不停机要求等。迫使工程系统必须具有良好的可靠性、维修性等专门特性。④系统的专门特性与使用者的生命安全直接相关。如核能系统、载人航空航天器、高速列车等系统的可靠与安全是生命安全的基本保证,受到了强烈的关注。⑤市场竞争的影响。“性能优良、功能齐全”并不是用户选择产品时考虑的惟一因素,产品是否可靠、是否好修、使用维护保养费用多少、寿命多长都对用户的选择产生重要影响。对于研究开发者来说,总是希望投资小、周期短、研发一次成功,这也与系统的专门特性密切相关。

从主要追求系统的性能特性,到兼顾、重视系统的专门特性,以及在有限的资源(费用、时间)的约束下实现系统的性能特性与专门特性的优化平衡,体现了现代系统设计思想的转变,带来了观念的更新,对系统设计实现的影响是巨大的。

系统的性能特性、专门特性及其优化权衡关系如图 1-1 所示。从图中可以看出,系统优化权衡的核心是效能、寿命周期费用两个概念之间的权衡。下面先简要介绍这两个概念。

(1) 系统效能就是系统在规定的条件下满足给定定量特征和服务要求的能力。它是系统可用性、可信性及固有能力的综合反映,一般可以表示为:

$$E = A \cdot D \cdot C \quad (1-1)$$

式中:  $E$ ——系统效能(Effectiveness);

$A$ ——可用性(Availability);

$D$ ——可信性(Dependability);

$C$ ——固有能(Capability)。

可用性( $A$ )表示战备完好,即系统在任一随机时刻需要开始执行任务时,处于工作或可使用状态的程,亦即系统“开则能动”的能力。它是系统可靠性和维修性(含保障性、测试性等)的函数,即  $A = f(R, M)$ 。

可信性( $D$ )表示任务成功,是指系统在任务开始时可用性给定的情况下,在规定的任务剖面<sup>①</sup>中的任一随机时刻,能够使用且能完成规定功能的能力,即系统“动则成功”的能力。它是系统可靠性和维修性(含保障性、测试性等)的函数。

固有能( $C$ )是系统在给定的内在条件下,满足给定的定量特性要求的自身能力,如飞行速度、航程、杀伤力等。

效能( $E$ )和可靠性( $R$ )、维修性( $M$ )之间的关系如图 1-2 所示。从图中可以看出,可用性( $A$ )、可信性( $D$ )均为可靠性( $R$ )、维修性( $M$ )的函数,因此,效能( $E$ )为可靠性( $R$ )、维修性( $M$ )、固有能( $C$ )的函数,即  $E = f(R, M, C)$ 。

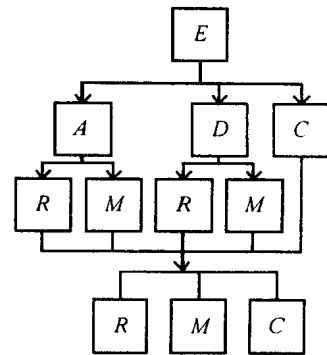


图 1-2 效能与可靠性、维修性的关系

(2) 系统的寿命周期费用(Life Cycle Costs, 以下简称 LCC),是指在系统的整个寿命周期内,为获取并维持系统的运营(包括处置)所花费的总费用。它包括硬件、软件的研制费、生产费、后勤保障费用,以及在研制、采办、使用、技术保障和处置过程中所需的各种人员费用。不同的系统,其寿命周期费用构成不完全相同,各构成成分间的比例关系也不完全一样。

图 1-3 给出了寿命周期费用的主要构成因素,并示意地表示了它们在寿命周期内的分布情况。

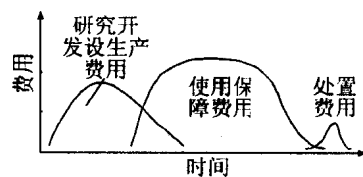


图 1-3 系统寿命周期费用构成示意图

实践表明,在寿命周期费用中,使用费用(使用维修与保障费用)所占的比例越来越大,美国军用飞机单架成本增长和装备使用费用的增长情况如表 1-1、表 1-2 所列。

① 任务剖面:产品在完成规定任务这段时间内所经历的时间和环境的时序描述。详见 2.1.2 节。

表 1-1 美国军用飞机单架成本增长

年 代	1945	1950	1960	1970	1972—1975	1975—1982	1983—2003
型 号	P-47	F-86	F-105	F-4E	F-15	F-18A	F-22
单架成本增长/万美元	10	40	300	360	1 300	3 270	7 200

表 1-2 美国空军装备使用费用的增长

年 代	1962	1968	1977
使用费用/采购费用	4/6	5/5	6/4

(3) 现代系统设计思想的转变主要体现在对三个概念的延伸上:①性能向效能的延伸,体现了从性能特性向系统全面特性(性能特性+专门特性)的延伸;②采购费用向寿命周期费用的延伸,体现了对系统经济性的考虑更加全面完善;③权衡对象的延伸,从“花最少的钱实现性能最好的系统”延伸到“以最小的寿命周期费用实现效能最好的系统”。上述三个概念上的延伸,体现了系统设计目标的根本性变化,它所带来的影响是全局性的。

现代系统设计思想与传统设计思想的简单比较如表 1-3 所列。

表 1-3 现代系统设计思想与传统设计思想的比较

	现代系统设计思想	传统设计思想
产品定位	市场牵引,用户需求	工程师及领导者的意见
系统综合方式	一开始就进行系统性能特性与专门特性的综合	重视性能,忽视系统综合
工作量投入	研制初期投入较多,研制后期投入较少,所需总投入较少	研制初期投入较少,研制后期投入较多,所需总投入较多
更改次数	研制初期更改较多,研制后期更改较少,更改代价较小	研制初期更改较少,研制后期更改较多,会出现局部甚至全局重新设计,更改代价较大
设计目标及评价标准	满足用户需求,质量稳定性好	满足验收标准,质量波动性大
工作姿态	主动寻找故障、预防故障发生	被动等待、解决故障问题
经济社会效益	低成本、高质量、适销对路	很难全部满足用户需求,可能会产生合格的“废品”

本书所讲述的是系统可靠性设计分析技术,它是系统可靠性工程(如图 1-1 中阴影方框所示)的关键,是系统维修性、保障性、安全性、测试性工程技术的基础,也是转变设计观念、进行系统效能与寿命周期费用优化权衡所必须掌握的技术内容。

## 1.2 系统可靠性设计分析流程

本书所讲述的各种可靠性设计分析技术都有着较强的工程应用背景,各种技术方法交叉配合使用,贯穿了系统研制的全过程。针对系统研制的特点,系统地规划和恰当地应用各种设计分析方法,才能使研制出的系统具有较高的可靠性水平。

大型工程系统(如军事装备等)的研制过程可分为(战术)技术指标论证、方案论证及确认、工程研制(包括初步设计与详细设计阶段)、设计定型、生产定型五个阶段。在分析系统各研制阶段的主要研制任务的基础上,根据目前工程实际中开展可靠性设计分析工作的经验可知:各种可靠性设计分析工作(如可靠性要求制定,可靠性建模、预计分配,故障模式影响及危害性分析(FMEA/CA)和故障树分析(FTA)等)主要集中在指标论证、方案论证和工程研制三个阶段。因此,本书对设计定型、生产定型阶段的可靠性设计分析技术未作专门论述。

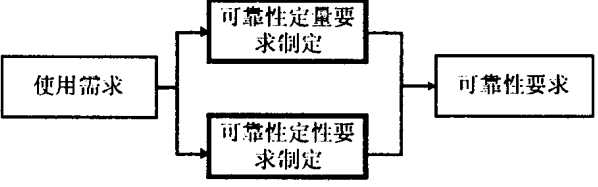
由于各种可靠性设计分析工作开展的阶段不完全相同,同一项工作在不同的阶段开展的深度也不同,而且,不少工作之间存在着前后的依赖性。因此,要在系统研制工作中有效地组织开展可靠性设计分析工作,达到高效、全面地提高系统的可靠性水平的目标,必须对各研制阶段中可靠性设计分析工作的关系和流程有清楚的认识。

本书首先讲述了系统研制中的可靠性设计分析流程,并把它作为选择与阐述各种可靠性设计分析方法的线索。

下面以武器系统为例,对各研制阶段的系统可靠性设计分析流程简述如下,图中粗线方框表示一种具体的可靠性设计分析工作和方法。

可靠性设计分析方法在各研制阶段的适用性汇总如表 1-4 所列。

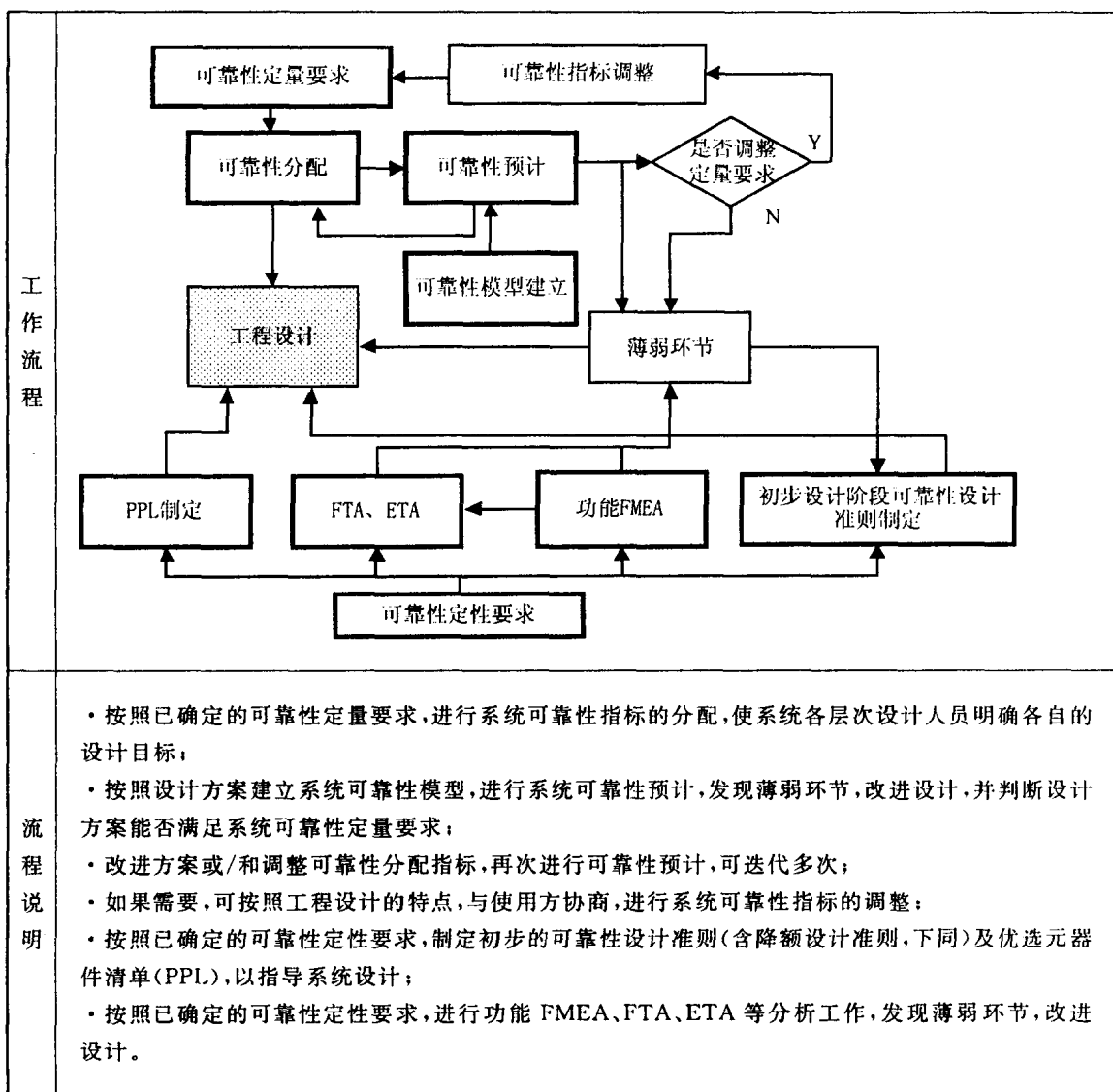
#### (1) 战术技术指标论证阶段

研制任务	进行战术技术指标、总体技术方案的论证及研制经费、保障条件、研制周期的预测,形成《武器系统研制总要求》。论证工作由使用部门组织实施。
工作流程	 <pre> graph LR     A[使用需求] --&gt; B[可靠性定量要求制定]     A --&gt; C[可靠性定性要求制定]     B --&gt; D[可靠性要求]     C --&gt; D     </pre>
流程说明	由使用方根据武器系统的使用需求和特征,制定可靠性定性要求与定量要求,并把它们作为系统战术技术指标的一部分。

#### (2) 方案论证及确认阶段

研制任务	<ul style="list-style-type: none"> <li>• 依据战术技术要求,进行装备总体及系统方案的优选及关键技术攻关,并确定总体技术方案;</li> <li>• 根据总体技术方案,进行系统方案设计、总体协调和系统布局,确定系统方案和主要部件的结构形式;</li> <li>• 进行模型样机或原理样机研制与试验。</li> </ul>
------	---

续

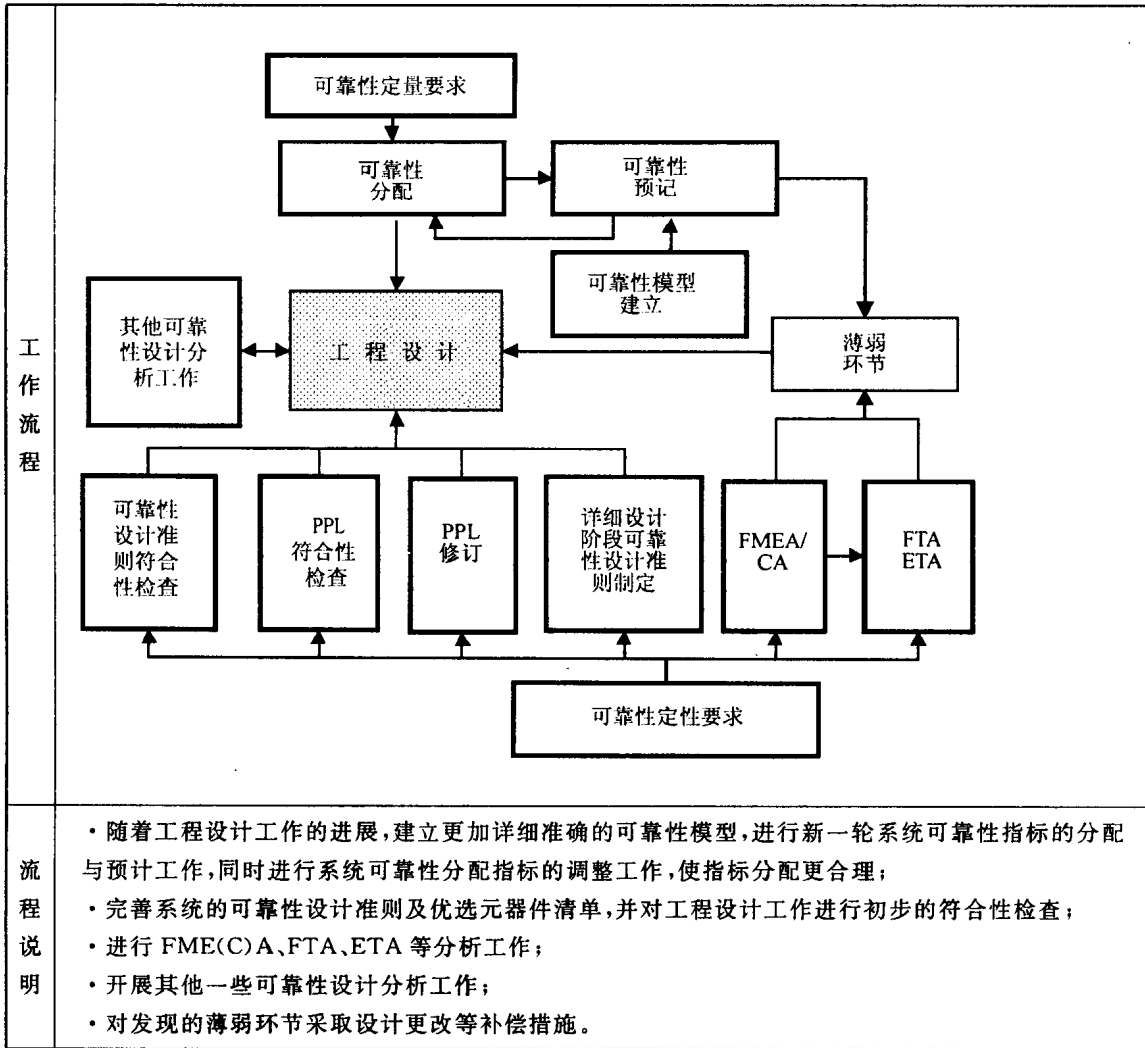


(3) 工程研制阶段

① 初步设计阶段

研 制 任 务	<ul style="list-style-type: none"> <li>• 细化方案论证阶段确定的方案;</li> <li>• 各系统的功能、性能分析计算;</li> <li>• 从系统到设备层次,产品的原理设计、组成和结构设计。</li> </ul>
------------------	---

续



② 详细设计阶段

研 制 任 务	<ul style="list-style-type: none"> <li>• 各层次产品全部详细图纸的设计;</li> <li>• 功能、性能的详细设计、计算;</li> <li>• 技术文件编制。</li> </ul>
------------------	--

① 手稿



续

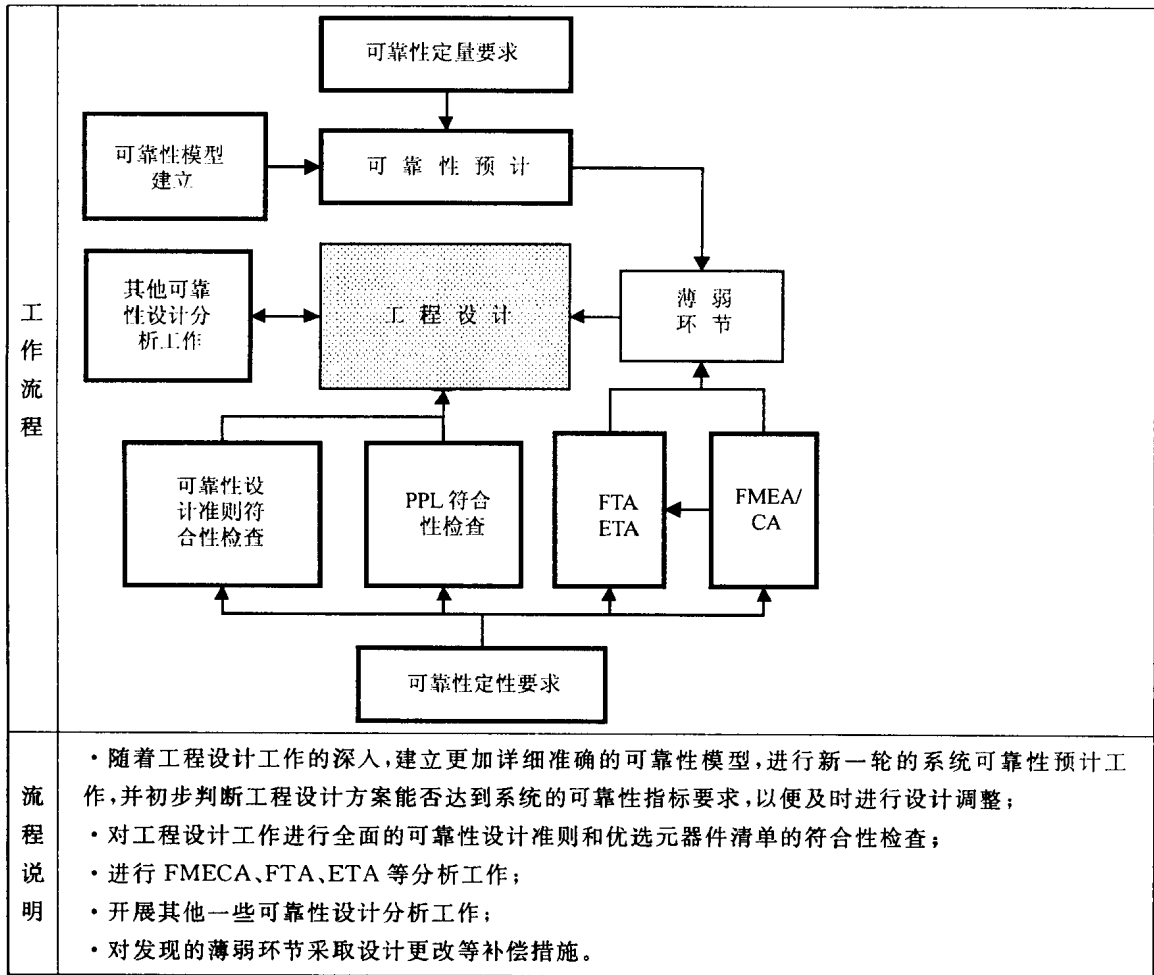


表 1-4 适用于不同研制阶段的各种可靠性设计分析方法

设计分析方法	研制阶段			
	指标论证	方案论证	工程研制	
			初步设计	详细设计
可靠性定性定量要求制定	√	√		
可靠性模型建立		√	√	√
可靠性分配		√	√	
可靠性预计		√	√	√
功能故障模式影响分析(功能 FMEA)		√		
硬件故障模式影响和危害性分析(硬件 FMEA/CA)			√	√
故障树分析(FTA)		△	√	√
事件树分析(ETA)		△	√	√
优选元器件清单(PPL)制定		√	√	