



航天发射场可靠性安全性 评估与分析技术

徐克俊 金星 郑永煌 编著



国防工业出版社

National Defense Industry Press

V55
1006



2007028713

V55
1006-1

总装部队军事训练“十五”统编教材

科研试验系列

航天发射场可靠性安全性 评估与分析技术

徐克俊 金星 郑永煌 编著



国防工业出版社

·北京·

2007028713

图书在版编目(CIP)数据

航天发射场可靠性安全性评估与分析技术/徐克俊,金星,郑永煌编著. —北京:国防工业出版社,2006.12
总装部队军事训练“十五”统编教材. 科研试验系列
ISBN 7-118-04928-X

I. 航... II. ①徐...②金...③郑... III. ①航天发射场-可靠性-教材②航天发射场-安全性-教材
IV. V551

中国版本图书馆 CIP 数据核字(2006)第 155683 号

※

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)

四季青印刷厂印刷

新华书店经售

*

开本 880×1230 1/32 印张 8 字数 225 千字

2006 年 12 月第 1 版第 1 次印刷 印数 1—3000 册 定价 22.00 元

(本书如有印装错误,我社负责调换)

国防书店: (010)68428422

发行邮购: (010)68414474

发行传真: (010)68411535

发行业务: (010)68472764

第三届总装备部军事训练教材 编辑工作委员会

主任委员	张建启			
副主任委员	曹保榆	夏长法	侯贺华	郭文敏
委 员	(按姓氏笔画排序)			
	于俊民	王宜标	王泽民	尤广志
	冯 章	朱双华	朱忠刚	刘树军
	刘瑞成	安敏建	李方洲	李治三
	肖力田	迟宝山	张忠华	张海东
	陈永光	胡利民	侯 鹰	姜世忠
	聂 皦	倪红星	徐 航	郭 勇
	黄伟强	彭华良	裴承新	潘贤伦
秘 书 长	聂 皦			
办公室主任	田 禾			
办公室副主任	石根柱	郝 刚		
办公室成员	李国华	李立法	郑晓娜	

第三届总装备部军事训练教材 导弹航天测试发射系统编委会

主任委员 李晓箭

副主任委员 徐克俊

委 员 (按姓氏笔画排序)

王泽民 刘卫东 张海联

陈新华 尚友虎 穆 山

秘 书 石根柱

序

军事训练教材是部队开展军事训练和培养高素质科研试验与管理人才的重要基础。“十五”期间是我军加速武器装备现代化建设的关键时期,随着科学技术不断发展,新武器、新装备大量投入部队使用,急需编写相应的配套教材,来满足部队军事训练和人才培养的需求。为此,总装司令部印发了《总装部队军事训练教材建设“十五”计划》,并组织部分专家、学者编著了这套总装部队军事训练“十五”统编教材。

编著这套总装部队军事训练“十五”统编教材是国防科研试验事业继往开来的大事,也是体现国防科研试验技术水平的一个重要标志。它以新时期军事战略方针为统揽,以军委和总装首长关于加强军事训练工作的一系列重要指示为指导,以《军事训练与考核大纲》、《继续教育科目指南》为依据,坚持科学性、前瞻性和实用性相结合,不断满足军事训练和人才培养对教材的需求,为圆满完成武器装备科研试验和管理保障任务提供了有力的技术支持。

“十五”统编教材共计69部,内容涉及科研试验、陆军装备科研订购、通用装备保障和试验后勤等4个系列的28个系统。这套教材既总结升华了武器装备科研试验和管理保障经验,又反映了国内外最新动态和发展方向,是对国防科研试验工程技术系列教材建设的进一步延续和扩展,是一批高质量的精品教材。其使用对象主要是部队具有大专以上学历的科技人员和管理干部,也可供院校有关专业师生使用或参考。

期望这套教材能够有益于部队高素质人才的培养,有益于武器装备科研试验和管理保障任务的完成,有益于国防科技事业的进步。

总装备部军事训练教材

编辑工作委员会

二〇〇五年十二月

前 言

航天工程是一项复杂的系统工程,涉及计算机、电子、机械、化工、冶金等各个工业领域,在任务的准备和实施过程中有可能出现难以预料的故障。因此,采用可靠性工程学和安全性工程学方法,可以确定系统的薄弱环节,采取相应措施,合理改进系统结构,控制故障的发生,达到最佳的安全可靠效果。使定性的、预防为主可靠性和安全性分析,发展成为能够预测故障发生的定性和定量的分析。

本书以航天发射场为研究对象,介绍具有单输入、多输出或多输入、多输出等特点和具有串并联混合结构的复杂系统的可靠性评估和安全性分析方法,阐述航天发射场典型系统可靠性评估和安全性分析的工程应用方法。

全书共分7章。第1章介绍可靠性和安全性的基本概念;第2章介绍航天发射场可靠性评估方法;第3章介绍航天发射场维修性和可用性分析方法;第4章介绍航天发射场安全性分析方法;第5章介绍航天发射场可靠性定量评估思路以及典型系统可靠性定量评估;第6章介绍航天发射场安全性定性分析思路以及典型系统安全性定性分析;第7章介绍航天发射场可靠性安全性评估系统。

本书编著过程中得到了总装备部司令部军训局和装备指挥技术学院、酒泉卫星发射中心各级领导及专家的指导与支持,在此表示衷心感谢!装备指挥技术学院陈景鹏副教授和酒泉卫星发射中心技术部二室王海锋工程师承担了辛苦的排版、校对和编辑工作,总装教材办石根柱同志在编著和出版中做了大量工作,在此一并表示感谢。

由于我们的水平有限,书中难免存在一些缺点和不足,请读者批评指正。

编著者

2006年6月

目 录

第1章 绪论	1
1.1 概述	1
1.2 可靠性的基本概念	1
1.2.1 寿命剖面与任务剖面	1
1.2.2 可靠性定义	2
1.2.3 基本可靠性指标	2
1.3 常用可靠性概率分布函数	5
1.3.1 指数分布	5
1.3.2 正态分布	6
1.3.3 对数正态分布	7
1.3.4 威布尔分布	8
1.3.5 β 分布	9
1.3.6 Γ 分布	10
1.3.7 负对数 Γ 分布	11
1.4 安全性的基本概念	13
1.4.1 安全性定义	13
1.4.2 危险严重性和危险可能性等级	13
1.4.3 危险风险评价指数	14
1.5 可靠性与安全性的关系	15
第2章 航天发射场可靠性评估方法	17
2.1 单元可靠性评估方法	17
2.1.1 成败型单元可靠性评定	17
2.1.2 指数型单元可靠性评定	19

2.1.3	正态分布的可靠度下限	20
2.1.4	非中心 t 分布与正态分布可靠度下限计算	21
2.2	典型系统可靠性评估方法	25
2.2.1	不同二项/指数单元构成的串联系统可靠性评定	25
2.2.2	不同分布单元构成的串联系统可靠性评定	28
2.2.3	不同二项与指数分布单元构成的并联系统可靠性 性下限	32
2.2.4	不同分布单元构成的并联系统可靠性评定	34
2.2.5	相同分布单元构成的 k/N 系统可靠性评定	34
2.3	由典型系统构成的复杂系统可靠性评定	36
2.4	复杂系统可靠性评估方法	38
2.4.1	概述	38
2.4.2	布尔逻辑和、逻辑积运算	38
2.4.3	复杂系统求最小路集和最小割集	41
2.4.4	复杂系统可靠度和部件敏感度计算	42
2.4.5	多工作状态复杂供配电系统分析方法	44
第3章	航天发射场维修性与可用性分析技术	50
3.1	维修性指标	50
3.1.1	维修度函数	50
3.1.2	维修概率密度函数	51
3.1.3	维修率函数	51
3.2	维修性模型中常用的分布函数	53
3.2.1	正态分布	53
3.2.2	对数正态分布	54
3.2.3	指数分布	56
3.3	马尔可夫过程模型分析可用性	57
3.3.1	单元的可用度	58
3.3.2	可修串联系统	61
3.3.3	可修相同分布并联系统	65
3.3.4	可修不同分布并联系统	68

3.3.5	r/n 可修系统	70
3.3.6	旁联可修系统	71
3.3.7	一般可修系统	74
3.3.8	应用举例	82
3.4	非指数分布单元可用性分析	90
3.4.1	可修单元的故障频率、修复频率和不可用度计算 ..	90
3.4.2	可修单元的故障频率、修复频率、可用度和不可用 度计算分析	91
3.5	单元可用度相互独立条件下计算系统可用度的近似方法	95
3.5.1	可修单元不可用度和可用度计算	96
3.5.2	可修系统不可用度和可用度计算	96
3.5.3	可用度的敏感性分析	98
3.5.4	可修系统故障频率和平均可用时间计算	99
3.5.5	应用举例	100
第4章	航天发射场安全性分析方法	108
4.1	安全性分析方法的选择	108
4.2	故障模式、影响及危害性分析(FMECA)方法	109
4.2.1	目的和作用	109
4.2.2	基本分析方法	109
4.2.3	基本分析程序	110
4.2.4	分析基本要求及 FMECA 报告	117
4.2.5	应用举例	118
4.3	故障树分析(FTA)方法	121
4.3.1	目的和作用	121
4.3.2	基本分析方法	121
4.3.3	故障树定性分析方法	123
4.3.4	故障树定量计算方法	126
4.3.5	底事件重要度计算	131
4.3.6	进行故障树分析时应注意的问题	132
4.3.7	应用实例	132

4.4	危险分析(HA)方法	138
4.4.1	目的和作用	138
4.4.2	基本分析方法	138
4.4.3	基本分析程序	143
4.4.4	危险分析报告要求	145
附录4.4A1	一般危险源清单	146
附录4.4A2	危险事件清单	149
4.5	潜在通路分析(SCA)方法	151
4.5.1	目的和作用	151
4.5.2	潜在通路的特点和表现形式	152
4.5.3	潜在通路分析方法的分析步骤	154
4.6	概率风险评估(PRA)方法	160
4.6.1	目的和作用	160
4.6.2	概率风险评估方法基本原理	160
4.6.3	概率风险评估实施步骤	165
4.7	软件安全性分析方法	166
4.7.1	目的和作用	166
4.7.2	软件安全性要求	166
4.7.3	系统安全性分析	167
4.7.4	软件安全性分析	168
4.7.5	软件安全性设计检查及检查单	170
第5章	航天发射场可靠性定量评估	175
5.1	航天发射场可靠性定义	175
5.1.1	设备固有可靠性	175
5.1.2	设备任务可靠性	175
5.1.3	设备固有可靠性与设备任务可靠性的关系	175
5.2	航天发射场可靠性数据分类及分布类型	176
5.2.1	可靠性数据分类	176
5.2.2	可靠性数据分布类型	176
5.3	航天发射场可靠性评估思路	177

5.3.1	可靠性定量评估思路	177
5.3.2	危害性分析	178
5.3.3	可靠性评估步骤	178
5.3.4	可靠性数据获取要求与选取方法	181
5.4	航天发射场典型系统可靠性评估	183
5.4.1	供配电系统可靠性评估	183
5.4.2	火箭推进剂加注系统可靠性评估	195
第6章	航天发射场安全性定性分析	202
6.1	安全性分析目的	202
6.1.1	安全性分析目的	202
6.1.2	安全性分析要求	202
6.2	安全性分析准则	203
6.2.1	不可接受	203
6.2.2	可接受	203
6.3	安全性分析方法	204
6.3.1	安全性分析内容	204
6.3.2	风险评估方法	205
6.4	关键系统安全性分析	205
6.4.1	加注系统安全性设计	206
6.4.2	加注系统安全性验证	207
6.4.3	加注系统安全性分析	208
6.4.4	加注系统主要问题统计分析	220
6.4.5	加注系统安全性评价结果	221
第7章	航天发射场可靠性安全性评估系统	222
7.1	评估系统的功能特点	222
7.1.1	评估系统功能	222
7.1.2	评估系统的特点	224
7.2	评估系统软件结构	225
7.3	评估系统应用实例	227
7.3.1	评估系统界面窗口	227
7.3.2	应用实例	230

附录 可靠性与安全性常用术语	234
参考文献	241

第1章 绪 论

1.1 概 述

“产品的可靠性是设计出来的,生产出来的,管理出来的”这一思想,越来越为人们所理解。航天发射场是一个复杂的系统,涉及机、电、液等各个专业,具有长期处于闲置维护保养阶段、任务期间使用时间较短的特点。因此,对于航天发射场这样的复杂系统,通过任务前的检测、检修发现设备存在的隐患和薄弱环节,在设计、工艺、生产、材料、元器件、管理、软件等方面,进行更改、更换、维修、调整等措施,提前消除隐患,可以提高设备可靠性。在任务实施过程中,通过管理措施、操作规程、技术安全检查、使用操作培训、专项质量评审、应急预案等质量控制措施,可以提高设备任务可靠性。根据航天发射场的特点,本书重点介绍了适用于航天发射场的可靠性评估方法、维修性与可用性分析方法、安全性分析方法,并介绍了航天发射场典型系统和设备的评估与分析过程。

1.2 可靠性的基本概念

1.2.1 寿命剖面与任务剖面

寿命剖面:指产品从制造到寿命终结或退出使用这段时间内所经历的全部事件和环境的时序描述。寿命剖面包含一个或多个任务剖面。通常把产品的寿命剖面分为后勤和使用两个阶段:后勤阶段包括采购、包装、运输、发送等内容;使用阶段包括运输、任务剖面、维修、报

废等内容。

任务剖面：指产品在规定任务这段时间内所经历的事件和环境的时序描述。一个产品完成不同任务时有多种任务剖面。

1.2.2 可靠性定义

可靠性：指产品在规定条件下和规定时间内，完成规定功能的能力。产品不能完成规定功能，称为故障（或失效）。可靠性一般用概率表示，也可以根据实际需要，用平均无故障工作时间或平均无故障里程表示。

不可靠性：指产品在规定条件下和规定时间内，不能完成规定功能的能力。

基本可靠性：指产品在规定条件下无故障的持续工作能力。是与寿命剖面相关的可取性，反映了产品对维修和后勤保障的要求。

任务可靠性：指产品在规定的任务剖面内完成规定功能的能力，是与任务剖面相关的可靠性。

1.2.3 基本可靠性指标

1. 可靠度和不可靠度

可靠度：是指产品在规定条件下和规定时间内，完成规定功能的概率。

产品寿命 T 是随机变量，可靠度 $R(t)$ 为

$$R(t) = P(T > t)$$

式中 t ——规定时间， t 时刻可靠度是指产品在 $[0, t]$ 内完成规定功能的概率。

不可靠度 $F(t)$ 为

$$F(t) = P(T \leq t)$$

即 t 时刻不可靠度，表示产品在 $[0, t]$ 内发生故障的概率。显然

$$R(t) + F(t) = 1$$

对于有限样本，设产品总数目为 N_0 ，经过 t 时间故障数目为 $r(t)$ ，则可靠度和不可靠度的估计值为

$$R(t) = \frac{N_0 - r(t)}{N_0}$$

$$F(t) = \frac{r(t)}{N_0}$$

随着时间增大,可靠度由开始时 $R(0) = 1$ 逐渐降低 ($R(\infty) = 0$), 不可靠度由开始时 $F(0) = 0$ 逐渐增加 ($F(\infty) = 1$)。

2. 故障概率密度函数

故障概率密度函数 $f(t)$ 是不可靠度的导数,

$$f(t) = \frac{dF(t)}{dt}$$

对于有限样本,设产品总数目为 N_0 ,经过 t 时间故障数目为 $r(t)$,经过 $t + \Delta t$ 时间故障数目为 $r(t + \Delta t)$,则故障概率密度函数估计值为

$$f(t) = \frac{r(t + \Delta t) - r(t)}{N_0 \Delta t}$$

故障概率密度函数的物理意义是:任意时刻 t ,全部产品在单位时间内发生故障的概率。

3. 故障率

故障率:是指任意时刻 t ,尚未发生故障产品,在单位时间内发生故障的概率。

对于有限样本,设产品总数目为 N_0 ,经过 t 时间故障数目为 $r(t)$,经过 $t + \Delta t$ 时间故障数目为 $r(t + \Delta t)$,则故障率估计值为

$$\lambda(t) = \frac{r(t + \Delta t) - r(t)}{[N_0 - r(t)] \Delta t}$$

故障率 $\lambda(t)$ 的物理意义是:任意时刻 t ,尚未发生故障的产品在单位时间内发生故障的概率。

当考察的产品总数目足够多 $N_0 \rightarrow \infty$,考察时间足够短 $\Delta t \rightarrow 0$,有

$$\lambda(t) = \lim_{\substack{\Delta t \rightarrow 0 \\ N_0 \rightarrow \infty}} \frac{\frac{r(t + \Delta t) - r(t)}{N_0 \Delta t}}{\frac{N_0 - r(t)}{N_0}} = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{R(t)}$$

4. 平均寿命

平均寿命是寿命的平均值。对于不可修复的产品,指产品失效前工作时间的平均值,通常记为 MTTF (Mean Time To Failure)。对于可修复产品,指故障间隔时间的平均值,记为 MTBF (Mean Time Between Failure)。

1) 平均失效前工作时间 (MTTF)

设 N_0 个不可修复产品在相同条件下进行试验,测得寿命数据为 $t_1, t_2, \dots, t_{N_0}$, 则其平均失效前工作时间的估计值为

$$MTTF = \frac{1}{N_0} \sum_{i=1}^{N_0} t_i$$

当寿命是连续型随机变量时,平均失效前工作时间为

$$\begin{aligned} MTTF &= \int_0^{\infty} t f(t) dt = \int_0^{\infty} t \left[-\frac{dR(t)}{dt} \right] dt \\ &= -[t \cdot R(t)] \Big|_0^{\infty} + \int_0^{\infty} R(t) dt = \int_0^{\infty} R(t) dt \end{aligned}$$

2) 平均故障间隔时间 (MTBF)

设一个可修产品在使用期间,发生了 N_0 次故障,每次故障修复后,又继续投入工作,工作时间分别为 $t_1, t_2, \dots, t_{N_0}$, 则其平均故障间隔时间为

$$MTBF = \frac{1}{N_0} \sum_{i=1}^{N_0} t_i$$

产品修复后和崭新的产品没有任何区别,称为完全修复。对于完全修复的产品,每次修复后继续工作时,与新产品投入使用完全一样,所以寿命是连续型随机变量时,平均故障间隔时间 (MTBF) 可表示为

$$MTBF = \int_0^{\infty} R(t) dt$$

5. 常用可靠性指标之间的关系

可靠度、不可靠度、故障概率密度和故障率中,只要知道其中一个指标,就可以确定另外三个指标,从而也可确定平均寿命指标。

常用可靠性指标之间的关系,如表 1-1 所示。