

空间系统安全设计

Safety Design for Space Systems

(美) 马斯格雷夫 (Gary Eugene Musgrave)

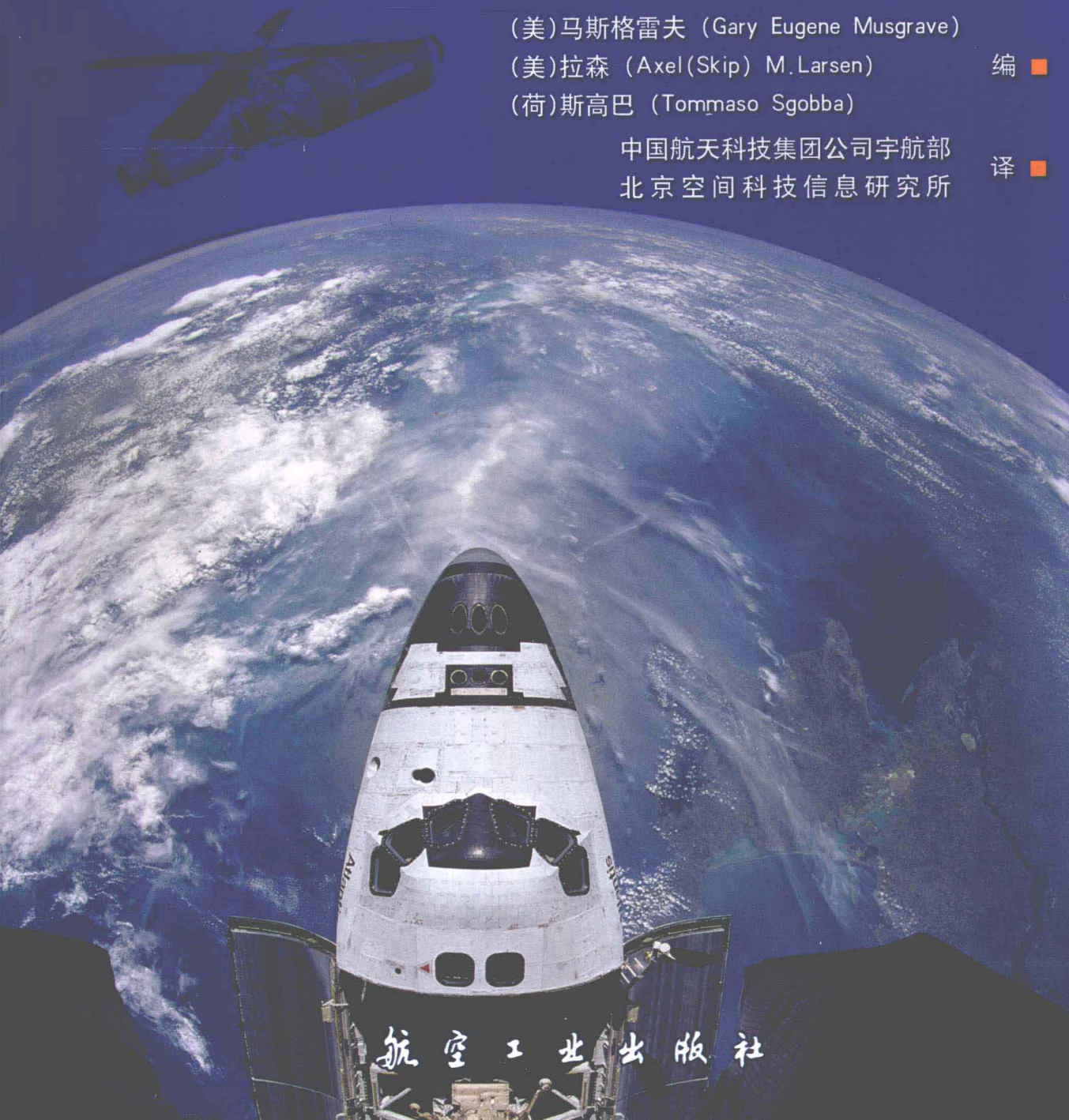
(美) 拉森 (Axel (Skip) M. Larsen)

(荷) 斯高巴 (Tommaso Sgobba)

编 ■

中国航天科技集团公司宇航部
北京空间科技信息研究所

译 ■



航空工业出版社

空间系统安全设计

(美) 马斯格雷夫 (Gary Eugene Musgrave)

(美) 拉森 (Axel (Skip) M. Larsen)

(荷) 斯高巴 (Tommaso Sgobba)

编

中国航天科技集团公司宇航部

北京空间科技信息研究所

译

航空工业出版社

北 京

内 容 提 要

自人类从事载人航天活动以来,为确保任务成功和航天员生命安全,载人航天系统的安全性成为一个极其关键和敏感的问题。空间环境、空间系统本身以及航天员操作等都存在诸多不确定因素,这些因素很可能导致事故或灾难发生。

美国国家航空航天局(NASA)在数十年载人航天活动中获得了成功的经验,也发生过惨痛的教训。这些经验教训促使NASA认真审视其安全文化,研究制定和完善空间系统的安全性要求,加强空间系统的安全设计。

本书共计29章,较为系统、全面地阐述了人类从事载人航天活动时所面临的安全问题,介绍了空间系统安全性的考虑因素和设计方法,汇集了国外近90位载人航天专家的智慧 and 心血。本书不仅可供航天科研人员参考,亦可供载人航天工程类大学本科学生或研究生使用。

图书在版编目(CIP)数据

空间系统安全设计/(美)马斯格雷夫
(Musgrave, G. E.), (美)拉森(Larsen, A. M.), (荷)
斯高巴(Sgobba, T.)编;中国航天科技集团公司宇航部
, 北京空间科技信息研究所译. --北京:航空工业出版社, 2011.8

ISBN 978-7-80243-805-7

I. ①空… II. ①马… ②拉… ③斯… ④中… ⑤北
… III. ①航天安全-安全设计 IV. ①V528

中国版本图书馆CIP数据核字(2011)第152521号

This edition of *Safety Design for Space Systems* by Gary Musgrave Ph. D, Axel Larsen, Tommaso Sgobba is published by arrangement with ELSEVIER LIMITED of The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK
Safety Desing for Space Systems 一书作者为 Gary Musgrave Ph. D, Axel Larsen, Tommaso Sgobba, 由爱思唯尔有限公司出版。

北京市版权局著作合同登记

图字:01-2011-1025号

空间系统安全设计 Kongjian Xitong Anquan Sheji

航空工业出版社出版发行

(北京市安定门外小关东里14号 100029)

发行部电话:010-64815615 010-64978486

北京地质印刷厂印刷

全国各地新华书店经售

2011年8月第1版

2011年8月第1次印刷

开本:787×1092 1/16

印张:43.25

字数:1104千字

印数:1—2000

定价:180.00元

译 序

自人类从事空间活动以来，特别是在载人航天活动中，空间系统的安全运行和操作成为一个极其关键和敏感的问题。空间的极端环境、空间系统本身以及人员操作等都存在诸多不确定因素，例如，辐射、噪声、碎片、有害材料、火灾等，这些因素很可能导致系统故障、任务失败，甚至人员伤亡。

国外在数十年的空间活动中获得了许多成功的经验，也发生过惨痛的教训。这些经验教训促使他们高度重视安全文化，研究制定和完善空间系统的安全要求，加强空间系统的安全设计。国外经验表明，必须运用科学、管理和系统工程的方法来分析、识别系统中不安全的因素，采取相应措施以消除、减少或控制潜在的危險，把安全性设计到空间系统的软硬件中去。

本书较为全面地阐述了空间活动中所面临的系统、人员、操作等安全问题，介绍了空间系统安全性的考虑因素和设计方法，对我国空间系统——尤其是载人航天系统的安全设计具有显著的参考意义。本书不仅可供航天科研人员参考，亦可供相关专业大学本科学士或研究生使用。为了方便读者使用，我们组织了部分科研人员对本书进行翻译。

在本书的翻译过程中，赵小津、原民辉对全书的翻译工作进行了统筹，王卫东、童旭东、杨之浩、于森等参加了全书审核，徐映霞、梁巍、李志阳、朱鲁青、张扬眉、刘豪、夏禹、张蕊、张鑫伟、龚燃、李铁骊、朱贵伟、成振龙、薛培元、杨倩、张杰、赵立军、栾文博、张志国、邱亮、周凯、唐军刚、陈塞崎、杜刚等参加了全书翻译，朱毅麟、王景泉、唐伯昶、张柏楠、徐映霞、田莉、范崑娜、刘志刚等参加了全书校对。

感谢中国航天科技集团公司宇航部、中国空间技术研究院、北京空间科技信息研究所、中航出版传媒有限责任公司（航空工业出版社）等单位在本书翻译和出版过程中给予的大力支持。

由于时间仓促及译者水平有限，本书的内容难免有错误和疏漏之处，恳请广大读者批评指正。

译者

2011 年 8 月

前 言

《空间系统安全设计》是近 90 位作者历时近 3 年撰写、编辑、校对及提供技术支持完成的劳动成果。本书是全球同类书中的唯一教材。书中对空间安全技术学科进行了详细考察，这些内容除了在少数工科院校外，通常不作为课程讲述。本书全体编者的共同认识是，安全只能由工程师在设计航天器及系统工作中才能了解，这一实际情况必须加以改变。刚参加工作的工程技术人员在工作中也应能够熟悉设计中必须满足的条件，以确保航天器、系统、航天员及相关操作的安全。

本书的编者及支持者都深切期望教材能够被各项学术计划、航天机构和商业航天企业广泛应用。本书可供工科本科高年级选修课或硕士生使用，是为其介绍有关安全原则和流程的较好入门书。

《空间系统安全设计》全体编者衷心感谢乔治·华盛顿大学的约瑟夫·佩尔顿（Joseph Pelton）教授构思了这一项目并安排本书出版；感谢空间安全领域的 78 位专家牺牲自己的宝贵时间撰写各自负责的内容；感谢助理编辑韦恩·斯托弗（Wayne Stauffer）负责本书的索引编排、互校，以及获得本书中所有受版权保护的图表的重印许可工作；感谢我的妻子克里斯蒂安·C. 马斯格雷夫（Kristine C. Musgrave），是她帮助我完成了繁琐的校对工作；此外还要对所有参与本书审查和批准的其他人员表示感谢。

有人曾问我这篇引言是技术性的还是抒情性的，很显然是后者。这是我从国家航空航天局（NASA）退休前从事的最后一项重要工作，是值得投入的且具有挑战性的工作。我想在引言结束前讲述一个故事来说明安全在工程工作中的重要性。我喜欢烹饪，很喜欢某个电视节目中出现过的一位厨师，这位已故的厨师因善于做家乡的 Cajun 菜系而闻名。几年前他说到，就他每天的工作来说，他就是一名安全工程师。他说他对安全的专注是显而易见的，因为他总是系着腰带和背带，这样就可以使自己在发生灾难性事件时免遭伤害。

马斯格雷夫 博士

(Gary Eugene Musgrave, Ph. D.)

序 言

在《设计是人的本性》(To Engineer Is Human)一书中,作者亨利·波卓斯基说,“谁也不想通过犯错来学习,但我们从成功中学不到超越现状的知识”。他的这一观点指出了航天系统安全工程师面临的机遇和挑战。那么,工程师究竟应如何将从失败中获得教训,并将其应用到未来的航天系统设计中呢?

本书汇集了航天安全领域众多卓越见解,内容包括航天头 50 年已被证明可以作为专业基础的原则、技术、方法、流程及标准等论述,本书的作者都是当今代表各航天大国水平的卓有成就的实践者和公认的领导者。他们论述的专题范围广泛,包括无人及载人航天系统。他们论述地球轨道及深空环境,还论述航天器在地面及飞行中的运行风险。他们介绍了设计小组系统安全成员在系统设计、研发和试验中采用的最新方法和技术,以及安全集成小组为整个系统所采用的综合风险方法。

如果要在本书中寻求一个主题,该主题则非常接近序言开始时波卓斯基语录表达的理念。目前的许多安全工程工具和技术模式固步自封,流程不够完善,因此造成了许多事故或任务失败。系统安全领域存在一个众所周知的问题,即事故调查委员会在调查报告中几乎总有一章专门讨论安全小组未能防止事故发生的失职。很明显,防止事故人人有责,但通常情况下,安全负责部门必须全力以赴执行参与、分析、预测的任务及防止再次失职。本书旨在明确哪些是进行中的流程改善的重点。利用本书中的知识去了解你的业务,更好地理解你的前任和同行在过去多年中获取的经验和教训。即使你从来没有经历过重大事故,也不应掉以轻心,应从你所经历的每一次幸运事件和高概率风险中吸取经验教训来持续改进你的业务和工具。学习永无止境,这也将是本书今后修订时的基础。

Bryan O'Connor

NASA 总部安全与任务保障办公室主任

目 录

第 1 章 空间安全概论	(1)
1.1 NASA 与安全	(1)
1.2 安全与风险	(2)
1.3 管理安全与风险	(2)
1.4 关于本书	(3)
参考文献	(4)
第 2 章 空间环境：自然的和诱导的	(5)
2.1 大气层	(5)
2.1.1 组成	(5)
2.1.2 原子氧	(9)
2.1.3 电离层	(11)
2.2 轨道碎片与流星体	(13)
2.2.1 轨道碎片	(13)
2.2.2 流星体	(19)
2.3 微重力	(22)
2.3.1 微重力定义	(22)
2.3.2 实现方法	(24)
2.3.3 对生物过程和航天员健康的影响	(28)
2.3.4 月球及行星航天的独特方面	(29)
推荐读物	(29)
2.4 声学	(31)
2.4.1 声学安全问题	(31)
2.4.2 声学要求	(31)
2.4.3 一致性与验证	(36)
2.4.4 结论和建议	(37)
推荐读物	(37)
2.5 辐射	(38)
2.5.1 电离辐射	(38)
2.5.2 射频辐射	(48)
推荐读物	(51)
2.6 自然及诱导热环境	(52)
2.6.1 热环境概论	(52)

2.6.2	航天器传热的考虑因素	(52)
2.6.3	自然热环境	(53)
2.6.4	诱导热环境	(57)
2.6.5	月球及行星环境的其他考虑因素	(62)
2.7	综合环境影响	(62)
2.7.1	环境影响概述	(62)
2.7.2	综合环境	(63)
2.7.3	综合影响	(63)
2.7.4	空间仿真地面试验	(66)
	参考文献	(67)
第3章	生物航天学概述	(82)
3.1	空间生理学	(82)
3.1.1	肌肉系统	(82)
3.1.2	骨骼系统	(83)
3.1.3	心肺系统	(84)
3.1.4	神经前庭系统	(85)
3.1.5	辐射	(86)
3.1.6	营养	(86)
3.1.7	免疫系统	(87)
3.1.8	出舱活动	(87)
3.2	短期及长期飞行任务影响	(88)
3.2.1	肌肉系统	(88)
3.2.2	骨骼系统	(89)
3.2.3	心血管及呼吸系统	(90)
3.2.4	神经系统	(90)
3.2.5	辐射	(91)
3.2.6	营养	(92)
3.2.7	免疫系统	(92)
3.2.8	出舱活动	(93)
3.3	健康保持	(93)
3.3.1	飞行前准备	(93)
3.3.2	飞行途中的措施	(95)
3.3.3	飞行中的医疗监测	(102)
3.3.4	飞行后恢复	(104)
3.4	航天员生存	(105)
3.4.1	航天飞行中的健康威胁概述	(105)
3.4.2	早期工作	(106)
3.4.3	航天员在发射台、发射时及上升期间的生存	(106)

3.4.4 在轨安全避险和航天员转移	(110)
3.4.5 再入、着陆和着陆后	(110)
3.5 结论	(112)
参考文献	(112)
第4章 航天安全性的基本原则	(123)
4.1 事故原因	(123)
4.2 基本原则和方法	(124)
4.2.1 危险消除和限制	(124)
4.2.2 屏蔽和互锁装置	(125)
4.2.3 故障安全性设计	(125)
4.2.4 故障与风险最小化	(126)
4.2.5 监测、恢复与规避	(127)
4.2.6 航天员生存系统	(127)
4.3 安全评审流程	(127)
4.3.1 安全性要求	(128)
4.3.2 安全小组	(128)
4.3.3 安全评审	(129)
4.3.4 不合格产品	(129)
参考文献	(130)
第5章 适人性设计方案	(131)
5.1 适人性方案的定义	(131)
5.1.1 适人性系统	(131)
5.1.2 NASA 适人性设计及流程	(132)
5.1.3 适人性方案的计划	(132)
5.1.4 NASA 适人性方案的认证流程	(133)
5.1.5 商业载人航天飞行中适人性方案	(133)
5.2 适人性方案的需求和方法	(133)
5.2.1 适人性方案的关键技术要求	(134)
5.2.2 管理要求	(135)
5.2.3 试验要求	(136)
5.2.4 数据需求	(137)
参考文献	(137)
第6章 生命保障系统安全性	(138)
6.1 空气调节与控制	(140)
6.1.1 监测是控制的关键	(140)
6.1.2 空气条件	(142)

6.1.3 二氧化碳的清除	(145)
6.2 痕量污染物控制	(146)
6.2.1 紧密结构和航天器舱	(146)
6.2.2 痕量污染物控制方法	(148)
6.2.3 痕量污染物控制设计考虑	(153)
6.3 航天器环境中水质量的评估:缓解健康与安全问题	(154)
6.3.1 与航天飞行相关的水源范围	(154)
6.3.2 航天器水的质量和风险评估样例	(155)
6.3.3 水质监测	(158)
6.3.4 结论和未来方向	(160)
6.4 废物管理	(161)
6.5 生命支持系统概要	(161)
参考文献	(162)
第7章 紧急救援系统	(166)
7.1 太空救援	(166)
7.1.1 法律和外交基础	(166)
7.1.2 救援能力的要求	(166)
7.1.3 救援模式和概率	(169)
7.1.4 不同飞行阶段的风险	(170)
7.1.5 历史上发生的故障事件	(171)
7.1.6 历史上的救援系统	(172)
7.1.7 航天救援以自我救援为主	(179)
7.1.8 地面救援的限制	(181)
7.1.9 作为航天救援研究的航天员返回飞行器	(183)
7.1.10 安全救援所	(187)
7.1.11 结论	(188)
7.2 个人防护设备	(188)
7.2.1 个人防护设备的目的	(188)
7.2.2 个人防护设备的类型	(188)
参考文献	(194)
第8章 碰撞规避系统	(196)
8.1 对接系统和运行	(196)
8.1.1 对接系统是航天器在轨连接的一种方式	(196)
8.1.2 保证对接安全性和可靠性的设计途径	(198)
8.1.3 俄罗斯对接系统保证安全性和可靠性的设计特点	(201)
8.1.4 俄罗斯对接系统安全性和可靠性完成验证的分析与试验	(203)
8.2 下降与着陆系统	(204)

8.2.1 降落伞系统	(205)
8.2.2 已知的降落伞异常现象和经验教训	(214)
参考文献	(217)
第9章 机器人系统安全	(219)
9.1 一般机器人系统	(219)
9.1.1 控制器和操作界面	(220)
9.1.2 臂和关节	(220)
9.1.3 驱动系统	(220)
9.1.4 传感器	(220)
9.1.5 末端执行器	(220)
9.2 空间机器人概述	(220)
9.3 危险及其原因识别	(222)
9.3.1 电路和电子机械故障	(223)
9.3.2 机械和结构故障	(223)
9.3.3 控制路径故障	(223)
9.3.4 操作员失误	(223)
9.3.5 其他危险	(223)
9.4 在设计中减轻危险	(223)
9.4.1 电路和机械设计及其冗余	(223)
9.4.2 操作员失误	(224)
9.4.3 系统健康检查	(224)
9.4.4 紧急拦阻减速	(224)
9.4.5 接近操作	(224)
9.4.6 机内测试	(225)
9.4.7 安全算法	(225)
9.5 通过训练减轻危险	(225)
9.6 减轻操作危险	(226)
9.7 案例研究：了解 Canadarm2 和空间安全	(227)
9.7.1 Canadarm2	(227)
9.7.2 照相机	(227)
9.7.3 力矩传感器	(228)
9.7.4 训练	(229)
9.7.5 危险关注和相关危险减轻	(230)
9.8 总结	(230)
参考文献	(231)
第10章 流星体和碎片防护	(232)
10.1 风险控制措施	(232)

10.1.1 机动	(232)
10.1.2 防护	(236)
10.2 航天器压力壁损坏的应急维修	(241)
10.2.1 平衡减轻计划的风险	(241)
10.2.2 泄漏定位系统和工作设计考虑	(244)
10.2.3 到达损坏区域的能力	(245)
10.2.4 工具包设计和验证考虑	(245)
10.2.5 航天员对维修后的压力舱进行重新鉴定	(245)
参考文献	(246)

第 11 章 噪声控制设计 (248)

11.1 前言	(248)
11.2 噪声控制计划	(248)
11.2.1 噪声控制策略	(248)
11.2.2 声学分析	(250)
11.2.3 试验和验证	(250)
11.3 噪声控制应用	(250)
11.3.1 噪声源的噪声控制	(252)
11.3.2 路径噪声控制	(252)
11.3.3 在接收空间的噪声控制	(256)
11.3.4 设计后噪声减轻	(257)
11.4 结论和建议	(258)
推荐读物	(258)
参考文献	(259)

第 12 章 材料的安全性 (260)

12.1 有毒放气	(261)
12.1.1 材料放气控制	(261)
12.1.2 材料测试	(262)
12.1.3 航天器舱段测试	(262)
12.2 应力腐蚀开裂	(263)
12.2.1 什么是应力腐蚀开裂	(263)
12.2.2 应力腐蚀开裂的预防	(264)
12.2.3 材料的应力腐蚀开裂测试	(265)
12.2.4 应力腐蚀开裂的设计	(266)
12.2.5 航天器硬件需求	(267)
12.2.6 推进系统中的应力腐蚀开裂	(268)
12.3 结论	(270)
参考文献	(270)

第 13 章 氧气系统安全	(273)
13.1 氧气压力系统设计	(273)
13.1.1 介绍	(273)
13.1.2 设计方法	(275)
13.1.3 氧气兼容性评估工序	(281)
13.2 氧气发生器	(285)
13.2.1 氧气产生的电气化学系统	(285)
13.2.2 固体燃料氧气发生器 (氧烛)	(289)
参考文献	(291)
第 14 章 宇航电子设备安全性	(294)
14.1 宇航电子设备的介绍	(294)
14.2 电气接地与电气连接	(295)
14.2.1 定义电气接地连接的特征	(295)
14.2.2 电流的控制	(296)
14.2.3 电气接地可以是信号返回通路	(296)
14.2.4 在什么位置、如何连接电气接地	(296)
14.2.5 定义电气连接的特征	(297)
14.2.6 电气连接类型	(298)
14.2.7 电气连接的异金属考虑	(298)
14.2.8 屏蔽的电气接地和连接	(299)
推荐读物	(299)
14.3 安全性关键的计算机控制	(300)
14.3.1 局部计算机控制	(300)
14.3.2 全局计算机控制: 故障安全	(301)
14.4 电路保护: 熔断	(302)
14.4.1 电路保护方法	(302)
14.4.2 电路保护器	(303)
14.4.3 设计指导	(304)
14.5 静电放电控制	(304)
14.5.1 基本原理	(304)
14.5.2 静电放电考虑的各个阶段	(307)
推荐读物	(310)
14.6 电弧跟踪	(312)
14.6.1 一个新的失效模式	(312)
14.6.2 电弧跟踪的特性	(314)
14.6.3 电弧跟踪事件的可能性	(315)
14.6.4 电弧跟踪的预防	(315)

14.6.5	危险的防护和管理验证	(316)
14.6.6	小结	(316)
14.7	高电压系统中的电晕控制	(316)
14.7.1	相关环境	(317)
14.7.2	设计原则	(317)
14.7.3	验证和测试	(318)
	推荐读物	(319)
14.8	舱外活动注意事项	(319)
14.8.1	太空中使用的显示器和指示器	(319)
14.8.2	通电电连接器的插拔	(320)
14.8.3	单根线熔点	(320)
14.8.4	电池的移除和安装	(322)
14.8.5	禁止功能的计算机或操作控制	(322)
14.9	飞行器电磁干扰和电磁兼容性控制	(322)
14.9.1	航天应用的电磁兼容性要求	(324)
14.9.2	基本的电磁兼容性作用和安全系数	(324)
14.9.3	任务驱动电磁干扰设计: 接地例子	(325)
14.9.4	航天器的电磁兼容性计划	(326)
14.10	安全关键电路的设计与试验	(328)
14.10.1	安全关键电路: 传导模式	(328)
14.10.2	安全性关键电路: 辐射模式	(333)
14.11	电气危险	(336)
14.11.1	引言	(336)
14.11.2	电击	(336)
14.11.3	生理学考虑	(337)
14.11.4	电气危险分类	(338)
14.11.5	漏电流	(338)
14.11.6	生物仪器	(339)
14.11.7	电气危险控制	(339)
14.11.8	电气危险控制的验证	(341)
14.11.9	电气安全性设计考虑	(342)
14.12	宇航电子设备的经验教训	(342)
14.12.1	电子设计	(343)
14.12.2	物理设计	(343)
14.12.3	资料与来源	(344)
14.12.4	损害避免	(344)
14.12.5	系统方面	(344)
	参考文献	(345)

第 15 章 软件系统安全	(347)
15.1 简介	(347)
15.2 软件安全问题	(347)
15.2.1 系统事故	(347)
15.2.2 与物理设计分离的作用和限制	(348)
15.2.3 软件可靠性和安全	(350)
15.2.4 系统工程存在问题	(352)
15.2.5 嵌入式软件的特点	(353)
15.3 目前的实践	(354)
15.3.1 系统安全性	(355)
15.4 最佳实践	(357)
15.4.1 软件密集型、安全关键项目的管理	(357)
15.4.2 基本的系统安全工程实践及其对软件密集型系统的意义	(358)
15.4.3 规范	(359)
15.4.4 需求分析	(360)
15.4.5 基于模型的软件工程和软件重复使用	(361)
15.4.6 软件架构	(361)
15.4.7 软件设计	(362)
15.4.8 人机交互设计	(364)
15.4.9 软件评审	(365)
15.4.10 验证和保证	(366)
15.4.11 操作	(366)
15.5 小结	(367)
参考文献	(367)
第 16 章 电池组安全性	(370)
16.1 介绍	(370)
16.2 通用设计和安全性规范	(370)
16.3 电池组类型	(371)
16.4 电池模型	(371)
16.5 危险与毒性分类	(371)
16.6 电化学	(371)
16.6.1 碱性电池	(371)
16.6.2 锂电池	(373)
16.6.3 银锌电池	(382)
16.6.4 铅酸蓄电池	(384)
16.6.5 镉镍蓄电池	(385)
16.6.6 镍金属氢化物电池	(386)

16.6.7 氢镍蓄电池	(389)
16.6.8 锂离子蓄电池	(391)
16.7 电池的贮存、运输和处理	(398)
参考文献	(398)

第 17 章 机械系统安全

17.1 安全系数	(404)
17.1.1 安全系数类型	(405)
17.1.2 安全系数是载人航天项目评估所特有的	(405)
17.1.3 影响安全系数选择的因素	(405)
17.2 航天器结构	(406)
17.2.1 机械需求	(407)
17.2.2 空间任务环境和机械载荷	(408)
17.2.3 项目总评：继承性设计和结构需求的反复验证	(409)
17.2.4 分析评估	(411)
17.2.5 结构的试验验证	(411)
17.2.6 航天器结构建模原理	(412)
17.2.7 材料和工艺	(413)
17.2.8 航天器结构的制造	(414)
推荐读物	(415)
17.3 断裂控制	(416)
17.3.1 基本需求	(416)
17.3.2 执行	(416)
17.3.3 小结	(417)
17.4 压力容器、管路和接头	(417)
17.4.1 压力容器	(417)
17.4.2 管路和接头	(421)
17.4.3 空间压力系统标准	(422)
17.4.4 小结	(422)
17.5 复合物编织压力容器	(422)
17.5.1 复合物编织压力容器系统	(422)
17.5.2 整体式金属压力容器的失效模式	(423)
17.5.3 复合物编织压力容器失效模式	(424)
17.5.4 复合物编织压力容器冲击敏感度	(425)
17.5.5 小结	(426)
17.6 考虑空间系统安全的玻璃和陶瓷组件结构设计	(426)
17.6.1 玻璃和陶瓷的强度特征	(426)
17.6.2 定义载荷和环境	(430)
17.6.3 设计系数	(431)

17.6.4 满足玻璃和陶瓷的寿命要求	(432)
17.7 安全危险机构	(433)
17.7.1 失效容差设计	(433)
17.7.2 安全危险机构的设计和验证	(435)
17.7.3 减小的失效容差	(441)
17.7.4 安全危险机构的评审	(441)
参考文献	(442)
第18章 有害材料的控制策略	(445)
18.1 有毒材料	(446)
18.1.1 毒理学基础	(446)
18.1.2 空间飞行中的空气质量毒物学风险	(449)
18.1.3 风险管理办法	(452)
18.2 生物有害材料	(454)
18.2.1 与航天有关的微生物危险	(454)
18.2.2 风险减缓办法	(455)
18.2.3 主要的空间飞行特殊微生物危险	(456)
18.3 易碎材料	(461)
18.3.1 居住区内的易碎材料	(462)
18.3.2 计划实施	(462)
18.3.3 内部设备的防护方案	(463)
18.3.4 外部设备的防护概念	(465)
18.3.5 关于利用易碎材料工作的常规注释	(466)
18.4 防护设计措施	(467)
18.4.1 故障容差	(467)
18.4.2 最小风险设计	(467)
18.5 防护设计方法	(467)
18.5.1 防护环境	(467)
18.5.2 防护系统的设计	(468)
18.6 安全控制	(470)
18.6.1 合理设计	(470)
18.6.2 材料选择	(470)
18.6.3 材料兼容性	(470)
18.6.4 合适的工艺	(470)
18.6.5 合适的装载和填充	(470)
18.6.6 断裂控制	(471)
18.7 安全验证	(471)
18.7.1 强度分析	(471)
18.7.2 鉴定试验	(471)