可靠性·维修性·保障性技术丛书 ⑩

RMS

丛书主编 王自力

安全性设计分析与验证

Safety Design Analysis and Verification

主编 赵廷弟

Reliability
Maintainability
Supportability

国防工业出版社
National Defense Industry Press

可靠性·维修性·保障性技术丛书

安全性设计分析与验证

Safety Design Analysis and Verification

主　　编　赵廷弟
副 主 编　焦　健
编写组成员　田　瑾　李晓磊　赵　诺
（按姓氏笔画排序）　鲍晓红

国防工业出版社
·北京·

内容简介

本书主要面向工程技术人员，以“危险”为核心，阐述了装备研制中的安全性工程工作、技术体系及具体技术方法，强调工程实用性。本书介绍了安全性工程的地位和作用以及发展历程；在介绍安全性度量与要求及安全性工程基本概念的基础上，梳理分析了装备研制、生产、使用各阶段的安全性分析工作，结合不同装备特点有针对性地介绍了各类产品的安全性设计原则和方法；详细阐述了安全性分析、设计技术方法。同时，本书针对装备中的软件安全性工作，介绍了相关的技术方法。最后，介绍了安全性验证的管理与技术方法。

本书供工程技术人员及管理人员在开展安全性工程工作时学习和参考，也可作为培训教材使用。同样也可用于高等院校高年级本科生及研究生学习参考。

图书在版编目(CIP)数据

安全性设计分析与验证/赵廷弟主编. —北京：国防工业出版社，2011.4
（可靠性·维修性·保障性技术丛书）
ISBN 978-7-118-07288-4

Ⅰ.①安… Ⅱ.①赵… Ⅲ.①软件开发－安全技术 Ⅳ.①TP311.52

中国版本图书馆 CIP 数据核字(2011)第 051552 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 100048）
北京嘉恒彩色印刷有限责任公司
新华书店经售
*
开本 710×960 1/16 印张 23¼ 字数 416 千字
2011 年 4 月第 1 版第 1 次印刷 印数 1—4000 册 定价 58.00 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

《可靠性·维修性·保障性技术丛书》编辑委员会

Preface 序

1995 年，国防科技及教育界著名专家杨为民教授组织编辑出版了国内第一套《可靠性·维修性·保障性丛书》，对推动武器装备质量观念的转变，提高武器装备的可靠性、维修性、保障性水平，发挥了重要的推动作用。

15 年后的今天，树立现代质量观，持续提高可靠性、维修性、保障性水平，已成为武器装备建设与国防科技发展中的共识，特别是《武器装备质量管理条例》的颁布实施，表明可靠性、维修性、保障性在现代质量观中具有战略性、全局性和基础性的地位和作用，高可靠、长寿命、好维修、易测试、能保障、保安全已成为武器装备研制、生产和使用中的普遍要求，可靠性、维修性、保障性工程活动已全面进入武器装备寿命周期各阶段，为提高武器装备的效能、降低寿命周期费用发挥了不可替代的作用。

在上述背景下，在武器装备建设与国防科技发展中，无论在技术上还是在管理上，都对可靠性、维修性、保障性提出了更高的要求。为适应这种新形势，我们组织有关专家重新编辑出版了这套《可靠性·维修性·保障性技术丛书》，共 12 册，以满足广大工程技术和管理人员的迫切需求。

本套丛书认真总结了 15 年来国内外武器装备可靠性、维修性、保障性最新实践经验，全面吸收了我国在预先研究和技术基础研究领域中取得的主要研究成果，从装备、系统、设备、元器件等多个产品层次和硬件、软件等不同产品类别，可靠性、维修性、测试性、保障性、安全性等多种质量特性，以及论证、研制、生产和使用与保障等寿命周期各阶段，全方位地论述了相关领域的基本概念、技术方法、实践经验及发展方向，具有系统性、实用性和前瞻性，从而有助于读者全面、系统地了解和掌握该项技术的全貌。本套丛书中阐述的可靠

性、维修性、保障性理论与技术，对武器装备和一般民用工业产品均具有普遍的适用性。

《可靠性·维修性·保障性技术丛书》是一套理论与工程实践并重的著作，它不仅可以为广大工程技术和管理人员提供有用的指导和参考，也可作为有关工程专业本科生、研究生的教学参考书。我们相信，这套丛书的出版，对我国武器装备可靠性、维修性、保障性工程的全面深入发展将起到重要的推动和促进作用。

丛书编辑委员会

2010 年 12 月

Preface 前言

安全性是产品的一种共性的固有属性。提高产品安全性，确保安全是武器装备研制、生产、使用和保障的首要要求，高安全性是保证武器装备使用效能的重要因素之一。安全性工程就是研究装备寿命周期中危险的发生、发展规律，达到预防危险、避免事故，提高装备效能的一门工程学科。

对于生产过程中的安全事故研究由来已久，而以复杂装备为对象，将安全性作为装备特性，面向装备寿命周期开展研究则起源于20世纪60年代美军研制洲际导弹的过程中。自美军于1969年颁布MIL－STD－882标准以来，经过40多年的发展，安全性工程已经在军事、航空航天、核工业、化工、交通运输等众多行业得到应用。

20世纪80年代初期，安全性工程首先在我国的民用生产领域开展了初步研究和应用。进入90年代以后，我国颁布了一系列安全性工程技术和管理规定，逐步在飞机、导弹、火箭等大型武器系统的研制中推行安全性工程技术，推动了我国工程型号的安全性工作的迅速发展。特别是进入21世纪以来，随着新型复杂装备的不断研制和应用，安全性工程得到了各级领导和工程技术人员的普遍重视，在理论研究和工程应用上都积累了丰富的经验，为进一步开展安全性工程的研究与应用奠定了良好的基础。

本书编写的指导思想：面向工程技术人员，以近年来型号的工程实践经验为基础，结合国内外安全性工程技术的最新发展，以“危险”为核心，以装备研制中的安全性分析、设计、验证工作为主线，选取成熟有效的技术方法，进行系统地整理并组织编写，强调工程实用性，满足装备研制要求。

本书共分6章。第1章绪论，简要介绍了安全性工程的地位和作用以及发展历程；第2章安全性度量与要求，在讨论安全性工程基本概念的基础上，对安全性工程的研究对象——危险——进行了讨论，以满足安全性要求为目标引导后续章节；第3章安全性分析，在对装备研制、生产、使用过程中的安全性分析工作梳理的基础上，对成熟有效的安全性分析技术进行逐一介绍；第4章安全性设计，以消除危险为目的，介绍了各类产品的安全性设计原则和方法；第5章软件安全性设计分析，重点针对装备中的软件安全性工作，介绍了相关的技术方法；第6章安全性验证，介绍了安全性验证工作的流程、方法和选取原则。

参加编写工作的有：赵廷弟（第1、2章）、焦健（第1、2、3、4章）、李晓磊（第3、4章）、赵诺（第2、3、6章）、鲍晓红（第5章）和田瑾（第3章）。全书由赵廷弟主编，曾天翔研究员、孙有朝教授主审。王薇、吴居宜、闫志付、吴洋、李国旗、曾福萍和徐小杰等也参与了查阅资料和部分内容的编写工作。在编写过程中，参考了大量国内外文献，已在参考文献中列出，在此一并表示感谢。

编者

2010年10月

Contents 目录

第1章　绪　论

1.1　安全性的作用与地位

安全第一，在装备研制与使用中是毋庸置疑的。安全性是产品的一种固有属性，是保障使用安全的前提条件。提高产品安全性，确保安全是武器装备研制、生产、使用和保障的首要要求，高安全性是保证武器装备使用效能的重要因素之一。在和平时期，产品自身是否安全，不仅关系到装备和人员安全，也关系到国防科技工业和武器装备建设的发展，甚至对国际关系、国家战略、社会政治和经济生活等产生重要影响；在战争对抗中，军事装备的安全性水平直接影响战斗力和敌我双方的力量对比，改变战场形势，甚至事关军事行动的成败。

现代复杂武器装备，往往工作在复杂恶劣环境和复杂任务环境中，并带有高能、易燃、易爆、有毒等物质，能够产生巨大的破坏力和杀伤力，因此，在研制、生产、使用、保障及处置等寿命周期过程中，对研制和使用人员、相关设备、基础设施、公共资源及环境等的安全也构成威胁。武器装备的技术越复杂、使用要求越高、威力越大，其对安全的威胁可能性也就越大。这种特殊性决定了武器装备不仅需要具备高可靠性以保证完成规定任务，更需要具备高安全性以保证人员、设备/设施安全，避免财产受损失或环境遭受损害。

国内外惨重事故不胜枚举，例如，2000 年 8 月，俄罗斯海军“库尔斯克”号核潜艇在执行演习任务中，因鱼雷推进装置使用的易燃气体泄漏，造成爆炸而沉入海底，艇上 118 名官兵全部遇难；苏联“联盟”－11 号飞船因返回舱中一个与外界连接的阀门提前打开，造成 3 名宇航员死亡；1986 年，美国“挑战者”号航天飞机因固体助推器密封圈泄漏导致爆炸，造成 7 名宇航员丧生；2003 年，美国“哥伦比亚”号航天飞机因隔热层损坏而造成失事，又有 7 名宇航员殉难等等。在我国装备研制和使用过程中，也曾发生过星箭爆炸、舰艇翻沉、飞机失事等灾难性事故，例如，1996 年，某卫星发射过程中发生爆炸，造成人员伤亡，卫星型号及发射场设施损毁；2003 年，我国海军某潜艇安全事故，造成 70 名官兵遇难；2006 年的 6.3 空难，导致 40 人死亡以及装备研制的重大损失等。

对这些事故的调查和分析表明，如果在研制中有效应用安全性分析设计等工程技术确保和提高产品的安全性水平，有相当一部分事故或灾难后果是可以避免的。实践证明，在装备的研制、生产、使用、保障及处置等寿命周期过程中，系统化、规范化实施安全性工程，是提高装备的安全性水平，最终确保任务成功，预防事故和减少事故损失、降低研制和使用风险、提高投资效益和装备使用效能、推进国防建设的一条有效途径。

实施安全性工程的作用主要有以下几方面。

1）有效地预防事故和减少损失

预防事故、减少损失（包括人员伤亡及职业病）是安全性工程的中心任务。系统全面地开展安全性工程工作，识别系统中存在的薄弱环节和可能导致事故发生的条件，通过系统分析查找导致事故发生的真正原因，特别是可以分析出未知的、易被忽视的危险因素，并且通过定量分析，预测事故发生的可能性及后果的严重性，从而可以采取相应的措施，预防、控制事故的发生。

2）用最少投资达到最佳安全效果

对系统的安全性进行定量分析、评价，优化系统的安全性设计，为安全管理和事故预防提供科学依据。根据分析可以选择出最佳方案，使各个分系统之间达到最佳配合，用最少的投资得到最佳的安全效果，从而可以最大可能地避免事故，降低损失。

3）迅速提高装备研制使用人员的安全技术水平

通过系统地实施安全性工程，不仅可以提高安全技术人员的业务水平，还能使装备系统的设计和使用维修人员了解掌握各种系统分析和评价方法，提高安全技术人员、操作人员和管理人员的业务水平和系统分析能力，以便能够很好地提高整个装备的安全水平，预防事故的发生。

4）系统地进行安全管理

现代武器装备的特点是规模大、自动化程度高，研制及使用过程日趋复杂，各分系统之间相互联系、相互作用、相互制约。安全性工程通过系统分析、评价，全面系统地、预防性地处理装备中的安全问题，而不是孤立地、就事论事地去解决安全问题，实现系统安全管理。

5）促进各项安全性标准制定和数据积累

安全性工程的一项重要工作就是要对装备的安全性做出定性或定量评价，这就需要有各项安全性标准和数据，如可接收的最低安全风险、人机工程设计要求和安全性设计准则等。因此，安全性工程工作可以促进各项安全性标准的制定和有关安全性数据的收集、积累，为建立安全性数据库打下基础。

1.2 安全性发展概况

1.2.1 发展历程

安全是伴随人类发展的永恒主题,但在不同时期,人们所面临的安全问题有很大不同。早期人们所面临安全问题相对简单,主要表现在自然灾害和人为灾害。随着科学技术的不断进步,人类在利用技术推动社会进步的同时,也伴随着新的灾难。特别是进入以社会化大生产为标志的工业社会以来,人员伤亡、环境破坏等事故显著增加,安全已成为广为关注的社会问题。为解决这一突出矛盾,19 世纪末至 20 世纪初期,欧美学者开始了安全(事故)相关理论和技术方法的研究,德、英、美、法、荷兰等国先后建立了上百个与安全科学有关的组织和科研机构。安全性工程起源于民用行业,在军事领域得到广泛应用并走向成熟,经过 100 多年的发展,安全性工程理论研究和工程应用在众多领域取得了显著成果,其发展过程大致可划分为三个阶段。

第一个阶段:20 世纪初期至第二次世界大战之前。工业的飞速发展,使得蒸汽动力和电力驱动的机械彻底取代了手工作坊中的手工工具,这些机械在极大地提高劳动生产率的同时,也增加了事故发生频率。当时设计的机械很少或者根本不考虑操作的安全和方便,几乎没有什么安全防护装置;工人很少受到培训,操作不熟练,加上长时间的疲劳作业,伤亡事故自然频繁发生。这一时期的安全理论把安全问题完全归结为人员,认为某些人较其他人更容易发生事故,他们是事故的主要原因。例如,英国的格林伍德(M. Greenwood)和伍兹(H. H. Woods)通过对工厂里伤害事故统计分析,认为存在事故频发倾向者,这些人具有容易发生事故的、稳定的个人内在倾向。在此基础上,有学者进一步提出事故遭遇倾向理论,认为某些人员在某些特定条件下容易发生事故。但经过多年的研究和实践,目前,这种把事故完全归结于人的理论已经不再被人们所接受,安全问题应从整个人—机系统的角度进行分析。在这一时期还产生了一个重要的事故理论:海因里希法则。美国安全工程师海因里希(Heinrich)在 20 世纪 40 年代通过统计 55 万件机械事故得出的一个重要结论:在机械事故中,死亡、重伤、轻伤或无伤害事故的比例为 1∶ 29∶ 300。这一规律已经在很多行业中得到了印证,它表明一起严重的事故总是由众多的轻微差错累计而成,要避免最终的事故就必须注意纠正日常中的轻微失误。

第二个阶段:第二次世界大战至 20 世纪 50 年代。第二次世界大战期间出现了高速飞机、雷达和各种自动化机械等新型装备,这些装备(设备)的结构和使用复杂程度已经远远超出了人的能力,单纯通过人员的培训已无法解决安全