国防科技工业质量与可靠性专业技术丛书

郑 恒 周海京 主编

概率风险评价

GAILU FENGXIAN PINGJIA

国防工业出版社
National Defense Industry Press

国防科技工业质量与可靠性专业技术丛书

概率风险评价

郑　恒　周海京　主编
邵德生　肖名鑫　主审

国防工业出版社
·北京·

内 容 简 介

通过强化风险意识并实施规范的风险分析、风险评价、风险决策等活动，有效降低或控制各类风险，是当前国防科技工业尤其是航天工程管理的一项重要工作内容。

本书作为《国防科技工业质量与可靠性专业技术》丛书之一，以支持工程项目的风险管理活动为目标，在介绍风险、风险分析的一般知识及其国内外发展概况的基础上，重点讲述了概率风险评价（PRA）程序、常用的建模方法、数据收集与分析方法、相关软件工具等内容。同时，为帮助读者理解概念、掌握方法并在实际工作中规范应用 PRA 技术，本书中还例举了航天工程与民用工程应用 PRA 的案例，并在书末附录中提供了 PRA 报告的编写范例。

本书可为国防科技工业领域广大工程技术人员、质量与可靠性专业人员及各级管理人员开展概率风险评价工作提供技术支持，也可作为各类人员学习、了解该项技术的参考用书。

图书在版编目（CIP）数据

概率风险评价 / 郑恒，周海京主编. —北京：国防工业出版社，2011.8
（国防科技工业质量与可靠性专业技术丛书）
ISBN 978-7-118-07448-2

Ⅰ.①概… Ⅱ.①郑… ②周… Ⅲ.①国防工业－风险评价 Ⅳ.①F407.483.7

中国版本图书馆 CIP 数据核字（2011）第 180866 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印刷
新华书店经售
*
开本 710×960　1/16　**印张** 18　**字数** 317 千字
2011 年 8 月第 1 版第 1 次印刷　**印数** 1—5000 册　**定价** 49.00 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

丛书前言

“质量是企业的生命”，是技术水平和管理水平的综合体现。提高产品质量水平，是加快转变经济发展方式的重要途径和必然要求。对于武器装备，质量关系型号成败，关系战争胜负，关系国家安危，“保质量就是保安全、保战斗力、保胜利。”

依靠先进技术和科学管理保证和提升质量，是我国国防科技工业质量工作的基本规律和有效经验。《武器装备质量管理条例》也明确规定，“国家鼓励采用先进的科学技术和管理方法提高武器装备质量”。特别是在武器装备机械化信息化复合式发展的新形势下，装备技术指标更高、系统更加复杂、软件更加密集、风险更难控制，对质量与可靠性技术的需求更大、要求更高。

为促进先进质量与可靠性技术方法在型号中的有效应用，在国防科技工业主管部门的指导和支持下，国防科技工业质量与可靠性研究中心牵头，在2003年编辑出版了包括统计过程控制，软件质量管理，危险分析与风险评价，故障模式、影响及危害性分析与故障树分析，元器件使用质量保证在内的《国防科技工业质量与可靠性专业技术丛书（第一批）》。为适应新形势和新任务的需求，又有针对性地遴选了潜在电路分析、概率风险评价、质量功能展开、六西格玛管理、健壮设计等五种技术方法，编辑形成了丛书的第二批书目。

新出版的这一批书目集中了五项行之有效的质量与可靠性技术方法，凝结了国防科技工业质量理论研究和工程实践的最新成果，对于促进先进技术推广应用、提高全员质量技能具有十分重要的意义，可为国防科技工业广大技术和管理人员开展质量工作提供技术支持，也可作为各类人员学习的参考用书。

考虑到丛书编写时间和资源有限，而且一些技术方法的研究和应用仍需继续深化，所以难免有不足和尚需完善的地方，欢迎广大读者提出宝贵意见。

《国防科技工业质量与可靠性专业技术丛书（第二批）》编委会

二〇一一年六月

《国防科技工业质量与可靠性专业技术丛书(第二批)》
编 委 会

前　言

概率风险评价(PRA)是一种定量风险评价技术,它综合运用事件树、故障树等方法构建出风险事件链模型,集成工程各类定性和定量信息(如试验数据、现场数据、专家判断等)进行模型量化与不确定性分析,从而合理地预测系统的风险水平,分析影响风险的关键因素,为复杂系统寿命周期内的风险管理提供决策支持。

在过去的三十年中,作为识别和分析复杂系统风险的主要方法,概率风险评价在风险管理中的作用已被航空航天、核能、电力、石油化工和国防等许多工业实践所证实。

本书在编写过程中,吸收借鉴了国内外有关文献资料所登载的成果,结合我国军工特别是航天、核能等工业领域应用该技术的工程经验以及该项技术的未来发展趋势,阐明了 PRA 的基本概念、程序和方法,并给出了典型工程应用示例。

本书共分 5 章,包括:

第 1 章概述,阐述了 PRA 的技术背景与特点,分析了 PRA 技术的国内外研究、应用现状与发展趋势。

第 2 章 PRA 基本概念,在分析风险、风险管理、风险评价、事件链、不确定性等 PRA 相关概念的基础上,阐述了 PRA 的 3 个基本内涵,即以事件链为基础的建模技术、以不确定性分析为核心的数据分析技术,以及以风险管理决策为目标的应用方向。

第 3 章 PRA 实施程序,结合某航天器的推进剂输送系统示例,对 PRA 实施程序的 9 个步骤进行详细论述,包括:定义目标和范围、熟悉系统、识别初因事件、事件链建模、故障建模、数据收集与分析、模型量化与集成、不确定性分析、重要度排序与结果分析等。

第 4 章 PRA 方法与工具,论述了 PRA 实施程序中常用的建模和数据分析方法,并介绍了常用的 PRA 软件工具。在建模方法中,主要讨论主逻辑图、事件序列图、事件树、故障树和贝叶斯网络等常用模型,以及共因、人因、软件、物理和现象模型等特殊模型。在数据分析方法中,主要讨论 PRA 的数据类型和数据

源、基本事件的不确定性分析、不确定性传播的蒙特卡罗仿真分析、重要度排序与薄弱环节确定、相对风险分析、评估结果表示等方法。本章最后介绍了常用的PRA软件工具。

第5章PRA工程应用示例，例举了PRA在泵动力系统、轨道空间站等不同系统上的应用，并介绍了PRA在设计方案相对风险评价中的应用。

本书的组织结构图如下：

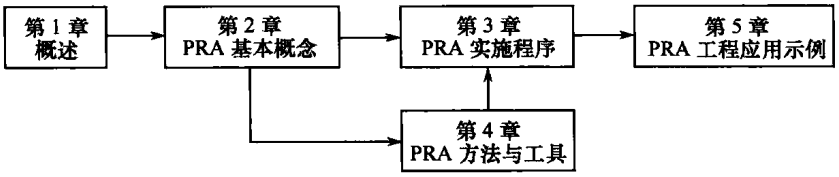

图1　本书的组织结构图

本书由郑恒、周海京主编。第1章由郑恒、周海京编写，第2章由周海京、李福秋、郑恒编写，第3章由郑恒、刘春雷、李福秋、周海京、刘金燕、杨静编写，第4章由刘金燕、郑恒、刘春雷、杨卓鹏、李海生编写，第5章由郑恒、郑云青、刘志、李海生、杨卓鹏编写。全书由郑恒统稿。周波、龚佩佩参与了校对工作。邵德生研究员和肖名鑫研究员担任本书主审。本书在编写过程中，还得到了卿寿松、顾长鸿、任立明、张仁兴、张华、邱邦清、周炽九、郑松辉、朱美娴、周鸣岐、曾天翔、遇今、周新蕾、陈凤熹、童洁娟等领导和专家的指导和帮助，在此一并致谢。

由于作者水平有限，对某些问题的理解尚不是十分透彻，书中定有不妥甚至错误之处，恳请读者批评指正。

编　者

2011年1月

目　录

第1章 概 述

1.1 技术背景与特点

随着技术的进步和应用需求的提升，人类越来越多地开发和应用大型复杂工程系统，如核电站、空间站和载人飞船等。为了满足特殊的应用需求，这些系统通常具有复杂的结构，采用大量高新技术或高能材料（如核材料），工作在高危环境（如空间环境），使得系统发生事故的可能性显著增大。而这些大型复杂工程系统又往往应用于国防和国民经济的重要领域，关乎国家安全和国计民生，具有重要的政治和经济意义，其事故后果影响重大。

为了确保任务成功和安全，工程技术人员在复杂工程系统的研制中常常采用“裕度设计”的方法来保证其可靠性和安全性。例如，假设要设计一条承重钢梁，工程师可能会把它增加到实际所需的两倍厚度，以尽可能大的裕度或余量来确保安全，而不做详细的风险分析或概率分析。在这种思想指导下，类似“故障模式及影响分析”（FMEA）等定性方法得到广泛应用，以获得复杂工程系统中可能引发灾难性事故的“单点失效”项目清单，并尽可能针对这些项目进行冗余设计或稳健性设计。这样，通过对每个关键项目或因素提供足够大的余量，来保证系统安全可靠。

这种定性分析方法能够为系统各个关键因素的裕度设计提供足够的信息，但却难以全面、准确地表征系统的总体风险。其局限性主要表现在：定性分析方法难以估计复杂工程系统发生事故的可能性有多大，也不能说明某些事件的累加风险是多少。而且，定性分析方法无法给出系统组成部件的重要度排序，也难以说明改进系统的某个或某些部件，对于提升系统整体的可靠性和安全性起到多大的作用。例如，增强航天飞机隔热瓦的耐久性，对于提高航天飞机安全性的贡献到底有多大。因此，也就说明不了复杂工程系统中哪个（或哪些）部件更为关键。

在1986年“挑战者”号航天飞机失事前，美国宇航局（NASA）运用FMEA指出航天飞机上有大约有2500个关键部件，但在事故发生后所进行的FMEA中，这个数目就激增到了4500个之多，使得决策者茫然不知所措。可见，在很多情

况下，仅仅使用定性分析方法并不能满足风险决策的要求。

为了解决大型复杂工程系统风险决策所面临的问题，必须借助相对风险的概念和定量风险评价的方法。通过定量评估哪些事件风险更高，更易于导致事故，可以为风险决策提供科学依据，以便把有限的资源投入到急需解决的问题上，对系统进行有效的改进或升级，从而使系统更为安全、可靠。

开展复杂工程系统定量风险评价，需要解决以下两个主要问题。

首先，必须正确模拟系统运行的真实过程，构建合理的风险事件链模型。为此，必须全面、准确地识别复杂工程系统的风险源，并正确处理系统运行中普遍存在的事件交互作用问题。识别风险源是构建事件链模型的前提，必须运用科学的方法确保复杂工程系统风险源识别的准确性和全面性。另一方面，复杂工程系统的耦合度较高，接口复杂，各分系统或部件之间往往构成相互关联、交叉的复杂事件链；单独看来，事件链中每一个事件对系统的负面影响可能并不严重，但若组合到一起却可能引起“关联失效”，导致灾难性的后果。三哩岛核电站泄漏事故和“挑战者”号航天飞机事故都是由于关联失效引起灾难的有力证据。正如美国耶鲁大学教授 Charles Perrow 在《常规事故》一书中指出的那样，“大部分工程师能够识别和处理复杂系统中的单点失效事件，但却难以有效识别因两个以上部件意外发生相互作用而导致的事故。”这就需要应用针对事件链的特殊建模技术。

其次，必须进行有效的不确定性分析。风险分析的一个关键问题，就是对不确定性进行科学分析。各种复杂工程系统（如航天系统）所面临的不确定性往往很大。应用环境的复杂多变、使用过程中人为因素的影响、经费不足所导致的试验量不足、不同层次产品的故障信息综合困难等原因，都会造成系统具有的较高的风险和不确定性，必须运用科学的数据分析方法进行处理，才能更好地支持风险评价和决策。

为此，人们相继开发、应用了许多定量风险评价方法，概率风险评价（Probabilistic Risk Assessment，PRA）就是其中一种有效的方法（注：在安全性工程领域，该项技术有时也称为概率安全性评价（Probabilistic Safety Assessment，PSA），由于技术原理相同，为简化叙述，本书统一采用概率风险评价（PRA）这一称谓）。借助于特殊的建模和不确定性数据分析技术，PRA 很好地解决了以上两个主要问题。经过多年的探索和应用，PRA 已成为在大型复杂工程系统开发和应用中实施持续风险评价和监控的重要工具，广泛应用于航天、航空、核电、石化和国防等诸多领域。

PRA 是一种识别与评估复杂工程系统风险的结构化、集成化的逻辑分析方法。它综合运用事件树、故障树等方法构建出风险事件链模型，集成工程各类定

性和定量信息(如试验数据、现场数据、专家判断等),利用贝叶斯分析、蒙特卡罗仿真方法等进行模型量化、不确定性分析与重要度排序。在此基础上,PRA可以评估复杂工程系统整体的安全性或可靠性,为工程决策提供支持。

PRA更为重要的作用在于其相对风险分析功能。利用这一功能,PRA能够分析影响系统安全性和任务成功的薄弱环节。其分析结果,为制定可行的风险控制策略提供了依据,为决策者指明哪些投资可以更有效地改进设计和运行效果。

一方面,PRA通过识别出主要的风险影响因素,可以将资源有效分配于主要的风险因素,避免将资源浪费在次要的风险因素上。

另一方面,通过对影响系统安全性或任务成功的事件进行不确定性分析,能够详细地描述风险评价结果的可信程度,也可以使决策者了解引起不确定性的原因,比较各种投资方案在降低不确定性方面的优劣。

PRA既关注事故后果的可能性,也考虑事故后果的严重性。从这个角度来看,PRA改进了传统的可靠性和安全性分析方法,能够更准确地支持风险决策。

PRA与传统可靠性分析、危险分析的关系如表1.1所列,其主要区别体现在两个方面:第一,PRA可以对单个事件或整个系统的不确定性进行更加精确的量化分析;第二,PRA可以更准确地量化评估后果的严重程度,而不像可靠性分析那样仅简单地用平均故障间隔时间(MTBF)来描述系统行为。PRA又不同于通常的危险分析方法。危险分析是把后果严重、低概率的事件视为已经发生的事件,并识别和评估其风险大小,也就是并不考虑事件发生的可能性;而且,危险分析方法难以保证事件链集合的完备性。相比而言,PRA的结果更为丰富,借助其对后果度量(严重度和可能性)的多维描述,可以直接应用于资源分配和其他风险管理决策。

表1.1 PRA与传统可靠性分析、危险分析的区别与联系

分析方法	对后果严重度的描述	对后果可能性的描述	不确定性分析程度
传统可靠性分析	简单(成—败两状态)	详细	简单(置信度)
危险分析	详细	无	无
概率风险评价	详细	详细	详细

PRA的局限性主要在于其技术上比较复杂,因此,PRA在工程应用领域的推广,需要较长的一段时间。PRA工作的有效性,还需要有一个多学科综合型的团队,运用科学的方法来保证。尽管对每位工程师来说,描述复杂系统的几条风险事件链并不困难;但是,若要详细列出复杂系统的所有事件链,就恐怕难以胜任了。因此,构建复杂系统在整个任务过程的全面事件链模型,必须依靠整个团队的力量。这不仅是因为工作量大,还牵涉到技术学科的多样性。

同时,PRA 的有效实施还需要科学的方法做保证。构建事件链模型的本质,是把复杂的实际情况映射为一组计算机可解的逻辑关系。随后,才能运用计算机程序进行有效的分析。事件链建模不可能一次完成,需经多次反复推演,才能构建出比较切合实际的模型。而模型输入参数的确定,更需要收集大量分散于各个信息源的设计信息和性能数据,并运用科学的方法进行整理和分析才能完成。由此可见,只有依靠科学的方法和团队的合作,才能取得 PRA 工作的最佳效果。

1.2 国外 PRA 技术的发展

20 世纪 60 年代初期,风险和可靠性评估方法最初应用于美国航空航天和导弹项目中,并产生了故障树分析法(FTA)。在"阿波罗"项目的早期阶段,NASA 就已经提出了登月任务成功(即运送宇航员到月球,再安全返回地球)的概率问题。经过大量的风险或可靠性计算,成功的概率值很低,结果相当令人失望。因此 NASA 丧失了进一步对风险或可靠性进行定量分析的信心,转而决定依靠 FMEA 方法来进行系统的安全性分析。此后 FMEA 一直应用于 NASA 所有与安全性相关的项目。

几乎与此同时,核工业界则把 PRA 作为评估安全性的最有效方法。核领域的工程师将故障树分析往前推进了一步,他们增强了核电站故障树的功能,计算出事故发生的概率,并度量出每种事故后果的严重度。通过综合计算,得到了特定严重度水平下事故的发生概率。1975 年,美国核管会编写了著名的《美国商用轻水堆核电站概率风险评价》报告(WASH - 1400),其主要结论是:

(1)即使发生堆芯熔化,也不一定会对公众产生重大影响。

(2)堆芯熔化后,预测的死亡人数比起火灾、爆炸、飞机事故造成的死亡人数要少得多,而堆芯熔化事故本身的发生概率也小于其他自然灾害或人为灾害的发生概率。具体结果是:造成 10 人以上死亡的事故概率为 4×10^{-6}/堆年;造成 100 人以上死亡的事故概率为 7×10^{-7}/堆年;平均发生一次事故最多约死亡 2300 人,发生概率约为 10^{-7}/堆年。

(3)以往对堆芯熔化所造成的反应堆事故的影响所作的分析(WASH - 740),是以事故发生在最恶劣的气象扩散条件下以及人口密度较高的地方为假定条件的。而实际上,气象条件和反应堆所在处的人口密度是各不相同的。因此,若考虑现实气象条件出现的频度和人口密度的分布,则造成最大影响的事故发生概率变小,它的规模也变小。

在 WASH - 1400 报告的结论中,还指出了核电站中的哪些子系统对事故风

险的贡献最大,指明了最需要实施设计改进的地方。WASH－1400 第一次比较系统地提出并实践了 PRA。而 1979 年 3 月美国三哩岛核电站泄漏事故的发展进程,则证实了 WASH－1400 的 PRA 研究成果的正确性。

此后,PRA 在核电站安全评价中得到广泛应用。核电站 PRA 的范围包括三个级别。一级(Level 1):主要任务是初因事件分析和系统分析,即事故序列分析和系统的可靠性分析,以获得堆芯损伤频率大小的估量。二级(Level 2):完成对堆芯物理熔化过程及安全壳可能失效过程的分析。其主要任务是确定堆芯在损坏后向环境的放射性释放的源项,包括核素的组成、强度及时间分布。三级(Level 3):分析放射性释放后的后果。根据放射性的源强分布和核电站的环境因素,如人口分布、气象条件等,计算电站周围的后果影响。目前世界上各个国家所完成的 PRA 分析,多数针对的是 Level 1 PRA 的内部事件(功率阶段和停堆阶段),内部灾害的分析正在逐步增加,但已完成了外部灾害分析的还比较少。

除了核工业,在石油化工和装备研制等工业领域也逐步推广并成功应用了 PRA,取得了显著的成果和效益。至"挑战者"号航天飞机事故发生时,PRA 已经成为备受推崇的、实用的安全性评估工具。由于 PRA 方法具有很高的逻辑性、系统性和综合性,事实已经反复证明其能够揭露系统在设计和运行过程中所存在的问题,而这些问题即便是最优秀的安全性工程专家也难以发现。PRA 方法表明,研究低概率且后果严重的灾难事件固然重要,然而对那些出现概率高的所谓良性事件,若其能组成事件链并导致严重后果,则同样值得重视。与常理相反,后者对安全性的危害往往超过前者。

直到 1986 年"挑战者"号事故后,NASA 才重新考虑开展量化风险分析的进一步研究。1986 年 10 月 29 日,美国众议院科技委员会(Slay)在《对"挑战者"号事故的调查》报告中指出:如果没有评估航天飞机部件失效概率方法的支持,NASA 将很难把精力和资源有效地集中在航天飞机的关键系统上。

1988 年 1 月,Slay 委员会在《"挑战者"号事故后对航天飞机的风险评价和管理评价》报告中指出:PRA 方法应该尽早应用于航天飞机系统风险管理活动中。该报告还指出:应系统地开发出由空间运输系统的失效和异常情况记录、正常飞行和测试结果等数据所构建的数据库,形成相应的数据分析技术,以支持 PRA、趋势分析和其他与可靠性、安全性相关的定量分析。

在 Slay 委员会的敦促下,NASA 开始尝试应用 PRA。航天领域中第一次试用 PRA 是在 1988 年,对航天飞机主推进系统进行 PRA 应用,该研究属于概念验证性的研究。在接下来的十年中,不少型号试用了 PRA,特别是在携带核载荷的任务(如 Galileo、Ulysses 和 Cassini)中开展了 PRA。但这些应用都仅是概念验证性质的。这是因为在这个阶段中始终存在这样一个逻辑矛盾:"工程师在

实施 PRA，前不会相信 PRA，但他们不会实施 PRA，除非他们相信 PRA。”

NASA 中真正的氛围改变是在 20 世纪 90 年代中期，时任 NASA 最高领导人的 Dan Goldin 对原有工作表示不满，他指出：“自从我 1992 年来到 NASA，我们已经花费了数十亿美元在航天飞机的升级上，却不知道到底这些升级对航天飞机的安全性提高了多少。我需要一种工具能进行基于风险的升级决策。”他希望知道航天飞机是否“足够安全”，如何使其更加安全。Dan Goldin 认识到 PRA 可以用来排序，指明航天飞机的哪些部分最需要进行升级，于是，他命令安全和任务保证办公室（OSMA）开发 PRA 工具以支持航天飞机升级资金分配的决策。NASA 随后开发了一种工具来回答这些问题，此工具即定量风险评价系统（QRAS）。

如今，NASA 已经真正接受了 PRA，并在不同研制阶段对各航天型号实施了 PRA。NASA 的安全性和任务成功政策指令性文件（NPD 8700.1）明确了实施定量风险评价的要求，规定在项目开发、试验和运行中必须使用 PRA，见表 1.2。该文件说明：NASA 的目的是“通过使用定量或定性的风险评价技术识别和了解风险，采取适当的措施控制或消除风险，从而在任务进行之前接受合理、适当等级的残余风险，以提高整个寿命周期的系统安全性和任务成功的可能性”。

表 1.2　NASA 的安全性和任务成功政策指令性文件（NPD 8700.1）的 PRA 要求

后果分类	标准/规定		NASA 计划/项目	PRA 范围*
人员安全与健康	公众安全	对星球的保护项目的要求	火星样本回收	F
		白宫议案（PD/NSC-25）	核有效载荷（如 Cassini、Ulysses、Galileo）	F
	载人航天飞行		国际空间站	F
			航天飞机	F
			轨道空间飞机 OSP，载人救援飞船 CRV 等	F
任务成功（对于无人的任务）	战略重要性高		火星项目	F
	计划关键度高		发射窗口（如星球任务）	F
	其他任务		地球科学任务（如 EOS）	L
			空间科学任务（如 SIM）	L
			技术展示和验证（如 EO-1）	L

* 注：F 指进行全面的 PRA；L 指进行有限的或简单的 PRA

PRA 的范围包括:航天器损失或航天员伤亡;航天器任务过程的风险;不同运载方式的技术性能风险;与发射场有关的发射和运行风险;航天器结构和性能退化的风险;航天器老化部件(需替换或重新设计的部件)的风险;航天器设计改进带来的性能风险等。PRA 的应用有力地支持了 NASA 的连续风险管理活动,可在风险、设计改进和费用之间进行有效的权衡。在使用 PRA 后,NASA 在不增加航天器安全风险和任务风险的前提下,节省了近 44% 的资源,如图 1.1 所示。

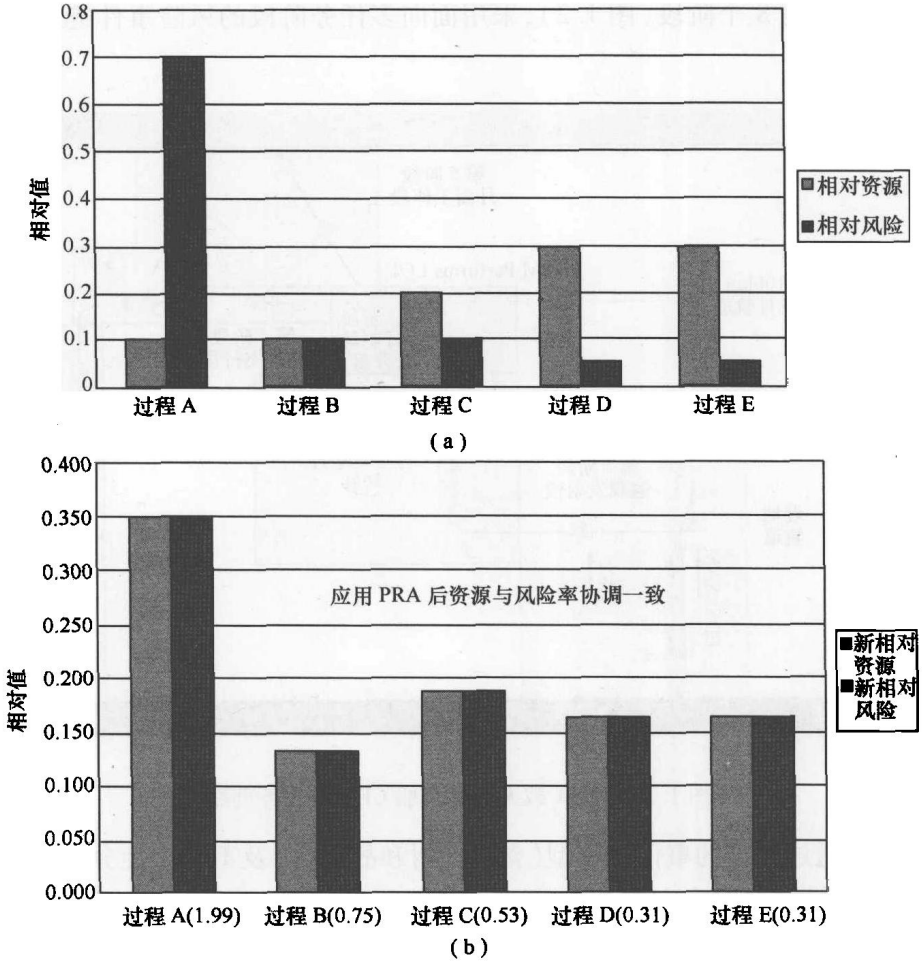

图 1.1 NASA 在使用 PRA 前后资源与风险之间的比例关系

(a)使用 PRA 前资源与风险的对比关系;(b)使用 PRA 后资源与风险的对比关系。

下面着重对各种航天型号(航天飞机、国际空间站、轨道空间飞机、外星探测器、卫星等)在方案阶段或研制/使用阶段的 PRA 应用进行介绍。