可靠性维修性保障性
学术专著译丛
丛书主编 康锐

可靠性与风险分析算法

Computational Methods for Reliability and Risk Analysis

【意】Enrico Zio 著
李 梓 主译
康 锐 主审

国防工业出版社
National Defense Industry Press

可靠性维修性保障性学术专著译丛

可靠性与风险分析算法

Computational Methods for Reliability and Risk Analysis

[意] Enrico Zio 著
李 梓 主译
康 锐 主审

国防工业出版社
·北京·

著作权合同登记　图字：军－2013－136 号

图书在版编目(CIP)数据

可靠性与风险分析算法/(意)齐奥(Zio,E.)著；
李梓主译. —北京：国防工业出版社，2014.8
(可靠性维修性保障性学术专著译丛)
书名原文：Computational methods for
reliability and risk analysis
ISBN 978-7-118-09644-6

Ⅰ.①可…　Ⅱ.①齐…②李…　Ⅲ.①系统
可靠性－风险分析－算法－研究　Ⅳ.①N945.17

中国版本图书馆 CIP 数据核字(2014)第 183606 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 710×1000　1/16　**印张** 13¼　**字数** 262 千字
2014 年 8 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 56.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777　　发行邮购：(010)88540776
发行传真：(010)88540755　　发行业务：(010)88540717

《可靠性维修性保障性学术专著译丛》
编 审 委 员 会

《可靠性维修性保障性学术专著译丛》
总　序

可靠性理论自20世纪50年代发源以来，得到了世界各地研究者的广泛关注，并在众多行业内得到了成功的应用。然而，随着工程系统复杂程度的不断增加，可靠性理论与方法也受到了日益严峻的挑战。近年来，许多国际知名学者对相关问题进行了深入研究，取得了一系列显著的成果，极大地丰富和充实了可靠性理论与方法。2012年，国际知名出版社Springer出版了一套“可靠性工程丛书”，共计61种，总结了近年来可靠性维修性保障性相关领域内取得的绝大部分研究成果，具有很强的系统性、很高的理论与实用价值。

经过国内最近30年的普及和发展，可靠性的重要性已经得到业界的普遍认可，即使在民用领域，可靠性的研究与应用也发展迅猛。他山之石，可以攻玉，系统地了解国际上可靠性相关领域近年来的最新研究成果，对于国内的可靠性研究者与实践者们都会大有裨益。为此，国防工业出版社邀请北京航空航天大学可靠性与系统工程学院以Springer出版的可靠性工程丛书中的10种，外加Wiley、World Scientific、Cambridge、CRC、Prentice Hall出版机构各一种，共15种专著，策划组织了《可靠性维修性保障性学术专著译丛》的翻译出版工作。我具体承担了这套丛书的翻译组织工作。我们挑选这15种专著的基本原则是原著内容是当前国内学术界缺乏的或工业界急需的，主题涵盖了相关领域的科研前沿、热点问题以及最新研究成果，丛书中各专著原作者均为相关领域国际知名的专家、学者。

组织如此规模的学术专著翻译出版工作，我们是没有现成经验的。为了保证翻译质量和进度，在组织翻译这套丛书的过程中，我们做了以下几方面的工作：一是认真遴选主译者。我们邀请了国内高校可靠性工

程专业方向的在校博士生作为主译者，这些既有专业知识又有工作激情的青年学者对翻译工作的投入是保证质量与进度的第一道屏障。二是真诚邀请主审专家。我们邀请的主审专家要么是这些博士生的导师，要么是这些博士生的科研合作者，他们均是国内可靠性领域的知名专家，他们对可靠性专业知识把握的深度和广度是保证质量与进度的第二道屏障。三是建立编审委员会加强过程指导。我们邀请了国内知名专家与主审专家一起共同组成了丛书编审委员会，从丛书选择、翻译指导、主审主译等多个方面开展了细致的工作，同时为了及时沟通信息、交流经验，我们还定期编辑丛书翻译工作简报，在主译者、主审者和编审委员中印发。可以说经过以上工作，我们坚信这批专著的翻译质量是有保证的。

本套丛书适合于从事可靠性维修性保障性相关研究的学者和在校博士、硕士研究生借鉴与学习，也可供工程技术人员在具体的工程实践中参考。我们相信，本套丛书的出版能够对国内可靠性系统工程的发展起到推动作用。

北京航空航天大学可靠性与系统工程学院

康　锐

2013 年 11 月 8 日

PREFACE

Today's modern systems have become increasingly complex to design and build, while the demand for reliability and cost effective development continues. Thus, reliability has become one of the most important attributes in these systems. Growing international competition has increased the need for all designers, managers, practitioners, scientists and engineers to ensure a level of reliability of their product before release at the lowest cost. This is the reason why interests in reliability have been continually growing in recent years and I believe this trend will continue during the next decade and beyond.

It is these growing interests from both industries and academia that motivate Springer to publish the Springer Series in Reliability Engineering, for which I serve as the series editor. This series consists of books, monographs and edited volumes in important subjects of current theoretical research development in reliability and in areas that attempt to bridge the gap between theory and application in fields of interest to practitioners in industry, laboratories, business and government.

I am very delighted to learn that the National Defense Industry Press from China is planning to translate selected books from the Springer Series as well as some other distinguished monographs from other presses into Chinese. The books in the collections to be translated cover most of the timely and important topics in reliability research areas and are of great values for both theoretical researchers and engineering practitioners.

The translations are organized and managed by Professor Rui Kang from Beihang University, who is a world-wide leading expert in reliability related areas. With his expertise and dedication, the quality of the translations is guaranteed. I'm sure that the translations of these outstanding books will be a great impetus to the research and application of reliability engineering in China.

Personally, I will treat the translation collection as an attempt to exchange ideas of reliability researchers in the international community with their Chinese counterparts. I really hope that these kinds of idea interchanges will be more common and frequently in the future. Specifically, I am really looking forward to hearing more from our Chinese colleagues. Wish the research and application of reliability in China a bright future!

Hoang Pham

Dr. Hoang Pham, IEEE Fellow
Distinguished Professor
Rutgers University
Series Editor, Springer Series in Reliability Engineering

序

不断发展的科技和日趋激烈的市场竞争对产品提出了日趋强烈的可靠性需求，希望能够以尽可能低的成本高效保证产品可靠性。可靠性业已成为现代工程系统最重要的属性之一。面向这种需求，Springer 出版社组织出版了《Springer 可靠性工程丛书》。这套丛书由 61 种专著组成（截止到 2013 年 11 月），涵盖了近年来可靠性相关领域内取得的最新理论成果，介绍了可靠性工程在实际工程上的应用，具有很强的理论和实践价值。

作为《Springer 可靠性工程丛书》的主编，我很高兴中国的国防工业出版社计划将这套丛书中的部分专著以及其他一些近年出版的可靠性优秀英文专著翻译出版，推出《可靠性维修性保障性学术专著译丛》。《可靠性维修性保障性学术专著译丛》中的专著选题覆盖了可靠性领域近期的大部分研究热点和重要成果，具有重要的理论价值和实践指导意义。

这套丛书的翻译工作由北京航空航天大学的康锐教授负责组织。康锐教授是国际知名的可靠性专家，我相信，康锐教授的专业知识和奉献精神，能够有效保证译著的质量。我确信，这些优秀专著的翻译出版将极大地推动中国的可靠性研究和应用工作。

就我个人而言，我更愿意将《可靠性维修性保障性学术专著译丛》看作是可靠性领域内的国际学者与中国同行们进行的一次思想交流。我期待这样的交流在未来更加频繁。特别地，希望中国优秀学者们能够更多地以英文出版学术专著，介绍他们的学术成果，从而向可靠性领域的国际同行们发出来自中国的声音。衷心祝愿中国的可靠性事业更上一个台阶！

Hoang Pham
博士，IEEE 会士
罗格斯大学特聘教授
Springer 可靠性工程丛书主编

译者序

随着现代高新技术和工业建设的迅速发展，许多大型复杂系统不断产生，对人类社会生活水平的提高发挥了重要作用，但由于产品设计、制造、使用等环节出现问题，这些系统也会发生故障，甚至造成严重的生命财产损失。

近些年，从可持续发展和环境保护的角度出发，我国大力发展核电站建设，目前已成为世界在建核电机组规模最大的国家。核电站是我国经济社会发展的重要组成部分，值得注意的是，其安全可靠供电是实现一切功能的前提。2011 年 3 月 11 日，日本宫城县东方外海发生的强烈地震及其引起的海啸，在福岛第一核电站造成一系列设备损毁、堆芯熔毁、辐射释放等灾害事件，造成了严重的人员伤亡、环境污染和经济损失。

铁路是我国重要的交通运输载体，2013 年，全国铁路累计发送旅客 20.75 亿人次，在经济社会运行发展中扮演了重要的角色，因此保证其安全可靠是设计、生产、使用、管理部门的重要职责。2011 年 7 月 23 日，因列控中心设备存在严重设计缺陷、上道使用审查把关不严、雷击导致设备故障后应急处置不力等因素，甬温线动车发生重大交通事故，造成 40 人死亡，200 多人受伤。

从资料中可以看到，小到手机、电脑等电子产品，大到互联网、水利等关键基础设施，遍布生产生活方方面面的系统，与人身安全和经济效益密切相关，应该从设计、生产、使用、管理等各个方面完善、提高产品的可靠性和安全性。对系统进行风险分析，是防止故障和事故发生、提高产品可靠性和安全性的前提之一。可靠性和风险分析涉及广泛，综合了系统工程、概率、统计、运筹和物理等多种学科的成果，经过半个多世纪的发展，已形成了诸多理论和技术。经典的安全防护措施是识别系统最坏情况，对造成最坏情况的事件进行深度防御。但是这种方法存在两个方面的问题：一是在定义“最坏”的过程中包含人的主观臆断，可能导致与实际情况的偏差；二是防护措施过于保守，成本较高，限制系统功能。因此，人们提出了更为合理的定量分析方法，运用概率风险评估，更为客观、高效地实现系统可靠安全保障。

本书是可靠性系统工程和安全工程领域理论和应用相结合的基础著作，阐述了复杂技术系统可靠性和风险分析的多种概率统计相关算法，同时运用数值算例对理论进行支撑，书中大量的图表直观、形象地描述和解释了理论与案例。该书作者 Enrico Zio 教授为可靠性工程与系统安全工程的专家，同时在巴黎中央理工学院（École Centrale Paris，俗称巴黎中央或 ECP）与米兰理工大学（Politecnico di Mi-

lano)任教,担任欧洲安全与可靠性协会(European Safety and Reliability Association,ESRA)主席,并担任多个可靠性与安全性领域期刊的编委。该书内容全面详实,基础性强,适合作为高年级本科生或研究生课程教材,或作为本领域研究者的基础理论资料。

本书共包括7章。第1章介绍了用马尔可夫方法对系统建模并进行可靠性和可用性分析的基础。第2章从直观和实用的层面上简要介绍了可靠性和可用性分析的蒙特卡罗仿真理论。第3章介绍了马尔可夫链蒙特卡罗方法,即将马尔可夫方法的建模能力和蒙特卡罗仿真的计算能力相结合,为高维空间的复杂概率分布提供了有效的抽样方法,并将其应用于零部件和结构的失效和退化行为分析中。第4章阐述了RAMS(可靠性、可用性、维修性和安全性)优化中遗传算法的理论及应用,用于对系统配置和维修决策提供支持。第5章讨论了相关失效,并阐述了用模型表示相关失效对系统可靠性影响的方法。第6章主要介绍了可靠性和风险分析中重要性度量的概念,它通常用于定量分析零部件对系统性能(如可靠性、可用性或安全性)的影响,有助于定位系统薄弱环节,并迅速提供有效改善措施。第7章主要介绍了灵敏度和不确定性分析中的一些基本概念,该方法在对系统行为了解不够全面的情况下,为复杂系统的可靠性和风险分析提供支持。

本书由北京航空航天大学博士研究生李梓主译,康锐教授主审。北京航空航天大学故障学基础理论实验室的研究生协助译者进行了本书初稿的翻译,并完成了全书公式的录入,对他们的辛勤工作,译者谨在此表示衷心的感谢(以参与翻译的章节顺序为序):黄榕(第1、2章)、肖莹(第3、5章)、樊可嘉(第4章)、曲思学(第6章)、李梓(第7章及附录)。在本书的翻译、出版过程中,得到了国防工业出版社白天明编辑与胡翠敏编辑、北京航空航天大学博士研究生曾志国的悉心指导和帮助,在此向他们致以由衷的谢意。

由于时间仓促和译者水平有限,翻译中难免有不妥之处,敬请广大读者批评指正。

译者

2014年5月28日

前　言

可靠性和安全性是现代技术系统应该具备的基本属性。实践中，为防止系统运行时发生危险，人们设置了多种保护屏障。这些屏障的作用是在零部件、硬件、软件、人为或组织等方面出现故障时，使系统不受到损害。相应地，系统的可靠性和风险分析就是对该系统及其保护屏障的故障发生概率进行量化。

可靠性和风险分析中一个基本的问题就是故障发生的时间和影响的不确定性。为了实现系统安全，必须保证系统免受不确定的事故的损害。

为了避免不确定的事故对系统造成损害，一个经典方法如下：

（1）确定能够导致最坏情况的失效事件序列组，记为$\{s^*\}$（设计基准事故）；

（2）预测失效事件的影响$\{x^*\}$；

（3）为防止上述事件的发生，并避免或降低不利影响，设计合适的安全屏障。

这种“结构主义”和“深度防御”的方法，通过系统设计和运行中保守的监管机制为系统增加了安全裕度。设计和运行的准则是：识别出的最坏情况，应包括对系统及其防护措施产生压力的所有事故。这一设置的基本原理是：如果将一个系统设计为可以承受所有最坏情况事故，那么理论上，它可以防范所有事故[1]。

这种方法作为一种经典方法在很多技术实践中进行了应用。它在保护系统免受来自零部件、系统和结构的未知的不确定的故障行为的损害时，无需直接量化，即可提供合理的保护，降低系统运行的风险。但是，实际上，人们在定义“最坏”时包含了主观臆断，这就可能导致在对事故情况进行考虑和分析时出现偏差，虽然可能性很小，但仍可能导致严重的后果。这也会导致对产品实施的监管过于严格，引起系统及其保护屏障的设计和运行过分保守，并最终抑制行业的发展。这种情况在核工业、航空航天工业和加工工业等尤为突出。

基于以上问题，人们提出了一种更合理的定量分析方法，应用于危险系统安全措施的设计、规范和管理。这种方法开始于20世纪60年代在核能源利用和航空航天领域投入增长的推动，其理念是从定量的角度处理事故预防和影响控制的防护系统可靠性，并且不再从主观上区别事故的大小、可信与不可信[2]。这种方法基于概率对事故发生和发展的不确定性进行处理，科学家们进行了大量研究来证实其优点[3]。这些研究的成果促成了第一个完备的核电装置的概率风险评估[4]。大量的工作表明导致风险的主要因素不一定是设计基准事故，这个“革命性”的发现打破了以前“结构主义”的、“深度防御”的系统安全理念[1]。

按照上述思路，通过概率法对风险进行分析的方法（Probabilistic Risk Analysis，PRA）已成为一种有效的系统安全分析方法。它并不仅仅局限于对最坏情况事件的考虑，而是放眼于所有可能出现的情况及其影响，将这些事件出现的概率进行定量分析，是一种更为合理的处理不确定性的方法[4-11]。这种新的安全规范的思路，同时考虑事件发生的概率和影响，是一种“理性客观”的深度防御方法。用此方法进行安全分析和规范时，可靠性工程在评估事故发生概率方面起到了重要的作用。

本书阐述了复杂技术系统可靠性和风险特征的多种计算方法。书中对支撑这些方法的理论进行的介绍是教学性质的，但提供的实例能够更清楚地说明这些方法在各领域中的应用。

第1章介绍了用马尔可夫方法对系统建模并进行可靠性和可用性分析的基础。在这种方法中，系统演化是随时间变化的一个随机过程，用系统状态、状态间的相互转换和状态发生的概率来描述。不同的系统状态由组成系统的零部件的状态来定义。零部件不仅限于两种状态，可以存在多种状态，如运行、待机、退化、部分失效、完全失效、维护等；此外，一个零部件不同的失效模式也可以定义为不同的状态。两个状态之间的转换在时间上是随机的，这是因为诱发系统状态的机理和事件是随机的，如失效、维修、更换和切换运行等。在规定条件下，系统演化的随机过程称为马尔可夫过程，在数学上用概率方程体系来描述，便于用解析或数值的方法分析。

第2章简要介绍了可靠性和可用性分析的蒙特卡罗仿真理论，主要是从直观和实用的层面上进行的。蒙特卡罗仿真的方法能够非常真实地反映系统的随机行为，是复杂系统分析的强有力工具。总体而言，它可以定义为一种通过生成随机数对数学问题的解进行估计的方法。这里所说的随机数早期是赌城蒙特卡罗的赌场中像转盘一样的机器生成的数字，此即蒙特卡罗方法名字的由来。在现代计算机产生之前，人们利用随机抽样数字进行仿真。蒙特卡罗方法的首次使用可以追溯到18世纪法国的博物学家布丰（Buffon）（1707—1788），考虑一个平面上有一组平行的直线，直线之间距离为 D，有一个长度为 $L < D$ 的线段，随机地放在平面上，计算线段与直线相交的概率 P。他得到的理论表达式为

$$P = \frac{L/D}{\pi/2}$$

由于无法确定这一结果的正确性，布丰设计了一个实验来验证这一表达式。他在地板上画了一组平行线，重复向地上抛一根针，用针和平行线相交的次数除以抛针的总次数来估计概率 P，并因此成为蒙特卡罗方法的发明者。有意思的是，拉普拉斯注意到布丰的实验隐含了一种通过向平行直线上抛针来计算 π 的方法。接着，很多科学家利用相同的方法解决了一些积分和概率问题。这一方法的复兴得益于第二次世界大战时期，费米（Fermi）、冯·诺依曼（von Neumann）和乌拉姆（Ulam）对曼哈顿计划的提出。当时，为设计核装置的屏蔽得到了一个六维积分方程，蒙特

卡罗方法成为解这一积分方程的唯一选择。这可能是人类历史上第一个使用试错法解决问题的案例,但显然太冒险了。目前,蒙特卡罗方法可以说是解决复杂多维问题的唯一方法。在约 30 年间,它在核技术中得到了广泛的应用,但却几乎只用于核技术。据推测,这是由于蒙特卡罗方法占用计算机大量的内存,并且十分耗时。随着计算机的运算速度越来越快,蒙特卡罗方法在各个领域的应用也越来越广泛,其中也包括可靠性和风险分析。

第 3 章将马尔可夫方法的建模能力和蒙特卡罗仿真的计算能力结合了起来,这就是马尔可夫链蒙特卡罗方法的由来,它为高维空间的复杂概率分布提供了有效的抽样方法。该方法可以用于图像重构、参数识别、统计力学系统的均衡分布与相关能量水平的计算、逆问题的解决等,并且更普遍地应用于贝叶斯后验推理。应用的实例是关于零部件和结构的失效以及退化行为的特征分析。

第 4 章阐述了 RAMS(可靠性、可用性、维修性和安全性)优化中遗传算法的应用,以及支撑遗传算法的理论。通过传统和高级育种描述了算法的实现步骤。适应度函数是优化的目标,本章对适应度函数仿射变换的必要性和变换本身进行了细节上的讨论。最后,给出了两个可靠性分配和定期检验维护问题的应用实例。系统设计和运行时不同的选择以及测试和维护过程会对一些系统属性产生影响,RAMS 优化则是以量化这些影响为基础的。相应的系统属性例如:

- $R(\boldsymbol{x})$为系统可靠性;
- $A(\boldsymbol{x})$为系统可用性(系统不可用性 $U(\boldsymbol{x}) = 1 - A(\boldsymbol{x})$);
- $M(\boldsymbol{x})$为系统维修性,即测试和维护导致的不可用性;
- $S(\boldsymbol{x})$为系统安全性,通常由系统的风险度量 Risk($\boldsymbol{x}$)量化(如通过概率风险分析进行评估)。

其中,$\boldsymbol{x}$ 表示设计、运行和维护决策变量的向量。定量模型可以用于评估设计、运行和维护的选择如何影响系统的 RAMS 属性和相应的成本($C(\boldsymbol{x})$为执行选择向量 $\boldsymbol{x}$ 所需的成本)。这样,设计、运行和维护问题可以化为一个多准则决策问题,相应的设计和维护参数(如冗余配置、零部件失效率、维护周期和测试频率等)就可作为备选向量 $\boldsymbol{x}$。这个多准则决策问题的目标就是对可靠性设计、测试和维护过程中的各变量进行适当的选择,以最优地平衡 RAMS 和成本(RAMS&C)属性。总体来看,决策变量 $\boldsymbol{x}$ 对固有设备可靠性(如每次指令的失效概率、瞬时失效率等)和系统逻辑配置(如冗余队列数量等)进行编码。系统逻辑配置决定了系统可靠性的分配,以及测试和维护(如测试间隔、维护周期、更新期、维护效率、平均维修时间、允许停机时间等)相关的配置,表征了系统可用性和维修性的水平。

第 5 章讨论了相关失效的一些问题,并阐述了用模型表示相关失效对系统可靠性影响的方法。这是可靠性和风险分析中的一个重要方面。虽然现代所有的系统都具备高度冗余,但相关失效仍然能够突破冗余防护,导致整个系统的失效,显著地提高了系统风险。因此,定量分析相关失效对于降低风险的作用是很有必

要的。

第6章主要介绍了可靠性和风险分析中重要性度量的概念。从宏观角度看，重要性度量用于定量分析零部件对系统性能（如可靠性、可用性或安全性）的影响。例如，重要性度量的计算是核电厂概率风险评估的相关结果之一，核电厂可以就零部件对整个系统风险的贡献来评价它们之间的关联性，通常有堆芯熔化频率（Core Damage Frequency，CDF）或大规模早期释放频率（Large Early Release Frequency，LERF）等指标。对于其他系统工程应用，如航空航天和交通运输中，零部件主要影响系统的不可靠性，而在生产制造设备和发电设备等系统中，零部件主要影响系统的不可用性。组成系统的零部件的重要度信息，对系统安全性和可用性起到重要作用。实际上，识别对整个系统行为影响最大的零部件可以帮助我们定位系统的瓶颈，并迅速提供有效的措施对系统加以改善。

第7章主要介绍了灵敏度和不确定性分析中的一些基本概念。灵敏度和不确定性分析是在对系统行为了解不够全面的情况下，为复杂系统的可靠性和风险分析提供支持。实际上，如开头提到的，不确定性是对系统行为以及失效极限产生影响的无法避免的因素。于是，不确定性出现在参数值和用来表示系统故障行为模型的结构的假设中。这种不确定性在计算系统可靠性和风险的模型中不断传递，而可靠性和风险也同时成为不确定的。我们通过收集系统、零部件和过程的代表性数据，不断加深对系统的认识和理解，但是不确定性的准确描述、表示方法、传递和诠释仍是可靠性和风险分析中的一个重要方面。在不确定性方面，可靠性和风险分析的最终目标是对分析的结果进行充分的认识，并为决策者提供帮助。这使得我们成功地解决了一些问题[12]：

（1）如何搜集信息（如以专家判断的形式）并把信息输入到正确的数学形式中；

（2）如何将多个不同来源的信息整合成一种不确定性的表示形式；

（3）如何确定不确定性在模型中的传递，以在分析结果中得到不确定性的适当的表示形式；

（4）如何以一种容易理解并且有用的形式向决策者呈现并解释不确定性的结果；

（5）如何进行灵敏度分析，以从输入不确定性控制输出不确定性的方面提供依据，来引导资源向不确定性有效减少的方向发展。

总的来说，不确定性可以分为两种：一方面是由于系统本身固有的不一致性导致的随机性（如系统随机行为所产生的不同结果）；另一方面是由于对系统缺乏全面的认识和了解所导致的不明确[12,13]。前一种不确定性通常被称作是客观的、偶然的、随机的，后一种则被称作是主观的、认知的和与知识水平相关的。由认知导致的不确定性可以通过增加对系统的认识和了解来减少，而偶然的不确定性则不能，因此它有时也被称为无法减少的不确定性因素。

偶然不确定性和认知不确定性的区别在对复杂工程系统（如核电厂）进行风险评估时扮演了非常重要的角色。在风险分析中，偶然不确定性与不同事件的发

生有关，认知不确定性则是由于在对概率和事件结果的估计时存在固定的但知之甚少的输入参数值导致的[13]。

在现有的可靠性分析和风险评估实践中，两种不确定性均是通过概率分布的方式处理的[6]。在可靠性和风险分析中，人们主张使用不同的方法表示不同的不确定性[12,14-16]，问题是，不确定性是否可以单纯地用一种概率表示，或者说是否需要利用不精确的（区间）概率给出一种更广泛的不确定性的表示形式[17-20]。人们也质疑概率是否只能表示二元的并且精确定义的事件的不确定性。建议的解决方法包括模糊可靠性[21-23]和可能性[24-26]的概念。此外，依据证据理论，有人质疑概率并不能准确地反映它们所依据的证据的权重[27]。

为不同来源的不确定性找到最合适的表示方法至今仍存在争议，需要进一步加以讨论。本章只讨论用概率的方法表示不确定性，这是目前在实践中应用最广泛的一种方法。最近发表了一篇关于不确定性不同表示方法的评论文章，其出发点是不确定性的完整数学表示应当包括对基本概念的明确解释[28]。这篇评论还说明这些解释可以用不同的简化程度和精确度表示。

从本书内容的角度看，大部分用来阐述和解决上述计算方法和问题的材料都已在复杂系统可靠性和风险评估的文献专著中阐释了。可靠性和风险分析是一门综合性很强的学科，本书虽然还不能彻底地囊括这门学科中的所有内容，但是可以作为高年级本科生或研究生课程的教材或开始研究本领域的研究者的基础资料。以此为目标，本书提供了一些数值算例来支持介绍的理论。

最后，我要感谢对本书提供大力支持的人们。特别感谢美国麻省理工学院（Massachusetts Institute of Technology）的 George Apostolakis 教授（第 7 章），意大利米兰理工大学（Politecnico di Milano）的 Marzio Marseguerra 教授（第 2、4 章），瑞士保罗谢勒研究所（Paul Scherrer Institute）的 Luca Podofillini 博士（第 1、4、6 章）和意大利米兰理工大学（Politecnico di Milano）的 Andrea Zoia 博士（第 3 章）对以上章节内容及实例的贡献。还要感谢 Giulio Gola 博士（哈尔登反应堆项目，Halden Reactor Project）根据第 7 章内容对意大利语讲义的初始翻译。最后我要感谢意大利米兰理工大学（Politecnico di Milano）正在我的指导下攻读博士学位的 Francesco Di Maio，感谢他编辑这本书时的认真、一丝不苟以及所投入的热情（他有如此的动力可能是因为在学习这门课时研究我的课程原始讲义太痛苦了）。

Enrico Zio 于米兰

2008 年 7 月

参 考 文 献

[1] Apostolakis G. E., PRA/QRA: An Historical Perspective, 2006, Probabilistic/Quantitative Risk Assessment Workshop, 29 - 30, November 2006, Taiwan.

[2] Farmer, F. R., The Growth of Reactor Safety Criteria in the United Kingdom, Anglo - Spanish Power Symposium, Madrid, 1964.

[3] Garrick, B. J. and Gekler, W. C., Reliability Analysis of Nuclear Power Plant Protective Systems, US Atomic Energy Commission, HN - 190, 1967.

[4] WASH - 1400, Reactor Safety Study, US Nuclear Regulatory Commission 1975.

[5] NASA, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, 2002.

[6] Aven, T., Foundations of Risk Analysis, Wiley, 2003.

[7] Bedford, T. and Cooke, R., Probabilistic Risk Analysis, Cambridge University Press, 2001.

[8] Henley, E. J. and Kumamoto, H., Probabilistic Risk Assessment, NY, IEEE Press, 1992.

[9] Kaplan, S. and Garrick, B. J., Risk Analysis, 1, p. 1 - 11, 1984.

[10] McCormick, N. J., Reliability and Risk Analysis, New York, Academic Press, 1981.

[11] NUREG/CR - 2300, PRA Procedures Guide, Vols. 1&2, January, 1983.

[12] Helton J. C., Alternative Representations of Epistemic Uncertainty, Special Issue of Reliability Engineering and System Safety, Vol. 85, 2004.

[13] Apostolakis G. E., The Concept of Probability in Safety Assessments of Technological Systems, Science, 1990, pp. 1359 - 1364.

[14] Cai K. - Y., System Failure Engineering and Fuzzy Methodology. An Introductory Overview, Fuzzy Sets and Systems 83, 1996, pp. 113 - 133.

[15] Da Ruan, Kacprzyk J. and Fedrizzi M. Eds, Soft Computing for Risk Evaluation and Management, Physica-Verlag, 2001.

[16] Soft Methods in Safety and Reliability, Special Sessions 1 - 111, Proceedings of ESREL 2007, Stavanger, Norway, 25 - 27 June 2007, Volume 1.

[17] Moore R. E., Methods and Applications of Interval Analysis, Philadelphia, PA: SIAM, 1979.

[18] Coolen, F. P. A., On the Use of Imprecise Probabilities in Reliability, Quality and Reliability Engineering International, 2004, 20, pp. 193 - 202.

[19] Coolen, F. P. A. and Utkin, L. V., Imprecise Probability: A Concise Overview, In Aven, T. & Vinnem, J. E. (eds) Risk, reliability and societal safety, Proceedings of the European Safety and Reliability Conference (ESREL), Stavanger, Norway, 25 - 27 June 2007, London, Taylor & Francis.

[20] Utkin, L. V. and Coolen, F. P. A., Imprecise Reliability: An Introductory Overview, In Levitin, G. (ed.) Computational Intelligence in Reliability Engineering - New Metaheuristics, Neural and Fuzzy Techniques in Reliability, Springer, 2007.

[21] Zadeh, L. A., Probability Measures of Fuzzy Events, Journal of Mathematical Analysis and Applications, 23, 1968, pp. 421 - 427.

[22] Klir G. J., Yuan B., Fuzzy Sets and Fuzzy Logic: Theory and Applications, Prentice Hall, 1995.

[23] Gudder, S., What is Fuzzy probability theory?, Foundations of Physics 30(10), 2000, pp. 1663 - 1678.

[24] Zadeh L. A., Fuzzy Sets, Information and Control, Vol. 8, 1965, pp. 338 - 353.

[25] Unwin, S. D., A fuzzy Set Theoretic Foundation For Vagueness in Uncertainty Analysis, Risk Analysis

6(1), 1986, pp. 27 – 34.

[26] Dubois D. and Prade H., Possibility Theory: An Approach to Computerized Processing of Uncertainty, New York, Plenum Press, 1988.

[27] Shafer G., A Mathematical Theory of Evidence, Princeton, NJ: Princeton University Press, 1976.

[28] Flage, R., Aven, T. and Zio E., Alternative Representations of Uncertainty in System Risk and Reliability Analysis: Discussion, Proceedings of ESREL 2008, Valencia Spain, 22 – 25 September 2008.