可靠性维修性保障性
学术专著译丛
丛书主编 康锐

软件工程师可信计算基础

Fundamentals of Dependable Computing for Software Engineers

【美】John Knight 著
古廷阳 主译
陆民燕 主审

CRC Press
Taylor & Francis Group
国防工业出版社
National Defense Industry Press

装备科技译著出版基金

可靠性维修性保障性学术

软件工程师可信计算基础

Fundamentals of Dependable Computing for Software Engineers

[美] John Knight 著

古廷阳 主译

陆民燕 主审

国防工业出版社

·北京·

著作权合同登记　图字:军-2014-003号

图书在版编目(CIP)数据

软件工程师可信计算基础/(美)莱特(Knight,J.)著;
古廷阳主译. —北京:国防工业出版社, 2014.12
(可靠性维修性保障性学术专著译丛)
书名原文: Fundamentals of dependable computing for software engineers
ISBN 978-7-118-10006-8

Ⅰ. ①软...　Ⅱ. ①莱...　②古...　Ⅲ. ①电子计算机-安全技术
Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2015)第043882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** 22¼　**字数** 416千字
2014年12月第1版第1次印刷　**印数** 1—2000册　**定价** 78.00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》

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

随着计算机系统广泛应用于各行各业，人们的生活和工作、组织的管理与运行越来越依赖于计算机系统，国家和军队的正常管理和运行也越来越依赖于计算机系统的可信运行。然而，社会对于计算机系统依赖程度的增加，使得计算机系统所承担的功能越来越多，复杂程度大幅提升，这使得计算机系统自身的可信运行受到了巨大的挑战。因此，系统的可信性、软件的可信性越来越受到关注。

软件可信性是最近三十年发展起来的新兴研究领域，它是集计算机科学与技术、软件工程、可靠性工程、统计学、管理学于一体的前沿交叉学科。近年来，软件可信性问题已引起国内外广大学者和实践者的普遍关注，各种政府组织、大型公司和科研机构也纷纷提出相应的研究计划。美国在《国家软件发展战略》(Software 2015)报告中，将高可信软件的开发作为下一代软件工程的首要课题。美国自然科学基金会于2006年—2008年三年间投入近1.52亿美元用以可信软件研究，并在加州大学设立科学与技术研究中心。此外，NASA、卡内基梅隆大学、德国教育研究部等也都提出了相关的研究计划。我国由信息科学部、数学物理科学部和管理科学部联合组织，于2008年初正式启动了“可信软件基础研究”重大研究计划，围绕可信软件的核心科学问题进行研究，旨在推动我国软件基础理论的探索与创新，促进国家软件产业及相关应用领域的发展。由此可以看出，计算机系统的可信性已成为目前研究的热点。

本书是CRC出版公司规划并出版的系统可信性系列图书之一，作者是美国弗吉尼亚大学计算机科学系的John Knight教授。John Knight教授获得了伦敦帝国理工学院理学学士学位和纽卡斯尔大学的计算机科学博士学位，在加入弗吉尼亚大学计算机科学系之前曾在美国宇航局的兰利研究中心工作。John Knight教授的研究领域包括可信性、生存性等方面，目前已发表150余篇学术论文，在软件工程领域和软件可信性领域享有较高的声誉。

本书根据John Knight教授的*Fundamentals of Dependable Computing for Software Engineers*一书翻译而成，是计算机系统可信性领域的前沿著作。本书介绍了计算机系统可信性的相关理论知识及具体的应用，并重点从软件工程师的角度对于计算机系统可信性进行了阐述。

本书不仅阐述了可信性的理论、技术和方法，还建立了一套明确的系统可信性的概念，同时凝聚了作者多年从事该领域研究所获得的宝贵经验，并将近年来的最

新研究成果包含其中。因此，本书对于国内正在兴起的软件可信性研究具有重要的指导意义和参考价值。本书的翻译可为相关研究人员、大学生、研究生提供很好的参考教材，也可以为软件工程从业人员提供工具和指导。

本书的翻译工作历时一年。由于本书较为前沿，涉及的很多概念和术语没有成熟的中文翻译可供参考，同时由于全书篇幅较大，因此由几位译者共同翻译完成，期间参考了大量软件工程、软件可靠性、软件可信性的相关书籍，进行了大量的讨论，并由几位译者和主审进行了术语的统筹和一致化处理。

本书由古廷阳、张虹、王轶辰、李秋英共同翻译完成，陆民燕教授担任主审。具体翻译分工如下：序言、引言以及第一章至第三章由古廷阳翻译；第四章至第六章由张虹翻译；第七章至第九章由王轶辰、古廷阳、李璐祎共同翻译；第十章至第十二章由李秋英翻译。全书翻译由古廷阳统筹并整理，由陆民燕教授审阅并校对，部分章节由李璐祎进行了审阅和修改。在本书的翻译、出版过程中，得到了北京航空航天大学康锐教授、国防工业出版社白天明编辑的悉心指导与帮助，在此向他们表示衷心的感谢。

由于时间仓促和水平有限，翻译难免有不妥之处，敬请广大读者批评指正。

译 者

2014 年 10 月

序　言

随着计算机系统已渗透到日常和公共生活的多个方面，个人、组织和社会越来越依赖于这些系统的满意运行。这种依赖关系可以有多种形式，例如，生产商召回不满足可靠性要求的大众市场产品带来的成本，由于计算机系统引发或未能阻止的不安全操作所造成的生命危险，或由于未能保护高度机密的信息而带来的信誉或财务的损失。

计算机系统可以应用于许多不同的情况，也可能以很多不同的方式失效。如果一个系统的失效既不是过于频繁，也不是太过严重，那么我们可以认为它是可信的。什么是失效、可接受的故障频率和故障严重程度，将会根据不同的情况和环境而不同。不同的利益相关者，如用户、运营商和系统所有者可以有不同的判定。

正如计算机系统可以以不同的形式发生失效，电脑系统发生失效可能有许多不同的原因，即各种不同类型的故障。尤其是由于元件老化出现的硬件操作故障、软件（和硬件）中残留的设计缺陷和用户故意的（或者只是偶然的）行为触发鲜为人知的漏洞。此外，一个系统中的故障可能是由其他一些系统中的故障引起的，即可与之发生交互的另一个系统、一个组件的子系统或创建和修改它的系统。因此，系统的边界问题和如何识别系统边界是至关重要的。事实上，如果参与的工程师没有详细的了解系统的边界和规范，那么系统就很难达到较高的可信性。

因此，在比以往都更加复杂的计算机系统中实现或证明已实现了足够的系统可信性是一个持续的挑战。不受控的复杂性产生了混乱，而混乱则产生了不可信。因此，正如本书的作者约翰·奈特所强调的，清晰的概念和仔细定义的术语是十分重要的。这本书中他介绍的和慎重使用的概念和术语适合所有类型的系统，例如，一个“可编程”的洗衣机、具有复杂操作系统的移动电话、一个支持大型软件设计团队工作的分布式数据库系统，以及包括大量计算机、网络和工作人员的全球银行系统。

从概念上说，这些不同类型的系统以及由各类故障导致的可信性问题，其实都是非常相似的，即如何以及在何种程度上可以避免将故障引入到一个系统中，找到并删除在系统中存在的故障，尽管存在故障、也可提供可接受的服务，及估计这些各种措施的有效性。然而，在不同的技术团体中使用不同的术语，这种相似性可能会被掩盖。如果我们对于应用于不同种类的系统、不同类型的失效以及不同的引起失效的原因的基本概念有了充足的理解，那么术语上的区别就不那么重要了。

基于计算机的系统失效的根本原因之一是其复杂性，而其中很多失效是由于技术性的原因残留在软件中的，所以，计算机系统可信性的许多挑战都与软件和软件工程有关。因此，这本书的一大优势是以系统的方式识别并讨论了许多优秀的软件工程可以对系统可信性作出的贡献，以及在确保软件本身足够可信方面所面临的挑战。

本书充分利用了近年来为创造丰富的系统可信性概念而进行的大量工作。John Knight 很好的使用了这些概念，直接面向软件工程师，来充分论证和全面阐述了他们可能会在实际系统中发现的各种可信性问题，以及他们解决这些问题应该使用的策略。这本书对具有相关专业水平的学生，以及已经在自己的职业生涯中遇到各种可信性相关的问题并寻求更深入的理解可信性的计算机专业人员，应当有很大益处。因此，我非常高兴且满腔热情地把它推荐给这两类读者。

Brian Randell
纽卡斯尔大学
2011 年 7 月 31 日

引　言

我们依赖计算机完成非常多的工作，而且我们对计算机的依赖远比我们意识到的要多。如果计算机不能正确工作，我们的生活毫无疑问会变得十分糟糕。计算机服务涉及的范围十分广泛，包括银行、教育、交通运输、能源、通信、医疗、国防、制造业等。例如客运铁路系统，不止是动力缺失、铁轨损坏、极端恶劣天气之类的问题能够迫使其停止运行，计算机的故障也能够造成这种不利后果。

本书主要关注的是计算机系统的可信性，或者更准确的说，关注的是对于软件工程师十分重要的那些方面。本书可用作计算机科学及工程专业高年级本科生或一年级研究生教材，也可用作自学及从业人员查阅之用。

本书只有一个教学目标：向软件及计算机工程师们展现一个全面的可信性工程过程，而在这个过程中，做各种工作的理由及各工作之间的内部关系都是明确和合理的。

本书介绍了许多技术，但是除了对过程技术的介绍之外，不会过深的涉及任何专项技术。本书通过适当深度的总结各个重要的话题，旨在让读者了解这些内容的形式与角色，以及拥有可以继续深入研究的基础知识背景。通过了解整个的工程过程，读者可以自行选择研究特定内容的深度，并且按照需要应用到自己的工程活动中去。

为了达到这个目标，本书包括了以下 4 个主要方面的内容：

（1）系统工程中可信性方面的充足信息，因此软件工程师们能够充分理解软件被要求做现有工作的原因并且理解为什么人们将软件开发成运行在系统设计者指定的平台上。

（2）明确的概念框架，因此工程师们能够根据框架来对软件及其可信性进行判断及决策。

（3）实现软件可信性的综合方案。

（4）相关文献的参考书目。

为什么要阅读这本书

学生或者从业者为什么要学习这些材料呢？有许多的技术等着你去学习，那么这本书占据一个怎样的地位？答案就在本书的名字中。系统的可信性与系统的功能性一样重要，甚至更加重要。功能性与目标存在偏差通常是可以容忍的，但是

很难接受一个系统以较高的频率失效。

只有我们采取措施，失效才有可能不会发生。而且如果失效发生的频率超出人们的接受范围，那么相关的系统可能整个都会被废弃不用。从业者和学生们应该掌握计算机系统可信性理论中的基本元素，来帮助他们做出合适的工程决策。所以，阅读本书是必要的。

本书将教你怎样采取可能的措施来将失效率降低到一个可接受的范围内。你将学习到以下内容：

- 可信性为什么重要。
- 什么样的系统是可信的。
- 怎样构建可信的系统。
- 怎样去评估一个系统，看其是否可信。

为了能够顺利的阅读并理解本书，我们假设您已经有如下的知识基础：

- 有使用高级语言（如 C，C ++，C#，JAVA）编程的经验。
- 对计算机结构有基本的理解，包括处理器、内存、磁盘存储系统和基本的通信设备的运作方式。
- 有一定的概率论基础。
- 有离散数学的应用经验，包括命题演算、谓词演算、映射基础以及集合论。
- 对操作系统基本理论的了解，包括处理器管理、内存管理、外围设备管理和用户接口的操作。
- 熟悉和精通软件工程的基本准则，包括需求分析、需求说明、设计、测试、文档编写和软件的开发过程等。

本书的重点在于可信性问题中的软件工程元素。因此，希望能够帮助软件工程师们克服挑战，在有限的时间和资源的条件下，构建出足够可信的系统。

怎样阅读本书

计算机系统可信性应该作为任何计算机科学或计算机工程专业的学位课程之一。至少应该开设一门介绍该方向基本内容的课程，并且伴随有讲解更加深入的有关各部分内容的选修课程，如形式化方法、数学建模、可信的计算架构，还有按照学位要求不同而设置的各种进阶软件工程课程。

本书可以作为半年的导论课程的参考资料，并且本书的绝大部分内容都可以在一学期的时间中介绍的。由于后面部分的内容与前面章节紧密相关，因此建议课程的顺序也应该与书中内容的安排顺序相一致。学习本书之后，学生应该熟悉和掌握的内容如下：

- 可信性是什么以及可信性为什么重要。

- 有关可信性的大量且必须的概念理论体系。
- 关键软件运行的各种计算平台，以及这些平台是怎样影响到软件的。
- 在软件工程中出现的能够引起软件失效的难题。
- 能够显著提高软件质量的各种以数学为基础的技术，而且这些技术甚至可以应用在大型的软件系统中。

对于从业者来说，本书也可以作为一种参考。可以根据自己的兴趣及熟悉的领域，以任意顺序阅读本书。从我与许多工程师们的交流可信性的经验来说，他们其实对本书所涉及的很多内容都缺乏足够的背景知识。因此开始阅读时，能够掌握一些例如可信性概念体系的内容，是相当值得做的。

本书的结构

本书分为十二章，建议读者按照顺序阅读。每一章都是对前一章内容的应用和发展。第一章介绍了可信性，并且激励读者能够继续研究；第二章介绍了可信性工程的基本术语；第三章介绍几种不同的故障模式以及应对这些故障的处理措施；第四章讨论了怎样识别那些系统常常会发生的故障；第五章介绍了 4 种基本的故障应对机制：故障避免、故障消除、容错和故障预测，同时也对拜占庭故障进行了一些探讨；第六章总结了退化故障的相关问题，该种故障只会在硬件中发生；第七章介绍了围绕软件可信性的一般问题；第八章和第九章就软件容错方面的一些重要内容进行了探讨；第十章有关软件故障消除；十一章有关软件容错；十二章介绍了可信性评估。

致谢

很高兴有机会在此感谢在这本书的创作过程中给予我帮助的人，来自纽卡斯尔大学的 Brian Randell 为本书写了序言，他在过去的许多年中教会了我很多的事情。加州大学戴维斯分校的 Premkumar Devanbu，邀请我在 2001 年的国际软件可靠性大会上做了报告，这促使我开始了这本书的材料收集工作；来自于 Kaiserlauten 大学的 Dieter Rombach 邀请我帮助开设一门关于可信性的远程学习课程，这促使我开始了这本书的材料组织工作。

这本书中的详细信息来自于我在弗吉尼亚大学教授的课程。我十分感谢那些选修了这门课的学生，他们接受了我的讲课风格，问了我许多十分具有建设性的问题，我也从学生们的身上学习了很多。非常感谢你们，你们所有人！

感谢 M. Anthony Aiello，Tom Anderson，Josh Dehlinger，Michael Holloway，Rich LeBlanc 和 Brian Randell，感谢你们在审阅手稿时对我的帮助，是你们的评阅使这本书最终成型。感谢 Patrick Graydon，和你的讨论使我受益匪浅。

感谢出版商的大力支持，感谢 Taylor 和 Francis，特别要感谢 Alan Apt 和 Randi Cohen。

最后，我要特别感谢我的家人：我的孩子 Richard、Abby 和 Katie，我的妻子魏金娜。在我写这本书的过程中，你们包容我为了写这本书没有陪你们共同度过的夜晚和周末，我爱你们。

扩展信息

高等教育机构的教师可以得到这本书中材料对应的幻灯片和书中习题的答案。关于本书的其他信息请参见如下地址：

http://www.dependablecomputing.com/fundamentals.html

John Knight

弗吉尼亚州，夏洛茨维尔

目　录