可靠性维修性保障性
学术专著译丛
丛书主编 康锐

系统软件可靠性

System Software Reliability

【美】Hoang Pham 著
李璐祎 主译
陆民燕 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

系统软件可靠性
System Software Reliability

[美] Hoang Pham 著
李璐祎 主译
陆民燕 主审

国防工业出版社

著作权合同登记　图字:军-2013-111号

图书在版编目(CIP)数据

系统软件可靠性/(美)洪范(Pham,H.)著;李璐祎主译.
—北京:国防工业出版社,2014.7
(可靠性维修性保障性学术专著译丛)
书名原文:System software reliability
ISBN 978-7-118-09474-9

Ⅰ.①系… Ⅱ.①洪… ②李… Ⅲ.①系统软件-软件可靠性-研究 Ⅳ.①TP311.5

中国版本图书馆CIP数据核字(2014)第131678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**25　**字数**492千字
2014年7月第1版第1次印刷　**印数**1—2000册　**定价**88.00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

近年来，计算机软件技术以及互联网技术飞速发展，软件运行的硬件环境如计算机或其他嵌入式设备、网络设施等也得到了迅速的发展。在计算机系统和其他嵌入式系统中，软件完成的功能呈日渐增长的趋势，大量以前依靠硬件完成的功能，现在都转而依靠软件来控制和完成。软件在系统中发挥着日益重要的作用。社会对于软件的依赖性也越来越强，无论是人们的日常生活，还是企业的生产制造，乃至军队以及国家的运行和管理，都离不开软件的支持。

然而，软件一旦发生了故障或者运行异常，将对人们生活、企业管理、工厂的生产制造带来很大的不便利或造成重大的财产损失。特别是对于诸如航空航天等领域的安全关键性软件系统（如飞机的飞行控制系统以及火箭的发射系统等），软件的故障甚至将危及人的生命安全以及国家安全。因此，从 20 世纪 80 年代开始，研究者就开始对软件可靠性进行研究，在软件可靠性早期预计、分析、设计、测试、评估等多方面提出了一系列的理论和方法来保障软件可靠性。此外，相关研究机构、组织和不同国家也制定了一系列的软件可靠性标准，目的均为保证最终的软件具备足够的可靠性。

而近年来，软件系统规模日益扩大，复杂程度不断增加，软件系统边界日渐模糊化，其可靠性越来越难以保证，也给现有的软件可靠性理论和方法带来了新的挑战。对于这些新问题，国内外的研究者进行了深入研究和探索，并提出了一系列新的理论与方法。

本书作者为美国罗格斯大学工业与系统工程系的系主任 Hoang Pham 教授。在加入罗格斯大学前，Hoang Pham 教授曾在波音公司、美国爱德华州工程与环境重点实验室担任高级工程专家，研究兴趣包括软件可靠性、软件可靠性建模、维护、容错计算、数据挖掘和环境风险评估等方面。Hoang Pham 教授长期致力于软件可靠性研究。

本书根据 Springer 出版社出版的《System Software Reliability》一书翻译而成，是软件可靠性领域的前沿著作。本书介绍了系统软件可靠性理论与实践的发展现状及最新研究成果，并融合了作者在软件可靠性领域 20 多年的经验。

本书的内容可以分为如下几部分：第 1 章 ~ 第 4 章介绍了软件工程、软件可靠性的基础知识，并阐述了随机过程及评估理论、常见的评估技术，为软件可靠性评

估打下坚实的基础;第5章~第9章介绍了软件可靠性评估模型及评估方法,包括传统的软件可靠性评估模型、基于非齐次泊松过程的软件可靠性模型、考虑测试覆盖率与缺陷移除的可靠性模型以及考虑环境因素的软件可靠性模型及其校准;第10章讨论了软件成本模型;第11章重点讨论了复杂软件系统的容错机制及可靠性模型,并介绍了考虑软硬件交互失效的复杂软件可靠性分析方法。本书由浅入深,从基础知识的介绍开始引入,再关注于传统软件可靠性模型,对软件可靠性模型给出了详细的数学推理过程,之后再扩展到考虑环境因素、测试覆盖率、缺陷移除等要素的复杂软件可靠性模型。由于在软件可靠性领域工业界耕耘多年,作者在本书中介绍了大量的实际软件可靠性失效案例,因此,本书是一本软件可靠性领域理论结合实际的优秀著作,不仅可以作为软件可靠性专业学生的教科书,也可以为软件可靠性领域的从业者提供工具和参考。

本书的翻译工作历时一年。由于本书内容丰富,不仅涉及软件可靠性领域的相关知识,且包含了较多的数理统计专业知识,因此翻译难度较大。译者在翻译过程中,不仅参考了软件可靠性、软件工程的相关书籍,同时参考了数理统计和随机过程的相关书籍,并咨询了数学系的相关博士。

本书由李璐祎担任主译,陆民燕教授担任主审。具体翻译工作分配如下:前言、第1章、第11章、附录由李璐祎翻译;第2章由苏文嵩、李璐祎共同翻译;第3章~第4章4.6节由陈文彬翻译;第4章4.7节~第5章由吴其隆、李璐祎共同翻译;第6章~第7章7.5节由吴泽豫、李璐祎共同翻译;第7章7.6节~第8章由江京、李璐祎共同翻译;第9章和第10章由薛凤桐、李璐祎共同翻译,书中的公式由李璐祎、叶千、徐彪、宋薇输入,全书翻译由李璐祎统筹并整理,由陆民燕教授审阅并校对。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老师的悉心指导与帮助,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3月

前　言

在当今的技术世界，几乎每个人都需要依靠一系列连续运转的复杂机械和设备来保障我们的日常安全、保密、移动性和经济福利。我们希望只要需要，在任何时间、任何地点，我们的电子工具、医院的监测控制设备、下一代的飞行器、数据交换系统和航天应用等都能够运转。这些系统的失效将会带来灾难性的后果。随着社会复杂性的增加，系统和软件的可靠性工程领域也面临着越来越复杂的关键挑战。

一般来说，系统软件可靠性是指在规定的条件下、规定的时间内系统不会失效的概率。今天，工业界面临的最大问题就是如何定量地评估系统的可靠性特性。

本书的作者于2000年出版了《软件可靠性》一书。由于在过去的五年内，现代嵌入式软件系统的复杂性及其带来的挑战不断增加，公共领域和专业团体都开始越来越注意寻找具有合理成本的高可靠性产品。与此同时，在过去五年间，科学家和研究者们也研发出了可供系统设计师、工程师、实践者使用的技术、工具和模型。

本书旨在介绍系统软件可靠性理论与实践的发展现状以及过去五年间本学科的最新研究。作为一本教科书，本书主要基于作者最近的研究和出版成果，并融合了作者在本领域20多年的经验。本书所包含的主题组织如下。

第1章简要介绍了系统软件可靠性以及本书所使用的相关术语。本章也给出了在软件可靠性领域可供参考的文献资料。第2章讨论了系统可靠性工程、系统能力、具有多失效模式的系统可靠性各个方面的概念，以及包括马尔可夫过程、更新过程、准更新过程和非齐次泊松过程等在内的随机过程的相关概念。

第3章描述了评估理论、常见的评估技术以及置信区间估计。第4章阐述了软件工程评估的基本概念，包括软件生命周期、软件开发过程及其应用、软件测试

以及数据分析等。第5章讨论了几组传统的软件可靠性模型和评估方法，并简要介绍了软件复杂性、残余缺陷数等其他软件性能度量的评估方法。

第6章全面覆盖了基于非齐次泊松过程（NHPP）的软件可靠性模型，同时讨论了广义NHPP模型、模型选择以及软件平均失效间隔时间等。第7章讨论了解决测试覆盖和缺陷移除问题的软件可靠性模型。

第8章描述了一些最近关于环境因素的研究，并讨论了环境因素对于软件可靠性评估的影响，同时也讨论了一些考虑环境因素的软件可靠性模型。第9章讨论了有关如何量化系统测试环境和外场环境间的差异的软件可靠性模型校准技术研究。

第10章讨论了为解决由软件失效带来的保用期问题和风险成本而提出的基于NHPP的软件成本模型。同时讨论了一个随机外场环境下的广义增益模型，以及软件系统的多种最优发行策略（即何时停止测试并发布软件）。

第11章关注于容错软件系统建模的基本概念以及其他高级技术，如自检机制等。本章对容错软件的一些机制进行了可靠性分析，如恢复块机制、N版本程序设计和混合容错系统等。此外，本章也讨论了一个包含了常见失效的三版本程序设计可靠性模型，并简要介绍了考虑软硬件交互失效的复杂软件可靠性分析方法。

每章的结尾都包含了可供深入阅读与参考的文献列表和思考题，书末附有部分思考题的答案。附录1包含了各种分布表。附录2包含了一些有用的拉普拉斯变换函数。附录3提供了一个软件工程师可以采用的调查表格，以便更好地理解软件开发过程和优先级。

本书的内容适合工业工程、系统工程、运筹学、计算机科学与工程、数学、统计学、工商管理等专业研究生的一学期软件可靠性课程。本书也可供可靠性工程、软件工程、统计、安全性工程等相关领域的实践者与研究者参考。我们希望读者在使用这本书后可以彻底准备好开展软件可靠性工程领域的高级研究。

我曾使用本书的前7章作为一个为期三天的关于系统软件可靠性的工业界研讨会的补充阅读材料，并把第8章～第10章的内容加到了为期五天的研讨会材料中。这些短期的课程——不论三天还是五天——都对软件可靠性学科进行了简

介,并介绍了软件可靠性的最新研究进展,同时可以很容易地由指导教师进行裁剪,从而适用于特定的工业领域或组织。类似地,读者可以利用前3章以及第6章、第11章的内容,作为为期两天的系统软件可靠性研讨会的阅读材料。

我十分感谢罗格斯大学工业与系统工程学院的学生们,他们在过去的两年中使用了本书的最初版本,并提供了大量的评论和建议。同时感谢来自于大学和工业界的很多同行,感谢他们提供的十分有用的建议。

另外,感谢 Springer – Verlag 出版社的高级编辑 Anthony Doyle 和 Kate Brown,感谢在我超过截止日期后他们的耐心和理解,感谢他们帮助我完成了本书的最终可印刷版本。

最后,同时也是最重要的,我想感谢我的妻子 Michelle,以及我的儿子 Hoang 二世及 David,感谢他们的爱、耐心、理解和支持。谨以本书献给他们。

Hoang Pham

美国,新泽西州,罗格斯大学

2005 年 12 月

目　录