软件可靠性——

度量、预计和应用

〔美〕J·D·穆莎
A·艾里诺　　著
〔日〕K·奥本

机械工业出版社

软 件 可 靠 性

——度量、预计和应用

〔美〕J. D. 穆莎
A. 艾里诺 著
〔日〕K. 奥本

姚一平 林典伦
裘忠侯 才 全 译
曾天翔 校

机 械 工 业 出 版 社

(京)新登字054号

本书全面、深入地论述了软件可靠性的度量、预计和应用，其中包含了作者大量的研究成果和应用实例，并附有示例分析、计算及图表说明。内容深入浅出，具有较高的学术水平和实用价值。本书是目前进行软件可靠性教育的理想教材，也是软件开发、使用和管理方面开展软件可靠性工程研究与应用的重要文献。

本书可作为高等院校学生和研究生的教材，也可作为涉及软件工程、可靠性、应用统计、运筹学和管理科学等方面的研究人员及工程技术人员的参考书。

SOFTWARE RELIABILITY

Measurement, Prediction, Application

John D. Musa

Anthony Iannino

Kazuhira Okumoto

McGraw-Hill Book Company

1987

※

软 件 可 靠 性

——度量、预计和应用

〔美〕J. D. 穆莎

A. 艾里诺 著

〔日〕K. 奥本

姚一平 林典伦 裘忠侯 才 全 译

曾天翔 校

*

责任编辑：范兴国 陆 叶 版式设计：胡金瑛

封面设计：郭景云 责任校对：熊天荣

责任印制：路 琳

*

机械工业出版社出版（北京阜成门外百万庄南街一号）

邮政编码：100037

（北京市书刊出版业营业许可证出字第117号）

北京市房山区印刷厂印刷

新华书店北京发行所发行·新华书店经售

*

开本 850×1168 1/32·印张 14 7/8·字数 391 千字

1992年10月北京第1版·1992年10月北京第1次印刷

印数 00.001—2,270·定价：13.00元

*

ISBN 7-111-03499-6/TP·170

译 者 的 话

20世纪后期，人类进入“信息时代”。在信息处理中占核心地位的计算机系统正在飞速发展，其硬件在可靠性方面已得到巨大提高，但随着计算机规模和复杂性的增加，软件的质量（包括可靠性）还存在不少问题。据统计，软件故障占整个计算机系统故障的65%。

软件工程是研究如何应用工程化的方法有效地管理软件开发，并在软件产品质量、费用和进度三特性间取得协调的方法学。软件可靠性是软件质量概念中最重要的固有特性，也是最容易定量的特征，其研究目的是改进可靠性。

随着系统规模和复杂性的增加，信息系统的开发管理也日益复杂，因此软件产品特性的度量、预计和开发期间的现状控制日益重要。在有关工程技术和管理人员中普及软件可靠性知识是一项迫切而繁重的任务，然而，目前国内还没有一本全面、深入论述软件可靠性的专著。国外公开出版的有R. L. Glass的《Software Reliability Guidebook》(1979)和G. J. Myers的《Software Reliability》(1976)。前者是一本实用性手册，后者是一本普及性书籍。在国内公开出版的有郦萌的《计算机软件可靠性》(1988)，这是可靠性与质量管理普及性丛书之一；还有金文秀等译的〔日〕菅野文友的《软件可靠性》(1988，机械工业出版社，1983年日文版)，亦是一本可靠性普及丛书。在其它一些有关软件工程和计算机可靠性的书中，有个别章节也涉及到软件的可靠性。如张复等译的〔英〕R 朗博顿的《计算机系统可靠性》(1988，国防工业出版社，1980英文版）及朱兆堂等译的〔美〕M L 舒曼等的《软件工程-设计、可靠性和管理》(1989，上海翻译出版公司，1983英文版)。

本书原著是最近出版的〔美〕J. D. 穆莎等著的《Software Reliability-Measurement, Prediction and Application》(1987

英文版），这是国际上第一本较全面、较深入地论述软件可靠性方面的专著，其理论系统全面，应用实例丰富。本书前两篇为应用。主要读者对象是开发和使用软件产品的工程技术人员与管理人员，他们中有的人只希望对软件可靠性度量有一个基本了解，有的人则需要使用软件可靠性度量和分析。第3篇是理论。读者对象是希望深入理解软件可靠性理论基础的软件开发者和使用者，其中也包括可靠性、软件工程、应用统计、运筹学和管理科学等方面的研究人员及广大的研究生、大学生。第4篇是软件可靠性的最新发展情况和研究方向。附录为名词术语。

该书汇集了作者大量的研究成果和丰富的实践经验，并系统地总结了近年来软件可靠性公开文献中的重要成果，因此，该书具有很高的学术水平和实用价值。书中许多软件可靠性的度量和预计的方法十分切合工程项目软件的开发和管理，其实例从银行数据网管理系统到空间飞行器，范围十分广泛。

译者自1985年从事软件可靠性方面研究工作以来，结合航空飞行控制系统的应用软件，进行了软件可靠性建模、预计评估和测试方法的研究。工作中深感软件可靠性度量、预计和测试的重要性，并急需一本在理论与实践上具有指导性的专著。为此我们翻译了本书供广大从事软件工程及可靠性研究的科技人员和管理人员使用。

本书全文翻译了原书的正文，因篇幅所限，部分附录及问题与解答未译。其中序言、第1至第4章及第16章由北京航空航天大学自动控制系姚一平译；第5至第8章由航空航天部301所才全译；第9至第12章（12.1，12.2）由航空航天部北京航空仪表厂裘忠侯译；第12章（12.3，12.4，12.5）至第15章及附录由航空航天部301所林典伦译。航空航天部628所研究员曾天翔对本书进行了审校。中国科学研究院应用数学所研究员曹晋华对本书的翻译给予了大力的推荐和支持，在此表示感谢。

由于水平所限，书中难免有不少错误和不足之处，望广大读者予以批评指正。

译者

序　言

本书共分四篇：

第 1 篇为概述。其中包括各部分内容的综述，各章顺序的安排以及全书的框架。本书通过通俗易懂的图表及实例来阐明软件可靠性度量的基本概念和各种用途。对需要了解数学公式的读者，本书还提供了符号及实例说明。

本篇适用于以下读者：需对软件可靠性度量作一般性了解的高级管理人员、使用软件或采购软件的人员和设计软件的工程师。他们虽然不直接使用软件可靠性度量，但需要懂得其用途。另外，软件工程、计算机科学、管理科学及可靠性方面的一般性课程，也可从中吸取所需的内容。

第 2 篇是应用部分。其中包括系统定义、参数确定、设计技术、应用方法以及实施计划的制定。它为后面的理论提供了丰富的应用经验和实例，并介绍了所需的计算公式。这部分的读者较多，包括使用软件可靠性度量、风险分析、管理决策和质量保证等方面的专业人员。

第 3 篇为理论部分。这部分是本书的理论精华，其中包括模型建立、参数估计和模型比较。第 9 章偏重一般概念并以历史和逻辑观点分析已公布的模型；第13章提出模型的比较准则并作出某些比较。这部分的读者需有概率论、统计学、随机过程和硬件可靠性的理论知识，以及计算机和软件开发方面的技术基础。

这部分的读者包括可靠性、软件工程、应用统计学、运筹学及有关学科的研究人员、学生和任何愿深入了解软件可靠性的人。

第 4 篇为展望。对博士研究生学位论文的选题很有帮助。

为了说明概念，书中引入了实例和示例分析，并附有索引、参考书目和名词术语汇编（附录）。名词术语和第 1、2 篇的概率

论术语均为目前标准用法，并且与ANIS（美国）标准、IEEE 软件工程专门名词标准汇编相一致。

作者将重点放在软件可靠性度量上，并不意味着研究故障原因和减少软件错误不重要。相反，在解决这些问题时，知道软件的情况及如何改进产品的经济效益是有必要的。软件错误的原因和解决的方法将在书中讨论，错误的引入和排除涉及软件工程师的认识、心理状态以及技术水平。显然，可靠性与软件产品及开发过程的许多特性有关，我们希望本书对研究人员定量研究软件可靠性度量能起到促进作用。

目　录

第3篇 理 论

第4篇 未来的发展

第1篇 概 述

本书这部分有三个主要目的：

1. 说明软件可靠性度量在工程和管理软件中的巨大潜在价值；

2. 介绍基本概念，使读者能与软件可靠性度量的专业人员进行交流；

3. 增进对软件可靠性度量应用的了解。

本部分还介绍了如何将这些概念应用到项目及工作系统中去。

第1章的重点为一般性介绍和基本概念；第2章介绍两类精选出来的软件可靠性模型，并讨论如何确定其参数；第3章讨论可能的应用范围，包括全面制定计划和组织应用。

第1章 软件可靠性导论

本章从软件工程方面来评价软件的可靠性，指出其重要性并与硬件可靠性进行比较；然后介绍基本定义和概念，并定义与可靠性有关的有效性；对软件可靠性建模做一般性讨论；最后是软件可靠性度量和预计的某些应用。

1.1 重要性

信息处理是当今和未来世界经济中最重要的产业，它正以很高的速度发展着。这种发展与计算机硬件费用效能的增加有一定关系。费用效能每10年约增长1000倍。只要这种增长率继续保

持下去，那么计算机应用的范围将迅速增加。由于软件是计算机系统最主要的部分，因此在软件工程领域也期望能有类似的增长速度。

当今影响软件工程领域的主要因素包括：

1. 商业竞争日益加剧的程度和竞争的国际性；
2. 信息系统的开发费用和故障费用不断增加；
3. 计算技术变化迅速；
4. 管理信息系统开发的复杂性不断增加。

大多数信息系统的用户实际上是商业用户，他们所面临的商业竞争使他们敏锐地意识到软件产品的重要性。由于在软件生产者之间也存在着竞争，这样软件用户就能更多地了解这些软件产品及他们可能得到的服务。这些用户曾经比较单纯地依赖他们的供应者，但现在已变得日益老练和有所要求，软件生产者必须充分而准确地理解他们的需求，其中最重要的三点需求是：所需产品的质量、交付时间和费用。

与此同时，随着系统的规模、复杂性和分散度的增加，软件的开发和使用费用也在增大。如许多联网计算机系统，它们可分成许多能够同时运行且相互作用的不同软件模块，因此其开发费用较高。信息系统应用的扩大，增加了研究机构对它们的依赖，这种依赖性延伸到较小的机构或较基层的组织。实时工作系统的比例正在增加，故障对工作影响很大，而且通常是关键性的。如航空公司航线预订机票、银行、自动飞行控制、军事防御和核电站安全控制等系统的中断，不仅使经济遭受很大损失，有时甚至是灾难性的。故障费用不仅包括直接费用，还产生责任风险及公司信誉下降，进而冲击股票市场。

计算技术的进步，意味着在经济领域中信息系统更新的速度更快。新的硬件技术或软件技术的发展，均会使软件过时。系统交付使用的时间变得日益重要，新产品在其性能和费用上被其它产品取代之前的推销时间，即市场窗口就已缩小了。

由于费用和进度的限制，要开发一种高质量、快速交付和低

成本的软件产品变得越来越难，也就是说要同时达到这三个目标是困难的。例如，要保证软件产品有较高的质量，就要降低其它方面的要求，即延长交付时间或增加成本。因此在软件产品的开发中就要权衡它们之间的关系，使软件的特性能够满足用户的要求，这意味着软件产品特性的度量和预计是必要的。

随着系统规模和复杂性的增加，信息系统开发的管理也日益复杂。目前许多系统被分成由不同公司开发的子系统，明确的需求是对系统和子系统特性的清晰标识及对开发过程中进度的指示。从管理、合同和法律的观点来看，这种标识也是重要的。因此，软件产品特性的度量、预计和开发期间的现状显得格外重要。

如前所述，软件产品最重要的三个特性是质量、费用和进度。应注意，这些特性是面向用户而不是面向开发者的。对后面两个特性可以进行定量度量，但质量的定量度量非常困难，然而却十分重要。缺乏软件质量的具体度量就意味着当质量、费用和进度产生矛盾时，将牺牲质量。事实上，这正是软件产品存在质量问题的主要原因。

可靠性是"软件质量"概念中最重要的固有特性。可靠性与缺陷（defects）直接相关，Jones(1986)指出：缺陷的多少对编程费用影响最大。软件可靠性的关键是软件功能如何才能更好地满足用户需求。第1.3节中对软件可靠性有明确定义，简而言之，软件可靠性是在规定的时间内软件无故障运行的概率。"故障"（Failure）是指程序功能的某些方面未能满足用户的要求。"功能未满足用户要求"实质上是一种广义的定义。因此，可靠性全面或部分地包括许多常提到的质量方面的特性，如正确性，未面向用户的程序特性。有些特性如软件安全性实际上是软件可靠性的具体方面，而可修改性和可读性则是与可靠性无关的两个质量特性。软件可靠性除了它的显著重要性外，已证实是软件质量中最容易定量的特征。

可靠性表示面向用户的软件质量观点。最初（和现在许多）

软件质量度量的研究方法是建立在计算程序中发现的错误（faults）数和缺陷数的基础上，这种研究方法是面向开发者的。通常还要计算故障数（异常事件数）或修复数（如维修或更改报告），但这两者并不等效于错误数。即使正确计算出所发现的错误数，这些错误数也不能作为软件好坏的状态标志，因为还可能有未发现的错误。发现的错误数只能用来与其它项目发现的错误数进行比较。进行这种比较的指标是每千条开发的源码行所产生的错误数。而可靠性是一种很有意义的度量。它面向用户而不面向开发者；与程序的运行有关而与程序的设计无关；是动态的而不是静态的〔Saunier(1983)〕。可靠性度量考虑到问题出现的频度并直接涉及运行经历和在此经历中错误的影响。因此可靠性度量很容易与费用相联系，非常适用于分析软件发展的趋势、指标的建立及预计何时能达到所需的指标。可靠性度量可以分析实时系统软件和硬件对系统质量的作用，因此，可靠性度量比错误数度量更加有用。

以上所述并不意味着研究错误数没有意义，而是这种研究应集中在作为可靠性预计因子的错误和错误的性质上。对错误和造成人为差错（error）过程的较好理解，有助于制定避免、检测、消除和改正错误的对策。

懂得软件可靠性度量和预计已成为软件管理人员和工程师的一项很重要的技能。这种知识不仅对与软件产品有关的管理人员和工程师很重要，而且对这些产品的用户也一样重要。近15年来我们开发了各种软件可靠性度量的模型，并通过在实际工程项目中的应用获得了不少实际应用知识。这个发展过程将在第9章叙述。由于这个领域已趋成熟并已付诸应用，因此有必要将这些知识整理并加以推广。尽管还存在一些问题，但可以在今后实际工程应用和有关数据积累的基础上加以解决和改进。这些模型有足够的精度（见第13章）和用途（见第3和第7章），它们在工程上获得的效益将超过开发它们所需的费用。

软件可靠性度量和预计在工程项目中应用的实际费用约占工

程开发费用的 0.1%～0.2%，其中包括培训费用、数据收集和处理费用及研究费用等。其实许多工程项目已承担了这些费用的一部分，如许多工程项目设有专门机构对软件系统的故障进行记录和报告，但作出决策的方法定量性较差且不够令人满意。因此，这些费用应取增加费用的上限。

本书的首要目的是帮助软件管理人员、工程师和用户学习软件可靠性度量与预计，以便做出更正确的决策；第二个目的是通过对软件质量最重要的特性——软件可靠性的集中研究来具体了解软件的质量。较好的决策可在许多方面节省工程项目或软件生存期的费用。一般来说，应用这些概念期望可节省 10 倍以上的费用。为了说明这些目的，举例如下：一个开发了 2 年的软件项目，进行 6 个月的测试是十分典型的。测试量虽不是影响可靠性的唯一的因素，但与可靠性密切相关。假定仅需 5 个月的测试就可确定实际应用所需的可靠性指标，则将节省 4 %的项目开发费。所以，这种方法的费用效能较高。

1.2 软件可靠性与硬件可靠性

硬件可靠性学科已建立了多年，它与软件可靠性的关系如何呢?事实上，硬件可靠性与软件可靠性是被人为划分开的，两者可以同样的方式加以定义，把它们结合起来就形成系统可靠性，两者均与环境有关。软件的故障来源是设计错误，硬件的故障来源一般是物理劣变。然而软件可靠性概念和理论适用于任何设计活动。一旦软件（设计）缺陷得到改正，则在整个运行时间内都不会改变，这时故障仅出现在程序运行到未曾暴露和测试到的环境中。虽然生产能影响实际部件的质量，但软件（设计）重复运行是无意义的，且软件（设计）可按高质量标准来实现。由于软件设计错误的引入和消除发生在开发期间，因此在开发期间的各阶段内，软件可靠性是变化的。

“设计可靠性”概念尚未全面应用到硬件方面，磨损或其它物理原因造成故障的概率，一般大于未发现的设计问题所造成故

障的概率。由于硬件没有软件复杂，因此减少硬件的设计故障是可能的。硬件的设计故障应该很少，因为生产项目在现场的改装十分昂贵。然而，目前以硬件可靠性为重点的做法正在开始转变。这可能影响到对软件可靠性研究的认识及增进对设计错误重要性的领会。我们可以通过同时进行软件工程和芯片的设计来加强这方面的认识。

软件可靠性的最终特性在测试期间往往不断变化，这个变化出现在新编码编好以后或修复并消除编码中存在的问题而引出新问题的时候。在规定期间内，硬件的可靠性也可能变化。但与软件相比，在使用寿命期间，其可靠性在很长一段时期内是常值。

尽管硬件可靠性和软件可靠性有上述不同之处，但在研究软件可靠性时仍可借鉴硬件可靠性理论，并可用标准的硬件综合技术来计算系统可靠性值。硬件和软件有许多相似点但也有某些不同之处，因此，不要错误地认为软件过于独特，但也不要将两者看得过于相似。

1.3 基本概念

在介绍具体模型和实际应用之前，首先需全面了解建立软件可靠性模型的基本术语和概念，读者会发现掌握软件可靠性是很容易的。建模的基础知识对实际应用中的正确决策往往有很大帮助。例如，如何对多处理机或分布式系统建立软件可靠性模型？这些基本知识与软件可靠性模型的应用及系统可靠性分析有关，它们将在第 2 篇深入讨论。基本理论的理解是建立在其概念基础之上的，本书第 3 篇将对这部分内容进行全面论述。建立软件可靠性概念可分为几步，并按顺序引出某些其它概念。

1.3.1 故障和错误

“软件故障”是指程序运行的外部结果偏离了需求规范（在第 4 章详细讨论）。所以“故障”是在动态中产生的，必须执行程序才会发现故障，故障与程序的运行状态有关。请注意，故障不同于程序错误也非“错误”，故障的定义是经过斟酌的，它可能包