中经管理文库
管理学精品系列（二）

Research on Trustworthy Software Quality Attributes' Evaluation Theories and Methods based on User Requirements

基于用户需求的可信软件质量属性评价理论与方法研究

文杏梓／著

中国经济出版社
CHINA ECONOMIC PUBLISHING HOUSE

湖南科技大学学术著作出版基金资助
中国博士后科学基金面上资助项目（No.2015M582327）
湖南省哲学社会科学基金项目（No.14JD22）

基于用户需求的可信软件质量属性评价理论与方法研究

Research on Trustworthy Software Quality Attributes' Evaluation Theories and Methods based on User Requirements

文杏梓／著

中国经济出版社
CHINA ECONOMIC PUBLISHING HOUSE
北京

图书在版编目（CIP）数据

基于用户需求的可信软件质量属性评价理论与方法研究 / 文杏梓著.
北京：中国经济出版社，2017.10
ISBN 978-7-5136-4733-5
Ⅰ.①基… Ⅱ.①文… Ⅲ.①软件质量—评价—研究 Ⅳ.①TP311.5
中国版本图书馆 CIP 数据核字（2017）第 128916 号

责任编辑　孙晓霞
责任印制　马小宾
封面设计　华子图文

出版发行　中国经济出版社
印 刷 者　北京九州迅驰传媒文化有限公司
经 销 者　各地新华书店
开　　本　710mm×1000mm　1/16
印　　张　13.25
字　　数　150 千字
版　　次　2017 年 10 月第 1 版
印　　次　2017 年 10 月第 1 次
定　　价　56.00 元
广告经营许可证　京西工商广字第 8179 号

中国经济出版社 **网址** www.economyph.com **社址** 北京市西城区百万庄北街 3 号 **邮编** 100037

本版图书如存在印装质量问题，请与本社发行中心联系调换（联系电话：010-68330607）

前　言

随着计算机与网络技术的发展，软件不仅运用于航空航天、武装设备、交通、核能等安全攸关领域，而且普遍应用于人们的经济生活。然而，随着人们需求的不断增加，软件系统的规模和设计复杂性都急剧提高，且软件系统始终处在动态、开放的环境中，系统行为的不可控性和不确定性，使得软件面临可信性问题的重大挑战。

由于软件失效引发的事故甚至灾难不胜枚举。如1996年，由于火箭控制系统软件故障，导致“阿丽亚娜（Ariane）5型”火箭发射失败，造成大约5亿美元的直接经济损失，且其耗资80亿美元的开发计划延迟了整整三年；2004年9月，由于航空管理软件系统的时钟管理模块缺陷，美国洛杉矶国际机场400多架飞机与机场中心指挥控制系统失去联系，数万名旅客的生命危在旦夕；2005年11月至2006年1月的三个月内，日本东京证券交易所或由于软件升级出现系统故障，或由于突发交易量大幅增加超过系统处理能力，东京证券交易所被迫两次全面停止股票交易；2007年，由于没有考虑用户的高需求、网站前期的测试工作不到位，北京奥运会门票销售系统刚刚投入运行就陷入瘫痪；2014年2月，滴滴打车软件由于短期流量剧增，导致服务器不稳定，软件出现拥堵，给市民出行带来了困扰；2014年2月28日，世界上最大的比特币交易平台MtGox运营商宣布，因其交易系统软件BUG被黑客利用，价值超过5亿美元的85万个比特币被盗，该公司已向日本东京法院申请破产保护。

一次次的软件故障，严重威胁着人们的生命财产安全，引起了人类社

会对高可信软件的渴望。发展高可信软件已经成为当前国际软件技术发展的战略制高点，引起了全世界的普遍关注。

国际组织 TCPA（Trusted Computing Platform Alliance）和 TCG（Trusted Computer Group）制定了关于可信计算平台、可信存储、可信网络连接、可信计算框架等一系列技术规范，致力于新一代具有安全、信任能力的计算平台的发展。美国计算研究协会 CRA（Computing Research Association）和美国国防部高级研究计划署 DARPA（Defense Advanced Research Projects Agency）都将高可信软件系统视为目前计算机研究领域必须应对的五大挑战之一。美国国家软件发展战略（2006—2015）将开发高可信软件放在首位。美国国家科学基金会 NSF（National Science Foundation）在可信软件领域投资 1.5 亿美元，为设计、构建和运行可信系统建立新的科学与技术基础，并与 IBM、SUN、微软、英特尔、惠普等 15 家跨国公司开展合作。欧洲于 2006 年启动了由 23 个科研机构和工业组织参与的“开放式可信计算”研究计划。德国科学研究基金委员会在奥尔登堡大学成立了可信软件研究院，旨在一个跨学科平台提升可信软件系统架构、评价、分析和认证。此外，德国研究联合会资助的 AVACS 项目、德国教育研究部资助的 Verisoft 项目都与可信软件相关。在中国，国家自然科学基金委员会于 2007 年联合信息学部、数学物理学部和管理学部共同启动“可信软件基础研究”重大研究计划，对可信软件的需求管理、可信软件的风险及过程管理、软件的可信性构造、可信环境的构造与评估、可信性验证与测试等方面进行资助，并在 2010 年、2011 年、2012 年和 2014 年四次发布该重大研究计划项目指南，进一步确定了“可信软件”这个研究计划的重要性及意义。国家高技术研究发展计划（863）中设立了专门的项目来研究高可信软件生产工具和集成环境。国家重点基础研究发展计划（973）将可信软件的研究置于重要地位，研究基于网络的复杂软件的可信度和服务质量。

近年来，可信软件已经渗透到国民经济乃至国防建设的各个领域，成

为影响人们生产、生活的重要组成部分。在学术研究领域，国内外学者对其研究取得了丰硕的成果。自 2007 年 1 月到 2017 年 7 月，以美国、中国、英国和意大利为代表的 32 个国家的研究者在 SCI、SCIE、SSCI 来源期刊发表高质量学术论文 500 余篇，极大促进了可信软件基础研究的发展。

通过仔细查阅相关文献发现：基于多维质量属性的可信软件评价是实现软件可信、开展可信软件管理的核心基础，也是可信软件开发管理过程中急需解决的问题之一。然而，目前绝大部分软件质量属性的研究都是基于软件设计、开发者的视角，而忽视了软件用户在使用过程中的客观实践及主观感受。因此，基于用户需求的可信软件质量属性评价理论与方法的研究，具有重要的理论价值和现实意义。本书研究内容主要包括以下 8 个部分。

第一章是可信软件质量属性研究概述。本章主要概括了可信软件的研究背景、研究内容和研究意义。系统阐述可信软件质量属性评价的研究内容、研究方法及本书的研究思路。本章是本书的总起概括章节。

第二章是相关理论及文献综述。本章主要概括了可信软件、软件质量属性的界定及其国内外的研究现状。介绍并评价 McCall 质量模型、Boehm 模型、软件能力成熟度模型、FURPS/FURPS+模型、Dromey 质量模型、ISO/IEC9126 模型、软件可信属性模型，7 个经典的软件质量模型。并阐述了软件质量度量的发展、分类、方法和过程。

第三章是可信软件质量属性评价方法与建模。本章主要阐述了可信软件质量属性评价常用方法：层次分析法和模糊综合评判法。研究认为软件质量属性评价应用可以被划分为多个相互独立的任务，采用体系结构的方法可以建立可信软件质量属性评价应用系统模型，并提出了相应的设计框架。

第四章是基于用户需求的可信软件质量属性的生成。可信软件质量属性指标体系的产生是软件质量属性评价的基础，也是评价过程中关键性环

节。针对用户对软件质量属性的需求及可信软件的特性，本章介绍了用户需求的表达及其本体生成、匹配方法，并将可信软件质量属性分成关键属性与非关键属性两大类。在此基础上，采用层层分解的方法构建可信软件质量属性证据模型、评估体系，形成满足用户需求的可信软件质量属性评价指标体系。该评价指标体系既能满足软件开发者规范软件质量属性体系结构，又能结合软件具体应用领域、运行环境及软件使用者的不同需求，为后续软件质量属性评价方法的研究奠定了基础。

第五章是基于一致性评判的可信软件质量属性评价方法研究。针对可信软件的某些质量属性不可直接测量、质量属性之间不具备可比性且测量标准不统一等问题。本章首先研究了软件质量属性之间的相互关系及这种关系的表达方式。通过设计结构矩阵、矩阵转换、矩阵运算来解决上述问题并间接度量软件质量属性。同时，由于可信软件运行环境的不同，不同的人对于质量属性有着不同的视角、解释和判断标准，在很大程度上人们没有办法达成一致的评判准则。针对这个问题，本章通过上述间接度量模型构建一致性、满意度和贴近度三个评价指标，以确定软件设计开发者和软件用户对于软件质量属性评判的一致性程度，并结合文献资料设计评判准则，帮助他们做出合理的决策。最后，通过一个应用实例，验证了本章提出方法的可行性及有效性。与其他方法相比，这种方法完全依赖于软件质量属性之间的相互关系，是一种间接的、客观的、具有统一标准和评价尺度的、考虑软件使用者和开发者一致性评价的方法。

第六章是基于前景理论的可信软件质量属性评价方法研究。现今绝大部分评价方法所假设的一个基本前提是评价者是完全理性的。但实际上由于软件运行环境的复杂不确定、评价者在评价过程中固有的主观偏好及风险性等实际问题，使得评价结果并不是完全科学、可靠的。针对这些问题，本章引入前景理论以描述、表达在复杂不确定环境下评价者的有限理性。通过阐述前景理论的提出背景及发展应用，重点论述了梯形模糊数的

前景价值函数，构建一个基于前景理论的软件质量属性评价模型，在“框架”内，通过正负理想参考方案的选择、信息的处理、综合前景值的确定、比较，来判断软件质量属性的优劣。并通过第五章的应用实例验证本方法的有效性及实践性。同时，考虑在评估过程中，评价者有限理性及其变化对可信软件质量属性评价结果的影响，进行对比分析，结果表明本章提出的评价方法更加严谨、科学。本章所提出的评价方法是一种直接的、考虑评价者有限理性的研究方法。

第七章是基于元胞自动机的可信软件质量属性动态评价方法研究。在第五章介绍可信软件质量属性间接评价方法、第六章提出可信软件质量属性直接评价方法的基础上，本章节研究的是一种动态的、考虑软件在受到干扰的环境下，其质量属性评价值是否发生变化、如何变化、软件是否总是可信的方法。软件系统是一个动态的系统，它总是在不断的发展、演变中，在受到干扰时，人们总是期望它能保持原来的状态，但实际上这并非总是可能的。系统运行状态的变化，必然导致系统内部能量的变化，本章创新地借助于物理学“熵”的概念来描述、表达这个现象，并详细分析了复杂系统内部能量的变化及可信性的传递过程。针对软件状态的变化是一个时间、空间完全离散的，且后一个状态受前一个状态影响的特征，结合元胞自动机的相关机理，对软件质量属性在受到干扰后的评价值进行了仿真模拟。研究结果表明：对于一个复杂系统，在受到干扰的情况下，软件系统质量属性评价值是逐步下降并逐渐趋于稳定的；持续干扰必然导致系统只有少数几个状态最终被用户信任。由此可知，干扰，尤其是持续干扰，对系统的影响是巨大的，并最终可能导致整个系统变得不可信。

本书系统的对可信软件、可信软件质量属性、评价理论与方法进行了梳理与补充。基于管理学的逻辑思想体系，从软件用户需求的视角，对可信软件质量属性进行间接、直接、动态的全面评价，并通过实验验证了本书评价理论与方法的可行性、有效性，以期有利于软件用户对可信软件质

量属性进行客观评价，也有利于为软件设计者在设计过程中更多地考虑用户需求提供客观依据。本书的研究有利于丰富可信软件质量属性评价理论与方法，也为推动我国可信软件产业的发展做出贡献。

本书系笔者8年来研究成果的一个总结，也是中国博士后科学基金面上资助项目“软件产业虚拟集群网络运行机制与信任演化模型研究”（No. 2015M582327）、湖南省哲学社会科学基金项目（No. 14JD22）的阶段性研究成果。

在笔者的研究过程中，有幸得到上海交通大学、中南大学、湖南大学、天津大学、湖南科技大学各位专家学者的鼎立支持与帮助。“落其实思其树，饮其流怀其源”，借此片纸，聊表谢忱！

才疏学浅，敬请读者批评斧正！

文杏梓　博士

2017年10月1日

目　录

第一章　可信软件质量属性研究概述

“可信软件基础研究”重大研究计划于2007年底正式启动到2017年已经有整整10个年头了。作为国家自然科学基金委员会“十一五”“十二五”期间启动的重大研究计划之一，国家自然科学基金委员会于2008~2012年、2014年共计6次发布了重大研究计划指南（2009年是国家科学技术部863计划发布的“高可信软件生成及集成环境”重点项目指南）。该计划得到了信息科学部、数学物理科学部和管理科学部联合组织与实施。至今，已资助“培育项目”73项，“重点支持项目”18项和“集成项目”5项，累计资助经费超过2亿元①。

“可信软件基础研究”重大研究计划的启动实施，是我国软件基础研究领域的一件大事，对于应对软件发展的重要科学挑战，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，提高我国在可信软件领域的原始创新能力和国际影响力，为国家相关重大计划和工程的可信软件研发提供科学支撑，培养一批高水平的研究人才，都具有深远的意义[1]。

① http://www.nsfc.gov.cn/.

1.1 可信软件的提出

现如今，以终端设备、网络技术和软件应用为基础的金融交易、工业制造、交通运输、移动商务、电子政务等各种嵌入式控制系统已经渗透到人们生产、生活的方方面面。软件已经成为人们日常工作与生活的一个重要组成部分。但随着软件系统的规模日益庞大，加之当前软件开发和运行环境的开放性、动态性、多变性，使得高质量的软件产品越来越难以产生。

据 Standish Group Chaos 公布的软件开发项目统计数据显示：1994 年全美 31.1%软件开发项目是完全失败的，52.7%的软件项目由于超过预算、延期，或不能满足用户需求而受到质疑，仅仅只有 16.2%的软件项目被认为是成功的。到 2008 年该报告显示：软件项目成功的比例上升到 32%，完全失败的比例为 24%，而受到质疑的项目下降到 44%。尽管这些数据是让人欣慰的，但 68%的软件产品是受到质疑或失败的事实表明：开发高质量的软件产品仍然存在很大的提升空间[2]。此外，即便软件项目开发成功，很多软件产品在推出时就含有很多已知或未知的缺陷，已经成了不争的事实。而人们对于软件的依赖加重或恶化了软件错误/失败的结果，导致其发生故障、失效后，造成的各种灾难性事件层出不穷[1-9]：

1992 年，英国伦敦的医疗救护派遣系统彻底崩溃，导致多名患者因延误抢救时机而失去宝贵的生命；

1996 年，欧洲航天局的火箭控制系统软件故障，导致其首次发射的“阿丽亚娜（Ariane）5 型”火箭失败，造成大约 5 亿美元的直接经济损失，且其耗资 80 亿美元的开发计划延迟了整整三年；

2002 年，黑客成功入侵澳大利亚墨尔本的 Transurban City Llik 电子付费系统，并通过网络窃取了超过 50 万用户的信用卡信息；

2003 年，由于分布式计算机系统试图同时访问同一数据资源，导致控制全美 80% 以上电力资源的电力检测与控制管理系统失效，造成美国东北部大面积停电，其经济损失超过 60 亿美元；

2004 年，德国社会服务系统软件（A2LL）由于调整失业补助账户位数错误，导致银行不能将失业补助及时支付给数千失业者；

2004 年 9 月，由于航空管理软件系统的时钟管理模块缺陷，美国 Los Angeles 国际机场 400 多架飞机与机场中心指挥控制系统失去联系，数万名旅客的生命危在旦夕；

2005 年 11 月至 2006 年 1 月的三个月内，日本东京证券交易所或由于软件升级出现系统故障，或由于突发交易量大幅增加超过系统处理能力，东京证券交易所被迫两次全面停止股票交易；

2007 年，由于网站系统设计不合理，没有考虑用户的高需求，网站前期的测试工作不到位，北京奥运会门票销售系统刚刚投入运行就陷入了瘫痪；

2014 年 2 月，一直深受中国打车一族喜爱的、由深圳腾讯公司开发的滴滴打车软件由于短期内流量剧增，导致服务器不稳定，软件出现拥堵，给广大市民的出行带来了不少的困扰；

2014 年 2 月 28 日，世界上最大的比特币交易平台 Mt. Gox 运营商宣布，因其系统存在漏洞，其平台比特币被盗一空，已向日本东京地方法院申请破产保护。

一次次的软件故障，严重威胁着人们的生命财产安全，引起了人类社会对高可信软件的渴望，软件可信性问题已经成为国际社会

普遍关注的问题，研究如何确保软件的高可信性质、对可信软件质量属性进行评价及预测、设计合理的软件系统满足用户的需求等一系列问题，具有重大的理论及现实意义。

目前，可信软件的研究已引起了各国政府、大型科研机构及跨国公司的高度重视。

在美国 National Development Strategy for Software（2006～2015）中，将开发高可信软件放在首位。美国政府的“网络与信息技术研究发展计划（Network Information Technology Research Development, NITRD）”是美国最重要的信息技术研究计划之一，在其 2006 年的 8 个重点领域中，与“可信软件”密切相关的重点领域就多达 4 个。此外，在高可信软件与系统领域，“信任：设计与建设具有多安全层次的系统”已经成为 2010 年 NITRD 战略规划的重点领域之一，其包括可信赖的系统、使数字世界更可信、信息保证与共享、网络空间的无忧生活、安全与隐私的平衡五个具体问题①。美国国家科学基金会（National Science Foundation, NSF）在 2006～2008 年三年期间，在可信软件研究领域拟投入 1.52 亿美元[9]，并在加州大学伯克利分校成立了科学与技术研究中心，其目标是为设计、构建和运行可信系统建立新的科学与技术基础[1]，该中心由 8 所大学参与，并与 IBM、SUN、微软、英特尔、惠普等 15 家跨国公司开展合作。同时，美国很多国家机构，如国家航空航天局、国防高级研究规划局、国土安全与卫生研究所、食品和药物管理局、国家科学院、国家标准技术研究院等都积极参与可信软件系统的开发和研究，并与国家科学技术委员会共同合作，先后形成一系列的研究报告[10]。

① http：//blog. sina. com. cn/s/blog_ 54e031af0100kp6o. html.