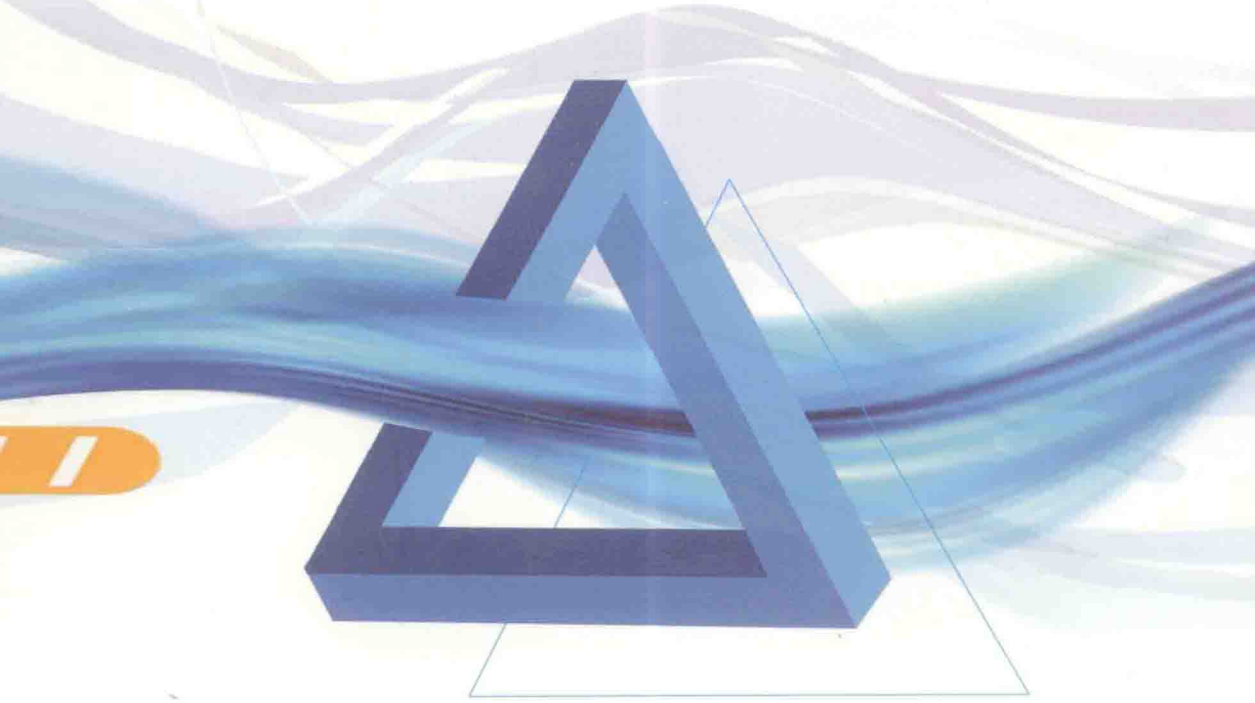
可信软件测度
理论与方法

于本海 著



科学出版社

可信软件测度
理论与方法

于本海 著

科学出版社

内 容 简 介

本书从软件开发的工程过程和管理过程入手，定义了可信软件过程，建立基于可信原则的可信软件过程改进模型；为正确评价可信软件水平，分别构建基于全生命周期过程实体、过程行为、过程产品、进度和成本可信的软件过程可信属性和评价指标体系；基于软件保密安全性、生存性、容错性、可靠性和防危性的软件可信属性和评价指标体系，为验证软件过程可信对软件产品可信影响关系，应用结构方程模型理论分析了软件过程可信属性和过程可信评价指标项的量化关系，从理论上验证软件过程对软件产品影响关系。本书理论意义在于：提出的软件过程可信和软件产品可信评价方法和技术，对丰富可信软件研究具有非常重要的理论价值。其实践意义在于：构建的可信软件评价指标体系、可信评价数学模型和可信软件过程改进模型，为软件组织与管理提供操作性较强的评价方法，为有关标准化部门制定政策提供支持。

本书适用于软件企业、咨询公司和软件项目管理部门的管理人员阅读，也可作为管理科学与工程类、软件工程类和计算机应用类研究生的教材或参考书。

图书在版编目(CIP)数据

可信软件测度理论与方法 / 于本海著. —北京：科学出版社，2014

ISBN 978-7-03-040937-9

Ⅰ. ①可… Ⅱ. ①于… Ⅲ. ①软件-测试 Ⅳ. ①TP311.5

中国版本图书馆 CIP 数据核字（2014）第 117687 号

责任编辑：林 剑 / 责任校对：郑金红

责任印制：赵德静 / 封面设计：耕者工作室

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京佳信达欣艺术印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2014 年 7 月第 一 版 开本：720×1000 1/16

2014 年 7 月第一次印刷 印张：10 1/4

字数：210 000

定价：68.00 元

（如有印装质量问题，我社负责调换）

前　言

软件已经应用到政治、经济、军事和文化生活等各个方面，成为人类发展不可或缺的工具，然而，软件不可信而引发的灾难给人类社会发展带来了许多不安全因素。因此，研究可信软件属性和评价指标体系，建立可信软件评价模型，提高可信软件水平具有重要意义。

以往的研究面向所有的软件项目，将软件开发过程可信和软件产品可信分开研究，单纯进行可信软件过程或可信软件产品研究，忽略了软件过程对软件产品的影响。现有的软件可信度测度模型，都是侧重于软件可信某一侧面的评价，评价的目的主要是测度软件在某个方面的可信水平，考虑因素不全，大多是事后评价，不能有效地指导软件过程改进，对于软件过程改进指导意义不大。本书将可信软件过程和可信软件研究有机结合起来，从软件全生命周期视角，提出基于全生命周期的可信软件评价模型。本书的主要工作如下。

（1）建立基于可信原则的可信软件过程改进模型

从软件开发的工程过程和管理过程入手，系统地分析了可信软件过程构建的复杂性，定义了可信软件过程；应用 TSM 中 44 个可信原则，在分析 CMMI 等主流软件过程模型基础上，定义了可信软件过程管理框架，形成可信保障过程域（TAPA）、可信监控过程域（TMPAs）、可信工程过程域（TEPAs）。为有效地实施可信软件过程管理模型，建立了可信软件过程裁剪、执行、度量与改进模型和可信软件过程改进支持系统逻辑模型。

（2）建立基于全生命周期的软件可信属性和评价指标体系

在软件可信的单一属性和指标体系，以及测度模型方面已有一些研究成果，对于软件过程可信评价指标体系，由于软件开发和运行的复杂性，根据系统工程原理，软件单一属性的可信，并不能保证软件的整体可信。所以，从软件开发过程和软件运行维护两个阶段，分别构建基于过程实体、过程行为、过程产品、进度和成本可信的软件过程可信属性和评价指标体系，基于软件保密安全性、生存性、容错性、可靠性和防危性的软件可信属性和评价指标体系。

（3）验证软件过程可信对软件产品可信影响关系

软件过程可信是制约软件（产品）可信的关键环节之一，研究软件过程可信影响软件产品可信机理，对于开发可信软件产品十分重要。根据结构方程模型

的理论，建立过程可信和软件可信映射关系模型。应用结构模型分析软件过程可信属性之间、软件产品可信属性之间以及软件过程可信属性与软件产品可信属性之间的对应关系；应用测量模型分析了软件过程可信属性和过程可信评价指标项的量化关系，以及软件可信属性和软件可信评价指标项的量化关系。系统地研究了影响软件可信的软件过程因素，从理论上验证软件过程对软件产品的影响关系。

（4）提出一种新的软件过程可信评价方法和技术

以往关于软件过程可信的研究大多集中在软件过程改进理论和方法方面，缺乏综合软件过程可信多个属性的测度模型，往往无法准确评测软件过程可信水平，难以定位软件过程的具体问题所在，盲目的过程改进浪费了有限的资源。同时由于过程可信属性和指标项较多，各个属性和评价指标项对于过程可信的影响程度也不尽相同。所以，首先应用层次分析模型确定软件过程可信属性和评价指标的权重，使主观评价客观化。其次，应用模糊综合评价理论，构建支持定性与定量度量数据的量化评价模型，通过可信评语集的评价项出现频率确定指标项的隶属度；根据指标项权重以及指标项的隶属度确定软件过程可信因素的隶属度，准确地分析影响软件过程可信的主要因素。最后，应用因素隶属度和权重给出软件过程在“不可信”“低可信”“基本可信”“可信”和“高可信”等级别上的隶属度，客观地描述软件过程整体可信水平，为软件组织实施有效的过程改进提供理论依据。

（5）提出一种新的软件可信评价方法与技术

传统的可信度分级方法往往给出相对数值（如0～1的数值），作为软件可信度的水平值，单一的数值描述不能全面地反映软件整体可信水平，使软件组织和用户难以把握软件可信程度。建立基于证据理论的反映软件产品总体可信水平的软件可信评价模型，解决单一属性的可信软件模型评价结论不准确的问题，把软件开发人员、测试人员、应用人员所获得的软件表现的状态信息作为软件可信证据，考虑各个软件可信证据对软件可信影响程度不同，以及软件可信因素间和指标项间重要程度不同，通过对于不同证据赋予权重的方式，更好地避免证据冲突，使可信软件评价结论更可靠。

笔者通过对我国可信软件开发状况和过程改进模型的应用情况进行调研分析，将可信软件过程评价和软件可信测度进行有效结合，构建了基于全生命周期的可信软件评价模型。该模型可以完成软件项目的开发前预测、事中控制和事后评价等全过程的可信评价工作。

软件可信评价的目的在于指导项目开发实践，提高软件可信水平。本书将管理学、统计学、人工智能理论、软件过程理论以及计算机理论相结合，综合地分

析了IT项目的绩效构成以及影响绩效水平的IT项目特征、IT组织特征等因素，建立了面向全生命周期的软件可信评价模型，通过分析评价项目的软件可信水平、识别软件项目的关键影响因素、制定并实施可信软件过程改进策略，使过程改进有据可依，符合我国软件项目开发的实际情况。

本书是笔者近年来从事可信软件领域研究成果的总结，立意新颖，具有一定的理论创新，实践性较强。本书旨在为我国可信软件开发提供操作性较强的理论和方法，提高软件可信水平。本书对于丰富可信软件评价和可信软件过程改进理论知识体系具有一定意义。

本书在写作过程中参考了大量国内外可信软件研究专家的最新成果，文献中只列出部分主要参考文献，作者谨向书中引用相关成果的所有专家学者一并表示感谢。本书第7章的软件可信评价模型案例分析由宁禄乔博士编写，在可信软件评价指标体系和可信软件评价模型的建立过程中得到了许多软件企业的项目经理、研发人员和软件项目用户无偿提供的基础数据，使模型更为准确地反映可信项目开发的实际情况，在此特向这些热忱关心我国可信软件开发的同志表示诚挚的谢意。

本书是国家自然科学基金重点项目“可信软件过程管理及风险控制模型和方法研究”（No：90718042）、国家自然科学基金面上项目“面向项目绩效评价的软件过程改进模型研究”（No：70971124）、中国博士后科学基金（一等项目）“面向项目过程改进的软件可信度测度模型研究”（No：20090450058）、中国博士后科学基金（特别资助）“不确定环境下可信软件风险分析模型研究”（No：201003164）、住房和城乡建设部科技计划项目“基于能力成熟度模型的工程项目绩效评价方法研究”（No：2010-R3-13）等课题的部分研究成果，并得到山东省特色重点建设学科出版资助。

鉴于作者研究水平有限、写作经验不足，书中难免存在疏漏之处，恳请广大读者批评指正；同时笔者欢迎与可信软件研究的学者、专家和软件开发应用的业内人士，对于可信软件研究的有关问题进行更深层次的交流探讨和合作研究，共同推动我国可信软件开发和应用的进展。

于本海

2014年3月

目　录

1 引　　言

1.1 可信软件研究的背景和意义

日趋庞大的软件系统越来越脆弱，发生各种故障和失效，直接或间接地对用户造成巨大损害。在一些特殊应用领域，软件系统一旦发生失效，给人类生命财产和环境造成重大甚至是灾难性损失的案例已经不胜枚举。1996 年 6 月 4 日，欧洲空间局的阿丽亚娜-5 火箭，在浮点数转换成整数操作时产生操作数错误，引起软件异常，发射 37 秒后爆炸，损失 70 亿美元（士元，1996；孟章荣，1997）。2002 年 6 月 28 日，美国商务部的国家标准技术研究所（National Institute of Standards and Technology，NIST）发布报告："据推测，（美国）由软件缺陷而引起的损失额每年高达 595 亿美元。这一数字相当于美国国内生产总值的 0.6%。"（刘克等，2008）2003 年 8 月 14 日下午 4 时 10 分，俄亥俄州的第一能源公司（First Energy）电力监测与控制管理系统软件 XA/21 出现错误，美国及加拿大部分地区发生历史上最大的停电事故，经济损失达 250 亿～300 亿美元（蔡春元，2009）。2006 年 4 月 20 日中国银联跨行交易系统出现故障，整个跨行交易系统陷入瘫痪约 8 小时，据不完全数据统计显示，34 万家商户以及 6 万台 ATM 机，因此受到影响（贺久松，2010）。2009 年 6 月 9 日，双色球 2009066 期开奖，深圳市某信息技术公司软件开发工程师企图利用计算机网络信息系统技术诈骗彩票奖金，通过木马攻击程序，恶意篡改彩票数据，以达到伪造双色球一等奖中奖事实，所涉金额高达 3305 万元（岳逍远，2009）。2010 年 3 月 16 日美国联邦航空局要求为数百架波音 777 型客机更新驾驶系统软件，以防机组人员无意间启动客机自动驾驶仪，致使飞机低速起飞进而滑出跑道。2012 年 1 月中国铁路客户服务中心网站（http：//www.12306.cn）在软件系统设计时，对春运期间互联网购票需求估计不足，在春运售票过程中，互联网售票日交易量超过系统设计能力，导致铁路售票网系统瘫痪；另外，还出现旅客已经支付票款，网站未及时或完整地收到银行成功支付信息，造成旅客成功支付但网站显示购票未成功现象，发生支付偏差。2013 年 12 月，安卓手机出现锁屏漏洞，黑客利用该漏洞绕过锁屏图案和用户密码，进入用户手机获取个人隐私信息，进而盗取用户的通信录、照片、

短信等。这些典型案例表明，无论对软件开发技术人员还是软件的最终用户，软件可信已经成为全社会共同关注的热点问题之一。开发软件可信的重要意义、需求以及调查研究同样被政府、企业和学术研究机构所重视，软件开发产品可信度理论和方法，已成为软件行业和计算机应用类等学术机构一项重要的工作（士元，1996）。

软件的应用范围越来越广，需求复杂度越来越高，可用性需求越来越强。一方面，软件应用广度和深度加大，在开放、互联、协作和共享为主旋律的互联网环境下，软件呈现出网络化、服务化、虚拟化和集成化的发展趋势（王桂玲，2012），对于软件安全的要求越来越高，而软件可信水平却日益下降。另一方面，软件项目的规模越来越大，开发环境越来越复杂，项目不能按期、按预算及预期的质量完成的比例越来越高，同时在项目开发前期，软件组织不能全面了解新开发项目的全部属性特征，对其复杂程度、技术难题和开发人员的频繁变更等潜在的关键影响因素识别分析不足，软件开发过程越来越不可控，软件产品越来越不可信，软件项目的高失败率已经得到国内外专家的广泛关注。

软件项目开发是一项复杂的系统工程，又是一个动态过程，随着开发过程的不断深入，软件开发和实施过程中常常遇到很多困难和障碍。具体包括：①项目的某些特征、外部环境都将发生变化，按预定计划执行软件开发过程，很难得到预期的软件产品；②开发人员与用户的信息不对称，开发人员缺乏与用户沟通的有效途径，项目前期用户不能全面地描述软件需求（尤其是软件的非功能性需求），导致软件需求不明确且频繁变动，软件难以满足需要；③国内许多企事业单位，管理机制没有理顺，人员素质参差不齐，在项目开发时机不成熟、开发条件不完全具备的情况下，开发了一些大型的软件项目，也是导致一些软件不可信的原因之一；④很多软件组织依然是作坊式的软件开发，缺乏有效的软件过程管理方法和工具，软件过程管理失控，导致软件产品质量难以保证；⑤软件开发工具、开发方法和开发平台选择不当；⑥软件设计有重大缺陷，导致维护工作复杂，维护费用不断上升等，如此种种最终导致项目开发延期、成本超支，甚至软件项目失败。

计算机软件已成为世界经济、科技、军事和社会发展的重要引擎，同时软件的安全问题也日益突出。软件漏洞是安全问题的根源之一（吴世忠等，2012）。信息安全建设的重要性也越发凸显，从个人隐私、商业机密、知识产权到国家信息安全，均需要可靠、严密的信息安全保障体系来维护（高常水，2013）。计算机软件潜在的漏洞和只能在部分已知的环境中执行，意味着需要将软件可信管理引入软件运行本身，以便跟踪软件运行过程的风险，构建适合软件可信管理的规避策略（Huth and Kuo，2013）。可信软件开发需要开发者根据不同工程分支领

域、学科交叉以及跨多个模型对软件评价的影响，通过合并成一个单一的控制和软件需求系统模型，努力减少系统开发人员对于相同系统架构的不同观点（Insaurralde，2013）。可信软件系统应该建立在构造技术能够分解软件复杂性没有隐藏的重要假设的基础上，并对软件目标执行环境和故障要有合理预期，架构设计注重访问系统收集的信息和知识，并提取这些信息，这将有助于将架构之间的不匹配的风险降到最低境（De Florio and Blondia，2011）。Li 等（2012）提出一个软件过程模型与风险管理和成本控制模块，整合有效的风险管理和可信软件过程，这个模型可以用来得到一个优化风险管理方案，加强软件过程成本和时间的约束，提高软件开发产品的可信性，特别对于低 CMMI（Capability Maturity Model Integration，CMMI）级别的公司更为有效。

可信软件开发过程以及软件有效运行是保证各类业务成功以及人类安全关键因素之一，软件产品可信在某种程度上取决于软件项目开发过程的可信性，许多错误或缺陷往往是在开发过程中引入的。因此，通过对软件开发过程和软件产品的应用情况分析，研究可信软件评价指标体系，构建面向全生命周期的软件可信度测度模型，对于提高软件可信度水平和软件成功率具有重要意义。

1.2 可信软件评价涉及的主要问题

1.2.1 可信软件评价涉及的主要领域

可信软件评价研究是管理学、软件工程学以及信息科学等多学科的交叉领域，侧重软件项目管理研究。软件项目管理是管理学科的一个重要研究领域，包括项目组织层面、项目层面、工程层面和支持层面的管理，包括软件范围管理、时间管理、进度管理、质量管理、成本管理、风险管理、人力资源管理、沟通管理、采购管理九大知识领域体系。软件工程研究的对象是大型软件系统开发的工程化的理论和方法，研究内容是软件开发过程，以及软件开发的目的、任务、方法、技术、工具、文档和产品规格等。本书将管理学科、软件工程学科和信息科学相结合，用管理科学的原理、方法，建立软件过程可信性属性及评价指标体系、软件可信属性及评价指标体系；结合软件工程理论，验证可信软件过程与可信软件产品的相关性，建立基于过程实体可信、过程行为可信、过程产品可信、过程成本可信和过程进度可信的软件过程可信测度模型，建立基于软件保密性、安全性、生存性、可靠性、防危性的软件可信测度模型。

1.2.2 可信软件评价研究面临的主要问题

国家自然科学基金重大研究计划“可信软件基础研究”2011 年度项目指南提出：采用理论研究和实证研究相结合方法，发挥管理科学、计算机科学、控制科学交叉研究优势，研究可信软件基础理论和方法，分析软件环境失效和软件可信度量和评价的基本规律，建立可信软件开发过程和运行支撑平台及环境，建立可信软件及环境构造与验证、演化与控制的方法和关键技术，促进我国软件从传统的单一度量评价理论到综合可信度量理论及其构造方法的飞越，系统推进我国软件开发及运行环境向软件行为可信、软件运行环境可信、软件使用可信和软件过程可信的进展，提升我国在可信软件领域的创新能力，为国家相关重大研究计划和工程开发提供科学理论支撑和操作性较强的工具支持。这些研究主题是目前我国从战略层面提出的可信软件研究面临的主要问题，概括了可信软件研究的学科前沿。本书主要从软件开发全生命周期的视角，分析、构建、验证可信软件过程和可信软件产品的评价理论和方法的知识体系。

（1）软件可信评价的理论与方法研究

现有的可信软件评价方法多从软件缺陷统计分析入手，在软件开发过程中往往通过文档分析的方法，查找软件需求、设计的存在的问题；对于软件产品（或中间产品）通过模块测试、单元测试、集成测试和系统测试发现软件缺陷（或不符合项），并作统计分析处理；但两者均无法反映开发与应用人员、软件和运行环境之间的交互造成的软件不可信问题，无法准确分析导致软件开发过程和软件产品存在深层次问题的原因。软件需求分析、设计以及开发技术人员和应用人员（用户）的行为属于管理学科研究的范畴，软件程序开发和计算机软硬件应用属于软件工程研究领域。在不确定性环境下，计算机软硬件、软件组织和开发人员以及用户之间交互作用于软件开发过程，完成较为复杂的软件产品开发。本书将管理科学理论和软件工程理论有机结合，研究评价软件过程可信和软件产品可信的理论和方法。

（2）软件过程可信对于软件产品可信影响关系研究

软件可信属性和评价指标包括定性指标和定量指标两类。部分定量指标尽管在理论上有较为客观的定义，但由于软件开发过程和软件运行过程的不可视性特点，收集软件开发和运行过程中数据较为困难；部分定性的软件过程可信和软件产品可信性的评价指标不易于量化。软件过程影响软件产品可信机理，以及软件

过程可信因素和软件产品可信影响因素的映射关系方面的研究比较缺乏，因此，建立软件可信评价模型是件十分困难的事情。本书将深入地分析软件过程可信属性对于软件产品可信属性的影响关系，即开发过程可信属性对软件产品可信属性的映射关系研究，研究软件产品可信属性与软件过程可信属性影响程度的定量关系。

（3）注重软件可信度度量模型研究忽略了软件过程可信性度量研究

软件过程可信是影响软件产品可信的主要因素之一。软件产品在运行过程的表现行为即为软件的可信性在某种程度上取决于软件开发过程的可信程度，即软件过程可信性。在现有的软件可信度量模型中，仅从软件产品本身性能表现的视角，集中在可信软件产品层面的验证和确认研究较为成熟，忽略软件开发过程可信度测度问题研究。事实上软件的缺陷往往是在软件开发过程中植入的，因此，研究软件过程的可信性，是从根本上解决软件产品可信问题的主要途径之一。

（4）单一属性的软件可信评价方法不足以反应软件可信总体水平，缺乏软件产品综合可信度测度模型

以往的软件可信评价模型，往往是单一可信属性的评价，如安全性、可靠性、成本、进度等评价，事实上软件可信属性之间相互作用、相互影响，软件可信评价是一项涉及人系统、物系统等不同领域的问题（席酉民和尚玉钒，2003），单一属性的评价有时不能反映软件的整体可信水平，因此，需要构建多目标多属性的综合软件可信评价模型，全面反映软件可信水平。

从现有的文献和调研的情况来看，关于软件过程的可信程度达到怎样的水平才能确保软件产品可信度，或者说软件开发过程可信度和软件产品的可信度之间存在着怎样的函数关系，以及如何客观地评价软件可信水平和软件过程可信水平等方面研究较为欠缺，本书主要从这些研究内容入手，提供操作性较强的软件可信评价模型。

1.3 可信软件评价的主要研究内容

（1）软件过程可信度评价指标体系建立

可信的软件设计模式，可以创建许多其他类型的可信软件解决方案（Hoekstra，2013）。软件开发过程本质是过程实体通过一系列逻辑较为严密的过程行为（或过程活动），借助一定的组织过程资产和软件组织资源生产预定需求

功能过程产品的系列活动集合。其中：①过程实体是负责执行软件过程开发人员或者执行过程中使用到的组织资产；②过程行为是计划、监控、度量、审计、评估以及执行过程的行为方式；③过程产品是软件开发过程中生产的制品，主要指开发过程的阶段性产品，如软件需求说明书、软件设计报告、软件测试报告、软件使用说明书、构成软件的模块或组件以及集成全部功能的软件产品等。本书将从软件过程的客观属性（过程实体、过程行为、过程产品）和主观属性（软件成本、软件进度和软件质量等）等多个维度，构建软件过程可信度测度指标体系。

（2）软件产品可信度评价指标体系建立

通过阅读文献、专家访谈和大型软件用户调研，考虑软件应用环境复杂性和不确定性（uncertainty）等特征，充分利用现有的软件产品可信研究成果，在以往的软件可信属性，如保密安全性（security）、生存性（survivability）、容错性（fault tolerance）、可靠性（reliability）、可靠安全性（reliable security）和防危性（safety）的基础上，构建软件可信属性以及二级评价指标体系，建立具有可操性的可信软件评价模型。

（3）软件过程可信影响软件产品可信水平机理研究

软件过程可信影响软件产品可信，面向软件可信性质的设计和推理，将软件可信性质融入软件开发过程，使软件可信性质成为软件系统开发与应用的全过程约束，伴随着软件开发过程进行，开发的软件逐步具备这些可信性质。在软件过程可信度评价指标体系和软件产品可信度评价指标体系基础上，本书将应用结构方程模型（structural equation modeling，SEM），从理论视角分析软件开发过程可信和软件产品可信相关性，建立可信软件过程属性和可信软件产品属性映射关系结构模型，发现影响软件过程可信和软件产品可信的关键属性，通过案例研究验证软件过程可信属性和软件产品可信属性的关系，为建立可信软件综合评价模型奠定理论基础。

（4）建立可信软件过程评价模型

软件过程可信度测度主要评价过程的可信水平。根据系统工程的部分最优整体不一定最优原理，过程实体、过程行为、过程产品、成本和进度单独一个维度或者几个维度达到最优，过程总体可信水平不一定最优，本书综合考虑各个维度的相互影响和相互作用，应用模糊层次分析理论，建立反映软件过程整体可信水平的综合评价模型。

(5) 建立可信软件评价模型

可信软件是满足基于既定需求的可信性目标的产品，软件可信度是软件满足既定需求的信心度，是软件产品各个可信因素的综合反映。软件错误是软件开发过程中引入的缺陷和人为的错误，难于检测修改，同时，软件可信属性又相互影响和相互制约，只有在软件的保密安全性、生存性、容错性、可靠性、可靠安全性和实时性等属性全部满足一定的要求时，或者根据评价目标满足特定几个属性，才表明软件是可信的。因此，本书应用证据理论，结合单一属性度量模型，建立软件可信评价综合模型。

1.4 可信软件评价研究框架

为了便于读者阅读本书以及熟悉可信软件过程和可信产品评价研究的主要框架，本节主要介绍可信软件评价研究的整体思路和本书的内容安排。

1.4.1 可信软件评价研究的思路

可信软件评价研究整体思路，如图 1-1 所示。

第 1 章简述了软件开发及应用现状，提出了可信软件研究问题的意义，以及可信软件评价研究的主要问题和内容。

第 2 章通过文献回顾、专家访谈、现场调研、文献研究，系统地分析了可信软件内涵、可信软件过程管理、可信软件产品和可信软件风险管理等现有研究成果，为构建可信软件评价指标体系和评价模型奠定基础。

第 3 章从软件开发的工程过程和管理过程入手，系统地分析了可信软件过程构建的复杂性，定义了可信软件过程；应用 TSM（trusted software methodology）中 44 个可信原则，在分析 CMMI 等主流软件过程改进模型的基础上，定义了可信软件过程管理框架，形成可信保障过程域（trusted assurance process area，TAPA）、可信监控过程域（trusted monitor process area，TMPA）和可信工程过程域（trusted engineering process area，TEPA）。为有效地实施可信软件过程管理模型，建立了可信软件过程裁剪、执行、度量和改进模型和可信软件过程改进支持系统逻辑模型。

第 4 章为正确评价可信软件水平，分别构建基于软件全生命周期过程实体、过程行为、过程产品、进度和成本可信的软件过程可信属性和评价指标体系，基于软件保密安全性、生存性、容错性、可靠性和防危性的软件产品可信属性和评

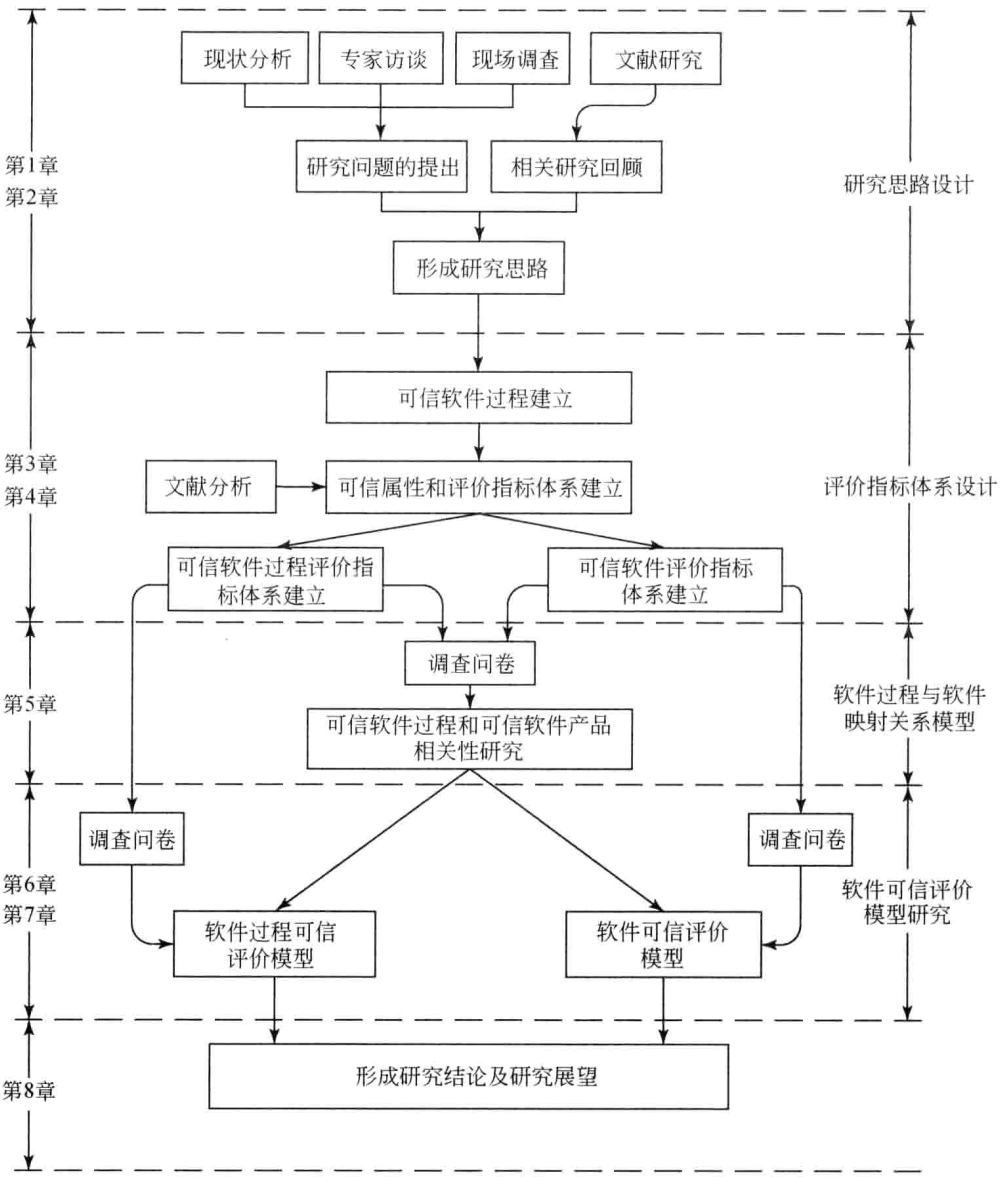


图 1-1　可信软件评价研究思路图

价指标体系，并对主要属性和指标项进行分析、定义和说明。

第 5 章根据第 4 章建立的软件可信属性和评价指标体系，应用结构方程模型（SEM）验证软件过程可信和软件产品可信的关系，定量地分析软件过程影响因素对软件产品可信因素影响映射关系。

第6章应用模糊层次分析原理，结合第4章的可信软件过程评价指标体系，建立软件过程可信评价模型，对于不同可信水平的软件过程给出其可信隶属度，表明软件过程可信到不可信的程度。通过调查问卷收集有关软件过程开发数据，对该模型进行了验证。

第7章应用证据理论（dempster-shafer，D-S），结合第4章的可信软件评价指标体系，建立软件可信评价模型，对于不同可信水平的软件给出其可信度，以及各个属性的可信水平，表明软件产品可信到不可信的程度。通过调查问卷收集有关软件产品数据，对于该模型进行了验证。

第8章总结本书研究的内容，对后续研究工作进行展望。

1.4.2 本书的主要贡献

（1）定量地分析软件过程和软件产品可信相关性

从理论上验证软件开发过程和软件产品可信的相关性，并定量地描述了软件过程可信对软件产品可信因素影响程度的数量关系；分析影响软件产品可信的软件过程因素。

（2）建立软件过程可信度评价模型

定义基于软件过程实体、软件过程产品、软件过程行为、成本和时间的可信软件过程评价指标体系，应用模糊层次分析理论，给出软件过程可信综合评价模型。模型能够分析过程可信各个属性的可信度水平，为软件过程改进提供依据。模型可以评价软件过程整体可信水平，为软件组织实施软件过程改进（software process improvement，SPI）提供决策参考。

（3）建立了软件可信评价模型

建立了基于软件保密性、软件安全性、软件生存性、软件可靠性和软件防危性等软件评价指标体系，应用证据理论，给出软件可信度测算模型。模型能够分析各个属性的可信水平以及软件的总体可信水平。由于不同软件评价指标和影响因素对于软件可信影响程度的不同，本书采用改变证据权重方法，满足不同软件产品评价的需要，同时也有效地解决了证据冲突影响软件可信水平的可信度。

（4）提出软件可信隶属度概念，更加准确地反映软件可信水平

传统的可信度分级方法往往给出相对数值（如0～1的数值），作为软件过程