中国基础研究报告

总主编 杨 卫

可信软件基础研究

可信软件基础研究项目组 编

The Fundamental Research for
Trustworthy Software

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

总主编　杨　卫

可信软件基础研究

The Fundamental Research for
Trustworthy Software

可信软件基础研究项目组 编

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

图书在版编目（CIP）数据

可信软件基础研究 / 可信软件基础研究项目组编
. — 杭州：浙江大学出版社，2018.12
ISBN 978-7-308-18871-5

Ⅰ. ①可… Ⅱ. ①可… Ⅲ. ①软件工具－研究 Ⅳ. ①TP311.56

中国版本图书馆 CIP 数据核字（2018）第 293752 号

可信软件基础研究
可信软件基础研究项目组 编

丛书统筹 国家自然科学基金委员会科学传播中心
策划编辑 徐有智 许佳颖
责任编辑 金佩雯
责任校对 高士吟
封面设计 程 晨
出版发行 浙江大学出版社
（杭州市天目山路 148 号 邮政编码 310007）
（网址：http://www.zjupress.com）
排 版 杭州中大图文设计有限公司
印 刷 浙江海虹彩色印务有限公司
开 本 710mm×1000mm 1/16
印 张 6.75
字 数 97 千
版 印 次 2018 年 12 月第 1 版 2018 年 12 月第 1 次印刷
书 号 ISBN 978-7-308-18871-5
定 价 68.00 元

总　序

合抱之木生于毫末，九层之台起于垒土。基础研究是实现创新驱动发展的根本途径，其发展水平是衡量一个国家科学技术总体水平和综合国力的重要标志。步入新世纪以来，我国基础研究整体实力持续增强。在投入产出方面，全社会基础研究投入从 2001 年的 52.2 亿元增长到 2016 年的 822.9 亿元，增长了 14.8 倍，年均增幅 20.2%；同期，SCI 收录的中国科技论文从不足 4 万篇增加到 32.4 万篇，论文发表数量全球排名从第六位跃升至第二位。在产出质量方面，我国在 2016 年有 9 个学科的论文被引用次数跻身世界前两位，其中材料科学领域论文被引用次数排在世界首位；近两年，处于世界前 1% 的高被引国际论文数量和进入本学科前 1‰的国际热点论文数量双双位居世界排名第三位，其中国际热点论文占全球总量的 25.1%。在人才培养方面，2016 年我国共 175 人（内地 136 人）入选汤森路透集团全球“高被引科学家”名单，入选人数位列全球第四，成为亚洲国家中入选人数最多的国家。

与此同时，也必须清醒认识到，我国基础研究还面临着诸多挑战。一是基础研究投入与发达国家相比还有较大差距——在我国的科学研究与试验发展（R&D）经费中，用于基础研究的仅占 5% 左右，与发达国家 15%~20% 的投入占比相去甚远。二是源头创新动力不足，具有世界影响

力的重大原创成果较少——大多数的科研项目都属于跟踪式、模仿式的研究，缺少真正开创性、引领性的研究工作。三是学科发展不均衡，部分学科同国际水平差距明显——我国各学科领域加权的影响力指数（FWCI值）在2016年刚达到0.94，仍低于1.0的世界平均值。

中国政府对基础研究高度重视，在“十三五”规划中，确立了科技创新在全面创新中的引领地位，提出了加强基础研究的战略部署。习近平总书记在2016年全国科技创新大会上提出建设世界科技强国的宏伟蓝图，并在2017年10月18日中国共产党第十九次全国代表大会上强调“要瞄准世界科技前沿，强化基础研究，实现前瞻性基础研究、引领性原创成果重大突破”。国家自然科学基金委员会作为我国支持基础研究的主渠道之一，经过30多年的探索，逐步建立了包括研究、人才、工具、融合四个系列的资助格局，着力推进基础前沿研究，促进科研人才成长，加强创新研究团队建设，加深区域合作交流，推动学科交叉融合。2016年，中国发表的科学论文近七成受到国家自然科学基金资助，全球发表的科学论文中每9篇就有1篇得到国家自然科学基金资助。进入新时代，面向建设世界科技强国的战略目标，国家自然科学基金委员会将着力加强前瞻部署，提升资助效率，力争到2050年，循序实现与主要创新型国家总量并行、贡献并行以至源头并行的战略目标。

“中国基础研究前沿”和“中国基础研究报告”两套丛书正是在这样的背景下应运而生的。这两套丛书以“科学、基础、前沿”为定位，以“共享基础研究创新成果，传播科学基金资助绩效，引领关键领域前沿突破”为宗旨，紧密围绕我国基础研究动态，把握科技前沿脉搏，以科学基金各类资助项目的研究成果为基础，选取优秀创新成果汇总整理后出版。其中“中国基础研究前沿”丛书主要展示基金资助项目产生的重要原创成果，体现科学前沿突破和前瞻引领；“中国基础研究报告”丛书主要展示重大资助项目结题报告的核心内容，体现对科学基金优先资助领域资助成果的

系统梳理和战略展望。通过该系列丛书的出版，我们不仅期望能全面系统地展示基金资助项目的立项背景、科学意义、学科布局、前沿突破以及对后续研究工作的战略展望，更期望能够提炼创新思路，促进学科融合，引领相关学科研究领域的持续发展，推动原创发现。

积土成山，风雨兴焉；积水成渊，蛟龙生焉。希望“中国基础研究前沿”和“中国基础研究报告”两套丛书能够成为我国基础研究的“史书”记载，为今后的研究者提供丰富的科研素材和创新源泉，对推动我国基础研究发展和世界科技强国建设起到积极的促进作用。

第七届国家自然科学基金委员会党组书记、主任

中国科学院院士

2017 年 12 月于北京

前　言

软件作为信息技术的重要载体，已渗透到政治、经济、军事、文化及社会生活的各个层面。但随着软件规模越来越大，软件的开发、集成和持续演化变得越来越复杂。复杂性带来的软件缺陷问题往往会导致各类事故甚至是严重的灾难，因此，关于可信软件的研究已成为国民经济发展的迫切需求。

针对软件可信需求的基础研究，国家自然科学基金委员会于 2007 年开始实施“可信软件基础研究”重大研究计划。这是“十一五”期间启动的重大研究计划之一，由信息科学部牵头，会同数学物理科学部、管理科学部联合组织实施。本重大研究计划历时十年，共资助项目 107 项，其中培育项目 73 项、重点支持项目 24 项、集成项目 5 项，资助总经费达 1.9 亿元。

本重大研究计划采用国家自然科学基金资助管理体制与专家学术指导体制相结合的管理架构，设立计划管理工作组（负责对实施重大研究计划的总体审核、协调及组织评估）；设立研究计划管理办公室（挂靠华东师范大学，负责向公众及时公布研究计划的立项情况、研究进展及相关事宜，便于计划的具体实施与管理）。

“可信软件基础研究”重大研究计划聚焦四大类核心科学问题——软

件可信性度量与建模、可信软件的构造与验证、可信软件的演化与控制以及可信环境的构造与评估。本重大研究计划以嵌入式软件和网络应用软件可信性问题为主攻目标，以国家关键应用领域中软件可信性问题为突破口，建立可信软件基础研究的研究框架，研究成果揭示了软件可信性和环境可信性度量与演化的基本规律，构建了可信软件及其环境构造与验证、演化与控制的方法和关键技术体系，建立了可信软件开发工具和运行支撑平台。

本重大研究计划在实施过程中，产生了大量研究成果。为了能够更好地推广这些研究成果，项目组总结了“可信软件基础研究”重大研究计划实施以来所取得的重大研究成果，包括基础理论、关键技术和关键领域应用的实施成果，编写了本书并收录到“中国基础研究报告”丛书。希望本书能够为我国从事可信软件基础研究的科研工作者以及从事安全攸关领域的技术研发者提供参考，进一步推动可信软件的发展。

最后，感谢国家自然科学基金委员会对“可信软件基础研究”重大研究计划的大力支持，感谢信息科学部、数学物理科学部和管理科学部的联合组织实施，感谢项目指导专家组所有同仁的努力，更要感谢研发任务的承担者和实施者为本重大研究计划圆满完成及实施做出的巨大贡献。

“可信软件基础研究”重大研究计划指导专家组组长

中国科学院院士

2018 年 12 月于上海

目 录

第 1 章　项目概况

1.1　项目介绍

随着现代信息技术创新及其广泛应用，软件已经成为现代计算机系统的灵魂，成为国家信息化建设的核心，成为当代社会生产力发展和人类文明进步的强大动力，在国民经济、社会发展和国防建设中发挥着举足轻重的作用。

现代信息社会对计算机系统的依赖，很大程度上体现为对软件的依赖，而计算机系统很大一部分缺陷都是软件问题导致的。随着软件的应用需求越来越多，复杂度越来越高，可用性要求越来越强，软件系统也越来越庞大和脆弱，而且并不总是值得信任的。很多时候它会不以人们所期望的方式工作，发生各种故障和失效，从而直接或间接地对用户造成巨大损害。这类问题被称为“软件可信性”问题。

“可信”是在传统的“安全”“可靠”等概念基础上发展起来的一个相对较新的学术概念。一般认为，所谓“可信”，是指一个实体在实现给定目标时，其行为及其结果是可以预期的。它强调目标与实现相符以及行为与结果的可预测性和可控制性。所谓“可信软件”，是指软件系统的运行行为及其结果总是符合人们的预期，并且在受到干扰时仍能提供连续的服务。

国际上由软件可信性问题导致的重大灾难、事故和严重损失屡见不鲜：1996 年 6 月 4 日，在欧洲阿丽亚娜 5 型火箭的首次发射过程中，惯性参考系统软件的数据转换错误导致软件失效，使得火箭在发射 40 秒后爆炸，造成 25 亿美元的经济损失；2005 年 11 月 1 日，日本东京证券交易所因软件升级出现系统故障，股市严重停摆；2017 年 5 月 12 日，WannaCry 勒索病毒在全球蔓延，渗透了至少 150 个国家的 20 万台电脑。软件可信性问题已经成为一个相当普遍的问题。在 Google 上可以搜索到的与软件错误相关的网页就有 100 多万个。软件故障和失效所带来的影响也愈来愈大。据美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）估计，美国软件失效所造成的年度经济损失约占其 GDP 的 0.6%。由此可见，如何高效地开发可信软件系统，已经成为软件研究领域必须面对的核心问题和重要挑战。

可信软件已成为现代软件技术发展与应用的重要趋势和必然选择。一方面，软件的规模越来越大，软件的开发、集成和持续演化越来越复杂，而目前的可信软件构造与运行技术和软件可信性度量与评测工作严重缺乏，使得软件产品在推出时就含有很多已知或未知的缺陷，对软件系统的安全可靠运行构成了严重威胁。另一方面，软件的运行环境和开发环境已经从传统的封闭静态环境拓展为开放、动态、多变的互联网环境，网络交互、共享、协同等带来了很多不可信因素，网络上对信息的滥用和恶意篡改使得可信问题日益突出。在互联网环境下，计算实体的行为具有不可控性和不确定性，这既对传统的软件开发方法和技术提出了严峻的挑战，也对软件运行时的可信保障提出了苛刻的要求。

国家自然科学基金委员会在广泛听取各界专家意见和反复深入研讨的基础上，由信息科学部、数学物理科学部和管理科学部联合组织，于 2007 年启动了“可信软件基础研究”重大研究计划（以下简称本重大研究计划）。这是我国软件基础研究领域的一件大事。本重大研究计划对应对软件发展

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，具有非常重大的意义。本重大研究计划共资助项目 107 项，其中培育项目 73 项、重点支持项目 24 项、集成项目 5 项，资助总经费达 1.9 亿元，全部资助项目已于 2017 年底顺利结题。

1.1.1 总体科学目标

本重大研究计划以国家关键应用领域中软件可信性问题为主攻方向，总体科学目标如下：

①采用理论研究和实证研究相结合的方法，揭示软件可信和环境可信失效、度量和演化的基本规律，建立可信软件及其环境构造与验证、演化与控制的方法和关键技术体系，研究可信软件开发工具和运行支撑平台及环境；

②在典型的嵌入式软件和网络应用软件中进行验证和示范，促进软件从传统的单一度量理论到综合性的可信度量理论及其构造方法的集成升华，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；

③在可信软件领域集聚和培养一批站在国际前沿、具有理论和源头技术创新能力的高水平研究人才队伍，促进我国软件产业的崛起和发展。

1.1.2 核心科学问题

本重大研究计划的核心科学问题包括以下四大类。

（1）软件可信性度量与建模

传统的软件理论是围绕程序正确性建立的，其正确性的刻画以定性方

法为主，并且是以静态确定性的表达给出的。对于可信软件，需要考查正确性、可靠性、安全性等诸多属性的综合度量空间，形成对软件可信性的科学理解，从管理科学的角度，以定量的方式建立可信性建模的系统方法论，以及适应环境依存稳定性条件下的可信度动态演化特征。因此，必须从如何认知软件可信性的角度建立新的软件系统方法论，从如何表述软件可信性的角度建立可信需求的建模、规约和分析方法，从如何把握软件可信性的角度揭示软件可信性演化的基本规律，从而解决如何建立软件系统可信度量标准以及如何在其工作环境中进行评估的问题，对软件系统的可信性进行分级，并提供量化指标。

软件可信性度量与建模研究需要解决的基础科学理论问题及研究要点包括以下几方面。

①软件可信性度量系统。研究软件缺陷与可信性的内在联系、软件缺陷预测和缺陷分布规律；研究多维可信属性的多尺度量化指标系统、度量和评估机制以及测评体系；研究可信属性之间的交互关系及其涌现特征，包括多属性 / 综合属性的局部 / 全局相容与失配等；建立可信软件度量的技术标准或管理标准方案。

②软件可信性的演化与预测。研究软件可信性相关数据的收集、分析和知识挖掘方法；研究软件在环境和自身演化下可信性的演化规律以及软件在线演化的基础理论；研究基于软件行为的软件可信性增长和面向威胁的在线评估与预测理论。

③可信软件的风险及过程管理。研究可信软件生命周期的风险识别、评估、管理和控制模式及方法；研究可信软件过程的属性和度量框架以及相应的量化控制和度量评估方法；研究适应分布性、敏捷性和过程资产复用性等需求的可信软件过程建模、定制、仿真和优化方法；研究可信软件的人—信息系统交互作用及优化机理。

（2）可信软件的构造与验证

传统的软件理论在软件构造与验证时注重在封闭环境下追求不可演化的绝对正确和效率优先。对于可信软件，必须适应开放环境下物理世界中的计算规律，从追求软件绝对正确和效率优先的软件方法学变为力求保证在可演化的环境下满足可信需求的软件方法学。因此，如何进行可信性算法设计和软件设计、如何消解多属性引起的可信性冲突、如何进行可信性保证成为解决可信软件开发问题的关键。

可信软件的构造与验证研究需要解决的基础科学理论问题及研究要点包括以下几方面。

①可信软件的程序理论与方法学。研究软件行为可信特征空间的概念模型及形式化体系，包括程序的近似和渐近正确性理论，以及刻画软件的近似可信性与演化可信性理论；针对可信软件形态的多样性、动态性和协同性，特别是数据与控制同时动态变化的新特征，研究网络环境下的可信软件系统形式化模型；研究软件系统集成的基础理论以及对可信性影响的推理基础；从风险和病态角度，研究可信约束下的软件病态特征提取技术、软件病态及环境间的关系，以及相应的预测理论与控制方法；建立可信软件全周期开发方法学。

②可信软件的需求工程。研究面向可信性的需求分析方法；研究基于社会的可信模型的需求工程方法；研究风险分析和可信性分析技术；研究软件可信性的性质获取与形式规约；研究多维异质非功能需求的冲突消解与完整性表述方式；探索基于领域知识的可信性分析方法和理论。

③可信软件设计、构造与编译。研究可信软件设计的系统化科学体系，包括基于构件的、面向服务的和基于面向方面技术的可信软件的构造方法和代码生成技术；研究支持软件自演化的可信软件体系结构；研究可信程序设计的基础要素和语言设计，以及可信编译技术；研究算法可信性度量

和可信算法设计的数学基础，针对典型科学计算问题，研究误差可控计算的基础算法等。

④可信软件的验证与测试。研究复杂环境下嵌入式软件和开放环境中网络软件的形式建模与分析技术，以及可信软件的模型自动抽取技术；研究多层次可信软件可扩展形式验证方法和错误定位方法；研究面向可信性的测试策略和基于控制理论的自适应测试方法；研究基于模型和规约的可信软件测试技术；研究可信软件验证与测试的集成方法，以及基于测试和验证数据的可信性评估与预测方法。

（3）可信软件的演化与控制

传统的软件理论仅从静态的角度认识软件部署后的变化，对于软件维护往往是事后被动响应；而开放环境下软件的演化是软件面向可生存性需求的重要特征。对于可信软件，需要从事后维护向事前设计、主动监控变化，形成与软件动态演化中的可信性相适应的控制方法。因此，如何认识环境的演化和软件自身的演化、如何动态获取可信性和控制可信性的变化、如何构建可信的运行平台是解决可信软件在开放动态环境中可信运行问题的关键。

可信软件的演化与控制研究需要解决的基础科学理论问题及研究要点包括以下几方面。

①可信软件运行监控机理。研究软件运行时环境变化和软件变化对可信性的影响；研究复杂开放环境下基于运行监控的可信软件模型和体系结构；研究面向可信软件演化特性的软件运行监控与保障机制。

②软件可信性动态控制方法。研究软件运行时的行为监控与可信性监测、诊断、恢复方法，以及基于虚拟化环境的软件系统故障范围控制和快速恢复方法与机制，包括基于动态控制更改的可信软件运行的自主管理机制和代码维护关键技术、多维度监控的关注点分离技术，以及基