DOI: 10.16262/j.cnki.1000-8217.2008.03.012

·学科进展与展望·

“可信软件基础研究”重大研究计划综述

刘 克[1] 单志广[2] 王 戟[3] 何积丰[4] 张兆田[1] 秦玉文[1]

(1 国家自然科学基金委员会信息科学部，北京 100085；2 国家信息中心信息化研究部，北京 100045；
3 国防科技大学计算机学院，长沙 410073；4 华东师范大学软件学院，上海 200241)

[摘 要] 国家自然科学基金委员会启动实施了“可信软件基础研究”重大研究计划。本文从该重大研究计划的立项背景和意义，可信软件的研究现状，该重大研究计划的科学目标与核心科学问题，以及预期成果等方面进行了介绍。

[关键词] 可信软件，重大研究计划，国家自然科学基金

1 引言

“可信软件基础研究”重大研究计划已于2007年底正式启动，它是国家自然科学基金委员会“十一五”期间启动的重大研究计划之一，由信息科学部、数学物理科学部和管理科学部联合组织，实施周期6年，计划经费1.5亿元。第一期项目经费2900万元，资助重点支持项目4项，培育项目38项。

“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，具有深远的意义。该重大研究计划启动以来，受到了学术界和产业界的广泛关注和热心支持。

2 立项背景和意义

2.1 立项背景

以通信、存储和计算为核心的信息基础设施已经渗透到政治、经济、军事、文化以及社会生活的各个层面，成为当代生产力发展和人类文明进步的强大动力。软件是信息基础设施的灵魂，随着人们对功能需求的不断增加，软件系统变得日趋庞大和难以驾驶，缺陷和漏洞难以避免，系统越来越脆弱，很多时候不以人们期望的方式工作，经常发生各种故障和失效，直接或间接地给用户带来损失。软件并不总是让人信任的，这就是我们所说的“软件可信性”问题。

国际上由于软件缺陷而导致的重大灾难、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型火箭的首次发射中，由于惯性参考系统软件的数据转换错误引起操作失误，致使火箭在发射40秒后爆炸，造成25亿美元的经济损失；2003年5月，由于飞船的导航计算机软件设计错误，俄罗斯“联盟-TMA1”载人飞船在返回途中偏离预定降落地点约460 Km；2003年8月14日，在美国电力检测与控制管理系统中，由于分布计算机系统试图同时访问同一资源引起软件失效，造成美国东北部大面积停电，损失超过60亿美元；2004年9月14日，由于空管软件中的时钟管理缺陷，美国洛杉矶机场400余架飞机与机场指挥系统一度失去联系，给几万名旅客的生命安全造成威胁；2005年11月1日，日本东京证券交易所由于软件升级出现系统故障，导致股市停摆。

在我国，仅2006年，中航信离港系统就发生了三次软件系统故障，造成近百个机场登机系统瘫痪；2006年4月20日，中国银联跨行交易系统出现故障，使整个交易系统瘫痪约8小时；网络犯罪问题日趋严重，2006年我国共查处境内信息网络犯罪案件41 379起，比2005年增加98.9%；2007年的“熊猫烧香”病毒一夜之间就使上百万台计算机感染并遭到损害；境外敌对势力也利用软件缺陷对大陆实施信息攻击计划(例如木马计划、达尔文计划和茉莉计划等)，严重危害着国家安全。

软件可信性问题已经成为国际上一个普遍关注

本文于2008年4月6日收到.

的问题,仅在 Google 上就可以搜索到 100 多万个与软件错误相关的网页。软件故障和失效所带来的影响也越来越大,2002 年美国 NIST 估算,美国每年因软件失效所造成的年度经济损失近 600 亿美元,约占其 GDP 的 0.6%。如何构造出缺陷较少的软件并保障其安全可靠运行,已经成为软件研发者义不容辞的责任。

"可信性"是在正确性、可靠性、安全性、时效性、完整性、可用性、可预测性、生存性、可控性等众多概念的基础上发展起来的一个新概念,是客观对象诸多属性在人们心目中的一个综合反映。学者们试图从不同角度、不同层次去诠释"可信性",但尚未形成共识,需要在实践中不断认识和把握。一般认为,"可信"是指一个实体在实现既定目标的过程中,行为及结果可以预期,它强调目标与实现相符,强调行为和结果的可预测性和可控制性。软件的"可信"是指软件系统的动态行为及其结果总是符合人们的预期,在受到干扰时仍能提供连续的服务。这里的"干扰"包括操作错误、环境影响、外部攻击等。

构造可信软件已成为现代软件技术发展和应用的重要趋势和必然选择。一方面,软件的规模越来越大,导致软件的开发、集成和维护工作越来越复杂,目前的可信软件构造与运行保障技术、可信性度量与评测方法严重缺乏,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不同程度的威胁。另一方面,软件的开发环境和运行环境已经从传统的封闭、静态环境发展为开放、动态、多变的互联网环境。网络交互、共享和协同带来了很多"不可信"因素,网络上对信息的滥用和恶搞,使得可信问题变得更加突出。互联网环境中计算实体的行为具有不可控性和不确定性,这种状况既对传统的软件开发方法和技术提出了重要挑战,也对软件运行时刻的可信保障提出了严峻要求。

基于以上背景,国家自然科学基金委员会在广泛听取专家意见和反复深入研讨的基础上,适时启动了"可信软件基础研究"重大研究计划。

2.2 科学与现实意义

"可信软件基础研究"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目标,分析、研究和解决相关科学问题,在嵌入式软件和网络应用软件中开展示范应用,旨在为提高国家重大工程中的软件可信度提供科学支撑。

(1) 可信软件研究计划可望推动软件基础理论的探索与创新

早期开发软件的首要目标是在效率和成本优先的前提下构造出功能正确的系统,对于可信任性、可用性、安全性等问题的考虑相对较少,尤其在软件构造理论与方法、构造过程、体系结构、运行环境等方面,没有建立相应的可信支撑机制,使得软件在规模增大以后,可信性问题越来越突出,具体表现为软件行为预测困难、软件失效代价增加。

单一的正确性属性已无法完成对软件这一复杂对象的刻画,人们已经认识到软件的各种属性之间相互关联和影响。在封闭、静态环境下发展起来的以正确性为核心的软件理论、方法、技术和机制,已经不足以构造出适应开放、动态、多变环境的可信软件。其局限性主要表现为:软件开发过程缺乏基础理论的有效支持;用户需求与软件构造难以直接映射;软件功能和性能的确认与验证自动化水平低下;软件的动态容错和演化缺乏方法和运行方面的支撑。

传统的"面向正确性的软件理论 + 工程化"模式已经不能适应现代软件系统的特点。软件基础理论正处于一个转型期——转向以软件可信性度量为基础,全面考虑软件需求分析、建模、生成、测试验证、维护和演化等阶段和运行支撑等方面的可信问题。因此,对可信软件进行系统而深入的研究,将有利于在新的需求和环境下,促进软件理论、方法和技术的源头创新,带动信息科学、数理科学、管理科学的交叉和共进。

(2) 可信软件研究计划有助于应对软件发展的重要科学挑战

可信软件研究计划将着力探索和建立可信软件系统并验证其可信度,积极应对当今软件发展历程中所面临的复杂性、开放性和演化性等一系列重要挑战:

(i) 复杂性。软件系统的规模和复杂性、以及用于构建系统的构件及其互联的规模和复杂性都在增长。以嵌入式软件为例,2005 年奥迪 A8 的嵌入式代码达到了 90 MB;空中客车 A380 在 400 MB 的嵌入式软件支持下实现了约 100 个飞机功能;此外,A380 还包括了约 60 万个信号接口,为完成一个功能,嵌入式软件运行在分布式互连的嵌入式控制单元上。而 Internet 上软件系统的规模与复杂性更有过之。

(ii) 开放性。网络已成为各种应用的重要平台,计算模式向"以网络为中心的环境和面向服务的

体系结构"发展,软件的运行环境(包括网络环境、物理环境)不断开放和动态变化,使得软件构件在无监督下实现可信安全交互的需求日趋强烈。然而目前的理论、技术和管理储备均不足以应对开放性带来的挑战。例如,无线技术的广泛采用可能会给网络中引入恶意或劣质的构件;开源软件与专有软件的开发方式显著不同,开源软件的大量引入对传统的软件质量提出了挑战;不同类型的软件构件(包括COTS、GOTS和定制软件,开源软件和专有软件等)组成的软件系统的行为如何把握也成为一个难题。

(iii) 演化性。随着软件需求多变性的发展,新技术、新功能的演变与拓展以及人们对软件生存性的要求,使得软件的开发已经不可能一蹴而就,而是可能贯穿软件的整个生命周期。软件的持续演化,给业已复杂的网络和自主软件构件带来了更多的复杂性。

(3) 可信软件研究计划有助于促进我国软件产业的振兴与发展

近年来,我国软件产业得到了长足发展,但从整体上看,在世界上所处的地位仍然偏低,其发展仍处在发达国家和周边发展中国家的"夹缝"之中。我国软件产业对国民经济发展的贡献较小,其规模和发展速度均不能满足国家信息化建设的要求,国产软件所占份额有限,缺乏核心产品和关键技术,产业竞争力薄弱,难与跨国公司抗衡。当前,我国经济的快速发展已经对新型软件(嵌入式软件和互联网服务型软件)提出大量需求,为软件产业发展提供了一个很好的机遇,希望该重大研究计划的实施能够推进软件技术与应用的创新,有助于我国软件行业走出一条既符合国情又能占领知识经济制高点的发展道路。

3　可信软件研究现状

上世纪60年代末的软件危机促成了软件工程学科的诞生,在计算机发展史上有着里程碑式的意义。软件工程的一个重要目标就是开发出高质量、高可靠的软件系统,其相关的理论和技术直接或间接地提高了软件的可信性。例如,结构化程序设计方法、软件的文档管理、程序生成技术、程序验证技术、软件测试技术、构件技术、软件过程控制等都不同程度地提高了软件的可靠性。然而,传统软件工程的首要目标是在有限的资源约束下开发出功能正确、质量可靠的软件系统,并没有把软件的可信性作为最主要的研究内容。

随着软件可信性问题的凸显,近年来人们开始从不同的角度、不同的出发点研究与软件可信有关的问题,如可靠性、可用性、安全性和生存性问题。可靠性(Reliability)关注在规定的条件和时间间隔内,计算机系统和软件能正常运行的概率。提高软件可靠性的技术途径有避错法和容错法等,其中容错计算(Fault-Tolerant Computing)是研究热点。可用性(Availability)则关注软件在某一时刻所能提供有效功能的程度,提高可用性的技术途径有软件系统的可靠性和可维护性理论与方法、故障诊断与测试技术、系统恢复技术等。网络软件安全则将信息安全的研究范围拓展到开放、动态、多变的网络环境下。人们不断从软件工程、形式化工程、软件过程等途径,研究如何开发高质量、低缺陷的软件系统,并开发各种支持工具,提高软件生产力,增强软件可信性。

近几年,发达国家的政府组织、跨国公司、大型科研机构逐步认识到可信软件研究的巨大价值和应用前景,纷纷有针对性地提出了相关研究计划。美国《国家软件发展战略(2006—2015)》将开发高可信软件放在首位,提出了下一代软件工程的构想。美国国土安全部2006年启动了Software Assurance Program,目的是改进可信软件产品的开发与部署。美国政府的"网络与信息技术研究发展计划(NITRD)"中,列出了8个重点领域,有4个与"可信软件"密切相关。在"高可信软件与系统"领域,NITRD在2006年投入约1.34亿美元,其中,美国自然科学基金会(NSF)投入约0.41亿美元;在2007年投入预算1.45亿美元,其中NSF投入预算0.53亿美元。NSF近3年(2006—2008)在可信软件研究领域拟投入1.52亿美元。NSF在加州大学伯克利分校建立了科学与技术研究中心TRUST,其目标是为设计、构建和运行可信信息系统建立新的科学与技术基础,从2005年6月至2010年10月拟投入1900万美元研究经费。该中心有8所大学参与,并与IBM、Intel、HP、Microsoft、SUN等15个跨国公司开展工业界合作。国际上著名的研究项目还有NSF新近启动的Science of Design计划,NASA在卡内基梅隆大学支持的HDCC项目,DARPA资助的OASIS,德国教育研究部资助的Verisoft和德国研究联合会(DFG)资助的AVACS项目,英国的INDEED和DIRC研究项目等。

在如何保证软件的可信性方面,形式化理论和软件验证技术获得了持续关注。例如,图灵奖得主

霍尔提议将 Verified Software(验证过的软件)作为计算机科学中的一个重大挑战性问题,希望能像人类基因组计划那样,通过国际合作取得重大进展。国际著名刊物《理论计算机科学》的两辑之一就是关于程序设计理论的讨论,特别是形式语义、形式验证。图灵奖得主迪杰斯特拉、霍尔、米尔纳、伯努利等人都在程序设计领域采用各种形式化方法提高程序的可靠性和安全性,例如,霍尔的顺序程序的公理化理论通过前后置断言,给出了顺序程序的部分正确性和完全正确性的形式推理系统。程序分析和验证技术在近几年取得了一些突破,例如,Poldelski 和 Rynbachenko 基于线性代数理论提出了一个完备的一类线性程序线性秩函数生成理论,并将其实现,即 RANKFINDER。RANKFINDER 是他们和微软联合开发的程序终止性分析工具 TERMINATOR 的核心部分。TERMINATOR 已经被成功应用到多个设备驱动程序的终止性分析中,这些 C 程序的规模从 5000 行到 35 000 行不等。在对 23 个设备驱动程序的验证中,TERMINATOR 发现了 8 个终止性错误。基于抽象解释的程序验证工具 ASTREE 分别对空中客车 A340 主飞控软件(13.2 万行 C 代码)和 A380 主飞控软件(35 万行 C 代码)进行了验证,在验证规模上有所突破,但仍然存在一定局限性,只能针对特定软件进行验证和调优,验证的性质也都是程序的内部性质。

目前的可信软件研究是从软件正确性、可靠性、安全性、生存性等基础上发展起来的,软件形式化理论和验证技术、可靠性工程、网络信息安全等领域均有针对若干可信属性的研究。但是软件可信性不是正确性、可靠性、安全性和生存性等性质的简单相加,可信软件研究也不是对已有的各种软件属性研究进行简单的综合。首先,由于软件系统越来越复杂,软件可信意味着软件行为可信、环境可信和使用可信等不同层次的可信要求,而局部的可信并不一定导致全局的可信。系统的可信性属于涌现类的性质,如何从整体上度量、获得并保证可信性将是非常困难的;其次,不同可信属性之间可能彼此有冲突,并且不同层次之间也可能会有冲突,如何最优化地协调与取舍也是一个关键问题;第三,当软件可信性成为研究目标之后,必然要针对"可信"性质建立分析、构造、度量、评价体系,使得可信性能够在软件生产活动中被有效地跟踪控制和验证实现,这也对现有的计算理论与技术体系提出了挑战。需要强调的是,要达到软件可信的目标,需要对软件系统开发的整个生命周期,需求分析、可信算法设计、软件设计与实现、测试与验证、运行维护等阶段进行全面而统一的研究。用户对软件可信性的认可还有一个积累和沉淀的过程,在软件运行过程中,软件的可演化特征也是现有静态分析、测试技术无法应对的。

从研究方法上看,已有的经验表明,软件开发过程过于依赖开发人员的知识和经验,有许多不规范之处;而软件动态行为高度复杂,难于定量预测。许多关于软件开发过程和软件动态行为的论述难于验证。这就促使许多软件工程研究人员开展实证软件工程(Empirical Software Engineering)研究,旨在以数据和证据来验证关于软件的论断。但目前实证软件工程研究存在两方面的问题。第一,在案例研究和数据收集过程中仍然依赖于人的参与,软件开发过程的活动和软件系统动态行为往往不具有可重复性;第二,研究目标局限于技术层次,旨在验证某种技术的有效性,而忽视了软件开发过程和软件系统动态行为可能存在某种不以人的意志为转移的客观规律。

可信软件离不开可信环境。可信计算的基本思想是:首先构建一个信任根,再建立一条信任链,从信任根开始到硬件平台、到操作系统、再到应用,一级认证一级,一级信任一级,从而把这种信任扩展到整个计算系统,确保整个计算系统的可信。1983 年美国国防部制定了世界上第一个《可信计算机系统评价准则》TCSEC(Trusted Computer System Evaluation Criteria)。1999 年,IBM、HP、Intel、微软等著名 IT 企业发起成立了可信计算平台联盟 TCPA(Trusted Computing Platform Alliance)。2003 年 TCPA 改组为可信计算组织 TCG(Trusted Computing Group),标志着可信计算技术和应用领域的进一步扩大。TCPA 和 TCG 已经制定了关于可信计算平台、可信存储和可信网络连接等一系列技术规范。欧洲于 2006 年 1 月启动了名为"开放式可信计算(Open Trusted Computing)"的可信计算研究计划,已有 23 个科研机构和工业组织参与。微软提出了代号为 Palladium 的可信计算计划,推出的新一代操作系统 VISTA 支持可信计算机制。然而,无论是国外还是国内,在构建可信计算环境方面都呈现出技术超前于理论、理论滞后于技术的状况。至今,尚没有公认的可信计算理论模型。TCG 提出的可信计算平台的系统结构,是迁就现有机器的结果,是向市场妥协的结果,并不一定是理想的可信系统结构。在关键技术上,可信的安全多方计算环境的构造、完

整的信任链机制、可信虚拟机以及相关的测评方法都存在需要攻克的难题。

4 科学目标与核心科学问题

4.1 科学目标

"可信软件基础研究"重大研究计划的科学目标是：针对国家信息化发展和重大工程应用对可信软件的战略需求，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的失效、度量和演化的基本规律，建立可信软件及其环境的构造与验证、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，并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性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，培养一批高水平的研究人才，促进我国软件产业的崛起和发展。

4.2 核心科学问题

该重大研究计划涉及以下四个科学问题：

(1) 软件可信性度量、建模与预测

传统的软件理论是围绕程序正确性建立的，对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。对于可信软件，我们需要考察包括正确性、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，以定量方式给出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，从而解决软件系统可信度量标准和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建立分级，并提供量化指标。主要研究内容包括：

(i) 软件可信性度量。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、度量和评估机制及测评体系；研究可信属性之间的交互关系及可能的涌现特征，包括多个属性/综合属性的局部/全局相容与失配情况；建立可信软件度量的技术标准或管理标准方案。

(ii) 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。

(iii) 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；研究可信软件中"人与信息系统"的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只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可演化的软件可信性满足需求的软件方法学。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是解决可信软件开发问题的关键。主要研究内容包括：

(i) 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的影响的推理基础；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。

(ii) 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。

(iii) 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，包括基于构件的可信软件的建模、构造方法与代码生成技术，面向服务的可信软件的建模、构造方法与代码生成技术，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，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。

(iv) 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和分析技术,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和预测方法。

(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,对于软件的维护往往是事后的被动响应。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,形成对软件动态演化中的可信性控制方法。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。主要研究内容包括:

(i) 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。

(ii) 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热维护关键技术、多维度监控的关注点分离技术,以及基于运行监控的可信性动态评估机制;研究网络计算环境的高可信支撑软件技术。

(4) 可信环境的构造与评估

软件可信性离不开环境的支撑,环境可信是可信软件的重要方面。但是可信环境的基础理论研究滞后于可信计算技术的研究,需要探求在网络环境下构建一个相对可信的计算环境的理论和方法。因此,可信环境体系结构的形态、如何建立信任链并且传递和管理信任关系、如何构造可信的安全多方计算环境、如何评价一个计算环境的可信程度成为必须面对的问题。主要研究内容包括:

(i) 可信环境的数学理论与信任传递理论。研究支持可信计算的数学模型、形式化模型,构建可信计算的理论体系;研究可信网络计算的形式化模型,形成完整性保护的理论体系;研究信任链的建立与信任的传递机理,重点研究支持信任链建立与扩展的无干扰模型。

(ii) 可信计算环境构造机理及方法。研究基于可信硬件层灵活扩展信任边界的体系结构,以及可信计算平台的完整性收集、度量、验证的体系结构和网络连接与认证的体系结构;研究可信计算与虚拟技术结合的新型可信虚拟平台架构,重点探索基于可信平台模块的虚拟平台安全体系结构以及可信平台模块的虚拟化技术;研究可信的安全多方计算环境的构造方法。

(iii) 可信计算环境测评。研究适用于可信计算平台的安全评估模型;研究可信平台模块协议检测方法,包括可信计算平台安全功能测试、标准符合性测试、穿透性测试等技术,对认证、授权和平台证明协议的正确性、安全性和性能的验证提供支持。

5 预期成果

(1) 基础理论研究方面:将在多维可信属性的多尺度量化指标系统、网络环境下可信软件系统形式化理论、软件的近似可信性与演化可信性理论、信任链建立与传递的无干扰模型等方向形成国际上有特色和影响力的理论成果。

(2) 关键技术研究方面:将突破需求工程中的可信性分析、自演化可信软件体系结构、误差可控计算基础算法、可信程序设计语言及编译、验证与测试集成的可信性保证、软件运行监控与保障框架和可信的安全多方计算环境的构造等一批可信软件构造与运行支撑的关键技术,通过软件工具和环境实现技术的"物化",建立可信软件开发工具集、可信软件运行支撑平台和可信虚拟机。

(3) 试验验证环境和典型应用示范方面:将建立一个大规模综合试验环境,以此为基础,面向嵌入式软件系统(航空、航天高可信软件等)、网络应用软件系统(网上银行交易系统等)分别建立嵌入式高可信软件系统试验验证环境和网络应用软件系统试验验证环境。具体指标是应用系统规模达到航空航天子系统(万行代码量级)高可信需要、网络应用软件系统(百万行代码量级)可信需要,建立面向国家重大工程的关键软件研制全过程的试验验证环境,集成的工具实现 60% 以上的自动化。通过实际应用

案例统计，与传统方法相比，基于该研究计划的成果，软件失效在整个系统的失效比例控制在10%以内，千行代码缺陷个数降低50%。对高可信软件的"归零率"到达99%。

(4) 可信软件标准和可信软件教育方面：将建立软件可信性的分级参考体系、可信软件的构造和运行保障方面的相关技术标准建议，发表有影响力的可信软件领域的论文和专著，支持研究成果的技术转移和知识传播。

(5) 国际交流与合作方面：将发起和建立有关国际学术组织、学术刊物和国际会议；与相关国家共同开展国际合作研究。

总之，该重大基础研究计划将通过软件可信性的度量理论和支持可信性演进的软件开发方法学形成基础性理论创新，形成对软件可信性多维、多尺度的建模和可信软件全生命期的决策支持，在研究方法上形成实验性和推理性综合的特色，充分利用我国特有的软件可信性实验数据开展研究，并将研究成果在大规模可控的国家级实验环境上进行验证和示范。

6 结语

大规模资助软件基础研究，在国家各个科研资助部门中尚属首次，对科研人员和管理人员而言，机会与风险共存。在今年6年时间里，可信软件研究计划能否取得高质量的学术研究成果，能否对国家信息化进程起到支撑作用，能否为我国软件产业和重大相关应用做出贡献，是各界人士共同关注的问题。作为基础性创新研究活动的参与者，我们能否形成有自己特色的研究思路，能否得到国际同行的充分认可，能否在国际学术界占有一席之地，能否在国际标准化组织中拥有话语权，都直接影响着研究计划的完成质量。该重大研究计划特别鼓励针对核心科学问题的具有原始创新思路和独具特色的探索性研究；鼓励研究单位与应用单位紧密合作，面向重大应用开展有针对性的研究；鼓励不同学科的交叉和融合；鼓励利用国际合作展开高效的研究。从第一期近300个申请项目的总体情况看，研究人员在已有研究基础上积极向"可信软件构建"这一核心任务靠拢，广泛联系国内重要应用单位和国际同行学者，表现出了很高的研究热情和责任感，但也存在一些问题，例如：对"可信性"这一核心概念的分析不够系统深入，对核心科学问题的触碰力度尚嫌不足，对核心任务和总体目标的把握还需要加强，在创新思路和研究特色方面也还有待进一步发掘。相信随着研究工作的不断深入，这些问题会逐步得到解决。

该重大研究计划自2006年9月召开第一次立项研讨会，到2007年9月发布第一期项目指南，其间经历了多次学术思想交流与碰撞，建议书修改十几稿，倾注了许多专家学者的心血，得到了各级领导和相关学科人员的鼎力支持。本文凝聚了很多专家学者的真知灼见，限于篇幅，不再悉数列举，在此一并表示感谢！

OVERVIEW ON MAJOR RESEARCH PLAN OF TRUSTWORTHY SOFTWARE

Liu Ke[1] Shan Zhiguang[2] Wang Ji[3] He Jifeng[4] Zhang Zhaotian[1] Qin Yuwen[1]

(1 *Department of Information Sciences, National Natural Science Foundation of China, Beijing* 100085;
2 *Department of Informatization Research, State Information Center, Beijing* 100045;
3 *School of Computer Science, National University of Defense Technology, Changsha* 410073;
4 *School of Software Engineering, East China Normal University, Shanghai* 200241)

Abstract The major research plan of trustworthy software was set up by the National Natural Science Foundation of China. This paper introduces the background and significance of the plan, the current status of the trustworthy software research, the scientific objectives and associated scientific problems of the plan, and the expected results.

Key words trustworthy software, major research plan