·研究进展·

“可信软件基础研究”重大研究计划结题综述

何积丰[1]　单志广[2*]　王　戟[3]　蒲戈光[1]
房毓菲[2]　刘　克[4]　赵瑞珍[4]　张兆田[4]

(1. 华东师范大学计算机科学与软件工程学院，上海 200241；2. 国家信息中心信息化和产业发展部，北京 100045；3. 国防科技大学计算机学院，长沙 410073；4. 国家自然科学基金委员会信息科学部，北京 100085)

[摘　要] 本文介绍了“可信软件基础研究”重大研究计划的立项背景、总体科学目标、总体布局、实施思路及总体完成情况，并从建设可信软件开发资源共享与服务平台、设立“智能化软件可信的基础理论与方法”重大研究计划、对长期而艰难的课题实施面上项目滚动申报和资助方式等方面概述了在该领域下一步发展的建议。

[关键词] 重大研究计划；可信软件；综述

“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，“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和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。“可信软件基础研究”具有战略性、基础性和前瞻性。“可信软件”将成为软件技术发展和应用的必然结果。

1　项目实施情况

1.1　立项背景

随着现代信息技术创新及其广泛应用，软件作为信息技术的重要载体，已经日益渗透到政治、经济、军事、文化以及社会生活的各个领域和各个层面。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。

现代信息社会对于计算机系统的依赖，很大程度上体现为对软件的依赖。而计算机系统的缺陷很大一部分都是由于软件的问题而引发的。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、越来越脆弱，而且并不总是可以让人信任的，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，这类问题被称之为“软件可信性”问题。

国际上由于“软件可信性”问题所导致的重大灾难、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由于软件升级出现系统故障，导致了严重的股市停摆；2017 年 5 月 12 日，开始在全球蔓延的 WannaCry 勒索病毒席卷了至少 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。仅在 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巨大，据美国 NIST 估计，美国因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和应用的

收稿日期：2018-02-01；修回日期：2018-02-12

* 通信作者，Email：shanzg@sic.gov.cn

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、集成和持续演化变得越来越复杂，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，使得可信问题变得日益突出。互联网环境下计算实体的行为具有不可控性和不确定性，这种状况既对传统的软件开发方法和技术提出了重要的挑战，也对软件运行时刻的可信保障提出了严峻的要求[1]。

国家自然科学基金委员会（以下简称“基金委”）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，在 2007 年底启动了“可信软件基础研究”重大研究计划。该重大研究计划是基金委“十一五”期间启动的重大研究计划之一，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，具有非常重大的意义。

1.2 总体科学目标

“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方向，总体科学目标为[2,3]：

（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。

1.3 总体布局和实施思路

在“可信软件基础研究”重大研究计划的实施过程中，遵循“有限目标、稳定支持，集成升华、跨越发展”的总体思路，围绕“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”和“可信环境的构造与评估”4 个核心科学问题作为重点资助领域和方向进行项目部署。指导专家组对 4 个核心科学问题的难点和要点进行了深入分析和分解，确定优先研究的科学问题，选择的原则包括：优先支持针对核心科学问题具有创新思路的研究；优先支持基础较好、条件较为成熟，近期可望取得突破性进展的研究；优先选择对实现研究计划总体目标起决定作用的研究方向开展的跨学科集成研究[3]。

在“软件可信性度量与建模”方面，重点研究软件可信性度量、软件可信性演化与预测、可信软件的风险及过程管理等问题，积极探索以定量的方式建立可信性建模的系统方法论。在“可信软件的构造与验证”方面，重点研究可信软件的程序理论与方法学，软件的需求工程，可信软件设计、构造与编译，可信软件的验证与测试等问题，积极探索保证可演化的软件可信性满足需求的软件方法学。在“可信软件的演化与控制”方面，重点研究可信软件运行监控机理、软件可信性动态控制方法等问题，积极探索软件动态演化中的可信性相应控制方法。在“可信环境的构造与评估”方面，重点研究可信环境的数学理论与信任传递理论、可信计算环境构造机理及方法、可信计算环境测评等问题，积极探索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。

在对上述核心科学问题研究的基础上，该重大研究计划进一步开展可信软件开发与运行保障的集成与验证研究，主要包括“可信软件综合试验环境”、“高可信嵌入式软件系统试验验证环境”、“可信的网络应用软件系统试验验证环境”。

项目前期立项工作主要集中在前 3 年，根据申请项目的创新思想、研究价值以及对研究计划总体目标的贡献，采取“培育项目”、“重点支持项目”和“集成项目”的形式（体现在资助强度和实现目标上有所不同）予以资助。中期后的立项选择对实现研究计划总体目标有决定作用的研究方向，在前期“培育项目”和“重点支持项目”成果的基础上，重点开展集成创新研究，采取“集成项目”与“重点支持项目”相结合的形式，以较大支持强度予以资助。在整个研究计划的后 2 年重点进行项目和成果的集成升华。

为解决上述科学问题，在该计划的实施过程中按时间段设立阶段性目标，在不同阶段设立不同的工作重点。各阶段的工作重点内容如下：

第一阶段为 2008—2011 年，基本建立以可信性为核心的软件理论体系，具体目标包括：(1) 分别从环境、软件体系结构和程序缺陷等角度研究软件可信多维建模、度量评价和管理基础，建立柔性程序理论、软件可信性多维多尺度度量系统理论、可信环境的基础理论，以及统一框架下的软件可信性指标、演化规律与监控理论。(2) 提出算法的可信性度量与可信算法设计的数学基础，发展无误差计算、容错计算与误差可控计算设计理论，探索开放、动态、多变环境下新型计算模型与计算方法，建立并形成可信软件设计的基本原理。(3) 建立可信性需求驱动的软件构造、验证和测试理论，解决主要可信属性在软件需求和构造中失配与冲突的发现与消解问题。(4) 建立可信软件与演化的生命周期理论，以及可信软件与人-机关系理论。

第二阶段为 2008—2012 年，基本建立可信软件开发和运行保障的关键技术体系，具体目标包括：(1) 构建可信软件研究基本试验环境，提出可信软件的复杂性数据和工程数据的收集与分析技术体系，建立软件可信性在生命周期各环节的评估与预测方法。(2) 建立可信软件的过程建模与管理方法和技术，形成支持软件生命全周期的可信软件开发关键技术体系，包括需求工程、设计、语言与编译、验证、测试等技术，以及软件可信性的风险管理指标系统，支持可信性的获取、设计、编码和验证确认。(3) 建立可信软件运行监控与可信性主动保障技术体系，支持可信性动态演化的监测和控制机理以及可信性的主动保障等技术。(4) 建立可信计算环境的体系结构、可信虚拟机技术、可信的多方安全协作环境构造技术和可信计算环境的测评技术。

第三阶段为 2010—2013 年，完成面向嵌入式软件系统和网络应用软件系统的试验环境，集成可信软件工具环境并在试验环境进行示范，具体目标包括：(1) 以航空航天领域中嵌入式软件系统为目标，建立高可信软件综合试验环境，并开展典型应用，突破万行代码规模的高可信软件核心模块的构建与运行保障。(2) 以金融和政务领域中网络应用软件系统为目标，建立可信网络软件综合试验环境，并开展典型电子交易等应用，突破百万行代码规模可信网络应用软件及环境的构建与运行保障。

该重大计划实施 10 年过程中，形成了较为合理的布局，体现了指导专家组顶层设计的思想，反映了"充分发挥团体和群组的创新优势，实现理论和技术的研究成果与系统和应用实现的有机结合与集成，以重点领域应用需求为导向引领理论和技术研究，以理论和技术研究成果支撑综合试验平台的研制，以综合试验平台承载典型应用示范，实现理论、技术、平台、应用的一体化、闭环化、集成化、协同化"的实施思路。

该重大研究计划高度重视研究成果的综合集成工作，部署了"可信软件理论、方法集成与综合实验平台"集成项目作为关键切入点和重要落脚点，由南京大学牵头研究，整合重大研究计划内相关集成、重点支持和培育项目的优势研究队伍和前期研究成果，针对可信软件度量与建模、构造与验证、演化与控制等重大科学问题，以综合集成与创造提升为手段，从基础理论体系、方法与平台架构、典型应用示范等三方面对软件可信性进行了深入研究，取得了系统性与创新性研究成果，有效推动了技术方法的标准固化、学术团队的互动融合、研究成果的集成升华。

2　总体完成情况

该计划实施 10 年间，共资助研究项目 102 项，其中重点支持项目 24 项，集成项目 5 项，培育项目 73 项。参研人员共发表期刊论文 2 641 篇，包括权威国际期刊发表论文 1 046 篇，国内核心期刊发表论文 732 篇。申请国家发明专利 433 项，授权国家发明专利 236 项；申请国外发明专利 21 项，授权国外发明专利 9 项。获得国家级科技奖励 12 项，其中国家自然科学二等奖 1 项，国家科技进步一等奖 1 项、二等奖 5 项，国家技术发明二等奖 4 项，国家国际科技合作奖 1 项；获得省部级科技奖励 31 项，其中省部级自然科学一等奖 5 项、二等奖 4 项，省部级科技进步一等奖 14 项、二等奖 8 项。参研人员中 4 人当选中国科学院院士，2 人当选中国工程院院士；3 人获批教育部长江学者奖励计划教授，2 人获批教育部长江学者奖励计划青年学者；4 人入选国家千人计划，3 人入选国家青年千人计划；5 人获国家杰出青年科学基金资助，4 人获国家优秀青年科学基金资助。举办国际学术会议 120 次，国内学术会议 78 次；在国际学术会议做特邀报告 75 次，在全国性学术会议做特邀报告 57 次。

从总体上看，该重大研究计划针对"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”和“可信环境的构造与评估”四个方面的基本科学问题和关键技术开展了深入研究，达到了预定的科学目标，推动了我国可信软件从小到大、从散到整、由弱到强的跨越式发展，形成了完整可信软件体系，进入该研究领域国际先进行列。

2.1 基础理论研究实现跨越式发展

该重大研究计划以可信软件所涉及的新理论、新结构、新方法和新技术为突破口，实现了在科学理论和实验技术方面的源头创新，带动我国可信软件基础理论研究跨越发展。在“软件可信性度量与建模”方面，形成了软件过程和制品的可信性度量体系，实现了从分散的可信侧面度量向系统化度量跨越。构建了国内首个软件过程与制品可信证据的指标体系；提出了网络交易风险防控的用户行为认证技术，该技术成功应用于我国最大的金融交易平台[4]；设计了软件过程可信度量模型，成为国内首个软件可信度量的国家标准[5]。在“可信软件的构造与验证”方面，建立了标准化科学化的可信计算环境构造与评估体系，实现了从部分环节可信计算向全栈化可信计算跨越。提出了面向实际可信计算产品的测评方法，研制了可实现标准符合性、安全性和实现特性检测的测评工具和系统；首次提出了移动设备的实时可信流密码算法和基于格理论的认证密钥协商算法，发现了国际可信计算标准规范 TPM2.0 接口存在安全隐患，促进了标准的修改[6]；提出了基于图搜索的服务组合方法与基于嗅觉的服务组件声誉评价方法。在“可信软件的演化与控制”方面，提出了网络软件监控与演化的一体化设计体系，实现了从静态补丁式演化向动态模型驱动体系结构的跨越。构建了完整的“模型指导、行为监控、分析诊断、动态演化”的可信保证技术体系，支撑了关键领域大型分布式软件系统可信服务；在电子交易支付系统中采用了形式化建模、脆弱域分析、模型切片等技术，解决系统脆弱性辨识的难题[7,8]。在“可信环境的构造与评估”方面，建立了面向领域可实际应用的软件可信性构造与验证方法与工具环境，实现了从实验性工具向集成实用化平台跨越。面向航天与高铁领域，构建了嵌入式软件可信保障集成方法和工具环境，为解决嵌入式领域软件可信性问题提供了系统全面的解决方案[9]；面向网络税务与交易领域，构建了可信网络计算环境，突破了开放分布式系统可信机理与持续服务保障技术[10]。此外，还提出了可信软件理论与方法的元级化软件可信性综合集成理论框架 META-T，实现了从传统正确性向开放、动态、多变环境下的软件可信性跨越。对比国际上已有的同类型框架（例如美国科学院的 3E 框架），具有更强的系统性和可操作性；该元理论定义了包括驾驭原理、核控机理、加框机理、评判机理、演化机理在内的软件可信性的基本理论，应用在航天嵌入式系统、网络化税务与交易系统、列车控制系统等重要领域。

2.2 关键技术平台实现创新性突破

该重大研究计划提出了软件可信性的综合集成框架 META-T，从主体和客体两个方面，开展可信性分析和评估。从主体方面，依据期望的可信目标和可信投入，基于可信机理，通过“选点-加框-证据-判定-评估-演化”的过程，完成可信评估；从客体方面，基于应用场景分析，在客体模型上分析可信问题，决定采取的措施，根据获得的证据，实现软件演化过程中可信提升判定。META-T 集成框架在具体领域的应用，可以根据主体的可信需求、客体及其应用场景，采取形式化模式、经验化模式、工程化模式、混合式模式等多种实施方式，并从多维度建立层次关系，根据可信的分级需求、可投入的资源，为客体局部可信提升提供指导，同时建立各种可信提升所需资源的投入与稳定时段实施情况的评估度量。

该重大研究计划实现了以可信软件理论为基础的关键技术集成，为软件全生命周期工具集的设计奠定了技术基础。（1）提出了基于基准测试的代码级可信保障工具评价方法，构造了基准测试集数据库。（2）研制了一批自主的软件工具，包括静态分析类工具（例如航天 C 语言安全规则检查工具 SpecChecker、堆栈分析工具 StackAnalyser 等）、测试与验证类的工具（例如软件缺陷代码检测系统 DTS、模型驱动的软件测试与验证工具集 Jasmine 等）和基础框架类的工具（例如基于虚拟机构建可信执行环境的基础框架艾维网络计算平台）等等。（3）建立了基于虚拟机架构的可信云计算支撑环境，构建了面向虚拟机的分布式可信计算平台，实现平台内并发 VM 执行和数据的隔离性、可靠性和可信性，在受到干扰时能够提供可信、连续的服务。

2.3 重大示范应用有力支撑国家战略

该重大研究计划支持了一批国家关键领域的示范应用，取得了突出的应用成效，某些方面实现赶超，在部分领域的规模化应用和效益处于国际先进

水平，实现了可信软件技术从实验室向实际应用跨越。在航天领域，形成了《航天器型号软件验收评分标准》，支持了型号软件出厂专项评审从定性验收转向量化分级验收。首次建立了覆盖软件研制全周期、以可信要素为核心的航天嵌入式软件可信保障技术体系以及相应的可信保障集成环境，在嫦娥等重大工程软件的可信性保障中发挥了重要作用；在轨道交通领域，基于可信方法论和 Tsmart 平台工具集开展了技术攻关工作，基于 FPGA 设计了高级别 MVB 通信控制器芯片，形成了具备完全自主知识产权的 MVB 1 至 5 类能力通信控制器，替代了国外同类产品，打破了国外技术垄断，其中 MVB4 类设备已进入批量化生产阶段。构建了机车牵引与制动运行模型，开发了能够自适应满足重载货运机车节能操纵要求的实时控制系统，搭建了具有开环/闭环测试功能的半实物仿真实验平台和产品实验平台，形成了货运机车运行节能优化操纵系统产品样机，并已在实车运行 12 月以上；在金融领域，提出了风险防控的行为分析技术与认证机制，建立了我国首个互联网交易风险防控体系。在第三方支付、自由贸易、电子商务和银行等成功应用，服务 21 个国家和地区的 4 亿多支付宝实名用户。在性能方面，可信平台的交易直接放行率超过 96%；案件识别系统进行交易风险识别的平均响应时间为 65 ms。该研究运用到实践三年来为支付宝减少资产损失达 173.03 亿元，资金损失率仅为十万分之 0.9，比国际先进水平的资损率降低了 200 余倍；在电子税务领域，提出了"软件调用网络(CN)"概念和模型，以及基于 CN 的软件可信度量与行为监控方法，突破了以往只能基于电子税务软件程序代码级的可信性评估，实现了纳税人身份、纳税行为、系统能力等的可信性综合分析与量化计算方法，研制出"电子税务可信监控"、"CN 构建与软件合理性评测"等工具，应用于网络电子报税、个税管理等的软件开发、测试和维护。2012 年以来，成果应用的 3 大类电子税务系统累计超过 1 000 个版本，连续 4 年未发生大规模报税数据错误、税款入库失败等重大事故；在车联网服务领域，搭建了面向车联网的信息服务平台与大数据云服务平台，实现实车接入超过 70 000 辆，是世界上规模最大的实车实时数据处理平台系统之一。实验环境中车辆作为客户端，通过车载设备对车内 CAN 总线网络、车载设备的移动通信网络以及互联网的跨网络可信数据采集、数据传递和信息融合实现了"端-网-云"架构的车联网示范应用——交通部重点营运车辆监管系统，北京市、重庆市等地方交通管理机关实时交通业务系统，神州专车等新型交通运输企业移动网联网平台。

该重大研究计划的实施，不仅在可信软件基础研究的关键基础科学问题方面有所突破，还取得了以下几方面成绩：

(1) 可信软件基础研究实现跨越式发展，取得了一批在国际上有重要影响力的原创性科研成果。(2) 关键技术平台实现创新性突破，解决了我国重大应用中的关键技术难题，在国际可信软件技术研究上处于前沿位置。(3) 网络和嵌入式应用与产业相结合，重大示范应用有力支撑了国家战略。(4) 形成了一支以中青年人为主力的高水平研究队伍，培养了一批站在世界科学研究前沿的学科带头人。

在重大研究计划实施的过程中，指导专家组通过重大研究计划启动会、重点支持项目交流会、培育类项目交流会、重点支持项目申请交流会等形式，调动专家参与的积极性，切实加强对重大研究计划项目研究的学术指导。其中召集项目承担专家召开了 29 次重大研究计划交流会。

3　下一步工作的建议

总体而言，该重大研究计划充分发挥了基础研究为国家重大战略需求服务的引领作用，大幅提升了我国该领域基础研究水平；取得了一批国际领先或国际先进的科学研究成果，在国际可信软件基础研究领域拥有一席之地；凝聚和培养了一批从事基础研究的科研人员和团队，扩大了重大研究计划的影响。

我们特在此提出下一步工作的建议，具体如下：

(1) 建设可信软件开发资源共享与服务平台，巩固和辐射本重大研究计划的成果。各类软件数据和软件工具的汇集是开展、促进、评价可信软件研究的重要支撑。互联网、开源软件、软件开发社交网络、软件服务的发展，使得充分利用群体智慧，建立形成可信软件的开放数据、开放服务、合作开发成为可能。建议建设国家支持的可信软件开发资源共享与服务平台，提供海量软件资源的标注、分析、测试、评估等基础服务，积累可信软件资源、数据和知识，使之成为可信软件研究持续发展和成果展示的基础设施。

(2) 设立"智能化软件可信的基础理论与方法"重大研究计划，开拓可信软件与人工智能交叉的新领域。建议设立一个为期十年的"智能化软件可信的基础理论与方法"重大研究计划，吸收可信软件基

础研究的成功经验，面向智能软件与智能系统可信中的基础科学问题，在智能软件可信理论与度量评估、形式化方法与数据驱动方法的融合、可信软件工程与智能软件可信的交叉等基础理论上有突破，在人机物融合智能软件范型、构造技术、运行支撑和可信评估等关键技术上有跨越，满足我国工业 4.0 和机器人等国家创新对智能化软件可信不断增长的急迫需求。

（3）尝试面上项目滚动申报和资助方式，对长期而艰难的课题予以持续的支持。可信软件基础研究之中有一批长期艰难的基础研究课题。有的难题已经长达 40 余年，虽有进展，但仍未解决好。对于这样难度大的题目，在申报评审时往往落入“新意不够、进展不大”的一类，一些优秀的研究难免在竞争激烈的项目申报中只能处于中游的位置。然而，这些问题一旦突破，其成果的影响和辐射力强、理论意义与应用价值大。因而如何设计一种合理的持续性支持机制，保护相对“陈旧”、需要耐心的难题上的基础研究非常重要，建议尝试面上项目滚动申报和资助方式，希望对长期而艰难的基础研究予以持续支持。

参 考 文 献

[1] 刘克，单志广，王戟，等. “可信软件基础研究”重大研究计划综述. 中国科学基金，2008，22(3)：145—151.

[2] 国家自然科学基金委员会信息科学部. “可信软件基础研究”重大研究计划实施规划书(内部报告).

[3] 国家自然科学基金委员会信息科学部. “可信软件基础研究”重大研究计划总结报告(内部报告).

[4] Yu WY，Yan CG，Ding ZJ，et al. Modeling and Verification of Online Shopping Business Processes by Considering Malicious Behavior Patterns. IEEE Transactions on Automation Science & Engineering，2016，13(2)：647—662.

[5] Feng D，Qin Y，Feng W，et al. The theory and practice in the evolution of trusted computing. Chinese Science Bulletin，2014，59(32)：4173—4189.

[6] Shao J，Qin Y，Feng D，et al. Formal Analysis of Enhanced Authorization in the TPM 2.0// 2015：273—284.

[7] Wang Z，Geguang P U，Jiangwen L I，et al. A novel requirement analysis approach for periodic control systems. Frontiers of Computer Science，2013，7(2)：214—235.

[8] Liu T，Guan X，Qu Y，et al. A layered classification for malicious function identification and malware detection. Concurrency & Computation Practice & Experience，2012，24(11)：1169—1179.

[9] Lei Bu，Qixin Wang，Xin Chen，et al. Toward online hybrid systems model checking of cyber-physical systems' time-bounded short-run behavior. Acm Sigbed Review，2011，8(2)：7—10.

[10] Jiang C，Ding Z，Wang J，et al. Big data resource service platform for the internet financial industry. Chinese Science Bulletin，2014，59(35)：5051—5058.

Review of the achievements of major research plan on “Trustworthy Software”

He Jifeng[1] Shan Zhiguang[2] Wang Ji[3] Pu Geguang[1]

Fang Yufei[2] Liu Ke[4] Zhao Ruizhen[4] Zhang Zhaotian[4]

(1. *School of Computer Science and Software Engineering*, *East China Normal University*, *Shanghai* 200241;

2. *Department of Informatization and Industry Development*, *State Information Center*, *Beijing* 100045;

3. *School of Computer Science*, *National University of Defense Technology*, *Changsha* 410073;

4. *Department of Information Sciences*, *National Nature Science Foundation of China*, *Beijing* 100085)

Abstract In this paper, we introduce the background and scientific objectives, the research agenda and overall outcome of the NSFC major research plan on Trustworthy Software. Developing resource sharing and service platform for Trustworthy Software, setting up major research plan on the Basic Theory and Method of Intelligent Software Trustworthiness, giving continuing support for long-term and difficult research projects and other future plans for this field are also proposed.

Key words major research plan; trustworthy software; review