

2026 年度陕西省自然科学奖公示信息

项目名称		航天控制软件形式化规约智能推演与验证					
提名者		陕西省知识产权局					
提名意见							
我单位认真审阅了该项目提名书及附件材料，确认全部材料真实有效，并按照要求对该项目的基本情况进行了公示，公示期间无异议。 项目围绕航天控制软件形式化规约难定义、难获取和难验证的关键问题，建立了具有完全正则表达能力的形式化规约理论框架，提出了大语言模型赋能的自然语言需求与程序代码规约智能推演方法，构建了规约驱动的统一验证及分层分解验证方法，形成了贯通“规约定义—智能推演—规约验证”的航天控制软件可信保障理论、方法与工具体系。项目成果成功应用于我国探月工程三期月地高速再入返回飞行器等多款航天软件，为国家重大工程得顺利实施提供了有力的保障。团队获批省部级智能软件构造与质量保障学科技术中心，入选陕西省三秦英才特殊支持计划“创全国一流团队”及陕西省重点科技创新团队，对相关研究有引领和示范作用，对学科建设和经济社会发展有重要的指导作用。 根据《陕西省科学技术厅关于 2026 年度省科学技术奖提名工作的通知》，参照自然科学奖评定条件和评定标准，提名该项目参评陕西省科学技术一等奖。							
主要完成人情况							
排名	姓名	技术职称	工作单位	完成单位			
1	田聪	教授	西安电子科技大学	西安电子科技大学			
2	段振华	教授	西安电子科技大学	西安电子科技大学			
3	文成	讲师	西安电子科技大学	西安电子科技大学			
4	王文胜	讲师	西安电子科技大学	西安电子科技大学			
5	苏杰	助理研究员	西安电子科技大学	西安电子科技大学			
6	于斌	副教授	西安电子科技大学	西安电子科技大学			
主要完成单位							
排名	单位名称						
1	西安电子科技大学						
代表性论文（专著）目录							
序号	论文（专著）名称/刊名/作者	年卷页码（xx 年 xx 卷 xx 页）	发表（出版）时间（年月日）	通讯作者（含共同）	第一作者（含共同）	作者	论文署名单位

1	Temporal logic and temporal logic programming/ 科学出版社 / Zhenhua Duan	2005 年	2005 年 01 月 01 日	Zenhua Duan	Zenhua Duan	段振华	西安电子科技大学
2	A decision procedure for propositional projection temporal logic with infinite models/Acta Informatica/Zenhua Duan, Cong Tian, Li Zhang	2008 年 45(1) 卷 43-78 页	2008 年 02 月 01 日	Zenhua Duan	Zenhua Duan	段振华, 田聪	西安电子科技大学
3	Making Streett determinization tight/LICS 2020/Cong Tian, Wensheng Wang, Zenhua Duan	2020 年 859-872 页	2020 年 07 月 08 日	Cong Tian	Cong Tian	田聪, 王文胜, 段振华	西安电子科技大学
4	Enchanting Program Specification Synthesis by Large Language Models Using Static and Program Verification/CAV 2024/Cheng Wen, Jialun Cao, Jie Su, Zhiwu Xu, Shengchao Qin, Mengda He, Haokun Li, Shing-Chi Cheung, Cong Tian	2024 年 302-328 页	2024 年 07 月 24 日	Jialun Cao, Shengchao Qin	Cheng Wen	文成, 苏杰, 田聪	西安电子科技大学

5	A distributed network-based runtime verification of full regular temporal properties/IEEE Transactions on Parallel and Distributed Systems/Bin Yu, Cong Tian, Xu Lu, Nan Zhang, Zhenhua Duan	2023 年 34(1) 卷 76-91 页	2023 年 01 月 01 日	Cong Tian, Zhenhua Duan	Bin Yu	于斌, 田聪, 段振华	西安电子科技大学
6	Conditional interpolation: making concurrent program verification more effective/FSE 2021/Jie Su, Cong Tian, Zhenhua Duan	2021 年 144-154 页	2021 年 08 月 23 日	Cong Tian	Jie Su	苏杰, 田聪, 段振华	西安电子科技大学

客观评价

1) 英国 Kent 大学著名学者 Bowman 和 Thompson 教授、加拿大滑铁卢大学 King 和 Cameron 教授在论文 “Mexitl: Multimedia in Executable Interval Temporal Logic” 中对项目关于投影时序逻辑方面的贡献做了大段评论: 本项目在以下方面发展了 ITL: (1)提出了过去操作, (2)定义了新的投影操作符, (3)研究了框架技术, (4)引入了无穷模型, (5)实现了并发和通信原语 (… extends Moszkowski’ s interval temporal logic in a number of respects: (1) past operators are added, (2) a new projection operator is defined, (3) framing of variables is investigated, (4) infinite models are incorporated and (5) concurrency and communication primitives are considered.) (摘自期刊《Formal Methods in System Design》, Vol. 22(1): 5-38)。

2) 曾与美国国家工程院院士 Halpern 一起错误证明区间时序逻辑不可判定的 Moszkowski, 在论文 “Verification and Enforcement of Access Control Policies” 中指出: 项目提出了命题投影时序逻辑在无穷区间的判定过程 (注: 给出了判定算法, 即可判定。) (In [18] a decision procedure was presented for propositional projection temporal logic with infinite models.) (摘自期刊《Formal Methods in System Design》, Vol. 43(3): 450-492)。

3) 中国科学院院士何积丰和美国科学院院士 Vardi 等人在论文 “Fast LTL Satisfiability Checking by SAT Solvers” 中指出: 本项目提出了 PPTL 的范式和范式图, 其中 PPTL 是 LTL 的超集。他们给出了可用于 PPTL 模型检测和可满足性检测的判定过程 (… proposed a similar normal form and normal form graph for PPTL, which is considered as a superset of LTL[10]. Based on these two concepts, they presented a decision procedure for PPTL that can be used in both model checking and satisfiability checking.)。他们还应用本项目提出的范式和范式图概念, 给出了一个高效的 LTL 可满足性判定算法 (摘自 <http://arxiv.org/abs/1401.5677>)。

4) 布尔诺理工大学 Ondřej Lengál 教授等在论文 “Complementation of Emerson-Lei Automata” 中指出: 本项目给出了 Streett 自动机确定化复杂度的紧界 (Tight determinization of Streett automata was presented in [43].) (摘自 FoSSaCS 2025, 88-110)。

5) 南京大学卜磊教授等在论文 “SpecGen: Automated Generation of Formal Program Specifications via Large Language Models” 中指出: 本项目提出的 AutoSpec 是当前性能最优的大模型规约生成方

法之一（“best-performing LLM-based approach”）（摘自 CCF A 类会议 ICSE 2025, 16-28），并在论文“SpecEval: Evaluating Code Comprehension in Large Language Models via Program Specifications”中指出：他们将利用本项目提出的形式化规约合成方法来扩充数据集（We plan to employ existing specification generation techniques to enlarge the benchmark in the future.）（摘自 arXiv:2409.12866）。

6）上海交通大学李国强教授等在论文“Enhancing Automated Loop Invariant Generation for Complex Programs with Large Language Models”中指出：AutoSpec 是当前最先进的规约生成工具（“state-of-the-art tool AutoSpec”）（摘自期刊《Science of Computer Programming》，248: 103387）。

7）布达佩斯技术与经济大学 Imre Kocsis 副教授在论文“Practical runtime verification of crossorganizational smart contracts”中指出：本项目提出的并行化验证能够提高运行时验证的效率，而不会显著降低性能（Distributing the monitoring tasks across multiple processors or systems [83] enables the system to handle a higher volume of events and data without significant performance degradation, hence improving the efficiency of runtime verification.）（摘自 <https://doi.org/10.21203/rs.3.rs-4606405/v1>）。

8）美国波特兰州立大学 Xiaoyu Song 教授在论文“A Reduced State-Space Generation Method for Concurrent Systems Based on CPN-PR Model 中”指出：项目提出了一种基于优先级约束的动态偏序规约方法，能够减少冗余状态（In [9], the prioritized constraint-aided dynamic partial-order reduction approach is proposed to reduce the redundant state.）（摘自期刊《IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems》，Vol. 44(6): 2328-2342）。

项目简介

航天控制软件承担姿态控制、轨道控制、模式切换、故障处置和任务管理等关键功能，具有状态耦合紧密、时序约束严格等特点，微小的软件缺陷都可能导致机毁人亡的严重后果。基于形式化规约的软件验证是保障航天控制软件可信性的重要手段，但随着航天任务自主化和复杂化，涉及的软件规模持续提升，导致复杂行为难以完整表达、形式化规约获取困难、验证效率低下等瓶颈越来越制约其工程化应用。在此背景下，西安电子科技大学在国家自然科学基金重点项目、国家重点基础研究发展计划、国家自然科学基金优秀青年基金等项目的资助下，历经多年的研究和实践，建立了“形式化规约定义—规约智能推演生成—规约驱动验证”的航天控制软件可信保障理论与方法体系，具体包括：

1、建立了具有完全正则表达能力的航天控制软件形式化规约理论框架。针对多阶段模式转换、长期状态依赖、嵌套控制约束和跨周期交互行为难以利用传统时序逻辑完整描述的问题，证明了命题投影时序逻辑具备表达完全正则语言的能力，并通过给出命题投影时序逻辑的判定算法，解决了命题投影（区间）时序逻辑的判定难题，纠正了美国国家工程院院士 Halpern 等 1983 年关于命题区间时序逻辑不可判定的错误结论，为完全正则形式化规约在程序验证中的应用奠定了理论基础。作为完全正则性质验证的基础，无穷字自动机的确定化复杂性问题是国际公认难题，通过设计 Streett 自动机确定化的最优数据结构，该结构亦可有效约简 Emerson-Lei 自动机的确定化复杂性，突破了完全正则性质验证效率提升的关键理论瓶颈，为复杂航天控制软件形式化规约描述与验证提供了基础理论支撑。

2、提出了大语言模型赋能的航天控制软件形式化规约智能推演方法。针对需求文本中隐含逻辑、时序关系和嵌套依赖难以识别的问题，提出了层次化语义分解规约生成方法，构建中间表示语言，结合大语言模型语义分解与规则化转换，将需求中的隐含逻辑、嵌套约束和时序关系逐步转化为具有完全正则表达能力的形式化规约；针对程序性质隐含于函数调用、循环结构和数据依赖中的问题，提出了程序结构引导与验证反馈驱动的规约推演框架，通过静态分析构建扩展调用图，利用大模型分层生成前置条件、后置条件和循环不变式等候选规约，并经形式化验证工具迭代校验与修正，实现了复杂程序多类型规约的自动生成。该智能推演方法在航天控制软件真实场景中达成 88.4%语义准确率与 100%语法正确率，显著优于现有工具，并在太阳搜索系统等 16 个关键软件构件上完成批量规约推演，结果经领域专家审查确认，有效突破了性质获取难、规约构造慢的工程化应用瓶颈。

3、建立了规约驱动的航天控制软件统一验证体系。基于投影时序逻辑的可执行子集，提出集系统建模、程序执行与规约验证于一体的可执行逻辑语言，实现程序模型、系统行为模型与形式化规约在同一逻辑框架下的统一描述与验证，突破传统验证方法中“软件模型难提取、规约难关联、验证难扩展”的限制。基于本项目提出的完全正则形式化规约理论以及规约智能推演方法，构建了统一执行、动静结合、并行优化的形式化规约验证方法。针对规约推演验证过程中执行路径和状态空间快速增长问题，提出条件插值与动态偏序约简新方法，有效降低时空开销。针对航天控制软件规模大、层次复杂等问题，进一步提出分层分解验证方法，将系统验证分解为系统规约、组件行为和代码实现三个层次，逐层验证并保持层间规约关联。相关方法已在太阳搜索控制系统等多个航天关键构件和型号控制分系统中成功应用，为形式规约由局部程序推演拓展至系统级航天控制软件验证提供了方法支撑。相关方法已用于十余个航天嵌入式基础功能构件的安全性和功能正确性验证，对百余条功能性质开展形式模型与代码实现的一致性检查，并在太阳搜索控制系统中完成系统规约、组件行为和代码实现的逐层验证。

项目相关成果发表于 LICS、CAV、FSE、TPDS、Acta Informatica 等计算机科学和软件工程领域国际顶级期刊/会议，并由科学出版社出版专题学术专著 1 部，得到了国内外同行的积极评价，项目主要成果编入中国计算机科学技术发展报告。研究工作同步带动了高层次人才梯队与省部级学科平台建设，项目第一完成人获国家优秀青年科学基金资助及中创软件人才奖；团队获批组建省部级智能软件构造与质量保障学科技术中心，入选陕西省三秦英才特殊支持计划“创全国一流团队”及陕西省重点科技创新团队，全面建成了在以航天控制软件为代表的安全攸关软件可信验证方向国内引领、具备国际学术影响力的特色研究高地。

项目平台已集成于航天五院嵌入式软件可信集成环境，对“嫦娥五号”等飞行器中的 GNC 系统（制导导航与控制系统）开展验证，保障了位置确定、姿态控制、起飞参数计算等关键核心模块的可靠性和正确性，为飞行任务的圆满成功提供了有力保障，并在北京轩宇信息技术有限公司所承担的嫦娥五号试验器等多个型号嵌入式软件的第三方测试中进行应用，能够对多种安全性质进行形式化验证，检查出软件系统中时序冲突、数组越界及空指针等多个缺陷，提高了系统的正确性和可靠性，降低了软件失效的风险，对保障型号软件的质量做出了贡献；应用于“嫦娥六号”探测器等近 10 个型号控制分系统应用软件研制过程中，针对多种关键的形式化规约开展了正确性验证工作，保障了航天嵌入式控制软件的安全运行，有效降低了安全攸关软件系统的失效风险，并在中国航天科技集团空间飞行器软件检测站所承担的“嫦娥六号”移动相机任务的嵌入式智能软件的第三方测试中开展了应用，测试了“移动相机”自主移动、路径规划等阶段的多个智能模型和算法的正确性和可靠性，保障了嵌入式智能软件的安全运行，在国家航天重大工程中做出了突出贡献，支持了我国航空、航天关键领域的可信软件生产。另外还应用于中国航天科工集团第二研究院七〇六所承担的某航天型号武器装备软件中某指挥控制系统的开发中，通过建模和模型转换工具建立系统的完整 UML 模型，通过测试和验证工具可保证模型完整性、一致性以及代码的正确性、可靠性，满足用户需求。

完成人合作关系说明

主要完成人田聪、于斌在段振华教授的指导下完成了博士论文，王文胜、苏杰在田聪教授的指导下完成了博士论文，现均为省部级智能软件构造与质量保障学科技术中心、陕西省三秦英才特殊支持计划“创全国一流”团队、陕西省安全攸关智能软件重点科技创新团队，以及西安市软件可信认证关键技术重点实验室成员。长期共同致力于安全攸关软件系统的可信理论研究，提出了航天控制软件形式化规约智能推演与验证理论和方法。主要完成人文成作为省部级智能软件构造与质量保障学科技术中心，以及陕西省三秦英才特殊支持计划“创全国一流”团队成员，提出了大语言模型赋能的航天控制软件形式化规约智能推演方法，有效突破了性质获取难、规约构造慢的瓶颈，与其他主要完成人合作发表了论文。