项目名称	实时和嵌入式系统形式设计理论
候选单位	中国科学院软件研究所
候选人	詹乃军（第一），周巢尘（第二），
项目简介	**研究目的**：复杂实时和嵌入式系统广泛应用于国民经济发展和国防建设的众多重要领域，如轨道交通、航空航天、核电、军工等。在这些领域，系统安全是至关重要的，如果发生失效将会给生命、自然环境、国家安全、社会经济等带来重大灾难性后果，因此也被称为安全攸关系统。如何设计安全、可靠的实时和嵌入式系统是计算机科学和控制理论面临的巨大挑战。本研究针对该问题，基于严格数学理论（即形式化方法），提出实时和嵌入式系统形式设计理论，并应用于实践。 **主要科学发现点：** 1. 创立时段演算理论：时段演算基于区间逻辑，以实数作为时间模型，用时间域上的布尔函数模拟系统的实时状态。称状态在时间区间上的积分为该状态在该区间上占有的时段，并以状态时段的特性刻画实时系统的全局行为。时段演算包括表述和推导状态时段特性的语言和规则。由于状态可看作实函数所满足特性的特征函数，区间逻辑又适用于分段描述系统结构，故时段演算也可用来探索实时混成系统的形式设计。时段演算是由周巢尘和 C.A.R. Hoare 及 A.P. Ravn 在 1991 年创立，已是国际学术界公认的探索实时系统形式设计的一种主流方法，对实时系统形式方法的发展产生了重要影响。 2. 建立一套嵌入式系统形式设计理论，解决了嵌入式系统验证中的若干难题：i)针对复杂嵌入式系统缺乏具有较强表达能力的规范逻辑问题，首次将经典 Hoare 逻辑扩充到混成系统，建立混成 Hoare 逻辑（HHL），并开发其定理证明器；ii)以混成 CSP 作为形式建模基础，深入研究各种形式语义模型；iii)建立了基于 HHL 的嵌入式系统验证技术，解决若干验证难题；iv) 将该形式设计理论应用于形式化工业界广泛使用的图形建模语言 Simulink/Stateflow。定义了 Simulink/Stateflow 迄今最为完整的形式语义，实现了 Simulink/Stateflow 图形模型到混成 CSP 形式模型的自动转换，从而可以使用 HHL 及相关验证技术对 Simulink/Stateflow 进行形式验证。这项工作获得了国际同行高度评价，推广和发展。 **在国家重大战略需求中的实际应用：**上述理论成果已应用于国家重大战略，例如：高速铁路控制系统（CTCS-3），航天器控制软件设计（如嫦娥-3 软着陆控制软件），等等。

四、代表性论文、著作发表情况及第三方评价

4.1 代表性论文、著作发表情况（限 10 篇）					检索机构	中国科学院软件研究所						
序号	论文(著作)名称	刊名/出版社	影响因子	发表时间(年月日)	通讯作者	第一作者	论文全部作者	SCI他引次数	EI他引次数	他引总次数	年卷期页码	是否国内完成
1	Duration Calculus: A Formal Approach to Real-Time Systems	Springer-Verlag		2004-01-01	周巢尘	周巢尘	周巢尘，Michael Hansen	14		34	0	是
2	A calculus of durations	Information Processing Letters		1991-12-13	周巢尘	周巢尘	周巢尘，Tony Hoare，Anders Ravn	190		312	40(5),269-276	否
3	A higher-order duration calculus	Millenial Perspectives in Computer Science Proceedings of the 1999 Oxford-Microsoft Symposium		1999-01-01	周巢尘	周巢尘	周巢尘，Dimitar Guelev，詹乃军	1		1	0	是
4	Duration Calculus: Logical Foundations	Formal Aspects of Computing		1997-05-01	Michael Hansen	Michael Hansen	Michael Hansen，周巢尘	42		62	9(3),283-330	否
5	Formal Verification of Simulink/Stateflow Diagrams: A Deductive Approach	Springer-Verlag		2016-11-08	詹乃军	詹乃军	詹乃军，王淑灵，赵恒军	0		0	0	是
6	A calculus for hybrid CSP	Programming Languages and Systems/Springer		2010-12-01	詹乃军	刘江	刘江，吕继东，权墨，詹乃	50		98	LNCS 6461,1-15	是

		-Verlag					军，赵恒军，周巢尘，邹亮					
7	Computing semi-algebraic invariants for polynomial dynamical systems	EMSOFT ‘11 Proceedings of the ninth ACM international conference on Embedded software/ACM Press		2011-09-16	赵恒军	刘江	刘江，詹乃军，赵恒军	3		6	97-106	是
8	Verifying Simulink diagrams via a Hybrid Hoare Logic prover	Embedded Software (EMSOFT)/IEEE		2013-10-04	詹乃军	邹亮	邹亮，詹乃军，王淑灵，MArtin Fraenzel，秦胜潮	0		6	1-10	是
9	Verifying Chinese train control system under a combined scenario by theorem proving	Springer-Verlag		2014-01-01	詹乃军	邹亮	邹亮，吕继东，王淑灵，詹乃军，唐涛，袁磊，刘雨	1		9	LNCS 8164, p.262-280	是
10	Formal verification of a descent guidance control program of a lunar lander	Formal Methods. FM 2014/Springer-Verlag		2014-05-16	詹乃军	赵恒军	赵恒军，杨孟飞，詹乃军，顾斌，邹亮，陈尧	0		3	LNCS 8442, p.733-748	是

四、代表性论文、著作发表情况及第三方评价

4.2 代表性论文、著作被他人引用情况（限 10 篇）

序号	被引代表性论文、著作序号	引文名称/引文作者	刊名/影响因子（引文）	引文发表时间（年 月 日）
1	1	Temporal logic / Ian Hodkinson and Mark Reynolds	Handbook of Modal Logic	2007-05-01
2	2	A Road Map of Interval Temporal Logics and Duration Calculi / Valentin Goranko, Angelo Montanari, Guido Sciavicco	Journal of Applied Non-Classical Logics14(1-2): 9-54 (2004)	2004-02-01
3	2	From Duration Calculus To Linear Hybrid Automata / Ahmed Bouajjani, Yassine Lakhnech, Riadh Robbana	CAV 1995: 196-210	1995-03-01
4	4	Metric propositional neighborhood logics on natural numbers/Davide Bresolin, Dario Della Monica, Valentin Goranko, Angelo Montanari, Guido Sciavicco	Software and System Modeling 12(2): 245-264 (2011)	2011-02-26
5	6	Towards Verification of Cyber-Physical Systems with UTP and Isabelle/HOL / Simon Foster and Jim Woodcock	Concurrency, Security, and Puzzles 2017: 39-64	2016-12-18
6	7	A Method for Invariant Generation for Polynomial Continuous Systems/Andrew Sogokon1, Khalil Ghorbal, Paul B. Jackson and Andre Platzer	VMCAI 2016: 268-288	2015-12-25
7	7	Direct Formal Verification of Liveness Properties in Continuous and Hybrid Dynamical Systems / Andrew Sogokon and Paul B. Jackson	FM 2015: 514-531	2015-06-24
8	8	C2E2: a verification tool for stateflow models / Parasara Sridhar Duggirala1, Sayan Mitra, Mahesh Viswanathan1 and Matthew Potok	TACAS 2015: 68-82	2015-04-18
9	9	Decoupling Abstractions of Non-linear Ordinary differential equations / Andrew Sogokon1, Khalil Ghorbal and Taylor T. Johnson	FM 2016: 628-644	2016-11-08
10	10	Combining Mechanized Proofs and Model-Based Testing in the Formal Analysis of a Hypervisor/ Hanno Becker, Juan Manuel Crespo, Jacek Galowicz, Ulrich Hensel, Yoichi Hirai, Cesar Kunz, Keiko Nakata, Jorge Luis Sacchini, Hendrik Tews and Thomas Tuerk	FM 2016: 69-84	2016-11-08

四、代表性论文、著作发表情况及第三方评价

4.3 其他第三方评价证明目录（结题验收证明、检测报告等，限 10 个）					
序号	评价证明形式	项目名称	第三方单位（人）	评价时间	评价结论（意见）摘要（限 30 字）
1	结题验收证明	航天嵌入式软件设计一致性验证技术及其应用	国家自然科学基金委员会	2017-03-23	
2	结题验收证明	航天嵌入式软件可信保障集成环境和示范验证与应用	国家自然科学基金委员会	2016-03-24	评为优秀。
3	结题验收证明	实代数符号计算方法在形式方法中的应用	国家自然科学基金委员会	2009-04-30	

五、其他证明内容

1. 嫦娥-3-应用证明

2. 周巢尘、詹乃军国际会议邀请报告或专题报告证明

3. 一些引用文献