软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(2):179−180 [doi: 10.13328/j.cnki.jos.004789]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

安全攸关软件系统建模与验证专题前言*

李宣东[1], 刘 超[2], 毛晓光[3]

[1](计算机软件新技术国家重点实验室(南京大学),江苏 南京 210023)

[2](北京航空航天大学 计算机学院,北京 100191)

[3](国防科学技术大学 计算机学院,湖南 长沙 410073)

通讯作者: 李宣东, E-mail: lxd@nju.edu.cn

中文引用格式: 李宣东,刘超,毛晓光.安全攸关软件系统建模与验证专题前言.软件学报,2015,26(2):179−180. http://www.jos.org.cn/1000-9825/4789.htm

随着计算机技术应用的日益普及和不断深入,软件系统的规模和复杂性急剧增大,软件在越来越多的系统中成为主要的使能部件.在航空航天、武器装备、医疗设备、交通、核能、金融等安全攸关的应用领域,软件系统失效将导致灾难性的后果,保障软件系统的质量成为迫切的需求和挑战.建模、分析与验证是保障软件系统质量的重要环节和手段.本专题收录的14篇论文反映了近年来我国学者在安全攸关软件系统建模与验证领域的部分研究成果.

《基于形式化方法的航空电子系统检测》基于形式化方法研究面向航空电子系统的检测方法,建立了航空电子系统的形式化模型,并在此基础上提出了从静态和动态两方面对航空电子系统进行检测的途径.

《基于时间抽象状态机的 AADL 模型验证》提出了一种基于时间抽象状态机的 AADL 形式转换语义,并在此基础上给出了一种 AADL 模型的验证方法.

《基于时间 STM 的软件形式化建模与验证方法》针对实时嵌入式软件提出一种基于状态迁移矩阵(STM)的形式化建模方法,通过为 STM 各单元格增加时间语义和约束,使其适用于软件行为的时间性质刻画,并给出了相应的有界模型检验方法.

《设备驱动程序可靠性和正确性保障方法与技术研究进展》是一篇综述性论文,以设备驱动程序可靠性和正确性保障为目标,较为全面地分析和讨论了设备驱动程序的故障隔离与恢复,正确性分析和验证,设计建模与复杂性控制这 3 个方面的方法和技术.

《基于数据链的软件故障定位方法》从数据流角度研究相关的数据流故障模型、数据链模型以及相应的故障定位方法,提出了一种综合考虑变量操作状态变化以及变量操作状态间依赖关系的数据链模型.利用该模型对程序中数据流故障进行定位.

《一种面向列车控制系统中安全攸关场景的测试用例自动生成方法》围绕列车控制系统的安全攸关场景建模以及测试用例自动生成方法展开研究,对 UML 活动图扩充了事件驱动机制和时间特性描述机制,以满足对安全攸关场景建模的需要,提出了简单路径覆盖准则以定义对场景中系统行为的覆盖,并基于这一覆盖准则给出了自动生成测试用例的方法.

《多处理器实时系统可调度分析的 UPPAAL 模型》提出了一个用于多处理器实时系统可调度分析的模板,将与系统可调度性相关的部分,包括实时任务、运行平台和调度管理模块都用时间自动机建模,并使用模型检验工具 UPPAAL 验证可调度的性质是否被满足.

《多分支单变量循环程序的终止性分析》研究一类简单确定程序终止性分析问题,即单变量确定循环程序

* 收稿时间: 2014-12-22

的终止性问题,将该问题归结为由赋值函数构成的方程是否有不动点问题.

《面向安全攸关系统中小概率事件的统计模型检测》提出了一种面向安全攸关系统中小概率事件的统计模型检测框架,基于机器学习途径实现在相对少的样本数量下预测、评估小概率事件发生的概率.

《面向航天嵌入式软件的形式化建模方法》提出了一种面向航天嵌入式软件的形式化建模语言 SPARDL,并研究了从 SPARDL 模型自动生成对应 C 程序代码并进行快速仿真的方法.

《同步数据流语言高阶运算消去的可信翻译》针对构建从 Lustre*到 Clight 的可信编译器需求,研究了其中的高阶运算消去翻译算法,并证明了该翻译算法的正确性.

《一种基于特征矩阵的软件脆弱性代码克隆检测方法》提出了一种基于特征矩阵的软件代码克隆检测方法,在此基础上对软件的脆弱性进行源代码静态检测.

《一个机器检测的 Micro-Dalvik 虚拟机模型》针对 android 的 Dalvik 虚拟机,建立了可以通过定理证明助手 Isabel/HOL 验证的虚拟机模型,并证明了语义满足的性质.

《信息物理融合系统控制软件的统计模型检验》基于时间自动机,以模块化的方式描述实时多任务系统中的主要成分,包括实时操作系统、周期性任务、偶发任务、共享资源以及物理环境,提出了一种利用统计模型检验技术分析多任务系统功能正确性的方法.

本专题主要面向软件工程、嵌入式系统、实时系统、信息物理融合系统及其相关领域的研究人员和专业软件工程师.审稿过程历经 5 个月,有 20 余名相关领域的专家和学者参与审稿工作.审稿过程中还选择了部分投稿论文在全国软件与应用学术会议(NASAC 2014,桂林)上交流.经过初审、复审和终审等多道严格程序,最终确定收录以上 14 篇论文.在此,我们感谢踊跃投稿的相关领域学者,感谢辛勤工作的审稿专家和《软件学报》编辑部.

李宣东(1963－),男,湖南邵东人,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为软件工程,重点包括软件建模与分析,软件测试与验证.

刘超(1962－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为软件工程,重点包括软件测试,软件建模与分析,软件质量保证,软件过程改进.

毛晓光(1970－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为软件工程,重点包括软件错误定位与修复,软件测试与分析,软件可靠性.