International Journal of Software and Informatics, ISSN 1673-7288
http://www.ijsi.org, ijsi@iscas.ac.cn, +86-10-62661048
IJSI, 2024, 14(4): 349–351, doi: 10.21655/ijsi.1673-7288.00336

International Journal of Software and Informatics

Preface

Preface to the Special Issue on Formal Methods and Applications

Qinxiang Cao (曹钦翔)[1], Fu Song (宋富)[2], Naijun Zhan (詹乃军)[2]

[1] (School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

[2] (Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

Corresponding author: Qinxiang Cao, caoqinxiang@sjtu.edu.cn; Fu Song, songfu@ios.ac.cn; Naijun Zhan, znj@ios.ac.cn

Citation Cao QX, Song F, Zhan NJ. Preface to the special issue on formal methods and applications, *International Journal of Software and Informatics*, 2024, 14(4): 349–351. http://www.ijsi.org/1673-7288/336.htm

With the increasingly fast computing speed and complex architecture of hardware, software functions are also becoming increasingly powerful and complex. Accordingly, developing reliable software systems has become a huge challenge. Formal methods are techniques that use mathematical theories and methods to demonstrate and test the reliability and security of software systems, including model testing and theorem proving. Their mathematical foundation is based on formal logics such as formal languages, semantics, and reasoning proofs. At present, formal methods have been widely applied in various stages of the computing system lifecycle to varying degrees and in different ways. They play an increasingly important role in improving system reliability and security.

In recent years, Chinese scholars have attained new research achievements in formal methods and applications, and thus we publish a special issue on formal methods and applications; we also launched a symposium on formal methods and applications at the ChinaSoft2023 Conference to explore and exchange new achievements attained by Chinese scholars in the last year. This special issue called for articles publicly and received a total of 44 manuscripts. More than 30 experts were invited to review these manuscripts in two rounds, with 2–3 experts reviewing each paper. Among these manuscripts, 21 have entered the second round of review, and 15 of the reviewed papers have been invited to give presentations at the symposium on formal methods and applications of the ChinaSoft2023 Conference, answering questions from scholars in a face-to-face manner. Finally, 14 articles were selected to be published by this special issue, including reviews of research frontiers, cutting-edge achievements in model testing, theorem proving, and automata, and application of formal methods in critical security fields.

Five out of these 14 articles are selected for bilingual publication, encompassing the latest research results in the following two aspects.

(1) Formal verification and analysis of critical systems. As software and hardware scales are expanding, the demand for formal methods in critical systems is growing. For example, as the scale of real-time embedded systems keeps increasing, more and more systems are transitioning from being single-core to multi-core, and the software that needs to be verified is changing

Received 2024-03-25; Accepted 2024-03-26; IJSI published online 2024-12-31

from single-threaded programs to concurrent programs. With the progress in the research on formal methods, researchers and developers have attached importance to the verification of more complex program properties. Particularly, in the verification of important system software such as operating system kernels and compilers, the functional correctness needs to be verified in addition to memory security and other properties of the system software. The articles published by this special issue introduce the latest research achievements attained by Chinese scholars in this field, encompassing the achievements of automated verification based on theoretical probability models such as Petri nets and the research progress in interactive verification based on interactive theorem proving.

(2) Formal methods and theories. Different systems and verification problems involve special theories, and the application of formal methods needs formal modeling of these theories or targeted formal verification and analysis strategies. For example, in the verification of a concurrent program, an important question is how to verify or correct linearization. The articles published by this special issue introduce some new achievements of Chinese scholars in this field, especially in the research associated with concurrent objects and algorithm validation.

Here are the summaries of the five articles published by this special issue.

The article "*Analysis of Real-time Embedded Multi-core Systems Based on Prioritized Time Petri Nets*" proposes the prioritized time Petri nets and a task dependency graph with resource allocation and priority to improve the performance of point-interval prioritized time Petri nets in analyzing real-time embedded multi-core systems.

The article "*Strong Linearizability Checking and Determination for Concurrent Objects*" investigates strong linearizability from two aspects: verification algorithm and approach for proving non-strong linearizability of concurrent objects. On the one hand, two verification algorithms for strong linearizability are proposed, and on the other hand, an approach is provided for proving that the concurrent objects violate strong linearizability.

The article "*Formal Verification of Functional Correctness for Mutexes in Microkernel*" conducts formal verification on the code of the mutex module of a preemptive microkernel in the interactive theorem prover Coq, gives the formal specifications of the interface functions of this module, and formally proves the functional correctness of these interface functions.

The article "*Program Derivation and Mechanized Verification of Imperative Dynamic Programming Algorithms*" proposes an imperative dynamic programming algorithm based on the functional modeling and verification of imperative dynamic programming algorithms Isabelle/HOL.

The article "*Safety Analysis for Mixed-criticality System with Random Errors and Burst Errors Based on AADL*" proposes new thread state machine semantics to describe the thread execution process with burst errors. In addition, it proposes model transformation rules and assembly methods to enable the derivation of PRISM models from AADL models, and on this basis, a set of methods for security analysis of random and burst errors is formed. Finally, a power boat autopilot system is adopted to verify the effectiveness of the proposed method.

We hope that this special issue can promote the research and application of formal methods.

Qinxiang Cao, Ph.D., associate professor at Shanghai Jiao Tong University, has received funding from the Shanghai Pujiang Program. He has long been engaged in program verification and program logic research based on theorem proving. His papers have been published in internationally renowned conferences or journals such as POPL, OOPSLA, and JAR. His representative work is the VST tools developed under his leadership. Additionally, he participates in the writing of the fifth volume of the well-known textbook Software Foundations on Coq theorem proving.

Fu Song, Ph.D., professor at the Institute of Software, Chinese Academy of Sciences, mainly engaged in the research on verification and testing of system and software security and related logic and automata theory. He has presided over and participated in a number of youth, general, and key projects of the National Natural Science Foundation of China. He is a member of the Shanghai Pujiang Program and the Shanghai Chenguang Scholar, and he won the Amazon Research Award in the autumn of 2021. His paper was selected as the 2023 excellent paper on cyberspace security of the Chinese Institute of Electronics. He has published more than 80 papers in internationallywell-known conferences or journals such as IEEE S&P, USENIX Security, NDSS, POPL, OOPSLA, CAV, ESEC/FSE, ICSE, ASE, ISSTA, FM, ACM TOSEM, IEEE TSE, IEEE TDSC, and I&C.

Naijun Zhan, Ph.D., professor at the Institute of Software, Chinese Academy of Sciences, distinguished fellow of the Chinese Academy of Sciences, professor at the University of Chinese Academy of Sciences, executive director of the State Key Laboratory of Computer Science, and winner of the National Science Fund for Distinguished Young Scholars. His main research fields include real-time, embedded, and hybrid system design theory and program theory. He serves as an editorial board member of Journal of Automated Reasoning, Formal Aspects of Computing, J. of Logical and Algebraic Methods in Programming, Research Direction: Cyber Physical Systems, Journal of Software, Journal of Computer Research and Development, Acta Electronica Sinica, and Science and Technology Foresight, a member of the steering committee for international conferences MEMOCODE and SETTA, co-chair of several international conference program committees (such as FM 2021), and a member of renowned international conference program committees (such as CAV, RTSS, HSCC, ICCPS, and EMSOFT). He has published over 100 papers in renowned international conferences and journals, 2 monographs, and 4 books.