Special Issue on Automated Verification of Critical Systems (AVoCS'12)

Gerald Lüttgen[a,1,*], Stephan Merz[b,1,*]

[a] *Software Technologies Research Group, Otto-Friedrich University of Bamberg, Germany*
[b] *Inria & LORIA, Nancy, France*

AVoCS is an annual international workshop of researchers and practitioners interested in tools and techniques for the verification of critical systems. Topics of interest cover all aspects of automated verification, including model checking, theorem proving, abstract interpretation, and refinement concepts suitable for various types of critical systems such as safety-critical, security-critical, business-critical and performance-critical systems. Contributions that describe integrations of different techniques or applications to industrial case studies are of particular interest. The 12th workshop took place in September 2012 at the Otto-Friedrich University of Bamberg, Germany. Its post-proceedings appeared in December 2012 as volume 53 of the *Electronic Communications of the EASST*.

The present issue of *Science of Computer Programming* results from an open call for contributions to all researchers in the field, including authors of papers accepted at AVoCS 2012, to submit mature articles on their research. As for similar issues in previous years, the objective has been to have a competitive process and thus select the best submissions for publication in this journal. Three of the six articles are based on work presented at the AVoCS workshop, and the other three are based on conference and workshop papers published elsewhere. All six submissions were subject to a stringent peer-reviewing process.

The articles included in this issue explore a broad range of facets on automatically verifying critical systems, both from a theoretical and a practical perspective.

- Marché describes a challenging case study on the formal verification of a C program in the presence of rounding errors on floating point numbers. The goal is to prove claims on the error drift, for which the program is annotated by clauses in the specification language ACSL. The Frama-C environment with the Jessie plugin is then employed to forward the claims either to automatic solvers based on real arithmetic and SMT techniques, or to the interactive proof assistant Coq.

- Tofan, Travkin, Schellhorn and Wehrheim evaluate two different proof techniques for verifying linearizability of concurrent data structures over a challenging case study. The first technique is based on assertional reasoning, while the second uses an interval temporal logic with rely-guarantee reasoning. Both techniques are supported by the KIV theorem

[*] Corresponding author
Email addresses: gerald.luettgen@swt-bamberg.de (Gerald Lüttgen), stephan.merz@loria.fr (Stephan Merz)
[1] Guest editor

prover, and interesting insights are gained concerning the underlying concepts as well as their mechanization.

- James, Moller, Nguyen, Roggenbach, Schneider and Treharne present a modelling methodology based on CSP||B for the safety analysis of interlocking railway systems, which has been developed in collaboration with railway engineers. They formally establish that it is sufficient to only consider two trains in a network when verifying safety properties. The novelty lies in the way how the length of a train is captured abstractly.

- Zhao and Rozier describe the formal modelling and specification of a coordination protocol for an automated air-traffic control system developed by NASA, employing symbolic model checking and satisfiability checking for model validation, specification debugging and system verification. In particular, two flaws were discovered that led system engineers to make significant design changes in order to meet safety standards.

- Mateescu and Wijs develop enhanced techniques for reducing state spaces when model checking systems against temporal properties expressed in the modal mu-calculus. They show how one may automatically determine the maximal set of actions that can be hidden in a labelled transition system without affecting a formula's truth value. In addition, their article identifies a fragment of the mu-calculus that characterizes divergence-sensitive branching bisimilarity, and employ it for reducing state spaces globally and on-the-fly.

- Talpin, Brandt, Gemünde, Schneider and Shukla propose a uniform, constructive and operational semantics for synchronous modules, in the style of Quartz, that are coordinated by multi-clocked polychronous data-flow networks, in the style of Signal. The semantics serves as a basis for reasoning about globally-asynchronous, locally-synchronous systems, and gives new insights on the relation between synchronous and asynchronous determinism, endochrony and synchronous and asynchronous constructiveness.

We are grateful to the SCP managing editor Jan Bergstra and the editorial assistant Bas van Vlijmen for the excellent collaboration in producing this special issue. In particular, we thank the many authors who responded to our call for contributions. The reviewers – a significant number of whom had already participated in the AVoCS'12 workshop as members of the programme committee – did a wonderful job in providing timely, in-depth reports, which have contributed notably to the quality of this issue.