OASIcs – OpenAccess Series in Informatics

OASIcs aims at a suitable publication venue to publish peer-reviewed collections of papers emerging from a scientific event. OASIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

Editorial Board

- Daniel Cremers, TU Munich, Germany
- Barbara Hammer, Uni Bielefeld, Germany
- Marc Langheinrich, University of Lugano, Switzerland
- Dorothea Wagner, KIT, Germany

ISSN 2190-6807

www.dagstuhl.de/oasics
Contents

Preface

   Jörg Brauer, Marco Roveri and Hendrik Tews ........................................ i

Structuring Interactive Correctness Proofs by Formalizing Coding Idioms

   Holger Gast ................................................................. 1

Verification of Dependable Software using SPARK and Isabelle

   Stefan Berghofer ............................................................ 15

Adaptable Value-Set Analysis for Low-Level Code

   Jörg Brauer, René Rydhof Hansen, Stefan Kowalewski, Kim G. Larsen, and
   Mads Chr. Olesen ........................................................... 32

Verification of Safety-Critical Systems: A Case Study Report on Using Modern
Model Checking Tools

   Antti Jääskeläinen, Mika Katara, Shmuel Katz, and Heikki Virtanen ............ 44

A Tool for the Certification of Sequential Function Chart based System Specifications

   Jan Olaf Blech ............................................................... 57

Automatic Derivation of Abstract Semantics From Instruction Set Descriptions

   Dominique Gückel and Stefan Kowalewski .......................................... 71
Industrial-strength software analysis and verification has advanced in recent years through the introduction of model checking, automated and interactive theorem proving, and static analysis techniques, as well as correctness by design, correctness by contract, and model-driven development. However, many techniques are working under restrictive assumptions that are invalidated by complex embedded systems software such as operating system kernels, low-level device drivers, or micro-controller code.

The aim of SSV workshop series is to bring together researchers and developers from both academia and industry who are facing real software and real problems with the goal of finding real, applicable solutions. It has always been the goal of SSV program committees to let “real problem” really mean real problem (in contrast to real academic problem).

The 6th SSV workshop was held on August 26 in Nijmegen in the Netherlands. The workshop was co-located with the second conference on Interactive Theorem Proving (ITP 2011), which took place from 22–25 August at the same place.

The program chairs and organization committee of SSV 2011 have been

Jörg Brauer, Verified Systems International GmbH, Germany
Marco Roveri, FBK-irst, Italy
Hendrik Tews, TU Dresden, Germany

The SSV program chairs gratefully acknowledge the sponsorship of National ICT Australia Ltd (NICTA), Australia’s Information and Communications Technology Research Centre of Excellence, and of the Ultra high speed mobile information and communication (UMIC) cluster of excellence at RWTH Aachen University in Germany.