

# 6th International Workshop on Systems Software Verification

SSV'11, August 26, 2011, Nijmegen, The Netherlands

Edited by

Jörg Brauer

Marco Roveri

Hendrik Tews



#### *Editors*

Jörg Brauer  
Verified Systems International GmbH  
Bremen  
brauer@verified.de

Marco Roveri  
Embedded Systems Unit  
Fondazione Bruno Kessler  
roveri@fbk.eu

Hendrik Tews  
Operating Systems Group  
TU Dresden  
tews@os.inf.tu-dresden.de

*ACM Classification 1998*  
D.2.4 Software/Program Verification

**ISBN 978-3-939897-36-1**

#### *Published online and open access by*

Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at <http://www.dagstuhl.de/dagpub/978-3-939897-36-1>.

#### *Publication date*

July 2012

#### *Bibliographic information published by the Deutsche Nationalbibliothek*

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>.

#### *License*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs (BY-NC-ND): <http://creativecommons.org/licenses/by-nc-nd/3.0/legalcode>



In brief, this license authorizes each and everybody to share (to copy, distribute and transmit) the work under the following conditions, without impairing or restricting the authors' moral rights:

- Attribution: The work must be attributed to its authors.
- No derivation: It is not allowed to alter or transform this work.
- Noncommercial: The work may not be used for commercial purposes.

The copyright is retained by the corresponding authors.

Digital Object Identifier: 10.4230/OASlcs.SSV.2011.i

**ISBN 978-3-939897-36-1**

**ISSN 2190-6807**

**<http://www.dagstuhl.de/oasics>**

## OASlcs – OpenAccess Series in Informatics

OASlcs aims at a suitable publication venue to publish peer-reviewed collections of papers emerging from a scientific event. OASlcs 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](http://www.dagstuhl.de/oasics)**



## ■ Contents

Preface	
<i>Jörg Brauer, Marco Roveri and Hendrik Tews</i> .....	i
Structuring Interactive Correctness Proofs by Formalizing Coding Idioms	
<i>Holger Gast</i> .....	1
Verification of Dependable Software using SPARK and Isabelle	
<i>Stefan Berghofer</i> .....	15
Adaptable Value-Set Analysis for Low-Level Code	
<i>Jörg Brauer, René Rydhof Hansen, Stefan Kowalewski, Kim G. Larsen, and     Mads Chr. Olesen</i> .....	32
Verification of Safety-Critical Systems: A Case Study Report on Using Modern Model Checking Tools	
<i>Antti Jääskeläinen, Mika Katara, Shmuel Katz, and Heikki Virtanen</i> .....	44
A Tool for the Certification of Sequential Function Chart based System Specifications	
<i>Jan Olaf Blech</i> .....	57
Automatic Derivation of Abstract Semantics From Instruction Set Descriptions	
<i>Dominique Gückel and Stefan Kowalewski</i> .....	71





## ■ Preface

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.

11th July 2012

Jörg Brauer, Marco Roveri and Hendrik Tews

