Proceedings of the 3rd Workshop on

Automated Verification of Critical Systems

AVoCS'03

Michael Leuschel, Stefan Gruner,
Stéphane Lo Presti
(editors)

Southampton, United Kingdom
2nd - 3rd April, 2003

Technical Report DSSE-TR-2003-2

University
of Southampton

Preface

This volume contains the proceedings of the Third Workshop on Automated Verification of Critical Systems (AVoCS'03) held at the Department of Electronics and Computer Science, University of Southampton on the 2nd-3rd April, 2003. The first meeting, AVoCS'01, was held in Oxford, continuing the tradition of the annual QinetiQ/OUCL series. The second meeting, AVoCS'02, was held in Birmingham.

The aim of AVoCS is to foster a research community in verification in Europe through encouraging communication among researchers. Specific objectives include efforts at the integration as well as the transfer of methods between different groups. The topics are to be interpreted broadly and inclusively, and in particular cover all aspects of verification (model checking, theorem proving, specification and refinement proofs, etc.) pertaining to various types of critical systems, be it safety-critical, business-critical, or performance-critical.

This technical report includes 24 contributed papers. The invited speakers are:

- **David LeBlanc** (Microsoft)
- **Doron Peled** (University of Warwick, U.K.)

We wish to thank the following for their contribution to the success of the workshop:

- Microsoft Research Labs, Cambridge;
- Formal Methods Europe (FME);
- Formal Systems (Europe), Limited;
- QinetiQ;
- The European Office of Aerospace Research & Development, Air Force Office of Scientific Research, United States Air Force Research Laboratory.

We would also like to thank the University of Southampton for providing many facilities; the members of the programme committee and the local organisers for their efforts; Adelle Chapman and Mike Shep, Southampton, for designing the new logo of the workshop; the invited speakers for giving a talk; and finally the authors of the contributed papers for making this workshop possible.

Michael Leuschel, Stefan Gruner, Stéphane Lo Presti March 2003

Local Organisers

Stefan Gruner, University of Southampton, U.K.
Michael Leuschel, University of Southampton, U.K.
Stéphane Lo Presti, University of Southampton, U.K.

Programme Committee

Sadie Creese, QinetiQ, U.K.
Marta Kwiatkowska, University of Birmingham, U.K.
Michael Leuschel (Chair), University of Southampton, U.K.
David Nowak, CNRS & ENS Cachan, France
Joy Reed, Armstrong Atlantic State University, USA
Mike Reed, Oxford University, U.K.
Bill Roscoe, Oxford University, U.K.
Ulrich Ultes-Nitsche, Université de Fribourg, Switzerland
Irfan Zakiuddin, QinetiQ, U.K.

Invited Speakers

David LeBlanc, Microsoft
Doron Peled, University of Warwick, U.K.

Workshop Contact Person

Michael Leuschel
DSSE, University of southampton
Highfield, SO17 1BJ, U.K.
e-mail: `mal@ecs.soton.ac.uk`

AVoCS Workshop WWW Sites:

AVoCS'03 `http://www.ecs.soton.ac.uk/~mal/avocs03/`
AVoCS'02 `http://www.cs.bham.ac.uk/~gxn/avocs/`
AVoCS'01 `http://web.comlab.ox.ac.uk/oucl/conferences/wavcs2001/`

Sponsors and Supporters:

Microsoft Research

AVoCS'03 Workshop Programme

Wednesday, April 2nd, 2003

- 10:00 - 11:00 **Invited Talk**
  Writing Secure Code
  David LeBlanc

- **11:00 - 11:30 Break**

- 11:30 - 12:00 *Automatic Structural Coverage Testing of Java Bytecode*
  J. Doyle and C. Meudec **1 -14**

- 12:00 - 12:20 *A probabilistic coverage for on-the-fly test generation algorithms*
  N. Goga **15 - 30**

- 12:20 - 12:40 *Model Checking Multi-Agent Programs with CASP*
  Rafael H. Bordini, Michael Fischer, Carmen Bardavilla, Willem Visser, and Michael Wooldridge **31 - 35**

- 12:40 - 13:00 *A Synchronous Bisimulation Based Approach for Information Flow Analysis*
  Siva Anantharaman and Gaétan Hains **36 - 49**

- **13:00 - 14:00 Lunch**

- 14:00 - 14:30 *CSP + Clocks: a Process Algebra for Timed Automata*
  Stefano Cattani and Marta Kwiatkowska **50 - 63**

- 14:30 - 14:50 *Projection onto State in the Duration Calculus: Relative Completeness*
  Dimitar P. Guelev and Dang Van Hung **64 - 73**

- 14:50 - 15:10 *CSP model-checking of liveness properties over eventual delivery networks*
  William Simmonds **74**

- 15:10 - 15:30 *A First Glimpse at Patterns of Data-Independent Induction*
  M. Goldsmith (and others) **75**

- **15:30 -16:00 Break**

- 16:00 - 16:30 *On the expressiveness of CSP refinement checking*
  Bill Roscoe **76 - 97**

- 16:30 - 16:50 *Automatic Verification of Real-Time Systems: A case study*
  Danièle Beauquier, Tristan Crolard, and Evguenia Prokofieva **98 - 108**

- 16:50 - 17:10 *Compositional CSL model checking for Boucherie product processes*
  P. Ballarini and J. Hillston **109 - 122**
- 17:10 - 17:30 *A Hoare Logic for Single-Input Single-Output Continuous-Time Control Systems*
  Richard J. Boulton, Ruth Hardy, and Ursula Martin **123 - 132**
- **17:30 - 18:00 Break**
- 18:00 - 19:00 **Model Checking Competition**
- **20:00 Conference Dinner**

Thursday, April 3rd, 2003

- 9:00 - 10:00 **Invited Talk**
  Model Checking, Testing and Verification Working Together
  Doron Peled
- **10:00 - 10:30 Break**
- 10:30 - 11:00 *Automated property verification in UML models*
  Ambrosio Toval, José Sáez, and Francisco Maestre **133 - 142**
- 11:00 - 11:20 *Robust models for generalized model checking (extended abstract)*
  Michael Huth **143 - 149**
- 11:20 - 11:40 *Model Checking Graph Grammars*
  Arend Rensink **150 - 160**
- 11:40 - 12:00 *A New encoding and Implementation of Not Necessarily Closed Convex Polyhedra*
  Roberto Bagnara, Patricia M. Hill, and Enea Zaffanella **161 - 176**
- **12:00 - 13:30 Lunch (and PC meeting)**
- 13:30 - 14:00 *Deductive Verification of Cache Coherence Protocols*
  Michael Fischer and Alexei Lisitsa **177 - 186**
- 14:00 - 14:20 *Modelling Ad hoc On-demand Distance Vector (AODV) Protocol with Timed Automata*
  Sibusisiwe Chiyangwa and Marta Kwiatkowska **187 - 196**
- 14:20 - 14:40 *Modelling Ad-hoc Routing Protocols using Game Search: Extended Abstract*
  Irfan Zakiuddin, Tim Hawkins, Nick Moffat, Sadie Creese, and Chris Leow **197 - 201**