

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Shmuel Ur Eyal Bin
Yaron Wolfsthal (Eds.)

Hardware and Software Verification and Testing

First International Haifa Verification Conference
Haifa, Israel, November 13-16, 2005
Revised Selected Papers



Springer

Volume Editors

Shmuel Ur

Eyal Bin

Yaron Wolfsthal

IBM Labs, Haifa University, Mount Carmel, Haifa 31905, Israel

E-mail: {ur,bin,wolfstal}@il.ibm.com

Library of Congress Control Number: 2006921186

CR Subject Classification (1998): D.2.4-5, D.2, D.3, F.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743

ISBN-10 3-540-32604-9 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-32604-5 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11678779 06/3142 5 4 3 2 1 0

Preface

The First Haifa Verification Conference was held at the IBM Haifa Research Lab and at the Haifa University in Israel from November 13 to 16, 2005. The conference incorporated three different workshops that took place separately in previous years. The IBM Verification Workshop is now its sixth year, the IBM Software Testing Workshop is now in its fourth year, and the PADTAD Workshop on testing and debugging multi-threaded and parallel software was held for the third time. The Verification Conference was a three-day, single-track conference followed by a one-day tutorial on the testing and review of multi-threaded code.

The conference presented a unique combination of fields that brought together the hardware and software testing communities. Merging the different communities under a single roof gave the conference a distinctive flavor and provided the participants with added benefits. While the applications in these separate fields are different, the techniques used are often very similar. By offering lectures in these disparate but related disciplines, the conference engendered an environment of collaboration and discovery.

The conference emphasized applicability to real world challenges, which was very important to the many attendees coming from industry. A relatively large number of invited speakers presented topics of great interest to the audience. These outstanding speakers included Sharad Malik, Amir Pnueli, Cindy Eisner, Yoav Katz, Yoav Hollander, and Michael Rosenfield on hardware verification, Thomas Wolf, Scott Stoller, Dan Quinlan, Yael Dubinsky, Orit Hazzan, Bernd Finkbeiner, and Thomas Ball on software verification, and Scott Stoller and Dan Quinlan for the PADTAD track.

Thirty-one papers, from 11 countries, were submitted and thoroughly reviewed by the Program Committee and additional referees, with an average of 3.5 reviews per paper. Of the papers submitted, fourteen were accepted. The acceptance was based on the score received and in the case of an equal score, industry papers were given preference. Some of the invited speakers were also encouraged to submit papers. This volume is composed of the 14 papers accepted by the committee and three invited papers.

Attendance at the conference was very high, with more than 170 participants (225 registered) from 12 countries (Israel, USA, Germany, Switzerland, Brazil, Finland, India, Canada, Denmark, Bulgaria, Italy, Portugal). The facilities provided by the IBM Haifa Research Labs and the Caesarea Edmond Benjamin de Rothschild Foundation Institute for Interdisciplinary Applications of Computer Science (C.R.I.) were remarked upon very favorably by the attendees, as was the proficiency of the administrative assistants.

We would like to thank our sponsors, IBM and CRI, the Organizing Committee, and the Program Committee. Our appreciation goes out to the administrative assistants, especially Vered Aharon and Efrat Shalom-Hillman from IBM and Ornit Bar-Or from CRI, and to Yair Harry our web master. We would also like to thank all

the authors who contributed their work. Special thanks go to Yaniv Eytani, the Local Arrangement Chair, for his boundless energy in working with the invited speakers.

We hope this conference is the first of many and that these communities continue to work together and learn from each other. There is a lot of knowledge and insight that can be shared by the hardware verification and testing communities, and we hope this conference represents a step in this important direction.

November 2005

Shmuel Ur
Program Chair

Organization

The Haifa Verification Conference was organized by:

Program Chair

Shmuel Ur, IBM Haifa Labs, Israel (ur@il.ibm.com)

Verification Conference Organizing Committee

Shmuel Ur (ur@il.ibm.com)

Eyal Bin (bin@il.ibm.com)

Eitan Farchi (farchi@il.ibm.com)

Yaron Wolfsthal (wolfstal@il.ibm.com)

Avi Ziv (aziv@il.ibm.com)

Verification Track Chair

Avi Ziv, IBM Haifa Labs, Israel (aziv@il.ibm.com)

Software Testing Track Chair

Eitan Farchi, IBM Haifa Labs, Israel (farchi@il.ibm.com)

PADTAD Chair

Shmuel Ur, IBM Haifa Labs, Israel (ur@il.ibm.com)

Proceedings Chair

Tsvi Kuflik, University of Haifa, Israel (tsvikak@mis.hevra.haifa.ac.il)

Local Arrangements Chair

Yaniv Eytani, University of Haifa, Israel (ieytani@cs.haifa.ac.il)

Program Committee

Jose Nelson Amaral, University of Alberta, Canada (amaral@cs.ualberta.ca)

Yosi Ben-Asher, University of Haifa, Israel (yosi@cs.haifa.ac.il)

Valeria Bertachio, Department of Electrical Engineering and Computer Science, University of Michigan, USA (valeria@umich.edu)

Angelos Bilas, University of Toronto, Canada (bilas@eecs.toronto.edu)

Eyal Bin, IBM Haifa Labs, Israel (bin@il.ibm.com)

Roderick Bloem, Graz University of Technology, Austria

(Roderick.Bloem@ist.TUGraz.at)

Alessandro Cimatti, IRST - Istituto per la Ricerca Scientifica e Tecnologica, Italy (cimatti@itc.it)
 Giorgio Delzanno, Universita di Genova, Italy (giorgio@disi.unige.it)
 Jong-Deok Choi, IBM Research, USA (jdchoi@us.ibm.com)
 Jack Dongarra, University of Tennessee, USA (dongarra@cs.utk.edu)
 Orit Edelstein, IBM Haifa Labs, Israel (edelstein@il.ibm.com)
 Eitan Farchi, IBM Haifa Labs, Israel (farchi@il.ibm.com)
 Mike Feeley, University of British Columbia, Canada (feeley@cs.ubc.ca)
 Bernd Finkbeiner, Universität des Saarlandes, Germany (finkbeiner@cs.uni-sb.de)
 Cormac Flanagan, University of California, Santa Cruz, USA (cormac@cs.ucsc.edu)
 Ian Harris, University of California, Irvine, USA (harris@ics.uci.edu)
 Alan Hartman, IBM Haifa Labs, Israel (hartman@il.ibm.com)
 Warren Hunt, The University of Texas, Austin, USA (hunt@cs.utexas.edu)
 Abraham Kandel, University of South Florida, USA (kandel@cse.usf.edu)
 Tsvi Kuflik, University of Haifa, Israel (tsvikak@mis.hevra.haifa.ac.il)
 Mark Last, Ben Gurion University, Israel (mlast@bgumail.bgu.ac.il)
 Mauro Pezze, Università degli Studi di Milano, Bicocca, Italy (pezze@disco.unimib.it)
 Daniel J. Quinlan, Lawrence Livermore National Laboratories, USA (dquinlan@llnl.gov)
 Grigore Rosu, University of Illinois at Urbana-Champaign, USA (<http://cs.uiuc.edu/grosu>)
 Simon Rushton, IBM England, UK (RUSHTON@uk.ibm.com)
 Frank Scholz, IBM, Germany (FSCHOLZ@de.ibm.com)
 Assaf Schuster, Technion Institute, Haifa, Israel (assaf@cs.technion.ac.il)
 Scott Stoller, SUNY Stony Brook, USA (stoller@cs.sunysb.edu)
 Ofer Strichman, Technion, Israel (ofers@ie.technion.ac.il)
 Paul Strooper, University of Queensland, Australia (pstroop@itee.uq.edu.au)
 Serdar Tasiran, Ko- University, Turkey (stasiran@ku.edu.tr)
 Willem Visser, NASA, USA (wvisser@email.arc.nasa.gov)
 Yaron Wolfsthal, IBM Haifa Labs, Israel (wolfstal@il.ibm.com)
 Tao Xie, North Carolina State University, USA (taoxie@acm.org)
 Avi Ziv, IBM Haifa Labs, Israel (aziv@il.ibm.com)

Additional Referees:

Davide Lorenzoli
 Giovanni Denaro
 Sergey Polyakov
 Jinlin Yang
 Yarden Nir-Buchbinder
 Davide Tosi
 Leonardo Mariani
 Marina Biberstein

Table of Contents

Hardware Verification

Path-Based System Level Stimuli Generation <i>Shady Coptly, Itai Jaeger, Yoav Katz</i>	1
The Safety Simple Subset <i>Shoham Ben-David, Dana Fisman, Sitvanit Ruah</i>	14
A Case for Runtime Validation of Hardware <i>Sharad Malik</i>	30
Assertion-Based Verification for the SpaceCAKE Multiprocessor – A Case Study <i>Milind Kulkarni, J. Benita Bommi</i>	43
Simultaneous SAT-Based Model Checking of Safety Properties <i>Zurab Khasidashvili, Alexander Nadel, Amit Palti, Ziyad Hanna</i>	56
HAIFASAT: A New Robust SAT Solver <i>Roman Gershman, Ofer Strichman</i>	76

Software Testing

Production-Testing of Embedded Systems with Aspects <i>Jani Pesonen, Mika Katara, Tommi Mikkonen</i>	90
Assisting the Code Review Process Using Simple Pattern Recognition <i>Eitan Farchi, Bradley R. Harrington</i>	103
An Extensible Open-Source Compiler Infrastructure for Testing <i>Dan Quinlan, Shmuel Ur, Richard Vuduc</i>	116
Effective Black-Box Testing with Genetic Algorithms <i>Mark Last, Shay Eyal, Abraham Kandel</i>	134
Optimal Algorithmic Debugging and Reduced Coverage Using Search in Structured Domains <i>Yosi Ben-Asher, Igor Breger, Eitan Farchi, Ilia Gordon</i>	149

Benchmarking and Testing OSD for Correctness and Compliance <i>Dalit Naor, Petra Reshef, Ohad Rodeh, Allon Shafir, Adam Wolman, Eitan Yaffe</i>	158
--	-----

PADTAD

A Kernel-Based Communication Fault Injector for Dependability Testing of Distributed Systems <i>Roberto Jung Drebes, Gabriela Jacques-Silva, Joana Matos Fonseca da Trindade, Taisy Silva Weber</i>	177
Detecting Potential Deadlocks with Static Analysis and Run-Time Monitoring <i>Rahul Agarwal, Liqiang Wang, Scott D. Stoller</i>	191
Dynamic Deadlock Analysis of Multi-threaded Programs <i>Saddek Bensalem, Klaus Havelund</i>	208
Verification of the Java Causality Requirements <i>Sergey Polyakov, Assaf Schuster</i>	224
Choosing Among Alternative Futures <i>Steve MacDonald, Jun Chen, Diego Novillo</i>	247
Author Index	265