

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

University of California, Los Angeles, CA, 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

Luís Miguel Pinho
Michael González Harbour (Eds.)

Reliable Software Technologies – Ada-Europe 2006

11th Ada-Europe International Conference
on Reliable Software Technologies
Porto, Portugal, June 5-9, 2006
Proceedings



Springer

Volume Editors

Luís Miguel Pinho
Polytechnic Institute of Porto
School of Engineering (ISEP)
Rua Dr. António Bernardino de Almeida, 431, 4200-072 Porto, Portugal
E-mail: lpinho@dei.isep.ipp.pt

Michael González Harbour
Universidad de Cantabria
Departamento de Electrónica y Computadores
Avda. de los Castros s/n, 39005-Santander, Spain
E-mail: mgh@unican.es

Library of Congress Control Number: 2006926424

CR Subject Classification (1998): D.2, D.1.2-5, D.3, C.2.4, C.3, K.6

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-540-34663-5 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-34663-0 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: 11767077 06/3142 5 4 3 2 1 0

Preface

The 11th International Conference on Reliable Software Technologies, Ada-Europe 2006, took place in Porto, Portugal, June 5-9, 2006. It was as usual sponsored by Ada-Europe, the European federation of national Ada societies, in cooperation with ACM SIGAda. It was organized by members of the School of Engineering of the Polytechnic Institute of Porto, in collaboration with several colleagues from different institutions in Europe.

Following the usual style, the conference included a three-day technical program, during which the papers contained in these proceedings were presented, bracketed by two tutorial days where attendants had the opportunity to catch up on a variety of topics related to the field, at both introductory and advanced levels. Continuing the success achieved in the previous year, the technical program also included an industrial track, with contributions illustrating challenges faced and solutions encountered by industrialists from both sides of the Atlantic. Furthermore, the conference was accompanied by an exhibition where vendors presented their products for supporting reliable-software development.

The conference presented four distinguished speakers, who delivered state-of-the-art information on topics of great importance, both for the present and the future of software engineering:

- Correctness by Construction: Putting Engineering into Software
by Rod Chapman (Praxis HIS, UK)
- Empirical Software Risk Assessment Using Fault Injection
by Henrique Madeira (University of Coimbra, Portugal)
- Model-Driven Technologies in Safe-Aware Software Applications
by Miguel Angel de Miguel (Technical University of Madrid, Spain)
- I Have a Dream: ICT Problems We All Face
by John L. Hill (Sun Microsystems, USA)

We would like to express our sincere gratitude to these distinguished speakers, well known to the community, for sharing their insights with the conference participants.

A large number of regular papers were submitted, from as many as 23 different countries. The Program Committee worked hard to review them, and the selection process proved to be difficult, since many papers had received excellent reviews. Finally, the Program Committee selected 19 papers for the conference. The industrial track of the conference also received valuable contributions from industrialists, and the Industrial Committee finally selected 9 of them for the conference. The final result was a truly international program with contributions from Australia, Austria, Canada, China, France, Germany, Iran, Italy, Japan, Portugal, Spain, the UK, and the USA, covering a broad range of topics: real-time systems, static analysis, verification, applications, reliability, industrial experience, compilers and distributed systems.

The conference also included an interesting selection of tutorials, featuring international experts who presented introductory and advanced material in the domain of the conference:

- Verification and validation for reliable software systems, *William Bail*
- The Ada 2005 Standard Container Library, *Matthew Heaney*
- Developing Web-Aware Applications in Ada with AWS, *Jean-Pierre Rosen*
- SAE Architecture Analysis and Design Language, *Joyce L. Tokar*
- Model-Driven Development with the Unified Modeling Language (UML) 2.0TM and Ada, *Colin Coates*
- Distribution in Ada 95 with PolyORB, A Schizophrenic Middleware, *Jérôme Hugues*
- Requirements Management for Dependable Systems, *William Bail*
- Real-Time Java for Ada Programmers, *Benjamin M. Brosgol*

We would like to express our appreciation to these experts, for the work on preparing and presenting this material in the conference.

Many people contributed to the success of the conference. The Program and Industrial Committees, made up of international experts in the area of reliable software technologies, spent long hours carefully reviewing all the papers, presentations and tutorial proposals submitted to the conference. A subcommittee comprising Dirk Craeynest, Michael González Harbour, Laurent Pautet, Luís Miguel Pinho, Erhard Plöedereder, Jorge Real, and Tullio Vardanega met in Porto to make the final program selection. Various Program Committee members were assigned to shepherd some of the papers. We are grateful to all those who contributed to the technical program of the conference.

We would also like to thank the members of the Organizing Committee, for their valuable effort in taking care of all the bits and pieces that must fit together for a smooth run of the conference. We would like to thank Peter Dencker for the effort in the preparation of the industrial track, to Jorge Real for the attractive tutorial program and to José Ruiz for preparing the appealing exhibition of the conference. Also to Dirk Craeynest, who worked very hard to make the conference prominently visible, and to all the members of the Ada-Europe board for helping with the intricate details of the organization. A special thanks to Sandra Almeida, who took care of all details of the local organization.

Finally, we would like to express our appreciation to the authors of the contributions submitted to the conference, and to all the participants who helped in achieving the goal of the conference: providing a forum for researchers and practitioners for the exchange of information and ideas about reliable software technologies. We hope they all enjoyed the program as well as the social events of the 11th International Conference on Reliable Software Technologies.

Organization

Conference Chair

Luís Miguel Pinho, Polytechnic Institute of Porto, Portugal

Program Co-chairs

Luís Miguel Pinho, Polytechnic Institute of Porto, Portugal

Michael González Harbour, Universidad de Cantabria, Spain

Industrial Committee Co-chairs

Peter Dencker, Aonix GmbH, Germany

Michael González Harbour, Universidad de Cantabria, Spain

Tutorial Chair

Jorge Real, Universidad Politécnica de Valencia, Spain

Exhibition Chair

José Ruiz, AdaCore, France

Publicity Chair

Dirk Craeynest, Aubay Belgium and K.U. Leuven, Belgium

Local Chair

Sandra Almeida, Polytechnic Institute of Porto, Portugal

Ada-Europe Conference Liaison

Laurent Pautet, Telecom Paris, France

Program Committee

Alejandro Alonso, Universidad Politécnica de Madrid, Spain

Lars Asplund, Mälardalens Högskola, Sweden

Janet Barnes, Praxis High Integrity Systems, UK

Guillem Bernat, University of York, UK

Johann Blieberger, Technische Universität Wien, Austria

Ben Brosgol, AdaCore, USA
Bernd Burgstaller, University of Sydney, Australia
Alan Burns, University of York, UK
Dirk Craeynest, Aubay Belgium and K.U. Leuven, Belgium
Alfons Crespo, Universidad Politécnica de Valencia, Spain
Raymond Devillers, Université Libre de Bruxelles, Belgium
Michael González Harbour, Universidad de Cantabria, Spain
José Javier Gutiérrez, Universidad de Cantabria, Spain
Andrew Hatelly, Eurocontrol CRDS, Hungary
Günter Hommel, Technische Universität Berlin, Germany
Hubert Keller, Institut für Angewandte Informatik, Germany
Yvon Kermarrec, ENST Bretagne, France
Jörg Kienzle, McGill University, Canada
Fabrice Kordon, Université Pierre and Marie Curie, France
Albert Llamosi, Universitat de les Illes Balears, Spain
Franco Mazzanti, ISTI-CNR Pisa, Italy
John McCormick, University of Northern Iowa, USA
Stephen Michell, Maurya Software, Canada
Javier Miranda, Universidad Las Palmas de Gran Canaria, Spain
Laurent Pautet, Telecom Paris, France
Luís Miguel Pinho, Polytechnic Institute of Porto, Portugal
Erhard Plödereder, Universität Stuttgart, Germany
Juan A. de la Puente, Universidad Politécnica de Madrid, Spain
Jorge Real, Universidad Politécnica de Valencia, Spain
Alexander Romanovsky, University of Newcastle upon Tyne, UK
Jean-Pierre Rosen, Adalog, France
José Ruiz, AdaCore, France
Edmond Schonberg, New York University and AdaCore, USA
Joyce Tokar, Pyrrhus Software, USA
Tullio Vardanega, Università di Padova, Italy
Andy Wellings, University of York, UK
Jürgen Winkler, Friedrich-Schiller-Universität, Germany

Reviewers

Gaetan Allaert	Bernd Burgstaller
Alejandro Alonso	Alan Burns
Mrio Amado Alves	Dirk Craeynest
Wolfram Amme	Alfons Crespo
Lars Asplund	Garreg Lewis Dawe
Ricardo Barbosa	Raymond Devillers
Janet Barnes	Michael González Harbour
Johann Blieberger	José Javier Gutiérrez
Maarten Boasson	Andrew Hatelly
Ben Brosgol	Günter Hommel

Stefan Kauer
 Hubert Keller
 Yvon Kermarrec
 Jörg Kienzle
 Fabrice Kordon
 Albert Llamosi
 Kristina Lundqvist
 Franco Mazzanti
 John McCormick
 Stephen Michell
 Javier Miranda
 Gustaf Naeser
 Martin Ouimet
 Laurent Pautet

Luís Miguel Pinho
 Erhard Plödereder
 Juan A. de la Puente
 Jorge Real
 Alexander Romanovsky
 Philippe Rose
 Jean-Pierre Rosen
 José Ruiz
 Edmond Schonberg
 Joyce Tokar
 Tullio Vardanega
 Andy Wellings
 Jürgen Winkler

Table of Contents

Real-Time Systems

Hierarchical Scheduling with Ada 2005

<i>José A. Pulido, Santiago Urueña, Juan Zamorano, Tullio Vardanega, Juan A. de la Puente</i>	1
---	---

A Comparison of Ada and Real-Time JavaTM for Safety-Critical Applications

<i>Benjamin M. Brosgol, Andy Wellings</i>	13
---	----

POSIX Trace Based Behavioural Reflection

<i>Filipe Valpereiro, Luís Miguel Pinho</i>	27
---	----

Static Analysis

Static Detection of Access Anomalies in Ada95

<i>Bernd Burgstaller, Johann Blieberger, Robert Mittermayr</i>	40
--	----

One Million (LOC) and Counting: Static Analysis for Errors and Vulnerabilities in the Linux Kernel Source Code

<i>Peter T. Breuer, Simon Pickin</i>	56
--	----

Bauhaus – A Tool Suite for Program Analysis and Reverse Engineering

<i>Aoun Raza, Gunther Vogel, Erhard Plödereder</i>	71
--	----

Verification

SPARK Annotations Within Executable UML

<i>Damian Curtis</i>	83
----------------------------	----

Runtime Verification of Java Programs for Scenario-Based Specifications

<i>Xuandong Li, Linzhang Wang, Xiaokang Qiu, Bin Lei, Jiesong Yuan, Jianhua Zhao, Guoliang Zheng</i>	94
--	----

Applications

Secure Execution of Computations in Untrusted Hosts

<i>S.H.K. Narayanan, M.T. Kandemir, R.R. Brooks, I. Kolcu</i>	106
---	-----

A Systematic Approach to Developing Safe Tele-operated Robots

<i>Diego Alonso, Pedro Sánchez, Bárbara Álvarez, Juan A. Pastor</i>	119
---	-----

Towards Developing Multi-agent Systems in Ada <i>G. Aranda, J. Palanca, A. Espinosa, A. Terrasa, A. García-Fornes</i>	131
--	-----

Reliability

A Software Reliability Model Based on a Geometric Sequence of Failure Rates <i>Stefan Wagner, Helmut Fischer</i>	143
Adaptive Random Testing Through Iterative Partitioning <i>T.Y. Chen, De Hao Huang, Zhi Quan Zhou</i>	155
Run-Time Detection of Tasking Deadlocks in Real-Time Systems with the Ada 95 Annex of Real-Time Systems <i>Jingde Cheng</i>	167

Compilers

Abstract Interface Types in GNAT: Conversions, Discriminants, and C++ <i>Javier Miranda, Edmond Schonberg</i>	179
Using Mathematics to Improve Ada Compiled Code <i>Ward Douglas Maurer</i>	191

Distributed Systems

Replication-Aware Transactions: How to Roll a Transaction over Failures <i>Mohsen Sharifi, Hadi Salimi</i>	203
The Arbitrated Real-Time Protocol (AR-TP): A Ravenscar Compliant Communication Protocol for High-Integrity Distributed Systems <i>Santiago Urueña, Juan Zamorano, Daniel Berjón, José A. Pulido, Juan A. de la Puente</i>	215
Interchangeable Scheduling Policies in Real-Time Middleware for Distribution <i>Juan López Campos, J. Javier Gutiérrez, Michael González Harbour</i>	227
Author Index	241