Lecture Notes in Computer Science 3555

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Tullio Vardanega Andy Wellings (Eds.)

Reliable Software Technology – Ada-Europe 2005

10th Ada-Europe International Conference
on Reliable Software Technologies
York, UK, June 20-24, 2005
Proceedings

Springer

Volume Editors

Tullio Vardanega
University of Padua
Department of Pure and Applied Mathematics
via G. Belzoni 7, 35131 Padua, Italy
E-mail: tullio.vardanega@math.unipd.it

Andy Wellings
University of York
Department of Computer Science
Heslington, York, YO10 5DD, UK
E-mail: andy@cs.york.ac.uk

Library of Congress Control Number: 2005927232

CR Subject Classification (1998): D.2, D.1.2-5, D.3, C.2-4, C.3, K.6

ISSN 0302-9743
ISBN-10 3-540-26286-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-26286-2 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11499909 06/3142 5 4 3 2 1 0

Preface

Started on the inspired initiative of Prof. Alfred Strohmeier back in 1996, and spawned from the annual Ada-Europe conference that had previously run for 16 consecutive years, the International Conference on Reliable Software Technologies celebrated this year its tenth anniversary by going to York, UK, where the first series of technical meetings on Ada were held in the 1970s.

Besides being a beautiful and historical place in itself, York also hosts the Department of Computer Science of the local university, whose Real-Time Group has been tremendously influential in shaping the Ada language and in the progress on real-time computing worldwide. This year's conference was therefore put together under excellent auspices, in a very important year for the Ada community in view of the forthcoming completion of the revision process that is upgrading the language standard to face the challenges of the new millennium.

The conference took place on June 20–24, 2005. It was as usual sponsored by Ada-Europe, the European federation of national Ada societies, in cooperation with ACM SIGAda. The conference was organized by selected staff of the University of York teamed up with collaborators from various places in Europe, in what turned out to be a very effective instance of distributed collaborative processing. The conference also enjoyed the generous support of 11 industrial sponsors.

This year's conference was very successful indeed. It attracted the largest number of submissions in years, from as many as 15 countries worldwide, which made the selection process tougher than ever. Overall, the conference program included 21 carefully selected and refereed papers assigned to 8 thematic sessions spanning a variety of high-profile subjects. The technical program included an industrial track, a first in the conference's history, which encompassed 10 contributions illustrating challenges faced by a cross-section of high-integrity software industry in Europe and the US. As usual, the conference program was itself bracketed by two full days of tutorials, with a special half-day presentation on the new Ada 2005 language, offered by four of its lead designers: John Barnes, Alan Burns, Pascal Leroy and Tucker Taft. Furthermore, three keynote presentations, delivered by John McDermid, Martin Thomas and Bev Littlewood, respectively, marked the opening of each of the main conference days. Finally, much in keeping with the well-established tradition of the conference series, the program made provisions for an excellently populated vendor exhibition and for a half-day vendor session, in which participants were able to catch up with the latest advances in reliable software technology products.

Let us now go into the details of some of the conference highlights.

The invited talks were as follows:

- Prof. John McDermid, University of York, UK
  Model-Based Development of Safety-Critical Software
  where the opportunities and challenges of model-based development were discussed.
- Prof. Martyn Thomas, Thomas Associates, UK
  Extreme Hubris
  where the principles of Extreme Programming were critically examined and an alternative manifesto for dependable software development was proposed.
- Prof. Bev Littlewood, City University, London, UK
  Assessing the Dependability of Software-Based Systems: a Question of Confidence
  where the controversial contention was made that dependability claims ought to be associated with a probability-based assessment of the inherent uncertainty about the truth of the claim.

The technical sessions of the program ranged from the illustration of successful applications and distributed systems, to the discussion of design, analysis and implementation methodologies, to formal methods, certification and verification, through to the latest advances with Ravenscar technology, to finish with Ada-related concerns regarding education and language implementation issues.

The tutorial program gathered the following assortment of topics and international expert speakers

- Developing Web-Aware Applications in Ada with AWS, Jean-Pierre Rosen, *Adalog, France*
- Correctness by Construction — A Manifesto for High Integrity Systems, Peter Amey and Neil White, *Praxis High Integrity Systems, UK*
- Real-Time Java for Ada Programmers, Benjamin M. Brosgol, *AdaCore, US*
- SAE Architecture Analysis and Design Language, Joyce Tokar, *Pyrrhus Software, US* and Bruce Lewis, *US Army*
- High-Integrity Ravenscar Using SPARK, Brian Dobbing, *Praxis High Integrity Systems, UK*
- Software Safety Cases, John McDermid and Rob Weaver, *University of York, UK*
- Requirement Engineering for Dependable Systems, William Bail, *The MITRE Corporation, US*
- Software Fault Tolerance, Patrick Rogers, *AdaCore, US*
- Programming with the Ada 2005 Standard Container Library, Matthew Heaney, *On2 Technologies, US*

in addition of course to a special half-day session where four of the lead designers of Ada 2005, John Barnes, Alan Burns, Pascal Leroy and S. Tucker Taft, provided an extensive overview of the new features introduced by the language revision.

A number of people crucially contributed to the success of the conference. First and foremost the authors of all the papers, talks and presentations, for it was from their contribution that the conference was put together. The Program Committee members helped promote the conference in their own circles and also successfully solicited submissions from a variety of authors. The same members along with a number of others also devoted considerable effort to refereeing the submissions in a thorough and timely fashion. The program itself was put together by a smaller group including the Conference Chair, Alan Burns, the Program Co-chairs, Tullio Vardanega and Andy Wellings,

the Tutorials Chair, Iain Bate, the Exhibition and Industrial Track Chair, Rod Chapman, and Dirk Craeynest, representing Ada-Europe. Selected PC members also undertook to shepherd some papers to their final versions. All of these people deserve our gratitude, along with the local organizers, in particular Ian Broster, also in charge of the conference publicity along with Dirk Craeynest, and Sue Helliwell, who oversaw the administrative details of the registration process.

We trust the attendees enjoyed both the technical and social program of the conference, and we close this volume with the confidence of a job well done and the satisfaction of a thoroughly enjoyed experience.

June 2005 Tullio Vardanega

Organization

Conference Chair

Alan Burns, University of York, UK

Program Co-chairs

Tullio Vardanega, University of Padua, Italy
Andy Wellings, University of York, UK

Tutorial Chair

Iain Bate, University of York, UK

Exhibition and Industrial Track Chair

Rod Chapman, Praxis High Integrity Systems, UK

Publicity Co-chairs

Ian Broster, University of York, UK
Dirk Craeynest, Aubay Belgium, Katholieke Universiteit Leuven, Belgium

Local Organization Administrator

Sue Helliwell, University of York, UK

Ada-Europe Conference Liaison

Laurent Pautet, ENST Paris, France

Other Program Commitee Members

Lars Asplund, Mälardalens Högskola, Sweden
Alejandro Alonso, Universidad Politecnica de Madrid, Spain
Janet Barnes, Praxis High Integrity Systems, UK
Guillem Bernat, University of York, UK
Johann Blieberger, Technische Universität Wien, Austria
Bernd Burgstaller, Technische Universität Wien, Austria
Ulf Cederling, Vaxjo University, Sweden
Alfons Crespo, Universidad Politecnica de Valencia, Spain
Raymond Devillers, Université Libre de Bruxelles, Belgium
Michael González Harbour, Universidad de Cantabria, Spain
Andrew Hately, CEATS Research Development Simulation Centre, Hungary
Günter Hommel, Technischen Universität Berlin, Germany
Stefan Kauer, EADS Dornier, Germany
Hubert Keller, Institut für Angewandte Informatik, Germany
Yvon Kermarrec, ENST Bretagne, France
Jörg Kienzle, McGill University, Canada
Fabrice Kordon, Université Pierre & Marie Curie, France
Albert LLamosi, Universitat de les Illes Balears, Spain
Franco Mazzanti, Istituto di Scienza e Tecnologie dell'Informazione, Italy
John McCormick, University of Northern Iowa, USA
Javier Miranda, Universidad Las Palmas de Gran Canaria, Spain
Juan A. de la Puente, Universidad Politecnica de Madrid, Spain
Erhard Plödereder, Universität Stuttgart, Germany
Alexander Romanovsky, University of Newcastle upon Tyne, UK
Jean-Pierre Rosen, Adalog, France
Edmond Schonberg, New York University and AdaCore, USA
Jörgen Winkler, Friedrich-Schiller-Universität, Germany

Referees

Alejandro Alonso
Las Asplund
Khaled Barbaria
Janet Barnes
Guillem Bernat
Johann Blieberger
Maarten Boasson
Ben Brosgol
Ian Broster
Bernd Burgstaller
Alan Burns
Ulf Cederling
John Clark
Dirk Craeynest
Alfons Crespo
Raymond Devillers
Claude Dutheillet
Javier Esparza
Michael González-Harbour
Andrew Hately
Günter Hommel
Erik Hu
Jerome Hugues
Alexei Iliasov

Stefan Kauer
Hubert Keller
Yvon Kermarrec
Jörg Kienzle
Fabrice Kordon
Albert Llamosi
Moreno Marzolla
Franco Mazzanti
Javier Miranda
John McCormick
Laurent Pautet
Juan A. de la Puente
Erhard Plödereder
Alexander Romanovsky
Jean-Pierre Rosen
Bo Sandèn
Edmond Schonberg
Tullio Vardanega
Thomas Vergnaud
Andy Wellings
Jörgen Winkler

Table of Contents

Applications

Design and Scheduling Issues

Formal Methods

Ada and Education

Certification and Verification

Distributed Systems

Language Issues

Ravenscar Technology