Lecture Notes in Computer Science 2655

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Jean-Pierre Rosen Alfred Strohmeier (Eds.)

Reliable Software Technologies – Ada-Europe 2003

8th Ada-Europe International Conference
on Reliable Software Technologies
Toulouse, France, June 16-20, 2003
Proceedings

Springer

Volume Editors

Jean-Pierre Rosen
Adalog
19-21 rue du 8 mai 1945
94110 Arcueil, France
E-mail: rosen@adalog.fr

Alfred Strohmeier
Swiss Federal Institute of Technology Lausanne
Software Engineering Laboratory
1015 Lausanne EPFL, Switzerland
E-mail: alfred.strohmeier@epfl.ch

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

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

ISSN 0302-9743
ISBN 3-540-40376-0 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by PTP-Berlin GmbH
Printed on acid-free paper SPIN: 10936917 06/3142 5 4 3 2 1 0

Preface

The 8th International Conference on Reliable Software Technologies, Ada-Europe 2003, took place in Toulouse, France, June 18–20, 2003. It was sponsored by Ada-Europe, the European federation of national Ada societies, and Ada-France, in cooperation with ACM SIGAda. It was organized by members of Adalog, CS, UPS/IRIT and ONERA.

Toulouse was certainly a very appropriate place for this conference. As the heart of the European aeronautic and space industry, it is a place where software development leaves no place for failure. In the end, reliability is a matter of human skills. But these skills build upon methods, tools, components and controlled practices. By exposing the latest advances in these areas, the conference contributed to fulfilling the needs of a very demanding industry.

As in past years, the conference comprised a three-day technical program, during which the papers contained in these proceedings were presented, along with vendor presentations. The technical program was bracketed by two tutorial days, when attendees had the opportunity to catch up on a variety of topics related to the field, at both introductory and advanced levels. On Friday, a workshop on "Quality of Service in Component-Based Software Engineering" was held. Further, the conference was accompanied by an exhibition where vendors presented their reliability-related products.

Invited Speakers

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

- An Invitation to Ada 2005
  Pascal Leroy, Rational Software, France
- Modules for Crosscutting Models
  Mira Mezini and Klaus Ostermann, Darmstadt University of Technology, Germany
- Software Fault Tolerance: An Overview
  Jörg Kienzle, McGill University, Canada

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 and for having written up their contributions for the proceedings.

Submitted Papers

A large number of papers were submitted, from as many as 20 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 29 papers for the conference. The final result was a truly international program with authors from Austria, Belgium, Finland, France, Germany, Hong Kong, India, Israel, Italy, Portugal, Spain, the United Kingdom, and the USA, covering a broad range of software technologies: fault tolerance, high integrity and the Ravenscar profile, real-time systems, distributed systems, formal specifications, performance evaluation and metrics, testing, tools, OO programming, software components, HOOD, UML, XML, language issues, and teaching.

Tutorials

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

- The Personal Software Process^{SM} for Ada, *Daniel Roy*
- Developing High Integrity Systems with GNAT/ORK, *Juan Antonio de la Puente and Juan Zamorano*
- Implementing Design Patterns in Ada 95, *Matthew Heaney*
- Principles of Physical Software Design in Ada 95, *Matthew Heaney*
- High Integrity Ravenscar Using SPARK, *Peter Amey*
- Architecture Centric Development Using Ada and the Avionics Architecture Description Language, *Bruce Lewis*
- A Semi-formal Approach to Software Systems Development, *William Bail*
- An Overview of Statistical-Based Testing, *William Bail*

Workshop on Quality of Service in Component-Based Software Engineering

It is now widely recognized that what makes Component-Based Software Engineering (CBSE) hard is not the production of components but their composition. The workshop focused on methods and tools, but also on the difficulties involved in predicting the overall behavior of a composite from the properties of its components, including emerging properties, i.e. performance, reliability, safety, etc. Ideally, it should be possible for the software engineer to express the qualities of service required for each component, and a composition "calculus" would then predict the quality of service of the composite. The workshop brought together practitioners and academics currently working on these issues.

Acknowledgements

Many people contributed to the success of the conference. The program committee, made up of international experts in the area of reliable software technologies, spent long hours carefully reviewing all the papers and tutorial proposals

submitted to the conference. A subcommittee comprising Pierre Bazex, Agusti Canals, Dirk Craeynest, Michel Lemoine, Albert Llamosi, Thierry Millan, Laurent Pautet, Erhard Plödereder, Jean-Pierre Rosen and Alfred Strohmeier met in Toulouse to make the final paper selection. Some 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. Special thanks to Jean-Michel Bruel whose dedication was key to the success of the workshop.

We would also like to thank the members of the organizing committee, and especially the people at CS, UPS/IRIT and ONERA, for the work spent in the local organization. Agusti Canals managed the general organization of the conference. Pierre Bazex and Thierry Millan supervised the preparation of the attractive tutorial program. Frédéric Dumas was in charge of the conference exhibition. Dirk Craeynest and Michel Lemoine worked hard to make the conference prominently visible. Jean-Marie Rigaud dealt with all the details of the local organization, and Carole Bernon did a great job in preparing the web pages and all the Internet facilities. Voyages 31 had the important duty of taking care of the registration and financial management. Many thanks also to Laurent Pautet, who was in charge of the liaison with Ada-Europe.

A great help in organizing the submission process and the paper reviews was the START Conference Manager, provided graciously by Rich Gerber.

Special thanks are due to our sponsors, the French DGA, Mairie de Toulouse and Conseil Régional Midi-Pyrénées.

Last, but not least, we would like to express our appreciation to the authors of the papers 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 technical program as well as the social events of the 8th International Conference on Reliable Software Technologies.

June 2003

Jean-Pierre Rosen
Alfred Strohmeier

Organizing Committee

Conference Chair

Agusti Canals, CS, France

Program Co-chairs

Jean-Pierre Rosen, Adalog, France
Alfred Strohmeier, Swiss Fed. Inst. of Technology, Lausanne, Switzerland

Tutorial Co-chairs

Pierre Bazex, UPS/IRIT, France
Thierry Millan, UPS/IRIT, France

Exhibition Chair

Frédéric Dumas, CS, France

Publicity Co-chairs

Dirk Craeynest, Offis, Belgium
Michel Lemoine, ONERA, France

Local Organization Co-chairs

Jean-Marie Rigaud, UPS/IRIT, France
Carole Bernon, UPS/IRIT, France

Ada-Europe Conference Liaison

Laurent Pautet, ENST, France

Program Committee

Alejandro Alonso, ETSI Telecomunicacion, Spain
Ángel Álvarez, Technical University of Madrid, Spain
Lars Asplund, Uppsala University, Sweden
Neil Audsley, University of York, UK
Janet Barnes, Praxis Critical Systems Ltd., UK
Pierre Bazex, IRIT, France

Guillem Bernat, University of York, UK
Johann Blieberger, Technische Universität Wien, Austria
Maarten Boasson, University of Amsterdam, The Netherlands
Ben Brosgol, ACT, USA
Bernd Burgstaller, Technische Universität Wien, Austria
Agusti Canals, CS, France
Ulf Cederling, Vaxjo University, Sweden
Roderick Chapman, Praxis Critical Systems Ltd., UK
Dirk Craeynest, Offis nv/sa and KU Leuven, Belgium
Alfons Crespo, Universidad Politécnica de Valencia, Spain
Juan A. de la Puente, Universidad Politécnica de Madrid, Spain
Peter Dencker, Aonix GmbH, Germany
Raymond Devillers, Universite Libre de Bruxelles, Belgium
Wolfgang Gellerich, IBM, Germany
Jesús M. González-Barahona, Universidad Rey Juan Carlos, Spain
Michael González-Harbour, Universidad de Cantabria, Spain
Thomas Gruber, Austrian Research Centers, Seibersdorf, Austria
Helge Hagenauer, University Salzburg, Austria
Andrew Hately, Eurocontrol, Belgium
Hubert B. Keller, Institut für Angewandte Informatik, Germany
Yvon Kermarrec, ENST Bretagne, France
Jörg Kienzle, Swiss Federal Institute of Technology, Lausanne, Switzerland
Fabrice Kordon, UPMC, France
Michel Lemoine, ONERA, France
Albert Llamosi, Universitat de les Illes Balears, Spain
Kristina Lundqvist, Massachusetts Institute of Technology, USA
Franco Mazzanti, Istituto di Elaborazione della Informazione, Italy
John W. McCormick, University of Northern Iowa, USA
Thierry Millan, IRIT, France
Pierre Morere, Aonix, France
Pascal Obry, EdF, France
Laurent Pautet, ENST Paris, France
Erhard Plödereder, University of Stuttgart, Germany
Ceri Reid, CODA Technologies, UK
Jean-Marie Rigaud, Université Paul Sabatier, France
Alexander Romanovsky, University of Newcastle, UK
Jean-Pierre Rosen, Adalog, France
Bo I. Sandén, Colorado Technical University, USA
Bernhard Scholz, Technische Universität Wien, Austria
Edmond Schonberg, New York University and ACT, USA
Gerald Sonneck, ARC Seibersdorf research GmbH, Austria
Alfred Strohmeier, Swiss Fed. Inst. of Technology, Lausanne, Switzerland Tullio
Vardanega, University of Padova, Italy
Andy Wellings, University of York, UK
Jürgen Winkler, Friedrich-Schiller-Universität, Germany
Thomas Wolf, Paranor AG, Switzerland

Table of Contents

Distributed Information Systems

Metrics

Software Components

Formal Specification

Real-Time Kernel

Testing

Real-Time Systems Design