

# Lecture Notes in Computer Science

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

2655

**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

## Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

## 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

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003  
Printed in Germany

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<sup>SM</sup> 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, Université 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

## Invited Papers

An Invitation to Ada 2005 .....	1
<i>Pascal Leroy</i>	
Modules for Crosscutting Models .....	24
<i>Mira Mezini, Klaus Ostermann</i>	
Software Fault Tolerance: An Overview .....	45
<i>Jörg Kienzle</i>	

## Ravenscar

High Integrity Ravenscar .....	68
<i>Peter Amey, Brian Dobbins</i>	
Adding Temporal Annotations and Associated Verification to Ravenscar Profile .....	80
<i>Alan Burns, Tse-Min Lin</i>	
Impact of a Restricted Tasking Profile: The Case of the GOCE Platform Application Software .....	92
<i>Niklas Holsti, Thomas Långbacka</i>	

## Language Issues

Booch's Ada vs. Liskov's Java: Two Approaches to Teaching Software Design .....	102
<i>Ehud Lamm</i>	
A Comparison of the Asynchronous Transfer of Control Features in Ada and the Real-Time Specification for Java™ .....	113
<i>Benjamin M. Brosgol, Andy Wellings</i>	
Exposing Memory Corruption and Finding Leaks: Advanced Mechanisms in Ada .....	129
<i>Emmanuel Briot, Franco Gasperoni, Robert Dewar, Dirk Craeynest, Philippe Waroquiers</i>	

## Static Analysis

Busy Wait Analysis .....	142
<i>Johann Blieberger, Bernd Burgstaller, Bernhard Scholz</i>	

Eliminating Redundant Range Checks in GNAT Using Symbolic Evaluation	153
<i>Johann Blieberger, Bernd Burgstaller</i>	

Quasar: A New Tool for Concurrent Ada Programs Analysis	168
<i>Sami Evangelista, Claude Kaiser, Jean-François Pradat-Peyre, Pierre Rousseau</i>	

## Distributed Information Systems

A Graphical Environment for GLADE	182
<i>Ernestina Martel, Francisco Guerra, Javier Miranda, Luis Hernández</i>	

The Use of Ada, GNAT.Spitbol, and XML in the Sol-Eu-Net Project	196
<i>Mário Amado Alves, Alípio Jorge, Matthew Heaney</i>	

Transactions and Groups as Generic Building Blocks for Software Fault Tolerance	208
<i>Marta Patiño-Martínez, Ricardo Jiménez-Peris, Alexander Romanovsky</i>	

## Metrics

Getting System Metrics Using POSIX Tracing Services	220
<i>Agustín Espinosa Minguet, Vicente Lorente Garcés, Ana García Fornes, Alfons Crespo i Lorente</i>	

Some Architectural Features of Ada Systems Affecting Defects	232
<i>William M. Evanco, June Verner</i>	

Evidential Volume Approach for Certification	246
<i>Silke Kuball, Gordon Hughes</i>	

## Software Components

A Survey of Physical Unit Handling Techniques in Ada	258
<i>Christoph Grein, Dmitry A. Kazakov, Fraser Wilson</i>	

Charles: A Data Structure Library for Ada95	271
<i>Matthew Heaney</i>	

A Quality Model for the Ada Standard Container Library	283
<i>Xavier Franch, Jordi Marco</i>	

## Formal Specification

Experiences on Developing and Using a Tool Support for Formal Specification	297
<i>Tommi Mikkonen</i>	

A Behavioural Notion of Subtyping for Object-Oriented Programming in SPARK95 .....	309
<i>Tse-Min Lin, John A. McDermid</i>	

## Real-Time Kernel

Running Ada on Real-Time Linux .....	322
<i>Miguel Masmano, Jorge Real, Ismael Ripoll, Alfons Crespo</i>	
A Round Robin Scheduling Policy for Ada .....	334
<i>A. Burns, M. González Harbour, A.J. Wellings</i>	
A Proposal to Integrate the POSIX Execution-Time Clocks into Ada 95 .....	344
<i>Javier Miranda, M. González Harbour</i>	

## Testing

A Test Environment for High Integrity Software Development .....	359
<i>Alejandro Alonso, Juan Antonio de la Puente, Juan Zamorano</i>	
Normalized Restricted Random Testing .....	368
<i>Kwok Ping Chan, Tsong Yueh Chen, Dave Towey</i>	
Testing Safety Critical Ada Code Using Non Real Time Testing.....	382
<i>Y.V. Jeppu, K. Karunakar, P.S. Subramanyam</i>	

## Real-Time Systems Design

The Standard UML-Ada Profile .....	394
<i>Francis Thom</i>	
HRT-UML: Taking HRT-HOOD onto UML .....	405
<i>Silvia Mazzini, Massimo D'Alessandro, Marco Di Natale, Andrea Domenici, Giuseppe Lipari, Tullio Vardanega</i>	
A Case Study in Performance Evaluation of Real-Time Teleoperation Software Architectures Using UML-MAST .....	417
<i>Francisco Ortiz, Bárbara Álvarez, Juan Á. Pastor, Pedro Sánchez</i>	

<b>Author Index</b> .....	429
---------------------------	-----