Lecture Notes in Computer Science 2043

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

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

Dirk Craeynest Alfred Strohmeier (Eds.)

Reliable Software Technologies – Ada-Europe 2001

6th Ada-Europe International Conference
on Reliable Software Technologies
Leuven, Belgium, May 14-18, 2001
Proceedings

Springer

Series Editors

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

Volume Editors

Dirk Craeynest
Offis & K.U. Leuven
Offis nv/sa - Aubay Group
Weiveldlaan 41/32, 1930 Zaventem, Belgium
E-mail: dirk.craeynest@offis.be

Alfred Strohmeier
Swiss Federal Institute of Technology Lausanne (EPFL)
EPFL-DI-LGL, 1015 Lausanne EPFL, Switzerland
E-mail: alfred.strohmeier@epfl.ch

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Reliable software technologies : Ada Europe ... ; ... Ada Europe
international conference ... ; proceedings. - 5. 2000 (Juni 2000)-. -
Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;
Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
Erscheint unregelmäßig. - Früher begrenztes Werk in verschiedenen
Ausg. - Bibliographische Deskription nach 6. 2001
(Lecture notes in computer science ; ...)
6. Ada Europe 2001 : Leuven, Belgium, May 14 - 18, 2001. - (2001)
(Lecture notes in computer science ; Vol. 2043)
ISBN 3-540-42123-8

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

ISSN 0302-9743
ISBN 3-540-42123-8 Springer-Verlag Berlin Heidelberg New York

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

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna
Printed on acid-free paper SPIN 10782549 06/3142 5 4 3 2 1 0

Foreword

The Sixth International Conference on Reliable Software Technologies, Ada-Europe 2001, took place in Leuven, Belgium, May 14-18, 2001. It was sponsored by Ada-Europe, the European federation of national Ada societies, in cooperation with ACM SIGAda, and it was organized by members of the K.U. Leuven and Ada-Belgium. This was the 21st consecutive year of Ada-Europe conferences and the sixth year of the conference focusing on the area of reliable software technologies.

The use of software components in embedded systems is almost ubiquitous: planes fly by wire, train signalling systems are now computer based, mobile phones are digital devices, and biological, chemical, and manufacturing plants are controlled by software, to name only a few examples. Also other, non-embedded, mission-critical systems depend more and more upon software. For these products and processes, reliability is a key success factor, and often a safety-critical hard requirement.

It is well known and has often been experienced that quality cannot be added to software as a mere afterthought. This also holds for reliability. Moreover, the reliability of a system is not due to and cannot be built upon a single technology. A wide range of approaches is needed, the most difficult issue being their purposeful integration. Goals of reliability must be precisely defined and included in the requirements, the development process must be controlled to achieve these goals, and sound development methods must be used to fulfill these non-functional requirements.

All artifacts produced must be verified. Useful verification techniques are numerous and complementary: reviewing design documents, proving properties of a program, including its correctness, reasoning about a program, performing static analysis, but also dynamic testing based on program execution, to mention just a few.

Development of software requires tools, and some are more helpful than others for tracking down or avoiding errors. Some techniques are well established, such as strong type checking of the source code by the language compiler. Here, the Ada programming language excels, for it was designed with reliability as a goal. Other techniques are less common and considered as more advanced, such as automatic test generation based on formal specifications.

Clearly, the domain is vast and not all issues related to reliable software technologies can be covered in a single conference, but we are proud to say that these proceedings span a wide range of them and constitute a rich collection of contributions.

Invited Speakers

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

- Building Formal Requirements Models for Reliable Software
  Axel van Lamsweerde, Université Catholique de Louvain, Belgique
- Using Ada in Interactive Digital Television Systems
  Pascal Héraud, CANAL+ Technologies, France

- Testing from Formal Specifications, a Generic Approach
  Marie-Claude Gaudel, Université de Paris-Sud, France
- Logic versus Magic in Critical Systems
  Peter Amey, Praxis Critical Systems, UK
- Can Java Meet its Real-Time Deadlines?
  Brian Dobbing, Aonix Europe Ltd,UK, and co-author Ben Brosgol, ACT, 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 and for having written up their contributions for the proceedings.

Submitted Papers

A large number of papers were submitted. 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 27 papers for inclusion in the proceedings, and 2 contributions for presentation only. The final result was a truly international program with authors from Australia, Belgium, China, France, Germany, Israel, Portugal, Russia, Spain, Sweden, Switzerland, the United Kingdom, and the USA, covering a broad range of software technologies: Formal Methods, Testing, High-Integrity Systems, Program Analysis, Distributed Systems, Real-Time Systems, Language and Patterns, Dependable Systems, APIs and Components, Real-Time Kernels, Standard Formats: UML & XML, System Evolution, and Software Process.

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:

- Non-Standard Techniques in Ada
  Art Duncan, RPI, USA
- Practical Experiences of Safety-Critical Ada Technologies
  Peter Amey and Rod Chapman, Praxis Critical Systems, UK
- Early Reliability Measurement and Improvement
  Jeff Tian, SMU, USA
- An Introduction to XML
  Gregory Neven, Maarten Coene, and Roel Adriaensens, K.U. Leuven, Belgium
- From Full Concurrency to Safe Concurrency
  John Harbaugh, Boeing, USA
- Building Distributed Systems with Ada
  Samuel Tardieu, Laurent Pautet, and Thomas Quinot, ENST, France
- Implementing Design Patterns in Ada: Sequential Programming Idioms
  Matthew Heaney, USA
- Architecture Centred Development and Evolution of Reliable Real-Time Systems
  Bruce Lewis and Ed Colbert, USA

Workshop on Exception Handling

At the initiative of Alexander Romanovsky, Alfred Strohmeier, and Andy Wellings, a full-day workshop was held on ”Exception Handling for a 21st Century Programming Language”. As the complexity of modern software systems grows, so does the need to deal reliably and efficiently with an increasing number of abnormal situations. The most general mechanism for this is exception handling, which is becoming a standard feature in modern languages. Ada has been the first mainstream programming language integrating exceptions in the procedural paradigm, and Java has fused exceptions with object-orientation. However, integration of exceptions and concurrency are still the subject of research, and the performance of ”object-oriented exceptions” for hard real-time systems should be investigated.

The aims of the workshop were therefore:

- to share experience on how to build modern systems that have to deal with abnormal situations;
- to discuss how solutions to those needs can be developed employing standard Ada features including the current exception handling paradigm;
- to propose new exception handling mechanisms/paradigms that can be included in future revisions of the Ada language and also fit high integrity language profiles for safety critical systems.

Participation to the workshop was by invitation upon acceptance of a submission, e.g. a brief position paper, an experience report, or a full research paper. The papers were made available to the participants before the workshop. The workshop included talks based on the submitted papers and intensive shepherded discussion sessions. Selected submissions will be published in Ada Letters.

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 Luc Bernard, Johann Blieberger, Dirk Craeynest, Erhard Ploedereder, Juan Antonio de la Puente, and Alfred Strohmeier met in Leuven 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 Alexander Romanovsky, whose dedication was key to the success of the workshop. We are also grateful to Raul Silaghi who did most of the clerical work for the preparation of this volume.

We would also like to thank the members of the organizing committee, and especially the people of the K.U. Leuven, for the work spent in the local organization. Karel De Vlaminck and Yolande Berbers were in charge of the overall coordination and took care of all the clerical details for the successful running of the conference. Luc Bernard supervised the preparation of the attractive tutorial program. Yvan Barbaix worked long hours contacting companies and people to prepare the conference

exhibition. Dirk Walravens created and maintained the conference Web site, and supported the paper submission and review process. Special thanks to Andrew Hately for publicizing the conference by post and e-mail, and for preparing the brochure with the conference program. A great help in organizing the submission process and the paper reviews was the START Conference Manager, provided graciously by Rich Gerber.

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 6th International Conference on Reliable Software Technologies.

May 2001

Alfred Strohmeier

Dirk Craeynest

Organizing Committee

Conference Chair
Karel De Vlaminck, K.U. Leuven, Belgium

Program Co-chairs
Dirk Craeynest, Offis nv/sa & K.U. Leuven, Belgium
Alfred Strohmeier, Swiss Fed. Inst. of Technology Lausanne (EPFL), Switzerland

Tutorial Chair
Luc Bernard, Offis nv/sa, Belgium

Exhibition Chair
Yvan Barbaix, K.U. Leuven, Belgium

Publicity Chair
Andrew Hately, Eurocontrol - CFMU, Belgium

Finance Co-chairs
Karel De Vlaminck, K.U. Leuven, Belgium
Marc Gobin, Royal Military Academy, Belgium

Local Organization Chair
Yolande Berbers, K.U. Leuven, Belgium

Organizing Board
Karel De Vlaminck, Dirk Craeynest, Yolande Berbers

Ada-Europe Conference Liaison
Alfred Strohmeier, Swiss Fed. Inst. of Technology Lausanne (EPFL), Switzerland

Advisory Board

Brad Balfour, Objective Interface, USA
Ben Brosgol, Ada Core Technologies, USA
Roderick Chapman, Praxis, UK
Robert Dewar, ACT, USA
Franco Gasperoni, ACT Europe, France
Ian Gilchrist, IPL Information Processing, UK
Mike Kamrad, Top Layer Networks, USA
Hubert B. Keller, Forschungszentrum Karlsruhe, Germany
Rudolf Landwehr, CCI, Germany
John Robinson, John Robinson & Associates, UK
Jean-Pierre Rosen, Adalog, France
Bill Taylor, Rational Software, UK
Theodor Tempelmeier, Rosenheim University of Applied Sciences, Germany
Joyce Tokar, DDC-I, USA
Andy Wellings, University of York, UK

Program Committee

Ángel Álvarez, Technical University of Madrid, Spain
Lars Asplund, Uppsala University, Sweden
Ted Baker, Florida State University, USA
Yvan Barbaix, K.U. Leuven, Belgium
Stéphane Barbey, Paranor AG, Switzerland
John Barnes, UK
Yolande Berbers, K.U. Leuven, Belgium
Luc Bernard, Offis nv/sa, Belgium
Guillem Bernat, University of York, UK
Johann Blieberger, Technical University of Vienna, Austria
Jim Briggs, University of Portsmouth, UK
Bernd Burgstaller, Technical University of Vienna, Austria
Alan Burns, University of York, UK
Agusti Canals, CS-SI, France
Ulf Cederling, Växsjö University, Sweden
Dirk Craeynest, Offis nv/sa & K.U. 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
Michael Feldman, George Washington University, USA
Jesús M. González-Barahona, Universidad Rey Juan Carlos, Spain
Michael González Harbour, Universidad de Cantabria, Spain
Gerhard Goos, University of Karlsruhe, Germany
Thomas Gruber, Austrian Research Centers, Austria
Helge Hagenauer, University of Salzburg, Austria
Günter Hommel, Technische Universität Berlin, Germany
Yvon Kermarrec, ENST Bretagne, France
Jörg Kienzle, Swiss Fed. Inst. of Technology Lausanne (EPFL), Switzerland
Fabrice Kordon, Université P.& M. Curie, France
Björn Källberg, SaabTech, Sweden
Albert Llamosí, Universitat de les Illes Balears, Spain
Kristina Lundqvist, Uppsala University, Sweden
Franco Mazzanti, Ist. di Elaborazione della Informazione, Italy
John W. McCormick, University of Northern Iowa, USA
Hugo Moen, Navia Aviation AS, Norway
Pierre Morere, Aonix, France
Paolo Panaroni, Intecs Sistemi, Italy
Laurent Pautet, ENST Paris University, France
Erhard Plödereder, University of Stuttgart, Germany
Ceri Reid, Coda Technologies, UK
Jean-Marie Rigaud, Université Paul Sabatier, France
Sergey Rybin, Moscow State University, Russia & ACT Europe, France

Edmond Schonberg, New York University & ACT, USA
Alfred Strohmeier, Swiss Fed. Inst. of Technology Lausanne (EPFL), Switzerland
Matthias Suilmann, CCI, Germany
Jan van Katwijk, Delft University of Technology, The Netherlands
Stef Van Vlierberghe, Offis nv/sa, Belgium
Tullio Vardanega, European Space Agency, The Netherlands
Ian Wild, Eurocontrol, Belgium
Jürgen Winkler, Friedrich-Schiller-Universität, Germany
Thomas Wolf, Paranor AG, Switzerland

Table of Contents

Invited Papers

Program Analysis

Distributed Systems

Real-Time Systems

Language and Patterns

Dependable Systems

APIs and Components

Real-Time Kernels

Standard Formats: UML & XML

System Evolution