Lecture Notes in Computer Science 2361
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

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

Johann Blieberger Alfred Strohmeier (Eds.)

Reliable Software Technologies – Ada-Europe 2002

7th Ada-Europe International Conference
on Reliable Software Technologies
Vienna, Austria, June 17-21, 2002
Proceedings

Springer

Series Editors

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

Volume Editors

Johann Blieberger
Technical University Vienna, Institute of Computer-Aided Automation
Treitlstraße 1-3, 1040 Vienna, Austria
E-mail: blieb@auto.tuwien.ac.at

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

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Reliable software technologies : proceedings / Ada Europe 2002, 7th Ada Europe International Conference on Reliable Software Technologies, Vienna, Austria, June 17 - 21, 2002. Johann Blieberger ; Alfred Strohmeier (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2361)
ISBN 3-540-43784-3

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

ISSN 0302-9743
ISBN 3-540-43784-3 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 Boller Mediendesign
Printed on acid-free paper SPIN: 10870279 06/3142 5 4 3 2 1 0

Foreword

The Seventh International Conference on Reliable Software Technologies, Ada-Europe 2002, took place in Vienna, Austria, June 17–21, 2002. 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 Technical University of Vienna.

The conference on Reliable Software Technologies provides the forum for researchers, developers, and users to share their research results, present tools, report on experiences, and discuss requirements that have recently arisen from the ever-changing application domains. 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 "Standard Container Libraries" was held. Further, the conference was accompanied by an exhibition where vendors presented their reliability-related products.

This year's conference had a specific focus on embedded systems which resulted in a special session. In addition, other sessions were related to embedded systems and several tutorials concentrated on problems and solutions for embedded systems.

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:

- Embedded Systems Unsuitable for Object Orientation
  Maarten Boasson, University of Amsterdam, The Netherlands
- On Architectural Stability and Evolution
  Mehdi Jazayeri, Technical University of Vienna, Austria
- Encapsulating Failure Detection: From Crash to Byzantine Failures
  Rachid Guerraoui, Swiss Federal Institute of Technology, Lausanne, Switzerland
- Contextware: Bridging Physical and Virtual Worlds
  Alois Ferscha, Universität Linz, Austria

We would like to express our sincere gratitude to the invited speakers, well-known to the community, for sharing their insights and information with the audience and for having written down 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 24 papers for inclusion in the proceedings, and one contribution for presentation only. The final result was a truly international program with authors from Australia, Austria, Belgium, Canada, China, France, Germany, Greece, Israel, Japan, Malaysia, The Netherlands, Portugal, Russia, Spain, Switzerland, the United Kingdom, and the USA, covering a broad range of software technologies: Embedded Systems, Distributed Systems, Real-Time Systems, OO Technology, Case Studies, Ada Language Issues, Tools, High Integrity Systems, Program Analysis, Libraries, APIs, and Bindings.

Tutorials

The tutorial program featured international experts presenting introductory and advanced material on a variety of subjects relevant to software engineers:

- SPARK, an "Intensive overview", *Peter Amey & Rod Chapman*
- MaRTE OS: Bringing Embedded Systems and RT POSIX Together, *Michael González Harbour & Mario Aldea*
- Principles of Physical Software Design in Ada 95, *Matthew Heaney*
- Implementing Design Patterns in Ada 95, *Matthew Heaney*
- CORBA 3 and CORBA for Embedded Systems, *S. Ron Oliver*
- Using Open Source Hardware and Software to Build Reliable Systems, *Joel Sherrill & Jiri Gaisler*
- Cleanroom Software Engineering: An Overview, *William Bail*
- Exceptions – What You Always Wanted to Know about Exceptions, But Were Afraid to Ask, *Currie Colket*

Workshop on Standard Container Libraries for Ada

At the initiative of Ehud Lamm a half day workshop was held on "Standard Container Libraries for Ada". Since both contemporary dominant general purpose programming languages, Java and C++, come equipped with a standard set of reusable containers, such as Maps and Sets, and since there are quite a few Ada libraries for these purposes, the need of standard container libraries for Ada was discussed.

There is little agreement on the exact details of a standard container library. There is however a general feeling, as could be witnessed during discussions on comp.lang.ada, that such a library is important for Ada's future. A standard container library is important for achieving many of Ada's goals, top among them the use of reusable components for efficient software engineering. Other important goals that can be served by a standard container library are educational

uses and efficient implementation of common algorithms and data structures, which is important for real-time systems. Designing a useful standard container library for Ada is a difficult task, as the language is used in a wide variety of different domains, with different and at times conflicting demands. Hence the need for debating and elaborating the issues among a group of interested Ada users.

The workshop was confined to container library issues, and did not address more general questions regarding the Ada standard library. The library designed is intended to be a collection of abstract data types, data structures (i.e., concrete data types), and common algorithms, useful for sequential programming. Possible candidates for inclusion in the library were judged according to this mission statement. Concurrent versions of the containers were considered to the extent that their inclusion does not interfere with the mission statement, either by complicating the design, or by imposing unacceptable run-time overhead.

Acknowledgments

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 Johann Blieberger, Bernd Burgstaller, Erhard Plödereder, Jean-Pierre Rosen, and Alfred Strohmeier met in Vienna 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 Ehud Lamm for organizing and holding the workshop.

We would also like to thank the members of the organizing committee. Gerhard H. Schildt and Johann Blieberger were in charge of the overall coordination and took care of all the clerical details for the successful running of the conference. Helge Hagenauer supervised the preparation of the attractive tutorial program. Thomas Gruber worked long hours contacting companies and people to prepare the conference exhibition. Bernd Burgstaller supported the paper submission and review process and together with Dirk Craeynest he created most of the brochures and the Advance and Final Program of the conference. Bernhard Scholz was a great help in finding sponsors and organizing social events.

Last but not least, we would like to express our appreciation to the authors of the papers submitted to the conference, and to all participants who helped to achieve the goal of the conference, to provide 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 7$^{\text{th}}$ International Conference on Reliable Software Technologies.

June 2002

Johann Blieberger
Alfred Strohmeier

Organizing Committee

Conference Chair
Gerhard H. Schildt, TU Vienna, Austria

Program Co-chairs
Johann Blieberger, TU Vienna, Austria
Alfred Strohmeier, Swiss Fed. Inst. of Technology Lausanne (EPFL), Switzerland

Tutorial Chair
Helge Hagenauer, University of Salzburg, Austria

Exhibition Chair
Thomas Gruber, ARC Seibersdorf research GmbH, Austria

Publicity Chair
Dirk Craeynest, Offis nv/sa & K.U.Leuven, Belgium

Local Organization Chair
Bernd Burgstaller, TU Vienna, Austria

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

Program Committee

Ángel Álvarez, Technical University of Madrid, Spain
Lars Asplund, Uppsala University, Sweden
Neil Audsley, University of York, UK
John Barnes, UK
Guillem Bernat, University of York, UK
Maarten Boasson, University of Amsterdam, The Netherlands
Ben Brosgol, ACT, USA
Bernd Burgstaller, TU Vienna, Austria
Ulf Cederling, Vaxjo University, Sweden
Roderick Chapman, Praxis Critical Systems Limited, UK
Paolo Coppola, INTECS HRT, Italy
Dirk Craeynest, Offis nv/sa & K.U.Leuven, Belgium
Alfons Crespo, Universidad Politécnica de Valencia, Spain
Peter Dencker, Aonix GmbH, Germany
Raymond Devillers, Université Libre de Bruxelles, Belgium
Brian Dobbing, Praxis Critical Systems Limited, UK
Wolfgang Gellerich, IBM, Germany

Jesús M. González-Barahona, ESCET, Universidad Rey Juan Carlos, Spain
Michael González Harbour, Universidad de Cantabria, Spain
Thomas Gruber, Austrian Research Centers Seibersdorf, Austria
Helge Hagenauer, University of Salzburg, Austria
Andrew Hately, Eurocontrol, Belgium
Günter Hommel, TU Berlin, Germany
Wolfgang Kastner, TU Vienna, Austria
Jan van Katwijk, Delft University of Technology, The Netherlands
Hubert B. Keller, Forschungszentrum Karlsruhe, Germany
Yvon Kermarrec, ENST Bretagne, France
Jörg Kienzle, Swiss Federal Institute of Technology Lausanne, Switzerland
Albert Llamosí, 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
Pierre Morere, Aonix, France
Laurent Pautet, ENST Paris, France
Erhard Plödereder, University Stuttgart, Germany
Juan A. de la Puente, Universidad Politécnica de Madrid, Spain
Gerhard Rabe, TÜV Nord e.V., Hamburg, Germany
Jean-Marie Rigaud, Université Paul Sabatier, Toulouse, France
Alexander Romanovsky, University of Newcastle, UK
Jean-Pierre Rosen, Adalog, France
Bo Sanden, Colorado Technical University, USA
Bernhard Scholz, TU Vienna, Austria
Edmond Schonberg, New York University & ACT, USA
Tullio Vardanega, Dept. of Pure and Applied Math., Univ. of Padova, Italy
Stef Van Vlierberghe, Eurocontrol CFMU, Belgium
Andy Wellings, University of York, UK
Ian Wild, Eurocontrol CFMU, Belgium
Jürgen Winkler, Friedrich-Schiller-Universität, Jena, Germany
Thomas Wolf, Paranor AG, Switzerland

Table of Contents

High-Integrity Systems

Ada Language

Program Analysis

Tools

Distributed Systems

Libraries, APIs, and Bindings

Object-Orientation