Lecture Notes in Computer Science 1622
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

Michael González Harbour
Juan A. de la Puente (Eds.)

Reliable Software Technologies – Ada-Europe '99

1999 Ada-Europe International Conference
on Reliable Software Technologies
Santander, Spain, June 7-11, 1999
Proceedings

Springer

Series Editors

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

Volume Editors

Michael González Harbour
Universidad de Cantabria, Facultad de Ciencias
Departamento de Electrónica y Computadores
Avda. de los Castros s/n, E-39005 Santander, Spain
E-mail: mgh@ctr.unican.es

Juan A. de la Puente
Universidad Politécnica de Madrid, ETSI Telecommunicacion
E-28040 Madrid, Spain
E-mail: jpuente@dit.upm.es

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Reliable software technologies : proceedings / Ada Europe '99, 1999 Ada Europe International Conference on Reliable Software Technologies, Santander, Spain, June 7 - 11, 1999. Michael González Harbour ; Juan A. de la Puente (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1622)
ISBN 3-540-66093-3

CR Subject Classification (1998): D.2, D.1.2-5, D.3, D.4, C.2.4, C.3, K.6

ISSN 0302-9743
ISBN 3-540-66093-3 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10705270 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Foreword

The Fourth International Conference on Reliable Software Technologies, Ada-Europe'99, took place in Santander, Spain, from June 7 to 11, 1999. It was sponsored by Ada-Europe, the European federation of national Ada societies, in cooperation with ACM SIGAda and Ada-Spain, and it was organized by members of the University of Cantabria and the Technical University of Madrid, in Spain. This was the 19th consecutive year of Ada-Europe conferences, which have always been the main Ada events in Europe, with their counterparts being the ACM SIGAda conferences in the USA (formerly Tri-Ada).

The conference is not just devoted to the Ada language, but rather to the more general area of reliable software technologies. In this sense, there are papers on formal methods, testing, software architectures and design, software engineering tools, etc. We believe that the role of reliable software technologies is becoming increasingly important, as computer applications control more and more of our everyday systems. The goal of our conference is to contribute to advancing the state of the art of all the technologies that help us in achieving better and more reliable software at a lower overall cost.

After the substantial revision that represented the Ada 95 standard, the Ada language is receiving renewed interest in many research institutes. One of the driving forces behind this interest is the availability of the free software GNAT compiler, as well as other free or low-cost compilers. The fact that researchers have the source code of the compiler and the run-time system available makes it possible for them to "play" with new language constructs, new run-time features, and new alternate implementations. Several of the papers presented at the conference go along these lines.

Certainly, the language is not only used for research. Industry experience with the Ada language is common in the areas where software reliability is a requirement. This typically, but not only, involves safety-critical systems such as aeroplane, train, or nuclear power station control systems. The recently developed Ravenscar Profile for safety-critical systems ---a set of restrictions on the tasking model that allows building certifiable run-time systems --- is receiving a lot of attention because it allows application programs running under Ada 95's tasking model to be used in systems with very stringent safety requirements. A few of the papers given at this conference discuss safety-critical systems and the role of the Ravenscar Profile.

There were also papers on industry's experience with Ada for application areas that are not safety critical at this conference. In these application areas, it is recognized that other languages such as C++ and, more recently, Java, receive much more attention from programmers and system developers. However, two factors seem to forecast an increase in the use of the Ada language in those areas. Firstly, as more and more systems become computer controlled, demand for reliable software is increasing. For example we need our mobile phones, TV sets, automobiles, etc., to work reliably; and they rely heavily on computers, and thus on software. Secondly, there are many academic institutions teaching Ada today. This has changed considerably over the last few years because of the low cost of Ada compilers now.

And for instructors and students the Ada language is just perfect for teaching and practising. As a first language, a Pascal-like subset of the language can be used; later, more in-depth concepts, such as abstraction, object-oriented programming, concurrent programming, real-time programming, etc., can be experienced using the same robust language that was learnt in the first place.

Experience with distributed systems programmed in Ada is also receiving increasing attention, since many more computer systems are distributed nowadays. In fact, the distributed systems section of this conference is one of the largest in number of papers. There are different approaches available to Ada programmers, who can choose to support distribution through operating system calls, by using middleware such as CORBA, or by using the language-defined Distributed Systems Annex. Papers presented to the conference explore all these possibilities. Also included in the conference are sections traditional to the Ada community such as real-time systems and fault tolerant systems.

This year, the conference included a special section on Hardware/Software Codesign. Although this topic has not been addressed in previous conferences, we thought that it would be interesting for this audience because there are several groups who are proposing Ada as a system-level specification language for hardware/software codesign. It is interesting for the Ada community to learn about these proposals because, if they get enough support, they may represent another important and expanding area in which the language may be used in the future.

The conference presented three distinguished invited speakers, who delivered state-of-the-art information on topics of great importance for now and for the future. Participation of one of the invited speakers had not been confirmed at the time this foreword was written; the other two invited speakers were:

- An Architectural Perspective of Real-Time Ada Applications
  C. Douglass Locke, Lockheed Martin Corporation
- The Evolving Architecture of GNAT
  Edmond Schonberg, New York University & Ada Core Technologies (ACT)

We are very proud to have been able to host these keynote speakers, and are very grateful to them for their efforts.

For this conference a large number of papers were submitted from 17 countries, almost doubling the paper submissions of previous years. The program committee worked hard to review all these papers and the paper selection process proved to be very difficult, since many papers had received excellent reviews. As a result of this process, the program committee selected 36 high quality papers covering a broad range of software technologies:

- Ravenscar Profile and High Integrity Systems
- Software Architectures and Design
- Testing
- Formal Methods

- Education
- Distributed Systems
- Real-Time Scheduling and Kernels
- Tools
- The Role of Ada in Hardware/Software Codesign
- Fault Tolerance
- Case Studies

The conference also included an interesting set of tutorials, featuring international experts who presented introductory and advanced material on reliable software technologies:

- Java for Ada Programmers
  Benjamin M. Brosgol
- Windows Development with Ada
  Orjan Leringe
- Software Interoperability: Principles and Practice
  Jack C. Wileden and Alan Kaplan
- Building Ada Development Tools: ASIS and other GNAT Technologies
  Cyrille Comar and Sergey I. Rybin
- MetaH -- An Architecture Description Language for Building Avionics Systems with Ada
  Bruce Lewis and Dennis Cornhill
- High Integrity Ada - The SPARK Approach
  John Barnes
- FUSION: An Object-Oriented Development Method, with Mapping to Ada
  Alfred Strohmeier
- Ada & Java: A Manager's and Developer's Road Map
  Franco Gasperoni and Gary Dismukes
- Using GNAT for the Java Platform
  Emmanuel Briot, Gary Dismukes and Franco Gasperoni

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, paper abstracts, and tutorial proposals submitted to the conference. A subcommittee formed by Lars Asplund, Johann Blieberger, Erhard Plödereder, Ángel Álvarez, and the program co-chairs met in Santander to make the final paper selection. Some program committee members were assigned to shepherd some of the papers. We are grateful to all of those who contributed to the technical program of the conference.

The work of the members of the organizing committee deserves a special mention. In particular, Ángel Álvarez, who together with John Barnes, Dirk Craeynest, and Stéphane Barbey prepared an extremely attractive tutorial program. Alejandro Alonso worked long hours contacting many companies and people to prepare the conference exhibition. And always helping the organizing committee was Alfred Strohmeier, Ada-Europe's Conference Liaison, who had good advice for us every time we needed it.

We also want to thank the people of the University of Cantabria for the work spent in the local organization. Special thanks to J. Javier Gutiérrez García, for publicising the conference by post and e-mail and by creating the conference Web page and preparing the brochure with the conference program. We also want to thank Mario Aldea Rivas, who worked many hours on the Web server that we used to manage the paper submission and revision process. This Web server was based on the Start Conference Manager, which was provided free of charge by Rich Gerber, and proved to be extremely useful and convenient.

Last but not least, we would like to thank all the authors who submitted their papers to the conference, and all the participants who helped in accomplishing the goals of the conference, providing a forum for the exchange of ideas between researchers and practitioners of reliable software technologies. We hope that they all enjoyed the technical program as well as the social events of the International Conference on Reliable Software Technologies.

March 1999 Michael González Harbour and Juan A. de la Puente

Organizing Committee

Conference Chair

Michael González Harbour, *Universidad de Cantabria, Spain*

Program Co-Chairs

Michael González Harbour, *Universidad de Cantabria, Spain*
Juan A. de la Puente, *Universidad Politécnica de Madrid*

Tutorial Chair

Ángel Álvarez, *Universidad Politécnica de Madrid*

Exhibition Chair

Alejandro Alonso, *Universidad Politécnica de Madrid*

Publicity Chair

J. Javier Gutiérrez García, *Universidad de Cantabria, Spain*

Ada-Europe Conference Liaison

Alfred Strohmeier, *Swiss Federal Institute of Technology in Lausanne*

Ada-Europe Board

John Barnes, *JBI*
Dirk Craeynest, *OFFIS nv/sa, Belgium*
Erhard Plödereder, *University of Stuttgart, Germany*
Björn Källberg, *CelsiusTech Systems AB*
Alfred Strohmeier, *Swiss Federal Institute of Technology in Lausanne*
Lars Asplund, *Uppsala University*
Michael González Harbour, *Universidad de Cantabria, Spain*

Program Committee

Ángel Álvarez, *Universidad Politécnica de Madrid*
Lars Asplund, *Uppsala University*
Paul A. Bailes, *The University of Queensland*
Ted Baker, *Florida State University*
Brad Balfour, *Objective Interface*
Stéphane Barbey, *Swiss Federal Institute of Technology, Lausanne*
John Barnes, *JBI*
Johann Blieberger, *Technical University Vienna*
Jim Briggs, *University of Portsmouth, UK*
Benjamin Brosgol, *Aonix*
Jorgen Bundgaard, *DDC-I*
Alan Burns, *University of York*
Dirk Craeynest, *OFFIS nv/sa, Belgium*
Alfons Crespo, *Universidad Politécnica de Valencia*
Peter Dencker, *Chairman of Ada-Deutschland*
Jesús González-Barahona, *Universidad Carlos III de Madrid*
Michael González Harbour, *Universidad de Cantabria*
Mike Kamrad, *BlazeNet*
Jan Van Katwijk, *Delft University of Technology*
Hubert B. Keller, *Forschungszentrum Karlsruhe*
Yvon Kermarrec, *ENST de Bretagne*
Fabrice Kordon, *Université P. & M. Curie*
Albert Llamosí, *Universitat de les Illes Balears*
Franco Mazzanti, *Istituto di Elaborazione della Informazione , CNR*
John McCormick, *University of Northern Iowa*
Paolo Panaroni, *Intecs Sistemi S.p.A.*
Laurent Pautet, *ENST Paris*
Juan A. de la Puente, *Universidad Politécnica de Madrid*
Erhard Plödereder, *University of Stuttgart, Germany*
Jean-Pierre Rosen, *ADALOG*
Sergey Rybin, *Moscow State University & ACT*
Edmond Schonberg, *New York University & ACT*
Andreas Schwald
Martin J. Stift, *Universität Wien*
Alfred Strohmeier, *Swiss Federal Institute of Technology, Lausanne*
Theodor Tempelmeier, *Rosenheim*
Stef Van Vlierberghe, *OFFIS N.V./S.A.*
Tullio Vardanega, *European Space Agency*
Andy Wellings, *University of York*

Table of Contents

Invited Paper

Ravenscar Profile and High Integrity Systems

Software Architectures and Design

Testing

Formal Methods

Education

Distributed Systems

Real-Time Scheduling and Kernels