Lecture Notes in Computer Science 7308

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Mats Brorsson Luís Miguel Pinho (Eds.)

Reliable Software Technologies – Ada-Europe 2012

17th Ada-Europe International Conference on Reliable Software Technologies
Stockholm, Sweden, June 11-15, 2012
Proceedings

Springer

Volume Editors

Mats Brorsson
KTH Royal Institute of Technology
Department of Software and Computer Systems
Forum 120, 164 40 Kista, Sweden
E-mail: matsbror@kth.se

Luís Miguel Pinho
Polytechnic Institute of Porto
CISTER Research Unit
Rua Dr. António Bernardino de Almeida, 431, 4200-072 Porto, Portugal
E-mail: lmp@isep.ipp.pt

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-30597-9 e-ISBN 978-3-642-30598-6
DOI 10.1007/978-3-642-30598-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012938027

CR Subject Classification (1998): D.3, D.2, F.3, C.2, H.4, C.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The 17th edition of the International Conference on Reliable Software Technologies – Ada-Europe 2012—took place during June 11–15, in the beautiful scenery of Stockholm, returning to Sweden for the second time in the series. The conference represents the main annual event promoted by Ada-Europe, this year jointly organized with Ada-Sweden, and in the largest ever cooperation with ACM (SIGAda, SIGBED and SIGPLAN). Previous editions of the conference were held in Switzerland (Montreux 1996 and Geneva 2007), the UK (London 1997, York 2005 and Edinburgh 2011), Sweden (Uppsala 1998), Spain (Santander 1999, Palma de Mallorca 2004 and Valencia 2010), Germany (Potsdam 2000), Belgium (Leuven 2001), Austria (Vienna 2002), France (Toulouse 2003 and Brest 2009), Portugal (Porto 2006), and Italy (Venice 2008).

The week included a three-day technical program, during which the peer-reviewed manuscripts contained in these proceedings were presented, bracketed by two tutorial days where participants had the opportunity to catch up on topics related to the conference focus. The technical program also included three invited talks and two panels, on topics related to the conference focus, and an industrial track, with contributions illustrating challenges faced and solutions adopted by industry. The conference was accompanied by an exhibition where vendors presented their products for reliable-software development, and by a special session, entitled "Ada in Motion," showing cases of Ada being used in moving equipment, such as Lego Mindstorms robots or Arduino-based devices.

An extensive program in an important and busy year for Ada, with the completion of the long and intense technical work for the specification of the new language revision and the launch of the formal process leading to official promulgation at ISO level.

A good number of technical papers were submitted, from as many as 16 different countries. The Program Committee worked hard to review them, and the selection process proved to be difficult, since many submissions had received excellent review marks. The final program was the result of this thorough selection process, with 15 submissions out of 34 being accepted for the conference. The industrial track of the conference also received excellent contributions, and the Industrial Committee selected nine of them for the conference.

The final result was a truly international program with contributions from Australia, Austria, Brazil, China, Denmark, Italy, Finland, France, Germany, Norway, Portugal, Spain, Switzerland, UK and USA, on a broad range of topics, such as application frameworks, modeling, testing and validation, real-time systems, the use of Ada for education, for safety or security and in application domains such as space and avionics.

The central days of the conference were opened by three distinguished speakers, who delivered state-of-the-art talks on topics of relevance to the conference:

- Bertrand Meyer (ETH Zurich, Switzerland), discussed the integration of design by contract techniques into a programming language, a topic well aligned with the Ada 2012 revision, in his talk entitled "Life with Contracts."
- Göran Backlund (Combitech, Sweden), provided insights into the role of human knowledge in the software development process, in a talk entitled "What Is the Mission of a Software Developer?"
- Jean-Loup Terraillon, (ESTEC/ESA, The Netherlands), presented the European Space Agency roadmap on multicore architectures, in a talk entitled "Multicore Processors—The Next-Generation Computer for ESA Space Missions."

We would like to express our sincere gratitude to these distinguished speakers for sharing their insights with the conference participants.

The conference program also included two panels on the topics of "What Is Language Technology in Our Time?" and "Reliable Software, a Perspective from Industry."

It is not a coincidence that marking the completion of the Ada 2012 revision, the conference discussed what is nowadays expected from language technology. In this panel, a group of experts and the audience discussed whether more than a language (in the traditional sense) is currently needed, and if focus should also be given to methodologies, tools, libraries, patterns and frameworks. The panel was moderated by Tullio Vardanega (University of Padua), with Bertrand Meyer (Chief Architect of Eiffel Software), Franco Gasperoni (co-founder of AdaCore), Erhard Plödereder (educator and researcher in software engineering) and José María Martínez (Software Engineering Manager at Cassidian) as panelists.

As a forum that aims to connect academic with industrial knowledge and experience, the second panel discussed the most pressing and challenging industrial needs in the way of software technology to facilitate the production of reliable software. Issues such as quality and safety standards, life-cycle models, processes, methods and techniques, languages and tools were debated. This panel was moderated by Jørgen Bundgaard (Rovsing A/S), with Ana Rodríguez (GMV), Mike Rennie (Deimos Space) and João Brito (Critical Software) as panelists.

Also with the goal to connect academia and industry around reliable software technologies, the conference included an interesting series of Industrial Presentations whose proceedings will appear in forthcoming issues of Ada-Europe's *Ada User Journal*. That part of the conference program included:

- "Using an Ada/Firmware Co-design to Emulate an Obsolete Processor," by Rod White (MBDA Ltd, UK)
- "A Portfolio Model for Natural Catastrophe Reinsurance—Experience Using Ada and the GNAT Programming Environment," by Gautier de Montmollin (Partner Reinsurance, Switzerland)
- "Development of Controller Pilot Automatic Data Communication (Data Comm) System," by Alok Srivastava (TASC Inc., USA) and Jeff O' Leary (FAA, USA)

- "ATV Flight Application Software Command Checker," by Jørgen Bundgaard (Rovsing A/S, Denmark)
- "Use of Model-Driven Code Generation on the ASIM Project," by Steen Palm (Terma A/S, Denmark)
- "Including Hardware/Software Co-design in the ASSERT Model-Driven Engineering Process," by Francisco Ferrero (GMV, Spain), Elena Alaa (GMV, Spain), Ana I. Rodrguez (GMV, Spain), Juan Zamorano (Universidad Politécnica de Madrid, Spain) and Juan A. de la Puente (Universidad Politécnica de Madrid, Spain)
- "Tool Support for Verification of Software Timing and Stack Usage for DO-178B Level A System," by Felipe Kamei (Embraer, Brazil), Daniela Cristina Carta (Embraer, Brazil) and Ian Broster (Rapita Systems Ltd, UK)
- "Combining Ada Generics and Code Generation to Implement a Software Product Line," by Richard Bridges (Eurocopter Deutschland GmbH, Germany), Frank Dordowsky (ESG Elektroniksystem- und Logistik-GmbH, Germany) and Holger Tschöpe (Eurocopter Deutschland GmbH, Germany)
- "Modernising Legacy Applications," by Derek Russell (Objektum Solutions Ltd, UK) and Catherine Robson (Objektum Solutions Ltd, UK)

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

- "Advanced Ada Support for Real-Time Programming," by Mario Aldea Rivas (Universidad de Cantabria, Spain)
- "Developing High-Integrity Systems with GNAT GPL and the Ravenscar Profile," by Juan A. de la Puente and Juan Zamorano (Universidad Politécnica de Madrid, Spain)
- "How to Optimize Reliable Software," by Ian Broster and Andrew Coombes (Rapita Systems Ltd, UK)
- "DO-178C: The Next Avionics Software Safety Standard," by Ben Brosgol (AdaCore, USA)
- "Designing and Checking Coding Standards for Ada," by Jean-Pierre Rosen (Adalog, France)
- "Experimenting with ParaSail – Parallel Specification and Implementation Language," by Tucker Taft (SofCheck div. of AdaCore, USA)
- "Basics of Oracle Database Programming with Ada: Introduction to the Konada.Db Library" and "Oracle Database GUI-Programming on MS Windows," by Frank Piron (KonAd GmbH, Germany)
- "The Benefits of Using SPARK for High-Assurance Software" and "The Use of Proof and Generics in SPARK," by Trevor Jennings and Robin Messer (Altran Praxis, UK)
- "Design of Multitask Software: The Entity-Life Modeling Approach," by Bo Sandén (Colorado Technical University, USA)

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

presentations and tutorial proposals submitted to the conference. A committee comprising Ahlan Marriott, Albert Llemosí, Dirk Craeynest, Jørgen Bundgaard, Luís Miguel Pinho, Mats Brorsson and Tullio Vardanega met in Stockholm to make the final program selection. Several Program Committee members were required to shepherd some of the papers. We are grateful to all those who contributed to the technical program of the conference.

We would also like to thank the members of the Organizing Committee, for their valuable effort in taking care of all the bits and pieces that must fit together for a smooth run of the conference: Ahlan Marriott, Conference Chair, orchestrating the different components of the conference; Jørgen Bundgaard for the effort on the preparation of the industrial track; Albert Llemosí for the excellent tutorial program; Dirk Craeynest, who worked very hard to make the conference prominently visible; and Rei Stråhle, who took care of all details of the local organization. We would also like to thank all the members of the Ada-Europe board for helping with the intricate details of the organization. Also, Filipe Pacheco for building the conference website and registration system.

Finally, we would like to express our appreciation to the authors of the high-quality contributions submitted to the conference, and to all the participants who helped in achieving the primary goal of the conference: providing a forum for researchers and practitioners to exchange information and ideas about Ada and reliable software technologies. We hope they all enjoyed the program as well as the social events of the 17$^{\text{th}}$ International Conference on Reliable Software Technologies – Ada-Europe 2012.

June 2012

Mats Brorsson
Luís Miguel Pinho

Organization

The 17th International Conference on Reliable Software Technologies – Ada-Europe 2012—was organized by Ada-Europe and Ada-Sweden, in cooperation with ACM (SIGAda, SIGBED and SIGPLAN).

Organizing Committee

Conference Chair

Ahlan Marriott	White Elephant GmbH, Switzerland

Program Co-chairs

Mats Brorsson	KTH Royal Institute of Technology, Sweden
Luís Miguel Pinho	CISTER Research Centre/ISEP, Portugal

Tutorial Chair

Albert Llemosí	Universitat de les Illes Balears, Spain

Industrial Chair

Jørgen Bundgaard	Rovsing A/S, Denmark

Publicity Chair

Dirk Craeynest	Aubay Belgium & K.U.Leuven, Belgium

Local Chair

Rei Stråhle	Ada-Sweden

Program Committee

Ted Baker
Johann Blieberger
Mats Brorsson
Jørgen Bundgaard
Bernd Burgstaller
Alan Burns
Dirk Craeynest
Alfons Crespo
Michael González Harbour
José Javier Gutiérrez
Peter Hermann
Jérôme Hugues
Jan Jonsson
Albert Llemosí
Kristina Lundqvist
Franco Mazzanti
Julio Medina
Jürgen Mottok
John McCormick
Stephen Michell
Laurent Pautet
Luís Miguel Pinho
Erhard Plödereder

Juan A. de la Puente
Jorge Real
José Ruiz
Sergio Sáez
Ed Schonberg
Theodor Tempelmeier
Elena Troubitsyna
Santiago Urueña
Tullio Vardanega
Juan Zamorano

Industrial Committee

Jamie Ayre
Ian Broster
Jørgen Bundgaard
Rod Chapman
Dirk Craeynest
Hubert Keller
Ismael Lafoz
Ahlan Marriott
Paolo Panaroni
Paul Parkinson
Jean-Pierre Rosen
Alok Srivastava
Jean-Loup Terraillon
Erik Wedin
Rod White

External Reviewers

Gøran Bertheau
Néstor Cataño
Etienne Borde
Linas Laibinis
Risat Pathan
Robert Pathan
Kristian Wiklund

Supporting Organizations

The organizers of the conference are grateful to the exhibitors and supporters of the conference.

Exhibitors, at the time of writing:
AdaCore
Altran Praxis
Ellidiss Software
Rapita Systems Ltd
Vector Software Inc
Objektum Solutions

Supporters, at the time of writing:
Siemens Switzerland
KonAd GmbH

Table of Contents

Application Frameworks

Use of Ada

Modeling

Testing and Validation

Real-Time Systems