Lecture Notes in Computer Science 6106

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

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Alfred Kobsa
University of California, Irvine, CA, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
TU Dortmund University, Germany

Madhu Sudan
Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Jorge Real Tullio Vardanega (Eds.)

Reliable Software Technologies – Ada-Europe 2010

15th Ada-Europe International Conference
on Reliable Software Technologies
Valencia, Spain, June 14-18, 2010
Proceedings

Springer

Volume Editors

Jorge Real
Universidad Politécnica de Valencia, DISCA-ETSINF
Camino de Vera s/n, 46022 Valencia, Spain
E-mail: jorge@disca.upv.es

Tullio Vardanega
University of Padua, Department of Pure and Applied Mathematics
Via Trieste 63, 35121 Padua, Italy
E-mail: tullio.vardanega@math.unipd.it

Library of Congress Control Number: 2010927689

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-642-13549-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-13549-1 Springer 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. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

The 15th edition of the International Conference on Reliable Software Technologies – Ada-Europe 2010—took place in the attractive venue of Valencia, deservedly making Spain the most visited country in the conference series. Previous editions of the conference were held in Switzerland (Montreux 1996 and Geneva 2007), United Kingdom (London 1997 and York 2005), Sweden (Uppsala 1998), Spain (Santander 1999 and Palma de Mallorca 2004), Germany (Potsdam 2000), Belgium (Leuven 2001), Austria (Vienna 2002), France (Toulouse 2003 and Brest 2009), Portugal (Porto 2006), and Italy (Venice 2008).

The conference represents the main yearly event promoted by Ada-Europe, in cooperation with ACM SIGAda. This third visit to Spain acknowledges the fact that Ada-Spain is the largest national association of Ada-Europe, and is a major contributor to Ada-Europe's activities. This year the conference was organized by members of the Instituto de Automática e Informática Industrial (AI2) and the Departamento de Informática de Sistemas y Computadores (DISCA) of the Universidad Politécnica de Valencia.

The year 2010 is important for Ada: this is the year when the new amendment to the language (known as Ada 2012) is taking its definitive shape. The conference program was not unaware of this fact, and these proceedings reflect it by including papers about multicore programming in Ada, along with an overview of the key elements of the Ada 2012 amendment in the making.

The scientific program of the conference, which feeds these proceedings, also included sessions devoted to software dependability, critical, real-time and distributed systems, and language technology, all under the more general heading of "Reliable Software Technologies." This program is the result of a thorough selection process of 17 submissions out of 42 received from authors of 19 different countries.

The conference was enriched with three keynote talks delivered by prestigious speakers, whose insightful contributions opened the central days of the conference:

- Theodore Baker (Florida State University, USA), a long-time contributor to Ada and a leading researcher in real-time systems, opened the conference by reviewing the state of the art in multiprocessor real-time scheduling in his talk entitled "What to Make of Multicore Processors for Reliable Real-Time Systems?"
- Pedro Albertos (Universidad Politécnica de Valencia, Spain), a leading figure of the automatic control community, explored the relationship between implementation and performance of control algorithms in a talk entitled "Control Co-design: Algorithms and Their Implementation"
- James Sutton (Lockheed Martin, USA), a worldwide expert software architect, in his talk "Ada: Made for the 3.0 World," analyzed the fitness of Ada

for the so-called 3.0 World, where complexity and chaos are appeased, and both can be used to the user's advantage.

These proceedings give account of the first two keynote talks by including papers contributed by their respective authors. Both papers appear in the "Keynote Talks" section.

As a forum that aims to connect academic with industrial knowledge and experience around reliable software technologies, the conference also 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:

- "HRT-UML and Ada Ravenscar Profile: A Methodological Approach to the Design of Level-B Spacecraft Software," by R. López, A. I. Rodríguez from GMV, Spain
- "Applying Model-Driven Architecture and SPARK Ada – A SPARK Ada Model Compiler for xtUML," by E. Wedin from Saab, Sweden
- "Ada 95 Usage Within the Airbus Military Advanced Refuelling Boom System," by I. Lafoz from Airbus Military, Spain
- "Ada 95 Usage Within the Airbus Military Generic Test Environment System," by B. Lozano from Airbus Military, Spain
- "Implementing Polymorphic Callbacks for Ada/C++ Bindings," by M. Sobczak from CERN, Switzerland
- "A Reusable Work Seeking Parallel Framework for Ada 2005," by B. Moore from General Dynamics Canada
- "Database Programming with Ada," by F. Piron from KonAd GmbH, Germany
- "Future Enhancements to the U.S. FAA's En-Route Automation Modernization (ERAM) Program and the Next Generation Air Transportation System (NextGen)," by J. O'Leary from FAA, USA, and A. Srivastava from Northrop Grumman IT, USA
- "System Architecture Virtual Integration Case Study," by B. Lewis from U.S. Army Aviation and Missile Command, USA
- "Lessons Learned from the First High Assurance (EAL 6+) Common Criteria Software Certification," by D. Kleidermacher from Greenhills Software, USA
- "An Introduction to ParaSail: Parallel Specification and Implementation Language," by S. T. Taft from SofCheck, USA

The conference also scheduled a series of tutorials that, once more, gave participants the opportunity to learn about particular approaches, techniques and tools aimed at the development of reliable software. The program was formed by the following nine tutorials, all given by recognized experts in the relevant areas:

- "Developing High-Integrity Systems with GNATforLEON/ORK+," by J. A. de la Puente and J. Zamorano from the Technical University of Madrid, Spain

- "Software Design Concepts and Pitfalls," by W. Bail from The MITRE Corporation, USA
- "Using Object-Oriented Technologies in Secure Systems," by J.P. Rosen from Adalog, France
- "Hypervisor Technology for Building Safety-Critical Systems: XtratuM," by I. Ripoll and A. Crespo from Universidad Politécnica de Valencia, Spain
- "How to Optimize Reliable Software," by I. Broster from Rapita Systems Ltd, UK
- "Developing Web-Aware Applications in Ada with AWS," by J.P. Rosen from Adalog, France
- "MAST: Predicting Response Times in Event-Driven Real-Time Systems," by M. González Harbour from University of Cantabria, Spain
- "SPARK: The Libre Language and Toolset for High-Assurance Software," by R. Chapman from Altran Praxis Ltd, UK
- "C#, .NET and Ada: Keeping the Faith in a Language-Agnostic Environment," by B. Brosgol and J. Lambourgh from AdaCore, USA and France

The conference success heavily depended on the active and generous contribution of a number of individuals and organizations. All of them deserve our most sincere gratitude. We especially thank all who submitted quality contributions that enabled us to offer an attractive and technically sound program. Of course we are most grateful to all attendees, who made the conference thrive. The Organizing Committee was formed by Albert Llemosí, Tutorial Chair, who conjured a high-quality tutorial program; Erhard Plödereder, Industrial Chair, who coordinated the elaboration of the industrial program; Ahlan Marriott in his role as Exhibition Chair; and Dirk Craeynest, serving as Publicity Chair. The members of this committee met with the Program Co-chairs in Valencia to make the final program selection and composition.

The organizers are also grateful to the members of the Local Organizing Committee at the Universidad Politécnica de Valencia, Francisco Blanes, Sergio Sáez, and José Simó. The Program and Industrial Committees did a splendid job at raising submissions and providing quality reviews that aided in the difficult task of eliciting the final contents of the conference. Last but not least, we wish to express our gratitude to the exhibitors at the conference, at the time of writing: AdaCore, Altran Praxis, Atego and Ellidiss; and the sponsors: Ministerio de Ciencia e Innovación of the Spanish Government, Consellería d'Educació of the Generalitat Valenciana, Universidad Politécnica de Valencia and its entities Departamento de Informática de Sistemas y Computadores, Escuela Técnica Superior de Ingeniería Informática, and Instituto de Automática e Informática Industrial.

June 2010

Jorge Real
Tullio Vardanega

Organization

The 15th International Conference on Reliable Software Technologies – Ada-Europe 2010—was organized by Ada-Europe and Universidad Politécnica de Valencia, in cooperation with ACM SIGAda.

Organizing Committee

Conference Chair:	Jorge Real (Universidad Politécnica de Valencia, Spain)
Program Co-chairs:	Jorge Real (Universidad Politécnica de Valencia, Spain) Tullio Vardanega (Università di Padova, Italy)
Tutorial Chair:	Albert Llemosí (Universitat de les Illes Balears, Spain)
Industrial Chair:	Erhard Plödereder (Universität Stuttgart, Germany)
Exhibition Chair:	Ahlan Marriott (White Elephant GmbH, Switzerland)
Publicity Chair:	Dirk Craeynest (Aubay Belgium & K.U.Leuven, Belgium)

Program Committee

Alejandro Alonso
Ted Baker
John Barnes
Johann Blieberger
Jørgen Bundgaard
Bernd Burgstaller
Alan Burns
Rod Chapman
Dirk Craeynest
Alfons Crespo
Juan A. de la Puente
Raymond Devillers
Franco Gasperoni
Michael González Harbour
José-Javier Gutiérrez
Andrew Hately
Peter Hermann
Jérôme Hugues
Hubert Keller
Albert Llemosí
Kristina Lundqvist
Franco Mazzanti
John McCormick
Julio Medina
Stephen Michell
Javier Miranda
Daniel Moldt
Laurent Pautet
Luís Miguel Pinho
Erhard Plödereder
Jorge Real
Alexander Romanovsky
Jean-Pierre Rosen
Ed Schonberg
Sergio Sáez
Theodor Tempelmeier
Jean-Loup Terraillon
Santiago Urueña
Tullio Vardanega
Francois Vernadat
Andy Wellings
Daniel Wengelin
Jürgen Winkler
Luigi Zaffalon

External Reviewers

Björn Andersson
Etienne Borde
Pierre-Emmanuel Hladik
Didier Le Botlan
Ilya Lopatkin
Yannick Moy
Florent Peres
Jose Quenum
José Ruiz
Jayakanth Srinivasan
Thomas Wagner

Sponsoring Institutions

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

Exhibitors, at the time of writing:
AdaCore
Altran Praxis
Atego
Ellidiss Software

Sponsors:
Ministerio de Ciencia e Innovación, Spanish Government (project TIN2009-06669-E)
Consellería d'Educació, Generalitat Valenciana
Universidad Politécnica de Valencia (program PAID-03-09)
Departamento de Informática de Sistemas y Computadores, UPV
Escuela Técnica Superior de Ingeniería Informática, UPV
Instituto de Automática e Informática Industrial, UPV

Table of Contents

Keynote Talks

What to Make of Multicore Processors for Reliable Real-Time Systems? 1
Theodore P. Baker

Control Co-design: Algorithms and Their Implementation 19
Pedro Albertos, Alfons Crespo, José Simó, and Adel Fernández

Multicores and Ada

Dispatching Domains for Multiprocessor Platforms and Their Representation in Ada 41
Alan Burns and Andy Wellings

Implementing Multicore Real-Time Scheduling Algorithms Based on Task Splitting Using Ada 2012 54
Björn Andersson and Luís-Miguel Pinho

Preliminary Multiprocessor Support of Ada 2012 in GNU/Linux Systems 68
Sergio Sáez and Alfons Crespo

Software Dependability

Practical Limits on Software Dependability: A Case Study 83
Patrick J. Graydon, John C. Knight, and Xiang Yin

Program Verification in SPARK and ACSL: A Comparative Case Study 97
Eduardo Brito and Jorge Sousa Pinto

Static Versioning of Global State for Race Condition Detection 111
Steffen Keul

Critical Systems

Using Hardware Support for Scheduling with Ada 125
Rod White

Cache-Aware Development of High-Integrity Systems 139
Enrico Mezzetti, Adam Betts, José Ruiz, and Tullio Vardanega

Preservation of Timing Properties with the Ada Ravenscar Profile 153
Enrico Mezzetti, Marco Panunzio, and Tullio Vardanega

Real-Time Systems

Towards the Definition of a Pattern Sequence for Real-Time Applications Using a Model-Driven Engineering Approach 167
Juan Ángel Pastor, Diego Alonso, Pedro Sánchez, and Bárbara Álvarez

Scheduling Configuration of Real-Time Component-Based Applications 181
Patricia López Martínez, Laura Barros, and José M. Drake

The Evolution of Real-Time Programming Revisited: Programming the Giotto Model in Ada 2005 196
Andy Wellings and Alan Burns

Language Technology

AdaStreams: A Type-Based Programming Extension for Stream-Parallelism with Ada 2005 208
Gingun Hong, Kirak Hong, Bernd Burgstaller, and Johann Blieberger

A Comparison of Generic Template Support: Ada, C++, C#, and Java™ 222
Benjamin M. Brosgol

Towards Ada 2012: An Interim Report 238
Edmond Schonberg

Distribution and Persistency

Managing Transactions in Flexible Distributed Real-Time Systems 251
Daniel Sangorrín, Michael González Harbour, Héctor Pérez, and J. Javier Gutiérrez

An Efficient Implementation of Persistent Objects 265
Jacob Sparre Andersen

Author Index 277