Lecture Notes in Computer Science 4498

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

Nabil Abdennadher Fabrice Kordon (Eds.)

Reliable Software Technologies – Ada-Europe 2007

12th Ada-Europe International Conference
on Reliable Software Technologies
Geneva, Switzerland, June 25-29, 2007
Proceedings

Springer

Volume Editors

Nabil Abdennadher
University of Applied Sciences Western Switzerland, HES.SO
École d'ingénieurs de Genève
Rue de la Prairie 4, 1202 Geneva, Switzerland
E-mail: Nabil.Abdennadher@hesge.ch

Fabrice Kordon
Université Pierre et Marie Curie
Laboratoire d'Informatique de Paris 6
104 Avenue du Président Kennedy, 75016 Paris, France
E-mail: Fabrice.Kordon@lip6.fr

Library of Congress Control Number: 2007929319

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-73229-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73229-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12080861 06/3180 5 4 3 2 1 0

Preface

Reliable Software Technologies is an annual series of international conferences devoted to the promotion and advancement of all aspects of reliable software technologies. The objective of this series of conferences, initiated and sponsored by Ada-Europe, the European federation of national Ada societies, is to provide a forum to promote the development of reliable softwares both as an industrial technique and an academic discipline.

Previous editions of the Reliable Software Technologies conference were held in: Porto (Portugal) in 2006, York (UK) in 2005, Palma de Mallorca (Spain) in 2004, Toulouse (France) in 2003, Vienna (Austria) in 2002, Leuven (Belgium) in 2001, Potsdam (Germany) in 2000, Santander (Spain) in 1999, Uppsala (Sweden) in 1998, London (UK) in 1997 and Montreux (Switzerland) in 1996.

The 12th International Conference on Reliable Software Technologies took place in Geneva, Switzerland, June 25-29, 2007, under the continued sponsoring of Ada-Europe, in cooperation with ACM SIGAda. It was organized by members of the University of Applied Sciences, Western Switzerland (Engineering School of Geneva), in collaboration with colleagues from various places in Europe. The 13th conference, in 2008, will take place in Venice, Italy.

Continuing the success achieved in previous years, the conference included a three-day technical program, where the papers contained in these proceedings were presented. The technical program was bracketed by two tutorial days where attendants had the opportunity to catch up on a variety of topics related to the fields covered by the conference, at both introductory and advanced levels. The technical program also included an industrial track, with contributions illustrating challenges faced and solutions devised by industry from both sides of the Atlantic, as well as from the rest of the world (we note several contributions from South-East Asia). Furthermore, the conference was accompanied by an exhibition where vendors presented their products for supporting the development of reliable software.

The conference featured four distinguished speakers, who delivered state-of-the-art information on topics of great importance, both for the present and the future of software engineering:

- Challenges for Reliable Software Design in Automotive Electronic Control Units *by Klaus D. Mueller-Glaser (University of Karlsruhe, Germany)*
- Synchronous Techniques for Embedded Systems *by Gerard Berry (Esterel Technologies, France)*
- Perspectives on Next-Generation Software Engineering *by Ali Mili (New Jersey Institute of Technology, USA)*
- Observation Rooms for Program Execution Monitoring *by Liviu Iftode, (Rutgers University, USA)*

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

A large number of regular papers were submitted, from as many as 15 different countries. The Program Committee worked hard to review them, and the selection process proved to be difficult, since many papers had received excellent reviews. The Program Committee eventually selected 18 papers for the conference and these proceedings.

The industrial track of the conference also received valuable contributions from industry, and the Industrial Committee selected nine of them for presentation in Geneva. The final result was a truly international program with contributions from Australia, Austria, China, France, Germany, Italy, Republic of Korea, Spain, Tunisia, and the UK, covering a broad range of topics: real-time systems, static analysis, verification, applications, reliability, industrial experience, compilers and distributed systems.

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

- An Overview of Model-Driven Engineering, *William Bail*
- CbyC: A UML2 Profile Enforcing the Ravsenscar Computational Model, *Tullio Vardanega*
- Verification and Validation for Reliable Software Systems, *William Bail*
- Object-Oriented Programming in Ada 2005, *Matthew Heaney*
- Security by Construction, *Rod Chapman*
- Synchronous Design of Embedded Systems: the Esterel/Scade Approach, *Gerard Berry*
- Building Interoperable Applications with PolyORB, *Thomas Quinot and Jérôme Hugues*
- Situational Method Engineering: Towards a Specific Method for Each System Development Project, *Jolita Ralyté*

We wish to extend our gratitude to these experts for the work they put into preparing and presenting this material during the conference.

The 12th Reliable Software Technologies (Ada-Europe 2007) conference was made possible through the generous support and diligent work of many individuals and organizations. A number of institutional and industrial sponsors also made important contributions and participated in the industrial exhibition. Their names and logos appear on the Ada-Europe 2007 Web site.We gratefully acknowledge their support. A subcommittee comprising Nabil Abdennadher, Dirk Craeynest, Fabrice Kordon, Dominik Madon, Ahlan Marriott, Tullio Vardanega and Luigi Zaffalon met in Geneva to elaborate the final program selection. Various 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.

We would like to thank the members of the Organizing Committee for their valuable effort in taking care of all the details needed for a smooth run of the

conference. Dominik Madon did a superb job in organizing an attractive tutorial program. Luigi Zaffalon took on the difficult task of preparing the industrial track. We would also like to thank Dirk Craeynest and Ahlan Marriott, who worked very hard to make the conference prominently visible, and to all the members of the Ada-Europe board for helping with the intricate details of the organization. Special thanks go to Régis Boesch and Albena Basset, who took care of all details of the local organization.

Finally, we also thank the authors of the contributions submitted to the conference, and to all the participants who helped in achieving 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 program as well as the social events of the 12th International Conference on Reliable Software Technologies.

June 2007

Nabil Abdennadher
Fabrice Kordon

Organization

Conference Chair

Nabil Abdennadher, University of Applied Sciences, Geneva, Switzerland

Program Co-chairs

Nabil Abdennadher, University of Applied Sciences, Geneva, Switzerland
Fabrice Kordon, Université Pierre & Marie Curie, Paris, France

Industrial Committee Chair

Luigi Zaffalon, University of Applied Sciences, Geneva, Switzerland

Tutorial Chair

Dominik Madon, University of Applied Sciences, Geneva, Switzerland

Exhibition Chair

Neville Rowden, Siemens Switzerland

Publicity Co-chairs

Ahlan Marriott, White-elephant, Switzerland
Dirk Craeynest, Aubay Belgium and K.U.Leuven, Belgium

Local Chair

Régis Boesch, University of Applied Sciences, Geneva, Switzerland

Ada-Europe Conference Liaison

Fabrice Kordon, Université Pierre et Marie Curie, Paris, France

Program Committee

Abdennadher Nabil, University of Applied Sciences, Geneva, Switzerland
Alonso Alejandro, Universidad Politécnica de Madrid, Spain
Asplund Lars, Mälardalens Högskola, Sweden
Barnes Janet, Praxis High Integrity Systems, UK

Blieberger Johann, Technische Universität Wien, Austria
Boasson Maartin, University of Amsterdam, The Netherlands
Burgstaller Bernd, University of Sydney, Australia
Craeynest Dirk, Aubay Belgium and K.U.Leuven, Belgium
Crespo Alfons, Universidad Politécnica de Valencia, Spain
Devillers Raymond, Université Libre de Bruxelles, Belgium
González Harbour Michael, Universidad de Cantabria, Spain
Gutiérrez José Javier, Universidad de Cantabria, Spain
Hadded Serge, Université Paris-Dauphine, France
Hately Andrew, Eurocontrol CRDS, Hungary
Hommel Günter, Technische Universität Berlin, Germany
Keller Hubert, Institut für Angewandte Informatik, Germany
Kermarrec Yvon, ENST Bretagne, France
Kienzle Jörg, McGill University, Canada
Kordon Fabrice, Université Pierre et Marie Curie, France
Llamosi Albert, Universitat de les Illes Balears, Spain
Lundqvist Kristina, MIT, USA
Mazzanti Franco, ISTI-CNR Pisa, Italy
McCormick John, University of Northern Iowa, USA
Michell Stephen, Maurya Software, Canada
Miranda Javier, Universidad Las Palmas de Gran Canaria, Spain
Moldt Daniel, University of Hamburg, Germany
Pautet Laurent, Telecom Paris, France
Petrucci Laure, LIPN, Université Paris 13, France
Pinho Luís Miguel, Polytechnic Institute of Porto, Portugal
Plödereder Erhard, Universität Stuttgart, Germany
de la Puente Juan A., Universidad Politécnica de Madrid, Spain
Real Jorge, Universidad Politécnica de Valencia, Spain
Romanovsky Alexander, University of Newcastle upon Tyne, UK
Rosen Jean-Pierre, Adalog, France
Ruiz José, AdaCore, France
Schonberg Edmond, New York University and AdaCore, USA
Seinturier Lionel, INRIA Lille, France
Shing Man-Tak, Naval Postgraduate School, USA
Tokar Joyce, Pyrrhus Software, USA
Vardanega Tullio, Università di Padova, Italy
Wellings Andy, University of York, UK
Winkler Jürgen, Friedrich-Schiller-Universität, Germany
Zaffalon Luigi, University of Applied Sciences, Geneva, Switzerland

Sponsoring Institutions

Ada-Europe
AdaCore
Aonix
Ellidiss Sowftare
Green Hills Software Inc.
Praxis

PostFinance
Sun Microsystems
Siemens
Telelogic

Fédération des Entreprises Romandes
Swiss Informatics Society
The Quality Software Foundation

Table of Contents

Real-Time Utilities for Ada 2005 1
Andy Wellings and Alan Burns

Handling Temporal Faults in Ada 2005 15
José A. Pulido, Santiago Urueña, Juan Zamorano, and Juan A. de la Puente

Implementation of New Ada 2005 Real-Time Services in MaRTE OS and GNAT 29
Mario Aldea Rivas and José F. Ruiz

Enhancing Dependability of Component-Based Systems 41
Arnaud Lanoix, Denis Hatebur, Maritta Heisel, and Jeanine Souquières

On Detecting Double Literal Faults in Boolean Expressions 55
Man F. Lau, Ying Liu, Tsong Y. Chen, and Yuen T. Yu

Static Detection of Livelocks in Ada Multitasking Programs 69
Johann Blieberger, Bernd Burgstaller, and Robert Mittermayr

Towards the Testing of Power-Aware Software Applications for Wireless Sensor Networks 84
W.K. Chan, Tsong Y. Chen, S.C. Cheung, T.H. Tse, and Zhenyu Zhang

An Intermediate Representation Approach to Reducing Test Suites for Retargeted Compilers 100
Gyun Woo, Heung Seok Chae, and Hanil Jang

Correctness by Construction for High-Integrity Real-Time Systems: A Metamodel-Driven Approach 114
Matteo Bordin and Tullio Vardanega

A Metamodel-Driven Process Featuring Advanced Model-Based Timing Analysis 128
Marco Panunzio and Tullio Vardanega

ArchMDE Approach for the Development of Embedded Real Time Systems 142
Nourchène Elleuch, Adel Khalfallah, and Samir Ben Ahmed

Generating Distributed High Integrity Applications from Their Architectural Description 155
Bechir Zalila, Irfan Hamid, Jerome Hugues, and Laurent Pautet

Automatic Ada Code Generation Using a Model-Driven Engineering Approach 168
Diego Alonso, Cristina Vicente-Chicote, Pedro Sánchez, Bárbara Álvarez, and Fernando Losilla

Towards User-Level Extensibility of an Ada Library: An Experiment with Cheddar 180
Frank Singhoff and Alain Plantec

Modelling Remote Concurrency with Ada 192
Claude Kaiser, Christophe Pajault, and Jean-François Pradat-Peyre

Design and Performance of a Generic Consensus Component for Critical Distributed Applications 208
Khaled Barbaria, Jerome Hugues, and Laurent Pautet

SANCTA: An Ada 2005 General-Purpose Architecture for Mobile Robotics Research 221
Alejandro R. Mosteo and Luis Montano

Incorporating Precise Garbage Collection in an Ada Compiler 235
Francisco García-Rodríguez, Javier Miranda, and José Fortes Gálvez

Author Index 247