Lecture Notes in Computer Science 10300

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

Editorial Board

David Hutchison
Lancaster University, Lancaster, UK
Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
University of Surrey, Guildford, UK
Jon M. Kleinberg
Cornell University, Ithaca, NY, USA
Friedemann Mattern
ETH Zurich, Zurich, Switzerland
John C. Mitchell
Stanford University, Stanford, CA, USA
Moni Naor
Weizmann Institute of Science, Rehovot, Israel
C. Pandu Rangan
Indian Institute of Technology, Madras, India
Bernhard Steffen
TU Dortmund University, Dortmund, Germany
Demetri Terzopoulos
University of California, Los Angeles, CA, USA
Doug Tygar
University of California, Berkeley, CA, USA
Gerhard Weikum
Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at http://www.springer.com/series/7408

Johann Blieberger · Markus Bader (Eds.)

Reliable Software Technologies – Ada-Europe 2017

22nd Ada-Europe International Conference on Reliable Software Technologies
Vienna, Austria, June 12–16, 2017
Proceedings

Springer

Editors
Johann Blieberger
Institute of Computer Aided Automation
Vienna University of Technology
Vienna
Austria

Markus Bader
Institute of Computer Aided Institute
Vienna University of Technology
Vienna
Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-60587-6 ISBN 978-3-319-60588-3 (eBook)
DOI 10.1007/978-3-319-60588-3

Library of Congress Control Number: 2017943008

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer International Publishing AG 2017
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 22nd edition of the International Conference on Reliable Software Technologies (Ada-Europe 2017) took place in Vienna, returning to Austria 15 years after 2002. The previous editions of the conference were held in Spain (Santander, 1999, Palma de Mallorca, 2004, Valencia, 2010, Madrid, 2015), France (Toulouse, 2003, Brest, 2009, Paris, 2014), the UK (London, 1997, York, 2005, Edinburgh, 2011), Switzerland (Montreux, 1996, Geneva, 2007), Sweden (Uppsala, 1998, Stockholm, 2012), Germany (Potsdam, 2000, Berlin, 2013), Italy (Venice, 2008, Pisa, 2016), Belgium (Leuven, 2001), and Portugal (Porto, 2006).

TU Wien was the lead organizer for this edition, with aid from an international core team that included members of Ada-Europe, the organization that oversees and sponsors the conference series.

The conference took place in the week of June 12–16, 2017, with a rich program for both technical content and social opportunities. The scientific program featured 15 papers selected among 37 peer-reviewed submissions, grouped into five presentation sessions and one panel discussion, entitled "The Future of Safety-Minded Languages," scheduled in the central days of the conference week, to address topics ranging from runtimes, safety and security, timing verification, programming models, and mixed criticality. The proceedings contained in this volume reflect these contributions (see the table of contents for details).

The conference program also included nine industrial contributions arranged in three industrial presentation sessions. Vendor presentations with accompanying exhibitions completed the core program. Eight tutorials for the equivalent of nine half-day sessions were offered on Monday and Friday. The Friday program included the fourth edition of the Workshop on Challenges and New Approaches for Dependable and Cyber-Physical Systems Engineering (De-CPS), this year focusing on the theme "Transportation of the Future." The proceedings from this part of the conference program will be published, in successive installments, in the *Ada User Journal*, the quarterly magazine of Ada-Europe.

The scientific and industrial submissions originated from 24 countries and 124 distinct authors, from Europe, Asia, North and South America, Australia, and Africa. Thanks to that wealth, the final program was an international digest of contributions from Australia, Austria, Denmark, France, Italy, Portugal, South Korea, Spain, Sweden, Switzerland, UK, and USA.

Each central day of the week opened with a keynote talk focusing on topics of interest to the conference scope. The three keynote talks were:

– "The Laws of Robotics and Autonomous Vehicles May Be Much More Than Three, But Don't Panic… Yet" by Giovanni Battista Gallus, from Array, Italy, who discussed the future European legal framework for the development of autonomous vehicles, especially for programming issues.

- "Behavioral Software Metrics" by Tom Henzinger, from IST, Austria, who showed how the classic satisfaction relation between programs and requirements can be replaced by quantitative preference metrics that measure the "fit" between programs and requirements. Depending on the application, such fitness measures can include aspects of function, performance, resource consumption, and robustness.
- "Dependable Internet of Things" by Kay Römer from TU Graz, Austria, who presented the challenge resulting from the increasing use of wireless networked embedded systems in safety-critical applications, which must be proven to meet strict dependability requirements even under the harshest environmental conditions. The presentation highlighted recent results that improve the dependability of wireless communication and localization, embedded computing, and networked control for the Internet of Things.

The tutorial program covered the following topics:

- "Introduction to SPARK 2014," Peter Chapin, Vermont Technical College
- "Ada on ARM Cortex-M, A Zero-Run-Time Approach," Maciej Sobczak, GE Aviation and Inspirel
- "Software Measurement for Dependable Software Systems," William Bail, The MITRE Corporation
- "Real-Time Parallel Programming with the UpScale SDK," Luis Miguel Pinho, ISEP, and Eduardo Quinones, BSC
- "Using Gnoga for Desktop/Mobile GUI and Web development in Ada," Jean-Pierre Rosen, Adalog
- "Frama-C, a Collaborative Framework for C Code Verification," Julien Signoles, CEA LIST
- "On Beyond ASCII: Characters, Strings, and Ada 2012," Jean-Pierre Rosen, Adalog
- "Modular Open System Architecture for Critical Systems," William Bail, The MITRE Corporation

The industrial program featured the following presentations:

- "Astronomical Ada," Ahlan Marriott, White Elephant GmbH, Switzerland
- "IP Network Stack in Ada 2012 and the Ravenscar Profile," Stephane Carrez, France
- "Hardware-Based Data Protection/Isolation at Runtime in Ada Code for Micro-controllers," German Rivera, USA
- "Automated Testing of SPARK Ada Contracts: Progress and Case Study Report," Simon Daniel, Rolls-Royce plc, UK, and Stuart Matthews, Altran UK, UK
- "Introducing Static Analysis to a Mature Project," Jacob Sparre Andersen, JSA Research & Innovation, Denmark
- "Challenges and Opportunities for Improvements of the Testing Process for Ada based Safety Critical Systems," Guillem Bernat, Rapita Systems, UK
- "Experiences with Ada in the Safety-Critical Communication and Ground Control Systems of the nEUROn UCAV," Luis Pabón, Artemio Jiménez, and José M. Martínez, Airbus Defence & Space, Spain

– "Experience with Use of Model-Driven Code Generation on the ASIM Project," Steen Palm, Terma A/S, Denmark
– "A Time-Triggered Middleware for Safety-Critical Automotive Applications," Ayhan Mehmed, Wilfried Steiner, and Maximilian Rosenblattl, TTTech Computertechnik AG, Austria.

We would like to acknowledge the work of all the people who contributed, with various responsibilities and official functions, to the making of the conference program overall. The success of the conference depends in large part on the quality of the program contents. The authors of the selected contributions are to be thanked first and foremost for that. The members of the Program and Industrial Committees had the difficult task of screening the submissions and selecting the contributions to include in this proceedings volume and in the *Ada User Journal*.

The Organizing Committee put it all together: Wolfgang Kastner (Conference Chair); Jacob Sparre Andersen (Industrial Chair); Ben Brosgol (Tutorial and Workshop Chair); Dirk Craeynest (Publicity Chair); Ahlan Marriott (Exhibition Chair). All of them deserve our gratitude for their effort.

We hope that the attendees enjoyed every element of the conference program at least as much as we did in organizing it.

June 2017

Johann Blieberger
Max Bader

Organization

Conference Chair

Wolfgang Kastner	TU Vienna, Austria

Program Co-chairs

Johann Blieberger	TU Vienna, Austria
Markus Bader	TU Vienna, Austria

Tutorial and Workshop Chair

Ben Brosgol	AdaCore, USA

Industrial Chair

Jacob Sparre Andersen	JSA Consulting, Denmark

Publicity Chair

Dirk Craeynest	Ada-Belgium and KU Leuven, Belgium

Exhibition Chair

Ahlan Marriott	White Elephant, Switzerland

Local Chair

Markus Bader	TU Vienna, Austria

Sponsoring Institutions

AdaCore
Ellidiss Technologies
PTC Developer Tools
RAPITA Systems Ltd.
Vector Software

Program Committee

Mario Aldea	Universidad de Cantabria, Spain
Ted Baker	NSF, USA

Ezio Bartocci	Vienna University of Technology, Austria
Bernd Burgstaller	Yonsei University, South Korea
Juan A. de la Puente	Universidad Politécnica de Madrid, Spain
Lukas Esterle	Vienna University of Technology, Austria
Michael González Harbour	Universidad de Cantabria, Spain
J. Javier Gutiérrez	Universidad de Cantabria, Spain
Jérôme Hugues	ISAE, France
Raimund Kirner	University of Hertfordshire, UK
Wilfried Kubinger	FH Technikum Wien, Austria
Albert Llemosí	Universitat de les Illes Balears, Spain
Kristina Lundkvist	Mälardalen University, Sweden
Franco Mazzanti	ISTI-CNR, Italy
Laurent Pautet	Telecom ParisTech, France
Justus Piater	University of Innsbruck, Austria
Luís Miguel Pinho	CISTER/ISEP, Portugal
Erhard Plödereder	Universität Stuttgart, Germany
Jorge Real	Universitat Politècnica de València, Spain
José Ruiz	AdaCore, France
Sergio Sáez	Universitat Politècnica de València, Spain
Tucker Taft	AdaCore, USA
Theodor Tempelmeier	University of Applied Sciences Rosenheim, Germany
Elena Troubitsyna	Åbo Akademi University, Finland
Santiago Urueña	GMV, Spain
Tullio Vardanega	Università di Padova, Italy
Armin Wasice	University of California at Berkeley, USA
Michael Zillich	Vienna University of Technology, Austria

Industrial Committee

Ian Broster	Rapita Systems, UK
Jørgen Bundgaard	Rambøll Denmark A/S
Dirk Craeynest	Ada-Belgium & KU Leuven, Belgium
Thomas Gruber	Austrian Institute Of Technology (AIT), Austria
Egil Harald Høvik	Kongsberg, Norway
Ismael Lafoz	Airbus Defence and Space, Spain
Björn Lundin	Consafe Logistics, Sweden
Ahlan Marriott	White Elephant, Switzerland
Paolo Panaroni	Intecs, Italy
Paul Parkinson	Wind River, UK
Andreas Richtsfeld	DS Automotion GmbH, Austria
Jean-Pierre Rosen	Adalog, France
Emilio Salazar	GMV, Spain
Jacob Sparre Andersen	JSA Consulting, Denmark
Jean-Loup Terraillon	European Space Agency, The Netherlands
Sergey Tverdyshev	SysGO, Germany

Additional Reviewers

Jorge Garrido Balaguer
Hector Perez
Juan Zamorano

Contents