Introduction

After 13 years, the International Conference on Reliable Software Technologies, Ada-Europe, returned once again to Germany. In its 18th incarnation as a conference addressing software reliability issues, research, and experience, it is one of the premier conferences on this subject whose importance and actuality remain unbroken. It was also the 33rd annual Ada-Europe conference, with Ada being one of the foremost technologies that have focused specifically on software reliability. Editions of the conference with its focus on reliability were held in Switzerland (Montreux 1996 and Geneva 2007), the United Kingdom (London 1997, York 2005 and Edinburgh 2011), Sweden (Uppsala 1998 and Stockholm 2012), Spain (Santander 1999, Palma de Mallorca 2004 and Valencia 2010), Belgium (Leuven 2001), Austria (Vienna 2002), France (Toulouse 2003 and Brest 2009), Portugal (Porto 2006), Italy (Venice 2008), and Germany (Potsdam 2000 and now Berlin-Dahlem 2013).

Organized by Ada Deutschland e.V. and its scientific counterpart, the special interest group Ada of the Gesellschaft für Informatik (GI), the conference was sponsored by Ada-Europe, the European federation of national Ada societies, in cooperation with GI, ACM SIGAda, SIGBED, and SIGPLAN. We gratefully acknowledge additional sponsorship by DFG, the German Research Foundation. The conference took place in Berlin-Dahlem during June 11–15, 2013, at the Seminaris Conference Center Dahlem Cube. Before and after the conference, three ISO Working or Rapporteur Groups conducted their meetings at the conference location.

Thirteen years ago, we noted in the foreword of the proceedings of the conference in Potsdam: “It is not an overstatement to note that our daily life is beginning to literally depend on the reliability of the software embedded in products. Yet such reliability does not come about by accident. It needs to be infused into the software and the processes of the software life cycle by the application of appropriate techniques and technologies.” These statements still hold true today, except that entrusting our lives and fortunes to software-based systems is no longer a vision of the future but daily reality as we drive in our cars, fly in airplanes, bank online, or are screened or operated upon by medical equipment with fascinating new capabilities most of which are the result of software support of ever-increasing complexity.

An added dimension in today’s world is the advent of multi-core technologies or, to put it in software terms, the forced departure from fully deterministic execution models and the advent of systems in which computations occur in a non-deterministic parallel order. Design principles that for decades were applied to ensure certain reliability aspects in safety-critical software are no longer applicable when parallel executions become feasible and necessary.
The paper contributions to the conference mirrored these long-range issues as well as solutions to near-term problems.

Once again, the conference attracted submissions from around the world. Submissions were received from authors residing in Canada, China, Denmark, France, Germany, India, Israel, Italy, Macedonia, Mauritius, Portugal, Spain, Switzerland, Taiwan, Thailand, UK, and the USA. A total of 11 papers were accepted for the proceedings and five additional industry contributions were accepted for presentation at the conference. The overall acceptance rate was 38%. Two conference sessions were reserved for presentations by vendors of products supporting the development and management of reliable software.

As in past years, the conference comprised a three-day technical program at which the papers contained in these proceedings were presented, along with shorter presentations on related topics. The technical program was bracketed by two tutorial days when attendees had an opportunity to catch up on a variety of topics interesting to the field, at both introductory and advanced levels. Further, the conference was accompanied by an exhibition where vendors presented their reliability-related products.

Each conference day opened with a keynote presentation. The keynote speakers and their themes were:

- Bruce Powel Douglass, Chief Evangelist IBM Rational: Model-Based Ada Development for DO-178B/C and the Application of Agile Methods
- Giorgio C. Buttazzo, Scuola Superiore Sant’Anna of Pisa, Italy: Research Challenges in Exploiting Multi-Core Platforms for Real-Time Applications

In addition, Tucker Taft, the principal designer of Ada95, gave an invited overview of the new features of Ada 2012, the latest standard for Ada announced by ISO in December 2012.

We would like to express our sincere gratitude to these distinguished speakers, well known to the community, for sharing their insights and information with the audience.

The tutorial program featured international experts presenting introductory and advanced material on a variety of subjects relevant to software engineers:

- “Multicore programming using divide-and-conquer and work stealing,” Tucker Taft
- “Designing and checking coding standards for Ada,” Jean-Pierre Rosen
- “Effective requirements development practices and their role in effective design,” William Bail
- “Understanding dynamic memory management in safety critical Java,” Kelvin Nilsen
- “Developing code analysis applications with ASIS,” Jean-Pierre Rosen
- “Verification and validation techniques for dependable systems,” William Bail
introduction

vii

- "Design of multitask software: The entity-life modelling approach," Bo Sanden
- "Testing real-time software," Ian Broster
- "Service-oriented architecture and enterprise service bus," Rick Sward
- "Developing high-integrity systems with GNAT GPL and the Ravenscar profile," Juan de la Puente
- "Maximize your application potential," David Sauvage

Many people contributed to the success of the conference. The Program Committee spent part of their Christmas vacation carefully reviewing all submitted papers and providing detailed evaluations. The Industrial Committee reviewed all proposals for experience reports submitted by industry. A subcommittee comprising Johann Blieberger, Jørgen Bundgaard, Hubert B. Keller, Ahlan Marriott, Jürgen Mottok, and Erhard Plödereder, met on a weekend in early February to compose the program based on the reviews.

We thank the committees for their dedication and hard work to get the reviews done in time. A significant help in organizing the paper review was the EasyChair system.

The Organizing Committee deserves special mention. Peter Dencker put together the exhibition where vendors presented their tools or services to make software more reliable and its production easier. Jürgen Mottok composed the attractive tutorial program. Jørgen Bundgaard dedicated extraordinary effort to soliciting contributions for the industrial sessions of the conference and coordinating their review. Erhard Plödereder organized the technical program together with Hubert Keller, who also put together the Preliminary and Final Program of the conference, along with the materials for the web presence. Dirk Craeynest did his usual best in contributing to the public relation material and in distributing the electronic calls for papers, contributions, and participation. Raúl Rochas helped with the local arrangements in Berlin. We also would like to thank Christine Harms who handled the registration and the local organization at Berlin.

Foremost, however, we wish to express our appreciation to the authors of the papers submitted to the conference, and to the participants who came to exchange their ideas and results. Without you, there would be no conference. We hope that you were satisfied by the technical program of the conference and enjoyed the social events of this 18th International Conference on Reliable Software Technologies.

April 2013

Hubert Keller
Erhard Plödereder
Organization

The 18\textsuperscript{th} International Conference on Reliable Software Technologies - Ada-Europe 2013 was organized by Ada-Europe and Ada-Germany, in cooperation with ACM SIGAda, SIGBED, and SIGPLAN, GI, KIT, University of Stuttgart, VDE, VDI.

Organizing Committee

Conference and Program

Co-chairs

Hubert B. Keller Karlsruhe Institute of Technology, Germany
Erhard Plödereder University of Stuttgart, Germany

Tutorial Chair

Jürgen Mottok Regensburg University of Applied Sciences, Germany

Industrial Chair

Jørgen Bundgaard Ada in Denmark and Rambøll Danmark, Denmark

Exhibition Chair

Peter Dencker ETAS GmbH, Germany

Publicity Chair

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

Proceedings Chair

Herbert Klenk Cassidian, Germany

Local Chair

Raúl Rojas FU Berlin, Germany

Local Organizer

Christine Harms ccH, Germany
Program Committee

Ted Baker
Johann Blieberger
Bernd Burgstaller
Alan Burns
Dirk Craeynest
Juan A. de la Puente
Franco Gasperoni
Michael González Harbour
Xavier Grave
Christoph Grein
J. Javier Gutiérrez
Peter Hermann
Jérôme Hugues
Hubert Keller
Pascal Leroy
Albert Llemosí
Kristina Lundqvist

Franco Mazzanti
John McCormick
Stephen Michell
Luís Miguel Pinho
Erhard Plödereder
Jürgen Mottok
Manfred Nagl
Laurent Pautet
Jorge Real
Jean-Pierre Rosen
José Ruiz
Ed Schonberg
Tucker Taft
Theodor Tempelmeier
Elena Troubitsyna
Tullio Vardanega
Juan Zamorano

Industrial Committee

Jørgen Bundgaard
Jacob Sparre Andersen
Jamie Ayre
Ian Broster
Dirk Craeynest
Peter Dencker
Michael Friess
Ismael Lafoz
Ahlan Marriott
Robin Messer

Steen Ulrik Palm
Paolo Panaroni
Paul Parkinson
Ana Isabel Rodríguez
Jean-Pierre Rosen
Alok Srivastava
Claus Stellwag
Jean-Loup Terrailon
Rod White

Supporting Organizations

The organizers of the conference would like to express their thanks to the exhibitors and supporters of the conference.

Exhibitors, at the time of writing, were:

AdaCore
Atego
Ellidiss
ETAS
Rapita Systems
Vector Software
# Table of Contents

## Session: Multicore and Distributed Systems

Experience with the Integration of Distribution Middleware into Partitioned Systems .............................................. 1  
*Héctor Pérez and J. Javier Gutiérrez*

Tasklettes – A Fine Grained Parallelism for Ada on Multicores ........ 17  
*Stephen Michell, Brad Moore, and Luís Miguel Pinho*

Model-Based Deployment of Mission-Critical Spacecraft Applications on Multicore Processors ........................................... 35  
*J. Reinier van Kamphout and Robert Hilbrich*

## Session: Ada and Spark

A SPARK/Ada CubeSat Control Program .......................... 51  
*Carl Brandon and Peter Chapin*

Lady Ada Mediates Peace Treaty in Endianness War ............... 65  
*Thomas Quinot and Eric Botcazou*

## Session: Dependability

Provably Secure DNS: A Case Study in Reliable Software ............ 81  
*Barry Fagin and Martin Carlisle*

Using Ontologies in the Integration of Structural, Functional, and Process Perspectives in the Development of Safety Critical Systems .... 95  
*Irene Bicchierai, Giacomo Bucci, Carlo Nocentini, and Enrico Vicario*

Measuring the Odds of Statements Being Faulty ..................... 109  
*Xiaozhen Xue and Akbar Siami Namin*

## Session: Real-Time Systems

A Model-Based Framework for Developing Real-Time Safety Ada Systems ................................................................. 127  
*Emilio Salazar, Alejandro Alonso, Miguel A. de Miguel, and Juan A. de la Puente*

Towards a Time-Composable Operating System ....................... 143  
*Andrea Baldovin, Enrico Mezzetti, and Tullio Vardanega*
Worst–Case Execution Time Analysis Approach for Safety–Critical Airborne Software

Esteban Asensio, Ismael Lafoz, Andrew Coombes, and Julian Navas

Author Index