Preface

The 16th edition of the International Conference on Reliable Software Technologies – Ada-Europe 2011—took place in the John McIntyre Conference Centre, Edinburgh (UK). 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, 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).

This year Ada-Europe was combined with the Ada Conference UK 2011 in one event, the Ada Connection, a union of two Ada events that have both been very successful in their own right. The Ada-Europe series of conferences has become established as an international forum for providers, practitioners and researchers in all aspects of reliable software technologies. The Ada Conference UK has been running in its current form since 2006 as a series of biennial one-day events, to highlight the increased relevance of Ada in safety- and security-critical systems. By combining these events, the Ada Connection provides a unique opportunity for interaction and collaboration between academics and industrial practitioners.

The Ada-Europe conference represents the main annual event promoted by Ada-Europe, in cooperation with ACM SIGAda. This third visit to the UK acknowledges the fact that the Ada community in this country is a major contributor to Ada-Europe’s activities. This year the conference was organized by members of the Centre for Software Reliability (CSR) and School of Computing Science, Newcastle University (Newcastle upon Tyne, UK).

The scientific program of the conference, which feeds these proceedings, also included sessions devoted to multicore, verification, architecture and modelling, education and mixed criticality, all combined under a more general heading of reliable software technologies. This program is the result of a thorough selection process of 12 papers out of 30 submissions received from authors representing 14 countries.

The conference was enriched with the three keynote talks delivered by the invited speakers, opening the three central days of the conference:

- Peter Bernard Ladkin (University of Bielefeld CITEC and Causalis Limited), a recognized specialist in system safety, spoke about “Functional Safety of Software-Based Critical Systems.”
- Pippa Moore (UK Civil Aviation Authority), an Avionic Systems Design Surveyor working with the CAA for over 14 years, gave a talk entitled “Hippocrates and DO-178B.”
– Jeff O’Leary (US Federal Aviation Administration) with more than 18 years’ experience in software development, systems acquisition and deployment of large-mission critical command and control systems, gave a keynote on “Assuring Software Reliability While Using Web Services and Commercial Products.”

These proceedings include a paper by O’Leary based on the material he presented during the conference.

The conference program included two panels: Programming Languages Meet Multicore and DO178C and Object-Orientation for Critical Systems. The first panel discussed how the advent of multicore is shaking the very foundations of programming languages for concurrency, resource sharing, synchronization, etc. The panel was moderated by Erhard Ploedereder (University of Stuttgart) with Alan Burns (University of York), Tucker Taft (Sofcheck, Inc), and Kevin Hammond (University of St. Andrews) taking part as the panelists. The panel on DO178C and Object-Orientation for Critical Systems discussed how the high-integrity systems industry could reap the benefit of object orientation in their rigid and demanding development process. The panel was moderated by Tim Kelly (University of York) and involved Cyrille Comar (AdaCore), Jean-Pierre Rosen (Adalog) and Dewi Daniels (Verocel) debating pros and cons, risks and opportunities and ways to introduce elements of object orientation into safety-critical system development. The proceedings include a number of position statements.

As a forum that aims at connecting academics with the industrial knowledge and experience centered around reliable software technologies, the conference also included an exciting set of industrial presentations:

– The Transition from MISRA C to SPARK Ada in Active Life Support, by Alex Deas (DeepLife)
– Executable UML Models for High-Integrity Development, by Sam Moody (AWE)
– Implementing a Software Product Line for a Complex Avionics System in Ada83, by Frank Dordowsky (ESG Elektroniksysterm)
– Crimeville - Using Ada Inside an On-line Multi-user Game, by Jacob Sparre (J.S. Andersen Consulting)
– Monitorisation of Real-Time Properties of Certified Distributed Systems, by Urueña Pascual (GMV Aerospace)
– Debugging Mechatronic Applications Written in Ada, by Wiljan Derks (NXP)
– Automatic Code Generation Tools Developed in the Ada Language in a Safety-Critical Context, by Laurent Duffau (Airbus)
The conference also included a series of tutorials offering the participants an opportunity to learn particular approaches, technologies and tools, all aiming at the development of reliable software:

- **Experimenting with ParaSail: Parallel Specification and Implementation Language**, by S. Tucker Taft (SofCheck, Inc.)
- **Designing and Checking Coding Standards for Ada**, by Jean-Pierre Rosen (Adalog)
- **Programming Distributed Systems with YAMI4**, by Maciej Sobczak (Inspirel)
- **Why and How to Measure Non-functional Properties On-target**, by Ian Broster (Rapita Systems Ltd.)
- **Use of Object-Oriented Technologies in High-Reliability Systems**, by Jean-Pierre Rosen (Adalog)
- **SPARK. The Libre Language and Toolset for High-Assurance Software**, by Roderick Chapman (Altran Praxis)
- **Distributed Programming Techniques in Ada**, by Thomas Quinot (AdaCore)

The conference program also included an invited lecture by Les Hatton, Professor of Forensic Software Engineering at Kingston University, well known for his contributions in software engineering. A paper drawn from Hatton’s talk is included in these proceedings.

The conference’s success heavily depends on the active and generous contribution of a number of individuals and organizations. All of them deserve our most sincere thanks. We are specially grateful to all who submitted quality contributions that enabled us to build an attractive and technically sound program. Of course we would like to thank all the attendees, who enable the conference to thrive. We want to thank the Organizing Committee for their help and support during the preparation of this event: Rod Chapman and Steve Riddle (Conference Co-chairs), Jamie Ayre (Industrial Chair), Albert Llemosí (Tutorial Chair), Joan Atkinson (Exhibition Chair), and Dirk Craeynest (Publicity Chair). The organizers are also grateful to the members of the Local Organizing Committee at Newcastle University: Claire Smith and Dee Carr.
The members of the Program and Industrial Committees did a fantastic job in providing quality reviews helping the Organizing Committee in the difficult task of eliciting the final contents of the conference. Last but not least, we wish to express our gratitude to the sponsors at the conference: AdaCore, Altran Praxis, Atego, BAE Systems, Ellidiss Software, Green Hills Software, INTECS and Rapita Systems Ltd.

June 2011

Alexander Romanovsky
Tullio Vardanega
The 16th International Conference on Reliable Software Technologies – Ada-Europe 2011—was organized by Ada-Europe and Newcastle University (UK), in cooperation with ACM SIGAda.

Organizing Committee

Honorary Chair  
John Barnes  
(John Barnes Informatics, UK)

Conference Co-chairs  
Rod Chapman  
(Altran Praxis Ltd., UK)
Steve Riddle  
(Newcastle University, UK)

Conference Program Co-chairs  
Alexander Romanovsky  
(Newcastle University, UK)
Tullio Vardanega  
(Università di Padova, Italy)

Tutorial Chair  
Albert Llemosí  
(Universitat de les Illes Balears, Spain)

Industrial Chair  
Jamie Ayre  
(AdaCore, France)

Exhibition Chair  
Joan Atkinson  
(CSR, UK)

Publicity Chair  
Dirk Craeynest  
(Aubay Belgium and K.U. Leuven, Belgium)

Financial Chair  
Neil Speirs  
(Newcastle University, UK)

Program Committee

Alejandro Alonso  Franco Gasperoni  Stephen Michell
Ted Baker  Michael González  Javier Miranda
Johann Blieberger  Harbour  Daniel Moldt
Jørgen Bundgaard  José-Javier Gutiérrez  Jürgen Mottok
Bernd Burgstaller  Andrew Hately  Laurent Pautet
Alan Burns  Peter Hermann  Luís Miguel Pinho
Jon Burton  Jérôme Hugues  Erhard Plödereder
Rod Chapman  Albert Llemosí  Jorge Real
Dirk Craeynest  Franco Mazzanti  Alexander Romanovsky
Alfons Crespo  John McCormick  Bo I. Sanden
Juan A. de la Puente  Julio Medina  Sergio Sáez
External Reviewers

Albert Black  Ramn Fernandez  Alexei Iliasov
Lawrence Cabac  Alex Green  Hector Perez Tijero
# Table of Contents

## Keynote Talk

Assuring Software Reliability While Using Web Services and Commercial Products ............................................ 1

*Jeffrey O’Leary*

## Multicore

Detecting High-Level Synchronization Errors in Parallel Programs ...... 17

*Syed Aoun Raza, Stefan Franke, and Erhard Ploedereder*

Design and Implementation of a Ravenscar Extension for Multiprocessors ................................................ 31

*Fabien Chouteau and José F. Ruiz*

A Real-Time Framework for Multiprocessor Platforms Using Ada 2012 .......................................................... 46

*Sergio Sáez, Silvia Terrasa, and Alfons Crespo*

## Verification

The SQALE Quality and Analysis Models for Assessing the Quality of Ada Source Code ........................................ 61

*Thierry Coq and Jean-Pierre Rosen*

Adapting ACATS to the Ahven Testing Framework .................. 75

*Dan Eilers and Tero Koskinen*

Model-Based Analysis and Design of Real-Time Distributed Systems with Ada and the UML Profile for MARTE 89

*Julio L. Medina and Alvaro Garcia Cuesta*

## Architecture and Modelling

Developing Dependable Software-Intensive Systems: AADL vs. EAST-ADL .................................................. 103

*Andreas Johnsen and Kristina Lundqvist*

A Formal Approach to Design and Verification of Two-Level Hierarchical Scheduling Systems ........................ 118

*Laura Carnevali, Giuseppe Lipari, Alessandro Pinzuti, and Enrico Vicario*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecting a Common Bridge Abstraction over Different Middleware</td>
<td>132</td>
</tr>
<tr>
<td>Paradigms</td>
<td></td>
</tr>
<tr>
<td><em>Iago Rodríguez-López and Marisol García-Valls</em></td>
<td></td>
</tr>
<tr>
<td><strong>Education and Mixed Criticality</strong></td>
<td></td>
</tr>
<tr>
<td>Using Robotics as a Motivational Tool: An Ada Interface to a Pioneer</td>
<td>147</td>
</tr>
<tr>
<td>Robot</td>
<td></td>
</tr>
<tr>
<td><em>Rigoberto Chil, Diego Alonso, Francisco Ortiz, and Juan Pastor</em></td>
<td></td>
</tr>
<tr>
<td>ORK+/XtratuM: An Open Partitioning Platform for Ada</td>
<td>160</td>
</tr>
<tr>
<td>Ángel Esquinas, Juan Zamorano, Juan A. de la Puente,</td>
<td></td>
</tr>
<tr>
<td>Miguel Masmano, Ismael Ripoll, and Alfons Crespo</td>
<td></td>
</tr>
<tr>
<td>Implementing Mixed Criticality Systems in Ada</td>
<td>174</td>
</tr>
<tr>
<td><em>Sanjoy Baruah and Alan Burns</em></td>
<td></td>
</tr>
<tr>
<td><strong>Panel: Language Paradigms for Multicore Programming</strong></td>
<td></td>
</tr>
<tr>
<td>Programming Languages Meet Multicore</td>
<td>189</td>
</tr>
<tr>
<td><em>Erhard Ploedereder</em></td>
<td></td>
</tr>
<tr>
<td>Programming Languages for Real-Time Applications Executing on</td>
<td>193</td>
</tr>
<tr>
<td>Parallel Hardware</td>
<td></td>
</tr>
<tr>
<td><em>Alan Burns</em></td>
<td></td>
</tr>
<tr>
<td>Multicore Programming in ParaSail: Parallel Specification and</td>
<td>196</td>
</tr>
<tr>
<td>Implementation Language</td>
<td></td>
</tr>
<tr>
<td><em>S. Tucker Taft</em></td>
<td></td>
</tr>
<tr>
<td>Why Parallel Functional Programming Matters: Panel Statement</td>
<td>201</td>
</tr>
<tr>
<td><em>Kevin Hammond</em></td>
<td></td>
</tr>
<tr>
<td><strong>Panel: DO178C and Object-Orientation for Critical Systems</strong></td>
<td></td>
</tr>
<tr>
<td>OOT, DO-178C and SPARK</td>
<td>206</td>
</tr>
<tr>
<td><em>Roderick Chapman and Trevor Jennings</em></td>
<td></td>
</tr>
<tr>
<td>Position Paper: DO-178C/ED-12C and Object-Orientation for Critical</td>
<td>211</td>
</tr>
<tr>
<td>Systems</td>
<td></td>
</tr>
<tr>
<td><em>Dewi Daniels</em></td>
<td></td>
</tr>
<tr>
<td>Object Orientation in Critical Systems: Yes, in Moderation – Position</td>
<td>214</td>
</tr>
<tr>
<td>Paper for the DO178C and Object-Orientation for Critical Systems</td>
<td></td>
</tr>
<tr>
<td>Panel</td>
<td></td>
</tr>
<tr>
<td><em>Jean-Pierre Rosen</em></td>
<td></td>
</tr>
</tbody>
</table>
Signet Library Talk

On the Evolution of Unnatural Language ....................... 219

Les Hatton

Author Index .................................................. 227