

# Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

1411

Lars Asplund (Ed.)

# Reliable Software Technologies – Ada-Europe

1998 Ada-Europe International Conference  
on Reliable Software Technologies  
Uppsala, Sweden, June 8-12, 1998  
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Lars Asplund  
Uppsala University, Department of Computer Systems  
P.O. Box 325, S-751 05 Uppsala, Sweden  
E-mail: asplund@docs.uu.se

Cataloging-in-Publication data applied for

**Die Deutsche Bibliothek - CIP-Einheitsaufnahme**

**Reliable software technologies : proceedings / Ada Europe '98, 1998  
Ada Europe International Conference on Reliable Software  
Technologies, Uppsala, Sweden, June 8 - 12, 1998. Lars Asplund  
(ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong  
Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo :  
Springer, 1998  
(Lecture notes in computer science ; Vol. 1411)  
ISBN 3-540-64536-5**

CR Subject Classification (1991): D.2, D.1.2-5, D.3, D.4, C.2.4, C.3, K.6

ISSN 0302-9743

ISBN 3-540-64536-5 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1998  
Printed in Germany

Typesetting: Camera-ready by author  
SPIN 10637192 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

## Foreword

The third International Conference on Reliable Software Technologies – Ada-Europe'98 took place in Uppsala, Sweden, from June 8 to 12, 1998. It was the 18<sup>th</sup> conference organized by Ada-Europe in co-operation with ACM and is the main Ada event in Europe with its counterpart being the SIGAda Conference in the USA in fall.

The programming language Ada with the new standard, Ada 95, is very stable and mature. The language itself provides support for distributed systems, real-time systems, object-oriented programming and design, and the implementation of High Integrity Systems.

The importance of reliable software has grown over the years, and we are today dependent on software in a large number of areas where a malfunction of the software can result in loss of human lives. The programming language Ada may not be the ultimate solution, but it is definitely the best programming language available today for safety critical software. It is not by chance that Boeing decided to use Ada in its fly-by-wire 777 aircraft. The FAA (Federal Aviation Administration) has very strict rules for certifying an avionics system according to the standard DO-178B.

The importance of High Integrity Systems will be more pronounced in the future due to the increased capacity of micro-controllers, and the temptation to use more and more complex software. Other areas where safety is already known to be crucial are systems for nuclear power plants and medical applications.

Ada is being used in real-time systems and with the new abstraction, the protected object, it is now possible to efficiently implement a real-time system using tasks, protected objects, priority inheritance, and the priority ceiling protocol. By the use of these features and methods a system can be guaranteed to meet deadlines, avoid deadlocks, and keep blocking time to a minimum for high priority tasks.

The use of the Internet has exploded over the last few years, and we now see many innovations. We get not only documents with text but also pictures and sound. The documents are also now equipped with programs. The new technology works well with Ada, and the abstract machine for executing the Java byte code can be utilized by an Ada compiler thereby giving us access to a safe programming language for the design and implementation of Graphical User Interfaces.

The three invited keynote speakers, who gave talks about the current and future use of Ada and important aspects on safety critical systems, were:

- *Franco Gasperoni*, E.N.S.T. Paris, France, Embedded Opportunities
- *Pierre Chapront*, GEC Alsthom Transport, Saint Ouen, France, Ada+B The formula for safety critical software development
- *Martyn Thomas*, Chairman Emeritus, Praxis Critical Systems Ltd, U.K., Engineering Quality in Software

The technical program of the conference features 23 papers, selected by a program committee of highly qualified researchers in academia and industry in the following sessions

- Ada 95 and Java
- Ada 95 Language and Tools
- Distributed Systems
- Real-Time Systems
- Case Studies and Experiments
- Software Quality
- Software Development Methods and Techniques
- Software Architectures
- High Integrity Systems

The conference also contained an excellent set of tutorials, featuring international experts who presented introductory and advanced material on software engineering:

- Ada 95 as a Foundation Language for Undergraduate Programs, *Michael B. Feldman*
- Java for Ada Programmers, *Ben Brosgol*
- Software Systems Architecture: A Practical Architecture Method, *David Emery, Rich Hilliard, Timothy Rice*
- Distributed Systems Annex of Ada 95 and an Inside Look at the GLADE Implementation, *Laurent Pautet, Samuel Tardieu*
- The End of the Age of Miracles, *Richard T. Dué*
- Ada-Based Systems Engineering with O4S, *Ingmar Ögren*
- Building Development Tools for Use with GNAT, *Cyrille Comar, Sergey Rybin*
- Ada, Java & GNAT: A Manager's and Developer's Roadmap, *Franco Gasperoni, Edmond Schonberg*
- Guaranteeing Timing Requirements under Real-Time POSIX, *Michael González Harbour*
- SPARK, *John Barnes*

Many people have contributed towards making this conference a success.

Kristina Lundqvist deserves my sincere gratitude for her work as tutorial chair and as a much valued colleague for planning the conference generally. Örjan Leringe has taken care of the practical arrangements, and I am very thankful for his effort with the Web pages, and the printed program. I also would like to thank May-Lill Hansen for her efforts in getting exhibitors to the exhibition.

Last but not least I would like to thank the program committee members, for their hard work during the review process.

The technical program was complemented by a number of social events, the highlight being the musical divertimento by ACT.

# Organization

The International Conference on Reliable Software Technologies – Ada-Europe'98 was organized by Ada-Europe, in cooperation with ACM/SIGAda.

## Executive Committee

Program Chair: Lars Asplund, Department of Computer Systems, Uppsala University, Sweden  
Tutorials: Kristina Lundqvist, Department of Computer Systems, Uppsala University, Sweden  
Exhibition: May-Lill Hansen, Ericsson Radar AS, Norway

## Program Committee

Angel Alvarez, Technical University of Madrid, Spain  
John Barnes, JBI, U.K.  
Lars Björnfot, Ericsson, Sweden  
Alan Burns, University of York, U.K.  
Dirk Craeynest, OFFIS nv/sa, Belgium  
Michael Feldman, The George Washington University, U.S.A.  
Mark Gerhardt, Lockheed Martin Corp., U.S.A.  
May-Lill Hansen, Ericsson Radar AS, Norway  
Michael Gonzáles Harbour, Universidad de Cantabria, Spain  
Jan Van Katwijk, Delft University of Technology, The Netherlands  
Yvon Kermarrec, ENST de Bretagne, France  
Björn Källberg, CelsiusTech Naval Systems AB, Sweden  
Doug Locke, Lockheed Martin Corp., U.S.A.  
Steve Michell, ORA, Canada  
Laurent Pautet, ENST Paris University, France  
Erhard Plödereder, University of Stuttgart, Germany  
Jean-Pierre Rosen, ADALOG, France  
Edmond Schonberg, New York University & Ada Core Technologies, U.S.A.  
Alfred Strohmeier, Swiss Federal Institute of Technology, Lausanne, Switzerland  
Joyce Tokar, DDC-I, U.S.A.  
Göran Wall, Enator Telub AB, Sweden  
Stef Van Vlierberghe, OFFIS nv/sa, Belgium  
Brian Wichmann, National Physical Laboratory, U.K.  
Daniel Wengelin, CelsiusTech Systems AB, Sweden

## Conference Administrator

Mariadata, Box 1085, SE-141 22 Huddinge/Stockholm, Sweden

# Table of Contents

## Invited Speaker

Embedded Opportunities .....	1
<i>F Gasperoni</i>	
Ada+B The Formula for Safety Critical Software Development .....	14
<i>P Chapront</i>	

## Ada 95 and Java

Porting the GNAT Tasking Runtime System to the Java Virtual Machine .	19
<i>L Millet, T Baker</i>	
Automating the Ada Binding Process for Java - How Far Can We Go?....	29
<i>D E Emery, R F Mathis, K A Nyberg</i>	

## Ada 95 Language and Tools

Synchronizing Multiple Clients and Servers .....	41
<i>M Ben-Ari</i>	
How to Avoid the Inheritance Anomaly in Ada .....	53
<i>G Schumacher, W Nebel</i>	

## Distributed Systems

Inside the Distributed Systems Annex .....	65
<i>L Pautet, S Tardieu</i>	
Integrating Groups and Transactions: A Fault-Tolerant Extension of Ada .	78
<i>M Patiño-Martínez, R Jiménez-Peris, S Arévalo</i>	

## Real-Time Systems

Implementing and Using Execution Time Clocks in Ada Hard Real-Time Applications.....	90
<i>M González Harbour, M Aldea Rivas, JJ Gutiérrez García, JC Palencia Gutiérrez</i>	
Programming Hard Real-Time Systems with Optional Components in Ada	102
<i>A Espinosa, V Julián, C Carrascosa, A Terrasa, A García-Fornes</i>	
Object Oriented Abstractions for Real-Time Distributed Systems .....	112
<i>S A Moody</i>	

## Case Studies and Experiments

(Astro)Physical Supercomputing: Ada95 as a Safe, Object Oriented Alternative .....	128
<i>M J Stift</i>	

Ada 95 for a Distributed Simulation System .....	140
<i>H Hagenauer, W Pohlman</i>	

PINROB: A Portable API for Industrial Robots .....	151
<i>M González Harbour, R Gómez Somarriba, A Strohmeier, J Jacot</i>	

## Software Quality

Quality-for-ASIS : A Portable Testing Facility for ASIS .....	163
<i>A Strohmeier, V Fofanov, S Rybin, S Barbey</i>	

Ten Years of Tool Based Ada Compiler Validations. An Experience Report .....	176
<i>M Tonndorf</i>	

## Software Development Methods and Techniques

A Two-Level Matching Mechanism for Object-Oriented Class Libraries ...	188
<i>S Araban, A S M Sajeev</i>	

Modern Avionics Requirements for the Distributed Systems Annex .....	201
<i>B Lewis, S Vestal, D McConnell</i>	

## Software Architectures

A Case Study in Quantitative Evaluation of Real-Time Software Architectures .....	213
<i>J L Fernández, B Álvarez, F García, Á Pérez, J A de la Puente</i>	

Building Modular Communication Systems in Ada: The <i>Simple-Com</i> Approach .....	225
<i>J M González-Barahona, P de-las-Heras-Quirós, J Centeno-González, F Ballesteros</i>	

## High Integrity Systems

Symbolic Reaching Definitions Analysis of Ada Programs .....	238
<i>J Blieberger, B Burgstaller</i>	

Looking at Code With Your Safety Goggles On .....	251
<i>K Wong</i>	

The Ravenscar Tasking Profile for High Integrity Real-Time Programs ...	263
<i>A Burns, B Dobbing, G Romanski</i>	

Guidance on the Use of Ada95 in High Integrity Systems . . . . .	276
<i>S Michell, M Saaltink</i>	
Ada in the JAS 39 Gripen Flight Control System . . . . .	288
<i>B Frisberg</i>	
<b>Author Index</b> . . . . .	<b>297</b>