



7th International Conference on RELIABLE SOFTWARE TECHNOLOGIES -ADA-EUROPE 2002



VIENNA, AUSTRIA, JUNE 17-21, 2002

http://www.ada-europe.org/conference 2002.html







PRELIMINARY PROGRAM

The information presented here is preliminary - please refer to the conference website for the latest details.

In 2002, the 7th International Conference on Reliable Software Technologies will take place in Vienna, Austria, from June 17th to June 21st. The conference offers a technical program and exhibition, plus a series of tutorials and a workshop.

The conference provides an international forum for researchers, developers and users of reliable software technologies. Presentations and discussions cover applied and theoretical work currently conducted to support the development and maintenance of software systems.

Vienna, a city with about 2 million inhabitants is situated in the heart of Europe. It is a city on

which its ever-changing history has left an indelible mark, manifested also in the rich cultural heritage. Shaped by its hundreds of years as capital of an empire, the city's ultimate fascination nowadays stems from combining imperial grandeur with explosive modernity.

The conference will take place in the Parkhotel Schönbrunn which originated in 1907 as the guest house of Emperor Franz Josef I. The newly renovated hotel is located in the immediate vicinity of the "Schönbrunn Palace" and its beautiful surrounding park, situated close to the center of Vienna.

	Morning	Late Morning	After Lunch	Afternoon		
	SPARK, an "Intensive Overview", P. Amey and R. Chapman					
Monday June 17th Tutorials	MaRTE OS: Bringing Embedded Systems and Real-Time POSIX Together, <i>M. González and M. Aldea</i>					
	Principles of Physical So <i>M. H</i>	oftware Design in Ada95, eaney	Implementing Design Patterns in Ada 95 , <i>M. Heaney</i>			
Tuesday June 18th	Embedded Systems unsuitable for	Embedded Systems	Real-Time Systems	High Integrity		
Sessions & obj Exhibition Ma	object orientation, Maarten Boasson	Case Studies	Vendor presentations	Systems		
Wednesday June 19th	On Architectural	Ada Language	Program Analysis	Tools		
Sessions & Exhibition	Mehdi Jazayeri	Issues	Vendor presentations			
Thursday June 20th	Reasoning About Reliable Distributed	Distributed Systems	Libraries	Contextware: Bridging Physical and Virtual		
Sessions & Exhibition	Programs, Rachid Guerraoui	Vendor presentations	OO Technology	Worlds, Alois Ferscha		
	CORBA 3 and CORBA for Embedded Systems, S. Ron Oliver					
Friday June 21st Tutorials & Workshop	Using Open Source Har Build Reliab J. Sherrill an	rdware and Software to ble Systems, <i>nd J. Gaisler</i>	Cleanroom Software Engineering: An Overview $W.$ Bail			
	Workshop: Container Lib <i>E. L</i>	A Standard prary for Ada, amm	Exceptions – What You Always Wanted to Know About Exceptions, But Were Afraid to Ask <i>C. Colket</i>			

OVERVIEW OF THE WEEK



INVITED SPEAKERS

Embedded Systems Unsuitable for On Architectural **Object** Orientation

Maarten Boasson, Quaerendo Invenietis bv & University of Amsterdam

It will be argued that the current focus on object technology is detrimental to progress in embedded systems. The core of the problem is that OO is fine for analysis but does not answer the design needs. Solutions for shortcomings are sought within the OO dogma, making things worse. This talk will outline a different approach.

Maarten Boasson studied mathematics in Groningen, the Netherlands. He became involved in advanced studies aiming at control of complexity, both of the development process and of the system under development itself. This resulted in the creation of a novel architecture for distributed reactive systems, that has been applied successfully in numerous systems and is, more than 10 years after its introduction, still unsurpassed in its support for integration, fault tolerance and component reuse. In 1996 Boasson was appointed professor of computer science at the University of Amsterdam, where he holds a chair in Industrial Complex Computer Systems. He played a major role in establishing a dutch national research program in embedded systems, and is currently associate editor-in-chief of IEEE Software.

Reasoning About Reliable Distributed Programs

Rachid Guerraoui, Swiss Federal Institute of Technology in Lausanne (EPFL)

What does it mean for a distributed program to be reliable? A program is reliable if it looks like a centralized program that does never fail. This talk aims at addressing the ramifications underlying this first glance intuitive answer. While doing so, the talk overviews several decades of work on correctness of distributed programs, from Lamport's atomicity and Papadimitrious' serializability, to linearizability and x-ability.

Rachid Guerraoui is professor in computer science at the Swiss Federal Institute of Technology in Lausanne (EPFL). He leads the Distributed Programming Laboratory and teaches object-oriented programming and distributed algorithms. He is interested in devising abstractions for reliable distributed programming.

Stability and **Evolution**

Mehdi Jazayeri, Technical University of Vienna

Many organizations are now pursuing software architecture as a way to control their software development and evolution challenge. A software architecture describes the properties of a family of products, thus addressing the problems of both development and evolution. An important problem is to be able to evaluate the "goodness" of a proposed architecture. The talk will propose stability or resilience as a measure of goodness of an architecture. The stability of an architecture is a measure of how well it accommodates new family members. It can be measured by the amount of code changes necessary for the introduction of a new member. A case study of several releases of a telecommunication software system containing a few million lines of code will be used to demonstrate one way to try to estimate architectural stability. The talk will also present the challenges in software evolution and conclude with recommendations for future research.

Mehdi Jazayeri is a professor of computer science at the Technical University of Vienna. He spent many years in software research and development at several Silicon Valley companies, including ten years at Hewlett-Packard Laboratories in Palo Alto, California. His recent work has been concerned with component-base software engineering of distributed systems, particularly Web-based systems. He is a coauthor of Programming Language Concepts (John Wiley, 1998), Fundamentals of Software Engineering (Prentice-Hall, 2002), and Software Architecture for Product Families (Addison-Wesley, 2000).

Bridging Physical Contextware: and Virtual Worlds

Alois Ferscha, University of Linz

Alois Ferscha joined the University of Linz as full professor in 2000. He published more than 60 technical papers on topics related to parallel and distributed computing. Currently his research interests are in the areas of Pervasive Computing, Embedded Software Systems, Wireless Communication, Multiuser Cooperation, Distributed Interaction and Distributed Interactive Simulation.



Sessions and Presentations

Embedded Systems

Evaluating Performance and Power of Objectoriented vs. Procedural Programming in Embedded Processors, *Alexander Chatzigeorgiou and George Stephanides (Greece).*

OMC-INTEGRAL Memory Management, Jose Manuel Pérez Lobato and Eva Martín Lobo (Spain).

Language Issues of Compiling Ada to Hardware, Michael Ward and Neil C. Audsley (UK).

Case Studies

Software Development Reengineering – An Experience Report, Adrian Hoe (Malaysia).

Using a Secure Java Micro-kernel on Embedded Devices for the Reliable Execution of Dynamically Uploaded Applications, *Walter Binder and Balázs Lichtl (Austria)*.

Development of a Control System for Teleoperated Robots using UML and Ada95, Francisco J. Ortiz, Alejandro Martínez, Bárbara Alvarez, Andrés Iborra, and José M. Fernández (Spain).

Real-Time Systems

A POSIX-Ada Interface for Application-Defined Scheduling, *Mario Aldea Rivas and Michael González Harbour (Spain)*.

The Formal Development of a Real Time Kernel: Kernel Modelling, Stephen G. Michell and Douglas J. Howe (Canada).

Vendor Presentations

Each vendor will give a presentation in the vendor presentation track. Please find a (preliminary) list of vendors on the last page.

High Integrity Systems

Closing the Loop: The Influence of Code Analysis on Design, Peter Amey (UK).

High-Integrity Systems Development for Integrated Modular Avionics using VxWorks and GNAT, Paul Parkinson and Franco Gasperoni (UK, France).

Tools

A Tailorable Distributed Programming Environment, E. Martel, F.Guerra, and J. Miranda (Spain).

About the Difficulties of Building a Pretty-Printer for Ada, Sergey Rybin and Alfred Strohmeier (Russia, Switzerland).

Ada Language Issues

Adding Design by Contract to the Ada Language, *Ehud Lamm (Israel).*

How to Use GNAT to Efficiently Preprocess New Ada Sentences, J. Miranda, F. Guerra, E. Martel, J. Martín, and A. González (Spain).

Exposing Uninitialized Variables: Strengthening and Extending Run-Time Checks in Ada, *Robert Dewar*, *Olivier Hainque*, *Dirk Craeynest*, and *Philippe Waroquiers (US, France, Belgium)*.

Program Analysis

Static Dependency Analysis for Concurrent Ada95 Programs, Zhenqiang Chen, Baowen Xu, Jianjun Zhao, and Hongji Yang (China, Japan, UK).

DataFAN: A Practical Approach to Data Flow Analysis for Ada95, Krzysztof Czarnecki, Michael Himsolt, Ernst Richter, Falk Vieweg, and Alfred Rosskopf (Germany).

Prioritization of Test Cases in MUMCUT Test Sets: An Empirical Study, Yuen T. YU and Man F. LAU (China, Australia).

Distributed Systems

Concurrency Control in Transactional Drago, Marta Patiño-Martínez, Ricardo Jiménez-Peris, Jörg Kienzle, and Sergio Arévalo (Spain, Switzerland).

Transparent Environment for Replicated Ravenscar Applications, *Luís Miguel Pinho and Francisco Vasques (Portugal).*

Modeling and Schedulability Analysis of Hard Real-Time Distributed Systems Based on Ada Components, Julio L. Medina, J. Javier Gutiérrez, José M. Drake, and Michael González Harbour (Spain).

Libraries, APIs, Bindings

An Ada Binding to the IEEE 1003.1q (POSIX Tracing) Standard, Agustín Espinosa Minguet, Ana García Fornes, and Alfons Crespo i Lorente (Spain).

GNAT Ada Database Development Environment, Michael Erdmann (Germany).

OO Technology

Ada, Interfaces and the Listener Paradigm, Jean-Pierre Rosen (France).

Using Object Orientation in High Integrity Applications: A Case Study, Alejandro Alonso, Roberto López, Tullio Vardanega, and Juan Antonio de la Puente (Spain, the Netherlands).



TUTORIALS AND WORKSHOP

SPARK, an "Intensive Overview"

Peter Amey & Rod Chapman, Praxis Critical Systems

SPARK is an annotated sub-language of Ada which is unambiguous and suitable for rigorous static analysis. The tutorial, which is extracted from the four-day "Software Engineering with SPARK" course will provide an intensive introduction to SPARK and the static analysis performed by the SPARK Examiner. Attendees will be encouraged to bring laptop computers on which the SPARK Examiner will be installed.

MaRTE OS: Bringing Embedded Systems and Real-Time POSIX Together

Michael Gonzalez Harbour & Mario Aldea, University of Cantabria

MaRTE OS is a free software implementation of the POSIX minimum real-time system profile. It is designed for embedded systems and provides a development environment for Ada, C, or mixed language real-time applications. The tutorial will describe the main features of MaRTE OS, its architecture and performance, and the details on its development environment.

In addition, the tutorial will discuss the main real-time operating system services defined in the POSIX.13 minimum real-time profile. These services allow application developers to write portable applications that meet their real-time requirements, and that may be be implemented on small embedded systems.

Principles Of Physical Software Design in Ada95

Matthew Heaney

The tutorial addresses issues concerning the compilation of large software systems and presents many techniques for ameliorating the problems.

Most texts on software design concentrate almost exclusively on logical design, and provide only a cursory explanation of physical design. Discussions about types and objects are important, but there are also many pragmatic compilation issues that cannot be ignored. Unless care is taken, dependencies among modules often force a substantial recompile when seemingly innocuous changes are made. This can stymie development, especially for large systems that require hours (or even days) to rebuild.

Implementing Design Patterns in Ada95

Matthew Heaney

This tutorial addresses the question of what "design patterns" are and presents many advanced idioms for object-oriented programming in Ada95.

CORBA 3 and CORBA for Embedded Systems

S. Ron Oliver, Top Graph'X

The tutorial starts with an overview of CORBA 3 with emphasis on changes from CORBA 2. Thereafter it addresses CORBA principles, the Interface Definition Language (IDL), client programs, object (server) programs, CORBA Services, CORBA Facilities, and the CORBA Component Model (CCM). Several advanced features of CORBA 3, including Minimum CORBA and Real-Time CORBA, are also discussed. These topics are of particular interest when using CORBA in the area of embedded systems.

Using Open Source Hard- and Software to Build Reliable Systems

Joel Sherrill, OAR Corporation Jiri Gaisler, Gaisler Research

A framework for the development of embedded systems based solely on open-source components is presented. The framework is based on the LEON SPARC-V8 processor, RTEMS real-time operating system, and the GNU Ada toolchain. The tutorial includes a discussion of the implications of applying the open source model to hardware and embedded systems software. An overview of the characteristics of real-time embedded systems, the cross development process, and the features of Ada95 that aid the development of real-time embedded systems is presented. A demonstration is made on how to configure the target processor, adapt the RTEMS operating system to custom boards, and develop Ada applications.

Cleanroom Software Engineering: An Overview

William Bail, MITRE & University of Maryland

Cleanroom Software Engineering is an approach to the development of software that emphasizes defect avoidance and that is strongly rooted in formal methods and mathematics. While not gaining the notoriety that other techniques have enjoyed, projects that have applied Cleanroom have



experienced significant benefits, including low defect rates. It emphasizes multiple builds in an incremental model, with each build constructed using forms known as box structures. Verification of the structures is accomplished using correctness proofs, while software certification is based on usage models which facilitate statistical testing. Recent work has integrated Cleanroom with object-oriented models. In addition the SEI has released a Cleanroom Software Engineering Reference Model, providing an integrated set of work products and processes for organizations wishing to apply this technique.

Exceptions - What You Always Wanted to Know About Exceptions, But Were Afraid To Ask

Currie Colket, MITRE & ACM SIGAda

Exception processing has the power to detect serious problems in the execution of a program and return one back to a known safe state with high integrity. As such, it can be a very powerful tool for developing high quality software.

To be effective, exceptions and their handling must be addressed at the design level and not at the code level. This presentation will discuss several alternative approaches to addressing error handling in the design using exceptions.

Moreover the use of exceptions can be assessed via automated tools. Several analyses that can be performed on a program via automated tools so the program quality can be improved will be discussed. The tutorial will conclude by addressing proposed needs for exceptions resulting from the Exception Workshop held at Ada-Europe 2001.

Workshop: A Standard Container Library for Ada

Workshop Co-Chairs

Ehud Lamm, The Open University of Israel Email: ehudla@openu.ac.il

John English, University of Brighton Email: je@brighton.ac.uk

Both contemporary dominant general purpose programming languages, Java and C++, come equipped with a standard set of reusable containers. There are several Ada libraries for these purposes, but there is little agreement on the exact details of a standard container library. A standard container library is important in terms of reusable components for efficient software engineering. Moreover it can be used for educational purposes and for efficient implementation of common algorithms and data structures.

Designing a useful standard container library for Ada is a difficult task, as the language is used in a wide variety of different domains, with different and at times conflicting demands. Hence the need for debating and elaborating the issues among a group of interested Ada users. It is the aim of the workshop to come up with the basis for a recommendation which would lead to the adoption of a standard container library as part of the Ada standard library, in the next revision of the Ada language.

Prospective participants should consult the conference web pages or directly contact the workshop Co-Chairs to learn about the terms of workshop participation.

Other Program Details

Exhibiting

Exhibition space will be provided at the Parkhotel Schönbrunn in the area of the so-called "Kaisersalon". The exhibition and a summary of the exhibits will be publicized in handouts, conference schedule, and conference program. Announcements will be made in the course of technical presentations.

Sponsoring

A sliding scale of sponsorship provides a range of benefits. All levels include display of the sponsor's logo on the conference web site and in the program.

Social Program

Several activities have already been organized. On Tuesday the City of Vienna has invited us all for a reception at the historic town hall. Before that we will enjoy a guided tour by bus that will provide a first impression of the city and several of its well-known sights.

Wednesday evening the conference banquet will take place at a famous "Heurigen" in Grinzing. Over a glass of wine and traditional Viennese cuisine we will have the opportunity to experience several of the mundane ingredients such as "Schrammel-Musik" and "Wiener Gemütlichkeit" that add to the flair of this city.

See the conference web site for more details (http://www.ada-europe.org/conference2002.html).



7th International Conference on Reliable Software Technologies - Ada-Europe 2002 Vienna, Austria, June 17-21, 2002 REGISTRATION FORM

PARTICIPANT					Ple	ease use block capitals
Ms/Mrs Mr Title						
Family name Affiliation/Organisation			F	irst name		
Street						
City	Р	ost / Zip code	e		Country	
Telephone	Fa	ax			Email	
Special requirements (e.g. diet)					
Reduced registration fee	member Ada-	Europe; natio	nal orga	nization		academia
	member ACM	; membership	numbe	r		
Additional CommentsRegistration timeEarly presented	registration (by M	fay $15^{\rm th}$)]	Late or on site	(after May 15^{th})
REGISTRATION FEES	5					
Conference registration fe	e (see table on	next page)				
Three day conference						$\dots EUR$
Individual days (Tue Wed	Thu $)\ldots$					$\dots EUR$
Tutorial/Workshop registr Please indicate tutorials/work	ration (see table shop for which ye	e on next pa ou want to reg	a ge) gister:			
Monday, June	e 17th T 1	T 2 T 3	T4			
Friday, June 2	21st T 5	Т6 Т7	T8	W		
Tutorial/Workshop regist	ration fee					$\dots EUR$
Extra Banquet ticket:	tickets @ 5	3 EUR				$\dots EUR$
Extra proceedings:	proceedings @	30 EUR				$\dots EUR$
TOTAL PAYMENT D	OUE					$\dots EUR$
PAYMENT METHOD						
By bank transfer		By chequ	le			By credit card
By bank transfer to account CA-BV Austria whose bank ic name and attach proof of pays	nt number 0130-3 lentifier (swift) co ment, e.g., a copy	0655/00, "TU ode is CABVA of the bank of	J Wien TWW (draft, to	- Ada-Eu Please me this form	rope 2002". T ention "Ada-Eu).	The account is at the prope 2002" and your
By cheque drawn on an Aus TU	trian Bank and m Wien Reliable S	nade payable t oftware Techn	to: cologies	-Ada-Euro	ope 2002.	
By credit card Master	Card Visa					
$\operatorname{Card} \#$				Ex	piration Date	
Name as shown on cred	it card			Się	gnature	
Mail or fax this form to: AE2002 Registration, CON.E0 Kaiserstr. 14, A-1070 Vienna,	CT, Event Manag Austria	gement Gesmb	ьH,			

Fax ++43 1 522 36 36-10



Conference Registration Fee:

Three days of conference (June 18th–June 20th) including one copy of the proceedings, coffee breaks, lunches, and visit and reception in town hall on Tuesday 18th.

	member Ada-Europe or ACM SIGAda		non member	
	non academia	academia	non academia	academia
Early registration (by May 15 th)	$530 \ \mathrm{EUR}$	470 EUR	590 EUR	$530 \ \mathrm{EUR}$
Late registration (after May 15 th)	590 EUR	$590 \ \mathrm{EUR}$	650 EUR	$650 \ \mathrm{EUR}$
Individual day registration (per day)	270 EUR	270 EUR	300 EUR	300 EUR

Tutorial Registration Fee:

Prices are per tutorial, including tutorial notes and coffee breaks. Lunches are only included when registered for full day tutorial or two half day tutorials on the same day.

	half day	full day or two halves on same day	Workshop (by invitation only)
$\begin{array}{c} \text{Early registration} \\ \text{(by May 15^{th})} \end{array}$	120 EUR	230 EUR	$50 \ \mathrm{EUR}$
Late registration (after May 15^{th})	$150 \ \mathrm{EUR}$	290 EUR	$70 \ \mathrm{EUR}$

Overview of Tutorials:

Monday June 17 th	T1	full day	SPARK, an "Intensive overview" – Amey/Chapman		
	Т2	full day	MaRTE OS: Bringing Embedded Systems and RT POSIX Together – $Gonzalez/Aldea$		
	T 3	morning	Principles of Physical Software Design in Ada 95 – Heaney		
	T4	afternoon	Implementing Design Patterns in Ada 95 – <i>Heaney</i>		
Friday June 21 st	T 5	full day	CORBA 3 and CORBA for Embedded Systems – Oliver		
	T 6	6 morning Using Open Source Hardware and Software to Build Reliable S Sherrill/Gaisler			
	T 7	afternoon	Cleanroom Software Engineering: An Overview – Bail		
	W	morning	Workshop: Standard Container Library for Ada – Lamm (by invitation only)		
	Т8	afternoon	Exceptions – What You Always Wanted to Know About Exceptions, But Were Afraid to Ask – <i>Colket</i>		

Note: No registration request will be confirmed until payment has been received. CANCELLATIONS must be in writing. A Cancellation fee of 120 EUR will be applied to all cancellations. No refunds will be given for cancellations postmarked after June 1st. Substitutions will be accepted. The hotel information can be found through the web page of the conference. Additional lunch tickets will be on sale throughout the conference.

For latest information see the web page at http://www.ada-europe.org/conference2002.html, or send email to ae2002-info@auto.tuwien.ac.at.

For any information, please contact:

Bettina Hainschink (Conference Secretariat), CON.ECT CON.ECT, Event Management GesmbH Kaiserstr. 14, A-1070 Vienna, Austria Tel: ++43 1 522 36 36 Fax: ++43 1 522 36 36-10 Email: events@conect.at



ORGANIZATION

Conference Chair

Gerhard H. Schildt Technical University Vienna Department of Computer-Aided Automation Schildt@auto.tuwien.ac.at

Program Co-Chairs

Johann Blieberger Technical University Vienna Department of Computer-Aided Automation Blieberger@auto.tuwien.ac.at

Alfred Strohmeier Swiss Fed. Inst. of Technology Lausanne Software Engineering Lab Alfred.Strohmeier@epfl.ch

In cooperation with



SIGAda

Tutorial Chair

Helge Hagenauer University of Salzburg Dept. Comp. Science & System Analysis hagenau@cosy.sbg.ac.at

Exhibition Chair

Thomas Gruber Austrian Research Centers Seibersdorf thomas.gruber@arcs.ac.at

Publicity Chair

Dirk Craeynest Offis nv/sa & K.U.Leuven Dirk.Craeynest@cs.kuleuven.ac.be

Local Organization Chair

Bernd Burgstaller Technical University Vienna Department of Computer-Aided Automation Burgstaller@auto.tuwien.ac.at

TU TECHNISCHE UNIVERSITÄT WIEN

seibersdorf research An Enterprise of the Austrian Research Centers.

the exhibitors (preliminary list)



and the supporters (preliminary list) of the conference.



Document Version 1.0