



23<sup>rd</sup> International Conference on  
**RELIABLE SOFTWARE TECHNOLOGIES**

# Ada-Europe 2018



18-22 June 2018, Lisbon, Portugal

## FINAL PROGRAM

<http://www.ada-europe.org/conference2018>

In cooperation with



Ada Resource Association

## PRESENTATION

In 2018, the 23<sup>rd</sup> International Conference on Reliable Software Technologies - Ada-Europe 2018 - takes place in Lisbon, Portugal, from 18 to 22 of June. The conference is the latest in a series of annual international conferences started in the early 80's, under the auspices of Ada-Europe, the international organization that promotes knowledge and use of Ada and Reliable Software in general into academia, research and industry.

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

The conference program includes three days with keynote talks, refereed papers, sessions with industrial presentations, an industrial exhibition and two days of

tutorials and co-located workshops. A new workshop on “Runtime Verification and Monitoring Technologies for Embedded Systems” (RUME) will take place on Monday and, on Friday, the program will be complemented with the 5<sup>th</sup> workshop on “Challenges and new Approaches for Dependable and Cyber-Physical Systems Engineering” (DeCPS). There are also social events, including a welcome reception on Tuesday 19<sup>th</sup>, after the Ada-Europe General Assembly, and a conference banquet on Wednesday 20<sup>th</sup>.

Lisbon is currently considered one of the best touristic cities in Europe. It is the capital of Portugal and is well known for its medieval castle, for the Belém tower, for the natural light and breath-taking scenery views, and for so many other nice things that you should discover for yourself.

Ada-Europe 2018 provides a unique opportunity for dialogue and collaboration between academics and industrial practitioners interested in reliable software.

## OVERVIEW OF THE WEEK

	Morning	Late Morning	After Lunch	Afternoon
Monday June 18 <sup>th</sup> Tutorials & Workshop	Tutorial: P. Chapin, <i>Recent Developments in SPARK 2014</i>			
	Tutorial: J.P. Rosen, <i>Access Types and Memory Management in Ada 2012</i>		Tutorial: J.P. Rosen, <i>Numerics for the Non-Numerical Analyst</i>	
	Tutorial: W. Bail, <i>Design and Architecture Guidelines for Trustworthy Systems</i>		Tutorial: W. Bail, <i>Requirements Development for Safety- and Security-Critical Systems</i>	
	Workshop: <i>Runtime Verification and Monitoring Technologies for Embedded Systems</i>			
Tuesday June 19 <sup>th</sup> Sessions & Exhibition	Keynote Talk: Paulo Veríssimo <i>(Univ. of Luxembourg)</i>	Regular Session: <i>Safety and Security</i>	Industrial Session: <i>Ada in Industry</i>	Regular Session: <i>Ada 202X</i>
Wednesday June 20 <sup>th</sup> Sessions & Exhibition	Keynote Talk: Carl Brandon <i>(VTC, USA)</i>	Regular Session: <i>Handling Implicit Overhead</i>	Industrial Session: <i>Space Systems</i>	Regular Session: <i>Real-Time Scheduling</i>
Thursday June 21 <sup>st</sup> Sessions & Exhibition	Keynote Talk: Erhard Plödereder <i>(Univ. of Stuttgart, Germany)</i>	Industrial Session: <i>V&amp;V of Safety-Critical Software</i>	Industrial Session: <i>Software Methodologies</i>	Regular Session: <i>New Application Domains</i>
Friday June 22 <sup>nd</sup> Tutorials & Workshop	Tutorial: F. Singhoff and P. Dissaux, <i>Scheduling Analysis of AADL Architecture Models</i>			
	Tutorial: J. Sparre Andersen, <i>Writing Contracts in Ada</i>		Tutorial: J. Sparre Andersen, <i>Unit-Testing with Ahven</i>	
	Tutorial: R. Amiard and P.M. Rodat, <i>Introduction to Libadalang</i>		Tutorial: J. Signoles, <i>Frama-C, a Framework for Analysing C Code</i>	
	Workshop: <i>Challenges and new Approaches for Dependable and Cyber-Physical Systems Engineering</i>			

## KEYNOTE SPEAKERS

### Security and Dependability Challenges of IT/OT Integration

**Paulo Esteves-Veríssimo**

University of Luxembourg, Luxembourg

**(Tuesday June 19<sup>th</sup>)**

A great deal of society's stakes is today placed on the cyber sphere. The pillars of this new environment are critical information infrastructures (CII), where an accelerated convergence, or integration, of information technology (IT) like the internet-cloud complex, and operational technology (OT) like cyber-physical systems, is becoming the norm e.g., in utilities, like power grid operators, or transportation systems, including autonomous vehicles. This global convergence leads to extremely large-scale and decentralised computer and network systems, in whose interconnection the natural difference of the threat and risk models of both kinds of realms (IT/OT) is sometimes not taken into account, opening threat surfaces both to occasional accidents and targeted attacks, or advanced persistent threats (APT).

We believe, and discuss in the talk, that paradigms and techniques are required that endow systems with the capacity of defeating incremental adversary power and sustaining perpetual and unattended operation, in a systematic and automatic way.

#### Short Bio



Paulo Esteves-Veríssimo is a Professor and FNR PEARL Chair at the University of Luxembourg Faculty of Science, Technology and Communication (FSTC), since fall 2014, and head of the CritiX lab (Critical and Extreme Security and Dependability) at SnT, the

Interdisciplinary Centre for Security, Reliability and Trust at the same University (<https://www.wen.uni.lu/snt>). He is adjunct Professor of the ECE Dept., Carnegie Mellon University. Previously, he has been a Professor of the Univ. of Lisbon, member of the Board of the same university and Director of LaSIGE (<http://lasige.di.fc.ul.pt>). Veríssimo is Fellow of the IEEE and Fellow of the ACM, and he is associate editor of the IEEE Transactions on Computers (TC - 2015---). He is currently Chair of the IFIP WG 10.4 on Dependable Computing and Fault-Tolerance and vice-Chair of the Steering Committee of the IEEE/IFIP DSN conference. He

is currently interested in secure and dependable distributed architectures, middleware and algorithms for: resilience of large-scale systems and critical infrastructures, privacy and integrity of highly sensitive data, and adaptability and safety of real-time networked embedded systems. He is author of over 180 peer-refereed publications and co-author of 5 books.

### From Physicist to Rocket Scientist, and how to make a CubeSat that works

**Carl Brandon**

Vermont Technical College, USA

**(Wednesday June 20<sup>th</sup>)**

After getting experience with SPARK/Ada on an Artic Sea Ice Buoy, we used the same CPU and software system on our first CubeSat. Our CubeSat, launched on November 13, 2013, was in orbit for two years and two days, travelling 293 million miles during 11,071 orbits of the Earth. It was operational the entire time, sending us many photos, until burning up over the Pacific during re-entry. It is still the only successful university satellite on the East coast of the US. I will explain how to have a successful CubeSat, where many, many others have failed, in which the reliability of SPARK/Ada software plays a big part. We are now developing a complete spacecraft software system, CubedOS, using SPARK/Ada, and are looking forward to being part of a deep space, self-propelled CubeSat mission with partners at NASA's Jet Propulsion Lab, visiting asteroids controlled by SPARK/Ada software.

#### Short Bio



I was interested in space from an early age, but my education led to a B.S. in physics from Michigan State. I worked on the cyclotron there, starting out with a vacuum tube computer. Then at IBM, with two colleagues, I designed their first memory chip. I used computer analysis for my M.S. on the aerodynamics of seagull soaring flight and Ph.D. on bat flight aerodynamics and flight mechanics with bats flying in a wind tunnel, at UMass, Amherst. I got involved with Ada at its beginning, teaching the first undergrad course in Ada in the early 1980's. I just finished my 41st year teaching physics at Vermont Technical College. 13 years ago, I got involved with CubeSats (10 cm x 10 cm x 10 cm, 1 kg satellites). Being a physicist (with a good software



background) is a great background for CubeSats. We built the first CubeSat launched by any university in New England or New York. We credit our success with the use of SPARK/Ada for our software. We are now working on a complete spacecraft software package, CubedOS written in SPARK/Ada.

## Vulnerabilities in Safety, Security, and Privacy

### Prof. Dr. Erhard Plödereder

University of Stuttgart, Germany

(Thursday June 21<sup>st</sup>)

Prof. Plödereder will discuss the differences and commonalities in threats that affect safety, security or privacy in today's systems. He will argue that vulnerabilities made possible by programming language features form a common base for violating safety, security, or privacy. None of these three concerns can be satisfied without first eliminating these vulnerabilities in the code of today's systems. Regrettably all known languages in actual use contain constructs that give rise to such vulnerabilities. He will describe several useful information sources about vulnerabilities and about rules that are geared to prevent them from arising in real code.

Examples will illustrate the knowledge conveyed by these sources.

### Short Bio



Erhard Plödereder holds the Chair for Programming Languages and Compilers at the University of Stuttgart, Germany. His research interests are static program analysis tools to detect vulnerabilities in safety-critical code. He is a member of ISO WG23, which focuses on

identifying vulnerabilities in programming languages and on providing advice for their prevention generally and in various programming languages.

In the past Erhard Plödereder was president of Ada-Europe (2001-2008), chairman of IFIP 2.4. (2002-2008), ISO WG9/ARG (1994-2001), ISO WG9/XRG and the Distinguished Reviewers for Ada95 (1989-1994), and maintains an active involvement in today's Ada and ISO groups. He served as vice dean and dean at the Faculty of Computer Science, Electrical Engineering and Information Technology of the University of Stuttgart (1998-2010). He earned M.Sc. and Ph.D. degrees at Harvard University and a Diploma in Computer Science at the TU Munich, Germany.

# Revolutionize your software verification

+ *Efficiency, Automation, Reliability* +



 **RAPITA** Systems Ltd  
A DARWIN Company

**Unit testing · System testing · Coverage analysis · Timing analysis**

**V&V services · Multicore timing services · DO-178C training**

**Ada · C · C++**

[www.rapitasystems.com](http://www.rapitasystems.com)

## TUTORIALS

### T1 – Recent Developments in SPARK 2014

Peter Chapin, Vermont Technical College, USA

**(Monday June 18<sup>th</sup>, full day)**

This tutorial will quickly cover the basics of SPARK 2014 for the benefit of those attendees who have no SPARK 2014 experience (assumed to be the majority of the attendees). This overview will not cover every detail of SPARK. Instead it will provide the necessary background so that the newer features of SPARK can be understood. The bulk of the time will focus on the newer features that have been added to SPARK in recent years, along with some general comments about where SPARK development may be heading in the future. Sample code will be provided in machine readable form, so attendees can experiment with SPARK first hand during allocated “lab” times during the tutorial. Attendees are encouraged to bring a computer.

**Level:** *Intermediate*

Attendees should have working familiarity with Ada including exposure to, but not necessarily expertise with, Ada’s concurrency and object-oriented features. No prior experience with SPARK is required. Experienced SPARK users who are interested in SPARK’s newer features are also welcome.

#### Reasons for attending

Attendees will leave the tutorial with a general understanding of SPARK’s abilities and of the direction SPARK development has been moving. Attendees will be in a good position to explore SPARK further by trying it on their own projects.

#### Presenter



Dr. Chapin is a professor of software engineering at Vermont Technical College (VTC) in the United States. He has been a faculty member there for 32 years and has taught both Ada and SPARK to undergraduate and graduate

students. He is a co-author, along with John McCormick, of “Building High Integrity Applications with SPARK”, published by Cambridge University Press in 2015. Dr. Chapin has been the Software Directory at VTC’s CubeSat Laboratory since 2009 where he has overseen the development of CubeSat flight software in SPARK done by students.

### T2 – Access Types and Memory Management in Ada 2012

Jean-Pierre Rosen, Adalog, France

**(Monday June 18<sup>th</sup>, morning)**

In most languages, pointers are either low-level (pure hardware addresses in C), or implicit (Java, C#). Ada provides explicit pointers, but of a higher level of abstraction (hence the use of the term “access”), disconnected from the hardware level, and as safe as possible. In addition, the language includes sophisticated features for controlling memory allocation and deallocation. While this has great benefits, it may confuse those who are used to pointers in other languages. Proper usage also requires some difficult to grasp notions, like accessibility levels. This tutorial explains all the issues with Ada access types, from basic usage to sophisticated features like remote access types. Many practical examples demonstrate how to use them and how to control memory allocation, and special emphasis is provided for the latest features offered by Ada 2005 and 2012. A must-attend for all those using access types.

**Level:** *Intermediate*

Expected audience experience: casual knowledge of Ada.

#### Reasons for attending

- Understand what makes Ada access types different from other languages’ pointers.
- Explore rarely taught issues, like accessibility levels, storage pools and subpools, remote access types...
- Learn when and how to use access types – and when not to use them.

#### Presenter



J.P. Rosen is a professional teacher, teaching Ada (since 1979, it was preliminary Ada!), methods, and software engineering. He runs Adalog, a company specialized in providing training, consultancy, and services in all areas connected

to the Ada language and software engineering. He is chairman of AFNOR’s (French standardization body) Ada group, AFNOR’s spokesperson at WG9, member of the Vulnerabilities group of WG9, and chairman of Ada-France. Adalog offers regularly on-site and off-site training sessions in Ada. This tutorial is based in part on the “advanced Ada” course offered by Adalog.

### T3 – Design and Architecture Guidelines for Trustworthy Systems

William Bail, The MITRE Corporation, USA

**(Monday June 18<sup>th</sup>, morning)**

Software design and architecture together play a central role in software development. Understanding their concepts and principles is essential to being able to develop a trustworthy and dependable software system. This tutorial examines these concepts, discusses design quality attributes necessary to ensure trustworthy behaviour, and provides an overview of different design approaches. It will differentiate architecture and design, their relationship to coding styles, and describe examples of good and faulty design. It will introduce a variety of design challenges that are commonly encountered and will discuss the impact of complexity in the quality of the software, recognizing that complexity presents significant risk to the dependable design understood by developers. Design features need to be correlated to counteract potential threats to security and safety. All designs have inherent properties, but not all designs have the same properties, resulting in a need to select a design for a system that is coherent with the system's intended role and usage profile.

**Level:** *Intermediate / Advanced*

Targeted at practitioners who are involved in designing and developing complex systems which have high dependability and trust requirements.

#### Reasons for attending

The tutorial will provide a perspective on the roles of design and architecture in the development of software intensive systems that have safety and cyber-secure roles, and will provide guidance on how to approach such development. As such, it will directly support process improvement, and provide a basis for achieving trustworthy performance. It emphasizes the role of design features that enhance achieving desirable dependability goals. It recommends practical approaches for soliciting, deriving and documenting design features.

#### Presenter



Since 1990, Dr. Bail has worked for The MITRE Corporation in McLean VA as a Computer Scientist in the Software Engineering Center (SWEC). MITRE is a not-for-profit corporation chartered to provide systems engineering services to the

U.S. Government agencies, including the DoD, the FAA, and the IRS. Within MITRE, the SWEC focuses on supporting various programs with consultation, particularly transitioning emerging technologies into practice. Dr. Bail has been involved with establishing modular open system guidance and policy for multiple customers.

Dr. Bail's technical areas of focus include dependable software design and assessment, error handling policies, techniques for software specification development, design methodologies, metric definition and application, and verification and validation. Prior to 1990, Dr. Bail worked at Intermetrics Inc. in Bethesda MD.

From 1989 to 2011, he served as a part-time Adjunct Professor at the University of Maryland University College where he developed instructional materials and taught courses in software engineering, in topics such as Software Requirements, Verification and Validation, Software Design, Software Engineering, Fault Tolerant Software, and others. Previously, Dr. Bail taught part-time at The University of Maryland from 1983-1986 in the Computer Science Department for undergraduate courses in discrete mathematics, computer architecture, and programming language theory.

Dr. Bail has presented tutorials on Cleanroom Software Engineering, Semi-Formal Development Techniques, Statistical Testing, Verification and Validation, and Requirements Engineering at SIGAda, Ada-Europe, NDIA Systems Engineering Conference, and other conferences. Dr. Bail received a BS in Mathematics from Carnegie Institute of Technology, and an MS and Ph.D. in Computer Science from the University of Maryland.

### T4 – Numerics for the Non-Numerical Analyst

Jean-Pierre Rosen, Adalog, France

**(Monday June 18<sup>th</sup>, afternoon)**

Numerics are a special area of software development, and numerically intensive programs are best developed by specialists of the domain. On the other hand, many programs have to deal with mathematical computations, without being really numerically intensive.

This tutorial addresses the techniques (and pitfalls) that every application developer needs to know as soon as there are some computations that go beyond simple integer arithmetic, without requiring them to be advanced numerical analysts. The tutorial also addresses the various tools offered by Ada, from numeric types to libraries.



**Level:** *Intermediate*

Expected audience experience: casual knowledge of Ada.

**Reasons for attending**

- Learn how to select the most appropriate numeric type for your applications.
- Avoid pitfalls and increase the accuracy and portability of numeric computations.
- Discover the standard libraries provided by Ada.

**Presenter**

Please see Tutorial T2.

## T5 - Requirements Development for Safety- and Security-Critical Systems

William Bail, The MITRE Corporation, USA

**(Monday June 18<sup>th</sup>, afternoon)**

The requirements defined for a system form the foundation for the development of the system, and as such, are fundamentally core to the successful realization and delivery of the system to the eventual users. Cost and schedule increases in the development of systems, and shortcomings in deployed systems are closely correlated to weaknesses in the system's requirements. Some historic data suggests that requirements are responsible for nearly half of all system development failures. For dependable systems, shortcomings in requirements development have an especially dramatic impact. For example, systems requiring a high level of security are often not addressed until later in the development process. This tutorial discusses shortcomings in current practices, and provides guidance for enhanced practices that address historic shortcomings. It also provides an approach to weighing trade-offs associated with ambitious goals and realistic limits, and recognizes the complex and multiple interplays between different requirements. It specifically addresses the issue of stakeholder acceptability, allowing trade-offs of various system qualities to determine overall system acceptance. It also emphasizes the tight relationship between design and requirements development, showing how good practice can directly improve the quality of the resulting system. The tutorial describes the ways that requirements need to be handled to maximize the likelihood of success. This tutorial has been updated significantly from versions presented at previous Ada-Europe conferences.

**Level:** *Intermediate / Advanced*

Targeted at practitioners who are involved in developing complex systems which have high dependability and trust requirements.

**Reasons for attending**

The tutorial will provide a framework for development of requirements for cyber and safety critical systems and provide advice on how to approach such development. As such, it will directly support process improvement, and provide a basis for a predictable and reliable requirements development activity. It justifies the level of attention that needs to be placed on the development and maturation of system and software requirements. It supports obtaining a perspective against which requirements can be viewed and suggests practical approaches for soliciting and documenting requirements. It will explain the underlying basis for how requirements need to be handled and will provide solutions for some commonly-encountered challenges when developing requirements for large, software-intensive systems.

**Presenter**

Please see Tutorial T3.

## T6 – Scheduling Analysis of AADL Architecture Models

Frank Singhoff, Lab-STICC/UBO, France

Pierre Dissaux, Ellidiss Technologies, France

**(Friday June 22<sup>nd</sup>, full day)**

In this tutorial, we will provide an overview of scheduling analysis capabilities that are proposed by the real-time scheduling theory, AADL and tools implementing it. The objective of this tutorial is to show to the attendees the benefits that can be expected by performing early scheduling/timing analysis for real-time software.

The Architecture Analysis and Design Language (AADL) is an SAE International Standard dedicated to precise modeling of complex embedded systems, covering both hardware and software concerns. Its definition relies on a precise set of concepts inherited from industry and academics best practice: clear separation of concerns among layers, rich set of properties to document system metrics and support for many kind of analysis: scheduling, safety and reliability, performance, but also code generation.

14 years after the first release of the AADL standard, the AADL community has implemented many AADL tools that are mature enough to be handled by embedded critical real-time systems designers. Then, we propose in this tutorial to show how to apply AADL scheduling analysis

tools. The tutorial will be illustrated by AADL models and labs with the tools AADLInspector and Cheddar.

Cheddar is a GPL open-source scheduling analysis tool (<http://beru.univ-brest.fr/~singhoff/cheddar>). It has been designed and distributed to allow users to understand the main concepts of the real-time scheduling theory. The tool is built around a simplified Architecture Description Language devoted to support real-time constructs. Users can directly build their real-time systems models with this ADL and its associated editor, however, it is expected that other more general modeling front-ends have to be used while integrating scheduling analysis into an engineering process.

AADLInspector (<http://www.ellidiss.fr>) is a model processing framework that embeds a set of generic features to load real-time models and let them be properly processed by various analysis or production tools. AADLInspector uses AADL V2 standard as a base reference for its input models and embeds a commercial version of Cheddar as well as the interactive Marzhin simulator that emulates the AADL run-time.

The tutorial will illustrate how to model typical real-time architectures with AADL V2 and how to analyse them

with AADLInspector/Cheddar (both the GPL version and the commercial version embedded into AADLInspector).

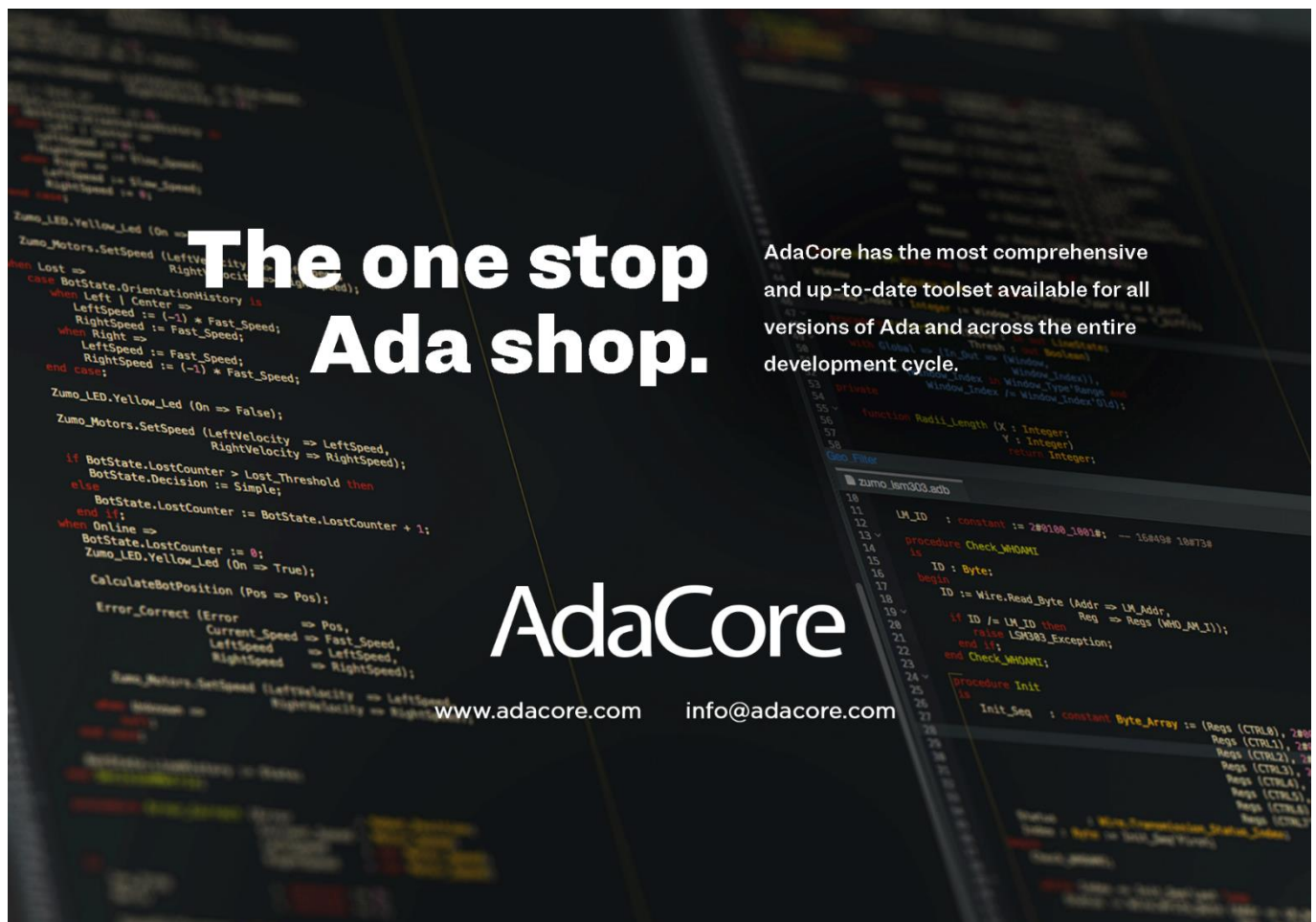
#### Level: *Intermediate*

The tutorial is designed for attendees who have no background on AADL nor scheduling analysis. Modelling and verification background may help.

#### Reasons for attending

AADL is notation which is part of the model-based families, along with OMG SysML, MARTE or EASTADL. It has been defined with a strong focus on analysis capabilities from its inception, while being versatile enough to be applied to a wide set of embedded systems. European projects (FP5-ASSERT, TASTE, Flex-eWare), but also US projects (SAVI, Meta) demonstrated that AADL could help engineers in their design effort in the space, avionics and embedded domains. In the meantime, the academic community adopted AADL as a conveyor to bind numerous tools, covering model checking, scheduling, power evaluation or simulation capabilities to name a few.

Furthermore, scheduling analysis is not used as much as it could be, because many practitioners may find it



**The one stop  
Ada shop.**

**AdaCore**

[www.adacore.com](http://www.adacore.com)    [info@adacore.com](mailto:info@adacore.com)

AdaCore has the most comprehensive and up-to-date toolset available for all versions of Ada and across the entire development cycle.



difficult to apply. The motivation of the tutorial is to highlight the level of maturity of the real-time modelling and analysis solutions around AADL, which is an outcome of the past ten years of academic and industrial research work in this area.

## Presenters



Frank Singhoff (UBO/Lab-STICC, Brest, France) is Professor of Computer Science in the Lab-STICC laboratory, UMR CNRS 6285 and in the Computer Science Department at the Université de Bretagne Occidentale, France. He received

his engineering degree in Computer Science from the CNAM/Paris in 1996 and his PhD from Télécom-Paris-Tech in 1999. His current research focuses on real-time scheduling analysis and architecture description languages on multi- and many-cores. In 2002, he started Cheddar, a toolset designed to perform analysis with the real-time scheduling theory. Frank Singhoff is also a member of the SAE AS-2C committee working on AADL. He received an ACM SIGAda “Outstanding Ada Community Contributions Award” in 2010. Frank Singhoff gave several tutorials at ESWeek in 2013, MODELS in 2014, HILT in 2014, SIGAda in 2011 and 2007, Ada-Europe in 2008, ETR in 2017, 2015 and 2009.



Pierre Dissaux has an engineering degree in electronics and is the owner and managing director of Ellidiss Technologies. Before founding the company in 2004, he held various job positions in a large telecommunication company

(1983-1985), in a research center of the French Ministry of Defense (1985-1991) and in an innovating software house (1991-2003). He is also a member of the SAE AS-2C standardisation committee (AADL) and the main architect of the AADL Inspector tool.

## T7 – Writing Contracts in Ada

Jacob Sparre Andersen, JSA Research & Innovation, Denmark

(Friday June 22<sup>nd</sup>, morning)

One of the important new features in Ada 2012 was an extended support for contract-based programming with “contract aspects”. They allow you to specify even more details about types and subprograms in a formal and testable form. If used carefully, they can make package specifications easier to read, and help identifying use and implementation errors faster.

To really make sense, the contracts should be consistent across your whole library or application. This tutorial will introduce you to writing contracts in Ada and give you guidance on writing consistent contracts. It is organised in three sections: an introduction to writing contracts in Ada using features all the way from Ada 83 to Ada 2012/TC1. Guidelines for writing contracts. And, finally, a guided, practical exercise in writing contracts in Ada.

**Level:** *Intermediate*

The intended audience is software engineers, who already know an earlier version of Ada, but have not yet used the “programming by contract” aspects added in Ada 2012.

### Reasons for attending

After having completed the tutorial, the participants will be ready to apply contract aspects on a project in a consistent and effective manner.

The tutorial is intended to prepare existing Ada programmers to use Ada 2012 contract aspects, both in future projects and on existing Ada projects.

### Presenter



Jacob Sparre Andersen has previously given talks and tutorials on the use of Ada 2012 for contract-based programming at Ada-Europe conferences, as well as at DANSAS, FOSDEM and LinuxDay/Cagliari. He also has a long experience as a teacher of physics, mathematics, statistics, software engineering, and financial instruments.

Jacob Sparre Andersen runs his own consulting company in Hørsholm, Denmark and is an associate at the Niels Bohr Institute at University of Copenhagen. He is specialised in mathematical modelling and (of course) Ada. See <http://www.jacob-sparre.dk/cv/> for a full curriculum vitae.



Join Ada-Europe!

Become a member of Ada-Europe and support Ada-related activities and the future development of the Ada programming language.

To apply for membership visit our web page at <http://www.ada-europe.org/join>



## T8 – Introduction to Libadalang

Raphaël Amiard, AdaCore, France  
Pierre-Marie de Rodat, AdaCore, France

**(Friday June 22<sup>nd</sup>, morning)**

This tutorial will introduce the Libadalang Ada source code analysis library, and the way it can be used to create source aware custom tools.

It will cover: 1) How to use Libadalang for simple metrics using syntax; 2) How to use Libadalang for simple metrics using semantic analysis; 3) How to use Libadalang to perform automatic refactorings on your code-base based on a set of rules; 4) How to use Libadalang to implement checkers for custom coding rules.

Attendees should bring a computer with GNAT GPL 2017 installed. These are available for download from <https://adacore.com/download>.

**Level:** *Intermediate*

No prior experience with Libadalang is expected, but attendees should be familiar with Ada. A modicum of familiarity with Python or another scripting language is a plus, but definitely not a requirement.

### Reasons for attending

- Learn about creating custom Ada tooling easily.
- Learn about the main differences between Libadalang and ASIS.
- See real world uses of custom made source analysis technology.

### Presenters



Raphaël Amiard is a software engineer at AdaCore working on tooling and compiler technologies. He joined AdaCore in 2013, after an internship on AdaCore's IDEs. His main interests are compiler technologies, language design, and sound/music making.



Pierre-Marie joined AdaCore in 2013, after he got an engineering degree at EPITA (IT engineering school in Paris). He mainly works on GNATcoverage, GCC, GDB and Libadalang.

ptc<sup>®</sup> apexada | ptc<sup>®</sup> objectada<sup>®</sup>

## Complete Ada Solutions for Complex Mission-Critical Systems

- Fast, efficient code generation
- Native or embedded systems deployment
- Support for leading real-time operating systems or bare systems
- Full Ada tasking or deterministic real-time execution

Learn more by visiting: [ptc.com/developer-tools](http://ptc.com/developer-tools)



## T9 – Unit-Testing with Ahven

Jacob Sparre Andersen, JSA Research & Innovation, denmark

**(Friday June 22<sup>nd</sup>, afternoon)**

Testing is a useful activity, even when you don't have authorities breathing down your neck to document that you know what your software is doing.

Ahven is an Open Source framework for writing unit tests. It is intended to work with any Ada 95 compiler and is regularly tested with several different compilers.

This tutorial will introduce you to writing unit tests with Ahven as the testing framework. You will learn how to write simple tests, how to structure larger test suites, and how you can measure statement coverage of your unit tests with GNAT and Gcov.

**Level:** *Intermediate*

The intended audience is software engineers, who already know Ada, and are interested in a lightweight alternative to the unit testing tools used for certification purposes.

### Reasons for attending

The tutorial will give you a good start writing unit tests, without tying you to a specific Ada compiler, or requiring you to pay license fees for one of the more advanced closed source Ada unit testing tools.

### Presenter

Please see Tutorial T7.

## T10 – Frama-C, a Framework for Analysing C Code

Julien Signoles, CEA LIST

**(Friday June 22<sup>nd</sup>, afternoon)**

Frama-C is an extensible source code analysis platform that aims at conducting verification of industrial-size C programs. It provides its users with a collection of plug-ins that perform static and dynamic analysis for safety-

and security-critical software. Collaborative verification across cooperating plug-ins is enabled by their integration on top of a shared kernel, and their compliance with a common formal specification language named ACSL. Frama-C is currently used in several industrial settings, notably (but not limited to) avionic, nuclear and defense industries.

This tutorial on Frama-C takes participants on a journey into the Frama-C world along its main plug-ins: the deductive verification tool WP, the abstract-interpretation based plug-in Eva, and the run-time verification tool E-ACSL. It also includes a presentation of the formal specification language ACSL and emphasizes possible collaborations between these plug-ins and a few others. The presentation is illustrated with concrete examples of C programs.

**Level:** *Introductory / Intermediate*

Attendees should know the C programming language but no former experience with formal methods is required.

### Reasons for attending

- If you don't know formal methods: learn what they are (not) good for and how to use them concretely.
- If you already know formal methods and a verification tool for another programming language (e.g. SPARK 2014), learn a state-of-the-art tool currently used for analysing critical C software.

### Presenter



Dr Julien Signoles is a researcher-engineer at CEA LIST's Software Security and Reliability Lab (LSL) in France and one of the main developers of Frama-C. His research focuses on runtime assertion checking, software

security, and applications of program analysis techniques. He has already delivered many lectures and tutorials and provides professional training on Frama-C and its plug-ins.

Morning tutorial sessions run from 09:30 to 13:00, with a break 11:00-11:30. Afternoon tutorial sessions run from 14:00 to 17:30 with a break 15:30-16:00.

## CO-LOCATED WORKSHOPS

The conference week features two workshops, which will run in parallel with the tutorials. On Monday, June 18<sup>th</sup>, takes place the workshop on Runtime Verification and Monitoring Technologies for Embedded Systems (RUME), while the 5<sup>th</sup> edition of the International Workshop on Challenges and new Approaches for Dependable and Cyber-Physical Systems Engineering (DeCPS) is on Friday, June 22<sup>nd</sup>.





## SOCIAL EVENTS

The program includes 1-hour long coffee breaks, providing the opportunity for participants to discuss their work, to visit the exhibition and to socialise. Lunches will be served at the hotel restaurant, from Monday to Friday, providing further interaction opportunities.

### WATERX CATAMARAN



The welcome reception will take place on Tuesday, after the Ada-Europe General Assembly. It will be on board of a modern catamaran, which will take participants down the Tagus river to see Lisbon from a different perspective and watch the sunset from the river. The tour will take approximately 2 hours, from 20h00 to 22h00, departing and returning to the marina of Parque das Nações. This is walking distance from the conference hotel and a suggested path is provided in the image on the right. Given that the tour will be during dinner time, we will have some food on board, accompanied with a welcome glass of Champagne and an open bar with several other drinks (beer, juice, water, coffee). The food will include cheese, smoked ham, and a variety of typical Portuguese appetizers such as miniature chicken pies, miniature puff pastry with chèvre cheese and red fruits, miniature veal croquettes, miniature shrimp patties and two additional vegetarian appetizers. A couple of sweets (before you ask, yes, including mini Pastéis de Belém, the very typical Lisbon sweet) will complement this menu.



And on Wednesday, the day will end with the conference banquet, at the “Casa do Bacalhau” restaurant. The restaurant name means "The House of the Codfish", so it is not too difficult to guess what is its main speciality.

The restaurant is located in the old stables of the Duke of Lafões palace. In fact, the Duke and his family still live today in another part of the building where the restaurant is located. The palace was built after the great earthquake of 1755 that destroyed most of the city (the Lisboa Story Center, which you may visit in downtown Lisbon, tells it all), because the palace in which the Duke's family was living at that

date was partially destroyed. When it was built, there was almost nothing around it and the Tagus river was reaching almost to its entry. The room where dinner will be served has a wonderful ceiling, which is original from the eighteenth century, built in vault with a typical brick. We hope you enjoy the food and the wine!





## CONFERENCE SCHEDULE

	Tuesday 19 <sup>th</sup>	Wednesday 20 <sup>th</sup>	Thursday 21 <sup>st</sup>
8:45 - 9:00	<b>Welcome &amp; Opening</b>		
9:00 - 10:00	<b>Keynote Talk</b> Chair: António Casimiro <i>Security and Dependability Challenges of IT/OT Integration</i> Paulo Esteves-Veríssimo University of Luxembourg, Luxembourg	<b>Keynote Talk</b> Chair: Marco Panunzio <i>From Physicist to Rocket Scientist, and How to Make a CubeSat that Works</i> Carl Brandon Vermont Technical College, USA	<b>Keynote Talk</b> Chair: Tullio Vardanega <i>Vulnerabilities in Safety, Security, and Privacy</i> Erhard Plödereder University of Stuttgart, Germany
10:00 - 11:00	<b>Coffee &amp; Exhibition</b>	<b>Coffee &amp; Exhibition</b>	<b>Coffee &amp; Exhibition</b>
11:00 - 11:30	<b>Regular Session: Safety and Security</b> Chair: Marcus Völz	<b>Regular Session: Handling Implicit Overhead</b> Chair: Michael González Harbour	<b>Industrial Session: V&amp;V of Safety-Critical Software</b> Chair: Johann Blieberger
	<i>Using Safety Contracts to Verify Design Assumptions During Runtime</i> O. Jaradat and S. Punnekkat	<i>On the Effect of Protected Entry Servicing Policies on the Response Time of Ada Tasks</i> J. Garrido, J. Zamorano, A. Alonso and J. A. de La Puente	<i>Applying Formal Timing Analysis to Satellite Software</i> A. Wortmann
	<i>Tool-Supported Safety-Relevant Component Reuse: From Specification to Argumentation</i> I. Sljivo, B. Gallina, J. Carlson, H. Hansson and S. Puri	<i>Improved Cache-Related Preemption Delay Estimation for Fixed Preemption Point Scheduling</i> F. Markovic, J. Carlson and R. Dobrin	<i>Multicore Timing Analysis for Safety-Critical Software</i> I. Broster, G. Bernat, F. Cazorla, C. Evripidou and S. Milutinovic
	<b>Presentation</b> <i>The IRONSIDES Project: Final Report</i> B. Fagin and M. Carlisle	<b>Vendor presentation</b> AdaCore	<i>KhronoSim: Simulation and Testing of Real-Time Critical Cyber-Physical Systems</i> G. Gouveia, J. Esteves, C. Maia and L. M. Pinho
12:00 - 12:20			
12:20 - 12:40	<b>Presentation</b> <i>Concurrent Reactive Objects in Rust - Secure by Construction</i> M. Lindner, J. Aparicio and P. Lindgren	<b>Vendor presentation</b> PTC	
12:40 - 14:00	<b>Lunch &amp; Exhibition</b>	<b>Lunch &amp; Exhibition</b>	<b>Lunch &amp; Exhibition</b>

Conference sessions take place in the hotel auditorium. Coffee breaks take place in the Exhibition hall (rooms Ruby 1+2+3). Lunch will be in the hotel restaurant.





	Tuesday 19 <sup>th</sup>	Wednesday 20 <sup>th</sup>	Thursday 21 <sup>st</sup>
	<b>Industrial Session: Ada in Industry</b> Chair: Philippe Gast	<b>Industrial Session: Space Systems</b> Chair: Maurizio Martignano	<b>Industrial Session: Software Methodologies</b> Chair: Andreas Wortmann
14:00 - 14:30	<i>Managing the Endianness of Software Building Blocks with GNAT Ada Pragmas: a Case Study</i> P. L. Cueva and M. Panunzio	<i>Ariane 6 Flight Software Designed for a Simpler Validation</i> P. Gast and C. Pierre	<i>C Guidelines Compliance and Deviations (the MISRA and CERT Cases)</i> M. Martignano
14:30 - 15:00	<i>Using Ada in Non-Ada Systems</i> A. Marriott	<i>I3DS – A Modular Sensor Suite for Space Robotics</i> K. N. Gregertsen	<i>Agile in Safety Critical Projects</i> P. Zakrzewski
15:00 - 15:30	<i>Easy Ada Tooling with Libadalang</i> P.-M. de Rodat and R. Amiard	<i>Multi-Concern Dependability-Centered Assurance for Space Systems via ConcertoFLA</i> B. Gallina, Z. Haider, A. Carlsson, S. Mazzini and S. Puri	<i>AGILE-R: Agile Software Development for Railways</i> S. Mazzini, J. Favaro, G. Ioele, P. Panaroni, G. Gennaro and U. Paone
15:30 - 16:30	<b>Coffee &amp; Exhibition</b>	<b>Coffee &amp; Exhibition</b>	<b>Coffee &amp; Exhibition</b>
	<b>Regular Session: Ada 202X</b> Chair: Luís Miguel Pinho	<b>Regular Session: Real-Time Scheduling</b> Chair: Frank Singhoff	<b>Regular Session: New Application Domains</b> Chair: Jorge Real
16:30 - 17:00	<i>Safe Dynamic Memory Management in Ada and SPARK</i> M. Maalej, Y. Moy and T. Taft	<b>Vendor presentation</b> RAPITA	<i>Safe Parallelism: Compiler Analysis Techniques for Ada and OpenMP</i> S. Royuela, X. Martorell, E. Quiñones and L. M. Pinho
17:00 - 17:30	<i>Safe Non-Blocking Synchronization in Ada2x</i> J. Blieberger and B. Burgstaller	<i>Combined Scheduling of Time-Triggered and Priority-Based Task Sets in Ravenscar</i> J. Real, S. Sáez and A. Crespo	<i>Microservice-based Agile Architectures: An Opportunity for Specialized Niche Technologies</i> S. Munari, S. Valle and T. Vardanega
17:30 - 17:50	<b>Presentation</b> <i>Alire: A Library Repository Manager for the Open Source Ada Ecosystem</i> A. R. Mosteo	<i>Theory and Practice of EDF Scheduling in Distributed Real-Time Systems</i> J. Javier Gutiérrez and H. Perez	<b>Presentation</b> <i>Real-Time Ada Applications on Android</i> A. P. Ruiz, M. A. Rivas and M. G. Harbour
18:00 - 19:00	<b>Ada-Europe General Assembly</b>		<b>Best Presentation Award</b> <b>Presentation of future related events</b> <b>Closing</b>
19:30	<b>Welcome Reception</b> (Parque das Nações Marina – WaterX Catamaran)	<b>Conference Banquet and Best Paper Award</b> (Restaurant “A Casa do Bacalhau”)	

## ORGANIZATION

### General Chair

*Nuno Neves*  
LASIGE/U. Lisboa, Portugal

### Program Chair

*António Casimiro*  
LASIGE/U. Lisboa, Portugal

### Special Session Chair

*Marcus Völz*  
University of Luxembourg, Luxembourg

### Tutorial and Workshop Chair

*David Pereira*  
CISTER/ISEP, Portugal

### Industrial Co-Chairs

*Marco Panunzio*  
Thales A.S., France  
*José Rufino*  
LASIGE/U. Lisboa, Portugal

### Publication Chair

*Pedro Ferreira*  
LASIGE/U. Lisboa, Portugal

### Exhibition Co-Chairs

*José Neves*  
GMV Skysoft, Portugal  
*Ahlan Marriott*  
White Elephant GmbH, Switzerland

### Publicity Chair

*Dirk Craeynest*  
Ada-Belgium & KU Leuven, Belgium

### Local Secretariat

*Madalena Almeida*  
Viagens Abreu, Portugal

### Program Committee

Mario Aldea (Universidad de Cantabria), Ezio Bartocci (Vienna University of Technology), Johann Blieberger (Vienna University of Technology), Rakesh Bobba (Oregon State University), Bernd Burgstaller (Yonsei University), António Casimiro (LASIGE/U. Lisboa), Juan A. de la Puente (Universidad Politécnica de Madrid), Virgil Gligor (Carnegie Mellon University), Michael González Harbour (Universidad de Cantabria), J. Javier Gutiérrez (Universidad de Cantabria), Jérôme Hugues (ISAE), Ruediger Kapitza (Technische Universität Braunschweig), Hubert Keller (Karlsruhe Institute of Technology), Raimund Kirner (Univ. of Hertfordshire), Adam Lackorzynski (TU Dresden and Kernkonzept GmbH), Kristina Lundkvist (Mälardalen University), Franco Mazzanti (ISTI-CNR), Laurent Pautet (Telecom ParisTech), Luís Miguel Pinho (CISTER/ISEP), Erhard Plödereder (Universität Stuttgart), Jorge Real (Universitat Politècnica de València), José Ruiz (AdaCore), Sergio Sáez (Universitat Politècnica de València), Elad Schiller (Chalmers University of Technology), Frank Singhoff (Université de Bretagne Occidentale), Jorge Sousa Pinto (University of Minho), Tucker Taft (AdaCore), Elena Troubitsyna (Åbo Akademi University), Santiago Urueña (GMV), Tullio Vardanega (Università di Padova), Marcus Völz (University of Luxembourg).

### Industrial Committee

Ian Broster (Rapita Systems), Luís Correia (EMPORDEF-TI), Dirk Craeynest (Ada-Belgium & KU Leuven), Thomas Gruber (Austrian Institute Of Technology - AIT), Andreas Jung (European Space Agency), Ismael Lafoz (Airbus Defence and Space), Ahlan Marriott (White Elephant GmbH), Maurizio Martignano (Spazio IT), Marco Panunzio (Thales Alenia Space), Paul Parkinson (Wind River), Jean-Pierre Rosen (Adalog), José Rufino (LASIGE/U. Lisboa), Emilio Salazar (GMV), Helder Silva (EDISOFT), Jacob Sparre Andersen (JSA Consulting), Andreas Wortmann (OHB System).

## CONFERENCE SPONSORS

AdaCore

PTC®  
Developer Tools

  
RAPITA  
SYSTEMS LTD

  
CRITICAL  
SOFTWARE

  
Ciências  
ULisboa

LASIGE

  
Ellidiss  
Software  
TNI Europe Limited

FCT  
Fundação  
para a Ciência  
e a Tecnologia

Springer Verlag publishes the proceedings of the conference, in the  
Lecture Notes in Computer Science series (LNCS 10873)

  
Lecture Notes in  
Computer Science  
LNCS LNAI LNBI