

19th International Conference on Reliable Software Technologies

Ada-Europe 2014

↘ **23-27 June 2014** Paris, France

www.ada-europe.org/conference2014



↘ **Final Program**



ECE PARIS
ÉCOLE D'INGÉNIEURS

On behalf of the whole organizing committee, it is my pleasure to welcome all participants to the 19th International Conference on Reliable Software Technologies - Ada-Europe 2014. We managed a combination of a very rich and valuable program and an attractive place, and we are very happy that the fame of the conference has attracted more interesting events that will take place during this week.

In addition, we designed our own registration system, in Ada of course, that makes registering easier than ever before. Don't hesitate and book early, Paris in June attracts many people!

Looking forward to welcoming you in Paris.

J-P. Rosen, General Chair

The 19th International Conference on Reliable Software Technologies - Ada-Europe 2014 will take place in Paris, France. As per its traditional style, the conference will span a full week, including, from Tuesday to Thursday, three days of parallel scientific, technical and industrial programs, along with tutorials and workshops on Monday and Friday.

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



The proceedings will be published by Springer in the «Lecture Notes in Computer Science (LNCS)» series, volume 8454.

Overview of the Week

Monday	Tuesday	Wednesday	Thursday	Friday
	Opening / Welcome			
3 tutorial tracks T1: EM 222, T3: EM 223, T5: EM 224 + CPS workshop EM 225	Keynote talk Robert Lainé Regular session 1 Formal methods	Keynote talk Alun Foster Regular session 2 Uses of Ada	Ada-France workshop Keynote talk Mohamed Shawky Regular session 3 Real-Time Scheduling	3 tutorial tracks T7: EM 222, T9: EM 223, T10: EM 224 + WMCIS workshop EM 225
3 tutorial tracks T2: EM 222, T4: EM 223, T6: EM 224 + CPS workshop EM 225	Industrial track Ada in Aerospace Experience reports	Vendor session GNAT retrospective	Industrial track Ada in Railways Regular session 4 Applications	3 tutorial tracks T8: EM 222, T9: EM 223, T10: EM 224 + CPS workshop EM 225
	Ada-Europe General Assembly	Cruise and conference banquet Best paper award	Best presentation award Closing session	

The conference thanks its sponsors who help make this event possible and enjoyable:



On the three central days of the conference week, a keynote will be delivered as the opening event to address hot topics of relevance in the conference scope.

Robert Lainé ↘ Tuesday morning

Lessons Learned and Often Forgotten



Robert Lainé will talk about Lessons learned and easily forgotten, drawing from his many years of experience in space projects leadership at the European Space Agency and EADS Astrium.

Dr. Robert Lainé has had the privilege of leading a number of important and challenging spacecraft development projects in his long professional career. He will report on 41 years of observations of the key issues related to successful leadership of large aerospace projects at the European Space Agency and EADS Astrium.

This talk is more like a retrospective reflection on a vast personal experience than a scientific essay on the art of project and team management. In the hope that this contribution can benefit others, these personal reflections are offered first to the community that keeps this conference series alive and kicking, and then to those who consult the conference proceedings.

Alun Foster ↘ Wednesday morning

From ARTEMIS to ECSEL : Growing a Large Eco-System for High-Dependability Systems



Alun Foster, Acting Executive Director and Programme Manager of the ARTEMIS Joint Undertaking will present From ARTEMIS to ECSEL: growing a large eco-system for high-dependability systems, about the results achieved in ARTEMIS and the objectives of the new

ECSEL program, which will be integrated in the Horizon 2020 framework program for research and development in Europe. This keynote presents the results achieved in ARTEMIS and the objectives of the new ECSEL program, which will be integrated in the Horizon 2020 framework program for research and development in Europe. It demonstrates the power of larger-scale collaborative research, and the importance of the Public-Private Partnership model for maximising the impact of R&D investments.

Mohamed Shawky

↘ Thursday morning

Future Challenges in Design Tools and Frameworks for Embedded Systems; Application to Intelligent Transportation Systems



Mohamed Shawky is currently with the Heudiasyc laboratory (Heuristics and diagnosis for complex systems), at the Department of Computer Science, Université de Technologie Compiègne, France. He will present his futuristic work

on Intelligent Transportation Systems.

Environment perception technologies and sophisticated signal processing algorithms yield today mature understanding of dynamics of transportation vectors. Uncertainty management became inherent to decision making following such environment understanding processes. However, designers of critical embedded systems remain skeptical about considering uncertainty, probably as design tools and frameworks have not yet integrated advances in state-of-the-art of confidence management approaches. On the other hand, hesitant multicore programming tools do not provide yet enough native redundancy for applications offered by such technologies, which would have been a precious contribution to increase their reliability. In this keynote, we will present a synopsis of these new challenges that will face in the near future designers and tool developers for Intelligent Transportation Systems.

Environment perception technologies and sophisticated signal processing algorithms yield today mature understanding of dynamics of transportation vectors. Uncertainty management became inherent to decision making following such environment understanding processes. However, designers of critical embedded systems remain skeptical about considering uncertainty, probably as design tools and frameworks have not yet integrated advances in state-of-the-art of confidence management approaches. Furthermore, hesitant multicore programming tools do not provide yet enough native redundancy for applications offered by such technologies, which would have been a precious contribution to increase their reliability. In this keynote, we present a synopsis of these new challenges that will face in the near future designers and tool developers for Intelligent Transportation Systems.

Conference Schedule



Tuesday		Wednesday		Thursday	
9:00	Opening/Welcome	9:30	Keynote talk: Alun Foster <i>From ARTEMIS to ECSEL: Growing a Large Eco-System for High-Dependability Systems</i>	9:30	Keynote talk: Mohamed Shawky <i>Future Challenges in Design Tools and Frameworks for Embedded Systems: Application to Intelligent Transportation Systems</i>
9:30	Keynote talk: Robert Lainé <i>Lessons Learned and Often Forgotten</i>	10:30	Break + Exhibition	10:30	Break + Exhibition
10:30	Break + Exhibition	10:30	Break + Exhibition	10:30	Break + Exhibition
11:30	Regular session 1: Formal methods: Chair: <i>TBA</i> Rigorous Development of Fault-Tolerant Systems through Co-Refinement <i>I. Lopatkin and A. Romanovsky</i> Kronecker Algebra for Static Analysis of Ada Programs with Protected Objects <i>Bernd Burgstaller and Johann Bieleberger</i> A TASM-based Requirements Validation Approach for Safety-critical Embedded Systems <i>Jiale Zhou, Yue Lu and Kristina Lundqvist</i>	11:30	Regular session 2: Uses of Ada: Chair: <i>Albert Llemosi</i> Towards a Runtime Verification Framework for the Ada Programming Language <i>A. De Matos Pedro, D. Pereira, L. M. Pinho and J. Sousa Pinto</i> Reliable Handling of Real-Time Scheduling Attributes on Multiprocessor Platforms in Ada 2012 <i>S. Sáez, J. Real and A. Crespo</i> Parallelism in Ada: Status and Prospects <i>L. M. Pinho, B. Moore and S. Michell</i>	11:30	Regular session 3: Real-Time Scheduling: Chair: <i>Luis Miguel</i> Deadline-Aware Programming and Scheduling <i>Alan Burns and Andy Wellings</i> Schedulability Analysis for Directed Acyclic Graphs on Multiprocessor Systems at a Subtask Level <i>Manar Qamhieh and Serge Midonnet</i> Integrated Schedulers for a Predictable Interrupt Management on Real-Time Kernels <i>Sergio Sáez and Alfons Crespo</i>
13:00	Lunch + Exhibition	13:00	Lunch + Exhibition	13:00	Lunch + Exhibition

T1 - Proving Safety of Parallel/Multi-Threaded Programs

➤ Monday morning



Tucker Taft, AdaCore, USA

This tutorial will introduce the attendees to analysis and proof techniques for programs using parallelism and multi-threading. There are no specific prerequisites, but a familiarity with the notions of preconditions and postconditions, aliasing, race conditions, and deadlocks would be of value. The examples will be based on the threading and parallelism models of Java, Ada, and two new parallel languages, one called ParaSail[4] and another, inspired by the verifiable SPARK[1][2] subset of Ada, called Sparkel[3]. We will introduce the distinction between safety and liveness properties, and then focus primarily on techniques for the verification of safety properties, including the absence of race conditions and deadlocks. We will also discuss the issue of determinism vs. non-determinism in parallel and multi-threaded programs.

Level

Intermediate to advanced level, with some familiarity with the notions of preconditions and postconditions, aliasing, race conditions, and deadlocks.

Reasons for attending

This tutorial will enable the attendee to better understand the literature relating to formal verification of concurrent systems.

Presenter

S. Tucker Taft is VP and Director of Language Research at AdaCore, a company focused on open-source tools to support the development of high-integrity software. Tucker joined AdaCore in 2011 as part of a merger with SofCheck, a company he had founded in 2002 to develop advanced static analysis technology. Prior to that Tucker was a Chief Scientist at Intermetrics, Inc. and its follow-ons for 22 years, where in 1990-1995 he led the design of Ada 95. Tucker received an A.B. Summa Cum Laude degree from Harvard University, where he has more recently taught compiler construction and programming language design. Tucker has given many talks and tutorials, and has spent the last 4 years focused on language issues associated with parallel programming.

T2 - Multicore Programming using Divide-and-Conquer and Work Stealing

➤ Monday afternoon

Tucker Taft, AdaCore, USA

This half-day tutorial will introduce the attendee to some of the issues of parallel programming for multicore systems. We will discuss some of the models used for creating and then managing efficiently large numbers of «picothreads.» The tutorial will first cover the basic technique of «divide and conquer» as it applies to splitting up computations into large numbers of separate sub-computations. We will provide examples using Intel's Cilk+ language, as well as using Go, Rust, and ParaSail, three new parallel programming languages. The tutorial will then go on to investigate the «work-stealing» scheduling mechanism used by the Cilk+ run-time, Intel's Threaded Basic Blocks library, as well as the ParaSail virtual machine. Work-stealing is an efficient way to handle the large number of very small «picothreads» created in abundance by these parallel programming technologies. We will also discuss the issues of managing storage to provide safety and separation between concurrent tasks, including per-task heaps, unique pointers, and region-based storage management. We will include a short discussion of heterogeneous parallel programming, using auxiliary chips such as Graphics Processing Units (GPUs) as general purpose processors (GPGPU).

Level

Intermediate to Advanced knowledge of programming, with some understanding of multi-threaded/multi-tasking issues, including race conditions and synchronization.

Reasons for attending

Attendees will learn the various paradigms for creating algorithms that will take advantage of the growing number of multicore processors, while avoiding the overhead of excessive synchronization overhead. Attendees will also learn the theory and practice of «work stealing,» a multicore scheduling approach which is being adopted in numerous multicore languages and frameworks, as well as the various tradeoffs associated with different multicore storage management approaches.

T3 - Debugging Real-Time Systems

↘ Monday morning

Ian Broster and Andrew Coombes,
Rapita Systems Ltd, UK



Needle in a haystack? That's what real-time systems debugging can feel like sometimes, especially when the problems are intermittent. Race

conditions, priority inversion, different orderings, locking, operating system interactions and scheduling can make getting to the bottom of the problem hard and time consuming.

This tutorial will cover tools and techniques for debugging real-time software, focusing on issues that hit embedded and real-time systems such as operating system interactions, scheduling, race conditions, software timing, performance. We analyse the differences between on-target and on-host testing and understand the challenges of working in real-time systems. Different ways of getting access to an embedded computer are discussed, including interfacing with real-time operating systems, obtaining traces and displaying and interpreting them. We will introduce ideas and new tools for verifying that your assumptions are met at run-time, and diagnosing/debugging when they are not, checking real-time constraints, ordering constraints and detection of anomalies. Importantly, when something goes wrong, you need to have the information to dig into the detail and work backwards and we will explain how to be prepared to catch intermittent faults.

This tutorial includes interactive sessions, and there is an element of practical work in Ada and other languages.

Level

Intermediate. The tutorial is suitable for anyone with an interest in embedded, reliable software, real-time or Ada. Familiarity with some of these topics is beneficial but not essential.

Reasons for attending

You will come away with ideas for how to debug and

diagnose problems in reliable real-time software, particularly you will learn practical techniques for tracing and verification of real-time conditions.

Presenters

Dr Ian Broster is a founder and Director of Rapita Systems Ltd, a company specializing in on-target software verification. He is an experienced, lively lecturer who has given numerous training courses, lectures and presentations on this and other topics. His previous Ada-Europe tutorials receive consistently excellent feedback. He has been involved with Ada since 1995 and earned his PhD at the Real-Time Systems Research Group of University of York.

Dr Andrew Coombes runs the Marketing and Engineering Services group at Rapita Systems Ltd, a company specialising in tools for on-target verification of high-integrity embedded software. Since 1996 he has been involved in the development and commercialisation of software tools for embedded, real-time applications. Prior to this, he worked in a consultancy and for the BAE Systems DCSC (Dependable Computing Systems Centre). He received his DPhil in Computer Science at the High-Integrity Systems Engineering Group at the University of York.

T4 - Developing Mixed-Criticality Systems with GNAT/ORK and Xtratum

↘ Monday afternoon

Alfons Crespo, Alejandro Alonso
and Jon Pérez, UPV, UPM and IKERLAN, Spain



Modern embedded applications typically integrate a multitude of functionalities with potentially different criticality levels into a single system. In addition, the increasing power of mono-core and multi-core processors make it possible to integrate them in a single platform. However, this implies a number of challenges, being the integration of mixed-criticality applications

one of them. System partitioning emerges as a powerful alternative for dealing with these challenges. A hypervisor enables several virtual machines to be created, with spatial and temporal separation between them. Applications are assigned to partitions, according to different criteria, such as criticality. Resources are assigned to virtual machines so as to guarantee the fulfilment of the temporal requirements of the applications. This approach is also valid for multi-core computers.

This tutorial will introduce the attendee the basic techniques in the development of partitioned high integrity embedded systems, which will be illustrated with a case study. This development relies on the XtratuM hypervisor and supporting tools for validation, partitioning, and code and configuration files generation.

This tutorial will benefit attendees from the industry, as it will show in a practical manner the basics in the development of partitioned embedded systems. They could have an idea on how to integrate this approach on their current practices. Attendees from the academia will get acquainted with advance development techniques and open research topics. In addition, the availability of the development framework can be the base of laboratory assignments on advanced courses.

Level

Intermediate. The tutorial is aimed at project managers, systems engineers, and developers of high-integrity software systems, as well as academics teaching or researching on embedded systems.

Reasons for attending

Attendants will learn the main concepts and techniques needed to develop high-integrity partitioned real-time systems on a representative platform.

Presenters

Alfons Crespo is a Professor at the Department of Computer Engineering of the Technical University of Valencia. He received a PhD in Computer Science from the Technical University of Valencia, Spain, in 1984. He held the position of Associate professor in 1986 and full Professor in 1991. He leads the group of Industrial Informatics and has been responsible for several European and Spanish research projects. His main research interest include virtualization techniques for real-time embedded systems, real-time scheduling, scheduling and control integration. He has published more than 100 papers in specialised journals and conferences in the area of real-time systems.

Alejandro Alonso received his Ph. D. in Computer Science in 1985. He became full professor of computer science. He belongs to the Department of Telematic Systems Engineering at the School of Telecommunication Engineering of the Universidad Politecnica de Madrid. His current research interests are in real-time and embedded systems, including design methods, software architectures, resource management, and operating systems. He has participated in several EU funded projects, as well as national government and industry funded research projects. His recent research activities include the development of a component for managing QoS and resources in embedded systems, and mixed-criticality systems, based on hypervisors. He is active member of ACM, IFAC, IEEE and Ada-Europe.

Jon Pérez is a Researcher at IKERLAN research center. He is currently head of the embedded systems research line and works in the design and development of safety-critical embedded systems, for example SIL4 railway signaling (ERTMS/ETCS). He is a certified TÜV Functional Safety engineer for the design of hardware and software based on the IEC-61508 standard.

He has received a B. Eng in Industrial and Robotics at Mondragon University, a M.Sc. in Electronics & Electrical Engineering with distinction at the University of Glasgow and he finished his doctoral studies in Computer Science at Technische Universität Wien (TU Wien) in the field of safety-critical embedded systems.

T5 - High-Integrity Object-Oriented Programming with Ada 2012

➤ **Monday morning**

Ben Brosgol, AdaCore, USA



Object-Oriented Programming (OOP) and associated features such as exceptions have been successfully used for many kinds of systems because of their benefits in software maintainability and reuse.

However, until recently they have not made much traction among developers of High-Integrity software -- i.e., systems where high levels of safety and/or security are required. This tutorial, based on the Object-Oriented Technology and Related Techniques supplement (DO-332) to the DO-178C standard for commercial

airborne systems, will describe the issues that arise with OOP in High Integrity systems and show how they can be addressed in Ada 2012. Among the topics to be covered is «Local Type Consistency Verification», a novel and practical approach to dealing with the verification issues associated with class inheritance, polymorphism, and dynamic binding.

Level

Knowledge of some Object-Oriented language is assumed, and experience with the OO features of Ada 95 will be useful. Familiarity with the new Ada 2012 features, or with software certification standards such as DO-178B/C, is not required.

Reasons for attending

Attendees will learn how to anticipate and avoid the various «traps and pitfalls» associated with OOP in safety-critical or high-security software, and how to use Ada 2012 to write OO programs that can comply with software standards such as DO-178C.

Presenter

Dr. Benjamin Brosgol is a senior member of the technical staff at AdaCore in the US. He has been involved with programming language design and implementation for more than 30 years, concentrating on languages and technologies for high-integrity systems. He participated in the design of Ada 83 and Ada 95, and he was a member of the Expert Group for the Real-Time Specification for Java. Dr. Brosgol has presented papers and tutorials at numerous conferences including Ada-Europe, ACM SIGAda, ESC (Embedded Systems Conference), ICSE (IEEE/ACM International Conference on Software Engineering), and SSTC (Systems & Software Technology Conference). He has in-depth knowledge of and experience with the specific topic of Object Orientation and software safety certification, and he has delivered conference presentations and written articles and papers on this subject. Dr. Brosgol holds a BA in Mathematics from Amherst College, and MS and PhD degrees in Applied Mathematics from Harvard University.

T6 - Ada 2012 (Sub) type and Subprogram Contracts in Practice

↘ Monday afternoon



Jacob Sparre Andersen, JSA
Research & Innovation, Denmark

The tutorial is organised in three sections. As an introduction, Ada 2012 contract aspects are presented, and it is discussed how they extend and complement the pre-2012 «contracts» (subtype constraints and parameter modes). The second section gives guidance on how one can ensure a consistent application of contract aspects across a set of (sub)types and subprograms. In the final section the tutorial attendees will be guided through a practical exercise in applying contract aspects.

Level

The tutorial is intended to be on an intermediate level. The intended audience is software engineers, who already know Ada, but have not yet used the new «programming by contract» aspects added in Ada 2012.

It is advised that the attendees bring laptops (with an Ada 2012 compiler installed) along for the tutorial, even if the practical exercises can be worked through with pen and paper.

Reasons for attending

The tutorial will give the participants guidance and practical exercises in applying contract aspects consistently across a set of (sub)types and subprograms.

Presenter

Jacob Sparre Andersen has previously given talks on his practical experiences with Ada 2012 (including the contract aspects) at Ada-Europe 2013 in Stockholm and DANSAS'13 in Odense.

Jacob Sparre Andersen has worked as a lecturer in software engineering at CEUS with responsibility for courses in:

- Software design
- System programming
- Computer networks and network programming
- Software mediated games

On other occasions he has been a teaching assistant at the Niels Bohr Institute on courses in:

- Mathematics (for the biologists and geophysicists)
- Physics of complex systems

T7 - Technical Basis of Model Driven Engineering

Friday morning

William Bail, The MITRE Corporation, USA



Model Driven Engineering (MDE) in its various names, such as Model Driven Architecture[®], has matured since it was first envisioned, and as a consequence has become much more widely used

throughout industry. Some practitioners are claiming significant gains in productivity and product quality, while others cite more modest benefits. This tutorial examines MDE, looking at the mechanics of its process, revealing its constituent elements, and describing how it automates portions of the development process. It analyzes the parts of the process where the productivity and quality gains are realized, and also takes a critical look at the various claims that are being made about its benefits. The tutorial provides an objective assessment of the maturity of MDE, and objectively assesses the potential benefits of using this technology. The tutorial does describe any specific tool but rather describes the underlying technical basis.

Level

Intermediate. Practitioners who have direct responsibility in planning of software system development, and in the selection of tools and techniques to be used for such developments.

Reasons for attending

This tutorial will provide the attendee with the basic understanding of the technical underpinnings of Model Driven Engineering, and thereby provide a basis for selection of this technique for candidate software development projects. The tutorial will also provide an assessment of the level of maturity of the technology, and provide a perspective regarding where additional research is needed. Understanding the underlying principles, and the relative strengths and weaknesses of MDE, is essential to making informed decisions and selecting (or not selecting) MDE as a development strategy

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, primarily 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'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 develops instructional materials and teaches 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, and Requirements Engineering for Dependable Systems at SIGAda, AdaEurope, 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.

T8 - An Overview of Software Testing with an Emphasis on Statistical Testing

Friday afternoon

William Bail, The MITRE Corporation, USA

Testing software systems is a critical stage in the overall development process. However, often, the testing approaches used fall short, allowing latent defects to leak through into deployed systems that are placed into service, even after what seems to be extensive testing. These defects become visible

after the system is brought through a usage pattern that was unanticipated. In order to overcome these shortcomings, a combination of test techniques is recommended, ranging from coverage-based unit testing to operational profile based statistical testing. In this latter approach, the expected usage patterns of the system are identified and modeled. For these patterns, predicted probabilities of occurrence are generated, and test cases and scenarios are defined. The results may then be used to estimate an overall reliability of performance. Stopping criteria is then applied to determine if the testing process has been sufficient for the system's goals. This approach also supports a significant increase in automation, thereby increasing the intensity of the testing and reducing the time needed to create and run the tests. The tutorial will present the basic of software testing, and will focus on the practice of statistical testing, in order to provide a basis for improving the quality of the overall test process.

Level

Intermediate. Attendee background should have direct involvement in planning for, designing, and implementing test programs for software systems.

Reasons for attending

Understanding the fundamentals of test approaches, and applying the concepts of statistical testing, will enable developers to more effectively detect latent defects, and ensure that the resulting system will present a more dependable pattern of operation after it is placed into operation.

T9 - Robotics Programming

↘ Friday, all day



Lars Asplund, Asplund Data AB, Sweden

A number of small robots equipped with the Lars-board with an architecture that is similar to the Arduino, but build in H-bridges and protection on all signals. They are programmed in Ada (no run-time) and the robots have two motors, two range-sensors both mounted on servos. You can with the servos direct the range sensors in different directions. Some robots have built in Wi-Fi for Robot-Robot communication.

The Tutorial is going to cover programming of an 8-bit micro-controller. There will be hands on programming, and each participant is required to bring a PC running windows. The tutorial will cover both low level programming, access to registers in the MCU and interrupt handling, as well as high-level programming. At the end of the day the participants will program the robot to do various tasks using packages for all needed functionality.

Level

Intermediate level. The audience should have a basic knowledge about Ada. First course in Computer Science...

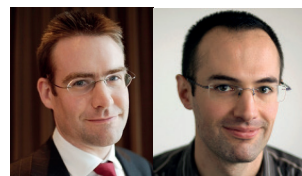
Reasons for attending

Ada is today available for one of the most popular micro-controllers, and with this board or an Arduino you can make your own embedded system. It should be of particular interest for professors in universities.

Presenter

Lars Asplund has been involved with Ada since many years, and is currently a full professor in Computer Science at Mälardalen University in Sweden. Lars has recently published a book in Robotics (still in Swedish) where a lot of material for this tutorial is available.

T10 - Introduction to Verification with SPARK 2014 ↘ Friday full day



Rod Chapman and Yannick Moy, Altran UK and AdaCore, France

SPARK 2014 is the latest evolution of the SPARK programming language. Based on Ada 2012, it encompasses a rich subset of the language and augments it with further language constructs designed to support advanced static verification techniques.

This tutorial will provide a broad overview of the SPARK 2014 language: the subset of Ada 2012 which it includes and the additional constructs which it adds to support verification. The morning session will cover basic features and static analysis techniques. This will be followed by an introduction to one of the most novel features of the language - the dual nature

of the contracts as both executable and mathematical statements and how these can be verified by testing, proof, or a combination of the two.

In the afternoon, the tutorial will look at more advanced language features that are essential for industrial-scale specification, such as abstraction and refinement. We will also look at more advanced verification techniques supported by the language such as information flow analysis and proving the absence of run-time exceptions (divide-by-zero, numeric overflow). Finally we will touch on some of the more advanced proof techniques that may be required.

Level

Intermediate. Prerequisites : knowledge of Ada (but not necessarily Ada 2012) and some basic familiarity with the concepts of static analysis

Reasons for attending

People wishing to learn more about the SPARK 2014 language and the opportunities it offers for novel verification techniques should attend. Attendees may be involved in or interested in new techniques for the engineering of safety- or security-critical applications or interested in languages and methods suitable for reducing post-delivery defect rates in consumer products.

Presenters

Roderick Chapman is a Principal Engineer with Altran UK, specializing in the design and implementation of safety and security-critical systems. He currently leads the programming language design and static analysis tools group at Altran.

Rod is a well-known conference speaker and has presented papers, tutorials, and workshops at many international events including STC, NSA HCSS, ACM HILT, Reliable Software Technologies Europe, and ESC San Jose. Roderick has been a key contributor to many of Altran's major projects such as SHOLIS, MULTOS CA, Tokeneer and the SPARK verification tools. He received a MEng in Computer Systems and Software Engineering and a DPhil in Computer Science from the University of York, England, in 1991 and 1995 respectively. He is a Chartered Engineer, a Fellow of the British Computer Society, and also an SEI-Certified PSP Instructor.

Yannick Moy is a Senior Software Engineer at AdaCore, where he works on software source code analyzers CodePeer and SPARK, aiming either at detecting bugs or at verifying safety/security properties.

Yannick lead the three-years project Hi-Lite leading to the new version of SPARK known as SPARK 2014. He presented SPARK at many international conferences and events, and is used to teaching SPARK through classes, webinars and blogs. Yannick previously worked on source analyzers for PolySpace (now The MathWorks) and INRIA Research Labs.



Challenges and New Approaches for Dependable and Cyber-Physical System Engineering (De-CPS 2014) ↘ Monday 23 June 2014

From the USA to Europe, there is a crescendo of industrial and research interest in Cyber-Physical Systems (CPS). One distinguishing trait of CPS is that they integrate software control and decision making with signals from and sensing of an uncertain and dynamic environment. CPS often involve heterogeneous and hierarchical systems, and their design makes extensive use of models. The Horizon 2020 program framework of the European Union devotes considerable attention in the current work program to various aspects of the CPS challenges. The De-CPS workshop intends to focus on the relationships between CPS and contract-based approaches. The latter are a means to assert desired guarantees on specific properties of a system model and to attain them in the corresponding implementation. The workshop will gather industrial practitioners and research actors interested in dependable and Cyber-Physical Systems engineering, and use the momentum of the 19th International Conference on Reliable Software Technologies to foster further collaborative initiatives that may use the funding opportunities of the H2020 framework program.

The topics addressed by the workshop include the following:

- Industrial challenges and experience reports on co-engineering for multiple dependability concerns in CPS engineering.
- Modeling and analysis of Cyber-Physical Systems (CPS) via contract-based approaches
- Tools and methodologies to guarantee safety-related properties, including real-time and mixed-criticality cohabitation.

The authors of the accepted submissions will be invited to publish an extended version of their contribution in the Ada-Europe Journal.

- Workshop : 23/6, Paris, France
- after-workshop final version: 15/9
- publication: December 2014

Organizers

- Daniela Cancila, CEA (Commissariat à l'énergie atomique et aux énergies alternatives)
- Laurent Rioux, Thales

Steering Committee

- Antoine B. Rauzy, Director of the Chair Blériot-Fabre (Centrale-Supélec, Safran)

Preliminary Program Committee

- Katrina Attwood, University of York, UK
- Benoit Caillaud, INRIA, France
- Philippa Comny, University of York, UK
- Vincent David, Krono-Safe, France
- Ali Koudri, Thales, France
- Pavithra Prabhakar, IMDEA, Spain
- Roberto Passerone, University of Trento, Italy
- Alejandra Ruiz, Tecnalia, Spain
- Bran Selic, Malina SW & Carleton Univ, Canada
- Safouan Taha, Supélec, France
- Masumi Toyoshima, DENSO, Japan

Publicity Chair

- Karima Nahhal, CEA (Commissariat à l'énergie atomique et aux énergies alternatives)
- Jean-Louis Gerstenmayer, CEA (Commissariat à l'énergie atomique et aux énergies alternatives).

Ada-France Day: Ada 2012: Le Point sur le Langage

(Ada 2012: Assessing the Language)

Organized by Ada-France, a special session (in French) for software managers who want to learn about Ada's current state. It will feature a technical presentation of the benefits of Ada, an overview of technology providers, users reports, and a panel to answer all participants questions.

Participants will be allowed to the exhibition where they can meet users of the language, and to the afternoon sessions featuring vendor sessions and the Gnat retrospective.

Une présentation de l'état actuel d'Ada, pour les responsables qui souhaitent comprendre l'intérêt du langage dans sa toute dernière version.

La journée comporte une présentation des aspects techniques particuliers à Ada et de leur intérêt, un panorama des fournisseurs d'outils associés, des témoignages d'utilisateurs et une table ronde pour répondre aux questions des participants.

De plus, les participants pourront visiter l'exposition, discuter pendant les pauses avec les utilisateurs qui assistent à la conférence, et profiter des séances de l'après-midi (présentations des vendeurs et rétrospective Gnat).

Mixed Criticality for Industrial Systems (WMCIS'2014): Challenges of Mixed Criticality approaches and benefits for the industry

Friday 27 June 2014

The workshop will be targeted towards research and practice in Mixed Criticality Systems (MiCS), showing how MiCS interact with industrial needs. The format of this workshop will encourage the interaction between participants to promote a spirit of co-operation and collaboration between the different communities.

MiCS are new systems trying to combine on the same platform critical functions with flexible functions mostly originating from the consumer systems. The consumer market is constantly redefining embedded systems, and is source of many hardware and software evolutions. Critical systems (automotive, aerospace) should take advantage of those new platforms to produce robust and predictable systems at a competitive cost with affordable time-to-market. Critical and consumer applications are usually provided by distinct, isolated, systems; research on Mixed-Criticality Systems aims at closing the gap.

Research challenges for MiCS are numerous, and intersect multiple different domains. Among them, the workshop invites submissions in areas such as, but not limited to:

- New concepts for hardware and software architectures (hardware isolation, hypervisor, operating systems, ...);
- Data Management: memory and communication models for sharing/communicating data between critical and non-critical applications.
- Mixed criticality scheduling and schedulability analysis, worst-case executing times.
- Security and dependability issues with MiCS. How to design systems of different criticality which need to cooperate, design frameworks, formal methods, ...
- High performance computing and MiCS. By-pass Moore's law by handling power consumption, heat dissipation limitations; cache scheduling and related issues (CRPD), parallel scheduling, 3D architectures.
- Probabilistic Mixed Criticality: how a probabilistic approach can be used to leverage integration of mixed criticality functions.
- Application of MiCS to new domains: mobile telecommunication networks, energy management systems, ...

Of particular interest in the workshop is experimentations on MiCS and feedbacks from industrial and European projects showing the challenges and benefits of MiCS for the industry.

The workshop will be composed of one keynote and thematic sessions.

The keynote will be given by **Albert Cohen**, senior research scientist in the PARKAS group at INRIA, France on: *Correct-by-Construction Multiprocessor Programming: A Common Approach for Parallel and Mixed-Critical System Design*.

The submission process will be based on extended abstracts (4 pages) describing on-going results on MiCS. Submissions are handled by easychair at: www.easychair.org/conferences/?conf=wmcis2014

All papers accepted for presentation at the workshop will be made available in a workshop booklet.

Authors of outstanding papers will be invited to submit extended versions to a forthcoming special issue of the Elsevier Journal of Systems Architecture (JSA) on the topic of the workshop.

Chairs

- Laurent George, LIGM/UPEMLV, France
- Luis Miguel Pinho, CISTER - Porto, Portugal

Program Committee

- Hakan Aydin, George Mason University, US
- Sanjoy Baruah, University of North Carolina at Chapel Hill, US
- Guillem Bernat, Rapita, UK
- Alfons Crespo, UPV, Spain
- Liliana Cucu-Grosjean, INRIA, France
- Juan Antonio de la Puente, UPM Spain
- Sebastien Faucou, IRCCyN, Nantes, France
- Joel Goossens, ULB, Belgium
- Leandro Indrusiak, York University, UK
- Mathieu Jean, CEA, France
- Claire Maiza, INPGrenoble / Verimag, France
- Moritz Neukirchner, TU Braunschweig, Germany
- Laurent Pautet, Telecom Paristech, France
- Zlatko Petrov, Honeywell, Bulgaria
- Eduardo Quinones, BSC, Spain
- Yves Sorel, INRIA, France
- Benoit Triquet, Airbus, France
- Wang Yi, Uppsala University, Sweden

Registration and Accommodation



For latest updates, as well as information on accommodation, see the web page at www.ada-europe.org/conference2014

Registration

Please access the registration system at: www.ada-europe.org/conference2014/registration.html

Conference

	Members		Non members		Student
	Non academic	Academic	Non academic	Academic	
Early registration	670.00 €	610.00 €	730.00 €	670.00 €	490.00 €
Late registration	730.00 €		790.00 €		530.00 €
Single day registration	370.00 €		400.00 €		265.00 €

The registration fee for the three days of the technical program (June 24 - June 26) includes one copy of the proceedings, coffee breaks, lunches, and banquet. The registration fee for a single day of the technical program includes one copy of the proceedings, coffee breaks, and lunch for the day of the registration.

Members discount: Reserved to members of Ada-Europe and members of an “in cooperation with” SIG of ACM (SIGAda, SIGBED, SIGPLAN).

Academic discount: Reserved to full-time faculty members of a university or equivalent educational institution.

Student discount: The conference offers a limited amount of passes under the “student discount” category.

This scheme provides full access to all of the conference program, including lunches, banquet, and complimentary proceedings. Access to the tutorials may also be requested. Applicants for this discount should take contact with the conference chair, providing a copy of a valid student ID. Students that are co-authors of papers accepted for the conference program are eligible for this discount scheme only if at least one other co-author has registered in full.

Student waiver program: The conference this year also features a novel scheme that allows students to access the conference program for free, but strictly without any other benefit. Applicants for this student waiver program should take contact with the conference chair, providing a copy of a valid student ID.

Tutorials

	Full day	Half day
Early registration	290.00 €	145.00 €
Late registration	320.00 €	160.00 €

Lunch is included for full day tutorials, and for two half-day tutorials on the same day.

Canceling Information

Cancellations must be given in writing. A cancellation fee of 5% will be applied to all cancellations. No refunds will be given for cancellations received after the 22nd of May. Substitutions will be accepted.

Conference Venue and Social Program



The conference will take place at **ECE Paris**, a French engineering school located right in the heart of Paris. ECE enjoys superb modern facilities and convenient access by Metro and RER, close to the Eiffel tower.

➤ Address

ECE - Campus Paris/Eiffel
10 rue Sextius Michel 75015 Paris - France
www.ece.fr

➤ Welcome party

Get together at the welcome party at ECE Paris, featuring buffet dinner and entertainment.



➤ FIFA World Cup

Some of the FIFA World Cup matches will be broadcast in the auditorium!

Dinner Cruise



The traditional Ada-Europe banquet will take place on board an entirely glass-encased boat, where you'll be in on the secret of the city of lights. You will enjoy French cuisine meticulously presented, and your eyes will sparkle as never before as you cruise along the most famous parisian monuments...

This is a must-do, a cultural and very Parisian experience that is unique and must be shared!

Dinner cruise: Wednesday evening.

Organizing Committee

General chair

Jean-Pierre Rosen (rosen@adalog.fr), France

Local co-chairs

Magali Munos (munos@ece.fr), France

Laurent George (lgeorge@ece.fr), France

Program co-chairs

Laurent George (lgeorge@ece.fr), France

Tullio Vardanega (tullio.vardanega@math.unipd.it), Italy

Financial chair

Paul Duquennoy (paul@duquennoy.fr), France

Tutorial co-chairs

Liliana Cucu (Liliana.Cucu@inria.fr), France

Albert Llemosí (albert.llemosi@uib.cat), Spain

Industrial chair

Jørgen Bundgaard (jogb@ramboll.dk), Denmark

Publicity chair

Dirk Craeynest (Dirk.Craeynest@cs.kuleuven.be), Belgium

Exhibition co-chair

Jamie Ayre (ayre@adacore.com), France

Guillaume Foliard (guillaume.foliard@ada-europe2014.org), France