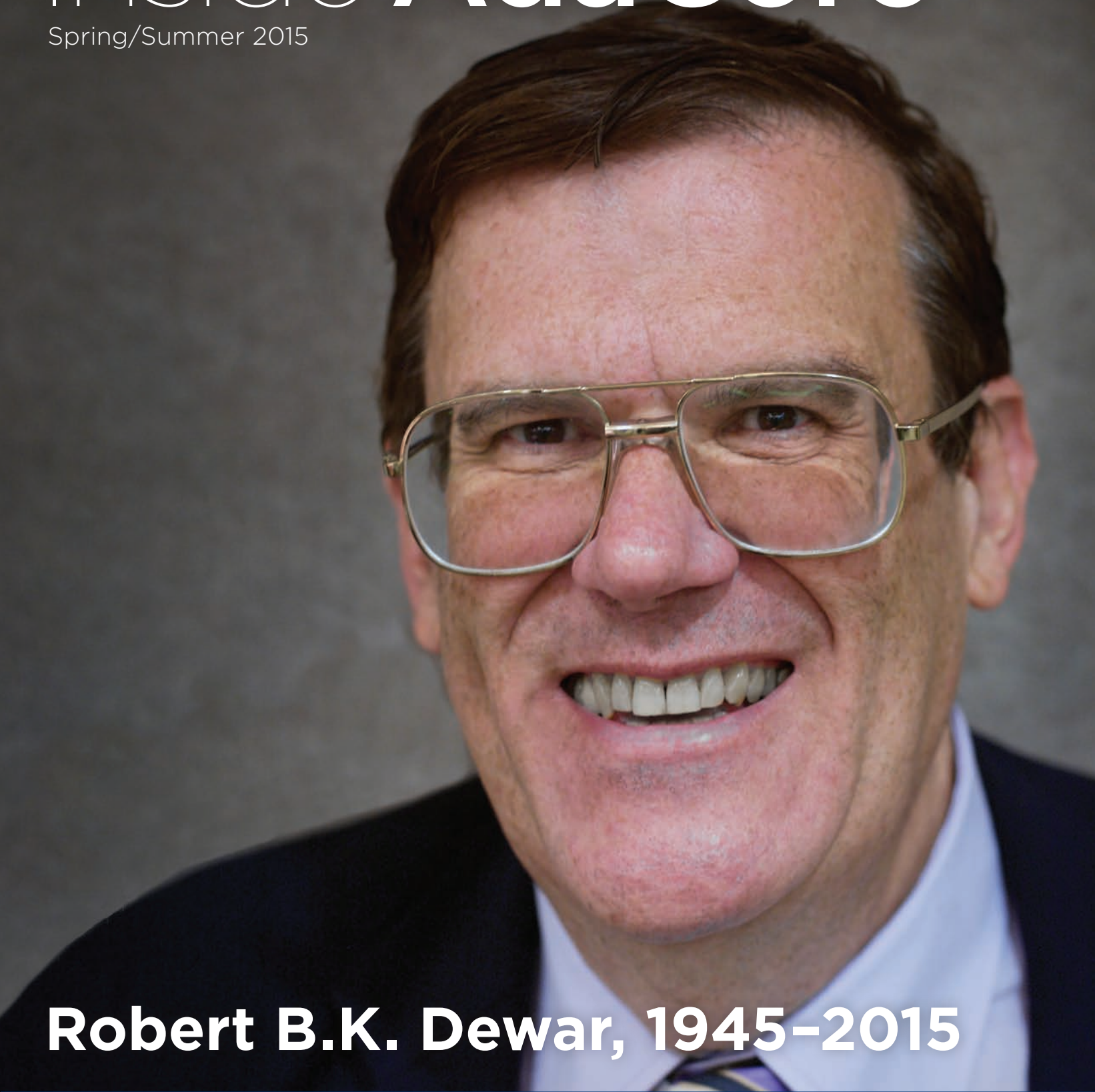


Inside AdaCore

Spring/Summer 2015



Robert B.K. Dewar, 1945–2015

inside this issue **AdaCore Tech Days in Paris and Boston • QGen Launched •
AdaCore Blog Introduced • Ghost Code in SPARK 2014 • Ada Course in Paris**

Robert B.K. Dewar, 1945–2015

Robert Dewar, company President and one of its founders, succumbed to cancer on June 30, 2015. He had a distinguished career as a Professor of Computer Science at New York University (NYU), played a key role in the design and implementation of the Ada programming language, and founded AdaCore, along with four colleagues, in 1994. He served as its CEO until 2012 and as its President until his death.

At AdaCore, Dr. Dewar was active in all phases of the company's business, going well beyond the typical duties of his office. He was the principal architect of the GNAT compiler technology, a member of several product development teams, interacted directly with customers in response to questions or problem reports, wrote numerous journal articles and opinion pieces on topical events in the industry, and served as company spokesman to customers and the trade press. He was an outspoken advocate of Freely Licensed Open Source Software, gave many talks on the subject, and was instrumental in establishing a cooperative relationship between AdaCore and the Free Software Foundation.

During his time as CEO, Dr. Dewar guided AdaCore's strategic decisions that allowed the company to achieve and sustain steady growth and profitability, and he put in place by example an egoless corporate culture based on technical excellence and mutual respect. What he created is still very much a part of the AdaCore team and guides its current management.

Dr. Dewar was born in Oxford, England, on June 21, 1945. After moving to the US, he attended the University of Chicago, receiving a BS in 1964 and a PhD in Chemistry in 1968. While a graduate student, he started working with computers to analyze x-ray crystallography and soon shifted careers. He joined the Computer Science faculty at NYU in 1975, became Full Professor in 1976, and later served as the Chair of the Department.

Specializing in programming language design and implementation, he participated in the SETL project and became involved with Ada from the outset, first as a consultant to one of the language design teams and subsequently as a Distinguished Reviewer. He was one of the architects of the Ada/Ed compiler at NYU, which was written in SETL and served as an operational definition of the Ada 83 language. He was actively involved

with Ada throughout the language's history, as a member of the Ada Rapporteur Group that maintains the language standard and as a designer and implementor of AdaCore's GNAT Ada technology.

Dr. Dewar was involved in the design of Algol 68, a member of IFIP WG2.1 on Algorithmic Languages and Calculi, and served as that group's chair

from 1978 to 1983. He was an expert in all aspects of language technology and co-developed compilers for SPITBOL (SNOBOL), Realia COBOL for the PC, and Alsys Ada. He also designed and implemented several real-time operating systems for Honeywell Inc.

He co-authored several books and wrote dozens of articles and technical papers. His talents as an articulate and knowledgeable expert on topics ranging from computers and the law to software safety and security certification made him a sought-after speaker at conferences. He was a recognized expert in copyright and patent law for software and testified as such in many well-known cases.

Outside of his professional life, Dr. Dewar was a superb baritone, a bassoon and recorder player, a conductor, and a member of the North American Heckelphone Society. He was the lifeblood of the Village Light Opera Group (VLOG) in New York, serving for 35 years in numerous capacities from producer to president, from fly master to music director. He was a major benefactor and performed in a myriad of productions with the group. VLOG's Dewar Center for the Performing

Arts is named in recognition of Robert and Karin Dewar's contributions.

Dr. Dewar was in many ways a "Renaissance Man" with deep expertise in fields ranging from Intellectual Property law to Gilbert and Sullivan operettas, and he was equally at ease discussing fine points of compiler optimization technology and the origins of English language usage of "shall" versus "will". But beyond his keen intellect and many talents he was a witty, entertaining, and engaging gentleman who enriched the lives of all who knew him.

Dr. Dewar is survived by two children, Jennifer and Keith Dewar, and two grandchildren. His wife Karin predeceased him in 2013.



AdaCore

TECH DAYS

AdaCore is hosting two customer-oriented events this year, providing an opportunity to learn more about our products, meet other AdaCore users, and for the Boston event to get hands-on training from the company's technical experts.

**Register now for the
Paris or Boston events**

www.adacore.com/techdays



Paris, France

October 1, 2015



Boston, MA, USA

November 3-4, 2015

SPARK going to the moon

Vermont Technical College in the US was awarded a contract to develop the flight software for the NASA-sponsored Lunar IceCube project, which will launch a CubeSat into lunar orbit in late 2018 to perform a variety of analyses on water and other volatiles occurring on the moon's surface. This project is part of a lunar exploration program that is being administered by Morehead State University. The software will be written in SPARK and Ada using AdaCore's GNAT and SPARK technology. Lunar IceCube is a follow-on to an earlier NASA-sponsored Vermont Tech project, also developed using GNAT and SPARK, that has been successfully transmitting data from an earth-orbiting CubeSat since its launch in November 2013. Please visit www.adacore.com/academia/projects/cubesat-1/ for information about this earlier project.

GNAT Pro selected for new Spanish satellite project

AdaCore's GNAT Pro cross-development environment has been selected by the Polytechnic University of Madrid (*Universidad Politécnica de Madrid / UPM*), for the UPMSat-2 UNION satellite project's real-time on-board and ground control software. The 50kg micro-satellite, scheduled to be launched in Q4 2015, will provide a technology demonstration platform for the university from a sun-synchronous orbit nearly 600 km above Earth. The software component of the project is being led by UPM's Real-Time Systems and Telematic Services Engineering Research Group (*Grupo de Sistemas de Tiempo Real e Ingeniería de Servicios Telemáticos*). The development environment is GNAT Pro for 32-bit Linux, targeted to the LEON3 processor.

GNAT GPL released

GNAT GPL 2015 includes support for a new platform—the Raspberry Pi 2 board—with a full Ada run-time. The implementation for this target provides an excellent platform for developers of non-proprietary software to gain experience with Ada and is especially useful in academic settings.

Ada Bicentennial celebrated

This year marks the 200th anniversary of the birth of Augusta Ada Lovelace, the “Enchantress of Numbers”, whom the Ada language was named for. Born on December 10, 1815 and the daughter of the British poet Lord Byron, Ada pursued a career in mathematics—a rarity for women in that era—and is generally considered the world's first programmer thanks to her work with Charles Babbage on the Analytical Engine. Ada's bicentennial year marks an appropriate time to acknowledge the many significant contributions of women in the science, technology, engineering and mathematics (STEM) disciplines, and to help in this effort AdaCore has initiated the #AdaLove Twitter hashtag. Please check out this hashtag for ongoing tweets.

QGen Launched

Earlier this year AdaCore launched QGen, a qualifiable and customizable code generator and model verifier for Simulink® and Stateflow® models. This tool can generate MISRA-C and SPARK source code that is understandable, traceable, and efficient. It is particularly suited for developing and verifying high-integrity real-time control applications, especially where safety certification is required. The tool is highly configurable thanks to its visible and nonproprietary intermediate representation.

QGen currently handles around 100 Simulink® blocks. These were selected as a safe subset that guarantees predictable code generation patterns, does not require any run-time support, and simplifies the tool qualification effort for in safety certification contexts. QGen also implements a variety of Stateflow® features including parallel states, actions, and junctions.

The tool's static model verifier detects run-time errors such as integer overflow and division by zero. It also can find logic errors such as dead execution paths, and verify functional properties through Simulink® Assertion blocks. QGen can be integrated with AdaCore's GNATemulator and GNATcoverage tools to support Processor-in-the-Loop (PIL) testing and structural coverage analysis without any code instrumentation. For further information please visit www.adacore.com/qgen/.

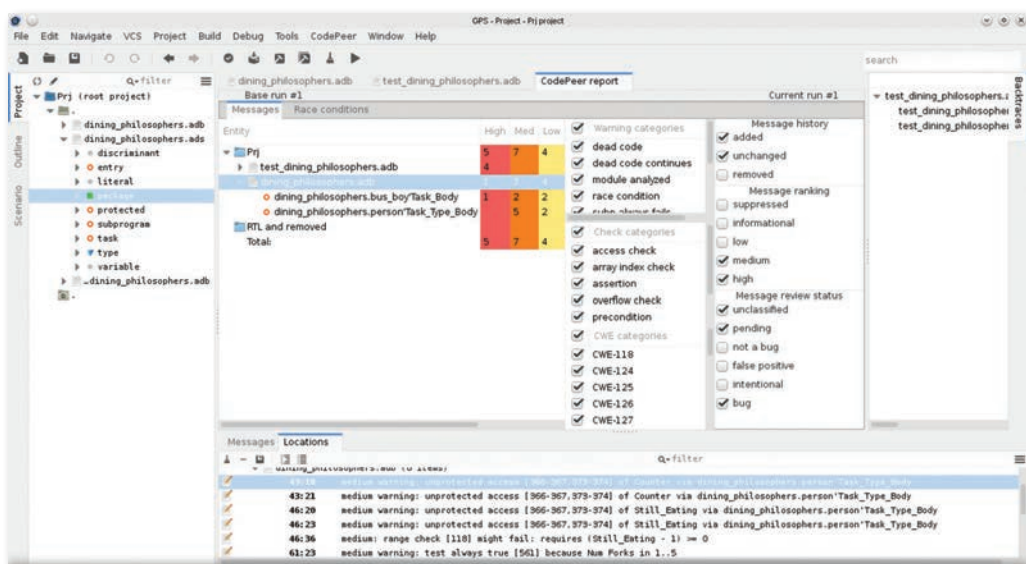
current releases

GNAT Pro 7.3

GNAT Pro 7.3 incorporates upgraded technology for the back end (GCC 4.9) and debugger (GDB 7.8) and includes more than 175 new features, many of which are based on customer recommendations. Enhancements include improved diagnostic messages and fine-grained control over the treatment of warnings, extended support for non-default endianness, a bare-board platform math library designed for use in safety-certified systems, support for large files on 32-bit systems, improved handling of inlining, and enhanced code generation and debugging capabilities. In addition, most GNAT Pro tools now support aggregate projects.

CodePeer 3.0

CodePeer 3.0 has introduced many new features, including support for precise IEEE 754 floating point semantics, added flexibility in analyzing complex projects, improved support for legacy Ada compilers, more precise diagnostic messages, and a new check on parameter aliasing. Tool qualification material for both the avionics and railway domains is available as a product option as CodePeer has now been qualified for DO-178B and EN 50128. For a demo of the tool highlighting the new features please visit www.adacore.com/knowledge/demos/codepeer-3/.



CodePeer Report with References to Common Weakness Enumeration

AdaCore Blog Introduced

AdaCore has joined the blogosphere with the launch of its blog earlier this year. The format allows immediate communication on a much wider range of topics than are practical through traditional channels, and an opportunity to interact directly with various user communities on an informal basis. Subject matter encompasses industry news and trends, opinion pieces, and company technology and product information.

In the short time that the site has been up, a number of posts have attracted considerable interest. “Tetris in SPARK on ARM Cortex M4” (blog.adacore.com/tetris-in-spark-on-arm-cortex-m4) by Tristan Gingold and Yannick Moy details their work creating a SPARK version of the popular game

Tetris on an Atmel SAM4S ARM microprocessor. All the code and tools are available for download, so blog visitors can build the game at home.

Another SPARK-related post, this one on replacing existing drone firmware written in C, elicited a number of comments. “How to prevent drone crashes using SPARK” (blog.adacore.com/how-to-prevent-drone-crashes-using-spark) gives a step-by-step account of the work of AdaCore intern Anthony Leonardo Gracio in proving that a version of the Crazyflie stabilization system from Swedish company Bitcraze, rewritten in SPARK, is free of run-time errors.

Have a look at blog.adacore.com and join the conversation!

technology corner

Ghost Code in SPARK 2014

Ada 2012 defines powerful features for specifying program properties, for example the preconditions and postconditions of a subprogram. Such properties are expressed through the language’s contract or assertion syntax, and they may be verified dynamically by testing or (for SPARK code) statically by proof. But sometimes the variables and functions that are present are not sufficient to specify the needed properties. One approach is to introduce additional variables and functions, which will then only be used for the purpose of verification. But in a certification context such as DO-178B or DO-178C the additional code will then need to be verified at the same level as the application. This means performing structural coverage analysis, showing traceability to requirements, and demonstrating absence of interference between this verification-related code and the rest of the program if the verification code is to be deactivated in the final executable. A better solution is to use so-called “ghost code”.

GNAT defines a new aspect named Ghost that can be attached to variables, types, subprograms, and packages to indicate that these entities are only used in verification code. The compiler checks that such code indeed only appears in contracts, assertions, the definition of other ghost entities, and ghost statements (assignments to ghost variables and calls to ghost procedures). As a benefit, any unintended interference between verification-related code and application code is caught automatically, and the verification code can be removed when the final executable is built (hence the name ‘ghost code’).

Various kinds of ghost code are useful in different situations:

- ▶ Ghost functions can express properties used in contracts.
- ▶ Global ghost variables can keep track of the current state of a program, or maintain a log of past events. This information can then be referenced in contracts.
- ▶ Ghost types are types that are only used for defining ghost variables.

For a complete example, please see the Tetris code in an article posted to the AdaCore blog (blog.adacore.com/tetris-in-spark-on-arm-cortex-m4). A state automaton that the program is supposed to emulate is encoded as subprogram contracts, with the ghost type State expressing the possible states of the automaton:

```
type State is (Piece _ Falling, Piece _ Blocked, Board _ Before _ Clean, Board _ After _ Clean) with Ghost;
```

The current state of the automaton is maintained in a global ghost variable Cur _ State:

```
Cur _ State : State with Ghost;
```

This variable is updated as required in the various subprograms, to encode the semantics of the state automaton, while the main invariant property of the program is expressed as a ghost expression function:

```
function Valid _ Configuration return Boolean is
  (case Cur _ State is
    when Piece _ Falling | Piece _ Blocked => No _ Overlap (Cur _ Board, Cur _ Piece),
    when Board _ Before _ Clean => True,
    when Board _ After _ Clean => No _ Complete _ Lines (Cur _ Board))
with Ghost;
```

This function is called in subprogram contracts to ensure that it is preserved by all operations, for example:

```
procedure Do _ Action (A : Action; Success : out Boolean) with
  Pre => Valid _ Configuration,
  Post => Valid _ Configuration;
```

In a SPARK context, the GNATprove tool will check additionally that ghost code cannot have any effect on the behavior of the program. For an overview of the possible uses of ghost code in SPARK, please see the SPARK User’s Guide: docs.adacore.com/spark2014-docs/html/ug/spark_2014.html#ghost-code. And for the detailed rules defining ghost code, please see the SPARK Reference Manual: docs.adacore.com/spark2014-docs/html/lrm/subprograms.html#ghost-entities.

upcoming events

Ada Course in Paris

A 5-day course on Ada fundamentals will be held at the company's Paris offices during **October 26-30**, consisting of lectures and hands-on workshops using the latest AdaCore tools. The course will cover language basics as well as topics relevant to embedded systems applications and will explain important Ada 2012 features including contract-based programming. The course is open to the public and does not require previous Ada experience.

For registration information and a detailed schedule please visit www.adacore.com/public-ada-training/.

AdaCore Tech Days in Paris and Boston

AdaCore's annual user's group meeting is being expanded this year, with conference-style events scheduled on both sides of the Atlantic during Autumn 2015. At these AdaCore Tech Days company staff will present the latest news about current products as well as a roadmap for future plans. Attendees will receive an update on the CodePeer deep static analysis tool, learn how QGen can simplify the certification effort when model-based development is used and how SPARK 2014 can integrate formal verification with testing, and gain insights into a number of other facets of AdaCore's technology. The agenda will include presentations from users describing their experience with AdaCore products as well as a session on AdaCore's educational and training activities, and ample time will be reserved for questions and answers.

The Paris AdaCore Tech Day will be held on Thursday, **October 1**.

The Boston-area AdaCore Tech Days will be held Tuesday and Wednesday, **November 3 and 4**, and will include workshop/training sessions. Attendees will get hands-on practice with tools such as AdaCore's cross-compiler to bareboard ARM, gain experience with the GPS and Workbench IDEs, and also learn from tutorials including an introduction to Ada 2012's contract-based programming.

For a detailed agenda and specific venue/registration information, please visit www.adacore.com/techdays.

software tools

A Complete High-Integrity Software Development Stack

At the December 2014 Flight Software Workshop hosted by NASA's Jet Propulsion Laboratory in Pasadena, CA, Tucker Taft made a presentation describing a comprehensive approach to developing and verifying High-Integrity software. By complementing traditional testing-based methods with a "stack" of tools supporting static analysis, formal methods, and model-based design, users can gain confidence in code quality compliant with the highest levels of software integrity standards. AdaCore's product line illustrates this approach, offering advanced static analyzers such as CodePeer, program proof systems such as GNATProve for SPARK, and model-driven code generators such as QGen. For a video of the presentation please visit youtube.com/watch?v=Z4QkItGfFnA.

calendar highlights / May–November 2015

For up-to-date information on conferences where AdaCore is participating, please visit www.adacore.com/events/.

Embedded Systems Conference Boston May 6–7, 2015 / Boston MA, USA

AdaCore was an exhibitor at this event.
www.embeddedconf.com/boston/

Unmanned Systems 2015 / AUVSI May 4–7, 2015 / Atlanta GA, USA

AdaCore was an exhibitor at this event.
www.auvsihow.org/auvsi2015/public/enter.aspx

Test et Méthodes Formelles June 16, 2015 / Toulouse, France

Cyrille Comar led a panel discussion on the status of testing and formal methods.
projects.laas.fr/IFSE/FMF/

Ada-Europe 2015 June 22–26, 2015 / Madrid, Spain

AdaCore was a sponsor and exhibitor at this conference. Tutorials were presented by Pat Rogers ("Real-time/Embedded Programming with Ada 2012") and Ben Brosgol and Emmanuel Briot ("When Ada Meets Python: Extensibility through Scripting").
www.ada-europe.org/

UK Space Conference 2015 July 13–15, 2015 / Liverpool, UK

AdaCore was an exhibitor at this event.
www.ukspace2015.co.uk/

Embedded Systems Conference Silicon Valley July 20–22, 2015 / Santa Clara CA, USA

AdaCore was an exhibitor at this event.
www.embeddedconf.com/silicon_valley/conference/

International Conference on Model Transformation 2015 July 20–24, 2015 / L'Aquila, Italy

Elie Richa presented "Translating ATL Model Transformations to Algebraic Graph Transformations".
www.model-transformation.org/

AdaCore Tech Day 2015 / Europe October 1, 2015 / Paris, France

www.adacore.com/techdays/eu

Public Ada Training 2015 October 26–30, 2015 / Paris, France

www.adacore.com/public-ada-training/

AdaCore Tech Days 2015 / USA November 3–4, 2015 / Boston MA, USA

www.adacore.com/techdays/us

ARM TechCon November 10–12, 2015 / Santa Clara CA, USA

AdaCore will be exhibiting at this event at Booth 217.
www.armtechcon.com/

Inside AdaCore is published twice a year simultaneously in New York and Paris by AdaCore.

150 W. 30th Street, 16th floor
New York, NY 10001, USA
tel +1 212 620 7300
fax +1 212 807 0162

46 rue d'Amsterdam
75009 Paris, France
tel +33 1 49 70 67 16
fax +33 1 49 70 05 52

info@adacore.com
www.adacore.com

AdaCore
The GNAT Pro Company

© Copyright 2015 AdaCore. All rights reserved.
All trademarks are the property of their respective owners.