Spring/Summer 2016

- GNATcoverage Extends Platform Support, Adds Features
- AdaCore Tech Days 2016
- Interview with Jamie Ayre
- QGen update
- Spotlights a GAP Member: Technical University of Munich (Germany)
- Public Ada Training in Boston and Paris
- AdaCore Sponsoring Ada Programming Competition
GNATcoverage Extends Platform Support, Adds Features

GNATcoverage, AdaCore’s non-intrusive tool for structural code coverage analysis, will see a number of significant enhancements in 2016. The tool is being offered on a variety of new native and cross platforms, with a number of new features.

For native applications, possibly requiring full Ada run-time semantics, GNATcoverage is now available for 32-bit Windows; it relies on the DynamoRIO dynamic monitoring framework to produce execution traces. The new Windows support complements GNATcoverage’s existing native solutions on 32-bit and 64-bit Linux environments. Work to support 64-bit Windows applications is underway.

For cross configurations and unit-testing campaigns based on GNATemulator, GNATcoverage now handles a range of ARM targets. In addition to Leon, Leon3, PowerPC and E500v2, GNATcoverage provides off-the-shelf solutions for two standard boards equipped with ARM Cortex M4 and ARM Cortex R4 cores. Work is in progress on expanded support for integration testing campaigns when suitable probes can provide traces from execution on real hardware boards.

GNATcoverage is also adding several new features in upcoming releases. An improved coverage consolidation engine will let users combine intermediate coverage results instead of relying on raw execution traces, resulting in better performance and increased flexibility. Support for coverage analysis on code in dynamic libraries is also in progress, as is work on controlling/preventing propagation of so called “incidental coverage” effects. (A unit’s incidental coverage is the partial coverage it receives based not directly on the tests designed for that unit, but indirectly from tests of other code which happen to invoke the given unit).

Additionally, the GNATcoverage team is investigating how several Ada 2012 features affect compliance with coverage-related DO-178B/C objectives, and a paper on that topic was presented at the Embedded Real Time Software and Systems conference in January 2016. For example, expressions appearing in assertion-based contracts (such as pre- and postconditions) need to be taken into account, and likewise expressions in control expressions (if, case).

These enhancements and ongoing work preserve GNATcoverage’s key characteristic: to allow precise assessments of object-level or DO-178B/C source-level coverage criteria up to MC/DC without instrumenting the application program. Instead, instrumented operating environments provide execution traces that the tool maps back to source constructs, based on debug information and Source Coverage Obligations (SCO) tables produced by the compiler. The non-intrusive nature of GNATcoverage simplifies the software certification effort, and the tool has been qualified as a verification tool for several airborne systems.

For further information please visit www.adacore.com/gnatcoverage/.

Additional GNATcoverage Output Example
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.

BOSTON, MA SEP 21-22, 2016  PARIS, FRANCE OCT 6, 2016

www.adacore.com/techdays
AdaCore's QGen model-based development toolset continues to grow. One of its newest capabilities is support for Processor-In-the-Loop (PIL) simulation: users can take the code that QGen generates from a Simulink®/Stateflow® model and execute it on both emulated and hardware targets. Models can thus be tested in realistic environments, directly from the Matlab® console. Another new feature, now available for beta testing, is the QGen model-level debugger. It supports a synchronized view of the model and the corresponding source code while debugging, along with the ability to set block-level breakpoints in auto-generated code and to display and set signal values when stopped at such breakpoints. Recent usage of QGen in industrial settings confirms that it can generate efficient code for very large models and also support development using multiple versions of the Simulink® environment, from R2008a through R2016a. Several new videos are available on the AdaCore website demonstrating QGen's various capabilities. For additional information please visit www.adacore.com/qgen.
Spotlighting a GAP Member

### Technical University of Munich (Germany)

#### A weather balloon that comes back to its takeoff location

The Real-Time Computer Systems group at the Technical University of Munich is developing a light-weight weather balloon that climbs up to the stratosphere, logs data such as pressure, wind, and temperature, and subsequently performs a controlled descent back to the takeoff location. The operators can thus conveniently retrieve the payload of high-rate sensor data and save the equipment for later reuse. Since ordinary weather balloons can drift away hundreds of kilometers and might never be located, the homing function is a major advantage. The core of the system is a fixed-wing glider configuration that needs to be stabilized and guided home by an on-board autopilot, without external control.

Mr. Martin Becker, a PhD candidate in the Real-Time Computer Systems group, is Project Director, and much of the work is being done in the context of graduate theses. Since the University is a member of AdaCore’s GNAT Academic Program (GAP), the group has chosen the latest Ada/SPARK environment to develop and verify the autopilot software. “We had some experience verifying C programs, where we learned that a large portion of the software defects stemmed from weaknesses in the language,” said Mr. Becker. “By choosing SPARK together with the Ravenscar run-time, we get the strict semantics that we need, the ability to use well-structured concurrency features, and the formal underpinning to identify defects by analysis. This gives us high confidence in the software’s correctness while also saving testing and debugging effort; there’s no need to extensively test all the possible failure scenarios and simulate the environmental conditions.”

The glider weighs less than 1kg and will have to cope with wind speeds above 100km/hour and temperatures below -40°C. Fitting the necessary electronics brings the system close to its power and weight limits. Thus there is no room for redundancy, and failures need to be avoided by construction as far as possible.

“We know, before running the program the first time, that we will not have run-time errors, and this allows us to invest more time addressing the challenges with the airframe and sensors,” added Mr. Becker. “Additionally, the software is being designed to detect and mitigate hardware failures as far as possible, so our verification efforts will also include proving the high-level behavior for specific failure cases.”

As part of this project the group is porting the ARM Cortex M4 STM32F4 bareboard run-time with the Ravenscar Small Footprint profile to the Pixhawk flight controller, and rewriting those parts in SPARK where formal verification is most useful. The launch of the weather balloon is expected later this year.

To find out more about this project please contact Martin Becker at becker@rcs.ei.tum.de, and for information about GAP please visit [www.adacore.com/academia/](http://www.adacore.com/academia/).

### Ada training

#### Ada Programming with GNAT: Fundamentals

AdaCore is holding public Ada courses in its Paris and Boston (Lexington) offices during the week of November 14–18. Combining live lectures and hands-on workshops using the latest GNAT toolsuite, these courses will cover major features of the Ada language and explain important points of software engineering style. Attendees will learn Ada essentials such as the datatype system, exceptions, packages / encapsulation, separate compilation, and generics. The courses will focus on Ada 95 and will also cover recently added features such as Ada 2012’s contract-based programming support. No previous experience with Ada or the GNAT tools is required.

For a detailed outline and pricing/registration information please visit [www.adacore.com/training/](http://www.adacore.com/training/).

#### AdaCore Sponsoring Ada Programming Competition

Enter the “Make with Ada” competition for a chance to win 5000 euros!

To help promote the use of Ada, AdaCore is sponsoring a competition to design and implement an embedded software project where Ada and/or SPARK are the principal language technologies. This “Make with Ada” competition will award five prizes, based on the criteria of software dependability, openness, collaborativeness, and inventiveness. For example, entrants will need to demonstrate that their system meets its requirements and has been developed using sound software engineering practices. The top prize is 5000 euros.

By encouraging the use of Ada and SPARK, the competition aims to help the embedded software community improve the quality of their code. It is open to individuals and to teams of up to four people; participants should have a new idea for an embedded system and a desire to realize that idea using Ada or SPARK.

For more information please visit [www.makewithada.org/](http://www.makewithada.org/).

### Newsflash

#### Ada UK launched

The Ada UK technical society has been chartered to promote the Ada language in the UK as a means of improving software quality. The new group, a successor to its namesake society that was active around Ada 83, will be a member organization of Ada-Europe and will represent the interests of the growing number of Ada users in the UK in aerospace and other industries. For further information please contact Dene Brown at denebbrown@gmail.com.

#### HIS 2016 conference presents best practices

This year’s High Integrity Software conference will be held in Bristol UK on November 1. Featuring experts from industry and academia, HIS 2016 will highlight best practice across a variety of safety- and security-critical domains. Dino Distefano (Facebook) and Duncan Brown (Rolls Royce) will be keynote speakers. To see the full program and to register, please visit [his-2016.co.uk](http://his-2016.co.uk).
newsflash

CodePeer officially registered as CWE-Compatible

The MITRE Corporation has awarded AdaCore’s CodePeer advanced static analysis tool the formal designation of “CWE-Compatible” in their Common Weakness Enumeration (CWE) Compatibility and Effectiveness Program, a web-based initiative that consolidates and organizes information about cyber security products and services. CodePeer can detect several of the Top 25 Most Dangerous Software Errors in the CWE: CWE-120 (Classic Buffer Overflow), CWE-131 (Incorrect Calculation of Buffer Size), and CWE-190 (Integer Overflow or Wraparound). For details please visit cwe.mitre.org/compatible/program.html and cwe.mitre.org/compatible/organizations.html.

ProofInUse joint lab with Inria helps enhance SPARK toolset

The ProofInUse cooperative project between AdaCore and French research institute Inria has completed its second year, successfully achieving several milestones in connection with its underlying goal of solving hard problems in formal verification technology. The overall usability of the SPARK environment has been enhanced with the ability to generate counterexamples when an automatic proof fails, and the Why3 engine can now automatically prove bitwise and modulo operations. These results were being presented at a NASA Formal Methods symposium in June and at a Software Engineering and Formal Methods conference in July (see the calendar highlights section of this newsletter). Work is continuing on the proof of floating-point properties and on interactive proof. For more information please visit www.spark-2014.org/proofinuse/.

EN 50128 booklet available

A booklet is available explaining how AdaCore’s technologies can help developers meet the requirements of the CENELEC EN 50128:2011 safety standard on software for railway control and protection systems. Authored by CERTIFER safety assessor Jean-Louis Boulanger and AdaCore’s Quentin Ochem, this booklet summarizes the EN 50128 standard and describes how the Ada and SPARK languages together with AdaCore tools and run-time libraries can be used to develop software up to the highest safety integrity level. For a free copy of this booklet please contact info@adacore.com; a pdf version is available on line at adacore.com/en-50128/.

HILT 2016 workshop focusing on model-based development

ACM’s Special Interest Group on Ada (SIGAda) will be holding an open workshop on Model-Based Development and Contract-Based Programming during October 6 and 7 in Pittsburgh, as the latest in its series of High Integrity Language Technology (HILT) conferences and events. HILT 2016 will be part of the Embedded Systems Week activities and will feature Prof. Philip Koopman (Carnegie-Mellon University) and John Knight (University of Virginia) as keynote speakers. The HILT workshop will provide a forum for researchers and practitioners to discuss tool and language technologies that offer a formal approach to model-based development. For further information including a link to a registration page please visit www.sigada.org/conf/hilt2016/.

calendar highlights / July–November 2016

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

SEFM 2016: International Conference on Software Engineering and Formal Methods
July 4–8, 2016 / Vienna, Austria

David Hauzar is presenting a paper “Counterexamples from Proof Failures in SPARK”. staf2016.conf.tuwien.ac.at/sefm/

GNU Cauldron
September 9–11, 2016 / Hebden Bridge, UK

AdaCore is a major sponsor and exhibitor. gcc.gnu.org/wiki/cauldron2016

AdaCore Tech Days 2016—US
September 21–22, 2016 / Burlington MA, USA

AdaCore is holding its annual customer-focused Tech Days event. www.adacore.com/techdays/

DASC 2016: 35th Digital Avionics Systems Conference
September 25–29, 2016 / Sacramento CA, USA

AdaCore is a sponsor / exhibitor at this event. 2016.dasconline.org/

ARM TechCon
October 25–27, 2016 / Santa Clara CA, USA

AdaCore is exhibiting at this event. www.armtechcon.com

High Integrity Software (HIS) 2016
November 1, 2016 / Bristol, UK

AdaCore is a major sponsor and an exhibitor. his-2016.co.uk

Public Ada Training
November 14–18, 2016 / Lexington MA, USA and Paris, France

AdaCore is conducting an Ada Fundamentals course at its Boston-area and Paris offices. www.adacore.com/training

Embedded Software Engineering (ESE) Kongress
November 28–December 2, 2016
Sindelfingen, Germany

AdaCore is exhibiting at this event. www.ese-kongress.de/english/