

GNAT Pro insider

an AdaCore Publication
Autumn/Winter 2011–2012
www.adacore.com

newsflash

Siemens selects GNAT Pro and CodePeer

The Mobility Division of Siemens Switzerland has chosen GNAT Pro, along with the CodePeer static analysis tool, to develop the next generation of its railway control and information system. The Siemens railway control system is a modern networked application that covers every aspect of the railway control domain. The developed architecture guarantees high availability in accordance with European railway software standards. The current version of the system controls the train traffic throughout major parts of Switzerland and also parts of Austria, Hungary and Malaysia.

Thales selects GNAT Pro High-Integrity Edition

Thales Airborne Systems has chosen the GNAT Pro High-Integrity Edition to develop onboard instrument software for the next generation of the Argos satellite project. Argos is a unique, satellite-based worldwide location and data collection system dedicated to studying and protecting the environment. In addition to these core tasks, the Argos satellite family has a number of safety- and security-related functions, including boat position determination, territorial security, and law enforcement.

contents

GPS 5.1 Strengthens Multi-Language Support, Tightens CodePeer Integration	1
GNATcoverage wins Electron d'Or Prize	1
Current Releases	2
In the Pipeline	2
Academia Corner: University of Southampton, UK	2
Interview with JC Berredo	3
Webinar Schedule	3
SPARK Prevents Software Vulnerabilities	3
Technology Corner: Contract-Based Programming in Ada 2012	4
Conferences/Events	4

GPS 5.1 Strengthens Multi-Language Support, Tightens CodePeer Integration

A new major release of the GNAT Programming Studio (GPS) IDE brings a number of enhancements including extended support for C and C++, improved integration with the CodePeer automated code review and validation tool, more powerful source editing, and improved GUI performance.

Mixed-language development is common on large projects. To make it easier to write and browse applications involving Ada and other languages, GPS has enhanced its support for C and C++ in several areas:

- ▶ Basic support for a new feature, smart completion of identifiers, is available for variables, types/classes, and macros.
- ▶ New support for Ada-to-C navigation allows the developer to go directly from the invocation of a C function to its Ada specification, and then immediately bring up the corresponding C function body.
- ▶ GPS now supports navigation in C itself, from a function call to its definition and vice versa, as well as call graph construction.

GPS 5.1 provides better integration with CodePeer. Among the enhancements are new views for race conditions (global data used across tasks without protection) and for "score cards" (total passed/checks counters per file or project). The GPS locations view is now synchronized with CodePeer reports, so that clicking on a CodePeer diagnostic will highlight

the relevant line in the GPS locations view. More flexible filtering allows the user to focus on either warnings or checks. And to facilitate sharing across a development team, the GPS/CodePeer integration supports alternate database/output directories.

A variety of other new features combine to improve the IDE's overall quality and scope. Here are some examples:

- ▶ Based on customer suggestions, GPS now allows centralized handling of all Version Control System menus, making it easier to perform customization.
- ▶ The browser contents are drawn using vector graphics, allowing export to pdf.
- ▶ A number of new automatic code fixes have been added.
- ▶ Users can interactively specify the metrics to be computed by GNATmetrics.

GPS 5.1 is compatible with GNAT Pro versions 3.16a1 through 6.4.2. It is available on a wide variety of host configurations, including platforms running Linux, Solaris, and Windows. To learn more, please contact info@adacore.com.

GNATcoverage Wins Electron d'Or Prize

In June 2011 the GNATcoverage tool was awarded an *Electron d'Or* prize in the Software Tools category. This annual prize, sponsored by the French trade publication *Electroniques* magazine, is awarded to the most innovative products in several different categories, highlighting technologies that will have a significant impact. The jury for the Software Tools category consisted of industry experts who recognize the importance of Open Source tools for software certification.

Originally developed as part of the Couverture research project, GNATcoverage performs coverage analysis on both Ada and C language source code and also on object code, without requiring instrumentation. GNATcoverage helps software developers assess the breadth of a testing campaign and meets the needs of software safety certification standards such as DO-178B and its upcoming revision, DO-178C, for avionics.

Breaking News

AdaCore and SofCheck are merging!
For up-to-date information, please see www.adacore.com.

SPARK Pro 10

The SPARK Pro 10 release includes a number of important enhancements:

Automatic selection of flow analysis mode

The Examiner now supports automatic selection of information flow or data flow analysis on a per subprogram basis.

KCG language profile

A new language profile developed by Altran Praxis and Esterel Technologies has been added to the Examiner for processing automatically-generated SPARK code produced by Esterel's KCG code generator for SCADE.

Derived numeric types

New language and tool support for explicitly derived numeric types simplifies the programming of numeric applications.

SPARKBridge preview for Windows

SPARKBridge—a bridge between the SPARK tools and Satisfiable Modulo Theories (SMT) solvers—is now available as a preview on Windows platforms, allowing users to try alternate provers for discharging Verification Conditions.

Library additions

The SPARK library has been augmented with several new packages including Interfaces, Ada.Characters.Handling, and Ada.Text_IO

Improvements to proof tools

The Simplifier now has enhanced reasoning capabilities for modular types, allowing more proofs to be automatically discharged. In addition, the proof summary output (from the POGS tool) has been improved, making it easier for large projects to manage the proof process.

GNATbench 2.6

The latest version of GNATbench supports Eclipse 3.7 and implements a number of ergonomic improvements including new view expansions based on user actions, and additional tooltip functionality. The debugger for the Eclipse/CDT version of GNATbench has also been enhanced. Among its new features is support for breakpoints on exceptions, with control over the desired triggering action (a specific exception or any exception, whether handled or unhandled, and so on). In addition, the QuickFix facility now repairs a wider range of constructs, such as redundant "with" clauses and unnecessary type conversions.

Ada in Research and Teaching University of Southampton, UK

The University of Southampton's Electronics and Computer Science Department uses Ada as a target language in their Formal Methods research, and has introduced Ada for student projects with Lego Mindstorms.

The research interests of the new Electronics and Software Systems group include the formal specification of embedded systems, using the Event-B modeling language. Ada is an attractive target for code generation, and its use has attracted interest from a number of industrial partners in fields such as aerospace, automotive, mass transportation, and space systems.

The Event-B modeling language is based on set theory, with refinement semantics for representing different layers of abstraction and with proof techniques for checking both model consistency and consistency between different abstraction levels.

The language is supported by an Open Source toolset, the Rodin platform plug-in for Eclipse. Rodin includes editors, powerful proof tools, and a variety of extensions. Event-B models may be annotated to facilitate code generation. For the research group at the University of Southampton, Ada is the preferred code generation target, with its multi-tasking and encapsulation facilities especially useful. The research work in this area is part of the EU-funded Deploy project: www.deploy-project.eu.

On the teaching side, the university has introduced an Ada-based fourth-year student Group Development Project, to engineer a "model" automotive application. They are using Lego Mindstorms, with the GNAT GPL version. In future work it is hoped to link Event-B to Mindstorms through Ada. As stated by Dr. Andy Edmunds: "We would like to enthuse students by showing that there are some interesting practical aspects to Formal Methods. In addition to the educational value, experience gained using the Lego sensors and actuators could be of use when conducting research with the safety-critical systems that we are interested in".

Contact information for Dr. Edmunds: ae2@ecs.soton.ac.uk

A number of products are scheduled for release during Q1 2012.

GNAT Pro 7.0

The next major release of the GNAT Pro Ada Development Environment will provide complete Ada 2012 support as well as new or improved features in several areas.

► **Compiler** Enhancements include a new implementation of controlled types with better memory usage, improved diagnostic messages, optimizations for array processing (less intermediate copying, more parallelization opportunities) and composite return values, and more compact debugging information.

► **Tools** Improvements have been made to GNATpp and GNATmetric, and the new GNATtest automatic test framework tool, described below, is being launched.

► **Run-Time Libraries** A variety of new target configurations are supported, including Ravenscar bareboard on PowerPC, Multicore Ravenscar, Ravenscar Cert for VxWorks 6 Cert Real-Time Processes, and Zero-Cost Exceptions in the run-time library for VxWorks 6 kernel-smp.

GNATtest

The new GNATtest tool helps create and maintain a complete unit testing infrastructure for complex projects. Based on AUnit, it captures the simple idea that each visible subprogram should have at least one corresponding unit test. GNATtest takes a project file as input, and produces two outputs:

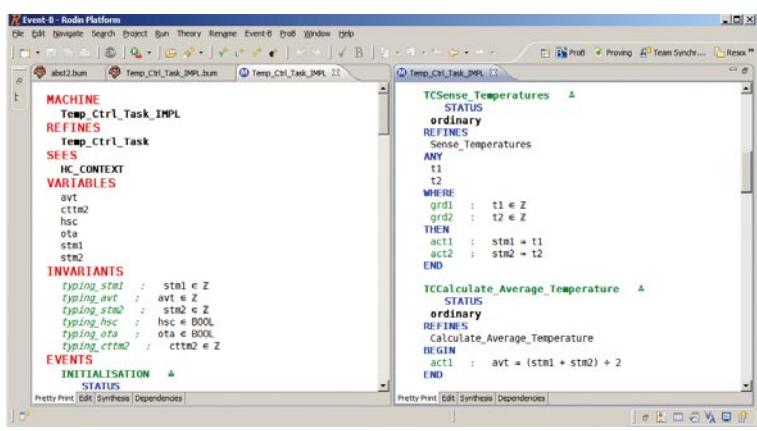
► The complete harnessing code for executing all the unit tests under consideration. This code is generated completely automatically.

► A set of separate test stubs for each subprogram to be tested. These test stubs are to be completed by the user.

GNATtest handles Ada's Object-Oriented Programming features and can be used to help verify tagged type substitutability (the Liskov Substitution Principle) as required by the upcoming DO-178C avionics software safety standard.

CodePeer 2.1

The next release of the CodePeer automated code review and analysis tool will provide a variety of enhancements, including full support for Ada 2012, detection of uninitialized global variables, more precise preconditions, more extensive analysis for race conditions, improved support for access-to- subprogram types, and improved handling of unused assignments.



Event-B Screen Snapshot (Rodin Platform)



Interview with Juan Carlos (JC) Bernedo Director of Strategic Accounts, AdaCore US

Tell us about your background and how you came to be involved with Ada and AdaCore. What is your current role?

started back then, and the computer industry was going through one of its periodic technological earthquakes. This all looked pretty exciting to a new college graduate, so I moved into the computer field and got a variety of different perspectives from jobs at SAIC, Cachebox, and GTE Government Systems. My background is technical, but I am very much a “people person”. On one occasion, after I had presented an enterprise deployment design for a DoD program, one of my colleagues told me that I should be in technical product sales. I soon had the chance to see if he was right; I accepted a job offer from Aonix as a sales representative selling Ada compilers to Department of Defense integrators. I found that I definitely enjoyed this kind of work, and after Aonix I joined Harris Corporation selling security solutions to various federal departments. This was a very good growth experience and gave me a perspective on sales to government agencies and contractors. I joined AdaCore in 2007 as Director of Strategic Accounts, where my past experience in sales and customer relationships is proving very valuable.

You've been in Sales-related positions for more than ten years, so you have a direct customer-centric perspective. Any "lessons learned" from your experience?

touch with its customers, on a personal level, to understand their real requirements. Second, have an adaptable technology that can accommodate new requirements smoothly. At AdaCore we've been pretty successful on both fronts. It's my job, and the job of my sales colleagues, to keep in regular contact with our customers so that we know the directions they want to take with our products. Also, the way that we handle support, with questions going directly to the product developers, means that we get an immediate “heads up” on how our products are being used. New features in a product like GNAT Pro often result from customer comments and requests that come through our frontline support. And as far as our technology is concerned, it has proved to be highly adaptable over the years. There are technical reasons for this, but an important factor is our Open Source approach. This makes it easier for us to take advantage of complementary tools and products, as we did in developing the GNATemulator tool based on QEMU.

Any hobbies or outside interests that you'd like to share?

There's an old saying, “the customer is always right”. The mistake I've seen at some companies is to try to sell technology that might be top notch but doesn't solve the real problems that the customer has. So a company needs to do two things. First, stay in

My background is technical, so maybe it's not too surprising that I enjoy building my own computers, configuring my home theater/stereo setup, etc. I also love playing video games. And for something completely different, I have a pet parrot who can say a few words in both English and Spanish.

Webinar Schedule

A webinar introducing and demonstrating the new GPS 5.1 features was presented by Nicolas Setton on November 15. To view this webinar, or to learn more about the AdaCore webinar series, please visit www.adacore.com/home/products/gnatpro/webinars/

SPARK Prevents Software Vulnerabilities

In a study sponsored by the National Institute for Standards and Technology (NIST) in the U.S. and presented at the November 2011 ACM SIGAda conference, Dr. Joyce Tokar and her colleagues analyzed the SPARK language and toolset against twenty-one weaknesses from the Common Weakness Enumeration (CWE) database. Fifteen of these weaknesses would not occur at all, or else be detected by the SPARK tools. The others are either at a higher semantic level (for example hard-coded passwords) or are associated with concurrent accesses to files (which are outside the scope of SPARK protection). Dr. Tokar's study, which received the Best Paper award at the SIGAda conference, updates an earlier report that was cited by a NIST analysis of programming language vulnerabilities. The NIST publication—Source Code Security Analysis Tool Functional Specification Version 1.1 (NIST Special Publication 500-268 v1.1)—also considered C, C++, and Java, and concluded that SPARK had the fewest vulnerabilities.

Contract-Based Programming in Ada 2012

Ada 2012 directly supports *contract-based programming*: the ability to associate Boolean conditions (dynamic "contracts") with declared program entities. The contracts can be automatically checked at specific points in the program's execution.

The contracts likely to be of most benefit are subprogram preconditions and postconditions. A subprogram's caller has to ensure that the precondition holds when the subprogram is invoked; the implementer of the subprogram can then assume that the precondition holds upon entry. The implementer has to ensure that the postcondition is satisfied when the subprogram returns, and the client (caller) can then assume that the postcondition holds. This combination of requirements and permissions defines the subprogram's contract.

As an example, the procedure in the adjacent program fragment pushes a value onto a (fixed-size) stack whose element type is named Element. For simplicity Stack is declared as a record type rather than a private type.

The Check argument to the Assertion_Policy pragma means that the violation of either a precondition or postcondition will raise the Assertion_Error exception.

The Not_Full function illustrates a new Ada 2012 feature, the ability to provide an expression as a function implementation in a package specification. This is especially useful for a function invoked in a subprogram's pre- or postcondition, since the function implementation is in effect part of the interface for the subprogram.

The Push procedure includes both a precondition and a postcondition. (These are examples of "aspects" in Ada 2012.) The notation S'Old in the postcondition means the value of S on entry to the procedure. The postcondition reflects the semantics of Push: the element E is inserted at the position defined by the new Length, and the values at all other positions are unchanged. (The last term in the postcondition uses the new quantification syntax for purposes of illustration; it could have been expressed more succinctly using a slice comparison.)

Contracts apply to private types as well as concrete types and may be used with Ada's Object-Oriented Programming features.

The contract facility is already being utilized in practice. The Hi-Lite research project www.open-do.org/projects/hi-lite/ is developing a new verification strategy that combines formal proofs and testing, with Ada 2012's contract-based programming features serving as foundation.

```

pragma Assertion_Policy(Check);

package Stacks is

    type Vector is array (Positive range <>) of Element;

    type Stack (Max_Length : Natural) is
        record
            Length : Natural;
            Data   : Vector (1..Max_Length);
        end record;

    function Not_Full (S : Stack) return Boolean is
        (S.Length < S.Max_Length); -- Expression function

    procedure Push (S : in out Stack; E : in Element)
    with -- new aspect notation
        Pre => Not_Full (S),
        Post =>
            (S.Length = S'Old.Length+1) and
            (S.Data (S.Length) = E) and
            (for all J in 1 .. S'Old.Length =>
                S.Data (J) = S'Old.Data (J));
            ...
    end Stacks;

```

Conferences / Events ■ October 2011 – May 2012

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

SCADE User Group Conference October 13–14, 2011 / Paris, France

AdaCore is a sponsor and exhibitor.

www.estrel-technologies.com/news-events/events/2011/sugc/

ACM SIGAda 2011 November 6–10 / Denver CO, US

AdaCore is a Platinum level sponsor and exhibitor. Ben Brosgol is presenting a tutorial on the upcoming DO-178C avionics safety standard, and Greg Gicca is conducting a GNAT Birds-of-a-Feather session.

www.sigada.org/conf/sigada2011/

Medelec 2011 November 29, 2011 / Cambridge, UK

AdaCore is a Bronze level sponsor, and Quentin Ochem is giving a talk "Lessons to be learned from ultra-paranoid industries (or why software matters)".

www.medelec.co.uk/

Certification Together International Conference (CTIC) November 29–December 1, 2011 / Toulouse, France

AdaCore is a Platinum level sponsor of this event, and Michaël Friess is giving a talk "Efficient Safety-Critical Systems Development: is FLOSS the only answer?".

www.certification-together.com/

ERTS² (Embedded Real-Time Software and Systems) 2012
February 1–3, 2012 / Toulouse, France
AdaCore is a Platinum sponsor of this event, and AdaCore staff have authored or co-authored several papers: "Integrating Formal Program Verification with Testing" (Cyrille Comar, Johannes Kanig and Yannick Moy); "Compilation of Heterogeneous Models: Motivations and Challenges" (Matteo Bordin, Tonu Naks, Andres Toom and Marc Pantel); and "Formalization and Comparison of MCDC and Object Branch Coverage Criteria" (Cyrille Comar, Jerome Guittot, Olivier Hainque, Thomas Quinot).
www.erts2012.org/

Safety-critical Systems Symposium (SSS '12)
February 7–9, 2012 / Bristol, UK
AdaCore is a main sponsor of this event.
www.scsc.org.uk/ssss

Embedded World 2012
February 28–March 1, 2012 / Nuremberg, Germany
AdaCore is an exhibitor at this event, and Michaël Friess is presenting a paper on Open Source and Safety-Critical Systems.
www.embedded-world.de/en/

ESC (Embedded Systems Conference) Silicon Valley 2012

March 26–29, 2012 / San Jose CA, US

AdaCore is exhibiting at this conference.
esc.eetimes.com/siliconvalley/

Systems and Software Technology Conference (SSTC 2012)
April 23–26, 2012 / Salt Lake City UT, US
Ben Brosgol is delivering a presentation, "Object-Oriented Programming for High-Integrity Systems: Pitfalls and How to Avoid Them".
www.sstc-online.org/

The GNAT Pro insider is published twice a year simultaneously in New York and Paris by AdaCore

104 Fifth Avenue, 15th floor New York, NY 10011-6901, USA	46 rue d'Amsterdam 75009 Paris, France
tel +1 212 620 7300	tel +33 1 49 70 67 16
fax +1 212 807 0162	fax +33 1 49 70 05 52

info@adacore.com
www.adacore.com

AdaCore
The GNAT Pro Company