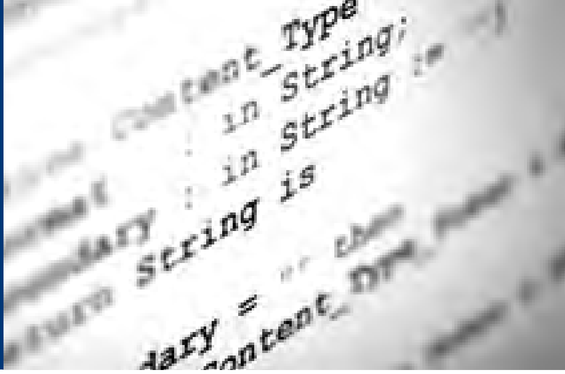
GNAT Pro insider

an AdaCore Publication
Spring 2010
www.adacore.com



newsflash

New Hire: Simplice Djoko Djoko

Simplice Djoko Djoko has joined AdaCore EU as a member of the CodePeer and Hi-Lite Project teams. Dr. Djoko has a background in formal methods, programming languages, and program verification, and he has recently completed a post-doctoral fellowship at the French Atomic Energy Commission in Saclay. Dr. Djoko completed his Ph.D. at INRIA Grenoble and École des Mines de Nantes, where his thesis investigated a formal framework for aspect-oriented programming.

GNAT Pro Available on LEON3

GNAT Pro has been ported to the LEON3, a configurable fault-tolerant system-on-a-chip that is designed for space applications. Hosted on 32-bit Linux platforms, the cross compilation toolset implements the full Ravenscar Profile and targets the UT-699 board. As part of the LEON3 development effort, AdaCore simulated the specific UT-699 target environment on low-cost field-programmable gate array (FPGA) hardware using third-party open source LEON3 VHDL specifications. Customers can adopt a similar approach and start development early, before their custom LEON3 hardware is available.

contents

CodePeer Launched 1
DO-178C Nearing Completion 1
Current Releases 2
In the Pipeline 2
Webinar Schedule 2
Academia Corner: University of Virginia 2
Interview with José Ruiz 3
AdaCore Awarded Grant for Hi-Lite Project 3
Technology Corner: Ada 2012 Nearing Completion 4
Open-DO Update 4
Conferences/Events 4
AdaCore at Wind River Regional Conferences 4

CodePeer Launched

The CodePeer source code analyzer / reviewer for Ada is now available. This tool identifies constructs that are likely to lead to run-time errors such as buffer overflows, and it flags legal but suspect code indicative of logic errors. Well surpassing typical static analysis tools, CodePeer also produces a detailed analysis of each subprogram, including pre- and postconditions. Potential bugs and vulnerabilities can thus be detected early: if the specification deduced by CodePeer does not match the component's requirements, a reviewer is alerted immediately to a likely logic error.

"Find the Bug" Challenge

Can you find as many bugs as CodePeer? The CodePeer page of the AdaCore website includes a program with some subtle errors. You can review the code yourself, and then click a button to compare your results with CodePeer's. The page also includes a video of AdaCore engineer Yannick Moy explaining CodePeer's analysis of the program. New programs will be posted periodically. See **www.adacore.com/home/products/codepeer/toolset/findthebug/**

CodePeer can be used productively during program development and upgrade, to prevent errors from being introduced or to augment a systematic code inspection process and thus maximize the efficiency of human review. It can also be used effectively on existing codebases, to detect and remove latent bugs.

CodePeer analyzes Ada programs for a wide range of flaws including pointer misuse, buffer overflows, numeric overflow or wraparound, division by zero, dead code, unused variables, and concurrency hazards (race conditions / improper or missing synchronization).

The tool is "sound" (no "false negatives"): if CodePeer does not flag any constructs for some specific category of error, then the program contains no errors in that category. Soundness is especially important for systems that need to comply with security and/or safety standards, since undetected vulnerabilities or hazards can lead to system penetration or failure.

CodePeer is efficient and, using an historic database, keeps track of the difference between any two runs. This minimizes the problems due to "false positives" (flagged constructs that are not real errors) since the user does not need to review the output for unchanged parts of the system. Moreover, CodePeer can work on partially complete programs, so units can be analyzed as required.

CodePeer was developed jointly by AdaCore and SofCheck and may be used either as a standalone tool or integrated into the GNAT Pro environment. For further information: **www.adacore.com/home/products/codepeer**.

DO-178C Nearing Completion

DO-178C, a revision to RTCA/EUROCAE's DO-178B software safety standard that governs commercial aircraft certification, is expected to be finalized later this year and officially accepted in 2011. The core document is substantially the same as DO-178B, with a number of clarifications and a few minor corrections. The major change is the inclusion of several supplements. One supplement deals with tool qualification, and three others adapt the core document guidance when specific technologies are used: Model-Based Development, Object-Oriented Techniques, and Formal Methods. AdaCore has been participating in the DO-178C revision process, with Dr. Cyrille Comar contributing to the Object-Oriented Techniques subgroup.

AdaCore has set up an infrastructure for producing DO-178C ready qualification material for GNATcheck, GNATstack, and tools from the "Couverture" project for structural coverage analysis up to level A. If you have specific questions about DO-178C related to AdaCore technology, do not hesitate to ask them through your GNAT Tracker account.

< current releases >

GNAT Pro 6.3

This major release is available on more than fifty native and cross platforms comprising hundreds of different environments (variations of Ada run-time libraries and host/target Operating System versions). Highlights include:

- CodePeer, a new add-on tool for automated code review and validation.
- C++ support as an option, for projects using C++ as well as Ada.
- Global tool improvements to the pretty printer (gnatpp), coding standard verifier (gnatcheck), stack size analyzer (gnatstack), and the C and C++ binding generators.
- Specific tool improvements
  - Unused dispatching subprogram elimination (gnatelim)
  - More flexible project handling
  - More efficient gnatmake and gprbuild
- Compiler and debugger enhancements
  - Many additional warnings
  - More flexibility in enabling/disabling warnings
  - Faster Unbounded_String implementation
  - Removal of redundant run-time checks
  - Support for Ada 2012 conditional expressions
  - Better code generation (speed and size)
  - More compact debugging information
  - Improved interfacing with C++

The 6.3 release also includes the latest versions of the GNAT Programming Studio (GPS 4.4) and GNATbench (2.4) IDEs. GPS 4.4 is compatible with GNAT Pro versions 3.16a1 up to 6.3.

SPARK Pro 9.0

The latest version of SPARK Pro, a joint offering from AdaCore and Altran Praxis, is a major release with many enhancements:

- New information-flow verification for safety and security policies, such as Bell-LaPadula, based on integrity labelling of own variables.
- New SPARK 2005 language profile, including 'Mod, 'Machine_Rounding, new reserved words, and the static semantics of "overriding".
- Detection of dead statements, branches and paths in SPARK code, complementing the Simplifier and POGS.
- Cross Referencing annotations in GPS.
- Treatment of function return annotations like procedure post-conditions. The annotations are substituted into the caller's VC hypotheses, thus greatly improving the theorem prover's effectiveness.
- A new output format for POGS designed to be both easier to read and easier to search automatically.
- Case checking, through a new Examiner switch that enforces consistent casing within code and annotations.

GPRbuild 1.4

The latest release of GPRbuild, a tool for constructing systems written in a combination of programming languages, offers a number of enhancements. Analysis is more precise, so GPRbuild is now much better at detecting implicit coupling between subsystems (option -no-indirect-imports). Performance is greatly improved on large projects, especially when remote disks are used, since the number of system calls has been significantly reduced. GPRbuild also supports new configurations including Apple Snow Leopard, LynuxWorks LynxOS 5, and SYSGO ELinOS.

< in the pipeline >

GNATstack

The GNATstack static stack analysis tool is being tightly integrated with GPS, making it easier for developers to use the tool and to visualize the stack usage information. GPS will gather the required data, launch GNATstack, and then display the worst-case call tree from any subprogram and annotate the subprogram with stack usage information.

GNATstack is also being enhanced to analyze object-oriented applications more precisely, automatically determining maximum stack usage on code that uses dynamic dispatching in both Ada and C++. A dispatching call challenges static analysis because the identity of the subprogram being invoked is not known until run time. GNATstack and the compiler will be able to statically determine the subset of potential target primitive operations for every dispatching call. This will heavilly reduce the analysis effort and will yield precise stack usage bounds on complex Ada/C++ code.

Webinar Schedule

Tuesday, April 27 / SPARK Pro 9.0

The InSight webinar series continues this Spring with a presentation by Robin Messer (Altran Praxis) on the new version of SPARK Pro, the AdaCore / Altran Praxis joint offering. The webinar discusses and demonstrates the new features of this major release and includes a question and answer session. To register, please visit **www.adacore.com/home/products/gnatpro/webinars**.

< academia corner >

Spotlighting a GAP Member
University of Virginia (USA)

At the University of Virginia, Ada lies at the core of a comprehensive approach to creating software for safety-critical applications.

Dr. John Knight and his student, Xiang Yin, have created a practical approach to formal verification called Echo. In Echo verification, a program written in SPARK Ada is verified to conform to its SPARK annotations using the SPARK tools. The developer then uses automated Echo tools to simplify the annotated code and extract a specification in the PVS language (PVS is a specification and verification system from SRI). Finally, the extracted specification is shown to refine an original formal specification using the semi-automated PVS proof system.

Echo's strategy of splitting the formal verification process down the middle and attacking it from both sides dramatically reduces the effort needed to complete a formal verification, enabling Dr. Knight and his students to complete verification of systems as large as 10,000 lines of Ada code.

One project that has benefited from Ada and Echo verification is the University of Virginia's LifeFlow artificial heart pump. Designed for the long-term (10–20 year) treatment of heart failure, this pump has a continuous-flow, axial design. The use of magnetic bearings and computational fluid dynamics simulations permit a streamlined path for blood flow. Compared with earlier pumps that used mechanical bearings, this flow path reduces the damage done to blood cells, thus reducing the potential for the formation of dangerous blood clots.

Control of the magnetic bearings is provided by a Freescale MPC5554 microcontroller executing control software written in SPARK Ada by Patrick Graydon and compiled using AdaCore's GNAT Pro High-Integrity Edition compiler. The control software runs natively on the microcontroller with no operating system, limiting the software base that must be verified for this safety-critical application. Comprehensive Echo formal verification complements functional testing to Modified Condition / Decision Coverage (MC/DC), providing high confidence that the magnetic bearing controller is as free of defects as can practically be achieved.

For further information about the Echo approach and the LifeFlow project, please see **dependability.cs.virginia.edu/info/Echo** and **dirac.mae.virginia.edu./lifeflow/**.

Interview with José Ruiz Senior Software Engineer, AdaCore EU

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

I discovered Ada as a student at the Technical University of Madrid, thanks to Professors Juan Antonio de la Puente and Alejandro Alonso. My first major Ada project involved porting the GNAT Ada run-time system to bareboard PCs, and I was fascinated by the embedded world where you control everything that is executing on your system. Then, during my Ph.D. work, I helped implement a run-time library supporting the Ravenscar profile for space processors. That project tightened my relationship with AdaCore and subsequently led to an offer to join their Paris office. This was an excellent career opportunity, and my wife liked the prospect of living in Paris, so saying "yes" was an easy decision.

Here at AdaCore I'm working on applied research for safety-critical embedded real-time systems. Projects include adapting Ravenscar towards new functionalities and targets, and exploring qualification and certification solutions for high-integrity software. I also work on GNAT technology development, and I've recently been implementing some enhancements to GNATstack.

AdaCore has been providing software development solutions for high-integrity systems for many years. How do you see the marketplace evolving, and what is AdaCore doing to meet the new demands?

I see an encouraging increase in the number of new projects focusing on safety aspects. Systems are growing in size and complexity—not only in our traditional markets like aerospace but also in others such as automotive. With the safety and economic implications of failures in these systems, I expect high-integrity methodologies to be much more widely embraced in the near future.

AdaCore has been deeply involved in the safety-critical community for many years, through compiler and tool support and also through partnerships with other solution providers. One of our goals is to make it more efficient to achieve and demonstrate safety, security and reliability properties, and that's the idea behind the Open-DO initiative: to increase the agility and the level of automation in producing and certifying safety-critical software.

AdaCore is also partnered with Altran Praxis for SPARK Pro, and with SofCheck for CodePeer. These tools are especially useful for safety-critical and high-security applications, and they nicely complement our GNAT Pro products. They are tightly integrated with GNAT Pro, which simplifies software development.

When I started working with Ada, one of its strongest attractions was the wide range of programming errors that were detected by the compiler. SPARK Pro and CodePeer go much further, preventing defects through construction and inspection respectively.

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

I enjoy reading and traveling, and thanks to AdaCore I travel quite a bit. I also like practicing different sports (cycling, jogging, swimming, gym). After a day spent sitting in front of my computer, some physical activity is relaxing. I recently started experimenting with modeling technologies to develop control systems for robots. I use the LEGO MINDSTORMS, and it is really fun! My young daughter also appreciates my new hobby, but she is remarkably demanding in terms of functional requirements.

AdaCore Awarded Grant for Hi-Lite Project

Combines Testing, Static Analysis, and Formal Proofs

In March 2010 AdaCore was awarded a grant by French national and local government agencies to develop an innovative set of tools integrated with its GNAT Pro platform. AdaCore is leading a consortium of two research institutes (CEA-List and the ProVal team of INRIA) and four industrial companies (AdaCore, Altran, Astrium and Thales Communications) in this effort. The project, named Hi-Lite, is starting in mid-2010 and will continue for three years.

Hi-Lite's aim is to promote the use of formal methods in developing high-integrity software. It loosely integrates formal proofs with testing and static analysis, thus allowing developers to combine different techniques around a common expression of properties and constraints. Hi-Lite's focus on modularity allows a divide-and-conquer approach to large software systems and encourages early adoption by all programmers. By relying only on sound static analyses, Hi-Lite can assist industrial users who wish to apply the Formal Methods Supplement of the upcoming DO-178C avionics safety standard.

Hi-Lite is completely based on Free Software. The project is structured as two different toolchains for Ada and C based on GNAT/GCC compilers (Ada and C), the CodePeer static analyzer (Ada), the SPARK verification toolset (Ada) and the Frama-C platform (C). The integration of these toolchains inside AdaCore IDEs will offer to the user a consistent way of dealing with Ada and C programs. In particular, mixed Ada/C programs can be verified against a common expression of properties and constraints.

José Ruiz photo by Gary Matoso

< technology corner >

Ada 2012 Nearing Completion

Next Version of Language Standard Offers Numerous Enhancements

As part of the natural evolution of the language design, a new version of the Ada standard is nearing completion. Referred to as Ada 2012, this is an upwards compatible increment to Ada 2005. A number of new features are currently under consideration, including:

- Improved support for specifying assertions (membership predicates for subtypes, pre- and postconditions for subprograms, invariants for packages and types, global in-out annotations);
- Improved support for real-time and concurrent programming (multiprocessor Ravenscar, barriers, task/processor affinities, task-safe queues);
- Bounded forms of the container packages appropriate in applications that cannot use dynamic storage allocation or controlled types;
- Improved support for iterating over the elements of a container or array;
- More flexible forms of expressions (if-expressions, case-expressions, quantified expressions, more general membership tests);
- Improved support for controlling visibility of names (use all type, integrated packages);
- Region-based memory management via subpools of storage pools;
- "in out" and "out" mode parameters for functions;
- New uses for incomplete types (to introduce a private type, as a parameter or result type, as a generic formal parameter);

For details, please see **www.ada-auth.org/ai05-summary.html**.

As their design firms up, many of these features are being prototyped in the GNAT technology (for example if- and case-expressions), allowing customers to gain early experience. With this phased-in approach, comprehensive support for Ada 2012 is expected soon after the final language definition is approved.

newsflash

Italian Distribution Agreement with MICROTASK

AdaCore has signed a distribution agreement with Milan-based MICROTASK Embedded, who will provide pre-sales support and also resell AdaCore's GNAT Pro Ada development environment throughout Italy. The new partnership arrangement will help reinforce AdaCore's presence in Italy, especially in the avionics sector.

Ada 2005 Support in Papyrus

AdaCore contributed to the Papyrus UML and SysML modeling environment (papyrusuml.org) with a code generator for UML2 models. Exploiting some of the features added in Ada 2005, the code generator handles class, state machine, and sequence diagrams. It also includes a dedicated UML profile to support concurrency features conforming to the Ravenscar profile. The code generator was developed within the LAMBDA research project (founded within the French System@tic cluster) and is available on the Papyrus update site.

Open-DO Update

Launched in early 2009, the Open-DO initiative promotes using open source software and lean / agile methodology in developing and certifying high-integrity systems. This year's Open-DO conference took place in Paris on March 11 and focused on how to combine formal methods with agile development. More than 60 people attended the event. Keynote speakers included Neil White (iFACTS project manager, Altran Praxis), Hervé Delseny (Airbus), Peter Gardner (Silver Atena) and Paul Boca (Hornbill Systems). Videos of the conference are available at www.open-do.org/conference-2010. The Open-DO community web site now has more than 100 registered members, who can comment on posted articles through a blog-like interface. Several new projects have also joined the Open-DO forge, including Couverture and the Qualifying Machine. More information on the Open-DO initiative can be found on www.open-do.org, and the Open-DO forge can be accessed on www.forge.open-do.org.

Conferences / Events ■ March – October 2010

Open-DO Conference
March 11 / Paris, France
AdaCore is the organizer of the Open-DO conference "Combining Formality with Agility for Critical Software Development".
www.open-do.org/conference-2010/

ESC Silicon Valley 2010
April 27–28 / San Jose CA, US
AdaCore is exhibiting at this event.
esc-sv09.techinsightsevents.com/

Systems & Software Technology Conference (SSTC) 2010
April 26–29 / Salt Lake City UT, US
Ben Brosgol is presenting a talk on DO-178C.
www.sstc-online.org/

ERTS 2010
May 19–21 / Toulouse, France
AdaCore is a sponsor at this event. AdaCore authors or co-authors are Matteo Bordin, Cyrille Comar, Franco Gasperoni, Tristan Gingold, Jérôme Guitton, Olivier Hainque, Yannick Moy, and Thomas Quinot. **www.erts2010.org/**

DASIA 2010
June 1–4 / Budapest, Hungary
AdaCore is exhibiting at this event, and José Ruiz is presenting a paper on safety and embedded multi-processors with Ada.
pagesperso-orange.fr/eurospace/DASIA%202010%20First%20Announcement.pdf

Ada-Europe 2010
June 14–18 / Valencia, Spain
AdaCore is a major sponsor of this event. AdaCore authors and tutorial presenters are Ben Brosgol, Jérôme Lambourg, José Ruiz, and Ed Schonberg.
www.ada-europe.org/conference2010.html

ESC Boston 2010
September 20–23 / Boston MA, US
AdaCore is exhibiting at this event.
esc-boston.techinsightsevents.com/

SIGAda 2010
October 24–28 / Fairfax VA, US
AdaCore is a Platinum sponsor of this event.
www.sigada.org/conf/sigada2010/

AdaCore at Wind River Regional Conferences

AdaCore is participating at all the Wind River Aerospace and Defense Technical Forums in the US this year: April 20 (Manhattan Beach, CA), April 22 (Phoenix, AZ), April 27 (Orlando, FL), April 29 (Huntsville, AL), May 18 (Hanover, MD), May 20 (Reston, VA), May 26 (Grapevine, TX), June 8 (Sunnyvale, CA), and October 20 (Burlington, MA). For further information see www.windriver.com/announces/ad-tech-forum-2010/.

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
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