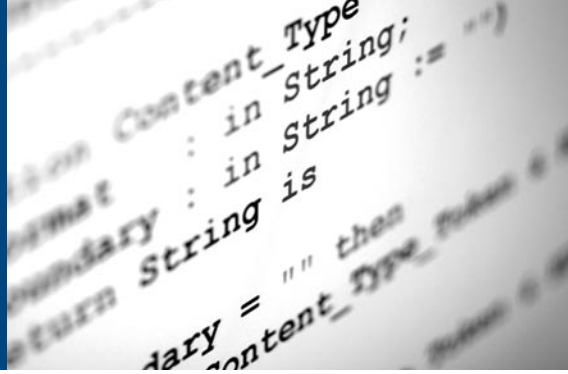
GNAT Pro insider

an AdaCore Publication
Spring/Summer 2012
www.adacore.com



newsflash

Modeling language research projects initiated

AdaCore is participating in "Project P" and "Hi-MoCo" (High-Integrity Model Compiler), two open-source research efforts supported and partly funded by the French and Estonian national governments and the European EUREKA agency. The combined projects, which started in October 2011, aim to provide an open-source, adaptable and qualifiable code generation framework for domain-specific modeling languages. The key idea is to allow control engineers (using Simulink, Stateflow and Scicos/XCos), system engineers (using SysML/MARTE and AADL), and software engineers (using UML) to easily collaborate for system-level model integration, verification, and final optimized code generation targeting the Ada 2012, C, C++ and VHDL languages.

High-Integrity Edition products renamed

The GNAT Pro High-Integrity Edition family has been partitioned into two product lines, *GNAT Pro Safety-Critical* and *GNAT Pro High-Security*. GNAT Pro Safety-Critical replaces the previous GNAT Pro High-Integrity Edition for DO-178B and GNAT Pro High-Integrity Edition for Servers, and is oriented towards industries including avionics, ATM/ATC, rail transport, and space. GNAT Pro High-Security replaces the previous GNAT Pro High-Integrity Edition for MILS and is aimed at developers of highly secure systems. It can be used in conjunction with the SPARK Pro toolset to reach the highest Evaluation Assurance Levels (EAL).

contents

AdaCore and SofCheck Join Forces 1
Ada 2012 Reference Manual Submitted to ISO 1
Who's New at AdaCore 1
Current Releases 2
In the Pipeline 2
New Course on DO-178C 2
Academia Corner: Kansas State University, US 2
Interview with Nicolas Setton 3
Open-DO Update 3
Webinar Schedule 3
Technology Corner: ParaSail 4
GNAT Pro User Day 4
Conferences/Events 4

AdaCore and SofCheck Join Forces

Ada expert Tucker Taft named AdaCore's Director of Language Research

AdaCore has merged with SofCheck, Inc., a Lexington, Massachusetts-based automated software quality (ASQ) company that has specialized in static analysis technology and Ada language expertise. SofCheck engineers Sheri Bernstein, Mike Cleaves, Mireille Gart, and Mahua Roy have joined the AdaCore technical team, and SofCheck Founder and Chairman Tucker Taft has been named as AdaCore's Director of Language Research. In this new role Mr. Taft will be in charge of efforts to advance the state of the art in language design and implementation for high-reliability, safety-critical, and high-security systems.

With this merger AdaCore has acquired SofCheck's products, including static error detection tools. AdaCore has also acquired ParaSail, a new Parallel Specification and Implementation Language designed by Mr. Taft and intended for high-reliability applications on multicore target platforms (see Page 4 for more information about ParaSail).

AdaCore and SofCheck personnel share a long and direct involvement in the design of the Ada programming language, and the two companies have specialized in software development tools that nicely complement each other. SofCheck's advanced static analysis technology fits in smoothly with AdaCore's GNAT Pro development environment, and prior to the merger the two companies jointly developed AdaCore's CodePeer product, an efficient and accurate code reviewer that incorporates the SofCheck static analysis engine. The merger will facilitate further enhancements to CodePeer, provide personnel and technology resources for new product offerings, and also simplify the support arrangements for CodePeer customers.

Ada 2012 Reference Manual Submitted to ISO

The design process for Ada 2012 is complete. The Ada Rapporteur Group (ARG) has submitted the reference manual for this latest version of the language to WG9, the ISO working group in charge of Ada. After the document has been approved by the WG9 national delegations, the International Organization for Standardization (ISO) is expected to approve the new standard before the end of 2012. The new Ada 2012 reference manual is available at **www.ada-auth.org/standards/ada12.html/**.

All the major new Ada 2012 features are implemented in GNAT Pro 7.0, enabled by the compiler's -gnat2012 switch. Total coverage of Ada 2012 is planned for GNAT Pro 7.1.

As with previous versions, acclaimed author John Barnes is preparing a Rationale for the language. The first installments of the Rationale can be downloaded from **www.adacore.com/home/ada_answers/ada-2012/**.

Who's New at AdaCore

AdaCore's European and North American offices have been growing. In the Paris office the new staff include recent graduates David Assamoi, who has a Masters degree from Université Paris Descartes, and Fabien Chouteau and Jean-Charles Delay, each with a Masters degree from École Pour l'Informatique et les Techniques Avancées (EPITA). They will be working on a variety of projects including the Qualifying Machine, GNATemulator, and AdaCore infrastructure development.

In the US, in addition to the SofCheck personnel who joined AdaCore as part of the merger (see above), Dudrey Smith has joined AdaCore's team of external consultants. Based in Grand Rapids, Michigan, Dr. Smith is a recognized expert in embedded avionics software development (including DO-178B certification) and a long-time member of the Ada community. He has had a distinguished career at Smiths Aerospace and GE Aviation Systems and is consulting for AdaCore on a number of certification-related projects. Dr. Smith has a Ph.D. from the University of Michigan.

Also in the US, Vincent Pucci came on board for a one-year internship starting in September 2011. Vincent is a student at Télécom Bretagne (Brest, France) where he is majoring in Telecommunications and Computer Science. At AdaCore's New York office he has been working on adding dimensionality checking to the GNAT compiler and also on a lock-free implementation of protected objects.

< current releases >

GNAT Pro 7.0

This major new release supports the upcoming Ada 2012 language revision, introduces a flexible and powerful testing tool (GNATtest), incorporates a range of improvements (many based on user suggestions), and adds several new platforms. Some of the key enhancements:

Compiler. In addition to its Ada 2012 support, the GNAT Pro compiler exhibits more efficient memory usage in its handling of controlled types, provides new warnings and improved error messages, and performs optimizations for array processing (using vectorization instructions when available) and composite return values.

Tools. The new GNATtest tool, based on AUnit, can be used to create and maintain a complete unit testing infrastructure for complex projects. Other tool enhancements include new options and pretty-printing improvements in GNATpp, and the availability of coupling metrics in GNATmetric.

CodePeer 2.1

CodePeer 2.1, the latest version of AdaCore's advanced static analysis / abstract interpretation tool, introduces a number of significant enhancements, including:

- Complete support for all new features of the Ada 2012 language revision,
- Improved analysis of race conditions,
- Detection of access to global uninitialized variables,
- More precise preconditions, which help produce more accurate messages and fewer "false alarms",
- Improved handling of unused assignments,
- New warning on infinite loops, and
- The new functionalities in GNATpp and GNATmetric mentioned above, since these are incorporated in CodePeer.

GDB in GNAT Pro 7.0

GDB's scripting capabilities have been significantly enhanced by the integration of a Python interface. Python has been used successfully in other AdaCore tools (such as GPS) as a powerful and flexible extensibility and customization mechanism. For an overview of how to use this facility, please refer to Ada Gems #121 and #122 at **www.adacore.com/adaanswers/gems/**.

< in the pipeline >

GNAT Pro for Wind River Linux

GNAT Pro will be available during Q3 2012 on x86 Linux host platforms for Wind River embedded Linux, versions 4.2 and 4.3, for PowerPC and PowerQUICC III (e500v2 family) processors. This will be a full version of GNAT Pro with support for GPS and a full GNATbench integration with Wind River WorkBench.

GNATcoverage and GNATemulator

GNATcoverage, a non-intrusive source and object coverage tool, and GNATemulator, a machine emulator and virtualizer based on QEMU technology, recently added support for several new platforms: PowerPC ELF, Leon ELF, and P55xx/e500v2 ELF for GNATcoverage, and VxWorks 6 for GNATemulator. During Q3 2012 the planned enhancements include improvement of the GPS plugins for both products, and GNATcoverage support (except for MC/DC) of VxWorks 6 with the full run-time library.

GtkAda

GtkAda 3, coming out later this year, will support version 3 of the Gtk+ library. This will bring a number of enhancements including a simplified API, several new widgets, complete new features such as CSS-based theming, and an experimental HTML5 backend. GtkAda 3 will also include all the new features introduced in recent versions, such as support for low-level drawing with the Cairo graphics library, printing support, and the GLADE GUI builder.

New Course on DO-178C

Following its participation in the group that developed the new DO-178C avionics software certification standard, AdaCore is now offering a three-day course for engineers and project managers. The course covers the key concepts behind DO-178C including a summary of the differences with DO-178B, shows how to apply the guidance in the Object-Oriented Technologies and Related Techniques supplement (DO-332), and explains how to best use the Ada language and GNAT Pro tool suite to comply with the certification objectives. For further information, please contact **info@adacore.com**.

< academia corner >

SPARK in Formal Verification Research
Kansas State University, Manhattan, Kansas (US)

Prof. John Hatcliff and his team at Kansas State University's Static Analysis and Transformation of Software (SAnToS) Laboratory have found the SPARK language technology to be an ideal research vehicle for exploring novel techniques in formal program verification. The SAnToS team has worked for over a decade on innovative tools that incorporate model checking, symbolic execution, dataflow, and program dependence analyses. "We started out using Java", said Prof. Hatcliff. "But Java is a large language with complex semantics, and it certainly wasn't designed for, or often used in, safety-critical systems. It was hard for us to produce clean technical results and robust tools with Java, and to apply those tools to interesting safety-critical examples. SPARK has proved to be a much more appropriate base language."

Inspired by challenges they observed while collaborating with Rockwell Collins engineers on certified embedded information assurance applications, and with US Food and Drug Administration engineers on next generation medical devices, SAnToS researchers are working on several innovative enhancements to SPARK's annotations for software contracts:

- ***Precise information flow specification and checking***. Embedded information assurance components such as crypto-graphical controllers and cross domain solutions often have information flow policies that are conditional (i.e., data can flow from one domain to another only under certain conditions). This requires specifying how information flows through individual cells or ranges of elements in complex data structures built using arrays and records. SAnToS researchers are extending SPARK's *derives* annotations to support declaration of conditional flows and precise descriptions of flows through arrays.
- ***Highly automated checking of complex pre/postconditions***. Checking complex pre/postconditions in SPARK can require significant manual interactions with SPARK's Proof Checker. SAnToS researchers have developed an alternate tool chain based on symbolic execution that can perform bounded checking of such contracts in a completely automated fashion, and can automatically generate unit test cases representing the paths explored in the analysis.

SAnToS researchers are currently working with AdaCore and Altran Praxis to include some of these functionalities in the upcoming SPARK 2012 framework. For more information, please visit the **santoslab.org** website.

Interview with Nicolas Setton

Product Manager, GPS and GtkAda, AdaCore EU

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

My initial encounter with Ada was as an undergraduate at Télécom ParisTech (ENST). I can remember the shock when the compiler rejected my program because it refused to perform an implicit conversion between pointer (I mean access) types. At first I felt quite outraged ("What? The C compiler never complained like this!"). After some effort, I understood that I was in fact dealing with a very powerful tool—and the fun began! Later, my Computer Science professor told me about an internship opportunity at AdaCore, and I joined the company's Paris office right after graduating.

I've worked on a variety of projects, mainly on the GPS IDE, and on our infrastructure for quality management and tool qualification. I also took charge of some entertaining systems administration projects, like setting up the virtualization cluster. I am currently Product Manager for the GtkAda graphical toolkit and GPS, which entails what you would expect: coordinating with the technical team, developing product roadmaps, etc.

Based on your experience with graphical software and workstation technology, what do you see as future trends for GUIs?

Many GUI decisions are simply good adaptations to hardware changes, so, by looking at the hardware of today and the directions it is taking, we can make some predictions about the GUIs of tomorrow.

As an example, the geometry of our workstation screens has evolved to an ever-increasing width: at present, 1366x768 has topped 1024x768 as the most widely used resolution. Earlier this year, I noticed that the layout of my email program changed from an up-down division to a side-by-side approach. This is not a coincidence; the GUI has been cleverly reorganized to match the evolution of the hardware. I expect to see more desktop interfaces adapting to this wider form factor, for example by removing controls from the top or bottom and putting them on the sides.

The pixel pitch of our displays will reach a maximum: some devices can already match the capabilities of the human retina, and we will never need to exceed this capacity. GUI engineers will have to find new areas for innovation.

With regard to input devices, things are even more interesting! After 20-odd years of very few improvements (the mouse wheel being the only one that comes to mind that had an influence on GUI design), a breakthrough has occurred with the advent of multi-touch surfaces and displays. I think this is a very promising breeding ground for new paradigms! One example is model-driven engineering: I would love to manipulate UML diagrams directly on a tablet, while I edit code on my current workstation. In general, the ability to "touch" our data is I think a game-changer, and I look forward to seeing this integrated with the code-quality dashboards and other reporting tools that are emerging.

The industry of today is more demanding of aesthetically pleasing interfaces than it was 20 years ago, involving graphical designers and sometimes ergonomists. The toolkits help, by separating the GUI design from the actual coding. The latest generation of toolkits allows users without programming skills to create GUI layouts, and separates theming and customizing activities from the GUI development through CSS-like approaches.

At some point I would love to see on-eye displays operated by micro-gestures or eye movements, but this might just be my love for science fiction.

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

Aside from programming or assembling computers? I was recently both invigorated and traumatized by a brush with amateur theatre. I now have a very deep respect for people who are able to put themselves on stage and perform. I'm sure I'll have another go in the future!

Open-DO Update

The Open-DO initiative, which seeks to bring the benefits of open source and agile technology to the safety certification community, continues to grow. The ERTS 2012 conference in Toulouse this past February featured an Open-DO session with presentations on topics such as the integration of formal methods with testing; all papers from this session are available at **www.erts2012.org/Default.aspx?Id=1050&Idd=1129#7A/**.

Several new projects have joined the Open-DO initiative including Riposte, the Nose Gear Challenge Problem, and explanatory documents on DO-178C. They can be found at **forge.open-do.org/**.

An Open-DO day will be organized in early 2013 where these projects, and others, will be presented. Details will be posted on the Open-DO web site **www.open-do.org** later this year.

Webinar Schedule

AdaCore's 2012 Insight Webinar series has covered SPARK Pro 10.1, the new GNATtest Unit Test Harness Generator tool, and CodePeer 2.1.

To view any of these, or to learn about future webinars, please visit **www.adacore.com/knowledge/webinars/**.

Nicolas Setton photo by Gary Matoso

ParaSail: Less Is More when Parallel Programming for Multicore

As part of the merger between SofCheck and AdaCore, the programming language ParaSail will now be under AdaCore auspices. ParaSail (Parallel Specification and Implemention Language) was specifically designed to make parallel programming pleasant and productive, in contrast with the experience one gets from most existing programming languages.

ParaSail achieves its goal by removing impediments that stand in the way of using multicore chips, and by adding an inherently safe, pervasively parallel programming model. The impediments that were eliminated include constructs that complicate software analysis and verification (pointers, global variables, global garbage-collected heap, run-time exception handling, hidden aliasing), features that are error-prone in practice (explicit lock/unlock, explicit wait/signal, explicit threads) and features that frustrate learning (special syntax reserved for predefined types).

Despite the significant simplification, ParaSail still provides a familiar class-and-interface-based object-oriented programming model. Programmers coming from languages such as Ada, Java, C#, or C++ will be able to immediately read, and to quickly learn how to write, ParaSail programs.

Here is a simple recursive ParaSail function that counts the number of words in a string `S`, using `Separators` as the set of characters that separate one word from another.

A key point is that although this function does not appear to be explicitly parallel, the basic ParaSail semantics imply that the two recursive calls of `Word_Count` in the initialization of `Sum` are in fact evaluated in parallel. Those recursive calls then continue the "divide-and-conquer" approach to counting the words in the string. Thus *N* picothreads are spawned for a string of length *N*, with their results added together in a computation tree of depth *log2(N)*. A potential speedup of *N/log2(N)* relative to a sequential algorithm is achieved.

For more information about ParaSail, please visit the web sites **parasail-programming-language.blogspot.com/** or **www.adacore.com/labs/**.

```
func Word_Count
  (S : Univ_String;
   Separators : Countable_Set<Univ_Character> := [' '])
  -> Univ_Integer is
    // Return count of words separated by given set of separators
    case Length(S) of
      [0] => return 0; // Empty string
      [1] =>
        if S[1] in Separators then
            return 0;  // A single separator
        else
            return 1;  // A single non-separator
        end if;
      [..] =>          // Multi-character string; divide and conquer
        const Half_Len := Length(S)/2;
        const Sum := Word_Count(S[1 .. Half_Len], Separators) +
          Word_Count(S[Half_Len <.. Length(S)], Separators);

        if S[Half_Len] in Separators
          or else S[Half_Len+1] in Separators then
            return Sum;    // At least one separator at border
        else
            return Sum-1;  // Combine words at border
        end if;
    end case;
end func Word_Count;
```

GNAT Pro User Day

The next annual GNAT Pro User Day will be held on September 25 in Paris. Topics to be presented include an Ada 2012 overview, news on the latest tools and toolset features, product roadmaps, and practical tips from technology experts. Many AdaCore staff will be on hand to answer questions. For further information, please contact events@adacore.com or visit adacore.com/gnatpro-day/.

Conferences / Events ■ April – December 2012

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

System and Software Technology Conference (SSTC 2012)
April 23–26 / Salt Lake City UT, US

AdaCore is a sponsor/exhibitor at this conference, and Ben Brosgol is delivering a presentation "Object-Oriented Programming for High-Integrity Systems: Pitfalls and How to Avoid Them".
sstc-online.org/

SAE 2012 World Congress
April 24–26 / Detroit MI, US

Stuart Matthews (from AdaCore's partner Altran Praxis) and Greg Gicca are presenting a paper, "Building Security In: The SPARK Approach to Software Development" addressing some issues in automotive software security.
www.sae.org/congress/

DESSERT'12
Dependable Systems, Services & Technologies
May 25–28 / Sevastopol, Ukraine

Vadim Godunko is a co-author of the paper "Dynamic Generation of HTML Pages for Ada Web-Server" at the Workshop on Ada Technology and Language Diversity. This workshop discusses Ada technologies as one of the basic approaches to developing critical software and embedded systems.
www.stc-dessert.com/conf2012/

Ada-Europe 2012
June 11–15 / Stockholm, Sweden

AdaCore is a sponsor/exhibitor at this conference, and AdaCore staff are participating in the technical program. Ben Brosgol is presenting a tutorial on DO-178C; Tucker Taft is presenting a tutorial on ParaSail; Cyrille Comar, José Ruiz and Yannick Moy are delivering a paper "Source Code as the Key Artifact in Requirement-Based Development: the Case of Ada 2012"; and Franco Gasperoni is a panelist in a session on language technology.
www.cister.isep.ipp.pt/ae2012/

Embedded Masterclass 2012
June 27 / Cambridge, UK

AdaCore is a sponsor/exhibitor at this event and Quentin Ochem is presenting a paper "Higher abstraction in low-level development: the Ada 2012 answer".
www.embedded-masterclass.com/index.html

Embedded Konferenz 2012
July 3 / Stuttgart, Germany

AdaCore is a sponsor/exhibitor at this conference.
www.embedded-konferenz.de/ (in German)

ESC / Design East
September 17–20 / Boston MA, US

AdaCore is exhibiting at this event.
esc.eetimes.com/boston/

SAE Aerospace Electronics and Avionics Systems Conference
October 30–November 1 / Phoenix AZ, US

Greg Gicca is presenting a paper "Meeting Top Safety and Security Requirements while Reducing Cost, Size, Weight, and Energy: Achieving High Assurance through a Verifiable Language on a MILS Architecture".
www.sae.org/events/aeas/

High-Integrity Language Technology (HILT 2012, sponsored by ACM SIGAda)
December 2–6 / Boston MA, US

AdaCore is a Platinum Sponsor and is exhibiting at this conference. Ben Brosgol is Conference Chair.
www.sigada.org/conf/hilt2012/

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

© Copyright 2012 AdaCore. All rights reserved.
All trademarks are owned by their respective companies.