Inside AdaCore

January–June 2020

Webinar on NVIDIA Use of SPARK for Secure Firmware | AdaCore UK Participating in HICLASS Program | Tech Days 2019 | V20 Product Release | AdaCore in Space | AdaCore Toolsuite for Ada, SPARK, and C Qualified under ISO 26262 and IEC 61508 | GNAT Ada Targeted to LLVM | Spotlighting a GAP Member: Universidad Politécnica de Madrid (Spain) | Enhancements to learn.adacore.com | Blog Summary: RecordFlux- A Secure SPARK-Based Message Parsing Framework | GNAT Pro C++ Available for Embedded Applications

Cybersecurity requires a multifaceted defense.

For software developers the programming language technology plays a critical role, and Ada and SPARK stand out with a proven track record of preventing vulnerabilities or detecting them early.

This issue of *Inside AdaCore* highlights some of the recent cybersecurity-related news from AdaCore, including a webinar on NVIDIA's selection of SPARK for some of their firmware products, and an announcement of AdaCore's participation in the UK's HICLASS program. Another security-related piece is a summary of a blog on RecordFlux, a secure SPARK-based message-parsing framework from Componolit.

Webinar on NVIDIA Use of SPARK for Secure Firmware

A webinar *Securing the Future of Safety and Security of Embedded Software*, delivered by Daniel Rohrer and Dhawal Kumar from NVIDIA on November 21, 2019, explained how NVIDIA hardware combined with Ada and SPARK deliver robustness, security, safety, and improved efficiency in the development pipeline.

In the first part of the webinar ("Adoption Journey"), Mr. Rohrer described the technical and business rationale for adopting a new and formal methods-based language and development model for NVIDIA's firmware, and identified why NVIDIA selected SPARK/Ada and AdaCore. Key factors included specific language features (e.g., SPARK/Ada's strong typing, C interoperability, and contract-based programming) and its credible ecosystem, along with AdaCore's highly responsive support and ability to engage with NVIDIA engineers at a deep technical level.

In the second part ("Securing the Future of Safety and Security of Embedded Software"), Mr. Kumar explained the nature of firmware and its environment, gave an overview of SPARK, discussed alternative language technologies (including Frama-C and Rust) that were considered and rejected, described the Proof of Concept (PoC) project that was undertaken for SPARK, detailed the key SPARK benefits (e.g., less effort in debugging, "if it proves, it works"), and summarized the NVIDIA experience. As a result of the successful PoC, SPARK is now used for some of NVIDIA's security- and safety-critical firmware applications.

To view the webinar, please visit **www.adacore.com/nvidia-webinar/**.

AdaCore UK Participating in HICLASS Program

AdaCore is leading a technical effort researching and developing SPARK-related capabilities for the High-Integrity, Complex, Large, Software and Electronic Systems (HICLASS) project in the UK. This four-year collaborative work package includes a cybersecurity-focused evolution of the SPARK language and verification tools, while enhancing the company's existing cybersecurity-related technologies based on the needs and feedback of industrial partners. During the course of the project AdaCore will also be expanding its existing fuzzing capability, researching and implementing compile-time cyberattack countermeasures, and leading / participating in industrial case studies for cybersecure aerospace systems. AdaCore's QGen model-based engineering toolsuite, which is a key player in the future of safe and secure aerospace development platforms, is also featured in HICLASS; extensive work will be undertaken to raise the Technical Readiness Level of a prototype SPARK verification round trip capability.

As a research and development program, HICLASS is an excellent fit with AdaCore's core values and its existing and future capabilities. In addition, a new UK entity, AdaCore Ltd, has been created to rapidly grow into the company's UK Centre of Excellence, ensuring that current and future UK aerospace customers will continue to receive the high level of technical expertise and quality products associated with AdaCore.

For more information, please see Paul Butcher's blog at **blog.adacore.com/adacore-for-hiclass/**.

Tech Days 2019

AdaCore conducted its annual Tech Days conferences in Paris on October 3, and in Boston on November 12–13, with insightful presentations from the company's technical staff and guest speakers. Attendees learned about AdaCore's product updates and roadmaps, market trends for high-assurance software, a new GNATcoverage technology/tool, fuzzing and other cybersecurity techniques, certification-related products and services, education and community resources for Ada and SPARK, AdaCore's approach to SSI (System-to-Software Integrity), R&D projects using SPARK and Ada, embedded C and C++ support, and Ada language tips. Live demos offered practical guidance on how to best use products such as CodePeer, GNATtest, and GNATcoverage.

Tech Days Paris featured user presentations from Alexander Senier (Componolit) on "Closing the Gap: From Protocol Specification to Proven SPARK Code" and Stephane Carrez (Twinlife) on "Ada for Web Development". Tech Days Boston was highlighted by a customer presentation from Dhawal Kumar (NVIDIA) on "SPARK Ada for Safe and Secure Firmware Development - The NVIDIA Story" and a keynote talk from Raymond Richards (DARPA/IPO) on "The Role of Design Languages and Tools in Building Secure Systems".

Videos from the conferences are available at **tinyurl.com/techdays2019videos/**.

For information on AdaCore's plans for Tech Days 2020, please visit **www.adacore.com/techdays/**.

V20 Product Release

AdaCore issues an annual major release of its products during the 1st quarter of the year, with many enhancements based on customer suggestions. Several specific improvements in the v20 release are highlighted below; full lists with details may be found on the products' "New Features" pages:

- GNAT Pro technology: **docs.adacore.com/R/relnotes/features-20**
- GNAT Studio and GNATbench IDEs: **docs.adacore.com/R/relnotes/features-ide-20**
- GPR library and tools: **docs.adacore.com/R/relnotes/features-gprbuild-20**
- CodePeer: **docs.adacore.com/R/relnotes/features-codepeer-20**
- SPARK Pro: **docs.adacore.com/R/relnotes/features-spark-20**
- QGen: **docs.adacore.com/R/relnotes/features-qgen-20**

GNAT Pro 20.1 Development Environments

- Support for all VxWorks 7 SR0620 platforms
- Upgrade to GCC 7 and GDB 8.3
- GNAT Pro C++ available on ARM Linux, PowerPC Linux, VxWorks 6 PowerPC (support for C++ on VxWorks 7 SR06x0 series will be available in GNAT Pro 21)
- New elaboration algorithm taking the complete call graph into account
- Improved performance of generated code and faster compilation time
- New warnings and improved diagnostics
- GNATstub, GNATmetric, and GNATpp transitioned to libadalang, providing support for partial sources (among other enhancements)
- GNATcoverage: preliminary support for source instrumentation (see separate newsflash in this issue)

IDEs

- Rebranding of GPS as GNAT Studio, with major upgrade of language engine to Microsoft Language Server Protocol (with both an LSP client and an Ada Language Server)
- Support for latest versions of Eclipse in GNATbench
- Support for technical debt/remediation effort computation in GNATdashboard

CodePeer 20.1 Advanced Static Analyzer for Ada

- Improvements in GNAT Studio integration and web engine
- Improved Jenkins integration
- Reduced false positives

SPARK 20.1 Formal Verification Toolsuite

- Support for pointers through ownership
- Support for using volatile variables to prevent compiler optimizations
- Contracts added to Ada standard library
- Improved floating-point support in Alt-Ergo prover

QGen 20.1 Qualifiable Model-Based Engineering Toolsuite

- Integrated Ada and C S-Function generation and debugging during simulation
- New option to remove non-covered code caused by specific modeling patterns
- New option to help create a block configuration to customize code generation
- Support for Simulink String, Data Dictionary, Unit Conversion, Stateflow State Transition Table

AdaCore in Space

Ada and AdaCore have a long and successful track record in the Space domain, and 2019 saw a continuation of that tradition.

The aerospace company AVIO selected the GNAT Pro Assurance Ada Development Environment, including the GNATemulator host-based target emulation tool, to implement the on-board software for AVIO's Vega-C launch vehicle. Sponsored by the European Space Agency (ESA), this safety-critical hard real-time embedded system is the flight software that handles guidance, navigation and control for the Vega-C.

AVIO is using the GNAT Pro Assurance Ada cross environment for certified / safety-critical development, hosted on Intel x86 Linux and targeted to LEON 2 ELF with the ZFP ("Zero Footprint Profile") minimal run-time support library. The host environment includes the GNATemulator target emulation tool, which translates from target to host instructions on the fly and allows efficient and convenient functional testing. The Vega-C on-board software project includes certification of the ZFP run-time library at level B of the European Space standards ECSS-E-ST-40C and ECSS-Q-ST-80C.

In another Space-related effort, ESA selected AdaCore to provide a qualified multitasking solution for spacecraft software development to support multiple ongoing and future ESA projects. As part of this contract AdaCore implemented a pre-qualified version of the Ravenscar SFP (Small Footprint) library—a configurable Ada run-time library that implements the Ravenscar profile, allows customization for specific platforms and capabilities, and is suitable for qualification in different domains, particularly those in which certification or a reduced footprint is needed. This multitasking runtime, named Ravenscar SFP QUAL, targets Ada development on LEON2 and LEON3 boards and has been pre-qualified according to the ECSS Criticality Level B for software. As part of the validation and verification activities, a comprehensive test suite is also being developed to check compliance with restricted Ada profiles.

For additional information on these projects please visit **www.adacore.com/avio-press-release/** and **www.adacore.com/esa-press-release/**.

AdaCore Toolsuite for Ada, SPARK, and C Qualified under ISO 26262 and IEC 61508

AdaCore has qualified three of its development and verification tools as compliant with ISO 26262, the functional safety standard for automotive systems, and with IEC 61508, the generic functional safety standard for electrical and electronic systems.

All three products have been certified by TÜV SÜD, an independent, globally recognized organization that confirms that products meet national and international standards. TÜV SÜD certification is widely acknowledged and respected as a trusted indicator of quality, safety, and sustainability.

The GNAT Pro environment has been qualified at Tool Confidence Level TCL-3 under ISO 26262 and at T3 under IEC 61508; the Common Code Generator (CCG), which compiles from a SPARK-like subset of Ada to C code, has been qualified at TCL-3 and T3; and the SPARK Pro formal verification toolset has been qualified at TCL-3 and T2.

By qualifying these tools, AdaCore has shown that its high-integrity technologies can meet the demanding assurance requirements of the software-intensive automotive industry. For further information, please see the press release **www.adacore.com/press/iso-26262/**.

interview

Michelle Ricardo

Account Manager

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

I first learned about AdaCore from a recruiter, who told me about an open position as an account manager. Before working at AdaCore I had managed client relationships with large matrix organizations across various industries. My clients included global law firms, pharmaceutical companies, banks, insurance companies, and even a few utility companies. Because I had worked with complex organizations in very regulated industries, I was intrigued by the prospect of serving clients from the Department of Defense and its contractors. My only real concern was that I am not an engineer, and . . . I had never compiled. But after meeting a few members of the AdaCore team, I quickly realized that this company actively seeks out individuals of varied backgrounds and talents in order to foster new ideas. A company culture that is open to new ideas is refreshing, and I like working with clients whose needs are constantly evolving. So I eagerly joined AdaCore as an account manager, as part of a team who knows that "helping people build software that matters" today is different than yesterday, and it will be different tomorrow. I enjoy the challenges that this brings and the opportunity to meet and talk to the people who depend on us for their projects' success.

As an account manager, you are AdaCore's representative to your customers, and in the other direction you also serve as your customers' advocate to AdaCore. How do these roles interact?

As AdaCore's representative, I first seek to understand the needs of our government and industry developer teams. It's important to learn what matters to the market and why. In my position I have the opportunity to hear directly from the developers, and I can often help connect their needs to an existing AdaCore product or service. However, sometimes a customer's needs are not addressed by anything currently available. Then I bring the issue to the attention of various AdaCore stakeholders, and also brainstorm with colleagues for out-of-the-box solutions. These internal conversations often result in new products or services that we later make more widely available as an official offering.

A good example is AdaCore's Mentorship service, which was initiated in 2017 as a customized solution for a customer who wanted to migrate a C application to Ada and SPARK. Their team was not very familiar with the SPARK language and toolset, and they needed training, coding assistance, and dedicated technical support. We listened to their needs and tailored a solution in response. During that process we quickly realized that other customers had similar goals and challenges and that they would also benefit from a customized service. Thus the "AdaCore Mentorship" was born.

I should mention that there are times when a request is beyond the scope of what we can realistically provide. In those cases I explain the reasons to the customer, and, when applicable, refer a partner company that might be able to help. I also make a note of the request; although we cannot solve every problem that comes our way, keeping a record allows us to observe trends and plan future enhancements

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

When I am not working, I enjoy traveling and sharing new experiences with my family and friends. My mother and I recently traveled to the French Riviera where we enjoyed the pebble beaches of Nice, the Picasso Museum in Antibes, and the famed Casino de Monte-Carlo in Monaco. Last year I traveled to Japan for the first time, for a friend's wedding, which was held in a traditional Shinto shrine. Although I do not yet have specific travel plans for 2020, I am currently researching Greece, Iceland, and a possible second trip to Japan.

GNAT Ada Targeted to LLVM

As part of the company's ongoing research in compiler technology, AdaCore has developed a GNAT Ada compiler that interfaces with the LLVM back end, thus providing a different code generator than the GCC back end found in other GNAT compilers. This research project, called "GNAT LLVM", aims to demonstrate the feasibility of generating LLVM bitcode from Ada and to open the LLVM ecosystem to Ada; it is not intended as a replacement for any existing GCC-based GNAT ports. Indeed, the two code generator technologies are compatible: code produced by current GCC-based GNAT compilers and LLVM-based C compilers can already be combined, as is evidenced on recent versions of VxWorks.

AdaCore published the GNAT LLVM sources on GitHub in September 2019, for hobbyists and researchers to experiment with and report back their comments.

This technology has a number of potential uses / benefits. For example, by providing two different modern code generators for the latest Ada standard, GNAT LLVM addresses the need for "compiler diversity" as required by some certification standards. Another potential use, planned as a follow-on research project, is to add Ada support to LLVM-based static analysis tools such as KLEE and potentially support Ada on new architectures.

Michelle Ricardo photograph by Albert Lee

Spotlighting a GAP Member

Universidad Politécnica de Madrid (Spain)

For the past several years Prof. Juan Zamorano at the Technical University of Madrid (UPM) has been directing a team of colleagues and students in the development of a UPMSat-2 microsatellite. The project originally started in 2013 as a follow-to the UPM-Sat 1, launched by an Ariane-4 in 1995.

The UPMSat-2 weighs 50kg, and its geometric envelope is a parallelepiped with a base measuring 0.5m x 0.5m and a height of 0.6m. The microsatellite is scheduled to be launched in March 2020 on a Vega launcher, and is expected to be operational for two years.

The primary goals of the project were:

- to improve the knowledge of the project participants, both professors and students;
- to demonstrate UPM's capabilities in space technology;
- to design, develop, integrate, test, launch and operate a microsatellite in orbit from within a university environment; and
- to develop a qualified space platform that can be used for general purpose missions aimed at educational, scientific and technological demonstration applications.

The project encompasses development of the software together with the platform, thermal control, attitude control, and other elements. In 2014, AdaCore's GNAT cross-development environment was selected for the UPMSat-2 microsatellite project's real-time on-board and ground control software.

While Java is the primary language used to teach programming at UPM, Ada was chosen as the main language for the project because it was judged the best for developing high-integrity systems. In total, the on-board software consists of more than 100 Ada packages, comprising over 38K lines of code. The altitude control subsystem uses C code that was generated automatically from Simulink® models (there are 10 source files in C, with a total of about 1,600 lines of code). The software also contains database and XML interfaces to support the development of the ground control software.

Enhancements to learn.adacore.com

AdaCore's interactive learn.adacore.com site, a free resource for Ada, SPARK and GNAT training, has been upgraded with new content and other improvements. This evolving platform currently hosts five self-paced and modern courses: Introduction to Ada, Introduction to SPARK, Ada for the C++ or Java Developer, SPARK Ada for the MISRA C Developer, and Introduction to GNAT Toolchain.

The courseware serves as a practical training choice both for newcomers who wish to come up to speed with these technologies, and for experienced users who would like to sharpen their skills on specific topics.

Recent enhancements include an updated Introduction to GNAT Toolchain course covering several advanced topics, including a new chapter on tools from the GNAT Community edition. Another improvement is a "Download PDF" button for each course, allowing users to study the training material offline.

Blog Summary

RecordFlux– A Secure SPARK-Based Message Parsing Framework

Componolit, a German company specializing in technologies for trustworthy software, has implemented a parser generator named RecordFlux that takes a SPARK-like specification of complex binary messages and produces a parser that can be proved to be free of run-time errors and compliant with key integrity properties. The ability to process messages securely, even when the origin might be an adversary seeking to exploit a vulnerability, is critical in thwarting attacks such as Heartbleed.

The key element of the RecordFlux technology is a domain-specific language that defines the message structure. The syntax, inspired by SPARK (and thus Ada), includes extensions that can capture complex dependencies between fields of a record. For example, the RecordFlux notation for messages is expressive enough to define the structure of a general Ethernet frame, including optional fields and other subtleties.

RecordFlux comes with the command line tool rflx, which parses specification files and subsequently generates SPARK packages that can be used to parse the messages. These packages, along with a user-supplied driver program, can then be analyzed by gnatprove to obtain several kinds of guarantees. First, the absence of run-time errors can be shown for the generated code and also for suitably written user code. No matter what input is presented to the parser, the program will not raise an exception at run time. Thus its control flow cannot be circumvented, e.g., by buffer overrun or integer overflow. This is called "silver level" in SPARK parlance. Additionally, key integrity properties ("gold level") can be proved; for example, guaranteeing that optional fields are accessed if and only if all requirements defined in the RecordFlux specification are met.

To demonstrate the practical application of the RecordFlux technology, Componolit formalized the message format of the TLS v1.3 security protocol, generated a SPARK parser, and verified the parser at the "gold" level. They then compared the performance of the SPARK parser with an unverified parser written in C++: the SPARK version was provably more secure than the C++ version while showing only a 2.7% lower throughput for the TLS handshake layer, and only a 1.1% lower throughput for the TLS record encryption/decryption layer.

For more information please see Alexander Senier's blog article at **tinyurl.com/recordflux/**.

GNAT Pro C++ Available for Embedded Applications

AdaCore has extended its GNAT Pro product line to support C++, up to and including C++17, on a number of embedded platforms. Hosted on x86 GNU Linux, GNAT Pro C++ is targeted to VxWorks 7 SR06x0 (ARM, PowerPC, and x86), Embedded Linux (ARM and PowerPC), and VxWorks 6.9.x (PowerPC 32 bits). It is available on both the GNAT Pro Enterprise and GNAT Pro Assurance product lines, and supports projects that use C++ either mixed with Ada or standalone.

GNAT Pro C++ offers advanced interfacing capabilities between Ada and C++, such as binding generation to and from both languages, mixed-language exception propagation and catching, and cross-language inheritance and dispatching. The GNAT Pro Assurance edition provides unique benefits for pure-C++ developers, including long-term support, known problem analysis, and safety-critical fixes provided by the same experts who developed the product. It also improves multiple platform portability, providing consistent technology across native and embedded environments.

For more information, please see **www.adacore.com/embedded-c-press-release/**.

calendar highlights / January–June 2020

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

ERTS 2020 (Embedded Real-Time Systems)
January 29–31, 2020 / Toulouse, France

AdaCore is a sponsor and exhibitor at this conference.
www.erts2020.org/

FOSDEM'20 (Free and Open source Software Developers' European Meeting)
February 1–2, 2020 / Brussels, Belgium

Fabien Chouteau and Pierre-Marie de Rodat are delivering presentations in the Ada room.
fosdem.org/2020/

ScaleUp 360° Automotive AI
Feb 4–5, 2020 / Online event

Rob Tice is presenting a webinar *Beyond the Boundaries of C: Writing ASIL-4 Software with Verification-Centric Language SPARK Ada and Formal Proof.*
www.scale-up-360.com/en/automotive-ai/

SSS'20 (Safety-Critical Systems Symposium)
February 11–13, 2020 / York, UK

AdaCore is the symposium sponsor and an exhibitor.
scsc.uk/e619/

Embedded World 2020
February 25–27, 2020 / Nuremberg, Germany

AdaCore is exhibiting at this conference.
www.embedded-world.de/en/

ACM SIGCSE 2020 (Computer Science Education)
March 11–14, 2020 / Portland OR, USA

AdaCore is exhibiting at this conference.
sigcse2020.sigcse.org/

Aerospace Tech Week
March 18–19, 2020 / Toulouse, France

AdaCore is exhibiting at this conference, and Ben Brosgol is delivering a presentation in the FACE pavilion: *Attaining Reusability and High Assurance for Avionics Software: the FACE™ Approach Meets DO-178C.*
www.aerospacetechweek.com/

NVIDIA's GPU Technology Conference (GTC) Silicon Valley 2020
March 22–26, 2020 / San Jose CA, USA

Quentin Ochem is presenting *Exterminating Buffer Overflows and Other Embarrassing Vulnerabilities with SPARK Ada on Tegra.*
nvidia.com/en-us/gtc/

Public Ada Training
May 11–15, 2020 / Paris, France

AdaCore is conducting an introductory Ada course at its Paris office.
www.adacore.com/public-ada-training/

TU-Automotive Detroit
June 2–4, 2020 / Novi MI, USA

AdaCore is a sponsor and exhibitor at this conference, and is presenting a Masterclass with NVIDIA on using SPARK to develop ISO 26262 safety-certified software.
www.automotive.knect365.com/tu-auto-detroit/

Ada-Europe 2020 (International Conference on Reliable Software Technologies)
June 8–12, 2020 / Santander, Spain

AdaCore is a sponsor and exhibitor at this conference.
www.istr.unican.es/ae2020/

GNU Tools Cauldron 2020
June 12–14, 2020 / Paris, France

AdaCore is an organizer and major sponsor of this event.
gcc.gnu.org/wiki/cauldron2020/

Sound Static Analysis for Security Workshop
June 19–20, 2020 / Menlo Park CA, USA

AdaCore is a co-sponsor of this workshop (hosted by SRI International).
www.adacore.com/frama-c-spark-2020/

newsflash

Initial Release of Instrumentation-Based GNATcoverage

AdaCore has extended its Ada code coverage tool, GNATcoverage, with a mode where coverage data is obtained from source code instrumentation. The new mode is available in the GNATcoverage v20.1 release on native Windows and GNU Linux platforms, with support for all versions of Ada. Operating in instrumentation mode, the new GNATcoverage tool brings significant performance boosts compared to the original technology, which relies on execution traces obtained from the environment. It currently handles statement and decision coverage, with partial support for MC/DC. Development is underway to complete the MC/DC support and to allow usage in cross environments without requiring an emulator or a probe.

Inria-AdaCore Cooperation Brings Prize for Applied Research

In October 2019 Claude Marché, director of Inria's Toccata research team, was awarded the French Federation of Electrical, Electronic and Communications Industries (FIEEC) Carnot first prize in Applied Research. The prize comes in recognition of a longstanding cooperation between Inria and AdaCore in formal proof technology, a joint effort that has productized advanced research and integrated the results into the SPARK verification environment. For more information on this prize, please see tinyurl.com/fieec-carnot-prize/.

Formal Methods White Paper Published

AdaCore has prepared a white paper explaining the rationale for using formal methods on critical software, with examples drawn from commercial practice. The report, When testing is not enough: Software complexity drives technology leaders to adopt formal methods, is available at www.adacore.com/papers/when-testing-is-not-enough/.

contact us!

Please contact us at info@adacore.com with questions/comments or to get further information about any of the items in this newsletter.

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