AdaCore DIGEST FEBRUARY 2024

AdaCore DIGEST

NEWSLETTER 02|24

24.1 Release

We're happy to announce the release of the stable version on branch 24 of our technology, GNAT Pro 24.1. This is the first version of branch 24 that we recommend for production builds. It will be followed by a bugfix release in July (24.2), which will be the last release for enterprise customers. Subscribers to GNAT Pro Assurance products will still be eligible for critical bugfix releases after that point.

Highlights of the 24 branch include our yearly GCC upgrade (now on version 12), C++ bare metal support, an in-depth and upgraded design of the CodePeer user interface (which is now known as the GNAT Static Analysis Suite), and much more. Full release notes are available here.

Crate of the Year 2023

We're excited to announce the winners of the 2023 Ada/SPARK Crate of the Year Awards, celebrating the best in the Alire ecosystem. For 2023, we broadened our approach to include all Alire crates, showcasing the community's rich diversity and innovation.

Winners at a glance:

Ada Crate of the Year: Tama McGlinn's AdaBots, an engaging educational platform that introduces children to programming through interactive gameplay.

Embedded Crate of the Year: German Rivera's HiRTOS, a high-integrity RTOS kernel in SPARK Ada, enhancing the Alire ecosystem for embedded developers.

SPARK Crate of the Year: Rod Chapman's SPARKNaCl, a cryptography library that highlights SPARK's capabilities in handling complex applications.

Congratulations to the winners and thanks to all who participated. These awards underscore the vibrant growth and potential within the Ada/SPARK community. Stay tuned for more exciting developments!

Glitch Hardening

AdaCore has significantly enhanced hardening of GNAT Pro compiled software with a suite of security features against cyber threats.

Hardening Comparisons and Conditional Branches

To protect against control-flow attacks, the option -fharden-compares enables hardening of comparisons that compute results stored in variables, adding verification that the reversed comparison yields the opposite result.

Control Flow Redundancy Verification

The introduction of this new option prevents attacks that manipulate control flow within functions. With -fharden-control-flow-redundancy, the compiler now verifies, on return from functions, whether the traversed basic blocks align with a legitimate execution path.

Hardened Booleans for C and Ada

We have introduced a new type attribute, hardbool, for both the C and Ada programming languages. Hardened booleans allow users to define custom representations for true and false, each with a higher Hamming distance than standard booleans. These representations are rigorously validated at every use, effectively detecting memory corruption and certain malicious attacks.

Stack Scrubbing Control

A second type attribute, strub, enables stack scrubbing properties of functions and variables. Functions marked with strub trigger a zeroing-out of the stack frame upon return or exception propagation, fortifying against unauthorized access. Additionally, scalar variables tagged with this attribute implicitly enable stack scrubbing for any function containing or accessing them. This sophisticated feature enhances the protection against memory-based attacks, contributing to a more resilient software infrastructure.

These advancements mark a significant step forward in securing GNAT Pro compiled software across languages like Ada and C, showcasing AdaCore's proactive approach to combating cyber threats and increasing users' confidence in their applications' security.

Public Ada Training

There are still spaces available for our upcoming five-day Public Ada Training course on March 18th-22nd. This in-depth course, conducted remotely by our expert instructors, will provide you or your team with a fast track to software engineering proficiency in Ada. Find details about this and other upcoming courses and registration here.

Latitude Adopts Ada and SPARK for Light Launcher Software in New Space Industry

In the competitive New Space industry, French aerospace company Latitude developed their Zephyr small satellite launcher and recognized the critical role played by the programming language and its support tools in the software life cycle. After evaluating various options, they chose Ada and its formally verifiable SPARK subset as providing the best support for sound software engineering practice, reducing costs, and ensuring high performance in real-time systems. Their success with these technologies has led Latitude to plan their continued use in future projects as key enablers.

AdaCore's specialized training, including hands-on workshops, provided guidance on Ada's safety features and best practices, enabling the Latitude team to quickly become proficient and transition to SPARK for critical software components. This strategic choice supports Latitude's aim to maintain innovation, reliability, and efficiency in their space ventures.

Read the case study here.

LatenceTech: Innovating Network Tools

LatenceTech, a Canadian telecom startup, focuses on developing high-precision latency measurement tools for 5G and IoT networks. Their primary goal was to transform intricate latency metrics into actionable strategies to improve Quality of Service (QoS) and enhance customer satisfaction regarding network performance.

Initially, LatenceTech developed their Minimum Viable Product (MVP) using C# and Python, but they later transitioned to Scala to better align with industry standards. The pivotal shift came when they adopted Ada, known for its robust support in high-assurance systems, leading to a fruitful partnership with Orange, a leading French telecom provider, on projects like energy-efficient network bandwidth testing.

Utilizing AdaCore's GNAT Pro for Ada, LatenceTech was able to create stable and resourceefficient network tools, successfully meeting real-time telecom demands. Their success demonstrates the effectiveness of AdaCore's tools in developing and verifying complex network applications, spotlighting AdaCore's role in fostering telecom innovations.

Read the case study here.

Events

On 31 January, AdaCore hosted the second in a series of webinars focused on SPARK Pro, covering the topic of Memory Safety with Formal Proof. Attendees learned how to prove that code cannot fail at runtime, including insights into proof of memory safety and correct data initialization, by using SPARK Pro. Memory Safety with Formal Proof is available to watch on demand here.

Our next and final webinar in the series, Proving Software Security, will take place on 27 March and will highlight methods for proving program correctness. AdaCore's Yannick Moy will outline key features of SPARK Pro for proving that code obeys its specification, including the language to express this specification, and the process to successfully prove compliance. Learn more about our Proving Software Security with SPARK Pro webinar.

AdaCore will be exhibiting at SIGCSE on March 20-23, showcasing capstone projects using Ada and meeting with the academic Ada community.

On 11 April, we will be running a High-Integrity Technology Update webinar, created exclusively for AdaCore customers to boost their programming security and safety in 2024. AdaCore Product Manager José Ruiz will provide a deeper dive into AdaCore's latest software releases and future roadmap for customers based in European and US time zones.

Sign up for the Technology Update (Europe | 15:00 BST / 16:00 CEST) Sign up for the Technology Update (US | 15:00 EDT / 12:00 PDT)

The 2024 Ada-Europe International Conference on Reliable Software Technologies (AEiC) will take place in Barcelona, Spain from June 11th to 14th. The Industrial Track seeks contributions within the conference's scope, particularly emphasizing practitioner insights on reliable software, high-integrity, and cyber-physical systems development, including open challenges, experiences with tools and methodologies, lessons learned, and reports from significant projects where software reliability is crucial. We warmly invite you to consider sharing your insights and experiences at the conference. Head over to the submission page for more information.

SPARK in the Communications of the ACM

We're excited to announce that the Communications of the ACM has published a paper on SPARK: "Co-Developing Programs and Their Proof of Correctness". The paper provides a comprehensive and up-to-date presentation of SPARK, including: an overview of the programming language and its design goals; an explanation of what it means to co-develop a program and its proof of correctness; and approaches to practical, incremental adoption that allow at-scale application to industrial, highintegrity systems.

If you have questions about any of the technologies or services mentioned above, please reach out to your Account Manager or email us at info@adacore.com