AdaCore

AdaCore Toolchain for Ada, SPARK and C Now Qualified for ISO 26262 and IEC 61508

NEW YORK & PARIS, February 18, 2020 - AdaCore today announced that three of its signature software development/verification tools for Ada, SPARK and C have been qualified under the ISO 26262 and IEC 61508 functional safety standards. AdaCore has over two decades of certification experience in safety-critical domains such as avionics, space, and rail. By completing the qualification process for automotive and industrial standards, the company has shown that its high integrity technologies can meet the demanding assurance requirements of the software-intensive automotive industry.

The three development/verification tools qualified for compliance are:

- **GNAT Pro**, a robust and flexible development environment comprising an industrial-grade toolchain that supports the Ada and C programming languages, either standalone or mixed in a single binary. GNAT Pro comes with a range of development and verification tools, including stack size computation, coding standard verification, and a customizable/extensible IDE.

- The **Common Code Generator (CCG)**, which compiles from a SPARK-like Ada subset to C code. CCG allows projects to cross-compile Ada and SPARK applications to any hardware target that provides a C compiler, including targets that do not come with off-the-shelf Ada support.

- **SPARK Pro,** a toolset based on an Ada language subset that allows developers to formally guarantee properties of source code, such as the absence of certain categories of vulnerabilities (buffer overflow, division by zero, references to uninitialized variables), and to prove custom functional assertions.

Both the GNAT Pro compiler and CCG received TCL3 qualification under ISO 26262, and T3 qualification under IEC 61508. The SPARK Pro verification tool received TCL3 and T2 qualification. All three products have been certified by TÜV SÜD, an independent, globally recognized organization which confirms that products meet national and international standards. The TÜV SÜD certification mark is widely acknowledged and respected as a trusted symbol of quality, safety, and sustainability.

“The demand for cost-effective tools and methodologies have greatly increased in the automotive and industrial domains over the past few years,” said Quentin Ochem, Lead of Business Development at AdaCore. “The Ada and SPARK languages have emerged as viable

alternatives to C for many developers needing higher integrity software. The completion of our safety certification under the corresponding standards demonstrates our commitment to support these industrial projects on their own path to adoption."

About ISO 26262 and IEC 61508

ISO 26262 is a functional safety standard for automotive systems and a derivative of the generic IEC 61508 standard for electrical/electronic/programmable electronic ("E/E/PE") systems. It defines an automotive safety lifecycle's phases and their associated activities and uses a risk-based approach to determine Automotive Safety Integrity Levels (ASILs) and the relevant requirements. An analysis of the system's functions focuses on the potential hazards in the event of a failure, and the consequences to life and property. The computed ASIL ranges from A (least critical) to D (most critical) and takes into account the estimated probability of the failure being exposed, whether the driver can ameliorate the hazard in response, and the severity of the hazard's occurrence.

ISO 26262 specifies requirements for tool qualification, recognizing the benefits from automation in terms of both productivity and accuracy, and defines four tool qualification methods:

- Increased confidence from use,
- Evaluation of the tool development process,
- Validation of the software tool, and
- Development in accordance with a safety standard.

Qualification is based on the calculated Tool Confidence Level (TCL), ranging from 1 (lowest) to 3 (highest). A tool's TCL is in turn determined by whether / how an error in the tool or its output can lead to a safety hazard (the "Tool Impact"), and the probability of preventing/detecting such errors ("Tool Error Detection"). A tool at TCL1 does not need qualification. TCL2 and TCL3 tools require qualification, with the system's ASIL determining which qualification methods are most recommended. Tool qualification artifacts include a Software Tool Qualification Plan, Software Tool Documentation, a Software Tool Classification Analysis (which establishes the relevant TCL), and a Software Tool Qualification Report.

IEC 61508 is an international standard for functional safety in E/E/PE systems and is the "umbrella" for domain-specific standards such as ISO 26262. The standard is based on the concepts of a *safety life cycle* (the engineering processes needed for functional safety) and *safety integrity level*, or SIL (the level of risk reduction). The SILs range from SIL1 (lowest requirement for risk reduction) to SIL4 (highest). The SILs are defined in terms of probability of failure on demand; e.g. for SIL4 the probability of a dangerous failure per hour of continuous operation is between 10^{-9} and 10^{-8}.

Software-related requirements are defined in Part 3 of IEC 61508, with the identification of techniques and measures for software development/verification; the specific requirements are based on the SIL. The standard specifies three tool qualification categories:

- T1: the tool is not used to either verify the code or to produce output that is part of the executable (e.g., a text editor),
- T2: the tools may fail to detect an error but does not generate code that is part of the executable (i.e., a verification tool such as a coding standard checker), and
- T3: the tool can produce output that is part of the executable (e.g., a compiler).

Tools classified at T2 or T3 must have the appropriate documentation, with T3 requiring additional justification (based on user experience or test cases) that the tool complies with its documentation.

About AdaCore

Founded in 1994, AdaCore supplies software development and verification tools for mission-critical, safety-critical and security-critical systems. Four flagship products highlight the company's offerings:

- The *GNAT Pro* development environment, a complete toolset for designing, implementing, and managing applications that demand high reliability and maintainability. GNAT Pro is available for Ada and also for C and C++.
- The CWE-Compatible *CodePeer* advanced static analysis tool, an automatic Ada code reviewer and validator that can detect and eliminate errors both during development and retrospectively on existing software. CodePeer can detect a number of the "Top 25 Most Dangerous Software Errors" in the MITRE Corporation's Common Weakness Enumeration (CWE).
- The *SPARK Pro* verification environment, a toolset providing full formal verification oriented toward high-assurance systems with stringent security requirements.
- The *QGen* model-based development tool suite for safety-critical control systems, providing a qualifiable and customizable code generator and static verifier for a safe subset of Simulink® and Stateflow® models, and a model-level debugger.

Over the years customers have used AdaCore products to field and maintain a wide range of critical applications in domains such as commercial and military avionics, automotive, railway, space, defense systems, air traffic management/control, medical devices, and financial services. AdaCore has an extensive and growing worldwide customer base; see www.adacore.com/industries for further information.

AdaCore products are open source and come with expert online support provided by the developers themselves. The company has North American headquarters in New York and European headquarters in Paris. www.adacore.com.

Press Contacts

AdaCore US	AdaCore EU	AdaCore UK
Jessie Glockner	Pamela Trevino	Singleton PR
E: glockner@adacore.com	E: trevino@adacore.com	E: abigail@singletonpr.com
T: +1-646-532-2723	T: +33 1 49 70 87 82	T: +44 (0)1252 448 169

http://www.adacore.com

http://twitter.com/AdaCoreCompany