DENSO Using AdaCore's SPARK Technology for Automotive Research Project

Formal methods help to demonstrate Freedom from Interference

NUREMBERG, Germany, Embedded World Conference, February 27, 2018 – AdaCore today announced the successful completion of a research project for DENSO, *Application of Formal Methods to Help Achieve Freedom from Interference*. This project, conducted jointly with the University of Nagasaki, had the goal of simplifying the development of safety-critical automotive applications in an ISO 26262 context. The project investigated the use of VDM as a design method, and SPARK as an implementation language, for safety-critical components in systems where legacy C code is prevalent. The SPARK components need to be protected from potential interference from the legacy C code, as required by ISO 26262 ("Freedom from Interference", or "FFI"). DENSO selected AdaCore because of the company's expertise in formal methods, as proven by the SPARK Pro technology.

In the first phase of the project, AdaCore and the University of Nagasaki investigated the FFI problem. The University of Nagasaki team analyzed the use of formal methods and determined that the SPARK approach can significantly simplify the effort in demonstrating system safety. AdaCore showed that the SPARK technology can prove the absence of errors in the critical (high ASIL) components themselves, which simplifies the verification effort. AdaCore also produced guidelines for adding SPARK executable contracts (function pre- and postconditions) to lower ASIL legacy C code. Such contracts can help in demonstrating safety, by insulating the more critical components against failures of less critical components.

After the initial phase of the contract was completed, DENSO authorized AdaCore and the University of Nagasaki to continue with Phase 2. During this phase, AdaCore explored the possibility of applying formal methods to the more general problem of safety analysis of a software architecture. The University of Nagasaki used VDM to specify guidelines for applying safety process measures and safety mechanisms to detect / prevent cascading failures. Phase 2 was completed in October 2017.

“Our SPARK technology makes formal methods a practical tool for critical automotive software, and we’re pleased that DENSO gave us the opportunity to demonstrate these benefits on their FFI project,” said J.C. Bernedo, Automotive Market Product Manager at AdaCore. “A frequent question is how formal methods can be used in existing systems where there may be lots of legacy code in C. Our work for DENSO showed that SPARK can be easily integrated and combined with traditional testing-based verification methods, to achieve the highest levels of confidence in the software's reliability, safety and security.”

“AdaCore is not only a tool vendor but also an excellent research partner,” said Mr. Tetsuya Tohdo, Project Manager at DENSO's Tokyo Office in the ePF Advanced R&D Department. “This project gave us a rapid understanding of several research subjects, and we have been able to take advantage of the ideas that were presented. In particular, the proposal for Phase 2 called for the usage of powerful open source tools, and we expect that these will not only promote research projects effectively but will also provide a shortcut to practical applications afterwards. With its technical knowledge of development tools and their underlying research foundations, AdaCore supplied a comprehensive solution.”

“We use VDM (Vienna Development Method), one of the established model-oriented formal methods for the development of computer-based systems and software,” said Professor Shigeru Kusakabe from the University of Nagasaki. “Constructing and analyzing the VDM model helps us to identify incompleteness and ambiguity in the system specifications from the early stages of the development. We are working to combine this well-established formal method with emerging holistic system engineering approaches for FFI.”

About Freedom from Interference

Automotive manufacturers need to conduct a safety analysis of their software, showing that it carries out its safety-related functionality even in the presence of certain faults. Part of this analysis is to demonstrate that the Freedom from Interference (FFI) objective is met. FFI is required by ISO 26262 and is defined as the “absence of cascading failures between two or more elements that could lead to the violation of a safety requirement,” when safety-critical and non-safety features co-exist. For example, the software that controls an automated driving system is safety critical and must be protected from lower-ASIL components (such as infotainment); FFI is a practical approach to addressing this issue.

About SPARK Pro

SPARK Pro is an integrated static analysis toolsuite for verifying high-integrity software through formal methods. It supports the SPARK 2014 language and provides advanced verification tools that are tightly integrated into the GNAT Programming Studio (GPS) and GNATbench IDEs.

Using SPARK Pro, developers can formally define and automatically verify software architectural properties, and guarantee a wide range of software integrity properties, such as freedom from run-time errors, enforcement of security policies, and functional correctness (compliance with a formally defined specification). This automated verification is particularly well-suited to applications where software failure is unacceptable. SPARK Pro helps reduce delivery costs and timescales, and, through the use of formal methods, prevents, detects and eliminates defects early in the software lifecycle with mathematics-based assurance. The SPARK language and tools have a proven track record in the most demanding safety-critical and high-security systems.

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 for Ada, a complete toolset for designing, implementing, and managing applications that demand high reliability and maintainability,
- The *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,
- The *SPARK Pro* verification environment, a toolset based on formal methods and oriented toward high-assurance systems, and
- The *QGen* model-based development tool suite for safety-critical control systems, providing a qualifiable and customizable code generator, a static verifier for 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 avionics, automotive, railway, space, military systems, air traffic management/control, medical devices and financial services. AdaCore has an extensive and growing worldwide customer base; see www.adacore.com/customers/ 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

About DENSO

DENSO is a worldwide supplier of advanced technology, systems and components in the automotive industry, and employs more than 150,000 people in 38 countries and regions. www.denso.com

About University of Nagasaki

The University of Nagasaki established the Faculty of Information Systems in 2016. This new faculty consists of the Department of Information Systems and the Department of Information Security, Japan's first undergraduate department designed for information security. This combination is expected to facilitate integrated approaches to safety and security.

Press Contacts

press-info@adacore.com

http://www.adacore.com

http://twitter.com/AdaCoreCompany

EU:

Emma Adby
AdaCore Marketing Operations Manager
+33 1 49 70 87 82

US:

Jessie Glockner
AdaCore Public Relations Representative
+1-646-532-2723