Light-weight static analysis of critical embedded code

AdaCore
46 rue d'Amsterdam
75009 Paris, France

moy@adacore.com

Brief company description

Founded in 1994, AdaCore is the leading provider of commercial software solutions for Ada, a state-of-the-art programming language designed for large, long-lived applications where safety, security, and reliability are critical. AdaCore's flagship product is the GNAT Pro development environment, which comes all open-source with expert on-line support and is available on more platforms than any other Ada technology.

Our main offices are located in Paris, New-York and Lexington.

Internships coordination: Olivier Hainque

This internship

AdaCore develops compilers and static analyzers for the critical embedded market, around the Ada, SPARK, C and C++ languages. AdaCore is providing state-of-the-art deep static analyzers for ensuring correct operation of critical embedded software, but lacks a solution for light-weight static analysis as performed in less critical industries. The goal of this internship is to prototype such a solution.

AdaCore is developing and commercializing two major static analysis products: CodePeer for finding bugs (http://www.adacore.com/codepeer) and SPARK for providing guarantees (http://www.adacore.com/spark) on Ada programs. These products require to develop a degree of expertise in the underlying technology to be used effectively, and their use can be costly in terms of resources (machines, people). Hence these tools are typically used for high assurance software, where the additional confidence provided by deep static analysis outweights the costs.

On the contrary, many Web companies have adopted light-weight static analysis integrated in their agile code-review-commit cycle. Some of these tools are deployed for checking all commits in the huge codebases of Google (Tricorder) or Facebook (Infer). Others are commercial tools implementing hundreds of small checkers (SonarLint, PVS Studio). The recent Libadalang technology, developed at AdaCore, provides an ideal basis on which to develop such light-weight static analysis, as it can parse and analyze thousands of lines of code in seconds. As an experiment, we implemented two simple checkers using the Python binding of Libadalang, and we found a dozen bugs in the codebases of the tools we develop at AdaCore (including the compiler and static analyzers).

The goal of this internship is to adapt some of these checkers for the critical embedded industry using Ada.

Goals

- Briefly study the available checkers / competing solutions.
- Define a set of light-weight checkers targeting critical embedded code.
- Implement the checkers with the Python binding of Libadalang.
- Apply the checkers to codebases in Ada (AdaCore tools and customer software).
- Give recommendations for an industrial tool for light-weight static analysis of critical embedded code.

References

- Libadalang: https://github.com/AdaCore/libadalang
- Tricorder: research.google.com/pubs/archive/43322.pdf
- Infer: https://research.facebook.com/publications/moving-fast-with-software-verification/
- SonarLint: http://www.sonarlint.org/
- PVS Studio: http://www.viva64.com/en/pvs-studio/

Skills required

- Good programming skills
- Knowledge or interest in static analysis
- Knowledge of Python is a plus

Location & Timeframe

Paris, during 2017 - 4 to 6 months

Contact

Yannick Moy