

# COUVERTURE - Project Coverage

## An Innovative Open Framework for Coverage Analysis of Safety Critical Applications

Intended speaker: Matteo Bordin, AdaCore (bordin@adacore.com)

One domain where Ada is very present is that of Safety Critical applications, when human lives depend on the correct behavior of computer programs. Certification is the process through which safety critical applications get official authorization to operate, which typically materializes as a strict guidance/audit of their development process. An example is the DO-178B standard enforced by the US Federal Aviation Administration in the civil avionics area. This abstract is a proposal for an industrial presentation of COUVERTURE (French word for Coverage), a recently started French project with strong connections to certification activities.

COUVERTURE aims at offering an innovative framework to address a common aspect of certified developments: the requirement to perform structural coverage analysis to assess the quality of a testing campaign. In the context of the French government “Competitive Clusters” initiative to encourage research, a two-years funding was awarded to the project, submitted as part of the Free Software thematic group. Two companies are involved in the development: AdaCore and OpenWide, together with the CS labs of two academic partners: Telecom ParisTech and the Paris 6 university.

The core idea is to analyze coverage from machine-level execution traces out of an instrumented execution environment such as a target microprocessor emulator. For common traditional processors, we are using Qemu for this purpose, as a reliable and efficient free-software emulator we can instrument to generate the traces. This allows very flexible non-intrusive analysis on final target code with emulators running on development hosts.

The software components will come with material to demonstrate that their outcome is dependable and allow qualification of the tools for use in a certification context, up to the strictest level for DO-178B. Compliance with such certification levels represents an interesting challenge, in particular regarding the Modified Condition/Decision Coverage criteria.

Both the software components and the qualification material are going to be Freely licensed. Significant parts of the software are developed in Ada. We believe this project is a nice opportunity to initiate a constructive synergy between the Free Software community and the industrial teams who develop certified applications. This is actually a part of a wider project, informally called “OpenDO” to date, whose intent is to federate such initiatives on various aspects of the certification activities.

The proposed “industrial presentation” talk would include

- A brief introduction of the COUVERTURE project context and major drivers (safety-critical apps, certification, Free software movement),
- A brief presentation of the target activity (what is structural coverage, what is the intent in DO-178B like certification processes),
- An introduction to the project essential ideas and challenges, then a short prototype demo.