2018-01106 - Engineer R&D in Formal Methods for Software Engineering (M/F)

Contract type: Public service fixed-term contract
Renewable contract: Oui
Level of qualifications required: PhD or equivalent
Fonction: Temporary scientific engineer

About the research centre or Inria department

Located at the heart of the main national research and higher education cluster, member of the Université Paris Saclay, a major actor in the French Investments for the Future Programme (Idex, LabEx, IRT, EquipeX) and partner of the main establishments present on the plateau, the centre is particularly active in three major areas: data and knowledge; safety, security and reliability; modelling, simulation and optimisation (with priority given to energy).

The 450 researchers and engineers from Inria and its partners who work in the research centre's 31 teams, the 100 research support staff members, the high-level equipment at their disposal (image walls, high-performance computing clusters, sensor networks), and the privileged relationships with prestigious industrial partners, all make Inria Saclay Île-de-France a key research centre in the local landscape and one that is oriented towards Europe and the world.

Context

The job is directly funded by the Joint Laboratory « ProofInUse » (https://www.adacore.com/proofinuse). The objective of ProofInUse is to provide verification tools, based on mathematical proof, to industry users. These tools would be aimed at replacing or complementing the existing test activities, whilst reducing costs. ProofInUse originates from the sharing of resources and knowledge between the Inria team Toccata specializing in techniques for program proofs and the SME AdaCore (https://www.adacore.com), a software publisher, specializing in providing software development tools for critical software technology. A previous successful collaboration between Toccata and AdaCore enabled Toccata’s Why3 technology, to be put into the heart of the AdaCore-developed SPARK technology. The SME TrustInSoft (https://trust-in-soft.com/), specialized in advanced static analysis techniques for safety and security of C/C++ critical source code, recently joined the ProofInUse Laboratory.

The purpose of ProofInUse is to increase significantly the number of customers of the TrustInSoft Analyzer technology, by popularizing the use of formal proof techniques. This popularization requires the resolution of several scientific and technological challenges. A first axis of work is to design and implement a new plug-in for deductive verification in the TrustInSoft Analyzer, making use of the Why3 intermediate (https://why3.iri.fr/) tool for verification condition generation, along the guidelines and design choices previously adopted for SPARK, that include strong restrictions on the analyzed code regarding the possibility of aliasing in data structures. This new plug-in must support new techniques for analyzing bit-level and floating-point codes, as well as new facilities for providing counterexamples when proofs fail. A second axis of work is to leverage the former non-aliasing restrictions, via an alias analysis based on a Rust-style sharing control and borrowing. A third axis is to actively participate to the development of a formally proved C/C++ software library.

The job will take place both on Toccata's lab site in building 650 of University Paris-Sud in Orsay, and at TrustInSoft's site in Paris. Travel expenses are covered within the limits of the scale in force.

Assignment

The recruited engineer will work in close collaboration with the ProofInUse Research and Development team, to address both the scientific and the technological challenges presented above. It is expected that the engineer contributes both to advancing the academic knowledge in ProofInUse context and to the transfer of this knowledge into the software products distributed by AdaCore and TrustInSoft.
Main activities

The engineer will participate actively to the production of scientific publications, and to the software development of the Why3 tool and the TrustInSoft Analyzer.

Skills

We expect from the candidate some experience with Formal Methods for Software Engineering in a broad sense, typically the candidate should have defended a PhD in the domain of Formal Methods. More specifically, a plus would be some experience in formal logic and proof techniques, in automated deduction, in Satisfiability Modulo Theory solvers, in Model Checking or in Abstract Interpretation techniques.

The candidate should have a fair experience in software development, a plus would be the knowledge of functional programming, and the knowledge of the programming languages Ocaml, C/C++ and Rust.

The candidate should be able to write and speak in English fluently.

Benefits package

- Subsidised catering service
- Partially-reimbursed public transport
- Social security
- Paid leave
- Flexible working hours
- Sports facilities

Remuneration

Salary in regard to diplomas and professional experiences.