Offer #2024-08516

Research and Development Engineer (M/F), Formal Verification of Rust Programs

Contract type : Fixed-term contract

Renewable contract : Yes

Level of qualifications required : Graduate degree or equivalent

Other valued qualifications : PhD Thesis in Computer Science

Fonction : Temporary scientific engineer

Level of experience : Recently graduated

About the research centre or Inria department

The Inria Saclay-Île-de-France Research Centre was established in 2008. It has developed as part of the Saclay site in partnership with **Paris-Saclay University** and with the **Institut Polytechnique de Paris** .

The centre has **40 project teams** , 32 of which operate jointly with Paris-Saclay University and the Institut Polytechnique de Paris; Its activities occupy over 600 people, scientists and research and innovation support staff, including 44 different nationalities.

Context

This job is proposed in the context of the Décysif project (https://decysif.fr/), a collaborative project aiming at applying formal methods to the development of high-assurance software that are critical for safety and security. This project gathers the Inria project-team Toccata (https://toccata.gitlabpages.inria.fr/toccata/) and industrial partners located in Paris: TrustInSoft, AdaCore and OCamlPro. The general objective is to contribute to the activities of formal verification performed by these partners, those conducted around the verification of programs in Ada, C, C++ and Rust, with techniques using the proof tools developed by the Toccata team, in particular Why3.

The work will be carried out mainly in the Toccata team location in Gif-sur-Yvette and partly in the partner company offices in Paris. Travel expenses are covered within the limits of the scale in force.

Assignment

In direct collaboration with the research scientists at Toccata and with the research engineers at the industrial partners, the person recruited will have to work on the maturation of the Creusot prototype (https://github.com/xldenis/creusot) dedicated to formal verification of Rust programs. This prototype comes from a doctoral thesis and must be improved to be able to be applied to industrial case studies. The objectives concern, among other things, the extension of the supported Rust fragment, the need to complete specifications of Rust libraries, the improvement of the usability of the graphical user interface, the increase of the rate of proof automation, to set up methods to help proof (such as the generation of counterexamples in case of proof failure), to strengthen the robustness and reproducibility of proofs.

Main activities

Software development in Rust and OCaml, development of library specifications in Why3 and Rust, use of

external SMT solvers, software experimentation, writing documentation, contribution to the writing of scientific articles.

Skills

We seek for candidates with as much experience and skills as possible in several domains among : development using the OCaml language ; development using the Rust language ; techniques for evaluation, compilation and/or transformation of programs ; formal methods for software engineering ; formal logics ; static analysis of programs ; computer-assisted theorem proving ; use of formal proof environments.

A level of English at least in writing is required. In oral English or French must be sufficiently mastered.

Benefits package

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Remuneration

Regards to professional experiences

General Information

- **Theme/Domain :** Proofs and Verification
  Software engineering (BAP E)
- **Town/city :** Gif-sur-Yvette
- **Inria Center :** Centre Inria de Saclay
- **Starting date :** 2025-03-01
- **Duration of contract :** 2 years
- **Deadline to apply :** 2025-05-31

Contacts

- **Inria Team :** TOCCATA
- **Recruiter :**
  Marche Claude / Claude.Marche@inria.fr

About Inria

Inria is the French national research institute dedicated to digital science and technology. It employs 2,600 people. Its 200 agile project teams, generally run jointly with academic partners, include more than 3,500 scientists and engineers working to meet the challenges of digital technology, often at the interface with other disciplines. The Institute also employs numerous talents in over forty different professions. 900 research support staff contribute to the preparation and development of scientific and entrepreneurial projects that have a worldwide impact.

The keys to success

The candidate will be required to work in a team with all Why3 and Creusot developers and also to participate in joint activities of the research team: joint seminar, working groups, etc. Likewise, he/she will be required to work in collaboration with engineers at AdaCore, TrustInSoft and OCamlPro.

Warning : you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.

Instruction to apply

Defence Security :
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating

to the protection of national scientific and technical potential (PPST).Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy :
As part of its diversity policy, all Inria positions are accessible to people with disabilities.