INVENTEURS DU MONDE NUMÉRIQUE

Engineer R&D in Formal Methods for Software Engineering (H/F)

Type d'offre : **Engineer Research and Development**

Lieu de travail : Inria-Saclay center at Palaiseau / University Paris-Sud at Orsay / Adacore company in Paris

Thème de recherche : Formal Software Engineering Methods, Formal Verification of safety-critical Ada programs

Projet : Toccata (http://toccata.lri.fr)

About Inria and the job:

« Established in 1967, Inria is the only public research body fully dedicated to computational sciences. Combining computer sciences with mathematics, Inria's 3,500 researchers strive to invent the digital technologies of the future. Educated at leading international universities, they creatively integrate basic research with applied research and dedicate themselves to solving real problems, collaborating with the main players in public and private research in France and abroad and transferring the fruits of their work to innovative companies. The researchers at Inria published over 4,450 articles in 2012. They are behind over 250 active patents and 112 start-ups. The 180 project teams are distributed in eight research centers located throughout France. »

The job is directly funded by the Joint Laboratory « ProofInUse » (http://www.spark-2014.org/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 (http://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.

Mission:

The purpose of ProofInUse is to increase significantly the number of industrial customers of the SPARK technology, thus democratizing the use of proof techniques. This democratization requires the resolution of several scientific and technological challenges. A first axis of research and innovation is to facilitate the use of automatic provers. This first aspect requires the provision of a better interaction with the user, especially for debugging non-provable specifications as it is customary to expect for other development activities. Then, the Joint Laboratory aims at improving the ratio of provability of programs commonly used in industry, in particular for numerical computations and data manipulations. Indeed, the economic interest of proof techniques is based largely on their automation, hence any improvement in this respect will result in the SPARK technology becoming more attractive. These two points require scientific breakthroughs in terms of support to the generation of counter-examples and modeling of data types adapted to the intrinsic capacities of automated provers. A second axis of research and innovation is to allow the user to go beyond what is possible with the current SPARK technology, in terms of specification of programs and the proofs of these specifications. On the specification side, it will require the support for more complex constructions in the Why3 technology, permitting the extension of the programming language included in SPARK. This will, in particular, satisfy the user's need to specify data invariants. On the proof side, the objective of the Joint Laboratory is to give the user the possibility to guide the proof for more complex properties-for instance, those resistant to automated provers. These two points require scientific advances not only

CENTRE DE RECHERCHE
SACLAY - ÎLE-DE-FRANCE
Bâtiment Alan Turing
1 rue Honoré d'Estienne d'Orves
Campus de l'École Polytechnique
91120 Palaiseau
Tél. : +33 (0)1 72 92 59 00
Fax : +33 (0)1 74 85 42 42
www.inria.fr

at the level of the intermediate language constructs used for proofs, but also in the methods for generating proof obligations, permitting these uses.

Job offer description:

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. Concretely, the engineer will participate actively to the production of scientific publications, to the software development of SPARK-related tools, and to the support for Adacore customers.

Skills and profile:

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 and Ada.

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

Benefits:

- Canteen and cafeteria;
- Local transportation reimbursment

Start and duration of the contract:

The job should as soon as possible starting from May 1st, 2016
Duration : 12 months

Salary:

Gross salary between 2600 and 2900 €, that is approximately 2150 to 2400 € net salary.

Contact(s):

Claude Marché
Batiment 650, Université Paris-Sud, 91405 Orsay cedex, France
phone : +33-1-69-15-66-08
email :Claude.Marche@inria.fr

Yannick Moy
Adacore, 46 rue d'Amsterdam, 75009 Paris, FRANCE
phone : +33-1-49-70-87-75
email : Yannick.Moy@adacore.com