**Context and qualifications**

**Mission description**

The B, Event-B, and TLA+ methods are well-known formalisms that target the development of software systems used in critical applications, subject to stringent certification requirements. Mathematically, they are based on variants of Zermelo-Fraenkel set theory, and their application generates proof obligations, for example for ensuring the preservation of invariants or the correctness of refinements between models described at different levels of abstraction. All three methods are supported by toolssets (Atelier B, Rodin, and the TLA+ ToolBox) that include trusted engines for automatic proof and implement translations from the set-theoretic language underlying the methods to the input languages of automatic theorem provers.

The ANR project ICSPA aims at improving confidence in the proofs carried out in the context of B, Event-B, and TLA+ by formally and independently verifying these proofs using an independent proof checker with a small trusted base. Moreover, given the similarity between the underlying mathematical theories of these methods, it aims at enabling sharing and reusing proofs and theories between B, Event-B, and TLA+. Both objectives rely on the use of a common logical framework, called the calculus modulo theory and implemented in the system Dedukti, in which any formal proof system can be expressed.

ICSPA brings together academic experts in formal methods and deductive reasoning (Samovar, Inria Nancy, Inria Saclay, IRIT, and LIRMM) and the Clearsy company, a leader in the application of formal methods to the design of critical systems, in a 4-year effort that aims to increase confidence and reuse of theories and proofs.

**Principales activités**

**Project description**

The first objective of the thesis is to express TLA+ set theory and proofs in the calculus modulo theory and implement it in Dedukti, in a way that enables interoperability with the set theory of B and Event-B. In particular, the logic of TLA+ is untyped whereas B and Event-B are based on a typed logic. It is therefore expected that it will only be possible to define partial translations between the two formalisms, exploiting the fact that many proofs do not use the full power of the theory they are expressed in. The representation of TLA+ set theory can reuse ideas from the existing encoding in the logical framework Isabelle for TLAPS, the TLA+ Proof System.

In a second step, the back-end proof engines of TLAPS have to be instrumented in order to export proofs for checking by Dedukti. A similar mechanism has already been implemented for checking proofs produced by the Z3 back-end in Isabelle, but it will be adapted for Dedukti and extended to the proof traces provided by SMT solvers such as veriT and CVC5.

Finally, the thesis will study the export to Dedukti of full TLA+ specifications, rather than just individual formulas as for proof obligations, as well as the import of transition systems represented in Dedukti, in particular those arising from the translations from B and Event-B models. The purpose of these translations is to achieve reuse of (parts of) specifications expressed in B, Event-B, and TLA+, including importing libraries without having to reprove the associated theorems.

The thesis will be carried out at the Inria research center in Nancy, France, in joint supervision with Gilles Dowek from Inria Saclay, and in close collaboration with the partners of the BLaST project that focus on the B and Event-B methods. The expected starting date is September 1 or October 1, 2022, but a later starting date can be agreed upon.

**Compétences**

**Required qualifications**

The candidate must hold (or be about to obtain) a Master degree in computer science. Candidates must have solid knowledge in mathematical logic and preferably in automated or interactive reasoning. Experience with formal methods such as B, Alloy, TLA+ or Z would be a plus. The candidate should be fluent in a mainstream programming language such as OCaml, C++ or Java.

**Language**

English or French.

**Avantages**

- 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

**Rémunération**


Monthly salary after taxes: around 1596,05€ for 1st and 2nd year. 1678,99€ for 3rd year.

**Politique de recrutement:**

Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.

**Attention:** Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.