

Internship proposal M/F (6 months)

Design and Implementation of a GUI for a Specification Design Aid Tool Incorporating Exhaustive Verifications

Reference DME022019

Supervisor

Mitsubishi Electric R&D Centre Europe: David MENTRÉ, Research Manager

Overall context

With over 90 years of experience in providing reliable, high-quality products, MITSUBISHI ELECTRIC CORPORATION is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. Designing so many products require constant improvements in the manufacturing process, as much as the design stage than at the implementation stage. This internship proposal focuses on the improvement of the design stage within Information and Network Systems team of MITSUBISHI ELECTRIC R&D CENTRE EUROPE.

Internship subject

For product manufacturing, specification is crucial. This is especially true for software which, while being more “soft”, therefore making people think, that it is easier to modify, can trigger very high reworking costs if specification errors are detected too late in the development process. There are nowadays means to improve the clarity of the specification and do several checks on them for consistency, completeness or redundancy. An example of such a mean is “Parnas Tables” imagined by David Lodge Parnas: a table represents the specification of a function, each cell being a case of the specification. From this tabular representation, one can do exhaustive verifications (using mathematically based formal methods) by translating the specification into logical formula that can be automatically checked using an automated prover. However such tool should be easy to use, the design of a both intuitive and helpful Graphical User Interface (GUI) is thus crucial. The purpose of this internship is to design and implement such a GUI in a tool that allows to specify functions of a software, automatically do verifications on them, give a nice and helpful feedback of this verification to the user within the GUI and then generate prototype of C code annotated with formal annotation (allowing further formal verification of the implementation against the specification).

Detailed objectives (and different steps)

The internship will consist in

- Design the GUI of the tool and implement it;
- Design and implement translation of input specification within the GUI into logical formula and then application of formal verification using Why3 logical framework;
- Design and implement back translation of errors (i.e. counter-examples) found through formal verification into easy to understand information at the GUI level;

- Design and implement translation of verified specification of the GUI into C code prototypes annotated with formal specification in ACSL language of Frama-C framework.

Different steps will be:

- Quick bibliographic study to acquire required knowledge in needed technologies (Parnas Tables, Why3 logical framework, automated provers and counter-examples generation, Frama-C framework and ACSL language);
- Design and implement the tool regarding its several aspects (as described above);
- Apply the tool on several industrial use cases to evaluate its usefulness and improve the GUI;
- Write final report on the tool, its documentation and an evaluation of its strengths and weaknesses.

Prerequisites

- Strong interest in Graphical User Interfaces and/or logic and formal methods;
- Demonstrable capacity to develop appealing GUI;
- Demonstrable practical knowledge in at least one functional or object-oriented language (OCaml, Haskell, Java, C++, Scala, Rust, ...);
- Strong practical knowledge in Software Engineering;
- Knowledge in one or more of following domains or tools would be a plus: graphical toolkits (e.g. Qt), Why3, SMT solvers (Z3, CVC4, ...), Embedded systems;
- Autonomy;
- English: read and written.

Duration: 6 months

Period: February 2019 to March 2020 (dates are flexible)

Contact: Magali BRANCHEREAU (jobs@fr.mercede.mee.com)

Thank you to provide us an application letter and your CV mentioning the reference of the internship (both in Pdf versions).

The signature of an Internship Agreement with your school is mandatory.