Proposition de stage niveau bac+5

Composition de composants et de contrats pour systèmes synchrones : formalisation en Why3

Cadre

Le CEA LIST est un centre de recherche technologique sur les systèmes à logiciel prépondérant qui mène ses recherches en partenariat avec les grands acteurs industriels du nucléaire, de l'automobile, de l'aéronautique, de la défense et du médical pour étudier et développer des solutions innovantes adaptées à leurs besoins. Au sein du CEA LIST, le Laboratoire de Sûreté des Logiciels (LSL), localisé à Saclay (Essonne, 91), développe des outils d'aide à la validation et à la vérification de logiciels et de systèmes matériels/logiciels, tout particulièrement dans le domaine des systèmes embarqués critiques.

Si le lieu du stage est le LSL du CEA LIST à Saclay, son sujet résulte d'une collaboration entre le LSL, Mitsubishi Electric R&D Centre Europe (MERCE) et l'ENSIIE. Il est donc co-encadré par des chercheurs de ces différents organismes.

Objectifs

Les systèmes matériels/logiciels sont aujourd'hui utilisés pour remplir des tâches de plus en plus critiques, tout en étant de plus en plus gros et complexes. Il est donc de plus en plus important et compliqué de s'assurer de leur correction, c'est-à-dire de vérifier qu'ils fournissent bien les fonctionnalités attendues. Parmi ces systèmes, ceux dits *synchrones* permettent de considérer que les flots de données et d'événements reçus et émis par le système peuvent être synchronisés sur une unique horloge globale. De tels systèmes synchrones sont particulièrement intéressants dans les domaines critiques car ils permettent de discrétiser le temps et de maîtriser plus facilement les interactions entre les différentes parties du système et leur environnement extérieur.

Une approche intéressante pour garantir la correction des systèmes, synchrones ou asynchrones, consiste à les développer corrects par construction en s'appuyant sur la notion de *contrat*. Un contrat définit, pour chaque *composant* du système, ses *pré-conditions*, c'est-à-dire les hypothèses requises pour son bon fonctionnement, ainsi que ses *post-conditions*, c'est-à-dire les propriétés fournies par le composant lorsque ses pré-conditions sont satisfaites.

Ces notions ont notamment été définies dans la méta-théorie de Benveniste *et al* [2]. Cette méta-théorie a ensuite été adaptée aux systèmes synchrones [1] et par Antonin Butant durant son stage de master [3]. Tout particulièrement, la théorie définie au cours de ce dernier a notamment pris en compte la notion de *rétro-action* qui permet de faire dépendre un composant de ses propres sorties, comme ce peut être le cas pour un compteur temporel dont la valeur à l'instant t dépend de sa valeur à l'instant $t-1$. Le pouvoir expressif de cette théorie a ensuite été validée expérimentalement sur une étude de cas fondée sur le système de vol d'un drone. Cette théorie et l'étude de cas associée méritent néanmoins d'être formellement vérifiées afin de garantir leurs propriétés fondamentales.

L'objectif principal du stage est ainsi de formaliser en Why3 cette théorie. En fonction du profil du candidat et du temps effectif du stage, des objectifs secondaires pourront être ajoutés, comme formaliser le système de vol du drone et/ou prouver en Coq les principales propriétés théoriques.

Plus précisément, la mission du stagiaire consistera à :

1. étudier et comprendre la théorie [3] et la méta-théorie [2] des contrats pré-existantes ;
2. définir formellement en Why3 les notions et les propriétés fondamentales de cette théorie ;
3. s'assurer que cette formalisation n'introduit pas d'incohérence ;
4. de manière optionnelle :
   - utiliser cette formalisation pour modéliser le système de vol du drone en Why3 ;
   - prouver les propriétés préalablement définies, à l'aide de prouveurs automatiques lorsque c'est possible et en Coq sinon.

En fonction du projet professionnel du candidat, une poursuite en thèse dans la continuité du stage est possible.

Candidatures

Le candidat idéal connaîtra Why3 et/ou Coq ou un environnment similaire. Il sera également à l'aise avec les méthodes formelles et les raisonnements logiques.

Contacts : Virgile Prevosto (`virgile.prevosto@cea.fr`) Julien Signoles (`julien.signoles@cea.fr`), Benoît Boyer (`B.Boyer@fr.merce.mee.com`) et Catherine Dubois (`catherine.dubois@ensiie.fr`)

Les délais administratifs de recrutement au CEA étant de 2 à 3 mois minimum, merci de prendre contact le plus tôt possible.

Références

[1] Albert Benveniste and Benoît Caillaud. Synchronous Interfaces and Assume/Guarantee Contracts. In *Models, Algorithms, Logics and Tools - Essays Dedicated to Kim Guldstrand Larsen on the Occasion of His 60th Birthday*, volume 10460 of *Theoretical Computer Science and General Issues*, pages 233–248. Springer, July 2017.

[2] Albert Benveniste, Benoît Caillaud, Dejan Nickovic, Roberto Passerone, Jean-Baptiste Raclet, Philipp Reinkemeier, Alberto Sangiovanni-Vincentelli, Werner Damm, Tom Henzinger, and Kim Guldstrand Larsen. Contracts for Systems Design : Theory. Research Report RR-8759, Inria Rennes Bretagne Atlantique, July 2015.

[3] Antonin Butant. Mixing proved and unproved system parts through contracts to ensure correct-by-construction system design. Master report, CEA LIST, September 2016.