MITSUBISHI ELECTRIC
Changes for the Better

MITSUBISHI ELECTRIC R&D CENTRE EUROPE

1, ALLEE DE BEAULIEU, CS 10806
35708 RENNES CEDEX 7, FRANCE
TEL. (+33) 02.23.45.58.58 – FAX (+33) 02.23.45.58.59

for a greener tomorrow

Proposition de thèse CIFRE

Un formalisme logique pour vérifier les exigences des modèles de systèmes hybrides

Ref BBY_PhD_201810

Partenaire industriel:	**MITSUBISHI ELECTRIC R&D CENTRE EUROPE (MERCE)** 1 allée de Beaulieu, CS 10806, 35708 Rennes Cedex 7, France Site web: http://www.mitsubishielectric-rce.eu/
Partenaire académique :	**Centre de recherche Inria Rennes Bretagne Atlantique** Equipe projet TEA Campus universitaire de Beaulieu 35042 Rennes Cedex
Type de contrat:	CDD de 3 ans, octobre 2018
Référence:	BBY_PhD_201810
Sujet de recherche:	Un formalisme logique pour vérifier les exigences des modèles de systèmes hybrides

Sujet proposé par:	Benoît BOYER, co-advisor, MERCE
et	Jean-Pierre TALPIN, advisor, INRIA
	Thierry GAUTIER, co-advisor, INRIA

Contexte:

L'objectif principal de ce projet doctoral est de construire des systèmes cyber-physiques avec une approche corrective par construction afin de vérifier les exigences vis-à-vis des deux facettes des aspects cybernétiques et physiques de telles conceptions. En particulier, l'approche envisagée est basée sur des composants étendus avec des contrats formels, de sorte que les composants et les contrats peuvent être composés, abstraits ou raffinés. L'accent devra être mis sur la preuve des propriétés au niveau du système en rassemblant les propriétés individuelles qui sont prouvées au niveau « composant ». Cette approche reposera sur une sémantique formelle, et devra être utilisable par des ingénieurs non spécialisés dans les preuves et outillés. Ainsi, trois parties principales seront à développer:

1. Un formalisme mathématique fournissant la base théorique sur laquelle la sémantique des composants et leurs interactions pourront être exprimées et utilisées pour prouver les propriétés visées. Ce formalisme devra être accompagné d'une méthodologie qui prescrive comment l'utiliser pour construire efficacement des systèmes cyber-physiques, c'est-à-dire modéliser la partie continue, spécifier et implémenter la partie discrète pour finalement vérifier les propriétés par rapport au comportement associé;
2. Une approche au niveau de l'utilisateur pour décrire les spécifications formelles, approche qui doit être expressive, facile à utiliser et pouvant être traduite dans le formalisme ci-dessus. En particulier, une approche de type Simulink (orientée flots de données) sera considérée pour spécifier le système conjointement avec les tables Parnas (par exemple, les outils SRC de NRL [1]) pour spécifier les contrats des composants du système;
3. Une implémentation concrète du formalisme dans un ensemble d'outils permettant de construire et de prouver les propriétés clés (latence, timing, invariant ...) des systèmes cyber physiques.

Objectifs:

La première partie s'appuiera sur des travaux antérieurs avec une approche basée sur les composants pour la conception de systèmes avec une sémantique exécutable de contrats [3] ainsi que sur des systèmes cyber-physiques formalisés en composants avec une base logique solide basée sur la logique différentielle dL et associée à un théorème de composition automatique pour prouver les propriétés de contrats de composants individuels [2].

Le projet doctoral consistera à fusionner les différents concepts introduits par ces travaux dans un cadre cohérent et à l'appliquer pour spécifier la sémantique d'un langage de composants de type Simulink permettant également de spécifier et de prouver des composants continus et discrets. En particulier, le cadre logique permettra de vérifier les exigences considérées comme des propriétés impliquées par les invariants différentiels du modèle analogique à l'interface entre les mondes cyber et physique. Les contrats de ces composants seront basés sur des actions gardées ou des propositions logiques (quantitatives) dans une logique de séparation. Enfin, la mise en œuvre de la partie cyber (ou discrète) devrait pouvoir être mise en œuvre en tant qu'ensemble de tâches écrites en langage C.

La deuxième partie devrait permettre de capturer et de formaliser les exigences en termes simples de logique de séparation pour permettre leur vérification formelle dans un processus industriel de conception de systèmes cyber-physiques. Les composants des modèles CPS considérés sont implémentés dans un langage de type Simulink étendus avec des contrats formels exprimés sous une forme simple comme les tables Parnas. Ces tables de Parnas seront complétées par des exigences tirées d'éventuelles spécifications textuelles ou informelles.

La troisième partie rassemblera les outils de preuve existants (Frama-C pour le langage C, Keymaera X pour dL, Liquid Haskell pour les types liquides, F * pour les types dépendants, ...) et les organisera de manière à ce que les propriétés industrielles pertinentes prouvées, c'est-à-dire vérifier les exigences par rapport à un raffinement de composants informatiques/numériques (obtenu, par exemple, par analyse statique ou vérification déductive). L'utilisation de la technologie de preuve devrait maximiser l'automatisation de la preuve. En cas d'erreur, des contre-exemples seront proposés au niveau de l'utilisateur, c'est-à-dire au même niveau de description que les contrats de composants initiaux en langage similaire à Simulink développés dans la seconde partie.

Afin de renforcer l'adéquation du projet doctoral avec les besoins industriels réels, Mitsubishi Electric R & D Centre Europe fournira un ensemble de cas d'utilisation pertinents du point de vue industriel dans les domaines de l'automatisation ferroviaire, automobile ou industrielle.

Candidatures

Le/la candidat(e) idéal(e) aura une solide expérience en logique mathématique, de l'expérience et de l'intérêt à la fois en analyse de programme, en théorie du contrôle et en conception de systèmes embarqués. En fonction de sa formation et de son expérience, il / elle relèvera l'un ou l'autre des défis posés par la vérification des exigences numériques et analogiques.

Le/la candidat(e) retenu(e) sera employé(e) par le partenaire industriel du projet Mitsubishi Electric R & D Centre Europe dans le cadre d'une subvention CIFRE et intégré à l'équipe-projet Inria TEA à l'Inria, à Rennes (Bretagne, France).

Merci d'adresser CV et lettre de motivation en format PDF par email (en spécifiant en objet : votre nom et la référence BBY_PHD_201810) au contact suivant : jobs@fr.merce.mee.com

Références

[1] Software cost reduction. Naval Research Laboratory: https://www.nrl.navy.mil/itd/chacs/5546/SCR

[2] "Compositional proofs in dynamic differential logic". S. Lunel, B. Boyer, J.-P. Talpin. International Conference on Applications of Concurrency to System Design (ACSD'17). Springer, 2017.

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