Soutenance de thèse

Hamza BOURBOUH soutiendra sa thèse de doctorat, préparée au sein de l'ENAC et intitulée «*Compilation et vérification formelle de modèles à base d'automates et de flots de données pour les systèmes critiques*»

Le 16 mars 2023 à 9h00, Amphi Bréguet, ENAC, 7 avenue Edouard Belin, 31400 Toulouse

devant le jury composé de

M. Pierre-Loïc GAROCHE	Professeur ENAC	Directeur de thèse
Mme Laure GONNORD	Professeure Université de Grenoble Alpes	Rapporteure
M. Benoit COMBEMALE	Professeur Université de Rennes 1	Rapporteur
M. Xavier THIRIOUX	Professeur ISAE-SUPAERO	
M. Éric FERON	Professeur Kubg Abdullah University of Science and Technology	
M. Guillaume BRAT	Chercheur NASA	Co-encadrant
Mme Yassamine SELADJI	Maîtresse de conférences Université Abou Bekr Belkaid	

Résumé : Ce travail de thèse porte sur la vérification de modèles Simulink/Stateflow par les méthodes formelles. L'objectif est de permettre la vérification des modèles Simulink par rapport aux propriétés formelles qui représentent les exigences du système. Nous avons proposé une traduction bidirectionnelle de Simulink/Stateflow vers Lustre, un langage synchrone avec une sémantique formelle bien définie. Le principal résultat de ce travail de thèse est la boîte à outils CoCoSim: un projet open source pour spécifier et vérifier les exigences définies par l'utilisateur sur les modèles Simulink. La boîte à outils a été conçue pour faciliter les activités de vérification et de validation (V&V) des modèles Simulink. De plus, la boîte à outils est hautement automatisée et possède une architecture personnalisable et configurable qui permet d'intégrer d'autres techniques pour augmenter l'évolutivité. La boîte à outils a également été intégrée avec d'autres outils de vérification pour accroître son applicabilité.

Mots clés : vérification formelle, automate, système embarqué critique, compilation, Conception basée sur des modèles, Vérification et validation

Summary: This Ph.D. work is focused on the verification of Simulink/Stateflow models by means of formal methods. The objective is to enable the verification of Simulink models with respect to formal properties that represent system requirements. We proposed a bidirectional translation from Simulink/Stateflow to Lustre, a synchronous language with well-defined formal semantics. The primary outcome of this Ph.D. work is the CoCoSim toolbox: an open-source framework for specifying and verifying user-defined requirements on Simulink models. The toolbox has been designed to ease verification and validation (V&V) activities for Simulink models. In addition, the toolbox is highly automated and has a customizable and configurable architecture that allows other techniques to be integrated to increase scalability. The toolbox has also been integrated with other verification tools to increase its applicability.

Keywords: Model-based design, Cyber-physical system, Formal methods, Simulink/Stateflow, Lustre, Verification and validation