Sémantique formelle d'un langage de modélisation du comportement des composants logiciels pour les systèmes de contrôle cyber-physiques

Formal semantics of a modeling language for the behavior of software components in cyber-physical control systems

Sujet de thèse de doctorat – Ph.D. subject
proposé par — proposed by
Jacques Malenfant
Jacques.Malenfant@lip6.fr

6 avril 2021

English description below

Les systèmes de contrôle cyber-physiques (SCCP) intègrent dans une coopération étroite des calculs sur dispositifs numériques (ordinateurs, systèmes embarqués, etc.) avec des processus physiques qu'ils supervisent et pilotent par une boucle de contrôle. Avec l'émergence de la société numérique, le potentiel économique et sociétal des SCCP est d'une importance cruciale, étant la technologie clé d'un grand nombre d'applications dans les domaines du transport, de l'énergie, de la santé, de l'industrie 4.0, des bâtiments et villes intelligentes, de la robotique, etc. Cependant, les SCCP sont bien connus pour être extrêmement difficiles à spécifier, à développer, à tester, à vérifier, à valider et à faire évoluer. Cette thèse se situe dans le contexte d'un projet plus global visant à développer un modèle à composants logiciels et une méthodologie de développement adaptée à la construction modulaire d'applications SCCP qui favorisent à la fois l'exactitude par construction et la réutilisabilité des composants et de leur assemblage.

L'approche qui sera plus précisément développée consiste à intégrer dans un modèle à composants une spécification formelle composable du comportement du composant et de son environnement physique sous la forme d'automates hybrides stochastiques et sa traduction en modèles exécutables sous la forme de modèles de simulation modulaires et composables. Ainsi, un système complet, incluant sa spécification, son code et les moyens de le tester, le vérifier et le valider, pourra être obtenu par composition parallèle des automates hybrides, des composants logiciels et des modèles de simulation individuels. Cette approche doit permettre de développer une méthodologie couvrant toutes les phases de développement d'un système, depuis l'élicitation des besoins jusqu'à l'évolution dynamique de l'application, en passant, par les phases de spécification, programmation, tests, vérification, validation, auto-configuration au déploiement ainsi que l'apprentissage machine préalable à l'exécution et pendant l'exécution de même que l'auto-adaptation dynamique du système.

Dans le cadre de cette thèse, l'objectif sera plus précisément de s'attaquer au langage de modélisation fondé sur les automates hybrides stochastiques. Le modèle à composants logiciels pour les SCCP que nous souhaitons développer doit intégrer dans son langage de définition la possibilité d'exprimer conjointement le code et le modèle de comportement fondé sur les automates hybrides. L'objectif sera donc de concevoir la partie de ce langage permettant de définir le modèle de comportement du composant. Pour cela, il s'agira de partir de deux sources d'inspiration majeures :

1. Les travaux de l'équipe de Nancy Lynch sur les automates hybrides dits Hybrid Input/Output Automata (HIOA), connus pour leur capacité à modéliser de manière composable les aspects états discrets et transitions discrètes au sein du système hybride stochastique.
2. Les travaux de Platzer sur un langage permettant d'exprimer plus précisément les aspects continus du système hybride stochastique et qui est doté d'une sémantique formelle par une approche logique.

Ces deux lignes de travaux présentent des idées très intéressantes, mais insuffisantes pour atteindre les objectifs que nous visons. En effet, notre objectif est d'utiliser concrètement cette modélisation dans le processus de développement logiciel pour exécuter conjointement le code des composants et les modèles de simulation de la partie physique pour faciliter le test, la validation, etc. Pour cela, il faut doter la langage de modélisation du comportement d'une sémantique d'exécution qui permettra de générer automatiquement les modèles de simulation correspondants en définissant de manière précise comment l'exécution du code et les modèles de comportement doivent interagir au fil du temps. Nous proposons donc d'utiliser une approche de type sémantique dénotationelle non pas fondée sur les domaines de Scott classiques mais plutôt sur les espaces de Banach, tel qu'illustré dans les travaux de de Bakker et de Vink, pour aborder la partie continue de la sémantique.

À titre de preuve de concept, le langage de modélisation conçu et formalisé dans la thèse sera utilisé pour modéliser un système de contrôle cyber-physique visant à gérer dynamiquement l'équilibre entre la consommation d'électricité et la production de cette dernière par l'utilisation d'énergie renouvelable dans un logement semi-autonome (ayant ses propres moyens de production et donc faisant de l'auto-consommation, mais pouvant aussi tirer de l'énergie du réseau classique lors des pointes de consommation). Pour cette application, il s'agira de modéliser par systèmes hybrides stochastiques à la fois la consommation d'appareils électriques courants (réfrigérateurs, four, machine à laver, etc.) et la production par des panneaux solaires et des éoliennes.

Publications et références

Les deux publications récentes de l'encadrant sont :

— J. Malenfant. Stochastic hybrid systems meet software components for well-founded cyber-physical systems software architectures. 13th European Conference on Software Architecture (ECSA), vol. 2, Paris, France, pp. 132-138 (ACM Press), 2019.
— J. Malenfant. Towards a well-founded software component model for cyber-physical control systems. Second IEEE International Conference on Robotic Computing (IRC 2018), pp. 262-265, 2018.

Les publications sur les travaux cités dans la description :

— N. Lynch, R. Segala and F. Vaandrager. Hybrid I/O Automata, Information and Computation 185, pp. 105-157, 2003.
— A. Platzer. Logical Foundations of Cyber-Physical Systems, Springer, 2018.
— J. de Bakker and E. de Vink. Control Flow Semantics, MIT Press, 1996.
— M.S. Branicky, V.S. Borkar and S.K. Mitter. A Unified Framework for Hybrid Control: Model and Optimal Control Theory, IEEE Trans. on Automatic Control, 43, 1, janvier 1998, pp. 31–45.

Profil de l'étudiant recherché

De formation informatique, la personne recrutée devra avoir d'excellentes compétences dans le domaine de la conception des langages et de la sémantique formelle des langages. Une bonne connaissance en mathématiques des systèmes dynamiques ainsi qu'en automatique et contrôle sera un plus.

English version

Cyber-physical control systems (CPCS) integrate in a tight cooperation digital devices (computers, embedded chips, *etc.*) with physical processes, which they supervise and actuate in a control loop. With the emergence of the digital society, CPCS have gain a crucial importance as a key technology in a large number of applications : transportation, energy, health, industry 4.0, inteliigent building and cities, robotics, *etc.* However, CPCS are well-known to be very hard to specify, develop, test, verify, validate and evolve. This Ph.D. will take place within a larger project aiming at the design and implementation of a component-based language as well as a software engineering

methodology targeting the modular programming of CPCS which favors both the correctness by construction and the reusability of components and their assemblies.

The approach that will be more specifically developed consists in integrating within the component model a composable formal specification of their behavior and the one of their physical environment in the form of stochastic hybrid automata and their translation into modular composable simulation models. Hence, a complete system including its specificaiton, its software and the means to test, verify and validate it, will be obtained through the parallel composition of the individual hybrid automata, software and simulation models of the cyber-physical components. This approach must allow to develop a software engineering methodology covering the whole software development process from initial requirement elicitation to the dynamic adaptation of the system, through specificaiton, programming, testing, verifying, validating, self-configuration at deployment time as well as static and run-time machine learning and run-time self-adaptation.

In this Ph.D., the objective will more precisely attack the modeling language based on stochastic hybrid automata. The component model for CPCS that we are designing must integrate in its language the capability to jointly express the software and the behavioral models based on hybrid automata. The aim of the thesis will be to design the part of this language that will define the behavioral models of the component. We propose to start from two lines of previous work :

1. The work of Nancy Lynch and her team on hybrid automata called Hybrid Input/Output Automata (HIOA), known for their ability to composably model discrete and continuous aspects within the stochastic hybrid systems approach.
2. The work of Platzer on a language able to express more precisely the continuous aspects of stochastic hybrid systems and which his equipped with a formal semantics along a logical approach.

These two lines of work are indeed very interesting but insufficient to fully address our goals. Our wider goal is to be able to actually use these models in the software development process to jointly execute the code of the components and the simulation models of the physical part to help in the testting, the verficaiton, the validation, *etc.* To this end, the modeling language must be quipped with an execution semantics that will enable the automatic generation of simulation models by defining precisely the way code execution and behavioral models must interact over time. To corectly capture this, we propose to adtop a denotational semantics approach not based on traditional Scott domains but rather on Bnach spaces, as illustrated in the work of de Bakker and de Vink, to better attack the continuous part of the semantics.

As a proof of concept, the designed and formalised language will be used to model a cyber-physical control system aiming at dynamically managing the balance between consumption and production of energy in an semi-autonomous home, which can produce its own energy with renewables but also call upon the distribution network to cover consumption peaks. In this application, stochastic hybrid systems will be used to model the consumption of appliances (refrigerators, oven, washing machine, *etc.*) but also the production of solar panels and wind turbines.

Applicants profile

Having a master or an engineering degree in computer science, the applicants must have strong knowledge and skills in coputer language design and semantics, especially with denotational semantics. Knowledge of mathematics of dynamical systems as well as automatic control would strengthen the application.