Développement de CPS, correct-par-construction, en combinant des modèles SysML, des connecteurs de coordination REO, et des approches formelles : application au domaine médical

Encadrants: Samir Chouali(schouali@femto-st.fr), Ahmed Hammad(ahammad@femto-st.fr)
Établissement d'accueil: Département DISC de l'institut Femto-St, UMR CNRS 6174, université de Franche-Comté, Montbéliard.

Mots-Clés : Systèmes Cyber-Physiques, E-santé, composants, génie logiciel, SysML, REO, coordination, systèmes hybrides, conception par contrats, exigences, traçabilité, vérification formelle, simulation.

1 Contexte

Cette thèse se place dans le cadre de la conception des systèmes Cyber-Physiques (Cyber-Physical Systems, CPS) critiques. Ces dernières années, les CPS deviennent de plus en plus complexes, car ils se composent de plusieurs composants logiciels et matériels, provenant de fournisseurs différents, qui doivent fonctionner en harmonie avec un environnement physique incertain. En outre, ils sont généralement déployés dans des domaines critiques tels que : l'e-santé, la domotique et les bâtiments intelligents, la robotique autonome, les véhicules connectés autonomes...En raison de leur criticité, la sûreté de fonctionnement des CPS doit donc être garantie lors de l'étape de conception. Toutefois leur nature complexe (interactions complexes entre composants matériels et logiciels d'où des difficultés de coordination, comportements avec des contraintes temporelles et probabilistes,...) pose des problématiques tant au niveau modélisation qu'au niveau vérification. Ainsi des questions concernant la conception et le développement des CPS restent posées : quel langage semi-formel utiliser pour capturer l'ensemble des facettes d'un CPS et leurs contraintes inhérentes ? Comment formaliser et coordonner l'ensemble des interactions entre les entités logicielles et matérielles ? Comment garantir l'interopérabilité de l'ensemble des entités hétérogènes composant un CPS ? Quelles approches exploiter pour vérifier les exigences définies au niveau semi-formel ?...

2 Objectifs

L'objectif de cette thèse est de définir et de mettre en œuvre une nouvelle méthodologie de modélisation et de vérification formelle des CPS critiques qui s'appuie, d'une part sur le formalisme SysML [11] comme un langage pivot de modélisation, enrichi par les primitives de coordination REO [7], et d'autre part sur le formalisme des contrats comportementaux des composants [10] (l'une de nos contributions dans le domaine des composants), pour vérifier formellement des propriétés sur les CPS. Quelques travaux [2, 3, 4] ont été proposés dans ce domaine, mais aucun ne propose une approche complète exploitant SysML, comme langage de modélisation, REO, comme langage de coordination, et les contrats comportementaux des composants, en vue de garantir la sûreté de fonctionnement des CPS.

Au niveau modélisation, il serait intéressant de s'inspirer du travail présenté dans [1], qui propose une approche de modélisation basée sur les langages SysML/MARTE/pCCSL pour capturer les différents aspects d'un CPS tels que : la structure, le comportement, les contraintes temporelles et probabilistes, et les propriétés non fonctionnelles. Une première contribution par rapport à ce travail serait de considérer, en plus, le diagramme des exigences SysML (qui n'est pas pris en compte), en vue de l'exploiter pour la vérification des propriétés et de considérer la traçabilité des exigences lors du processus du développement.

Pour spécifier les interactions exogènes complexes entre les différents composants d'un CPS, et coordonner ainsi l'échange de leurs messages et données, il serait intéressant d'exploiter le langage de REO [7] (développé par l'équipe méthodes formelles du Professeur Arbab du centre de recherche CWI d'Amsterdam) qui offre un ensemble de connecteurs permettant de construire des protocoles de coordination complexes pour les systèmes concurrents. En outre, les connecteurs REO ont une représentation graphique, ce qui va nous permettre d'enrichir les notations SysML pour modéliser les CPS, et une sémantique formelle qui pourra être exploitée lors de la vérification.

Au niveau vérification, nous projetons d'étendre notre travail présenté dans [10], concernant les contrats comportementaux des composants orientés objet, pour prendre en compte tous les aspects des CPS (temporels, probabilistes,...). Il faudrait ensuite définir un cadre formel pour vérifier l'interopérabilité des composants dans un CPS. Et pour vérifier les exigences SysML et étudier l'impact de leur évolution sur l'ensemble du système, il faudrait considérer le protocole de coordination entre les différents composants défini avec REO et proposer une approche de vérification en considérant la sémantique formelle des connecteurs REO dans le cadre des CPS (définie par exemple avec les automates à contraintes temporisés et probabilistes [3]), ainsi que celle des exigences. Un premier travail [8, 9] dans ce contexte a été réalisé dans le cadre de notre collaboration avec l'équipe méthodes formelles du centre de recherche CWI (Amsterdam, Pays-Bas). Il serait donc intéressant de l'étendre pour prendre en considération les aspects temporelles et stochastiques des CPS. Ainsi, une approche combinant de la vérification par Model-Checking et de la simulation, pourrait être proposée pour prendre en considération les comportements continues et discrets d'un CPS. Donc, une continuité de collaboration avec le CWI pourrait être envisagée dans le cadre de cette thèse.

Enfin, il serait intéressant d'étudier la faisabilité de l'approche et de montrer la construction correcte des CPS, de la conception à l'implémentation, en proposant une implémentation des contrats des composants avec le langage ADA et son extension SPARK [15], utilisée pour la vérification formelle. En effet, SPARK est une extension du langage ADA avec des annotations formelles basées sur les contrats (donc plus appropriée pour implémenter les contrats des composants), qui sont considérées lors de la vérification.

2.1 Domaine d'application

Nous proposons d'orienter ces travaux dans le domaine médical. Ce choix est motivé par le fait que nous sommes impliqués dans le montage d'un projet recherche PHC Tassili Franco-Algérien 2022, qui porte sur la spécification et le développement d'un système cyber-physique médical, centré sur les lits hospitaliers connectés et intelligents.

3 Profil du candidat

Diplôme : Master 2 (ou diplôme d'ingénieur) en informatique.
Compétences :

- Connaissances en ingénierie dirigée par les modèles : modélisation avec UML/SySML, transformation de modèles...
- Connaissances des méthodes formelles.
- Compétences en programmation.
- Capacité de communication écrite et orale en anglais.

4 Candidature

Pour candidater, merci d'envoyer un CV, une lettre de motivation, les relevés de notes du Master, des lettres de recommandation (ou les coordonnées d'une ou deux personnes à contacter pour vous recommander).

Références

[1] Ping Huang, Kaiqiang Jiang, Chunlin Guan, Dehui Du: Towards Modeling Cyber-Physical Systems with SysML/MARTE/pCCSL. COMPSAC (1) 2018: 264-269.

[2] Taussef Rana, Yawar Abbas Bangash and Haider Abbas. Flow Constraint Language for Coordination by Exogenous Connectors. IEEE Access 7:138341-138352 (2019).

[3] Kangli He, Holger Hermanns, Yixiang Chen: Models of Connected Things: On Priced Probabilistic Timed Reo. COMPSAC (1) 2017: 234-243.

[4] Kangli He, Holger Hermanns, Hengyang Wu, Yixiang Chen: Connection models for the Internet-of-Things. Frontiers Comput. Sci. 14(3): 143401 (2020).

[5] OMG Systems Modeling Language (OMG SysMLTM). Tech. Rep. Version 1.4, Object Management Group (September 2015), http://www.omg.org/spec/SysML/1.4/.

[6] Derler, P., Lee, E.A., Sangiovanni-Vincentelli, A.: Modeling Cyber-Physical Systems. Proceedings of the IEEE (special issue on CPS) 100(1), 13 - 28 (January 2012).

[7] Farhad Arbab. Reo : A channel-based coordination model for component composition. Mathematical. Structures in Comp. Sci., 14(3) :329-366, June 2004.

[8] Benjamin Lion, Samir Chouali, and Farhad Arbab. Compiling protocols to promela and verifying their LTL properties. In Proceedings of MODELS 2018 Workshops Copenhagen, Denmark, October, 14, 2018, pages 31-39.

[9] Benjamin Lion, Samir Chouali, and Farhad Arbab. Compiling synchronous protocols to asynchronous promela programs for ltl properties verification. Technical report, DISC department, FEMTO-ST Institute, UMR CNRS 6174, 2021. to be submitted for publication.

[10] Sebti Mouelhi, Khalid Agrou, Samir Chouali, Hassan Mountassir: Object-Oriented Component-Based Design using Behavioral Contracts: Application to Railway Systems. CBSE 2015: 49-58.

[11] Bouaziz Hamida, Chouali Samir, Hammad Ahmed and Mountassir Hassan, "SysML Model-Driven Approach to Verify Blocks Compatibility", International Journal of Computer Aided Engineering and Technology (IJCAET), vol. 11, 2, pp. 206-231, 2019.

[12] Wang, B., Baras, J.S.: HybridSim: A Modeling and Co-simulation Toolchain for Cyberphysical Systems. In: 17th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications, DS-RT 2013, Delft, The Netherlands, October 30?November 1, 2013. pp. 33-40. IEEE Computer Society (2013).

[13] Evgeny Kusmenko, Alexander Roth, Bernhard Rumpe, Michael von Wenckstern: Modeling Architectures of Cyber-Physical Systems. ECMFA 2017: 34-50.

[14] Larsen, Peter Gorm, Fitzgerald, John, Woodcock, Jim orcid.org/0000-0001-7955-2702 et al. (3 more authors). Towards Semantically Integrated Models and Tools for Cyber-Physical Systems Design. In: 7th International Symposium on Leveraging Applications of Formal Methods, Verification, and Validation. pp. 171-186,2016.

[15] AdaCore. SPARK 2014 reference manual, 2014.