Conception compositionnelle de dispositifs biomédicaux portables certifiables

Résumé

Les dispositifs biomédicaux combinent parties analogiques tels que capteurs et actuateurs avec un contrôle numérique et le logiciel applicatif. La tolérance aux pannes et la performance sont d'une importance cruciale. La conception de ces systèmes nécessite l'intégration d'un grand nombre de composants issus de différentes disciplines. Ceci rend extrêmement difficile la tâche de trouver des garanties de performance, sûreté et sécurité. Nous investigons la compositionnalité comme façon de maîtriser la complexité et l'hétérogénéité en nous focalisant sur la combinaison de deux aspects : premièrement, des stratégies de conception et de modélisation et deuxièmement, la vérification. Le but de ce projet de recherche doctoral est donc de proposer une méthodologie de conception de ces dispositifs médicaux intégrant tous ces aspects.

1 Contexte

Les dispositifs biomédicaux sont nombreux sur le marché et couvrent un large éventail entre accessoires sportifs et de bien-être et dispositifs destinés aux usages médicaux encadrés par des professionnels de santé. Ces dispositifs doivent remplir des règles de certification fixés par l'Agence Nationale de Sécurité du Médicament et des produits de santé (ANSM, [ANS19]), tandis que pour les dispositifs dits "de bien-être", le but est simplement d'obtenir des garanties de bon fonctionnement. Tous sont composés de parties analogiques (notamment les capteurs), numériques et logicielles, et sont soumis à de fortes contraintes physiques (poids, étanchéité, résistance à la chaleur/au froid). Cette combinaison d'aspects électroniques, informatiques, biologiques, optiques, thermiques, mécaniques, et acoustiques justifie de les classer parmi les systèmes *multi-physiques*. Portables, ils dépendent de communications sans fils, par exemple WIFI et Bluetooth, soit pour assurer la communication entre un capteur et un dispositif portable, soit entre le dispositif portable et une station statique.

Aussi, il est souhaitable que ces connexions garantissent une très bonne confidentialité des échanges, tandis qu'en règle générale elle n'est pas garantie, ni du point de vue de l'authenticité ni de l'intégrité comme le constate l'Agence nationale de la sécurité des systèmes d'information [SSI19]. L'autonomie est un autre critère essentiel : le poids, l'encombrement et la consommation d'énergie doivent être réduits. Enfin, le coût doit être limité en raison de la charge pour la sécurité sociale ou pour attaquer un marché de masse (sport/bien-être).

1.1 Bases

L'ingénierie dirigée par les modèles (*MDE, Model-Driven Engineering*) est très répandue dans l'industrie lors des premières étapes de la conception et d'exploration de systèmes embarqués et, plus récemment, d'objets connectés. Pour ces dispositifs, l'on souhaite identifier un processus de conception encore plus rapide (*time-to-market*). Le MDE est progressivement en train de s'étendre aux systèmes multi-physiques, mais les approches sont actuellement divergentes et peinent à intégrer les différents modèles de calcul (*Model of Computation, MoC*), comme le montre [Tri16]. SystemC-AMS [BCD+10] s'est établi comme quasi-standard pour la modélisation de systèmes multi-physiques ; les équipes ALSOC et CIAN du LIP6 participent activement à sa standardisation et sont impliquées dans la recherche. Un environnement de conception et de simulation commun permettant de gérer la multi-disciplinarité a été proposé [BA17, AMV+15].

1.2 Projets connexes

Plusieurs projets menés dans nos équipes ont préparé le terrain ; un détecteur d'endormissement portable a été développé, un détecteur de crampes musculaires est en développement, les deux en coopération avec l'Institut de Cardiométabolisme et de la Nutrition (ICAN [1]).

1. www.ican-institute.org

Une étude de cas d'envergure sous la forme d'une modélisation haut-niveau d'un capteur échographique [GBAC20] est développée dans le cadre du projet EchOpen [com17]. La communauté à la base de ce projet, qui revendique le matériel et logiciel libre, réunit médecins, physiciens experts d'ultrason, concepteurs matériels et niveau système. Elle a pour but de concevoir un dispositif d'échographie portable à bas coût pour des diagnostics préliminaires (on parle d'echo-stéthoscopie [TLL14]), en première intention destiné aux médecins des pays en voie de développement pratiquants dans des conditions difficiles.

2 Objectifs

Si l'on considère des critères physiques multiples, l'exploration de l'espace de conception est un défi important. Pour les systèmes mentionnés ci-dessus, il est nécessaire de garantir les caractéristiques suivantes lors de l'exploration :

- Afin d'assurer la minimisation du coût du système final, et notamment celui de la partie électronique numérique, il faut identifier de nouveaux moyens pour explorer : modéliser et simuler, à différents niveaux d'abstraction, les architectures matérielles-logicielles.
- Afin d'obtenir la certification à terme, des moyens de vérifier, de manière formelle, la sûreté du système matériel-logiciel.
- Afin d'assurer que la confidentialité, l'authenticité et l'intégrité des données médicales, des moyens de garantir la sécurité des communications, en particulier celles sans fil.

Pour atteindre ces objectifs, en termes de sûreté, de sécurité, d'autonomie et de bas coût, nous proposons d'intégrer des outils et méthodes jusque-là séparés.
Nous proposons de construire un environnement en mode libre basé sur des méthodes de MDE, des techniques de co-simulation analogique/numérique/logiciel et de vérification formelle, en utilisant des techniques **compositionnelles** d'abstraction et de décomposition hiérarchique et ainsi de décomposer la complexité de manière hiérarchique en composants locaux et en analysant les dépendances entre eux. L'approche que nous souhaitons adopter devrait permettre de prendre en considération de multiples domaines (biologie, mécanique, ...).

Pour cela, plusieurs aspects doivent être traités :

- **Dépendances entre Modèles de calcul** Composants analogique et numériques ne suivent pas le même MoC. Des problèmes de causalité temporelle surgissent pour lesquels des solutions basées sur SystemC-AMS ont été développées dans le passé au sein de nos équipes [AMV+15]. Dans une thèse de fin d'études (master's thesis) encadrée par Daniela Genius, commune avec l'université de Kaiserslautern, nous avons proposé des techniques de co-simulation basées sur SystemC et SystemC-AMS prenant en compte les problèmes de causalité dès les premières étapes de la conception [CP18, CGA21].
- **Vérification formelle** Tandis qu'il est très difficile de vérifier une plate-forme matérielle System-sur-puce complète au niveau cycle — on peut espérer vérifier des sous-parties comme le montre les travaux d'autres membres de l'équipe ALSOC [BE06] — Nous comptons donc explorer la compositionnalité entre méthodes de vérification pour le matériel et le logiciel.
- **Intégration des spécificités des applications biomédicales** Afin de prendre en compte la spécificité des dispositifs biomédicaux, qui ont une forte proportion de traitement du signal (images echographiques, sous-échantillonnage...), il est nécessaire de modéliser très précisément des signaux et des types de donnée variés (flottants, point fixe, vecteur de bit, ...).
- **Validation** Nous prévoyons de construire au fur et à mesure une bibliothèque de modèles de capteurs standards recombinables entre eux (gyroscope, flex sensor, ...), des microcontrôleurs (ESP, Arduino, ...), à constituer cela dit à modéliser au niveau SysML, et d'appliquer des transformations de modèles selon la méthode compositionnelle à définir. La méthode sera validée en allant jusqu'à un prototype sur FPGA – ce dernier point sera abordé dans plusieurs projets d'étudiants de Master en collaboration avec le doctorant/la doctorante.

Concernant la mise en œuvre, nous disposons d'un outil de modélisation et vérification de systèmes embarqués à plusieurs niveaux d'abstraction, des modèles UML/SysML à un prototypage cycle-bit près utilisant des modèles SystemC/SystemC-AMS générés. TTool [Apv] est un outil en mode libre de conception et prototypage virtuel de systèmes embarqués, auquel l'encadrante ALSOC contribue depuis 2013. Elle a récemment ajouté un volet de modélisation et co-simulation de systèmes analogiques/numériques [GCAP19].

Un point fort de TTool est sa capacité de vérification formelle des aspects de sûreté — basée sur UPPAAL et un model-checker interne — et des aspects de sécurité basés sur ProVerif. Il permet d'ailleurs de modéliser le niveau de sécurité des canaux de communication [AR15].

3 Profils souhaités

Titulaire d'un master en informatique ou électronique ou diplôme équivalent, le candidat/la candidate devra disposer de solides compétences en architectures multiprocesseurs et en modélisation de systèmes. La maîtrise ou une expérience préalable dans l'un ou l'autre de ces domaines sera appréciée : langage SystemC, MDE, vérification formelle, objets connectés, informatique biomédicale.

4 Cadre

La thèse se déroulera au sein des équipes ALSOC et CIAN du LIP6 (laboratoire d'informatique de Sorbonne Université), encadrée par Daniela Genius et sous la direction de Roselyne Chotin. Des interactions avec des partenaires français (Télécom Paris, SupAéro), étrangers (Kaiserlautern en première ligne), du domaine médical (ICAN, EchOpen, ...) sont envisagées au cours des travaux de cette thèse.

5 Bibliographie

Références

[AMV+15] Liliana Andrade, Torsten Maehne, Alain Vachoux, Cédric Ben Aoun, François Pêcheux, and Marie-Minerve Louërat. Pre-simulation symbolic analysis of synchronization issues between discrete event and timed data flow models of computation. In Wolfgang Nebel and David Atienza, editors, *DATE*, pages 1671–1676. ACM, 2015.

[ANS19] ANSM. Certification dispositif médical, 2019.

[Apv] Ludovic Apvrille. TTool. In *https ://gitlab.telecom-paristech.fr/mbe-tools/TTool.*

[AR15] L. Apvrille and Y. Roudier. SysML-Sec : A model driven approach for designing safe and secure systems. In *3rd International Conference on Model-Driven Engineering and Software Development, Special session on Security and Privacy in Model Based Engineering*, France, February 2015. SCITEPRESS Digital Library.

[BA17] C. Ben Aoun. *Principes et réalisation d'un environnement de prototypage virtuel de systèmes hétérogènes composables.* PhD thesis, Université Pierre et Marie Curie, 2017.

[BCD+10] Martin Barnasconi, Christoph Grimm, Markus Damm, Karsten Einwich, Marie-Minerve Louërat, Torsten Maehne, François Pecheux, and Alain Vachoux. *SystemC AMS extensions Users Guide, Version 1.0.* Accellera systems initiative, March 2010.

[BE06] Cécile Braunstein and Emmanuelle Encrenaz. Formalizing the incremental design and verification process of a pipelined protocol converter. In *Seventeenth IEEE International Workshop on Rapid System Prototyping (RSP'06)*, pages 103–109. IEEE, 2006.

[CGA21] Cortés Porto, Rodrigo, Genius, Daniela, and Apvrille, Ludovic. Handling causality and schedulability when designing and prototyping cyber-physical systems. *Software and Systems Modeling*, pages 1–17, 2021.

[com17] EchOpen community. Designing an open-source and low-cost echo-stethoscope. http ://www.echopen.org/, 2017.

[CP18] R. Cortés Porto. Integration of SystemC-AMS simulation platforms into TTool. Master's thesis, Technische Universität Kaiserslautern, 2018.

[GBAC20] Genius, Daniela, Bournias, Ilias, Apvrille, Ludovic, and Chotin, Roselyne. High-level partitioning and design space exploration for cyber physical systems. In *MODELSWARD*, 2020.

[GCAP19] Genius, Daniela, Cortés Porto, Rodrigo, Apvrille, Ludovic, and Pêcheux, François. A tool for high-level modeling of analog/mixed signal embedded systems. In *MODELSWARD*, 2019.

[SSI19] SSI. recommandations de securite relatives aux reseaux wifi, 2019.

[TLL14] Ka Hei Tse, Wing Hang Luk, and Mau Chu Lam. Pocket-sized versus standard ultrasound machines in abdominal imaging. *Singapore medical journal*, 55(6) :325, 2014.

[Tri16] Stavros Tripakis. Compositional model-based system design and other foundations for mastering change. In *Transactions on Foundations for Mastering Change I*, pages 113–129. Springer, 2016.