Programme Doctoral DGA-INRIA – Sujet de Thèse

Méthodes formelles pour la modélisation d'architectures et d'infrastructures

INTRODUCTION

Un modèle d'architecture est un artefact de conception au croisement de plusieurs points de vue dans la conception d'un système: il décrit des logiciels, embarqués sur une architecture matérielle, connecté à l'environnement physique au moyen de capteurs et d'actuateurs et à d'autres systèmes au moyen de support de communication. Le temps se perçoit de manière différente, et supporte donc différentes représentations, qu'on observe son écoulement d'un point de vue ou de l'autre: il est discret et événementiel dans le logiciel, discret et temporisé dans le matériel, continu en physique.

De plus, les langages de modélisation et de programmation qu'on utilise usuellement pour spécifier les composants logiciels, matériels et physiques d'un système altèrent significativement cette perception du temps. Habituellement, la représentation, le calcul, la mesure du temps est spécifique à la résolution d'un problème de conception particulier: la simulation, le profilage, l'analyse de performances, d'ordonnançabilité, la parallélisation, ou le prototypage virtuel.

CONTEXTE

Le but du projet TEA (temps, événements et architectures) est de définir un cadre sémantique permettant de raisonner globalement sur le temps dans les systèmes puis de mettre en pratique ces résultats en revisitant l'état de l'art en analyse, en vérification et en synthèse, mettant à profit la compositionalité obtenue. En particulier, le projet TEA défend la standardisation d'une annexe comportementale au standard SAE AADL (« architecture analysis design standard »), fondé sur le modèle de calcul et de communication synchrone de l'environnement Polychrony (Eclipse project POP du consortium Polarsys).

SUJET

S'agissant plus généralement d'infrastructures, de systèmes de systèmes, le standard NAF (« NATO architecture framework ») permet semblablement de représenter des infrastructures et réseaux selon différents points de vue d'analyse et de simulation (concepts, services, logique, physique). Mettant à profit notre expérience pour le support à l'analyse de modèles AADL pour la co-simulation, l'orchestration, l'ordonnancement, la vérification, l'objectif de cette thèse sera de définir un modèle de calcul formel d'un ou plusieurs points de vue du modèle NAF afin de supporter la vérification formelle et la synthèse de simulateurs selon les points de vue considérés.

PROGRAMME

Pour cela, nous pourrons nous intéresser au modèles de calcul flot-de-donnée en général (synchrones, asynchrones, temporisés, stochastiques), aux outils algébriques permettant leur composition et leur vérifications (notions d'interfaces, de contrats, raisonnement hypothèse/garantie), et mettre en œuvre les méthodes d'analyse spécifiques à chaque point de vue à vérifier.
Notre méthodologie de travail consistera en la sélection de plusieurs points de vue (« viewpoints ») du standard NAF chacun sujet d'une étude de cas, possiblement anonyme ou public (« open-source »). Pour chaque point de vue considéré, nous procèderons tout d'abord par l'élaboration d'un modèle de calcul et de communication (modèle de concurrence, analytique, temporisé, quantitatif, stochastique) reflétant au mieux les exigences et spécifications du standard et leur utilisation, leur pouvoir d'expression, exprimé dans l'étude de cas. Nous associerons la formalisation de ce point de vue à un outil existant, ou une évolution prototypique de cet outil, la mieux adaptée à la mise en œuvre du problème à résoudre (simulation, analyse, vérification). Enfin, nous validerons la solution proposée par son expérimentation sur l'étude de cas.

REFERENCES

Architecture Analysis and Design Standard http://www.aadl.info
Nato Architecture Framework http://nafdocs.org
Project POP http://www.eclipse.org/proposals/polarsys.polychrony
Jean-Pierre Talpin http://www.irisa.fr/prive/talpin

BIBLIOGRAPHIE

"Logically timed specifications in the AADL : a synchronous model of computation and communication (recommendations to the SAE committee on AADL)". L. Besnard, E. Borde, P. Dissaux, T. Gautier, P. Le Guernic, J.-P. Talpin. INRIA Technical Report n.446, 2014.

"Timed behavioural modelling and affine scheduling of embedded software architectures in the AADL using Polychrony". L. Besnard, A. Bouakaz, T. Gautier, P. Le Guernic, Y. Ma, J.-P. Talpin, H. Yu. In Science of Computer Programming (SCP). Elsevier, 2014.

"Polychronous modeling, analysis, verification and simulation for timed software architectures". H. Yu, Y. Ma, T. Gautier, L. Besnard, P. Le Guernic, J.-P. Talpin. In Journal of Systems Architecture (JSA). Elsevier, 2013.

"System-level co-simulation of integrated avionics using polychrony". Yu, H., Ma, Y., Glouche, Y., Talpin, J.-P., Besnard, L., Gautier, T., Le Guernic, P., Toom, A., and Laurent, O. ACM Symposium on Applied Computing (SAC'11). ACM, 2011.