Points de vue et sémantiques ad hoc

Frédéric Boniol[1], **Philippe Dhaussy**[2], **Claire Pagetti**[3]

[1] *ENSEEIHT - 2 rue C. Camichel 31071 Toulouse*
[2] *ENSIETA - DTN - 2 rue F. Verny 29806 Brest*
[3] *ONERA-CERT - 2 av. E. Belin 31055 Toulouse*
boniol@enseeiht.fr, dhaussy@ensieta.fr, pagetti@cert.fr

RÉSUMÉ. *La conception des systèmes embarqués (de plus en plus complexes, critiques, et désormais à logiciels prépondérants) nécessite le concours de plusieurs équipes spécialisées dans des domaines différents (sûreté de fonctionnement, conception de plateforme d'exécution . . .). Toutes ces équipes ne peuvent avoir chacune qu'un "point de vue" partiel du système qu'elles doivent pourtant concourir à spécifier, réaliser, et tester. Cette notion de point de vue est par conséquent centrale lorsque l'on cherche à dessiner les contours d'une ingénierie des modèles pour les systèmes embarqués. Se pose alors la question de la définition de ces points de vue, et notamment de leur sémantique et leur cohérence. Ce court article se propose d'entamer une réflexion sur cette question, en montrant que l'ingénierie des modèles, en découplant les notions de syntaxe et de sémantique dans les approches par méta modélisation, ouvre une voie potentiellement intéressante pour la notion de point de vue.*

ABSTRACT. *Designing embedded systems, (more and more complex, critical, software intensive and often interacting with a disturbing environment), involve several highly domain-specialized teams (safety, execution platform. . .) collaborating together. Each of those teams can only have a partial, restricted "point of view" on the system it contributes to build. The goal of this short article is to identify the notion of viewpoint, and to show that this notion is central when dealing with embedded systems. It proposes then a reflexion on the viewpoint semantics by showing that the model engineering approach, by separating syntax and semantics, give an interesting way for viewpoints définition.*

MOTS-CLÉS : *Point de vue, système embarqué, sémantique*

KEYWORDS: *Point of view, embedded system, semantics*

1. Introduction à la conception multi points de vue

Le contexte des systèmes embarqués. Les systèmes informatiques embarqués connaissent depuis plusieurs années un essor considérable dans tous les domaines : automobile, aéronautique, espace, contrôle industriel, télécommunications.... L'appel à l'informatique dans l'ensemble de ces domaines a tendance à se généraliser avec les progrès constants des équipements numériques. Pour autant, ces systèmes informatiques embarqués ne peuvent pas être assimilés à des systèmes informatiques généraux. D'une part, ils sont souvent soumis à des contraintes strictes imposées par leur environnement (résistance aux vibrations, aux variations importantes de températures, ...). Et d'autre part, en raison même de ces contraintes, ils répondent fréquemment à des caractéristiques particulières qui en rendent l'analyse à la fois plus spécifique et plus pointue.

Un système embarqué est avant tout un système réactif dont la fonction est de contrôler l'évolution de son environnement. A titre d'exemple, un pilote automatique est un système embarqué chargé de guider un avion conformément à un plan de vol défini par l'équipage. Pour assurer un bon fonctionnement, les trois critères suivants doivent être assurés :

– la *réactivité* : si l'environnement présente un comportement changeant ou de type événementiel, il est nécessaire que le système informatique soit capable de s'adapter à ces *rafales* d'événements en mettant en œuvre des calculs et des communications également événementiels ;

– le respect des contraintes *temps réel* : si l'environnement est dynamique, voire instable, alors le système de contrôle informatique est soumis à des exigences de temps de réponse portant sur les délais introduits par le système informatique entre des stimuli et des actions correspondantes ;

– la *criticité* si les défaillances sont catastrophiques, alors le système de contrôle informatique doit satisfaire des contraintes de sûreté de fonctionnement.

Un passage obligé : la notion de point de vue. Ces critères impliquent des activités de validation souvent essentielles qui se traduisent en pratique par la définition de modèles de vérification pour chacun des points de vue critiques du système : un modèle fonctionnel décrivant le comportement fonctionnel et nominal du système, un modèle de tolérance aux défaillances explicitant les comportements en cas de pannes, un modèle d'évaluation de performances permettant de calculer les latences, charges, débits et autres caractéristiques temps réel, des modèles de robustesse aux perturbations mécaniques, électromagnétiques... Chacun de ces modèles est un modèle spécialisé du système étudié, orienté selon un point de vue spécifique tout en abstrayant les autres points de vue.

Cette approche par point de vue présente l'avantage considérable d'offrir un moyen naturel de casser la complexité intrinsèque à la validation d'un système en découpant cette tâche (de validation) selon un ensemble de préoccupations transverses. La définition d'une ingénierie de modèles de *points de vue* apparaît alors comme un besoin

central de la question de la vérification des systèmes embarqués, voire même un passage obligé dans le cas de systèmes complexes.

Les approches naturelles : les démarches multi modèles. Plusieurs solutions, partielles ont été proposées par le passé. P. Kruchten [KRU 95] a été un des premiers à présenter un modèle d'architecture de systèmes logiciels reposant sur l'utilisation de vues afin de traiter séparément les préoccupations des différents intervenants et de capturer séparément les exigences fonctionnelles et non-fonctionnelles.

Dans le domaine des systèmes logiciels, le cadre UML peut apparaître comme une tentative multi modèles ou multi formalismes pour la définition et la validation (informelle) de systèmes complexes.

Dans le contexte de l'ingénierie des systèmes avioniques, [BON 01] décrit un système dans quatre domaines *métiers* (i.e., quatre points de vue) : fonctionnel, sûreté de fonctionnement, performances temps réel et résistance électromagnétique. Dans sa thèse, W. Theurer [THE 06] propose un cadre conceptuel multi points de vue. Il recommande l'utilisation de modèles pour chaque point de vue avec des parties publiques et privées permettant à l'intégrateur d'avoir, via les parties publiques, une vision globale du système.

On peut également citer les approches du domaine militaire telles que DoDAF (US Department of Defense Architecture Framework) ou MODAF (UK Ministry of Defence Architectural Framework) développées pour la spécification de systèmes d'armes complexes et reposant sur plusieurs dizaines de points de vue clairement identifiés.

Toute ces approches sont représentatives des pratiques industrielles utilisant bien souvent une grande variété de formalismes et de langages pour modéliser le système en conception ou en vérification sous l'ensemble de ses points de vue. Toutefois, si elles sont intéressantes parce qu'essayant de donner un sens à la notion de point de vue, ces approches se heurtent cependant à plusieurs difficultés majeures, sans réellement les résoudre, dont notamment le problème de la cohérence de ces points de vue.

Formalisation d'une approche multi points de vue. Formalisons le problème de l'ingénierie de la conception et de la vérification par point de vue. Soit un système S, soient un ensemble de modèles $\{M_i\}_{i=1,\ldots,n}$ de S décrits chacun dans un langage spécifique L_i, soient également φ_i les exigences devant être vérifiées par le système dans chacun des points de vue considérés. Notons $[\![M_i]\!]_{L_i}$ le comportement du modèle M_i selon la sémantique du formalisme L_i. Alors la question de la vérification du système S se ramène à n vérifications : $\forall i,\ [\![M_i]\!]_{L_i} \models \varphi_i$

La vérification dans chaque point de vue peut se faire par preuve, model checking, simulation ou tout autre technique mathématiquement fondée. Cependant, plusieurs problèmes apparaissent.

Problème 1 : les modèles M_i sont-ils conformes au système S ?

Problème 2 : est-il toujours possible de raffiner les exigences devant être satisfaites par le système S en exigences élémentaires propres à chaque point de vue (les exigences φ_i) ?

Problème 3 : les modèles M_i sont-ils cohérents entre eux ?

La première question n'est pas spécifique aux approches par points de vue, et est donc en dehors du champ de la réflexion. Nous écartons également, dans le cadre de cette réflexion, la deuxième question bien que centrale à la question des points de vue. En revanche, nous nous concentrons sur la troisième question : comment être sûr que les différents modèles M_i, et en particulier leur sémantique $[\![M_i]\!]_{L_i}$, représentent le même système. Ces modèles étant décrits dans des langages différents, souvent très éloignés les uns des autres, cette question n'a en général pas de solution, et constitue ainsi une limite difficile des approches multi modèles.

2. Une alternative : un découplage entre modèle et sémantiques

Une des origines du problème vient de l'utilisation de langages (les langages L_i) qui "embarquent" à la fois une syntaxe et une sémantique. Ces langages étant en effet spécifiques (parce que définis pour formaliser des points de vue spécifiques), ils reposent en conséquence sur des ensembles de concepts et de notations également spécifiques et leur attribuent un sens (la sémantique) précis. Cette spécificité d'un langage à l'autre, si elle est inévitable car concomitante à la notion de point de vue spécialisé, n'en demeure pas moins un obstacle à la confrontation des modèles et la vérification de la cohérence entre les points de vue.

Une approche différente consiste à voir les points de vue comme des interprétations sémantiques différentes d'un même modèle global et complet du système étudié. Cette idée repose sur l'intuition qu'un point de vue est une vue partielle du système, retenant et formalisant (en leur donnant un sens) les détails pertinents pour le point de vue considéré, et abstrayant les autres (détails).

2.1. *Le modèle global*

Un modèle global intégrant tous les comportements, les différentes architectures et propriétés n'est pas manipulable. En revanche, une description syntaxique d'éléments constituants le système est envisageable. Soit M ce modèle, il représente la description structurelle du système. Un point de vue sera alors construit comme un modèle structurel M_i sous ensemble de M (restreint aux éléments pertinents pour le point de vue i) et comme une interprétation sémantique $[\![M_i]\!]_{L_i}$ de ce modèle restreint, cette interprétation sémantique pouvant être construite par la projection de M_i dans un langage spécifique.

Cette idée n'est pas compatible avec l'approche classique des langages embarquant à la fois leur syntaxe (le modèle structurel) et leur sémantique (l'interprétation du modèle structurel). Elle devient en revanche possible dans le cadre de l'ingénierie

dirigée par le modèle offrant naturellement un découplage entre ces deux notions avec d'un coté des modèles structurels définis comme des instances de méta modèles et de l'autre une expression d'une ou plusieurs sémantiques par la définition de règles de transformation de modèles.

Un formalisme solution peut être AADL [FEI 03] car il permet la description des architectures matérielle et fonctionnelle, du mapping fonctionnel sur l'architecture ainsi que bon nombre d'annotations permises dans le champ *Properties*. Ces annotations serviront pour la construction des points de vue et pour maintenir la cohérence globale.

2.2. *Transformation de modèles : du modèle global aux points de vue et réciproquement*

La construction d'un point de vue à partir du modèle global peut se faire par des transformations de modèles [JéZ 06] vers un langage spécifique (par exemple Altarica pour la sûreté de fonctionnement, le formalisme des files d'attente pour l'évaluation de performances…), chaque langage spécifique embarquant quant à lui et à son niveau sa syntaxe et sa sémantique propres.

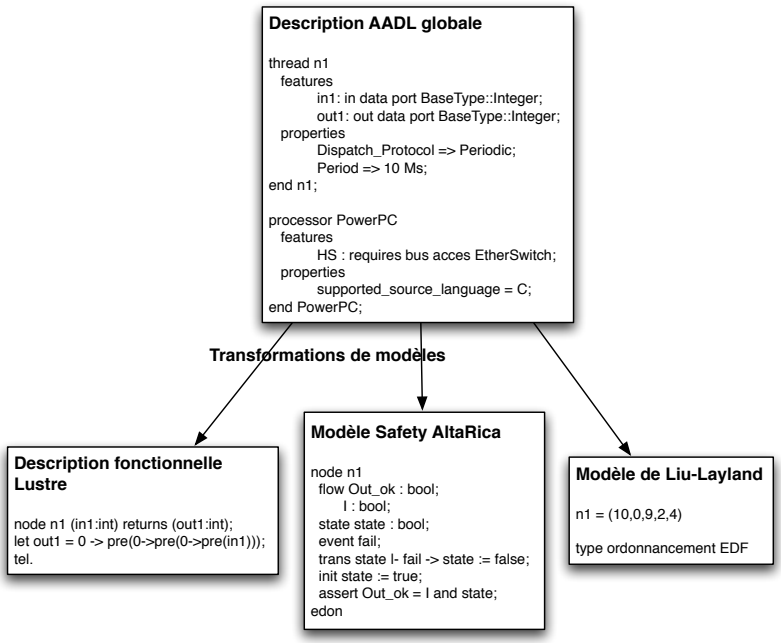

Figure 1. *Architecture d'un cadre multi vue*

Dans la figure 1, on illustre la mise en œuvre de l'approche. Une description AADL globale explicite les équipements, les moyens de communication, les différents processus et des annotations nécessaires aux points de vue. Un thread périodique n_1 est décrit par sa période et ses entrées sorties. Ce thread correspond à un nœud LUSTRE. A partir des threads du modèle global, le squelette des différents programmes peut être obtenu par transformation de modèles, et inversement la description des threads peut être générée à partir des spécifications fonctionnelles. Un processus AADL décrit la mise en relation de différents nœuds LUSTRE et donc se heurte à la question de l'ordonnancement, l'hypothèse synchrone étant irréaliste pour des tâches complexes et gourmandes en temps CPU. Un point de vue exécutif est alors nécessaire pour valider le mapping. Toujours dans la catégorie de l'évaluation de performance, un modèle de type file d'attente permettra la validation des temps d'exécution de bout en bout.

Pour assurer un niveau de safety, un modèle de propagation de pannes [KEH 04] doit être développé. AltaRica est un langage dédié à ces modèles. Dans la figure, on veut assurer que la fonction n_1 (implantée par le nœud n_1 et correspondant à la tâche temps réel n_1) est assurée à un certain taux (par exemple taux de défaillance $\leq 10^{-5}$ par heure de vol pour un avion). Un modèle du système est réalisé en AltaRica par transformation de modèle depuis la description globale AADL et enrichi par des propriétés spécifiques à la sûreté de fonctionnement. Dans la figure, la description AltaRica décrit les cas où la fonction est assurée : si la donnée d'entrée est correcte et si la fonction n_1 n'est pas défaillante. L'événement *fail* doit ensuite être décrit, il peut correspondre à la perte du CPU et du réseau de communication en sortie.

3. Conclusion et perspectives

La thèse, mise en débat suite à cette courte réflexion, est qu'une approche du type ingénierie des modèles, parce que découplant modèles et sémantiques, constitue un cadre naturel et adéquat pour la modélisation multi points de vue. L'idée est d'offrir

– des moyens d'expressions d'un modèle structurel global avec une sémantique minimale

– et des transformations de modèles, chaque transformation encodant en quelque sorte la sémantique d'un point de vue donné, et permettant la génération de squelette vers des langages dédiés aux points de vue.

Des travaux sont en cours pour décrire les transformations de modèles de la description globale vers les points de vue et réciproquement.

4. Bibliographie

[BON 01] BONIOL F., FOISSEAU J., WIELS V., « Un exemple de modèle conceptuel de référence pour le développement de systèmes avioniques », 2001, 2ème Conférence annuelle d'Ingénierie Système.

[FEI 03] FEILER P. H., LEWIS B., VESTAL S., « The SAE Architecture Analysis & Design Language (AADL) Standard : A Basis for Model-Based Architecture Driven Embedded Systems Engineering », *RTAS 2003 Worshop on Model-Driven Embedded Systems*, Washington, D.C., May 2003, IEEE.

[JéZ 06] JÉZÉQUEL J.-M., GÉRARD S., BAUDRY B., « *L'ingénierie dirigée par les modèles* », chapitre Le génie logiciel et l'IDM : une approche unificatrice par les modèles, Lavoisier, Hermes-science, 2006.

[KEH 04] KEHREN C., SEGUIN C., BIEBER P., CASTEL C., BOUGNOL C., HECKMANN J. P., METGE S., « Advanced simulation capabilities for multi-systems with AltaRica », *International System Safety Conference (ISSC)*, Providence RH USA, 2004.

[KRU 95] KRUCHTEN P., « Architectural Blueprints—The "4+1" View Model of Software Architecture », *IEEE Software*, vol. 12, n° 6, 1995, p. 42–50.

[THE 06] THEURER W., « Une méthodologie de modélisation multi-modèles distribuée par métier pour les sytème embarqués », PhD thesis, Supaéro, 2006.