Vérification d'architectures embarquées : un enjeu aux multiples facettes

Frédéric Boniol*

*IRIT-ENSEEIHT - Université de Toulouse
2 rue Charles Camichel - 31071 Toulouse cedex 7, France
frederic.boniol@enseeiht.fr
http://irit.enseeiht.fr/boniol/boniol.html

Il est désormais trivial de constater que les systèmes informatiques embarqués, tant dans le domaine des transports, de l'énergie, que de la domotique et des communication, occupent une place toujours grandissante. Autrefois cantonnés dans des fonctions non critiques, les ingénieurs n'hésitent plus à confier à ces systèmes des rôles vitaux (les commandes de vol d'un avion de transport par exemple).

Il est aussi une deuxième évidence, ou prétendue comme telle, souvent issue de la pragmatique des ingénieurs : la fragilité des systèmes augmente avec leur complexité et surtout avec leur intégration. C'est le syndrome des systèmes spatiaux « russes », réputés robustes parce que simples, comparés aux systèmes américains ou européens réputés performants car sophistiqués mais fragiles car complexes. Mythe ou réalité ? Force est d'admettre que les systèmes embarqués critiques étaient, jusqu'à présent, conçus selon le précepte de la simplicité. C'est notamment le cas des systèmes avioniques jusqu'à la gamme A330-A340. La vérification et la certification de ces systèmes pouvaient alors être réalisées élément par élément ou sous-système par sous-système, et surtout point de vue par point de vue.

Or, l'apparition de nouveaux besoins (par exemple l'embarquement de fonctions de gestion des pannes et de la maintenance), couplés aux exigences de réduction des coûts et du poids, conduit à l'accroissement de l'intégration des systèmes, et par suite à une plus grande dépendance entre fonctions et, plus grave, entre points de vue fonctionnels et non fonctionnels. Cette évolution, déjà forte dans les secteurs militaire et automobile, se généralise dans l'avionique civile avec l'A380. Les systèmes, de plus en plus interconnectés, sont désormais construits autour d'infrastructures embarquées partagées, matérielles et logicielles, mais aussi autour de systèmes d'informations disséminés dans tout l'avion. La vérification et la certification d'un tel entrelacement deviennent alors des tâches ardues, qui ne peuvent plus se contenter d'une modélisation / vérification séparée élément par et point de vue par point de vue. Le problème de la vérification globale d'une architecture embarquée est désormais posé comme un enjeu bloquant pour le développement des futurs systèmes critiques.

L'objectif de cette présentation est de poser ce problème et de montrer qu'il doit passer clairement par la définition d'une ingénierie des points de vue reposant sur un ensemble de modèle interconnectés. On se posera alors la question du type des modèles mis en jeu, de leur organisation, de leur sémantique et de leur niveau d'abstraction. Une solution émergente notamment peut consister en la définition d'un modèle central mais « squelettique » du système (modèle appelé parfois « pivot », par exemple modélisé en AADL) et la définition de modèles de point de vue (fonctionnel, temps réel, matériel, dysfoncitonnel…) comme des habillages cohérents de ce squelette. Se pose alors la question de la sémantique de ces modèles de pivot et de point de vue.