Villeurbanne, mardi 20 octobre 2015

Conception sûre d'architectures embarquées de contrôle commande

Emil Dumitrescu

Maître de conférences – INSA de Lyon – Laboratoire Ampère – Dpt Génie Industriel

21 avenue Jean Capelle
Bât Leonard de Vinci
69621 Villeurbanne Cedex
Tel 33 4 72 43 60 32
emil.dumitrescu@insa-lyon.fr

Mots clés : *systèmes embarqués, conception, spécification, méthodes formelles, contrôleurs discrets, simulation.*

Les systèmes embarqués mettent souvent en œuvre une logique de contrôle/commande discrète. Ils doivent généralement répondre à une contrainte de criticité, entraînant une exigence forte en matière de correction de la conception. Des techniques formelles ont été développées durant les trois dernières décennies et apportent de véritables garanties, permettant d'établir mathématiquement la correction d'un système. Un des principaux verrous dans l'application des méthodes formelles au sein de projets industriels est l'absence d'algorithmes capables d'effectuer efficacement la vérification lorsque la taille des systèmes à vérifier augmente. Les démarches basées sur les composants offrent la possibilité de maîtriser dans une certaine mesure cette complexité. Cependant, de telles démarches opèrent un « transfert de difficulté et de responsabilité » depuis la machine vers le concepteur, qui doit être capable de gérer manuellement des ensembles vastes de spécifications formelles.

Dans ce contexte, il semble prometteur d'enrichir l'arsenal formel avec un outil complémentaire, permettant de générer automatiquement du code de contrôle commande correct par construction. La théorie du contrôle par supervision offre un cadre théorique intéressant, mais n'a pas abouti à une maturité industrielle comparable à celle de la vérification formelle. Cette présentation montre une démarche méthodologique permettant d'utiliser en synergie trois techniques d'aide à la conception, dans le cadre d'une approche de conception par composants : la vérification formelle, la synthèse de contrôleurs discrets et la simulation. La méthode est illustrée sur une étude de cas tirée d'un projet industriel.