→ Tendances Un cluster de stations de travail pour la modélisation 3D. page 24

→ Tendances Visual Studio .Net efficace, mais perfectible. page 26

Enquête

Les méthodes formelles sonnent le glas des tests unitaires

Cette technologie remet en cause le cycle de développement traditionnel pour garantir un niveau de fiabilité logicielle encore jamais atteint.

La preuve est plus puissante que le test », argue Thierry Servat, directeur général de Clearsy. Cette filiale des sociétés de services Steria et Teamlog, spécialisée dans la production de logiciels prouvés et dans l'expertise de systèmes, a fait de la méthode formelle B son cheval de bataille. Et son discours rallie à sa cause un nombre croissant d'entreprises utilisatrices. Gemplus, la RATP, la SNCF, Peugeot, le CEA (Commissariat à l'énergie atomique)... sont autant de références dont se targue la SSII. Les méthodes formelles seraient-elles en train de gagner leurs lettres de noblesse ? Elles ont, en tout cas, d'ores et déjà prouvé leur efficacité lorsqu'il s'agit de fiabiliser des logiciels embarqués. Elles sont en mesure de garantir la cohérence des spécifications d'un système et la conformité du code produit par rapport à celles-ci. A tel point que Thierry Servat n'hésite pas à affirmer : « *La méthode formelle B permet de supprimer les tests unitaires.* »

J. WALLACE

Depuis 1998, date de mise en service de Météor (ci-dessus, son centre de commandes centralisé), les logiciels sécuritaires du métro automatique parisien, développés à l'aide des méthodes formelles, n'ont connu aucune défaillance.

▸ Mariage de la modélisation et de la preuve

Appliquer une méthode formelle revient d'abord à construire un modèle mathématique correspondant aux spécifications informelles d'un système. Pour cela, on utilise un formalisme mathématique de haut niveau. Celui-ci est composé, entre autres, d'ensembles, de propriétés et d'opérateurs. La seule lecture du modèle obtenu permet de retrouver les spécifications. Il est ensuite transformé afin de prendre de plus en plus en compte les contraintes de codage. C'est-à-dire des caractéristiques propres à la réalisation d'un logiciel. Il s'agit du « raffinement ». Le modèle est décomposé en modules successifs, toujours plus précis. A chaque étape de cette décomposition, il est « prouvé » que tout nouveau module n'introduit pas d'incohérence avec le niveau supérieur. Ce processus, mené à son terme, aboutit à la production d'un pseudo-code de programmation, qu'il suffit alors de traduire dans le langage de développement choisi pour le logiciel. Les « preuves » émises lors des phases de spécification, de conception et de codage permettent de se dispenser de procéder aux tests unitaires et de validation. C'est une remise en cause des cycles de développement traditionnels, et notamment du cycle en V. Les méthodes formelles suscitent depuis peu un engouement croissant chez les industriels. Pourtant, elles ne sont pas nouvelles. Issues du milieu universitaire, elles ont plus de vingt ans. Mais il a tout de même fallu attendre la fin des années quatre-vingt pour que certains d'entre eux commencent à s'y intéresser. Alstom, spécialiste des infrastructures pour l'énergie et le transport, fut l'un des premiers, à l'occasion du développement du Sacem (système d'aide à la conduite, l'exploitation et la maintenance) pour la ligne A du RER (réseau express régional) parisien. Ce système permet au conducteur de se passer de la signalisation latérale – ramenée en cabine – et assure un contrôle continu de la vitesse des trains. S'en remettre à des automatismes lorsqu'il s'agit de transporter des

Outils

L'Atelier B rend possible l'utilisation de la méthode B en milieu industriel

Intégrant tous les composants nécessaires à l'automatisation de l'activité de preuve, cet outil a déjà été mis en œuvre notamment sur le projet Météor.

L'utilisation des méthodes formelles dans un contexte industriel ne peut être envisagée sans l'aide d'outils. L'Atelier B est l'un d'eux. Il a été constitué grâce aux efforts conjoints de plusieurs entreprises voulant utiliser la méthode B : les constructeurs Alstom et Matra Transport International, la SSII Stéria, la RATP et la SNCF. Il permet une utilisation opérationnelle de la méthode B sur des projets d'envergure et a déjà été mis en œuvre, entre autres, sur le projet Météor (quatorzième ligne du métro parisien, entièrement automatisée). Il comprend un générateur automatique de preuves destiné à générer les conditions de validation qui rendent corrects les modèles abstraits, un «prouveur» qui se charge de prouver automatiquement les énoncés résultants, et un traducteur qui, lui, transforme le dernier niveau de raffinement du modèle B en langage de programmation traditionnel. L'Atelier B intègre aussi un analyseur lexical, un analyseur syntaxique et un vérificateur de type.

EN RÉSUMÉ

Si le zéro défaut logiciel demeure encore aujourd'hui une utopie, il est désormais possible de s'en rapprocher grâce aux méthodes formelles avec preuve. Celles-ci remettent en cause le cycle de développement classique et imposent de se pencher plus longuement sur les spécifications. En échange, un certain nombre de tests, dont les tests unitaires, peuvent être supprimés. Les entreprises qui ont osé se lancer dans l'expérience en sont sorties convaincues.