Testé en entreprise

Les méthodes formelles, garantes de la sécurité des systèmes

En complément du cycle de développement traditionnel, les méthodes formelles imposent de se pencher plus longuement sur les spécifications.

Les méthodes formelles permettent d'être plus rigoureux dans le développement des logiciels et d'éliminer les erreurs de spécification, de conception et de codage », explique Luis-Fernando Meija, responsable méthodes formelles chez Alstom. Car, lorsqu'il s'agit de concevoir le pilote automatique d'un train ou le programme d'une puce de carte bancaire, les exigences de sécurité sont extrêmes. Ces programmes ne supportent aucune défaillance. Le principe des méthodes formelles consiste à traduire les spécifications du système dans un langage mathématique – ensembles, propriétés, etc. Les techniques de transformation et de vérification du modèle obtenu reposent sur la preuve mathématique. Elles prouvent que le système est complet vis-à-vis de ses exigences. La preuve garantit l'élimination des erreurs. La méthode formelle aboutit à la production d'un pseudo-code de programmation, qu'il suffit de traduire dans le langage de développement.

▸La méthode B appliquée au monde ferroviaire

Alstom est à la genèse de l'industrialisation de la méthode B, à l'occasion du développement du Sacem (Système d'aide à la conduite, l'exploitation et la maintenance) pour la ligne A du RER parisien. « *La RATP estimait les méthodes de sécurité traditionnelles insuffisantes* », développe Luis-Fernando Meija. Le constructeur s'est donc appuyé sur les travaux de Jean-Raymond Abrial, professeur au Cnam (Conservatoire national des arts et métiers), pour appliquer la méthode B au monde ferroviaire. « *Au début des années quatre-vingt-dix, nous avons développé des outils pour industrialiser B. Sans eux, c'était impossible* », précise Luis-Fernando Meija. Face aux quatre-vingt-six mille lignes de code Ada des logiciels « sécuritaires » (liés à la sécurité du voyageur) de Météor (quatorzième ligne du métro parisien, entièrement automatisée), Matra Transport International (MTI) a choisi la même méthode. « *Pour un logiciel sécuritaire, le développement n'est pas plus coûteux, car il supprime les tests unitaires* », justifie Jean-Marc Meynadier, responsable du service équipement pilote automatique chez MTI. Chez Trusted Logic, spécialiste du logiciel Java embarqué sur cartes à puce, Coq a été choisi. « *L'intérêt est de modéliser la partie complexe du logiciel et de démontrer qu'il résiste à des attaques* », explique Daniel Le Métayer, directeur technique de Trusted Logic. « *C'est surtout un élément complémentaire par rapport au cycle de développement classique* », ajoute Claire Loiseaux, responsable évaluations sécuritaires et méthodes formelles de la société. **Jean-Marie Portal**


J. WALLACE

Jean-Marc Meynadier, responsable du service équipement pilote automatique chez Matra Transport International

« La réutilisation permet d'en réduire fortement les coûts »

▸ MATRA TRANSPORT INTERNATIONAL

- **Activité :** réalisation de systèmes de transport ferroviaire urbain entièrement automatisés.
- **CA 2000 :** 200 M€.
- **Effectif :** 600 personnes.
- **Localisation :** mondiale, siège à Montrouge.
- **Technologie utilisée :** méthode B.


J.L. DESNOS

Luis-Fernando Meija, responsable méthodes formelles chez Alstom

« On réfléchit beaucoup plus aux spécifications »

▸ ALSTOM

- **Activité :** spécialiste global des infrastructures pour l'énergie et le transport.
- **Chiffre d'affaires 2000 :** 22 Md€.
- **Effectif :** 122 000 personnes.
- **Localisation :** 70 pays, siège à Paris.
- **Technologie utilisée :** méthode B.

EN RÉSUMÉ

Il est des domaines où les programmes informatiques n'ont pas le droit à l'erreur. Car, dans le cas d'un logiciel de pilotage automatique, la défaillance peut être synonyme d'accident grave de voyageurs. Pour parer à de tels scénarios catastrophes, les constructeurs se tournent désormais vers les méthodes formelles. Celles-ci permettent de garantir, sous certaines conditions, le bon fonctionnement d'un système.

POUR EN SAVOIR PLUS

www.inria.fr/recherche/equipes/coq.en.html
Le site du projet Coq de l'Inria.

www.atelierb.societe.com/lettre_b/volume_1/lettreb_1.html
Les utilisateurs partagent leurs expériences sur la méthode B.

The B-Book : Assigning Programs to Meanings,
par Jean-Raymond Abrial ; Cambridge University Press ; 1996.