



B pour la modélisation de spécifications systèmes

B pour la modélisation de systèmes ?

B est une technique de modélisation applicable aux spécifications systèmes (matériels et logiciels) ; par son association à des mécanismes de preuve, cette *méthode formelle* est **unique**. L'offre B'SYSTEME repose sur cette technique et permet d'obtenir **DES SPECIFICATIONS SYSTEME PROUVEES**.

Pour quels problèmes ?

Est-il acceptable que des spécifications de systèmes soient incomplètes, ambiguës, voire incohérentes ?

Exemple : Si une carte à puce est retirée inopinément d'un lecteur en cours de transaction, son état interne doit être "restauré". Cela lui permettra de fonctionner correctement à la prochaine occasion. Que se passe-t-il si la carte est de nouveau extraite pendant la "restauration" ? Si la spécification est incomplète ou ambiguë sur ce point, le comportement du système n'est pas garanti.

Peut-on être sûr qu'un système respecte les propriétés fondamentales attendues ?

Exemple : Certains systèmes de condamnation des portes de véhicules automobiles récents reposent sur l'utilisation d'une télécommande. On constate que certains modèles ne peuvent plus être décondamnés manuellement. Existe-t-il une configuration dans laquelle le passager puisse être bloqué ? Une spécification effectivement prouvée va garantir qu'un tel scénario n'est jamais possible.

Peut-on garantir que les multiples composants d'un système assurent bien ensemble les fonctions attendues ?

Exemple : Des bâtiments sont protégés par un système de contrôle d'accès par badge et lecteur. Leur accès est uniquement réservé à une liste de personnes gérée dans une base de données. Se peut-il qu'une personne n'ait plus accès au bâtiment suite à une demande ? Est-on sûr qu'aucune personne n'est présente dans les bâtiments après une certaine heure ? Toute personne entrée pourra t'elle sortir ? Ici, la multiplicité des "composants" (badges lecteurs, personnes, bâtiments) doit être harmonieusement organisée.

Quelles sont les conséquences humaines, économiques et stratégiques de la défaillance d'un système grand public ?

Exemples de "scénario catastrophes" bien connus : Arrêt d'un métro pendant les heures de pointe, retour constructeur d'une série d'un modèle de voiture, impossibilité de communiquer avec un satellite, ...

Utilisation de B pour la modélisation de systèmes

Cette utilisation de B s'adresse :

1. à ceux qui ont déjà fait la spécification de leurs systèmes et qui doutent qu'elle puisse en l'état servir de base à un développement
2. à ceux qui ont terminé le développement de leur produit et qui n'arrivent pas, sur la base des documents dont ils disposent, à en comprendre complètement le fonctionnement

Dans les deux cas il s'agit de reprendre et de donner beaucoup plus de cohérence aux documents de référence. La technique est basée essentiellement sur la modélisation et la preuve.

Le processus global de modélisation

Il repose sur l'utilisation de la méthode formelle B et de son environnement industriel : l'Atelier B.

Il comprend typiquement les phases suivantes :

1. élaboration itérative du modèle
 - ◆ modélisation progressive, établissement d'un glossaire et d'un questionnaire
 - ◆ interview des spécialistes, analyse des réponses
 - ◆ **preuve des modélisations**
2. finalisation du modèle et remise d'un document comprenant : un nouveau référentiel et l'énoncé des problèmes découverts en cours d'étude.

Clients et partenaires

Alstom, CEA, CNES, Crédit Agricole, DGA, EADS, EDF, Eurocopter, Gemplus, Intracom, INRETS, IPSN, Nokia, Perkin Elmer, PSA, RATP, Renault, Siemens Transportation System, SCLE ERJI, SNCF, Société Générale, ST Microelectronics, THALES, Volvo, ...

Méthode B, technique formelle éprouvée et reconnue

La méthode B a été inventée en 1980 par Jean-Raymond ABRIAL. Le langage B est fondé sur les concepts mathématiques de la théorie des ensembles ; il intègre des mécanismes de preuve et peut couvrir sans rupture tout un cycle de développement, jusqu'au code pour les éléments logiciels. **The B Book** (de J.R. ABRIAL, paru en 1996 chez Cambridge University Press) est l'ouvrage de référence sur B.

Dans la réalisation de Météor (ligne 14 du métro parisien qui fonctionne en automatisme intégral sans conducteur), B et son environnement industriel (Atelier B) ont été mis en œuvre. Depuis les premiers essais des systèmes de sécurité en novembre 1997, **aucune erreur** n'est apparue dans les services développés avec B. ClearSy commercialise l'Atelier B depuis 1993.