



B dans le domaine LOGICIEL B dans le domaine LOGICIEL

B dans le domaine LOGICIEL ?

B est une technique de modélisation applicable au développement de logiciels ; par son association à des mécanismes de preuve, cette *méthode formelle* est **unique au monde**. L'offre B'LOGICIEL repose sur cette technique et permet d'obtenir **DES PROGRAMMES PROUVES CONFORMES AUX EXIGENCES FONCTIONNELLES**.

Pour quels problèmes ?

Est-il acceptable qu'une spécification logicielle soit incomplète, ambiguë, voire incohérente ?

En Génie Civil, la construction d'un pont débute par une phase préalable d'étude pendant laquelle des simulations mathématiques garantissent l'homogénéité des structures. On ne pourrait se permettre, comme pour un logiciel, d'ajuster le pont au fur et à mesure de sa construction, ou de le reconstruire plusieurs fois.

➤ Dans le domaine du logiciel, B permet d'atteindre le même niveau de fiabilité.

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

Les développements "classiques" se caractérisent par deux défauts : les étapes sont réalisées avec des formalismes différents, les tests sont réalisés à la fin et ceux concernant l'étape de spécification (conformité fonctionnelle) sont effectués en dernier. Les propriétés du logiciel sont souvent implicites et difficilement traçables. Des techniques de traçabilité et d'analyse de sûreté sont mises en œuvre pour répondre à ces problèmes.

➤ Avec B, les propriétés sont explicitées dès la spécification et l'on prouve automatiquement, au fur et à mesure des étapes de conception, qu'elles sont respectées.

Peut-on alléger les phases de tests et les phases de sécurisation et d'industrialisation d'un logiciel ?

Plus de 70% du temps de développement est consacré à la mise au point globale (des spécifications à la validation) ; tel est le pourcentage souvent cité dans la pratique.

➤ Ce temps peut être réduit grâce à l'utilisation de B.

Quels sont les véritables coûts de maintenance ?

➤ Un logiciel pour lequel B a été utilisé pour toute les étapes de conception ne nécessite aucune maintenance.

Peut-on sécuriser un système à moindre coût ?

Un avion doit continuer à fonctionner même si l'un de ses calculateurs se révèle défaillant. Pour cela, les calculateurs sont redondés pour assurer la disponibilité des fonctionnalités. Les programmes sont développés indépendamment pour pallier aux pannes logicielles.

➤ Avec B, un seul programme suffit pour assurer la sécurité du logiciel, dans une architecture multi-calculateurs.

Quelles sont les conséquences humaines, économiques et stratégiques de la défaillance d'un logiciel intégré dans 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, ...

B et les normes

➤ La norme ISO/IEC 15408 (Critères Communs pour l'évaluation de la sécurité des technologies de l'information) préconise l'utilisation de modèles formels à partir du niveau 5, et indique que le niveau 7 est atteint par la réalisation *d'une spécification et d'une conception formelle de haut niveau*, avec *démonstration formelle de la correspondance entre elles*.

➤ Dans la norme française NF F 71-012 pour les installations fixes et matériel roulant ferroviaires, il est indiqué : *pour les spécifications, des méthodes formelles mathématiques sont recommandées car le modèle formel fournit précision, non ambiguïté et cohérence*.

➤ Il est indiqué dans la norme Aéronautique RTCA DO-178B/EUROCAE ED-12B (considération sur le logiciel en vue de la certification des systèmes et équipements de bord) qu'une *analyse avec méthode formelle (MF) peut fournir la preuve que le système est complet et correct vis-à-vis de ses exigences. L'utilisation de MF a pour but d'éviter et d'éliminer les erreurs de spécification, de conception et de codage lors du développement du logiciel. Les MF augmentent la certitude qu'un dysfonctionnement ne se produira pas ou qu'il sera hautement improbable. L'utilisation de spécifications formelles seules rend les exigences non ambiguës. L'utilisation de MF commence par la spécification des exigences de haut niveau du logiciel dans un langage formel et par la vérification au moyen de preuves formelles qu'elles satisfont les spécifications du système... il est ensuite démontré que le niveau d'exigences immédiatement inférieur satisfait les exigences de haut niveau. L'exécution de ce processus jusqu'au Code Source fournit la preuve que le logiciel satisfait les spécifications du système...*

Description d'un cycle de développement complet avec B

La méthode B utilise une notation - le langage B - fondée sur les concepts de la théorie des ensembles. C'est une notation uniforme couvrant toutes les étapes du développement depuis la spécification jusqu'à la réalisation des composants logiciels exécutables.

Un développement B débute par la construction d'un modèle reprenant toutes les descriptions du besoin. D'autres modèles sont ensuite élaborés par étapes, toujours à l'aide du langage B, jusqu'à obtenir un programme exécutable.

La cohérence des modèles aux différentes étapes et la conformité du programme au modèle initial sont garanties par des **preuves mathématiques**. A l'ultime étape, les programmes réalisés sont **corrects par construction et rendent inutiles les tests** de premier niveau destinés à éliminer les erreurs de programmation (débordement de tableaux, calcul arithmétique hors bornes, boucles infinies, ...) ou à vérifier leur conformité au modèle. Seuls subsistent les tests d'intégration d'ensemble : logiciel, environnement matériel et environnement logiciel.

Description d'utilisations possibles de B

La formalisation et preuve du cahier des charges

➤ permet à un donneur d'ordre d'établir un référentiel d'exigences de développement cohérent, sans ambiguïté et complet vis-à-vis des besoins exprimés.

L'élaboration de spécifications prouvées

➤ permet, sur la base des besoins exprimés, de réaliser des spécifications et la preuve de leur cohérence. Pour cela, un modèle B est réalisé puis prouvé. Puis il est ré exprimé en français (ou dans tout formalisme) qui servira ensuite de référence au développement qui suivra.

L'expertise/validation de spécifications

➤ permet, à partir du référentiel de spécification d'un développement déjà en cours, de détecter au plus tôt les problèmes. Leur correction peut alors s'effectuer immédiatement ou dans une version ultérieure du logiciel. L'expertise est menée en parallèle du développement et peut être réalisée par le maître d'ouvrage ou le maître d'œuvre dans le cadre des revues et des recettes.

Le développement des modules à exigence de certification

➤ consiste à utiliser la méthode B dans son plus large spectre, de la spécification au code exécutable.

Atelier B

L'Atelier B est un produit développé, supporté et commercialisé par ClearSy depuis 1993. Il permet une utilisation opérationnelle de la méthode B et offre, au sein d'un environnement cohérent, de nombreuses fonctionnalités permettant de gérer des projets en langage B. Ces fonctionnalités se regroupent en quatre catégories :

- ◆ les tâches automatisables lors du développement d'un projet : les vérifications syntaxiques des composants, la génération automatique des théorèmes à démontrer, la traduction automatique des modules B bas niveau vers les langages C, C++ ou Ada,
- ◆ une aide à la preuve, pour démontrer automatiquement ou interactivement les théorèmes,
- ◆ une aide au développement : gestion automatique des dépendances entre composants B, bibliothèques réutilisables, génération de documentation et génération de métriques,
- ◆ des outils de confort pour l'utilisateur : représentation graphique de projets, navigateur hypertexte pour se diriger dans un projet, affichage de l'état et des statistiques d'un projet, génération automatique du dictionnaire des termes d'un projet, archivage de projets.

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, ...