B : Une méthode de développement de logiciels sûrs

Loïc PELHATE,
Responsable de l'Atelier des Logiciels de Sécurité
de l'Ingénierie du Transport Ferroviaire

loic.pelhate@ratp.fr

Plan

- Contexte et problématique
- La méthode B
- L'Atelier B
- Bilan
- Utilisateurs industriels
- Etudes et recherches

Le contexte

- **1988 : Premiers logiciels de sécurité (SACEM - RER A)**
  - **Problèmes de spécification**
    - manque d'approche système
    - ambiguïtés
    - difficultés pour mesurer la cohérence et la complétude
  - **Problèmes de validation**
    - pas de certitude de la suffisance des tests
  - **Re-spécification formelle + Preuve**
    - Détection d 'une 20aine d'erreurs de conception/codage

Mise en service retardée d'un an

La problématique METEOR

- **Un système complexe**
  - pilotage automatique sans conducteur
  - possibilité d'une exploitation mixte
- **De fortes contraintes de performances**
  - fiabilité, disponibilité, maintenabilité
  - sécurité
- **Le retour d'expérience du SACEM**
  - utilisation de méthodes formelles

Le choix de la méthode B

- **Objectif**
  - **Obtenir un logiciel correct par construction**
- **Domaine d'application**
  - **Code séquentiel ininterruptible**

    (non prise en compte des aspects temps réel, des logiciels de base…)
- **Langage à large spectre**
  - **Cadre unifié et continu de la spécification au code**

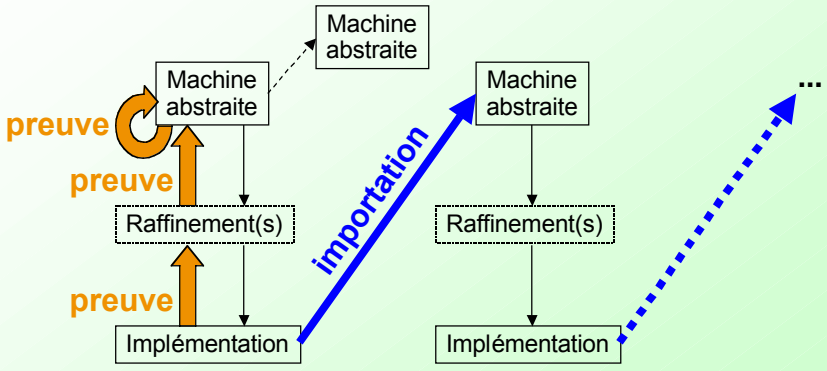
Les concepts de la méthode B

- **Méthode « orientée modèle »**
  - **Logiciel = données + propriétés + services**
- **Processus de raffinement**
  - **Passage de la spécification abstraite au code concret en une ou plusieurs étapes**
- **Obligations de preuve**
  - **Construction rigoureuse du logiciel basée sur les mathématiques**

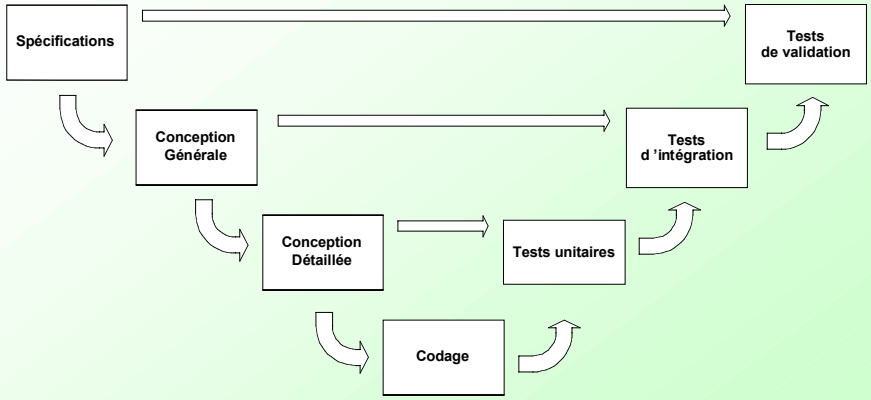
Le Langage B

- Modélisation des données et des propriétés
  - Théorie des ensembles
  - Logique du premier ordre
- Modélisation des services
  - Substitutions généralisées
- Décomposition et architecture
  - Machines abstraites

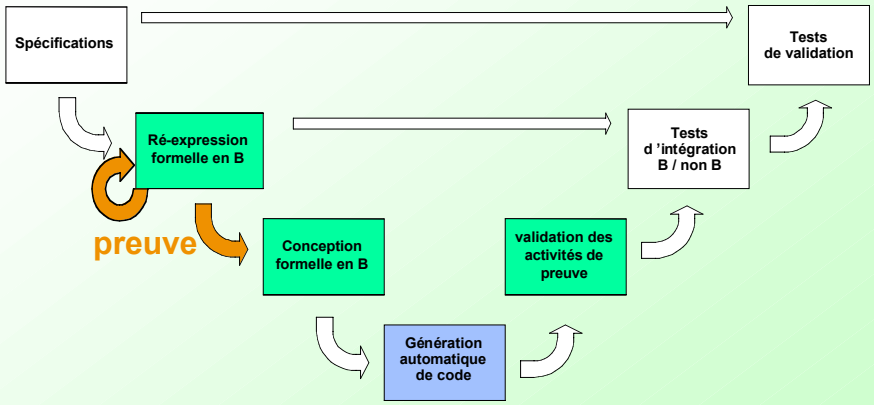
Architecture classique d'un modèle B



Cycle de vie standard



Cycle de vie avec B



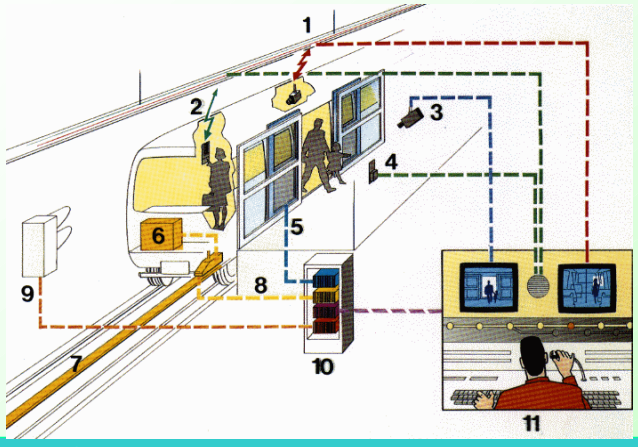
L'Atelier B

- Outil industriel de développement logiciel supportant la méthode B
- Eléments clés
  - Prouveurs automatiques et interactifs
  - Générateurs de code (ADA, C, C++)
- Eprouvé sur METEOR

METEOR : la ligne 14 du métro parisien

- Inaugurée le 15/10/1998
- 7.2 km, entre "Madeleine" et "Bibliothèque François Mitterrand" pour 7 stations
- 25 000 passagers/heure dans chaque sens
- 19 trains composés de 6 voitures (extension à 8 voitures possibles)
- 40 km/h : vitesse commerciale
- 85 s : intervalle entre les trains en automatique

Un système complexe



1 - Vidéo-surveillance de train (transmision par hyperfréquence)
2 - Interphone
3 - Video-surveillance de quai
4 - Interphone sur le quai
5 - Portes pallières
6 - Pilotage Automatique Embarqué
7 - Tapis de transmission
8 - Transmission SOL-BORD
9 - Signalisation
10 -Pilotage Automatique Section
11 -PCC

Maturité industrielle de l'Atelier B

- Le noyau sécuritaire de METEOR représente :
  - 1150 composants B
  - 115000 lignes de B
  - 27800 obligations de preuve
  - 86000 lignes de code ADA sécurisé

  Intégralement analysé et prouvé avec l'Atelier B

Bilan de l'utilisation de B

- Meilleur passage entre phases système et logicielle
- Meilleure maîtrise des spécifications
- Amélioration de l'intégration des logiciels
- Allègement du processus classique de validation
- Haut niveau de qualité du logiciel

Coûts des logiciels développés en B

- Comparable à celui d'un logiciel développé et validé selon des méthodes classiques mais …

  pour des niveaux de qualité et de sécurité supérieurs

- MTI l'utilise sur tous ses projets y compris sur des parties non sécuritaires

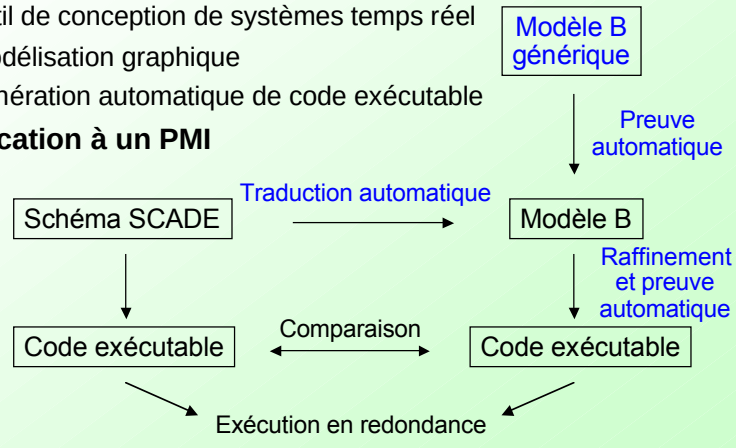
Utilisateurs industriels

- **Ferroviaire**
  - **Systèmes de contrôle de vitesse et de pilotage automatique intégral**
    - SACEM Mexico, métro de New York, métro de Lyon MPL75, métro de Hong Kong, KVB Bord (SNCF)
- **Automobile**
  - **Diagnostic de panne**

    Analyse système
- **Carte à puce**
  - **Validation de protocoles de sécurité**

Couplage B-SCADE

- **SCADE**
  - outil de conception de systèmes temps réel
  - modélisation graphique
  - génération automatique de code exécutable
- **Application à un PMI**



Etudes

- schémas EDF
- poste de manœuvre d'aiguillage
- systèmes temps réel
- système de gestion de bases de données
- protocoles cryptographiques
- protocoles de communication
- …

Tendances

Remontée aux niveaux systèmes :

- B-évènementiel et B-système
  - Conception système
  - Contraintes dynamiques
  - Système concurrent
- Site B du laboratoire du LSR Grenoble
  - http://www-lsr.imag.fr/B/