



# AtelierB

## Captronic

### 01 octobre 2013

**ClearSy**  
contact@clearsy.com

Téléphone :  
04.42.37.12.70  
01.40.28.14.57

[www.clearsy.com](http://www.clearsy.com)

---

Captronic/AtelierB



## ► Sommaire

- Résumé des dernières années
- Politique de distribution source et budget
- Projet : développement logiciel
- Projet : développement système
- Projet : de validation de donnée
- Développement en cours
- Développement envisagé



## ► AtelierB

Atelier logiciel qui permet une utilisation opérationnelle de la méthode formelle B.



- Ces fonctionnalités se regroupent en quatre catégories :
  - Une aide à la preuve : pour démontrer les obligations de preuve, grâce à des outils de preuve
  - Une aide au développement : Gestion des dépendances entre composants B, Le raffinement automatique, Analyse statique
  - Des outils de confort pour l'utilisateur: Représentation graphique de projets, Affichage de l'état d'un projet, Gestion des règles



# Résumé des dernières années



METEOR  
MATRA 2000



Clic'n'prove



ROISSY  
SIEMENS



PEKIN  
ALSTOM



ComenC

Bart



1994

1998



2010



COPPILOT



PARIS, SAO PAULO

4



# ► Politique de distribution

## ► Version :

- V X.Y : 1 Version tous les 2 ans environ. Téléchargeable directement sur le site <http://www.atelierb.eu> (V4.1).
- V X.Y.z : Version de maintenance (version de correction + version spécifique projet) .Téléchargeable après identification sur le site

The screenshot shows the homepage of the Atelier B website. The header features a large orange 'B' logo with 'ATELIER' written below it. To the right of the logo is the text '“ COMPUTER AIDED SOFTWARE ENVIRONMENT... ATELIER DE GENIE LOGICIEL ”'. A search bar is located in the top right corner. The navigation menu below the header includes links for ACCUEIL, ACTUALITÉS, ATELIER B, TÉLÉCHARGEMENTS, FORMATION B, SUPPORT, RÉFÉRENCES, LIENS, and CONTACT. The main content area includes sections for 'TÉLÉCHARGER L'ATELIER B', 'ATELIER B EN TÉLÉCHARGEMENT GRATUIT', and a sidebar with links for 'FRANÇAIS', 'REJOIGNEZ-NOUS', 'CLEARSY RECRUTE !', 'PROJETS R&D / OPEN SOURCE', 'MANUELS', 'PROJETS OPEN SOURCE', and 'R&D'.



## ► Source

### ► Source :

- Les IHM en Qt et le B compilateur (Bcomp) sont open source

**sourceforge**

Regrouper sur <http://www.tools.clearsy.com/tools/> :



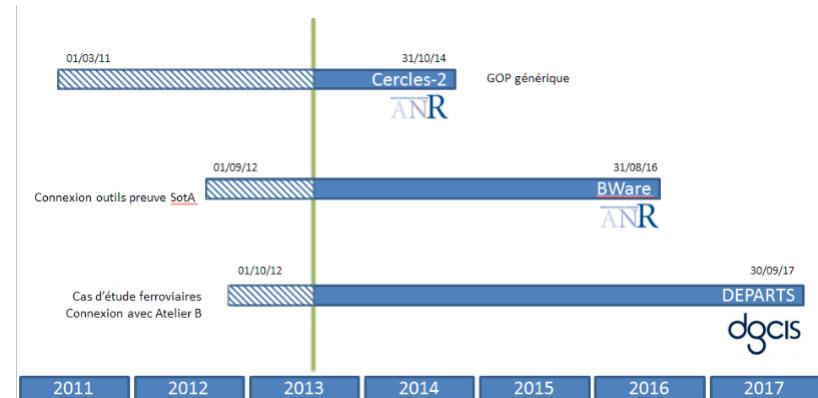
- Les autres outils (MS, krt, TC, PO, PR) restent fermés :  
Validation/Qualification des modifications



# ► Financement de l'AtelierB

## ► Projet de R & D (80%) :

- CERCLE 2
- DEPARTS BWare
- DEPARTS
- Cx



## ► Maintenance de l'AtelierB (10%) :

- Entreprise : Variable suivant utilisation.
- Université : 950€ licences illimité (élève, enseignant/chercheur)

## ► Développement particulier (10%) :

- Demande d'un projet Interne
- Demande d'un client



# ► Développement logiciel

## ► Méthode formelle de développement logiciel

- ▶ Modéliser de façon abstraite du comportement d'un programme
- ▶ Raffinements successifs jusqu'à un modèle concret transcodable
- ▶ Preuve de consistance et de raffinement

## ► Pas de magie

- ▶ Les tests sont remplacés par la preuve
- ▶ Les résultats obtenus dépendent de l'effort de spécification  
WYGIWYP : What you get is what you provided
- ▶ Not a « push-button » method



## ► Projet Urbalis Evolution (Alstom)

- **Environ 50 métros en exploitation**
- **11 versions majeures à ce jour**

### Plaquette URBALIS

## 12 raisons de plus de choisir URBALIS

- **Sécurité élevée** – Utilisation de méthodes formelles pour l'élaboration de logiciels
- **Economies d'énergie** – Jusqu'à 30 % en utilisant au maximum la marche sur l'erre
- **Interfaces standards** – TCP/IP et Ethernet, IEEE 802.11
- **Technologie radio robuste et fiable** – en service sur des lignes majeures depuis plus de 10 ans (depuis 2003)



# Some implementations (B)



L1  
Paris



L1  
Algiers



SHUTTLE  
ROISSY AIRPORT  
Paris



L2 L3  
Sao Paulo



Mexico



Airport Express  
Hong Kong



Madrid



New York  
Canarsie



L3  
Paris



Lille

L9  
Seoul



L9  
Barcelona



Instanbul

L2  
Budapest



Toronto



Metro L10  
Beijing



Circle Line  
Singapore



Singapore

San Juan



Delhi



Metro  
Lausanne



L1 L2  
Malaga



L5  
Milano



METEOR L14  
Paris



KVB  
6000 trains  
France



1990

2000

2010 0

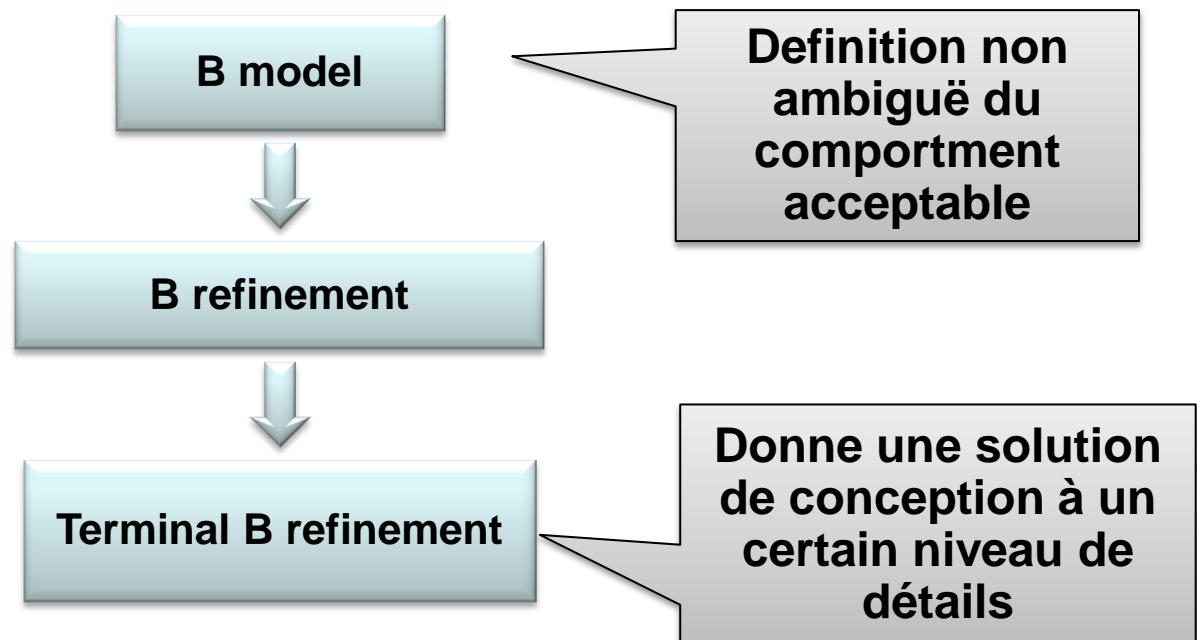


## ► B évènementiel / B système

Utilisée pour décrire formellement les systèmes et raisonner mathématiquement sur leurs propriétés.

### ► Basé sur la Méthode B :

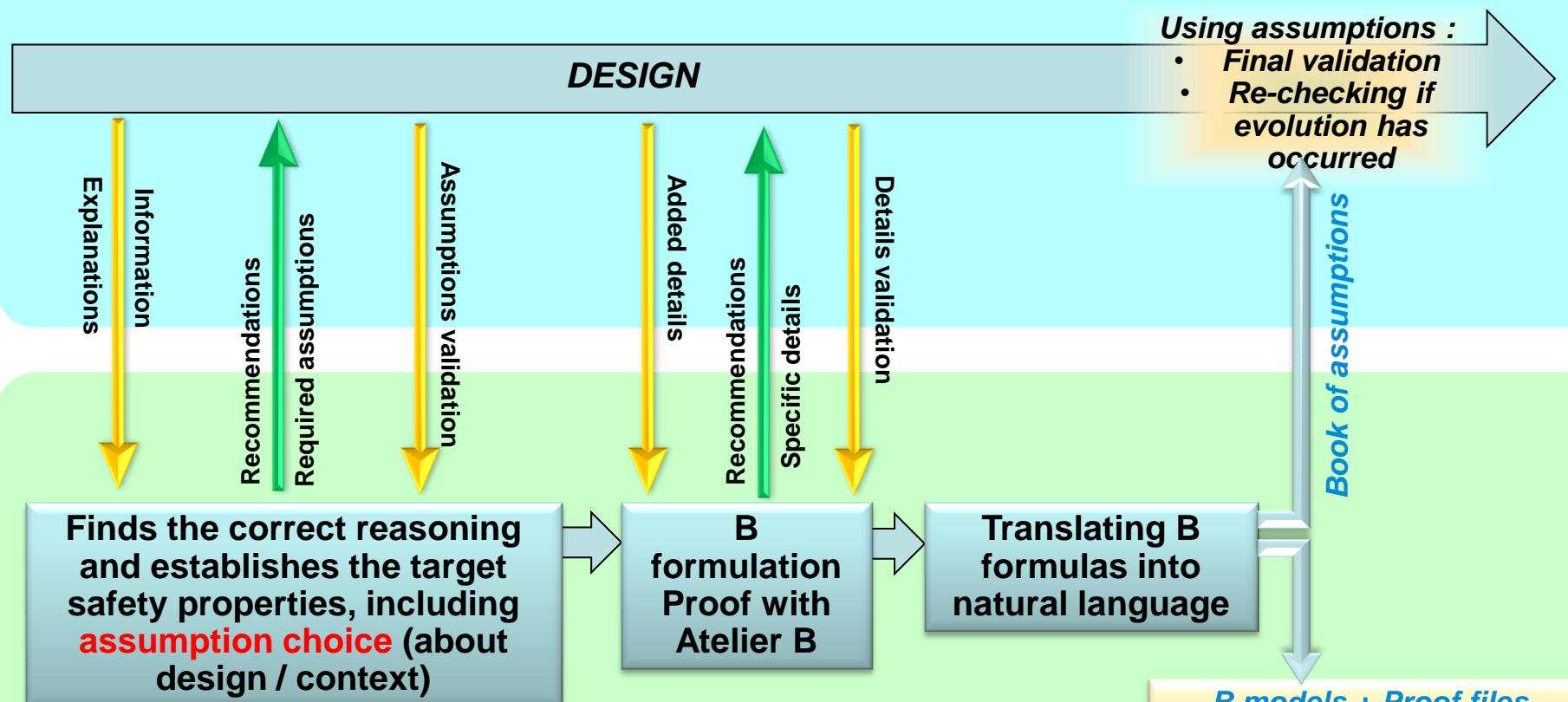
- Formalisme
- Preuve
- Raffinement





# ► Flushing line (New York)

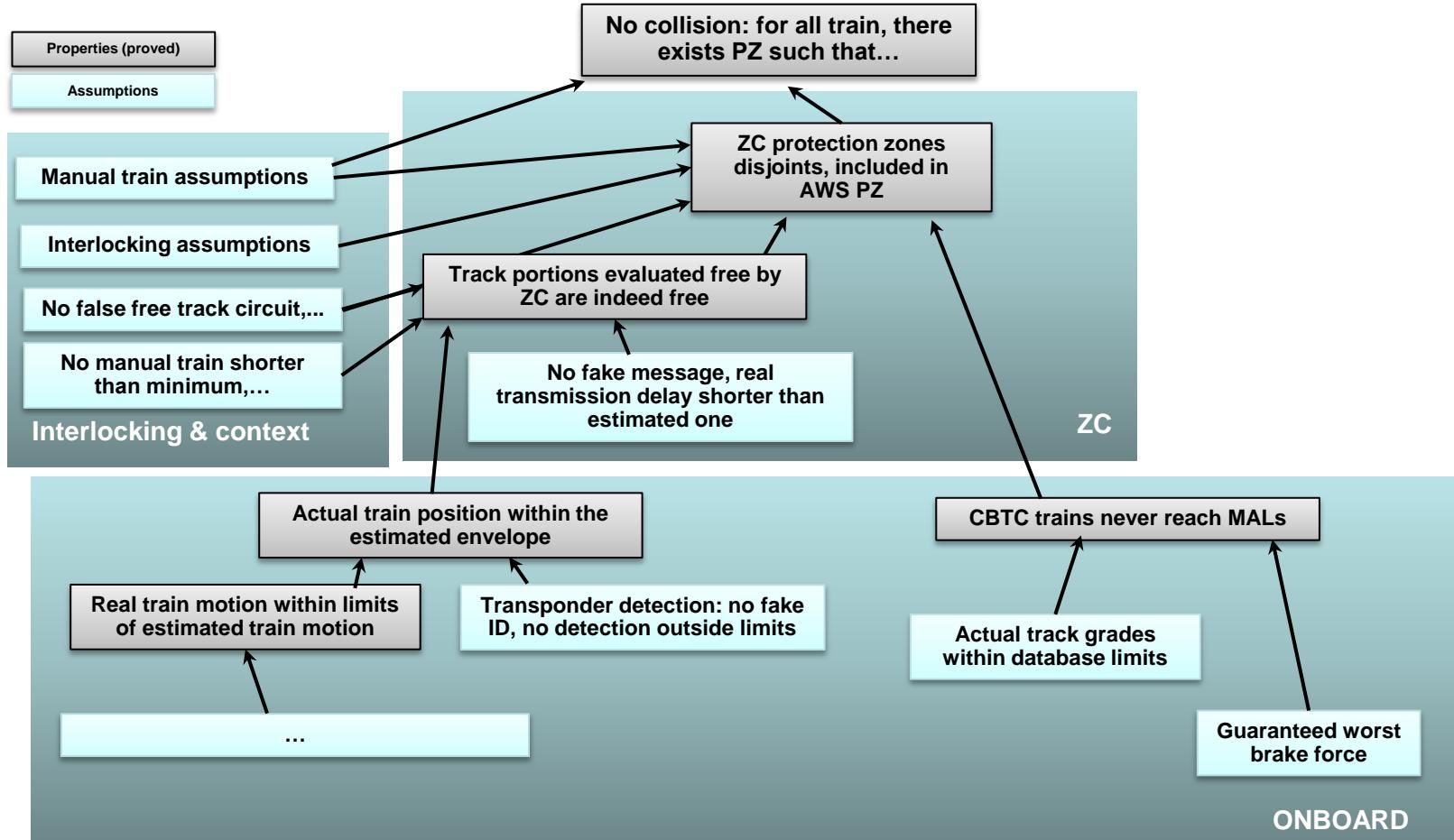
Project Team (THALES / NYCT)



System Proof Team (ClearSy)



# Properties & sub-properties





# ► Vérifications de Donnée

**Utilisée pour en vérifier mathématiquement les propriétés sur les données**

## ► Etats de l'art

- Plusieurs projets de R&D ont permis de développer les outils
- Utilisation courante dans le monde industriel : Alstom, RATP, Siemens



## ► Permet :

- Le traitement de grande quantité
- Formalisation des données (consistantes, corrections)
- Validation d'un ensemble de données partiellement construit
- Mise en évidence des contre-exemples de manière simple



## ► Projet : TMS DATA (Alstom)

- ▷ Gain en temps :
  - ▶ Environ 30 jours pour vérifier 300 règles manuellement,
  - ▶ Quelques heures pour vérifier 300 règles modélisées
- ▷ Plus de 100000 informations
- ▷ Environ 1500 propriétés modélisé
- ▷ Poursuite de l'automatisation sur d'autres données



## ► En développement

### ► AtelierB V 4.2.0

- Début 2014
- GOP Générique :
  - Possibilité de paramétriser les OP générer.
  - Traçabilité des OP
  - Parallélisations du GOP.
- Interfaçage avec plusieurs Prouveurs
- Gestion du 64 bits
- Améliorer le rajout de plug-in



# En développement : Gestion des exigences

- ▷ Lier une partie d'exigence avec des substitutions
- ▷ Vérification du lien et du commentaire
- ▷ Gestion des versions
- ▷ Vérification de couverture
- ▷ Métrique

The screenshot shows the Atelier B tool interface with the following windows:

- Project**: Shows a tree view of the project structure under "UEVOL (10.2.8)" and "UEVOL (10.2.5)".
- Code Editor**: Displays a C code snippet for "uevol\_ctrl\_minabis\_1". It includes several "#Requirement" blocks with various conditions and values.
- Requirement Details**: Shows requirement "CC\_ATP-A401464-SwRS-1292-1" with status "OK", linked to "Document.doc". The body of the requirement is described as "Other CC Synchro Report Minabis Distance Counter for end 1(Cycle)".
- Pragmas**: A window showing pragmas for the code.
- Specifications**: A table showing the status of requirements. The table has columns for "Specification", "Status", and "%". Many requirements are marked as 100% complete.



# En développement : SDV

- ▷ Vérification de propriété
- ▷ Double chaîne de vérification
- ▷ Production du rapport (csv)
- ▷ Visualisation des témoins

Double chaîne DTVT

**SECURE**  
DATA VALIDATION

*data + data model*

Pro B<sup>TM</sup> → verification → formal compliance

PREDICATE model animator → confirmation

Work in progress ....

Project: project, Version: 1

Metrics: Files: 22, Declarations: 450, Values: 2527, Properties: 22, Definitions: 0

Status: Project file: OK, Errors: 3, Completed: 36%

Property Steps ProB PredicateB

Property	Steps	ProB	PredicateB
1 DTVTR_v1.6.1/AL+10/Rule_DB_ALA_0001.xml	Rule_DB_ALA_0001		✗
2 DTVTR_v1.6.1/AL+10/Rule_DB_ALA_0002.xml	Rule_DB_ALA_0002		✓
3 DTVTR_v1.6.1/AL+10/Rule_DB_ALA_0003.xml	Rule_DB_ALA_0003		✗
4 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0001.xml	Rule_DB_ATCEQUIP_0001		✓
5 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0002.xml	Rule_DB_ATCEQUIP_0002		✓
6 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0003.xml	Rule_DB_ATCEQUIP_0003		✓
7 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0004.xml	Rule_DB_ATCEQUIP_0004		✓
8 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0006.xml	Rule_DB_ATCEQUIP_0006		⚠
9 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0008.xml	Rule_DB_ATCEQUIP_0008		work
10 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0010.xml	Rule_DB_ATCEQUIP_0010		
11 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0011.xml	Rule_DB_ATCEQUIP_0011		
12 DTVTR_v1.6.1/AL+10/Rule_DB_ATCEQUIP_0012.xml	Rule_DB_ATCEQUIP_0012		
13 DTVTR_v1.6.1/AL+10/Rule_DB_RIO_0003.xml	Rule_DB_RIO_0003		
14 DTVTR_v1.6.1/AL+10/Rule_DB_RIO_0005.xml	Rule_DB_RIO_0005		
15 DTVTR_v1.6.1/AL+10/Rule_DB_RIO_0006.xml	Rule_DB_RIO_0006		
16 DTVTR_v1.6.1/AL+10/Rule_DB_ROUTE_0002.xml	Rule_DB_Route_0002		
17 DTVTR_v1.6.1/AL+10/Rule_DB_ROUTE_0003.xml	Rule_DB_Route_0003		
18 DTVTR_v1.6.1/AL+10/Rule_DB_SIGAREA_0001.xml	Rule_DB_SIGAREA_0001		
19 DTVTR_v1.6.1/AL+10/RCD_Track_Container_0001.xml	Rule_RCD_Track_Container_0001		
20 DTVTR_v1.6.1/AL+10/Rule_CBTC_SPEED.xml	Rule_CBTC_SPEED		

powered by 



## ► En projet

### ► Théorique

- Prise en compte des réels/flottants dans les preuveurs
- Intégration plus fine avec pro-B
- Règles (Prouver interactif, recherche ...)
- Représentation graphique d'un modèle (équivalence)

### ► Pratique

- Service de gestion d'un pool de serveur.
- Gestion des modèles en conf par l'atelierB
- Amélioration de l'interfaçage GOP générique avec l'éditeur
- Génération de code : VHDL, Ladder, c, assemebleur