



# AtelierB

## Captronic

### 01 octobre 2013

**ClearSy**  
contact@clearsy.com

Téléphone :  
04.42.37.12.70  
01.40.28.14.57

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.

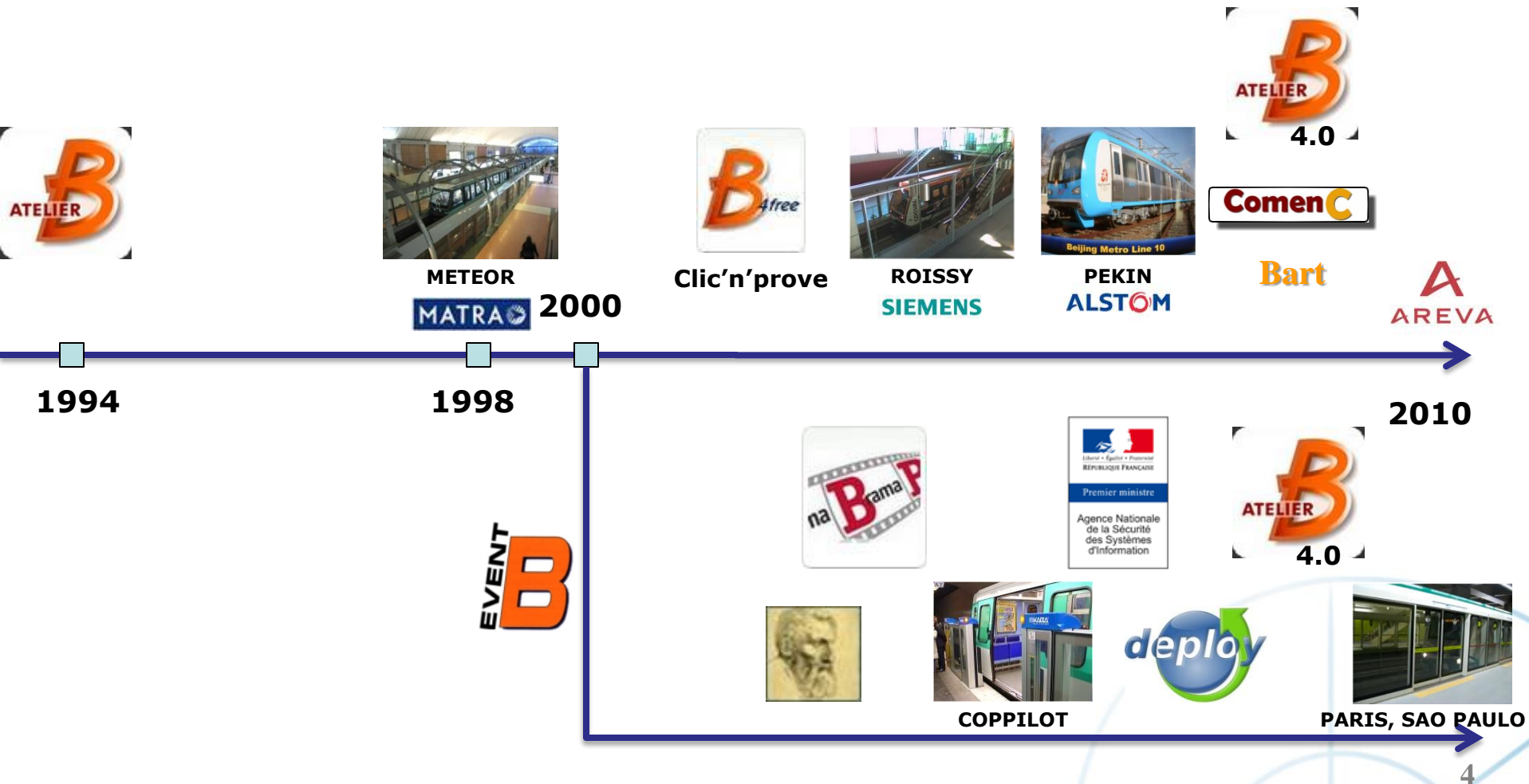


▷ Ces fonctionnalités se regroupent en quatre catégories :

- 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





# ► 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

**ATELIER B** " COMPUTER AIDED SOFTWARE ENVIRONMENT...  
ATELIER DE GENIE LOGICIEL "

ACCUEIL ACTUALITES ATELIER B TÉLÉCHARGEMENTS FORMATION B SUPPORT RÉFÉRENCES LIENS CONTACT

**TÉLÉCHARGER L'ATELIER B**

► **ATELIER B EN TÉLÉCHARGEMENT GRATUIT**

► La nouvelle licence Atelier B 4

► Atelier B 4.1 Community Edition

La nouvelle licence est associée à l'Atelier B V4, distribué gratuitement depuis ce site, à tous ceux désirant utiliser l'Atelier B à des fins de recherche, d'enseignement et de développement de projets industriels. Elle est attribuée dès la première utilisation de l'outil pour une durée illimitée.

- Atelier B 4.1 – Windows
- Atelier B 4.1 – Linux Rpm
- Atelier B 4.1 – Linux Debian
- Atelier B 4.1 – Mac OS

FRANÇAIS

**REJOIGNEZ-NOUS**

► CLEARSY RECRUTE !

**PROJETS R&D / OPEN SOURCE**

- MANUELS
- PROJETS OPEN SOURCE
- 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/> :



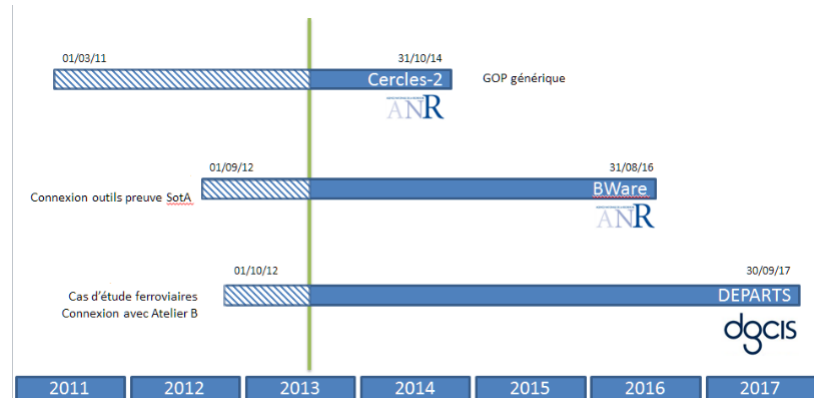
- ▶ Les autres outils (MS, krt, TC, PO, PR) restent fermés :  
Validation/Qualification des modifications



# ► 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



SHUTTLE  
ROISSY AIRPORT  
Paris



L1  
Algiers



L2 L3  
Sao Paulo



Mexico



Airport Express  
Hong Kong



Madrid



New York  
Canarsie



L3  
Paris



Lille

L9  
Seoul



L9  
Barcelona



Istanbul

L2  
Budapest



Toronto



Metro L10  
Beijing



Circle Line  
Singapore



San Juan



Metro  
Lausanne



L1 L2  
Malaga



L5  
Milano



Delhi



METEOR L14  
Paris



KVB  
6000 trains  
France



1990

2000

2010 0

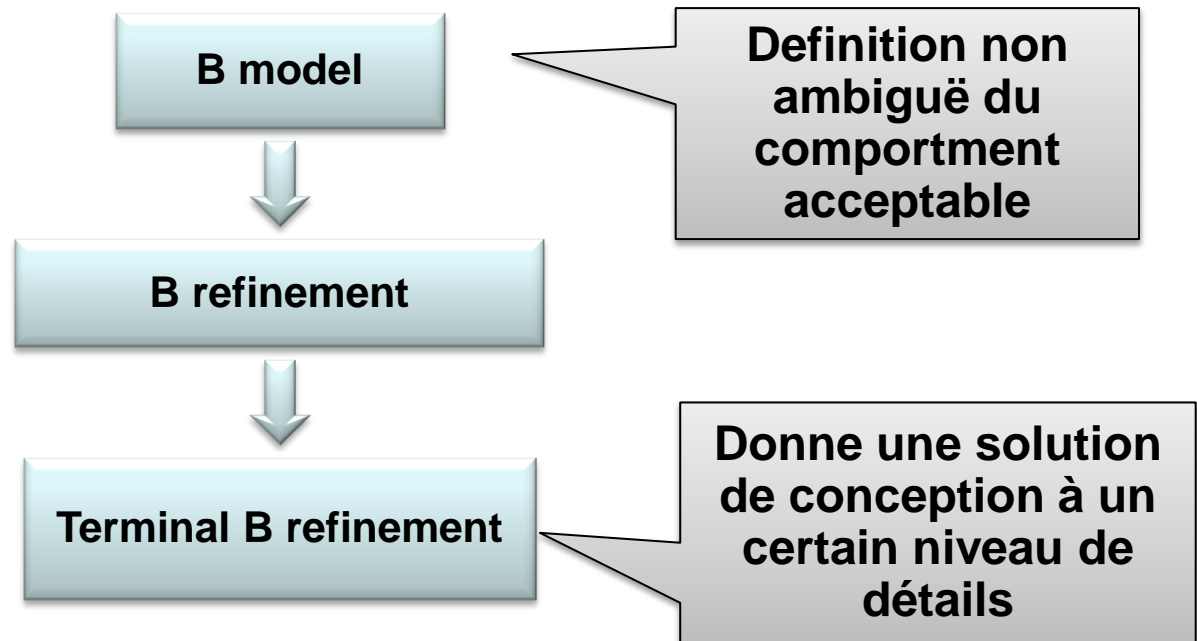


## ► B évènementiel / B système

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

### ▷ Basé sur la Méthode B :

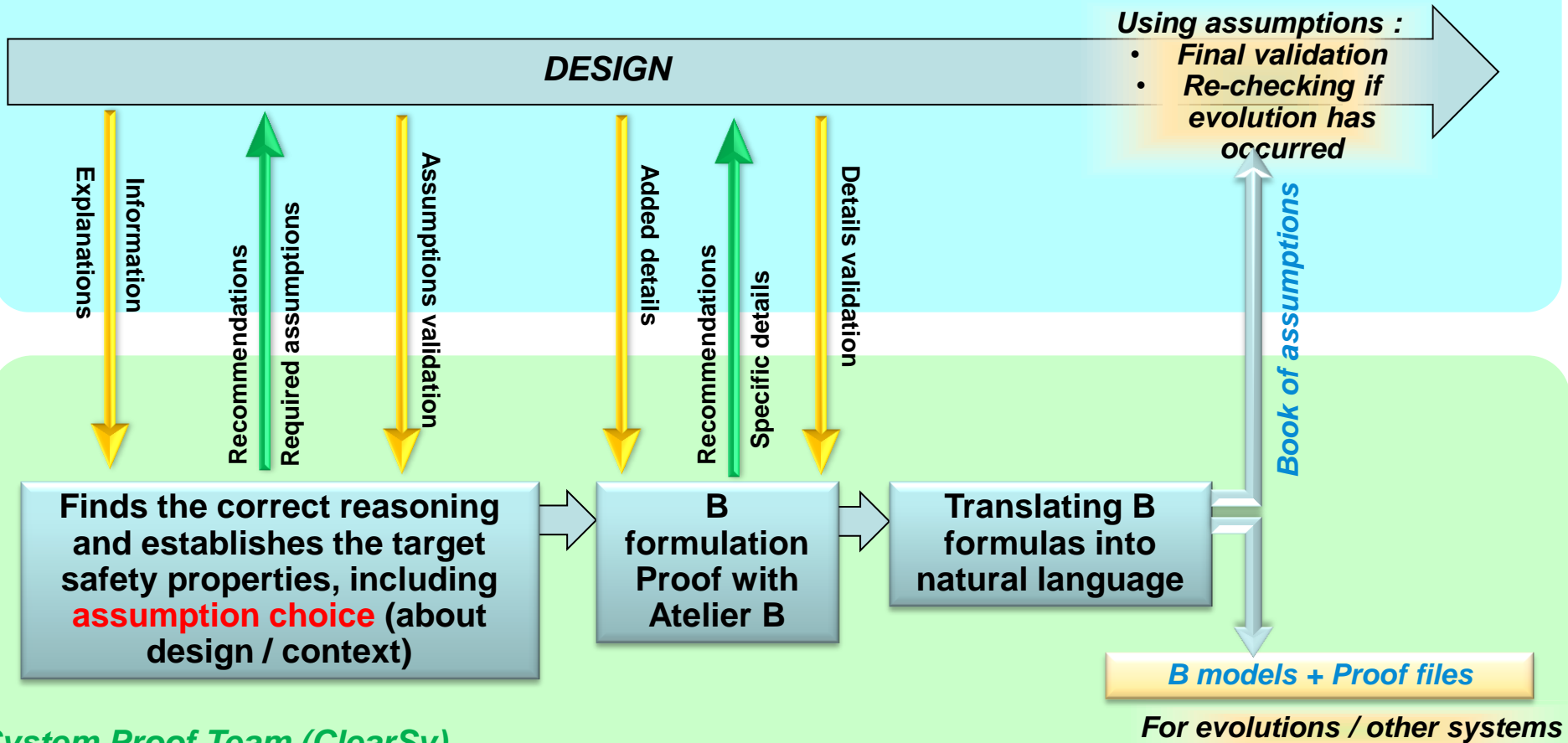
- Formalisme
- Preuve
- Raffinement





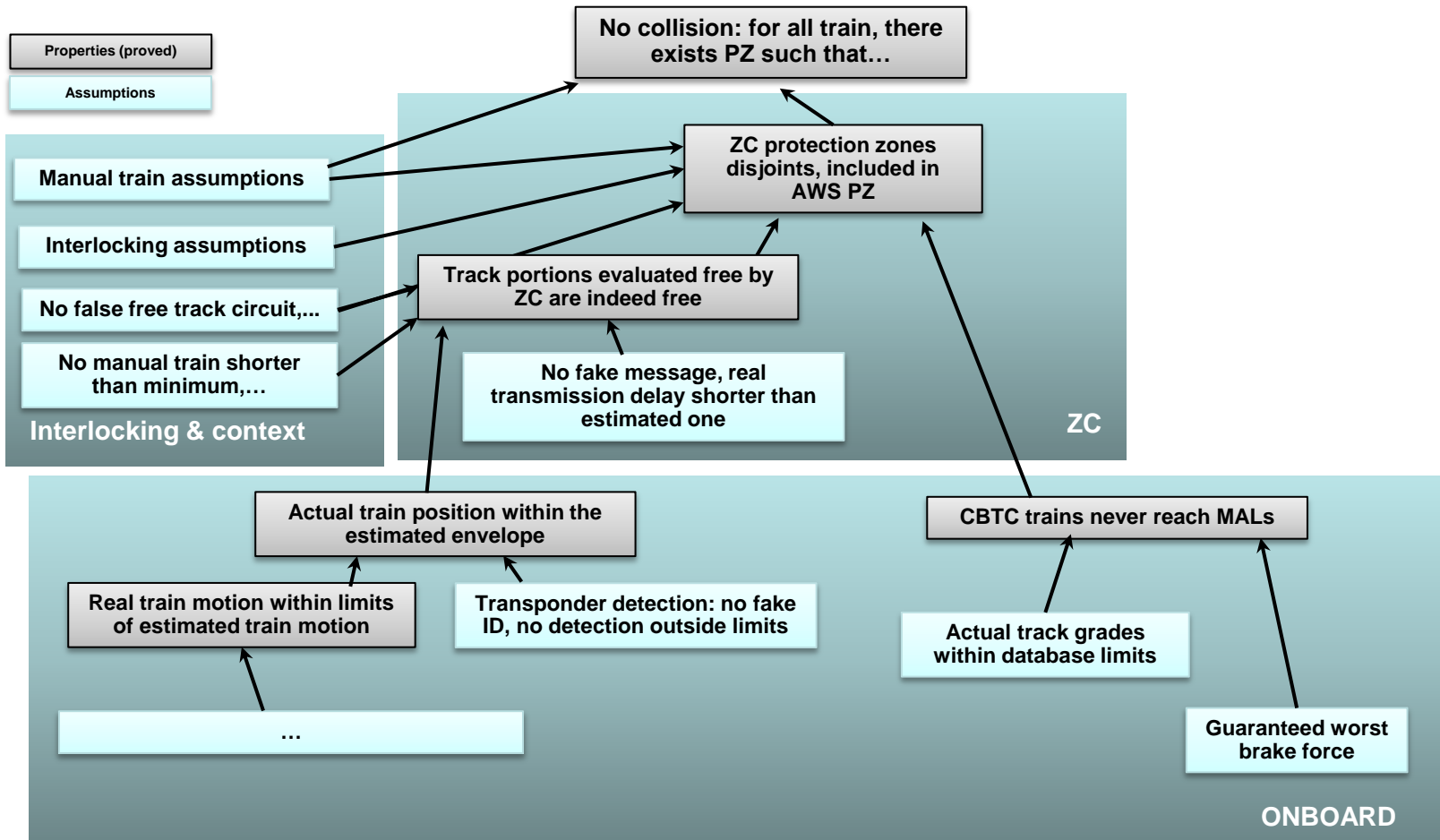
# ▶ Flushing line (New York)

**Project Team (THALES / NYCT)**





# ► 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 paramétrer 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

**uevol\_ctrl\_minabis\_1\* - Atelier B**

Project: uevol\_ctrl\_minabis\_1\*

Filter: \* (10.2.8)

- vesg\_abstract\_model.def
- vesg\_arith\_type.mch
- vesg\_arith\_type\_accel.mch
- vesg\_arith\_type\_coord.mch
- vesg\_arith\_type\_coord\_min.ma...
- vesg\_arith\_type\_gradient.mch
- vesg\_arith\_type\_int.mch
- vesg\_arith\_type\_square\_speed...
- vesg\_bad.mch
- vesg\_bad\_1.mch
- vesg\_bad\_1\_iimp
- vesg\_bad\_1\_iimp
- vesg\_beacon.mch
- vesg\_beacon\_1.mch
- vesg\_beacon\_1\_iimp
- vesg\_beacon\_2.mch
- vesg\_beacon\_2\_iimp

Outline: Expand Collapse

Pragmas

Requirement CC\_ATP-A401464-SwRS-1292-1

Original document: Document.doc

Body:

```
Other CC Synchro Report Minabis Distance Counter for end 1(Cycle)
| Value on condition
| Case
| | 0
| | Initialization
```

Comment: ctrl\_MINABIS\_counter\_end1 = Other CC Synchro Report Minabis Distance Counter for end 1 (Cycle)

Specifications

Specification	%
10_2's Requirements (10.2.8)	95.4225%
CC_ATP-A401464-SwRS-1293	100%
CC_ATP-A401464-SwRS-1292	100%
CC_ATP-A401464-SwRS-1292-2	100%
CC_ATP-A401464-SwRS-1292-1	100%
CC_ATP-A401464-SwRS-1291	100%
CC_ATP-A401464-SwRS-1290	100%
CC_ATP-A401464-SwRS-1289	100%
CC_ATP-A401464-SwRS-1271	100%
CC_ATP-A401464-SwRS-1270	100%
CC_ATP-A401464-SwRS-1269	100%
CC_ATP-A401464-SwRS-1268	100%
CC_ATP-A401464-SwRS-1267	100%
CC_ATP-A401464-SwRS-1266	100%
CC_ATP-A401464-SwRS-1265	100%
CC_ATP-A401464-SwRS-1264	100%
CC_ATP-A401464-SwRS-1263	100%
CC_ATP-A401464-SwRS-1262	0%
CC_ATP-A401464-SwRS-1261	100%
CC_ATP-A401464-SwRS-1258	100%
CC_ATP-A401464-SwRS-1257	66.6667%
CC_ATP-A401464-SwRS-1256	100%
CC_ATP-A401464-SwRS-1255	100%
CC_ATP-A401464-SwRS-1254	100%
CC_ATP-A401464-SwRS-1253	100%
CC_ATP-A401464-SwRS-1251	100%
CC_ATP-A401464-SwRS-1250	100%
CC_ATP-A401464-SwRS-1249	100%
CC_ATP-A401464-SwRS-1248	100%
CC_ATP-A401464-SwRS-1247	100%
CC_ATP-A401464-SwRS-1246	100%
CC_ATP-A401464-SwRS-1245	100%
CC_ATP-A401464-SwRS-1244	100%
CC_ATP-A401464-SwRS-1241	100%

Line: 137 Column: 1



# 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      verification  
PREDICATE model animator      formal compliancy  
confirmation

**Verify**  
Work in progress ....

	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		

**Project**

Name project

Version 1

**Metrics**

Files 22

Declarations 450

Values 2527

Properties 22

Definitions 0

**Status**

Project file OK

Errors 3

Completed  36%

powered by



## ▶ En projet

### ▷ Théorique

- ▶ Prise en compte des réels/flottants dans les prouveurs
- ▶ 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, assembleur