



AtelierB

RAIM2013

19 novembre 2013

ClearSy
contact@clearsy.com

Téléphone :
04.42.37.12.70
01.40.28.14.57

www.clearsy.com

RAIM2013/AtelierB

1 | SYSTEM ENGINEERING
WWW.CLEARSY.COM

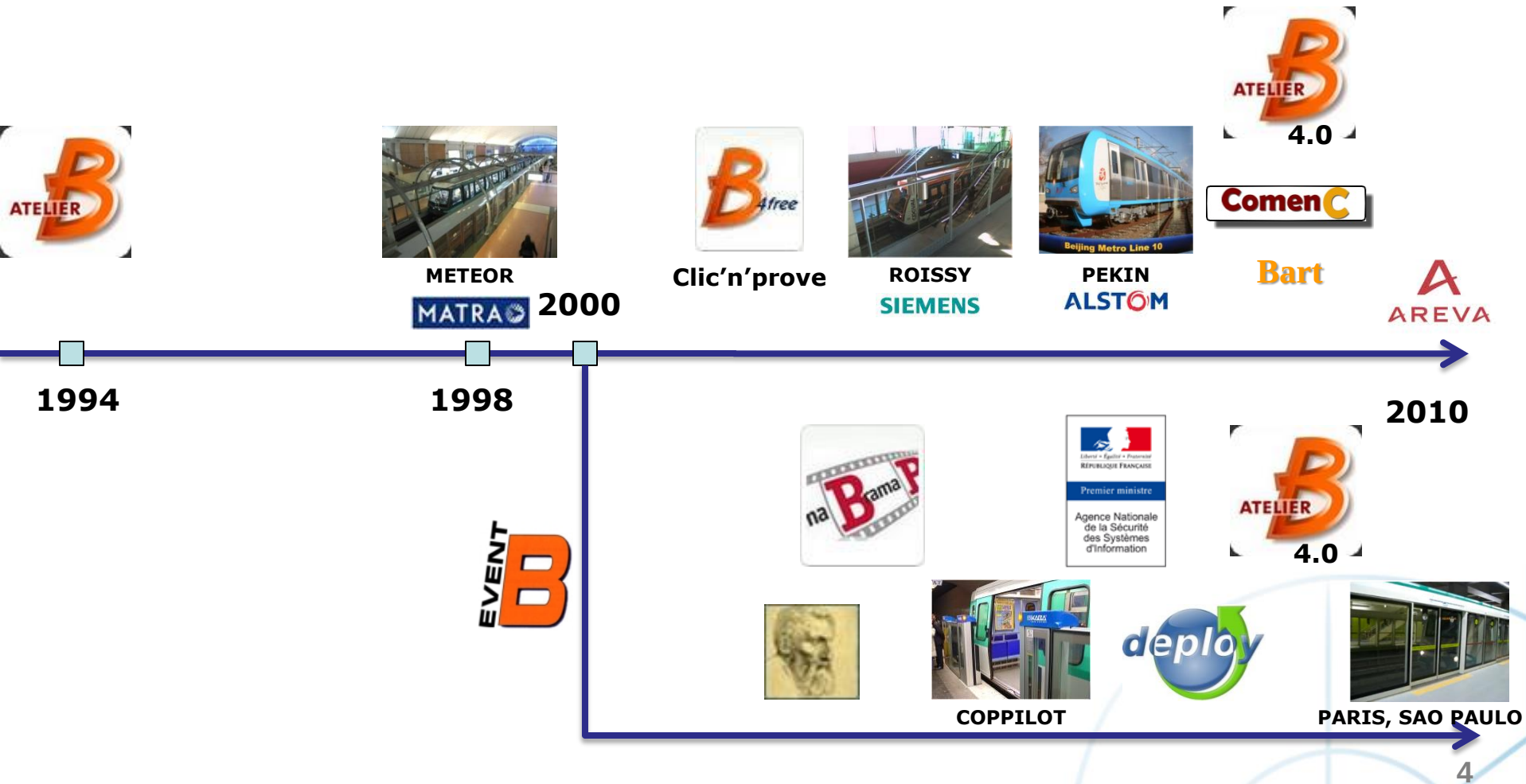


► Sommaire

- ▷ Résumé des dernières années
- ▷ Politique de distribution source et budget
- ▷ Atelier : Présentation générale des versions
- ▷ Utilisation des versions V4.X
 - ▶ Projet : développement logiciel
 - ▶ Projet : développement système
 - ▶ Projet : de validation de donnée
- ▷ Développement en cours
- ▷ Développement envisagé



Résumé des dernières années





Some implementations (B)



L1
Paris



SHUTTLE
ROISSY AIRPORT
Paris



L1
Algiers



NY
Flushing

L2 L3
Sao Paulo



Mexico



Airport Express
Hong Kong



New York
Canarsie



L3
Paris



Lyon

L9
Seoul



L9
Barcelona



Istanbul

L2
Budapest



Toronto



Madrid



Metro L10
Beijing



Circle Line
Singapore



KVB
6000 trains
France



METEOR L14
Paris



San Juan



Delhi



Metro
Lausanne



L1 L2
Malaga



L5
Milano



1990

2000

2010



Some implementations (microelectronics)

AT90SC12872RCFT

Low-power, high-performance, 8-/16-bit secure cryptocontroller with 128 Kbytes ROM and 72 Kbytes EEPROM. Security Features: OTP (One Time Programmable) EEPROM area, RNG (Random Number Generator), "out of bounds" detectors, side channel attack countermeasures. Hardware DES/TDES, 32-bit Cryptographic Accelerator, CRC, ISO 14443 Type B contactless interface and ISO 7816 contact interface, Common Criteria EAL5+ and EMVCo Certifications.

**Secure
microcontroller
ST19NA18
ST19NT66A
EAL5+
ST**

**Secure
microcontroller
ST23YR80
SA23YR80
EAL5+
ST**

**Secure
microcontrollers
ATS90SC6404
ATS90SC12872
EAL5+
Atmel**

**Secure
microcontroller
ST23YL80
ST23YL18
EAL5+
ST**

**Secure
microcontroller
ST19WR08
ST19WR66
ST19NR66
EAL5+
ST**

**Secure
microcontrollers
ATS90SC12872R
ATS90SC12836R
EAL5+
Atmel**

**Microcircuits
ST19WP
ST19WL
EAL5+
ST**

**Secure
microcontrollers
AT90SC20818
AT90SC13612
AT90SC24036
EAL5+
Atmel**

**Microcircuit
ST22L128
EAL5+
ST**

**Secure
microcontrollers
ATS90SC6404A
ATS90SC12872A
EAL5+
Atmel**

STMicroelectronics announced that the established [ST22L128 32-bit secure microcontroller](#) has received 'Common Criteria' security certification at [Evaluation Assurance Level EAL5+](#) (Augmented). The formal recognition will now enable 3G network operators to extend their secure mobile services with M-commerce and digital signature applications, and will provide new opportunities in banking and ID market segments.

1998

2000

2002

2004

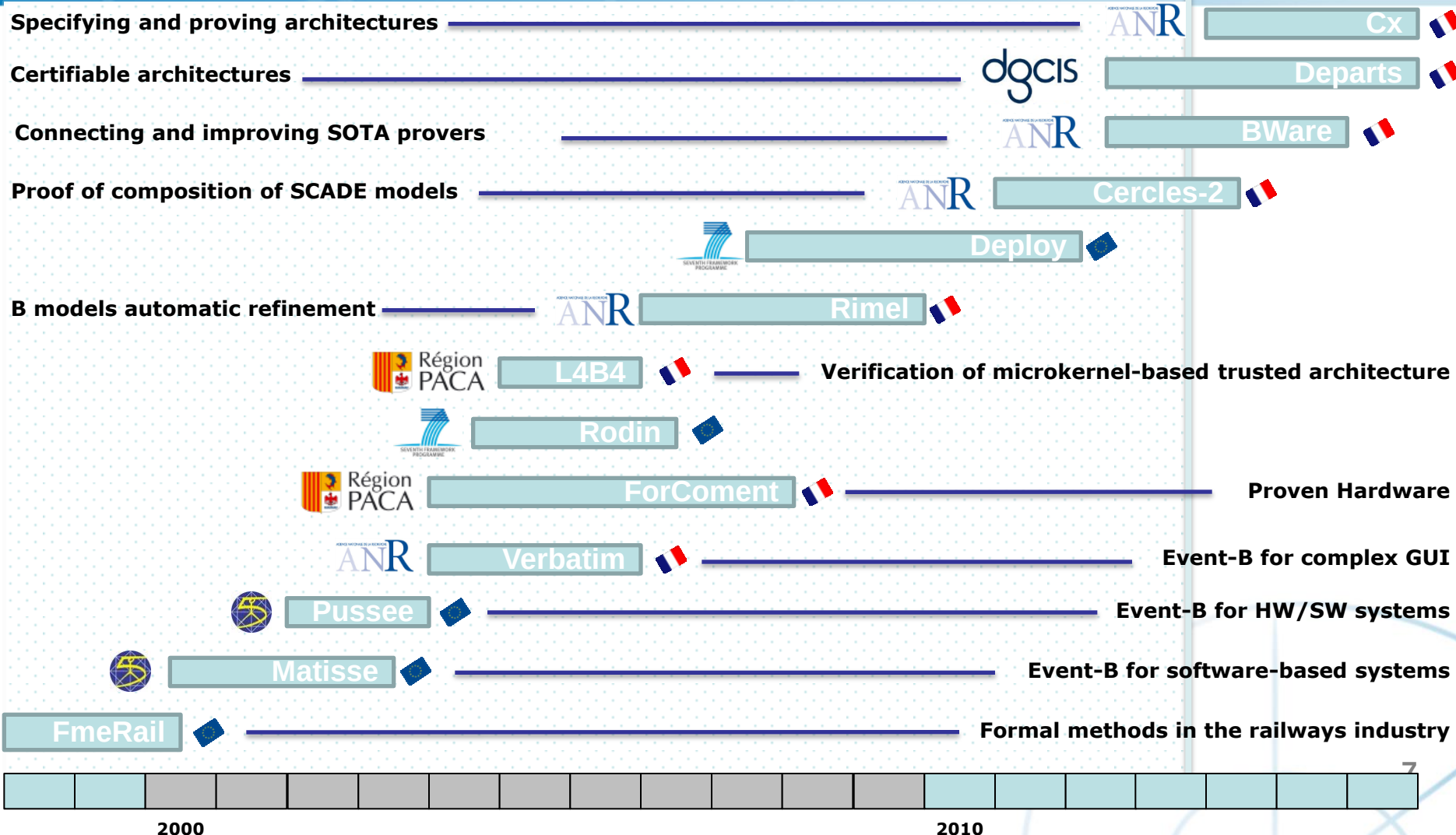
2006

2008

2010 ⁶



Projet de R&D public





► 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 ACTUALITÉS 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/> :



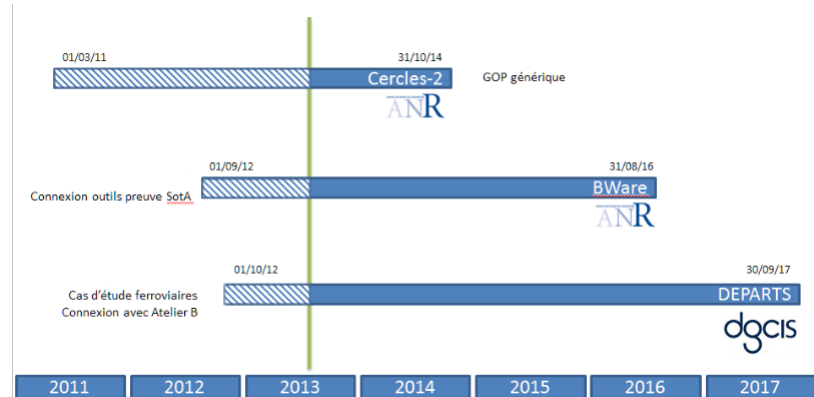
- ▶ Les autres outils (MS, krt, TC, PO, PR) restent fermés :
Validation/Qualification des modifications



► 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



► AtelierB V 4.1.0

▷ AtelierB V 4.1.0 :

- Ajout du type de projet « génération de données »
- Support amélioré des entiers (choix de la valeur max)
- Support expérimental des nombres réels et des flottants
- Ajout d'une vue graphique pour le statuts des composants
- Outil de preuve de règles
- Amélioration de l'interface du prouveur interactif
- Amélioration de l'éditeur
- Localisation de l'interface graphique en Anglais, Français, Japonais et Portugais.



► AtelierB V4,1,1

▷ AtelierB V 4.1.1 :

- Version de correction d'anomalie
- Modification des opérateurs réel
- Correction et amélioration sur BART
- Rajout de la vérification sur les règles de preuve

- Utilisé actuellement



► 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 mètres 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)

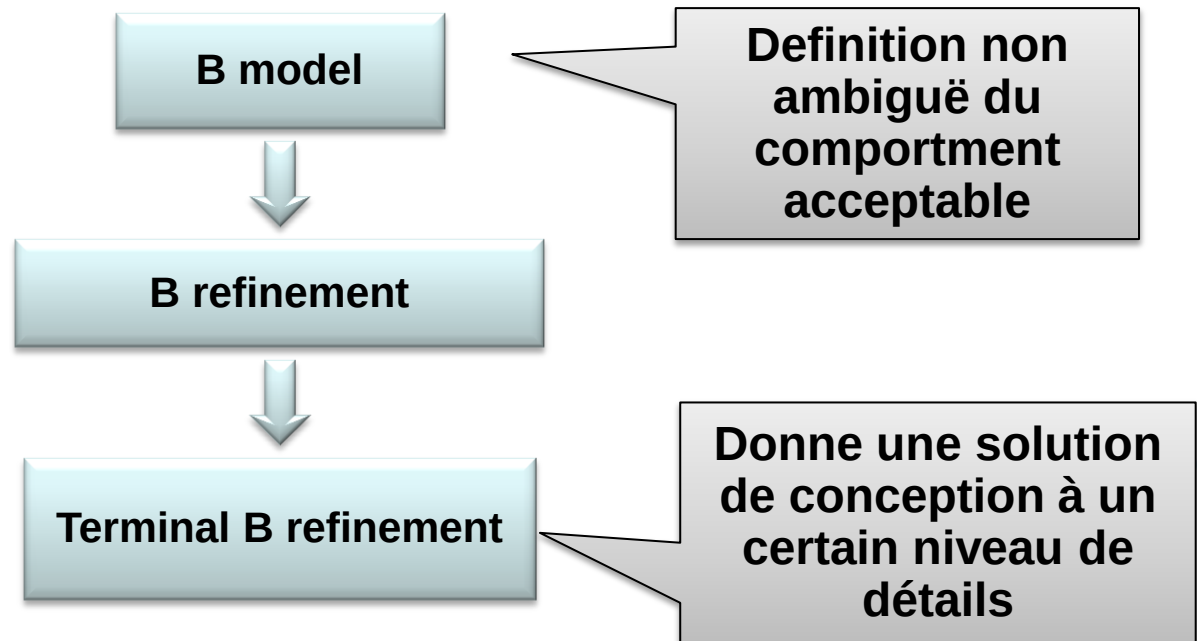


► B évènementiel / B système

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

▷ Basé sur la Méthode B :

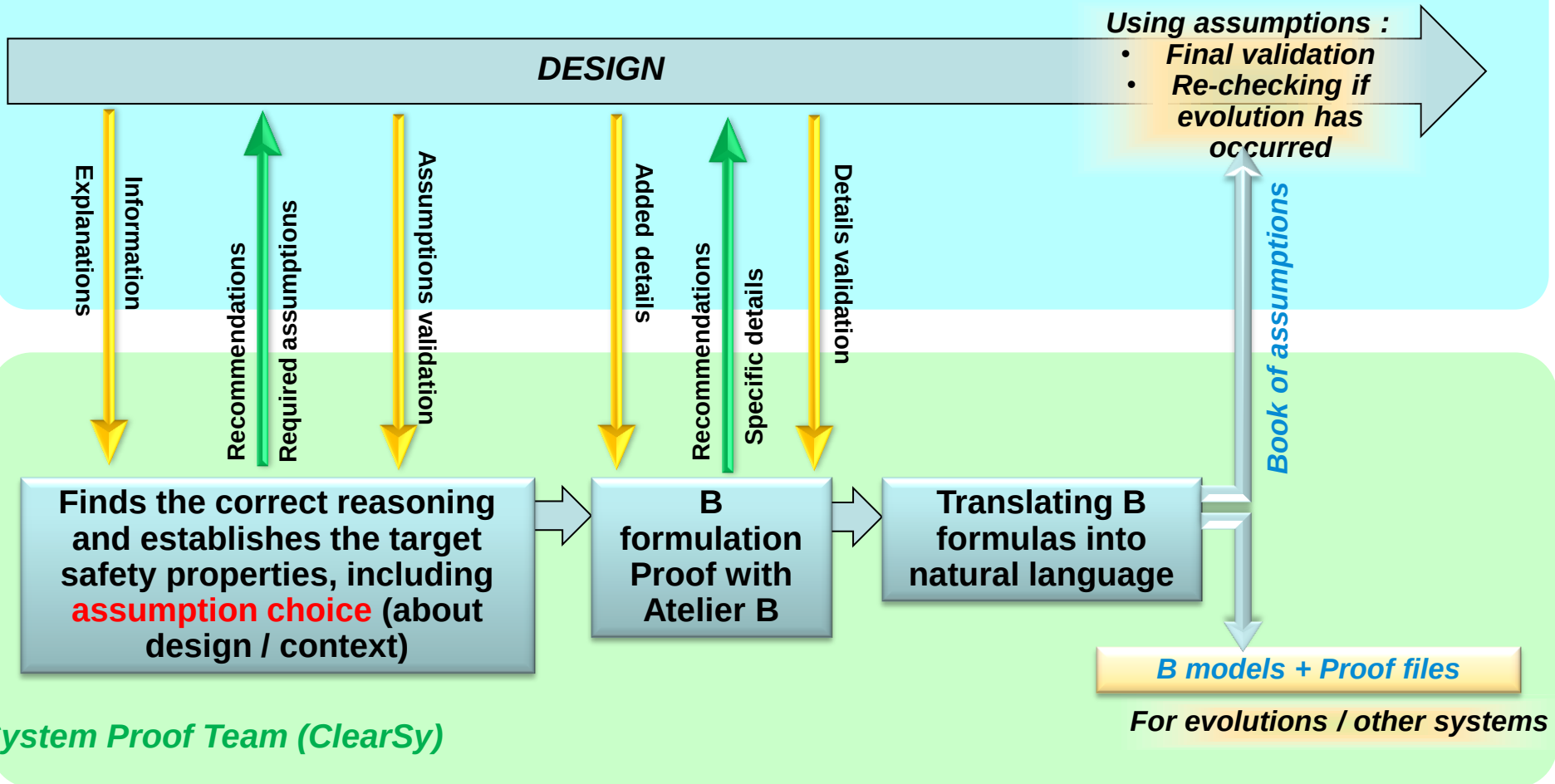
- Formalisme
- Preuve
- Raffinement





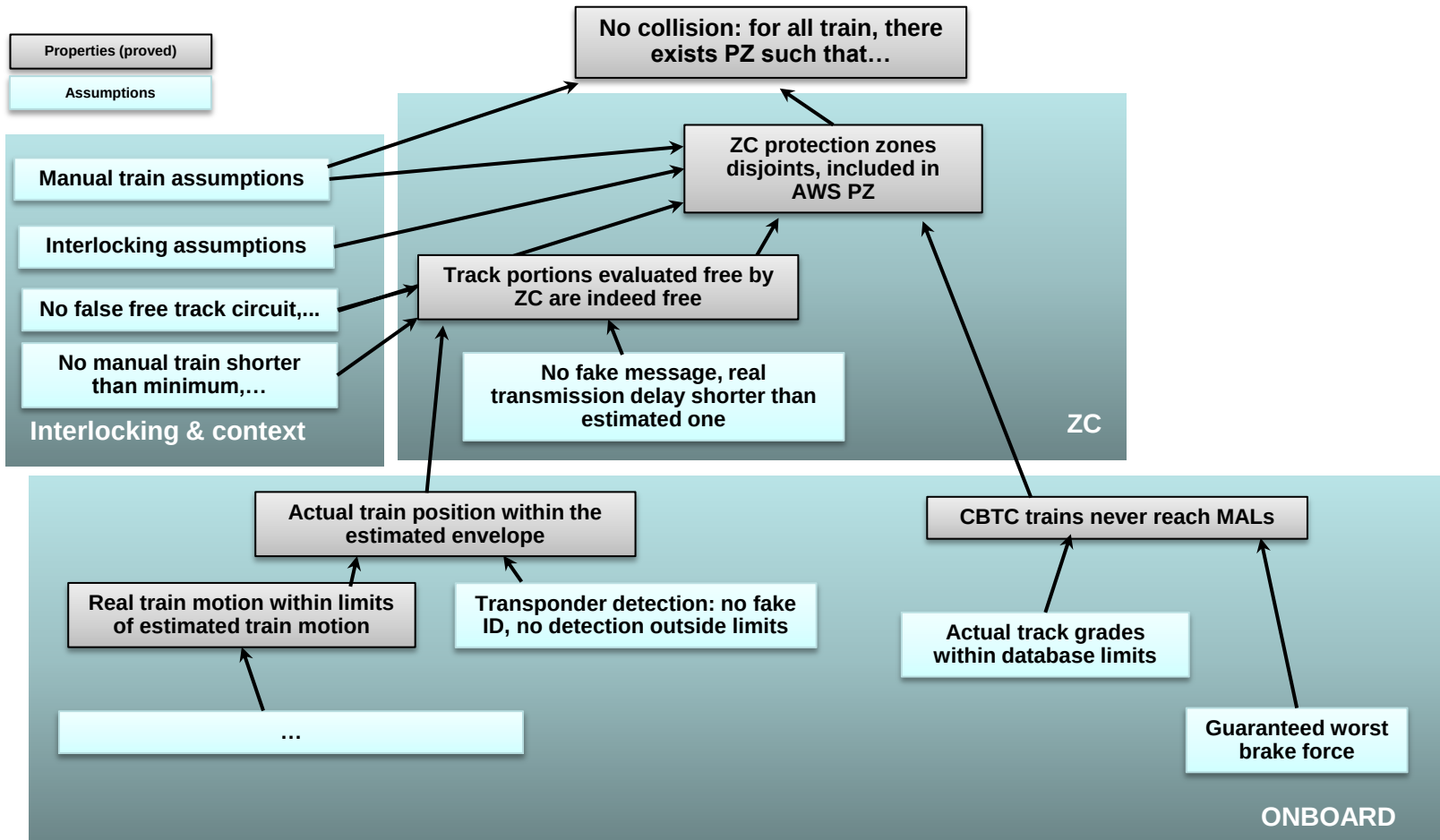
▶ Flushing line (New York)

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.
 - Disparition de certaine PO
- ▶ Interfaçage avec plusieurs Prouveurs
- ▶ Outils de liens Exigence/Modèle B
- ▶ Gestion du 64 bits
- ▶ Améliorer le rajout de plug-in



▶ 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)
- ▶ BART (les conflits, Méta règles donnée, heuristiques substitution, preuve)

▷ Pratique

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