



Méthodes formelles et langages pour le
développement de logiciel fiables dans
l'industrie

Méthode B:Flushing (NY)

28 Avril 2014

ClearSy
contact@clearsy.com

Téléphone :
04.42.37.12.70
01.40.28.14.57

www.clearsy.com

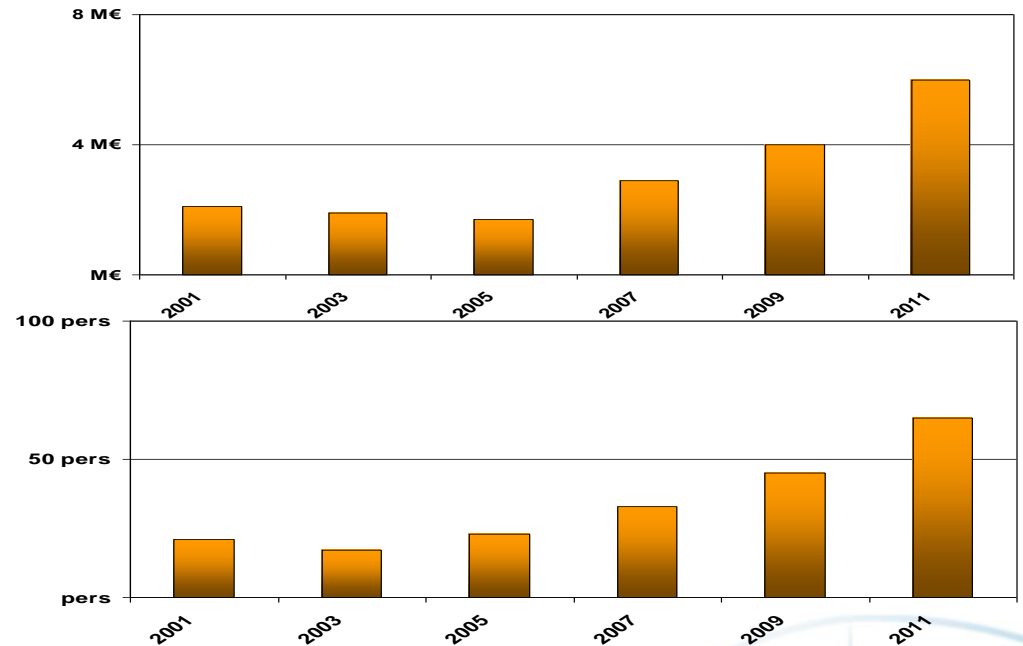
B Flushing

1 | SYSTEM ENGINEERING
WWW.CLEARSY.COM



Présentation

CLEARSY



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



Some implementations (B)



L1 Paris



L1 Algiers



NY Flushing

SHUTTLE ROISSY AIRPORT Paris



L2 L3 Sao Paulo



New York Canarsie



L3 Paris



Lyon

Mexico



Airport Express Hong Kong



L9 Seoul



L9 Barcelona



Istanbul

L2 Budapest



Toronto



Madrid



San Juan



Metro L10 Beijing



Circle Line Singapore



KVB 6000 trains France



METEOR L14 Paris



Delhi



Metro Lausanne



L1 L2 Malaga



L5 Milano



1990

2000

2010

B Flushing

3

SYSTEM ENGINEERING
WWW.CLEARSY.COM

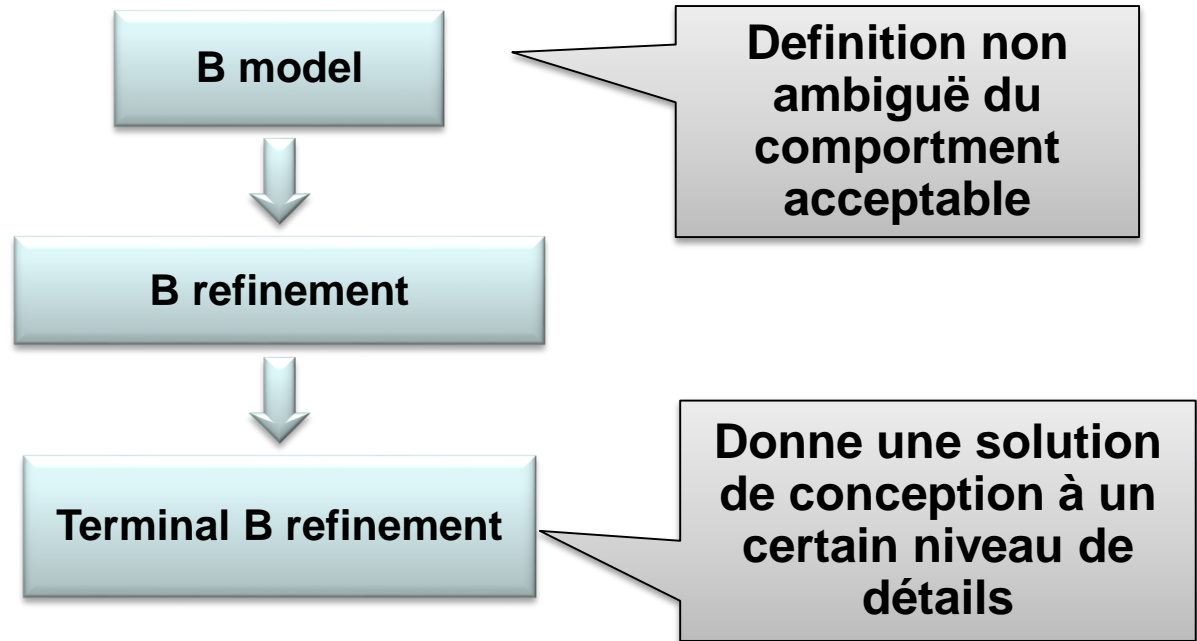


▶ B évènementiel / B système

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

▷ Basé sur la Méthode B :

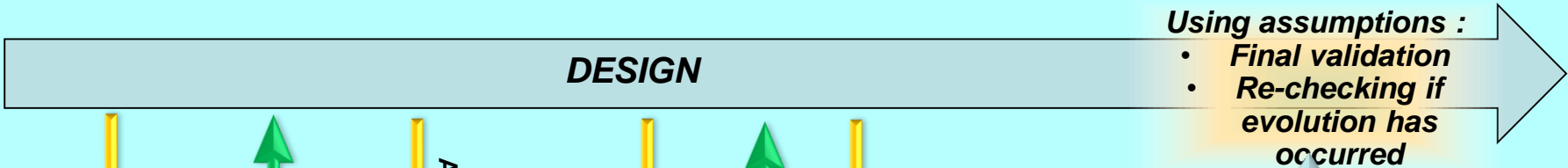
- ▶ Formalisme
- ▶ Preuve
- ▶ Raffinement





▶ Flushing line (New York)

Project Team (THALES / NYCT)



Explanations
Information

Recommendations
Required assumptions

Assumptions validation

Added details

Recommendations
Specific details

Details validation

Book of assumptions

1/6

Finds the correct reasoning and establishes the target safety properties, including **assumption choice** (about design / context)

B formulation
Proof with Atelier B

Translating B formulas into natural language

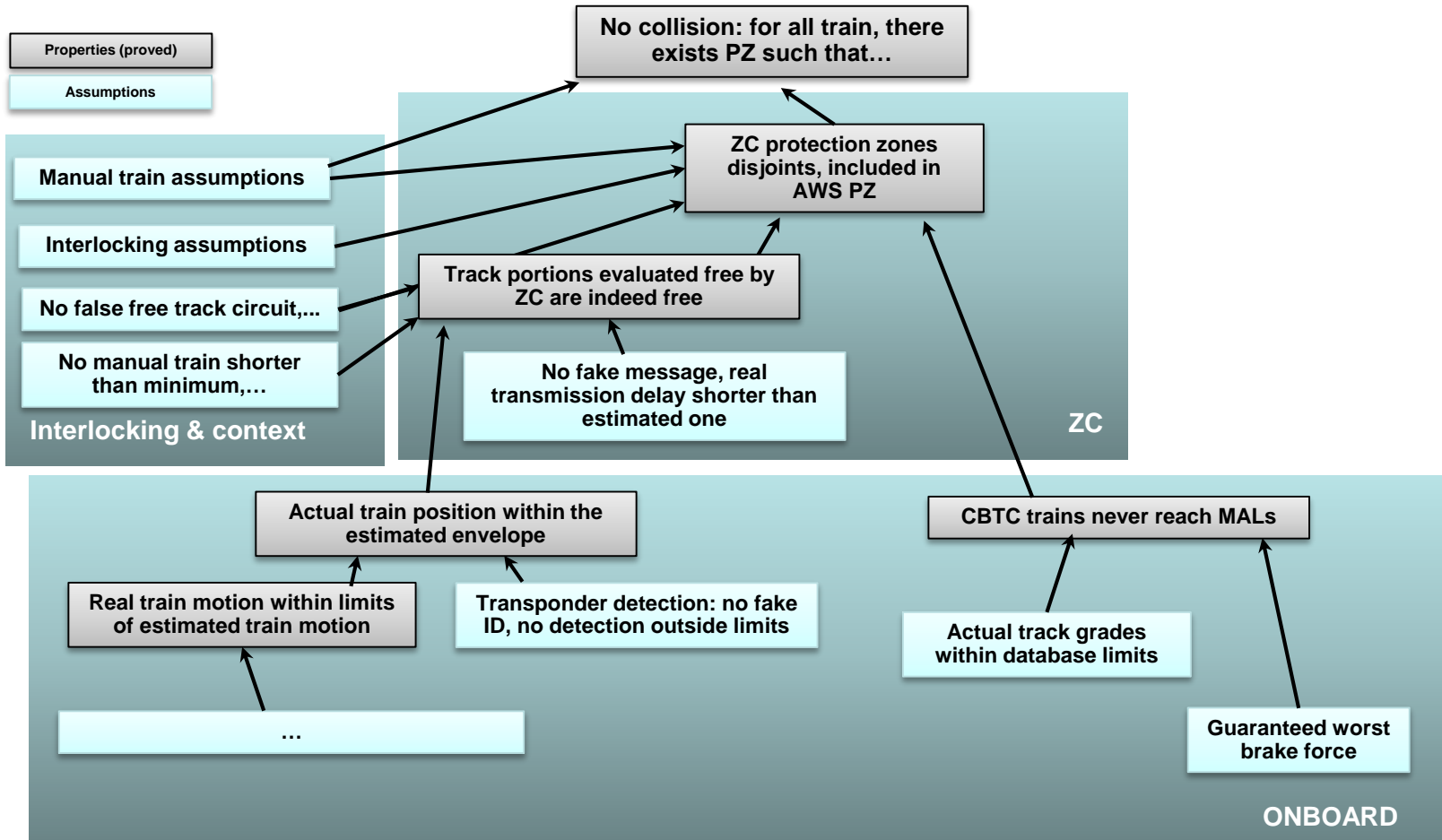
B models + Proof files

For evolutions / other systems

System Proof Team (ClearSy)



▶ Properties & sub-properties





▶ Répartition du temps

Project Team (THALES / NYCT)

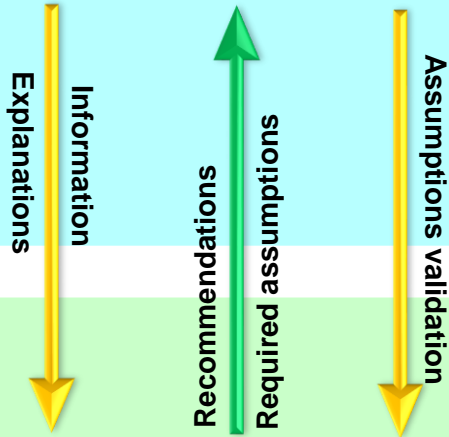
1/2

1/3

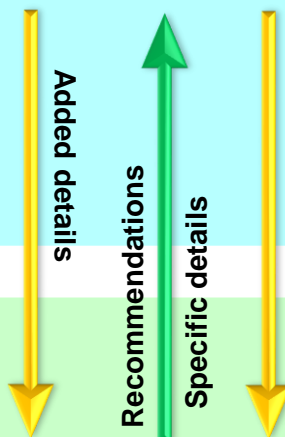
Using assumptions :

- Final validation
- Re-checking if evolution has occurred

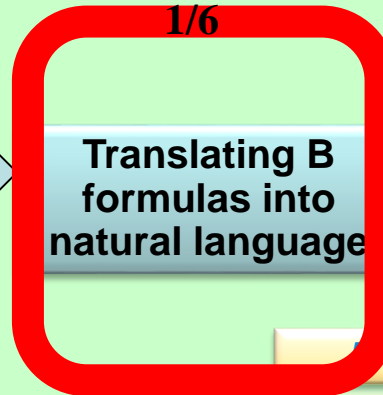
DESIGN



Finds the correct reasoning and establishes the target safety properties, including **assumption choice** (about design / context)



B formulation Proof with Atelier B



Book of assumptions

models + Proof files

For evolutions / other systems

System Proof Team (ClearSy)



Choisir de faire une preuve formelle système

Critères (d'après nous...)

- ▷ Besoin d'une garantie de sécurité globale
- ▷ Besoin d'avoir exprimées toutes les conditions nécessaires à la sécurité et le "pourquoi c'est sécuritaire".

On sait que c'est assez rigoureux pour être formalisé seulement si on l'a formalisé

- ▷ La résistance d'une chaîne est celle du maillon le plus faible

Utiliser les méthode formelles pour renforcer un maillon ou pour démontrer qu'il n'y a pas de maillon faible

