Approche formelle pour la réalisation d'un système sécuritaire de contrôle commande de façades de quais

Guilhem Pouzancre

03 mai 2006

ClearSy
Contact@Clearsy.com

20 rue Joubert
75 009 Paris

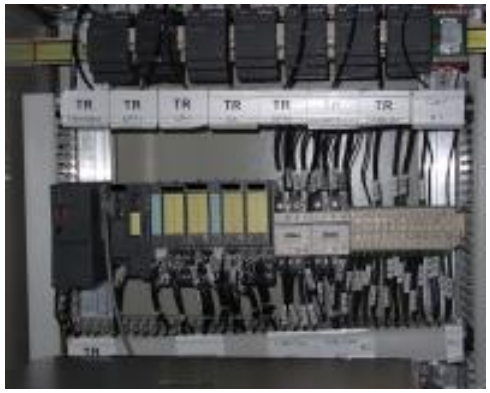
Téléphone : 01.53.25.97.79
www.clearsy.com

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

COPPILOT et Façades de Quai

- La RATP teste en exploitation les « façades de quai mi-hauteur »
- COPPILOT est le système de commande d'ouverture et de fermeture des portes des façades



AFIS Association Française d'Ingéniarie Système

CLEARSY SYSTEM ENGINEERING

Plan de la présentation

- Les responsabilités de ClearSy
- Présentation technique de COPPILOT
- Le processus d'ingénierie utilisé : centré sur la méthode B

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

ClearSy maître d'œuvre de COPPILOT pour la RATP

- **Responsabilités de ClearSy :**
  - ✓ Engagement au forfait sur résultat : délais, sécurité et disponibilité
  - ✓ Choix de l'architecture système et des fournisseurs
  - ✓ Commande et réception du matériel
  - ✓ Développement des logiciels de niveau de sécurité SIL 3
  - ✓ Installation, maintenance et retrait de COPPILOT
  - ✓ Démonstration de sécurité

- **Trois systèmes installés sur la ligne 13**
  - ✓ Stations : Invalides, St Lazare Quai 1 et St Lazare Quai 2
  - ✓ Trois constructeurs de façades différents : CNIM, Faiveley, Kaba

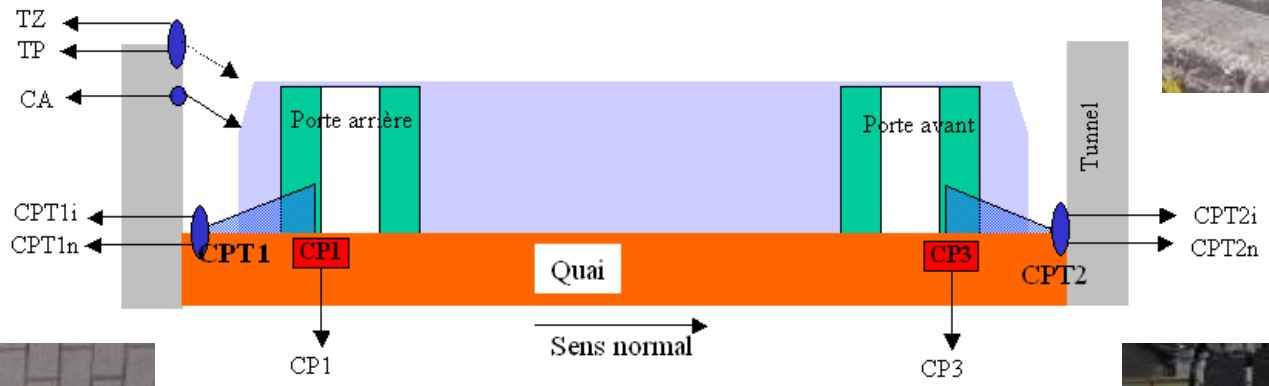
AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Capteur d'arrêt du train CA (Radar)

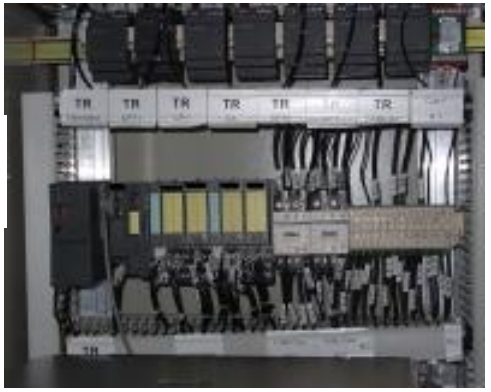
Station Invalides

Capteur de présence CP (IR)



Télémètre (Laser)

Armoire contenant un automate de sécurité et le programme SIL 3



AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Aspects techniques

- **Système de sécurité de niveau SIL 3**
  - ✓ Système de signalisation ferroviaire de sécurité SIL3 selon la norme EN 50129
  - ✓ SIL 3 : Événements redoutés < 10^{-7} occ/heure
  - ✓ Risque majeur : ouverture à tort des portes
  - ✓ Démonstration de sécurité auprès de la RATP : AQL et AQM
  - ✓ Démonstration de sécurité auprès des organismes de tutelle

- **Commande d'ouverture et de fermeture des portes par observation du train**
  - ✓ Utilisation de capteurs industriels du commerce (sans hypothèse de sûreté)
  - ✓ Sauf l'automate : automate industriel SIL 3
  - ✓ Développement d'un logiciel sécuritaire SIL 3

AFIS Association Française d'Ingéniarie Système

CLEARSY SYSTEM ENGINEERING

Contraintes de réalisation et d'installation

- **Conception et installation du système en 10 mois**
  - ✓ Définition de l'architecture système 2 mois
  - ✓ Conception du système et démonstration de sécurité en 4 mois
  - ✓ Installation des 3 quais sur 4 mois

- **Installation sur quais ouverts au public**
  - ✓ Trafic dense : environ 400 trains par jour (toute les 2')
  - ✓ Installation et mise en service sans interruption du trafic

Processus de développement

- **Processus ClearSy :**

Utilisation de l'approche formelle B sur tout le cycle d'ingénierie système

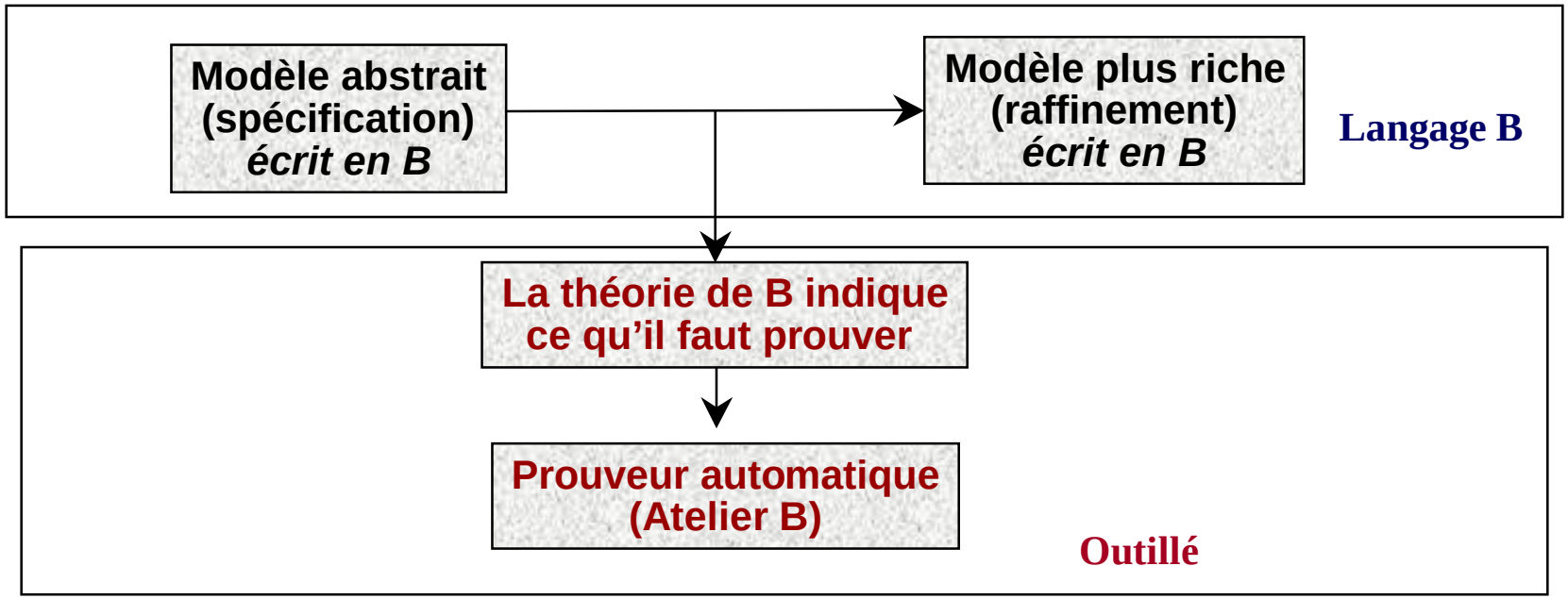
- **Équipe projet**
  - ✓ 1 chef de projet
  - ✓ 1 ingénieur développement
  - ✓ 1 ingénieur sécurité
  - ✓ 1 ingénieur validation

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Principes de B
3 ingrédients : modélisation, raffinement et preuve

Le langage B est basé sur la théorie des ensembles et la logique des prédicats



Apports du langage formel et de la preuve

- Le langage mathématique amène la précision
- Le raffinement amène la structuration des modèles : décomposition, précision, traçabilité, preuve
- Les preuves de propriétés amènent cohérence des fonctions entre elles et la vérification de celles-ci au besoin
- Les preuves de code logiciel : divisions par zéro, boucles, dépassement de tableau, mémoire

Outils utilisés

- COMPOSYS **www.composys.fr**
  - ✓ Outil de modélisation en B des systèmes répartis
  - ✓ Outil de génération de la documentation à partir des modèles B

- **Preuve des modèles B :**
  - ✓ www.B4free.com (version gratuite de l'atelier B pour les universités)
  - ✓ Atelier B : www.atelierb.societe.com

Spécifications formelles : du système jusqu'au code

Spécifications fonctionnelles du système

Portes – Trains - Voyageurs

Évitement des événements redoutés

Preuves de cohérence

Chaîne B

Étude commandée par la RATP avant la consultation

Façades de quai

Spécifications détaillées de COPPILOT

Spécifications logiciel

Conception logiciel

Logiciel SIL3 : Traduction du B en LADDER

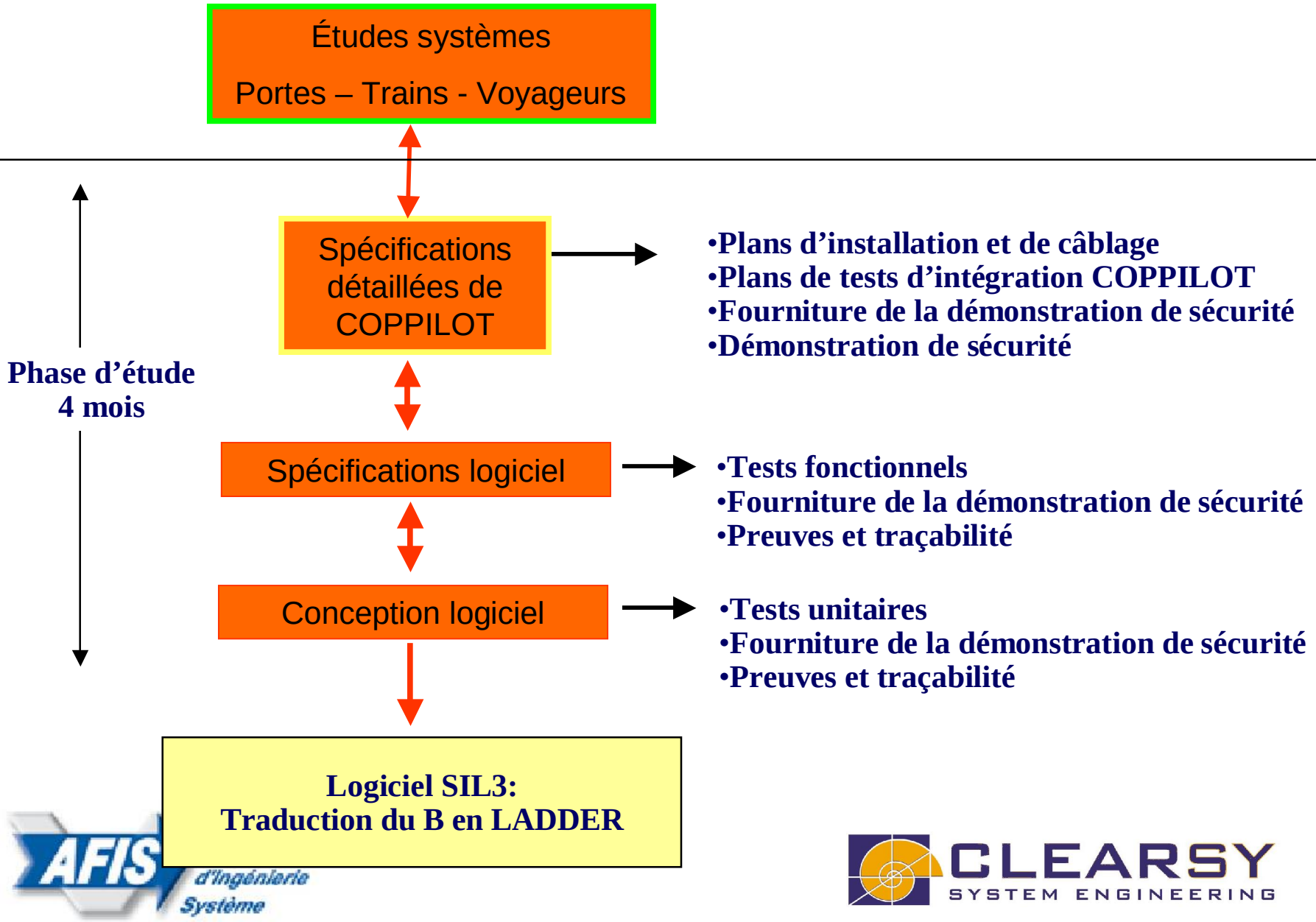
Spécifications des capteurs et du matériel

Processus ClearSy

Système

CLEARSY SYSTEM ENGINEERING

Utilisation des modèles B



AFIS d'ingénierie Système

CLEARSY SYSTEM ENGINEERING

Résultats

- **Aucune anomalie logiciel décelée même en phase de tests, deux retouches dues à des contraintes système**
- **Les modèles B et la preuve sont fournis avec la démonstration de sécurité système et logiciel**
- **Documentation complète acceptée par les autorités de tutelles**
  - ✓ Spécifications et conceptions systèmes
  - ✓ Spécifications matériel
  - ✓ Spécifications et conceptions logiciel
  - ✓ Plans d'installation
  - ✓ Cahiers de tests systèmes logiciels et matériels
  - ✓ Démonstration de sécurité
- **Grande souplesse pour réaliser des évolutions**

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING

Métriques

- **Documentation : 1300 pages**
- **Matériel :**
  - ✓ 500 références
  - ✓ 15 fournisseurs principaux
- **Équipe :**
  - ✓ 4 ingénieurs
- **Modèles B**
  - ✓ 3500 lignes 100% prouvées
- **Durée du projet 10 mois : études et installation**

Conclusions

- **ClearSy renforce son activité dans l'ingénierie de systèmes et de logiciels sécuritaires**
  - ✓ Systèmes conformes aux normes IEC 61508, EN 50126, 50128 et 50129
- **Développe son processus d'ingénierie autour des méthodes formelles**
- **Développe son offre de services autour de son savoir-faire dans :**
  - ✓ La mise en place de processus de développement systèmes sécuritaires en utilisant les méthodes formelles
  - ✓ L'assistance à l'ingénierie des systèmes et des logiciels sécuritaires
  - ✓ La démonstration de sécurité

AFIS Association Française d'Ingénierie Système

CLEARSY SYSTEM ENGINEERING