



A Formal Approach in the Implementation of a Safety System for Automatic Control of “Platform Doors”

Guilhem Pouzancre

3rd May 2006

ClearSy
Contact@Clearsy.com

20 rue Joubert
75 009 Paris

Tel: 01.53.25.97.79
www.clearsy.com



COPPILOT and "Platform Doors"

- ❑ The RATP is conducting operational trials of « half maximum Platform Doors »
- ❑ COPPILOT is the control system for opening and closing the screen doors



Overview of the Presentation

- ❑ **The remit of ClearSy**

- ❑ **Presentation on the COPPILOT methods**

- ❑ **The engineering process used: based on the B-method**

ClearSy - Project Manager of COPPILOT for the RATP

❑ The remit of ClearSy:

- ✓ **Fixed-price performance contract: deadlines, safety and availability**
- ✓ **Choice of system architecture and suppliers**
- ✓ **Ordering and acceptance of materials**
- ✓ **Development of software to safety integrity level SIL 3**
- ✓ **Installation, maintenance and removal of COPPILOT**
- ✓ **Safety demonstration**

❑ Three systems installed on line 13

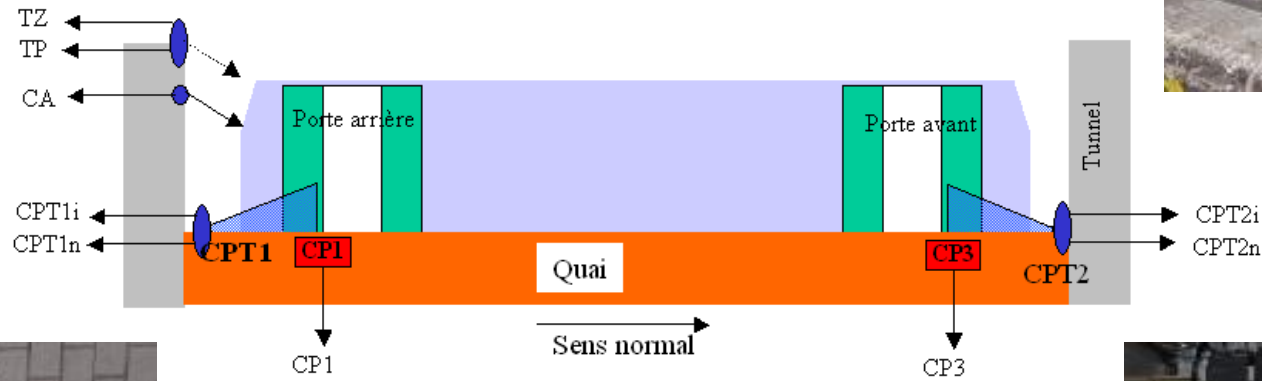
- ✓ **Stations: Invalides, St Lazare platform 1 and St Lazare platform 2**
- ✓ **Three different platform screen manufacturers: CNIM, Faiveley, Kaba**

**Train stop sensor CA
(Radar)**



Invalides Station

**Presence sensor
CP (IR)**



**Telemeter
(Laser)**

**Cabinet containing a safety
controller and the SIL 3 program**



Technical Aspects



□ Level SIL 3 safety system

- ✓ Level SIL 3 safety-integrated railway signaling system to EN 50129 standard
- ✓ SIL 3: Potentially dangerous events $< 10^{-7}$ occ/hour
- ✓ Major risk: Opening of the doors in error
- ✓ Safety demonstration for the RATP: AQL and AQM
- ✓ Safety demonstration for the supervisory agencies

□ Control of door opening and closing by train observation

- ✓ Use of standard industrial sensors (with no assumptions with regard to safety)
- ✓ Except the controller: SIL 3 industrial controller
- ✓ Development of SIL 3 safety software

Realisation and Installation Constraints

- ❑ **Design and installation of the system within 10 months**
 - ✓ Definition of the system architecture - 2 months
 - ✓ Design of the system and safety demonstration within 4 months
 - ✓ Installation on the 3 platforms over 4 months

- ❑ **Installation on platforms open to the public**
 - ✓ Heavy traffic: approximately 400 trains per day (every 2 minutes)
 - ✓ Installation and commissioning without any interruption to traffic

Development Process

❑ ClearSy process:

Use of the formal B-method throughout all engineering phases of the system

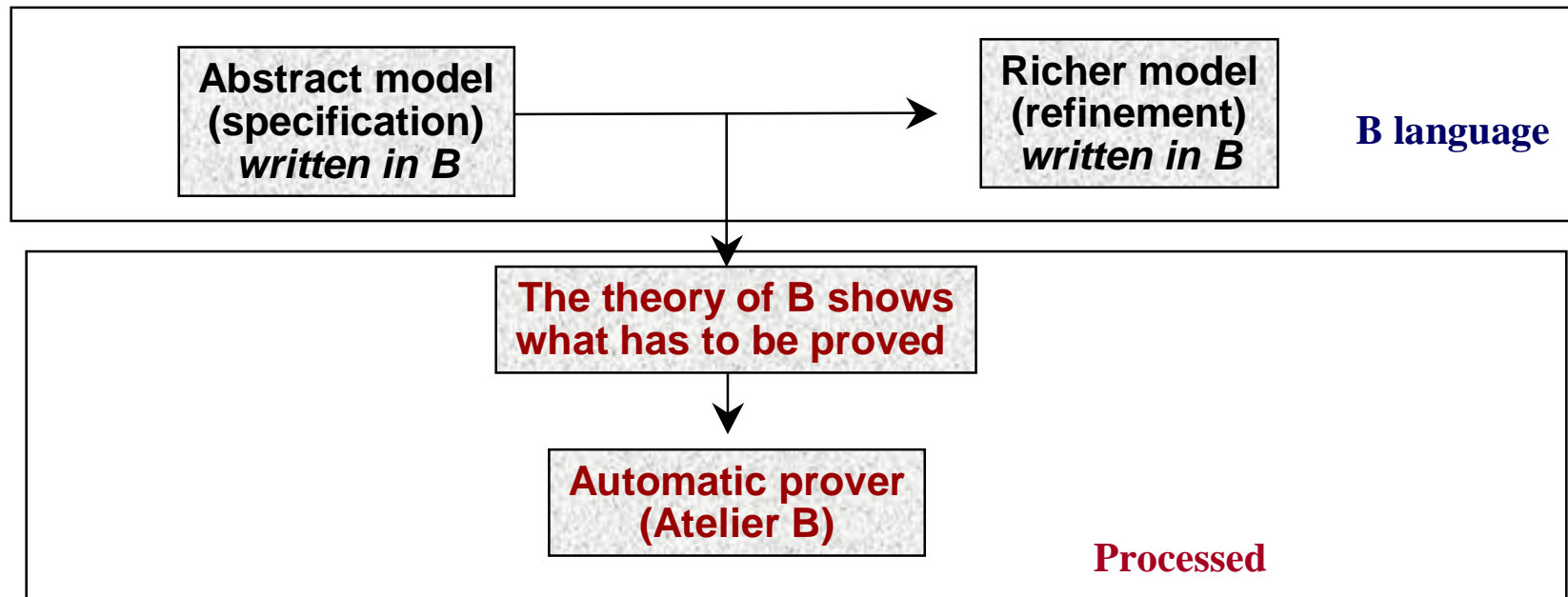
❑ Project team

- ✓ A project manager
- ✓ A development engineer
- ✓ A safety engineer
- ✓ A validation engineer

Principles of B

3 Ingredients: Modelling, Refinement and Proof

The B language is based on the theory of sets and predicate logic



The Benefits of Formal Language and Proof

- ❑ **Mathematical language gives precision**
- ❑ **Refinement gives structure to the models: decomposition, precision, traceability, proof**
- ❑ **Proofs of the properties give consistency of the functions between themselves and checking of them as needed**
- ❑ **Software code proofs: division by zero, loops, array overrun, memory**

Tools Used

□  www.composys.fr

- ✓ B modelling tool for distributed systems
- ✓ Tool for documentation generation from B models

□ Proof of the B models:

- ✓ www.B4free.com
(free version of Atelier B for universities)
- ✓ Atelier B: www.atelierb.societe.com

Formal Specifications: From System to Code



Functional specifications of the system
Doors – Trains - Passengers

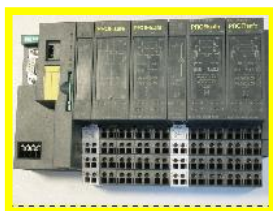
Avoidance of potentially dangerous events

Proofs of consistency

B Process

Study commissioned by the RATP before the consultation process

Platform doors



Detailed specifications of COPPILOT

Software specifications

Software design

SIL3 software:
Translation of B into LADDER

Sensor and materials specifications



ClearSy process

Using the B Models

System studies
Doors – Trains - Passengers

Detailed specifications of COPPILOT

- Installation plans and wiring diagrams
- Integration test schedules for COPPILOT
- Provision of the safety demonstration
- Safety demonstration

Software specifications

- Functional tests
- Provision of the safety demonstration
- Proofs and traceability

Software design

- Unit tests
- Provision of the safety demonstration
- Proofs and traceability

SIL3 software:
Translation of B into LADDER

Study phase
4 months

Results

- ❑ **No software anomalies found even in the test phase, two patches needed due to system constraints**

- ❑ **The B models and proof are provided with system and software safety demonstration**

- ❑ **Full documentation accepted by the supervisory agencies**
 - ✓ Systems specifications and designs
 - ✓ Materials specifications
 - ✓ Software specifications and designs
 - ✓ Installation plans
 - ✓ Test specifications for systems, software and materials
 - ✓ Safety demonstration

- ❑ **High flexibility for incorporating future modifications**

Metrics

- ❑ **Documentation: 1300 pages**
- ❑ **Materials:**
 - ✓ 500 referred leads
 - ✓ 15 main suppliers
- ❑ **Team:**
 - ✓ 4 engineers
- ❑ **B models**
 - ✓ 3,500 lines with 100% proof
- ❑ **Length of project - 10 months: Studies and installation**

Conclusions

- ❑ **ClearSy is intensifying its activity in systems engineering and safety software**
 - ✓ Systems which are IEC 61508, EN 50126, 50128 and 50129 compliant

- ❑ **It is developing its engineering process based on formal methods**

- ❑ **It is developing its range of services based on its know how in:**
 - ✓ The implementation of development processes for safety systems using formal methods
 - ✓ Safety systems and software engineering support
 - ✓ Safety demonstrations