



Safe and Reliable Metro Platform Screen Doors Control/Command Systems

a 3-year story

CLEARSY
SYSTEM ENGINEERING

320, avenue Archimède
Les Pléiades III - bât A
13 857 Aix en Provence Cedex 3
France

Téléphone : +33(0)4.42.37.12.70
Télécopie : +33(0)4.42.37.12.71

www.clearsy.com

Thierry Lecomte

FM'2008
May 28 2008, Turku

Plan

- Developing a safety-critical system
- Event-B: an introduction
- Case-studies
- Future work
- Conclusion

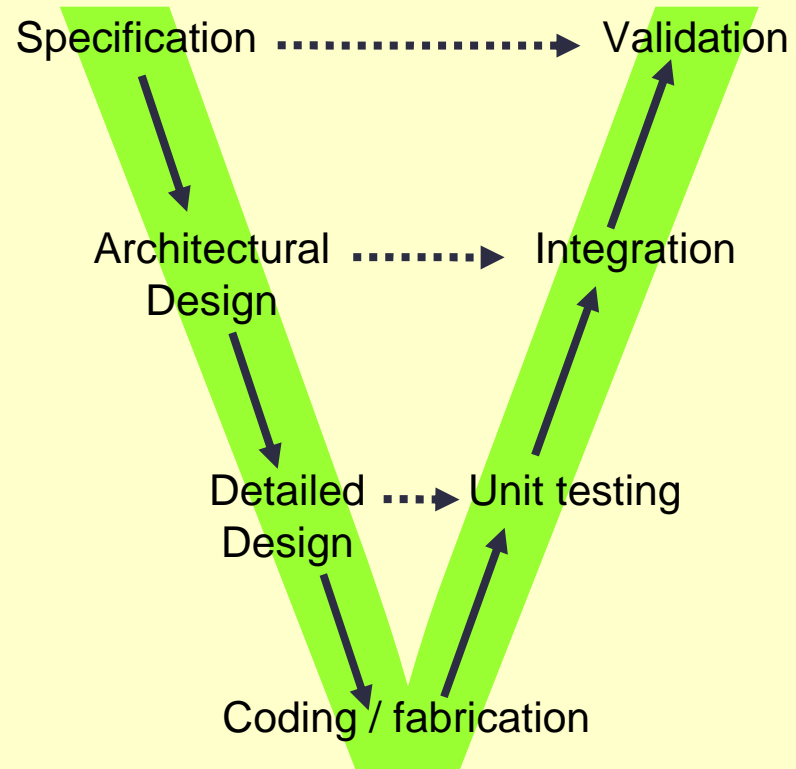


Developing a safety-critical system

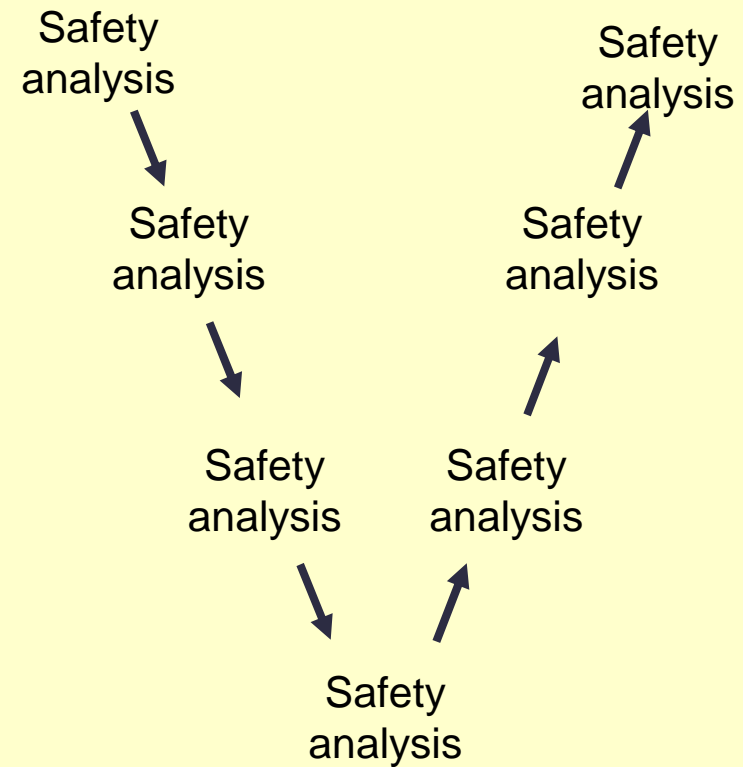
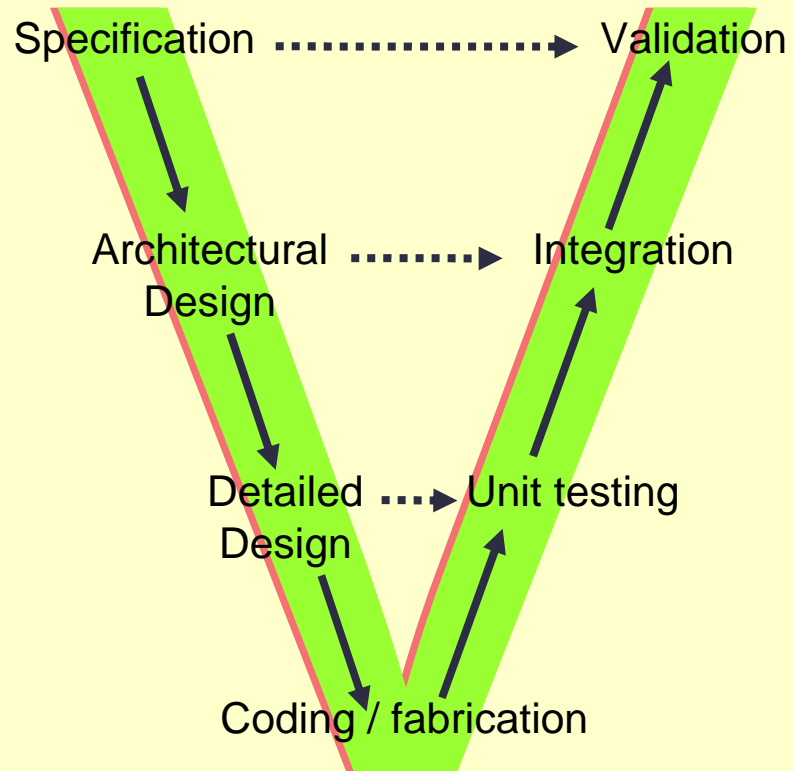
- Safety classification
 - Normative framework: EN 5012{6,8,9} for Railways, IEC 61508
 - Based on probability of occurrence of unwanted events
 - SIL1-SIL2: injury
 - SIL3-SIL4: death
 - Certification by an independent body (TÜV, Certifer, etc)
 - Qualification (client in-house evaluation)
- Covers both hardware and software
 - A software can't be SILx alone. Underlying hardware has to be taken into account.
- Random and systematic errors
 - Ex: electronic component failure can be computed accurately
 - This is no formula to determine software safety level. Set of methods/techniques are associated to a level.
 - Formal methods are (highly) recommended but not mandatory



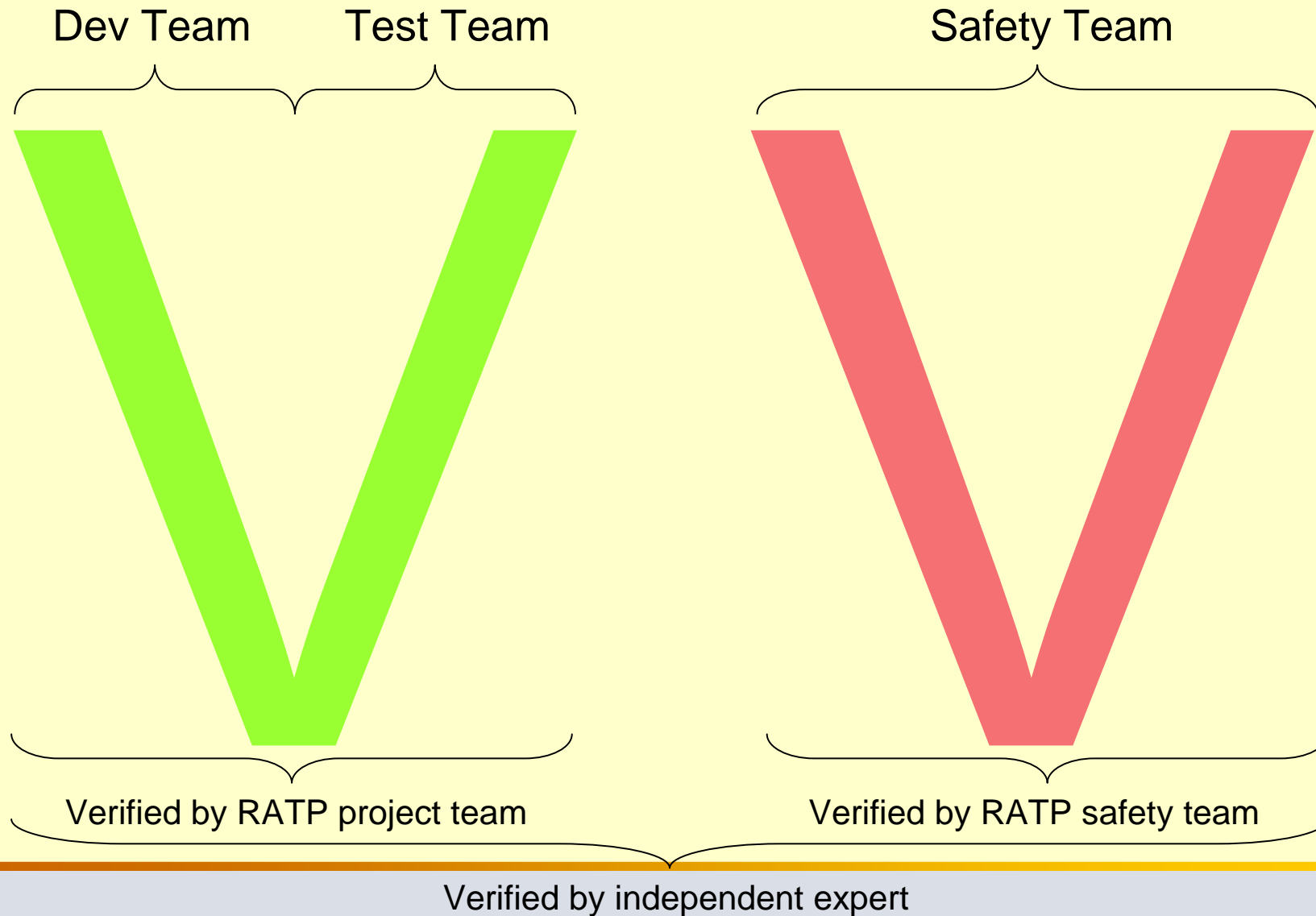
Project Development Cycle



Project Development Cycle



Project Development Cycle



Event-B: an introduction

- Event-B is B event-based evolution
 - Describing systems
 - Hardware and software parts
 - environment
 - using
 - events (condition / action)
 - refinement
 - decomposition



Event-B: an introduction

- Supported by the Rodin platform (<http://event-b.org>)
 - type checker,
 - proof obligation generator,
 - theorem provers, (Atelier B provers)
 - project manager,
 - Animators, model-checker, documentation generator, etc
- Models developed and proved with Atelier B (qualified tool)



Case-studies: platform screen-doors

- Projects for RATP (operates bus and metro public transport in Paris)
 - COPPILOT: line 13 (demonstrator) (completed)
 - DOF1: line 1 (complete deployment)(completed)
 - Cacolac: line 3 (local installation)(ongoing)



Platform screen-doors (PSD)

- To prevent passengers to fall on tracks and die
- To maximize number of passengers transported) (availability)
- To enable mixed circulations (manual and automatic trains)



Case-study: Coppilot (requirements)

- Command the opening of platform screen doors (PSD) safely (SIL3)
- No communication between train and command system
- 9 months to develop a demonstrator
- Experimented 8 months on 3 platforms



The Story

- Involvement in the a posteriori verification of a statement of work, using formal methods, before sub-contracting
- Finally we were given the responsibility to develop and to experiment the system on line 13
- Why were we selected ?
 - Good knowledge of the system
 - Small structure preferred for a very time-constrained, small project



The Story

- Another reason
 - Use off-the-shelf components (saving development costs and delay)
 - Calculator is S7 siemens PLC (SIL3 compliant)
 - Sensors had no safety-critical capabilities (easier to replace them with similar models available on the market)

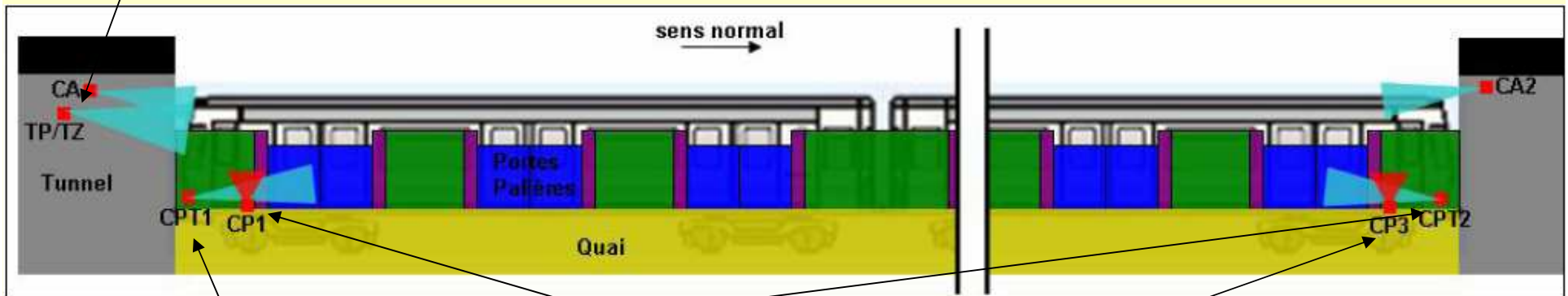


Case-study: Coppilot (decisions)



Train at +/- 1.1m from target location
Train at the standstill

2 PLC to command opening



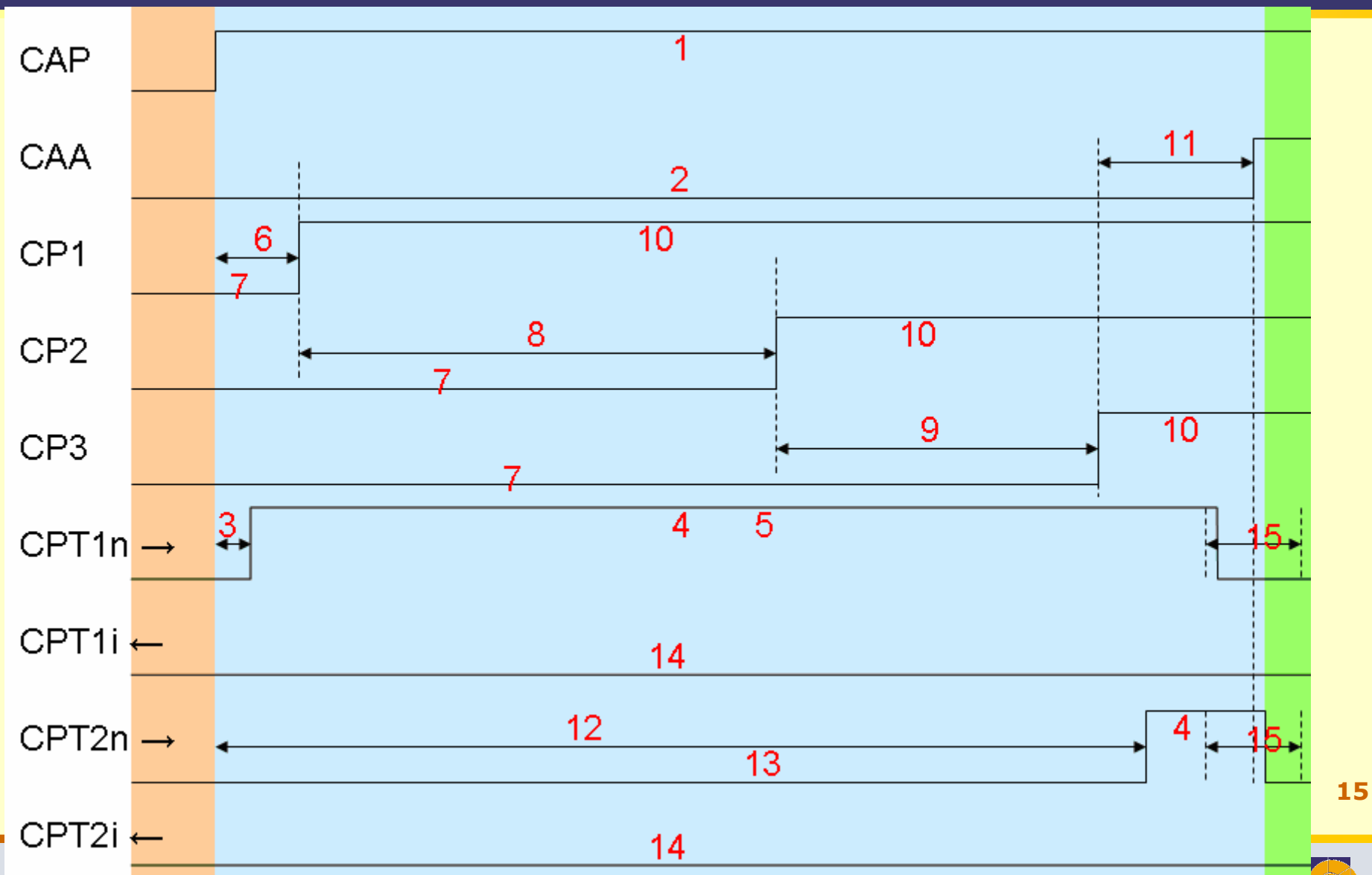
Train along the platform



Oriented movement detected



Sequence recognition

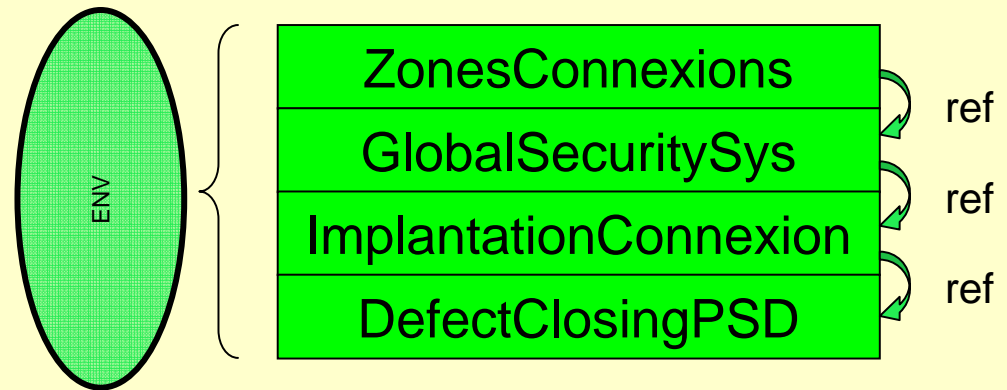


Technical organization

- Formal method for qualitative assessment
 - Verifying system safety in absence of perturbation
 - Express expected system safety properties
 - Find sub-systems safety properties and check them by proof
 - Model low level behaviour of the REAL components and verify by proof system safety properties
 - Export (complement) constraints on other components if required
 - specific sensors developed/adapted
- Quantitative evaluation (a priori reliability)
 - Determine how perturbations may lead to recognize as complete an incomplete arrival sequence
 - Spreadsheet based
 - Should be checked at the end of the experiment



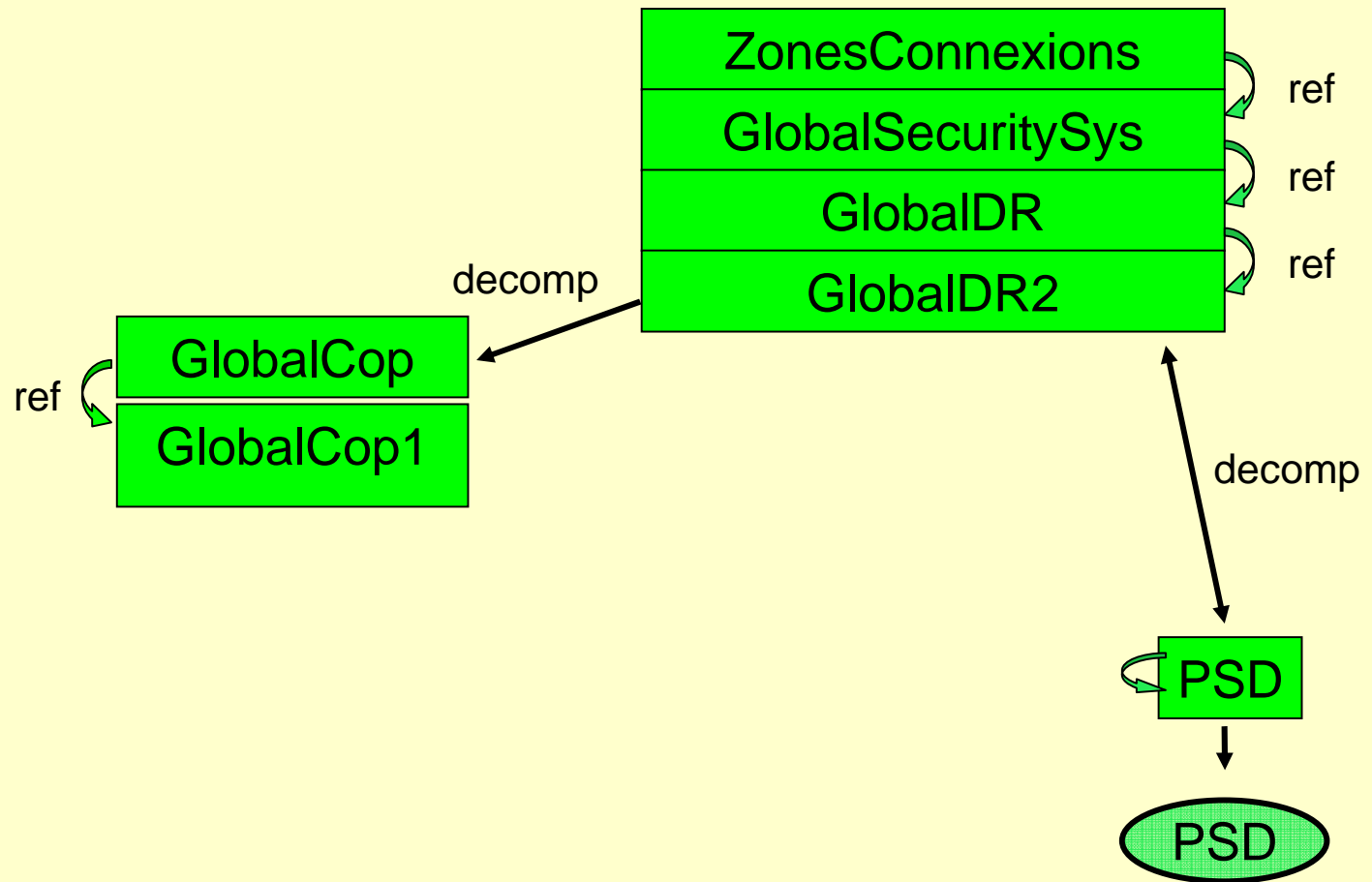
Modelling phase 1



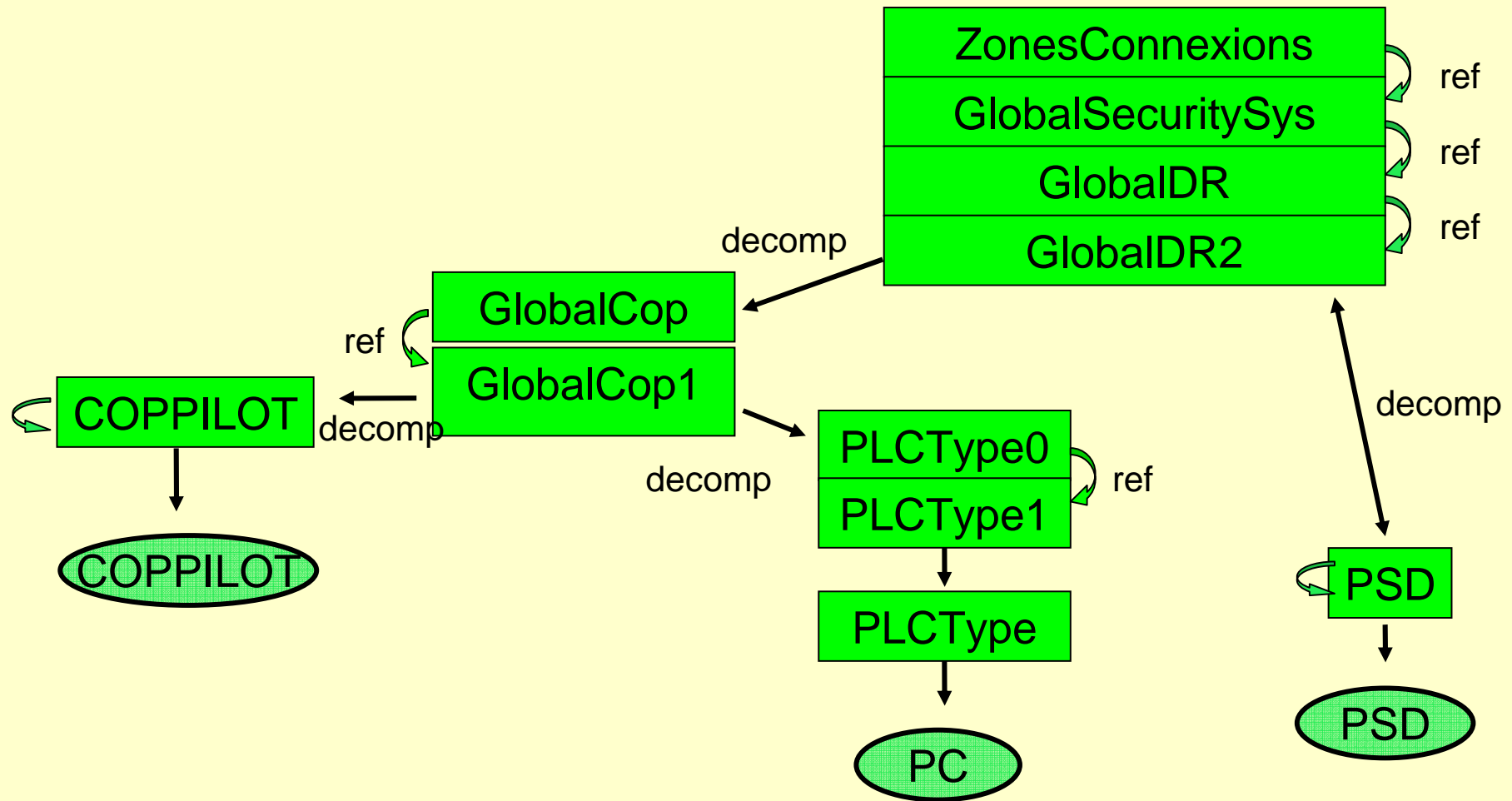
- define the properties expressing system safety
- demonstrate that any train + PSD system verifying some properties is safe
 - open train doors iff train is at the standstill and doors in front of PSD
 - open PSD iff train at the standstill is present or in case of evacuation
 - a train should not move if at least one PSD is not closed



Modelling phase 2



Modelling phase 2

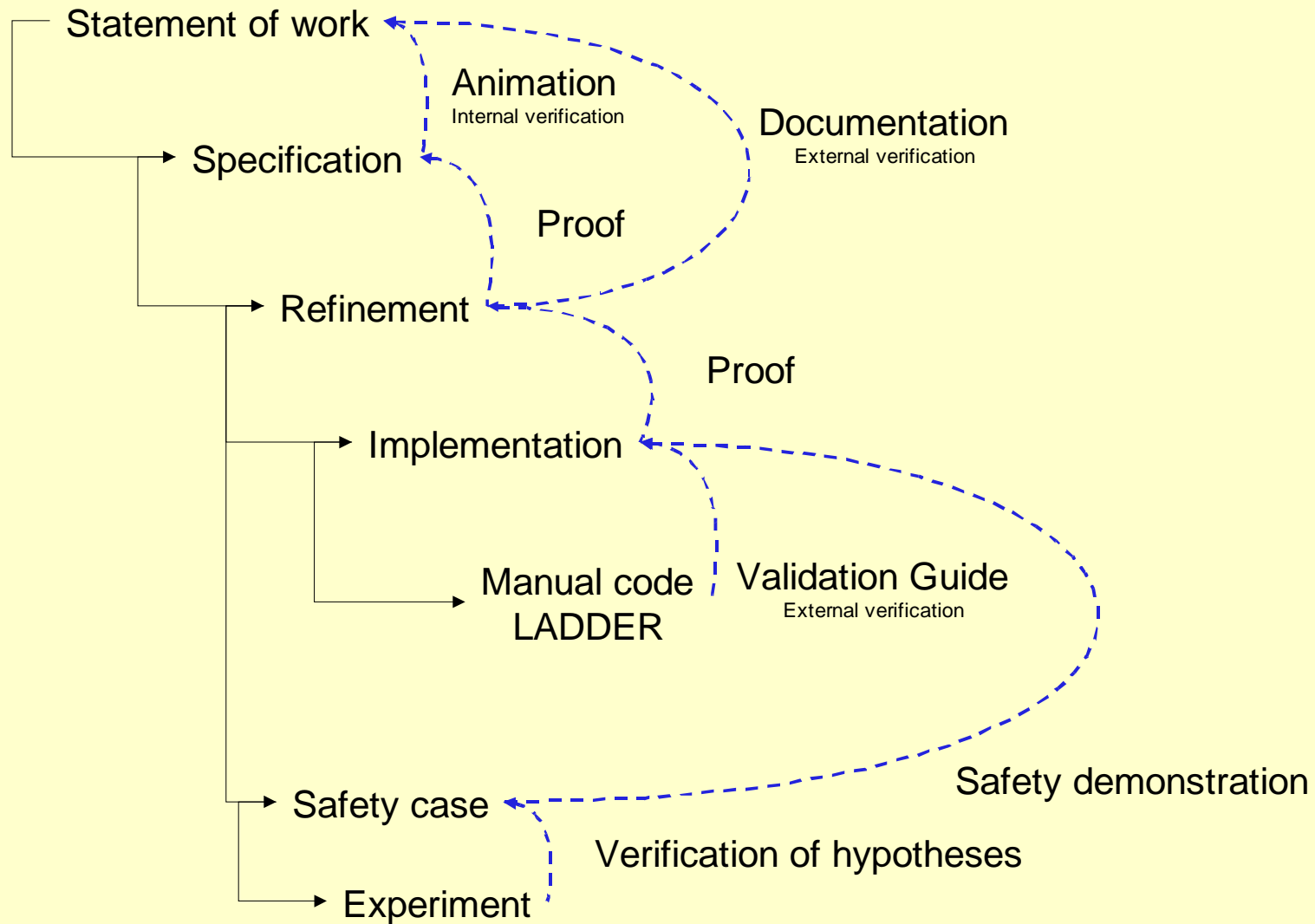


Modelling phase 3

COPPILOT



Verifications



COPPILOT: some figures

- 3 months for the event-B modelling
 - ~4 000 lines of model
 - ~500 safety related proof obligations
- 48 000 openings ordered, no miss, no failure
- A priori reliability confirmed by 8-month experiment



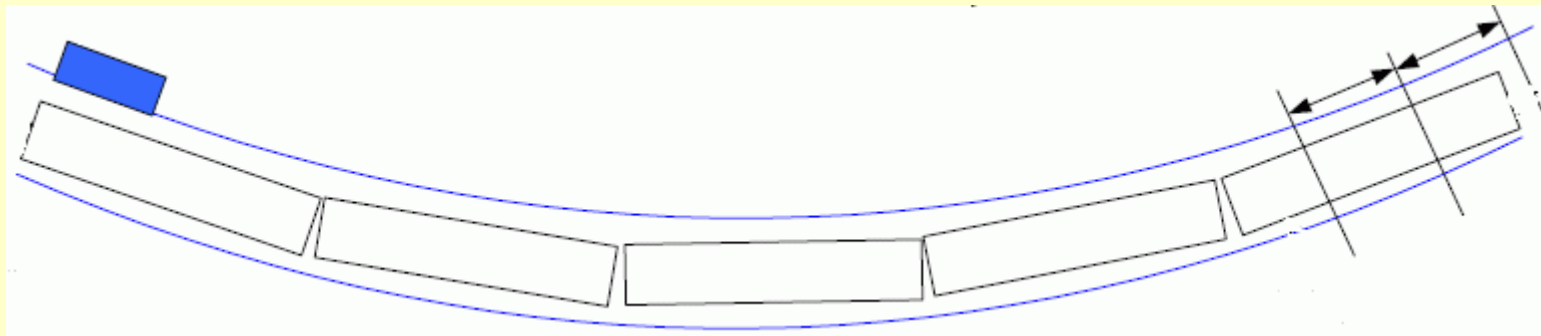
Case-study: Dof1 (completed)

- Line 1 (Paris): complete line equipped (50 platforms and 52 trains) – most crowded line
- Human driven trains will be replaced by driverless trains during next 6 years
- Dof1 should be able to control PSD opening and closing, for both kinds of train
- SIL4 required
- Dof1 is able to communicate with the train



Case-study: Cacolac (ongoing)

- Moving platform for curved platforms



- One station (Place d'Italie) – line 5
- SIL3 required

Metrics

Project	Model	Pos	Duration	Systems	Status
DOF1	4 000	500	9 m	3	Terminated
DOF1	9 000	2 500	10 m	50	In exploitation
Cacolac	8 000	3 000	9 m	2	Being deployed



Case-studies: platform screen-doors

- Forthcoming deployments:
 - Sao Paulo
 - Sevilla
 - Dubai
 - Etc (any location with increasing population and existing infrastructure)



Related R&D projects

- Joint research to combine functional and dysfunctional modelling (University of Marseilles, Arboost)
 - Altarica (Airbus 35x)
- Automatic LADDER Code Generation from B specification



Feedback & Conclusion

- No safety related mistake discovered after FM modelling
- It took time to “educate” our customer (extra work required to help him understanding and validating our work)
- Formal methods are used where they help much (structure our developments):
 - Increase confidence: animated formal models provided in tender as a reference
 - Save testing time, but coverage may be tricky to verify
- Applicable in absence of “generic product »



Thank you for your attention

