



PARIS  
2 ▶ 7  
OCTOBER  
2016 ▶ Pullman Bercy Hotel

INTERNATIONAL  
RAILWAY SAFETY COUNCIL

# 25 years of Formal Methods at RATP

▶ FROM MANUAL APPROACH FOR PROOF OF PROGRAMS TO  
INSTRUMENTED DEMONSTRATION OF RAILWAY SYSTEMS SAFETY

David BONVOISIN, RATP – Engineering Department – Head of RAMS division



# Synopsis



1. Introduction
2. Metro safety systems and their evolution
3. Experiences related to formal methods
4. Promoting and developing formal approaches
5. Further Developments

1. Introduction
2. Metro safety systems and their evolution
3. Experiences related to formal methods
4. Promoting and developing formal approaches
5. Further Developments

# Brief introduction to formal methods

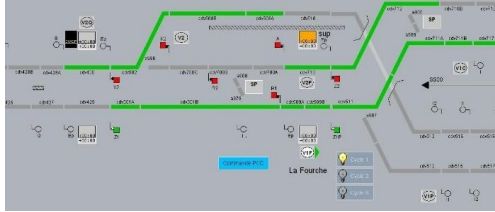


- ▶ Formal methods are system design techniques that use rigorously specified mathematical models to:
  - build software and hardware systems
  - use mathematical proof in order to ensure correct behaviour (i.e. the behaviour satisfies safety properties)
  
- ▶ Well-known strengths of formal methods:
  - rigorous mathematical specifications allow to get rid of ambiguities (in requirements)
  - mathematical proof covers exhaustively the possible behaviours (whereas tests are only samples)
  
- ▶ Usual drawbacks:
  - requires rare skills
  - scope limited to application software or hardware verification
  
- ▶ Formal methods are Highly Recommended by the EN50128 CENELEC standard for SIL3 and SIL4

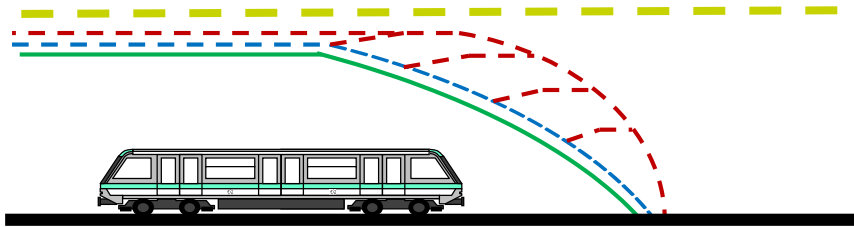
1. Introduction
2. Metro safety systems and their evolution
3. Experiences related to formal methods
4. Promoting and developing formal approaches
5. Further Developments

# Overview of RATP's Signalling Systems

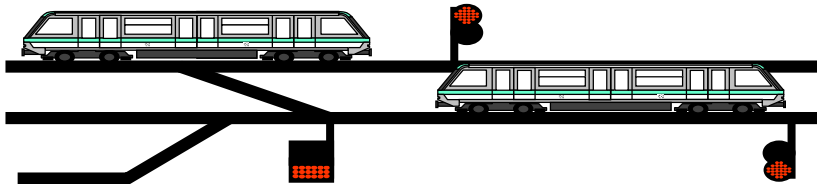
## ► Typical Signalling Systems Configuration:



Automatic Train Supervision and Energy Control (ATS)

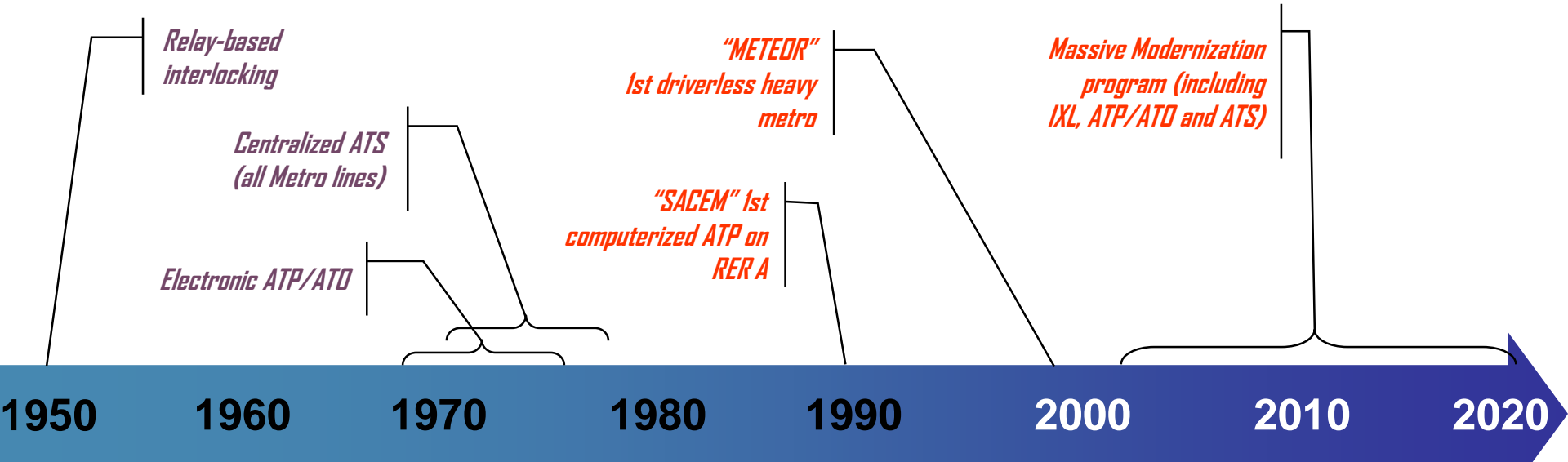


Automatic Train Protection and Operation  
(ATP/ATO)



Route Interlocking (IXL)

# From relays to computerized systems



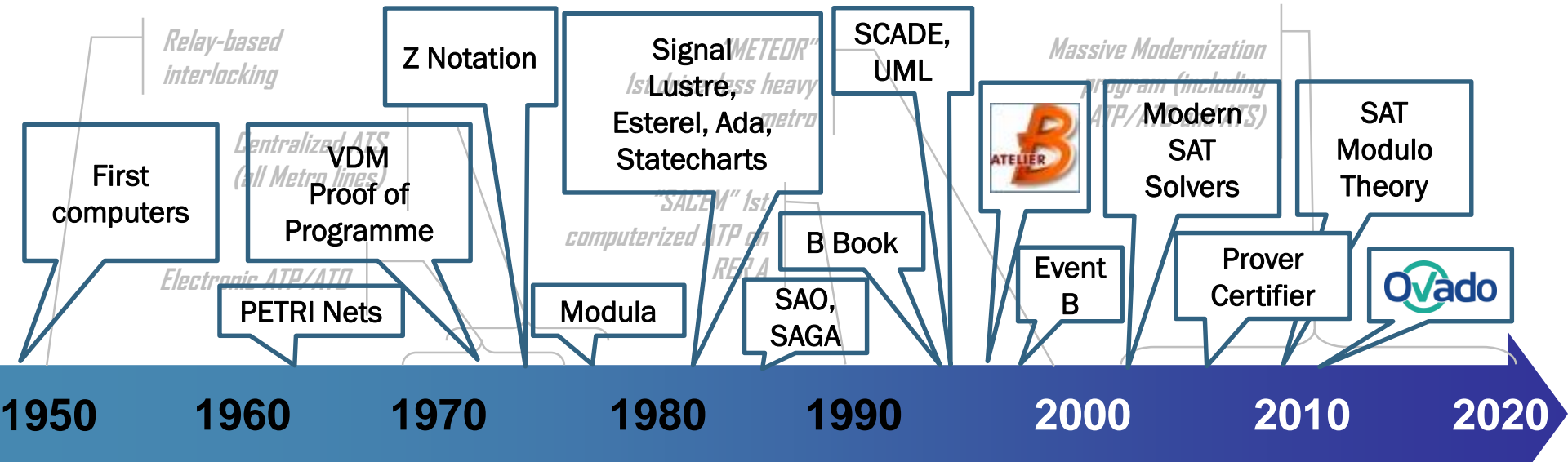
Electro-mechanical technology (failsafe relays)

Analog electronic used for safety critical application (using magnetic transmission)

Coming of computer techniques for safety critical applications (start for use of formal methods)

Generalization of computerized technology, used for all railway applications, including safety critical applications

# From relays to computerized systems



Electro-mechanical technology (failsafe relays)

Analog electronic used for safety critical application (using magnetic transmission)

Coming of computer techniques for safety critical applications (start for use of formal methods)

Generalization of computerized technology, used for all railway applications, including safety critical applications



# Synopsis



1. Introduction
2. Metro safety systems and their evolution
3. Experiences related to formal methods
4. Promoting and developing formal approaches
5. Further Developments

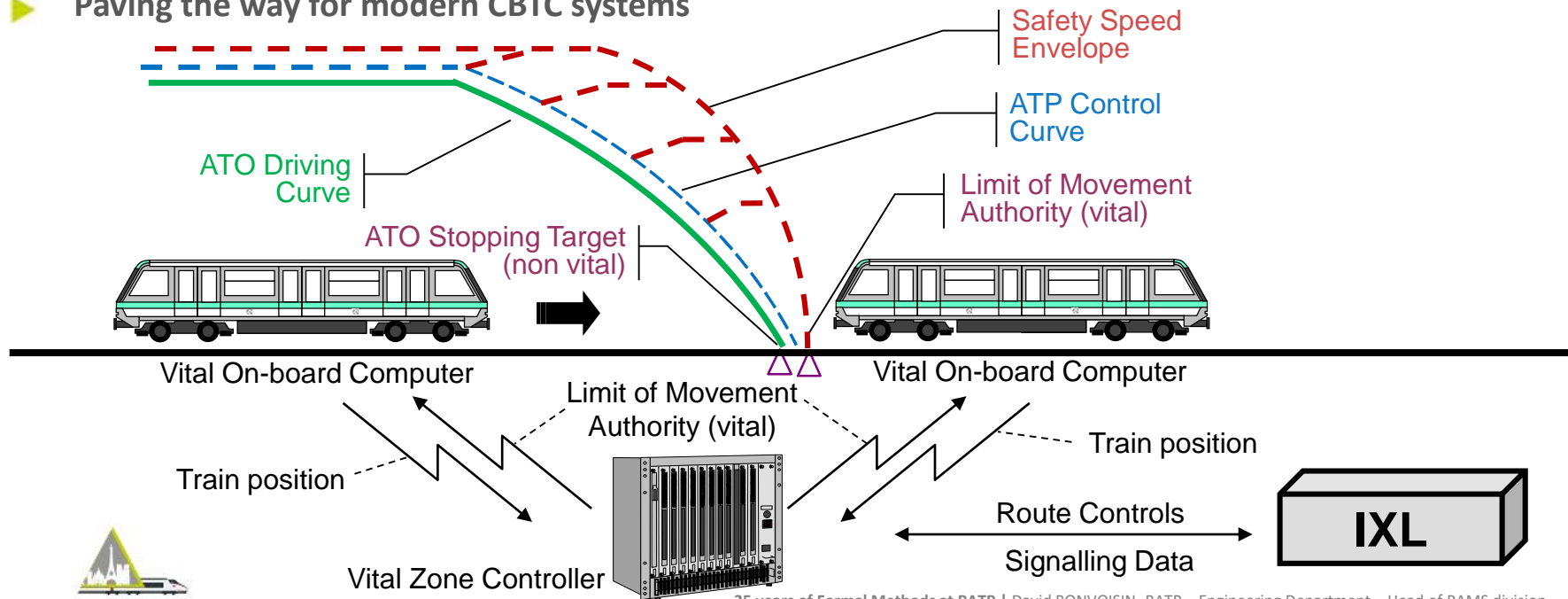
# SACEM on RER A: experiencing formal methods

- ▶ **Starting 1977, the SACEM development experienced new methods for safety related to computer-based application using:**
  - Rigorous development process
  - Coded mono-processor
  - Application software written in MODULA-2 (>60 000 lines of code)
- ▶ **Before revenue service, the concern for safety of the application software raised**
  - Decision taken for « retro-modelling » the application code using the « Z notation » (with Jean-Raymond Abrial)
  - About 20 unsafe scenarios discovered and corrected before revenue service in 1989
- ▶ **Decision taken to further develop and systematize the use of formal methods**
  - Based upon the newly issued “B book” by Jean-Raymond Abrial
  - Leading to industrialize the “B workshop” together with INRETS, SNCF, GEC-Althom & Steria (now Clearisy)



# METEOR on L14: industrializing the B method

- ▶ 1998 introducing the first computerized UTO system
  - 100% vital software build using B (150 000 lines of ADA code generated from B)
- ▶ Paving the way for modern CBTC systems



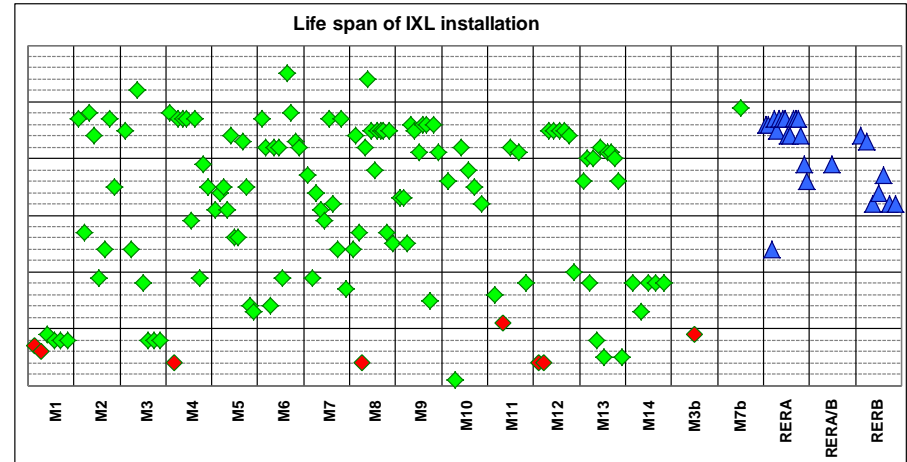
# IXL renewal : introducing a model-checking approach

## ▶ Starting 2001, RATP launched the program for IXL renewal:

- Using computerized technology “PMI” featuring Petri Nets
- Because of installation ageing and major threat about NS1 relays manufacturing

## ▶ Two different formal approaches experienced:

- Interlocking principles modelling in B, however this approach were considered not fully adequate because:
  - ✓ B language far too different from Signalling engineer common skills
  - ✓ None of the suppliers developed computerized IXL using B method
- Use of a semi-formal development language together with implementation of model checking approach:
  - ✓ formal proof capabilities demonstrated with **Prover-Technology, Thales and Verimag**
  - ✓ Leading to develop the **Prover Certifier** workshop widely used since then



- ◆ Metro (relay-based IXL)
- ◆ Metro (computerized IXL)
- ▲ RER (relay-based IXL)

1. Introduction
2. Metro safety systems and their evolution
3. Experiences related to formal methods
4. Promoting and developing formal approaches
5. Further Developments

# Requiring Formal Methods in Calls for Tender



- ▶ **From 2002, French regulations introduced a new legal framework for urban guided transportation systems, requiring for authorization:**
  - A complete transparency about safety demonstration of the system,
  - A systemic approach for safety demonstration together with a GAME approach (reference system),
  - An independent safety assessor (OQA: notified and independent assessment body):
    - ✓ Who shall assess conformity of the system towards the regulations, standards (EN 5012x) and “state of the art”
    - ✓ Evaluating level of safety as targeted and achieved by the system
  - Applicable not only to new safety related systems (or when substantially modified), but also to systems already in revenue service (regularized safety case)
- ▶ **Because of its past experience with safety critical systems, RATP considered having still to make up its own mind, by**
  - Continuing to assess safety demonstration by itself, independently from supplier and OQA (internal safety assessment)
  - Developing and promoting formal methods as far as possible
- ▶ **Accordingly, RATP is now accredited ISO 17020 as a type C inspection body**



# The PERF approach

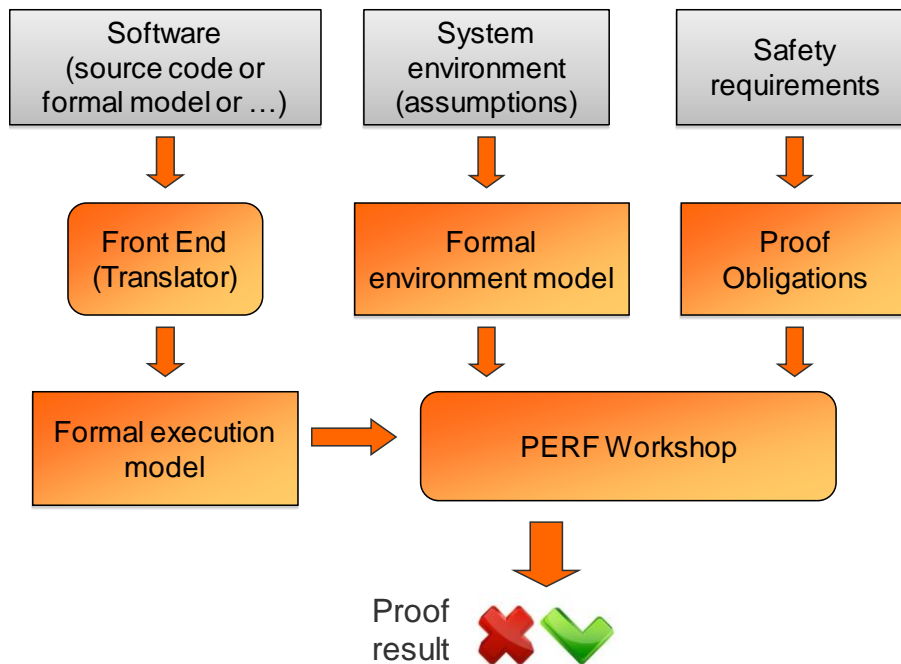
Since 2010, RATP uses a formal proof approach for its own software safety **assessment** activities:

- ▶ **PERF** approach: **P**roof **E**xecuted over a **R**etro-engineered **F**ormal model
- ▶ Independent from the supplier's software validation policy
- ▶ PERF is used for :
  - Formal verification of safety properties of PETRI-Nets, SCADE models, C or ADA source code,
  - Formal verification of equivalence between models and generated source code
- ▶ Strengths:
  - In an assessment process : PERF can take place concurrently with software test phases (reduction of projects global duration)
  - Makes regression analysis very efficient and very quick ("push button")
  - Reveals unexpected unsafe scenarios
  - Versatility
  - Ease of use (skills)



# The PERF workshop

A versatile model-checking workshop combining SAT-Solving and K-induction

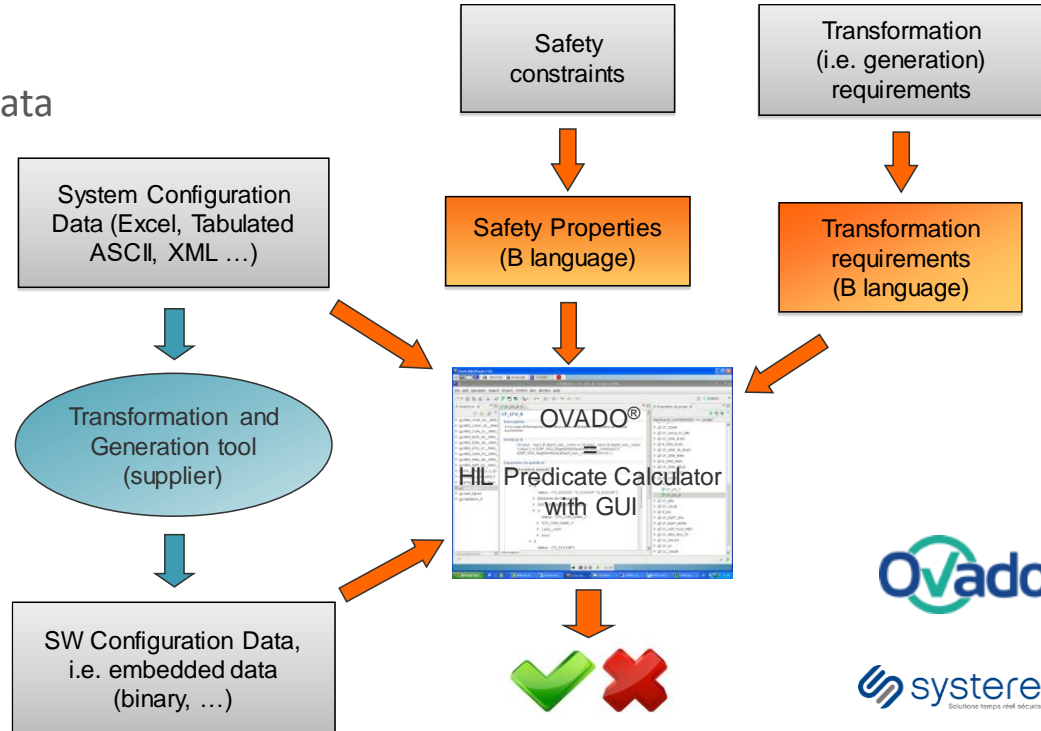




# The OVADO toolset

OVADO is used for :

- ▶ Formal verification of configuration data towards system safety constraints
- ▶ Formal verification of data transformation into source code elements towards software safety constraints








# Formal Methods application cartography



▶ IXL:

Line/system	Dvt Method	Toolkit	Year	Usage
<b>1</b> Maillot-La-Défense Ch.-de-Vincennes	PETRI Nets	Prover Certifier	2009 2010	Safety case
<b>12</b> Mairie d'Issy Front-Populaire	PETRI Nets	Prover Certifier	2011 2012	Safety case
<b>8</b> Créteil Préfecture Pointe du lac	PETRI Nets	Prover Certifier	2011	Safety case
<b>4</b> Mairie de Montrouge	PETRI Nets	Prover Certifier	2013	Safety case

▶ CBTC:

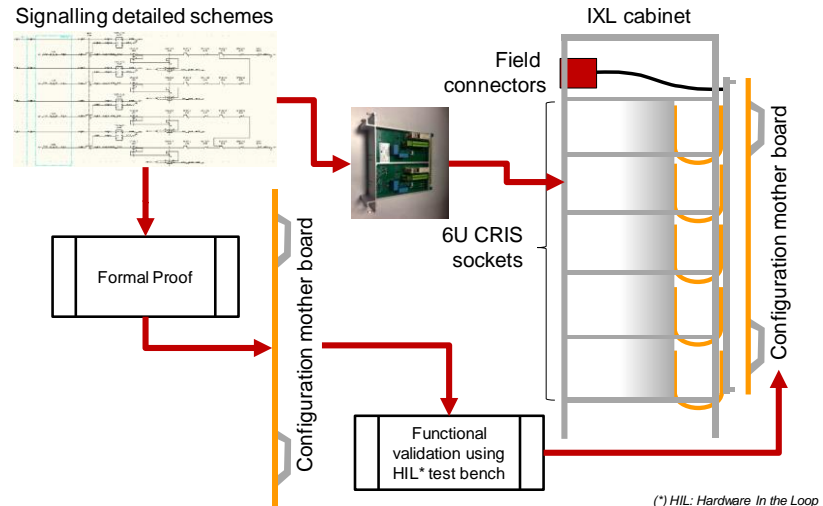
Line/system	Dvt Method	Toolkit	Year	Usage
<b>14</b> Driverless CBTC	B Method	Atelier B	1998	Safety case
<b>3</b> CBTC Onboard Ctrl CBTC Zone Ctrl	B Method SCADE 5	Atelier B Prover Certifier	 2010	Safety case
<b>1</b> Driverless CBTC	B Method	Atelier B	 2011	Safety case
<b>5 9</b> CBTC Zone Ctrl	B Method	Atelier B	 2013	Safety case
<b>5 9</b> CBTC Onboard Ctrl	SCADE 5	Prover Certifier	 2013	Safety assessment
<b>13</b> CBTC (GOA2)	SCADE 6	Prover Certifier	 2014	Safety assessment



1. Introduction
2. Metro safety systems and their evolution
3. Experiences related to formal methods
4. Promoting and developing formal approaches
5. Further Developments

# IXL modernization strategy

- ▶ At the end of the first deployment contract for computerized IXL, this technology “PMI” was not deemed so much appropriate, because of:
  - PMI is based on “COTS” computers, for which life span will not exceed 20 years
  - IXL application software is “proprietary”, the PMI product is linked to a unique supplier
  - Relay-based IXL will stay in operation for numerous years (PMI cannot renew instantly all IXL installations), RATP still has to support the corresponding knowledge and skills.
  
- ▶ Then, RATP entered in a R&D program for “hybrid IXL” using newly developed safety relays “CRIS” together with formal methods:
  - Thanks to previous development with formal proof, the PERF workshop is being adapted to cover “AUTOCAD relay schematic” models.



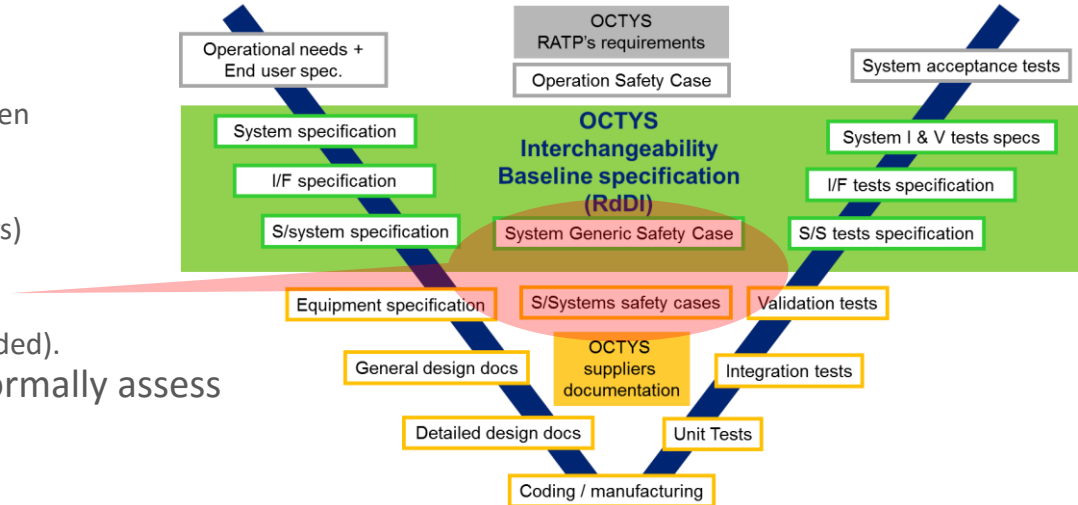
# Interchangeable CBTC: extending formal proof coverage

- ▶ OCTYS Interchangeability Baseline Specification “RdDI” has been developed jointly with RATP and suppliers (common working group)

- Safety case at system level has been assessed by RATP
- Some « system safety constraints » have been elaborated only through « expert review » (no justification document provided, due to industrial secrecy reasons amongst suppliers)
- Such constraints, might potentially be misinterpreted during future projects (depending of suppliers that might be awarded).

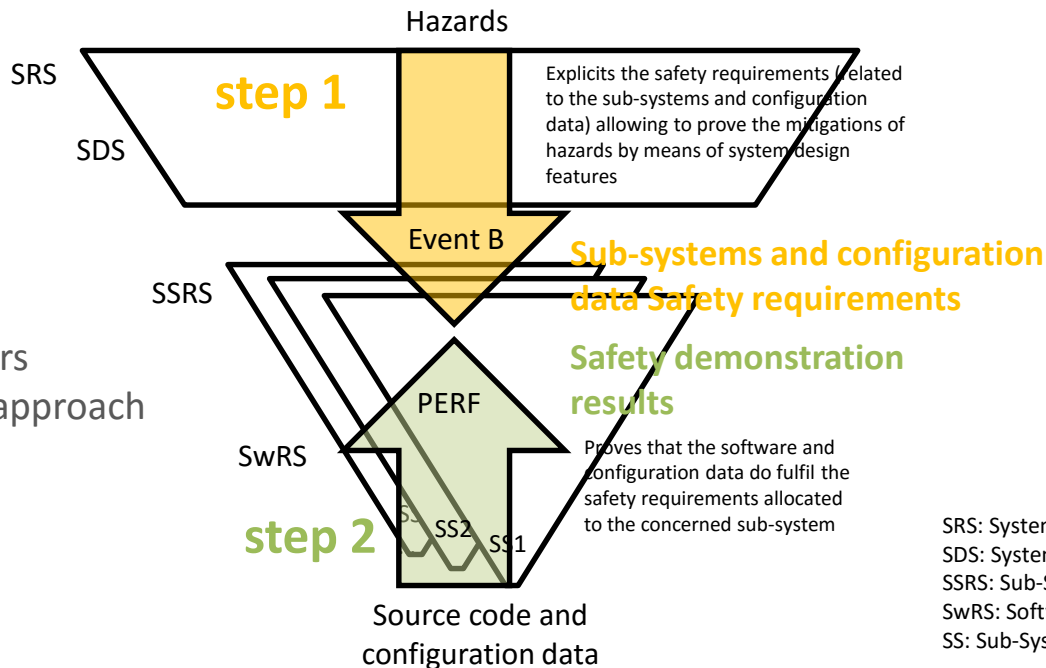
- ▶ To mitigate the risk, decision taken to formally assess such safety constraints

- Using B method (event B) at system level,
- Retro-modelling the OCTYS functionalities at system level will allow to formally identify and refine sub-systems related safety constraints,
- Project launched with Clearsy and Siemens.



# Our expectations (for a near future?)...

- ▶ Our Holy Grail: the complete and global formal demonstration of the safety



- ▶ RATP considers a composite approach

SRS: System Requirement Specification  
SDS: System Design Specification  
SSRS: Sub-System Requirement Specification  
SwRS: Software Requirement Specification  
SS: Sub-System

# Thank you for attention

