CLEARSY
Safety Solutions Designer

Nantes Université
Les Journées Scientifiques

Software Development (and other things) with B

NII / Grace Tower / Tokyo / 2014

Thierry Lecomte
R&D Director

THIERRY.LECOMTE@CLEARSY.COM

Heritage

- CLEARSY created in 2001
- To use, develop, and exploit B and Atelier B
- Atelier B ownership

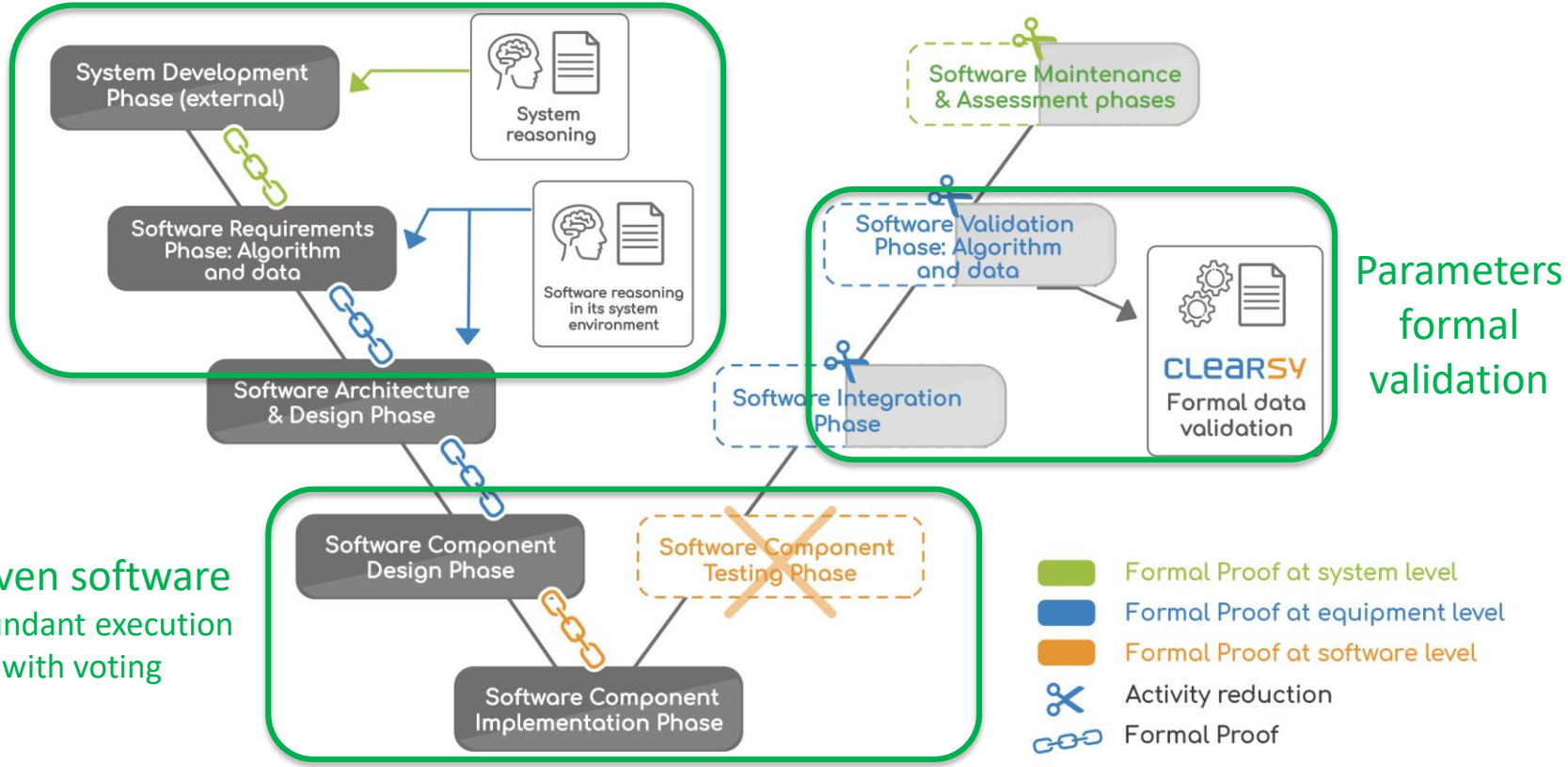
- What is the status almost 25 years later ?

Formal Methods in Railways

- Formal Software Development
- Formal System Proof
- Formal Data Validation
- Safety Platform

Formal activities throught the V cycle

Explain why it is designed this way



Parameters formal validation

Proven software

Redundant execution with voting

Formal Software Development

Safety critical software
formally specified & proved

No unit test
Most integration test avoided

SET THEORY
FIRST ORDER LOGIC
INTEGER
BOOLEAN
GRAPHS

IDE DEVELOPED DURING 25+ YEARS
FREELY AVAILABLE
CERTIFIED EN50128 T2 IN 2024

https://www.atelierb.eu/en/

References:

- *The B-book - Assigning Programs to Meanings*, Cambridge Press, 2001
- *The First Twenty-Five Years of Industrial Use of the B-Method*, FMICS, 2020

Formal Software Development

1998

Paris L14 Automatic Train Protection (ATP)
Emergency braking in case of danger (86 kloc B, 110 kloc Ada)

2000-2024

Used by ~30% radio-based control metro worldwide
CDGVAL shuttle (500 kloc / automatic refinement)

2006-2024

Used for Paris L1, L4, L13, L14 (Olympics)

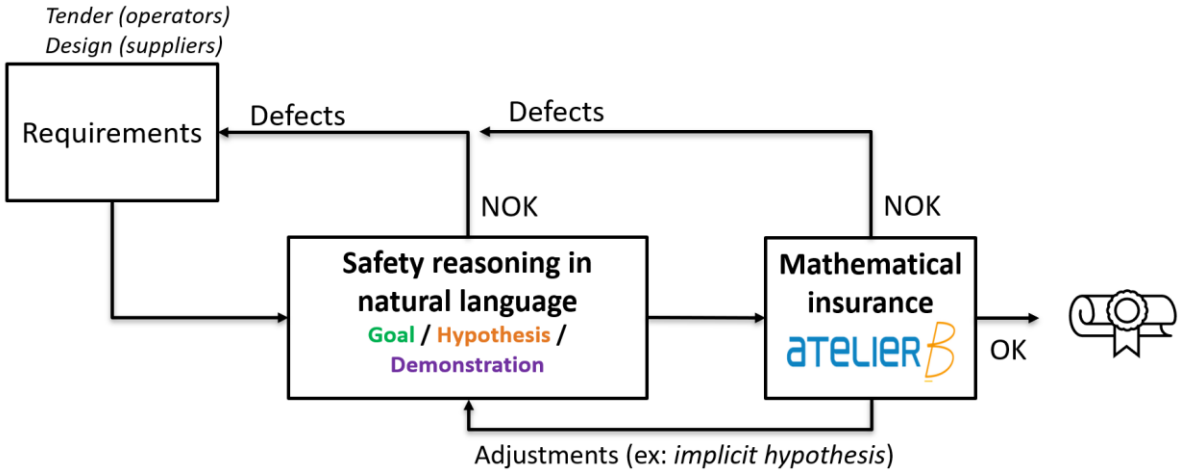
2024-2030

To be used for Paris L15, L16, L17, L18

Formal System Proof

Safety reasoning exhibited (“why its was designed this way”)
For legacy systems and never implemented specs

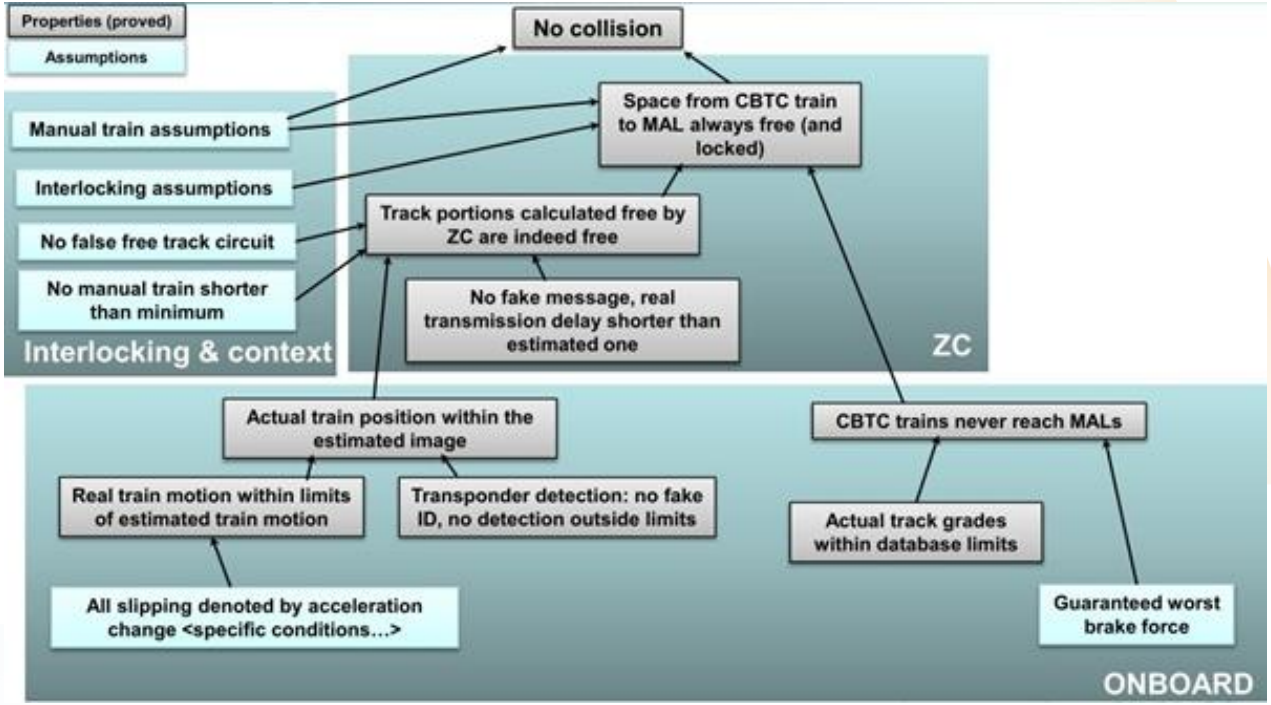
SET THEORY
FIRST ORDER LOGIC
INTEGER
BOOLEAN
GRAPHS



References:

- *Formal Proofs for the NYCT Line 7 (Flushing) Modernization Project*, ABZ, 2012
- *Safety Analysis of a CBTC System: A Rigorous Approach with Event-B*, RSSR, 2017

Formal System Proof



FPoSLS applied for NYCT to Thales CBTC [2007]

Formal System Proof

2010

New York City Transit (Culver, QBL line CBTC, 8th Avenue Line)
Proof of a new safety automation
Call for tender mentioned Formal Methods

2020-2024

RATP (L3, L5, L9, L6, L11)
Safety proof of OCTYS CBTC

2023-2026

SNCF (Marseille-Vintimiglia)
Safety proof of world-first ETCS L3 hybrid

2024

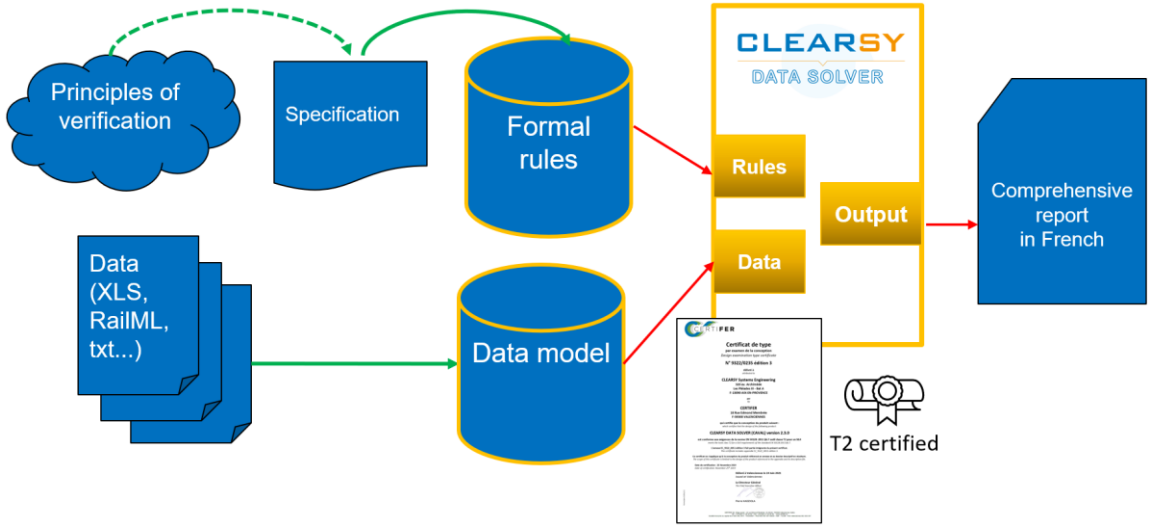
Calls for tender mention Formal Methods

Formal Data Validation

Safety critical constant data
formally specified & model-checked

100k data chunk, up to 2k rules
Human errors avoided

SET THEORY
FIRST ORDER LOGIC
INTEGER
BOOLEAN
GRAPHS



References:

- *Formally Checking Large Data Sets in the Railways*, ICFEM, 2012
- *ProB*, https://prob.hhu.de/

Formal Data Validation

2003

First tool to verify embedded topology data
For Certification

2012

First tool integrated into CBTC metro dev process

2018

First application to ERTMS (beacons)

2024

Core tool certified 50128 T2
Applied by major train manufacturers and metros
Call for tenders requiring formal data validation

Formal Data Validation: the proof !

- TGV overspeed over a switch
  - 170 km/h instead of 100 km/h in La Milesse (France)
  - due to errors not detected during **human** data validation (2019)

- BEA-TT supports FM

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

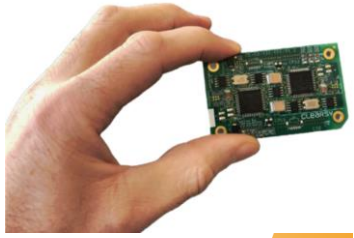
BEA-TT
Bureau d'enquêtes sur les accidents de transport terrestre

> *"Given the difficulty of controlling the growing quantity of parameter data, the use of validation algorithms is essential. The use of innovative formal methods, based on advanced mathematical concepts, is one answer."*

References:

- https://www.bea-tt.developpement-durable.gouv.fr/rapport-d-enquete-sur-la-survitesse-d-un-tgv-le-22-a1077.html

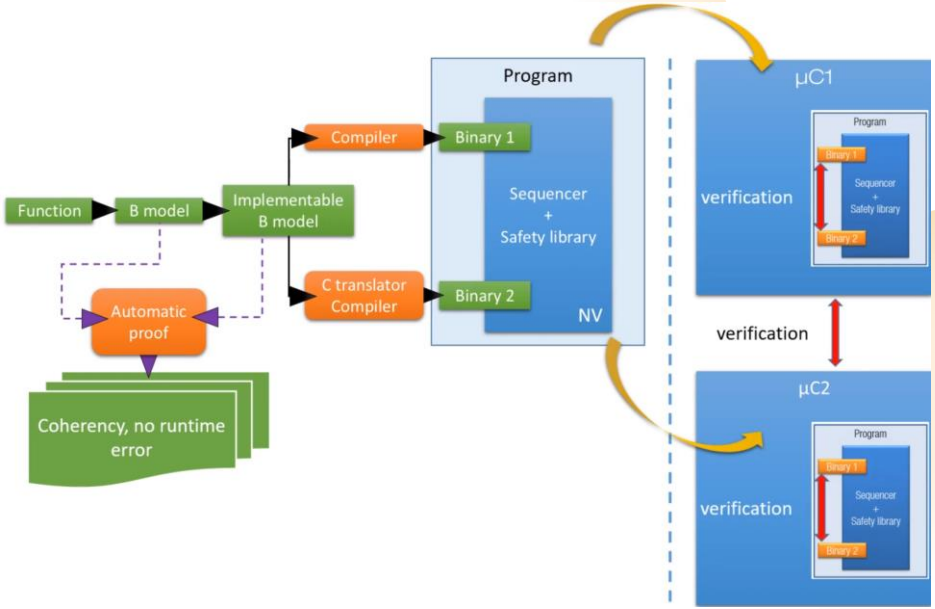
CLEARSY Safety Platform



Safety computer able to handle random failures
Programmed with B for systematic failures

4oo4 Software
2oo2 Hardware

SET THEORY
FIRST ORDER LOGIC
INTEGER
BOOLEAN
GRAPHS



References:

- *The CLEARSY safety platform: 5 years of research, development and deployment*, SBMF, 2020

CLEARSY Safety Platform

2006-2019

Building blocks developed for platform screen doors (PSD) controllers
French R&D project for academic-version safety computer

2020

Industry-ready generic safety computer developed

2021

Platform certified EN50129 T3 SIL4

2023-2024

Deployed in Brisbane to control PSD

2024

Deployed for ground and underwater autonomous mobility
French R&D project to add cybersecurity

REX: Formal Methods in Railways

- Well-oiled process: deliverables accepted, models audited, no fatalities in metros
- Exploiting companies mention more and more FM in call for tender (because of past problems)
- Standards not « degrading » over time
- FM not selling per se:
  - Continue to be used because already in dev cycle
  - Cost reduction is more synonymous of « subcontracting in low cost country »
  - Requests to inject FM into existing dev cycle with minimal impact

Formal Methods in Smart Card

- Standards
- History
- REX

Formal Methods in SmartCard

- Common Criteria:
  - Only standard imposing formal methods
  - EAL6+: formal model, functional specification complies with security policy, tracability with implementation
  - EAL7: formal model from top to bottom, 2 products in France (JVM by Thales, microkernel by ProvenRun)
- Research project to model circuit and generate VHDL
  - Formal model as a link between datasheet and VHDL
  - Demonstration on STMicroelectronics MPU (20k gates)

Common Criteria Certification

2003

Development of first FSPM for SmartCard microcircuit (CC 2.x EAL5+)

2004-2006

Modelling of Security Policies of 3 product lines

2007-2023

Certification with French and German Evaluation Centers
Knowledge Transfer (CC 3.1 EAL6+)

2024-2025

Transition to CC:2022

Formal Methods in Autonomous Mobility

- Standards
- History
- REX

Formal Methods in Autonomous Mobility

- Situation heterogenous:
  - Road + track shuttle
  - Low traffic regional train lines
  - Firefighter drone
  - Underwater drone
- Need real/agreed on standards
  - Driver/pilot to ensure safety
  - Remote control to handle unexpected situations
  - Who is responsible/covers accidents ?
  - Certified AI (How ? Who ?)
- Social acceptance

Autonomous Mobility

2018

Autonomous Shuttle navigating forest paths and roads

Stop if unwanted steering, breaking, acceleration

2023-2025

Firefighter Ground/air Drone

Stop if communication lost with base

2023-2024

Underwater drone

Empty ballast if drone lost

2023-2026

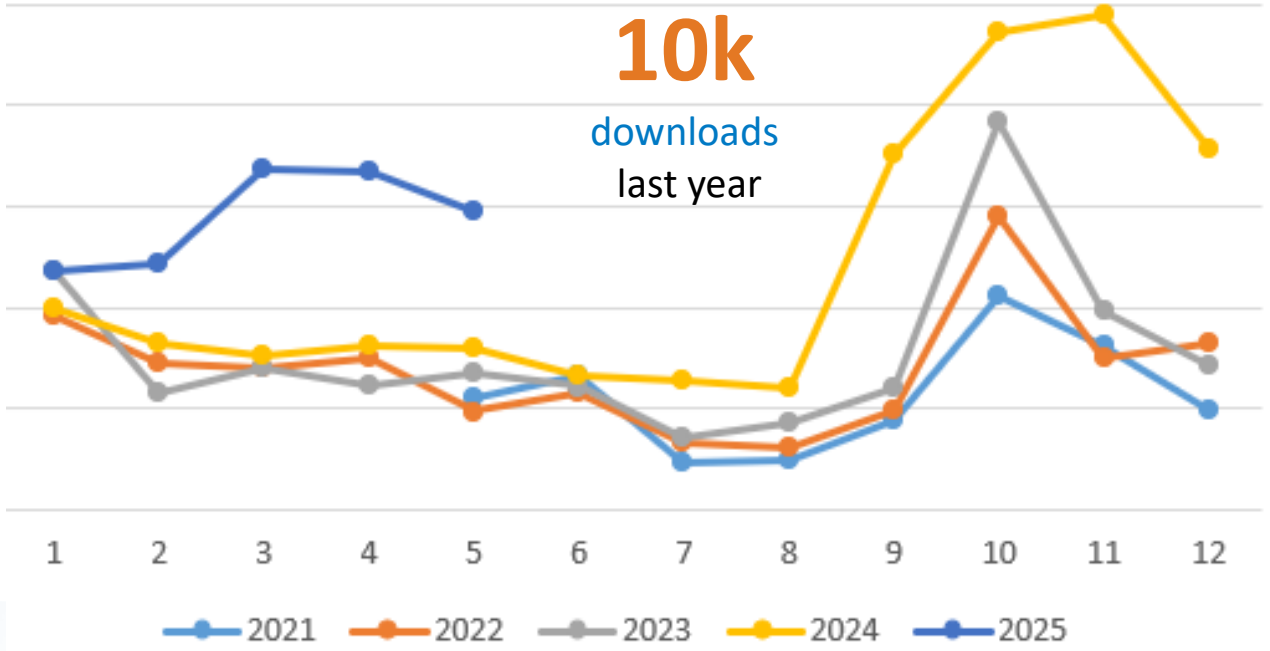
Autonomous Trains (3)

Locate and protect train

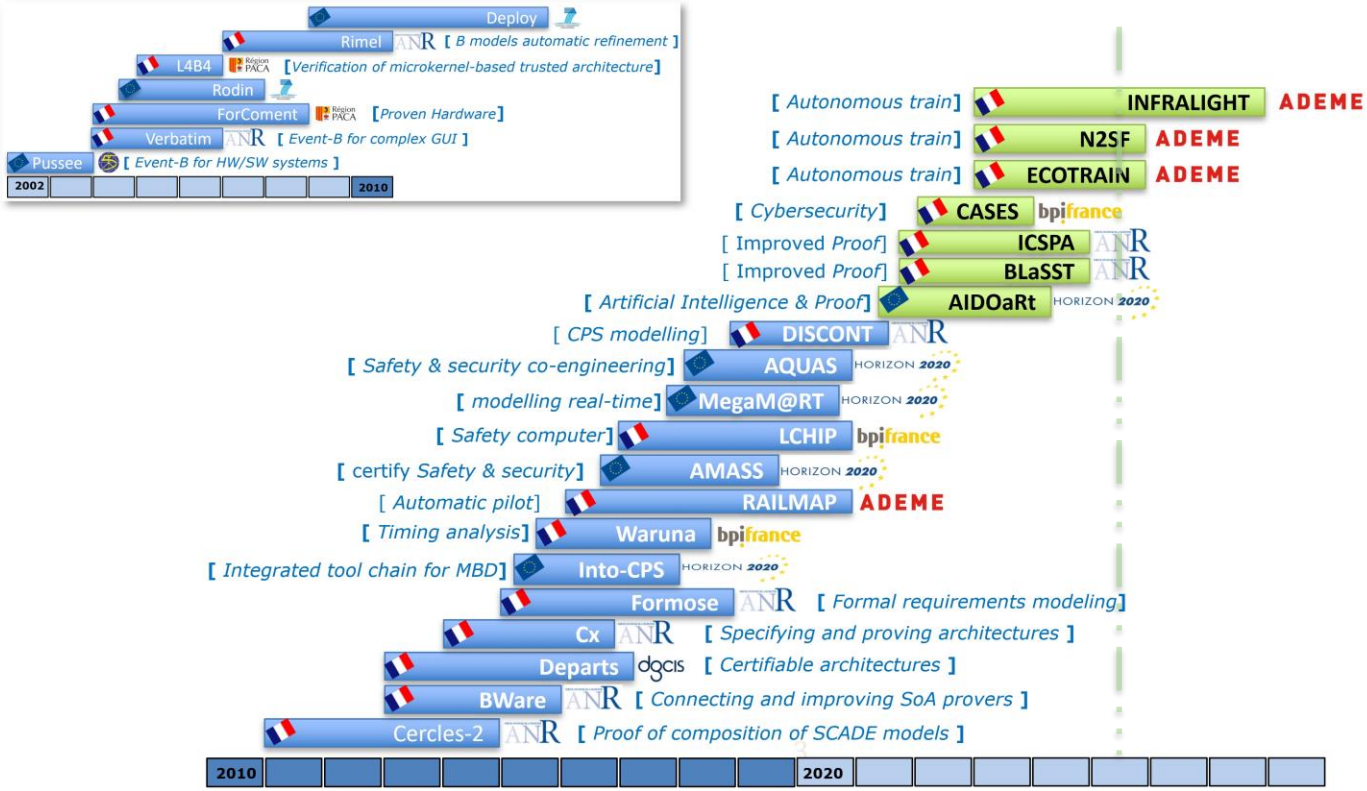
REX: Formal Methods in Autonomous Mobility

- Safety (as in railways) is rarely a subject
- FM not for perception-based AI
  - More for TRUE/FALSE, ON/OFF, Open/Close
- Automotive vs rails
  - More constraints because on tracks
- UIC « new methods for safety demonstration »

Downloads



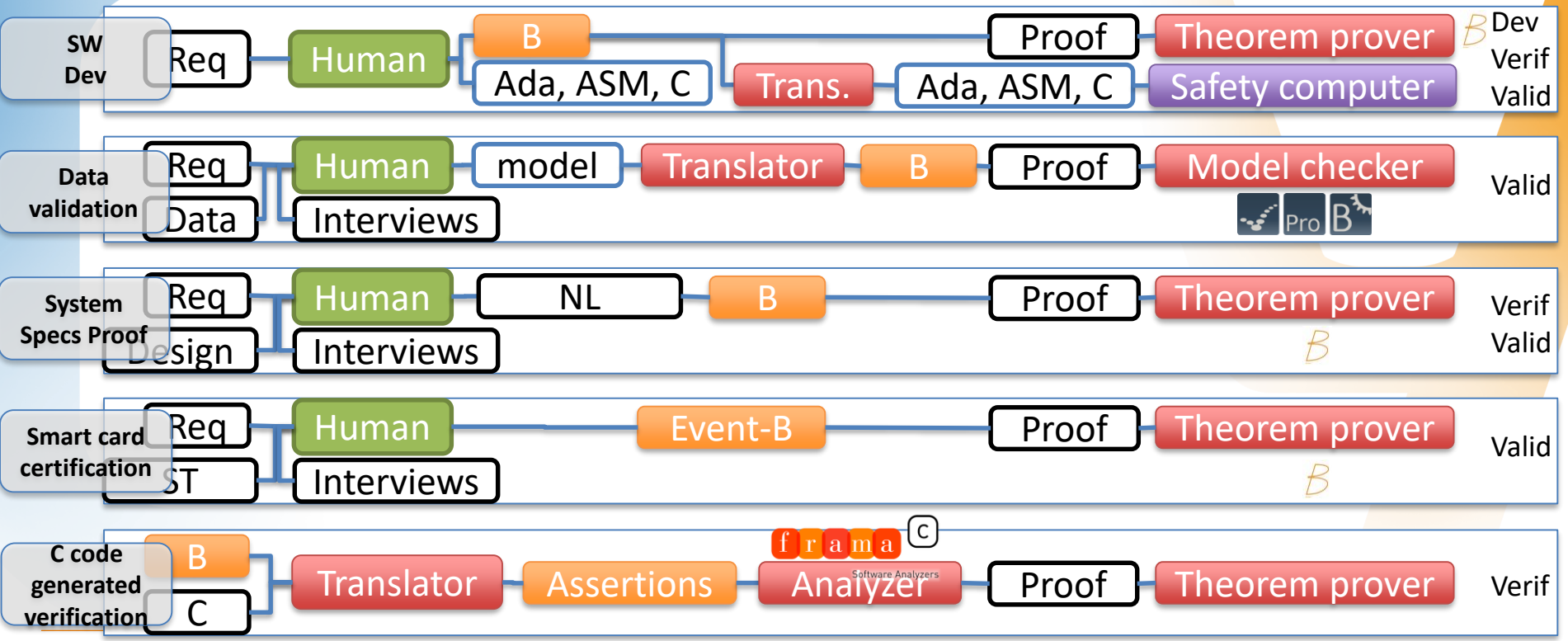
R&D Activity



Dissemination

Formal methods in action

Mostly Atelier B
www.atelierb.eu/en/



Conclusion

- B and Atelier B still alive
  - 10k downloads/year
- 2x tools certified in 2024 and 2025
  - Atelier B T2 Certified SIL4
  - CLEARSY Safety plaform T3 Certified SIL4
- 4 certified industrial processes
- 75% of 150 colleagues work directly or directly with B

CLEARSY
Safety Solutions Designer

Nantes Université
Les Journées Scientifiques

AIX
LYON
PARIS
STRASBOURG

WWW.CLEARSY.COM

Thank you for your attention

https://mooc.imd.ufrn.br/

MOOC
massive open online course

THIERRY.LECOMTE@CLEARSY.COM