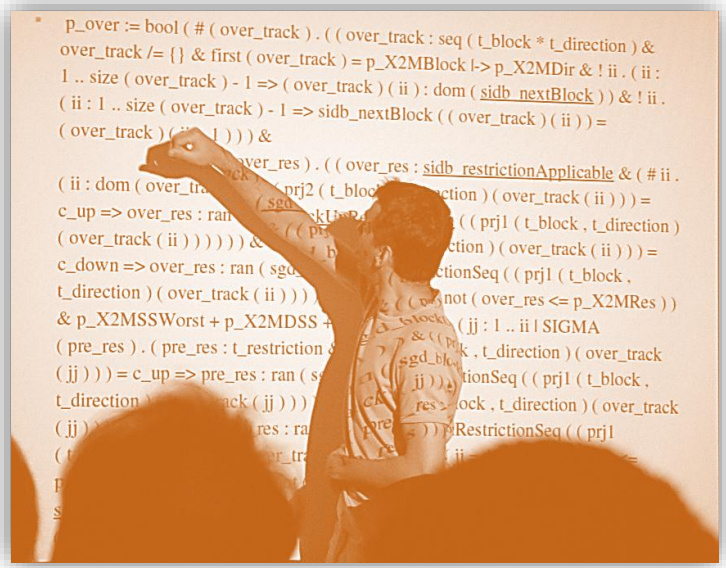
CLEARSY
Safety Solutions Designer

ABZ 2025
JUN2025

Mathematical Proofs And Moving Trains

The Double Life of Atelier B



Lilian Burdy
Engineer 100x
CLEARSY

Thierry Lecomte
R&D Director

THIERRY.LECOMTE@CLEARSY.COM

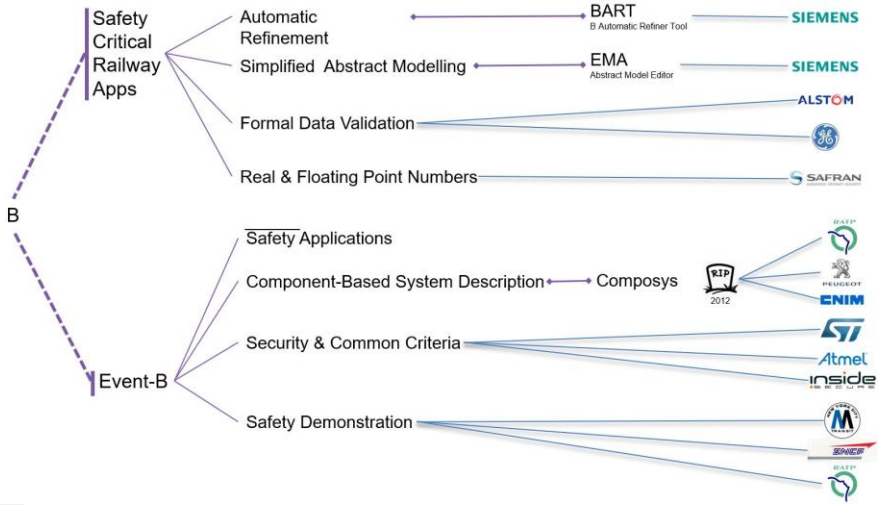
« The session showcases how the versatility of Atelier B has been harnessed to model, prove, and implement robust systems—from automated metros to industrial control.»

Art mostly generated with *ChatGPT or similar*

Flashback 2016

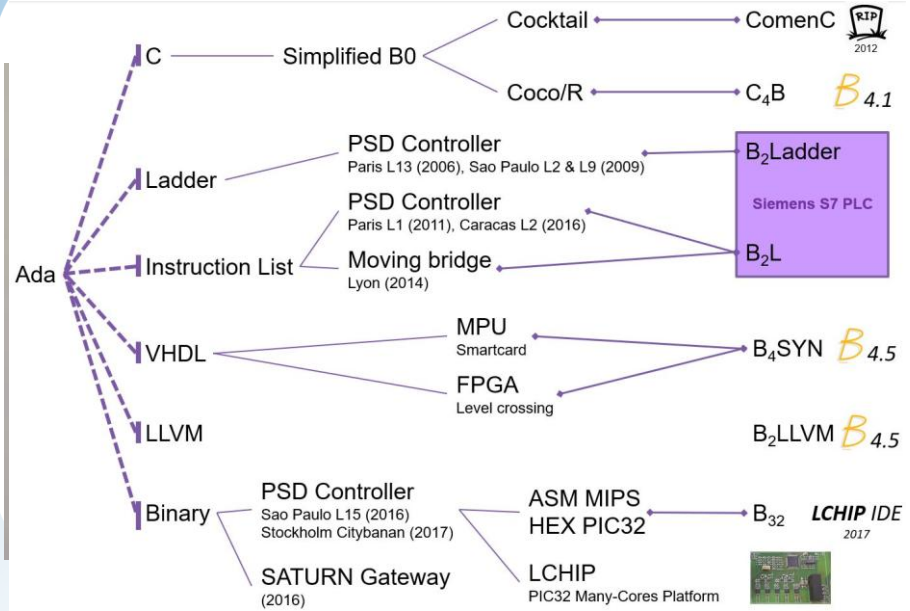
- REX on last 20 years

Flashback 2016



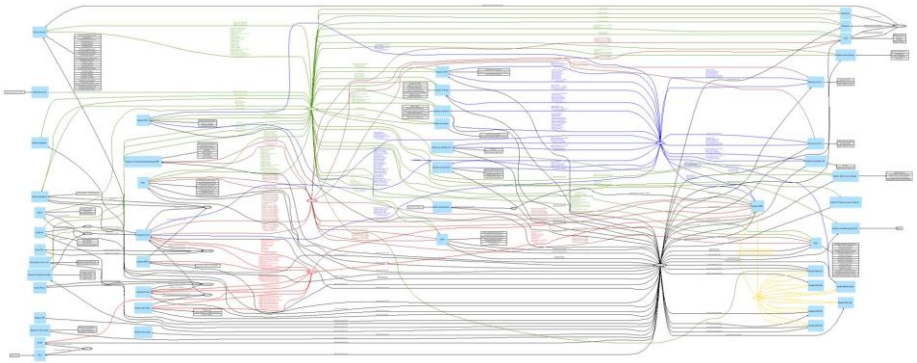
- REX on last 20 years
- Erratic experiments
  - Many domains
  - Many tools

Flashback 2016



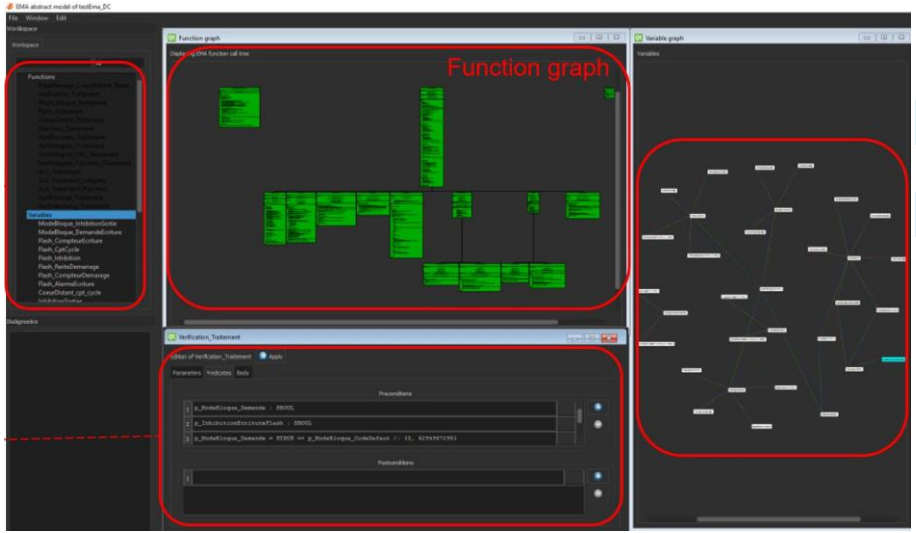
- REX on last 20 years
- Erratic experiments
  - Many domains
  - Many tools

Flashback 2016



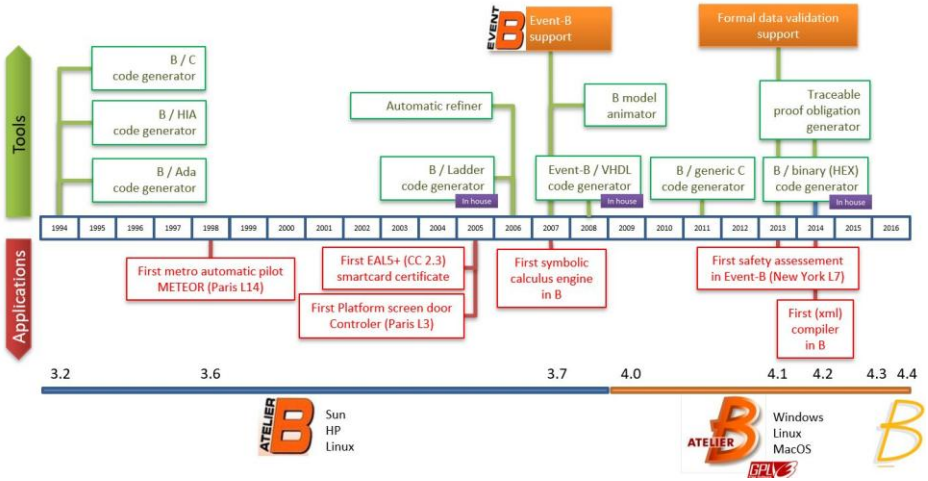
- REX on last 20 years
- Erratic experiments
  - Many domains
  - Many tools

Flashback 2016



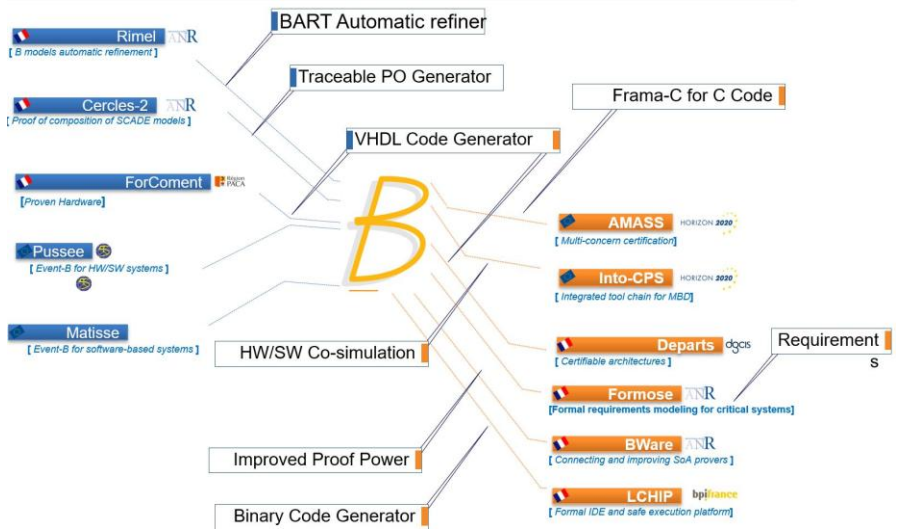
- REX on last 20 years
- Erratic experiments
  - Many domains
  - Many tools

Flashback 2016



- REX on last 20 years
- Erratic experiments
  - Many domains
  - Many tools

Flashback 2016



- REX on last 20 years
- Erratic experiments
  - Many domains
  - Many tools
- Weak vision (perhaps)

What has happened during 2016-2025 ?

from our point of view

Atelier B Community Edition

- Fully functional (Windows, Linux, Mac*)

*: big thanks to Guillaume Verdier for support

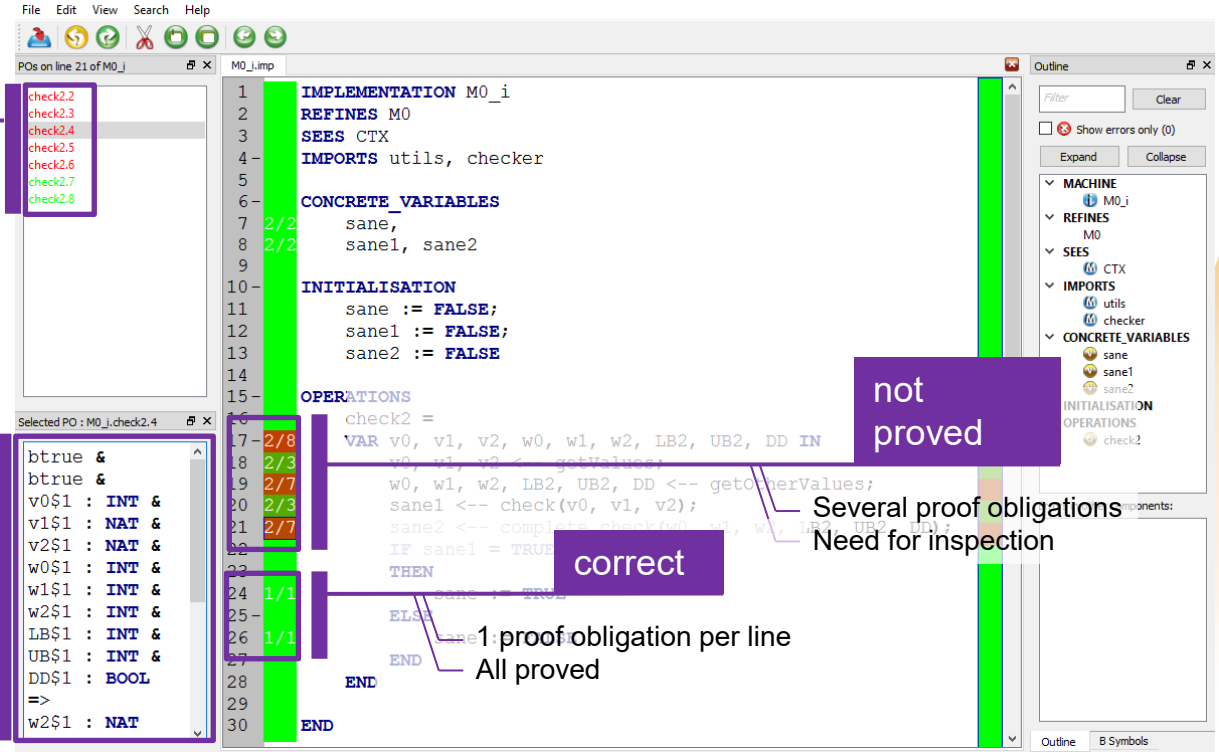
Atelier B Community Edition

- Fully functional (Windows, Linux, Mac*)
- Support B and Event-B
- Model editor with proof information

Model editor with proof information

7 proof obligations

- 2 are proved (green)
- 5 are unproved (red)



inspection

- Integer var is natural
- Obviously wrong

not proved

- Several proof obligations
- Need for inspection

correct

- 1 proof obligation per line
- All proved

Atelier B Community Edition

- Fully functional (Windows, Linux, Mac*)
- Support B and Event-B
- Model editor with proof information
- Automatic B refiner
- Several automatic provers, interactive prover
- Connection with third party provers
- Code generators: C, Rust

Dissemination

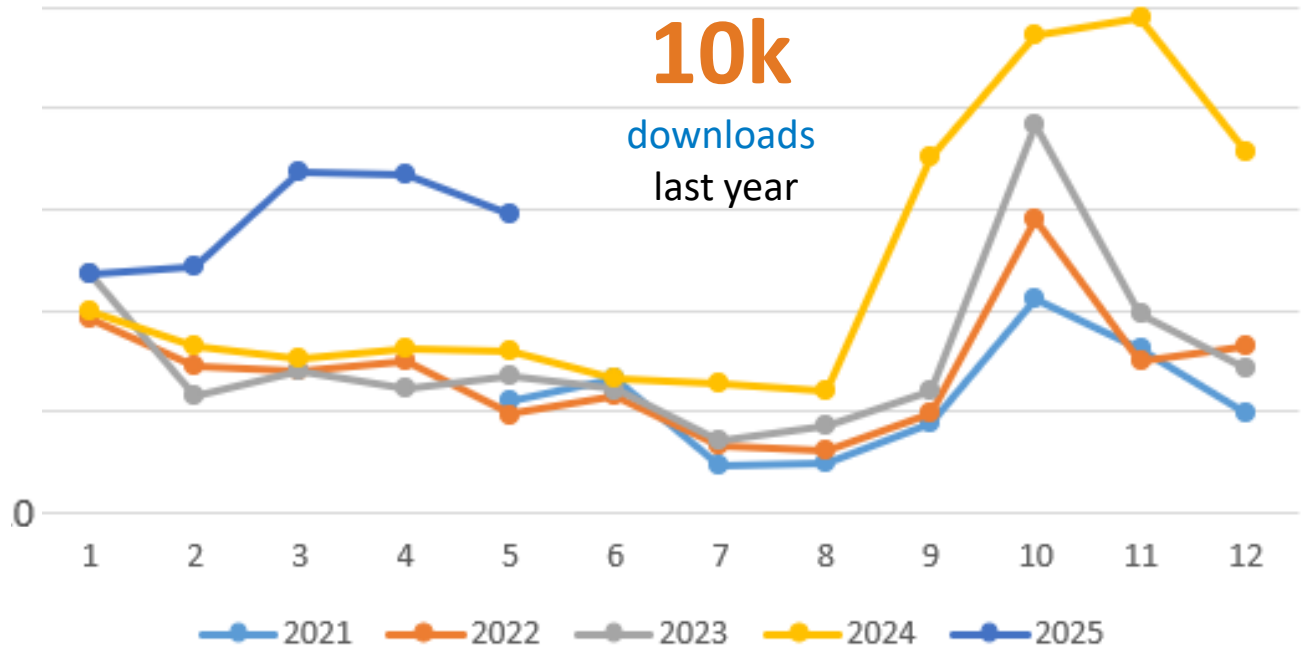
Conference SBMF

December 2016

Natal, Brazil

Dissemination

▶ Downloads



Dissemination

- Downloads
- MOOC on B

Dissemination

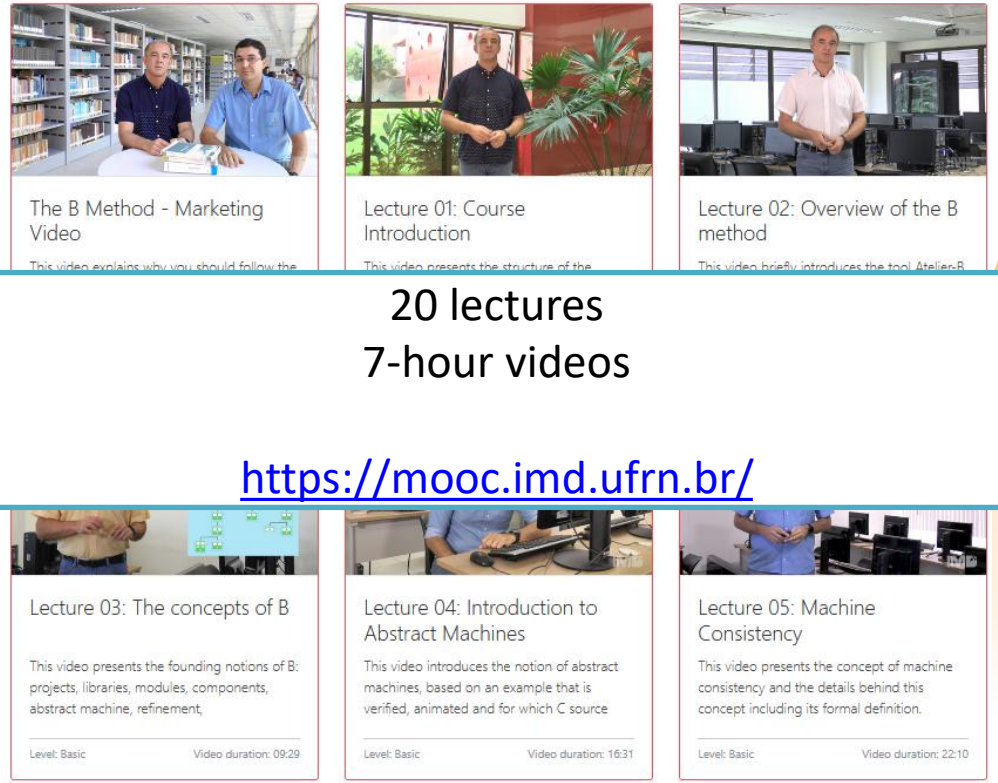
- Downloads
- MOOC on B

Dissemination

- Downloads
- MOOC on B

Dissemination

- Downloads
- MOOC on B



20 lectures
7-hour videos

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

Dissemination

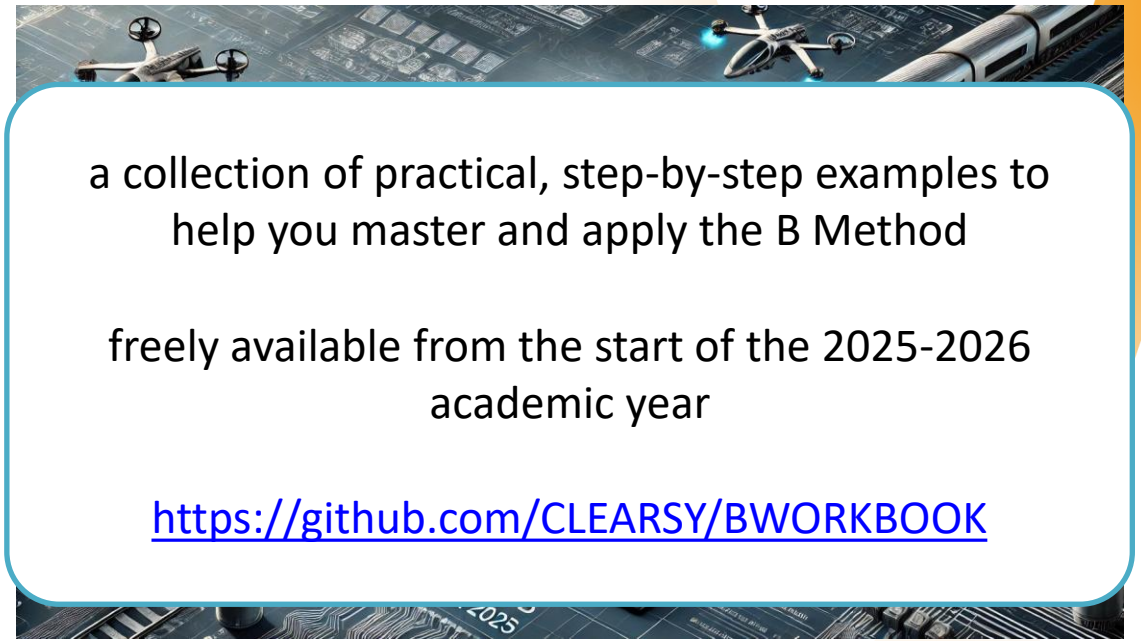
- Downloads
- MOOC on B
- Hackathon

https://github.com/CLEARSY/hackathon-2024

https://github.com/CLEARSY/hackathon-2025

Dissemination

- Downloads
- MOOC on B
- Hackathon
- B Workbook



a collection of practical, step-by-step examples to help you master and apply the B Method

freely available from the start of the 2025-2026 academic year

https://github.com/CLEARSY/BWORKBOOK

Dissemination

- Downloads
- MOOC on B
- Hackathon
- B Workbook
- Open source tools & data

•Half million proof obligations stored in POG files https://github.com/CLEARSY/apero

•A translation to SMTLib of these proof obbligations, stored as SMTLIB-2.6 files. The translation has been realized with ppTransSmt.

https://github.com/CLEARSY/pptranspog

Collaborative R&D Projects

- AMASS — **A**rchitecture-driven, **M**ulti-concern and Seamless **Ass**urance and Certification of Cyber-Physical Systems
- AQUAS — **A**ggregated **Qu**ality **A**ssurance for **S**ystems
- MegaM@RT — A scalable model-based framework for continuous development and runtime validation of complex systems

82 partners

Safety, security, and performances co-engineering

CLEARSY used Frama-C for code generation

Collaborative R&D Projects

- AMASS
- AQUAS
- MegaM@RT
- DISCONT

Correct Integration of **DIS**crete and **CONT**inous models

- LORIA (leader),
- IRIT,
- CLEARSY,
- LACL,
- TSP-SAMOVAR

DISCONT aims to provide efficient and easy to use refinement and proof-based techniques and tools that scale to complex systems and offer more convenient and automatic proof platforms centered around B and Event-B, with Atelier-B and Rodin.

ANR AGENCE NATIONALE DE LA RECHERCHE

Collaborative R&D Projects

- AMASS
- AQUAS
- MegaM@RT
- DISCONT
- AIDOART

AI-augmented automation supporting modelling, coding, testing, monitoring and continuous development in Cyber-Physical Systems

- Mälardalen University (leader)
- 31 partners …

AIDOaRt aims at using AIOps to automate decision and process and complete system development tasks.
CLEARSY used LLMs for interactive proof assistance.

Collaborative R&D Projects

- AMASS
- AQUAS
- MegaM@RT
- DISCONT
- AIDOART
- ICSPA

Interoperable and **C**onfident **S**et-based **P**roof **A**ssistants

- Samovar Paris (leader),
- CLEARSY,
- INRIA Nancy,
- INRIA Saclay,
- IRIT Toulouse,
- LRIMM Montpelier

ICSPA aims at designing and implementing an exchange framework, through B, Event-B and TLA+ systems can share their proofs and theories, making them effectively interoperable.

Collaborative R&D Projects

- AMASS
- AQUAS
- MegaM@RT
- DISCONT
- AIDOART
- ICSPA
- BLaSST

Enhancing **B La**nguage Reasoners with **S**AT and **S**MT **T**echniques

- INRIA Nancy (leader),
- CLEARSY,
- CRIL Lens,
- Université de Liège

The BLaSST project targets bridging combinational and symbolic techniques in automatic theorem proving and validating the results for proof obligations generated from B models.

ANR AGENCE NATIONALE DE LA RECHERCHE

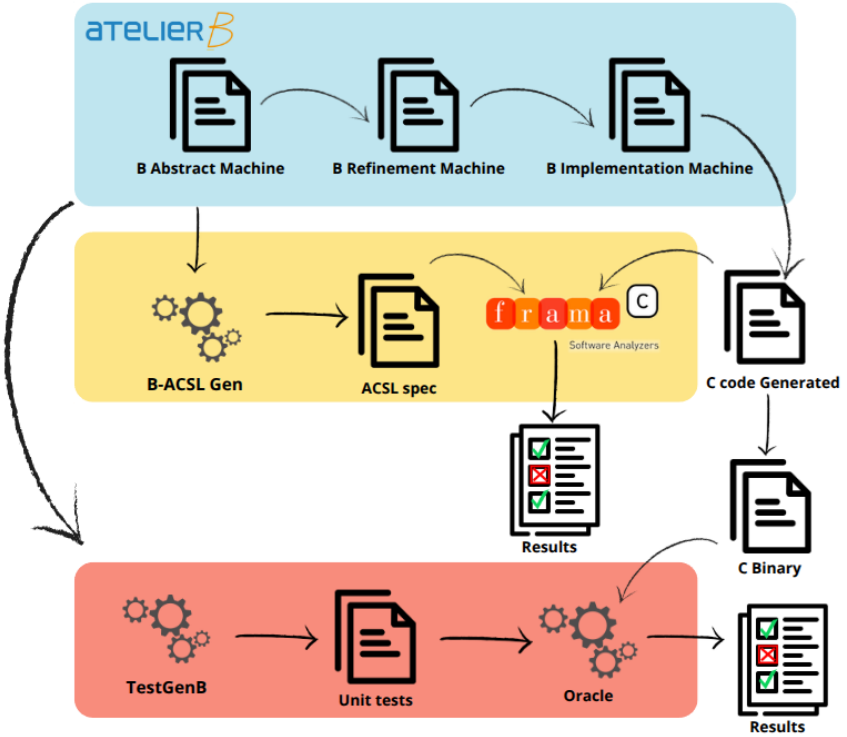
Collaborative R&D Actions

V&V of C code
generated from B model

Fagner Morais

Marcel Oliveira

Instituto Metrópole Digital
UFRN, Brazil



Agenda

Atelier B Professional Edition

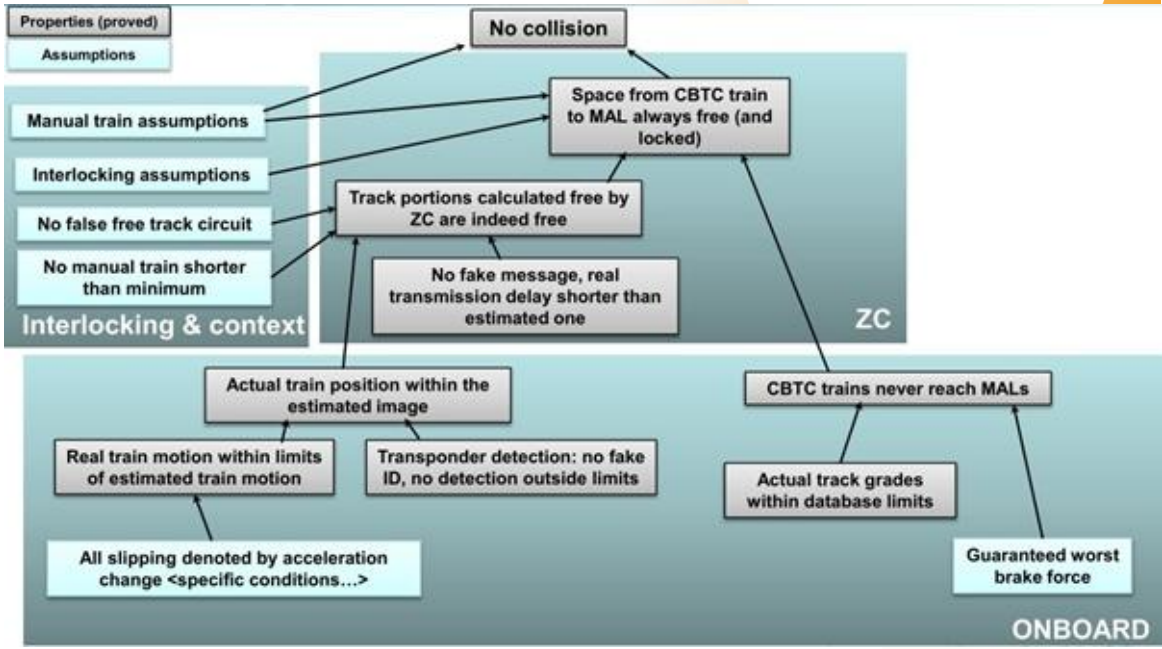
- Community Edition extended with
  - Tight support
  - More frequent updates
  - Rule proof tools
  - Ada Code generator

Applications: Safe Software

- ATP Paris
  - L1, L4, L14 (Olympics)
  - To come: L15, L16, L17, L18
- ~30% of worldwide CBTC
  - >20B passengers transported
  - 0 fatality
- Alstom: Urbalis
- Siemens: Trainguard

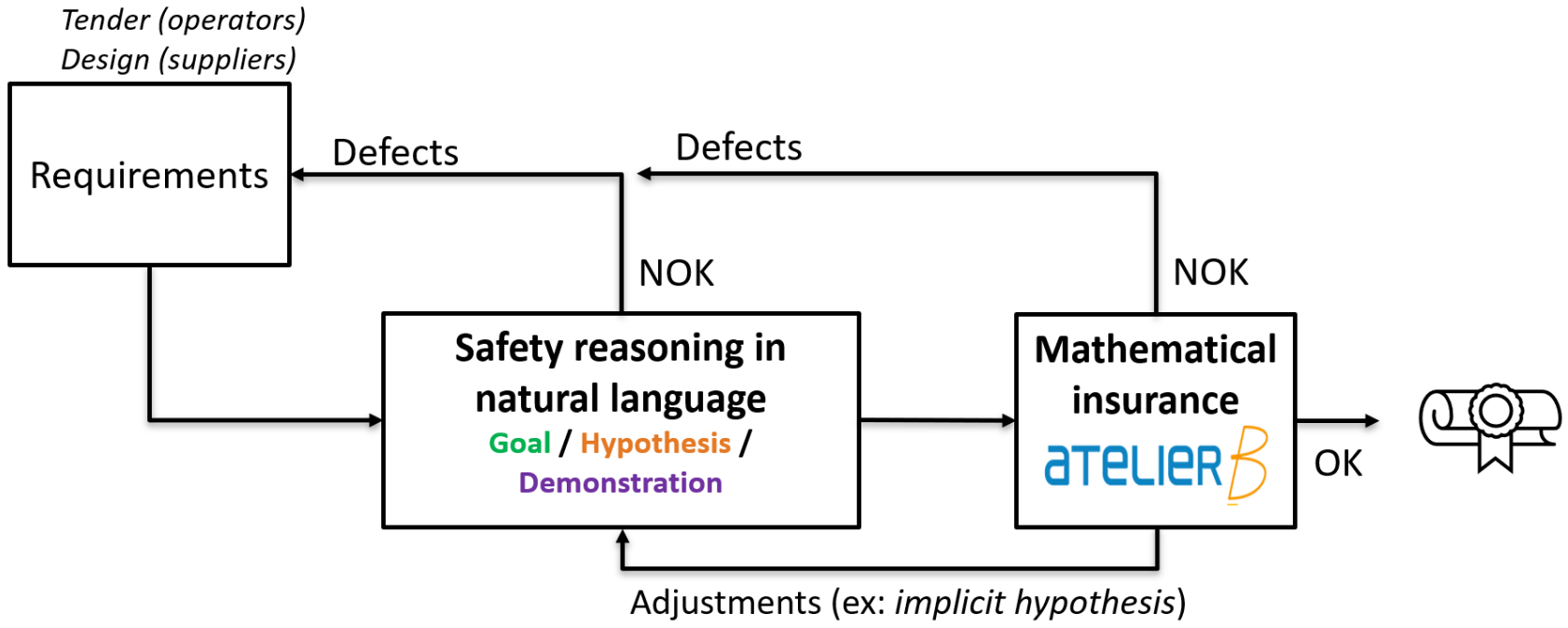
Applications: Safety System Proof

- Safety property obtained by **pure logical reasoning** only
- What is modelled is the safety reasoning instead of the whole system
- Output is natural language report (~200 pages) validated by an equivalent proven formal model



FPoSLS applied for NYCT to Thales CBTC [2007]

Applications: Safety System Proof



Applications: Safety 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

SNCF – ERTMS Regional
Preliminary Safety Analysis

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”

Applications: SmartCard

- Common Criteria:
  - Only standard imposing formal methods
  - EAL6+:
    - formal model,
    - functional specification complies with security policy,
    - tracability with implementation

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

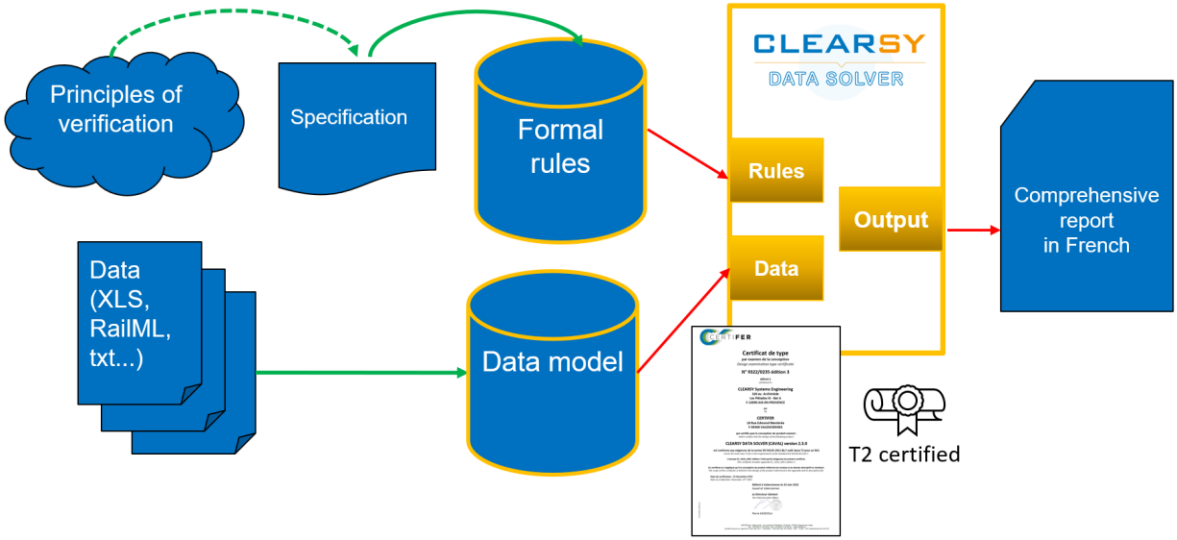
Certification with French and German Evaluation Centers
Knowledge Transfer (CC 3.1 EAL6+)

2024-2025

Transition to CC:2022

Applications: Formal Data Validation

- Verify parameters (constants) at the SIL4 level
- Ad-hoc formal data language based on B mathematical language
- ProB able to handle 10 Mloc



Applications: 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
Technical plans vs RailML

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."

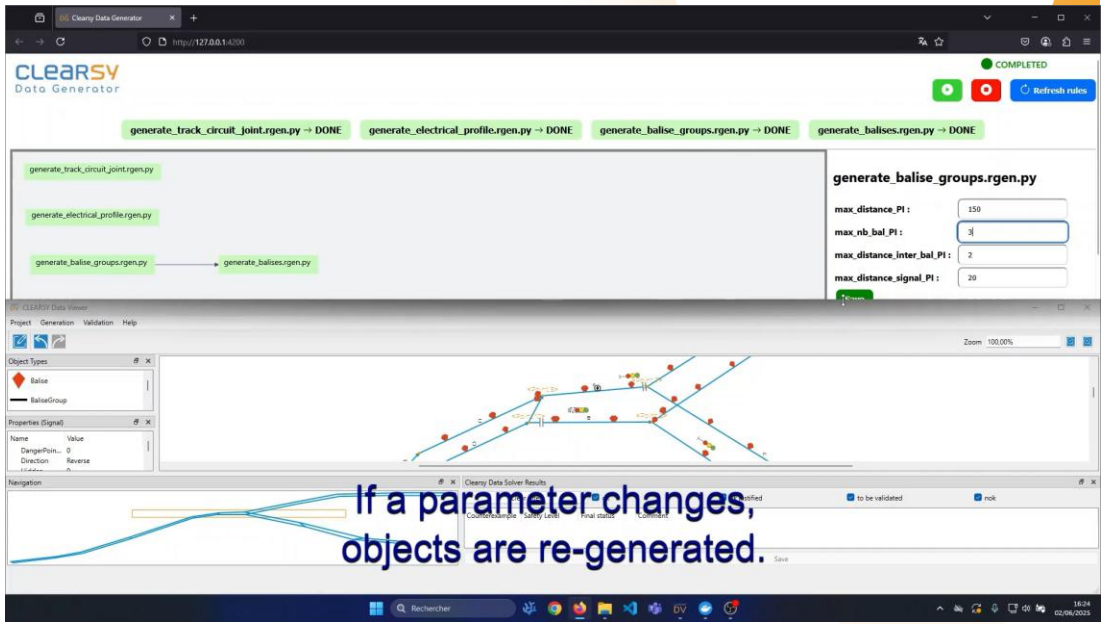
References:

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

Collaborative R&D Projects

▶ NS2F

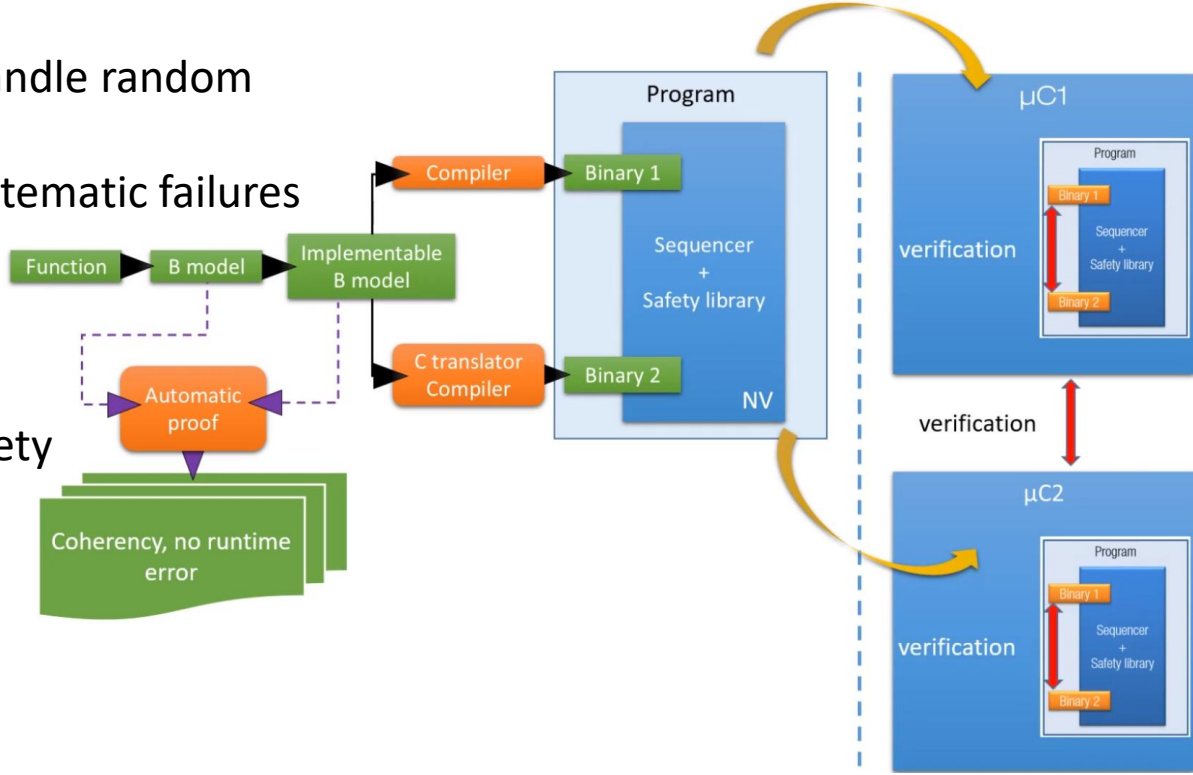
- Regional line, low traffic
- Track plan editor
- Signalling generated with scripts
- Validation with ProB



Agenda

CLEARSY Safety Platform

- Safety computer able to handle random failures
- Programmed with B for systematic failures
- 4oo4 Software
- 2oo2 Hardware
- Developer cannot alter safety
- Usable for any stoppable safety process

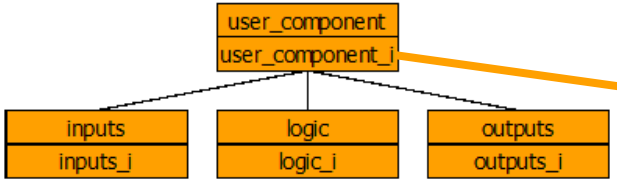


Atelier B CSP Educational Edition

ATELIER B 24.04
CSP EDUCATIONAL VERSION

> Atelier B 24.04 CSP – Windows 11 (also works with 10)
> Atelier B 24.04 CSP – Linux Debian 11
> Atelier B 24.04 CSP – Linux Debian 12
> Atelier B 24.04 CSP – Linux Ubuntu 22.04
> Atelier B 24.04 CSP – Linux Ubuntu 23.10
> Atelier B 24.04 CSP – Linux Ubuntu 24.04
> Script cssp_install.sh
> Installation Guide
> Programming Handbook (Feb 2020)

Atelier B CSP Educational Edition




```
user_app =
BEGIN
    divergence_test_var :=  0;
    read_inputs;
    user_logic;
    write_outputs
END;
```

call

call

call

```
read_inputs  =
BEGIN
    I0 <-- read_global_input(0);
    I1 <-- read_global_input(1);
    I2 <-- read_global_input(2)
END;

po <-- get_I0 =
BEGIN
    po <-- read_global_input(0)
END;

po <-- get_I1 =
BEGIN
    po <-- read_global_input(1)
END;

po <-- get_I2 =
BEGIN
    po <-- read_global_input(2)
END
```

used by

```
user_logic = skip;

po <-- get_O0 =
BEGIN
    po := O0
END;

po <-- get_O1 =
BEGIN
    po := O1
END
```

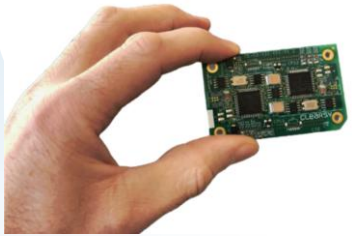
used by

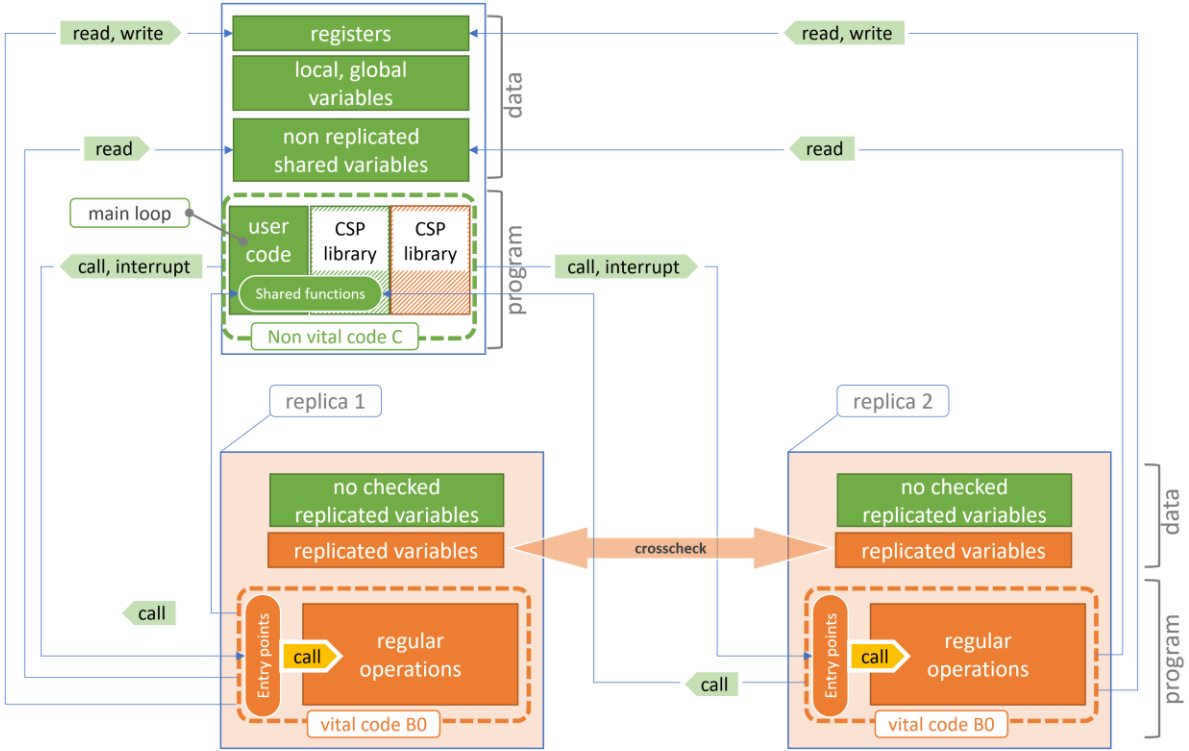
used by

```
write_outputs =
VAR
    lsb
IN
    lsb:(lsb : uint8_t);

    lsb <-- get_O0;
    write_global_output(0, lsb);

    lsb <-- get_O1;
    write_global_output(1, lsb)
END
```

Programming the CLEARSY Safety Platform
Academic version

Atelier B CSP Industrial Edition





Applications

- PSD São Paulo

Applications

- PSD São Paulo
- PSD Stockholm
- PSD Brisbane

Applications

- PSD São Paulo
- PSD Stockholm
- PSD Brisbane

- Ground and underwater drones

Dissemination

▶ Course with CSP*

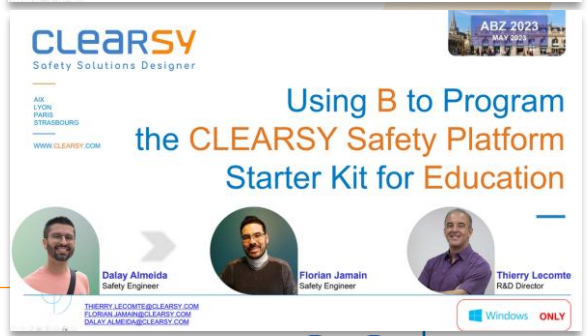
- France: CentraleSupelec, Telecom-Paris, Univ. Dauphine, Univ. Aix-Marseille, ESIEE, UPEC, UPMC, ENSIIE, etc.
- Europe: Univ. Liège, Univ. Swansea, Univ. Florence, etc.
- South-America: IFRN, UFRN, UFRJ

*: CLEARSY Safety Platform is not CSP

Dissemination

- Course with CSP*
- Hackathon

- Tutorials first (Europe, North and South America)
- Hackathon after COVID
  https://github.com/CLEARSY/hackathon



Dissemination

- Course with CSP*
- Hackathon
- Summer school

Dissemination

- Course with CSP*
- Hackathon
- Summer school

ROBOTICS APPLICATIONS & INNOVATION 2025
Third Summer School on Robotic Mission Engineering.

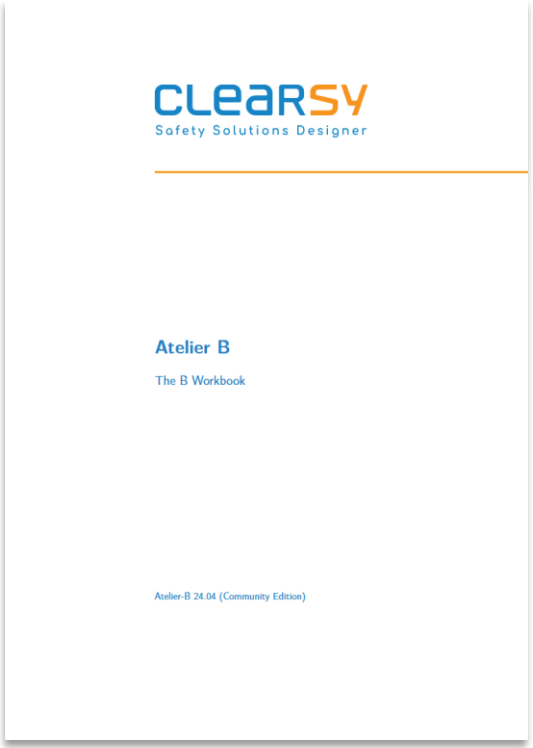
Modelling with Robosim and implementing a safety function with the CLEARSY Safety Platform for a flying firefighter drone

https://rome.gesaduece.com.br/

Dissemination

- Course with CSP*
- Hackathon
- Summer school
- B Workbook

  - Specific exercices



Collaborative R&D Projects

▶ LCHIP

Low **C**ost **H**igh **I**ntegrity **P**latform

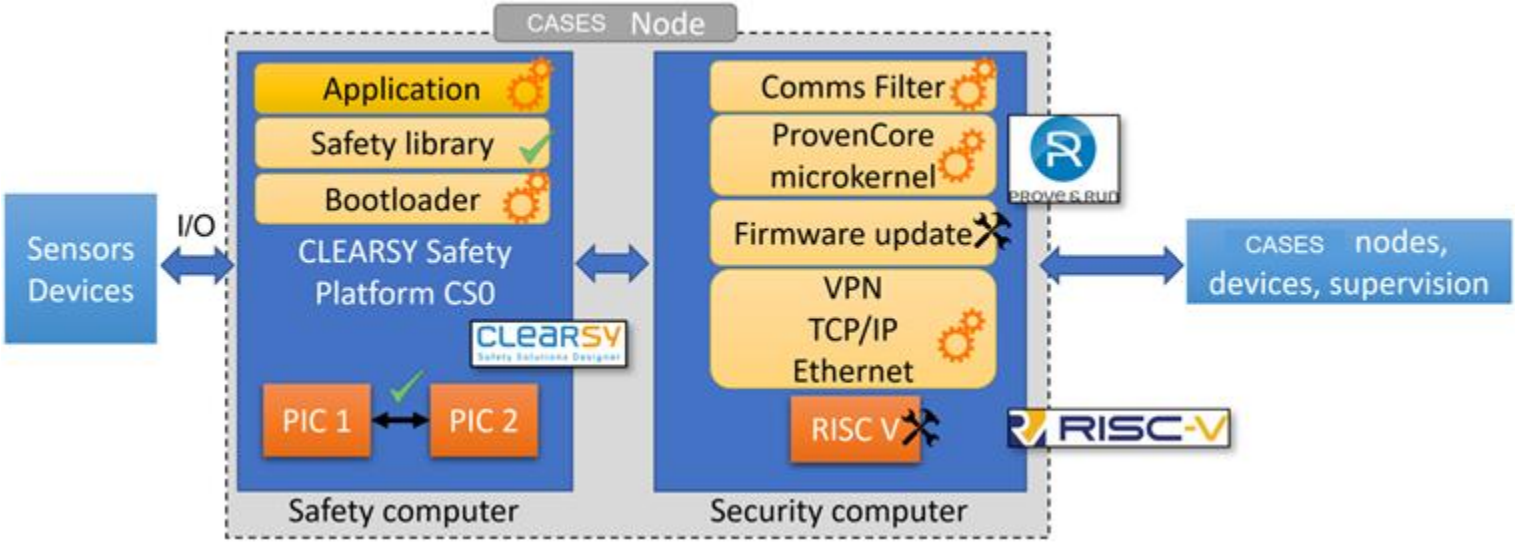
- CLEARSY (leader),
- OCaml Pro,
- SNCF,
- IFSTTAR,
- LIP6,
- LRI

The LCHIP project aims to provide:
• a complete IDE,
• a secure and low-cost platform for the execution of these applications,

bpifrance

Collaborative R&D Projects

- LCHIP
- CASES



bpifrance

Stratégie Nationale Cyber
« Développement de technologies innovantes critiques »

Collaborative R&D Projects

- LCHIP
- CASES
- ECOTRAIN

  - Autonomous train
  - Regional, low-traffic train line
  - Localization with electromagnetic waves in the rails

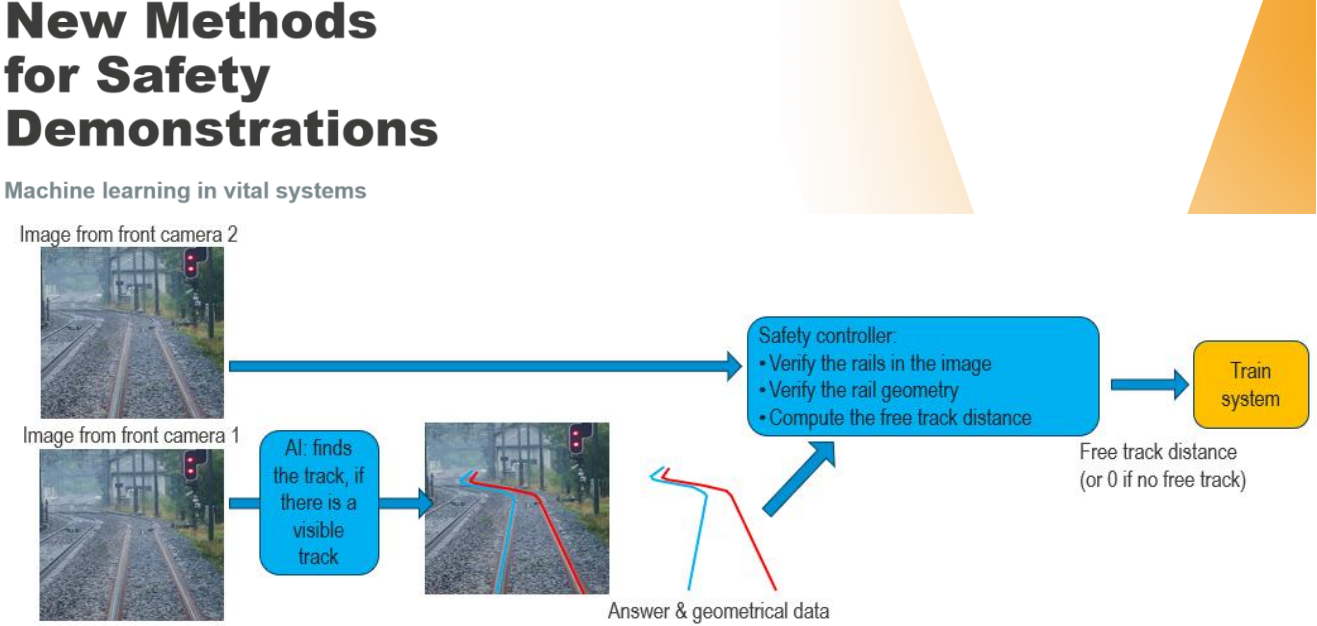
Collaborative R&D Projects

- LCHIP
- CASES
- ECOTRAIN
- INFRALIGHT

- Autonomous train
- Regional, low-traffic, lightweight train line
- Composite, pile-mounted, ballast less track, with all infrastructure integrated into the track, including on-board/ground communication radio

Collaborative R&D Projects

- LCHIP
- CASES
- ECOTRAIN
- INFRALIGHT
- UIC NMSD



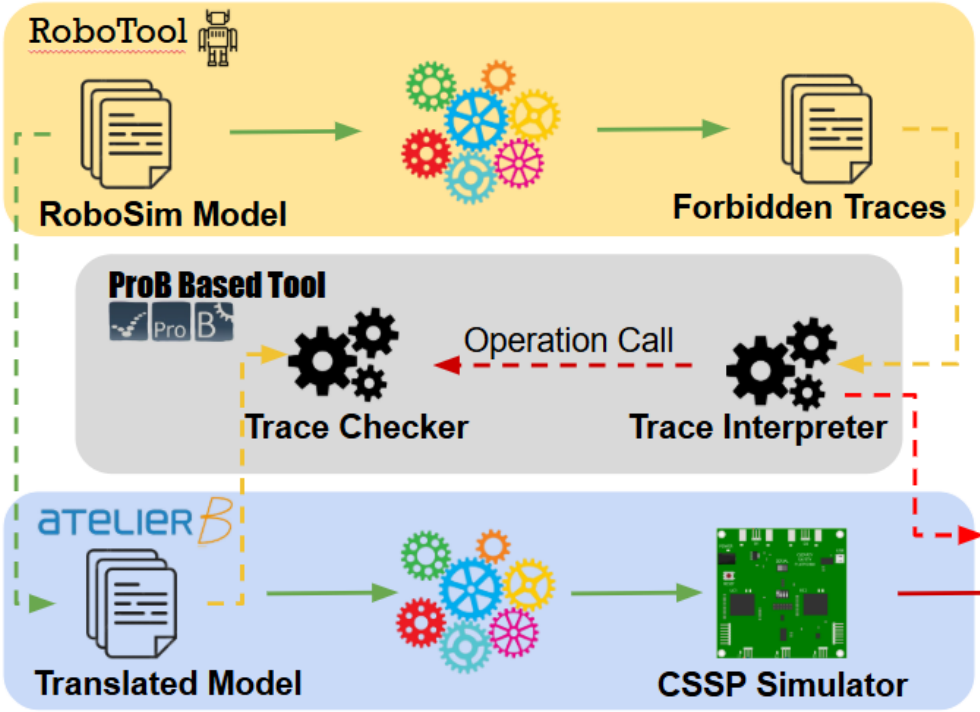
Collaborative R&D Actions

Translation of RoboSim Language to CLEARSY Safety Platform

Paulo Bezerra

Marcel Oliveira

Instituto Metrópole Digital
UFRN, Brazil



Agenda

Railways Certification

▶ Atelier B T2 Certified Edition

- Joint effort from Alstom, CLEARSY, RATP, Siemens
- Certifier tool to replay recent projects
- Development process up to proof
  - Code generation excluded

2024

CERTIFER

DESIGN EXAMINATION TYPE CERTIFICATE

Reference : EC_9825_0450 edition V01

The scope of this certificate is limited to the design of the product referenced in the appendix and its description file. This certification was performed in accordance with CERTIFER repository RF0015 version 4.

Object:	**ATELIER B T2** Version: certifier-1.0 (450e2faf23718286e5e0db3681f01a613cdb12f0) SOFTWARE VERSION FILE D689 version 01-00
Owner of Certificate:	CLEARSY Parc de la Duranne 320 Av. Archimède - Les Pléiades III, Batiment A 13100 Aix en Provence - FRANCE
Requirements:	**T2 for a SIL4**
Bases of Assessment:	CENELEC EN50128 :2011/A2 section 6.7 IEC 62279 :2015 section 6.7 CENELEC EN50129 :2018 section 6.3
Accompanying Documentation:	Appendix to certificate reference EC_9825_0460 revision 01 This documentation is an integral part of this certificate and may not be separated from it.
Conditions and limits of use:	See section 4.5 of the Accompanying Documentation.
Validity:	This certificate validity is unlimited as long as the object of certification remains unchanged (refer to section 4.3.1 of the Accompanying Documentation). Start: 20/12/2024 End: Unlimited.
Date of issue:	20/12/2024

Issued in Valenciennes by
The Technical Director

Jérôme CARLIER

Railways Certification

- Atelier B T2 Certified Edition
- CLEARSY Safety Platform T3

  - Development process includes proof and code generation
  - 26 Safety Related Application Conditions to fulfill

CERTIFER 2023

Design examination type certificate

Certificat de type par examen de la conception

N° 9594/0262 edition 2

Attributed to
Délivré à

CLEARSY
320 Av. Archimède - Pléiades III
F-13100 Aix-en-Provence
by
par

CERTIFER SA
18 Rue Edmond Membrée
F-59300 VALENCIENNES

Which certifies that the design of the following product:
Qui certifie que la conception du produit suivant :

GENERIC PRODUCT
CLEARSY SAFETY PLATFORM
BASELINE 1.0.2
Meets SIL4 requirements of the standards
Est conforme aux exigences SIL4 des normes
CENELEC EN 50126:2017, EN 50129:2018, EN 50128:2011

This certificate includes appendix EC_9594_0263 version 2
L'annexe EC_9594_0263 version 2 fait partie intégrante du présent certificat

The scope of this certificate is limited to the design of the product referenced in the appendix and its description file.
Ce certificat ne s'applique qu'à la conception du produit référencé en annexe et au dossier descriptif en résultant.

This certification was performed in accordance with CERTIFER standard RF0015 version 4.
La présente certification a été conduite en conformité avec le référentiel CERTIFER RF0015 version 4.

Date of certification: January 11th, 2021
Date de certification : 11 Janvier 2021

Issued at Valenciennes on July 28th, 2023.
Délivré à Valenciennes

The Technical Director
Le Directeur Technique

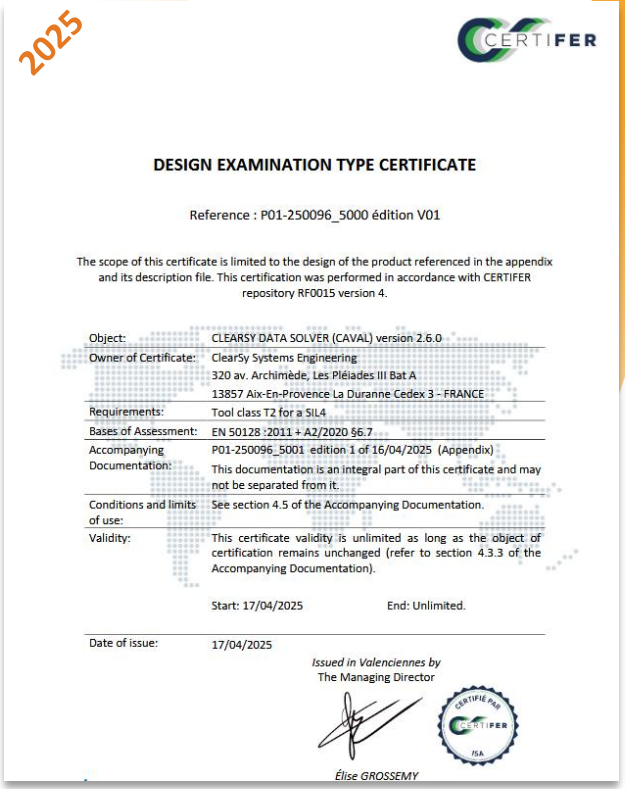
Jérôme CARLIER

Railways Certification

- Atelier B T2 Certified Edition
- CLEARSY Safety Platform T3
- CLEARSY Data Solver T2

SIL4

- Tool integrated into customer dev, V&V cycle
- ProB inside



2025

CERTIFER

DESIGN EXAMINATION TYPE CERTIFICATE

Reference : P01-250096_5000 édition V01

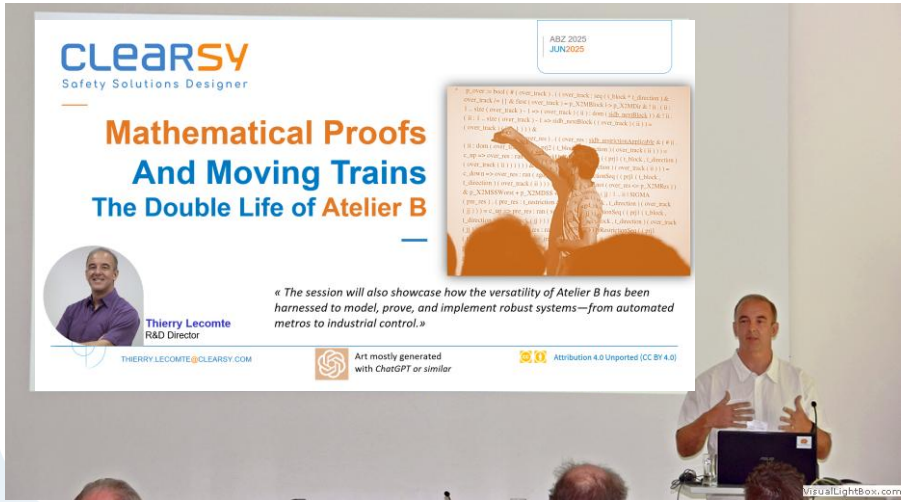
The scope of this certificate is limited to the design of the product referenced in the appendix and its description file. This certification was performed in accordance with CERTIFER repository RF0015 version 4.

Object:	CLEARSY DATA SOLVER (CAVAL) version 2.6.0
Owner of Certificate:	ClearSy Systems Engineering 320 av. Archimède, Les Pléiades III Bat A 13857 Aix-En-Provence La Duranne Cedex 3 - FRANCE
Requirements:	Tool class T2 for a SIL4
Bases of Assessment:	EN 50128 :2011 + A2/2020 §6.7
Accompanying Documentation:	P01-250096_5001 edition 1 of 16/04/2025 (Appendix) This documentation is an integral part of this certificate and may not be separated from it.
Conditions and limits of use:	See section 4.5 of the Accompanying Documentation.
Validity:	This certificate validity is unlimited as long as the object of certification remains unchanged (refer to section 4.3.3 of the Accompanying Documentation). Start: 17/04/2025 End: Unlimited.
Date of issue:	17/04/2025

Issued in Valenciennes by
The Managing Director

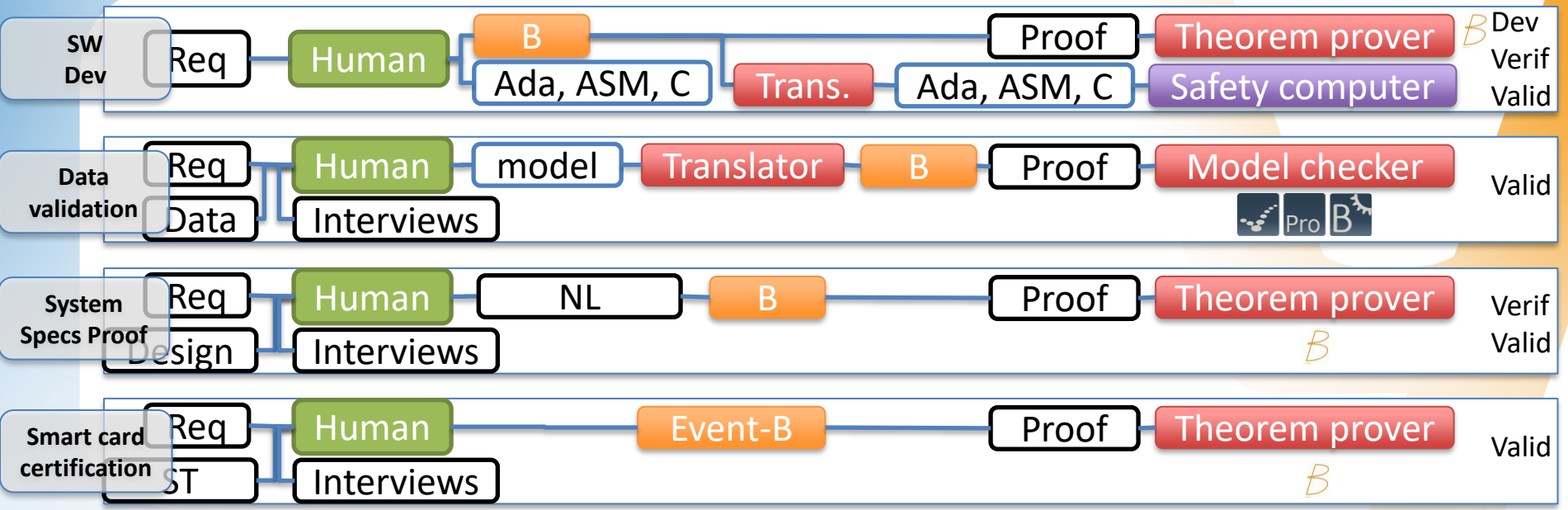
Élise GROSSEMY

Feedback on 2016-2025



- Maturity
- More focused experiments
  - Safety-related domains
  - Application-oriented tools
- Stronger vision

Industrial Formal Processes



Conclusion & Perspectives

From 2016

- Atelier B still alive
- Is not only a tool for piloting metros
  - Opening doors safely
  - Validating parameters
  - Contributing to the certification of microcircuits
- New usage
  - Integrated to PLC
  - Applications to (nuclear) energy automation
- Forthcoming evolutions
  - Linked with industrial needs
  - Funded by industrial & collaborative R&D projects
- Let's meet for ABZ 2026 !

From 2025

✓ 10k downloads/year, CSP in CS, certified 2x

✓ Is not only a tool for piloting metros
- Opening doors safely
- **Validating parameters**
- **Safety reasoning proof**
- *Contribution to the certification of microcircuits*

✓ New usage
- Integrated to PLC for **automatic/autonomous mobility** (ground, air, underwater)

✓ Forthcoming evolutions
- Linked **only** with industrial needs
- Funded by industrial & collaborative projects
- Application to nuclear energy automation?

✗ Back one year in advance!
ABZ 2035?

Conclusion & Perspectives

What's next ?

Autonomous Mobility

Where's next ?

Driverless car !

Newton bridge

Redinha beach

Natal, Brazil

Perfect place to practice Formal Methods

Daring autonomous driving there ?

CLEARSY
Safety Solutions Designer

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