CLEARSY
Safety Solutions Designer

DISCORAIL
OCT2024

Formal Validation and ERTMS Simulation

*« Presentation of the challenges and methods involved in implementing and verifying the **European Railway Traffic Management System**, including **formal modeling**, automatic proof, and model-checking to enhance deployment confidence.»*

Thierry Lecomte
R&D Director

THIERRY.LECOMTE@CLEARSY.COM

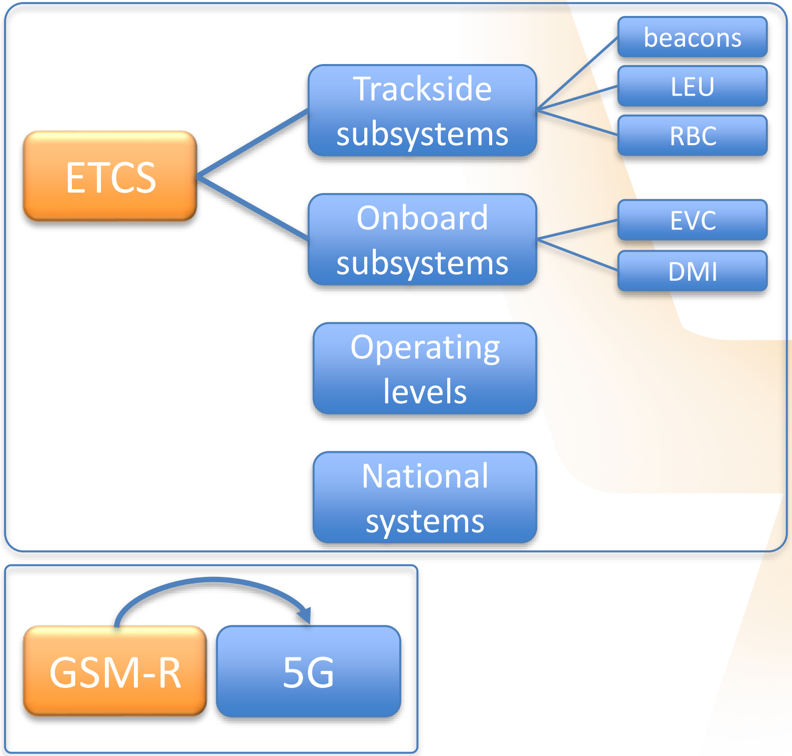
Art mostly generated
with *ChatGPT or similar*

ERTMS

- Structure and Concepts
- Support
- Conformance
- Application of Formal Methods

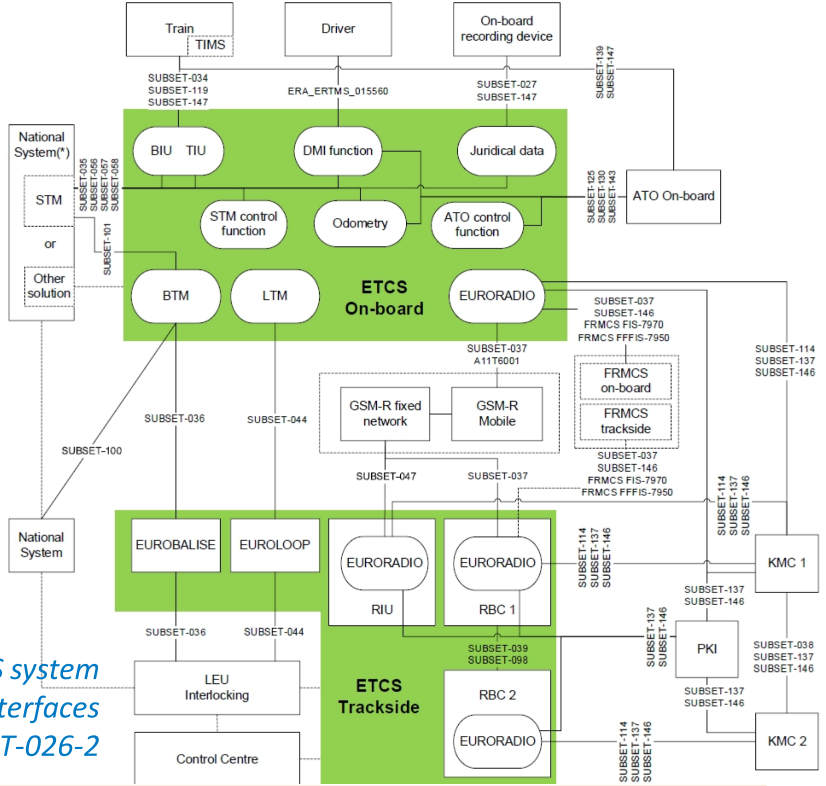
ERTMS: Structure and Concepts

- New system of standards
- Replace national C&C systems
- Increased capacity
- Higher reliability rates
- Improved safety
- Open supply market



ERTMS: Support

- Specification as 100x SUBSETS
- System, implementation, testing specs
  - Glossary of Terms and Abbreviations (SS-023)
  - ETCS System Requirements (SS-026)
  - Dimensioning and Engineering Rules (SS-040)
  - Functional Interface Specification
  - Form Fit Interface Specification
  - Test specification (SS-076), sequences (SS-094)
- Continuous evolution
  - Baseline 1: 2000
  - Baseline 2: 2008
  - Baseline 3: 2016
  - Baseline 4: ongoing writing



ERTMS/ETCS system
and its interfaces
SUBSET-026-2

ERTMS: Conformance

- Testing
- Mainly based on simulators
- Functional aspects, interactions with trackside
- Testbenches with
  - simulated components (ex: SS-094)
  - Integrated with real interface (ex: SS-111-2)

CLEARSY Operational Simulator

Connexion with DB Cargo equipements

ERTMS: Application of Formal Methods

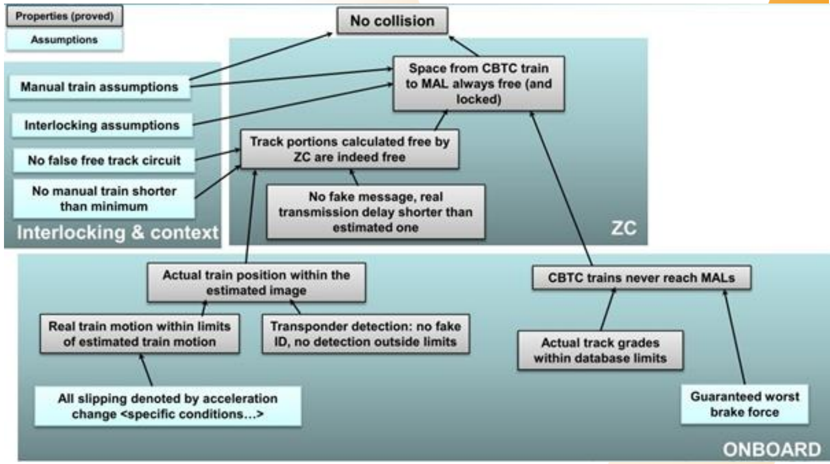
- 2021 ▶ ERJU program
- 2018 ▶ ABZ case-study + Thales/DB POC
  - ▷ Hybrid L3 / management of Virtual Sub-Sections
  - ▷ Formal specification as Model-In-The-Loop
- 2016 ▶ Shift2Rail program (X2Rail-2, ASTRail)
- 2013 ▶ OpenETCS
- 2012 ▶ RobustRails Verification tool set
  - ▷ Safety verification of IXL systems ETCS L2

Formal Proof of System Level SPecification

- Rationale
- Application to ERTMS
  - Proving localization for one configuration
  - Ambiguous localization for one configuration
  - Overview

FPoSLS: Rationale

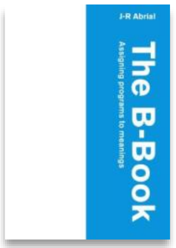
- To obtain a formal proof of the main safety properties
  - No collision, no overspeed
- Safety property obtained from well defined assumptions by **pure logical reasoning** only
- What is modelled is the safety reasoning instead of the whole system
- Output is natural language report (~200 pages) validated by an equivalent proven formal model
- Main lines have more complex scenarios than metros
  - More problems to be discovered



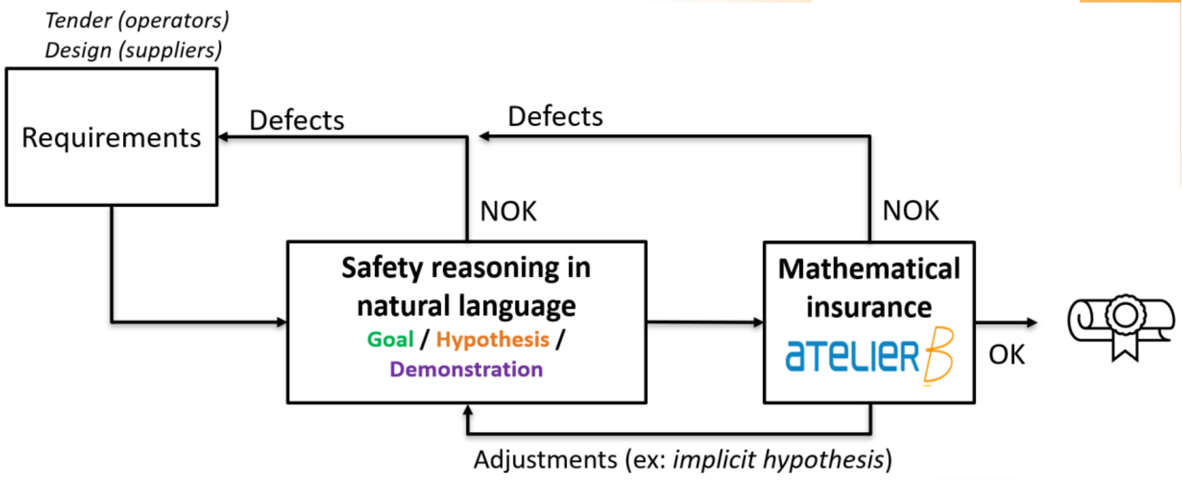
FPoSLS applied for NYCT to Thales CBTC [2007]

FPoSLS: Process

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

FPoSLS: Achievements

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

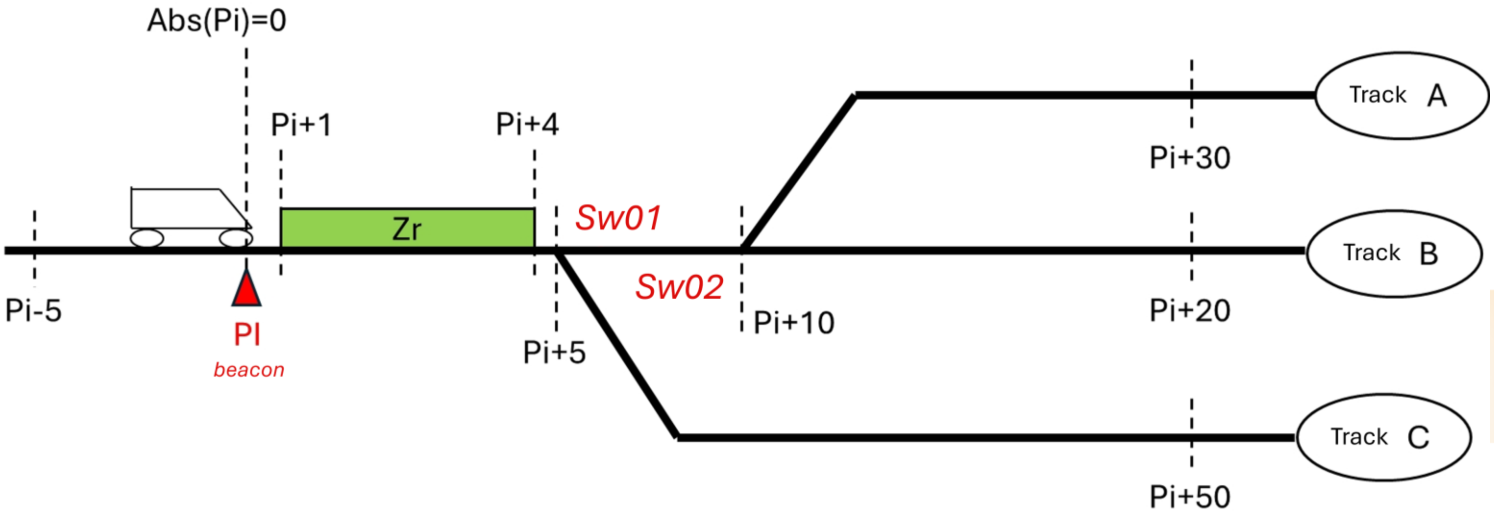
2023-2026

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

Application to ERTMS: train localization

- Locating train ang managing movement authorizations are critical points with strict requirements
- Trains send to RBC
  - Indicator of last beacon read (LRBG)
  - Algebraic distance travelled (#wheel revolutions in one direction - #wheel revolutions in the other direction)
- If no switch, indication is unambiguous
- If switch, indication is ambiguous

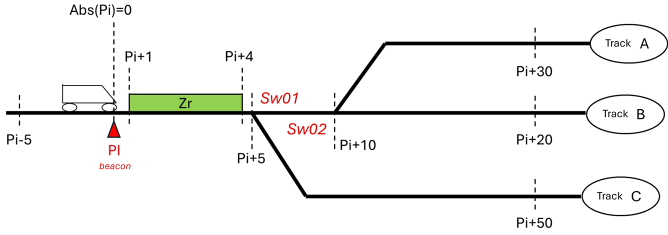
Application to ERTMS: train localization



- Is it possible that the train reports being in Zr while it is not in ? (ETCS has 17 modes, maneuvres allowed)
  - No if only diverging switches (B model to demonstrate it)
  - Yes if converging switches

Application to ERTMS: train localization

- [C1] There is no diverging switch between PI and ZR
- [C2] Whatever the movement of the train on the track plane considered, the ‘return’ path enabling it to return from its current position to the starting position ‘PI’ is a single path.
- [H1] The train will read any PI on its way
  - problematic maneuvers are rare and so are missed PIs, so it is unlikely that a train will make a problematic maneuver and miss a PI in its movement.



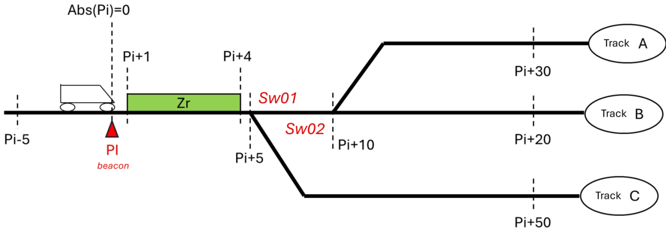
Application to ERTMS: train localization

```
PROPERTIES
    pdv <: track &

    pdv_adj : pdv * dir <-> pdv * dir &
    opp_pdv : pdv * dir --> pdv * dir &

    opp_dir = { UP |-> DN, DN |-> UP } &

    opp_pdv = %(pos, dd).(pos : track & dd : dir | pos |-> opp_dir(dd)) &
```




```
moins_un_odo =
ANY
    pdv2
WHERE
    pdv2 : pdv_adj[{opp_pdv(trainHead)}] &
    odo > 0
THEN
    trainHead := opp_pdv(pdv2) ||
    odo := odo-1
END
```

```
plus_un_odo =
ANY
    pdv2
WHERE
    pdv2 : pdv_adj[{trainHead}] &
    odo < MAX_ODO
THEN
    trainHead := pdv2 ||
    odo := odo+1
END
;
```

```
trainHead : iterate(pdv_adj, odo)[{REF}]
```

Application to ERTMS: train localization

```
trainHead : iterate(pdv_adj, odo)[{REF}]
```

Safety property

reflects the consistency at all times between the odometer value and the actual position of the train on the track surface

```
!(oo).(oo : 0..MAX_ODO &
    iterate(pdv_adj, oo)[{REF}] /\ (ZR * dir) /= {}
    =>
    card(iterate(pdv_adj, oo)[{REF}]) = 1
)
```

Extra invariant 1

The odometer distance between ZR and REF must be such that there is no other track point (not belonging to ZR) with the same odometer distance to REF.

```
!(kk).( kk : 1..MAX_ODO
    =>
    opp_pdv[pdv_adj[opp_pdv[iterate(pdv_adj, kk)[{REF}]]]] = iterate(pdv_adj, kk-1)[{REF}]
) &
```

Extra invariant 2

Starting from 'REF' and applying 'odo' chain links in the direction given by REF, if the resulting track point has a chance of falling in the ZR wake-up zone, then the head of the train definitely belongs to ZR.

```
iterate(pdv_adj, odo)[{REF}] /\ (ZR * dir) /= {}
=>
trainHead : ZR * dir
```

Assertion

Starting from 'REF' and applying 'odo' chain links in the direction given by REF, if the resulting track point has a chance of falling in the ZR wake-up zone, then the head of the train definitely belongs to ZR.

Application to ERTMS: train localization

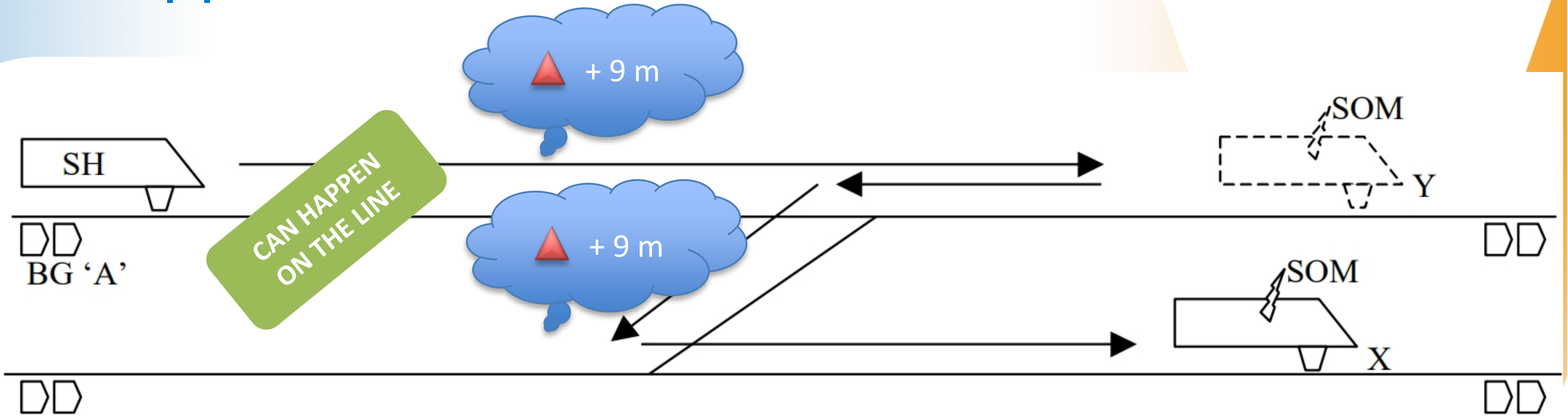
- **Small Model**
  - 94 lines of B
  - 2 variables, 2 operations
  - 22 proof obligations
  - 100% proved
  - 2 user rules (manual demonstration)

HPMV2 (OK|OK|-|-|1058|0|100%)

Vue Classique

Composant	Typage vérifié	OPs générées	Obligations de Preuve	Prouvé	Non-pro
HPMV_Zones	OK	OK	110	110	0
HPMV_Zones_events_IXL	OK	OK	169	169	0
HPMV_Zones_events_RBC	OK	OK	197	197	0
HPMV_Zones_events_Train	OK	OK	214	214	0
HPMV_Zones_exceptionsRBC	OK	OK	346	346	0
Subset113_H0003	OK	OK	22	22	0

Application to ERTMS: train localization



- Scenario with diverging switch, train falls back and stops before beacon, train switched off
- When switched on « later », after the Start of Mission, the RBC could send the train on a wrong track

[**ETCSH0003]SUBSET-113 ETCS Hazard log**.

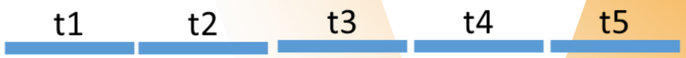
Proposed mitigation are either "trackside engineering shall ensure that a valid position reported by a train can be trusted, i.e. is unambiguous, or RBC shall evaluate position reports in an area with different routes in a way that takes into account the possibility of a position ambiguity. The former might be difficult to implement on some infrastructures. The latter is systematic but likely to lead to a loss of performance".

Formal Data Validation

- Rationale
- Application to ERTMS
- Interaction reasoning / validation

Properties with the B Mathematical Language

- Modelling language based on set theory and first order predicates logic (B mathematical language)



Let the set TrackCircuit = {t1, t2, t3, t4, t5}

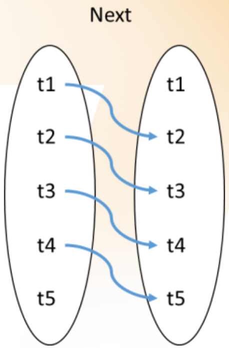
Let the function Next $\in$ TrackCircuit $\nrightarrow$ TrackCircuit

Example: Next(t1) = t2, Next(t2) = t3, Next(t3) = t4, Next(t4) = t5

Next = {t1 $\mapsto$ t2, t2 $\mapsto$ t3, t3 $\mapsto$ t4, t4 $\mapsto$ t5}

Let the function KpAbs : TrackCircuit $\rightarrow$ N

$\forall$x.(x$\in$ TrackCircuit $\wedge$ x $\in$ dom(Next) $\Rightarrow$ KpAbs (Next(x)) > KpAbs(x))

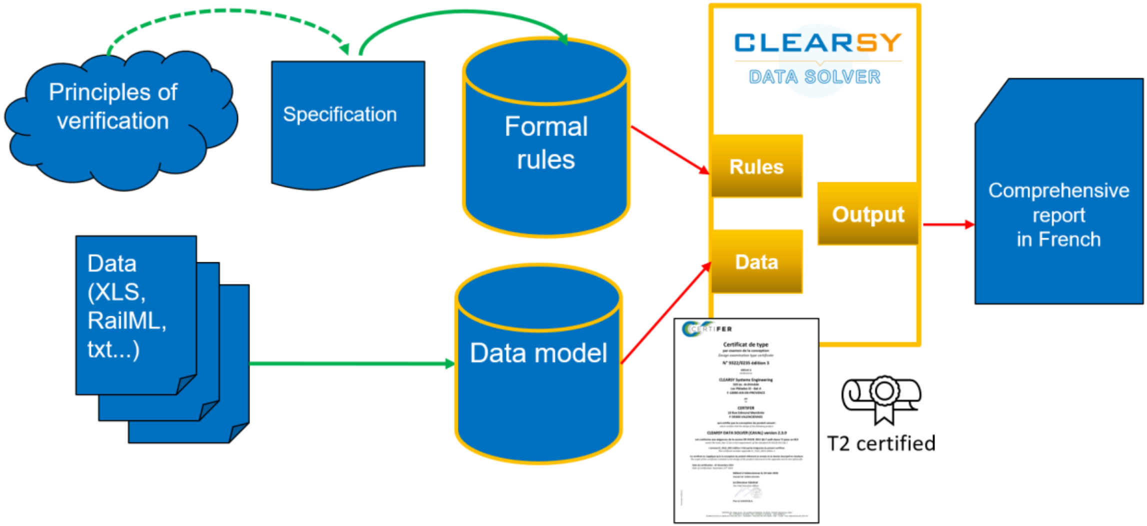


Formal Data Validation

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/

Achievements

2003

First tool to verify embedded topology data
For Certification

2012

First tool integrated into CBTC metro dev process

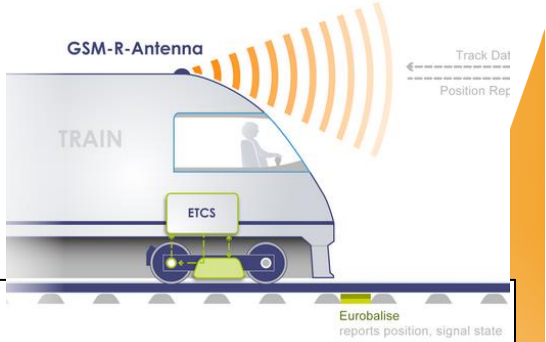
2018

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

Interaction
Reasoning / Validation



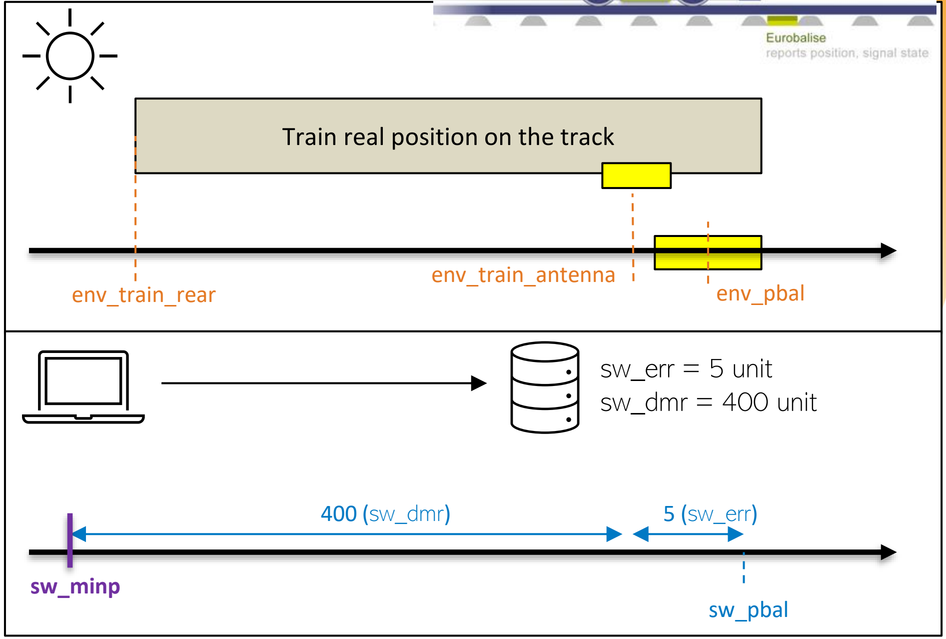
- Formalising the safety property:

  sw_minp ≤ env_train_rear

- Formalisation of hypotheses linking the environment and the software:

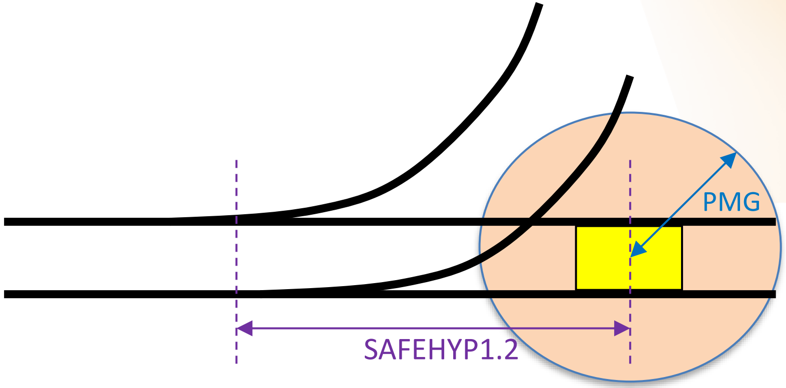
  H1) sw_pbal – sw_err ≤ **env_pbal** ≤ sw_pbal + sw_err
  H2) env_train_antenna – env_train_rear ≤ sw_dmr

- Missing concept: maximal guaranteed range



Link with the Formal Data Validation

- SAFEHYP1_2 : Balises must not be too close to switch toes on its common incident edge
  - **Allocation** : Formal validation of parameters



'Too close' can be calculated: as a function of the Maximum Guaranteed Range (MGR) and the radius of curvature.

Conclusion

- **ERTMS** is a complex specification
  - with many degrees of freedom
  - difficult to assess especially when never implemented
  - trains and trackside with different baselines can be met
- **Formal Methods** could complement conformance testing by
  - verifying safety reasoning in the specification of technical systems implementing
  - checking low-level, technical plans

CLEARSY
Safety Solutions Designer

DISCORAIL
OCT2024

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