Statistical model checking of hazards in an autonomous tramway positioning system

Davide Basile [1] Alessandro Fantechi [1]
Luigi Rucher[2] Gianluca Mandò[2]

[1]University of Florence

[2]Thales S.p.A.

DISCORAIL 2019

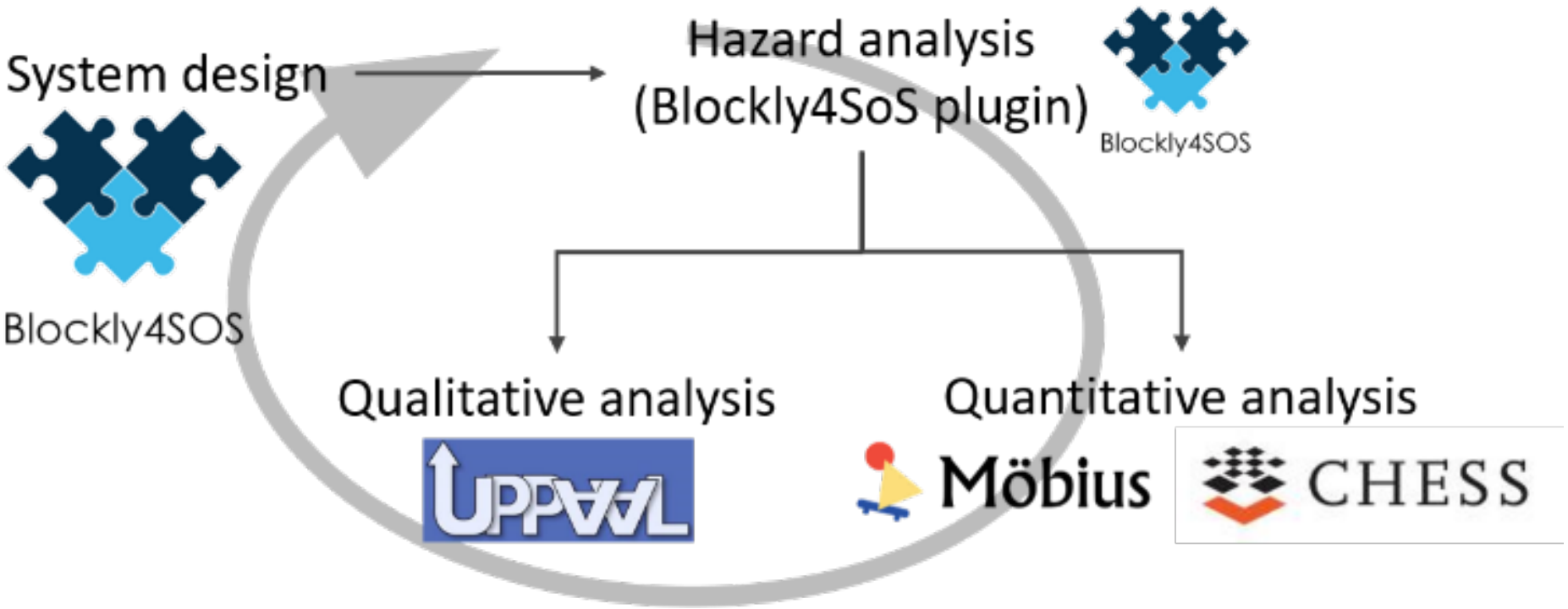
Next Generation of Signaling Systems in Tramway Lines

Goal transition to the next generation ERTMS/ETCS signaling systems, with satellite-based positioning, moving block distancing, and automatic driving (e.g. H2020 Shift2Rail initiative)

SISTER project: autonomous positioning system in light rail transport systems, fixed block with responsibility left to the driver, challenges: urban canyons, multi-path

"*Formal methods are fundamental for safe and reliable technological advances to increase the competitiveness of the European rail industry*"

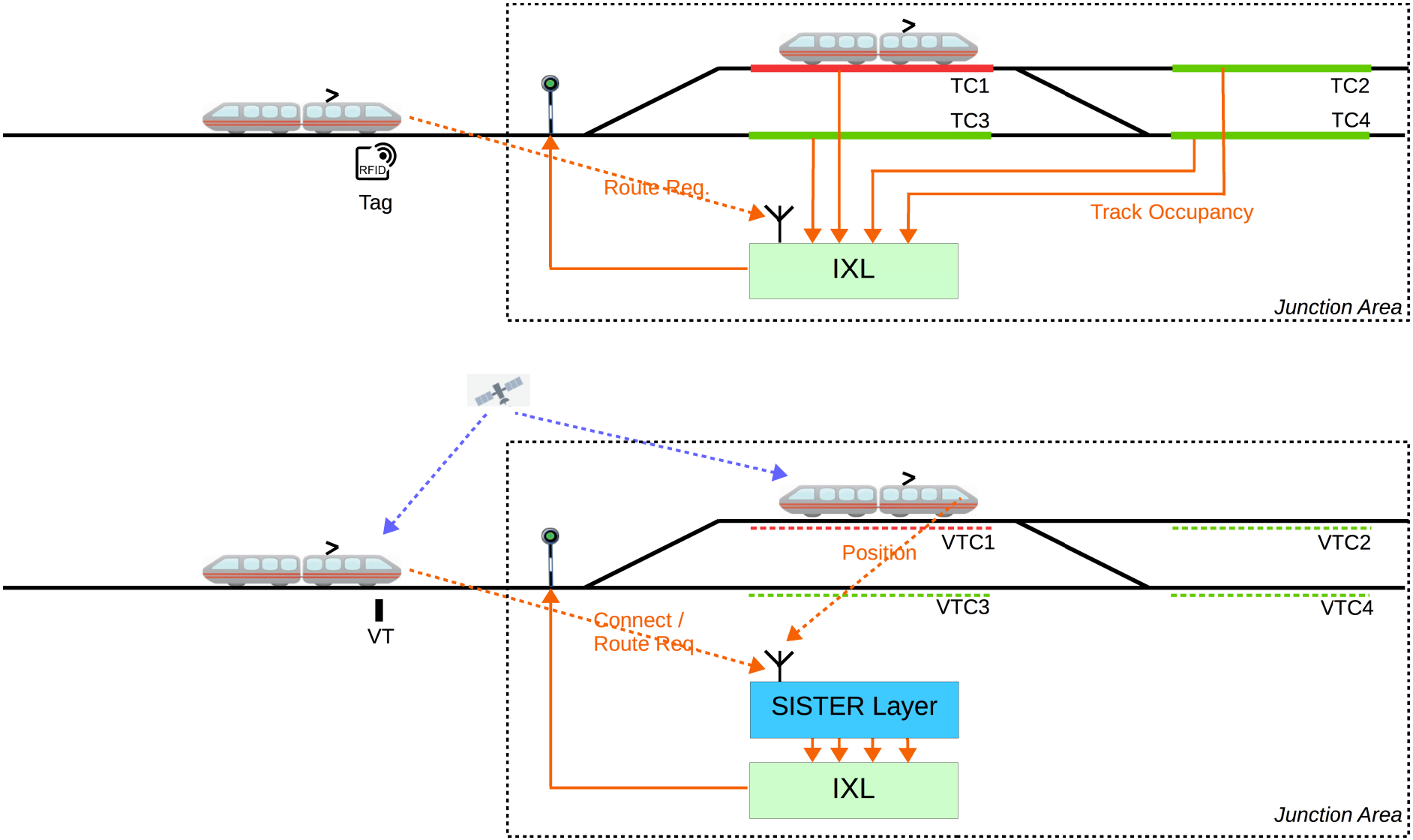
SISTER approach



Operative Scenarios $\rightarrow$ State machine model

Requirements $\rightarrow$ Hazards $\rightarrow$ Formalised properties

Old vs New Positioning System



Backward compatible solution

Sensor Fusion Algorithm

- **Sensor Fusion Algorithm** data coming from :
  - GPS/GNSS satellites,
  - Inertial Measurement Units,
  - Odometers,
  - etc...
- The SFA computes a virtual position by fusing data coming from different sensors,
- modeled as a black box

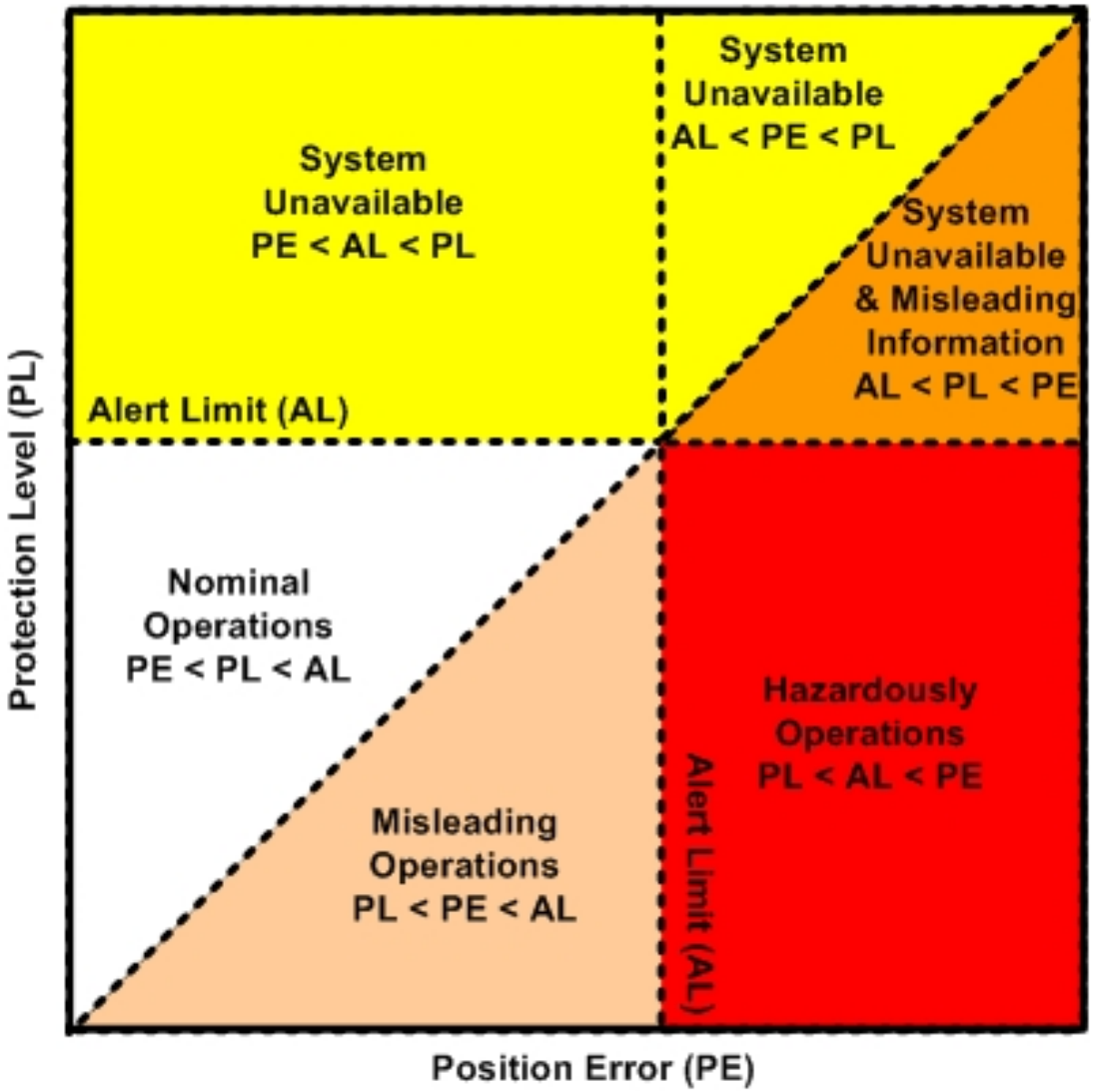
Aeronautical Principles of Satellite Navigation

- Virtual position L_v comes with an *uncertainty*:
  - *Integrity* a real time decision criterion for using or not using the system
  - *position uncertainty* (φ) : from empirical evaluations we know that the error follows a Gaussian distribution centered in L_v
  - *alert limit (AL)* : the maximum allowable position error beyond which the system should be declared unavailable
  - *time-to-alert (TTA)* : the maximum allowable time elapsed from the onset of the navigation system being out of tolerance until the equipment enunciates the alert.

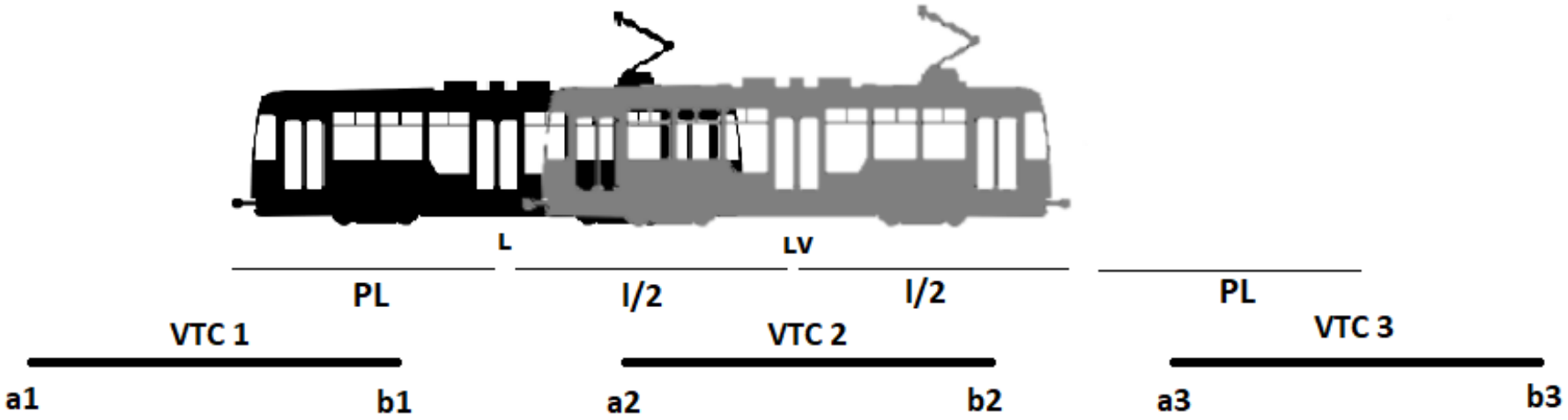
Protection Level

- *Protection level (PL)* : a statistical bound of the position error computed so as to guarantee that the probability of the absolute position error exceeding said number is smaller than or equal to the target integrity risk.
- The interval $[L_v - PL, L_v + PL]$ contains the position with probability $>= 1 - IR$
- The PL is modeled as a black box: probabilistic choice
  - weights of probabilistic choice are inflated to analyse dangerous scenarios

Stanford diagram



Location Referencing



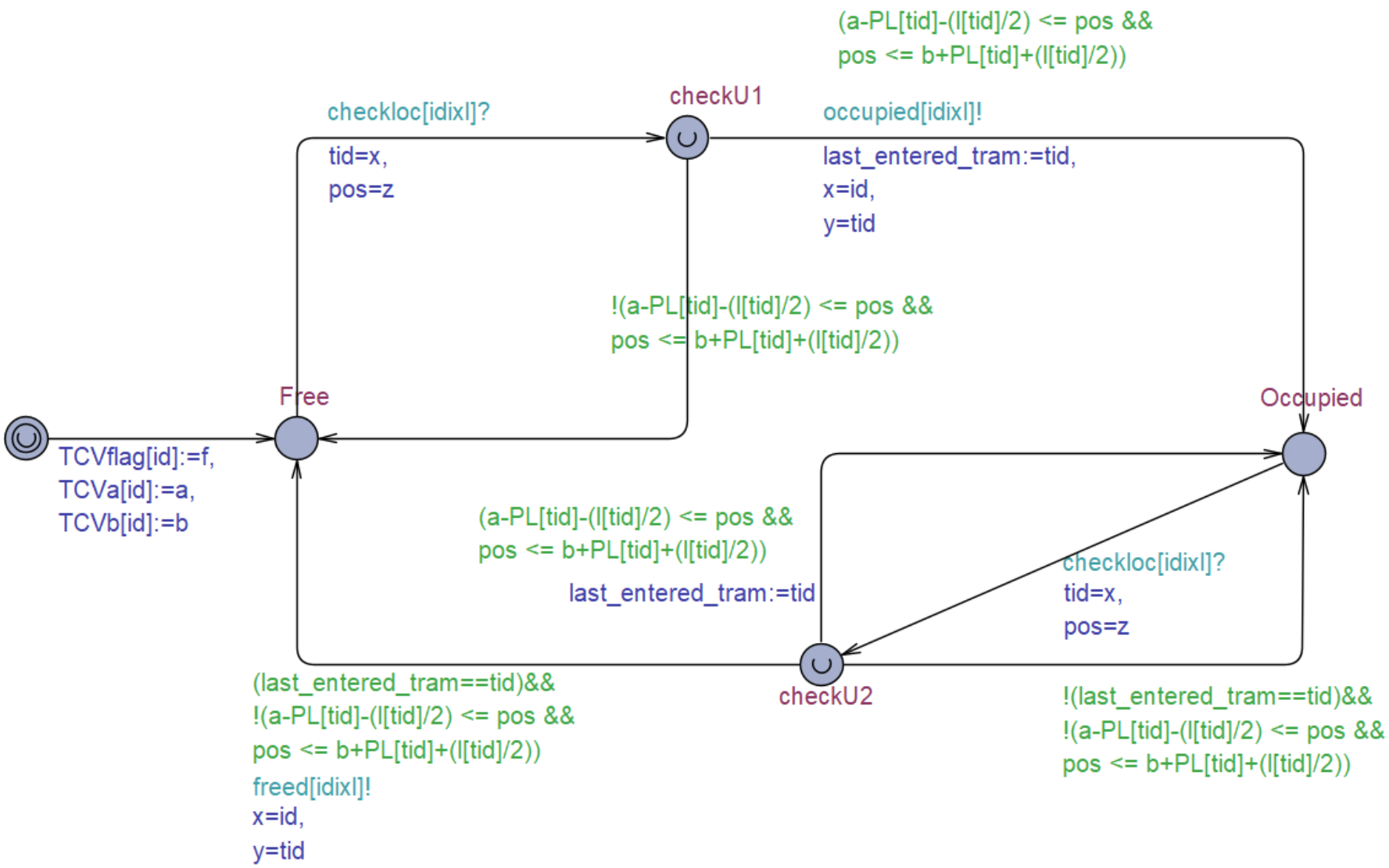
$$LocationReferencingVTC(L_v, PL, a, b) = (a - PL - \frac{l}{2} \leq L_v) \wedge (L_v \leq b + PL + \frac{l}{2})$$

unidimensional space

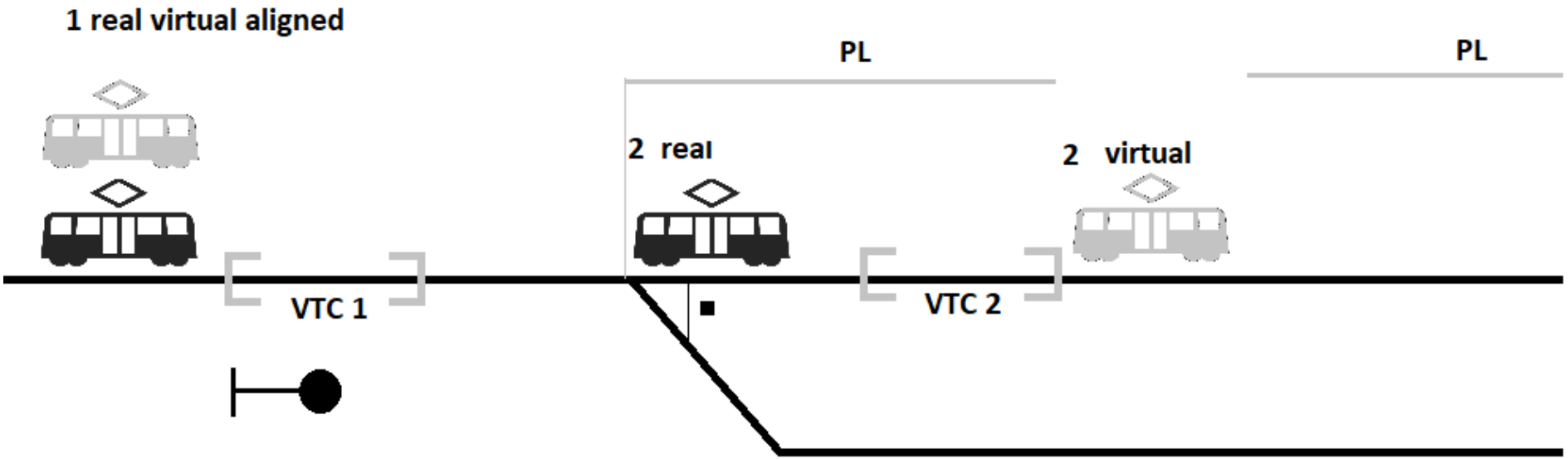
Formal model

- formalised using Stochastic Finite State Automata and **Uppaal SMC**
- *Statistical Model Checking* running simulations to estimate values of properties, easy to implement, avoid full state exploration
- Properties expressed as : `P(<>[t,t'] ap)`
- Formal model : compositions of different components for the On-board Unit and the Interlocking Sister Layer
  - template mechanism, highly configurable
- Inflate probabilities of hazards occurrence : high position uncertainty

Virtual Track Circuits Template Model

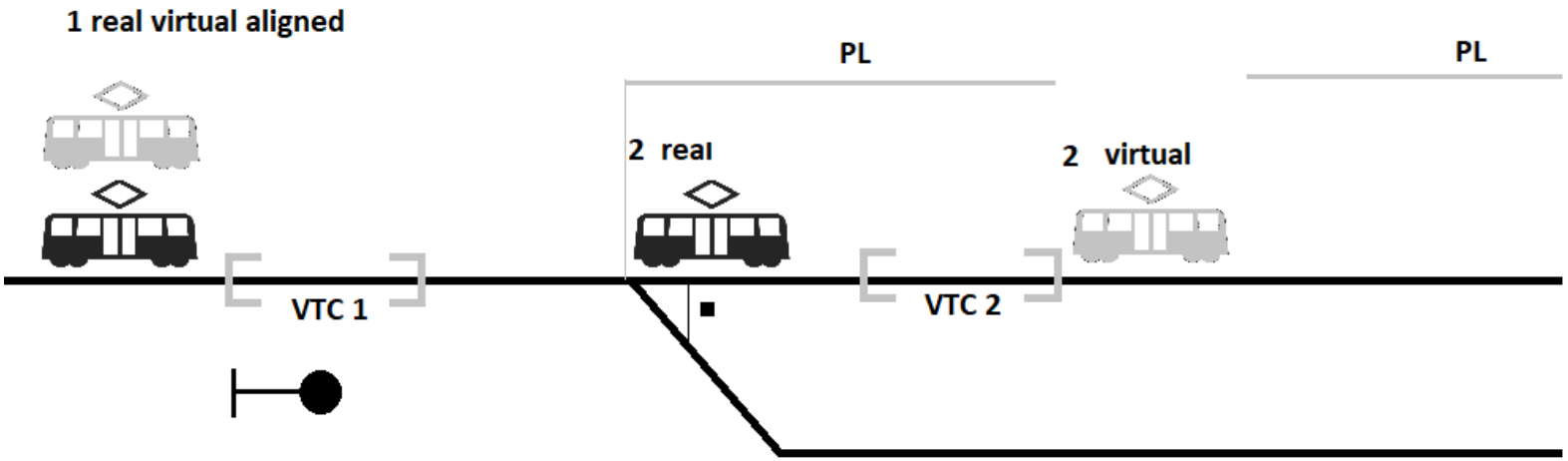


Analysis of a Scenario



Nominal operations : $\varphi < PL < AL$

Experiment 1

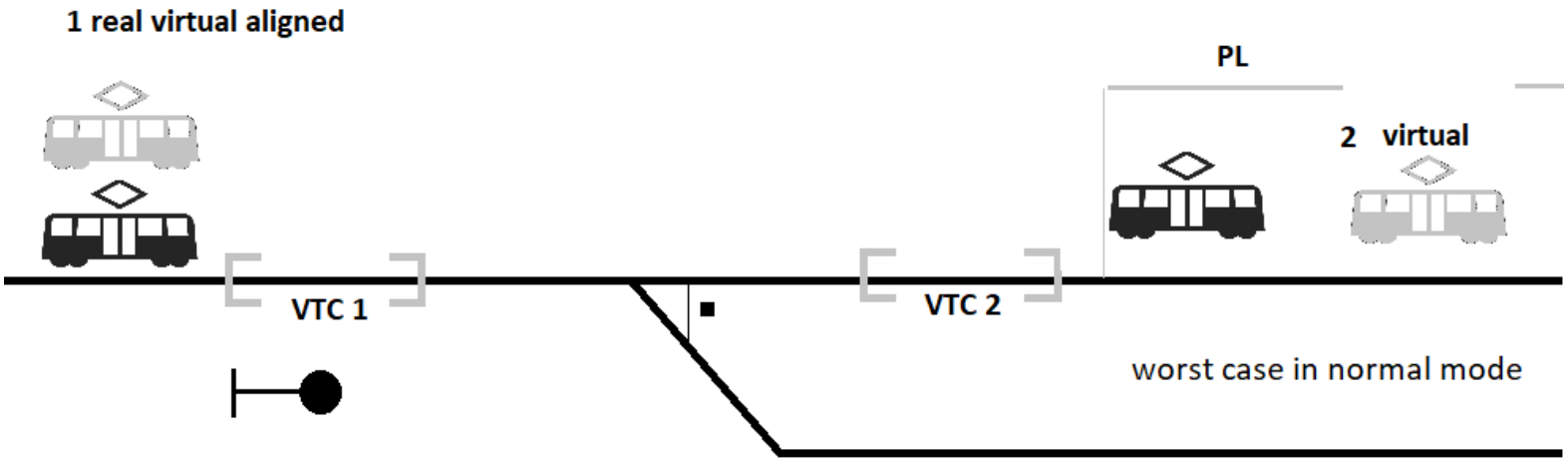


$$\texttt{Pr}(<>\,[0,150](\texttt{L}+1/2<\texttt{VTCa})\&\&(\texttt{Lv}-1/2>\texttt{VTCb}))$$

Protection level: ignored - Release Condition: free - Result ≈ 1

first hazard: ignoring positioning error

Experiment 2

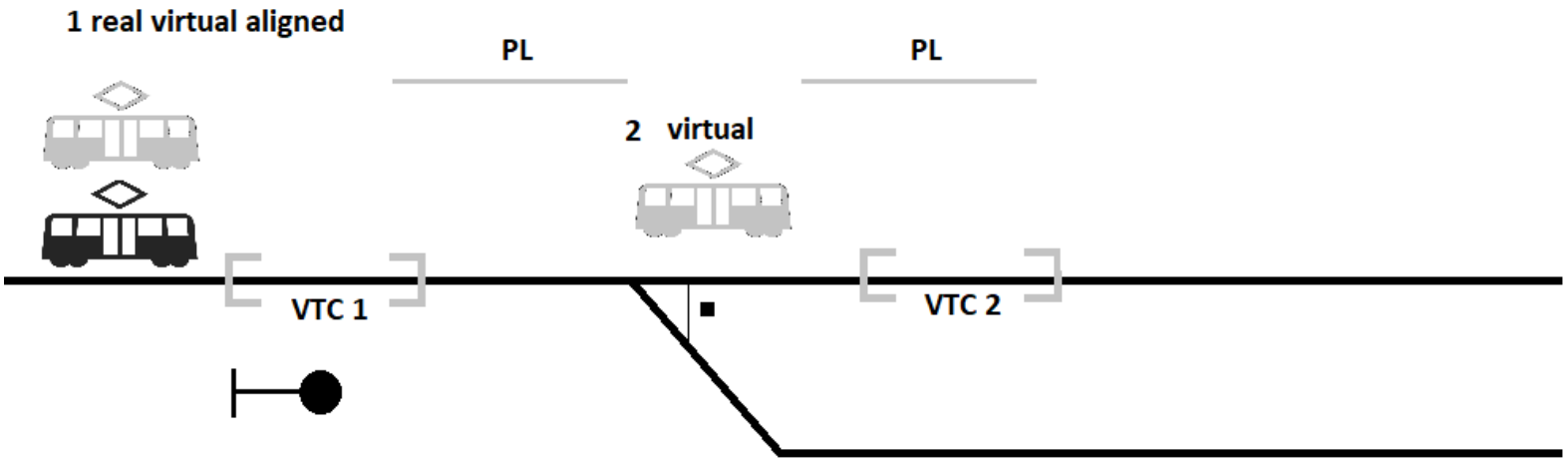


$$\texttt{Pr}(<>\,[0,150](\texttt{IXLD\_0.Disconnecting}\&\&(\texttt{Lv}+1/2<\texttt{VTCa})))$$

Protection level wide - Release Condition: free - Result ≈ 0

first mitigation: use Location Referencing

Experiment 3

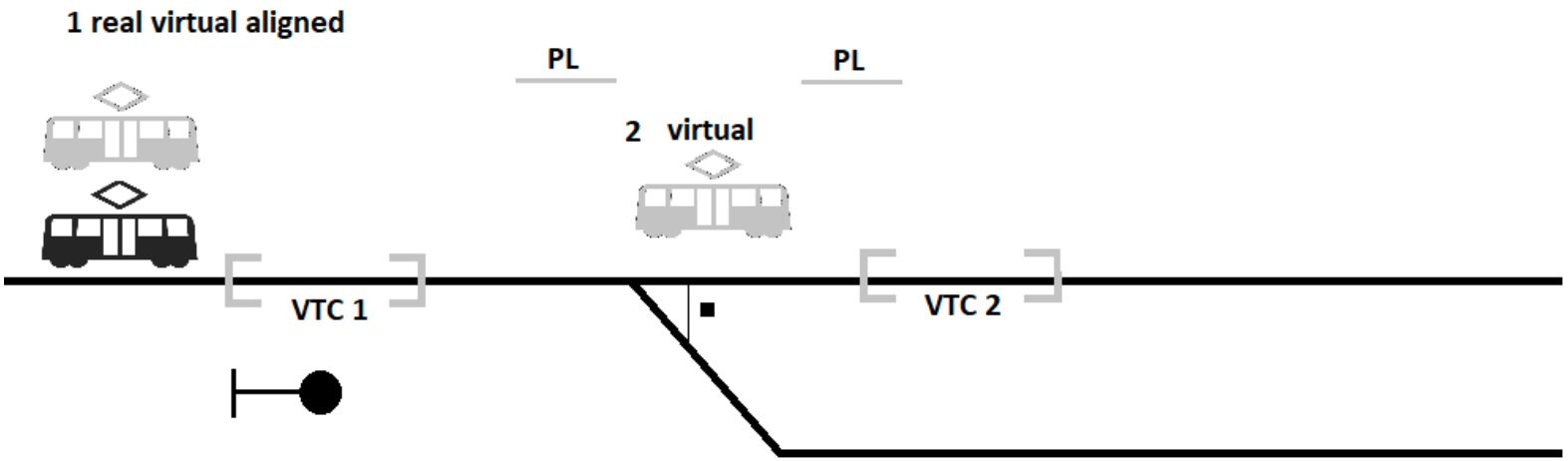


$$\texttt{Pr}(<>\,[0,150](\texttt{IXLD\_0.Disconnecting\&\&}(\texttt{Lv}+1/2<\texttt{VTCa})))$$

Protection level wide - Release Condition: occupied - Result ≈ 1

second hazard: release occupied condition

Experiment 4



$$\texttt{Pr}(<>\,[0,150](\texttt{IXLD\_0.Disconnecting\&\&}(\texttt{Lv}+\texttt{l}/2<\texttt{VTCa})))$$

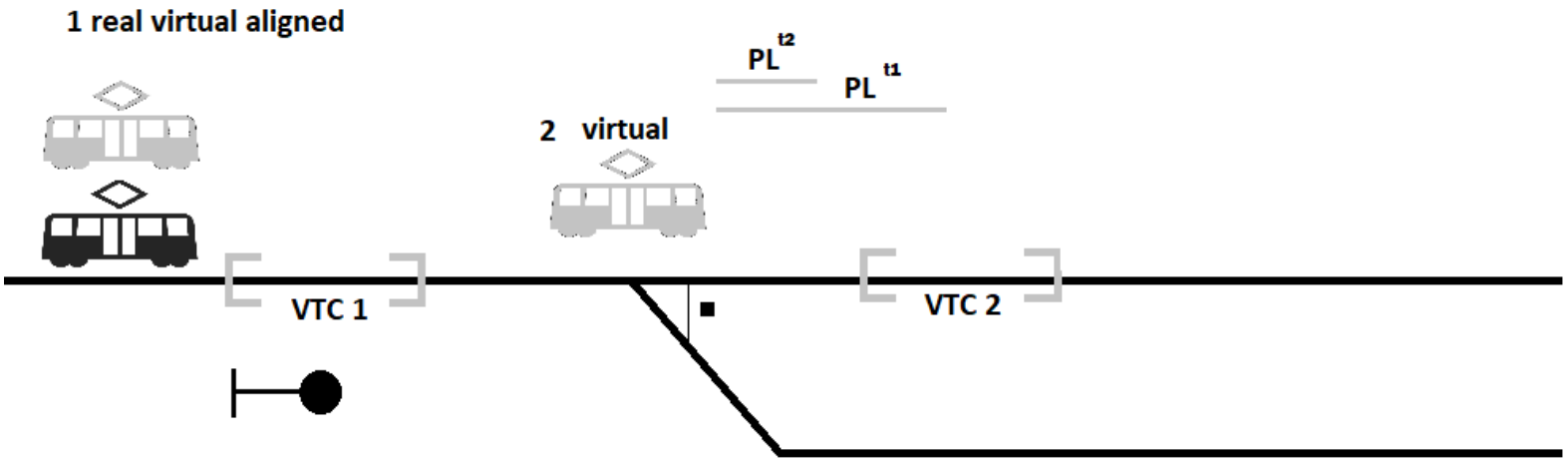
Protection level tight - Release Condition: occupied - Result ≈ 0.16

second hazard also with tight PL

second mitigation: only use release free condition, change IXL configuration

already evaluated in Exp.1

Experiment 5

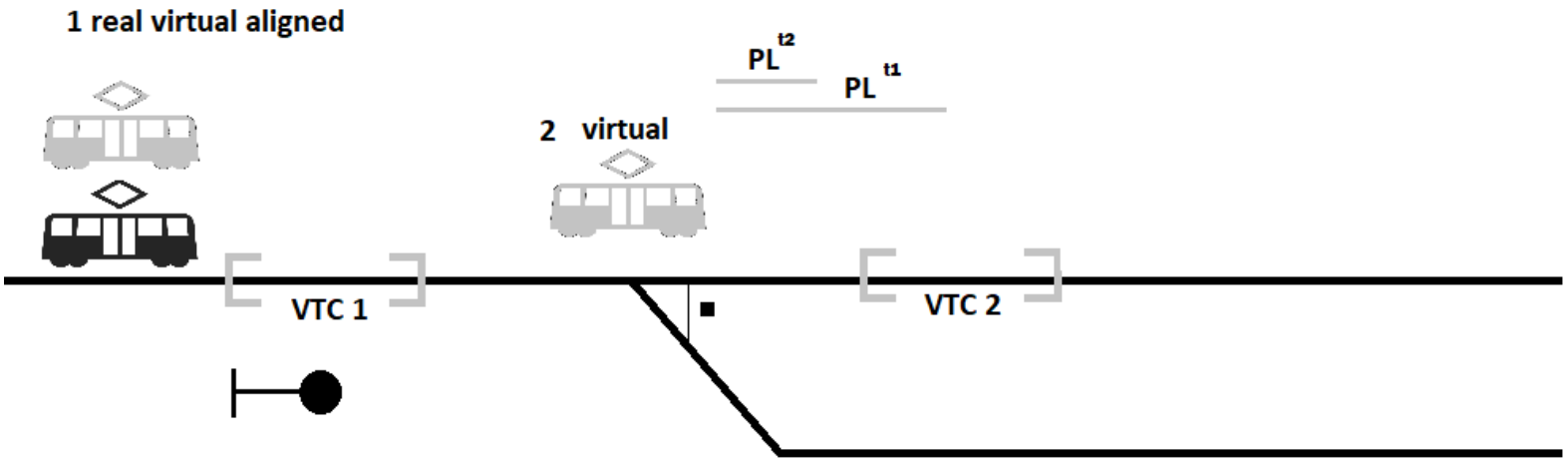


$$\texttt{Pr}(<>\,[0,150](\texttt{IXLD\_0.Disconnecting}\&\&(\texttt{Lv}+\texttt{l}/2<\texttt{VTCa})))$$

Protection level tight/wide - Release Condition: free - Result ≈ 0.03

third hazard : high PL variability

Experiment 6



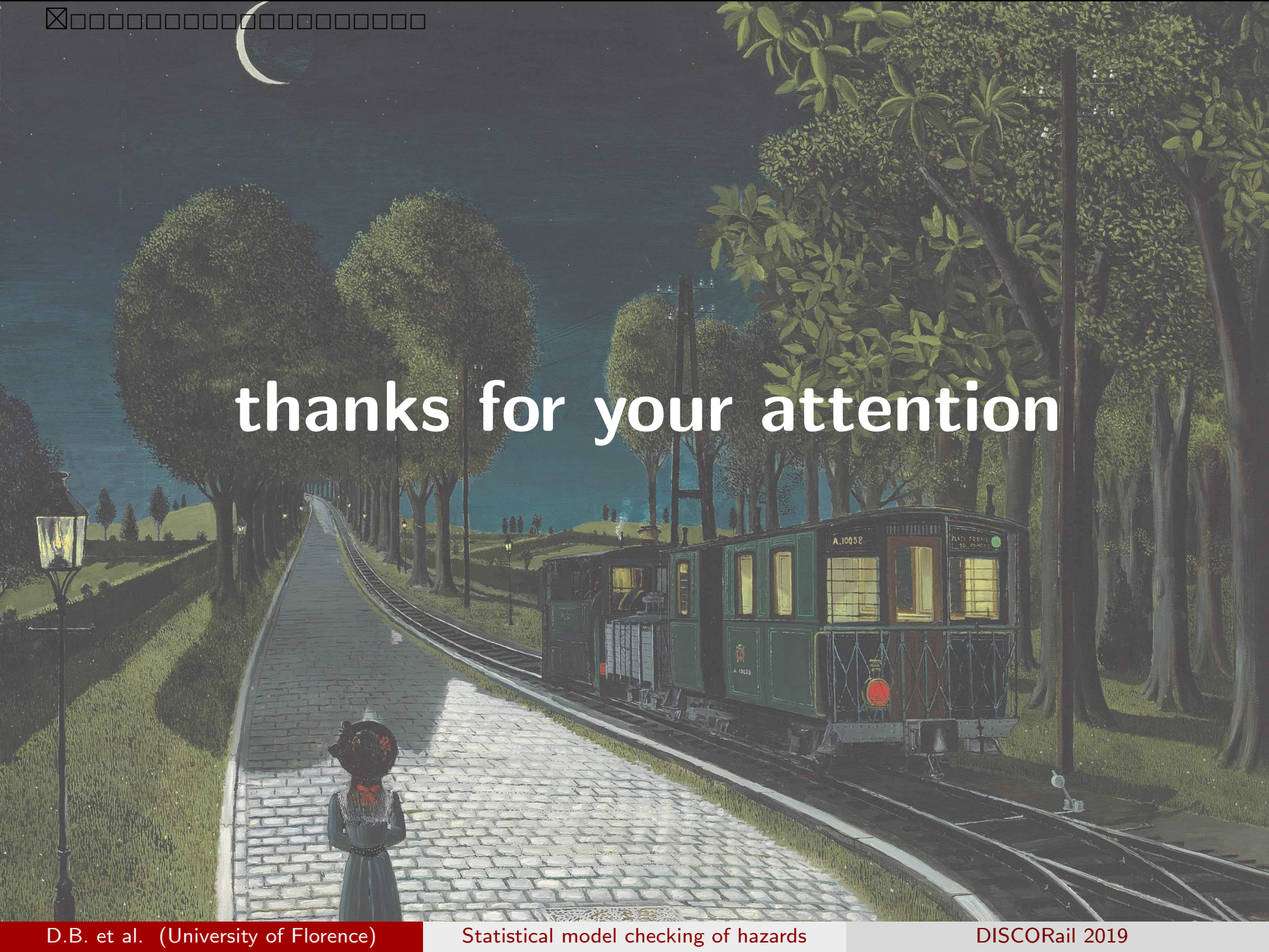
$$\texttt{Pr}(<>\,[0,150](\texttt{IXLD\_0.Disconnecting}\&\&(\texttt{Lv}+\texttt{l}/2<\texttt{VTCa})))$$

Protection level = AL - Release Condition: free - Result ≈ 0

third mitigation : use AL instead of PL

Conclusion

- formal methods have been proven useful in detecting and mitigate hazards in the informal system specification
- Uppaal SMC has been proven to be effective by industrial partners
- Future work: modeling other entities (Operational Control Centre), modeling communication faults, compute PL accurately


thanks for your attention