Statistical Model Checking of a Moving Block Railway Signalling Scenario with UPPAAL SMC

Experience and Outlook

Maurice H. ter Beek
ISTI–CNR, Pisa, Italy

joint work with

Davide Basile
UNIFI

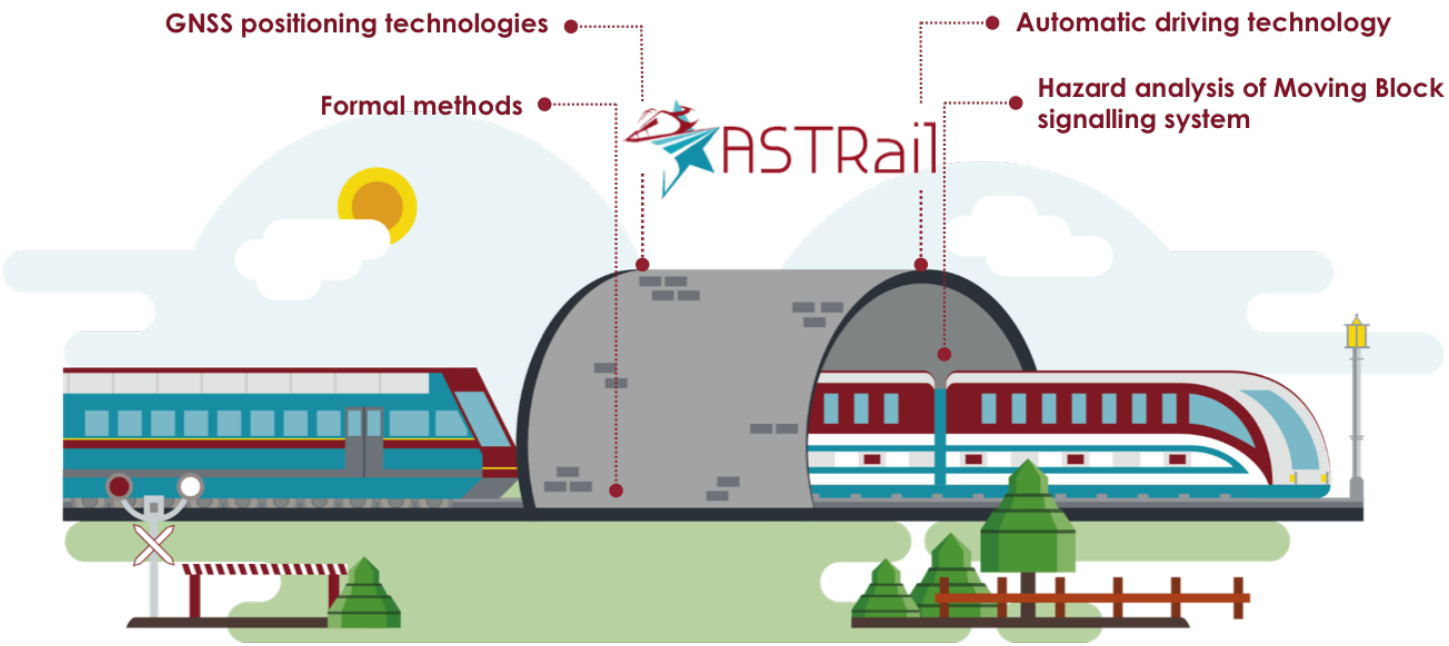
Vincenzo Ciancia
ISTI–CNR

ISoLA 2018

Limassol, Cyprus
6 November 2018

Outline

1. Industrial context: next generation railway signalling
2. Case study: moving block railway signalling scenario from Ardanuy Sirti
3. Experience: statistical model checking with UPPAAL SMC
4. Outlook: spatio-temporal analysis with UPPAAL SMC
5. Conclusion

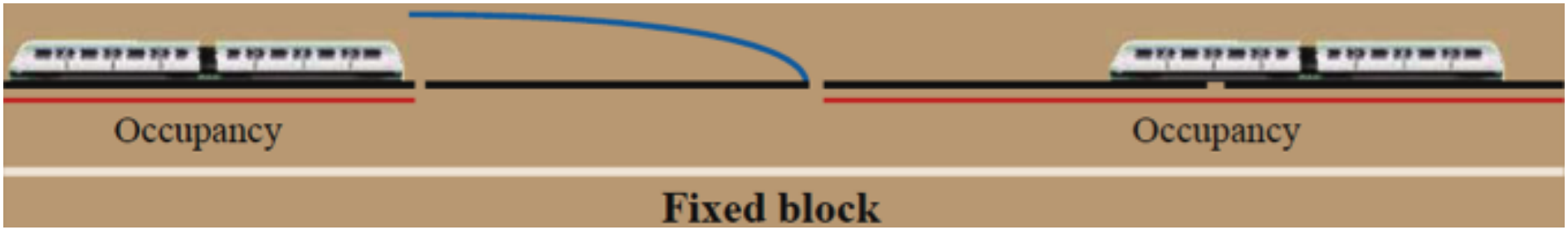


http://www.astrail.eu/

Industrial context: next generation railway signalling

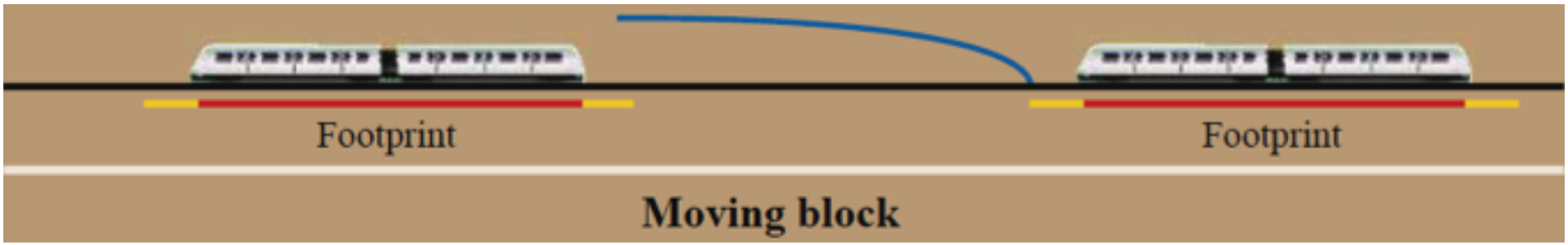
Current ERTMS / ETCS signalling systems max. level 2:

- fixed blocks (based on line's speed limit, train's speed/braking, etc., thus faster trains imply longer blocks imply lower track occupancy)
- trackside equipment for train positioning (with costly maintenance)

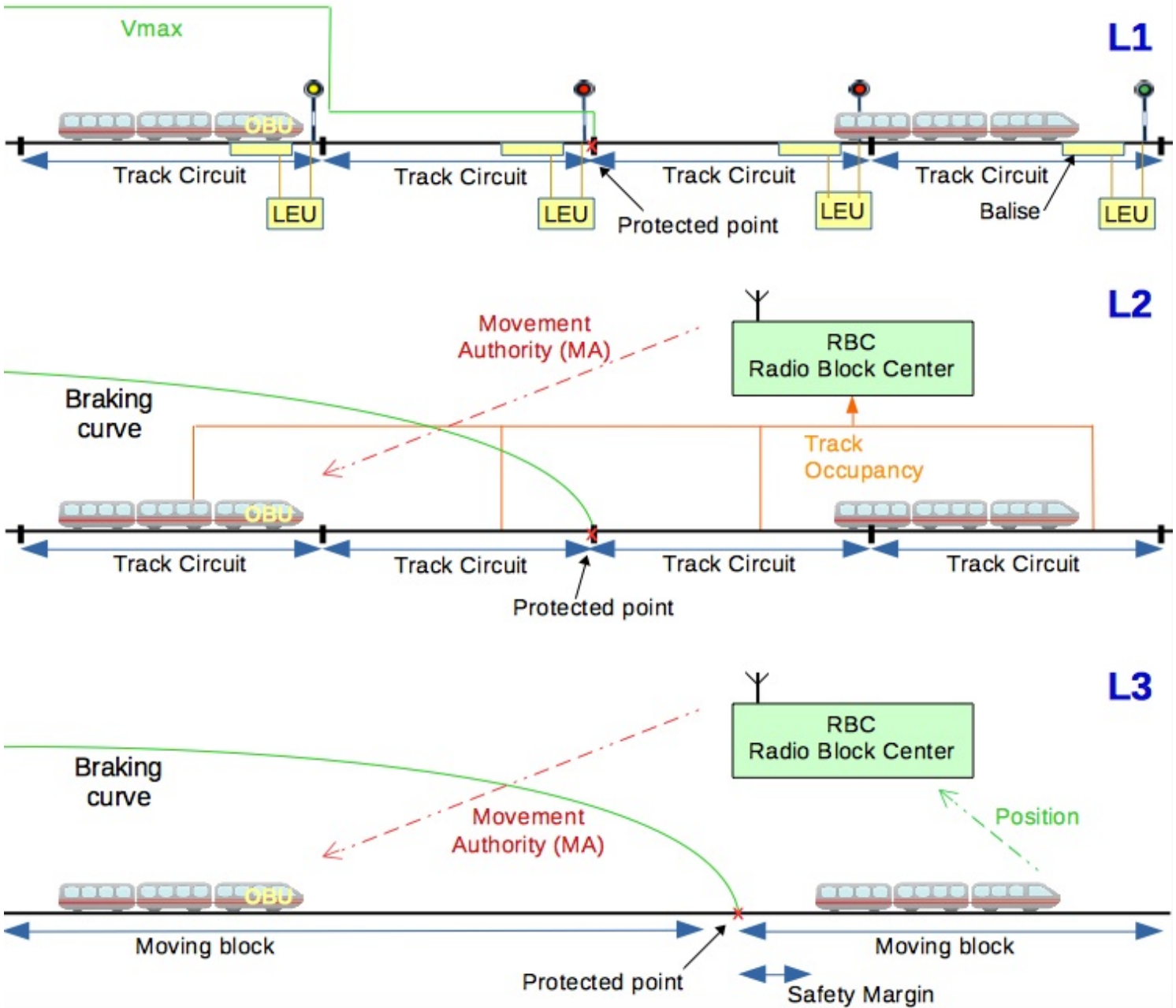


Next generation railway signalling systems from level 3:

- moving blocks (safe zone based on rear position of train ahead, thus reducing trains' headways, in principle to braking distance)
- onboard odometry for train positioning (no trackside equipment)



ERTMS/ETCS levels L1, L2, and L3



H2020 Shift2Rail initiative: €920 million (2014–2020)

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

Goal: analyse the suitability of formal methods in the transition to the next generation ERTMS/ETCS signalling systems, with satellite-based positioning, moving block distancing, and automatic driving

Challenge: effective and precise moving block signalling systems by means of GNSS-based satellite positioning, leveraging on an integrated solution for signal outages (e.g. tunnels) and the multipath problem

ASTRail (S**A**tellite-based **S**ignalling and Automation Sys**T**ems on **Rail**ways along with Formal Method and Moving Block Validation):

Requirements analysis plus safety, hazard and performance analyses of moving block signalling scenarios with formal methods and tools

---

Istituto Superiore Mario Boella sulle Tecnologie dell'Informazione e delle Telecomunicazioni (ISMB, Italy, coordinator), SIRTI S.p.A. (Italy), Ardanuy Ingeniería S.A. (Spain), École Nationale de l'Aviation Civile (ENAC, France), ISTI–CNR (Italy), Union des Industries Ferroviaires Européennes (UNIFE, Belgium)

Involvement Formal Methods & Tools lab at ISTI–CNR

WP4: Formal Methods for the railway field: identify most mature ones

- systematic literature review on applications of formal methods in railways (submitted)
- trial applications of formal methods and tools to ERTMS L3 moving block system
- survey with practitioners to investigate uptake of formal methods in railway industry

  Basile et al., On the Industrial Uptake of Formal Methods in the Railway Domain: A Survey with Stakeholders @ iFM'18

WP2: Safety analysis of moving block signalling system

Input: Real-Time UML (RT UML) model from industrial partners

Ardanuy

Sirti
building the future

Output: UPPAAL SMC model

- capable of natively accommodating both real-time and probabilistic aspects
- like UML state machine diagrams, easing understanding by industrial partners

Simplified: parameters like probability of failures of devices (e.g. GNSS receivers) to be instantiated with data provided by vendors

Main components L3 moving block signalling system

OBU train's onboard unit measures the train's current speed and verifies the train's integrity

LU train's localisation unit uses a GNSS-based positioning system to determine the train's location

RBC wayside radio block centre communicates continuously with OBU and LU

- receives data regarding the train's position and the train's integrity from the train
- sends speed restrictions, route configurations, and MAs (movement authorities) to the train
- computes MAs by communicating with neighbouring RBCs and with a Route Management System (RMS) for positions of switches and other trains (head and tail position)

Model abstraction: RMS, communication among neighbouring RBCs

- consider train to communicate with one RBC, based on a seamless hand-over when the train moves from one RBC supervision area to the adjacent

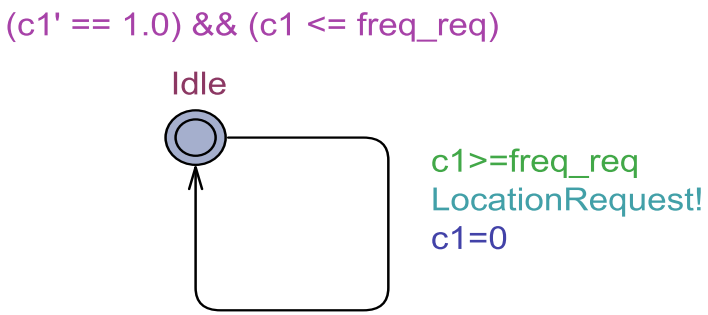
UNISIG: Functional Interface Specification for the RBC/RBC handover, 2014

Model transformation: RT UML → UPPAAL

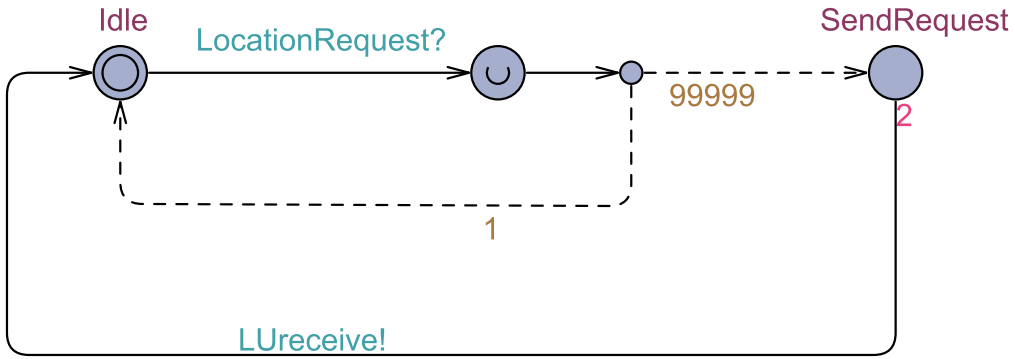
From RT UML state machine diagrams to stochastic timed automata

- each parallel region of the RT UML model translated into a separate automaton
- (pseudo) states and (probabilistic) transitions are in one-to-one correspondence
- failure probabilities currently set to placeholder value 10^{-5}, awaiting refinement
- guards and triggers modelled as input and output broadcast channels, implying
  - synchronous communication, discarding messages if receiver not ready to receive
  - fresh MA sent by RBC to OBU will supersede older MA if latter was not yet received
- straightforward, except a few time-related modelling choices, cleared with partners
  - timed events `RTat` of stereotype «`RTevent`», used to trigger transitions based on event's timing information, are modelled as invariant conditions and clock guards, forcing transitions to be executed when the precise moment in time is reached
  - probabilistic delayed events `RTduration` of stereotype «`RTdelay`», used to add durations to actions/transitions, are modelled as probabilistic delays: when an action/transition is enabled, the time at which it is fired is probabilistically distributed
- failure probabilities and rates of probabilistic distributions will be further refined based on input from our project partners

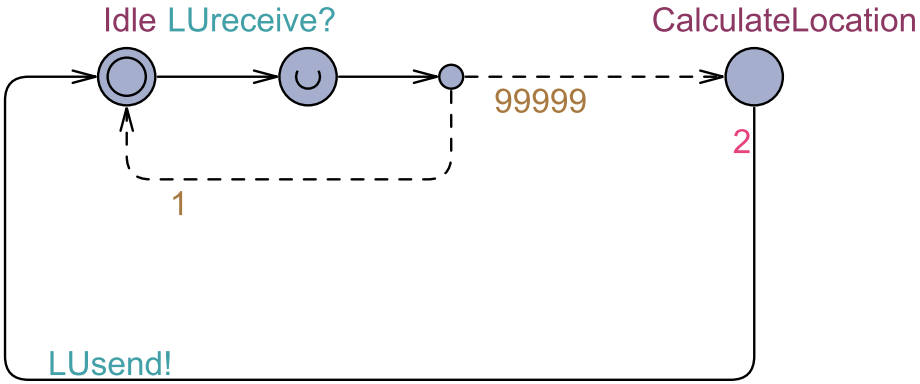
UPPAAL model of moving block signalling scenario (1/2)



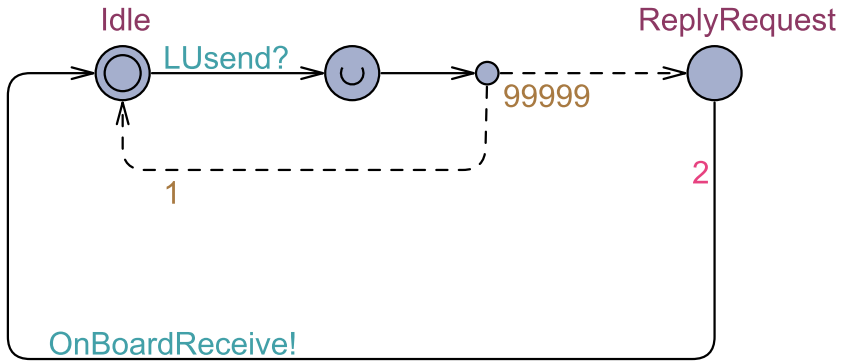
Generate location request



Send location request



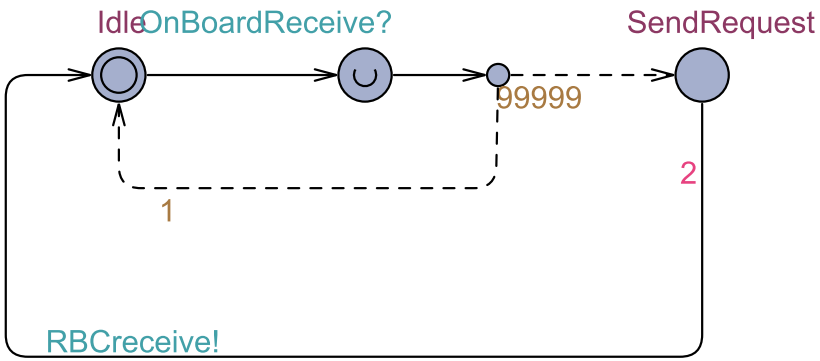
Calculate location



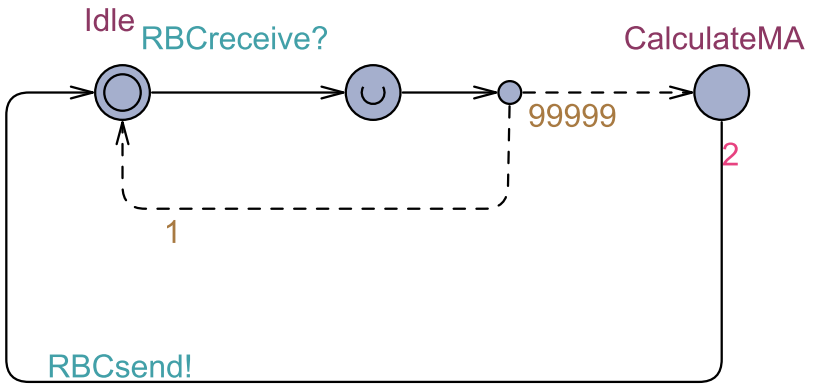
Send location

Industrial partners: `freq_req` = 5 sec., initial value clock `c1` is `freq_req`

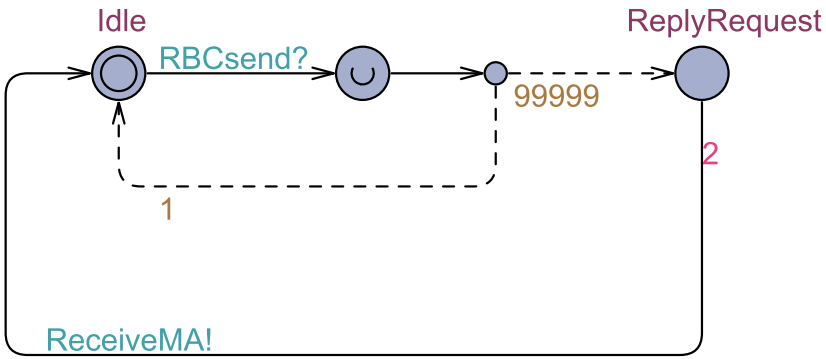
UPPAAL model of moving block signalling scenario (2/2)



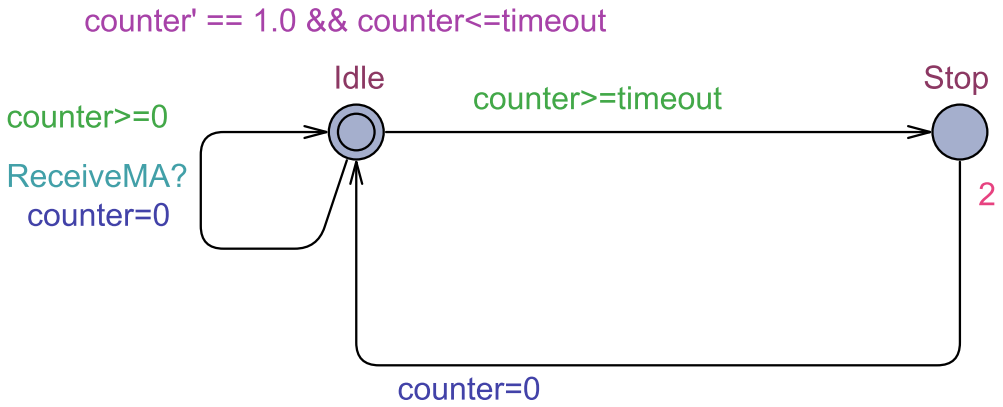
Send MA request



Calculate MA



Send MA



Control MA freshness

Industrial partners: `timeout` = 3×`freq_req`, initial value clock `counter` is 5

Preliminary hazard analysis by industrial partners

Goal: evaluate safety level of a moving block signalling system

Procedure: identify and analyse hazards (e.g. GNSS-related errors, communication failures, faulty states)

- risk assessment: probability of occurrence of a hazard and severity of its consequences
- risk qualifying according to CENELEC EN 50126 standard (RAMS: Reliability, Availability, Maintainability and Safety)

Outcome: hazard log

Examples from the hazard log

Requirements:

"Communication between RBC and OBU must be safe and continuously supervised, if the connection is lost an alarm must be triggered."

"OBU device must be SIL 4 device. Once OBU receives the alarm [...] it must immediately send an alarm to RBC."

Mitigation: "In case of communication loss enter in safe state mode."

Safety Related Application Conditions:

"If train position cannot be received within the maximum time limit, the OBU shall generate an alarm and must transit to degraded mode."

"If Train Integrity cannot be confirmed within the maximum time limit, the train shall be stopped."

Analyses with UPPAAL SMC

1 It must always be the case that eventually either a MA is received or the train enters a safe state `Stop`:

$$A \Diamond (\texttt{ReplyMA.ReplyRequest} \parallel \texttt{Controlling.Stop})$$

UPPAAL SMC reports that this CTL property holds

2 Probability that the train enters a safe state `Stop` upon a `timeout`:

$$\mathbb{P}_M(\Diamond_{\leq(\texttt{timeout})}\, \texttt{Controlling.Stop})$$

UPPAAL SMC reports that this probability is in the interval [0,9.99994e-005], with confidence 0.995 and obtained from 59912 runs in ± 5 min.

UPPAAL SMC v4.1.19 (rev. 5649) with statistical parameters: lower and upper probabilistic deviation $(-\delta, +\delta)$: 0.001; probability of false negative and false positive (α, β): 0.005; probability uncertainty (ϵ): 5.0^{-5}.

UPPAAL SMC: evaluating the freshness of the MA

Requirements: OBU attempts for three times to compute the train's location and receive the MA

Model: first attempt at time 0, after which OBU attempts again each 5 sec. until timeout at time 15

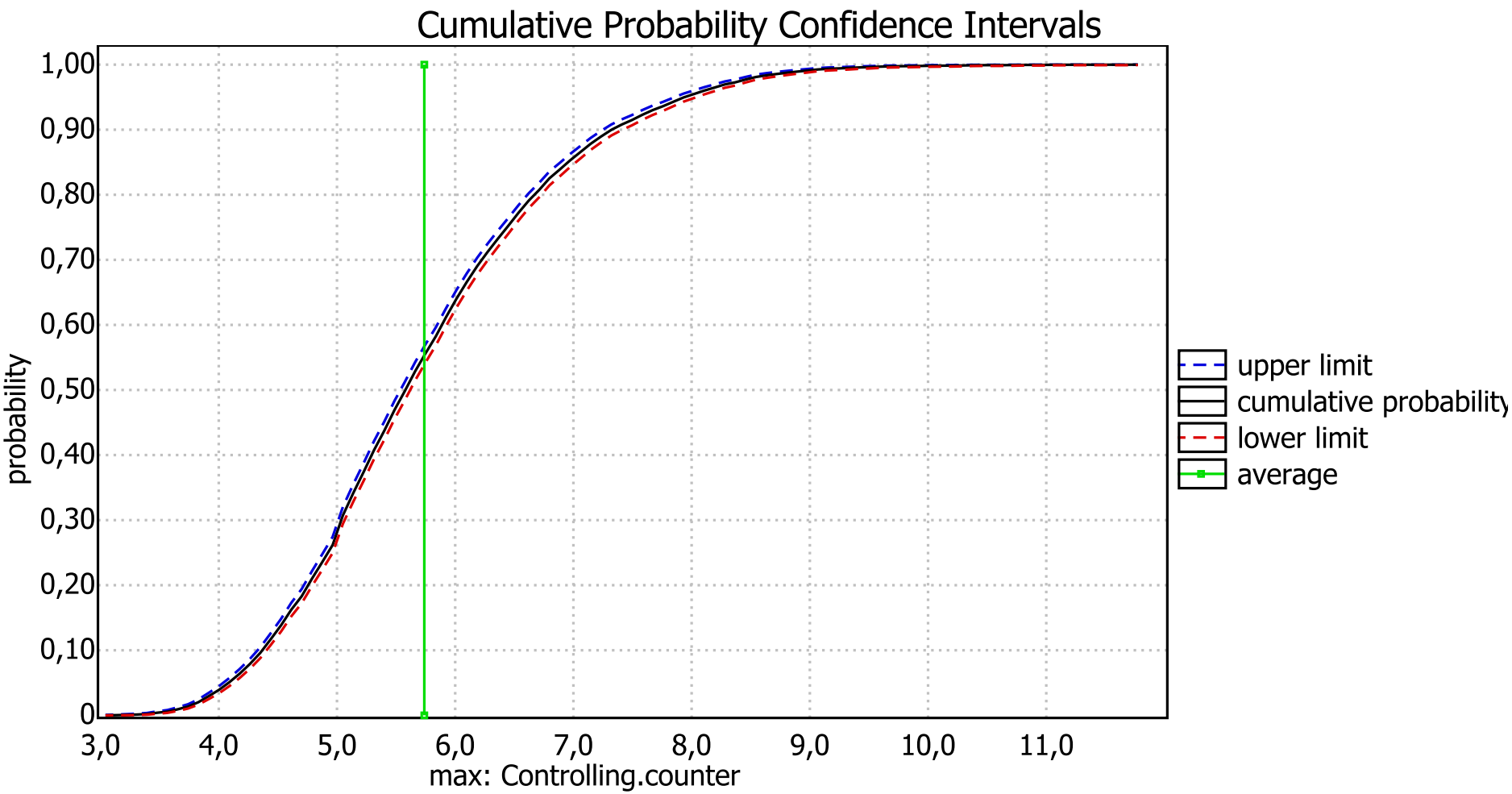
Goal: which of the three attempts has higher probability of success?

$$E[\leq \texttt{timeout}; 10000](\mathit{max} : \texttt{Controlling.counter})$$

This evaluation computes in the interval of time of `timeout` (i.e. 15 sec.) the average of the maximum value of clock `counter`, using 10,000 runs ; Since `counter` is reset each time a new MA is received, its average value is the average time in which a new MA is received

Result: MA messages have a higher probability of being received between the first and the second attempt

UPPAAL SMC: evaluating the freshness of the MA



Parameters: α=0.005, ε=0.005, bucket width=0.08733, bucket count=100
Runs: 10000 in total, 10000 (100%) displayed, 0 (0%) remaining
Span of displayed sample: [3.04171764778005, 11.7747301491212]
Mean of displayed sample: 5.73865788065071 ± 0.0327581295234518 (99.5% CI)

Future work: adding a spatial dimension?

Use spatial information like train location (their coordinates in a map)

- "**where** does property ϕ hold?", in which property ϕ could be, e.g., "the train is allowed in the current location"
- "does ϕ hold **near to** where ψ holds?" or "are the locations where ϕ holds **surrounded by** locations where ψ holds?"

Now assume

ϕ expresses the presence of a single train in a specific area

ψ expresses the absence of trains in a specific area

Then such formulae could be used to check whether it is true that

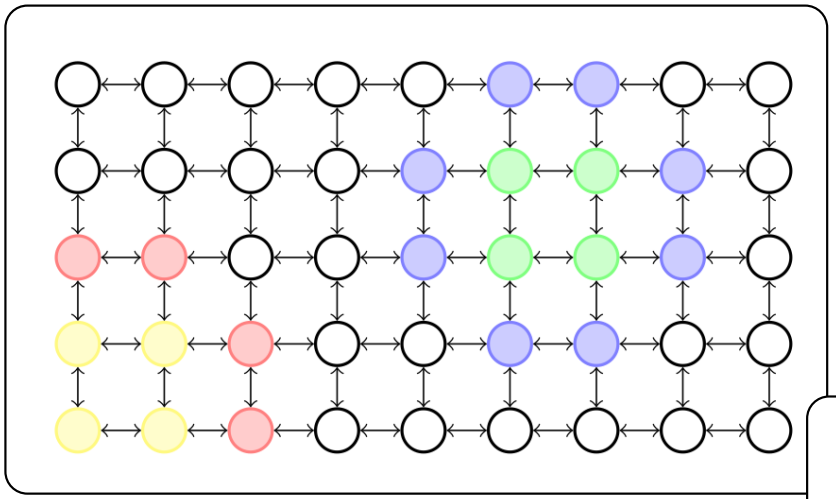
$\forall$ train (travelling at a specific speed)

$\nexists$ other train around it (given a specific diameter of distance)

$\Rightarrow$ guarantee a safety distance between trains during operation (i.e. moving block!) and compute MA messages

Spatial logic (topological spaces)

Graphs, reachability properties (discretisation of physical space)



$$
\begin{array}{lcll}
\Phi & ::= & p & [\textsc{Atomic proposition}] \\
 & | & \top & [\textsc{True}] \\
 & | & \neg\Phi & [\textsc{Not}] \\
 & | & \Phi \wedge \Phi & [\textsc{And}] \\
 & | & \mathcal{N}\Phi & [\textsc{Near}] \\
 & | & \Phi\,\mathcal{S}\,\Phi & [\textsc{Surrounded}]
\end{array}
$$

All red and yellow points satisfy: $\mathcal{N}\,yellow$
One yellow point satisfies: $\mathcal{I}\,yellow$
No points satisfy: $\mathcal{I}\,green$
Green points satisfy: $green\,\mathcal{S}\,blue$

Derived operators, like interior: $\mathcal{I}\Phi = \neg\mathcal{N}\neg\Phi$

Rail networks are (Euclidean) graphs!

Aiello, Pratt-Hartmann, van Benthem (eds.), Handbook of Spatial Logics
Ciancia et al., Spatial Logic of Closure Spaces @ *LMCS*'16

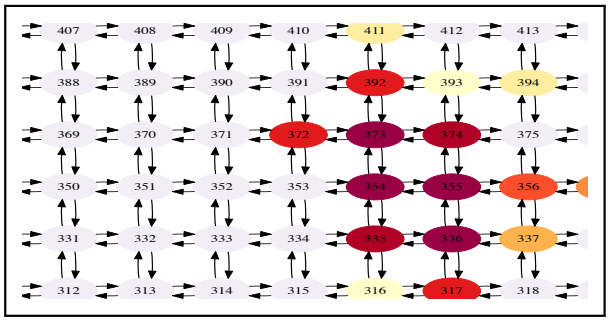
Topochecker

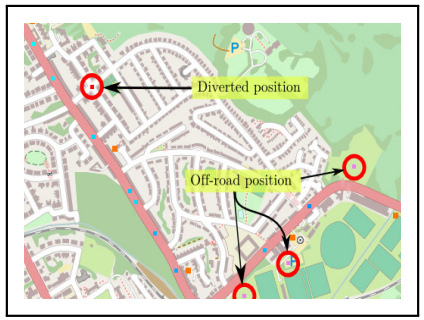
In-memory explicit-state **spatio-temporal** model checker

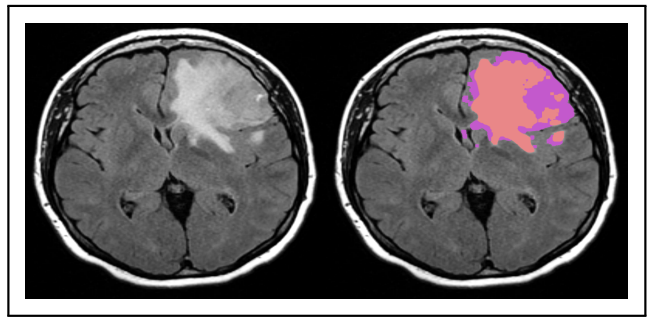
Spatial logic + branching-time temporal extension (CTL)

Efficient: millions of states / points analysed per second

Models: graphs, pictures or multi-dimensional (medical) images







topochecker already applied to smart buses

Ciancia et al., Spatio-temporal model checking of vehicular movement in public transport systems @ *STTT*'18

`https://github.com/vincenzoml/topochecker`, `http://topochecker.isti.cnr.it`

Topochecker: features and applicability

Efficient linear algorithms

- topological operators (e.g. near, surrounded, reachable)
- collective operators (e.g. group, connected, regions)
- metric-based formulae (Maurer's *distance transforms*)
- imaging operators (statistical texture analysis / similarity search)

Statistical spatio-temporal model checking

- "tool-chained" execution mode using MultiVeStA

  Sebastio & Vandin, MultiVeStA: Statistical Model Checking for Discrete Event Simulators @ VALUETOOLS'13

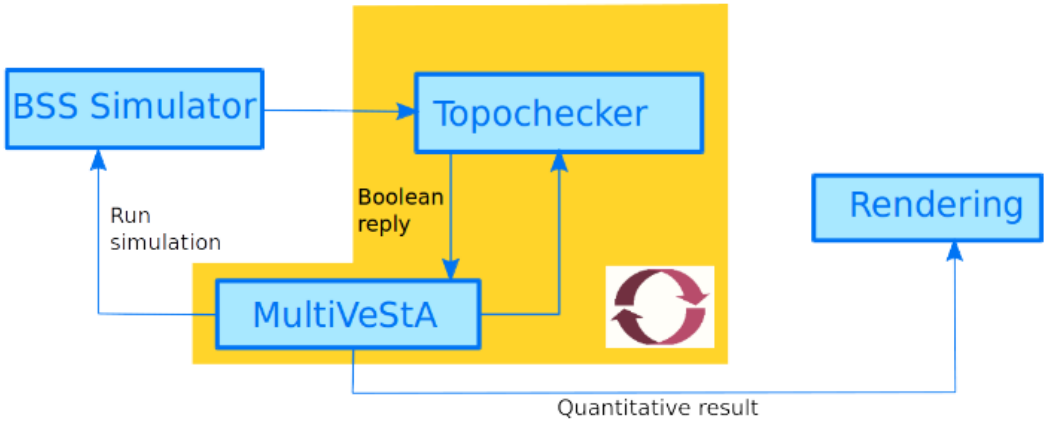
- applied to spot congestion in bike sharing systems

  Ciancia et al., A Tool-Chain for Statistical Spatio-Temporal Model Checking of Bike Sharing Systems @ ISoLA'16

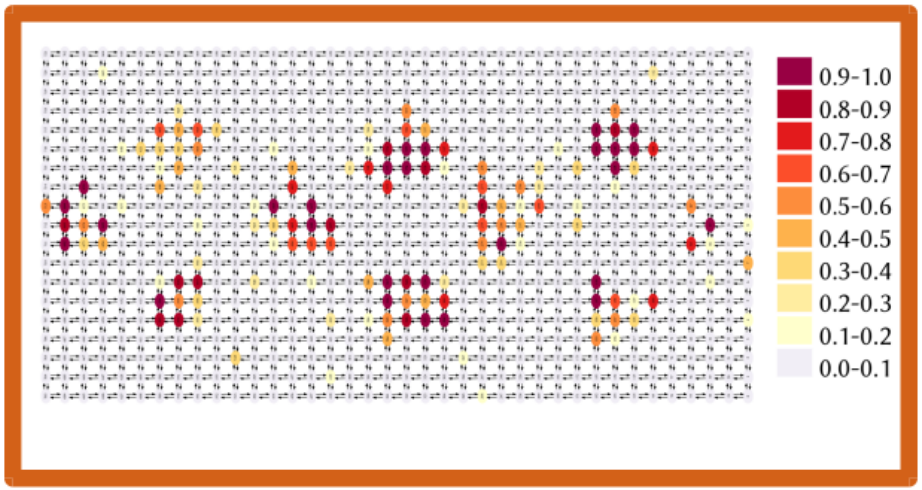
! spatio-temporal requirements are subtle:
"*eventually close to a congestion*" vs. "*close to an eventual congestion*"

`https://github.com/vincenzoml/topochecker`, `http://topochecker.isti.cnr.it`

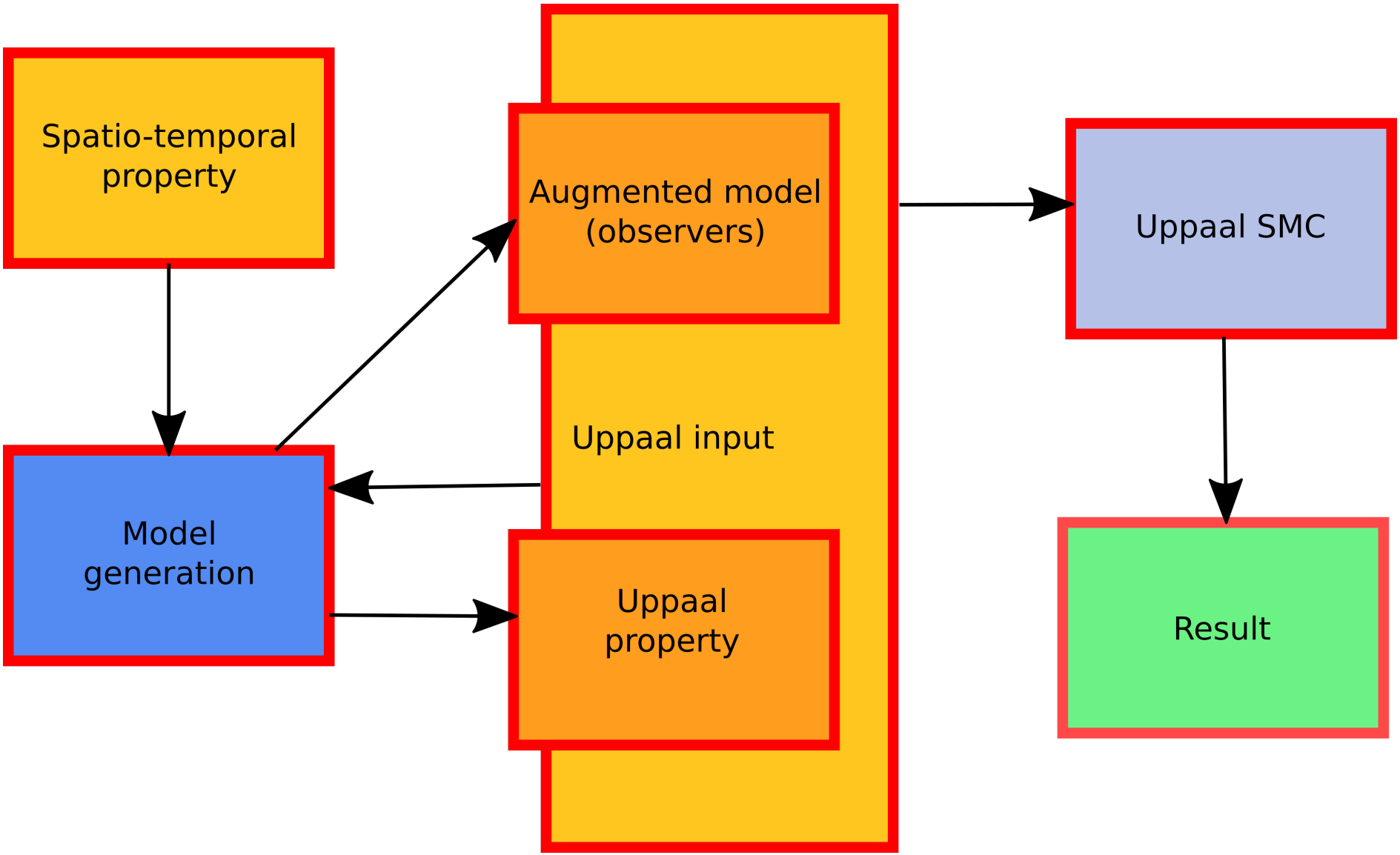
Statistical spatio-temporal model checking @ ISoLA'16



$$\text{full} = [\text{vacantPlaces} == 0]$$
$$\text{cluster} = \mathrm{I}\ \text{full}$$
$$\text{eventuallyCluster} = \mathrm{EF}\ \text{cluster}$$



Spatio-temporal analysis with UPPAAL SMC?



Encoding in UPPAAL SMC? (1/2)

Encode the spatial model as a 'grid of variables' and the spatial model checker as a Boolean function

> encode spatial logic primitives as UPPAAL functions and the spatial structure as a discrete graph, using variables of the model checker and a function to identify the neighbourhood relation between points (i.e. use spatial properties in UPPAAL formulae, as if they were atomic properties of temporal states)


simplicity of approach


very complex to achieve (reimplementation of a spatial model-checking algorithm in UPPAAL)


only simple properties (no nesting of temporal formulae inside spatial connectives)

? efficiency and computational feasibility for large spatial structures

Encoding in UPPAAL SMC? (2/2)

Spatial model checking using continuous variables (and difference equations) to encode the movement of entities

- encode space as an UPPAAL process, acting as primary observer, so that spatial properties (e.g. reachability in space) can be checked by UPPAAL;
- use continuous clock variables to represent movement in space, with each clock corresponding to a spatial dimension, and connect ODEs to spatio-temporal features of UPPAAL processes (i.e. position, speed, acceleration)

 apparently more promising

 also requires quite some work (design a suitable spatial language, define appropriate observers that allow to represent nested spatio-temporal formulae which need to be encoded in UPPAAL's logic)

 still limited properties (purely spatial properties nested inside temporal properties, but not the opposite)

? efficiency (e.g. can it handle grids of a million nodes?)

Outlook

Future work: apply UPPAAL SMC to a more elaborated version of the ASTRail case study and to a case study from Tuscany region's project **SISTER** (**SI**gnaling & **S**ensing **TE**chnologies in **R**ailway applications): Apply innovative signalling solutions to Light Rail Transit infrastructures

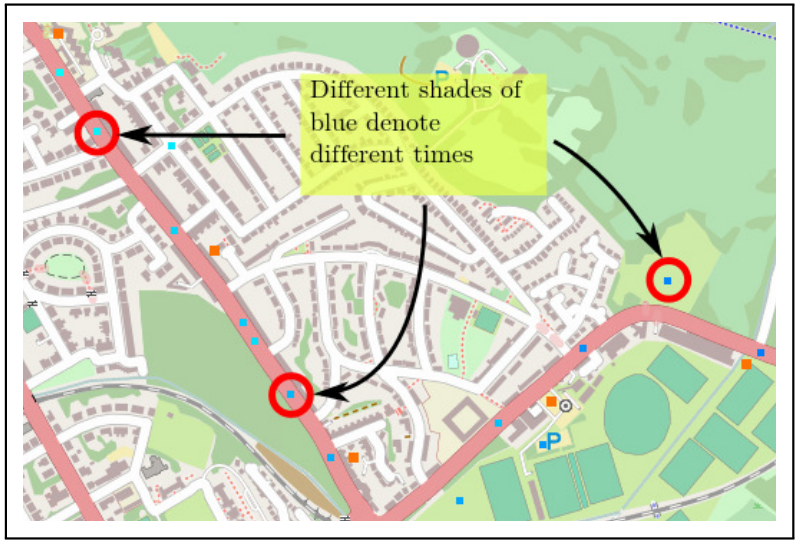
Collaboration (ongoing): profit from Axel Legay's expertise on (UPPAAL) SMC and his experience with SMC in the railway domain

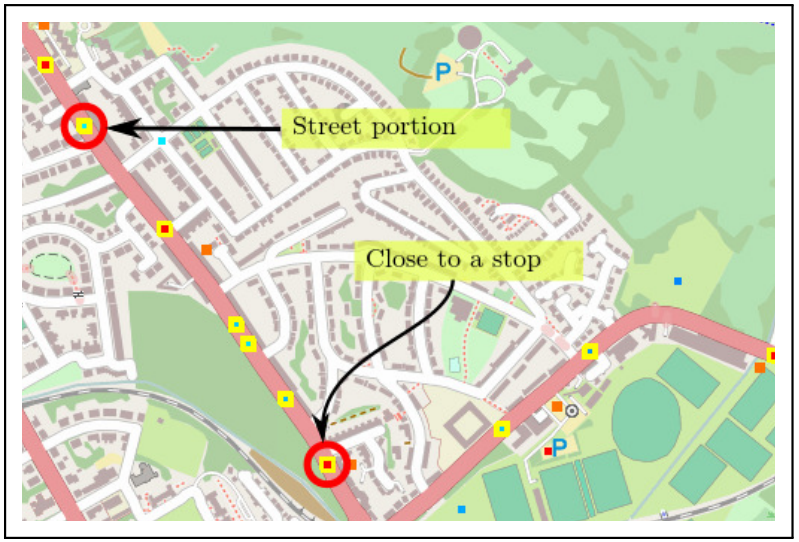
Cappart et al., Verification of Interlocking Systems Using Statistical Model Checking @ HASE'17

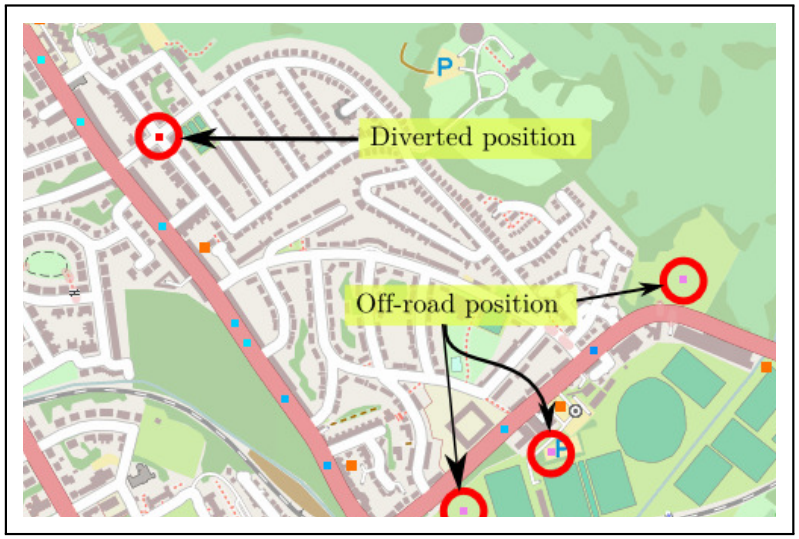
Tool support: can spatial model checking become a first class citizen in a continuous time model checker?

Thanks for your attention!

Topochecker already applied to smart buses







Ciancia et al., Spatio-temporal model checking of vehicular movement in public transport systems @ *STTT*'18