

Quantitative Analysis of Moving Block Railway Signalling Scenarios

Experiences and Outlook

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

joint work with

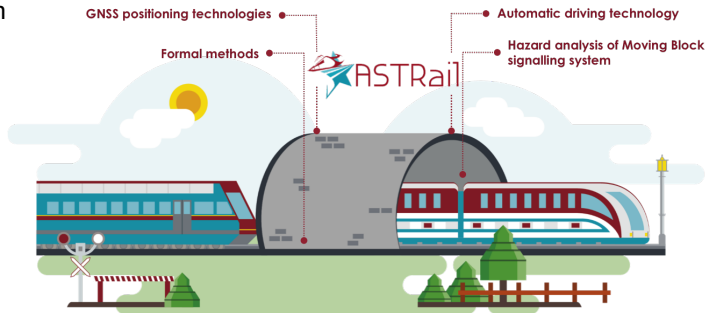
Davide Basile Vincenzo Ciancia Alessio Ferrari Axel Legay
UCL, Belgium

PRIN IT MaTTerS

12 June 2020

Outline

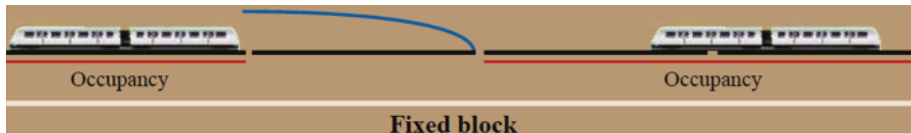
- 1 Industrial context: next generation railway signalling systems
- 2 Case study: moving block railway signalling scenarios from EU projects
- 3 Experiences: statistical model checking with UPPAAL SMC and strategy synthesis with UPPAAL Stratego
- 4 Outlook: spatio-temporal analysis with UPPAAL SMC or mCRL2
- 5 Conclusion



Industrial context: next generation railway signalling

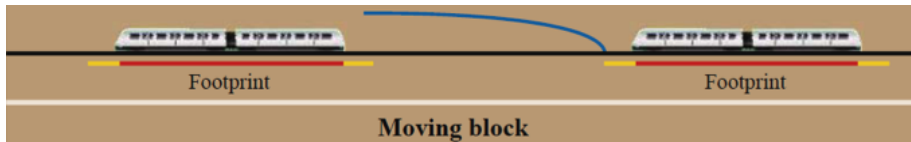
Current ERTMS / ETCS signalling systems max. level 2:

- 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)

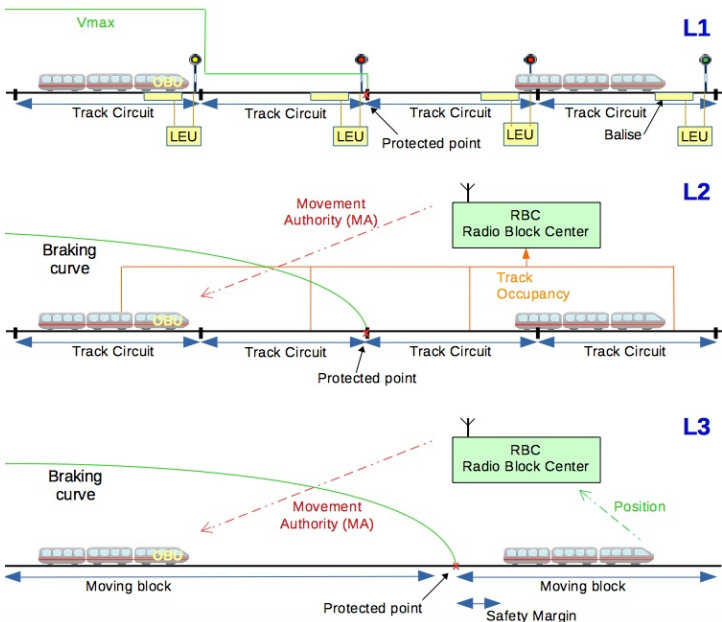


Next generation railway signalling systems from level 3:

- 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)

“Shift2Rail aims to double the capacity of the European rail system and increase its reliability and service quality by 50%, all while halving life-cycle costs”

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

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

Challenge: effective and precise moving block signalling systems by GNSS-based satellite positioning, leveraging on an integrated solution for signal outages (e.g. tunnels) and multipath interference in dense urban areas

FMT involved in H2020 Shift2Rail projects



SAatellite-based **S**ignalling and Automation Sys**T**ems on **RA**ilways
along with Formal Method and Moving Block Validation (2017–2019)

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

LINKS (IT), SIRTl (IT), Ardanuy Ingeniería (SP), Union des Industries Ferroviaires Européennes (UNIFE, BE),
École Nationale de l'Aviation Civile (ENAC, FR)



4SECURail Formal methods and CSIRT for the railway sector (2019–2021)

Formal Methods Demonstrator to evaluate cost, benefits and required learning curve of
using Formal Methods for the rigorous specification of a railway signalling infrastructure

Ardanuy, SIRTl, FIT Consulting (IT), HitRail (NL), Union Internationale des Chemins de fer (UIC, BE), Tree technology (SP)

**ASTRail-2: Advances in SaTellite positioning and moving block signaling for
RAILways (submitted)**

Modelling and analysis of moving block signalling for different railway systems and under
different operational conditions, using formal models that can capture the uncertainty of
moving block systems and tools that can perform quantitative analyses of safety concerns



UNIFE, LINKS, SIRTl, Ardanuy, Zabala (SP), Université Gustave Eiffel (FR)

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

- literature review and tool comparison of formal methods in railways submitted
Ferrari et al., Comparing Formal Tools for System Design: a Judgment Study @ ICSE'20
- 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 @ iFM'18
Ferrari et al., Survey on Formal Methods and Tools in Railways: The ASTRail Approach @ RSSRail'19
ter Beek et al., Adopting Formal Methods in an Industrial Setting: The Railways Case @ FM'19

WP2: Safety analysis of moving block signalling system

Basile et al., Statistical Model Checking of a Moving Block Railway Signalling Scenario with Uppaal SMC @ ISOla'18
Basile et al., Modelling and Analysing ERTMS L3 Moving Block Railway Signalling with Simulink and UPPAAL SMC @ FMICS'19

Input: Real-Time UML (RT UML) and Simulink models obtained from/ 
upon requirements elicitation and refinement with industrial partners 

Output: UPPAAL SMC model

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

Main components L3 moving block signalling system

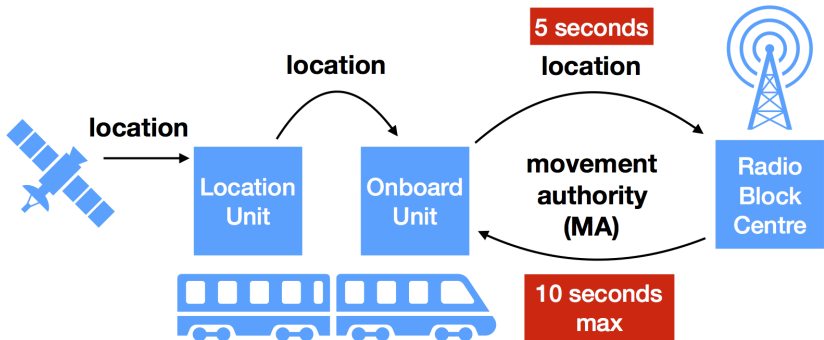
- OBU** train's onboard unit measures the train's current speed and verifies the train's integrity
- LU** train's localisation unit uses a GNSS-based positioning system to determine the train's location
- RBC** wayside radio block centre communicates continuously with OBU and LU
 - receives data regarding 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

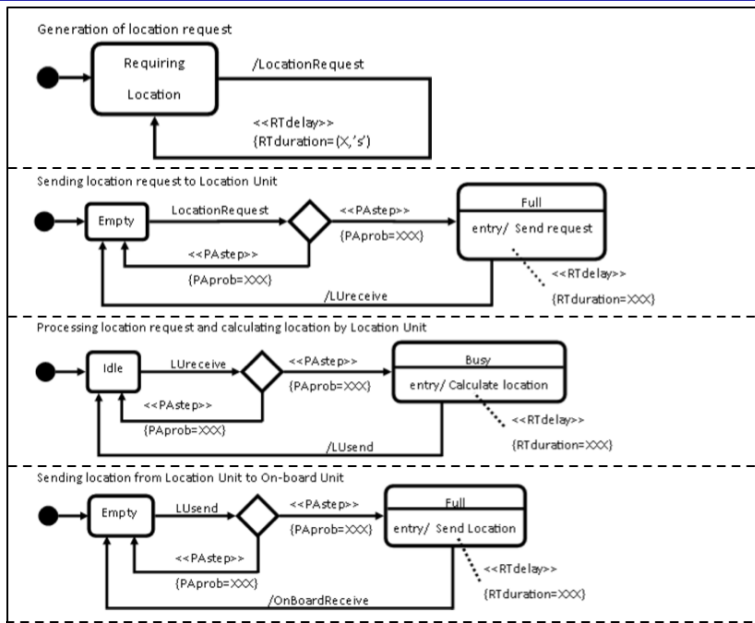
- consider train to communicate with one RBC, based on a seamless hand-over when the train moves from one RBC supervision area to the adjacent

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

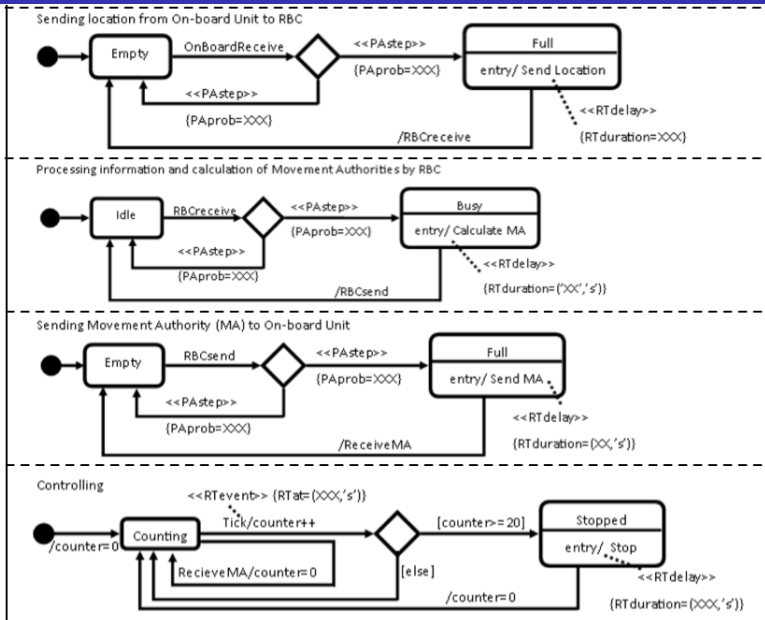
Moving Block system architecture



Model transformation: RT UML \rightarrow UPPAAL (1/2)

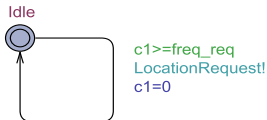


Model transformation: RT UML \rightarrow UPPAAL (2/2)

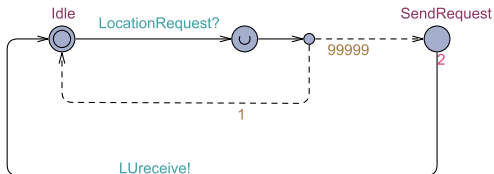


UPPAAL model of moving block signalling scenario (1/2)

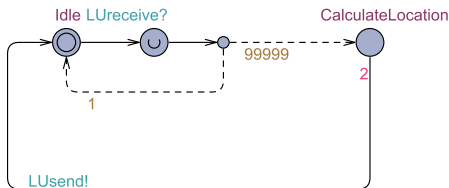
$(c1' == 1.0) \ \&\& \ (c1 \leq \text{freq_req})$



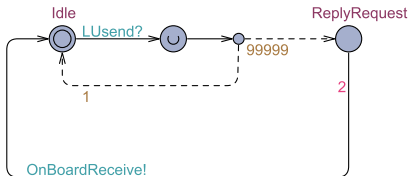
Generate location request



Send location request



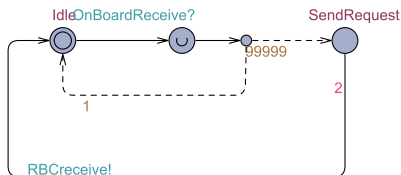
Calculate location



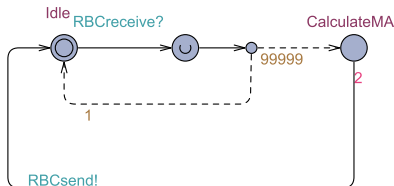
Send location

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

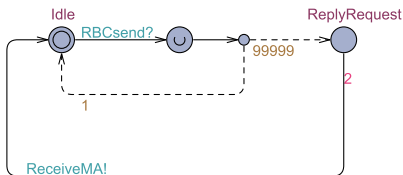
UPPAAL model of moving block signalling scenario (2/2)



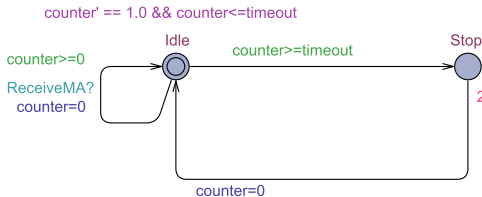
Send MA request



Calculate MA



Send MA



Control MA freshness

Industrial partners: $\text{timeout} = 3 \times \text{freq_req}$, initial value clock counter is 5

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

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.”

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

$$A \diamond (\text{ReplyMA.ReplyRequest} \parallel \text{Controlling.Stop})$$

UPPAAL SMC reports that this CTL property holds

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

$$\mathbb{P}_M(\diamond_{\leq(\text{timeout})} \text{Controlling.Stop})$$

UPPAAL SMC reports that this probability is in the interval $[0, 9.99994\text{e-}005]$, 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 negatives and false positives (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

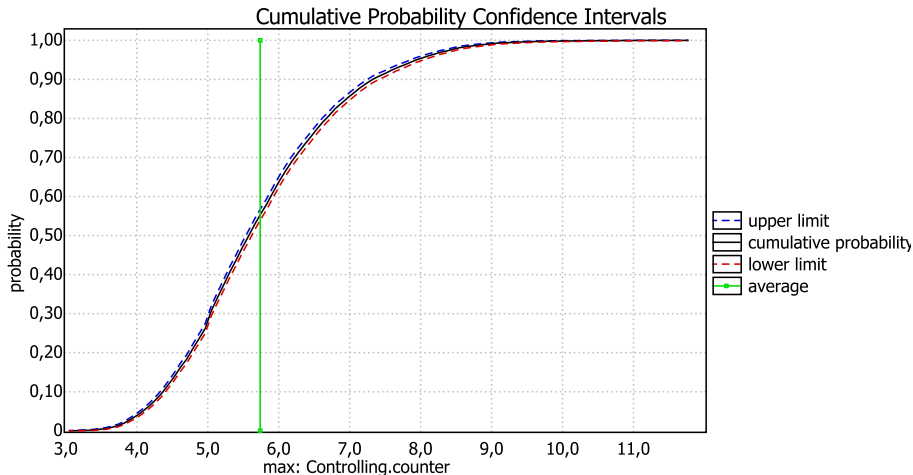
Goal: which of the three attempts has higher probability of success?

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

This evaluation computes in the interval of time of `timeout` (i.e. 15 sec.) the average of the maximum value of clock `counter`, using 10000 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



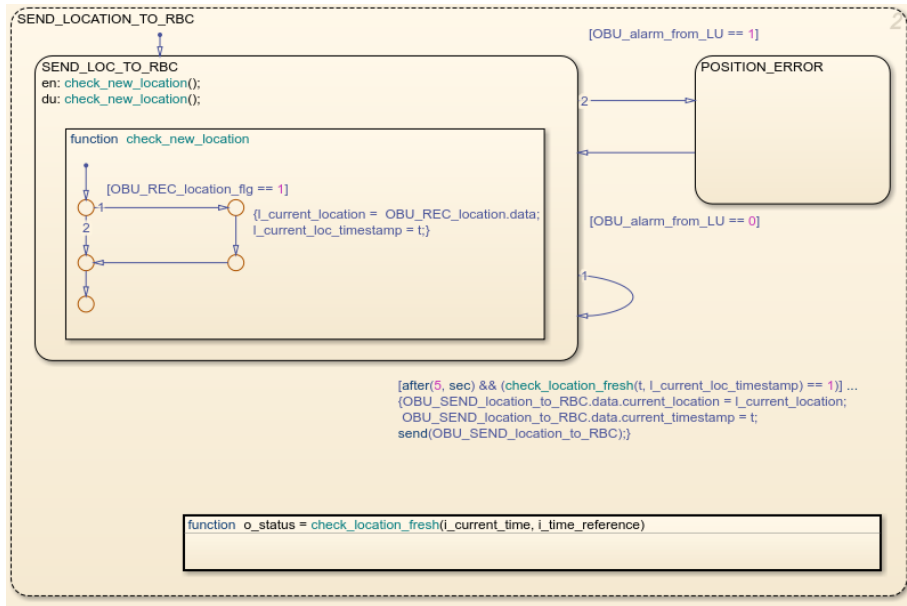
Parameters: $\alpha=0.005$, $\varepsilon=0.005$, bucket width=0.08733, bucket count=100

Runs: 10000 in total, 10000 (100%) displayed, 0 (0%) remaining

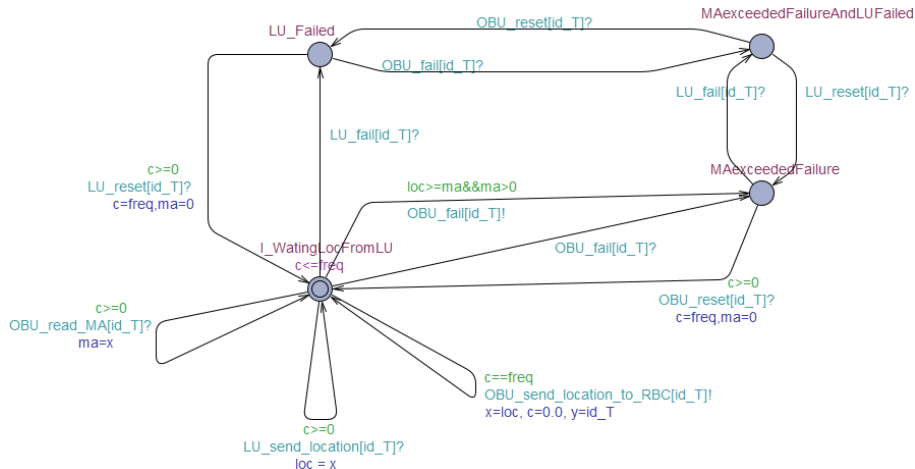
Span of displayed sample: [3.04171764778005, 11.7747301491212]

Mean of displayed sample: $5.73865788065071 \pm 0.0327581295234518$ (99.5% CI)

Model transformation: Simulink → UPPAAL



UPPAAL model of moving block signalling scenario



TRAIN_ATO_T models train movement (speed, acceleration/deceleration triggered by approaching the limit of the MA, simulating braking curves when reaching failure states)

1 Probability that the train's position exceeds the MA (with $ma = 1000$ m):

$\Pr[\leq 1000](\langle \rangle \text{ OBU_MAIN_SendLocationToRBC.MAexceededFailure})$

UPPAAL SMC reports that this probability is in the interval $[0, 0.00998576]$, with confidence 0.995 and obtained from 597 runs in ± 8 min.

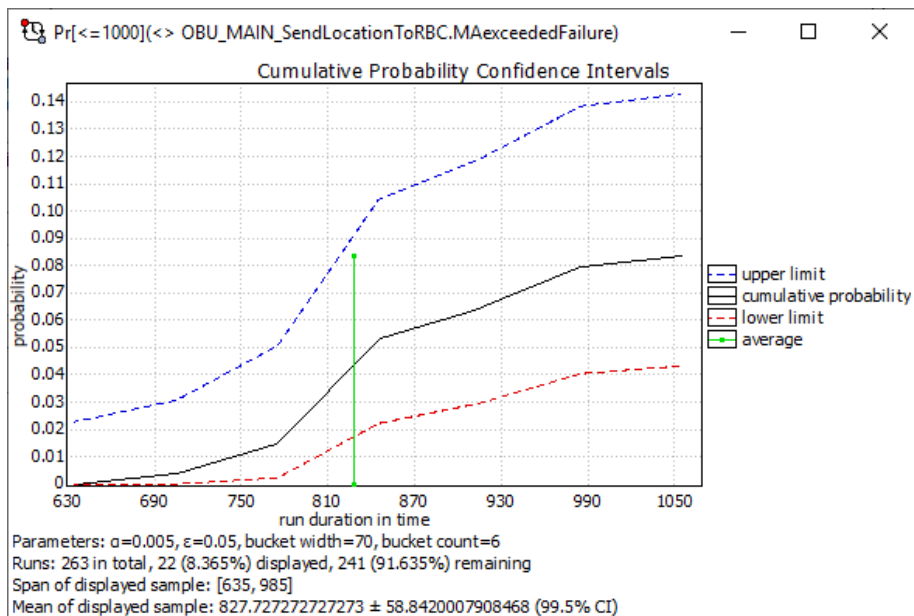
2 Probability that the train's position exceeds the MA (with $ma = 500$ m):

$\Pr[\leq 1000](\langle \rangle \text{ OBU_MAIN_SendLocationToRBC.MAexceededFailure})$

UPPAAL SMC reports that this probability is in the interval $[0.0430205, 0.14268]$, with confidence 0.995 and obtained from 263 runs in ± 3 min.

UPPAAL SMC v4.1.19 (rev. 5649) with statistical parameters: lower and upper probabilistic deviation $(-\delta, +\delta)$: 0.01; probability of false negatives $\alpha = 0.005$ and false positives $\beta = 0.5$; probability uncertainty (ϵ): 0.005.

Analyses with UPPAAL SMC



D. Basile, M.H. ter Beek, and A. Legay, Strategy Synthesis for Autonomous Driving in a Moving Block Railway System with Uppaal Stratego. In FORTE, LNCS 12136, Springer, 2020, 3–21.

- Extended the model to a stochastic priced timed game to account for automatic synthesis of autonomous driving
- Uppaal Stratego: strategy synthesis for timed games (safety) and reinforcement learning of the optimal strategy (reliability)
- While changing the set-up of the parameters, the driving strategy is automatically tuned to retain safety (MA never exceeded) as well as reliability (minimal expected arrival time)
- Experimentation needed interactions with developers, resulting in new releases, with patches fixing issues discovered through our model

Presentation by Davide @ FORTE: next Thursday, 18 June, 12:00–12:30

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

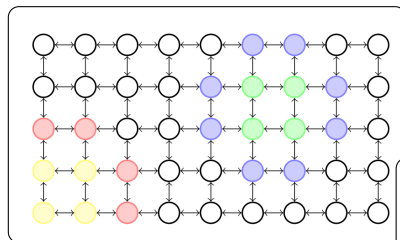
- ϕ expresses the presence of a single train in a specific area
- ψ expresses the absence of trains in a specific area

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)



Distance formulas, $\mathcal{D}^{\leq 3}\Phi$

RCC operators (overlaps, partially overlaps, etc.)

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: $green \mathcal{S} blue$

$\Phi ::=$	p	[ATOMIC PROPOSITION]
	\top	[TRUE]
	$\neg\Phi$	[NOT]
	$\Phi \wedge \Phi$	[AND]
	$\mathcal{N}\Phi$	[NEAR]
	$\Phi \mathcal{S} \Phi$	[SURROUNDED]

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

Ciancia, Latella, Massink: Embedding RCC8D in the Collective Spatial Logic CSLCS @ Rocco's Festschrift'19

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 and image analysis

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

Banci Buonamici et al., Spatial Logics and Model Checking for Medical Imaging @ STTT'20

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

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

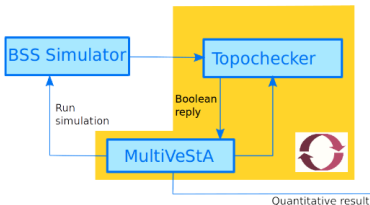
Sebastio & Vandin, MultiVeStA: Statistical Model Checking for Discrete Event Simulators @ VALUETOOLS'13

- applied to spot congestion in bike sharing systems

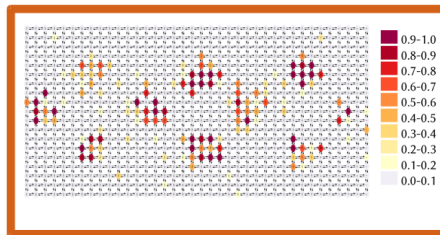
Ciancia et al., A Tool-Chain for Statistical Spatio-Temporal Model Checking of Bike Sharing Systems @ ISoLA'16

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

Statistical spatio-temporal model checking @ ISoLA'16



full = [vacantPlaces == 0]
cluster = I full
eventuallyCluster = EF cluster



VoxLogicA: see kick-off presentation by Vincenzo

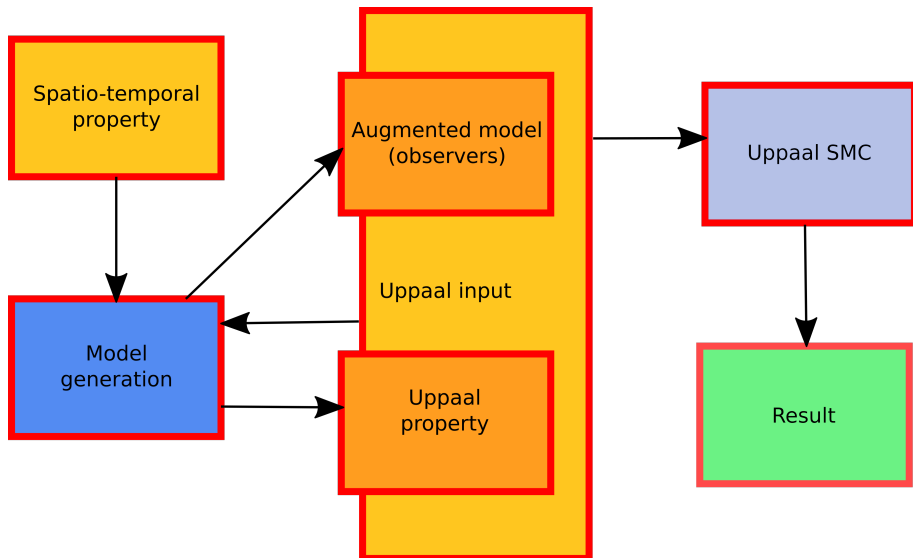
`www.voxlogica.com`

G. Belmonte, V. Ciancia, D. Latella, and M. Massink,

VoxLogicA: A Spatial Model Checker for Declarative Image Analysis @ TACAS'19

- Specific for images
- Much faster than topochecker, multiplatform
- No temporal or statistical fragments (yet!)
- Work in progress: GraphLogicA (for arbitrary graphs, available in github branch)

Spatio-temporal analysis with UPPAAL SMC? or mCRL2?



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?)

So far: train position in unidimensional space identified by one coordinate and, at each cycle, the train is allowed to either move one unit or stay idle

Future work: use topochecker for this case study? make it more realistic?

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

Thanks for your attention!

- D. Basile, M.H. ter Beek, A. Fantechi, S. Gnesi, F. Mazzanti, A. Piattino, D. Trentini, and A. Ferrari, On the Industrial Uptake of Formal Methods in the Railway Domain: A Survey with Stakeholders. In *Proceedings of the 14th International Conference on Integrated Formal Methods (IFM'18)* (C.A. Furia and K. Winter, eds.), Lecture Notes in Computer Science 11023, Springer, 2018, 20–29.
- D. Basile, M.H. ter Beek, and V. Ciancia, Statistical Model Checking of a Moving Block Railway Signalling Scenario with Uppaal SMC. In *Proceedings of the 8th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation: Verification (ISoLA'18)* (T. Margaria and B. Steffen, eds.), Lecture Notes in Computer Science 11245, Springer, 2018, 372–391.
- A. Ferrari, M.H. ter Beek, F. Mazzanti, D. Basile, A. Fantechi, S. Gnesi, A. Piattino, and D. Trentini, Survey on Formal Methods and Tools in Railways: The ASTRail Approach. In *Proceedings of the 3rd International Conference on Reliability, Safety, and Security of Railway Systems: Modelling, Analysis, Verification, and Certification (RSSRail'19)* (S. Collart-Dutilleul, T. Lecomte, and A. Romanovsky, eds.), Lecture Notes in Computer Science 11495, Springer, 2019, 226–241.
- D. Basile, M.H. ter Beek, A. Ferrari, and A. Legay, Modelling and Analysing ERTMS L3 Moving Block Railway Signalling with Simulink and UPPAAL SMC. In *Proceedings of the 24th International Conference on Formal Methods for Industrial Critical Systems (FMICS'19)* (K.G. Larsen and T. Willemse, eds.), Lecture Notes in Computer Science 11687, Springer, 2019, 1–21.
- M.H. ter Beek, A. Borälv, A. Fantechi, A. Ferrari, S. Gnesi, C. Löfving, and F. Mazzanti, Adopting Formal Methods in an Industrial Setting: The Railways Case. In *Formal Methods – The Next 30 Years—Proceedings of the Third World Congress on Formal Methods (FM'19)* (M.H. ter Beek, A. McIver, and J.N. Oliveira, eds.), Lecture Notes in Computer Science 11800, Springer, 2019, 762–772.
- A. Ferrari, F. Mazzanti, D. Basile, M.H. ter Beek, and A. Fantechi, Comparing Formal Tools for System Design: a Judgment Study. In *Proceedings of the 42nd International Conference on Software Engineering (ICSE'20)*, ACM, 2020.
- D. Basile, M.H. ter Beek, and A. Legay, Strategy Synthesis for Autonomous Driving in a Moving Block Railway System with Uppaal Stratego. In *Proceedings of the 40th IFIP WG 6.1 International Conference on FORmal TEchniques for Distributed Objects, Components, and Systems (FORTE'20)* (A. Gotsman and A. Sokolova, eds.), Lecture Notes in Computer Science 12136, Springer, Berlin, 2020, 3–21.

Topochecker already applied to smart buses

