# Modelling and Verification of ERTMS Level 2

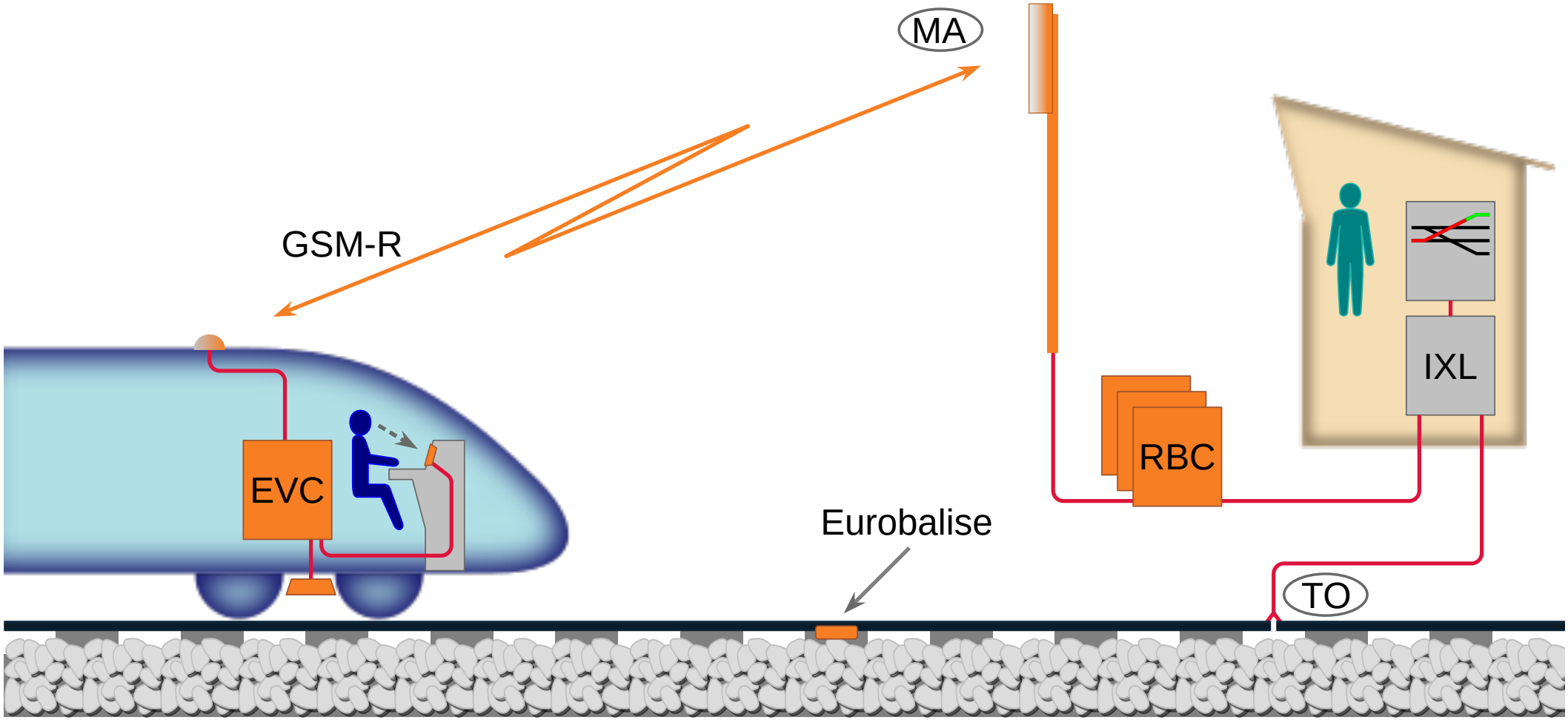
## A Comparison of KeYmaera, Real-Time Maude, and UPPAAL

M Roggenbach (Swansea, Wales, UK)

P James, A Walters, M Seisenberger, Y Zhang

DisCoRail, June 2019

# ERTMS Level 2



# Modelling and Verification of ERTMS in Real-Time Maude

- U Berger, P James, A Lawrence, M Roggenbach, M Seisenberger: Verification of the European Rail Traffic Management System in Real-Time Maude. Sci. Comput. Program. 154: 61–88, 2018.

Results:

- Successful safety verification in a whole system approach in Real-Time Maude
- Design mistakes in XL, RBC, Train setup alone can lead to safety violations (no fault tolerance)

# New PhD project with Siemens Rail UK: Test the location-specific part of a RBC

Siemens concern: RBC is 'new', quality assurance?

Outline of our approach:

1. Model ERTMS
2. Demonstrate that the model has qualities (e.g., is safe)
3. Develop test theory
   (along M-C Gaudel's "Testing can be formal too")
4. Test RBC against (XL || Controller || Trains)

# Current state of the project

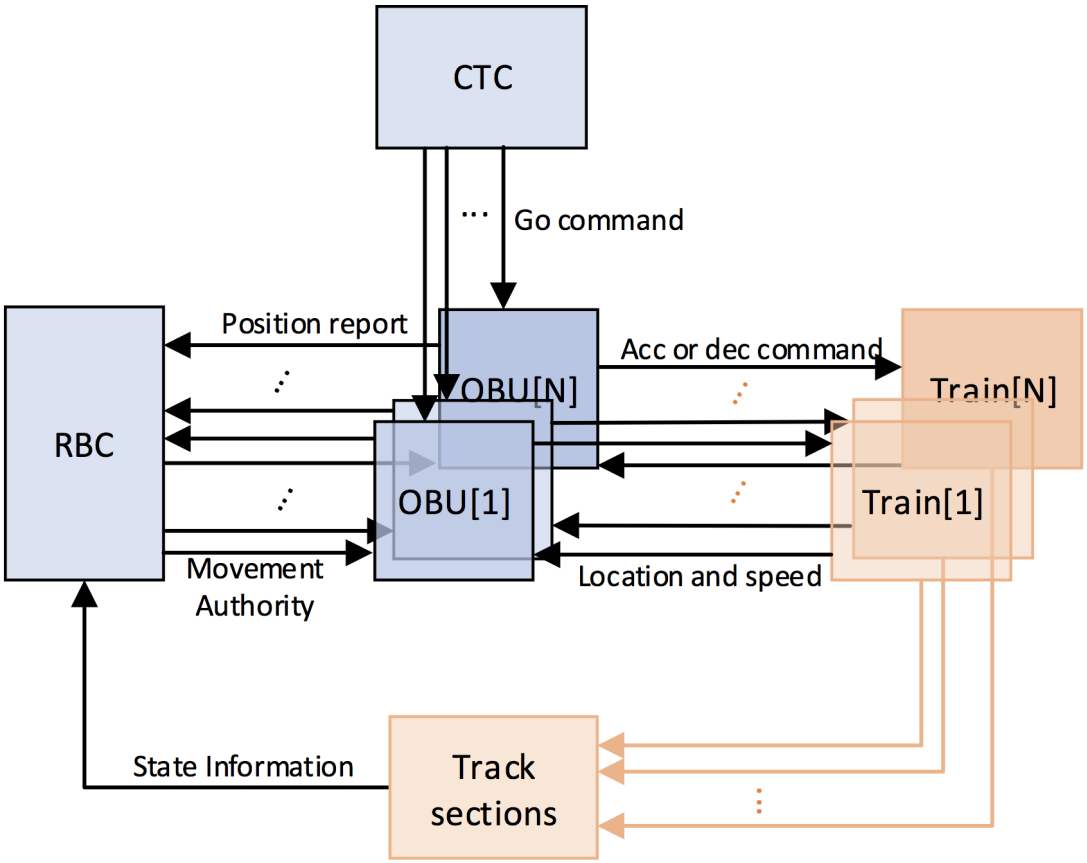
- Investigate the suitability of timed FMs to model ERTMS (here)
- Feasibility-Study: testing Real-Time Maude against Siemens RBC (on the way)

# Overview

Starting point: narrative of a simplified system
Open question: how rich shall the train model be?
Three FMs their suitability

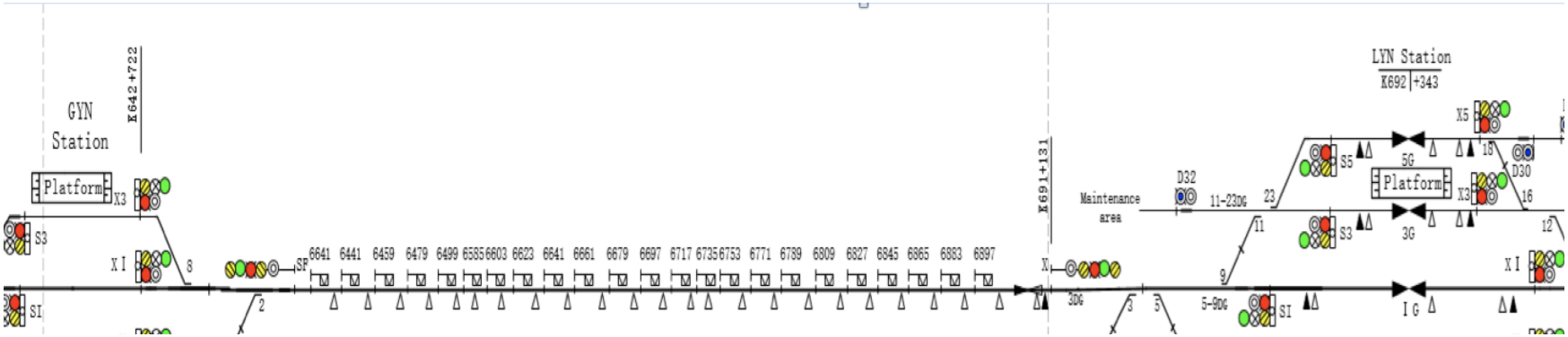
# Starting point: narrative of a simplified system

# System architecture




"Run $N$ trains on a single line"

# Track Layout




Uni-directional line from GYN station to LYN station

points replaced by tracks of the same length

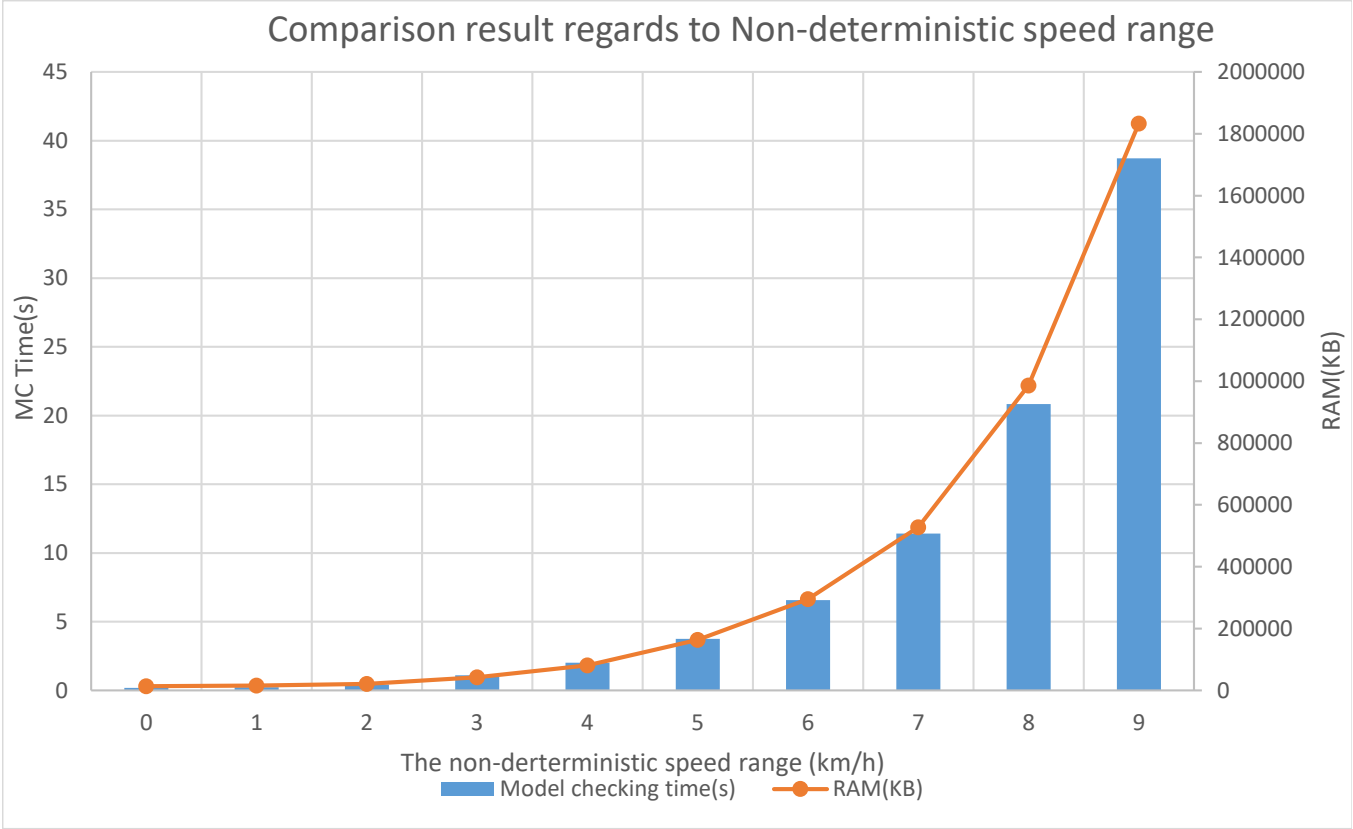
# Open question: how rich shall the train model be?

# The maximal progress assumption

Trains accelerate till the reach maximal speed
travel then at maximal speed
till they are forced to break.

$\leadsto$ makes the train behavior ‘deterministic’

# Price in model checking with Uppaal for weakening the maximal progress assumption




One train; Gyn to Lyn; safety: train stays within MA.

# Which braking behavior?

- Only emergency braking?
- Only service braking?
- Non deterministic choice between the two?

Probably: ndtm (probabilistic?) choice.

# Which physical model?

Simple setting: $acc = 1m/s^2$ and $dec = -1m/s^2$

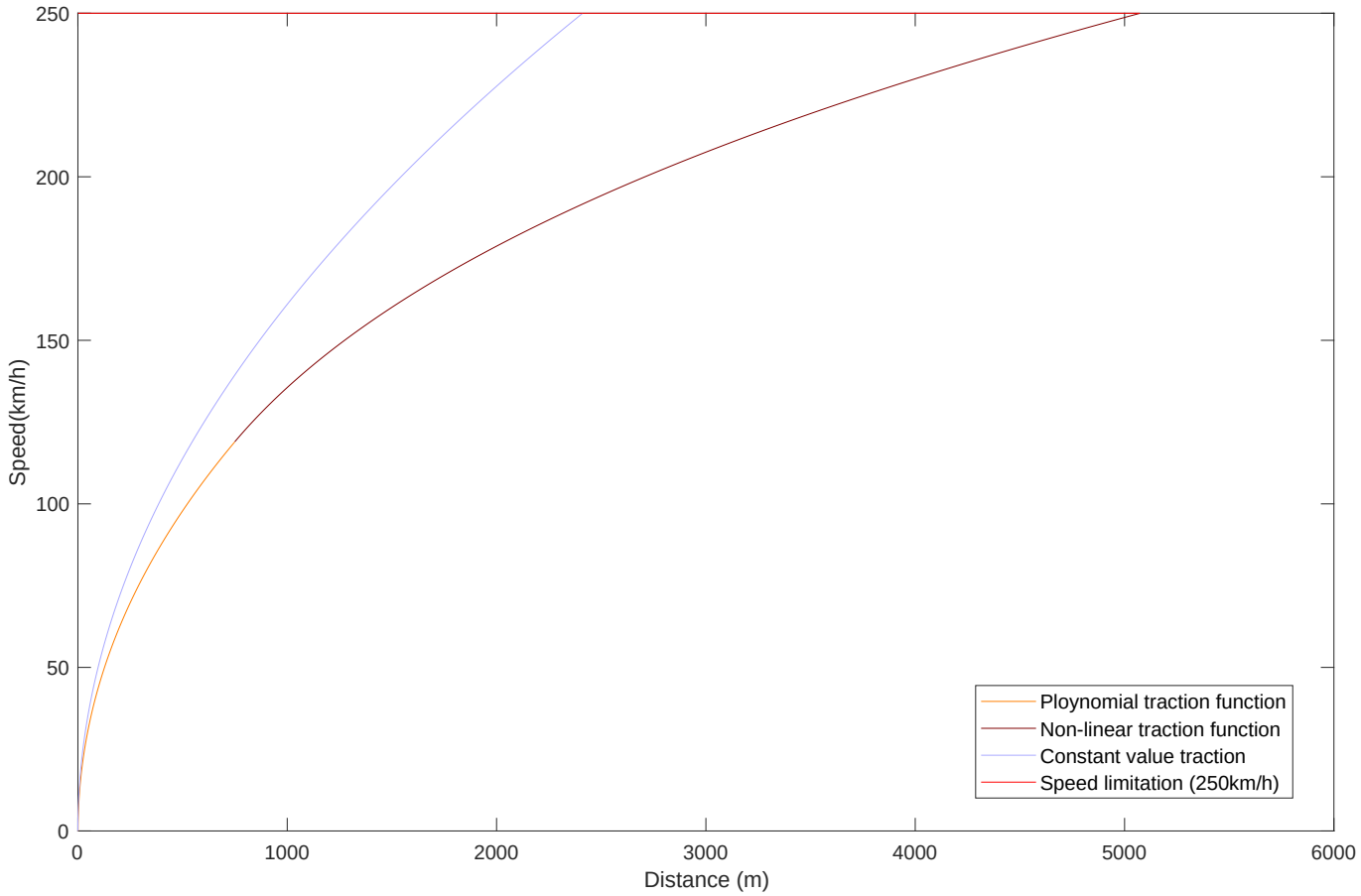
Realistic setting: e.g., $acc = F_T/M_T$ with $M_T = 380t$ and

$$F_T = \begin{cases} -0.285v + 300 & 0 \leq v \leq 119km/h \\ 31500/v & v > 119km/h \end{cases}$$

and similar formulae for $dec$.

The realistic setting possibly poses questions concerning numerics.

# Effect of different traction functions



# "Shopping list" concerning train behavior

- free choice of travel speed
- ndtm choice (probabilistic) between behaviors
- non-linear functions for acc and dec

# Three FMs and their suitability

# Comparison

| | Distributed system | Communication | Railway specific data types | Continuous and discrete control | Safety verification | Non-deterministic train operation | Timed system property | Subjective criteria | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Modeling | Simulation | Verification |
| **UPPAAL** | ✓ | ✓ | ✓<br>Via C-like structs | (✓)<br>Realized in C | (✓)<br>Under maximal progress assumption | ✓ | (✓)<br>Sub-language of timed CTL | Natural, information flow needs consideration | ✓<br>Visual support | ✓<br>Scaling is a challenge |
| **KeYmaera** | -<br>One integrated model | - | - | (✓)<br>Modeled via encoding | ✓ | ✓ For speed<br>? For state-based control | ?<br>Duration calculus | Challenging | - | Interactive proof, but response can be time consuming |
| **Real-Time Maude** | ✓ | ✓<br>Through data parsing | ✓<br>Via classes | (✓)<br>Rational | (✓)<br>Under maximal progress assumption | ? | ✓<br>Timed CTL | Natural | ✓<br>Text heavy output | ✓<br>Scaling is a challenge |

# Open question: how to turn this comparison into a more 'scientific' one?

Comparison projects:

- Survey on Formal Methods and Tools in Railways: The ASTRail Approach. RSSRail 2019.
- Comparing Formal Verification Approaches of Interlocking Systems. RSSRail 2016.

# Conclusion

# Summary

- Underlying problem: Testing of RBCs
- Leads to: modelling of ERMTS Level 2
- Central question: how rich must train behavior be?

# Future work

- Address the unanswered criteria
- Benchmark comparison of verification
- Semantical comparison of the models (?)

# I hope you liked our (fairy)tale