# Model-Based Testing of ETCS RBCs

Aled Rhys Walters

Swansea University

An iCASE PhD in conjunction with
Siemens Rail Automation

BCTCS - 06/04/2020

Swansea University
Prifysgol Abertawe

# Contents

# Section 1

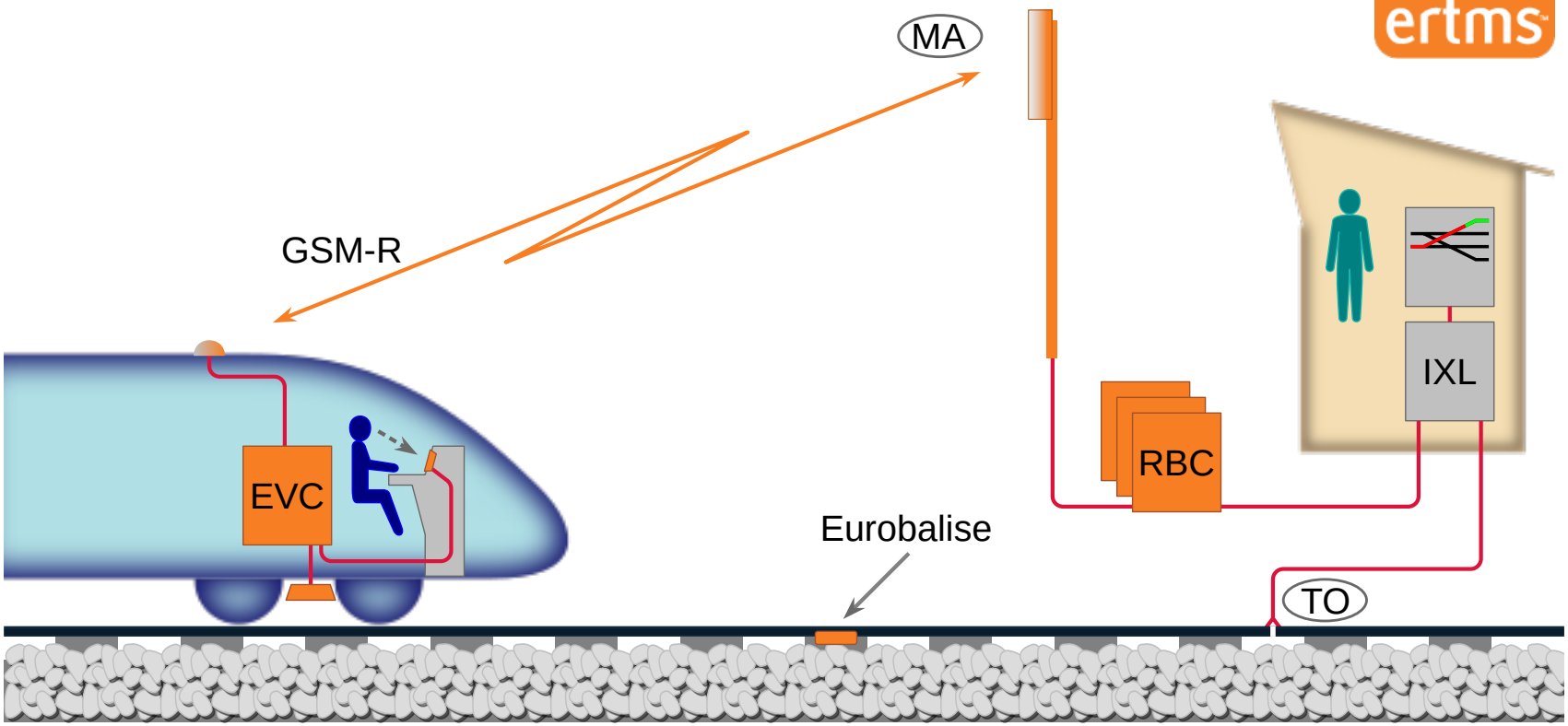
## ERTMS and the Railway

# Railway Control Systems

- Rich history of railways in Britain
- Mixed priorities for public and industry
- Signalling one key element for safety

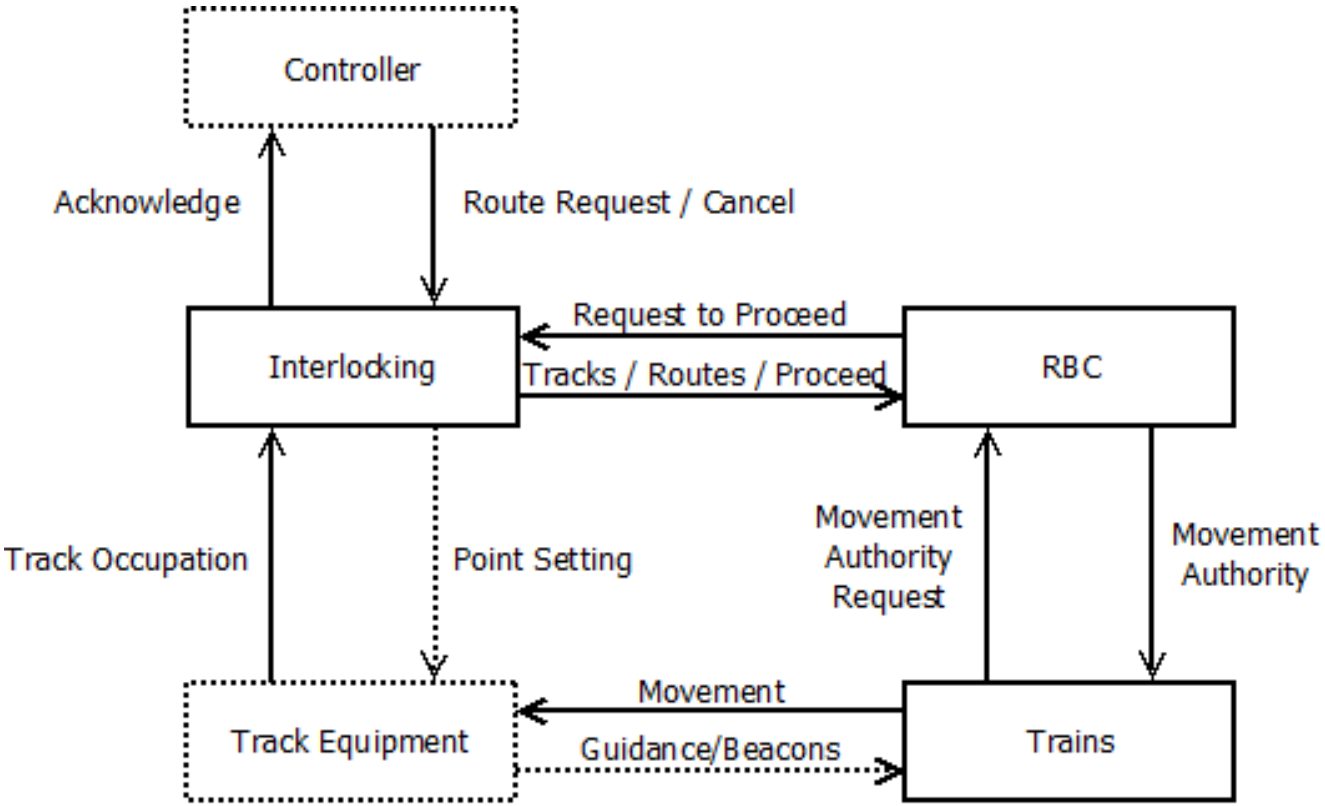
Safety encompasses e.g. avoiding train collisions, derailment, and run-through

# European Rail Traffic Management System




- State-of-the-art
- Safety critical
- Aimed at unification

# Radio Block Centre




The RBC and onboard computer are new components with little engineering history, motivating the need for quality assurance

# Section 2

# Our Testing Approach

# Testing

Definition: Testing is the process of systematically experimenting with a material object (in the physical world) in order to establish its quality.

- Testing is a dynamic activity
  - The tester interacts with the System Under Test (SUT)
  - The SUT is executed
- In contrast with static analysis, abstract interpretation, formal verification, or model checking
  - Analyse a mathematical object

# Current Test Practice at Siemens

- Begin with requirements in standardised documents
- From these write a scenario to run that tests these conditions
- Write these scenarios into scripts to run on the rig
- Observe the simulation, and analyse the communication log

# Model-Based Testing

General Approach:

- Develop a test model
- Prove that the test model exhibits the 'right' properties
- Derive a test suite from the model
- Execute the tests on the system

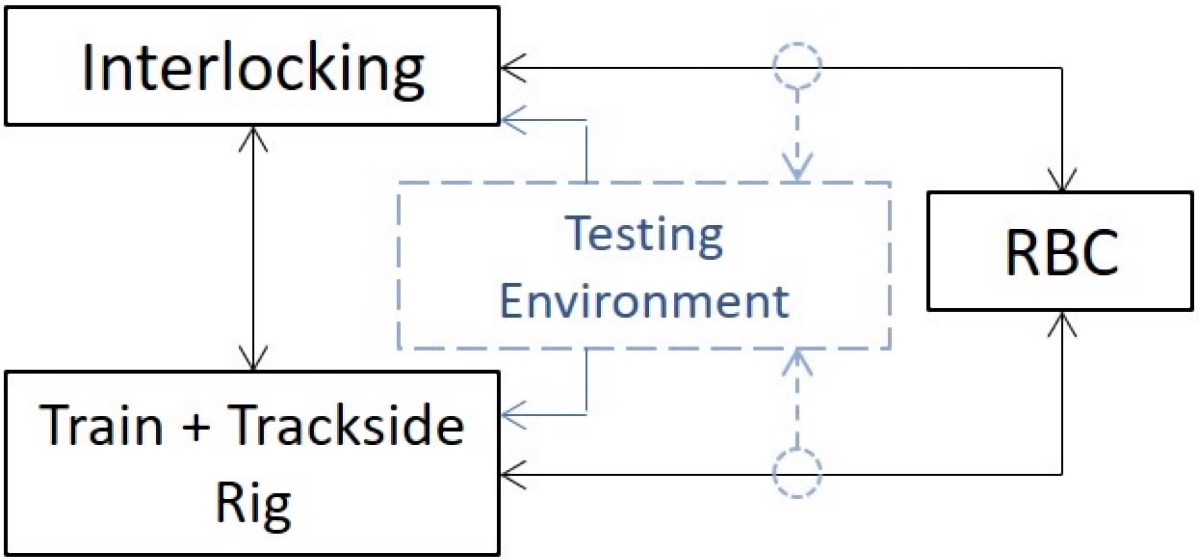
Fundamental properties of a test suite include:

Soundness: Each correct implementation should pass

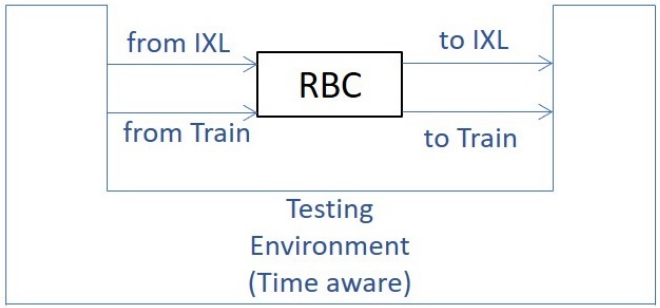
Exhaustiveness: Each incorrect implementation should fail

# Test Architecture

A:




B:




B is a usual test architecture

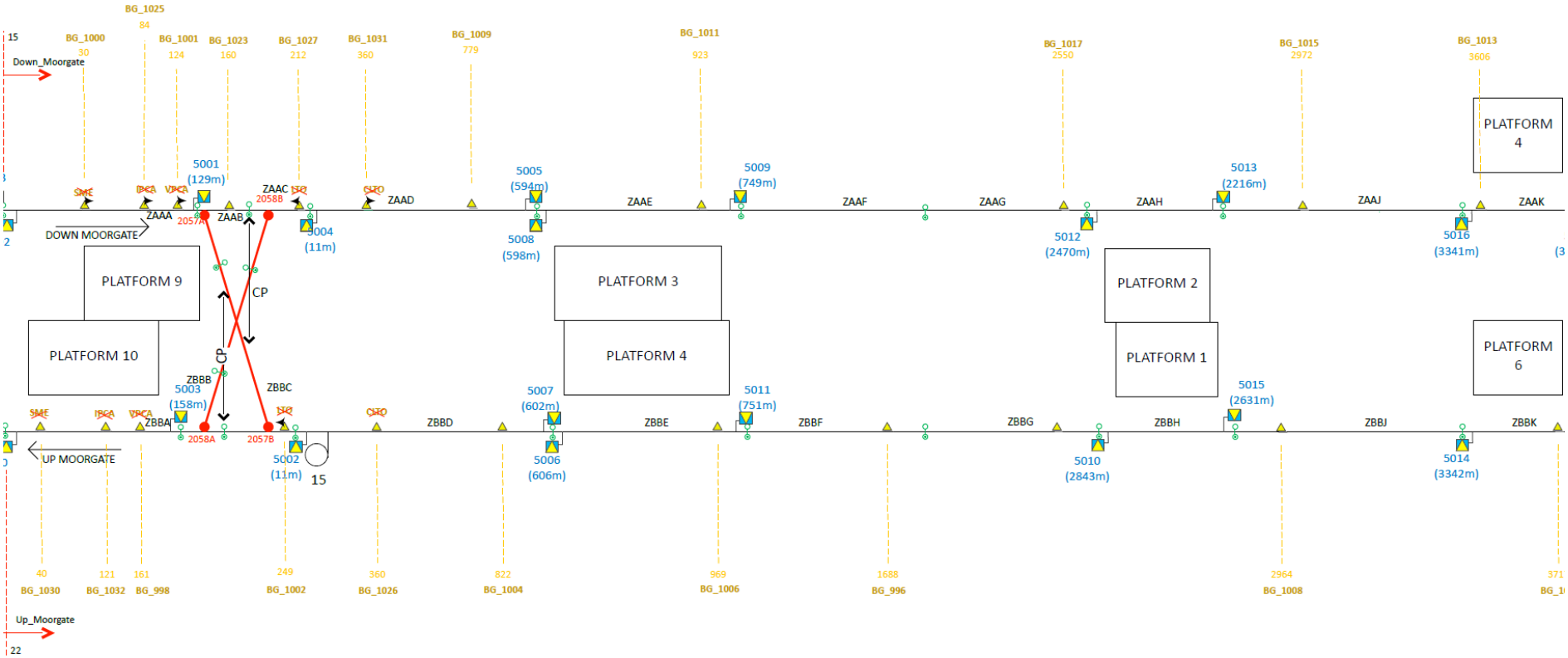
A is the test architecture (Siemens) that we are reusing

The interlocking and rig (simulation environment) are physical components that are assumed to be correct, thus the RBC is the system under scrutiny

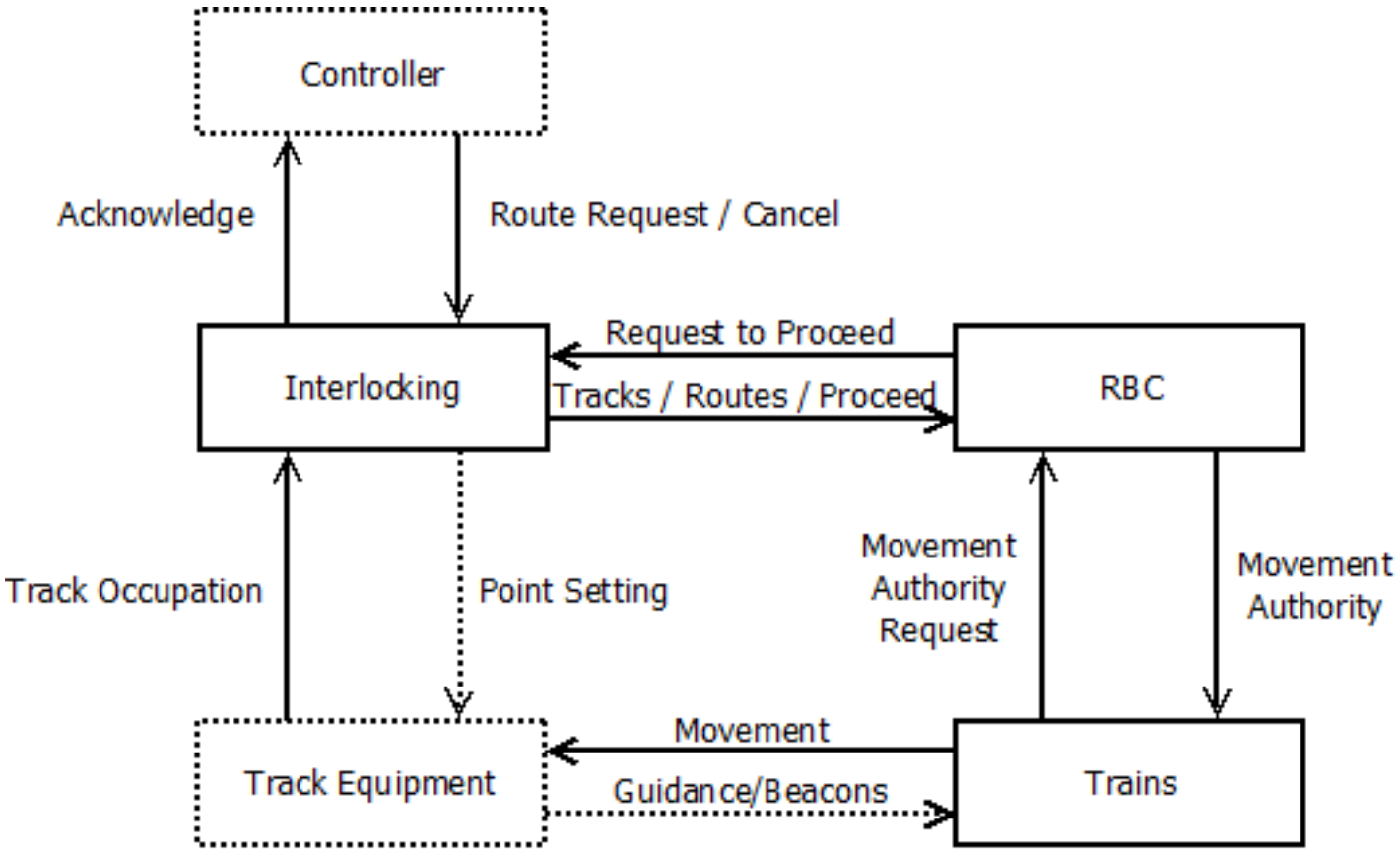
Section 3

# Modelling

# Scheme Plan


Down_Moorgate
Up_Moorgate
DOWN MOORGATE
UP MOORGATE
PLATFORM 9
PLATFORM 10
PLATFORM 3
PLATFORM 4
PLATFORM 2
PLATFORM 1
PLATFORM 4
PLATFORM 6
CP
CP
ZAAA
ZAAB
ZAAC
ZAAD
ZAAE
ZAAF
ZAAG
ZAAH
ZAAJ
ZAAK
ZBBA
ZBBB
ZBBC
ZBBD
ZBBE
ZBBF
ZBBG
ZBBH
ZBBJ
ZBBK
5001 (129m)
5002 (11m)
5003 (158m)
5004 (11m)
5005 (594m)
5006 (606m)
5007 (602m)
5008 (598m)
5009 (749m)
5010 (2843m)
5011 (751m)
5012 (2470m)
5013 (2216m)
5014 (3342m)
5015 (2631m)
5016 (3341m)
2057A
2057B
2058A
20588
BG_1000
BG_1001
BG_1023
BG_1025
BG_1027
BG_1031
BG_1009
BG_1011
BG_1017
BG_1015
BG_1013
BG_1030
BG_1032
BG_998
BG_1002
BG_1026
BG_1004
BG_1006
BG_996
BG_1008

# Communications




1

[1] Berger, U.; James, P.; Lawrence, A.; Roggenbach, M. & Seisenberger, M. Verification of the European Rail Traffic Management System in Real-Time Maude Science of Computer Programming, 2018, 154, 61–88

# Test Model: Instantiation of Generic Real-Time Maude Model

```
sort MarkerBoard . ops 5001, 5005, 5009, 5013, 5017, K359, K361, EMB : -> MarkerBoard .

sort RouteName .
ops R5001, R5005, R5009, R5013, R5017, RK359, RE : -> RouteName .

sort Track .
ops CrossBack CrossForward ZAAA ZAAB ZAAC ZAAD ZAAE ZAAF ZAAG ZAAH ZAAJ ZAAK ZAAL 0832 0833 0834 0835
Entry Exit NullTrack : -> Track .

sort Point .
ops 2057A 2057B 2058A 2058B 2059A 2059B : -> Point .

ceq next(0832, MB, PPos) = 0833 if MB == K361 or MB == EMB .
ceq next(0833, MB, normal) = 0834 if MB == K361 or MB == EMB .
eq next(0834, EMB, PPos) = 0835 .
eq next(0835, EMB, PPos) = Exit .

op clearTracks : RouteName -> SetOfTracks .
op normalPts : RouteName -> SetOfPoints .
op reversePts : RouteName -> SetOfPoints .
op isReleaseTrack : Track Track -> Bool .
op release : Track -> Point .
op conflictingRoutes : RouteName -> SetOfRouteNames .

op TrackToPoint : Track -> Point .
eq TrackToPoint(ZAAB) = 2057A .
eq TrackToPoint(ZAAC) = 2058B .

eq TrackToPoint(0834) = 2059B .
```

# Proving Properties: No Collisions

Model is verified for safety properties, namely Collision-freedom

1. Set minimum distance between trains
2. One train per track

# Derive Test Suite: Model Simulation

```
(trew {
< inter1 : Inter | pointPositions : empty,
routeset : empty, occ : empty, pointslocked : empty >
 newmte(< train1 : Train | state : acc, dist : 700, speed : 0, ac : 1, ma : 750,
 tseg : ZAAE , tsegR : ZAAE, maxspeed : 60, length : 0,
 mtemin : 1, end : false, mb : 5009 > )
< rbc1 : RBC | availableRoutes : empty , designatedRoutes : empty >
< ctr1 : Controller | counter : 1 , routes : routeOrder, end : false >

} in time <= 97 .)
```

- Distance: 700
  - Track: ZAAE
- Markerboard: 5009
  - Movement Authority: 750

# RT-Maude Simulation Output

- **in time** 31
- **marequest**(train1, ZAAE)
- **routerequest**(R5013)
- **marequest**(train1, ZAAE)
- **setroutes**((R5001 |− > true, R5005 |− > true, R5009 |− > true, R5013 |− > true))
- **marequest**(train1, ZAAE)
- **proceedrequest**(R5013)
- **proceedgrant**(R5013)
- **setroutes**((R5001 |− > true, R5005 |− > true, R5009 |− > true, R5013 |− > false))
- **magrant**(train1, 5013, 2216)
- **in time** 31
- **in time** 32

# Section 4

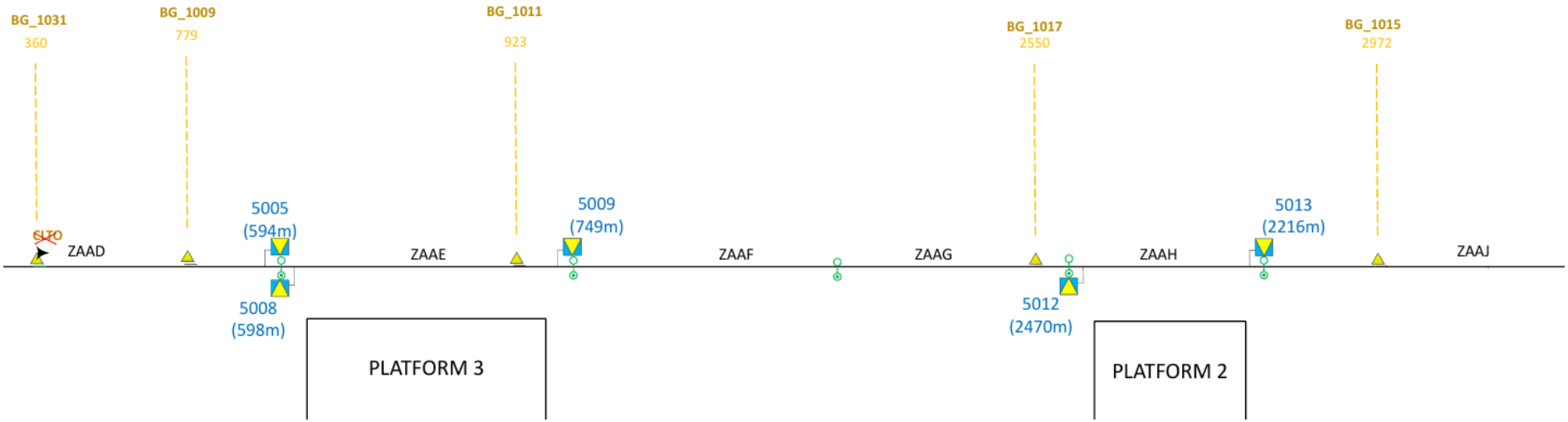
# A Typical Test Cycle

# A Typical Test Cycle: After a Movement Authority request, the RBC hands out the correct Movement Authority

My Approach:

1. Realisation of Scenario
   - R-T Maude : Start Configuration
   - Railway Environment and Train Simulator (RETS) : Scripts
2. Filtering of logs
3. Log Comparison

# Track Layout



# Realisation

## RETS Script:

```
InitTrain ("S5005", 10, "NC", "Apply Brake")
OperateTrain
ChangeCommsStatus ("C","Valid")
FailTC ("TZAAF", "Occupied")
SetTrackCctTrigger ("TZAAE", "Occupied", 0)
FailTC ("TZAAF", "None")
FailTC ("TZAAJ", "Occupied")
```

---

## RT Maude Start Configuration:

$$< \text{train1} : \text{Train} \mid \text{state} : \text{acc}, \text{dist} : 700, \text{speed} : 0, \text{ac} : 1, \text{ma} : 750, \text{tseg} : \text{ZAAE} , \text{tsegR} : \text{ZAAE}, \text{maxspeed} : 60, \text{length} : 0, \text{mtemin} : 1, \text{end} : \text{false}, \text{mb} : 5009 > )$$

Start configuration in both systems is 'equivalent' : Signal S5005 corresponds to track beginning of track ZAAE

# Filtering and Comparison of Logs

Filtered RETS Log:

```
Time: 0s # MA Req (MsgId 132)
»    »    »    Distance = 789 (ZAAD)
Time: 1.1909982s # MA (MsgId 3)
»    »    »    MA = 950 (5009)
Time: 2.206023 # MA Req (MsgId 132)
»    »    »    Distance = 789 (ZAAD)
Time: 110.421223s # MA (MsgId 3)
»    »    »    MA = 2821 (5013)
Time: 121.421501s # MA Req (MsgId 132)
»    »    »    Distance = 2295.1 (ZAAG)
Time: 121.457402s # MA (MsgId 3)
»    »    »    MA = 2821 (5013)
Time: 122.41759s # MA Req (MsgId 132)
»    »    »    Distance = 2302 (ZAAG)
Time: 132.00754s # MA Req (MsgId 132)
»    »    »    Distance = 2440.9 (ZAAG)
Time: 132.044782s # MA (MsgId 3)
              MA = 2821 (5013)
```

Filtered RT Maude Log:

```
marequest(train1, ZAAE)
in time 28.3769
in time 29.3769
marequest(train1, ZAAE)
in time 29.3769
in time 30.3769
marequest(train1, ZAAE)
in time 30.3769
in time 31
marequest(train1, ZAAE)
magrant(train1, 5013, 2216)
in time 31
.
.
marequest(train1, ZAAF)
magrant(train1, 5017, 3485)
in time 54.7854
in time 55.7854
marequest(train1, ZAAF)
magrant(train1, K359, 3769)
in time 55.7854
.
.
marequest(train1, ZAAG)
magrant(train1, EMB, 4200)
in time 72.2339
```

The test passes: The model simulation and the RBC simulation "correspond"

# Lessons Learned

- Model-based testing works in principle
  - Test architecture works
  - Model simulation traces can be translated into suitable test scripts
  - Model simulation traces and test logs can be compared
- Defining distances in ERTMS are a challenge
- Siemens test objectives (for this project: test for location specific RBC data) don't require time
  - MA extent and balise groups
  - Static speed profiles

# Section 5

# Continuation and Current Plans

# Plan for Going Forward

Build a "richer" model in CSP||B:

- Scheme plan: Add balises
- Train, RBC: Distances in relation to balise groups
- Messages: To include speed profiles
- Train, RBC: Different modes of operation

verify it, and test from it

# Thank you