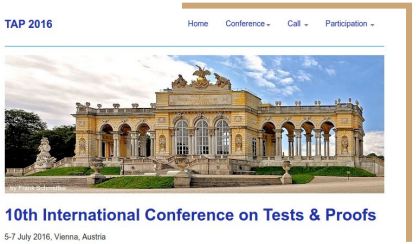


Using Formal Methods for Verification and Validation in Railway

THALES
Together • Safer • Everywhere

Klaus Reichl

Klaus.Reichl@thalesgroup.com
System and Software Architect
Handelskai 92
A-1200 Vienna

Klaus.Reichl@gmail.com
Computer Hacker and Guitar Player
Living in Vienna

https://www.thalesgroup.com/en/worldwide/transportation/rail-public-transport-0
http://www.thalesgroup.com/austria

Outline

- Railway Theory - The Norm
  - Excurse: CENELEC Standard
- A “Real” Model
  - Railway in Action
- Railway Theory - The Standards
  - Excurse: ERTMS, ETCS and Interlocking
- Modelling Formally
  - Interlocking Architecture and its Model
- What comes next
  - Plans for the near Future

Bad Aibling 2016

Bad Aibling 2016 - Facts

- Head to head collision at 100 km/h each
- Trains were equipped with the PZB (*Punktförmige Zugbeeinflussung*) train protection system (= Indusi)
  - Enforces line-side signaling and prevent drivers from accidentally pass signals in case of danger
  - Main signals showing "*stop*" or are out of operation can be passed when subsidiary signals operated by the train dispatcher are set
- Both trains received permission by means of a subsidiary signal due to human error
- 150 people were on the trains, considerably fewer than normal because of Holiday season
  - 12 people died, 85 others were injured

Excurse: CENELEC Norm

CENELEC - a standard for (not only) Railways

CENELEC/TC 9X is responsible for the development of European Standards for Electro Technical Applications related to the Rail Transport Industry of the European Union.

- CENELEC is European (AREMA is the American counterpart)
- CENELEC includes Development Process beside RAMS and Hardware
  - CENELEC EN 50128
    - ***Railway applications - Communications, signalling and processing systems***
  - specialises EN 61508
    - ***Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems***

CENELEC railway standards for signalling

EN 50126-1 :1999: The specification and demonstration of reliability, availability, maintainability and safety (RAMS).

EN 50128:2011: Software for railway control and protection systems. Replaced 2001 version.

EN 50129:2003: Safety-related electronic systems for signalling. Replaced 1998 version.

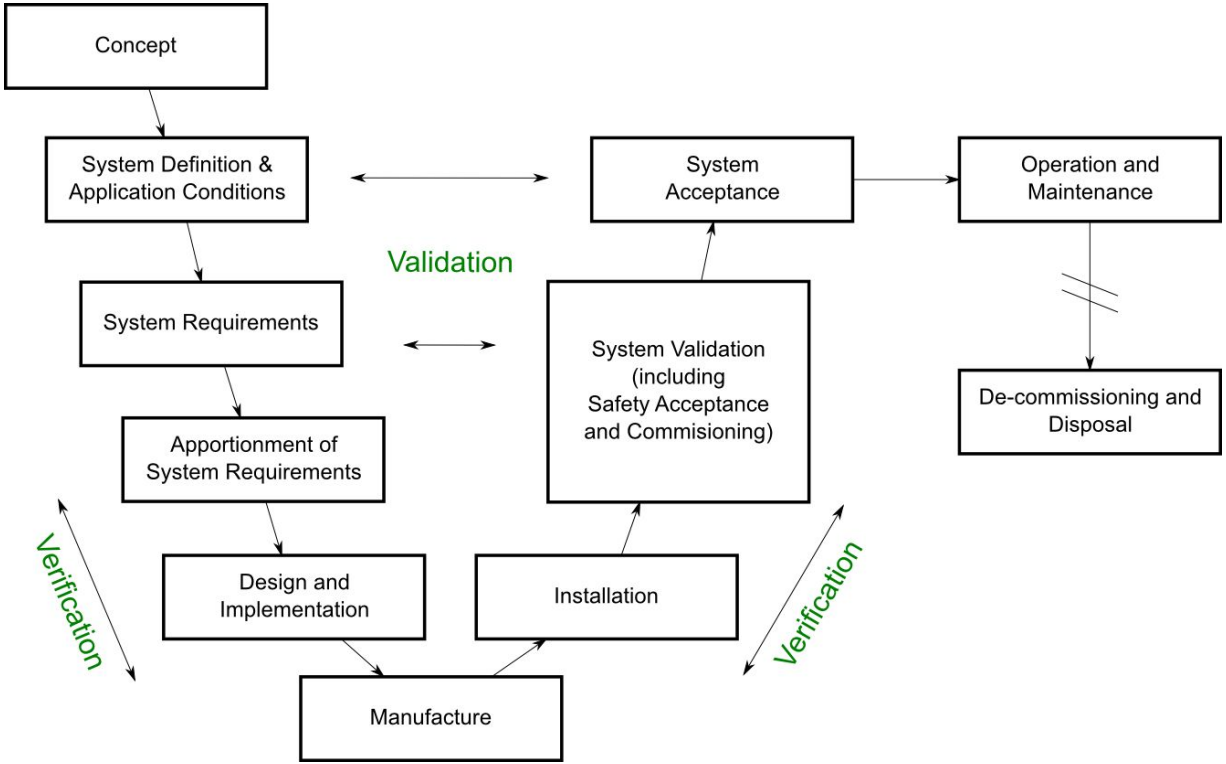
EN 50159:2010: Safety-related communication in transmission systems. Replaced 2001 version.

Safety Integrity Level

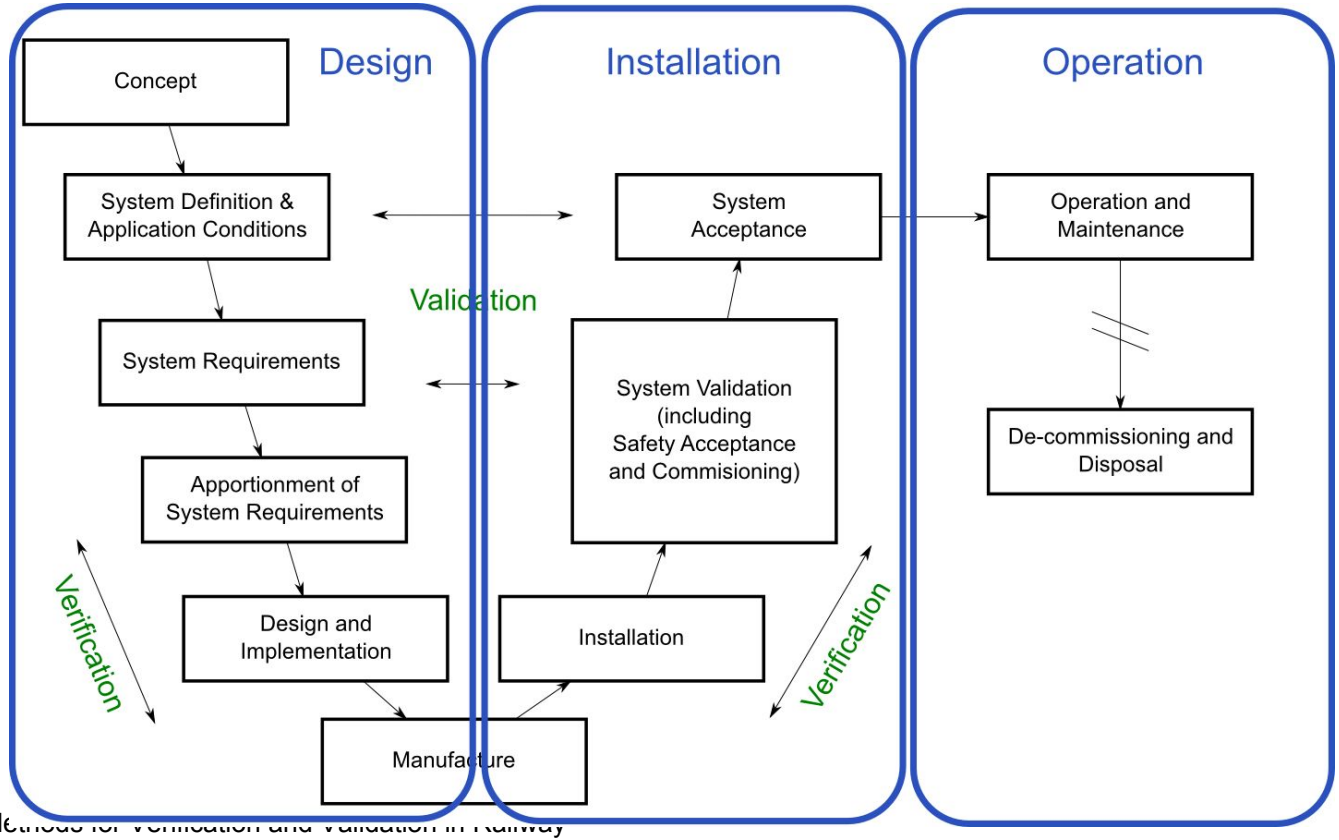
- Concept of Safety Integrity Level (SIL) based on the Tolerable Hazard Rate
- SIL 4 is the most stringent

Tolerable Hazard Rate THR per hour and function	Safety Integrity Level (SIL)
... 10^{-9} <= THR < 10^{-8}	4
10^{-8} <= THR < 10^{-7}	3
10^{-7} <= THR < 10^{-6}	2
10^{-6} <= THR < 10^{-5}	1
10^{-5} <= THR < 10^{-3} ...	0

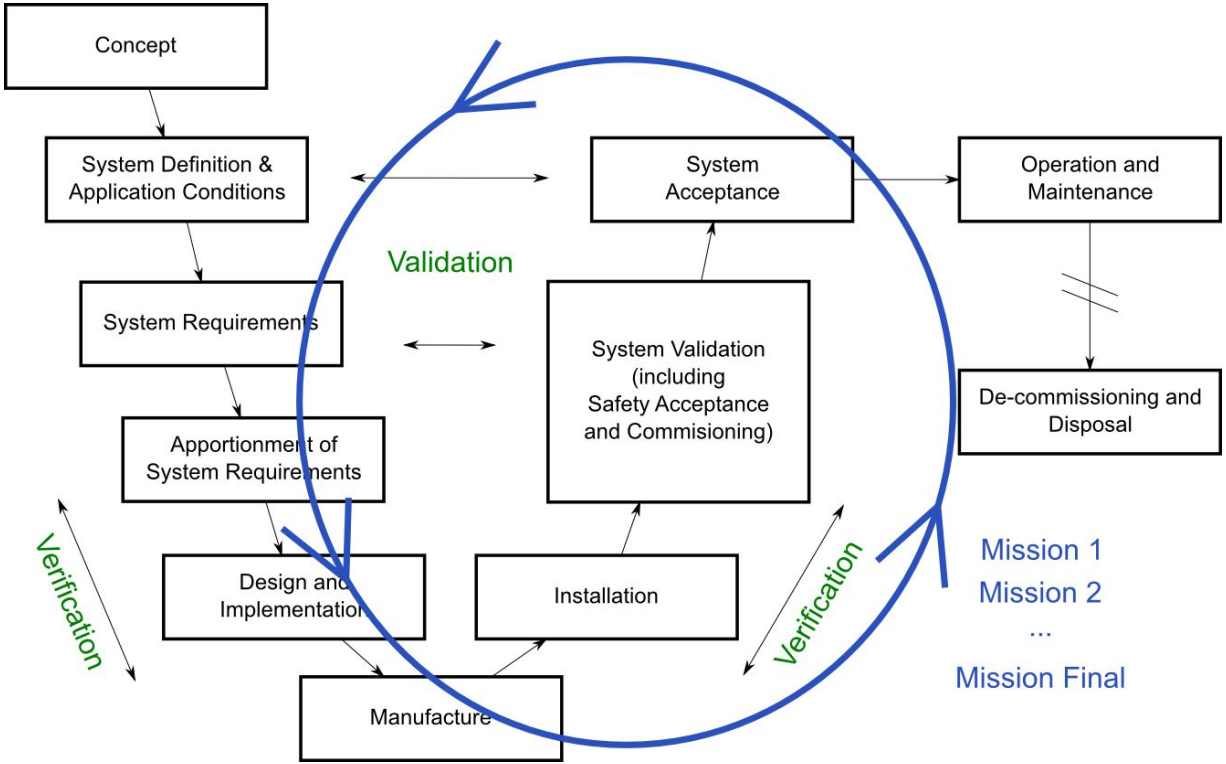
The V-Model in CENELEC



The V-Model in CENELEC - Phases



The V-Model in CENELEC - Missions



CENELEC Recommendations

- Formal Methods are “recommended” for SIL 1/2 and “highly recommended” for SIL 3/4
  - Software Requirement Specification (Table A.2)
  - Software Architecture (Table A.3)
  - Modelling (Table A.17)
- Formal Proof is “recommend” for SIL 1/2 and “highly recommended” for SIL 3/4
  - Verification and Testing (Table A.5)
- Formal Proof of correctness of data is “highly recommended” for SIL 3/4
  - Data Preparation Techniques (Table A.11)

CENELEC on Formal Methods

- apply formal methods to requirements and high-level designs where most of the details are abstracted away
- apply formal methods to only the most critical components
- analyse models of software and hardware where variables are made discrete and ranges drastically reduced
- analyse system models in a hierarchical manner that enables "divide and conquer"
- automate as much of the verification as possible

Described are CSP, CCS, HOL, LOTOS, OBJ, Temporal Logic, VDM, Z, B, Model Checking and Formal Proof

CENELEC Tools Qualification

SOI - System of Interest <= SIL Level Qualification and Assessment
Enabling System <= Tool Qualification, part of the Assessment

- T3 - Tools which produces code or data for SOI
  - Code and Data Generators
- T2 - Tools which are used to verify and validate the SOI
  - Test and Verification Tools
- T1 - Other tools in the development process
  - Editors
- Grey Zone - Build Tools, Statistics, ...

TVR (Tool Validation Report) as framework to Qualification Process

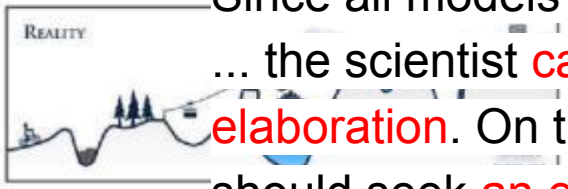
Back to modelling ...

All Models are Wrong

George Box 1976 (https://en.wikipedia.org/wiki/All_models_are_wrong#cite_note-1)

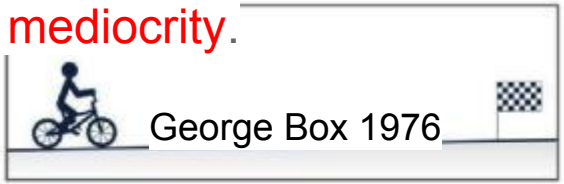
… but Some are Useful

George Box 1978 (https://en.wikipedia.org/wiki/All_models_are_wrong#cite_ref-2)



Since all models are wrong

... the scientist cannot obtain a "correct" one by excessive elaboration. On the contrary following William of Occam he should seek an economical description of natural phenomena. Just as the ability to devise simple but evocative models is the signature of the great scientist so overelaboration and overparameterization is often the mark of mediocrity.



George Box 1976

All Models are Right
… Most are Useless

Thaddeus Tarpey 2012

(http://corescholar.libraries.wright.edu/math/211/)

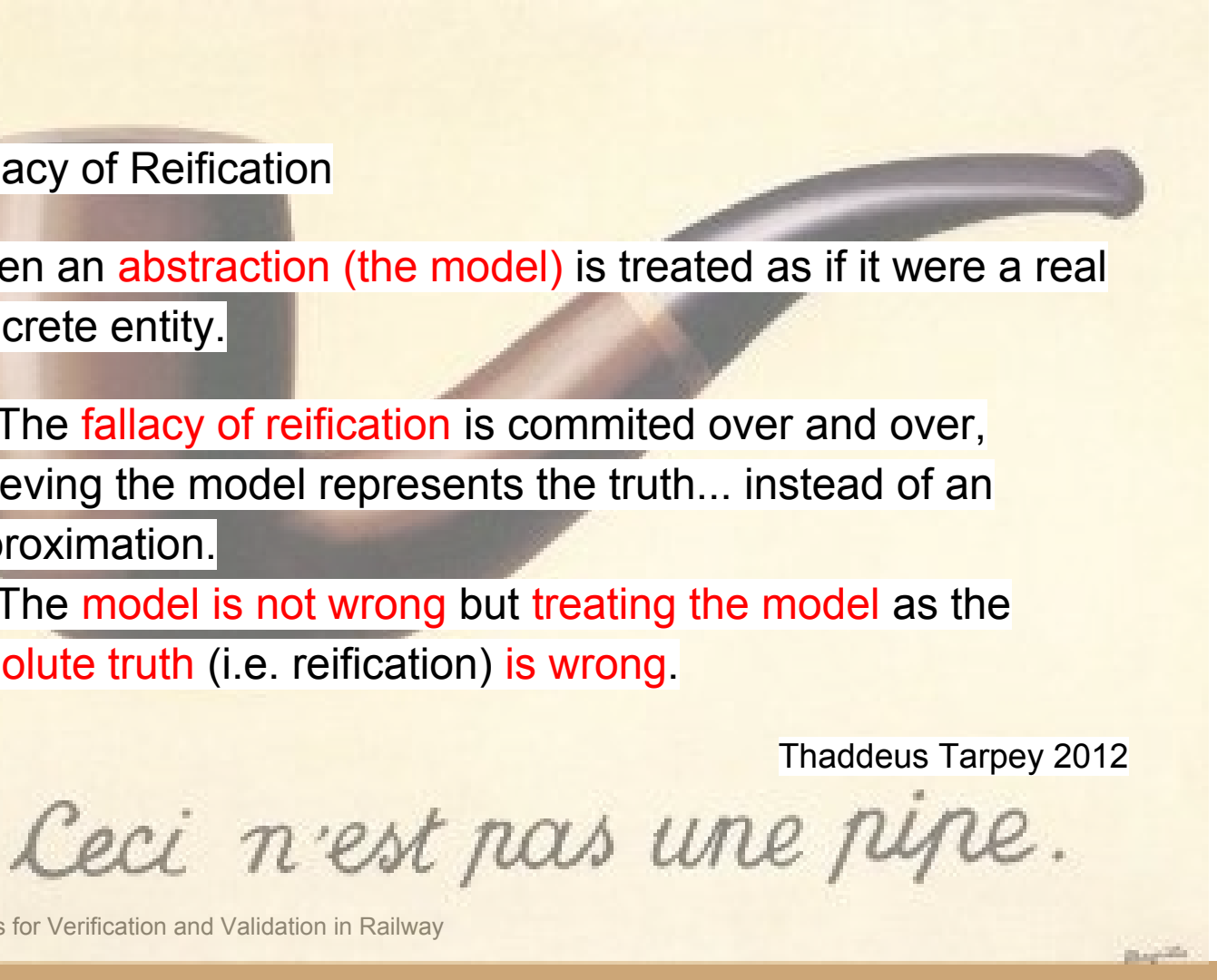
Fallacy of Reification

When an abstraction (the model) is treated as if it were a real concrete entity.

=> The fallacy of reification is commited over and over, believing the model represents the truth... instead of an approximation.

=> The model is not wrong but treating the model as the absolute truth (i.e. reification) is wrong.

Thaddeus Tarpey 2012

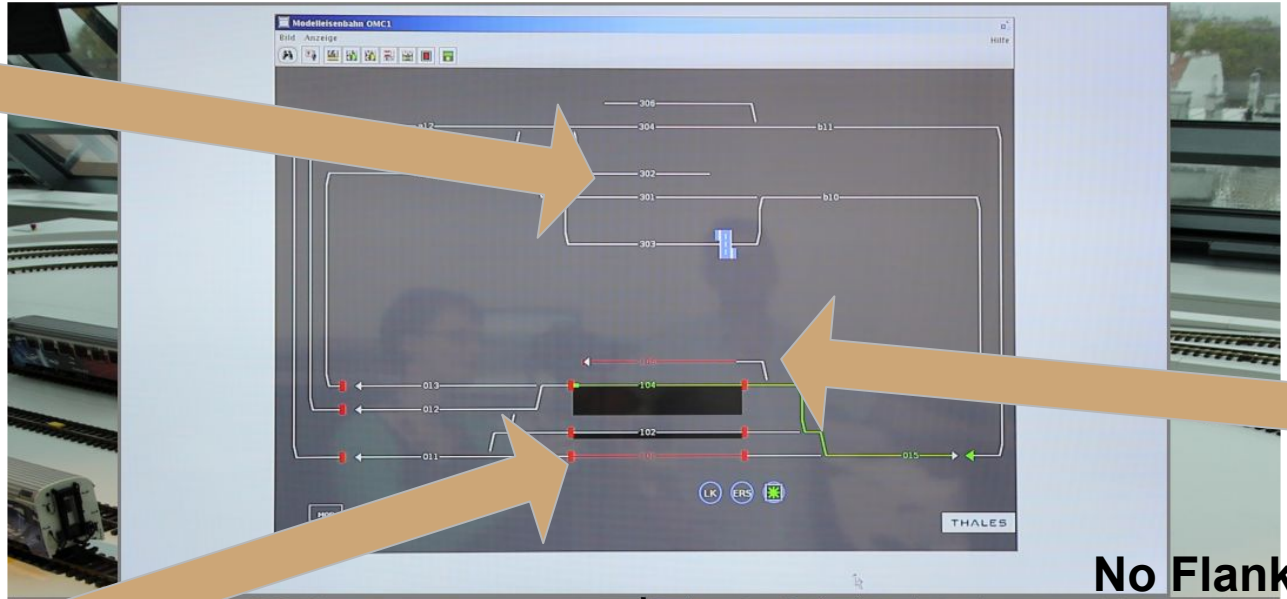


Model of a Classical Interlocking

Questions?

- Is the model right?
- Is the model useful?
- Is the model economically practical?

No Routes?
No Station?



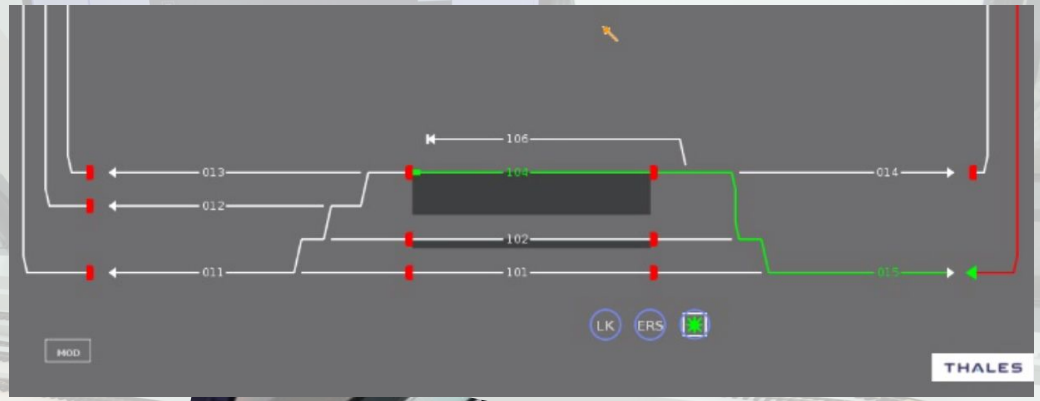
No Flank Protection?

Train Length?
Train Integrity?

Questions?

- Is the model right?
- Is the model useful?
- Is the model economically practical?

Classical Signalling



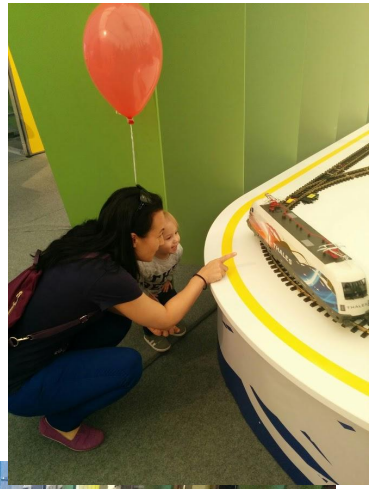
- Conventional Optical Signals
  - Optional Train Protection
- Route Control - pre configured
  - Priority Routes
  - Alternative Routes
- Trains (rather vehicles!) detected by
  - Track Circuit
- Element Control
  - Points and Signals

Questions?

- Is the model right?
- Is the model useful?
- Is the model economically practical?

Is the Model Economically Practical?

- Great Demo for Customers (Little & Big Girls)



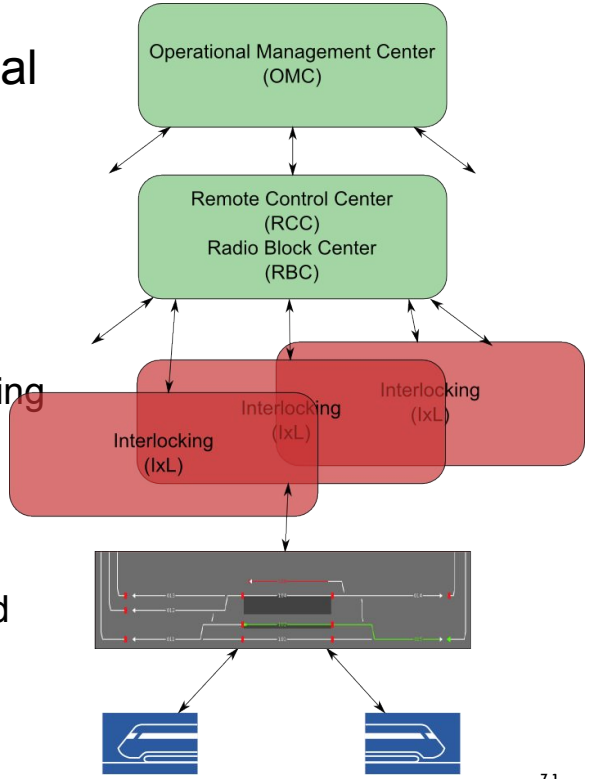
- Way too expensive
  - Maintenance by “Ferro-Sexual” Hobbyists
- Not shareable
- Not movable
  - However a small variant exists ;-)

Excurse: Some words on ERTMS, ETCS and Interlocking

ERTMS - European Rail Traffic Management System

European Union driven replacement to the different national train control and command systems in Europe.

- GSM-R (Global System for Mobiles - Railway)
  - Communication between vehicles and line controllers
- ETCS (European Train Control System)
  - In-cab train control supplementing or replacing trackside signaling
  - Interface to Interlockings
- ETML (European Traffic Management Layer)
  - Operation management level to optimize train movements
  - Augmentation to Interlockings by means of Remote Control and Traffic/Operational Management Centres

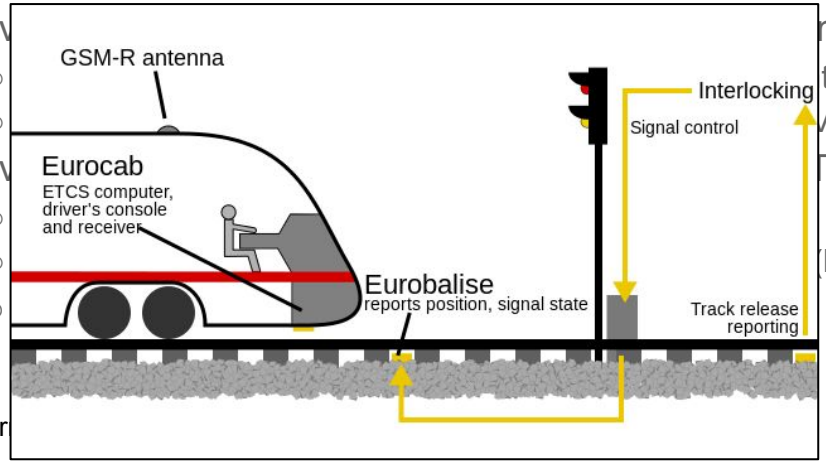


ETCS - European Train Control

- Level 0 - ETCS-fitted vehicles on non-ETCS route
  - Train driver observes trackside
  - Might be limited in speed by the last balises encountered
- Level 1 - Cab signalling which can be superimposed on the existing signalling system
  - Eurobalise radio beacons pick up signal aspects from the trackside signals via signal adapters and telegram coders (STM - Specific Transmission Module)
  - “Infill” Eurobalise or EuroLoop between the distant signal and main signal deliver new proceed aspects
- Level 2 - Cap signalling via digital radio-based system (Radio Block Center - RBC)
  - Movement Authority and other signal aspects are granted via radio
  - Breaking curves implemented by the Onboard Unit (EVC - European Vital Computer)
- Level 3 - From Train Protection to full Radio-Based Train Spacing
  - Trains find their position themselves
  - Fixed blocks (potentially) replaced by Moving Blocks (breaking distance spacing)
  - Reliable Train Integrity (End of Train device)

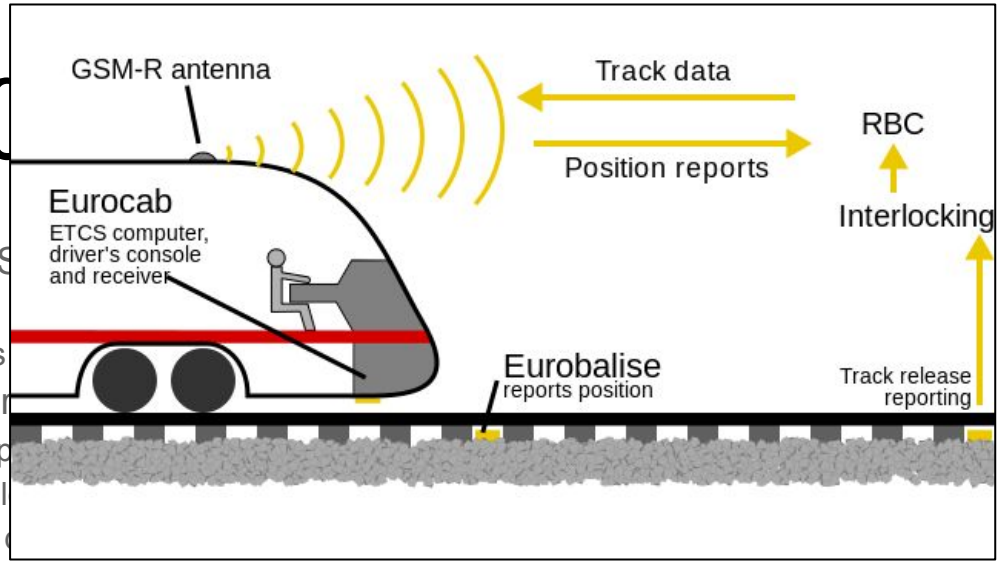
ETCS - European Train Control

- Level 0 - ETCS-fitted vehicles on non-ETCS route
  - Train driver observes trackside
  - Might be limited in speed by the last balises encountered
- Level 1 - Cab signalling which can be superimposed on the existing signaling system
  - Eurobalise radio beacons pick up signal aspects from the trackside signals via signal adapters and telegram coders (STM - Specific Transmission Module)
  - “Infill” Eurobalise or EuroLoop between the distant signal and main signal deliver new proceed aspects
- Lev m (Radio Block Center - RBC)
  - ted via radio
  - /C - European Vital Computer)
- Lev Train Spacing
  - (breaking distance spacing)



Graphic: https://en.wikipedia.org/wiki/European_Train_Control_System

ETCS - European Train C

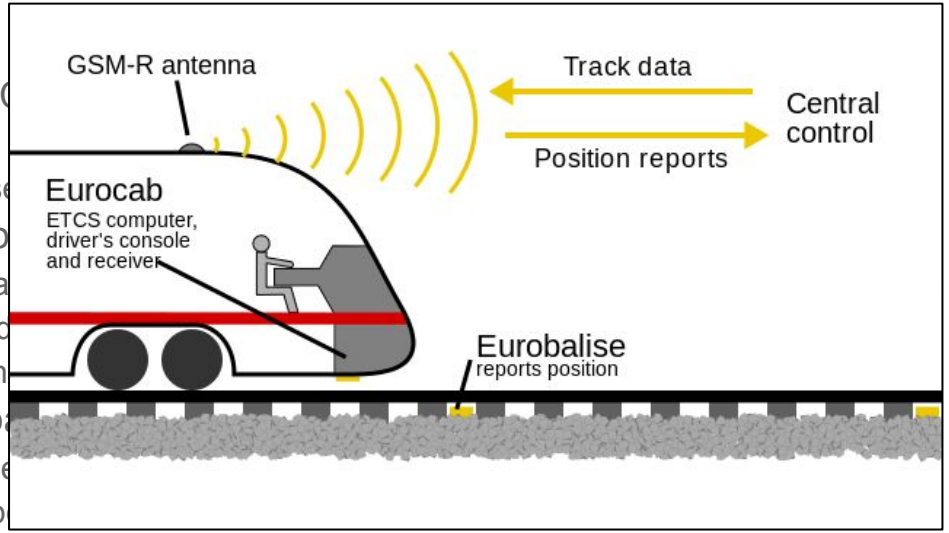


- Level 0 - ETCS-fitted vehicles on non-ETCS
  - Train driver observes trackside
  - Might be limited in speed by the last balises
- Level 1 - Cab signalling which can be super
  - Eurobalise radio beacons pick up signal asp
    coders (STM - Specific Transmission Modul
  - “Infill” Eurobalise or EuroLoop between the
- Level 2 - Cap signalling via digital radio-based system (Radio Block Center - RBC)
  - Movement Authority and other signal aspects are granted via radio
  - Breaking curves implemented by the Onboard Unit (EVC - European Vital Computer)
- Level 3 - From Train Protection to full Radio-Based Train Spacing
  - Trains find their position themselves
  - Fixed blocks (potentially) replaced by Moving Blocks (breaking distance spacing)
  - Reliable Train Integrity (End of Train device)

Graphic: https://en.wikipedia.org/wiki/European_Train_Control_System

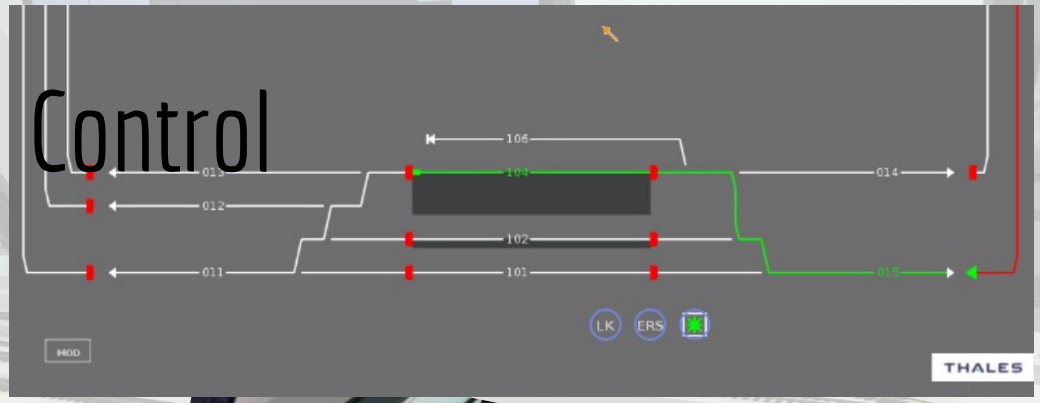
ETCS - European Train Control

- Level 0 - ETCS-fitted vehicles on non-ETC
  - Train driver observes trackside
  - Might be limited in speed by the last balise
- Level 1 - Cab signalling which can be sup
  - Eurobalise radio beacons pick up signal a
    coders (STM - Specific Transmission Moc
  - “Infill” Eurobalise or EuroLoop between th
- Level 2 - Cap signalling via digital radio-ba
  - Movement Authority and other signal aspe
  - Breaking curves implemented by the Onb
- Level 3 - From Train Protection to full Radio-Based Train Spacing
  - Trains find their position themselves
  - Fixed blocks (potentially) replaced by Moving Blocks (breaking distance spacing)
  - Reliable Train Integrity (End of Train device)



Graphic: https://en.wikipedia.org/wiki/European_Train_Control_System

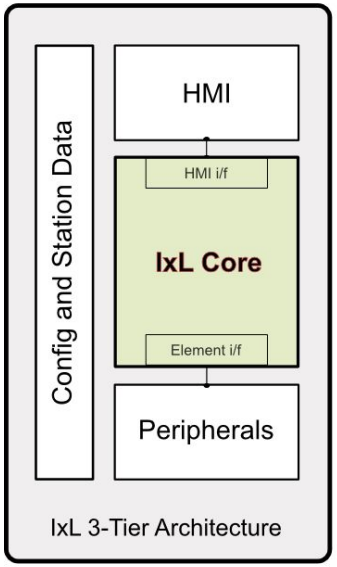
ETCS - European Train Control

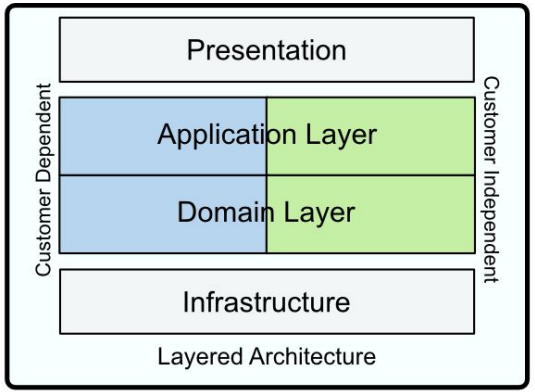


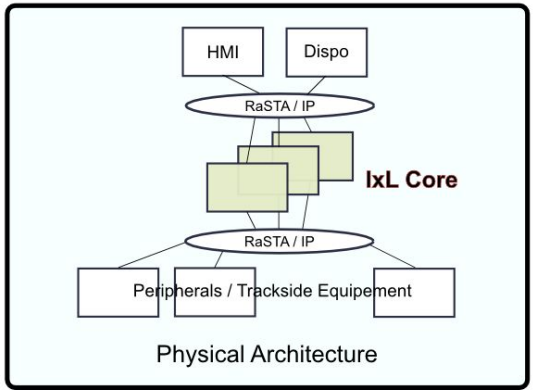
- Virtual Signals - Movement Authority
  - Train Protection
- Route Control - computed
  - In addition to pre configured
- Trains (rather vehicles!) detected by
  - Positioning Logic
- Element Control
  - Points and Level Crossings

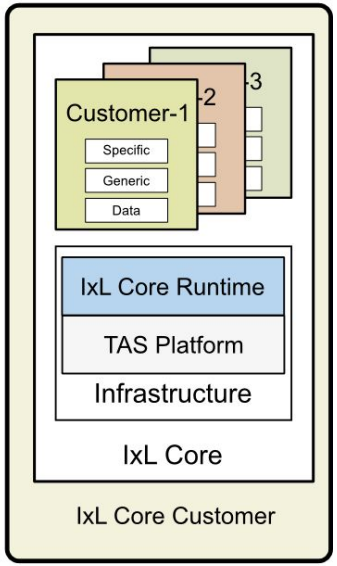
Now really modelling ...

Interlocking Architecture



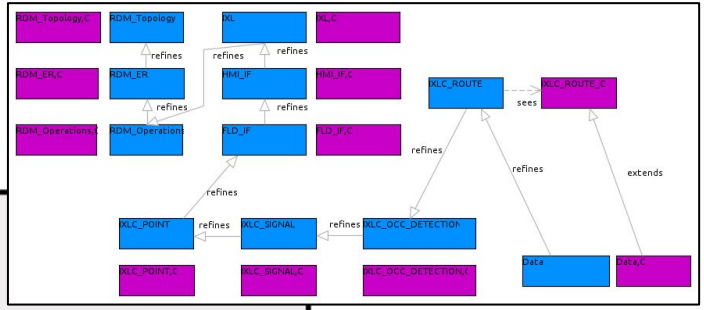


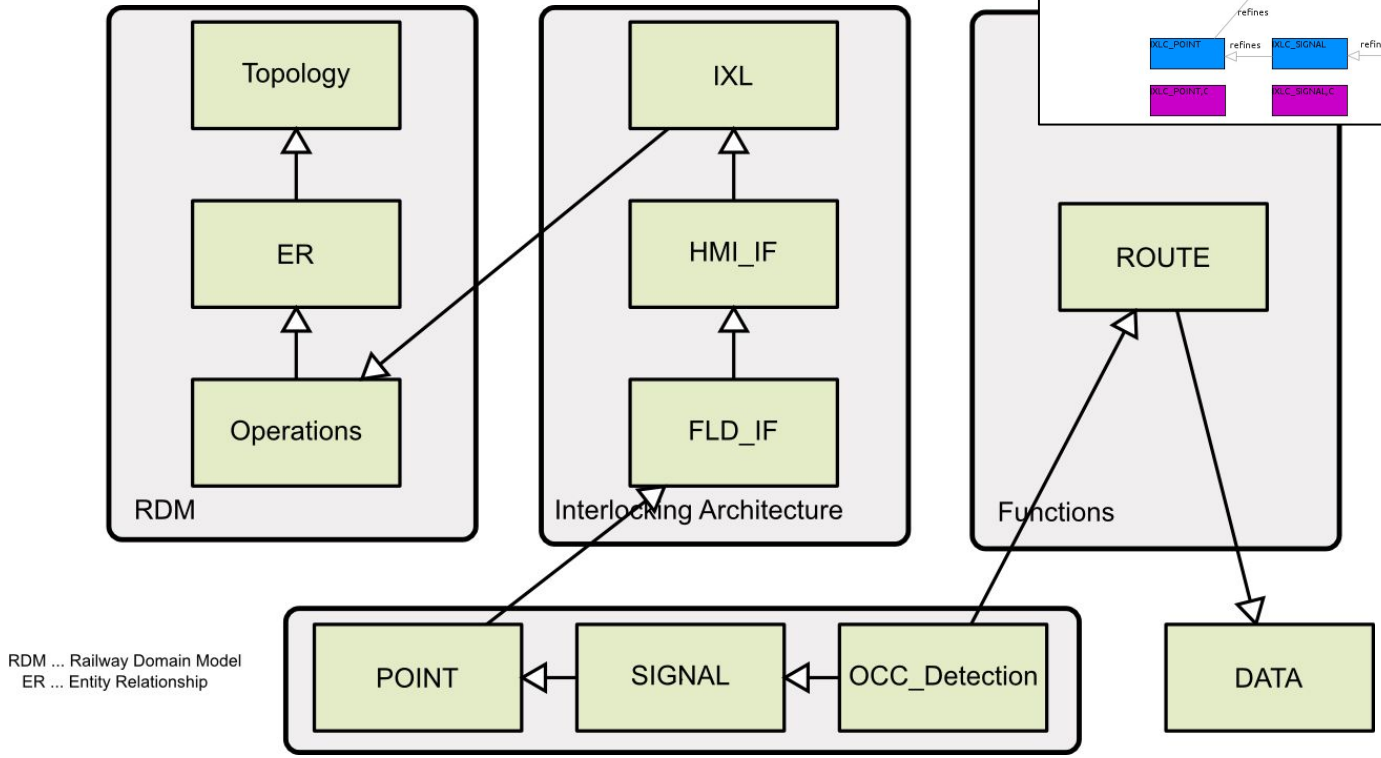




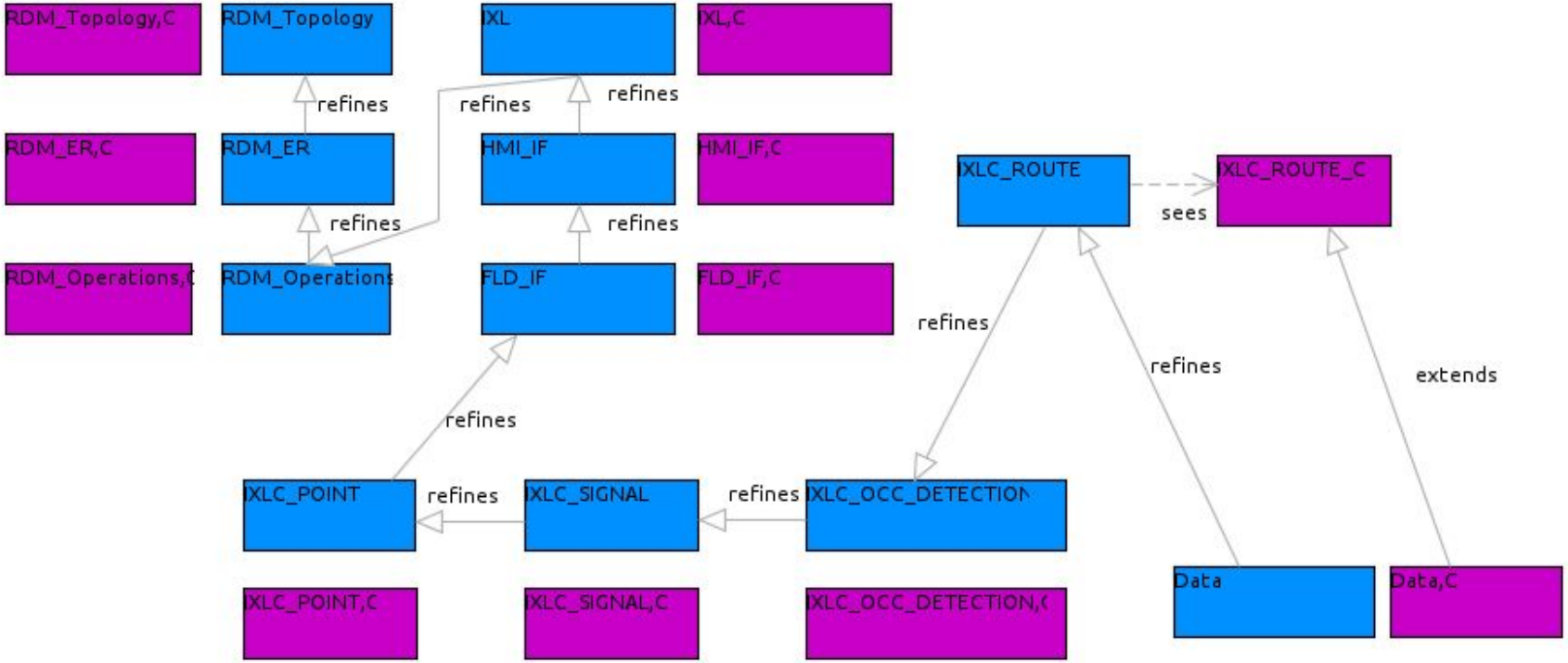
HMI ... Human Machine Interface
Dispo ... Dispositive Peer Systems
- Schedules, Operation Control, ...
RaSTA ... Rail Safe Transport Protocol @ IP

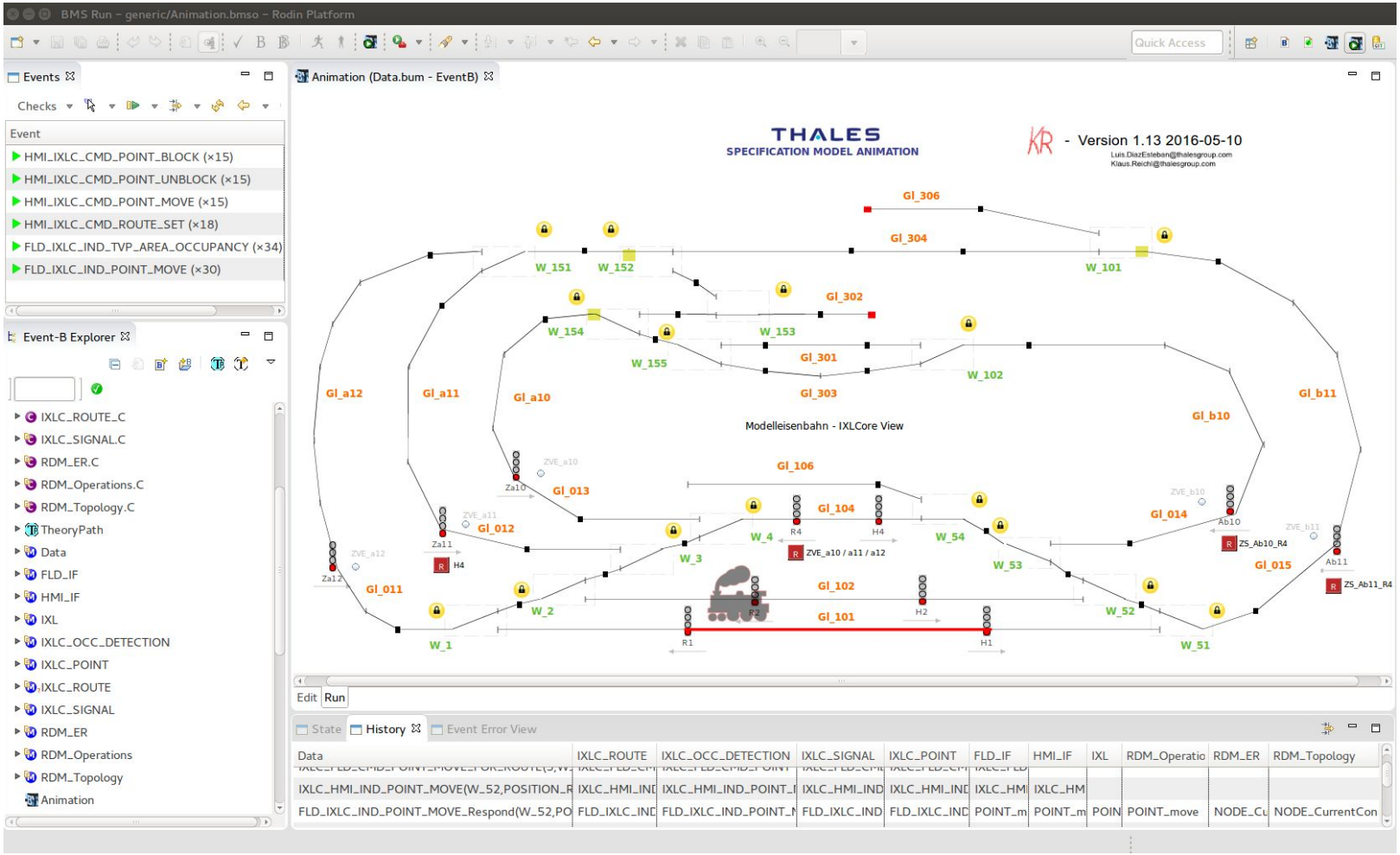
Refinement Strategy

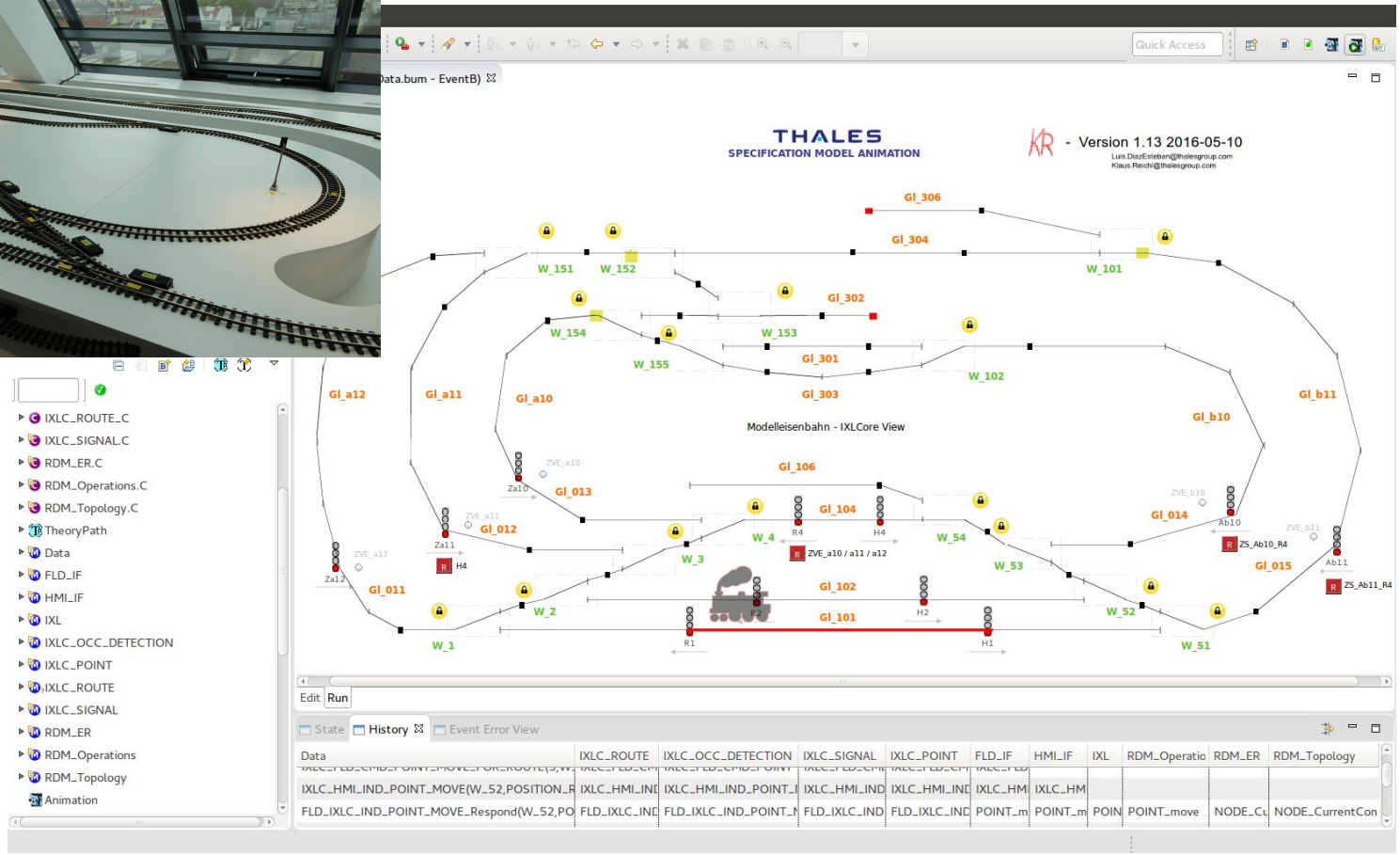




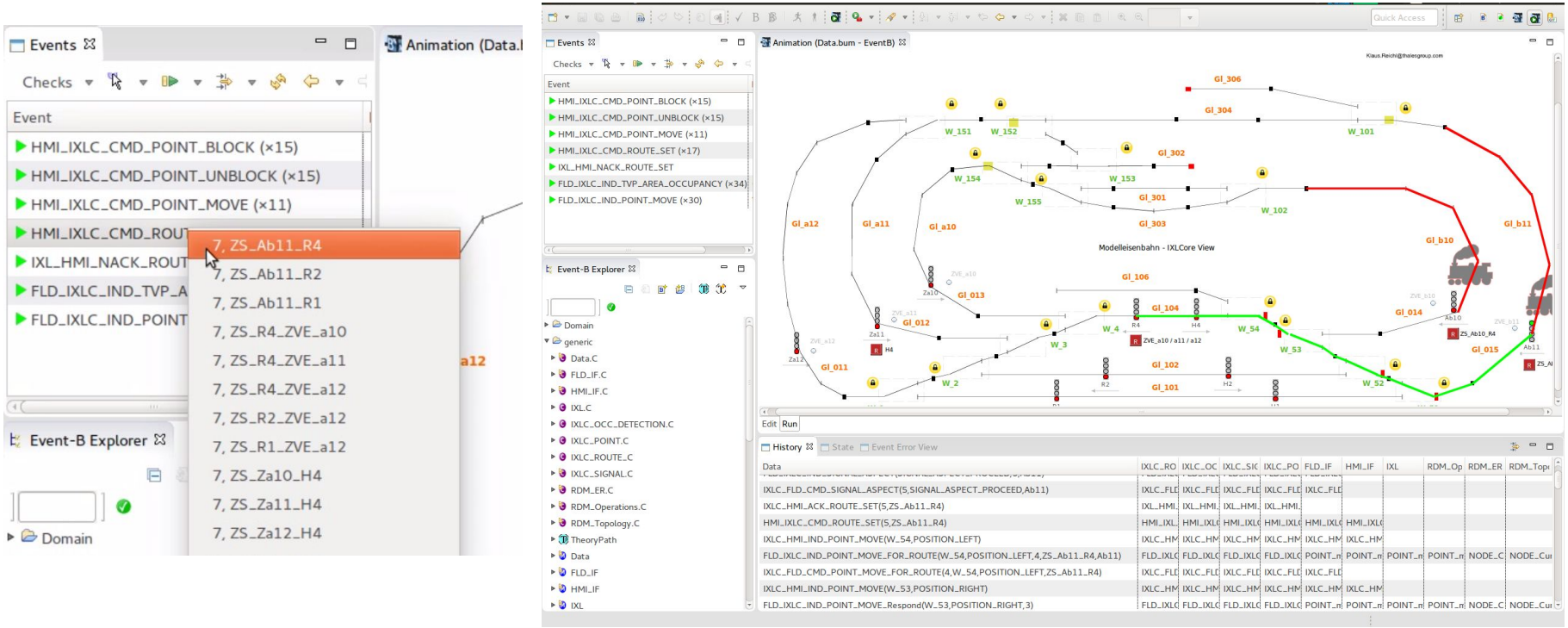
Refinement Strategy



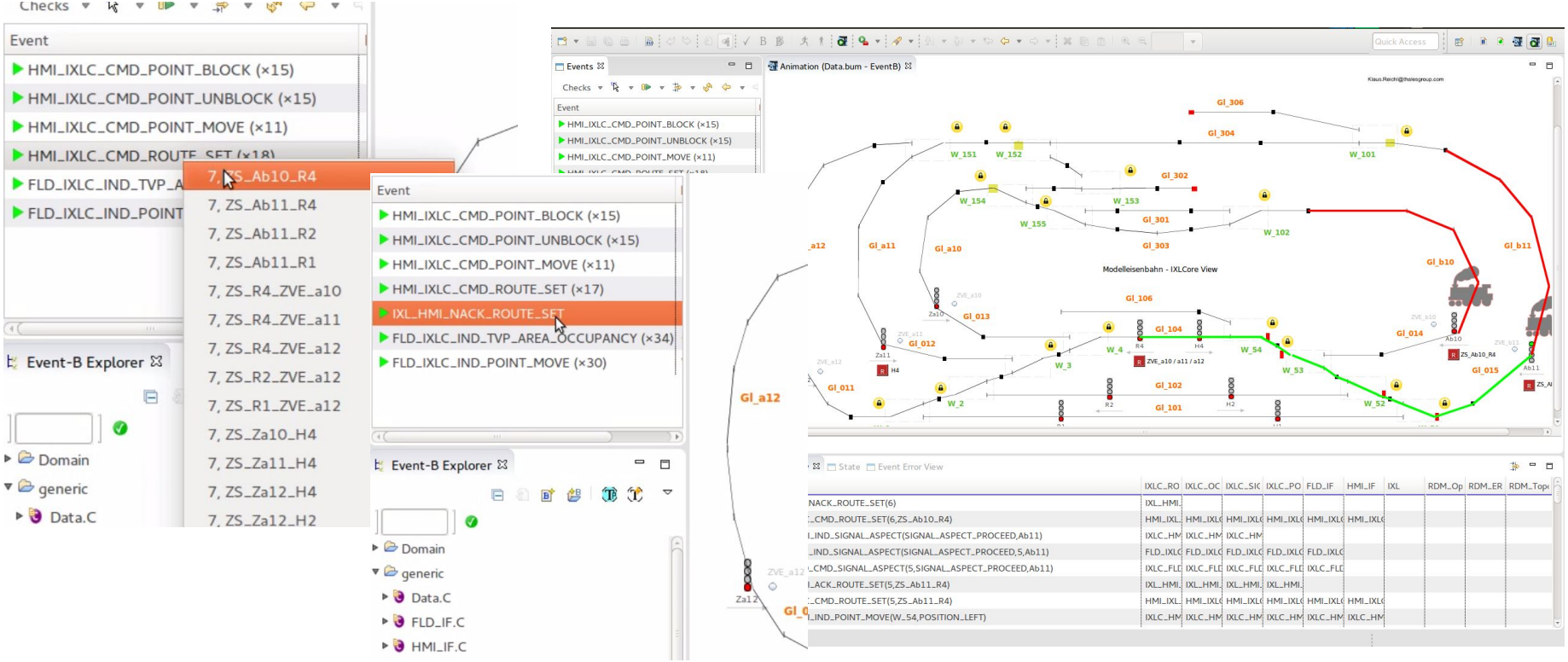

BMS Run – generic/Animation.bmso – Rodin Platform
Quick Access
Events
Checks
Event
HMI_IXLC_CMD_POINT_BLOCK (×15)
HMI_IXLC_CMD_POINT_UNBLOCK (×15)
HMI_IXLC_CMD_POINT_MOVE (×15)
HMI_IXLC_CMD_ROUTE_SET (×18)
FLD_IXLC_IND_TVP_AREA_OCCUPANCY (×34)
FLD_IXLC_IND_POINT_MOVE (×30)
Event-B Explorer
IXLC_ROUTE_C
IXLC_SIGNAL.C
RDM_ER.C
RDM_Operations.C
RDM_Topology.C
TheoryPath
Data
FLD_IF
HMI_IF
IXL
IXLC_OCC_DETECTION
IXLC_POINT
IXLC_ROUTE
IXLC_SIGNAL
RDM_ER
RDM_Operations
RDM_Topology
Animation
Animation (Data.bum - EventB)
THALES
SPECIFICATION MODEL ANIMATION
- Version 1.13 2016-05-10
Luis.DiazEsteban@thalesgroup.com
Klaus.Reichl@thalesgroup.com
Modelleisenbahn - IXLCore View
Gl_306
Gl_304
Gl_302
Gl_301
Gl_303
Gl_106
Gl_104
Gl_102
Gl_101
Gl_013
Gl_012
Gl_011
Gl_014
Gl_015
Gl_a12
Gl_a11
Gl_a10
Gl_b11
Gl_b10
W_151
W_152
W_101
W_154
W_153
W_155
W_102
W_4
W_3
W_2
W_1
W_54
W_53
W_52
W_51
Za10
Za11
Za12
Ab10
Ab11
ZS_Ab10_R4
ZS_Ab11_R4
ZVE_a10 / a11 / a12
H4
R4
H2
R1
R2
H1
Edit
Run
State
History
Event Error View
Data
IXLC_ROUTE
IXLC_OCC_DETECTION
IXLC_SIGNAL
IXLC_POINT
FLD_IF
HMI_IF
IXL
RDM_Operatio
RDM_ER
RDM_Topology
IXLC_HMI_IND_POINT_MOVE(W_52,POSITION_R
FLD_IXLC_IND_POINT_MOVE_Respond(W_52,PO
POINT_move
NODE_CurrentCon


Data.bum - EventB)
THALES
SPECIFICATION MODEL ANIMATION
- Version 1.13 2016-05-10
Modelleisenbahn - IXLCore View
Gl_306
Gl_304
Gl_302
Gl_301
Gl_303
Gl_106
Gl_013
Gl_012
Gl_011
Gl_104
Gl_102
Gl_101
Gl_014
Gl_015
W_151
W_152
W_101
W_154
W_153
W_155
W_102
W_4
W_3
W_2
W_1
W_54
W_53
W_52
W_51
Gl_a12
Gl_a11
Gl_a10
Gl_b11
Gl_b10
IXLC_ROUTE_C
IXLC_SIGNAL_C
RDM_ER_C
RDM_Operations_C
RDM_Topology_C
TheoryPath
Data
FLD_IF
HMI_IF
IXL
IXLC_OCC_DETECTION
IXLC_POINT
IXLC_ROUTE
IXLC_SIGNAL
RDM_ER
RDM_Operations
RDM_Topology
Animation
Edit
Run
State
History
Event Error View
Data
IXLC_ROUTE
IXLC_OCC_DETECTION
IXLC_SIGNAL
IXLC_POINT
FLD_IF
HMI_IF
IXL
RDM_Operatio
RDM_ER
RDM_Topology
IXLC_HMI_IND_POINT_MOVE(W_52,POSITION_R
FLD_IXLC_IND_POINT_MOVE_Respond(W_52,PO
POINT_move
NODE_CurrentCon

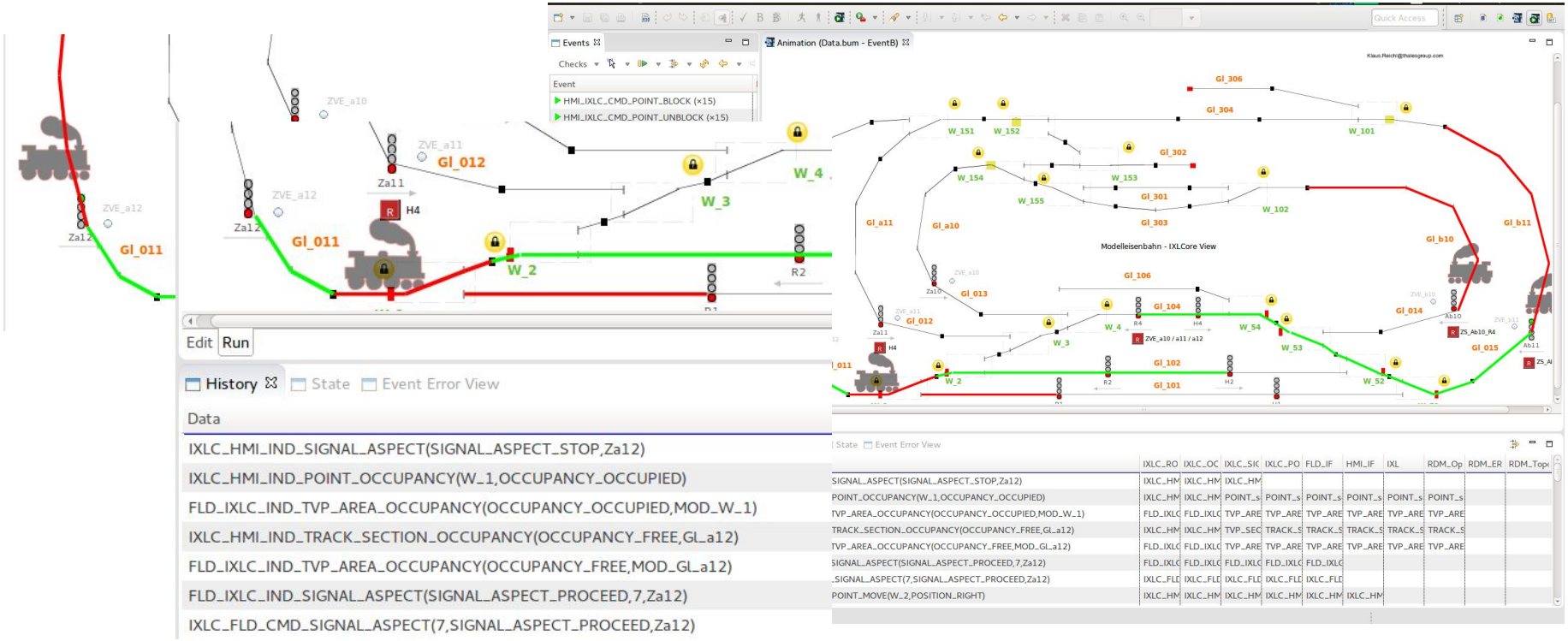
Establishing a Route



Establishing a Route (Locked by Another)

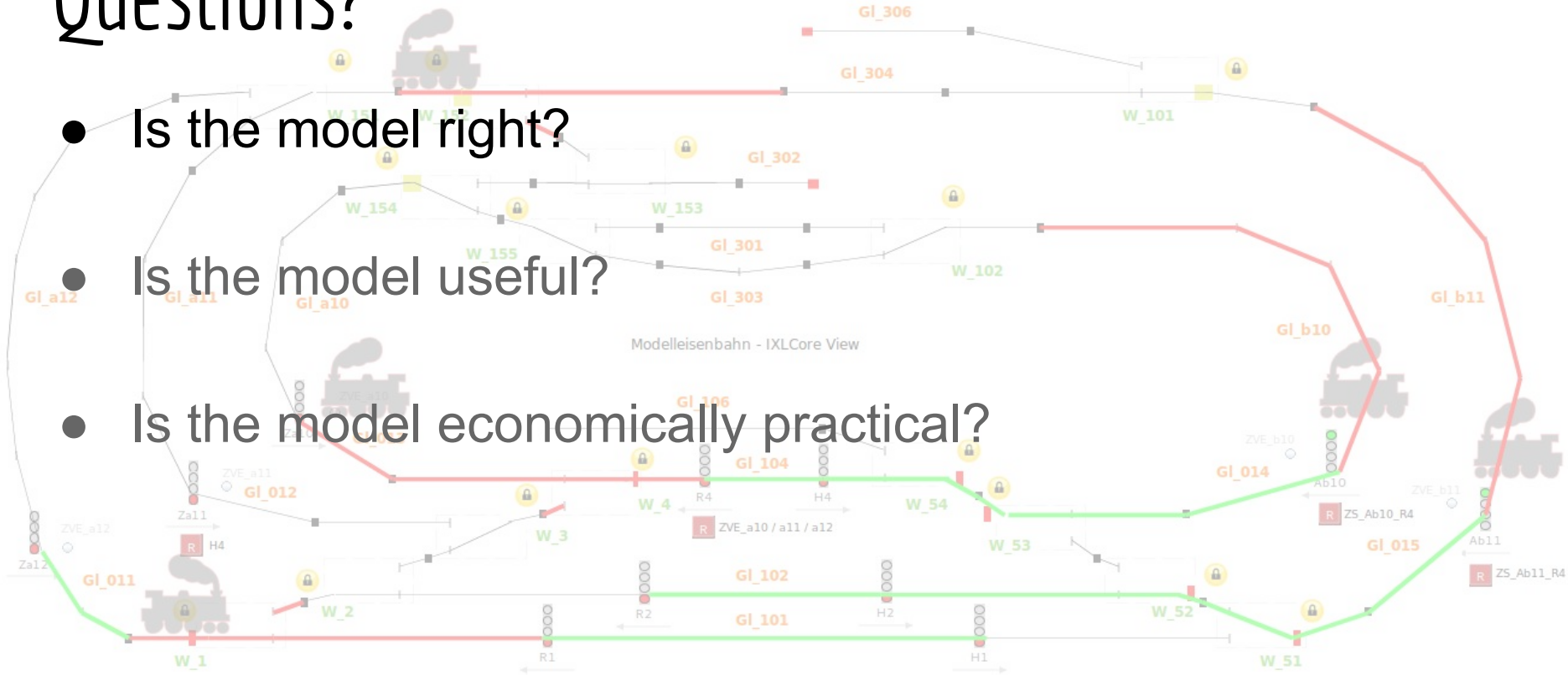


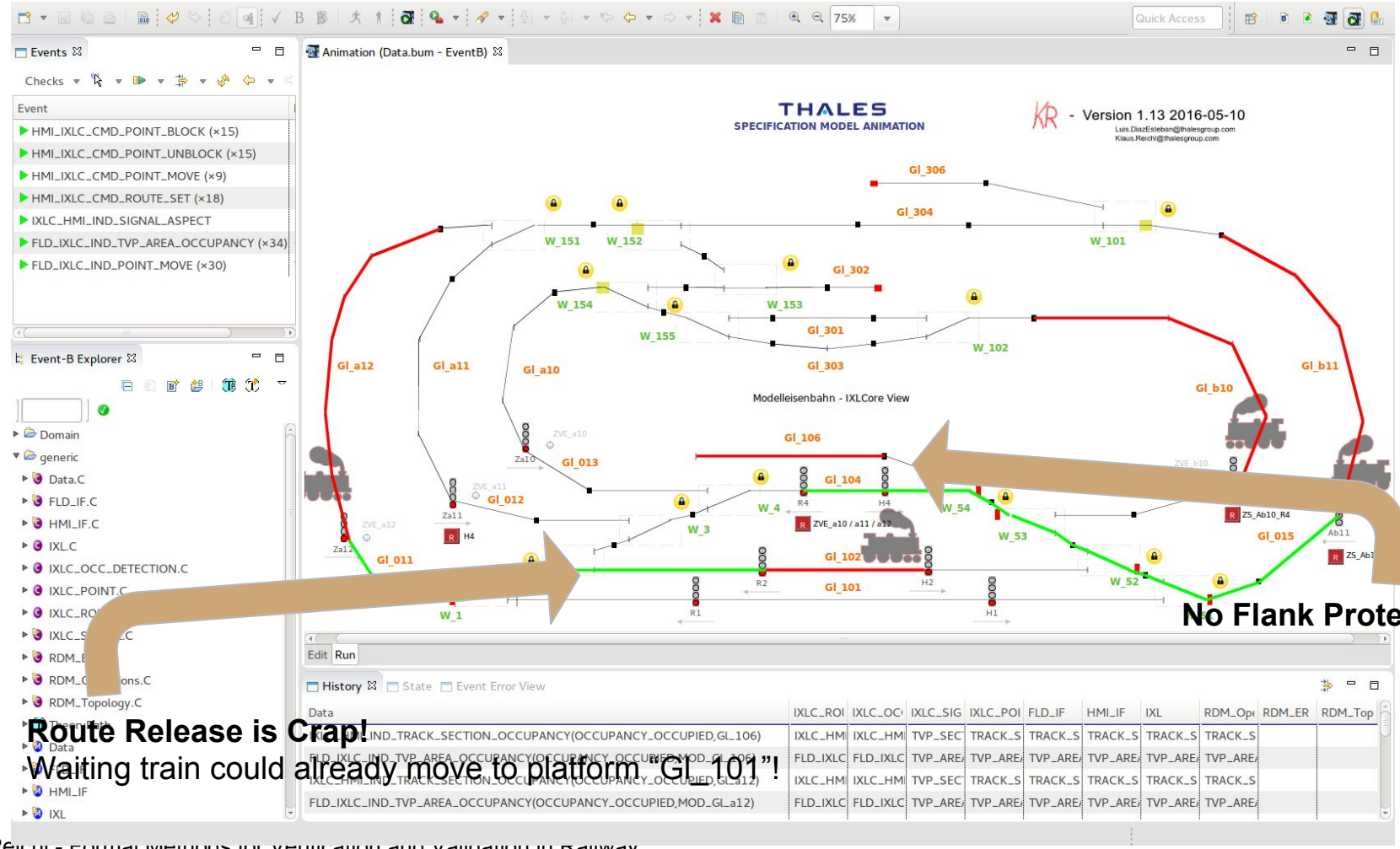
Closing a Signal after Track Occupancy



Questions?

- Is the model right?
- Is the model useful?
- Is the model economically practical?



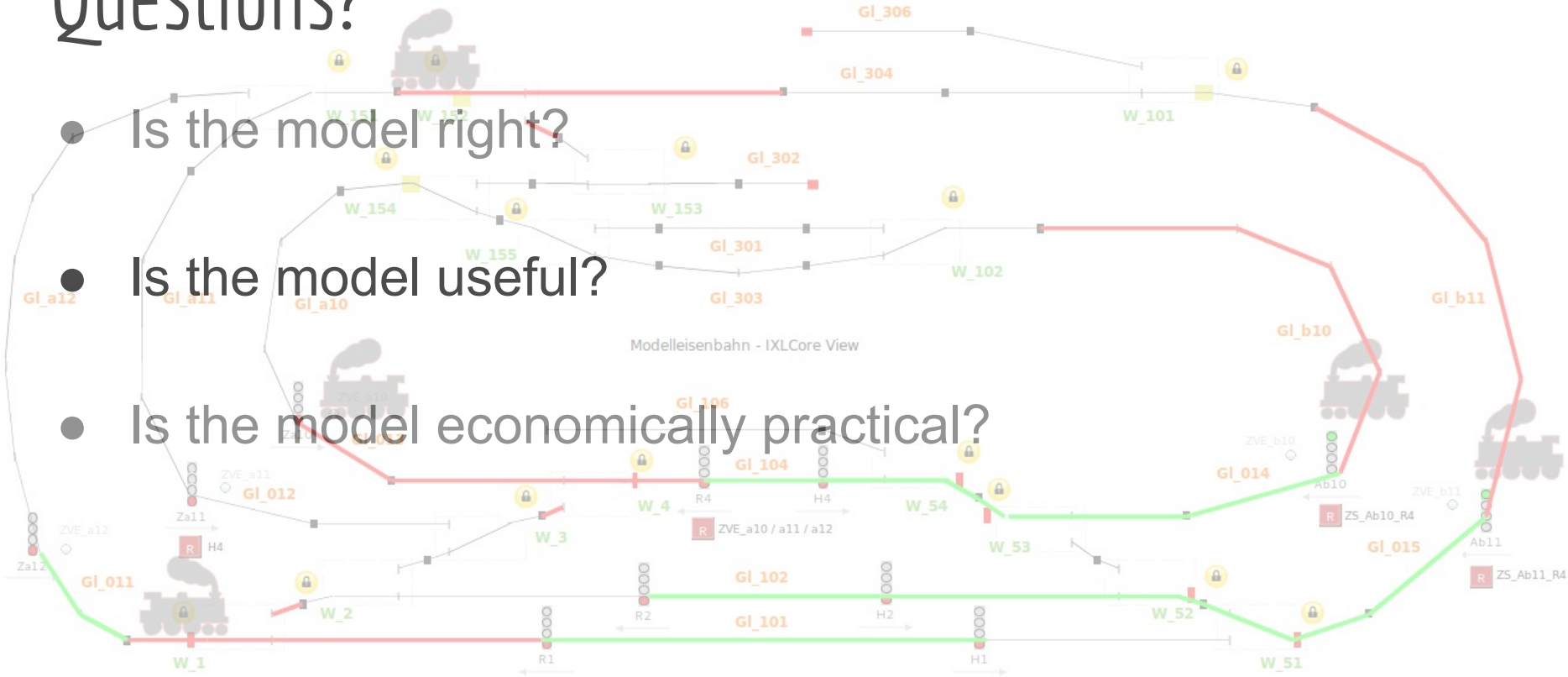


No Flank Protection?

Route Release is Crap!
Waiting train could already move to platform "Gl_101"!

Questions?

- Is the model right?
- Is the model useful?
- Is the model economically practical?

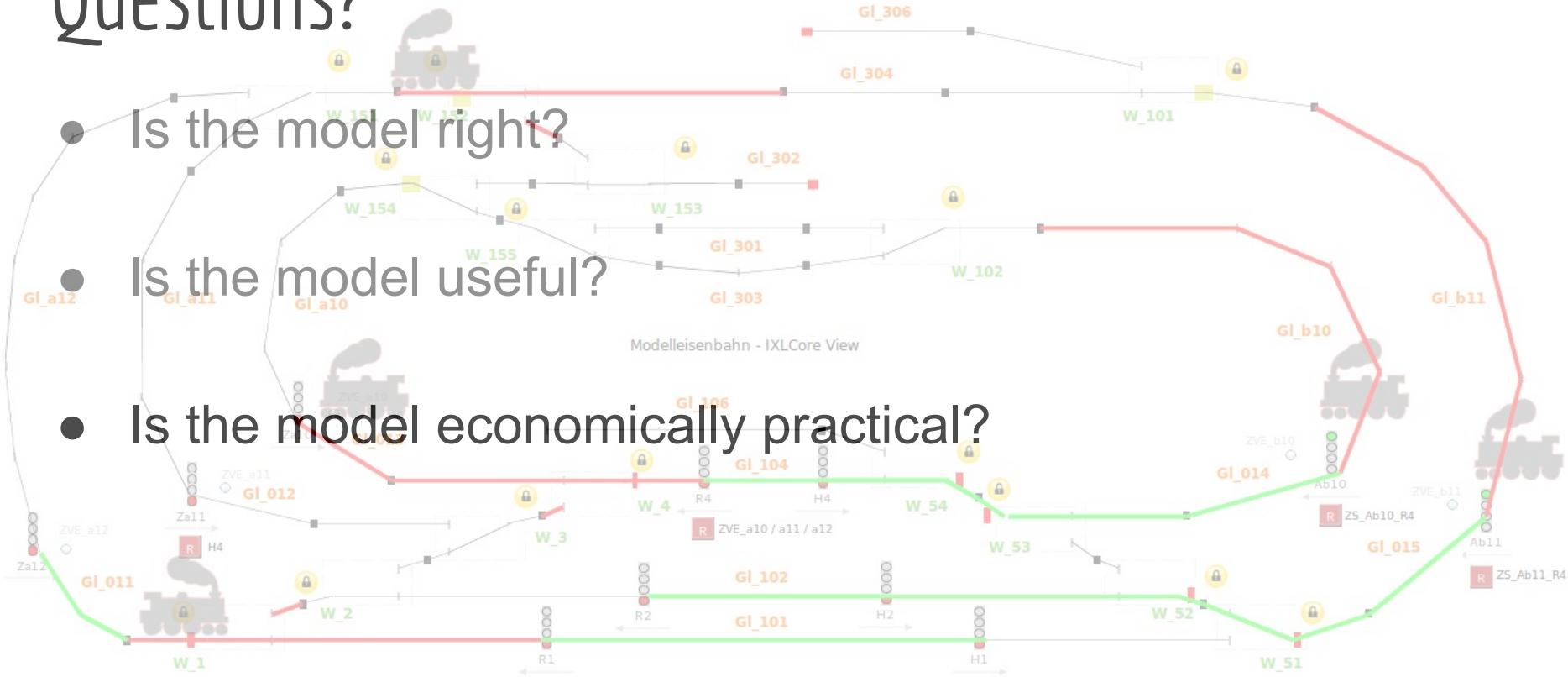


Is the model useful?

- Allows to formulate Business Rules
  - How to safely drive trains through the network
  - What can we optimize
- Domain Specific Language works well in Rodin Theories
- Hazards can be translated to Guards and Invariants
  - What are the constraints
  - Which situations need discussion
- Data Models can be used for Verification and Validation
  - Axioms on Data
  - Scenarios on given Topological and Geometric Situations

Questions?

- Is the model right?
- Is the model useful?
- Is the model economically practical?

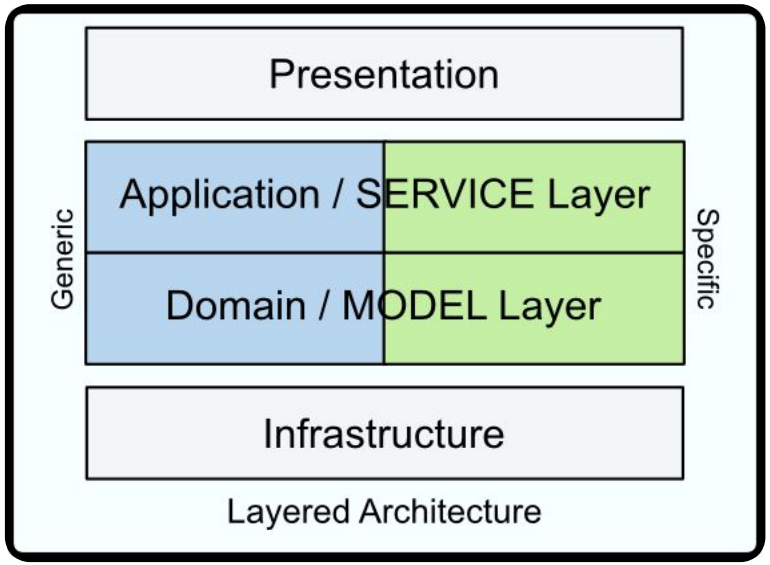


Is the model economically practical?

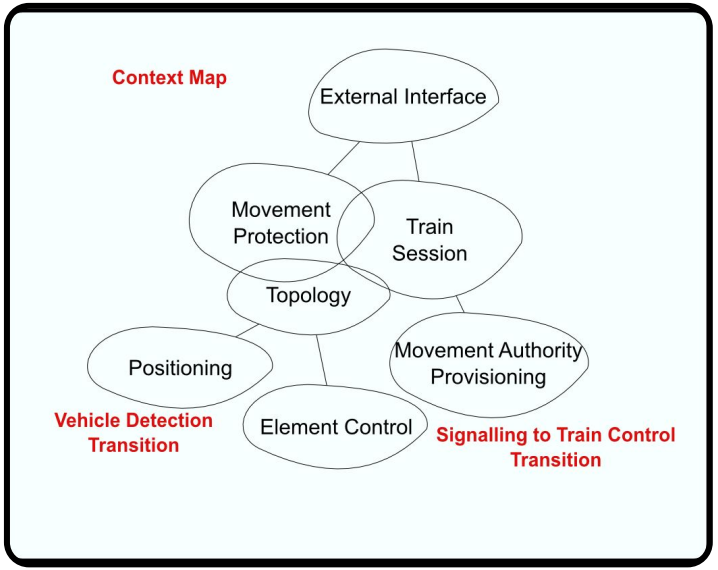
- Adding new Control Operations is painful
  - This should be done using an Adaptor
  - Protocol to HMI adds Incidental Complexity
  - ACK/NAK does not bring any value
- Business Domain and Architecture is Mixed
  - Should be strictly decoupled for Maintainability
  - Model is good for different Topologies, not for additional Functionality
- Adding new Features need Elaboration
  - Unclear how to properly do Feature Driven Development
  - How to evolve the Model

What we like to do about it ...

Layered Architecture - Context Map



Architecture Principle



Domain Model

The Plan ...

- Rework Interlocking Model according to DDD Principles
  - Use Domain Language as already defined
  - Adopt towards “railML.org” Standards (railTOPOMODEL - http://www.railtopomodel.org/en/)
- Put an Example Model into Open Source
  - “Railground” Project on github as playground (https://github.com/klar42/railground)
  - Explains modelling principles for Railway Models
  - Interested community can participate
- Integrate Verification and Validation Strategies with Model-Driven Architecture and Design
  - ECSEL EU ENABLE-S3 Project kicked-off June 2016
  - Work on Verification and Validation
  - Continuous Integration (CI) on the models as major step forward

Summary

Overview of (a bit) of the Railway Theory

- Norm, Standards

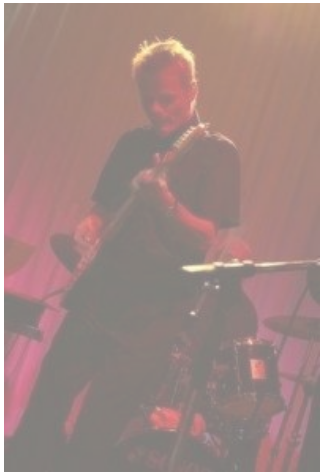
Feeling on how Railway Applications are Modelled

- Railway Domain Core, Generic Application, Station Data
- Distributed Problem

Where is it driving at

- Model Integration with various Stakeholders from various Domains

Klaus.Reichl@gmail.com
Computer Hacker and Guitar Player
Living in Vienna



Thank You!
Questions?

Klaus.Reichl@thalesgroup.com
System and Software Architect
Handelskai 92
A-1200 Vienna

https://www.thalesgroup.com/en/worldwide/transportation/rail-public-transport-0

References

CENELEC - https://www.cenelec.eu/

ERTMS - http://www.ertms.net/

ETCS - http://uic.org/ETCS

railML - https://www.railml.org/en/
- http://www.railtopomodel.org/en/

DDD - http://dddeurope.com/2016/#top
- https://groups.google.com/forum/#!forum/dddcqrs

Thales - https://www.thalesgroup.com/en

Thales Transportation
- https://www.thalesgroup.com/en/worldwide/transportation/ground-transportation

Polarsys Capella System Modelling
- https://www.polarsys.org/capella/

“railground” Playground Event-B Model
- https://github.com/klar42/railground

License