

Using Formal Methods for Verification and Validation in Railway



Klaus.Reichl@gmail.com

Computer Hacker and Guitar Player
Living in Vienna



Klaus.Reichl@thalesgroup.com

System and Software Architect
Handelskai 92
A-1200 Vienna



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

<http://www.thalesgroup.com/austria>

Outline

- Railway Theory - The Norm
 - Excuse: CENELEC Standard
- A “Real” Model
 - Railway in Action
- Railway Theory - The Standards
 - Excuse: 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

Excuse: 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.

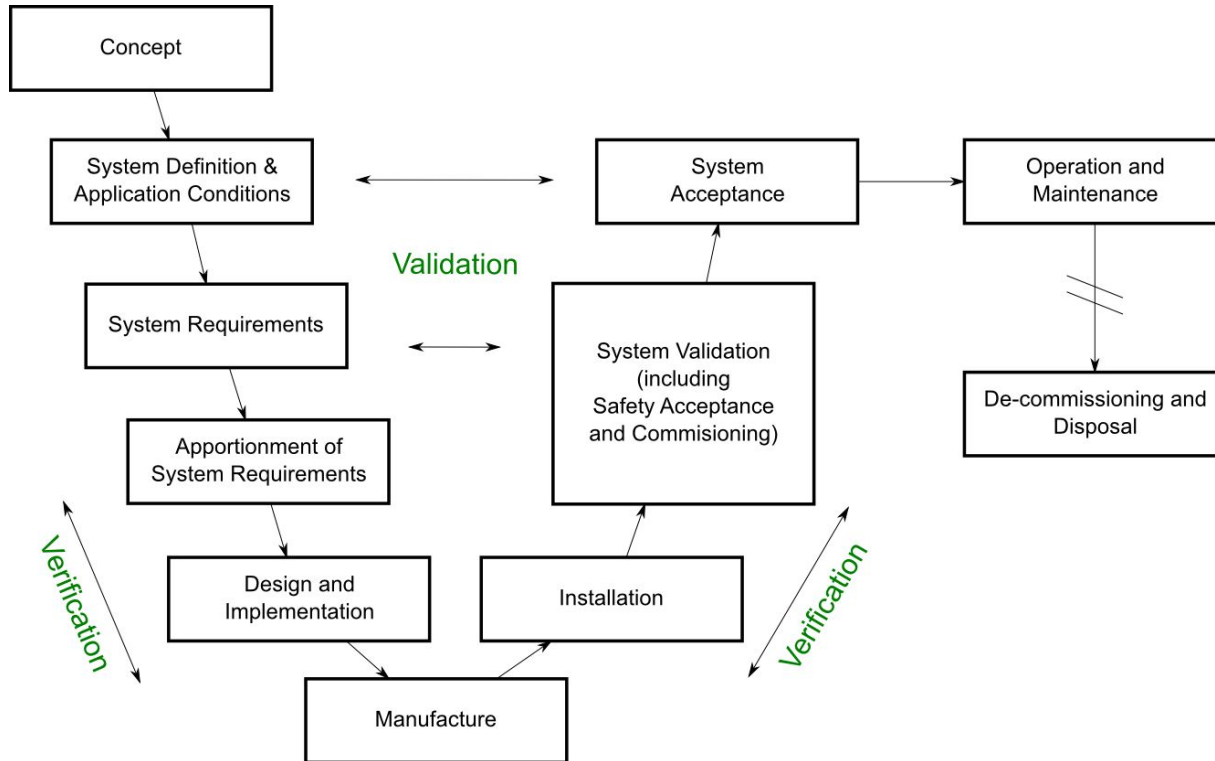
EN 50159:2010: Safety-related **communication in transmission systems**. Replaced 2001 version.

Safety Integrity Level

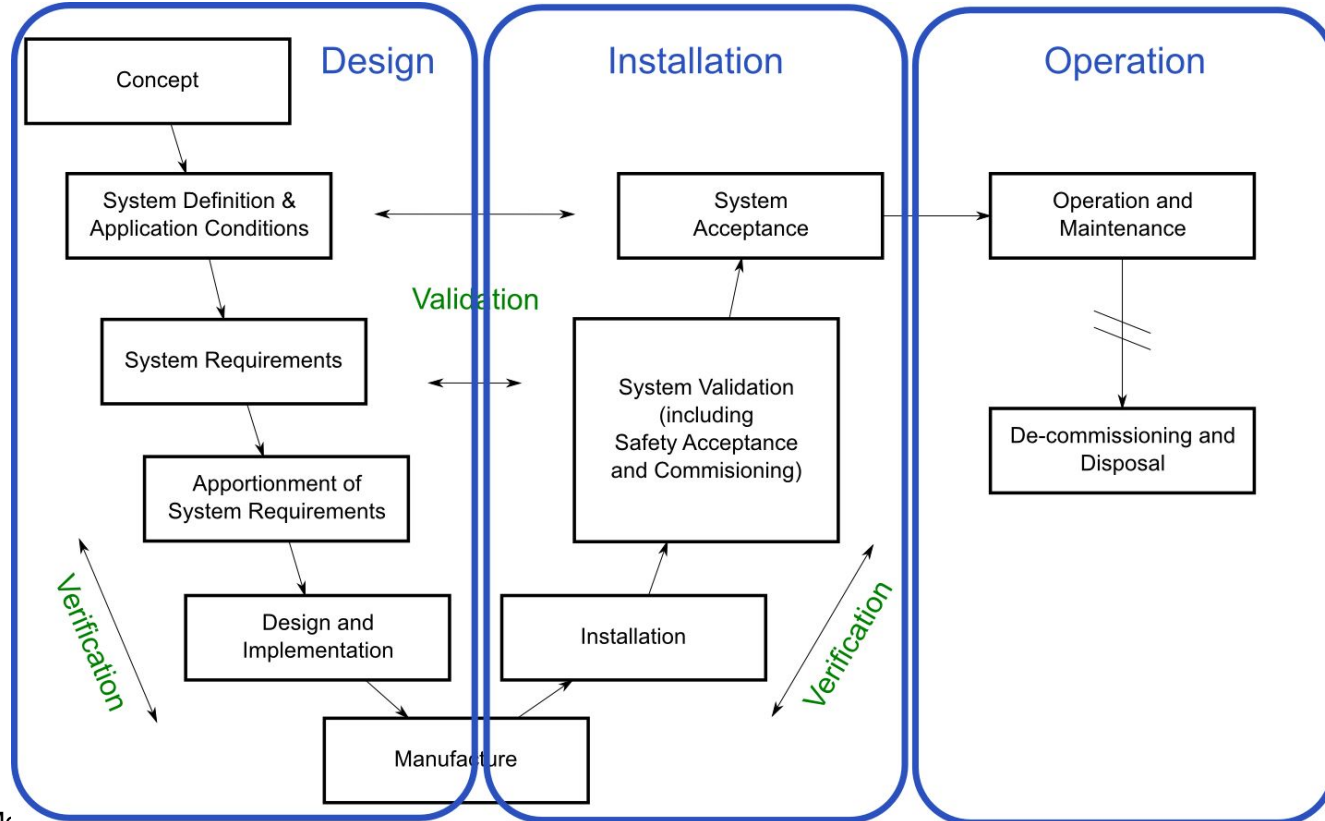
- Concept of **Safety Integrity Level (SIL)** based on the **Tolerable Hazard Rate**
- **SIL 4** is the **most stringent**

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

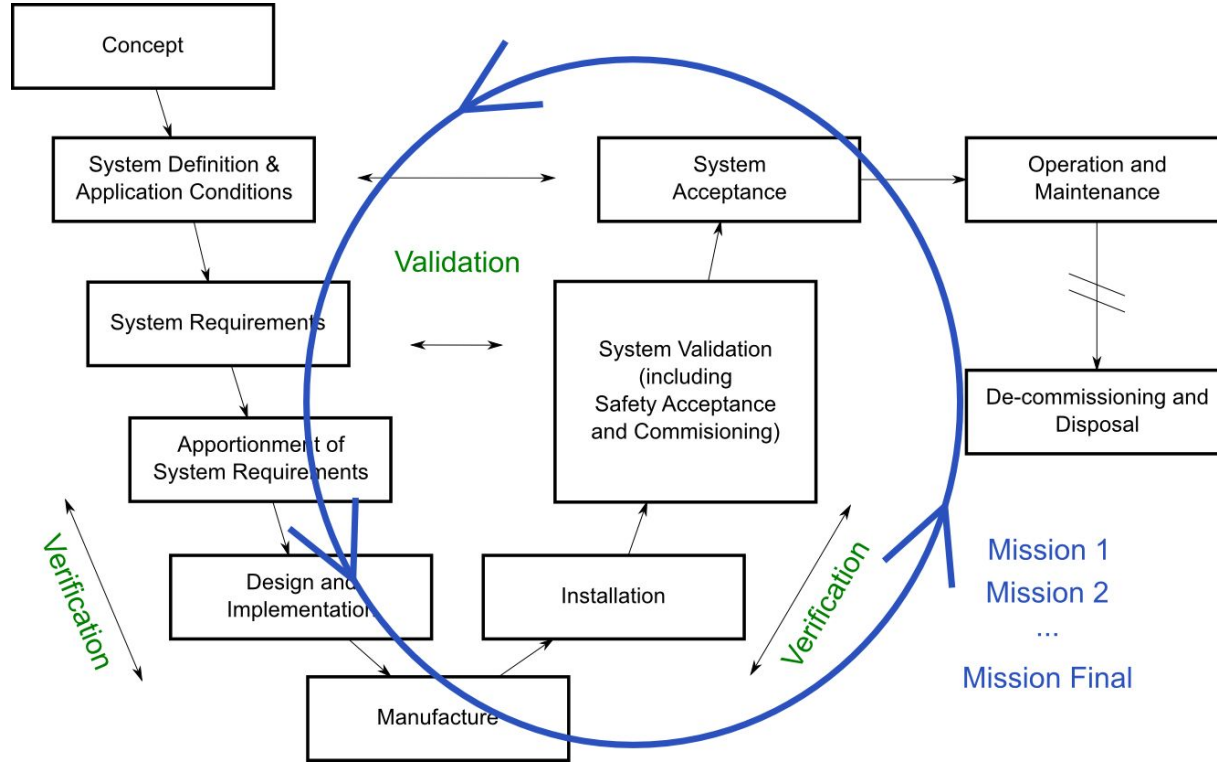
The V-Model in CENELEC



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 \leq SIL Level Qualification and Assessment

Enabling System \leq 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

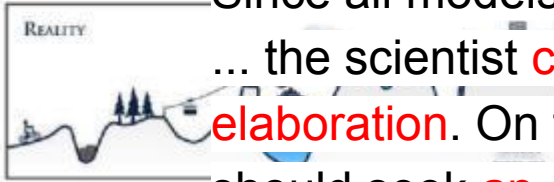
George Box 1976

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

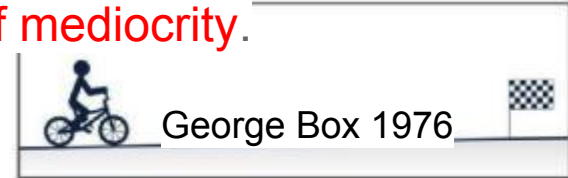
... but Some are Useful

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.



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.

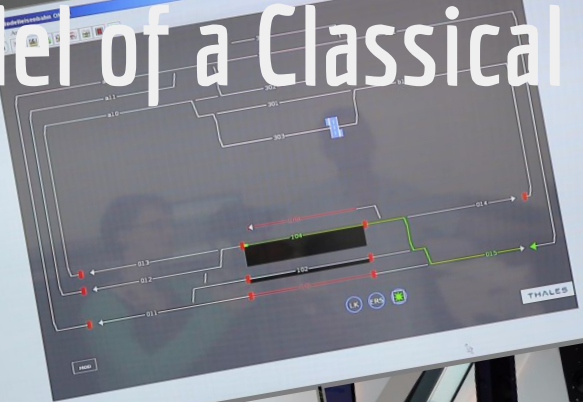
=> The **fallacy of reification** is committed over and over, believing the model represents the truth... instead of an approximation.

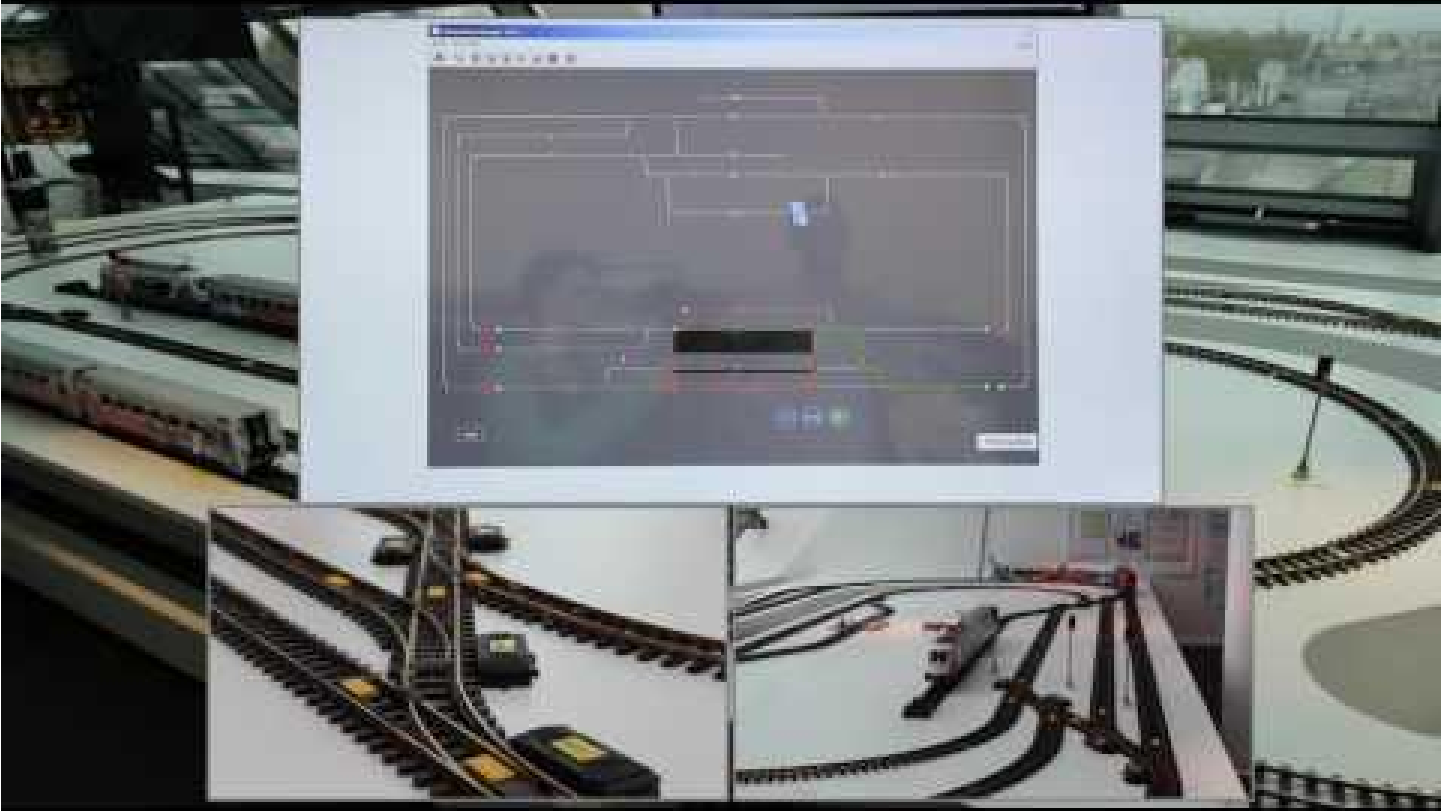
=> The **model is not wrong** but **treating the model** as the **absolute truth** (i.e. reification) **is wrong**.

Thaddeus Tarpey 2012

Ceci n'est pas une pipe.

Model of a Classical Interlocking



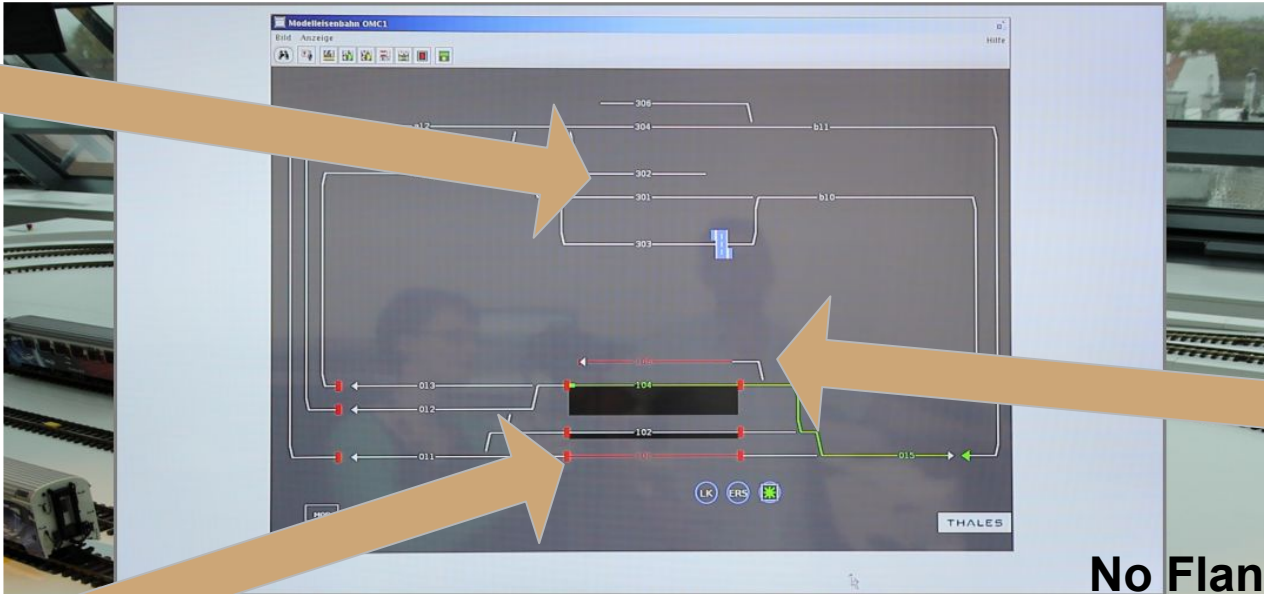




Questions?

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

**No Routes?
No Station?**



No Flank Protection?

**Train Length?
Train Integrity?**



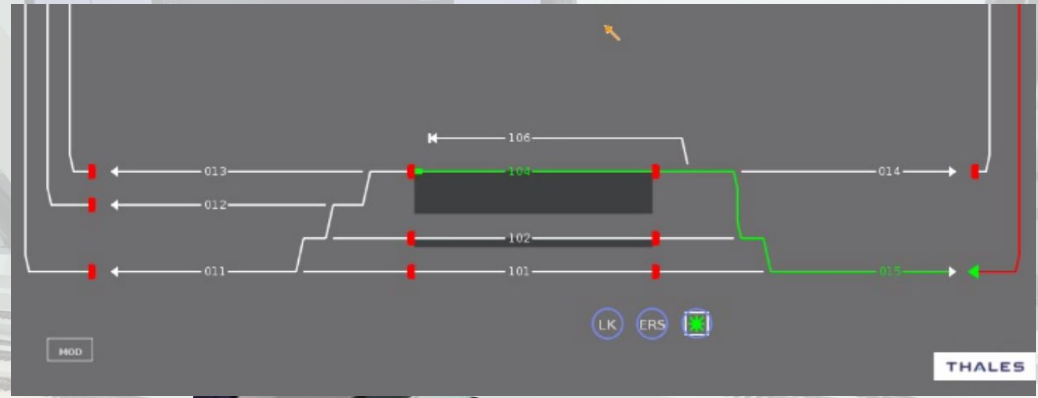
Questions?

- 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

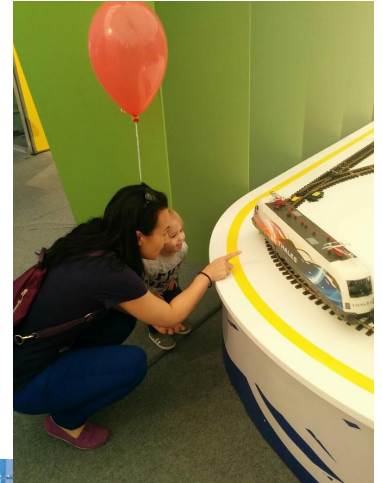


Questions?

- 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 ;-)

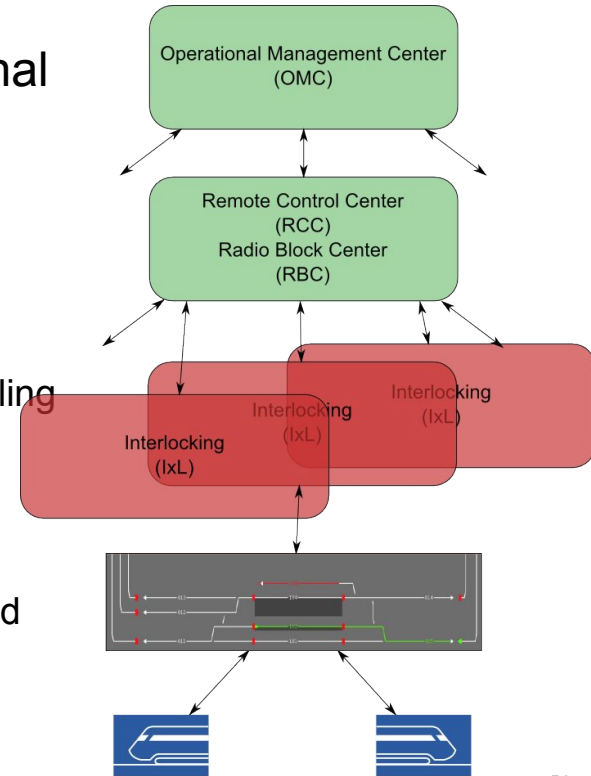


Excuse: Some words on ERTMS, ETCS and Interlocking

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

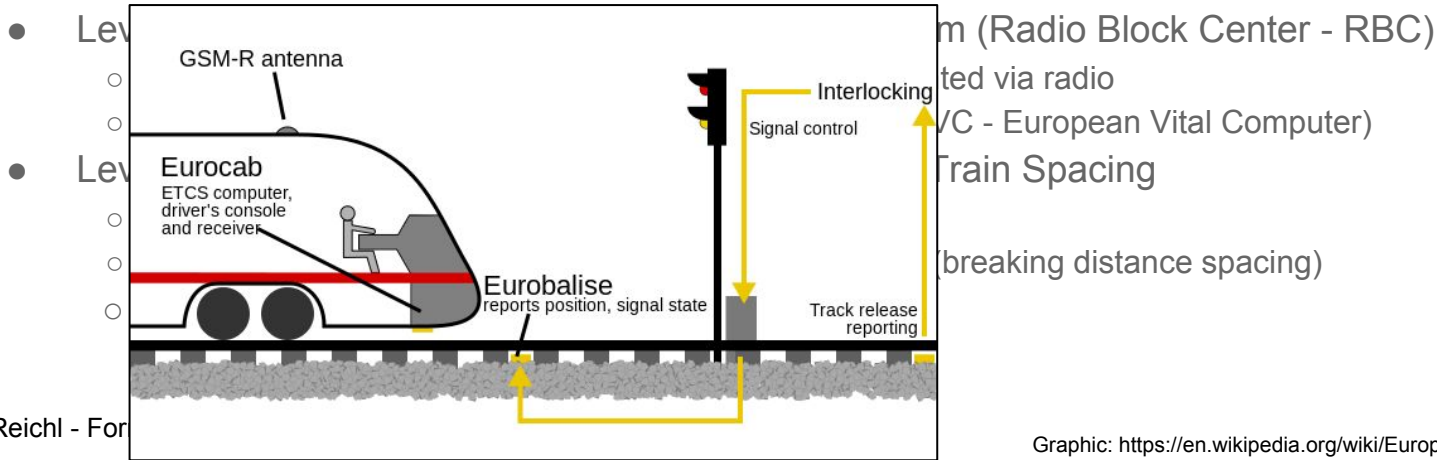


ETCS - European Train Control

- 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

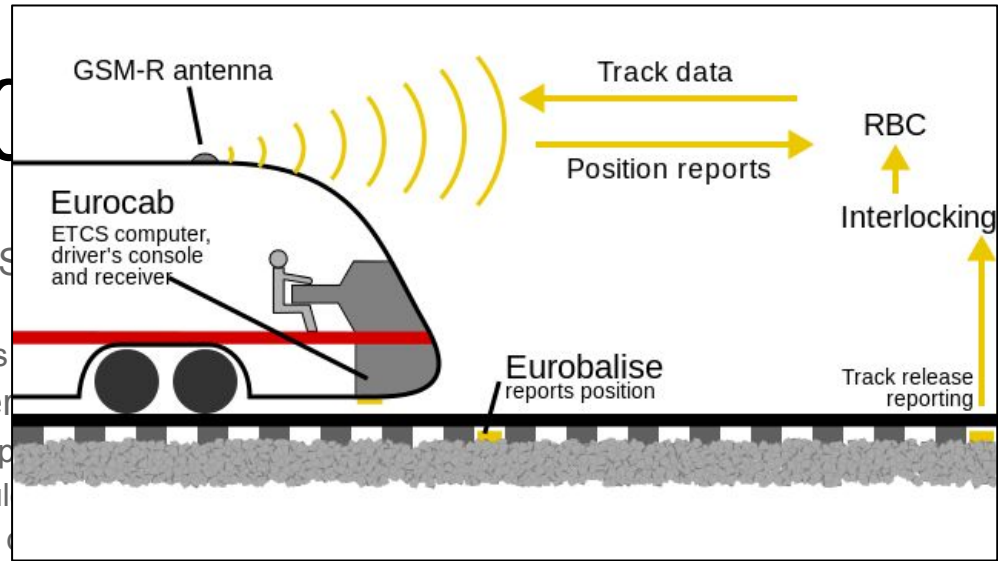
- Level 0 - ETCS-fitted vehicles on non-ETCS route
 - Train driver observes trackside
 - Might be limited in speed by the last balises encountered
- Level 1 - Cab signalling which can be superimposed on the existing signaling system
 - Eurobalise radio beacons pick up signal aspects from the trackside 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



m (Radio Block Center)
 ted via radio
 /C - European Vital Computer)
 Train Spacing
 (breaking distance spacing)

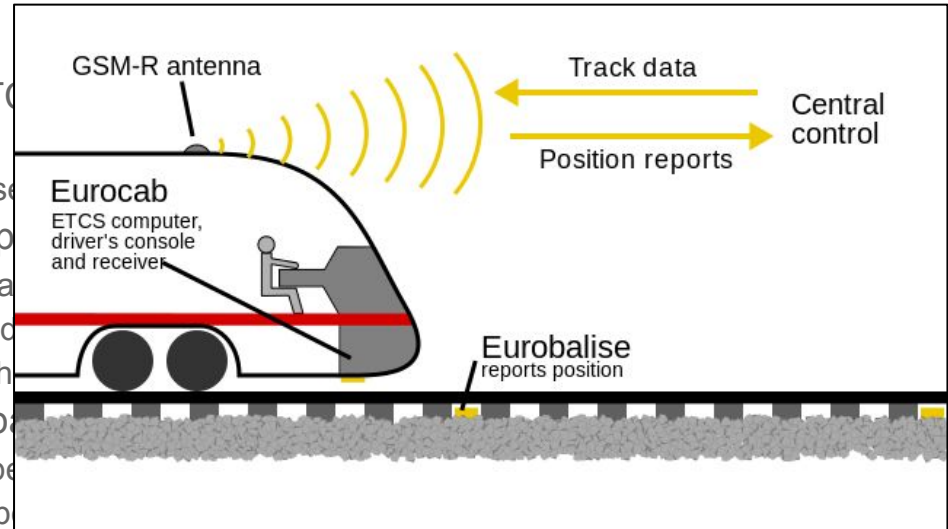
ETCS - European Train Control System

- Level 0 - ETCS-fitted vehicles on non-ETCS tracks
 - Train driver observes trackside
 - Might be limited in speed by the last balises
- Level 1 - Cab signalling which can be superimposed on trackside signals
 - Eurobalise radio beacons pick up signal as speeders (STM - Specific Transmission Module)
 - "Infill" Eurobalise or EuroLoop between the balises
- Level 2 - Cab 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)

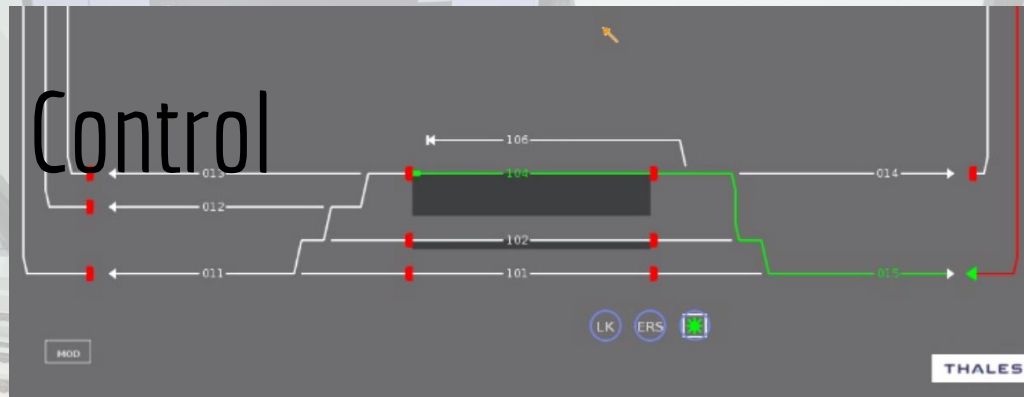


ETCS - European Train Control

- Level 0 - ETCS-fitted vehicles on non-ETCS tracks
 - Train driver observes trackside
 - Might be limited in speed by the last balise
- Level 1 - Cab signalling which can be supplemented by trackside balises
 - Eurobalise radio beacons pick up signal and send it to the cab (STM - Specific Transmission Mode)
 - “Infill” Eurobalise or EuroLoop between the trackside balises
- Level 2 - Cab signalling via digital radio-based communication
 - Movement Authority and other signal aspects are sent to the cab
 - Breaking curves implemented by the Onboard Unit
- 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

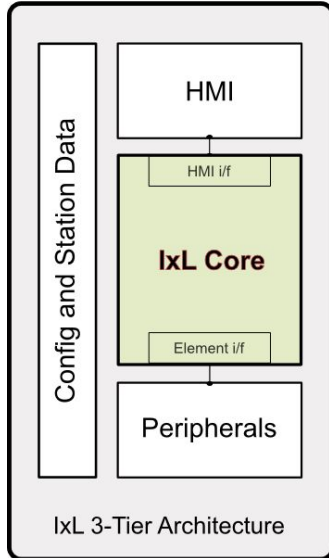


- Virtual Signals - Movement Authority
 - Train Protection
- Route Control - computed
 - In addition to pre configured
- Trains (rather vehicles!) detected by
 - Positioning Logic
- Element Control
 - Points and Level Crossings

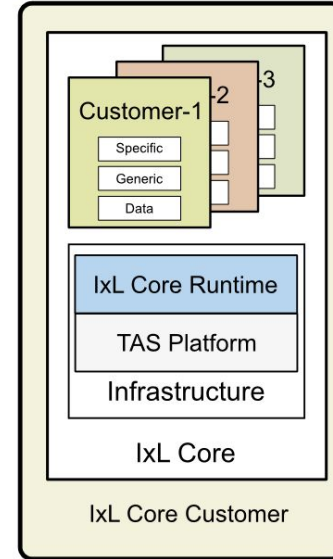
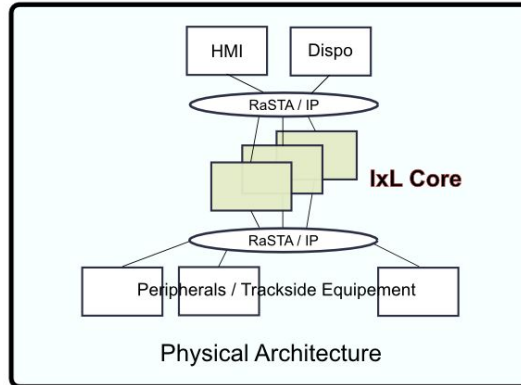
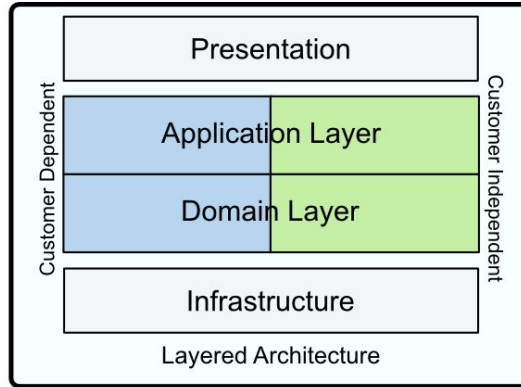


Now really modelling ...

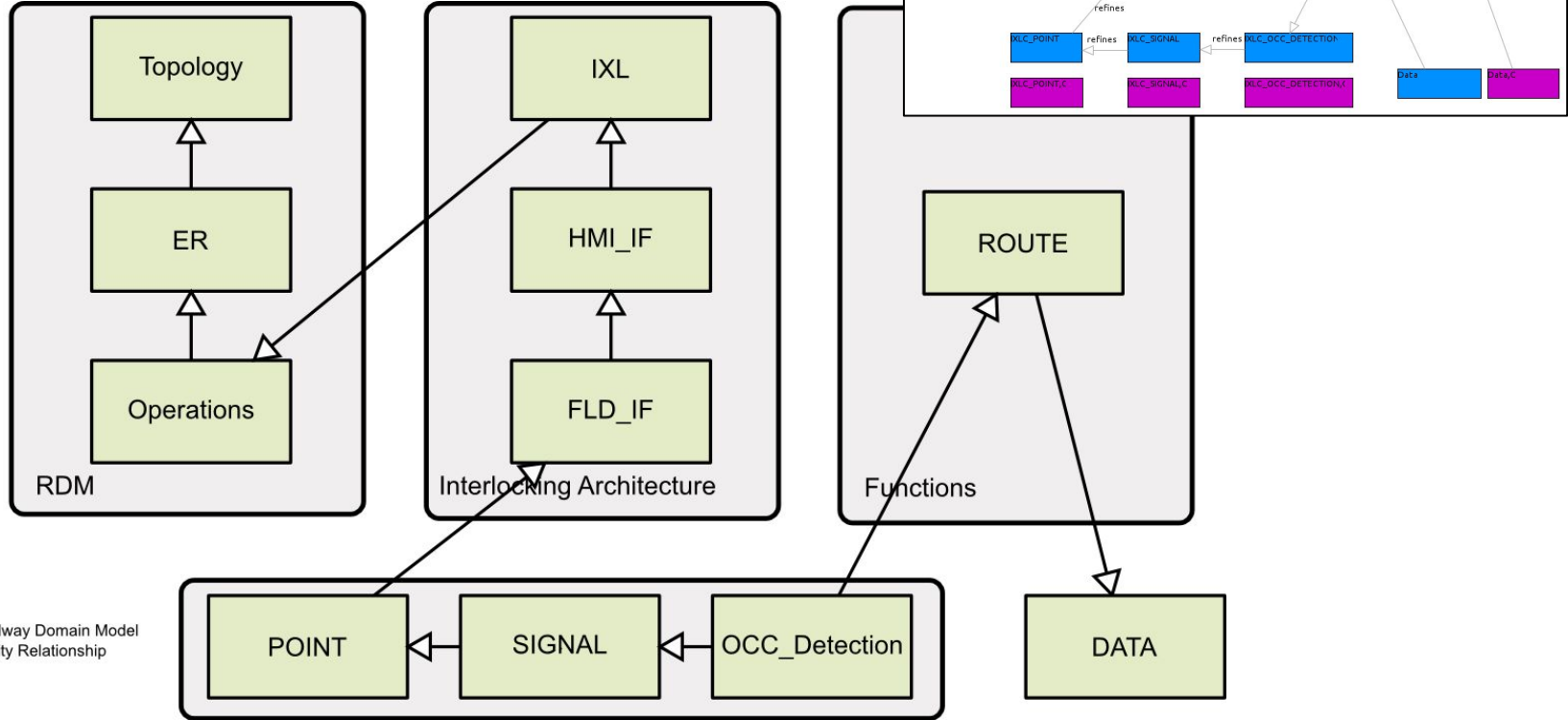
Interlocking Architecture



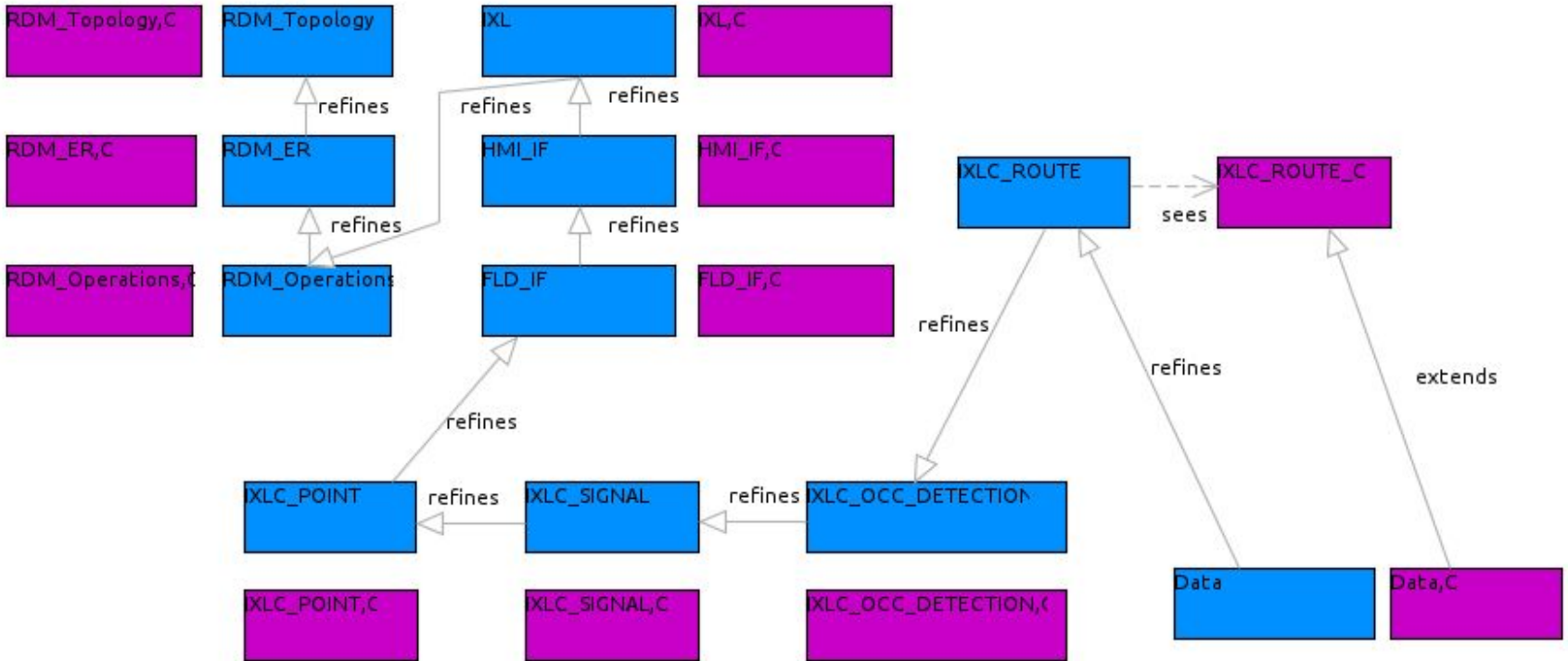
HMI ... Human Machine Interface
 Dispo ... Dispositive Peer Systems
 - Schedules, Operation Control, ...
 RaSTA ... Rail Safe Transport Protocol @ IP



Refinement Strategy



Refinement Strategy



BMS Run - generic/Animation.bmsa - Rodin Platform

Animation (Data.bum - EventB) ⌵

THALES
SPECIFICATION MODEL ANIMATION

KR - Version 1.13 2016-05-10
Lutz.Danz@thalesgroup.com
Klaus.Reichl@thalesgroup.com

Modelleisenbahn - IXLCore View

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)

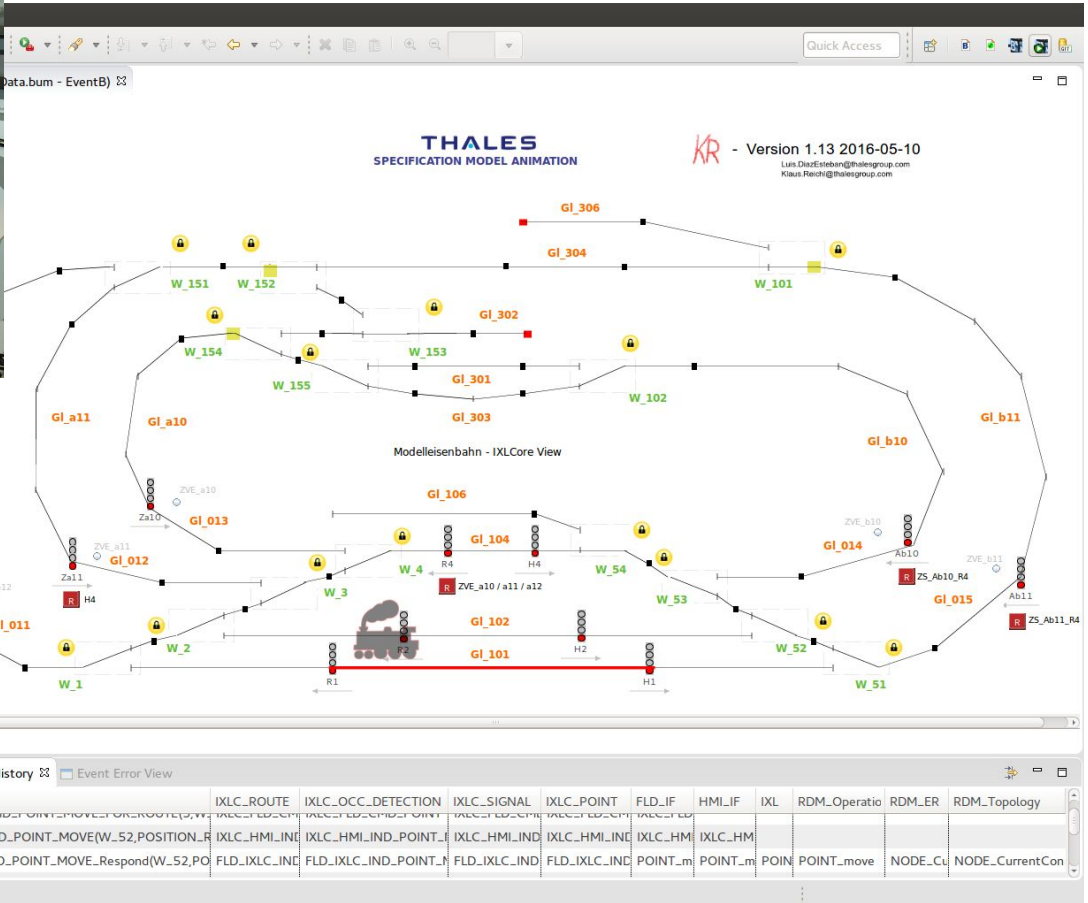
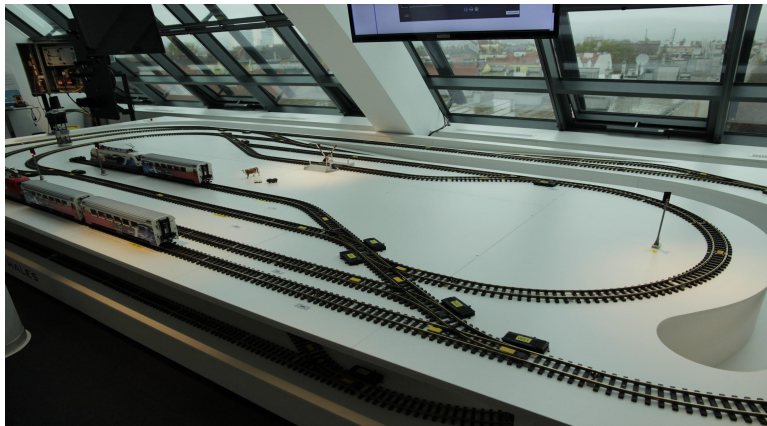
Event-B Explorer ⌵

- 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

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_F	IXLC_HMI_IND	IXLC_HMI_IND_POINT_I	IXLC_HMI_IND	IXLC_HMI_IND	IXLC_HMI	IXLC_HMI				
FLD_IXLC_IND_POINT_MOVE_Respond(W_52,PO	FLD_IXLC_IND	FLD_IXLC_IND_POINT_I	FLD_IXLC_IND	FLD_IXLC_IND	POINT_m	POINT_m	POINT	POINT_move	NODE_Cu	NODE_CurrentCon



Establishing a Route

The image displays a formal verification tool interface for railway systems, showing the process of establishing a route. The interface is divided into several panels:

- Events Panel:** Lists various events such as `HMI_I_XLC_CMD_POINT_BLOCK`, `HMI_I_XLC_CMD_POINT_UNBLOCK`, `HMI_I_XLC_CMD_POINT_MOVE`, `HMI_I_XLC_CMD_ROUTE_SET`, `IXL_HMI_NACK_ROUTE_SET`, `FLD_I_XLC_IND_TVP_AREA_OCCUPANCY`, and `FLD_I_XLC_IND_POINT_MOVE`.
- Event-B Explorer:** Shows a hierarchical domain structure including `generic`, `Data.C`, `FLD_IF.C`, `HMI_IF.C`, `IXL.C`, `IXLC_OCC_DETECTION.C`, `IXLC_POINT.C`, `IXLC_ROUTE.C`, `IXLC_SIGNAL.C`, `RDM_ER.C`, `RDM_Operations.C`, `RDM_Topology.C`, and `TheoryPath`.
- Diagram Panel:** A detailed view of a railway track layout labeled "Modellereisenbahn - IXLCore View". It shows various track segments (e.g., `W_151`, `W_152`, `W_153`, `W_154`, `W_155`, `W_101`, `W_102`, `W_103`, `W_104`, `W_105`, `W_106`, `W_107`, `W_108`, `W_109`, `W_110`, `W_111`, `W_112`, `W_113`, `W_114`, `W_115`, `W_116`, `W_117`, `W_118`, `W_119`, `W_120`, `W_121`, `W_122`, `W_123`, `W_124`, `W_125`, `W_126`, `W_127`, `W_128`, `W_129`, `W_130`, `W_131`, `W_132`, `W_133`, `W_134`, `W_135`, `W_136`, `W_137`, `W_138`, `W_139`, `W_140`, `W_141`, `W_142`, `W_143`, `W_144`, `W_145`, `W_146`, `W_147`, `W_148`, `W_149`, `W_150`, `W_151`, `W_152`, `W_153`, `W_154`, `W_155`, `W_156`, `W_157`, `W_158`, `W_159`, `W_160`, `W_161`, `W_162`, `W_163`, `W_164`, `W_165`, `W_166`, `W_167`, `W_168`, `W_169`, `W_170`, `W_171`, `W_172`, `W_173`, `W_174`, `W_175`, `W_176`, `W_177`, `W_178`, `W_179`, `W_180`, `W_181`, `W_182`, `W_183`, `W_184`, `W_185`, `W_186`, `W_187`, `W_188`, `W_189`, `W_190`, `W_191`, `W_192`, `W_193`, `W_194`, `W_195`, `W_196`, `W_197`, `W_198`, `W_199`, `W_200`), signal lights (e.g., `GI_306`, `GI_304`, `GI_302`, `GI_301`, `GI_303`, `GI_106`, `GI_104`, `GI_102`, `GI_101`, `GI_012`, `GI_013`, `GI_014`, `GI_015`, `GI_011`), and train positions (e.g., `ZVE_a10`, `ZVE_a11`, `ZVE_a12`, `ZVE_a13`, `ZVE_a14`, `ZVE_a15`, `ZVE_a16`, `ZVE_a17`, `ZVE_a18`, `ZVE_a19`, `ZVE_a20`, `ZVE_a21`, `ZVE_a22`, `ZVE_a23`, `ZVE_a24`, `ZVE_a25`, `ZVE_a26`, `ZVE_a27`, `ZVE_a28`, `ZVE_a29`, `ZVE_a30`, `ZVE_a31`, `ZVE_a32`, `ZVE_a33`, `ZVE_a34`, `ZVE_a35`, `ZVE_a36`, `ZVE_a37`, `ZVE_a38`, `ZVE_a39`, `ZVE_a40`, `ZVE_a41`, `ZVE_a42`, `ZVE_a43`, `ZVE_a44`, `ZVE_a45`, `ZVE_a46`, `ZVE_a47`, `ZVE_a48`, `ZVE_a49`, `ZVE_a50`, `ZVE_a51`, `ZVE_a52`, `ZVE_a53`, `ZVE_a54`, `ZVE_a55`, `ZVE_a56`, `ZVE_a57`, `ZVE_a58`, `ZVE_a59`, `ZVE_a60`, `ZVE_a61`, `ZVE_a62`, `ZVE_a63`, `ZVE_a64`, `ZVE_a65`, `ZVE_a66`, `ZVE_a67`, `ZVE_a68`, `ZVE_a69`, `ZVE_a70`, `ZVE_a71`, `ZVE_a72`, `ZVE_a73`, `ZVE_a74`, `ZVE_a75`, `ZVE_a76`, `ZVE_a77`, `ZVE_a78`, `ZVE_a79`, `ZVE_a80`, `ZVE_a81`, `ZVE_a82`, `ZVE_a83`, `ZVE_a84`, `ZVE_a85`, `ZVE_a86`, `ZVE_a87`, `ZVE_a88`, `ZVE_a89`, `ZVE_a90`, `ZVE_a91`, `ZVE_a92`, `ZVE_a93`, `ZVE_a94`, `ZVE_a95`, `ZVE_a96`, `ZVE_a97`, `ZVE_a98`, `ZVE_a99`, `ZVE_a100`).
- History Panel:** A table showing the sequence of events and their corresponding state transitions. The table has columns for event names and state variables.

Establishing a Route (Locked by Another)

The screenshot displays a railway simulation environment. On the left, there are two 'Event-B Explorer' windows. The top one shows a list of events, with '7_ZS_Ab10_R4' selected. The bottom one shows a similar list with 'IXL_HMI_NACK_ROUTE_SET' selected. The main window shows a track diagram titled 'Modelleisenbahn - IXLCore View'. The diagram features various track segments labeled with 'W' (e.g., W_151, W_152, W_153, W_154, W_155, W_101, W_102, W_103, W_104, W_54, W_53, W_52) and 'GI' (e.g., GI_a12, GI_a11, GI_a10, GI_a13, GI_106, GI_104, GI_102, GI_101, GI_306, GI_304, GI_302, GI_303, GI_b10, GI_b11). A red line and a green line represent different routes or states on the track. A train is visible on the right side of the track. At the bottom, there is a table with columns for event names and various state variables.

	IXL_CRO	IXL_COC	IXL_SIC	IXL_PO	FLD_IF	HMI_IF	IXL	RDM_Op	RDM_LER	RDM_Top
NACK_ROUTE_SET(6)	IXL_HMI									
_CMD_ROUTE_SET(6,ZS_Ab10_R4)	HMI_IXL	HMI_IXL	HMI_IXL	HMI_IXL	HMI_IXL	HMI_IXL				
L_IND_SIGNAL_ASPECT(SIGNAL_ASPECT_PROCEED,Ab11)	IXL_C_HM	IXL_C_HM	IXL_C_HM							
L_IND_SIGNAL_ASPECT(SIGNAL_ASPECT_PROCEED,S,Ab11)	FLD_IXL_C	FLD_IXL_C	FLD_IXL_C	FLD_IXL_C	FLD_IXL_C					
L_CMD_SIGNAL_ASPECT(5,SIGNAL_ASPECT_PROCEED,Ab11)	IXL_C_FLIC	IXL_C_FLIC	IXL_C_FLIC	IXL_C_FLIC	IXL_C_FLIC					
L_LACK_ROUTE_SET(5,ZS_Ab11_R4)	IXL_HMI	IXL_HMI	IXL_HMI	IXL_HMI	IXL_HMI					
_CMD_ROUTE_SET(5,ZS_Ab11_R4)	HMI_IXL	HMI_IXL	HMI_IXL	HMI_IXL	HMI_IXL	HMI_IXL				
L_IND_POINT_MOVE(W_54,POSITION_LEFT)	IXL_C_HM	IXL_C_HM	IXL_C_HM	IXL_C_HM	IXL_C_HM					

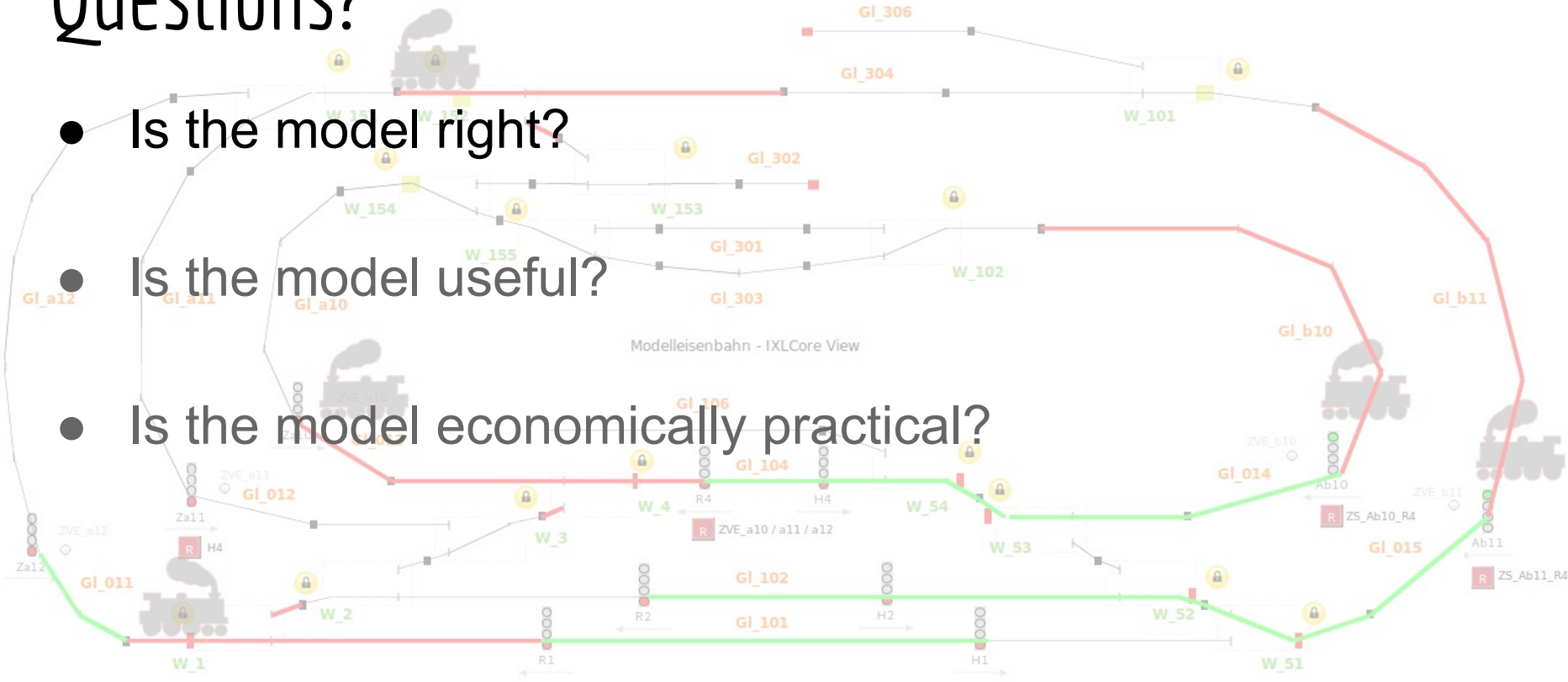
Closing a Signal after Track Occupancy

The screenshot displays a railway simulation interface. On the left, a track layout shows a train (Za12) and various signal and track elements (ZVE_a10, ZVE_a11, ZVE_a12, GI_011, GI_012, W_2, W_3, W_4, R2, R4). The 'Events' panel shows a list of events: 'HMI_I_XLC_CMD_POINT_BLOCK (x15)' and 'HMI_I_XLC_CMD_POINT_UNBLOCK (x15)'. The 'Data' table below the main view lists various occupancy and signal states. The 'Modellereisenbahn - IXLCore View' on the right shows a more detailed track layout with multiple tracks and signals (GI_010, GI_011, GI_012, GI_013, GI_014, GI_015, GI_101, GI_102, GI_104, GI_106, GI_301, GI_302, GI_303, GI_304, GI_306, W_101, W_102, W_150, W_151, W_152, W_153, W_154, W_155, W_52, W_53, W_54, ZS_A10, ZS_A10_R4, ZS_A11, ZS_A11_R4, ZS_A12).

Data		IXLC_RO	IXLC_OC	IXLC_SIC	IXLC_PO	FLD_IF	HMI_IF	IXL	RDM_Op	RDM_ER	RDM_Tops
IXLC_HMI_IND_SIGNAL_ASPECT(SIGNAL_ASPECT_STOP,Za12)	SIGNAL_ASPECT(SIGNAL_ASPECT_STOP,Za12)	IXLC_HM	IXLC_HM	IXLC_HM							
IXLC_HMI_IND_POINT_OCCUPANCY(W_1,OCCUPANCY_OCCUPIED)	POINT_OCCUPANCY(W_1,OCCUPANCY_OCCUPIED)	IXLC_HM	IXLC_HM	POINT_S	POINT_S	POINT_S	POINT_S	POINT_S	POINT_S		
FLD_I_XLC_IND_TVP_AREA_OCCUPANCY(OCCUPANCY_OCCUPIED,MOD_W_1)	TVP_AREA_OCCUPANCY(OCCUPANCY_OCCUPIED,MOD_W_1)	FLD_I_XLC	FLD_I_XLC	TVP_ARE	TVP_ARE	TVP_ARE	TVP_ARE	TVP_ARE	TVP_ARE		
IXLC_HMI_IND_TRACK_SECTION_OCCUPANCY(OCCUPANCY_FREE,GL_a12)	TRACK_SECTION_OCCUPANCY(OCCUPANCY_FREE,GL_a12)	IXLC_HM	IXLC_HM	TVP_SEC	TRACK_S	TRACK_S	TRACK_S	TRACK_S	TRACK_S		
FLD_I_XLC_IND_TVP_AREA_OCCUPANCY(OCCUPANCY_FREE,MOD_GL_a12)	TVP_AREA_OCCUPANCY(OCCUPANCY_FREE,MOD_GL_a12)	FLD_I_XLC	FLD_I_XLC	TVP_ARE	TVP_ARE	TVP_ARE	TVP_ARE	TVP_ARE	TVP_ARE		
FLD_I_XLC_IND_SIGNAL_ASPECT(SIGNAL_ASPECT_PROCEED,7,Za12)	SIGNAL_ASPECT(SIGNAL_ASPECT_PROCEED,7,Za12)	IXLC_FLG	IXLC_FLG	IXLC_FLG	IXLC_FLG	IXLC_FLG	IXLC_FLG	IXLC_FLG	IXLC_FLG		
IXLC_FLD_CMD_SIGNAL_ASPECT(7,SIGNAL_ASPECT_PROCEED,Za12)	POINT_MOVE(W_2,POSITION_RIGHT)	IXLC_HM	IXLC_HM	IXLC_HM	IXLC_HM	IXLC_HM	IXLC_HM				

Questions?

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



THALES
SPECIFICATION MODEL ANIMATION

KR - Version 1.13 2016-05-10
Luis DiazEsteban@thalesgroup.com
Klaus Reich@thalesgroup.com

Modelleisenbahn - IXLCore View

Event-B Explorer

- Event
 - HMI_IXLC_CMD_POINT_BLOCK (x15)
 - HMI_IXLC_CMD_POINT_UNBLOCK (x15)
 - HMI_IXLC_CMD_POINT_MOVE (x9)
 - HMI_IXLC_CMD_ROUTE_SET (x18)
 - IXLC_HMI_IND_SIGNAL_ASPECT
 - FLD_IXLC_IND_TVP_AREA_OCCUPANCY (x34)
 - FLD_IXLC_IND_POINT_MOVE (x30)
- Domain
 - generic
 - Data.C
 - FLD_IF.C
 - HMI_IF.C
 - IXLC
 - IXLC_OCC_DETECTION.C
 - IXLC_POINT.C
 - IXLC_ROUTE.C
 - IXLC_SIGNAL.C
 - RDM_ER
 - RDM_OCCURSIONS.C
 - RDM_Topology.C

History

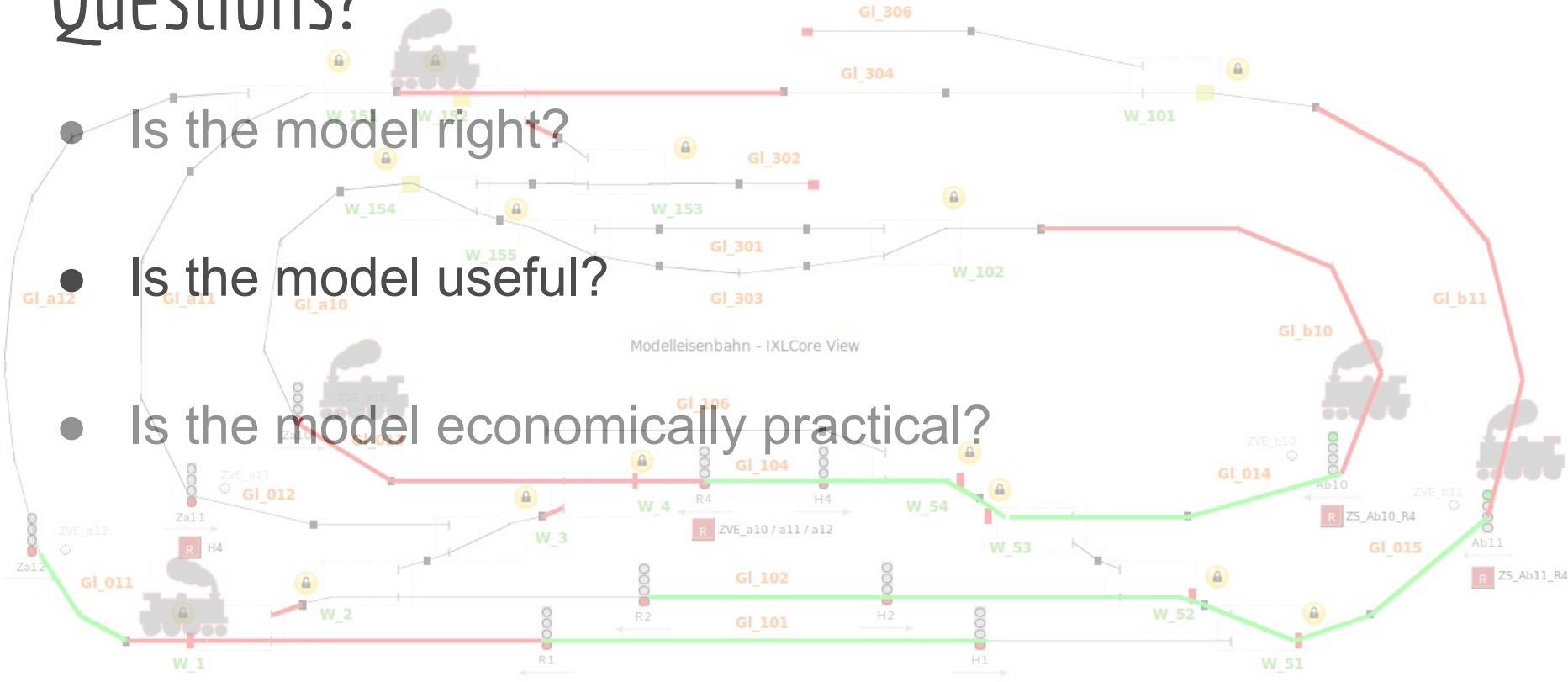
Data	IXLC_ROI	IXLC_OC	IXLC_SIG	IXLC_POI	FLD_IF	HMI_IF	IXL	RDM_Op	RDM_ER	RDM_Top
IXLC_IND_TRACK_SECTION_OCCUPANCY(OCCUPANCY_OCCUPIED, GL_106)	IXLC_HM	IXLC_HM	TVP_SEC	TRACK_S	TRACK_S	TRACK_S	TRACK_S	TRACK_S		
FLD_IXLC_IND_TVP_AREA_OCCUPANCY(OCCUPANCY_OCCUPIED, MOD_GL_106)	FLD_IXLC	FLD_IXLC	TVP_AREA	TVP_AREA	TVP_AREA	TVP_AREA	TVP_AREA	TVP_AREA		
IXLC_HMI_IND_TRACK_SECTION_OCCUPANCY(OCCUPANCY_OCCUPIED, GL_112)	IXLC_HM	IXLC_HM	TVP_SEC	TRACK_S	TRACK_S	TRACK_S	TRACK_S	TRACK_S		
FLD_IXLC_IND_TVP_AREA_OCCUPANCY(OCCUPANCY_OCCUPIED, MOD_GL_a12)	FLD_IXLC	FLD_IXLC	TVP_AREA	TVP_AREA	TVP_AREA	TVP_AREA	TVP_AREA	TVP_AREA		

Route Release is Crap!
Waiting train could already move to platform "GL_101"!

No Flank Protection?

Questions?

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

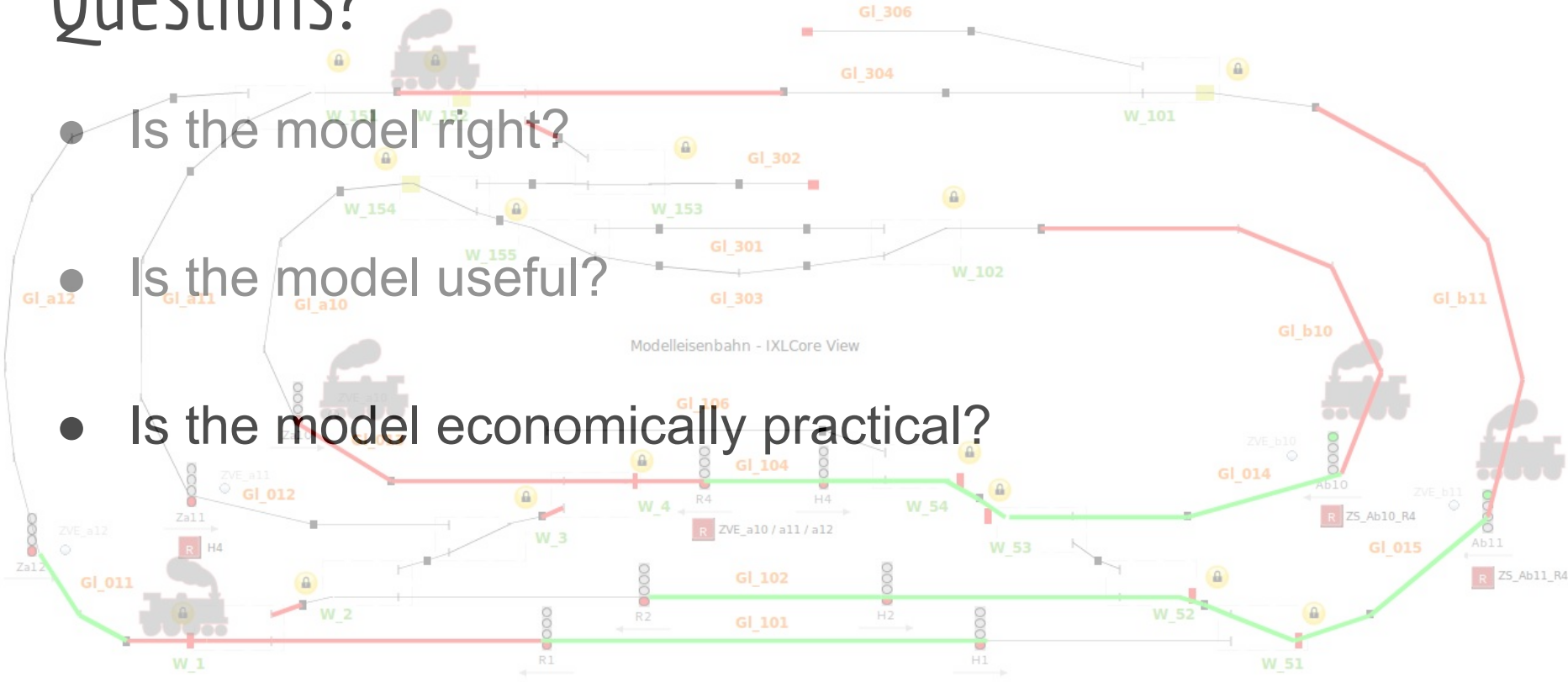


Is the model useful?

- 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?

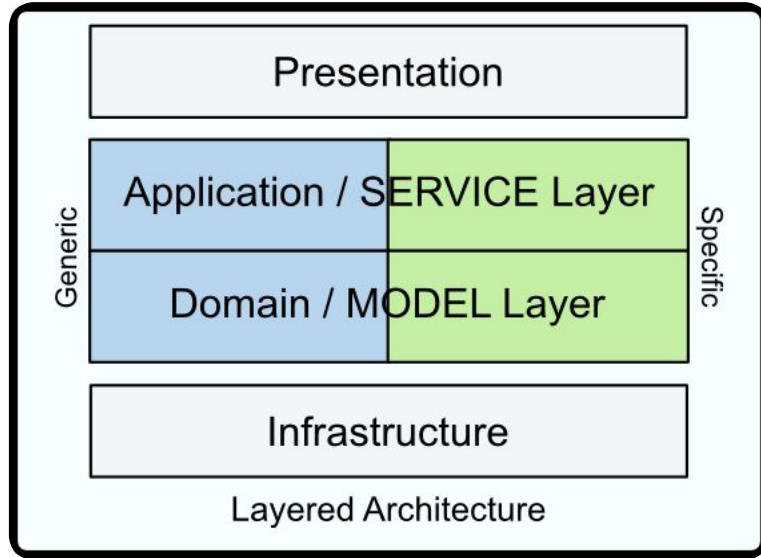


Is the model economically practical?

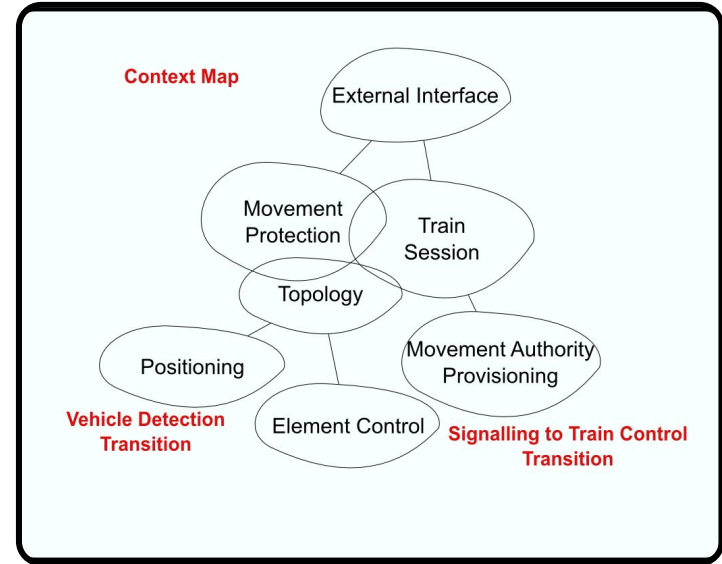
- Adding new Control Operations is painful
 - This should be done using an Adaptor
 - Protocol to HMI adds Incidental Complexity
 - ACK/NAK does not bring any value
- Business Domain and Architecture is Mixed
 - Should be strictly decoupled for Maintainability
 - Model is good for different Topologies, 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

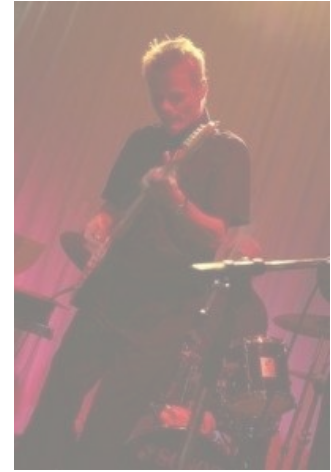
Where is it driving at

- Model Integration with various Stakeholders from various Domains



Klaus.Reichl@gmail.com

Computer Hacker and Guitar Player
Living in Vienna



Klaus.Reichl@thalesgroup.com

System and Software Architect
Handelskai 92
A-1200 Vienna

Thank You!

Questions?



<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

© 2016 - Klaus Reichl - Klaus.Reichl@thalesgroup.com, Klaus.Reichl@gmail.com

This document is licensed under a Creative Commons Attribution 4.0 Unported license. For more information about this license see <https://creativecommons.org/licenses/by/4.0/> (In short, you can copy, redistribute, and adopt this work as long as you give proper attribution).

