

Digital Railway Operation CyberSecurity in Critical Infrastructures



Prof. Dr. rer. nat. habil. Andreas Polze
Professur Betriebssysteme und Middleware
Hasso-Plattner-Institut, Universität Potsdam



Operating Systems and Middleware group

Prof. Dr. Andreas Polze -- osm.hpi.de



Forschung:

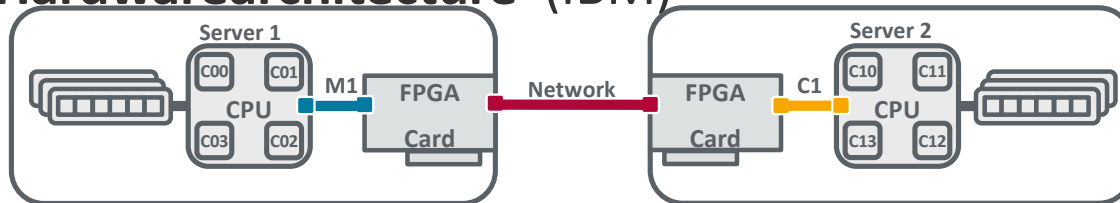
Digital Rail

- mFund Forschungsprojekte mit DB Systel, DB Netz: Rail2X, DiAK, RailChain, FlexiDug, SQuIRRL
- Verteiltes IoT-Lab für Testautomatisierung

Telemed5000 (Charité)



Hardwarearchitecture (IBM)



Teaching:

- Operating Systems
- Parallel and Distributed Systems
- Embedded Systems
- Digital Rail Summer School (2019-25)

Agenda

- **EULYNX - Digital Railway Operation**
- ENISA report - Security measures in the Railway Transport Sector
- RailSecurity
- Paradigm shift: from GIuV to permanent consistency checking
...“Using Simplicity to Control Complexity” (Lui Sha, IEEE Comp., 2001)
- Physical Security - Digitalization weakens systems
- NIS2 - The European CyberSecurity Act



SBB

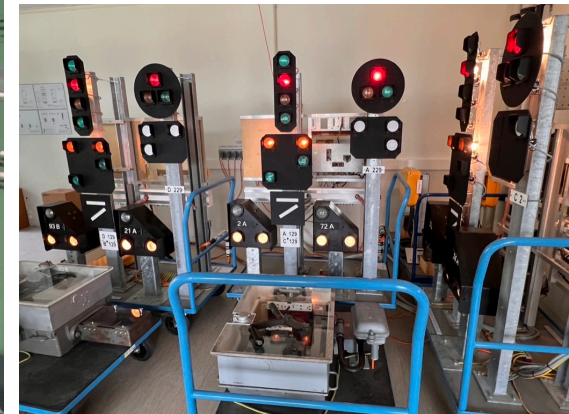
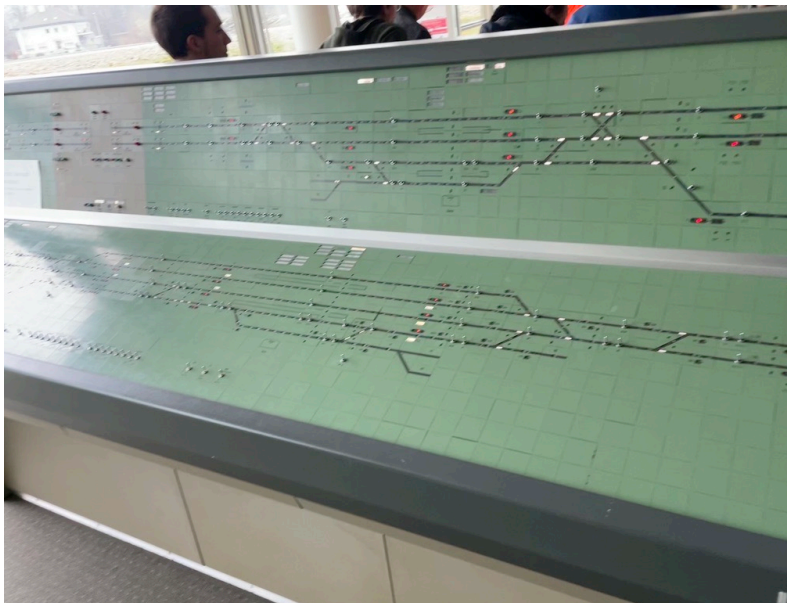
Loewenberg
training
center

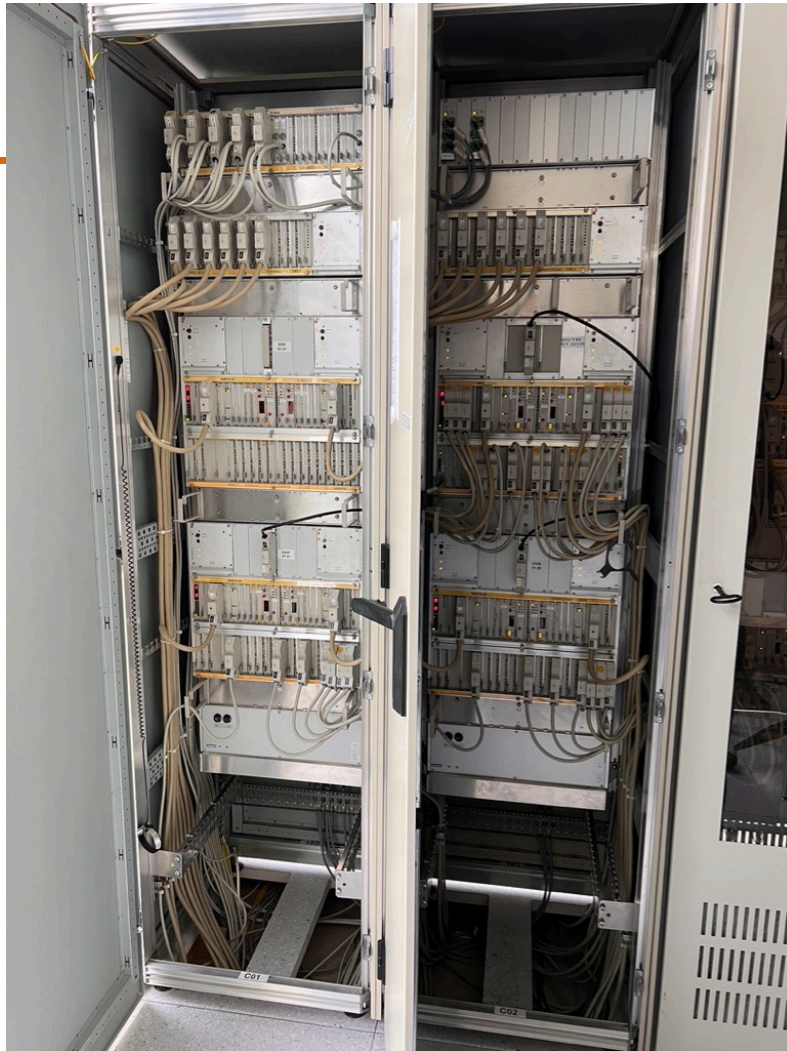
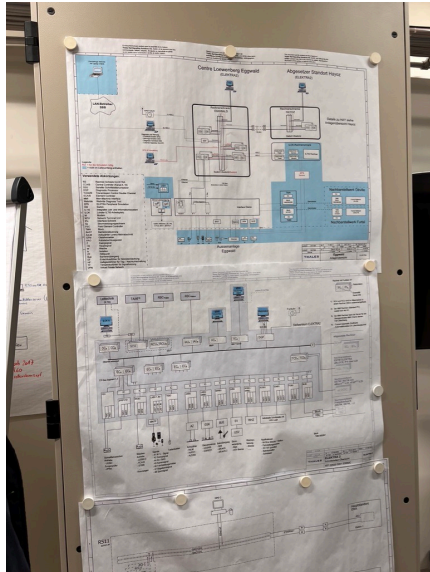




SBB  Hasso Plattner Institut

Loewenberg
training
center

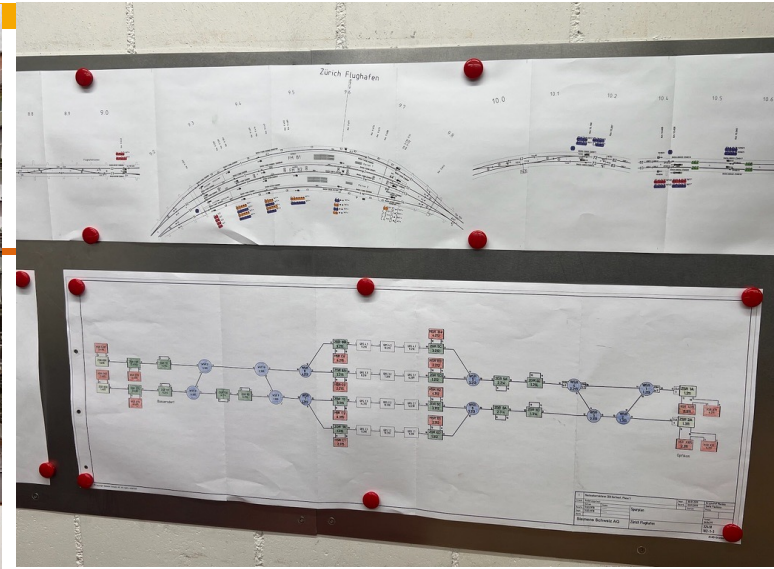
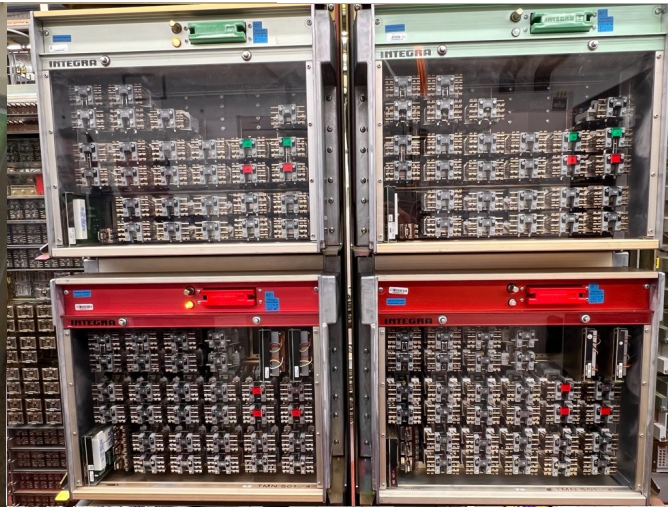
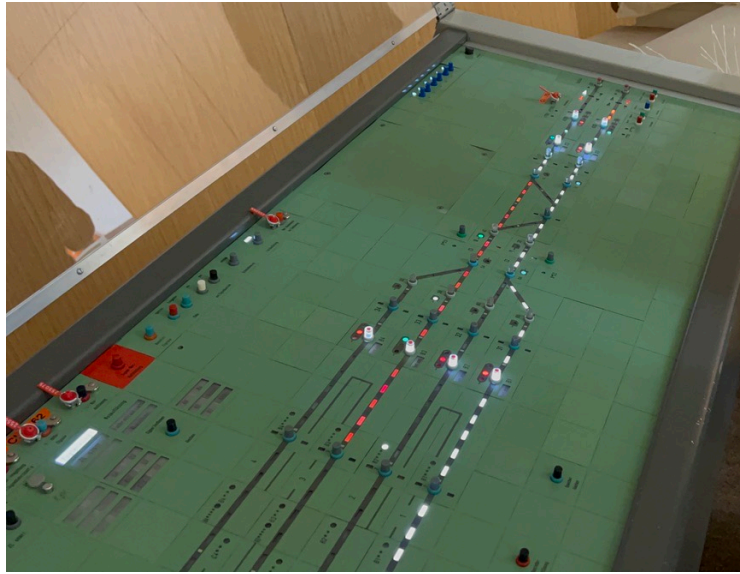




SBB

Loewenberg
training
center



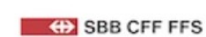


SBB Zurich airport interlocking





ON TRACK TOWARDS DIGITAL RAILWAYS

 BANE NOR CFL DB NETZE INFRABEL NetworkRail BB
INFRA ProRail RFI
RILEVAMENTO PERMANENTE ITALIANO
GRUPPO PERMANENTE DELLO STATO ITALIANO SBB CFF FFS SNCF Slovenske železnice TRAFIKVERKET Finnish Transport
Infrastructure Agency

EULYNX.eu



What is EULYNX

- ✓ **An initiative of European railway infrastructure managers**
- ✓ **Defining an internationally standardised signalling system**
- ✓ **Focus on modular signalling architecture with common standardised interfaces**
- ✓ **Standing organisation for continuous development, maintenance and change management of the standards**
- ✓ **Support the certification of products**
- ✓ **Support infrastructure managers in implementation of the standards**

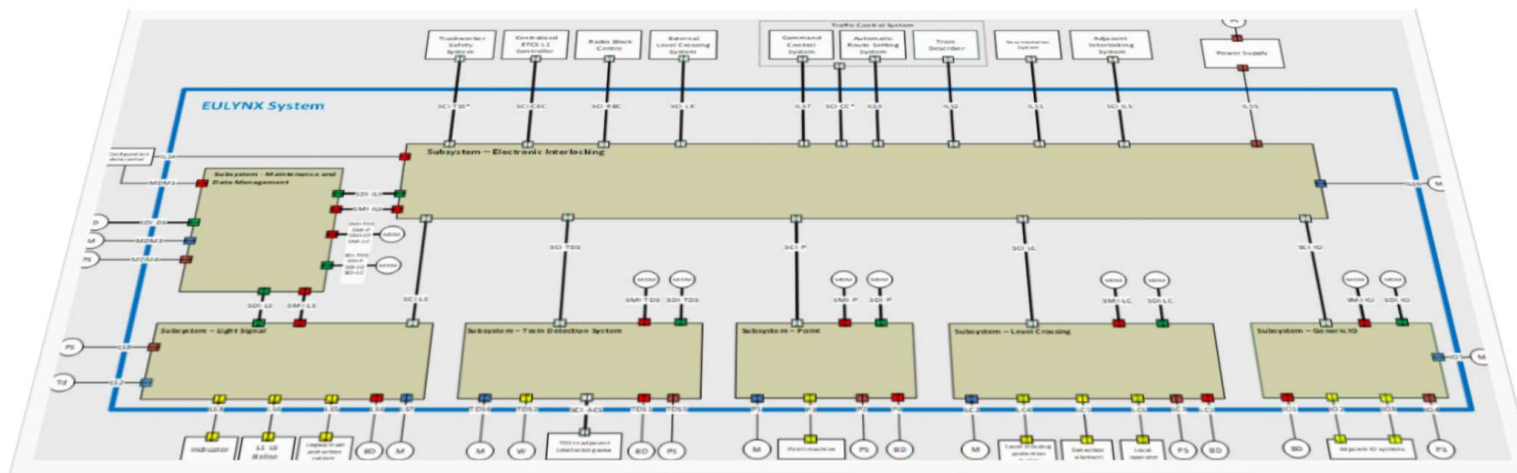
<https://eulynx.eu/index.php/documents/presentations-given/252-20200305-dp-workshop-presentation/file>



EULYNX

Modular architecture

- ✓ The reference architecture is a **modular structure** defining field elements as subsystems with **controllers** and **standardized interfaces** to command and control them
- ✓ Apply **IP-based** communication using closed and open networks
- ✓ **System design** that is based on components of the shelf (COTS) and mass industry solutions also used in other industries





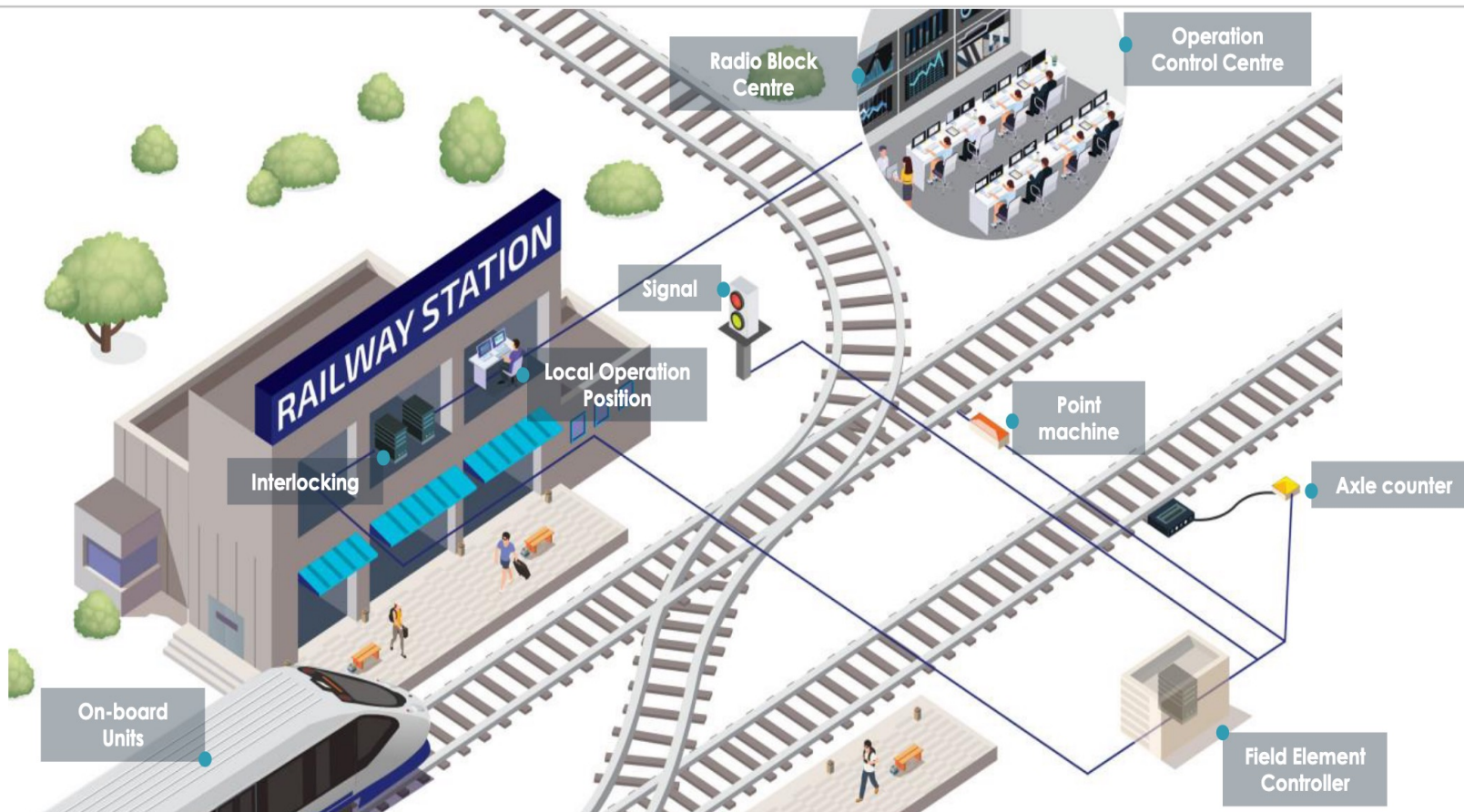
Standardised interfaces

Core business of EULYNX are standardised interfaces:

- ✓ **Functional interface (SCI): for signalling information**
- ✓ **Diagnostic interface (SDI): for monitoring and diagnostic information**
- ✓ **Maintenance interface (SMI): for engineering, configuration and software data of subsystems**

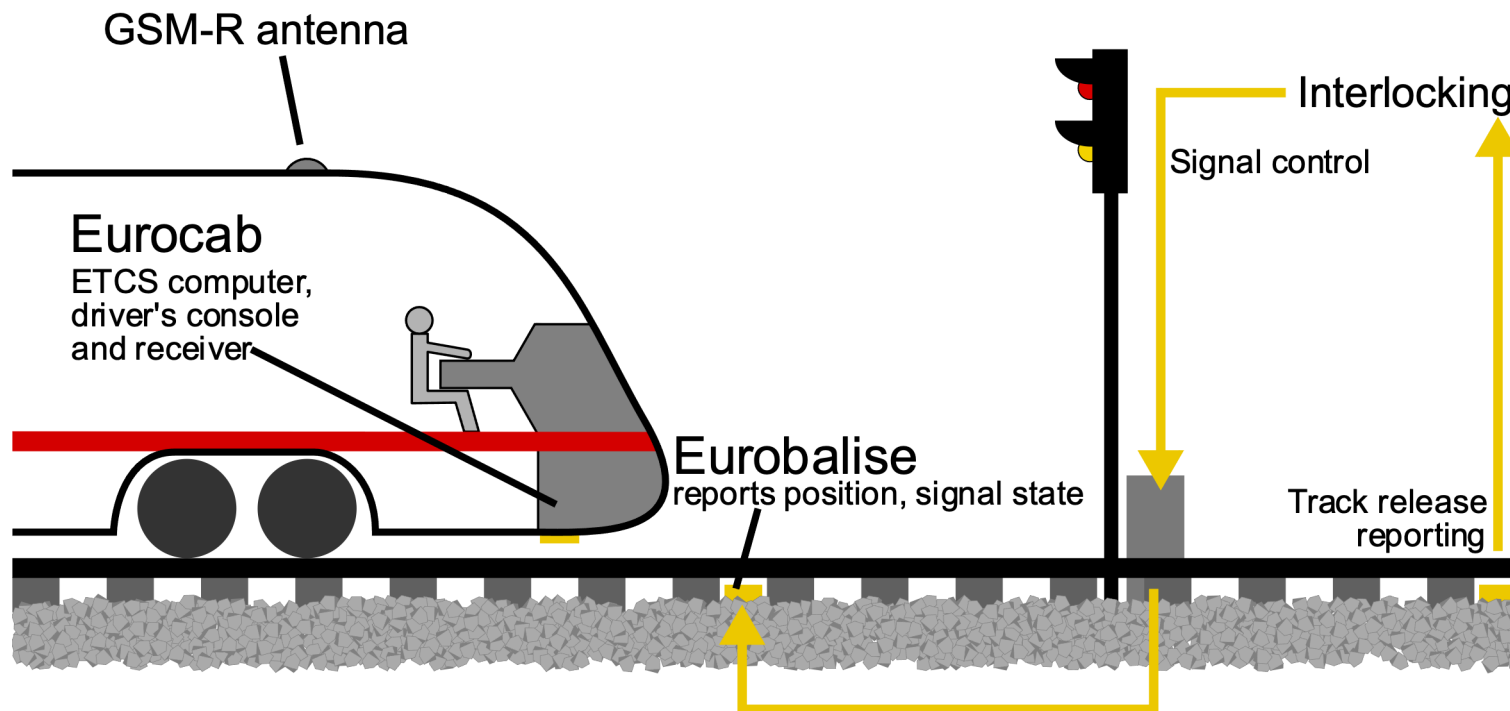
RaSTA: Rail Safe Transport Application network protocol

Railway: A Distributed Component-based System













**Digital Railway
Operation**

Railway: A Distributed Component-based System



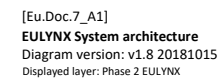
**Digital Railway
Operation**

The EULYNX Initiative: European Rail Agencies are Pushing Interoperability and Standardization

Factor	Current situation	EULYNX
Common Architecture	 Not available	 Standard architecture
European Standards	 Weak and incoherent	 Implemented and ready for Plug and play
Formal Methods	 In its infancy	 Established
Time to market	 Not transparent and hardly predictable	 Pilots successfully in operation, shortening time to market
Lifecycle	 System life time imposed by interlocking life time	 Independent life times of modules

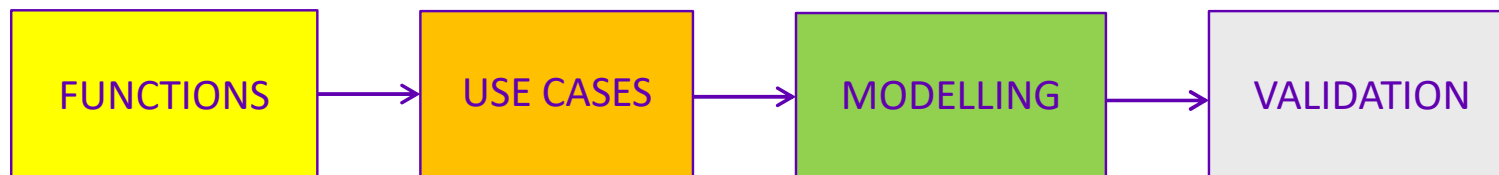
Source

**Digital Railway
Operation**



Unambiguous specifications

- ✓ EULYNX applies the Model-Based Systems Engineering (MBSE) methodology. This methodology is closely oriented on the life cycle phases defined in EN 50126.
- ✓ EULYNX delivers validated specifications in a modelled format. Modelled specifications are executable and can thus be tested to ensure that the behavior meets the users' needs.



EULYNX Object Controllers in our Lab



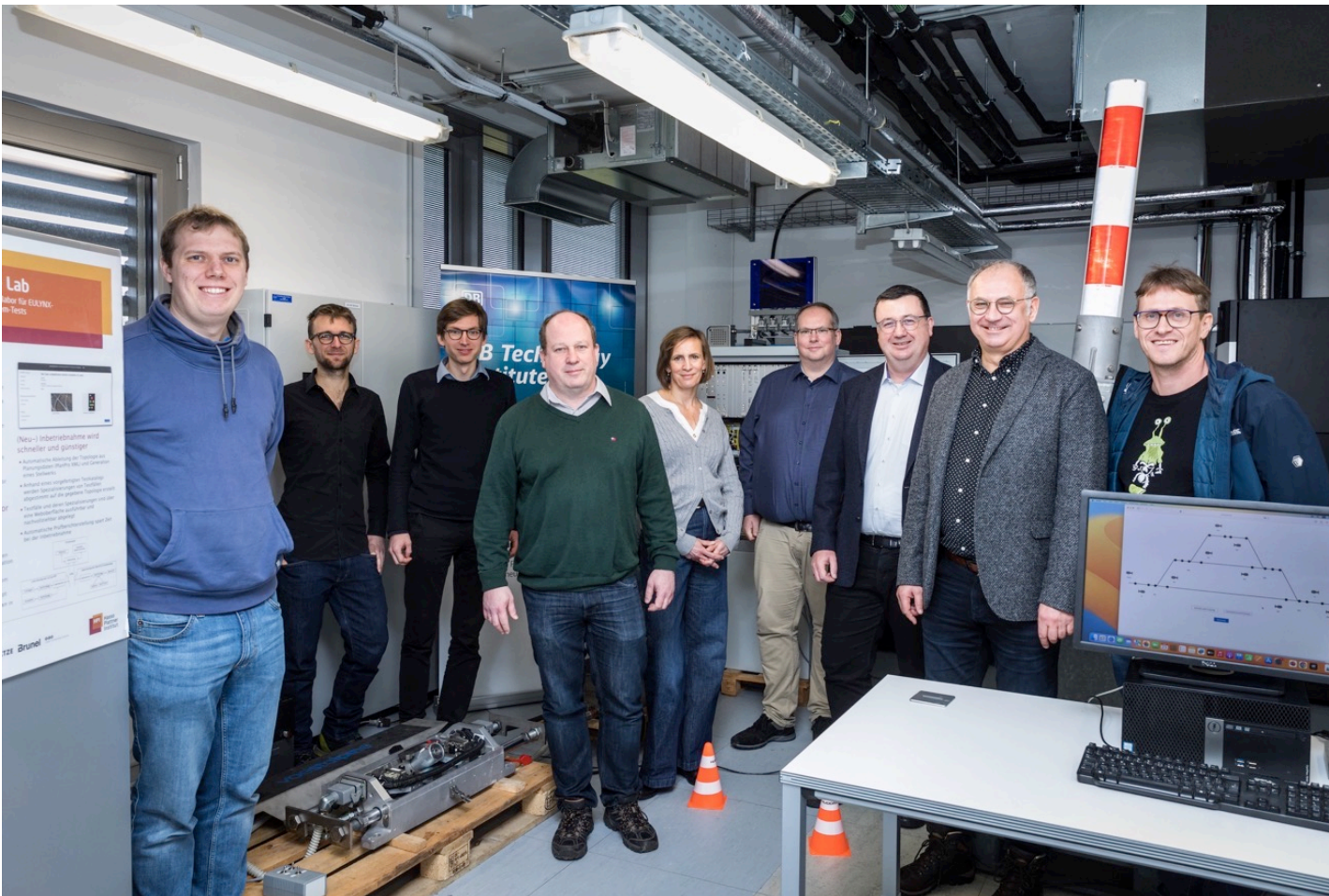
Frauscher Advanced Counter FAdC
Axle Counting Object Controller



Thales AzLM
Axle Counting Object Controller

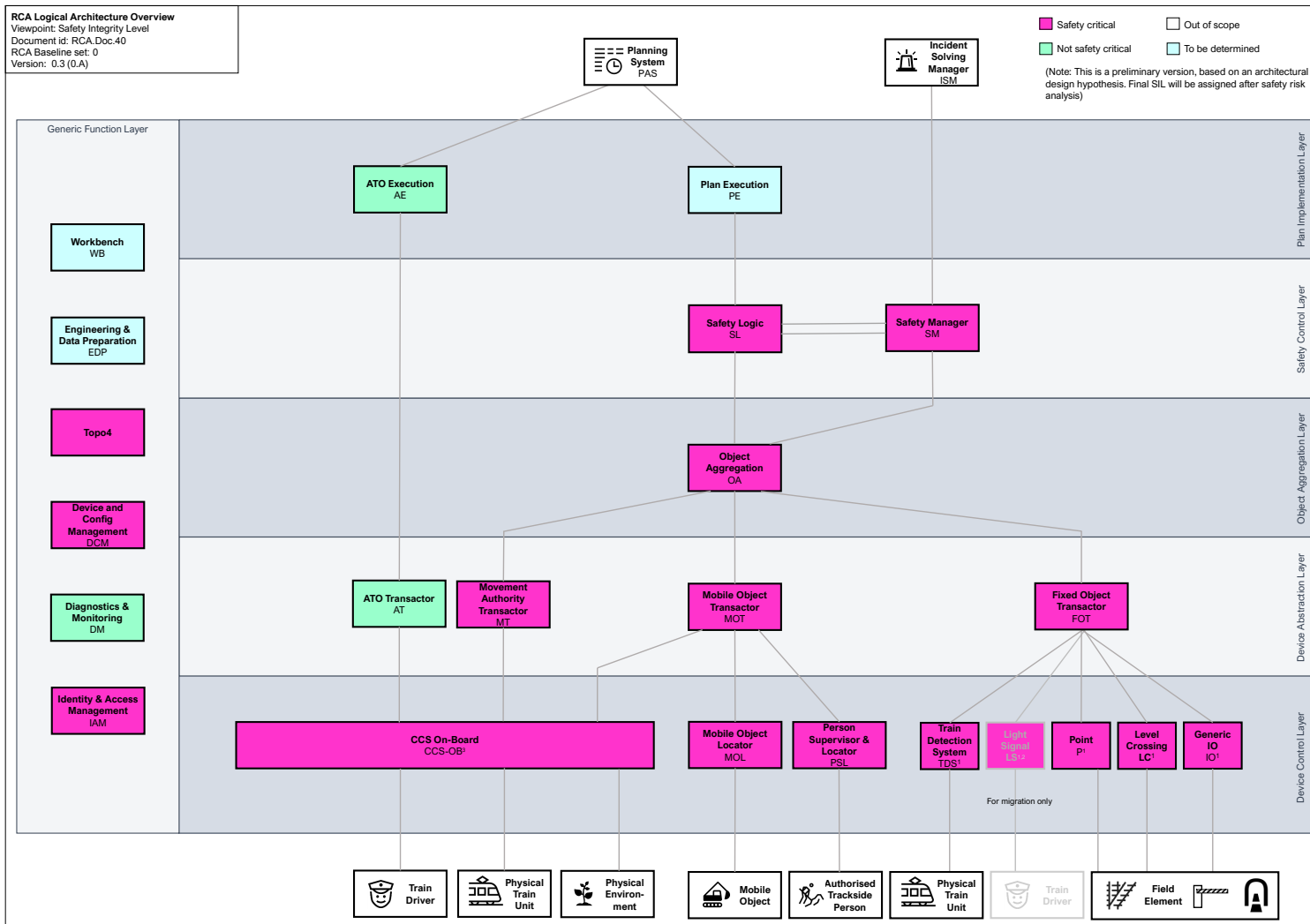
**Digital Railway
Operation**

Digital Rail Lab



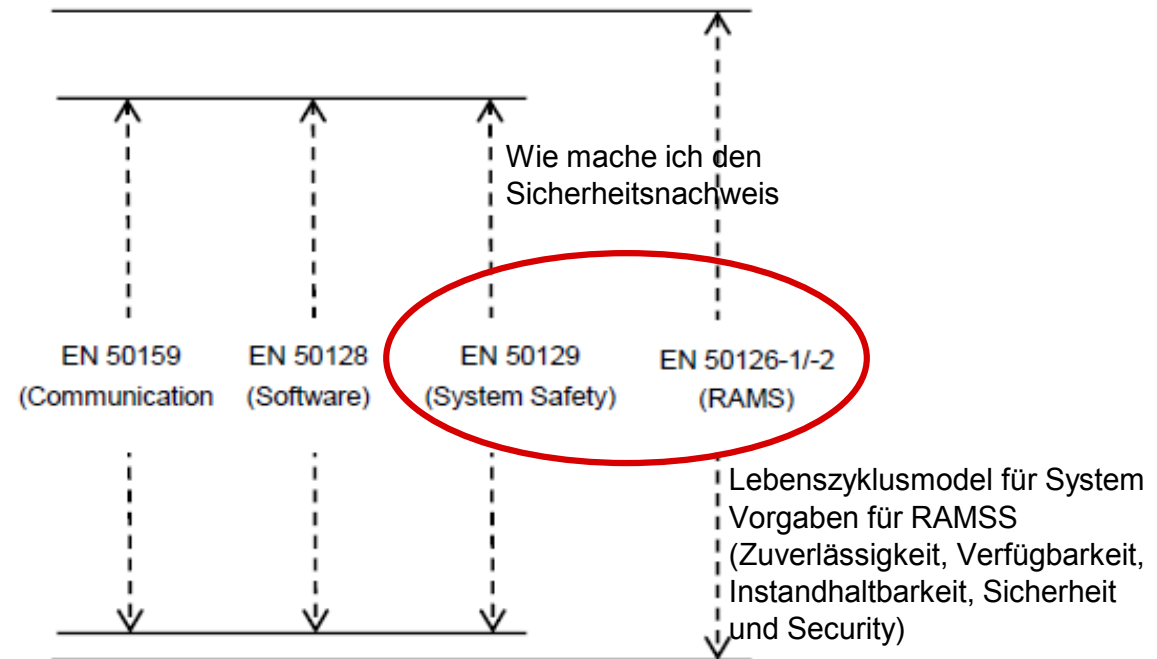
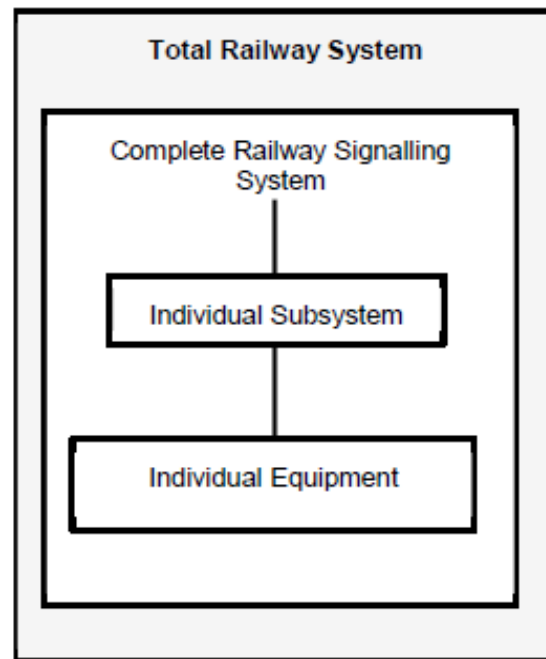
- Digital Rail Lab @ HPI
- Eisenbahninformatik.de

Reference Command, Control and Signalling Architecture (RCA)



Digital Railway Operation

Introduction to Development of Safety-Critical Software



Basisnorm: EN 61508
Funktionale Sicherheit

Figure 1 – Scope of the main CENELEC railway application standards

Source

Quelle: EN 50129:2016

Introduction to Development of Safety-Critical Software

Before software development, several phases have to be completed at system level.



These serve as input for software development.

- 1. Phase 1: System Concept
- 2. Phase 2: System Definition and Operational Context
- 3. Phase 3: Risk Analysis and Assessment
- 4. Phase 4: Defining System Requirements
- 5. Phase 5: Architecture and Partitioning of System Requirements

**Digital Railway
Operation**

[Source](#)

Introduction to Development of Safety-Critical Software



Table 2 — SIL quantitative and qualitative measures

TFFR [h^{-1}]	SIL attribution	SIL qualitative measures
$10^{-9} \leq \text{TFFR} < 10^{-8}$	4	Defined in sector-specific standards
$10^{-8} \leq \text{TFFR} < 10^{-7}$	3	
$10^{-7} \leq \text{TFFR} < 10^{-6}$	2	
$10^{-6} \leq \text{TFFR} < 10^{-5}$	1	

THR: Tolerable Hazard Rate (tolerierbare Gefährdungsrate)

TFFR: Tolerable Functional Failure Rate

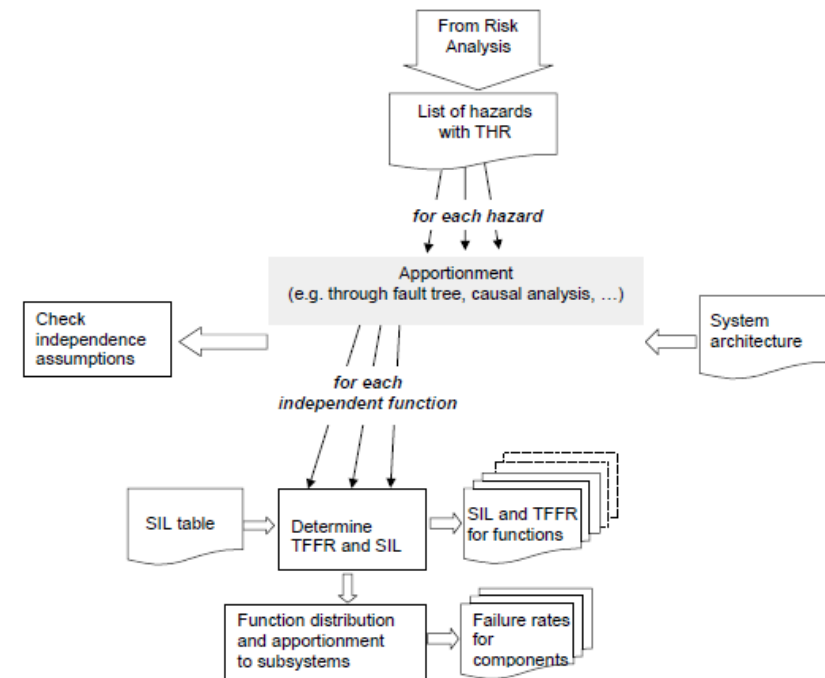
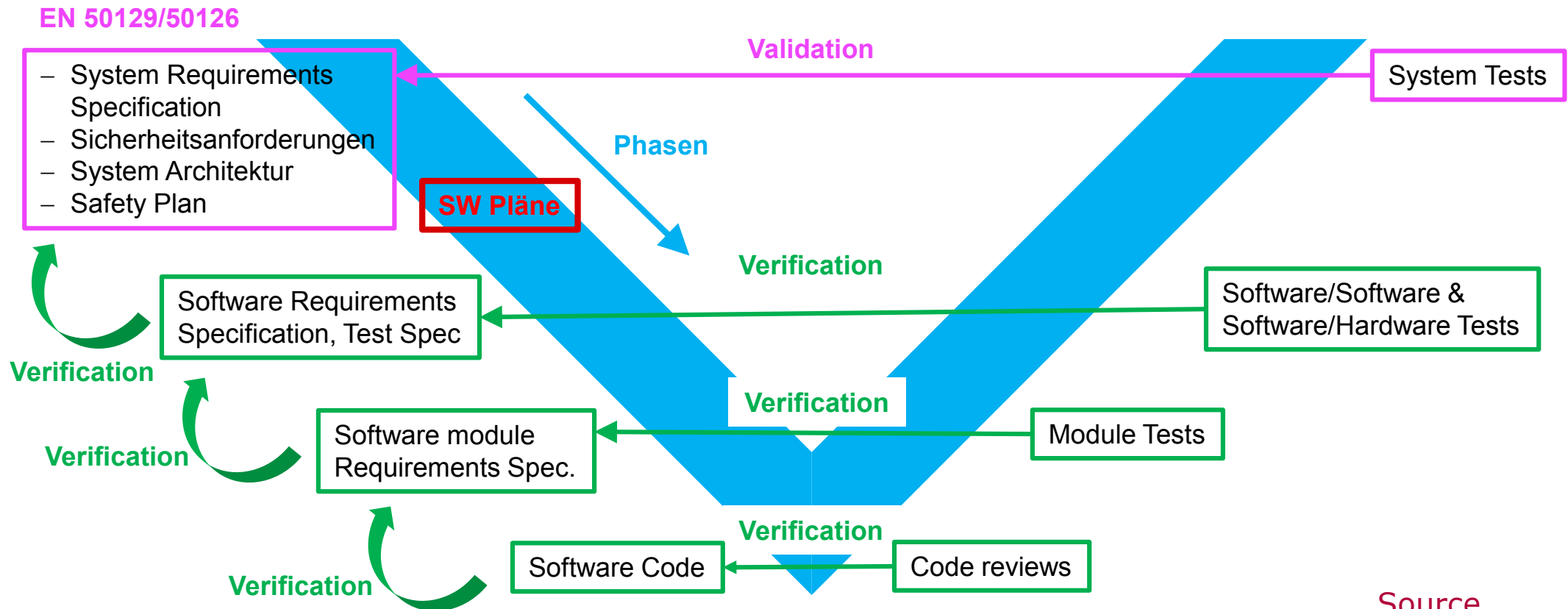


Figure 10 — Apportionment of functional safety requirements

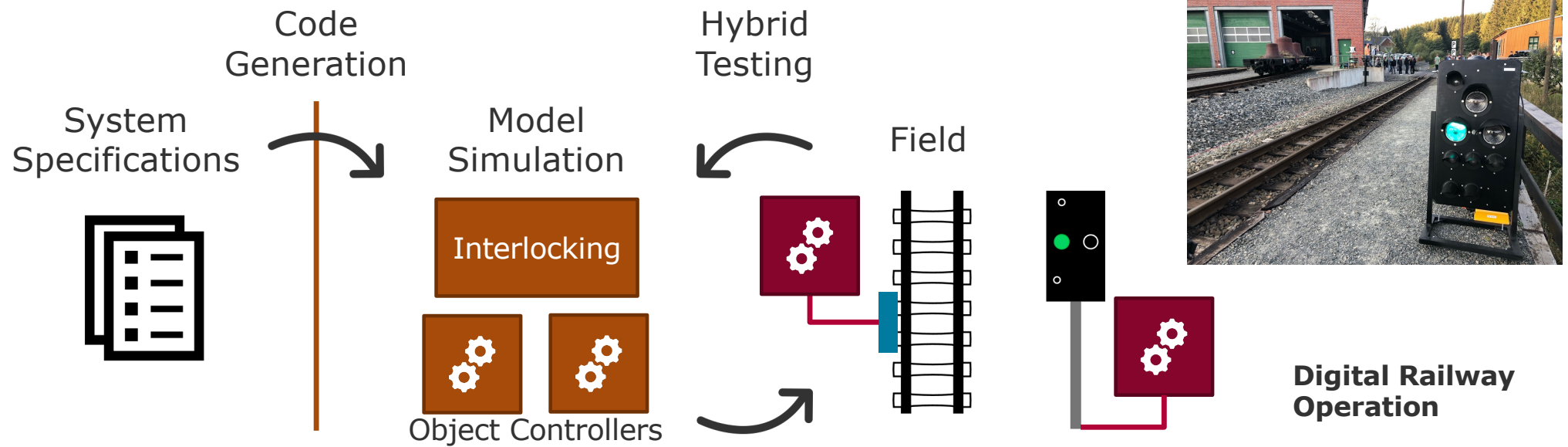
Source

Introduction to Development of Safety-Critical Software



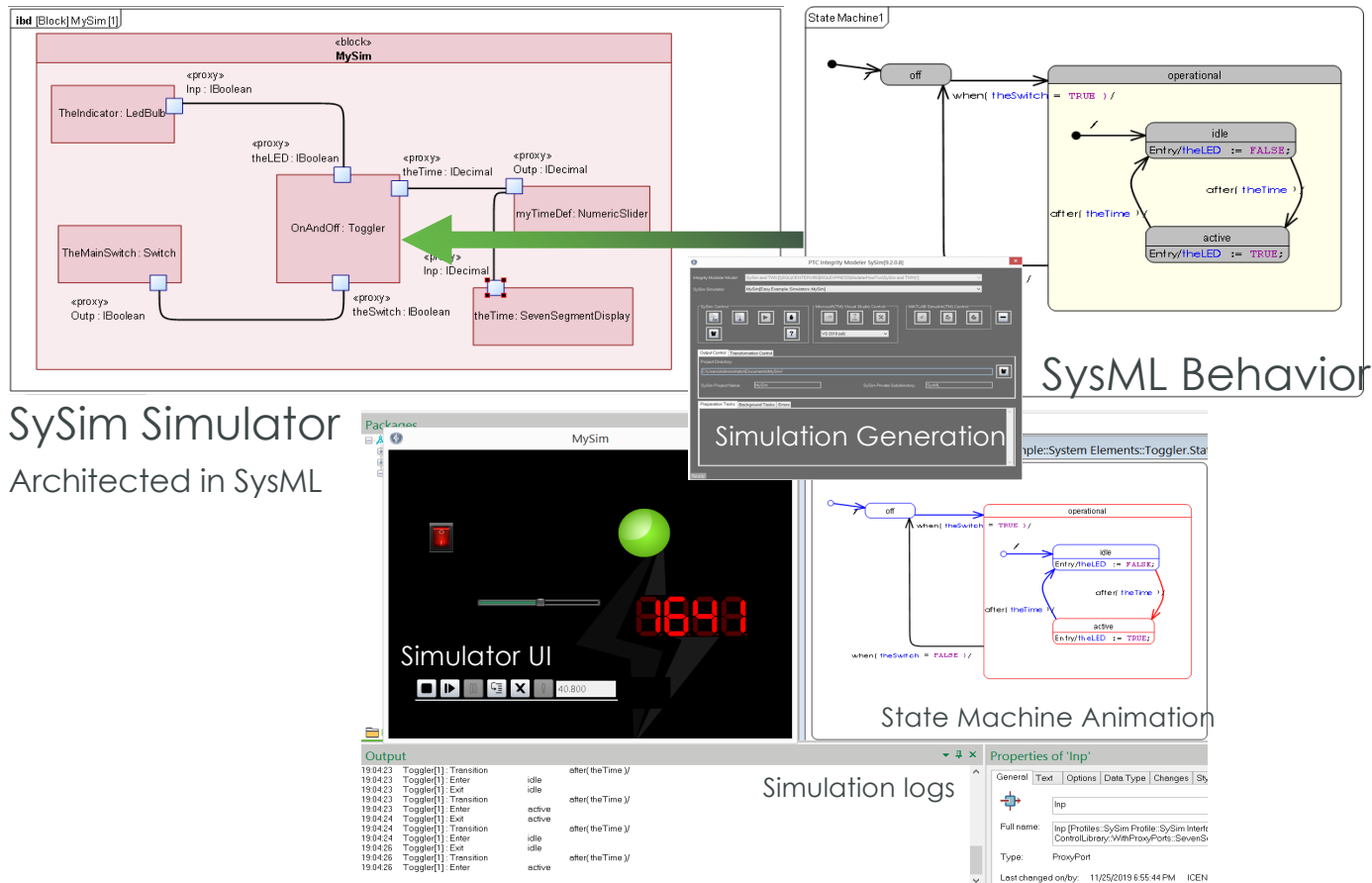
Source

EULYNX Live: A Shortcut in the V-Model Development Process



EULYNX Live: MBSE

Creating Executable Specifications from SysML Models



Digital Railway Operation

EULYNX: Protocol Stack and Communication Interfaces

Application Protocol: Subsystem
Communication Interfaces (SCI)

- SCI-Point, SCI-Train Detection System, SCI-Light Signal, ...
- Event-based

Transport Protocol: Rail Safe
Transport Application (RaSTA)

- Safe Transmission and Redundancy
- DIN VDE V 0831-200
- RaSTA over UDP
- RaSTA over TCP/TLS (since EULYNX Baseline 4.1)

SCI-*

RaSTA

**UDP or
TCP/TLS**

IP, Ethernet

**Digital Railway
Operation**

Example: Establish Connection between Interlocking and Field Element Subsystem

sd EfeSUC1.2 - Main Success Scenario [EfeS SD 1.2.1]

Main Success Scenario: Establish PDI connection

Precondition:

The **EULYNX field element Subsystem** is in the **INITIALISING** state.
Ready to establish **PDI** connection.

Interaction 1.2.1.A:

1. - The **EULYNX field element Subsystem** detects that the **SCP** connection to the **Subsystem - Electronic Interlocking** has been established.

Interaction 1.2.1.B:

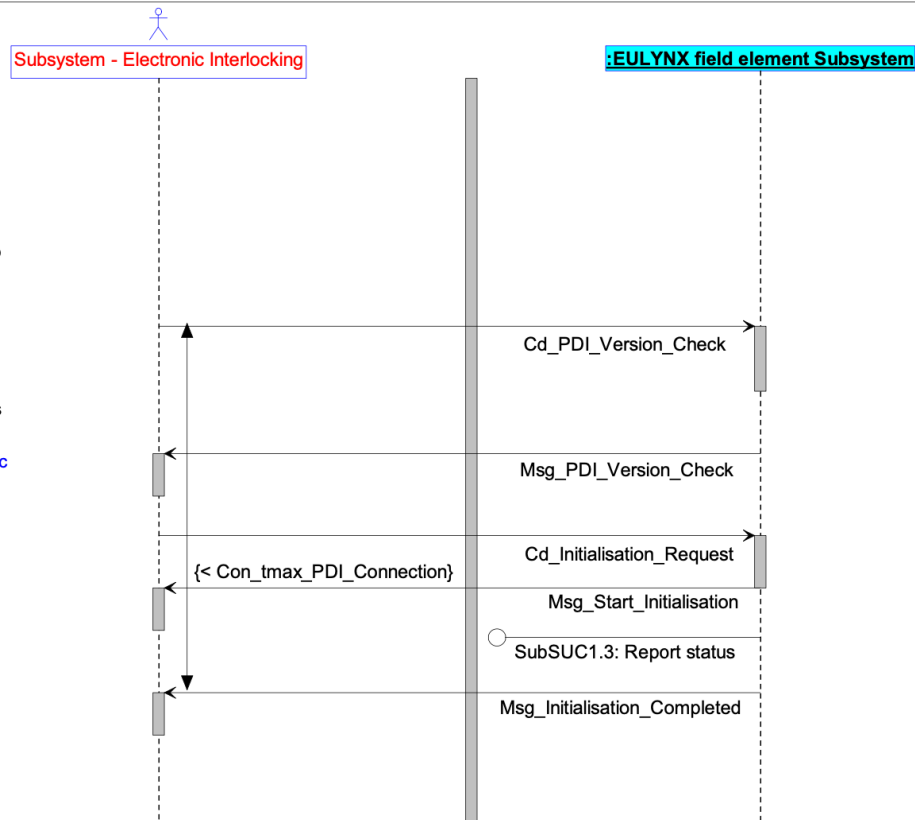
2. - The **EULYNX field element Subsystem** receives from the **Subsystem - Electronic Interlocking** the request to verify the match between the transmitted **PDI** and the **PDI** present in the **EULYNX field element Subsystem**.
3. The **PDI** transmitted by the **Subsystem - Electronic Interlocking** matches the own **PDI**.
4. The **EULYNX field element Subsystem** reports to the **Subsystem - Electronic Interlocking** the used **PDI** and newly calculated **CSS**.

Interaction 1.2.1.C:

5. - The **EULYNX field element Subsystem** receives from the **Subsystem - Electronic Interlocking** the request to transmit the status.
6. The **EULYNX field element Subsystem** notifies the **Subsystem - Electronic Interlocking** of the transmission of the status information.
7. The **EULYNX field element Subsystem** reports the status information to **Subsystem - Electronic Interlocking**. <<include>> **SubSUC1.3: Report status**
8. The **EULYNX field element Subsystem** notifies the **Subsystem - Electronic Interlocking** that the transmission of the status information is complete.
9. The event **T9_PDI_Connection_Established** is triggered.

Postcondition:

The **PDI** connection is established.



Example: Command Point

SubSUC2.1: Command Point

Main Success Scenario: Moving of the Point [SubSP SD 2.1.1]

Precondition:

The Subsystem - Point is in the state OPERATIONAL.

The Subsystem - Point is in:

- an End position "Y",
- No end position, or
- a Trailed position.

Interaction 2.1.1.A:

1. - The Subsystem - Electronic Interlocking sends a Command to the Subsystem - Point to move the Point to an End position "X".
2. The Subsystem - Point sends a Command to the Point machine to move the Point to an End position "X". At this moment the Subsystem - Point starts the timer Con_tmax_Point_Operation.

Interaction 2.1.1.B:

alt [The Subsystem - Point is in an End position or a Trailed position]

3. - The Point machine sends a Message to the Subsystem - Point indicating that the Point is in No end position.
4. The Subsystem - Point sends a Message to the Subsystem - Electronic Interlocking indicating that the Point is in No end position.

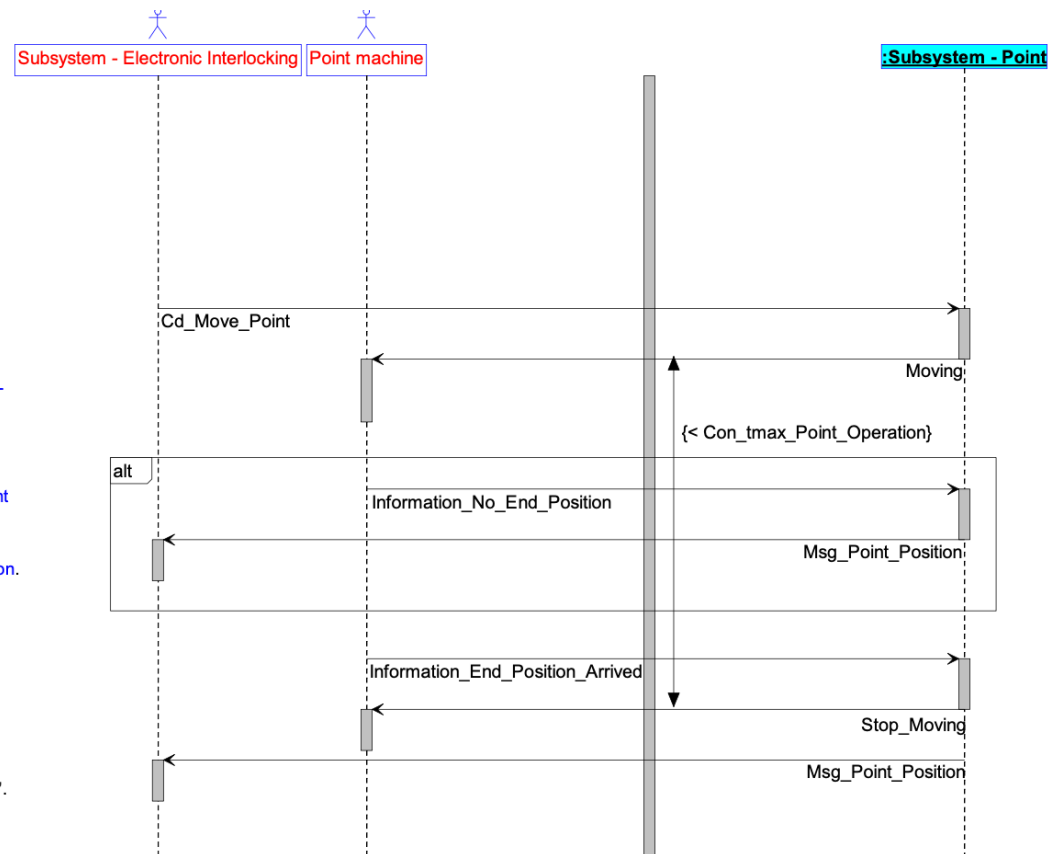
end alt

Interaction 2.1.1.C:

5. - The Point machine sends a Message to the Subsystem - Point indicating that the Point is in an End position "X".
6. The Subsystem - Point sends a Command to the Point machine to stop moving the Point. The timer Con_tmax_Point_Operation is reset.
7. The Subsystem - Point sends a Message to the Subsystem - Electronic Interlocking indicating that the Point is in an End position "X".

Postcondition:

The Subsystem - Point is in an End position "X".



Digital Railway Operation

Example: Command Point

■ Definition of SCI-P Protocol Messages

Telegram definition for command "Move Point"

Byte-Nr.	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
00	Protocol Type: 0x40 (1 Byte binary)							
01..02	Message Type: 0x0001 (2 Bytes binary)							
03..22	Sender Identifier (20 Bytes ISO IEC 8859-1:1998)							
23..42	Receiver Identifier (20 Bytes ISO IEC 8859-1:1998)							
43	Commanded Point Position (1 Byte binary)							

Telegram definition for message "Point Position"

Byte-Nr.	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
00	Protocol Type: 0x40 (1 Byte binary)							
01..02	Message Type: 0x000B (2 Bytes binary)							
03..22	Sender Identifier (20 Bytes ISO IEC 8859-1:1998)							
23..42	Receiver Identifier (20 Bytes ISO IEC 8859-1:1998)							
43	Reported Point Position (1 Byte binary)							

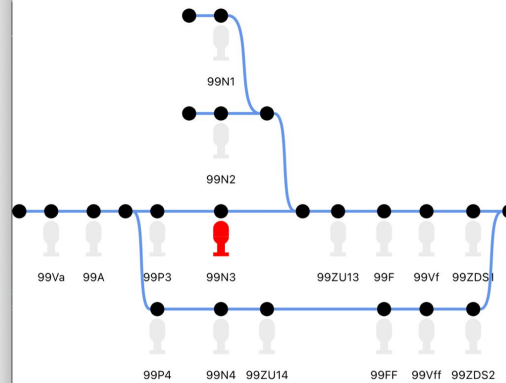
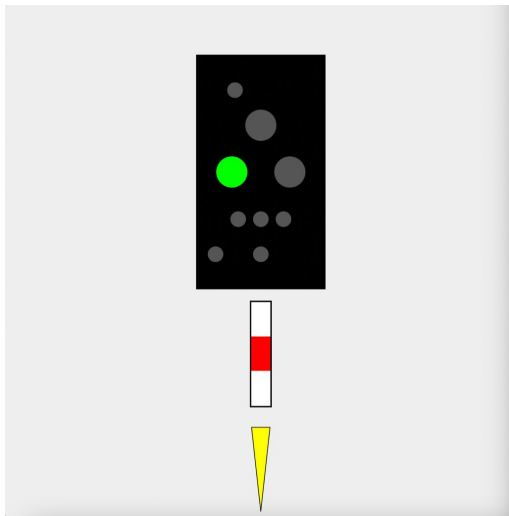


**Digital Railway
Operation**

Project Hackathon



Technology Institute



DRSS - Hackathon: RaSTA

Jonas Bücker, Mario Freund, Leonhard Hennicke

**Digital Railway
Operation**

EULYNX & IT Security: Protocol Stack and Communication Interfaces

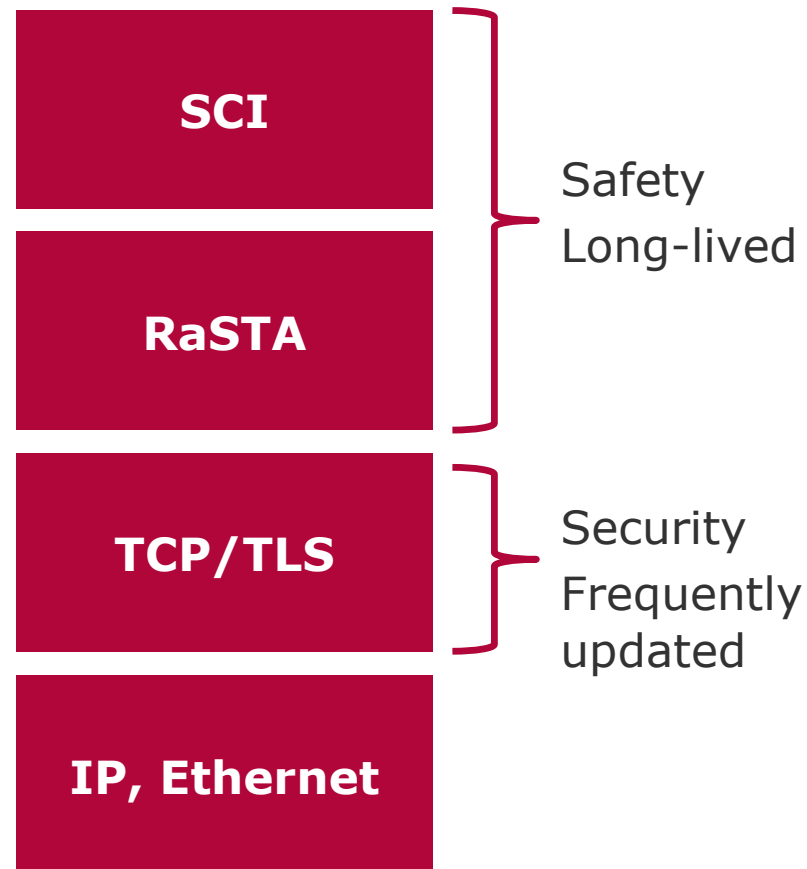
Event-based Protocols

Application Protocols: Subsystem Communication Interfaces (SCI)

- SCI-Point, SCI-Train Detection System, SCI-Light Signal, ...

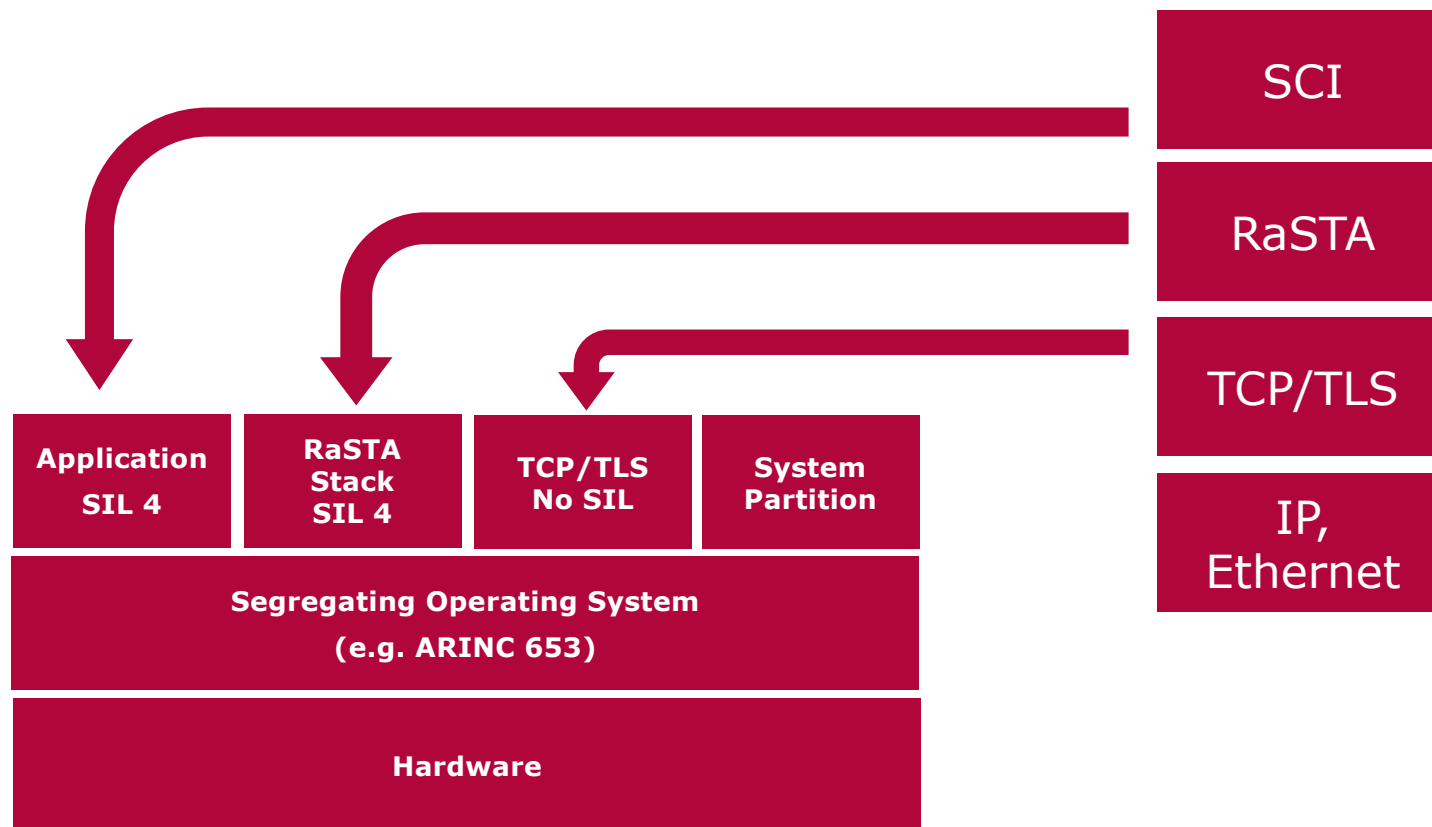
Transport Protocol: RaSTA (Safe Transmission and Redundancy)

- DIN VDE V 0831-200
- RaSTA over UDP
- RaSTA over TCP/TLS (since EULYNX Baseline 4.1)



**Digital Railway
Operation**

Running SIL and non-SIL Components Side by Side: Software-based Segregation



**Digital Railway
Operation**

Agenda

- EULYNX - Digital Railway Operation
- **ENISA report - Security measures in the Railway Transport Sector**
- RailSecurity
- Paradigm shift: from GIuV to permanent consistency checking
...“Using Simplicity to Control Complexity” (Lui Sha, IEEE Comp., 2001)
- Physical Security - Digitalization weakens systems
- NIS2 - The European CyberSecurity Act

Figure 6: Overview of railway systems

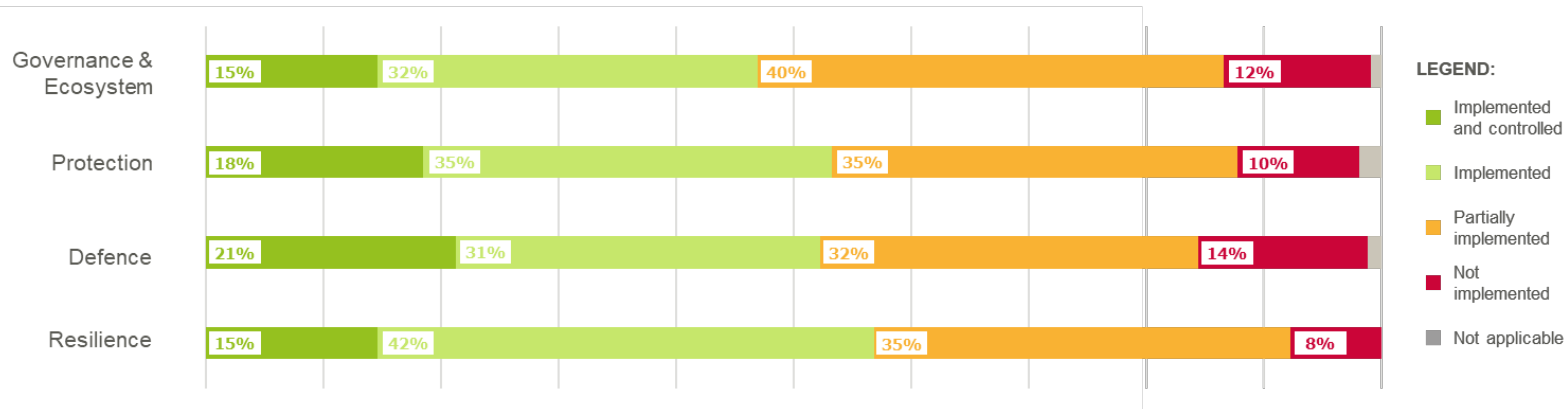


Figure Note: Background colours indicate the actor who is usually in charge of the system (this could vary according to the organisation or project). A coloured pastille shows the most likely location of the system; some systems have assets in several locations. ERTMS is considered as it is the ATC that is harmonised for EU. The scope of the ERTMS is depicted with a light blue colour, covering Signalling and Radio systems.

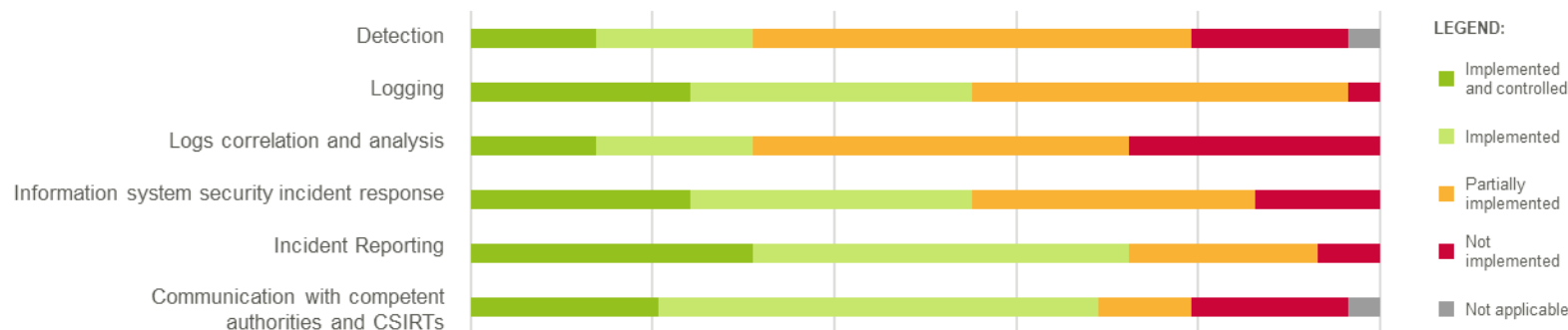
Cybersecurity Challenges

- Low digital and cybersecurity awareness in the railway sector.
- Difficulty in reconciling safety and cybersecurity worlds.
- Digital transformation of railway core business.
- Dependence on the supply chain for cybersecurity.
- Geographic spread of railway infrastructure and the existence of legacy systems.
- The need to balance security, competitiveness and operational efficiency.
- Complexity of regulations for cybersecurity.

Implementation level of CyberSecurity Measures



Implementation Level of „Defence“ Security Measures



**Digital Railway
Operation**

ERTMS

The European Rail Traffic Management System (ERTMS) is a single European signalling and speed control system that ensures interoperability of the railway systems, with the aim of reducing the purchasing and, possibly, maintenance costs of the signalling systems.

- European Train Control System (ETCS), i.e. a cab-signalling system that incorporates automatic train protection,
- Global System for Mobile communications for Railways (GSM-R) and operating rules.

ETCS (European Train Control System).

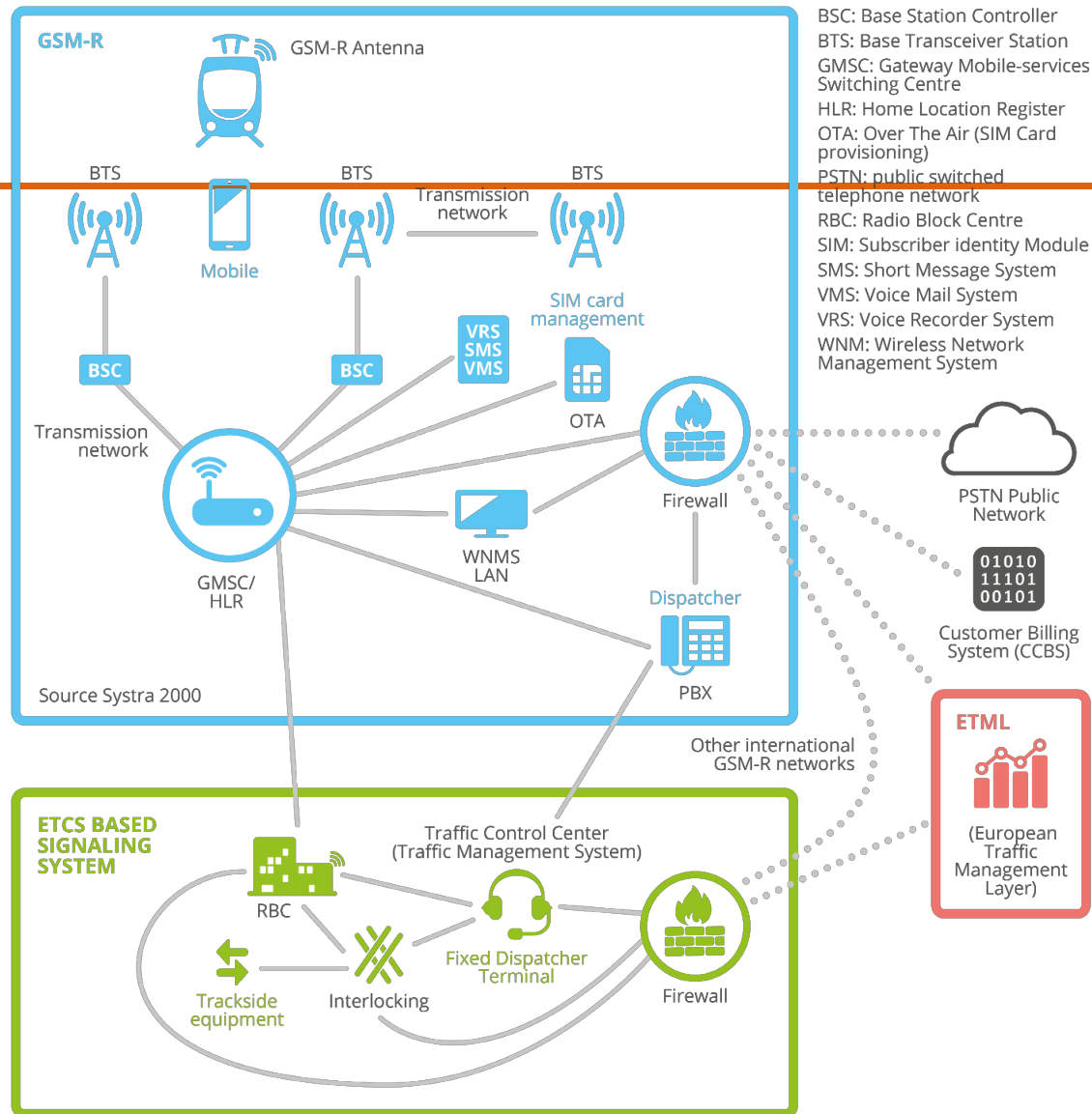
- The signalling element of the system
- Includes the control of movement authorities, automatic train protection and the interface to interlocking in a harmonised way.
- Reduction of complexity for train drivers (automation of control activities)
 - brings trackside signalling into the driver's cabin
 - provides information to the on-board display
 - allows for permanent train control
 - train driver concentrates on core tasks.

GSM-R (Global System for Mobiles - Railway)

A voice communication service between driving vehicles and line controllers and a bearer path for ETCS data.

- based on the public standard GSM with specific railway features for operation e.g. Priority and Pre-emption (eMLPP)
- Functional Addressing Location Dependent Addressing
- Voice Broadcast Service (VBS)
- Voice Group Call (VGC)
- Shunting Mode
- Emergency Calls
- Fast call set-up.
- General Packet Radio Service (GPRS option) can also be used in GSM-R networks to offer more data possibilities.

ERTMS



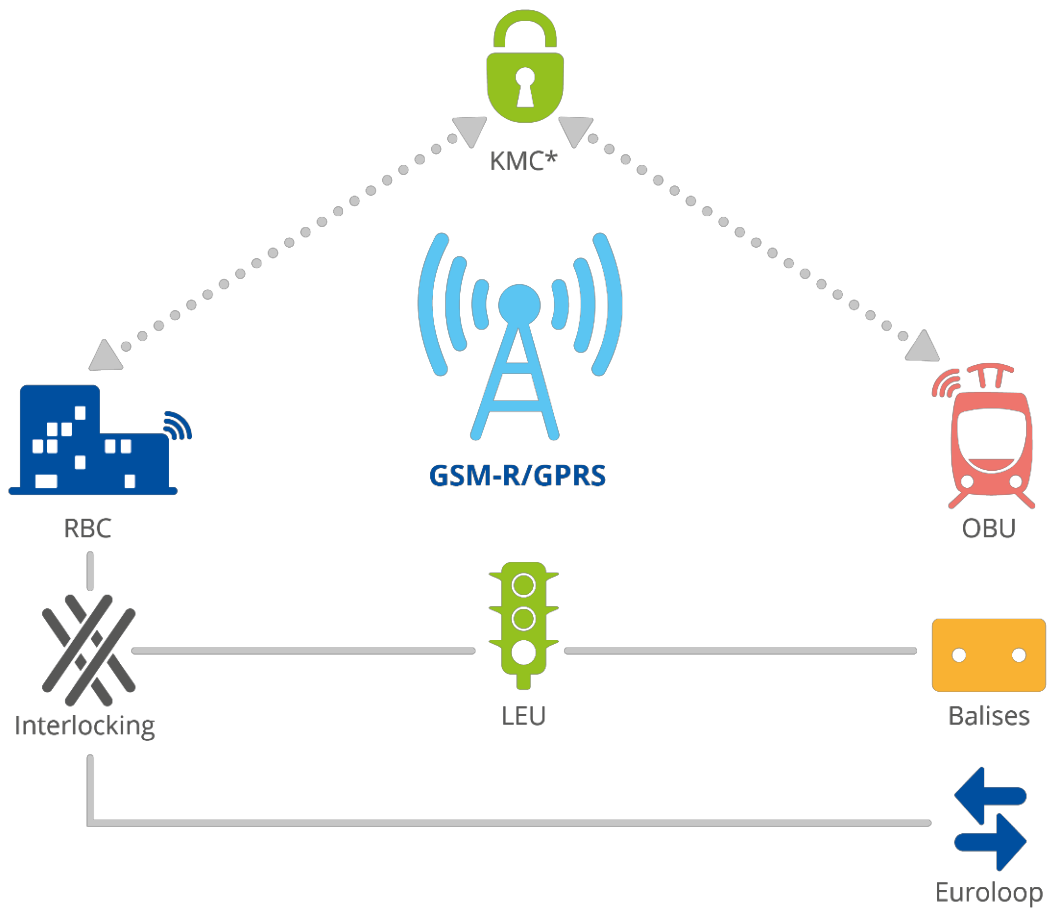
ERTMS systems

Digital Railway Operation

Communication subsystems and functions, that require protection:

- **Balise interfaces**
 - programming of balises
 - balise – infrastructure interface (train, interlocking, LEU, and/or field elements)
- **On-board unit (OBU) interfaces**
 - OBU – RBC via GSM-R or – in future – further data circuits according to the Future Railway Mobile Communication System (FRMCS)
 - OBU – vehicle bus system(s) (not ETCS-specific)
- **Radio block centre (RBC) interfaces**
 - RBC – OBU via GSM-R or – in future – further data circuits
 - RBC operator interface
 - RBC – interlocking
- **Key management centre (KMC) for the ETCS46**
 - operator interfaces, i.e. set-up keys and access authorisation
 - transmission of the keys to the operative subsystems, i.e. OBU and RBC o KMC-ETCS entities via GSM-R
 - KMC-KMC via different networks

Communication in the ERTMS

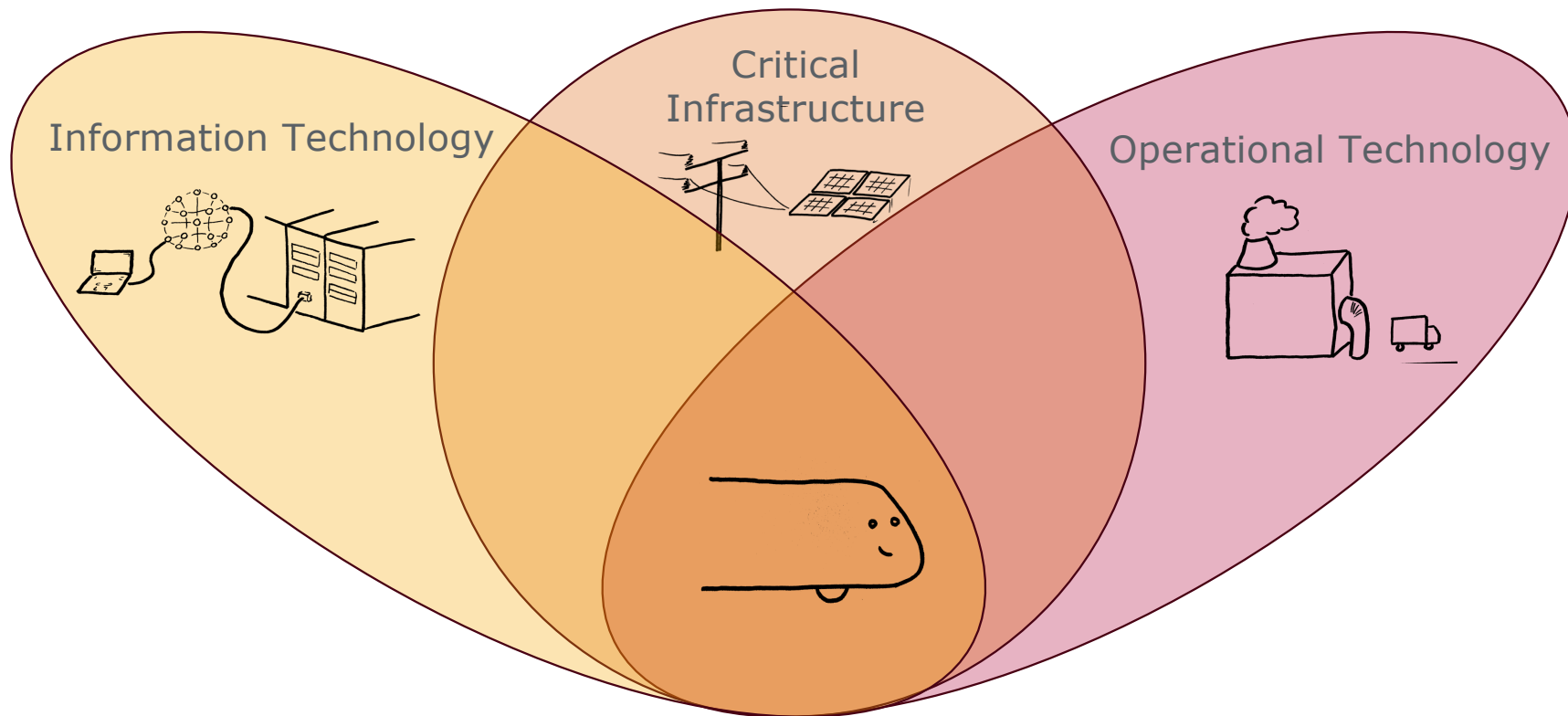


**Digital Railway
Operation**

Agenda

- EULYNX - Digital Railway Operation
- ENISA report - Security measures in the Railway Transport Sector
- **RailSecurity**
- Paradigm shift: from GIuV to permanent consistency checking
...“Using Simplicity to Control Complexity” (Lui Sha, IEEE Comp., 2001)
- Physical Security - Digitalization weakens systems
- NIS2 - The European CyberSecurity Act

Railway – A System of Systems



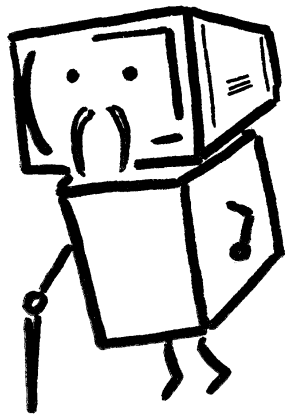
Why is railway not secure?

Identifying Challenges in Railsecurity

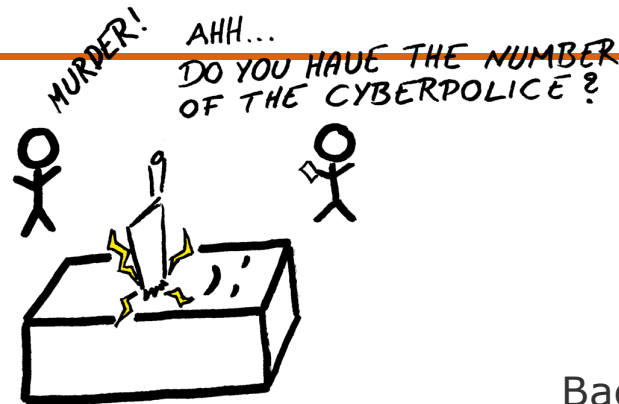
Katja Assaf and Andreas Polze
Planned for RSSRail 2025

What we See

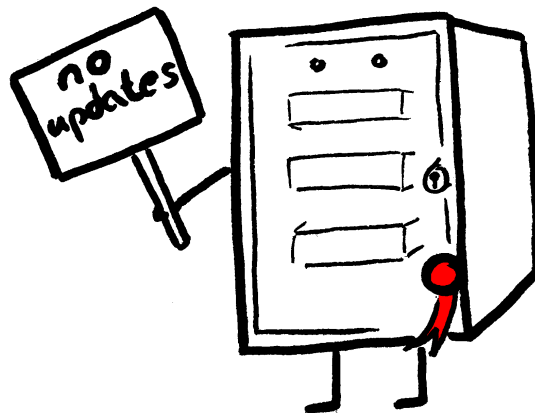
Missing emergency plan



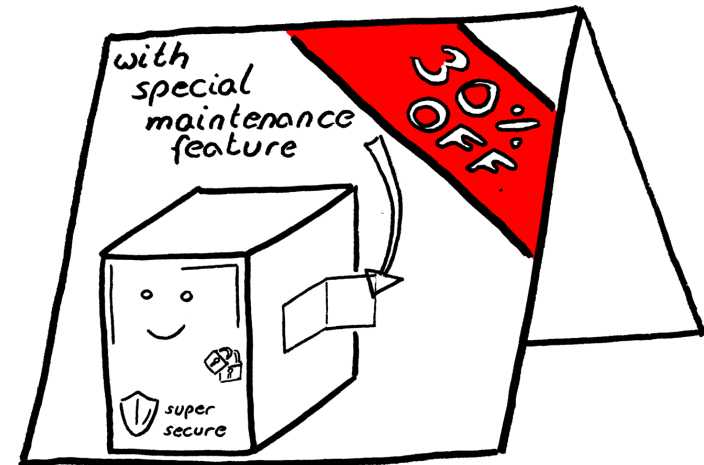
Old hardware



Old software



Backdoors

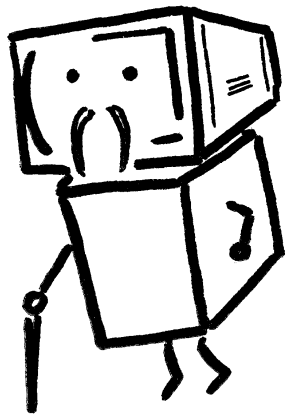


Digital Railway Operation

Awareness & Recovery Process

Missing emergency plan

Why do we See it

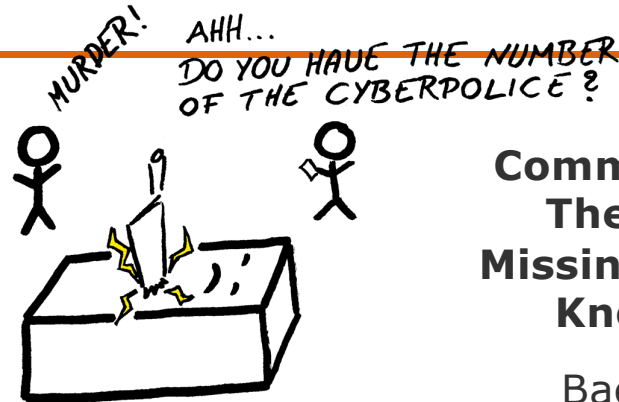
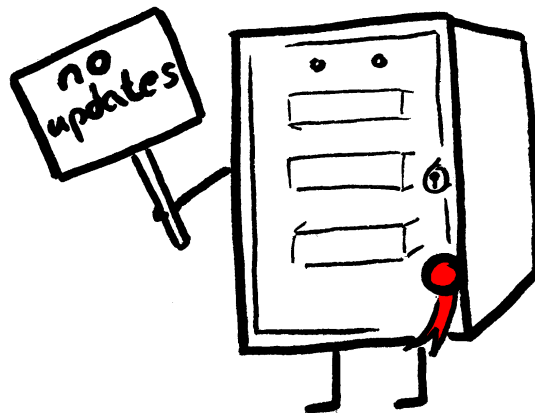


Old hardware

Legacy
& Long
Lifecycles

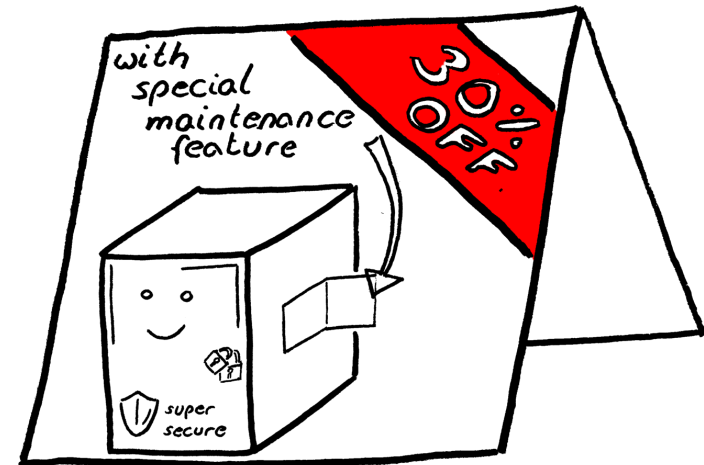
Certified &
Standardised
Software

Old software



Commercial Off-
The-Shelf &
Missing Technical
Know-How

Backdoors



What is the greatest challenge?

- Enough **Resources**: money and humans
- **Skilled Personnel** with **Awareness**
- Establishing **Basic Security**,
such as Asset Management, especially for Legacy Systems
- Network availability
- Remote Access (**Digitalization**)
- Vulnerability Management (**Updates**)
- **Safety-critical Impact**



Is safety a security goal?

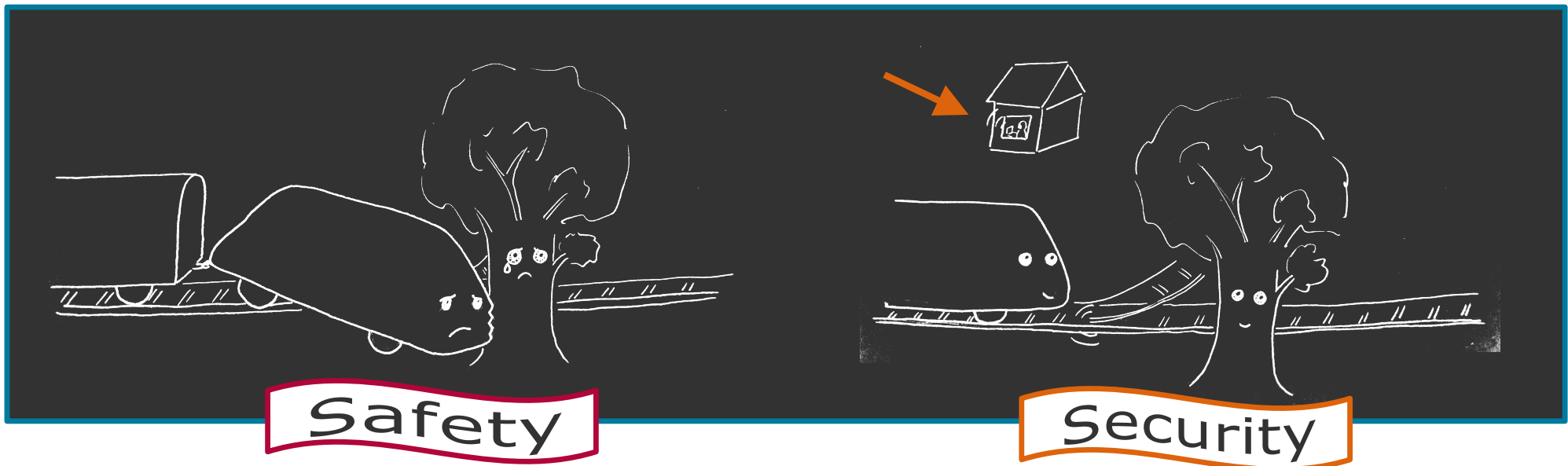
Defining Safety and Security Interaction Through A Multi-Level Attack-Fault-Graph

Katja Assaf, Christina Kolb, Simon Unger
Submitted to ESORICS 2025

What is Safety? What is Security?

Safety protects against **unintentional** failures,
Security protects against **malicious** intent.

Safety protects the **environment** from the system,
Security protects the **system** from the environment.

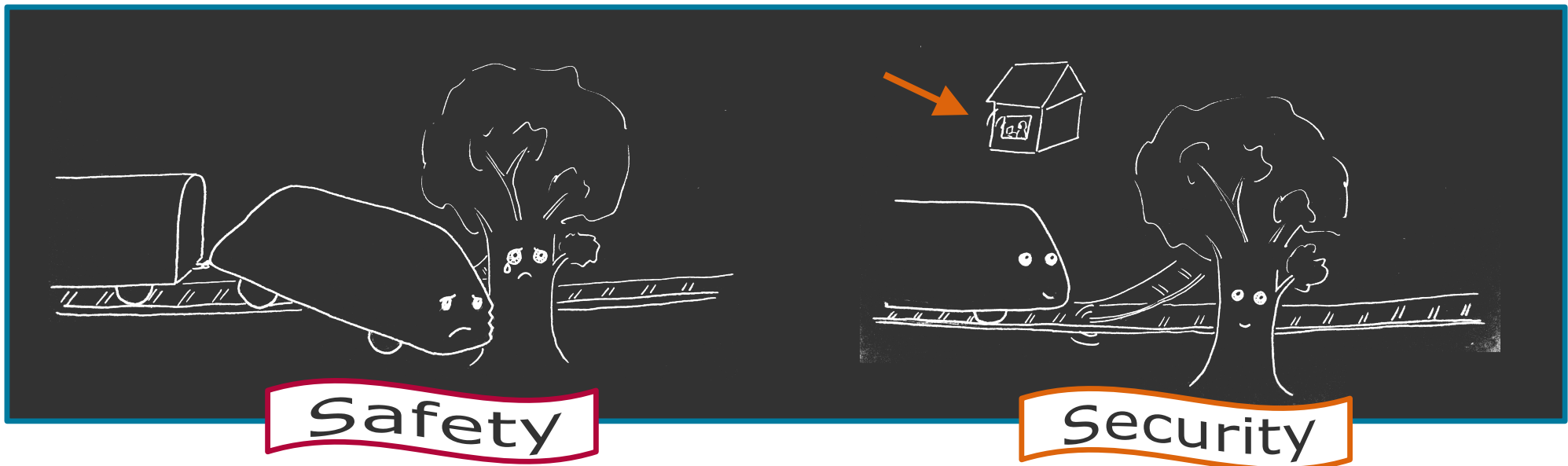


What is Safety? What is Security?

Security protects against **malicious** intent.

Safety protects the **environment/humans** from the system

- Safety and Security are not disjoint concepts!

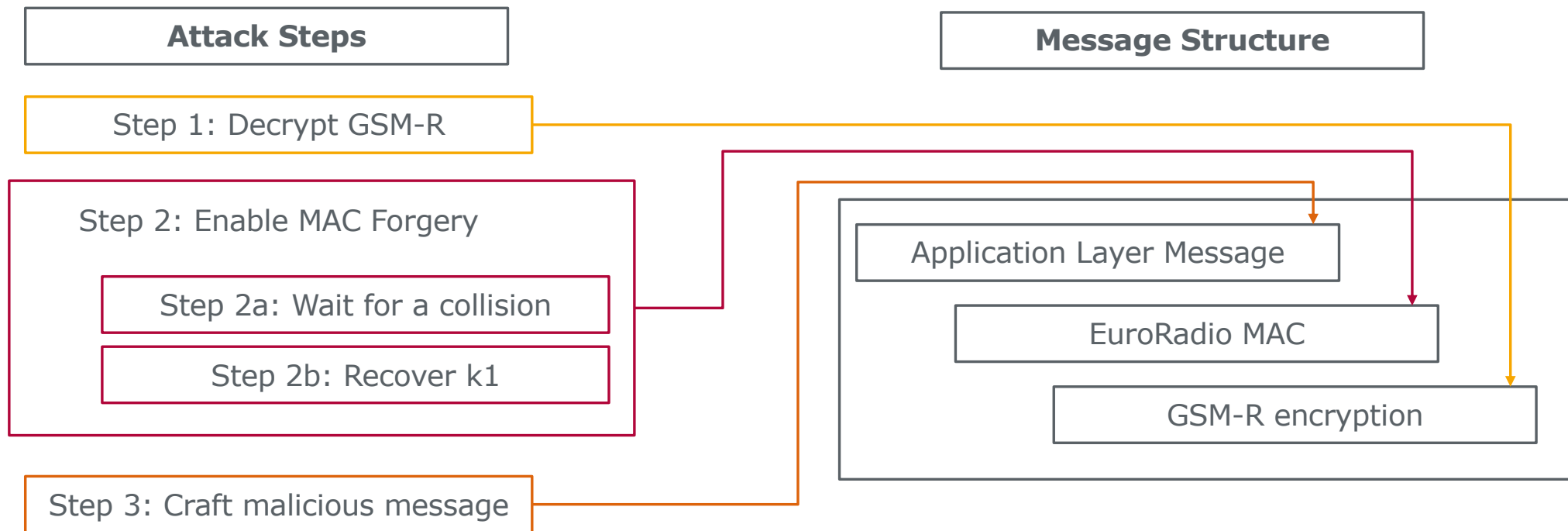


Let's steal a train!

Breaking GSM-R

Katja Assaf, Jörn Sobotta, Andreas Polze amongst others
Ongoing

COT17 attack



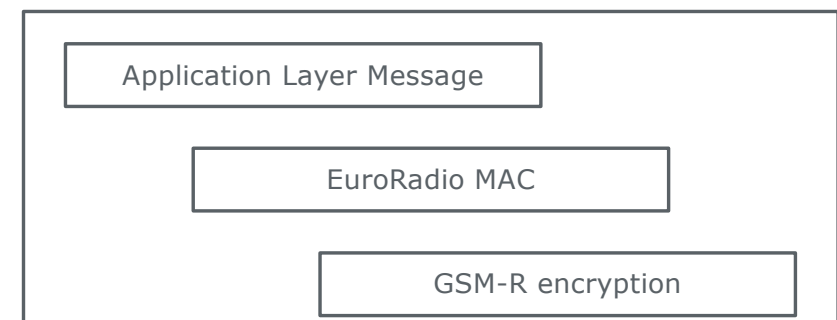
Chothia, T., Ordean, M., De Ruiter, J., & Thomas, R. J. (2017, April). An attack against message authentication in the ERTMS train to trackside communication protocols. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (pp. 743-756).

Railsecurity

Taking ETCS based on GSM-R as an Example



- GSM-R is a railway specific protocol based on GSM
- GSM A5/1 encryption is known to be broken (realtime)
- GSM A5/3 is vulnerable
- Vulnerability of GSM-R unproven for legal reasons
- ETCS uses a message authentication code (MAC) for integrity protection
- For safety-critical messages, such as emergency stop, the MAC is not checked
- Security significantly weakened for safety concerns
- MAC based on broken DES standard
- Proprietary protocols are a game of chance
Here: we got lucky so far



Goal:

Stealing a Train



HPI

1. Understand theoretical attack
2. Find legal test environment
3. Read GSM-R traffic with a Software Defined Radio
- 4. Understand practical implementation**
5. Use known Rainbow Table attack
6. Send Emergency Stop
7. Stop the Train
8. Collect enough data
9. Brute-force remaining key used for MAC
10. Forge Movement Authority
11. Steal the Train

We are here!

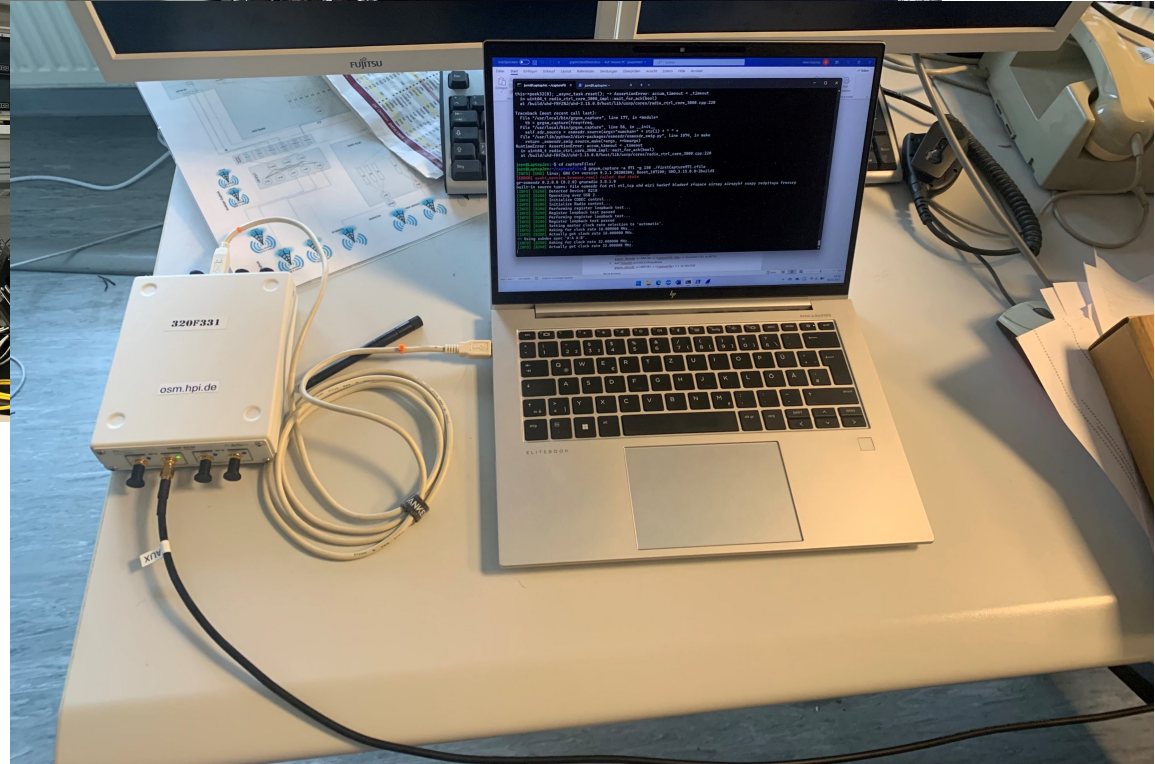
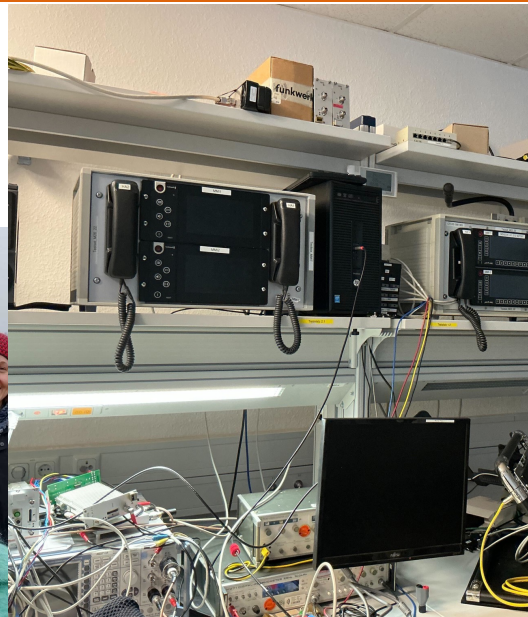


Excursion to Kölleda

Breaking GSM-R: Collecting data in GSM-R Lab

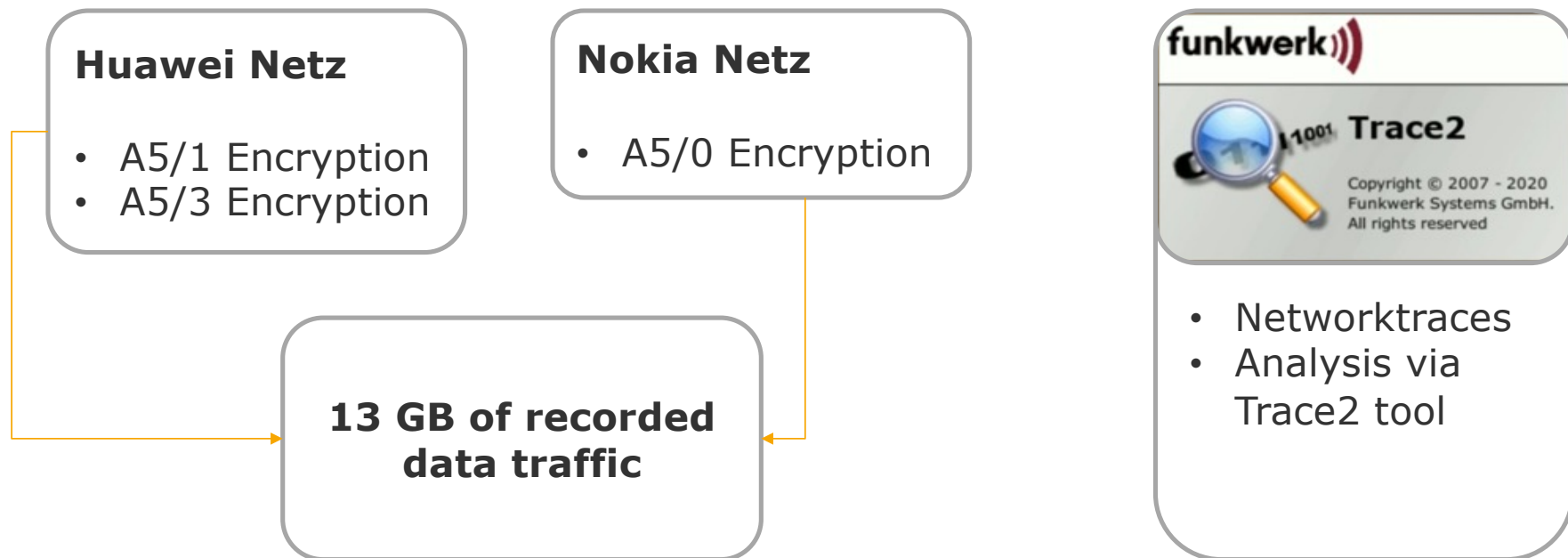
funkwerk

HPI



At Funkwerk

Breaking GSM-R: Collecting data in GSM-R lab



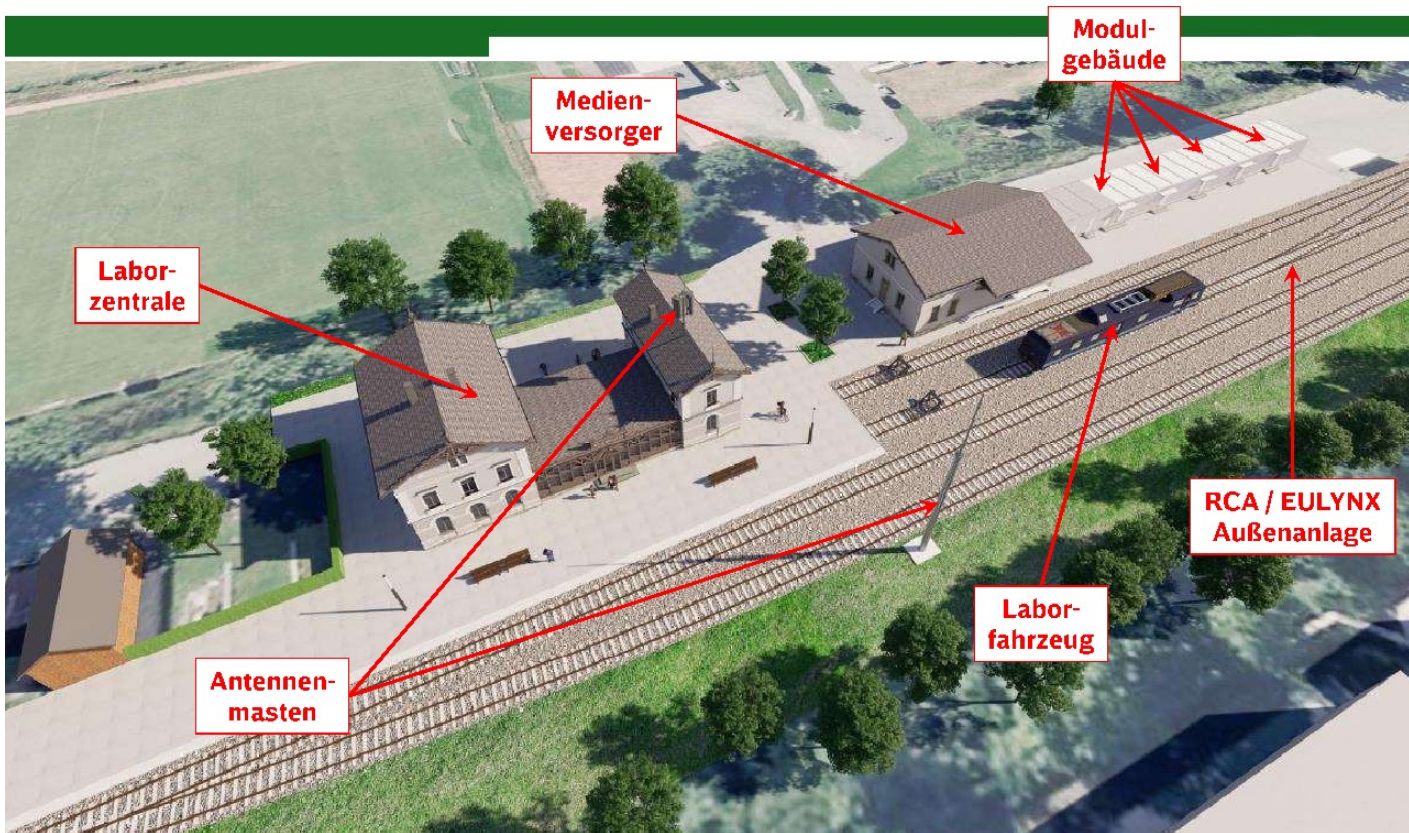
Agenda



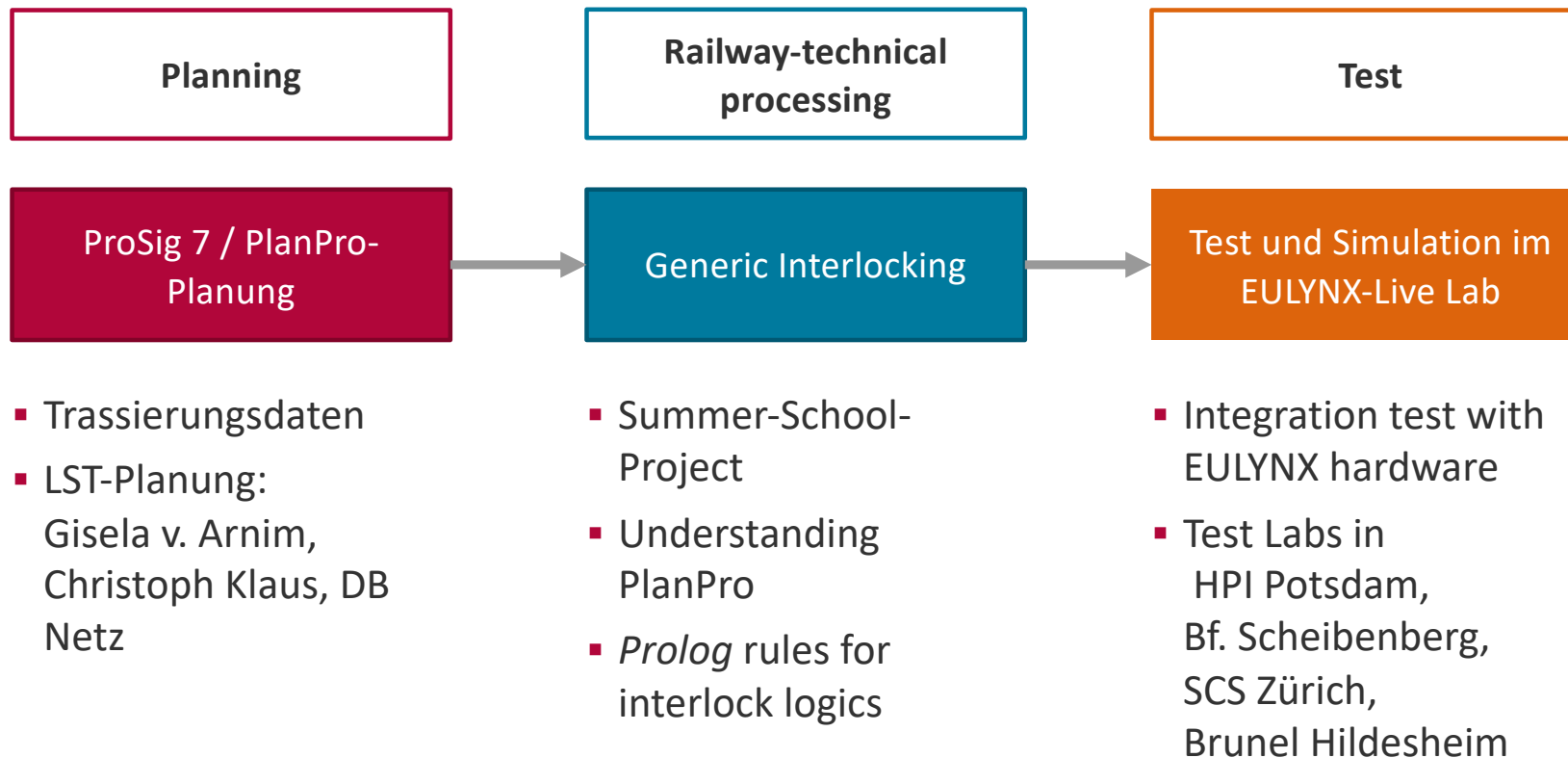
- EULYNX - Digital Railway Operation
- ENISA report - Security measures in the Railway Transport Sector
- RailSecurity
- **Paradigm shift: from GIuV to permanent consistency checking
...“Using Simplicity to Control Complexity” (Lui Sha, IEEE Comp., 2001)**
- Physical Security - Digitalization weakens systems
- NIS2 - The European CyberSecurity Act

Projekt EULYNX-Live (2021/2022)

A new (old) Scheibenberg station under construction

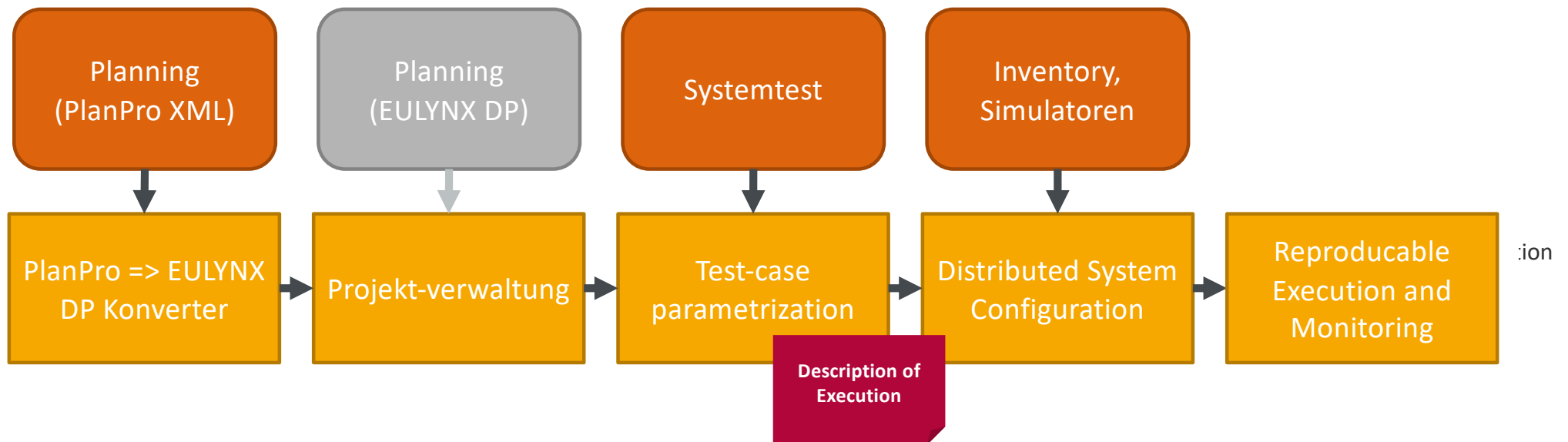
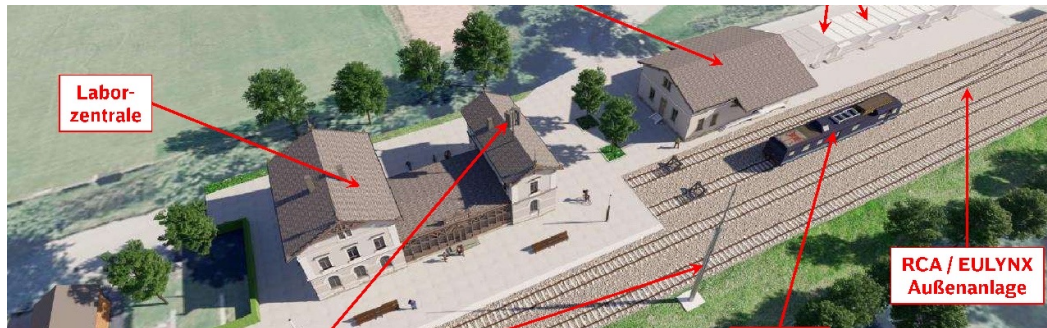


A new (old) Scheibenberg station under construction from digital planning to field test



EULYNX-Live Lab Demo

Simulation of Scheibenberg station



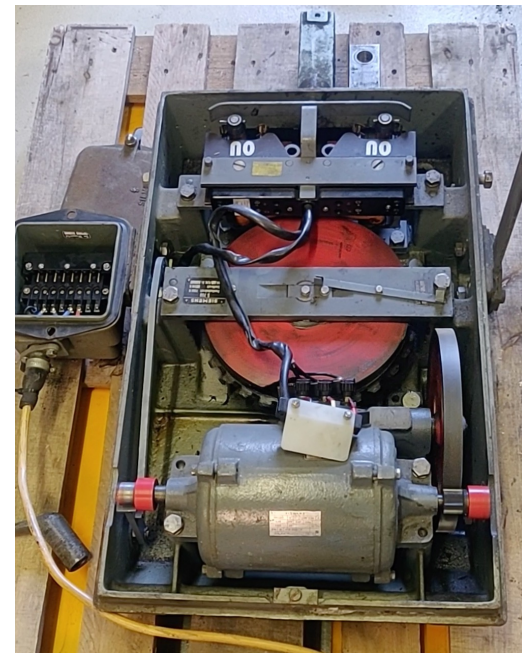
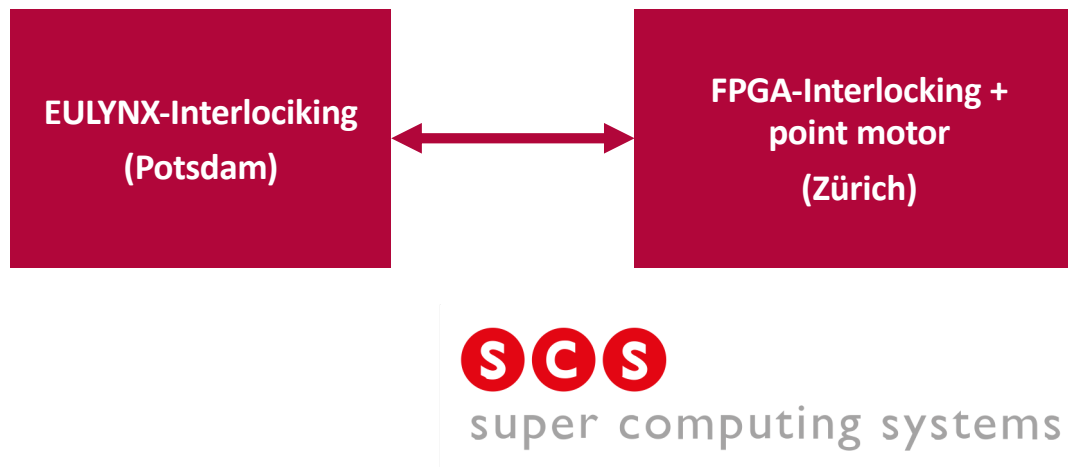
EULYNX-Live Interlocking signals movement authority at vehicle parade in '2021



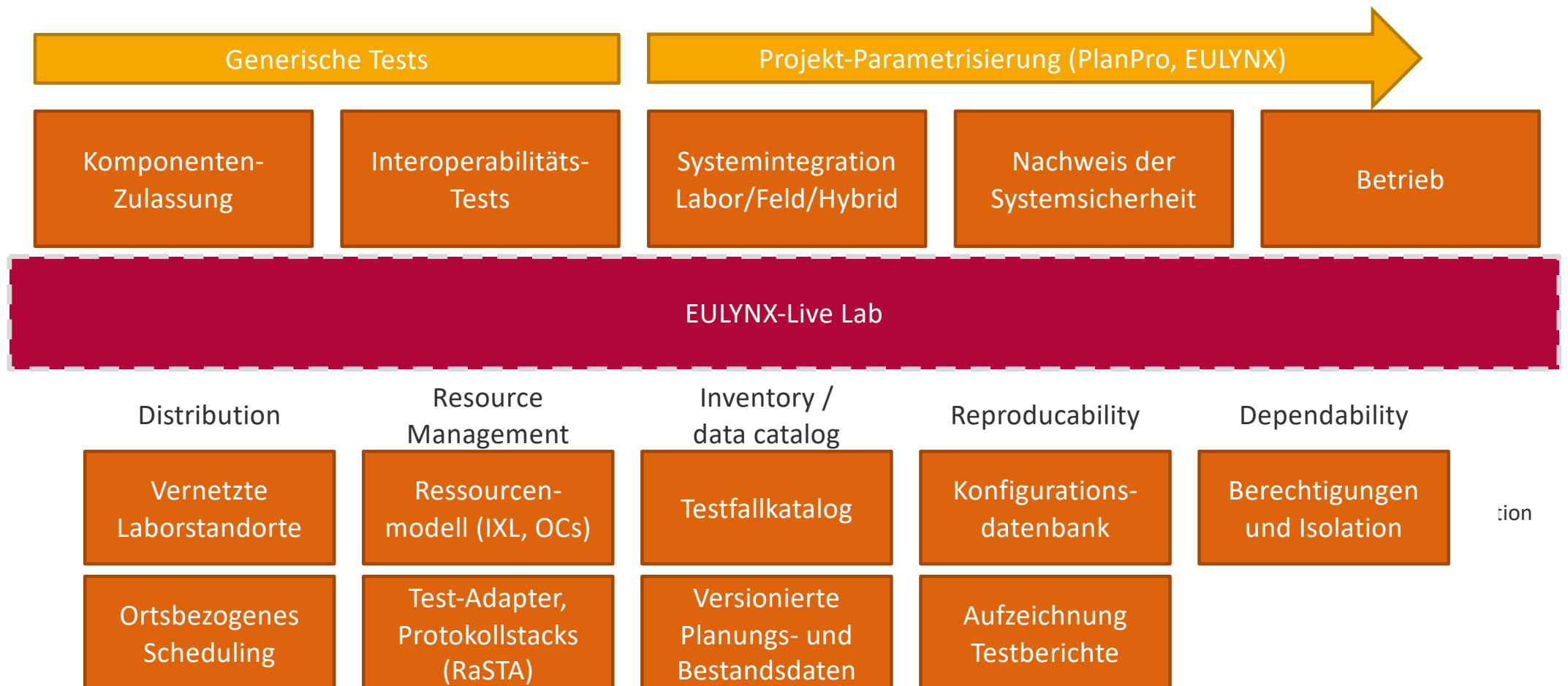
EULYNX-Live Lab Showcase

SCS FPGA-Interlocking acting as Point-Object Controller

- Implementation of EULYNX-SCI-P-Interface for SCS FPGA-Interlocking
- Samuel Kälin, ETH Zürich
- Interoperability demo RaSTA and EULYNX SCI-P

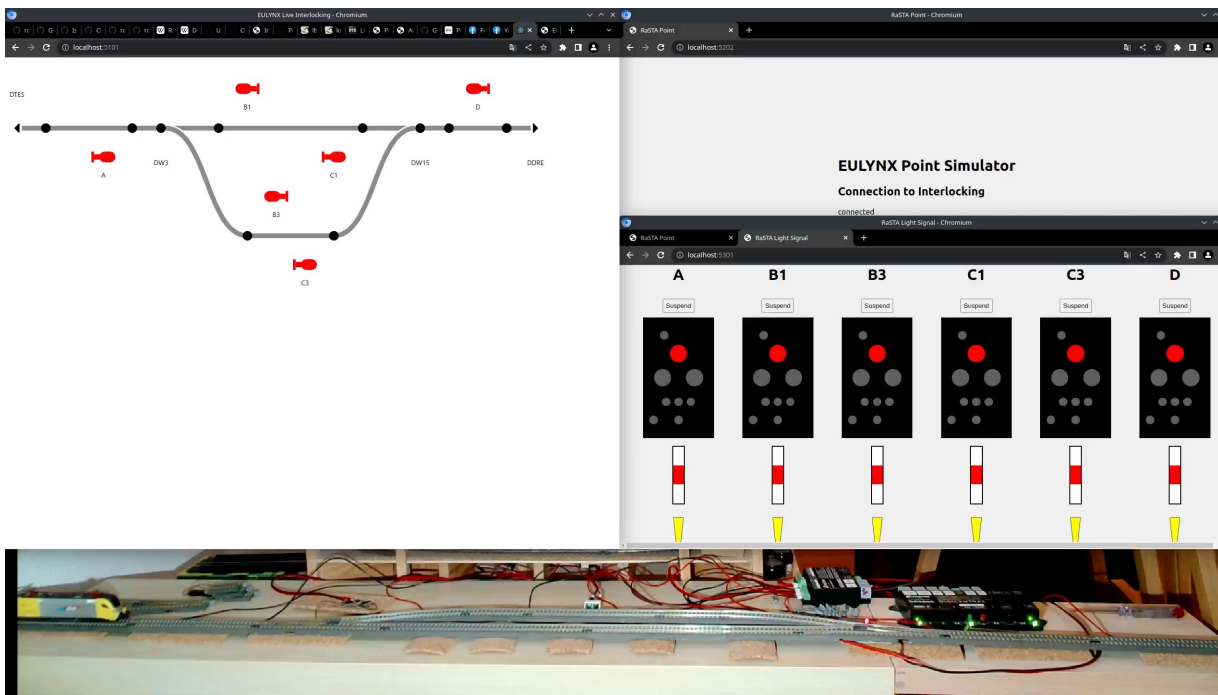


„Breadboard“ as generic test stand for DLST in geographically distributed test centers



Connection to Eisenbahnbetriebsfeld (EBuEf) at TU Berlin

- Niels Geist, Heiko Herholz, TU Berlin
- Entwicklung eines RaSTA-fähigen Multi-OC mit LocoNet-Backend



EULYNX Live Lab

Implementation of SCI-LX-Interface for Pintsch Protego



Digital Railway Operation

Software-based Command-Control-Systems for Railway need to be certifiable and updateable at low cost

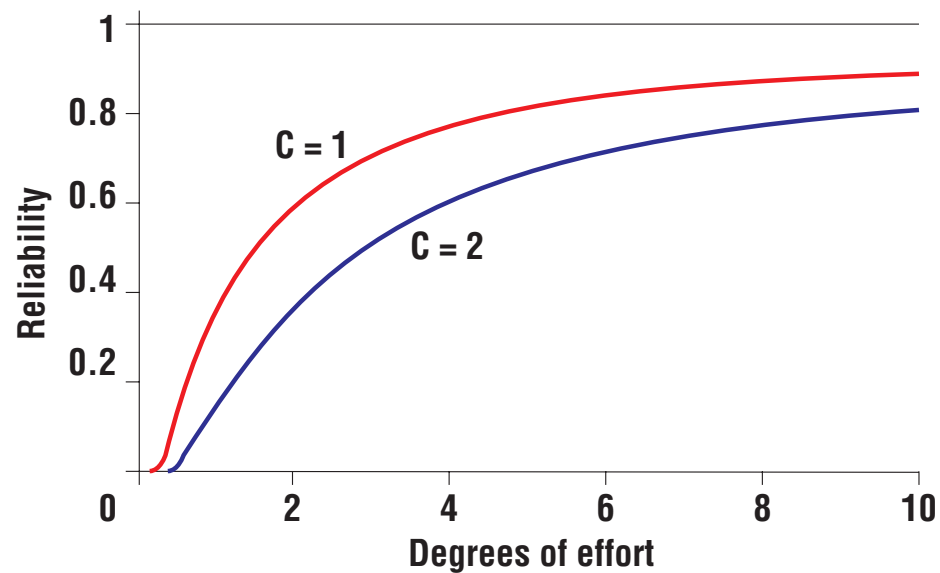
- Ergebnis des ersten Zulassungsworkshops am 19.04.2023
- Beispiel aus der Praxis (S-Bahn Hamburg): Änderung an der GoA 2-ATO-Software ohne Auswirkung auf Safety erforderte mehrwöchige Dokumentations- und Freigabeprozesse
- Nationale Umsetzung der EU Richtlinie 2016/797 (DE: EIGV, VV GluV, VV Bau-STE)
 - Gutachterrolle seitens des EBAs, hier muss technische Kompetenz vorhanden sein
 - Hello World:
Genehmigung eines Weichen-OCs



Digital Railway Operation

Correctness of Software

- Software contains errors
- Test may demonstrate presence of errors... but cannot prove correctness



Reliability of software in relation to complexity

**Digital Railway
Operation**

Using Simplicity to Control Complexity

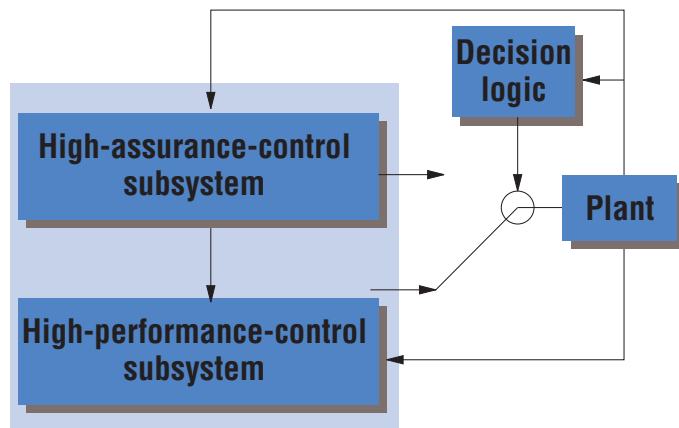
Analytic Redundancy

IEEE Software Juli/August 2001

We can exploit the features and performance of complex software even if we cannot verify them, provided we can guarantee the critical requirements with simple software.

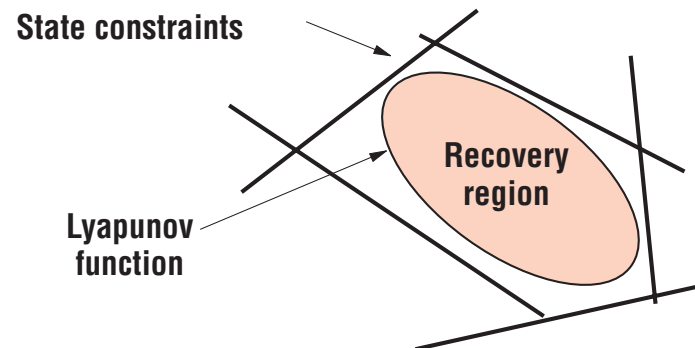
L. Sha, "Dependable System Upgrade," Proc. IEEE Real-Time Systems Symp. (RTSS 98), IEEE CS Press, Los Alamitos, Calif., 1998, pp. 440–449.

Andreas Polze and Lui Sha. Composite Objects: Real-time Programming with CORBA. In Proceedings. 24th EUROMICRO Conference (Cat. No. 98EX204), volume 2, 997–1004. IEEE, 1998.



The Simplex architecture.

The circle represents the switch that the decision logic controls.

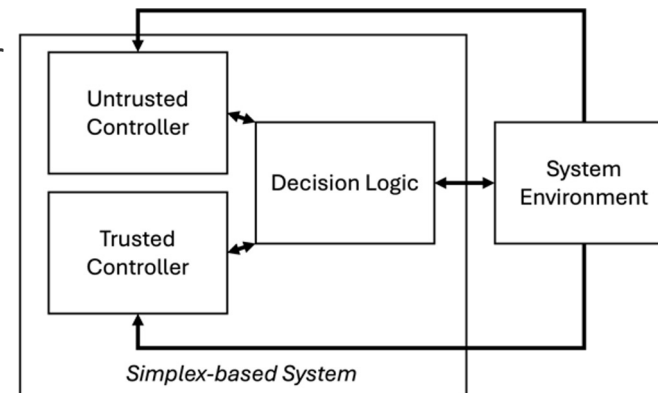


State constraints and the switching rule (Lyapunov function).

**Digital Railway
Operation**

Interface Upgrades using the Simplex Architecture

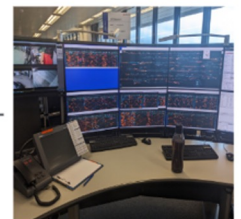
- Safety-critical components require **recertification** after updates
- Most interface updates do not affect core safety functionality
- Simplex Architecture (introduced by Sha et al.) uses **trusted controller** to supervise **untrusted controller**
- Untrusted controller can be updated without affecting dependability of system as a whole
- Prototypical implementation for axle counter



Digital Railway Operation



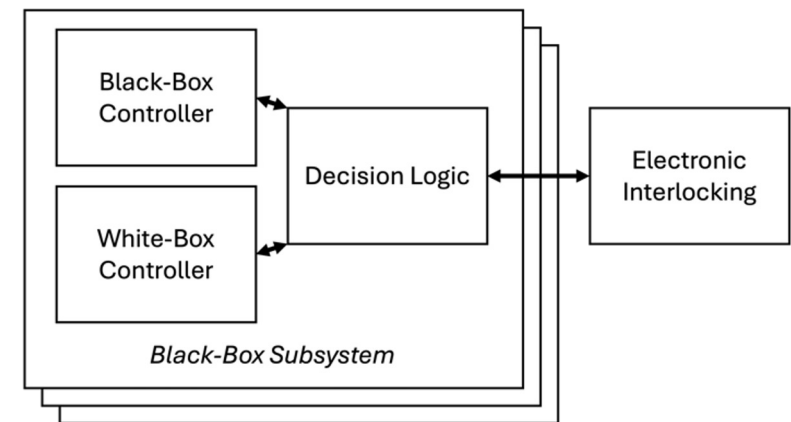
Eulynx Baseline 3 → ? ← Eulynx Baseline 4



Further Applications of the Simplex Architecture

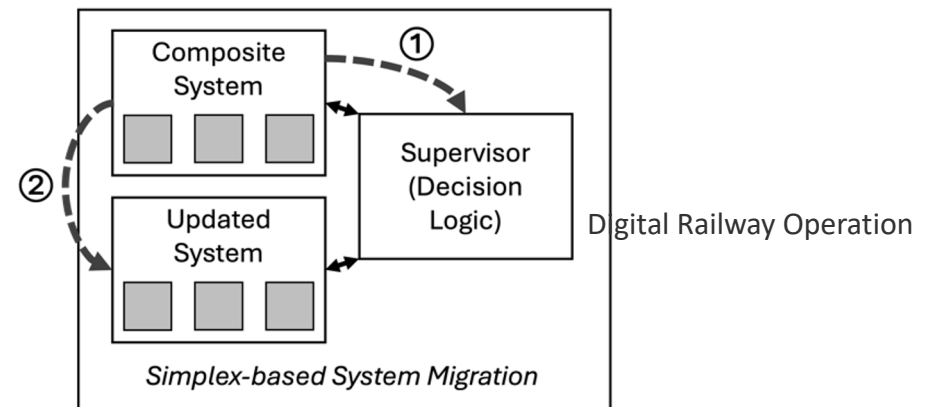
- **Simplex for System Integration**

- **Problem:** Difficult to enforce non-functional requirements on black-box object controller implementation
- **Approach:** Use white-box controller (e.g. generated from Eulynx specification) as trusted controller to supervise black-box implementation



- **Simplex for System Migration**

- **Problem:** No full system specification exists, safety is shown via equivalence to old systems
- **Approach:** After an update, existing system is kept to supervise safety-critical behavior of updated system



Agenda

- EULYNX
- ENISA report
- RailSecurity
- Paradigmenwechsel: von der GIuV zur permanenten Konsistenzprüfung
...“Using Simplicity to Control Complexity” (Lui Sha, IEEE Comp., 2001)
- **Physical Security - Digitalization weakens systems**
- NIS2 - European CyberSecurity act

Digitalization is open...

Many potential threat vectors can be derived
from publicly available infrastructure data...

Confidential information is available online



Technology Institute



Informationen zu GSM-R und zur Glasfaserinfrastruktur sind öffentlich.

DB Netze versorgt nicht nur die Bahn-eigenen Tochterunternehmen mit Infrastruktur, sondern auch andere Eisenbahngesellschaften.

- Baufirmen und am Bahnbetrieb beteiligte Partner brauchen genaue Informationen.
- Das Infrastrukturregister, eine Online-Plattform mit interaktiver Kartenansicht, gestattet ausführliche Recherchen zum Schienennetz und seiner Ausstattung.

Der Aufbau von GSM-R inklusive Rückfallkonzept bei Ausfällen wird ausführlich erklärt

- weil das Mobilfunknetz von DB Netze an private Bahnbetreiber vermietet wird.

**Digital Railway
Operation**

Infrastructure register is available online



Technology Institute



DB NETZE Infrastrukturregister

APN TPS Strecken Neuigkeiten Grundsätze Meldung Benutzerhandbuch | Herunterladen

Abfragen & Auswerten Drucken, Laden & Speichern Zeichnen ISR

Merkmalen Spurplan Themen

- ☒ Betriebsstellen
 - ☒ Betriebsstellen pro Strecke
 - ☒ Streckenübergänge
- ☒ Streckenmerkmale
 - ☐ TSI Kategorie PV
 - ☐ TSI Kategorie GV
 - ☐ TEN Klassifizierung
 - ☐ KV-Kodifizierung
 - ☐ Streckenklasse
 - ☐ multinationales Lichttraumprofil
 - ☐ interoperables Lichttraumprofil
 - ☐ Gleisanzahl
 - ☐ PZB
 - ☐ LZB
 - ☐ ETCS Level
 - ☐ Neigetechnik
 - ☐ Streckenneigung
 - ☐ Höchster Zugstrom (Pz)
 - ☐ Höchster Zugstrom (Gz)
 - ☒ Kommunikationssystem
 - ☐ Traktionsart
 - ☐ Geschwindigkeit
 - ☐ Betriebsverfahren
 - ☐ Verkehrsart
 - ☐ Wirbelstrombremse
- ☒ Kapazitätsverbrauch RV
 - ☐ Notbremsüberbrückung
 - ☐ Güterverkehrskorridor 1
 - ☐ Güterverkehrskorridor 3
 - ☐ Güterverkehrskorridor 4
 - ☐ Güterverkehrskorridor 7

FABRIKSTRASSE

BEIEN-WEG

Maßstab 1: 500 ☐ freie Maßstabseingabe EPSG:31467 Version 2.9.0.1

© OpenStreetMap-Mitwirkende. Service by DB Systel, © DB Netz AG

Digital Railway Operation

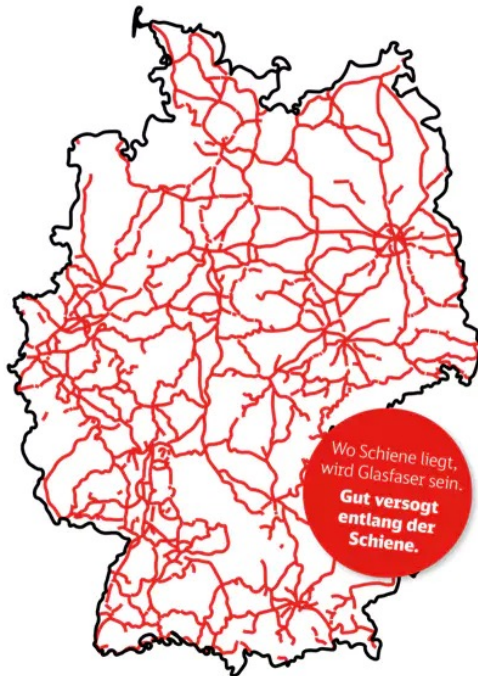
broadband.dbnetze.com



Technology Institute



DB NETZE *broadband*

[Dark Fiber](#)[Referenzen](#)[Unternehmen](#)[Aktuelles](#)[Kontakt](#)[Downloads](#)

Unser Netz verläuft entlang der Schienenwege und damit auch teilweise durch bislang noch unterversorgte oder gar unversorgte Regionen. Diese und viele weitere Regionen können mit uns einfach und effizient erschlossen werden. Dafür halten wir ein optimales Dark Fiber Angebot bereit.

Erfahren Sie mehr zu unserem Angebot: [Dark Fiber](#)



Glasfaserkabel überall dort wo Schienen liegen.

Bis 2026/2027 bauen wir unser Glasfasernetz weiter aus. Ziel ist es, das gesamte Schienennetz von **33.400 km** mit Glasfaser zu erschließen. Die künftigen Freikapazitäten kann man sich schon jetzt sichern.

Digital Railway Operation

Attacks on Rail Infrastructure

GSM-R Outage in Northern Germany (08. October 2022)



Technology Institute



Das Potenzial für Angriffe auf die Glasfaserleitungen der Bahn ist groß.

- Kabel verlegt die Bahn entlang der Trassen oft in Betonkabelkanälen mit Betondeckel.
- Ganz ohne Bagger und Spaten kann sich jeder Zugriff verschaffen.
- Saboteure die Kabel, an denen die norddeutsche GSM-R-Infrastruktur samt Backup hängt.

Die Reparatur gelang vergleichsweise schnell, nach knapp drei Stunden war die Leitung gespleißt.

Wichtige Infrastruktur hätte noch redundanter angebunden werden müssen

- In der Planungsphase scheint Sabotage mit so viel Hintergrundwissen noch nicht das beherrschende Thema gewesen zu sein.
- Gegen andere Probleme wie Hochwasser, Brand und lokale Stromausfälle ist die Wahl der Standorte Herne und Berlin sehr geeignet.
- Fraglich ist auch, ob mehr Anbindungen pro Standort geholfen hätten: Wer so genau Bescheid weiß, welche Standorte er abschalten muss, schreckt auch vor drei oder fünf Kabeln nicht zurück.

**Digital Railway
Operation**

Kabelbrand Ostkreuz



Technology Institute



**Digital Railway
Operation**

Kabelbrand Ostkreuz

(22.02.2013)



Technology Institute



Innovative technologies are prone to attacks...



Technology Institute



Hydrogen filling station at NEB



Fence segment temporarily removed



Digital Railway Operation



1826
4-digit
key-code

Agenda

- EULYNX
- ENISA report
- RailSecurity
- Paradigmenwechsel: von der GIuV zur permanenten Konsistenzprüfung
...“Using Simplicity to Control Complexity” (Lui Sha, IEEE Comp., 2001)
- Physical Security - Digitalization weakens systems
- **NIS2 - European CyberSecurity act**

KRITIS-Dachgesetz regelt Verantwortlichkeiten

European NIS2 Directive

KRITIS-Dachgesetz (openkritis.de)



Technology Institute



- The updated NIS2 Directive, focuses on enhancing the resilience of critical sectors across the EU by tightening cybersecurity requirements to ensure the security and continuity of essential services in the face of escalating digital threats.
- The NIS2 Directive has a broadened scope to additional sectors and entities vital to the EU's economy and society. Organisations are classified according to factors such as size, sector and criticality. They fall into two categories: essential and important entities.

**Digital Railway
Operation**

Resiliency in NIS2



Technology Institute



Highly critical sectors in scope are:

- Digital infrastructures (electronic communications, trust services, domain name services, top level domain registries, cloud services, data centers, internet exchange points, content delivery networks);
- Energy (electricity, district heating, oil, gas and hydrogen);
- Transport (air, rail, water, road);
- Banking and Financial market infrastructures;
- Health (healthcare providers, EU reference labs, research and manufacturing of pharmaceuticals and medical devices);
- Drinking water and waste water;
- Public administrations;
- Space.

**Digital Railway
Operation**

Conclusion



Technology Institute



- Digitalization is going to weaken CCS systems
- Need to cope with long system lifetime (...multiple decades)
 - Certification processes need to be adapted
 - Fail-stop vs fail-operational: trading off safety and availability
- Problem case: system update / construction / fallback states...
 - Resiliency need to be considered separately
 - Redundancy concept not working / applicable
 - Insider knowledge among attackers
- Physical Security of digital CCS today of much bigger concern than CyberSecurity

**Digital Railway
Operation**