

# DRSS

## Digital Rail Summer School



Bildquelle: *Bredt, Markus*, online unter <http://architektur.mapolismagazin.com/sites/default/files/berlin-3.jpg>

Bildquelle: *Tim Grams*, online unter <https://derbloggendebahner.de/downloads/>

Bildquelle: *Railway Technology*, online unter [http://www.railway-technology.com/projects/7117/images/142451/large/5\\_image\\_05.jpg](http://www.railway-technology.com/projects/7117/images/142451/large/5_image_05.jpg)



## Digital Rail Aufaktveranstaltung



## Agenda



- Einführung und Motivation
- Vorstellung der Fachgebiete
- Lehrveranstaltung
  - Ablauf
  - Projektarbeit
    - Sicherheitsbetrachtung Hinderniserkennung
    - EULYNX-Live
    - Security-Analyse Eurobalise
    - Intrusion Detection System für Object Controller
- Infrastruktur
  - IoT-Labor, HPI
  - Digitales Testfeld Bahn, Erzgebirge
- Nächste Schritte



### Railway (Digital LST) Certification

#### Zulassung (EN 50128, SIL4)

Sicherheitsnachweis

Nachweis (= praktischer Beweis) und Gutachten, dass das System (Gesamtsystem) immer einen Sicheren Zustand annimmt

im Fehlerfall: Fehleroffenbarung, Fehlerbehandlung, Degraded Mode über Redundanz, 2-out-of-3, etc.

**Bahnbetrieb** (Funktionalität)  
BTSF  
(Betrieblich-Technische Systemfunktionen;  
FRS & SRS = Functional & System  
Requirement Specification)  
Geschwindigkeiten, Längen/Abstände,  
Fahrstraßen, Fahrerlaubnisse  
„Produktionsprozesse des Bahnbetriebes“  
(Fahrdienstvorschrift, Signalbuch)

### IT Systems (Software Engineering)

#### Informatik (Softwaretechnik)

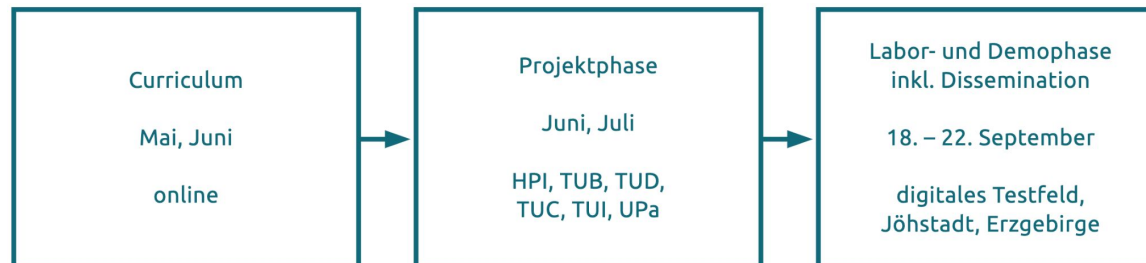
Modellgetriebene Entwicklung, V-Modell, Agil  
Simulation, Verifikation, Komponenten, Test,  
Fehlerinjektion, Kontinuierliche Integration,  
DevOps

Co-Simulation, IoT-Labor, Feldtest  
Reallabor / Living Lab

Nichtfunktionale Systemeigenschaften: Echtzeit,  
Fehlertoleranz, Sicherheit

## Struktur

- Vorkurse (online) + Q&A
  - Teilnehmer:innen wählen Vorlesungen aus dem Curriculum nach Absprache mit der jeweiligen eigenen Universität
  - Details unter: <https://hpi.de/drss>
- Projektarbeit in kleinen (interdisziplinären) Gruppen, wenn möglich
- Ausflug ins Pressnitztal am 18.05.2023
- Besuch im EbueF am 06.07.2023
- Ausflug nach Karow am 20.07.2023
- Exkursion nach Jöhstadt im September (18.09. - 22.09.)



# Problembeschreibung



## Simulation, Verifikation, Testen, Fehlerinjektion

Die ICE 1, die für den **ETCS-L2-Betrieb** auf der **VDE 8** mit dem Alstom System „Atlas 200“ (SRS 3.4.0) ausgerüstet wurden, erfuhren am 3. November 2019 eine ETCS-Störung mit größeren betrieblichen Folgen.

### Ursache: Datumswidrigkeit

Das Satelliten-Navigationssystem nach 1024 Wochen (etwa 20 Jahre) **1980** zurückfällt. Im ICE 1 wurde das **Jahr 2000** zurückgesetzt. Aufgrund dieser Daten gab es ein Verschlüsselungsproblem, das schließlich die Kommunikation mit dem Boden unmöglich machte, wodurch die ETCS-Führung fehlerhaft wurde.

„Eisenbahn-Revue International“ (ERI, 12/2019)

### Wuppertaler Schwebbahn:

ETCS habe nach Inbetriebnahme am 1. September 2019 „seine Mucken“ gehabt und die Bahn immer wieder lahmgelegt – von wenigen Minuten bis zu über einer Stunde.

Ursache seien **Funkstörungen**, die auf viele kleine Störungen an Strecke und Fahrzeugen zurückgingen. Die Störungsbehandlung, die anfangs eine Viertelstunde gedauert habe, gehe inzwischen in 2 bis 3 Minuten, oftmals helfe ein **Neustart von ETCS...**

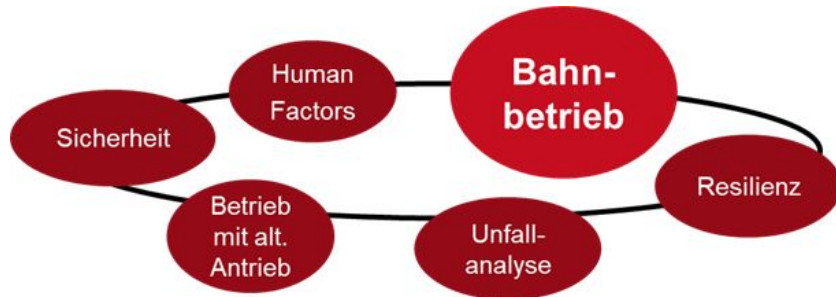
„Westdeutsche Zeitung“ (31.12.2019)

# Vorstellung der Fachgebiete

**Ziel in Lehre und Forschung:**

Betrachtung des Schienenverkehrs als Gesamtsystem

[www.railways.tu-berlin.de](http://www.railways.tu-berlin.de)



**Ausstattung**

- Eisenbahn-Betriebs- und Experimentierfeld
- Virtuelles Betriebsfeld
- Fahrsimulatoren



# Hasso-Plattner-Institut, Universität Potsdam

## Professur für Betriebssysteme & Middleware



Arne Boockmeyer, Dirk Friedenberger, Lukas Pirl, Andreas Polze, Robert Schmid

Details unter: [osm.hpi.de](https://osm.hpi.de)





## “extending the reach of middleware”

### “Middleware for Predictable Systems”

- Paradigms, Design patterns, implementation strategies
- Real-time, Fault-Tolerance, Security
- Fontane Project – Charité, Prof. Dr. Friedrich Köhler, Rail2X



### Operating Systems

- New Concepts for New Hardware Paradigms (NUMA, Intel SCC, IBM Power platform, GPU accelerators, Xilinx FPGA)
- Programming models for hybrid parallelism: CPU vs. Xeon Phi vs. Nvidia Tesla vs. Cluster



### Wide-Area Distributed Systems – Grid, Cloud, IoT

- Predictable behavior in heterogeneous distributed systems
- Service-Oriented Cloud Computing Environments
- Cooperation with (embedded) Device Vendors – Getemed, ECG devices



### Embedded Systems

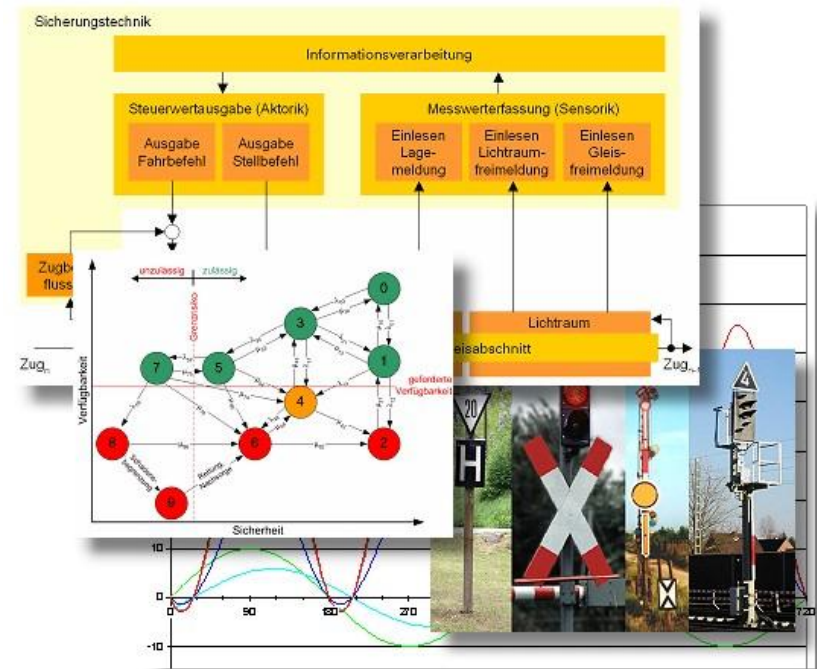
- Analytical Redundancy and Online Replacement, Dynamic (Re-)Configuration of Component Software

Wissenschaftlicher Gegenstand:  
**Steuerung und Sicherung  
spurgeführter Verkehrssysteme**

Dafür werden folgende  
wissenschaftlichen Disziplinen vereint:

- Sicherheitswissenschaft
- Eisenbahnbetriebswissenschaft
- Automatisierungstechnik

<https://tud.de/vst>



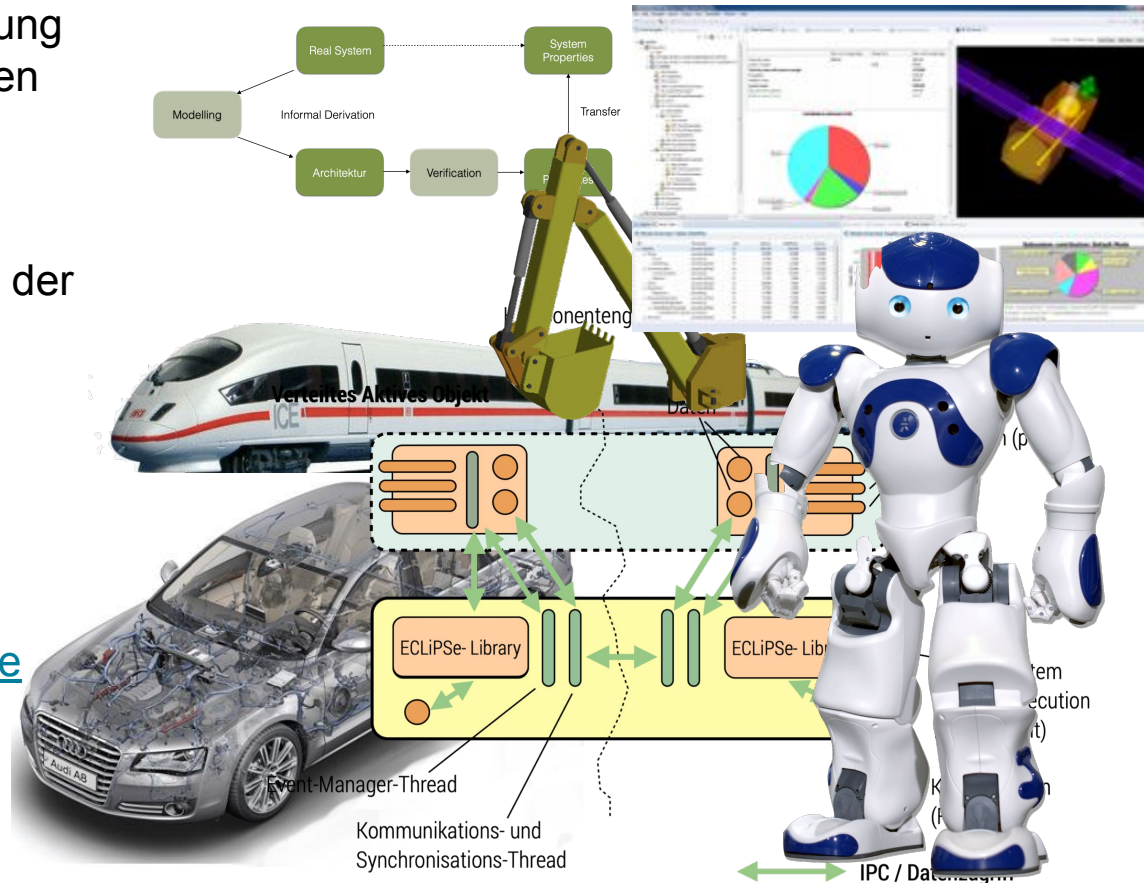
### Forschungsschwerpunkte:

- Modellierung und Gewährleistung meta-funktionaler Eigenschaften
- Moderne Laufzeitsysteme für dynamische Anwendungen

Anwendung vorwiegend im Bereich der mobiler Systeme, insbesondere Transportation Systeme

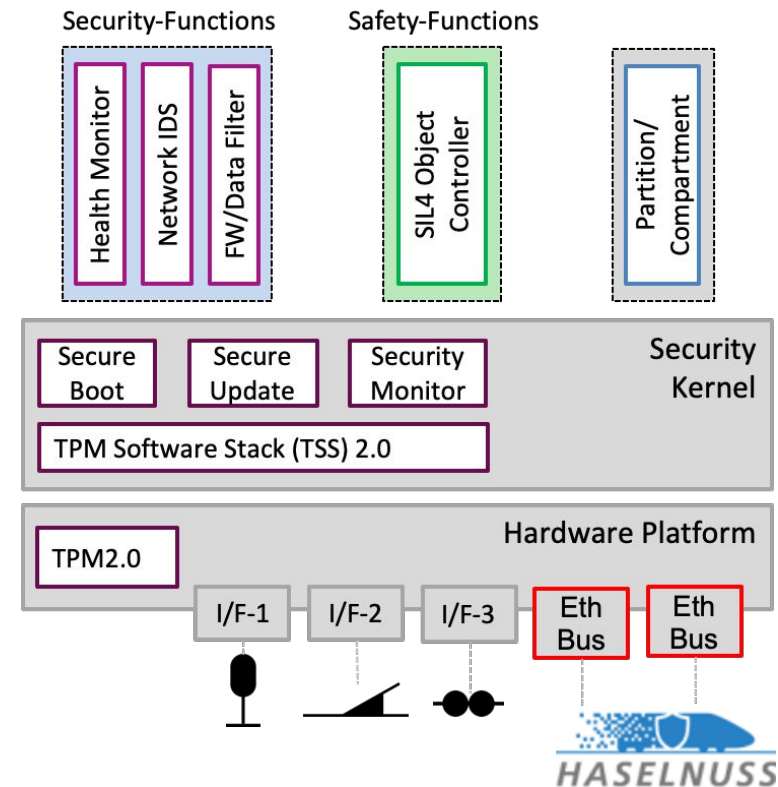
- Automobile
- Bahn
- Raumfahrt
- Nutzfahrzeuge

<https://osg.informatik.tu-chemnitz.de>



## Forschungsschwerpunkte:

- IT-Sicherheit, hardware-nahe Sicherheit
- Sichere Kritische Infrastrukturen
- Digitalisierung im Schienenverkehr



## Schwerpunkte im Kontext Rail:

### Beratung/ Spezifikation

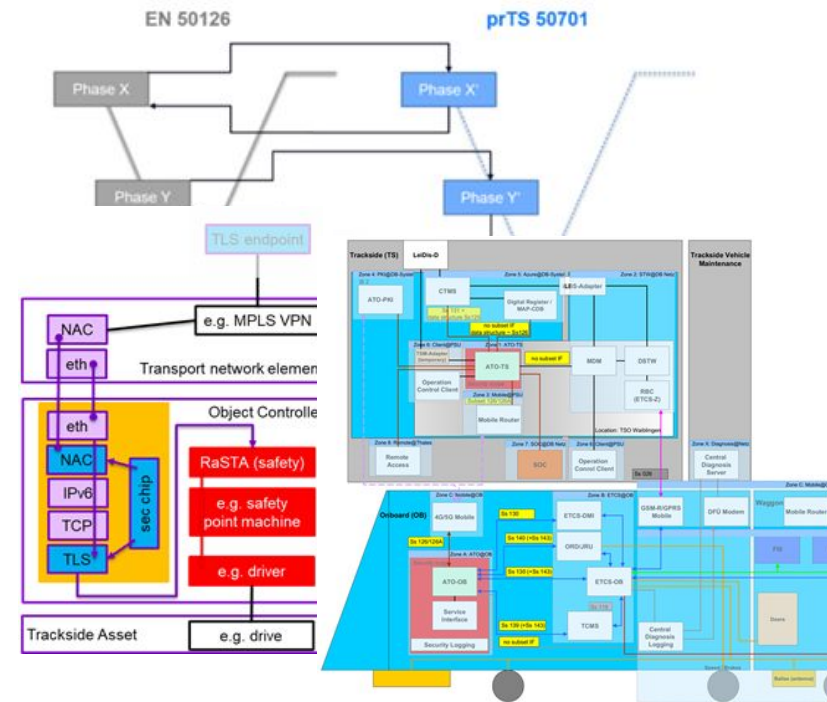
- Bedrohungs- Risikoanalyse
- Maßnahmenableitung- und Umsetzung, Betriebsführung, Testen
- IEC 62443, prTS 50701 konform
- Digitale Stellwerkstechnik, ATO, ETCS
- Fahrzeugtechnik
- Technologieprognose / Forschung

### Begutachtung/ Bewertung

- Security Konzept
- Spezifikation
- Betriebsführungskonzept
- Security Case
- Testplanung
- Netzwerke (offen+geschlossen)

### Standard- disierung

- EULYNX & RCA
- OCORA
- VDE 831-10x
- ERTMS Users Group



EULYNX



OCORA

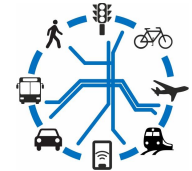
# TH Wildau

## Professur für Verkehrssysteme/ Studiengang Verkehrssystemtechnik



### Ziel in Lehre und Forschung:

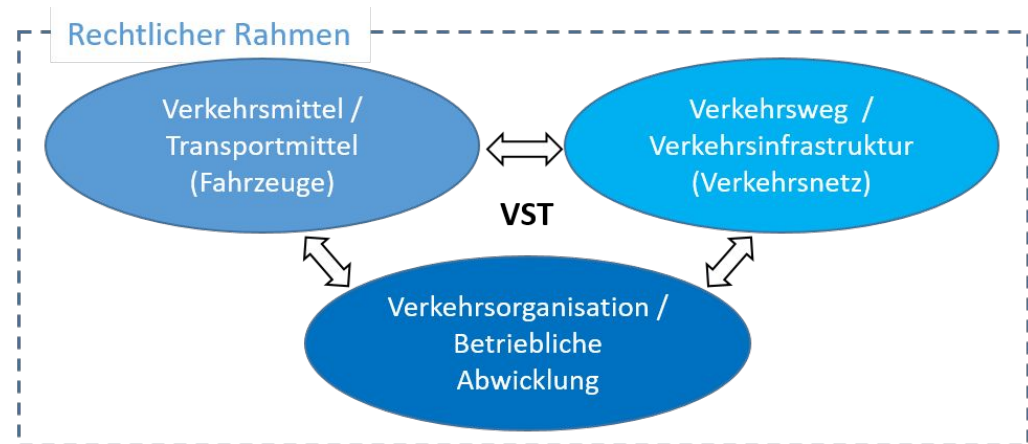
- grundlegendes Gesamtverständnis des Systems Verkehr aus Sicht der Nutzer und Betreiber von Fahrzeugen und Betriebszentralen



### Themengebiete der Professur:

- Verkehrstelematik, IT im Verkehr und Datenmanagement im Personenverkehr
- Leit- und Sicherungstechnik
- Fahrerassistenzsysteme

<https://www.th-wildau.de/vst/>



# Die Lehrveranstaltung

- integrierte Lehrveranstaltung
- umgedrehter Unterricht (“flipped classroom”)

## Online verfügbar

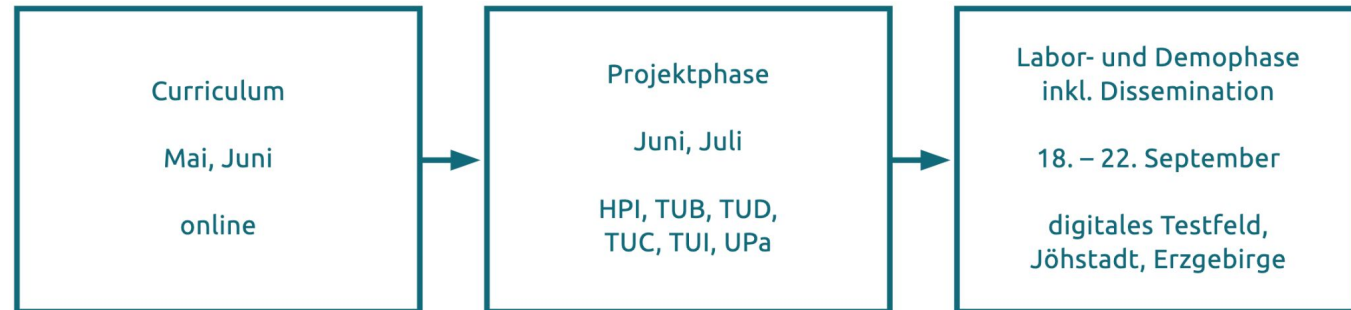
- Screencasts

## Live-Veranstaltungen

- Präsenzvorlesungen
- Gastvorlesungen

## Live-Veranstaltung und Gruppenarbeit

- Projektarbeit





- Vorlesungsplanung: <https://osm.hpi.de/drss/2023/curriculum/>

20.04., 13:00 – 15:00: Auftakt der DRSS 2023	>
27.04., 13:00 – 15:00	
04.05., 13:00 – 15:00	
11.05., 13:00 – 15:00: EULYNX: Grundlagen & Hintergründe	
18.05.: Himmelfahrt, kein Curriculum.	
25.05., 13:00 – 15:00	
01.06., 13:00 – 15:00	
08.06.: Fronleichnam, kein Curriculum.	
15.06., 13:00 – 15:00: externer Vortrag <i>Vom DSTW in die Cloud</i> (Sonja Steffens, Siemens)	
22.06., 13:00 – 15:00	
29.06., 13:00 – 15:00	
06.07., 13:00 – 15:00: Besuch des <a href="#">EBuEf</a>	
13.07., 13:00 – 15:00	
20.07., 13:00 – 15:00: Exkursion	
27.07., 13:00 – 15:00	

# #1 Projektarbeit

## Sicherheitsbetrachtung

### Hinderniserkennung

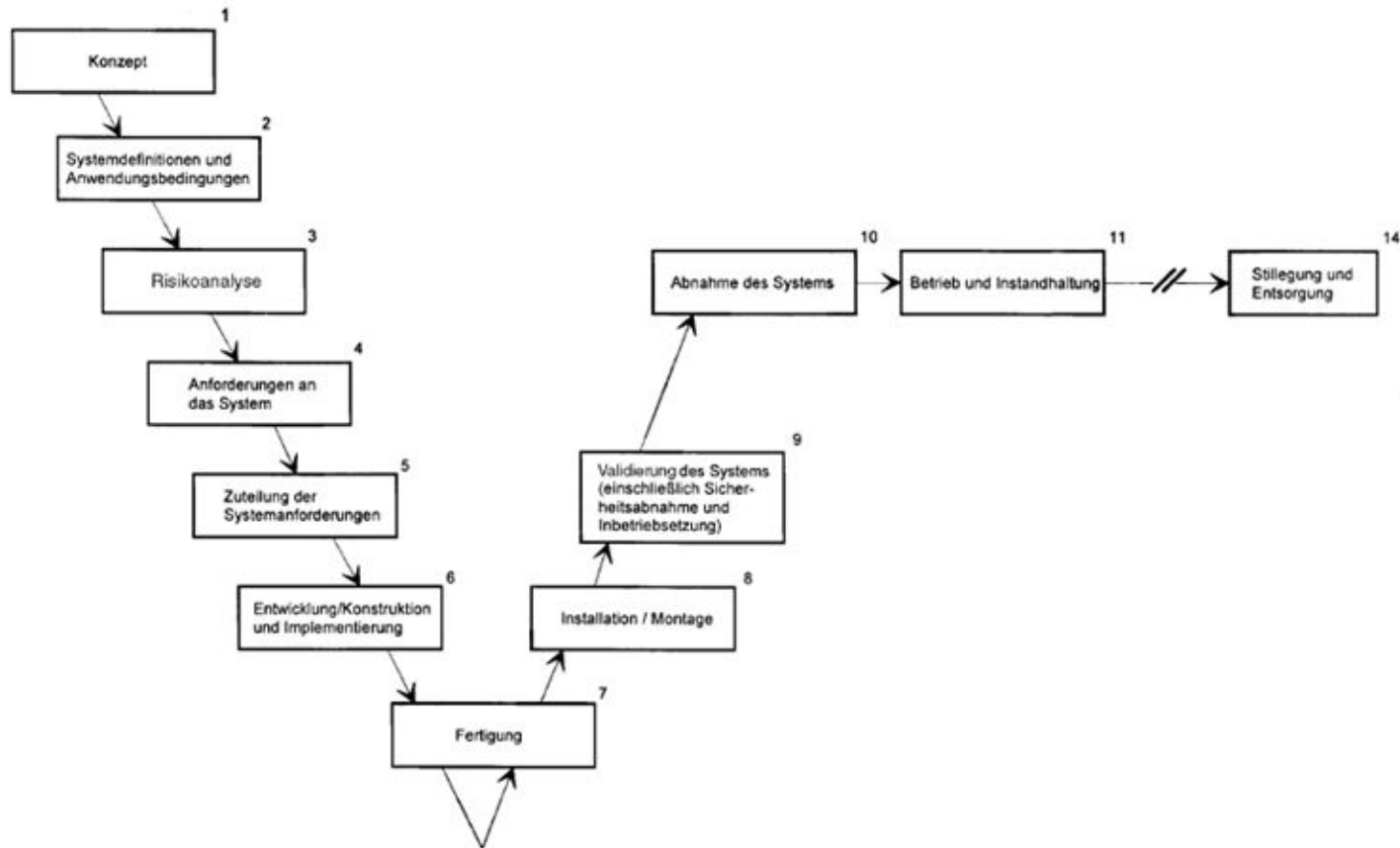


- Hinderniserkennung ist wesentliche Komponente des automatisierten Fahrens
- im Rahmen der Projektarbeit erarbeiten wir, wie solch ein System aussehen könnte
- Funktionen & Schnittstellen
- Ableitung von Gefährdungen
- Sicherheitsanforderungen aus den Gefährdungen an die Funktionen
- Arbeit in Kleingruppen
- Präsenz-Online-Termine alle zwei bis drei Wochen

# #1 Projektarbeit

## Sicherheitsbetrachtung

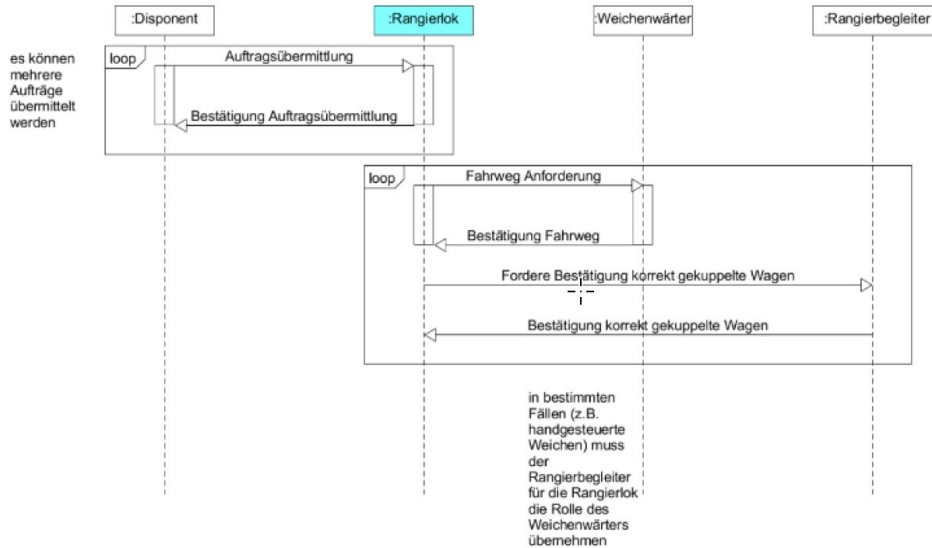
### Hinderniserkennung



# #1 Projektarbeit

## Sicherheitsbetrachtung

### Hinderniserkennung



Geschwindigkeit kontrollieren (F.1)	Die Fahrgeschwindigkeit muss permanent entsprechend einer vom Routing vorgegebenen Sollgeschwindigkeit geregelt werden. 25 km/h dürfen nicht überschritten werden.	
Anfahren (F1.1)	Schleuderfreies Anfahren muss gewährleistet werden.	1
Anhalten (F1.2)	Beim Erreichen der Zieldistanz muss angehalten werden.	2
Nothalt (F1.3)	Bei einem Nothaltauftrag muss sofort die Leistung abgeschaltet und eine Schnellbremsung eingeleitet werden.	3
Ziel vorgeben (F2.1)	Über den Aufgabenmanager wird ein Fahrziel vorgegeben.	-
Route ermitteln (F2.2)	Die Software muss selbstständig alle fahrbaren Routen von der aktuellen Position zum vorgegebenen Ziel ermitteln und dem Aufgabenmanager melden.	-
Anforderung des Fahrwegs (F2.3)	Zur Sicherung des Fahrwegs muss das Betriebspersonal beauftragt werden, um den Fahrweg einzustellen.	
Bestätigung der korrekten Fahrwegelage (F2.4)	Das Betriebspersonal muss aufgefordert werden, die korrekte Lage der Fahrwegelemente zu bestätigen.	
Richtung wählen (F3)	Die Fahrtrichtung muss entsprechend der Route richtig gewählt werden, bevor angefahren wird.	1
Kuppeln (F4)	Das Fahrzeug muss bei entsprechendem Auftrag automatisch eine Kuppelverbindung mit einem Wagen herstellen oder auflösen.	2

Consequence	Frequency	Possibility	Probability	Risikominderung	SIL
C3	F1	x	W1	d	2

### **EULYNX-Live**

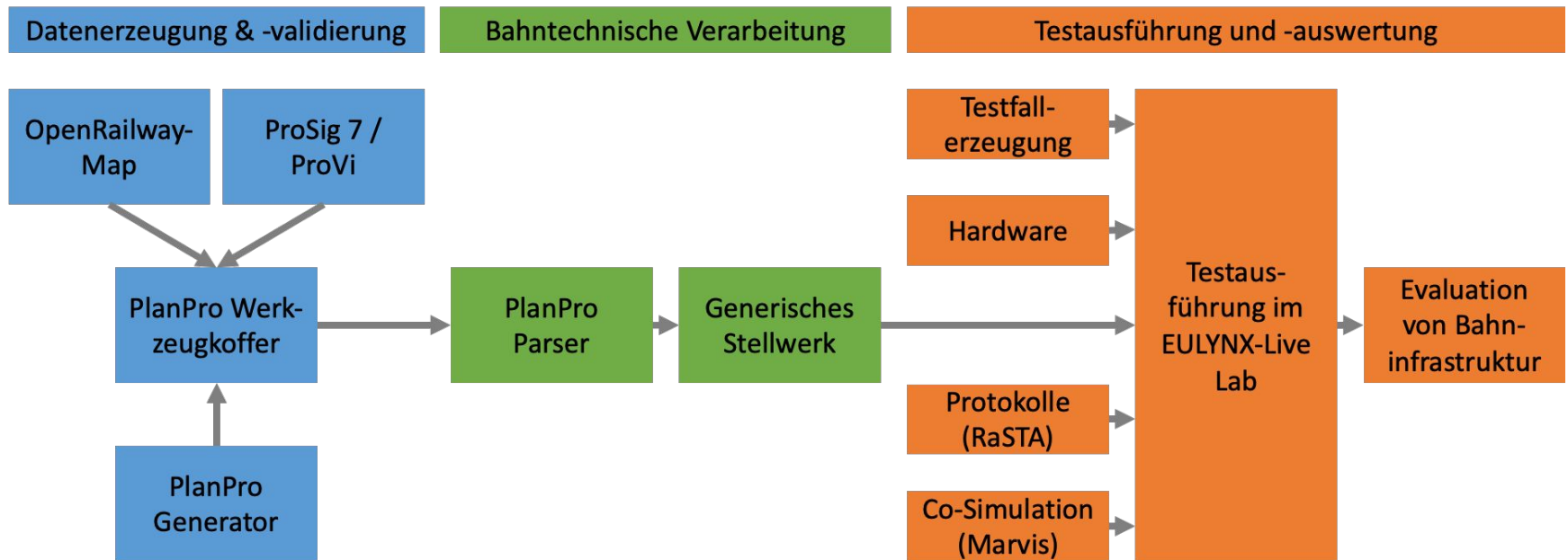
- Herausforderungen durch Verkehrswende & Digitalisierung
  - mehr Kapazität, schnellerer Ausbau, Prozesse beschleunigen
- benötigt modernes Software-Engineering
  - Co-Simulation, kontinuierliches Testen, Fehlerinjektion, ...
- Adaption moderner Methoden und Werkzeuge in die Bahnwelt
  - durchgängige digitale Datenhaltung: Planung bis Inbetriebnahme
  - Automatisierung und kontinuierliches Integrieren
  - Standardisierung / Interoperabilität zwischen Herstellern

# #2 Projektarbeit

## EULYNX-Live

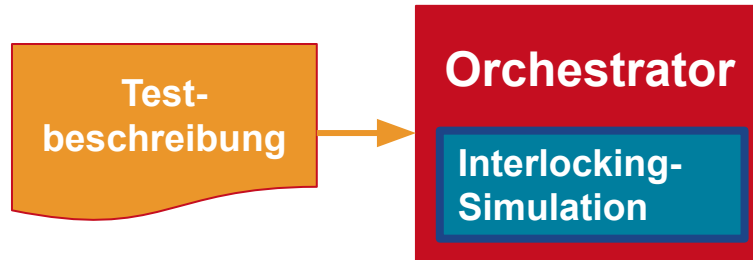


### Projektübersicht:



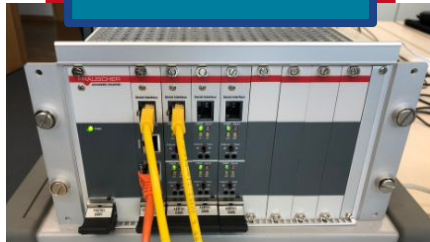
# #2 Projektarbeit

## EULYNX-Live: verteilte Laborumgebung



Laborknoten

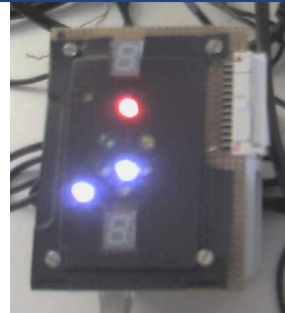
RaSTA-Bridge

A red box containing the text 'Laborknoten' at the top and 'RaSTA-Bridge' in a blue box at the bottom.

HPI IoT-Lab,  
Potsdam

Laborknoten

RaSTA-Bridge

A red box containing the text 'Laborknoten' at the top and 'RaSTA-Bridge' in a blue box at the bottom.

Brunel,  
Hildesheim

Laborknoten

RaSTA-Bridge

A red box containing the text 'Laborknoten' at the top and 'RaSTA-Bridge' in a blue box at the bottom.

Digital Rail Lab,  
Scheibenberg

Laborknoten

RaSTA-Bridge

A red box containing the text 'Laborknoten' at the top and 'RaSTA-Bridge' in a blue box at the bottom.

NEU:  
TU Dresden

### EULYNX-Live

- Ziele des diesjährigen Projektes (VST, TU Dresden / OSM, HPI)
  - Ausbau des vernetzten EULYNX-Labors
  - Errichtung Demonstrator für EULYNX am Bsp. SCI-LS
  - Betrieb Ks im Sicherungstechnischen Labor (SIL)
  - Anwendung EULYNX an HI-Signalen
- Teilaufgaben
  - Datenübertragung zwischen HPI und VST
  - Konzeption und Errichtung OC für Ks in Dresden
  - Anpassungen EULYNX an HI-Signalsystem
- Ansprechpartner: Richard Kahl, Robert Schmid, Clemens Tiedt



# #3 Projektarbeit



## Security-Analyse Eurobalise

### Was ist eine Eurobalise?

- induktiv gekoppelter Transponder zwischen den Gleisen
- wird beim Überfahren vom Fahrzeug energetisiert und sendet eine Nachricht (Telegramm) an das Fahrzeug
- Gegenstück: Balisenantenne
- sicherheitsrelevantes Element des ETCS



Foto: DB AG



Foto: Siemens

## Security-Analyse Eurobalise

### Teilaufgabe 1 - Emulierung einer Balisenantenne

- Recherche zu Aufbau und Funktionsweise einer Eurobalise
- Recherche zur Telegrammstruktur
- Auslesen einer Eurobalise mithilfe eines Software Defined Radios
- Security-Analyse der Kommunikation zwischen Balise und Antenne

### Teilaufgabe 2 - Emulierung einer Balise

- Nachbau einer Balise mithilfe eines *Software Defined Radios*
- Testen der Kommunikation zwischen Balise und Antenne
- Aufbau Kommunikation virtueller Balisen

### Teilaufgabe 3 - Untersuchung der Balisenprogrammierung

- Recherche zur Funktionsweise der Balisenprogrammierung
- *Reverse Engineering* des Prozesses

# #3 Projektarbeit



## Security-Analyse Eurobalise

### Ziele:

- Auslesen einer Balise
- Hacking durch Bau unserer eigenen “Balise”
- Verstehen des Programmierungsprozesses

### Euer Beitrag:

- gutes Teamwork, Spaß am gemeinsamen “Tüfteln”
- selbstständiges Arbeiten
- Programmiergrundkenntnisse

### Euer Benefit:

- tiefe Einblicke ins System Bahn und die Digitalisierung
- Networking über verschiedenste Partner in Industrie und Wirtschaft
- Security in Kritischen Infrastrukturen
- Hacking = Fun

# #4 Projektarbeit

## Intrusion Detection System für Object Controller



- Security-Risikobehandlung hat Grenzen
  - Kryptographie ist nicht die Antwort auf alle Fragen
  - Nicht alle Mechanismen können immer eingesetzt werden
- Laufzeitüberwachung als wichtiger Baustein
  - Ermöglicht Erkennung von Angriffen
  - (Ermöglicht Reaktion auf Angriffe)

News zum [#Totalausfall](#) bei der [#Bahn](#): Mehrere Quellen aus den Sicherheitsbehörden sprechen von ersten Hinweisen auf mögliche Sabotage. 2 für das Kommunikationssystem (GSM-R) wichtige Kabel seien an 2 unterschiedlichen Tatorten durchtrennt worden. Daraufhin fiel ganzes System aus.

8.10.2022, 09:51:09 via Twitter



Quelle: Stuttgarter Zeitung

# #4 Projektarbeit

## Intrusion Detection System für Object Controller



### Teilaufgabe 1 - Analyse von Angriffsvektoren auf *Object Controller*

- Evaluation von Angriffsvektoren und unterliegender Schwachstellen
- Kategorisierung inwieweit die Schwachstellen behoben werden können oder durch *Intrusion Detection* behandelt werden müssen

### Teilaufgabe 2 - Auswahl von Methoden zur *Intrusion Detection*

- Evaluation von IDS-Methoden
- Eingrenzung auf im Schienenverkehr umsetzbare Methoden
- Untersuchung des Simulators hinsichtlich Anwendbarkeit der Methoden in *Object Controllern*

### Teilaufgabe 3 - Umsetzung von ausgewählten Methoden und Simulation

- Prototypische Umsetzung der ausgewählten Methoden im Simulator
- Umsetzung der sog. Fehleroffenbarung, also die Meldung des Angriffs an die Leitstelle

# #4 Projektarbeit

## Intrusion Detection System für Object Controller



### Ziele:

- Evaluation der Grenzen derzeitig genutzter Security-Ansätze
- Weiterentwicklung derzeitiger Cybersecurity Ansätze im Schienenverkehr
- Aufbau einer Simulation zur Erprobung von IDS-Ansätzen

### Euer Beitrag:

- Spaß daran wie ein Angreifer zu denken
- Grundkenntnisse Simulation

### Euer Benefit:

- Einblicke in Cybersecurity im Bahnbereich
- Grenzen von Design-Ansätzen kennenlernen
- Networking zwischen verschiedenen Fachgebieten und mit Industriepartnern

## Cybersicherheit: Bahnindustrie entwickelt Lösungen

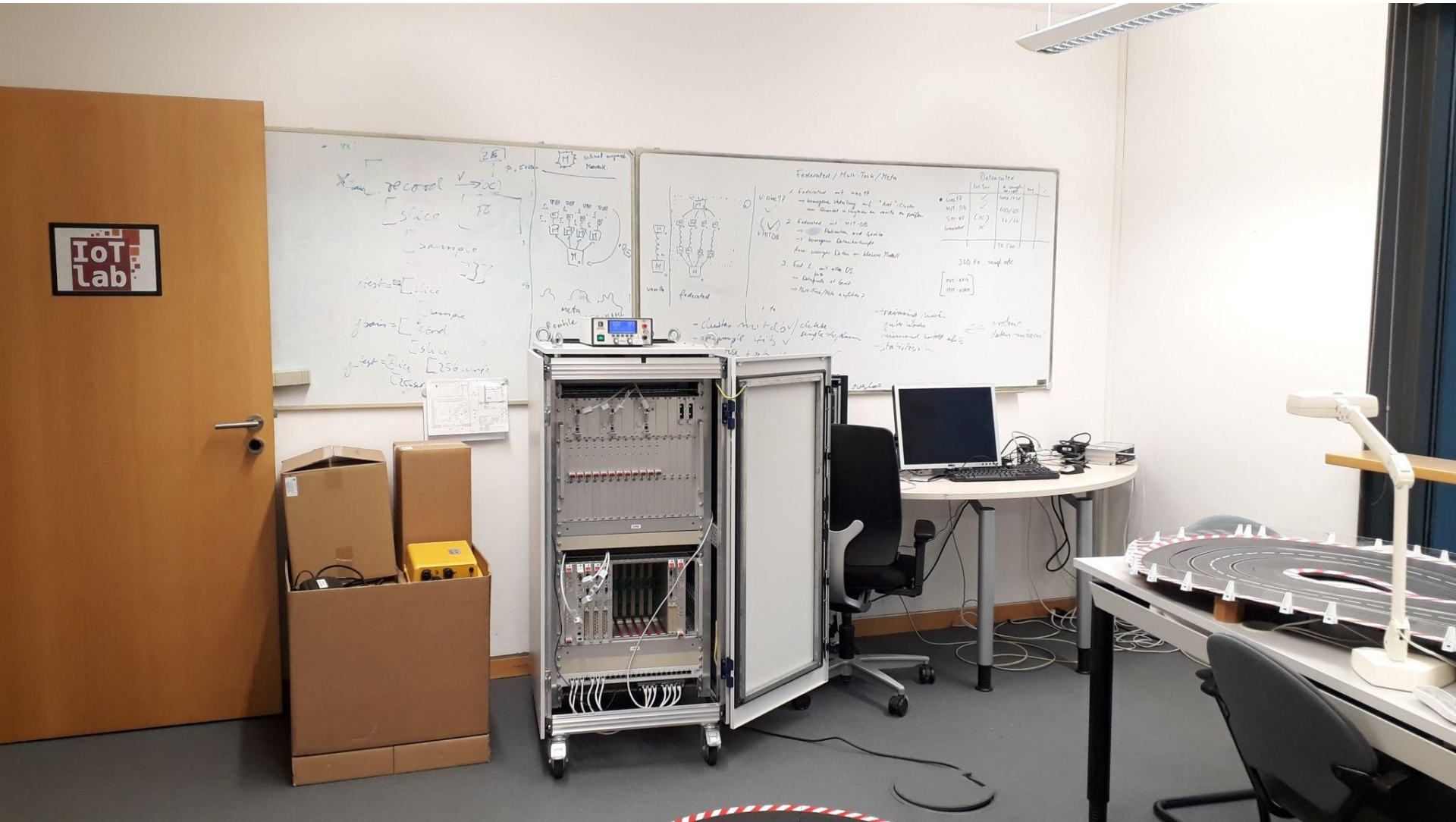
Die Zahl der Cyberattacken nimmt seit Jahren zu. Insbesondere der Schutz kritischer Infrastrukturen wird zu einer immer wichtigeren Aufgabe. Dies gilt auch für den Schienenverkehr, dessen Systeme zunehmend digital und vernetzt agieren – und dadurch angreifbar für Cyberkriminalität werden. Die heimische Bahnindustrie stellt sich der Herausforderung und entwickelt Lösungen. Quelle: Bahnindustrie.info

# Infrastruktur









## Hardware von Frauscher, Thales, voestalpine

### Frauscher FAdC

- Achszähl-OC für zwei Track Sections
- Konfiguration per CF-Karte
- Frauscher Stellwerkssimulator



### Thales Object Controller

- Point und Train Detection
- Konfiguration per Ethernet



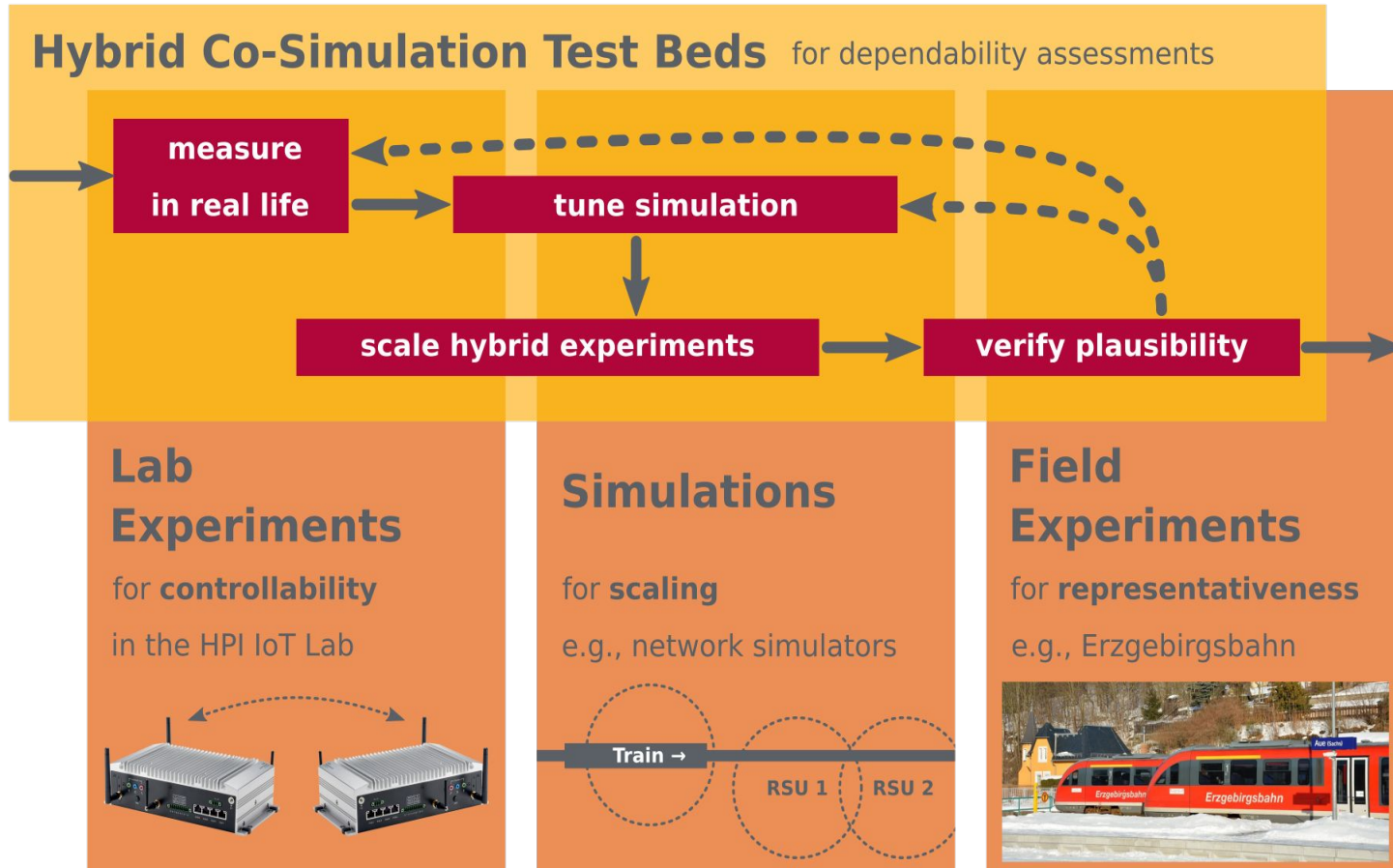
### Thales Kombinationssignal (LTE)



### voestalpine Weichenantrieb

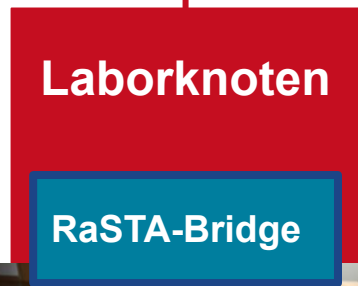
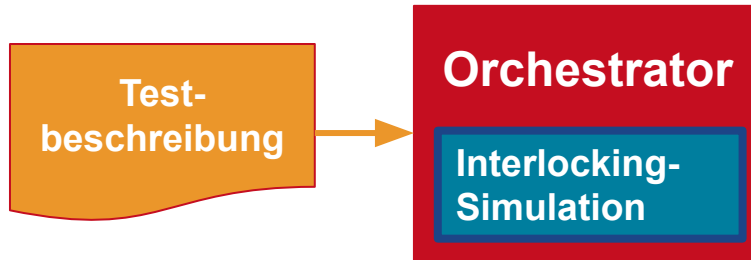


- building, DIY, testing, ...
- across/coupling of different domains
- model-driven and -supported approaches
- alternatives to specialized (test) hardware
- hardware, software and model "in the loop"
- focus on interoperability and dependability
- **hybrid, co-simulated**, and distributed setups

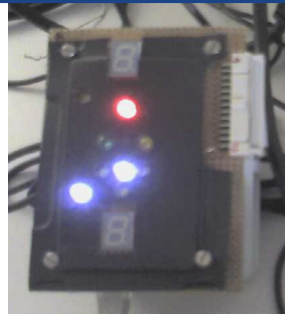
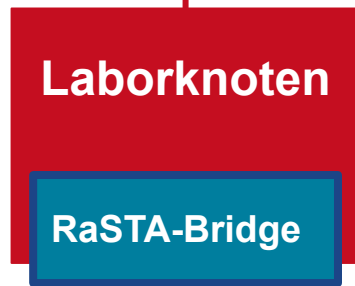




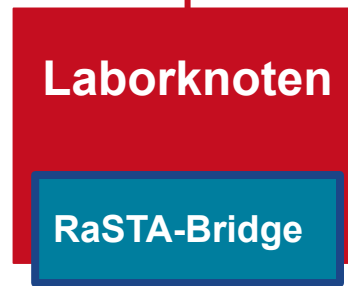
- building, DIY, testing, ...
- across/coupling of different domains
- model-driven and -supported approaches
- alternatives to specialized (test) hardware
- hardware, software and model "in the loop"
- focus on interoperability and dependability
- hybrid, co-simulated, and **distributed setups**



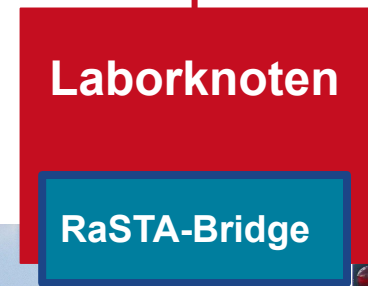
HPI IoT-Lab,  
Potsdam



Brunel,  
Hildesheim



Digital Rail Lab,  
Scheibenberg

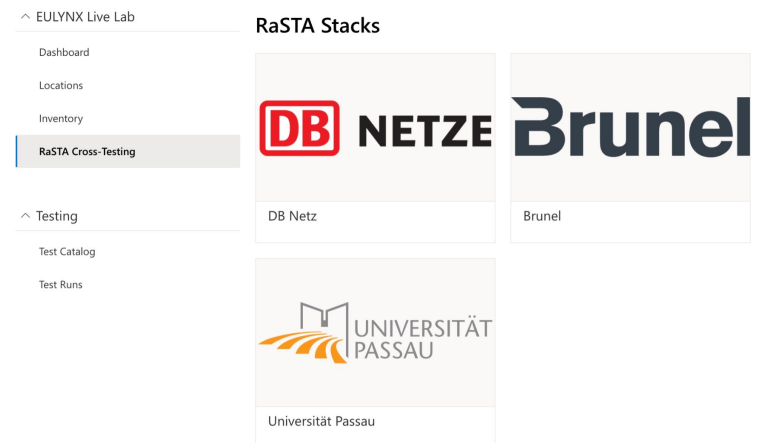
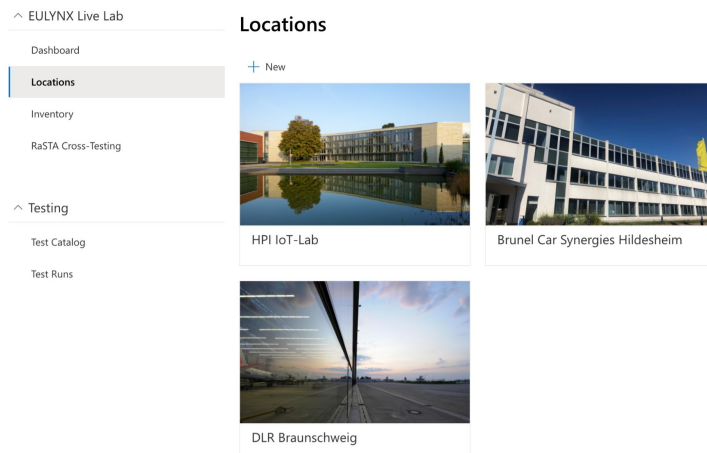


DLR,  
Braunschweig

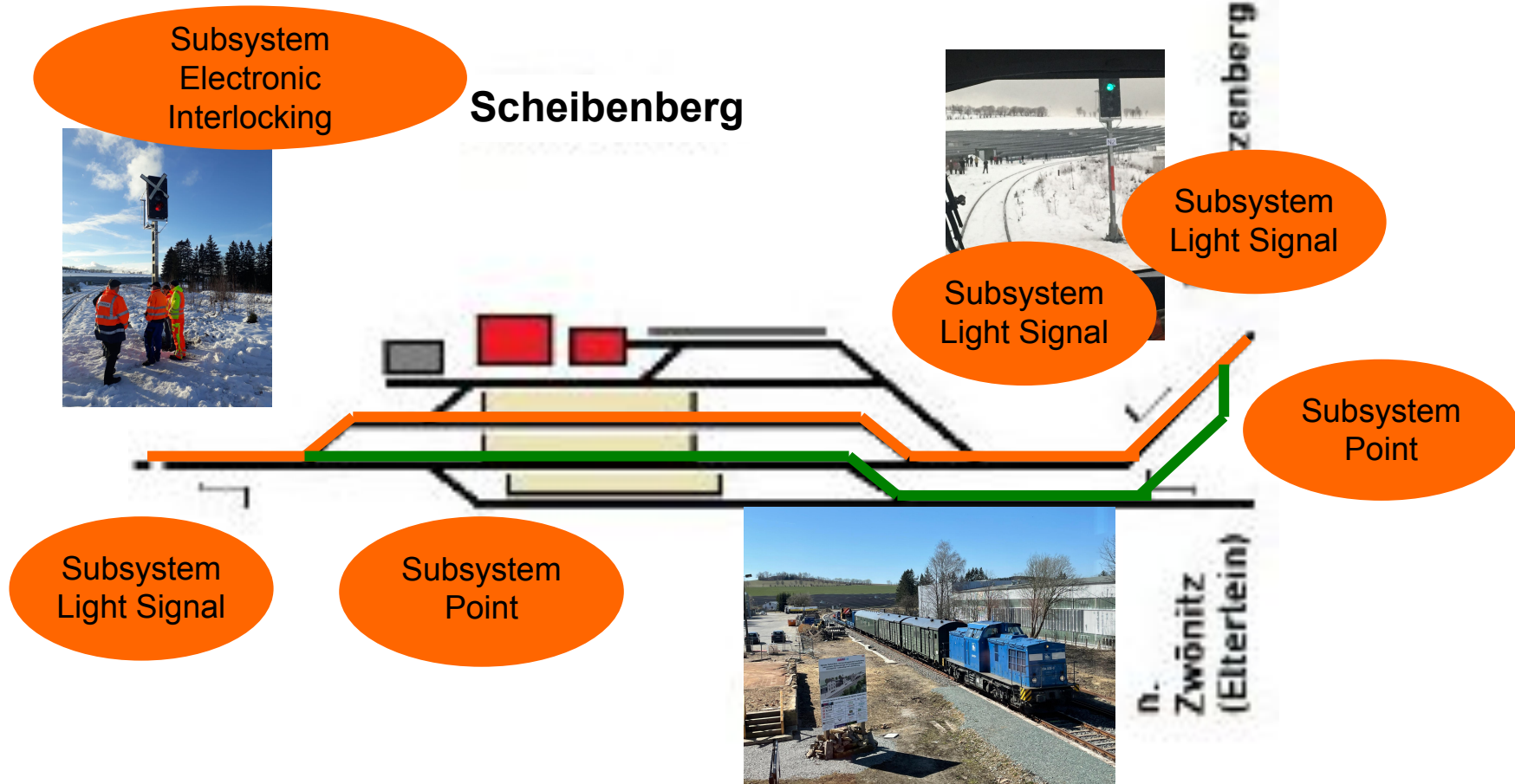
### Automatisierte Abnahmetests von Gesamtsystemen (Stw. und Feldelemente)

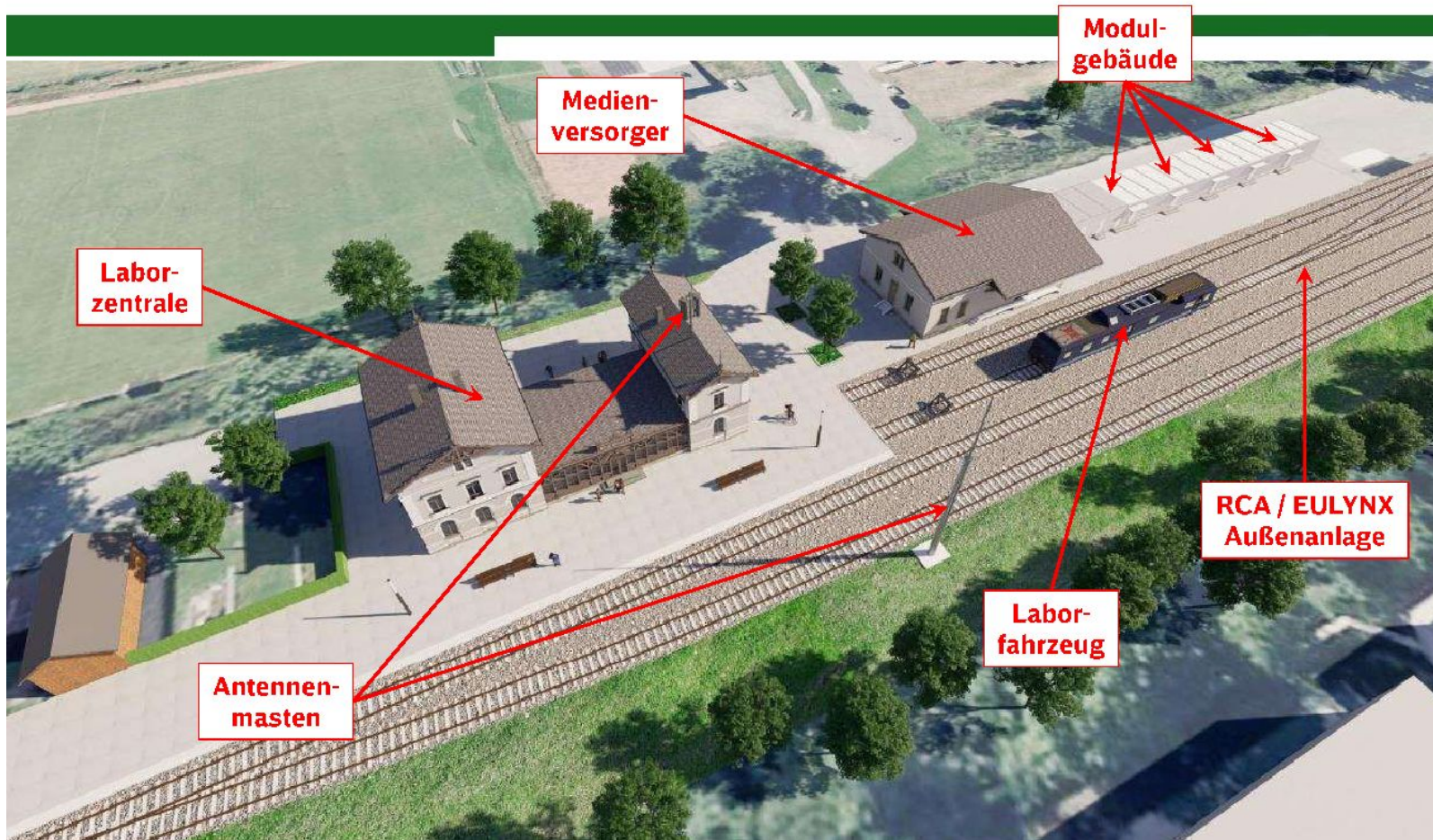
- EULYNX Testfallkatalog
- Verwaltung Laborstandorte, Geräteinventar
- Cross-Testing verschiedener RaSTA Implementierungen
- Co-Simulation

<https://lab.eulynx.live>

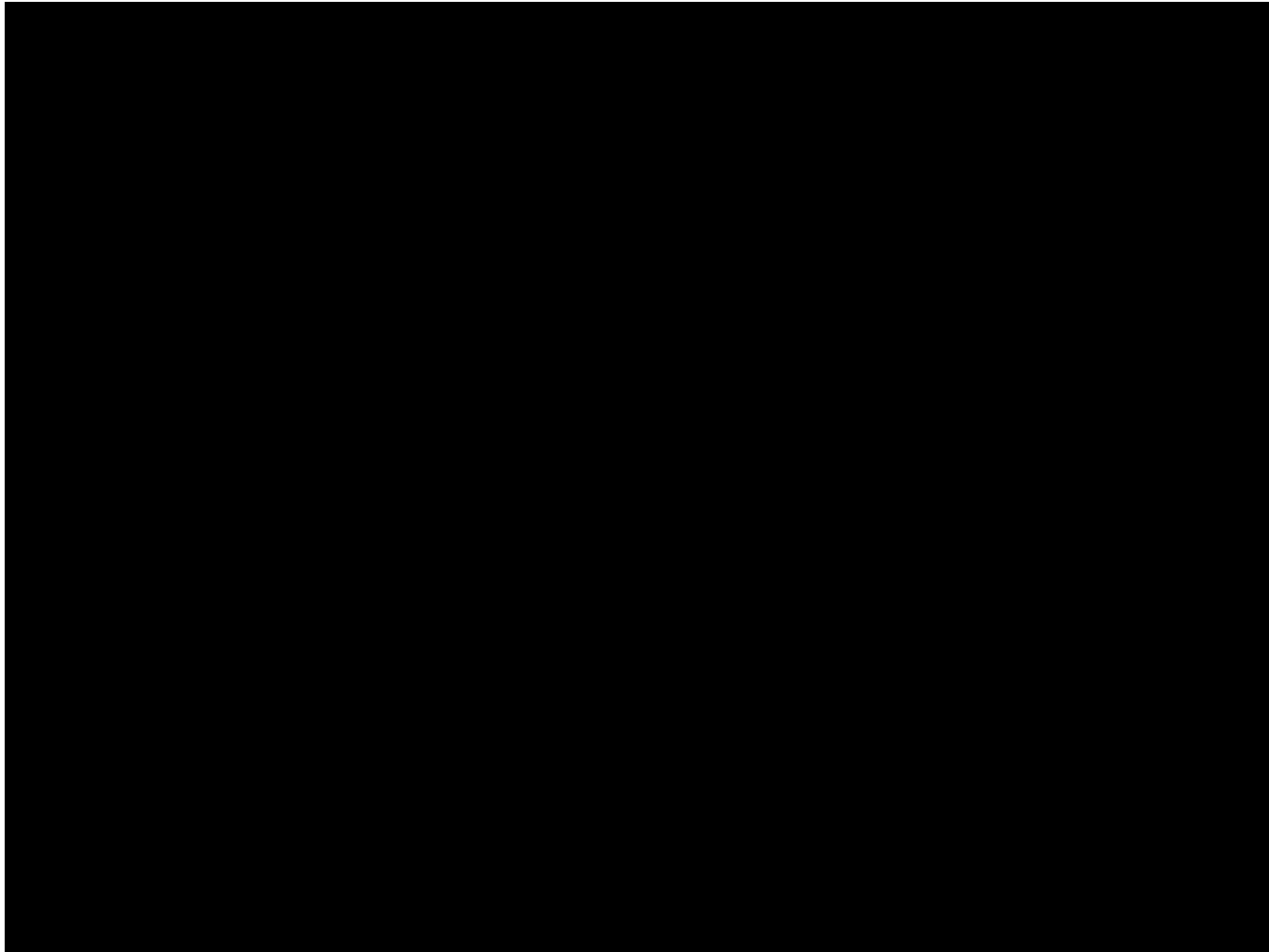








# Verteiltes IoT-Labor + Hersteller-Hardware + Erprobungsbahnhof Scheibenberg



# Nächste Schritte



- 6 ECTS
- Portfolioprüfung:
  - Projektaufgabe 1/2
  - Mündliche Prüfung o. MC-Test 1/2
- beide Prüfungsteile obligatorisch
- Prüfung ist insgesamt zu bestehen

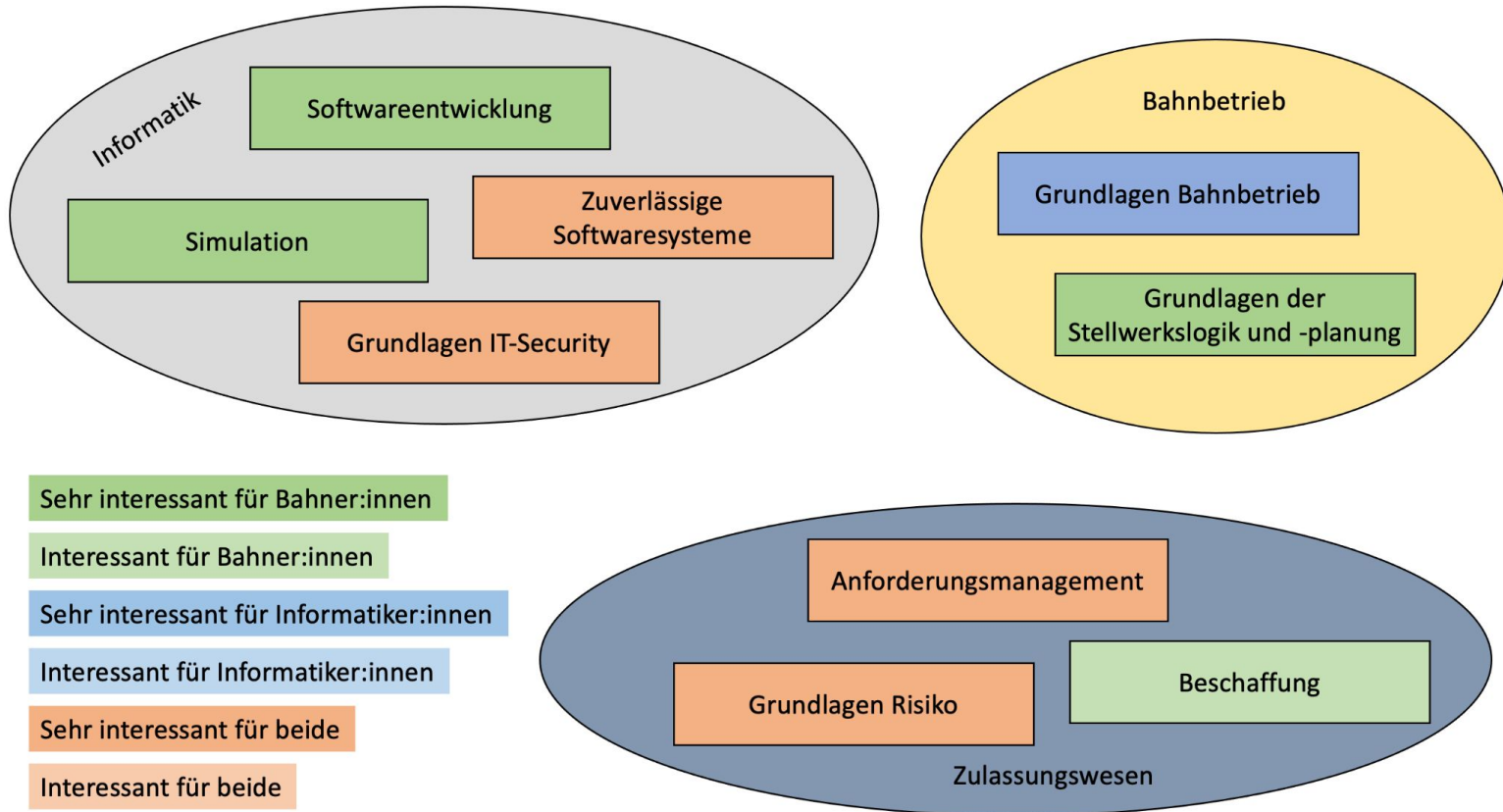
## Prüfungsanmeldung:

- QISPOS  
bis 08. Mai 2021
- Prüfungsamt  
siehe StuPO



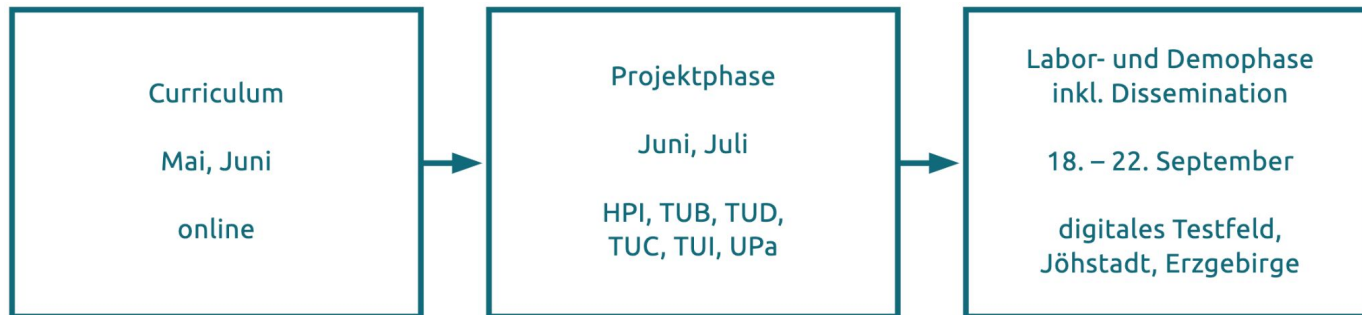
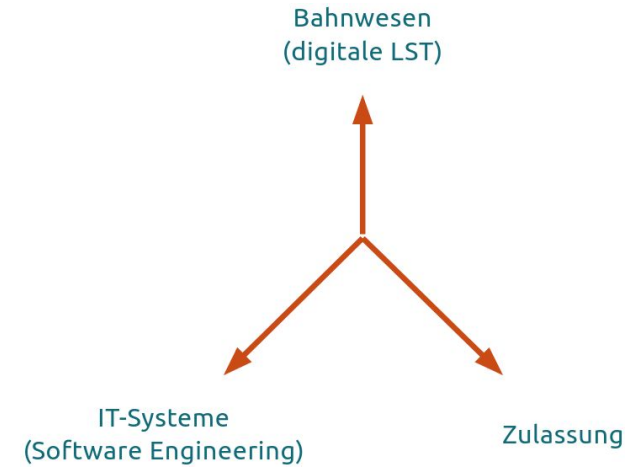
- Auftakttreffen am 20. April 2023, 13.00 Uhr
- Screencasts hören bis 11. Mai 2022
- Sprechstunde zu den Screencasts am 12. Mai, 13.30 Uhr
- Weitere Sprechstunden nach Bedarf
- Gastvorlesungen nach Vorankündigung
  
- Projektarbeiten beginnen zu unterschiedlichen Zeitpunkten
  - Projektarbeit TU Berlin beginnt am 29. April 2022

- Zu hörende Screencasts: <https://osm.hpi.de/drss/2023/curriculum/>



Die genaue Auswahl der Videos erfolgt in Abstimmung mit der Heimat-Uni und dem Projekt

# Digital Rail Viel Spaß!







Birgit Milius (TUB)

[birgit.milius@tu-berlin.de](mailto:birgit.milius@tu-berlin.de)

Andreas Polze (HPI)

[andreas.polze@hpi.de](mailto:andreas.polze@hpi.de)

Simon Unger (Uni Passau)

[simon.unger@uni-passau.de](mailto:simon.unger@uni-passau.de)

Armin Zimmermann (TU Ilmenau)

[Armin.Zimmermann@tu-ilmenau.de](mailto:Armin.Zimmermann@tu-ilmenau.de)

Matthias Werner (TUC)

[mwerner@informatik.tu-chemnitz.de](mailto:mwerner@informatik.tu-chemnitz.de)

Ulrich Maschek (TUD)

[ulrich.maschek@tu-dresden.de](mailto:ulrich.maschek@tu-dresden.de)

Max Schubert (INCYDE)

[max.schubert@incyde.com](mailto:max.schubert@incyde.com)

Martin Lehnert (TH Wildau)

[martin.lehnert@th-wildau.de](mailto:martin.lehnert@th-wildau.de)