Joint Final Conference CONNECTA & Safe4RAIL

Paris, 26th September 2018

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

Joint Final Conference

- CONNECTA and Safe4RAIL
  - Blueprint for next-generation TCMS
  - More functionality and interoperability, lower system complexity and cost

Goals of today's event

- Inform and learn about the technological developments in an early stage
  - new solutions for existing technological challenges to make the TCMS systems more cost-efficient and more reliable at the same time, while keeping current safety levels.

Agenda

Start	End	Topic	Partner	Duration
9:00	9:30	**Registration**		
9:30	9:40	**Opening of the Final Conference**	Javier Goikoetxea (CAF) Arjan Geven (TTTech)	0:10
9:40	9:55	**Welcome and Background**	Sébastien Denis (Shift2Rail JU)	0:15
9:55	10:20	**General Presentation of CONNECTA & Safe4RAIL**	Javier Goikoetxea (CAF) Arjan Geven (TTTech)	0:25
10:20	10:40	**General Specification of next-generation TCMS**	Stefan Tesar (Deutsche Bahn)	0:20
10:40	11:15	**Drive-by-Data & Integrated Modular Platform**	Gernot Hans (Bombardier) Mirko Jakovljevic (TTTech)	0:35
11:15	11:35	*Coffee break*		0:20
11:35	12:05	**Functional Distribution Framework**	Xabier Artaetxebarria (CAF) Iñigo Odriozola (Ikerlan)	0:30
12:05	12:40	**Integrated FDF & DbD Demo**	Arjan Geven (TTTech) Iñigo Odriozola (Ikerlan) Maryam Pahlevan (USIE)	0:35
12:40	13:00	**Application Profiles**	Thomas Waschulzik (Siemens)	0:20
13:00	14:00	*Lunch*		1:00

Agenda

14:00	14:25	**Functional Open Coupling**	Vincent Mayeux (Alstom)	0:25
14:25	15:05	**Distributed Simulation Framework / Virtual Certification**	Tobias Pieper (U. Siegen) Mikel Colera (CAF)	0:40
15:05	15:35	**Electronic Brake-by-wire**	Angelo Grasso (Faiveley) Ugo Prosdocimi (Eletech)	0:30
15:35	15:55	*Coffee break*		0:20
15:55	16:10	**Wireless Train-2-Ground (T2G)**	Armin Heindel (Siemens) Richard Pecl (Unicontrols)	0:15
16:10	16:25	**Wireless Train Backbone (WLTB)**	Igor Lopez (CAF)	0:15
16:25	16:40	**Revisiting InnoTrans Demonstrator**	Javier Goikoetxea (CAF)	0:15
16:40	17:00	**Wrap-up / Closing**	Javier Goikoetxea (CAF) Arjan Geven (TTTech)	0:20
17:00	17:00	**End of Conference**		

Shift2Rail presentation

CONNECTA & SAFE4RAIL Final Conference
Paris 26 September 2018

Sébastien DENIS

Programme Manager

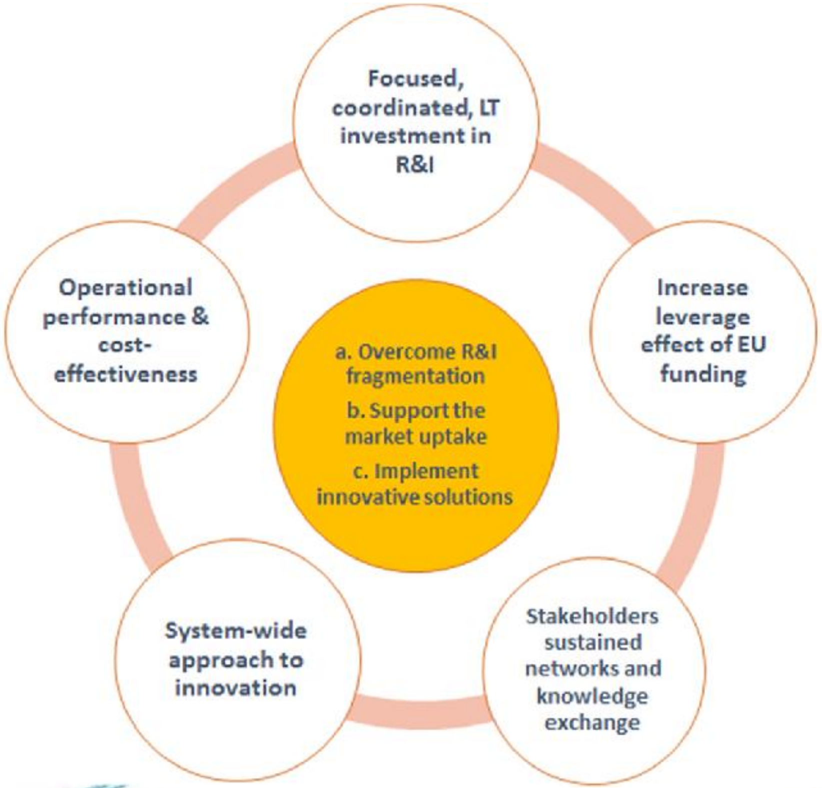
S2R Joint Undertaking

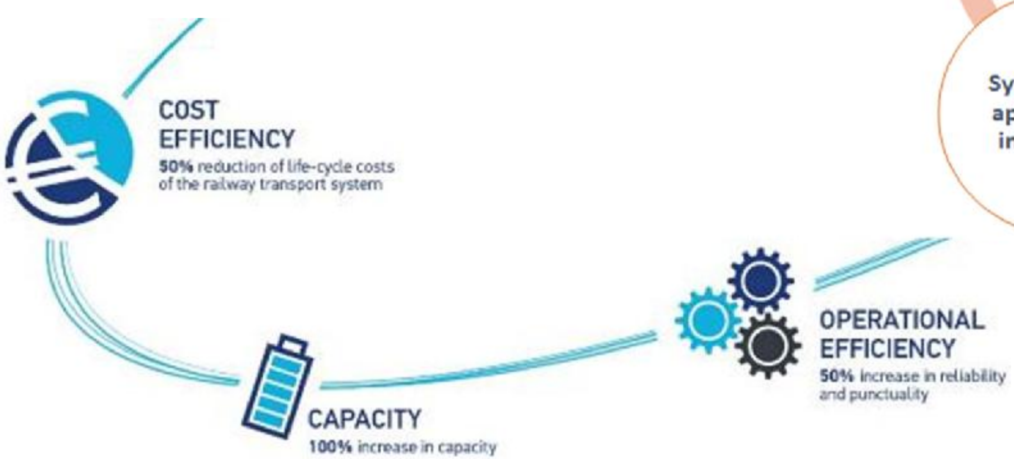
@Shift2Rail_JU
#Horizon2020

S2R PUBLIC PRIVATE PARTNERSHIP

A NEW APPROACH TO R&I IN RAILWAY

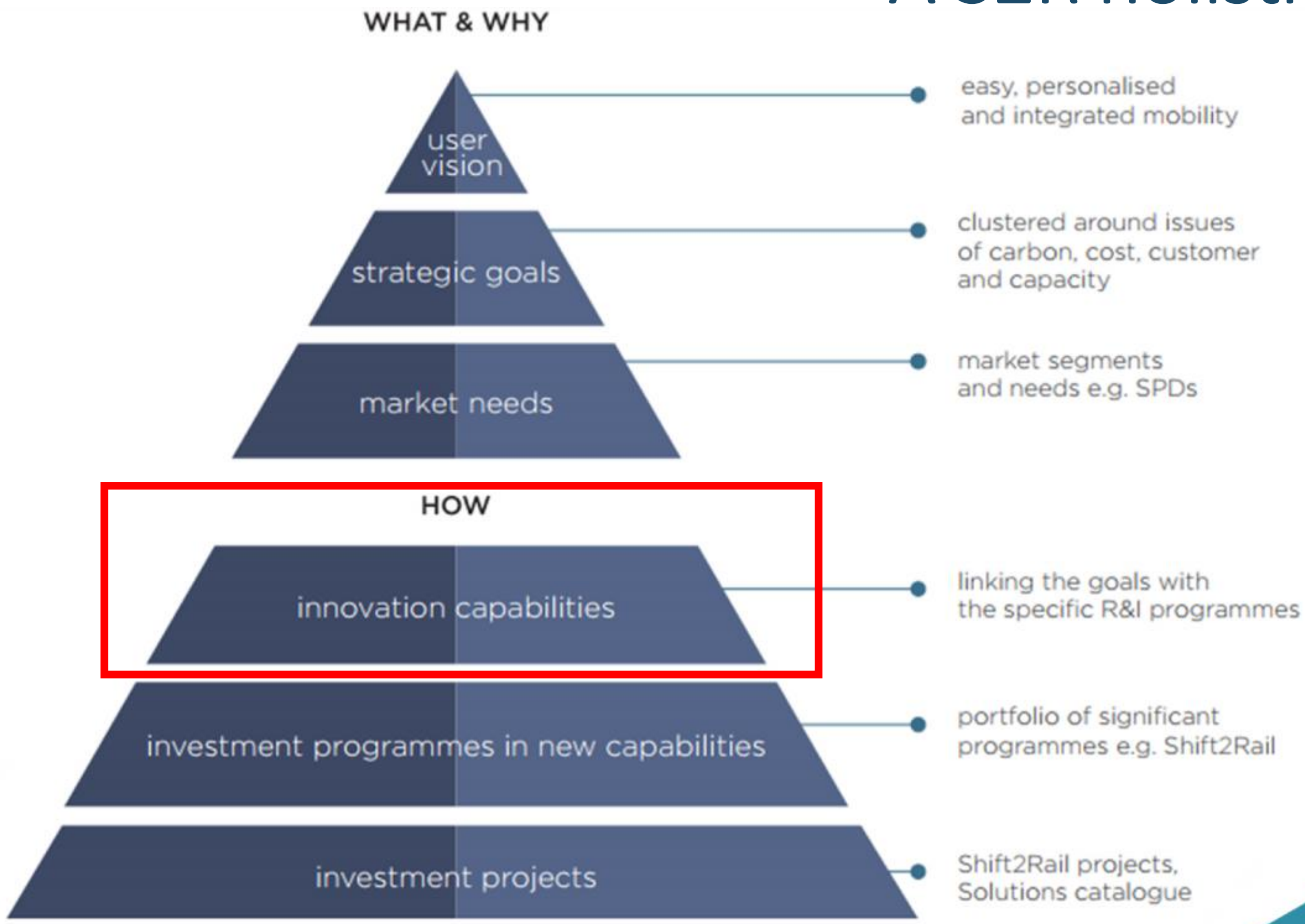
Working together & driving innovation



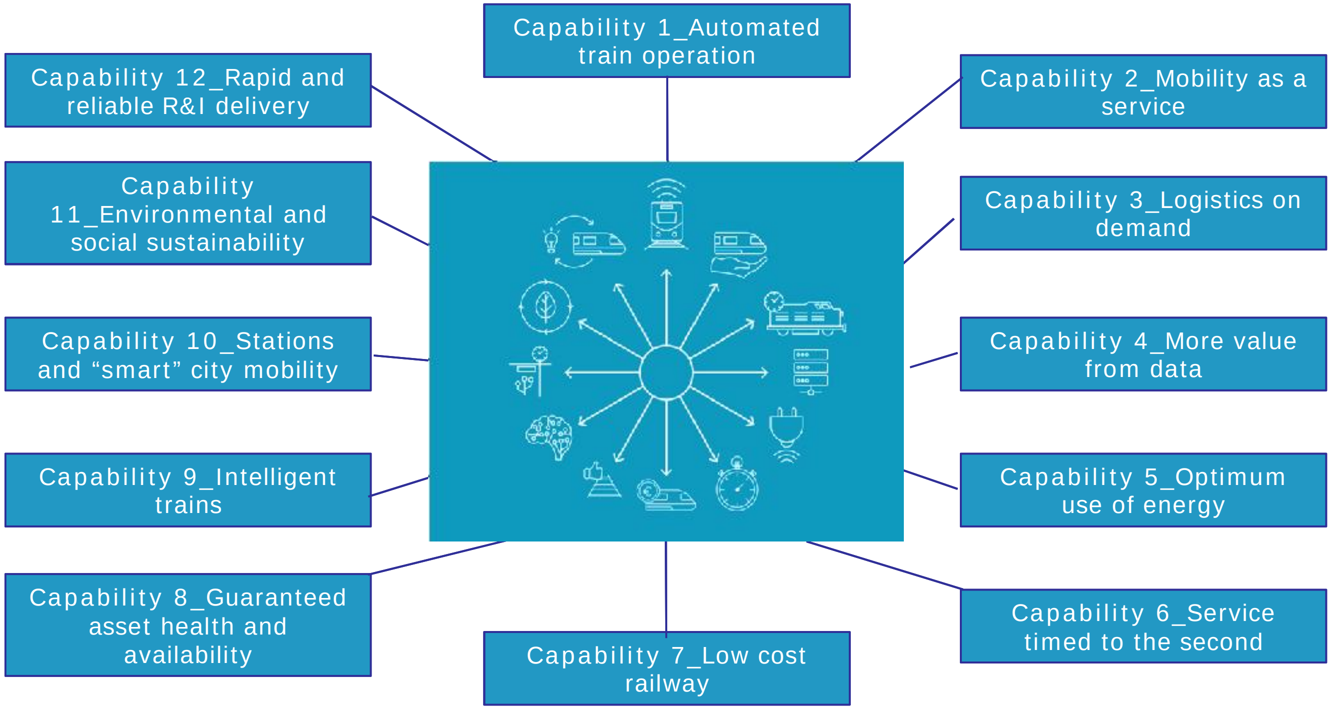


Shift2Rail

A S2R holistic approach…

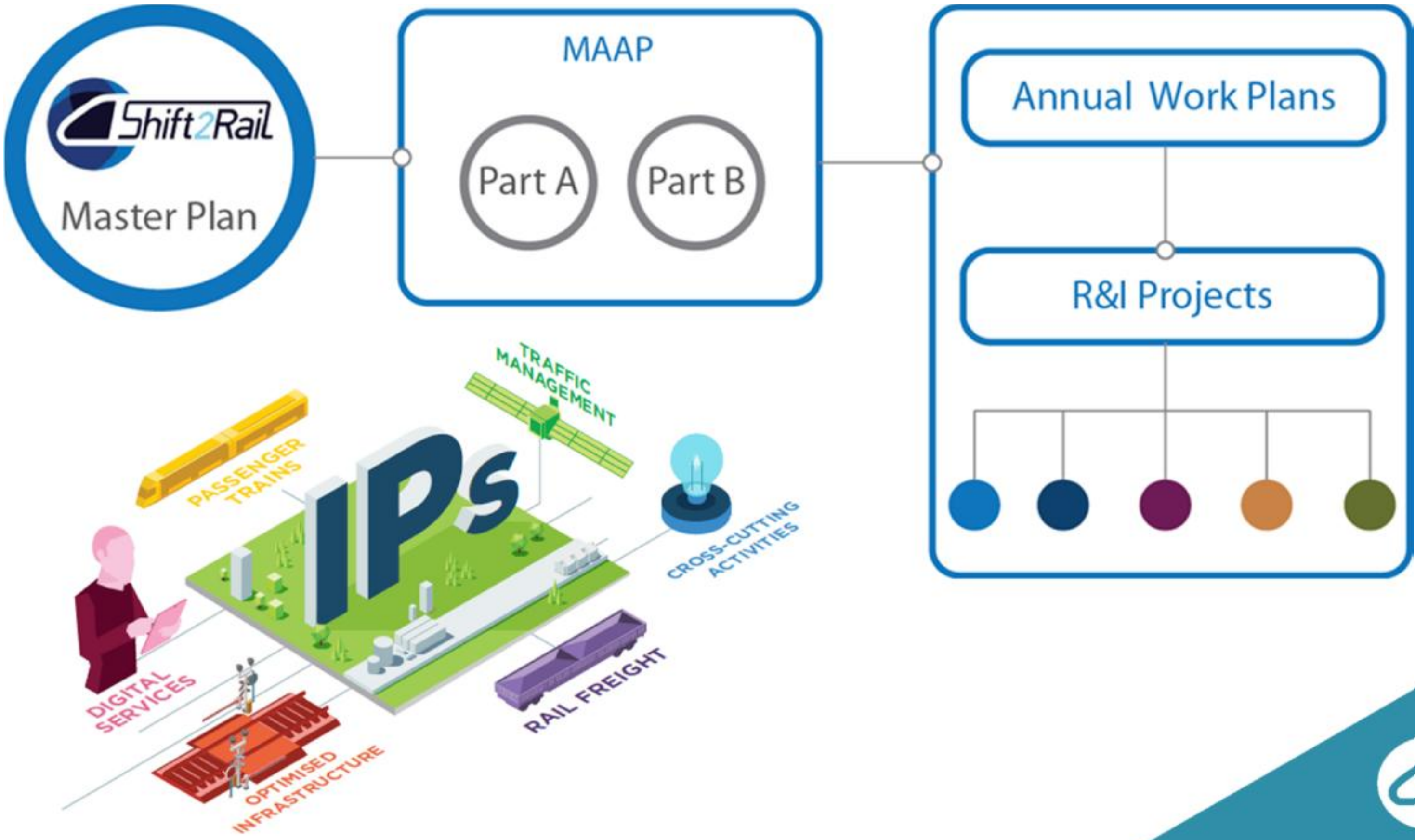


Innovation Capabilities



A S2R holistic approach…

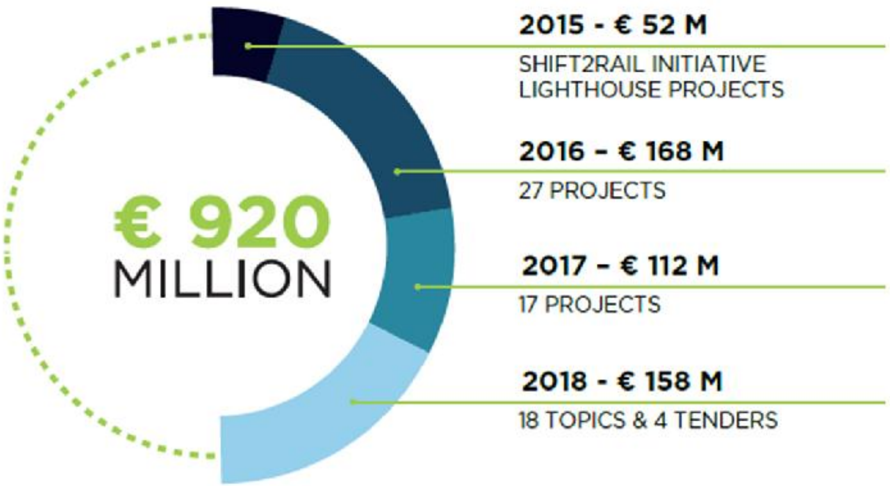
The S2R Programme implementation



S2R Key Data

S2R BUDGET 2014-2020

S2R FUNDING IS AVAILABLE THROUGH
CALLS FOR MEMBERS, OPEN CALLS FOR PROPOSALS & PROCUREMENT



S2R Key Data

UNIQUE PARTNERSHIP[1]

S2R is sustaining the competitiveness of the European rail industry to meet future mobility needs of EU citizens, acting as a rail R&I hub bringing together the manufacturers, rail operators, SMEs and research institutions.

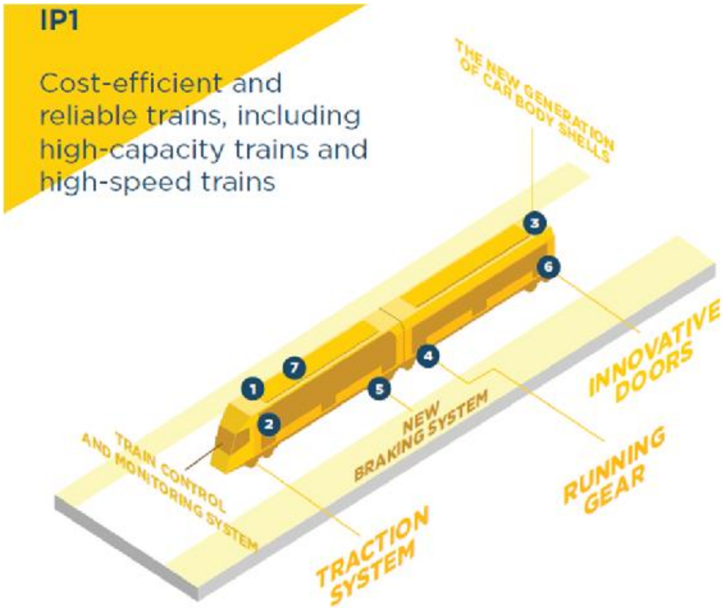
28
MEMBERS

343
PARTICIPANTS INVOLVED FROM **27** COUNTRIES

92
SMEs

84
RESEARCH CENTRES AND UNIVERSITIES

IP1 Results



Designing and Prototyping components in SiC in the full traction system

Wheel Slide Protection Validation on test rig

Prototypes for innovative running gear components (e.g. wheelset for metro bogie, composite antenna

Shift2Rail

Other IPs Results : examples

Technical enablers for Travel Companion

Specifications for Automatic Train Operations (ATO) semi-automated trains over ETCS

3D Simulator for interior and exterior noise

Intelligent Video Gate Demonstrator

Proof of concept for smart energy metering

Shift2Rail

Thank you for your attention

@Shift2Rail_JU
#Horizon2020

General Presentation of CONNECTA & Safe4RAIL

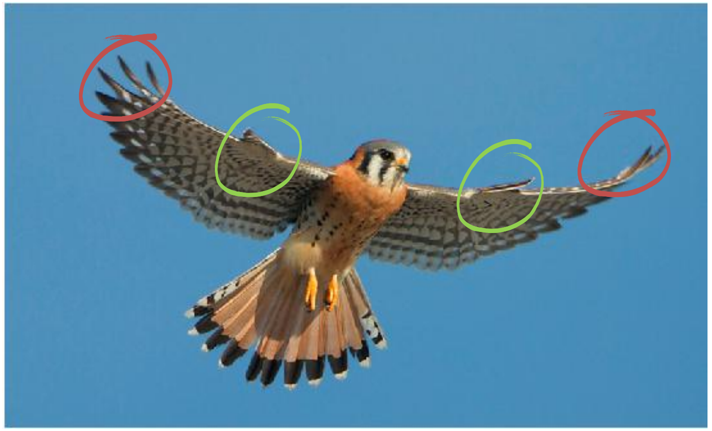
Javier Goikoetxea (CAF) & Arjan Geven (TTTech)

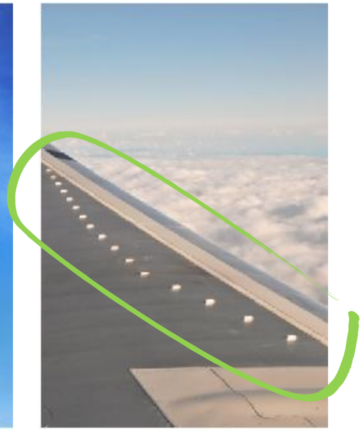
CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

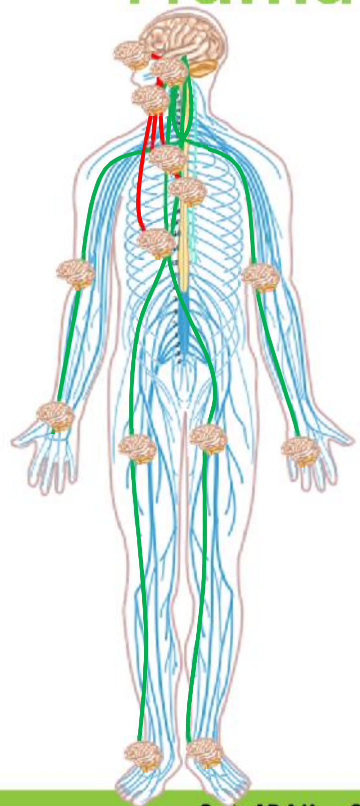
Who is the best engineer ever?

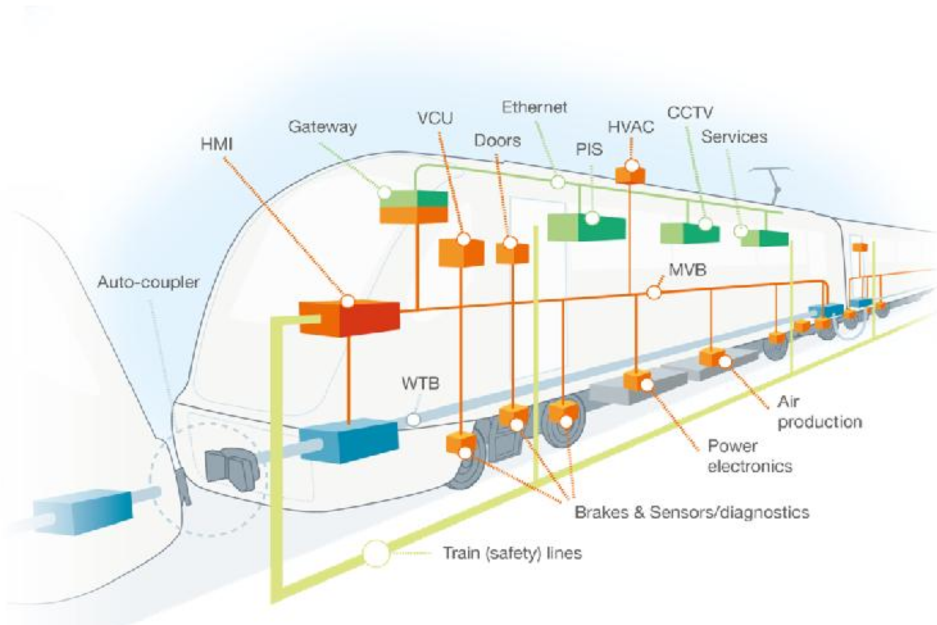




Human body, a clever system

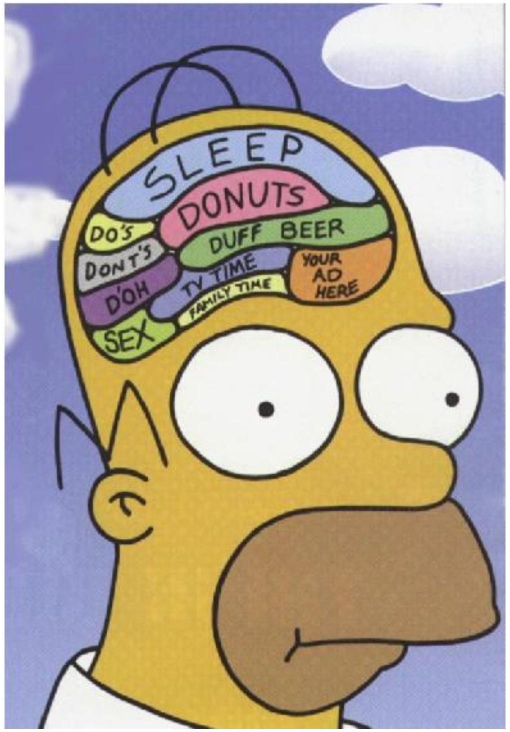
Human nervous central system



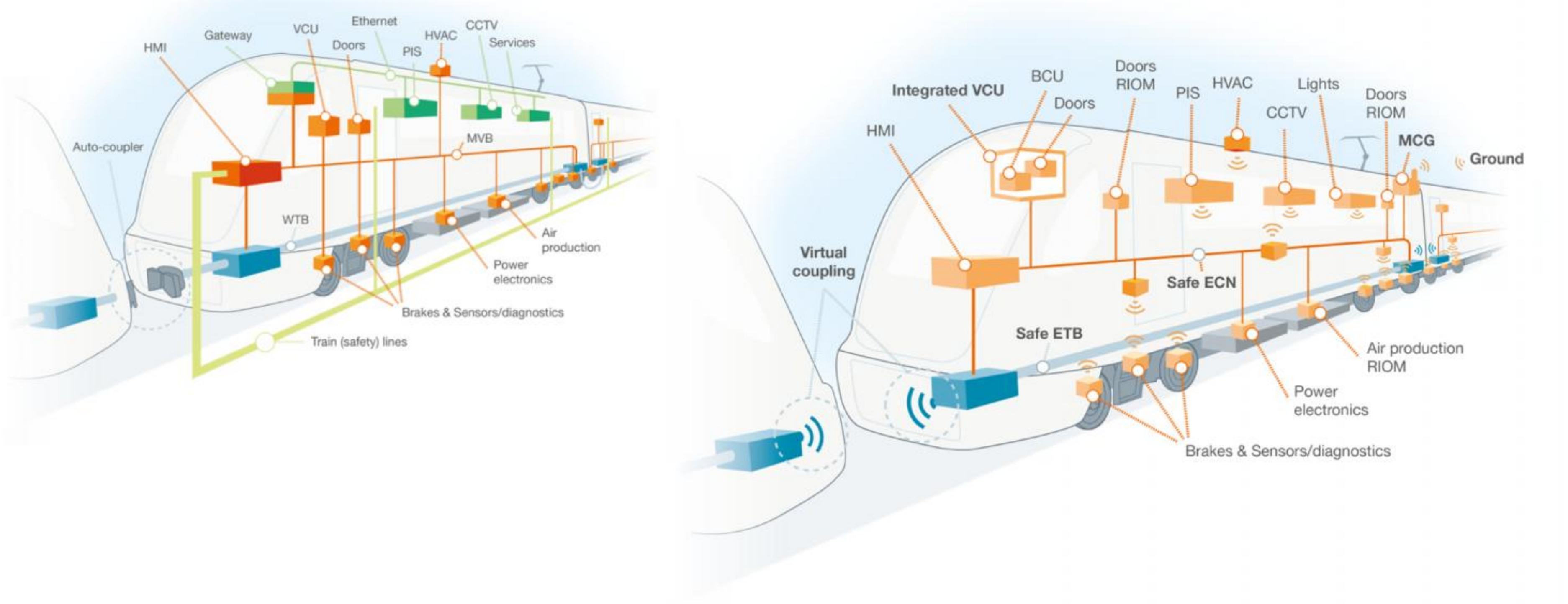


Train nervous central system

A well structured brain



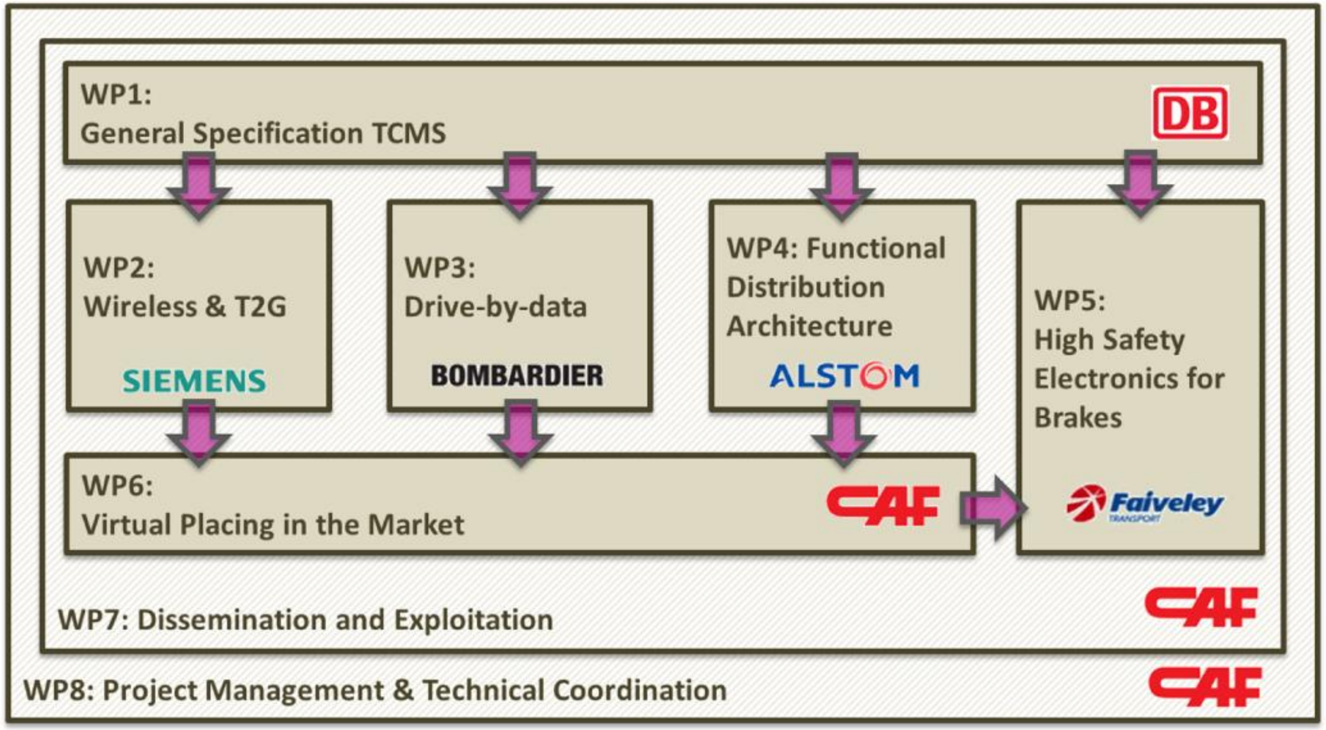
CONNECTA (TD1.2) vision



CONNECTA objectives

CONNECTA aims at contributing to the S2R's next generation of TCMS **architectures** and **components** with wireless capabilities as well as to the next generation of electronic braking systems. **CONNECTA** will conduct research into **new technological concepts**, **standard specifications** and **architectures** for train control and monitoring, with specific applications in train-to-ground communications and high safety electronic control of brakes.

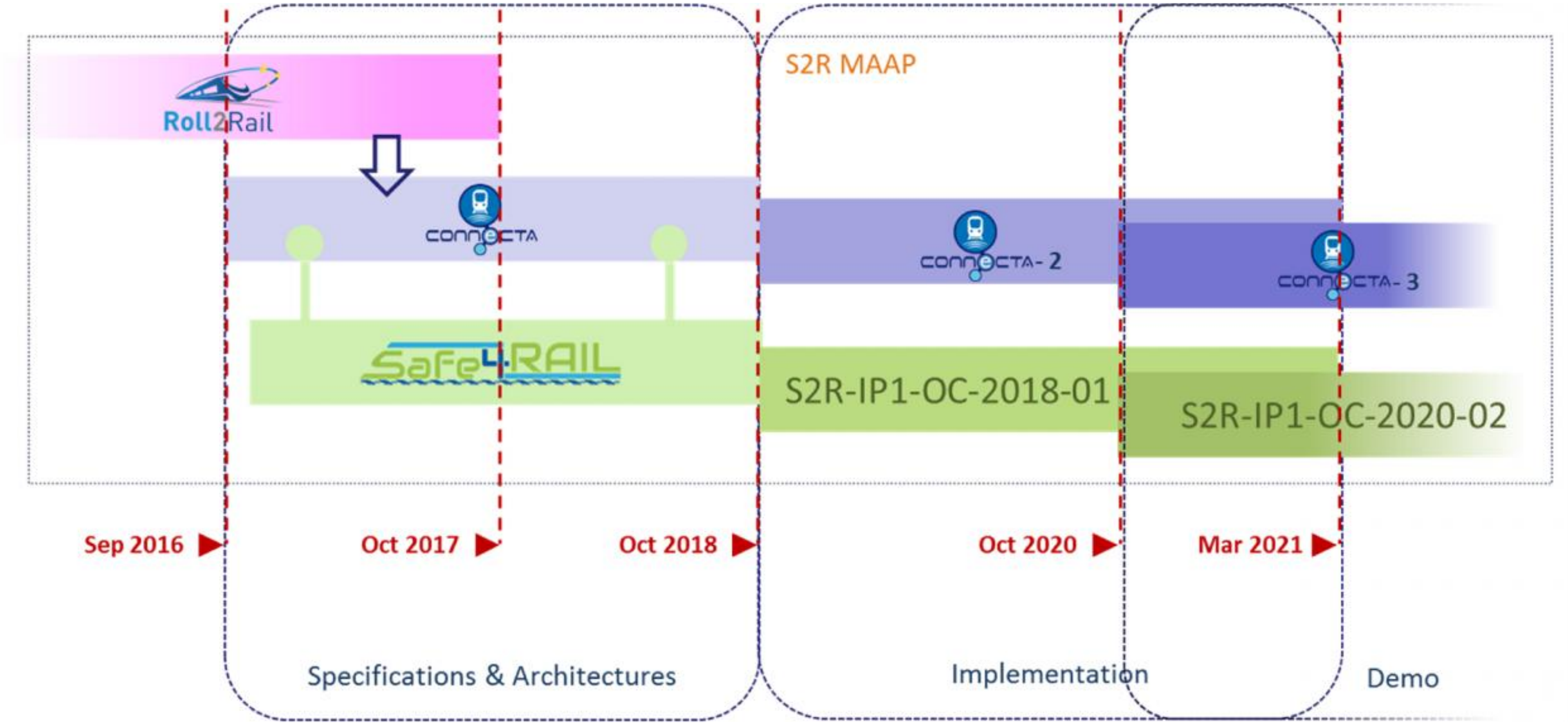
Project structure and main facts



- 1 September 2016
- 30 September 2018
- 33 deliverables
- 13.3 M€
- 5.9 M€
- www.s2r-connecta.eu

ALSTOM, BOMBARDIER, SNCF, Ansaldo STS A Hitachi Group Company, CAF, Faiveley Transport, DB, SIEMENS, KNORR-BREMSE

Shift2Rail TD1.2 TCMS



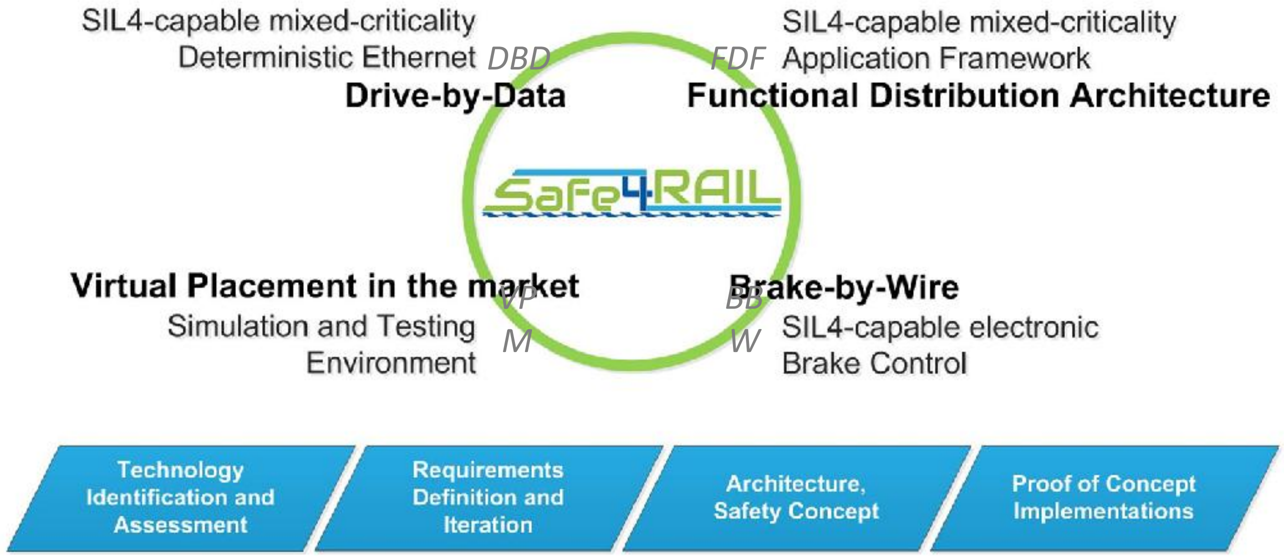
About Safe4RAIL

- „Open Call“ Project to support the achievements of Shift2Rail
  - IP1 “Cost-effective and Reliable Trains”
  - TD1.2 “Train Control and Monitoring System (TCMS)”

- Project data:
  - Start of the project: Oct 2016
  - End of the project: Dec 2018 (27 months)
  - Complementary project: CONNECTA

- Project partners:

Safe4RAIL Project objectives



Technology and feasibility studies

Safe4RAIL Video

Safe4RAIL Partner overview

Enterprise	TTTech Computertechnik AG	AT
	IAV Ingenieursgesellschaft für Auto und Verkehr GmbH	DE
	Eletech S.r.l.	IT
	TÜV Süd Rail GmbH	DE
SME	NIER Ingegneria S.p.A.	IT
	TECHNIKON Forschungs- und Planungsgesellschaft mbH	AT
	UniControls A.S.	CZ
	NewTec GmbH System-Entwicklung und Beratung	DE
RTD	IK4-Ikerlan SCL	ES
	Universität Siegen	DE
	IFSTTAR	FR

QUESTIONS & ANSWERS

General Specification of next-generation TCMS

Stefan Tesar, DB

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

What is the General Specification NG TCMS?

- It describes what a **NG TCMS needs to do**
- It describes the **functions of the NG TCMS**
- It describes what functions a **NG TCMS needs to fulfil**
- It's the **basis** for the development **of the NG TCMS**
- It's the basis for **ALL further development**

Why General Specification TCMS?

Today	NG TCMS SPECIFICATION
TCMS today is described by requirement specifications	The NG TCMS is described by its functions by User Stories and Use Cases
TCMS today is described by long lists of requirements	For the NG TCMS we used a SysML Modelling Tool, named Magic Draw
Local Databases within company	Tracing from functional requirement to technical requirement to implementation
Working on databases within the company LAN	Europe wide collaboration to work on the general specification on a secure server
Inconsistencies in requirement specifications	Structured procedure from function to technical implementation

System Engineering

- Engineering and Modelling the System Step by Step

SB • Definition of the System's boundaries

EP • Definition of Epics as funtion groups

AC • Analysis of the actors

US • Creation and compilation of User Stories

UC • Creation and compilation of Use Cases

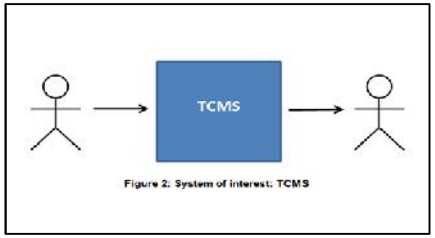
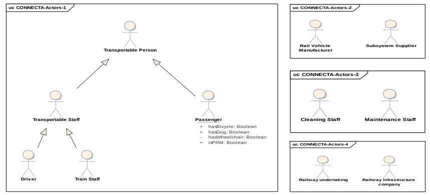
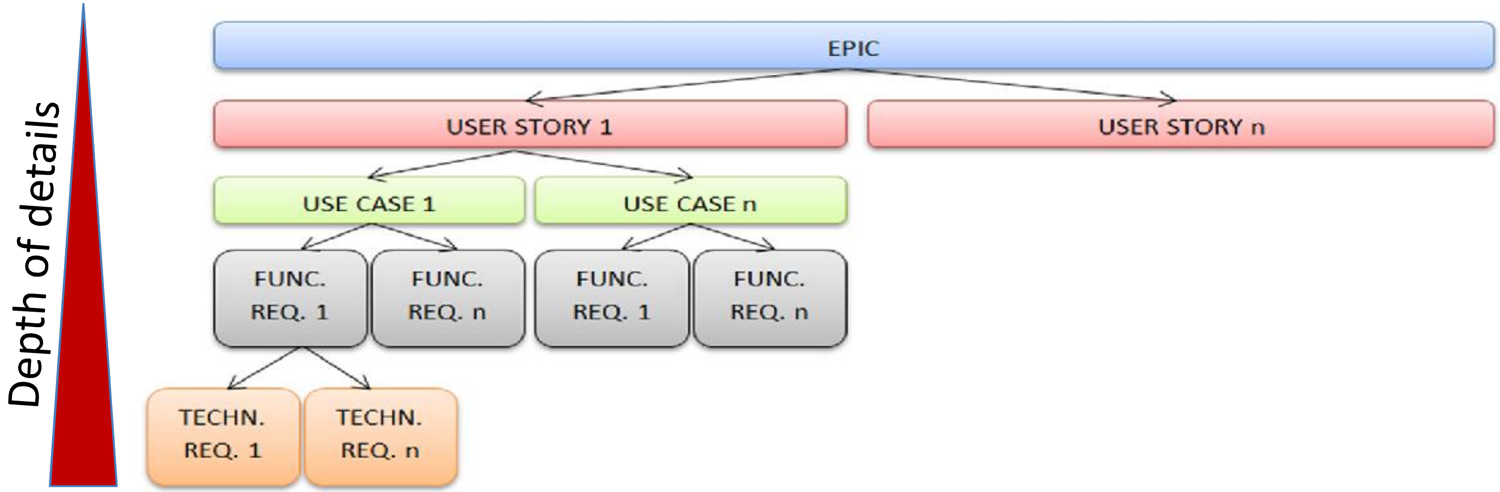


Figure 2: System of interest: TCMS



Structuring the „General Specification“

- From the system’s Big Picture to the technical detail
- Structure for functional specification created Epics - UserStories - UseCases - non functional requirements



Functional System Development II
User Stories

A "user story" describes what a user wants to achieve with the system. It describes the **"who", "what"** and **"why"** of a request at the highest abstraction level.

The user story sentence template is:

"*As a <role>, I want <goal/desire> so that <benefit>*"

Example:

1. As a train driver, I want to release the doors so that passengers can exit and enter the train.
2.

…

300.

Functional System Development III – Use Cases

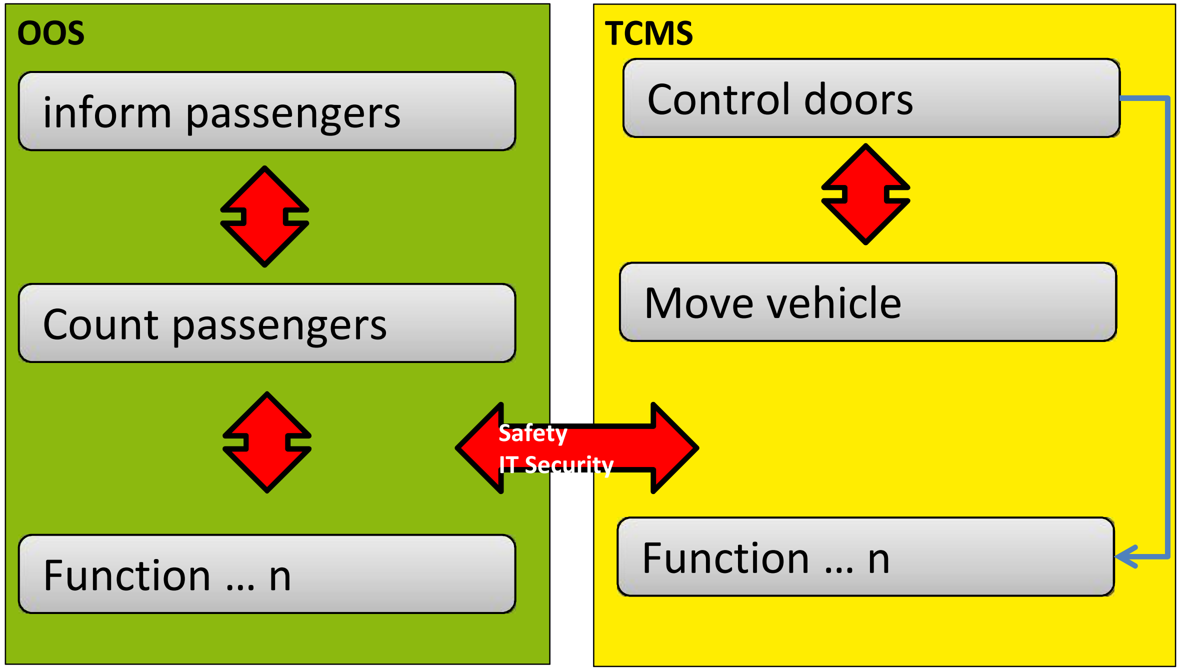
- A use case describes the different ways a user (actor) can use a system to achieve a specific goal. An entire set of use cases describes all uses of the system and the resulting benefits. A complete set describes the scope of the system - which functions it fulfills and which function does not.

ID	Epic	User Story ID	Name	Short Description	Basic Flow	Subject	PrimaryActor	SecondaryActor	Trigger	Precondition
UC-1.2-008	[1.2] Superordinated Vehicle Control		Set Seat Reservation	The RU wants to set the seat reservation.	1.) RU has the collec ted data forthe seat reservation of the train 2.) RU triggers the transfer mechnism 3.) Information is received by train 4.) Reservation system transfer the reservation information to the seat	TCMS	Railway Undertaking		Railway Undertaking uses the Set Seat Reservation Mechanism to set the seat reservations.	PIS is onlin communic

Functional System Development III: Logical architecture

Logical structures of a system.

The communication requirements between the functions are shown. Interfaces do derive from that



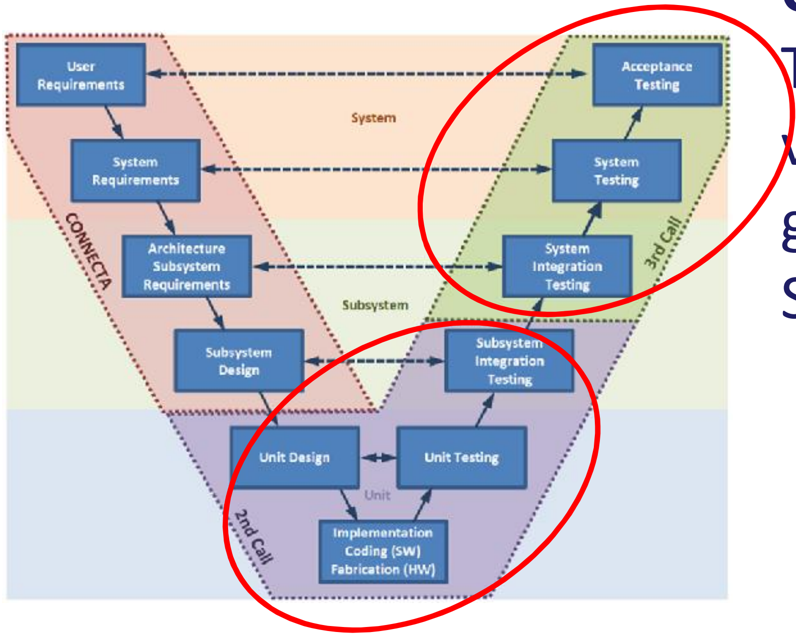
Functions of a system and their classification to a function domain are shown

Conclusions

- NG TCMS needs to be **modeled by using SysML** due to the high complexity
- Great **team collaboration** that supports the common understanding of the system
- The "General Specification" **leaves open space** for possible technical implementations
- The "General Specification" will be **consequently updated, specification gaps closed** with new insights generated during the system development

Next station is

CTA II:
Development of the NG TCMS based on the general specification and iteration loops



CTA III:
Testing and validation of the general Specification

QUESTIONS & ANSWERS

Drive-by-Data & Integrated Modular Platform

Gernot Hans, Bombardier Transportation

Mirko Jakovljevic, TTTech Computertechnik AG

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

What is Drive-by-Data?

- Drive-by-Data investigates and specifies a new generation of train onboard communication network (NG-TCN).
- The NG-TCN shall interconnect all on-board devices including
  - TCMS (with safety function up to SIL4 like doors, brakes, …)
  - CCTV, PIS, … (operator oriented services)
  - ETCS Level 3 onboard equipment, ATO
  - Passenger WiFi (customer oriented services)
- NG-TCN adopts the established Ethernet network topology of a static consist network and a dynamic train backbone

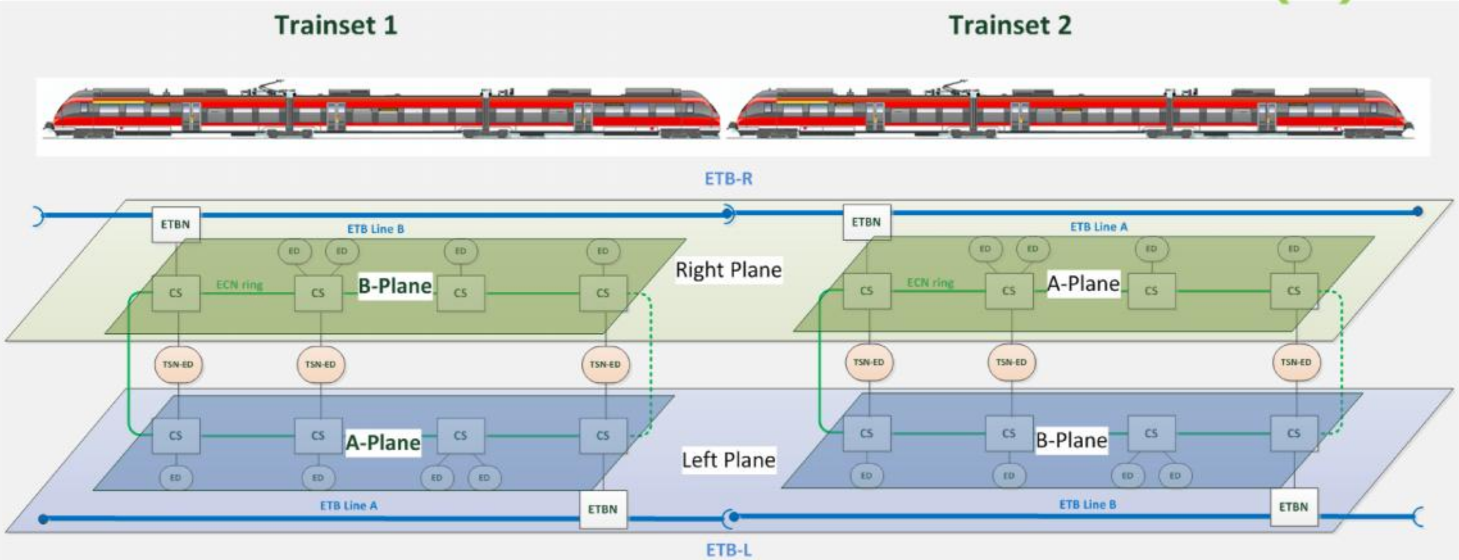
Why Drive-by-Data?

Today	With Drive-by-Data
Complexity: High networked system complexity High amount of cabling, for e.g. safety lines, signalling, safety and control functions.	Unified networking infrastructure with high part commonality, reduced system complexity and improved reliability,
Lifecycle: Limited network reconfigurability, upgradeability and scalability for new functions	Reduced integration and (re)commissioning effort and costs. Support for simplified verification and modular certification. System integration does not affect the behaviour of already integrated and verified functions.
Performance: Limited determinism and support for "functional distribution" (missing support for fault propagation prevention, QoS/latency/jitter control, system-level time partitioning)	Safe integration of all mixed-criticality safety functions (up to SIL4), time- and mission-critical functions as well as non-critical train functions High performance Deterministic Ethernet

Drive-by-Data in Detail

- NG-TCN Architecture – Topology & Redundancy
- Clock Synchronization (802.1AS-rev & IEEE1588v2)
- Data Transmission & Flow control with TSN (802.1Qbv)
- IMP / FDF Integration
- Safe Data Transmission (SDTv4)
- Safe Train Inauguration
- Safety Certification

NG-TCN Network Architecture (1)



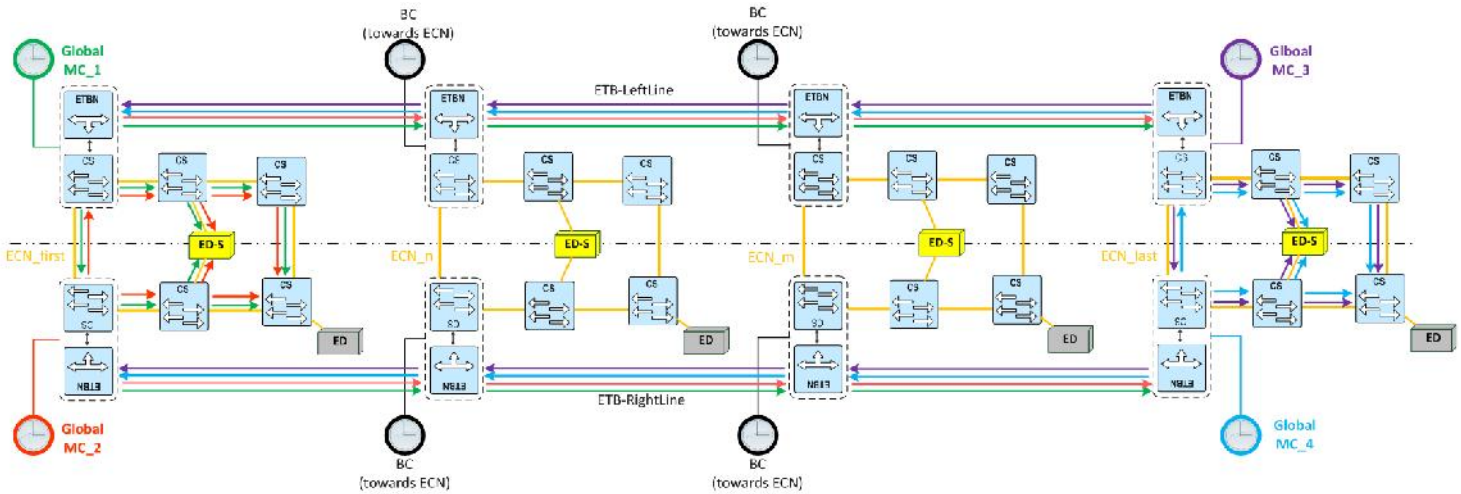
- 2 virtual data planes for reliable scheduled traffic
- Separated GbE ETB Lines along the train (difference to IEC 61375-2-5 !)
- Physical ring topology inside Consist (ECN)

NG-TCN Network Architecture (2)

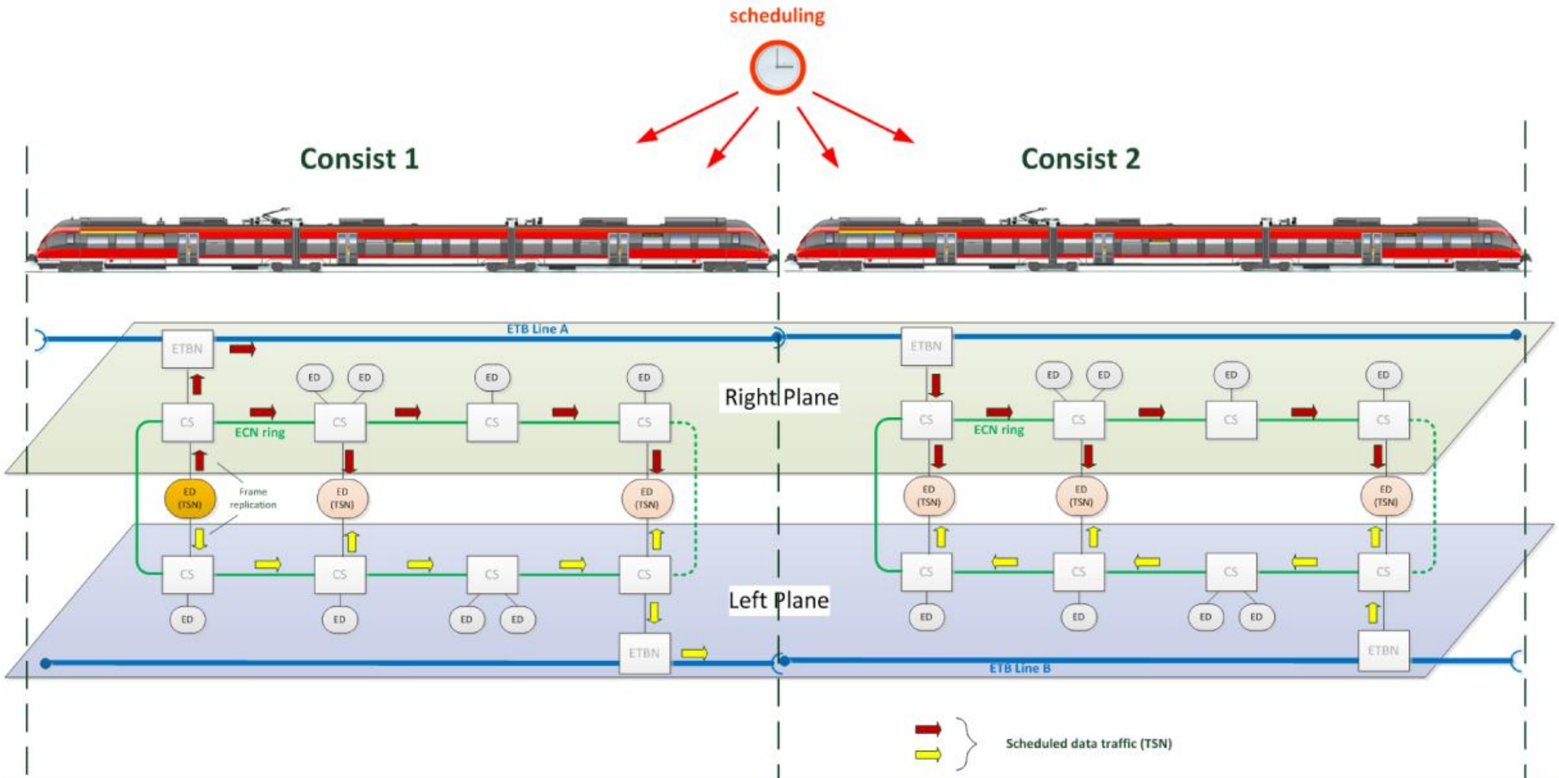
Key benefits	Restrictions
Support of TSN (Time Sensitive Networking)	No communication continuation over powerless consists
Seamless redundancy of time critical data traffic	
Elimination of train lines	
High reliability (independency of transmission channels)	
Compliance to existing ECN architecture	
Intrinsic consist orientation detection (safety)	
No bypass function	
Fire protection support (EN 50553 type 2 fires)	

Precise Clock Synchronization

- IEEE802.1AS-rev based train-wide clock synchronization
- 4 redundant grand master clocks in train

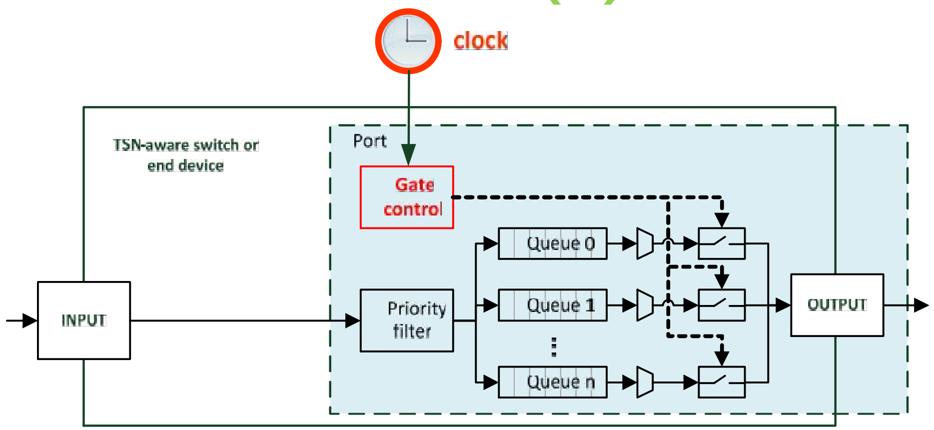


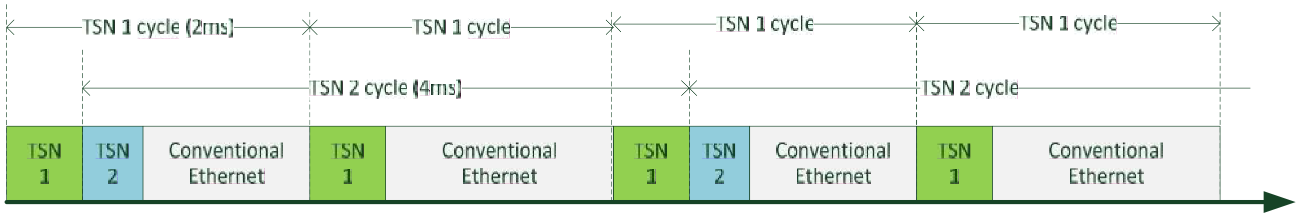
Scheduled Data Transmission (1)



Scheduled Data Transmission (2)

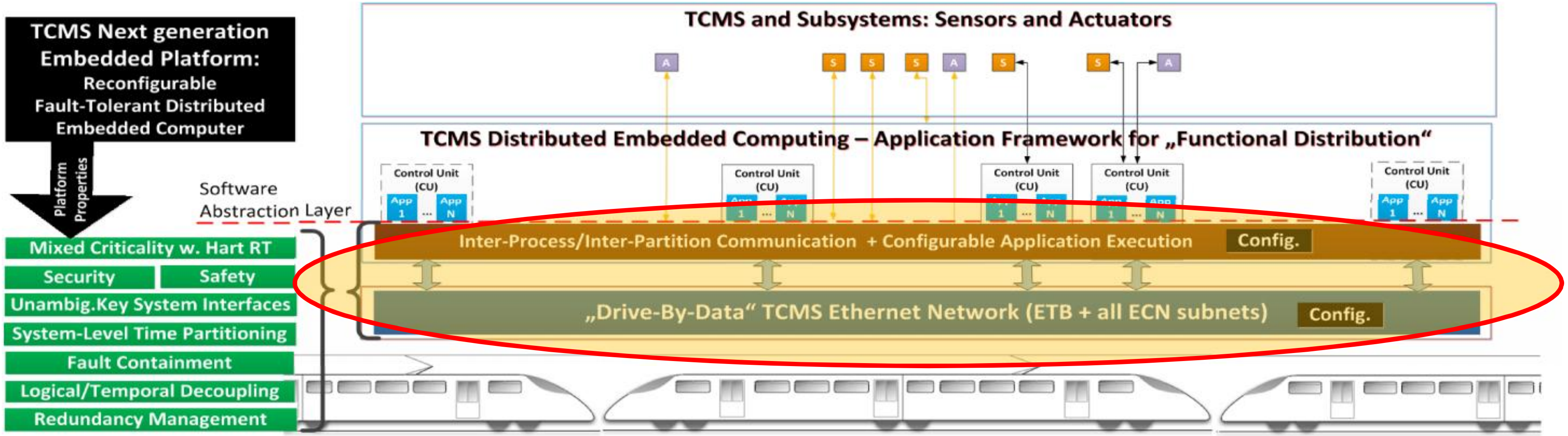
Traffic scheduled in each component



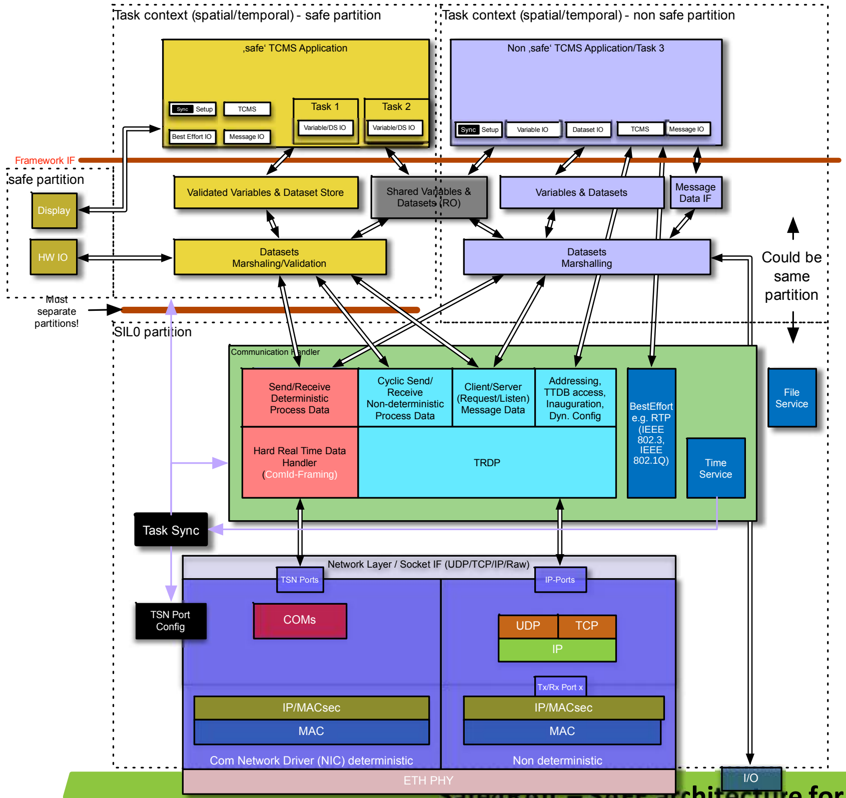


IMP = Integrated Modular Platform

- System Integration Part / Network Communication for „Reconfigurable and Scalable Fault Tolerant Distributed Embedded Computer“
- Viable only with SW platform and network integration as a „standalone“ NG TCMS IMP



IMP / FDF / DbD Integration



FDF

Applications with function distribution

Middleware with data distribution support

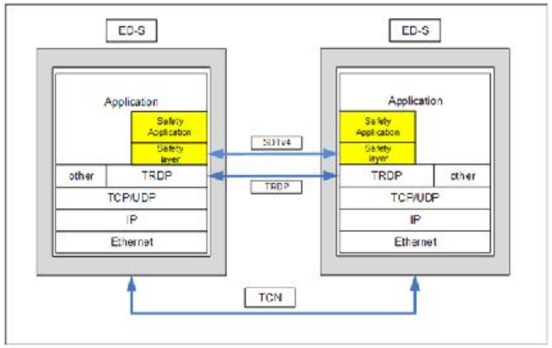
DbD

Upper communication layers & network services

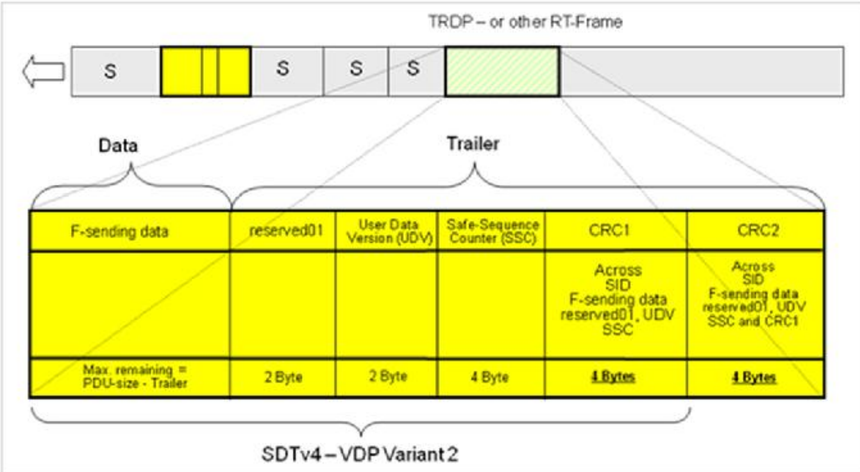
Lower communication layers (OSI 1..4) for conventional and scheduled data traffic

Safe Data Transmission (SDTv4)

- Trainwide safe data communication
- Enhancement of standardized SDTv2 protocol for supporting functions up to SIL4



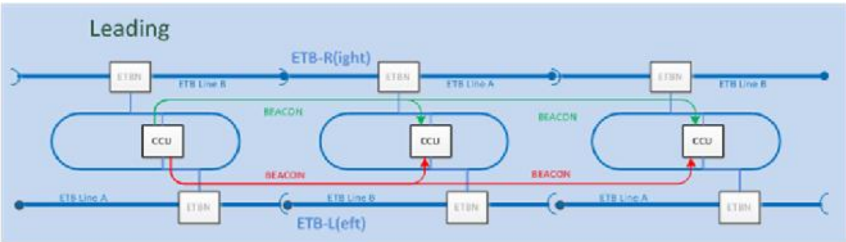
SDTv4 in OSI Model



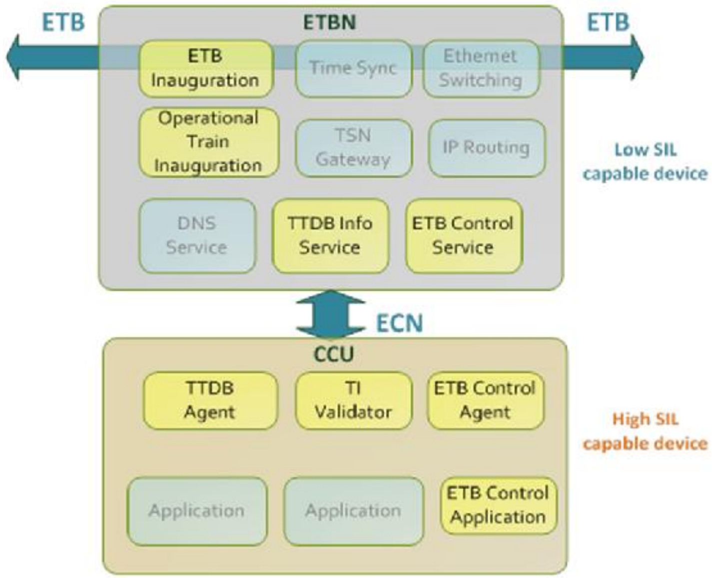
Safe Train Inauguration

Safe discovery of

- Train directions (driving direction)
- Vehicle sequence
- Vehicle orientation
- Train end



ETB lines as „virtual“ train lines

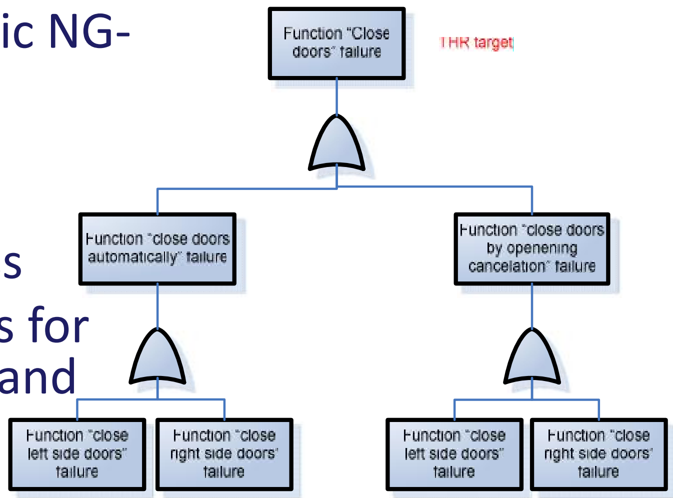


Cooperation of ETBN and CCU

Safety Certification

Study about improved safety approval concept

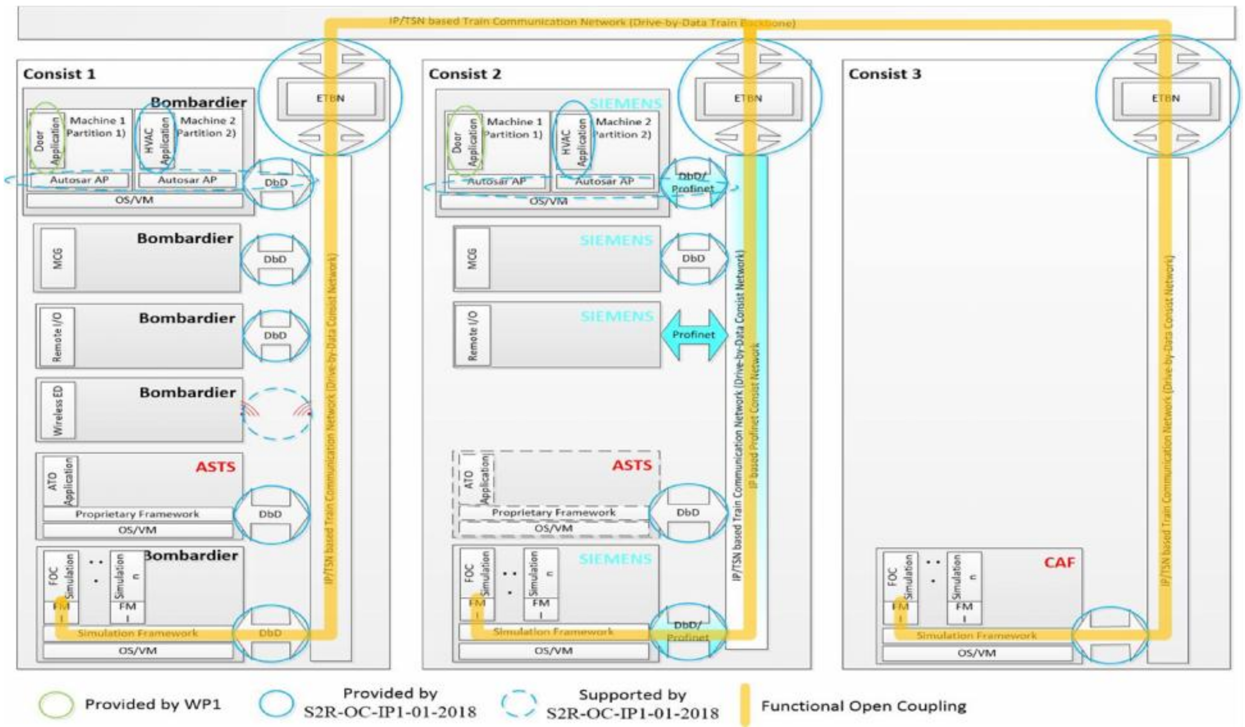
- generic safety concept for a drive-by-data centric NG-TCMS
- incremental certification through functional separation
- considerations for a generic certification process
- exemplary demonstration of safety case process for two selected train functions, the door function and the brake function



Next station is… (1/2)

- Integrate and test DbD:
  - Definition of test cases and lab setup to test the DbD architecture
  - Development of DbD components
  - DbD in urban demonstrator
  - DbD in regional demonstrator
- Investigate wireless communication:
  - Wireless train backbone (WLTB, using LTE release 14 and 5G technologies)
  - Wireless TCMS (WLCN, using WLAN technologies)
- Launch standardization (IEC WG43, CLC WG15)

Next station is… (2/2)



Example:

Regional demonstrator

Conclusions (1)

The main achievements of this work are:

- Introduction of a new **traffic class for scheduled data traffic** based on standard IEEE 802.1Qbv.
- **Clock synchronization concept** based on IEEE 802.1AS-rev and IEEE1588v2 as prerequisite for scheduled traffic.
- Definition of a new network architecture with separated ETB lines and diverse **virtual data communication planes** for scheduled data traffic.

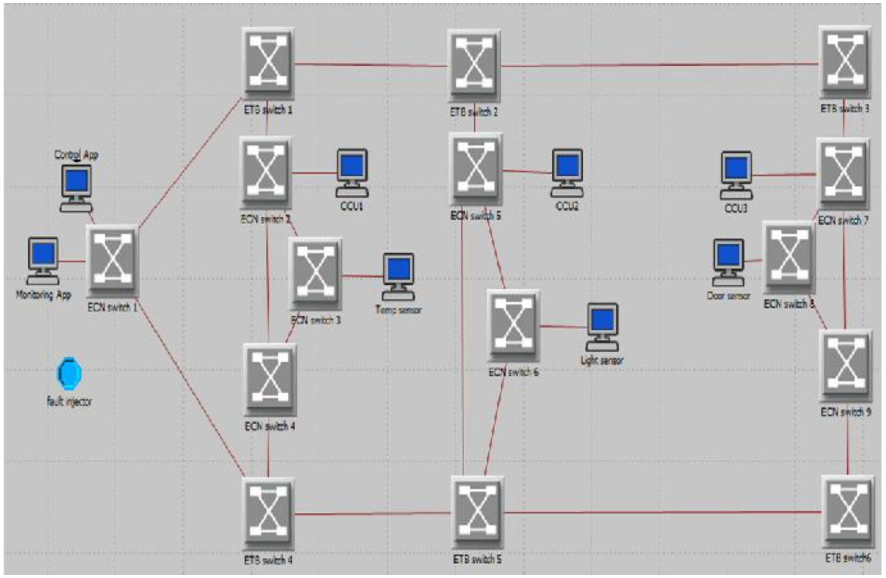
Conclusions (2)

- Supporting **functional distribution framework** and embedding into **integrated modular platform**
- **Safe Data Transmission protocol** and safety layer definition for the transport of safety critical data up to highest safety integrity levels (SIL4).
- **Safe train inauguration concept** for train composition discovery with highest safety integrity levels (SIL4).
- Definition of a **security architecture** and security methods to achieve state-of-the-art cyber security in alignment with actual security standards.

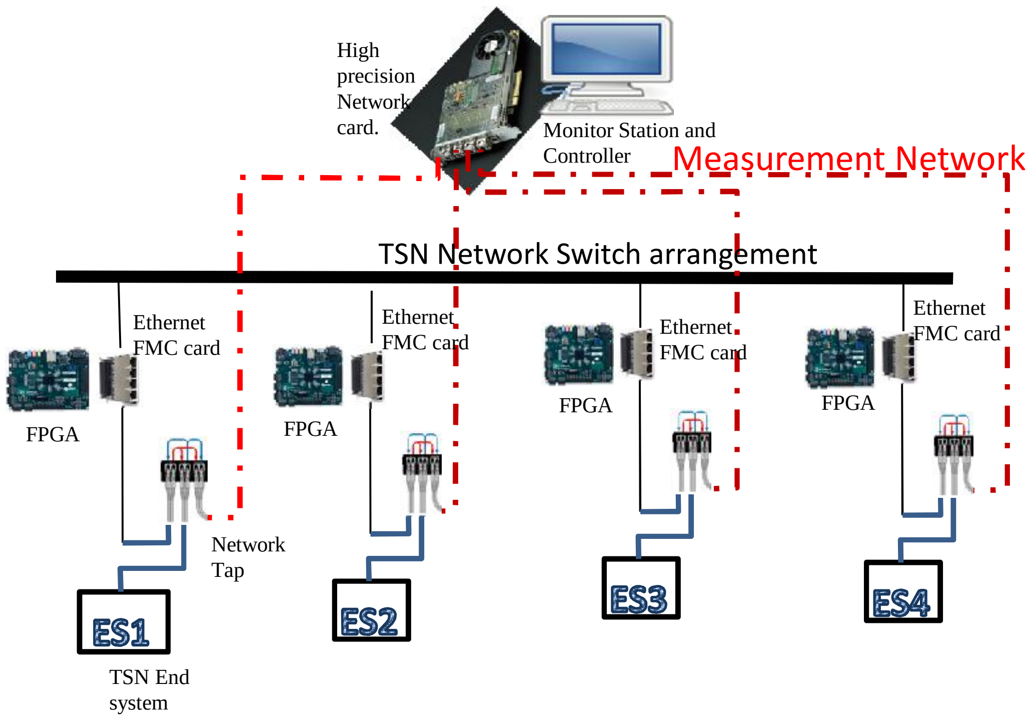
Demo of DbD & Network Simulation Short Introduction

DbD Simulation Framework

- Evaluate and validate the applicability of TSN solutions for DbD concepts
  - The V/V processes of train components compliant to TSN protocols are expensive and timely
  - The simulation tools are time and cost efficient alternative for analyzing the temporal and non-temporal attributes of TSN-capable components
- DbD simulation components
  - Configuration Manager
    - Heuristic TT scheduler
    - Network Generator
  - TSN-capable Switches and End-system
    - Time-Aware Shaper (IEEE 802.1Qbv)
    - Ingress Time-based Filtering (IEEE 802.1Qci)
    - Frame Replication and Elimination for Reliability (IEEE 802.1CB)



Fault Injection Framework



QUESTIONS & ANSWERS

COFFEE BREAK

20 minutes, punctuality is expected from the railway people

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Functional Distribution Framework

Xabier Artaetxebarria, CAF

Iñigo Odriozola, Ikerlan

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

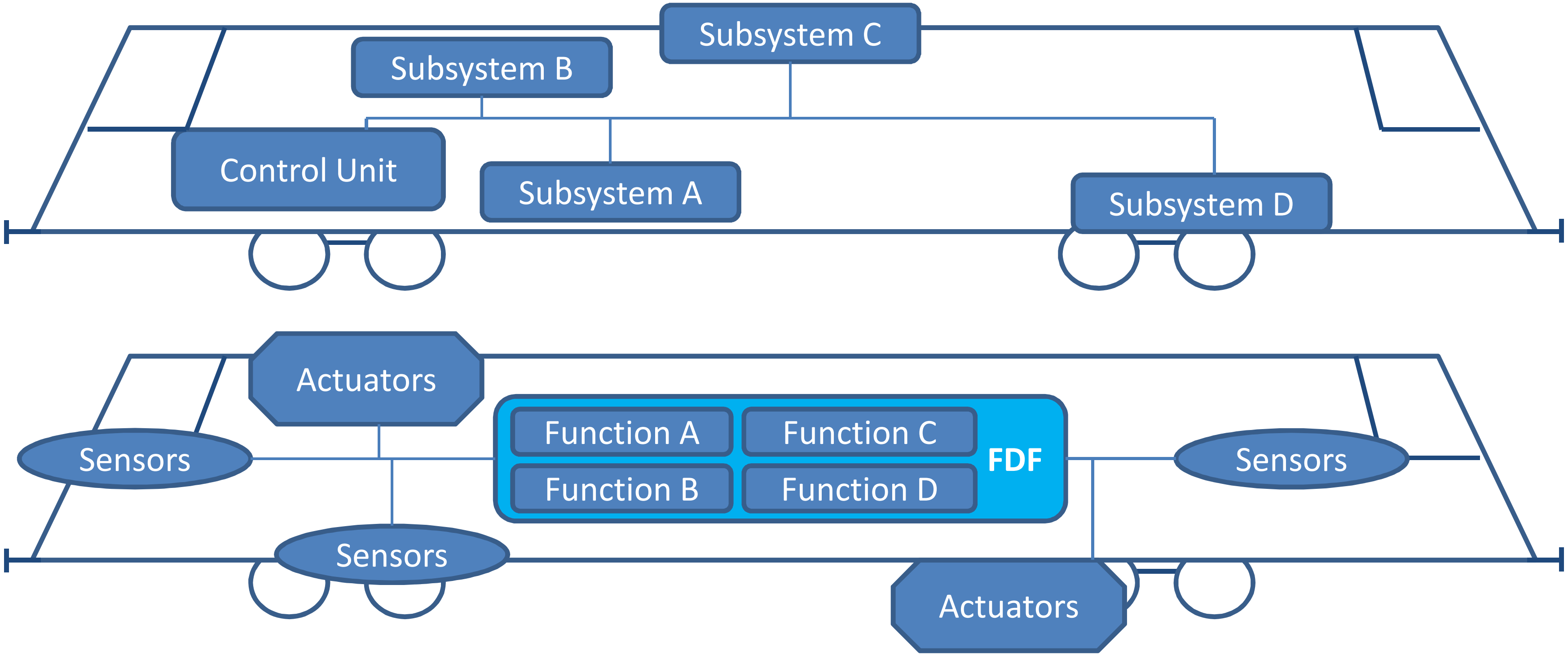
Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

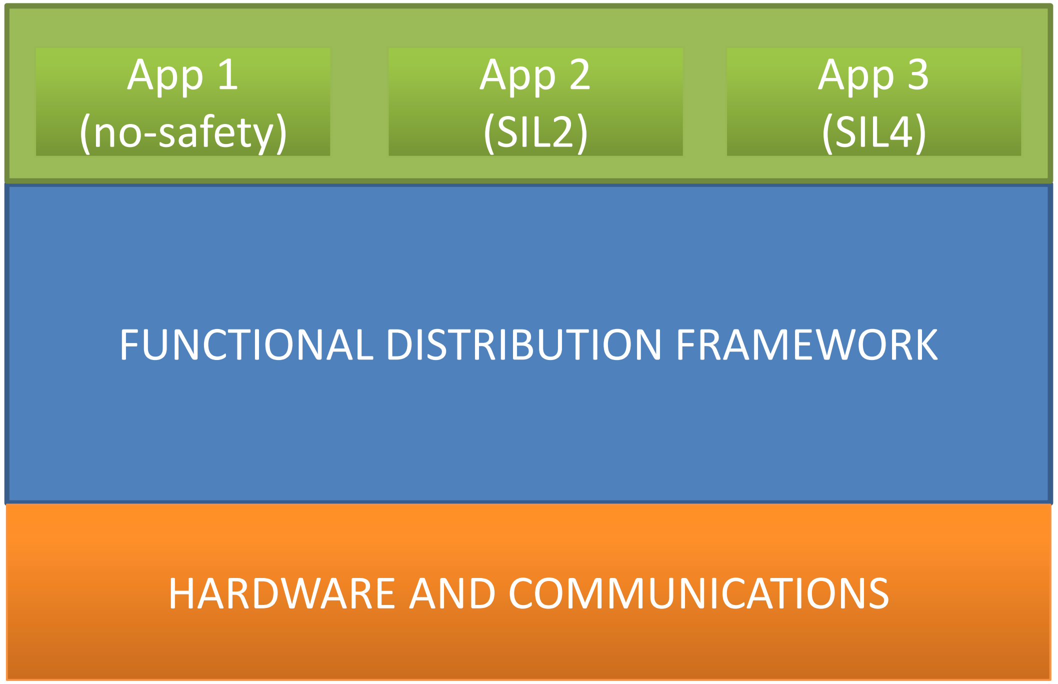
What is the FDF?

- A middleware to run software applications on top of it
- An abstraction layer from underlying hardware and communications
- A tool to facilitate the achievement of functional safety and application independence

What is the FDF?



What is the FDF?



Why FDF?

Today	With FDF
Device-based TCMS architecture	Function-based TCMS architecture
Heterogeneous software and hardware on board	Unified software and hardware on board
Multiple heterogeneous computing units	Few homogeneous computing units
Costly re-certification and re-commissioning after functions changes	Simplified re-certification and re-commissioning process
Complex obsolescence management	Simplified obsolescence management

FDF in detail

- Solutions in other domains
  - Automotive: AUTOSAR
  - Aviation: ARINC653
- Proposed solution for the railway domain
  - Safety
  - Security
  - Use example
  - Safe4RAIL implementations

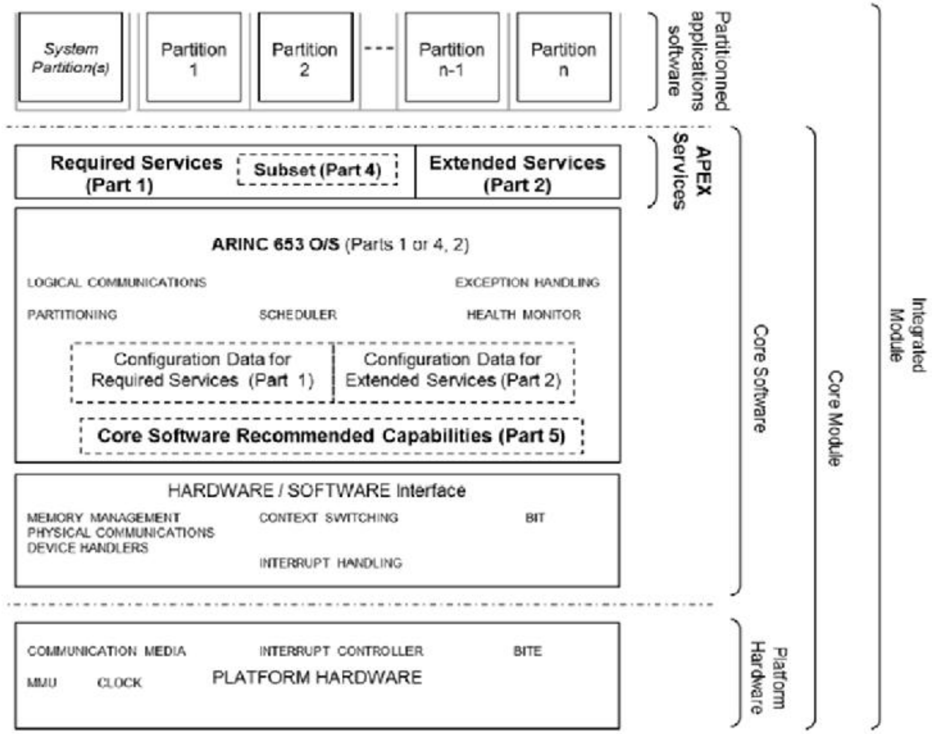
Solutions in other domains

AUTOSAR

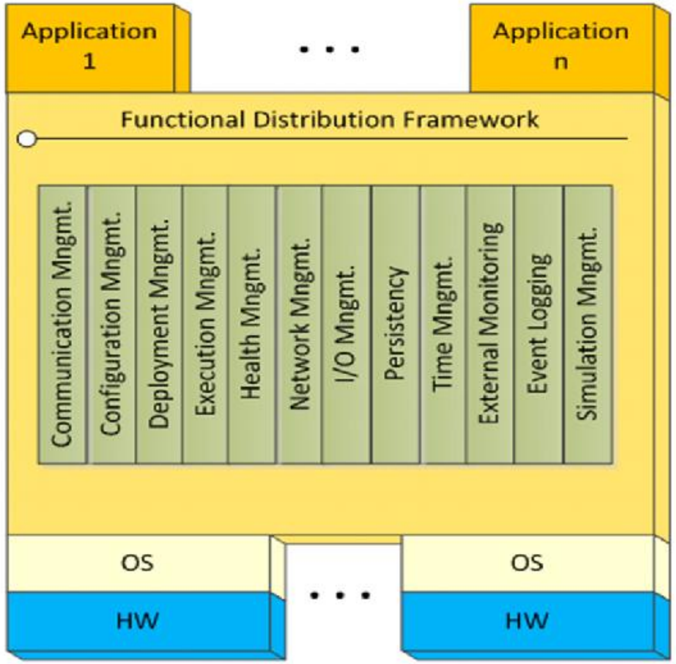
Enabling continuous innovations

Solutions in other domains

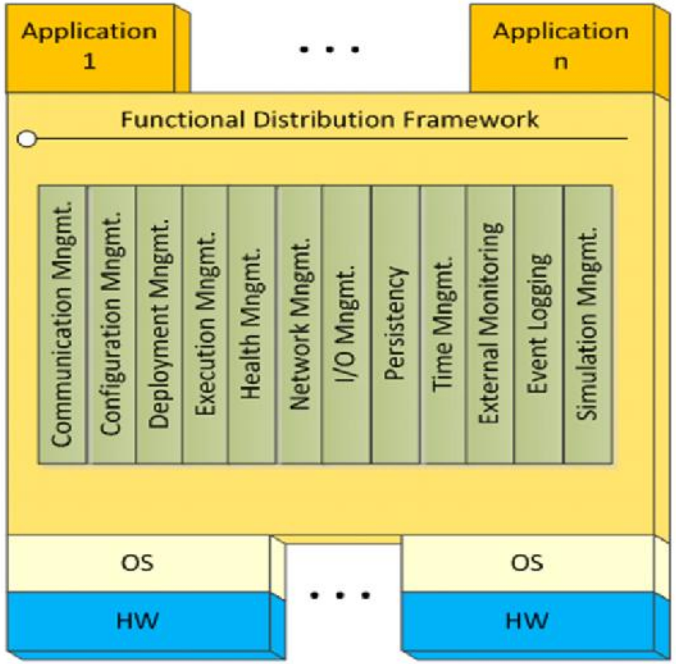
ARINC 653



Proposed solution



Proposed solution



Deployment Management

Brief description

Component that provides the ability to install and update application executables on the functional distribution framework partitions.

Requirement specification

REQ Id	Name/Text	Safety-related
CTA-D4.4-DM-1	**Install executable on a partition (direct connection)** The FDF component "Deployment Management" shall provide the maintenance staff with the ability to install an executable on a partition via direct connection to the device. Documentation: Rationale: Derived from: Requirement CTA-D4.1-128 CTA-D4.1-128 Satisfied by: Block Deployment Management	yes
CTA-D4.4-DM-2	**Install executable on a partition (network connection)** The FDF component "Deployment Management" shall provide the maintenance staff with the ability to install an executable on a partition via train network. Documentation: Rationale: Derived from: Requirement CTA-D4.1-128 CTA-D4.1-128 Satisfied by: Block Deployment Management	yes

Safety

FDF Safety concept is defined by the set of safety measures coming from the **FDF Hazard Analysis.**

The FDF HA has been carried out in order to:

- **identify any deviation**
- **assess the effects of hazardous deviations**
- **specify the measures**

Safety measures include:

- **Countermeasures** - to be implemented by the FDF
- **Application conditions** - to be exported to users and/or external technical systems
- **Recommendations** - indications for the implementation of countermeasures

Safety

Countermeasures are classified according to the Technical Safety Report (EN 50129) sections:

- **Assurance of functional operation**
- **Detection of faults**
- **Action following detection**
- **Independence of items**
- **Systematic and Random faults**

RESULT

Countermeasures – FDF Requirements & FDF Requirements – FDF Components Traceability

Security

- **Risk analysis** for services provided by FDF by defining assets to be protected and threats.
- **Risk assessment** based on ISA/IEC 62443-3-3 "System security requirements and security levels".

Target Security Level: SL3

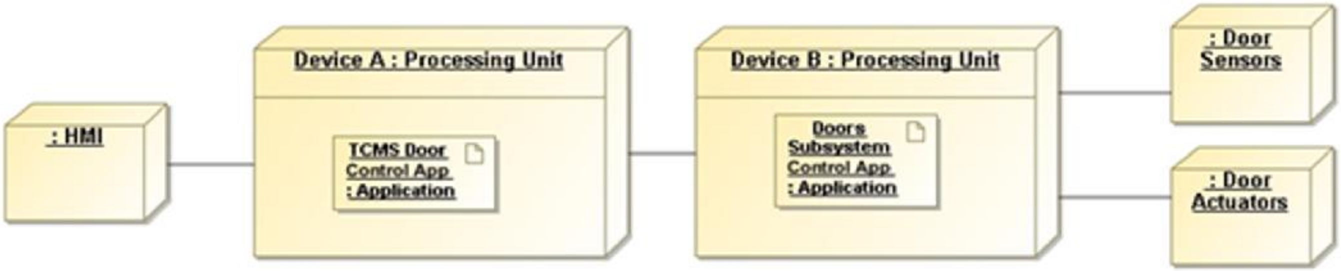
Cybersecurity: Security Objective	Cybersecurity: Attack	Attack Potential (worst case): Elapsed Time	Expertise	Information about the target	Access to Target	Equipment	Damage Potential (worst case): Personal Damage	Operative Damage	Financial Damage	Cybersecurity Risk Estimation: Attack Potential		Damage Potential		Risk Value
SO.1 Authorized use of FDF	Session hijacking	Months	Multiple Experts	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rare	43	Catastrophic	1020	Undesirable
	FDF manipulation	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Unusable	< 1.000.000 euros	Beyond High-Rare	46	Catastrophic	1200	Undesirable
	Authorization/Privileges modification	Months	Expert	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rare	41	Catastrophic	1020	Undesirable
	Password hack	Months	Proficient	Restricted	Moderate	Standard	Severe and life-threatening injuries (survival possible	Comfort affected	< 100.000 euros	High	20	Catastrophic	1011	Undesirable
	Power failure	Hours	Layman	Public	Difficult	Standard	No effect	Maintenance required	< 10.000 euros	Enhanced-Basic	11	Medium	10	Undesirable
	Hard drive failure	Hours	Expert	Public	Difficult	Standard	No effect	Unusable	< 10.000 euros	Moderate	17	Critical	100	Undesirable
	User supplantation	Weeks	Proficient	Restricted	Moderate	Standard	No effect	Comfort affected	< 100.000 euros	Moderate	14	Medium	11	Undesirable
SO.2 Restricted access to ECU instructions:	CPU manipulation	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Unusable	< 1.000.000 euros	Beyond High-Rare	46	Catastrophic	1200	Undesirable
	Data injection/deletion	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Unusable	< 100.000 euros	Beyond High-Rare	46	Catastrophic	1110	Undesirable
SO.3 Application isolation	Data corruption	Months	Proficient	Restricted	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rare	35	Catastrophic	1020	Undesirable
	Network flooding	Years	Expert	Sensitive	Moderate	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rare	46	Catastrophic	1020	Undesirable
SO.4 Data authentication and encryption	Breach of cryptography	Years	Multiple Experts	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rare	53	Catastrophic	1020	Undesirable
	Collect sensitive information (keys, logs)	Months	Expert	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rare	41	Catastrophic	1020	Undesirable
SO. 5 Trusted message exchange	Message injection	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Comfort affected	< 100.000 euros	Beyond High-Rare	46	Catastrophic	1011	Undesirable
	Man-in-the-Middle	Months	Multiple Experts	Sensitive	Moderate	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Comfort affected	< 10.000 euros	Beyond High-Rare	38	Catastrophic	1001	Undesirable
SO.6 Trusted input/output devices	Peripheral device supplantation	Months	Multiple Experts	Public	Difficult	Bespoke	Severe and life-threatening injuries (survival possible	Maintenance required	< 10.000 euros	Beyond High-Rare	35	Catastrophic	1010	Undesirable
	Port tampering	Hours	Expert	Public	Difficult	Bespoke	No effect	Maintenance required	< 10.000 euros	High	24	Medium	10	Tolerable
	Ethernet tampering	Hours	Expert	Public	Difficult	Bespoke	No effect	Maintenance required	< 10.000 euros	High	24	Medium	10	Tolerable
	Repudiation	Hours	Expert	Public	Difficult	Bespoke	No effect	Maintenance required	< 10.000 euros	High	24	Medium	10	Tolerable

Counter-measures

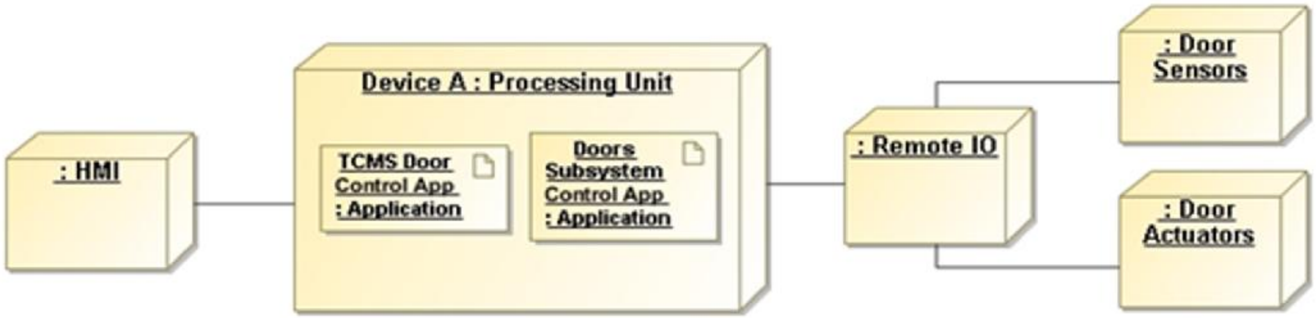
RESULT

- *62443-3-3 Requirements – **Countermeasures – FDF Requirements** - FDF software components – Security Objectives* traceability

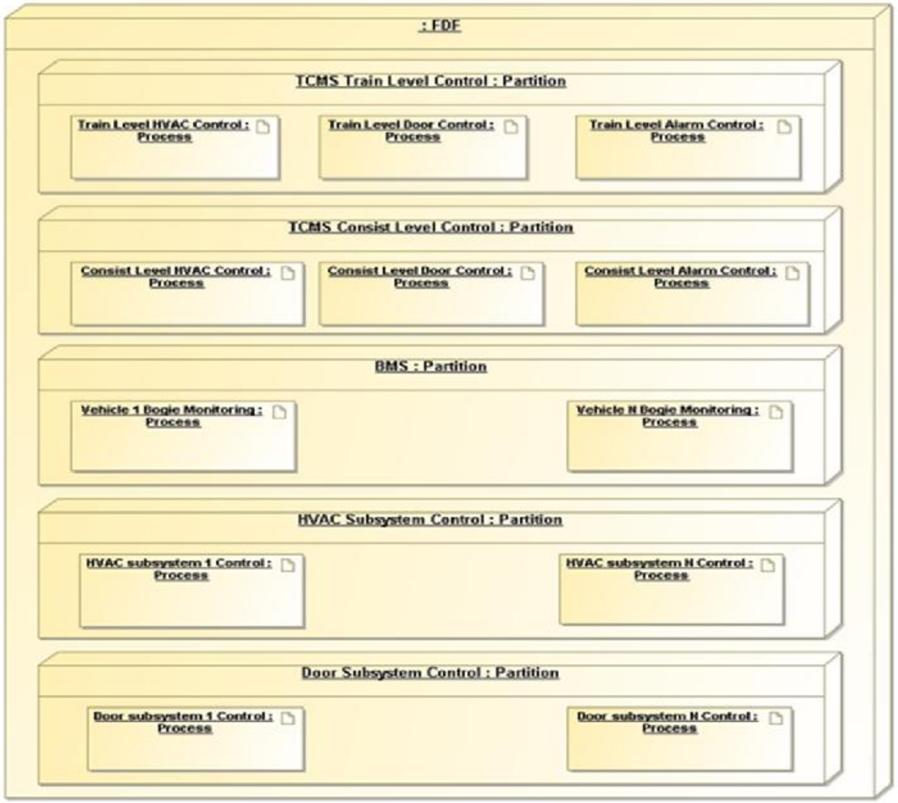
Use example: Door control without FDF



Use example: Door control with FDF



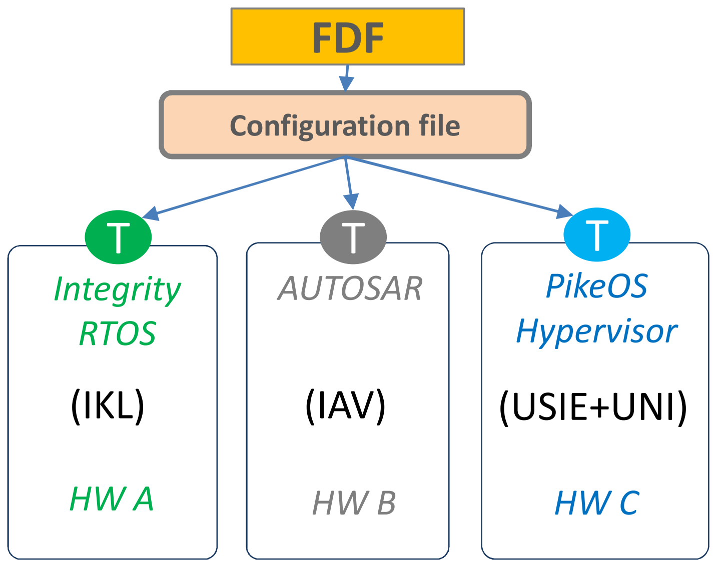
Use example



: FDF
TCMS Train Level Control : Partition
Train Level HVAC Control : Process
Train Level Door Control : Process
Train Level Alarm Control : Process
TCMS Consist Level Control : Partition
Consist Level HVAC Control : Process
Consist Level Door Control : Process
Consist Level Alarm Control : Process
BMS : Partition
Vehicle 1 Bogie Monitoring : Process
Vehicle N Bogie Monitoring : Process
HVAC Subsystem Control : Partition
HVAC subsystem 1 Control : Process
HVAC subsystem N Control : Process
Door Subsystem Control : Partition
Door subsystem 1 Control : Process
Door subsystem N Control : Process

Safe4RAIL implementations

- 3 Proof-of-concept demonstrators of FDF
- Bogie Monitoring System application
  - Read temperature sensors
  - Activate warm or hot alarm



Next station is

- CONNECTA-2 & OC
  - Higher TRL implementations of FDF
  - Development of applications on top of FDF
  - Maintenance of detailed specification and addition of interfaces (if required)
  - Handling technical issues not addressed by Safe4RAIL FDF implementations

Conclusions

- The FDF aims to have isolated but integrated applications instead of dedicated equipment (HW, SW, I/Os) for each train function

- **Benefits**:
  - Reduce the number and complexity of devices
  - Reduce re-/certification complexity
  - Interoperability, reconfiguration, deterministic inter-partition communication
  - Hardware and communication abstraction

QUESTIONS & ANSWERS

Integrated FDF and DbD Demo
Converged Communication and Computation

Arjan Geven, TTTech Computertechnik AG

Iñigo Odriozola, Ikerlan

Maryam Pahlevan, University Siegen

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

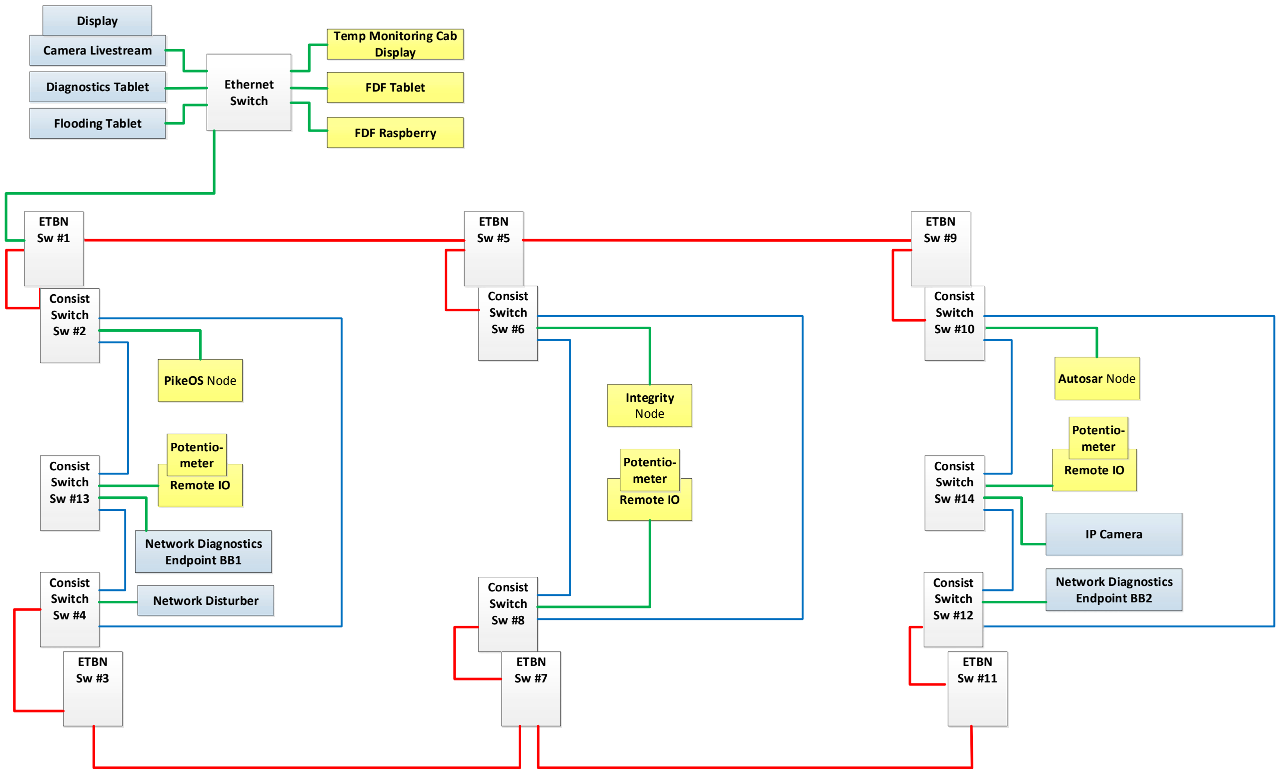
Demonstrator Overview

- Converged Communication (DbD)
  - Deterministic Communication
  - Full Network Isolation
  - Robust Topology
- Converged Computation (FDF)
  - Deterministic Computation
  - Full Partition Isolation
  - Spatial Separation
  - Access control for shared memory
  - Monitoring and error-prevention

Demonstrator Contents

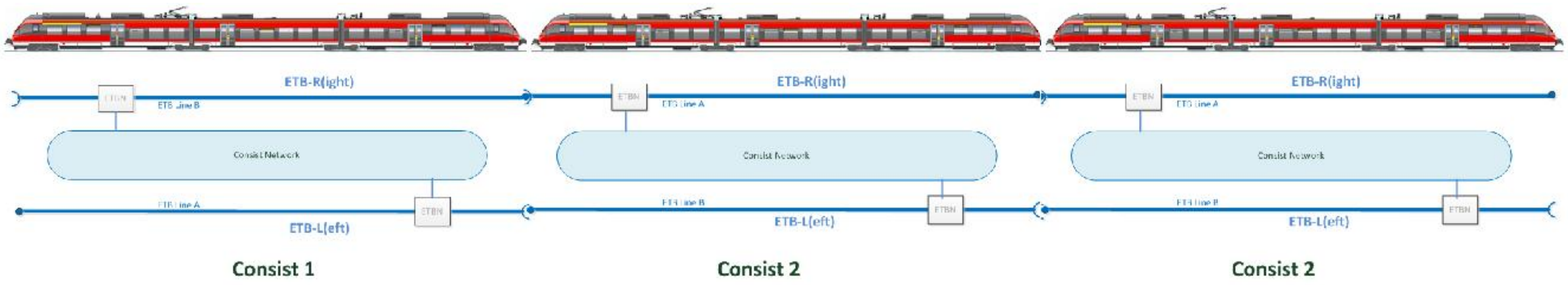
- Network
  - Three consist networks + Backbone network
  - IP Camera
  - Network Diagnostics Application
  - Network Disturbance Control
- Computation platform
  - Three instantiations
  - Bogie Monitoring (BMS) Display
  - BMS Diagnostics and Control Terminal

Demonstrator Layout



Robust Redundancy

- Use two separated Ethernet lines along the train: ETB-L(eft) and ETB-R(ight).
- ECN ring topology
- Three consists connected

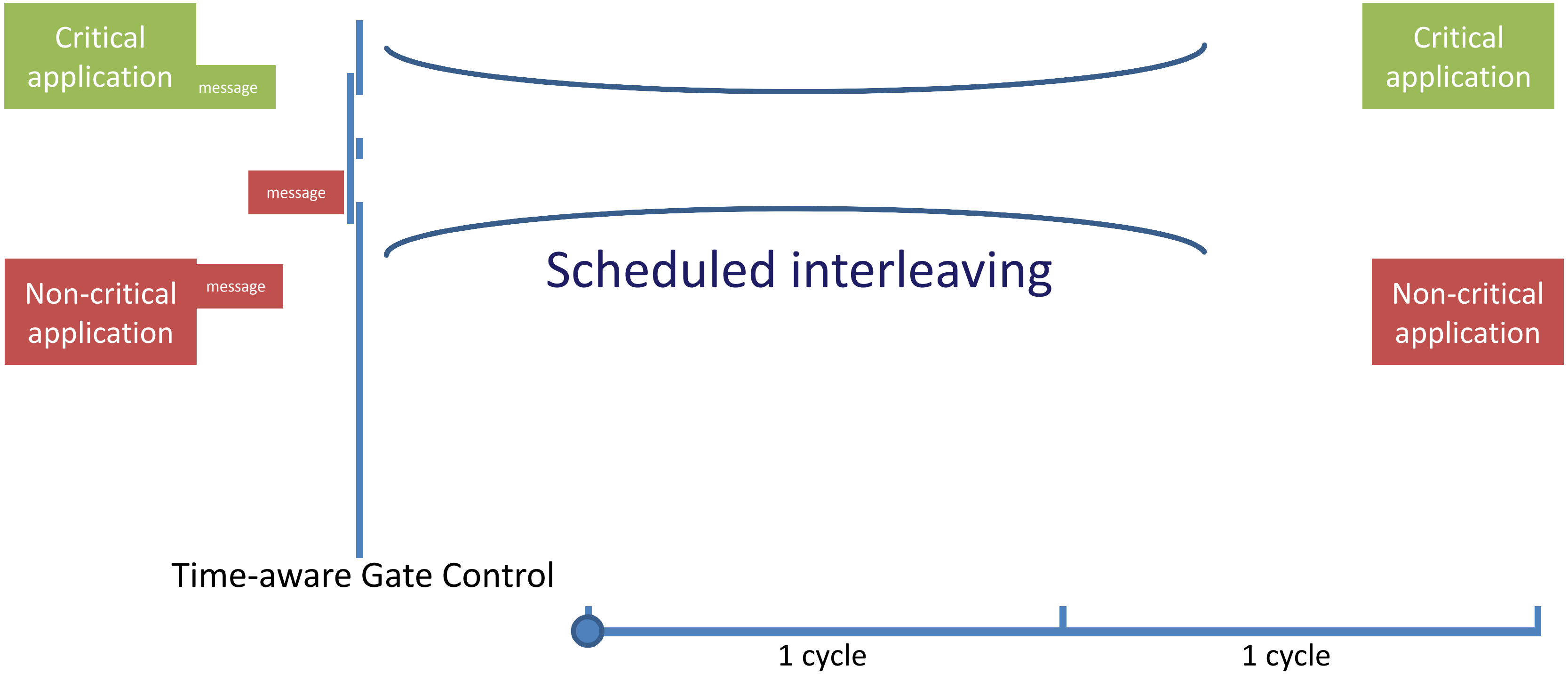


Converged Communication

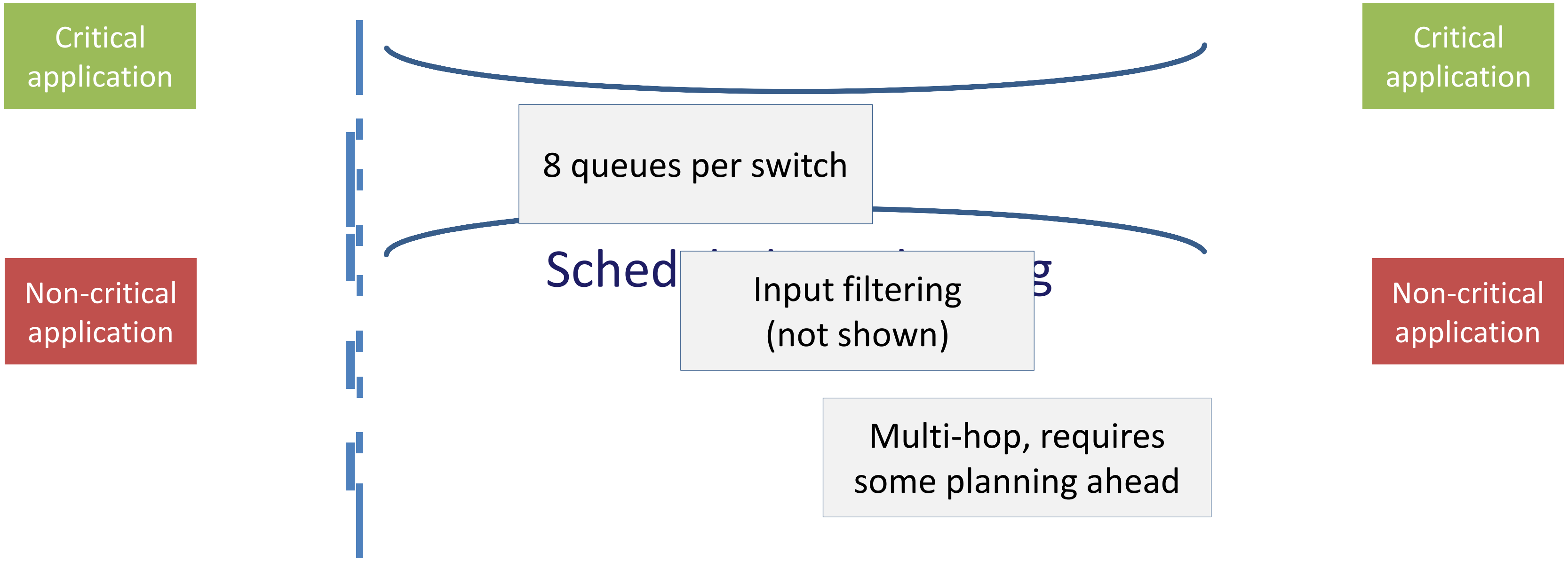
Deterministic Communication

- Synchronized clocks
  - according to 802.1AS-rev
- Scheduled Communication
  - Priority queue gates are open and closed according to 802.1Qbv

Gate Schedule



Gate Schedule

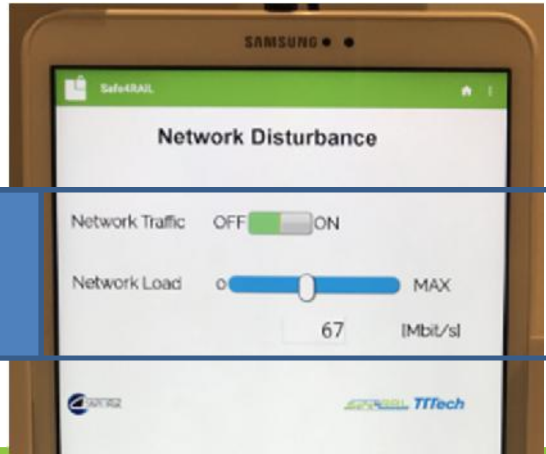


Converged Communication

Full Network Isolation

- Full network virtualization
- Safety and non-safety streams side-by-side
- Misbehaving nodes or wrongly configured nodes can do no harm
- Incoming traffic controlled through 802.1Qci ingress policing
- Not affected by high traffic load

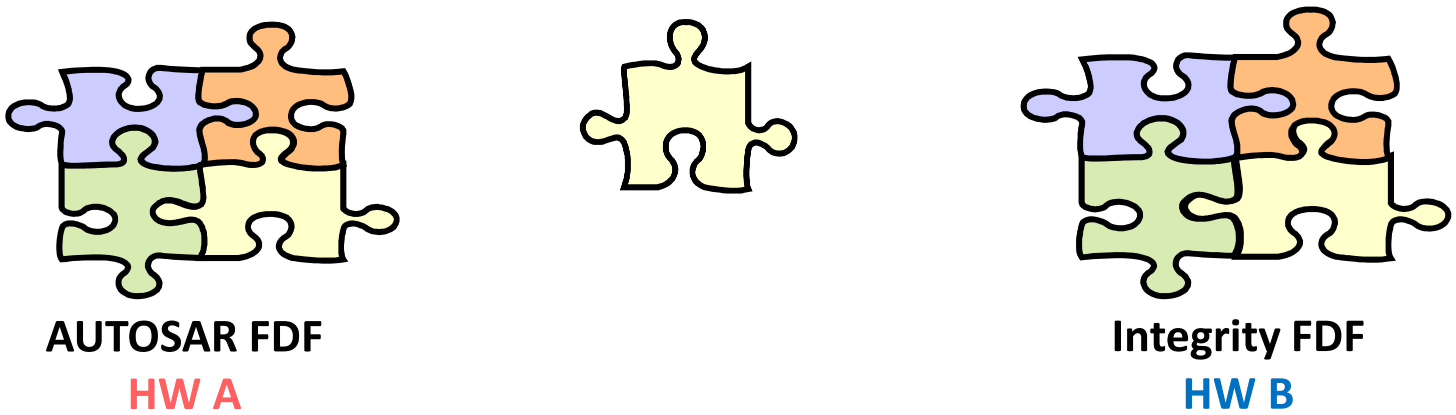
Simulate misbehaving application



Live view

- Follow the camera!

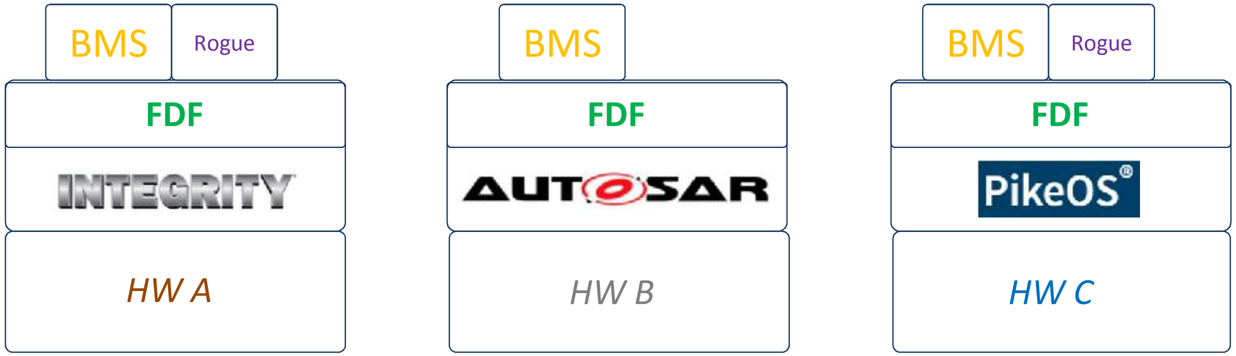
Modular integration concept



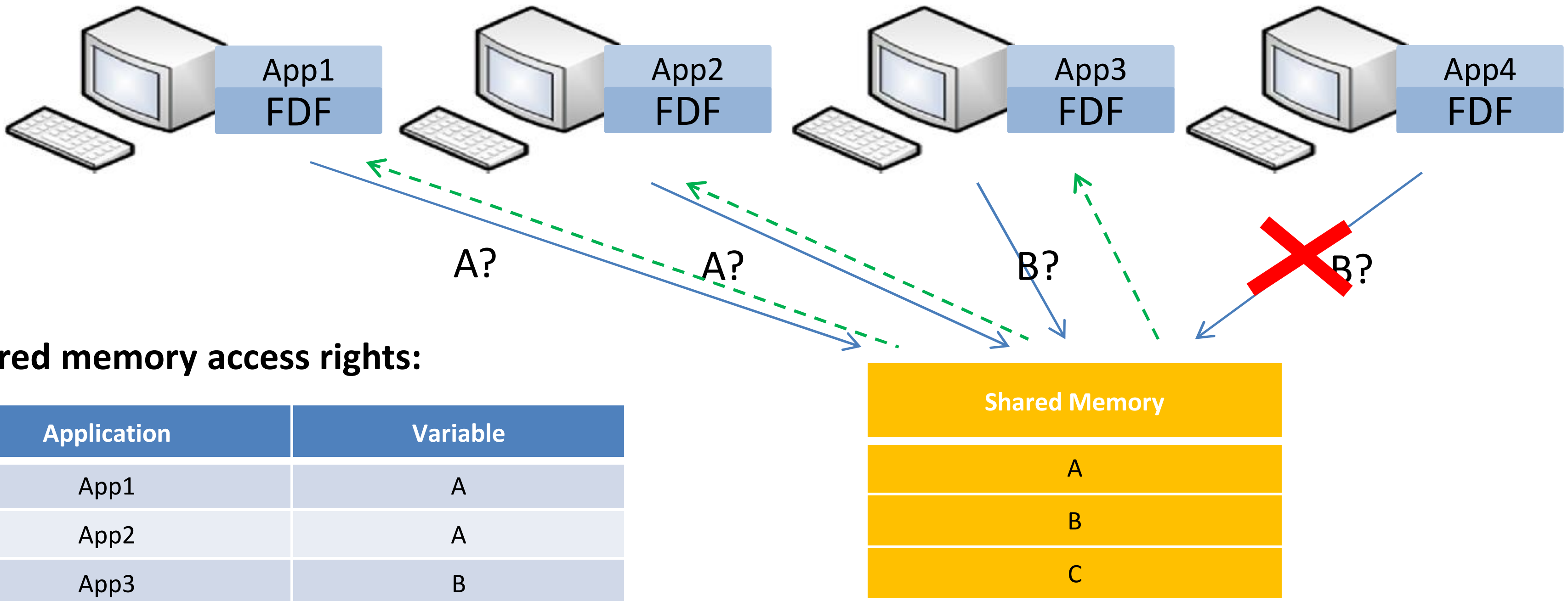
Safety-critical and non-critical application side-by-side on the same platform =>

- Non-interference guaranteed
- HW and communication abstraction

Interoperability



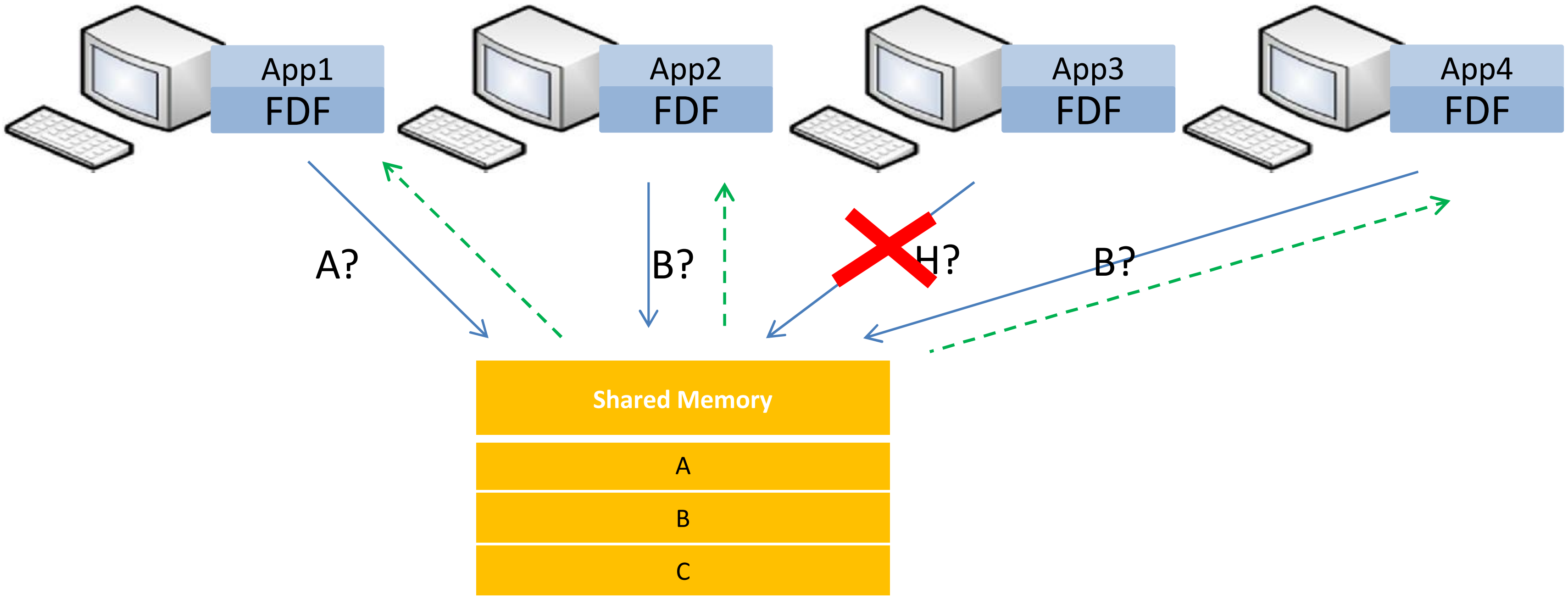
Spatial separation



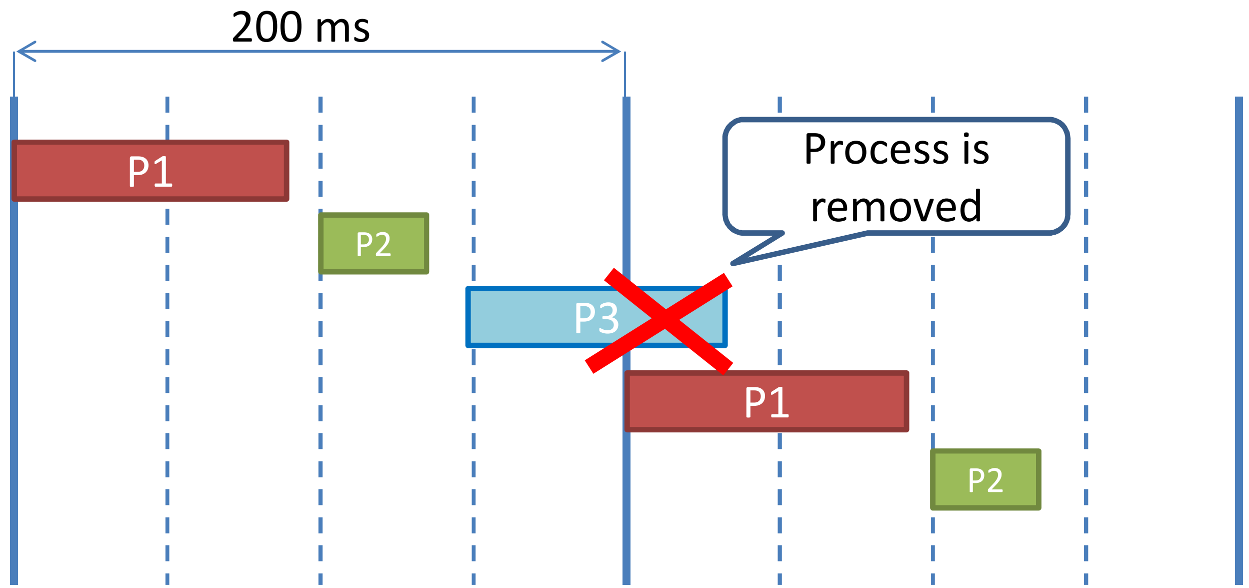
Shared memory access rights:

Application	Variable
App1	A
App2	A
App3	B

Protection & Isolation



Temporal separation



P1: SIL (Safety Integrity Level) 4

P2: SIL 2

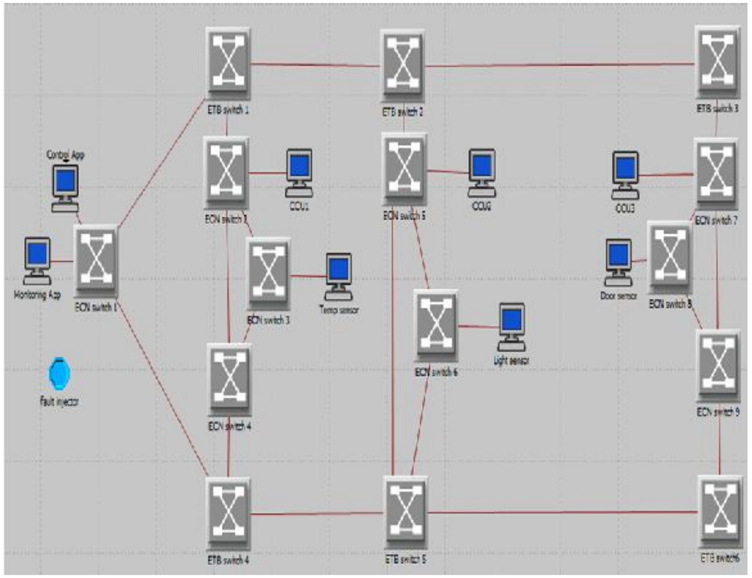
P3: SIL 0 tries to use more than the assigned slot!

Live view

- Follow the camera!

DbD Simulation Framework

- Evaluate and validate the applicability of TSN solutions for DbD concepts
  - The V/V processes of train components compliant to TSN protocols are expensive and timely
  - The simulation tools are time and cost efficient alternative for analyzing the temporal and non-temporal attributes of TSN-capable components
- DbD simulation components
  - Configuration Manager
    - Heuristic TT scheduler
    - Network Generator
  - TSN-capable Switches and End-system
    - Time-Aware Shaper (IEEE 802.1Qbv)
    - Ingress Time-based Filtering (IEEE 802.1Qci)
    - Frame Replication and Elimination for Reliability (IEEE 802.1CB)

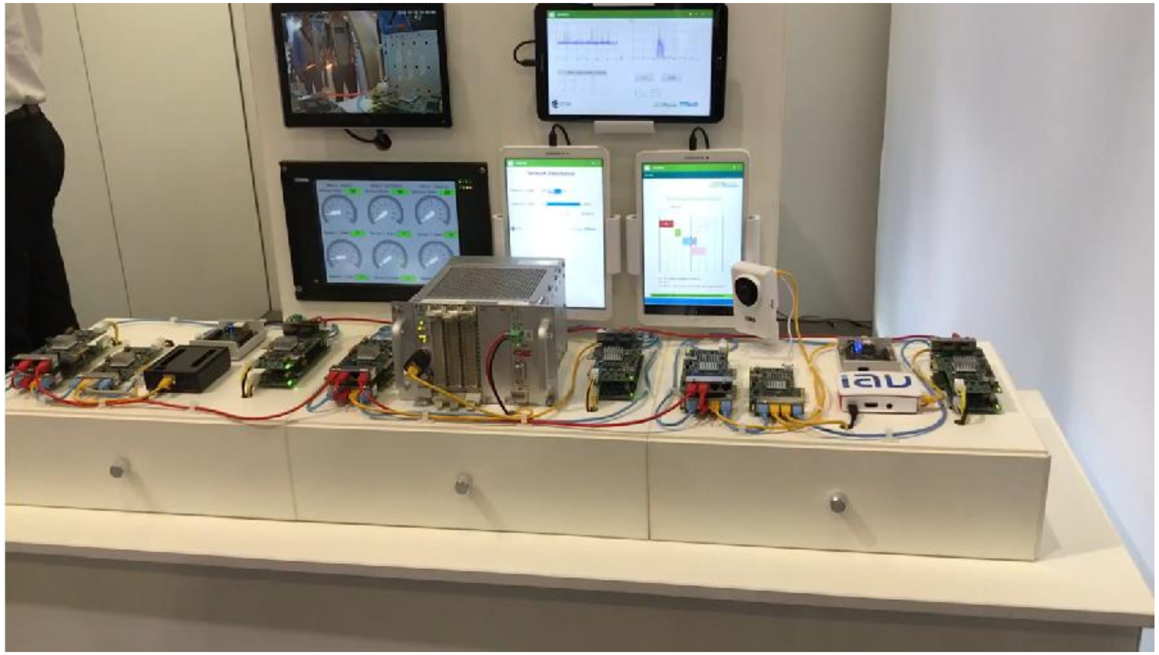


Configuring the DbD Simulator

- Set up the example TCN layout taken from the proof-of-concept implementation of the demonstrator with minor adaptations
  - Run the heuristic TT scheduler to compute the global TT transmission schedule
  - Run configuration management to generate device-specific GCLs and the network layout XML file
  - Import the network topology XML file and create the demonstrator network
  - Set up statistics parameters of end-systems and switches
  - Run the simulation and examine the simulation results
  - Set the fault injector to inject different faults into the simulation network
  - Evaluate the impact of every faults on different streams in the simulated network

On your way to lunch...

...come visit the demo!



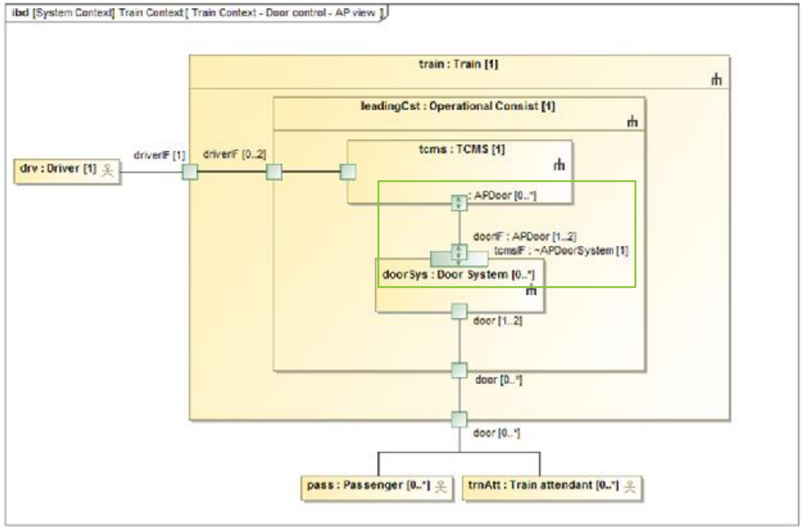
QUESTIONS & ANSWERS

Application Profiles

Dr. Thomas Waschulzik (Siemens Mobility)

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

What is an Application Profile?



Train Context - Door control - AP view

- According to our project goal an Application Profile describes a functional interface between the Train Control and Monitoring System (TCMS) and a subsystem
- The interface definition is based on an analysis of which use cases have to be supported and defines the information (flow properties) that can be exchanged between the communication partners

Why did we define the Application Profiles?

Reduce

- Engineering costs due to standardization of
  - Requirements for the subsystem (e. g. Use cases)
  - Interface between TCMS and the subsystem
  - Documentation
  - Tests
- Project duration due to less negotiations between subsystem supplier and integrator
- Problems during system introduction phase, due to less changed software and hardware components

Criteria for the Subsystem Selection for the Definition of the Application Profiles

1. Critical number of suppliers for the subsystem exists
2. Low differentiation potential due to the subsystem
    1. Prerequisite for the disclosure of internal information that is necessary to standardize the interface
    2. Expectation that the existing interfaces are not too unique and that only affordable resources are required to support the new defined standard
3. Ongoing standardization activities

Selected Application profiles

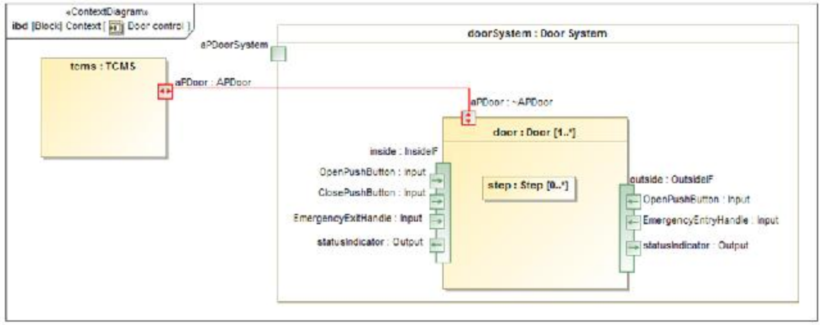
1. Application Profiles according the modeling guide line
   1. HVAC
   2. Doors
   3. BMS
2. Ongoing standardization activities inside X2Rail for ATO subset 139

Results from the State of the Art Analysis about application profile guidelines

- Several are existent in application domain
- None fulfilled the requirements
- Decision analysis “Which of the existing solutions should be used in WP4” brought heterogeneous results
- Decision to define a new guideline

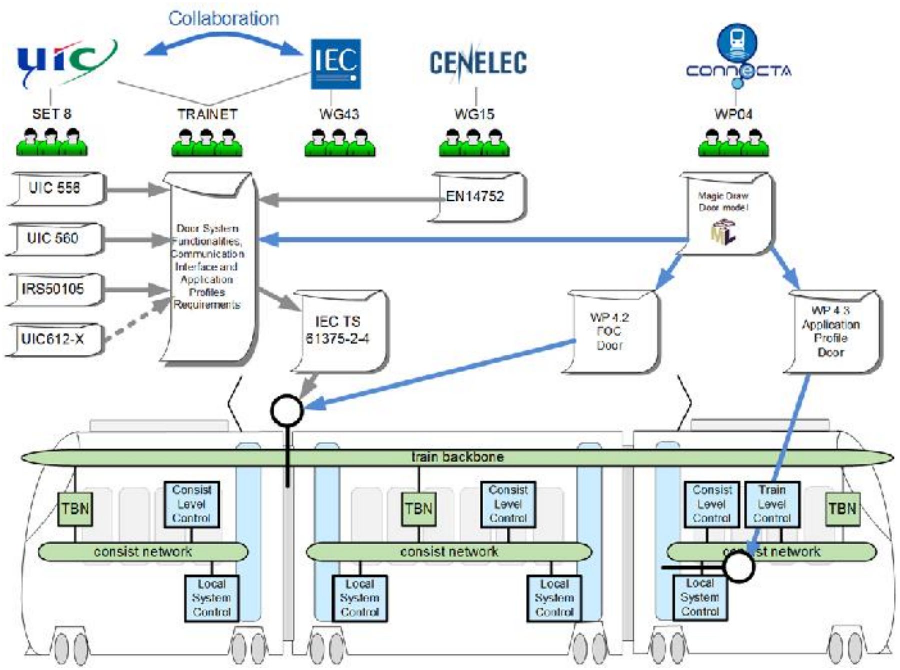
Application profiles in Detail: Basic Concept

- Use established SysML to define
  - static and dynamic architecture of TCMS and subsystem
  - use cases that have to be supported
  - interfaces between components
- Build integrated model for FOC and Application profiles
- Generate consistent reports from this model for different purposes (FOC, Application profiles, ..)



Context of the Application Profile "Door"

Cooperation between Connecta WP4 and TRAINET-Group

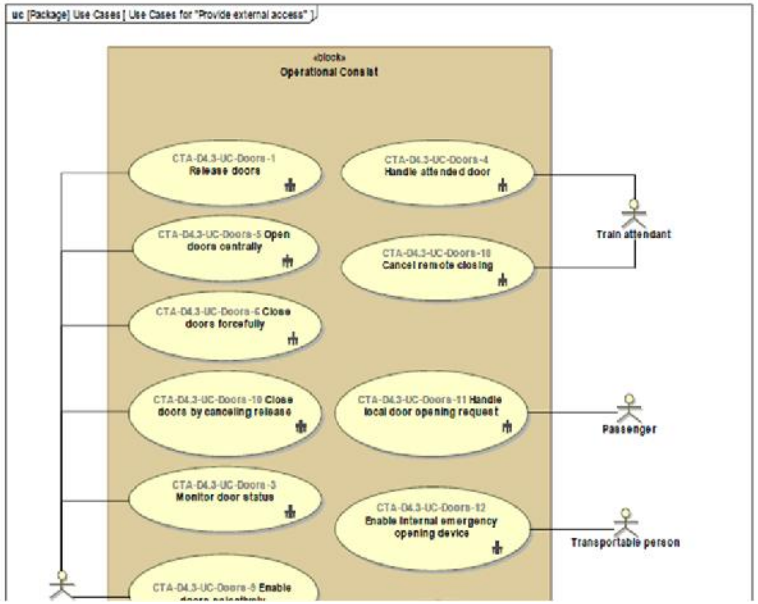


Assured consistency between

- Application Profiles
- FOC and
- TRAINET

due to export of the documents from the same SysML Model

Application Profile – Example Doors



Use cases for Application Profile Doors

	Flow property *Name : Type [Multiplicity]*	Attributes *Name : Type [Multiplicity]*
out	doorReleaseState : DoorReleaseCmd [1]	release : DoorReleaseCmdKind [1] Command to set the release state. • `none` The door should not be released. • `releaseInside` - The door should be released from the inside (the outside should not be released). • `releaseOutside` - The door should be released from the outside (the inside should not be released). • `release` - The door should be released from the inside and outside.

Example of flow properties

Next station is

- Finalize the review of the ATO subset 139 together with X2Rail
- Implement together with the complementary action an example of the BMS, Doors, and HVAC applications on the urban and the regional demonstrator using the FDF
- Update of the existing Application Profiles and definition of new ones for TCMS functions using the methodology defined in Connecta-1

Conclusions

- ✓ Adequate guideline for the definition of application profiles has been defined
- ✓ Agreement on the application profile for BMS, HVAC and Doors reached
- ✓ Ongoing review for the ATO subset 139

QUESTIONS & ANSWERS

LUNCH & NETWORKING

1 hour, punctuality is still expected from the railway people

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Functional Open Coupling

Vincent Mayeux, Alstom

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

What is the Functional Open Coupling ?

- Allows to couple heterogeneous units functionally regardless of:
  - type of consists: train can be operated with units of different type, e.g. 2 car unit coupled with a 4-car unit and 3-car unit
  - version of consists providing upward compatibility between fleet
  - manufacturer consists providing interoperability

- Through a set of functional interfaces and physical topology description

What is the Functional Open Coupling ?

Source: Youtube Railsimu https://www.youtube.com/watch?v=yQvbYcFYcGs

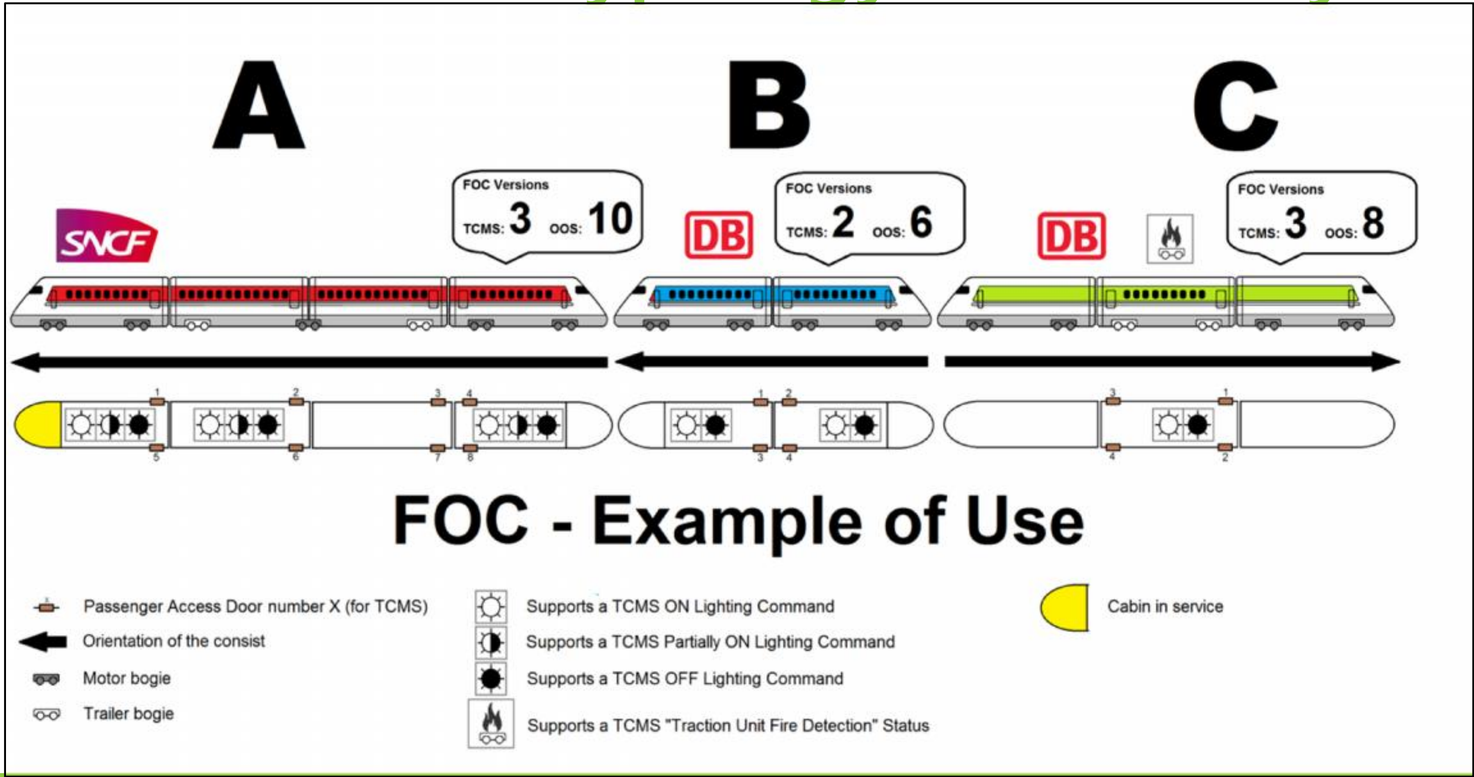
Why Functional Open Coupling ?

Today	With Functional Open Coupling
In most of the cases, a consist can only be coupled to another one it was specifically designed for	Heterogeneous consists will be able to couple.
Operators do not have sufficient flexibility in the fleet	Operator will be able to manage their fleet with greater flexibility (e.g. in case of maintenance)
Consists that have a diversity (type of traction techno, options) cannot be coupled together	Diversity and options are managed
New software version often impose to recertify the existing fleet for multiple unit operation with new fleet	New and existing fleets will be able to couple without recertification costs on the existing fleet

Functional Open Coupling in detail

- **Use cases**
- Communication concept & data exchanges
- Example
- Next steps and conclusion

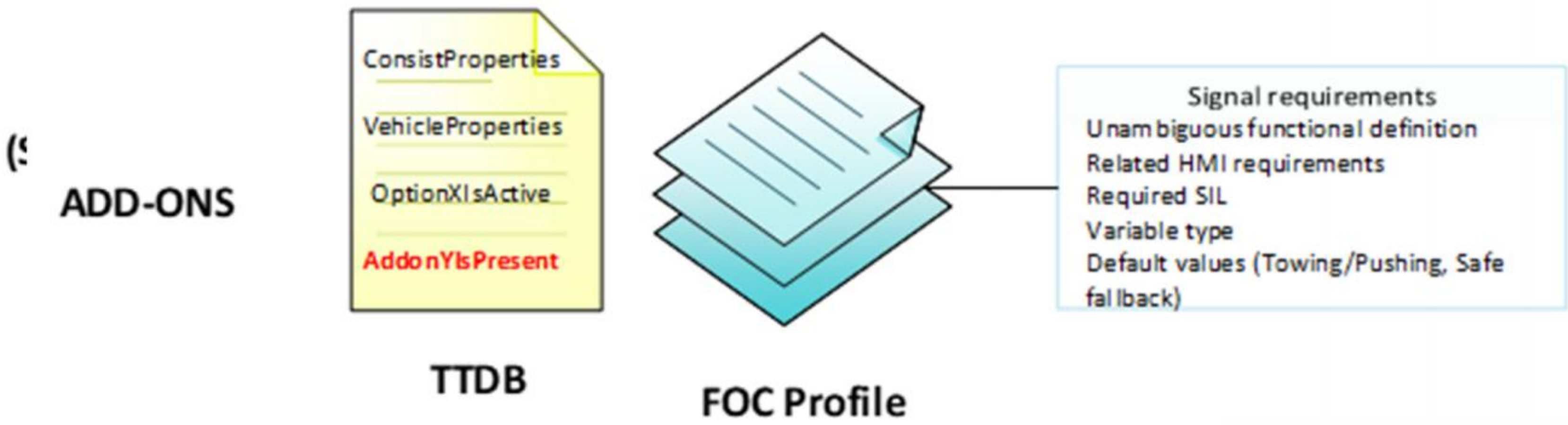
Use cases: typology of diversity



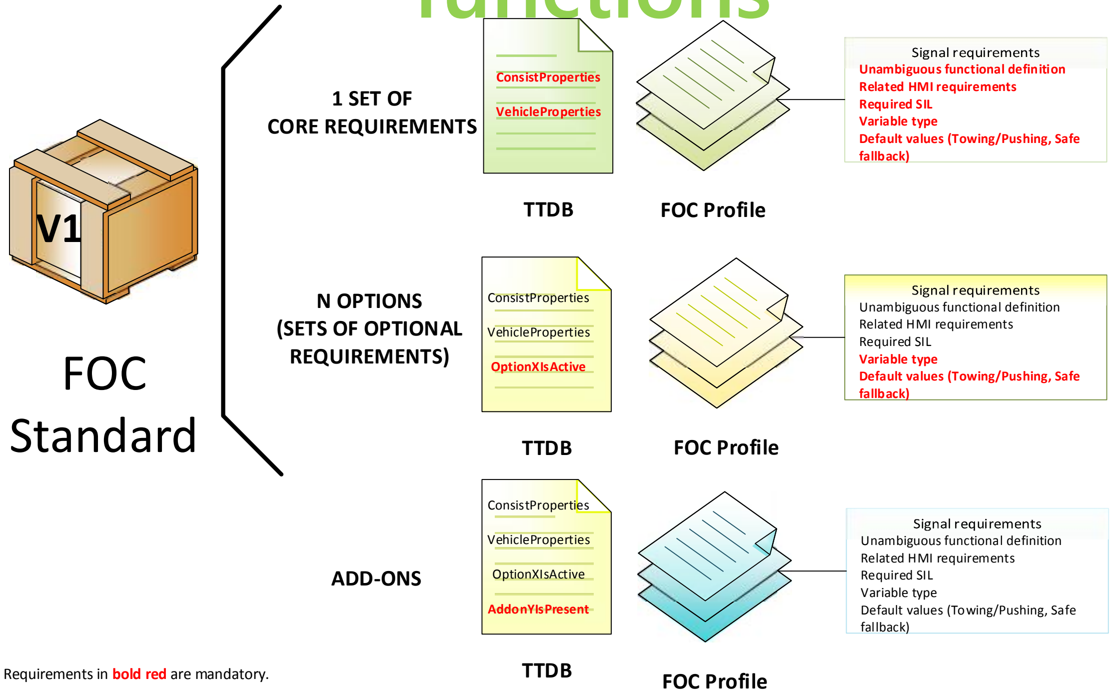
Functional Open Coupling in detail

- Use cases
- **Communication concept & data exchanges**
- Examples
- Next steps and conclusion

Definition of core and option functions

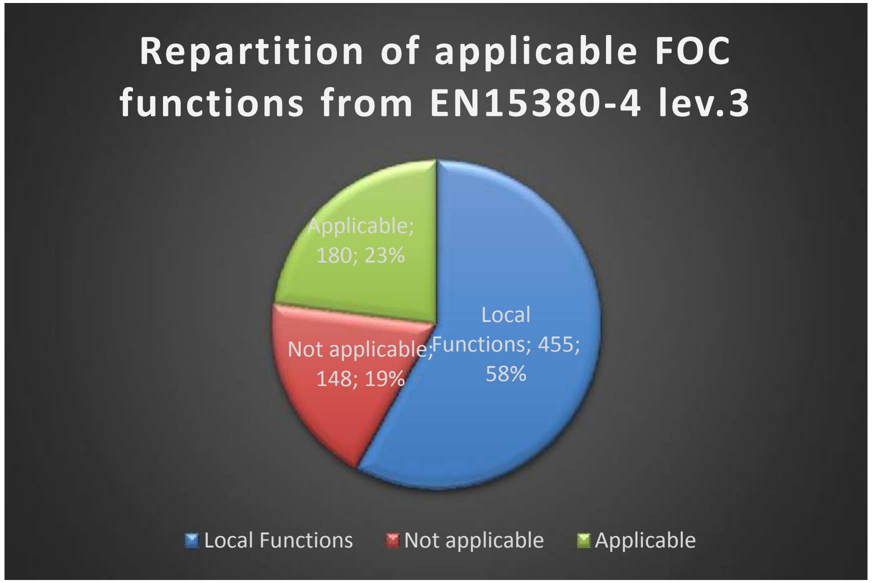


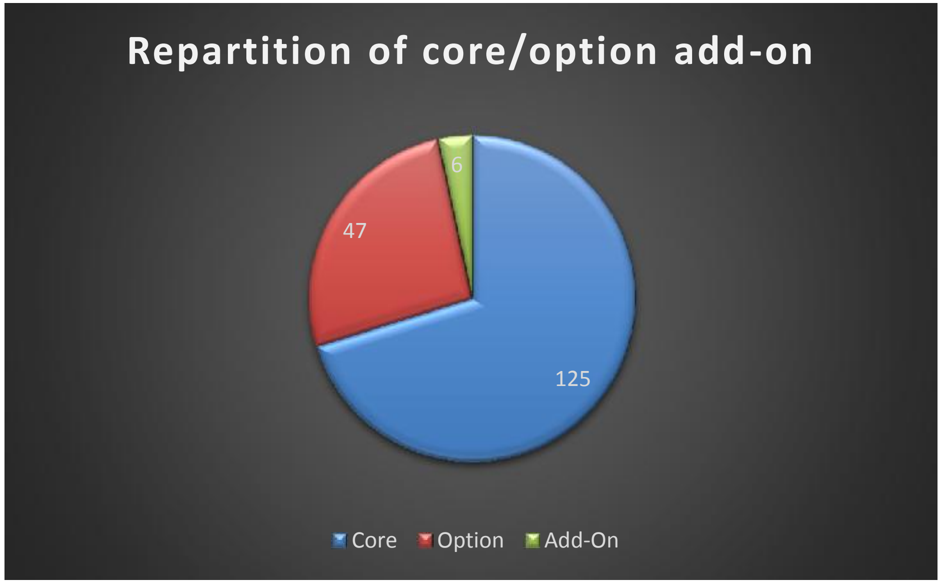
Definition of core and option functions



Requirements in **bold red** are mandatory.

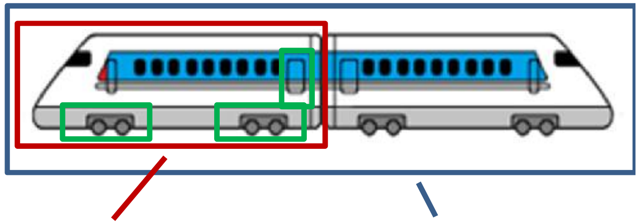
Communication concept





Definition of a FOC layer

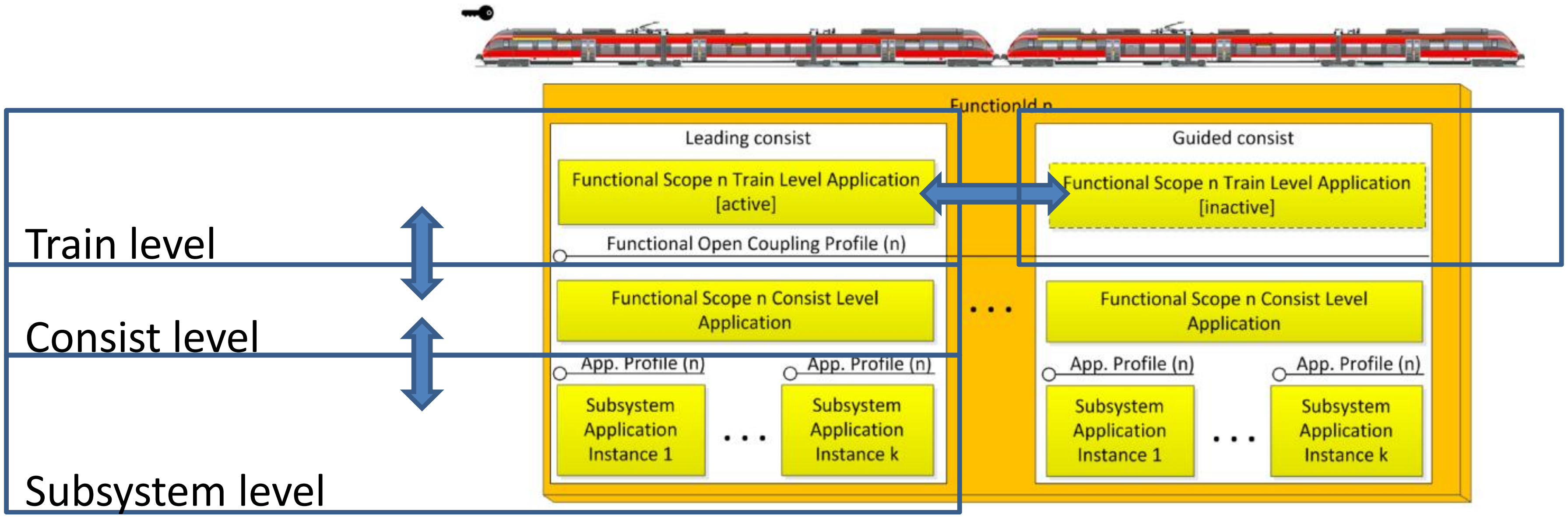
- a set of **organic information** aimed at being shared by the consists using the FOC included in the TTDB



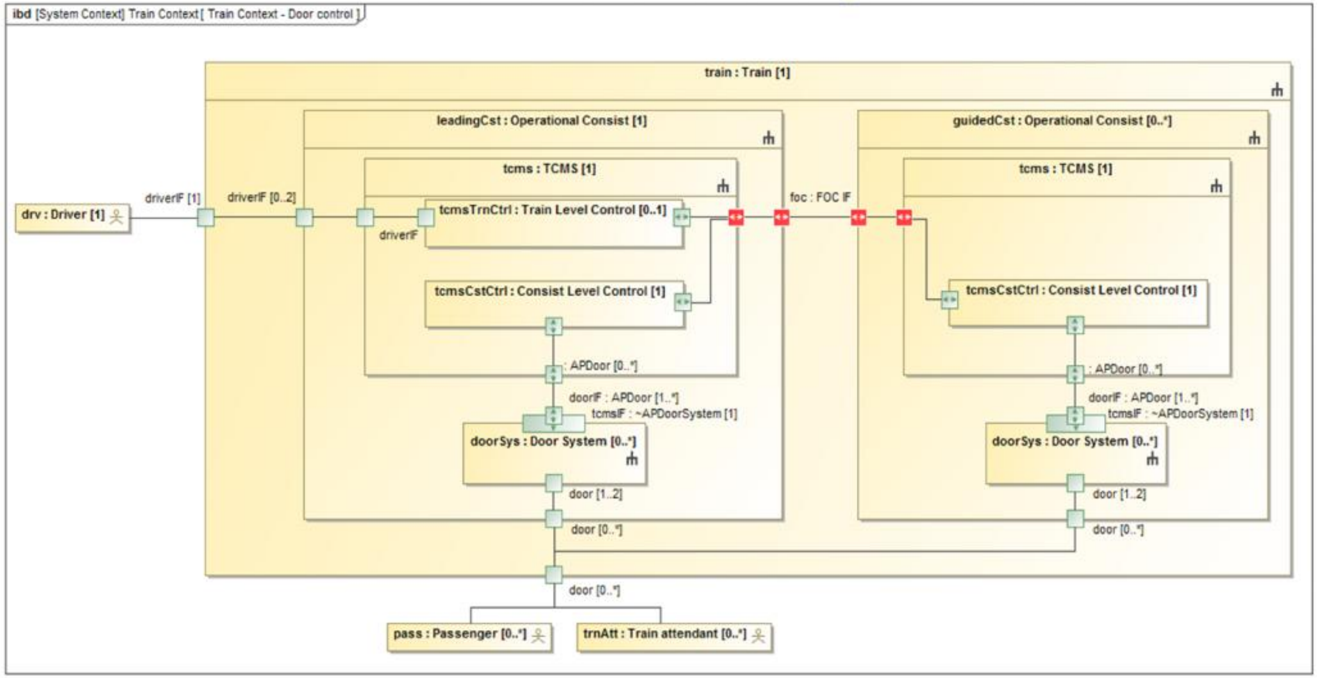
- a set of **signals** to be exchanged called "**FOC profile**" taking into consideration **Application Profile** Methodology

Flow property *Name : Type [Multiplicity]*	**Attributes** *Name : Type [Multiplicity]*	Leading	Guided	Classification
statusAllCstExtDrsClosedLockedTrnSide : StatusCstAllExtDrsClosedAndLockedTrnSide [1]	allCstDrsClosedAndLocked : TrainSideKind [1] Status which consist doors are closed and locked based on train side. All consist doors on the given train side are closed and locked. • `none` - No side of the train. • `left` - Only the left side of the train. • `right` - Only the left side of the train. • `both` - Both sides (left and right) of the train.	in	out	core

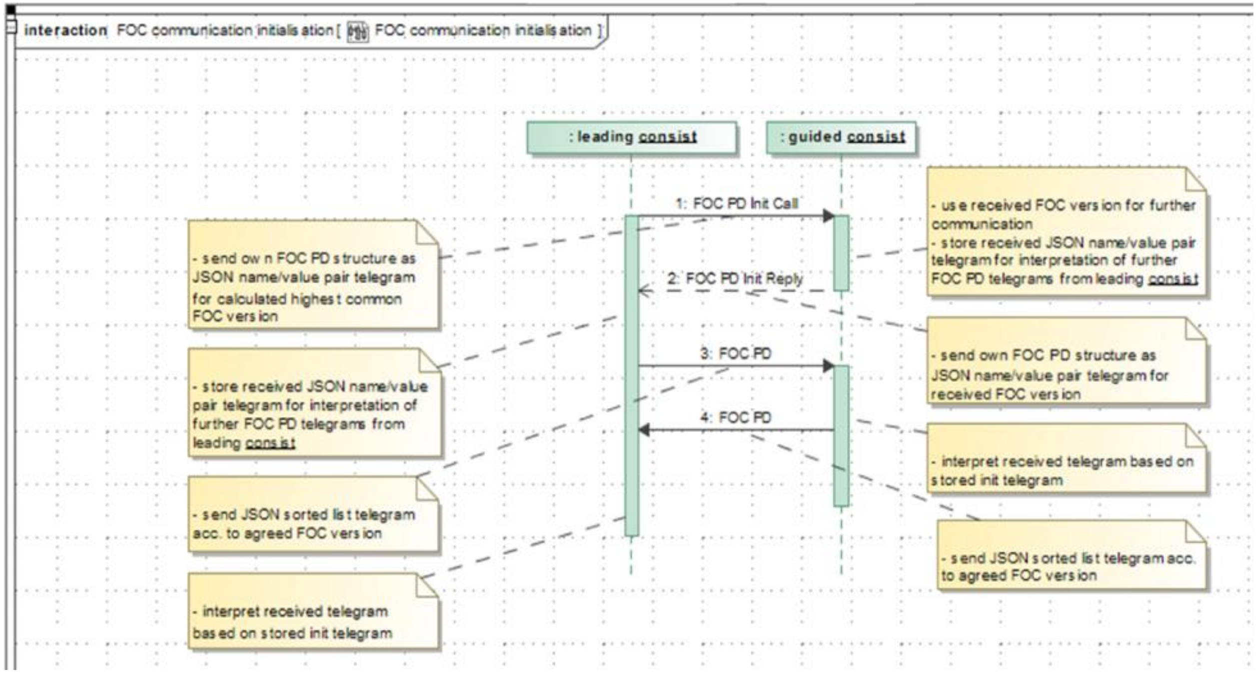
Data exchanges



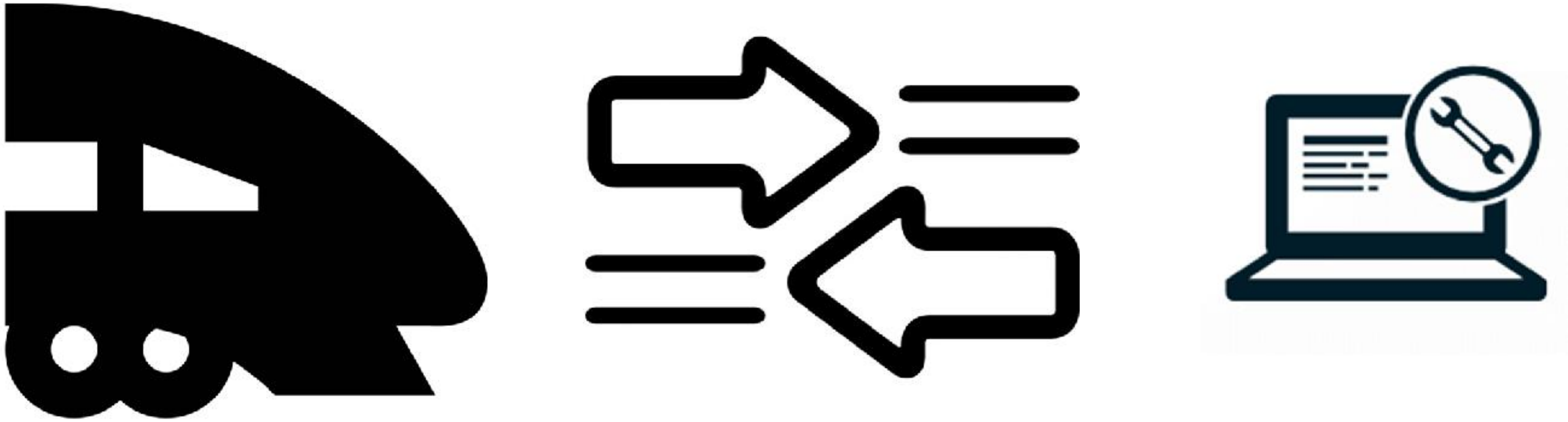
Data exchanges



Function Telegram Structure Initialisation



Certification of a consist type towards FOC standard

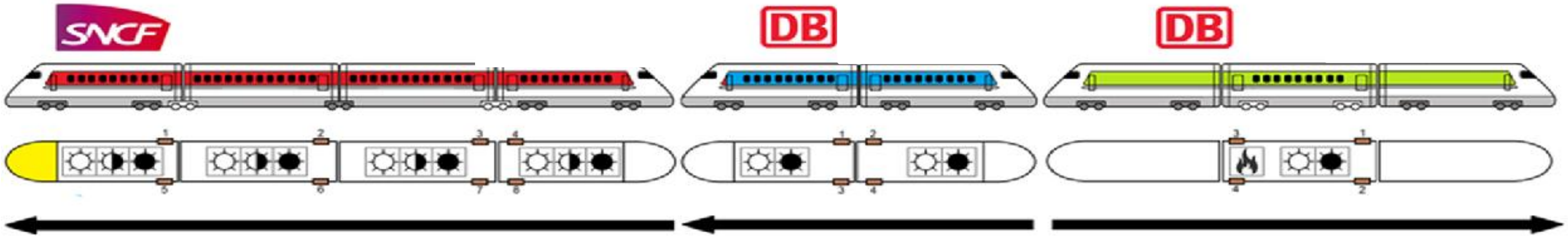


A consist type tested OK with the certified simulator shall operate successfully with any other consist that has passed the same test.

Functional Open Coupling in detail

- Use cases
- Communication concept & data exchanges
- **Examples**
- Next steps and conclusion

Example for traction effort capacity



Mass+ rotation inertia at full speed = 400 tons, Maximal effort 500kN	M+i 100 tons, Max 100kN	M+i 300 tons, Max 250kN
2 motor blocks OK 2 motor blocks Isolated	2 motor block OK 0 motor block Isolated	3 motor block OK 1 motor block Isolated
In case an average of consist is made : (50%+100%+75%)/3 = **75%** In case a fraction by motor block counting is made : "7/10 = **70%** of perf is available" In reality (2*125kN+2*50kN+3*62,5kN)/ 850kN = **63%** of force is available		

Need for specific definition of some interfaces with the right abstraction level

Functional Open Coupling in detail

- Use cases
- Communication concept & data exchanges
- Examples
- **Next steps and conclusion**

Next station is

- Completion of Function Open Coupling regarding **DMI visualization**
- Design and implementation of Functional Open Coupling **protocol**
- Definition of a certification strategy and definition of a conformance/interoperability test
- Definition of test cases, test scenarios, implementation and test execution

Quite a dense program for Connecta 2!

Conclusions

- The Functional Open Coupling allows a better **flexibility** in fleet management for operators (interoperability)
- A **FOC standard is necessary** to ensure compliancy:
  - Interface signals and their SIL Level
  - Physical description and specific abstraction level
- For some functions, due to diversity among consists, a specific level of abstraction has to be define
- With the **cumulative effects** of other new technologies such as **Application Profiles**, **Drive-by-Data** and **Wireless Coupling**, it is paving the way towards **Open Coupling**

Conclusions

Source: Youtube Railsimu https://www.youtube.com/watch?v=yQvbYcFYcGs

QUESTIONS & ANSWERS

VIRTUAL CERTIFICATION

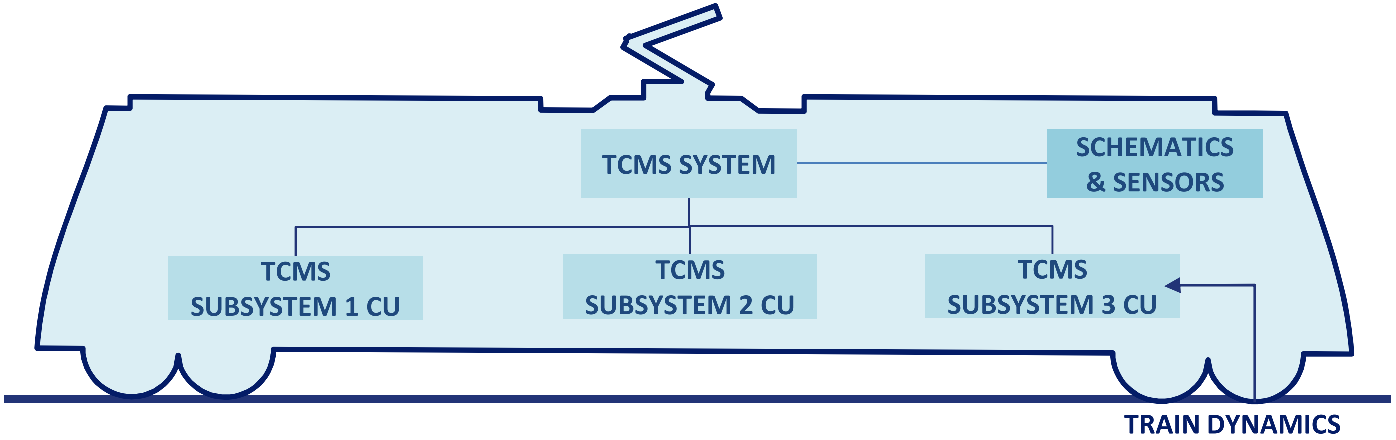
Simulation Framework and Train Virtualisation

Mikel Colera (CAF)

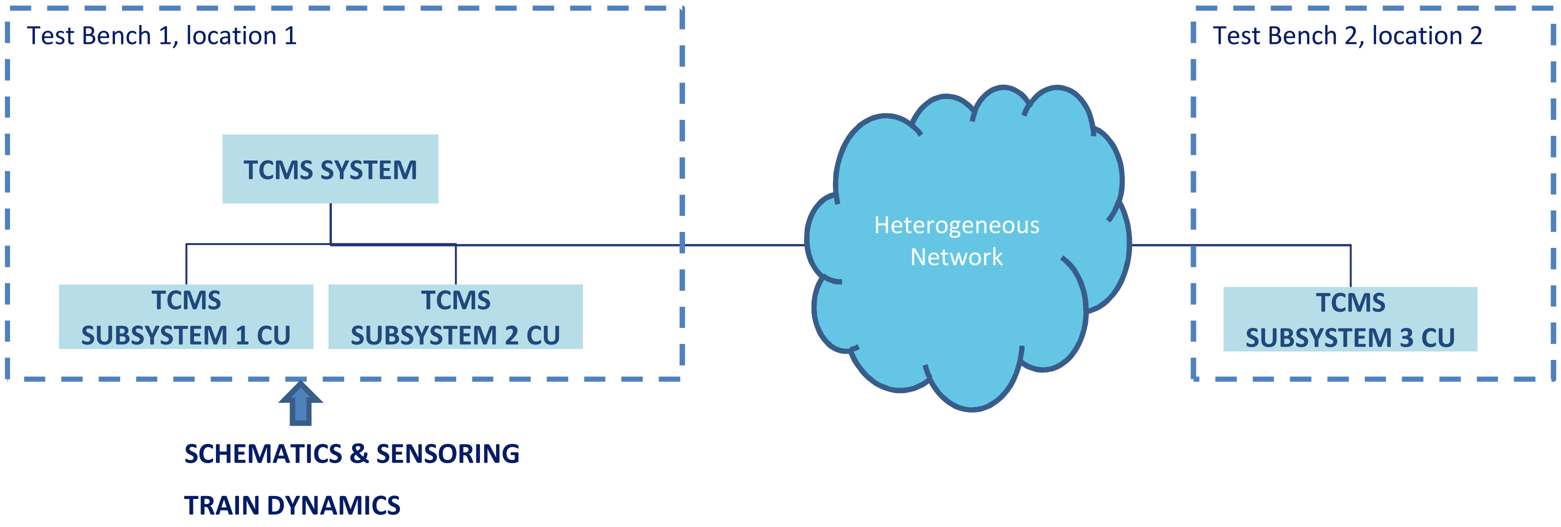
CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

What is VIRTUAL CERTIFICATION?

- It is the VALIDATION/CERTIFICATION of a TCMS SYSTEM and its subsystems in a lab environment with local/distributed virtual/real devices.

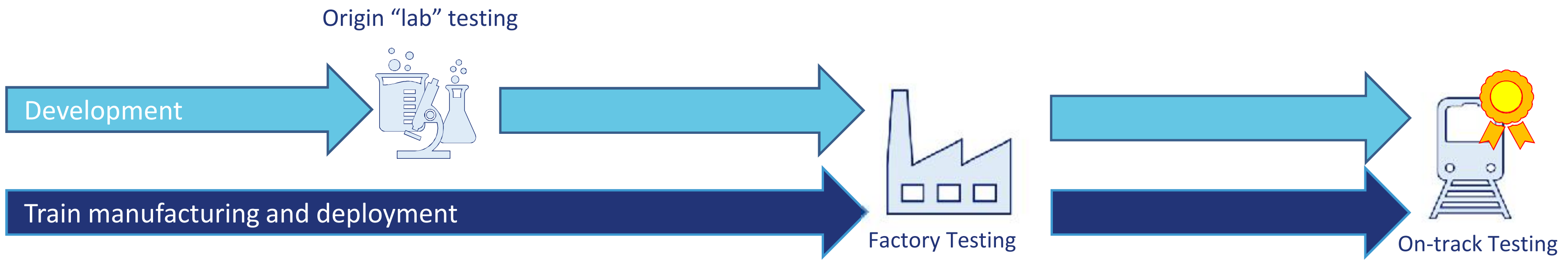


What is VIRTUAL CERTIFICATION?



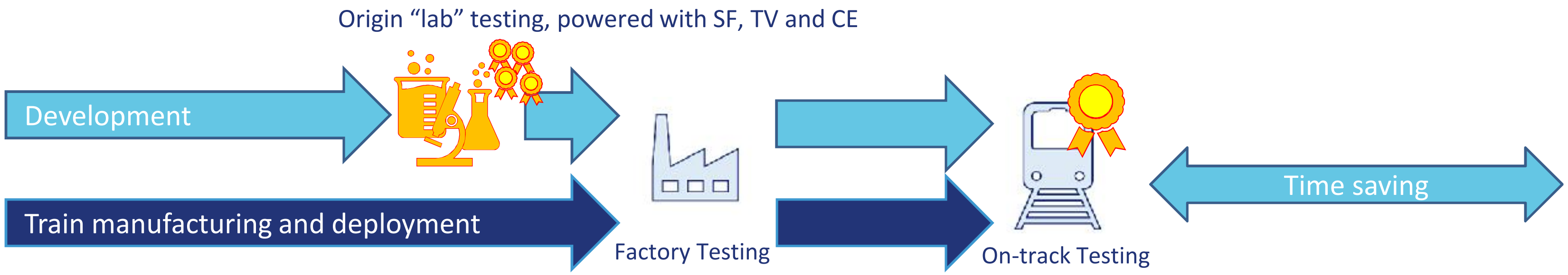
Why VIRTUAL CERTIFICATION?

Current state



Why VIRTUAL CERTIFICATION?

Future state



Why VIRTUAL CERTIFICATION?

Today	With VIRTUAL CERTIFICATION
TCMS system integration test with its subsystem are done with the real system and subsystems.	TCMS system integration with its subsystems will be done in a lab environment with some real devices and some simulated devices. The devices will be located locally or remotely.
TCMS system and subsystem integration with the train is done with the real train in track.	TCMS system and subsystem integration with the train will be done in a lab environment with simulated train environment information: schematics, wiring, train dynamics, etc.
Certification of the train is done with the real train in track	Partial or complete certification of a train will be done in a lab with simulated and distributed devices, simulated environment information.

VIRTUAL CERTIFICATION in detail

- VIRTUAL CERTIFICATION BUILDING BLOCKS

TV
TRAIN VIRTUALISATION

SF
SIMULATION FRAMEWORK

CE
COMMUNICATION EMULATOR

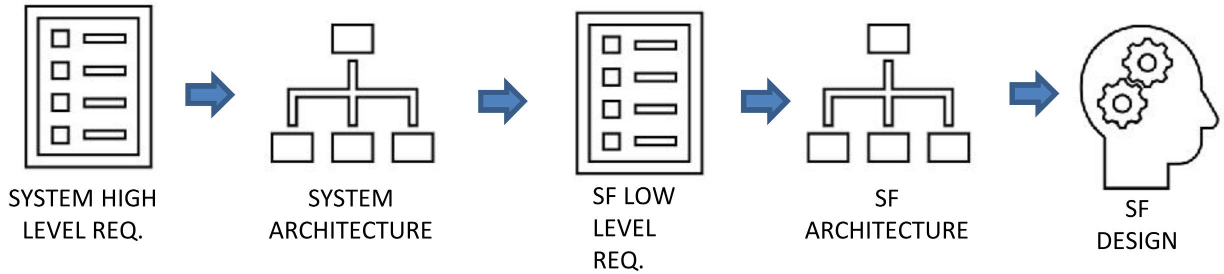
SW TS
SOFTWARE TOOLSET

VIRTUAL CERTIFICATION in detail

	TV TRAIN VIRTUALISATION	SF SIMULATION FRAMEWORK	CE COMMUNICATION EMULATOR	SW TS SOFTWARE TOOLSET
High Level Requirements	CTA 1	CTA 1	CTA 1	CTA 1
Low Level Requirements Arch&Desing	CTA 1	CTA 1	S4R	CTA 1
Implementation	CTA 1	CTA 2	S4R	CTA 1

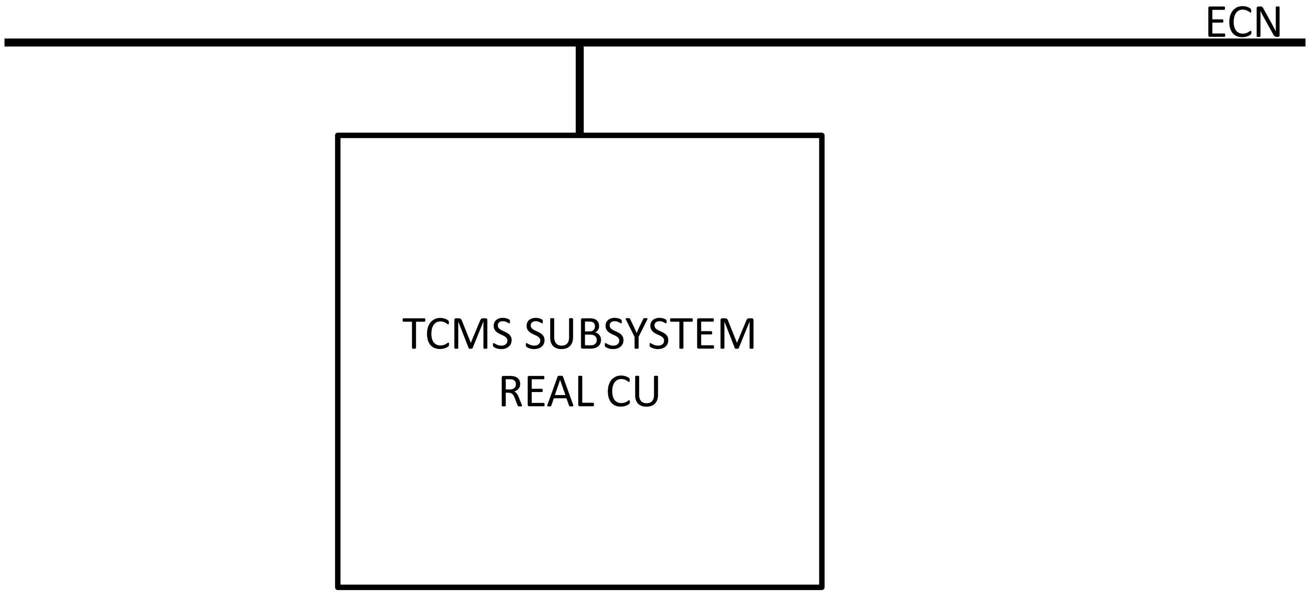
SIMULATION FRAMEWORK

- SF (SIMULATION FRAMEWORK)
  - SW MODULE FOR THE INTEGRATION OF:
    - REAL AND SIMULATED END DEVICES
    - TRAIN ELCTROMECHANIC SIMULATIONS (TRAIN DYNAMICS, SCHEMATICS)
    - MONITORING AND CONTROL FUNCTIONS OF THE SW TS

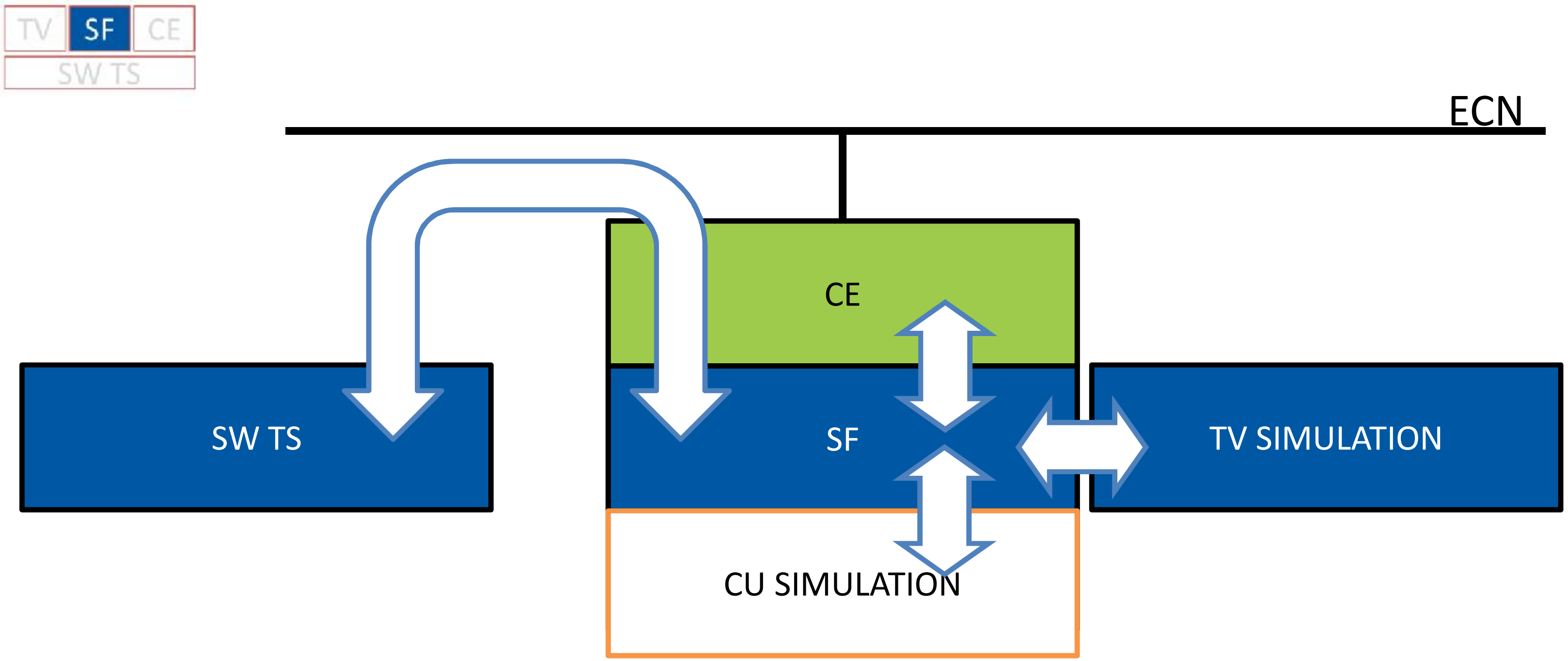


SIMULATION FRAMEWORK

TV SF CE
SW TS



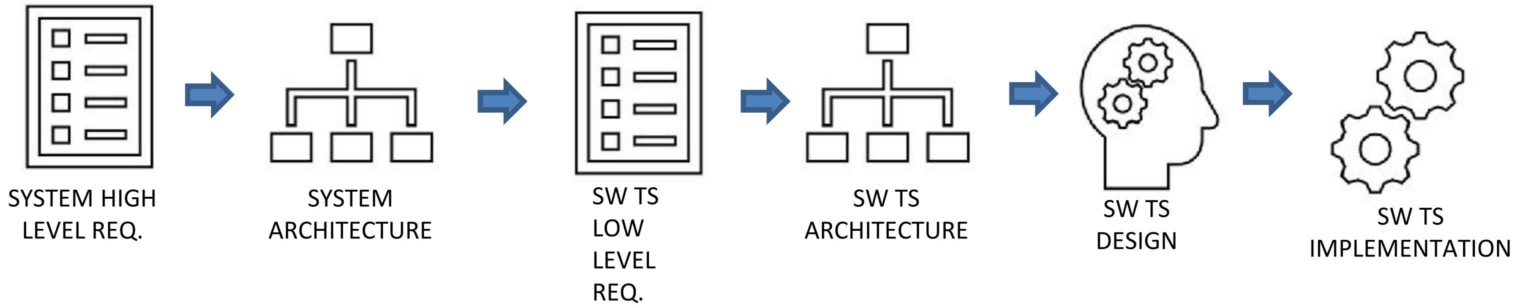
SIMULATION FRAMEWORK



SOFTWARE TOOLSET

TV SF CE
SW TS

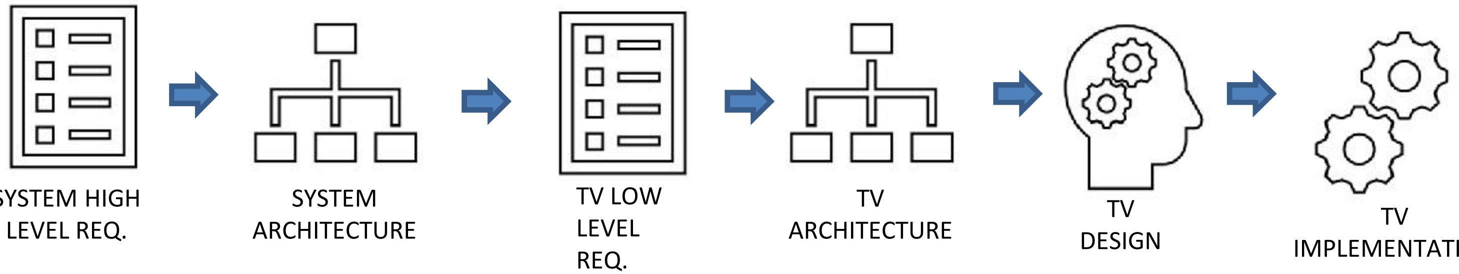
- SW TS (SOFTWARE TOOLSET)
  - SW TOOL FOR
    - SIMULATION AND TEST SCENARIO CONFIGURATION
    - MANAGEMENT AND CONTROL OF SIMULATIONS
    - TEST AND SIMULATION EXECUTION



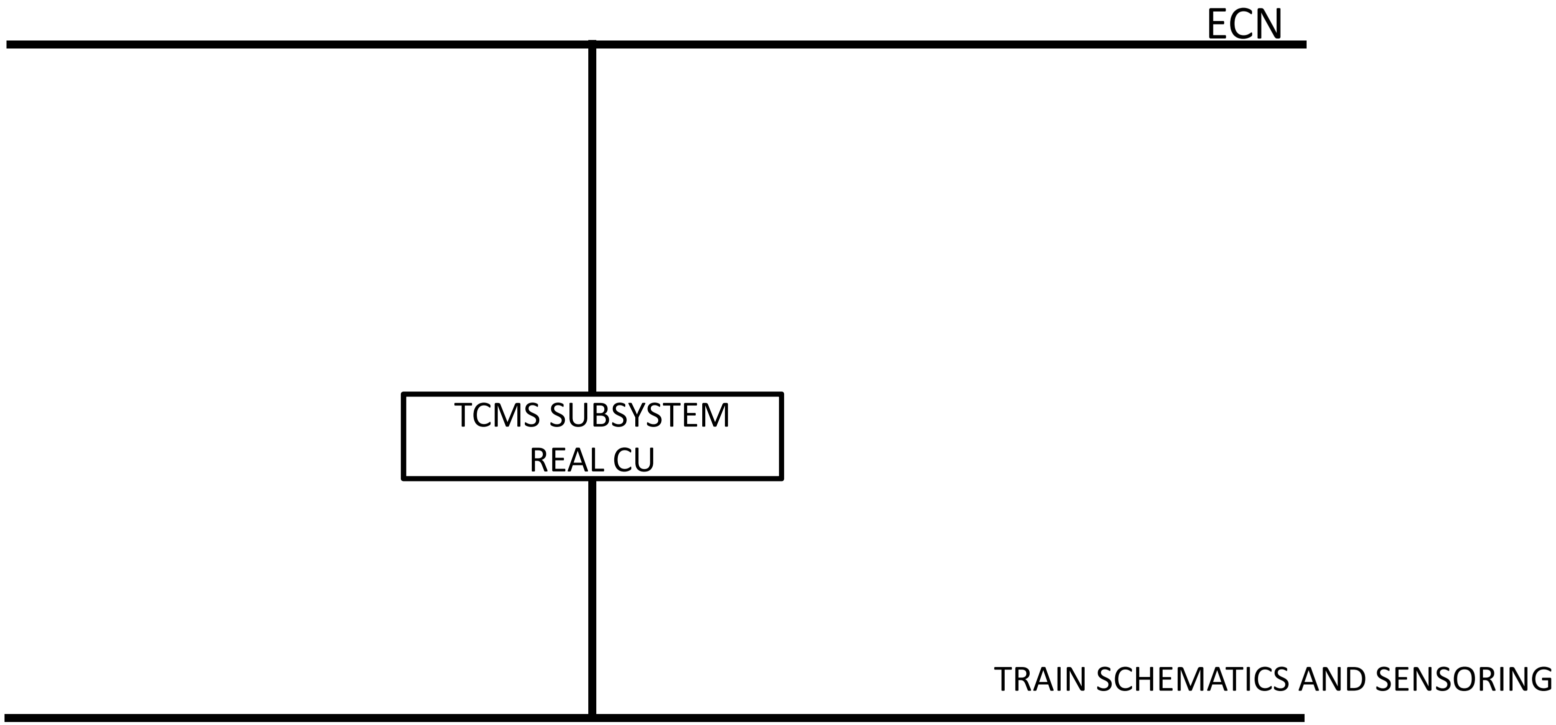
TRAIN VIRTUALISATION

TV SF CE
SW TS

- TV (TRAIN VIRTUALISATION)
  - SW FOR THE SIMULATION OF TRAIN BEHAVIOUR (DYNAMICS, PHYSICS AND ELECTRICAL)

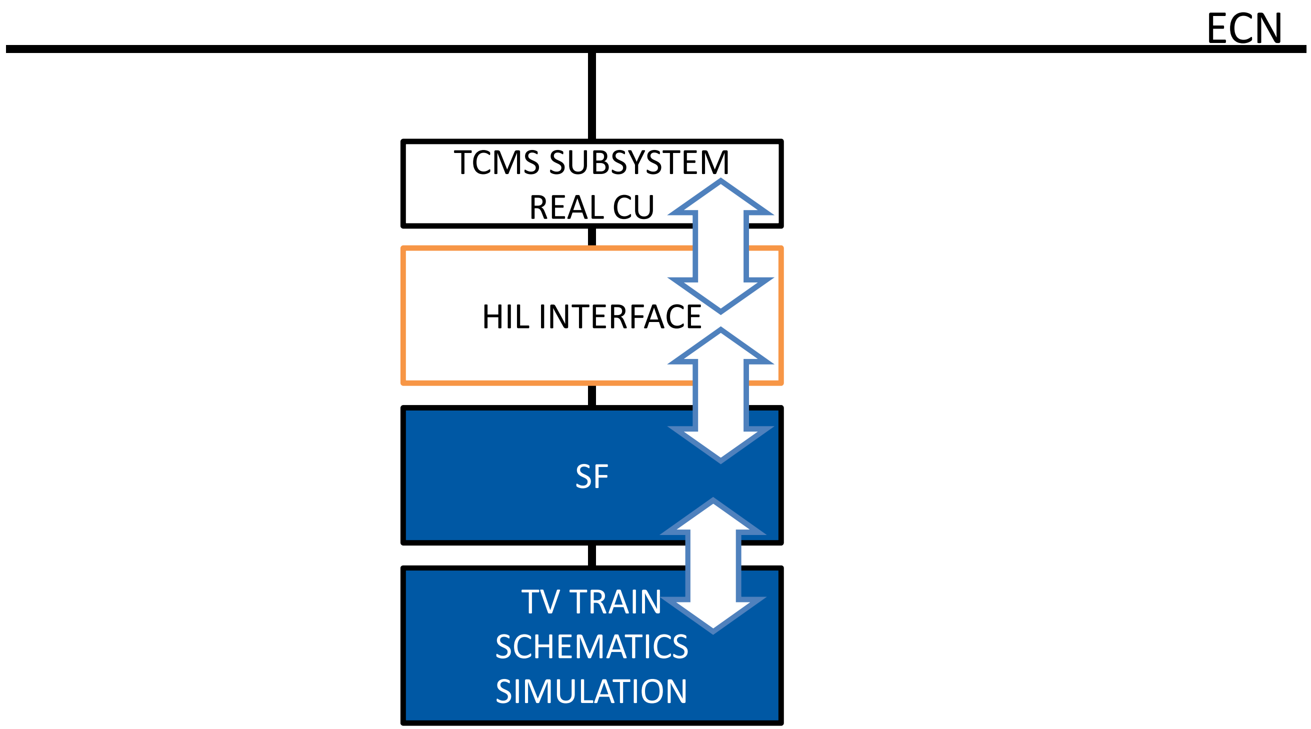


TRAIN VIRTUALISATION



TRAIN VIRTUALISATION

TV SF CE
SW TS

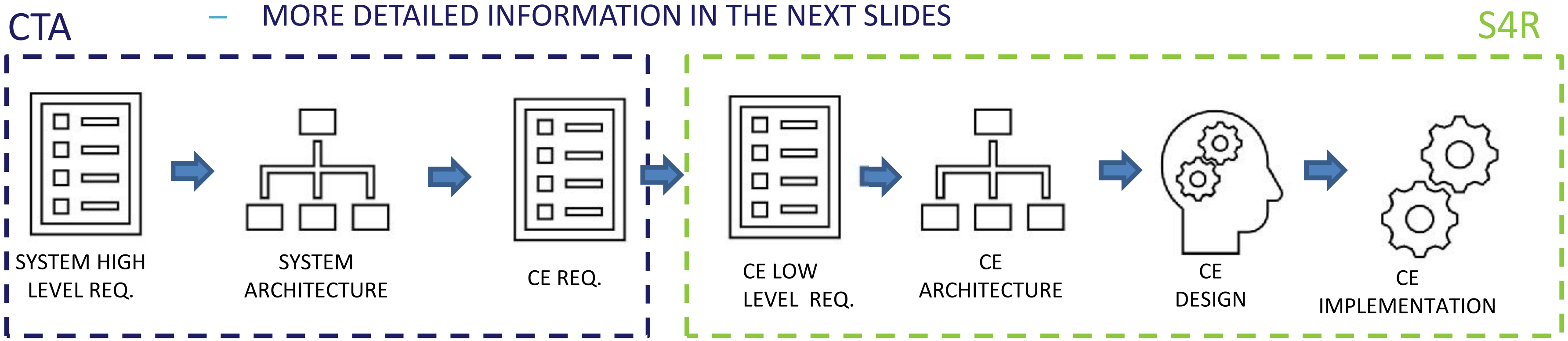


COMMUNICATIONS EMULATOR

TV | SF | CE
SW TS

CE (COMMUNICATION EMULATOR)

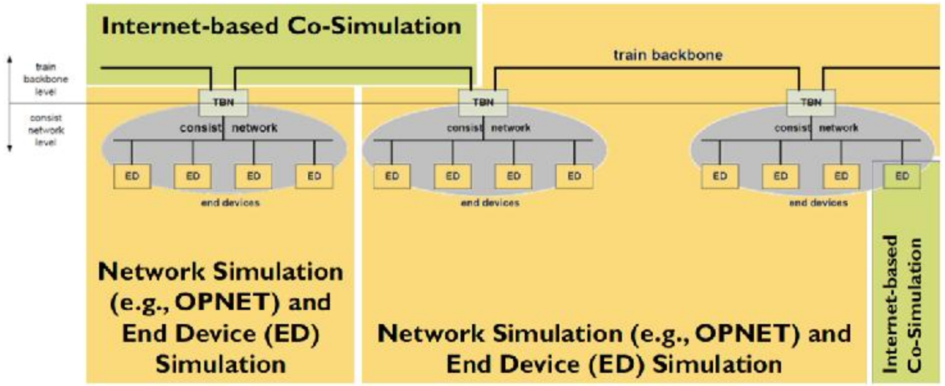
- SW FOR COMMUNICATION PURPOSE THAT ALLOWS THE EXCHANGE OF DATA BETWEEN REAL AND SIMULATED, LOCAL AND DISTRIBUTED DEVICES AND WITH THE SW TS.
- CTA DEFINED THE HIGH LEVEL REQUIREMENTS AND S4R DID THE LOW LEVEL REQUIREMENTS, ARCHITECTURE AND IMPLEMENTATION.
- MORE DETAILED INFORMATION IN THE NEXT SLIDES



TV | SF | CE
SW TS

COMMUNICATION EMULATOR

- Focus lies on the virtualization of a train via heterogeneous communication networks
- Co-Simulation of end device and network models on a network-centric abstraction level



COMMUNICATION EMULATOR Concept

TV | SF | CE
SW TS

- Design of a simulation bridge between real and simulated devices
  - Local or geographically distributed devices
  - Connection via heterogeneous communication networks (Internet, Local Area Networks, etc.)
- Definition of a generic interface based on Ethernet

COMMUNICATION EMULATOR Concept

TV | SF | CE
SW TS

- Synchronization and data exchange between devices
- Configuration for different protocols and real/simulated devices
- Mechanisms for monitoring and fault-injection (EN 50159)
- Management of delays introduced by the heterogeneous network
  - Measure delays and stop simulation if threshold exceeded
  - Estimate future input packets and forward packet to device if delay too large

COMMUNICATION EMULATOR subsystems

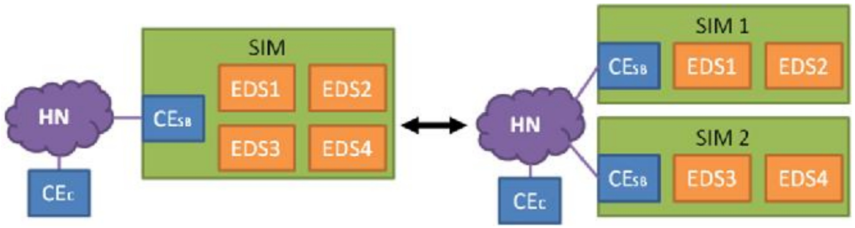
TV | SF | CE
SW TS

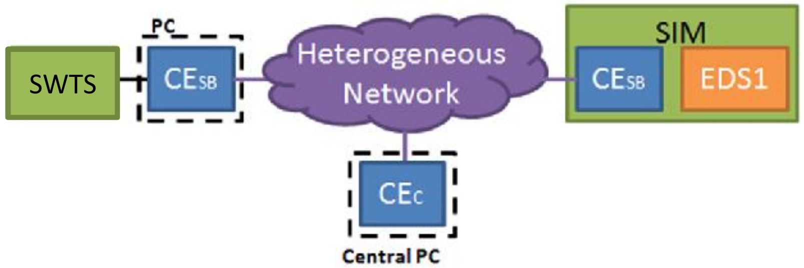
- Communication Emulator Simulation Bridges (CESB)
  - Connect real and simulated devices
  - Create communication channel
  - Based on High Level Architecture simulation standard (IEEE 1516-2010)
- Central Communication Emulator (CE_C)
  - Manages data exchange and synchronization of simulation bridges
  - Hosts an instance of the Runtime Infrastructure
  - Central component of the High Level Architecture
- Heterogeneous Network
  - Used to connect the simulation bridges
  - Internet, Local Area Network, etc.

COMMUNICATION EMULATOR Usage

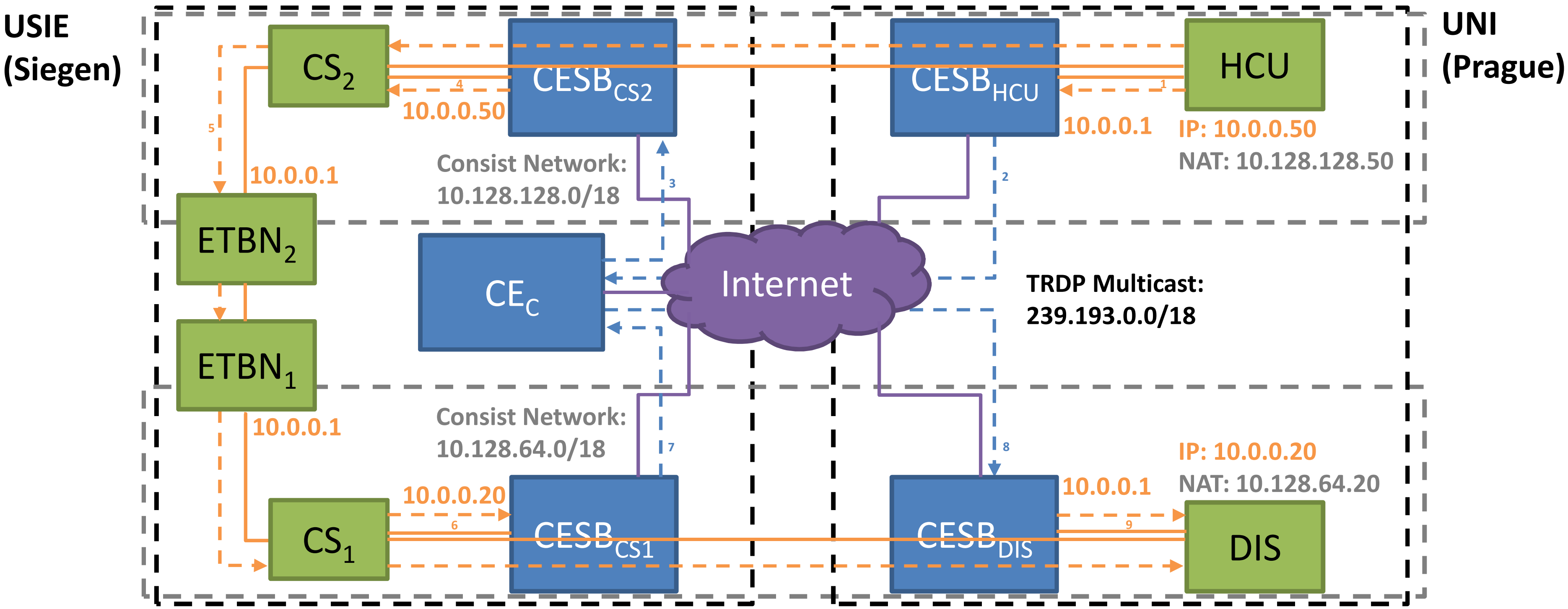
TV | SF | CE
SW TS

- Simulation host handles multiple End Device Simulations (EDS)
  - Simulated system can be distributed between multiple hosts
  - Connection via Simulation Bridges (CESB)
  - CE_C: Central Communication Emulator
  - HN: Heterogeneous Network
- Simulation host is controlled by Software Toolset (SWTS)
  - Commands are sent via CESBs
- Connection of real devices also possible (Hardware-In-The-Loop) → Demo





COMMUNICATION EMULATOR Demo



Next station is

	TV TRAIN VIRTUALISATION	SF SIMULATION FRAMEWORK	CE COMMUNICATION EMULATOR	SW TS SOFTWARE TOOLSET
High Level Requirements	CTA 1	CTA 1	CTA 1	CTA 1
Low Level Requirements Arch&Desing	CTA 1	CTA 1	S4R	CTA 1
Implementation	CTA 1	CTA 2	S4R	CTA 1

- Design and implementation of the SM
- Implementation of two test benches (urban and regional trains)
- Integration of all VIRTUAL CERTIFICATION building blocks

Conclusions

- In order to validate the development to use it for the validation /certification of a train, first we need to test and compare the results with those of a real environment.
- Validation of time sensitive requirements by means of distributed devices may be not achievable with the current technology.
- Standardisation of this technology is highly recommended by the experts in order for all the stake holder to accept the virtual certification.
- Integration activities must be carried out in CTA 2 in order to have a whole working system.

QUESTIONS & ANSWERS

Electronic Brake by Wire

Angelo Grasso, Wabtec

Martin Deuter, Knorr Bremse

Ugo Prosdocimi, Eletech

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

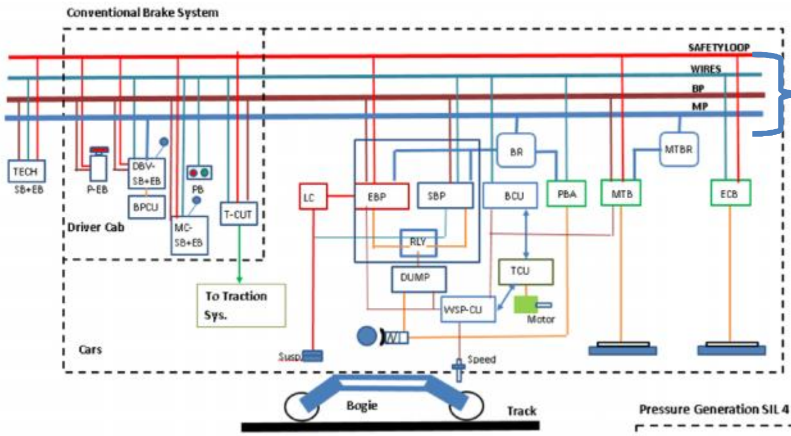
CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

Why? Brake by Wire

Today	With Brake by Wire
Train brakes control largely based on mixed pneumatic electrical technologies	Train brakes control and communication based on safe electronic technologies
Emergency Brake based on pneumatic command and safety loop control	EB part of an electronic system able to work with safety requirements up to SIL4
Braking distances limited by pneumatic components behaviour	Electronic improves brake efficiency, reduces braking distances and increase railway traffic capacity
Different subsystems for different brakes functionalities (EB, ES, PB, WSP ..)	Integrated controller able to manage all the main brakes functionalities
Different brake parts	Optimisation, reducing the number of sophisticated pneumatic components. Improving overall LCC
Custom solutions to interface brakes and train technical systems	IMP to support safety system integration between brake and technical systems

WP5 Achievements

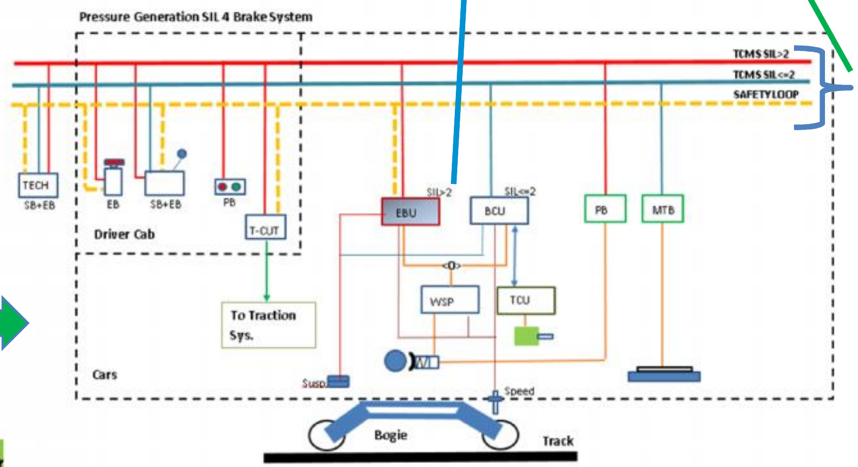
- Redu



- Reduce Complexity
- Improve Brake Performance (accuracy) Using High SIL Electronic

From Conventional
To Future

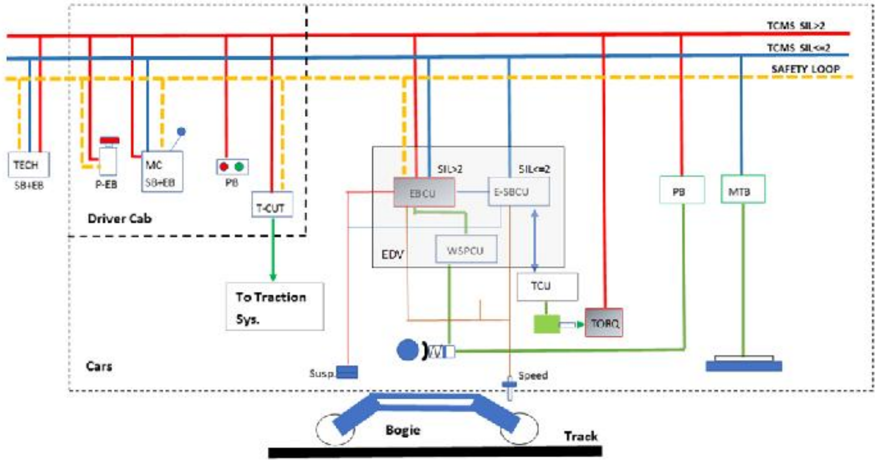
Task 1 Architecture



- High Safety Electronic pressure control, used to implement Electric Brake in Service and Emergency with integrated WSP:

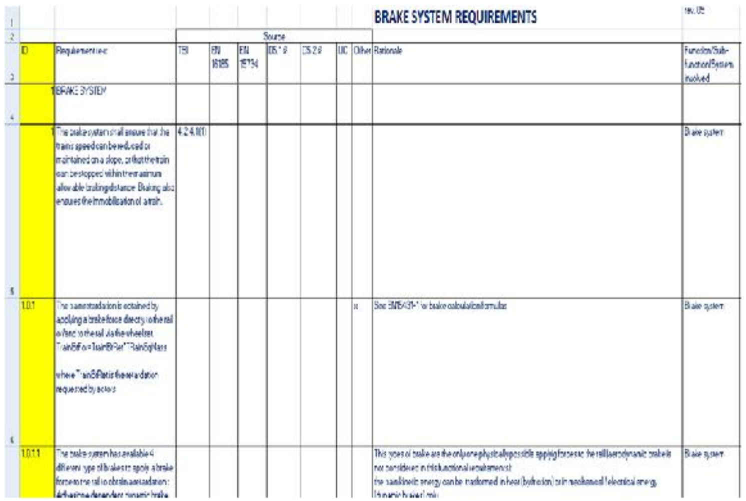
Advantages:

1. Improvement of the cylinder EB pressure output accuracy.
2. Simplification of train wiring & piping
3. Regulate emergency brake effort based on actual speed in a continuous way.
4. Simplification & scalability of brake system: possibility to use Electro Dynamic brake in Emergency
5. advantages LCC, noise reduction and energy saving.



Process Approach

- The conceptual organization of the technical activities is provided through a **V-cycle** tailoring the generic representation provided by the EN 50126.
- Functional model and Functional Requirements have been jointly defined by CTA & S4R
- Requirements taking care:
  - TSI safety requirements
  - Pre HAZARDs outputs
- Result:
  EDV Brake Function REQs
  & NG-TCN Communication Data



Safety

Brake system Safety analysis performed jointly with S4R

Inputs

- Brake System functional model and use cases
- Collection of the main hazardous scenario related to brake system

Output

- List of **Countermeasures** to be applied in the System Design
- List of **Application Conditions**
- List of **Safety Recommendations**

		THR	SIL
EB1.	Emergency brake command generation	≤ 10-9	SIL4
EB2.	Actual Emergency Braking Power Calculation	≤ 10-9	SIL4
EB3.	Emergency brake command transmission	≤ 10-9	SIL4
EB4.	Emergency Local brake force generation	≤ 10-9	SIL4
EB5.	Emergency brake energy storing	≤ 10-9	SIL4
EB6.	Traction cut off	≤ 10-9	SIL4
EB7.	Emergency brake state and fault detection and indication (applied/ released/ faulty/ isolated/ no info)	≤ 10-9	SIL4
EB8.	Emergency brake isolation	≤ 10-9	SIL4
SB1.	Service brake train retardation request	10-7 < THR ≤ 10-5	SIL1-SIL2
SB2.	Service brake request transmission	10-7 < THR ≤ 10-5	SIL1-SIL2
SB3.	Train Load Calculation	10-7 < THR ≤ 10-5	SIL1-SIL2
SB4.	Train Brake Force Calculation	10-7 < THR ≤ 10-5	SIL1-SIL2
SB5.	Blending (speed and/or adhesion and/or load and/or brake disk temperature dependent)	10-7 < THR ≤ 10-5	SIL1-SIL2
SB6.	Service brake force application energy storing	10-7 < THR ≤ 10-5	SIL1-SIL2
SB7.	Holding brake	10-7 < THR ≤ 10-5	SIL1-SIL2
SB8.	Traction cut off	-	-
SB9.	Service brake state and fault detection and indication (applied/ released/ faulty/ isolated/ no info)	-	-
SB10.	Service brake isolation	10-7 < THR ≤ 10-5	SIL1-SIL2
PB1.	Parking brake command generation	≤ 10-9	SIL4
PB2.	Parking brake train command transmission	≤ 10-9	SIL4

Hazard Analysis | Inputs | Safety Targets Allocation

SAFETY REQs for EDV

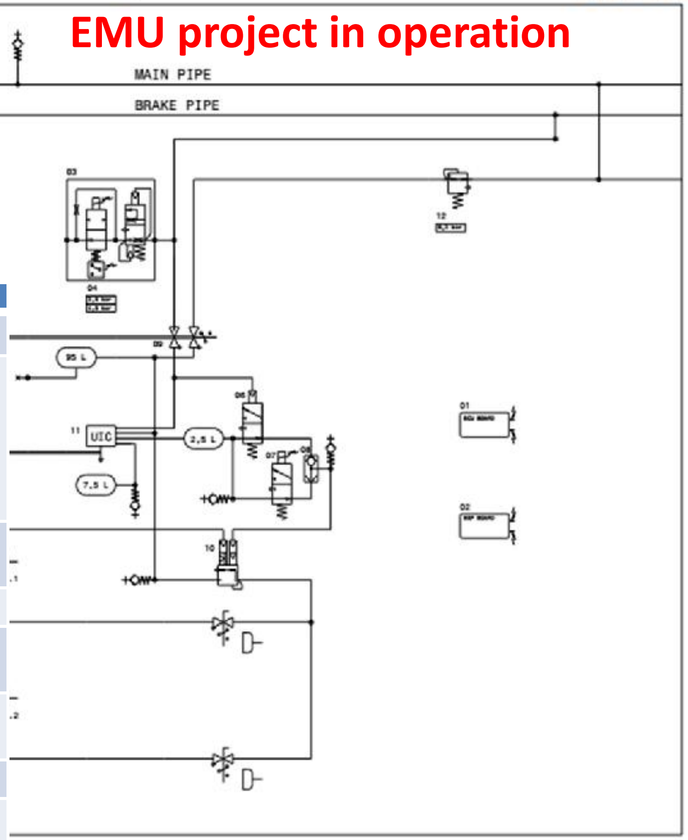
LCC Analysis

LCC costs reduction

- EDV architecture compared ⟺
- EMU regional

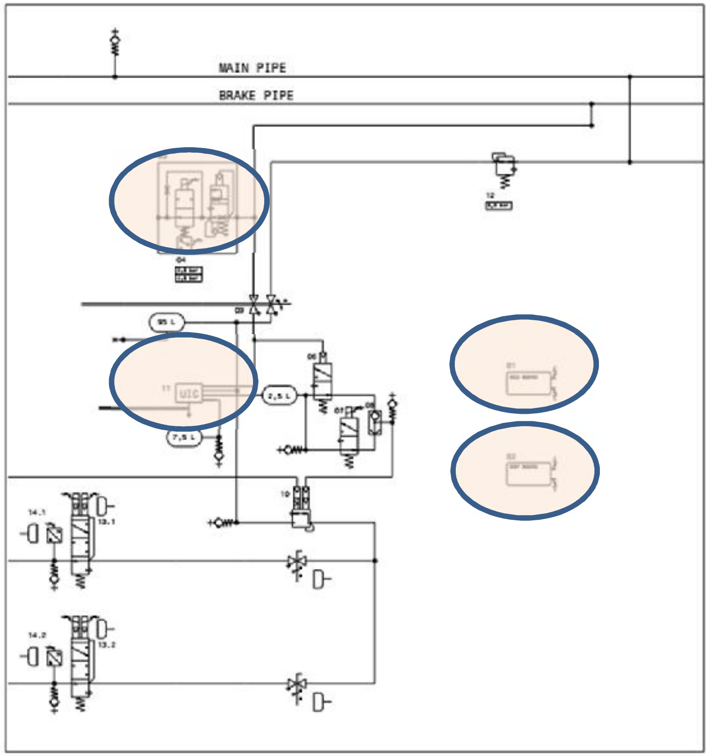
Equivalent components are identify

EMU			EDV		
Nr.	Cd.	Component	Nr.	Cd.	Component
2	(14.1) (14.2)	Pressure Transducer	2	P_BC	Transducer
1	(05)	Pressure Transducer	2	P_Load	Pressure Load Transducer
1	(07)	Magnet Valve	1	mvF	Magnet Valve Fill
			1	mvS	Magnet Valve Vent
			1	mvRR	Magnet Valve Remote Release
1	(10)	Relay Valve	1	RV	Relay Valve
1	(12)	Pressure Reducer	1	PnRg	Pressure reducer



LCC (II)

From the LCC analysis, the EDV device allows to reduce the use of pneumatic components



Preventive Maintenance

➡ **28% Reduction Off.**

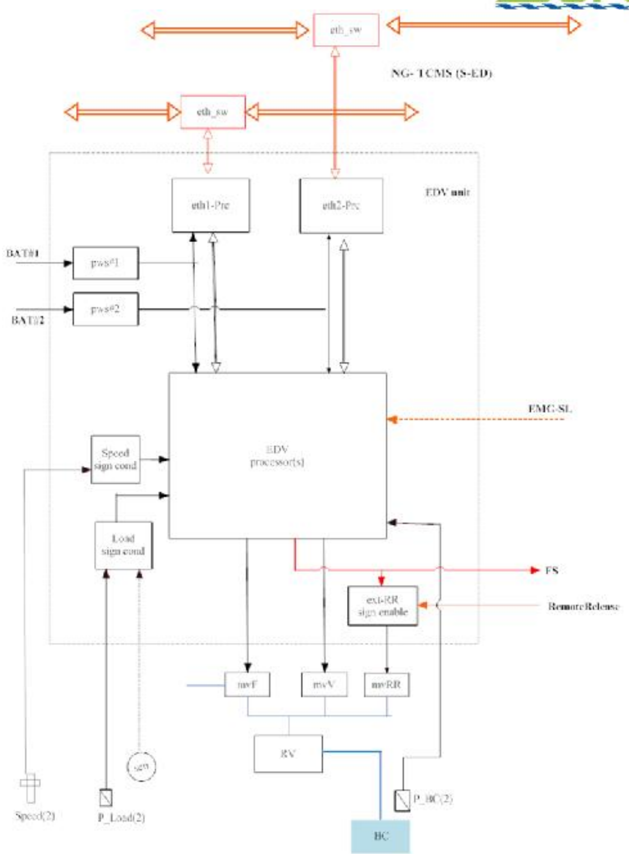
Corrective Maintenance

➡ **27% Reduction Off.**

EDV FT Architecture

WP5 Competitive Design

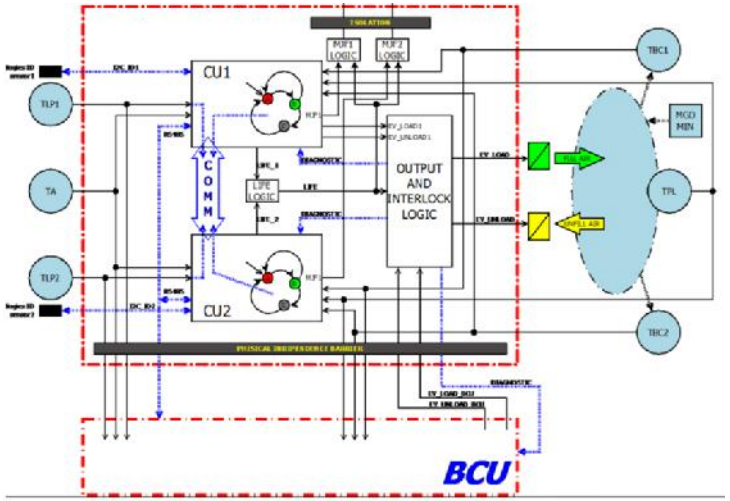
- EDV Sub System Design: the activity will be finalized to development of a control board for the HIGH SIL system, identified as Electronic Distributor Valve (EDV).
- integration with NG_TCN proposed architecture
  - embedded virtual A-Plane and B-Plane for scheduled data traffic (TSN domains)
  - Safety-End Device (e.g EDV) are connected to both planes

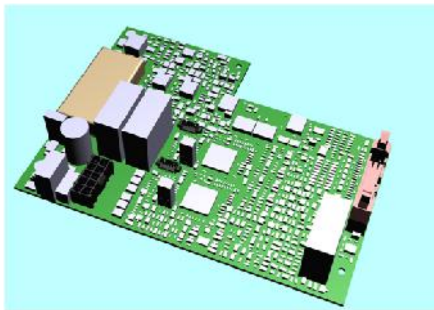


EDV FT Goal

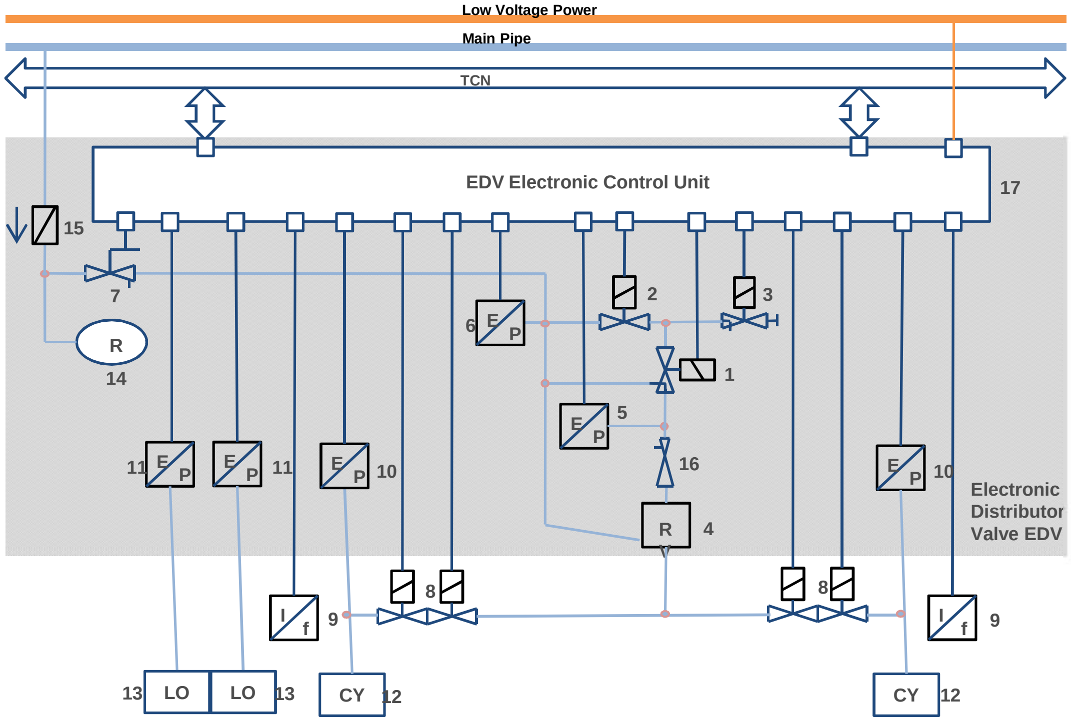
EDV FT hw architecture

- Safety requirements taking care of axle redundancy
  - THR applicable target
  - resilience to single fault not requested
- Architecutre is 2oo2 acting “reactive failsafety” as EN_50129
- LCU1 is the “main computation channel”
- LCU2 is the “checking channel”.
- Interface to NG-TCN control is support by specific BCU I/O





KB EDV Architecture



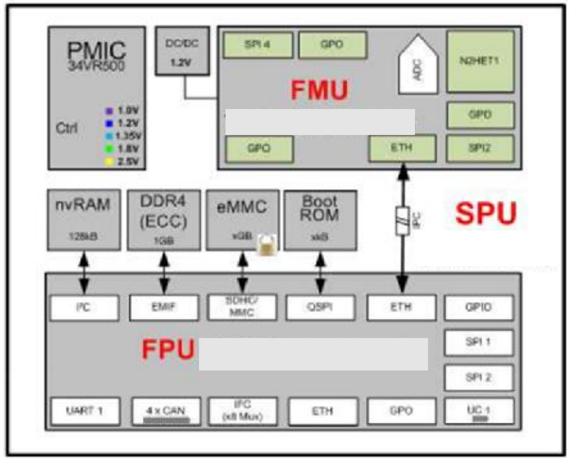
emergency valve (1)
brake valve (2)
release valve (3)
relay valve RV (4)
pilot pressure sensor (5)
air supply pressure sensor (6)
isolation cock (7)
dump valve (8)
speed sensor (9)
cylinder pressure sensors (10)
load sensors (11)
brake cylinder (12)
air suspension (13)
local reservoir (14)
check valve (15)
pressure limiting valve (16)
EDV electronic distributor valve (17)

Knorr-Bremse Goal

Local Application Device LAD with CPU sub device for High Safety Level Architecture

Technology:

- High Safety Level Electronic Architecture on SIL 3/4 Level for Brake Control
- LAD Application SW on SIL 3/4 Level
- NG TCN Communication to Brake Control Electronic Units
- SIL3/4 Assessment of the Local Application Device LAD



S4R Brake by Wire

- **S4R Brake by Wire project goal**
  - define the requirements and the safety concept for a high safety (SIL4) Brake Electronic Control (EC) based on the IMP

- **S4R Brake by Wire means**
  - system design down to electronic control
  - fully integrated with train technical systems
  - focused on the **E**mergency **B**rake as the highest safety demanding brake functionality (SIL4)

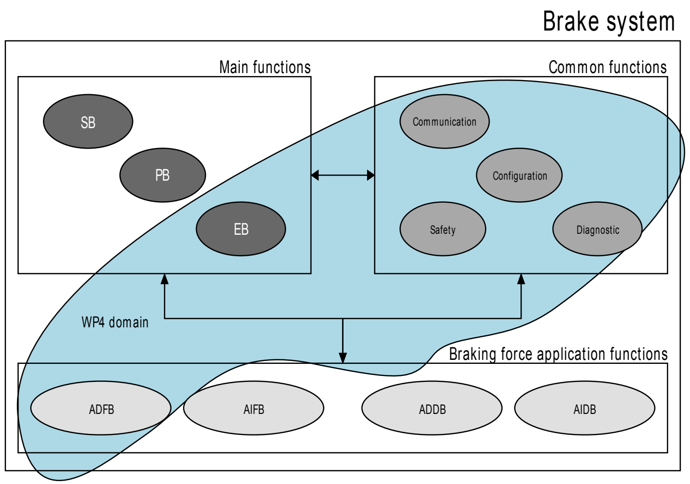
S4R Brake by Wire

- **development covers :**
  - functional model of an advanced train brake system
  - safety requirements added through an Hazard Analysis with safety countermeasures definition
  - System architectural development
  - Electronic Control requirements, parted in:
  - central control (**V**ehicle **C**ontrol **U**nit)
  - local physical brakes i/o control (**R**emote **B**rake **C**ontrol **U**nit)
  - requirements propagated to IMP and train technical systems

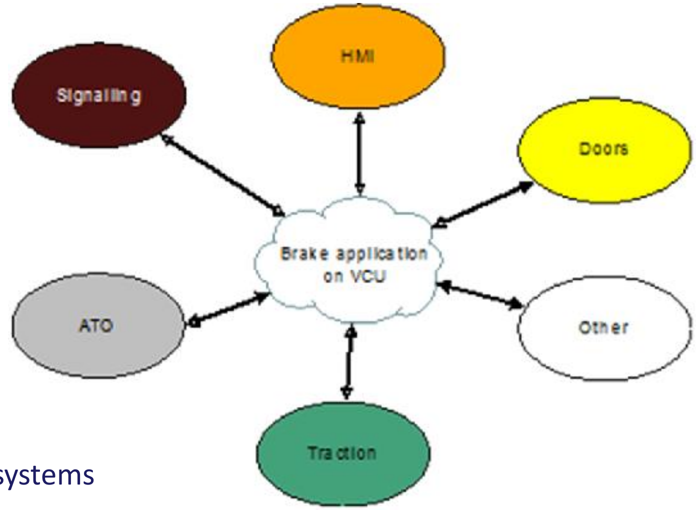
- **development executed :**
  - respecting railway standard EN50126 with :
    - top down V process
    - safety process
    - Safety V&V
    - Safety Indipendent A**s**sesment

S4R Brake by Wire : requirements

- **Project boundaries:**



- EB Emergency Brake
- ADFB (disk brake)
- Interface to other brake types subsystems and peripherals

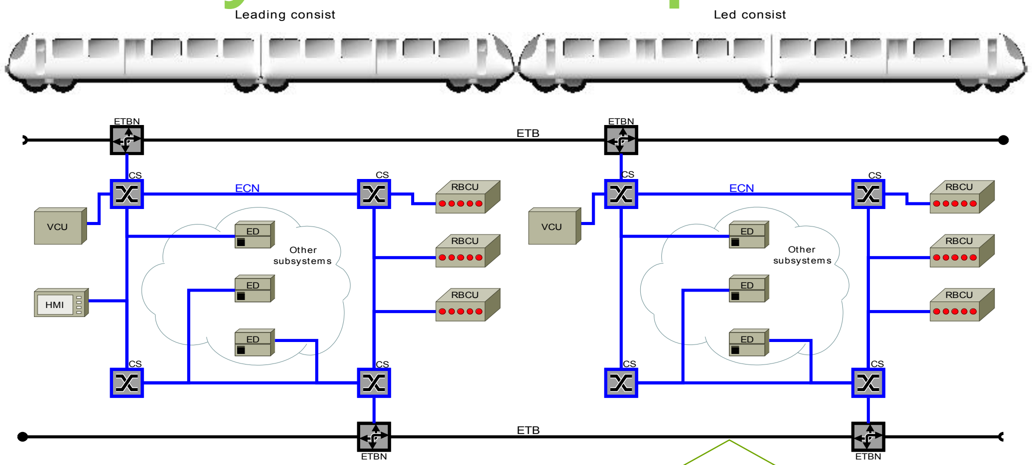


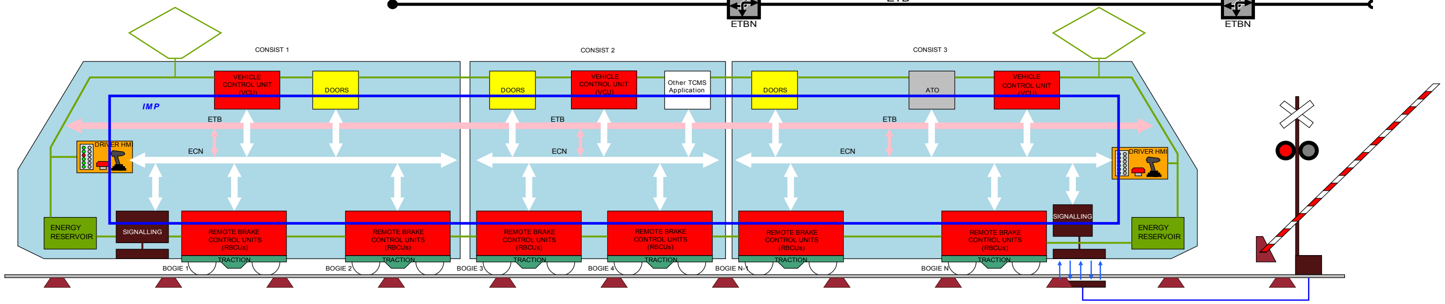
- Interfaces to train technical systems

S4R WP4 Brake by Wire : Requirements

- **Train architecture**

- Consist local (ECN) and train backbone (ETB) networks
- Vehicle Control Unit
- Remote Control Units at axle/bogie level



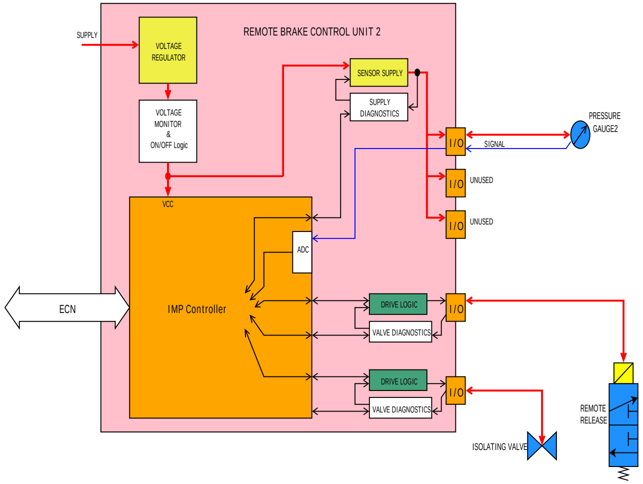


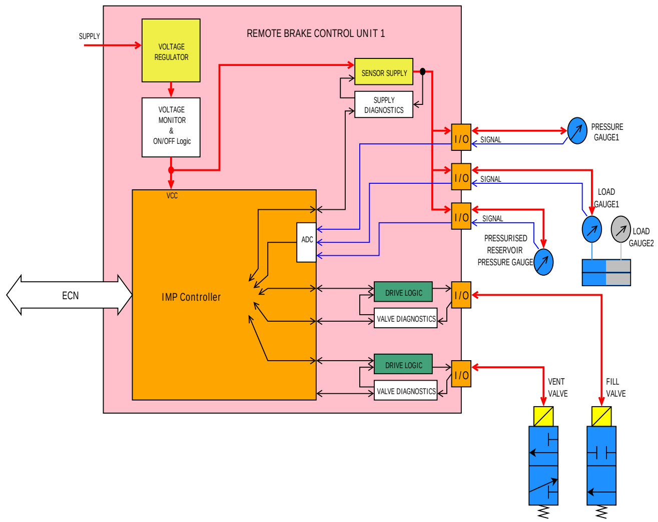
S4R Brake by Wire : Requirements

- **Central brake control (Vehicle Control Unit) :**
  - IMP high availability and SIL4 features
  - coordinates differents type of brake requests : Service Brake, Parking Brake, Emergency Brake
  - allows speed management aligned with the available brake capacity granting safety stopping distances
  - automatically manages running capability
  - manages single brake units isolation
  - manages single brake units remote release
  - manages train weight measure

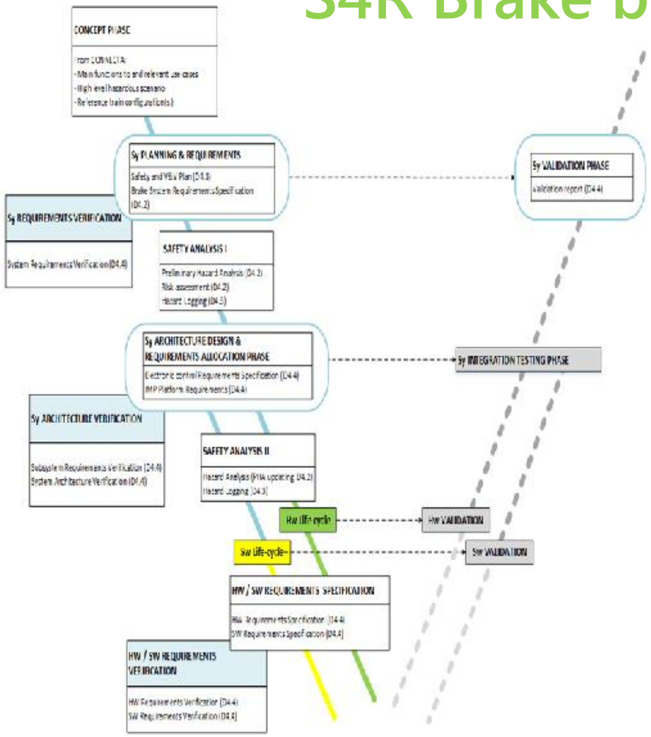
S4R Brake by Wire : Requirements

- **Local brake disk control (Remote Brake Control Unit RBCU) :**
  - remote i/o
  - safety monitoring fuctionalities
  - local pneumatic pressure loop control
  - i/o interfaces parted on the base of safety functional indipendency needs
  - IMP based controller





S4R Brake by Wire : Safety Process



- **Safety activities** defined consistently with EN 50126 and EN 50129
    - Process planned
    - Preliminary Hazard Analysis
    - Risk Assessment
    - FTA THR allocation
    - Safety Requirements Verification & Validation
    - Anomalies Management
    - Hazard Logging
    - Safety Assessment

S4R Brake by Wire : conclusion

- **System developments based on this concept work will :**
  - be able to substitute with a SIL4 electronic control the pneumatic and electric control technologies
  - deliver the innovative functionalities provided by the model jointly defined with Connecta
  - allow full integration for the whole braking functionalities
  - ask for the use of the IMP platform at its highest level of safety and availability features

- **The work delivers a clear evidence for the need of a train integrated high safety control and communication platform as the IMP :**
  - the brake system, surely for the emergency brake function, is a SIL4 application distributed all along the train with the need to interface at the maximum safety level almost all the other train technical system
  - the complexity of this task, since it involves the whole train control systems, seems affordable only if based a strong common safety platform

QUESTIONS & ANSWERS

COFFEE BREAK

20 minutes, c’mon show you can do it well now!

CONNECTA has received funding from the European Union’s Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme.

Train to Ground

Armin Heindel, SIE/ Richard Pecl, UC

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

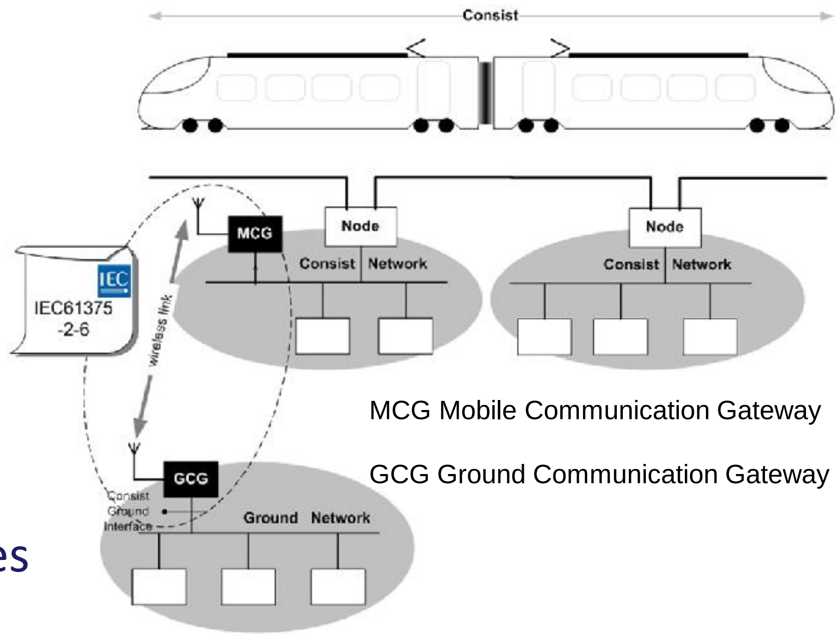
Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)

What is Train to Ground Communication ?

- Integration of the train on-board communication network in the operator on-ground network infrastructure
- Definition of a set of communication protocols
- Provisioning a set of services

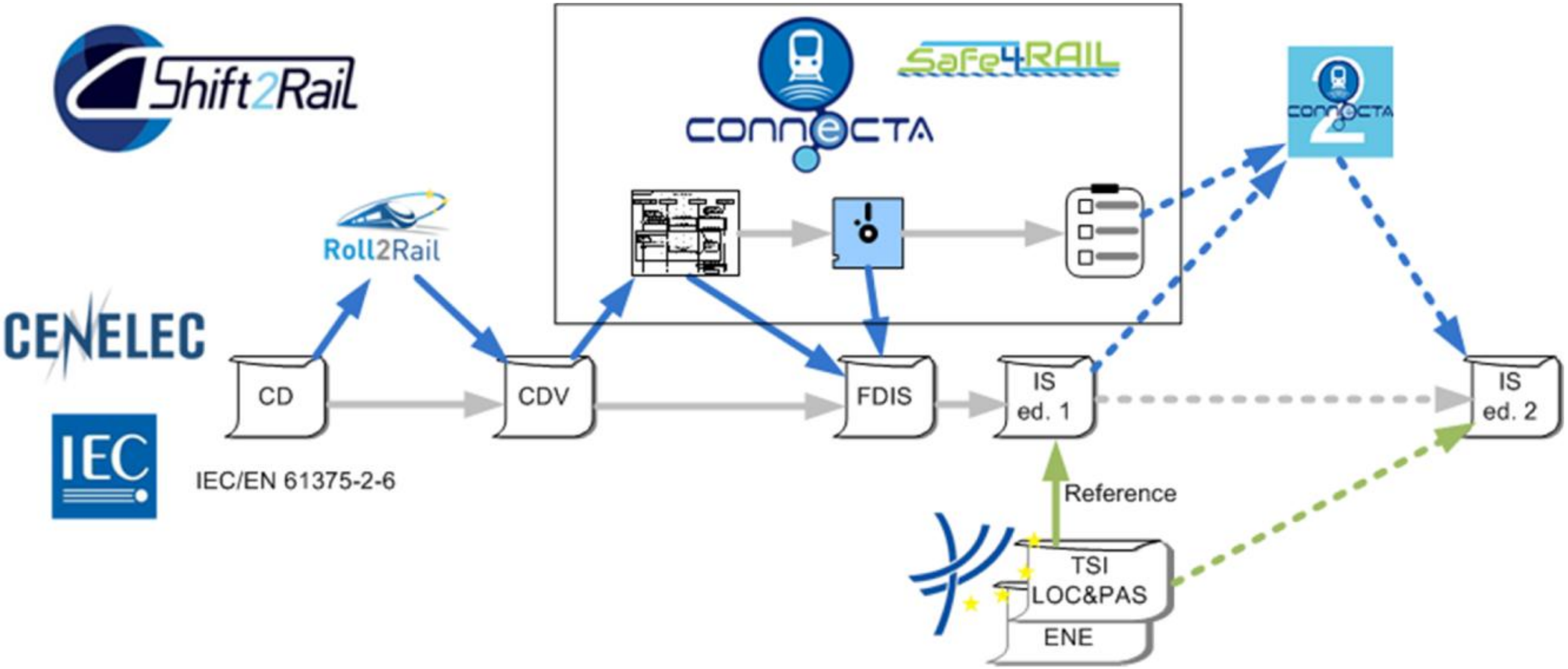
- Communication partners shall understand each other, therefore communication protocols and services need to be clearly defined



Why ?

Today	With standard IEC/EN 61375-2-6
Many different implementations of Train to Ground communications from different manufacturers for different railway operators are existing:	The standard defines a clear set of requirements for Train to Ground communication protocols and services
• using proprietary, non-interoperable communication protocols	Implementations according to the standard understand each other
• using different non-interoperable services	Common used services are available
• increasing efforts and costs in maintenance or operation with different railway operators	Only one solution (per manufacturer or operator) needs to be maintained, easier border crossing traffic possible

Shift2Rail and Standardisation

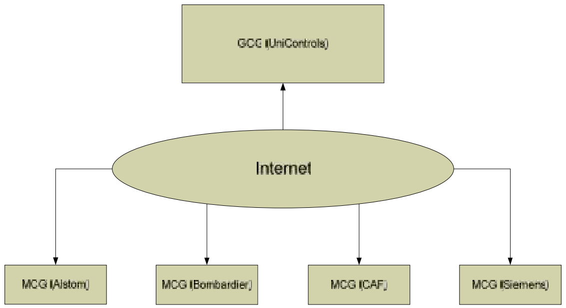


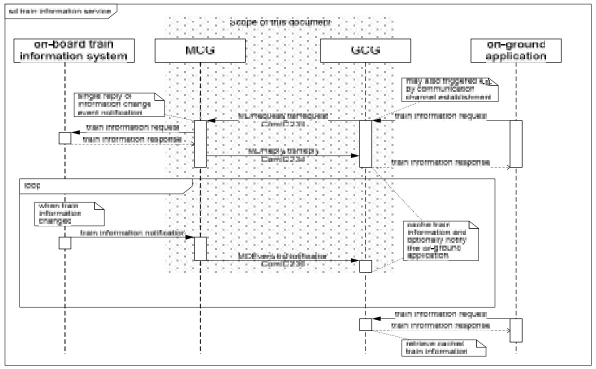
Verification of IEC/EN 61375-2-6

- Analysis of the requirements of the draft versions of the standard
- Selection of three use cases for implementation (Train identification, Train location, File transfer)
- Detailed specification of communication protocols between MCG and GCG
- MCG implementation by four CONNECTA partners (ALS, BTG, CAF, SIE)
- Test Environment & GCG implementation by Safe4RAIL (UC, IKL, IFS)
- Cooperative test by CONNECTA and Safe4Rail
- Feedback of experiences to IEC TC9 WG43

MCG & GCG Implementation

Four independent MCG implementations	Dynamic behaviour	Telegram definition



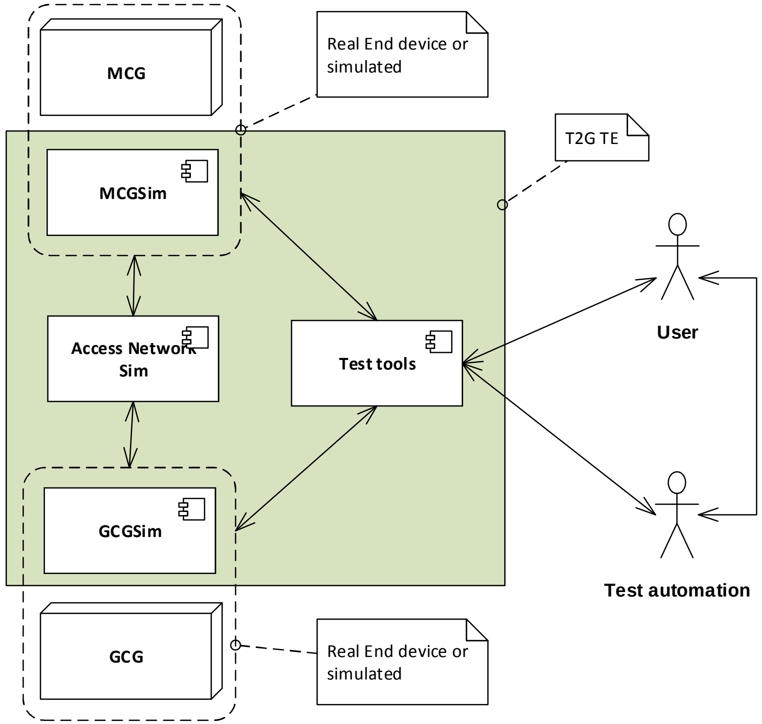


Data Element	Description	Datatype	Value Range	Value
object	Payload of MD body parameter "mdPayload"	JSON		
fileTransferUID	Unique identifier. Defined by the MCG, used by the MCG and GCG to identify a file that is uploaded. Must be unique number for each MCG.	number	uint32	computed
filename	Name of the file to be transferred to the GCG. Used by the GCG later to enable access the uploaded file.	string	char[256]	predefined
fileType	Indicates the type of file that is uploaded.	number	uint8	0 = n.a. 1 = ASCII 2 = Binary 3 = Audio 4 = Video 5-255 not used
fileServiceFunction	Specifying the source service. (Complete list is not in the scope of the interface specification.)	number	uint8	0 = not in the list 1 = EMS 2 = CCTV other values reserved
fileSize	Indicates the size of the file to be uploaded, in bytes. Determined by the MCG.	number	uint64	predefined

Implementation and deployment

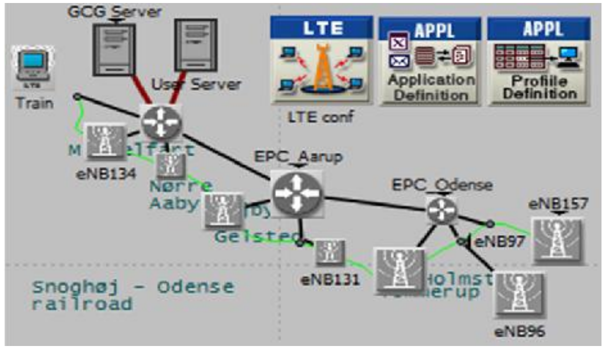
Train2Ground Test Environment

- MCG Simulator
- GCG Simulator
- Access Network Simulator
  - LTE
  - Wi-Fi
- Test Tools
  - Test scripts



Train2Ground Test Environment

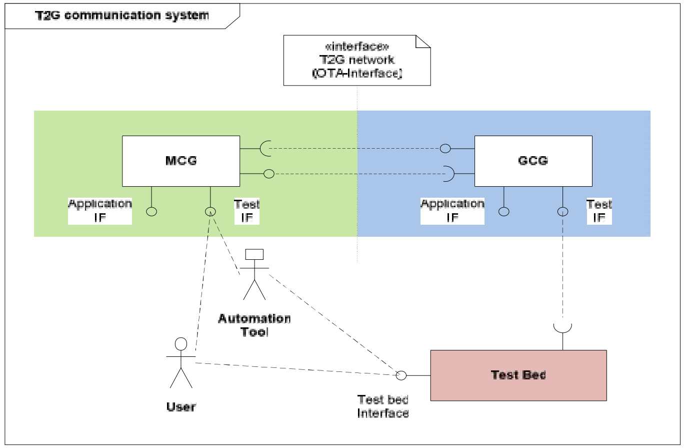
- LTE network simulator (Riverbed Modeler)
  - Pure simulations
  - Co-simulations
- Wi-Fi network simulator

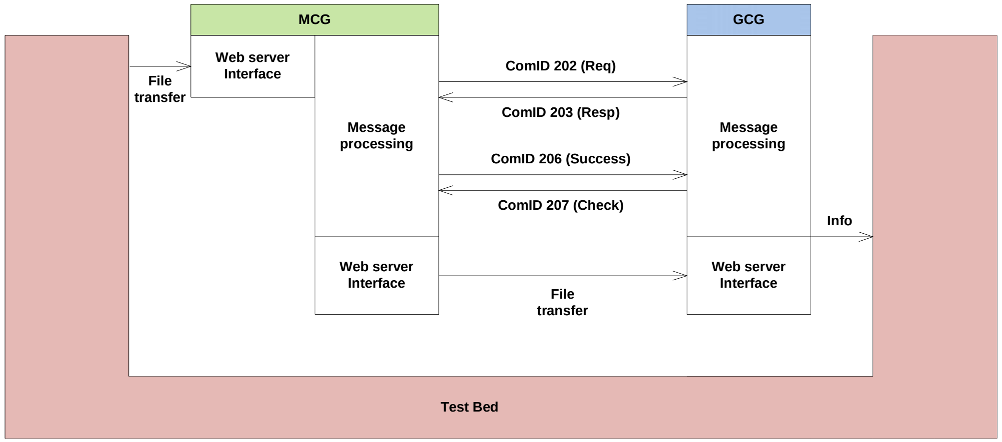


- Simulations: handovers, signal fading, simultaneous usage by passengers, jamming

MCG-GCG-Test

- Test setup (MCG/GCG) and test case (example File transfer)





- → Test report with list of observations as input to IEC for improvement of the standard

Next station is

- We are on the way:
  - The time lines of IEC and CONNECTA were not in sync
  - First edition of IEC 61375-2-6 is already released, but some deficiencies were experienced by CONNECTA

- CONNECTA-2 will implement further use cases (e.g. telemetry)
- Experience from implementation and test will be provided to IEC TC9 WG43 for revision of the standard IEC 61375-2-6
- Evolution for co-existence and cooperation with Train to Ground communication of Shift2Rail IP2 (signalling application)

Conclusions

- The standard is a base for interoperable train to ground solutions
- The implementation is a way to verify the feasibility of the standard
- The experience from the implementation and test revealed opportunities to improve the existing standard

QUESTIONS & ANSWERS

Wireless Train Backbone (WLTB)

Igor Lopez, CAF

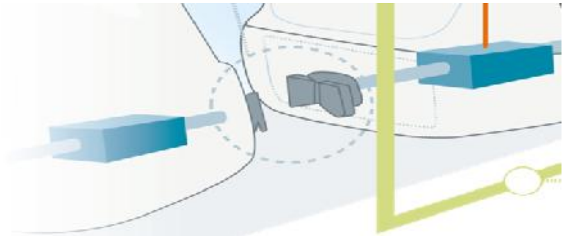
CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

What is WLTB?

- The Wireless Train Backbone (WLTB) is a new train-level network proposed for TCMS.
- WLTB removes the inherent cost of cabling and connectors of traditional wired Train Control networks.
- A reliable and performant wireless TCMS allows the introduction of new functions with relative low cost:
  - Train Integrity function which will help to reduce trackside.
  - Virtual Coupling which supposes a new paradigm in railway operations.

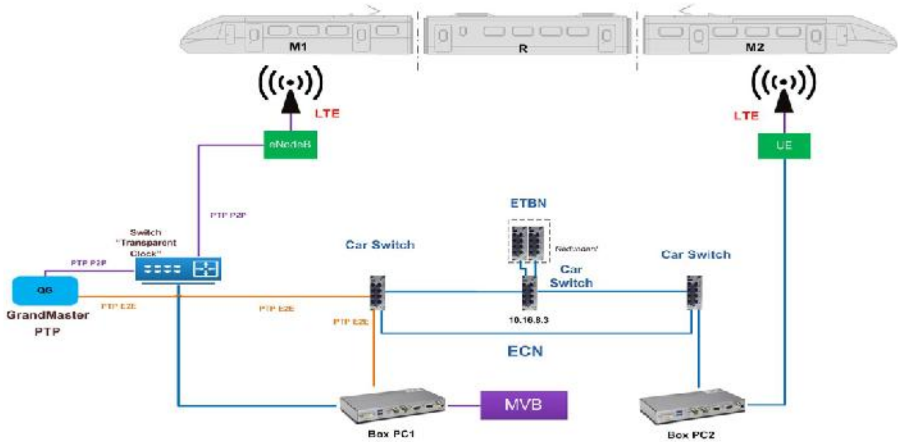
Why WLTB?

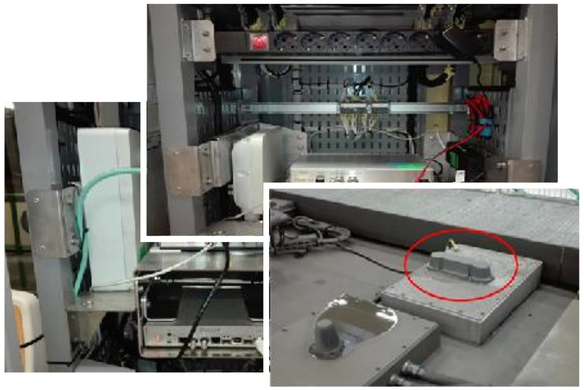
Today	With WLTB
Multiple wired network in a single train, increasing cost and weight.	Removes wires decreasing drastically the associated cost and weight.
Difficult to install new wired networks in existing train units.	Possible to install simply in modernization projects.
Coupling has to be done when consists are stopped and the process takes couple of minutes, reducing the capacity of the infrastructure.	The units are automatically associated to the WLTB and the wireless link is transparent for onboard devices. WLTB allows faster coupling.



WLTB tests in detail

- No couple units in Bilbao’s underground -> Tests from the front to the rear of the same consist.
- To validate the maximum throughput, additional traffic will be injected on the Test Setup network (ECN)





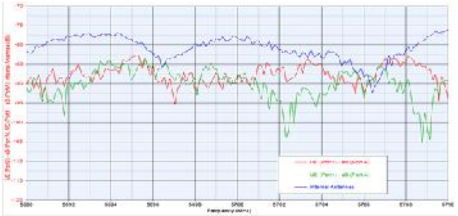
Field Tests Results of WLTB

WLTB Dissemination video

Conclusions (I)

- Depot tests:
  - Theoretical performance: 50Mbps Downlink and 25Mbps Uplink.
  - Tests at 3.2 Mbps have been supported with low FER and latency; not at 256 Mbps.

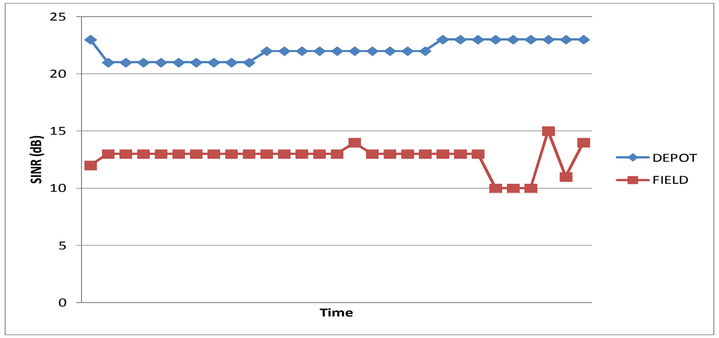
Uplink-downlink configuration	Downlink-to-Uplink Switch-point periodicity	Subframe number									
		0	1	2	3	4	5	6	7	8	9
0	5 ms	D	S	U	U	U	D	S	U	U	U
1	5 ms	D	S	U	U	D	D	S	U	U	D
2	5 ms	D	S	U	D	D	D	S	U	D	D
3	10 ms	D	S	U	U	U	D	D	D	D	D
4	10 ms	D	S	U	U	D	D	D	D	D	D
5	10 ms	D	S	U	D	D	D	D	D	D	D
6	5 ms	D	S	U	U	U	D	S	U	U	D

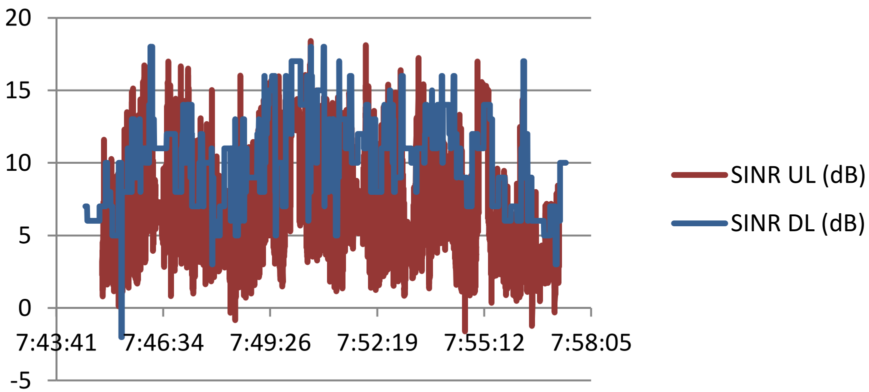


freq.	UE	Losses (dB)
5.8 GHz	Cable LTE 1	7,5
5.8 GHz	Cable LTE 2	7,3
freq.	eNodeB	Losses (dB)
5.8 GHz	Cable LTE 1	8,6
5.8 GHz	Cable LTE 2	8,5

Conclusions (II)

- *Field Tests:*
  - Much better performance in the DL than in the UL:
    - UL uses a single-carrier modulation, which is less robust against multipath and Doppler effects.
    - UL is also based on 1x2 MIMO, while DL is based on 2x2 MIMO and multicarrier modulation.



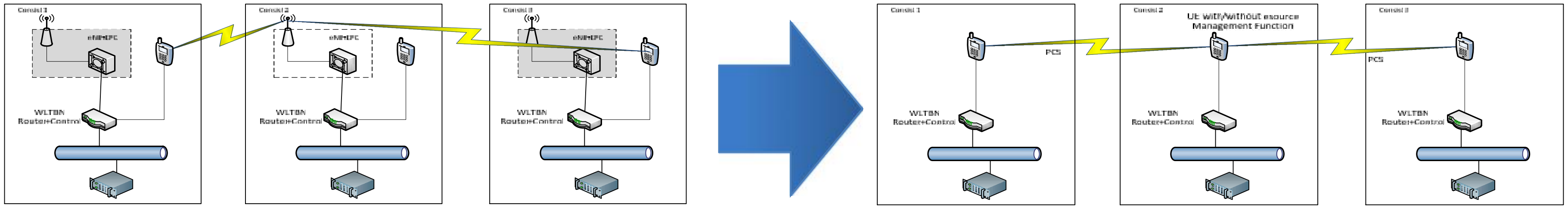


Conclusions (III)

- General conclusions:
  - Current architecture is complex and expensive: 1 eNB+EPC per consist.
  - Up to 100 Mbps throughput can only be achieved with broader bandwidth: difficulties to obtain such big frequency reservation.
  - High effect of environment, need for more directive communications, pay special attention in the installation phase (RF cabling, antenna positions, etc).

Next station is

- Evolve to PC5-based communications: 1UE per consist instead of eNB+EPC+EU.
- Evaluate the division of C2C communications in 2 networks:
  - TCMS->Cellular-based communications. High reliability, low latency, low throughput needs.
  - OMTS->802.11-based communications. Best effort traffic, high throughput needs.
- Evaluation of a Safe Wireless Inauguration.
- Apply MIMO and higher transmission power (below the legal limits) to improve the SNR.
- Adapt the SDTv4 (Safety Layer) for wireless channel (e.g. apply EN50159)
- Standardization activities:
  - Propose WLTB Use Case in ETSI/3GPP to be adopted by upcoming releases
  - IEC 61375-2-7



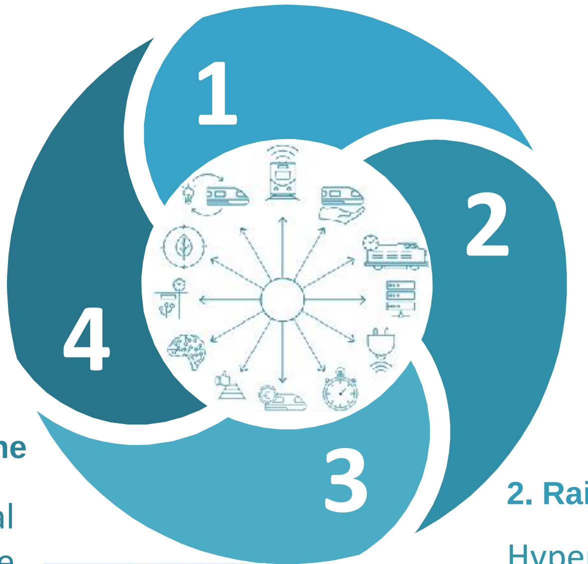
QUESTIONS & ANSWERS

Revisiting Innotrans Demonstrator

Javier Goikoetxea (CAF)

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

Motivation

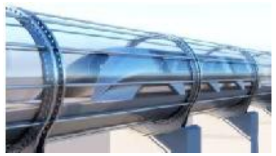


1. Other transport means are becoming more appealing

Electric/hybrid cars and buses, cleaner airplanes, electric bikes and personal mobile devices

2. Rail is old fashioned

Hyperloop effect, new mobility concepts like car sharing or truck platooning



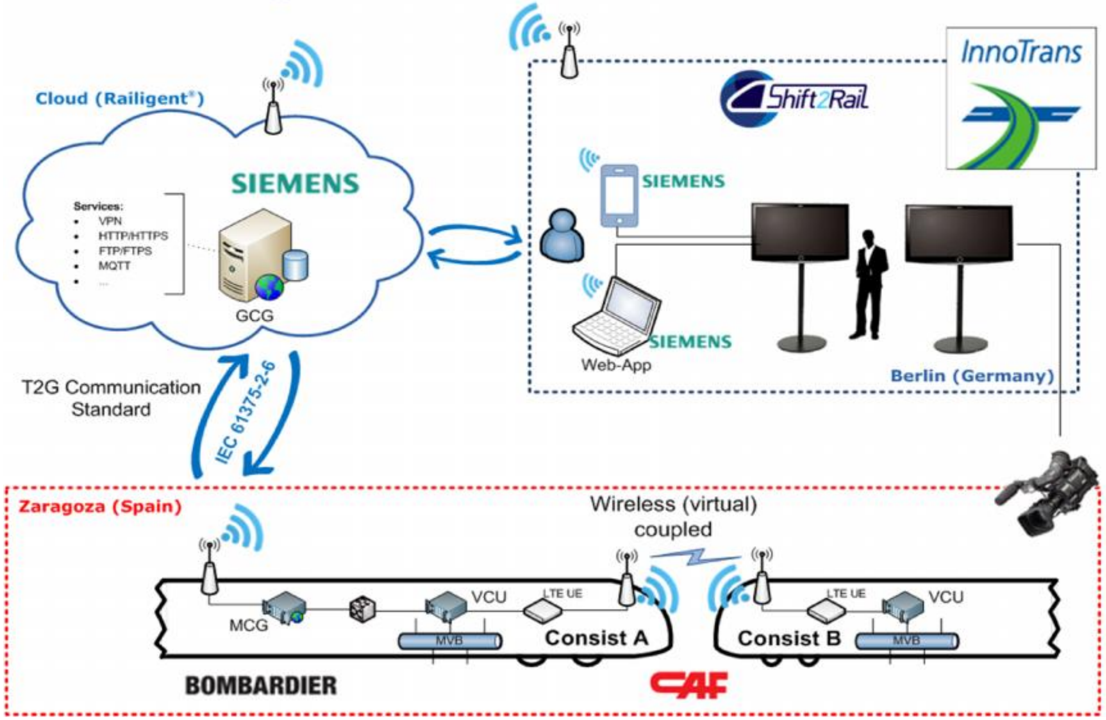
3. Railway to remain as backbone

Fully integrated in the intermodal transport system, and key player of the mobility-as-a-service paradigm. New operational concepts are required.

4. Railways must be connected and digitalised

New technologies in the fields of communications and computing must be deployed. New functions are required. TCMS is one of the key the future.

General Layout of Connected Trams



Video
CONNECTED TRAMS in action

Conclusions

1. **Key building blocks showcased**

   Connectivity, automation, computing techniques, digital services

2. **First results only after 2 years of S2R**

   WLTB, Virtual Coupling, FDF, T2G, Digital Services

3. **New functions**

   The railway ecosystem is getting ready to integrate new functions like the virtual coupling

4. **TCMS as key role for the future**

   Providing new set of communication and computing services to host new functions

5. **Shift2Rail**

   S2R is the right instrument to foster innovation and shorten time-to-market through collaboration

6. **Collaboration**

   Connected Trams' success relies on the smooth collaboration between partners still competitors.

QUESTIONS & ANSWERS

Wrap-up and Closing

Javier Goikoetxea (CAF)
Arjan Geven (TTTech)

CONNECTA has received funding from the European Union's Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme.

The partners of both CONNECTA & Safe4RAIL would like to thank you for attending this Final Conference we have prepared with passion

Shift2Rail Joint Undertaking
White Atrium Building, 2nd Floor
Avenue de la Toison d'Or 56-60,
B-1060 Brussels

www.shift2rail.org
www.s2r-connecta.eu
www.safe4rail.eu

CONNECTA & Safe4RAIL have received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme, with agreements No: 730539 and No: 730830., respectively.

For further information please contact:

Coordinator of CONNECTA:
CAF
Javier Goikoetxea:
connecta@caf.net

Coordinator of Safe4RAIL:
TTTech Computertechnik AG
Arjan Geven:
arjan.geven@tttech.com