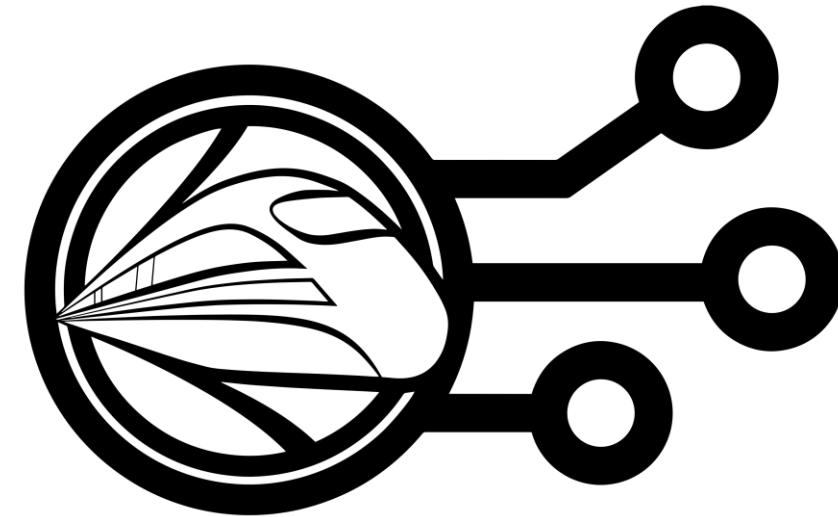




SBB CFF FFS



# OCORA

## Technical Slide Deck

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

## Logical Architecture

- Actors and External Interfaces
- Components and Internal Interfaces
- Automatic Train Protection On-Board (ATP-OB)
- Localisation On-Board (LOC-OB)
- Functional Vehicle Adapter (FVA)
- Envisioned Software Building Blocks (tentative)

## Physical Architecture

- Final View
- Transition View
- Actors, External Interfaces
- Components, Internal Interfaces
- Envisioned Hardware Building Blocks (tentative)

## Train Integration Scenarios / Network Topology / Integration

- **Scenario A: NG-TCN Train**  
CCN physically separated
- **Scenario B: NG-TCN Train**  
Common train network – CCN logically separated
- **Scenario C: NG-TCN Train**  
Common train network – common critical control network logically separated
- **Scenario D: NG-TCN Train**  
Common train network – common critical control network physically separated
- **Legacy Train**

## Computing Platform

- High-Level Architecture
- Deployment Options

## Functional Vehicle Adapter

### Modular Safety

### Security

### Methodology & Tooling

### Operational Concept

### Supporting Slides

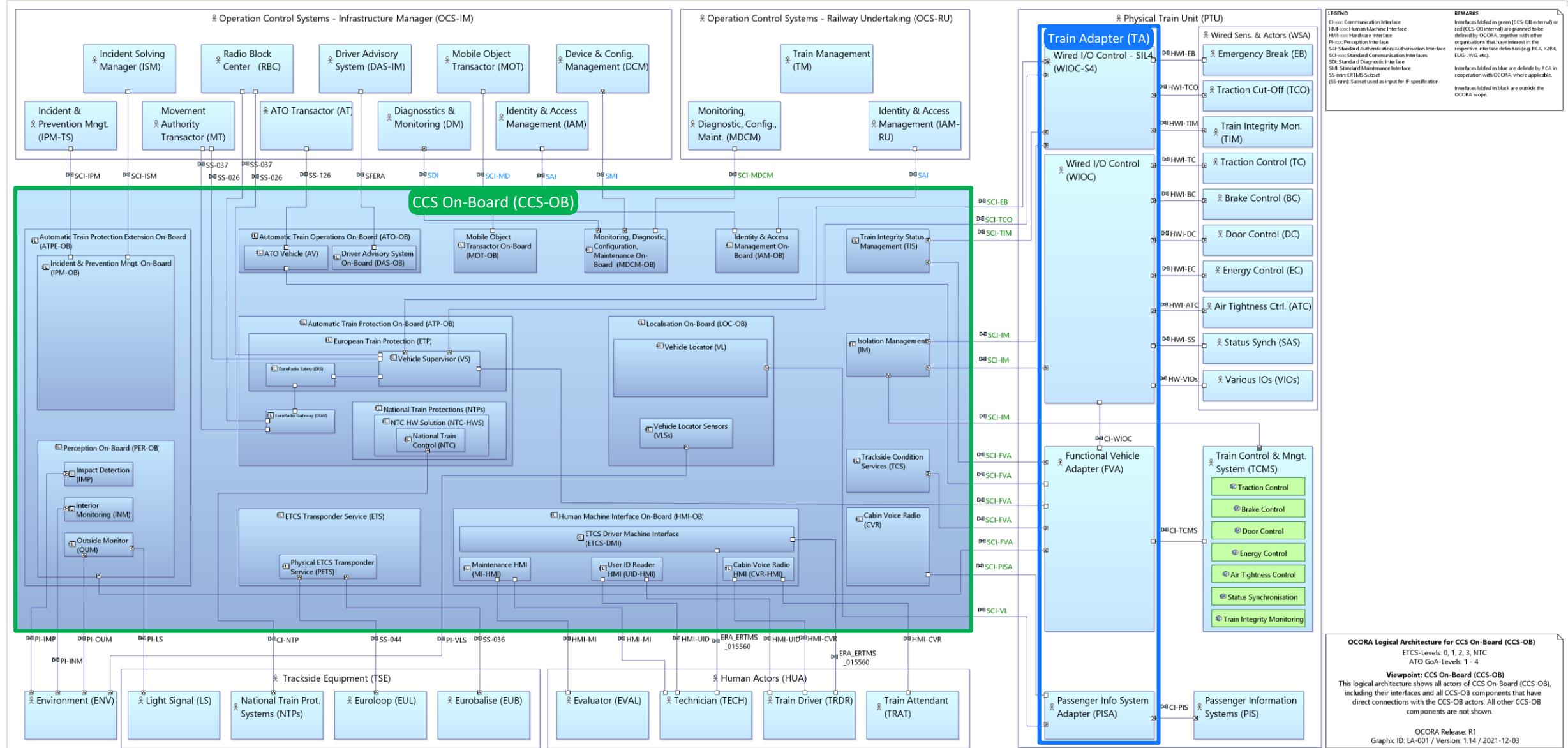




# Logical Architecture

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

# CCS On-Board (CCS-OB) Actors and External IFs (only CCS-OB components with external IFs shown)



OCORA Logical Architecture for CCS On-Board (CCS-OB)

ETCS-Levels: 0, 1, 2, 3, NTC

ATO GoA-Levels: 1 - 4

Viewpoint: CCS On-Board (CCS-OB)

This logical architecture shows all actors of CCS On-Board (CCS-OB), including their interfaces and all CCS-OB components that have direct connections with the CCS-OB actors. All other CCS-OB components are not shown.

Graphic Release: R1

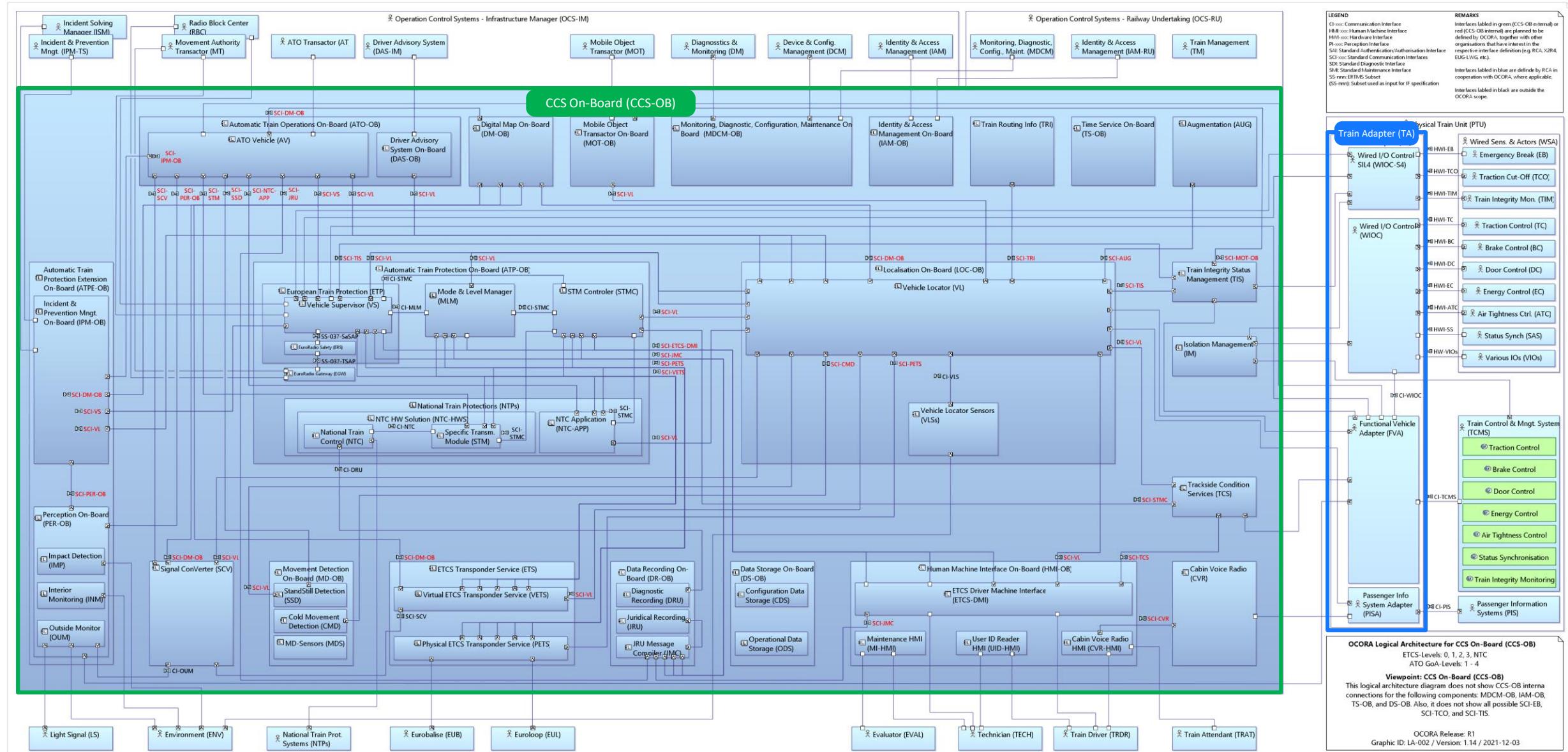
Graphic ID: LA-001 / Version: 1.14 / 2021-12-03



OCORA

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

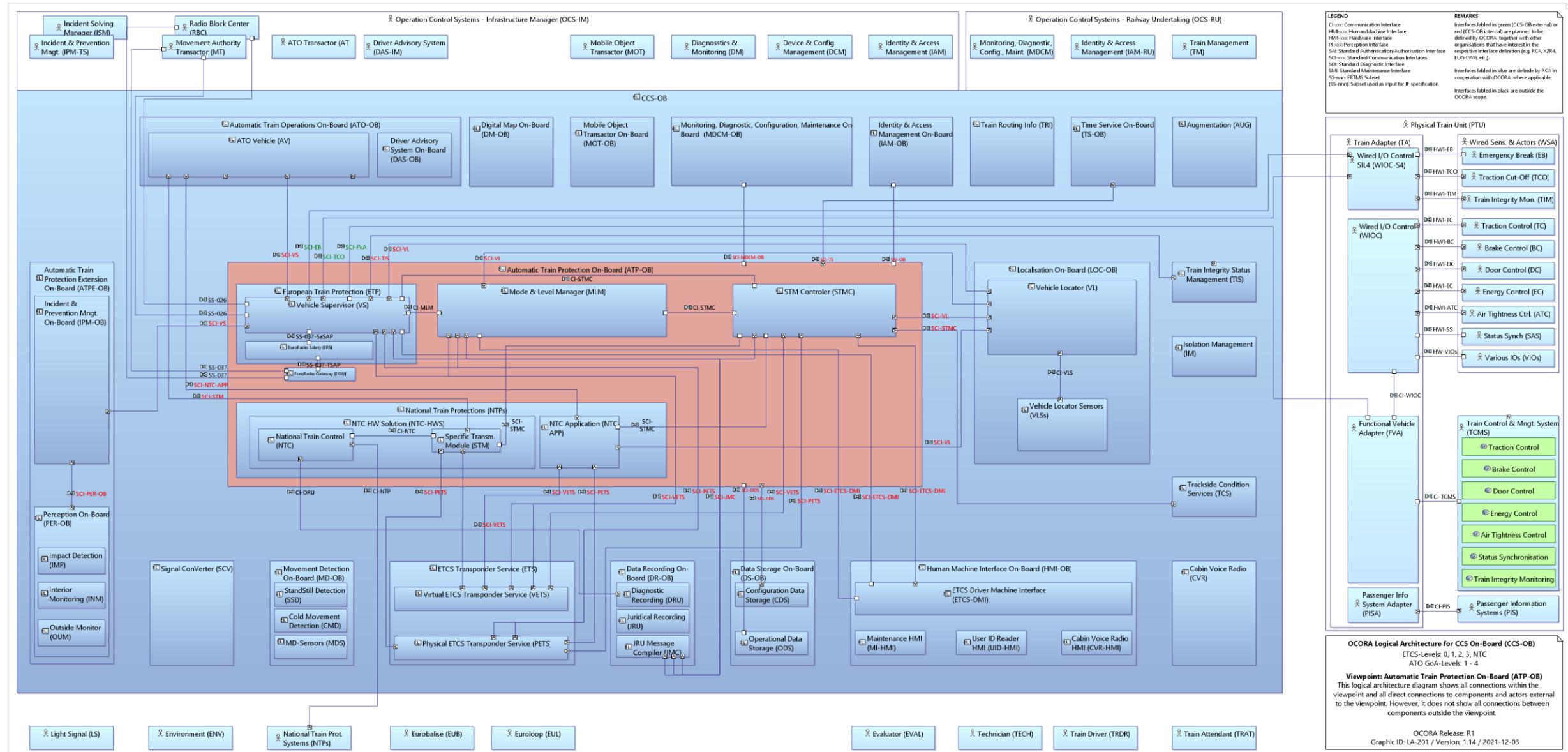
# CCS On-Board (CCS-OB) Components and Internal IFs



OCORA

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

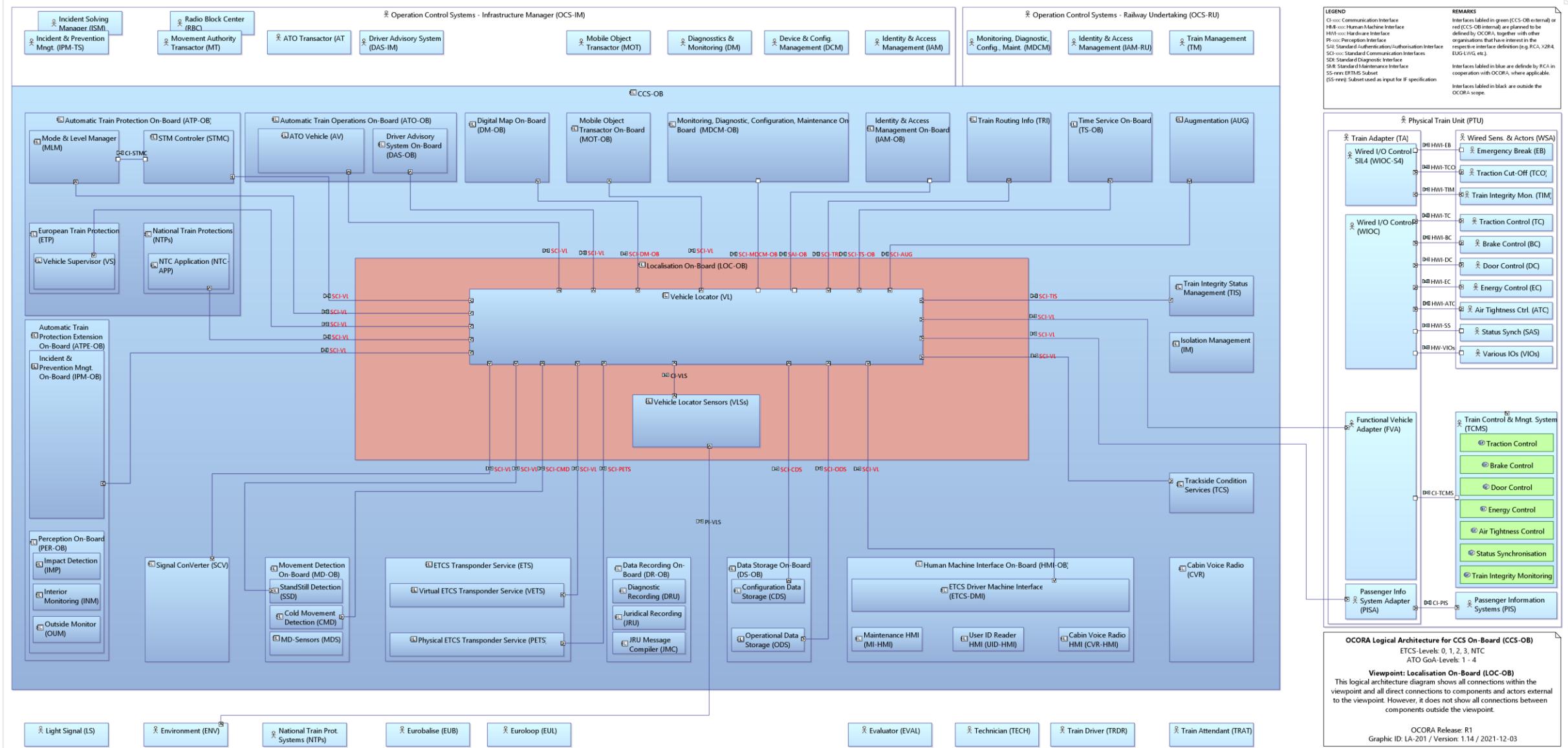
Automatic Train Protection On-Board (ATP-OB) Actors and External IFs



# Localisation On-Board (LOC-OB) Actors and External IFs



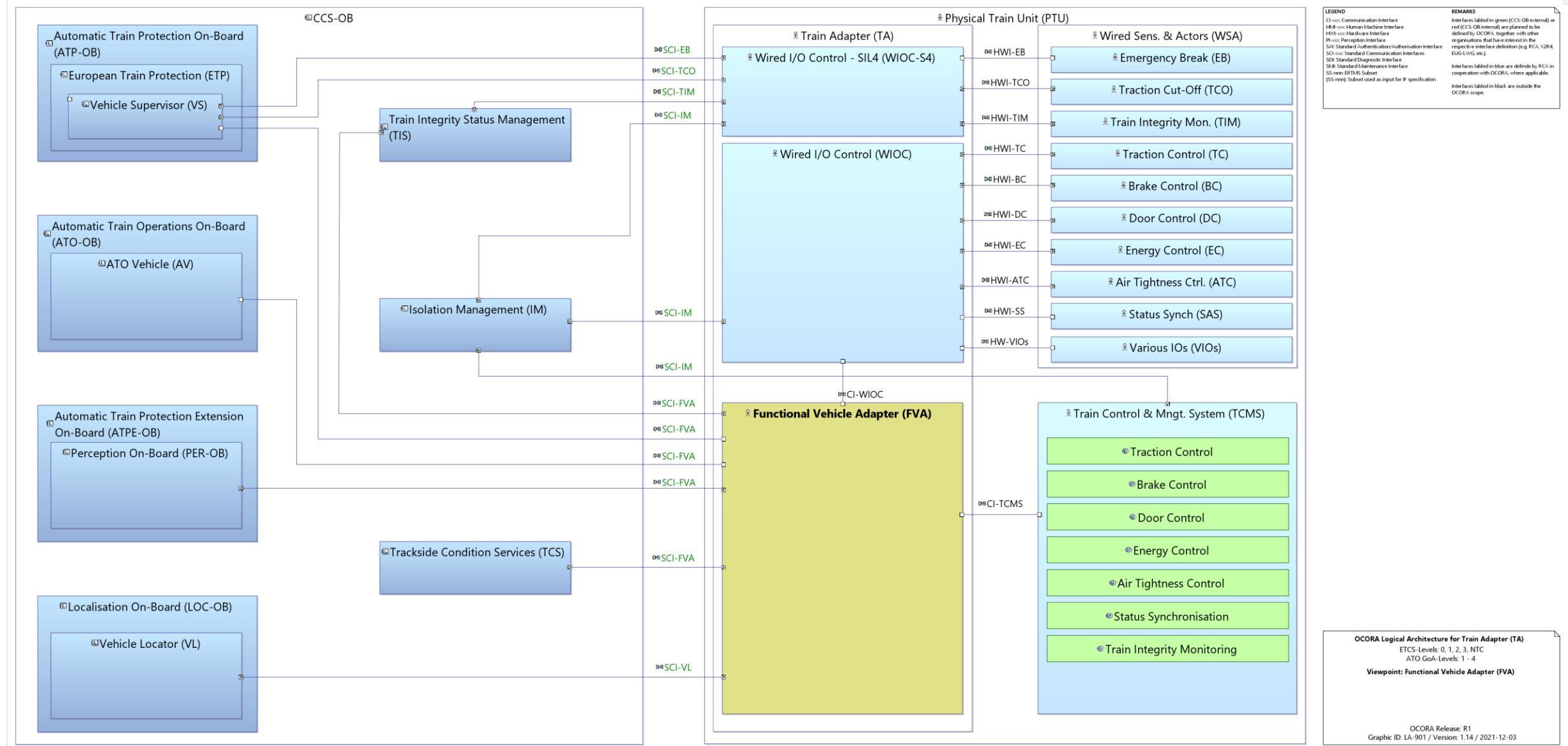
 SBB CFF FFS



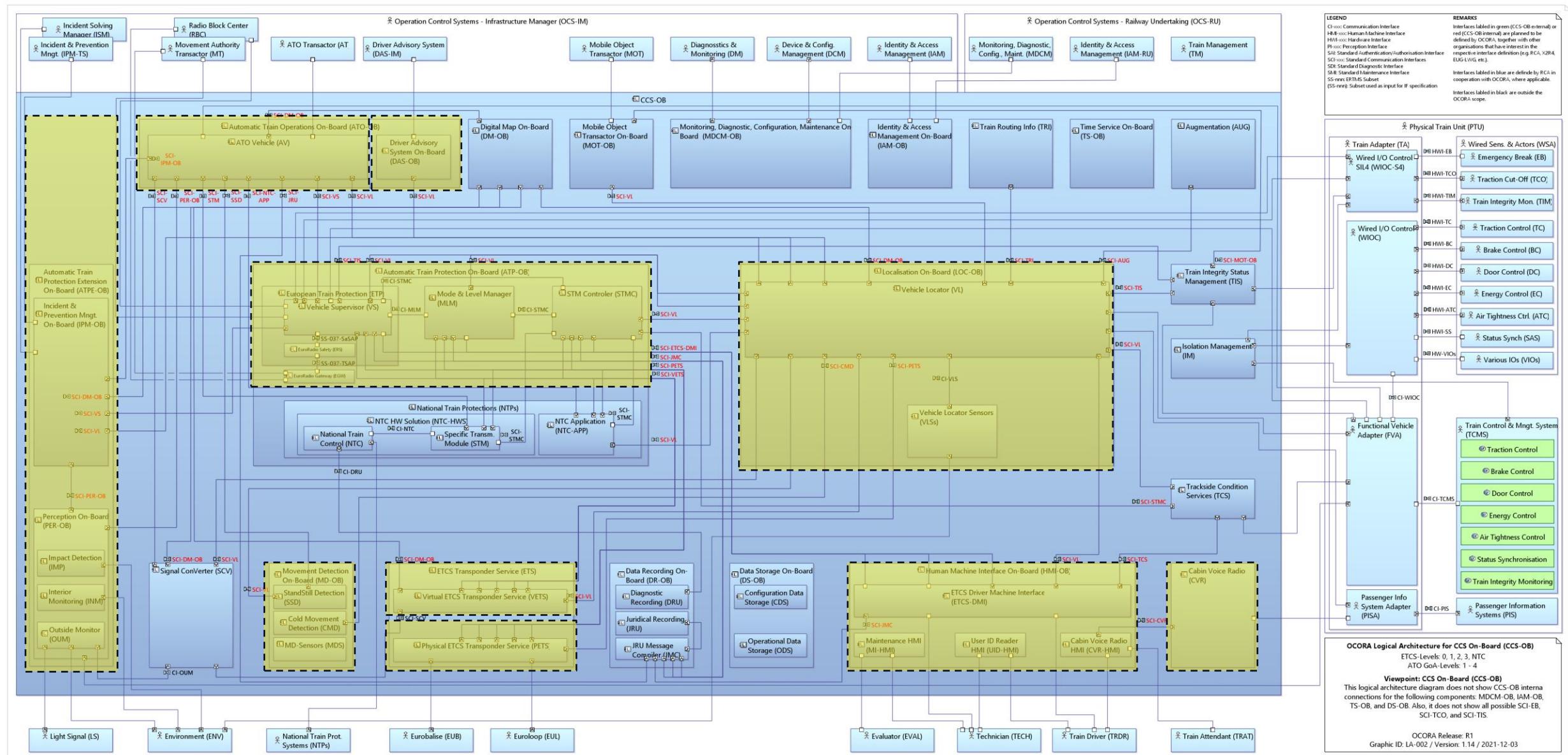
OCORA

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

Functional Vehicle Adapter (FVA) Actors and External IFs



# OCORA envisioned software building blocks (tentative)

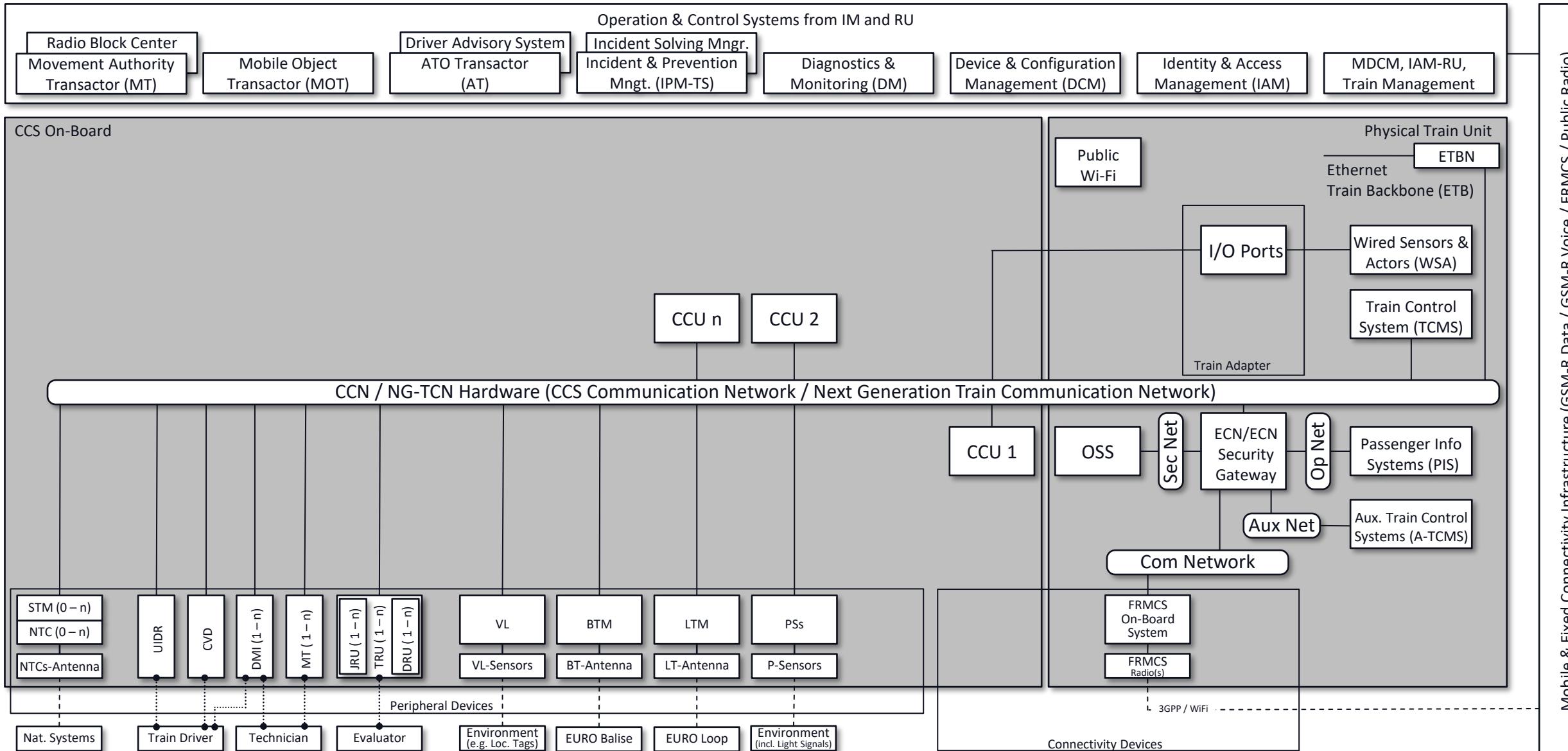




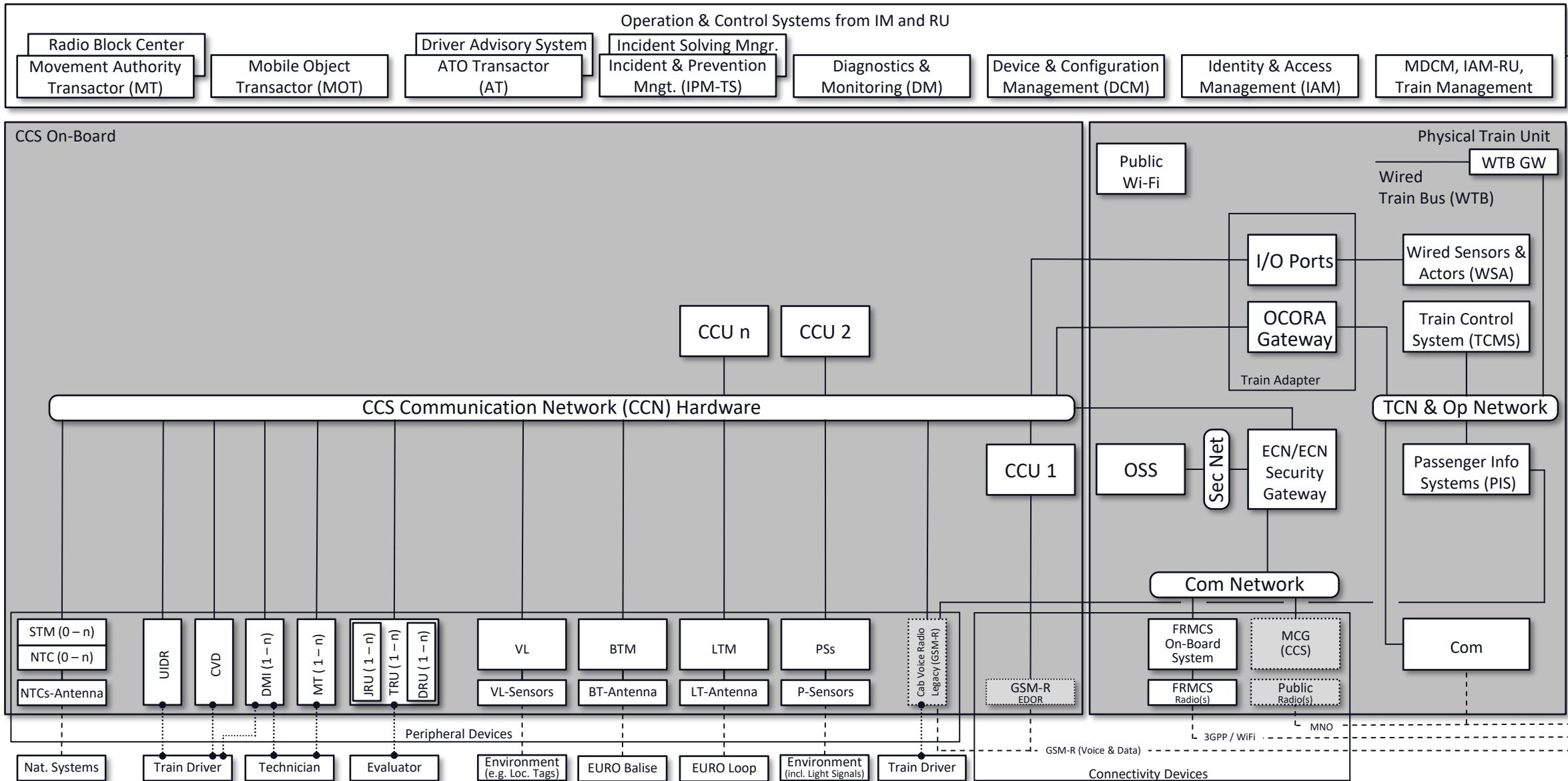
# Physical Architecture

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

# Physical Architecture – FINAL VIEW



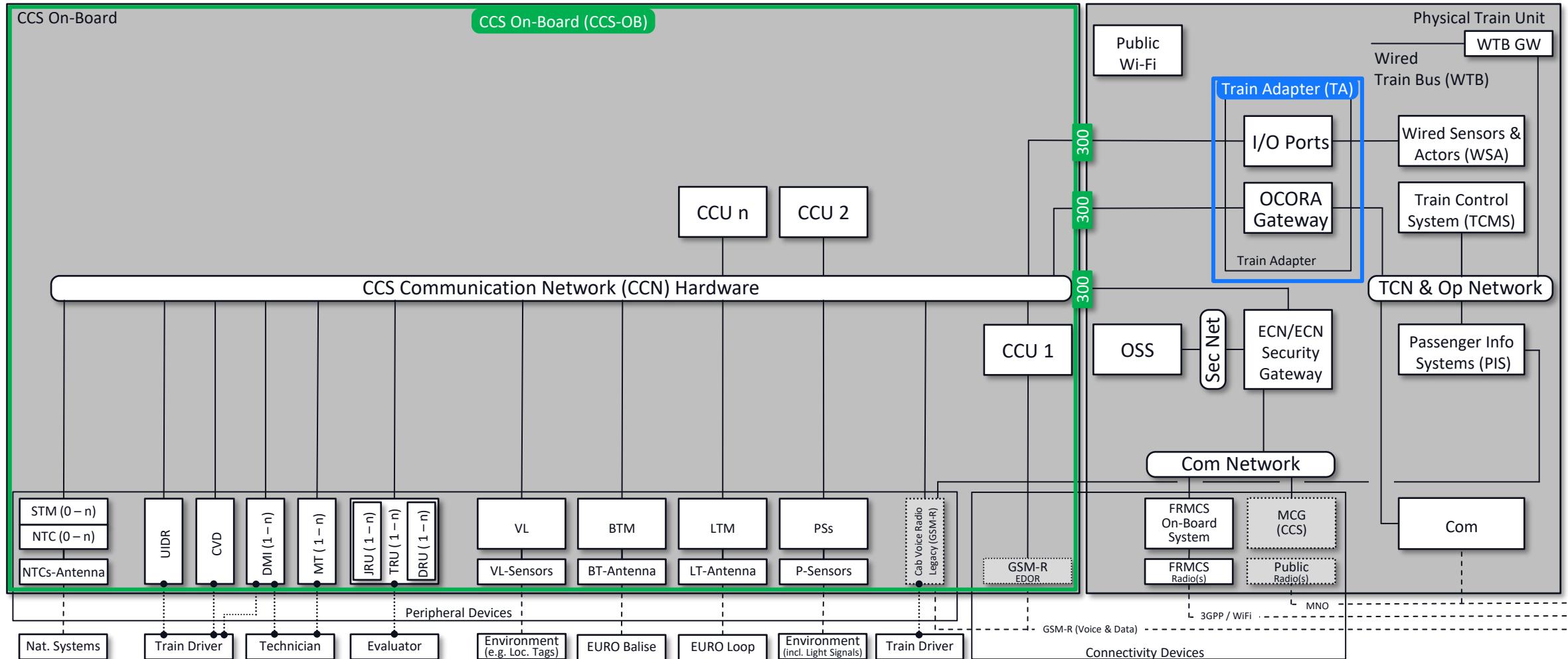
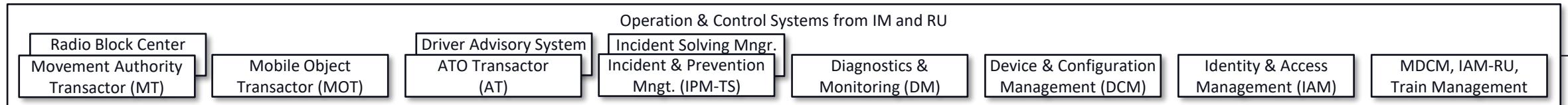
# Physical Architecture – TRANSITION VIEW



# CCS On-Board (CCS-OB) and Train Adapter (TA)



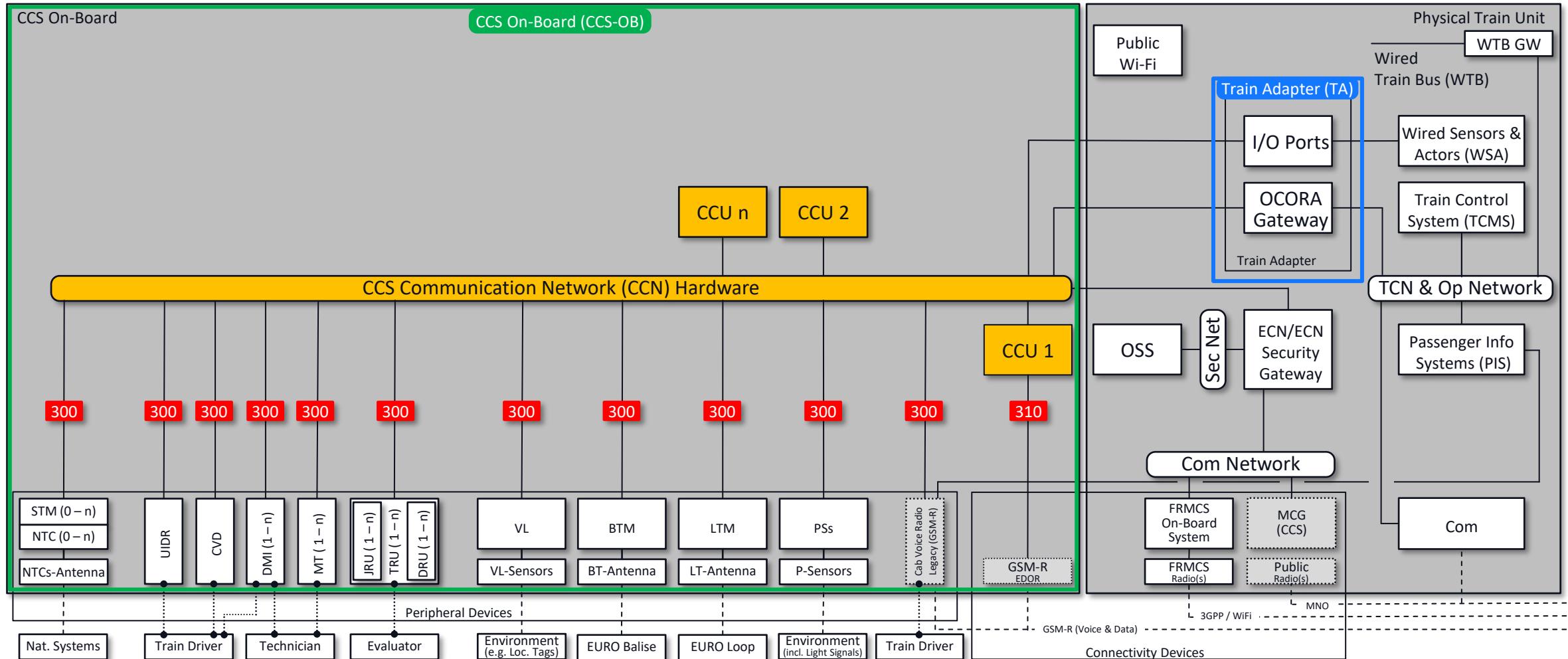
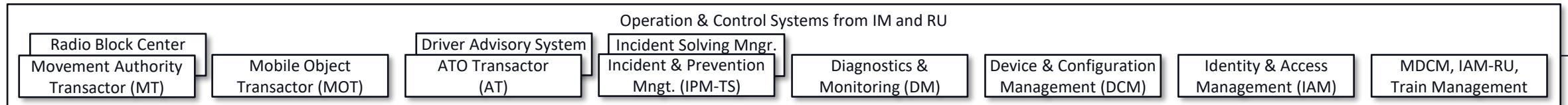
Actors and External IFs



# CCS On-Board (CCS-OB) and Train Adapter (TA)

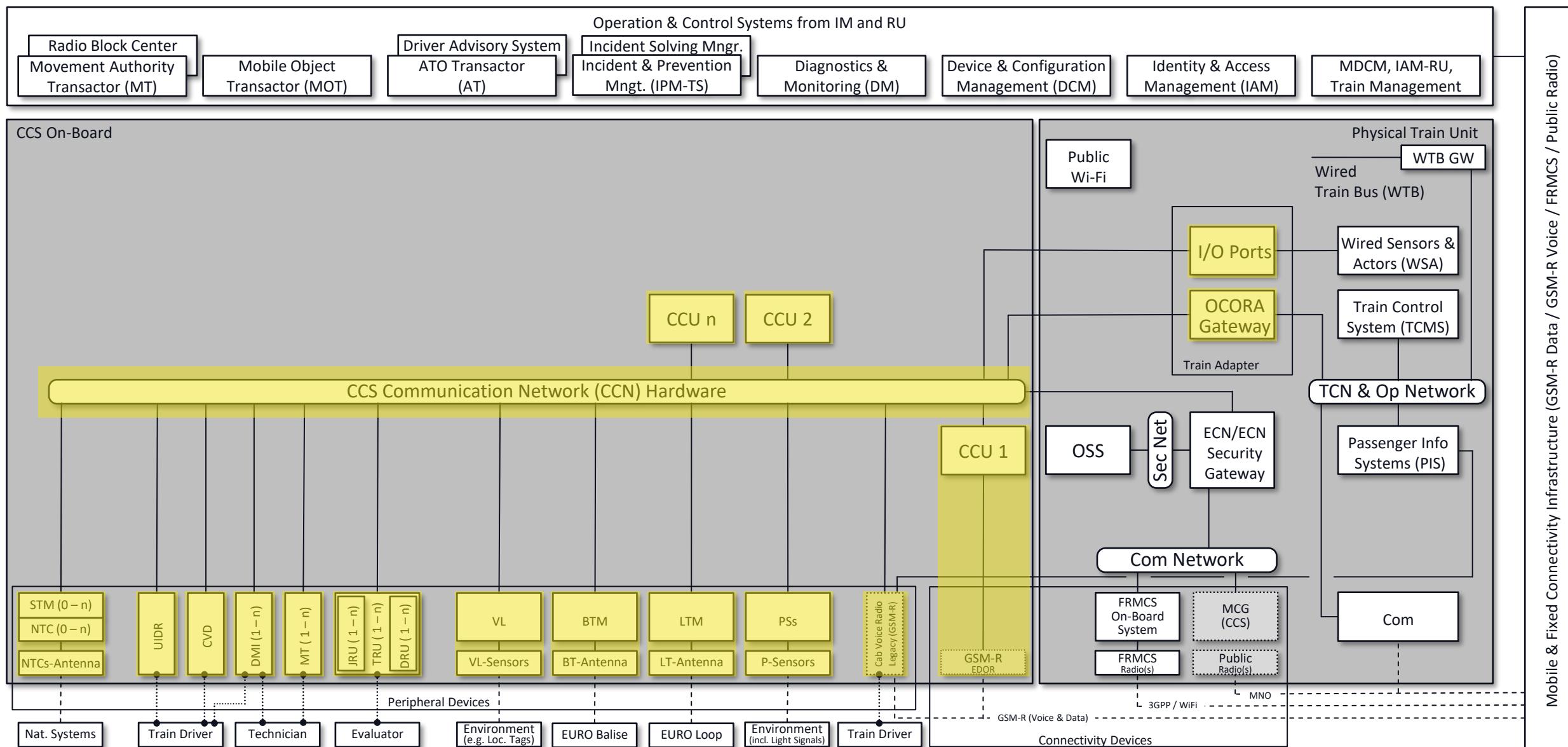


Components and Internal IFs



Mobile & Fixed Connectivity Infrastructure (GSM-R Data / GSM-R Voice / FRMCS / Public Radio)

# OCORA envisioned hardware building blocks (tentative)



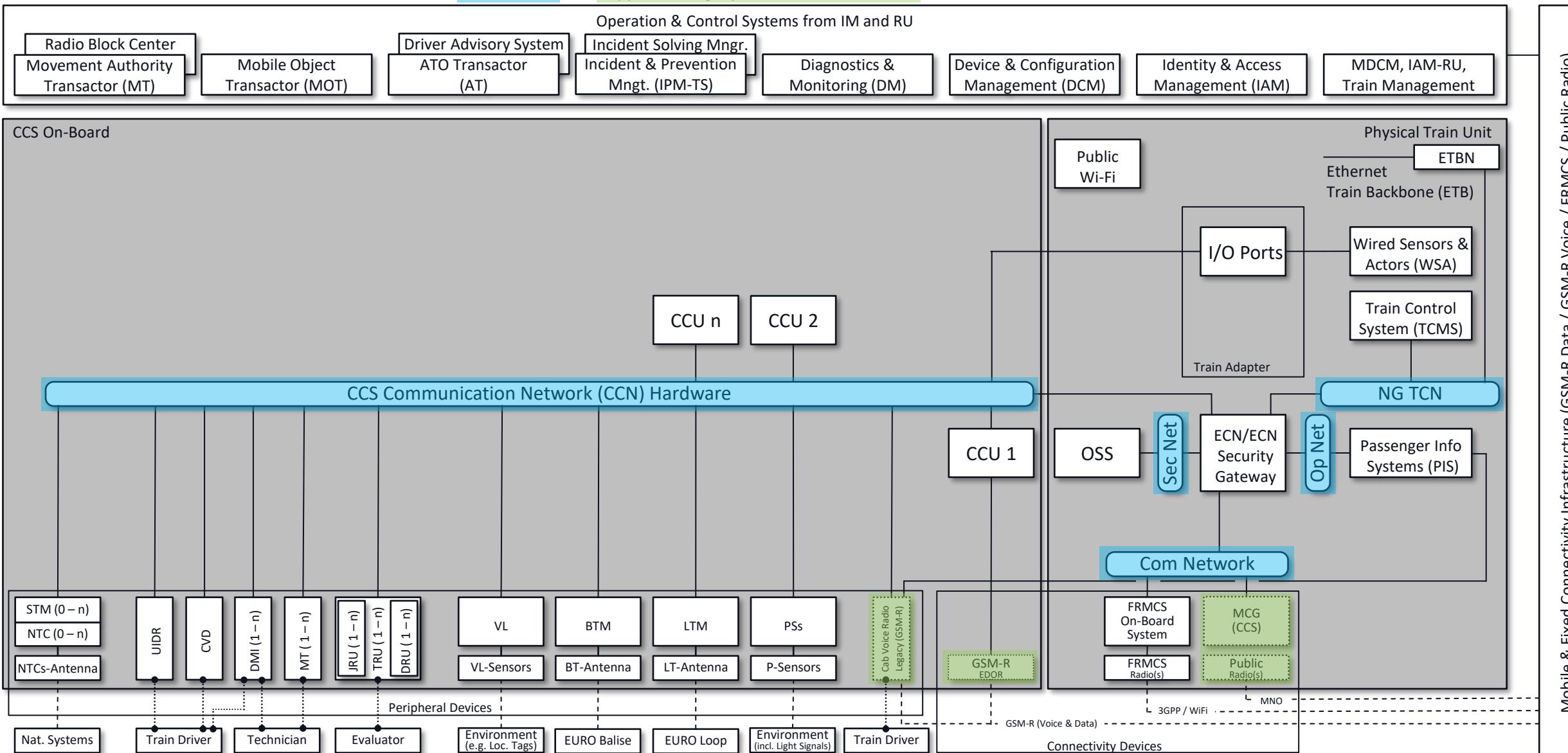


# Train Integration Scenarios

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

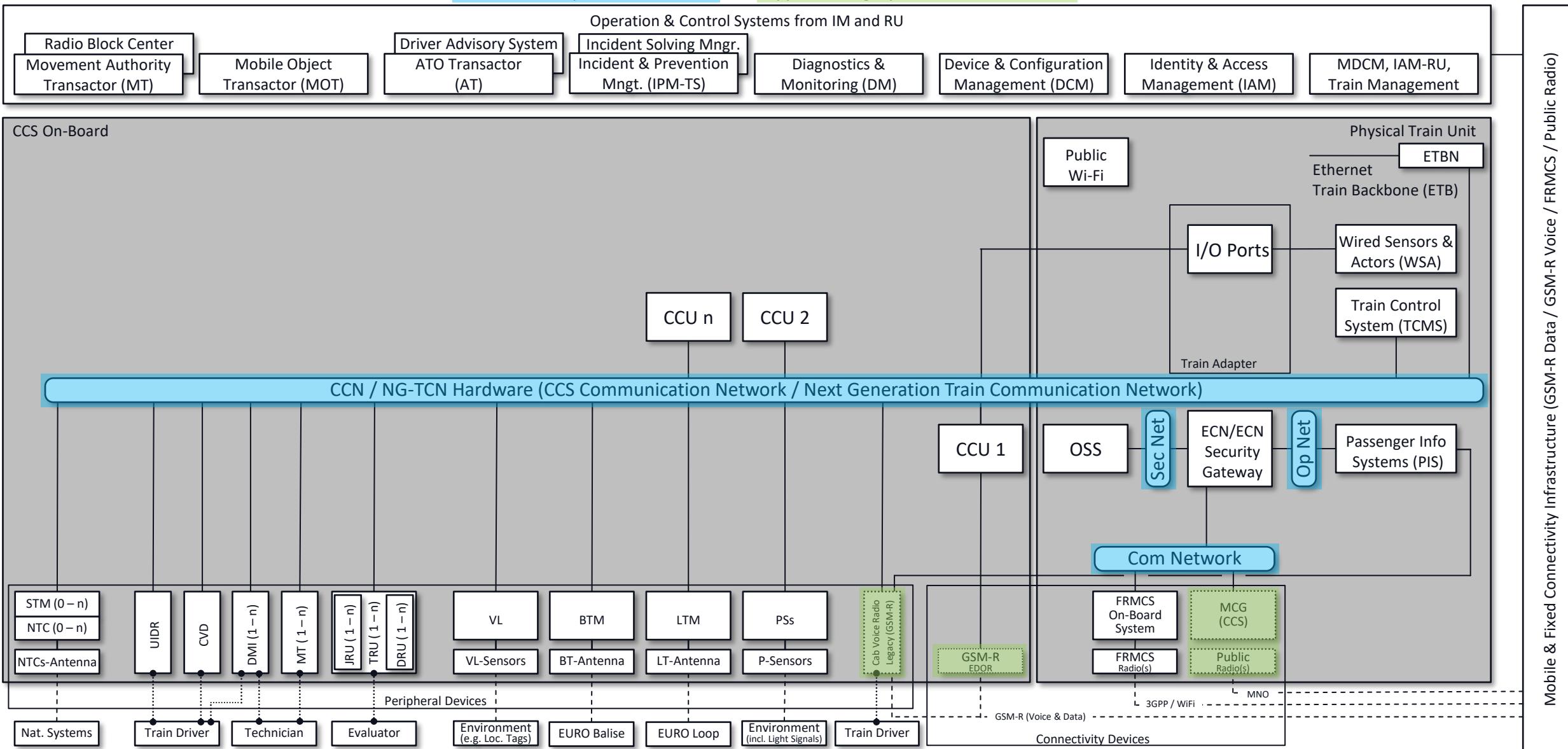
# NG-TCN Train – Scenario A

(CCN as physically separated network from Sec Net, Op Net, NG TCN and Com Net with support for legacy trackside infrastructure)



# NG-TCN Train – Scenario B

(CCN as logically separated network from NG TCN and logically separated from Sec Net, Op Net and Com Net with support for legacy trackside infrastructure)



# NG-TCN Train – Scenario C

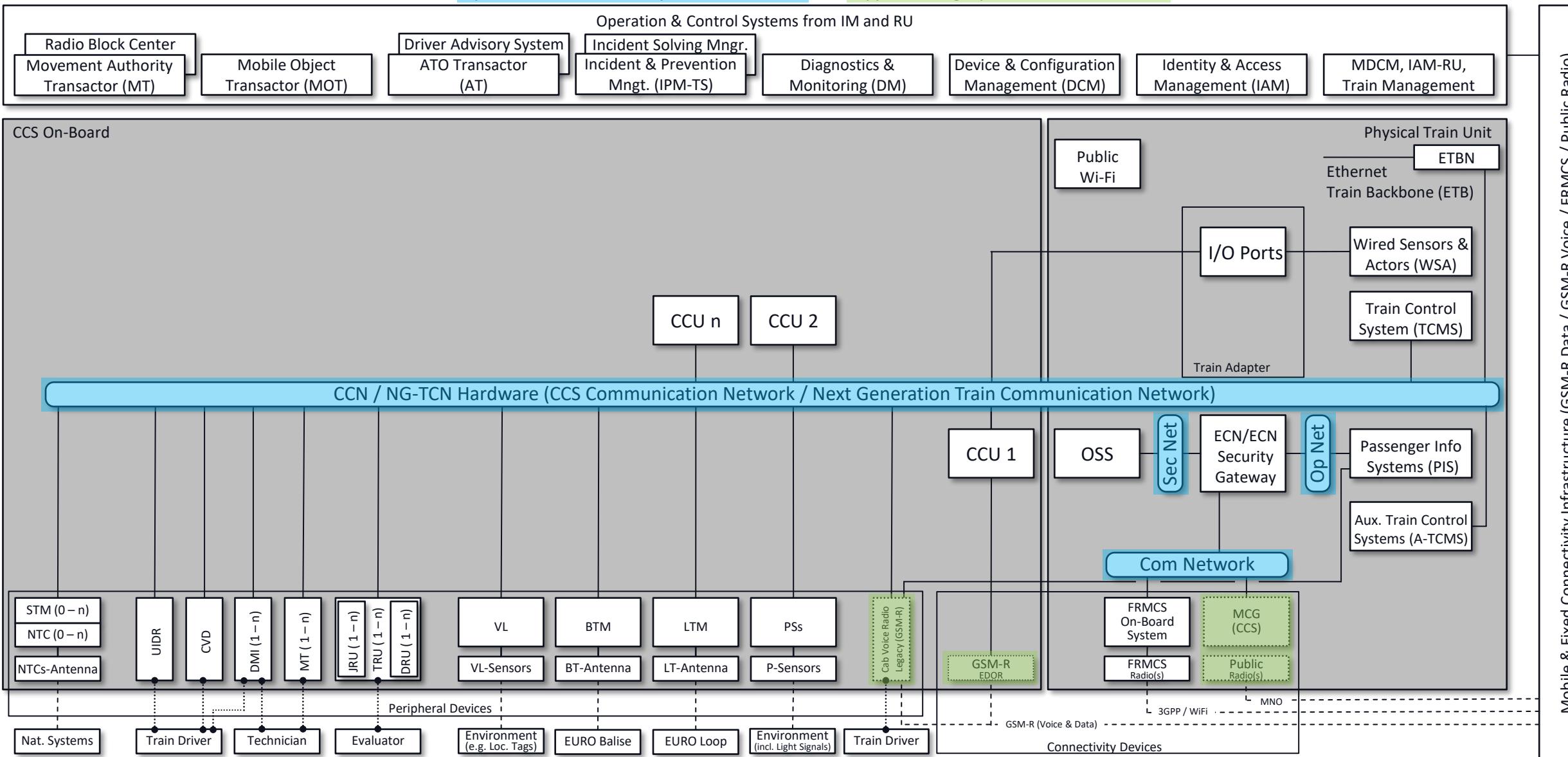
(Common CCN and TCMS network logically separated from A-TCMS and physically separated from Sec Net, Op Net and Com Net with support for legacy trackside infrastructure)



SBB CFF FFS

ÖBB

DB

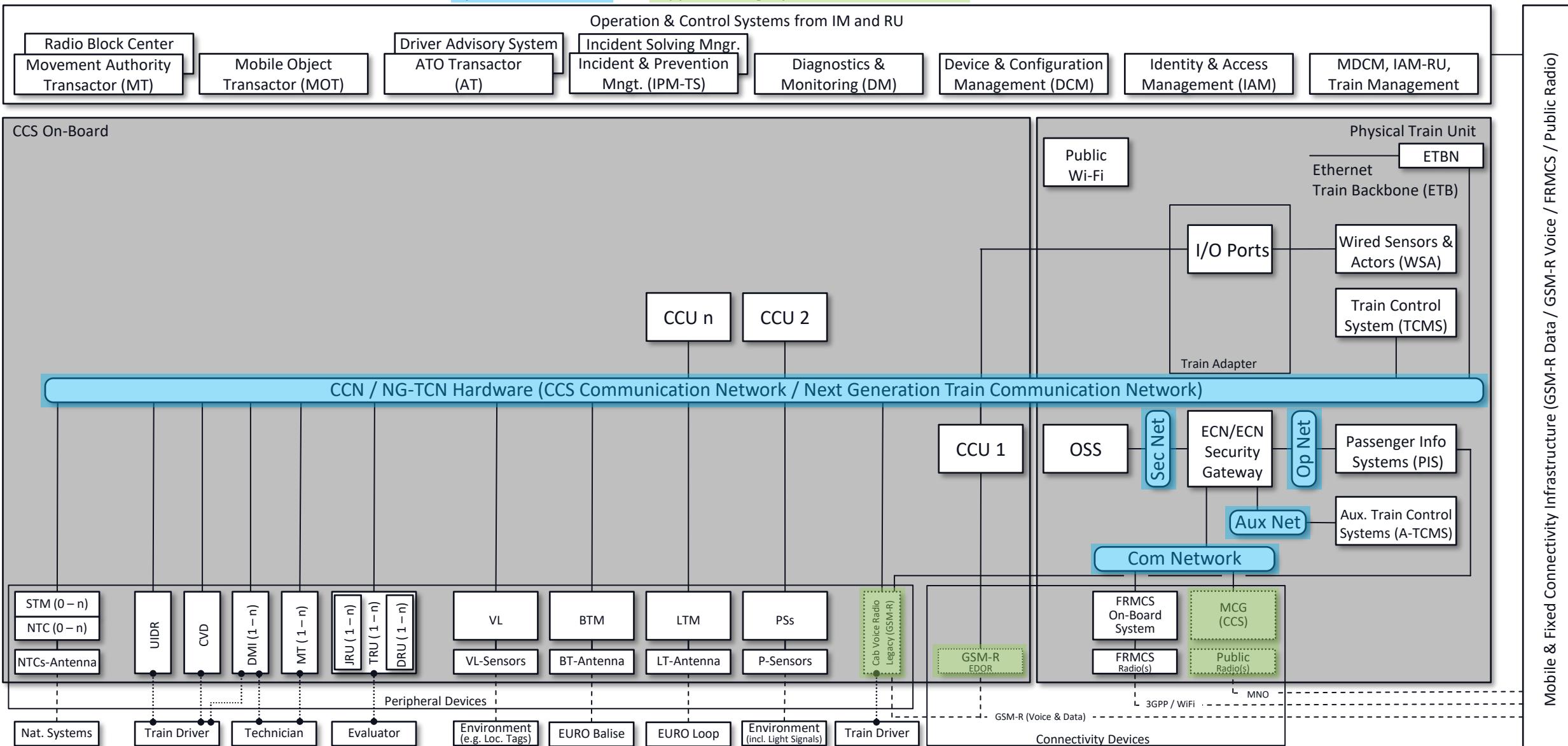


OCORA

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

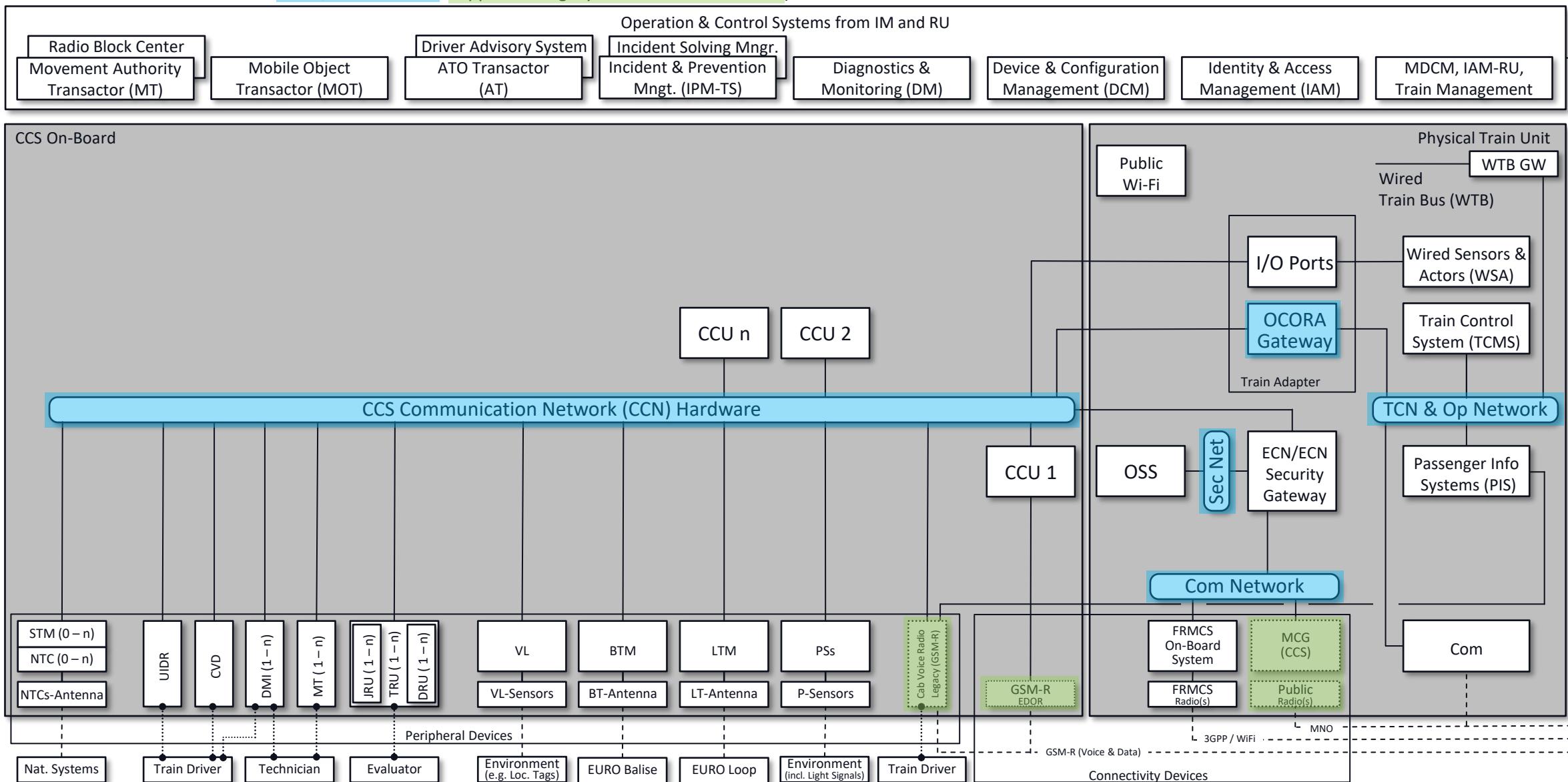
# NG-TCN Train – Scenario D

(Common CCN and TCMS network physically separated from A-TCMS, Sec Net, Op Net and Com Net with support for legacy trackside infrastructure)



# Legacy Train

(CCN physically separated from Sec Net and Com Net using the OCORA GW connecting to the TCMS / PIS Networks. Support for legacy trackside infrastructure)



OCORA

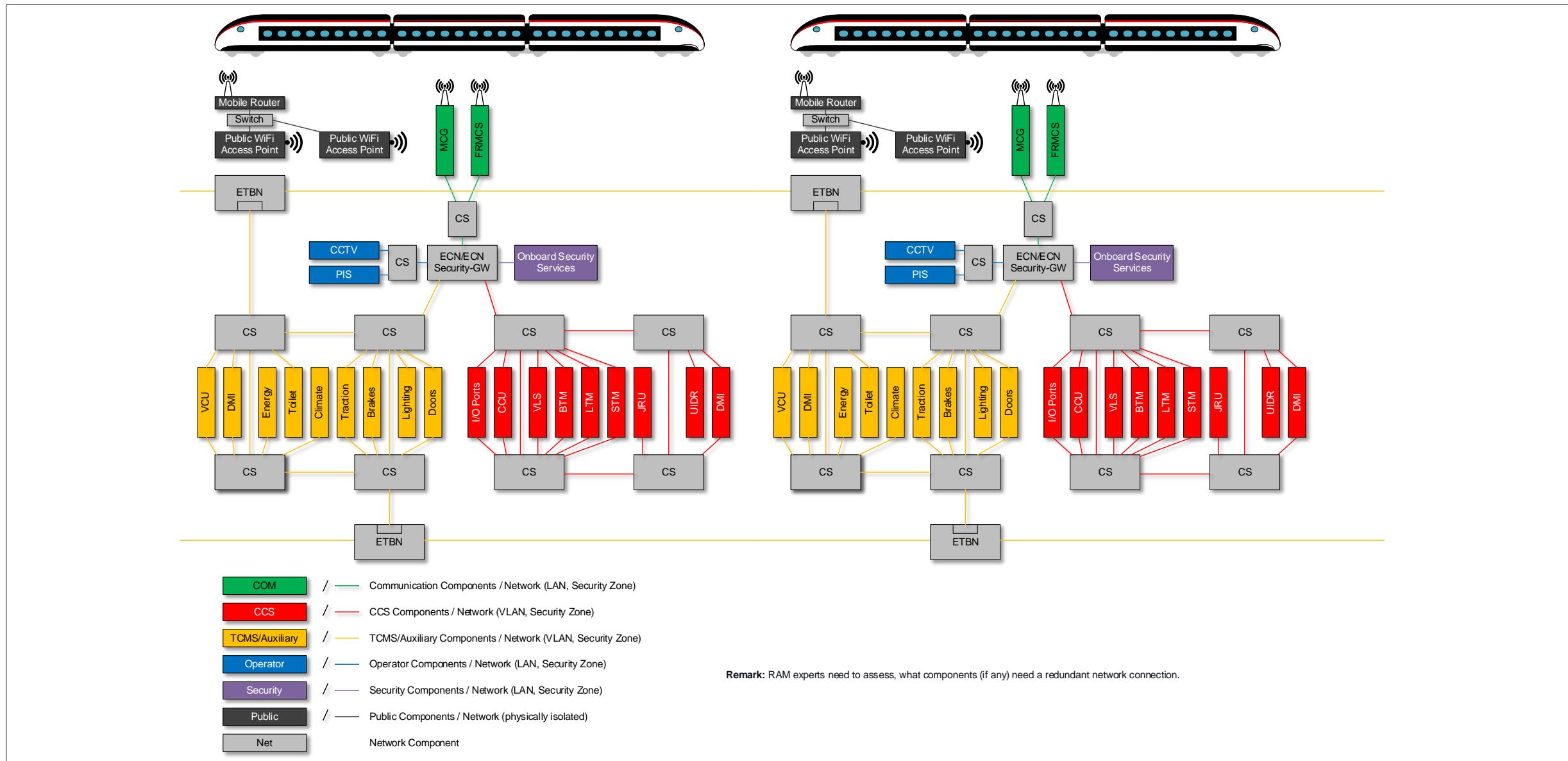
OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1



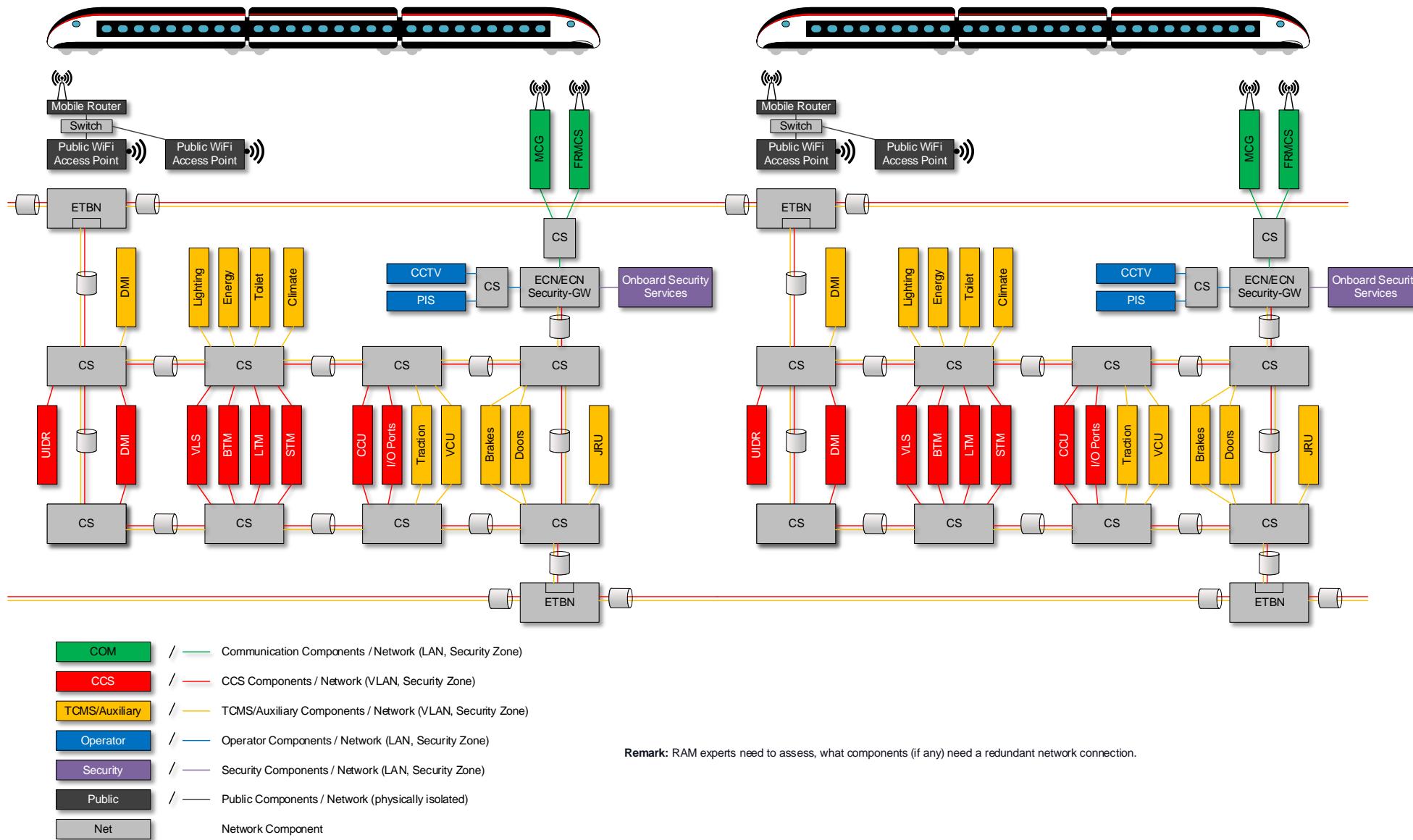
# Network Topology Scenarios

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

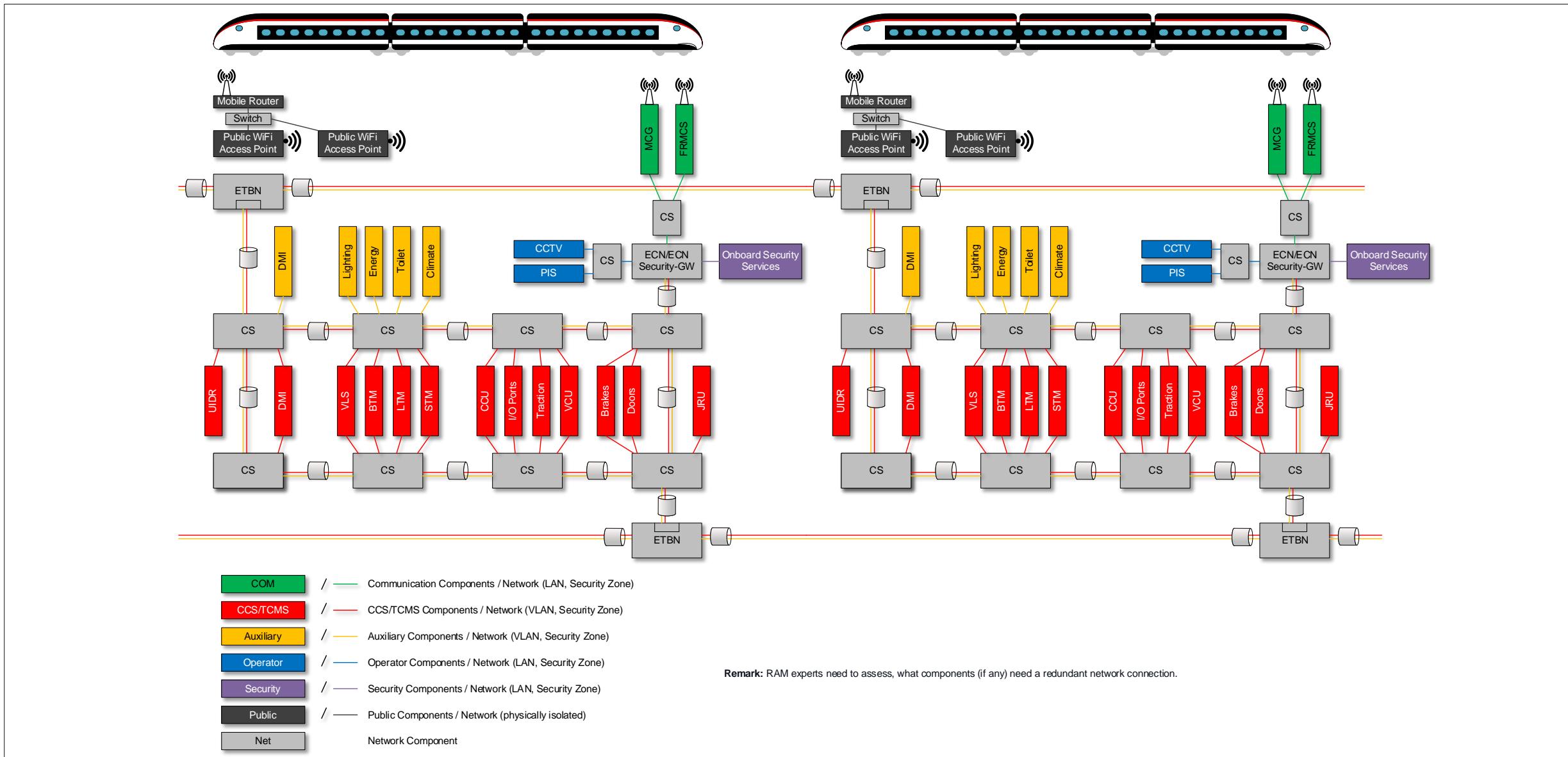
# Scenario A: CCN as physically separated network



# Scenario B: CCN as logically separated network



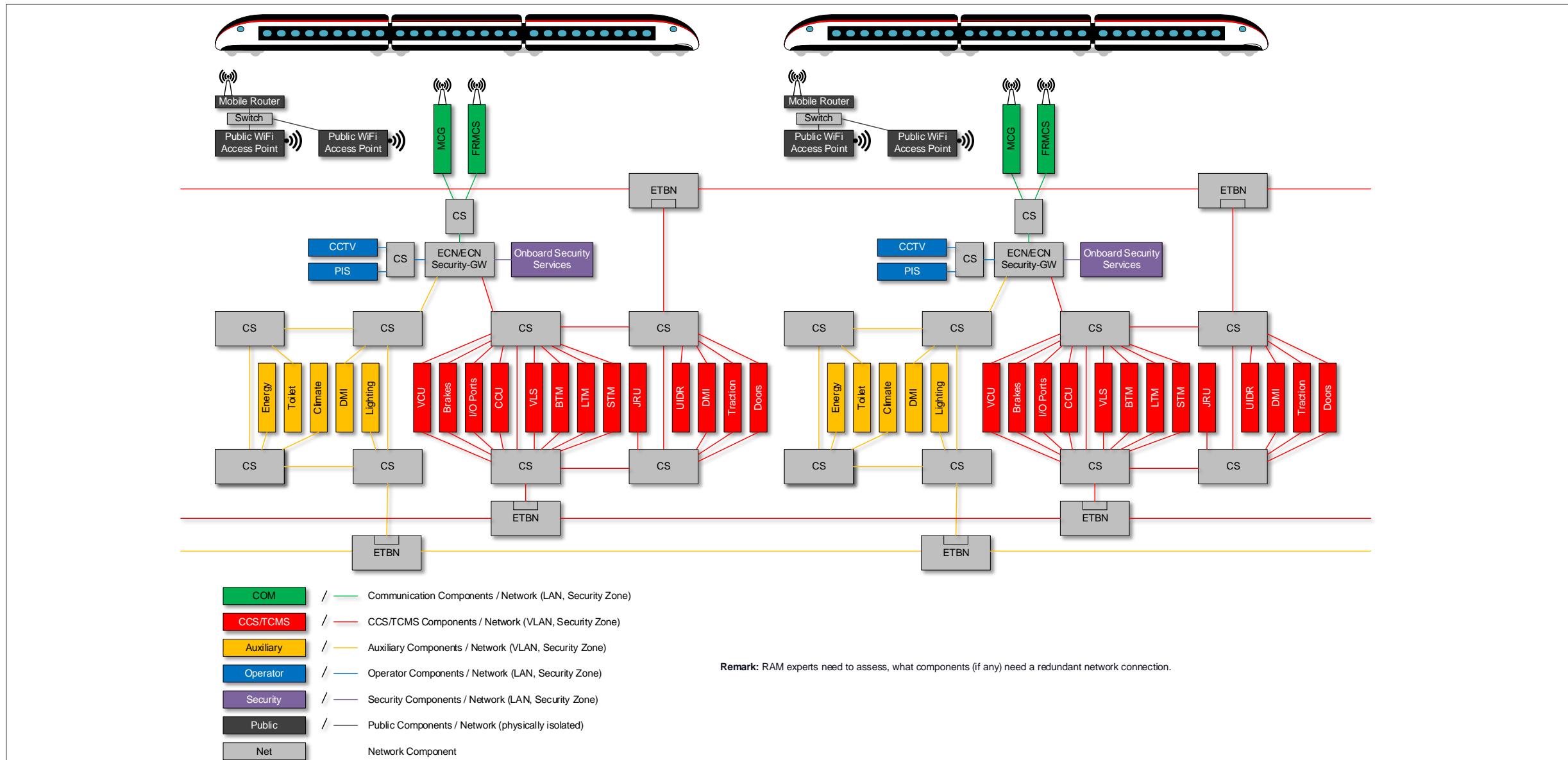
# Scenario C: Common critical control network logically separated



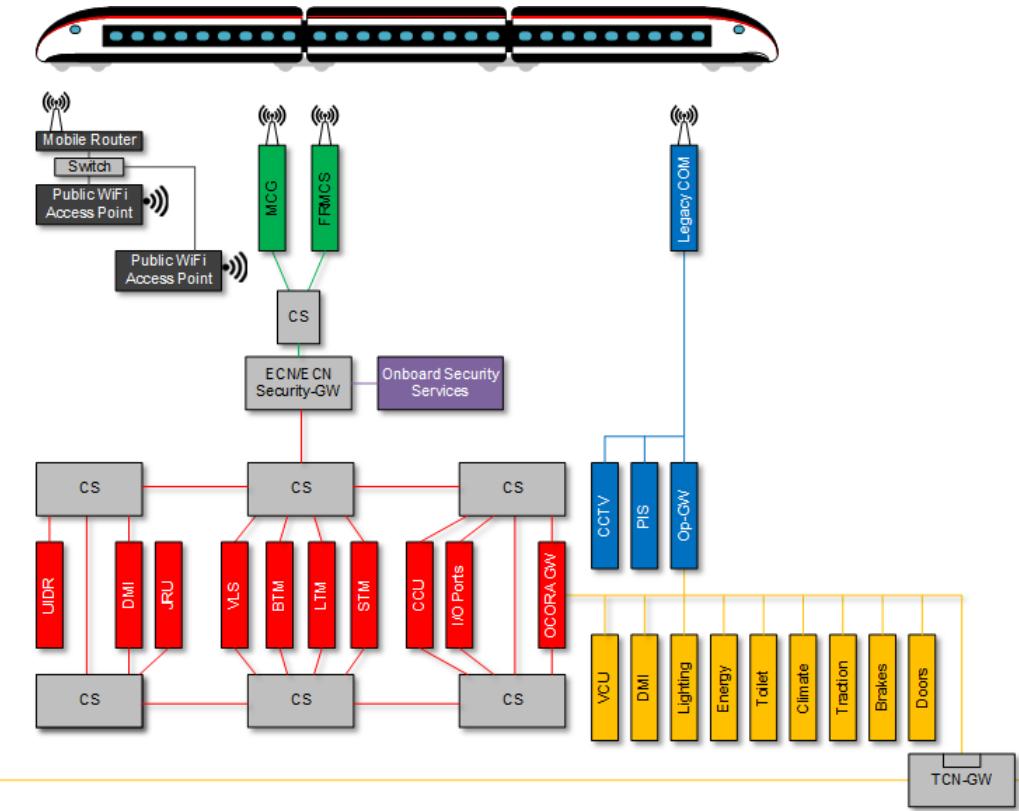
# Scenario D: Common critical control network physically separated



SBB CFF FFS



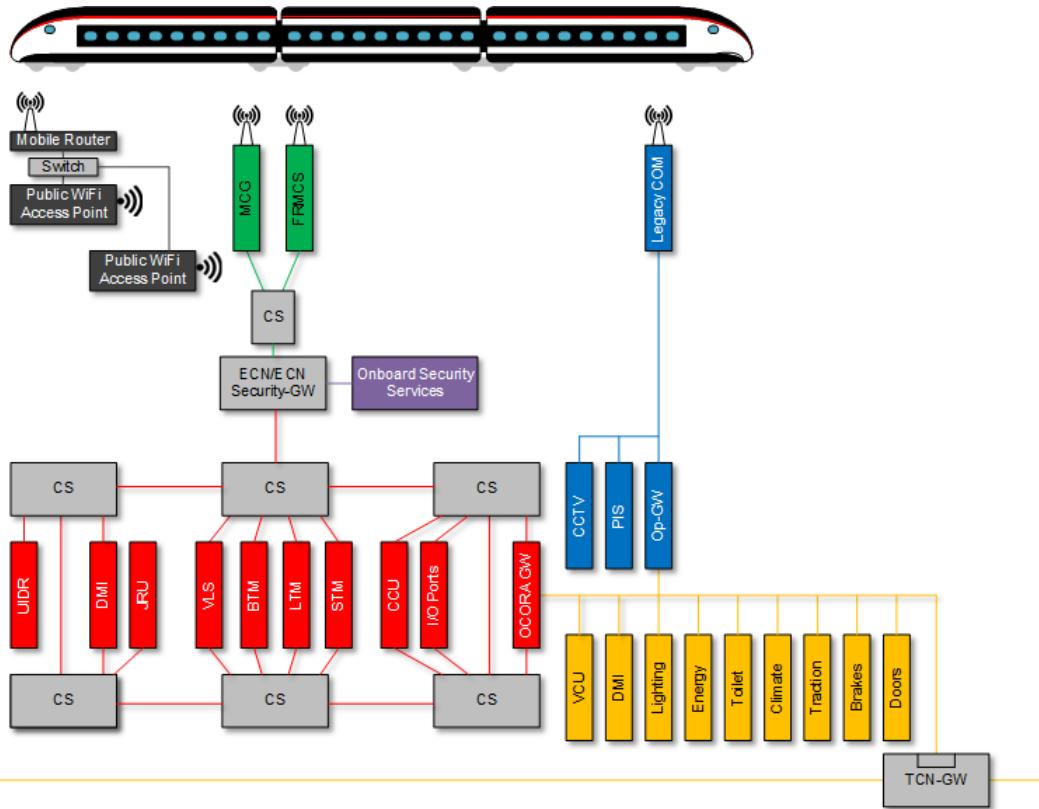
# Legacy Train – Integration with OCORA-GW



	/	Communication Components / Network (LAN, Security Zone)
	/	CCS Components / Network (VLAN, Security Zone)
	/	TCMS/Auxiliary Components / Network (VLAN, Security Zone)
	/	Operator Components / Network (LAN, Security Zone)
	/	Security Components / Network (LAN, Security Zone)
	/	Public Components / Network (physically isolated)
		Network Component

**Remark:** The network architecture of retrofit vehicles is only an example. Legacy architectures are always vehicle dependent and therefore the CCS integration is project specific.

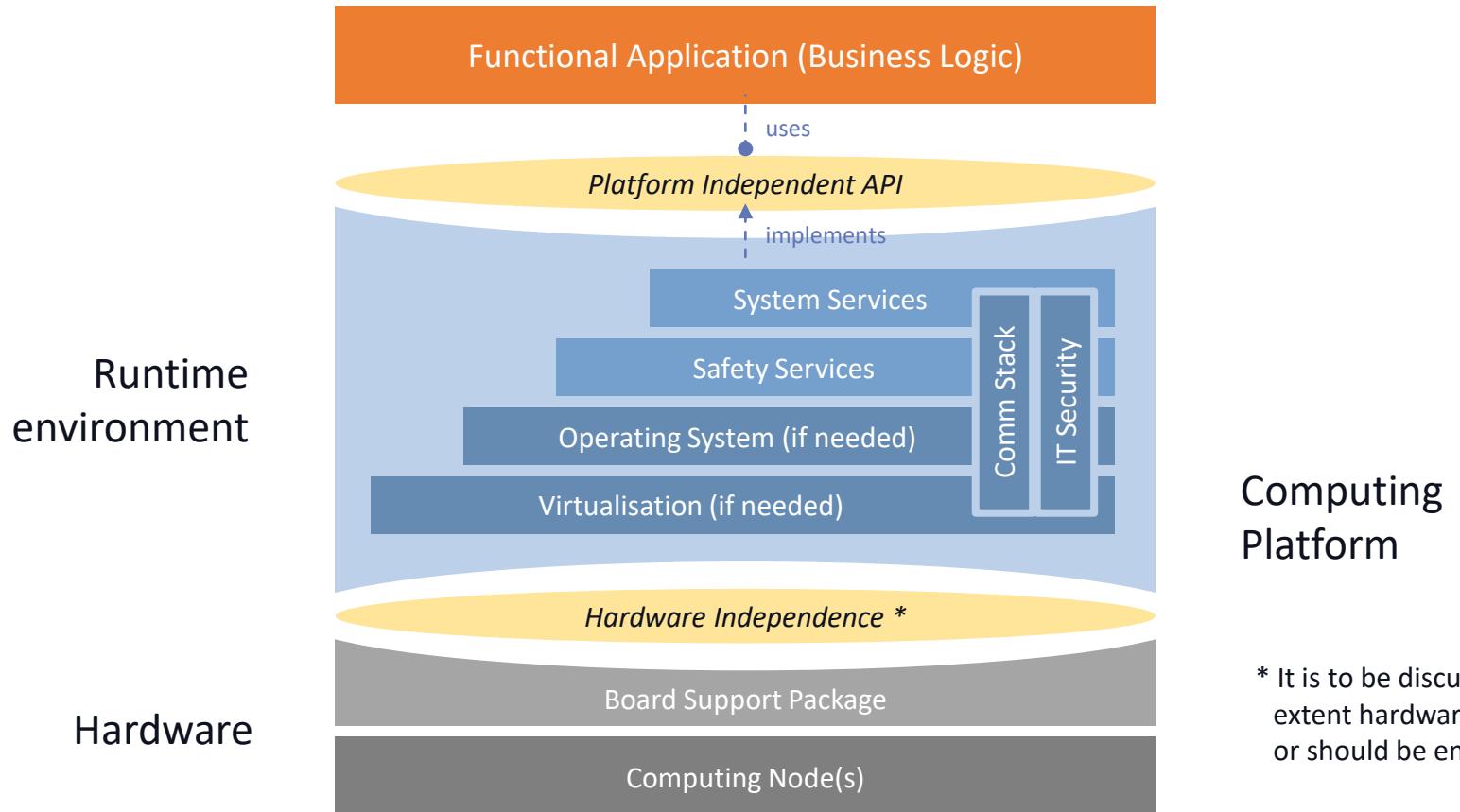
**Remark:** RAM experts need to assess, what components (if any) need a redundant network connection.



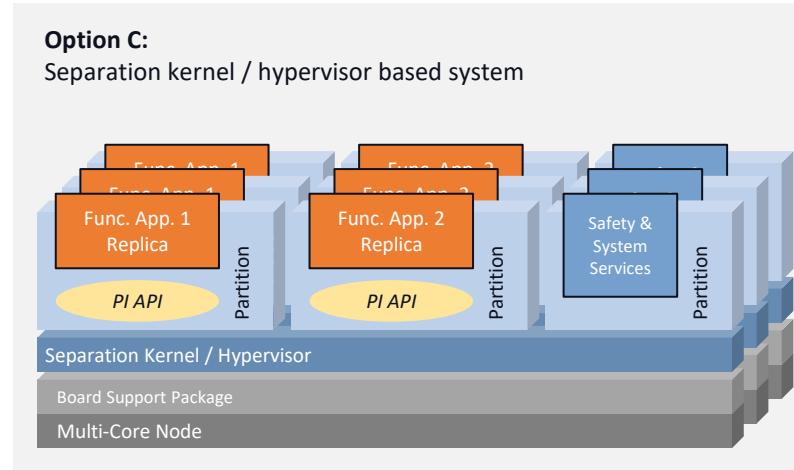
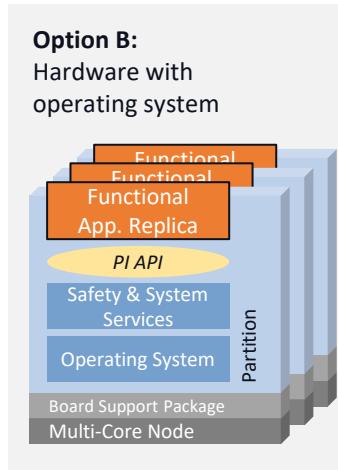
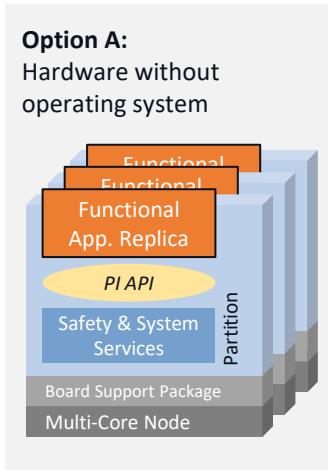


# Computing Platform

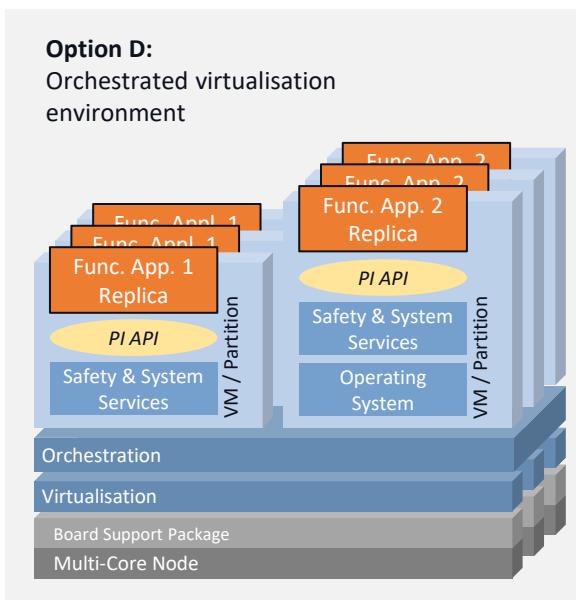
OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1



# Computing Platform – Deployment Options



Likely options for **onboard** deployments



Likely option for **trackside** deployments

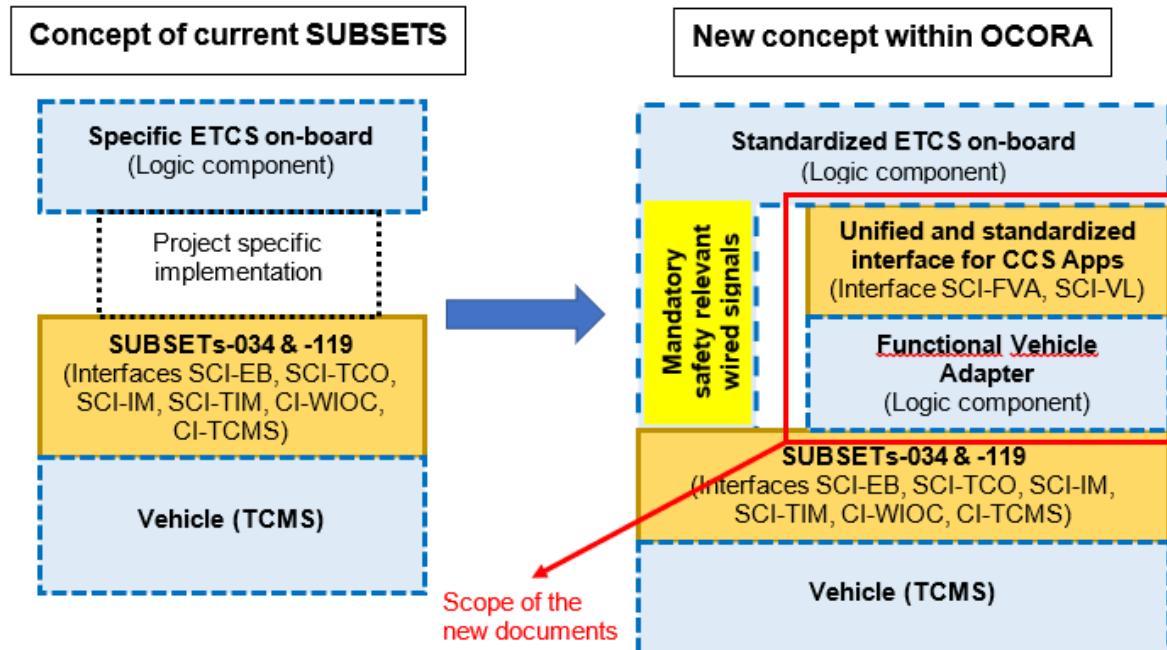
Platform options where applications are programmed against PI API  
*Approaches depicted in the diagram are non-exhaustive. The industry may propose different state-of-the-art solutions.*



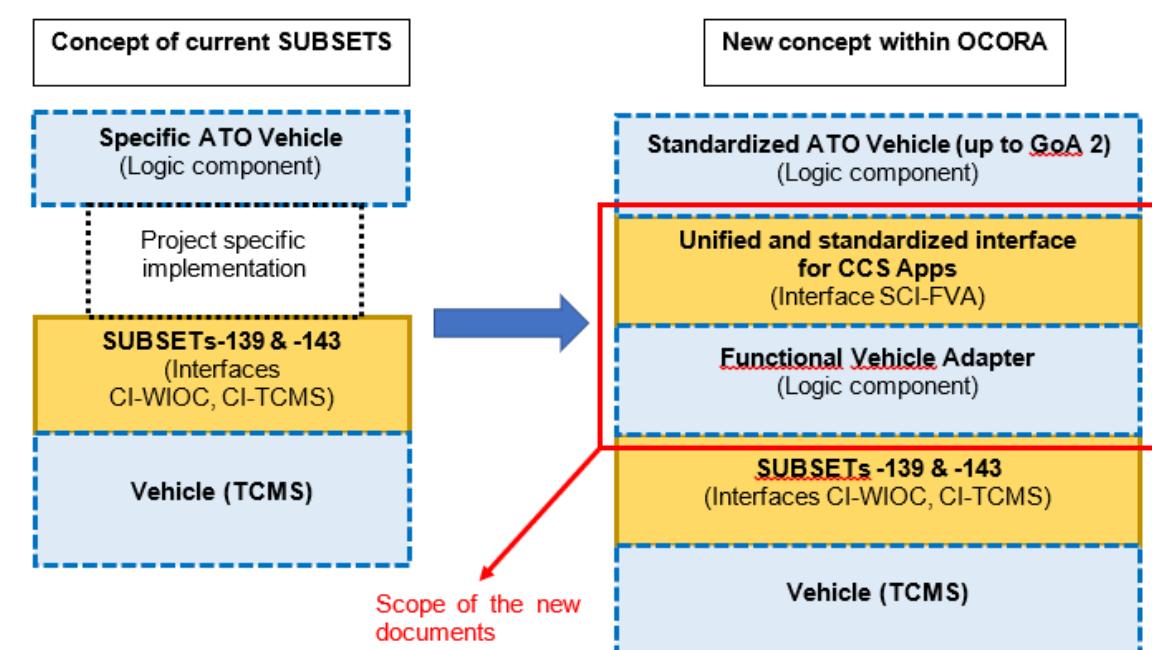
# Functional Vehicle Adapter (FVA)

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

## ETCS

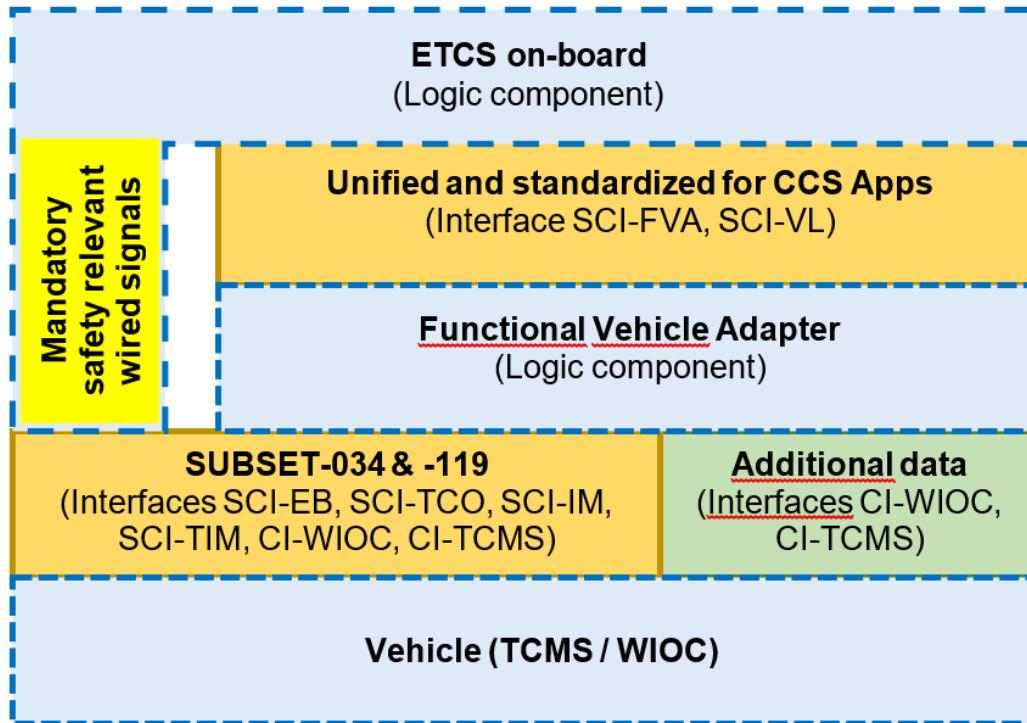


## ATO

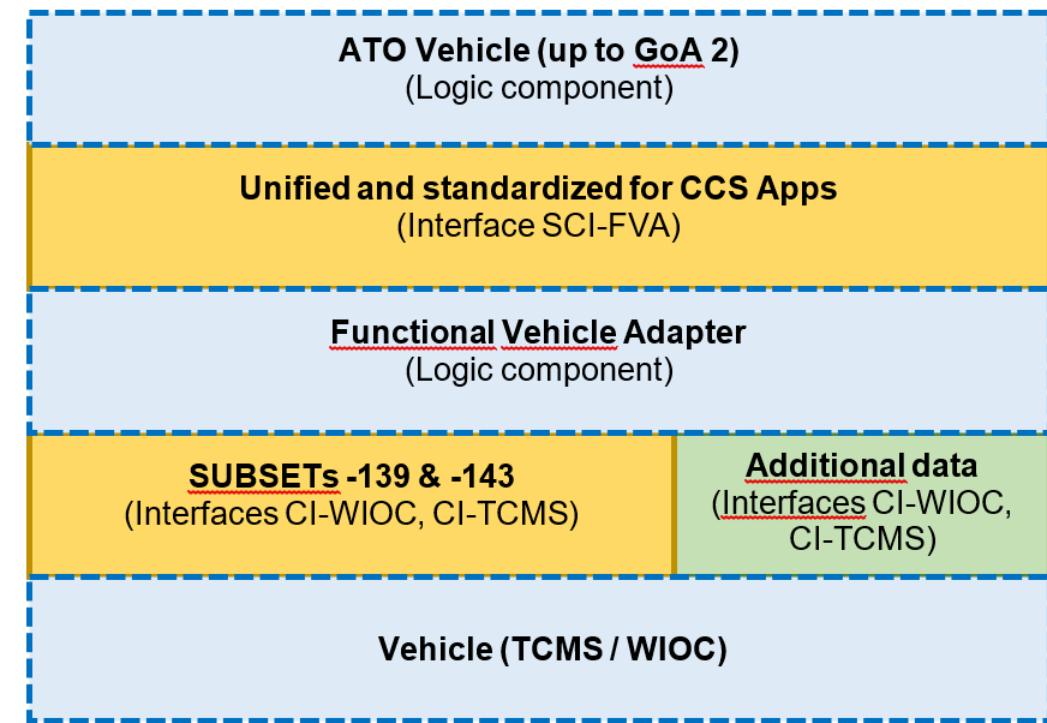


Details in Document: OCORA-TWS04-010 – Functional Vehicle Adapter - Introduction

## ETCS



## ATO



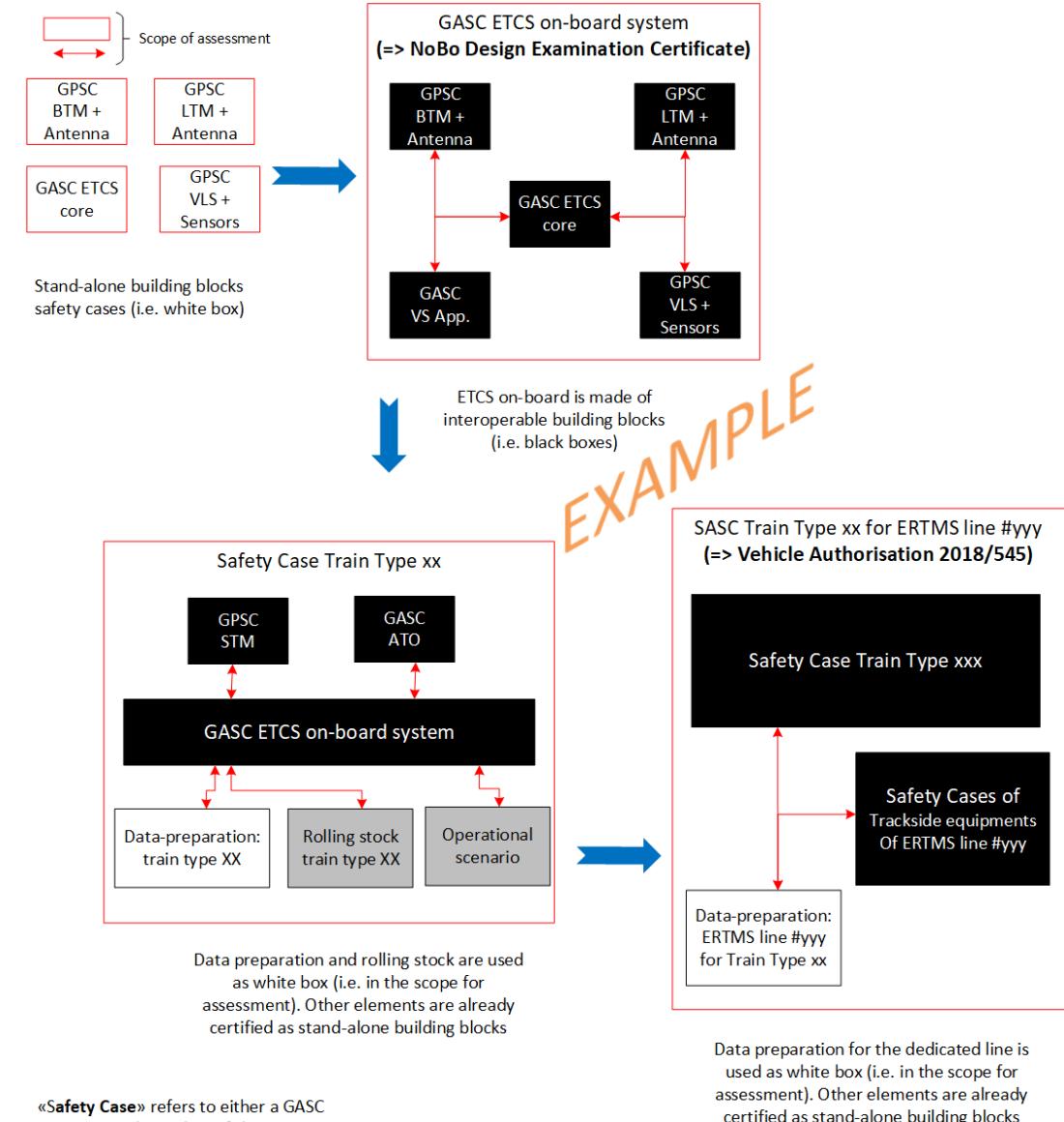
Details in Documents: OCORA-TWS04-013 – Design Guideline

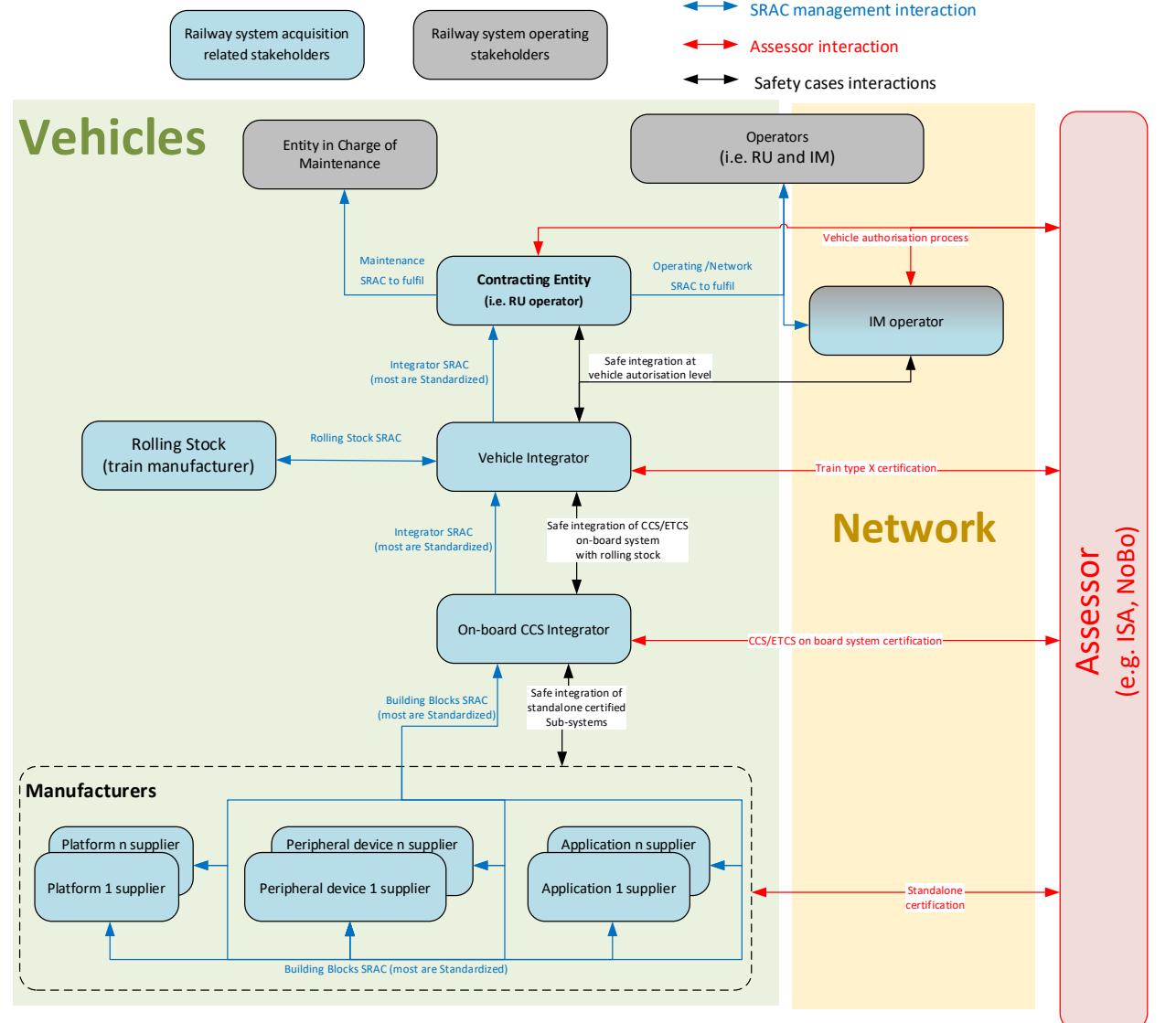


# Modular Safety

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

- Modular Safety defines the hierarchy between safety cases from building blocks to specific application(s).
- One of the main goal is to **reduce the certification efforts** (initial- and re-certification) at all levels without degrading the safety level of the analyses.
- Modular Safety shall also defines the safety elements to allow the homologation of stand-alone building blocks:
  - Hazardous events based on TSI CCS SUBSET-088
  - TFFR (Tolerable Functional Failure Rate) based on TSI CCS SUBSET-088
  - Safety requirements based on OCORA Delta release
  - Harmonised and generic set of SRAC

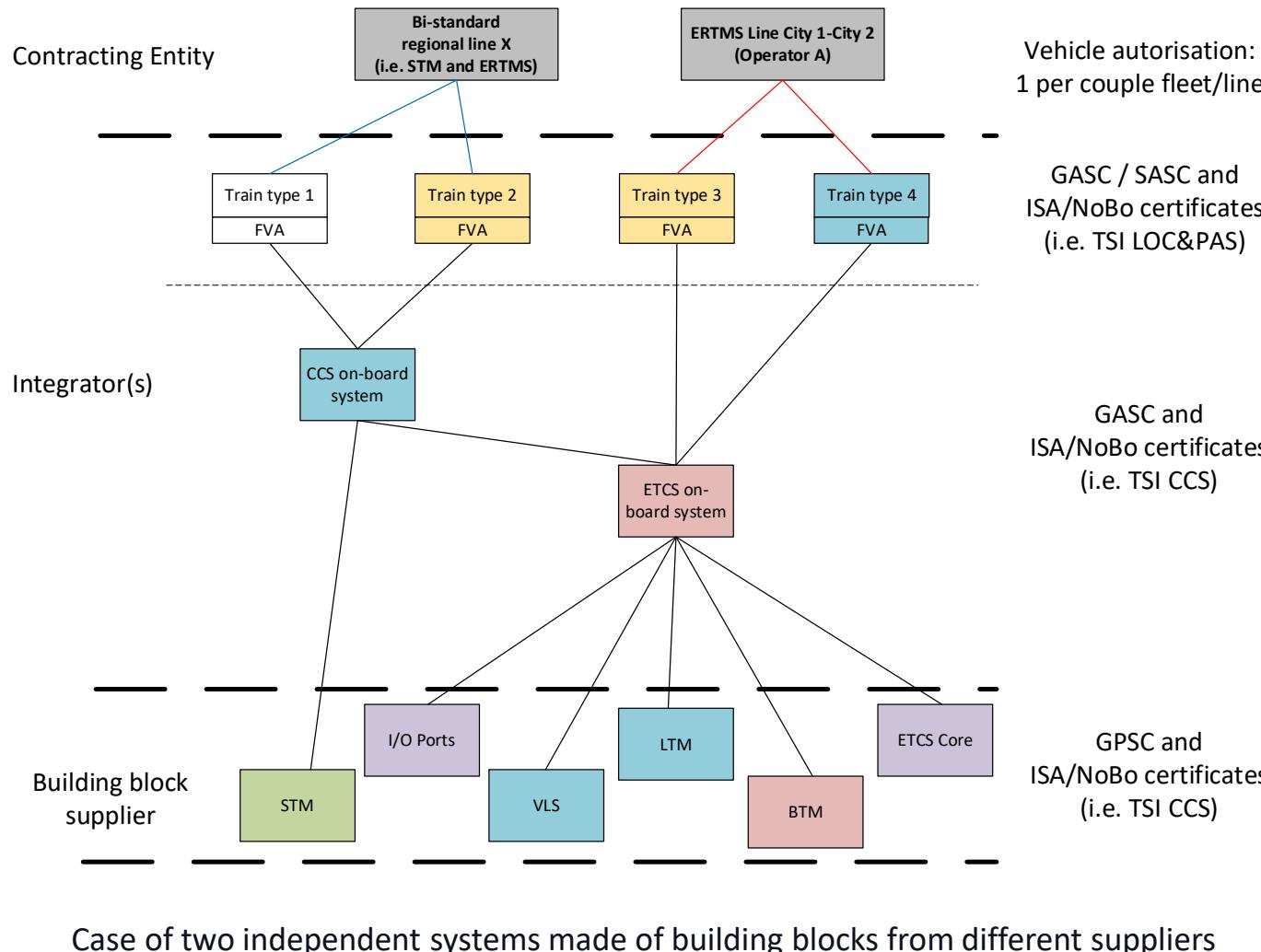




The integrator of the CCS/ETCS on-board system shall **coordinate the activities** of the different suppliers to **integrate** their sub-systems and ensure that finally, ISA and NoBo certificates of the CCS/ETCS on-board system will be delivered by the assessor

## Key roles

Each color represents a different supplier

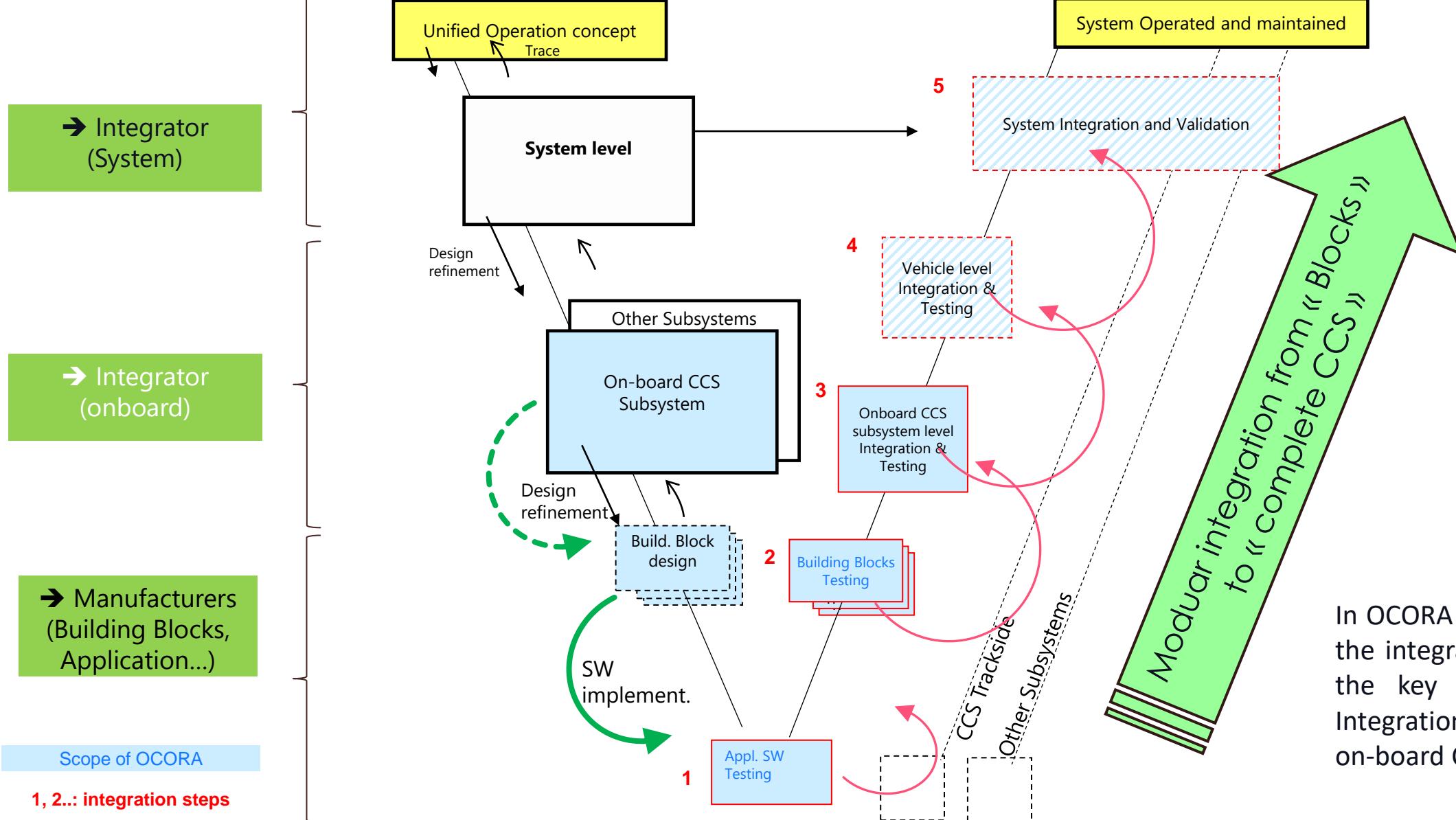


- **Each building block** is delivered to the ETCS on-board integrator with its **own ISA/NoBo certificates**
- ETCS on-board integrator realise their "**safe integration**" as defined in era\_1209-063 Clarification Note On Safe Integration (I.e. black boxes)
- Based on ETCS on-board ISA/NoBo certificates, CCS on-board integrator realise the **safe integration of the STM** (I.e. black boxes)
- CCS and ETCS on-board systems are used by the vehicle integrator to get the train type ISA/NoBo certificates (I.e. **integration is eased thanks to the FVA**)
- The contracting entity can apply for the different vehicle authorisations required
- A generic and systematic approach defined by OCORA, based on CSM-RA will then help any above stakeholder to handle easier (I.e. less delay and costs than today) the evolutions at any level

# OCORA – Modularity & Integration Tasks



SBB CFF FFS



In OCORA compliant projects, the integrator is identified as the key player for Safety, Integration and Testing of the on-board CCS system.



OCORA

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

## Modular CCS Stakeholders

→ Contracting entities (RU  
§IM)

→ Integrator(s)

→ Manufacturers (Building  
Blocks, Application...)

→ Other (ISA/ NoBo, DeBo..)

In OCORA compliant projects, the integrator is identified as the key player for Safety, Integration and Testing of the on-board CCS system



SBB CFF FFS



# Security

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

# Asset Classification



Name of data or data group	Description of data or data group	SIL	Confidentiality	Integrity	Availability	Privacy
CCU data	Computing data	SIL4	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
Location data	Vehicle location data	SIL4	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
BTM data	Balise data, location data	SIL4	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
LTM data	EURO Loop data	SIL4	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
NTC data	National Train Control data	SIL4	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
JRU/TRU/DRU data	Speed, position, communication, audio, video signals	noSIL	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P1 - Personal
I/O Module (EB/TCO) data	Command and monitor data	SIL4	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
DMI data	Supervised Distance Info (active braking curve), speed info (braking curve, speed monitoring), Supplementary Driving Info (ETCS L or NTC), Planning info (train speed profile crossing station), Monitoring (technical systems), driver input	SIL2	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P1 - Personal
Cab Voice data	Driver communication, audio data	noSIL	C1 - Internal	I1 - Basic Integrity	A2 - High availability	P0 - Anonymous
Radio data GSM-R	RBC communication	SIL0**	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
Radio data FRMCS	RBC communication	SIL0*	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
Vehicle Control data	Command and monitor data	SIL2	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous
Passenger data	Audio and video data for the passengers	noSIL	C1 - Internal	I1 - Basic Integrity	A1 - Business hours	P0 - Anonymous
Gateway data	Communication between networks	noSIL	C2 - Confidential	I2 - Special Integrity	A2 - High availability	P0 - Anonymous

x0 = no requirements

x1 = standard requirements

x2 = enhanced requirements

\* The functions and SIL for the FRMCS radio are not yet defined.

\*\* SIL for GSM-R radio depends on the view. In the integration phase 'basic integrity' is needed.

Indication 'SIL0' is equivalent to 'Basic Integrity'

Indication 'noSIL' notes a function that has no functional safety requirements

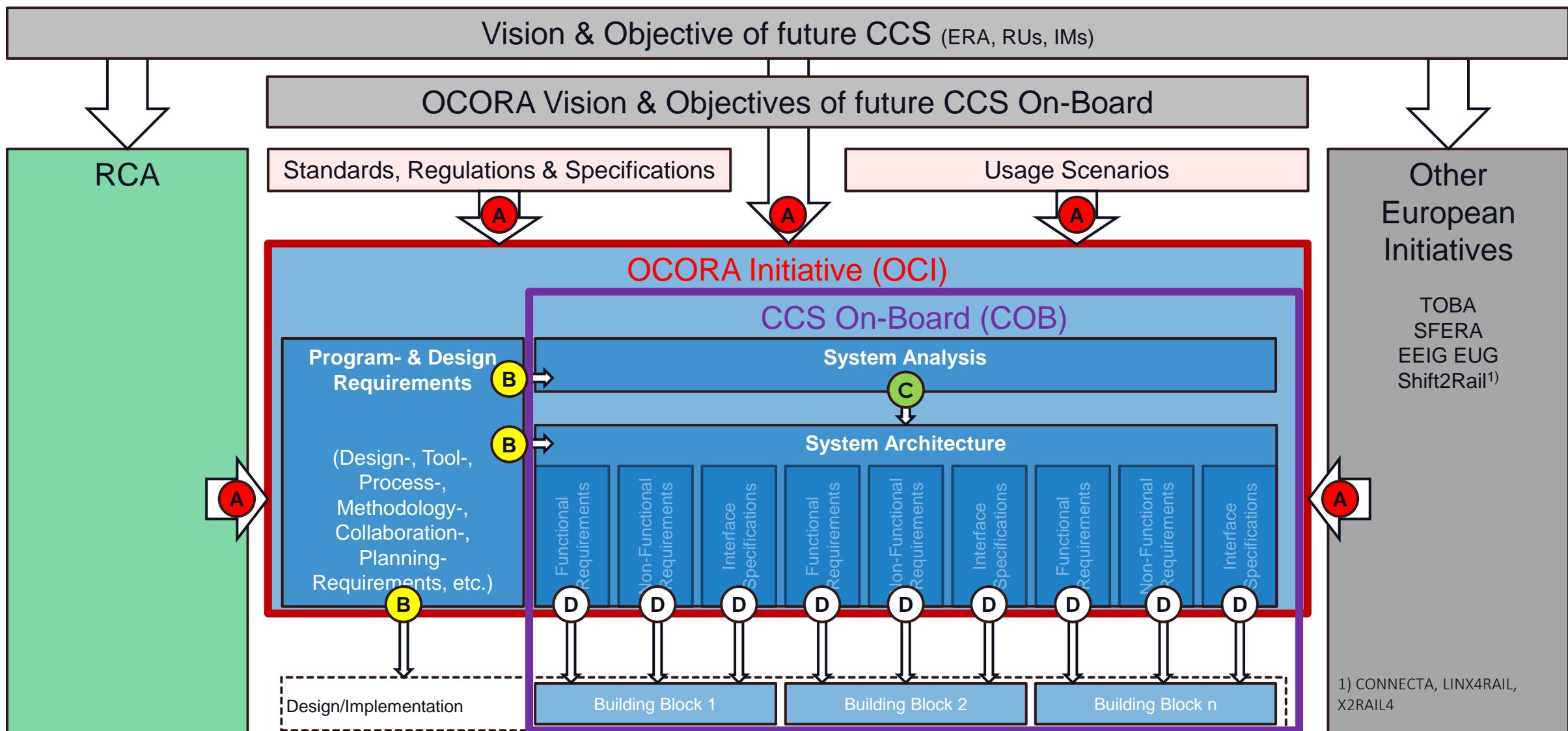




# Methodology & Tooling

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

## Structuring the Requirements



# OCORA Requirements Engineering

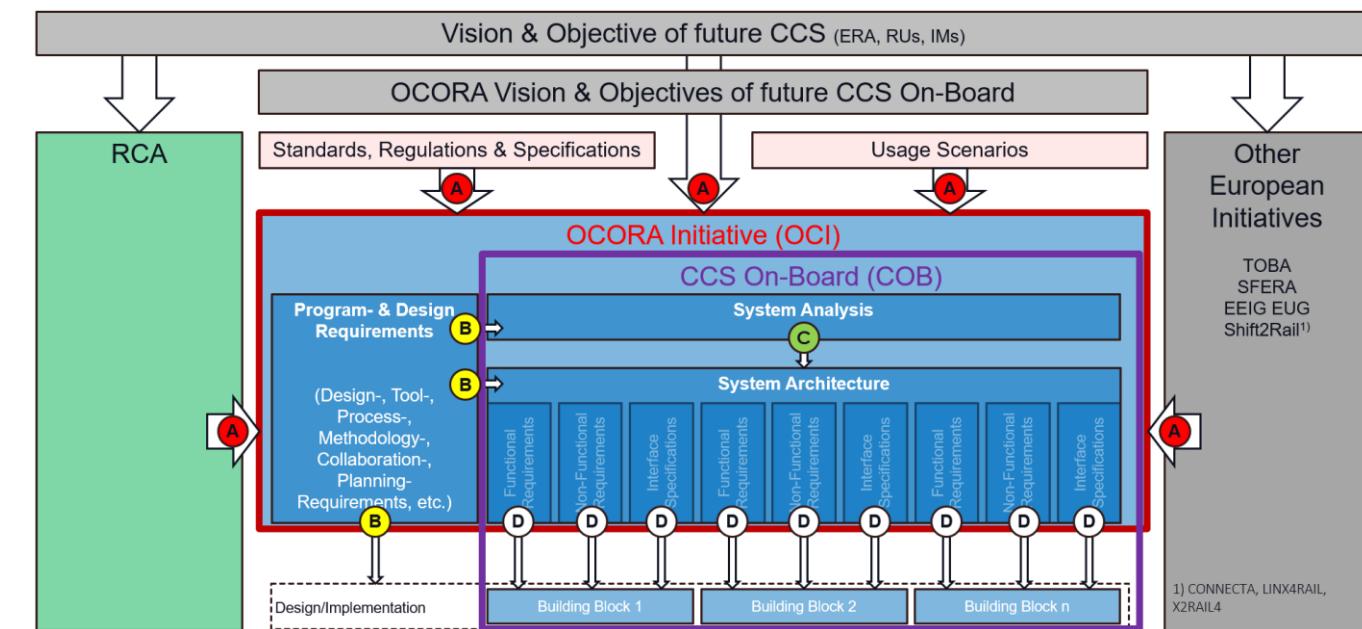
## Requirement Definitions

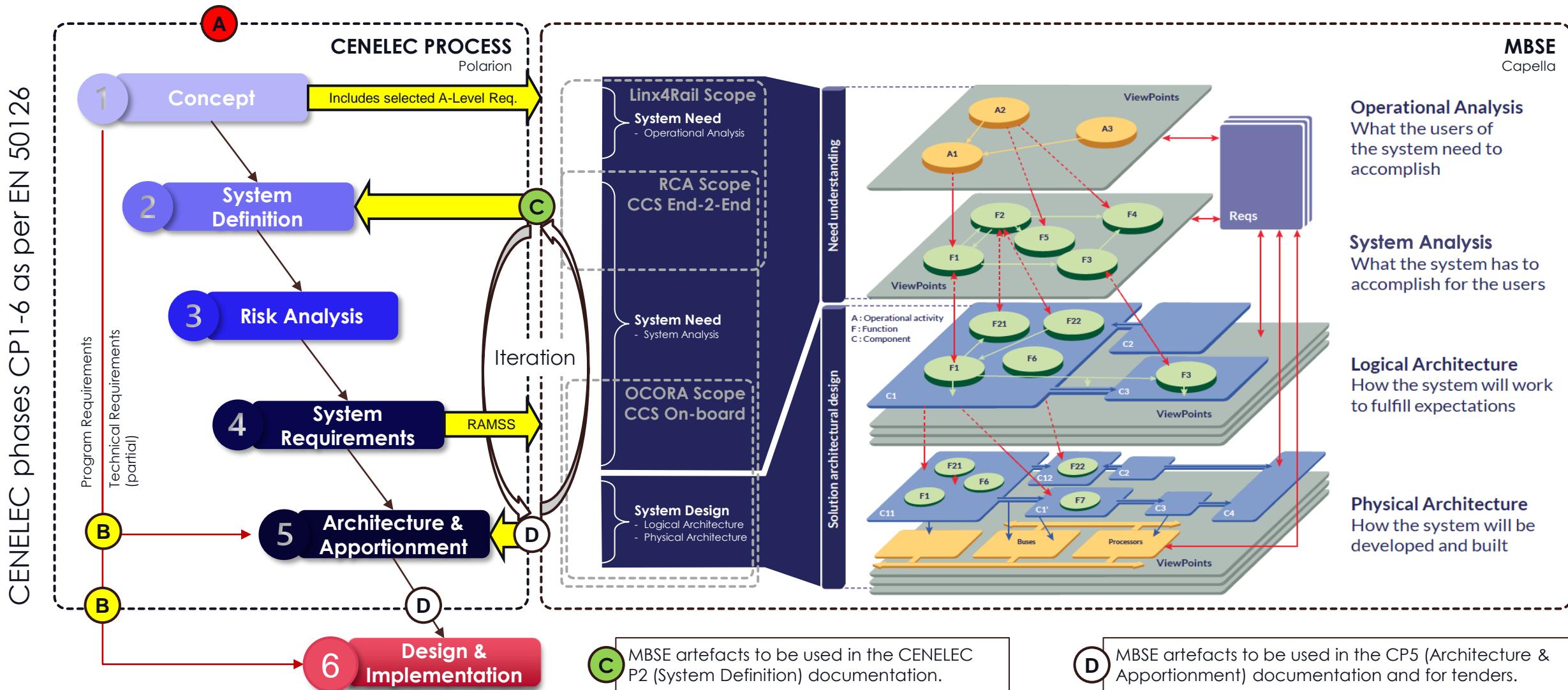
**A Stakeholder Requirements:** OCORA has to manage many different requirements, coming from many different stakeholders.

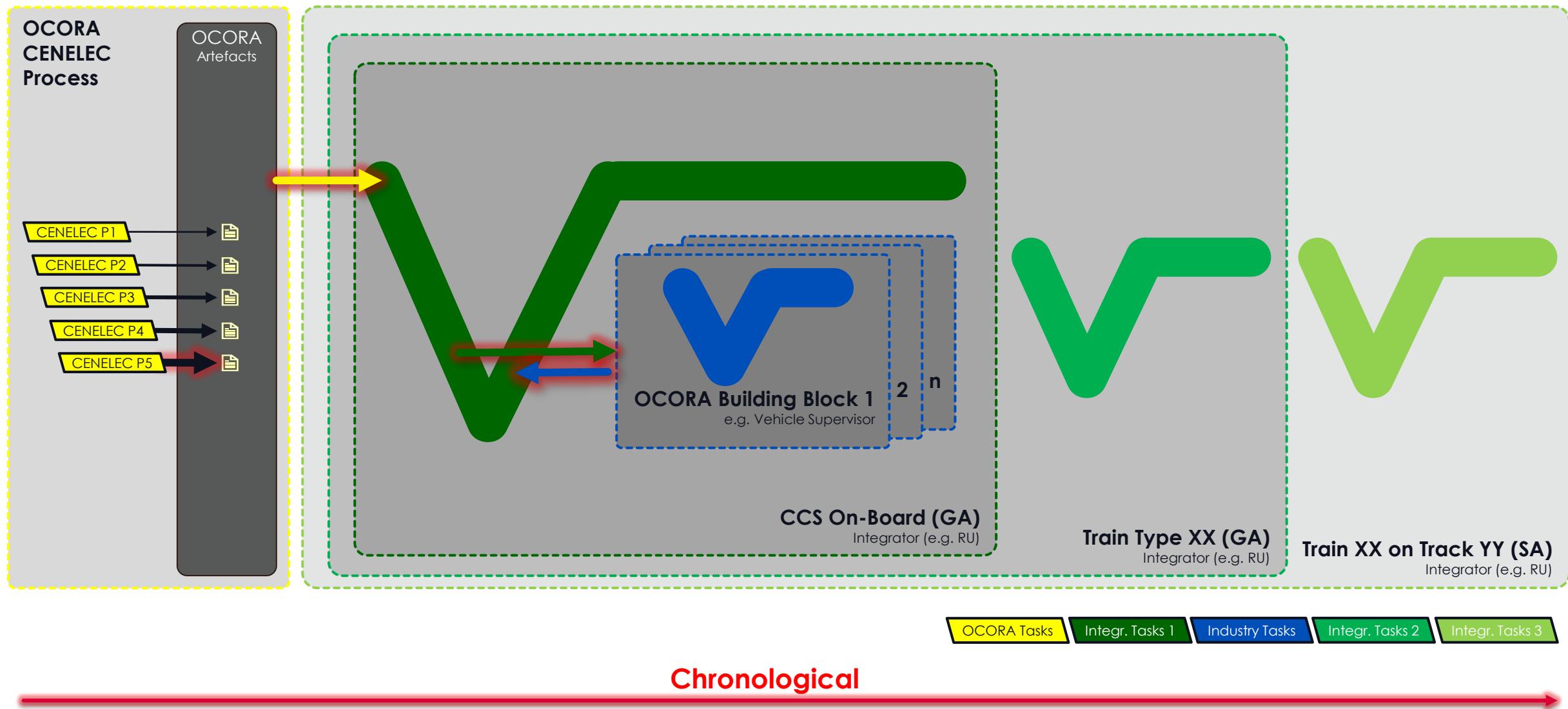
**B Program- & Design Requirements:** The OCORA program defines tools, processes, methodologies and design rules to be used within the program and to be considered during the system analysis and the system design/architecture work.

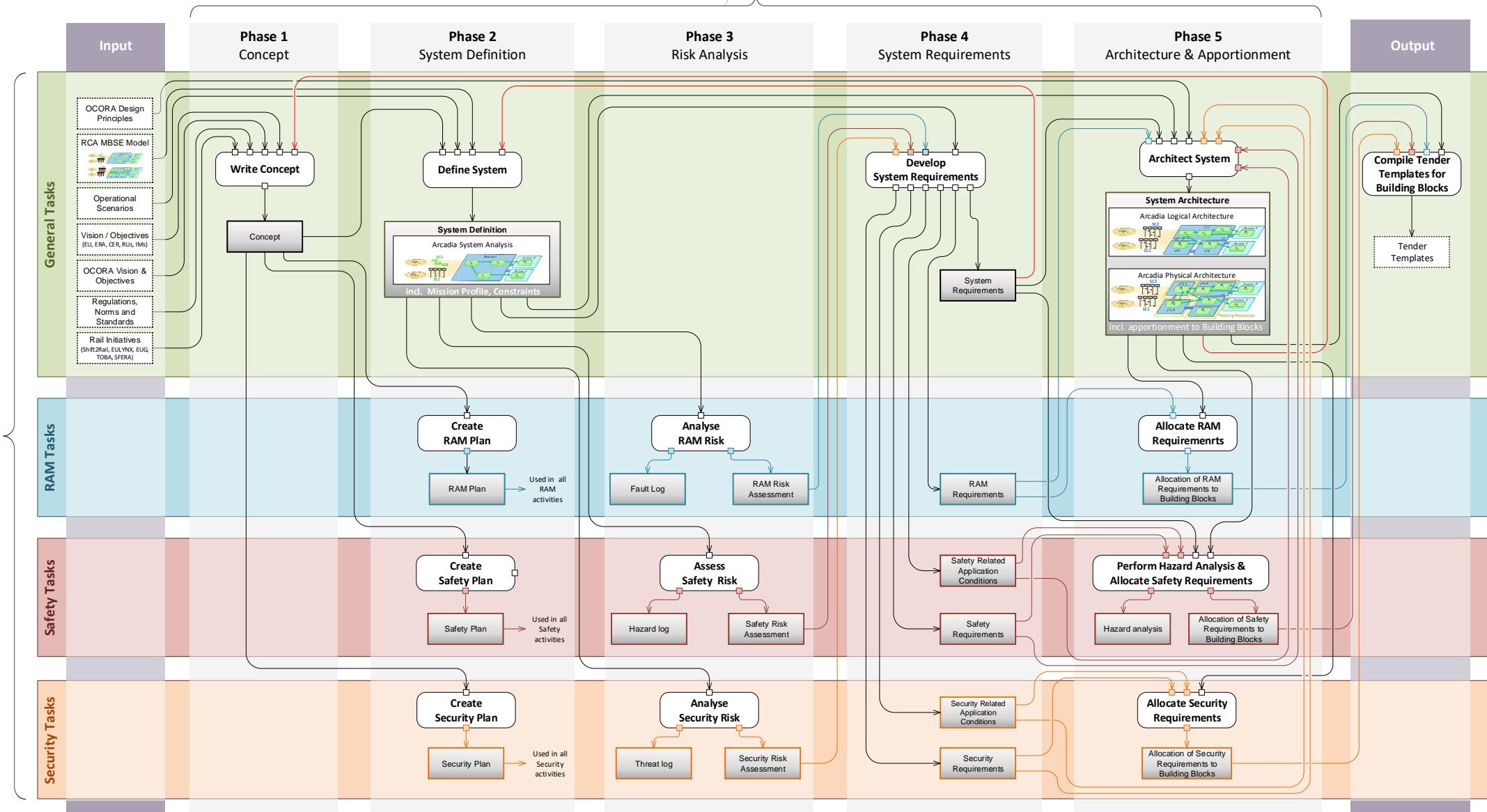
**C System Requirements:** Requirements in regards to the OCORA system are developed in the MBSE System Analysis (RCA & OCORA), taking into account the A- and B-Level Requirements.

**D Building Block Requirements:** Requirements in regards to the OCORA building blocks are developed in the MBSE System Architecture (logical / physical), taking into account the MBSE System Analysis. The resulting documentation form the OCORA tender templates, together with the applicable program requirements.











# Operational Concept

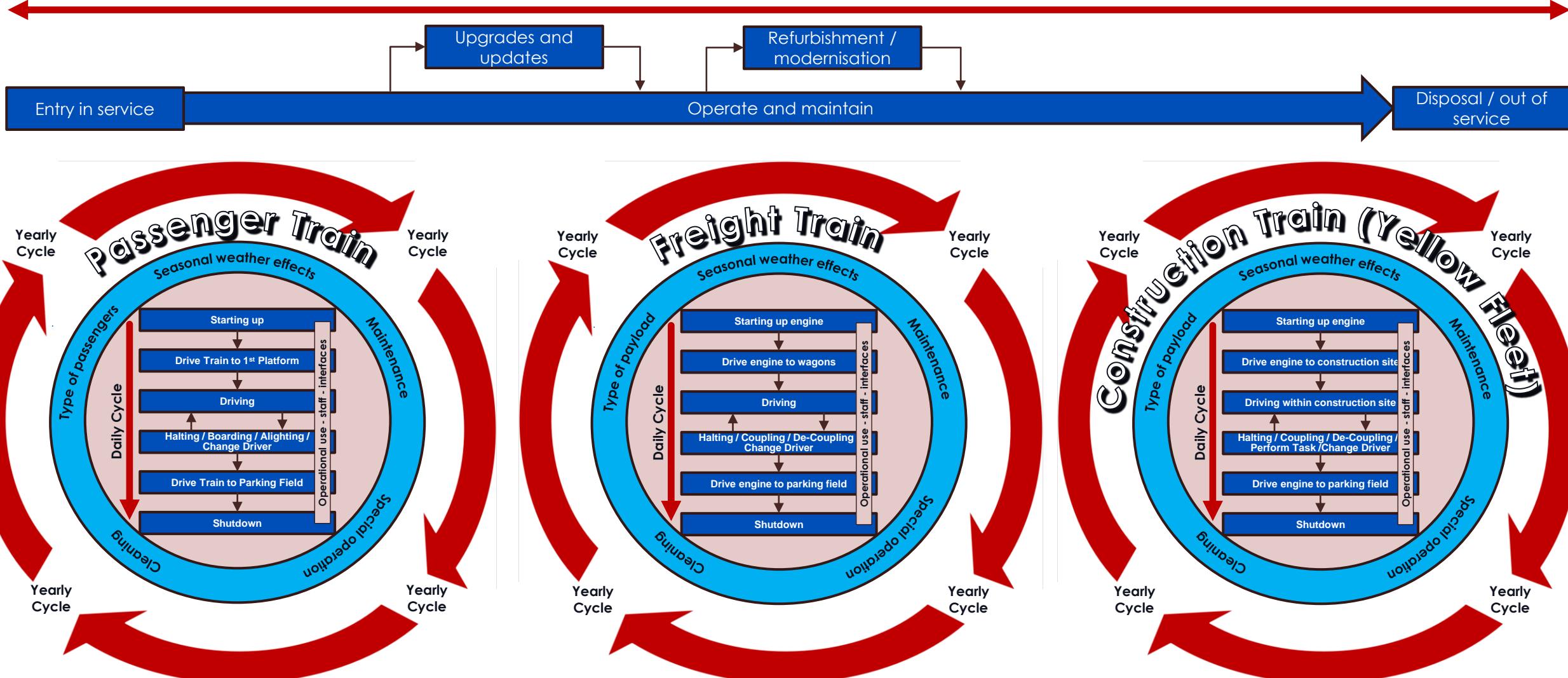
OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1

# Operational Concept Overview

## Live Cycle of Passenger & Freight Trains



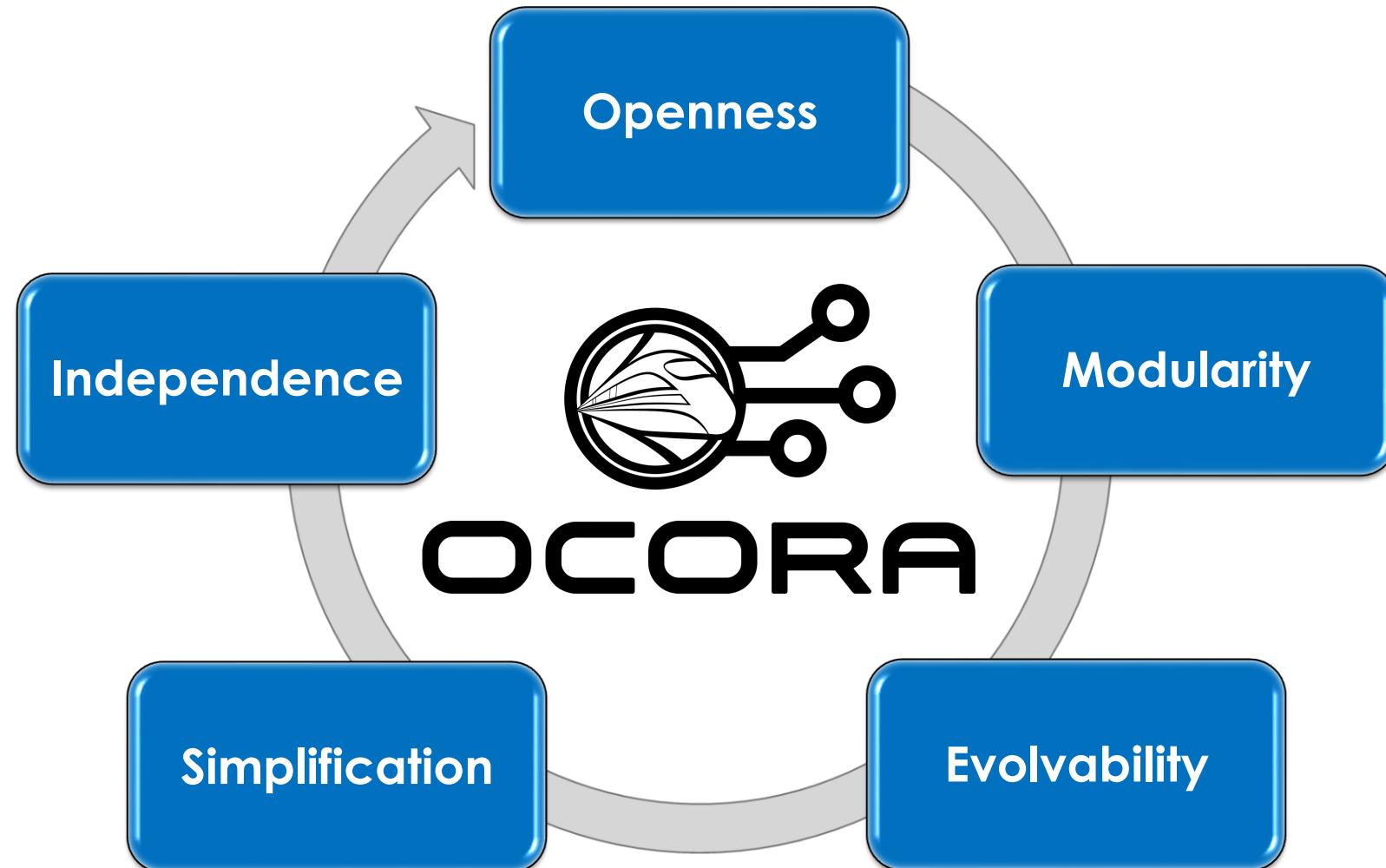
+/- 40 years overall life-time





# Supporting Slides

OCORA-BWS02-030 / v2.02 / 23.12.2021 / R1



## Business Workstreams

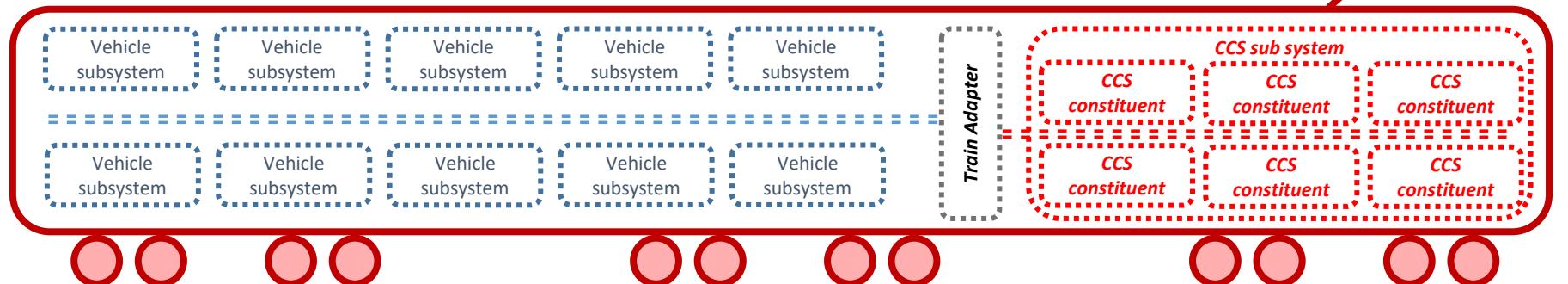
BWS01	Core Team
BWS02	Program & Technical Slides & Posters
BWS03	Introduction to OCORA
BWS04	Problem Statements
BWS05	Roadmap & Planning
BWS06	Business Model
BWS07	Alliances
BWS08	High Level Methodology & Tooling
BWS09	Acceptance of Global Standards

## Technical Workstreams

TWS01	System Architecture
TWS02	CCS Communication Network (CCN)
TWS03	Computing Platform
TWS04	Functional Vehicle Adapter
TWS05	Requirements
TWS06	(Cyber-) Security
TWS07	Modular Safety
TWS08	Diagnostic, Configuration, Monitoring
TWS09	Testing

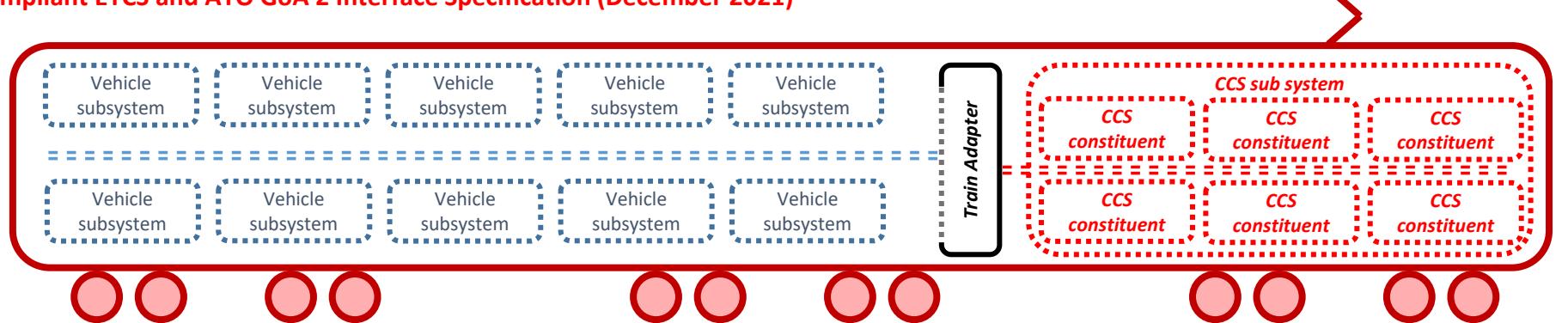
WP01	Open Points from Gamma Release
WP02	MBSE Preparation
WP03	Synchronisation with RCA & S2R
WP04	Localisation
WP05	ATO
WP06	ETCS
WP07	Connectivity
WP08	System Capabilities
WP09	CENELEC Documentation

**Level of Modularity 0** (current situation): the integrated proprietary CCS system is (again) fully integrated in the proprietary vehicle environment, driving costs and risks and complicating obsolescence issue



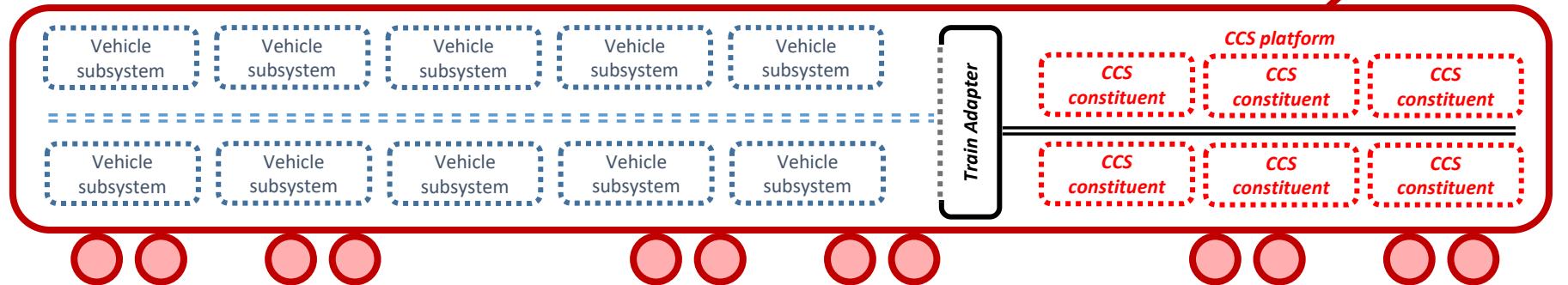
#### Project proposal: SS119 and SS139 Compliant ETCS and ATO GoA 2 Interface Specification (December 2021)

**Level of Modularity 1** (imminent retrofit projects): the interface between the proprietary CCS system is isolated from the fully integrated proprietary vehicle environment, enabling exchange of the CCS environment without affecting the vehicle and vice versa, simplifying obsolescence issues



#### Project proposals: Modular ETCS and GOA 2 Semi Formal Functional Model (December 2021); Modular ETCS and GOA 2 Full Formal Functional Model (December 2022); Modular ETCS and ATO GoA 2 Executable Software (December 2023); MVP - Prototype (starting from May 2023)

**Level of Modularity 2** (short term OCRA objective): the interface between proprietary constituents of the CCS system are isolated, enabling exchange of those constituents without affecting either the vehicle or other CCS constituents, simplifying obsolescence and migration issues



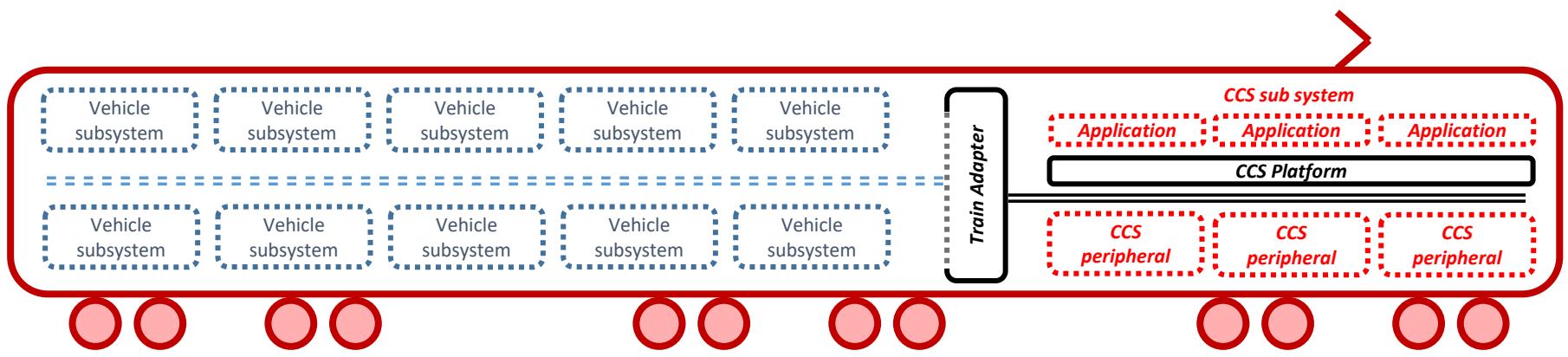
**Urgent project proposal**

**Next project proposals**

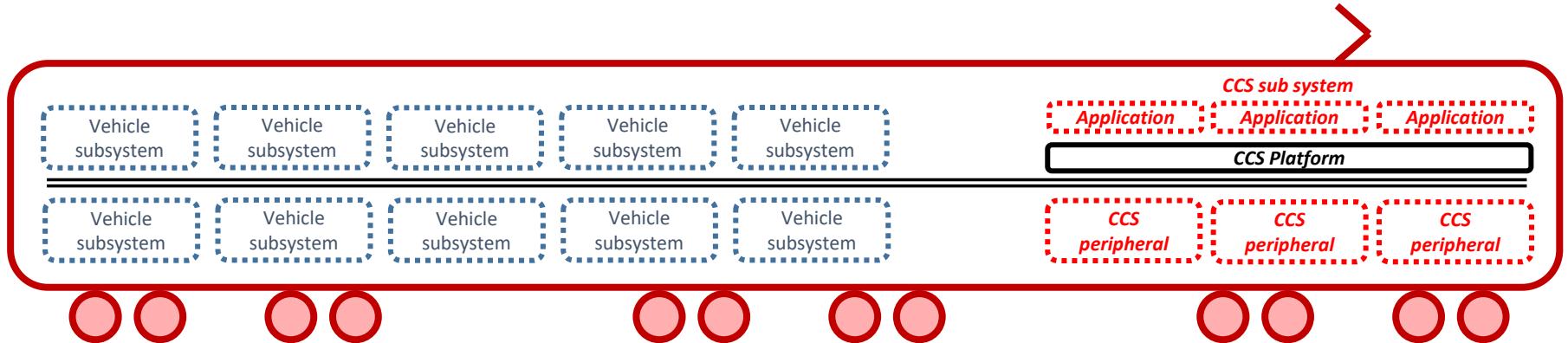
Integrated, proprietary subsystem or constituent

Open, universal subsystem or constituent – MVP

**Level of Modularity 5** (full OCORA on-board): the CCS system is composed of a platform, hosting independent application and connected to peripheral through a CCS standardized communication network. This open CCS environment is isolated from the fully integrated proprietary vehicle environment



**Level of Modularity  $n$**  (long term perspective): the standardised CCS communication network interface any vehicle constituents, simplifying obsolescence and migration issues



Urgent project proposal

Next project proposals

Integrated, proprietary subsystem or constituent

Open, universal subsystem or constituent – MVP

OSI Layer		Protocol	
		Protocol for hard-real-time data	
(Safety*)		<b>(SDTv2 / SDTv4)</b>	
5	Session	TRDP - OPC-UA Pub/Sub - DDS-RTPS	
4	Transport	UDP (for process and message data) TCP (for message data)	
3	Network	IPv4	
2	Data Link	<b>Time-Sensitive Networking (TSN) IEEE 802.1</b>	<b>Standard Ethernet IEEE 802.3</b>
1	Physical	<b>100BASE-TX or 1000BASE-T</b>	

\*Safety layer is only applicable for safety function related data traffic

Details im Document: OCORA-TWS02-010 - CCN Evaluation