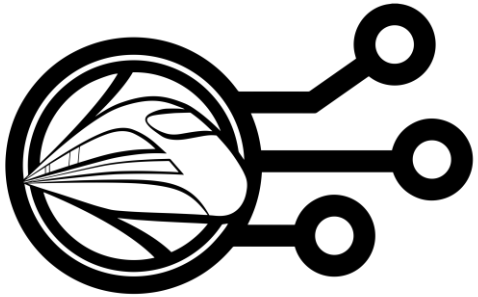


OCORA

Open **C**CS **O**n-Board **R**eference **A**rchitecture

A Collaboration of 5 European Railway Undertakings

Technical Slide Deck

OCORA-BWS02-030 / v2.20 / 24.06.2022

Presentation Overview

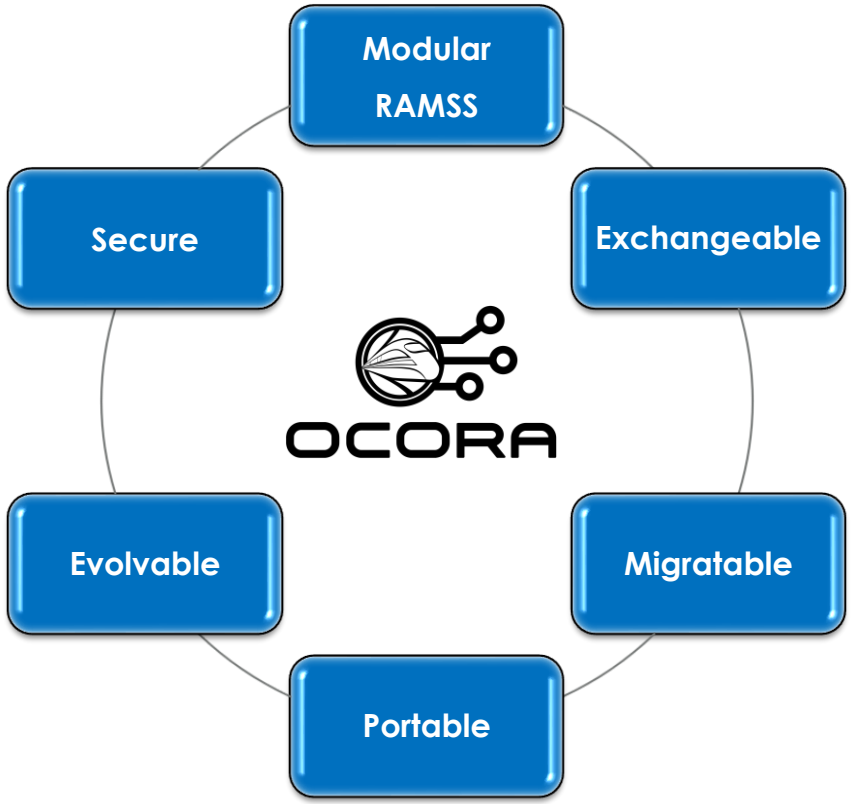
- **Design Objectives / Technical Roadmap & Vision**
- **OCORA Scope**
- **CCS On-Board Logical Architecture**
- **CCS On-Board Physical Architecture**
- **Building Blocks**
- **Train Integration Scenarios**
- **Network Topology Scenarios**
- **Computing Platform**
- **Functional Vehicle Adapter (FVA)**
- **Modular Safety**
- **Methodology & Tooling**
- **Operational Concept**

Design Objectives
Technical Roadmap & Vision

OCORA-BWS02-030 / v2.20 / 24.06.2022

OCORA Design Objectives

A reasonable number of Building Blocks are defined for CCS On-Board. Each Building Blocks has standardised functionality, standardised interfaces, standardised performance (RAM), standardised safety (including Tolerable Functional Failure Rate [TFFR], Safety Integrity Level [SIL] and Safety Related Application Conditions [SRAC]), and standardised security.



Ability to protect the CCS On-Board from attacks. In context of OCORA security means the protection of (especially safety related communication and data used in) CCS on-board systems against threats (in particular cyber-attacks and hacks). To achieve this, all main security functionality like identify, protect, detect, respond and recover are considered.

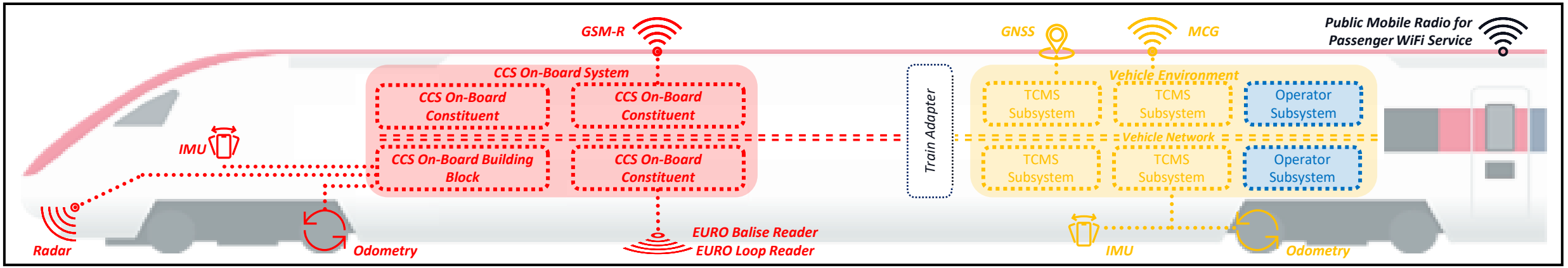
Ability to replace CCS On-Board Building Block. In the context of OCORA exchangeability means the ability to replace one or multiple OCORA defined building blocks with (a) respective building block(s) of (an)other supplier(s), without affecting other building blocks of the train or the overall CCS on-board system.

Ability to easily adapt the CCS On-Board to new technologies and to easily add new Building Blocks. In the context of OCORA evolvability means the ability to easily adopt to new technologies or to extend the functionality of an on-board CCS system without the involvement of the original supplier.

Ability to introduce changes to any CCS On-Board Building Block. In the context of OCORA migrateability is the ability to introduce changes to one or multiple OCORA defined building blocks, without affecting other building blocks or the overall CCS on-board system.

Ability to port CCS On-Board Software Building Blocks (software applications) from one computing platform to another. In the context of OCORA portability is achieved when a functional application, based on the generalized abstraction, runs un-changed on different (computing) platform implementations. For this, the functional application shall only use external functions through a defined application programming interface (API).

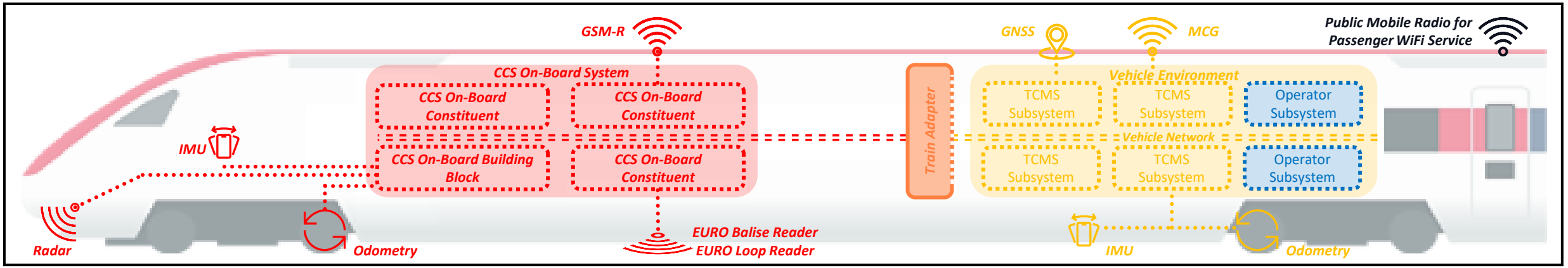
Technical Roadmap – Current Situation



Step 0: Current Situation

Today, the proprietary CCS On-Board System is fully integrated in the proprietary Vehicle Environment, driving costs, risks, and complicating the life-cycle and obsolescence management for the railway undertakings. This current situation hinders the railways to take advantage of innovations in a timely and cost-effective manner.

Technical Roadmap Step 1 – Short-Term



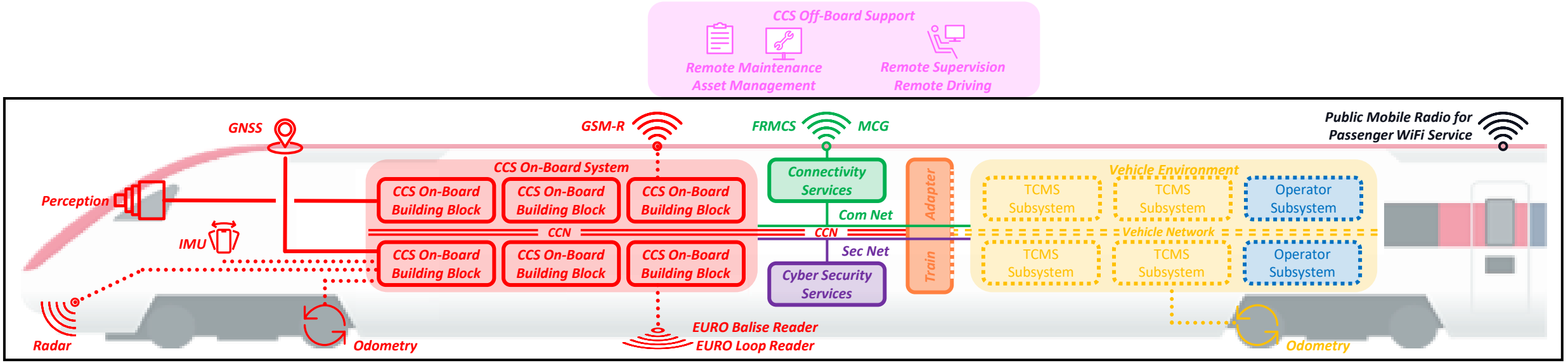
Step 1: Short-Term (TSI-2022)

The interface between the proprietary CCS On-Board System and the Vehicle Environment is unambiguously standardised.

Step 1 is enabling exchangeability, is supporting migrateability and portability of the CCS On-Board System without affecting the Vehicle Environment.

Step 1 is simplifying life-cycle and obsolescence management for the CCS On-Board System.

Technical Roadmap Step 2 – Mid-Term



Step 2: Mid-Term (TSI-2025)

The CCS On-Board System consists of a well balanced number of CCS On-Board Building Blocks. Each Building Blocks has standardised functionality, standardised performance (RAM), standardised safety (including Tolerable Functional Failure Rate [TFFR], Safety Integrity Level [SIL] and Safety Related Application Conditions [SRAC]), standardised security, and standardised interfaces towards other building blocks and/or external systems, allowing to mix-and-match Building Blocks from different suppliers.

The CCS On-Board Building Blocks communicate with each other, with the Vehicle Subsystems and any Off-Board System via the standardized CCS Communication Network (CCN) and the Connectivity Services, using FRMCS or the MCG. Cyber Security Services provide Identity and Access Management (IAM), security patch updates, synchronized time services, and other means to allow secure operations.

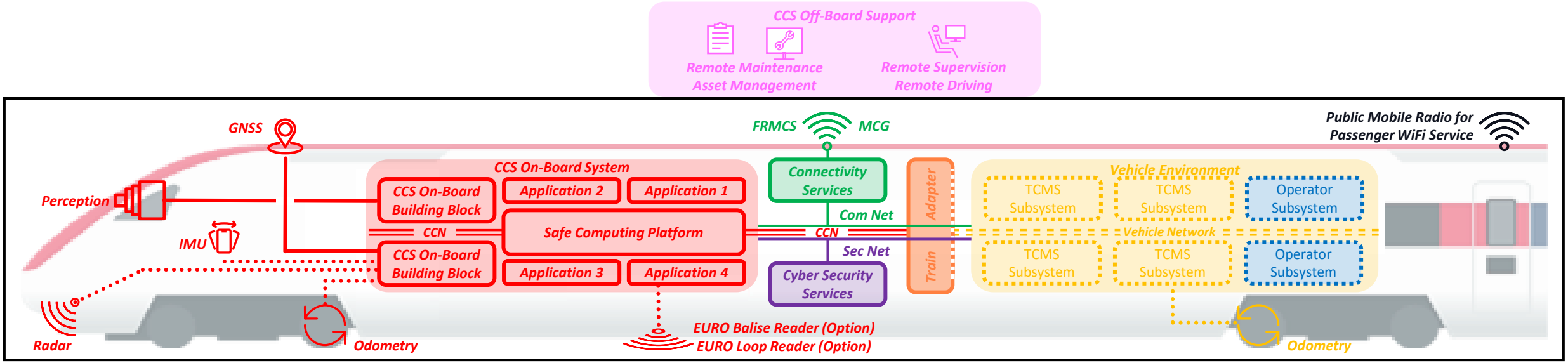
Step 2 is enabling exchangeability, is supporting migrateability and portability of the individual CCS On-Board Building Blocks without affecting other CCS On-Board Building Blocks, the Vehicle Environment, and any Off-Board Systems. This step is simplifying life-cycle management and is the basis for the railways to consider adding new functionality such as:

- Remote Maintenance
- Asset Management
- Absolut continues safe localisation (GNSS)
- Safe Train Integrity determination
- Safe Train Length determination
- ETCS L3
- ATO GoA 1-4
- Remote Supervision
- Remote Driving

Step 2 is enabling the sharing of the following peripheral devices between CCS On-Board and the Vehicle Environment:

- Mobile Communication Gateway (MCG)
- GNSS antenna and receiver
- Inertial Measurement Unit (IMU)

Technical Roadmap Step 3 – Long-Term



Step 3: Long-Term (TSI-2028)

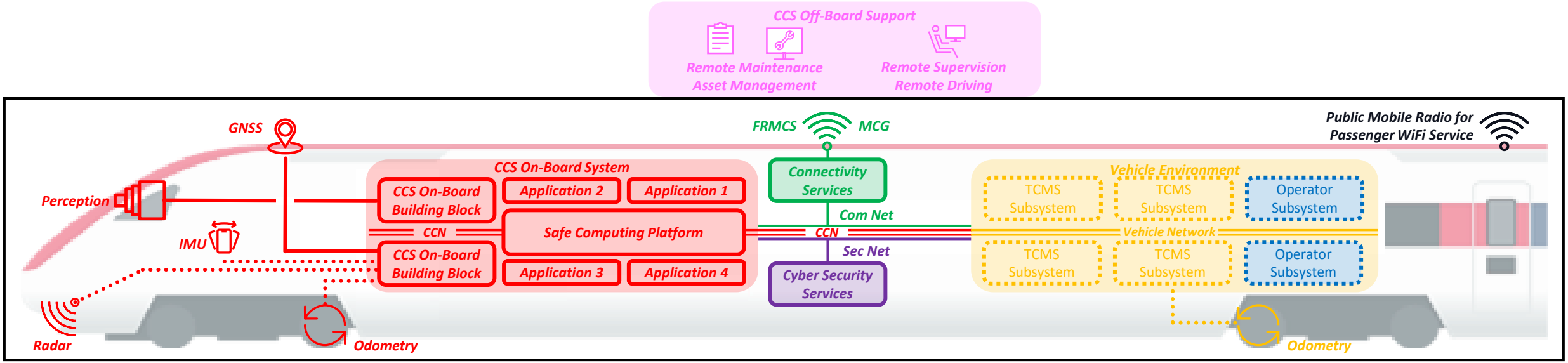
The CCS On-Board System includes a safe computing platform, hosting CCS Building Blocks as applications that communicate with each other, with the Vehicle Subsystems and any Off-Board System via a standardized API, the standardized CCS Communication Network (CCN) and the Connectivity Services, using FRMCS or Public Mobile Radio.

Due to the increased performance of the CCS On-Board localisation, EURO Balise and EURO Loop readers may not be needed anymore for trains running on certain tracks.

Step 3 is simplifying the portability of the business logic.

Step 3 is simplifying the development and deployment of new functionalities by separating the business logic from the hardware. In addition, the Safe Computing Platform is reducing the number of CCS computing units (CCUs) needed, increasing availability and reducing maintenance efforts.

Technical Roadmap Step 4 – Vision



Step 4: Vision (> TSI 2028)

The standardised CCS On-Board Communication Network (CCN) is fully integrated with the Vehicle Network, allowing to interface from any CCS On-Board Application directly with any Vehicle Subsystems and vice-versa. The need for a Train Adapter vanishes and certain Applications from the Vehicle Environment may be hosted on the CCS On-Board Safe Computing Platform.

Due to the increased performance of the CCS On-Board localisation through better sensor fusion algorithms, the use of GNSS localisation, digital map data, and augmentation data, the EURO Balise and EURO Loop readers are not needed anymore.

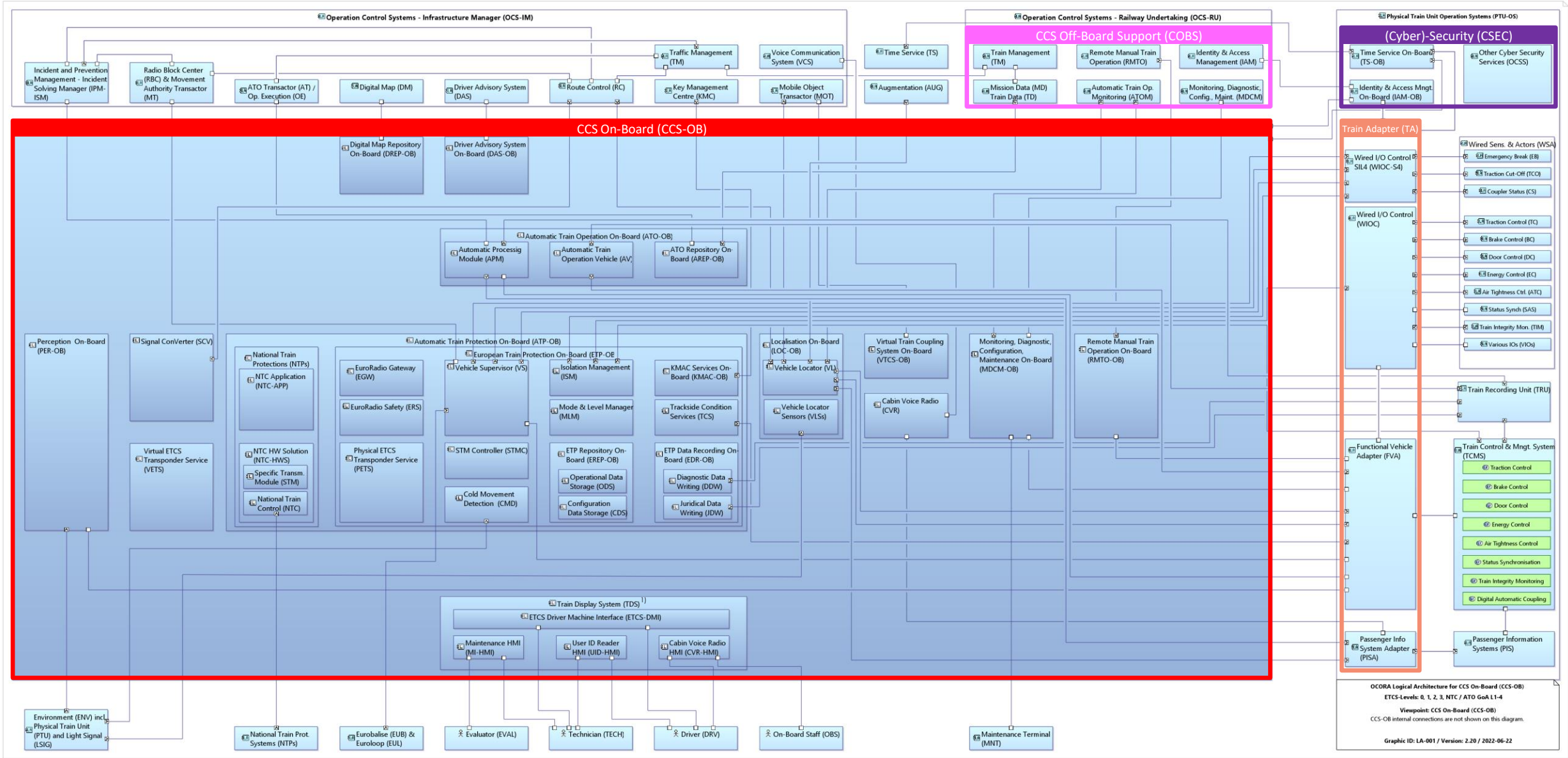
Step 4: integrating the CCS On-Board domain with the Vehicle Environment allows to reuse peripherals and applications throughout the whole train, reducing the level of hardware systems and applications needed on a train. This again will increase availability and will reduce maintenance

Step 4: eliminating the EURO Balise and EURO Loop readers further reduces the maintenance efforts and enables the infrastructure managers to implement changes more quickly.

OCORA Scope

OCORA-BWS02-030 / v2.20 / 24.06.2022

OCORA Scope – Logical Architecture

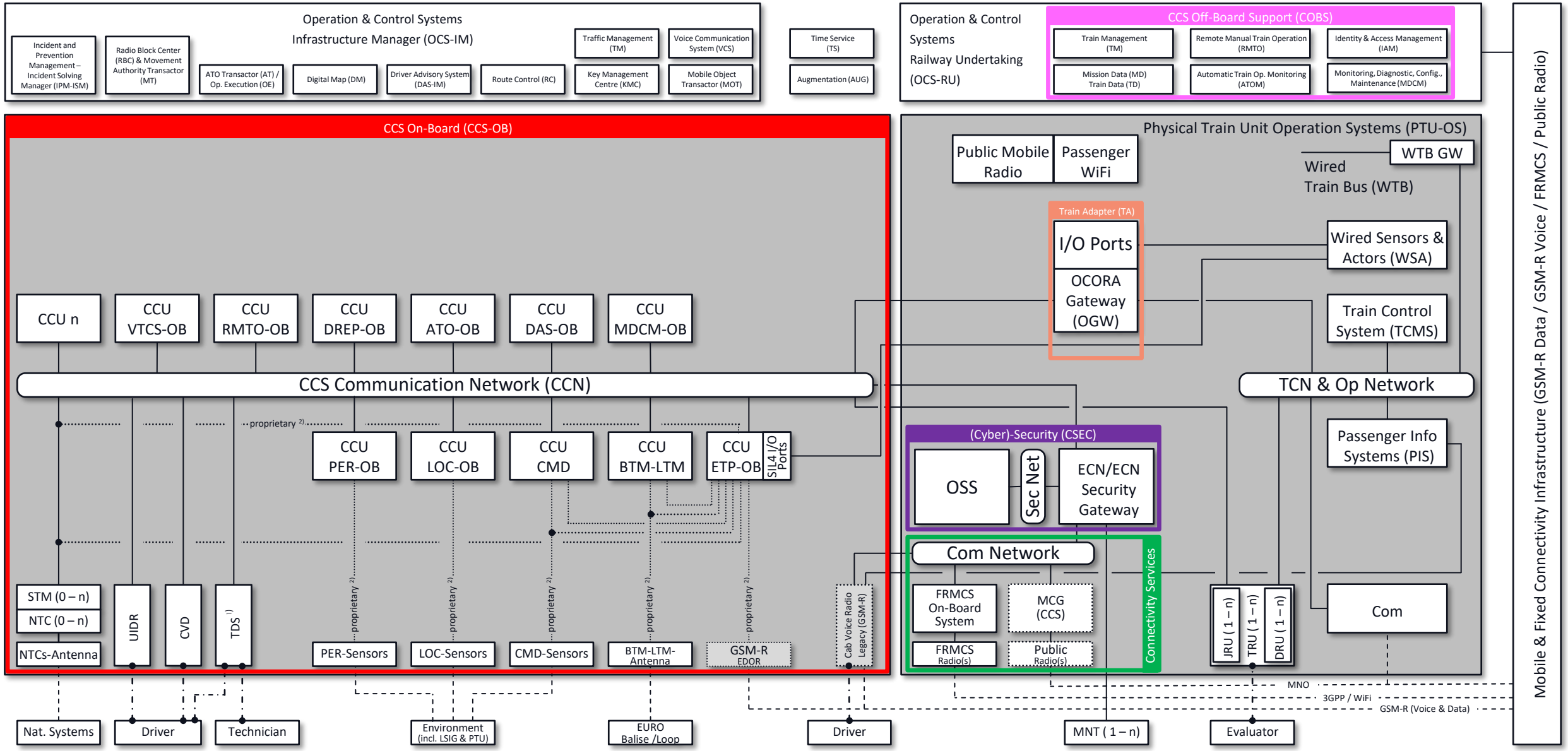


1) May be moved into the PTU-OS / LOC&PAS domain.

SS-nnn Respective subset contains information for the interface

SS-nnn* Respective subset does not address the interface but should contain the information in the future.

OCORA Scope – Physical Architecture (Legacy Train)

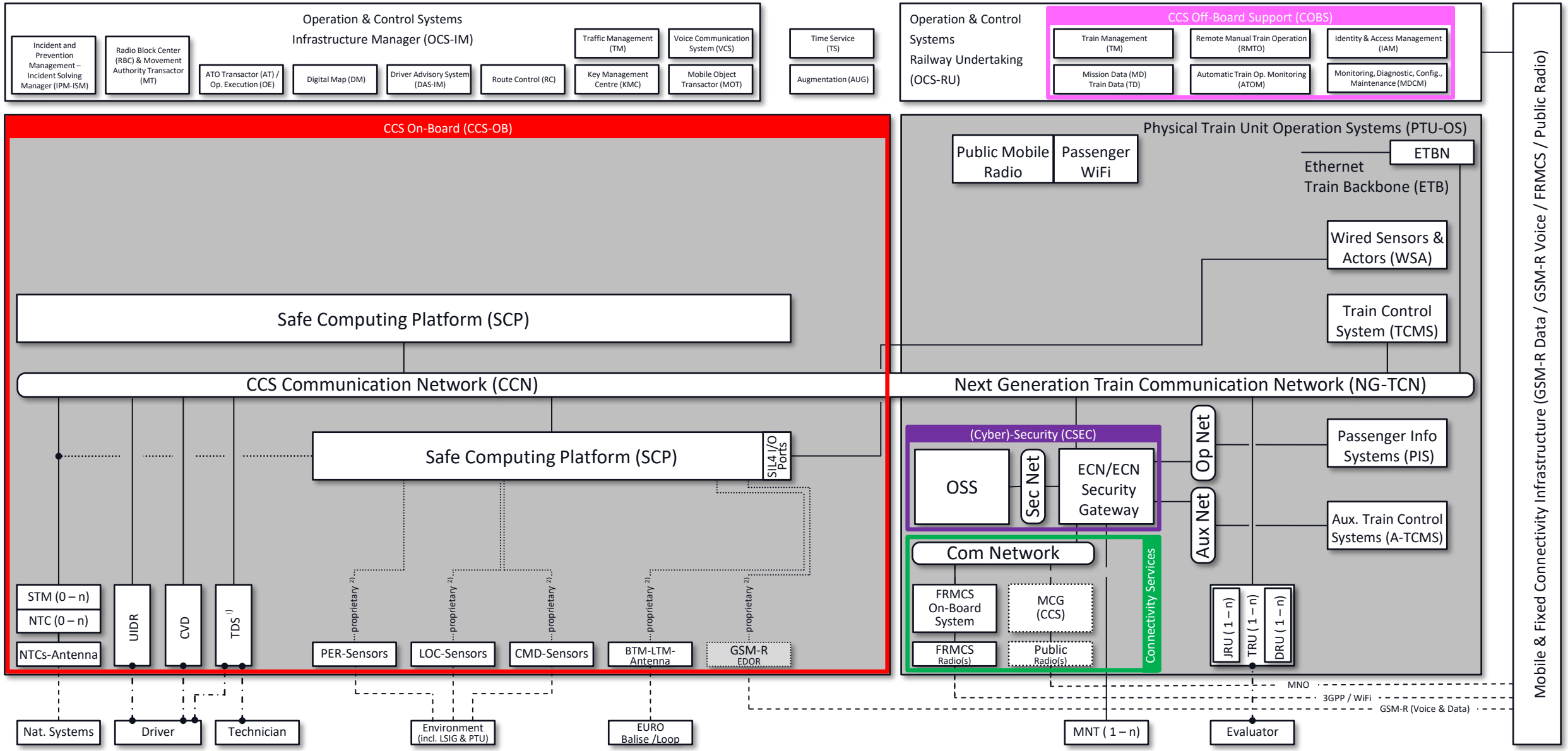


Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

OCORA Scope – Physical Architecture (New Generation Trains)



Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

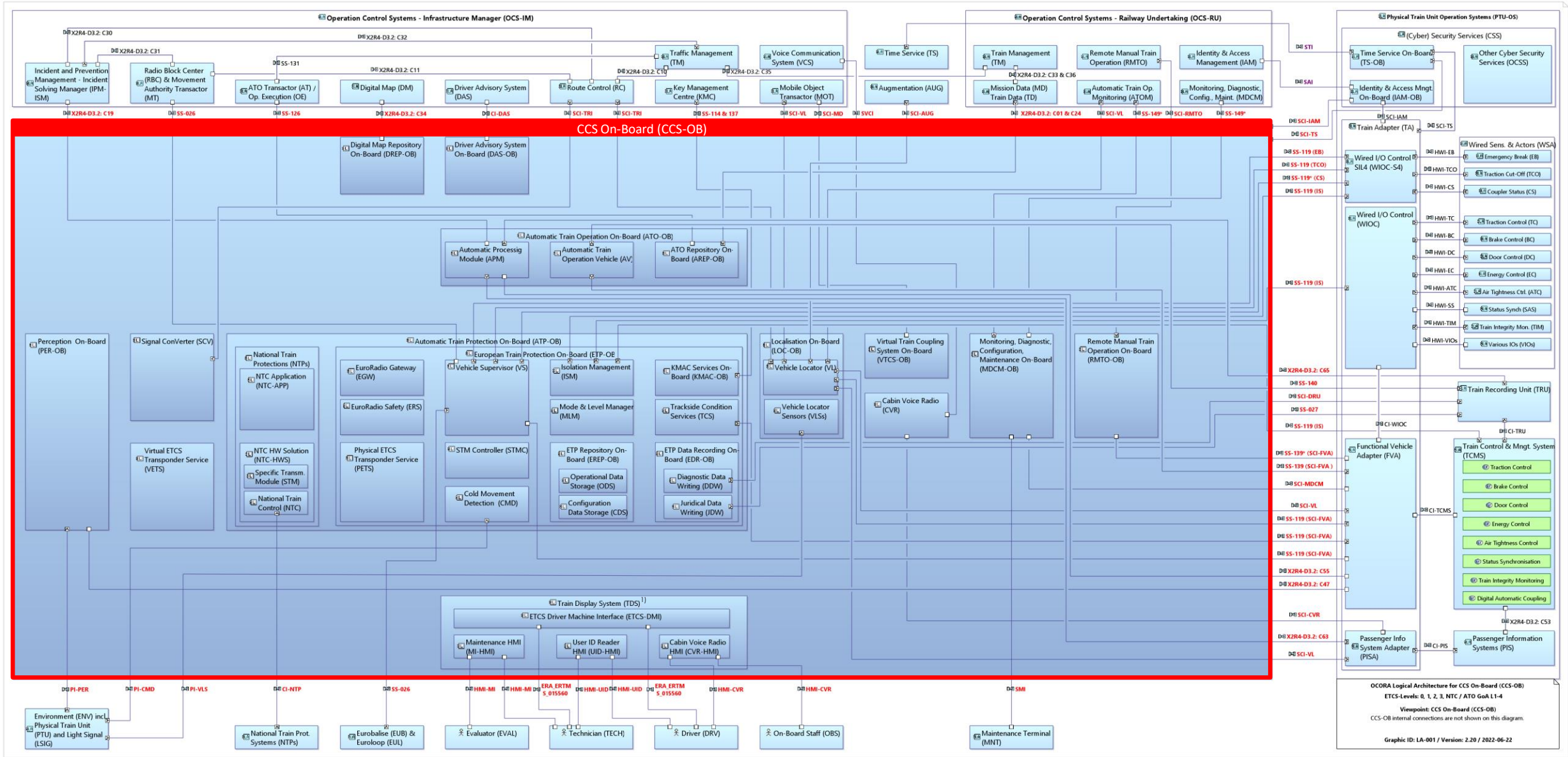
2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

CCS On-Board (CCS-OB)

Logical Architecture

OCORA-BWS02-030 / v2.20 / 24.06.2022

Logical Architecture CCS-OB Actors, External Interfaces, Functional Components



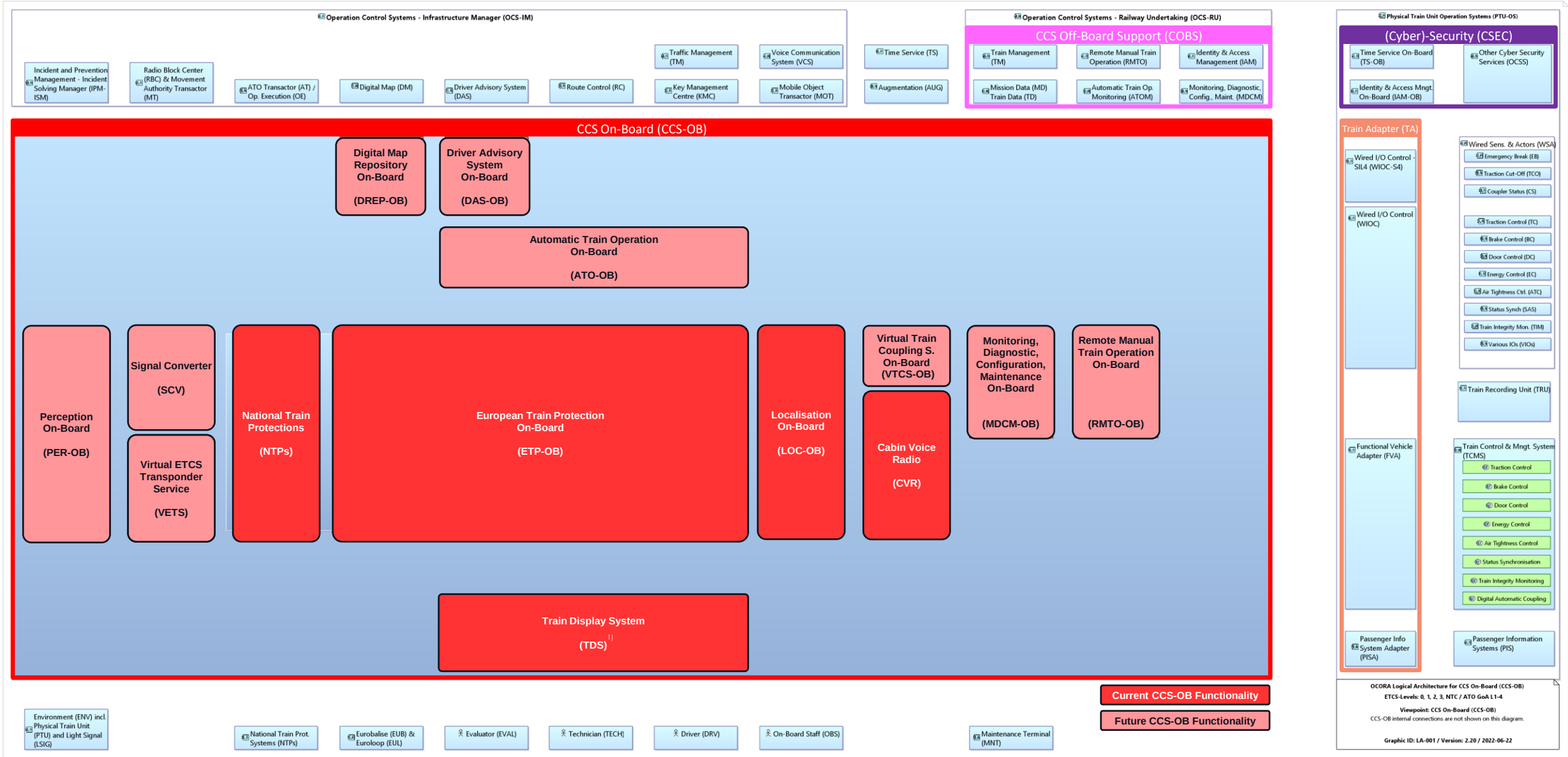
1) May be moved into the PTU-OS / LOC&PAS domain.

1) May be moved into the PTU-OS / LOC&PAS domain.

SS-nnn Respective subset contains information for the interface

SS-nnn* Respective subset does not address the interface but should contain the information in the future.

Logical Architecture CCS-OB Functional Clustering for Building Block Assignment



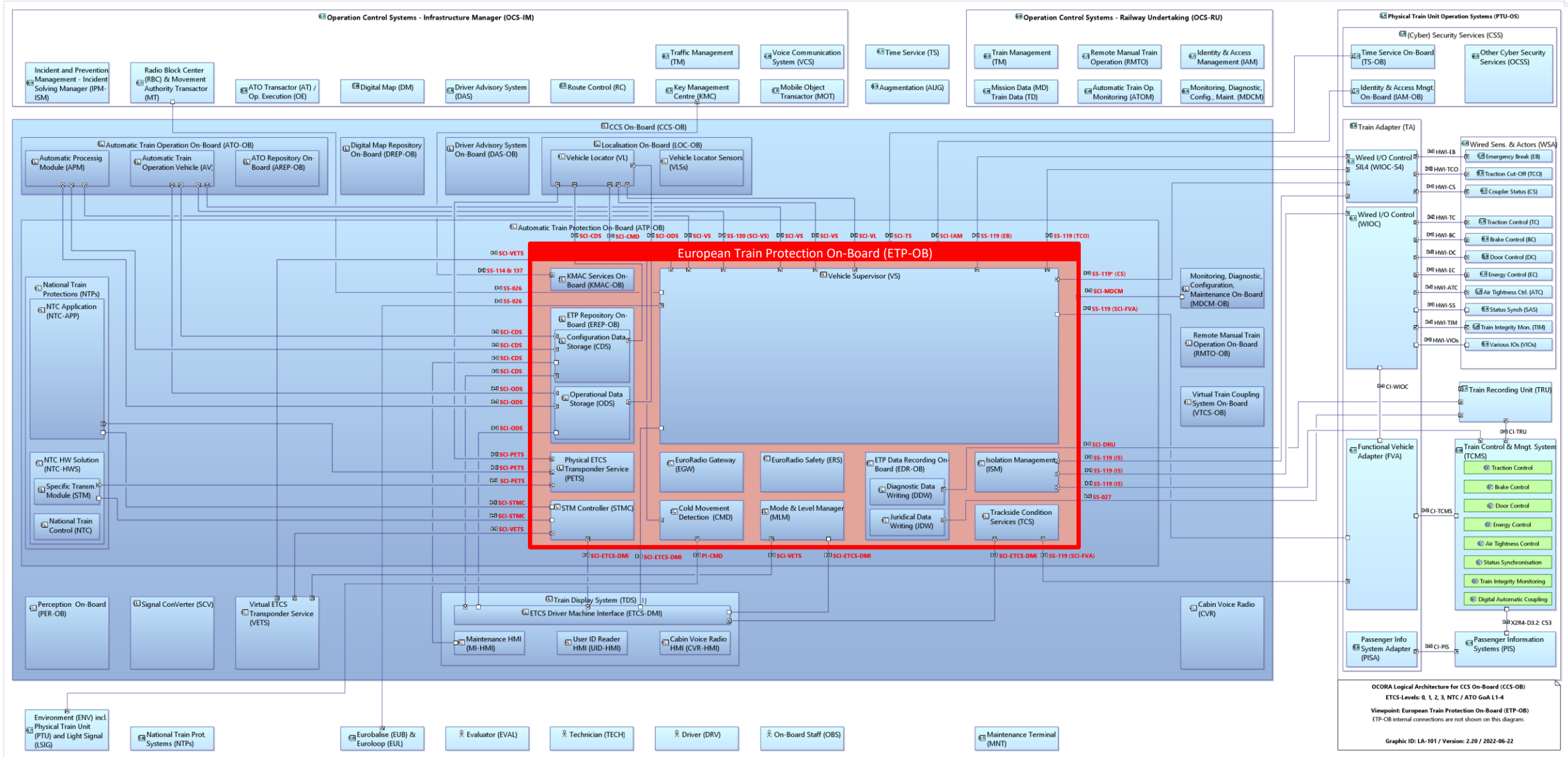
1) May be moved into the PTU-OS / LOC&PAS domain.

1) May be moved into the PTU-OS / LOC&PAS domain.

SS-nnn Respective subset contains information for the interface

SS-nnn* Respective subset does not address the interface but should contain the information in the future.

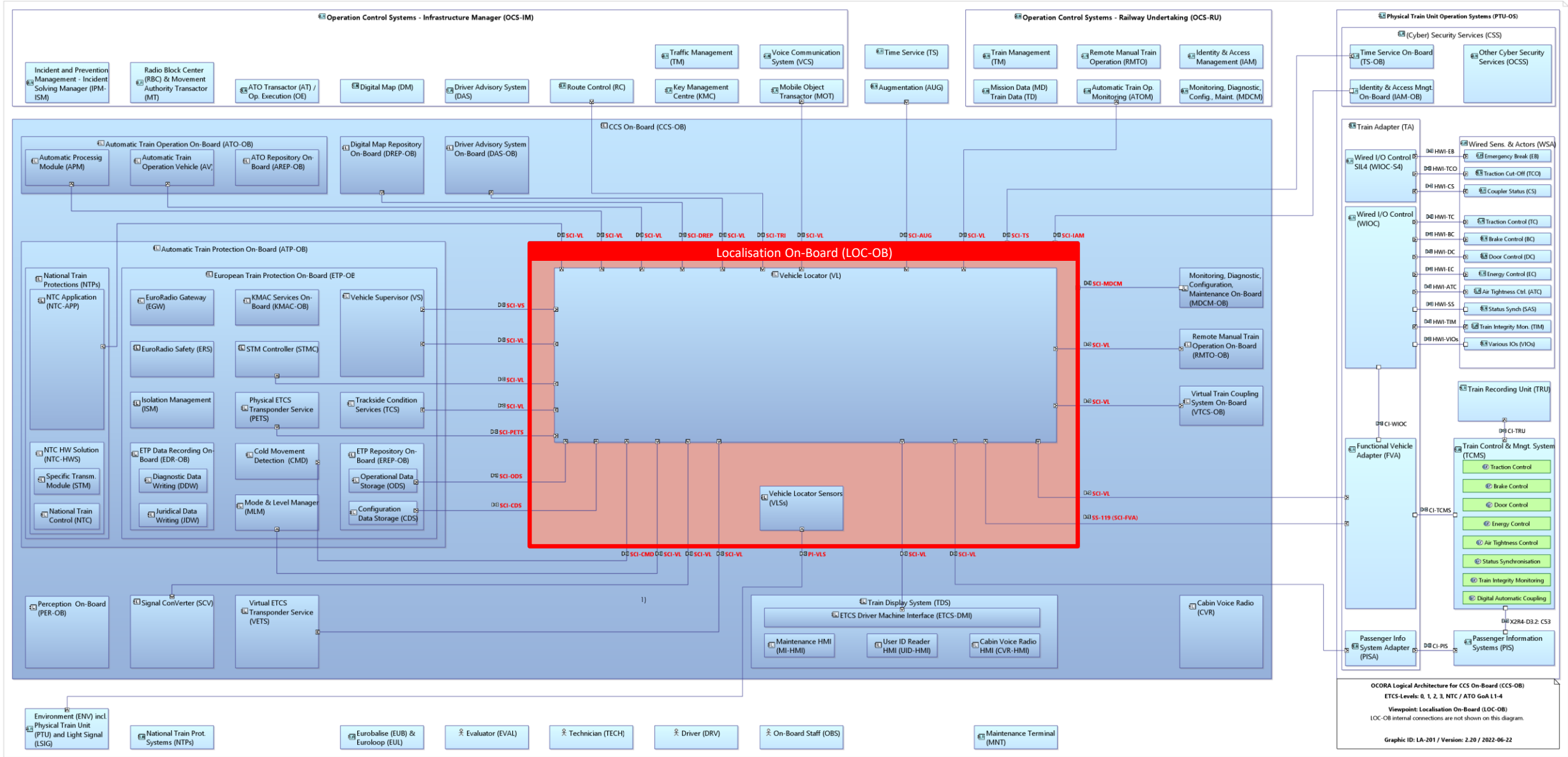
Logical Architecture ETP-OB Actors, External Interfaces, Components



1) May be moved into the PTU-OS / LOC&PAS domain.

1)	May be moved into the PTU-OS / LOC&PAS domain.
SS-nnn	Respective subset contains information for the interface
SS-nnn*	Respective subset does not address the interface but should contain the information in the future.

Logical Architecture LOC-OB Actors, External Interfaces, Components



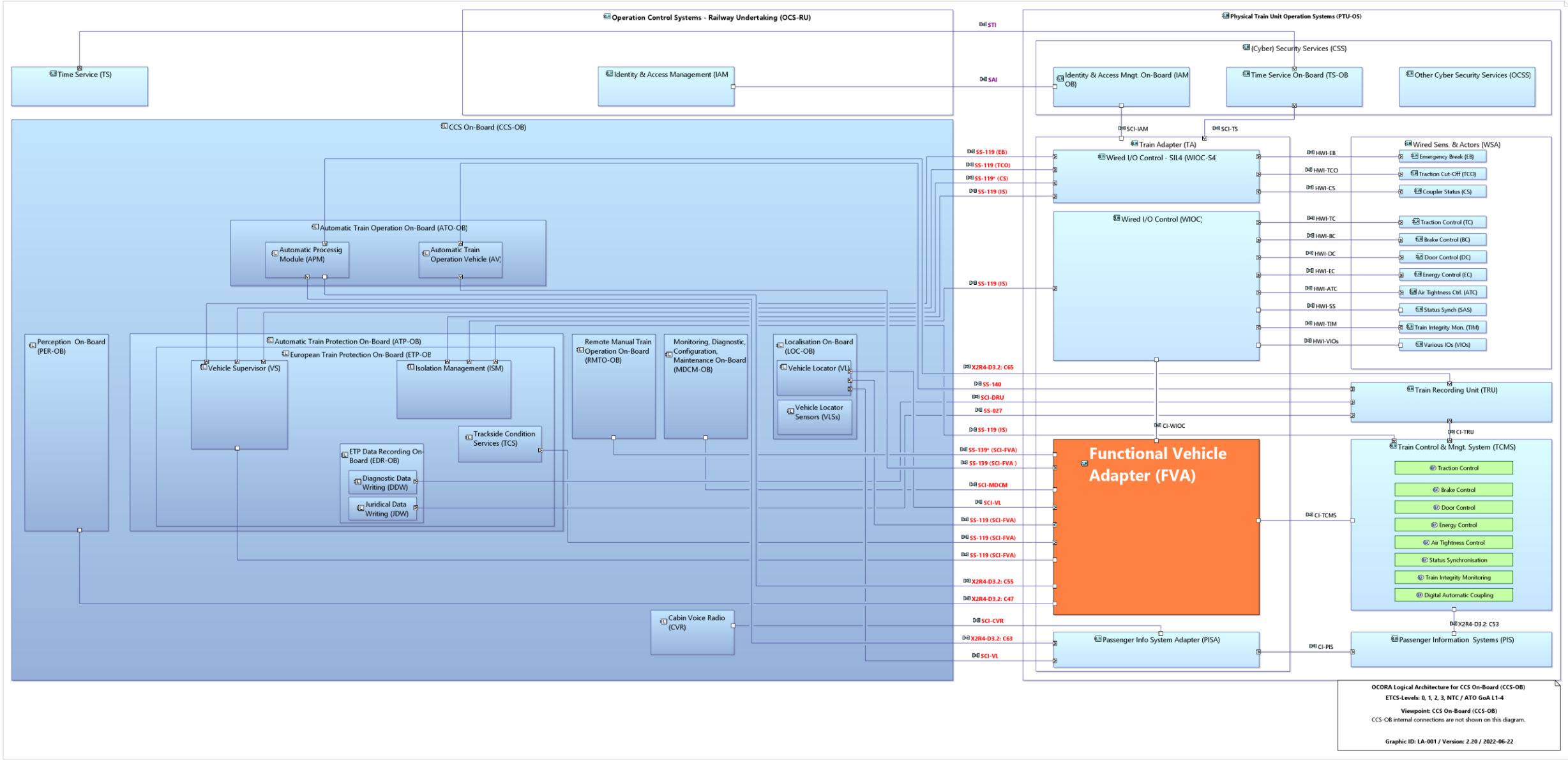
1) May be moved into the PTU-OS / LOC&PAS domain.

1) May be moved into the PTU-OS / LOC&PAS domain.

SS-nnn Respective subset contains information for the interface

SS-nnn* Respective subset does not address the interface but should contain the information in the future.

Logical Architecture FVA Actors and External Interfaces



1) May be moved into the PTU-OS / LOC&PAS domain.

1) May be moved into the PTU-OS / LOC&PAS domain.

SS-nnn Respective subset contains information for the interface

SS-nnn* Respective subset does not address the interface but should contain the information in the future.

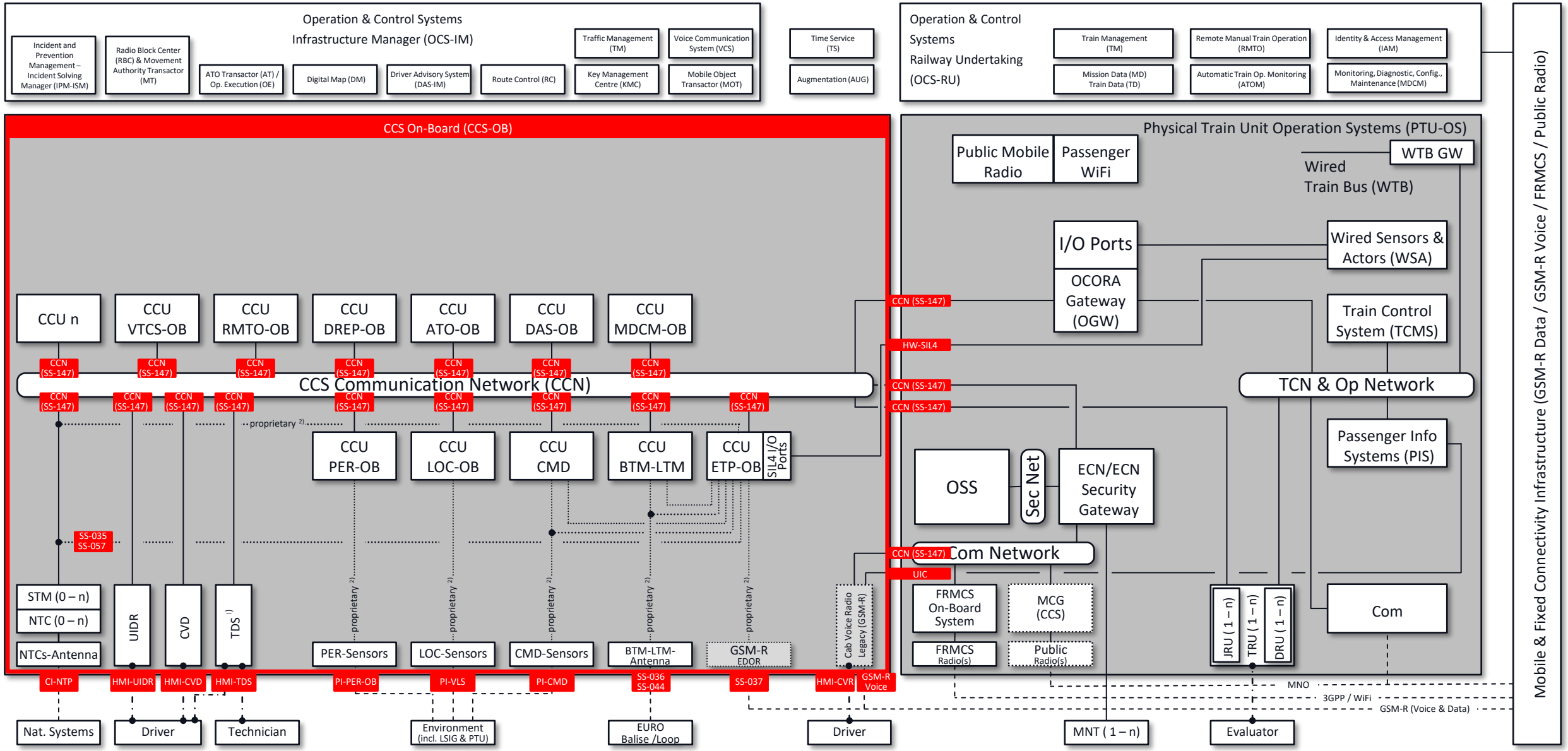
CCS On-Board (CCS-OB)

Physical Architecture

OCORA-BWS02-030 / v2.20 / 24.06.2022

Physical Architecture CCS-OB – Legacy Train

Actors, Interfaces, Hardware Components

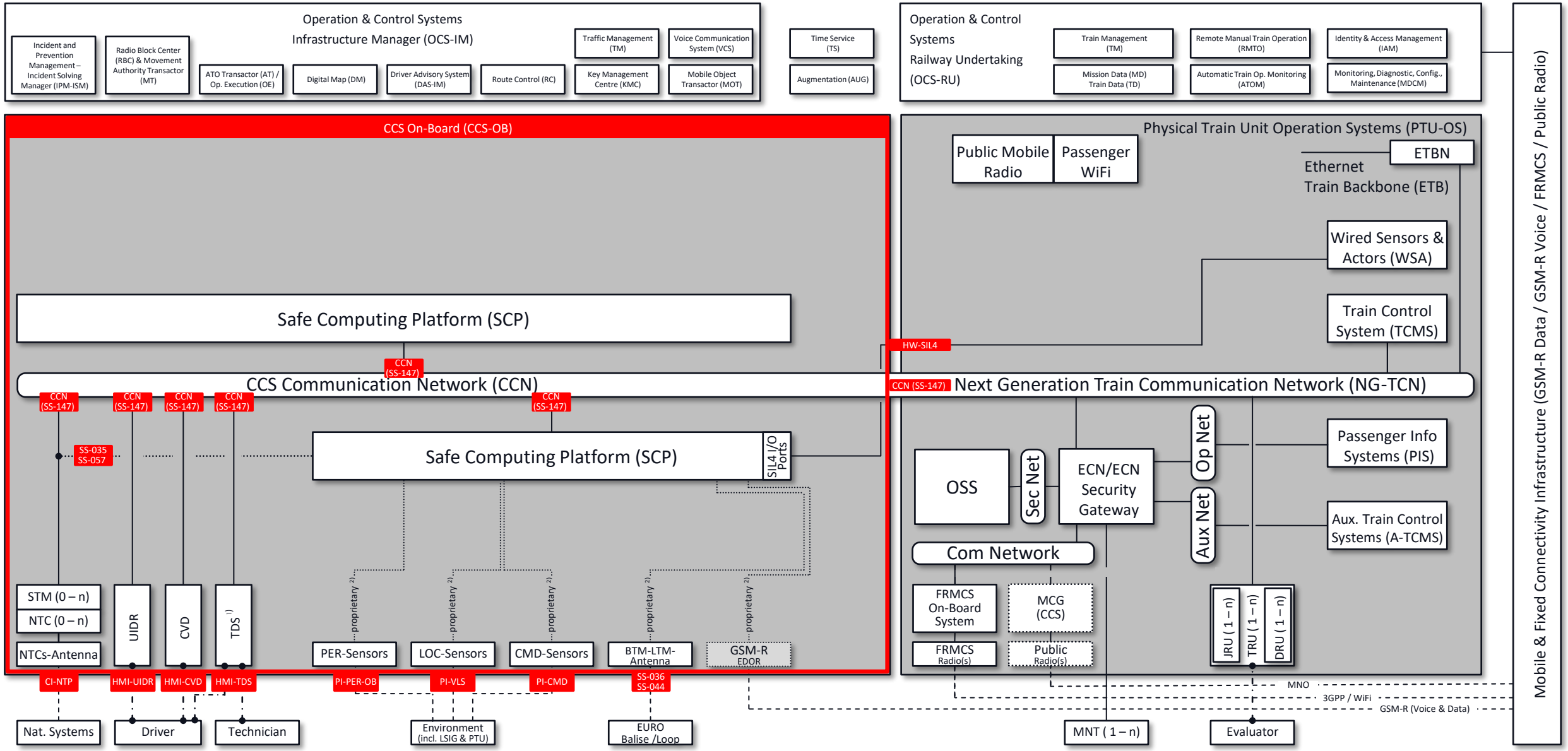


Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

Physical Architecture CCS-OB – NG Train Actors, Interfaces, Hardware Components



Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

Building Blocks

OCORA-BWS02-030 / v2.20 / 24.06.2022

Building Blocks

Definition

A building block is a sourceable unit of the CCS on-board system (hardware and/or software), having standardised functionality, standardised performance (RAM), standardised safety (including Tolerable Functional Failure Rate [TFFR], Safety Integrity Level [SIL] and Safety Related Application Conditions [SRAC]), standardised security and standardised interfaces towards other building blocks and/or external systems.

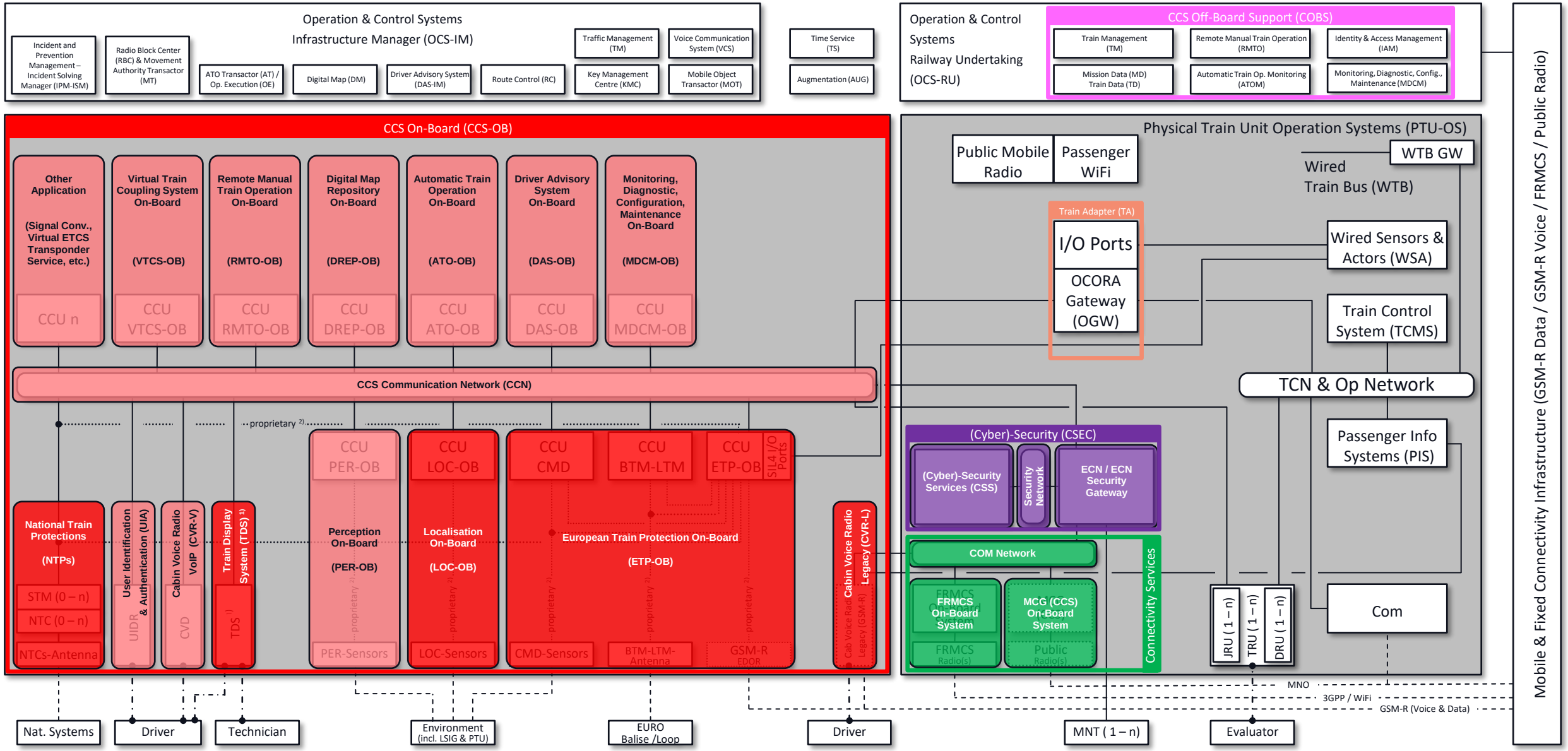
Combined HW/SW Building blocks exclusively communicating with each other through the CCS Communication Network (CCN) through standardise interfaces.

SW Building blocks, deployed on an instance of the generic Safe Computing Platform, shall communicate with each other through the standardised platform independent Application Programming Interface (API). Communication with computing platform external systems will be realised by the computing platform (integrating with the CCN).

Building blocks are modifiable / adaptable and therefore portable / replaceable, without impacting other building blocks.

Scenario 1

Building Blocks without Safe Computing Platform (dedicated hardware for each functional cluster)
Legacy Train Example



Current CCS-OB Functionality

Future CCS-OB Functionality

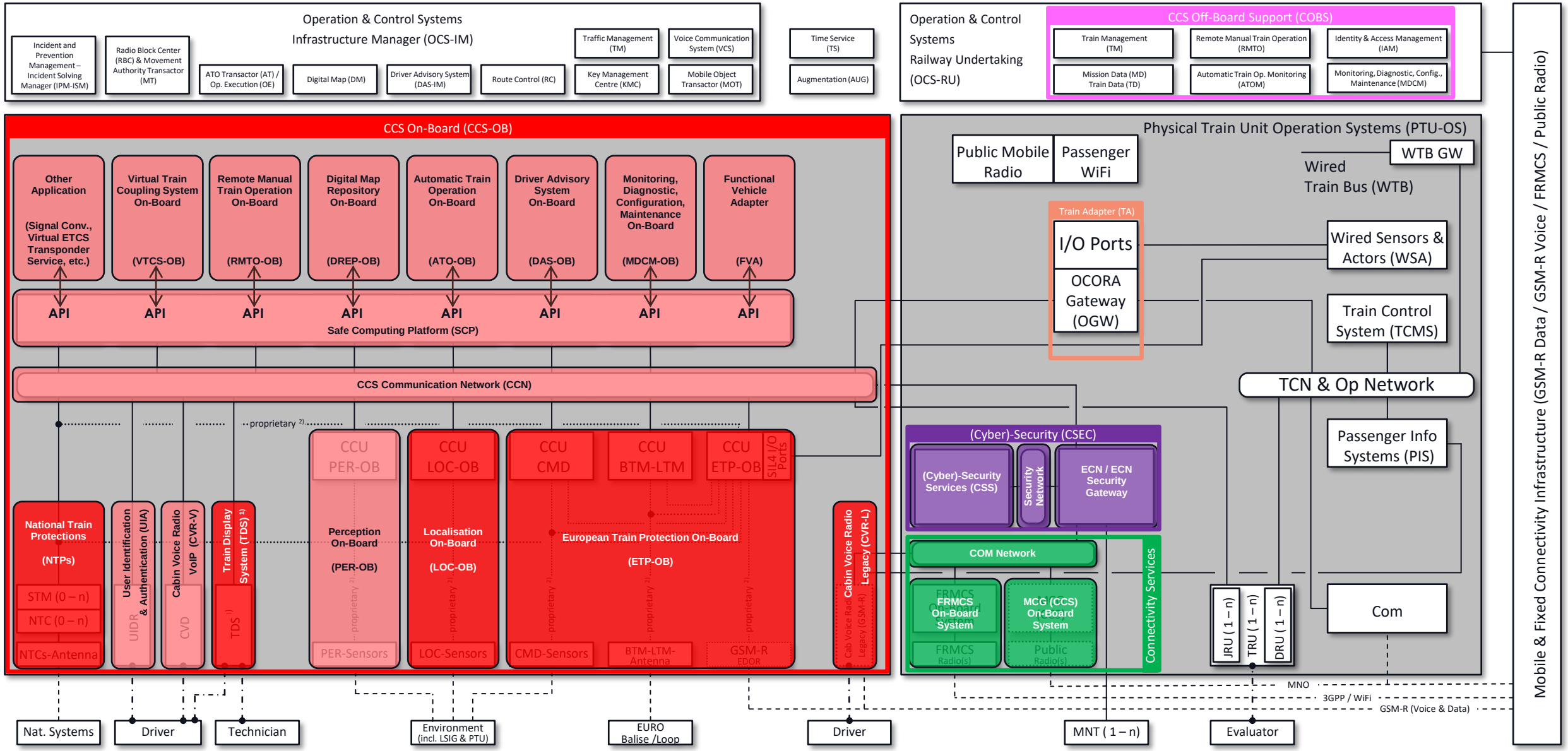
Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

Scenario 2

Building Blocks with Safe Computing Platform for some Applications
Legacy Train Example



Current CCS-OB Functionality | Future CCS-OB Functionality

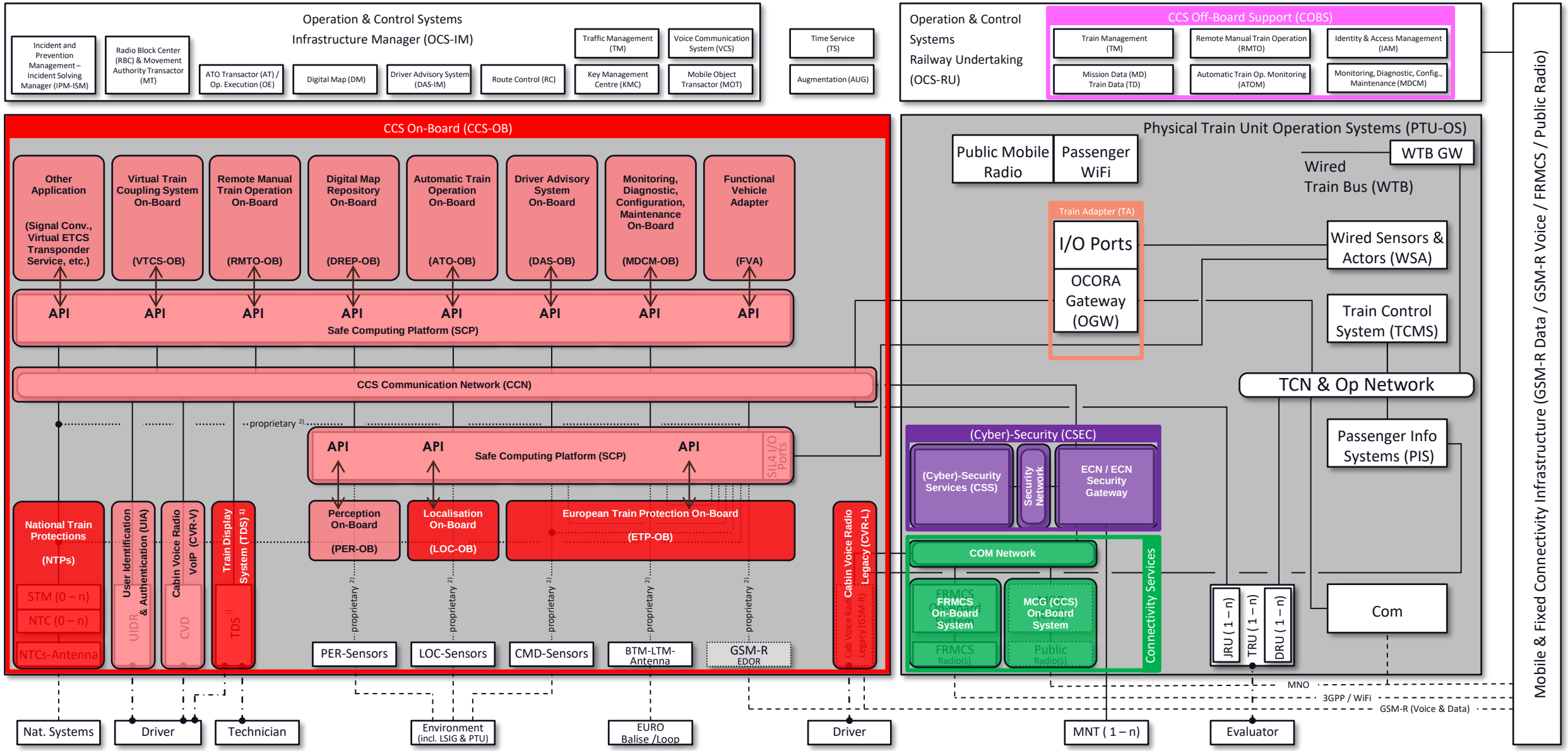
Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

Scenario 3

Building Blocks with Safe Computing Platform for all Applications
Legacy Train Example



Current CCS-OB Functionality | Future CCS-OB Functionality

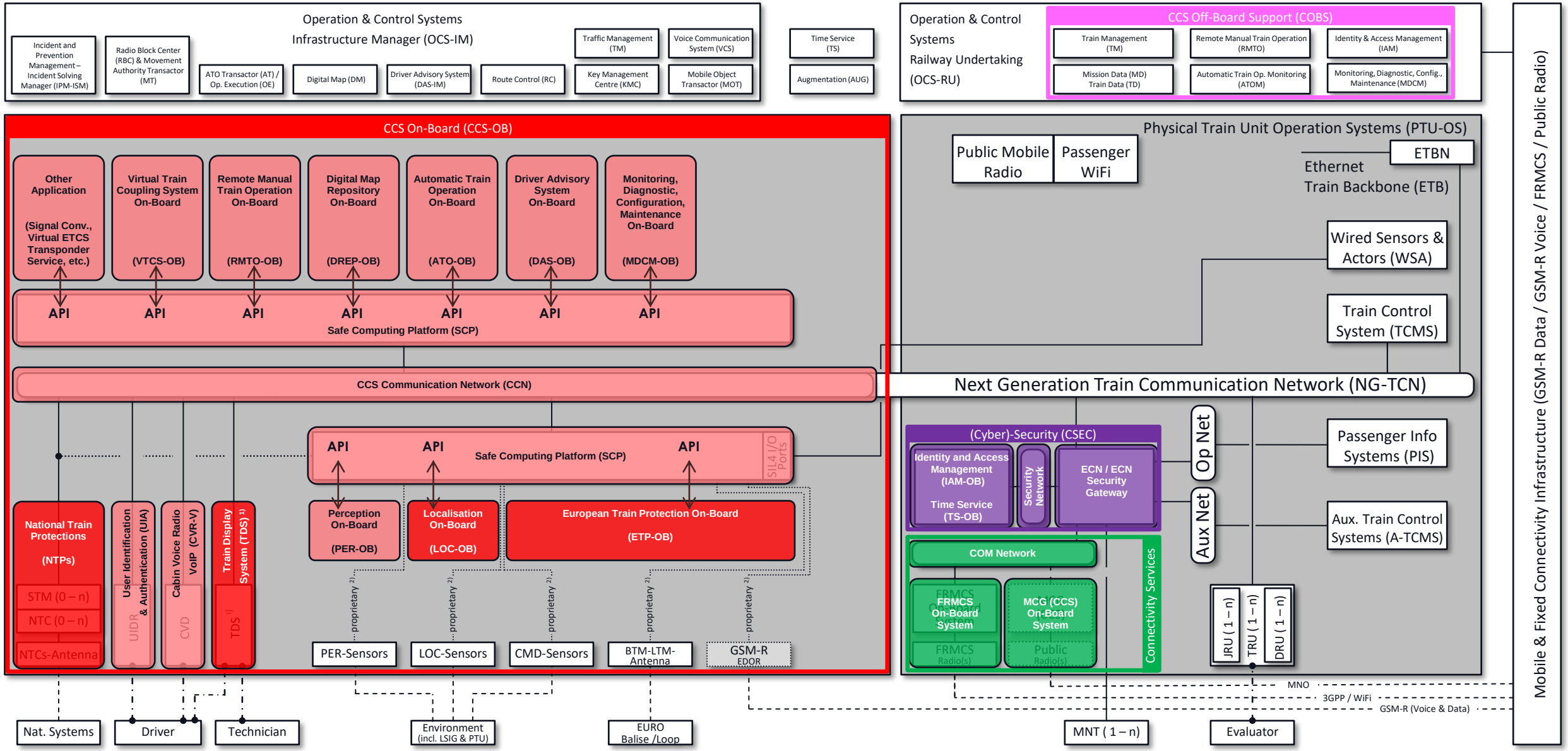
Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

Scenario 4

Building Blocks with Safe Computing Platform for all Applications
New Generation Train Example



Current CCS-OB Functionality | Future CCS-OB Functionality

Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

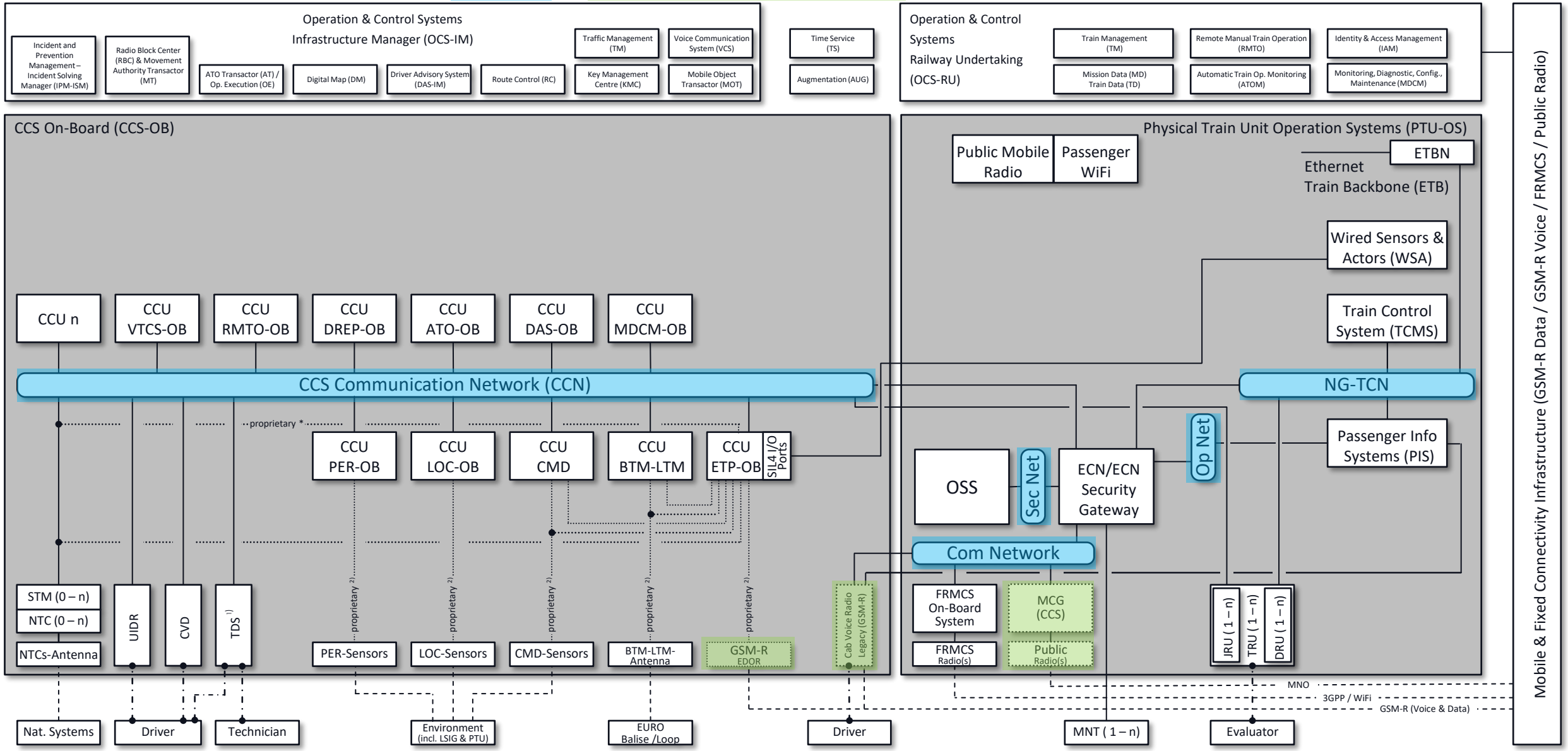
2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

Train Integration Scenarios

OCORA-BWS02-030 / v2.20 / 24.06.2022

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)



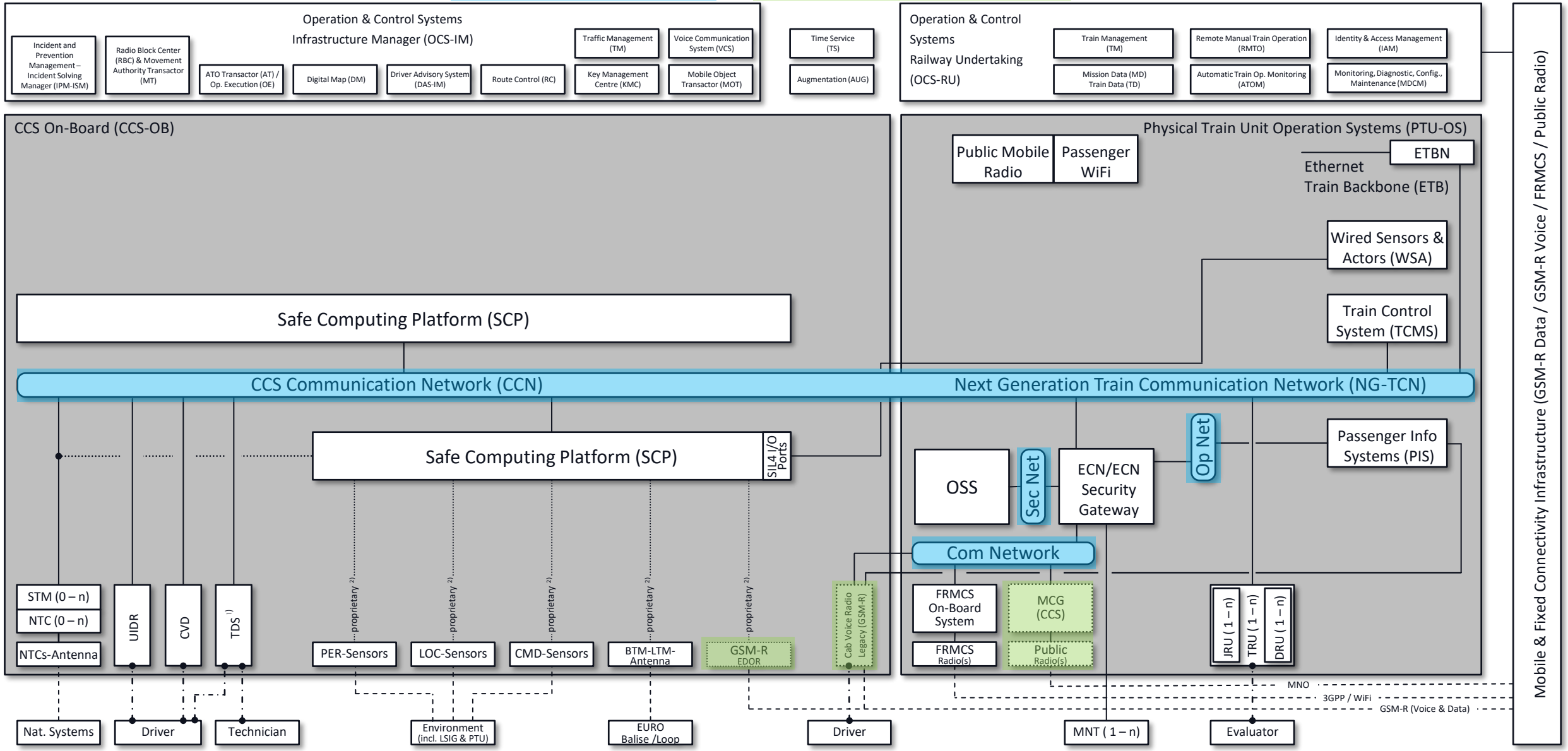
Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

NG-TCN Train – Scenario B

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



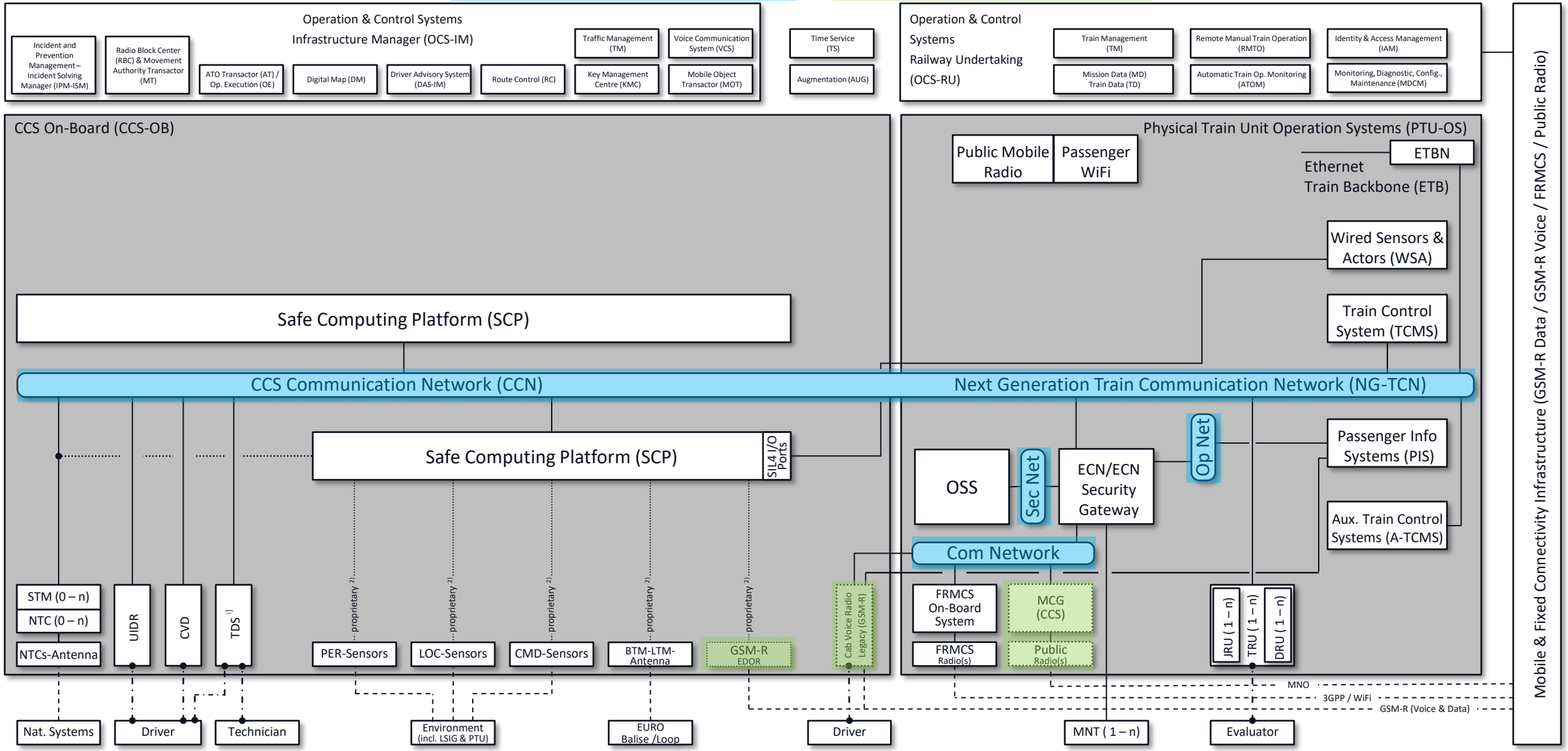
Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

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)



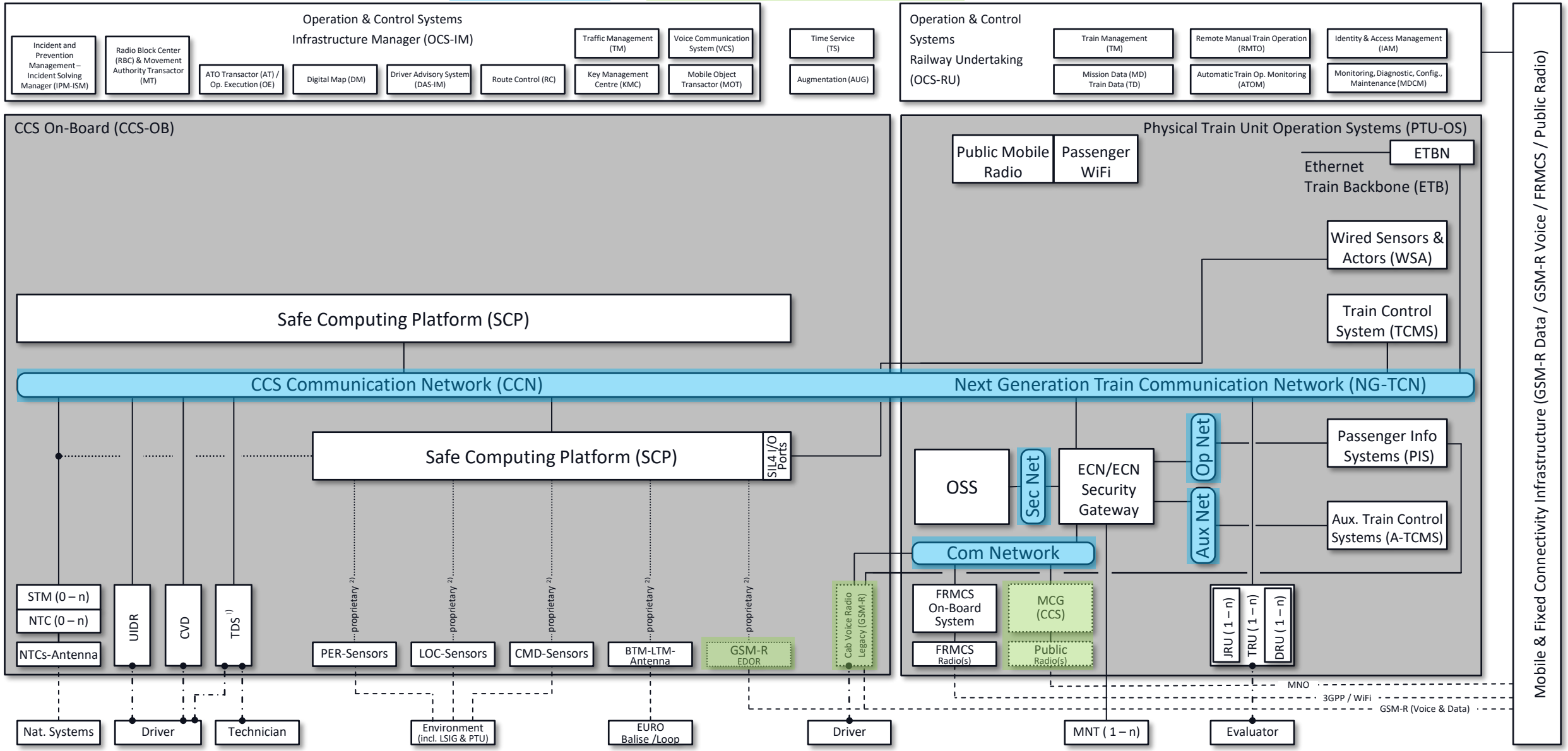
Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

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)



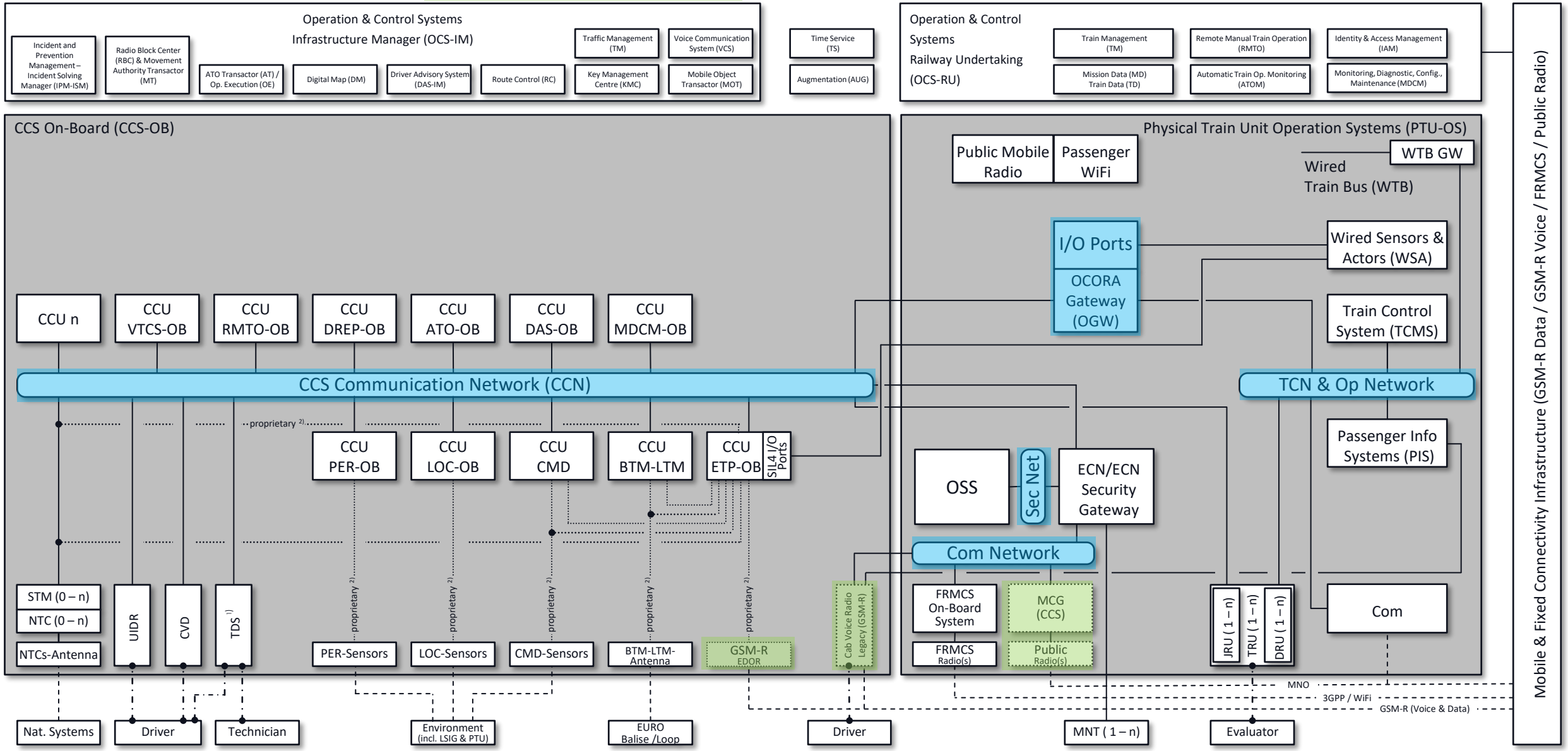
Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

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)



Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

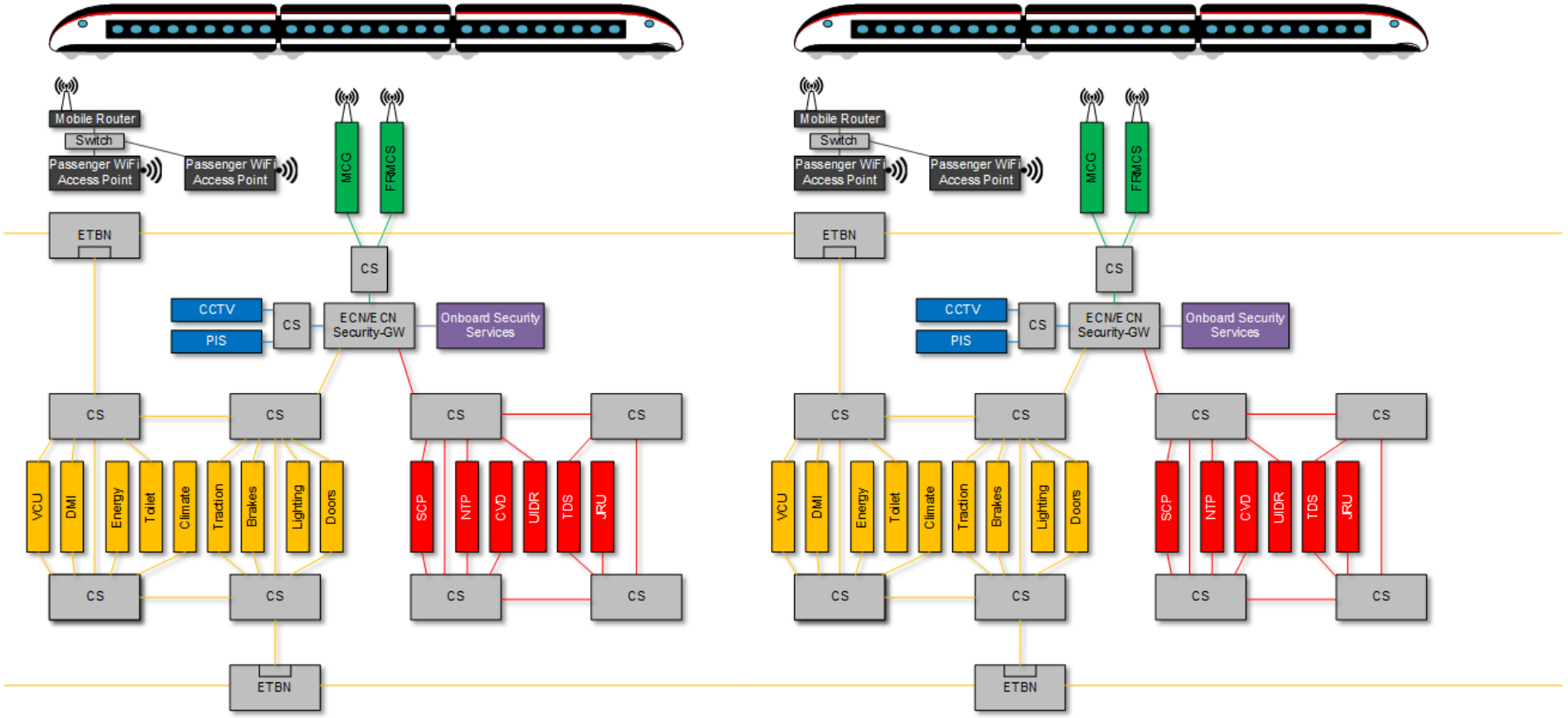
1) May be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

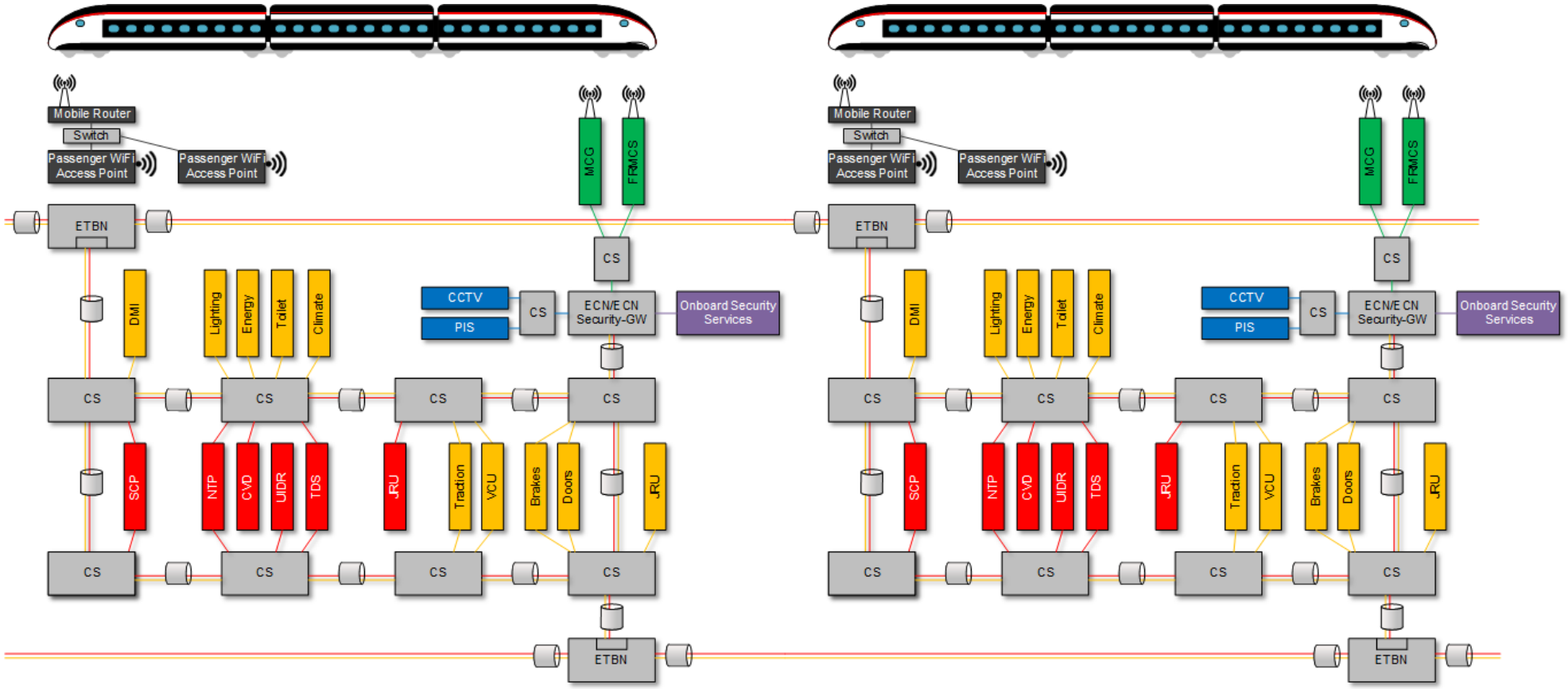
Network Topology Scenarios

OCORA-BWS02-030 / v2.20 / 24.06.2022

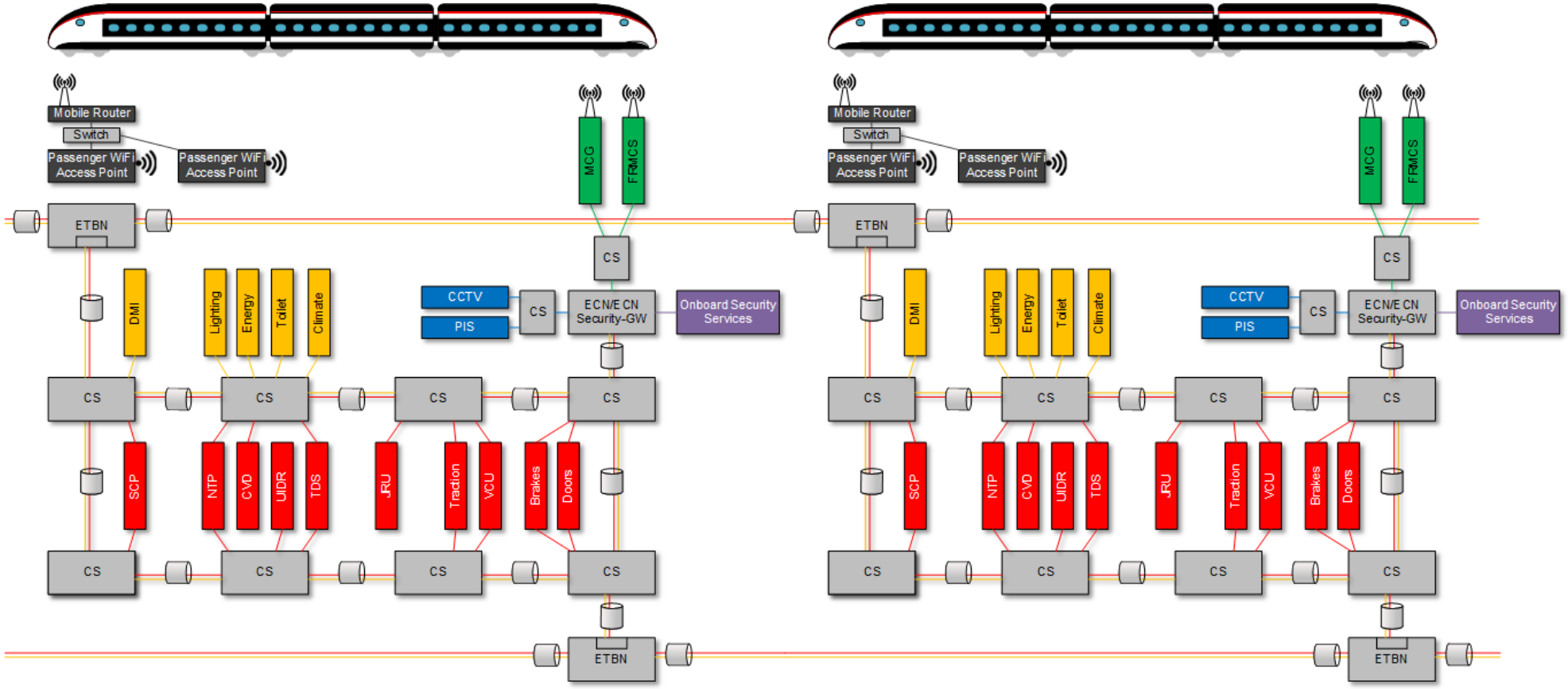
Scenario A: CCN as **physically** separated network



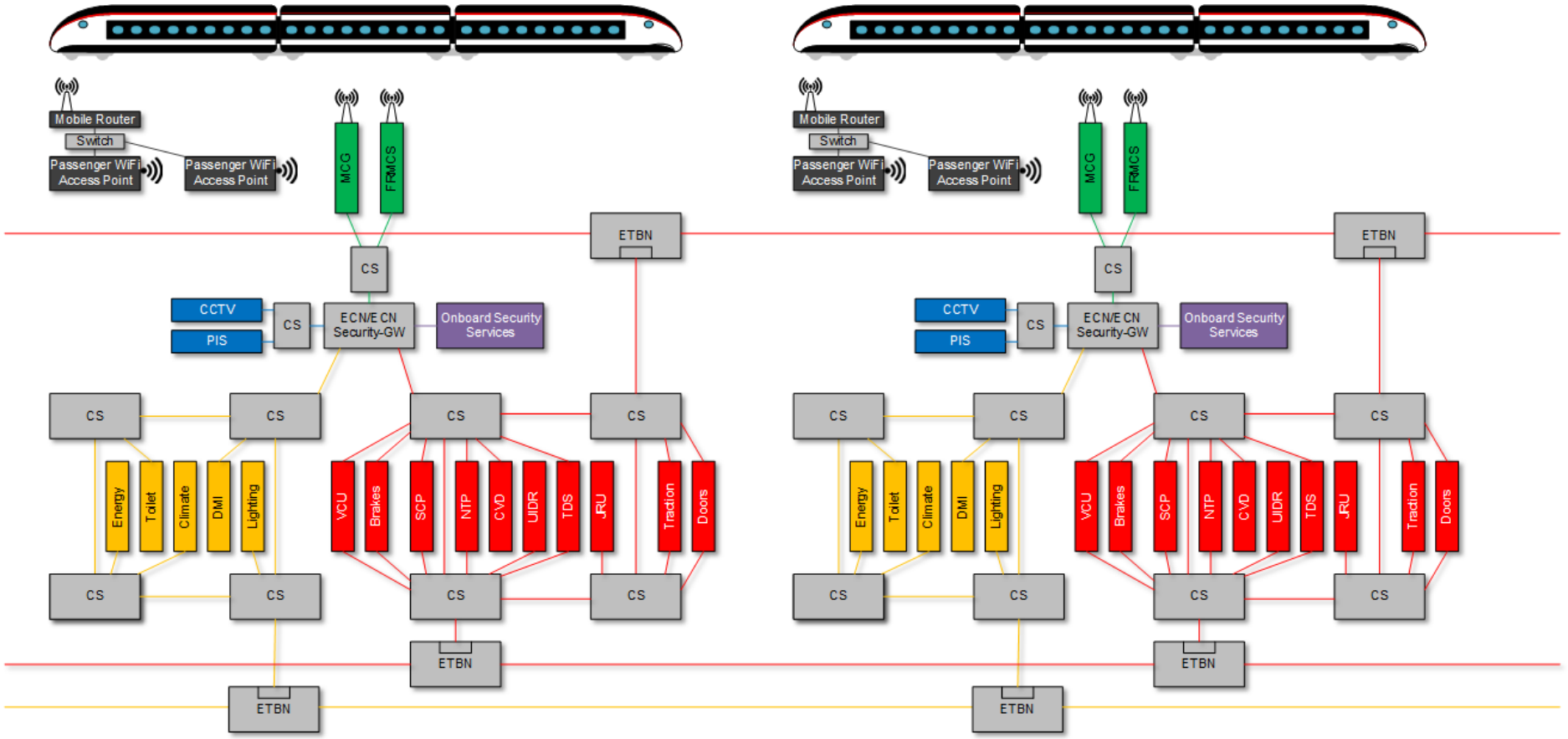
Scenario B: CCN as **logically** separated network



Scenario C: Common critical control network **logically** separated

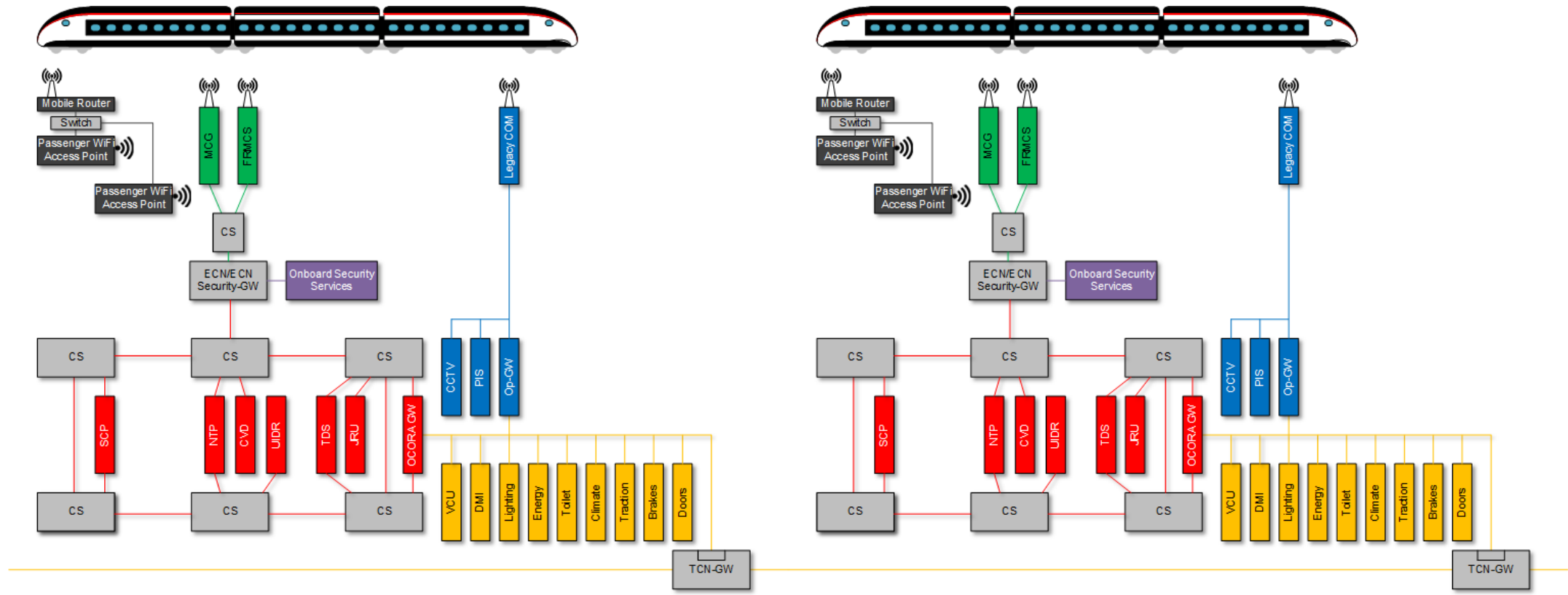


Scenario D: Common critical control network **physically** separated



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

Legacy Train – Integration with OCORA-GW



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

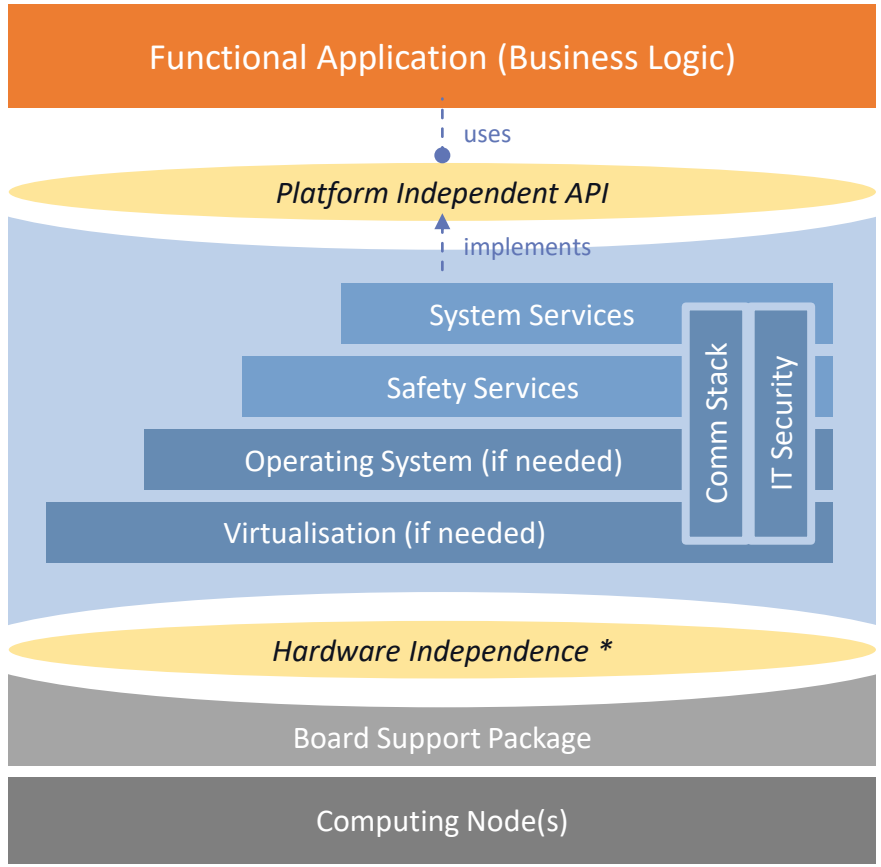
Remark: The network architecture of retrofit vehicles is only an example. Legacy architectures are always vehicle dependent and therefore the CCS integration is project specific.

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

Computing Platform

OCORA-BWS02-030 / v2.20 / 24.06.2022

Computing Platform – High Level Architecture



Runtime environment

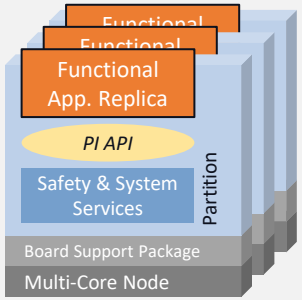
Hardware

Computing Platform

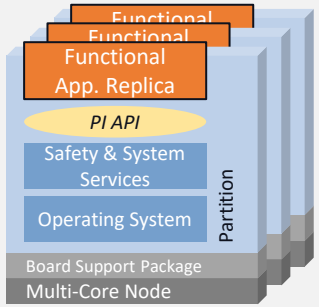
* It is to be discussed to which extent hardware independence can or should be enforced

Computing Platform – Deployment Options

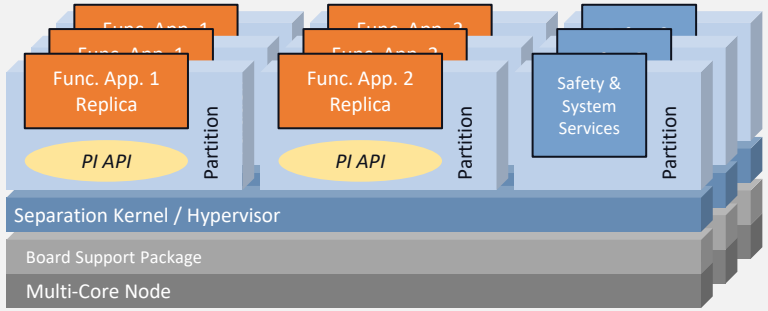
Option A:
Hardware without operating system



Option B:
Hardware with operating system

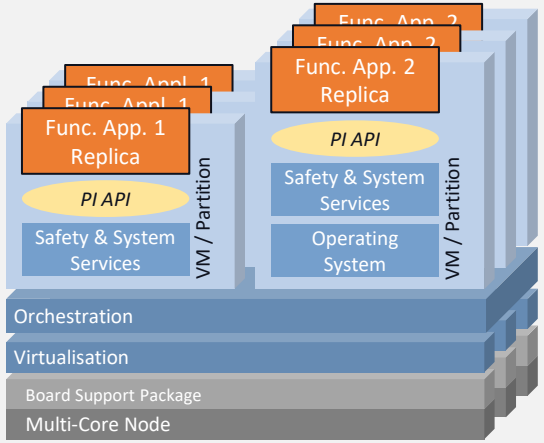


Option C:
Separation kernel / hypervisor based system



Likely options for ***onboard*** deployments

Option D:
Orchestrated virtualisation environment



Likely option for ***trackside*** deployments

Platform options where applications are programmed against PI API

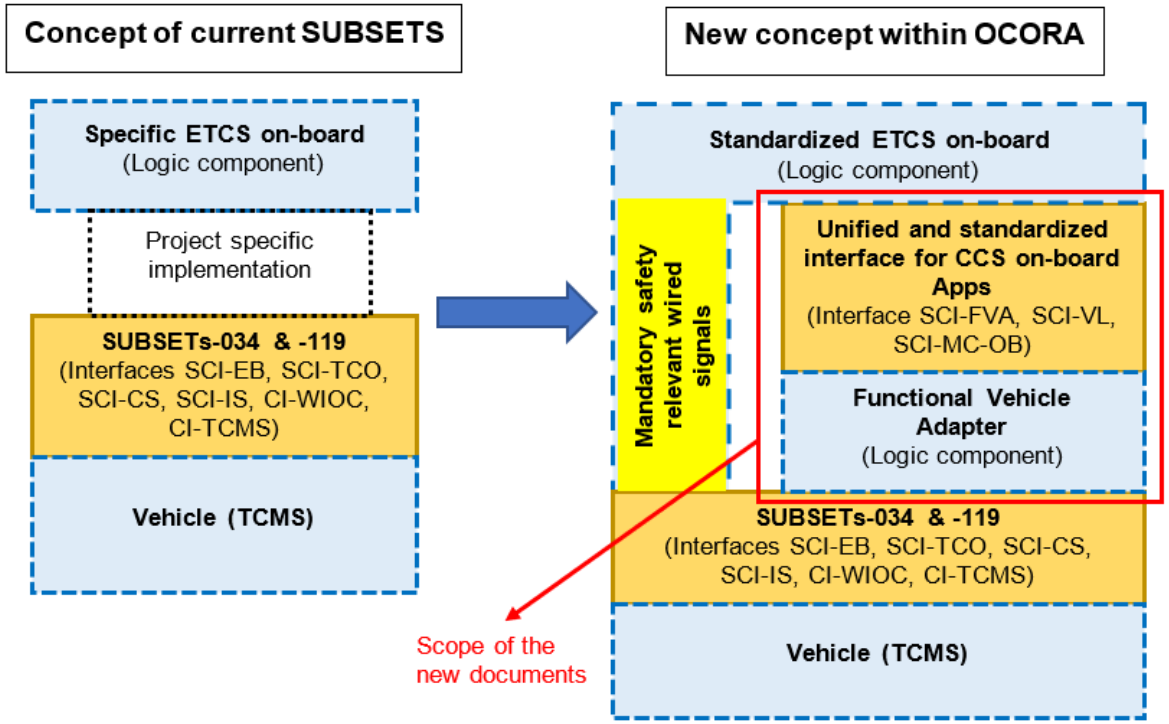
Approaches depicted in the diagram are non-exhaustive. The industry may propose different state-of-the-art solutions.

Functional Vehicle Adapter (FVA)

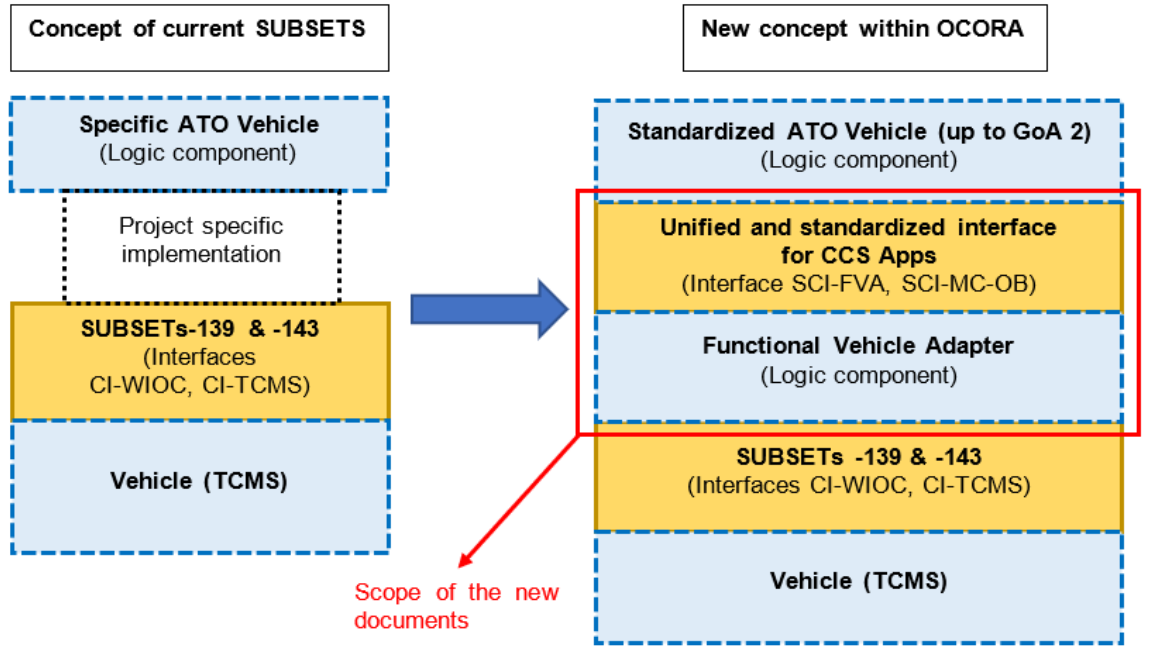
OCORA-BWS02-030 / v2.20 / 24.06.2022

OCORA – Functional Vehicle Adapter

ETCS



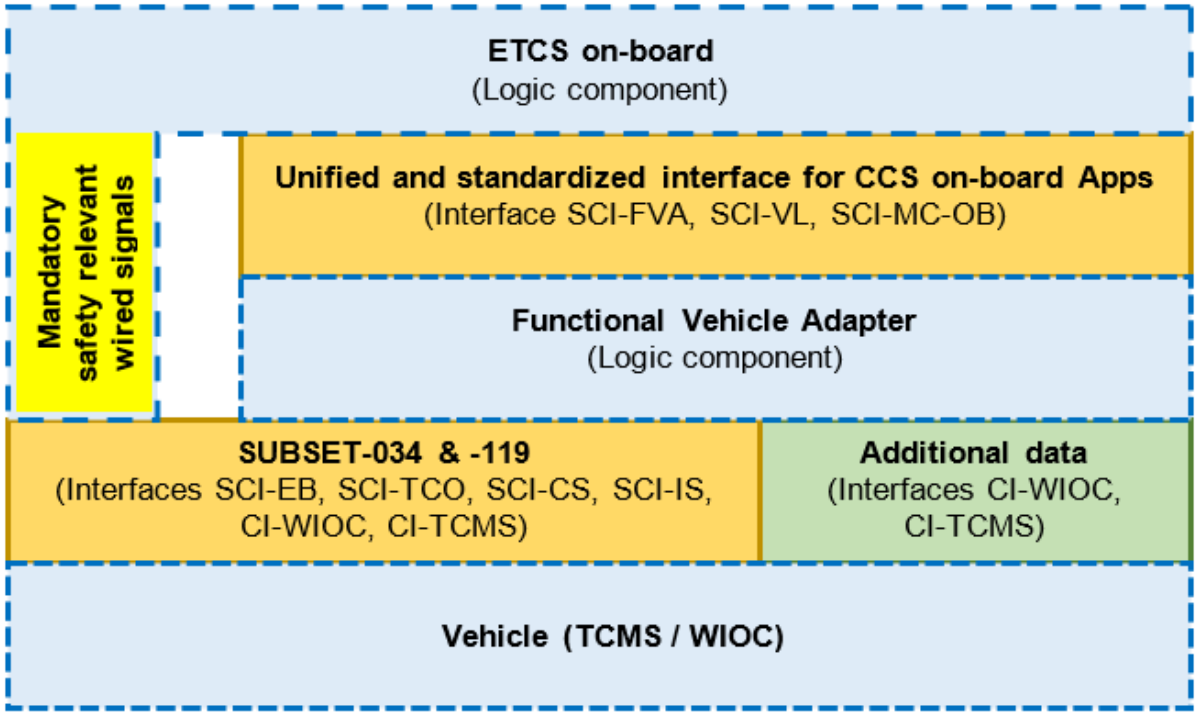
ATO



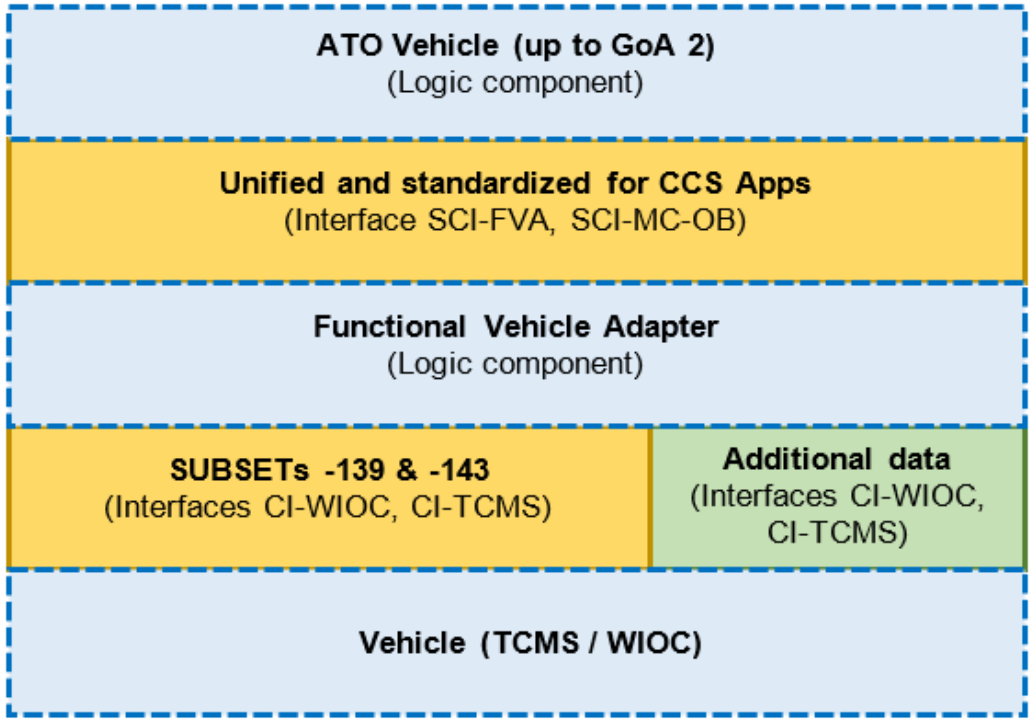
Details in Document: OCORA-TWS04-010 – Functional Vehicle Adapter - Introduction

OCORA – Functional Vehicle Adapter: Extensions

ETCS



ATO



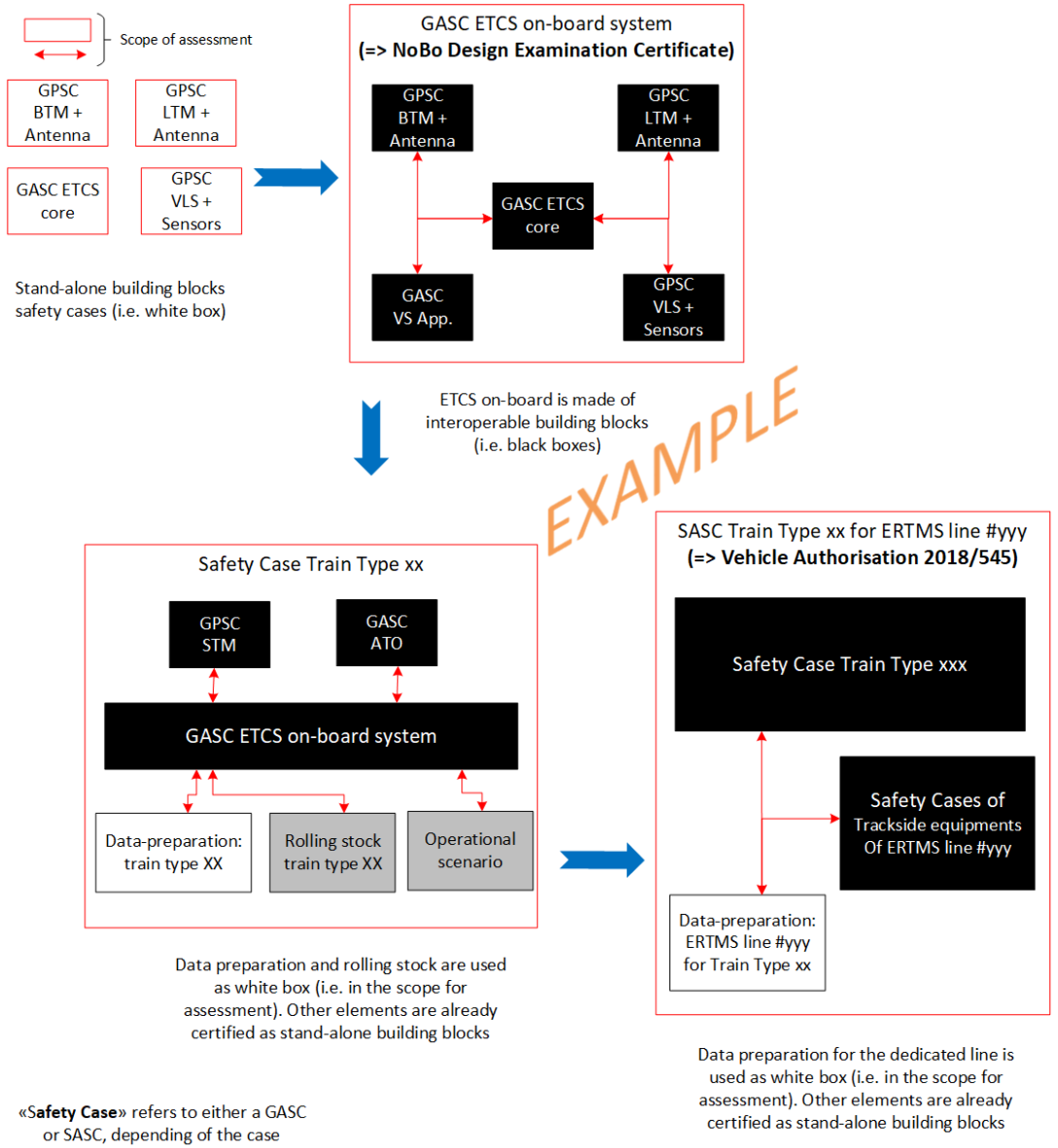
Details in Documents: OCORA-TWS04-013 – Design Guideline

Modular Safety

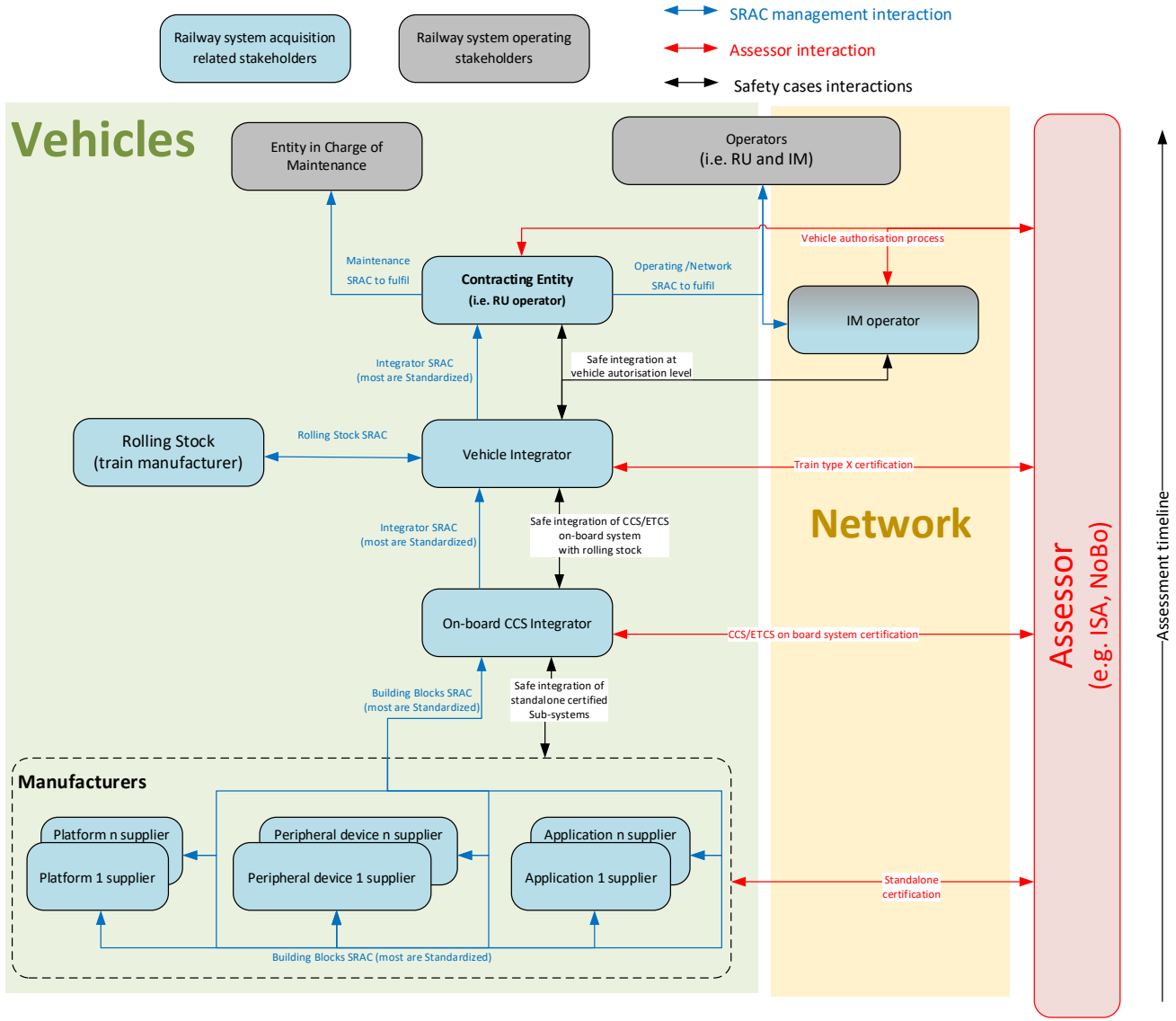
OCORA-BWS02-030 / v2.20 / 24.06.2022

OCORA – Modular Safety

- 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



OCORA – Modular Safety - Stakeholders



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

➔ Contracting entities (Oprators)

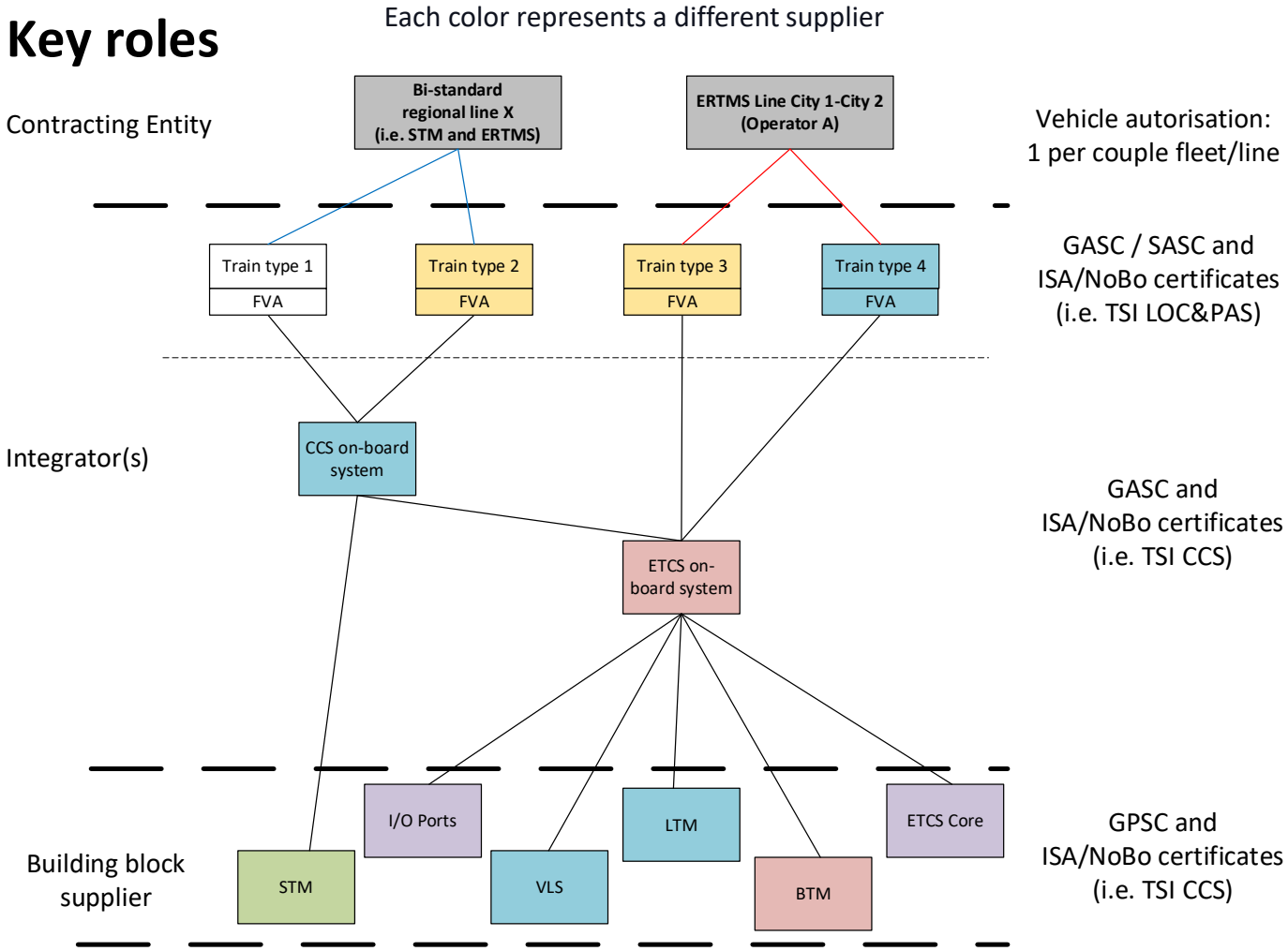
➔ Integrator(s)

➔ Manufacturers (Building Blocks, Application…)

➔ Other (ISA/ NoBo, DeBo..)

OCORA – Modularity & Safety Approval

Key roles



Case of two independent systems made of building blocks from different suppliers

- 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

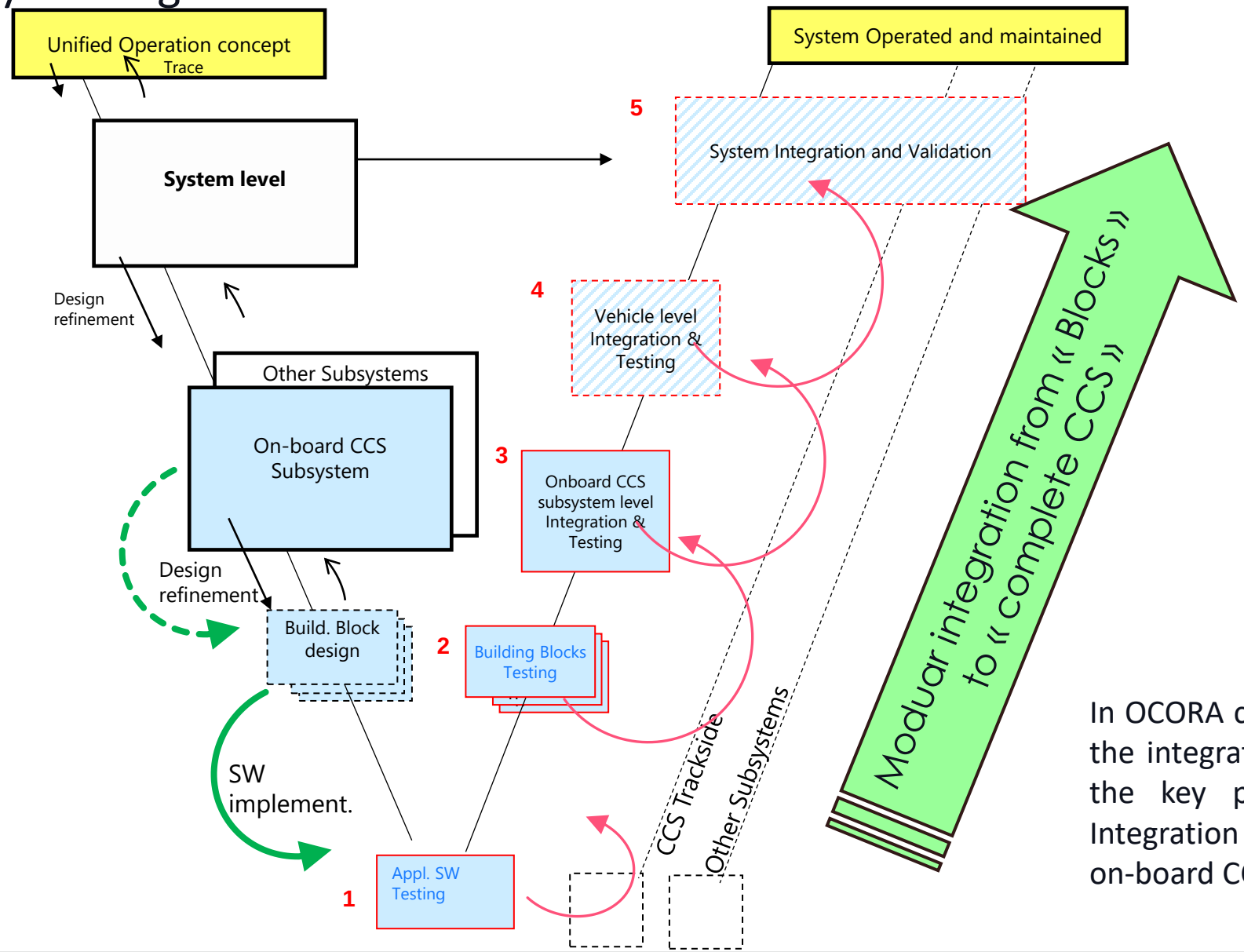
➔ Integrator (System)

➔ Integrator (onboard)

➔ Manufacturers (Building Blocks, Application…)

Scope of OCORA

1, 2..: integration steps



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

Modular CCS Stakeholders

- ➔ Contracting entities (RU §IM)
- ➔ **Integrator(s)**
- ➔ Manufacturers (Building Blocks, Application…)
- ➔ Other (ISA/ NoBo, DeBo..)

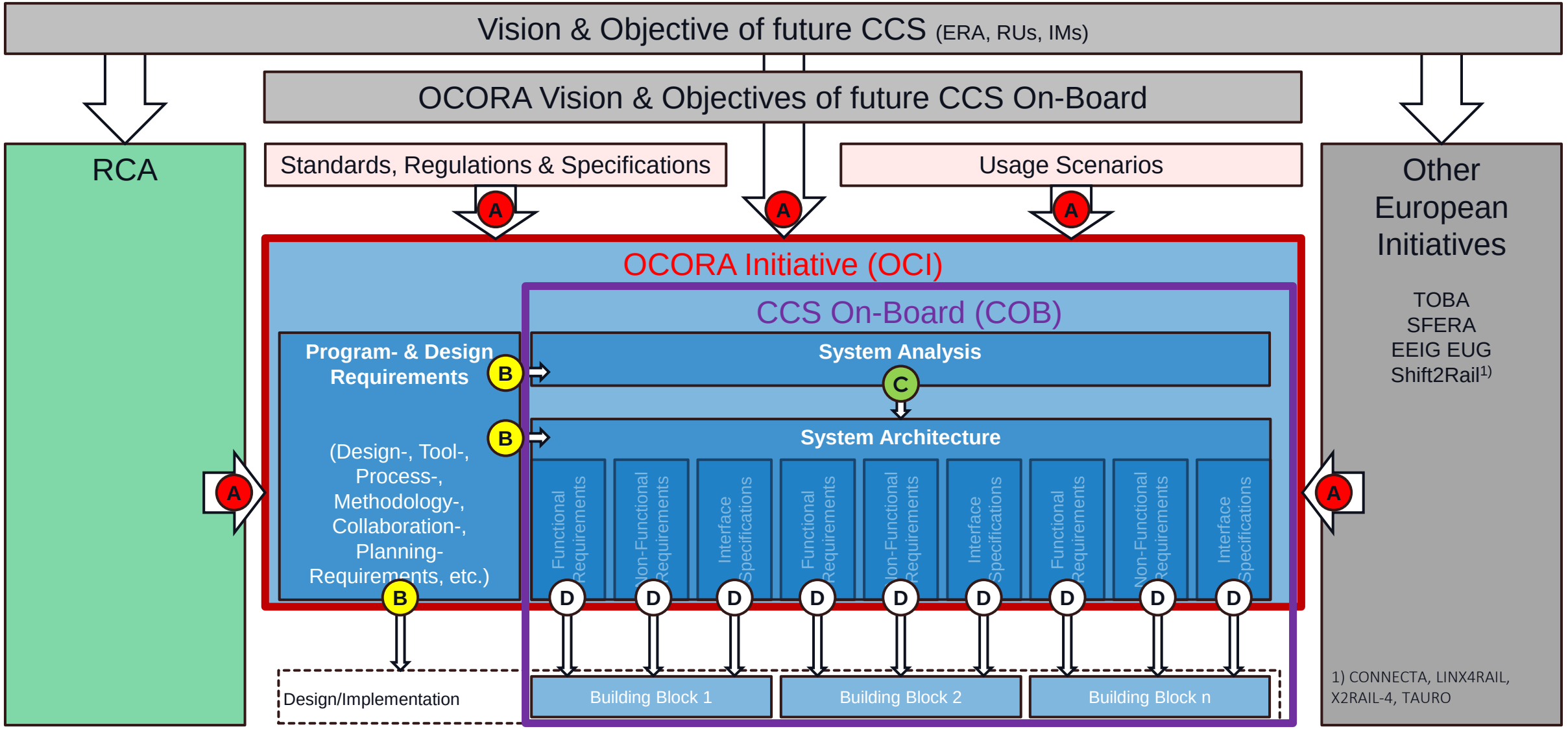
In OCORA compliant projects, the integrator is identified as the key player for Safety, Integration and Testing of the on-board CCS system

Methodology & Tooling

OCORA-BWS02-030 / v2.20 / 24.06.2022

OCORA Requirements Engineering

Structuring the Requirements



OCORA Requirements Engineering

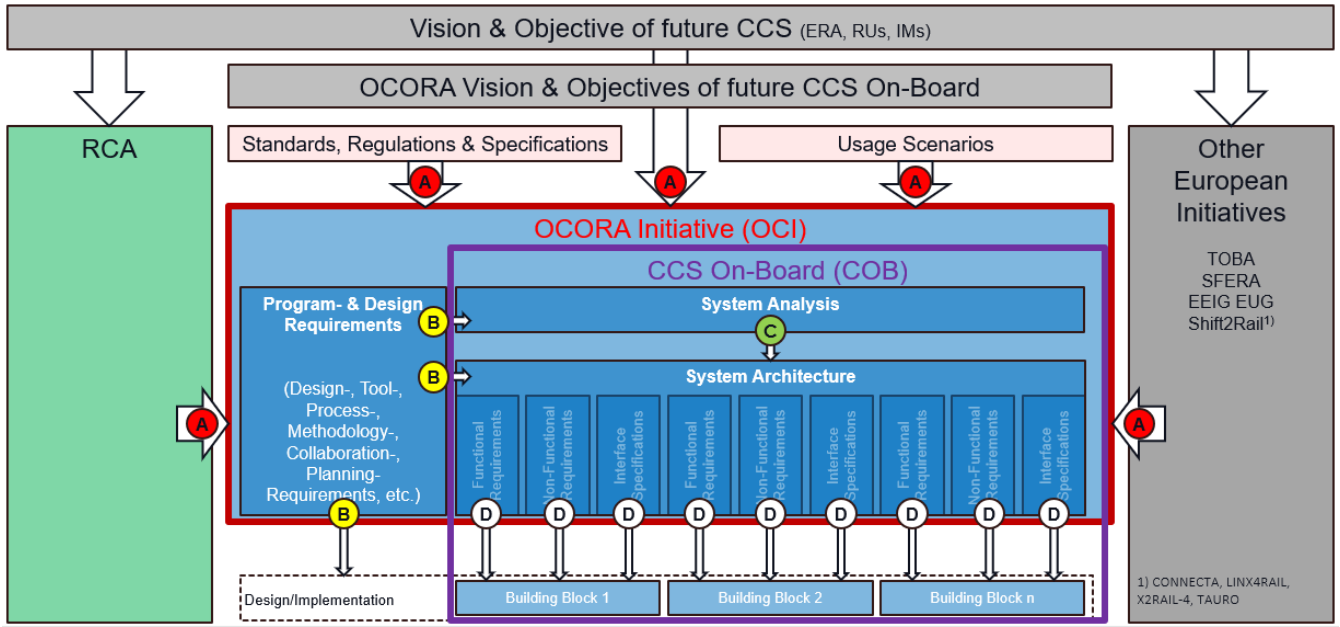
Requirement Definitions

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

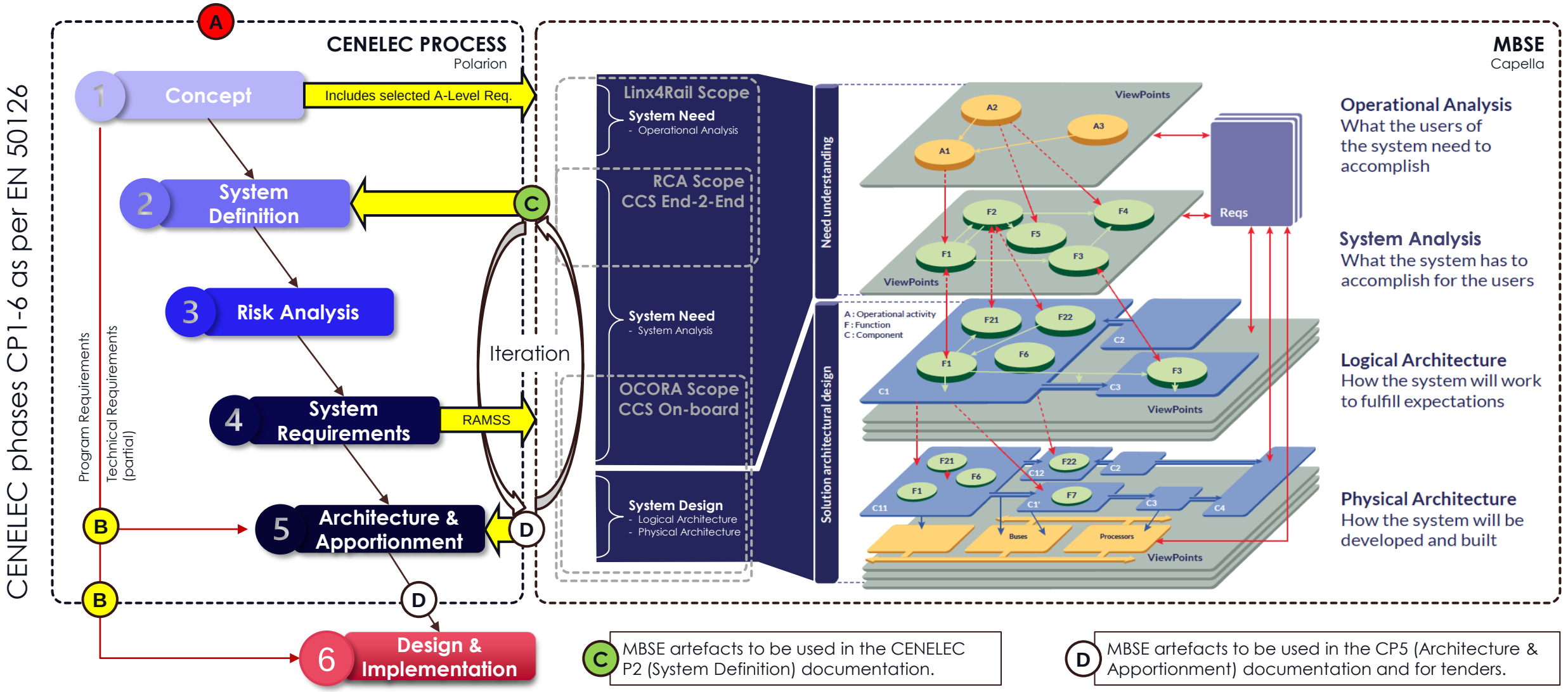
B **Program- & Design Requirements:** The OCORA program defines tools, processes, methodologies and design rules to be used within the program and to be considered during the system analysis and the system design/architecture work.

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.



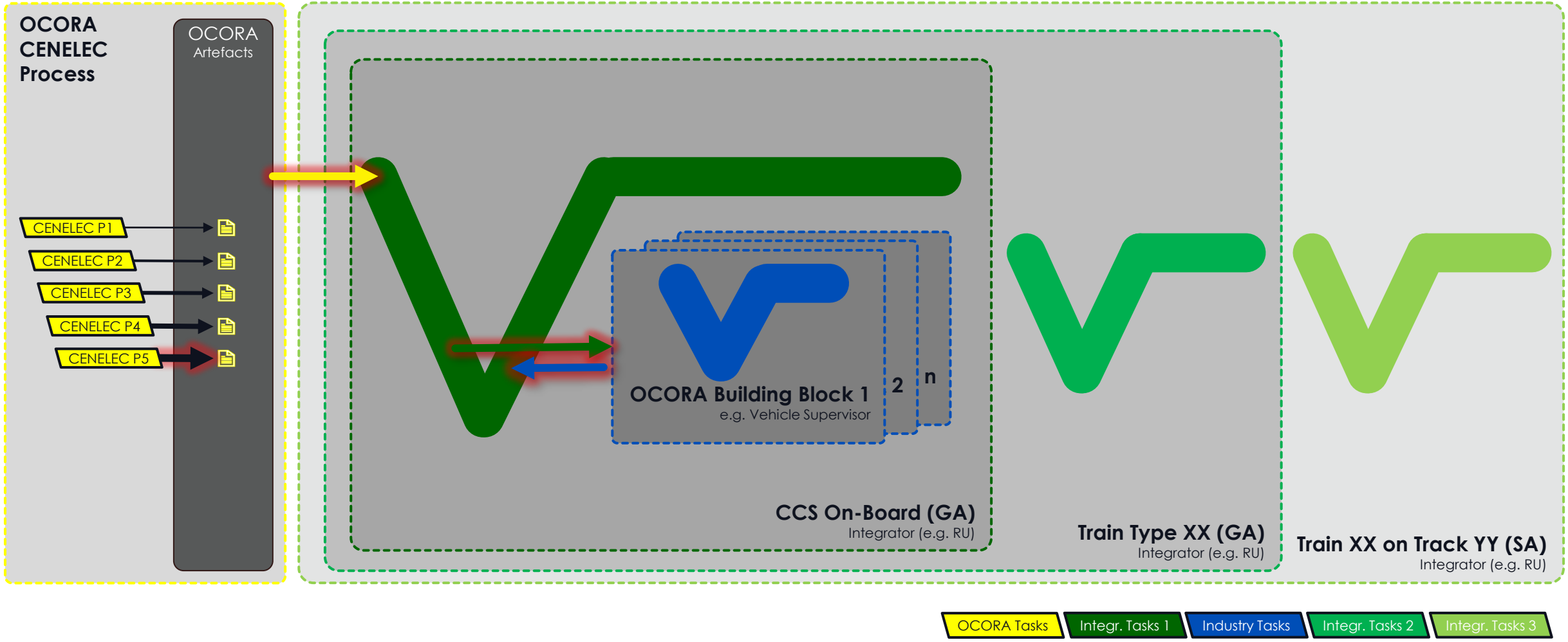
Interaction between CENELEC Process and MBSE



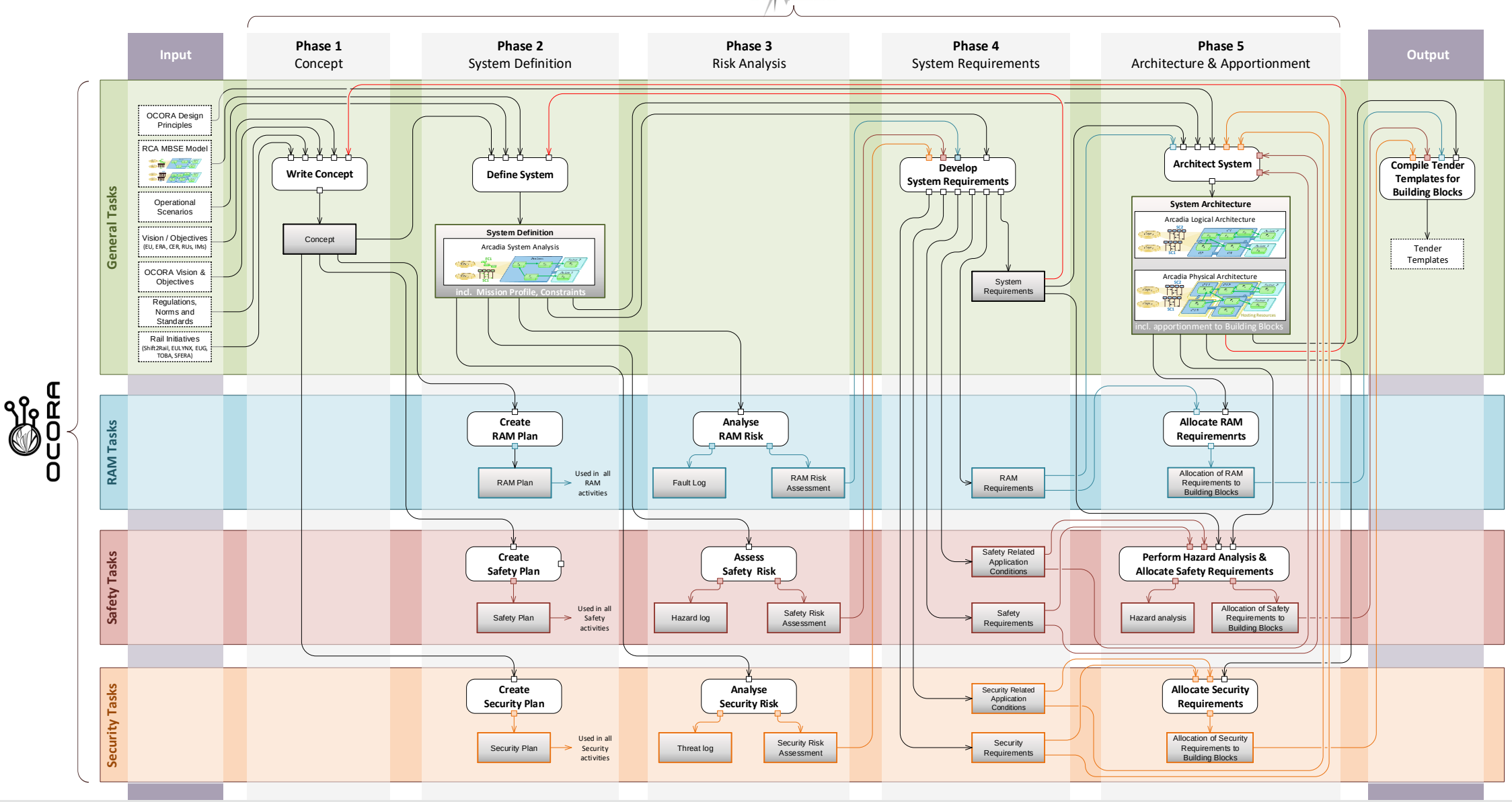
C MBSE artefacts to be used in the CENELEC P2 (System Definition) documentation.

D MBSE artefacts to be used in the CP5 (Architecture & Apportionment) documentation and for tenders.

OCORA in Context of the relevant CENELEC Projects



OCORA CENELEC Process

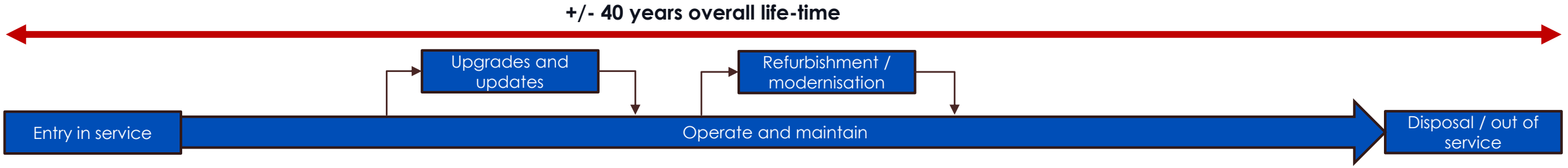


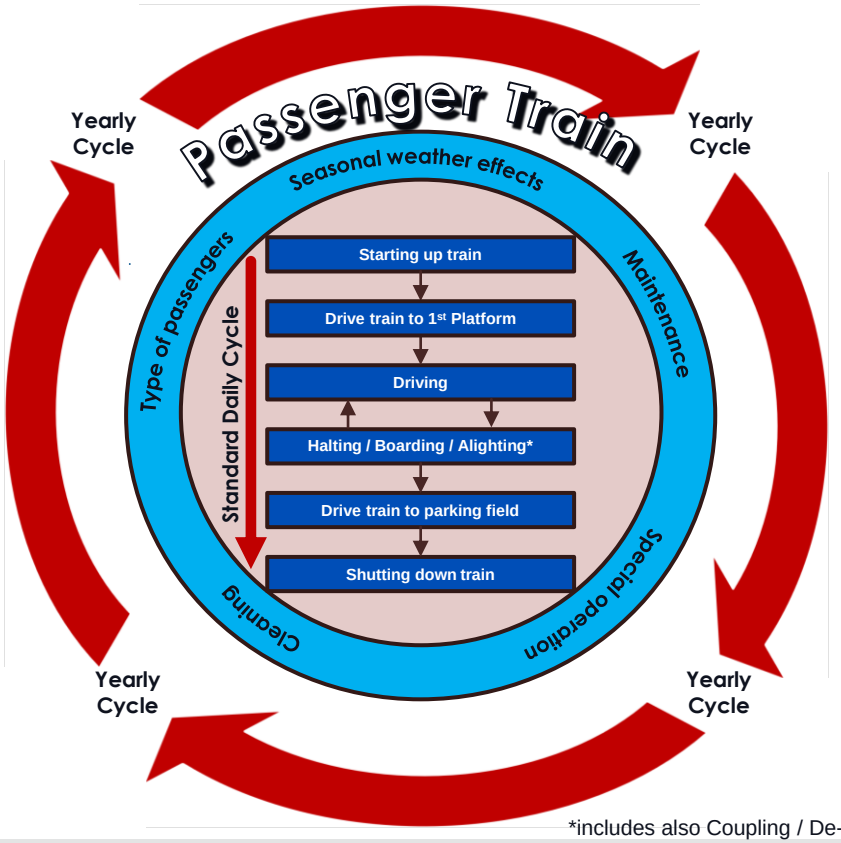
Operational Concept

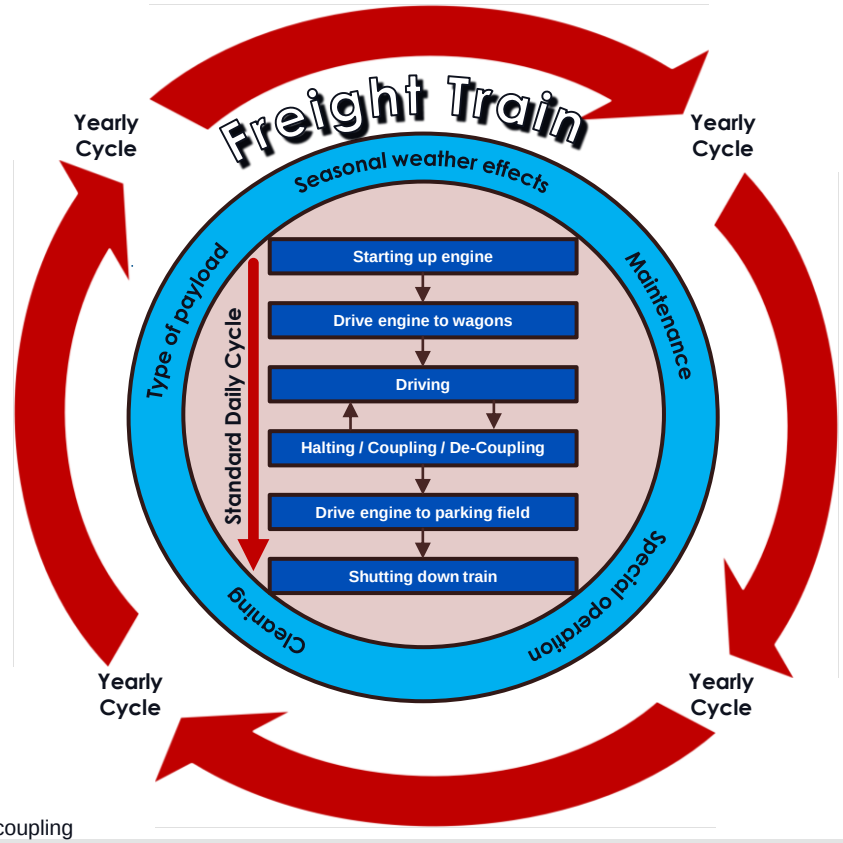
OCORA-BWS02-030 / v2.20 / 24.06.2022

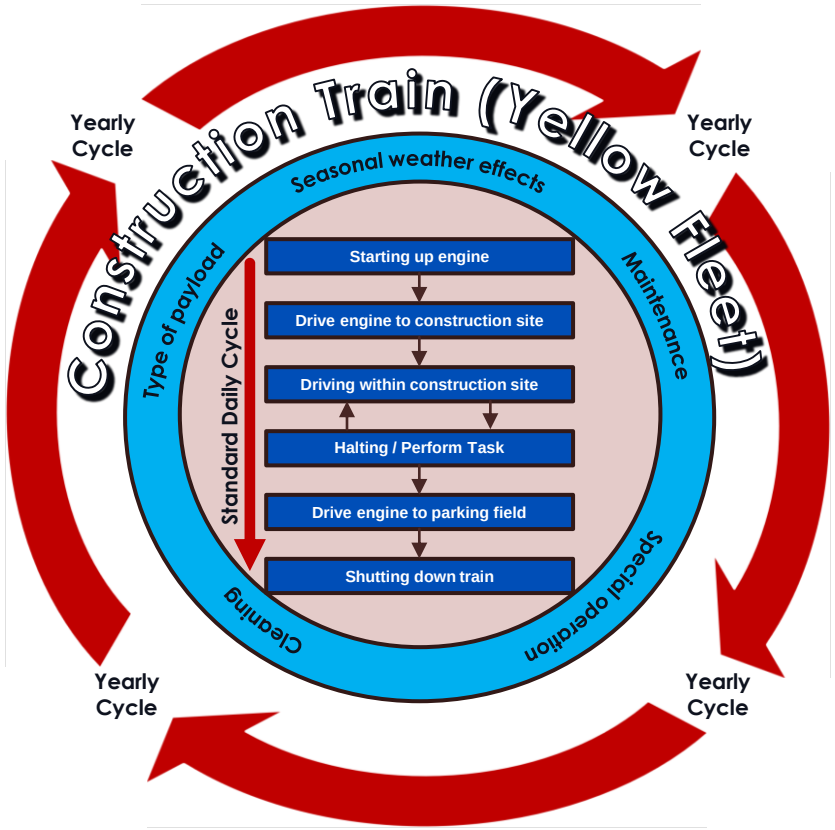
Operational Concept Overview

Live Cycle of Passenger, Freight, and Construction Trains









*includes also Coupling / De-coupling