OCORA System Architecture

Introduction

OCORA

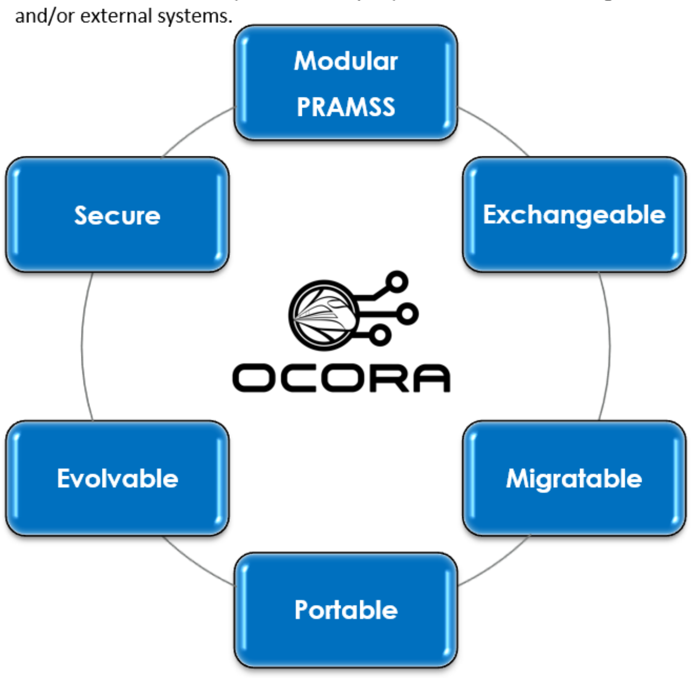
Open **CCS** **O**n-Board **R**eference **A**rchitecture

A Collaboration of 5 European Railway Undertakings

Technical Slide Deck

OCORA Design Objectives

A reasonable number of Building Blocks are defined for CCS On-Board. Each Building Blocks has standardised functionality, standardised PRAMSS requirements (including Tolerable Functional Failure Rate [TFFR], Safety Integrity Level [SIL] and Safety Related Application Conditions [SRAC]), standardised interfaces (on all OSI Layers) towards other building blocks and/or external systems.



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.

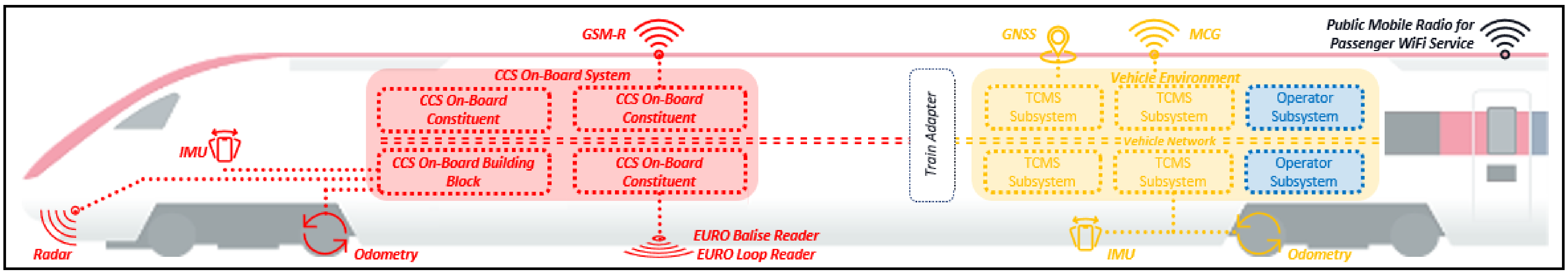
Ability to easily adapt the CCS On-Board to new technologies and to easily add new Building Blocks. In the context of OCORA evolvability means the ability to easily adopt to new technologies or to extend the functionality of an on-board CCS system without the involvement of the original supplier.

Ability to introduce changes to any CCS On-Board Building Block. In the context of OCORA migrateability is the ability to introduce changes (bug-fixes, improvements, new functionality) 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).

OCORA System Architecture

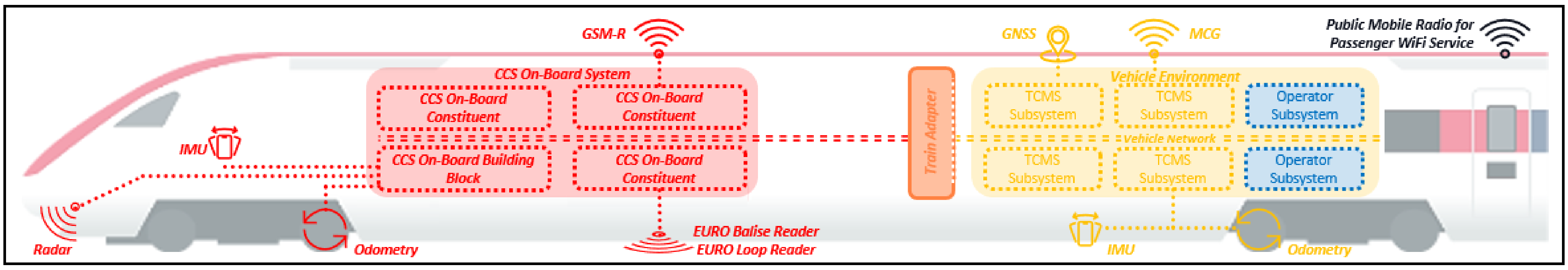
Technical Roadmap – Current Situation



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



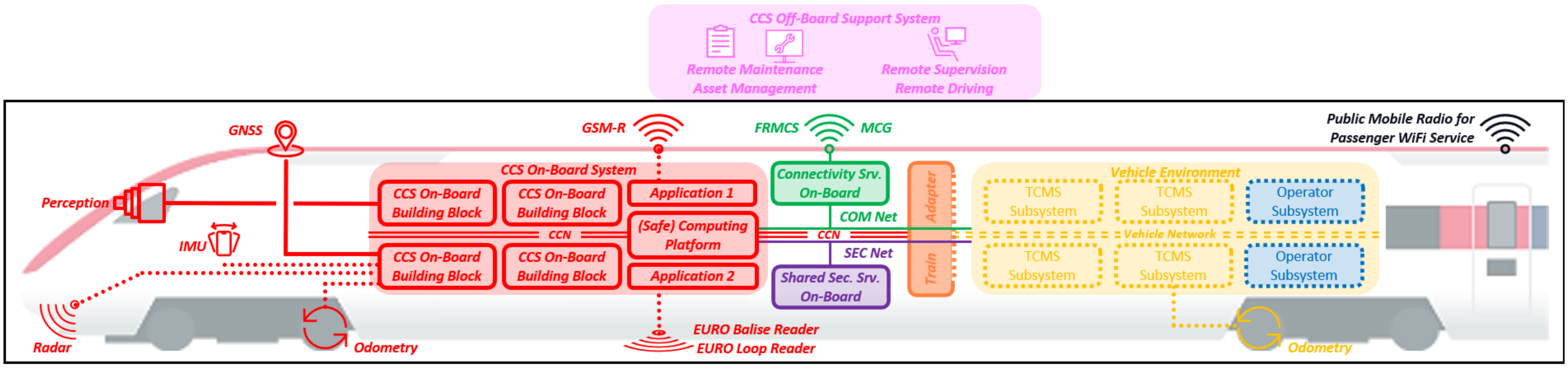
Step 1: Short-Term (TSI-2022)

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 (e.g. TSI-2025/26)

The CCS On-Board System consists of a reasonable number of CCS On-Board Building Blocks. Each Building Blocks has standardised functionality, standardised PRAMSS requirements (including Tolerable Functional Failure Rate [TFFR], Safety Integrity Level [SIL] and Safety Related Application Conditions [SRAC]), standardised interfaces (on all OSI Layers) towards other building blocks and/or external systems. 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). **First applications (e.g. MDCM, ATO GoA 1-2) are running on a (safe) computing platform.**

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:

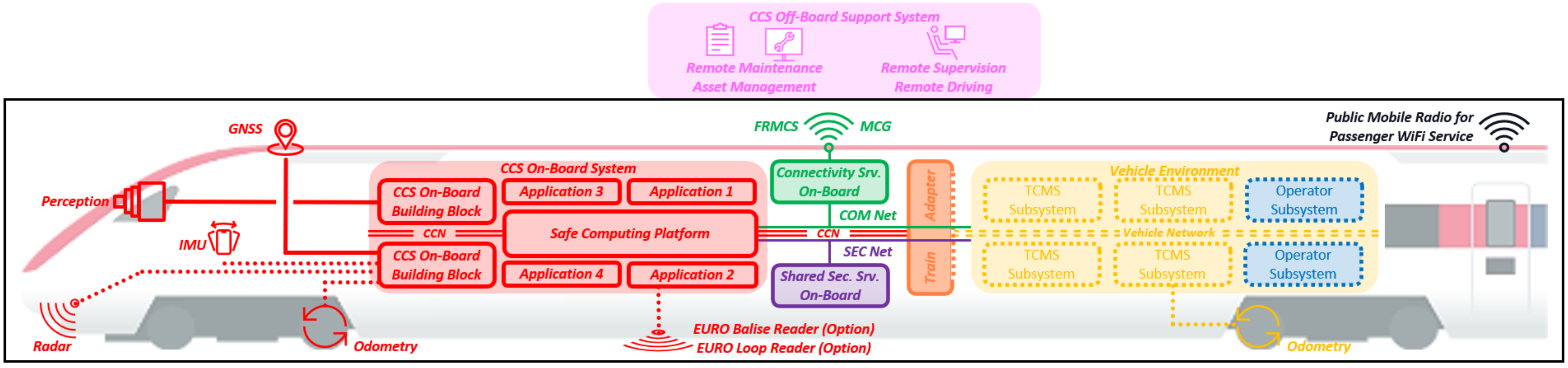
- Remote Maintenance
- Asset Management
- Absolut continues safe localisation (GNSS)
- Safe Train Integrity determination
- Safe Train Length determination
- ETCS L3
- ATO GoA 1-4
- Remote Supervision
- Remote Driving

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)

OCORA System Architecture

Technical Roadmap Step 3 – Long-Term



Step 3: Long-Term (TSI-2028/29)

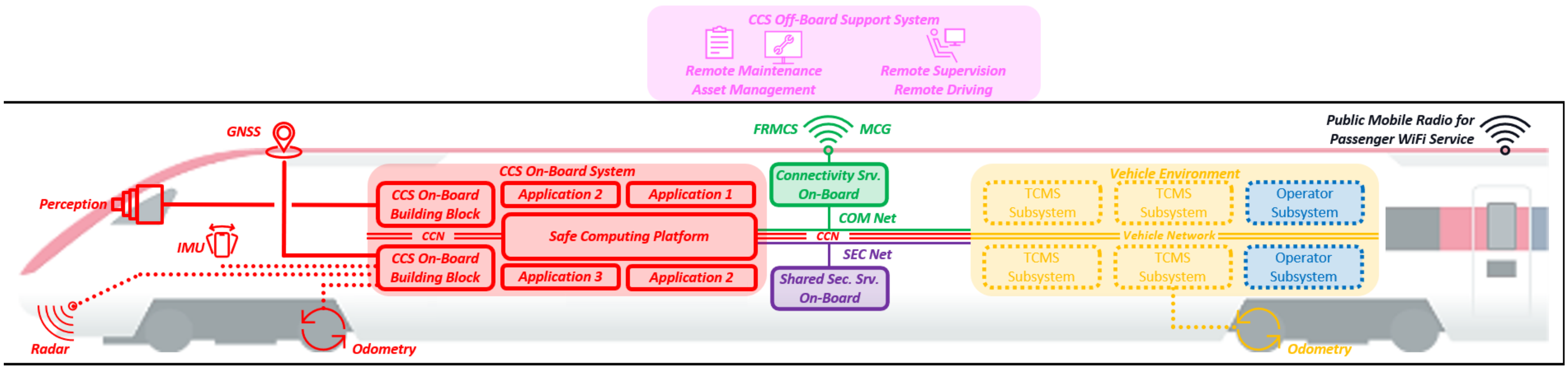
The CCS On-Board System includes a safe computing platform, hosting CCS Building Blocks as applications (SW Building Blocks). They are deployed on an instance of the Generic Safe Computing Platform (SCP) and communicate with each other through the standardised Platform Independent Application Programming Interface (PI-API). Communication with computing platform external building blocks and systems is realised by the Computing Platform (integrating with the CCN).

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 2028/29)

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.

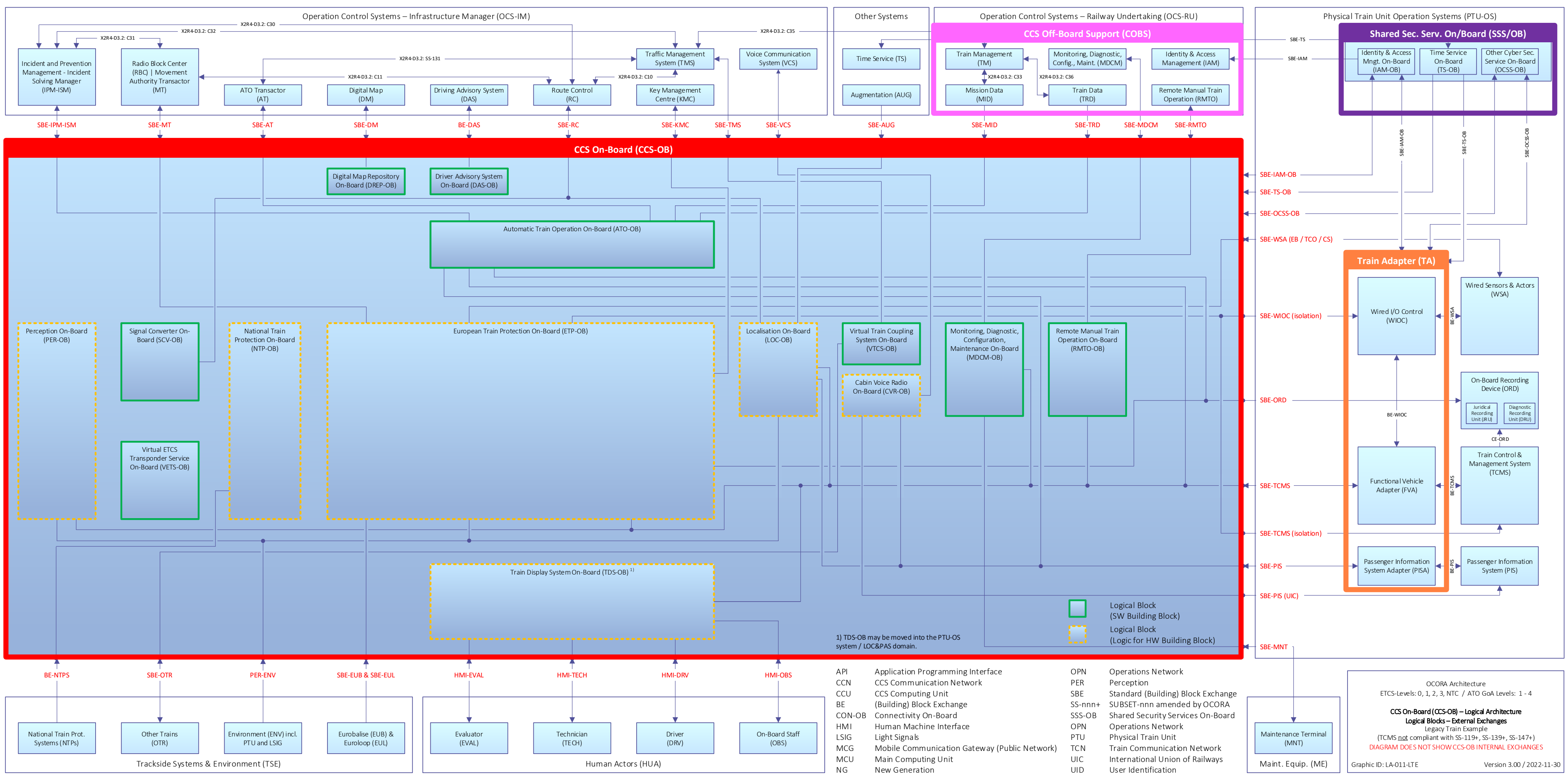
Due to the increased performance of the CCS On-Board localisation through better sensor fusion algorithms, the use of GNSS localisation, digital map data, and augmentation data, the EURO Balise and EURO Loop readers are not needed anymore.

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

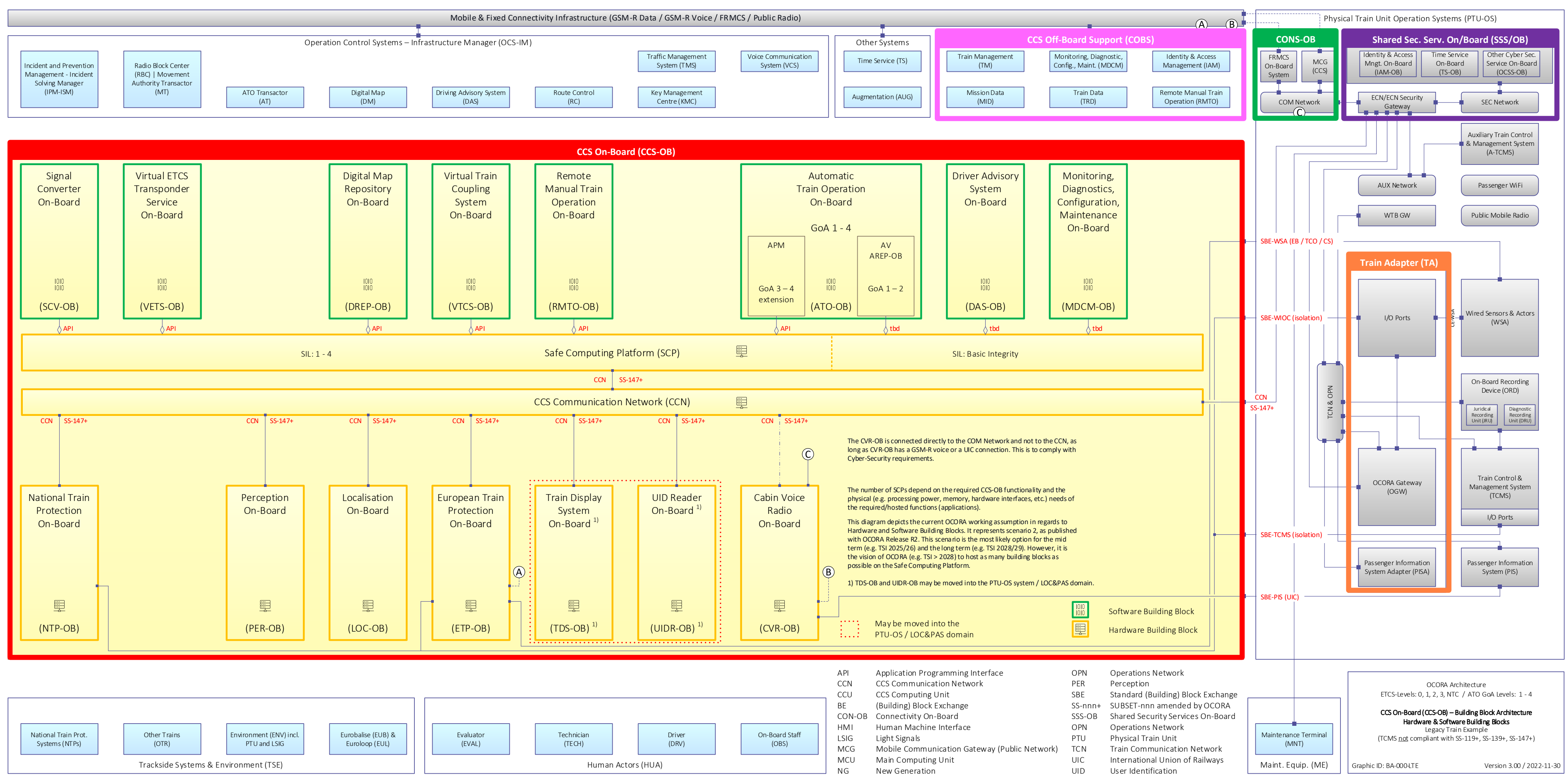
Step 4: eliminating the EURO Balise and EURO Loop readers further reduces the maintenance efforts and enables the infrastructure managers to implement changes more quickly.

OCORA System Architecture

OCORA Scope – Logical Architecture – Legacy Train Example

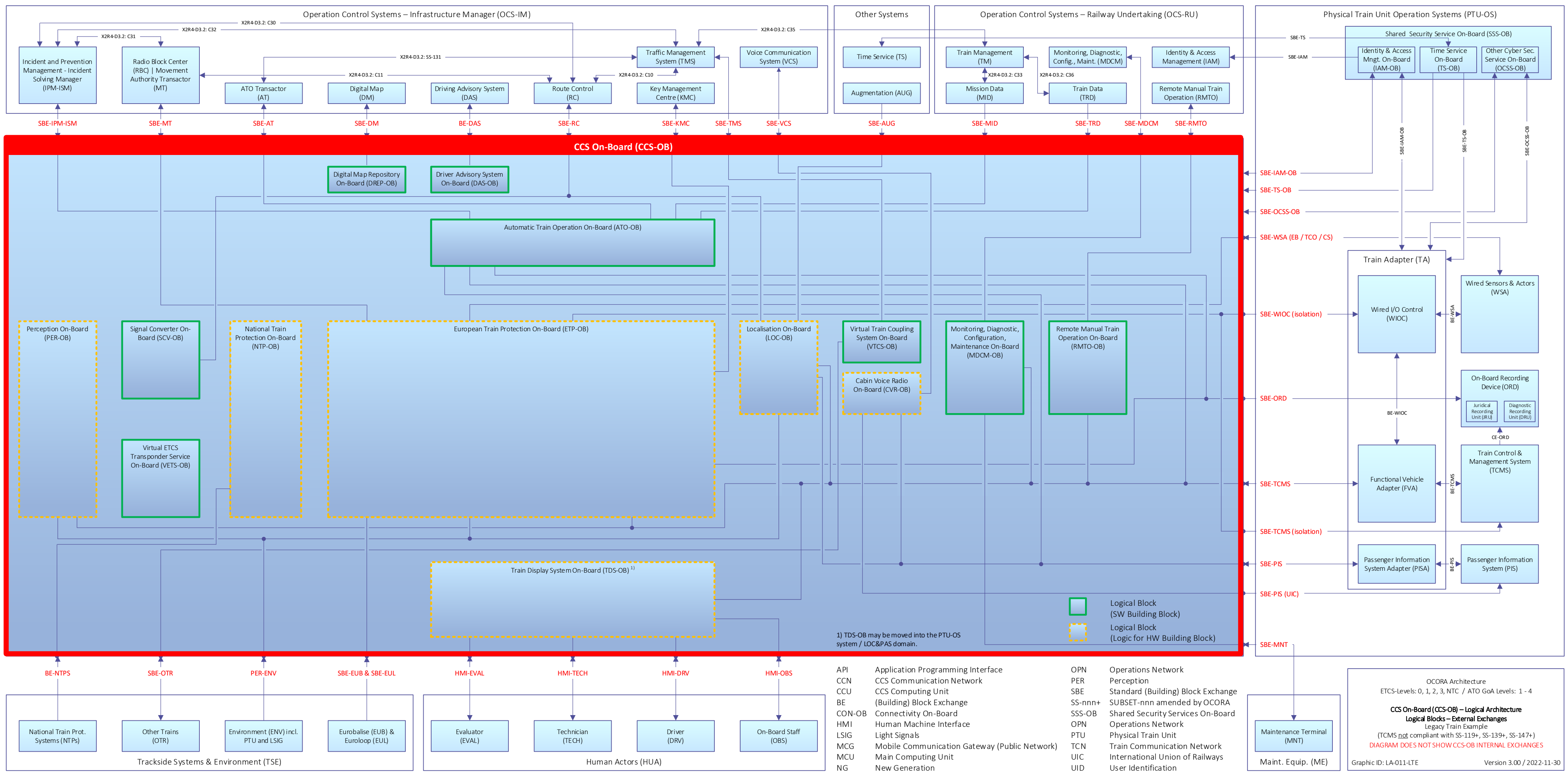


OCORA Scope – Physical Architecture – Legacy Train Example

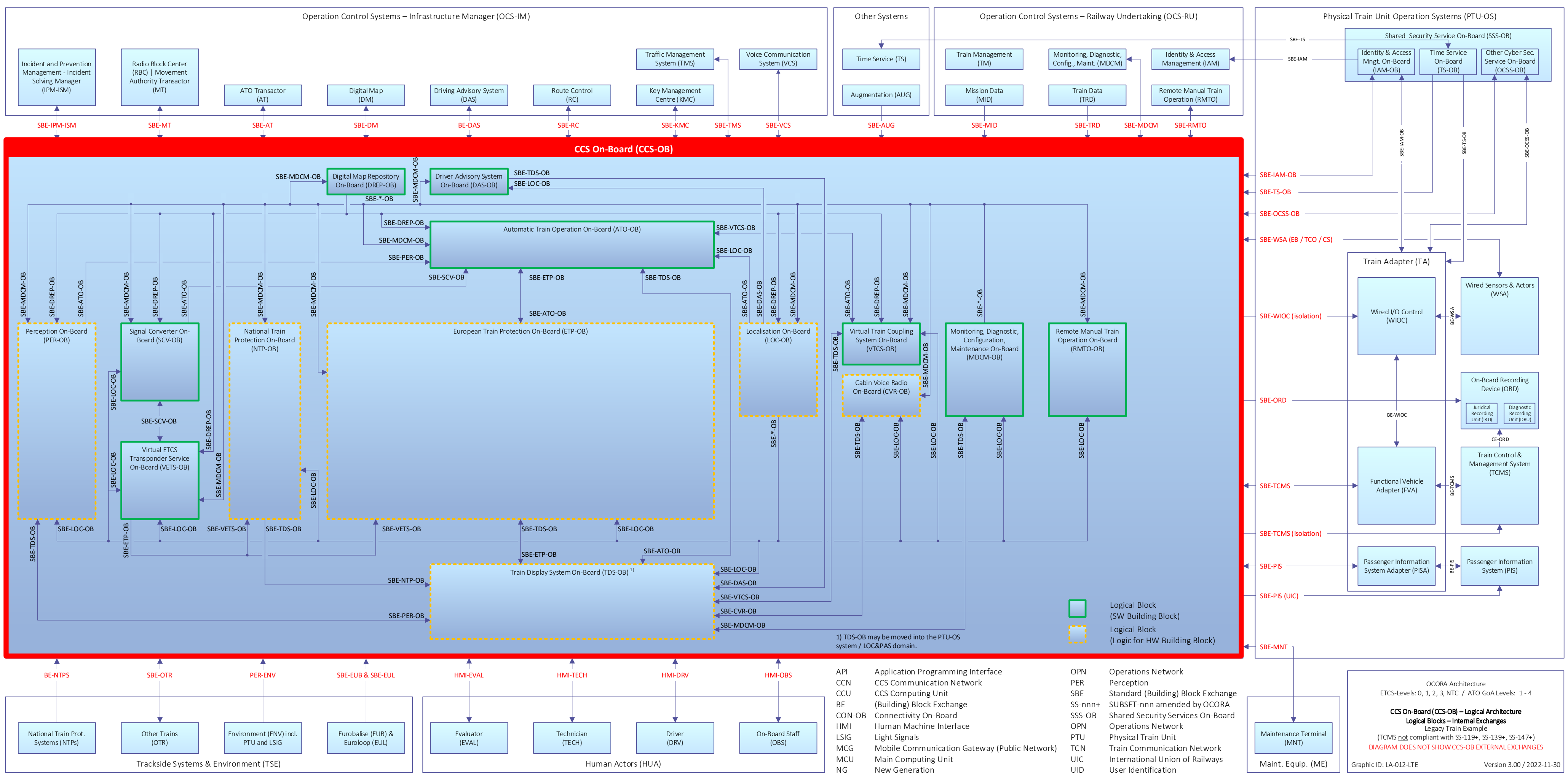


OCORA System Architecture

Logical Architecture CCS-OB – Functional Blocks – External Exchanges – Legacy Train Example

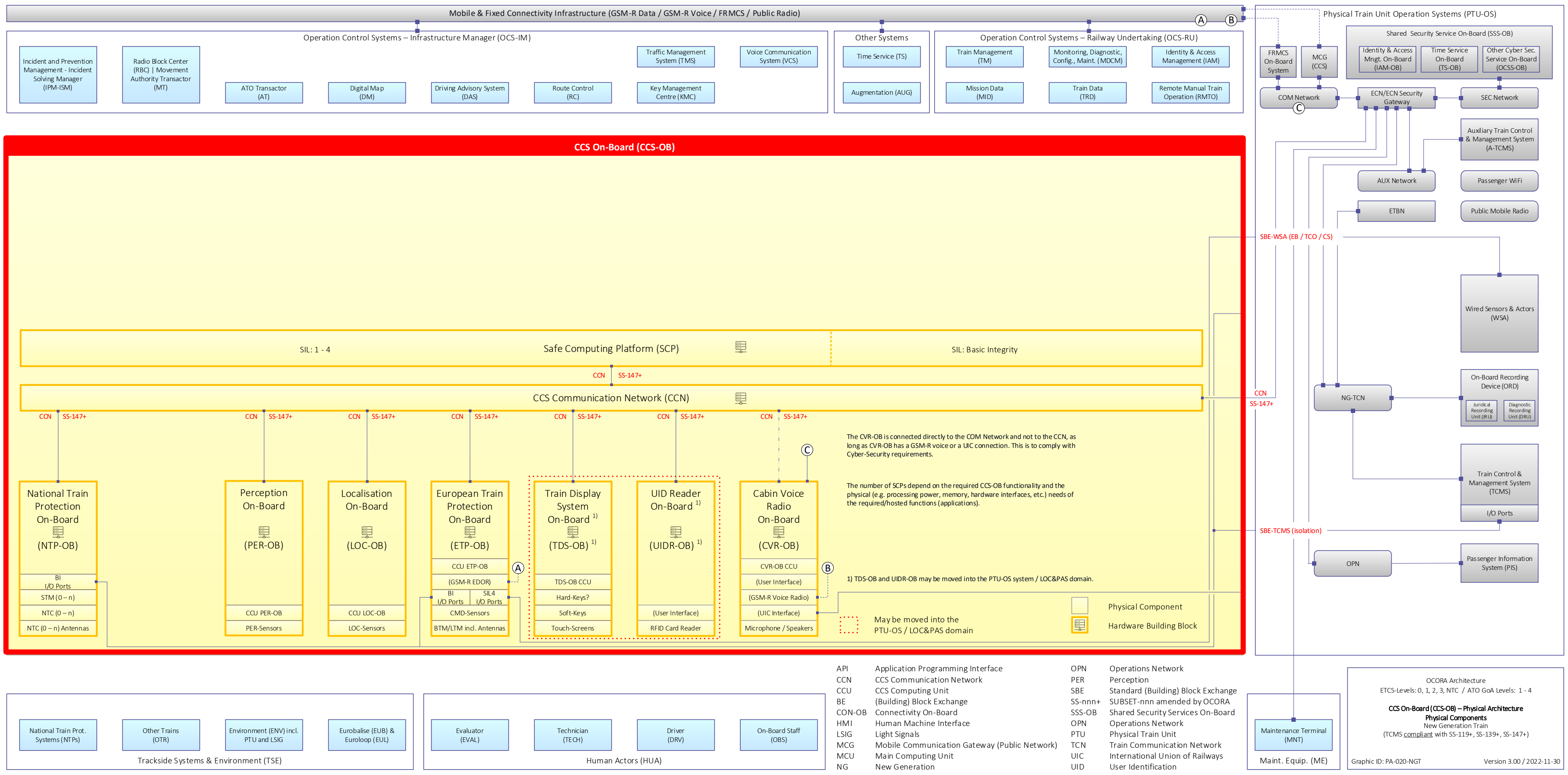


Logical Architecture CCS-OB – Functional Blocks – Internal Exchanges – Legacy Train Example

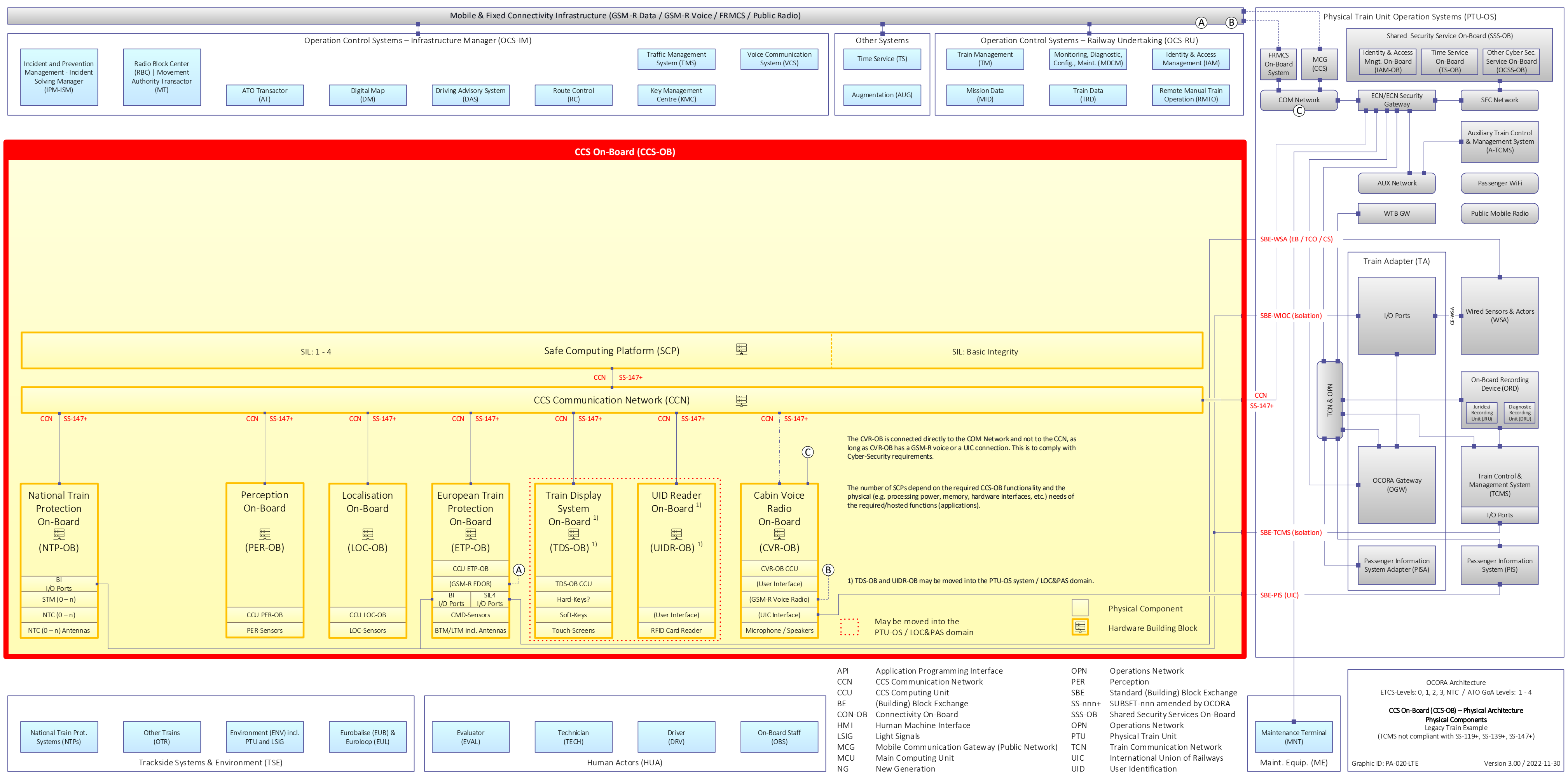


OCORA System Architecture

Physical Architecture CCS-OB – Hardware Block Diagram – New Generation Train

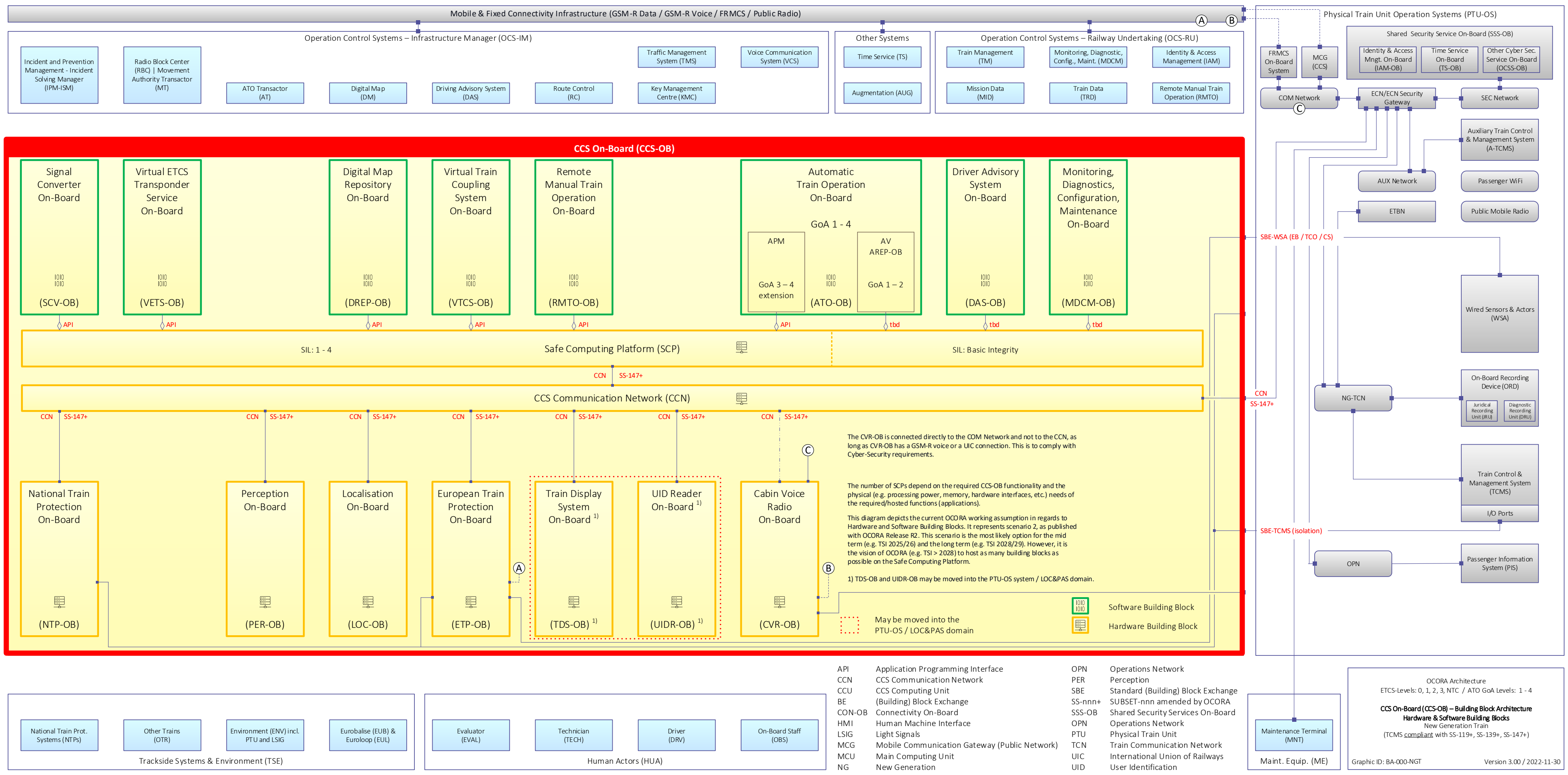


Physical Architecture CCS-OB – Hardware Block Diagram – Legacy Train Example

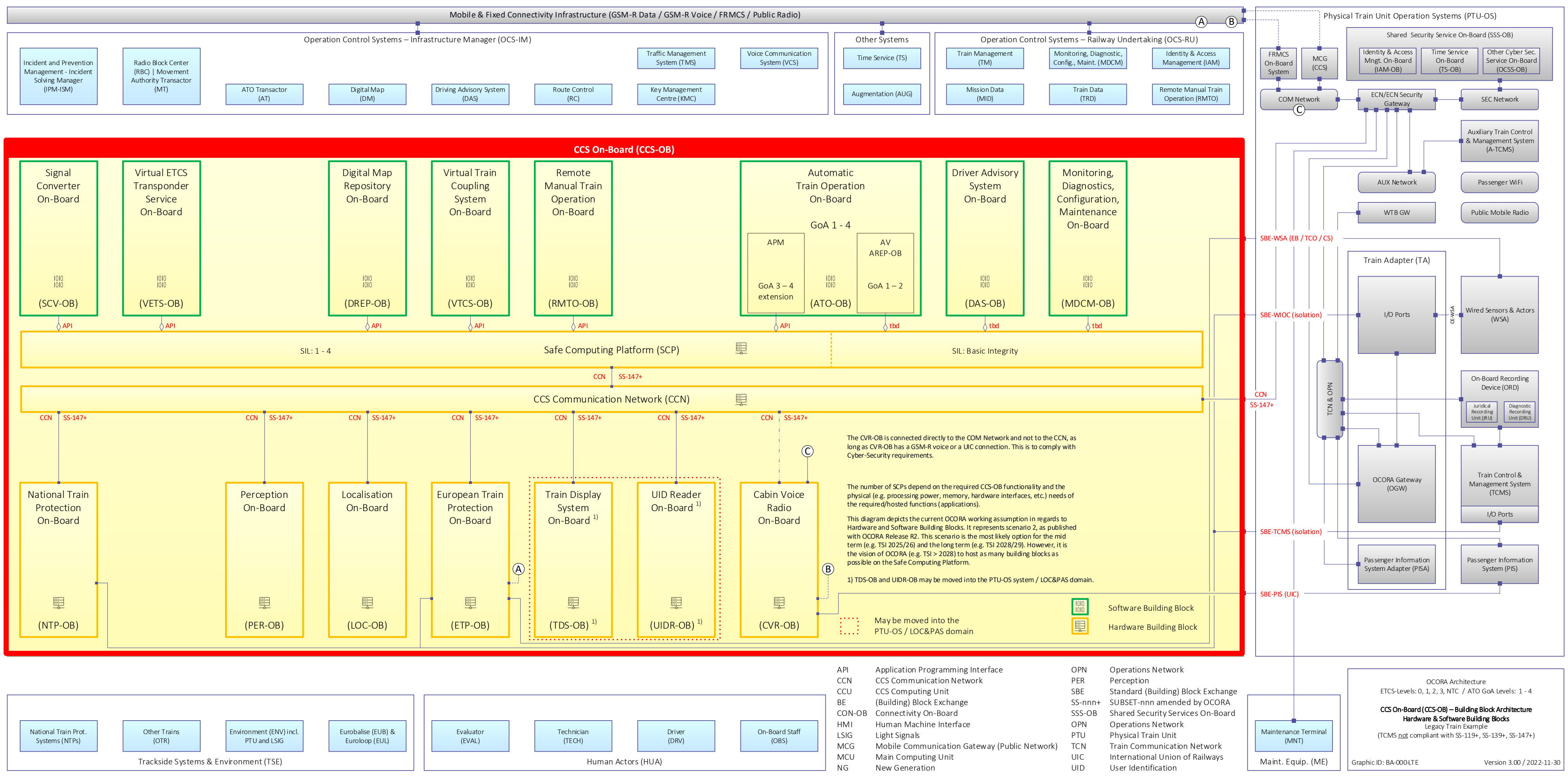


OCORA System Architecture

Building Blocks – New Generation Train



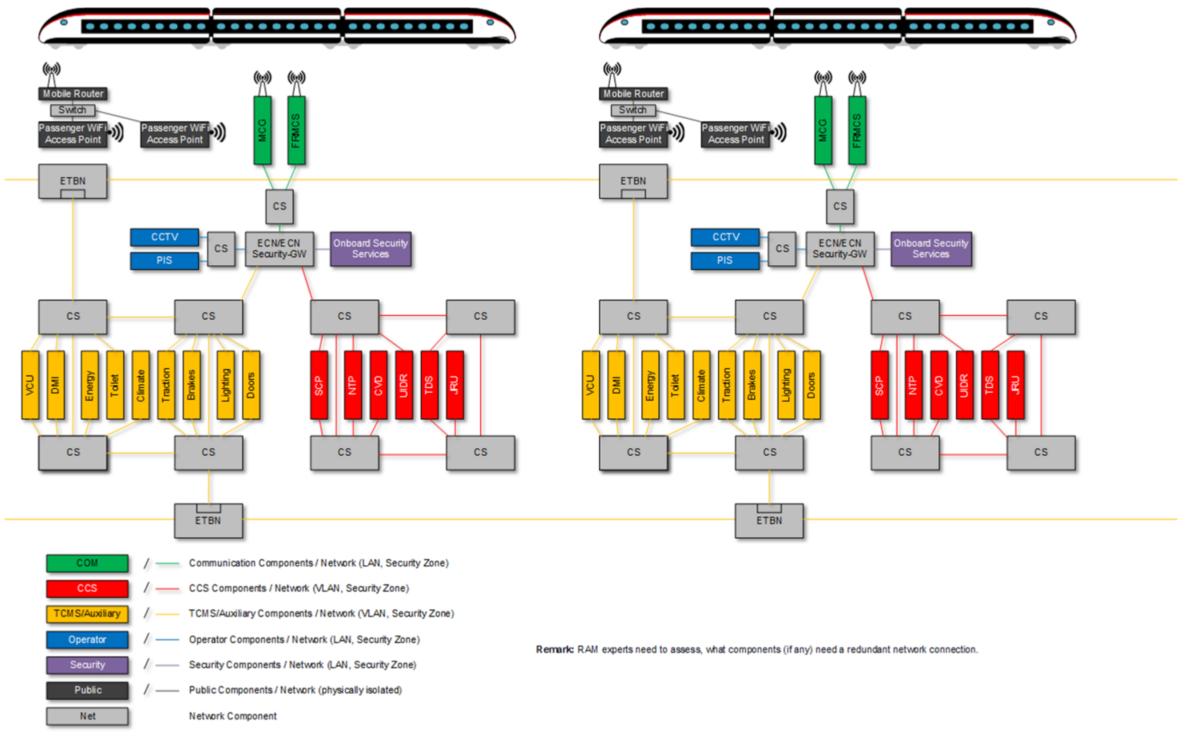
Building Blocks – Legacy Train Example



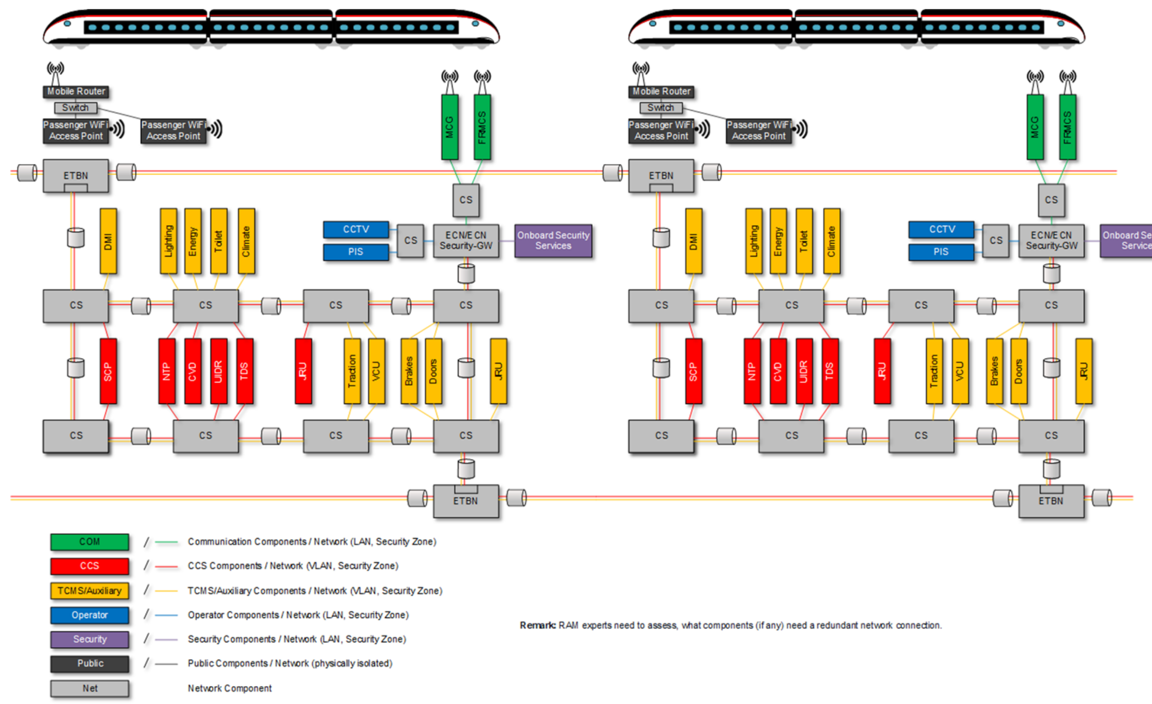
OCORA System Architecture

Network Topology Scenario – New Generation Train

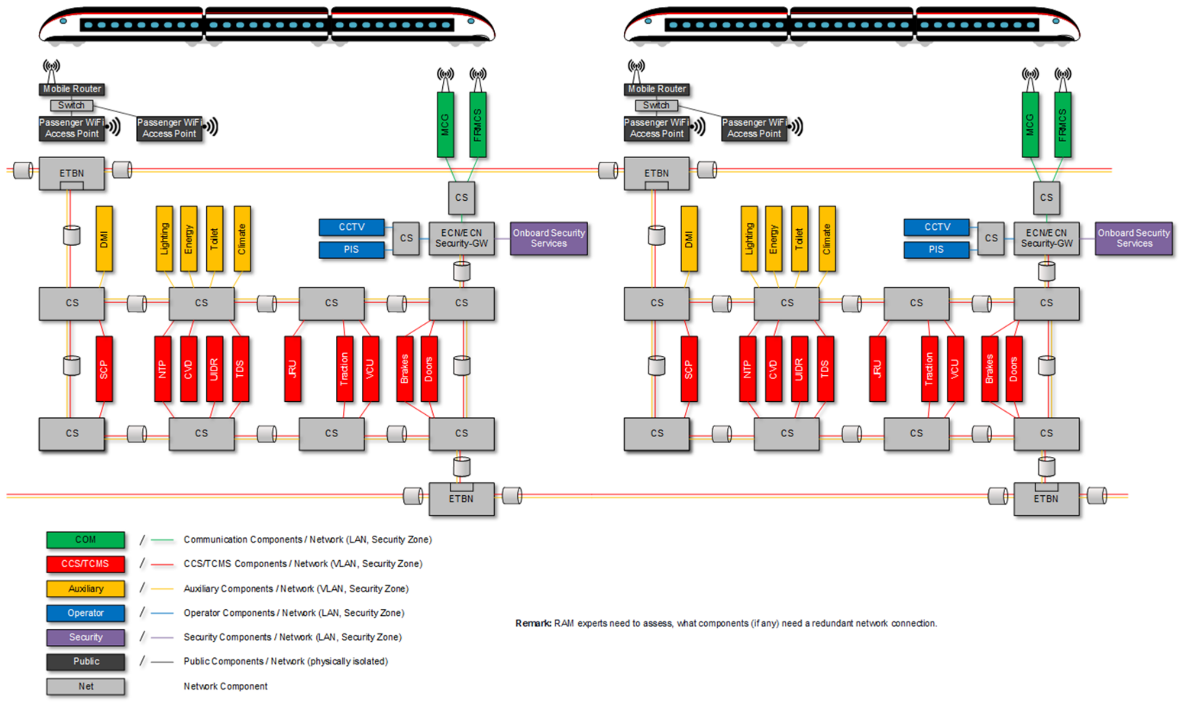
SCENARIO A: CCN AS PHYSICALY SEPARATED NETWORK



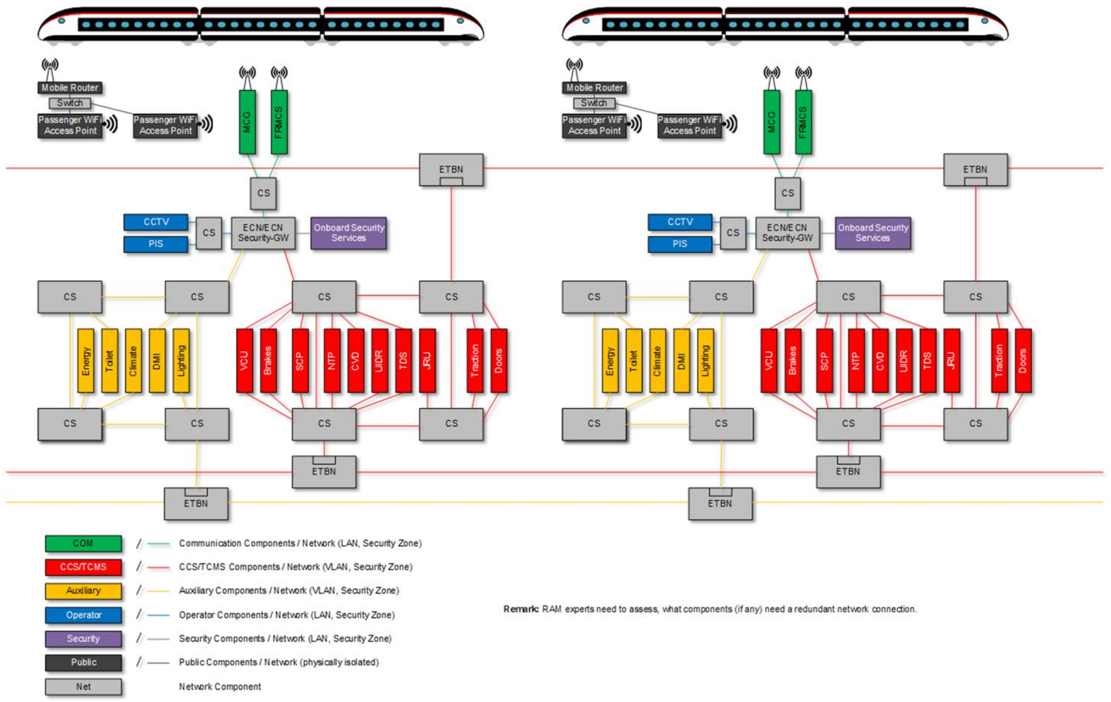
SCENARIO B: CCN AS LOGICALLY SEPARATED NETWORK



SCENARIO C: COMMON CRITICAL CONTROL NETWORK LOGICALLY SEPARATED

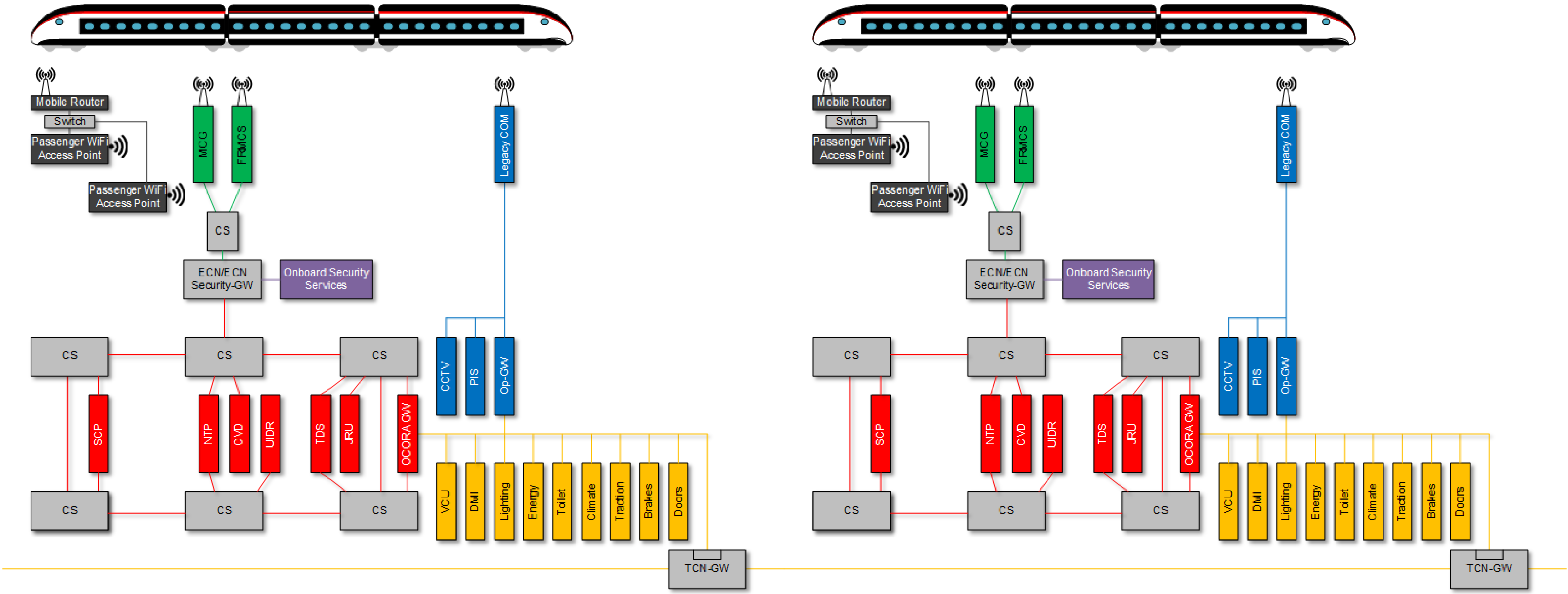


SCENARIO D: COMMON CRITICAL CONTROL NETWORK PHYSICALLY SEPARATED



OCORA System Architecture

Network Topology Scenario – Legacy Train: Integration with OCORA Gateway



- 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.