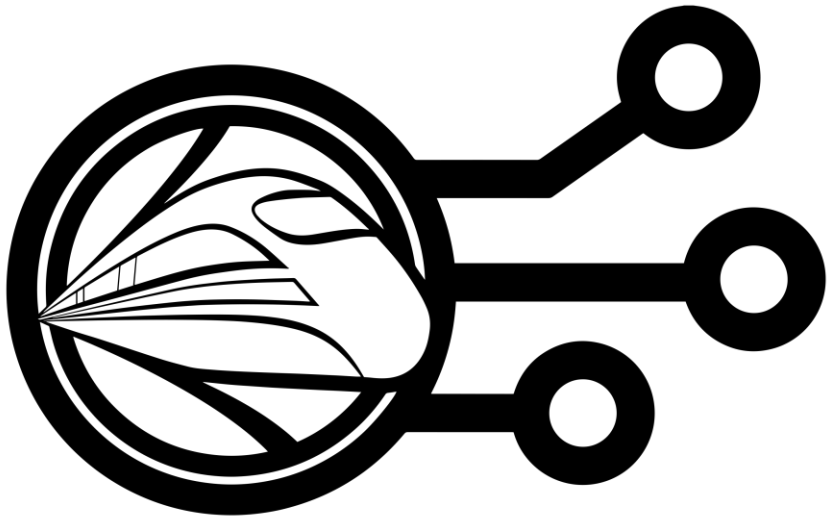


# OCORA

## Gamma – Architecture

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# Presentation Overview

**Hardware / Physical View**

- Components
- Scope
- Interfaces
- Building Blocks

**HW Integration Scenarios**

- Legacy Train (with and without Legacy CCS Peripherals)
- NG-TCN (Separate Networks / Common Network)

**Network Topology / Integration**

- Legacy Train
- NG-TCN (Separate Networks / Common Network)
- Connecting Multiple Consists

**Functional / Logical View**

- SW Components
- Scope
- Interfaces
- Building Blocks

**Computing Platform**

- High-Level Architecture
- Approaches

**Functional Vehicle Adapter**

**Modular Safety**

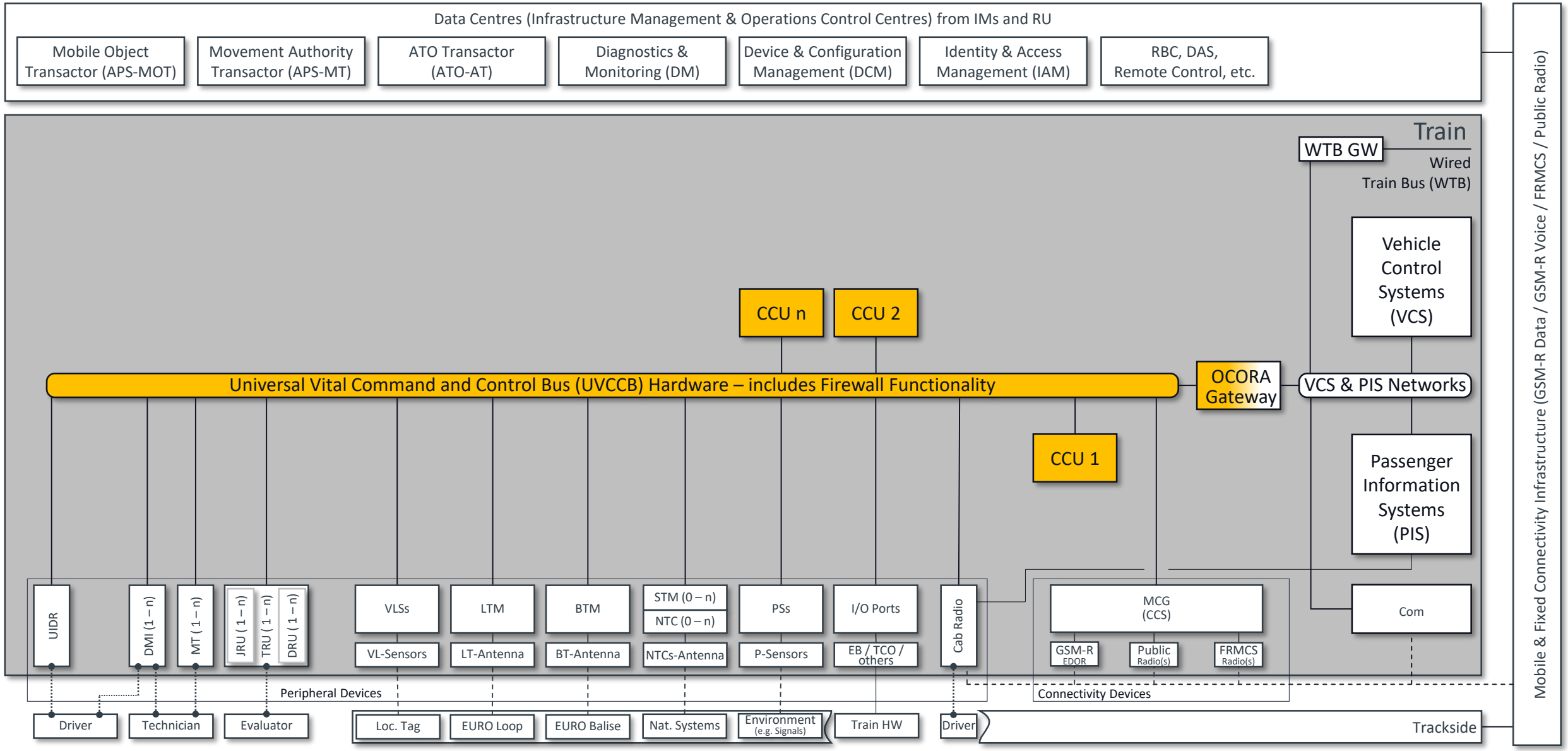
**Security**

**Supporting Slides**

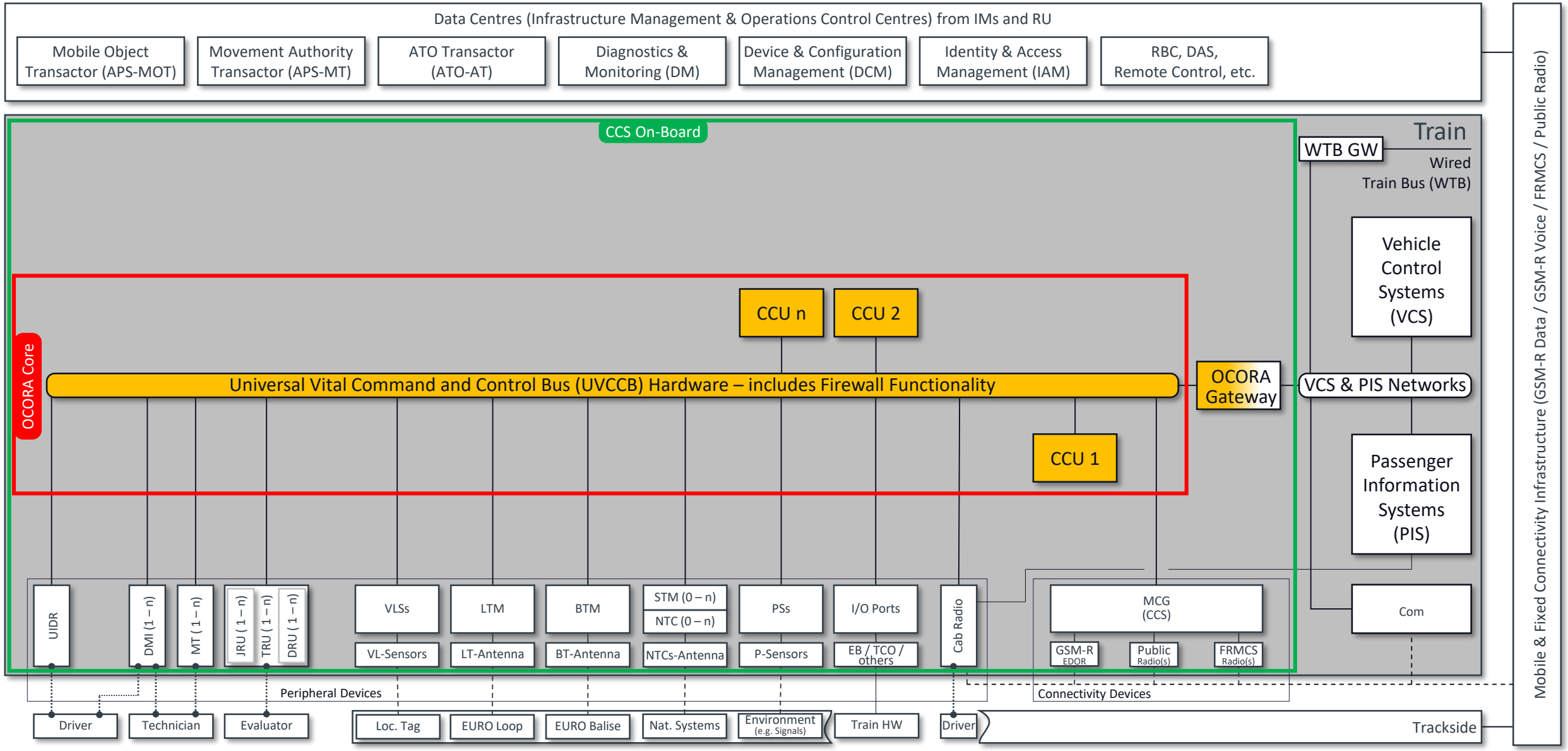
# Hardware / Physical View

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

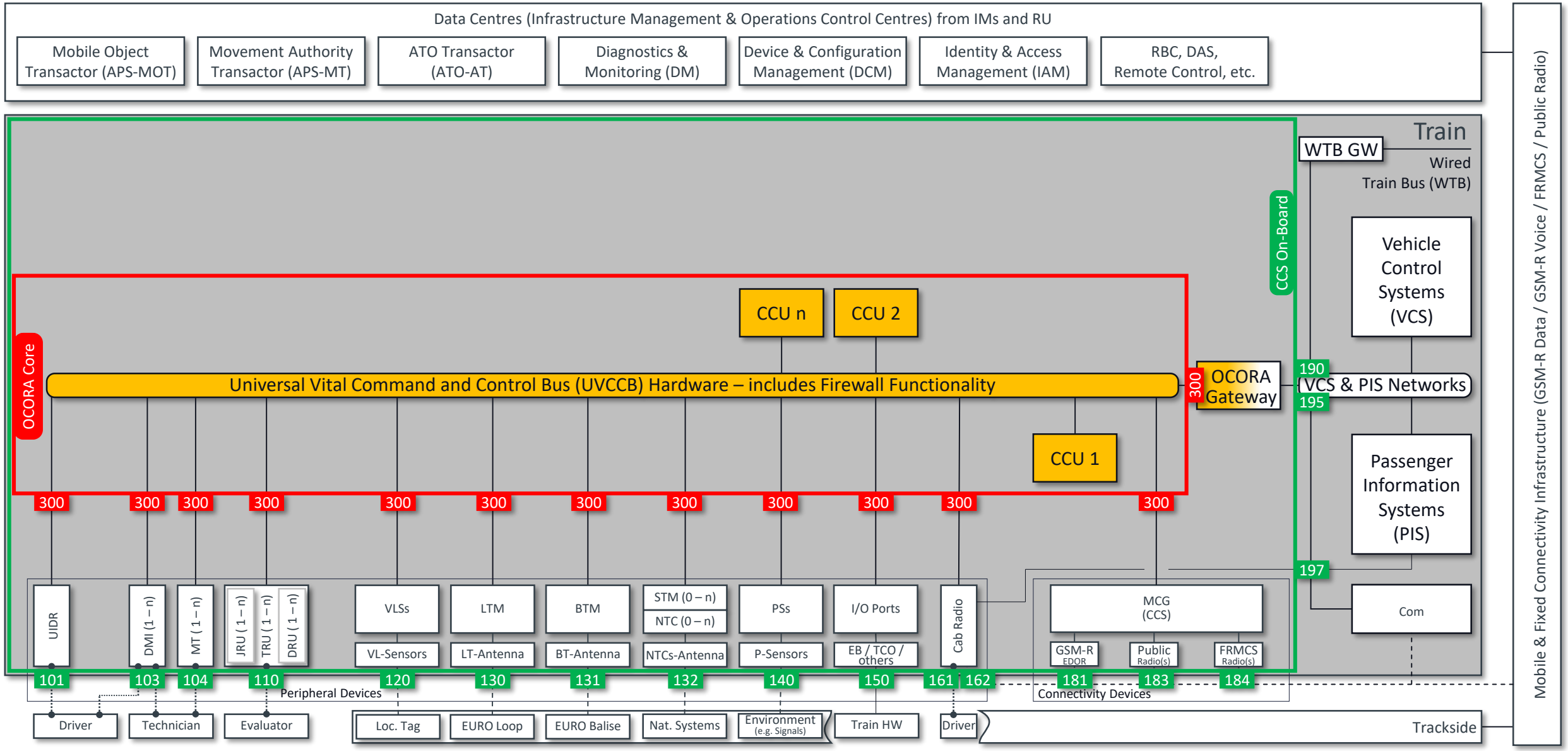
# Hardware Components



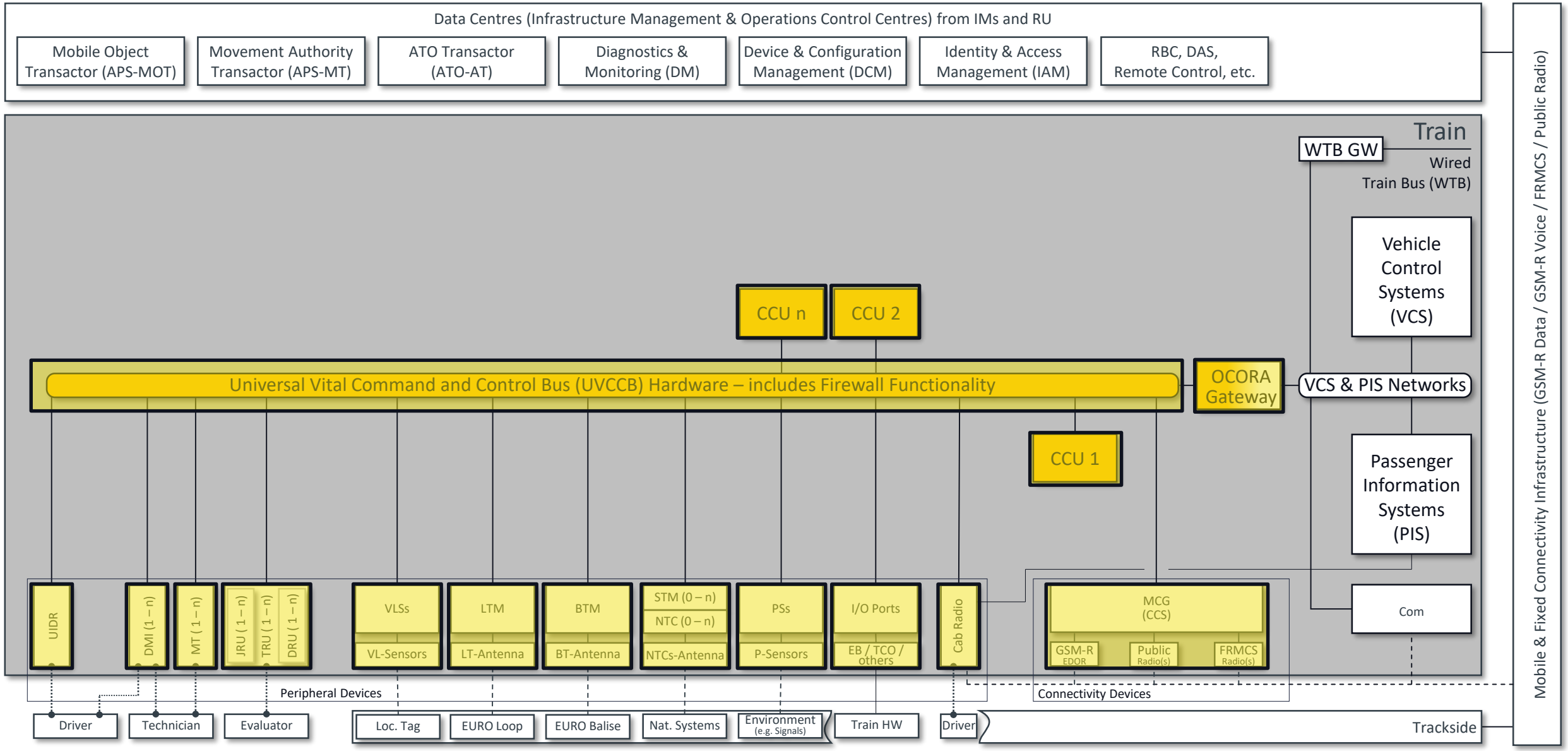
# Hardware Components – Scope



# Hardware Components – Interfaces



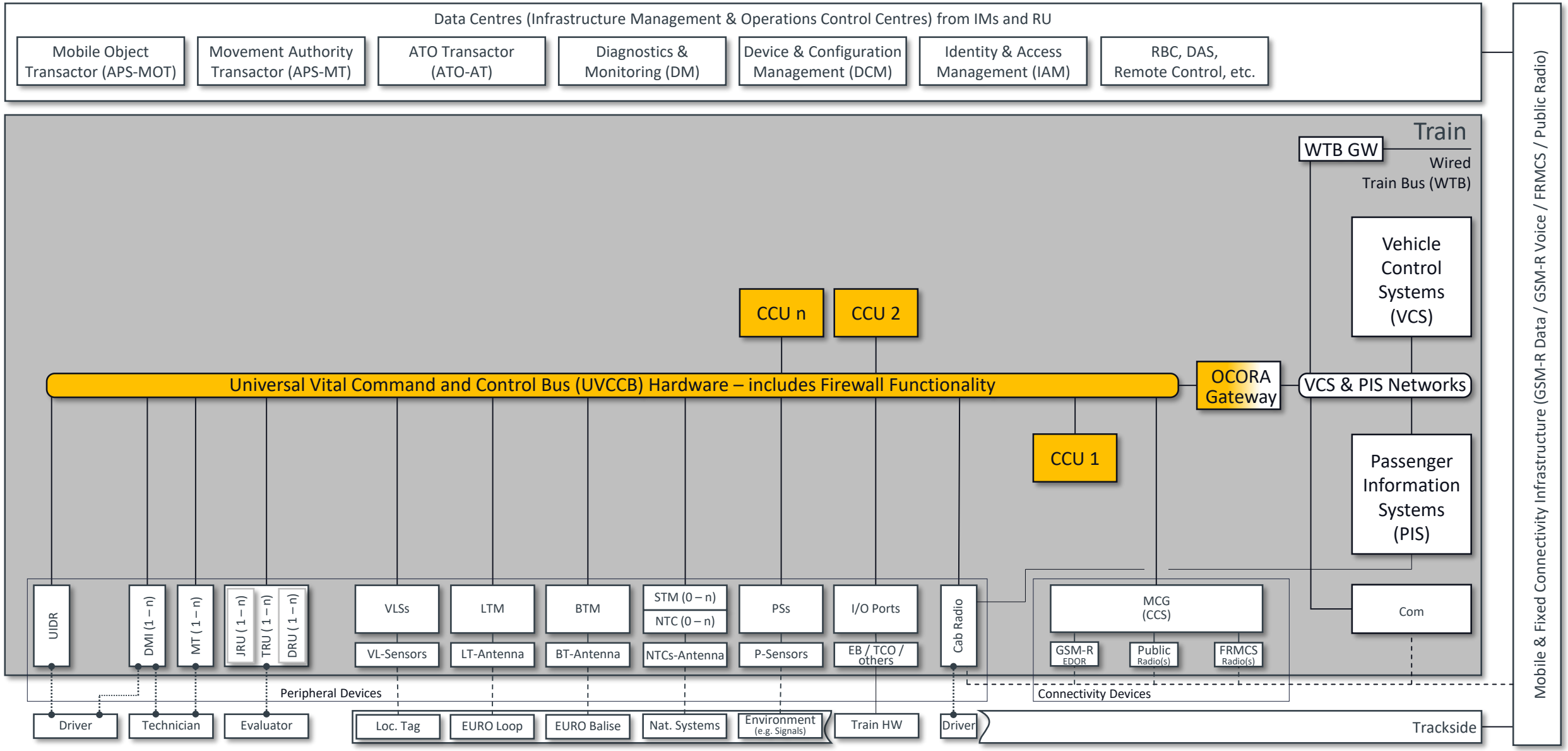
# Hardware Components – Building Blocks (tentative)



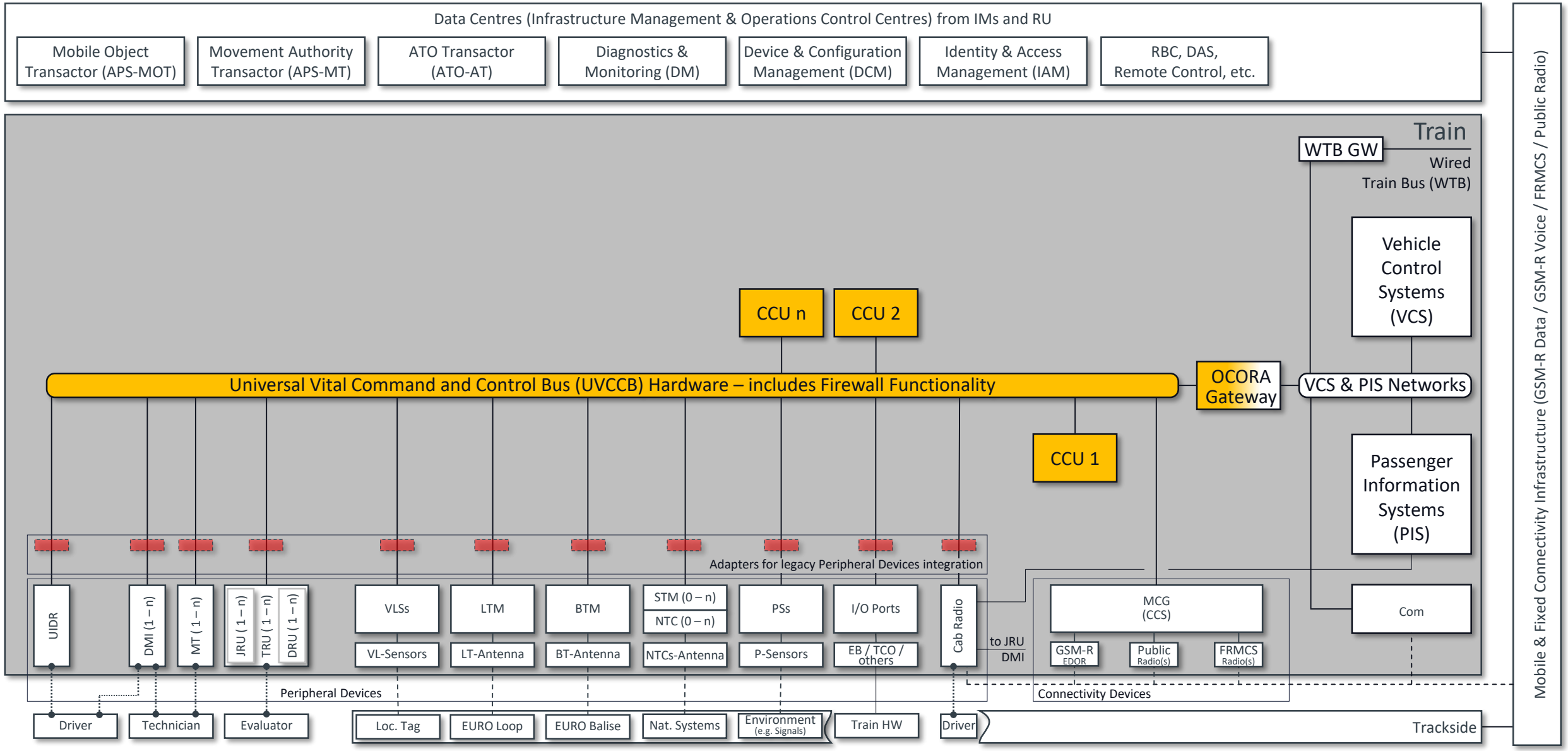
# Train Integration Scenarios

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

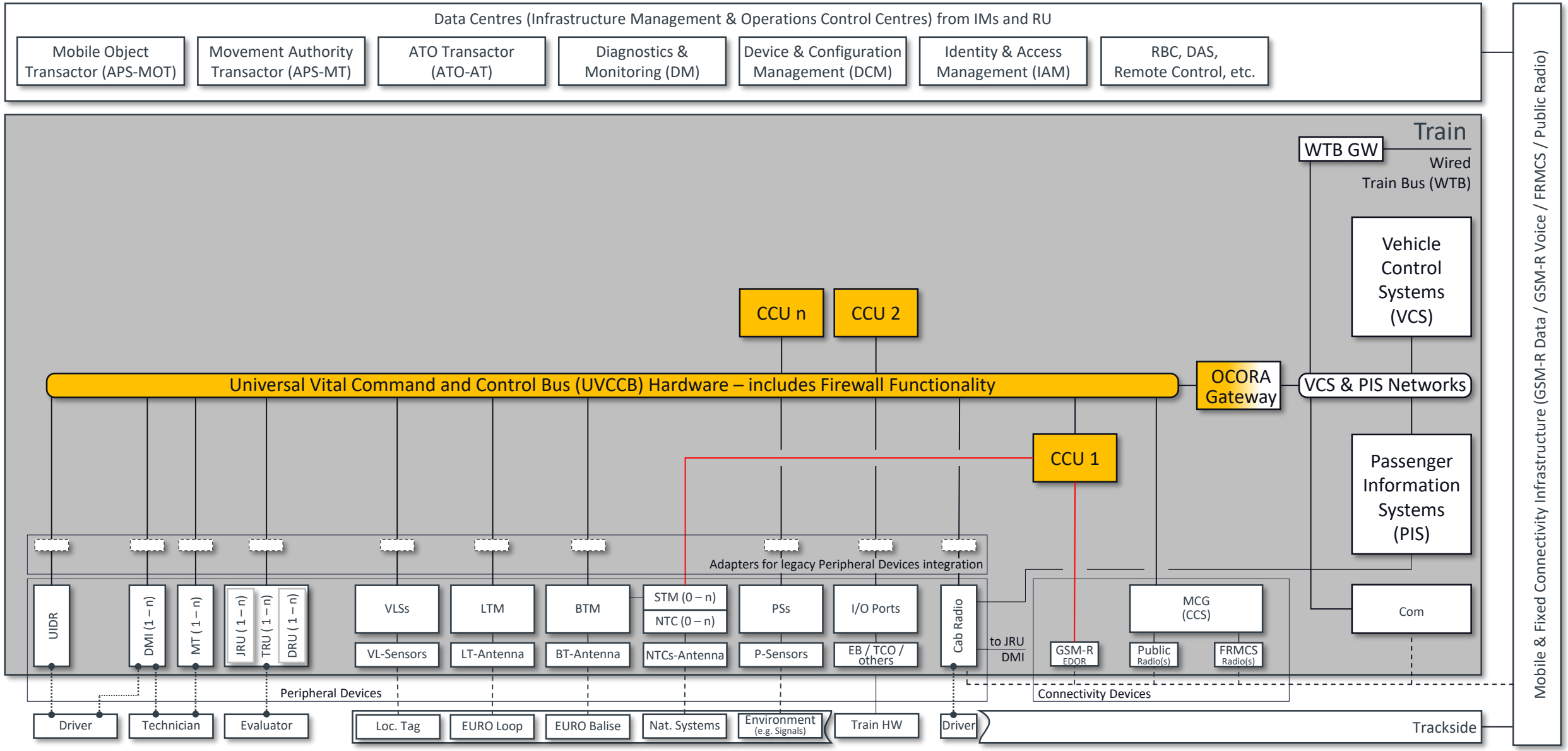
# Scenario 1a: Legacy Train – OCORA Compliant CCS Peripherals



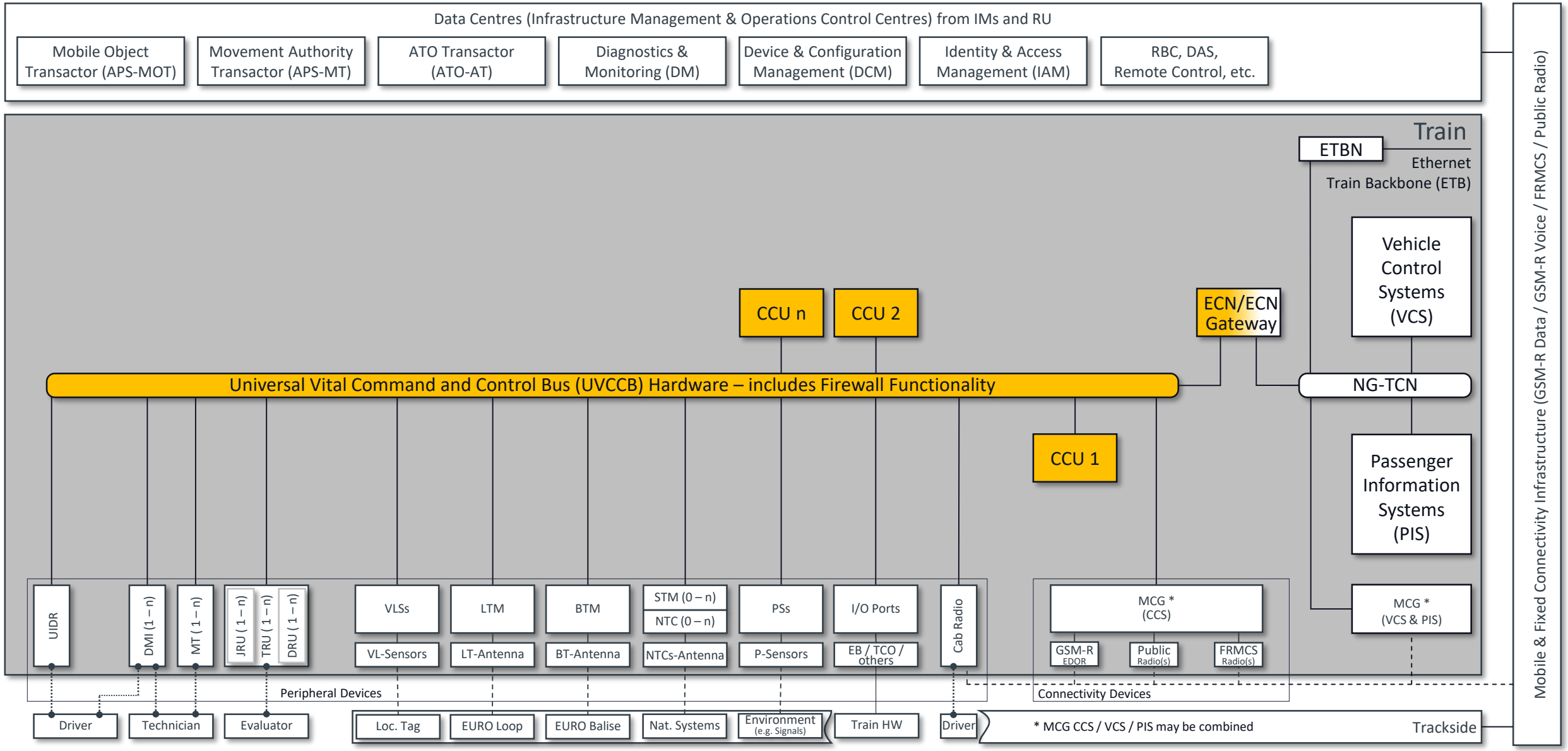
# Scenario 1b: Legacy Train – Legacy CCS Peripherals with Adapters



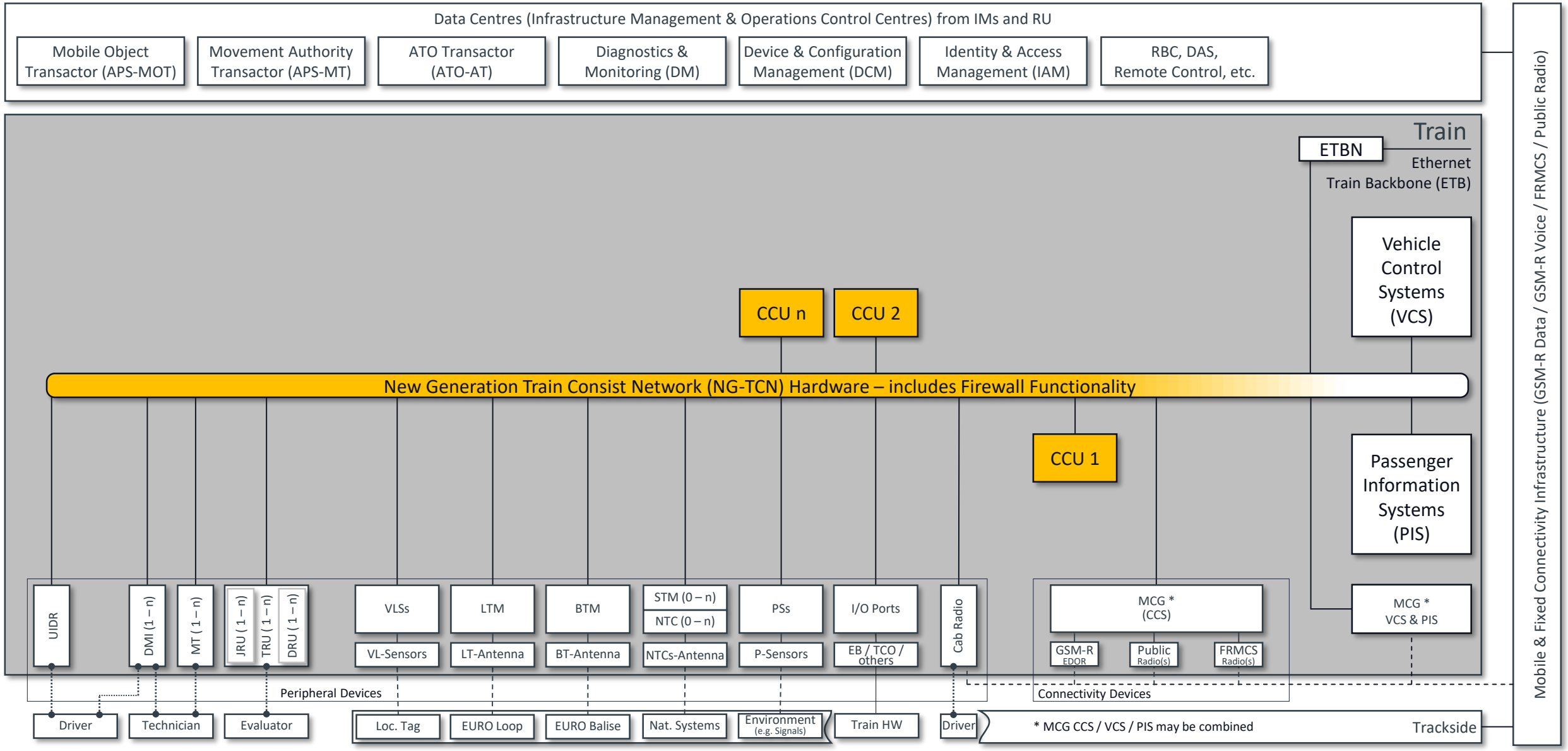
# Scenario 1c: Legacy Train – Legacy CCS Peripherals w/o Adapters



# Scenario 2: NG-TCN Train (Separate Network)



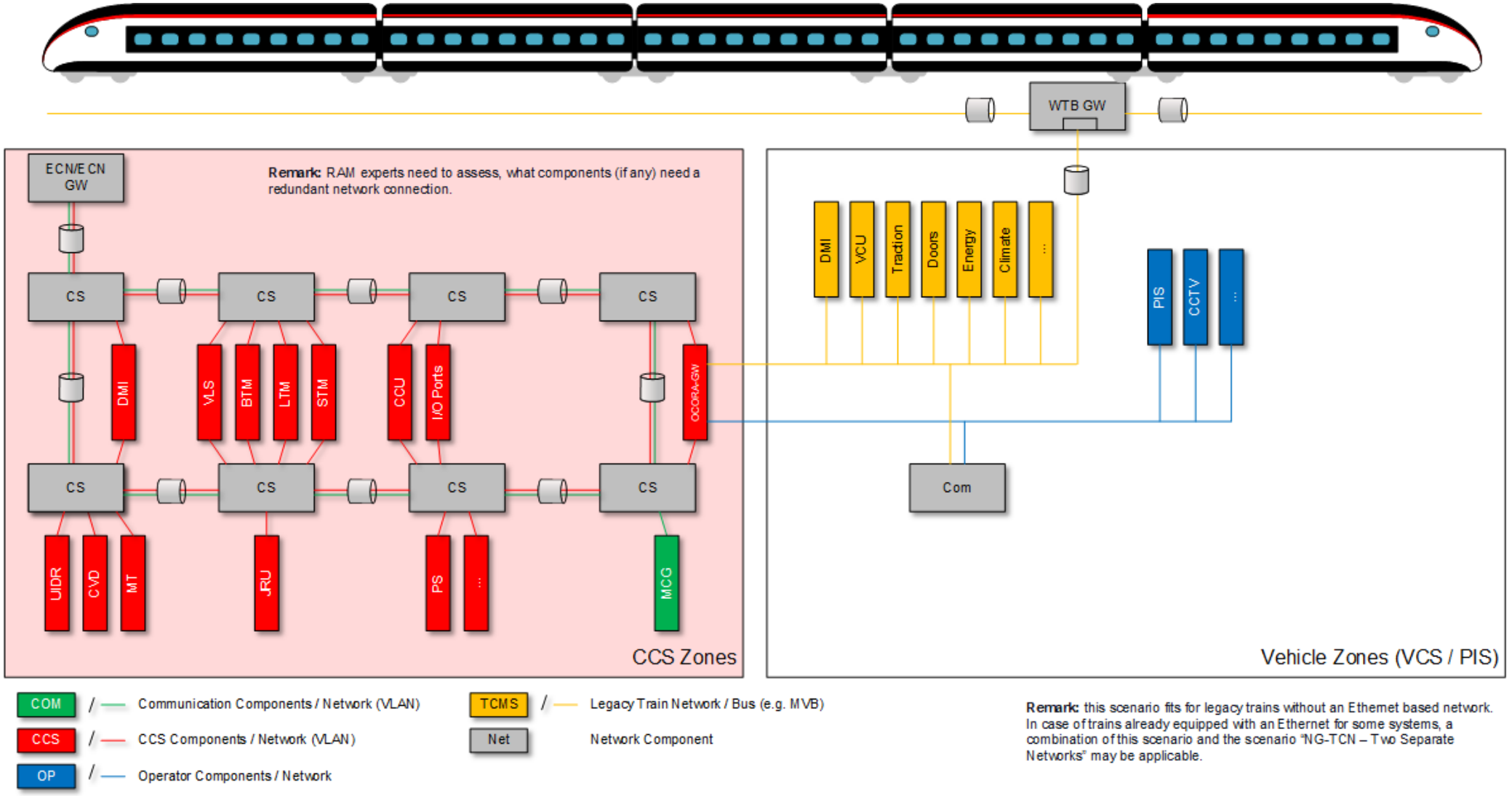
# Scenario 3: NG-TCN Train (Common Network)



# Network Topology Scenarios

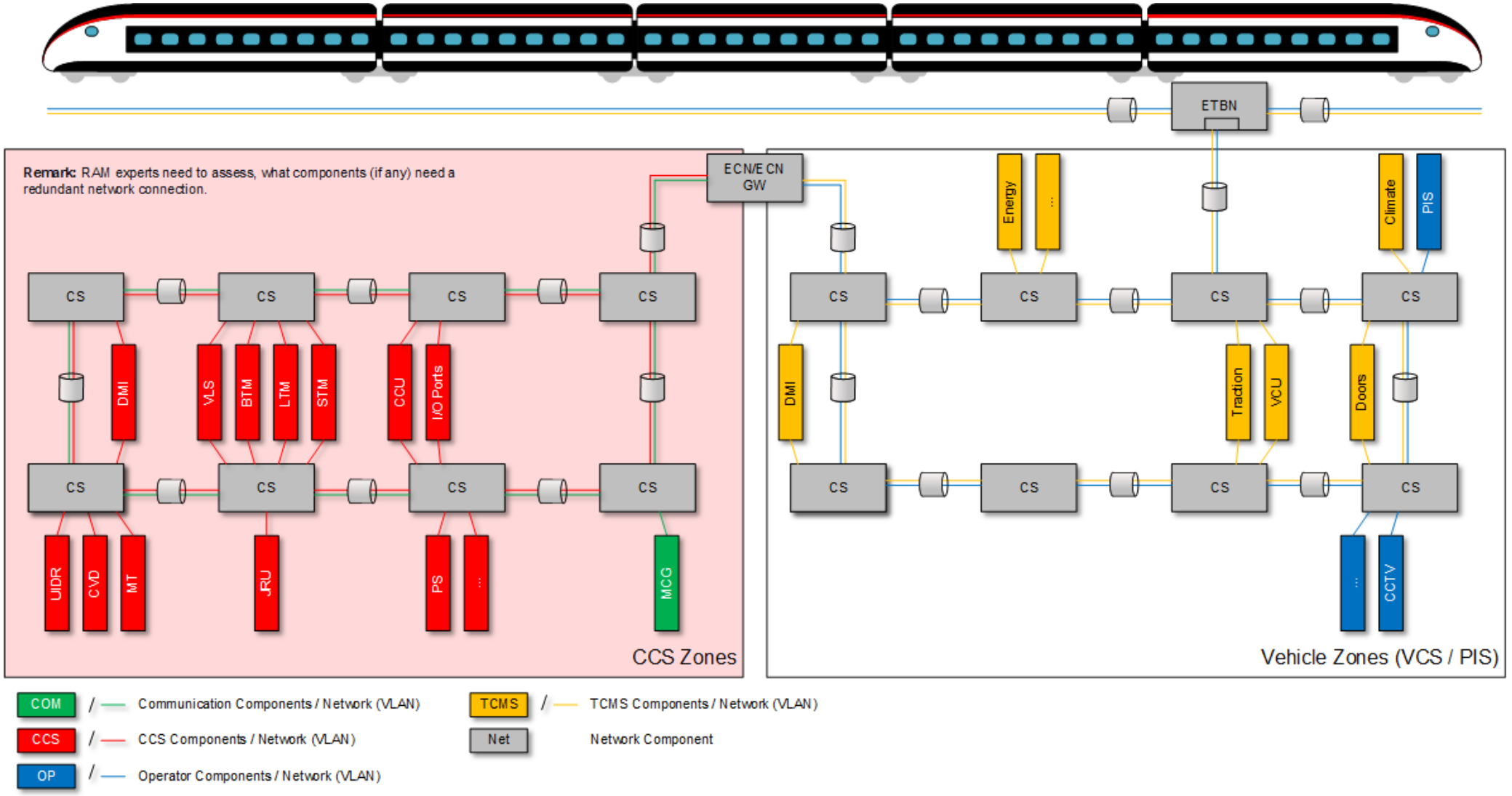
OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# Scenario 1: Legacy Train – Network Integration with OCORA-GW

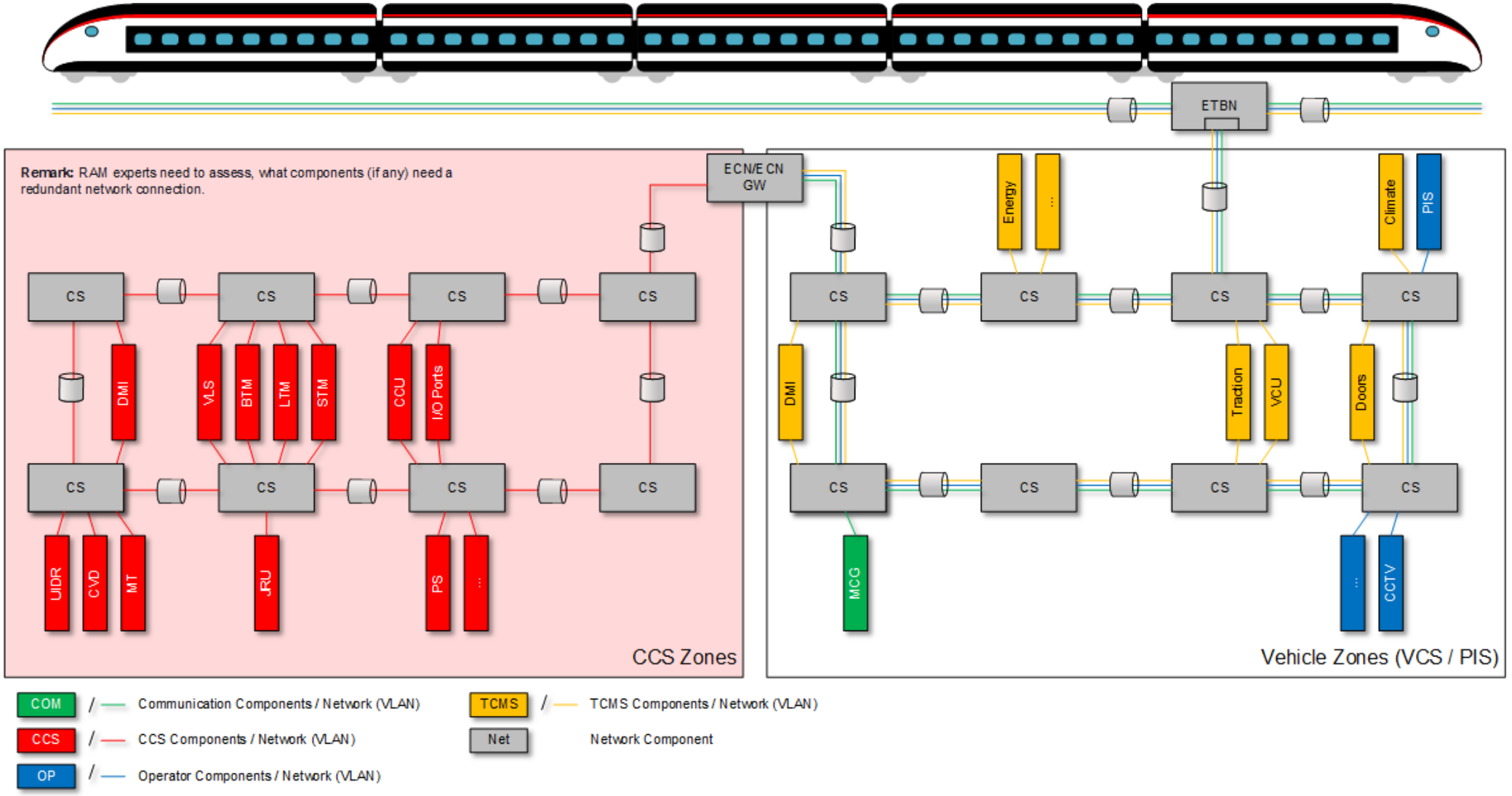



**Remark:** this scenario fits for legacy trains without an Ethernet based network. In case of trains already equipped with an Ethernet for some systems, a combination of this scenario and the scenario "NG-TCN – Two Separate Networks" may be applicable.

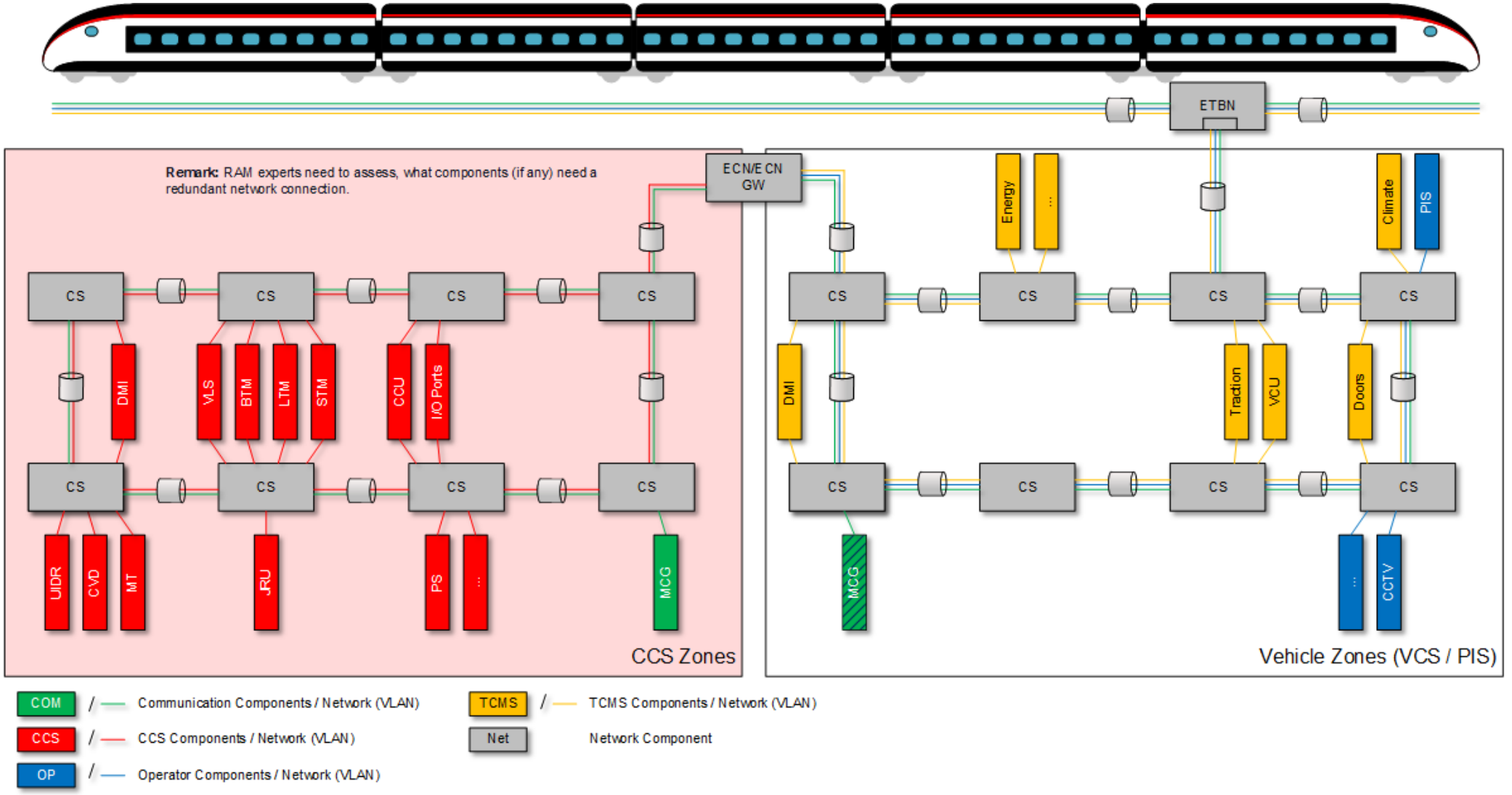
# Scenario 2: NG-TCN Train – Two Separate Networks



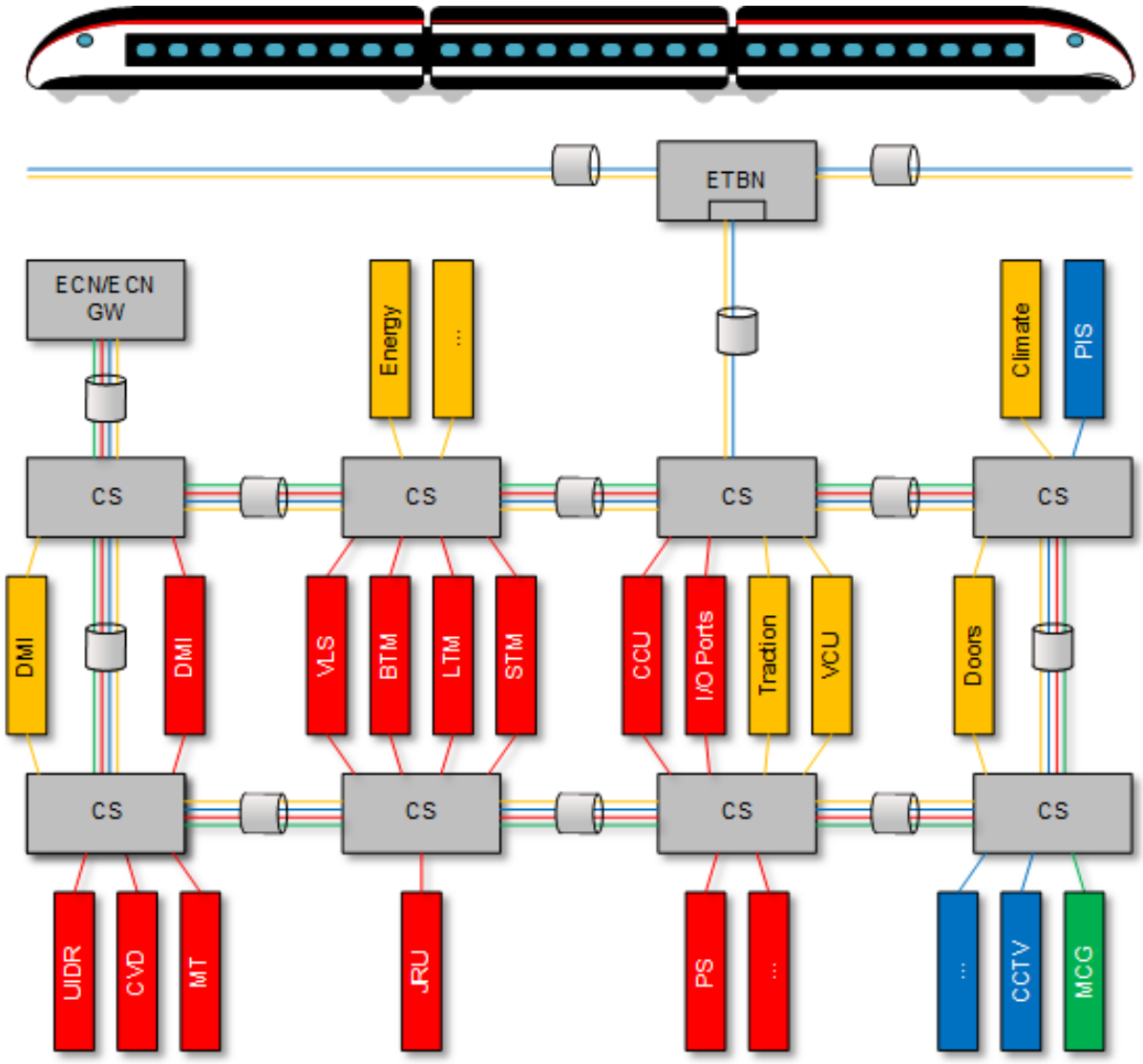
# Scenario 2a: NG-TCN Train – Two Separate Networks



# Scenario 2b: NG-TCN Train – Two Separate Networks



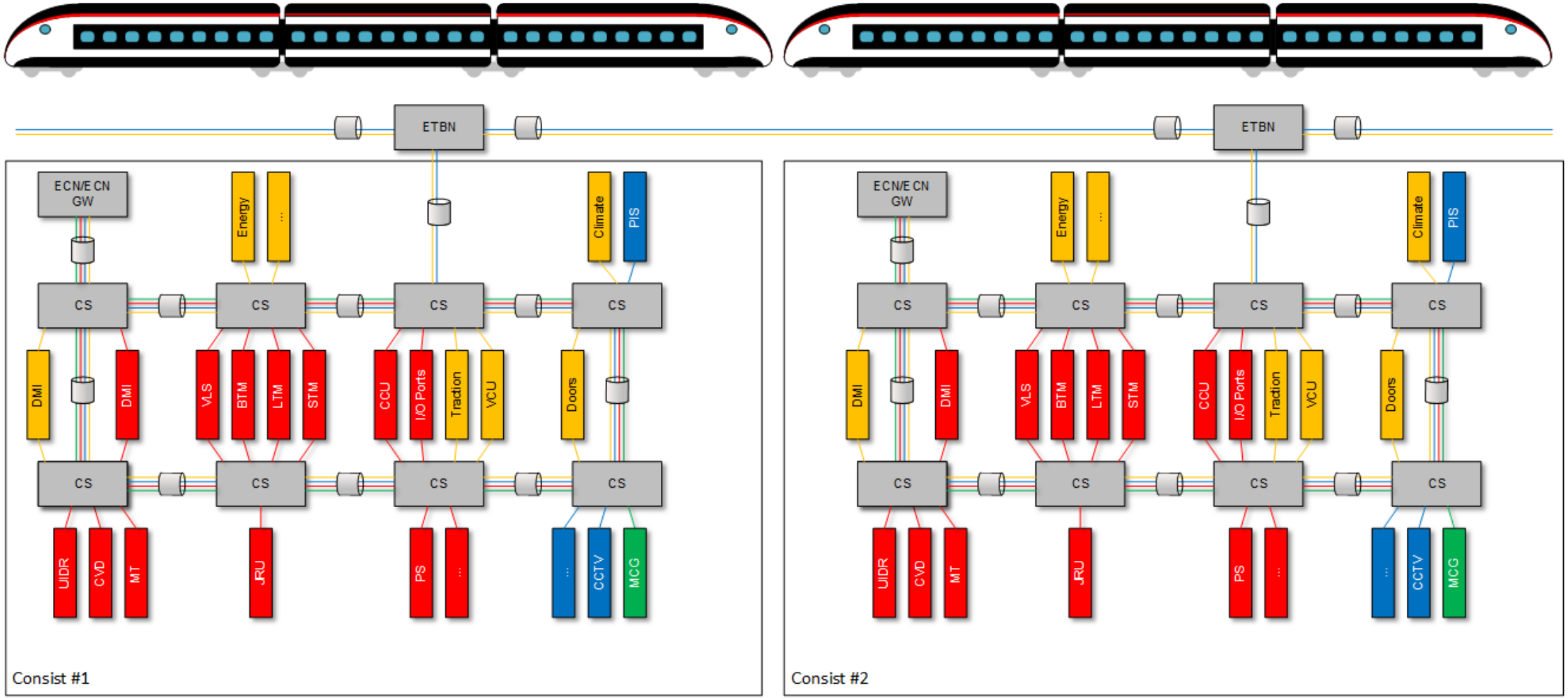
# Scenario 3: NG-TCN Train – Common Network (Virtual LANs)




**Remarks:**
-Security experts need to assess, if this is a feasible scenario.
-RAM experts need to assess, what components need a redundant network connection.

COM / Communication Components / Network (VLAN)
CCS / CCS Components / Network (VLAN)
OP / Operator Components / Network (VLAN)
TCMS / TCMS Components / Network (VLAN)
Net Network Component

# Connecting Multiple Consists



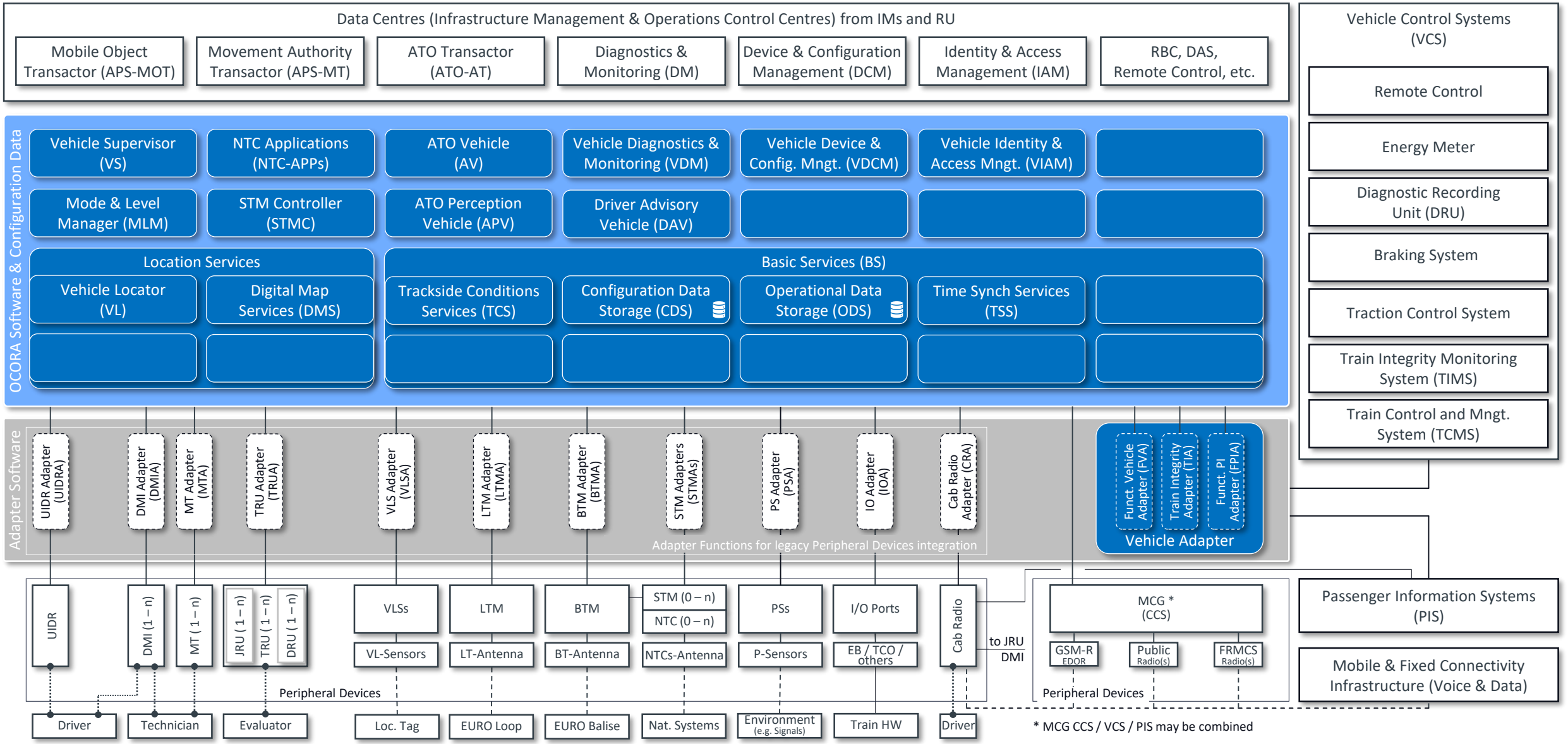

COM / Communication Components / Network (VLAN)
CCS / CCS Components / Network (VLAN)
OP / Operator Components / Network (VLAN)
TCMS / TCMS Components / Network (VLAN)
Net Network Component

**Remarks:**
- The network topology depicted in the consists correspond to the «Common Network (Virtual LANs)» scenario. However, others network topology scenarios are also possible.
- Refer also to remarks on previous slides.

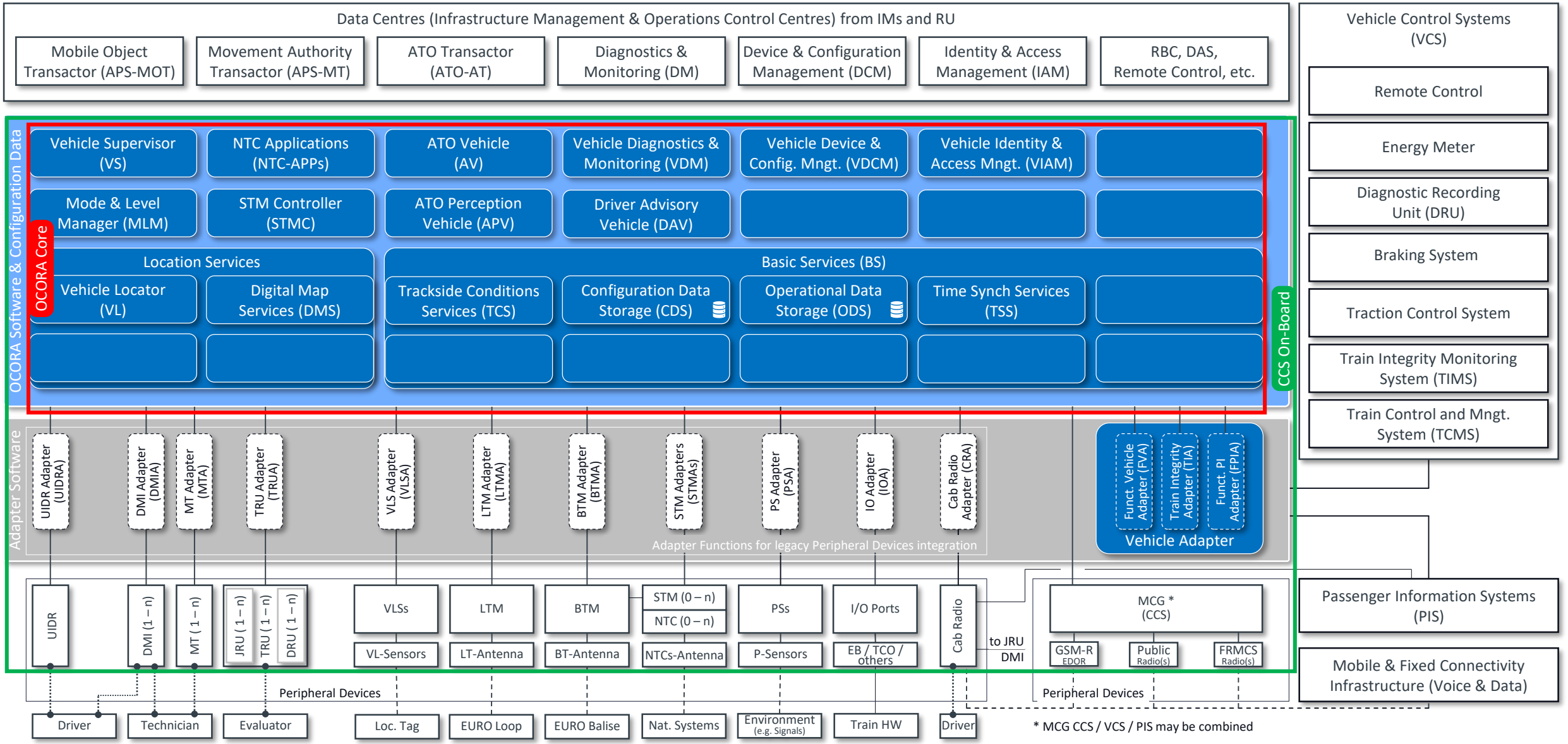
# Functional / Logical View

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

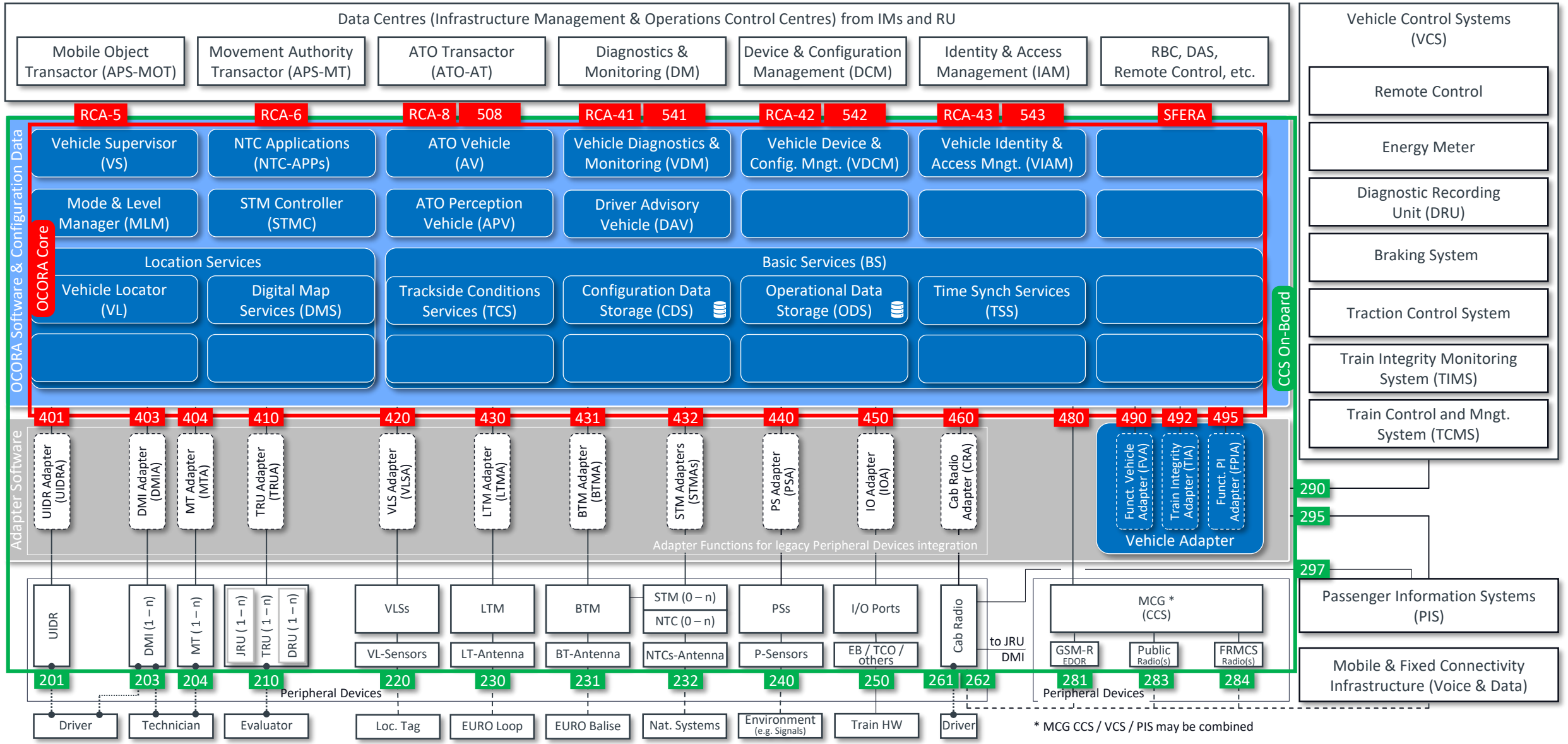
# Functional SW Components



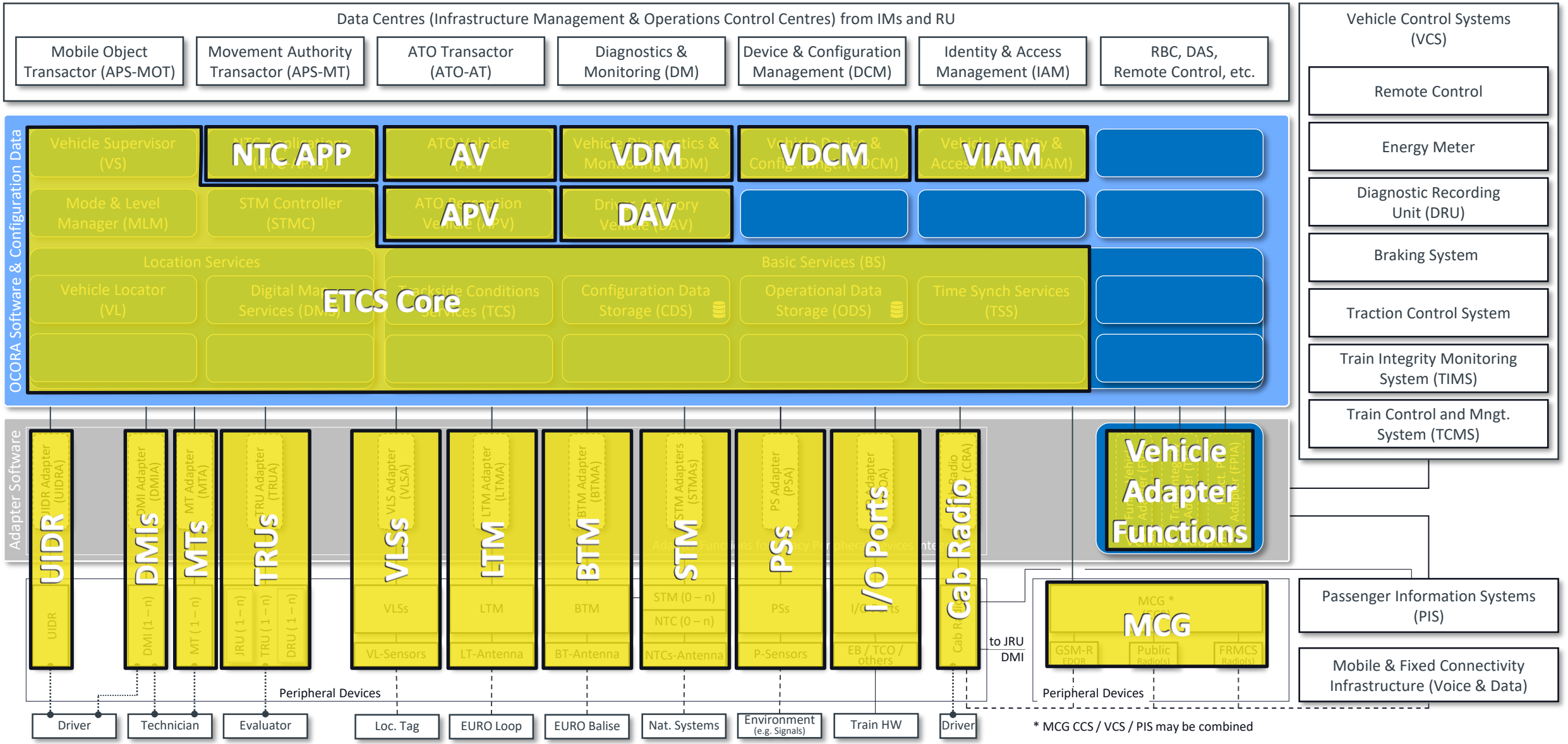
# Functional SW Components – Scope



# Functional SW Components – Interfaces



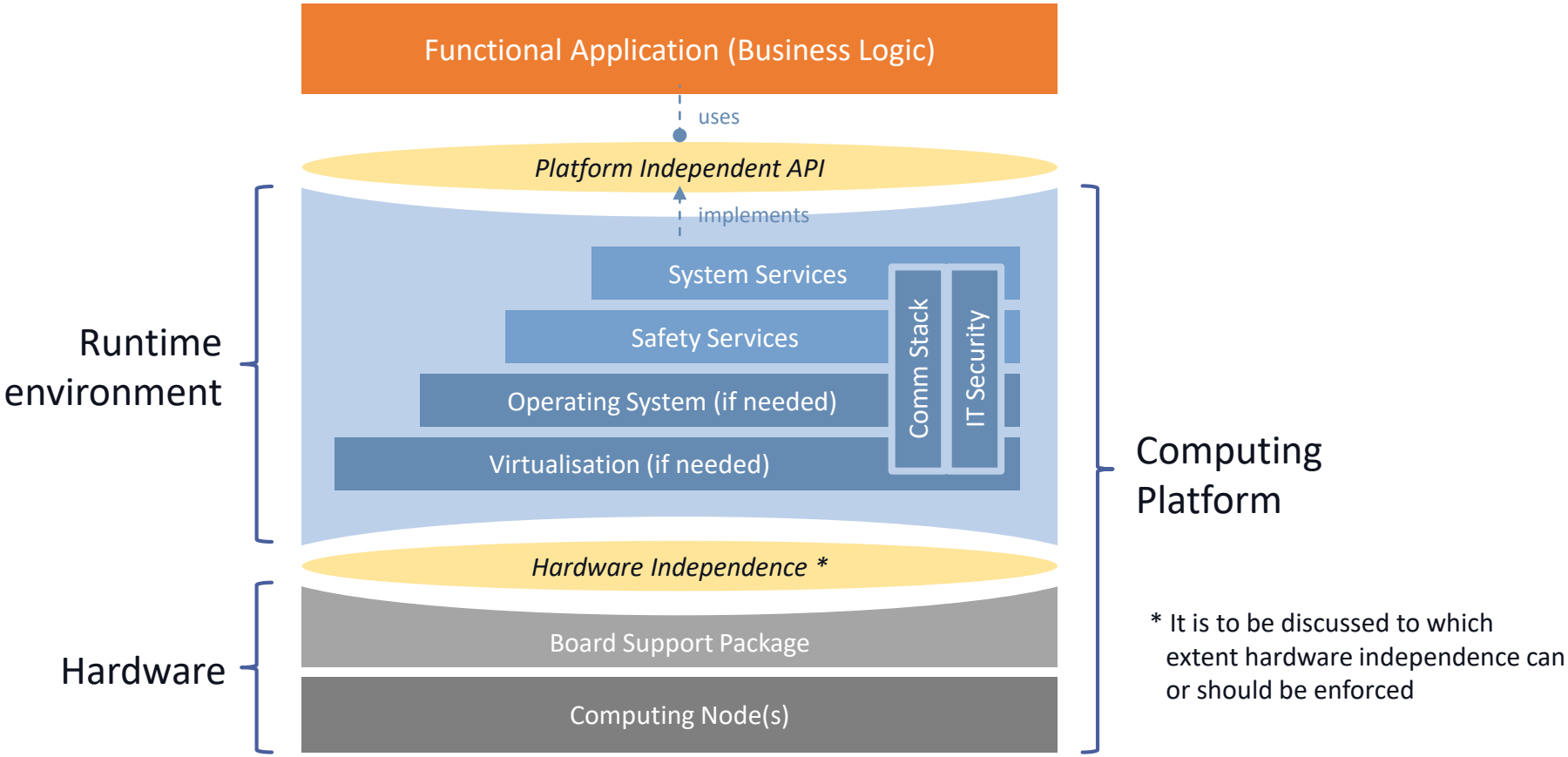
# Functional SW Components – Building Blocks (tentative)



# Computing Platform

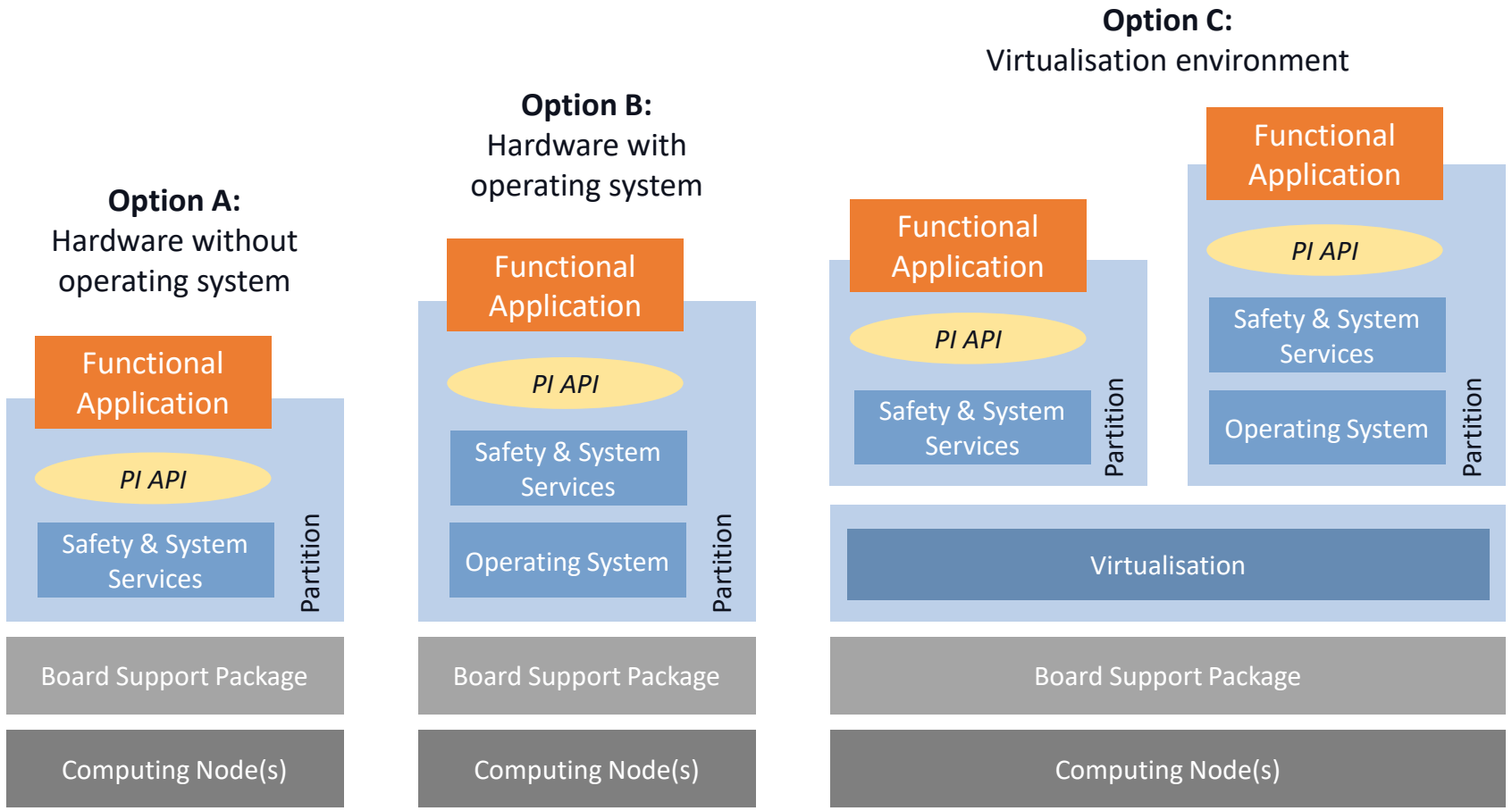
OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# Computing Platform – High Level Architecture




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

# Computing Platform – Approaches

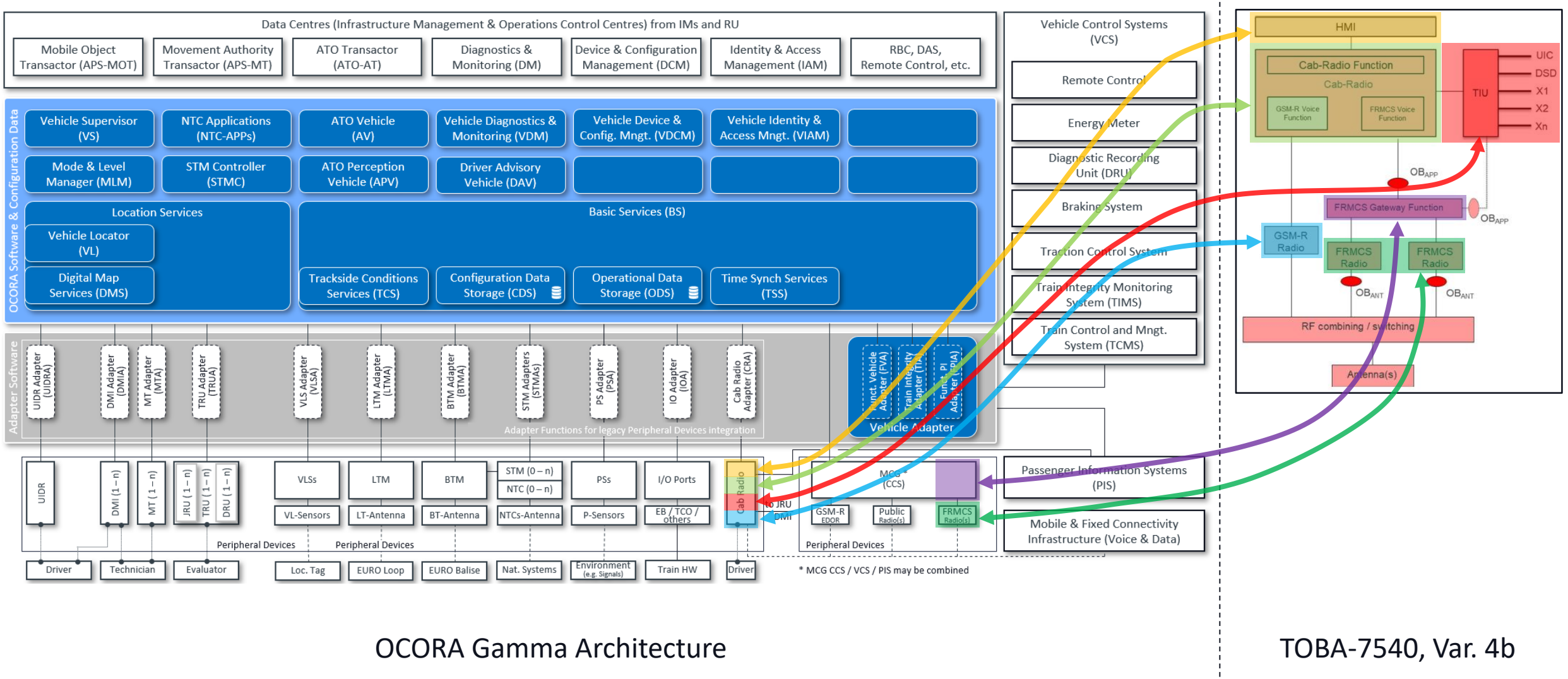



Platform options where applications are programmed against PI API. Approaches depicted in the above diagram are non-exhaustive. The industry may propose different state-of-the-art solutions

# Mapping OCORA with TOBA Architecture

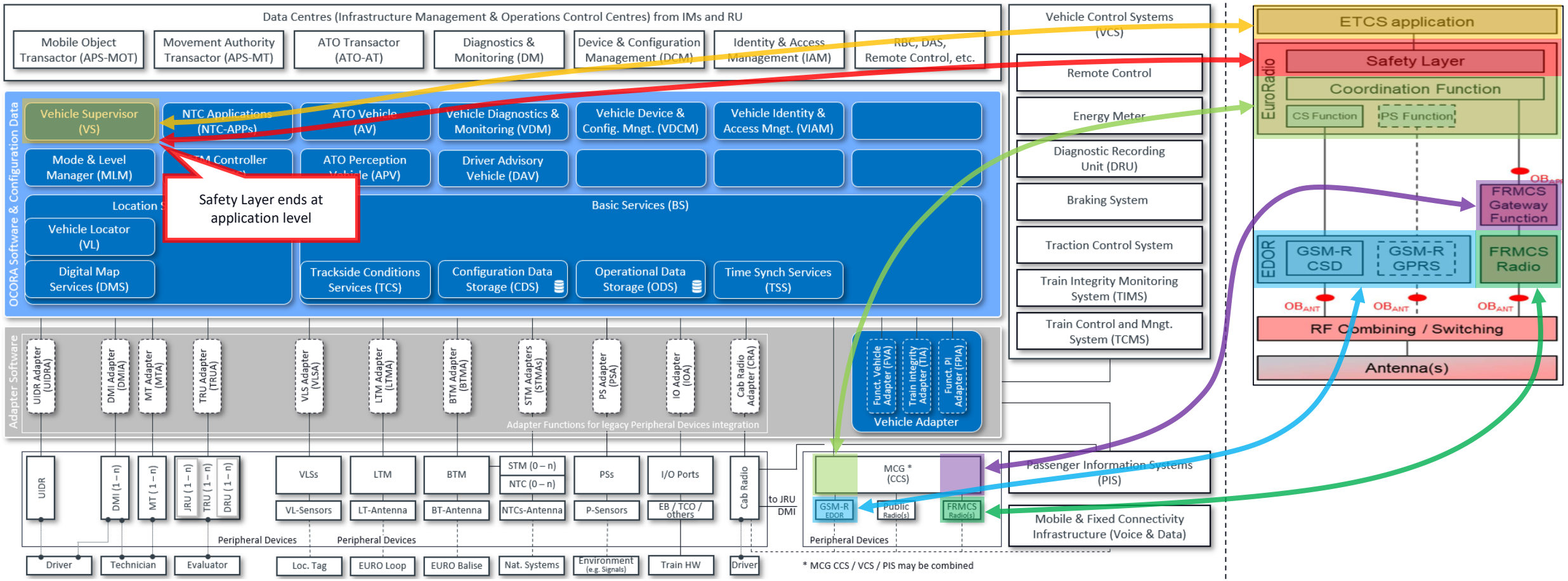
OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# Cab Radio




OCORA Gamma Architecture

TOBA-7540, Var. 4b



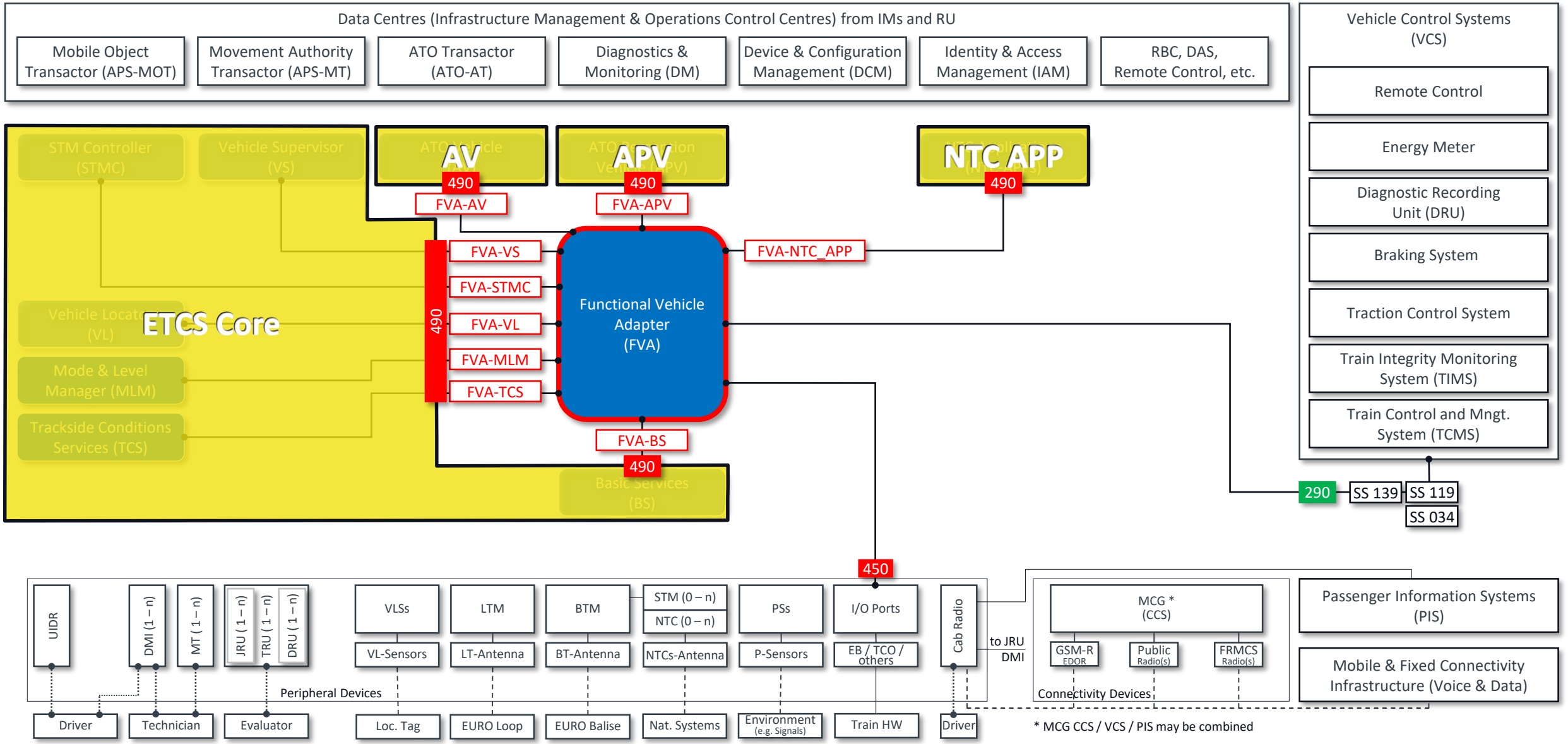

OCORA Gamma Architecture

TOBA-7540, Var. 3

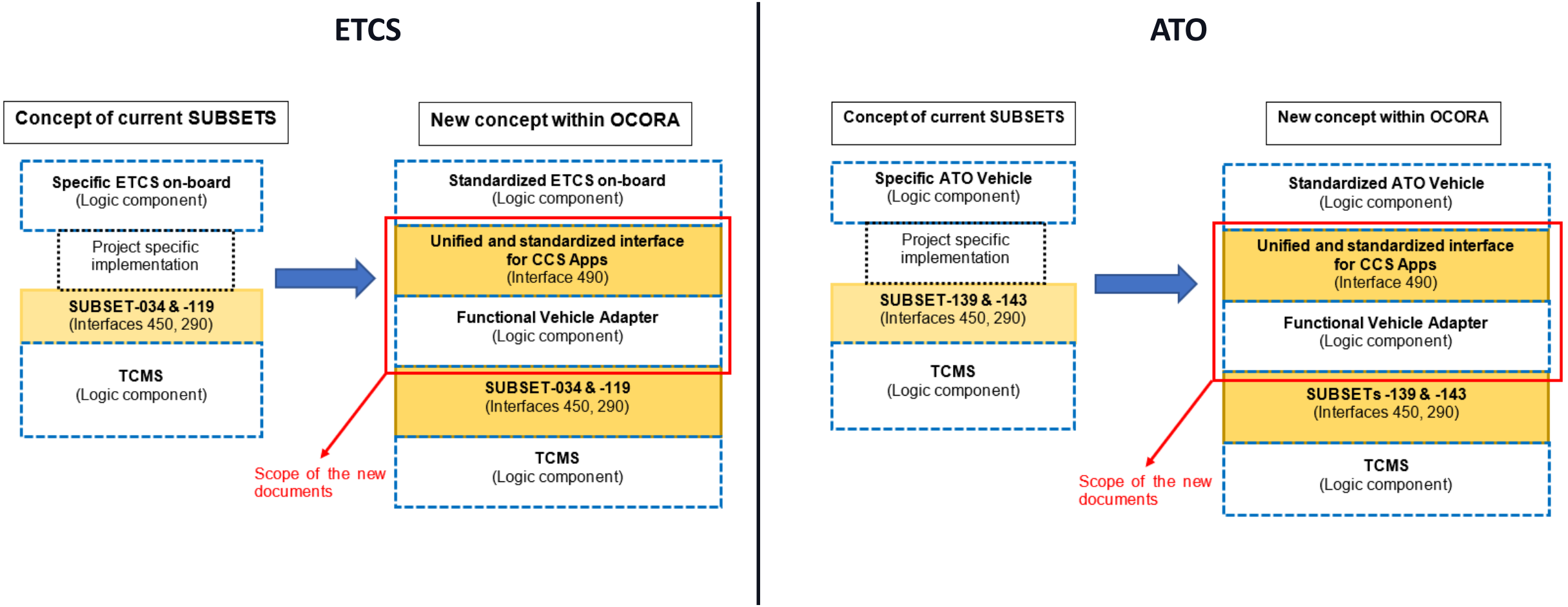
# Functional Vehicle Adapter (FVA)

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# Functional Vehicle Adapter (FVA) – Functional IFs



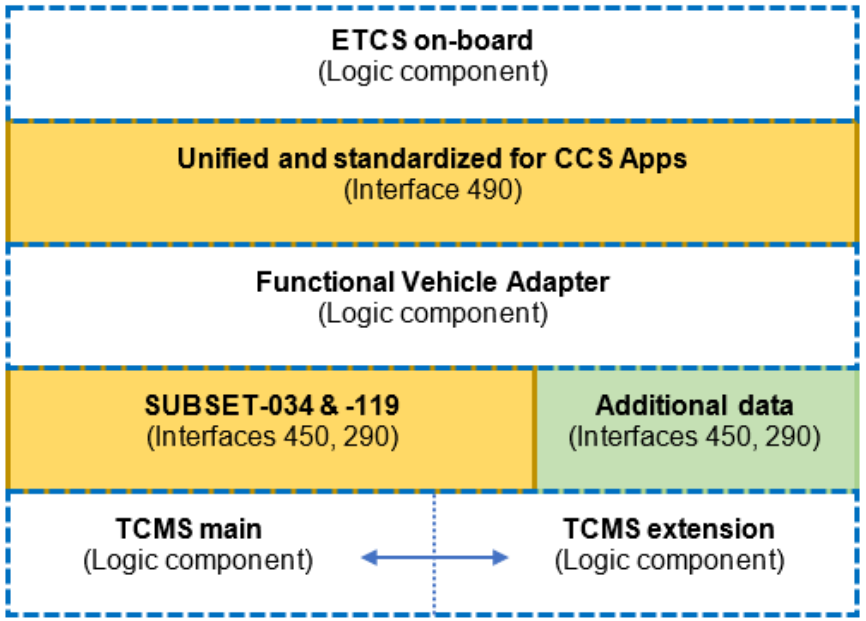
# OCORA – Functional Vehicle Adapter



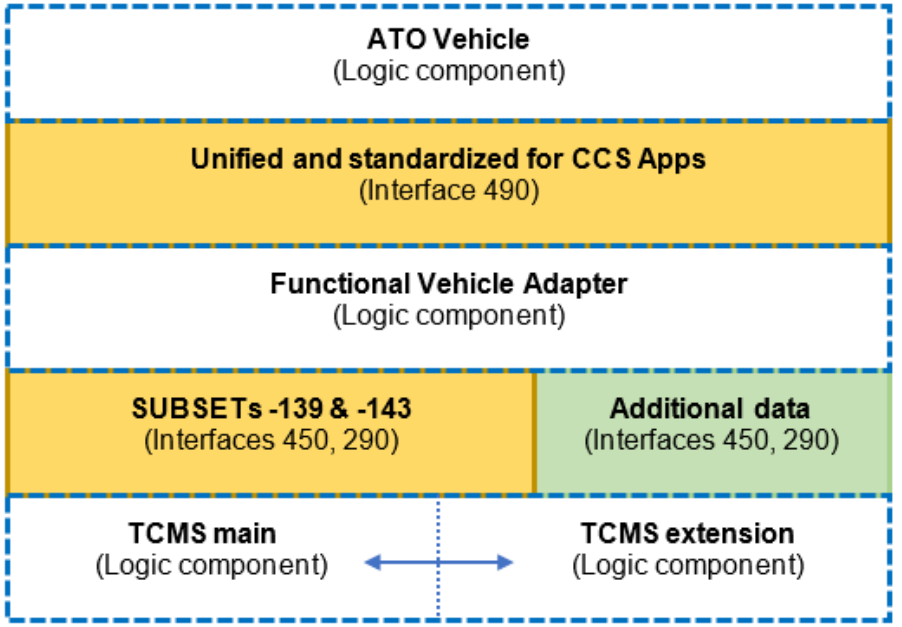

Details in Document: OCORA-40-005-Functional Vehicle Adapter – Introduction & Overview

# OCORA – Functional Vehicle Adapter: Extensions

## ETCS




## ATO




Details in Document:

OCORA-40-006-CCS-TCMS Interface - ETCS Functionality SS119

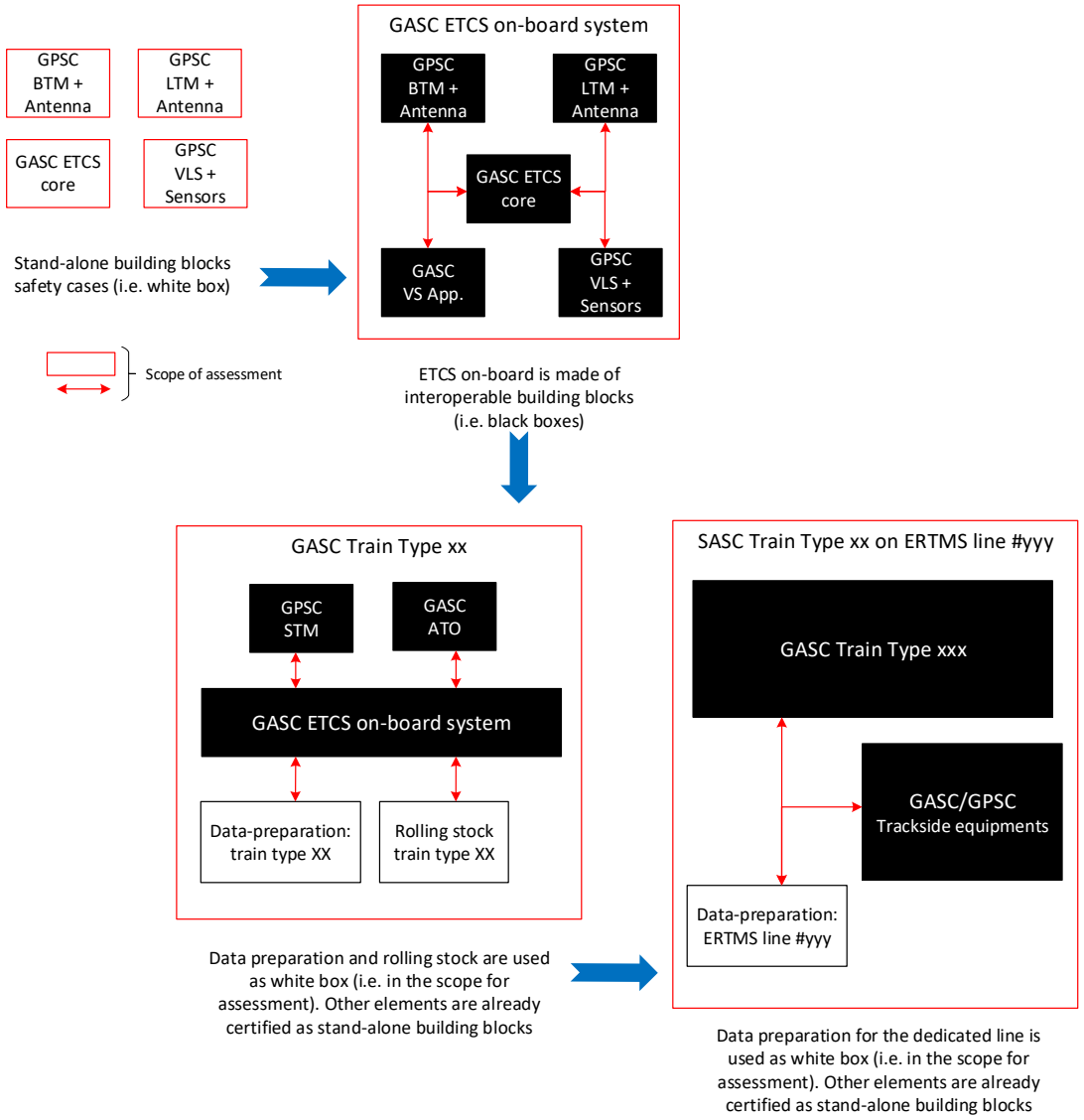
OCORA-40-007-CCS-TCMS Interface - ATO Functionality SS139

# Modular Safety

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# OCORA – Modular Safety

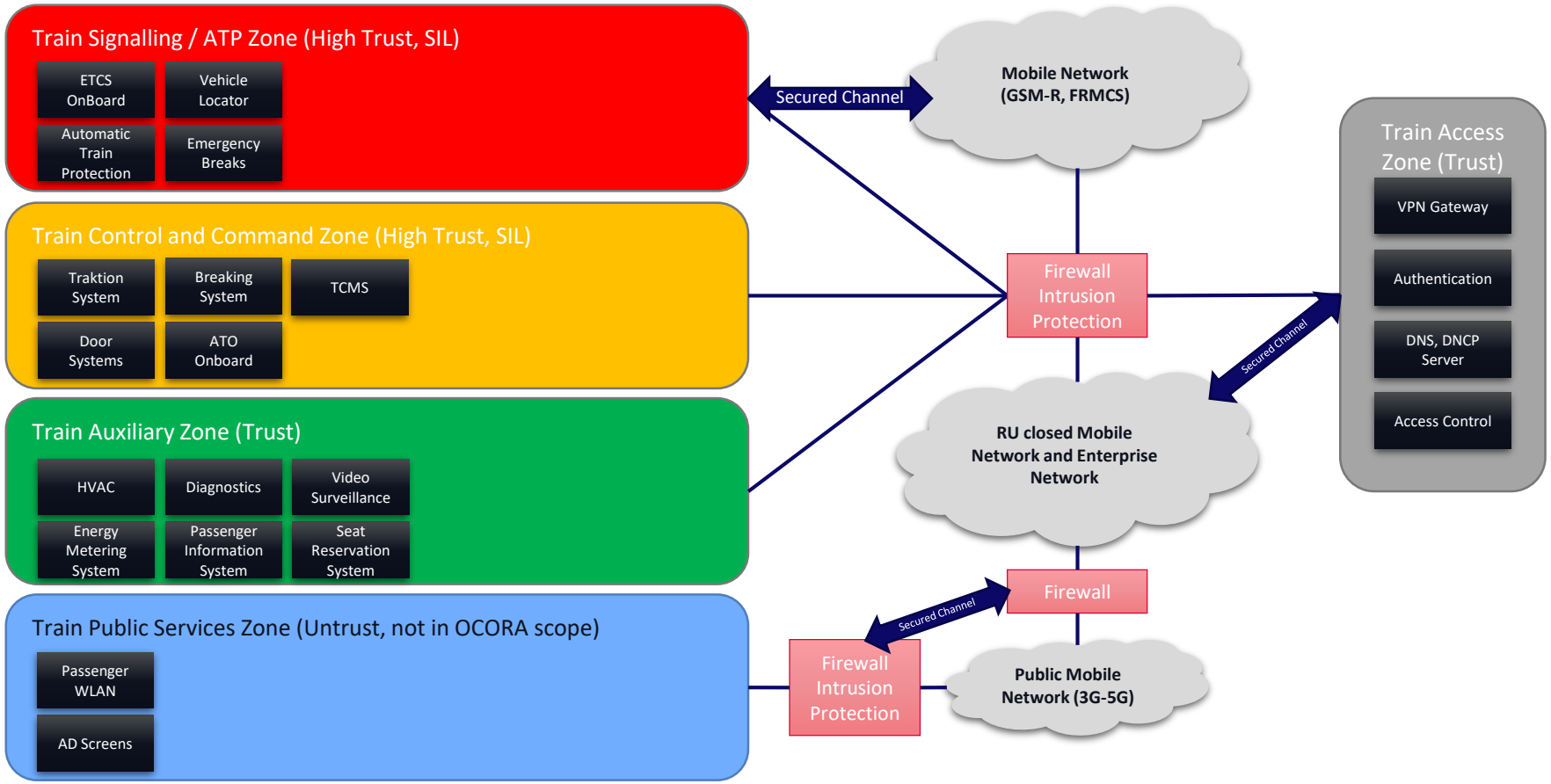
- Modular Safety defines the hierarchy between safety cases from building blocks to specific application(s).
- One of the main goal is to reduce the certification efforts (initial- and re-certification) at all levels without degrading the safety level of the analyses.
- Modular Safety shall also defines 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 Gamma release
  - Harmonised and generic set of SRAC



# Security

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# OCORA – Security High Level Zones



# OCORA – Security 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 |

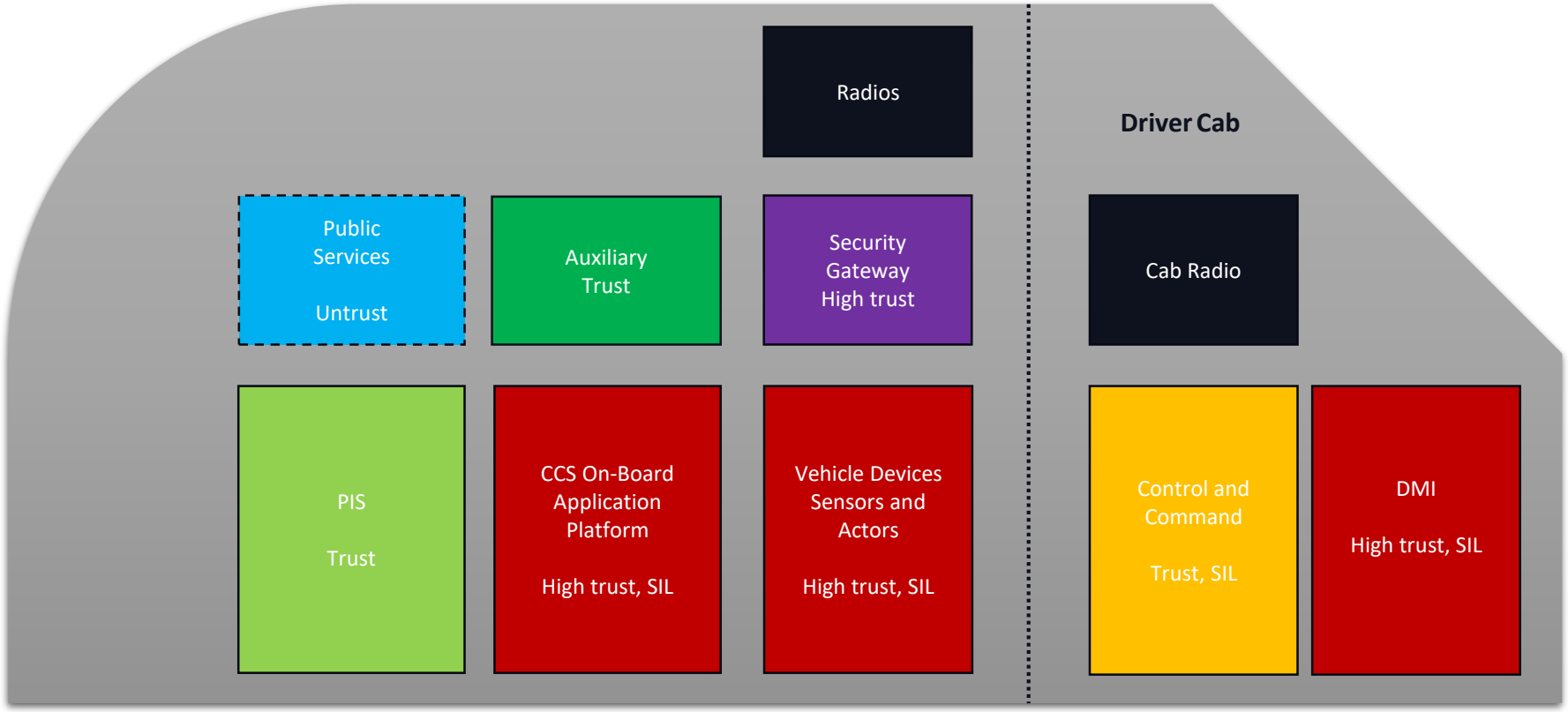
x0 = no requirements
x1 = standard requirements
x2 = enhanced requirements

* 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

# OCORA – Security Zones

Zones:

- Train
- Vehicle
- Driver Cab
- Wagon (passenger area)
- CCU
- Device Sensors and Actors
- Gateway
- Radios (GSM-R, FRMCS)
- Cab Radio
- DMI
- Control and Command
- PIS
- Auxiliary
- Public Services*



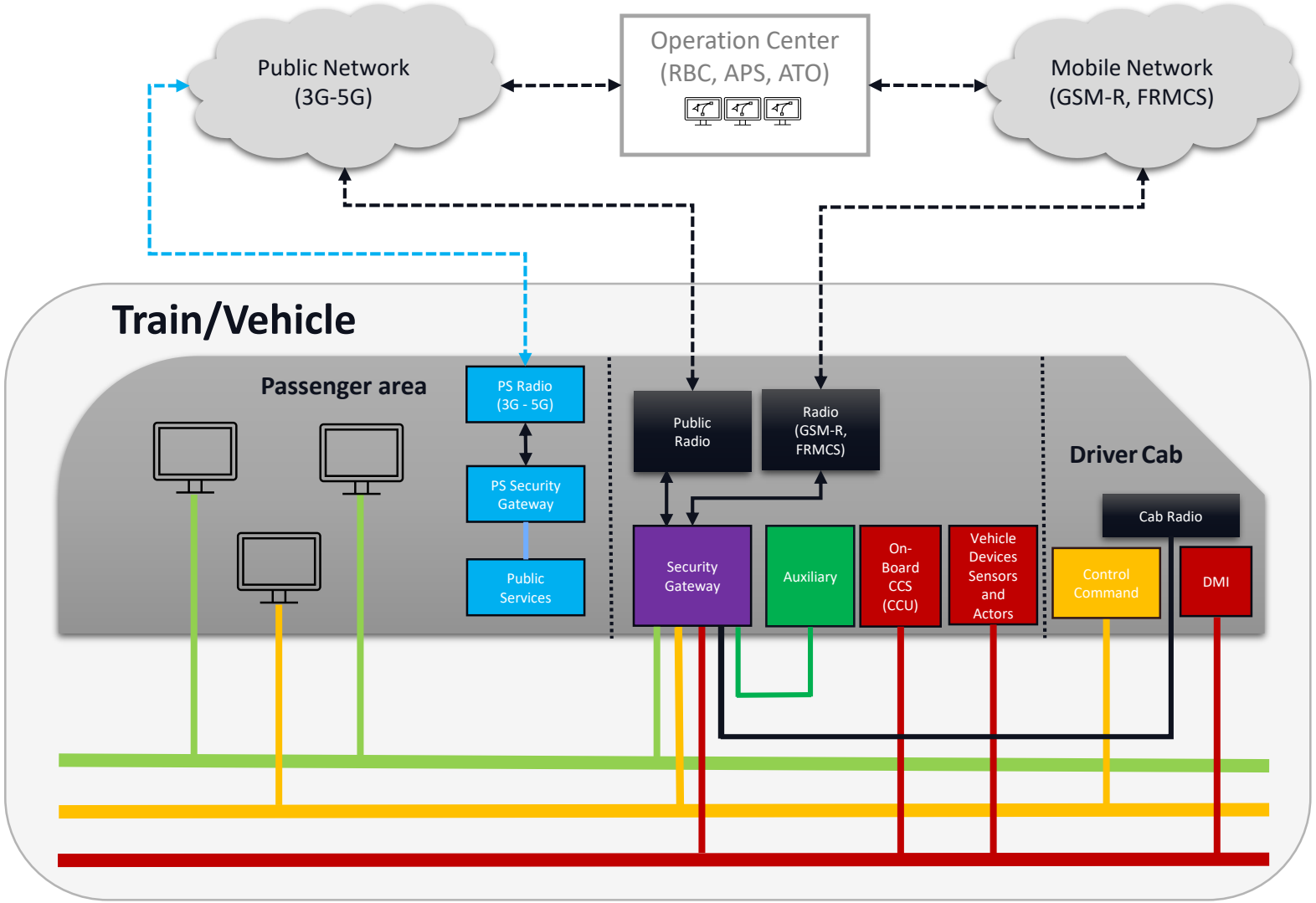

* Not in OCORA scope

# OCORA – Security Zones and Conduits

## Conduits

- PIS
- VCN/TCN
- UVCCB
- Auxiliary
- Radio (GSM-R, FRMCS)
- Public Radio (secured)
- Cab Radio
- PS Radio
- Public Services*

* Not in OCORA scope




Passenger Information Network

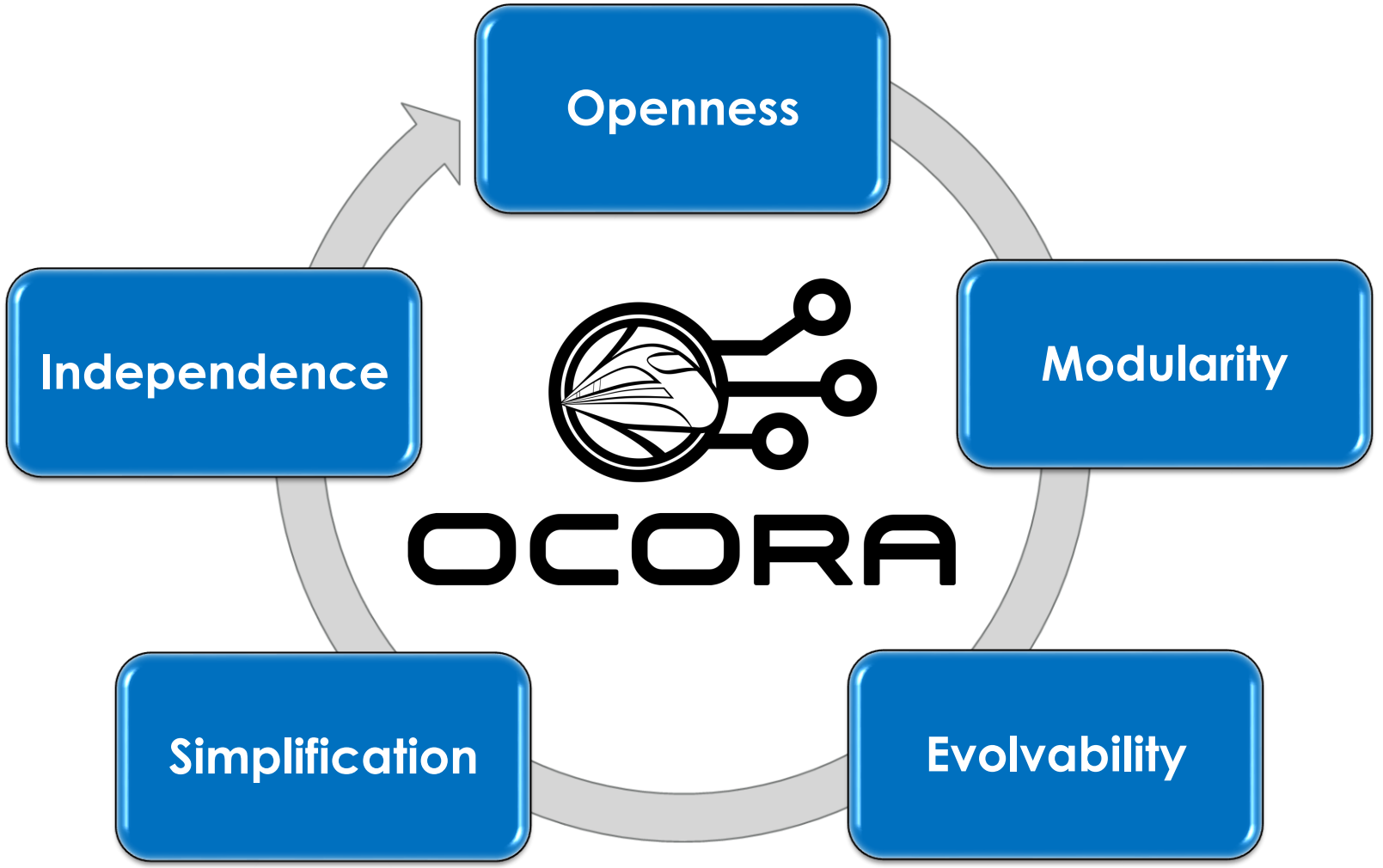
Vehicle Control Network

Universal Vital Control and Command Bus
(UVCCB; CCS-On-Board Network)

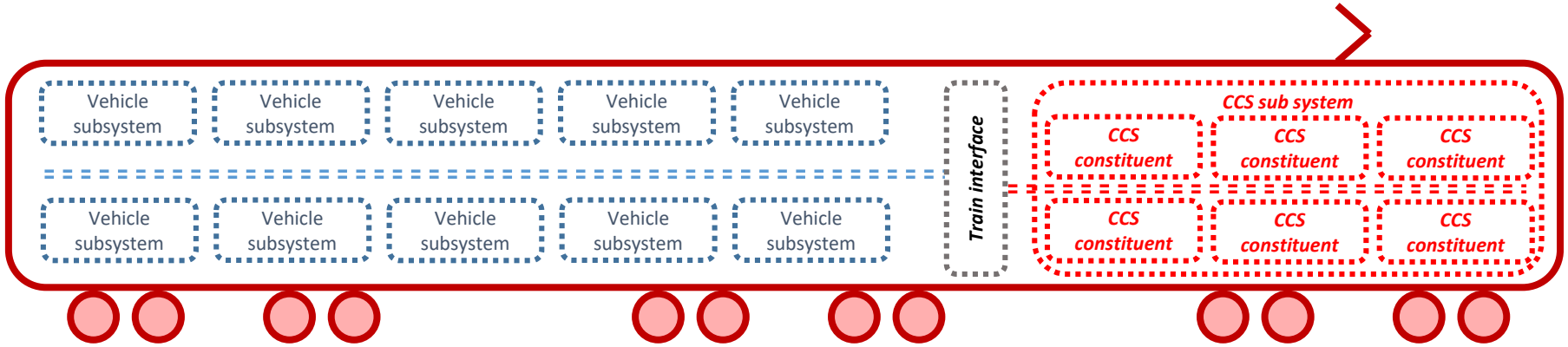
# Supporting Slides

OCORA-20-003-Gamma / v1.02 / 04.12.2020 - Final

# OCORA Key Principles

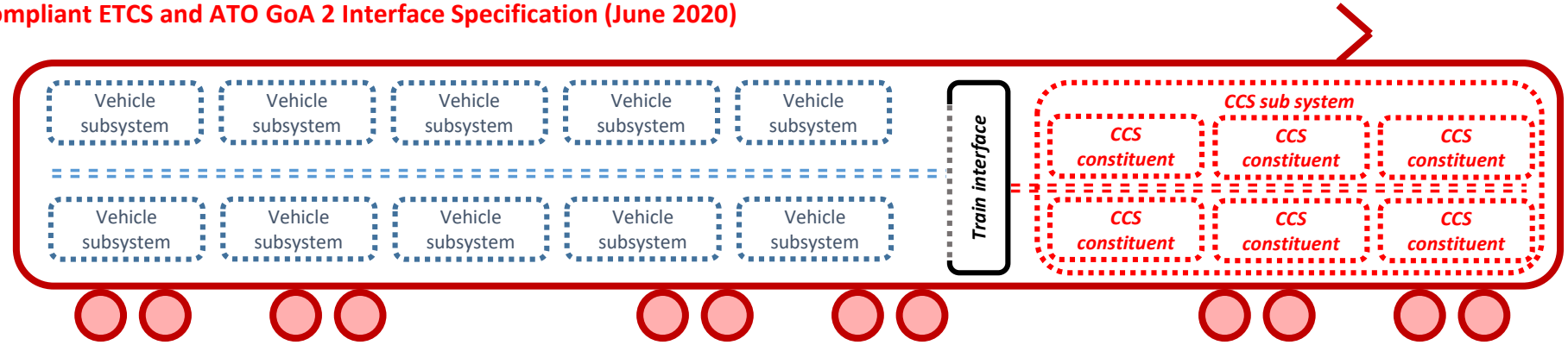


**Level of Modularity 0** (current situation): the integrated proprietary CCS system is (again) fully integrated in the proprietary vehicle environment, driving costs and risks and complicating obsolescence issue



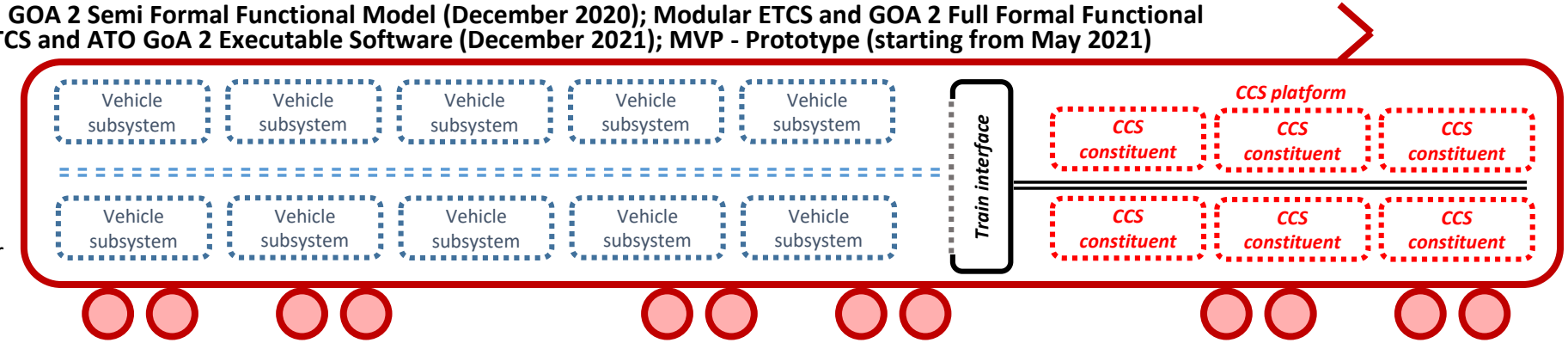

**Project proposal: SS119 and SS139 Compliant ETCS and ATO GoA 2 Interface Specification (June 2020)**

**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



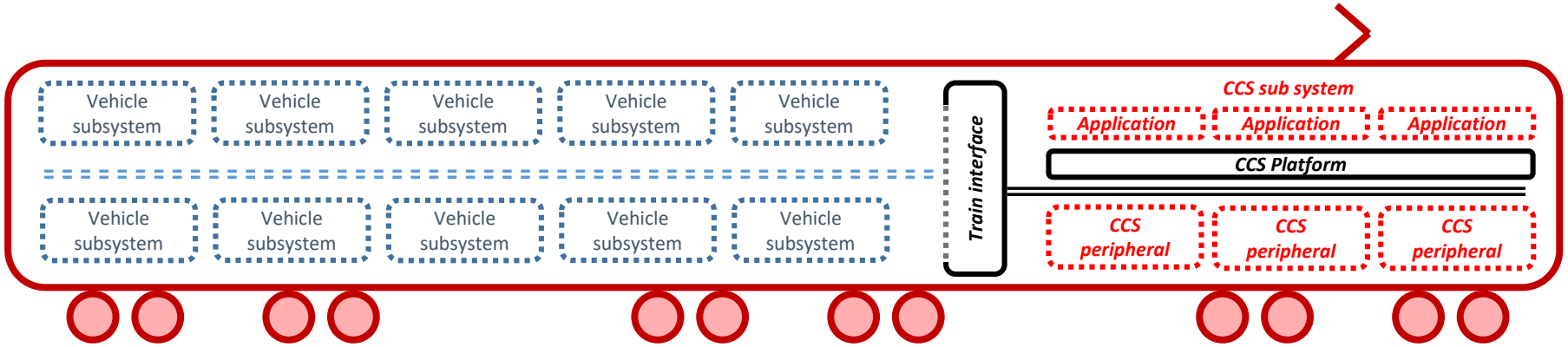

**Project proposals: Modular ETCS and GOA 2 Semi Formal Functional Model (December 2020); Modular ETCS and GOA 2 Full Formal Functional Model (December 2021); Modular ETCS and ATO GoA 2 Executable Software (December 2021); MVP - Prototype (starting from May 2021)**

**Level of Modularity 2** (short term OCORA 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

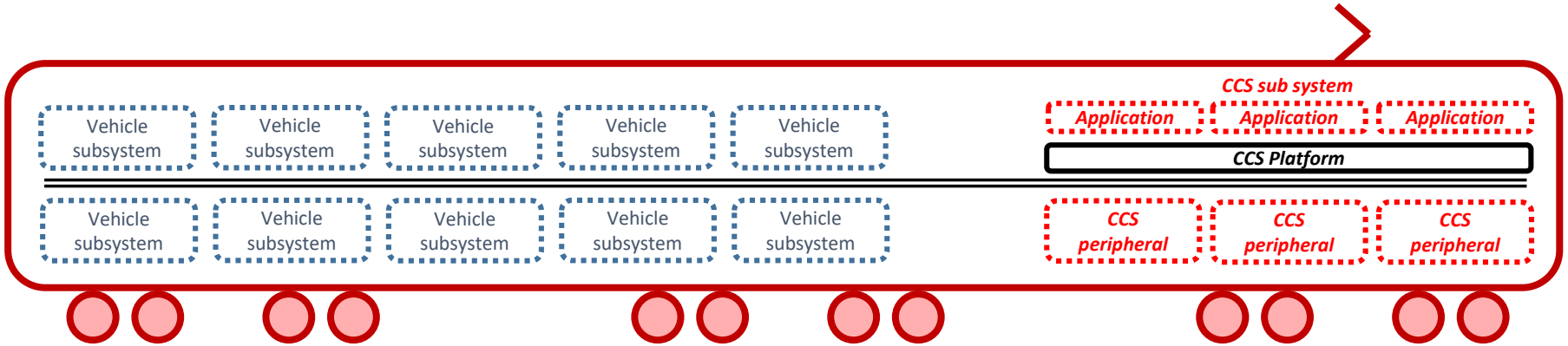



Urgent project proposal  **Next project proposals**  Integrated, proprietary subsystem or constituent  Open, universal subsystem or constituent – MVP

**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 universal bus. This open CCS environement is isolated from the fully integrated proprietary vehicle environment




**Level of Modularity *n*** (long term perspective): the CCS universal bus 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

# OCORA - UVCC Bus

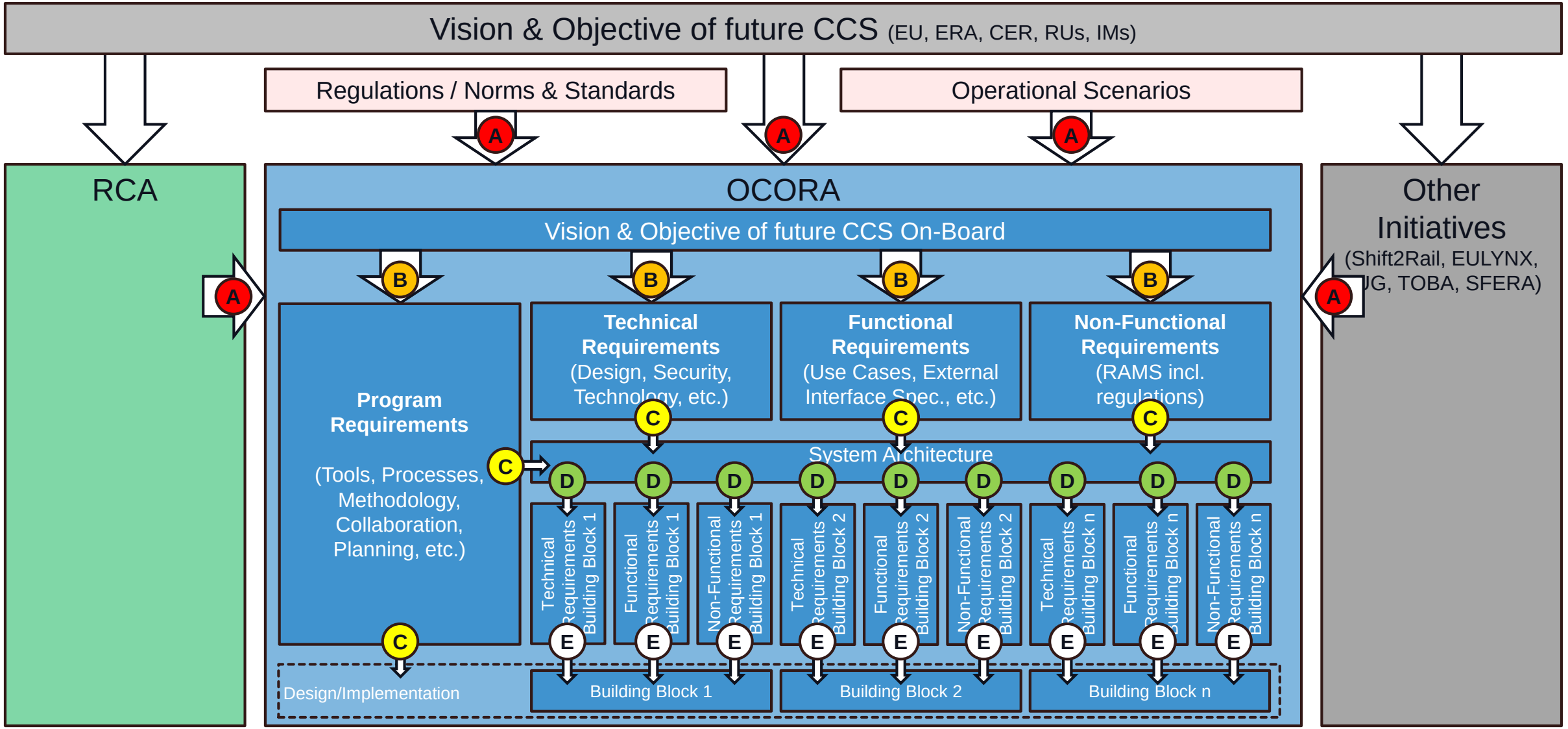
| OSI Layer | | Protocol | |
|---|---|---|---|
| | | *Protocol for hard-real-time data* | *Protocol for soft- or non-real-time data* |
| | (Safety*) | **(SDTv2 / SDTv4)** | |
| 5 | Session | TRDP - OPC-UA Pub/Sub - DDS-RTPS | |
| 4 | Transport | UDP (for process and message data)<br>TCP (for message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

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

Details im Dokument: OCORA-40-003-Beta UVCC Bus Evaluation

# Requirements Engineering

## Structuring the Requirements



# OCORA Set of Requirements

## Problem Statement

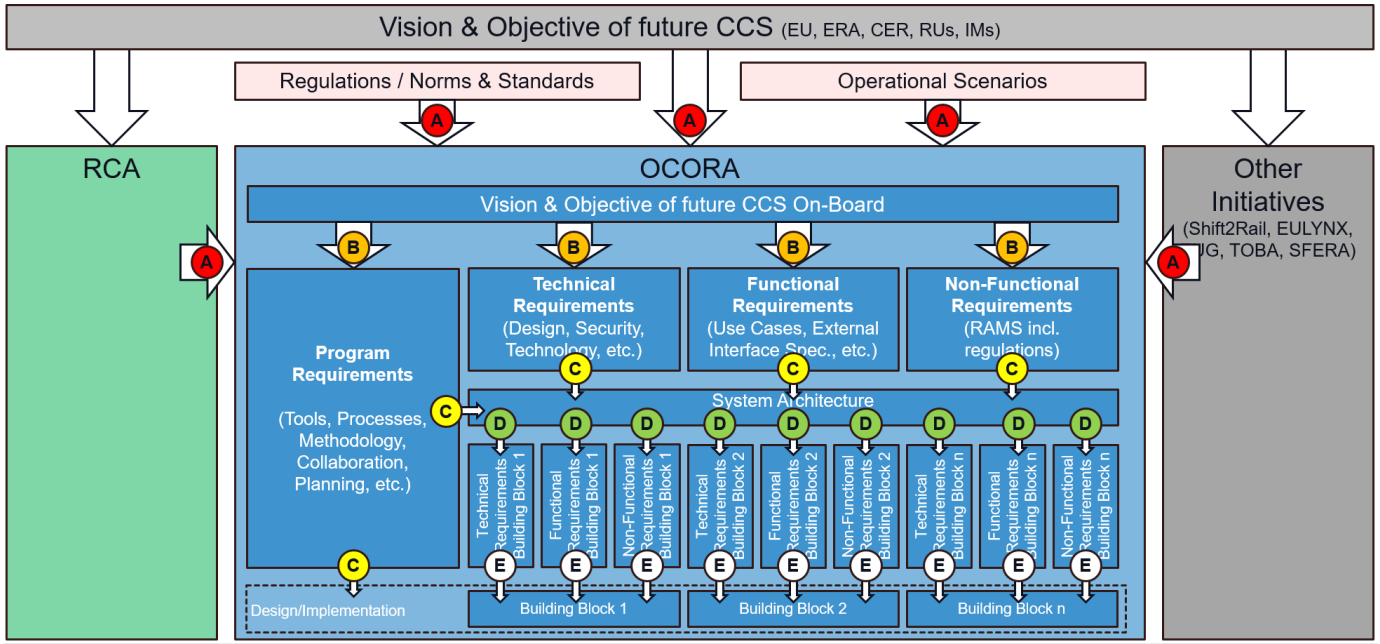
**A** OCORA has to manage many different requirements, coming from many different stakeholders.

**B** I addition, the OCORA initiative has defined its own vision and objectives that lead to requirements for the initiative and the on-board system to be developed.

**C** Further more, program, technical, functional, and non-functional requirements are developed in the different OCORA workstreams.

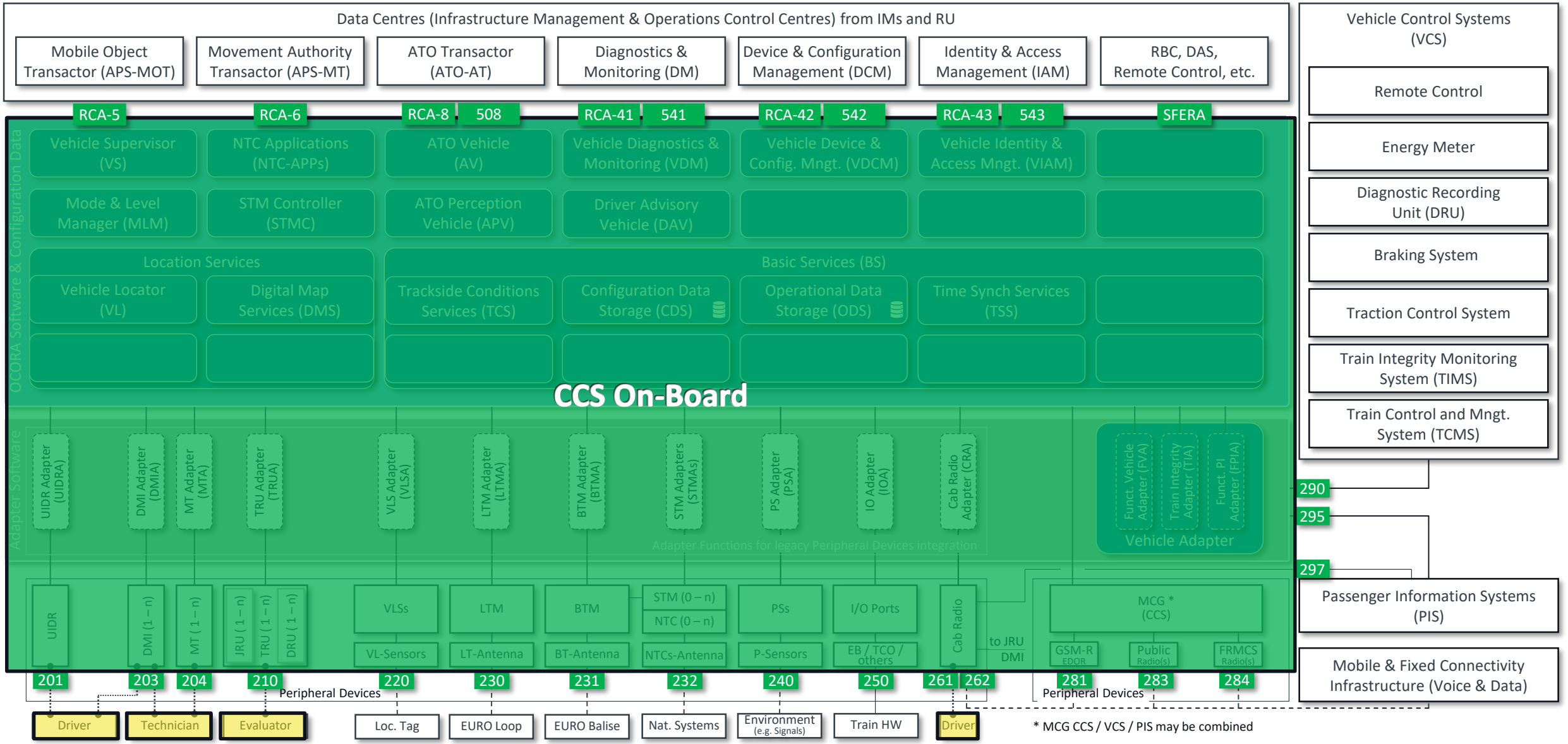
**D** While building the system's architecture, the different requirements need to be apportioned to the identified subsystems.

**E** These apportioned requirements, together with the specifications of the system architecture define the requirements applicable for the different subsystems and can be used as tender templates.

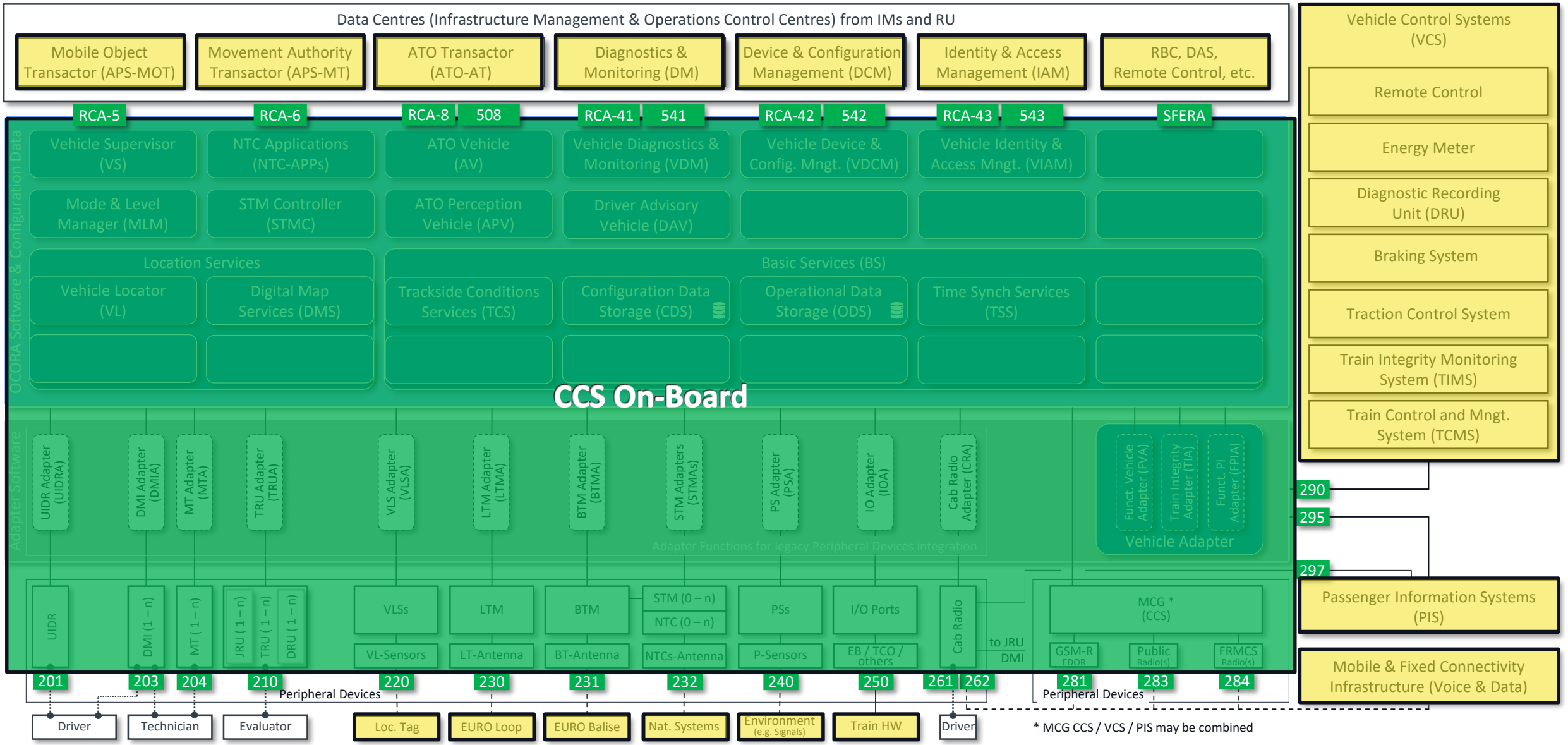



Requirements engineering is an important and difficult task, requiring dedicated resources and therefore a separate workstream.

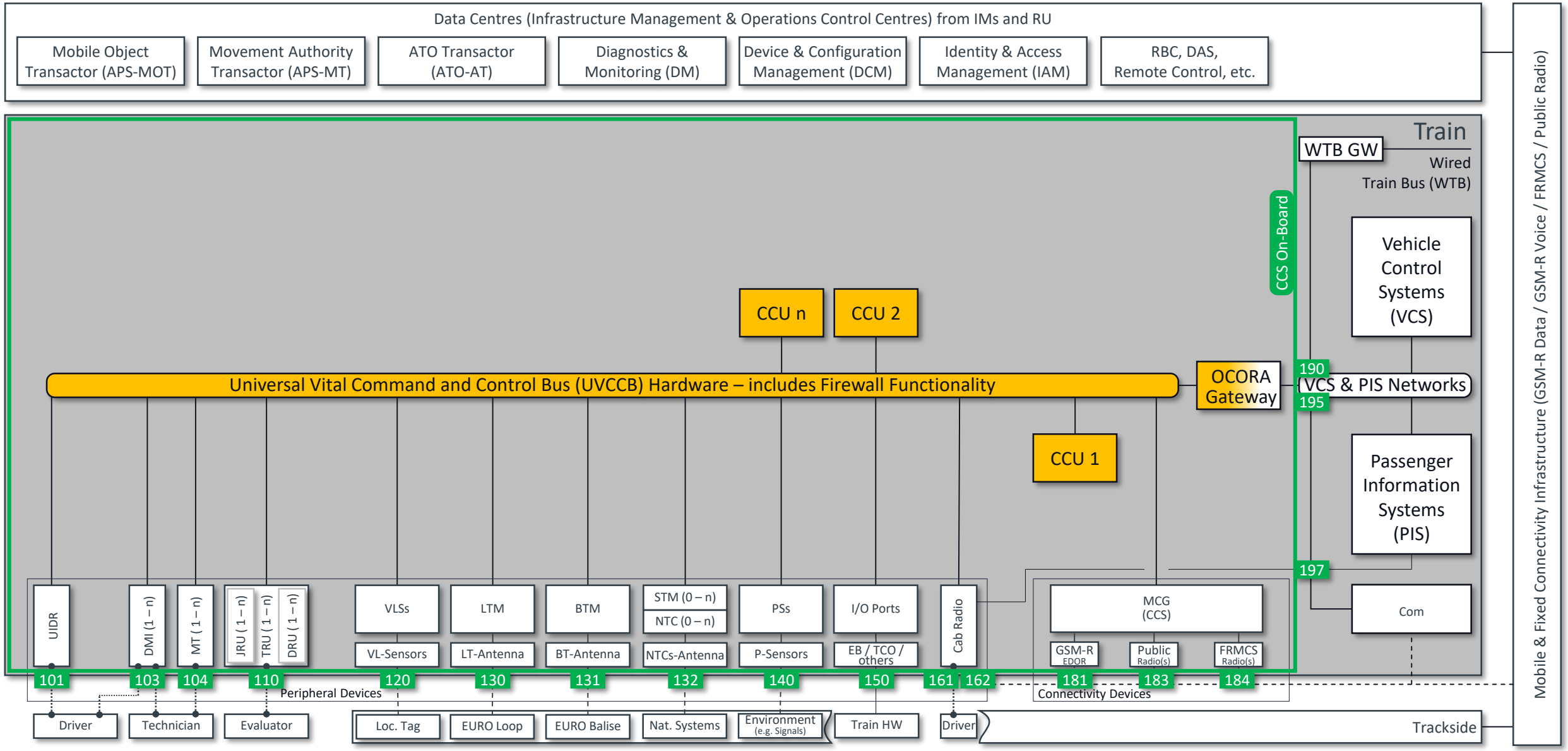
# Actors


Data Centres (Infrastructure Management & Operations Control Centres) from IMs and RU
Mobile Object Transactor (APS-MOT)
Movement Authority Transactor (APS-MT)
ATO Transactor (ATO-AT)
Diagnostics & Monitoring (DM)
Device & Configuration Management (DCM)
Identity & Access Management (IAM)
RBC, DAS, Remote Control, etc.
Vehicle Control Systems (VCS)
Remote Control
Energy Meter
Diagnostic Recording Unit (DRU)
Braking System
Traction Control System
Train Integrity Monitoring System (TIMS)
Train Control and Mngt. System (TCMS)
RCA-5
RCA-6
RCA-8
508
RCA-41
541
RCA-42
542
RCA-43
543
SFERA
OCORA Software & Configuration Data
Vehicle Supervisor (VS)
NTC Applications (NTC-APPs)
ATO Vehicle (AV)
Vehicle Diagnostics & Monitoring (VDM)
Vehicle Device & Config. Mngt. (VDCM)
Vehicle Identity & Access Mngt. (VIAM)
Mode & Level Manager (MLM)
STM Controller (STMC)
ATO Perception Vehicle (APV)
Driver Advisory Vehicle (DAV)
Location Services
Vehicle Locator (VL)
Digital Map Services (DMS)
Basic Services (BS)
Trackside Conditions Services (TCS)
Configuration Data Storage (CDS)
Operational Data Storage (ODS)
Time Synch Services (TSS)
CCS On-Board
Adapter Software
UIDR Adapter (UIDRA)
DMI Adapter (DMIA)
MT Adapter (MTA)
TRU Adapter (TRUA)
VLS Adapter (VLSA)
LTM Adapter (LTMA)
BTM Adapter (BTMA)
STM Adapters (STMAs)
PS Adapter (PSA)
IO Adapter (IOA)
Cab Radio Adapter (CRA)
Funct. Vehicle Adapter (FVA)
Train Integrity Adapter (TIA)
Funct. PI Adapter (FPIA)
Vehicle Adapter
Adapter Functions for legacy Peripheral Devices integration
290
295
297
Passenger Information Systems (PIS)
Mobile & Fixed Connectivity Infrastructure (Voice & Data)
UIDR
DMI (1 – n)
MT (1 – n)
JRU (1 – n)
TRU (1 – n)
DRU (1 – n)
VLSs
LTM
BTM
STM (0 – n)
NTC (0 – n)
PSs
I/O Ports
Cab Radio
to JRU
DMI
MCG * (CCS)
GSM-R EDOR
Public Radio(s)
FRMCS Radio(s)
VL-Sensors
LT-Antenna
BT-Antenna
NTCs-Antenna
P-Sensors
EB / TCO / others
201
203
204
210
Peripheral Devices
220
230
231
232
240
250
261
262
281
283
284
Peripheral Devices
Driver
Technician
Evaluator
Loc. Tag
EURO Loop
EURO Balise
Nat. Systems
Environment (e.g. Signals)
Train HW
Driver
* MCG CCS / VCS / PIS may be combined

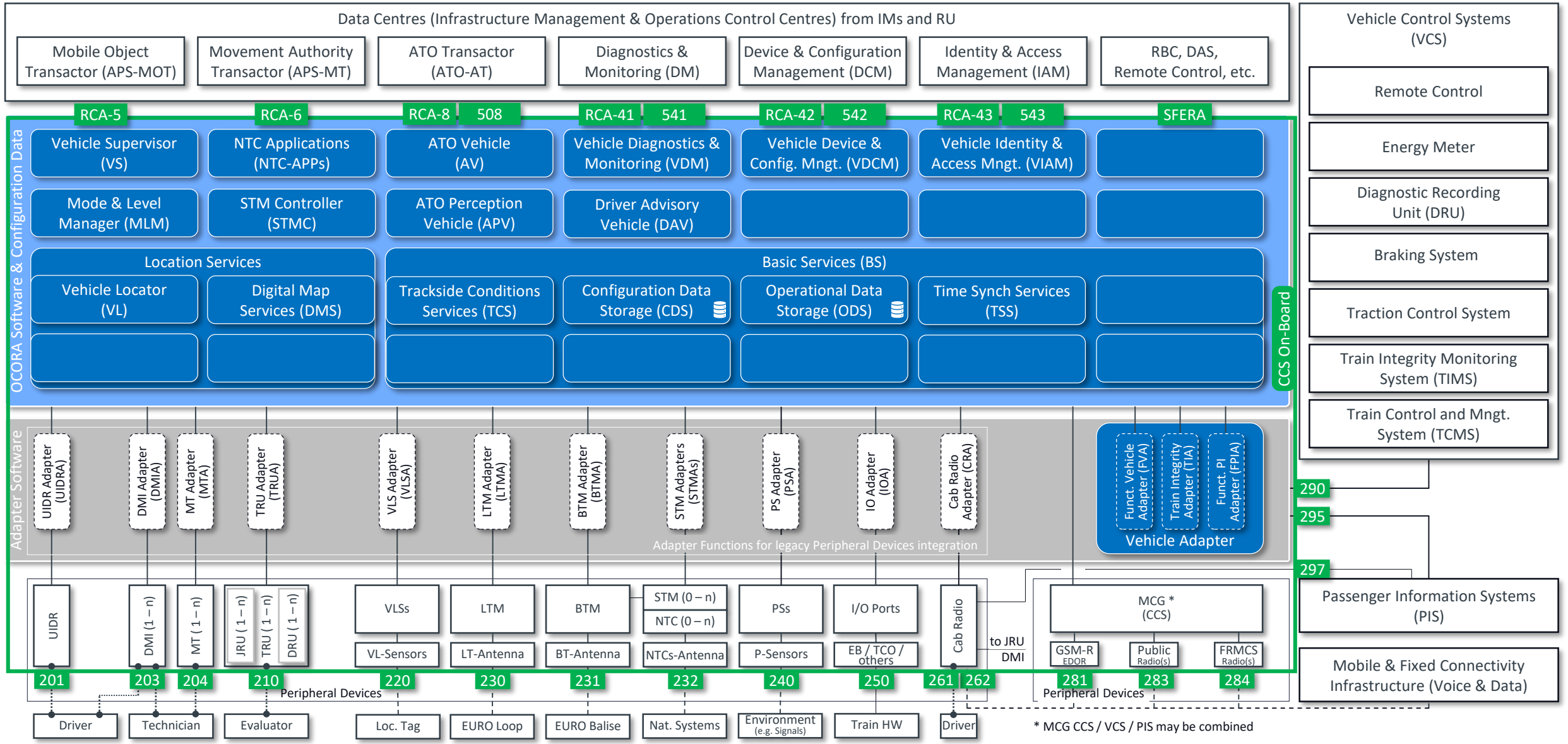
# External Systems



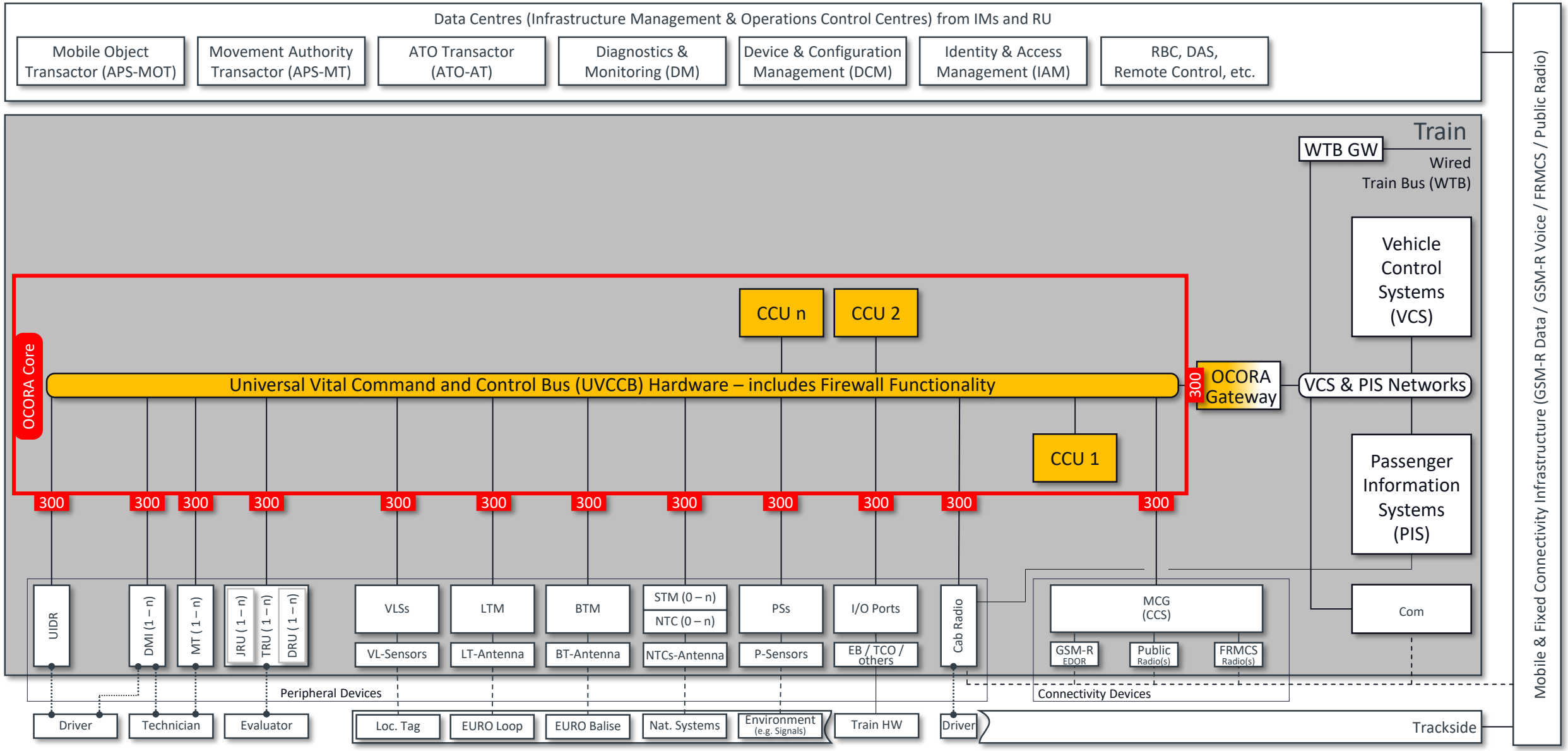
# Hardware Interfaces – CCS On-Board



# Functional Interfaces – CCS On-Board



# Hardware Interfaces – OCORA Core



# Functional Interfaces – OCORA Core