EEIG ERTMS Users Group
123-133 Rue Froissart, 1040 Brussels, Belgium
Tel: +32 (0)2 673.99.33 - TVA BE0455.935.830

LOCALISATION WORKING GROUP (LWG)

LOC-OB Risk Analysis

Ref:	22E135
Version:	1.0
Date:	17/06/2022

Modification history

Version	Date	Modification / Description	Editor
0a	31.01.2022	Initial draft suggestion of outline revised in two working sessions	SNCF(MPD/SEF)
0b	23.02.2022	Agreement on the ToC	SNCF(MPD/SEF)
0c	09.03.2022	List of feared events issued from subset 91/88 (section 7.3)	SNCF(MPD/SEF)
0d	18.05.2022	1st draft	SNCF(MPD)
0e	10.06.2022	Draft version for internal LWG review	SNCF(MPD) EUG (DC/GR)
1.0	17.06.2022	Final release	SNCF(MPD) EUG (DC/GR)

Table of Contents

1 List of References and Acronyms

References

[R1]	22E126	LOC-OB System Definition & Operational Context, v1.0, 30/05/2022
[R2]	19E100	Localisation Performance Requirements - Vehicle Locator - v3, 10/12/2019
[R3]	OCORA-TWS01-030	OCORA - System Architecture, v2.01, 03.12.2021
[R4]	OCORA-TWS01-100	OCORA - Localisation-On-Board-(LOC-OB)_Introduction, v1.01, 03.12.2021
[R5]	EN 50126-1:2017	Railway Applications - The Specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 1: generic RAMS process
[R6]	EN 50126-2:2017	Railway Applications - The specification and demonstration of reliability, availability, maintainability and safety (RAMS) - Part 2: systems approach to safety
[R7]	CSM-RA	Commission Implementing Regulation (EU) 2015/1136 on the Common Safety Method for Risk Evaluation and Assessment.
[R8]	ERA/GUI/01-2008/SAF	Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)'a) of the Railway Safety Directive reference
[R9]	ERA-REC-116-2015-GUI	Guideline for the application of the CSM design targets reference
[R10]	SUBSET-023 v3.3.0	ERTMS/ETCS - Glossary of Terms and Abbreviations
[R11]	SUBSET-026 v3.6.0	ERTMS/ETCS - System Requirements Specification
[R12]	SUBSET-088 v3.7.0	ETCS Application Levels 1 & 2 - Safety Analysis
[R13]	SUBSET-091 v3.6.0	Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2
[R14]	SUBSET-035 v3.2.0	ERTMS/ETCS Specific Transmission Module FFFIS, 3.2.0, 16.12.2015
[R15]	RCA.Doc.14	RCA Terms and Abstract Concepts, v0.4, 26.04.2022, BL0 R4
[R16]	RCA.Doc.59	RCA Digital Map System Definition, v0.5, 22.04.2022, BL0 R4
[R17]	RCA.Doc.69	RCA Map Object Catalogue, v0.2, 16.03.2022, BL0 R4

Acronyms

ATO	Automatic Train Operation
APS OA	Advanced Protection System Object Aggregator
CCS	Command Control & Signalling
CMD	Cold Movement Detection
DM-OB	Digital Map On-Board
DM-TS	Digital Map TrackSide
EGNOS	European Geostationary Navigation Overlay Service
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EU	European Union
EUG	ERTMS Users Group
FMEA	Failure Mode and Effect Analysis
FRMCS	Future Railway Mobile Communication System
FTA	Fault Tree Analysis
LGPR	Localizing Ground Penetrating Radar
LiDAR	Laser imaging, Detection and Ranging
LOC-OB	Localisation On-Board
LWG	Localisation Working Group
MCI	Maximum Confidence Interval for operations
OCORA	Open CCS On-board Reference Architecture
PHA	Preliminary Hazard Analysis
RA	Risk Analysis
RCA	Reference CCS Architecture
RFID	Radio Frequency Identification
SCI	Standard Communication Interface
SRAC	Safety Related Application Conditions
SSD	Stand Still Detection
TIMS	Train Integrity Monitoring System
TTFR	Tolerable Functional Failure Rate

THR	Tolerable Hazard Rate
VL	Vehicle Locator
VLS	Vehicle Locator Sensors
WLAN	Wireless Local Area Network

2 Glossary and Definitions

2.1.1.1 Terms not explicitly mentioned in this chapter but used in this document can be found in the RCA Glossary [R15].

2.1.1.2 Reference point. Estimated distances are given in relation to this point that is known by the on-board (although not necessarily geographically) and trackside. Also referred to as “Reference Location” or “Location Reference” in subset 23 [R10].

3 Scope of the Document

3.1.1.1 The objective of this document is to provide a Risk Analysis of the LOC-OB system, to provide safety requirements to railway undertakings (RUs) in terms of preparing OCORA/RCA compliant tenders, and to prepare for Europe’s Rail Joint Undertakings System & Innovation Pillar

3.1.1.2 LOC-OB shall be considered for the Europe’s Rail Joint Undertaking (ERJU) Innovation Pillar flagship areas that cover “absolute safe train positioning, highly accurate and safe, incorporating new sensory”.

3.1.1.3 This document is further seen as an input for several further EUG LWG activities/deliverables that will ultimately lead to revised ERTMS/ETCS specifications (TSI) in order to enable new enhanced localisation principles covering a more holistic localisation system.

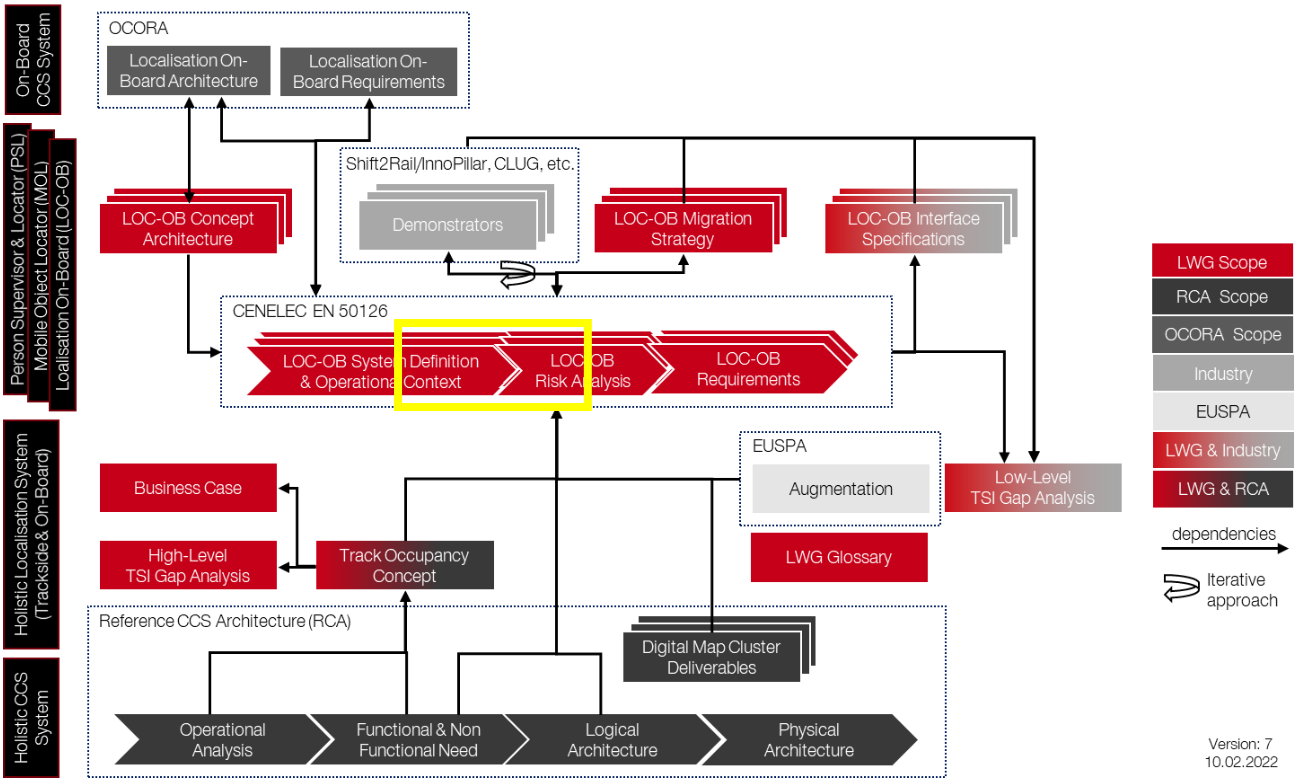

On-Board CCS System
Person Supervisor & Locator (PSL)
Mobile Object Locator (MOL)
Localisation On-Board (LOC-OB)
Holistic Localisation System (Trackside & On-Board)
Holistic CCS System
OCORA
Localisation On-Board Architecture
Localisation On-Board Requirements
Shift2Rail/InnoPillar, CLUG, etc.
Demonstrators
LOC-OB Concept Architecture
LOC-OB Migration Strategy
LOC-OB Interface Specifications
CENELEC EN 50126
LOC-OB System Definition & Operational Context
LOC-OB Risk Analysis
LOC-OB Requirements
EUSPA
Augmentation
Low-Level TSI Gap Analysis
Business Case
High-Level TSI Gap Analysis
Track Occupancy Concept
LWG Glossary
Reference CCS Architecture (RCA)
Digital Map Cluster Deliverables
Operational Analysis
Functional & Non Functional Need
Logical Architecture
Physical Architecture
LWG Scope
RCA Scope
OCORA Scope
Industry
EUSPA
LWG & Industry
LWG & RCA
dependencies
Iterative approach
Version: 7
10.02.2022

Figure 1: LWG Documentation Structure - LOC-OB Risk Analysis – yellow rectangle in the centre.

3.1.1.4 This document follows the structure/topics that are to be covered in phase 3 of risk analysis and evaluation according to CENELEC EN50126 [R5] but only for the early steps of the risk assessment process.

3.1.1.5 It should be clarified that this document does not report a trusted analysis. The aim of this analysis is not to get an approval from safety organisation nor assessment from an authorised body, the analysis is performed outside project safety organisation by the EUG-LWG team.

3.1.1.6 At the early stage of the LOC-OB system definition, this document gives a first approach to identify potential hazards and events that may lead to an accident and to carry out the risk assessment of these hazards. This allows to define barrier/ mitigation measures to reduce identified risks and to derive THR/TFFR apportionments.

3.1.1.7 It should be shared that the system context used to carry out the analysis is based on the existing ERTMS/ETCS for level 2 where the concepts of independent onboard vehicle localisation component, virtual balise and digital map are added.

3.1.1.8 Accordingly, the following references will be considered as applicable within the context of the LOC-OB safety analysis:

- Glossary of Terms and Abbreviations (UNISIG Subset 023 [R10])
- System Requirements Specifications (UNISIG Subset 026 [R11]
- Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 (UNISIG Subset 091 [R13])

- ETCS Application Level 2 - Safety Analysis (Parts 1 & 2) (UNISIG Subset 088 [R12])

3.1.1.9 The analysis should be extended for level 3 of ERTMS/ETCS, when inputs from the OCORA project or RCA/EUG groups are available.

3.1.1.10 The LOC-OB system under analysis in this document is based on the component of the OCORA architecture (see [R3] and [R4]) and the System Definition and Operational Context delivered by the EUG-LWG group (see [R1]).

3.1.1.11 As the sub systems VL and VLS of LOC-OB system are viewed as black-box equipment, the internal functions and interfaces of VL and VLS are not defined.

3.1.1.12 The analysis will be limited to the outputs, inputs and when possible extended to some operational contexts of the LOC-OB system.

3.1.1.13 This document will:

a) give the risk analysis objectives,
b) define the risk analysis methodology,
c) describe the system under analysis, its external functions and its mission profile,
d) provide hazard and risk assessment,
e) identify the safety requirements,
f) allocate safety target to the functions,
g) list the assumptions made during the analysis.

4 Risk analysis objectives

4.1.1.1 The preliminary phase of the system definition and system requirements defines the limits of the system and its main components. This first phase is a prerequisite before carrying out a risk assessment for identifying system behaviour leading to unsafe events, to danger.

4.1.1.2 For railway operations, safety is of the most importance and must be carefully monitored and assessed all along the life cycle of system and products from the engineering phases to the operation and maintenance activities until the system, the products are removed from operation.

4.1.1.3 At EU level, the legislation sets the framework for harmonized approach to rail safety across the EU. It lays down the conditions for granting the safety certifications that every railway company must obtain before it can run trains on the European network.

4.1.1.4 Among harmonized safety regulations, the Common Safety Methods (CSMs) [R7] describe how the safety levels, the achievement of safety targets and compliance with other safety requirements should be fulfilled.

4.1.1.5 The CSMs are directly applicable and enforceable in the Member States. Depending on their scope, they are applied either by authorities or bodies, or by specific actors of the railway system (e.g. railway undertakings, infrastructure managers, entities in charge of maintenance), or even by both.

4.1.1.6 The risk analysis is performed in accordance with the CSMs and follows the guide for the application of the Common Safety Methods on Risk Evaluation and Assessment (CSM-RA) [R8] and [R9]. For details see link https://www.era.europa.eu/activities/common-safety-methods_en. The CSMs support CENELEC 5012x series of standards or IEC 61508 standard to demonstrate the achievement of quantified design targets and to cope with systematic failures which cannot be quantified.

4.1.1.7 According to CSM-RA, the Risk Analysis takes place only in case of “significant change”. In the case of the LOC-OB the following significant changes are identified:

- The architecture OCORA is new and different of what is previously done by the industrials, with identification of independent components.
- Due to this new architecture the localisation function is now redefined independently of the whole ERTMS functions.
- LOC-OB input interfaces have been deeply redefined with use of new kind of sensors to replace odometer systems.

4.1.1.8 LOC-OB is a subsystem of the OCORA system, and it contributes also to the overall performance of the system ERTMS/ETCS. Thus, in this first stage of LOC-OB deployment, the risk analysis is performed within the context of the ERTMS/ETCS system. Thus, the analysis is based on the hazards of the ERTMS/ETCS system identified in Subset 91[R13].

4.1.1.9 The risk analysis main goals shall contribute to identify:

- hazards where the LOC-OB system is involved,
- safety requirements on functions and external interfaces,
- barrier and mitigation measures for reducing hazard to an acceptable risk.

5 Risk Analysis methodology

5.1.1.1 The risk analysis is the first step in the system safety process to identify and categorize hazards associated with the operation of the system.

5.1.1.2 The method used to carry out the risk analysis follows the principles applicable to the risk management process defined in the CSMs and depicted in the Figure 1 (see Guide for the application of the Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of the Railway Safety Directive [R7] and [R8]).

5.1.1.3 The main phases of the risk and risk analysis can be defined as follows:

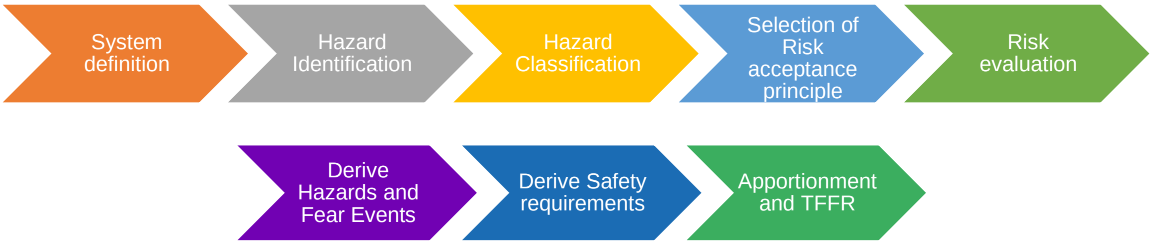


Figure 2: Risk analysis methodology

5.1.1.4 The apportionment of risks and the safety requirements of functions are derived from the results of the risks analysis. The safety requirements are the results of the Failure Mode and Effect Analysis and the Fault Tree Analysis.

6 System under analysis

6.1 System objectives

6.1.1.1 The Localisation On-Board (LOC-OB) system is a safe CCS On-Board building block component composed of a set of sensors (VLS) and a Vehicle Locator (VL) equipment that uses sensor data and supporting information to provide train location output information safely and reliably. The LOC-OB shall provide the absolute and relative position of the front-end of the train, train orientation information as well as kinematic parameters such as speed, acceleration, or rotational angles.

6.1.1.2 The LOC-OB shall provide localisation information such as 1D position relative to a reference point, orientation, speed and acceleration of the train which complies with the current ERTMS/ETCS principle (distance and orientation from a LRBG and a speed) and can also provide additional localisation information such as:

a) The absolute (3D) geographic positioning (Long, Lat, Alt),
b) The vector velocity within the 3D coordinate system based on the track axis,
c) The vector acceleration within the 3D coordinate system based on the track axis,
d) The attitude (roll, pitch, and yaw angles)

Refer to chapter 6.6 for the various System Functions.

6.1.1.3 This localisation information is computed by the LOC-OB based on data provided by sensors and supporting information (e.g., digital map, augmentation data, routing information) upon availability.

6.1.1.4 A detailed description of the LOC-OB system is given in the LOC-OB System Definition & Operational Context Report [R1].

6.2 Operational Context

6.2.1.1 In today’s ETCS implementations, the LOC-OB functionality is part of the monolithic ETCS On-Board Unit.

6.2.1.2 Since innovation cycles for the LOC-OB are expected to occur more frequently than for the remaining part of the ETCS On-Board Unit (e.g., Automatic Train Protection - On-Board (ATP-OB)), it is essential that the LOC-OB is a separate component, containing just the functionality needed to locate safely and reliably the vehicle and its orientation on the track and determining associated kinematic parameters of the vehicle.

6.2.1.3 With a separation of the LOC-OB functionality, guiding principles such as modularity and single-responsibility are fulfilled leading to reduced complexity in terms of testing and certification of conformity.

6.2.1.4 Standardising the external interfaces of LOC-OB allows to leverage new localisation technologies in the future without the need to modify the remaining part of the ETCS On-Board functionality.

6.2.1.5 Thus, with standardised LOC-OB interfaces in place (e.g., that cover performance, technical interface conformity and the allocated tolerable hazard rate), updates to the internal LOC-OB logic such as

a) adding new types or generations of sensors (e.g., from a simple GPS to a multi-frequency multi-constellation GNSS receiver)

b) improving fusion algorithms output quality (e.g., higher accuracy)

c) considering additional standardised data sources in the fusion algorithms (e.g, train routing information, augmentation information delivered through terrestrial dissemination)

6.2.1.6 will not trigger a re-certification (homologation) of the entire ETCS On-Board Unit if the standardised interfaces are not impacted by the change.

6.2.1.7 Sharing localisation information not only with ATP-OB (logical component of CCS-OB) but also with other on-board actors through a standardised interface is a key requirement.

6.2.1.8 Besides, new functionalities (game changers) with potential impact on the LOC-OB are:

- FRMCS
- ATO
- Train integrity detection and safe train length determination for ETCS L3
- GNSS augmentation
- Digital map

6.2.1.9 The goal of the LOC-OB is to provide localisation information not only to the VS (core ETCS) and the AV (ATO Vehicle), but also to other (future) actors which require different types of localisation information.

6.2.1.10 LOC-OB is deployed on every OCORA based CCS as a mandatory equipment.

6.2.1.11 In the first stage the risk analysis will be limited in the context of an ERTMS/ETCS system using the LOC-OB system. This will be the basis to identify at the system level the hazards and the feared events.

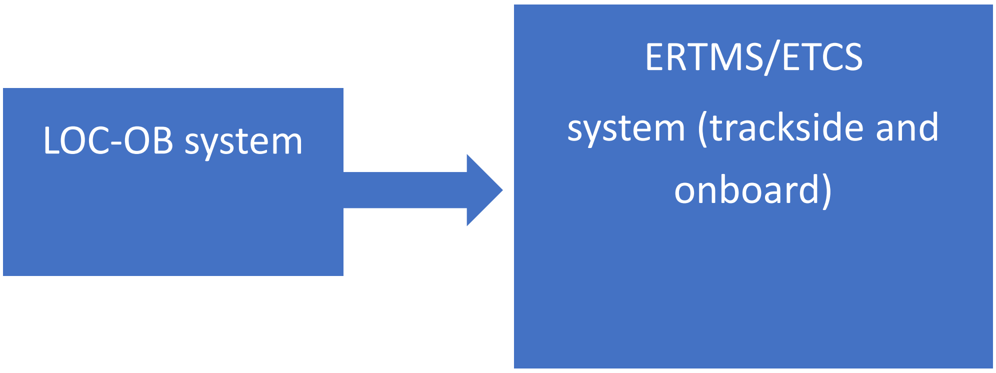


Figure 3: Input from the LOC-OB to the ETCS system

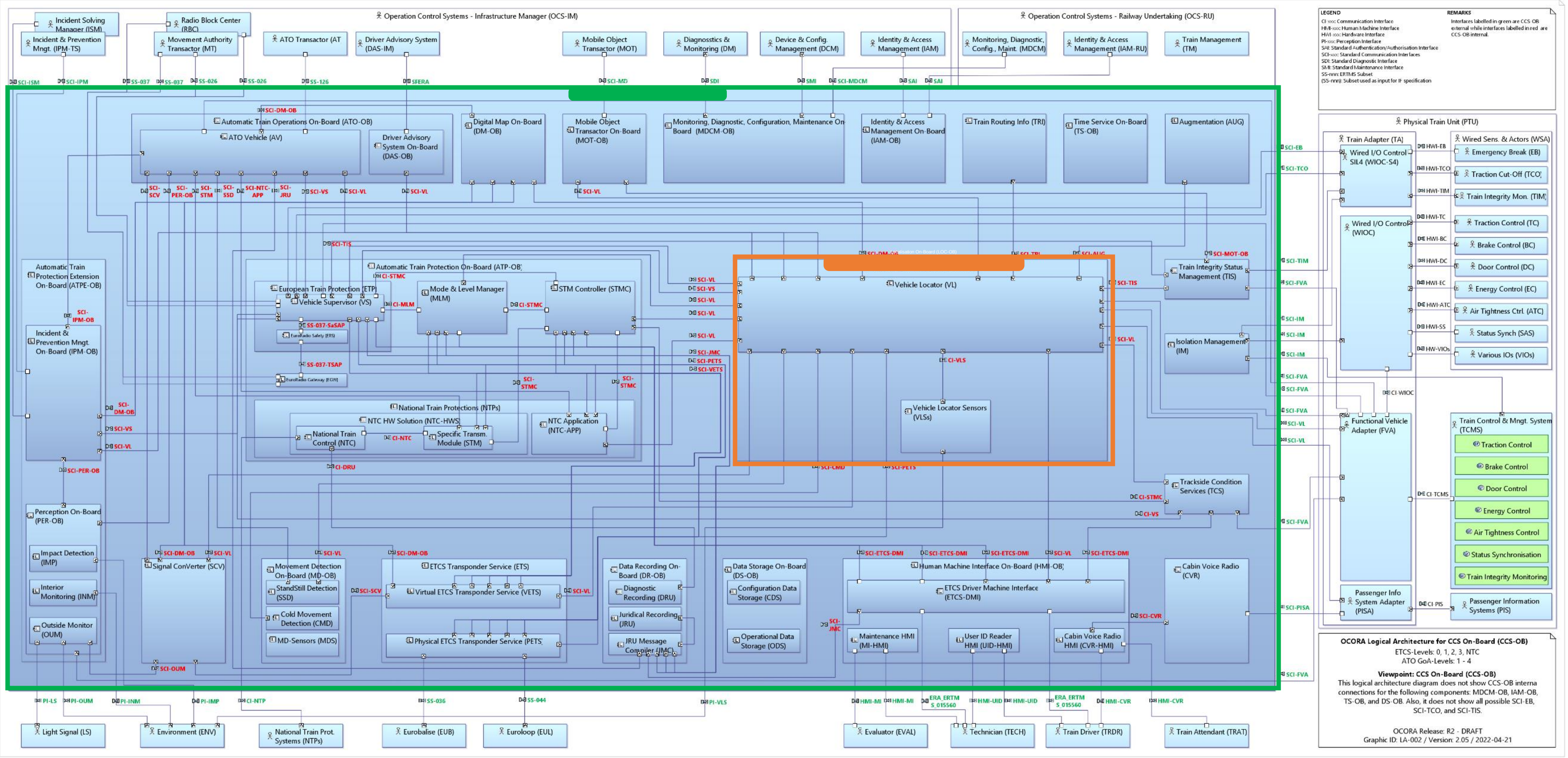
6.3 System Architecture

6.3.1 LOC-OB in the Context of the CCS on-board Architecture

6.3.1.1 The LOC-OB system is a safe CCS On-Board building block component composed of a set of sensors (VLS) and a Vehicle Locator (VL) equipment that uses sensor data and supporting information to provide train location output information safely and reliably.

6.3.1.2 A detailed description of the LOC-OB system is given in the LOC-OB System Definition & Operational Context Report [R1].

6.3.1.3 OCORA defines the reference architecture for the on-board [R3]. This reference architecture is depicted in Figure 4.


Operation Control Systems - Infrastructure Manager (OCS-IM)
Incident Solving Manager (ISM)
Incident & Prevention Mngt. (IPM-TS)
Radio Block Center (RBC)
Movement Authority Transactor (MT)
ATO Transactor (AT
Driver Advisory System (DAS-IM)
Mobile Object Transactor (MOT)
Diagnosstics & Monitoring (DM)
Device & Config. Management (DCM)
Identity & Access Management (IAM)
Operation Control Systems - Railway Undertaking (OCS-RU)
Monitoring, Diagnostic, Config., Maint. (MDCM)
Identity & Access Management (IAM-RU)
Train Management (TM)
SCI-ISM
SCI-IPM
SS-037
SS-037
SS-026
SS-026
SS-126
SFERA
SCI-MD
SDI
SMI
SCI-MDCM
SAI
SAI
SCI-DM-OB
Automatic Train Operations On-Board (ATO-OB)
ATO Vehicle (AV)
Driver Advisory System On-Board (DAS-OB)
Digital Map On-Board (DM-OB)
Mobile Object Transactor On-Board (MOT-OB)
Monitoring, Diagnostic, Configuration, Maintenance On-Board (MDCM-OB)
Identity & Access Management On-Board (IAM-OB)
Train Routing Info (TRI)
Time Service On-Board (TS-OB)
Augmentation (AUG)
SCI-SCV
SCI-PER-OB
SCI-STM
SCI-SSD
SCI-NTC-APP
SCI-JRU
SCI-VS
SCI-VL
SCI-VL
SCI-VL
SCI-TIS
Automatic Train Protection Extension On-Board (ATPE-OB)
SCI-IPM-OB
Incident & Prevention Mngt. On-Board (IPM-OB)
SCI-DM-OB
SCI-VS
SCI-VL
SCI-PER-OB
Automatic Train Protection On-Board (ATP-OB)
CI-STMC
European Train Protection (ETP)
Vehicle Supervisor (VS)
CI-MLM
Mode & Level Manager (MLM)
CI-STMC
STM Controller (STMC)
SS-037-SaSAP
EuroRadio Safety (ERS)
SS-037-TSAP
EuroRadio Gateway (EGW)
SCI-STMC
SCI-STMC
National Train Protections (NTPs)
NTC HW Solution (NTC-HWS)
National Train Control (NTC)
CI-NTC
Specific Transm. Module (STM)
NTC Application (NTC-APP)
CI-DRU
SCI-VL
SCI-VS
SCI-VL
SCI-VL
SCI-VL
SCI-JMC
SCI-PETS
SCI-VETS
Localisation On-Board (LOC-OB)
SCI-DM-OB
SCI-TRI
SCI-AUG
Vehicle Locator (VL)
CI-VLS
Vehicle Locator Sensors (VLSs)
SCI-TIS
SCI-VL
SCI-CMD
SCI-PETS
SCI-MOT-OB
Train Integrity Status Management (TIS)
Isolation Management (IM)
Trackside Condition Services (TCS)
CI-STMC
CI-VS
Perception On-Board (PER-OB)
Impact Detection (IMP)
Interior Monitoring (INM)
Outside Monitor (OUM)
SCI-DM-OB
SCI-VL
Signal ConVerter (SCV)
SCI-OUM
SCI-VL
Movement Detection On-Board (MD-OB)
StandStill Detection (SSD)
Cold Movement Detection (CMD)
MD-Sensors (MDS)
SCI-SCV
SCI-DM-OB
ETCS Transponder Service (ETS)
Virtual ETCS Transponder Service (VETS)
Physical ETCS Transponder Service (PETS)
SCI-VL
Data Recording On-Board (DR-OB)
Diagnostic Recording (DRU)
Juridical Recording (JRU)
JRU Message Compiler (JMC)
Data Storage On-Board (DS-OB)
Configuration Data Storage (CDS)
Operational Data Storage (ODS)
SCI-JMC
SCI-ETCS-DMI
SCI-ETCS-DMI
SCI-ETCS-DMI
SCI-VL
SCI-ETCS-DMI
Human Machine Interface On-Board (HMI-OB)
ETCS Driver Machine Interface (ETCS-DMI)
Maintenance HMI (MI-HMI)
User ID Reader HMI (UID-HMI)
Cabin Voice Radio HMI (CVR-HMI)
SCI-CVR
Cabin Voice Radio (CVR)
PI-LS
PI-OUM
PI-INM
PI-IMP
CI-NTP
SS-036
SS-044
PI-VLS
HMI-MI
HMI-MI
ERA_ERTM S_015560
HMI-UID
HMI-UID
ERA_ERTM S_015560
HMI-CVR
HMI-CVR
Light Signal (LS)
Environment (ENV)
National Train Prot. Systems (NTPs)
Eurobalise (EUB)
Euroloop (EUL)
Evaluator (EVAL)
Technician (TECH)
Train Driver (TRDR)
Train Attendant (TRAT)
SCI-EB
SCI-TCO
SCI-TIM
SCI-FVA
SCI-IM
SCI-IM
SCI-IM
SCI-FVA
SCI-FVA
SCI-FVA
SCI-VL
SCI-VL
SCI-FVA
SCI-PISA
SCI-FVA
Physical Train Unit (PTU)
Train Adapter (TA)
Wired I/O Control SIL4 (WIOC-S4)
Wired I/O Control (WIOC)
Wired Sens. & Actors (WSA)
HWI-EB
Emergency Break (EB)
HWI-TCO
Traction Cut-Off (TCO)
HWI-TIM
Train Integrity Mon. (TIM)
HWI-TC
Traction Control (TC)
HWI-BC
Brake Control (BC)
HWI-DC
Door Control (DC)
HWI-EC
Energy Control (EC)
HWI-ATC
Air Tightness Ctrl. (ATC)
HWI-SS
Status Synch (SAS)
HW-VIOs
Various IOs (VIOs)
CI-WIOC
Functional Vehicle Adapter (FVA)
CI-TCMS
Train Control & Mngt. System (TCMS)
Traction Control
Brake Control
Door Control
Energy Control
Air Tightness Control
Status Synchronisation
Train Integrity Monitoring
Passenger Info System Adapter (PISA)
CI-PIS
Passenger Information Systems (PIS)

LEGEND

CI-xxx: Communication Interface
HMI-xxx: Human Machine Interface
HWI-xxx: Hardware Interface
PI-xxx: Perception Interface
SAI: Standard Authentication/Authorisation Interface
SCI-xxx: Standard Communication Interfaces
SDI: Standard Diagnostic Interface
SMI: Standard Maintenance Interface
SS-nnn: ERTMS Subset
(SS-nnn): Subset used as input for IF specification

REMARKS

Interfaces labelled in green are CCS-OB external while interfaces labelled in red are CCS-OB internal.

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 diagram does not show CCS-OB interna connections for the following components: MDCM-OB, IAM-OB, TS-OB, and DS-OB. Also, it does not show all possible SCI-EB, SCI-TCO, and SCI-TIS.

OCORA Release: R2 - DRAFT
Graphic ID: LA-002 / Version: 2.05 / 2022-04-21

Figure 4: OCORA Logical Architecture for CCS On-Board (CCS-OB) – green border. Localisation On-Board (LOC-OB) – orange border

6.3.2 Vehicle Locator (VL)

6.3.2.1 The VL is a safe CCS On-Board component that uses sensor data and supporting information to provide train location output information safely and reliably. The VL is able to provide the absolute and relative position in reference to of the front-end of the train, train orientation information as well as kinematic parameters such as speed, acceleration, or rotational angles; hence, the VL is more than just an odometry component. The VL is the functional block whose main responsibility is to determine and provide the localisation information of the train to other on-board subsystems which in turn pass the localisation information on to trackside subsystems, e.g., as part of position reports.

6.3.2.2 Architecture view of the on-board vehicle locator is depicted in Figure 5

6.3.2.3 The Vehicle Locator functional box is surrounded by different elements grouped by their influence with the VL:

6.3.2.4 Sensor Data of VLS. Data that responds to some type of input from the physical environment and helps to locate the vehicle. These data can come from elements deployed on tracks such as Eurobalises or other on-board equipment that can acquire data from the environment or the kinematic characteristics of the vehicle itself (see section 6.3.3).

6.3.2.5 Supporting Information. Information not directly translatable into localisation information but needed to provide the desired output. This information will be used by internal VL processes to enable, improve or validate localisation information.

6.3.2.6 VL Output Consumers. Grouping of on-board and trackside consumers of localisation information. Further details on identified consumers can be found in OCORA [R4] and section 6.4.1.

6.3.2.7 Generic Functions. Generic functions common to every functional box (diagnostic, maintenance and access control) in the context of RCA and OCORA.

6.3.2.8 Several interfaces link the VL with the surrounding elements as depicted in Figure 5 (red and green labels). The other sources are more provider choice, not to be standardised (in principle) and are outside the scope of this architecture.

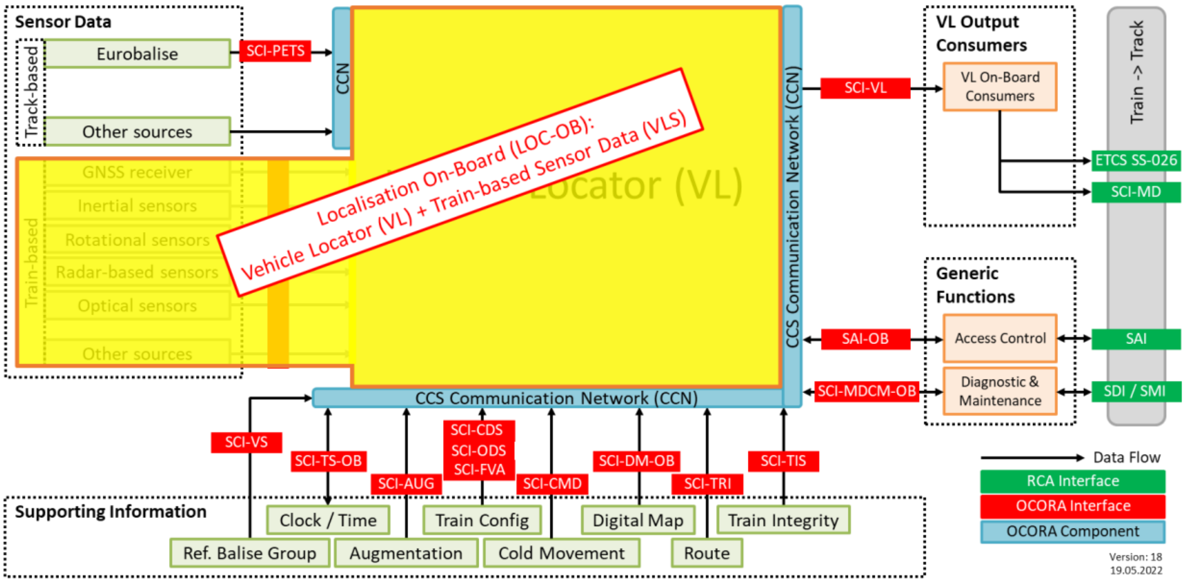


Figure 5 Localisation Concept Architecture Including the interface specification

6.3.2.9 Interface and component/subsystem (without SCI- and CI-prefix) descriptions can be found in section 6.4 and documents [R3] and [R4].

6.3.2.10 One VL is installed on every OCORA based CCS On-Board system. The sensors connected to it may differ from one installation to the other.

6.3.3 Vehicle Locator Sensors (VLS)

6.3.3.1 The Vehicle Locator Sensors provide raw data to determine speed, direction of travel, acceleration, position, and cold movement information to the Vehicle Locator. Depending on the RU's need and the progress of technology (e.g. GNSS, IMU) different type and quality of sensors may be used.

6.3.3.2 As an example, this logical component may include the functionality the locator sensors are providing. Sensor Data (train-based) is grouped into the following types ([R4]):

- GNSS Receiver. Autonomous geo-spatial positioning and time information based on satellite navigation systems.
- Inertial sensors. Provides the specific force, angular rate and the orientation of the body by using a combination of accelerometers, gyroscopes, and potentially magnetometers.
- Rotational sensors. Provides speed (e.g., tachometer, speed probe) and travelled distance (e.g., wheel revolution counter) measurements.
- Radar-based sensors. Distance and speed measurements, e.g., doppler radar, LiDAR, LGPR. May also be used to determine position information if used along with a sensor map.
- Optical sensors. Sensors based on image acquisition and analysis to recognise known elements from trackside that may be referenced, e.g., visual odometry, object recognition.
- Other sources. Other not explicitly identified sources gathered/measured on-board that may provide useful input information to the VL (e.g., radio-based technologies like FRMCS, WLAN, Ultra-Wideband).

6.3.3.3 Multiple Vehicle Locator Sensors are installed on every OCORA based CCS On-Board system, but the configuration of the sensors may differ from one installation to the other.

6.4 System Interfaces

6.4.1 Overview

6.4.1.1 Figure 6 gives a logical architecture description from the LOC-OB viewpoint. For a detailed description of the LOC-OB actors and the interfaces see [R3] and [R4].

6.4.2 Actors interacting with LOC-OB

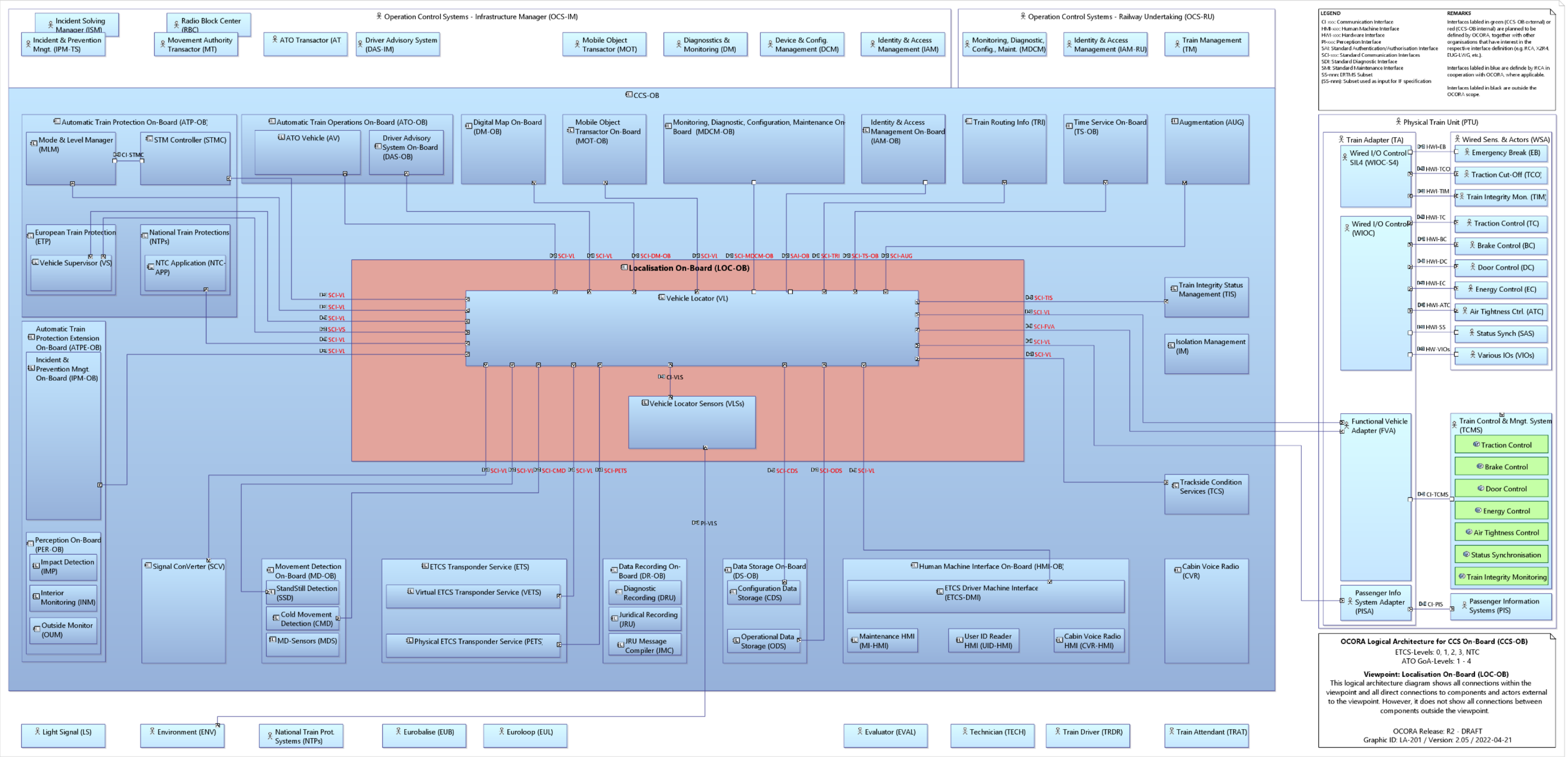
6.4.2.1 The OCORA Localisation On-Board Introduction [R4] identified the actors interacting with the Localisation On-Board (LOC-OB) the table is copied below.

6.4.2.2 There are two types of actors. The “consumers” are actors that receive localisation information from LOC-OB through the interface SCI-VL. The “providers” are actors that provide information to LOC-OB. The latter are not using the SCI-VL interface but provide the information to LOC-OB through their standardised interface.

6.4.2.3 See OCORA Localisation On-Board Introduction [R4] for a detailed description of the actors.

6.4.2.4 Details of the data exchanged between LOC-OB and the actors are given with the description of the LOC-OB functions in section 6.6

6.4.2.5 RA-A- 5: Potential actors in ERTMS/ETCS Level 3 are not defined in this version of the document. Thus, an update of the Risk Analysis might be necessary to include level 3 actors.


Operation Control Systems - Infrastructure Manager (OCS-IM)
Incident Solving Manager (ISM)
Radio Block Center (RBC)
Incident & Prevention Mngt. (IPM-TS)
Movement Authority Transactor (MT)
ATO Transactor (AT
Driver Advisory System (DAS-IM)
Mobile Object Transactor (MOT)
Diagnosstics & Monitoring (DM)
Device & Config. Management (DCM)
Identity & Access Management (IAM)
Operation Control Systems - Railway Undertaking (OCS-RU)
Monitoring, Diagnostic, Config., Maint. (MDCM)
Identity & Access Management (IAM-RU)
Train Management (TM)
CCS-OB
Automatic Train Protection On-Board (ATP-OB)
Mode & Level Manager (MLM)
STM Controller (STMC)
CI STMC
European Train Protection (ETP)
Vehicle Supervisor (VS)
National Train Protections (NTPs)
NTC Application (NTC-APP)
Automatic Train Operations On-Board (ATO-OB)
ATO Vehicle (AV)
Driver Advisory System On-Board (DAS-OB)
Digital Map On-Board (DM-OB)
Mobile Object Transactor On-Board (MOT-OB)
Monitoring, Diagnostic, Configuration, Maintenance On-Board (MDCM-OB)
Identity & Access Management On-Board (IAM-OB)
Train Routing Info (TRI)
Time Service On-Board (TS-OB)
Augmentation (AUG)
SCI-VL
SCI-VL
SCI-DM-OB
SCI-VL
SCI-MDCM-OB
SAI-OB
SCI-TRI
SCI-TS-OB
SCI-AUG
Localisation On-Board (LOC-OB)
Vehicle Locator (VL)
SCI-VL
SCI-VL
SCI-VL
SCI-VS
SCI-VL
SCI-VL
SCI-TIS
SCI-VL
SCI-FVA
SCI-VL
SCI-VL
CI-VLS
Vehicle Locator Sensors (VLSs)
SCI-VL
SCI-VL
SCI-CMD
SCI-VL
SCI-PETS
SCI-CDS
SCI-ODS
SCI-VL
PI-VLS
Train Integrity Status Management (TIS)
Isolation Management (IM)
Trackside Condition Services (TCS)
Automatic Train Protection Extension On-Board (ATPE-OB)
Incident & Prevention Mngt. On-Board (IPM-OB)
Perception On-Board (PER-OB)
Impact Detection (IMP)
Interior Monitoring (INM)
Outside Monitor (OUM)
Signal ConVerter (SCV)
Movement Detection On-Board (MD-OB)
StandStill Detection (SSD)
Cold Movement Detection (CMD)
MD-Sensors (MDS)
ETCS Transponder Service (ETS)
Virtual ETCS Transponder Service (VETS)
Physical ETCS Transponder Service (PETS
Data Recording On-Board (DR-OB)
Diagnostic Recording (DRU)
Juridical Recording (JRU)
JRU Message Compiler (JMC)
Data Storage On-Board (DS-OB)
Configuration Data Storage (CDS)
Operational Data Storage (ODS)
Human Machine Interface On-Board (HMI-OB)
ETCS Driver Machine Interface (ETCS-DMI)
Maintenance HMI (MI-HMI)
User ID Reader HMI (UID-HMI)
Cabin Voice Radio HMI (CVR-HMI)
Cabin Voice Radio (CVR)
Physical Train Unit (PTU)
Train Adapter (TA)
Wired I/O Control SIL4 (WIOC-S4)
Wired I/O Control (WIOC)
Wired Sens. & Actors (WSA)
HWI-EB
Emergency Break (EB)
HWI-TCO
Traction Cut-Off (TCO)
HWI-TIM
Train Integrity Mon. (TIM)
HWI-TC
Traction Control (TC)
HWI-BC
Brake Control (BC)
HWI-DC
Door Control (DC)
HWI-EC
Energy Control (EC)
HWI-ATC
Air Tightness Ctrl. (ATC)
HWI-SS
Status Synch (SAS)
HW-VIOs
Various IOs (VIOs)
Functional Vehicle Adapter (FVA)
Train Control & Mngt. System (TCMS)
Traction Control
Brake Control
Door Control
Energy Control
Air Tightness Control
Status Synchronisation
Train Integrity Monitoring
CI-TCMS
Passenger Info System Adapter (PISA)
CI-PIS
Passenger Information Systems (PIS)
Light Signal (LS)
Environment (ENV)
National Train Prot. Systems (NTPs)
Eurobalise (EUB)
Euroloop (EUL)
Evaluator (EVAL)
Technician (TECH)
Train Driver (TRDR)
Train Attendant (TRAT)

LEGEND

CI-xxx: Communication Interface
HMI-xxx: Human Machine Interface
HWI-xxx: Hardware Interface
PI-xxx: Perception Interface
SAI: Standard Authentication/Authorisation Interface
SCI-xxx: Standard Communication Interfaces
SDI: Standard Diagnostic Interface
SMI: Standard Maintenance Interface
SS-nnn: ERTMS Subset
(SS-nnn): Subset used as input for IF specification

REMARKS

Interfaces labled in green (CCS-OB external) or red (CCS-OB internal) are planned to be defined by OCORA, together with other organisations that have interest in the respective interface definition (e.g. RCA, X2R4, EUG-LWG, etc.).

Interfaces labled in blue are definde by RCA in cooperation with OCORA, where applicable.

Interfaces labled in black are outside the OCORA scope.

OCORA Logical Architecture for CCS On-Board (CCS-OB)
ETCS-Levels: 0, 1, 2, 3, NTC
ATO GoA-Levels: 1 - 4

Viewpoint: Localisation On-Board (LOC-OB)
This logical architecture diagram shows all connections within the viewpoint and all direct connections to components and actors external to the viewpoint. However, it does not show all connections between components outside the viewpoint.

OCORA Release: R2 - DRAFT
Graphic ID: LA-201 / Version: 2.05 / 2022-04-21

Figure 6 Logical architecture - Viewpoint Localisation On-Board (LOC-OB)

6.5 System Function principle

6.5.1 Localisation Principle

6.5.1.1 The LOC-OB shall provide localisation information which complies with the current ERTMS/ETCS principle (distance and orientation from a LRBG and a speed) called 1D positioning and can also provide additional localisation information such as:

- The absolute (3D) geographic positioning (Long, Lat, Alt),
- The vector acceleration within the 3D coordinate system based on the track axis,
- The vector velocity within the 3D coordinate system based on the track axis,
- The behaviour (roll, pitch, and yaw angles) of the coach where sensors are installed.

6.5.1.2 This localisation information is computed by the LOC-OB based on data provided by sensors and supporting information (e.g., digital map, augmentation data, routing information) upon availability.

6.5.1.3 As of now, the reference point is a LRBG but to take full advantage of the Digital Map, in the future, any designated point of the track on the map could be used as a reference point.

6.5.1.4 The LOC-OB architecture intends to break the strong coupling of the on-board ETCS logic and balise technology (LRBG) to allow vendors to produce industry-independent localisation products by adhering to the standardised interfaces.

6.5.1.5 Despite the tendency of reducing trackside assets such as balises and moving towards enhanced on-board localisation sensor technologies, the performance of the localisation system is seen as a key requirement to improve the capacity and the availability of the line and shall be further improved. As example, focus can be done to define a higher accuracy of the estimated position/speed and (more regularly) to reduce the confidence interval to a minimum.

6.5.2 Functions of Subset 26

6.5.2.1 Appendix C of the [R3] contains, on a very high-level, a first proposed split of functionality between the OCORA components, based on SUBSET-026 functions. The functions for which VL is partly involved are:

- Determine train position referenced to LRBG (Subset_ 26 section 3.6.1 and section 3.6.4)
- Determine train speed, train acceleration, train standstill (not explicitly defined in Subset 26 section 3)
- Determine Geographical Position (Subset_ 26 section 3.6.6)

6.6 System Functions

6.6.1 Definition

6.6.1.1 The system definition of LOC-OB is following the black box approach, i.e., only the inputs and outputs of LOC-OB have been identified and described.

6.6.1.2 Internal functions of LOC-OB (incl. the choice of localisation sensor technologies) will not be defined as part of this document.

6.6.1.3 The supplier is responsible for deciding on the technical solution in compliance with the agreed system requirements, system functions, and system interfaces.

6.6.1.4 System Functions describe the interactions with the System under Consideration (SuC), in our case LOC-OB.

6.6.1.5 In the following sub-chapters system functions are described based on one of the three prefixes:

a) Provide (LOC-OB_SF-**0xx**): Output function of LOC-OB

b) Acquire (LOC-OB_SF-**1xx**): Input function of LOC-OB

c) Control (LOC-OB_SF-**2xx**): Generic function of LOC-OB covering aspects such as authentication, authorisation, diagnostics, and maintenance

6.6.1.6 For a complete description of the functions see [R1]

6.6.2 List of functions of the LOC-OB system

6.6.2.1 LOC-OB_SF-001: Provide safe Train Front End 1D Position

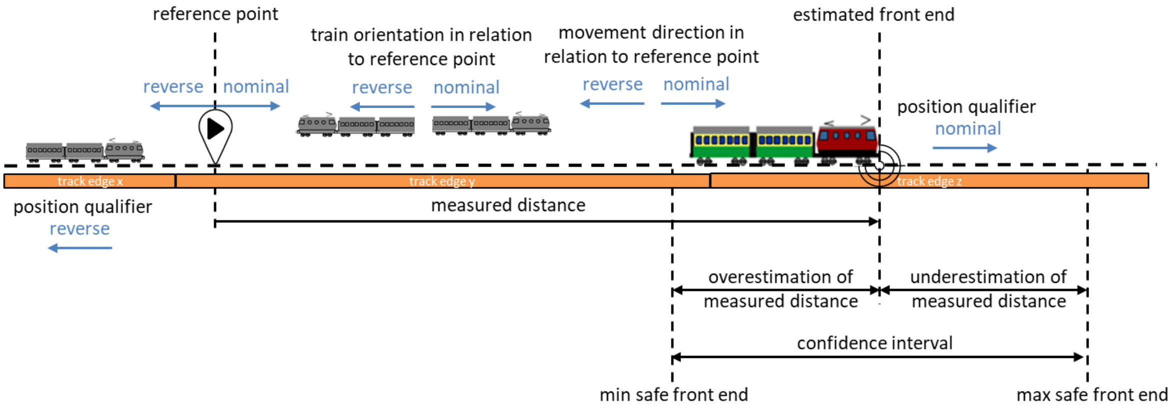


Figure 7: Illustration of terms used in LOC-OB_SF-001: Provide safe Train Front-end 1D Position.

6.6.2.2 LOC-OB_SF-002: Provide safe Train Speed

6.6.2.3 LOC-OB_SF-003: Provide safe Train Acceleration

6.6.2.4 LOC-OB_SF-004: Provide 3D Position and Uncertainty

6.6.2.5 LOC-OB_SF-005: Provide 3D Velocity and Uncertainty

6.6.2.6 LOC-OB_SF-006: Provide 3D Acceleration and Uncertainty

6.6.2.7 LOC-OB_SF-007: Provide 3D Attitudes (rotational Angles) and Uncertainty

6.6.2.8 LOC-OB_SF-008: Provide Estimated Distance Travelled (since power-on)

6.6.2.9 LOC-OB_SF-101: Acquire Digital Map

6.6.2.10 LOC-OB_SF-102: Acquire Route

6.6.2.11 LOC-OB_SF-103: Acquire Augmentation

6.6.2.12 OC_OB_SF-104: Acquire Train Integrity

6.6.2.13 LOC-OB_SF-105: Acquire Static Train Configuration

6.6.2.14 LOC-OB_SF-106: Acquire Dynamic Train Configuration

6.6.2.15 LOC-OB_SF-107: Acquire Eurobalise Telegram

6.6.2.16 LOC-OB_SF-108: Acquire Last Relevant Balise Group (LRBG)

6.6.2.17 LOC-OB_SF-109 Acquire Cold Movement

6.6.2.18 LOC-OB_SF-201: Control Time

6.6.2.19 LOC-OB_SF-202: Control Security Access

6.6.2.20 LOC-OB_SF-203: Control Diagnostic & Maintenance

6.6.3 Vehicle Locator Sensors Input

6.6.3.1 PI-VLS is a non-standardised perception interface between the Vehicle Locator Sensors (VLS) and their environment (ENV) that can, for example, include trackside mounted location tags on catenary poles. This interface is not further described/specified but listed for the purpose of architectural completeness.

6.6.3.2 Input PI-VLS

Group Name	Group contains
Sensor Data (Train-based)	GNSS Receiver. Autonomous geo-spatial positioning and time information based on satellite navigation systems. Inertial sensors. Provides the specific force, angular rate and the orientation of the body by using a combination of accelerometers, gyroscopes, and potentially magnetometers. Rotational sensors. Provides speed (e.g., tachometer, speed probe) and travelled distance (e.g., wheel revolution counter) measurements. Radar-based sensors. Distance and speed measurements, e.g., doppler radar, LiDAR, LGPR. Optical sensors. Sensors based on image acquisition and analysis to recognise known elements from trackside that may be referenced, e.g., visual odometry, object recognition. Other sources. Other not explicitly identified sources gathered/measured on-board that may provide useful input information to the VL (e.g. radio-based technologies like FRMCS, WLAN, Ultra-Wideband).

Table 1: Sensor Data

6.7 LOC-OB Functions and their intended consumers

6.7.1.1 The preliminary document Localisation Performance Requirements [R2], as defined a table which maps the functions and their intended consumers. This table is adapted here with the functions, which provides outputs, defined in section 6.6, and the consumers defined in section 6.4.2.2

6.7.1.2 The following legend has been used to denote the relationship between the consumer and the function:

- ‘+’ means that the function and its output(s) are consumed by the system of interest
- ‘-’ means that the function and its output(s) are not consumed by the system of interest
- ‘n.a.’ Not enough information is available in the reference documents to evaluate the needs of the system of interest at this stage

Table 2: LOC-OB Functions and their intended consumers

		System function / Output function							
Subsystem of interest (based on OCORA architecture)	***Subsystem Description (based on OCORA Localisation On-Board Introduction [R4])***	***LOC-OB_SF-001 1D Position***	***LOC-OB_SF-002 1D Speed***	***LOC-OB_SF-003 1D Acceleration***	***LOC-OB_SF-004 3D Position***	***LOC-OB_SF-005 3D Velocity***	***LOC-OB_SF-006 3D Acceleration***	***LOC-OB_SF-007 3D Attitudes***	***LOC-OB_SF-008 Estimated Distance travelled***
Vehicle Supervisor (VS)	The Vehicle Supervisor (VS) application, deployed on the OCORA computing platform, is a safe ETCS application (mandatory requirements are specified in SUBSET-026) in charge of calculating location specific speed limits (based on various inputs) and activating the braking system in case of speed limit overshoot. Location information is received from the Vehicle Locator (VL). In addition, information is received from the Balise Transmission Module (BTM) and the Loop Transmission Module (LTM) and processed adequately. In ETCS L2 and L3 mode, the VS interacts with the RBC or the APS-MT respectively. It receives the movement authority (MA) and reports the train position (TPR) to the respective system. The VS is agnostic to the communication technology used. Therefore, communication via GSM-R as well as via FRMCS or any future technology is possible. The VS also displays to the driver the necessary information (including cab signalling in ETCS L1, L2 and L3). It supports all ETCS modes and ETCS levels defined in the TSI-CCS.	+	+	+	n.a.	n.a.	n.a.	n.a.	+

		System function / Output function							
Subsystem of interest (based on OCORA architecture)	***Subsystem Description (based on OCORA Localisation On-Board Introduction [R4])***	***LOC-OB_SF-001 1D Position***	***LOC-OB_SF-002 1D Speed***	***LOC-OB_SF-003 1D Acceleration***	***LOC-OB_SF-004 3D Position***	***LOC-OB_SF-005 3D Velocity***	***LOC-OB_SF-006 3D Acceleration***	***LOC-OB_SF-007 3D Attitudes***	***LOC-OB_SF-008 Estimated Distance travelled***
Mode and Level Management (MLM)	The Mode & Level Manager (MLM) is a safe component of the ETCS Core in charge of managing the ETCS modes and levels. It ensures that the proper ETCS mode and level are active and manages the transitions from one mode or level to the other. In the latter context it also handles the handover between different R This logical component is in the train and should substitute Train Driver and Train Attendant responsibilities for reacting in case of an incident (Incident and Prevention Management - Onboard). It manages safe reflexive reactions, computed reactions, and safety procedures in cooperation with IPM-TS and ISM. This logical component is primarily used in case of GoA3/4 but may also assist the train driver in GoA1/2 operations. BCs. Furthermore, it makes sure that the correspondent information (e.g., current mode and level) is transmitted to the TCMS.	+	-	-	n.a.	-	-	-	+
STM Controller (STMC)	The STM Controller (STMC) is a safe component of the ETCS Core in charge of managing the safety authority between ETCS and installed national ATP systems (STM / NTC). It ensures that the proper ATP system is active and manages the switch-over from ETCS to the national ATP system and vice versa. The STMC interacts with the national ATP systems as defined in SUBSET-035 and SUBSET-058. The STMC with the respectively integrated national ATP systems enable an automatic transition from ETCS to the national ATP system and vice versa while the vehicle is driving.	+	+	n.a.	n.a.	n.a.	n.a.	n.a.	+
NTC Application (NTC-APP)	The National Train Controls Applications (NTC-APP), deployed on the OCORA computing platform, are safe applications in charge of ensuring Automatic train protection based on national systems. NTC-APPs, implemented on the OCORA computing platform, must communicate, as a minimum, with the Mode and Level Manager (MLM) and can use their specific sensors and actuators. In addition, they can take advantage of the	+	+	n.a.	n.a.	n.a.	n.a.	n.a.	+

		System function / Output function							
Subsystem of interest (based on OCORA architecture)	***Subsystem Description (based on OCORA Localisation On-Board Introduction [R4])***	***LOC-OB_SF-001 1D Position***	***LOC-OB_SF-002 1D Speed***	***LOC-OB_SF-003 1D Acceleration***	***LOC-OB_SF-004 3D Position***	***LOC-OB_SF-005 3D Velocity***	***LOC-OB_SF-006 3D Acceleration***	***LOC-OB_SF-007 3D Attitudes***	***LOC-OB_SF-008 Estimated Distance travelled***
	standard OCORA interfaces. E.g., location information can be received from the Vehicle Locator (VL), data can be recorded in the DR-OB, DMI can be used, the TCMS can be accessed through the Functional Vehicle Adapter (FVA) and the NTC-APPs can also access balise telegrams through the ETCS Transponder Service (ETS) in order to get the packet 44 information.								
Incident & Prevention Management On-Board (IPM-OB)	This logical component is in the train and should substitute Train Driver and Train Attendant responsibilities for reacting in case of an incident (Incident and Prevention Management - Onboard). It manages safe reflexive reactions, computed reactions, and safety procedures in cooperation with IPM-TS and ISM. This logical component is primarily used in case of GoA3/4 but may also assist the train driver in GoA1/2 operations.	n.a.	n.a.	n.a.	+	+	+	+	n.a.
ATO Vehicle (AV)	The ATO Vehicle (AV) application, deployed on the OCORA computing platform, is a non-safe application for Automatic train operations. A safe extension is needed for GoA3 and GoA4 operations. This is provided by the ATO Perception Vehicle (APV). The AV in GoA2 – GoA4 controls the vehicle’s speed, using information received through the interface SS126. It also communicates with the Vehicle Supervisor (VS) over the interface SS130 (between AV and ETCS Core). Remark: AV is called ATO-OB in GoA2 Shift2Rail SUBSET-125.	+	+	+	-	-	-	-	+
Driver Advisor System On-Board (DAS-OB)	The Driver Advisory System On-Board is an optional and non-safe application calculating an energy efficient speed profile to achieve the pre-planned and dynamically updated train timings. It generates detailed driver advice for adhering to the planned timings while driving energy efficient. The trackside Driver Advisory or the Traffic Management System (TMS) is responsible for conflict detection and calculation of new target train timings, that are forwarded to the DAS-OB and evaluated	+	+	n.a.	n.a.	n.a.	n.a.	n.a.	+

		System function / Output function							
Subsystem of interest (based on OCORA architecture)	***Subsystem Description (based on OCORA Localisation On-Board Introduction [R4])***	***LOC-OB_SF-001 1D Position***	***LOC-OB_SF-002 1D Speed***	***LOC-OB_SF-003 1D Acceleration***	***LOC-OB_SF-004 3D Position***	***LOC-OB_SF-005 3D Velocity***	***LOC-OB_SF-006 3D Acceleration***	***LOC-OB_SF-007 3D Attitudes***	***LOC-OB_SF-008 Estimated Distance travelled***
	accordingly. The typical integration of DAS-OB application is defined EN 15380-4. The DAS-OB can also operate standalone (e.g., without integration into the vehicle). The DAS-OB is not needed if ATO Vehicle (AV) is installed, since the AV already includes the DAS functionality. The implementation of DAS application on the OCORA computing platform is an open issue to be solved in subsequent versions of this document (unsafe information displayed on the driver DMI).								
Mobile Object Transactor On-Board (MOT-OB)	The logical component MOT-OB communicates with various CCS On-Board logical components and communicates with the MOT. The need for this component is an open issue to be solved in subsequent versions of this document.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Digital Map On-Board (DM-OB)	The logical component DM-OB is a safe service deployed on the OCORA computing platform. The DM-OB provides topology and topography data (a.k.a. map data) that are certified for the usage in safety-relevant On-Board applications / services (e.g., VL, VS, PER-OB) up to SIL4. The service guarantees that the map data fulfils the quality criteria stated by trackside, e.g., accurate, precise, reliable, complete, and up-to-date map data. The DM-OB uses its own On-Board data storage that is updated, if required, using the functionality of the Monitoring, Diagnostic, Configuration, Maintenance On-Board (MDCM-OB) to propagate trackside map data (e.g., from Topo4) to the On-Board data storage. It provides Map Data to the LOC-OB (see 6.6.10 LOC-OB_SF-101 : Acquire Digital Map).	+	-	-	-	-	-	-	-
Monitoring, Diagnostic. Configuration, Maintenance On-	The logical component MDCM-OB deployed on the OCORA computing platform, collects data relevant for local (through the Maintenance Terminal or DMI) and remote diagnostic and monitoring. For local maintenance, it provides the relevant data upon request to the Maintenance Terminal or DMI in a standardised format. For remote	+	+	+	+	+	+	+	+

		System function / Output function							
Subsystem of interest (based on OCORA architecture)	***Subsystem Description (based on OCORA Localisation On-Board Introduction [R4])***	***LOC-OB_SF-001 1D Position***	***LOC-OB_SF-002 1D Speed***	***LOC-OB_SF-003 1D Acceleration***	***LOC-OB_SF-004 3D Position***	***LOC-OB_SF-005 3D Velocity***	***LOC-OB_SF-006 3D Acceleration***	***LOC-OB_SF-007 3D Attitudes***	***LOC-OB_SF-008 Estimated Distance travelled***
Board (MDCM-OB)	diagnostics and monitoring the data can be sent to multiple recipients (e.g., the RU of the vehicle, the IM the vehicle currently operates in, the vehicle provider, the CCS On-Board provider etc.). The owner of the vehicle can define in the vehicle's configuration (refer to Configuration Data Storage) what data is forwarded to which recipient(s). The MDCM-OB also allows for local (through the Maintenance Terminal) and remote (through the centralised DCM services) configuration of the vehicle's devices (CCUs, Gateway, Peripherals, etc.). The component can process data received by the IMs (network related operational data) and the RU (vehicle related operational and configuration data). The service also allows the RU to execute commands (e.g., reboot of a specific component) and allows to install updates (e.g., new software).								
Identity & Access Management On-Board (IAM-OB)	The Identity & Access Management On-Board (IAM-OB) is a service deployed on the OCORA computing platform. It integrates with the IAM System providing the central management for the identification, authentication and authorisation of devices and applications to resources and functions of the CCS On-Board and trackside systems. For the identification, the IAM System manages a unique ID for each entity (e.g., device, application). The granularity, on what level the system will be split into separate entities is not yet defined. It can reach from one single ID for the overall CCS On-Board system to IDs for any single device connected to the CCN and to applications, running on the OCORA Platform. For the authentication of a device or an application, the solution could be based on the Public Key Infrastructure (PKI) or Message Authentication Codes (MAC) using symmetrical encryption mechanisms like 3DES or AES. The access to resources and functions is centrally managed by roles and granted on a Need-to-Know principle to limit unauthorised access to resources and functions within the CCS On-Board system.	n.a.	-	-	n.a.	-	-	-	-

		System function / Output function							
Subsystem of interest (based on OCORA architecture)	***Subsystem Description (based on OCORA Localisation On-Board Introduction [R4])***	***LOC-OB_SF-001 1D Position***	***LOC-OB_SF-002 1D Speed***	***LOC-OB_SF-003 1D Acceleration***	***LOC-OB_SF-004 3D Position***	***LOC-OB_SF-005 3D Velocity***	***LOC-OB_SF-006 3D Acceleration***	***LOC-OB_SF-007 3D Attitudes***	***LOC-OB_SF-008 Estimated Distance travelled***
Trackside Condition Services (TCS)	The Trackside Condition Services (TCS) is a non-safe component of the ETCS Core in charge of managing the trackside condition information received from balises, RIU, or RBC. It calculates the remaining distance to specific trackside points and triggers the appropriate actions according to the location. Location information is received from the Vehicle Locator (VL). Also, the TCS informs the driver about the trackside points: it sends the commands to display the different pictograms on the DMI depending on the trackside point and the relative location to it. Furthermore, it makes sure that the correspondent information is transmitted using the SCI-FVA interface via FVA to the vehicle, and the distance information is updated as needed. The TCS remains active during level transitions, including transition to level NTC.	+	n.a.	-	n.a.	-	-	-	n.a.
ETCS Driver Machine Interface (ETCS-DMI)	The ETCS-DMI component provides the functionality for any user interaction with the ETCS On-Board system.	+	+	-	-	-	-	n.a.	+
Virtual ETCS Transporter Service (VETS)	The VETS component generates virtual ETCS telegrams based on the current location using the Digital Map On-Board (DM-OB).	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Standstill Detection (SSD)	The logical component SSD detects if the train is standing still.	+	+	+	-	-	-	-	-
SIgnal Converter (SCV)	The Signal Converter (SCV) is in the train and converts the information coming from optical signals into SUBSET-026 compliant information.	-	-	-	+	+	+	+	-
Functional Vehicle Adapter (FVA) / Train Interface Unit (TIU).	The Functional Vehicle Adapter (FVA) is a piece of software deployed on the OCORA computing platform, on a separate computing unit, or on the OCORA Gateway. Its job is to provide an OCORA unified and standardised interface (SCI-FVA) for the OCORA Software to access vehicle functions and vehicle information. Furthermore, it uses a specific	+	+	+	-	-	-	-	-

		System function / Output function							
Subsystem of interest (based on OCORA architecture)	***Subsystem Description (based on OCORA Localisation On-Board Introduction [R4])***	***LOC-OB_SF-001 1D Position***	***LOC-OB_SF-002 1D Speed***	***LOC-OB_SF-003 1D Acceleration***	***LOC-OB_SF-004 3D Position***	***LOC-OB_SF-005 3D Velocity***	***LOC-OB_SF-006 3D Acceleration***	***LOC-OB_SF-007 3D Attitudes***	***LOC-OB_SF-008 Estimated Distance travelled***
	interface (SCI-VL) to provide localisation information to the TCMS. Although the TSI-CCS SUBSET-034, SUBSET-119, and SUBSET-139 are defining the interface to the TCMS system, vehicles from different suppliers and especially from different generations have still different interfaces implemented. This adapter allows to map, on a functional level, the commands sent, and the information received from a specific TCMS into the OCORA standard. This includes that the FVA can likewise be used to integrate vehicles through wired connections.								
Passenger Info System Adapter (PISA)	The Passenger Information System Adapter (PISA) is a non-safe piece of software deployed on the OCORA computing platform, or on the OCORA Gateway. Its job is to provide an OCORA unified and standardised interface towards the Cabin Voice Radio (CVR), allowing the PISA to receive CCS information of interest to the PIS.	+	+	+	-	-	-	-	-

7 Hazard and Risk assessment

7.1 Methodology

7.1.1.1 The guideline for the application of the CSM design targets [R7], [R8] provides classification of hazards when they arise as a result of failures of functions of the technical system. The following harmonised design targets shall apply to those failures:

1) Class a: where a failure has a credible potential to lead directly to an accident typically affecting a large number of people and resulting in multiple fatalities, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less than or equal to $10^{–9}$ per operating hour. Those the design target for the function involves in this failure is $10^{-9/}$h
2) Class b: where a failure has a credible potential to lead directly to an accident typically affecting a very small number of people and resulting in at least one fatality, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be less than or equal to $10^{–7}$ per operating hour. Therefore, the design target for the function involves in this failure is 10^{-7}/h.
3) Acceptable risk: when the risk is acceptable it is classified as broadly acceptable risks.

7.1.1.2 The risk assessment follows the methodology defined in the Common Safety Methods [R7].

7.1.1.3 The risk acceptability of the system under assessment shall be evaluated by using one or more of the following acceptance principles:

1) Code of practice: application of codes of practice
2) Similar reference system: similarly, analysis with reference system
3) Explicit of risk estimation: identification of scenarios & associated safety measures, if safety criteria is quantitative risk estimation based on frequency and severity has to be carried out.

7.1.1.4 CSM guide [R8] for the application of the Common Safety Method recommends:

When the hazards are not covered by one of the two risk acceptance principles **code of practice** or **similar reference system,** the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account.

7.2 Context and assumptions

7.2.1.1 By applying the CSM guideline to the LOC-OB, a first selection of risk acceptance method for each part of the LOC-OB has been done. **Similar reference system** has been selected: this risk assessment criteria might be applied for initial focus if equivalent system could be identified. This risk assessment criteria is relevant to the LOC-OB as it contributes to the overall performances of the ERTMS/ETCS. In our context at system level, the reference system is ERTMS/ETCS. LOC-OB hazards are bear by the ERTMS/ETCS and based on the hazards defined in Subset-091 [R13].

7.2.1.2 This selection of risk acceptance method will be updated with the availability of RCA/OCORA documentation or change of environment.

7.2.1.3 The result of the application of the CSM is, if some failures lead to hazard not broadly acceptable and no risk reduction is foreseen, the function shall be assigned by a design target of 10-9/h or 10-7/h depending on the class of the failure.

7.2.1.4 For the risk assessment criteria at system level, the following assumptions applied.

7.2.1.5 **RA-A- 1**: The boundary of the hazard analysis is limited to the impact of the Localisation system on the ETCS system, based on an OCORA architecture.

7.2.1.6 **RA-A- 2**: The reference system is ERTMS/ETCS, at system level, Localisation system hazards are bear by the ERTMS/ETCS.

7.2.1.7 **RA-A- 3**: In this context it is relevant to reuse the ERTMS/ETCS Fault Tree Analysis and Failure Mode and Effects analysis results to identify in the existing hazards list, fear events list, which of them can be considered in a possible involvement of the Localisation system.

7.2.1.8 **RA-A- 4**: The Risk Analysis is based on available subsets 091 and 088 at the time of the analysis which do not include ERTMS/ETCS level 3 and changes under definition. The results are based on the existing ERTMS/ETCS hazards analysis limited to level 1 & 2. Thus, an update of the Risk Analysis might be necessary to include level 3 findings, changes.

7.2.1.9 After analysis subsets 091 [R13] and 088 [R12], among the hazards listed in subset 091, 8 hazards of the ERTMS/ETCS system have been identified with a possible involvement of the LOC-OB.

7.3 Hazard Identification

7.3.1.1 The following table presents the results of the analysis of the ERTMS/ETCS system with the links between hazards and the references to the FTA and FMEA of subset 088 [R12].

Table 3: Hazard Identification

Subset 091_V360 Annex A Event Id.	Event Description	SUBSET-088-2 Part 1 reference to FTA Main parent sheet	SUBSET-088-2 Part 2 FMEA Affected ETCS function
MMI-2a.1	False presentation of train speed	Driver exceeds safe speed/distance	Information to driver
MMI-2a.2	False presentation of speed (except train speed) or distance, including supervision status	Driver exceeds safe speed/distance	Information to driver
ODO-1	Incorrect standstill indication	Failure of Brake control function Incorrect determination of actual speed and position	Standstill Indication
ODO-2	Speed measurement underestimates trains actual speed	Driver exceeds safe speed/distance Incorrect determination and Supervision of EOA/LOA, SL, Shortening of MA Incorrect determination of actual speed and position	Determination of distance travelled, Determination of train position relative to LRBG Position reporting, Provision of MA. Common mode error as it affects both the supervision and the display to the driver
ODO-3	Incorrect actual physical speed direction	Incorrect determination of train position ref to LRBG	Determination of train position relative to LRBG

Subset 091_V360 Annex A Event Id.	**Event Description**	**SUBSET-088-2 Part 1 reference to FTA Main parent sheet**	**SUBSET-088-2 Part 2 FMEA Affected ETCS function**
ODO-4	The confidence interval for distance measurement does not include the real position of the train	Incorrect determination of train position ref to LRBG	Position Reports, Information to driver. Incorrect determination of speed and position.
ODO-5	Acceleration measurement overestimates train actual acceleration during traction	Unsafe dynamic speed profile	Dynamic Speed Profile
ODO-6	Deceleration measurement underestimates train actual deceleration during braking (see figure 45 in subset 26 §3.13.9.3.2)	Unsafe dynamic speed profile	Dynamic Speed Profile
KERNEL-28	Incorrect confidence interval	Incorrect determination of train position ref to LRBG	Determination of distance travelled Determination of train position to LRBG

7.3.1.2 **RA-OP-5**: ODO_5 and ODO_6 are new proposals (linked to KERNEL-11 and KERNEL -25): expecting the next subset 88 version will cover acceleration and deceleration to confirm this event (acceleration and deceleration are used in the last version of subset 26)

7.4 Derived Hazard and Fear Events

7.4.1.1 Following hazard identification at the ERTMS/ETCS system level, the following table presents the derived hazards, fear events at the level of the LOC-OB.

Table 4: Derived hazard and fear events

Subset 091_V360 Annex A Event Id.	Event Description	LOC-OB Feared Event
MMI-2a.1	False presentation of train speed	Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed **RA-OP-1**: To confirm if the speed provided by VL is used by the DMI
MMI-2a.2	False presentation of speed (except train speed) or distance, including supervision status	Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed **RA-OP-1**: To confirm if the speed provided by VL is used by the DMI
ODO-1	Incorrect standstill indication	Fail to provide the correct train movement direction Fail to provide the correct train orientation Fail to use the correct reference point information from digital map Fail to use the correct reference point id Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed Fail to provide confidence position interval which include the real train position (measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties) **RA-OP-2**: To confirm the interface between VL and SSD

Subset 091_V360 **Annex A** **Event Id.**	**Event Description**	**LOC-OB Feared Event**
ODO-2	Speed measurement underestimates trains actual speed	Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed
ODO-3	Incorrect actual physical speed direction	Fail to provide the correct train movement direction Fail to provide the correct train orientation Fail to use the correct reference point information from digital map Fail to use the correct reference point id
ODO-4	The confidence interval for distance measurement does not include the real position of the train	Fail to provide confidence position interval which include the real train position (measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties) Fail to provide confidence estimated distance travelled
ODO-5	Acceleration measurement overestimates trains actual acceleration during traction	Fail to provide overestimated acceleration lower than the ground train acceleration **RA-OP-5**: ODO_5 and ODO_6 are new proposals (linked to KERNEL-11 and KERNEL -25): expecting the next subset 88 version will cover acceleration and deceleration to confirm this event (acceleration and deceleration are used in the last version of subset 26)
ODO-6	Deceleration measurement underestimates trains actual deceleration	Fail to provide underestimated deceleration higher than the ground train deceleration

Subset 091_V360 **Annex A** **Event Id.**	**Event Description**	**LOC-OB Feared Event**
	during braking (see figure 45 in subset 26 §3.13.9.3.2)	**RA-OP-5**: ODO_5 and ODO_6 are new proposals (linked to KERNEL-11 and KERNEL -25): expecting the next subset 88 version will cover acceleration and deceleration to confirm this event (acceleration and deceleration are used in the last version of subset 26)
KERNEL-28	Incorrect confidence interval	Fail to provide confidence position interval which includes the real train position (measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties) Fail to provide confidence incorrected estimated distance travelled interval **RA-OP-6:** To confirm that the function 3.6.4 Train Position Confidence Interval and Relocation from subset 26 shall be covered by LOC-OB in the future architecture

7.5 Summary of Fear Events for LOC-OB

7.5.1.1 From the previous section 7.4 hazards are identified at the level of the LOC-OB:

LOC-OB Feared Event Id.	LOC-OB Feared Event Description
LOC-OB_FE_01	Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed
LOC-OB_FE_02	Fail to provide the correct train movement direction
LOC-OB_FE_03	Fail to provide the correct train orientation
LOC-OB_FE_04	Fail to use the correct reference point information from digital map
LOC-OB_FE_05	Fail to use the correct reference point id
LOC-OB_FE_06	Fail to provide confidence position interval which include the real train position (measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties)
LOC-OB_FE_07	Fail to provide overestimate acceleration lower than the ground train acceleration
LOC-OB_FE_08	Fail to provide underestimated deceleration higher than the ground train deceleration
LOC-OB_FE_09	Fail to provide incorrected confidence estimated distance travelled interval

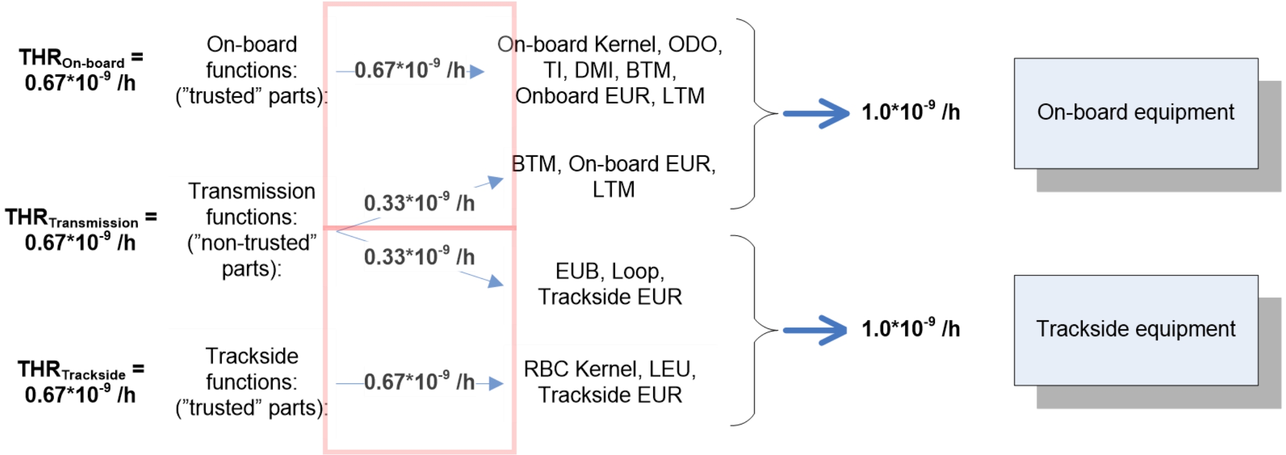
Table 5: Summary of ferared events

8 Safety requirements and apportionment

8.1 Methodology

8.1.1.1 The THR/TFFR apportionment for each function of the LOC-OB is derived from the overall ERTMS/ETCS apportionment principles.

8.1.1.2 The apportionment between the onboard functions, the transmission functions and the trackside functions are defined in subset 091 [R13]. The following figure presents the apportionment between the subsystems of the ERTMS/ETCS.



THR On-board = 0.67*10-9 /h
On-board functions: (”trusted” parts):
0.67*10-9 /h
On-board Kernel, ODO, TI, DMI, BTM, Onboard EUR, LTM
BTM, On-board EUR, LTM
1.0*10-9 /h
On-board equipment
THR Transmission = 0.67*10-9 /h
Transmission functions: (”non-trusted” parts):
0.33*10-9 /h
0.33*10-9 /h
EUB, Loop, Trackside EUR
1.0*10-9 /h
Trackside equipment
THR Trackside = 0.67*10-9 /h
Trackside functions: (”trusted” parts):
0.67*10-9 /h
RBC Kernel, LEU, Trackside EUR

Figure 8 ERTMS/ETCS apportionment between the 3 subsystems

8.1.1.3 With the development of the vehicle locator and the main goal to reduce the number of trackside assets, the number of physical balises will be limited, new architecture or changes will be introduced, therefore, this apportionment might be amended in the future, especially with risk analysis on the OCORA architecture.

8.1.1.4 The apportionment of each feared events of the core ERTMS/ETCS is depending on the supplier design. The apportionment of each hazard at the gate level is not defined. The THR is defined only at the overall onboard level.

8.1.1.5 At the minimum when safety related function is involved, the TFFR should be at least less than the onboard system THR 0.67*10-9/h and by taking into account the LOC-OB in the ERTMS/ETCS fault tree it could be more around of 10-10/h. The exact figure cannot be derived at this stage of the analysis.

8.1.1.6 Despite the specific TFFR of each function is not identified, it is possible at least to define the relevant SIL allocated to the function (e.g. if the TFFR < 10-9/h, safety requirements for the function SIL 4)

8.2 FMEA of LOC-OB

8.2.1.1 The following table provides the results of FMEA for each LOC-OB function (see chapter 6.6), identifying the possible feared events leading to the LOC-OB hazard (see chapter 1.1) and the barriers (safety relevant function) to be put in place.

8.2.1.2 Only the safety relevant functions and safe data provided are identified previously are detailled in this table.

8.2.1.3 Some barriers are defined on the inputs of the LOC-OB unit, when these inputs have been identified as used by the function. However, this identification cannot be exhaustive as the LOC-OB unit is view as a black-box.

Table 6: FMEA of LOC-OB

Functions		**Feared Events**		**Explanations**	**Hazards**	**Barriers (external/Mitigation)**	**Design Target TFFR**
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_05	Fail to use the correct reference point id	The reference point id provided by the safe 1D position function is incorrect or missing.	ODO-1	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the reference point Id shall be safely done according to EN 50159	$< 10^{-9}$/h
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_05	Fail to use the correct reference point id	The reference point id provided by the safe 1D position function is incorrect or missing.	ODO-3	Function shall be designed in SIL4 and the output safely provided according to EN 50159	$< 10^{-9}$/h

						A safety CCS communication network between component shall be available to exchange data Acquisition of the reference point Id shall be safely done according to EN 50159	
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_03	Fail to provide the correct train orientation	The train orientation provided by the safe 1D position function is incorrect or missing	ODO-1	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the Static Train Configuration shall be safely done according to EN 50159Acquisition of the Dynamic Train Configuration shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159	< 10^{-9}/h
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_03	Fail to provide the correct train orientation	The train orientation provided by the safe 1D position function is incorrect or missing	ODO-3	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the Static Train Configuration shall be safely done according to EN 50159	< 10^{-9}/h

						Acquisition of the Dynamic Train Configuration shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159	
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_02	Fail to provide the correct train movement direction	The train movement direction provided by the safe 1D position function is incorrect or missing	ODO-1	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the Static Train Configuration shall be safely done according to EN 50159 Acquisition of the Dynamic Train Configuration shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159	< 10^{-9}/h
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_02	Fail to provide the correct train movement direction	The train movement direction provided by the safe 1D position function is incorrect or missing	ODO-3	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data	< 10^{-9}/h

						Acquisition of the Static Train Configuration shall be safely done according to EN 50159 Acquisition of the Dynamic Train Configuration shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159	
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_04	Fail to use the correct reference point information from digital map	The position quantifier provided by the safe 1D position function is incorrect or missing	ODO-1	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the reference Id shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the LRBG shall be safely done according to EN 50159	$< 10^{-9}$/h
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_04	Fail to use the correct reference point information from digital map	The position quantifier provided by the safe 1D position function is incorrect or missing	ODO-3	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the reference Id shall be safely done according to EN 50159	$< 10^{-9}$/h

						Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the LRBG shall be safely done according to EN 50159	
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_04	Fail to use the correct reference point information from digital map	The Track edge Id provided by the safe 1D position function is incorrect or missing	ODO-1	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the reference Id shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159	$< 10^{-9}$/h
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_04	Fail to use the correct reference point information from digital map	The Track edge Id provided by the safe 1D position function is incorrect or missing	ODO-3	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the reference Id shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159	$< 10^{-9}$/h
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_06	Fail to provide confidence position interval which include the real	The measured distance interval and position qualifier and reference point id and track edge id and train front end	ODO-1	Function shall be designed in SIL4 and the output safely provided according to EN 50159	$< 10^{-9}$/h

			train position (measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties)	safety properties provided by the safe 1D position function is incorrect or missing		A safety CCS communication network between component shall be available to exchange data Acquisition of the reference Id shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159 Acquisition of the LRBG shall be safely done according to EN 50159 Acquisition of the train integrity information shall be safely done according to EN 50159 Acquisition of the Augmentation information shall be safely done according to EN 50159 Acquisition of the Eurobalise Telegram shall be safely done according to EN 50159	
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_06	Fail to provide confidence position interval which include the real train position (measured distance interval and position qualifier and reference point id and track	The measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties provided by the safe 1D position function is incorrect or missing	ODO-4	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the reference Id shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159	$< 10^{-9}$/h

			edge id and train front end safety properties)			Acquisition of the LRBG shall be safely done according to EN 50159 Acquisition of the train integrity information shall be safely done according to EN 50159 Acquisition of the Augmentation information shall be safely done according to EN 50159 Acquisition of the Eurobalise Telegram shall be safely done according to EN 50159	
LOC-OB_SF-001	Provide safe Train Front End 1D Position	LOC-OB_FE_06	Fail to provide confidence position interval which include the real train position (measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties)	The measured distance interval and position qualifier and reference point id and track edge id and train front end safety properties provided by the safe 1D position function is incorrect or missing	KERNEL-28	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the reference Id shall be safely done according to EN 50159 Acquisition of the Digital Map shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159 Acquisition of the LRBG shall be safely done according to EN 50159 Acquisition of the train integrity information shall be safely done according to EN 50159 Acquisition of the Augmentation information shall be safely done according to EN 50159 Acquisition of the Eurobalise Telegram shall be safely done according to EN 50159	< 10^{-9}/h

LOC-OB_SF-002	Provide safe Train Speed	LOC-OB_FE_01	Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed	The underestimated train speed provided by the safe 1D train speed function is incorrect or missing	MMI-2a.1	Function shall be designed in SIL4 and the output safely provided according to EN 50159	$< 10^{-9}$/h
LOC-OB_SF-002	Provide safe Train Speed	LOC-OB_FE_01	Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed	The underestimated train speed provided by the safe 1D train speed function is incorrect or missing	MMI-2a.1	Function shall be designed in SIL4 and the output safely provided according to EN 50159	$< 10^{-9}$/h
LOC-OB_SF-002	Provide safe Train Speed	LOC-OB_FE_01	Fail to provide correct speed by providing underestimated speed when the train is actually travelling at a higher speed	The underestimated train speed provided by the safe 1D train speed function is incorrect or missing	ODO-1	Function shall be designed in SIL4 and the output safely provided according to EN 50159	$< 10^{-9}$/h
LOC-OB_SF-002	Provide safe Train Speed	LOC-OB_FE_01	Fail to provide correct speed by providing	The underestimated train speed provided by the safe 1D train speed	ODO-2	Function shall be designed in SIL4 and the output safely provided according to EN 50159	$< 10^{-9}$/h

			underestimated speed when the train is actually travelling at a higher speed	function is incorrect or missing			
LOC-OB_SF-003	Provide safe Train Acceleration	LOC-OB_FE_07	Fail to provide overestimate acceleration lower than the ground train acceleration	The overestimated train acceleration provided by the safe 1D train acceleration function is incorrect or missing	ODO-5	Function shall be designed in SIL4 and the output safely provided according to EN 50159	< 10^{-9}/h
LOC-OB_SF-003	Provide safe Train Acceleration	LOC-OB_FE_08	Fail to provide underestimate deceleration higher than the ground train deceleration	The underestimated train deceleration provided by the safe 1D train deceleration function is incorrect or missing	ODO-6	Function shall be designed in SIL4 and the output safely provided according to EN 50159	< 10^{-9}/h
LOC-OB_SF-004	Provide 3D Position and Uncertainty	No evaluation: expected safety target of the potential consumer is to define					
LOC-OB_SF-005	Provide 3D Velocity and Uncertainty	No evaluation: expected safety target of the potential consumer is to define					
LOC-OB_SF-006	Provide 3D Acceleration and Uncertainty	No evaluation: expected safety target of the potential consumer is to define					

LOC-OB_SF-007	Provide 3D rotational Angles and Uncertainty	No evaluation: expected safety target of the potential consumer is to define					
LOC-OB_SF-008	Provide Estimated Distance Travelled	LOC-OB_FE_09	Fail to provide confidence estimated distance travelled	The estimated distance travelled interval provided by the Estimated Distance Travelled function is incorrect or missing	ODO-4	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the Static Train Configuration shall be safely done according to EN 50159 Acquisition of the DynamicTrain Configuration shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159 Acquisition of the cold movement shall be safely done according to EN 50159 Acquisition of the LRBG shall be safely done according to EN 50159	< 10^{-9}/h
LOC-OB_SF-008	Provide Estimated Distance Travelled	LOC-OB_FE_09	Fail to provide confidence estimated distance travelled	The estimated distance travelled interval provided by the Estimated Distance Travelled function is incorrect or missing	KERNEL-28	Function shall be designed in SIL4 and the output safely provided according to EN 50159 A safety CCS communication network between component shall be available to exchange data Acquisition of the Static Train Configuration shall be safely done according to EN 50159	< 10^{-9}/h

						Acquisition of the Dynamic Train Configuration shall be safely done according to EN 50159 Acquisition of the Route shall be safely done according to EN 50159 Acquisition of the LRBG shall be safely done according to EN 50159 Acquisition of the cold movement shall be safely done according to EN 50159	

8.3 Safety target apportionment

8.3.1.1 Consequently, the following table presents the synthesis of the safety requirements in terms of function classification and the design target with regard the TFFR.

RA Function ID	RA: Safety-related?	Design target TFFR
LOC-OB_SF-001	Yes	$< 10^{-9}$/h
LOC-OB_SF-002	Yes	$< 10^{-9}$/h
LOC-OB_SF-003	Yes	$< 10^{-9}$/h
LOC-OB_SF-004	No	n.a.
LOC-OB_SF-005	No	n.a.
LOC-OB_SF-006	No	n.a.
LOC-OB_SF-007	No	n.a.
LOC-OB_SF-008	Yes	$< 10^{-9}$/h

Table 7: Safety apportionment

8.3.1.2 As said in section 8.1, the THR is defined only at the overall on-board level. These designed target TFFR should be reviewed according to the availability of detailed needs from the supplier and consumers modules.

9 Assumptions, Safety Related Application Conditions and Open Points

9.1.1.1 The table presents the synthesis of assumptions identified during the risk analysis of the LOC-OB.

Id	Assumptions
RA-A-01	The boundary of the hazard analysis is limited to the impact of the Localisation system on the ETCS system, based on an OCORA architecture.
RA-A-02	The reference system is ERTMS/ETCS, at the system level, Localisation system hazards are bear by the ERTMS/ETCS.
RA-A-03	In this context it is relevant to reuse the ERTMS/ETCS Fault Tree Analysis and Failure Mode and Effects analysis results to identify, within the existing hazards list/ fear events list, which of them apply to the Localisation system.
RA-A-04	The Risk Analysis is based on available subsets 091 and 088 at the time of the analysis which do not include ERTMS/ETCS level 3 and changes under definition. The results are based on the existing ERTMS/ETCS hazards analysis limited to level 1 & 2. Thus, an update of the Risk Analysis might be necessary to include level 3 changes.
RA-A-05	Potential actors in ERTMS/ETCS Level 3 are not defined in this version of the document. Thus, an update of the Risk Analysis might be necessary to include level 3 actors.
RA-A-06	LOC-OB_SF_106 “Acquire Dynamic Train Configuration” provides the TIMS availability information

Table 8: Assumptions

9.1.1.2 The following Safety Related Application Conditions (SRAC) are identified:

Id	SRAC	Receiver
RA-SRAC-01	A safety CCS communication network between component shall be available to exchange data	OCORA-SCI
RA-SRAC-02	Acquisition of the reference point Id shall be safely done according to EN 50159	OCORA-DM-OB/ SCI-DM-OB
RA-SRAC-03	Acquisition of the Dynamic Train Configuration shall be safely done according to EN 50159	OCORA-ODS/ SCI-ODS
RA-SRAC-04	Acquisition of the Digital Map shall be safely done according to EN 50159	OCORA-DM-OB/ SCI-DM-OB

RA-SRAC-05	Acquisition of the Route shall be safely done according to EN 50159	OCORA-TRI/ SCI-TRI
RA-SRAC-06	Acquisition of the LRBG shall be safely done according to EN 50159	OCORA-VS/ SCI-VS
RA-SRAC-07	Acquisition of the train integrity information shall be safely done according to EN 50159	OCORA-TIS/ SCI-TIS
RA-SRAC-08	Acquisition of the Static Train Configuration shall be safely done according to EN 50159	OCORA-CDS/ SCI-CDS
RA-SRAC-09	Acquisition of the cold movement shall be safely done according to EN 50159	OCORA-CMD/ SCI-CMD
RA-SRAC-10	Acquisition of the Augmentation information shall be safely done according to EN 50159	OCORA-AUG/ SCI-AUG
RA-SRAC-11	Acquisition of the Eurobalise Telegram shall be safely done according to EN 50159	OCORA-PETS/ SCI-PETS

Table 9: SRAC

9.1.1.3 The following open points are identified:

Open point #	**Event Id**	**Issue**
RA-OP-01	MMI-2a.1 MMI-2a.2	To confirm if the speed provided by VL is used by the DMI
RA-OP-02	ODO-1	To confirm the interface between VL and SSD
RA-OP-03	ODO-3	Closed
RA-OP-04	ODO-3	Closed
RA-OP-05	ODO-5	ODO_5 and ODO_6 are new proposals (linked to KERNEL-11 and KERNEL -25): expecting the next subset 88 version will cover acceleration and deceleration to confirm this event (acceleration and deceleration are used in the last version of subset 26)
RA-OP-06	KERNEL-28	To confirm that the function 3.6.4 “Train Position Confidence Interval and Relocation” from subset 26 shall be covered by LOC-OB in the future architecture

Table 10: Open points