Horizon 2020
European Union Funding
for Research & Innovation

Shift2Rail

X2RAIL 2

X2Rail-2

Project Title:	Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach and standard interfaces, enhancing traffic management system functions
Starting date:	01/09/2017
Duration in months:	36
Call (part) identifier:	H2020-S2RJU-CFM-IP2-01-2017
Grant agreement no:	777465

Deliverable D3.9

System Architecture Specification and System Functional Hazard Analysis for Stand Alone Fail-Safe Train Positioning

Due date of deliverable	Month 35
Actual submission date	22/04/2020
Organization name of lead contractor for this deliverable	CAI
Dissemination level	PU
Revision	05

Deliverable template version: 02 (12/10/17)

Authors

Author(s)	**CAF Investigación y Desarrollo (CAF I+D)** Iban Lopetegi, Josune Aranburu, Daniel Gutierrez
Contributor(s)	**Siemens Mobility (SMO)** Bernhard Stamm, Roger Staubli
	Thales Transportation Systems GmbH Dietmar Vogel

Version Management		
Version Number	**Modification Date**	**Description / Modification**
01	10/01/2020	First version delivered
02	05/05/2020	Version with WP3 members' revision proposals. - Architecture drawing and concepts clarified (SMO) - Annex reference coordinates clarifiyed (TTS) - Concepts and requirements for sensor interfaces revised and agreed (CEIT, TRV, SMO, TTS)
03	18/12/2020	Naming update according to grant agreement.
04	30/03/2021	Minor changes due to TMT review
05	06/04/2021	Minor changes from JU revision

1 Executive Summary

The European Union Agency for Railways (ERA) defined different mid and longer term strategic challenges related to the ERTMS specifications roadmap in [2]. The objective was to identify the optimal balance between (a) ERTMS Specification stability on one side and (b) their evolution (enhancements and errors) and ERTMS products on the other side, while safeguarding interoperability in the most economical way. In particular, ERA states that *"The strategic challenges linked to the evolution are mainly linked to developments which support the need for* ***further capacity increase*** *and to developments that* ***decrease the overall life cycle costs*** *of the ERTMS implementations.".* Furthermore, ERA has also recognized the satellite positioning as one of the main key elements of the future signalling system/concept aimed at allowing "*Potential reduction in* ***deployment*** *and* ***maintenance*** *of* ***balises*** *and* ***improved performance*** *due to* ***more accurate odometry****;"*

Previous projects focusing exclusively in GNSS, such as GSA STARS [3], have shown that the use of GNSS only it is not enough neither for performance reasons nor for safety reasons. As a consequence, GNSS shall be combined with other sensors to ensure a more accurate and reliable within the specified performance odometry subsystem than the existing one.

In order to solve the train positioning problem applicable to all environments, [1] defined the system requirements specifications and in this document a cost-effective architecture is presented. The document provides the description of the main functional blocks and the interfaces. In addition the document also provides the corresponding safety analysis.

Clarification/Disclaimer: The solutions described in this document are guideline specifications for the preparation of demonstrators of a GNSS based positioning system in Shift2Rail IP2 TD 2.4, which will then be lab and field tested. The results from these tests will then be used to further refine the architecture, as well as functional and interface definitions and in making choices where options currently exist. The results will then be provided as input to the ERA Change Control Management process, where they will be transformed into an interoperable, European standard

2 Table of Contents

3 Abbreviations, Acronyms and Definitions

Abbreviation, Acronyms and Definitions	Description
Absolute Position	Absolute position refers to a position that defines the train location unambiguously. For instance, an absolute position can be given by WGS84 coordinates but it can also be given by a track identifier and the travelled distance within a specific track.
Confidence Interval	It refers to a range of values so defined that there is a specified probability that the value of a parameter lies within it.
E_ODO_TS	Enhanced ODOmetry Track Side.
E_ODO_OB	Enhanced ODOmetry On-board.
ETCS-OB	European Train Control system - On-board
TF_PVT	Train's Front Position, Velocity and Timestamp
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
TCP	Transport Control Protocol
FTP	File Transfer Protocol
MD	Cold Movement Detector

4 Background

The present document constitutes the first issue of WP3's Deliverable D3.9 "Architecture Specification", which is part of the Stream 2 development agreed by the proposed amendment. The Deliverable D3.9 is part of the framework of the Project titled "Enhancing railway signalling systems based on train satellite positioning, on-board safe train integrity, formal methods approach and standard interfaces, enhancing traffic management system functions" (Project Acronym: X2Rail-2; Grant Agreement No 777465).

5 Objective / Aim

The X2Rail-2 D3.9 defines the architecture for a stand-alone fail-safe train positioning system. This document is using as an input the system requirement specification defined in [1].

Clarification/Disclaimer: The solutions described in this document are guideline specifications for the preparation of demonstrators of a GNSS based positioning system in Shift2Rail IP2 TD 2.4, which will then be lab and field-tested. The results from these tests will then be used to further refine the architecture, as well as functional and interface definitions and in making choices where options currently exist. The results will then be provided as input to the ERA Change Control Management process, where they will be transformed into an interoperable, European standard

6 General Description

6.1 Introduction

6.1.1 This document defines the architecture for a stand-alone fail-safe train positioning system as understood by X2RAIL2-WP3 stream 2. The document defines the functional blocks, interfaces and necessary technologies to meet the system requirements specification defined in [1].

6.1.2 Notice that the architecture from this document assumes that the aim for the presented work is to standardise the sensors and the environment to guarantee interoperability and leave out the fusion algorithm open to each member to develop it to its best, not forgetting that the system requirement specifications must be always fulfilled.

6.1.3 Note: By this statement, this architecture considers each sensor as a constituent for which a concrete specification, tests and environment definition are needed to guarantee full interoperability.

7 Architecture

7.1 Architecture Specification

7.1.1 The following Figure 7-1 shows the architecture for Stand-Alone Fail-Safe Train Positioning system represented by E_ODO. The system interfaces to two external entities: the trackside data manager and the ETCS On Board Unit (ETCS-OB). The E_ODO is comprised of two main subsystems: the track side enhanced odometry (E_ODO-TS) and the on-board enhanced odometry (E_ODO-OB).

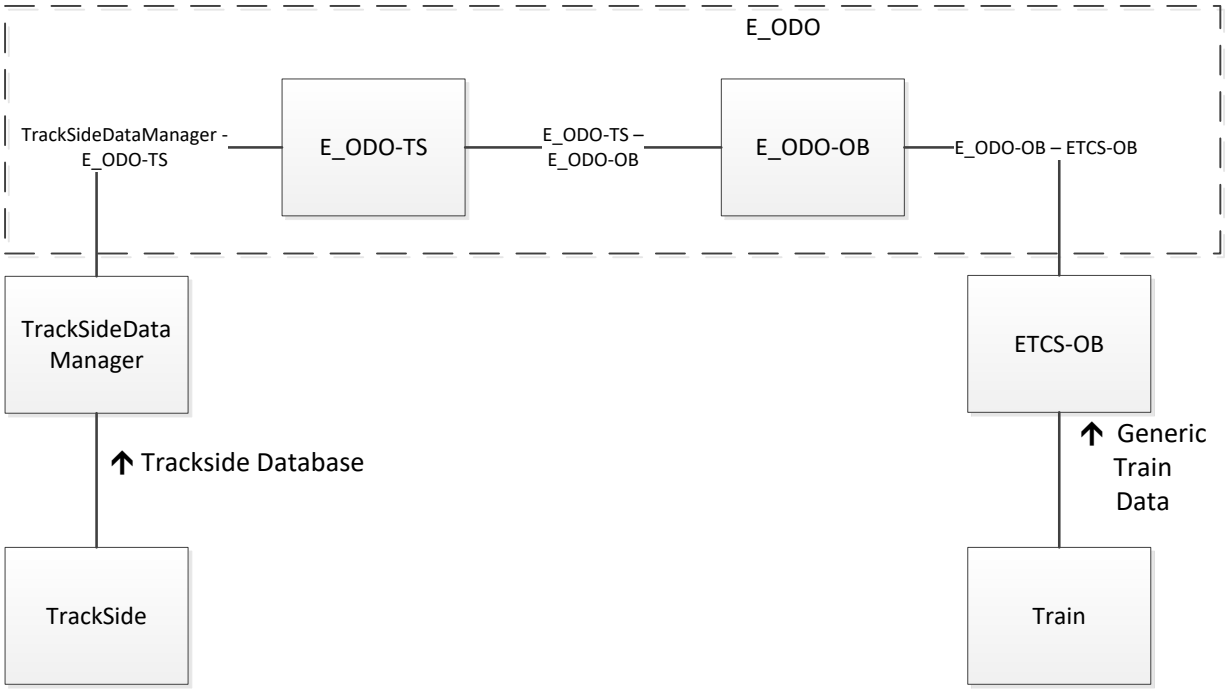

Figure 7-1 Architecture for Stand-Alone Fail Safe Train Positioning

7.1.2 E_ODO-OB subsystem is divided in the following functional blocks shown in Figure 7-2. For each sensor input, an interface is defined to the main “Safe Fusion Algorithm” (SFA). In addition, the SFA receives balise data, CMD data and other generic train data through the ETCS-OB interface. Finally, the SFA also receives the track data through the “Data Client Manager”. Ultimately, the SFA is the main functional block responsible to do the calculation of the train velocity and position. The reporting of the calculated position is handled by the “Position Reporting Manger” functional block.

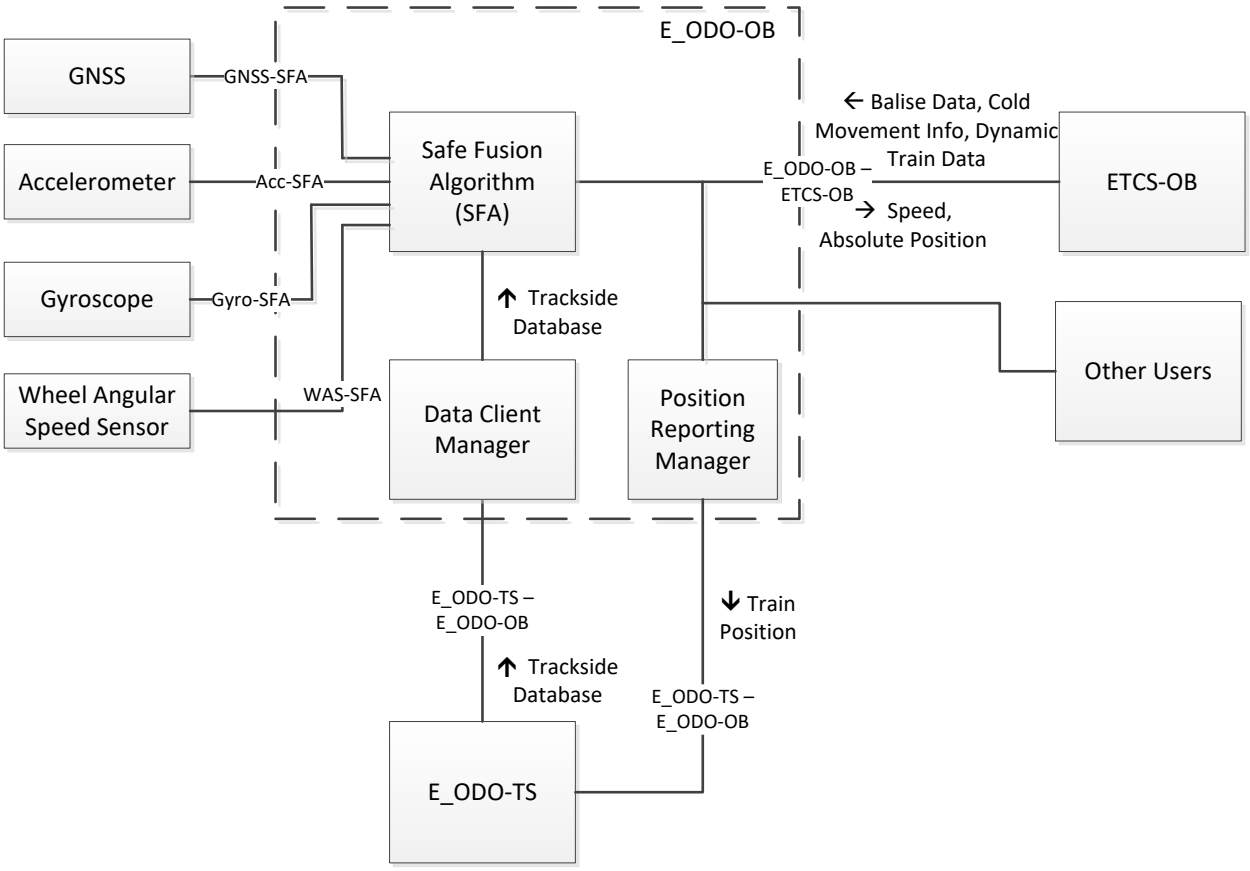

Figure 7-2 Architecture for E_ODO-OB

7.1.3 E_ODO-TS subsystem is divided into the following functional blocks shown in Figure 7-3. 'TrackSideData Connection Manager' is responsible to exchange the data between the TrackSideDataManager and the E_ODO-TS. 'Process Data' is responsible to process the data from the TrackSideDataManager and generate the required data for E_ODO-

OB. Finally, 'Data Server Manager' is responsible to handle the Server that offers the information to each E_ODO-OB client.

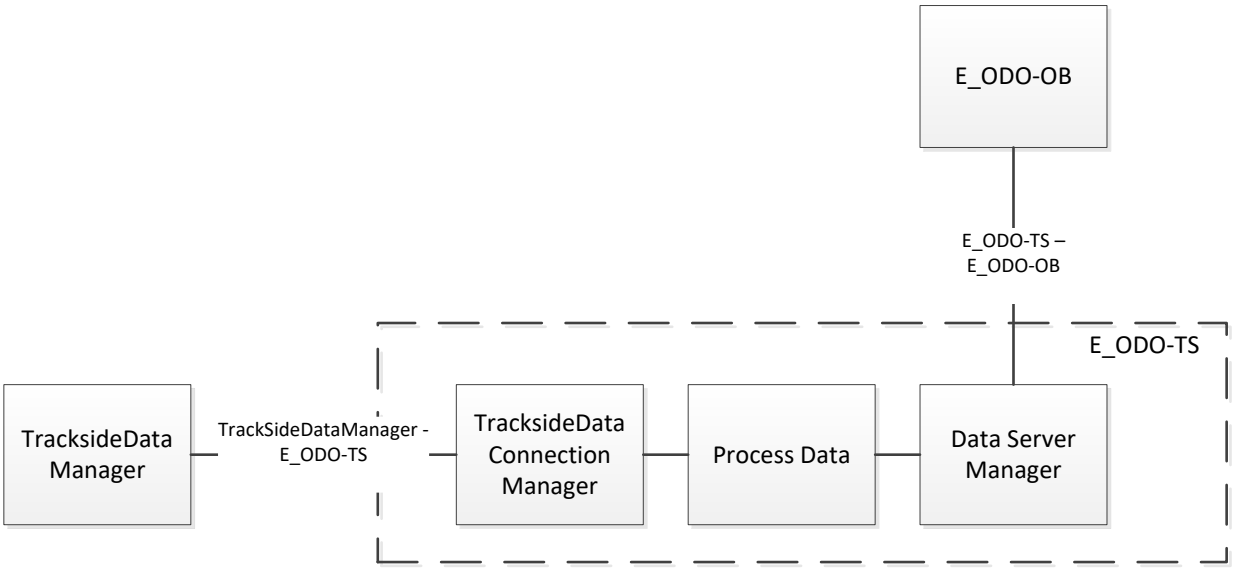

Figure 7-3 Architecture for E_ODO-TS

7.2 Enhanced Odometry On-board (E_ODO-OB)

7.2.1 General Functional Requirements

7.2.1.1 '*Safe Fusion Algorithm*' (SFA) function shall calculate the train's front absolute position, velocity and the time stamp (TF_PVT) fulfilling the requirements defined in **[1]** SRS 7.2.

7.2.1.2 SFA function shall use the following input information to compute the TF_PVT:

- Wheel's Angular Speed Based Longitudinal Speed (see 7.2.2.1 for further details)
- Accelerometers (see 7.2.2.2 for further details)
- Gyroscopes (see 7.2.2.3 for further details)
- GNSS data (see 7.2.2.4 for further details)
- Cold Movement Detector (see 7.2.2.5.1.1 for further details)
- Static Digital Map (see 7.2.2.6.1.1 for further details)
- Balise Identifier (see 7.2.2.5.1.2 for further details)
- Dynamic Train information (see 7.2.2.5.1.3 for further details)

7.2.1.3 SFA function shall calculate train's velocity and its confidence interval in scalar values that represent the train's longitudinal speed.

7.2.1.4 SFA function shall calculate train's position and its confidence interval that represents the absolute position of the front of the train.

7.2.1.5 The position and velocity parameters calculated by the SFA function shall provide the corresponding time stamp of these parameters.

7.2.1.6 The time stamp is defined as an internal time of the on-board unit. However, whenever possible the corresponding GNSS time stamp shall also be defined.

7.2.1.6.1 Note: There are cases when the train may know its position but has no GNSS signal. The typical scenario for that is the start-up of the train without GNSS signal where the CMD ensures the train has not moved and therefore the last stored train's position is valid.

7.2.1.7 SFA function shall be active since switch on.

7.2.1.8 SFA function shall store persistently and periodically its last calculated position with timestamp, the corresponding active reference cab and the train length to ensure the values are available at start up.

7.2.1.9 The SFA function shall detect whether the train has been moved or not when the train has been without power. This information shall be used at start-up to determine whether the stored last position, if any, is currently valid or not.

7.2.1.10 At start-up the SFA shall first check whether there is a position value stored or not. If such value exists, the system shall check whether it has been moved or not during power switch off. If the train has been moved the position is considered as invalid and if the train has not been moved, then the stored position is considered valid. If there is not a position value stored, then the train needs to calculate its position.

7.2.1.11 At start-up the SFA shall check with the "Data Client Manager" whether its stored static digital map information is up to date.

7.2.1.11.1 Note: the checks required to consider digital map up to date can either be by checking the expiration date or by performing a cross-check with E_ODO-TS.

7.2.1.12 "Data Client Manager" is responsible for maintaining up to date the static digital map and informing the SFA.

7.2.1.13 Once the train start-up is carried out (see 7.2.1.10) the SFA function shall calculate the TF_PVT values periodically at a minimum rate higher than the requirement specified in [1] SRS 7.2.1.1.9.

7.2.1.14 Optionally, the SFA shall report its position to trackside by using the “Position Report Manager”.

7.2.1.14.1 Note: The train position reporting could be defined either by setting up a configuration parameter for periodic reports and it could be also defined to be sent at specific positions defined in the digital map.

7.2.1.15 “Position Report Manager” may use the same communication channel between E_ODO_OB and E_ODO_TS as the one defined to obtain the static digital map.

7.2.2 Interface Requirements

7.2.2.1 WSA-SFA Interface

7.2.2.1.1 The WSA-SFA interface shall define a longitudinal train speed value based on wheel’s angular speed sensors.

7.2.2.1.2 Longitudinal train speed value shall be defined in meters per second.

7.2.2.1.3 Longitudinal train speed shall offer a confidence interval value transformed into meters per second.

7.2.2.1.4 Note: The wheel speed angular sensor calculates angular speed value and not linear speed. Thus, by using the corresponding radius of the wheelset the train longitudinal speed can be calculated. In addition, any algorithm used to detect wheel’s slip and slide

deviations is out of the specification but the correct value of the confidence interval shall guarantee that the provided value lies in between specified limits.

7.2.2.1.5 The minimum period between samples of the longitudinal speed shall be 10ms.

7.2.2.1.6 Note: Consider a maximum acceleration of 4m/s^2 read at a 10ms period then sensor is able to detect 0.04 m/s speed changes which is equivalent to 0.144 km/h, more than enough for a train.

7.2.2.2 Acc-SFA Interface

7.2.2.2.1 The Acc-SFA interface shall define acceleration values of the train.

7.2.2.2.2 Acceleration values shall be generated for all three axis of the coordinate reference system (see Appendix A Coordinate System).

7.2.2.2.3 Acceleration values shall be compensated with its calibration values, e.g. its offset, bias and misalignment between axes shall be corrected. Thus, the algorithm will assume that acceleration values are without these errors. However, the gravity term of the acceleration shall not be compensated, but be part of the vector components in the body frame and it shall be handled by the Safe Fusion Algorithm.

7.2.2.2.4 Acceleration values shall be filtered in order to reduce the effect of the train's vibrations on the measurements.

7.2.2.2.4.1. Note: A filter for the acceleration values is typically carried out to avoid vibration from other subsystems to be inserted in the data.

7.2.2.2.5 The minimum sampling rate for the accelerometers is 100Hz.

7.2.2.2.5.1. Note: the sampling rate defined here corresponds to the periodicity at which the data needs to be read after filtering and compensation is applied. Consider a digital accelerometer where the data can be sampled at high frequency but only it is read by the application every 100Hz. If this is the case, with an assumption of 2g maximum forces the speed increment from read sample to sample is 0.194m/s, which is better than the

speed error margin confidence interval defined in [1] ([2km/h-12km/h] ≈ [0.55m/s-3.3m/s]) and it still leaves room for accumulative errors in the acceleration data.

7.2.2.3 Gyro-SFA Interface

7.2.2.3.1 The Gyro-SFA interface shall define rotation speed values of the train

7.2.2.3.2 There shall be three gyroscopes one per axis of the coordinate reference system (see Appendix A Coordinate System).

7.2.2.3.3 Gyroscope values shall be compensated with its calibration values, i.e. its bias shall not be considered by the Safe Fusion algorithm.

7.2.2.3.4 Gyroscope values shall be filtered ensuring that no other vibration that the ones corresponding to the train's physical movement are integrated within read data.

7.2.2.3.4.1. Note: A filter for the gyroscope values is typically carried out to avoid vibration from other subsystems to be inserted in the data. The aim here is that at design phase to be aware of ensuring the used data is filtered.

7.2.2.3.5 The minimum sampling rate for the gyroscopes is 100Hz.

7.2.2.3.5.1. Note: the sampling rate defined here corresponds at the level of filtering and compensation of the data. It is expected that the true sampling frequency of the Gyroscope values to be at a 200Hz which by Nyquist law provides to the user a valuable 100Hz bandwidth of usable data. With 100Hz data sampling the aim is not to lose a turn of the train due to a slow sampling rate. Therefore, consider the worst case scenario with a very tight curve, for instance 20m radius turn, at a maximum speed of 20km/h (5.55 m/s), the overall turn rate outcome is ((5.55*180)/(Pi*20)) ≈62.83º/s. Using a 100Hz sample rate the system is able to detect 0.6283º at a 10ms period which is considered enough to track train motion (e.g. heading change).

7.2.2.3.6 Note: Notice that the critical aspect for a Gyroscope is its sensitivity to detect rotation angles at a very slow speed in a very large radius curvature. Though, this parameter, if defined, it is considered part of the following task that defines the fusion algorithm minimum performance requirements.

7.2.2.4 GNSS-SFA Interface

7.2.2.4.1 GNSS-SFA interface shall read the following information:

- Observation data of each satellite. Such measurements include Pseudo Ranges, Carrier Phase measurement, Doppler measurements and Carrier to Noise Ratio (see [4] Observation code data example).
- Navigation Message. (see [4] Navigation Message Files data).

7.2.2.4.1.1. Note: The objective of this requirement is to clarify that the GNSS data to be used is the raw data coming from a receiver.

7.2.2.4.2 GNSS Data shall consider dual-frequency dual constellation information (GPS and Galileo).

7.2.2.4.3 GNSS Data shall consider the information coming from EGNOS Augmentation system as part of the information to calculate the train position.

7.2.2.4.4 EGNOS Augmentation data is received by the receiver itself and it is not considered the case of receiving from other sources.

7.2.2.4.4.1. Note: The 'Safe Fusion Algorithm' will have to cope with this limitation of EGNOS.

7.2.2.4.5 Minimum sampling rate of GNSS data is 1Hz.

7.2.2.5 E_ODO-OB-ETCS-OB interface

7.2.2.5.1 E_ODO_OB-ETCS-OB Interface inputs

7.2.2.5.1.1. Cold Movement Detector (CMD)

7.2.2.5.1.1.1. CMD data defines whether the train engine has been moved or not during a period of 72 hours after the train has been switched off.

7.2.2.5.1.1.1.1. Note, the CMD may be implemented in the same hardware the wheel speed sensor is mounted and thus the corresponding CMD functionality may also be integrated.

7.2.2.5.1.2. Balise Information

7.2.2.5.1.2.1. Whenever a balise is read, the E_ODO_OB shall obtain the time stamp and the balise id information.

7.2.2.5.1.2.1.1. Note: By obtaining the read balise id, E_ODO_OB can use its static digital map to unambiguously identify the track where the train is at that moment. This information is important as it ensures track discrimination.

7.2.2.5.1.3. Dynamic Train information

7.2.2.5.1.3.1. Dynamic train information is required to ensure that the travelled distance sign and speed calculated by the E_ODO_OB are correct with respect to the active cab. For this purpose E_ODO_OB shall read the following dynamic train information:

- **Cab status**: it is defined as a two state input that defines whether the cab is active or not either in the current train unit or any other train coupled.
- **Active Cab**: it is defined as three state input that defines whether Cab A is active, Cab B is active or none is active.
- **Train Length**: the train length corresponding to the current train composition.

7.2.2.5.1.3.2. In addition, the following optional information may be required for functional purposes:

- **Train is switching off**: it is defined a Boolean input that defines that the train is going to switch off.

7.2.2.5.2 E_ODO_OB-ETCS-OB Interface Outputs

7.2.2.5.2.1. Speed Output Information

7.2.2.5.2.1.1. Speed information is referred to the longitudinal axis speed of the train where positive values represent train's movement in reference to the active cab or reference cab.

7.2.2.5.2.1.2. Note: The active cab and the reference cab are concepts described in *Appendix B Train Sense*, where the meaning and differences between these concepts are described.

7.2.2.5.2.1.3. The speed information and its confidence interval shall be provided in SI units, i.e. meters per second.

7.2.2.5.2.1.4. The confidence interval defined for speed value shall be defined as a twofold parameter:

- Upper Bound speed confidence interval: speed interval greater from the provided speed value.
- Lower Bound speed confidence interval: speed interval lower from the provided speed value.

7.2.2.5.2.2. Absolute Position Output Information

7.2.2.5.2.2.1. Train's absolute position is defined in two possible formats described hereafter. The reason behind such distinction is that the train only moves forward and backward and thus, if the position of the train is already known, the positioning becomes simpler. Though, it is foreseen that there will be cases where it is not possible to locate the train guaranteeing track discrimination, for instance at start up with multiple parallel lines. For those cases the train shall be able to provide as much as information as possible to any other subsystem. The two possible formats are described below:

7.2.2.5.2.2.1.1. Absolute train position based on a reference

7.2.2.5.2.2.1.1.1. The absolute position shall be referred to a fixed reference of the static digital map, if and only if the fusion algorithm has been able to calculate train's position within the map unambiguously, including track discrimination. This formatting requires the following information:

- Unique identifier of reference to the fixed point of the digital map.
- Travelled distance since the fixed node of the digital map with a resolution down to centimetres if only the unique identifier of the node is known.

7.2.2.5.2.2.1.2. The confidence interval referred to this formatting shall be an absolute scalar value with a resolution down to centimetres that defines the bounding of the train position forwards and backwards.

7.2.2.5.2.2.1.3. Note: The is an illustration that defines the case scenario where the train is positioned unambiguously in the map and it has run a D_Trav_Dist distance from the beginning of a Segment, which is the common node for track and on-board

(refer to 7.2.2.5.1.1 for further details on segment), with a given Confidence Interval value.

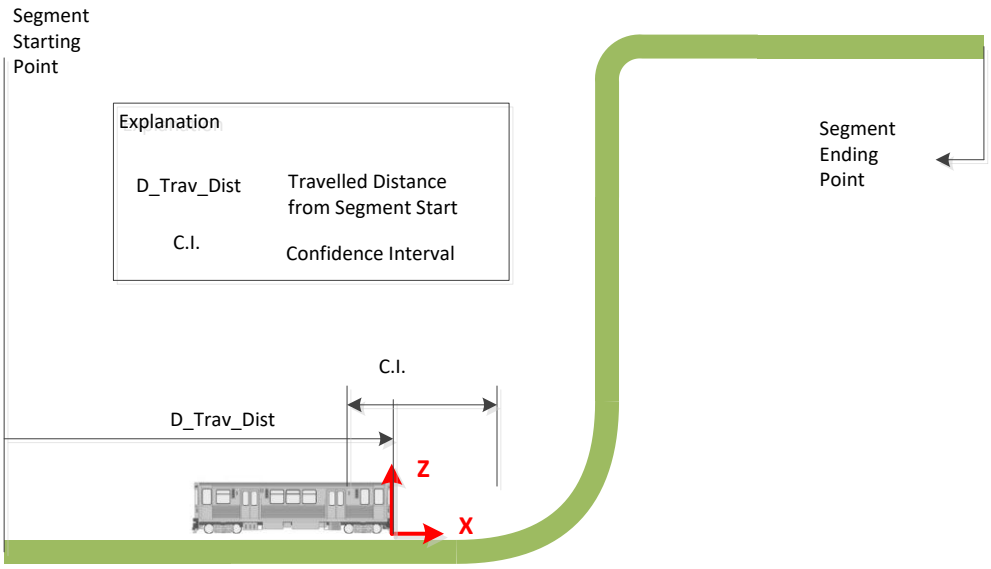

Figure 7-4 Absolute distance referenced to segment start.

7.2.2.5.2.2.2. Absolute train position without a reference

7.2.2.5.2.2.2.1. Absolute train position without a node shall be defined by the Latitude and Longitude value of the train position using WGS84 geodetic ellipsoid to ease compatibility with GNSS usage. This formatting requires the following information:

- Latitude value in radians
- Longitude value in radians

7.2.2.5.2.2.2.2. The resolution of the absolute position parameters should have 9 decimals.

7.2.2.5.2.2.2.2.1. Note: The earth radious is 6378137.0m, the hall circumference is 40075016.68557m, so 111319.49 m/grades. To reach 10cm precision, 0.0000001

grades are needed. Converted to radians, 9 decimals should be used to represent latitude and longitude values.

7.2.2.5.2.2.2.3. The confidence interval for an absolute position shall be given by the radius of a circle in centimetres that bounds the worst case scenario.

7.2.2.5.2.2.2.4. Note: The following diagram is an illustration that defines the case scenario where the train is positioned without a digital map (refer to 7.2.2.5.1.1 for further details on segment) with a given Confidence Interval value.

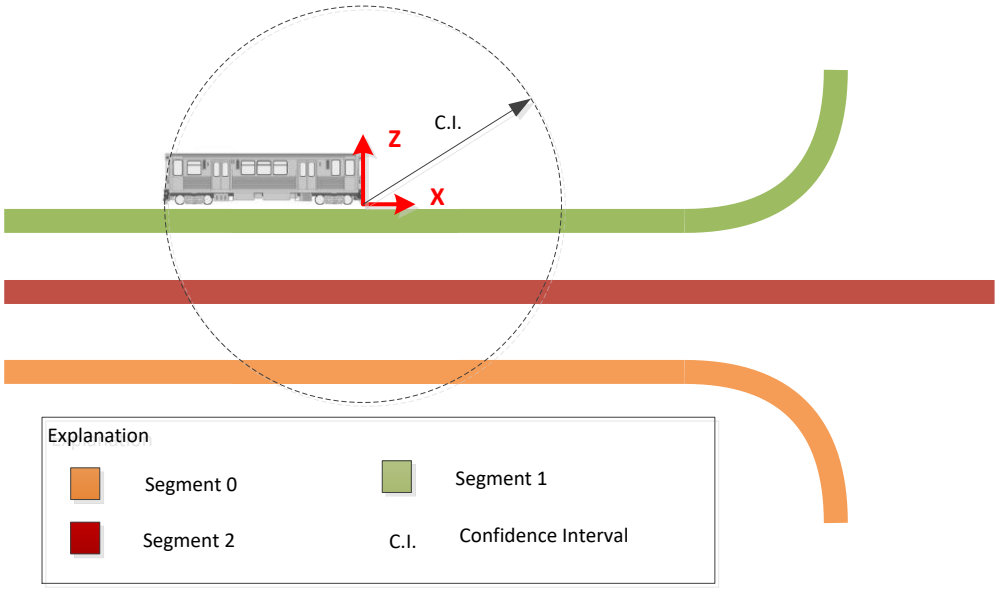

Figure 7-5 Absolute distance without a reference.

7.2.2.5.2.2.2.5. Notice that the absolute position without a node could be always published regardless of knowing a node or not. However, in the previous case scenario, shown in , it is the obvious scenario where there is a clear need for such information.

7.2.2.6 E_ODO-TS-E_ODO-OB Interface

7.2.2.6.1 E_ODO_TS-E_ODO-OB Interface Inputs

7.2.2.6.1.1. The E_ODO-TS shall provide a static digital map.

7.2.2.6.1.2. Static digital Map is defined as the data that represents the topography of the railway track. The topography of a railway track shall be represented by the following information at any point of the digital map:

- Absolute position in terms of **latitude** and **longitude** based on a given ellipsoid reference, for instance WGS84.
  - Note: This information also represents implicitly a segment id and a position from the beginning of this segment. (See for further information)
- **Height** value from a given ellipsoid reference, for instance WGS84.
- **Orientation** value, for instance with respect to true North.
- **Cant** value or deficiency, it represent the roll angle of the railway as defined in (Appendix A Coordinate System)
- **Curvature** value. In the special case of a straight line the curvature value shall be represented by a special valuefor “infinite”.
- **Balise** information

7.2.2.6.1.2.1. Note: The rationale to have absolute positioning in the digital map is to ensure that any reported value of the E_ODO-OB can be referenced to the map instead of the GNSS data only. It is therefore the duty of the E_ODO-OB to project its position to the right track but the position itself is a value guaranteed by the map. The height and the cant value are considered required information because they facilitate the removal of the gravity effect in the measurement of acceleration values. The height related to travelled distance could also solve the problem on different railway tracks crossing each other on different levels in height scenarios. The orientation information along with the curvature value is considered required information because both GNSS and IMU sensors can compute map matching techniques by making use of such information. Finally, the balise information, when identified in the map, can provide track discrimination unambiguously.

7.2.2.6.1.2.2. Note 2: Orientation value can be obtained from latitude/longitude as long as you have many of them. However, if the map is discretized to avoid large size files, the orientation as individual information becomes necessary.

7.2.2.6.1.3. Static digital map shall represent its information with regards to static reference points called “nodes” in the railways, which are virtual points of the railway run.

7.2.2.6.1.3.1. Note: Next is a representation of the Static Digital Map. The information provided by static digital map, when referenced to nodes, divides the railway in sections, named hereafter as segments. Thus, the start of the segment becomes the node in this example. When the train is located on a segment, the digital map can provide its instantaneous

information according to the stored data. For instance when the train is a D_Travel_Dist from Node 1 the static digital map information shall be able to provide all the information defined in 7.2.2.6.1.2. Notice that for this example the segment is never bidirectional and for the cases where there is a 2-way segment two different segments shall be represented.

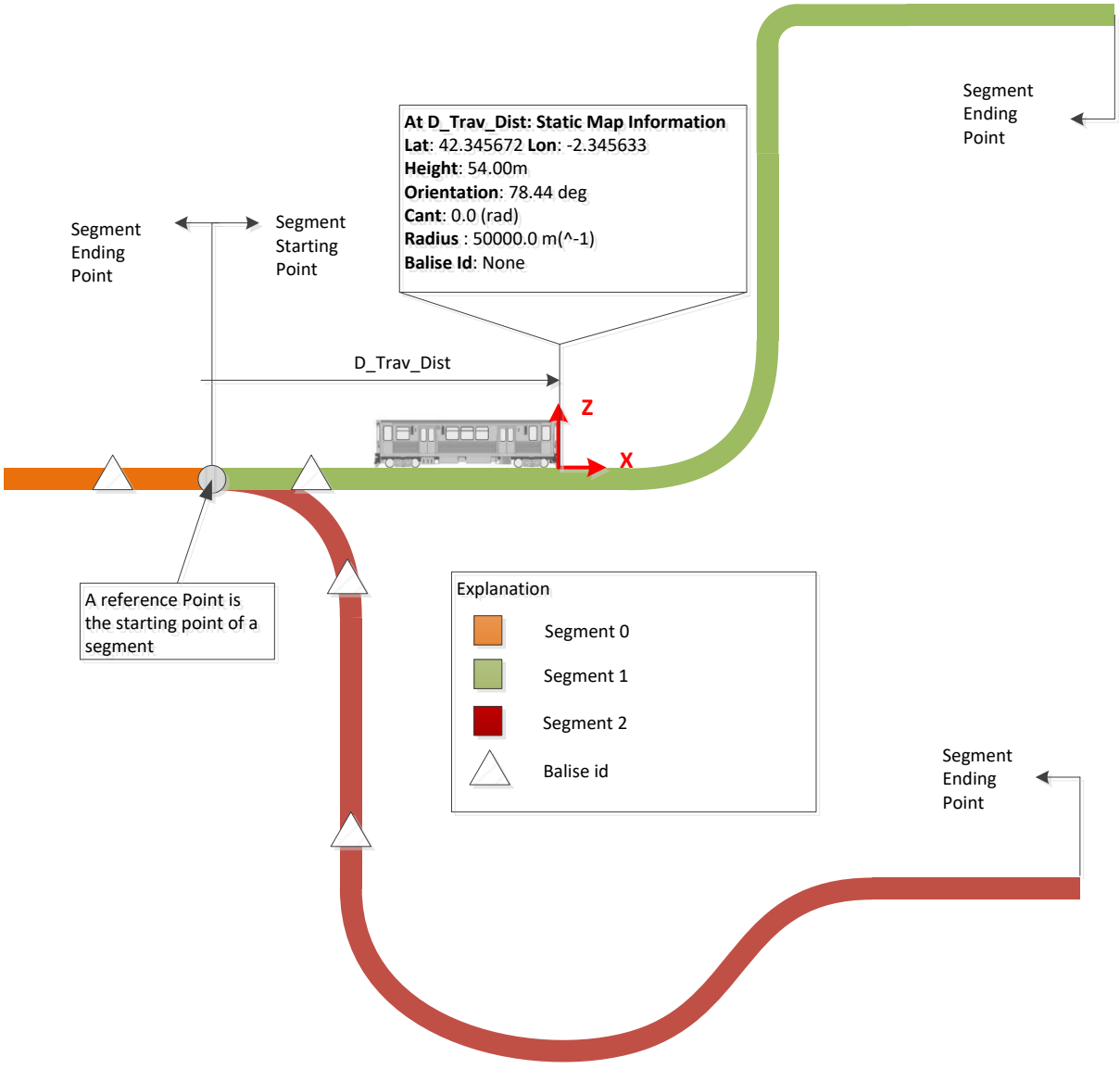

Figure 7-6 Static digital Map

7.2.2.6.1.4. In order to guarantee the correct use of the digital map, an exported constraint that ensures there are not switch points between nodes must be fulfilled.

7.2.2.6.1.4.1. Note: if there is a switch point then the information for the static digital map cannot be unambiguously represented. Consider the example of segment one and two were a unique segment, then D_travel_dist would not define a unique point in the map.

7.2.2.6.2 E_ODO_TS-E_ODO-OB Interface Outputs

7.2.2.6.2.1. The E_ODO-OB optionally can provide a position report to track side.

7.2.2.6.2.2. The E_ODO-OB position report shall contain the same information as defined in 7.2.2.5.2.

7.3 Enhanced Odometry Track Side (E_ODO-TS)

7.3.1 General Functional Requirements

7.3.1.1 E_ODO-TS's "Track Side Data Connection Manager" shall maintain up to date the static digital map as defined by track side.

7.3.1.1.1 Notice that it is assumed that the corresponding checks to guarantee a safe static digital map are out of the scope of E_ODO-TS.

7.3.1.2 E_ODO-TS's "Process Data" shall read the static digital map from "TrackSideData Connection Manager" and it shall convert it to the appropriate formatting.

7.3.1.3 E_ODO-TS's "Process Data" shall offer the possibility to manage positions reports from a E_ODO-OB

7.3.1.4 E_ODO-TS's "Data Server Manager" shall offer an external connection capability with a secured File Transfer Protocol (FTP).

7.3.1.4.1 Note: FTP protocol is based on a Transport Control Protocol (TCP) as a transport protocol and an IP based network layer. FTP uses two TCP connections one for control of connection and another to exchange the files. The purpose of this requirement is to

set the minimum requirements to design a safe communication channel to ensure the data can be exchanged in a safe and efficient manner.

7.3.1.5 E_ODO-TS's "Data Server Manager" and E_ODO-OB shall communicate over a safe radio communication link.

7.3.1.6 When an E_ODO-OB starts up it shall set up a safe connection with the E_ODO-TS. Once the connection is set up, E_ODO-OB shall download the summary information of the static digital map stored at the E_ODO-TS. E_ODO-OB is responsible to cross check its internal summary information with the downloaded one. If any of the local files is out of date E_ODO-OB shall download the corresponding file from E_ODO-TS.

7.3.1.6.1 Note: the area covered by each E_ODO-TS and how are different E_ODO_TS synchronised it is not part of this specification.

7.3.1.7 Additionally, once the safe connection between E_ODO-OB and E_ODO-TS is established, optionally a position report can be sent from E_ODO_OB to E_ODO_TS.

7.3.1.8 Note: The periodicity of the position report is out of the scope of this document.

7.3.2 Interface Requirements

7.3.2.1 E_ODO-TS-E_ODO_OB Interface

7.3.2.1.1 See 7.2.2.6 for specification

7.3.2.2 TrackSideDataManager-E_ODO-TS- Interface

7.3.2.2.1 E_ODO-TS and TrackSideDataManager shall exchange static digital map information and ensure that E_ODO_TS is updated on a daily basis from the TrackSideDataManager.

7.3.2.2.1.1. Note: It is assumed that track data cannot be prepared for the train in advance in lower than one day basis. However, even if the current specification targets for a daily basis update of the data, this process could be configurable depending on the protocol defined between TrackSideDataManager and E_ODO_TS.

8 Safety

8.1.1.1.1

8.2 Function Definitions

8.2.1 The following safety functions are considered based on the descriptions from section 7.

8.2.2 E_ODO-OB Functions

8.2.2.1 The following sets of functions are based on Figure 7-2.

8.2.2.2 [E_ODO-OB/F1]: Function to manage the safe communication with E_ODO-TS

8.2.2.3 [E_ODO-OB/F2]: 'Safe Fusion Algorithm' function to calculate position and velocity, including track discrimination.

8.2.2.4 [E_ODO-OB/F3]: Function to read wheel's angular speed based longitudinal speed.

8.2.2.5 [E_ODO-OB/F4]: Function to read accelerometers data.

8.2.2.6 [E_ODO-OB/F5]: Function to read gyroscopes data.

8.2.2.7 [E_ODO-OB/F6]: Function to read GNSS data.

8.2.2.8 [E_ODO-OB/F7]: Function to retrieve Static Digital Map from the server.

8.2.2.9 [E_ODO-OB/F8]: Function to read the downloaded static digital map.

8.2.2.10 [E_ODO-OB/F9]: Function to read the balise identifier information.

8.2.2.11 [E_ODO-OB/F10]: Function to read the cab status information.

8.2.2.12 [E_ODO-OB/F11]: Function to read the train is switching off.

8.2.2.13 [E_ODO-OB/F12]: Function to write the calculated position to ETCS-OB.

8.2.2.14 [E_ODO-OB/F13]: Function to write the calculated velocity to ETCS-OB.

8.2.2.15 [E_ODO-OB/F14]: Function to read the train length information.

8.2.3 E_ODO-TS Functions

8.2.3.1 The following set of functions are based on Figure 7-3.

8.2.3.2 [E_ODO-TS/F1]: Function to manage the connection to TrackSideDataManager

8.2.3.3 [E_ODO-TS/F2]: Process Data Function to maintain up to date the static digital map.

8.2.3.4 [E_ODO-TS/F3]: Data Server Manager function to manage the safe communication with E_ODO-OB

8.3 SIL per Function

8.3.1 The following table summarises the expected Safety Integrity Level associated to each function, as a conclusion from the more detailed Safety analysis shown in Appendix 12. Notice that although the FMECA provides some of the arguments that justify the SIL levels detailed here, this is still a proposal from top-down approach. Whenever the final algorithm is described these values may change:

Ref.	SIL
E_ODO-OB/F1	SIL4
E_ODO-OB/F2	SIL4
E_ODO-OB/F3	SIL4
E_ODO-OB/F4	SIL4
E_ODO-OB/F5	SIL4
E_ODO-OB/F6	SIL4
E_ODO-OB/F7	SIL0
E_ODO-OB/F8	SIL4
E_ODO-OB/F9	SIL4
E_ODO-OB/F10	SIL0
E_ODO-OB/F11	SIL4
E_ODO-OB/F12	SIL0
E_ODO-OB/F13	SIL4

E_ODO-OB/F14	SIL4
E_ODO-TS/F1	SIL4
E_ODO-TS/F2	SIL4
E_ODO-TS/F3	SIL4

Table 8-1 Functions SIL level

9 References

[1] X2R2-TSK3.9-D-CAI-001-06 - System Requirement Specification for Stand-Alone Fail Safe Train Positioning, Version 06

[2] ERA, Report ERTMS Longer Term Perspective, 18/12/2015.

[3] STARS project. D5.1 - State of the art of EGNSS projects for the rail application, STR-WP5-D-IFS-033 (IFSTTAR – 21/03/17).

[4] Rinex 304 Standard

[5] EN 50126:2017 - Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

10 Appendix A Coordinate System

Coordinate reference system for stand alone fail safe train positioning is shown in the next Figure 10-1. The coordinate system reference location is at the active cabin's side, grounded to top of rail and centered with respect to train's transversal axis. Considering this coordinate system, it can be seen that the longitudinal axis refer to 'X' axis, transversal axis refer to 'Y' axis and vertical axis refer to 'Z' axis.

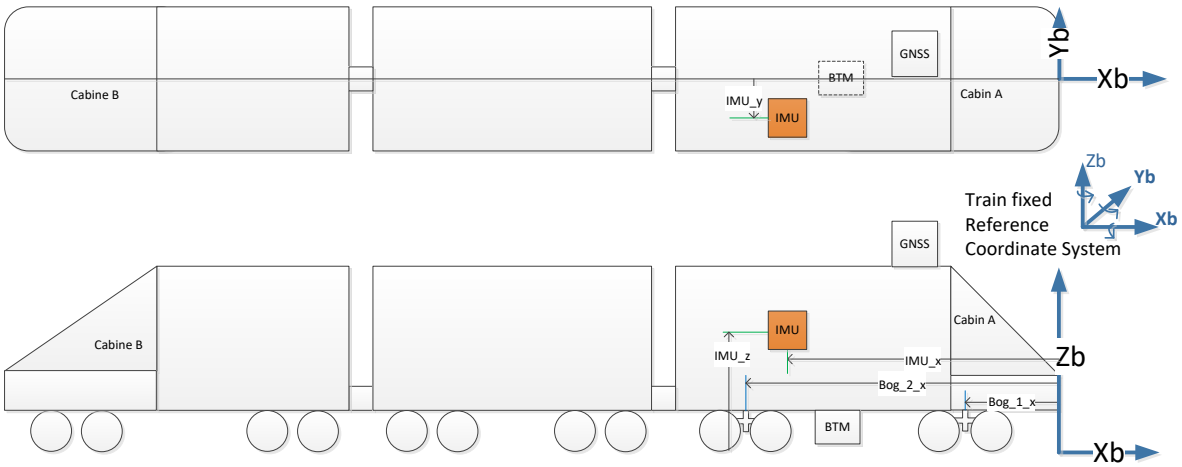

Figure 10-1 Train Coordinate System

In addition to the reference coordinate system the definition of the Euler angles is also defined here after. Fist the Roll angle is depicted in Figure 10-2 where the symbol Φ (phi) is used to represent the corresponding angle. Similarly, Figure 10-3 and Figure 10-4 illustrate the Pitch angle by using θ(theta) angle and the Yaw angle by using Ψ(psi) respectively.

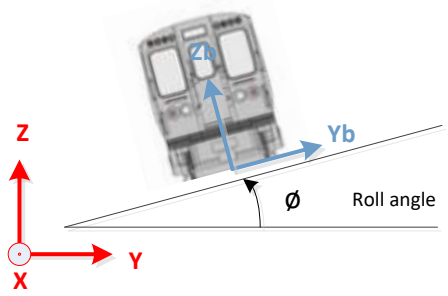

Figure 10-2 Roll Angle illustration

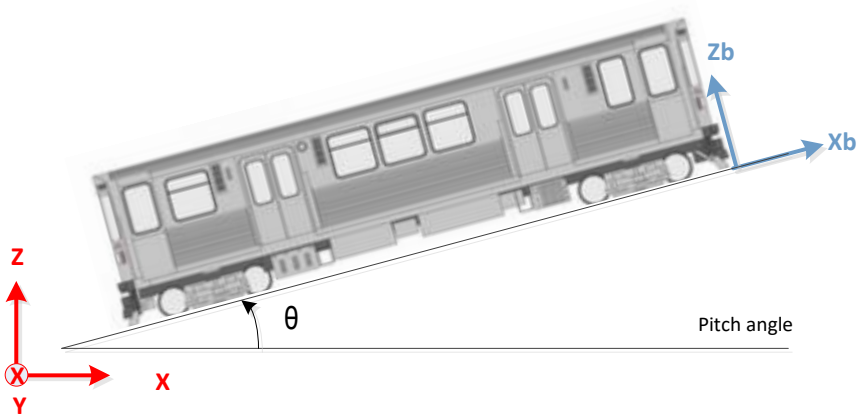

Figure 10-3 Pitch Angle illustration

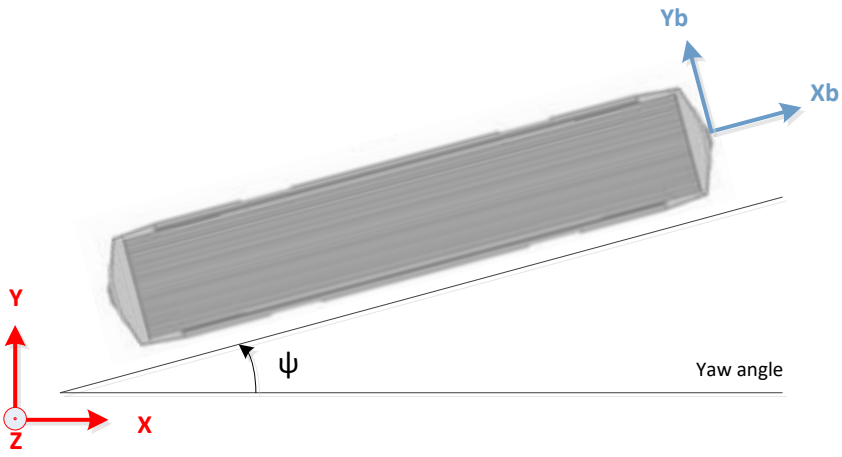

Figure 10-4 Yaw Angle illustration, top view

11 Appendix B Train Sense

In a multiple unit scenario the fail-safe train positioning system shall be executed in both the leading unit and the non- leading / sleeping train unit. This implies that for the non- leading / sleeping unit there must be a deterministic manner to determine the train orientation. Current trains, in their inauguration process are available to determine whether the train unit is oriented in favour of the active cab or opposite to the active cab. Therefore these two cases illustrate the logic to be determined by the stand alone fail safe train positioning to identify the reference cab. In Figure 11-1 two train units are illustrated. On one hand the active train unit has a reference cab determined by the active cab, which is Cab A. On the other hand, the non- leading train unit needs to know the train unit orientation with respect to the active train unit. In this case the train orientation is positive and hence the Cab A is the reference cab. The opposite case is illustrated in Figure 11-2 where the case of the active train unit does not change but in the case of the non-active train unit the train orientation is negative. As a consequence in this latter illustration the reference cab is Cab B.

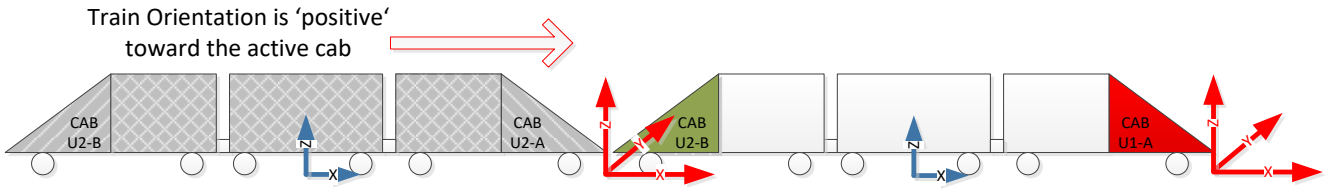

Figure 11-1 Multiple Train Unit where in the active Train unit, the reference cab is Active Cab A and in the non-active train unit, the reference cab is Cab A.

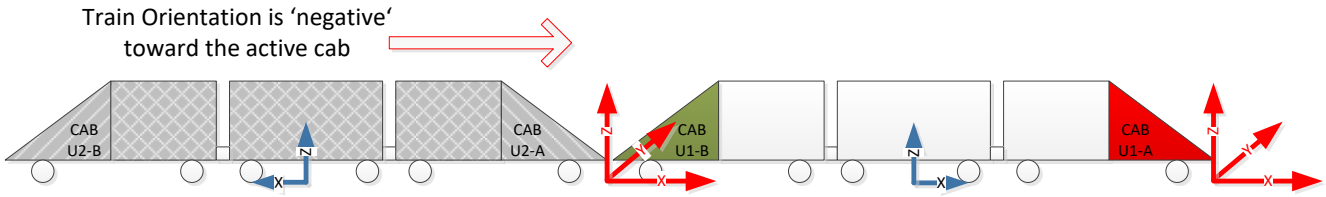

Figure 11-2 Multiple Train Unit where in the leading Train unit, the reference cabine is Active Cab A and in the non- leading / sleeping train unit, the reference cabine is Cab B.

12 Appendix C Safety analysis

Fail safe train positioning system description is defined in 7.1. Main blocks of the odometry system are defined according to the description in Figure 7-1 . Responsibilities of these blocks are defined in chapter 7, interfaces between blocks are defined in section 7.2.2 and section 7.3.2, where the main functions for the blocks of E_ODO_OB and E_ODO_TS are defined in section 8.2. Those functions can be classified as follows:

Functions to read:

- [E_ODO-OB/F3]-[E_ODO-OB/F11]

Functions to write:

- E_ODO-OB/F12
- E_ODO-OB/F13

Functions to interface

- E_ODO-OB/F1

Function to calculate

- E_ODO-OB/F2

Assumptions for the safety analysis are:

- TrackSideDataManager safety analysis is out scope of this document
- How the exchange information between E_ODO-OB and ETCS-OB, and E_ODO-TS and TrackSideDataManager is out of this analysis
- How the fusion algorithms are performed is out of this analysis.
    - Note, the design of the appropriate fusion algorithm is carried out in future tasks.
- It is assumed that input data listed in Figure 7-2 for the TF_PVT calculation are mandatory
    - Note: in the design phase, different situations depending on the availability of input will be analysed.

12.1 Methodology of Risk evaluation and Hazard identification

12.1.1 Hazard Identification

For the hazard identification, the FMECA technique is used. The approach used for accomplishing the FMECA is the functional approach. For each function identified in 8.2, possible failure modes are analysed. For the analysis, each single item failure is to be considered the only failure in the system.

12.1.2 Failure Modes

This section lists the failure modes applicable sequentially to each element defined in 8.2. Typical failure modes include:[1]

- failure to perform the function;
- incorrect performance of output function;
- incorrect timing of output function;

Note: an example of a generic function to read a data is defined in the next figure:

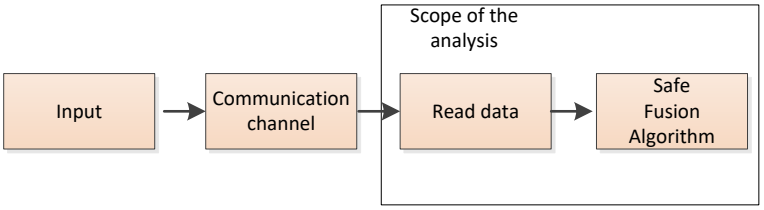

Figure 3: Scope of analysis in a generic function

12.1.3 Failure Causes

For each failure mode, all probable failure causes will be identified and described.

12.1.4 Failure Effects

Three possible failure effects will be identified:

Local: Local effects concentrate specifically on the impact the assumed failure mode has on the operation and function of the *item under consideration*. The local effect can be the failure mode itself;

Intermediate: Intermediate effects will define the impact that the assumed failure mode has on the *other module or functions*;

Initial End Effect: End Effect will define the total effect the assumed single macro function failure has on the *operation, function or status of the system*.

12.1.5 Risk evaluation without mitigations

A severity classification is assigned to each failure mode according to the failure consequences. An example of Severity categories is defined in EN 50126 Standard (Ref. [5][5]) and is reported in the Table 12-1:

Severity Level	Consequence to Persons or Environment

[1] Communication channel is out of scope of this analysis

Catastrophic	• Affecting a large number of people and resulting in multiple fatalities, and/or • Extreme damage to the environment
Critical	• Affecting a very small number of people and resulting in at least one fatality, and/or • large damage to the environment
Marginal	• No possibility of fatality, severe or minor injuries only, and/or • minor damage to the environment
Insignificant	• Possible minor injury

Table 12-1: Severity Level (EN 50126)

For each failure mode a frequency of occurrence is evaluated. An example of Frequencies of occurrence is defined in EN 50126 Standard (Ref. [5]) and is reported in the Table 12-2:

Category	**Description**
Frequent	Likely to occur frequently. The event will be frequently experienced
Probable	Will occur several times. The event can be expected to occur often
Occasional	Likely to occur several times. The event can be expected to occur several times
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.

Table 12-2: Frequency of Occurrence

A first qualitative risk estimation is performed by combining the frequency of occurrence of a hazardous event with the severity of its consequences. To establish the risk level generated by the hazardous event, the categories defined in EN 50126 Standard (Ref.[5]) are used and are reported in the table below:

Risk Acceptance Category	Action to be applied
Intolerable	The risk shall be eliminated
Undesirable	The risk shall only be accepted if its reduction is impracticable and with the agreement of the railway duty holders or the responsible Safety Regulatory Authority
Tolerable	The risk can be tolerated and accepted with adequate control (e.g. maintenance procedures or rules) and with the agreement of the responsible railway duty holders
Negligible	The risk is acceptable without the agreement of the railway duty holders.

Table 12-3: Risks Acceptance Categories

The following matrix, defined in EN 50126 (Ref.[5]), identifies an example of risk evaluation and acceptance:

	Insignificant	Marginal	Critical	Catastrophic
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable

Table 12-4: Risk evaluation and acceptance

12.1.6 Mitigations Identification

In this step of the analysis, all possible measures to protect or to mitigate against the effect of the failure shall be identified. Such measures could be for example requirements to be implemented by the Fail Safe Train Positioning or operation rules/actions.

12.1.7 Risk evaluation with mitigations

Risk evaluation considering all the mitigations identified.

12.1.8 FMECA Worksheet

The FMECA worksheet includes the following fields

1. **Function ID**: function identification as reported in 12;
2. **Function Name**: name of the function as reported in 12;
3. **Failure Modes**: This field specifies the failure modes applied (see 12);
4. **Failure Effects**: local, intermediate and end possible effects
5. **Impact**: This field specifies what the type of the end impact is. Possible values:
    - Safety issue, or
    - RAM issue, or
    - No effect;
6. **Hazard ID**: This field reports the hazard ID in the form of "*HZ_XXX*" where XXX is a progressive number;
7. **Risk evaluation without mitigation** (frequency/severity/risk classification): first qualitative risk evaluation without considering any mitigation. The risk evaluation is performed only if the "Impact" field specifies an impact on the safety of the system;
8. **Mitigations**: This field lists the mitigations identified to mitigate the hazard in the form of "*MIT_XXX*" where XXX is a progressive number of three digits.
9. **Risk evaluation with mitigation** (frequency/severity/risk classification): final qualitative risk evaluation considering all the mitigations identified;
10. **Comments**

12.2 Hazard analysis

12.2.1 Functions to read (F3-F11 and F14)

This group of functions are the responsibility to read an input. The input could be a sensor, a register or a status. Failure modes of these functions are similar but the effects can be different with respect to the safety side.

12.2.1.1 F3. Function to read wheel's angular speed based longitudinal speed.

This function is the responsible to read the wheel´s angular speed. E_ODO-OB block shall ensure the correctness of reading of the data.

Hazard scenario 1: E_ODO-OB read a wrong signal/data

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

Hazard scenario 2: E_ODO-OB read a delayed signal/data

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

12.2.1.2 F4. Function to read accelerometer data.

This function is the responsible to read the accelerometer data. E_ODO-OB block shall ensure the correctness of reading of the data.

Hazard scenario 1: E_ODO-OB read a wrong data/signal

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

Hazard scenario 2: E_ODO-OB read a delayed signal/data

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

12.2.1.3 F5. Function to read gyroscope data.

This function is the responsible to read the gyroscope data. E_ODO-OB block shall ensure the correctness of reading of the data.

Hazard scenarios and mitigation are the same as the previous section.

12.2.1.4 F6. Function to read GNSS data.

This function is the responsible to read the GNSS data. E_ODO-OB block shall ensure the correctness of reading of the data.

Hazard scenario 1: E_ODO-OB read a wrong data/signal

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall implement check of the data with other type of sensors integrated in the system.

- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

Hazard scenario 2: E_ODO-OB read a delayed data/signal

- E_ODO-OB shall implement check of the data with other type of sensors integrated in the system.

12.2.1.5 F7/F8. Function to retrieve Digital Map from the server/ Function to read the downloaded static Digital Map

This function is the responsible to read or retrieve the static digital map data. E_ODO-OB block shall ensure the correctness of reading of the data.

Hazard scenario 1: E_ODO-OB stores a wrong data of digital map

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB HW shall implement protections against random errors of the data stored according EN 50129.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.
- Digital map shall be protected to ensure its data integrity (for example using a CRC)

Hazard scenario 2: E_ODO-OB does not update the digital map.

- E_ODO-OB shall ensure to have the Digital Map updated

12.2.1.6 F9. Function to read Balise identifier.

This function is the responsible to read the Balise identifier. E_ODO-OB block shall ensure the correctness of reading of the data.

Hazard scenario 1: E_ODO-OB reads a wrong data of balise identifier

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall ensure a balise identifier read in order to have a track discrimination in the system
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

Hazard scenario 2: E_ODO-OB reads a delayed data/signal.

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.

12.2.1.7 F10. Function to read Cab status info.

This function is the responsible to read the Cab status. E_ODO-OB block shall calculate the distance of the sensors respect the leader cab.

Hazard scenario 1: E_ODO-OB calculates the relative position of sensors respect to the wrong cab

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.

Hazard scenario 2: E_ODO-OB does not know the leader cab.

- E_ODO-OB cannot provide an accuracy absolute position.. Degraded mode with inaccuracy in the absolute position[2]

12.2.1.8 F11. Function to train is switching off.

This function is the responsible to read the status of the switching off. E_ODO-OB block shall store the last position known. CMD function is out of scope of E_ODO-OB.

Hazard scenario 1: E_ODO-OB does not store the last position or stores erroneously

- E_ODO-OB shall store the position cyclically

Hazard scenario 2: E_ODO-OB store the last position before switching off but the train moves before switching on again.

- E_ODO-OB shall read the CMD input to validate its last position stored.

12.2.1.9 F14. Function to read train length

This function is the responsible to read the train length. E_ODO-OB block shall calculate the distance of the sensors respect the leader cab.

Hazard scenario 1: E_ODO-OB calculates the relative position of sensors respect to the active cab using a wrong train length

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.

[2] If the leader cab is not known, the system has an additional error in the absolute position due to the relative length of the sensor/system respect the leader cab. This additional error will be equal or smaller than the train length.

12.2.2 Functions to write (F12-F13)

12.2.2.1 F12/F13. Function to write position or speed in ETCS-OB

This function is the responsible to write position or velocity in ETCS-OB. E_ODO-OB block shall ensure the correctness of writing of the data.

Hazard scenario 1: E_ODO-OB writes a wrong data in ETCS-OB

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB HW shall implement protections against random errors of the data stored according EN 50129.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

Hazard scenario 2: E_ODO-OB writes a delayed data.

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

12.2.3 Functions to interface (F1)

12.2.3.1 F1. Function to access E_ODO_TS to manage the interface with E_ODO_TS

This function is the responsible to manage the interface with ODO_TS

Hazard scenario 1: E_ODO-OB has not interfaces with E_ODO-TS (RAM impact)

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

Hazard scenario 2: E_ODO-OB manages erroneously the interface to E_ODO-TS

- E_ODO-OB shall implement protections against the threats of the transmission systems as specified in EN 50159.
- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

12.2.4 Functions to calculate (F2)

12.2.4.1 F2. Safe fusion algorithm

This function is the responsible to calculate position, velocity and track discrimination

Hazard scenario 1: E_ODO-OB calculates a wrong data

- E_ODO-OB shall fulfil techniques and measures according EN50128 to avoid systematics faults.

12.3 FMECA

The following link provides the information to the Hazard Identification analysis but in case it fails a separate document is also attached to the deliverable.

Hazard_identification_analysis.xlsx