RCA

Reference CCS Architecture

An initiative of the ERTMS users group and the EULYNX consortium

Digital Map - PHA
Preliminary Hazard Analysis

Preliminary Issue

Document id: RCA.Doc.58

Table of contents

List of Figures

List of Tables

Version history

0.1	23.07.2021	Saïd el Fassi	Created
0.2	03.07.2021	Saïd el Fassi	Version after cluster review (V1)
0.3	10.09.2021	Saïd el Fassi	Version after cluster review (V2)
0.4	30.09.2021	Saïd el Fassi	Final review (V3) and version for MVP
0.5	15.12.2021	Saïd el Fassi	Consolidation after MVP review

1 Introduction

1.1 Release information

Basic document information:

RCA-Document Number: RCA.Doc.58

Document Name: Digital Map - PHA

Cenelec Phase: 3

Version: 0.5

RCA Baseline set: BL0R4

Approval date: 22.04.2022

1.2 Imprint

Publisher:

RCA (an initiative of the ERTMS Users Group and EULYNX Consortium)

Support and Feedback: For feedback, or if you have trouble accessing the material, please contact rca@eulynx.eu.

1.3 Disclaimer

- The (Digital) MAP as cross-cutting topic requires coordination with RCA/Trackside CCS Domain and OCORA/On-Board CCS Domain and Cross-Cutting Domain.
- The MAP process is divided into the phases "Prepare Map Data", "Publish Map Data to Trackside", and "Publish Map Data to On-Board"
- This Digital Map document is focused on the phase "Publish Map Data to On-Board".
- In general, Digital Map does not define its own Subsystem(s), rather Digital Map functionalities will be allocated to several RCA subsystems. Therefore, Digital Map uses "DM Trackside" and "DM On-Board" as functional clusters (not systems) to describe the Digital Map functionalities.
- Besides the RCA, the Digital Map context also considers the legacy architecture, which is based on the existing ERTMS/ETCS along with the introduced concepts of independent on-board Vehicle Localisation component and Virtual Balise.

1.4 Scope of this document

This document aims to provide the results of the Preliminary Hazard Analysis (PHA) of the Digital Map.

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 RCA Digital Map joint core team.

At the early stage of the Digital Map definition, it is 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.

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

Due to new architecture, game changers and changing environment, results from RCA/OCORA projects, Digital Map system definition and its environment may change along the way. Therefore, all these impacts have to be taken into consideration when documents, new versions will be released. For this reason, it will be desirable to check and update this PHA with the document issued, the results obtained by the RCA/OCORA projects.

1.5 Related documents

The following documents provide related references:

1 RCA Digital Map Concept version 1.1 [RCA.Doc.46]

2 EN 50126-1 release 2000 /-2 release 2018

3 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 ERA/GUI/01-2008/SAF

4 Guideline for the application of the CSM design targets reference ERA-REC-116-2015-GUI

5 ERTMS/ETCS subset 088-0 to -3 issue 3.7.0

6 ERTMS/ETCS subset 091 issue 3.6.0

7 RCA Terms and Abstract Concepts [RCA.Doc.14]

8 RCA Digital Map – Evaluation Publish Onboard Map Approaches [RCA.Doc.56]

9 EUG-LWG Vehicle locator Architecture Concept reference 21E109 version 1.0

10 OCORA Onboard architecture release delta Reference OCORA-TWS01-030 version 1.04

12 RCA Digital Map System Definition version 1.0 [RCA.Doc.59]

1.6 Target audience

The target group consists of members of the RCA/OCORA.

2 Definitions and Acronyms

2.1 Definitions

The definitions provided here are to assist with better understanding and readability of the document. For complete list of all the other terms and abbreviations, refer to RCA Glossary [11] or RCA DM Glossary [7].

1. Digital Map (DM): *RCA Terms and Abstract Concepts [7]*
2. Map Data: *see RCA Terms and Abstract Concepts [7]*
3. Safety-related data: *see RCA Digital Map Concept [1]*
4. Non-Safety-related data: *RCA Digital Map Concept [1]*
5. Reliable Data: *RCA Digital Map Concept [1]*
6. DM Trackside (DM-TS): *RCA Digital System Definition [12]*

   Digital Map system part of the trackside system in charge of publishing Onboard Map Data to the train.

7. DM Onboard (DM-OB): *RCA Digital System Definition [12]*

   Onboard Digital Map system in charge of managing and publishing to the onboard consumer Digital Map data.

8. Onboard Map Data: *RCA Digital System Definition [12]*

   Part of the Map Data that is transmitted to the Onboard systems, i.e. for the purpose of localisation enhancement with ERTMS.

9. (Onboard) Map Version Data:

   Unique version id of (part of) the Map Data.

10. (Onboard) Map Id Data:

    Unambiguous/unique reference to a certain part of the whole Map Data (id).

11. (Onboard) Map Integrity Data:

    Suitable information (protection data such as hash) to reveal potential transmission or processing faults

12. (Onboard) Map Reference Data:

    Unambiguous reference to a certain version and region of Onboard Map information. It includes information containing Map Version Data, Map Id Data and Map Integrity data required to validate Onboard Map Data.

2.2 Acronyms

CCS: Control-Command and Signalling

CSMs: Common Safety Methods

DT: Design Target

EU: European Union

FMEA: Failure Mode and Effect Analysis

FTA: Fault Tree Analysis

MT: Movement Authority Transactor

OBU: On-Board Unit

OCORA: Open CCS On-board Reference Architecture

PHA: Preliminary Hazard Analysis

RBC: Radio Block Centre

RCA: Reference CCS Architecture

TFFR: Tolerable Functional Failure Rate

THR: Tolerable Hazard Rate

VL: Vehicle Locator

VS: Vehicle Supervisor

3 Preliminary hazards analysis objectives

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.

For railway operations, safety is of the most importance and has to 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.

The EU sets legislations and directives to ensure that the approach of safety and the granting of safety certifications across the Member States are harmonised.

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

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.

The preliminary hazards analysis is performed in accordance with the Common Safety Methods and follows the guide for the application of the Common Safety Methods on Risk Evaluation and Assessment [3]. For details see link https://www.era.europa.eu/activities/common-safety-methods_en. The CSMs is supporting 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.

Digital Map is a subsystem of the RCA system. The DM-OB contributes also to the overall performance of the system ERTMS/ETCS. Thus, in this first stage of DM deployment, the preliminary hazard analysis is performed within the context of the ERTMS/ETCS system.

With regard to the context of the Digital Map architecture, the PHA is based on the results of RCA Digital Map Evaluation Publish Onboard Map Approaches [8], Vehicle Locator concept architecture [9] and OCORA onboard architecture [10] documents. Map Service Approach architecture as recommended in document [8] is the basis of the analysis.

The preliminary hazard analysis main goals shall contribute to identify:

- hazards where the Digital Map (DM-TS and DM-OB incl. interface) is involved,
- safety requirements on functions,
- barrier and mitigation measures for reducing hazard to an acceptable risk.

4 Methodology

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

The method used to carry out the PHA 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 [3]).

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

Figure 1 PHA methodology

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.

5 System under analysis

The system concept of the Digital Map is introduced in RCA Digital Map Concept [1], the publish principles are described in RCA Digital Map Evaluation Publish Onboard Map Approaches [8] and RCA Digital Map System Definition [12]. The publish principles are limited to the interplay/data between the trackside and the onboard. The provisioning of Map Data to trackside systems is excluded.

5.1 Digital Map objective

Digital Map is the functionality which pivots around providing static topological and topographical information about the track and trackside infrastructure in the form of Map Data. In addition, it also ensures map management functionalities like map versioning, map structuring, fulfilment of Map Data qualities.

Digital Map addresses the interplay of the relevant RCA systems through definition of exchanged Map Data content between relevant RCA interfaces, Map Data quality requirements as well as the functional needs for relevant RCA systems to realize the Digital Map services including management functions.

5.2 Digital Map consumers

Digital Map is one of the transversal functionalities that RCA envisages. Static Map Data provided by the Digital Map may be consumed by many consumers.

In the first stage of DM deployment, we limit the consumer to the onboard vehicle locator.

5.3 Digital Map function and elements

On a high-level, Digital Map shall ensure fulfilment of functionalities based on the provision, content, structure, and management of the Map Data. For details of functionalities see chapter 5.5

The fulfilment of these functionalities shall rely on:

1. Incoming (imported) requirements from the trackside/on-board systems,
2. Outgoing (exported) requirements to the on-board/track side systems.

5.4 Digital Map boundary for the PHA

The Digital Map is made of two main parts as depicted in the following figure.

- Part 1 The engineering data and preparation processes that build up the Digital Map data. This set of processes is not part of the PHA.
- Part 2 is the production system that manages the Digital Map data from the trackside to the onboard and publishes Map Data to the onboard consumers. This set of processes is part of the PHA.

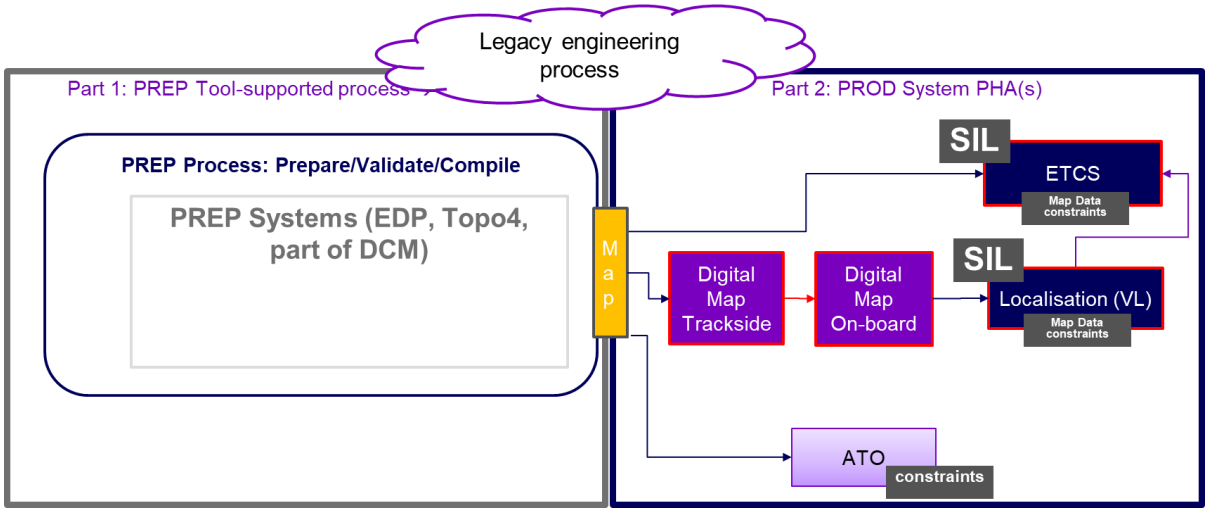

Figure 2 Digital Map overview subsystem

PHA-A- 1: The boundary of the hazard analysis is limited to the impact of the Digital Map on the localisation system through the VL interface, and therefore on the ETCS system.

The main interface is between the Digital Map and the vehicle locator.

PHA-A- 2: The Map Data on the Digital Map trackside are considered prepared, compiled, and validated and ready for use by the Digital Map Trackside.

The following figure depicts in red the boundary of the PHA analysis.

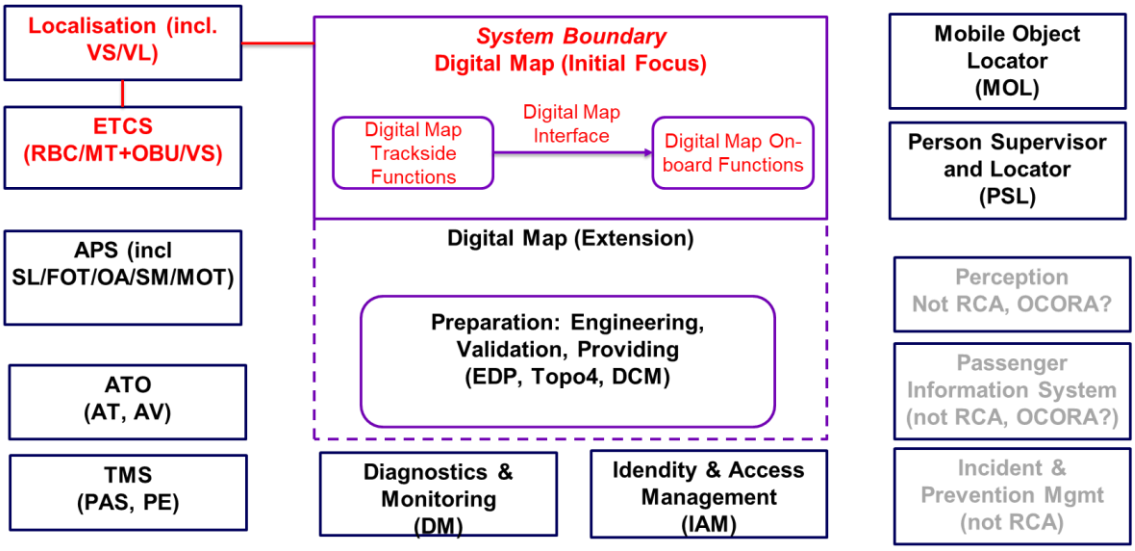

Figure 3 System Boundary of Digital Map PHA

5.5 Digital Map functionalities

PHA-A- 3: The main functionalities are based on the (plain) Map Service approach as recommended in RCA Digital Map Evaluation Publish Onboard Map Approaches [8].

PHA-A- 4: Digital Map functionalities described are based on the availability of a radio link system between Digital Map Data trackside and onboard.

RCA Digital Map System definition [12] describes in chapter 6 the Digital Map functional clusters and in chapter 7 the Digital Map functionalities. Detailed process on how different functions of DM-OB or DM-TS functional groups interact with each other are provided in chapter 7 and figures 3, 4 and 5 of document [12]. This process includes the following aspects,

1. Requesting of Map Data/Reference Data
2. Provision of Map Data/Reference Data
3. Validation of Map Data
4. Downloading of Map Data
5. Activation of Map Data
6. Providing Map Data to On-Board consumer
7. Deactivation of Map Data

Functions are identified in table 1 of [12]. Flow charts defining the processes are defined through the figures 3 to 5 of [12] .

6 Hazard and Risk assessment

The guideline for the application of the CSM design targets [4] 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.

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

CSM guide [3] 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.

By applying the CSM guideline to the Digital Map, a first selection of risk acceptance method for each part of the DM has been done.

1) Code of practice: this risk assessment is relevant for the PREP process (not scope of this PHA).
2) Reference system: this risk assessment might be applied for initial focus if equivalent system could be identified. This risk assessment is relevant to the DM as it contributes to the overall performances of the ERTMS/ETCS. In our context at the system level, the reference system is ERTMS/ETCS. Digital Map hazards are bear by the ERTMS/ETCS.
3) Explicit of risk estimation: this risk assessment is not relevant for the Digital Map as long it is based on the reference system (ERTMS/ETCS).

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

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.

For the risk assessment at the system level, the following principle applied.

PHA-A- 5: At the system level the main identified final user is the ERTMS/ETCS system

PHA-A- 6: The reference system is ERTMS/ETCS, at the system level, Digital Map hazards are bear by the ERTMS/ETCS.

PHA-A- 7: 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 Digital Map.

The following figure shows the links between the Digital Map PHA and the ERTMS/ETCS findings summarized in subsets 91 [6] and 88 [5].

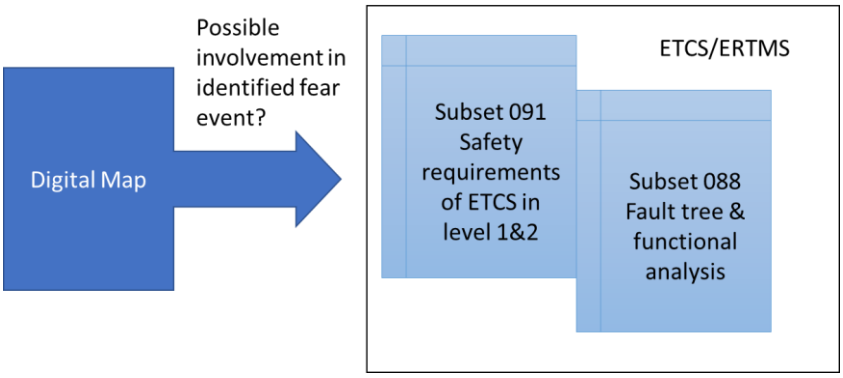

Figure 4 Links between the Digital Map Risk assessment and findings of ERTMS/ETCS system

After analysis subsets 091 [6] and 088 [5], among the hazards listed in subset 091, 11 hazards of the ERTMS/ETCS system have been identified with a possible involvement of the Digital Map.

PHA-A- 8: The 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 PHA might be necessary to include level 3 findings, changes.

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 [5].

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-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.
KERNEL-1	Balise linking consistency checking failure	_ Incorrect session status/ transmission status (e.g. radio link reaction) _ Failure of braking intervention (e.g. linking reaction) _ Incorrect Emergency Stop Location	Linking reaction
KERNEL-7	Incorrect LRBG	Incorrect determination of train position ref to LRBG	Determination of train position to LRBG
KERNEL-23	Incorrect train position / train data sent from on-board to trackside	Incorrect Provision of data (trackside)	Supervision of EoA / LoA Provision and revocation of emergency messages
KERNEL-28	Incorrect confidence interval	Incorrect determination of train position ref to LRBG	Determination of distance travelled Determination of train position to LRBG
BTM-H1	A balise group is not detected, due to failure within the on-board BTM function	Incorrect provision of data	
BTM-H7	Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)	Incorrect provision of data	

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
BTM-H8	The order of reported Balises, with reception of valid telegrams, is erroneous due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal	Incorrect provision of data	
BTM-H9	Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failure within the onboard BTM function (erroneous threshold function or significantly excessive Telepowering signal)	Incorrect provision of data	

Table 1 ERTMS/ETCS hazards relevant to Digital Map risk assessment

PHA-A- 9: The effect of lack of radio system between the trackside and the onboard Digital Map is not taken into consideration in this version of the PHA.

PHA-A- 10: The determination of the LRBG is not done by the VL. VL is providing the position of the train from a reference point.

Following hazard identification at the ERTMS/ETCS system level, the following table presents the derived hazards, fear events at the level of the Digital Map.

Subset 091_V360 Annex A Event Id.	Event Description	Digital Map Feared Event
ODO-2	Speed measurement underestimates trains actual speed	Fail to provide the correct Map Data (track description) ***Open point:*** *Impact of incorrect Map Data on the train speed measurement has to be confirmed by expert*
ODO-3	Incorrect actual physical speed direction	Fail to provide the correct Map Data (virtual balise information, track description) ***Open point:*** *Impact of incorrect Map Data on the train speed direction has to be confirmed by expert.*
ODO-4	The confidence interval for distance measurement does not include the actual position of the train	Fail to provide the correct Map Data (track description) ***Open point:*** *Impact of incorrect Map Data on confidence interval and the actual position of the train has to be confirmed by expert*

Subset 091_V360 Annex A Event Id.	Event Description	Digital Map Feared Event
KERNEL-1	Balise linking consistency checking failure	Fail to provide the correct Map Data (virtual balise information)
KERNEL-7	Incorrect LRBG	Fail to provide the correct Map Data (virtual balise information, track description) ***Open point:*** *Impact of incorrect Map Data on LRBG determination for physical balise has to be confirmed by expert.*
KERNEL-9	Speed calculation underestimates train speed	Covered by ODO events
KERNEL-23	Incorrect train position / train data sent from on-board to trackside	Covered by ODO events
KERNEL-28	Incorrect confidence interval	Fail to provide the correct Map Data (track description) ***Open point:*** *Impact of incorrect Map Data on the confidence interval has to be confirmed by expert.*
BTM-H1	A balise group is not detected, due to failure within the on-board BTM function	Fail to provide the correct virtual balise Map Data e.g. deletion of virtual balise data
BTM-H7	Erroneous localisation of a Balise Group, with reception of valid telegrams, due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal)	Fail to provide the correct virtual balise Map Data, e.g. virtual balise localisation is corrupted
BTM-H8	The order of reported Balises, with reception of valid telegrams, is erroneous due to failure within the on-board BTM function (erroneous threshold function or significantly excessive Tele-powering signal	Fail to provide the correct virtual balise Map Data, e.g. localisation of virtual balise are corrupted balises are not in the right order

Subset 091_V360 Annex A Event Id.	Event Description	Digital Map Feared Event
BTM-H9	Erroneous reporting of a Balise Group in a different track, with reception of valid telegrams, due to failure within the onboard BTM function (erroneous threshold function or signifi-cantly excessive Telepowering signal)	Fail to provide the correct virtual balise Map Data, e.g. track Id is corrupted.

Table 2 Derived Digital Map Hazards, Feared Events

From the Table 2 two hazards are identified at the level of the Digital map

- DM_Haz1: Fail to provide the correct Map Data for track description.
- DM_Haz2: Fail to provide the correct Map Data for virtual balise information.

7 Safety requirements and apportionment of the Digital Map

The THR/TFFR apportionment for each function of the Digital Map is derived from the overall ERTMS/ETCS apportionment principles.

The apportionment between the onboard functions, the transmission functions and the trackside functions are defined in subset 091[6]. The following figure presents the apportionment between the subsystems of the ERTMS/ETCS.

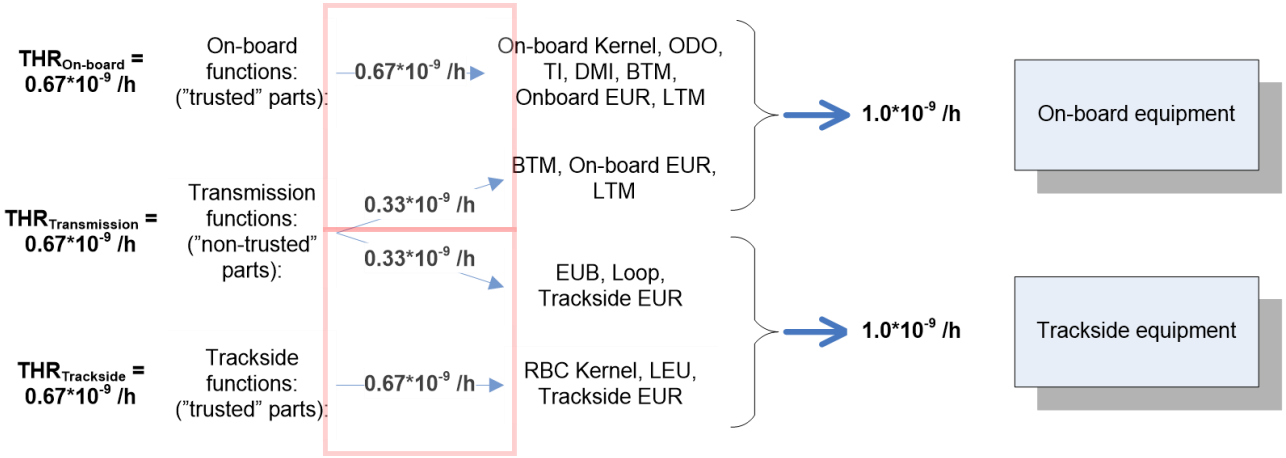

Figure 5 ERTMS/ETCS apportionment between the 3 subsystems

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.

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.

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 Digital Map 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.

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)

The following table provides the results of FMEA for each DM function (see chapter 5.5), identifying the possible feared events leading to the Digital Map hazard DM_Haz1 and/or DM_Haz2 and the barriers (safety relevant function) to be put in place.

PHA-A- 11: The activation of onboard Map Data that are not consistent with the train location is not considered as a feared event. VL shall check if the onboard Map data received from DM-OB are consistent with the train location.

PHA-A- 12: The safe deactivation of the Map Data is ensured only by the function DM_O_11 determining the deactivation. This function shall be safely triggered by the external trigger **like system shutdown, Map Data updates, disconnection from DM-TS, etc..**

Function	Feared Event		Explanation	Hazard	Barrier (external/Mitigation)	Design Target TFFR
DM_O/T_1	FE_1	Incorrect request	The request is not consistent with the need	DM_Haz1 DM_Haz2	DM_O_10	Non safety related
DM_O/T_1	FE_2	Incorrect message Insertion Corruption Repetition Deletion	Message is modified during transmission	DM_Haz1 DM_Haz2	DM_O_10	Non safety related
DM_T_2	FE_3	Incorrect Onboard Map Reference Data determination	The request is incorrectly processed, leading to incorrect Onboard Reference Map Data	DM_Haz1 DM_Haz2	DM_O_10	Non safety related
DM_T_2	FE_4	Corrupted Onboard Map Reference Data	DM_T_2 is introducing errors in Onboard Map Reference Data	DM_Haz1 DM_Haz2	Method to guarantee the integrity of Onboard Map Reference Data. Processing with SIL4	$<10^{-9}$/h
DM_O/T_3	FE_5	Incorrect Onboard Map Reference Data	Due to incorrect map determination or incorrect processing	DM_Haz1 DM_Haz2	The integrity of Onboard Map Reference Data or processing has to be guaranteed, Processing with SIL4	$<10^{-9}$/h
DM_O/T_3	FE_6	Insertion Corruption Repetition	Message modified during transmission	DM_Haz1 DM_Haz2	Method to protect the message during transmission	$<10^{-9}$/h
DM_O_4	FE_7	Incorrect need for updating Map Data	Data to identify the need or processing is incorrect	DM_Haz1 DM_Haz2	DM_O/T_3 DM_O_8 DM_O_10	Non safety related
DM_O/T_5	FE_8	Incorrect request	The request is inconsistent with the need	DM_Haz1 DM_Haz2	DM_O/T_3 DM_O_8 DM_O_10	Non safety related

DM_O/T_5	FE_9	Insertion Corruption Repetition	Message is modified during transmission	DM_Haz1 DM_Haz2	DM_O/T_3 DM_O_8 DM_O_10	Non safety related
DM_T-6	FE_10	Incorrect determination of Map data	Due to incorrect request or processing	DM_Haz1 DM_Haz2	DM_O/T_3 DM_O_8 DM_O_10	Non safety related
DM_O/T_7	FE_11	Downloading incorrect data	Due to incorrect determination or incorrect processing	DM_Haz1 DM_Haz2	DM_O/T_3 DM_O_8 DM_O_10	Non safety related
DM_O/T_7	FE_12	Insertion Corruption Repetition	Message is modified during transmission	DM_Haz1 DM_Haz2	DM_O/T_3 DM_O_8 DM_O_10	Non safety related
DM_O_8	FE_13	Incorrect Map Data validation	Onboard Map Reference Data and Map data are not consistent, or processing is incorrect	DM_Haz1 DM_Haz2	Method to guarantee the integrity of Onboard Map Reference Data. Processing with SIL4. Map data shall be used by safety relevant applications only when validated	$<10^{-9}$/h
DM_O_9	FE_14	Incorrect activation	Version, Reference, and Integrity data or processing are incorrect	DM_Haz1 DM_Haz2	Protect Version, Reference, and Integrity data Processing with SIL4	$<10^{-9}$/h
DM_O_10	FE_15	Incorrect request Insertion Corruption Repetition	Message is corrupted or processing the request is incorrect	DM_Haz1 DM_Haz2	Method to detect incorrect message Processing with SIL4	$<10^{-9}$/h
DM_O_10	FE_16	Incorrect Map Data	Map Data are corrupted Map Data are inconsistent with the request Processing is incorrect	DM_Haz1 DM_Haz2	Method to guarantee the integrity of Map Data Processing with SIL4	$<10^{-9}$/h

DM_O_11	FE_17	DM_O_11 is not triggered.	Deletion (information received through the network) Failure of information (information received by wire)	DM_Haz1 DM_Haz2	Method to guarantee the integrity of the trigger information	$<10^{-9}$/h
DM_O_11	FE_18	No determination of Map Data deactivation	The processing is incorrect leading to a potential use by the onboard of an unauthorised Map Data version.	DM_Haz1 DM_Haz2	Processing with SIL4	$<10^{-9}$/h
DM_O_12	FE_19	No deactivation of Map Data, use of an unauthorised Map Data	The processing is incorrect leading to a potential use by the onboard of an unauthorised Map Data version.	DM_Haz1 DM_Haz2	Processing with SIL4	$<10^{-9}$/h
External data input	FE_20	Request not received	No update of Map Reference Data, Map Data	DM_Haz1 DM_Haz2	DM_O_11	Non safety related
External data input	FE_21	Incorrect Map Reference Data trigger Insertion Corruption Repetition	The request is not consistent with the need	DM_Haz1 DM_Haz2	DM_O_10	Non safety related

Table 3 Feared events of Digital Map functions and safety requirements.

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

PHA Function ID	PHA: Safety-related?	Design target TFFR
DM_O/T_1	No	N/A
DM_T_2	Yes	$<10^{-9}$/h
DM_O/T_3	Yes	$<10^{-9}$/h
DM_O_4	No	N/A
DM_O/T_5	No	N/A
DM_T_6	No	N/A

PHA Function ID	PHA: Safety-related?	Design target TFFR
DM_O/T_7	No	N/A
DM_O_8	Yes	$<10^{-9}$/h
DM_O_9	Yes	$<10^{-9}$/h
DM_O_10	Yes	$<10^{-9}$/h
DM_O_11	Yes	$<10^{-9}$/h
DM_O_12	Yes	$<10^{-9}$/h
External data input	No	N/A

Table 4: Function classification and design target

8 Assumptions

The table presents the synthesis of assumptions identified during the preliminary hazard analysis of the Digital Map.

Id	Assumption
PHA-A- 1	The boundary of the hazard analysis is limited to the impact of the Digital Map on the localisation system through the VL interface, and therefore on the ETCS system.
PHA-A- 2	The Map Data on the Digital Map trackside are considered prepared, compiled, and validated and ready for use by the Digital Map Trackside
PHA-A- 3	The main functionalities are based on the Map Service approach as recommended in RCA Digital Map Evaluation Publish Onboard Map Approaches [8]
PHA-A- 4	Digital Map functionalities described are based on the availability of a radio link system between DM-TS and DM-OB.
PHA-A- 5	At the system level the main identified final user is the ERTMS/ETCS system
PHA-A- 6	The reference system is ERTMS/ETCS, at the system level, Digital Map hazards are bear by the ERTMS/ETCS
PHA-A- 7	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 Digital Map
PHA-A- 8	The PHA 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 PHA might be necessary to include level 3 findings, changes.
PHA-A- 9	The effect of lack of radio system between the trackside and the onboard Digital Map is not taken into consideration in this version of the PHA.
PHA-A- 10	The determination of the LRBG is not done by the VL. VL is providing the position of the train from a reference point.
PHA-A- 11	The activation of onboard Map Data that are not consistent with the train location is not considered as a fear event. VL shall check if the onboard Map data received from DM-OB are consistent with the train location (completeness check: required map area around train location completely covered).
PHA-A-12	The safe deactivation of the Map Data is ensured only by the function DM_O_11 determining the deactivation. This function shall be safely triggered by external trigger like system shutdown, Map Data updates, disconnection from DM-TS, etc..

Table 5 List of assumptions from the Digital Map preliminary hazard analysis

9 Open Points

The following open issues are identified:

Open point #	Event Id	Issue
PHA-OP-1	ODO-2	Does incorrect Map Data could lead to an underestimation of speed?
PHA-OP-2	ODO-3	Does incorrect Map Data could lead to wrong train speed direction?
PHA-OP-3	ODO-4	Does incorrect Map Data could lead to the actual position of the train not included in the confidence interval?
PHA-OP-4	KERNEL 7	Incorrect LRBG Does it apply only to virtual balises or also physical balises
PHA-OP-5	KERNEL 28	Does the track data have an impact on the confidence interval?

Table 6 List of PHA open points