European Global Navigation Satellite Systems Agency

ERSAT GGC

WP3 - Safety and Hazard Analysis of the Enhanced ERTMS Architecture

RINA Consulting

ERSAT-GGC Final Meeting

Prague, November 26th 2019

WP3 Key Objectives

- Develop the **Qualitative & Quantitative Safety Study of ERSAT-GGC** reference architecture**,** on **basis** of previous research projects **(e.g., NGTC)** outcomes and upon **Operational Scenarios** of **ERSAT GCC project**
- **Work jointly with WP2,** devoted to ERSAT-GGC reference architecture definition, in order to realistically identify the possible system functional deviations and support the formalization of a safe Enhanced Architecture in view of the assessment performed by the Notified Bodies within WP5
- **Definition of the Functional and Operational Safety Requirements** and **development of the Fault Tree** necessary to validate the safety and technical interoperability of the new ERTMS system.

WP3 Starting Point

Starting point from other projects:

- NGTC: Safety Analysis of WP7 (D7.7):
  - First analysis combining ETCS and GNSS requirements
  - High Level Qualitative & Quantitative requirements on Railway and GNSS

Starting point from Standards:

- UNISIG:
  - ERTMS Reference Architecture
  - Subset-088 Core Hazard apportionment approach
  - Subset-091 Tolerable Hazard Rates, especially for Eurobalise Transmission System

WP3 Challenges

Adoption of an analysis approach capable of:

- Assessing the failure modes risk according to CSM EU 402/2013
- Defining the necessary, but also generic functional and operational safety requirements
- Defining the VB Information Point Hazards as UNISIG does for the Eurobalise ones
- Modelling the new technology functional faults (at on-board and trackside level) within the Fault Tree
- Defining numerical targets (THR) that ensure safety and technical interoperability according to the existing UNISIG THR

Work performed:
Qualitative Safety Study

FMECA ID	Architectural Block	Guide Word	Failure Mode	Failure Cause	Directl Failure Mode Effects
FB-K 1.2.1	GNSS Receiver	NO	The Block does not execute its function	Internal HW/SW failure	The block does not output any code/phase measurement upon the RF input
FB-K 1.2.2		MORE	The Block executes its functions more times then needed.	Internal HW/SW failure	The block outputs more than once the pseudorange measurement for the same RF signal
FB-K 1.2.3		LESS	The Block executes its functions less times then needed	Internal HW/SW failure	see NO
FB-K 1.2.4		OTHER THAN	Case 1) The Block's output information is other than expected: Valid Data, but different from the effective one	Internal HW/SW failure Environment Configuration	The block outputs a formally valid pseudorange measurement, but undue (i.e. wrong)
FB-K 1.2.5			Case 2) The Block's output information is other than expected: Non-Valid Data.	Internal HW/SW failure Environment Configuration	The block outputs a non-usable pseudorange information
FB-K 1.2.6		EARLY	The Block executes its function before than expected	Internal HW/SW failure	Case 1) - the device has no memory The receiver outputs a non-usable pseudorange measurement before the data processing completion
FB-K 1.2.7					Case 2) - the device has an internal memory The receiver outputs an undue (i.e. old) pseudorange measurement before the computing of the instantaneous one is completed
FB-K 1.2.8		LATE	The Block executes its function later than expected	Internal HW/SW failure Environment Configuration	The pseudorange measurement is issued later than expected

Extract of the Project FMECA

The first step of WP3 has been the systematic identification of the credible failure modes

- For each functional block and interface of the ERSAT-GGC VBTS sub-system
- For each ERSAT-GGC Operational Scenario

Work performed:
Qualitative Safety Requirements

Concerning the Track Database validation:

- Once the RBC-EVC communication session is established the Track DB version shall be verified
- The ERTMS/ETCS Trackside subsystem shall not provide any MA till the Track DB version has not been verified with a positive result

Concerning the VBR initialization:

- The ERTMS/ETCS Trackside subsystem shall not provide any MA till the positive VBR initialization has not been performed and communicated
- VBR shall be set "initialized" only if all the information necessary to enable the VB detection functionality have been correctly received and processed

Work performed:
Qualitative Safety Requirements

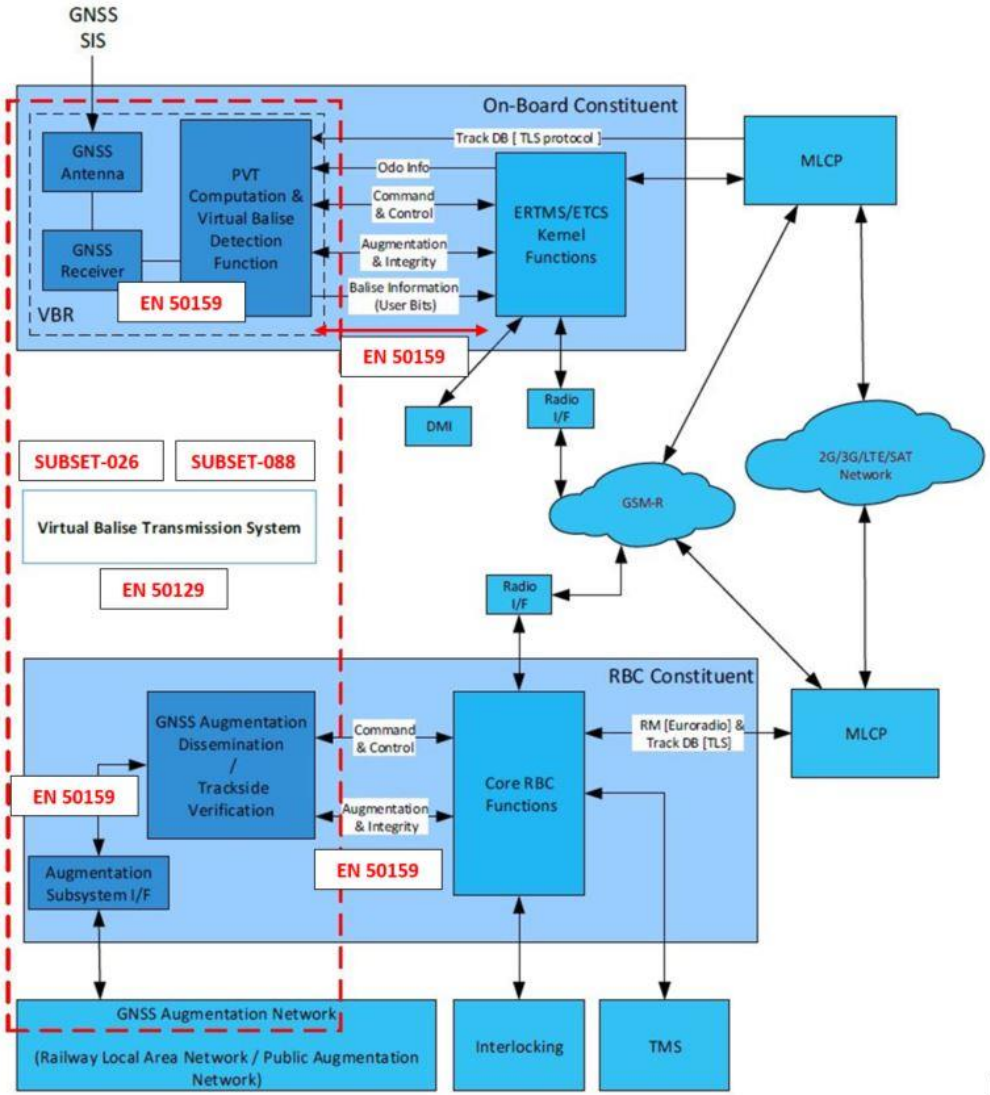
Concerning the new Communication Interfaces:

- The EVC-VBR, GAD/TV-RBC, VBR internal interfaces shall be closed safety-related transmission system compliant to the EN 50159 standard

Concerning the VB detection:

- The on-board GNSS chains (i.e. from the GNSS antenna to the Balise delivery function) shall be implemented to guarantee the required THR
- VBR shall detect the unavailability of the fresh and consistent PVT solution
- If the fresh and consistent PVT is missing, VBR shall use the last fresh and consistent PVT (if any) by taking into account their impact on the confidence interval. VBR has to inform ETCS/ Kernel when there is a failure in the VBR detection function. Then, ERTMS/ETCS shall manage this warning properly and react in accordance to the applicable conditions
- The PVT solution shall be always crossed-check with other information
- The fresh GNSS augmentation on-board unavailability shall be treated as a safety affecting fault

Work performed:
Risk Acceptance



The residual risk level has been accepted identifying a set of applicable Codes of Practice:

- CENELEC EN 50159
- CENELEC EN 50129
- UNISIG Subset-026
- UNISIG Subset-088

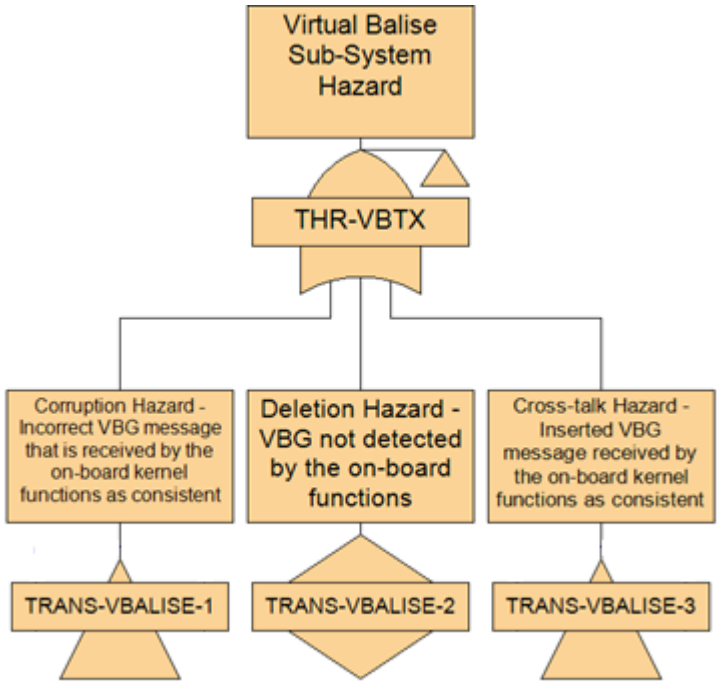
Including applicative conditions compliant with ERSAT –GGC Safety Requirements

Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach

- Identification of hazards related to a Virtual information point, for a Track Section equipped with VBG
- Development of a constituent-based fault-tree to link the VB information point hazards to the top-level ETCS Core Hazard
- Preliminary apportionment is made to the VB information point hazards

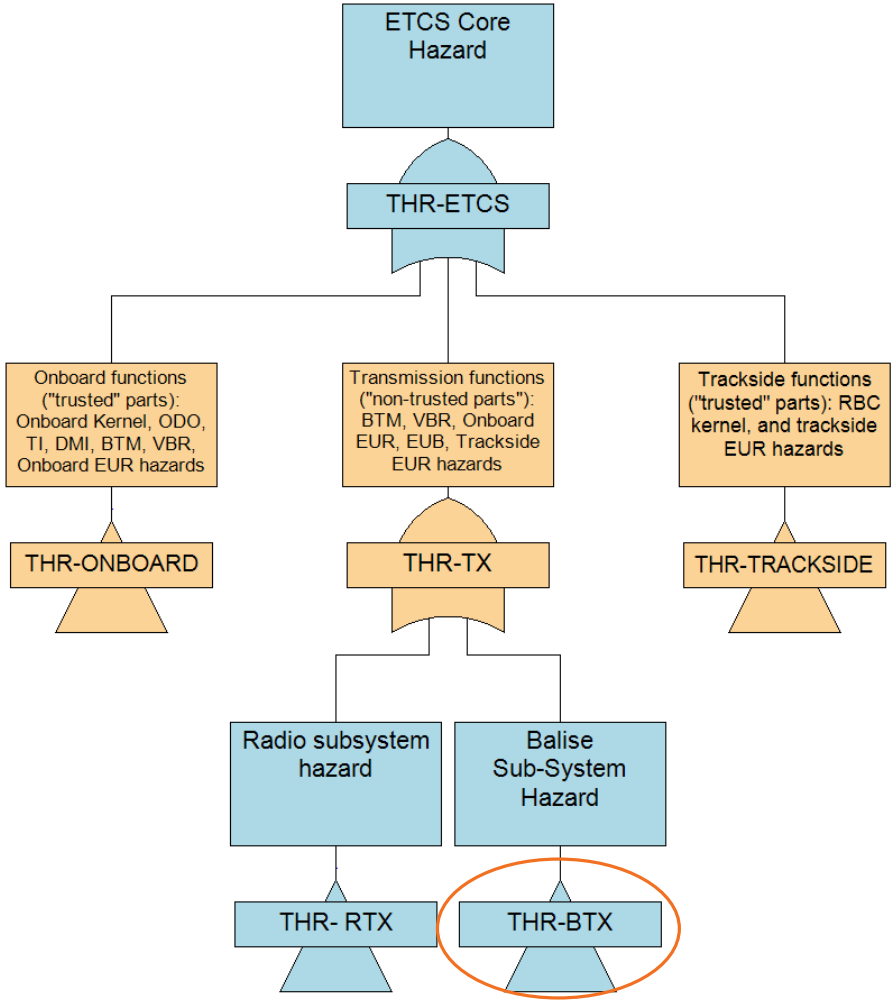


Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach

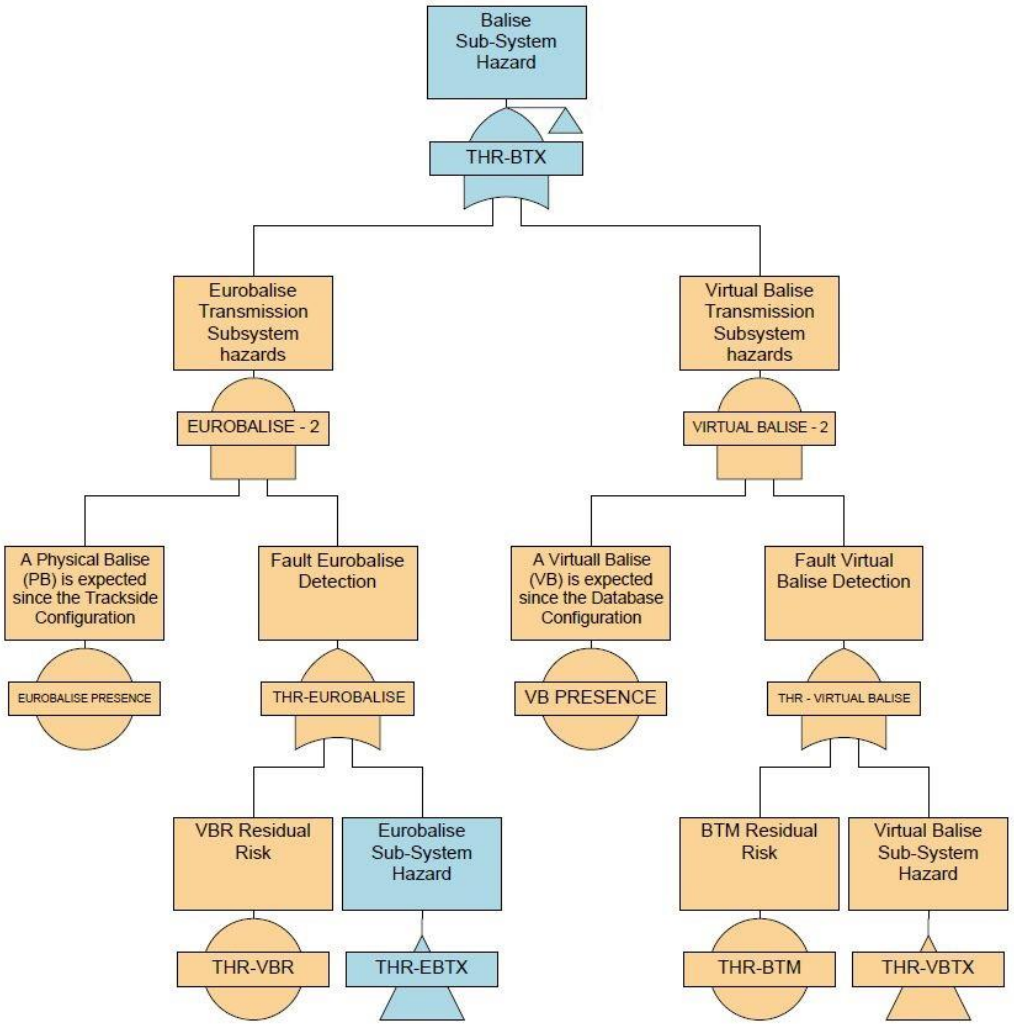
- Identification of hazards related to a Virtual information point, for a Track Section equipped with VBG
- Development of a constituent-based fault-tree to link the VB information point hazards to the top-level ETCS Core Hazard
- Preliminary apportionment is made to the VB information point hazards



Work performed:

Quantitative Analysis - Interoperability

ERSAT-GGC Novelty



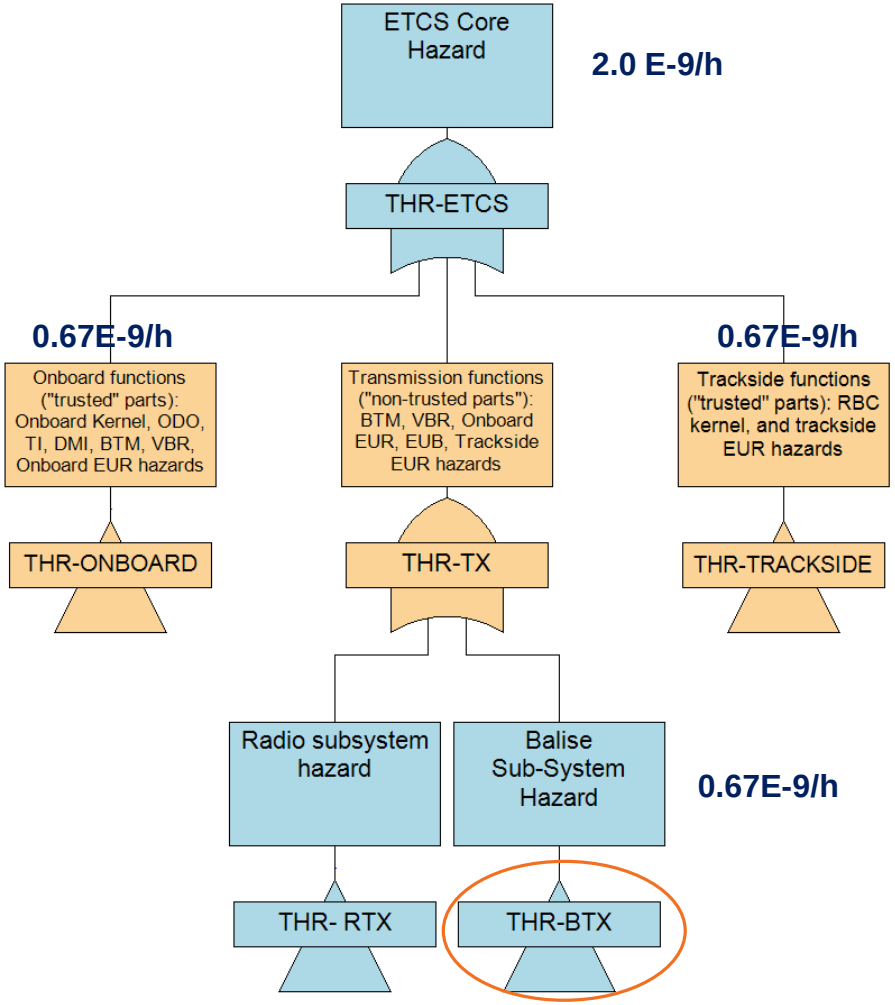
- **EUROBALISE PRESENCE** & **VB PRESENCE**: are **True** or **False** according to the safe (SIL4) Trackside or Database Configuration
- **VBR / BTM residual risk** is required to be negligible

Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach

- Identification of hazards related to a Virtual information point, for a Track Section equipped with VBG
- Development of a constituent-based fault-tree to link the VB information point hazards to the top-level ETCS Core Hazard
- Preliminary apportionment is made to the VB information point hazards

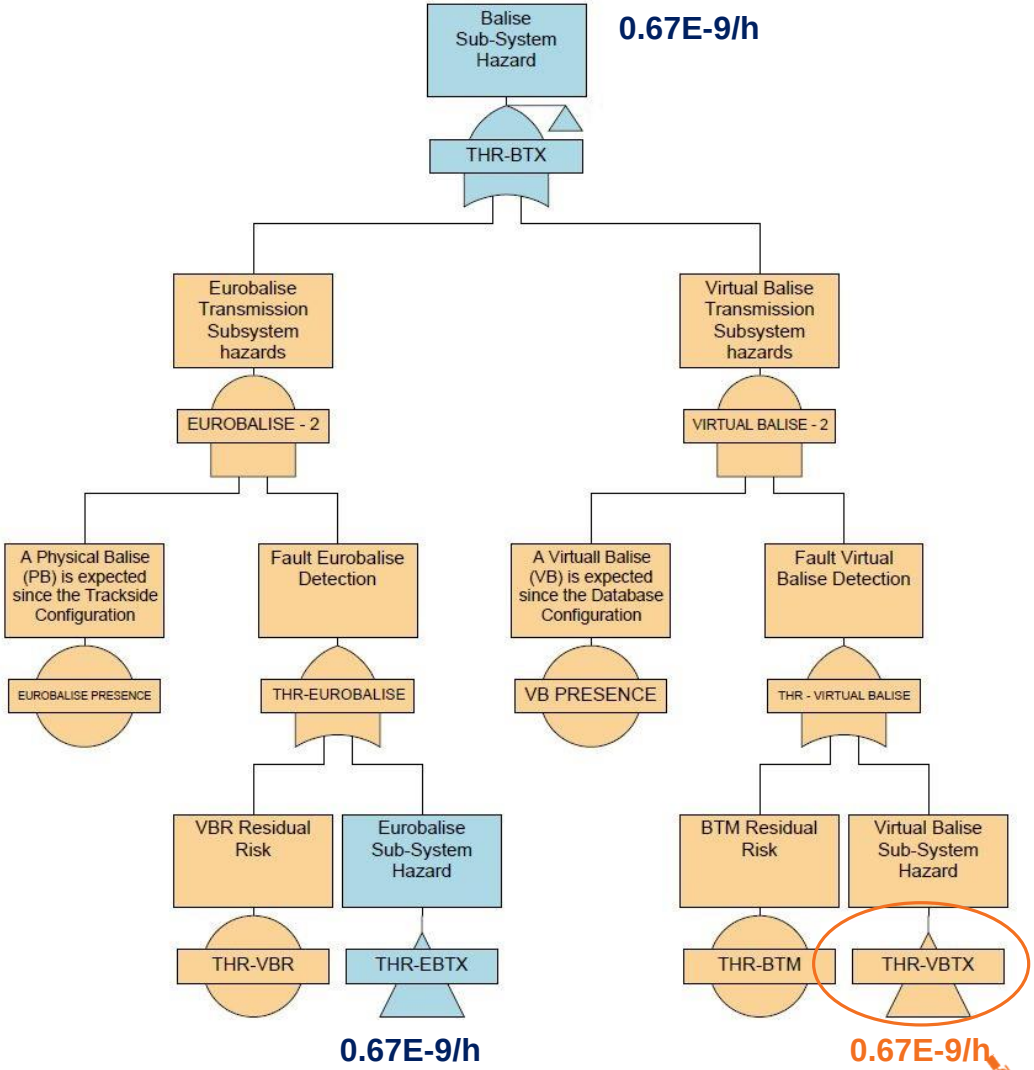


Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach

- Identification of hazards related to a Virtual information point, for a Track Section equipped with VBG
- Development of a constituent-based fault-tree to link the VB information point hazards to the top-level ETCS Core Hazard
- Preliminary apportionment is made to the VB information point hazards

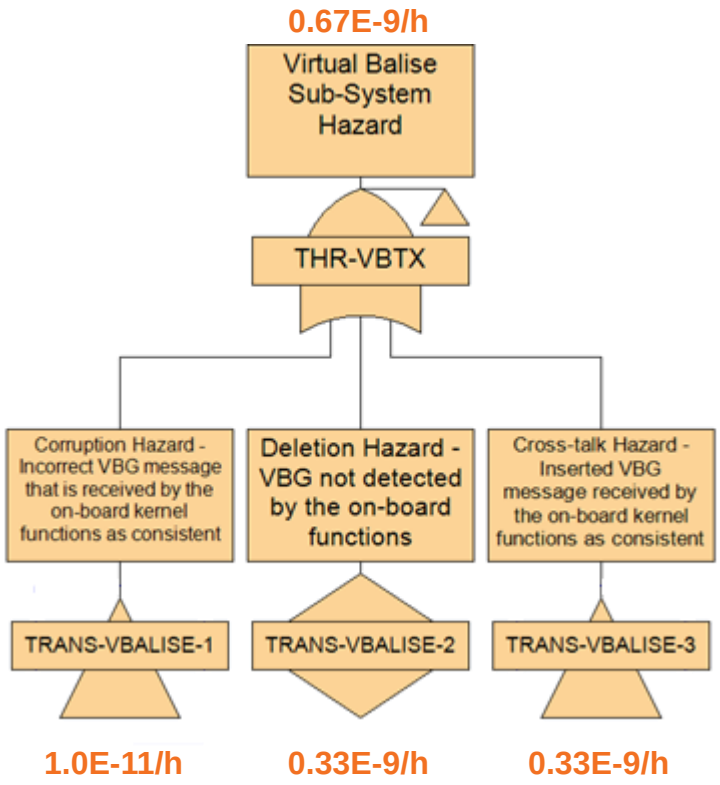


Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach

- Identification of hazards related to a Virtual information point, for a Track Section equipped with VBG
- Development of a constituent-based fault-tree to link the VB information point hazards to the top-level ETCS Core Hazard
- Preliminary apportionment is made to the VB information point hazards



Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach

- Study of ERSAT-GGC Operational Scenarios to identify the worst cases and make considerations on the THR apportionment
- Rules are specified for too demanding scenarios
- Amendment of the preliminary apportionment on basis of any inherent ETCS protections and / or rules, which limit the migration of the information point hazards towards the ETCS Core Hazard

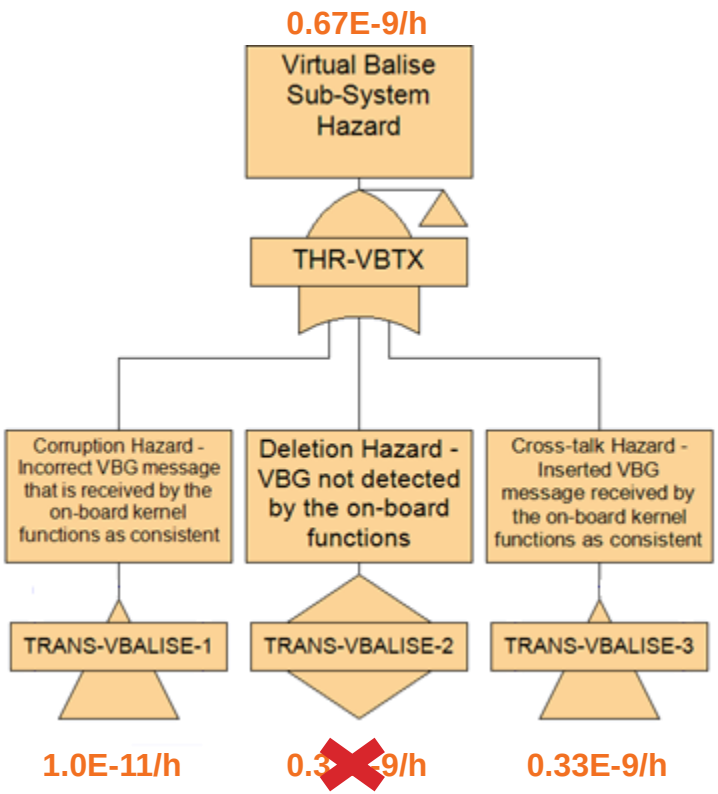
Start of Mission in Line with Unknown Position Report

With Staff Responsible authorization

Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach



Deletion Hazard:

- **Rule**: Temporary Speed Restriction are not transmitted via VBG
- VBR shall be designed and configured in compliance to SIL4 process
- Residual On-board risk is negligible

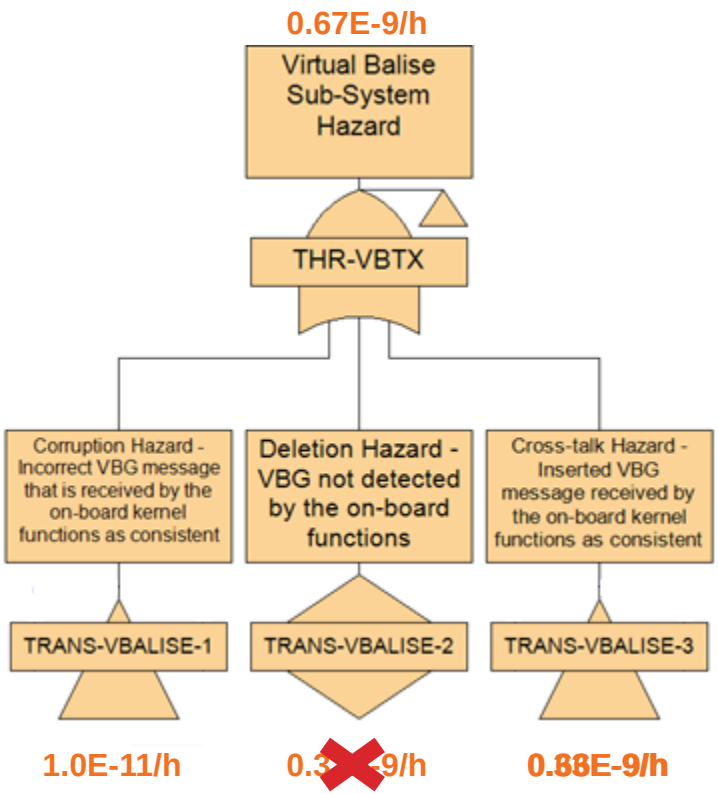
Insertion Hazard:

- Worst Case: SoM / Entry in ETCS Areas with SR authorisation
- **Rule**: The Track shall be discriminated with a safe procedure compatible to the SIL4 targets

Work performed:

Quantitative Safety Analysis

Use of UNISIG Subset-091 & Subset-088 Part 3 approach



Deletion Hazard:

- **Rule**: Temporary Speed Restriction are not transmitted via VBG
- VBR shall be designed and configured in compliance to SIL4 process
- Residual On-board risk is negligible

Insertion Hazard:

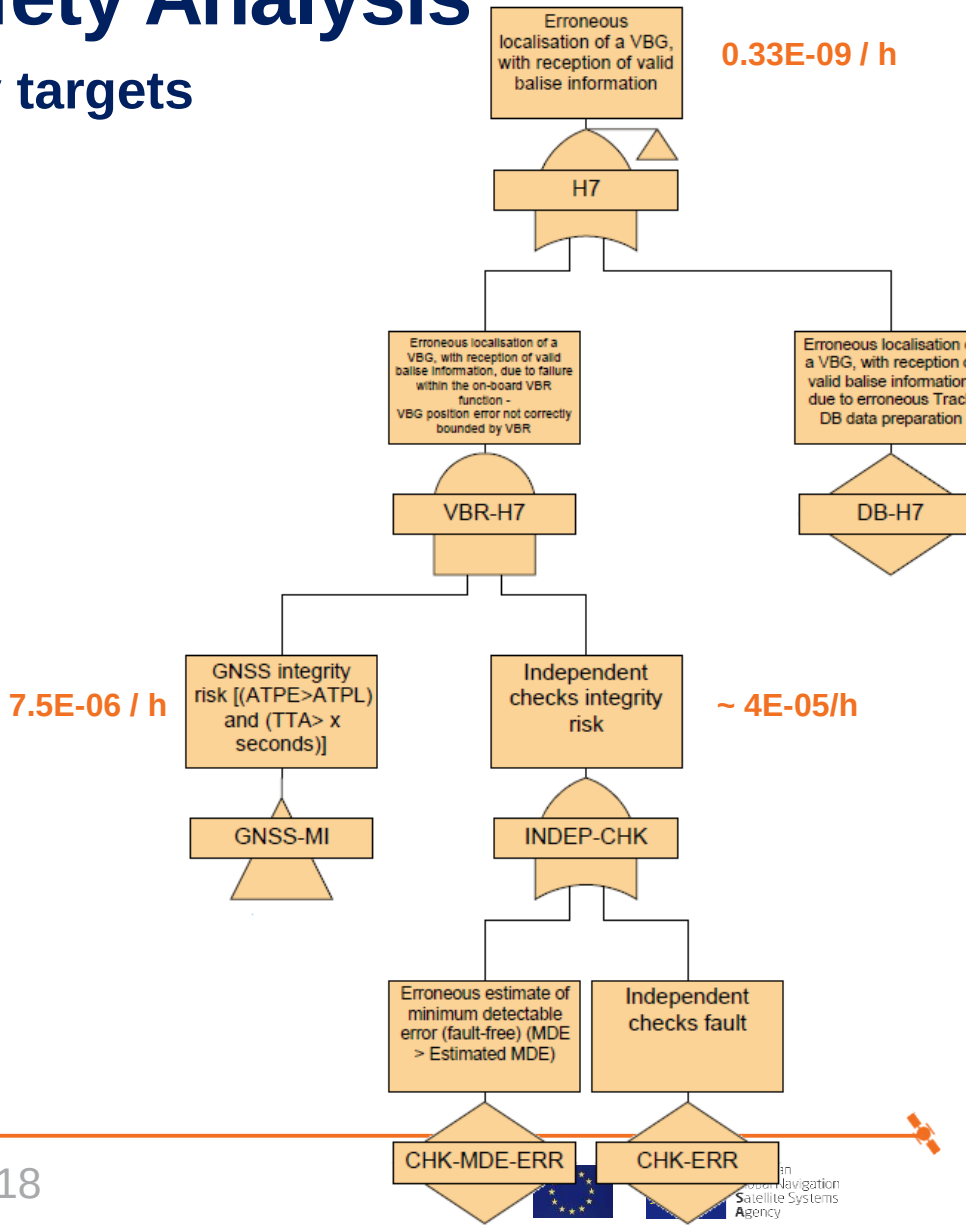
- Worst Case: SoM / Entry in ETCS Areas with SR authorisation
- **Rule**: The Track shall be discriminated with a safe procedure compatible to the SIL4 targets

Work performed:

Quantitative Safety Analysis

GNSS and Augmentation integrity targets

- Inclusion of GNSS and Augmentation performances in the railway environment, on basis of NGTC and ESA outcomes
- Preliminary definition of ranges for the User Local Effects integrity targets.



Project findings and next steps (1/3)

In collaboration **with WP2 (focused on the Enhanced Reference Architecture)**, the safety analysis has

- Better investigated and managed the Enhanced Architecture weakness
- Thoroughly identified the components, at trackside and onboard level, of each failure mode
- Defined a set of necessary qualitative Safety Requirements, without putting excessive constraints

In collaboration **with WP5 (focused on WP2 and WP3 assessment)**, the safety analysis has

- Strengthen the parallelism with UNISIG approach in the FT development
- Formalized the relationship with the existing UNISIG FT ensuring the technical interoperability

Project findings and next steps (2/3)

WP3 Analysis has found that **ERSAT-GGC Reference Architecture is capable** of managing the hazards emerged from the safety analysis of the operational scenarios with an **acceptable residual risk** level provided that:

- the agreed functional and operational safety measures are fulfilled
- the THRs < 1.0E-9 dangerous failure/ hour shall be addressed with SIL4 compliant safety process:
  - Track Database incorrect preparation
  - Incorrect Track Discrimination
  - The VBG position error not correctly bounded by VBR (longitudinal cross-talk)
  - The residual risk of interfering fault from VBR and BTM when not functionally involved

Project findings and next steps (3/3)

ERSAT-GGC Added Value:

The WP3 work, moving from NGTC basis, has confirmed the FT development approach and the main quantitative targets.

Furthermore, the generic and complete FT of ERSAT-GGC is contributing to the **Technical Interoperability,** which has been **demonstrated possible** provided that:

- A tolerable residual risk on BTM and VBR
- A safe preparation of the Track Database, as is done for the Trackside yet.

This result is expected to support and speed up the certification process for a first operational deployment on the RFI Pilot line.

Thank you for your attention!