

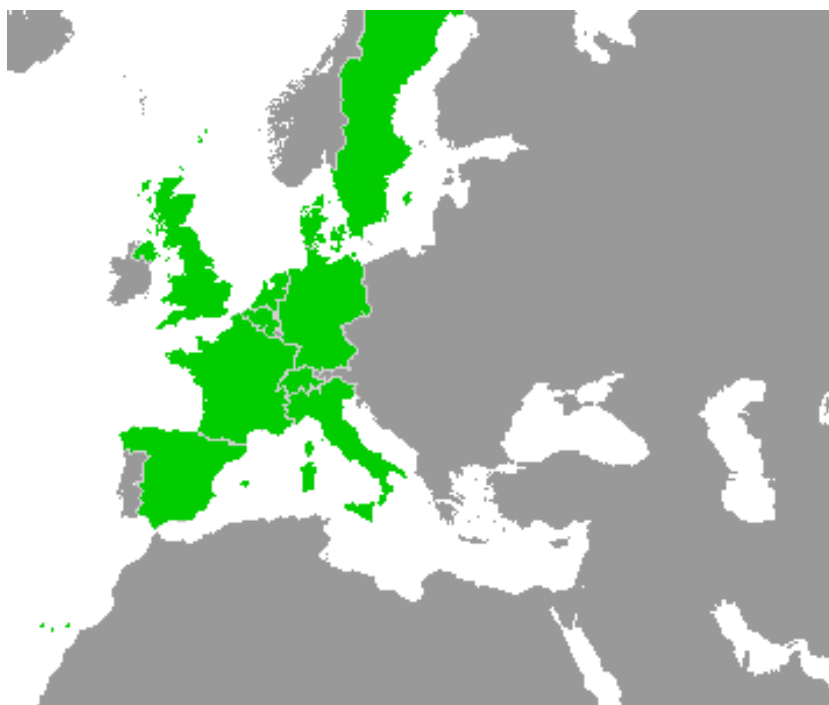
Work-Package 2: “Definition”

## OpenETCS process

**Definition of the overall process for the formal description of ETCS and the rail system it works in**

Marielle Petit-Doche

February 2013



This page is intentionally left blank

# OpenETCS process

**Definition of the overall process for the formal description of ETCS and the rail system it works in**

Marielle Petit-Doche

Systerel

## Definition

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.



Prepared for ITEA2 openETCS consortium  
Europa

**Abstract:** This document give a description of the process to be applied in the OpenETCS project. It gives a description of the activities to specify and design a critical system in a first part. The second part presents an abstract description of the case study issued from subset 26.

**Disclaimer:** This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

<http://creativecommons.org/licenses/by-sa/3.0/>

# Table of Contents

1	Introduction.....	4
2	Reference documents .....	4
3	Conventions.....	4
4	Glossary .....	5
5	OpenETCS process.....	5
5.1	Motivation .....	5
5.2	Overall description .....	6
5.3	System specification.....	7
5.4	Model definition .....	9
5.5	Abstract Code .....	10
5.6	Safety activities .....	10
5.7	Verification and Validation.....	11
6	OpenETCS case study .....	11
6.1	Aim of the OpenETCS project .....	11
6.2	High level description of the case study .....	12
6.3	Environement and abstract architecture .....	12
6.4	Safety properties .....	12
7	Goals .....	12
7.1	Goal 5: Provide a subset of the safety case .....	12
7.2	Goal 6: Promote OpenETCS.....	13
8	Requirements.....	13
9	Verification, Validation and Safety issues .....	13
10	Language and formalism .....	13
11	Tool chain.....	14

## Figures and Tables **Figures**

Figure 1. Main process .....	8
Figure 2. Safety analyses .....	8
Figure 3. Architecture .....	12

## **Tables**

## 1 Introduction

The purpose of this document is to describe, for the OpenETCS project, the activities of specification and design. However the activities of verification and validation are not in the scope of this document and will be described in `%%WP4/D4.x.x%%`.

These activities shall follow the requirements of EN 50126 and EN 50128 and reflect usual activities for the development of railway critical systems (see D2.1.0 and D2.2.0).

This document contents two parts :

- the description of the process to applied in the OpenETCS project
- the abstract description and the limit of the case study

## 2 Reference documents

- CENELEC EN 50126-1 — 01/2000 — *Railways applications — The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) — Part 1: Basic requirements and generic process*
- CENELEC EN 50128 — 10/2011 — *Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems*
- CENELEC EN 50129 — 05/2003 — *Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling*
- FPP — *Project Outline Full Project Proposal Annex OpenETCS – v2.2*
- SUBSET-026 3.3.0 — *System Requirement Specification*
- SUBSET-076-x 2.3.y — Test related ERTMS documentation
- SUBSET-088 2.3.0 — *ETCS Application Levels 1 & 2 - Safety Analysis*
- SUBSET-091 2.5.0 — *Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2*
- CCS TSI — *CCS TSI for HS and CR transeuropean rail has been adopted by a Commission Decision 2012/88/EU on the 25th January 2012*

## 3 Conventions

The requirements are prefixed by “R-zz-x-y”, and are written in a roman typeface, where “R” stands for “Requirement”, “zz” identifies the source document, “x” is the version number and “y” is the identifier of the requirement. All the text written in italics is not a requirement: it may be a note, an open issue, an explanation of the requirements, or an example.

The placeholder “`%%xxx%%`” is used to indicates that a paragraph or section is not finished, to be defined or to be confirmed.

## 4 Glossary

**API** Application Programming Interface

**FME(C)A** Failure Mode Effect (and Criticity) Analysis

**I/O** Input/Output

**OBU** OnBoard Unit

**QA** Quality Analysis

**RBC** Radio Block Center

**RTM** RunTime Model

**SIL** Safety Integrity Level

**THR** Tolerable Hazard Rate

**V&V** Verification & Validation

## 5 OpenETCS process

### 5.1 Motivation

This document describes the process to be applied during the OpenETCS project to achieve the following goals of the OpenETCS project :

#### **A formal reference specification for the ETCS requirements and architecture**

The first goal of the project is to propose a formalization of a subset of the on-board subsystem, as defined in the SUBSET-26.

The purpose of the formalization is:

- to enhance the understanding of modelled subset;
- to allow formal analysis of the modelled subset;
- to be able to animate the model for testing an analyzing purpose;
- to provide information on the completeness and soundness of the SUBSET-26;
- to be used as a reference formal specification for the implementation of an OBU (by the OpenETCS project team and by industrial actors);
- ...

The output of this goal is a formal specification, understandable by many tools (SCADE, Simulink, B tools, OpenETCS tool chain. . . ) that can be given to all railway actors, and if possible associated to SRS documents in the ERA database. The final goal is that industrial actors work with this formal specification instead of natural language specification.

### **Definition of a tool chain and process/methodologies for developing on onboard software that can fulfill the EN 50128 requirements**

The process and the associated tools, shall provide a certifiable product. For this purpose all the step of the process and the choice of methods and tools shall be justified to ensure a safe approach to build a system.

The full safety process needed for the OpenETCS to be *certifiable* according to CENELEC 50126 and 50128 shall be described in details. This safety plan will detail precisely which activities are required or not, why, and the choices that are made that allows to claim that safety is guaranteed.

### **Building an implementation of the subset of an onboard ETCS using the system model and the tool chain**

It is the demonstration that all the work done in the OpenETCS project is coherent, and that the tool chain is operational.

The output is the result of an implementation for the ETCS requirements and architecture which can be used by the industrial as references.

### **Define the safety properties at the model level**

In order to comply the CENELEC standards, it is necessary to conduct safety activities to identify errors and anomalies in the process. One important step for this is to define safety properties which are on the same level than the formal model.

These safety properties:

- will be used for the validation of the model itself;
- will be used as reference proof obligations for the subsequent activities.

Because the full design, development, validation and safety analysis process for a SIL4 OBU is a huge task far beyond the project possibilities, the full safety activities will not be conducted on the whole subsystem (see below). Nevertheless the safety process description shall be complete according to CENELEC requirements.

However this safety analysis is out of the scope of the OpenETCS project. SUBSET-088 2.3.0 and SUBSET-091 2.5.0 will provide elements of safety analysis.

## **5.2 Overall description**

%%highlevel description of the full process for OpenETCS : main step as defined in the synthesis of requirement. %

%%To check there is no conflict with req on CENELEC (D.2.2) and QA plan%%

%%Elements are issue form req\_synthesis of D2.6, D2.7, D2.8, D2.9%%

In order to pursue this goals, the development cycle for the project may be presented as follow. The proposed process shall comply the CENELEC standard EN 50126, EN 50128 and EN50129. References to the chapter of these standard will be given in the sequel. However proof that the process satisfies the requirements of the standard is out of the scope of this document and shall



be managed by the Safety Case (WP4). Amount the requested quality assurance Plan request by EN 50128, the current document only contributes to the definition of the life-cycle model by giving a description of each step of the process (activities, input and output documents, entry and exit of each activity).

Fig. 1 shows the main part of the development process. This process may be seen as a “triple-V”. The smaller V corresponds to the development of the formal model.

It starts by the SRS which is not part of the project (SUBSET-26), then outlines the boundaries and the applicable requirements from the SUBSET-26 that will be used in the formal model.

%%to link to system development phase (see EN50129)%%

The next step is the creation of the formal model itself. Because this model is executable, it can be validated as itself, thus the first “closing branch” of the V.

%%to link to software design phases : SW requirement, SW Architecture and Design, SW component Design (see

From the model can be derived some “abstract” code. The word “abstract” is used to emphasize that this code is not necessarily capable of running of a full SIL4 platform. This code can be validated in the second “closing branch”, possibly using some of the work done in the first branch.

%%to link to software design phases : SW component implementation Design (see EN50128)%%

A project demonstrator may be derived from this code (or may be the “abstract” code itself).

The third “closing branch” corresponds to the production of code capable of running on a given SIL4 platform, and the associated validation activities. This is not part of the project.

The yellow boxes corresponds to activities that should be covered completely in order to produce a certifiable product, but of which only a subset will be conducted in order to demonstrate the capabilities of the product.

Fig. 2 shows activities that are needed for the safety analyses. It should be considered in parallel of the descending branch of the V, but has been put on a separate diagram for the sake of clarity.

High level safety properties are provided, which must be refined side-to-side with each step on the descending branch of the V. These properties are then used for the safety analysis of the model. The validation (safety analyses) boxes are yellow because the full activity will not be conducted. Only a subset of the safety properties will be proved.

Regarding the process, WP2 shall issue (through this document) the requirements on V&V, including safety activities. From these requirements, WP4 shall propose the corresponding plans (Safety, Verification and Validation). This plans will then be reviewed by WP2 to check conformance to the requirements. The reviewed plans will then be used as reference for the activities of the WPs.

### 5.3 System specification

%%To develop%%

*Comment. This section as to define the activities links to the system specification and model.*

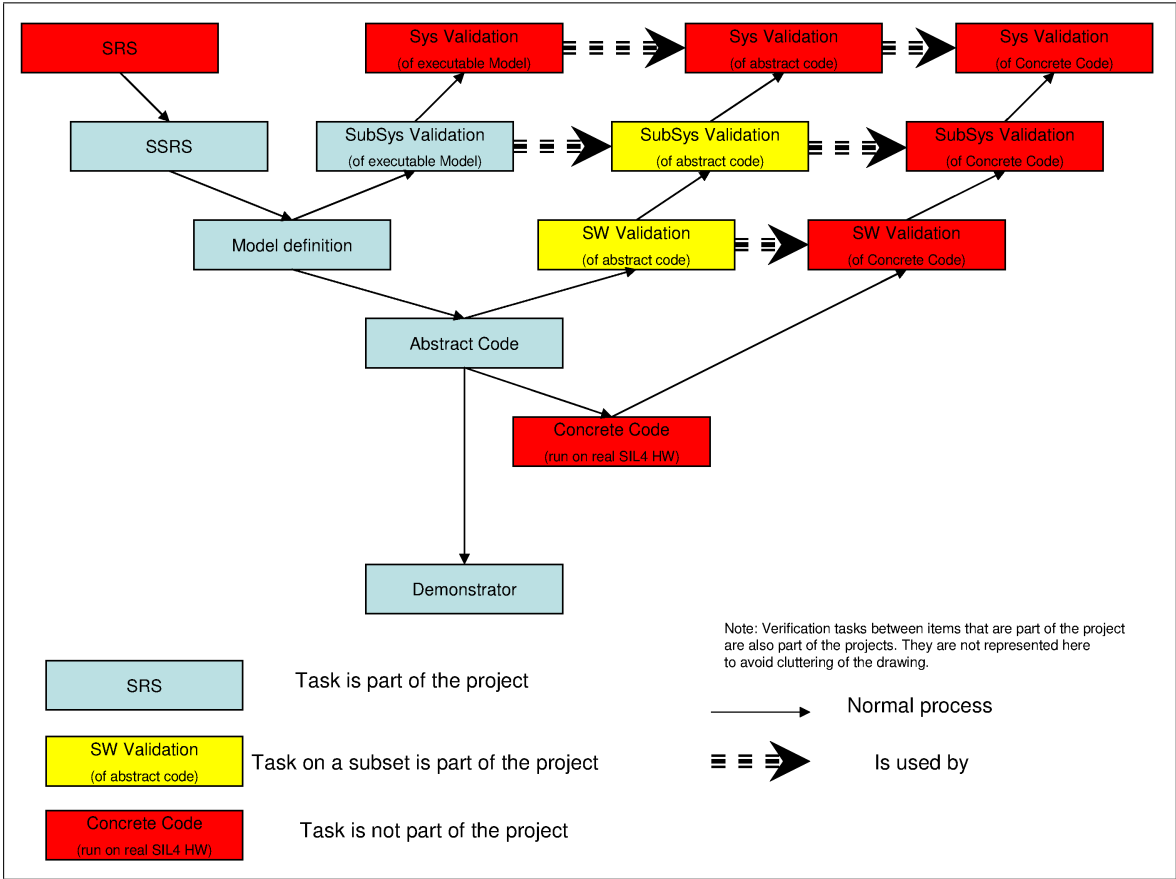


Figure 1. Main process

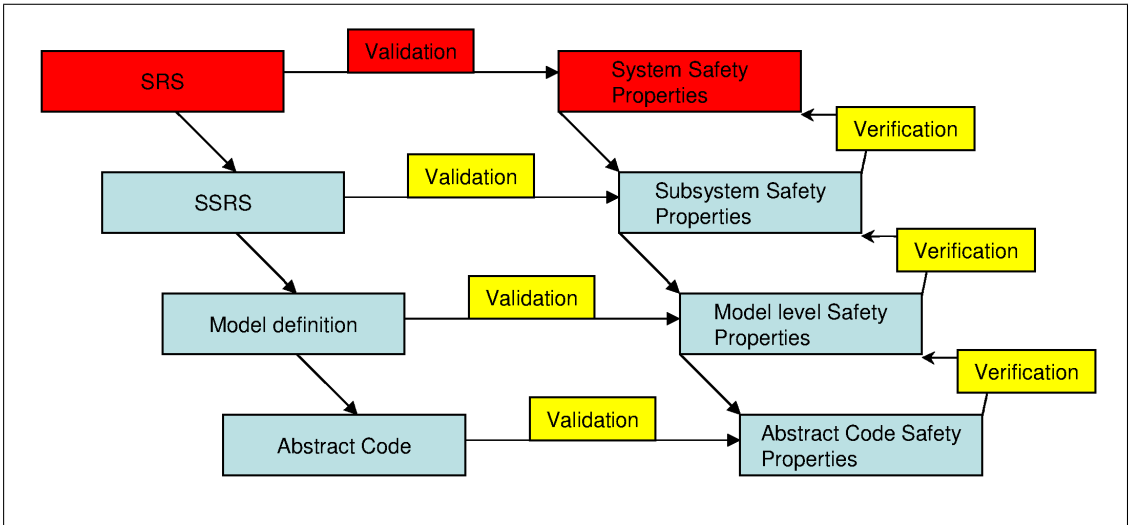


Figure 2. Safety analyses

*This step is not explicitly defined in EN 50128 but is defined in EN 50129. However EN 50128 give the expected output from this step for the software activities : System Requirements Specification, System Safety Requirements Specification, System Architecture Description, External Interface Specifications*

*Open Issue. To discuss with all partners : Do we need a SSRS ? This is expected by EN50129.*

*S. Baro comments (15/02/2013) :*

*SSRS*

*We had a un-conclusive discussion on the necessity to insert a SubSystem Requirement Specification between the SRS (subset 26) and the formal model. The reason of this is that the model we want corresponds to a subsystem (part of the OBU), but the SRS corresponds to the whole system. The SRS also does not provide any functional architecture, and we think it is necessary to provide one. In the other hand, it adds one document between the SRS and the model. The question is thus to know if this document will remove more errors than it will add. Proposal: To provide a SSRS which contains: - a formal or semi-formal functional architecture of the OBU part which will be modeled, with function "boxes" and I/O "arrows"; - the requirements allocated to the functions and I/O, rewritten but still in natural language; - the tagging Safety/Non Safety of these requirements. This document should be seen as an important step of the modeling process, and would be under the responsibility of WP3.*

## 5.4 Model definition

%%To have a discussion with Sylvain Baro on his choice of step for the process%%

*Comment. Some requirements to take into account :*

**R-WP2/D2.3.0-X-1** The model shall be consistent with the SRS level and shall yield as few as possible “design choices”.

**R-WP2/D2.3.0-X-1.1** Traceability with the SRS shall be provided.

**R-WP2/D2.3.0-X-1.2** Each interpretation of the SRS shall be indicated precisely.

**R-WP2/D2.3.0-X-1.3** Each SRS requirement not formalized in the model (e.g. allocated to RBC) should be traced and justified.

**R-WP2/D2.3.0-X-2** When the boundary of the formalized subsystem corresponds to a FIS or FFFIS, the Functional Architecture shall try to comply to it even when it is not mandatory.

**R-WP2/D2.3.0-X-3** The Functional Architecture shall split the KERNEL into independent functions.

**R-WP2/D2.3.0-X-4** The Functional Architecture shall identify a subset of these functions that will be modeled.

**R-WP2/D2.3.0-X-5** The Functional Architecture shall allow a universal method of adding function (modularity).

#### 5.4.1 Software requirements

%%To detail according § 7.2 of EN 50128%%

#### 5.4.2 Software architecture and design

%%To detail according § 7.3 of EN 50128%%

#### 5.4.3 Software component design

%%To detail according § 7.4 of EN 50128%%

#### 5.5 Abstract Code

%%To detail according § 7.5 of EN 50128%%

#### 5.6 Safety activities

%%this activity is not explicitly detailed in 50128 (except some task in different activities) but in 50126 and 50129

*Comment. from D.2.6,7,8,9 :*

*Justification. Side to side with the model (which should be a dynamic model), should lay a set of static safety properties on the model. The higher level properties will be provided by the WP2 (equivalent to a preliminary hazard analysis) from the SUBSET-91 document, They will be refined by the safety analysis process (WP4) into properties of the same level than the model. The process of doing so shall be described in the Safety Plan.*

*This will provide Safety Properties on the model (or Dread Events). The lower level Safety Properties/ Dread Events shall address variables, state and interfaces used in the formal model.*

*Formal proof would then be used to prove that the OpenETCS model never enter a Dread State, as long as the other subsystem (RBC, communication layer...) fulfill their own safety properties (axiom describing the environment).*

**R-WP2/D2.3.0-X-6** A safety plan shall be provided and complied with.

**R-WP2/D2.3.0-X-7** The Functional Architecture shall identify the Vital and Non Vital functions.

*Comment. MPD : Identification of Vital and non vital can be done only if the safety analysers have provided safety properties and have allocated them to functions.*

**R-WP2/D2.3.0-X-8** The subsystem shall be compatible with the THR required in the SUBSET-091.

**R-WP2/D2.3.0-X-9** The safety analysis shall consider the Dread Event of the SUBSET-091, restricted to the scope of the subsystem.

**R-WP2/D2.3.0-X-10** The model-level safety properties shall be written in a formal language.

*Open Issue. To discuss with all partners : what is expected on this activity in the process.*

*S. Baro comments (15/02/2013) :*

*Safety*

*Are safety activities required in this project? The project require "certifiability" of some items (toolchain? model?) and compliance to 50128. For the toolchain, it is quite clear what it means, but for the model it is much more complicated. Is it really required for the model? If safety activities are required on the model, I think it makes no sense to refer only to 50128: it should refer to 50126 and 50129 too (excluding the hardware part which is not in the scope of the project). This pulls system safety analysis, safety properties,... but provides the initial properties required for formal proof on the model (once refined through system safety analysis). Proposal: The "Safety" WP provides a safety case concept and safety plan according to Merlin's document and to the requirements. It is not realistic to expect that the full safety case will be provided for OpenETCS, but I think it will be useful to conduct a sample of the tasks, or all tasks but on a sample of the model. The higher level properties will be provided by subset 91, and refined by the safety analysis to properties on the model (I provided an example on how to do this in another document). Please note that even covering the whole subset 91 properties is certainly not sufficient to ensure the safety of the model. Question: who will provide the manpower for safety activities? WP4?*

## 5.7 Verification and Validation

The Verification and Validation activities have to be planned on the whole process according the requirement of EN50128 § 6.2 and 6.3.

This plan is out of the scope of the document and shall be defined in the WP4 process.

%%To check the existing draft on this subject%%

## 6 OpenETCS case study

%%This section is intentionnally empty for the moment : %%

%%it will be completed when the document provided by Alstom on API will be available.%%

### 6.1 Aim of the OpenETCS project

*Comment. The goal of The OpenETCS project is to provide a formal model of the On board Unit from the Subset 26 specification.*

*The following sections are going to give a high level description of this case study and expected elements.*

*Detailed specification of the system will be given during WP3 activities.*

## 6.2 High level description of the case study

high level description of the subset + link to reference documentation (subset 26)

**R-WP2/D2.3.0-X-11** The model shall comply all OBU ETCS mandatory requirements for level upto 2, in the functional perimeter provided by the Functional Architecture.

**R-WP2/D2.3.0-X-11.1** The model shall comply the OBU part of SUBSET-26-3.3.0.

**R-WP2/D2.3.0-X-11.2** The reference ETCS baseline shall be modified only by project decision, according to the QA Plan.

**R-WP2/D2.3.0-X-11.3** All divergences against the chosen baseline shall be documented and tracked, according to the QA Plan.

## 6.3 Environment and abstract architecture

high level description of the environment of the system and main function

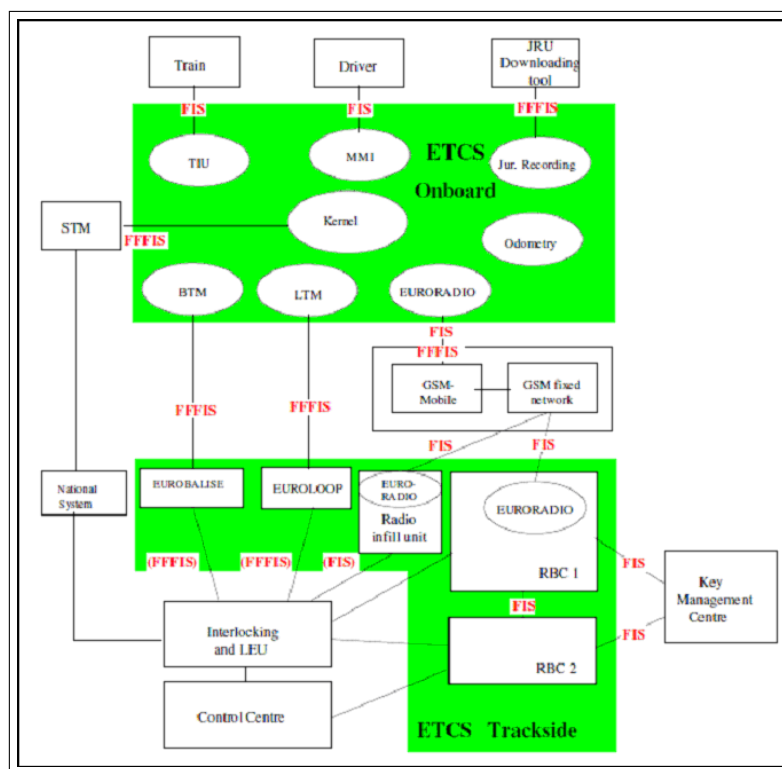


Figure 3. Architecture

## 6.4 Safety properties

reference document subset 091 to the list of safety properties