openETCS

OETCS/WP2/D2.3.0 – 00/00

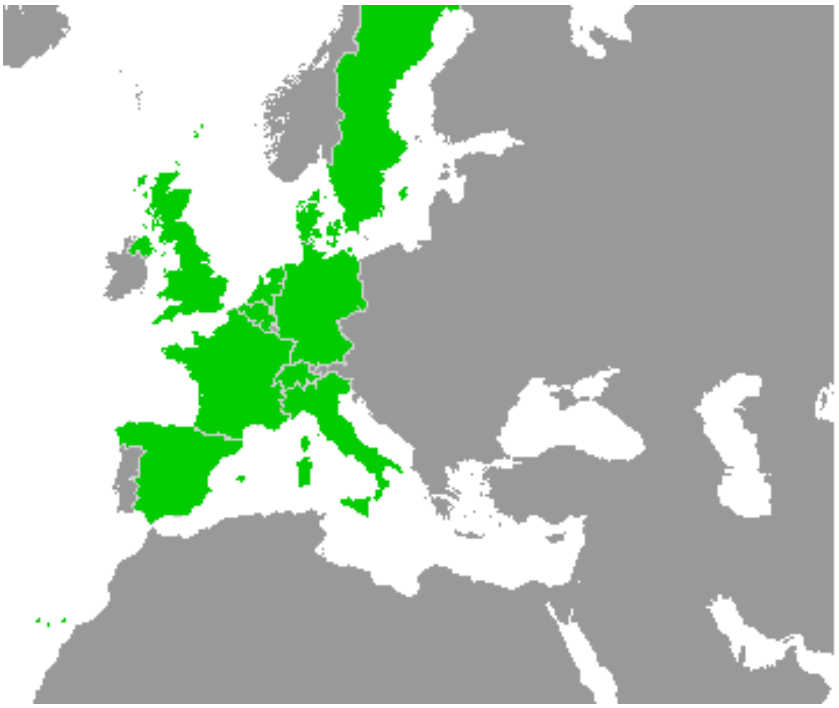
ITEA2 Project
2012 – 2015

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 and Matthias Güdemann 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

Matthias Güdemann

Systerel

Definition

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.

Table of Contents

Figures and Tables **Figures**

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 safety, verification and validation are not in the scope of this document and will be described in WP4.

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).

1.1 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 justifyed 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 activies.

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.

1.2 Contents of this document

As the Quality Plan D1.3.1 focusses in means to apply during the OpenETCS project (as for example opensource approaches or Scrum organization) the aim of this document is to define the main step of the OpenETCS necessary to produce a certifiable system according to CENELEC standard.

Then this document focusses :

- on the description of the mandatory step of a lifecycle to design a critical system according to CENELEC standard
- on the abstract description of the system to design during the OpenETCS project

2 Reference documents

- CENELEC EN 50126-1 — 01/2000 — *Railways applications — The specification and demonstration of Reliability, Availability, Maintenability 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*
- Project Quality Assurance Plan – D1.3.1

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 Overall description

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

In order to pursue the goals given in the introduction, the development cycle for the project may be presented in this document.

The two most important goals of the SW development lifecycle model of CENELEC EN 50128 [**?**] are the separation of the lifecycle into well-defined phases and the focus on the production

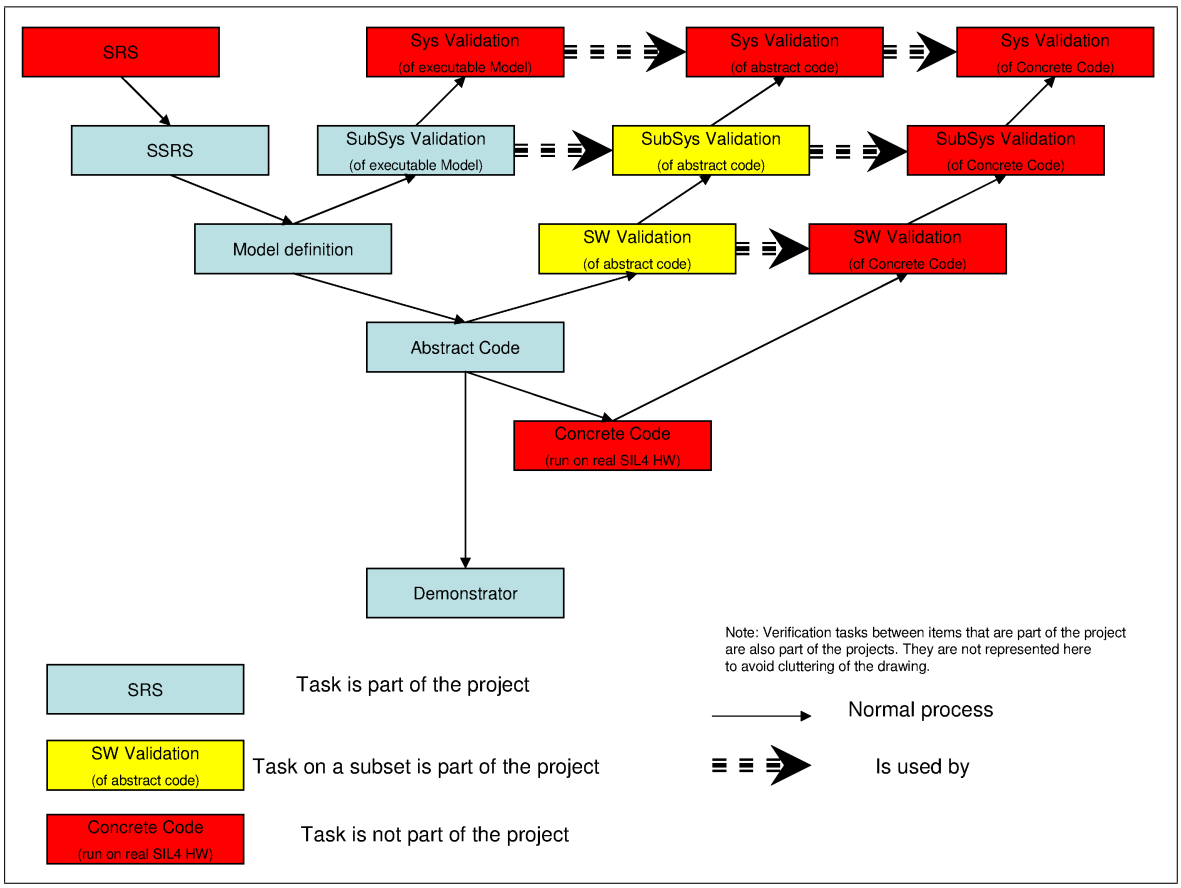


Figure 1. Main process

and recording of all documentation of the development process. To achieve this, an appropriate software lifecycle model must be used and appropriate roles and responsibilities must be assigned. For this, the standard specifies several constrains which must be fulfilled.

Fig. 1 shows the main part of the development process in an abstract view. 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. This step is described in EN50129 as system development phase.

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. This step has to been linked with the following phases described in EN50128 :

- Software requirement
- Software architecture and design
- Software component design

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. This step is described as software component implementation design in EN50128.

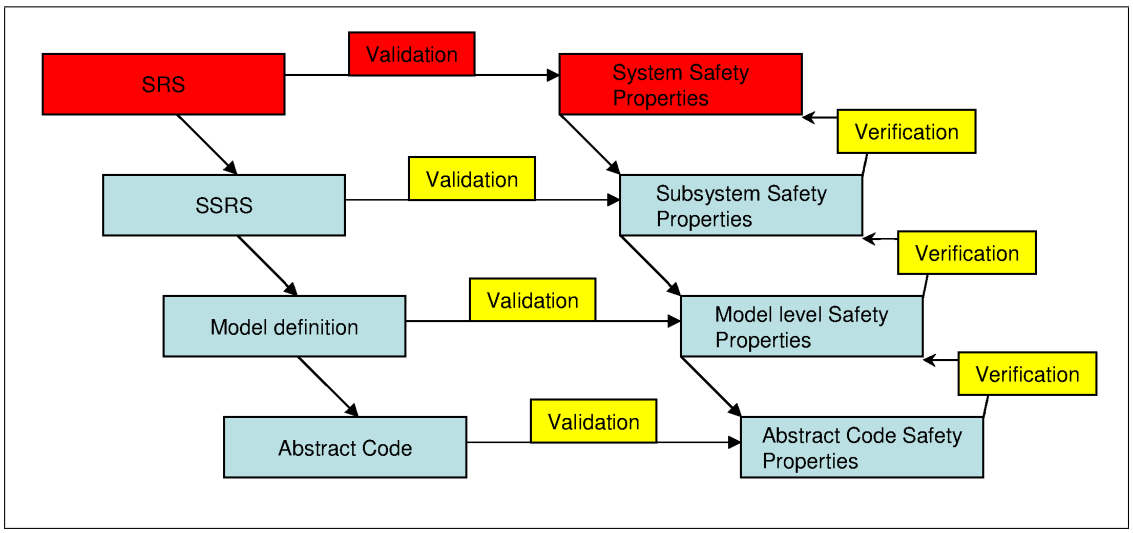


Figure 2. Safety analyses

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.

The proposed process shall comply the CENELEC standard EN 50126, EN 50128 and EN50129, expecially the proposed lifecycle of 3.

It consists of the SW planning phase in the beginning, the SW assessment phase at the end and the following development phases:

- System Development Phase
- SW Development Phases
  - SW Requirements Phase
  - SW Architecture and Design Phase
  - SW Component Design Phase
  - SW Component Implementation Phase
- SW Test / Validation Phases
  - SW Validation Phase
  - SW Integration Phase

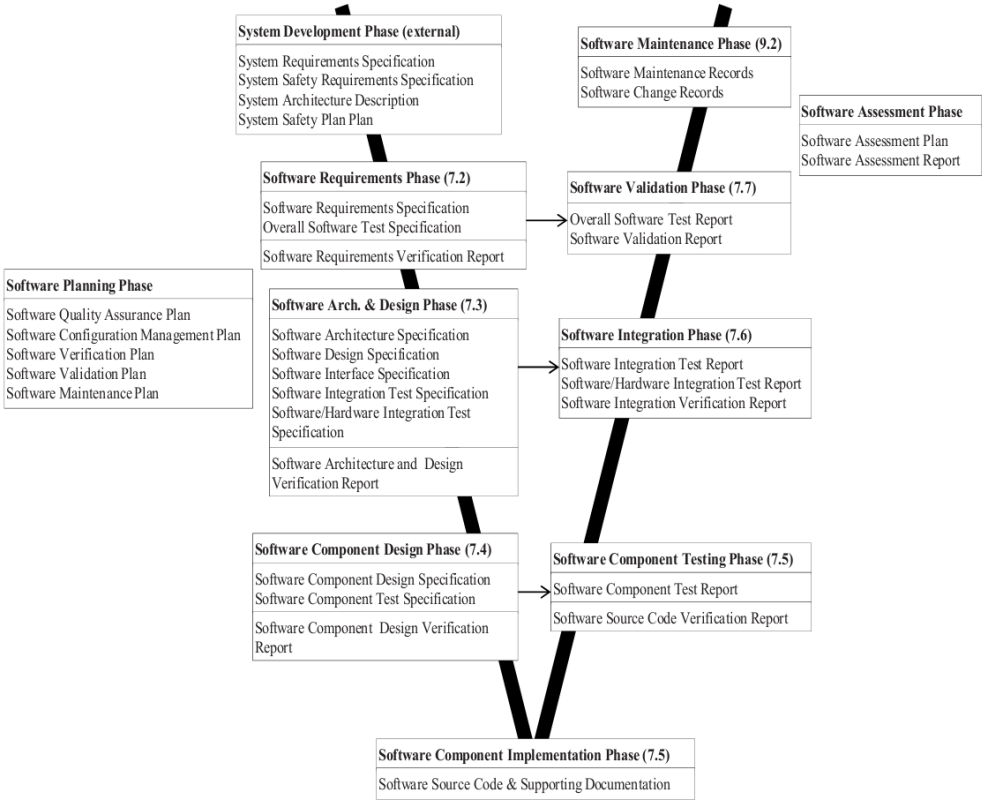


Figure 3. General Development Lifecycle [?]

– SW Component Testing Phase

Software planning phase is defined by WP1 in the Quality Assurance Plan. Software Test / Validation phase is defined by WP4 in Validation Plan. Software Verification activities are defined by WP4 in Verification Plan.

Safety activities are described in EN50126. However proof that the process satisfies the requirements of the standard is out of the scope of this document and shall be manage by the Safety Case (WP4).

5.2 System Development Phase

%%To develop%%

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

This step is not explicitly defined in EN 50128 but is defined in EN 50129. However EN 50128 gives 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 betwen 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.

Objectives:

The aim of this phase is to have a clear definition of the system to design :

- a set of system requirements which discribe the functionality of the system as the expected results concerning performance, maintenability, safety, fiability,...
- the description of the architecture of the system
- interface descriptions

Safety activities are necessary to define the safety requirements of the system and to defined which functions are tagged Vital or Non-Vital.

Documents:

The documents to produce in this phase are :

- the system safety plan explains the overall approach to ensure safety in the developed system
- the system requirements specification describes all requirements of the system
- the system safety requirements specification focusses on the safety aspects
- the system architecture specification and SW / HW interface definition which specify how the SW and the HW interact and the location of the boundary between the two

Detailed Description:

Figure 4 describes an iteration in this phase in more detail.

The first phase is the formalization of the safety requirements, this it iterated until internal consistency is ensured. The next phase is the formalization of the system requirements, analogously with an iteration to ensure their consistency.

Both sets of requirements are combined in the requirement integration phase. They shall be transformed into a common formal specification format if necessary. The consistency of the

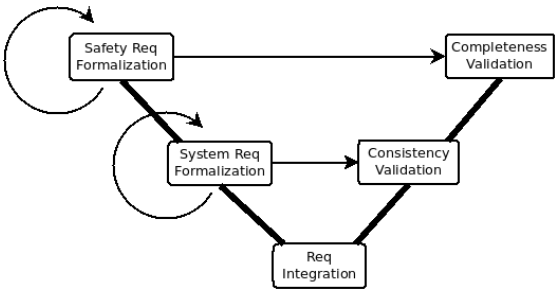


Figure 4. Sub Process in System Development Phase

combination is verified in the next phase and finally the completeness of the requirement wrt. informal specification. Any deviation from the consistency of the combined requirements or from the completeness shall be documented and the phases reiterated until consistency and completeness is achieved.

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).

5.3 Model definition

5.3.1 SW Requirements Phase

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

Objectives:

In this phase, the system requirements shall be declined to take into account software constraints.

In particular software requirements specification shall give a description of all the input/output of the software, a description of the operational modes and behaviour. It shall provides all the element to have testable requirements. All function to perform shall be clearly identify. All existing constraints of the constraints between HW and SW will be taken into account (cf. §7.2.1.1).

Documents:

The documents to produce in this phase are :

- the SW requirements specification
- the overall SW testing specification will provide the detailed approach to test the developed SW, concretizing the approach in the SW testing plan
- the SW requirements verification report will document the results of the verification of the SW requirements specification wrt. the criteria specified in §7.2.4.22 (cf. §7.2.3).

Responsible:

RQM

Detailed Description:

%%To Be Confirmed%%

5.3.2 SW Architecture and Design Phase

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

Objectives:

In this phase a SW architecture shall be developed which allows to meet the SW requirements and the necessary safety requirements without introducing unnecessary complexity. In this phase there shall also be an evaluation of the HW / SW interaction, its influence on the safety aspects of the system and the valuation of the usage of already existing SW. It shall also ensure the testability and the appropriateness for formal proofs of the resulting SW, in particular by minimizing the complexity and the size of the safety relevant parts (cf. §7.3.1.1 to 7.3.1.5).

Documents:

In this phase the following documents shall be produced:

- the specifications for the SW architecture
- the SW design and the SW interface
- the specification for the SW integration test and for the SW / HW integration test

- the SW architecture and design verification report will document whether this phase has been finished in accordance with the standard (cf. §7.3.3)

Responsible:

DES, VER, INT

Detailed Description:

The details of the sub-process of the SW architecture and design phase is shown in Figure 5.

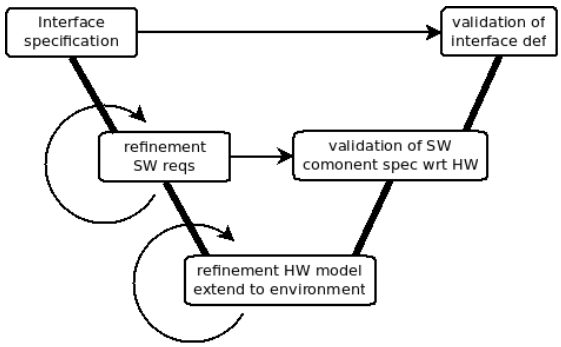


Figure 5. Sub Process in SW Architecture and Design Phase

%%To Be Confirmed%%

5.3.3 Software Component Design Phase

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

Objectives:

This phase shall develop a low level specification for each of the SW components which is correct wrt. requirements of the SW design specification and of the SW component design specification (cf. §7.4.1.1, §7.4.1.2).

Documents:

%%To Be Confirmed%%

Responsible:

DES, VER

Detailed Description:

%%To Be Confirmed%%

5.4 Abstract Code

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

5.4.1 Software Component Implementation Phase

%%To Be Confirmed%%

Open Issue. Manual versus automatic code generation ?

Shall be replaced by automatic code generation from formal models using refinement techniques.

5.4.2 Software Component Testing Phase

Open Issue. Verification step ?

5.4.3 Software Integration Phase

Open Issue. Verification or validation step ?

5.5 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?

5.6 Verification and Validation

Each of the SW development phases shall have an appropriate test / validation counterpart, as illustrated in the V form of the lifecycle.

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.%%

Comment. From QA :

The EVC (European Vital Computer) is the heart of the ERTMS onboard system. This safety computer implements the functions of the SRS subset 026 of UNISIG (for SRS versions beginning with baseline 3, published by ERA) in order to guarantee the safety of the train movements. The OpenETCS scope of application is related to the only EVC part of whole ERTMS system. The Track-side part of the ETCS (the Radio Based Control) is excluded from the project activities, and only considered through its interfaces with the On-Board part of ETCS.

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.

Detailled 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 Environement and abstract architecture

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

%%To Be Confirmed%%

6.4 Safety properties

reference document subset 091 to the list of safety properties

%%To Be Confirmed%%

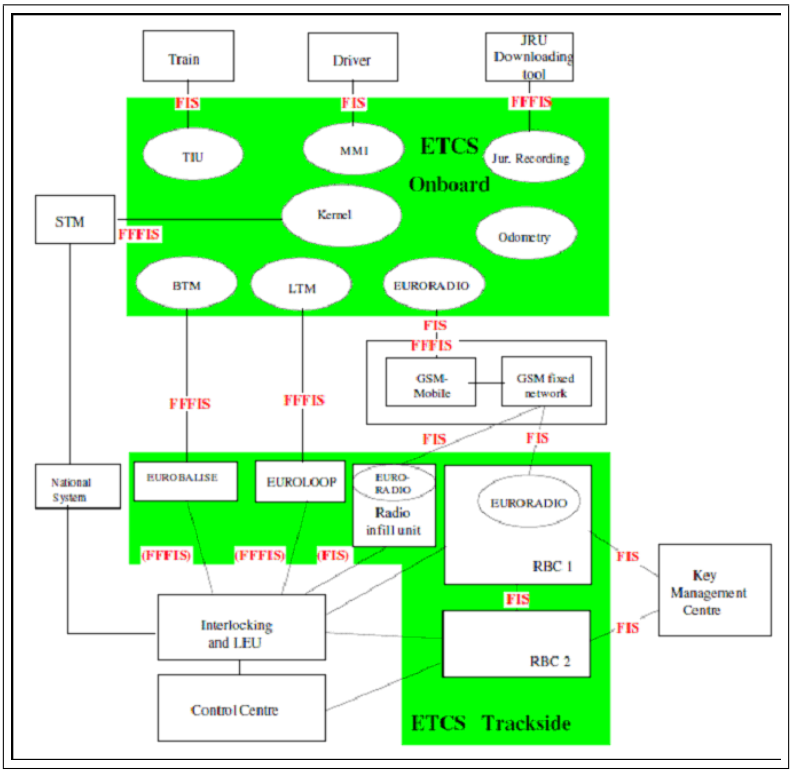


Figure 6. Architecture