OETCS/WP4/D4.4V0.1

openETCS

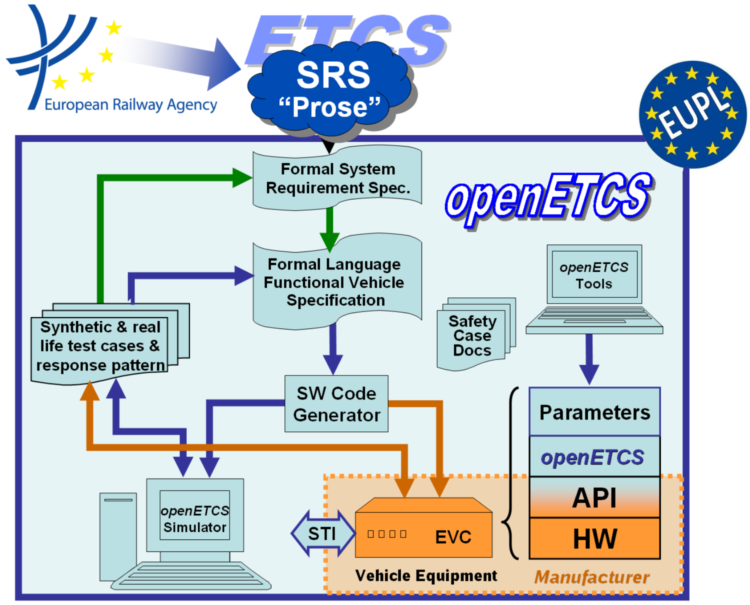
ITEA2 Project
Call 6 11025
2012 – 2015

Work-Package 4: “Verification & Validation Strategy”

openETCS Final Report on Verification and Validation

Marc Behrens and Hardi Hungar

December 2015



Funded by:

Federal Ministry
of Education
and Research

République Française
Ministère de l'Enseignement Supérieur et de la Recherche

Investissements d'avenir

Région de
Bruxelles-
Capitale

Gobierno de España
Ministerio de Industria, Energía y Turismo

This page is intentionally left blank

Work-Package 4: “Verification & Validation Strategy”

OETCS/WP4/D4.4V0.1
December 2015

openETCS Final Report on Verification and Validation

Document approbation

Lead author:	Technical assessor:	Quality assessor:	Project lead:
location / date	location / date	location / date	location / date
signature Marc Behrens (Deutsches Zentrum für Luft und Raumfahrt e.V.)	signature [assessor name] ([affiliation])	signature Jan Welte (TU Braunschweig)	signature Klaus-Rüdiger Hase (DB Netz)

Marc Behrens and Hardi Hungar

DLR
Lilienthalplatz 7
38108 Brunswick, Germany

Final Report

Prepared for openETCS@ITEA2 Project

Abstract: This document summarizes the approach, scope and result of the verification and validation activities in the project openETCS.

Modification History

Version	Section	Modification / Description	Author
0.0	all	initial	Marc Behrens
0.1	all	revision and addition	Hardi Hungar

Table of Contents

Figures and Tables

Figures

Tables

1 Introduction

According to [1, 3.1.48], verification is an activity to check whether the output of a development phase meets the requirements. This concerns formalities, traceability, and, w.r.t. the main content, completeness, correctness and consistency. Within openETCS, examples of each kind of verification have been performed. Thereby, also new methods and tools have been evaluated and adapted.

Validation concerns the compliance of the end result of the development with the user requirements. This has been done employing the demonstrator of the EVC software.

This document summarizes the activities described in more detail in separate reports. It explains how these separate activities fit into the development process of openETCS as defined in the deliverable D2.3a.

Most verification activities are actually reviews of documents (or even programs). For general review activities, a process has been defined in [2].

2 Verification and Validation in the Development Lifecycle

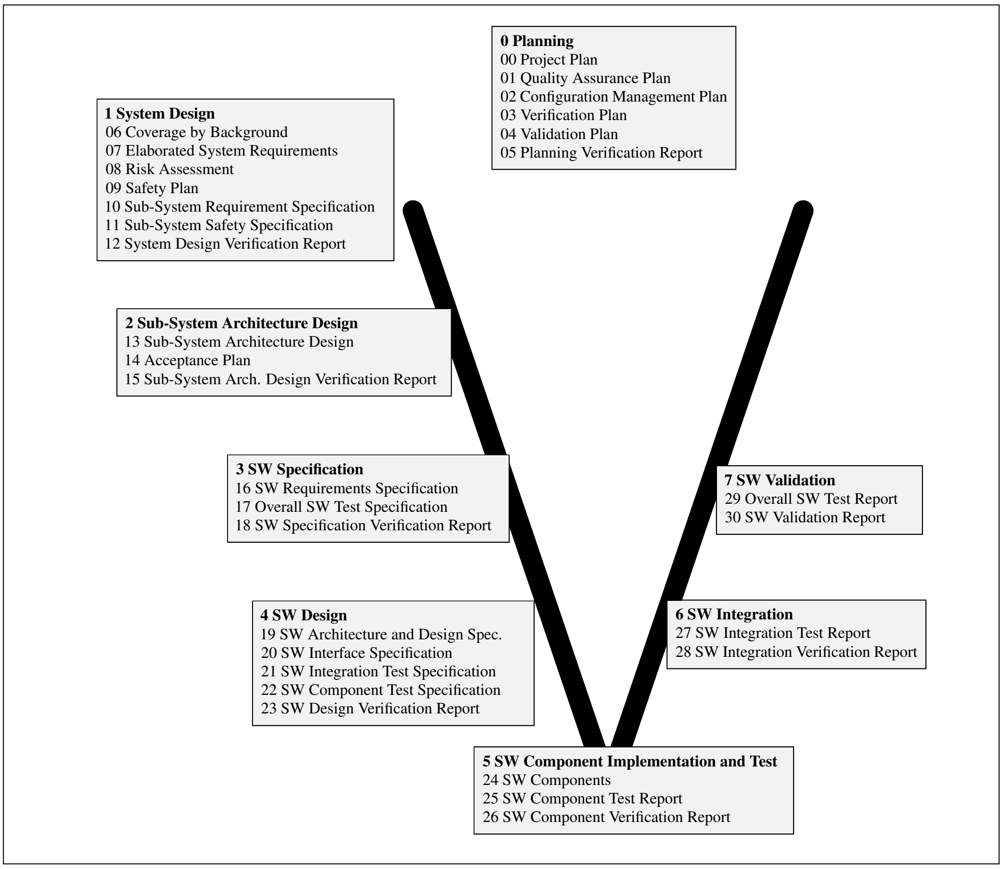

0 Planning
00 Project Plan
01 Quality Assurance Plan
02 Configuration Management Plan
03 Verification Plan
04 Validation Plan
05 Planning Verification Report
1 System Design
06 Coverage by Background
07 Elaborated System Requirements
08 Risk Assessment
09 Safety Plan
10 Sub-System Requirement Specification
11 Sub-System Safety Specification
12 System Design Verification Report
2 Sub-System Architecture Design
13 Sub-System Architecture Design
14 Acceptance Plan
15 Sub-System Arch. Design Verification Report
3 SW Specification
16 SW Requirements Specification
17 Overall SW Test Specification
18 SW Specification Verification Report
7 SW Validation
29 Overall SW Test Report
30 SW Validation Report
4 SW Design
19 SW Architecture and Design Spec.
20 SW Interface Specification
21 SW Integration Test Specification
22 SW Component Test Specification
23 SW Design Verification Report
6 SW Integration
27 SW Integration Test Report
28 SW Integration Verification Report
5 SW Component Implementation and Test
24 SW Components
25 SW Component Test Report
26 SW Component Verification Report

Figure 1. openETCS Development Lifecycle

Fig. 1 is an overview of the openETCS development lifecycle, taken from D2.3a. It depicts the process for a complete development of the EVC software, of which a part has been performed within the project. Verification, resp., validation, has to be done in each of the phases of the development.

3 Overview of Verification and Validation Activities

Some sample notes are included in the subsections. To be checked for correct assignment to the phases, extended to become self-contained summaries of the activities with results and contributions. Note: Also evaluating a new verification method is a contribution to be mentioned, if this is a side or main effect of the activity. Do not forget to add yourself as an author if you contribute.

3.1 Verification and Validation in the Planning Phase

There have been reviews of the planning documents compile a list.

Template Start

3.1.1 Template Verification [Validation] of [what]

Contributing project partners

Process step

Object of verification

Available specification

Objective

Method/Approach

Means/Tools

Results

Observations/Comments

Conclusion

Template End

3.2 Verification and Validation in the System Design Phase

3.2.1 Verification of Chapter 5 of Subset 026 (TWT)

Contributing project partners

The work has been performed by TWT.

Process step

This activity is part of the verification of the Elaborated System Requirements which are based on Subset 026 [3]. It contributes to the System Design Verification Report (1-12). In formalizing and analyzing the procedures it findings contribute also to the definition of the Elaborated System Requirements themselves (1-07).

Object of verification

The object of verification are the procedures defined in Chapter 5 of Subset 026 [3, 5]. *NN* of the ¿25? procedures have been analyzed.

Available specification

The procedures are checked for consistency. They are not checked against an external specification.

Objective

The main objective w.r.t. verification is check the procedure definitions for consistency and some sanity conditions. A by-product are formalizations which can enter the Elaborated System Requirements (1-07).

Method/Approach

The control flow of the procedures is modeled with colored Petri nets (CPNs) in the tool [**?**]. Each model is checked independently by a second person. The necessity of formalization coming with the modeling uncovers inconsistencies in textual specifications. With the help of the simulation and checking facilities of the CPN tools, sanity conditions on the models are checked.

Means/Tools

The CPN tools are ...

Results

The modeling and analysis uncovered 36 inconsistencies, ambiguities and gaps in the Subset 026 which were reported in [**?**]. to be revised/completed

Observations/Comments

Conclusion

Missing procedures? The numerous specification findings illustrate the need for validating the specification. CPNs are well-suited to model the behavioral aspects described in Subset-026 chapter 5. The size of the model clearly indicates the complexity of the procedures, even at the current level of abstraction. The main benefit comes from the activity of formalization itself, and of incomplete, but valuable, simulations.

3.3 Verification and Validation in the Sub-System Architecture Design Phase

The DLR verified the Sub-System Architecture Design citations. ¿correct phase?

3.4 Verification and Validation in the SW Specification Phase

3.5 Verification and Validation in the SW Design Phase

Model-based testing applied to design models ¿U Bremen?

3.6 Verification and Validation in the SW Component Phase

- Dedicated tests on single components ¿DB?
- Formal code verification (FRAMA C on the bitwalker)

3.7 Verification and Validation in the SW Integration Phase

Automatized integration tests on the SW components.

3.8 Verification and Validation in the SW Validation Phase

There have been validations on

- the integrated software within the ¿SCADE simulation environment?, subjecting the SW with a simulated environment to operational use cases.
- an integration of the SW on a reference hardware, applying operational use cases.

4 Conclusion

References

[1] Railway applications – Communication, signalling and processing systems – software for railway control and protection systems. Norm EN 50128:2011, CENELEC, Brussels, Belgium, 2011.

[2] Ainhoa Garcia. Project quality assrance plan - review process. Technical Report D1.3.1, OpenETCS, July 2013.

[3] UNISIG. SUBSET-026 - System Requirements Specification. Technical Report 3.3.0, ERA, March 2012.