

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

 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	signature	signature	signature
Marc Behrens (Deutsches Zentrum für Luft und Raumfahrt e.V.)	[assessor name] ([affiliation])	Jan Welte (TU Braunschweig)	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.

Disclaimer: This work is licensed under the "openETCS Open License Terms" (oOLT) dual Licensing: European Union Public Licence (EURL v.1.1+) AND Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER openETCS OPEN LICENSE TERMS (oOLT) WHICH IS A DUAL LICENSE AGREEMENT INCLUDING THE TERMS OF THE EUROPEAN UNION PUBLIC LICENSE (VERSION 1.1 OR ANY LATER VERSION) AND THE TERMS OF THE CREATIVE COMMONS PUBLIC LICENSE ("CCPL"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS OLT 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/>
<http://joinup.ec.europa.eu/software/page/eupl/licence-eupl>

Modification History

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

Table of Contents

Modification History.....	3
1 Introduction.....	6
2 Verification and Validation in the Development Lifecycle.....	7
3 Overview of Verification and Validation Activities	7
3.1 Verification and Validation in the Planning Phase	7
3.2 Verification and Validation in the System Design Phase.....	7
3.3 Verification and Validation in the Sub-System Architecture Design Phase.....	8
3.4 Verification and Validation in the SW Specification Phase	8
3.5 Verification and Validation in the SW Design Phase.....	8
3.6 Verification and Validation in the SW Component Phase.....	8
3.7 Verification and Validation in the SW Integration Phase	8
3.8 Verification and Validation in the SW Validation Phase	8
4 Conclusion	8
References	8

Figures and Tables

Figures

Figure 1. openETCS Development Lifecycle 7

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

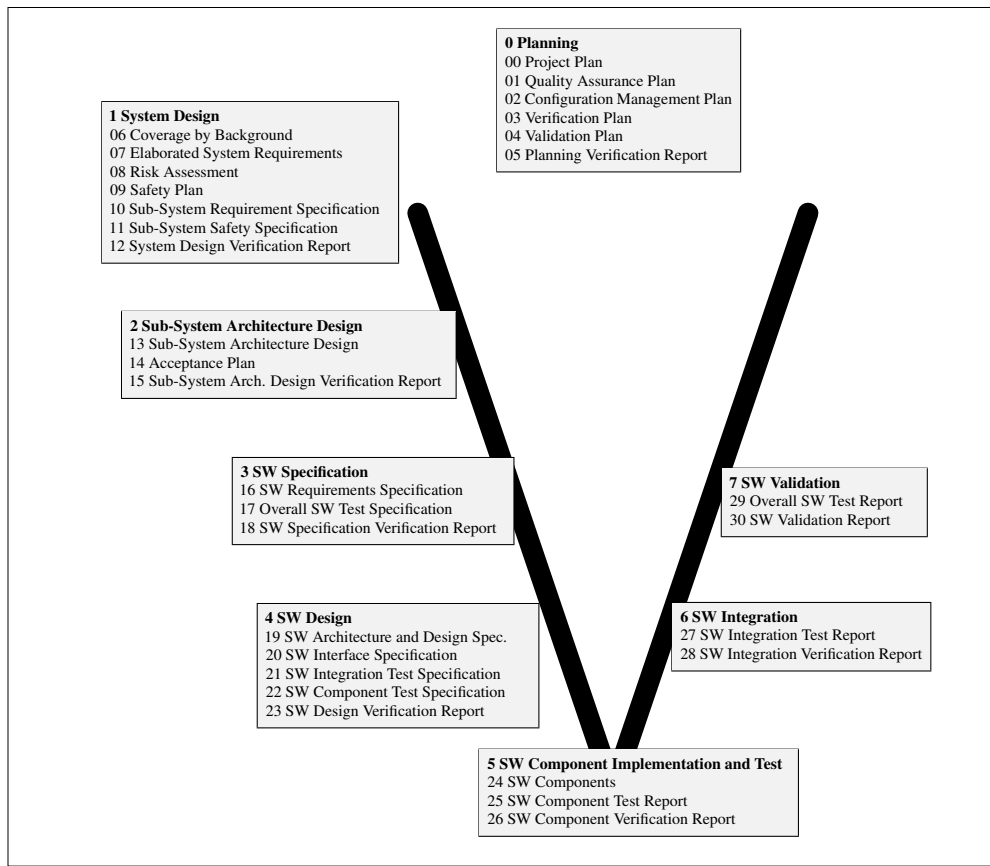


Figure 1. openETCS Development Lifecycle

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.

3.2 Verification and Validation in the System Design Phase

TWT analyzed sub-system requirements from [3, Chapter 5]. The requirements have been modeled as colored Petri nets and subjected to formal analyses. This activity is part of the System Design Verification.

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] Ainhua Garcia. Project quality assurance 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.