OETCS/WP4/D4.1V01

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

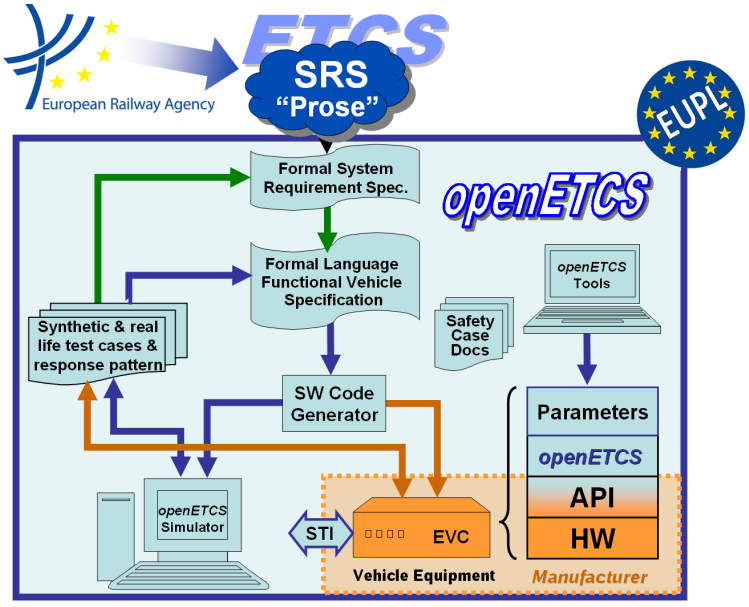
Work Package 4: “Validation & Verification Strategy”

openETCS Validation & Verification Plan

Version 01

Marc Behrens and Hardi Hungar and Stephan Jagusch

June 2013



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: "Validation & Verification Strategy" **OETCS/WP4/D4.1V01**
June 2013

openETCS Validation & Verification Plan

Version 01

Marc Behrens and Hardi Hungar

DLR
Lilienthalplatz 7
38108 Brunswick, Germany
eMail:{hardi.hungar,marc.behrens}@dlr.de

Stephan Jagusch

AEbt Angewandte Eisenbahntechnik GmbH
Adam-Klein-Str. 26
90429 Nürnberg, Germany
eMail: Stephan.Jagusch@AEbt.de

Deliverable

Prepared for openETCS@ITEA2 Project

Abstract: This document describes strategy and plan of the verification and validation activities in the project openETCS. As the goals of the project include the selection, adaption and construction of methods and tools for a FLOSS development in addition to performing actual development steps, differing from the plan for a full development project, the plan covers also activities evaluating the suitability of methods and tools, and it makes provisions for incorporation of V&V of partial developments which are actually done.

The overall strategy is to support the design process as specified in D2.3 and its partial instantiations within openETCS. In accordance with the project approach, V&V shall be done in a FLOSS style, and it has to suit a model-based development. A further main consideration shall be to strive for conformance with the requirements of the standards (EN 50128 and further). This means that the contribution of all activities to a complete verification and validation shall be defined and assessed.

The plan details how to perform verification & validation for a complete development which follows the process sketch from D2.3, so that the result conforms to the requirements of the standards for a SIL 4 development. This includes a definition of activities, the documentation to be produced, the organisation structure, roles, a selection of methods and tools, a format for describing design artifacts subject to V&V, and a feedback format for the findings during V&V.

As D2.3 gives only a rough description of the development steps and not yet a complete list of design artifacts, nor one of methods applied and formats to be used, this first version of the V&V plan will also lack detail which will to be added in later revisions as these informations become more concrete.

Besides the usual purpose of verification & validation activities, namely evaluating and proving the suitability of design artifacts, V&V in openETCS will also generate information on the suitability of the methods and tools employed. For that purpose, a format for describing methods and tools to be used in V&V and one for summarizing the findings about the suitability are defined.

The plan also contains partial instantiations of V&V which match partial developments that are realised within openETCS.

Table of Contents

Figures and Tables

Figures

Tables

Document information	
Work Package	WP4
Deliverable ID or doc. ref.	D4.1
Document title	openETCS Validation & Verification Plan
Document version	00.01
Document authors (org.)	Hardi Hungar (DLR), Marc Behrens (DLR), Stephan Jagusch (AEbt)

Review information	
Last version reviewed	–
Main reviewers	–

Approbation			
	Name	Role	Date
Written by	Hardi Hungar	WP4-T4.1 Task Leader	June 2013
Approved by	–	–	

Document evolution			
00.01	11/06/2013	H. Hungar	Document creation based on draft by S. Jagusch
Version	Date	Author(s)	Justification
–	–	–	–

Introduction

0.1 Purpose

The purpose of this document is to define the verification & validation activities in the project openETCS.

This document describes strategy and plan of the verification and validation activities in the project openETCS. As the goals of the project include the selection, adaption and construction of methods and tools for a FLOSS development in addition to performing actual development steps, differing from the plan for a full development project, the plan covers also activities evaluating the suitability of methods and tools, and it makes provisions for incorporation of V&V of partial developments which are actually done.

WP4-T1-G: A useful plan for WP 4, that is, one that defines a way to achieve the goals of WP 4:

WP4-G1: Identify and demonstrate methods and tools to handle the V&V of a FLOSS development of the EVC software

WP4-G2: Perform as much of V&V on the DAS2Vs produced in the project as possible

Detailed Goals and Means

WP4-T1-G1: The plan shall give an overview of and a structure to the things required from V&V for an openETCS (FLOSS-) development.

WP4-T1-M1: Identifies all (most) of the activities which have to be made for a full development according to the standards, in a form relevant to the approach of openETCS (FLOSS, participants). This may include alternatives.

WP4-T1-G2: The plan shall provide a framework into which the V&V activities which will be performed within the project do fit.

WP4-T1-M2-1: Design formats for collecting information about DAS2Vs (V&V tasks), about the results of V&V activities, about activities of V&V method and tool development, about the results of evaluations of V&V methods and tools. Sketch how all of the information is to be gathered and finally incorporated into the final V&V report (D4.4).

WP4-T1-M2-2: Identify potential variants of partial implementations of V&V processes which are likely going to be performed within the project. These may be (?should be?) related to design activities within the project which produce DAS2Vs.

WP4-T1-G3: The plan shall delineate means for V&V within openETCS

WP4-T1-M3-1: A partial V&V process (see WP4-T1-M2 above) consists of a set of related DASVs and V&V steps to be applied to them. A V&V step is described by input and output (result, purpose) with V&V methods and means.

WP4-T1-M3-2: The plan will prepare the selection of adequate methods and means (tools) by providing evaluation criteria and incorporating available evaluation results.

WP4-T1-M3-2-1: Definition of an evaluation format for tools and methods.

WP4-T1-G4: The plan shall incorporate currently available information on openETCS development process and means and be amendable to future changes and additions.

WP4-T1-M4-1: Use D2.3 in instantiating the general requirements laid down in the standards.

WP4-T1-M4-2: Use D2.1 for tools.

WP4-T1-M4-3: Identify open points and include delineations for things which are useful for a complete V&V but not yet planned or detailed by project activities already performed.

This document describes which verification and validation activities are needed for a full FLOSS development of the EVC software. It describes how the work performed within the project openETCS is to be organised to contribute to such a task, and how to demonstrate that it can be realised.

The document is only valid in conjunction with the Quality Assurance plan [1104G13-QA-plan]

0.2 Plan for Completing this Document

Terminology

DAS2V: *Design Artifact Subject to Verification or Validation*

G: *Goal*

M: *Means*

F: *Finding/Result/Action*

Detailed Goals and Means

WP4-T1-G1: *The plan shall give an overview of and a structure to the things required from V&V for an openETCS (FLOSS-) development.*

WP4-T1-M1: *Identifies all (most) of the activities which have to be made for a full development according to the standards, in a form relevant to the approach of openETCS (FLOSS, participants). This may include alternatives.*

WP4-T1-G2: *The plan shall provide a framework into which the V&V activities which will be performed within the project do fit.*

WP4-T1-M2-1: *Design formats for collecting information about DAS2Vs (V&V tasks), about the results of V&V activities, about activities of V&V method and tool development, about the results of evaluations of V&V methods and tools. Sketch how all of the information is to be gathered and finally incorporated into the final V&V report (D4.4).*

WP4-T1-M2-2: *Identify potential variants of partial implementations of V&V processes which are likely going to be performed within the project. These may be (?should be?) related to design activities within the project which produce DAS2Vs.*

WP4-T1-G3: *The plan shall delineate means for V&V within openETCS*

WP4-T1-M3-1: *A partial V&V process (see WP4-T1-M2 above) consists of a set of related DASVs and V&V steps to be applied to them. A V&V step is described by input and output (result, purpose) with V&V methods and means.*

WP4-T1-M3-2: *The plan will prepare the selection of adequate methods and means (tools) by providing evaluation criteria and incorporating available evaluation results.*

WP4-T1-M3-2-1: *Definition of an evaluation format for tools and methods.*

WP4-T1-G4: *The plan shall incorporate currently available information on openETCS development process and means and be amendable to future changes and additions.*

WP4-T1-M4-1: *Use D2.3 in instantiating the general requirements laid down in the standards.*

WP4-T1-M4-2: *Use D2.1 for tools.*

WP4-T1-M4-3: *Identify open points and include delineations for things which are useful for a complete V&V but not yet planned or detailed by project activities already performed.*

Concrete First Steps (in SCRUM terminology: the backlog)

WP4-T1-S1: *Assess the input material*

WP4-T1-S1-1: *Assess sketch of the V&V plan (partly done)*

WP4-T1-F1-1-1: *The current format is .doc*

WP4-T1-F1-1-2: *The plan currently lists mainly the requirements on the plan and does not yet detail much of the plan itself.*

WP4-T1-F1-1-3:

WP4-T1-S1-2: *Assess D2.3 “Process Definition” with definition of DAS2Vs and V&V steps*

WP4-T1-F1-2-1: *DAS2Vs and verification & validation steps defined on a high level*

WP4-T1-S1-3: *Assess D2.9 “Requirements for Verification & Validation”*

WP4-T1-F1-3-1: *very high-level, requirements included in the appendix for reference in further completion in relevant for future steps*

WP4-T1-S1-4: *Assess D2.1 (“Report on Existing Methodologies”)*

WP4-T1-F1-4-1: *Seems very sketchy*

WP4-T1-S1-5: *Assess development and V&V activities planned or already on the way for taking them into account in the V&V plan*

WP4-T1-S1-5-1: *Ask a lot of people (or the right people)*

WP4-T1-S1-5-1-1: *Design a query email (to be backed up by phone or personal inquiries)*

WP4-T1-S2: *Organize the writing*

WP4-T1-S2-1: *Make a detailed work plan*

WP4-T1-S2-1-1: *Transform the sketch to .tex*

WP4-T1-S2-1-2: *Revise the structure according to what is expected to be done - accommodating the info on the process (D2.3 -WP4-T1-S1-2) and on ongoing activities (WP4-T1-S1-5).*

WP4-T1-S2-1-3: *References to the requirements (D2.9 - WP4-T1-S1-3) are to be included*

WP4-T1-S2-1-4: *Tools and methods*

WP4-T1-S2-1-4-1: *Format for evaluation (formulate evaluation criteria, D4.1a)*

WP4-T1-S2-1-5: *Result collection*

WP4-T1-S2-1-5-1: *Sketch all the formats (purpose)*

WP4-T1-S2-1-5-2: *Sketch the process of information collection (T4.2 and T4.3 will have to do that)*

WP4-T1-S2-1-6: *Include section on V&V plan revision*

WP4-T1-S2-2: *Find contributors*

WP4-T1-S2-3: *Distribute the work*

WP4-T1-S3: *Do the work*

0.3 Background Information

%%Further Info, perhaps put the project context here %%

0.3.1 Definitions

Verification

Verification is an activity which has to be performed at each step of the design. It has to be verified that the design step achieved its goals. This consists at least of two parts:

- that the artifacts produced in the step are of the right type and contain allthe information they should. E.g., that the SSRS identifies all components addressed in SS 026, specifies their interfaces in sufficient detail and has allocated the functions to the components (this should just serve an example and is based on a guess what the SSRS should do)
- that the artifact correctly implements the input requirements of the design step. These typically include the main output artifacts of the previous step. “Correctly implements” includes requirement coverage (tracing). This can and should be supported by some tools. Adequacy of such tools depends on things like format compatibility, degree of automation, functionality (e.g., ability to handle m-to-n relations). Depending on the design step (and the nature of the artifacts) different forms of verification will complement requirement coverage, with different levels of support. The step from SS 026 to the SSRS will mainly consist of manual activities besides things like coverage checks. Verifying a formal (executable) model against the SSRS can be supported by animation or simulation to e.g. execute test cases which have been designed to check compliance with the SSRS. Even formal proof tools may be employed to check or establish properties. Model-to-code steps offer far more options (and needs) for tool support. And tools or tool sets for unit test will support dynamic testing for requirement or code coverage. This may include test generation, test execution with report generation, test result evaluation and so on. Also, code generator verification (or qualification) may play a role, here. Integration steps mandate still other testing (or verification) techniques.

Summarizing, one may say that verification subsumes highly diverse activities, and may be realized in very many different forms.

Validation

Validation is name for the activity by which the compliance of the end result with the initial requirements is shown. In the case of openETCS, this means that the demonstrator (or parts of it) are checked against the SS 026 or one of its close descendants (i.e., SSRS). This will consist of testing the equipment according to a test plan derived form the requirements and detailed into concrete test cases at some later stage. Tool support for validation will thus mainly concern test execution and evaluation, perhaps supplemented by test derivation or test management. Ambitous techniques like formal proof are most likely not applicable here.

Thus, the tool support for validation will not differ substantially from that for similar verification activities.

One might also consider “early” validation activities, e.g. “validating” an executable model against requirements from the SS 026. These are not mandated by the standards and can per se not replace design step verification. They may nevertheless be worthwhile as means for early defect detection.

Further (mostly complementary) information on V&V can be found in the report on the CENELEC standards (D2.2).

Verification & Validation Strategy

The overall strategy is to support the design process as specified in D2.3 and its partial instantiations within openETCS. In accordance with the project approach, V&V shall be done in a FLOSS style, and it has to suit a model-based development. A further main consideration shall be to strive for conformance with the requirements of the standards (EN 50128 and further). This means that the contribution of all activities to a complete verification and validation shall be defined and assessed.

0.4 Verification & Validation Strategy for a Full Development

Define the strategy for a full EVC software development.

0.5 Verification & Validation Strategy for openETCS

The project will only perform part of the development, and thus also only a part of the V&V activities. Define how the project demonstrates that a full development would be possible.

Verification & Validation Plan for a Full Development

%%detail%%

Instantiate the generic Verification & Validation plan from the standard (and the draft) to openETCS. That is, provide the requirements, define the design steps, identify verification & validation activities to be performed and documents to be produced.

The plan details how to perform verification & validation for a complete development which follows the process sketch from D2.3, so that the result conforms to the requirements of the standards for a SIL 4 development. This includes a definition of activities, the documentation to be produced, the organisation structure, roles, a selection of methods and tools, a format for describing design artifacts subject to V&V, and a feedback format for the findings during V&V.

As D2.3 gives only a rough description of the development steps and not yet a complete list of design artifacts, nor one of methods applied and formats to be used, this first version of the V&V plan will also lack detail which will to be added in later revisions as these informations become more concrete.

Besides the usual purpose of verification & validation activities, namely evaluating and proving the suitability of design artifacts, V&V in openETCS will also generate information on the suitability of the methods and tools employed. For that purpose, a format for describing methods and tools to be used in V&V and one for summarizing the findings about the suitability are defined.

The plan also contains partial instantiations of V&V which match partial developments that are realised within openETCS.

0.6 Structure of the Verification & Validation Report

The verification and validation plan covers the following central topics:

Header *containing all information to identify, this report, the authors, the approbation and reviewing entities.*

Executive Summary *giving an overview of the major elements from all sections.*

Problem Statement *describing the challenges to be answered by Verification & Validation as well as the decisions to be taken based on the V&V results as well as how to cope with potentially faulty output. It further describes the accreditation scope based on the risk assessment done on V&V-level.*

V&V Requirements Traceability Matrix *links every V&V artifact back to the requirements to measure e.g. test coverage and to directly link V&V results to the requirements.*

Acceptability Criteria, *describing the criteria for acceptance of the artifact into the Verification & Validation process e.g. as the direct translation of the requirements into metrics to measure success, are used e.g. for burndown charts within the process.*

Assumptions *that are identified during the design of the verification and validation strategy and how these assumptions have an impact on the verdict by listing capabilities and limitations.*

Risks and Impacts *that come across the execution of V&V tasks together with the impacts foreseen.*

V&V Design *states how the V&V process builds up including data preparation, execution and evaluation.*

V&V Methodologies *giving a step-by-step walkthrough of all possible V&V activities including the assumptions, and verdict-relevant limitations and criteria for, e.g., model verification, model-to-code verification, unit testing, integration testing and final validation (according to the standard, this involves running the software on the target hardware).*

V&V Issues *describing unsolved V&V issues and their impact on the affected proof or verdict.*

Peer Reviews *going into details on how the community can take part and how official bodies and partners are integrated into the development and review process.*

Test Plan Definition *going into the details of testing by describing among other things:*

- **Title** *as a unique identifier to the test plan.*
- **Description** *of the test and the test-item giving information about version and revision.*
- **Features** *to be tested and not to be tested in combination are listed together with information background.*
- **Entry Criteria** *which have to be met by the EVC before a test can be started, e.g. that the EVC has to be in level 3 limited supervision with the order to switch to level 2.*
- **Suspension criteria and resumption requirements** *are the central key to a smooth automation of the tests covering topics like* when exiting this test before step 10, which entry criteria does it comply to or which resumption sequence has to be executed to continue testing.
- **Walkthrough** *covering a step-by-step approach of the test plan.*
- **Environmental requirements** *going into the details of what is needed concerning the test environment, e.g. tools, adapter, data preparation.*

Discrepancy Reports *identifying the defects.*

Key Participants *describing the assignment and task for each role involved.*

- **Accreditation of Participants** *describing who was accredited to which role during the Verification & Validation phase.*
- **V&V Participants** *listing the partners participating in V&V activities,*
- **Other participants** *including other interest groups such as reviewer by affiliate partners*[1].

Timeline *giving the timeline for the baselines as input to the V&V process and identifying when each artifact should be created.*

0.7 Methods and Tools

The project shall select / develop / describe a chain of methods and tools for doing verification & validation in a full development.

[1] affiliate partners are non-funded companies who signed the project cooperation agreement and with it get read access to the repositories starting from incubation phase to contribute e.g. by reviewing

0.8 Implementation of Verification & Validation

The verification & validation has to be performed in cooperation with WP 3, which produces DAS2Vs (models and code), and with WP 7, where methods and tools are defined and developed.

To exchange information with WP 3, formats are needed for collecting information about DAS2Vs (V&V tasks) and for giving back information about the results of V&V activities. Similarly, with WP 7 communication shall use formats to describe V&V methods and tools (input from WP 7) and the results of evaluations of V&V methods and tools.

%%Formats, activity organisation%%

Verification & Validation Plan for openETCS

%%Describe how to proceed in openETCS to achieve the most.%%

- *verification & validation for partial developments*
- *evaluation*
- *demonstration story of capabilities*

Appendix A: Requirements on Verification & Validation

%%Explain the requirement chapter.%%

- *Requirements from D2.9.*
- *Take the lists from the draft from 121207, retain the structure (at least preliminarily).*

A.1 Requirements on Verification & Validation from D2.9

%%Adapt the intro text%%

The already provided requirements require a safety plan compliant to the CENELEC EN 50126, 50128 and 50129. This pulls a number of requirements on V&V, including Verification and Validation plans. On the topic of compliance to EN 50128, one shall also refer to the D2.2 document.

R-WP2/D2.6-02-061 A Verification plan shall be issued and complied with.

R-WP2/D2.6-02-061.01 The verification plan shall provide a method to demonstrate the requirements covering all the development artifacts.

R-WP2/D2.6-02-061.02 The verification plan shall state all verification activities required for each of these development artifacts.

R-WP2/D2.6-02-062 A Validation Plan shall be issued and complied with.

R-WP2/D2.6-02-062.01 The validation plan shall provide a method to validate all functional and safety requirements over all development artifacts.

R-WP2/D2.6-02-062.02 The validation plan shall state all validation activities required for each of these development artifacts.

R-WP2/D2.6-01-021 The test plan shall comply the mandatory documents of the SUBSET-076, restricted to the scope of the OpenETCS project.

Justification. It will possibly be difficult to model all the tests in the course of the project, but the test plan should at least be complete.

R-WP2/D2.6-02-063 Each design artifact needs a reference artifact which it implements (*e.g.* code to detailed model, SFM to SSRS model. . .)

R-WP2/D2.6-02-063.01 The implementation between them relation shall be specified in detail.

e.g. for state machine and a higher level state machine mapping of interfaces, states and transition is required. This includes additional invariants, input assumptions and further restrictions. This informaiton is the basis for verification activities.

R-WP2/D2.6-02-063.02 The design of the artifacts shall be made such to allow verifiability as far as possible.

R-WP2/D2.6-02-064 The findings from the verification shall be traced, and will be adequately addressed (taken into consideration, or postponed or discarded with a justification).

A.2 General Requirements on Verification

Excerpt from EN 50128:2011 [N01]	Requirement	Project Relevance
5.3.2.7	For each document, traceability shall be provided in terms of a unique reference number and a defined and documented relationship with other documents.	fully applicable

%%Complete the table.%%

%%Insert other tables.%%