OETCS/WP4/D4.1aV02

openETCS

ITEA2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

ITEA2 Project
Call 6 11025
2012 – 2015

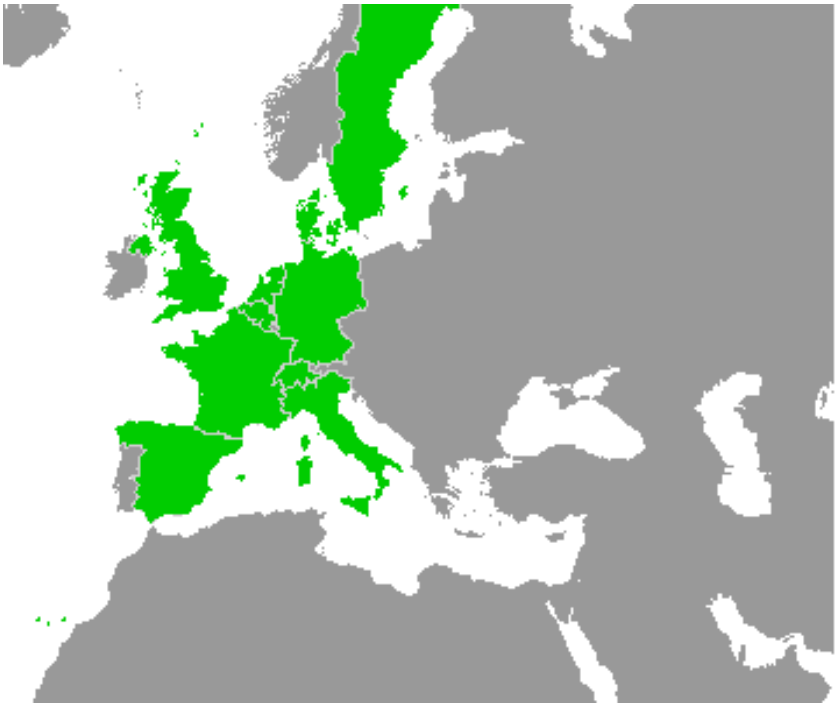
Work-Package 4: “Verification and Validation”

Preliminary Evaluation Criteria on Verification and Validation

Version O2

Hardi Hungar, Marc Behrens

May 2013



This page is intentionally left blank

Work-Package 4: “Verification and Validation” **OETCS/WP4/D4.1aV02**
May 2013

Preliminary Evaluation Criteria on Verification and Validation

Version O2

Hardi Hungar, Marc Behrens

DLR
Germany

Description of work

Prepared for openETCS@ITEA2 Project

Abstract: Evaluation criteria for tools and methods to be selected for use in V&V activities are derived from a decription of their purpose (i.e., the activities to be performed with the help of the tools). This description is complemented by
`WP41a-PreliminaryEvaluationCriteriaOnVAndVTables_V02_20130522.xml`.

Table of Contents

Figures and Tables

Figures

Tables

1 Verification and Validation Activities

1.1 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).

2 Evaluation Criteria

2.1 Preliminary List of Relevant Requirements

"When designing a new on-board Control-Command and Signalling subsystem or when performing a major modification/upgrade of an existing subsystem where the application of the TSI [1] is required[...]" [2]

2.1.1 Methodology of Extracting Requirements from Legal Reference

The possible relevant requirements were identified starting out from the table 1 documents. The document [1] amended with document [2] represents the current decisions taken by the European Commission concerning 'High-speed rail system (HS) and conventional rail system (CR)' in its subsystem 'control-command and signalling'. These documents will be referenced as TSI/CCS. The reference within the openETCS project will be the english version. From the total list of the mandatory requirements mentioned and referenced within the TSI/CCS the relevant requirements were identified according to the scope 'functional On-Board Unit' of openETCS. These requirements were then categorised to

- central requirements documents, direclty referenced with on-board functionality
- interface related requirements documents

not taking into account that within the interface related requirements there may be functionality for central requirements

2.1.2 Requirements Formulated Within the TSI

Still requirements explicitly formulated within the TSI and not being referenced within the TSI has to

And taking the following hypothesis in account:

- ETCS Level 2 is not excluded.
- Class B Systems are not excluded.

The hypothesis shall be validated taking in account the openETCS operational scenarios.

2.1.3 Disclaimer

The boundaries of the functional On-Board Unit within openETCS are not yet defined thus making this first draft document a not yet consolidated and non final or complete list of possible relevant requirements were extracted from the legal standards of table 1.

[1] Technical Specification of Iteroperability/Control-Command and Signalling

[2] Guide for the application of the TSI for the Subsystem Control-Command and Signalling Trackside and On-board, ERA/GUI/07-2011/INT

Table 1. High Level Reference documents

Ref. No	Document Reference	Title
[1]	2012/88/EU	Commission Decision of 25 January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system
[2]	2012/696/EU	Commission Decision of 6 November 2012 amending Decision 2012/88/EU on the technical specifications for interoperability relating to the control-command and signalling subsystems of the trans-European rail system

2.1.4 List of Central Requirements

Table 2. Central Requirements

TSI Reference Number	Req. Reference	Req. Name	Req. Version	4.2.1.1. S a f e t y	4.2.2. On-board ERTMS/ETCS functionality	referring to
27	UNISIG SUBSET-091	Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2	3.2.0	m		safety
14	UNISIG SUBSET-041	Performance Requirements for Interoperability	3.1.0		m	performance
4	UNISIG SUBSET-026	System Requirements Specification	3.3.0		m	functions
13	UNISIG SUBSET-040	Dimensioning and Engineering rules	3.2.0		m	functions
60	UNISIG SUBSET-104	ETCS System Version Management	3.1.0		m	functions
31	Reserved UNISIG SUBSET-094	Functional requirements for an on-board reference test facility			m	tests
37 b	Reserved UNISIG SUBSET- 076-5-2	Test cases related to features			m	tests
37 c	Reserved UNISIG SUBSET- 076-6-3	Test sequences			m	tests
37 d	Reserved UNISIG SUBSET-076-7	Scope of the test specifications			m	tests
23	UNISIG SUBSET-054	Responsibilities and rules for the assignment of values to ETCS variables	3.0.0		m	ETCS-ID Management

2.1.5 List of Interface Related Requirements

2.2 An Incomplete List of V&V Activities

The following activities, which can all be performed or supported by tools, might be relevant to openETCS.

Tracing: Relating requirement items to implementing items

Animation: Executing a model

Simulation: code/model, perhaps with some environment representation

Formal proof of properties: e.g. establishing some invariant

Proof checking: Verifying that a proof is correct (independently)

Table 3. Interface Related Requirements

TSI Reference Number	Req. Reference	Req. Name	Req. Version	4.2.2.1. Communication with the Control-Command and Signalling Track-side Subsystem	4.2.2.2 Communication with the driver	4.2.2.3. Communicating with the STM	4.2.2.4. Managing information about the completeness of the train	4.2.2.5. Equipment health monitoring and degraded mode support	4.2.2.6. Support data recording for regulatory purposes	4.2.2.7. Forwarding information/orders and receiving state information from rolling stock	4.2.13. GSM-R DMI (Driver-Machine Interface)	5.3 Constituents performance and specifications	referring to	optional if
20	UNISIG SUBSET-048	Trainborne FFFIS for Radio infill	3.0.0	m									Radio communications with the train	
6	ERA_ERTMS_ 015560	ETCS Driver Machine interface	3.3.0		m								communication with the driver	
7	UNISIG SUBSET-034	Train Interface FIS	3.0.0							m			forwarding information/orders	
64	EN 301 515	Global System for Mobile Communication (GSM); Requirements for GSM operation on railways	2.3.0	m									Radio communications with the train: interface operating in GSM-R Band	
65	TS 102 281	Detailed requirements for GSM operation on railways	2.2.0	m									Radio communications with the train: interface operating in GSM-R Band	
10	UNISIG SUBSET-037	EuroRadio FIS	3.0.0	m									Radio communications with the train: protocols	
39	UNISIG SUBSET-092-1	ERTMS EuroRadio Conformance Requirements	3.0.0	m									Radio communications with the train: protocols	
40	UNISIG SUBSET-092-2	ERTMS EuroRadio test cases safety layer	3.0.0	m									Radio communications with the train: protocols	
19	UNISIG SUBSET-047	Trackside- Trainborne FIS for Radio infill	3.0.0	o									Radio communications with the train: radio in-fill	level 1
20	UNISIG SUBSET-048	Trainborne FFFIS for Radio infill	3.0.0	o									Radio communications with the train: radio in-fill	level 1
9	UNISIG SUBSET-036	FFFIS for Eurobalise	3.0.0	m									Eurobalise communication with the train	
43	UNISIG SUBSET 085	Test specification for Eurobalise FFFIS	3.0.0	m									Eurobalise communication with the train	
16	UNISIG SUBSET-044	FFFIS for Euroloop	2.4.0	o									Euroloop communication with the train	level 1
50	UNISIG SUBSET-103	Test specification for Euroloop	1.1.0	o									Euroloop communication with the train	level 1
8	UNISIG SUBSET-035	Specific Transmission Module FFFIS	3.0.0			m							transitions between ERTMS/ETCS and Class B train protection (if not using the standardised interface additional steps must be taken)	
25	UNISIG SUBSET-056	STM FFFIS Safe time layer	3.0.0			m							transitions between ERTMS/ETCS and Class B train protection (if not using the standardised interface additional steps must be taken)	
26	UNISIG SUBSET-057	STM FFFIS Safe link layer	3.0.0			m							transitions between ERTMS/ETCS and Class B train protection (if not using the standardised interface additional steps must be taken)	
36 c	Reserved UNISIG SUBSET-074-2	FFFIS STM Test cases document				m							transitions between ERTMS/ETCS and Class B train protection (if not using the standardised interface additional steps must be taken)	
49	UNISIG SUBSET-059	Performance requirements for STM	3.0.0.			m							transitions between ERTMS/ETCS and Class B train protection (if not using the standardised interface additional steps must be taken)	
52	UNISIG SUBSET-058	FFFIS STM Application layer	3.0.0			m							transitions between ERTMS/ETCS and Class B train protection (if not using the standardised interface additional steps must be taken)	
29	UNISIG SUBSET-102	Test specification for interface ?K?	2.0.0			o							Interface K (to allow certain STMs to read information from Class B balises through the ERTMS/ETCS on-board antenna)	not implemented
45	UNISIG SUBSET-101	Interface ?K? Specification	2.0.0			o							Interface K (to allow certain STMs to read information from Class B balises through the ERTMS/ETCS on-board antenna)	not implemented
46	UNISIG SUBSET-100	Interface ?G? Specification	2.0.0			m							air gap between ETCS on- board antenna and Class B balises (if mandatory is depending on track project)	
34	A11T6001	(MORANE) Radio Transmission FFFIS for EuroRadio	12.4	m									Interace between GSM-R Radio Data Communication and ERTMS/ETCS	
20	UNISIG SUBSET-048	Trainborne FFFIS for Radio infill	3.0.0	o									Interace between GSM-R Radio Data Communication and ERTMS/ETCS: radio in-fill	level 1
44	Reserved	Odometry FIS										m	Odometry	
11	UNISIG SUBSET-038	Offline key management FIS	3.0.0	m									Key Management	
6	ERA_ERTMS_ 015560	ETCS Driver Machine interface	3.3.0		m					m			communication with the driver forwarding information/orders	
80	Reserved	GSM-R Driver Machine Interface									I		GSM-R DMI (Driver-Machine Interface)	
5	UNISIG SUBSET-027	FIS Juridical Recording	3.0.0						m				Data Recording for Regulatory Purposes	
													mandatory for Level 3, no additional requirement document	
													no additional requirement document Functionalities: - initialising the on-board ERTMS/ETCS functionality; - providing degraded mode support; - isolating the on-board ERTMS/ETCS functionality.	
							m							mandatory for Level 3, no additional requirement document

Model checking: Deciding properties of formal objects (specs, models, code)

Test case generation: From a formal object

Test sequence generation: Arranging test cases in a suitable way

Test execution: with subactivities test evaluation, report generation, perhaps test management, regression testing

Table 4 lists some verification techniques which may be used in openETCS to perform mandatory (according to the EN 50128) verification steps. It is taken from the accompanying document `WP41a-PreliminaryEvaluationCriteriaOnVAndVTables_V02_20130522.xml`.
The following abbreviations for design artifact are used in the table.

`C:` code.

`dM:` A detailed model (from which code is derived or generated).

`hM:` A higher-level model (e.g., design specification model.

`srsM:` A model of the requirements (SRS).

`SRS:` The system requirements specification.

Table 4. Verification Steps and Techniques in openETCS

Verification Step	Description	Evaluation Categorization	applicable in verification step			validation step	Verdict if passed	Verdict if not passed
			srsM->SRS	dM->hM	C->dM	C->srsM/SRS		
Model Verification	Checking that a model realises a set of requirements	Static Analysis	✓	✓			Requirements realised	Requirements not realised
Traceability	traceability of all artifacts towards the requirements of Subset-026 according to the CMB, CCB	Traceability	✓	✓	✓		Requirement covered	Requirement not covered
Functional Test		Functional/ Black-box Testing				✓	a) Functionality implemented correctly b) Functionality implemented with comments	a) Functionality not implemented b) Functionality not implemented correctly
Unit Test	verifying consistency of the implementation	Dynamic Analysis and Testing			✓		Unit is acceptable for integration	Unit is not not acceptable for integration
Software Integration Test	Checking that the software components provide the specified interfaces	Dynamic Analysis and Testing			✓		The software components work together in an appropriate manner	Software component interfaces do not match
Software Validation Test	Checking that the software implements the requirements	Functional/ Black-box Testing				✓	Requiements correctly implemented	Requirements not correctly implemented

2.3 An Incomplete List of V&V Tool Evaluation Criteria

As broad as the range of V&V activities and tools supporting them is the set of evaluation criteria:

Effectiveness: A tool must be able to perform a useful function

Efficiency: Very important for automatic routines like test case generation, model checking: They should not take forever or use infinite memory

Vertical workflow integration: input and output formats should match along a chain of dependent steps. Very specific input requirements can make a tool useless. More general, we should strive for a complete, rather well integrated tool chain

Horizontal workflow integration: Test management and test execution should go hand in hand.

Qualifiabilty: T2 or T3 qualification is required for some usages. Depends also on the process, as the failure of tool not being qualifiable in itself can be remedied by introducing a complemnting tool the checks the first's output (Example: Complementing code generation by verifying the equivalence of input and output)

FLOSS: of course (openETCS)

3 Summary

This document lists general criteria for the evaluation methods and tools for verification and validation within openETCS. Detailing the criteria needs more information on the design steps, which artifacts are produced by them and by which methods. Concrete criteria are at least as diverse as the different verification steps, and these depend highly on the objects and how they are produced.