OETCS/WP7/O7.2.1 – 00/05

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

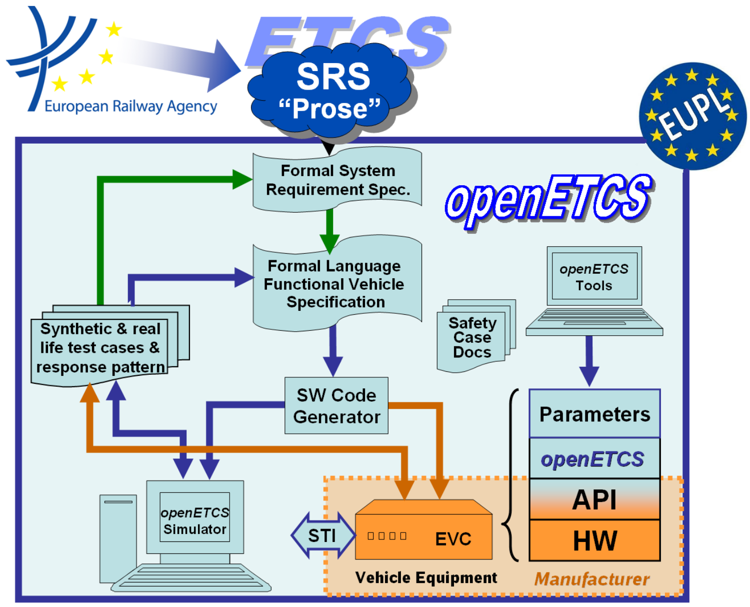
Work-Package 7: “Secondary tools - Verification and Validation ”

Evaluation of supporting tools and methods against the WP2 requirements and task 1

Means and tools for Verification and Validation

Marielle Petit-Doche, all participants of the benchmark and all participants of VnV and Safety process

October 2013



Funded by:

Federal Ministry of Education and Research

Liberté • Égalité • Fraternité
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 7: "Secondary tools - Verification and Validation "

OETCS/WP7/O7.2.1 – 00/05
October 2013

Evaluation of supporting tools and methods against the WP2 requirements and task 1

Means and tools for Verification and Validation

Marielle Petit-Doche
Systerel

all participants of the benchmark
WP7 partners

all participants of VnV and Safety process
WP4 partners

Evaluation

Prepared for openETCS@ITEA2 Project

Abstract: This document gives elements to evaluate the tools and methods to complete the primary toolchain and to support verification and validation activities, safety activities, moodel transformation and data management for the whole project. Evaluation on the means and tools of benchmark is also described.

Table of Contents

Figures and Tables iv

1 Introduction 1

1.1 Organisation of the document 1

2 Template 3

2.1 Instructions 3

2.2 Presentation 3

2.3 Common criteria on secondary means and tools 4

2.3.1 Project and WP2 requirements 4

2.3.2 Qualification 4

2.3.3 Complementarity with primary toolchain 5

2.4 VnV Activities 6

2.5 Properties 7

2.6 Verification methods and tools 8

2.7 Validation means and tools 8

2.8 Other Criterias 9

2.9 Other comments 9

3 Conclusion 10

3.1 Main usage of the approach 10

Figures and Tables

Figures

Figure 1. openETCS Process (rough view) 7

Tables

Document information	
Work Package	WP7
Deliverable ID or doc. ref.	O7.2.1
Document title	Evaluation of supporting tools and methods against the WP2 requirements and task 1 - Vnv
Document version	00.05
Document authors (org.)	Marielle Petit-Doche (Systerel)

Review information	
Last version reviewed	00.04
Main reviewers	

Approbation			
	Name	Role	Date
Written by	Marielle Petit-Doche	WP7-T7.1 Sub-Task Leader	
Approved by	Michael Jastram	WP7 leader	

Document evolution			
Version	Date	Author(s)	Justification
00.01	19/07/2013	M. Petit-Doche	Document creation
00.02	09/09/2013	M. Petit-Doche	Major evolutions in all document
00.03	19/09/2013	M. Petit-Doche	Issues: 167, 168, 170
00.04	23/09/2013	M. Petit-Doche	Issues: 164, 169, 174, 175, 177, 178
00.05	01/10/2013	M. Petit-Doche	Split of document O7.2.1. Verification and Validation part

1 Introduction

The aim of this document is to report the results of the evaluation of means and tools for the secondary means and tools, i.e. the means and tools which complete the primary tool chain dedicated to formal model and software design.

This evaluation task is part of work package WP7, task 2 "Secondary tools analyses and recommendations". According to the results of WP2, especially the OpenETCS process and the requirements on language and tools [**?**], and the results of T7.1 on the primary toolchain [**?**], the aim of this task is to determine the best candidates to complete and support the primary toolchain for the following activities:

- verification and validation (WP4)
- safety activities support (WP4)
- data, function and requirement management (SSRS, WP3 and WP4)
- model transformation and code generation (WP3 and WP4)

This document is dedicated to tools and means for verification and validation.

1.1 Organisation of the document

The chapter 2 provides a template to describe the means and tools and a list of criteria according WP2 requirements on language, models and tools, and T7.1 primary tool chain decision. The objectives of this description and criteria are to allow to determine the best means of description and associated tool for a given activities.

The chapter 3 resumes the results of the evaluation at the end of the benchmark activities.

In Appendix, a chapter is dedicated to each models produced during the benchmark activities :

- Scade Suite
- System C
- UPPAAL
- Rodin and Pluggins
- Tools around Classical B (ProB, SMT solver,...)
- CPN tools
- Matelo
- RT-Tester

- Fiacre and Tina
- Frama-C
- Diversity

2 Template

2.1 Instructions

Author Author of the approaches description %%Name - Company%%

Assessor 1 First assessor of the approaches %%Name - Company%%

Assessor 2 Second assessor of the approaches %%Name - Company%%

In the sequel, main text is under the responsibilities of the author.

Author: Author can add comments using this format at any place.

Assessor 1: First assessor can add comments using this format at any place.

Assessor 2: Second assessor can add comments using this format at any place.

When a note is required, please follow this list :

0 not recommended, not adapted, rejected

1 weakly recommended, adapted after major improvements, weakly rejected

2 recommended, adapted (with light improvements if necessary) weakly accepted

3 highly recommended, well adapted,strongly accepted

***** difficult to evaluate with a note (please add a comment under the table)

All the notes can be commented under each table.

This section defines the criteria for the means and tools dedicated to verification and validation activities, in the WP4 workpackage.

Criteria of this section are defined according [**?**].

2.2 Presentation

This section gives a quick presentation of the approach and the tool.

Name %%Name of the approach and the tool%%

Web site %%if available, how to find information%%

Licence %%Kind of licence%%

Abstract

Short abstract on the approach and tool (10 lines max)

Publications

Short list of publications on the approach (5 max)

2.3 Common criteria on secondary means and tools

This section discusses the common criteria of the means and tools according to the project requirements on tools and the results of T7.1.

2.3.1 Project and WP2 requirements

The objectives of this list of criteria is to check if the proposed means and tools meet the main criteria of the project: open-source approaches, usability, modularity, coverage of the objectives,...

According WP2 requirements, give a note for characteristics of the use of the tool (from 0 to 3) :

	Author	Assessor 1	Assessor 2	Total
Open Source (D2.6-02-074)				
Portability to operating systems (D2.6-02-075)				
Cooperation of tools (D2.6-02-076)				
Robustness (D2.6-02-078)				
Modularity (D2.6-02-078.1)				
Documentation management (D2.6-02-078.02)				
Distributed software development (D2.6-02-078.03)				
Simultaneous multi-users (D2.6-02-078.04)				
Issue tracking (D2.6-02-078.05)				
Differences between models (D2.6-02-078.06)				
Version management (D2.6-02-078.07)				
Concurrent version development (D2.6-02-078.08)				
Model-based version control (D2.6-02-078.09)				
Role traceability (D2.6-02-078.10)				
Safety version traceability (D2.6-02-078.11)				
Model traceability (D2.6-02-079)				
Tool chain integration				
Scalability				
User Friendliness				

2.3.2 Qualification

This section discusses how the tool can be classified according EN50128 requirements (D2.6-02-085). Some qualification shall be mandatory if the tool is involved to design a SIL4 software.

	Author	Assessor 1	Assessor 2	Total
Tool manual (D.2.6-01-42.02)				
Proof of correctness (D.2.6-01-42.03)				
Existing industrial usage				
Model verification				
Test generation				
Simulation, execution, debugging				
Formal proof				

Which scope of qualification is expected according EN50128 (section 6.7) ?

Score :

3 already qualified for this level

2 qualification possible to this level, but some elements shall be provided

0 qualification not recommended for this level

	Author	Assessor 1	Assessor 2	Total
class T1				
class T2				
class T3				

Other elements for tool certification

2.3.3 Complementarity with primary toolchain

The objectives of this list of criteria is to check if the proposed means and tools can be easily integrated to the primary toolchain.

2.3.3.1 Language

According to the decisions and the propositions of T7.1, how the mean and approach can be adapted to or can complete the chosen language and methods:

	Author	Assessor 1	Assessor 2	Total
SysML				
Scade method				
EFS language				
B Method				
C language				

SysML

How the means or tools can complete SysML ?

Scade, EFS, Classical B

How the means or tools can complete the current proposals for formal modeling language ?

C language

How the means or tools can complete or be adapted to SIL4 software in C language ?

2.3.3.2 Tools and platforms

According to the decisions and the propositions of T7.1, how the mean and approach can be integrated to or can complete the chosen tools and platforms:

	Author	Assessor 1	Assessor 2	Total
Eclipse				
Papyrus				
Scade				
EFS tools				
B tools				

Eclipse

How the means or tools can be integrated to the Eclipse platform ?

Papyrus

How the means or tools can complete Papyrus ?

Scade, EFS, Classical B

How the means or tools can complete the current proposals for formal modeling tools ?

2.4 VnV Activities

The VnV activities are described in details in the verification and Validation Plan [**?**].

According figure 1, for which activities is the mean or tool suitable (see also [**?**] section 5.1.2 for more details) ?

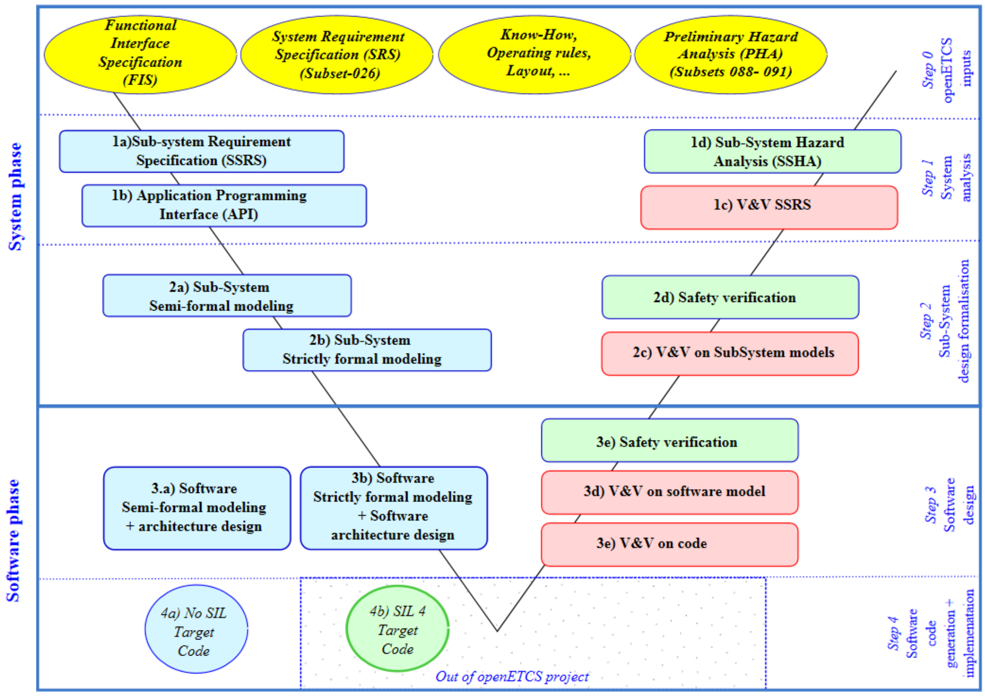

System phase
Software phase
Functional Interface Specification (FIS)
System Requirement Specification (SRS) (Subset-026)
Know-How, Operating rules, Layout, ...
Preliminary Hazard Analysis (PHA) (Subsets 088- 091)
Step 0 openETCS inputs
1a)Sub-system Requirement Specification (SSRS)
1b) Application Programming Interface (API)
1d) Sub-System Hazard Analysis (SSHA)
1c) V&V SSRS
Step 1 System analysis
2a) Sub-System Semi-formal modeling
2b) Sub-System Strictly formal modeling
2d) Safety verification
2c) V&V on SubSystem models
Step 2 Sub-System design formalisation
3.a) Software Semi-formal modeling + architecture design
3b) Software Strictly formal modeling + Software architecture design
3e) Safety verification
3d) V&V on software model
3e) V&V on code
Step 3 Software design
4a) No SIL Target Code
4b) SIL 4 Target Code
Out of openETCS project
Step 4 Software code generation + implemenataion

Figure 1. openETCS Process (rough view)

	Author	Assessor 1	Assessor 2	Total
1c SSRS Verification				
1c SSRS Validation				
2c SFM Verification				
2c SFM Validation				
3d SW-SFM Verification				
3d SW-SFM Validation				
3d SW-FFM Verification				
3d SW-FFM Validation				
3e Code Verification				
3e Code Validation				
DAS2V Verification [1]				
DAS2V Validation				

2.5 Properties

Which kind of properties or elements are verified or validated by the mean or tool (see also [?] section 4) ?

	Author	Assessor 1	Assessor 2	Total
Functionalities of the system and sub-system				
System and sub-system architecture				
External and internal interfaces of sub-system				
Software components				
Performance constraints				
Safety objectives				
Functional properties				
Safety properties				

2.6 Verification methods and tools

Which kind of methods is proposed (see also [?] section 5.3) ?

	Author	Assessor 1	Assessor 2	Total
Reviews				
Inspections				
Software Architecture Analysis Method				
Architecture Tradeoff Analysis Method				
Model-Based System Integration Testing				
Model-Based Testing of Generated High-Level Code				
Abstract Interpretation				
Deductive Verification				
Model Checking				
Correct by Construction Formal Methods				
Verification with Formal Methods				
Simulation-based				

2.7 Validation means and tools

The following list of criteria focuss on means and tools to support validation activities, according WP2 requirements :

	Author	Assessor 1	Assessor 2	Total
Simulation-based				
Step-by-step simulation (D2.6-01-036)				
Environment emulation (D2.6-01-037 and D2.6-02-080)				
Time-based test case (D2.6-02-081)				
Test cases writing (D2.6-01-038)				
Test cases execution (D2.6-01-038)				
Test cases storage (D2.6-01-038)				
Version management of test cases (D2.6-02-082)				
Test generation from independant test model (D2.6-02-083)				
Test sequences writing (D2.6-02-084)				
Test sequences execution (D2.6-02-084)				
Test sequences storage (D2.6-02-084)				

2.8 Other Criterias

Comment. MPD : Todo Ideas welcomed !

2.9 Other comments

Comment. This section is available for the author or the assessors to complete the description and criteria.

3 Conclusion

Comment. MPD : Todo

The sequel is let as an example is this early version.

Criteria to discuss here are those which concerns all the secondary tools as open-source issues, compatibility with primary tool-chain, compatibility with eclipse,...

This conclusion give a sum up of the evaluation results for each approach. The detailed results of each approach are given in the appendix.

Minus mark "-" means this criteria as not been evaluated for this approach.

Star mark "*" means this criteria has been difficult to evaluate for this approach.

The highest score is **9** and means that the criteria is fully respected, the lowest score is 0.

3.1 Main usage of the approach

Comment. MPD : Todo

The sequel is let as an example in this early version.

Score and results shall be corrected latter.

This section discusses the main usage of the approach.

According to the figure **??**, for which phases do you recommend the approach (give a note from 0 to 3) :

	GOPRR	ERTMSFormalSpecs	SysML with Papyrus	SysML with EA	SCADE	EventB	Classical B	System C	Petri Nets	GNATprove
Verification	5	1	7	**9**	3	**9**	3	2	**6(9)**	2 (3)
Validation	**9**	**9**	6	7	**9**	**9**	5	5	**6(9)**	3 (4)
Safety analysis	**9**	0	6	7	**9**	6	**9**	**9**	**6(9)**	**6(9)**
Data, function or requirement management	**9**	0	3	3	**9**	3	**9**	6	2 (3)	**6(9)**
Model or code transformation	**9**	0	3	3	**9**	3	**9**	6	2 (3)	**6(9)**