OETCS/WP7/O7.2.1 – 00/02

ITEA2 Project
Call 6 11025
2012 – 2015

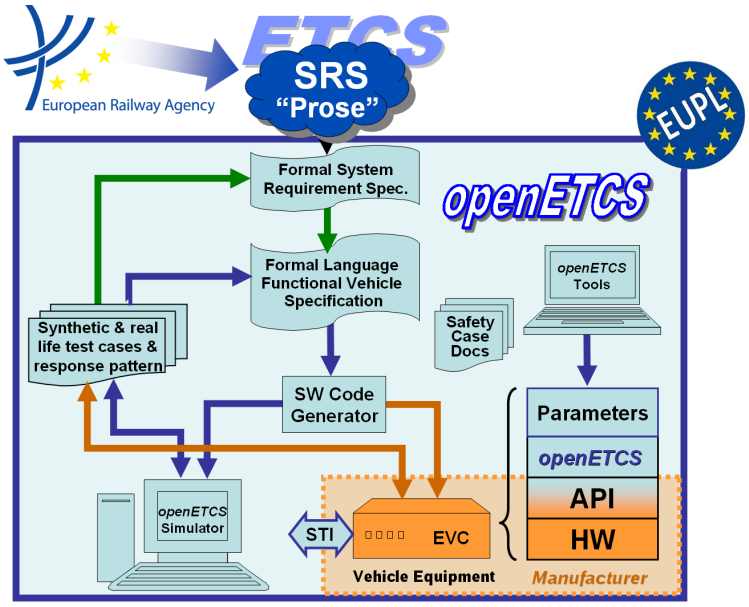
Work-Package 7: “Secondary tools”

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

List of criteria on supporting tools and methods and results on the benchmark

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

September 2013



Funded by:

Federal Ministry of Education and Research
Région de Bruxelles-Capitale
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

openETCS

This page is intentionally left blank

Work-Package 7: “Secondary tools” **OETCS/WP7/O7.2.1 – 00/02**
September 2013

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

List of criteria on supporting tools and methods and results on the benchmark

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

Figures

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
Document version	00.02
Document authors (org.)	Marielle Petit-Doche (Systerel)

Review information	
Last version reviewed	00.01
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

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 [1], and the results of T7.1 on the primary toolchain [2], 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
- safety activities support
- data, function and requirement management
- model transformation and code generation

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
- Rodin and Pluggins
- Tools around Classical B (ProB, SMT solver,...)
- CPN tools
- Matelo
- RT-Tester
- Fiacre and Tina
- Gnat Prove

- Frama-C
- Diversity
- Acceleo
- ATL
- QVTO and SmartQVT
- Goal Structuring Notation (GSN)
- Eclipse ProR
- Safety Architect
- Eclipse EMF Store
- Eclipse EMF Client Platform

1.2 Glossary

API Application Programming Interface

FME(C)A Failure Mode Effect (and Criticity) Analysis

FIS Functional Interface Specification

HW Hardware

I/O Input/Output

OBU On-Board Unit

PHA Preliminary Hazard Analysis

QA Quality Analysis

RBC Radio Block Center

RTM RunTime Model

SIL Safety Integrity Level

SRS System Requirement Specification

SSHA Sub-System Hazard Analysis

SSRS Sub-System Requirement Specification

SW Software

THR Tolerable Hazard Rate

V&V Verification & Validation

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.

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)

For which activities are dedicaded the means or tools (give a note from 0 to 3) :

	Author	Assessor 1	Assessor 2	Total
Verification				
Validation				
Safety analysis				
Data, function or requirement management				
Model or code transformation				

According the results of this table, some of the following sections can be skipped.

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

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				

2.3.2 Certifiability

This section discusses how the tool can be classified according EN50128 requirements (D2.6-02-085).

	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				

Other elements for tool certification

2.3.3 Complementarity with primary toolchain

According to the decisions and the propositions of T7.1, how the mean and approach can be addapted to or can complete:

	Author	Assessor 1	Assessor 2	Total
Eclipse				
SysML				
Papyrus				
Scade				
EFS				
Classical B approach				
C code				

Eclipse

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

SysML and Papyrus

How the means or tools can complete SysML with Papyrus ?

Scade, EFS, Classical B

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

C code

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

2.4 Means and tools for verification and validation purposes

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

2.4.1 VnV Activities

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

	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				

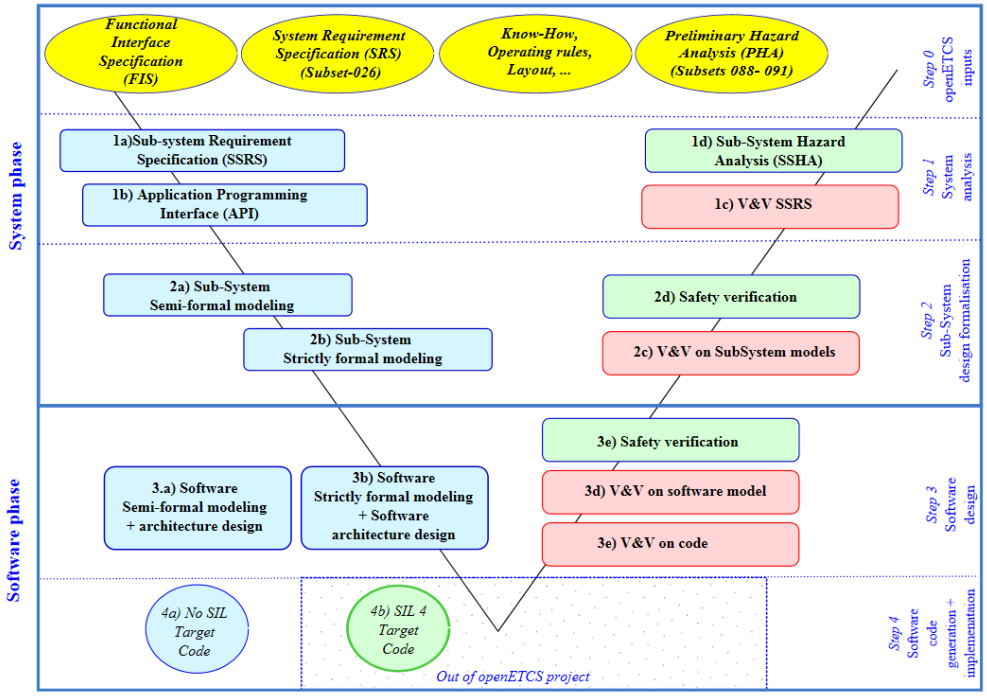


Figure 1. openETCS Process (rough view)

2.4.2 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				

Comment. MPD : Todo

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

Criteria to discuss here are those which concerns means and tools for VnV

7.7.3 Testing R-WP2/D2.6-01-036 The SFM shall be simulable in debug mode (step-by-step), allowing inspec- tion of states, variables and I/O. R-WP2/D2.6-01-037 The environment shall be emulated by high level construction of the inputs. Justification. "High level" means that it will not be necessary to define bitwise the inputs at each cycle.

On the contrary, some automation will be available to define the behavior of the inputs. R-WP2/D2.6-02-080 The environment shall be emulated by construction of the inputs compliant to SUBSET-026. R-WP2/D2.6-02-081 The tool chain shall allow time-based test cases. R-WP2/D2.6-01-038 The tool chain shall allow to write, execute and store test cases and use cases for the SFM. R-WP2/D2.6-02-082 Version management will allow to map test cases version to the SFM, the FFM and source code versions. R-WP2/D2.6-02-083 The tool chain shall allow to generate test cases for the SFM, the FFM and source code from a test model. R-WP2/D2.6-02-083.01 The test model is independant from the tested model. Justification. The test model can be either a model of the environment, or a model of the same subsystem that is being tested, but in both cases this test model must be completely independant from the tested model. R-WP2/D2.6-02-084 The tool chain shall allow to write, execute and store test sequences com- bining multiple test cases for the SFM, the FFM and source code.

2.5 Means and tools for safety activities support

Criteria of this section are defined according [3].

2.5.1 Safety activities

Which safety design activities are covered by the mean or tool (see [3] section 1.2) ?

	Author	Assessor 1	Assessor 2	Total
Preliminary Hazard Analysis				
Establish Safety Plan				
System Hazard and Risk Analysis				
Risk Assessment				
Specification of System Safety Requirements				
Define Safety Related Functional Requirements				
Specify Sub-System and Component Safety requirements				
Implement Safety Plan				
Verify System, Sub-System and Component Safety requirements				
Validate System Safety Requirements				
Establish Safety Case				

2.5.2 Input Artifacts

Which artifacts are used as input of the mean or tool (see [3] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Safety Requirement				
Hazard log				
Safety Plan				
Safety Case				
Code Safety Backlog				
Detailed Model Safety Backlog				
High Level Safety Backlog				

2.5.3 Output Artifacts

Which artifacts are used as output of the mean or tool (see [3] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Safety Requirement				
Hazard log				
Safety Plan				
Safety Case				
Code Safety Backlog				
Detailed Model Safety Backlog				
High Level Safety Backlog				

2.5.4 Expressiveness

Which degree of formalisation is given to the artifacts by mean or tools (see [3] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Informal				
Semi-Formal				
Formal				

2.5.5 Other criteria

According to [3] section 2.2, provide some complement on the mean or tool:

	Author	Assessor 1	Assessor 2	Total
Top-Down approach				
Bottom-up approach				
Database capability				
Database query ability				
Safety requirement VnV				
Traceability				
Generation of documentation				

2.6 Means and tools for data, function and requirement management

Which activites, linked to help the management of SSRS definition and whole process are covered by the mean or tool ?

	Author	Assessor 1	Assessor 2	Total
Requirement Capturing				
Requirement management				
Data management				
Function management				
Requirement traceability				
Model traceability				
Function architecture				
Version management				
Others (give details)				

2.6.1 Input Artifacts

Which artifacts are used as input of the mean or tool ?

	Author	Assessor 1	Assessor 2	Total
Informal description				
Structured description				
Spread sheet				
EFS model				
DSL				
Others (give details)				

2.6.2 Output Artifacts

Which artifacts are used as output of the mean or tool ?

	Author	Assessor 1	Assessor 2	Total
Informal description				
Structured description				
Spread sheet				
EFS model				
DSL				
Others (give details)				

2.6.3 Other Criterias

Comment. MPD : Todo Ideas welcomed !

2.7 Means and tools for model transformation and code generation

Which transformations are covered by the mean or tool ?

	Author	Assessor 1	Assessor 2	Total
Model transformation for design				
Model transformation for VnV				
Code Generation				
EMF transformation				

2.7.1 Input Artifacts

Which artifacts are used as input of the mean or tool ?

	Author	Assessor 1	Assessor 2	Total
Informal description				
SysML model				
Scade model				
EFS model				
Classical B modes				
C Code				
Others (give details)				

2.7.2 Output Artifacts

Which artifacts are used as output of the mean or tool ?

	Author	Assessor 1	Assessor 2	Total
Informal description				
SysML model				
Scade model				
EFS model				
Classical B modes				
C Code				
Others (give details)				

2.7.3 Process

How process the tool, with which characteristics (please provides comments) ?

	Author	Assessor 1	Assessor 2	Total
Informal				
Model To Text (M2T)				
Model To Model (M2M)				
EMF models				
others				

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)**

Appendix: References

[1] Sylvain Baro and Jan Welte. Requirements for openETCS. Technical Report D2.6, OpenETCS, 2013.

[2] Marielle Petit-Doche and WP7 Participants. D7.1: Report on the final choice of the primary toolchain. Primary Toolchain OETCS/WP7/D7.1, openETCS, July 2013.

[3] Jan Welte. Preliminary safety evaluation criteria. Technical Report D4.2a, openETCS, May 2013.