OETCS/WP7/O7.2.1 – 00/05

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

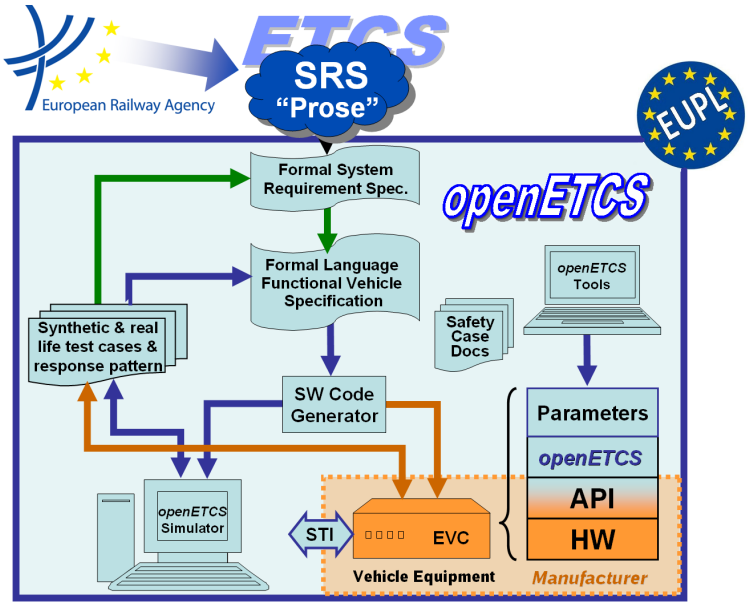
Work-Package 7: “Secondary tools - Safety”

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

October 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 7: “Secondary tools - Safety” **OETCS/WP7/O7.2.1 – 00/05**
October 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.

This document focusses on means and tools to support safety analyses.

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 - Safety
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. Safety part
00.06	18/10/2013	M. Petit-Doche	Issues: 174, 178, 167
00.07	08/11/2013	M. Petit-Doche	Issues: 176; Appendix added

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 [3], and the results of T7.1 on the primary toolchain [5], 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 to support safety analyses.

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 :

- Rodin and Pluggins
- CPN tools
- Goal Structuring Notation (GSN)
- Safety Architect

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 (inspired from Technology Readiness Level, see http://en.wikipedia.org/wiki/Technology_readiness_level) :

0 not recommended / rejected / no integration possible or valuable / not adapted for this topic / not available for this topic

1 weakly recommended / adapted after major improvements / weakly rejected / concept of integration roughly defined / adapted after major improvements / available after major developments

2 recommended / adapted (with light improvements if necessary) weakly accepted / integration prototyped or defined in details / adapted after small improvements / available after small developments or tests

3 highly recommended / well adapted / strongly accepted / integration done and tested / well adapted to the purpose / available and suitable for the purpose All the notes can be commented under each table.

***** 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)

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 level of tool qualification has been reached or will be reached within the next year ?

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 Means and tools for safety activities support

This section defines the criteria for the means and tools dedicated to support of safety activities, in the WP4 workpackage.

Criteria of this section are defined according [7].

2.4.1 Safety activities

Which safety design activities are covered by the mean or tool (see [7] section 1.2) ?

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

2.4.2 Input Artifacts

Which artifacts are used as input of the mean or tool (see [7] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Safety Requirement				
Hazard log				
Safety Case				

2.4.3 Output Artifacts

Which artifacts are used as output of the mean or tool (see [7] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Safety Requirement				
Hazard log				
Safety Case				

2.4.4 Expressiveness

Which degree of formalisation is given to the artifacts by mean or tools (see [7] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Informal				
Semi-Formal				
Formal				

2.4.5 Other criteria

According to [7] 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				

2.5 Other comments

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

3 Conclusion

The process of evaluation of secondary tools has evolved during the task: means and tools have been presented to all the partners but partly evaluated. Partners decided to based the evaluation and selection on the needs which are raised during the development of the toolchain or its use in the OpenETCS project.

In Appendix there are some results of the evaluation.

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.

Appendix A: Color Petri Nets tools

No results of evaluation.

Appendix B: Goal Structured Notation

No results of evaluation.

Appendix C: Safety Architect

No results of evaluation.

Appendix D: Rodin

D.1 Author and Assessors

Author Matthias Güdemann — Systerel

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

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

D.2 Presentation

Name Event-B and the Rodin platform

Web site `http://www.event-b.org`

Licence Common Public License Version 1.0 (CPL)

Abstract

Rodin is an open source tool for formal modeling and verification on the system level using the Event-B formalism. Event-B is based on set-theoretic notation of first-order logic (FOL) and has its roots in the B method which has a long history of successful application in industry on software level development.

Rodin is fully integrated into the Eclipse platform and is therefore fully extensible through plug-ins. Existing plug-ins include graphical modeling using state-machines, model simulators, modern state-of-the art SMT solvers and Rational DOORS interoperable requirements tracing using ReqIf documents and ProR.

Publications

- The leaflet [6] contains a short overview of the Rodin tool
- The book [4] explains the usage of Rodin and serves as a gentle introduction into Event-B modeling in Rodin
- The book [1] contains an extensive presentation of Event-B an several modeling examples for different system
- The scientific journal article [2] contains an in-depth look at the integration of Event-B into the Rodin platform

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

	Author	Assessor 1	Assessor 2	Total
Data Management	0			
Function Management	2			
Requirement Management	2			
Version Management	2			
Other (give details below)	3			

Author: Rodin is a specialized tool to formally model and verify abstract functional behavior. Therefore data management is not in its scope, as this is clearly a lower level detail aspect, more on the implementation level.

Function Management: *A Rodin model contains high level function descriptions, i.e., an abstract view of the observable system behavior and its effect on the system state. It is therefore well suited to be included in function management, by formalizing the abstract behavior of the functions, tracing any changes and observing their effect on the intended functioning of the system.*

Version Management: *Rodin does not contain a version management itself. Its files are based on XML, therefore any modern version control system can be used, in particular those (like svn/mercurial/git) for which an Eclipse plug-in exists. There also exists a pug-in that is compatible to model-compare in Eclipse, i.e., allows for comparison on the model level instead of text level.*

Other: *Rodin can provide an important support for* ***traceability****, which is missing here. It allows for linking formal model aspects to a requirements document, e.g., a ReqIf document in ProR. Any changes in the specification can therefore be traced in the formal Event-B model and system-level aspects can be formally verified.*

D.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.

D.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)	3			
Portability to operating systems (D2.6-02-075)	3			
Cooperation of tools (D2.6-02-076)	3			
Robustness (D2.6-02-078)	3			
Modularity (D2.6-02-078.1)	3			
Documentation management (D2.6-02-078.02)	2			
Distributed software development (D2.6-02-078.03)	3			
Simultaneous multi-users (D2.6-02-078.04)	2			
Issue tracking (D2.6-02-078.05)	2			
Differences between models (D2.6-02-078.06)	2			
Version management (D2.6-02-078.07)	3			
Concurrent version development (D2.6-02-078.08)	3			
Model-based version control (D2.6-02-078.09)	2			
Role traceability (D2.6-02-078.10)	1			
Safety version traceability (D2.6-02-078.11)	3			
Model traceability (D2.6-02-079)	3			
Tool chain integration	3			
Scalability	2			
User Friendliness	2			

Author: Rodin is based on Eclipse, therefore existing plug-ins can be used for many of the above aspects. Many of those are applicable without any changes, for others, some Rodin / Event-B specific modifications might be necessary.

D.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)	3			
Proof of correctness (D.2.6-01-42.03)	2			
Existing industrial usage	3			
Model verification	3			
Test generation	0			
Simulation, execution, debugging	3			
Formal proof	3			

Which level of tool qualification has been reached or will be reached within the next year ?

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	2			
class T2	2			
class T3	0			

Author: The Rodin tool aims at system-level analysis, therefore it will not be necessary to qualify it as T3 tool, as no output is generated that can directly contribute to the executable code.

Other elements for tool certification

D.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.

D.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	2			
Scade method	1			
EFS language	0			
B Method	3			
C language	2			

SysML

How the means or tools can complete SysML ?

Author: Rodin allows graphical modeling of (UML) state machines, which are encoded into Event-B models. SysML state machines are very similar to this and with a bit of effort could be supported directly.

Scade, EFS, Classical B

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

Author: A light-weight interoperability with SCADE is possible, either via SCADE Systems which uses SysML or via SCADE state machines. This would allow a larger effort for integration. The data-flow part of SCADE does not seem to be applicable in an Event-B model.

As Event-B has its roots in the B language, several aspects of these languages are definitively compatible. For example the invariant predicates of Event-B can directly be used in a lower level B model. If the abstraction levels for data are not the same, an additional refinement step could be added to solve this problem.

There does not seem to be a good interoperation possibility with the EFS language.

C language

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

Author: A possible combination of an Event-B model and a C implementation is to use the predicate logic invariants as C asserts and the guards as preconditions of functions. As the abstraction level of the C implementation is much lower than the Event-B models, this would require some work to identify the right functions and data formats or to introduce higher level wrapper functions similar to Event-B events. Such asserts and pre-conditions could be verified by tools like SPARK, why3 etc.

D.3.4 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	3			
Papyrus	2			
Scade	1			
EFS tools	1			
B tools	2			

Eclipse

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

Author: The Rodin platform is fully based on Eclipse.

Papyrus

How the means or tools can complete Papyrus ?

Author: The existing graphical modeling plug-ins for Rodin could be connected to Papyrus. This would require the development of a transformation of the different formats.

Scade, EFS, Classical B

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

Author: With SCADE there could be the possibility of interoperation via the SCADE System SysML framework.

With Classical B tools, there is the possibility to generate predicates for guards and invariants directly from the Event-B model. As classical B is based on text files and Event-B on XML file, there would be some development work to do.

For the EFS tools there are some interoperation possibilities on the EMF level, as both Rodin and EFS have an EMF model of the artifacts. However, as seen in the section above, how the two languages could interoperate is not clear.

D.4 Means and tools for safety activities support

This section defines the criteria for the means and tools dedicated to support of safety activities, in the WP4 workpackage.

Criteria of this section are defined according [7].

D.4.1 Safety activities

Which safety design activities are covered by the mean or tool (see [7] section 1.2) ?

	Author	Assessor 1	Assessor 2	Total
Preliminary Hazard Analysis	0			
System Hazard and Risk Analysis	0			
Risk Assessment	0			
Specification of System Safety Requirements	2			
Define Safety Related Functional Requirements	3			
Specify Sub-System and Component Safety requirements	2			
Verify System, Sub-System and Component Safety requirements	2			
Validate System Safety Requirements	3			
Establish Safety Case	2			

Author: Rodin and Event-B do not directly support a hazard or risk analysis. Their goal is to strengthen the confidence in the correctness of an external safety analysis, by providing means to represent safety requirements (in particular functional requirements) in a formal model and to verify them there or to validate the intended behavior wrt. safety by simulating and observing the model.

Sub-system requirements can be specified and verified, if the formal model contains a representation of the sub-systems. While this can be achieved by refinement, it should be

kept in mind that Event-B aims at system-level modeling and analysis, and therefore there could be better alternatives to analyze a very detailed model on implementation level.

D.4.2 Input Artifacts

Which artifacts are used as input of the mean or tool (see [7] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Safety Requirement	3			
Hazard log	1			
Safety Case	3			

Author: The main application of Rodin is to formalize and verify the safety requirements where applicable. This supports the verification of the correctness of the arguments in the safety case, therefore strengthening the confidence in these arguments, but also to provide insight into probably lacking aspects of the safety case.

D.4.3 Output Artifacts

Which artifacts are used as output of the mean or tool (see [7] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Safety Requirement	3			
Hazard log	1			
Safety Case	3			

Author: The output of Rodin could be a detected error or lacking element in on of the safety requirement or in the argumentation of the safety case. It can therefore provide important feedback and increase the quality of the requirements and the confidence in the safety case.

D.4.4 Expressiveness

Which degree of formalisation is given to the artifacts by mean or tools (see [7] section 1.4) ?

	Author	Assessor 1	Assessor 2	Total
Informal	0			
Semi-Formal	0			
Formal	3			

Author: The Event-B language is fully formal.

D.4.5 Other criteria

According to [7] section 2.2, provide some complement on the mean or tool:

	Author	Assessor 1	Assessor 2	Total
Top-Down approach	3			
Bottom-up approach	0			
Database capability	1			
Database query ability	1			
Safety requirement VnV	3			
Traceability	3			
Generation of documentation	2			

Author: The Event-B approach is based on iterative refinements form the most abstract model to the desired level of detail. It is therefore a to-down approach, a bottom-up approach does not make sense using Event-B.

And database connection would require the development of additional plug-ins, but would be possible.

VnV of safety requirements is achieved by formal proof and simulation to validate correct functionality.

Traceability is achieved by the connection to ProR.

Generation of some documentation is already supported, as Latex documents can be generated from models. For more extensive documentation, e.g., links with safety requirements, some additional functionality would have to be developed.

D.5 Other comments

Author: The application of Rodin for safety activity support consists mainly of a strong connection of (formalized) safety requirements to a formal model. This allows for

- *validation of the intended functionality via simulation*
- *tracing of the safety requirments in the formal model*
- *verification of the correctness and completeness of requirements via formal proof*
- *providing feedback of the safety requirements and safety case*
- *increasing the confidence in the argumentation of the safety case*

Appendix: References

[1] Jean-Raymond Abrial. *Modeling in Event-B: System and Software Engineering*. Cambridge University Press, New York, NY, USA, 1st edition, 2010.

[2] Jean-Raymond Abrial, Michael Butler, Stefan Hallerstede, Thai Son Hoang, Farhad Mehta, and Laurent Voisin. Rodin: an open toolset for modelling and reasoning in Event-B. *STTT*, 12(6):447–466, 2010.

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

[4] Michael Jastram (Ed.). Rodin user's handbook. `http://handbook.event-b.org`, 2012.

[5] 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.

[6] Systerel. `http://sourceforge.net/projects/rodin-b-sharp/files/Doc_Rodin_General/Rodin_Leaflets/Leaflet_Rodin_E.pdf/download`, 2012.

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