

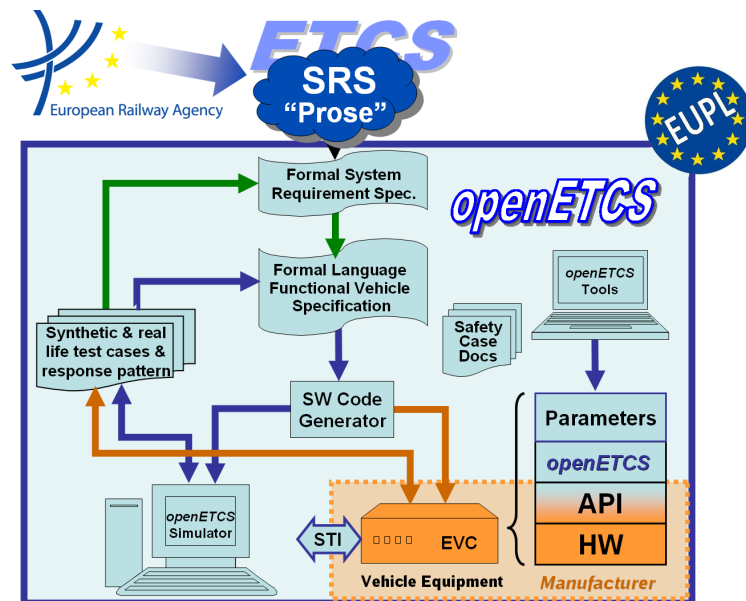
Work-Package 7: “Secondary tools - Safety”

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, model 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.

Disclaimer: This work is licensed under the "openETCS Open License Terms" (oOLT) dual Licensing: European Union Public Licence (EUPL v.1.1+) AND Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER openETCS OPEN LICENSE TERMS (oOLT) WHICH IS A DUAL LICENSE AGREEMENT INCLUDING THE TERMS OF THE EUROPEAN UNION PUBLIC LICENSE (VERSION 1.1 OR ANY LATER VERSION) AND THE TERMS OF THE CREATIVE COMMONS PUBLIC LICENSE ("CCPL"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS OLT LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

<http://creativecommons.org/licenses/by-sa/3.0/>
<http://joinup.ec.europa.eu/software/page/eupl/licence-eupl>

Table of Contents

| | |
|---|-----------|
| Figures and Tables..... | v |
| 1 Introduction..... | 1 |
| 1.1 Organisation of the document | 1 |
| 2 Template | 2 |
| 2.1 Instructions | 2 |
| 2.2 Presentation | 3 |
| 2.3 Common criteria on secondary means and tools | 3 |
| 2.3.1 Project and WP2 requirements | 3 |
| 2.3.2 Qualification | 4 |
| 2.3.3 Complementarity with primary toolchain | 5 |
| 2.4 Means and tools for safety activities support | 6 |
| 2.4.1 Safety activities | 6 |
| 2.4.2 Input Artifacts | 6 |
| 2.4.3 Output Artifacts | 7 |
| 2.4.4 Expressiveness | 7 |
| 2.4.5 Other criteria | 7 |
| 2.5 Other comments | 7 |
| 3 Conclusion..... | 8 |
| 3.1 Main usage of the approach | 8 |
| Appendix A: Color Petri Nets tools | 9 |
| A.1 Instructions | 9 |
| A.2 Presentation | 10 |
| A.3 Common criteria on secondary means and tools | 10 |
| A.3.1 Project and WP2 requirements | 10 |
| A.3.2 Qualification | 11 |
| A.3.3 Complementarity with primary toolchain | 12 |
| A.4 Means and tools for safety activities support | 13 |
| A.4.1 Safety activities | 13 |
| A.4.2 Input Artifacts | 13 |
| A.4.3 Output Artifacts | 14 |
| A.4.4 Expressiveness | 14 |
| A.4.5 Other criteria | 14 |
| A.5 Other comments | 14 |
| Appendix B: Goal Structured Notation | 15 |
| B.1 Instructions | 15 |
| B.2 Presentation | 16 |
| B.3 Common criteria on secondary means and tools | 16 |
| B.3.1 Project and WP2 requirements | 16 |
| B.3.2 Qualification | 17 |
| B.3.3 Complementarity with primary toolchain | 18 |
| B.4 Means and tools for safety activities support | 19 |
| B.4.1 Safety activities | 19 |

| | |
|---|-----------|
| B.4.2 Input Artifacts | 19 |
| B.4.3 Output Artifacts | 20 |
| B.4.4 Expressiveness | 20 |
| B.4.5 Other criteria | 20 |
| B.5 Other comments | 20 |
| Appendix C: Safety Architect..... | 21 |
| C.1 Instructions | 21 |
| C.2 Presentation | 22 |
| C.3 Common criteria on secondary means and tools | 22 |
| C.3.1 Project and WP2 requirements | 22 |
| C.3.2 Qualification | 23 |
| C.3.3 Complementarity with primary toolchain | 24 |
| C.4 Means and tools for safety activities support | 25 |
| C.4.1 Safety activities | 25 |
| C.4.2 Input Artifacts | 25 |
| C.4.3 Output Artifacts | 26 |
| C.4.4 Expressiveness | 26 |
| C.4.5 Other criteria | 26 |
| C.5 Other comments | 26 |
| Appendix D: Rodin..... | 27 |
| D.1 Instructions | 27 |
| D.2 Presentation | 28 |
| D.3 Common criteria on secondary means and tools | 28 |
| D.3.1 Project and WP2 requirements | 28 |
| D.3.2 Qualification | 29 |
| D.3.3 Complementarity with primary toolchain | 30 |
| D.4 Means and tools for safety activities support | 31 |
| D.4.1 Safety activities | 31 |
| D.4.2 Input Artifacts | 31 |
| D.4.3 Output Artifacts | 32 |
| D.4.4 Expressiveness | 32 |
| D.4.5 Other criteria | 32 |
| D.5 Other comments | 32 |
| Appendix: References | 33 |

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 [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 (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 [3].

2.4.1 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 | | | | |
| 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 [3] 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 [3] 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 [3] section 1.4) ?

| | Author | Assessor 1 | Assessor 2 | Total |
|-------------|--------|------------|------------|-------|
| Informal | | | | |
| Semi-Formal | | | | |
| Formal | | | | |

2.4.5 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 | | | | |

2.5 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) |

Appendix A: Color Petri Nets tools

A.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.

A.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)

A.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.

A.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 | | | | |

A.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

A.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.

A.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 ?

A.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 ?

A.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 [3].

A.4.1 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 | | | | |
| 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 | | | | |

A.4.2 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 Case | | | | |

A.4.3 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 Case | | | | |

A.4.4 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 | | | | |

A.4.5 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 | | | | |

A.5 Other comments

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

Appendix B: Goal Structured Notation

B.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.

B.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)

B.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.

B.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 | | | | |

B.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

B.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.

B.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 ?

B.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 ?

B.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 [3].

B.4.1 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 | | | | |
| 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 | | | | |

B.4.2 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 Case | | | | |

B.4.3 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 Case | | | | |

B.4.4 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 | | | | |

B.4.5 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 | | | | |

B.5 Other comments

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

Appendix C: Safety Architect

C.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.

C.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)

C.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.

C.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 | | | | |

C.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

C.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.

C.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 ?

C.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 ?

C.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 [3].

C.4.1 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 | | | | |
| 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 | | | | |

C.4.2 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 Case | | | | |

C.4.3 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 Case | | | | |

C.4.4 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 | | | | |

C.4.5 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 | | | | |

C.5 Other comments

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

Appendix D: Rodin

D.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.

D.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)

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) | | | | |
| 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 | | | | |

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) | | | | |
| 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

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 | | | | |
| 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 ?

D.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 ?

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 [3].

D.4.1 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 | | | | |
| 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 | | | | |

D.4.2 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 Case | | | | |

D.4.3 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 Case | | | | |

D.4.4 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 | | | | |

D.4.5 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 | | | | |

D.5 Other comments

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

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.