OETCS/WP7/D7.2 – 00/01

ITEA2 Project
Call 6 11025
2012 – 2015

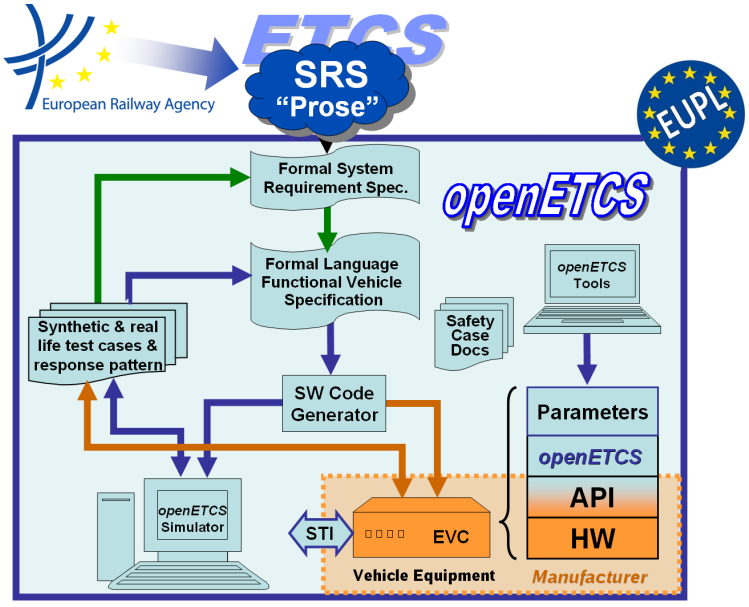
Work-Package 7: “Secondary tools”

Report on all aspects of secondary tooling

Results of T7.2

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

December 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/D7.2 – 00/01
December 2013

Report on all aspects of secondary tooling

Results of T7.2

Marielle Petit-Doche

Systerel

all participants of the benchmark

WP7 partners

all participants of VnV and Safety process

WP4 partners

Deliverable

Prepared for openETCS@ITEA2 Project

Abstract: This document gives results of the evaluation and selection of the tools and methods to complete the secondary toolchain and to support verification and validation activities, safety activities, model transformation and data management for the whole project.

Table of Contents

Figures and Tables

Figures

Tables

Document information	
Work Package	WP7
Deliverable ID or doc. ref.	D7.2
Document title	Report on all aspects of secondary tooling
Document version	00.01
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-T7.2 Sub-Task Leader	
Approved by	Michael Jastram	WP7 leader	

Document evolution			
Version	Date	Author(s)	Justification
00.01	19/12/2013	M. Petit-Doche	Document creation

1 Introduction

The aim of this document is to report the results of the evaluation of means and tools for the secondary toolchain, 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:

- data, function and requirement management (SSRS, WP3 and WP4), in chapter 2;
- verification and validation (WP4), in chapter 3;
- safety activities support (WP4), in chapter 4;
- model transformation and code generation (WP3 and WP4), in chapter 5.

1.1 Approach

(mj) Content to be discussed in https://github.com/openETCS/toolchain/issues/236

2 Data and Requirements Management

This section is dedicated to tools and means to support management of data, functions requirements and other artifacts along the openETCS process.

In total, seven tools have been proposed. Out of these, only one has been evaluated in detail (ProR). What follows is a qualitative description of the seven tools. A quantitative evaluation of ProR is included as well.

2.1 Candidates

The list of initial candidates is:

Scade Suite. Scade includes Reqtify as the requirements traceability solution. It allows to create traceability directly to Word, thereby making traceability to Subset-26 easy. However, there is no clear solution for authoring additional requirements (except using Word). Further, it is not clear how traceability to model artifacts should be realized. Last, this is a closed source solution and therefore only a last resort.

Rodin and Pluggin.

Matelo.

Goal Structuring Notation (GSN).

Eclipse ProR.

Eclipse EMF Store.

Eclipse EMF Client Platform.

During the evaluation phase, a number of challenges were identified that were not clearly defined before. The list of challengers discussed during the evaluation is:

- Ecore model + XML files
- UML library
- ReqCity

2.1.1 ProR Evaluation

TODO the details of the ProR evaluation, corresponding to the primary toolchain evaluations.

2.1.2 EventB, Rodin and pluggins

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

A quantitative evaluation is available in `https://github.com/openETCS/toolchain/blob/master/T7.2/O7.2.1_Safety/O7-2-1_Safety.pdf`

Added value for OpenETCS project

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.

Integration in OpenETCS process and toolchain

The Rodin platform is fully based on Eclipse.

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.

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.

2.2 Open issues

2.2.1 Traceability

TODO

2.2.2 How to Deal with Subset-26

TODO

2.3 Selected means and tools

Comment. To complete after decision meeting with a section for each tool with the following contents:

- *description of the means or tools, references and links*
- *added value for openETCS*
- *for which tasks and how (input/output/actions) is the mean or tools used.*

3 Verification and Validation

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

3.1 Candidates

The list of initial candidates is:

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

3.1.1 SystemC

Name SystemC

Web site `www.accellera.org/downloads/standards/systemc/about_systemc/`

Licence SystemC Open Source License

Abstract

SystemC is a C++ library providing an event-driven simulation interface suitable for electronic system level design. It enables a system designer to simulate concurrent processes. SystemC processes can communicate in a simulated real-time environment, using channels of different datatypes (all C++ types and user defined types are supported). SystemC supports hardware and software synthesis (with the corresponding tools). SystemC models are executable.

Publications

- D. C. Black, SystemC: From the ground up. Springer, 2010.
- IEEE 1666 Standard SystemC Language Reference Manual, http://standards.ieee.org/getieee/1666/
- The ITEA MARTES Project, from UML to SystemC, http://www.martes-itea.org/
- J. Bhasker, A SystemC Primer, Second Edition, Star Galaxy Publishing, 2004
- F. Ghenassia (Editor), Transaction-Level Modeling with SystemC: TLM Concepts and Applications for Embedded Systems, Springer 2006

A quantitative evaluation is available in https://github.com/openETCS/toolchain/blob/master/T7.2/O7.2.1_VnV/O7-2-1_VnV.pdf

Added value for OpenETCS project

Comment. To complete: Stefan Rieger ?

Integration in OpenETCS process and toolchain

Comment. To complete: Stefan Rieger ?

3.1.2 UPPAAL

Name UPPAAL

Web site www.uppaal.org

Licence Academic free or commercial license

Abstract

Uppaal is an integrated tool environment for modeling, validation and verification of real-time systems modeled as networks of timed automata, extended with data types (bounded integers, arrays, etc.).

Publications

Short list of publications on the approach (5 max) Please refer to http://dblp.org/search/#query=uppaal

A quantitative evaluation is available in https://github.com/openETCS/toolchain/blob/master/T7.2/O7.2.1_VnV/O7-2-1_VnV.pdf

Added value for OpenETCS project

Comment. To complete: Stefan Rieger ?

Integration in OpenETCS process and toolchain

Comment. To complete: Stefan Rieger ?

3.1.3 CPN Tools

Name CPN Tools

Website http://cpntools.org/

Licence Open Source (GPL/LGPL)

Abstract

CPN Tools is a tool for editing, simulating, and analyzing Colored Petri nets.

The tool features incremental syntax checking and code generation, which take place while a net is being constructed. A fast simulator efficiently handles untimed and timed nets. Full and partial state spaces can be generated and analyzed, and a standard state space report contains information, such as boundedness properties and liveness properties.

Publications

Please refer to http://cpntools.org/publications

Slides available on github `https://github.com/openETCS/model-evaluation/blob/master/Telco_Secondary_slides/b-Introduction_CPNTools.pdf`.

A quantitative evaluation is available in `https://github.com/openETCS/toolchain/blob/master/T7.2/O7.2.1_VnV/O7-2-1_VnV.pdf`

Added value for OpenETCS project

Comment. To complete: Stefan Rieger , Jan Welte ?

Integration in OpenETCS process and toolchain

Comment. To complete: Stefan Rieger , Jan Welte ?

3.2 Selected means and tools

Comment. To complete after decision meeting with a section for each tool with the following contents:

- *description of the means or tools, references and links*
- *added value for openETCS*
- *for which tasks and how (input/output/actions) is the mean or tools used.*

4 Safety support

This section is dedicated to tools and means to support safety analyses.

4.1 Candidates

The list of initial candidates is:

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

4.1.1 EventB, Rodin and pluggins

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 [**?**] contains a short overview of the Rodin tool
- The book [**?**] explains the usage of Rodin and serves as a gentle introduction into Event-B modeling in Rodin
- The book [**?**] contains an extensive presentation of Event-B an several modeling examples for different system

- The scientific journal article [**?**] contains an in-depth look at the integration of Event-B into the Rodin platform

A quantitative evaluation is available in `https://github.com/openETCS/toolchain/blob/master/T7.2/O7.2.1_Safety/O7-2-1_Safety.pdf`

Added value for OpenETCS project

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.

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.

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.

Integration in OpenETCS process and toolchain

The Rodin platform is fully based on Eclipse.

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.

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.

4.2 Selected means and tools

Comment. To complete after decision meeting with a section for each tool with the following contents:

- *description of the means or tools, references and links*
- *added value for openETCS*
- *for which tasks and how (input/output/actions) is the mean or tools used.*

5 Model transformation and Code generation

This section is dedicated to tools and means for model transformation and code generation.

5.1 Candidates

The list of initial candidates is:

- Scade Suite
- Rodin and Pluggins
- Acceleo
- ATL
- QVTO and SmartQVT
- Xtend

5.1.1 Acceleo

Name Acceleo

Web site http://www.eclipse.org/acceleo/

Licence Eclipse

Abstract

Short abstract on the approach and tool (10 lines max) Acceleo is an implementation of the Object Management Group (OMG) MOF Model to Text Language (MTL) standard. Based on a special template language model to text transformations can be defined. It is fully integrated with Eclipse and also part of Polarsys.

Publications

Short list of publications on the approach (5 max) Most imformation is available on the homepage http://www.eclipse.org/acceleo/

Added value for OpenETCS project

Comment. To complete: Stefan Rieger ?

Integration in OpenETCS process and toolchain

Comment. To complete: Stefan Rieger ?

5.2 Selected means and tools

Comment. To complete after decision meeting with a section for each tool with the following contents:

- *description of the means or tools, references and links*
- *added value for openETCS*
- *for which tasks and how (input/output/actions) is the mean or tools used.*

6 Conclusion

Comment. MPD : Todo

To complete after Munich meeting in January 2014.

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.