openETCS/WP2/D2.6

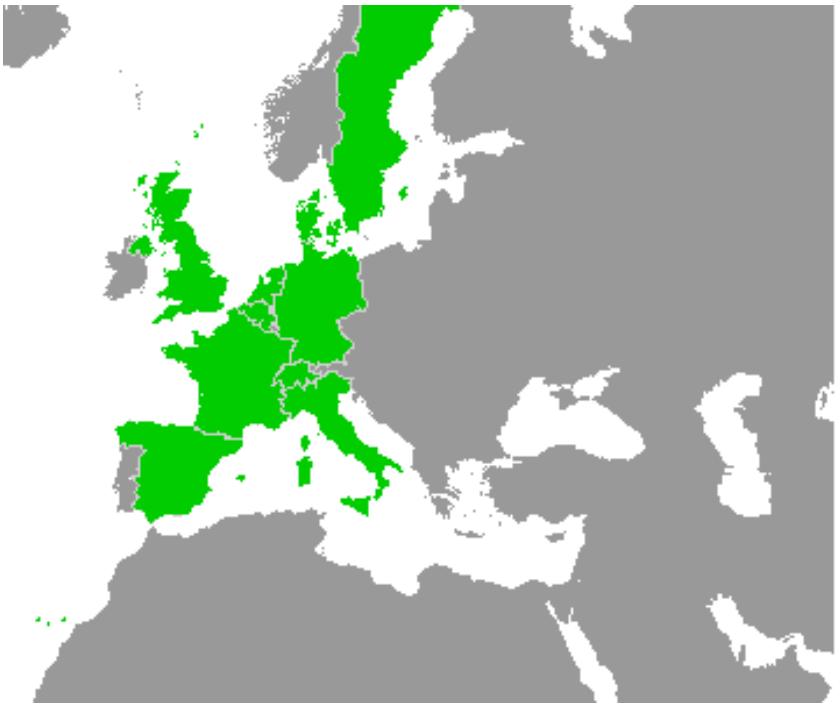
ITEA2 Project
2012 – 2015

Work-Package 2: "Requirements for Open Proofs"

Draft - List of Requirements for formal software development

Jan Welte and Hansjörg Manz

December 2012



openETCS

Draft - List of Requirements for formal software development

Jan Welte and Hansjörg Manz

Technische Universität Braunschweig
Institute for Traffic Safety and Automation Engineering
Langer Kamp 8
38106 Braunschweig, Germany
eMail: openetcs@iva.ing.tu-bs.de

Draft

Prepared for ITEA2 openETCS consortium

Abstract: This is a first collection of requirements based on the interviews with various experts from the railway industry. the list of requirements shall provide a starting point to collect and discuss requirements and their specifications for the open proof methodology and the resulting toolchain.

Table of Contents

1 Introduction

This documents presents the first collection of requirements for means of descriptions, methodologies and tools to establish a formal development process and a related toolchain. As this first collection of requirements is based on 14 interviews with experts from the railway sector and other industries. Overall between September and November 2012 21 experts from 12 organisation have answered questions concerning their development approaches, their experiences with different means of descriptions, methodologies and tools, and their requirements for formal model based development. Since the experts overall only described general requirements, more detail have to be defined to establish the requirements for all aspects of the software development process. Furthermore this collection of requirements does not provide any comparison of requirements to assess their affiliations.

As this first list shall serve as help to find a structured approach for the requirement collection further discussions have to specify the following hierarchical levels for all requirements to allow traceability:

- characteristic,
- property,
- measurement, and
- value.

2 Requirements

2.1 Means of Description

The VDI/VDE 3681 guideline provides a list of characteristics to classify means of description. This includes the following seven characteristics which could be used to group the requirements:

- Formal basis
- Representation
- Description of structure
- Description of behaviour
- Explicit time representation
- Synchronisation
- Tool support

Additionally the following two aspects are relevant for means of descriptions:

- Required expertise
- Level of standardisation

Table /reftab:reqMoD list the requirements that have been named during the interviews. Thereby the requirements are structured according to VDI/VDE 3681 characteristics.

Table 1. Collection of Requirements for Means of Description

Characteristic	Property	Measurement	Value
Formal basis	Support formal proof		
	Support model execution (especially for high level models)		
Representation	Support graphical modelling		
Description of structure	Capturing structure of all ETCS specifications		
Description of behaviour	Capturing behaviour of all ETCS specifications		
Explicit time representation			
Synchronisation			
Tool support	Support specification of test cases		
	Support model execution (especially for high level models)		
Required expertise	Understandable for domain experts, costumers and other relevant groups (communication with modelling experts)		
Level of standardisation	Well documented (better standardised)		

2.2 Methodology

The main requirements for the methodologies are provided by the EN 50128. The Open Proof approach in general only requires a combination of formal methods and model-based development as basis for verification and validation through formal proofs and testing.

The following requirements have been named during the interviews:

- Conform to CENELEC standards
- Easy to apply in practice
- Clear traceability of changes and their influences
- Provide mainly automatic theorem proving and model checking

2.3 Tools

As presented during the CENELEC workshop in Paris the ISO/IEC 9126 classifies software quality by six characteristics. These have been used in table 2 to make a first grouping of all requirements for tools presented during the interviews.

Table 2. Collection of Requirements for Tools

Characteristic	Property	Measurement	Value
Functionality	Compatible with existing configuration management systems		
	Allow automatic generation of textual documents from models		
	Automatic link generation between glossary and models		
Reliability	Robustness		
	Validated		
Usability	Visualisation for good usability		
	Allow multi user work (avoidance of conflicts)		
Efficiency	Good performance on standard systems		
Maintainability	High level support and easy maintenance		
Portability	Downwards compatible		
	Independent of operating system		
	Open interfaces for data (import and export data)		
	Integration in tool chain (data exchange and visual interface)		