OETCS/WP1/D1.3.1

openETCS

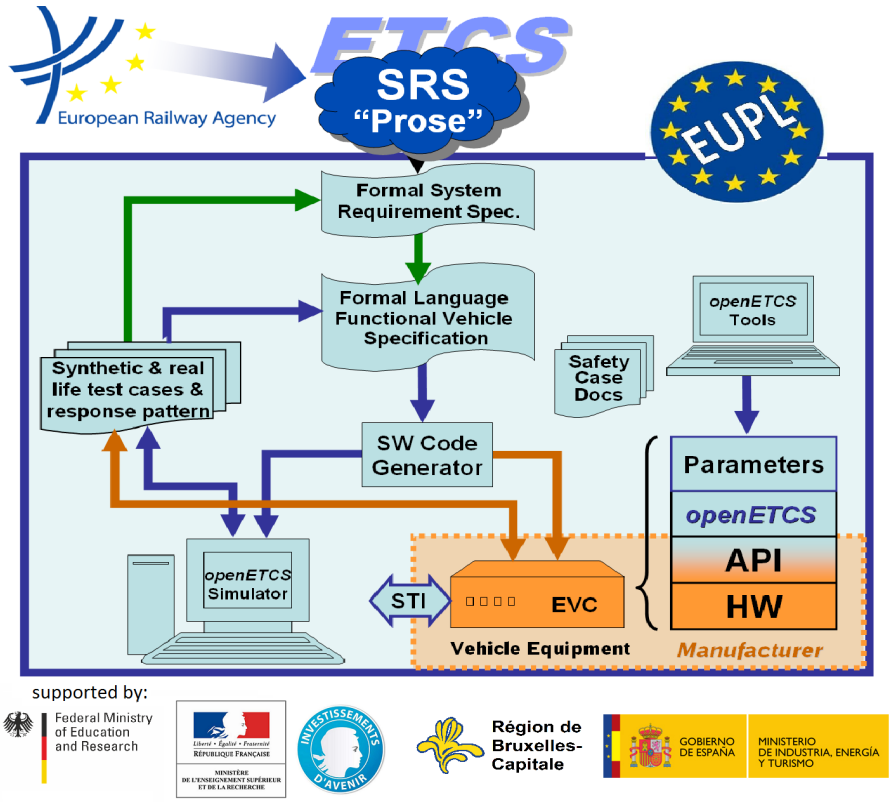
ITEA2 Project
Call 6 11025
2012 – 2015

Work-Package 1: “Management”

# Project Quality Assurance Plan

SQS

April 15, 2013



This page is intentionally left blank

**Work-Package 1: “Management”**

**OETCS/WP1/D1.3.1**
**April 15, 2013**

# Project Quality Assurance Plan

SQS

Avenida Zugazarte 8
48930 Getxo, Spain

Description of work



Prepared for ITEA2 openETCS consortium
Europa

# Contents



## Document History

| Version | Date | Chapters modified | Reason | Name |
|---|---|---|---|---|
| 0.0.0 | 15.11.2012 | All | First Steps on frame evaluation | Rico Kaseroni (DB)<br>Peyman Farhangi (DB) |
| 0.1.0 | 27.11.2012 | All | First Steps on Content | Rico Kaseroni (DB)<br>Jan Welte (TUB)<br>Peyman Farhangi (DB)<br>Matthias Kuhn (DB) |
| 0.1.1 | 29.11.2012 | All | Optimaziation of document structure, Revision of Chapters according to EN 50128, Merging with project specific tasks | Stephan Jagusch (AEbt)<br>Rico Kaseroni (DB)<br>Cyril Cornu (All4tec) |
| 0.2.0 | 30.11.2012 | Baseline Requirements for certification | Extention of Chapter according to EN 50128 | Jan Welte (TUB)<br>Rico Kaseroni (DB) |
| 0.3.0 | 19.12.2012 | All | Extention of Chapter 0, 1, 2, 3 | All4Tech, DB, SQS |
| 0.4.0 | 11.01.2013 | All | Extention to existing and further Chapters | All4Tech, DB, SQS |
| 0.6.0 | 28.01.2013 | All | IP Clean | Rico Kaseroni (DB)<br>Cyril Cornu (All4tec) |
| 0.6.1 | 29.01.2013 | Scrum | Contribution | Bernd Hekele (DB) |
| 0.7.0 | 01.02.2013 | All | More Content | Rico Kaseroni (DB) |
| 0.8.0 | 02.02.2013 | All | Jungle Content -> Smooth | Rico Kaseroni (DB) |
| 0.9.0 | 06.02.2013 | All | Review on 0.8.0 Version | Dr. Hase (DB) |
| 0.9.1 | 07.02.2013 | Scrum | Optimization | Bernd Hekele (DB) |
| 0.9.2 | 07.02.2013 | All | Restructuring | Rico Kaseroni (DB) |
| 0.9.3 | 11.02.2013 | 1-, 2-, Last Chapter Annex A and C | Graphic Figure 1, Definition of openETCS Process IP clean Job | Rico Kaseroni (DB) |
| 0.9.4 | 12.02.2013 | All | Optimization | Rico Kaseroni (DB) |
| 0.9.4.5 | 15.02.2013 | Chapter2 | System Testing | Rico Kaseroni (DB) |
| 0.9.4.6 | 15.02.2013 | ALL | Optimization | Rico Kaseroni (DB) |
| 0.9.5 | 22.02.2013 | ALL | Restructuring & Optimization | Rico Kaseroni (DB) |
| 0.9.5.1 | 01.03.2013 | ALL | LaTeX conversion | Peter Mahlmann (DB) |
| 0.9.5.2 | 04.03.2013 | ALL | LaTeX Optimization | Rico Kaseroni (DB) |
| 0.9.5.3 | 10.04.2013 | ALL | New Structure | SQS (DB) |

# 1 Introduction

## 1.1 Purpose

*Proposed Content: This document contains the procedures and control methods to achieve the end products of OpenETCS project with the desired levels of safety and quality. It also describes the processes, methods and tools to develop such products in accordance to CENELEC Standards and following Open Source principles.*

## 1.2 Scope

The OpenETCS main objective is the development of an “open proofs” platform that integrates technologies from various stakeholders and enables the use of formal verification techniques in order to dramatically improve the software quality for embedded control systems in terms of reliability, maintainability, safety, and security.

The openETCS results will be:

1. Creating a formal specification of the ETCS OBU functionality according to UNISIG Subset 026
2. An executable software package generated from the formal specification and a non-vital implementation of that software for laboratory test, simulation and reference purposes
3. A tools chain supporting both previous bullet points including code, test case and document generation meeting CENELEC EN50128:2011 (T3) requirements and certifiable for SIL4 software applications for signalling equipment (Certification itself is not part of the project)

## 1.3 Intended Audience

*Proposed Content: This document applies to the whole development life-cycle of the project and it addresses all the stakeholders involved in the project. This document should be available to all of them in read access mode and it's provides operational guidance and access to QA procedures*

## 1.4 Evolution

*Proposed content: Frequency, method, responsibilities,...*

## 1.5 References, Guidelines and Standards

*Proposed content:*

| ID | Document |
|---|---|
| Text1 | Text2 |
| Text1 | Text2 |

## 1.6 Definitions and acronyms

| Abbreviation | Meaning |
|---|---|
| ASR | Assessor |
| CCS | control-command and signalling subsystems |
| DES | Designer |
| ERTMS | European Rail Traffic Management System<br>Train signaling system equipment based on a single Europe-wide standard for train control and command systems. |
| ERA | European Railway Agency |
| ETCS | European Train Control System<br>It is a signalling, control and train protection system designed to replace the many incompatible safety systems currently used by European railways |
| EUPL | European Union Public Licence |
| EVC | European Vital Control |
| GSM-R (train radio) | Global System for Mobile Communications - Rail(way)<br>It is an international wireless communications standard for railway communication and applications. |
| HR | Highly Recommended |
| HW | Hardware |
| IMP | Implementer |
| INT | Integrator |
| MVB | Multifunction Vehicle Bus<br>It is a part of the Train Communication Network (TCN), and it takes part in digital operation in the train. MVB is the bus part in each coach, and the Wire Train Bus (WTB) allows connecting the MVB parts with the train control system. |
| NA | Not Applicable |
| OBU | On-Board Unit |
| PMP | Project Management Plan |
| REQ | Requirements Manager |
| R&D | Research and Development |
| SCMP | System Configuration Management Plan |
| SIL | Safety Integrity Level |
| SME | |
| SRS | Software Requirements Specification |
| SW | Software |
| SW-SIL | Software-Safety Integrity Level (EN 50128:2011) |
| TSI | Technical Specification for Interoperability |
| TST | Tester |

| | |
|---|---|
| VAL | Validator |
| VER | Verifier |
| V&V | Verification and Validation |
| WP | Work Package |
| FM | Formal Methods |
| IP | Intellectual Property |
| IP Clean | No IP without permission in writing |

# 2 Project Organization

## 2.1 Project structure diagram

*Proposed Content: Refer to the PMP(Project Management Plan) and/or to the Full Project Proposal where the Project Organisation is described in detail. In this chapter include only the way compliance to CENELEC and SCRUM high level requirements at organisational level is achieved. i. all organisations are ISO 9001, how independency between roles is achieved within the structure,...*

## 2.2 Committers assignment and responsibilities

*Proposed Content: Introduce the concept of Committers as the way to guarantee the required competences are available within the context of the large project, with many organisations involved in the context of a EU project and with an open source environment. Introduce the concept of Contributors also and the difference between them. Refer to the document where the process to become a Committer and/or contributor is detailed.*

## 2.3 Project QA Management

*Proposed Content: Provide a description of the tasks to be developed by the project QA organisational structure jointly with the QA tasks to be performed by the team to guarantee project procedures/... are met. This means to detail the overall QA strategy.*

# 3 Life Cycle

## 3.1 Project Life Cycle

*Proposed Content: Refer to a separate document (PMP and Full Project Proposal) that describes the WP structure, refer to the Iterative process; relation between WPs and Results; WP/Project Backlog creation and maintenance and Scrum implementation.*

## 3.2 Product Life Cycle

*Proposed Content: Refer to a separate document that describes the life cycle. Consider EN50126 and EN50129 Requirements, include Deployment and Maintenance, include activities to "adapt" the generic/abstract software to a concrete implementation. In this chapter, if applicable, include justification to "potential deviations" to CENELEC standards.*

### 3.2.1 Life Cycle of the OpenETCS Software

*Proposed Content: Prepare a separate document with a complete description of phases of the the SW development life-cycle, including V&V, QA and Safety processes. This description*

*shall contain the activities to be performed by each role. In the preparation of this document, contribution of the different WPs is necessary (i.e. WP2 for the Design and development phase and WP4 for the V&V activities). In this chapter, if applicable, include justification to "potential deviations" to standard (EN50128) standards.*

### 3.2.2 Life Cycle of the OpenETCS Tools chain

*Proposed Content: See 3.2.1*

### 3.3 QA Management

*Proposed Content: Refer to the procedures to implement the QA activities identified within the above mentioned development life-cycle.*

## 4 Roles

### 4.1 OpenETCS Roles

*Proposed Content: Refer to Annex with the Role/Competence Matrix at project level. Besides, in this chapter, outline or refer to the procedure that will be used to maintain this matrix up to date; identify (refer and/or outline) the measures and/or mechanisms in place to record the competencies of the personnel assigned to the different roles (i.e. each company has to maintain training records) and measures and/or mechanisms to identify and fill gaps (i.e.maintain a project specific incorporation programme; maintain a training programme)*

### 4.2 Roles within the Development process of the openETCS Software

*Proposed Content: Refer to Annex with the Role/Competence Matrix of the OpenETCS software. Besides in this chapter, outline key specific competences demanded by the ETCS software development to the different roles.*

### 4.3 Roles within the Development process of the openETCS Tools Chain

*Proposed Content: See Chapter 4.2*

### 4.4 QA Activities

*Proposed Content: Describe the measures applied to monitor/verify people assigned to the different roles meet the requirements imposed by the role and have an active/qualified participation to the project (i.e. committers: assess effective contribution activities; gap analysis;. . . ).*

## 5 Methods, measures and tools for quality assurance (product + open ETCS software + Tools chain) + Justification of chosen Tools and Methods

*Proposed Content: Refer to Annex where for each phase in the development life-cycle identify methods and tools as well as justification for selection*

### 5.1 QA Activities

*Proposed Content: Describe the measures to monitor the appropriate implementation of the selected methods and tools.*

# 6 Documentation

## 6.1 Documentation Structure within the development process of the openETCS Software

*Proposed Content: Prepare a separate document with a complete description of labelling; definitions and acronyms; control information to include in each document; documents QA criteria; documentation matrix*

## 6.2 Documentation Structure within the development process of the openETCS Tools chain

*Proposed Content: See Chapter 6.1*

## 6.3 QA Activities

*Proposed Content: Describe the methods to review the documentation structure*

# 7 Documentation Control

*Proposed Content: Refer to Review Process Document where the function develop by authors, reviewers is provider*

## 7.1 Documentation Control within the Development process of the openETCS Sotware

*Proposed Content: Refer to the list of active documents of the openETCS software*

## 7.2 Documentation Control within the Development process of the openETCS Tools chain

*Proposed Content: Refer to the list of active documents of the openETCS tools chain*

## 7.3 QA Activities

*Proposed Content: Describe the methods to monitor both the control and process*

# 8 Tracking and tracing of deviation

## 8.1 Traceability (openETCS software + Tools chain)

*Proposed Content: Provide a description of traceability requirements, as well as how the traceability will be achieved, implement, maintained and verified. At this stage, exceptions if they exist should be justified.*

## 8.2 Configuration Management

*Proposed Content: Refer to SCMP (System Configuration Management Plan). Overview table with the summary of main features of SCMP.*

*Describe the QA activities*

## 8.3 Fault Management

*Proposed Content: Refer to Incident Management Process. Overview table with the summary of main features of the procedure*

*Describe the QA activities*

### 8.4 Grievance Handling

*Proposed Content: Refer to the specific procedure.*

*Describe the QA activities*

### 8.5 Modification and change control

*Proposed Content: Refer to external procedure; Overview table with the summary of main features of the procedure.*

*describe the QA activities to be developed.*

## 9 Supplier Control

*Proposed Content: Requirements to external suppliers and how they will be verified*

*describe the QA activities to be developed.*

## 10 ANNEXES

### 10.1 ANNEX A -Role Matrix at project level-

**Role** Project role

**SCRUM** if applicable scrum role

**Functions** Responsibilities of the role

**Competences Profiles Required** identifier of the competence profile described in the competence matrix

| Role | SCRUM | Functions | Competence Profiles Required |
|---|---|---|---|
| Users | - | • create a viable ecosystem around an openETCS project,<br>• encourage additional open source and commercial organizations to participate<br>• ... | CPR01, CPR03 |

| | | | |
|---|---|---|---|
| Adopters | - | • Reuse of the frameworks (within the companies that are contributing to the project and outside of the project),<br>• Reuse of the tools (within the companies that are contributing to the project and outside of the project,<br>• ... | CPR03 and CPR04 |
| Project Leader | Product owner | Text3 | CPRXX |
| Project Assistant | OpenETCS Scrum master | Text3 | CPRXX |
| Project Contributor | OpenETCS Scrum team | Text3 | CPRXX |
| Project Committer | - | Text3 | CPRXX |
| WP1 Leader | WP1 product owner | Text3 | CPRXX |
| WP1 Assistant | WP1 Scrum master | Text3 | CPRXX |
| WP1 Contributor | WP1 Scrum team | Text3 | CPRXX |
| WP1 Committer | - | Text3 | CPRXX |
| WP2 Leader | WP2 product owner | • ultimately decides what is on the product backlog,<br>• sets the priority of all items on that list,<br>• responsible for making sure that all the items on the product backlog can be understood by the team and all the stakeholders<br>• ... | CPR05 and CPR02 |

| | | | |
|---|---|---|---|
| WP2 Assistant | WP2 Scrum master | Text3 | CPRXX |
| WP2 Contributor | WP2 Scrum team | Text3 | CPRXX |
| WP2 Committer | - | Text3 | CPRXX |
| WP3 Leader | WP3 product owner | Text3 | CPRXX |
| WP3 Assistant | WP3 Scrum master | Text3 | CPRXX |
| WP3 Contributor | WP3 Scrum team | Text3 | CPRXX |
| WP3 Committer | - | Text3 | CPRXX |
| WP4 Leader | WP4 product owner | Text3 | CPRXX |
| WP4 Assistant | WP4 Scrum master | Text3 | CPRXX |
| WP4 Contributor | WP4 Scrum team | Text3 | CPRXX |
| WP4 Committer | - | Text3 | CPRXX |
| WP5 Leader | WP5 product owner | Text3 | CPRXX |
| WP5 Assistant | WP5 Scrum master | Text3 | CPRXX |
| WP5 Contributor | WP5 Scrum team | Text3 | CPRXX |
| WP5 Committer | - | Text3 | CPRXX |
| WP6 Leader | WP6 product owner | Text3 | CPRXX |
| WP6 Assistant | WP6 Scrum master | Text3 | CPRXX |
| WP6 Contributor | WP6 Scrum team | Text3 | CPRXX |
| WP6 Committer | - | Text3 | CPRXX |
| WP7 Leader | WP7 product owner | Text3 | CPRXX |

| | | | |
|---|---|---|---|
| WP7 Assistant | WP7 Scrum master | Text3 | CPRXX |
| WP7 Contributor | WP7 Scrum team | Text3 | CPRXX |
| WP7 Committer | - | Text3 | CPRXX |
| Configuration manager | - | Text3 | CPRXX |

### 10.2 ANNEX B -Competence Matrix at project level-

**Profile Identifier** unique identifier

**Competence Description** description of the necessary competences for each profile

| Profile identifier | Competences |
|---|---|
| CPR01 | Infrastructure (track and signalling) management companies/organisations |
| CPR02 | • experience with requirements management process<br>• experience with requirements management tools<br>• knowledges, experience and deep understanding with subset 026<br>• experience in railways sector<br>• ... |
| CPR03 | Systems/Subsystems designers and manufacturers |
| CPR04 | Companies/Organisations that provide solutions/services to rail industry |
| CPR05 | • needs to be able to explain the needs and requirements to the developer and must be able to give answers to their questions about details. This does not mean that they need to know everything but a good WP leader knows who knows<br>• needs to be able to make decisions on the spot if this is necessary. And a WP leader needs to take responsibility for these decisions,<br>• must look at the whole picture and all stakeholders and be able to know which brings the most business value to the product<br>• prepared to be involved in conflicts. The biggest challenges in this role just come from the fact that the many different interest and stakeholders are concentrated into a single role<br>• ... |

| | |
|---|---|
| CPR06 | Text6 |
| CPR07 | Text6 |
| CPR08 | Text6 |

### 10.3 ANNEX C -Role Matrix of the OpenETCS software-

| CENELEC Roles | SCRUM | Functions | Competence Profiles Required |
|---|---|---|---|
| Project Leader | Product owner | Text3 | CPRXX |
| Project Assistant | Scrum master | Text3 | CPRXX |
| Requirement manager | Scrum team | • see cenelec annex<br>• ... | CPRXX |
| Designer | Scrum team | Text3 | CPRXX |
| Implementer | Scrum team | Text3 | CPRXX |
| Tester | Scrum team | Text3 | CPRXX |
| Integrator | Scrum team | Text3 | CPRXX |
| Verifier | Scrum team | • see cenelec annex<br>• ... | CPR09 |
| Validator | Scrum team | Text3 | CPRXX |
| Assesor | Scrum team | Text3 | CPRXX |

### 10.4 ANNEX D -Competence Matrix of the OpenETCS software-

| Profile identifier | Competences |
|---|---|
| CPR09 | • must be able to deduce the verification types from the specifications<br>• must be competent in various verification methodologies and able to identify the most appropriate method or combination of methods to the context<br>• see cenelec annex<br>• ... |

| | |
|---|---|
| CPRXX | Text6 |
| CPRXX | • see cenelec annex<br>• ... |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |

### 10.5 ANNEX E -Role Matrix of the OpenETCS Tools chain-

| CENELEC Roles | SCRUM | Functions | Competence Profiles Required |
|---|---|---|---|
| Project Leader | Product owner | Text3 | CPRXX |
| Project Assistant | Scrum master | Text3 | CPRXX |
| Requirement manager | Scrum team | • see cenelec annex<br>• ... | CPRXX |
| Designer | Scrum team | Text3 | CPRXX |
| Implementer | Scrum team | Text3 | CPRXX |
| Tester | Scrum team | Text3 | CPRXX |
| Integrator | Scrum team | Text3 | CPRXX |
| Verifier | Scrum team | Text3 | CPRXX |
| Validator | Scrum team | • see cenelec annex<br>• ... | CPR09 and CPR12 |
| Assesor | Scrum team | Text3 | CPRXX |

### 10.6 ANNEX F -Competence Matrix of the OpenETCS Tools chain-

| Profile identifier | Competences |
|---|---|
| CPRXX | Text6 |
| CPRXX | Text6 |

| | |
|---|---|
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPRXX | Text6 |
| CPR12 | • model knowledges<br>• ... |
| CPRXX | Text6 |

### 10.7 ANNEX G -Methods and tools/Justification for selection-

| Software Design and Implementation | | |
|---|---|---|
| Method/Technique | SIL 4 | Justification |
| Modular Approach | M | Text6 |
| Components | HR | Text6 |
| Design and Coding Standards | M | Text6 |
| Strongly Typed Programming Language | HR | Text6 |
| Formal Methods | HR | Text6 |
| Modeling | HR | Text6 |

| Quality mechanisms for Safe deployment | Technique & Approach |
|---|---|
| Software Self-identification Mechanisms (9.1.4.11) | |
| Error detection and/or avoidance mechanisms during deployment process (store, transfer, transmission and/or duplication of code operations) (9.1.4.20) | |
| Automatic detection and safe management of incompatible components/versions (9.1.4.8, 9.1.4.9) | |
| Provision of appropriate and accurate diagnostic information | |
| Safe Roll back capabilities | |

| Quality mechanisms for Maintainability | Technique & Approach |
|---|---|
| Coding Standards | |
| Impact Assessment | Before each implementation |

| | |
|---|---|
| Data register and analysis | Creation and maintenance of a project history register |
| Design method selection mechanisms to facility the maintainability (7.3.4.28) | |
| Attenuation actions mechanisms (9.2.4.20) | |
| Mechanisms for evaluating the appropriateness of the methods, tools and techniques used in the modification/maintainability (part of 9.2.4.2 and CENELEC 126 phase 13) | |
| SW description mechanisms (7.1.1.1) | |
| Control mechanisms to guarantee the corrective actions adoption (6.6.4.1) | |
| Provision of appropriate and accurate modification management system (6.6.4.1) and configuration management system (6.5.4.12) | |