OETCS/WP4/D4.2.2

openETCS

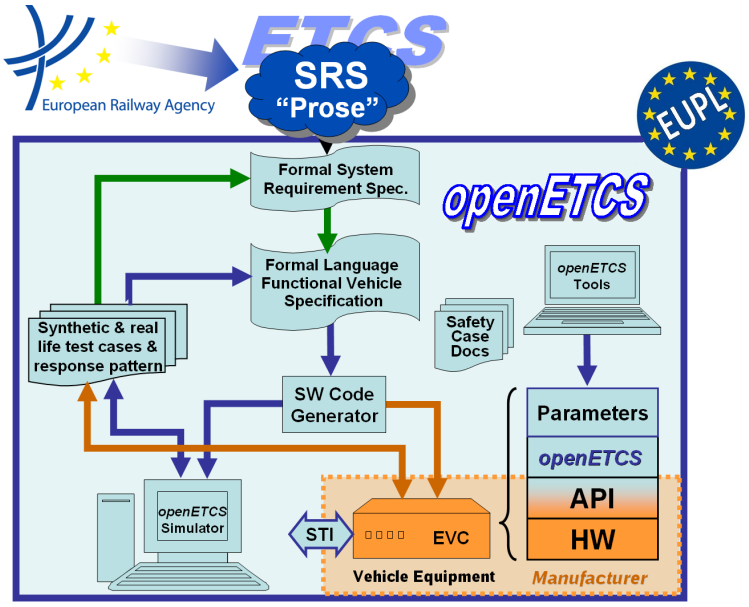
ITEA2 Project
Call 6 11025
2012 – 2015

openETCS@ITEA Work Package 4.2: “Verification & Validation of the Formal Model”

# D.4.2.2 1st interim V&V report on the applicability of the V&V approach to the formal abstract model

Ana Cavalli and João Santos

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

**openETCS@ITEA Work Package 4.2: “Verification & Validation of the Formal Model”**

**OETCS/WP4/D4.2.2**
**October 2013**

# D.4.2.2 1st interim V&V report on the applicability of the V&V approach to the formal abstract model

Ana Cavalli and João Santos

Télécom SudParis
9 rue Charles Fourier
91011 Evry Cedex, France

Prepared for openETCS@ITEA2 Project

**Abstract:** Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

# Table of Contents

# Figures and Tables

## Figures

## Tables

## Introduction

To ensure the correctness and consistency of the model and its implementation, the validation and verification has to be performed alongside with the modelling process. Thus these tasks will be performed repeatedly during WP3 and will provide feedback to it.

This document presents the results of the first iteration of verification and validation of the formal model. This was be accomplished by applying the methods chosen in WP4 Task 1 onto the formal model using the tool chain developed in WP7.

# 1 Model Verification Techniques

## 1.1 Proof Technique

A proof is a demonstration that if some fundamental statements (axioms) are assumed to be true, then some mathematical statement is necessarily true. As mentioned in the requirements document produced by WP2, as much as possible, formal proof would then be used to prove that the OpenETCS model never enter a Feared State, as long as the other subsystem (RBC, communication layer. . . ) fulfill their own safety properties (axiom describing the environment). Such theorem proving helps to increase our confidence on the specified model. The proof techniques should be integrated in the selected tool chain. In order to use formal proof to verify if the SFM (Semi-formal model) and FFM (fully formal model) comply with the safety and function requirements (cf. R-WP2/D2.6-02-058), the properties to be proven have to be identified and described. There will be a set of axioms that will describe both functional and/or safety properties of the system. The choice of axioms describing functional and/or safety properties will be provided by safety analysis in an independent way from approaches used to specify, design, validate or verify. It must be noted that the model obtained from the Subsystem Requirements Specification should be verified in this manner at a first stage.

## 1.2 Model Checking

Model checking is an automatic technique for verifying finite-state reactive systems. As such, one could automatically check if the model specifies most of the requirements of the system, such as the important safety properties described in Task 4.4. Similar to proof techniques, in order to use model checking to verify if the SFM (Semi-formal model) and FFM (fully formal model) comply with the safety and function requirements (cf. RWP2 /D2.6-02-058), the properties to be proven have to be identified and described. To implement the use model checking, it is mandatory to specify the model using finite-state reactive systems, and they should also provide an intuitive way to express the properties to be model checked. The set of critical requirements to be verified need to be clearly identified. The criteria for the model to be considered a representation of the standard is that all properties are checked. The proposed model checking techniques should be supported in the selected tool chain.

**Should include the list of properties to be evaluated by model checking

## 1.3 Simulation

As for simulation, the artifacts should provide means to execute the model. The simulator must be automatically generated, so that, when run against test scenarios (inputs/outputs for the model), we may conclude whether the model follows the specification or not. In particular, it is important to define test scenarios for the safety critical properties. Since, the development

within openETCS has to the goal to reach the CENELEC EN 50128 SIL 4 standard, it is highly recommended (cf. SIL 4) that the simulation needs to cover all states, transitions, data-flow, and paths in the model. It would also be desirable to include graphical representation of the simulation/model and also provide a report of the visited components as specified by CENELEC EN 50128 SIL 4. CENELEC EN 50128 SIL4 also advocates to perform tracing. Being able to trace the requirements that are met during a simulation is also advisable to allow simple requirement coverage.

**Should include the list of properties to be evaluated by simulation

### 1.4 Other Techniques

Reviews, Inspections, static analysis and walkthroughs, mostly manual techniques, are also to be considered for the verification of models.

**To be completed with the techniques proposed by the partners.

## 2 Tools used for the Verification of the model

The tools used with these techniques are described in WP7.

## 3 Applied Techniques

This section will describe results from V&V on each of the categories. Categories for other techniques proposed by partners should be added.

Each used technique should presented as follows

- Description of the applied technique
- Description of the model
- Description of the results

### 3.1 Proof Technique

Results obtained by applying proof techniques

### 3.2 Model Checking

Results obtained by applying Model Checking

### 3.3 Simulation

Results obtained by applying simulation

### 3.4 Other Techniques

## Conclusions

Final deliberation on the results presented on the previous chapters