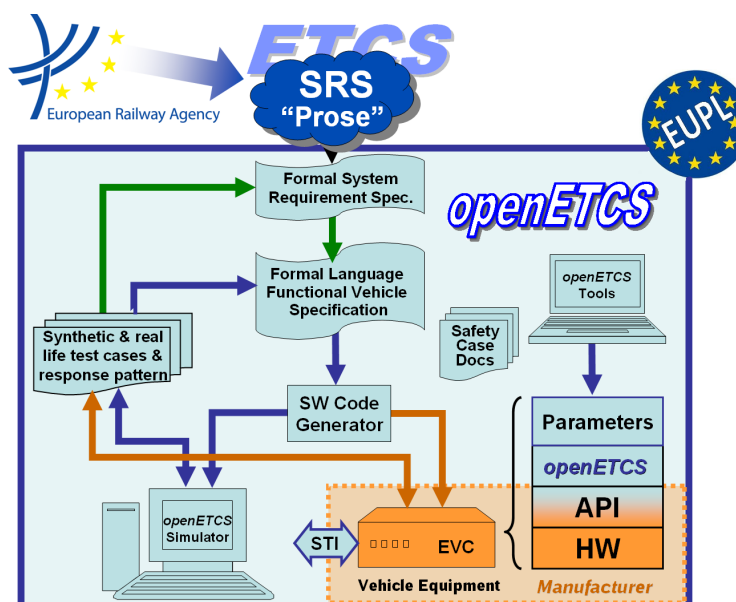


Work Package 4: "Validation &amp; Verification Strategy"

# First Validation and Verification Report on Implementation/Code

Marc Behrens and Jens Gerlach

November 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 4: “Validation & Verification Strategy”**

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

# First Validation and Verification Report on Implementation/Code

Marc Behrens

WP4 Leader

Jens Gerlach

WP4.3 Task Leader (Validation and Verification of Implementation/Code)

Description of work

Prepared for openETCS@ITEA2 Project

**Abstract:** This work package will comprise the activities concerned with verification and validation within openETCS. This includes verification & validation of development artifacts, that is, showing that models and code produced correctly express or implement what they are supposed to. And also, methods and tools to perform such tasks will be evaluated with the goal of assembling a suitable method and tool chain to support a full development.

**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

1	Introduction.....	5
2	Formal Verification of Bitwalker .....	5
2.1	Verification Objectives .....	5
2.2	Informal Specification .....	5
2.3	Formal Specification with ACSL .....	5
2.4	Formal Verification with Frama-C/WP .....	5
2.5	Open Issues .....	5
3	SQS.....	5
4	CEA LIST .....	5
5	Systerel .....	5
6	Conclusions .....	5

# Figures and Tables

**Figures**

**Tables**

- 1 Introduction**
- 2 Formal Verification of Bitwalker**
  - 2.1 Verification Objectives**
    - 2.1.1 Functionality**
    - 2.1.2 Robustness**
  - 2.2 Informal Specification**
  - 2.3 Formal Specification with ACSL**
  - 2.4 Formal Verification with Frama-C/WP**
  - 2.5 Open Issues**
- 3 SQS**
- 4 CEA LIST**
- 5 Systerel**
- 6 Conclusions**