openETCS/WP4/D4.5.1

openETCS

ITEA2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

ITEA2 Project
Call 6 11025
2012 – 2015

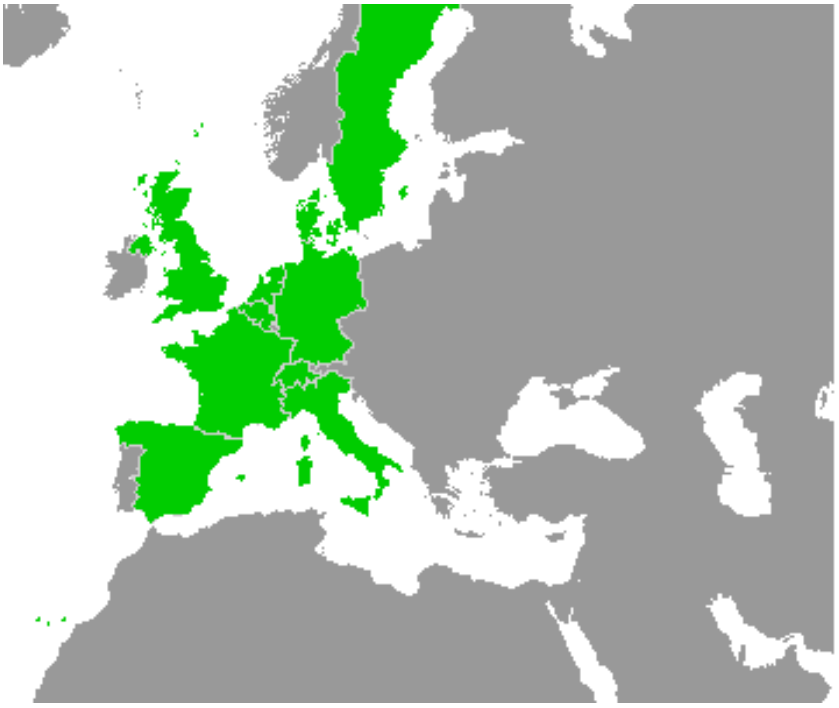
Work-Package 4: "V&V Strategy"

openETCS D4.5.1: OpenETCS Internal Assessment Plan

Planning and Description of tasks that are performed within Internal Assessment Activities in the Open ETCS project

Cyril Cornu (All4tec)

February 2013



This work is licensed under the "openETCS Open License Terms" (oOLT) dual Licensing:

This page is intentionally left blank

Work-Package 4: "V&V Strategy" **openETCS/WP4/D4.5.1**
February 2013

openETCS D4.5.1: OpenETCS Internal Assessment Plan

Planning and Description of tasks that are performed within Internal Assessment Activities in the Open ETCS project

Cyril Cornu (All4tec)

All4tec
2-12, Rue du Chemin des femmes
91 300 MASSY
France

Preliminary Report draft version

Prepared for openETCS@ITEA2 Project

This work is licensed under the "openETCS Open License Terms" (oOLT).

Abstract: The Internal Assessment Plan describes the Internal Assessment strategy and plan in the frame &V activities in the Open ETCS project. The assessment is a ¨ Process of analysis to determine whether software, which may include process, documentation, system, subsystem hardware and/or software components, meets the specified requirements, and to form a judgment whether the software is fit for its intended purpose.¨
The dates, highlights, deliverables and activities split presented in this plan are willing to be adapted in accordance with the FPP final version.

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

This work is licensed under the "openETCS Open License Terms" (oOLT).

1 Introduction

The role of the Assessor is to perform an assessment of the software developed during the project OpenETCS. According to the standard EN 50128 and the software safety integrity level (SIL4) of the project, it is very important to remind that the Assessor shall be independent from the project and shall be given authority to perform the software assessment. Then, the Assessor shall not be part of project stakeholders, and is totally independent from the project teams. Furthermore, the Assessor shall have the knowledge of the both ERTMS and ETCS, of the dependability and of the standard EN 50128, even if only the On Board Unit EVC Software part in the project scope. For these reasons, the need of an internal assessment has been identified at the beginning of the project. This activity would simulate a real external assessment process, that would be enhanced by people part of the Open ETCS project, and responding to the 2 main skills conditions to perform such a task: the technical knowledge on the ETCS OBU and the technical independency regarding the whole Software development and project activities.

1.1 project context

The aim of the internal assessment is to simulate a real assessor activity regarding a standard Railway signaling system design and production by a railway company. The Open ETCS project main objectives are:

- Transformation of higher-level, informal (i.e. expressed in natural language) ETCS requirements in formal and semi-formal requirements that will be used for validation and verification activities of embedded control systems.
- Adaptation of modelling languages such that train control systems can be designed in suitable formalisms and verified against ETCS requirements in early design phases.
- Integrating and developing formal and semi-formal validation and verification techniques in order to prove the correctness of train control systems against formalized ETCS requirements.
- Generating symbiotic effects of large companies, R&D institutes, and SMEs in order to bring together all relevant experts in the field taking advantage from their diverse knowledge within a value adding chain (so called “eco-system” or “Co-Competition”).

These four objectives are all related to specific steps of an On Board Unit Software design and development (European Vital Computer). Moreover, they all encompass underneath performance, reliability, availability, maintainability and safety objectives, that are usually translated into a Safety Integrity Level (SIL), and the conditions regarding quality, process and overall development activities are gathered in the CENELEC standards EN50128, EN20126 and EN50129. Therefore, apply the common development strategy for such a railway system makes sense, and allows the project to base the whole OBU EVC Software development on existing CENELEC standards for such Railway signaling systems allows us to meet these both conditions on design process and Safety Level.

1.2 Internal Assessment Plan objectives

This document provides the overall assessment plan and objectives that will be followed in the frame of internal assessment activities. The activities are shared according to the main software development categories they deal with:

- Quality insurance

This work is licensed under the "openETCS Open License Terms" (oOLT).

- Verification & Validation
- Safety

For each assessment activities, this assessment plan will identify the relevant deliverables, and the criteria that will be considered for the assessment. The Internal Assessment Plan shall provide and detail the following aspects:

- All versions of the present Assessment Plan and modification tracking are provided in the part 1.3 of this document.
- Authors of this document are:
  - Cyril Cornu (All4tec) is the Internal Assessment Activity Organizer.
  - Frederique Vallee (All4tec) is an Internal Assessor for Open ETCS project
  - Merlin Pokam (AEbT) is an Internal Assessor for Open ETCS project (to be confirmed)
  - Jean-louis Boulanger (Certifer) is an Internal Assessor for Open ETCS project (to be confirmed)
- Customer identification (to be defined for our specific case, the Open ETCS)
- Mission context (product description, context regarding the existing assessment of tools or artifacts in the project)
- The Product and Process assessment scope
- The standards to be applied for Assessment are the CENELEC EN50126, EN50128 and EN50129 Standards.

According to the CENELEC standards, the Independant External Assessor has to get the agreement signature for submission of the customer (here open ETCS project) to the assessor expectations according to the EN45001 standard, defining the juridical and technical standard for an independent evaluating structure. This point is major because it defines precisely the difference between the Internal Assessment Task

Date of modification	**Paragraph/ Page**	**Modification object**	**Author**
28/06/2013	all	1st document draft issue	Cyril Cornu (All4tec)

2 Project Quality Assessment

This chapter details what are the main features to be checked regarding the quality insurance regarding the whole Open ETCS activities, from the very beginning of the project to the end of it. The Safety Criteria are defined in the document D2.2 appendix B3, and these criteria will be checked during the Internal Assessment review. The main points to be assessed are:

- The Quality Assurance Plan completeness
- The Project Deliverables compliance with QAP
- The Management and Responsibilities management

This work is licensed under the "openETCS Open License Terms" (oOLT).

2.1 Applicable Standards

The compliance to the applicable standards is a major point for the quality management system assessment. The major standards to considered within Open ETCS are:

- CENELEC EN 50126
- CENELEC EN 50128
- CENELEC EN 50129

2.2 Quality Assurance Plan - QAP

The purpose of the QA Plan is to define the processes, methods and tools that will be used to develop the OpenETCS project meeting ITEA requirements, following Open Source principles and practices and applying the SCRUM Methodology. Besides, two of the project outcomes, the OpenETCS software, the OpenETCS Tool Chain, will have to comply with CENELEC requirements.

The following parts of the QAP will be precisely checked by the assessor, whether they belong to the QAP document or to another document.

- Open ETCS development process. This process describes the whole documentation to be issued in the framework of Open ETCS project, and the connexions between the project inputs, the project outcomes, and the work packages and tasks identified in the project. The coherency between the IO documents and informations identified in the development process and the related document content will be checked.
- Open ETCS tool development process. This process has to be described as precisely as the Quality Assurance related to the OBU EVC Software development activity. The same verifications and assessments activities will be performed on this process than on the software development process.
- Configuration Management Plan. This Configuration Management Plan has to consider each outcomes of the project from its very first release version to end of the document whole life-cycle. The documentation change management related to the toolchains definitions or related to the OBU EVC software development have to be considered for both aspects of Open ETCS project development. This configuration management plan shall consider documentation change but also toolchain, model (formal and semi-formal) and code issued in the frame of Open ETCS project.
- Review Process. The review process has to be applied from the very beginning of the project to its end.
- Project Development Process. All the development phases have to be described and specified for the whole software development process and cycle.

2.3 Project Deliverables compliance with QAP

The Safety Criteria are defined in the document D2.2, and these criteria will be checked during the Internal Assessment review. The main points to be assessed for the project deliverables are:

This work is licensed under the "openETCS Open License Terms" (oOLT).

- the documentation compliance for Software Safety Integrity Level 4. This includes a functional and interface description of the system, the application conditions, the configuration or architecture of the system, the hazards to be controlled, the safety integrity requirements, the SIL allocation to Software and Hardware, and the timing constraints.
- the Requirements for tools class T1, T2 and T3. Tools have been identified so far for each category (text editor, requirements support, configuration support tool for T1, static code analyzers, model checkers, model based testing tools, simulators for T2, and compilers or code generation tools for T3), and all proof of compliance with the CENELEC standard and justification for use will be check within internal assessment activities.

2.4 Project Development Process

The Project Development Process is a major point of the Quality Management System. It describes the overall project process, from the very first inputs used in the project, the all activities that going to be performed and the corresponding outcomes to be issued, to the final deliverables of the project. The Inputs/outputs of each task and documents, within a work package or a specific task, as well as the interfaces between all these tasks and activities, have to be described in this process description. The documents have to be identified in this process, and the connection between the activities to be performed and the related document shall be provided.

Documents or information related to some points of this process are more important for the assessor. Here is a list of technical items that should be closer observed by the assessor:

- The organic Architecture;
- The Software components, with their functional interfaces (internal and external);
- The functions and sub-functions of the software;
- The Safety Requirement traceability;
- The coherency of applied technics and methods to the Quality Assurance Plan;
- ...

2.5 The Role and Responsibilities management

The Quality Assurance in Open ETCS has to claim the proof that all people involved in project has the sufficient skills and competencies to fulfill their responsibilities. All these competencies have to be gathered and tracked whether in the QAP or in a separate quality related document that has to be identified in the QAP. According to the CENELEC EN50128, the 10 software development key roles to be identified are:

- the Requirements Manager,
- the Designer,
- the Implementer,
- the Tester,
- the Verifier,

This work is licensed under the "openETCS Open License Terms" (oOLT).

- the Integrator,
- the Validator,
- the Project Manager,
- the Configuration Manager.

The information needed in Quality Assurance documentation is:

- The Actual Competencies Matrix of each committer in the project, linked to the work packages and the tasks they are involved in.
- The Needed Competencies Matrix for each task, document and project outcomes. Each people contribution as to be as detailed as possible (at least the contribution to a precise task or outcome).
- From the gab identified between the both actual competencies matrix and required competencies matrix, a Training plan has to be set up for all the commiters of the Open ETCS project. This plan will have to track all the identified needs, and then the solutions chosen in order to harmonize the competencies needs and the committers skills (training session, re-organization,

2.6 Quality Log and Traceability

In the framework of Asessment activities, all discrepancies related to Quality Assurance whatever the level considered, will be gathered in a table called the Quality Log. This log will be used by the Assessor as a list of possible or required improvements, to be used as a road map in order to get rid of all quality assurance concerns or discrepancies identified during the whole project life cycle. The Quality Log table will encompass the following information:

- Number of the log row
- Document/ Outcome concerned and precise discrepancy localization
- Document/ Outcome version
- Date
- Discrepancy description by assessor, and comments (assessor, author or else)
- Action planned to fix (commonly defined by at least the document author and the assessor)
- Action Deadline
- Status of the log (fixed, under investigation...)

2.7 deliverable

One deliverable will be issued in the frame of this part of internal assessment activity: The Project Quality Assurance Assessment Report. This deliverable will present the results of the overall quality assessment for the project. This document will be used as a frame for quality assessment during the whole project, and the very first version will be issued one month after the first QA Plan release. (To be defined)

This work is licensed under the "openETCS Open License Terms" (oOLT).

3 V&V Assessment

This chapter details what are the main features to be checked regarding the V&V activities regarding the whole Open ETCS software development activities, from the very beginning of the project to the end of it. The Quality Criteria regarding V&V activities are defined in the document D2.2 appendix B4, and these criteria will be checked during the Internal Assessment review. The main points to be assessed are:

- V&V Plan
- Verification & Validation activities for Model
- Verification & Validation activities for Primary Toolchain
- Verification & Validation activities for Code
- Safety

These activities are recorded in the following outcomes so far:

-

3.1 V&V Plan

The purpose of the V&V Plan is to define, describe and plan the verification and validation activities in the project openETCS. As the goals of the project include the selection, adaption and construction of methods and tools for a FLOSS development in addition to performing actual development steps, the V&V plan will deal separately with these two aspects. The Verification Plan for the model should describe the selection of verification strategies and techniques to be applied to the Open ETCS for Testing the Open ETCS Semi-Formal Model and Formal Model. The set of techniques, the definition of the process for test creation, test coverage and completeness, and roles in the testing team will be assessed in the same way than for the Quality Assurance Aspects. The Verification Plan for the tool is based on the same principle than for the Model Assessment, but related to the tool or the whole toolchain. The Assessment will focus on quality assurance and traceability of the verification.

The Validation Plan aims to give a frame to Validation activities to be performed within OpenETCS project. It aims at determining whether the developed tool fits the user needs, in particular with respect to safety and quality relatively to the environment it will be run in. The Validation plan shall describe the validation strategy for both primary and secondary toolchains and for the OBU EVC Software to be developed as well. The documentation shall be provided on techniques and tools used and on environment description. The assessment will focus on the coverage of artifacts to be covered within the Open ETCS project validation plan, and the coherency between the Validation outcomes description in the plan and the effective Validation activities performed in the Frame of Open ETCS project.

3.2 Verification and Testing Activities

The First aspect is related to the Verification activities. The Assessment for Verification will mainly concern the following points:

This work is licensed under the "openETCS Open License Terms" (oOLT).

- Evidence
- Test Specifications. The Test Specifications will have to fulfill the CENELEC requirements regarding the tests objectives, the precise content of the test in terms of environment handling, data and expected results. Their coherency with the test policy will be checked and assessed.
- Test Reports. The test report will have to report as precisely as possible the information related to the test performance. The tests results are compared with the expected results defined during the test specification, failures have to be recorded, described and then investigated. The test environment such as Tester names and test conditions have to be clearly described as well.

The Final reports of the Verification and Testing activities have to be integrated in the Quality Assurance Verification report, in order to prove the consistency of the Verification activities with the CENELEC Standards.

3.3 Validation Activities

The second aspect is related to the Validation Activities. The Assessment for Validation will mainly concern the following points:

- The creation of a Validation Plan in order to define a frame for Validation activities (as described in previous paragraph);
- The creation of a Validation Report. This report should describe the toolchain, the model or the code tested by functional approach, provide the results of validation activities and provide the analysis and the identified discrepancies between expected and actual results. All discrepancies detected and/or treated shall be gathered in the Software Validation Report (V&V log).

3.4 V&V log and traceability for Model

The V&V activities can be split in testing activities and verification activities. The testing activities aim at verifying the Model behavior and performances against the corresponding system and software specification, in order to achieve the capability, maintainability, portability, functionality, reliability and usability objectives for the OBU EVC Kernel Software Model. For each test, a Test Specification has to be issued and will have to fulfill the CENELEC requirements regarding the tests objectives, the precise content of the test in terms of environment handling, data and expected results. Their coherency with the test policy will be checked and assessed. At the end of the test, a test report is then created. The coherency between the Test specification and the Test Results is then gathered and Analyzed in the V&V documents. The internal Assessment will not focus on the Verification activity itself (which is dealt with in the frame of Verification and Validation activities), but on the following assessment activities:

- The coherency between the tests to be performed, and the coverage of the functional requirements by these tests;
- The traceability between the tests and the requirements;
- The robustness of the methods employed and its compliance to the CENELEC Standards;
- The fulfillment of V&V results according to the expected results defined in the V&V;

This work is licensed under the "openETCS Open License Terms" (oOLT).

3.5 V&V log and traceability for Code

V&V activities on code will have to take place, mainly in order to complete the coverage of the Model Verification and Validation activities. Indeed, requirements that are not covered at the sub-system level will have to highlighted in the Code Verification activity, whatever its content. The internal assessment activity will focus on the coverage of

- The method and process used to fill this log, and the accordance to the CENELEC EN50128;
- The tools supporting the process for V&V at Code level;
- The fulfillment of the V&V log, regarding all the information needed in order to track the issues raised during the V&V activities;
- The traceability respect between the V&V documentation issued in the frame of V&V activities, and the V&V log;

3.6 deliverable

One deliverable will be issued in the frame of this part of internal assessment activity: The V&V Assessment Report. This deliverable will present the results of the overall Verification and Validation assessment for the project. This document will be used as a frame for V&V assessment during the whole project, and the very first version of this document will be issued one month after the first V&V Plan release. (To be defined)

4 Safety Activities Assessment

The Safety Activity is particularly relevant to be assessed, as a necessary condition to develop and supply a SIL4 OBU EVC Software. The Safety Strategy defined within the WP4 activities for Open ETCS project assume that the overall Safety activities in Open ETCS project will be performed on a part only of the EVC Software, but the full software development life-cycle will covered by these Safety activities. The overall Safety Activities are described in the Open ETCS Safety Plan.

4.1 Safety Evaluation Criteria

The Safety Evaluation Criteria that will be considered for the Internal Assessment are described in the Safety Criteria deliverable. These criteria will be checked during the V&V phases, but will also be reviewed in the Frame of Internal Assessment. The main criteria to be assessed are:

- The method and process for Safety Activities, from Safety Plan to the whole Safety Case, and their consistency with the CENELEC. For instance
- The tools supporting the process and the method;
- The traceability between the software development process and the Safety related documents;
- The coverage of Safety requirements by V&V activities at different levels (System, sub-System, model, code) on Safety functions and components;

This work is licensed under the "openETCS Open License Terms" (oOLT).

4.2 Safety Documentation Assessment

The main Safety related documents to be assessed are:

- The Preliminary Risk Assessment (this document initiates the Safety log or Hazard Log).
- The System and Sub-System Safety Study. These points have to be clearly defined and connected according to the software design steps defined in the Open ETCS process. The following points are especially relevant for the
  - The transformation method from the Sub-System model (meta-model in MDD) to the Software model (COTS, branching, refinement and code generation algorithms and options);
  - The Software components refined from the sub-system model (components description and version, components traceability, SIL level, traceability for safety requirements traceability);
  - The compiling toolchain analysis (COTS, branching of the soft, the compilation options and scripts for compile or integration);
  - The Safety Requirements;
  - The software configuration management (version, date, developers, etc...);
  - The critical parameters, with the following :
    - Common parameters for whatever the train or the trackside to be considered;
    - Interlocking parameters;
    - Fault data and fall-back positions;
- The Code Safety Analysis activities:
  - The code metrics analysis;
  - The Function call graph Analysis;
  - The Safety Requirements traceability;
  - The SEEA (Software Errors and their Effects Analysis) for the whole code generated;
  - The CCR (Critical Code Review) for the Safety related functions;
- The Safety V&V activities:
  - The Verification activities on the transformation method from the system model to the sub-system model (bugs on process, side files needed, terminology coherency, proof on formalized properties);
  - The verification activities on the compilation toolchain (compilation bugs, side files generated, memories mapping, comparison of compiling options);
  - Test plan, catalogs and reports on the software components;
  -
- The Safety log or Hazard log, filled during the whole project duration. The main informations to be assessed in are:
  - The coverage for all hazardous situation identified during the project;
  - The list of all Safety tickets or corrective actions performed in the frame of safety activities, and their status regarding the Safety property or issue related;

This work is licensed under the "openETCS Open License Terms" (oOLT).

- The Global Safety requirements coverage. This sheet should gather all the Safety requirements identified since the very beginning of the project. All the concerns encountered during the very beginning of the Safety activities should be gathered too, and then linked to the solutions identified and applied, in order to get rid of the concern. The Safety Backlog

All these documents constitute the Global Safety Case, and are a relevant set of documentation to be evaluated by the assessor. The Global Safety Case is analyzed, with the verification that all risks identified in the Hazard log have been covered, and that external constraints (exported constraints) are precisely defined.

4.3 deliverable

One deliverable will be issued in the frame of this part of internal assessment activity: The Safety Assessment Report. This deliverable will present the results of the overall Safety assessment for the project. This document will be used as a frame for V&V assessment during the whole project, and the very first version of this document will be issued one month after the first Safety Plan release. (To be defined)

5 Assessment Method and Processes

5.1 Detail level for documentation evaluation

This table gives an overview of the depth of assessment and control activity according to the CERTIFER standards (Fench Asessor)

Document to be evaluated	**Not examined**	**Quick Read**	**Read by Sampling**	**Attentive Read**
Quality Assurance Plan				X
Quality Procedures (e.g review process)			X	
Quality logs documentation		X		
Software Risk Analysis			X	
Functional specification				X
Software Architecture and Safety properties (SSRS with Safety Properties)				X
Software Formal Model (System and Sub-System level)			X	
Source code	X			
Software Tests specification (Integration, installation and validation)			X	
Overall tests results			X	
Parameters Validation report			X	
Safety Case				X

5.2 Intermediate Evaluation Assessment

This work is licensed under the "openETCS Open License Terms" (oOLT).

The Internal Assessment activities is supposed to improve the Open ETCS project compliance with a standard need of Assessment for such a SIL4 Software. Therefore, different activities related to the assessment have to be performed during the on-going process for the Software development.These actions can be performed in different ways:

- Audits;
- Main document issue;
- ...

These specific assessment activities minutes and conclusions are gathered in

5.3 Assessment Report Evaluation

The Assessment Report is the global document gathering all the evaluations or audits that have been performed during the Internal Assessment of the project. This report shall bring the proof that the software developed within Open ETCS project is compliant with the Safety objectives and the customer need. The results presented in this report are:

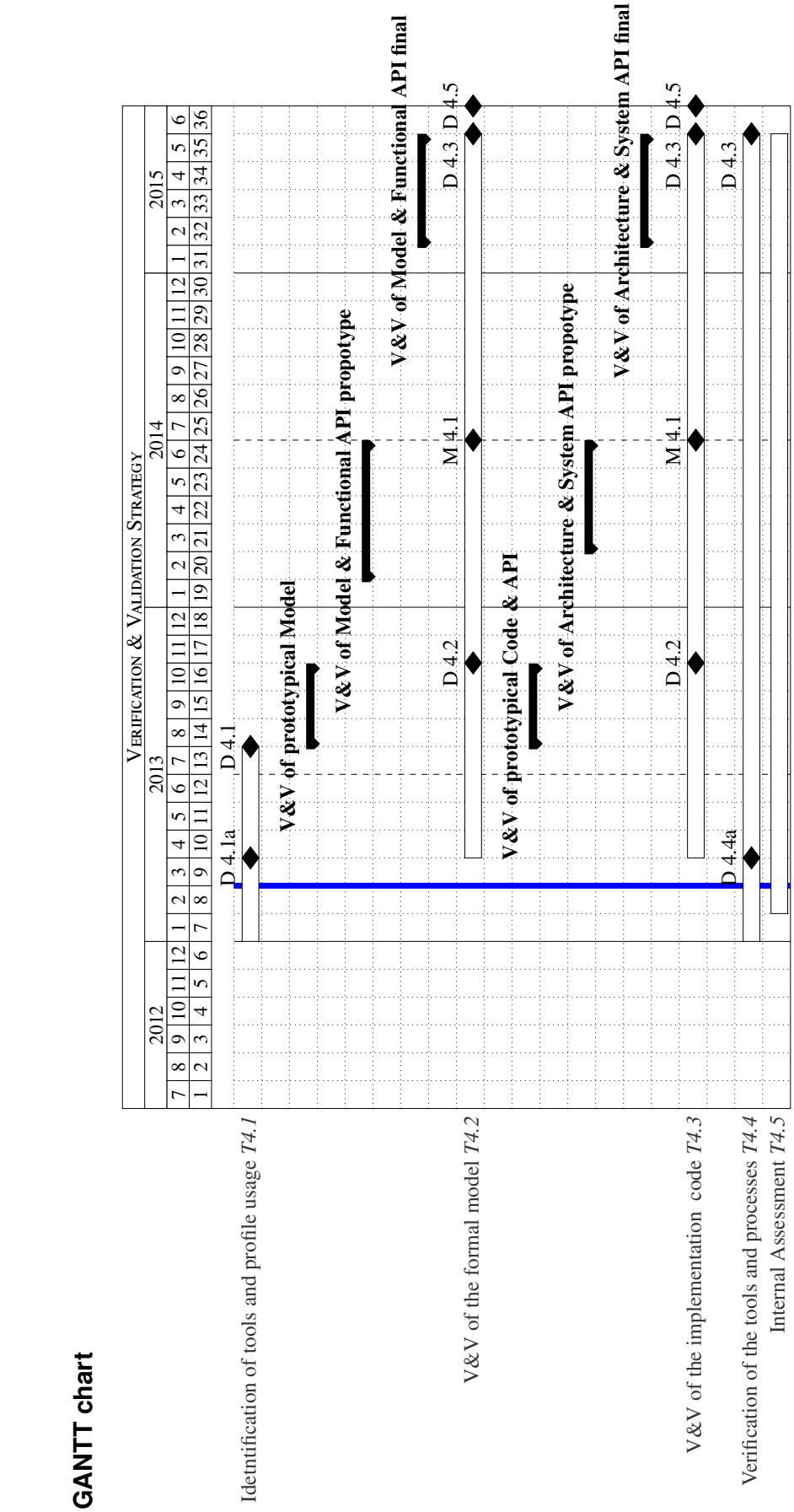
- justifications on cross-acceptance verification activities
- intermediate assessments synthesis;
- Quality and V&V audits conclusion (including the tracking of improvement axis and corrective actions);
- The list of software components evaluated (+configuration management results)
- Conslusions on Product Evaluation

6 Internal assessment activities planing

This part describes how will be performed the Internal Assessment along the Open ETCs project. It will identify the main project outcomes and deadlines that will trigger Internal Assessment activities. The current planning proposes

This work is licensed under the "openETCS Open License Terms" (oOLT).

7 GANTT chart



This work is licensed under the "openETCS Open License Terms" (oOLT).

So far, the deadlines that have been decided in the frame of Internal Assessment

8 Internal assessment formalism

9 Conclusion

This work is licensed under the "openETCS Open License Terms" (oOLT).