ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

Workpackage 4
Verification & Validation Strategy

supported by:

Federal Ministry of Education and Research

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

INVESTISSEMENTS D'AVENIR

Région de Bruxelles-Capitale

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

openETCS@ITEA2 Project

Marc Behrens, DLR

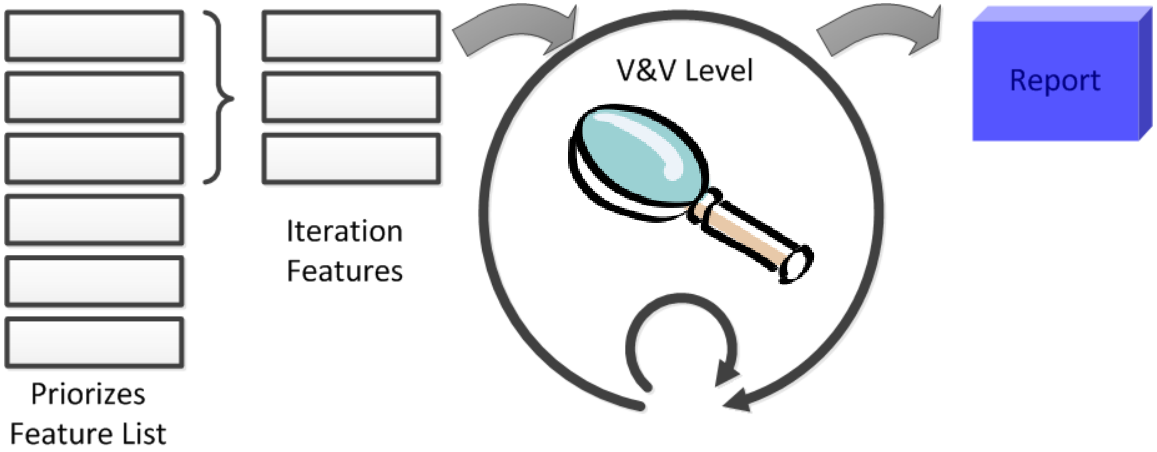
Paris, 03.07.2013

Verification and Validation

Challenge

Verification and Validation challenge is to merge

- Agile Methods
- Open Source Process
- Open Proofs Concept



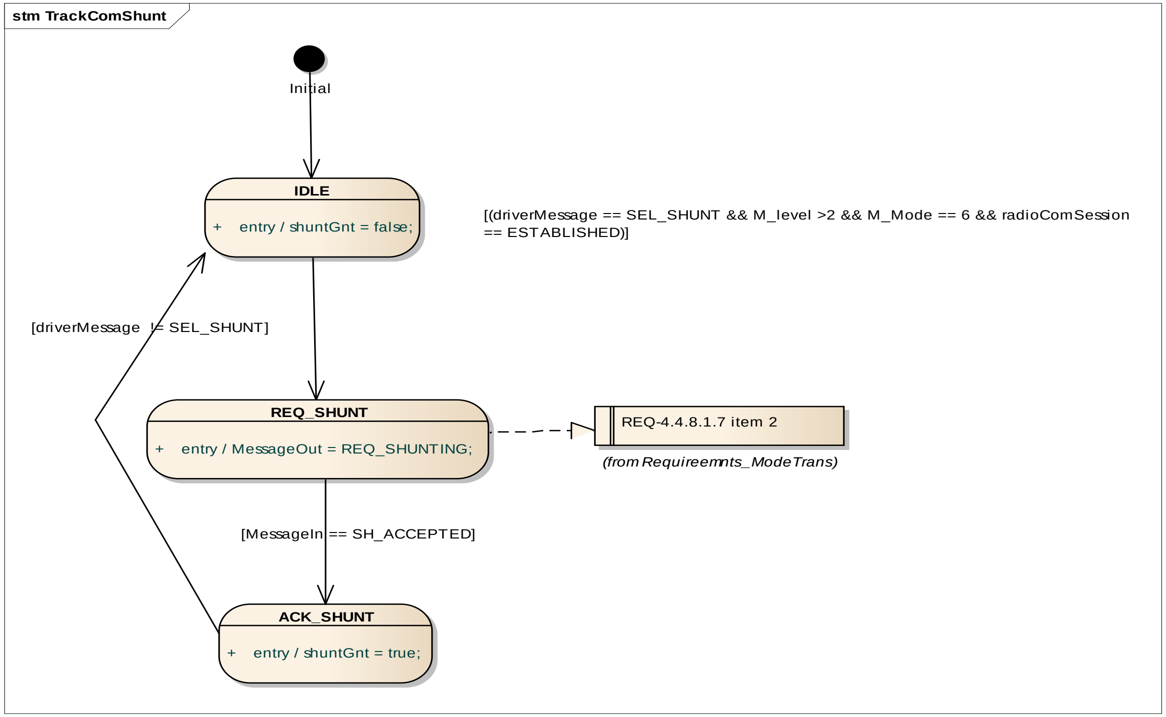
1) Pictures at the courtesy of opencliparts.org

Verification and Validation

Challenge

Verification and Validation challenge is to merge

- Agile Methods
- Open Source Process
- Open Proofs Concept
- Model Based Testing



stm TrackComShunt

Initial

IDLE

+ entry / shuntGnt = false;

[(driverMessage == SEL_SHUNT && M_level >2 && M_Mode == 6 && radioComSession == ESTABLISHED)]

[driverMessage != SEL_SHUNT]

REQ_SHUNT

+ entry / MessageOut = REQ_SHUNTING;

REQ-4.4.8.1.7 item 2

(from Requireemnts_ModeTrans)

[MessageIn == SH_ACCEPTED]

ACK_SHUNT

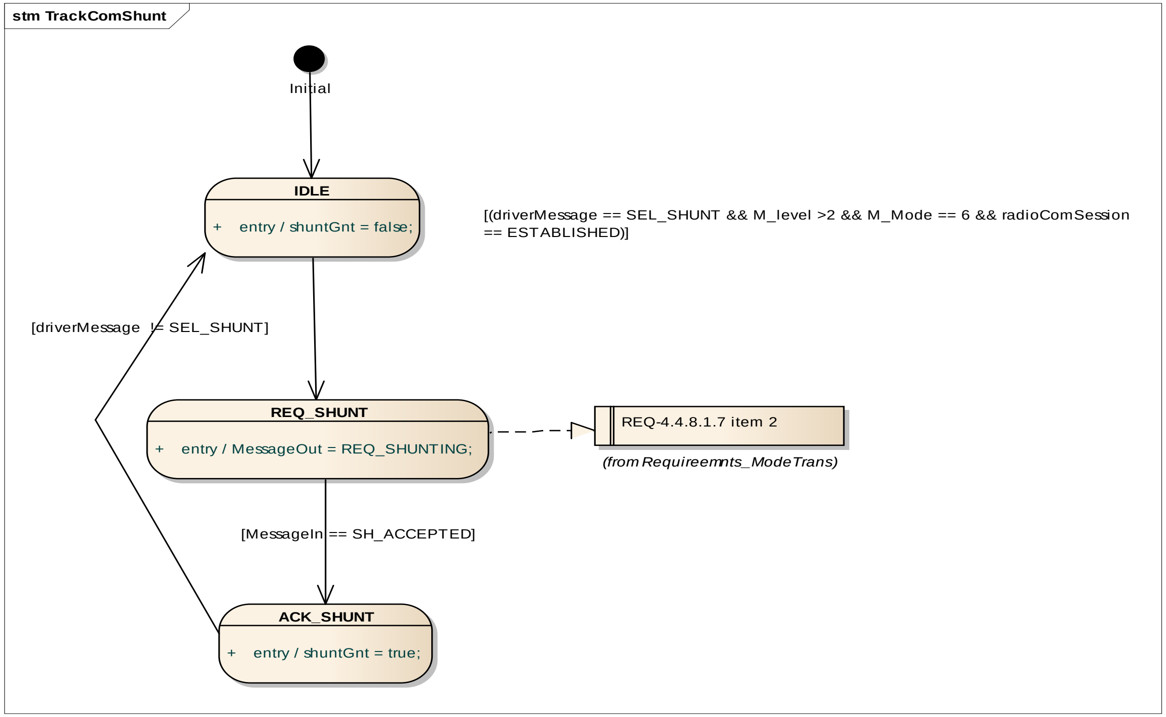
+ entry / shuntGnt = true;

Verification and Validation

Challenge

Verification and Validation challenge is to merge

- Agile Methods
- Open Source Process
- Open Proofs Concept
- Model Based Testing


stm TrackComShunt
Initial
IDLE
+ entry / shuntGnt = false;
[(driverMessage == SEL_SHUNT && M_level >2 && M_Mode == 6 && radioComSession == ESTABLISHED)]
[driverMessage != SEL_SHUNT]
REQ_SHUNT
+ entry / MessageOut = REQ_SHUNTING;
REQ-4.4.8.1.7 item 2
(from Requireemnts_ModeTrans)
[MessageIn == SH_ACCEPTED]
ACK_SHUNT
+ entry / shuntGnt = true;

to comply to

- Technical Specification for Interoperability (TSI)
- EN50128 – SIL4 Railway software development

Workpackage 4: Ongoing Meetings

Decision on which model to use for the first V&V Level

- 4th of July (WP4- & WP7- partner)

Weekly Online-Conference on Testing

- every Wednesday at 11h00 (DLR/ WP4- partner)

Weekly Online-Conference on Safety

- every Tuesday at 14h00 (TU-BS & All4Tec & AEbt / WP4- partner)

Weekly SCRUM meeting

- every Friday at 10h30 (WP4- partner)

Monthly Face-to-Face subcluster meeting

- At individual date in Braunschweig (Siemens, UB, DLR, ERTMS Sol.)

Code Verification subcluster meeting

- At individual date and location (Fraunhofer, CEA-List, ERSA)

Workpackage Structure 4

Workpackage 4 Verification and Validation Strategy (Marc Behrens, DLR)

Task 1 Tools & Profile Usage (Hardi Hungar, DLR)

- Verification and Validation Plan and Methodology

Task 2 Model Verification and Validation (Ana Cavalli, IT-Telecom)

- Applicability and Application of Verification and Validation for the abstract model

Task 3 Code Verification and Validation (Jens Gerlach, Fraunhofer)

- Applicability and Application of Verification and Validation for the implementation/ code

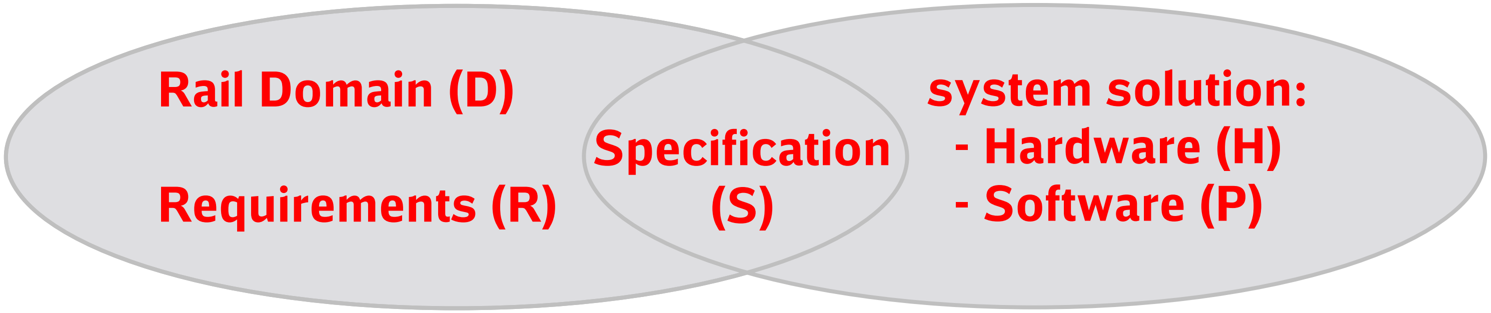
Task 4 Tools/ Process (Jan Welte, TU- BS)

- Generic Safety Case and for the tool chain and the processes

Task 5 Internal Assessor (Cyril Cornu, All4Tec)

- Internal Assessment Activities for the whole project

The World and the Machine[1]



Rail Domain (D)

Requirements (R)

Specification (S)

system solution:
- Hardware (H)
- Software (P)

Validation question:

Do we build the right system?

D and S ⇒ R

Verification question

Do we build the system right?

H and P ⇒ S

Conclusion:

D and H and P ⇒ R

[1] M. Jackson, 1995

Example: Procedure Train Reversing

Requirement

- (R) Reversing shall only be possible after exiting On-Sight, Limited Supervision or Full Supervision mode. (Subset-026-4.6.2)
- (R) Reversing shall only be applied if in standstill. (V=0) (SS_026_4-6-3[59])

Domain Properties

- (D1) Deploying reversing in full speed may have catastrophic outcome.
- (D2) Odometry sends speed signal to Onboard-Unit.
- (D3) Reversing shall only be applied if brakes are applied and display shows zero speed.

System specification

- (S) The system shall allow reversing thrust to be enabled if and only if wheels are at standstill and driver acknowledges.

Does D1 and D2 and D3 and S $\Rightarrow$ R?

Verification

According to the Degree of Formalization

Verification of…		
… the SRS-Model against Subset-026	meta model, SSRS	• Peer Review • Design Manual • …
… a detailed model against a higher level model	openETCS design model 1)	• Properties tests • Peer review • Test model • Test design …
… a detailed model against a higher level model	detailed model1)2)	• Equivalence checkers • Model based tester …
… code against a detailed model	Code	• Unit test • Properties checker • Simulator …

1) Design- and detailed- model can be the semi-formal model
2) Detailed model can be the strictly-formal model

Validation

According to the Degree of Formalization

Validation of…		
… the SRS-Model against operational rules	meta model, SSRS	• Review by operators • Peer Review • Risk-/ Safety-Analysis …
… a model by validator or validation logic	openETCS design model	• Data Preparation • Properties tests • Model checking • Risk-/ Safety-Analysis …
… code by validator or validation logic	detailed model	• Prep. of operation scenario • Model checking • Risk-/ Safety-Analysis …
… code by validator or validation logic	Code	• Properties checker • Preparation Simulator with operational scenario • Risk-/ Safety-Analysis …

User Stories for Verification - Example

Each Verification and Validation Step is linked to a user story:

A user could be a verifier/ validator of the design step.

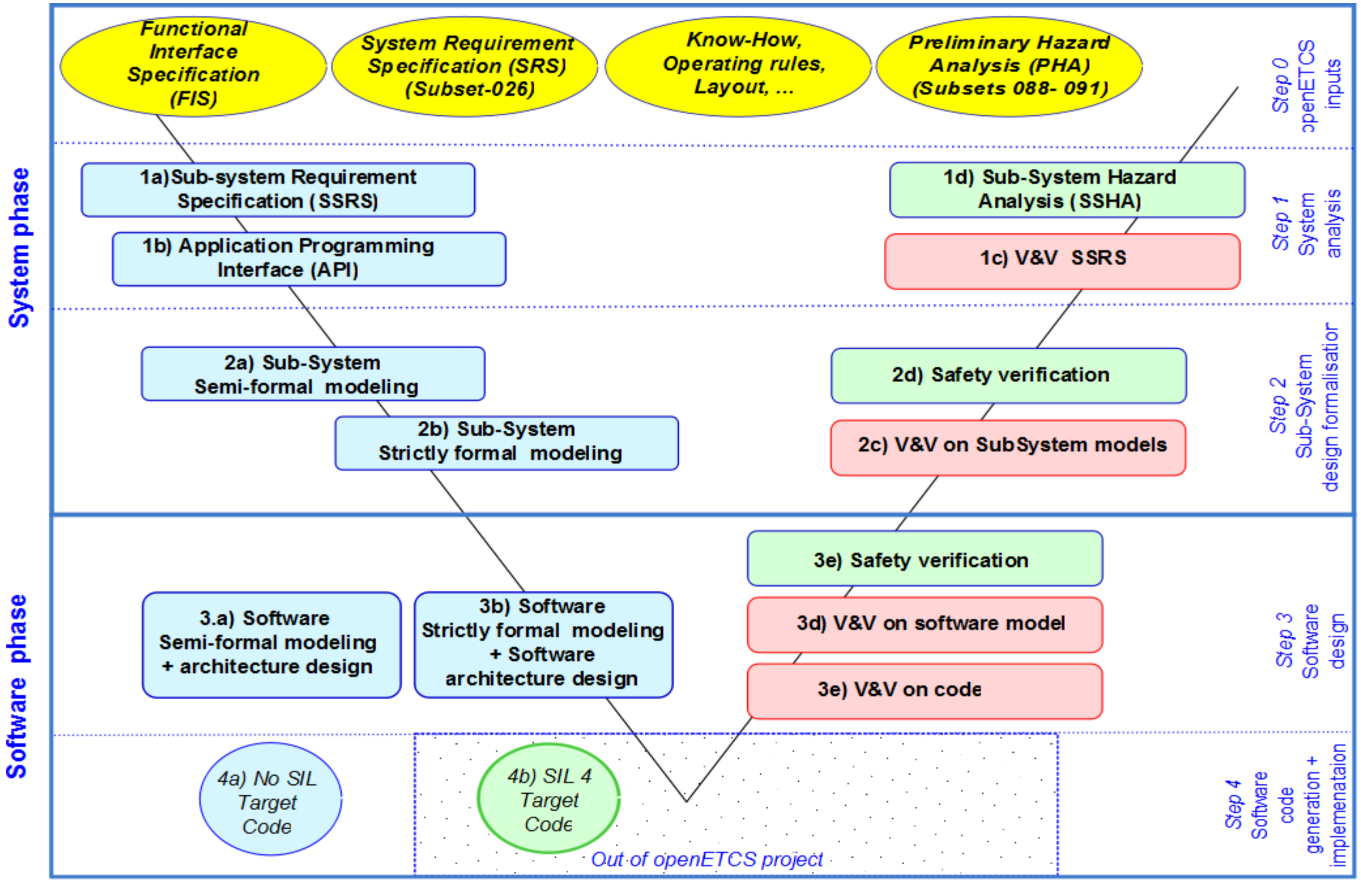
US1 user story to code unit tests

- **US1.1 code that implements the user story**
- **US1.2 unit tests that test the code that implement the user story**

US2 user story to validate code on an operational scenario

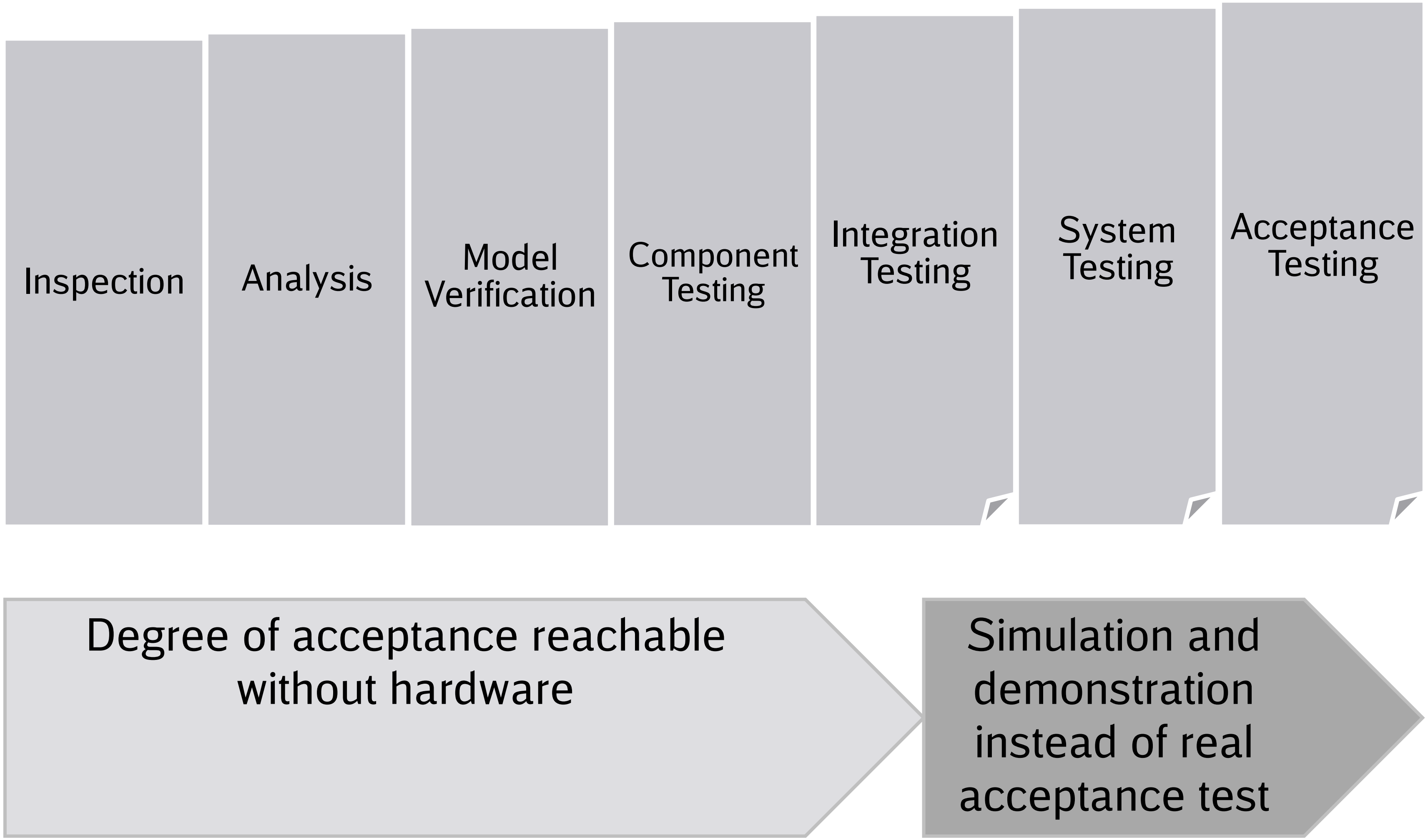
- **US2.1 prepare the code capable of running the operational scenario**
- **US2.2 identify the success criteria**
- **US2.3 execute and validate the operational scenario**

Verification and Validation Inside openETCS


Functional Interface Specification (FIS)
System Requirement Specification (SRS) (Subset-026)
Know-How, Operating rules, Layout, ...
Preliminary Hazard Analysis (PHA) (Subsets 088- 091)
Step 0 openETCS inputs
System phase
1a)Sub-system Requirement Specification (SSRS)
1b) Application Programming Interface (API)
1d) Sub-System Hazard Analysis (SSHA)
1c) V&V SSRS
Step 1 System analysis
2a) Sub-System Semi-formal modeling
2b) Sub-System Strictly formal modeling
2d) Safety verification
2c) V&V on SubSystem models
Step 2 Sub-System design formalisatior
Software phase
3.a) Software Semi-formal modeling + architecture design
3b) Software Strictly formal modeling + Software architecture design
3e) Safety verification
3d) V&V on software model
3e) V&V on code
Step 3 Software design
4a) No SIL Target Code
4b) SIL 4 Target Code
Out of openETCS project
Step 4 Software code generation + implemenataion

Verification and Validation

Way to acceptance



Inspection

Analysis

Model Verification

Component Testing

Integration Testing

System Testing

Acceptance Testing

Degree of acceptance reachable without hardware

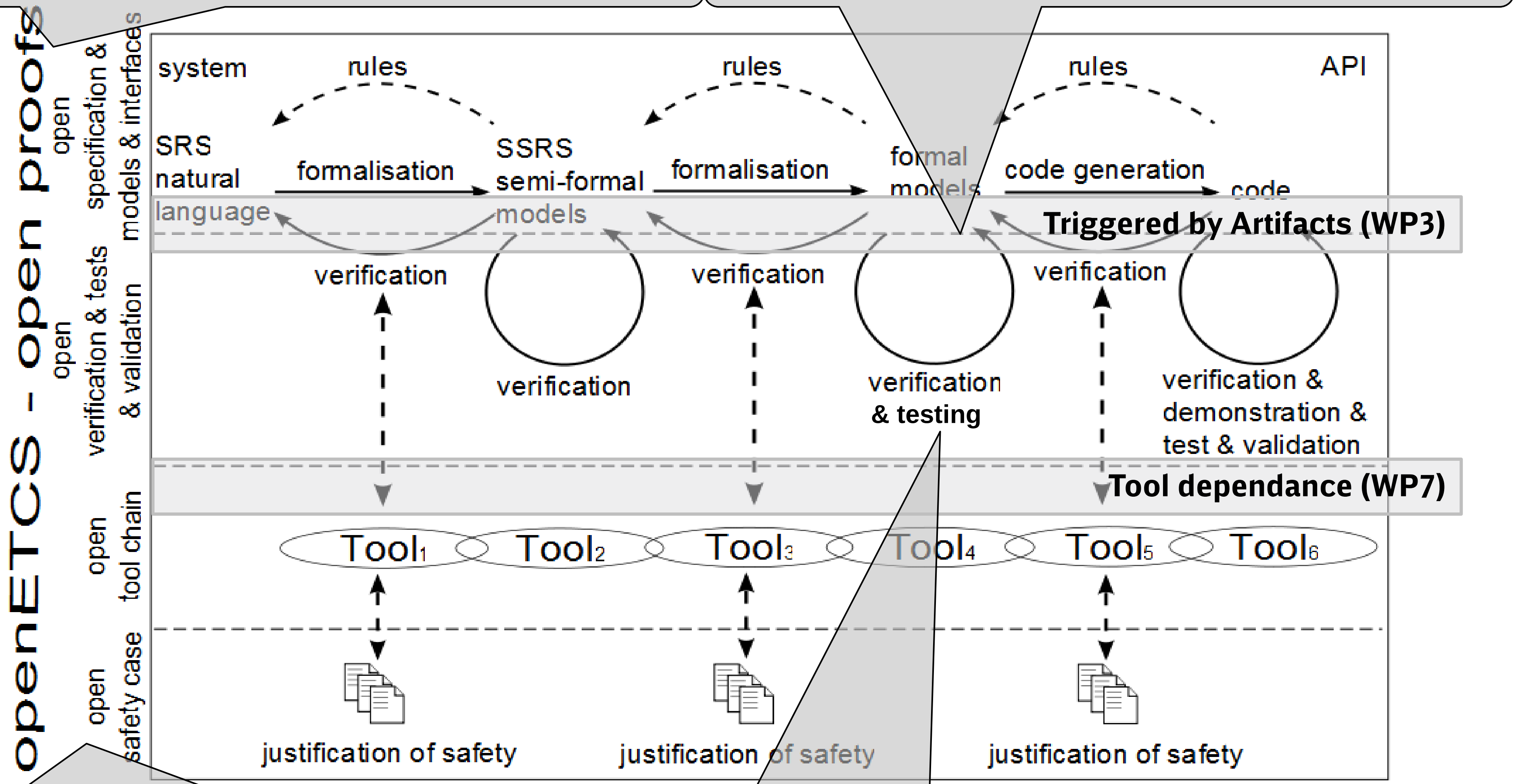
Simulation and demonstration instead of real acceptance test

Verification and Validation

Innovation

based on open source software

automatically-verifiable proofs



Triggered by Artifacts (WP3)

Tool dependance (WP7)

model-based safety case

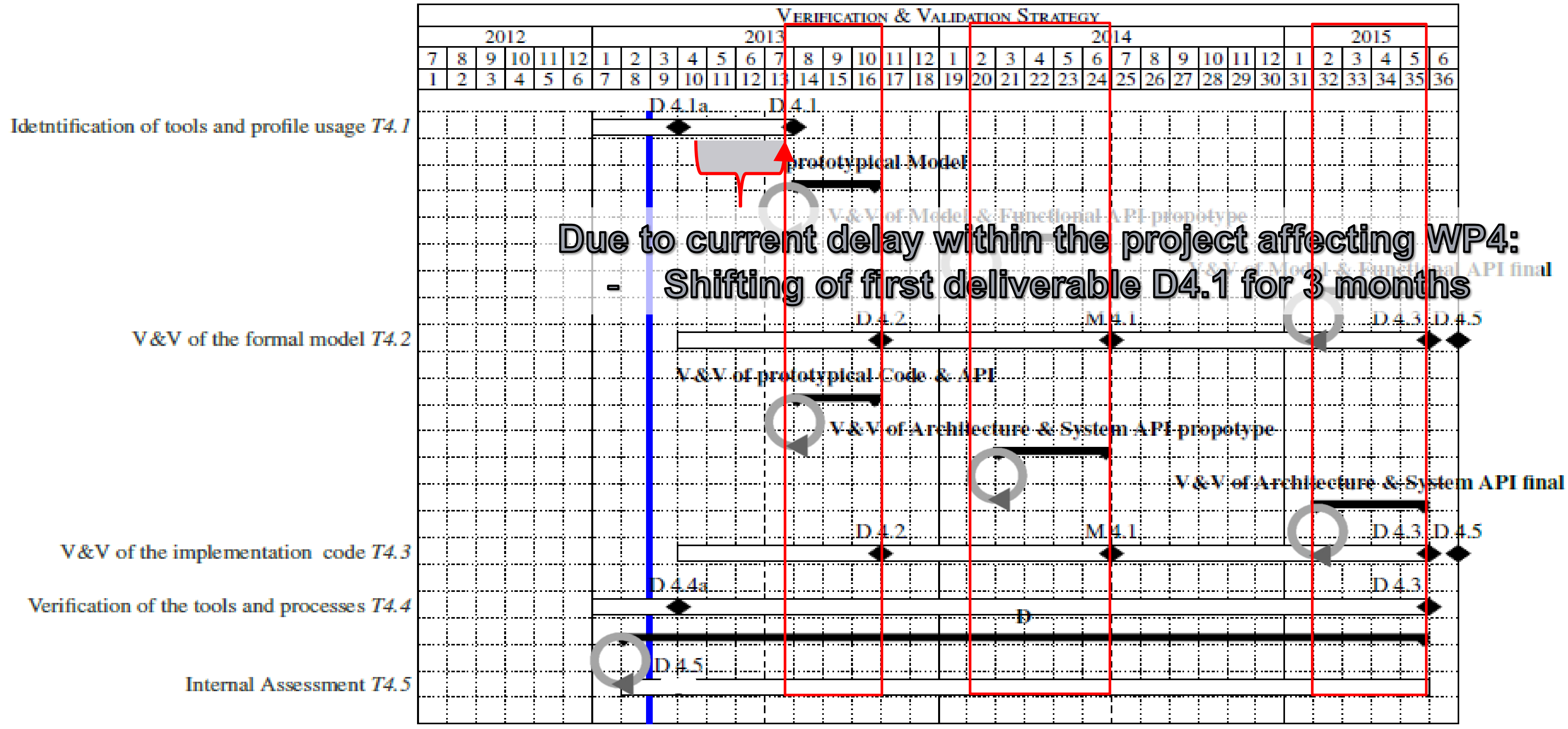
early model-based testing

Verification and Validation Activities

Artifacts Triggered SCRUM-Verificarion and Validation Level

3 Verification and Validation Level:

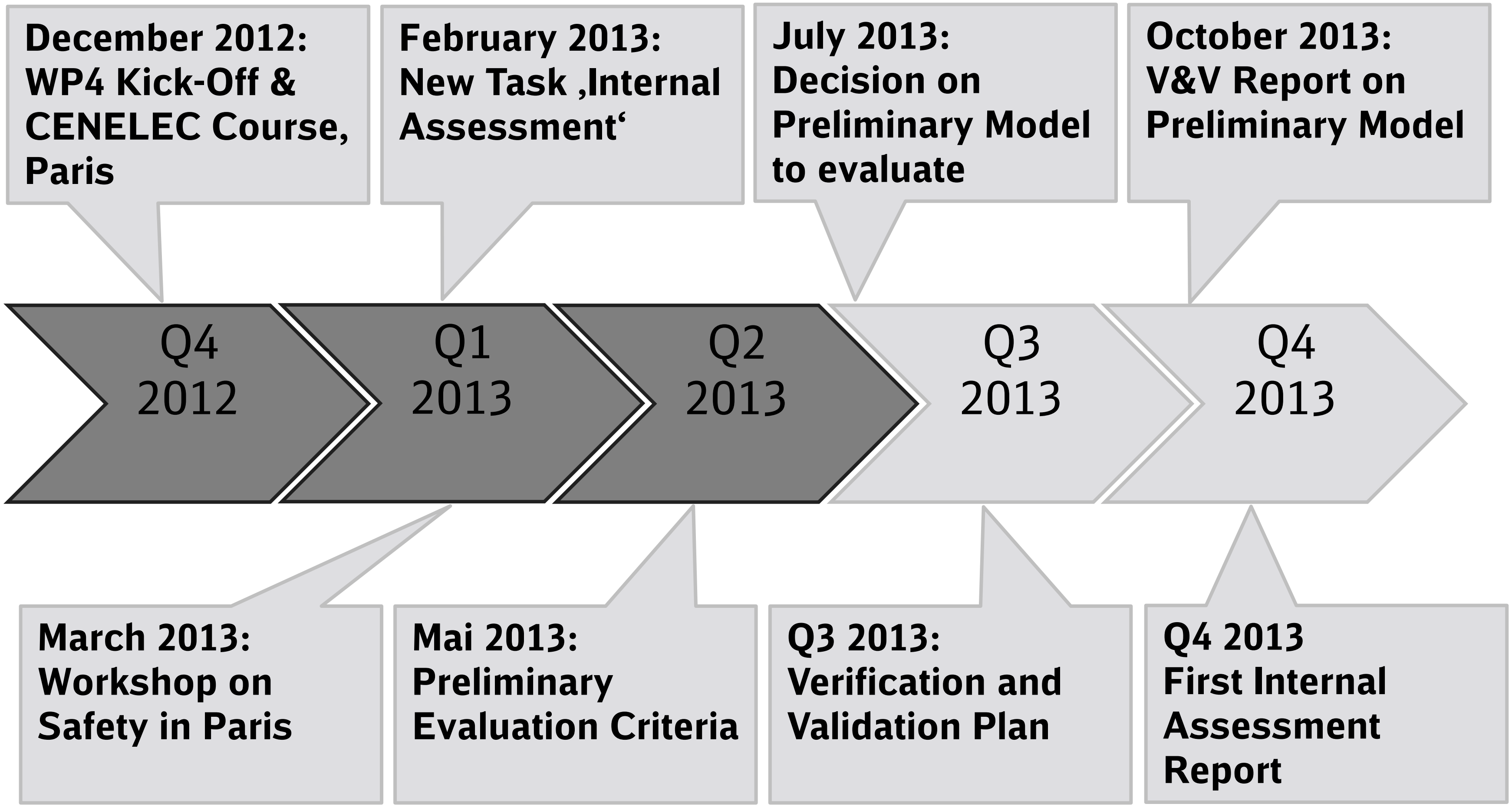
GANTT chart



Due to current delay within the project affecting WP4:

- Shifting of first deliverable D4.1 for 3 months

WP4 Progress



December 2012:
WP4 Kick-Off &
CENELEC Course,
Paris

February 2013:
New Task ‚Internal
Assessment‘

July 2013:
Decision on
Preliminary Model
to evaluate

October 2013:
V&V Report on
Preliminary Model

Q4 2012

Q1 2013

Q2 2013

Q3 2013

Q4 2013

March 2013:
Workshop on
Safety in Paris

Mai 2013:
Preliminary
Evaluation Criteria

Q3 2013:
Verification and
Validation Plan

Q4 2013
First Internal
Assessment
Report

- Thank you for your attention!

- For further regular information, please subscribe to the Verification & Validation group: wp4+subscribe@openetcs.org

Marc Behrens
Deutsches Zentrum für Luft- und Raumfahrt e.V.
Marc.Behrens@DLR.de
Tel: +49 (0) 531 295 3451