ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

Verification and Validation in openETCS: Methodology and Results

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

Halfterm Project Review

Marc Behrens, Hardi Hungar

Munich, 14.01.2014

WP 4 Review Schedule

- 17:00 - 17:20 Introduction and overview of the first V&V Level (Marc Behrens and Hardi Hungar, DLR)
- 17:20 - 17:50 Results on Model V&V (Ana Cavalli, Institute Telecom)

  [Video contribution]

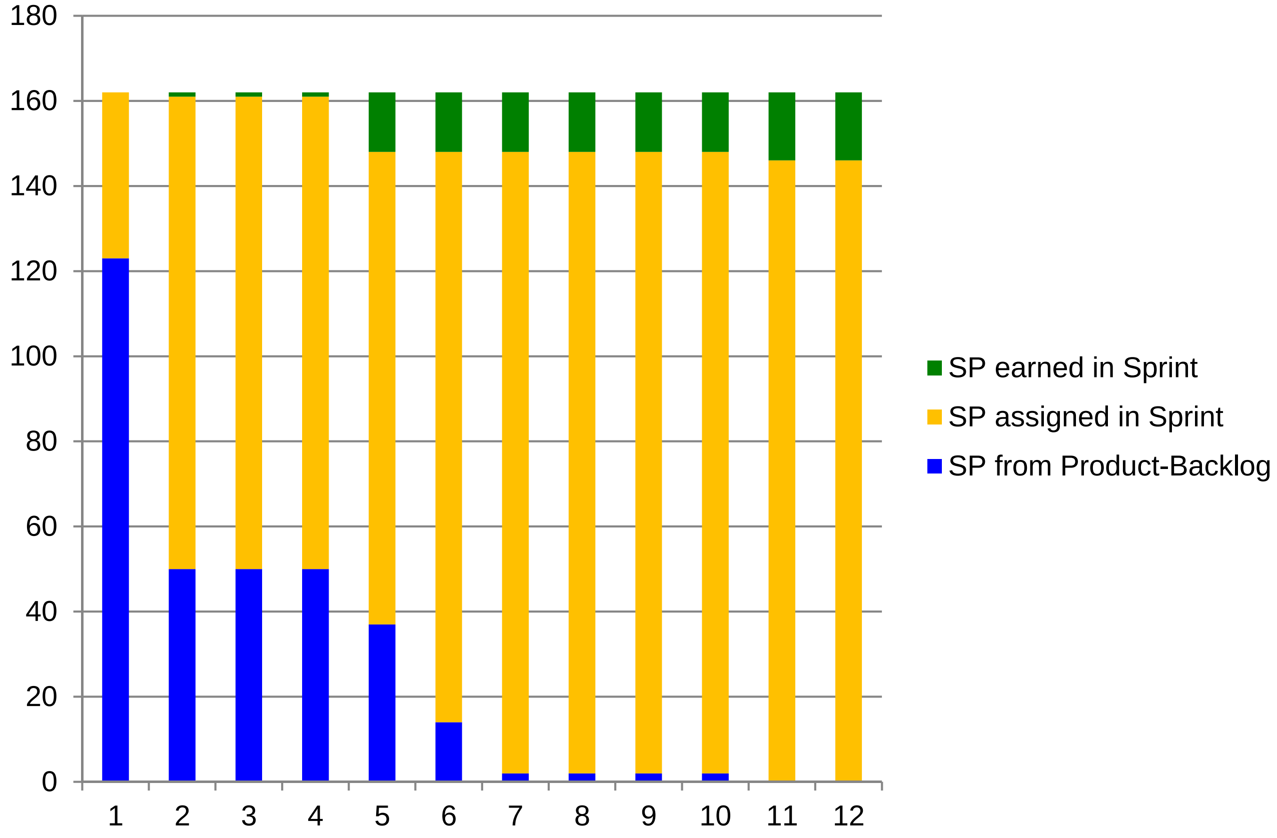
  - 17:50 - 18:00 Coffee Break
- 18:00 - 18:10 Results on Implementation / Code V&V (Jens Gerlach, Fraunhofer FOKUS)
- 18:10 - 18:30 Process and Safety (Jan Welte, TU BS)
- 18:30 - 18:40 Internal Assessment and Preparation of Workshop in Nuernberg (Hardi Hungar, DLR)
- 18:40 - 19:15 Overall Conclusions & Discussion of upcoming V&V activities (Marc Behrens, DLR)

First-Level Verification and Validation: Objectives, Approach and Results

- Objectives
  - Establish the work environment and form teams for V&V in openETCS
  - Select V&V tasks
  - Perform a round of evaluatory and factual V&V activities
- Approach
  - Agile (SCRUM) organisation of activities
  - Take up available input from other WPs (models, code, tools, specs)
  - Build on existing competences and use them for openETCS
- Results
  - Several V&V activities performed
  - Many more started
  - D4.2 in three parts

Organization of the VnV Process

- 12 Sprints over three months
  - Regular grooming
  - Daily standups
  - Weekly review

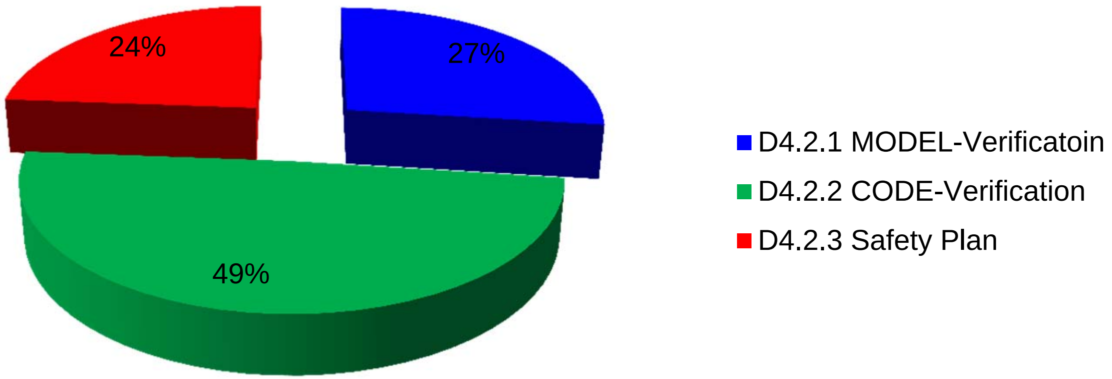


Organization of the VnV Process

Sprints

Thematic breakdown of 1st level VnV

- according to numbers of issues -



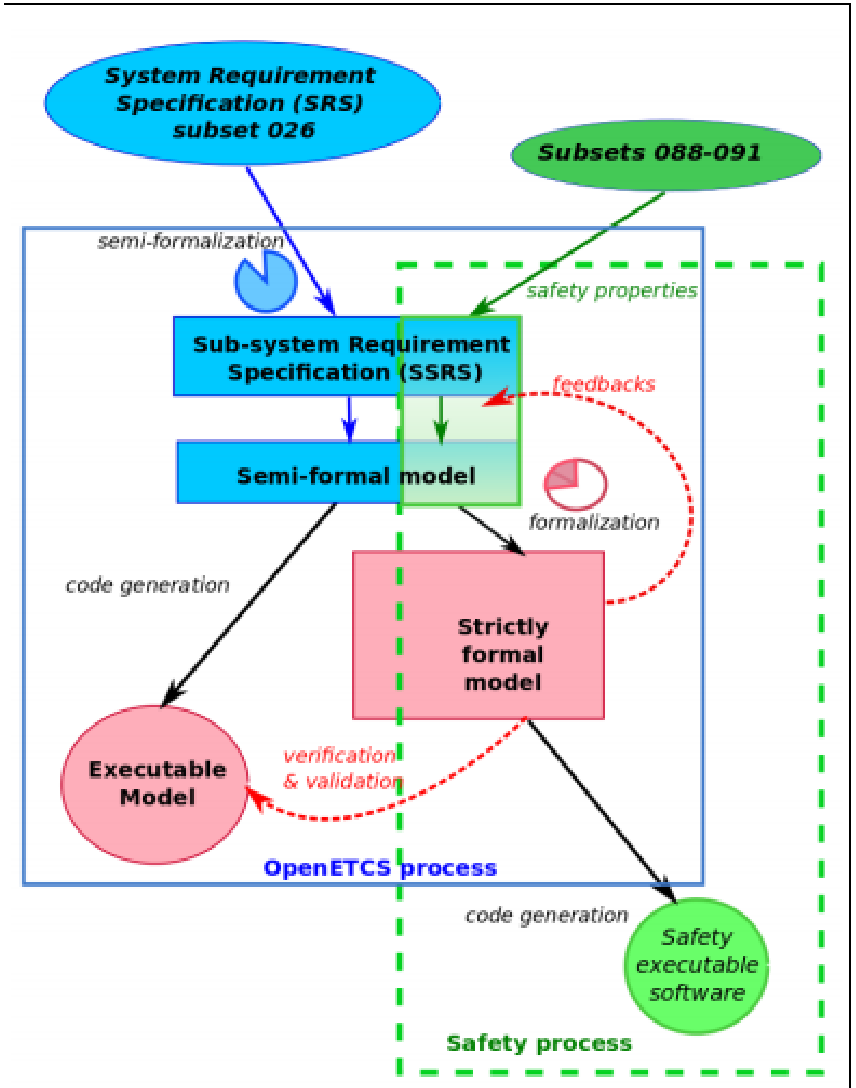
WP4 Deliverable Status

no.	title	due	state	actual/planned delivery
D4.1	Report on V&V Plan & Methodology	2013/Q3	100%	2013/Q3
D4.2.1	1st V&V report on model	2013/Q4	60%	2014/Q1
D4.2.2	1st V&V report on implementation / code	2013/Q4	100%	2013/Q4
D4.2.3	Safety Plan	2013/Q4	50%	2014/Q1

Methodology of Verification and Validation (1/5)

Specification:

- **Mostly derived from SS026**
  - **SSRS and formal model not yet available for VnV**



openETCS Process (D2.3)

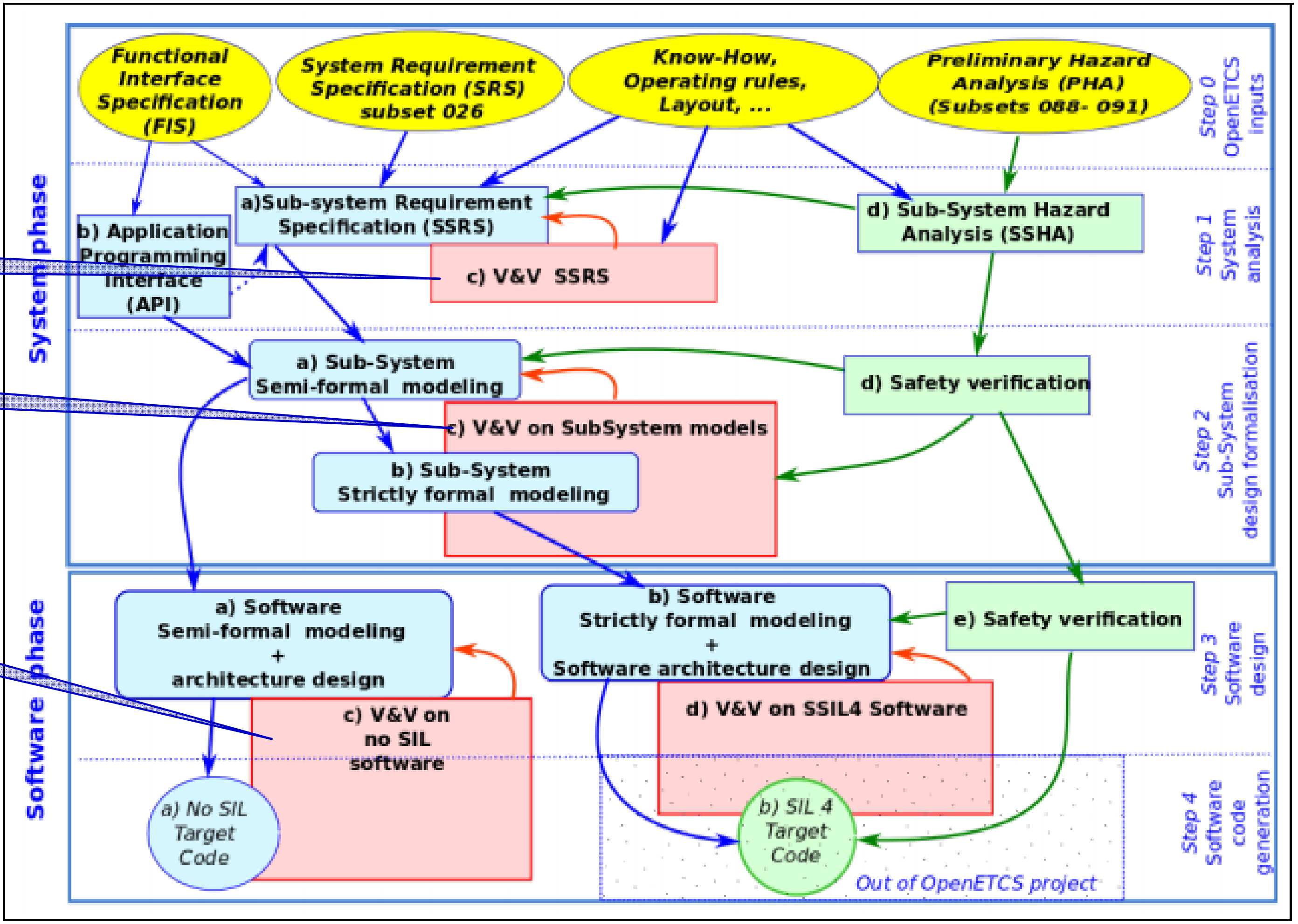
Methodology of Verification and Validation (2/5)

Verification objects

Model

Models

Code


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
a)Sub-system Requirement Specification (SSRS)
b) Application Programming Interface (API)
c) V&V SSRS
d) Sub-System Hazard Analysis (SSHA)
Step 1 System analysis
a) Sub-System Semi-formal modeling
c) V&V on SubSystem models
b) Sub-System Strictly formal modeling
d) Safety verification
Step 2 Sub-System design formalisation
Software phase
a) Software Semi-formal modeling + architecture design
c) V&V on no SIL software
b) Software Strictly formal modeling + Software architecture design
e) Safety verification
d) V&V on SSIL4 Software
Step 3 Software design
a) No SIL Target Code
b) SIL 4 Target Code
Out of OpenETCS project
Step 4 Software code generation

Methodology of Verification and Validation (3/5)

Verification objects:

- Models for
  - Management of radio communication (SCADE, Siemens)
  - Procedure on-sight (B, Event-B, Systerel)
  - Start of mission (CPN, TWT)
  - Braking curves (discretized function, ERA)
  - Abstract model of full system (ETFSM, Institut Telecom)
- Code
  - Bitwalker (C, Siemens)
  - Management of radio communication (C from SCADE, Siemens)

Methodology of Verification and Validation (4/5)

Verification Objectives

- Object verification !
  - Models and code fragments
  - Objects are expected to become more mature
- Exploration/evaluation of methods and tools !!!
  - Pre-existing and openETCS developments/adaptations
  - Data for selecting and further adapting methods and tools
- Detailing V&V process steps !!!
  - Exploring how things could look like
  - Input for revising the V&V plan

Methodology of Verification and Validation (5/5)

VnV Means

- Mostly pre-existing tools, partly adapted to openETCS
  - IF (test generation), RT-Tester (Test generation and execution), CPN (simulation), JPF, SPIN (model checking), Atelier B (tool suite), ProB (simulation, model checking), SCADE (static checks), Rodin (formal proof model), RSM, Understand, Clang, CPP (static analysis), FRAMA-C (formal proof code)
- Mixture of open-source and closed-source tools
- Main effort to evaluate/demonstrate suitability

Results of Verification and Validation

VnV results

- Verification activities
  - Evaluation of tools for VnV on models and code (Systerel)
  - Test generation and execution on code (U Bremen, Siemens)
  - Code fragments static analysis (SQS) and formal verification (Fraunhofer, CEA List)
  - Specification model setup for future verification (Institut Telecom)
  - Safety case preparation (All4Tec, TU BS)
  - Preparation of further verification activities (TWT, DLR, U Ro)
- Deliverable D4.2 in three parts
  - code verification part ready for review

Schedule

- 17:00 - 17:20 Introduction and Overview of the first V&V Level (Marc Behrens and Hardi Hungar, DLR)
- 17:20 - 17:50 Results on Model V&V (Ana Cavalli, Institute Telecom)

  [Video contribution]

  - 17:50 - 18:00 Coffee Break
- 18:00 - 18:10 Results on Implementation / Code V&V (Jens Gerlach, Fraunhofer FOKUS)
- 18:10 - 18:30 Process and Safety (Jan Welte, TU BS)
- 18:30 - 18:40 Internal Assessment and Preparation of Workshop in Nuernberg (Hardi Hungar, DLR)
- 18:40 - 19:15 Overall Conclusions & Discussion of upcoming V&V activities (Marc Behrens, DLR)