ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

WP2 ITEA2 Review
openETCS

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

Paris, 03.07.2013

Goals of openETCS as seen by WP2 (1/2)

To model an open source kernel for the onboard subsystem (baseline 3).

- A formal, simulable, high level model, that would be understandable by domain experts
- Lift the ambiguities of the specification
- Could be considered afterward as a reference implementation

Refining this model toward a non safety implementation ("demonstrator")

Goals of openETCS as seen by WP2 (2/2)

- To define and produce a tool-chain and a methodology/process that allow to reach these goals while being compliant to CENELEC standards for a SIL4 subsystem.
- To produce a Safety Case concept that covers all the required steps *w.r.t.* these standards, then to sample the safety activities on parts of the subsystem
- ... and all this in an open source context, using open source tools.

WP2 Deliverables

D2.1: Report on existing methodologies

D2.2: Report on CENELEC standards

D2.3: Process definition

D2.4: Methods definition

D2.5: A Subset of Requirements for Benchmarking of Tools

D2.6: Set of requirements for the model

D2.7: Set of requirements for API

D2.8: Set of requirements tools

D2.9: Set of requirements for V&V

D2.1: Report on existing methodologies

- This document provides the *state of the art* on modelisation and formalisation within signalling the system and train control/command
- The state of the art was provided by conducting interviews of railway undertaking and manufacturer
- Status: final version released

D2.2: Report on CENELEC standards

This report present the requirements of CENELEC standards (mainly EN50128) for the project. It also describes the requirement in term of computer security.

Status: final version released

D2.3: Process definition

This document describes the overall that will be used in the openETCS project for the modeling of the system.

This process shall instantiate the requirements that are provided in the D2.6-D2.9 requirement document.

Status: final version released

D2.4: Methods definition

This document define the methods that will be used for the formal description or the ETCS subsystem that is modelled.

In order to define the method, it is necessary to have chosen the language and formalism

- The final version was therefore postponed in order to follow the choice of the method by WP7

Status:

- intermediate version released
- final version will be provided in october

D2.5: A Subset of Requirements for Benchmarking of Tools

This document provides the elements for the benchmarking of the tools by WP7. In particular it provides a subset of the requirements of the ERTMS SRS that should be modelled on all the system that are evaluated.

Status: final version released

D2.6-D2.9: Requirements for openETCS

This document contains the higher level requirements for the openETCS project.

To enhance the consistency, it was decided to provide the deliverables as different chapters of a single document.

D2.6 (requirements for the model):

- 7.2 System & Architecture
- 7.3 Model(s)
- 7.6 Language & Formalism

D2.7 (requirements for the API)

- 7.1 Runtime model & API

D2.8 (requirements for tools)

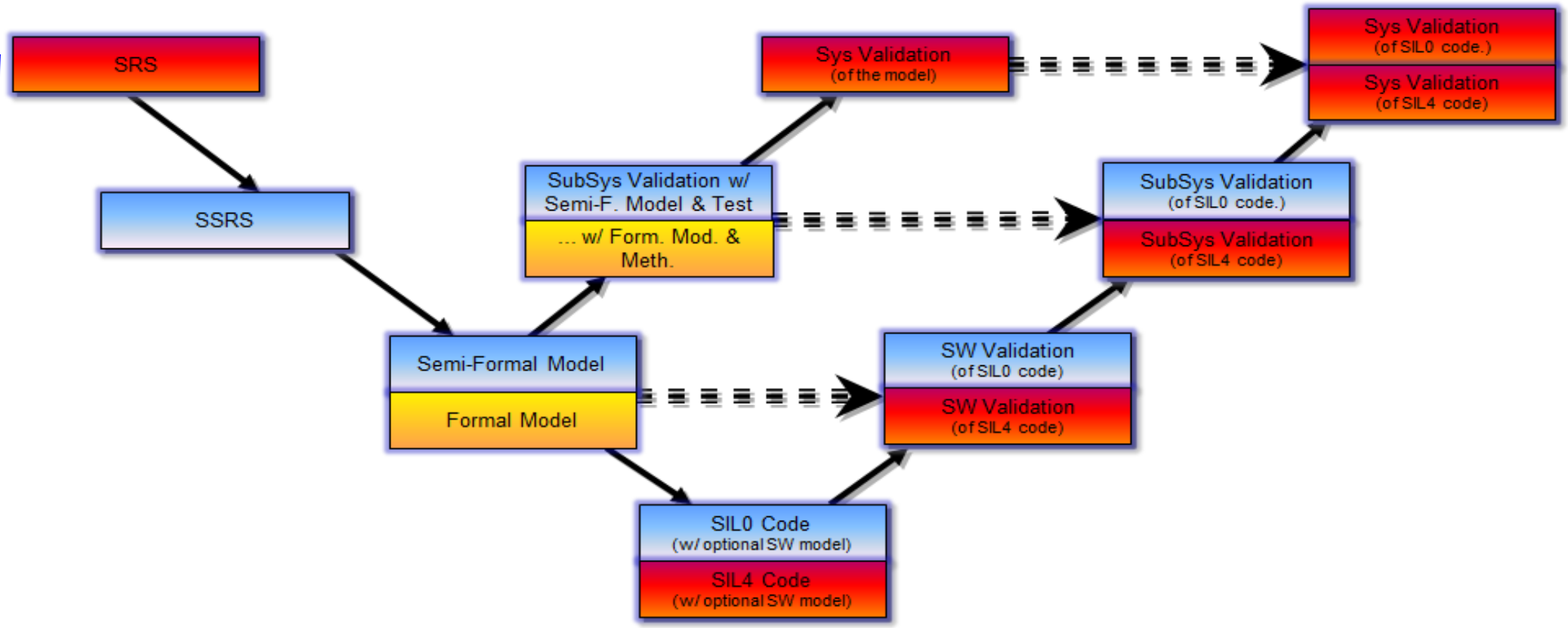
- 7.6 Language & Formalism
- 7.7 Tools chain

D2.9 (requirements for V&V)

- 7.4 Safety
- 7.5 Verification & Validation

Status: final version released

Main process proposed by WP2



SSRS

Formal Model

SW Validation
(of SIL4 code)

Task is part of the project

Task is part of the project but will done on a sample

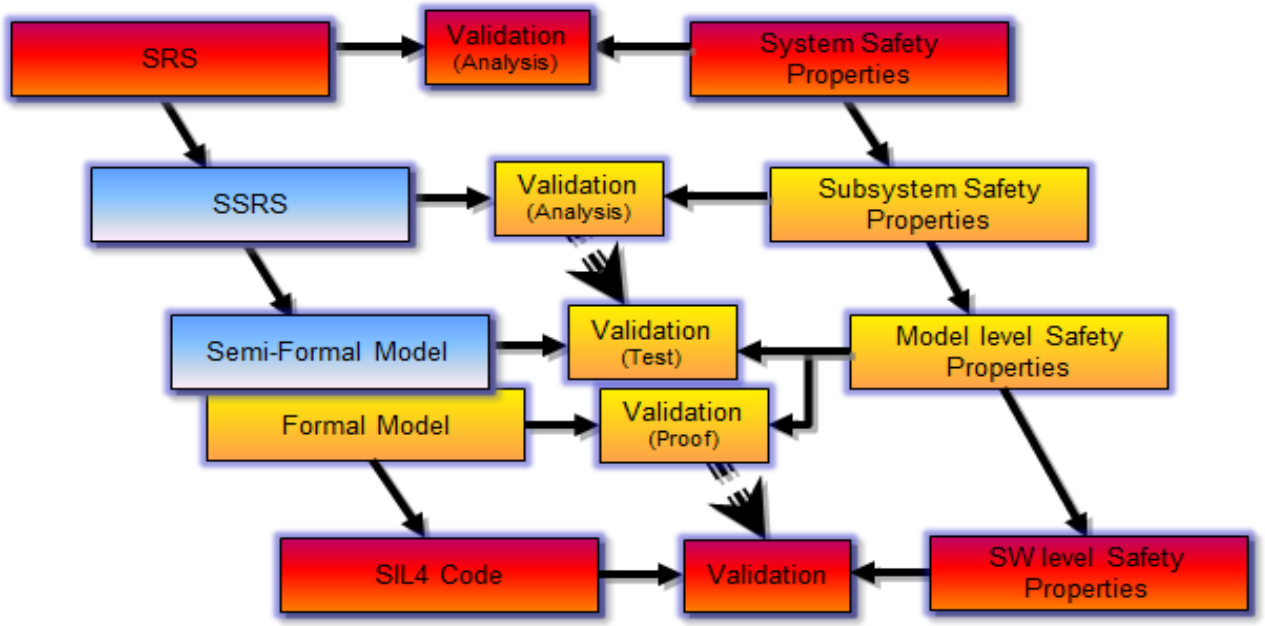
Task is not part of the project

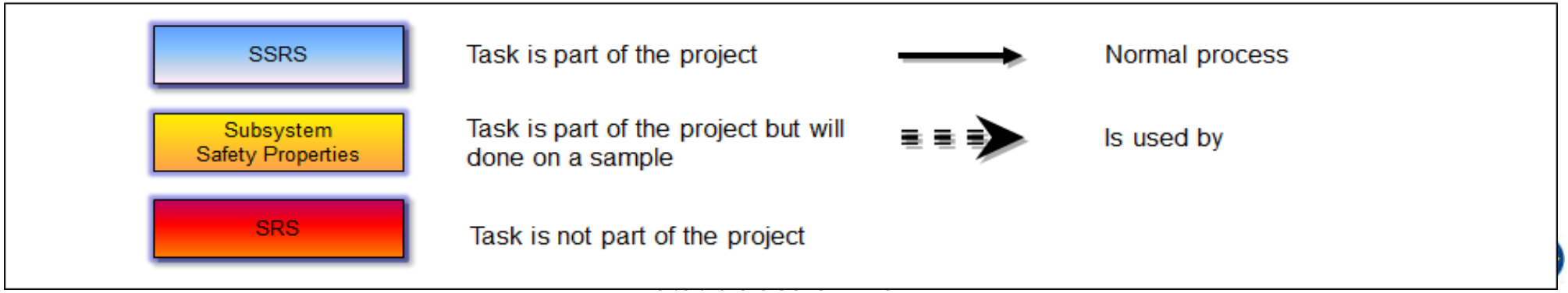
Note: Verification tasks between items that are part of the project are also part of the projects. They are not represented here to avoid cluttering of the drawing.

Normal process

Is used by

Safety process





Highlights of the process defined by WP2

The SRS SUBSET-026 is refined into a SSRS (subsystem requirement specification)

- Functional internal architecture of the subsystem
- Requirement refined into this architecture
- Safety/Non Safety tags

The SSRS is implemented into a Semi-Formal model, which should be simulable

The Semi-Formal model is completed on some parts by a Fully (Strictly) Formal Model.

A Safety Case Concept is provided, that should detail all the required safety activities in order to produce a SIL4 subsystem

Part of the safety activities are done on samples of the system

Internal safety assessment

A "demonstrator" (non SIL software) is produced from the model(s)

An open source tool chain that covers every steps is produced

Schedule for WP2 Requirements on Project