



Workpackage 4

Verification & Validation & Safety approach

supported by:



Federal Ministry
of Education
and Research



Région de
Bruxelles-
Capitale



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA
E INNOVACIÓN

openETCS@ITEA2 Project

Marc Behrens, Jan Welte

Paris, 04.07.2013

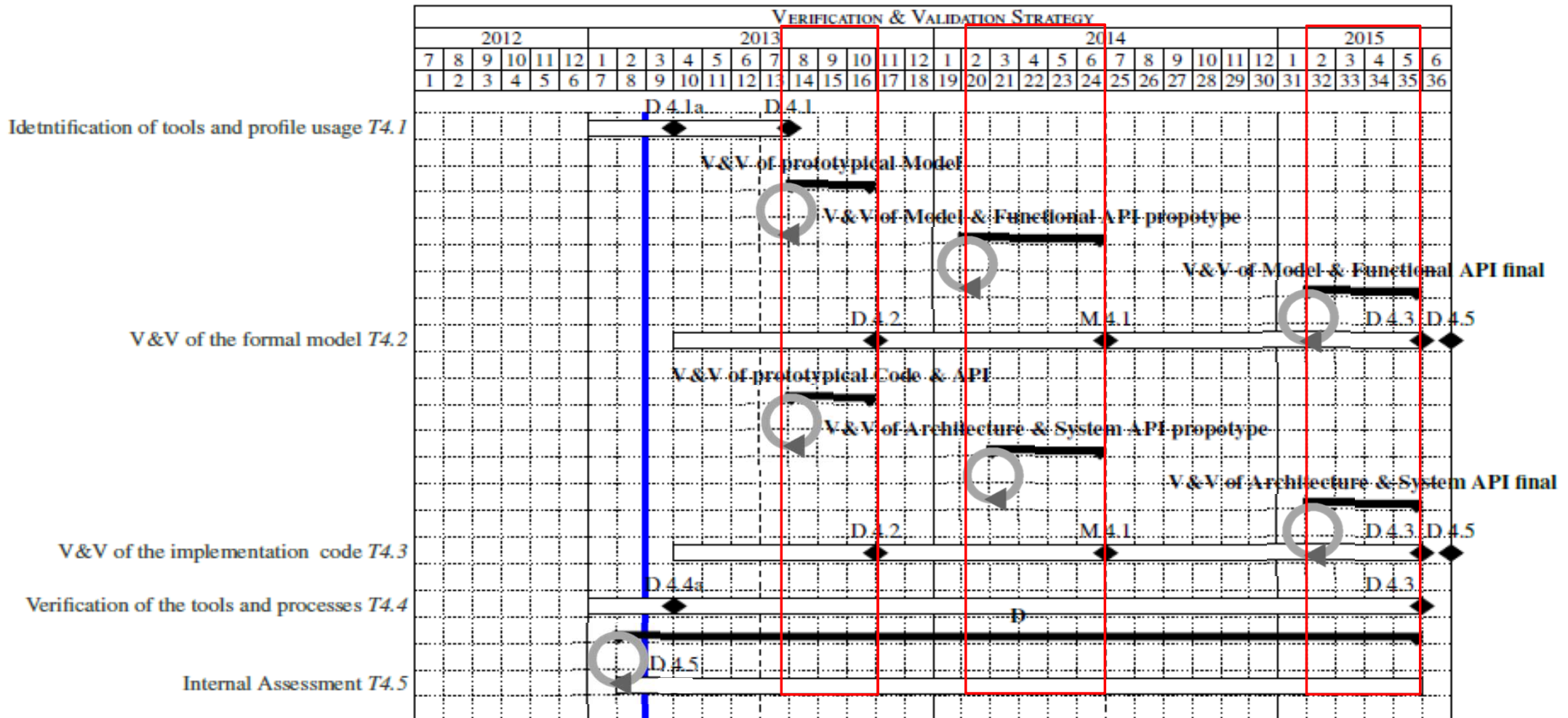


Verification and Validation Activities

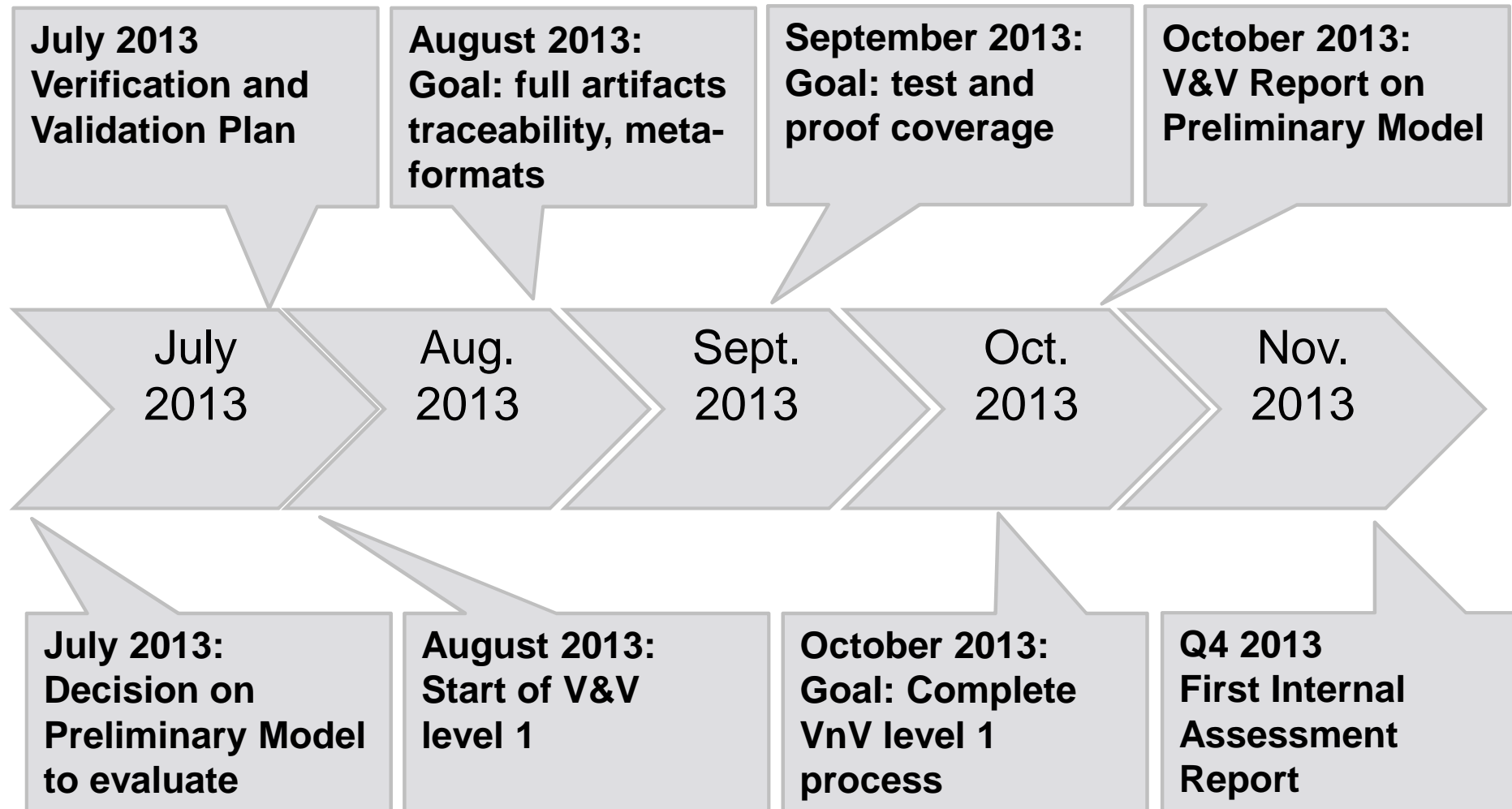
Artifacts Triggered SCRUM-Verification and Validation Level

3 Verification and Validation Level:

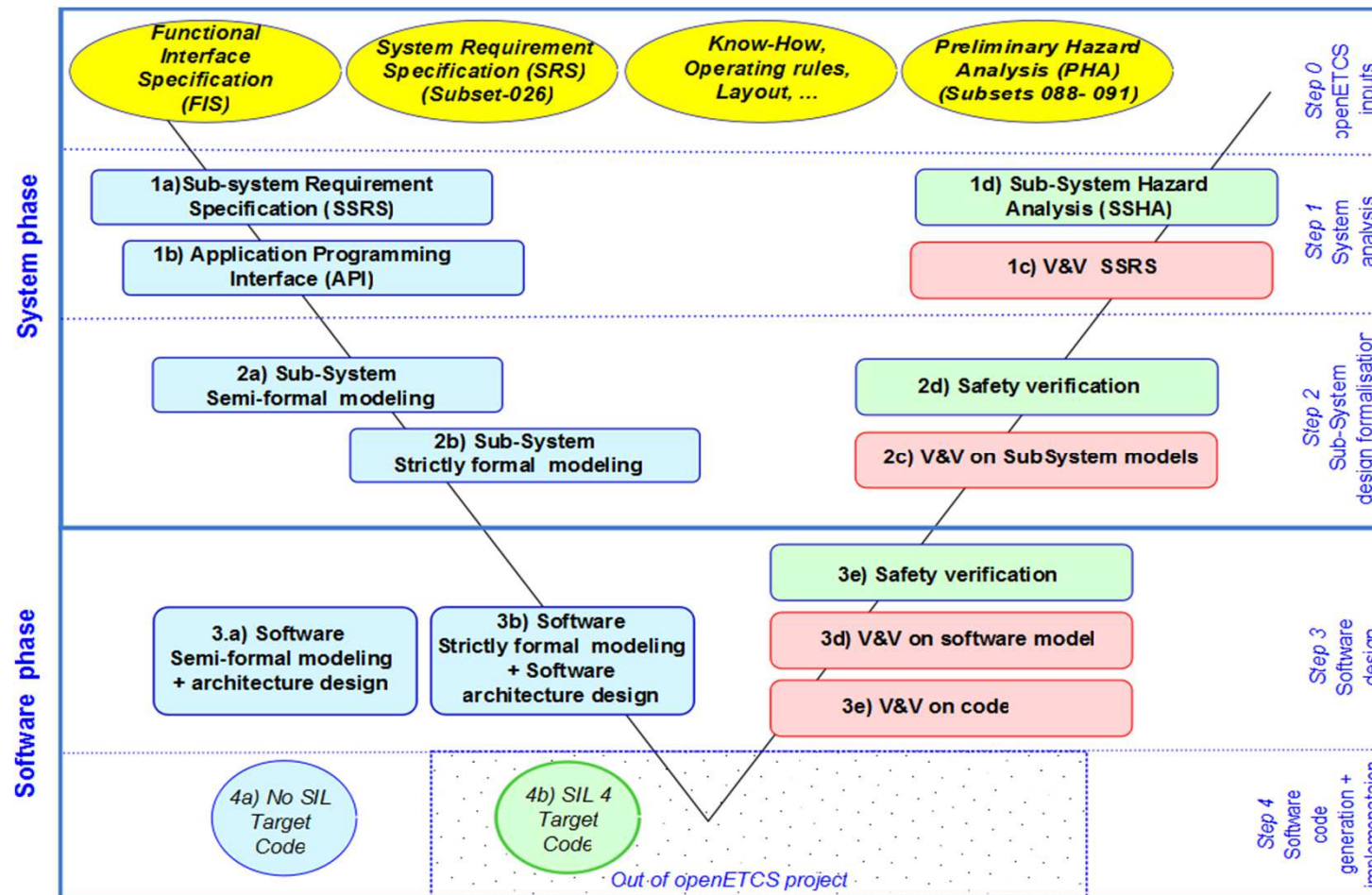
GANTT chart



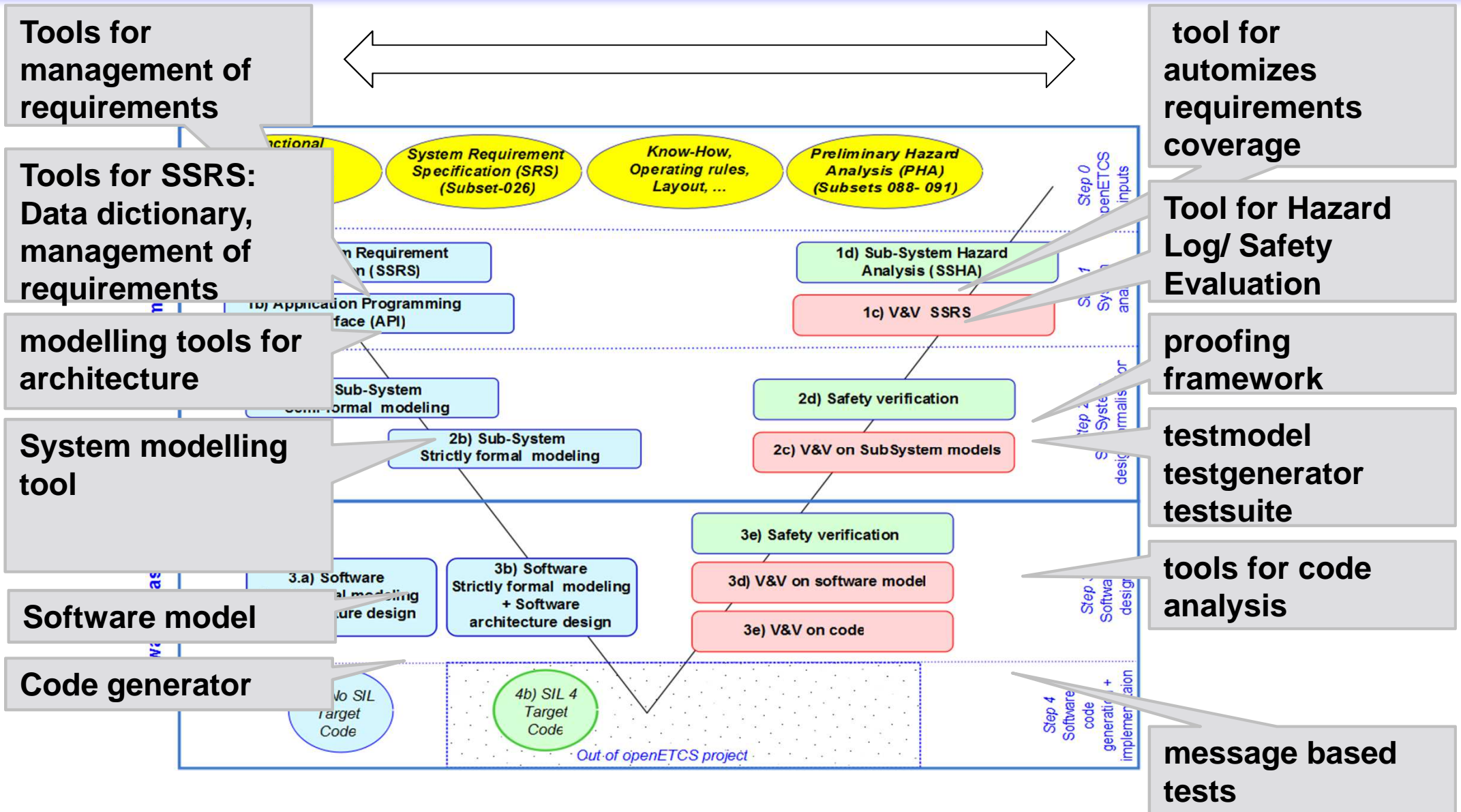
WP4 Progress



Verification and Validation Inside openETCS

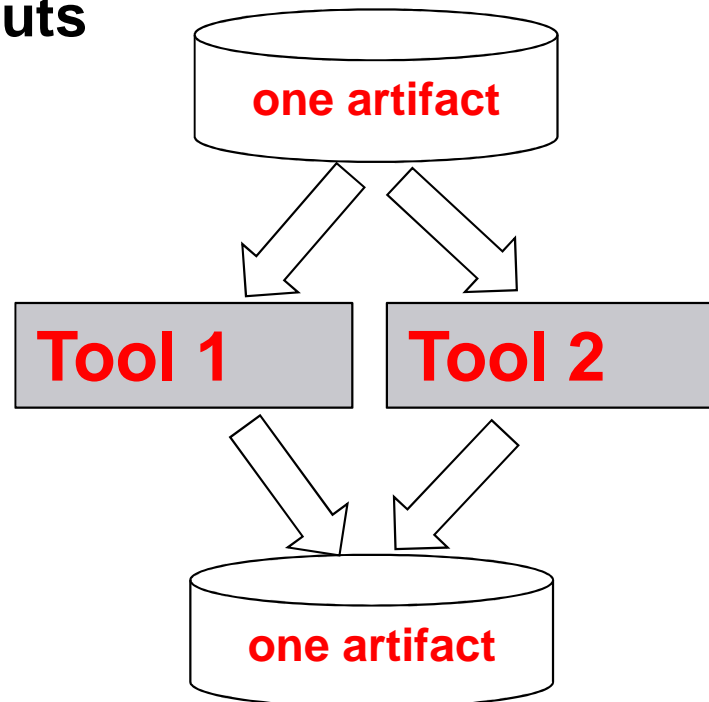


Verification and Validation Inside openETCS



Qualification for generated artifacts

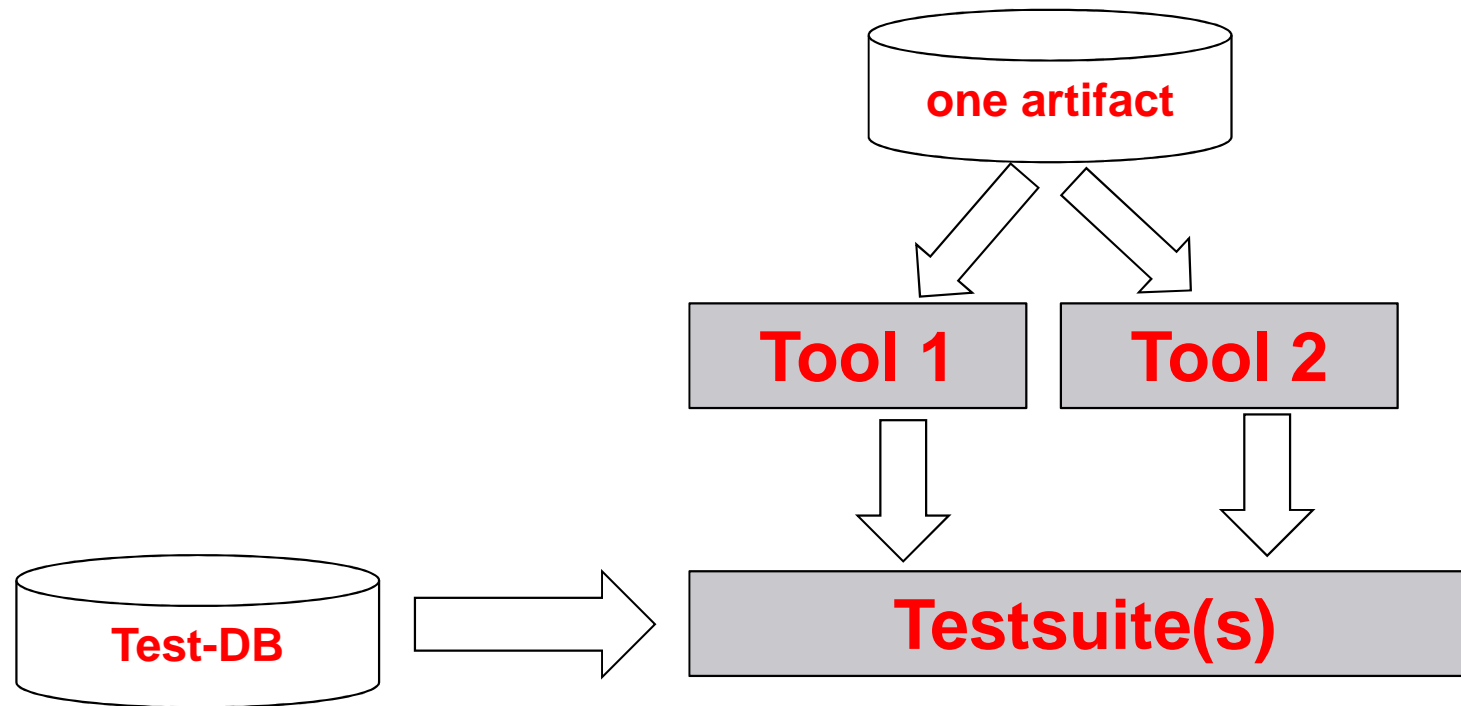
- Using the same artifact as input – clearly defined interface
- Having integrable outputs



- Advantage: Not more effort on artifacts

Principles for artifacts integration (1st VnV level)

Qualification for generated artifacts



- Message Based Tests (Subset-026 chapter 7 & 8 transferability)
- → Tests can contribute to Validation

Gaps in primary model

Top Level: Completing SSRS according to a first set of functions that can feed validation

- Is needed for Verification!

Selection of toolchain

- Selection of stable builds (all tool chain)

Code generator in the toolchain is needed

- If there is no open source code generator, code generated by closed source will be taken for VnV level 1

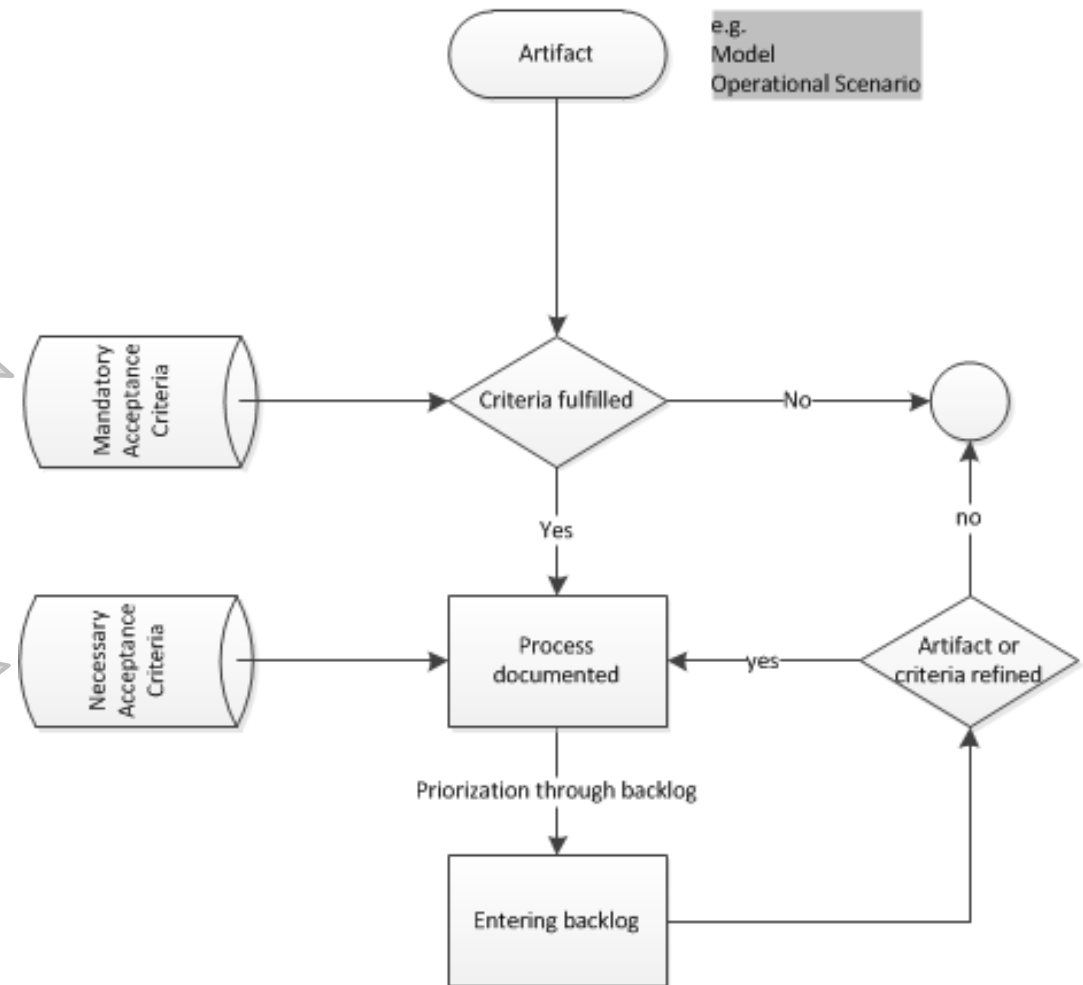
Artifacts decision process

Mandatory criteria

- Model in baseline 3 exists
- Existing interfaces to other VnV tools
- Modularity (D2.6-02-078.1)

Necessary criteria

- Model completeness
- Evaluation from state of the art
- Integration



Results WP7 Tool-Benchmark

- 3.1 Main usage of the approach for which phases do you recommend the approach
 0for which type of activities do you recommend the approach
- 3.2 Language Which are the main characteristics of the language
 0capabilities of the language
- 3.3 System Analysis how the approach can be involved for the sub-system requirement specification
- 3.4.1 Semi-formal model Concerning semi-formal model, how the WP2 requirements are covered ?
 0concerning safety properties management, how the WP2 requirements are covered ?
- 3.4.2 Strictly formal model 0Does the language allow to formalize (D2.6-02-069):
 Concerning strictly formal model, how the WP2 requirements are covered ?
 0Does the language allow to formalize (D2.6-02-070):
 How the approach allows to produce a functional software model of the on-board unit ?
- 3.5.1 Functional design How the approach allows to produce in safety a software model ?
- 3.5.2 SSIL4 design Which criteria for software architecture are covered by the methodology (see EN50128 table A.3) :
 Which criteria for software design and implementation are covered by the methodology (see EN50128 table A.4) :
- 3.6 Software code generation Which task are covered by the tool ?
- 3.7 Main usage of the tool 0
- 3.8 Use of the tool This section discusses how the tool can be classified according EN50128 requirements (D2.6-02-085).
- 3.9 Certifiability

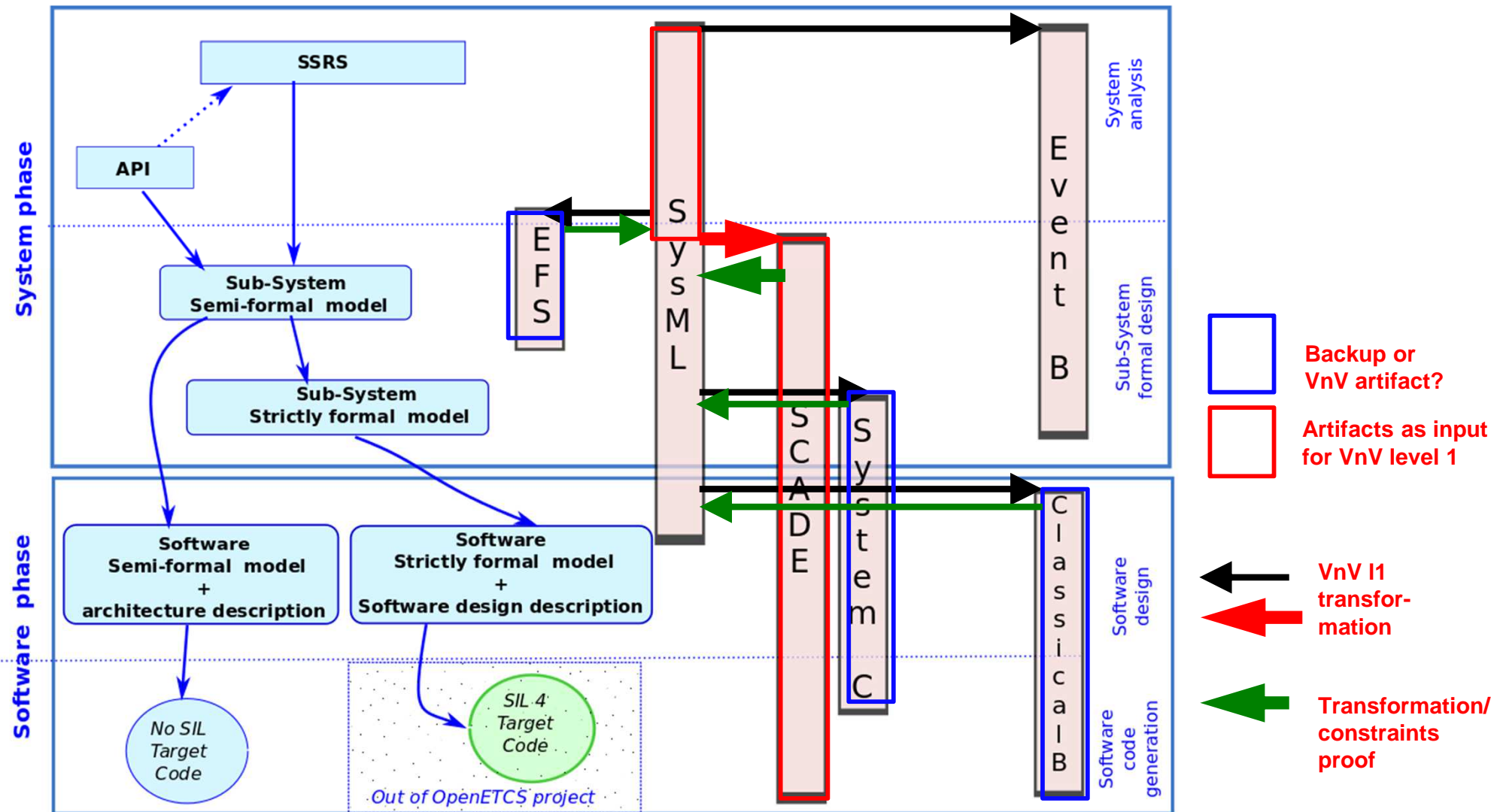
Weight	GOPRR	ERTMSFormalSpecs	SysML with papyrus	SysML with EA	SCADE	EventB	Classical	System	Petri	GNATprove	Semi-Formal	Formal
1	18	0	9	10	18	9	18	15	12	18	1	1
0,1	27	42	39	40	52	50	42	36	47	39	1	1
1	35	54	52	49	56	42	41	46	0	45	1	1
1	57	65	62	74	81	63	73	74	87	81	1	1
1	62	53	58	72	59	69	57	0	63	33	1	1
1	0	94	69	87	0	91	74	68	81	79	1	0
1	0	39	24	35	0	55	54	48	63	50	1	0
1	0	56	33	51	0	51	56	62	54	57	1	0
1	54	0	0	68	86	87	90	0	86	80	0	1
1	45	0	0	47	61	50	56	0	54	57	0	1
0,5	35	0	31	45	39	0	45	37	42	37	0	1
0	35	0	34	67	72	0	72	41	69	58	0	1
0	60	0	33	36	37	0	48	52	44	75	0	1
1	45	0	23	44	52	0	54	39	42	48	0	1
1	33	32	16	34	54	48	50	40	45	45	1	1
1	54	96	104	93	103	107	92	104	74	110	1	1
1	21	27	23	28	57	35	53	24	51	43	1	1
Sum	581	558	610	880	827	757	975	686	914	955		
Weight Sum	444	520	492	719	652	712	795	542	738	768		
Semi Formal	283	520	454	537	433	575	572	485	535	565		
Formal	444	331	366	546	652	515	611	364	540	582		

Expectations to WP7

To develop the VnV Process:

- **Support for consistency of process**
 - Does the process work?
- **Support for tool functionality**
 - Which tasks are supported by the tools?
- **Support for tool integration is needed**
 - Do the tools integrate?
- **Support for artifacts**
 - Do the artifacts trace?

Model Transformation Possible



Primary Model for VnV level 1

SysML/papyrus (High level model)

SCADE (Low level model & Code)

Justification:

SysML:

- agreed on as primary tools for modelling (WP7- Workshop 4.7.2013)

SCADE:

- Best available formal tool and code generation according to WP7 benchmark

- 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

Question round

Back