Decision meeting on primary toolchain

WP7 Task 7.1

Marielle Petit-Doche

4th of July 2013, UIC, Paris

ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

Outline

openETCS

Outline

openETCS

Aim

- Identify the modelling languages
- Identify the modelling tools
- Identify the tool platform (see Block 2)

⇒ **Proposal** : Benchmark of means, tools and tool platform

ITEA reviewers conclusion

- Do not spare time to select methods and tools
- Keep the essential aim in mind

openETCS

Aim

- Identify the modelling languages
- Identify the modelling tools
- Identify the tool platform (see Block 2)

⇒ **Proposal** : Benchmark of means, tools and tool platform

ITEA reviewers conclusion

- Do not spare time to select methods and tools
- Keep the essential aim in mind

openETCS

T7.1 Organisation

- Inputs: WP2 deliverables
  - States of art: D2.1 and D2.2 (and partly D2.4)
  - OpenETCS design process: D2.3
  - Case studies proposal: D2.5
  - OpenETCS requirements: D2.6-9
- Outputs :
  - Set of models: O7.1.1, O7.1.5
  - Criteria template: O7.1.3, O7.1.7, O7.1.9, O7.1.10
  - Selection: O7.1.4, O7.1.8, O7.1.11
  - **Decision : D7.1**
- Key dates for T7.1
  - November 2012: start for first models
  - April 2013: Criteria templates and Spring meeting
  - July 2013: Decision meeting and final report

T7.1 Organisation

- Inputs: WP2 deliverables
  - States of art: D2.1 and D2.2 (and partly D2.4)
  - OpenETCS design process: D2.3
  - Case studies proposal: D2.5
  - OpenETCS requirements: D2.6-9
- Outputs :
  - Set of models: O7.1.1, O7.1.5
  - Criteria template: O7.1.3, O7.1.7, O7.1.9, O7.1.10
  - Selection: O7.1.4, O7.1.8, O7.1.11
  - **Decision : D7.1**
- Key dates for T7.1
  - November 2012: start for first models
  - April 2013: Criteria templates and Spring meeting
  - July 2013: Decision meeting and final report

T7.1 Organisation

- Inputs: WP2 deliverables
  - States of art: D2.1 and D2.2 (and partly D2.4)
  - OpenETCS design process: D2.3
  - Case studies proposal: D2.5
  - OpenETCS requirements: D2.6-9
- Outputs :
  - Set of models: O7.1.1, O7.1.5
  - Criteria template: O7.1.3, O7.1.7, O7.1.9, O7.1.10
  - Selection: O7.1.4, O7.1.8, O7.1.11
  - **Decision : D7.1**
- Key dates for T7.1
  - November 2012: start for first models
  - April 2013: Criteria templates and Spring meeting
  - July 2013: Decision meeting and final report

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

OpenETCS criteria

- Criteria on means and tools for primary toolchain
  around 144
- Key criteria
  - Means and tools for design and modelling
  - From high level SRS specification to software code (non-vital or SIL4 compliant)
  - Open Source approaches
  - Interoperability of means and tools during design process
  - Interoperability with secondary means and tools (VnV, safety, requirement management,...)
  - (Semi-)formal approaches
- Criteria on tool platform (see Block 2)
- Criteria on secondary means and tools (see Block 3)

Outline

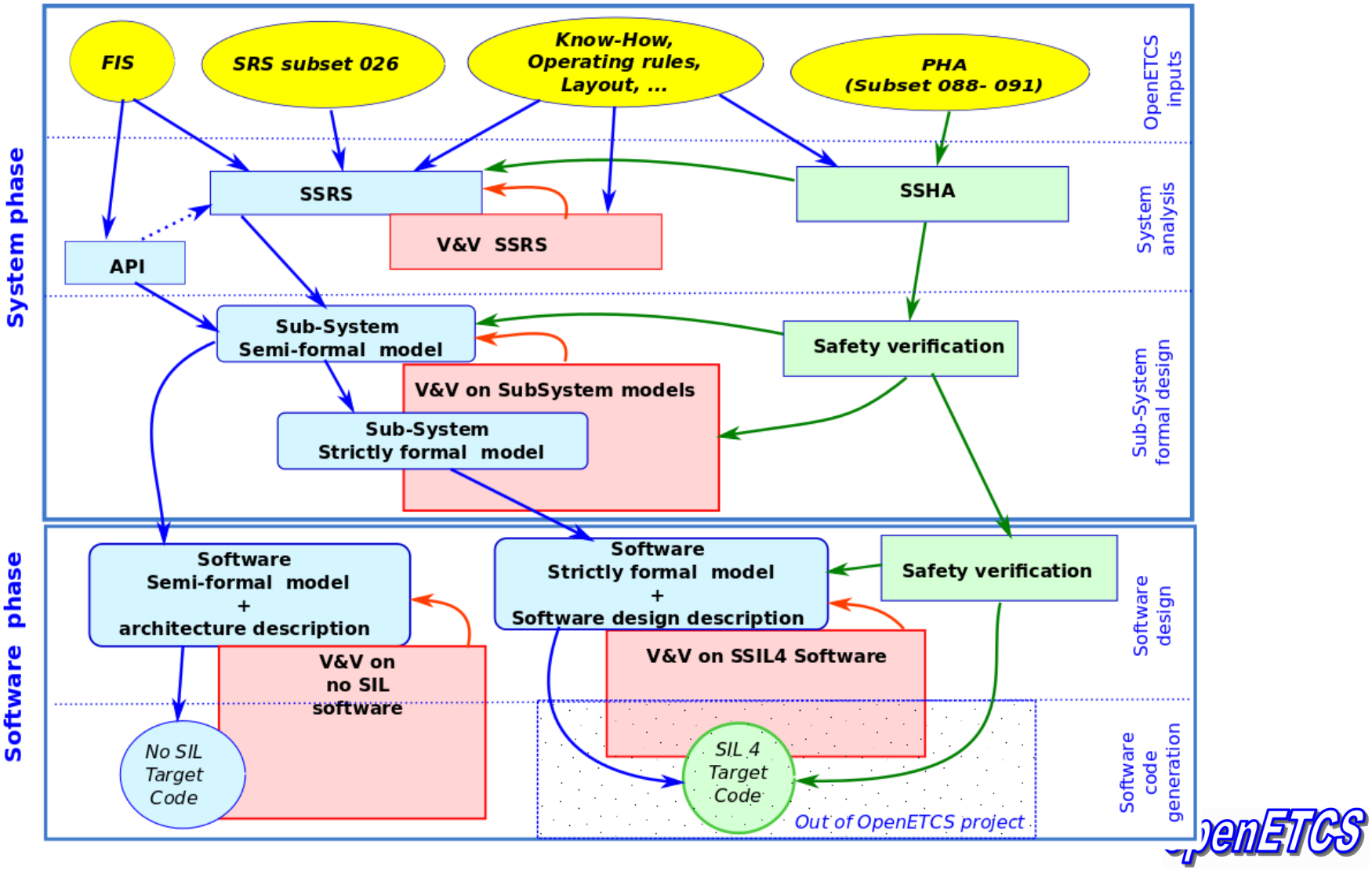
Benchmark activities

- 13 approaches proposed
- 15 partners involved
- Documented models available on github
- Criteria templates fill: O7.1.3-O7.1.7

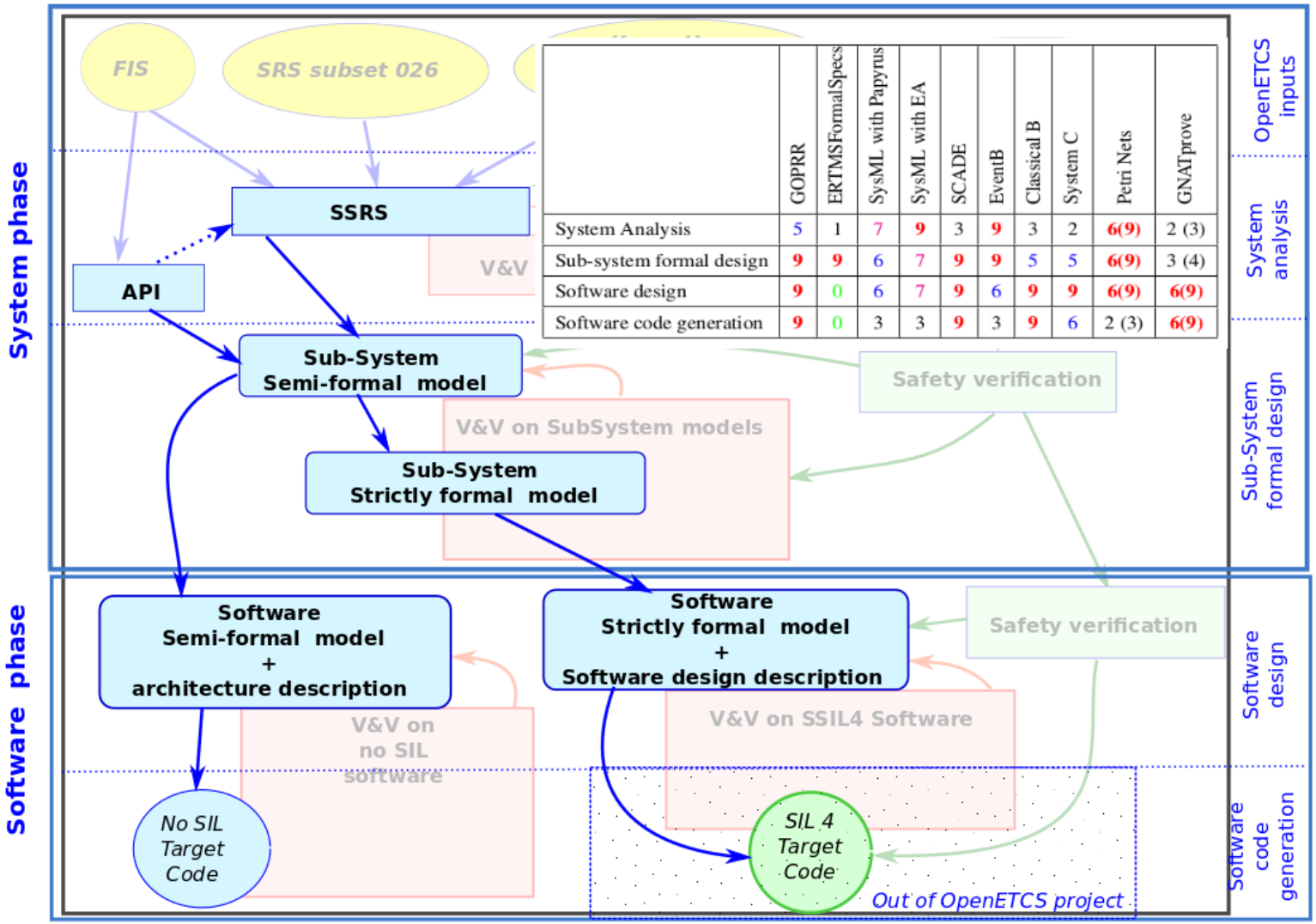
	GOPRR	ERTMSFormalSpecs	SysML with Papyrus	SysML with EA	SCADE	EventB	Classical B	System C	Petri Nets	GNATprove
Documentation	3	7	6	7	8	7	0	0	2 (3)	2 (3)
Modeling	**9**	**9**	**9**	**9**	**9**	**9**	**9**	8	**6(9)**	2 (3)
Design	6	**9**	6	7	**9**	7	8	**9**	5(7)	3 (4)
Code generation	**9**	1	3	4	**9**	3	**9**	5 *	2 (3)	**6(9)**
Verification	0	7	6	3	8	**9**	**9**	4 *	**6(9)**	**6(9)**
Validation	0	**9**	5	4	8	**9**	4	7	**6(9)**	**6(9)**
Safety analyses	0	0	4 *	6	1	6	3	3 *	5(7)	2(3)

openETCS

OpenETCS Design Process



Benchmark results (2)



	GOPRR	ERTMSFormalSpecs	SysML with Papyrus	SysML with EA	SCADE	EventB	Classical B	System C	Petri Nets	GNATprove
System Analysis	5	1	7	9	3	9	3	2	6(9)	2 (3)
Sub-system formal design	9	9	6	7	9	9	5	5	6(9)	3 (4)
Software design	9	0	6	7	9	6	9	9	6(9)	6(9)
Software code generation	9	0	3	3	9	3	9	6	2 (3)	6(9)

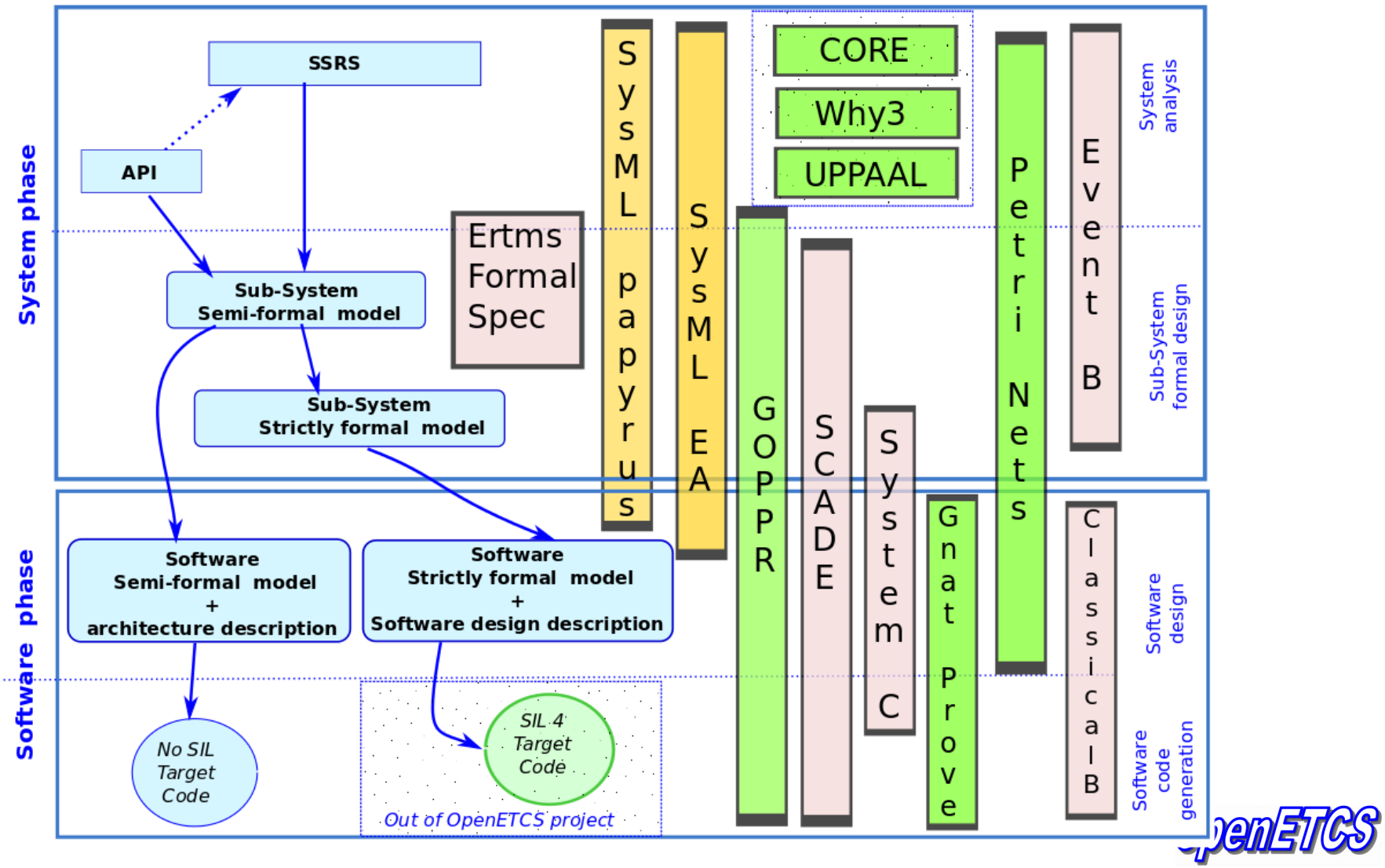
Benchmark results

	GOPRR	ERTMSFormalSpecs	SysML with Papyrus	SysML with EA	SCADE	EventB	Classical B	System C	Petri Nets	GNATprove
Documentation	3	7	6	7	8	7	0	0	2 (3)	2 (3)
Modeling	**9**	**9**	**9**	**9**	**9**	**9**	**9**	8	**6(9)**	2 (3)
Design	6	**9**	6	7	**9**	7	8	**9**	5(7)	3 (4)
Code generation	**9**	1	3	4	**9**	3	**9**	5 *	2 (3)	**6(9)**
Verification	0	7	6	3	8	**9**	**9**	4 *	**6(9)**	**6(9)**
Validation	0	**9**	5	4	8	**9**	4	7	**6(9)**	**6(9)**
Safety analyses	0	0	4 *	6	1	6	3	3 *	5(7)	2(3)

openETCS

Outline

Overview


System phase
Software phase
SSRS
API
Sub-System
Semi-formal model
Sub-System
Strictly formal model
Ertms
Formal
Spec
SysML papyrus
SysML EA
CORE
Why3
UPPAAL
GOPPR
SCADE
System C
Gnat Prove
Petri Nets
Event B
Classical B
System analysis
Sub-System formal design
Software design
Software code generation
Software
Semi-formal model
+
architecture description
Software
Strictly formal model
+
Software design description
No SIL
Target
Code
SIL 4
Target
Code
Out of OpenETCS project

Outline

CORE

- Proposed by All4Tec
- Approach and tool suitable for system analysis
- Evaluation stopped:
  - close source tools
  - difficulties to integrate the approach in the project
  - mising of inputs for this approach (operational rules)

Why3

- Proposed by MERCE
- Platform for deductive program verification
- Evaluation stopped:
  - GnatProve is more efficient to cover the same topics

GOPPRR

- Proposed by Uni. Bremen
- Domain specific language allowing definition of meta-models
- University of Bremen is currently more in favour of SysML based approach (Munich meeting)

Color Petri Nets

- Proposed by Uni. Braunschweig
- Formal notation, supported by various formal analysis mechanisms
- No model provided, Uni. Baunschweig proposes to discharged it

Outline

UPPAAL

- Proposed by TwT gmbh
- Tools for verification and validation of real-time properties
- Moved to the benchmark of tools for VnV

Gnat-Prove

- Proposed by MERCE
- Tools for formal verification on Ada code
- Moved to the benchmark of tools for VnV

Outline

One approach - two tools

- A standardized approach SysML
- Two tools proposed:
  - Papyrus (CEA/All4Tec/Fraunhofer)
  - Entreprise Architect (Uni. of Bremen)
- Exchanged of models between the tools seems difficult

Can we select only one tool now ?

One approach - two tools

- A standardized approach SysML
- Two tools proposed:
  - Papyrus (CEA/All4Tec/Fraunhofer)
  - Entreprise Architect (Uni. of Bremen)
- Exchanged of models between the tools seems difficult

Can we select only one tool now ?

Pros - Cons

Papyrus

+ EPL license
+ Eclipse platform
+ Interoperability
+ Active community
+ Modular architecture
- Poor with analysis tools
- SysML 1.2
- Diagrams
- GUI

Entreprise Architect

+ GUI
+ Diagrams
+ SysML 1.3
+ Stable tool
+ Analysis tools
- Proprietary licence
- Poorly adaptive
- Only on windows

Decision: all partners agree to keep only Papyrus

Pros - Cons

Papyrus

+ EPL license
+ Eclipse platform
+ Interoperability
+ Active community
+ Modular architecture
- Poor with analysis tools
- SysML 1.2
- Diagrams
- GUI

Entreprise Architect

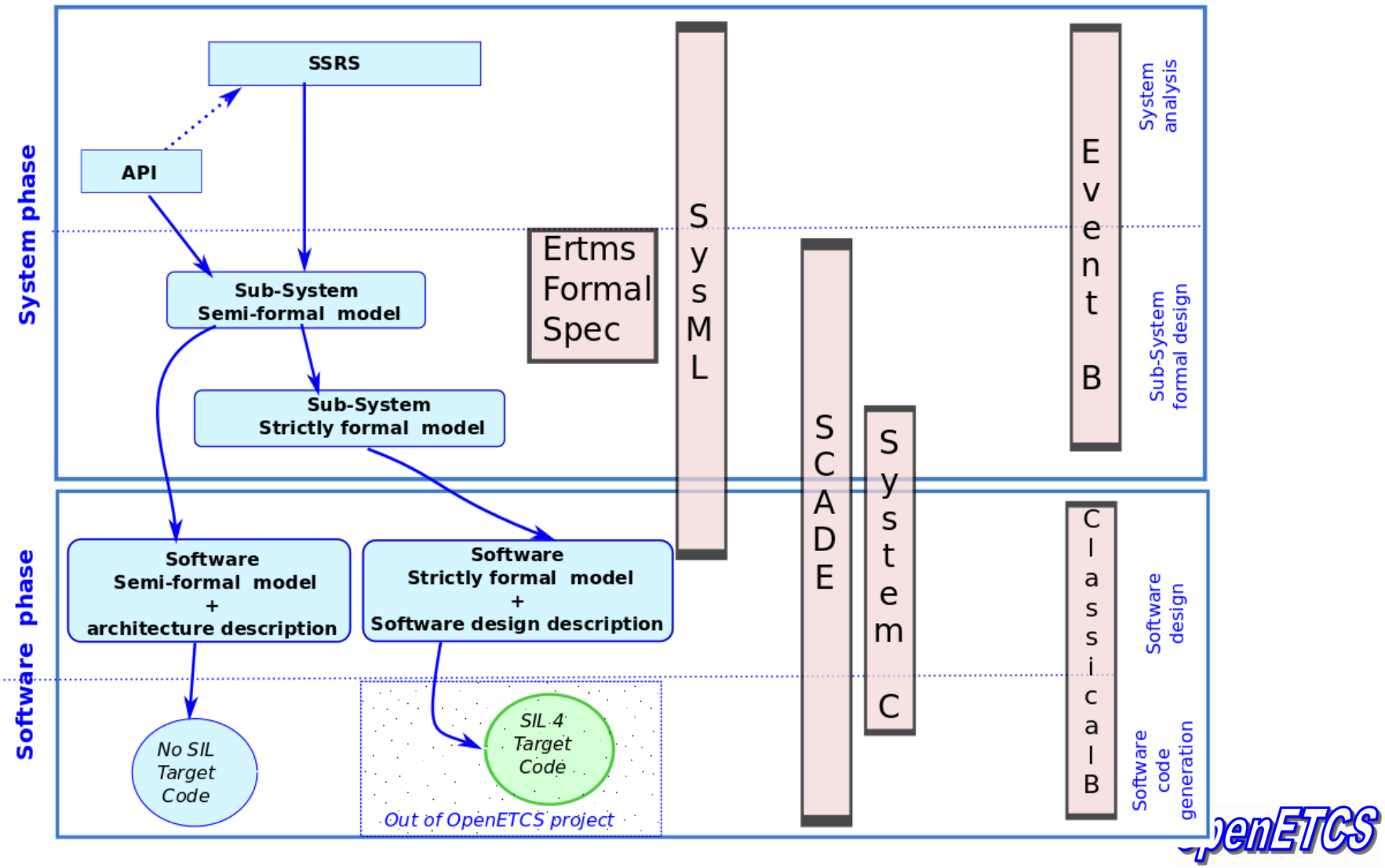
+ GUI
+ Diagrams
+ SysML 1.3
+ Stable tool
+ Analysis tools
- Proprietary licence
- Poorly adaptive
- Only on windows

Decision: all partners agree to keep only Papyrus

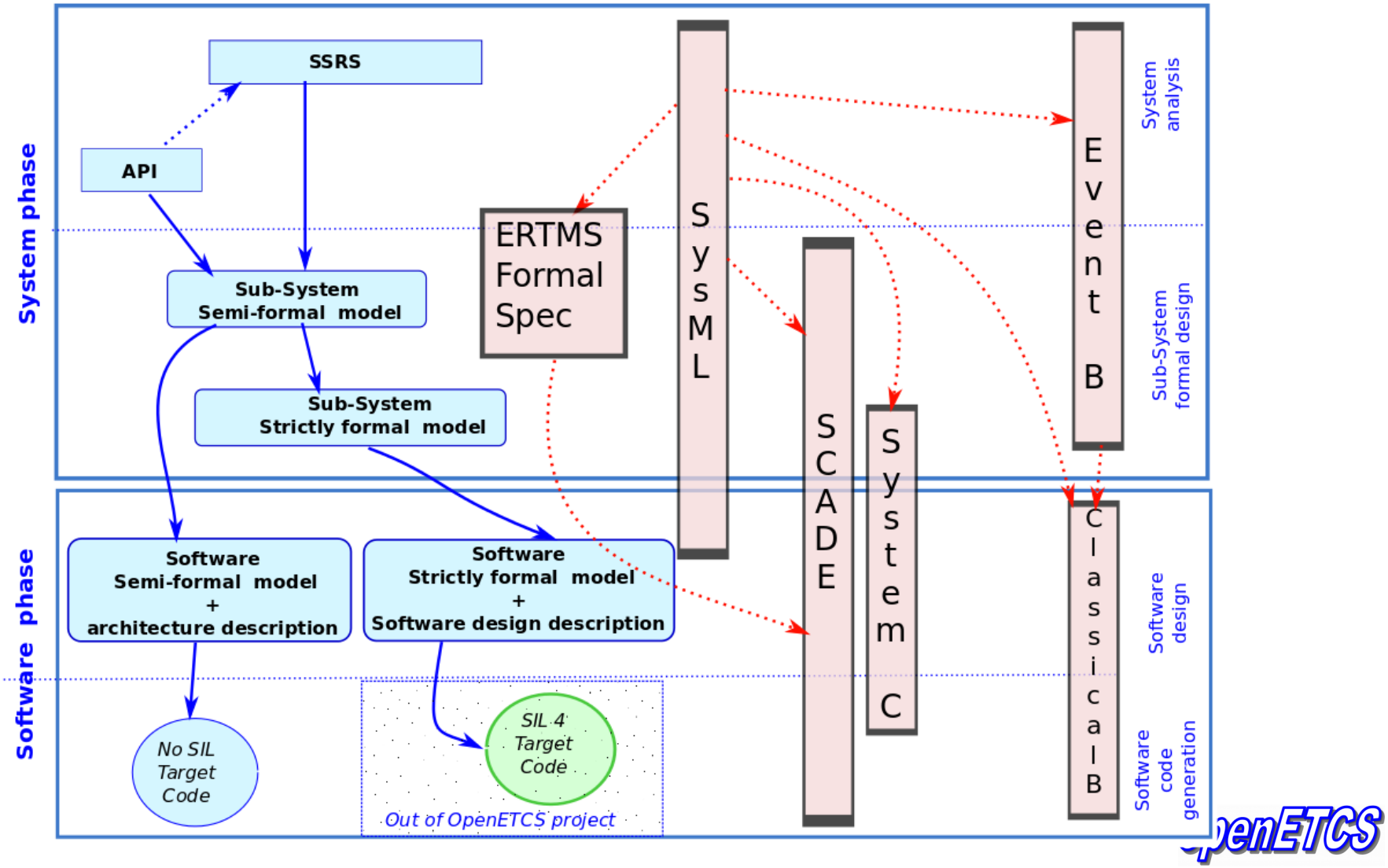
openETCS

Outline

Overview


System phase
SSRS
API
Sub-System
Semi-formal model
Sub-System
Strictly formal model
Ertms
Formal
Spec
SysML
SCADE
System C
Event B
System analysis
Sub-System formal design
Software phase
Software
Semi-formal model
+
architecture description
Software
Strictly formal model
+
Software design description
No SIL
Target
Code
SIL 4
Target
Code
Out of OpenETCS project
Classical B
Software design
Software code generation

Interactions



Items for open Discussions

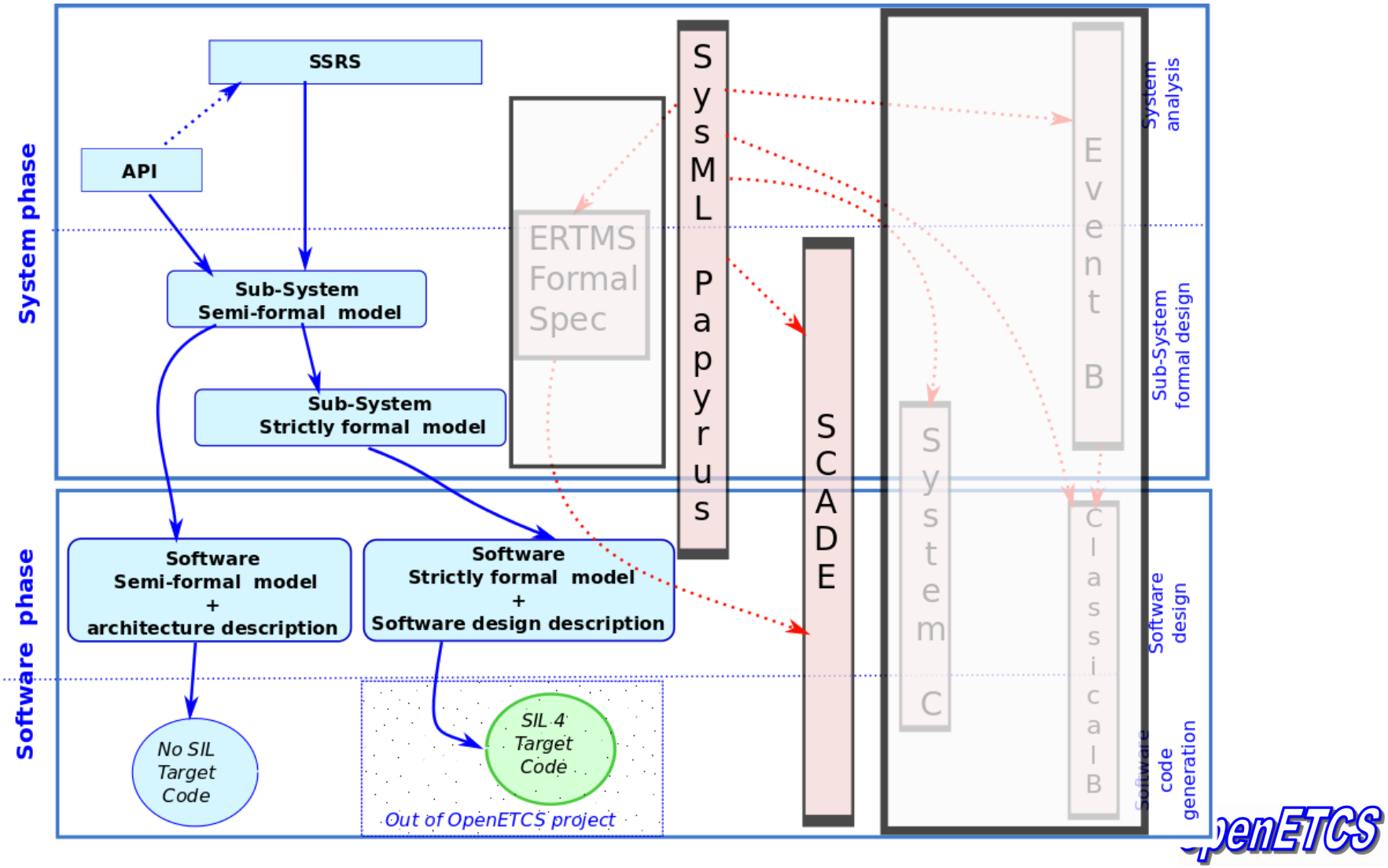
- Open source approach ?
- Approach easy to integrate in the toolchain ?
- End-user point of view (railway operators and industrials, modellers, VnV responsible, safety responsible,..) ?
- Cooperation between approaches ?
- . . .

Outline

Discussion

- open discussion
- decision ?

First proposal



Open questions

- How to use SysML and SCADE during the process (vertical integration) (WP2-WP7) ?
- How to integrate the approaches on the whole process (VnV, Safety,...) (horizontal integration) (WP2-WP4) ?
- Close property (WP1-WP7) ?
- Integration of Scade on eclipse tool platform (WP7) ?
- Who has knowledge to made effort on modelling with these approaches (WP3) ?
- Who has knowledge to made effort on VnV, safety,... around these approaches (WP4) ?
- Who has knowledge to participate to the development of the tool chain on these approaches (WP7) ?

openETCS

Back-up approaches

- ERTMS Formal Spec (Bracking curves + VnV)
- System C (VnV)
- Classical B (VnV)
- Event B (VnV and Safety analysis)