



# AMASS

Architecture-driven, Multi-concern and Seamless Assurance and  
Certification of Cyber-Physical Systems

## WP6 Cross and Intra Domain Reuse Progress and Achievements

First EAB Workshop  
Trento, 11 September, 2017

Barbara Gallina, Ph.D.  
WP6 Leader, T6.1-2 Leader, TM

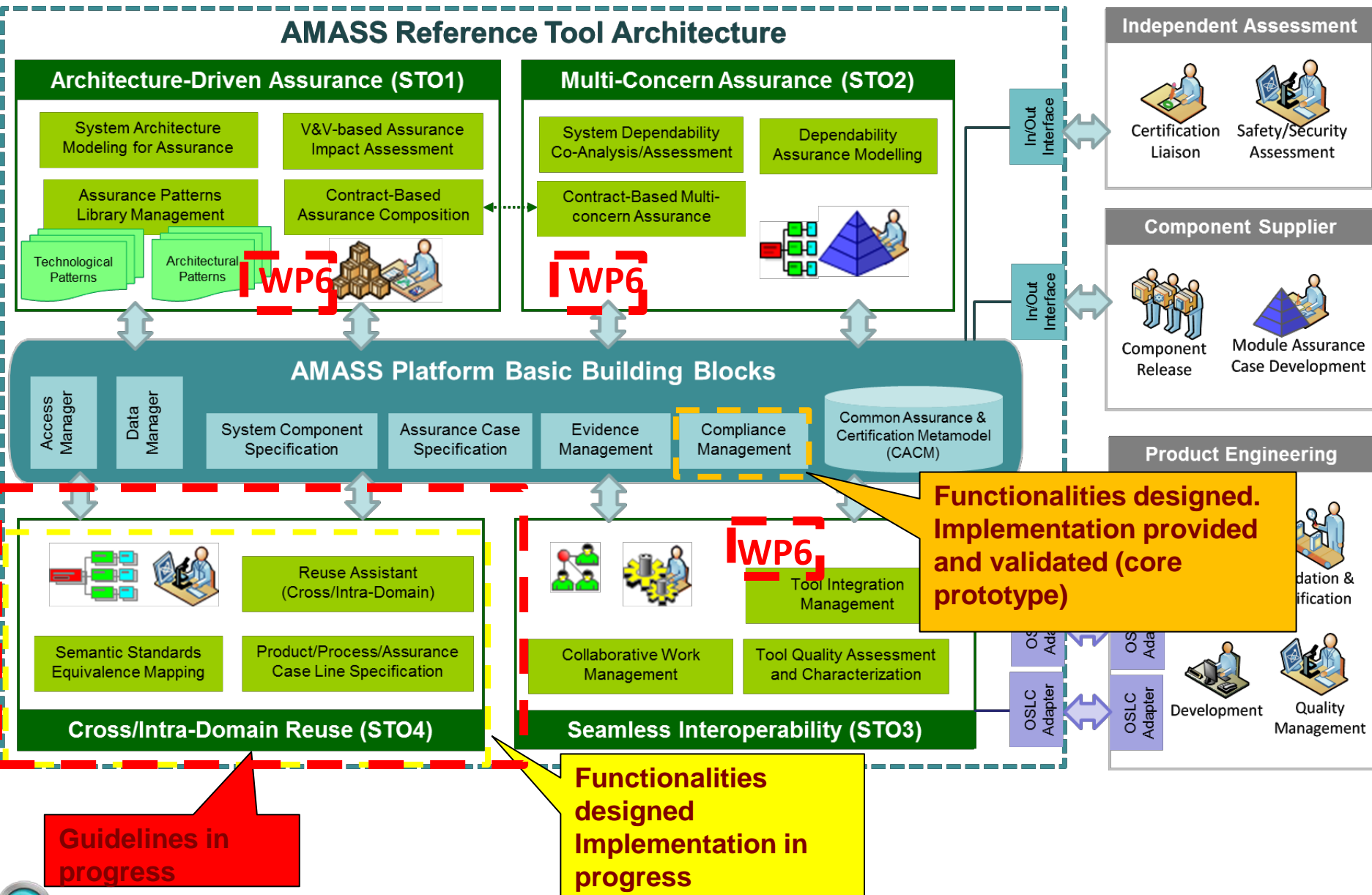


## Modelling and methodological capabilities for cross and intra domain reuse + compliance management

### Main specific objectives:

1. Investigation and provision of tool-supported **modelling capabilities** aimed at enabling **systematization and reuse of commonalities and variabilities** in terms of process-product-and-argumentation elements.
2. Investigation and provision of tool-supported **ontology-based methods** aimed at enabling the semantic mapping between the standards.
3. Investigation and provision of tool-supported **modelling capabilities** aimed at enabling **semi-automatic generation** of certification artifacts.
4. Investigation of **metrics** aimed at quantifying the increased efficiency via reuse and automatic-generation.
5. **Demonstration** of the reuse of assurance results.
6. Consolidation and integration of previous work on **compliance management**.

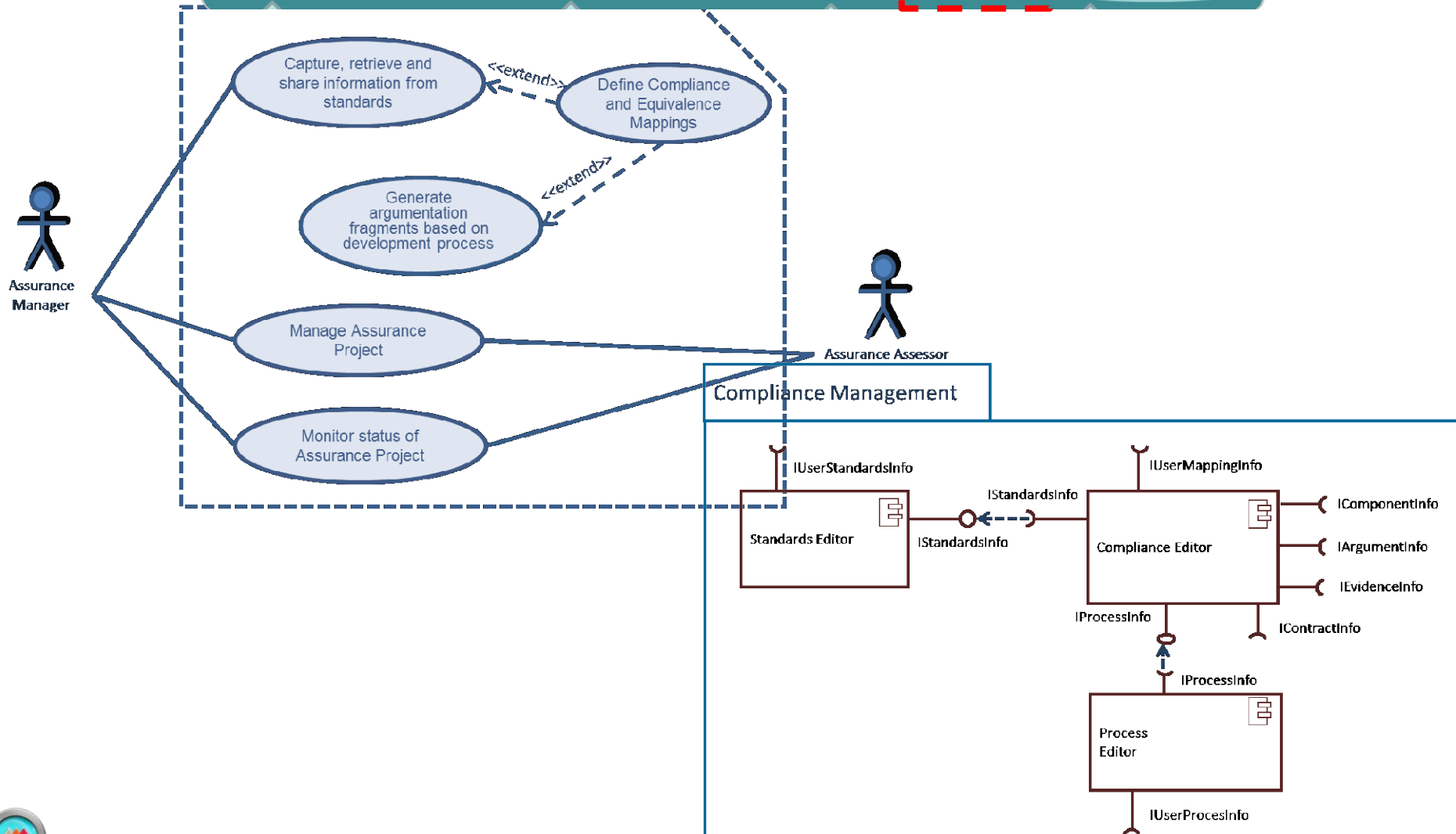
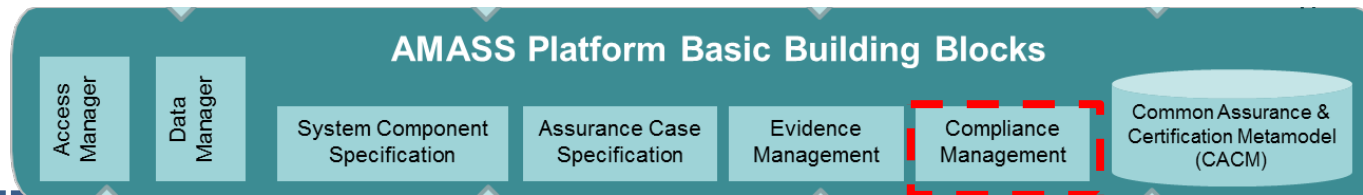
# AMASS Reference Tool Architecture: WP6 Scope

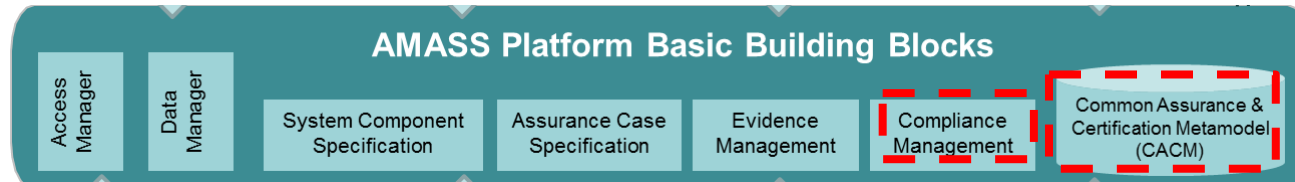


# WP6 – ARTA functionalities to achieve STO4 ++

- **Prototype Core**
  - **Compliance Management**
    - **Standards modelling for Compliance Management**
    - **Process Modelling for Compliance Management**
      - **Capability Patterns for Compliance Management**
        - » **Interaction between Capability Patterns and Compliance Management/Assurance**
    - **Compliance management: Process and standards mapping**
- **Prototype 1**
  - Systematization
  - Mapping
  - Reuse assistant
  - Compliance Management (formal)

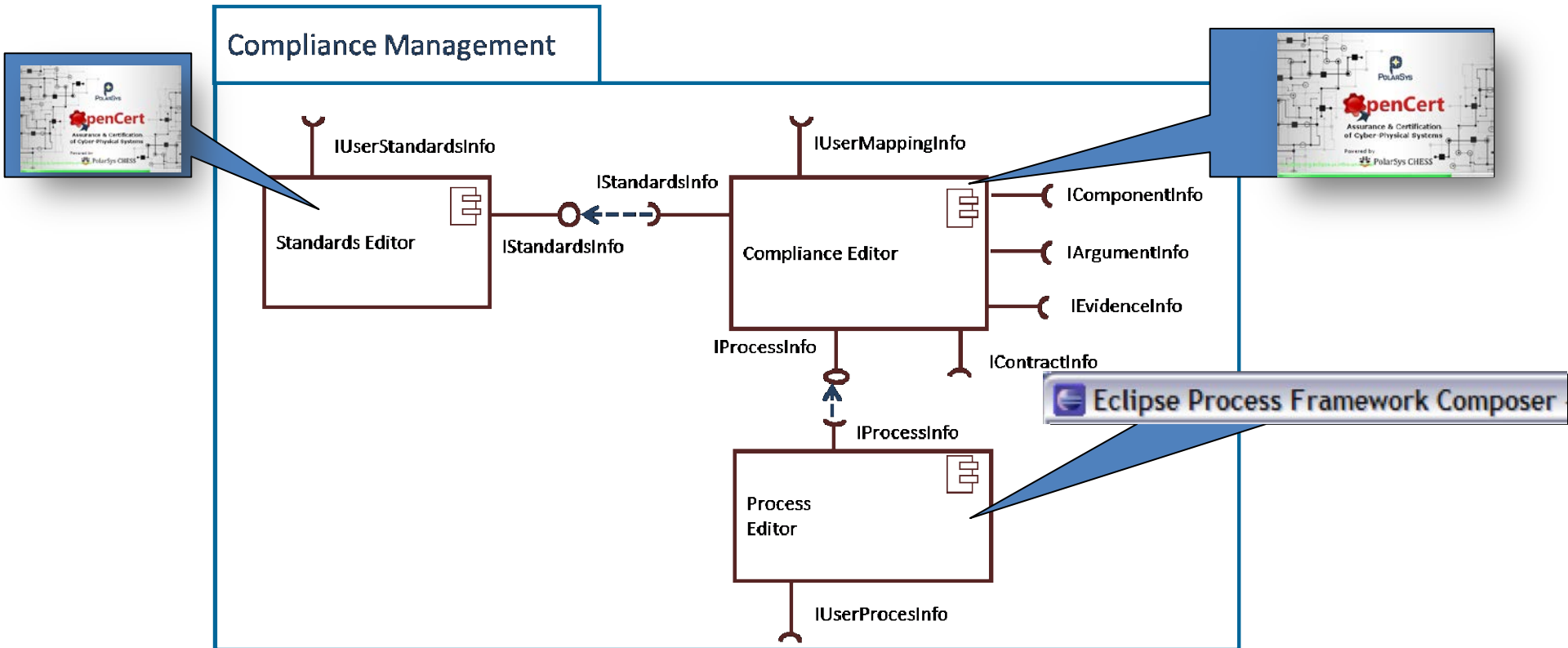
# WP6: Prototype Core Functionalities





- SafeCer EPF Composer-based approach has been integrated
  - CACM includes UMA/SPEM2.0
  - A model transformation has been implemented
- OPENCROSS OpenCert-based approach has been merged

# WP6: Core Prototype Tools Interplay



# WP6 – ARTA functionalities to achieve STO4 ++

- Prototype Core
  - Compliance Management
    - Standards modelling for Compliance Management
    - Process Modelling for Compliance Management
    - Compliance management: Process and standards mapping
- **Prototype P1**
  - **Systematization**
    - **Variability Management for Cross and Intra Domain reuse**
      - Process
      - Assurance Case
      - Product, including variability management of contexts
  - **Mapping**
    - **Semantics-based mapping of equivalent standards**
  - **Reuse assistant**
    - **Syntax-based mapping of equivalent standards**
  - **Compliance Management (formal)**



# WP6: Cross and Intra Domain Reuse



## Reuse Scenarios

**Cross-Concern**

**Cross-Domain**

**Intra-Domain**

**Cross-Systems  
(COTS)**

**Cross-Systems  
(SEooC-like)**

**Product  
Upgrade**



## Reusable Assets

**Compliance  
Checks**

**Artefacts**

**Activities**

**Requirements**

**Design**

**Code**

**Arguments**



## Tooling Needs

**Reuse  
Assistant**

**Reuse  
Discovering**

**Assets  
Management**

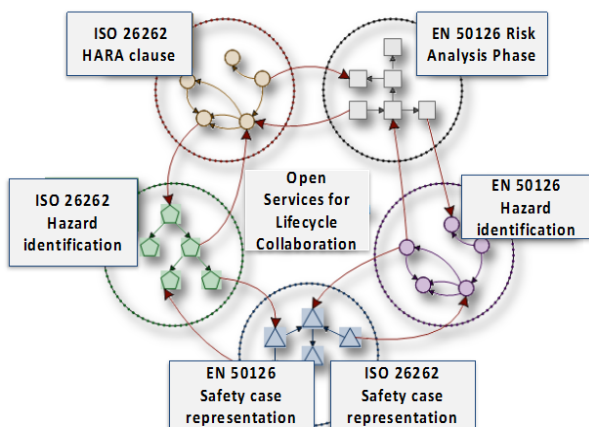
**Impact  
Analysis**

**Traceability**

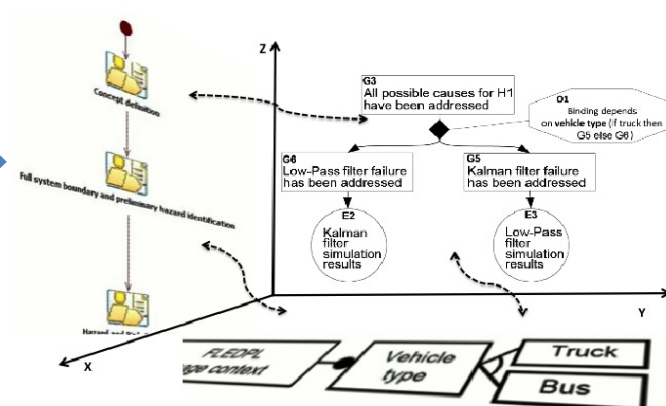
# WP6-STO4: Functionalities Interplay



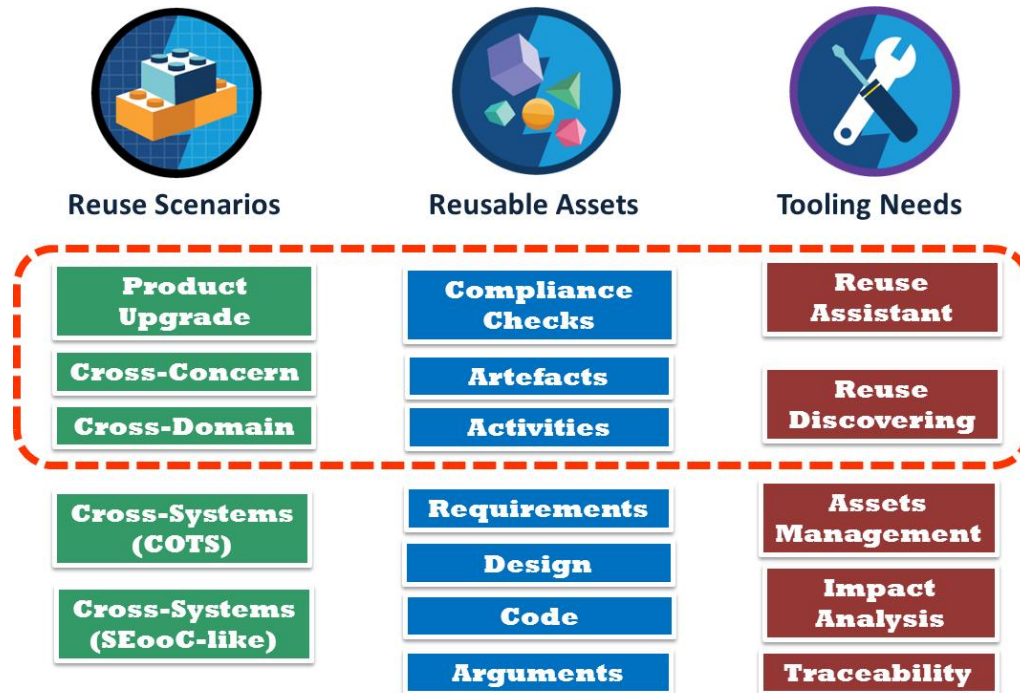
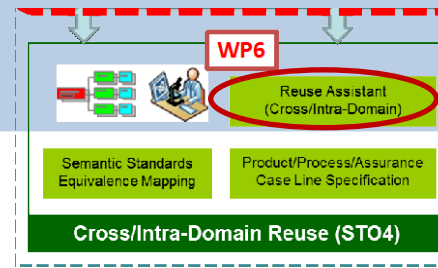
From Scratch



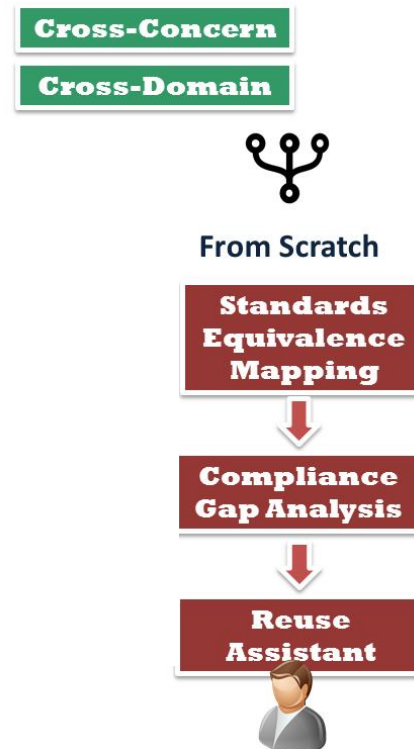
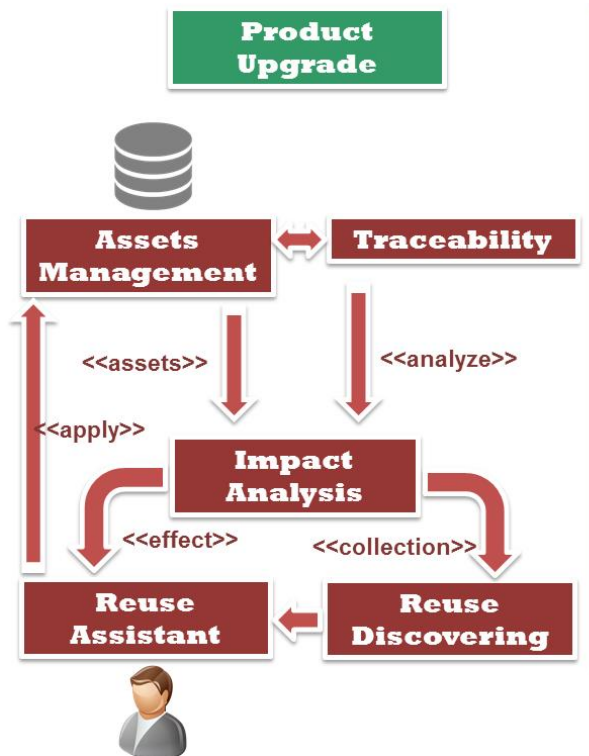
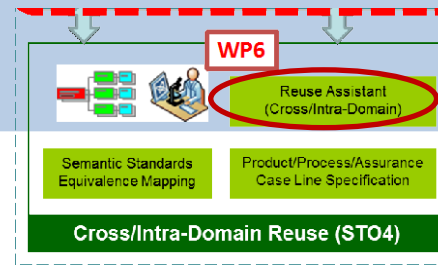
Systematization of commonalities and variabilities within and between families of Processes/Products/Assurance Cases



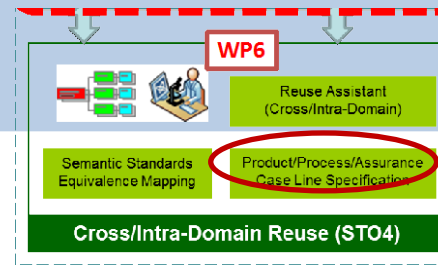
# Reuse Assistant



# Reuse Assistant



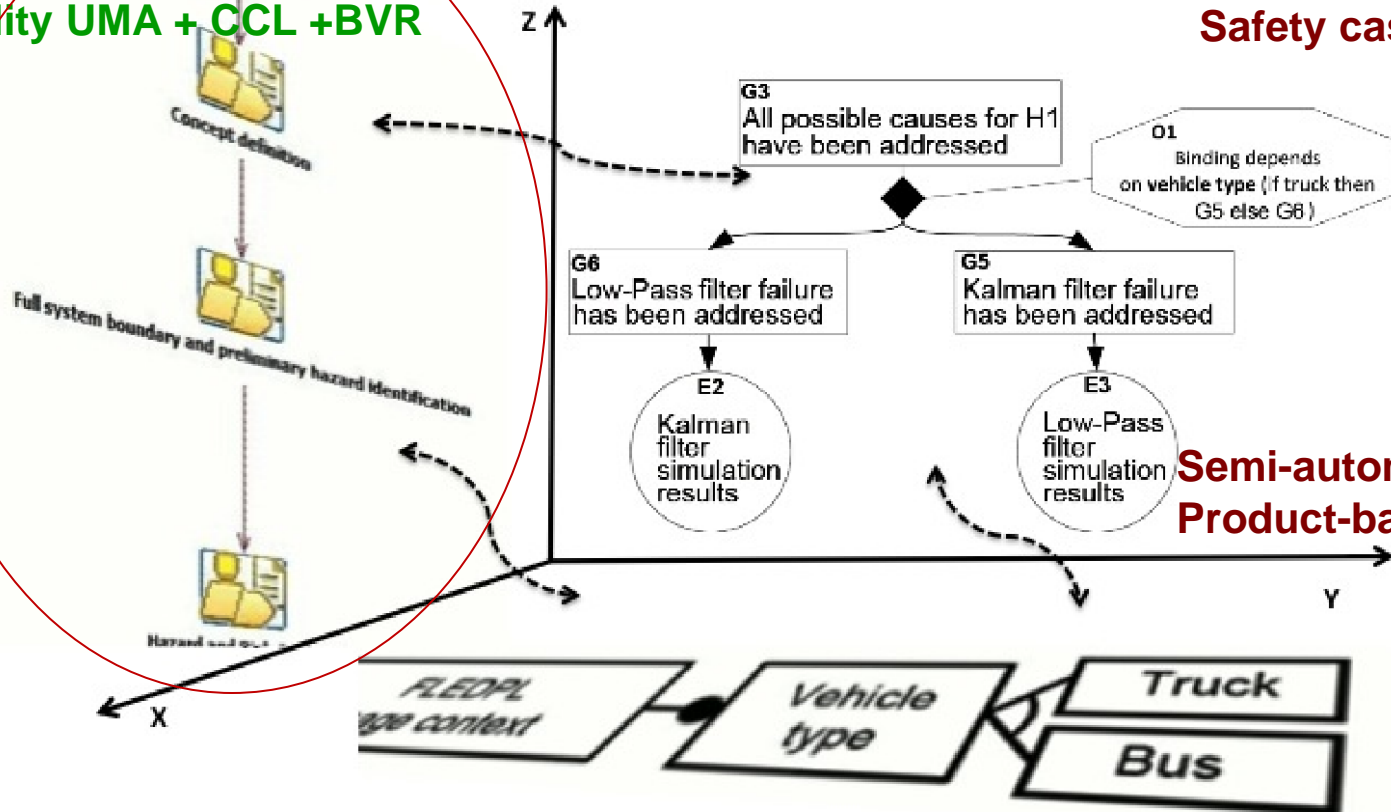
# Anti-Sysphus



**Semi-automatic generation of Process-based arguments**

**SACM ++  
Patterns  
Safety case lines**

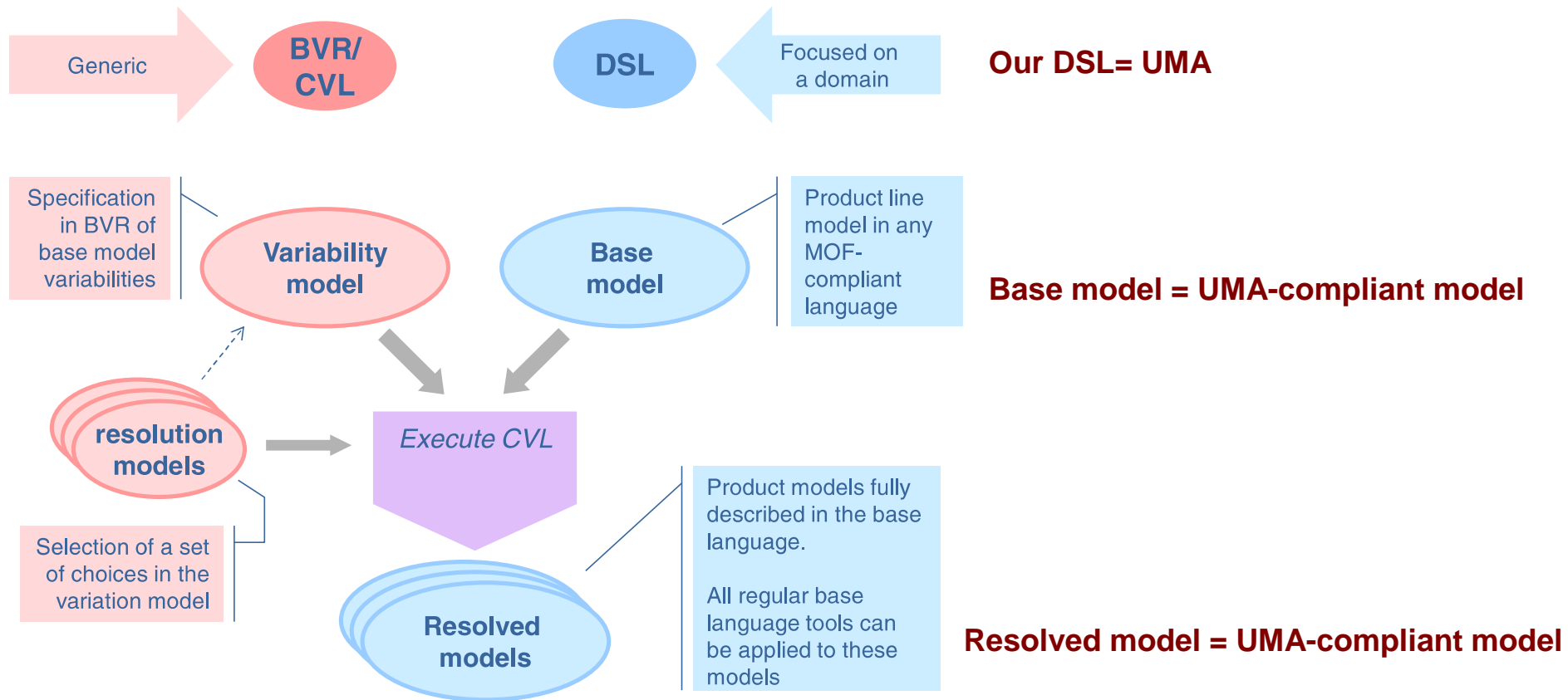
**SPEM2.0/UMA+  
Reality UMA + CCL +BVR**



**Semi-automatic generation of Product-based arguments**

# Process Reuse via EPF Composer & BVR Tool

## Modelling variability as an orthogonal separate model



# Process Reuse via EPF Composer & BVR Tool

software\_design\_and\_implementation\_engineering\_process

Presentation Name	Index	Predecessors	Model Info	Type	Planned	Repeatable	Multiple Occurrences	Ongoing	Event-Driven	Optional
Software Design and Implementation Engineering Process	0			Capability Pattern	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Design of software items	1			Phase	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Detailed the design of each software component	2			Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Develop and Document software interfaces	6			Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Produce the detail design model	8			Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Detail software design method	10			Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Detail Design of real-time software	12			Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Describe Software Behaviour	18			Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Determine design method consistency for real time	20			Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Space\_Engineering : BVRModel

ECSS\_E\_ST\_40C

Software\_design\_and\_implementation\_engineering\_process  
"S.5"

Criticality

(+) SUIPT  
"Software [unit/integration] test plan"

Space\_Engineering.bvr (VSpec)

Space\_Engineering.bvr (Resolution)

ECSS\_E\_ST\_40C[0]

ECSS\_E\_ST\_40C = true

Software\_design\_and\_implementation\_engineering\_process = true

Criticality = true

(+) SUIPT = true

(+) Design\_of\_software\_items = true

(+) Coding\_and\_testing = true

Integration = true

A = false

B = false

C = false

D = true

Develop\_software\_integration\_test\_plan = true

Integrate\_and\_test\_software\_units\_and\_components = true

Test\_plan = true

Integration\_and\_testing\_software\_units = true

New

Rename

Remove

Validate

Calculate Covarege

Export As PNG

Show/Hide Grouping

Show/Hide Constraints

Execute

Message

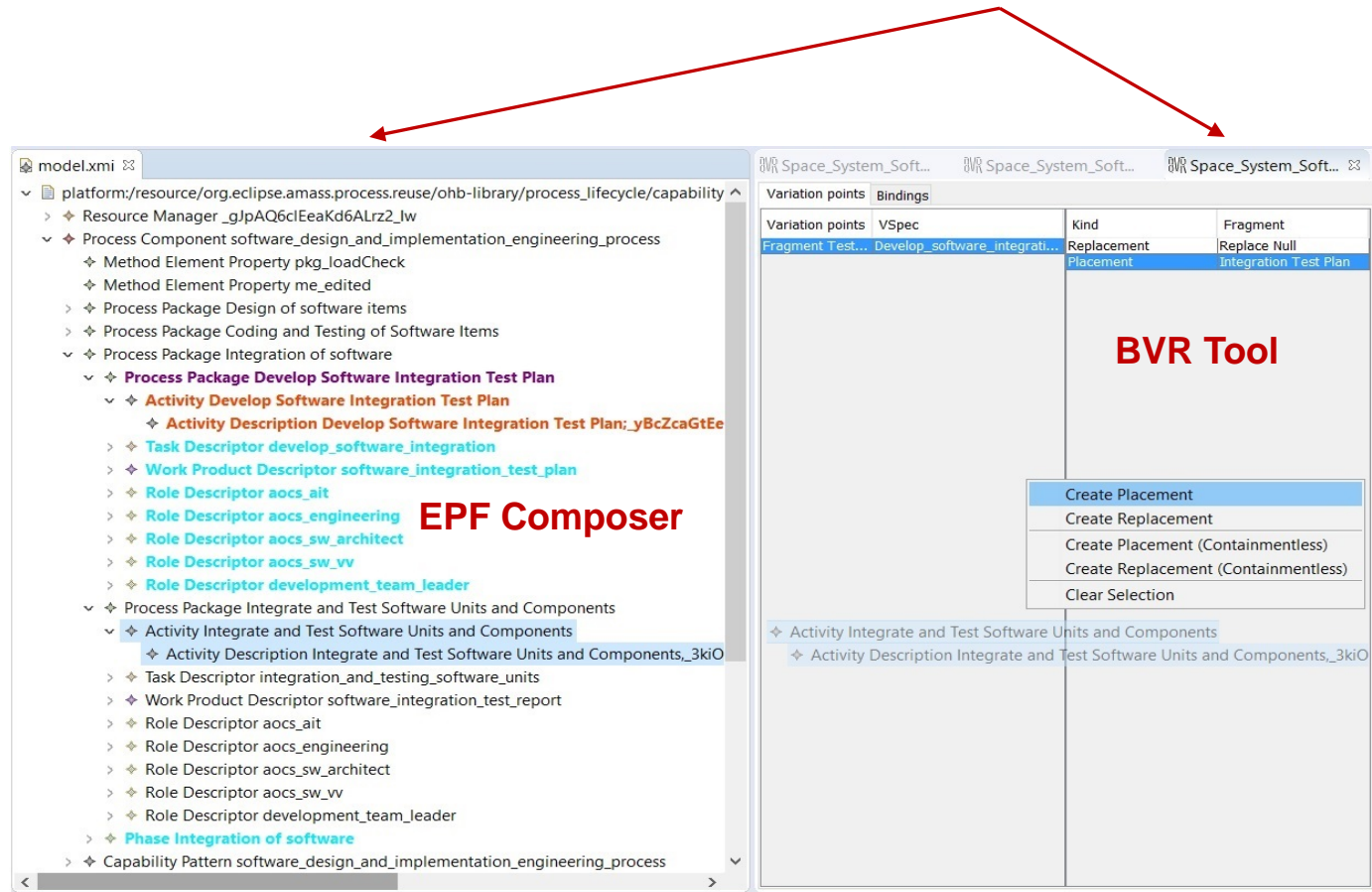
Valid: true []

OK



# Process Reuse via EPF Composer & BVR Tool

## Bind between model(s) using fragments

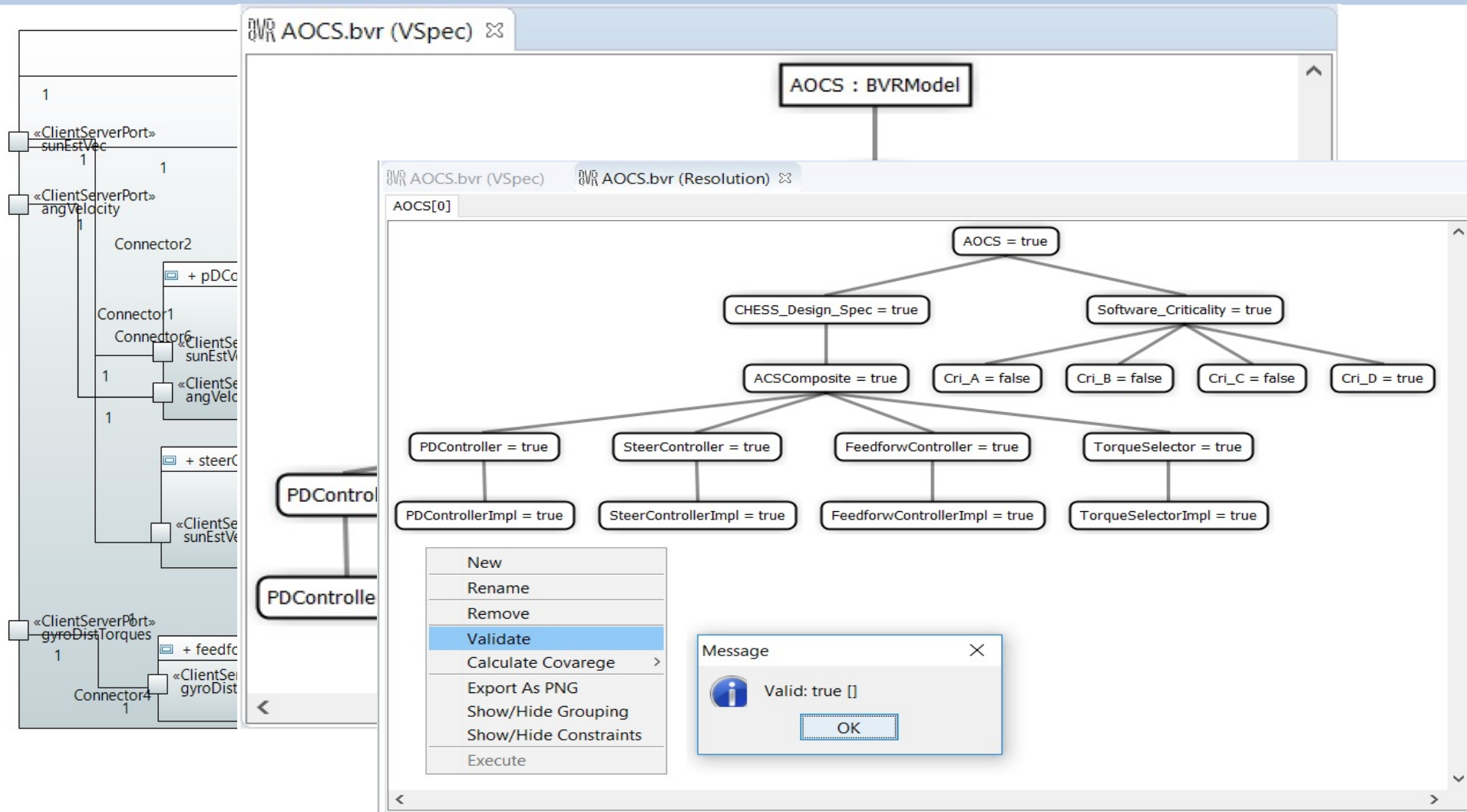


## UC11: Initial exploration of an intra domain (space) SoPLE

**UC3: Initial exploration of an intra domain automotive SiSoPLE, focused on ISO 26262 and SAE J3061**

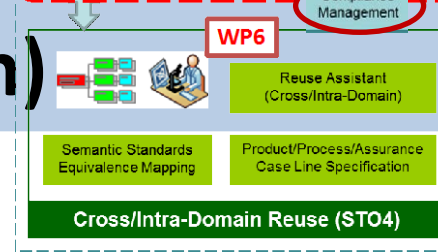


# Product Reuse via CHES & BVR Tool



**[System description modelled in a paper to be presented at ICRE-2017]**

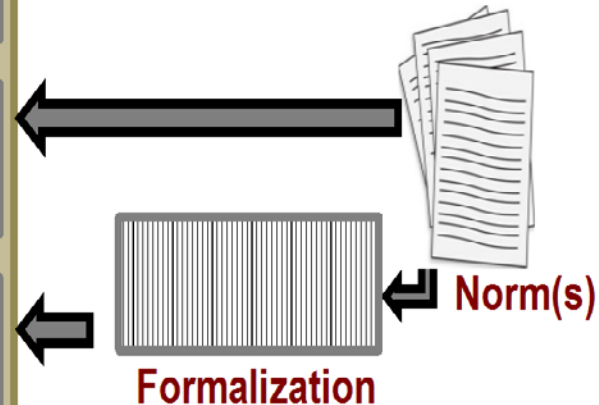
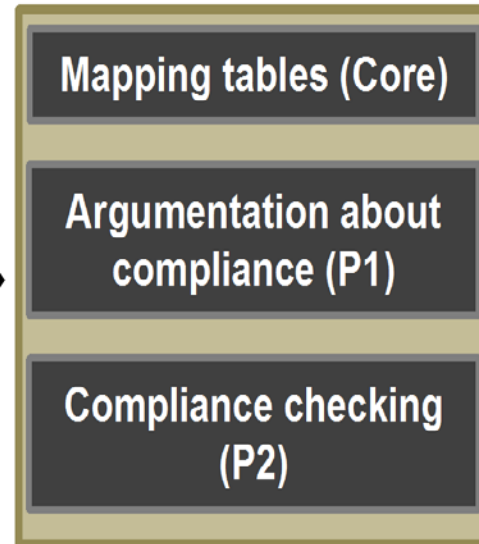
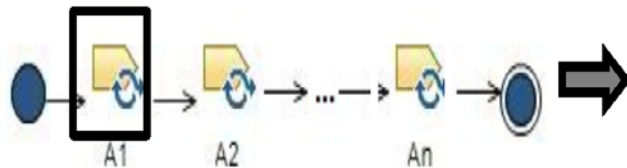
# Compliance management (global vision)



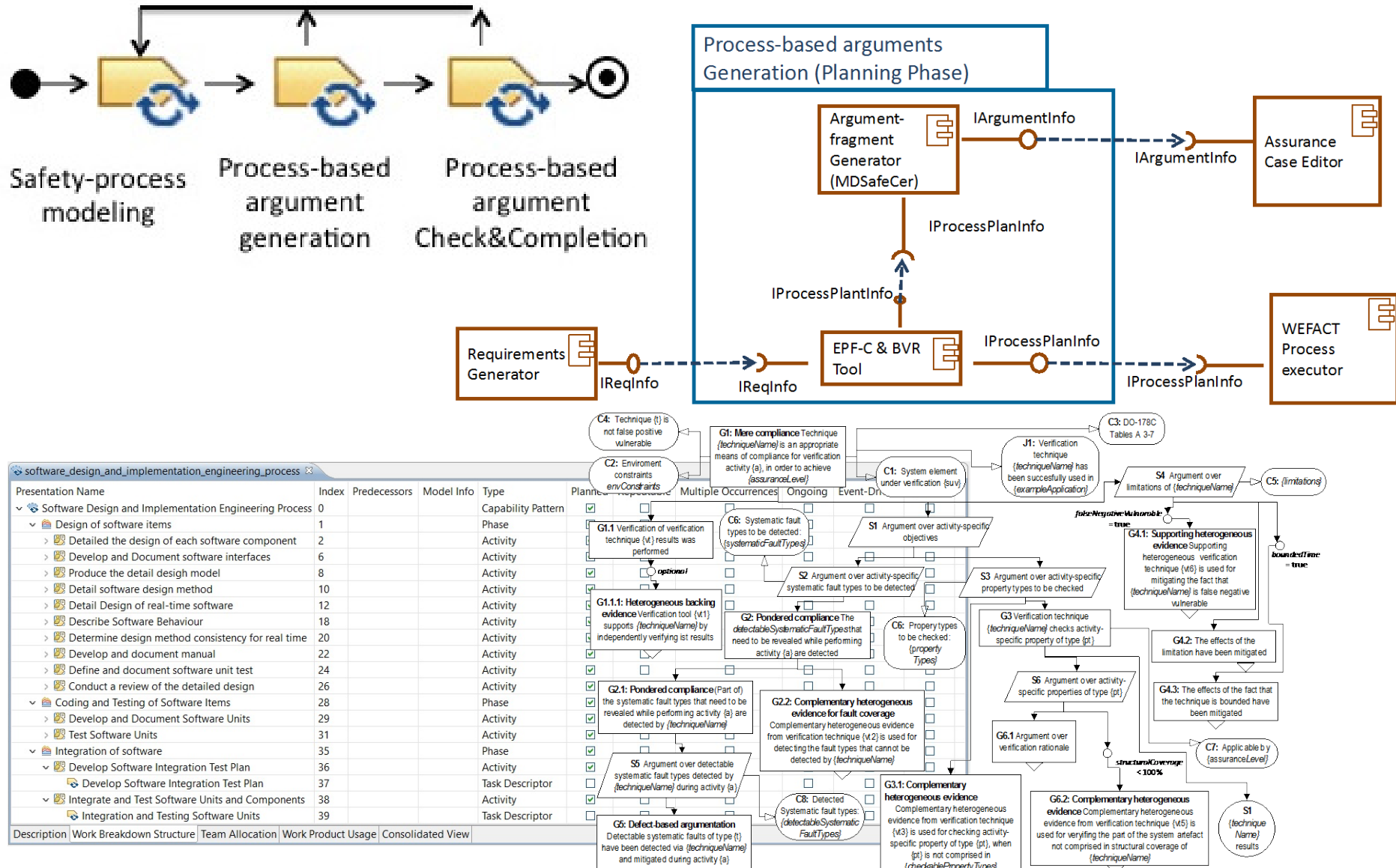
Process Space

Normative Space

Process Model(s)

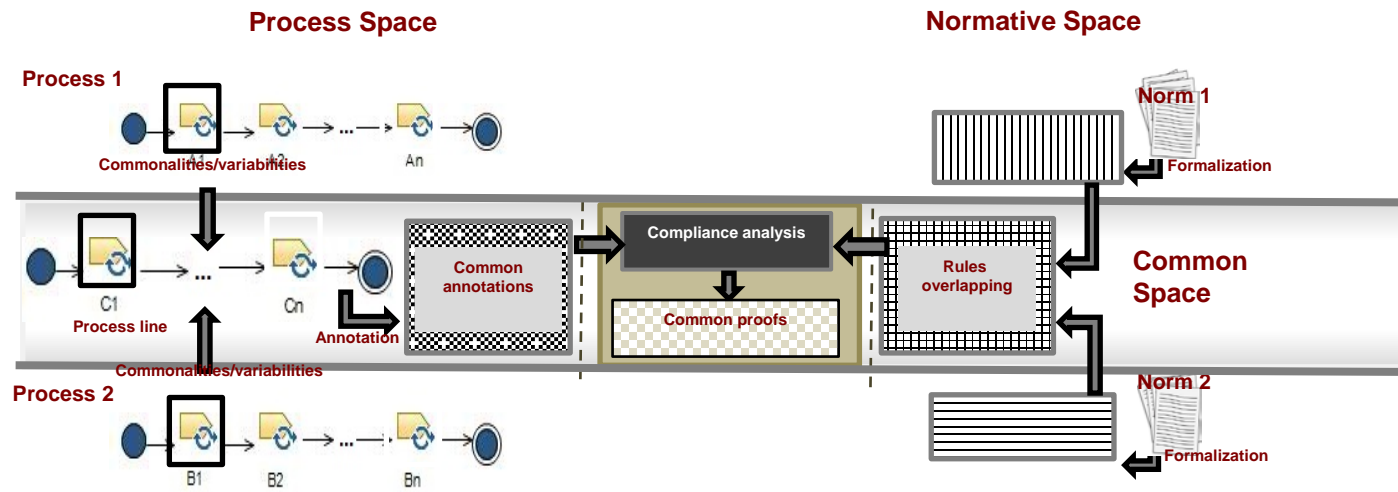


# Compliance management (via argumentation)



[Pattern introduced in a paper to be presented at SAFECOMP-2017]

# Compliance management (via checking)



[Presented at EuroSPI&ASIA<sup>2</sup> 2017]

[+ work to be presented at WoSoCER 2017]

# Summary and future work

- First AMASS prototype has been released
- Solutions for the second prototype have been designed and partially implemented
- Guidelines will be provided
- The second prototype will be evaluated based on the measurement program
- The third prototype will be designed and evaluated



# Thank you for your attention!

