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

MÄLARDALEN UNIVERSITY SWEDEN
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

AMASS Reference Tool Architecture

Architecture-Driven Assurance (STO1)
- System Architecture Modeling for Assurance
- Assurance Patterns Library Management
- V&V-based Assurance Impact Assessment
- Contract-Based Assurance Composition

Multi-Concern Assurance (STO2)
- System Dependability Co-Analyses/Assessment
- Dependability Assurance Modelling
- Contract-Based Multi-concern Assurance

AMASS Platform Basic Building Blocks

Access Manager Data Manager
- System Component Specification
- Assurance Case Specification
- Evidence Management
- Compliance Management
- Common Assurance & Certification Metamodel (CACM)

Cross/Intra-Domain Reuse (STO4)
- Semantic Standards Equivalence Mapping
- Product/Process/Assurance Case Line Specification
- Reuse Assistant (Cross/Intra-Domain)

Seamless Interoperability (STO3)
- Collaborative Work Management
- Tool Quality Assessment and Characterization
- Tool Integration Management

Guidelines in progress

Functionalities designed. Implementation provided and validated (core prototype)

Functionalities designed. Implementation in progress

Independent Assessment
- Certification Liaison
- Safety/Security Assessment

Component Supplier
- Component Release
- Module Assurance Case Development

Product Engineering
- Integration & Certification
- Development
- Quality Management

1st EAB Workshop, Trento, September 11, 2017
• **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**

AMASS Platform Basic Building Blocks

- **Access Manager**
- **Data Manager**
- **System Component Specification**
- **Assurance Case Specification**
- **Evidence Management**
- **Compliance Management**
- **Common Assurance & Certification Metamodel (CACM)**

**Processes:***

- **Capture, retrieve and share information from standards**
- **Define Compliance and Equivalence Mappings**
- **Generate argumentation fragments based on development process**
- **Manage Assurance Project**
- **Monitor status of Assurance Project**

**Interactions:***

- Assurance Manager to Compliance Management
- Assurance Assessor to Compliance Management
• SafeCer EPF Composer-based approach has been integrated
  – CACM includes UMA/SPEM2.0
  – A model transformation has been implemented
• OPENCOSS OpenCert-based approach has been merged
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

1st EAB Workshop, Trento, September 11, 2017
WP6-STO4: Functionalities Interplay

From Scratch

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

Compliance Gap Analysis

Reuse Assistant
Reuse Assistant

Reuse Scenarios
- Product Upgrade
- Cross-Concern
- Cross-Domain
- Cross-Systems (COTS)
- Cross-Systems (SEooC-like)

Reusable Assets
- Compliance Checks
- Artefacts
- Activities
- Requirements
- Design
- Code
- Arguments

Tooling Needs
- Reuse Assistant
- Reuse Discovering
- Assets Management
- Impact Analysis
- Traceability
Reuse Assistant

**Product Upgrade**

- **Assets Management**
  - <<assets>>
  - <<apply>>

- **Impact Analysis**
  - <<effect>>
  - <<collection>>

- **Reuse Assistant**
  - <<analyze>>

- **Reuse Discovering**

**Cross-Concern Cross-Domain**

- **From Scratch**
  - Standards Equivalence Mapping
  - Compliance Gap Analysis
  - Reuse Assistant
Anti-Sysiphus

Semi-automatic generation of Process-based arguments

SACM ++
Patterns
Safety case lines

Semi-automatic generation of Product-based arguments

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

1st EAB Workshop, Trento, September 11, 2017
Process Reuse via EPF Composer & BVR Tool

Modelling variability as an orthogonal separate model

Our DSL = UMA

Base model = UMA-compliant model

Resolved model = UMA-compliant model
Process Reuse via EPF Composer & BVR Tool
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 CHESS & 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)
  - A1, A2, An
- Formalization
- Mapping tables (Core)
- Argumentation about compliance (P1)
- Compliance checking (P2)
- Norm(s)
Compliance management (via argumentation)

Process-based arguments
Generation (Planning Phase)

Argument-fragment Generator (MDSafeCer)

Complementary heterogeneous evidence (techniqueName) is used for checking activity-specific property of type (pi).

PLD-Assurance Case Editor

WEFACT Process executor

[Pattern introduced in a paper to be presented at SAFECOMP-2017]
Compliance management (via checking)

[Presented at EuroSPI&ASIA² 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!