AMASS

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

Second AMASS Platform Prototype: An Overview

Second EAB Workshop
Västerås, Sept 17, 2018

Huáscar Espinoza
EAB Coordinator
Prototype Roadmap
Prototypes Schedule

- **2016**
  - **First Prototype “Core”**
    - Prot. Core Tools release for Case Study evaluation

- **2017**
  - **Second Prototype “P1”**
    - Prot. P1 Tools release for Case Study evaluation
    - Prot. Core Evaluation Results & Demo

- **2018**
  - **Third Prototype “P2”**
    - Prot. P2 Tools release for Case Study evaluation
    - Prot. P2 Evaluation Results & Demo

- **2019**
  - NOW

**Timeline**:
- Prot. Core 2016
- Prot. P1 Tools 2017
- Prot. P2 Tools 2018

**Key Events**:
- Core Evaluation Results & Demo
- Case Study evaluation

**Timeline Image**

**Year**
- 2016
- 2017
- 2018
- 2019
Prototypes Roadmap

AMASS Reference Tool Architecture

Architecture-Driven Assurance (STO1)
- System Architecture Modeling for Assurance
- Assurance Patterns Library Management
- Contract-Based Assurance Composition
- Architectural Patterns
- Technological Patterns

Multi-Concern Assurance (STO2)
- System Dependability Co-Analysis/Assessment
- Contract-Based Multi-concern Assurance
- Dependability 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)
- Automatic Generation of Process-Based Arguments
- Automatic Generation of Product-Based Arguments
- Reuse Assistant
- Process-Related Reuse via Management of Variability at Process Level
- Product-Related Reuse via Management of Variability at Product Level

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

Independent Assessment
- Certification Liaison
- Safety/Security Assessment

Component Supplier
- Component Release
- Module Assurance Case Development

Product Engineering
- Design
- Validation & Verification
- Development
- Quality Management
First Prototype “Core”

❖ Functional description in D2.2: AMASS Reference Architecture (a)
❖ Prototype Core has been built upon 3 pre-existing toolsets:

1. Tools from Papyrus and CHESS projects (Eclipse/PolarSys)
2. Tools from pre-existing OpenCert project (Eclipse/PolarSys)
3. Tools from EPF (Eclipse Process Framework) project (Eclipse)
Second Prototype “P1”

- Partial development of modules linked to AMASS objectives (STO), on top of basic building blocks
- Adoption of new tools as part of the AMASS platform: BVR (variability), CAPRA (traceability),...
- Ad-hoc Integration with external tools
(In-progress) Third Prototype “P2”

- Complete development of modules linked to AMASS objectives (STO), on top of basic building blocks
- Systematic integration (e.g. OSLC) with relevant external tools
- Dashboard as embedded guide for AMASS platform users
Conceptual Dashboard
Comprehensive view of the AMASS methodological framework including the steps of the proposed AMASS process and the interfaces between the steps

The intended readers are:

- AMASS Tool Platform Usage Guidance for Users
- Global Methodological Guidance for Users
- AMASS Tool Platform Guidance for Developers

Built upon Methodological Guidelines (Dx.7,Dx.8)
General AMASS Workflow

1. **Assurance Project Definition**
   - Project Lifecycle
   - Process Definition
   - Compliance Definition
   - Project Baseline

2. **System Design, Analysis and V&V**
   - System Architecture
   - System Requirements
   - Component Contracts
   - Safety/Security Analyses

3. **Assurance Case Management**
   - Compliance Arguments
   - Product Arguments
   - Safety/Security Conflicts
   - Link to Architecture

4. **Evidence Management**
   - Project Artefacts
   - Artefact Traceability
   - Process Execution

---

AMASS
Assurance Project Definition

Project-Independent Activities

From Scratch

Specify Compliance Standards

Map Knowledge from Different Standards

Project-Independent Activities

Systematic Path

(Variability Management)

Specify Reusable Compliant Process

Validate Process Reusability

Project-Specific Activities

Create Assurance Project

Define Compliance Baseline

Derive Project-Specific Process

Cross-System Project Reuse

Cross-Standard Project Reuse
System Design Analysis and V&V

Specify System Requirements

Specify System Architecture Model

Specify Component and Contracts

Validate Component Behaviour

Validate Safety Properties

Validate Security Properties

Analyse Multi-Concern Trade-offs

V&V of System Requirements

Implementation

System Engineer

Component Engineer

Safety Engineer

Security Engineer

Assurance Engineer

Assurance Manager

Design

Design

Design

Validation & Verification

Quality Management

Quality Management
Assurance Case Management

- Create Assurance Case Structure
- Develop Claims and Link to Evidence
- Derive Arguments from Process Models
- Manage Architecture—Assurance Links
- Validate Component Arguments & Assumptions
- Develop Component Arguments & Assumptions
- Manage Multi-Concern Argumentation Trade-offs

Roles:
- Assurance Manager
- Assurance Engineer
- Process Engineer
- System Engineer
- Component Engineer
- Quality Management Engineer
- Implementation Engineer
- Validation & Verification Assurance Engineer
- Component Release Engineer
- System Engineer
- Assurance Engineer

AMASS
Evidence Management

Create Evidence Specification

Characterize Evidential Artefacts

Manage Artefact Traceability

Execute Process and Generate Artefacts

Manage Compliance of Process and Artefacts

Assurance Engineer

Assurance Manager

Process Engineer

Process Engineer

Process Engineer

Process Engineer

Validation & Verification

Quality Management

Implementation

Implementation
AMASS Dashboard Implementation (In-progress Work)

On-going discussions; Example of technology: Eclipse Amalgam
Thank you for your attention!

Any questions