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

AMASS: Technical Vision

First EAB Workshop
Trento, September 11, 2017

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

ISO 26262 → Item definition → Hazards analysis and risk assessment

EN 50126 → Phase 1: concept

BOUNDARY OF SYSTEM/INTERFACES
ENVIRONMENT OF THE SYSTEM

INPUT

Users
Driver, pilot, maintainer...

SYSTEM
Cyberspace
Internet, cloud, wifi, sensors...

Physical World
Car brake, aircraft wing, train door...

OUTPUT
Context and motivation

- Process engineer addressing the safety process
- Architect addressing safety

ARP4761
ISO 26262

- Process engineer addressing the security process
- Architect addressing security

DO-326A
SAE J3061

→ Redundant and conflicting documentation/solutions
→ Waste of time and money
→ Risk for lower quality
ISO 26262 → Work products traceability
DO-178C → Work products traceability
Context and motivation

Proliferation of standards
→ thousands of pages!
→ terminological inconsistency
→ increasing complexity
→ intellectual unmanageability
→ (re)certainment is inefficient (time consuming and expensive!)

ISO 26262
EN 5012x
DO 178B/C
DO-326A
SAE J3061
AMASS Reference Tool Architecture

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

Multi-Concern Assurance (STO2)
- System Dependability Co-Analysis/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
- Reuse Assistant (Cross/Intra-Domain)
- Product/Process/Assurance Case Line Specification

Seamless Interoperability (STO3)
- Collaborative Work Management
- Tool Integration 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

1st EAB Workshop, Trento, September 11, 2017
Architecture-driven

INPUT

SYSTEM

OUTPUT

Conceptual design (perimeter definition)

High-level design

Low-level design
Architecture-driven

Contract-based, component based systems engineering

Semantic Requirements Analysis (supported by ForReq, OCRA, ..)

Verification of Requirements Against System Design
Multi-concern assurance

- Process engineer(s) addressing the security & safety process
- Architect jointly interacting with safety and security managers

→ Synergically conceived documentation/solutions
→ Increased quality
Multi-concern assurance

Trade-off analysis, Process-related co-assessment

[Presented at ISSA, 2016]
Seamless interoperability
Seamless interoperability

Safety Case-Argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development.

ISO 26262- Part 1, Definition 1.106

[Presented at RSSRail, 2017]
[Evolution, to be presented at WoSoCER, 2017]
Cross and intra domain reuse

Intra domain: Automotive normative space

- ISO 26262
- IEC 61508
- (A)SPICE

Cross-domain: Automotive/Avionics

- ISO 26262
- RTCA DO-254
- AEC – Q006
- AEC - Q100

Cross-concern Commonality

- ISO 26262
- Cross-concern Commonality

Intra-domain: Automotive cross concern reuse

- ISO 26262
- SAE J3061

SAE J3061

ISO 26262
Ant-Sysiphus

Process

G3
All possible causes for H1 have been addressed

G6
Low-Pass filter failure has been addressed

G5
Kalman filter failure has been addressed

E2
Kalman filter simulation results

E3
Low-Pass filter simulation results

G1
Binding depends on vehicle type (if truck then G5 else G6)

Assurance Case

x Product

y Vehicle type

z Concept definition

Full system boundary and preliminary hazard identification
Three prototyping dimensions:

1. **Conceptual/Research Development**: development of solutions from a conceptual perspective.

2. **Tool Development**: development of tools implementing conceptual solutions.

3. **Case Study Development**: development of industrial case studies using the conceptual and tooling solutions.

Prototype iterations has three phases:

a) **Prototype Development**: Involves the three dimensions above-mentioned

b) **Prototype Evaluation**: Results evaluated by research questions, tool objectives and case goal achievements.

c) **Prototype Refinement**: Changes to the AMASS approach as recommended by the Evaluation phase.
### Prototype Schedule (First and Second Prototype)

<table>
<thead>
<tr>
<th>2016</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan-Feb</td>
<td>Jan-Feb</td>
<td>Jan-Feb</td>
</tr>
<tr>
<td>Mar-Apr</td>
<td>Mar-Apr</td>
<td>Mar-Apr</td>
</tr>
<tr>
<td>May-Jun</td>
<td>May-Jun</td>
<td>May-Jun</td>
</tr>
<tr>
<td>Jul-Ago</td>
<td>Jul-Ago</td>
<td>Jul-Ago</td>
</tr>
<tr>
<td>Sep-Oct</td>
<td>Sep-Oct</td>
<td>Sep-Oct</td>
</tr>
<tr>
<td>Nov-Dec</td>
<td>Nov-Dec</td>
<td>Nov-Dec</td>
</tr>
</tbody>
</table>

**First Prototype “Core”**
- Prot-1 Tools release for Case Study evaluation
- Prot-1 Evaluation Results & Demo

**Second Prototype “P1”**
- Prot-2 Tools release for Case Study evaluation
- Prot-2 Evaluation Results & Demo

**Third Prototype**

NOW
**Prototype Core: Baseline Tools**

- 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)
*Tailoring EPF Standard models into Baseline models has not implemented yet.
AMASS Platform: Assurance Project Models

*System Models are edited in Papyrus + CHESS. Its links have not been created yet.*
AMASS Platform: Importing EPF Models

EPF Models
- Method Library Model (e.g. Thales SW Process Definition)
- Delivery Process Configuration (e.g. Thales SW Process Planning)
- Standard Model (e.g. DO-178C)

Assurance Project Models
- Baseline Configuration (e.g. ISO 26262 Configuration or SW/HW DO Configuration)
- Permissions Configuration (e.g. Audit mode access configuration)
- Assurance Assets Package (e.g. First product release package of assets)
- Argumentation Model (e.g. Safety Case for ePark)
- Evidence Model (e.g. Artifacts for ePark project, Artifacts for DO-178C)
- Process Model (e.g. Activities and participants for the ePark project)
- System Model (e.g. Architecture of the ePark system)

What Standards Prescribe in Project
- Baseline Model (e.g. DO-178C for Avionics SW)
- Baseline Model (e.g. ISO26262 for ePark)

What has Been Done
Prototype Core: Video
Thank you for your attention!