AMASS

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

Long Presentation

H2020-JTI-ECSEL-2015 # 692474
AMASS in a Nutshell

- **20,7** Million € Total budget
- **2500** Person-Months Effort
- **36** Months Duration
- **29** Partners
- **8** Countries

<table>
<thead>
<tr>
<th>No</th>
<th>Participant organisation name</th>
<th>Short</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tecnalia Research &amp; Innovation</td>
<td>TEC</td>
<td>ES</td>
</tr>
<tr>
<td>2</td>
<td>Honeywell</td>
<td>HON</td>
<td>CZ</td>
</tr>
<tr>
<td>3</td>
<td>Schneider Electric España</td>
<td>TLV</td>
<td>ES</td>
</tr>
<tr>
<td>4</td>
<td>ANSYS medini Technologies AG</td>
<td>KMT</td>
<td>DE</td>
</tr>
<tr>
<td>5</td>
<td>Mälardalen University</td>
<td>MDH</td>
<td>SE</td>
</tr>
<tr>
<td>6</td>
<td>Eclipse Foundation Europe</td>
<td>ECL</td>
<td>DE</td>
</tr>
<tr>
<td>7</td>
<td>Infineon</td>
<td>IFX</td>
<td>DE</td>
</tr>
<tr>
<td>8</td>
<td>AIT Austrian Institute of Technology GmbH</td>
<td>AIT</td>
<td>AT</td>
</tr>
<tr>
<td>9</td>
<td>Fondazione Bruno Kessler</td>
<td>FBK</td>
<td>IT</td>
</tr>
<tr>
<td>10</td>
<td>Intecs</td>
<td>INT</td>
<td>IT</td>
</tr>
<tr>
<td>11</td>
<td>Assystems Germany GmbH</td>
<td>B&amp;M</td>
<td>DE</td>
</tr>
<tr>
<td>12</td>
<td>GMV Aerospace and Defence, S.A.U.</td>
<td>GMV</td>
<td>DE</td>
</tr>
<tr>
<td>13</td>
<td>RINA</td>
<td>RINA</td>
<td>IT</td>
</tr>
<tr>
<td>14</td>
<td>Thales Alenia Space</td>
<td>TAS</td>
<td>ES</td>
</tr>
<tr>
<td>15</td>
<td>Universidad Carlos III de Madrid</td>
<td>UC3</td>
<td>ES</td>
</tr>
<tr>
<td>16</td>
<td>Rapita Systems</td>
<td>RPT</td>
<td>UK</td>
</tr>
<tr>
<td>17</td>
<td>The REUSE company</td>
<td>TRC</td>
<td>ES</td>
</tr>
<tr>
<td>18</td>
<td>OHB Sweden AB</td>
<td>OHB</td>
<td>SE</td>
</tr>
<tr>
<td>19</td>
<td>Masaryk University</td>
<td>UOM</td>
<td>CZ</td>
</tr>
<tr>
<td>20</td>
<td>Alstom Transport S.A.</td>
<td>ALS</td>
<td>FR</td>
</tr>
<tr>
<td>21</td>
<td>Kompetenzzentrum – Das virtuelle Fahrzeug Forschungsgesellschaft mbH</td>
<td>VIF</td>
<td>AT</td>
</tr>
<tr>
<td>22</td>
<td>Alliance pour les technologies de l' Informatique</td>
<td>A4T</td>
<td>FR</td>
</tr>
<tr>
<td>23</td>
<td>COMMISARIAT A LENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES</td>
<td>CEA</td>
<td>FR</td>
</tr>
<tr>
<td>24</td>
<td>CLEARSY SAS</td>
<td>CLS</td>
<td>FR</td>
</tr>
<tr>
<td>25</td>
<td>ALTEN SVERIGE AKTIEBOLAG</td>
<td>ALT</td>
<td>SE</td>
</tr>
<tr>
<td>26</td>
<td>Lange Research Aircraft Gmbh</td>
<td>LAN</td>
<td>DE</td>
</tr>
<tr>
<td>27</td>
<td>Thales Italia SpA</td>
<td>THI</td>
<td>IT</td>
</tr>
<tr>
<td>28</td>
<td>RISE Research Institutes of Sweden</td>
<td>SPS</td>
<td>SE</td>
</tr>
<tr>
<td>29</td>
<td>Comentor AB</td>
<td>COM</td>
<td>SE</td>
</tr>
</tbody>
</table>
Assurance is the planned and systematic activities to get justified confidence that systems conform to its requirements for safety, security, reliability, availability, maintainability, standards and regulations.

Certification is a (legal) recognition that a system complies with standards, rules and regulations designed to ensure it can be depended upon to deliver its intended service safely.
Safety Assurance and Certification are critical concerns:

→ Through the *entire system lifecycle* and *as early as possible*

→ In all *engineering domains* and levels of the *supply chain*
AMASS will develop an integrated and holistic approach and supporting tools for **assurance and certification of cyber-physical systems (CPS)** for the largest CPS vertical markets.

The approach will be **driven by architectural decisions**, including multiple assurance concerns such as safety, security, availability, robustness and reliability.

The main goal is to **reduce time, costs and risks** for assurance and (re)certification by extending the OPENCOSS and SafeCer approaches.
The AMASS approach will be driven by architectural decisions, including multiple assurance concerns such as safety, security, availability, robustness and reliability. The main goal is to reduce time, costs and risks for assurance and (re)certification.
AMASS will develop an integrated and holistic approach and supporting tools for **assurance and certification of CPS** by creating and consolidating the first European-wide open certification/qualification **platform, ecosystem and community** spanning the largest CPS vertical markets.
AMASS Tangible Outcomes

- **AMASS Reference Tool Architecture**
  - Tool Metamodels, Tool Adaptor Metamodels, Tool Usage Methodologies/Guidance

- **AMASS Open Tool Platform**
  - AMASS-Specific Tool Modules (To be Developed During the AMASS Project)
    - SafeCar (Baseline)
    - OPENCOSS (Baseline)
    - Others (Baseline)

- **Base Tool 1**
  - (e.g. DB Management)

- **Base Tool 2**
  - (e.g. Access Management)

- **External Tool 1**
  - (e.g. Testing)

- **External Tool 2**
  - (e.g. Safety Analysis)

- **Open AMASS Community**
  - (maintenance, evolution, industrialization)
OPENCOSS Project Approach

An open and customizable safety assets tool platform to improve reliability, transparency, and to reduce cost/times of assurance/certification processes.

Compliance Management and Transparent Assurance

Product Engineering “Project”

(Independent) Safety Assessment

Assurance “Project”

Supplier Chain

Evidence and Argumentation

Confidence Assessment

Compliance-Aware Engineering Process

Safety Case-based Compositional Assurance

CROSS-MAPPINGS BETWEEN STANDARDS

www.opencoss-project.eu

Evidence Traceability and Impact Analysis

Specification of Standards, Rules and Regulations

www.opencoss-project.eu
SafeCer Project Approach

- SafeCer component (meta) model
- Safety Cases complying to safety standards (e.g. ISO 26262)
- Derive the overall confirmation measures for verification and validation (Evidence gathered by analysis and testing)
- Development of a Certification Tool Framework
- Development of a Certification Artefact Repository
AMASS Reference Tool Architecture

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
- Technological Patterns
- Architectural Patterns

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
- 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

Independent Assessment
- Certification Liaison
- Safety/Security Assessment

Component Supplier
- Component Release
- Module Assurance Case Development

Product Engineering
- Design
- Validation & Verification
- Development
- Quality Management
AMASS aims to provide a modelling language, tools, and techniques to support an assurance that exploits and is linked to the system architecture in order to show system dependability and compliance with standards.

- System architecture modelling for assurance
- Assurance patterns library
- Assurance of new technologies
- Contract-based assurance composition approaches
- V&V-based assurance
Multi-concern Assurance

• Multi-concern assurance refers to the current need for justifying that several dependability aspects (safety, security, reliability…) have been adequately assured for a system

• This includes:
  – Co-analysis
  – Co-design
  – Co-V&V
  – Co-assurance

• Especial attention will be paid to safety and security co-engineering and to the integration of these two concerns
Seamless Interoperability

- The tasks executed for the engineering and assurance of CPS need to be better integrated so that (1) tools can seamlessly exchange data and (2) stakeholders can seamlessly collaborate.

- Tool support is usually limited to point-to-point data exchange in some specific data format.

- Modern web technologies can help in closing the gaps among tools and stakeholders.
Cross- and Intra-Domain Reuse

- Assurance information can in principle be reused across system versions and projects, and even domains; but reuse needs and consequences must be carefully analysed.

- Assurance reuse deals with process-based, product-based, argumentation-based, and cross-concern aspects.

- Although some existing solutions enable reuse, further support is necessary, e.g. based on semantic technologies and reasoning.
11 Case Studies

- **Industrial Automation (1):** Industrial and automation control systems
- **Automotive (4):** Advanced driver assistance function with electric sub-system, Collaborative automated fleet of vehicles, Connected hybrid powertrain, Automotive telematics function
- **Space (3):** Design and safety assessment of on-board software applications, Certification basis to boost the usage of MPSoC architectures, Design and efficiency assessment of model-based altitude and orbit control software development
- **Railway (1):** Platform screen doors controller
- **Avionics (1):** Safety assessment of multi-modal interactions in cockpits
- **Air Traffic Management (1):** Safety-critical software lifecycle of a monitoring system for NavAid
Technical Impact

• Cross-domain convergence of the industrial practice for assurance and certification, so as to share methods, tools, and knowledge across domains

• Inclusion of advanced practices such as model-based development, formal methods, and simulation techniques for CPS assurance & certification

• Reuse-geared development and certification processes as a major means to decrease costs

• Automation of labour-intensive activities

• Technology availability and support for the entire life cycle of a product
Societal Impact

• **OEMs** (including system integrators) and **Component suppliers** will use AMASS results to increase CPS design efficiency, reduce assurance and certification costs, ease innovation, and reduce assurance and certification risks.

• **Assessors and Certification authorities** will be able to provide services that better fit CPS-specific needs.

• **Tool vendors** will extend their products with new features and integrate them with the AMASS Platform.

• **Research partners** will be able to reach a leading position in research on CPS assurance and certification.

• **European society** will benefit from the use of CPS with a higher confidence in their dependability, for a wide range of applications.
Eclipse Open-Source Model

AMASS-Specific Building Blocks:
Architecture-Driven, Multi-Concern Assurance,
Seamless Interoperability, Cross/Intra-Domain Reuse

Basic Building Blocks (Eclipse, Tomcat,..):
Access Manager, Data Manager, Database
for CACL

Basic Building Blocks (OPENOSS, SafeCer,..):
System Component Spec., Assurance Case
Spec., Evidence Mgmt, Compliance Mgmt.

Products Added Value

Platform

Compete on products and services
Build this in and with open source, even if that means working with your direct competitors.

Proprietary solutions (Company-specific & Commercializable)
Public solution (Company-independent & Freely available)
AMASS Open Community: OpenCert

Introducing OpenCert: Evolutionary Assurance and Certification for Safety-Critical Systems

OpenCert at Polarsys-Eclipse:
- Industrial community
- Governance Structure
- Maturity/Industrialization Platform

Further links with Eclipse projects:
- Papyrus
- CHESS
- EPF
Conclusion

• AMASS will create and consolidate the **de-facto** European-wide open tool platform, ecosystem, and self-sustainable community for CPS assurance and **certification** in the largest industrial vertical markets (automotive, railway, aerospace, space, energy...)

• A novel holistic and reuse-oriented approach for architecture-driven assurance, multi-concern assurance, and seamless interoperability between assurance and engineering activities will be defined

• AMASS results will lead to
  – **Increase in design efficiency and** in assurance and certification harmonization
  – **Reduction of** assurance and certification **costs and risks**