AMASS

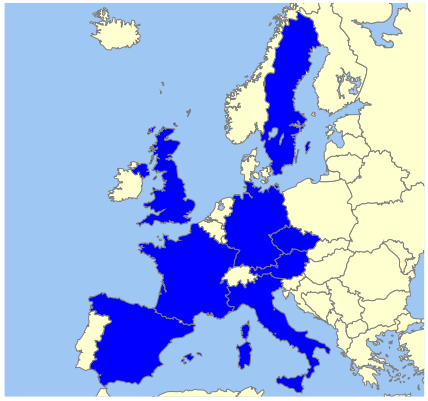
Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

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



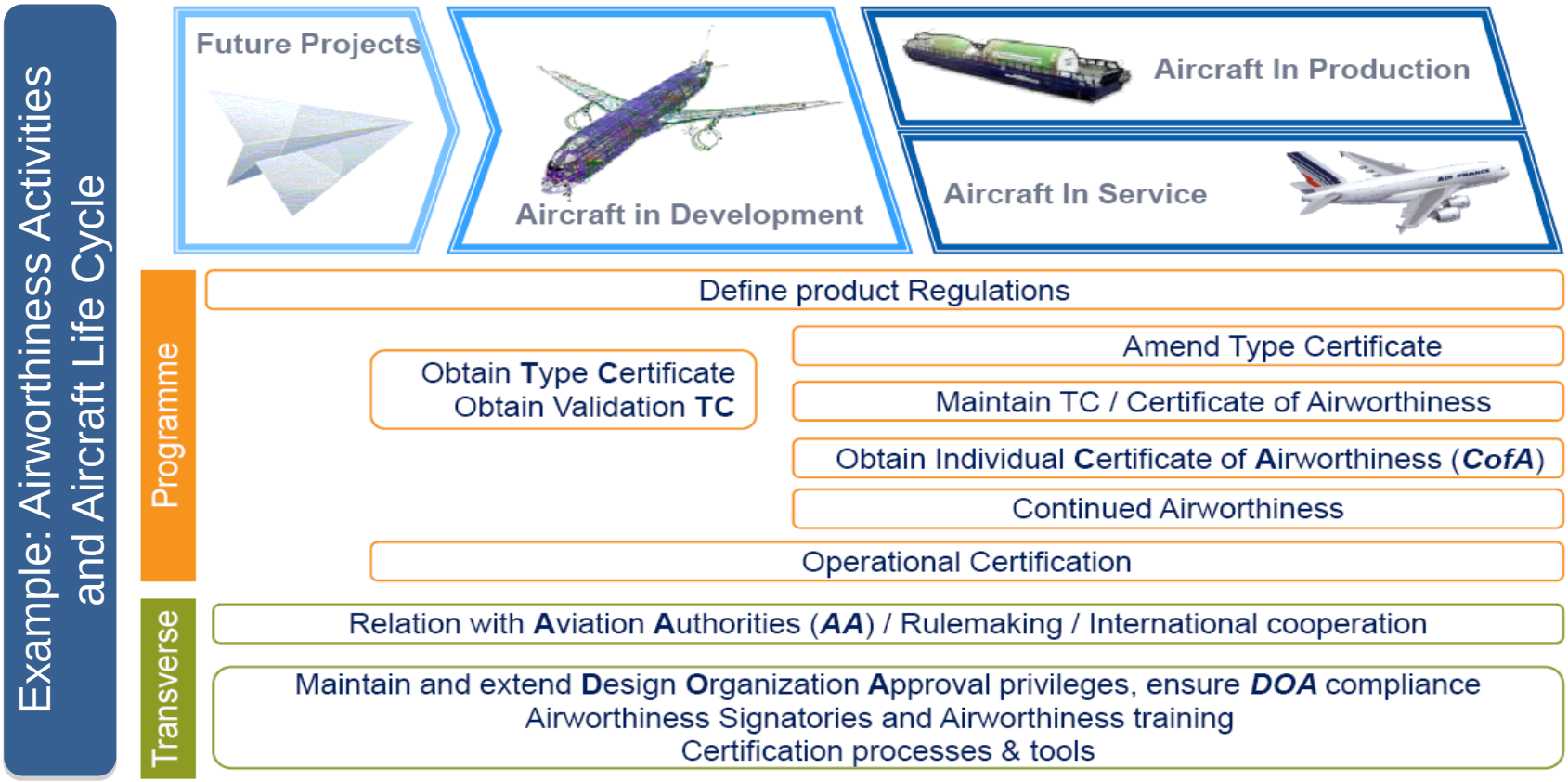
No	Participant organisation name	Short	Country
1	Tecnalia Research & Innovation	TEC	ES
2	Honeywell	HON	CZ
3	Schneider Electric España	TLV	ES
4	ANSYS medini Technologies AG	KMT	DE
5	Mälardalen University	MDH	SE
6	Eclipse Foundation Europe	ECL	DE
7	Infineon	IFX	DE
8	AIT Austrian Institute of Technology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

In the Safety-Critical Systems domain…

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.

The Certification Impact in Safety-Critical Systems



Safety Assurance and Certification are critical concerns:

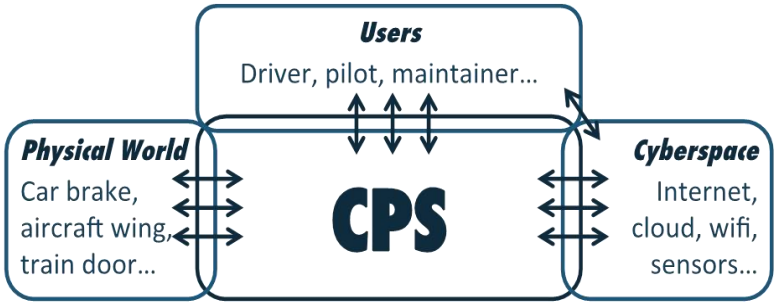
→Through the **entire system lifecycle** and **as early as possible**

→In **all engineering domains** and levels of the **supply chain**

General Objective

- 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.

AMASS Project Objectives



Increase in ***product complexity***

Very high costs & effort

Lack of standardized & harmonized practices

New assurance & certification risks

Architecture-specific *assurance* ***needs***

Need for addressing new, ***multiple concerns***

Wider ***variety of tools and stakeholders***

Insufficient reuse support

Problem

CPS assurance & certification

Solution

- Integrated & holistic approach
- CPS-specific needs addressed
- Maintained tool support

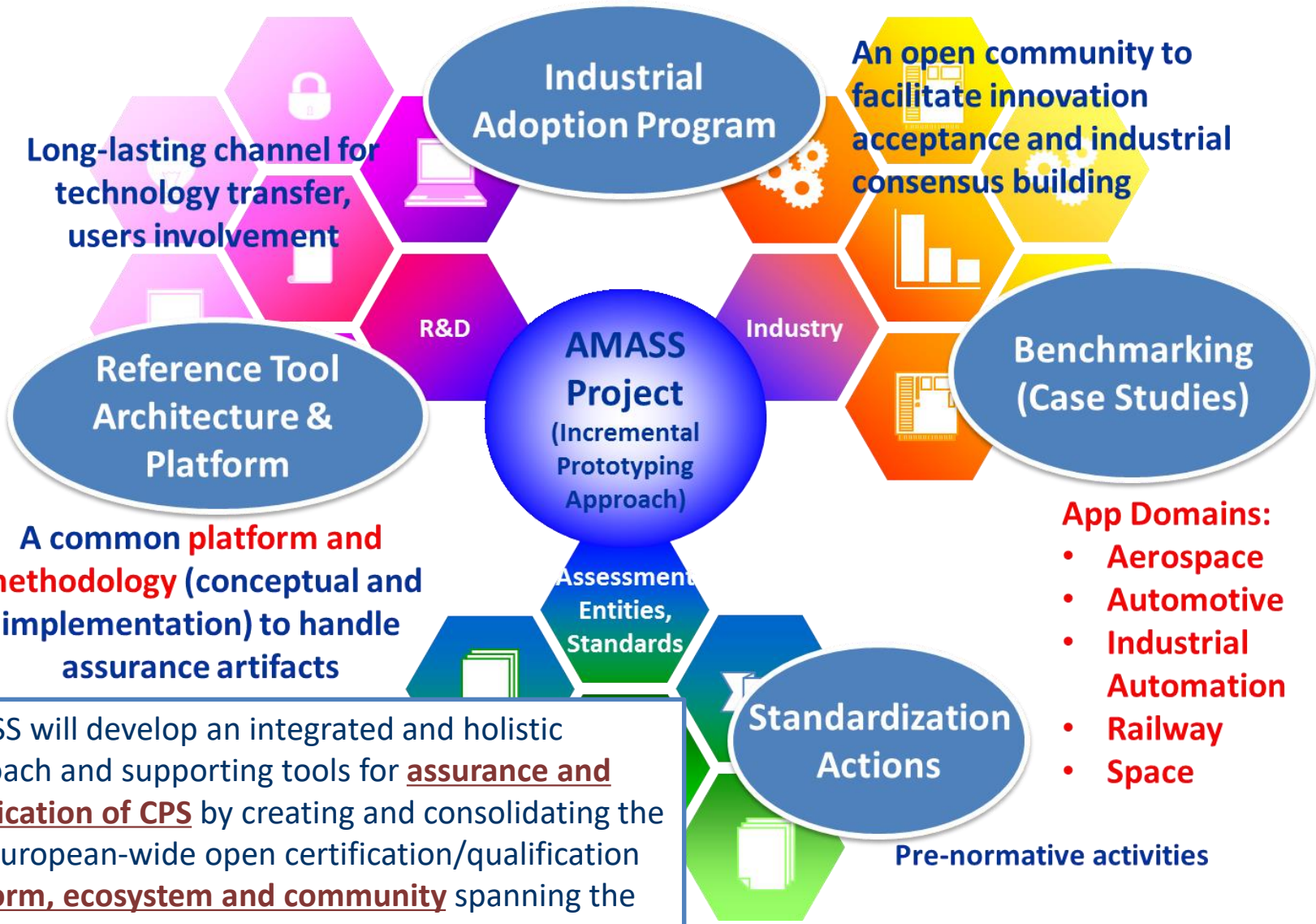
50% effort reduction
40% reuse cost reduction
35% assurance risks reduction
60% harmonization increase

✓ **Higher design efficiency**
✓ **Lower recurring costs**
✓ **Easier innovation**
✓ **Openness & interoperability**

Architecture-driven, Multi-concern, Seamless, Reuse-Oriented Assurance & Certification

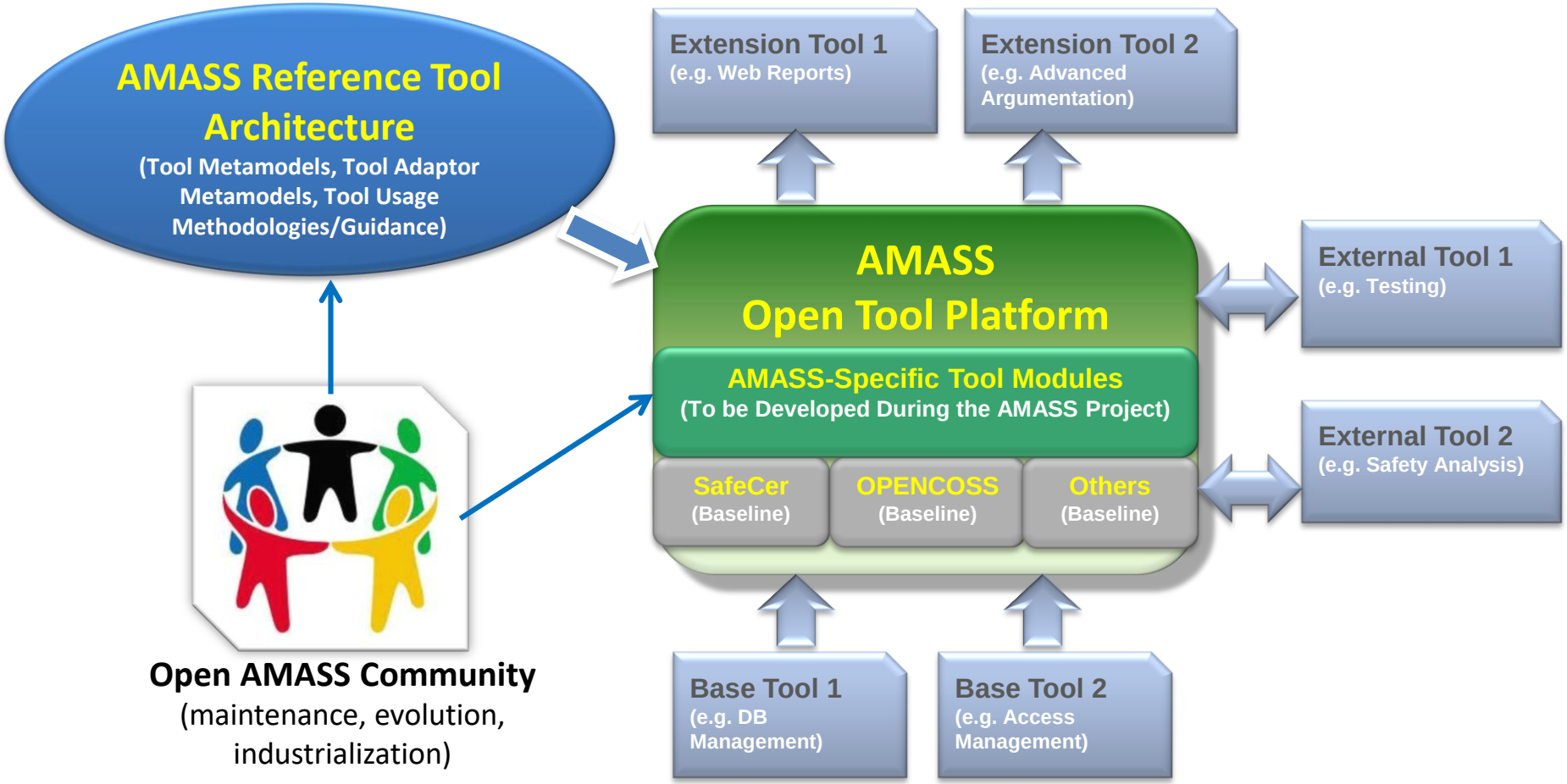
The AMASS approach will be driven by architectural decisions, including multiple assurance concerns such as **safety**, **security**, availability, robustness and reliability. The main goal is **to reduce time, costs and risks** for assurance and (re)certification.

AMASS Overall Strategy



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



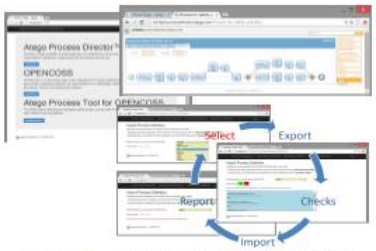
OPENCOSS Project Approach

OPENCOSS — Open Platform for EvolutioNary Certification Of Safety-critical Systems

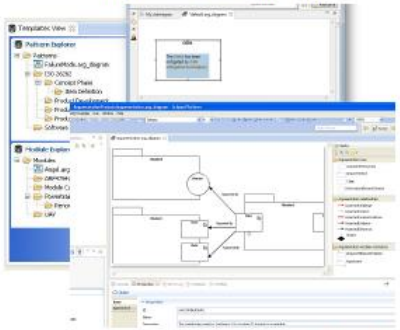
An open and customizable safety assets tool platform to improve reliability, transparency, and to reduce cost/times of assurance/certification processes.

Compliance Management and Transparent Assurance

Evidence and Argumentation Confidence Assessment



Compliance-Aware Engineering Process

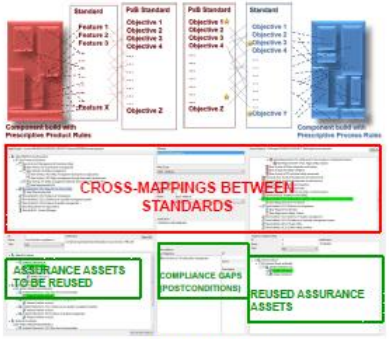


Safety Case-based Compositional Assurance

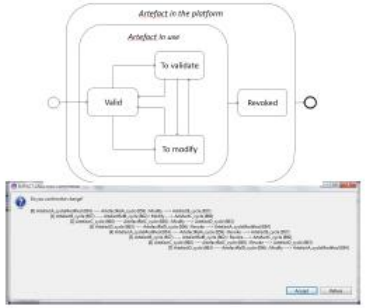
SEVENTH FRAMEWORK PROGRAMME

tecnalia Inspiring Business

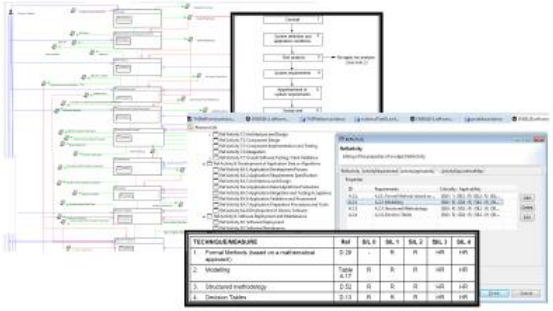
PolarSys Open Source Tools for Embedded Systems



Cross-Domain Reuse



Evidence Traceability and Impact Analysis

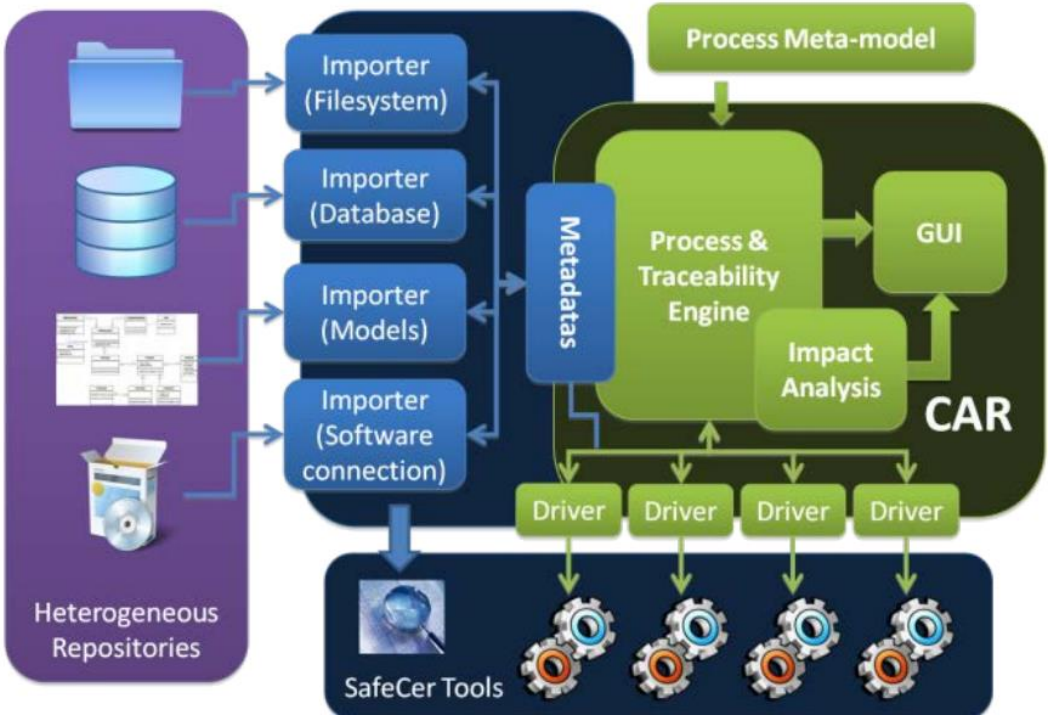


Specification of Standards, Rules and Regulations

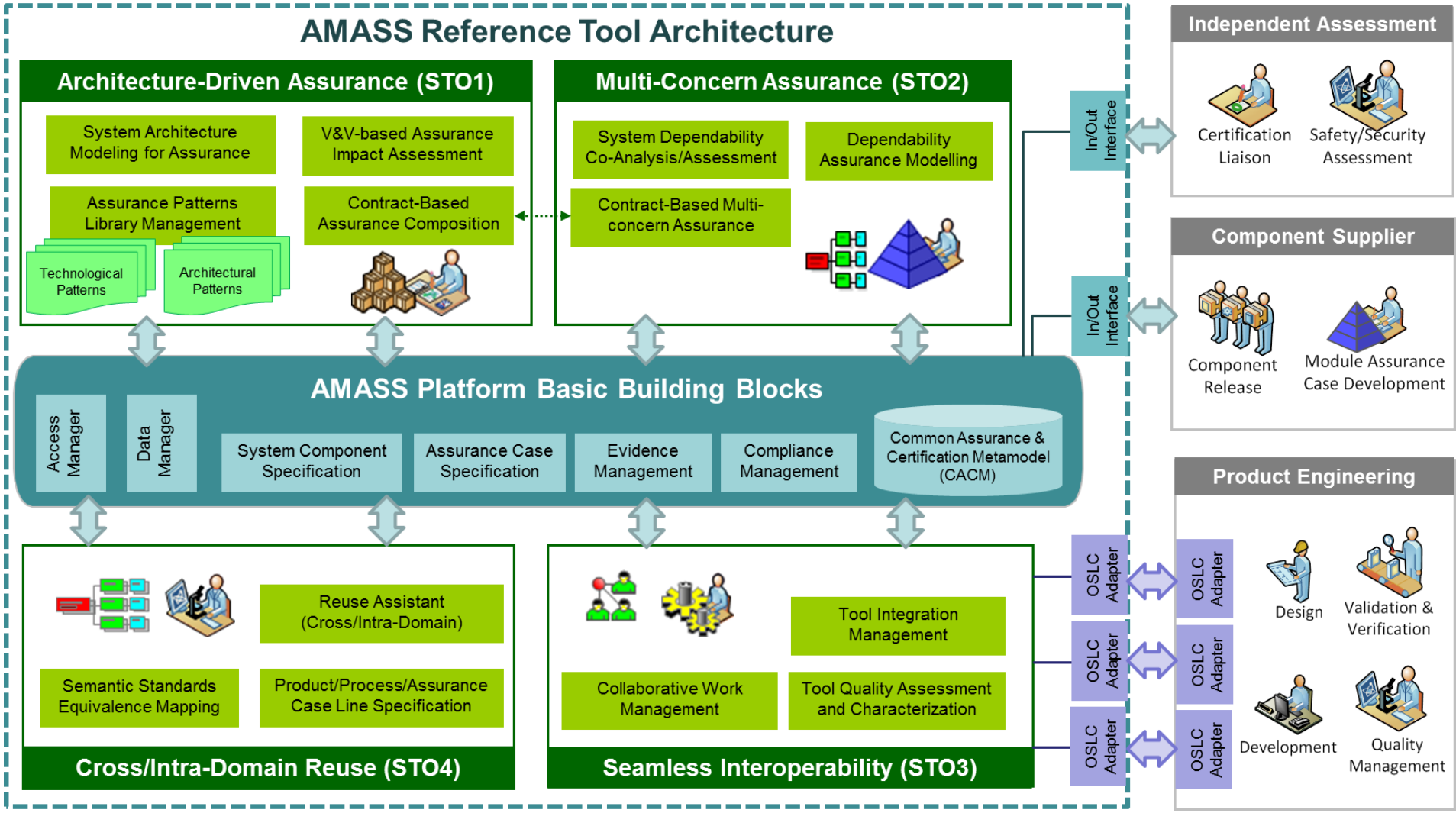
www.opencoss-project.eu

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

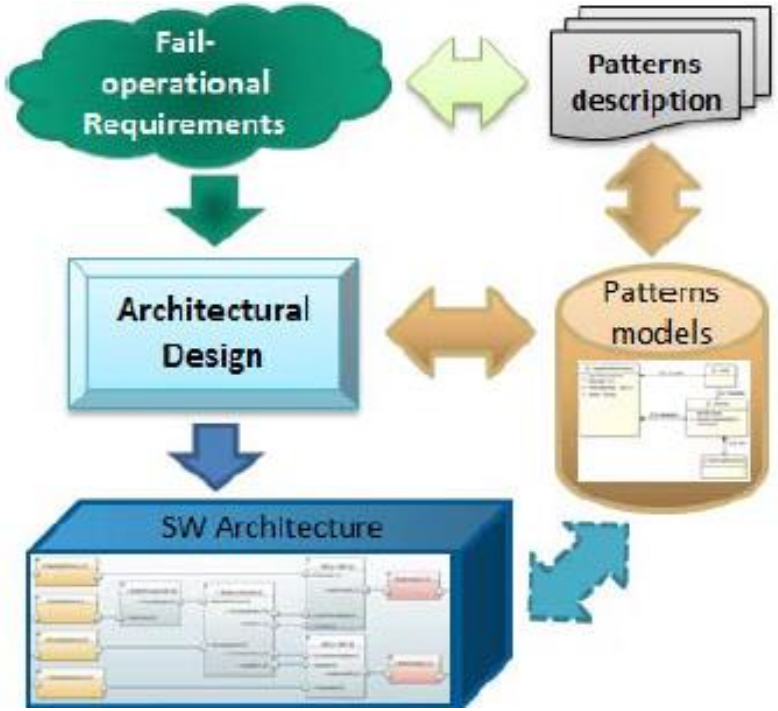


AMASS Reference Tool Architecture



Architecture-Driven Assurance

- 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
- This includes:
  - System architecture modelling for assurance
  - Assurance patterns library
  - Assurance of new technologies
  - Contract-based assurance composition approaches
  - V&V-based assurance



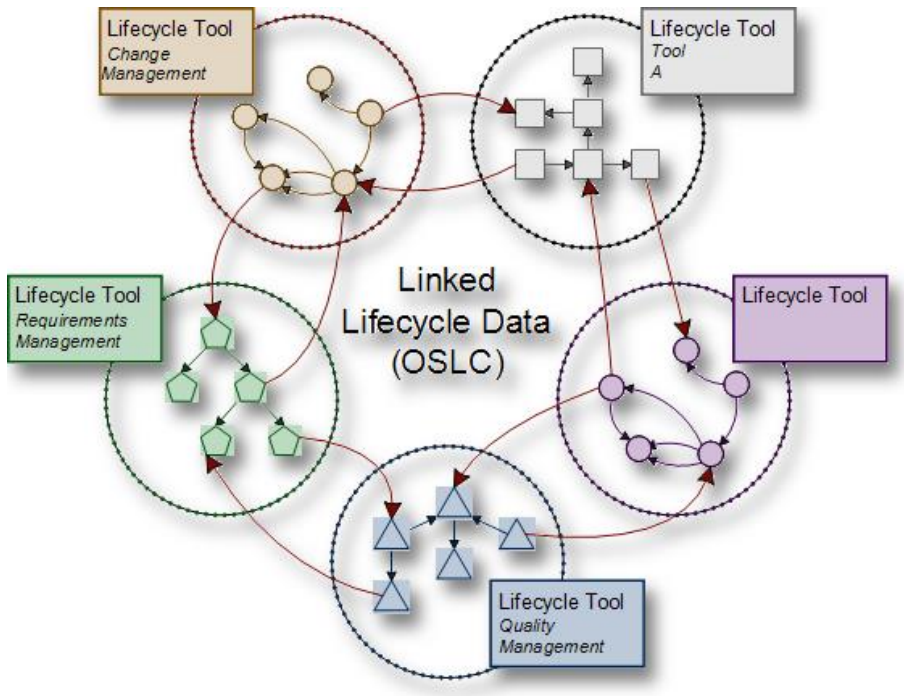
Multi-concern Assurance

- 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

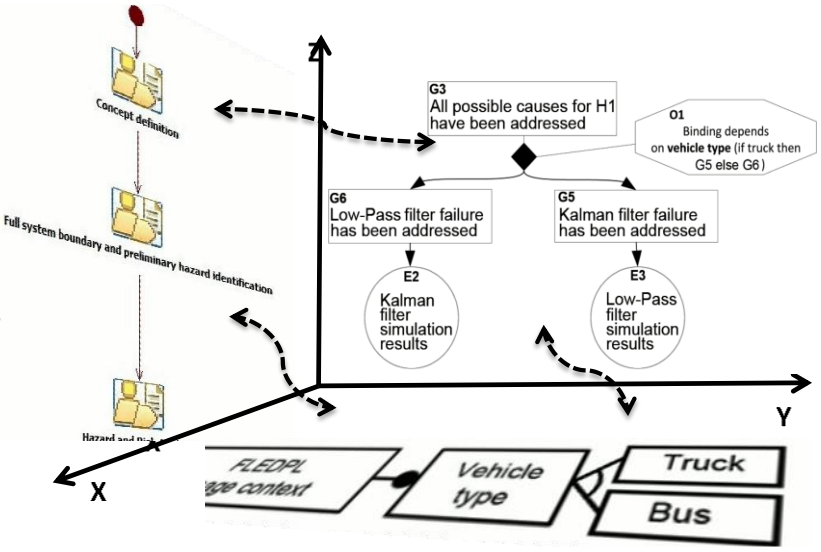
Seamless Interoperability

- 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

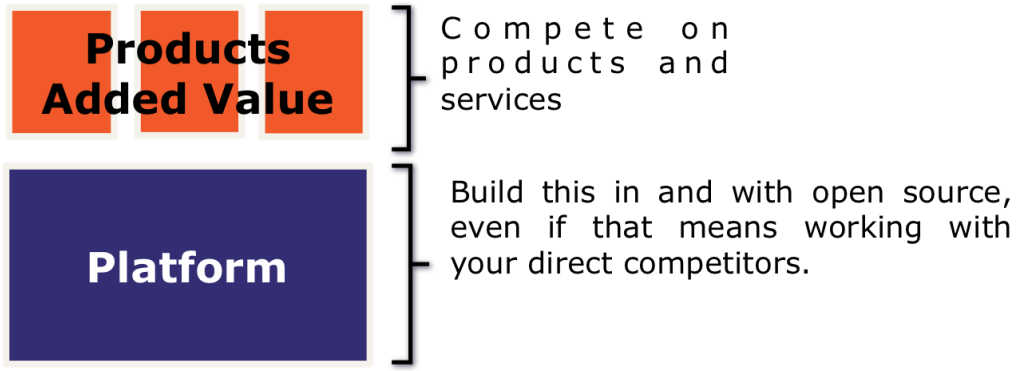
- **Cross-domain convergence** of the industrial practice for assurance and certification, so as to share methods, tools, and knowledge across domains
- Inclusion of **advanced practices** such as model-based development, formal methods, and simulation techniques for CPS assurance & certification
- **Reuse-geared 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

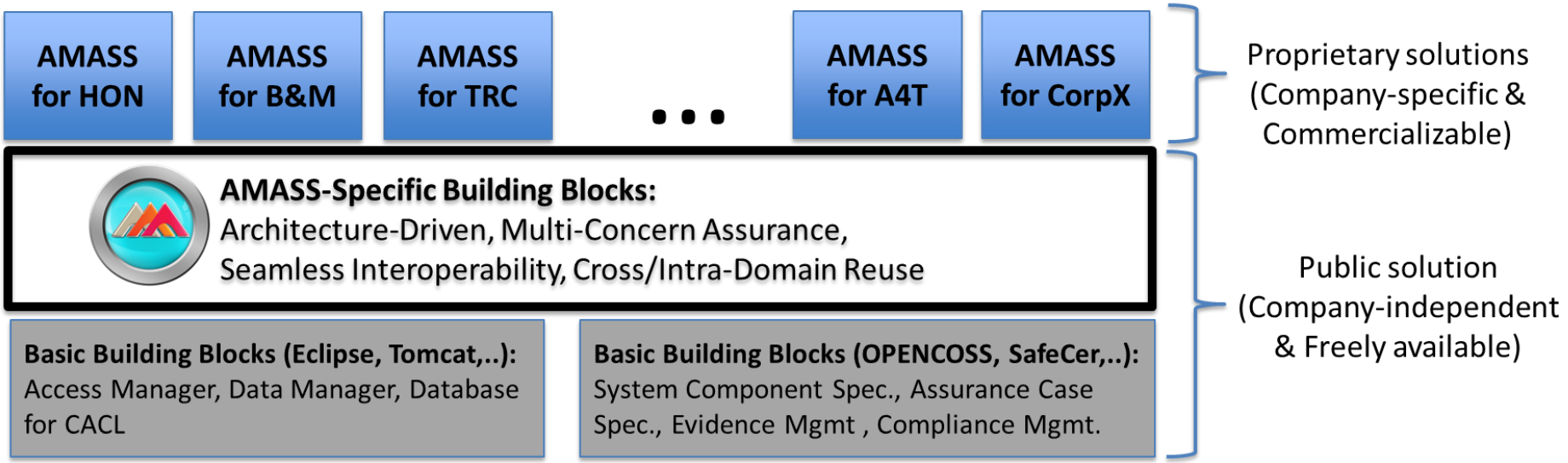
Societal Impact

- **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

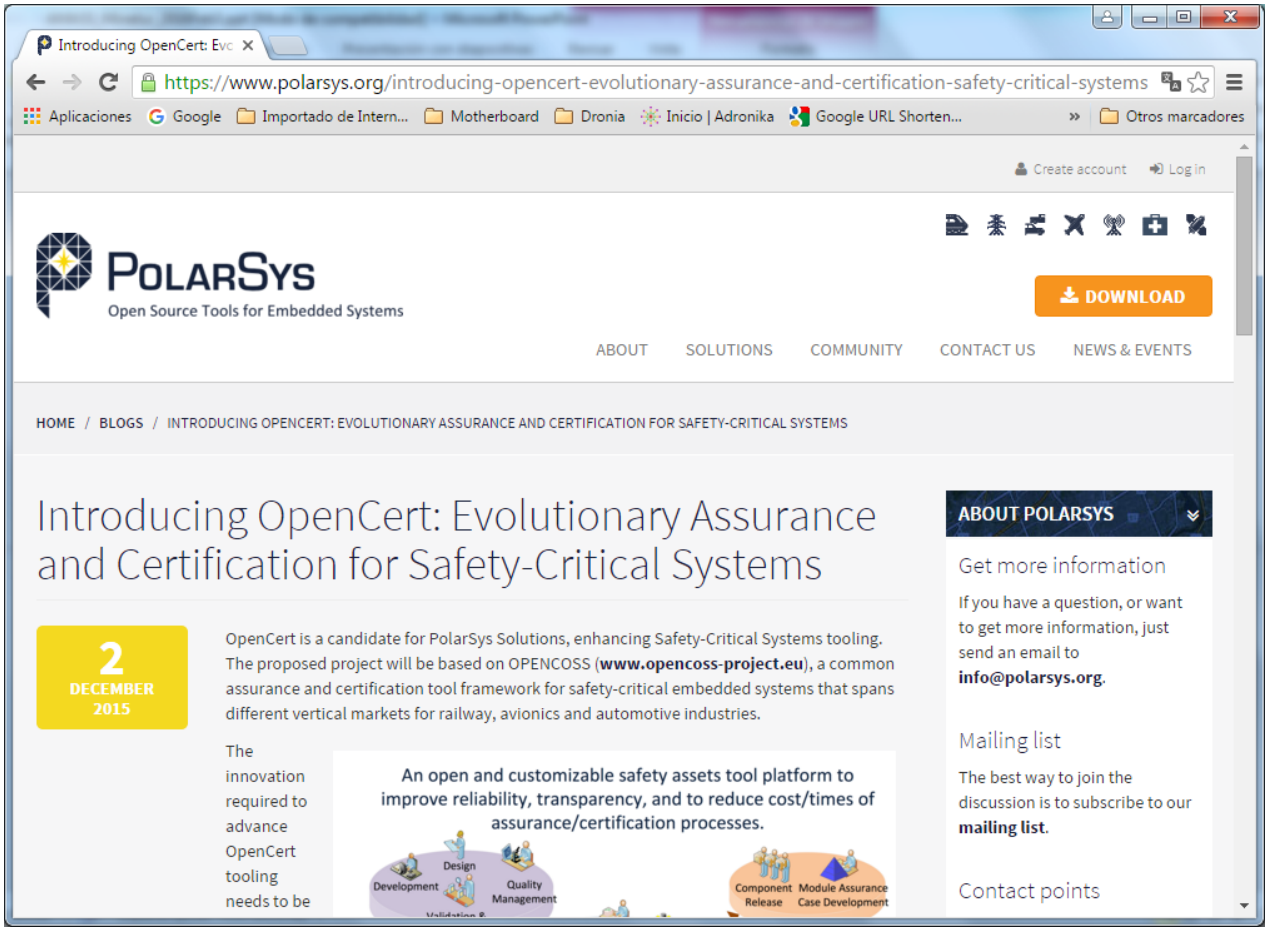
AMASS Open Community

Eclipse Open-Source Model





AMASS Open Community: OpenCert



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**