AMASS

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

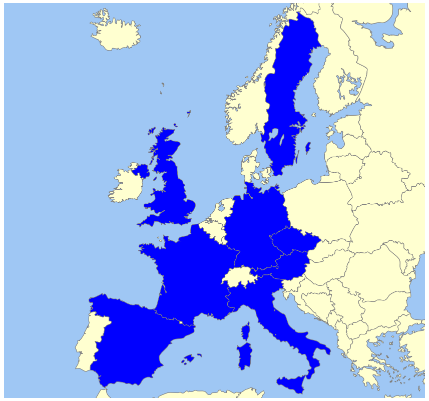
Project Overview

DeCPS Workshop
June 17, 2016

Silvia Mazzini.
Intecs Project Manager

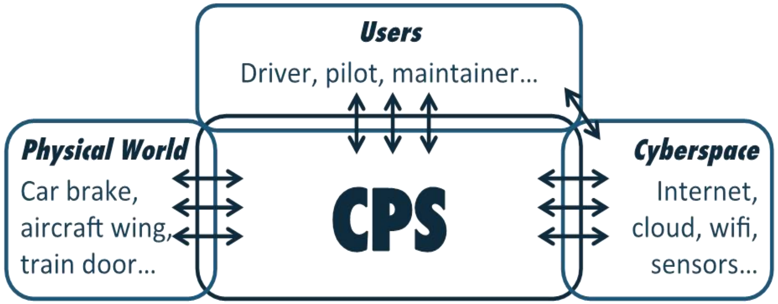
AMASS in a Nutshell

- **3rd** -Ranked RIA Project
- **20,5** 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	Telvent Energia SA – Schneider Electric Spain	TLV	ES
4	KPIT 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	Berner & Mattner	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	AVL List GmbH	AVL	AT
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 Aviation	LAN	DE
27	Thales Italia SpA	THI	IT
28	SP Sveriges Tekniska Forskningsinstitut	SPS	SE
29	Comentor AB	COM	SE

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***

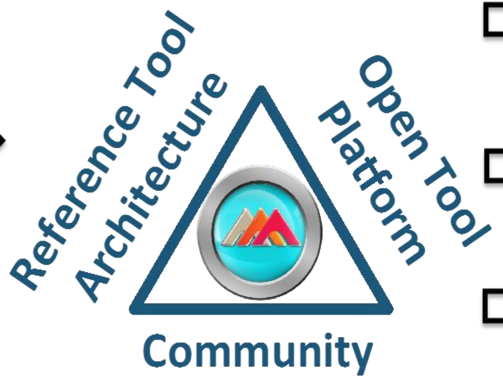
Wider ***variety of tools and stakeholders***

Insufficient reuse support

Problem

CPS assurance & certification

Solution



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

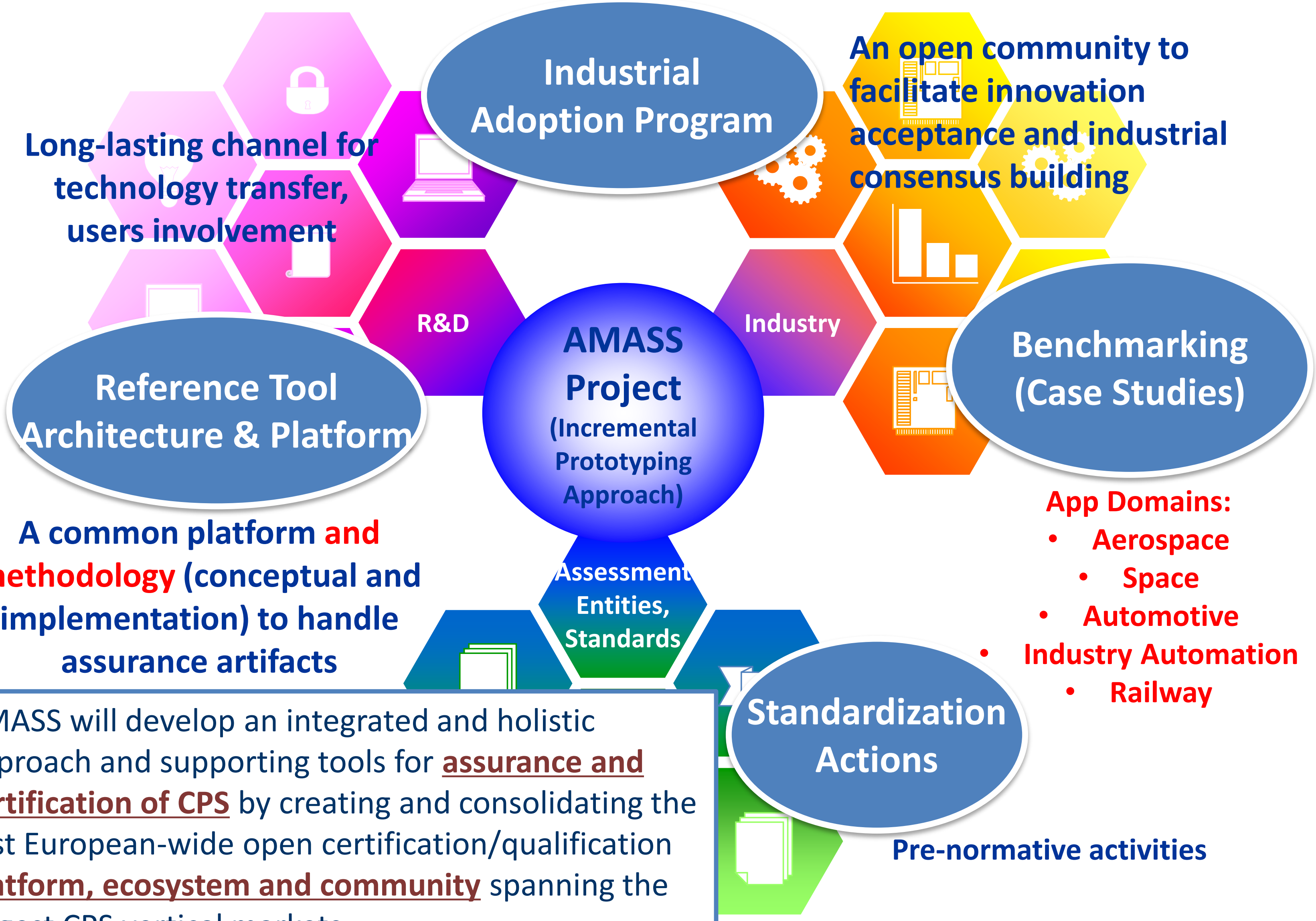
50% effort reduction
40% reuse cost reduction
35% assurance risks reduction
60% harmonization increase

- ✓ **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



Industrial Adoption Program

An open community to facilitate innovation acceptance and industrial consensus building

Long-lasting channel for technology transfer, users involvement

AMASS Project (Incremental Prototyping Approach)

Reference Tool Architecture & Platform

Benchmarking (Case Studies)

A common platform and methodology (conceptual and implementation) to handle assurance artifacts

App Domains:

- Aerospace
- Space
- Automotive
- Industry Automation
- Railway

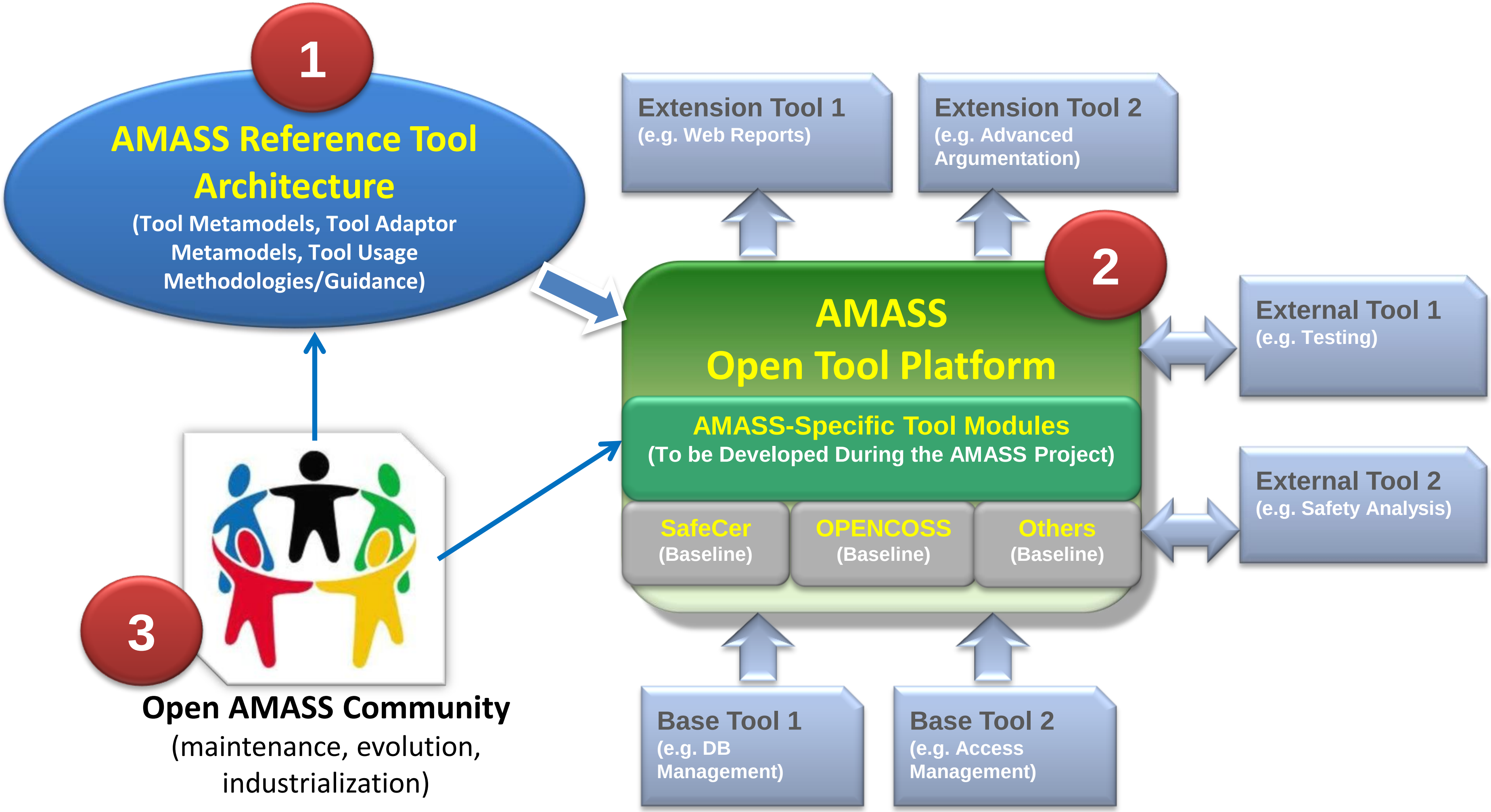
Assessment Entities, Standards

Standardization Actions

Pre-normative activities

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



1

AMASS Reference Tool Architecture

(Tool Metamodels, Tool Adaptor Metamodels, Tool Usage Methodologies/Guidance)

2

AMASS Open Tool Platform

AMASS-Specific Tool Modules

(To be Developed During the AMASS Project)

SafeCer (Baseline)

OPENCOSS (Baseline)

Others (Baseline)

Extension Tool 1 (e.g. Web Reports)

Extension Tool 2 (e.g. Advanced Argumentation)

External Tool 1 (e.g. Testing)

External Tool 2 (e.g. Safety Analysis)

Base Tool 1 (e.g. DB Management)

Base Tool 2 (e.g. Access Management)

3

Open AMASS Community

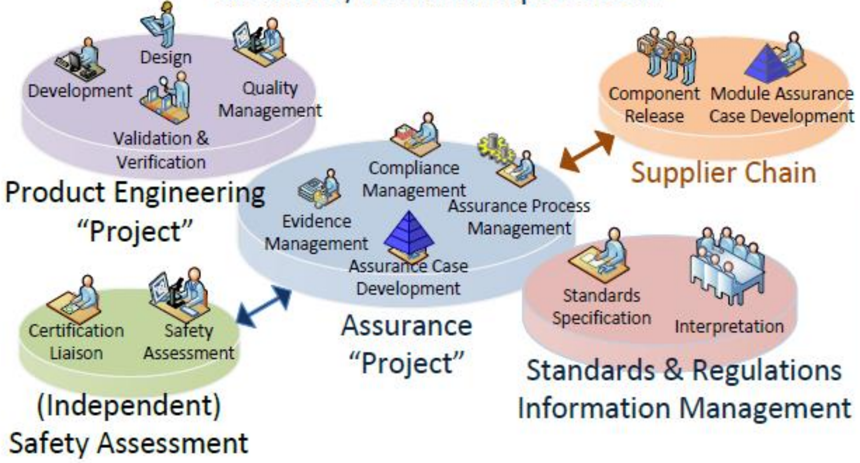
(maintenance, evolution, industrialization)

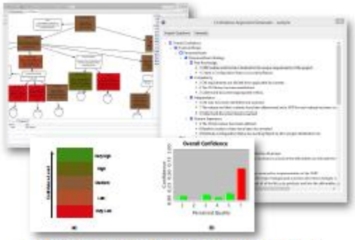
OPENCOSS Project approach

OPENCOSS Open Platform for EvolutioNary Certification Of Safety-critical Systems

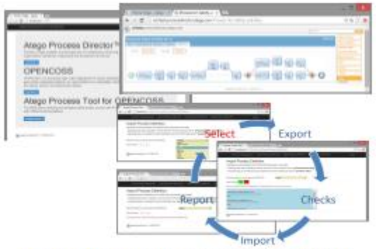
An open and customizable safety assets tool platform to improve reliability, transparency, and to reduce cost/times of assurance/certification processes.

Compliance Management and Transparent Assurance

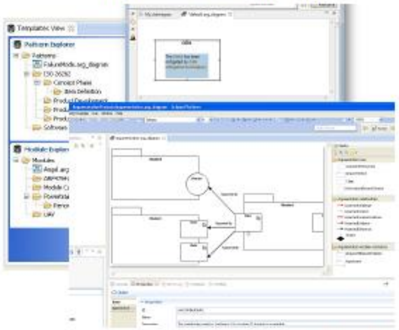

Design
Development
Quality Management
Validation & Verification
Product Engineering "Project"
Component Release
Module Assurance Case Development
Supplier Chain
Compliance Management
Assurance Process Management
Evidence Management
Assurance Case Development
Assurance "Project"
Certification Liaison
Safety Assessment
(Independent) Safety Assessment
Standards Specification
Interpretation
Standards & Regulations Information Management



Evidence and Argumentation Confidence Assessment



Compliance-Aware Engineering Process

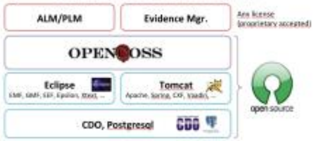


Safety Case-based Compositional Assurance

SEVENTH FRAMEWORK PROGRAMME

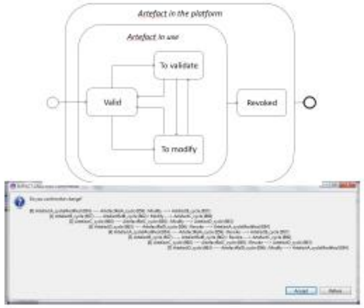
tecnalia Inspiring Business

POLARSYS Open Source Tools for Embedded Systems

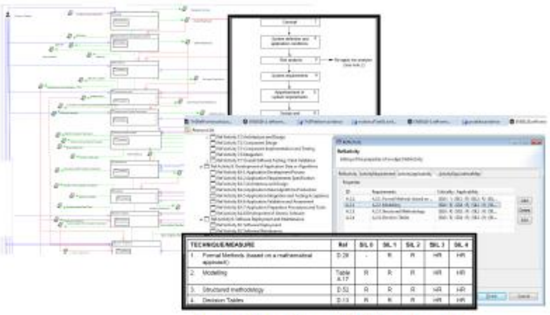

ALM/PLM
Evidence Mgr.
Any license (proprietary accepted)
OPENCOSS
Eclipse
EMF, GMF, EEF, Epsilon, Xtext, ...
Tomcat
Apache, Spring, CXF, Vaadin, ...
CDO, Postgresql
open source

Standard
Feature 1
Feature 2
Feature 3
Feature X
PoB Standard
Objective 1
Objective 2
Objective 3
Objective 4
Objective Z
Standard
Objective Y
Component build with Prescriptive Product Rules
Component build with Prescriptive Process Rules
CROSS-MAPPINGS BETWEEN STANDARDS
ASSURANCE ASSETS TO BE REUSED
COMPLIANCE GAPS (POSTCONDITIONS)
REUSED ASSURANCE ASSETS

Cross-Domain Reuse



Evidence Traceability and Impact Analysis

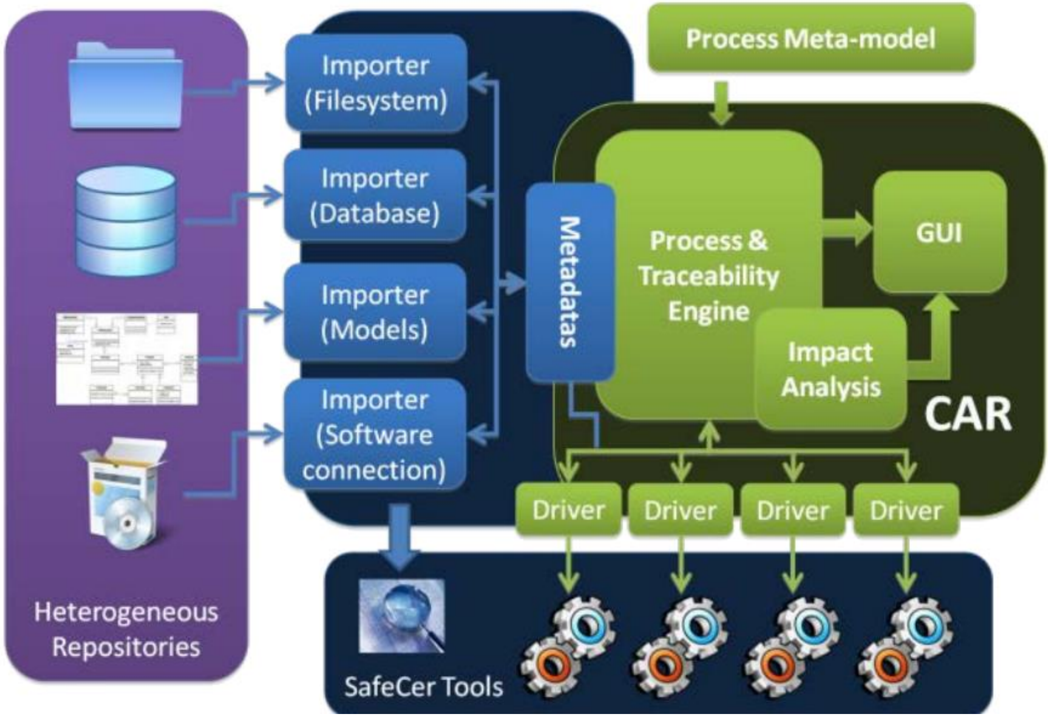


Specification of Standards, Rules and Regulations

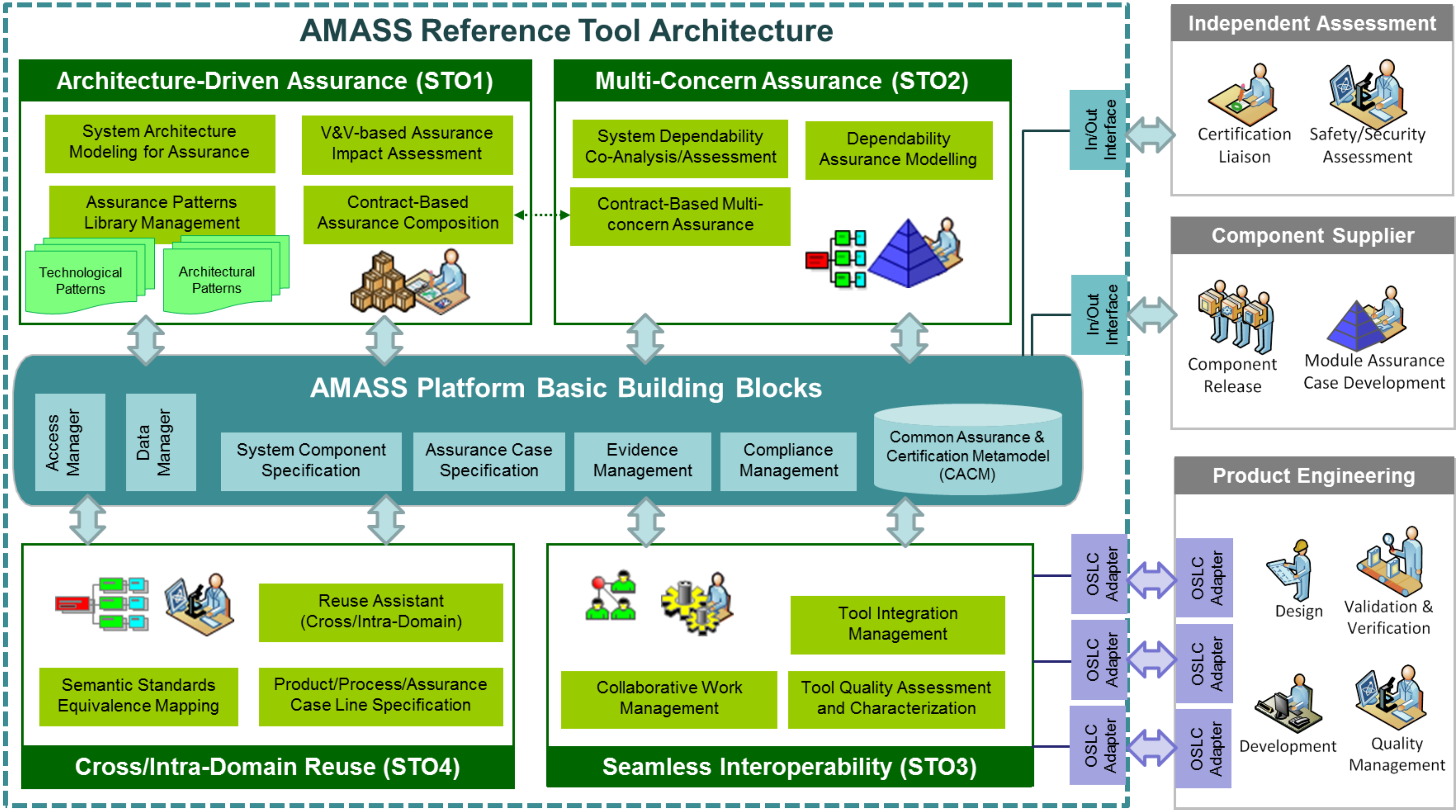
www.opencoss-project.eu

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

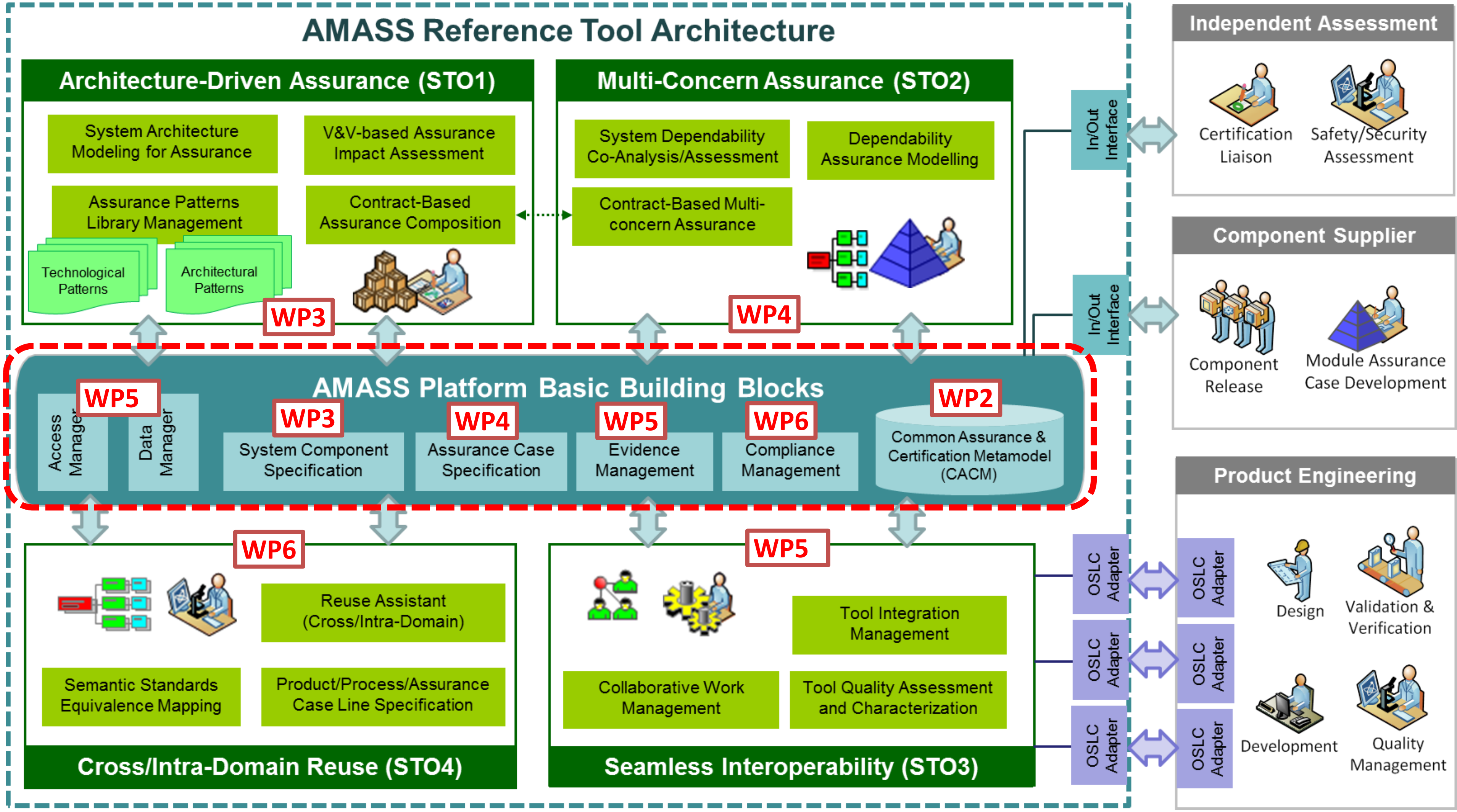


AMASS Reference Tool Architecture



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)
Reuse Assistant (Cross/Intra-Domain)
Semantic Standards Equivalence Mapping
Product/Process/Assurance Case Line Specification
Cross/Intra-Domain Reuse (STO4)
Tool Integration Management
Collaborative Work Management
Tool Quality Assessment and Characterization
Seamless Interoperability (STO3)
In/Out Interface
In/Out Interface
OSLC Adapter
OSLC Adapter
OSLC Adapter
Independent Assessment
Certification Liaison
Safety/Security Assessment
Component Supplier
Component Release
Module Assurance Case Development
Product Engineering
OSLC Adapter
OSLC Adapter
OSLC Adapter
Design
Validation & Verification
Development
Quality Management

High-Level AMASS 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

WP3

Multi-Concern Assurance (STO2)

System Dependability Co-Analysis/Assessment

Dependability Assurance Modelling

Contract-Based Multi-concern Assurance

WP4

AMASS Platform Basic Building Blocks

WP5

Access Manager

Data Manager

WP3

System Component Specification

WP4

Assurance Case Specification

WP5

Evidence Management

WP6

Compliance Management

WP2

Common Assurance & Certification Metamodel (CACM)

WP6

Reuse Assistant (Cross/Intra-Domain)

Semantic Standards Equivalence Mapping

Product/Process/Assurance Case Line Specification

Cross/Intra-Domain Reuse (STO4)

WP5

Tool Integration Management

Collaborative Work Management

Tool Quality Assessment and Characterization

Seamless Interoperability (STO3)

In/Out Interface

In/Out Interface

OSLC Adapter

OSLC Adapter

OSLC Adapter

Independent Assessment

Certification Liaison

Safety/Security Assessment

Component Supplier

Component Release

Module Assurance Case Development

Product Engineering

OSLC Adapter

OSLC Adapter

OSLC Adapter

Design

Validation & Verification

Development

Quality Management

Technical Objectives (1/2)

WP3 - SYSTEM ARCHITECTURE-DRIVEN ASSURANCE

- Architectural patterns for Assurance (AUTOSAR, IMA)
- Seamless link to System Modeling (Behavior, Safety, Security, Timing,…)
- Reinforce Component Contract-based Approach, including requirements refinement, safety analysis, and verification based on formal methods.
- Formalize behavioral & safety requirements to enable automatic validation (assess if we will merge with previous one or state its relation)
- Assurance of Specific Technology: NoC, Multicore, Reconfigurable (FPGA)

WP4 - MULTICONCERN ASSURANCE

- Multi-concerns Assurance Cases (dependability, ~~costs~~, etc.)
- Dependability: <u>Security + Safety</u> + maintainability, availability, reliability
  - → holistic approach for risk levels
  - → how to combine safety and security assurance processes, and how to apply them integrated in a development/assurance process
- Extension of Compositional approach for multi-concern assurance

Technical Objectives (2/2)

WP5 - SEAMLESS INTEROPERABILITY

- Tool Integration (e.g. OSLC). Consider Crystal as basis
- Integration with CHESS, WEFACT
- Collaborative work (seamless support for tool stakeholders from the whole supply chain)
- Quality/Assessment package to assess external tools integrated with AMASS.

WP6 - CROSS-DOMAIN AND INTRA-DOMAIN REUSE

- Consolidate OPENCOSS and SafeCer Cross-Domain and Intra-Domain Reuse approaches
- Semantic cross-domain mappings
- Cross-domain and intra-domain assurance process validation
- Cross-system Reuse using the contract-based approach
- *Combine Product lines w/ safety-oriented process lines and safety case lines*
- *[Standard’s text analysis for compliance management] → Evaluate if we will remove*

Project Schedule

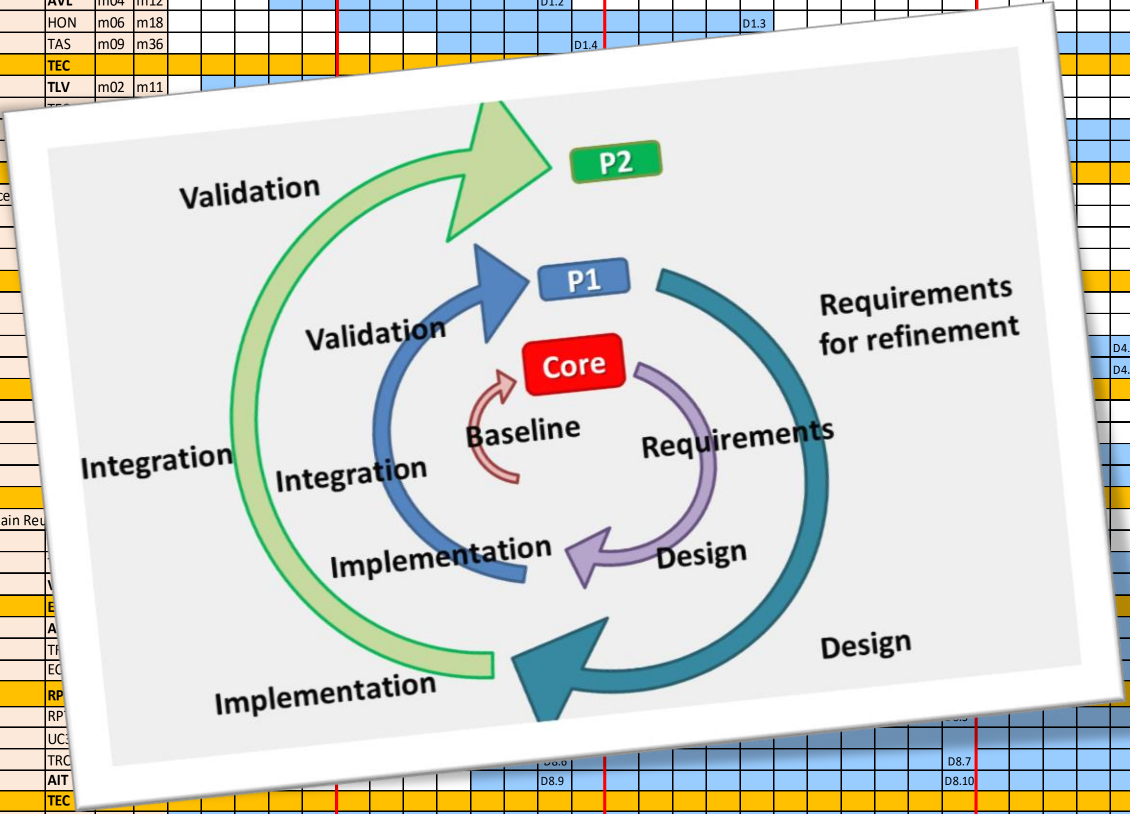
WP	WP/Task Title	Leader	Start	End	m01	m02	m03	m04	m05	m06	m07	m08	m09	m10	m11	m12	m13	m14	m15	m16	m17	m18	m19	m20	m21	m22	m23	m24	m25	m26	m27	m28	m29	m30	m31	m32	m33	m34	m35	m36
WP1	**Case Studies and Benchmarking**	**TAS**																																						
T1.1	Case Study Specification	**VIF**	m01	m08								D1.1																												
T1.2	Case Study Data Collection	**AVL**	m04	m12												D1.2																								
T1.3	Benchmarking Framework	HON	m06	m18																		D1.3																		
T1.4	Case Study Implementation and Benchmarking	TAS	m09	m36													D1.4																					D1.6		D1.7
WP2	**Reference Architecture and Integration**	**TEC**																																						
T2.1	Specification of Business Cases and High-level Requirements	**TLV**	m02	m11																																				
T2.2	AMASS Reference Tool Architecture and Integration	TEC																																						
T2.3	AMASS User Guidance and Methodological Framework																																		D2.5					
T2.4	AMASS Platform Validation																																			D2.8		D2.9		
WP3	**Architecture-driven Assurance**																																							
T3.1	Consolidation of Current Approaches for Architecture-driven Assurance																																							
T3.2	Conceptual Approach for Architecture-driven Assurance																																							
T3.3	Implementation for Architecture-driven Assurance																																							
T3.4	Methodological Guidance for Architecture-driven Assurance																																							
WP4	**Multiconcern Assurance**																																							
T4.1	Consolidation of Current Approaches for Multi-Concern Assurance																																							
T4.2	Conceptual Approach for Multi-Concern Assurance																																							
T4.3	Implementation for Multi-Concern Assurance																														D4.6							
T4.4	Methodological Guidance for Multi-Concern Assurance																														D4.8							
WP5	**Seamless Interoperability**																																							
T5.1	Consolidation of Current Approaches for Seamless Interoperability																																							
T5.2	Conceptual Approach for Seamless Interoperability																																							
T5.3	Implementation for Seamless Interoperability																															D5.6						
T5.4	Methodological Guidance for Seamless Interoperability																															D5.8						
WP6	**Cross-Domain and Intra-Domain Reuse**																																							
T6.1	Consolidation of Current Approaches for Cross-Domain and Intra-Domain Reu																																							
T6.2	Conceptual Approach for Cross-Domain and Intra-Domain Reuse																																							
T6.3	Implementation for Cross-Domain and Intra-Domain Reuse																																D6.6					
T6.4	Methodological Guidance for Cross-Domain and Intra-Domain Reuse	V																															D6.8					
WP7	**Industrial Impact and Community Building**	**E**																																						
T7.1	Networking and Coordination of External Advisory Board	**A**																																						
T7.2	Industrial Adoption Outreach Program	TI																																					D7.2	
T7.3	Building and Coordination of AMASS Open-Source Community	EC																																	D7.7				
WP8	**Exploitation, Dissemination and Standardization**	**RP**																																						
T8.1	Exploitation	RP																																		D8.4			
T8.2	Dissemination	UC3																																						
T8.3	Training	TRC												D8.6												D8.7												D8.8
T8.4	Standardization	**AIT**												D8.9												D8.10												D8.11
WP9	**Project Management**	**TEC**																																						
T9.1	Project Coordination	TEC	m01	m36						D9.2												D9.3												D9.4						
T9.2	Quality and Risk Management	TEC	m01	m36			D9.1																																	

M1
Project Inception

M2
First Prototype:
Core AMASS Platform
Validated in Laboratory

M3
Second Prototype:
Full AMASS Platform
Validated in Laboratory

M4
Final Prototype:
Full AMASS Platform Validated
in Relevant Environment



THANKS!

ANY QUESTIONS?