AMASS

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

WP8 Exploitation, Dissemination and Standardization

Objective: To ensure take up of AMASS results

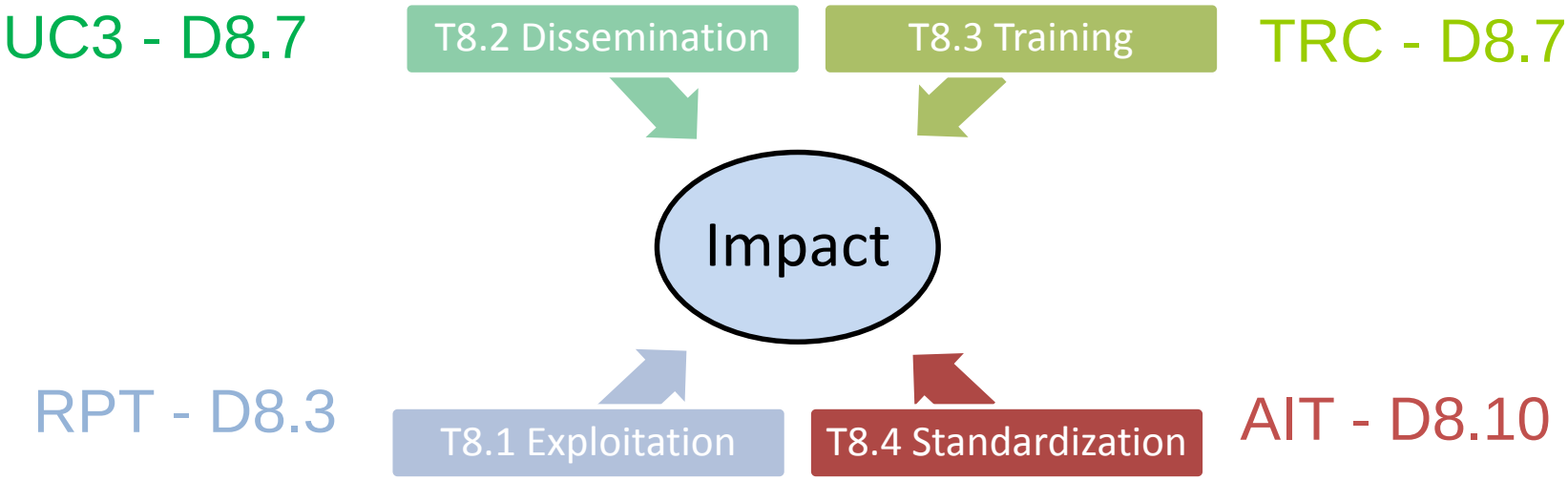
2nd EAB Workshop
Västerås, September 17, 2018

Ran Bi
WP8 Leader
RAPITA SYSTEMS LTD

WP structure and aims/summary of deliverable

- Dissemination means & collaboration platform maintained and further developed
- Videos and YouTube channel
- Organisation of conferences
- Increased number of publications

- Development team P1 tech training
- Industrial partner training
- Videos and presentations



- Overall Exploitation strategy
- Individual plan
- IPR log
- Opportunities and results log

Multi-concern issues put forward in:

- Generic Functional Safety Standards
- Automotive Safety and Cybersecurity
- Smart Manufacturing
- Human factors and safety
- Robotics
- IoT
- OMG Assurance Framework

2nd year achievements

- Dissemination

Items	Achievements
Publications	24 (41)
Events	31 (57)
Social media	50+ actions
Other materials	4 main elements
Audience	2,000+ people

- Standardization

Items influenced	Achievem.
Safety & Cybersecurity	5
Automotive (ISO TC22)	3
OMG (SysA, SACM2.0)	2
IoT, Smart Manufacturing	3
Robotic (ISO TC299)	2

- Training

Items	Achievements
Internal training	5 (12) training sessions
Recorded training video	9.5+ (23.5) hours
External training	9 (27) Research training activities

- Exploitation

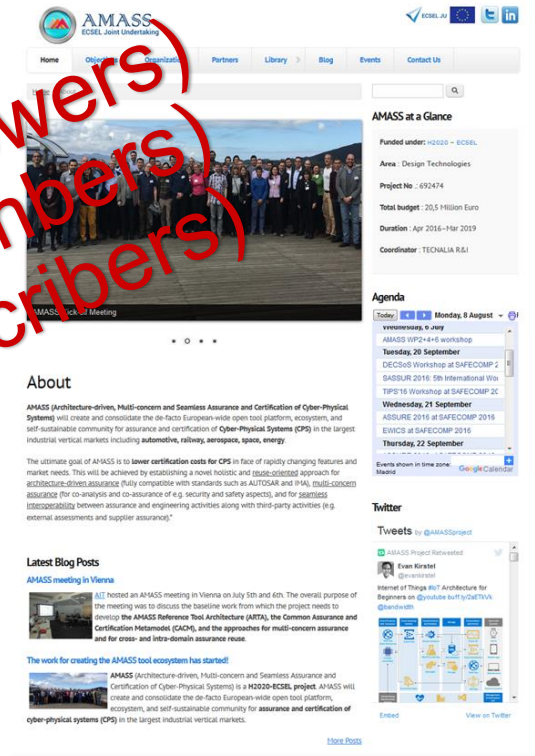
Items	Achievements
Background IP	2 (30)
Foreground IP	5 (21)
Exploitation	6 (19) activities

Notes: Figures are achievements in 2nd Year;
(Figures) are totals including 1st and 2nd years.

Dissemination highlights in D8.7

- On-line
  - Website (http://www.amass-ecsel.eu/)
  - Blog and events calendar
  - Twitter (@AMASSproject)
  - LinkedIn group
  - AMASS YouTube channel
- Off-line
  - Leaflet, Presentations
  - Newsletters 2
  - Publications 24
  - Events 31
  - Posters 1

8000+ visits
~40 items
39 (123 followers)
12 (270 members)
13 (34 subscribers)



Dissemination highlights in D8.7

HOME VIDEOS PLAYLISTS CHANNELS DISCUSSION ABOUT

MarketingVideoAMASSOpenCert

225 views • 4 months ago

AMASS is an EU-funded project in which 29 organizations from 8 countries collaborate, with the support of 16 influential advisory board members from industry and academia. AMASS is creating and consolidating the OpenCert tool platform, as well as its self-sustaining community for assurance and certification of Cyber-Physical Systems (CPS).

AMASS Training PLAY ALL

AMASS Prototype P1 WP3 Session#1

OpenCert

40 views • 4 months ago

AMASS Prototype P1 WP3 Session#2

OpenCert

17 views • 4 months ago

AMASS Prototype P1 WP4 Session#1

OpenCert

43 views • 4 months ago

AMASS Prototype P1 WP4 Session#2

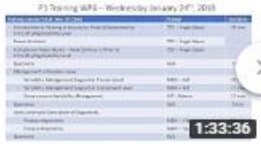
OpenCert

16 views • 3 months ago

AMASS Prototype P1 WP5 Session

OpenCert

13 views • 4 months ago



AMASS Prototype P1 WP6 Session

OpenCert

11 views • 4 months ago

AMASS Prototype PLAY ALL

AMASS Protype "Core"

OpenCert

129 views • 5 months ago

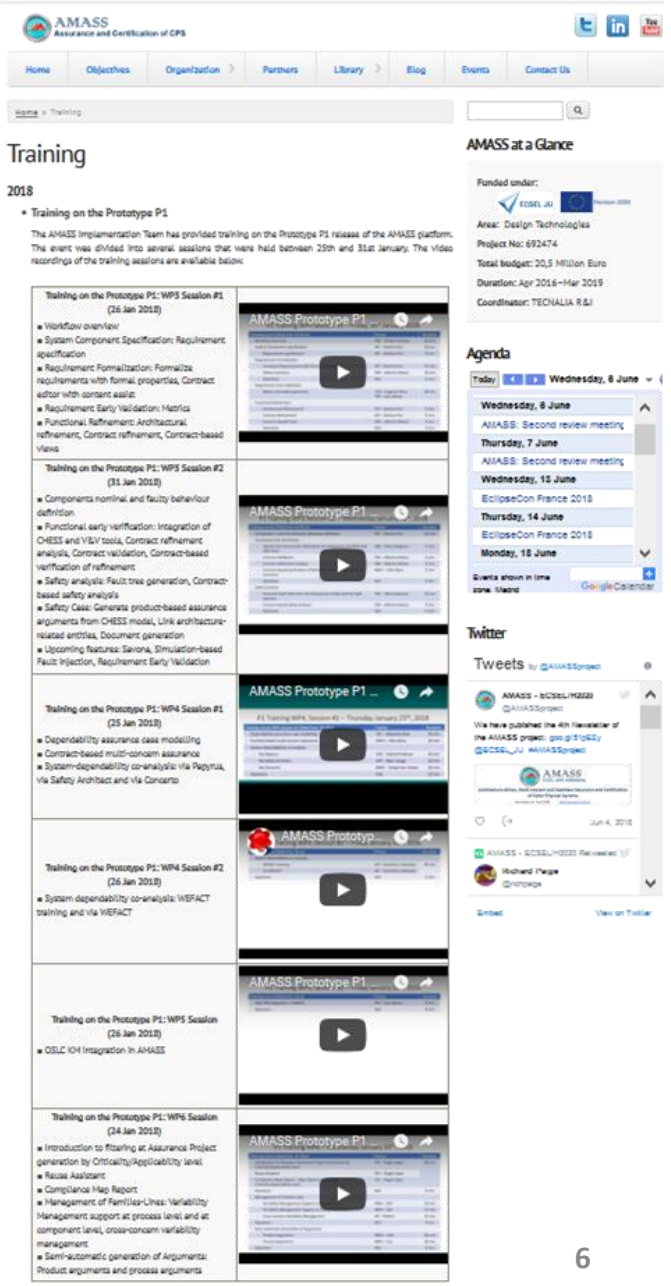
MarketingVideoAMASSOpenC

OpenCert

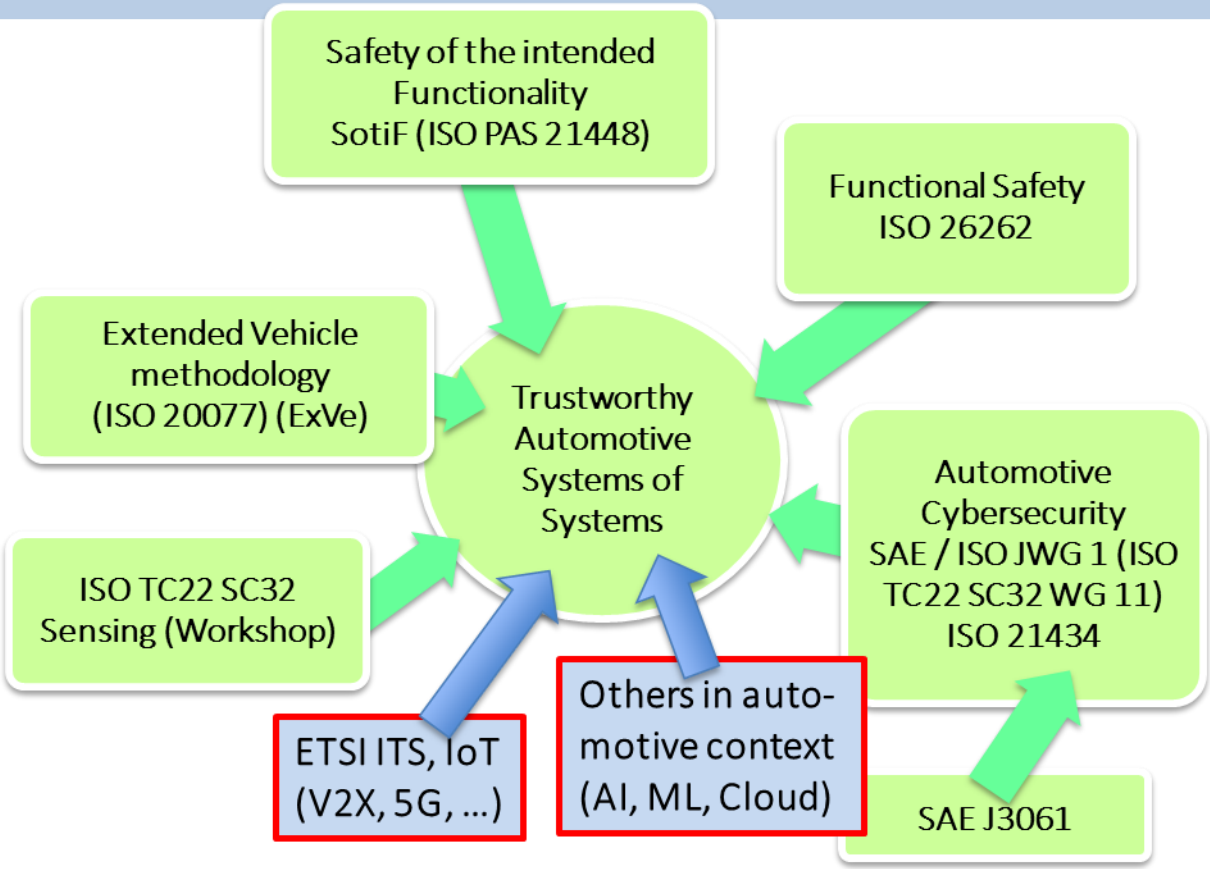
226 views • 4 months ago

Training highlights

- **Focus on internal training**
  - Training page on AMASS website and video links to YouTube, https://www.amass-ecsel.eu/content/training
  - Training on the P1 Prototype: how to use the new features within the AMASS P1 Prototype in difference with the Core Prototype from the previous year.
- **External training based on research training:**
  - 18 BSc, MSc and PhD.
  - 3 public presentations.
  - 9 internal research trainings.



Standardization highlights (ongoing and new work items)



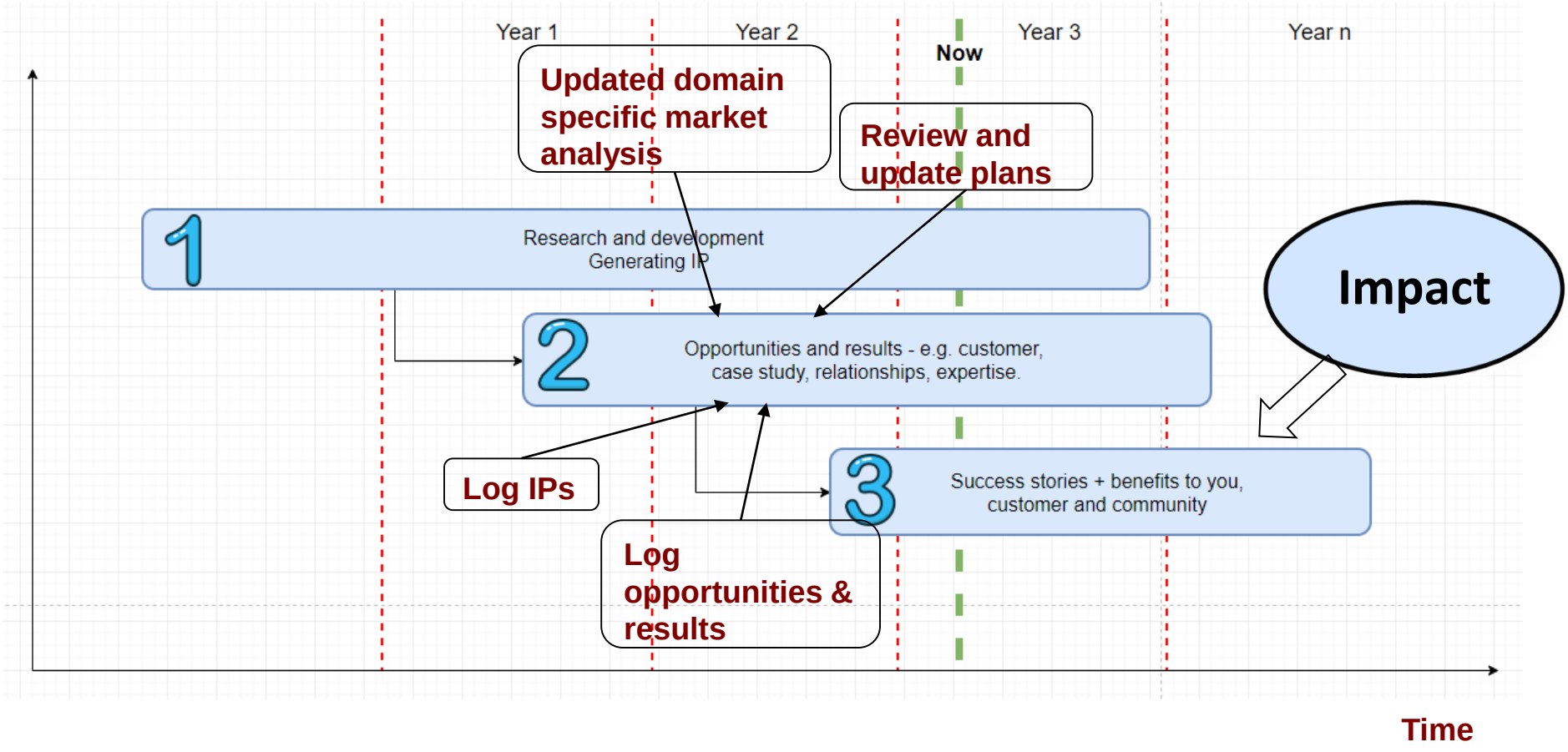
- **ISO 26262**, Ed. 2.0: consider security aware safety issues → successful inclusion in Part 2 (Safety Management), Part 4 (Product Development), Part 6 (Software Development) in FDIS
- **ISO 21434 "Road Vehicles – Cybersecurity Engineering": ISO/SAE JWG1 (ISO TC22 SC 32 WG 11)**
- **ISO TC22 SC31: security issues in connected cars, extended vehicles, NEW: Ad-Hoc Group Automated Driving (ISO ADAG, 2018), NEW Work Items: Sensor Interfaces, Automated Driving**
- **ETSI ITS, smartM2M (AIOTI), ISO Stds. Cloud Security**

Standardization highlights

NEW: IEC TC65 Ad Hoc Groups – Safety, Reliability, Cybersecurity, Smart Manufacturing, Human Factors, … (Examples) – Multi-concern Assurance!

- **IEC 61508-3** Ed 3.0 preparation: Security aware safety guidelines –consideration in part 1 and 2 agreed → **IEC 61508-1/2: Joint Task Force on Safety & Cybersecurity**
- **IEC TC65 AHG1 – now WG 20: "Framework for functional safety and cybersecurity – IEC TR 63069**
- **IEC TC65 AHG2 – now WG 22: "Reliability of Automation Devices and Systems",** looking at the demand of reliability design, test, verification and operational life of (safety related) automation devices for system integration "Assurance of automation devices reliability data and specification of their source" → **IEC TS 63164-1**
- **IEC TC65 AHG3: "Smart Manufacturing Framework and System Architecture"** addresses the issues of highly interconnected industrial automation systems for smart manufacturing in a multi-concern manner **(RAMI4.0) → Task Force "Safety & Cybersecurity"**
- **Task Force "Standards Landscape" → JWG21 ISO TC184/IEC TC65 AHG3, Smart Manufacturing Reference Models**
- **NEW: IEC SC65A WG18, IEC 63187 "Functional safety - Critical E/E/PE systems for defence industry applications" – under "System of interest – safety/security assessment" (June 2018!)**
- **IEC SC65E** (Devices and integration in enterprise systems) **AHG1 "Smart manufacturing information models"** (enterprise management systems from top level down to devices),
- **IEC SC65A WG 17: Human factors – Functional Safety (IEC TR 62879) → security issues to be integrated! (ref. ISO 27002)**

Exploitation progress



IPR and Exploitation Opportunity & Results log

Intellectual Property Register

Item No.	Intelectual Property Owner	Intelectual Property Type*	Intelectual Property Description**	Date Intellectual Property created	Paten, Trademark or Design No. (Denote 'A' for Application or 'G' for Granted No. as applicable)
3	AMT	Foreground IP	medini analyze model of automotive case studies		Copyright/Know-How
4	AMT	Foreground IP	Technology Experiments (source code) for collaborative engineering		Copyright/Know-how
5	AMT	Foreground IP	Requirements and Business cases for collaborative engineering		Know-how
6	AMT	Foreground IP	medini analyze connection to OpenCert		Copyright/Know-how
7	AMT	Foreground IP	Approach for cross-doamin and intra-domain re-use based on SysML libraries		Copyright/Know-how
16	FBK	Foreground IP	Eclipse Plugins for Architecture-driven Assurance		Copyright/Know-How
21	INT	Foreground IP	CHESS extensions for integration with OpenCert		Copyright/Know-How
25	MDH	Foreground IP	Automated and formal compliance checking	since 2016	Copyright / Know-how
31	TRC	Foreground IP	Creation of Papyrus connector for TRC tools	Since 2016	Copyright / Know-how
32	TRC	Foreground IP	Creation of Rhapsody connector for TRC tools	Since 2016	Copyright / Know-how
33	TRC	Foreground IP	Creation of structured-information file connector for TRC tools	Since 2016	Copyright / Know-how
35	UC3	Foreground IP	OSLC KM 2.0 specification	Since 2016	Know-how
36	TRC, UC3	Foreground IP	OSLC connectors of the AMASS Platform	Since 2017	Know-how
37	UC3, TRC	Foreground IP	Semantics-based models of assurance standards	Since 2017	Know-how
38	UC3, TRC	Foreground IP	Artefact Quality Analysis features	Since 2017	Copyright / Know-how
39	UC3, TRC	Foreground IP	System artefact search engine	Since 2017	Copyright / Know-how
43	TRC	Foreground IP	System Interoperativity Manager - AMASS plugin	Since 2018	Copyright/Know-How
44	TRC	Foreground IP	Creation of SQL Query connector for TRC tools	Since 2017	Copyright / Know-how
47	ALT	Foreground IP	Alten Car	Since 2017	Copyright/KnowHow
48	ALT	Foreground IP	Farkle AMASS	Since 2017	Copyright/knowHow
51	A4T	Foreground IP	Interface between Safety Architect and Cyber Architect	Since 2018	Copyright/ Know-How
52	MDH	Foreground IP	Anti-Sisyphus -further development: implementation via integration with BVR Tool and addition of impact analysis capabilities	2017	Copyright/Know-How
53	B&M	Foreground IP	TESTONA - Test Design Tool using the Classification Tree Method	Since 2006	Copyright/Know-How
55	B&M	Foreground IP	SAVONA - System Modelling & Specification Tool	Since 2018	Copyright/Know-How

IPR and Exploitation Opportunity & Results log

Exploitation Opportunities and Results

Owner	Description	Benefits to partner or community	Activity type	Status/Note
RPT	Activity engaging with customers on needs for v&v service contract	Reduce testing cost	Individual	Q4: C/C++ support and RPF V1.3
RPT	Evaluation for Rapita tools with OHB current process.	Integration with Matlab and reducing cost on testing for OHB; Future licence revenue for RPT	Cluster	Q4: Initial contact/introduction
CEA	Evaluation of CEA tools on railway engineering process	Increase the TRL of CEA tools.	Cluster	Q4: Initial contact/introduction
CEA	Definition of safety and security co-analyses tools/methods and methodologies based on Papyrus	Ensure the relevance and adequacy of CEA functional safety and cybersecurity tools to industry needs	Cluster	Q4: Initial contact/introduction
HON	Integration of data-symbolic C/C++ model checking using DIVINE from Masaryk University, integration of requirement analysis tools, integration of V&V tools from FBK	Reduced development cost, reduced number of development cycles, improved quality	Cluster	Q4: plan negotiated with tool providers (UOM, FBK)
CLS	Use of Frama-C (CEA) on code generated for railway applications	Ensure the relevance and adequacy of CEA formal verification tools to industry needs; improved quality; diversification of certification assets.	Individual	Q4: Proof of concept
INT	Evaluate how CHESS toolset can provide support design and safety assessment to then support assurance needs.	Ensure the relevance and adequacy of CHESS to industry needs.	Cluster	Q4:Initial contact/introduction
AMT	For the automotive case studies there will be medini analyze example models	demonstrate benefit of AMASS results to tool user community	Individual	
AMT	The demonstrators will showcase the potential of web based collaboration patterns in safety analysis	This will be used for in-house exploitation and later on influence general tool development strategy	Individual	
GMV	Evaluating the convenience of using Papyrus/CHESS as SysML/UML tool instead other commercial tools	Reduce costs in software licenses	Individual	Initial evaluation
TLV	Evaluate how AMASS tool can provide safety and security assessment in the RTU development process	Reduce effort and cost in safety/security certification process.	Individual	Initial evaluation
MDH	Investigation of a unified approach for systematic reuse and variability management-->tool support for Anti-Sisyphus. Initial application of the approach to OHB case study	Cost and time reduction	Individual (at the moment, INT and TEC will be involved later)	
MDH	Investigation of logic-based reasoning. Initial application of the approach to automotive standards.	In a long term, cost and time reduction related to compliance checking	Individual	
MDH	In initial application of the approach to the automotive domain	Cost and time reduction	Individual	
MDH	Design or model transformations. In initial application of the approach to the avionics domain	Cost and time reduction	Individual	
TRC	Evaluating the introduction of TRC Tools in the engineering tool ecosystem of the Use Cases by Alstom and B&M	Cost and time reduction	Cluster	Initial contact
TRC	Transfer of results from AMASS to the current TRC commercial products	Tool enhancement	Individual	Initial evaluation
A4T	Tool integration for Safety and Security co-analysis	Partners can import their system models from CHESS to Safety Architect, activate Safety&Security viewpoint in safety architect, reuse security analysis artifatcs from Cyber Architect to Safety Architect for safety and security co-analysis.	Cluster	demonstrator available
UC3	Definition of collaboration agreements or contracts with companies for UC3 results transfer	New incomer and collaboration projects	Individual	
TEC - B&M	Joint exploitation of Savona and Sabotage for Design of Automated Driving E/E systems	Tool enhancement	Join	Initial evaluation
AMT	Technology for the analysis and query of data at the server side on safety project content (elasticsearch, Kibana)	Multiple purpose technology - application for example to find information back in many safety projects or to increase consistency among different safety projects	Cluster	initial demonstrator available
AMT	Tool integration for the usage of system (SysML) models for safety analysis. Focus on seamless integration. Application of QVT technology	Customers could use their system models for safety analysis more user friendly by seamless import (including graphical information) and round-trip support	Individual	demonstrator available

Next steps in WP8

- Dissemination:
  - Journal publications (joint ones)
  - Organised workshops and conferences:

    SASSUR, DECSoS, WAISE, SAFECOMP, ICSR, QUATIC, SPLC…
- Training:
  - 1 Major Training on the AMASS second prototype
  - 7 External training courses
- Standardization:
  - Evolution of the SACM standard
  - Safety & Cybersecurity issues in various ISO and IEC standards – ongoing task in maintaining standards and for evolving new (domain) standards
  - Continue engaging with certification authorities
- Exploitation:
  - Success stories from case studies

Thank you for your attention!

Any questions