ECSEL Research and Innovation actions (RIA)

AMASS

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

AMASS solution benchmarking

D1.7

Work Package:	WP1 Case Studies and Benchmarking
Dissemination level:	PU = Public
Status:	Final
Date:	15th May 2019
Responsible partner:	Isaac Moreno (Thales Alenia Space - Spain) Gorka Lendrino (Thales Alenia Space - Spain)
Contact information:	Gorka.Lendrino@thalesaleniaspace.com Isaac.Moreno@thalesaleniaspace.com
Document reference:	AMASS_D1.7_WP1_TAS_V1.0

This deliverable is part of a project that has received funding from the ECSEL JU under grant agreement No 692474. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and from Spain, Czech Republic, Germany, Sweden, Italy, United Kingdom and France.

Contributors

Names	Organisation
Isaac Moreno, Gorka Lendrino	Thales Alenia Space – Spain (TAS)
Garazi Juez, Estibaliz Amparan, Cristina Martínez, Angel López, Alejandra Ruiz	TECNALIA Research & Innovation (TEC)
Elena Alaña, Javier Herrero	GMV Aerospace and Defence, S.A.U (GMV)
Fredrik Warg, Martin Skoglund	RISE Research Institutes of Sweden (SPS)
Benito Caracuel, David Pampliega	Schneider Electric (TLV)
Anna Carlsson	OHB Sweden (OHB)
Barbara Gallina	Maelardalen Hoegskola (MDH)
Thomas Gruber, Abdelkader Shabaan	Austrian Institute of Technology (AIT)
Helmut Martin, Robert Bramberger, Bernhard Winkler	Virtual Vehicle (ViF)
Thierry Lecomte	ClearSy (CLS)
Oliver Kreuzmann, Markus Grabowski	Assystem Germany GmbH (B&M)
Bernhard Kaiser, Nino Gabriel	ANSYS Medini Technologies AG (KMT)
Jose Luis de la Vara, Jose Maria Alvarez, Anabel Fraga, Roy Mendiete, Miguel Rozalen, Eugenio Parra	Universidad Carlos III de Madrid (UC3)
Luis Alonso, Borja Lopez, Elena Gallego, Roy Mendieta	The REUSE Company (TRC)
Camile Parillaud, Fabien Belmonte	Alstom Group (ALS)
Vít Koksa, Tomáš Kratochvíla	Honeywell International (HON)
Norbert Bartsch, Vladislav Gribov	Lange Research Aircraft GmbH (LAN)

Reviewers

Names	Organisation
Thomas Gruber	AIT Austrian Institute of Technology (AIT)
Stefano Puri	Intecs (INT)
Cristina Martínez (Quality Manager)	TECNALIA Research & Innovation (TEC)
Barbara Gallina (TC Review)	Maelardalens Hoegskola (MDH)

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

This deliverable (D1.7) reports the application of the AMASS Evaluation Framework already defined in previous deliverable (D1.3 Evaluation Framework and Quality Metrics [1]) to the results of the Case Studies Implementation (D1.6 AMASS demonstrators (c) [2]). It provides some assessment of the development methodology and runtime implementation of the case studies over the AMASS platform. Thus, the document contains the benchmarking exercise, comparing results achieved thanks to AMASS with former state of the art for reference case studies.

The AMASS evaluation framework is based on the Goal-Question-Metric (GQM) approach. The AMASS benchmarking has been driven by project goals, including gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort; and reuse of assurance results (qualified or certified before raise of technology innovation and sustainable impact in CPS industry).

This deliverable contains a condensed view on all evaluation results from the third and final AMASS Platform Prototype P2, as well as some conclusions and recommendations for improvement.

1. Introduction

1.1 Scope and Purpose

The document is the result of the benchmarking exercise done in the task 1.4. The objective of T1.4 is to validate the AMASS solution and provide feedback for future enhancements. The inputs for this task are: the benchmarking framework from the task T1.3 and the case study specification from the task T1.1.

The purpose of this deliverable is reporting the assessment of the development methodology and runtime implementation of the industrial case studies over the AMASS Platform. Each case study will present an assessment of the Platform, and the results will be discussed, harmonized and reported.

This deliverable also compares results achieved thanks to AMASS with the former state of the art for the reference case studies.

1.2 Relationship with other deliverables

This deliverable is the result of applying the metrics defined in deliverable D1.3 [1] to the different case studies, whose implementation is described in the deliverable D1.6 [2].

1.3 Structure of the document

The rest of the deliverable is structured as follows:

- Section 2 provides an overview on how the evaluation framework and the case studies have been implemented.
- Section 3 includes a detailed description of the measures collected from all AMASS case studies and provides a summary of the results from all case studies in order to support the project goals.
- Section 4 shows the conclusions derived from the benchmarking task.

2. Background

2.1 AMASS Evaluation Framework

The AMASS common evaluation framework defined for the CSs is described in D1.3 [1], where the full set of metrics to be used in the present document is defined and mapped to AMASS general goals. This approach has allowed to measure the degree of achievement of these goals.

Results quantification is based on manually measured metrics. However, most of the metrics can be obtained directly from the tool results itself, while the ones related to effort quantification will depend on human estimations.

These metrics have been individually selected for each CS, which has particular goals. The mapping to AMASS goals was also performed in D1.3 [1]. In some cases, there are some deviations from the initial metrics plan, mainly due to changes between the original demonstrator and its final practical implementation. These deviations are indicated in the applicable metrics tables.

2.2 AMASS Case Study Implementation

Details on final CS implementation can be found in D1.6 [2].

The metrics obtained for each CS that have been reported in this deliverable are aligned with the final CS demonstrator implementation.

3. Case Study Metrics

In the following sections, the metrics gathered for each of the AMASS CSs are presented. Each section will follow this organization:

- Benchmarking approach.
- Applicable metrics results (classified in Common, WP-related and CS-specific metrics).
- CS conclusions and AMASS goals fulfilment.

The tables below contain the definition of the quality metrics and their assignment to the AMASS goals as documented in D1.3 [1].

3.1 Case Study 1: Industrial Automation domain: Industrial and Automation Control Systems (IACS)

3.1.1 Approach for CS1 Benchmarking

The metrics for CS1 have been measured according to the approach recommended by D1.3 [1].

The metrics are calculated with the following conditions:

- Each metric is composed of sub-metrics which relate to parts and tools of the AMASS Platform used in the case study. Sub-metrics are weighed together using an estimation of each sub-metric relative importance.
- Since each sub-metric is related to activities performed in the case study which are affected by the used tools, the value of improvement for each metric reflects only the improvement of these activities, and not all assurance related activities needed in a project. Only the OpenCert, MORETO and FMVEA tools are used in the metrics.
- Most of the metrics are based on qualitative indicators – none, very low, low, medium, high, very high, full – since meaningful quantitative values have been difficult to obtain. It would require comparison of projects with the same scope (performed with and without the AMASS Platform) which is beyond the scope of this case study. Hence accuracy of the metrics is not possible to calculate.
- Qualitative indicators are based on a rationale. The qualitative indicators have then been converted to quantitative values according to Table 1, which is the same assessment method as used in D1.3 [1].

Table 1. Qualitative indicators

Qualitative indicator	Quantitative value
None	0%
Very low	10%
Low	30%
Medium	50%
High	70%
Very high	90%
Full	100%

3.1.2 Common metrics

Table 2. CS1 Common metrics

Common Metric	Value	Comment
M1	50%	*Automated architecture-driven and multi-concern assurance* Reduce effort needed for architecture-driven and multi-concern assurance by automation of the activities. This metric calculates the ratio of automated assurance effort (measured in person-time or cost) versus the total assurance effort (as if no automation was performed). It measures actual assurance effort reduction by automating or semi-automating some part of the assurance process. Automated effort for CS1 consists on: • System component specification (MORETO) • System architecture modelling (MORETO, FMVEA) • System dependability do-analysis (FMVEA) • Assurance, evidence and compliance management (OpenCert)
M4	50%	*Architecture-driven assurance results and architecture-driven certification/qualification results reused* This metric calculates the ratio of reused architecture-driven results from different systems, to the total architecture-driven assurance results for the target system. Architecture-driven results reuse for CS1 consist on: • Architectural patterns for assurance (MORETO)
M5	50%	*Multi-concern assurance results and multi-concern certification/qualification results reused* This metric calculates ratio of reused multi-concern assurance results for two different systems, out of the total multi-concern assurance results for the same systems. Multi-concern assurance results reuse for CS1 consists on: • System dependability co-analysis, rules reuse (FMVEA)
M14	30%	*Identified risks related to architecture-driven assurance* This metric is calculated as the ratio of the risks automatically identified based on architecture-driven assurance, out of all the risks. Identification of risks automatically for CS1 consists of: • The RTU analysis is conducted automatically and based on rules (MORETO/FMVEA)

3.1.3 WP3 metrics

Table 3. CS1 WP3 metrics

WP3 Metric	Value	Comment
MW3.4	6	*Number of V&V activities automatically supported* V&V activities automatically supported for CS1 consists of: • V&V activities relate here to proving sufficient fulfilment of system qualities (quality attribute or standard-conformance). • MORETO provides this proof by 3 activities: 1. security analysis 2. IEC 62443 conformance check 3. IEEE 1686 conformance check • FMVEA provides this proof by 3 entangled activities: 1. security analysis 2. safety analysis 3. performance analysis Summarizing, overall six V&V activities are supported in CS1.

3.1.4 WP4 metrics

Table 4. CS1 WP4 metrics.

WP4 Metric	Value	Comment
MW4.3	3	*Number or share of automatically generated evidences (solutions) for multi-concern arguments* Evidences automatically generated for CS1 consists of: • OpenCert: Evidence management • MORETO: These evidences relate to proving the fulfilment of sub-goals, or requirements, i.e. the non-violation of rules corresponding to IEC 62443 or IEEE 1686. Several rules were defined and evaluated in CS1, and no additional evidences were added manually. • FMVEA: These evidences relate to proving the fulfilment of sub-goals, or requirements, i.e. the non-violation of rules defined in the FMVEA tool. Several rules were defined and evaluated in CS1, and no additional evidences were added manually.

3.1.5 WP5 metrics

Not applicable for CS1.

3.1.6 WP6 metrics

Table 5. CS1 WP6 metrics

WP6 Metric	Value	Comment
MW6.2	70%	*Product-related Reusability (PrR): extent of reusability of a specific product in a product line* Reusability in CS1 consists of: • System Component Specification (MORETO). System components can be reused in MORETO Model Editor • System architecture modelling (MORETO, FMVEA). Model elements can be reused in MORETO and FMVEA • System dependability co-analysis (FMVEA). Rules can be reused in FMVEA. • Evidence and assurance management (OpenCert)

3.1.7 CS1 specific metrics

Table 6. CS1 specific metrics

CS1 Metric	Value	Comment
MC01.1	50%	*Automation of architecture-driven safety and security assurance process for the RTU* Automated effort for CS1 consists of: • System component specification (MORETO) • System architecture modelling (MORETO, FMVEA) • System dependability co-analysis (FMVEA) • Assurance, evidence and compliance management (OpenCert)
MC01.2	50%	*RTU compliance management effort* For CS1 consists of: • Compliance management (OpenCert)
MC01.3	50%	*Effort for determining the level of compliance of the RTU respect to the standards selected*

CS1 Metric	Value	Comment
		For CS1 consists of: • Compliance management (OpenCert)
MC01.4	50%	*Effort for running safety/security analysis of the RTU* For CS1 consists of: • System dependability co-analysis (FMVEA)
MC01.5	70%	*Reuse of security and safety assurance results for other RTU platforms* Reuse (other platforms) for CS1 consists of: • Evidence and assurance management (OpenCert) • Architectural patterns for assurance (MORETO). Reuse of patterns. • System dependability co-analysis (FMVEA). Reuse of rules.
MC01.6	70%	*Security and safety assurance reuse in RTU upgrade* Reuse (RTU upgrade) for CS1 consists of: • Evidence and assurance management (OpenCert) • Architectural patterns for assurance (MORETO). Reuse of patterns for assurance process • System dependability co-analysis (FMVEA). Reuse of rules.
MC01.7	50%	*Reusing architecture-driven assurance results for RTUs* Architecture-driven results reuse for CS1 consists of: • Architectural patterns for assurance (MORETO). Reuse of assurance results that is achieved by reusing the rules of the security standards.
MC01.8	30%	*Reduce the effort for identifying safety and security assurance risks for RTUs* Identification of risks for CS1 consists of: • FMVEA performs an automated, model-based safety and security co-analysis. This means that necessary risk mitigation measures for identified risks can be modelled within the FMVEA tool, and the automated analysis started subsequently shows immediately potential adversary effects on the system which violate the rules established for the other quality attribute.
MC01.9	30%	*Reduce the effort for identifying architecture-based assurance risks for RTUs* Identification of risks for CS1 consists of: • MORETO performs an automated, model-based security analysis. This means that necessary risk mitigation measures for identified risks can be modelled within the MORETO tool, and the automated security requirements selected for each component separately. That shows how immediately the potential adversary can be covered by the chosen security requirements.
MC01.10	50%	*Reduce compliance management risks and automated documentation* Compliance risks and documentation for CS1 consists of: • Compliance management (OpenCert)

3.1.8 CS1 conclusions

Table 7 shows how the different metrics collected in this case study support the project goals.

Table 7. CS1 metrics summary.

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	M1 Automated architecture-driven and multi-concern assurance	50%
		MW3.4 number of V&V activities automatically supported	6

Goal	Question	Metric	Value
assurance and certification/qualification effort by 50%.		MW4.3 number or share of automatically generated pieces of evidence (solutions) for multi-concern arguments	3
		MC01.1 Automation of architecture-driven safety and security assurance process for the RTU	50%
		MC01.4 Effort for running safety/security analysis of the RTU	50%
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	MC01.3 Effort for determining the level of compliance of the RTU respect to the standards selected.	50%
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	M4 Architecture-driven assurance results reused	50%
		M5 Multi-concern assurance results reused	50%
	Q9: What is the impact of cross-domain reuse of assurance results?	MW6.2 Product-related Reusability (*PrR_{SF}*) – the extent of reusability of the common components for a specific product while factoring the impact of the product line input costs	70%
	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	MC01.2 RTU compliance management effort	50%
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities	Q6: What is the impact of reusing architecture-driven assurance results?	MC01.7 Reusing architecture-driven assurance results for RTUs	50%
	Q7: What is the impact of reusing multi-concern assurance results?	MC01.5 Reuse of security and safety assurance results for other RTU platforms	70%
		MC01.6 Security and safety assurance reuse in RTU upgrade	70%
	Q9: What is the impact of cross-domain reuse of assurance results?	MW6.2 Product-related Reusability (*PrR_{SF}*) – the extent of reusability of the common components for a specific product while factoring the impact of the product line input costs	70%
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	M14 Identified risks related to architecture-driven assurance	30%
		MC01.9 Reduce the effort for identifying architecture-based assurance risks for RTUs	30%
	Q11: How can multi-concern assurance contribute to the reduction of assurance and certification risk?	MC01.8 Reduce the effort for identifying safety and security assurance risks for RTUs	30%
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	MC01.10 Reduce compliance management risks and automated documentation	50%

The AMASS Platform provides a reduction of time and effort in the RTU assurance process, increasing the level of automation of the activities and allows the reuse of assurance results for RTU upgrade and other RTU platforms.

As a conclusion, the following achievements have been achieved:

- High improvement in the security and safety assurance reuse
- Medium improvement in the architecture-driven and multi-concern assurance by automation of the activities
- Low improvement in reducing effort for identifying risks.

The tools used in this case study are: OpenCert, MORETO and FMVEA.

3.2 Case Study 2: Automotive domain: Advanced driver assistance function with electric vehicle sub-system.

3.2.1 Approach for CS2 Benchmarking

No metrics have been provided by the CS2 case study owner. The AMASS bundle has not been used, only external tools.

3.3 Case Study 3: Automotive domain: Collaborative automated fleet of vehicles.

3.3.1 Approach for CS3 Benchmarking

The process followed in CS3 for providing the metrics for the benchmarking was detailed in the deliverable D1.3 [1]. There have been no deviations from that process.

3.3.2 Common metrics

Table 8. CS3 Common metrics

Common Metric	Value	Comment
M1	458% increase	*Automated architecture-driven and multi-concern assurance* 58.46%: Due to the automation of quality analysis in requirements and models, the 58.46% of the effort has been decreased. 400%: Ontology evolution management: Automated ontology evolution management tasks.
M2	26	*Identification of consequences of CPS architecture on assurance and on certification/qualification* 26 issues are detected in the requirements and model quality analysis.
M4	260% increase	*Architecture driven assurance results and architecture driven certification/qualification results reused* 30%: Semantic artefact representation: amount of artefact information reused thanks to semantic artefact representation. 30%: Semantic artefact search: amount of artefact information that can be searched with semantic artefact search. 200: Ontology evolution management: amount of ontology information reused through ontology evolution management.

Common Metric	Value	Comment
M6	26	*Identification of architecture-based assurance risks* 26 issues are detected in the requirement and model quality analysis.
M8	95%	*Addressing architecture-based assurance risks* 20%: It is estimated that the feature for quality evolution analysis can increase the issue detection effectiveness/reduce issue detection effort by 20%. 75%: Ontology evolution management: effort to address ontology issues with ontology evolution management.
M12	400% increase	*Assurance results reused across domains* 200%: Ontology evolution management: amount of ontology information reused through ontology evolution management. 200%: Semantic representation of standards: semantic representation information reused across domains.
M14	26	*Identified risks related to architecture-driven assurance* 26 issues are detected in the requirements and model quality analysis.
M16	26	*Discovered unknown risks related to architecture-driven assurance* 26 issues are detected in the requirements and model quality analysis.
M23	400% increase	*Identified risks related to cross-domain assurance* 200%: Ontology evolution management: correctly identified ontology issues with ontology evolution management. 200%: Semantic representation of standards: correctly identified semantic representation-based issues.
M24	200% increase	*Mitigated risks related to cross-domain assurance* Ontology evolution management: mitigated ontology issues with ontology evolution management.
M25	400% increase	*Discovered unknown risks related to cross-domain assurance* 200%: Ontology evolution management: newly discovered ontology issues with ontology evolution management. 200%: Semantic representation of standards: newly discovered semantic representation-based issues.
M31	30% increase	*Assurance result types with seamless interoperability support* Automatic generation of OSLC KM connectors: number of assurance result types through automatic generation of OSLC KM connectors.
M32	25% decrease	*Common means for cross-domain assurance* Semantic artefact representation: effort for artefact information reuse with semantic artefact representation.
M33	300%	*Common cross-domain assurance needs met*

Common Metric	Value	Comment
	increase	Semantic representation of standards: features for semantic representation of standards used in several domains.
M38	290% increase	*Certification/qualification results reused* 30%: Automatic generation of OSLC KM connectors: amount of certification/qualification information reused through automatic generation of OSLC KM connectors. 30%: Semantic artefact representation: amount of artefact information reused thanks to semantic artefact representation. 30%: Semantic artefact search: amount of artefact information that can be searched with semantic artefact search. 200%: Ontology evolution management: amount of ontology information reused with ontology evolution management.

3.3.3 WP3 metrics

Table 9. CS3 WP3 metrics

WP3 Metric	Value	Comment
MW3.4	58.46%	*Number of V&V activities automatically supported* About 58.46% of effort for architecture-driven and multi-concern assurance is automated.

3.3.4 WP4 metrics

Not applicable to CS3.

3.3.5 WP5 metrics

Table 10. CS3 WP5 metrics

WP5 Metric	Value	Comment
MW5.4	30% increase	*Tool interoperability domains: number of artefact types for which some tool interoperability means exists* Automatic generation of OSLC KM connectors: artefact types supported through automatic generation of OSLC KM connectors.
MW5.5	30% increase	*Tool connectors: number of available tool connectors* Automatic generation of OSLC KM connectors: number of connectors created through automatic generation of OSLC KM connectors.
MW5.6	30% increase	*Inter-connected tools: number of inter-connected tools* Automatic generation of OSLC KM connectors: number of inter-connected tools through automatic generation of OSLC KM connectors.

3.3.6 WP6 metrics

Not applicable to CS3.

3.3.7 CS3 specific metrics

Not applicable to CS3.

3.3.8 CS3 conclusions

Table 11 shows how the different metrics collected in this case study support the project goals.

Table 11. CS3 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	M1 Automated architecture-driven and multi-concern assurance	458.46%increase
		MW3.4 number of V&V activities automatically supported	58.46%
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	M2 Automated identification of consequences of CPS architecture on assurance	26
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	M4 Architecture-driven assurance results reused	260% increase
	Q4: How can the effort for identifying issues in architecture-driven and multi-concern assurance be reduced?	M6 Identification of architecture-based assurance risks	26
	Q5: What impact can the early identification of the above issues have on design efficiency?	M8 Addressing architecture-based assurance risks	95% reduction
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities	Q6: What is the impact of reusing architecture-driven assurance results?	M4 Architecture-driven assurance results reused	458.46% increase
	Q8: What is the impact of reusing certification/qualification results?	M38 Certification and qualification results reused	290% increase
	Q9: What is the impact of cross-domain reuse of assurance results?	M12 Assurance results reused across domains	400% increase
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q13: How can cross-domain assurance contribute to the reduction of assurance and certification risk?	M23 Identified risks related to cross-domain assurance	200% increase
		M24 Mitigated risks related to cross-domain assurance	200% increase
		M25 Discovered unknown risks related to cross-domain assurance	200% increase
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and	Q16: How can seamless interoperability contribute to sustainable impact?	M31 Assurance result types with seamless interoperability support	30% increase
		MW5.4 Tool interoperability domains: number of artefact types	30% increase

Goal	Question	Metric	Value
interoperability of assurance and certification/qualification technologies by 60%		for which some tool interoperability means exist	
		MW5.6 Inter-connected tools: number of inter-connected tools	30% increase
	Q17: How can cross-domain assurance contribute to sustainable impact?	M32 Common means for cross-domain assurance	25% decrease
		M33 Common cross-domain assurance needs met	300% increase
	Q18: How can AMASS eco-system contribute to sustainable impact?	MW5.5 Tool connectors: number of available tool connectors	30% increase

Even though no WP4 specific metrics have been provided, the impact on multi-concern management is reflected in some of the common metrics such as M1, M2, M4 or M3. The AMASS approach has been very beneficial identifying potential risk at early development phases which results in a cost and effort reduction.

Another important point to be mentioned is that a variety of tools are interoperating in a transparent way reducing the risk of duplicating work or introducing inconsistencies.

3.4 Case Study 4: Space domain: Design and safety assessment of on-board software applications in Space System

3.4.1 Approach for CS4 Benchmarking

The details about the CS4 demonstrator implementation can be found in the document D1.6 [2].

This section contains the values and the rationales for the metrics defined in the document D1.3 [1]. Those metrics are used for evaluating the AMASS Platform.

3.4.2 Common metrics

Table 12. CS4 Common metrics

Common Metric	Value	Comment
M4	6	*Architecture-driven assurance results and architecture-driven certification/qualification results reused* 1) Architectural patterns 2) Requirements 3) Requirements formalization (contracts/Formal properties) 4) System/SW architecture 5) V&V results 6) Evidences

3.4.3 WP3 metrics

Table 13. CS4 WP3 metrics.

WP3 Metric	Value	Comment

WP3 Metric	Value	Comment
MW3.1	100%	*Percentage of (safety and security) requirements formalized (as contracts)* All the safety requirements defined to test the AMASS functionalities.
MW3.4	7	*Number of V&V activities automatically supported* 1) Consistency check of formal properties 2) Model checking 3) Contract-based verification of state machines 4) Contract-refinement verification/contracts refinement view 5) Contract-based verification of strong/weak contracts 6) FTA-FMEA 7) Contract-based safety analysis
MW3.5	1	Number of applied architectural patterns
MW3.8	100%	*Percentage of requirements verified by V&V analysis* (by using contracts-based design approach).
MW3.9	4	*Percentage of reduction of system design errors* (automatically discovered by using contracts-based design approach). In the CS4, we have found 4 errors in the system design.

3.4.4 WP4 metrics

Not applicable for CS4.

3.4.5 WP5 metrics

Not applicable for CS4.

3.4.6 WP6 metrics

Not applicable for CS4.

3.4.7 CS4 specific metrics

Table 14. CS4 specific metrics

CS4 Metric	Value	Comment
MC04.1	84%	*Percentage of evidences automatically generated from the model-based design using the AMASS platform comparing to the original development process* 1. Identification of main functionalities based on the SW requirements • Yes. Formalization requirements 2. Traceability of functionalities to design entities • Yes. CHESS traceability from requirements to design entities – System/SW architecture 3. SFMEA/FTA table • Yes 4. Failure modes identification • Yes. Safety analyses 5. Identification of recovery actions/mitigation effects, compensation provisions • No 6. Traceability of failure modes to software components • Yes. Results associated to components

MC04.2	4	*Number of software development processes (ECSS-E-ST-40C) implemented using the AMASS Tool Framework.* 4 of 9 processes defined in the ECSS-E-ST-40C have been implemented using the AMASS Tool Framework.

3.4.8 CS4 conclusions

Table 15 shows how the different metrics collected in this case study support the project goals.

Table 15. CS4 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.1 percentage of (safety and security) requirements formalized (as contracts)	100%
		MW3.4 number of V&V activities automatically supported	7
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	Are RAMS issues discovered in early phases of the development? - MC04.1 Number of issues discovered during design phases	84%
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	M4 Architecture-driven assurance results reused	6
		MW3.5 number of applied architectural patterns	1
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities	Q6: What is the impact of reusing architecture-driven assurance results?	In case of changes in the system specification, how many RAMS issues have changed? MC04.2 Ratio of RAMS issues that differ after a system specification change	4
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.8 percentage of requirements verified by V&V analysis (by using contract-based design approach)	100%
	Q5: What impact can the early identification of the above issues have on design efficiency?	MW3.9 percentage of reduction of system design errors (automatically discovered by using contract-based design approach)	4
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	Are RAMS issues discovered in early phases of the development? - MC04.1 Number of issues discovered during design phases	84%

The metrics obtained during the CS4 implementation allow us to conclude that the AMASS Platform is suitable for designing CPS in the space domain:

- It is possible to automate the generation of assurance results and the evidence management
- It is possible to reuse certification/qualification results when changes happen.

- The AMASS Platform is able to accommodate activities described in the processes that the ECSS standard specifies.

A more complete evaluation of the AMASS Platform can be found in the document D1.6 [2].

3.5 Case Study 5: Railway domain: Platform Screen Doors Controller

3.5.1 Approach for CS5 Benchmarking

The process followed for CS5 benchmarking was described in D1.3 [1].

3.5.2 WP3 metrics

Table 16. CS5 WP3 metrics

WP3 Metric	Value	Comment
MW3.1	90%	*Percentage of (safety and security) requirements formalized (as contracts)* - some electronics aspects of the demo remain human-based MW3.1 was obtained by comparing the number of requirements expressed in the specification document and the number of contracts formalized in the formal models.
MW3.8	100%	*Percentage of requirements verified by V&V analysis (all functional properties)* MW3.8 was obtained by counting the number of proved formalized contracts over the total number of formalized contracts.

3.5.3 WP4 metrics

Table 17. CS5 WP4 metrics

WP4 Metric	Value	Comment
MW4.1	Not evaluated	*Number of design iterations required when applying combined multi-concern engineering methods in relation to those needed with traditional separate treatment of concerns* No multi-concern engineering performed during the project. The focus was on safety.

3.5.4 WP5 metrics

Table 18. CS5 WP5 metrics

WP5 Metric	Value	Comment
MW5.3	Not evaluated	*Common collaboration means: number of technologies that can be applied to several collaboration scenarios* No collaboration scenario was assessed during the project.

3.5.5 CS5 specific metrics

Table 19. CS5 specific metrics

CS5 Metric	Value	Comment
CS5.1	30%	*Effort spent on assurance activities* - not measured directly – model reuse 30% CS5.1 was measured by estimated the modelling parts reused from one formal model to another.

3.5.6 CS5 conclusions

Table 20 shows how the different metrics collected in this case study support the project goals.

Table 20. CS5 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.1 percentage of (safety and security) requirements formalized (as contracts)	90%
		CS5.1 Effort spent on assurance activities	30%
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.8 percentage of requirements verified by V&V analysis (by using contract-based design approach)	100%

CS5 has been focused on applying the architecture-driven approach, getting benefit from a more formal design so as to reduce the time in V&V analysis which is one of the costliest activities in the development process. The AMASS approach has been applied in most of the case study scope with a good response providing the capability to automate certain activities that were done manually before as it has been detailed in D1.6 [2].

Globally, the AMASS approach has demonstrated its adequacy for the safety analyses of CLEARSY railways systems as it is able to handle 90% of the requirements and to formally verify 100% of them. Analyses were performed a posteriori (on the existing COPPILOT system – already certified - during year one) and a priori (on the CLEARSY Safety Platform SK (starter kits) 0 and 1 – certification to come on the final product – during year two and three). 30% model reuse (between SK0 and SK1) was also well appreciated, that could foreshadow a sensible cost saving when certifying a product family. The final assessment will be provided in Q3/Q4 2019 with the evaluation of the CLEARSY Safety Platform certification kit by Bureau Veritas.

3.6 Case Study 6: Railway domain: Automatic Train Control Formal Verification

3.6.1 Approach for CS6 Benchmarking

The benchmarking approach in CS6 was detailed described in detail in D1.3 [1]. Outcomes of this process are described in the following sections.

3.6.2 Common metrics

Table 21. CS6 Common metrics

Common Metric	Value	Comment
M2	75%	*Automated identification of consequences of CPS architecture on assurance* Three out of the four existing interfaces have been modelled and their consequences on assurance have been analysed through the B models.
M6	75%	*Identification of architecture-based assurance risks* Three of the four interfaces are safety-related and are therefore linked to a specific risk each.
M8	100%	*Addressing architecture-based assurance risks* Three out of the three critical interfaces have been analysed relating to the Automatic

Common Metric	Value	Comment
		Protection management function risks.
M10	10%	*Assurance needs met after architecture-driven assurance reuse* It is estimated that the Automatic Protection management function represents about 10% of the total functionalities of the Zone Controller. One global safety property of this function has been proven and can be reused as assumption for the proof of the other functions of the ZC.
M14	33%	*Identified risks related to architecture-driven assurance* One out of three risks related to the ZC has been identified through CS6.
M15	33%	*Mitigated risks related to architecture-driven assurance* Previously identified risk has been mitigated during CS6 implementation.
M16	0%	*Discovered unknown risks related to architecture-driven assurance* No new risk was identified related to architecture-driven assurance.
M26	30%	*Common means for architecture-driven assurance* About 30% of effort can be reduced by using common means for architecture-driven assurance.

3.6.3 WP3 metrics

Table 22. CS6 WP3 metrics

WP3 Metric	Value	Comment
MW3.1	16%	*Percentage of (safety and security) requirements formalized (as contracts)* Out of the 515 requirements included in the specification, 83 have been formalized in the B models, given the fact that only one function was modelled.
MW3.4	1	*Number of V&V activities automatically supported* Specification review can be avoided thanks to the B model proof.
MW3.8	100%	*Percentage of requirements verified by V&V analysis (by using contract-based design approach)* All requirements are automatically verified thanks to the proof of the B models.
MW3.9	60%	*Percentage of reduction of system design errors (automatically discovered by using contract-based design approach)* The verification approach used in CS6 has allowed Alstom to identify 15 investigation requests (still under analysis) that could potentially lead to modifications of the ZC specification. However, since only one of its functionalities was modelled, the percentage of system design errors reduction is not significant. When all functions are modelled, it is estimated that 60% of the design errors can be discovered. This corresponds to 100% of design errors of the part of the system design that is modelled (60%). The errors of the non-modelled part are not discovered.

3.6.4 WP4 metrics

Not applicable for CS6.

3.6.5 WP5 metrics

Not applicable for CS6.

3.6.6 WP6 metrics

Not applicable for CS6.

3.6.7 CS6 specific metrics

Table 23. CS6 specific metrics

CS6 Metric	Value	Comment
MC06.1	Not evaluated	*Cost of formal proof versus functional tests* Due to the late completion of the prerequisites, the refinement between the ZC System B-model and the ZC software B-model could not be performed. Therefore, this metric cannot be computed yet.
MC06.2	30%	*Early detection of safety issues* The formal verification of Alstom's ZC performed during CS6 has led to 15 investigation requests that could potentially be safety-related issues. These investigation requests are still under analysis today, but it is estimated that about 5 of them will lead to modifications in the specification.
MC06.3	80%	*Assurance raise thanks to use of the approach* The new development and verification process of the ZC that was implemented in CS6 has not been assessed by any Independent Safety Assessor yet. It is estimated that the number of ISA remarks related to the specifications can be reduced by around 80% because of the exhaustive verification stemming from the formal verification. However, new remarks will come up relating to the correctness of the level and upper level assumptions used during the modelling phase.
MC06.4	66%	*Reducing qualification effort* Out of the 6 artefacts that were planned to be logged in the AMASS Platform in order to centralize the evidence and thus reduce qualification effort, only 4 were indeed integrated in the Platform.
MC06.5	10%	*Automation of architecture driven assurance* The scope of CS6 was limited to only one safety-related function of the ZC which was "management of the Automatic Protections around the trains". Therefore, only 10% of the properties were automatically generated.

3.6.8 CS6 conclusions

Table 24 shows how the different metrics collected in this case study support the project goals.

Table 24. CS6 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.1 percentage of (safety and security) requirements formalized (as contracts)	16%
		MW3.4 number of V&V activities automatically supported	1
		MC06.3 Assurance raise thanks to use of the approach	80%
		MC06.5 Automation of architecture driven assurance	10%
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	M2 Automated identification of consequences of CPS architecture on assurance	75%
	Q3: How can the effort for documenting architecture-driven	MC06.4 Reducing qualification effort	66%

Goal	Question	Metric	Value
	and multi-concern assurance be reduced?		
	Q4: How can the effort for identifying issues in architecture-driven and multi-concern assurance be reduced?	M6 Identification of architecture-based assurance risks	75%
	Q5: What impact can the early identification of the above issues have on design efficiency?	M8 Addressing architecture-based assurance risks	100%
		MC06.2 Early detection of safety issues	30%
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities	Q6: What is the impact of reusing architecture-driven assurance results?	M10 Assurance needs met after architecture-driven assurance reuse	10%
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	MC06.4 Reducing qualification effort	66%
	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MC06.3 Assurance raise thanks to use of the approach	80%
		MC06.5 Automation of architecture driven assurance	10%
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	M14 Identified risks related to architecture-driven assurance	33%
		M16 Discovered unknown risks related to architecture-driven assurance	0%
	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.8 percentage of requirements verified by V&V analysis (by using contract-based design approach)	100%
		MC06.3 Assurance raise thanks to use of the approach	80%
		MC06.5 Automation of architecture driven assurance	10%
	Q5: What impact can the early identification of the above issues have on design efficiency?	MW3.9 percentage of reduction of system design errors (automatically discovered by using contract-based design approach)	60%
		MC06.2 Early detection of safety issues	30%
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	MC06.4 Reducing qualification effort	66%
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and	Q14: How can architecture-driven assurance contribute to sustainable impact?	M26 Common means for architecture-driven assurance	30%

Goal	Question	Metric	Value
certification/qualification technologies by 60%			

These metrics show that the methodology and process established in this case study along with the use of the AMASS platform (OpenCert) allow a high efficiency to gain in the safety demonstration by automating a certain number of activities and by reusing parts of the demonstration. This can lead to significant costs and time savings; especially as potential safety-related problematics can be discovered earlier than with a traditional design and verification process.

3.7 Case Study 7: Avionics domain: Safety assessment of multi-modal interactions in cockpits

3.7.1 Approach for CS7 Benchmarking

Based on recommended approach by D1.3 [1] and the observations that manually measured metrics have lower accuracy than automatically measured metrics due to human error, most of the metrics were measured automatically. However, some of these measurements were done both automatically and manually in order to estimate the accuracy and increase the confidence in the results.

The tools supporting automated metrics collection were:

- **V&V Manager**

  Stores to the database Linear Temporal Logic requirements, inputs, outputs, requestor of the verification task, ID, verification result, verification server and all times. Therefore, the information on time spent on requirements authoring and V&V, requirements in document, number and type of defects, and cost savings could be inferred.

- **Verification Server**

  Stores the same metrics as verification managers for all clients.

3.7.2 Common metrics

Table 25. CS7 Common metrics

Common Metric	Value	Comment
M1	92%	Automated architecture-driven and multi-concern assurance effort in this case was very high, since that most of the requirements were formal and most of the verification activities were automated.
M14	3	Identified risks related to architecture-driven assurance
M15	3	Mitigated risks related to architecture-driven assurance
M20	3	Identified risks related to seamless interoperability
M21	2	Mitigated risks related to seamless interoperability
M30	2	Common means for seamless interoperability
M31	1	Assurance result types with seamless interoperability support

3.7.3 WP3 metrics

Table 26. CS7 WP3 metrics

WP3 Metric	Value	Comment
MW3.1	100%	Percentage of (safety and security) requirements formalized (as contracts)
MW3.2	3	Number of evidences and claims automatically generated (from contract-based design)
MW3.4	7	Number of V&V activities automatically supported – *ambiguity, inconsistency, redundancy, unrealizability, vacuity, completeness, correctness*
MW3.8	100%	Percentage of requirements verified by V&V analysis (by using contract-based design approach).
MW3.9	13%	Percentage of reduction of system design errors (automatically discovered by using contract-based design approach).

3.7.4 WP4 metrics

Not applicable for CS7.

3.7.5 WP5 metrics

Table 27. CS7 WP5 metrics

WP5 Metric	Value	Comment
MW5.4	5	Tool interoperability domains: number of artefact types for which some tool interoperability means exists - *contracts, inputs, outputs, results, system.*
MW5.5	4	Tool connectors: number of available tool connectors – *V&V Manager, verification server*
MW5.6	6	Inter-connected tools: number of inter-connected tools – *DIVINE, NuSMV, nuXmv, Acacia+, Z3, Remus2*
MW5.7	2	Standardised tool interoperability means: number of standardised or standard-based tool interoperability means – *OSLC Automation, OSLC Performance Monitoring*

3.7.6 WP6 metrics

Not applicable for CS7.

3.7.7 CS7 specific metrics

Table 28. CS7 specific metrics

CS7 Metric	Value	Comment
MC07.1	2 PM	Effort Spent on Development Process
MC07.2	Unknown	Cost of Poor Quality of Development Process – we did not get any estimate from the production department on how much cost of the poor quality was improved.
MC07.3	1	Defect Introduced by Development Process
MC07.4	7	Defect Detected by Development Process
MC07.5	1	Defect Removed by Development Process
MC07.6	24	Total number of requirements
MC07.7	24	Number of formalized requirements
MC07.8	1	Number of components
MC07.9	21	Number of ports
MC07.10	14	Number of passed verified requirements
MC07.11	10	Number of failed verified requirements

CS7 Metric	Value	Comment
MC07.12	1	Number of processes
MC07.13	2	Number of product types
MC07.14	8	Number of tools
MC07.15	9	Number of standards
MC07.16	2	Time to formalize average requirement (in minutes)
MC07.17	330	Saved verification effort by automated formal verification and test generation (in minutes)
MC07.18	91%	Percentage of behavioural requirements formalized

3.7.8 CS7 conclusions

In Table 29 it is shown how the different metrics collected in this case study support to the project goals.

Table 29. CS7 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	M1 Automated architecture-driven and multi-concern assurance	92%
		MW3.1 percentage (safety and security) requirements formalized (as contracts)	100%
		MW3.2 number of pieces of evidence and claims automatically generated (from contract-based design)	3
		MW3.4 number of V&V activities automatically supported	7
		MC07.1 Effort Spent on Development Process	2 PM
	Q5: What impact can the early identification of the above issues have on design efficiency?	MC07.3 Defect Introduced by Development Process	1
		MC07.4 Defect Detected by Development Process	7
		MC07.5 Defect Removed by Development Process	1
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MC07.1 Effort Spent on Development Process	2 PM
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	M14 Identified risks related to architecture-driven assurance	3
		M15 Mitigated risks related to architecture-driven assurance	3
		MC07.2 Cost of Poor Quality of Development Process	Unknown
	Q12: How can	M20 Identified risks related to seamless	3

Goal	Question	Metric	Value
	seamless interoperability contribute to the reduction of assurance and certification risk?	interoperability	
		M21 Mitigated risks related to seamless interoperability	2
	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.8 percentage of requirements verified by V&V analysis (by using contract-based design approach)	100%
		MC07.1 Effort Spent on Development Process	2 PM
	Q5: What impact can the early identification of the above issues have on design efficiency	MW3.9 percentage of reduction of system design errors (automatically discovered by using contract-based design approach)	13%
		MC07.3 Defect Introduced by Development Process	1
		MC07.4 Defect Detected by Development Process	7
		MC07.5 Defect Removed by Development Process	1
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification technologies by 60%	Q16: How can seamless interoperability contribute to sustainable impact?	M30 Common means for seamless interoperability	2
		M31 Assurance result types with seamless interoperability support	1
		MW5.4 Tool interoperability domains: number of artefact types for which some tool interoperability means exist	5
		MW5.6 Inter-connected tools: number of inter-connected tools	6
	Q18: How can AMASS eco-system contribute to sustainable impact?	MW5.5 Tool connectors: number of available tool connectors	4
		MW5.7 Standardised tool interoperability means: number of standardised or standard-based tool interoperability means	2

In CS7, 17 touch gestures have been captured in 24 formal requirements. The formalization of just one requirement took an average of 2 minutes, saving 5 hours on verification effort. As a result of this verification, 2 defective requirements were detected in gesture (un-fireable rules and rules that mask them) and 32 more defects were detected in requirements about control systems (syntactic, IO related, ambiguous, missing, redundant, conflicting, defects).

An 11% reduction in cost saving distribution has been confirmed: from adoption of formal requirement standard (savings on alignment efforts) and 25% more cost reduction from requirement semantic verification and model checking (model checking does not scale well).

3.8 Case Study 8: Automotive domain: Telematics function

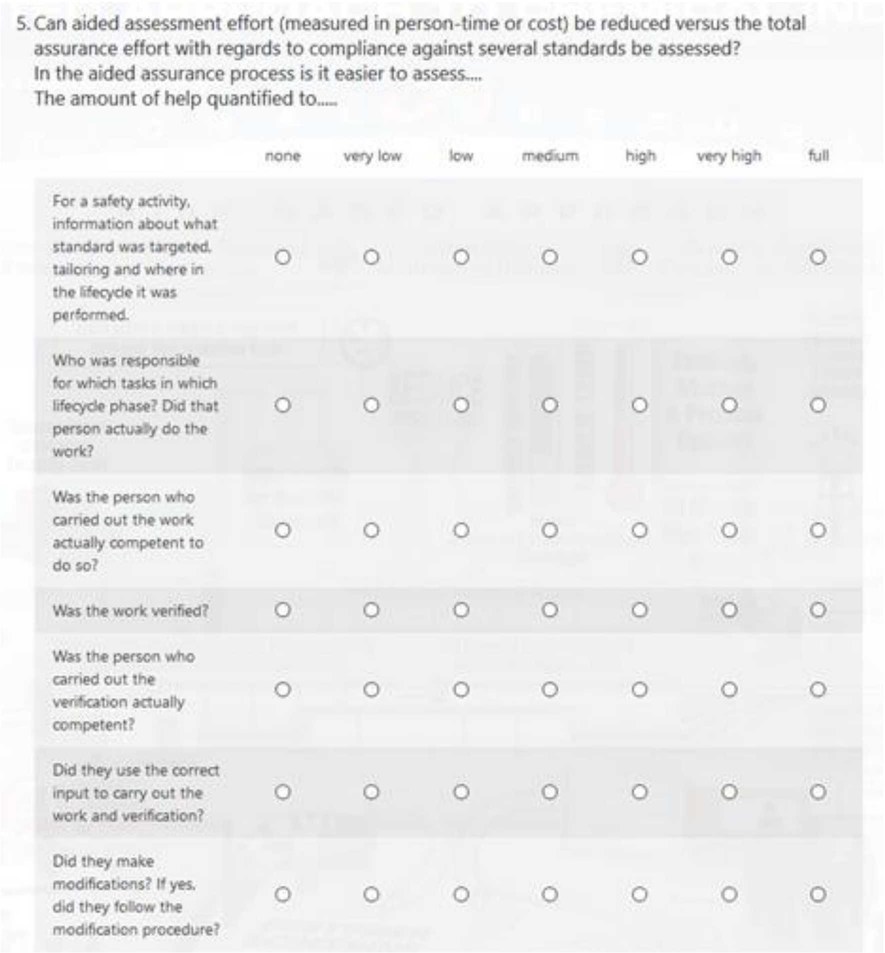
3.8.1 Approach for CS8 Benchmarking

This case study has focused on the common metrics that are related to the issue of multi-concern assurance. For further results of the case study see D1.6 [2]. The metrics have been calculated with the following conditions:

- Each common metric is composed of sub-metrics which relate to parts of the AMASS platform used in the case study. Sub-metrics are weighed together using an estimation of each sub-metric relative importance.
- Since each sub-metric is related to activities performed in the case study which are affected by the used tools, the value of improvement for each metric reflects the improvement of these activities only, and not all assurance related activities needed in a project. Only the OpenCert tool is used in the metrics.
- Most of the metrics are based on qualitative indicators – none, very low, low, medium, high, very high, full – since meaningful quantitative values have been difficult to obtain. It would require comparison of two full projects with the same scope (performed with and without the AMASS platform) which is beyond the scope of this case study. Hence accuracy of the metrics is not possible to calculate.
- Qualitative indicators are based on a rationale. The qualitative indicators have then been converted to quantitative values according to Table 30, which is the same assessment method as used in D1.3 [1].
- A questionnaire with one very experienced assessor is used for contribution from usage scenario 2, multi-concern assessment (i.e. this refers to functional safety assessment and cybersecurity assessment by an independent assessor). The aim was estimating the gain of using OpenCert for an independent assessor compared to the traditional way of getting a stack of paper/pdf documentation. The qualitative indicators were used in the questionnaire, and answers weighed together for use in the common metrics (relevant answers for each metric). Part of the questionnaire is shown in Figure 1 as an example.
- Initially M7 was also part of the evaluation but we could not find a meaningful metric for it.

Table 30. Qualitative indicators

Qualitative indicator	Quantitative value
None	0%
Very low	10%
Low	30%
Medium	50%
High	70%
Very high	90%
Full	100%



5. Can aided assessment effort (measured in person-time or cost) be reduced versus the total assurance effort with regards to compliance against several standards be assessed?
In the aided assurance process is it easier to assess....
The amount of help quantified to.....

	none	very low	low	medium	high	very high	full
For a safety activity, information about what standard was targeted, tailoring and where in the lifecycle it was performed.	○	○	○	○	○	○	○
Who was responsible for which tasks in which lifecycle phase? Did that person actually do the work?	○	○	○	○	○	○	○
Was the person who carried out the work actually competent to do so?	○	○	○	○	○	○	○
Was the work verified?	○	○	○	○	○	○	○
Was the person who carried out the verification actually competent?	○	○	○	○	○	○	○
Did they use the correct input to carry out the work and verification?	○	○	○	○	○	○	○
Did they make modifications? If yes, did they follow the modification procedure?	○	○	○	○	○	○	○

Figure 1. Questionnaire for assessor

3.8.2 Common metrics

Table 31. CS8 Common metrics.

Common Metric	Value	Comment
M1	53%	*Automated architecture-driven and multi-concern assurance* Ratio of automated assurance effort to total assurance effort Unit: Percentage gain from automation for multi-concern assurance
M3	66%	*Automated architecture-driven and multi-concern assurance* Automatically identified consequences of having to address several dependability aspects to the total identified consequences Unit: Percentage automatically identified consequences
M9	0.41	*Addressing multi-concern-based assurance risks* Unit: Ratio of cost of addressing multi-concern assurance risks to cost of not addressing them (e.g. results in cost of rework for later discovery of problem)

Table 32. Rationale for M1

Sub-metric	Evaluation	Weight	Rationale
Project-level tailoring	High (70%)	0.1	Work automated: Generation of the project-specific tailored standard, e.g. by selection of integrity level or applicable parts of the standard. While the project-specific parameters still need to be determined manually, this feature removes the need to manually go through all

Sub-metric	Evaluation	Weight	Rationale
			standard requirements to select and document the project applicable requirements one-by-one. The metric is an estimation made based on experience with both manual and automated tailoring and does not include the not tool-related activity to determine the tailoring.
Impact analysis	High (70%)	0.3	Work automated: Determining which artefacts need to be updated after a change in one artefact. Requires initial work setting up dependencies between artefacts in the evidence model. The efficiency is very dependent on how the artefact structure and dependence rules are set up, e.g. a more fine-grained division of the artefacts together with carefully modelled dependences can reduce manual work later significantly. In an agile setting, updates are frequent which is why the weight of this has been deemed high. The sub-metric refers to the work of identifying impact, not addressing it.
Reuse for new project	Low (30%)	0.1	Work automated: Reuse of assurance models from one project to another. If working component-based with assurance cases for out-of-context elements they tend to have many similarities, i.e. similar set of evidence, same process, similar argumentation, same baseline. Therefore, the gain from reuse of part of the assurance case can be significant. However, adjustments are always needed, and the reuse functionality has some improvement potential. Qualitative indicator evaluation based on testing of reuse functionality.
Automatic generation of argument from reference model	15%	0.1	Work automated: Generation of GSN arguments from reference framework. 30% (low) of effort spent on parts that can be automated, medium (50%) of generated argumentation useful without manual rework, total 0,3*0.5 = 15%. The generated fragments are not enough to constitute a complete argument. However, while the complete structure of the argument is built manually, the generated fragments can be used as leaf claims, connected (as away goals) to various parts of the manually built argument, an example is shown in D1.6 [2], Section 3.8.2.3. The advantage is time saved manually adding all requirements and time saved checking for completeness with respect to the normative requirements (for a conformance case). Example: The ISO 26262 standard (from the case study) contains over 600 normative requirements, 62 method/measure tables and 120 work products (note that not all these may be applicable in all projects). Note that the relatively low value of this sub-metric could be improved by fixing some deficiencies in the generation (see D1.6) which adds manual work to adjust the generated fragments and automating compliance mapping.
Use of argument patterns	Medium (50%)	0.2	Work automated: Aid when building argumentation for a new project by having a library of patterns. When building an argument for compliance to a standard e.g. for a number of out-of-context components, the argumentation is very repetitive and can be done faster and with less errors with a library of established patterns. The metric concerns creating the argument but not e.g. doing the design/requirements work the argument describes.

Sub-metric	Evaluation	Weight	Rationale
Assessment efficiency	50%	0.2	Work automated: Aid for assessor doing functional safety assessment or cybersecurity assessment. This includes functionality like compliance report, compliance mapping and argumentation (linked to evidence) compared to traditional assessments using a pile of documents. Based on questionnaire. Concerns the work of managing the assessment artefacts not the actual reading of documentation.

Weighted average: 53%

Table 33. Rationale for M3

Sub-metric	Evaluation	Weight	Rationale
Work process tailored for multi-concern assurance	70% (high)	0.8	This evaluation is made given the existence of a defined process, baselines and argument patterns for the multi-concern project in OpenCert. Given these, the tool will guide the work so that the consequences are identified (semi-) automatically by following the process. Identified consequences on a coarse level: • Standard req. for interaction between concerns • Dependencies between safety/security goals • Dependencies in functional safety concept safety/security analyses • Dependencies in technical safety concept safety/security analyses • Dependencies in software architecture safety/security analyses • Synergies in test environments • Synergies in test techniques • Synergies in test purposes /test cases • Dependencies for update procedures after start-of-production The sub-metric is qualitatively estimated since a count of total consequences is missing (and from our viewpoint even difficult to define).
Assessment consequences of multi-concern	50%	0.2	Based on questionnaire. Concerns the assessment part of identifying whether multi-concern consequences have been treated correctly.

Weighted average: 66%

Table 34. Rationale for M9

Sub-metric	Evaluation	Weight	Rationale
Fraction of work needed to solve multi-concern related risks early vs. late.	2/5	0.9	Example from case study: Separate safety and security analysis showed initial design with global positioning system receiver enhanced with real-time kinematics (RTK-GPS) and odometry to be sufficient to meet safety goals and cybersecurity goals. However, when the safety goals were considered in the security analysis the solution was insufficient, a security threat (spoofing) could break the safety goal. Hence a redesign adding a new safety mechanism (in this case redundant positioning with ultrawideband was chosen but other alternatives would be possible, too) was necessary with updates to both hardware, software and assurance case. Update work was about half the time compared to the original design (50% extra effort). Cost of addressing the risk earlier is estimated to have been 20% extra effort.
Work saved in assessment by	50%	0.1	Estimate from questionnaire concerning multi-concern assessment.

resolving risks early compared to late (re-assessment needed in part)			

Weighted average: 0.41

3.8.3 CS8 conclusions

Table 35 shows how the different metrics collected in this case study support the project goals.

Table 35. CS8 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	M1 Automated architecture-driven and multi-concern assurance	53%
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	M3 Automated identification of consequences of having to address several dependability aspects	66%
	Q5: What impact can the early identification of the above issues have on design efficiency?	M9 Addressing multi-concern-based assurance risks	0.41

In conclusion the main advantages of using AMASS tools found in CS8 was:

- Reduced effort for assurance activities for multi-concern assurance due to automation and re-use.
- Reduced risk of late discovery of multi-concern dependency problems requiring redesign due to co-assessment workflow supported by OpenCert.
- Reduced functional safety and cybersecurity assessment effort for an independent assessor due to better tracking of assurance progress, traceability and compliance mapping.
- Reduced effort in verification for multi-concern assurance due to re-use of tests between concerns.

3.9 Case Study 9: Air Traffic Management domain: Safety-Critical SW Lifecycle of a Monitoring System for NavAid

3.9.1 Approach for CS9 Benchmarking

In D1.3 [1], the process for benchmarking in the scope of CS9 was described. In the following sections we provide the results of this process.

3.9.2 Common metrics

Table 36. CS9 Common metrics.

Common Metric	Value	Comment
M2	Not evaluated	*Automated identification of consequences of CPS architecture on assurance*
M4	Not evaluated	*Architecture-driven assurance results reused*
M6	Not	*Identification of architecture-based assurance risks*

	evaluated	
M8	20%	*Addressing architecture-based assurance risks* It is estimated that the time needed for creating the complete model and verifying it, is 20% of the time needed to solve the functional and safety issues detected.
M14	4	*Identified risks related to architecture-driven assurance* The evaluation of the total number of risks is not available.
M15	4	*Mitigated risks related to architecture-driven assurance* The evaluation of the total number of risks is not available.
M16	0	*Discovered unknown risks related to architecture-driven assurance* No new risks have been identified.

3.9.3 WP3 metrics

Table 37. CS9 WP3 metrics

WP3 Metric	Value	Comment
MW3.2	2	*Number of pieces of evidence and claims automatically generated (from contract-based design)*
MW3.4	5	*Number of V&V activities automatically supported* 1) Consistency check of formal properties 2) Model checking 3) Contract-refinement verification/contracts refinement view 4) Contract-based verification of strong/weak contracts 5) FTA-FMEA
MW3.9	4	*Percentage of reduction of system design errors (automatically discovered by using contract-based design approach)*
MW3.10	2	*Percentage of reduction of components integration errors (automatically discovered by using contract-based design approach)*

3.9.4 WP4 metrics

Not applicable for CS9.

3.9.5 WP5 metrics

Not applicable for CS9.

3.9.6 WP6 metrics

Not applicable for CS9.

3.9.7 CS9 specific metrics

Table 38. CS9 specific metrics

CS9 Metric	Value	Comment
CS9.1	Not evaluated	*Effort spent on assurance activities* Time needed for certification process compared to previous developments. This metric cannot be evaluated since the certification process did not start yet.
CS9.2	3	*Number of functional issues discovered during design phases* Three functional issues were detected and corrected thanks to the state machine definition of the ECU.

CS9.3	1	*Number of safety issues discovered during design phases* One safety issue was discovered thanks to the contract-based analysis.

3.9.8 CS9 conclusions

Table 39 shows how the different metrics collected in this case study support the project goals.

Table 39. CS9 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.2 number of pieces of evidence and claims automatically generated (from contract-based design)	2
		MW3.4 number of V&V activities automatically supported	5
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	MC09.2 Number of functional issues discovered during design phases	3
	Q5: What impact can the early identification of the above issues have on design efficiency?	M8 Addressing architecture-based assurance risks	20%
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	M14 Identified risks related to architecture-driven assurance	4
		M15 Mitigated risks related to architecture-driven assurance	4
		M16 Discovered unknown risks related to architecture-driven assurance	0
		MC09.3 Number of safety issues discovered during design phases	1
	Q5: What impact can the early identification of the above issues have on design efficiency?	MW3.9 percentage of reduction of system design errors (automatically discovered by using contract-based design approach)	4
		MW3.10 percentage of reduction of components integration errors (automatically discovered by using contract-based design approach)	2
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	MC09.2 Number of functional issues discovered during design phases	3

CS9 has been focused in STO3, Architecture driven assurance. The AMASS approach has been beneficial for system architecture formalization which has improved the effort required for V&V by an early identification of issues. The identification and mitigation of errors in early phases together with the ED-109 standard[1] compliance management has resulted in a more efficient process.

3.10 Case Study 10: Space domain: Certification basis to boost the usage of MPSoC architectures in the Space Market

3.10.1 Approach for CS10 Benchmarking

CS10 demonstrator implementation is described in D1.6 [2]. The rationale how the CS10 metrics have been extracted is explained in the following sections.

3.10.2 Common metrics

Table 40. CS10 Common metrics

Common Metric	Value	Comment
M1	54%	*(Automated architecture-driven effort relative to total effort as if no automation were performed).* Automated effort for CS10 consists on: • SW requirements formalization (formal properties and contracts) • Requirements traceability to architecture functional blocks • Failure modes identification (FTA)
M4	7	*Architecture-driven results reused*: 1) System Definition 2) Requirements Formalization 3) Requirements Early Validation 4) Functional Refinement 5) Component's nominal and faulty behaviour definition 6) Functional Early Verification 7) Model-Based Safety Analysis
M5	1	*Multi-concern results reused*: 1) Multi-concern Contracts Definition (via concern-tagged formal properties)
M6	2	*Number of architecture-based risks identified:* 1) Output ports connected to the same input port. 2) Inner port not exported in the system block.
M7	0	*Number of risks multi-concern-based risks identified*
M8	2	*Number of architecture-based risks addressed* (addressing consists on changing requirements or system model definition to avoid quality risks)
M9	0	*Number of multi-concern-based risks addressed* (addressing consists on changing requirements formalization or contract definition to avoid quality risks)
M26	1	*Common means for architecture-driven assurance*:

[1] EUROCAE ED 109 Software Integrity Assurance Considerations For Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, 1 January 2012, https://standards.globalspec.com/std/1517993/eurocae-ed-109

Common Metric	Value	Comment
		OSLC
M30	1	*Common means for seamless interoperability:* OSLC connector
M31	3	*Assurance result types with seamless interoperability support* Verification server (RQT) reports obtained

3.10.3 WP3 metrics

Table 41. CS10 WP3 metrics

WP3 Metric	Value	Comment
MW3.1	100%	*Percentage of (safety and security) requirements formalized (as contracts)*
MW3.2	4	*Number of evidences and claims automatically generated (from contract-based design)*
MW3.4	7	*Number of V&V activities automatically supported:* 1) CHESS / Validate Contracts for Assurance 2) CHESS / Validate model for NuSMV3 analysis tool 3) CHESS / Validate core constraints 4) Validate model 5) Validate subtree 6) Select constraints and Validate model 7) Select constraints and Validate subtree
MW3.8	100%	*Percentage of requirements verified by V&V analysis (by using contract-based design approach)*
MW3.9	78%	*Percentage of reduction of system design errors (automatically discovered by using contract-based design approach).*
MW3.10	22%	*Percentage of reduction of components integration errors (automatically discovered by using contract-based design approach).*
MW3.11	3	*Number of languages and notations with which the AMASS system component/specification metamodel shares concepts:* 1) SysML 2) OCRA 3) SMV (FTA) With these languages, CS10 model shares concepts.

3.10.4 WP4 metrics

Table 42. CS10 WP4 metrics

WP4 Metric	Value	Comment
MW4.1	50%	*Number of design iterations required when applying combined multi-concern engineering methods in relation to those needed with traditional separate treatment of concerns* NOTE: Considering that 2 concerns are relevant for this CS (Safety and Security), when using the multi-concern feature, it can be assumed that the number of design iterations when using AMASS tool is half of the needed iterations when using traditional separate treatment of concerns, i.e. 50%.
MW4.2	87%	*Reduction of effort for the re-generation of evidences after changing functional/non-functional requirements to the system by using a multi-concern-compliant workflow tool* NOTE: These evidences are time consuming, so usually they are not generated, hand-made, based on user experience or are only generated in the last phases. This is a key goal using AMASS multi-concern-compliant workflow tools. For calculation of this value, it

WP4 Metric	Value	Comment
		has been taken the assumption that changing one requirement in the system would take 1 day of work for re-generation of evidences through manual processes, against 1 hour of work when using AMASS automation.
MW4.4	50%	*An estimation of time needed for separate safety and security engineering process and the co-engineering process.* See MW4.1
MW4.8	2	*Number or share of architectural/design modifications saved by combined safety/security co-engineering* NOTE: First modification due to requirements update in the co-engineering process. Second modification due to add the PUS_FLT in the security engineering.
MW4.9	0	*Number or share of architectural/design modifications saved by combined safety/performance co-engineering*
MW4.10	0	*Number or share of architectural/design modifications saved by combined security/performance co-engineering*
MW4.11	0	*Number or share of architectural/design modifications saved by combined safety/security/performance co-engineering*

3.10.5 WP5 metrics

Table 43. CS10 WP5 metrics

WP5 Metric	Value	Comment
MW5.3	1	*Common collaboration means: number of technologies that can be applied to several collaboration scenarios:* CHESS + CDO scenario
MW5.4	1	*Tool interoperability domains: number of artefact types for which some tool interoperability means exists:* interoperability CHESS + RQT
MW5.6	1	*Inter-connected tools: number of inter-connected tools:* Interconnected CHESS & RQT

3.10.6 WP6 metrics

Not applicable for CS10.

3.10.7 CS10 specific metrics

This section corresponds to metrics relevant to the results obtained in CS10 demonstrator implementation using the AMASS tools, some of which have not been previously defined in D1.3 [1].

Table 44. CS10 specific metrics

CS10 Metric	Value	Comment
MC10.1	17/17	Number of formalized requirements vs total number of requirements
MC10.2	19/47	Number of defined contracts vs number of formal properties
MC10.3*	1	Number of contracts which have been refined (sub-contracts)
MC10.4*	5	Number of contracts supporting multi-concern
MC10.5*	22	Number of formal properties whose concern has been tagged
MC10.6*	2	Number of requirements whose correctness must be improved
MC10.7*	1	Number of requirements whose consistency must be improved

CS10 Metric	Value	Comment
MC10.8*	17	Number of requirements whose completeness must be improved

(*) Updated metrics from the ones stated in D1.3

3.10.8 S10 conclusions

Table 45 shows how the different metrics collected in this case study support the project goals.

Table 45. CS10 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	M1 Automated architecture-driven and multi-concern assurance	54%
		MW3.1 percentage of (safety and security) requirements formalized (as contracts)	100%
		MW3.2 number of pieces of evidence and claims automatically generated (from contracts-based design)	4
		MW3.4 number of V&V activities automatically supported	7
		MW4.1 number of design iterations required when applying combined multi-concern engineering methods in relation to those needed with traditional separate treatment of concerns	50%
		MW4.2 reduction of effort for the re-generation of pieces of evidence after changing functional/non-functional requirements to the system by using a multi-concern-compliant workflow tool	87%
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	MW4.4 an estimation of time needed for separate safety and security engineering process and the co-engineering process	50%
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	M4 Architecture-driven assurance results reused	7
		M5 Multi-concern assurance results reused	1
		MC10.3 Number of contracts which have been refined (sub-contracts) (UPDATED METRIC)	1
		MC10.4 Number of contracts supporting multi-concern (UPDATED METRIC)	5
		MC10.5 Number of formal properties whose concern has been tagged	22
		MC10.6 Number of requirements whose correctness must be improved	1
		MC10.7 Number of requirements whose consistency must be improved	1
		MC10.8 Number of requirements whose completeness must be improved	17
	Q4: How can the effort for	M6 Identification of architecture-based assurance	2

Goal	Question	Metric	Value
	identifying issues in architecture-driven and multi-concern assurance be reduced?	risks	
		M7 Identification of multi-concern-based assurance risks	0
	Q5: What impact can the early identification of the above issues have on design efficiency?	M8 Addressing architecture-based assurance risks	2
		M9 Addressing multi-concern-based assurance risks	0
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.1 percentage of (safety and security) requirements formalized (as contracts)	100%
		MW3.2 number of pieces of evidence and claims automatically generated (from contract-based design)	4
		MW3.4 number of V&V activities automatically supported	7
		MW4.1 number of design iterations required when applying combined multi-concern engineering methods in relation to those needed with traditional separate treatment of concerns	50%
		MW4.2 reduction of effort for the re-generation of pieces of evidence after changing functional/non-functional requirements to the system by using a multi-concern-compliant workflow tool	87%
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	M4 Architecture-driven assurance results reused	7
		M5 Multi-concern assurance results reused	1
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	MC10.1 Estimate number of bugs in the code from static analysis and from dynamic execution of the code.	17/17
		MC10.2 Estimate the number of future failures.	19/47
	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.8 percentage of requirements verified by V&V analysis (by using contracts-based design approach)	100%
	Q5: What impact can the early identification of the above issues have on design efficiency?	MW3.9 percentage of reduction of system design errors (automatically discovered by using contract-based design approach)	78%
		MW3.10 percentage of reduction of components integration errors (automatically discovered by using contract-based design approach)	22%
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	MW4.8 number or share of architectural/design modifications saved by combined safety/security co-engineering	2
		MW4.9 number or share of architectural/design modifications saved by combined safety/performance co-engineering	0

Goal	Question	Metric	Value
		MW4.10 number or share of architectural/design modifications saved by combined security/performance co-engineering	0
		MW4.11 number or share of architectural/design modifications saved by combined safety/security/performance co-engineering	0
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	MC10.6 Number of requirements whose correctness must be improved	1
		MC10.7 Number of requirements whose consistency must be improved	1
		MC10.8 Number of requirements whose completeness must be improved	17
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification technologies by 60%	Q14: How can architecture-driven assurance contribute to sustainable impact?	M26 Common means for architecture-driven assurance	1
	Q16: How can seamless interoperability contribute to sustainable impact?	M30 Common means for seamless interoperability	1
		M31 Assurance result types with seamless interoperability support	3
		MW5.4 Tool interoperability domains: number of artefact types for which some tool interoperability means exist	1
		MW5.6 Inter-connected tools: number of inter-connected tools	1
	Q18: How can AMASS eco-system contribute to sustainable impact?	MW3.11 number of languages and notations with which the AMASS system component/specification metamodel shares concepts	3
		MW5.3 Common collaboration means: number of technologies that can be applied to several collaboration scenarios	1

The tasks that are being evaluated in this document for CS10 are related to architecture-driven design and multi-concern aspects, paying attention to collaborative work and interoperability with external tools to provide system requirements support. For this CS10 we can conclude that there is an important reduced effort compared with the traditional processes, having a considerably lower level of task automation in architecture definition, V&V and product assurance processes.

Regarding the multi-concern aspects, benefits are clear, and not easy to be quantified though, since this AMASS feature supports co-engineering activities, not possible to be traced before.

Especially remarkable for CS10 domain is the integration between the requirements definition phase and their automated verification, which helps to measure and refine their quality and iterate the architecture definition, functional verification and safety analysis.

3.11 Case Study 11: Space domain: Design and efficiency assessment of model-based Attitude and Orbit Control software

3.11.1 Approach for CS11 Benchmarking

In CS11, the process for benchmarking has been documented first in D1.3 [1] and a more detailed process regarding WP6 metrics was published in EuroSPI paper [4].

3.11.2 Common metrics

Table 46. CS11 Common metrics

Common Metric	Value	Comment
M30	2	*Common means for seamless interoperability.* EPF Composer & OpenCert. EPF Composer & BVR Tool.
M31	1	*Assurance result types with seamless interoperability support.* EPF Composer & OpenCert. Compliance Metrics and Compliance argumentation.

3.11.3 WP3 metrics

Not applicable for CS11.

3.11.4 WP4 metrics

Not applicable for CS11.

3.11.5 WP5 metrics

Not applicable for CS11.

3.11.6 WP6 metrics

WP6-specific metrics (Size of commonality and product reusability) were calculated for family of processes by MDH. Results were published in EuroSPI-2018 paper and documented in D6.3 [3] and [4].

3.11.7 CS11 specific metrics

Table 47. CS11 specific metrics

CS11 Metric	Value	Comment
MC11.1	40% decrease	Effort spent on assurance activities. RapiCov provided a gain of 40 % (mean).
MC11.2	0% decrease	The rate of detected and solved issues performing state of practice will be measured and compared to the rate of detected and solved issues measured performing state of the art. • State of practice: GCOV • State of the art: RapiCov The value is 0% because RapiCov and GCOV provided basically the same information. The reason for this is that the method of model-based design and autocoding is setting the rules for a very simplified code. For example, always one statement/line. Hence the GCOV application performs good enough.
MC11.3	Not evaluated	Reuse of contract-based assurance.

MC11.4	20% decrease	Manual work leading to poor quality. Integrated RapiCov to the existing tool chain (MATLAB/Simulink). No reduction of manual work. Used seamless integration of existing functionality in Matlab to seamlessly trace to requirements in DOORs.

3.11.8 CS11 conclusions

Table 48 shows how the different metrics collected in this case study support the project goals.

Table 48. CS11 metrics summary

Goal	Question	Metric	Value
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MC11.1 Effort spent on assurance activities	40%
		MC11.2 Rate of detected and solved issues during test phases	0
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification technologies by 60%	Q16: How can seamless interoperability contribute to sustainable impact?	M30 Common means for seamless interoperability	2
		M31 Assurance result types with seamless interoperability support	1
	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	MC11.4 Manual work leading to poor quality	20%

CS11 has focused on:

- Automatic generation of assurance artifacts (STO3 and STO4)
- Systematic reuse of process and product-based engineering and assurance artifacts. (STO4)
- Seamless link to process modelling (phases, responsibilities, work products etc in compliance with ECSS-Q-ST-80C. (STO3)

The tasks that are being evaluated in this document for CS11 are mainly related to seamless interoperability and intra-domain reuse aspects, paying attention to collaborative work and interoperability with external tools to provide support for system requirements traceability.

Concerning G4, based on the metrics calculated, it emerges that it is not straightforward to demonstrate a a potential sustainable impact in CPS industry since the increased interoperability was concrete but modest.

Concerning G2, based on the metrics calculated by applying the AMASS solution for variability management at process level on academic but illustrative enough set of ECSS processes, it emerges that the potential for reuse is concrete and that the proposed solutions are promising and should be adopted to larger portions of ECSS standards.

It has been a challenge to integrate the AMASS approach into the existing tool and method chain in our state of practice projects. This is because the central tool used for design, analysis, implementation, simulation is Matlab/Simulink.

4. Conclusions

The **overall goals** of AMASS, which are set to improve the current situation in CPS design technologies, are:

- **G1**: to demonstrate a potential gain for design **efficiency** of complex CPS by reducing their assurance and certification/qualification effort by 50%.
- **G2**: to demonstrate a potential **reuse** of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities.
- **G3:** to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification **risks** of new CPS products. The reduction of risks can be "invested" into the risky adoption of new technologies, for which there was no space without the reduction.
- **G4:** to demonstrate a potential sustainable impact in CPS industry by increasing the **harmonization** and **interoperability** of assurance and certification/qualification tool technologies by 60%.

In the "conclusions" sections of each of the case studies, we have described how AMASS has achieved these goals on the different domains and perspective. With regards to common metrics the following table shows the summary of the results.

Table 49. Summary of common metrics

Goal	Question	Metric	CS1	CS3	CS4	CS6	CS7	CS8	CS9	CS10	CS11
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	M1 Automated architecture-driven and multi-concern assurance	50%	58.46%			92%	53%		54%	
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	M2 Automated identification of consequences of CPS architecture on assurance		26 issues detected		75%					
		M3 Automated identification of consequences of having to address several dependability aspects						66%			
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	M4 Architecture-driven assurance results reused	50%	30% increase	6					7 results reused	
		M5 Multi-concern assurance results reused	50%							1 result reused	
	Q4: How can the effort for identifying issues in architecture-driven	M6 Identification of architecture-based assurance risks		26 issues detected		75%				2 risks	

Goal	Question	Metric	CS1	CS3	CS4	CS6	CS7	CS8	CS9	CS10	CS11
	and multi-concern assurance be reduced?	M7 Identification of multi-concern-based assurance risks								0 risks	
	Q5: What impact can the early identification of the above issues have on design efficiency?	M8 Addressing architecture-based assurance risks		20%		100%			20%		
		M9 Addressing multi-concern-based assurance risks						0,41		0 risks	
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification /qualification activities	Q6: What is the impact of reusing architecture-driven assurance results?	M10 Assurance needs met after architecture-driven assurance reuse				10%					
	Q8: What is the impact of reusing certification/qualification results?	M38 Certification and qualification results reused		30% increase							
		M39 Certification and qualification needs met after results reuse									
	Q9: What is the impact of cross-domain reuse of assurance results?	M12 Assurance results reused across domains		200% increase							
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q10: How can architecture-driven assurance contribute to the reduction of assurance and certification risk?	M14 Identified risks related to architecture-driven assurance	30%	26 issues detected		33%	3 risks		4 risks		
		M15 Mitigated risks related to architecture-driven assurance				33%	3 risks		4 risks		
		M16 Discovered unknown risks related to architecture-driven assurance		26 issues detected		0%			0 risks		
	Q12: How can seamless interoperability contribute to the reduction of assurance and certification risk?	M20 Identified risks related to seamless interoperability					3 risks				
		M21 Mitigated risks related to seamless interoperability					2 risks				
	Q13: How can cross-domain assurance	M23 Identified risks related to cross-domain		200% increa							

Goal	Question	Metric	CS1	CS3	CS4	CS6	CS7	CS8	CS9	CS10	CS11
	contribute to the reduction of assurance and certification risk?	assurance		se							
		M24 Mitigated risks related to cross-domain assurance		200% increase							
		M25 Discovered unknown risks related to cross-domain assurance		200% increase							
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification technologies by 60%	Q14: How can architecture-driven assurance contribute to sustainable impact?	M26 Common means for architecture-driven assurance				30%				1 mean	
	Q16: How can seamless interoperability contribute to sustainable impact?	M30 Common means for seamless interoperability					2 means			1 mean	2 mean
		M31 Assurance result types with seamless interoperability support		30% increase			1 result			3 types	1 mean
	Q17: How can cross-domain assurance contribute to sustainable impact?	M32 Common means for cross-domain assurance		25% decrease							
		M33 Common cross-domain assurance needs met		300% increase							

Regarding WP3 metrics, the following table shows the summary of the results.

Table 50. Summary of WP3 metrics

Goal	Question	Metric	CS1	CS3	CS4	CS5	CS6	CS7	CS9	CS10
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.1 percentage of (safety and security) requirements formalized (as contracts)			100%	90%	16%	100%		100%
		MW3.2 number of pieces of evidence and claims automatically generated (from contracts-based design)						3	2	4

Goal	Question	Metric	CS1	CS3	CS4	CS5	CS6	CS7	CS9	CS10
		MW3.4 number of V&V activities automatically supported	6	58,46%	7		1	7	5	7
	Q3: How can the effort for documenting architecture-driven and multi-concern assurance be reduced?	MW3.5 number of applied architectural patterns			1					
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW3.8 percentage of requirements verified by V&V analysis (by using contracts-based design approach)			100%	100%	100%	100%		100%
	Q5: What impact can the early identification of the above issues have on design efficiency?	MW3.9 percentage of reduction of system design errors (automatically discovered by using contract-based design approach)			4		60%	13%	4	78%
		MW3.10 percentage of reduction of components integration errors (automatically discovered by using contract-based design approach)							2	22%
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification technologies by 60%	Q18: How can AMASS eco-system contribute to sustainable impact?	MW3.11 number of languages and notations with which the AMASS system component/specification metamodel shares concepts								3

Regarding WP4 metrics, the following table shows the summary of the results.

Table 51. Summary of WP4 metrics

Goal	Question	Metric	CS1	CS10
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/qualification effort by 50%.	Q1: How can the effort for architecture-driven and multi-concern assurance be automated?	MW4.1 number of design iterations required when applying combined multi-concern engineering methods in relation to those needed with traditional separate treatment of concerns		50%
		MW4.3 number or share of automatically generated pieces of evidence (solutions) for multi-concern arguments	3	
	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	MW4.4 an estimation of time needed for separate safety and security engineering process and the co-engineering process		50%
G3: to demonstrate a potential raise of technology innovation led by 35% reduction of assurance and certification/qualification risks of new safety/security-critical products	Q2: How can the effort for determining the needs of architecture-driven and multi-concern assurance be reduced?	MW4.8 number or share of architectural/design modifications saved by combined safety/security co-engineering		2
		MW4.9 number or share of architectural/design modifications saved by combined safety/performance co-engineering		0
		MW4.10 number or share of architectural/design modifications saved by combined security/performance co-engineering		0

Regarding WP5 metrics, the following table shows the summary of the results.

Table 52. Summary of WP5 metrics

Goal	Question	Metric	CS3	CS7	CS10
G4: to demonstrate a potential sustainable impact in CPS industry by increasing the harmonization and interoperability of assurance and certification/qualification technologies by 60%	Q16: How can seamless interoperability contribute to sustainable impact?	MW5.4 Tool interoperability domains: number of artefact types for which some tool interoperability means exist	30% increase	5	1
		MW5.6 Inter-connected tools: number of inter-connected tools	30% increase	6	1
	Q18: How can AMASS eco-system contribute to sustainable impact?	MW5.3 Common collaboration means: number of technologies that can be applied to several collaboration scenarios			1
		MW5.5 Tool connectors: number of available tool connectors	30% increase	4	

		MW5.7 Standardised tool interoperability means: number of standardised or standard-based tool interoperability means		2	

Regarding WP6 metrics, the following table shows the summary of the results.

Table 53. Summary of WP6 metrics

Goal	Question	Metric	CS1
G1: to demonstrate a potential gain for design efficiency of complex CPS by reducing their assurance and certification/ qualification effort by 50%.	Q9: What is the impact of cross-domain reuse of assurance results?	MW6.2 Product-related Reusability (*PrR_{SF}*) – the extent of reusability of the common components for a specific product while factoring the impact of the product line input costs	70%
G2: to demonstrate a potential reuse of assurance results (qualified or certified before), leading to 40% of cost reductions for component/product (re)certification/qualification activities	Q9: What is the impact of cross-domain reuse of assurance results?	MW6.2 Product-related Reusability (*PrR_{SF}*) – the extent of reusability of the common components for a specific product while factoring the impact of the product line input costs	70%

In general, all the case studies have benefited from applying the AMASS solutions and the pre-defined goals have been achieved. Specifically, the metrics help in quantifying the benefits at the levels of architecture driven assurance, multi-concern assurance, seamless interoperability, and cross/intra domain reuse. Most of the metrics proposed as “common metrics” support in certain way the more specific WP related metrics.

The AMASS reuse-oriented goal, G2, could be achieved with various technologies. This claim is supported by the high rate of acceptance and positive feedback received in various academic conferences and industrial forums. Due to the short observation period in the AMASS case studies, and due to the limited effort that was planned for G2 since the project proposal submission, however, not all reuse-oriented functionalities, developed in the context of WP6, could be evaluated in real case studies.

Abreviations and Definitions

AMASS	Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems
CA	Consortium Agreement
CACC	Cooperative Adaptive Cruise Control
CoPQ	Cost of Poor Quality
CPS	Cyber-Physical Systems
CS	Case Study
Dx.y	Deliverable, x .. WP number, y .. numeric identifier
ECSS	European Cooperation for Space Standardization
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FMVEA	Failure Modes, Vulnerabilities and Effects Analysis
FTA	Fault Tree Analysis
GQM	Goal-Question-Metric
GSN	Goal Structuring Notation
Gx	Goal, x .. numeric identifier
IACS	Industrial and Automation Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IO	Input Output
ISA	Independent Safety Assessor
MPSoC	Multiprocessor System-on-Chip
NA	Not Applicable
NHPP	Non-homogeneous Poisson Process Models
OCRA	Othello Contracts Refinement Analysis
PrR	Product-related Reusability
RAMS	Reliability, Availability and Maintainability Analysis
RR	Relationship Ratio
RTU	Real Time Unit
SIL	Safety Integrity Level
SK	Starter Kit
SL	Security Level
SMV	Symbolic Model Verifier
STO	Scientific and Technical Objective
SysML	Systems Modelling Language
V&V	Verification and Validation
WP	Work Package
ZC	Zone Controller

References

[1] D1.3 AMASS Evaluation Framework and Quality Metrics, December 2017.

[2] D1.6 AMASS demonstrators (c), March 2019.

[3] D6.3 Design of the AMASS tools and methods for cross/intra-domain reuse (b), July 2018.

[4] https://www.es.mdh.se/publications/5119-Towards_Quantitative_Evaluation_of_Reuse_within_Safety_oriented_Process_Lines

[5] D1.4 AMASS Demonstrators (a), April 2017.

[6] D1.5 AMASS Demonstrators (b), March 2017.