ECSEL Joint Undertaking

European Commission

AMASS

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

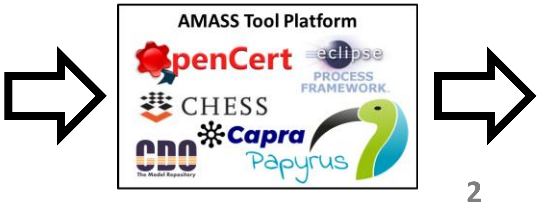
AMASS Usage Scenario 3: Toolchain for system specification and quality assessment

2nd EAB Workshop
Västerås, September 17, 2018

Jose Luis de la Vara
WP5 Leader
uc3m

Introduction

- Toolchains play a major role in CPS Assurance & Certification
  - CPS engineering is supported by different tools and with different purposes: system analysis, specification, V&V…
- Data from the tools of a toolchain can be necessary in the AMASS Tool Platform
  - A tool can need data from another for a different task, e.g. requirements data for quality analysis
  - Data from a tool can also be used as assurance evidence
- Means to enable data exchange between different tools, including the AMASS Platform, are necessary
  - **Seamless Interoperability** encompasses toolchain deployment



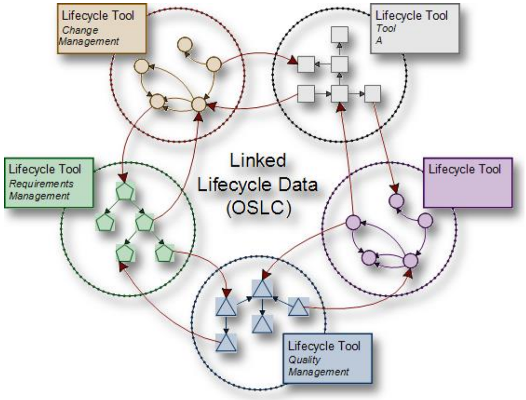
Introduction

Seamless Interoperability areas

- Tool Integration Management
  - Need for better intertwining assurance and engineering activities, and thus for integrating their tool support
  - Focus on OSLC
- Collaborative Work Management
  - Different stakeholders are involved in CPS assurance & certification, need to collaborate, and share information
- Tool Quality Assessment and Characterisation
  - CPS development and V&V tools can also pose risks
  - The tools must be characterized, tool output quality must be assessed, and tool selection impact must be analysed

Toolchain Scenario

- A company is developing a CPS component: *DC Drive for a collaborative automated fleet of vehicles*
- Different tools are used for system specification and design, including AMASS ones (Papyrus, CHESS…)
  - Tool users can be from the company or from others with whom data is exchanged (e.g. suppliers or customers)
- The AMASS Platform is also used as main support for assurance & certification-specific activities
  - Compliance management, evidence management, etc.
- The company aims to be able to seamlessly manage all the data from the different tools



Toolchain Scenario

Higher-level objectives & expected gains

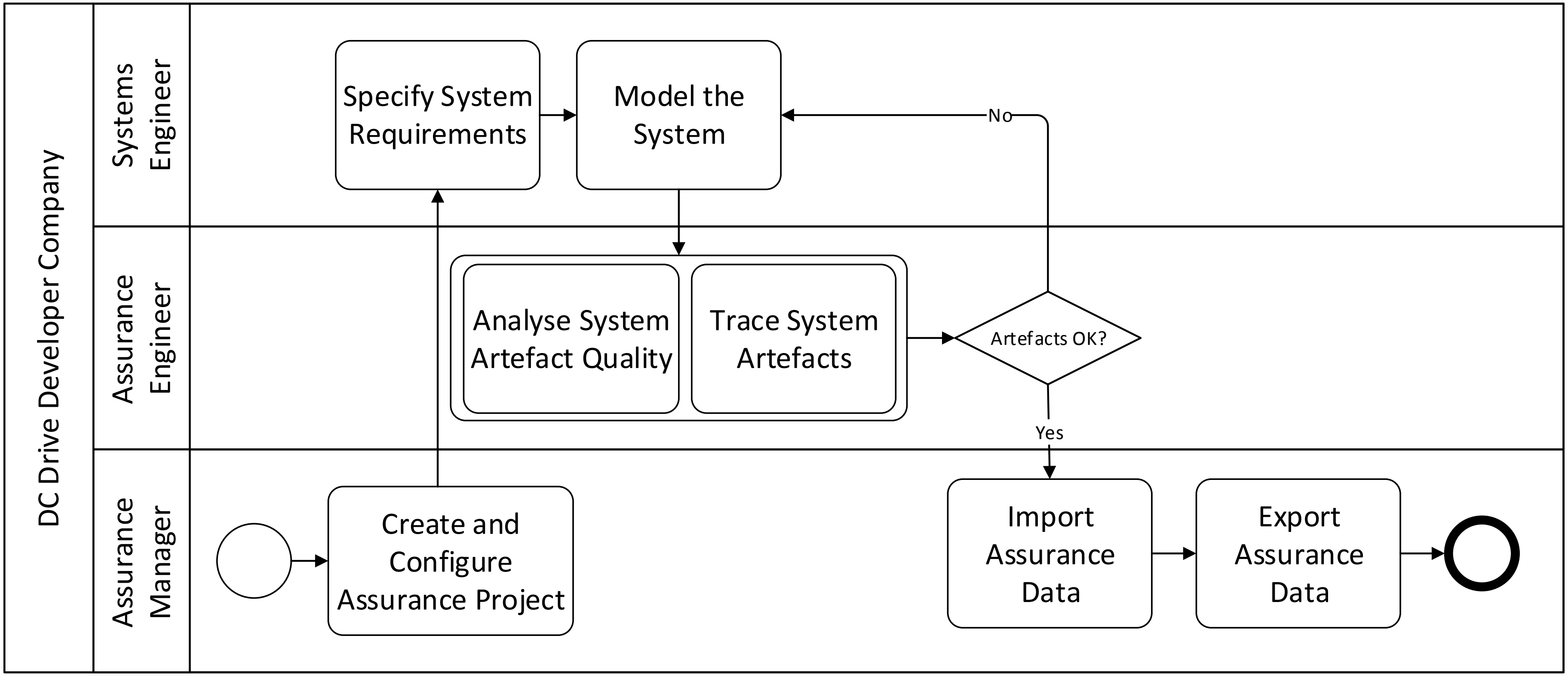
- *O4: develop a fully-fledged open tool platform that will allow developers and other assurance stakeholders to guarantee seamless interoperability of the platform with other tools used in the development of CPSs.*

  → Increased design efficiency, reuse support, reduction of risks, increased harmonization & interoperability

- Metrics (selection)
  - Effort for assurance information collection & exchange
  - Effectiveness in risks identification
  - Number of common means for tool interoperability
  - Number of connectors, connected tools & covered domains

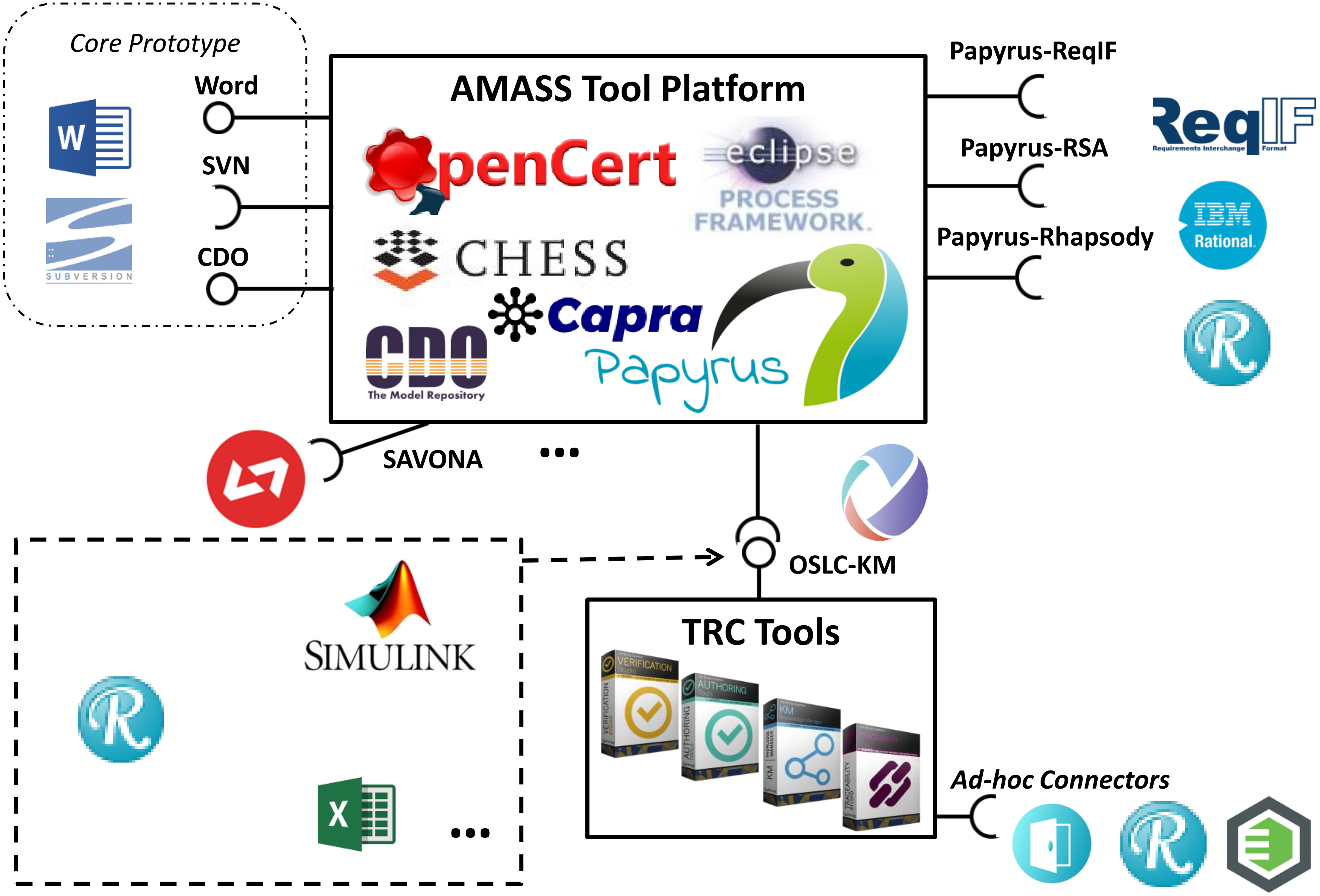
Toolchain Scenario

Engineering & assurance workflow



How many tools can be involved?

Toolchain Scenario



Core Prototype

Word

SVN

CDO

AMASS Tool Platform

Papyrus-ReqIF

Papyrus-RSA

Papyrus-Rhapsody

SAVONA

...

OSLC-KM

TRC Tools

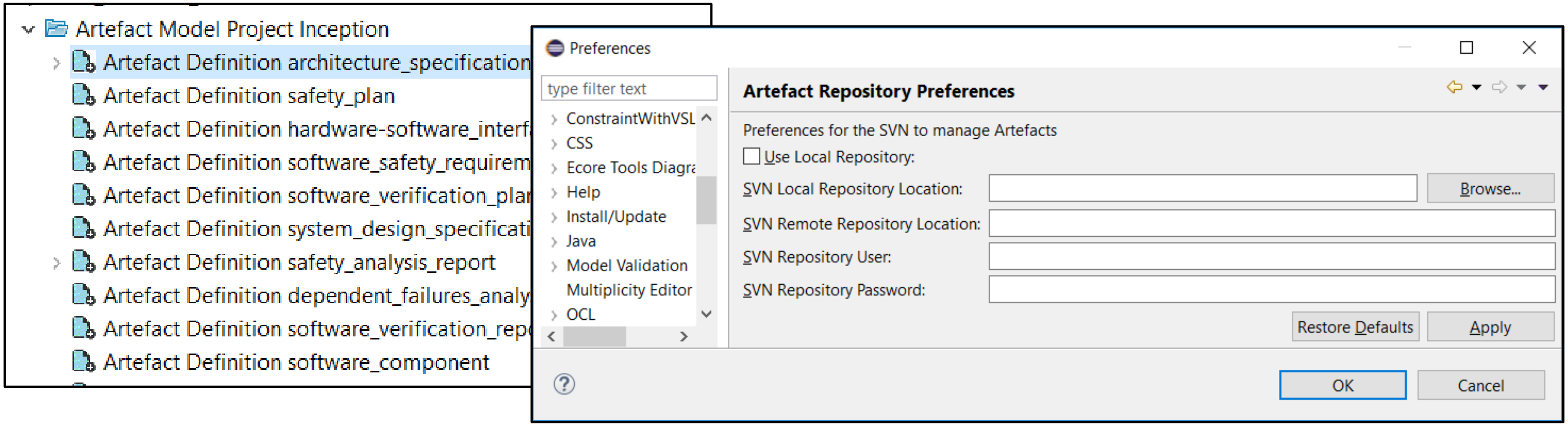
Ad-hoc Connectors

...

Toolchain Scenario

Assurance project for the DC Drive (Assurance Manager)

- An ISO 26262 reference framework is used to specify the assurance project baseline
- Argumentation, evidence, and process models are created
- Evidence artefacts can be linked to files in a SVN repository



Artefact Model Project Inception
- Artefact Definition architecture_specification
- Artefact Definition safety_plan
- Artefact Definition hardware-software_interf
- Artefact Definition software_safety_requirem
- Artefact Definition software_verification_plar
- Artefact Definition system_design_specificati
- Artefact Definition safety_analysis_report
- Artefact Definition dependent_failures_analy
- Artefact Definition software_verification_rep
- Artefact Definition software_component

Preferences

Artefact Repository Preferences

Preferences for the SVN to manage Artefacts

□ Use Local Repository:

SVN Local Repository Location:

SVN Remote Repository Location:

SVN Repository User:

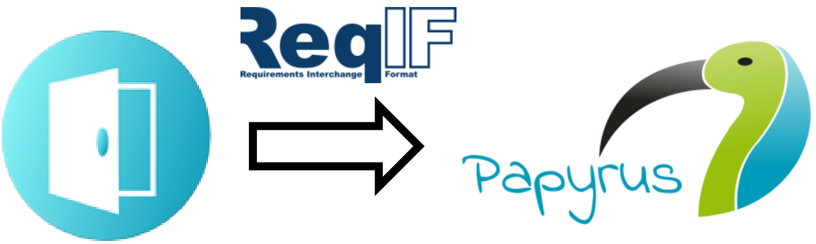
SVN Repository Password:

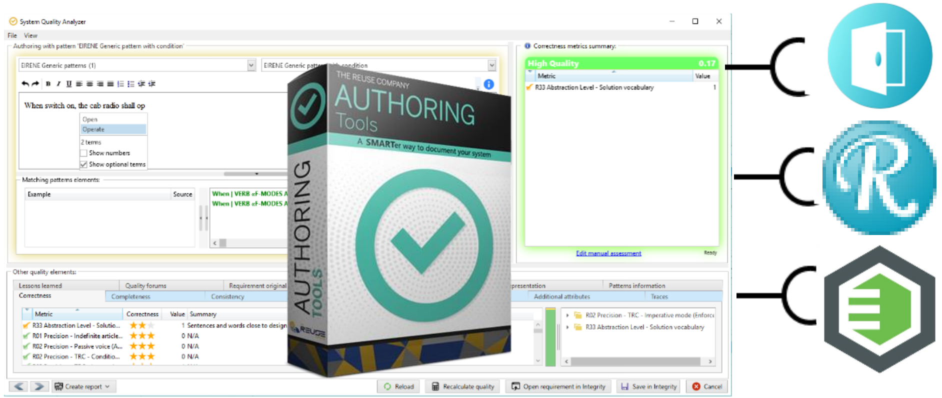
Toolchain Scenario

Requirements specification (Systems Engineer)

- Requirements can be specified with different tools and in different formats
  - DOORS, PTC Integrity, Excel, Word… and Papyrus/CHESS
- ReqIF is a standard for exchange that Papyrus can use
- Ad-hoc connectors can also be used

“After power up, the system shall enter the operation mode Passive”




System Quality Analyzer

Authoring with pattern 'EIRENE Generic pattern with condition'

EIRENE Generic patterns (1)

When switch on, the cab radio shall op

Open
Operate
2 terms
□ Show numbers
☑ Show optional terms

Matching patterns elements:

When | VERB «F-MODES A
When | VERB «F-MODES A

Correctness metrics summary:

High Quality 0.17

Metric	Value
R33 Abstraction Level - Solution vocabulary	1

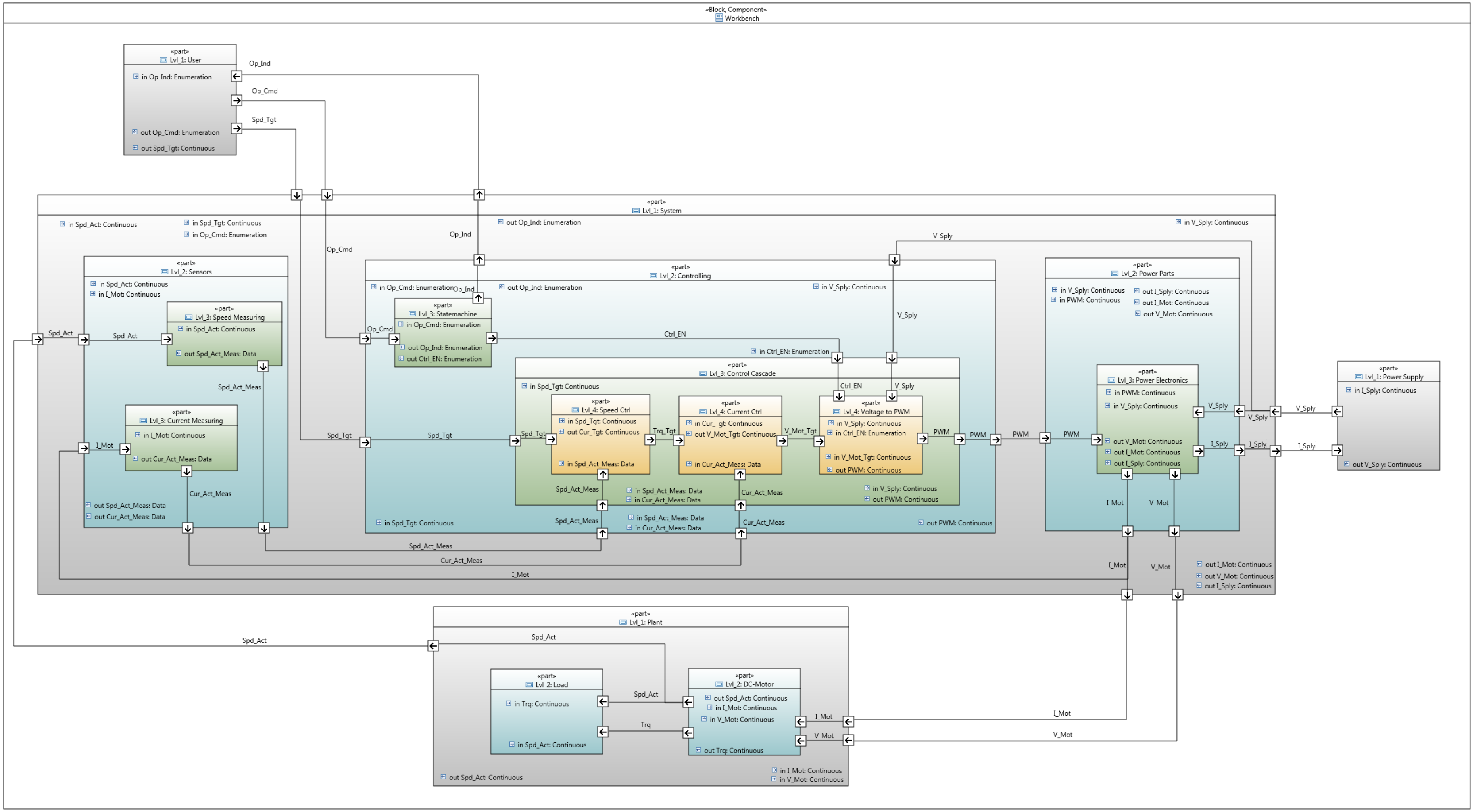
Other quality elements:

Metric	Correctness	Value	Summary
R33 Abstraction Level - Solutio...	★★	1	Sentences and words close to design
R01 Precision - Indefinite article...	★★★	0	N/A
R02 Precision - Passive voice (A...	★★★	0	N/A
R02 Precision - TRC - Conditio...	★★★	0	N/A

R02 Precision - TRC - Imperative mode (Enforce
R33 Abstraction Level - Solution vocabulary

Toolchain Scenario

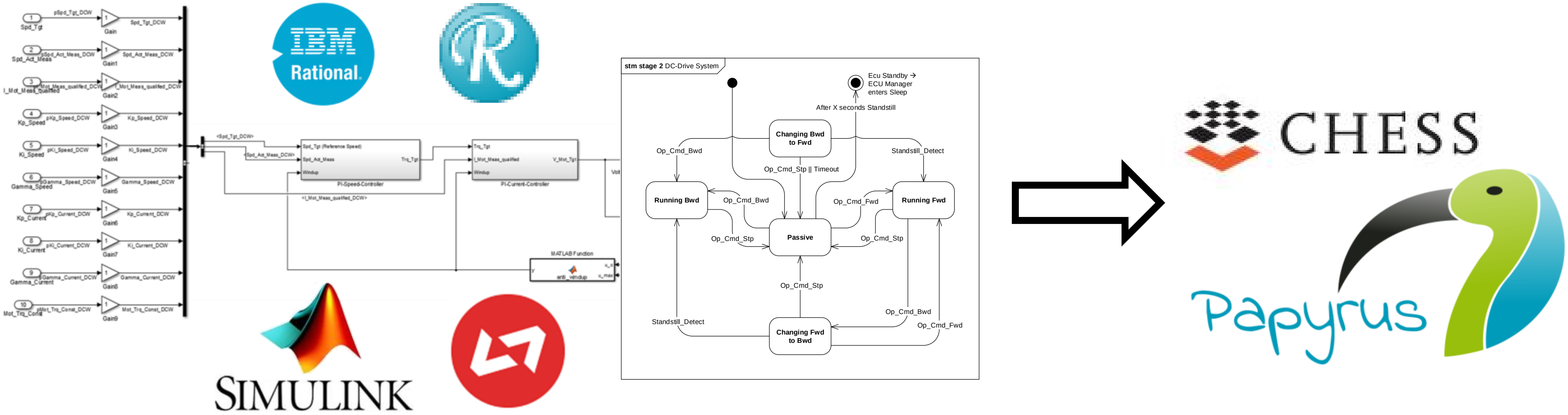
System modelling (Systems Engineer)



Toolchain Scenario

System modelling (Systems Engineer)

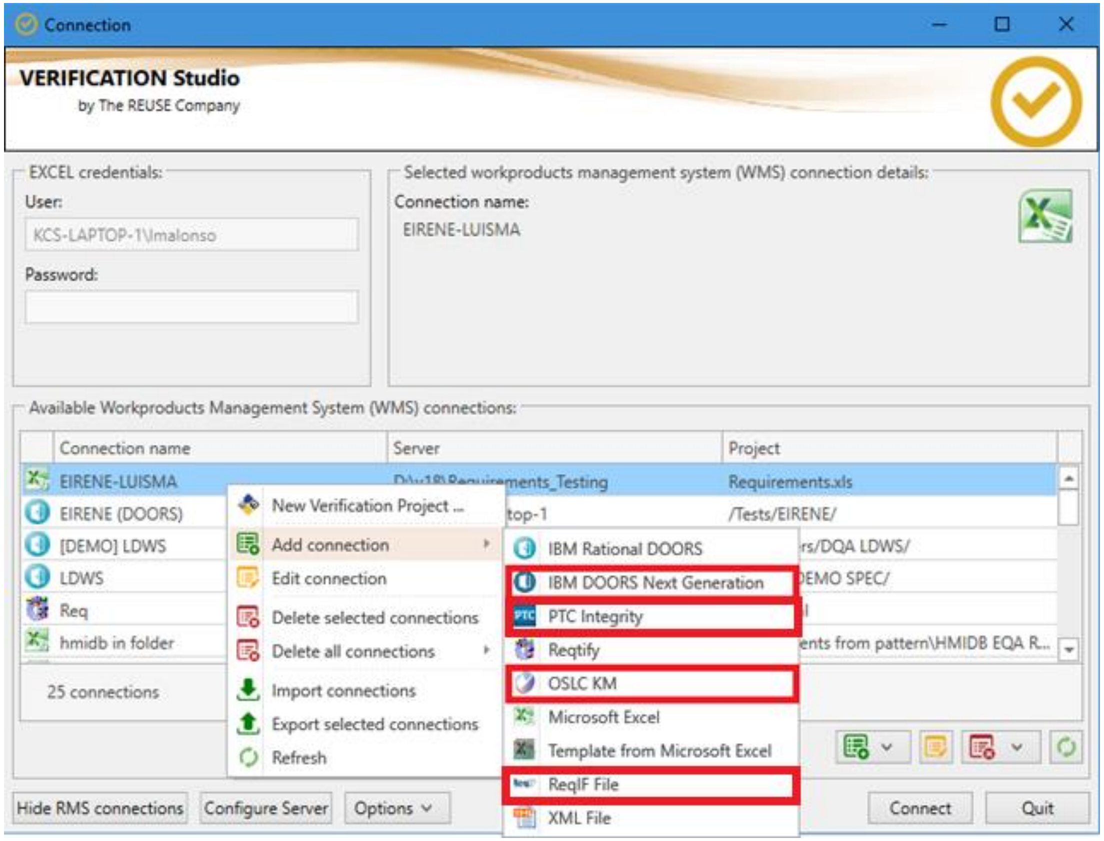
- Papyrus/CHESS is the system modelling tool proposed by AMASS, but others exist and are used
  - By major vendors (Rhapsody, RSA, MagicDraw, Simulink…) as well as by AMASS partners (SAVONA, medini…)
- Data from these tools can be imported to AMASS ones
  - To Papyrus/CHESS + as assurance evidence data (next slides)



Toolchain Scenario

Quality analysis (Assurance Engineer)

- The quality of system artefacts must be ensured, and thus analysed, for CPS assurance & certification
  - Correctness
  - Consistency
  - Completeness
  - …
- Verification Studio, by TRC, supports the analysis based on metrics



Connection

VERIFICATION Studio
by The REUSE Company

EXCEL credentials:
User: KCS-LAPTOP-1\lmalonso
Password:

Selected workproducts management system (WMS) connection details:
Connection name: EIRENE-LUISMA

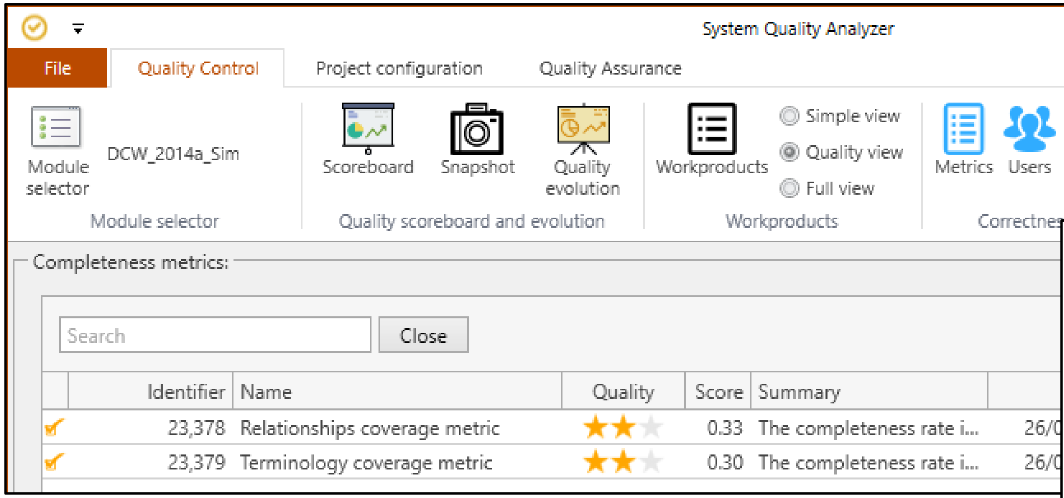
Available Workproducts Management System (WMS) connections:

Connection name	Server	Project
EIRENE-LUISMA	D:\u18\Requirements_Testing	Requirements.xls
EIRENE (DOORS)	top-1	/Tests/EIRENE/
[DEMO] LDWS		rs/DQA LDWS/
LDWS		DEMO SPEC/
Req		l
hmidb in folder		ents from pattern\HMIDB EQA R...

25 connections

Toolchain Scenario

Quality analysis (Assurance Engineer)

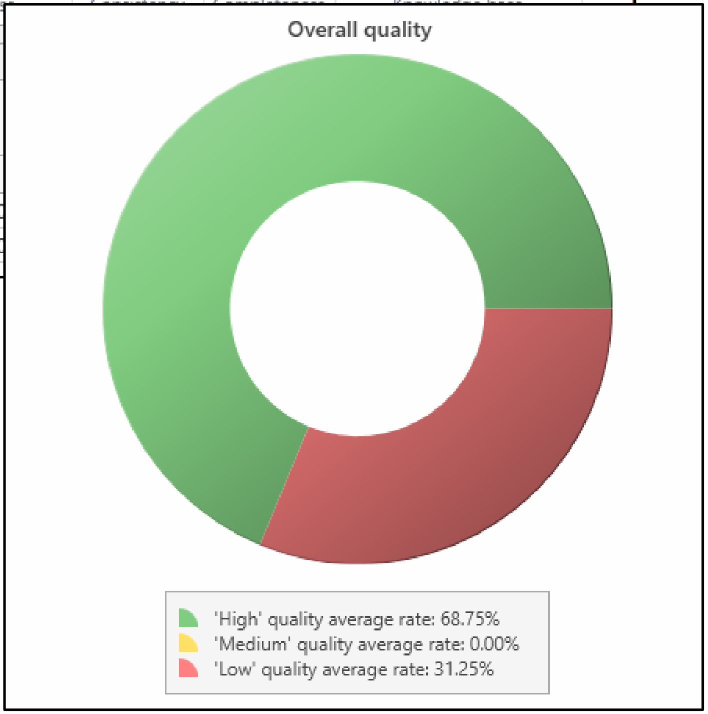


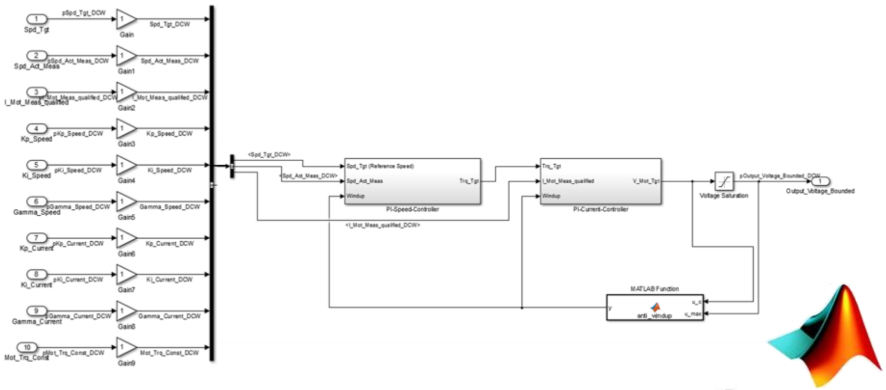
DCW_2014a_Sim

○ Simple view
● Quality view
○ Full view

Completeness metrics:

	Identifier	Name	Quality	Score	Summary	
✓	23,378	Relationships coverage metric	★★☆	0.33	The completeness rate i...	26/0
✓	23,379	Terminology coverage metric	★★☆	0.30	The completeness rate i...	26/0





SIMULINK

Toolchain Scenario

Quality analysis (Assurance Engineer)

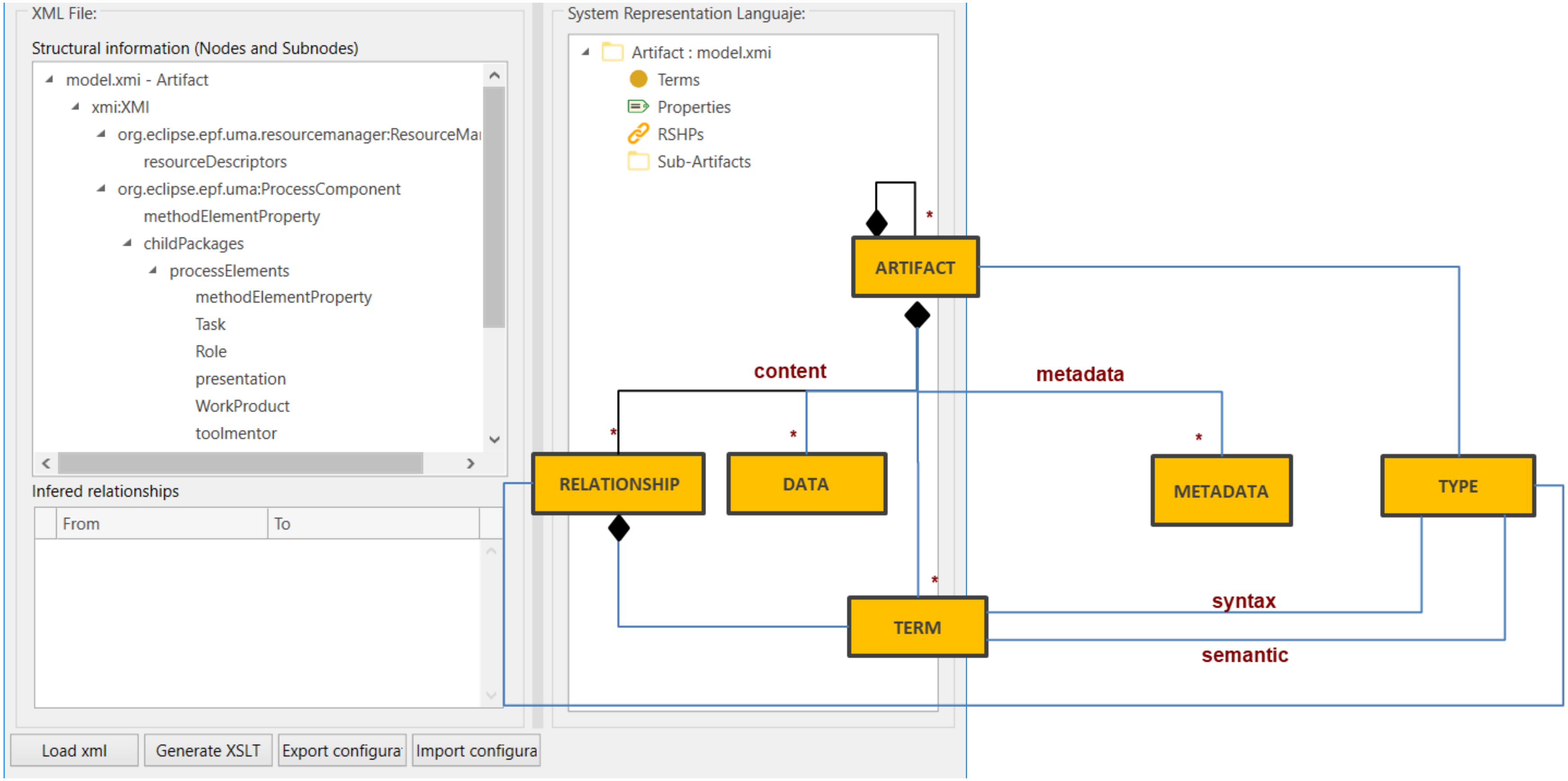
- OSLC KM enables the connection to a wide range of tools and thus quality analysis to a wide range of system artefact types

Domain	Tool Provider
Logical Models (SysML)	Rhapsody, Papyrus, Magic Draw
Physical model (Modelica & FMI/FMU)	Open Modelica
Physical model	Simulink
Formal ontologies (OWL 1.1, 2.0)	Protegé
Office	MS Excel + Word
Variability models	Pure variants

Toolchain Scenario

Connector generation (Assurance Engineer)

- It is possible to create OSLC KM-based connectors from XML files with Verification Studio



XML File:

Structural information (Nodes and Subnodes)

```
◢ model.xmi - Artifact
   ◢ xmi:XMI
      ◢ org.eclipse.epf.uma.resourcemanager:ResourceMa
           resourceDescriptors
      ◢ org.eclipse.epf.uma:ProcessComponent
           methodElementProperty
         ◢ childPackages
            ◢ processElements
                 methodElementProperty
                 Task
                 Role
                 presentation
                 WorkProduct
                 toolmentor
```

Infered relationships

From	To

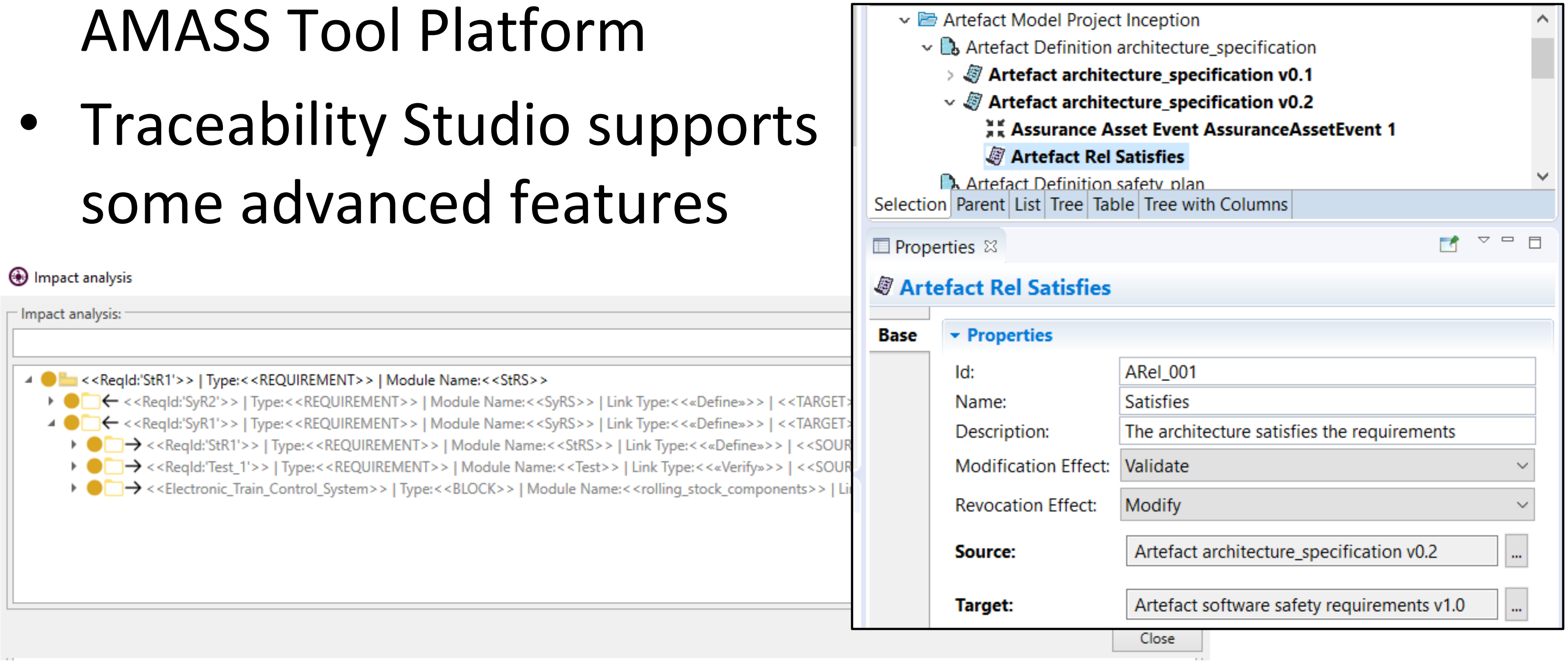
System Representation Languaje:

```
◢ Artifact : model.xmi
     Terms
     Properties
     RSHPs
     Sub-Artifacts
```

Toolchain Scenario

Traceability (Assurance Engineer)

- The OpenCert evidence editor is the default tool to trace evidence artefacts
- Capra is used as an extension mechanism in the AMASS Tool Platform
- Traceability Studio supports some advanced features



```
◢ <<ReqId:'StR1'>> | Type:<<REQUIREMENT>> | Module Name:<<StRS>>
  ▸ ← <<ReqId:'SyR2'>> | Type:<<REQUIREMENT>> | Module Name:<<SyRS>> | Link Type:<<«Define»>> | <<TARGET
  ◢ ← <<ReqId:'SyR1'>> | Type:<<REQUIREMENT>> | Module Name:<<SyRS>> | Link Type:<<«Define»>> | <<TARGET
    ▸ → <<ReqId:'StR1'>> | Type:<<REQUIREMENT>> | Module Name:<<StRS>> | Link Type:<<«Define»>> | <<SOUR
    ▸ → <<ReqId:'Test_1'>> | Type:<<REQUIREMENT>> | Module Name:<<Test>> | Link Type:<<«Verify»>> | <<SOUR
    ▸ → <<Electronic_Train_Control_System>> | Type:<<BLOCK>> | Module Name:<<rolling_stock_components>> | Li
```

```
⌄ Artefact Model Project Inception
  ⌄ Artefact Definition architecture_specification
    › Artefact architecture_specification v0.1
    ⌄ Artefact architecture_specification v0.2
        Assurance Asset Event AssuranceAssetEvent 1
        Artefact Rel Satisfies
  Artefact Definition safety_plan
```

Artefact Rel Satisfies

Properties

Id: ARel_001

Name: Satisfies

Description: The architecture satisfies the requirements

Modification Effect: Validate

Revocation Effect: Modify

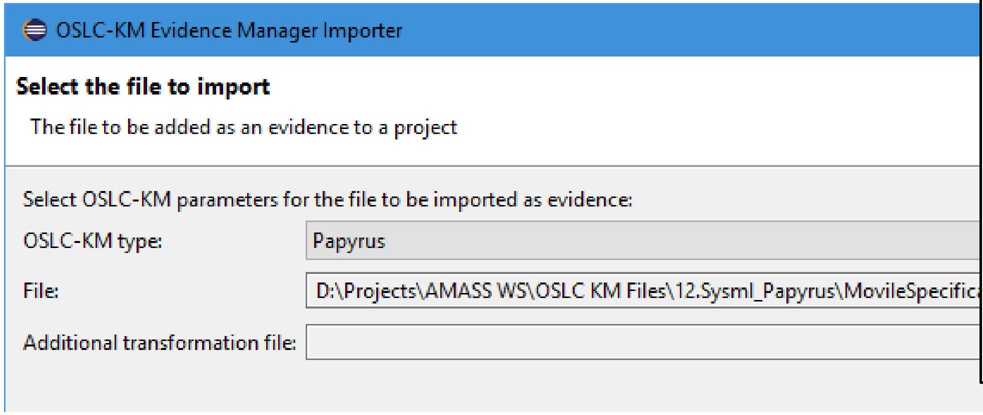
Source: Artefact architecture_specification v0.2

Target: Artefact software safety requirements v1.0

Toolchain Scenario

Data import to assurance project (Assurance Manager)

- OSLC KM supports the import of several artefact types
  - Standard XMI (output from many UML tools)
  - SysML from Rhapsody, Papyrus, Magic Draw…
  - Excel
  - FMI/FMU
  - Simulink
  - Pure Variants
  - ASCE
  - …



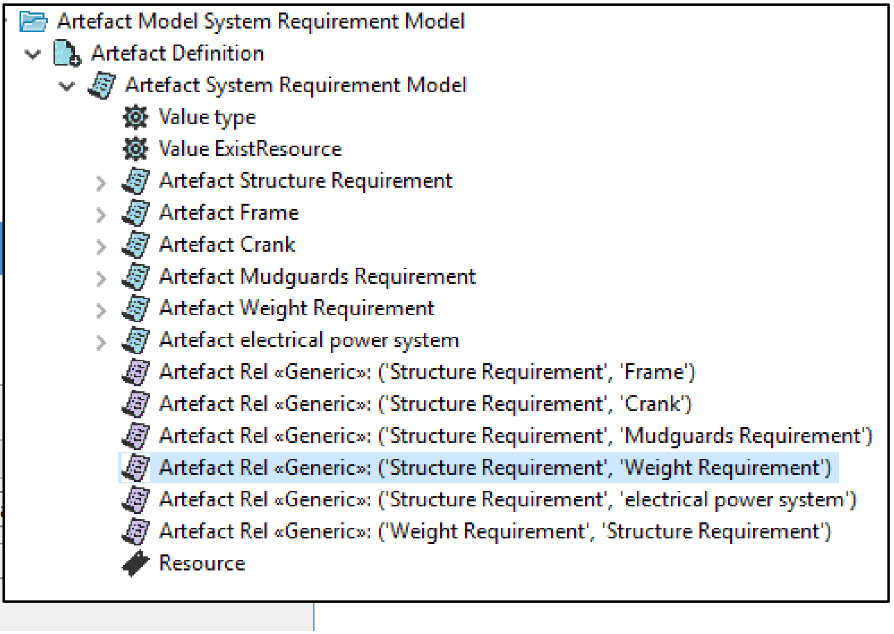
OSLC-KM Evidence Manager Importer

Select the file to import

The file to be added as an evidence to a project

Select OSLC-KM parameters for the file to be imported as evidence:

OSLC-KM type:	Papyrus
File:	D:\Projects\AMASS WS\OSLC KM Files\12.Sysml_Papyrus\MovileSpecifica
Additional transformation file:	

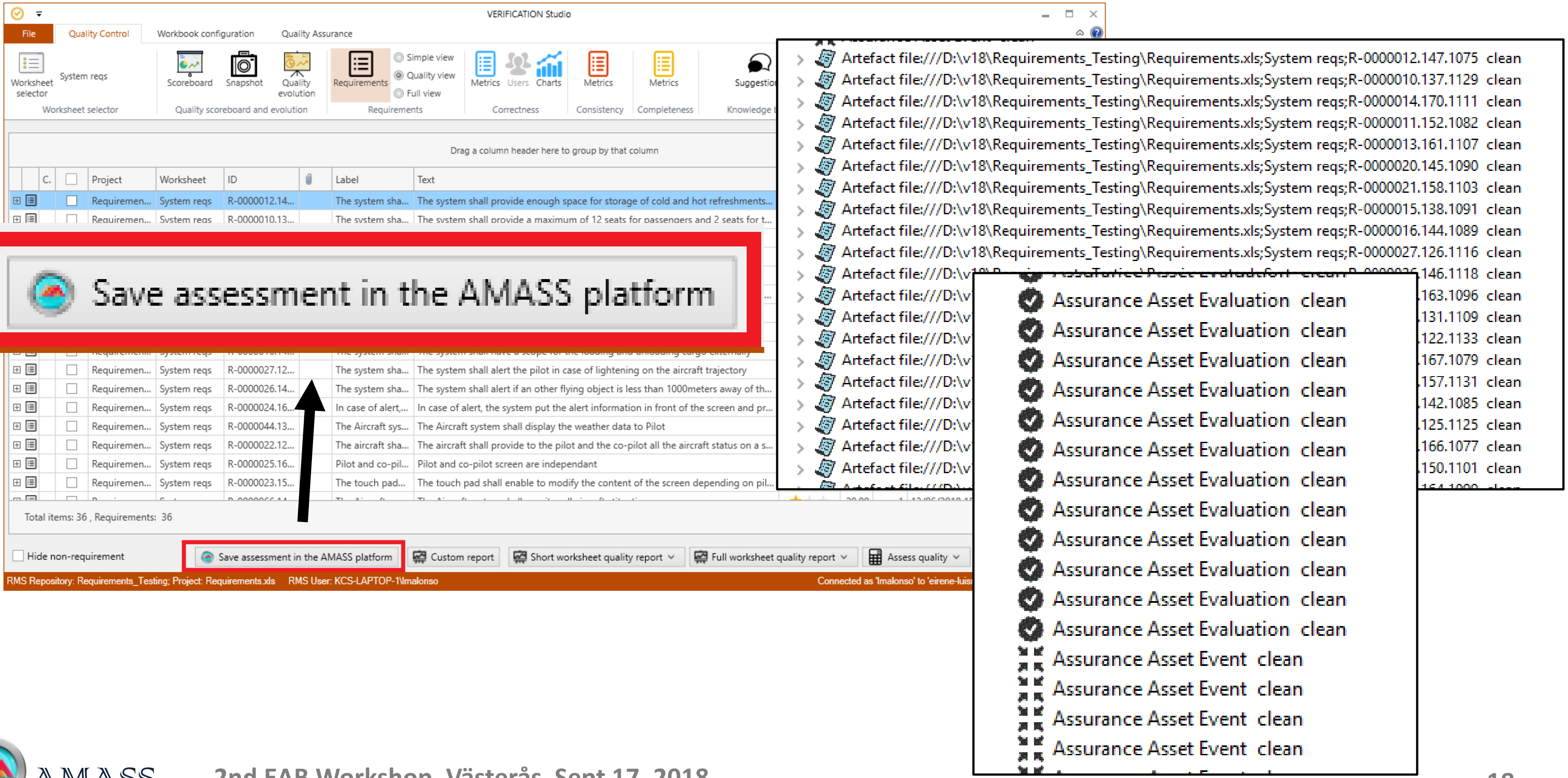


- Artefact Model System Requirement Model
  - Artefact Definition
    - Artefact System Requirement Model
      - Value type
      - Value ExistResource
      - Artefact Structure Requirement
      - Artefact Frame
      - Artefact Crank
      - Artefact Mudguards Requirement
      - Artefact Weight Requirement
      - Artefact electrical power system
      - Artefact Rel «Generic»: ('Structure Requirement', 'Frame')
      - Artefact Rel «Generic»: ('Structure Requirement', 'Crank')
      - Artefact Rel «Generic»: ('Structure Requirement', 'Mudguards Requirement')
      - Artefact Rel «Generic»: ('Structure Requirement', 'Weight Requirement')
      - Artefact Rel «Generic»: ('Structure Requirement', 'electrical power system')
      - Artefact Rel «Generic»: ('Weight Requirement', 'Structure Requirement')
      - Resource

Toolchain Scenario

Data import to assurance project (Assurance Manager)

- Quality data can be imported to evidence models of an assurance project from Verification Studio



C.	□	Project	Worksheet	ID	Label	Text
	□	Requiremen...	System reqs	R-0000012.14...	The system sha...	The system shall provide enough space for storage of cold and hot refreshments...
	□	Requiremen...	System reqs	R-0000010.13...	The system sha...	The system shall provide a maximum of 12 seats for passengers and 2 seats for t...
	□	Requiremen...	System reqs	R-0000027.12...	The system sha...	The system shall alert the pilot in case of lightening on the aircraft trajectory
	□	Requiremen...	System reqs	R-0000026.14...	The system sha...	The system shall alert if an other flying object is less than 1000meters away of th...
	□	Requiremen...	System reqs	R-0000024.16...	In case of alert,...	In case of alert, the system put the alert information in front of the screen and pr...
	□	Requiremen...	System reqs	R-0000044.13...	The Aircraft sys...	The Aircraft system shall display the weather data to Pilot
	□	Requiremen...	System reqs	R-0000022.12...	The aircraft sha...	The aircraft shall provide to the pilot and the co-pilot all the aircraft status on a s...
	□	Requiremen...	System reqs	R-0000025.16...	Pilot and co-pil...	Pilot and co-pilot screen are independant
	□	Requiremen...	System reqs	R-0000023.15...	The touch pad...	The touch pad shall enable to modify the content of the screen depending on pil...

Total items: 36 , Requirements: 36

Save assessment in the AMASS platform
□ Hide non-requirement
Save assessment in the AMASS platform
Custom report
Short worksheet quality report
Full worksheet quality report
Assess quality

RMS Repository: Requirements_Testing; Project: Requirements.xls RMS User: KCS-LAPTOP-1\lmalonso Connected as 'lmalonso' to 'eirene-luis

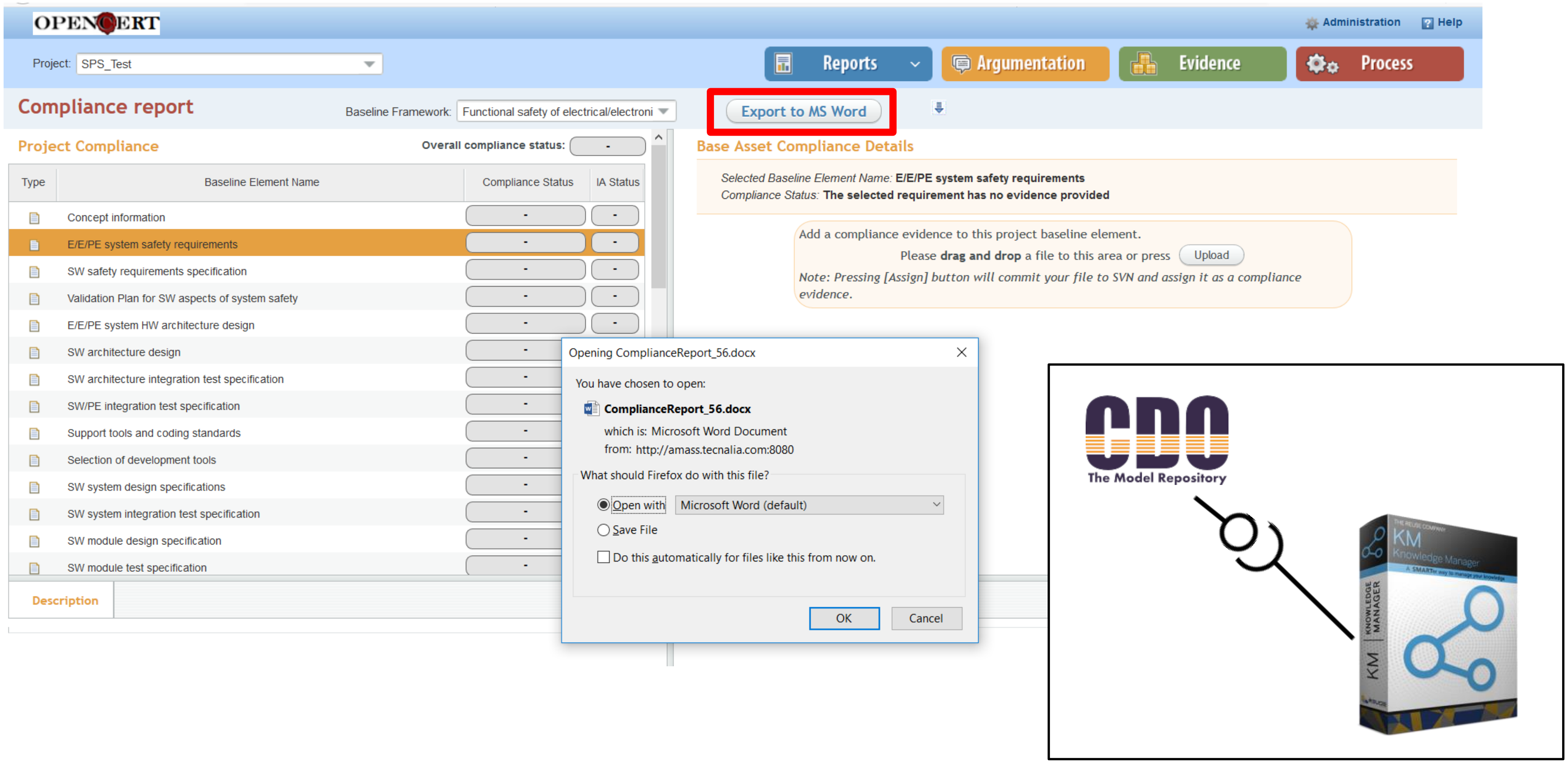
```
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000012.147.1075 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000010.137.1129 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000014.170.1111 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000011.152.1082 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000013.161.1107 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000020.145.1090 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000021.158.1103 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000015.138.1091 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000016.144.1089 clean
Artefact file:///D:\v18\Requirements_Testing\Requirements.xls;System reqs;R-0000027.126.1116 clean
Artefact file:///D:\v                                          146.1118 clean
Artefact file:///D:\v                                          163.1096 clean
Artefact file:///D:\v                                          131.1109 clean
Artefact file:///D:\v                                          122.1133 clean
Artefact file:///D:\v                                          167.1079 clean
Artefact file:///D:\v                                          157.1131 clean
Artefact file:///D:\v                                          142.1085 clean
Artefact file:///D:\v                                          125.1125 clean
Artefact file:///D:\v                                          166.1077 clean
Artefact file:///D:\v                                          150.1101 clean
```

```
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Evaluation clean
Assurance Asset Event clean
Assurance Asset Event clean
Assurance Asset Event clean
Assurance Asset Event clean
```

Toolchain Scenario

Data export from assurance project (Assurance Manager)

- Assurance project data can be exported as a Word document and via CDO API



Project: SPS_Test

Compliance report

Baseline Framework: Functional safety of electrical/electroni

Project Compliance

Overall compliance status: -

Type	Baseline Element Name	Compliance Status	IA Status
	Concept information	-	-
	E/E/PE system safety requirements	-	-
	SW safety requirements specification	-	-
	Validation Plan for SW aspects of system safety	-	-
	E/E/PE system HW architecture design	-	-
	SW architecture design	-	
	SW architecture integration test specification	-	
	SW/PE integration test specification	-	
	Support tools and coding standards	-	
	Selection of development tools	-	
	SW system design specifications	-	
	SW system integration test specification	-	
	SW module design specification	-	
	SW module test specification	-	

Base Asset Compliance Details

Selected Baseline Element Name: **E/E/PE system safety requirements**
Compliance Status: **The selected requirement has no evidence provided**

Add a compliance evidence to this project baseline element.
Please **drag and drop** a file to this area or press Upload
Note: Pressing [Assign] button will commit your file to SVN and assign it as a compliance evidence.

Opening ComplianceReport_56.docx

You have chosen to open:

ComplianceReport_56.docx
which is: Microsoft Word Document
from: http://amass.tecnalia.com:8080

What should Firefox do with this file?

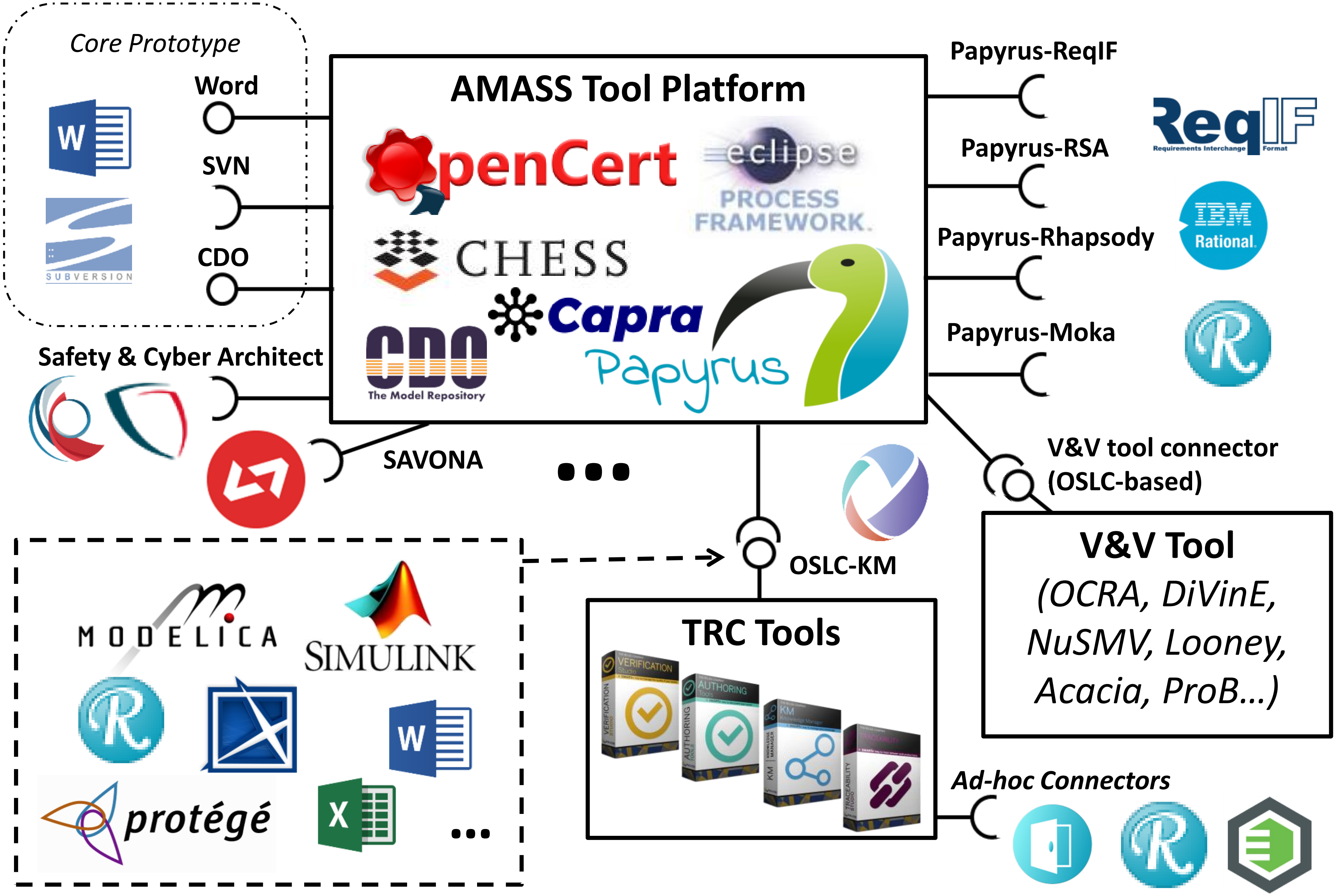
● Open with Microsoft Word (default)
○ Save File
□ Do this automatically for files like this from now on.

OK Cancel

Toolchain Scenario Outcome

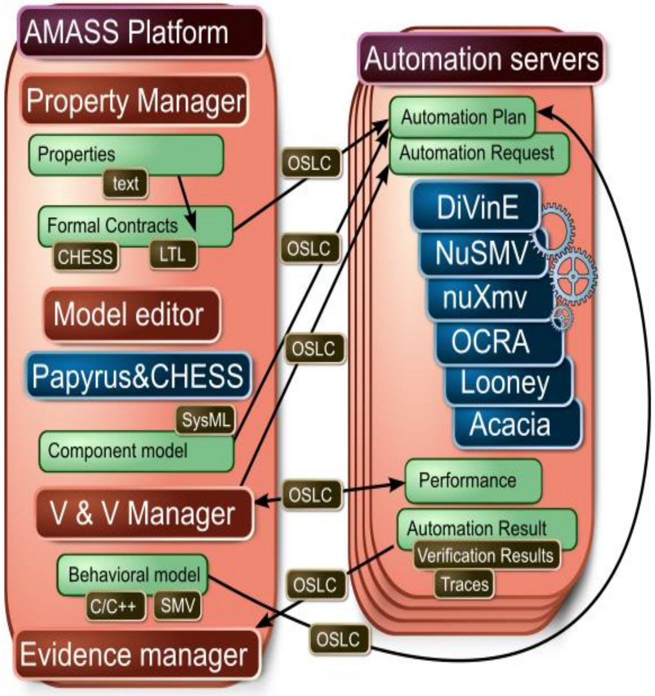
- Effort for assurance information collection & exchange
  - Easier and faster data collection & exchange
  - Easier and faster connector development
- Effectiveness in risks identification
  - Increased by data exchange & quality analysis possibilities
- Number of common means for tool interoperability
  - 1 common means: OSLC KM
- Number of connectors, connected tools & covered domains (inc. all project)
  - From 5 to 12 connectors (~10 to 25+)
  - From 5 to 15 connected tools (~7 to 30+)
  - From 3 to 7 covered domains (~5 to 10+)

Summary of Toolchain Possibilities



Seamless Interoperability Results for P1

- Tool integration
  - Tool integration with OSLC-KM (inc. connector generation)
  - Ad-hoc tool integration
  - Papyrus interoperability
  - V&V tool integration
- Collaborative work
  - Seamless tracing
  - Collaborative real-time modelling
  - Data mining
  - Automatic translations



- Tool Quality Assessment and Characterisation
  - Exploitation of compliance management support

Seamless Interoperability Results for P2

- Tool integration
  - V&V evidence management
  - Operations for tool integration with OSLC-KM
  - Integration with Safety and Security Analysis Tools
  - New integration solutions for Farkle, SAVONA, WEFACT, and MORETO
- Collaborative Work
  - Improved security management and data management
  - Extended collaborative modelling
  - New traceability management mechanisms
  - Extended data mining-enabled collaboration
  - Further exploitation of CDO features

Conclusion

- Toolchains play an important role in CPS assurance & certification and are a part of Seamless Interoperability
- AMASS has paid great attention to toolchains:
  - OSLC as a reference technology, inc. OSLC KM
  - Integration means for the AMASS Tool Platform and others
  - … and further Seamless Interoperability features
- The results lead to several important gains:
  - Easier & faster CPS design and risk identification
  - OSLC KM as a common approach for tool integration
  - x2.5+ connectors
  - x4+ connected tools
  - x2+ covered domains

Questions?