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

AMASS Tool Platform

- openCert
- eclipse
- CHESS
- TRC Tools
- Papyrus
- Papyrus-ReqIF
- Papyrus-RSA
- Papyrus-Rhapsody
- IBM
- OSLC-KM
- ReqIF
- Ad-hoc Connectors

Core Prototype

- Word
- SVN
- CDO
- SAVONA

2nd EAB Workshop, Västerås, Sept 17, 2018
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
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”
Toolchain Scenario

System modelling (Systems Engineer)
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)
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
Quality analysis (Assurance Engineer)
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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Tool Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Models (SysML)</td>
<td>Rhapsody, Papyrus, Magic Draw</td>
</tr>
<tr>
<td>Physical model (Modelica &amp; FMI/FMU)</td>
<td>Open Modelica</td>
</tr>
<tr>
<td>Physical model</td>
<td>Simulink</td>
</tr>
<tr>
<td>Formal ontologies (OWL 1.1, 2.0)</td>
<td>Protegé</td>
</tr>
<tr>
<td>Office</td>
<td>MS Excel + Word</td>
</tr>
<tr>
<td>Variability models</td>
<td>Pure variants</td>
</tr>
</tbody>
</table>
Connector generation (Assurance Engineer)

- It is possible to create OSLC KM-based connectors from XML files with Verification Studio
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
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
  - ...
Data import to assurance project (Assurance Manager)

- Quality data can be imported to evidence models of an assurance project from Verification Studio.
Data export from assurance project (Assurance Manager)

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

AMASS Tool Platform

Core Prototype

Word
SVN
CDO

Safety & Cyber Architect

SAVONA

V&V Tool
(OSLC, DiVinE, NuSMV, Looney, Acacia, ProB...)

TRC Tools

Ad-hoc Connectors

Papyrus-ReqIF
Papyrus-RSA
Papyrus-Rhapsody
Papyrus-Moka
V&V tool connector (OSLC-based)

OSLC-KM

Modelica
Simulink
Protégé

AMASS

2nd EAB Workshop, Västerås, Sept 17, 2018
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
• 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?