AQUAS: Aggregated Quality Assurance for Systems

Matthieu PFEIFFER
8th December, 2017
Brussels
Motivation

- Great complexity of systems engineered nowadays
- Difficult to assure interrelated qualities like:
  - Safety
  - Security
  - Performance
- Hard to harmonize such interdependent requirements during product lifecycle, especially for mission-critical real-time systems:
  - Transportation
  - Medical devices
  - Aerospace
  - Industrial control
Main goals

- Co-engineering inside and across product lifecycle phases. Standards evolution. The three key goals: CE, PLC4CE, SE4CE

- Achieved by establishing a global concept framework for safety, security, and performance co-engineering:
  - Based on the needs of *industrial application* domains
  - Efficient analysis of *trade-offs* between system quality attributes
  - Taking into account the complete *product lifecycle*
  - *Tools* and *platforms* upgraded to implement and test the co-engineering approaches
  - Effective *support* for design breakthroughs
  - Reducing engineering *costs* for building and maintaining systems
  - Influencing the evolution of *standards*
Driven by use cases

- Demonstrators are combined results of workpackages
Application Domains

- Rail Carriage Mechanisms
- Air Traffic Management
- Medical Devices
- Space Multicore Architectures
- Safety, Security, Performance, System modelling
- Industrial Drive
- External Domains
Good synchronisation between safety/performance/security at each stage and along the stages.

Safety/performance/security Co-engineering goes beyond the V-model.

Operation & maintenance updates, recovery, decommissioning & disposal
Methodology – Interactions Points

- Design decisions must rely on an holistic view of the system (safety, security and performance)
- Through the development cycle, initial decisions and allocation of goals and properties are subject to refinements
- Each of the refinements may (or may not) serve as an interaction point
- If a refinement results in significant deviation, an interaction point is triggered in order to establish a new trade-off
Design Tooling

- New tools features to support co-engineering and interaction points.
- Improving tools interoperability through
  - standardised formats and interfaces.
- Subsets covering one or several use cases.
- Dynamic perimeters depending on lifecycle.

N.B. More details in appendix
Dissemination & Exploitation

**Exploitation tracks** laid out for **Industry engagement**, particularly via:

- an **External Advisory Board**
- significant involvement in **standardisation meetings**
- **AQUAS project open workshops**

---

**Communication & Dissemination**

- **WWW**
- **Leaflets, newsletters**
- **Platforms, networks, associations**
- **Social networks**
- **Specialized & generalized media**

- **University courses**
- **Open source tools**
- **Scientific conferences**
- **Journals, Open access**
- **Fairs, exhibitions, events**
- **Workshops**
AQUAS partners

- **24 partners in 7 countries**

- **16 Saf-Sec**
- **15 Saf-Perf**
- **11 Sec-Perf**
- **8 Product Lifecycle**
Impact & Conclusions

- Generate momentum for industry to properly adopt co-engineering.
  - Decisive competitive advantage for organisations following co-engineering recommendations and standards

- Unlocks a significant hurdle for innovative products on the market accelerating:
  - Digitalisation of Europe, IoT uptake by CPS, Agile Engineering, accessibility of new technology to large industry.

- Limiting risk in design whilst increasing efficiency of development
- Improved standards for dependability of complex systems

- Safety, security and performance co-engineering framework
- Partners selected for high motivation and good balance of expertise
- AQUAS rated 2\textsuperscript{nd} out of 28 proposals
THANK YOU

ECSEL JU
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TASE</td>
<td>Thales Alenia Space Espana, SA - project coordinator</td>
</tr>
<tr>
<td>TRT</td>
<td>Thales SA</td>
</tr>
<tr>
<td>Integrasys</td>
<td>Integrasys SA</td>
</tr>
<tr>
<td>RGB</td>
<td>R G B Medical Devices SA</td>
</tr>
<tr>
<td>CITY</td>
<td>City University Of London</td>
</tr>
<tr>
<td>AIT</td>
<td>Austrian Institute Of Technology</td>
</tr>
<tr>
<td>GSM</td>
<td>Siemens Industry Software SAS</td>
</tr>
<tr>
<td>MDS</td>
<td>Magillem Design Services SAS</td>
</tr>
<tr>
<td>ClearSy</td>
<td>Clearsy SAS</td>
</tr>
<tr>
<td>CEA</td>
<td>Commissariat A L’Energie Atomique</td>
</tr>
<tr>
<td>Et Aux Energies Alternatives</td>
<td></td>
</tr>
<tr>
<td>TrustPort</td>
<td>Trustport, A.S.</td>
</tr>
<tr>
<td>MTTP</td>
<td>Institut Mines-Telecom</td>
</tr>
<tr>
<td>Tecnalia</td>
<td>Fundacion Tecnalia Research &amp; Innovation</td>
</tr>
<tr>
<td>BUT</td>
<td>Brno University of Technology</td>
</tr>
<tr>
<td>All4Tec</td>
<td>Alliance Pour Les Technologies De L'informatique</td>
</tr>
<tr>
<td>ITI</td>
<td>Instituto Tecnologico De Informatica</td>
</tr>
<tr>
<td>Intecs</td>
<td>Intecs Solutions SPA</td>
</tr>
<tr>
<td>SAG</td>
<td>Siemens Aktiengesellschaft</td>
</tr>
<tr>
<td>Oesterreich</td>
<td></td>
</tr>
<tr>
<td>HSRM</td>
<td>Hochschule Rheinmain</td>
</tr>
<tr>
<td>AMT</td>
<td>Ansys Medini Technologies AG</td>
</tr>
<tr>
<td>SYSGO</td>
<td>Sysgo AG</td>
</tr>
<tr>
<td>AbsInt</td>
<td>Absint Angewandte Informatik GmbH</td>
</tr>
</tbody>
</table>
Design Tooling

- New tools features to support co-engineering and interaction points.
- Improving tools interoperability through
  - standardised formats and interfaces.
- Subsets covering one or several use cases.
- Dynamic perimeters depending on lifecycle.

Examples of Involved Tools and Their Improvements

- **CHESS (Intecs)**
  - Support for SysML/UML/MARTE-based model-driven, component-based development of high-integrity software systems for different domains.
  - *To be done in Aquas*: performance considerations in early stages, code generation improved by security features, WCET analysis, analysis of the impact of specific security measures on the overall performance.

- **FramaC (CEA)**
  - A tool suite for formal code analysis and verification of safety as well as security related aspects using various forms of static analysis.
  - *To be done in Aquas*: analyzable assertions in generated code to increase trust, static value analysis to quickly discover safety/security code issues, modular formal verification applicable on (sub-)systems whose (re-)analysis turns out necessary.
Design Tooling

- **Art2kitekt – A2K (ITI)**
  - Tool-suite for modeling, simulation, and analysis of embedded critical systems.
  - *To be done in Aquas*: new features for modelling and analysis of safety and performance of real-time systems, generating code skeletons for various operating systems, sensitivity analysis, relating analysis results to specifications.

- **Safety and Cyber Architects (ALL4TEC)**
  - Model-based tools for safety and security analysis based on fault trees and attack trees.
  - *To be done in Aquas*: bridge with tools for system modeling (e.g., CHESS), support for integrated safety/security co-analysis.

- **SysML-Sec (MTTP)**
  - Environment to design safe and secure embedded systems with an extended version of the SysML language.
  - *To be done in Aquas*: support for dealing with security in relation with safety and performance through improved modeling environments, updated model operators, improved/added views, integration of new model transformations.
Design Tooling

- **ANaConDA (BUT)**
  - A framework for dynamic code analysis and noise-based testing targeting in particular concurrency-related issues.
  - *To be done in Aquas:* improved checkers to allow for efficient re-analysis whenever a need be (interaction points), richer checkers to analyze more properties, focusing the analysis on sub-systems currently found problematic, collection of suitable metrics to steer analysis/testing.

- **Astrée/TimingProfiler (AbsInt)**
  - Tools for static code analysis targeting safety, security, and performance.
  - *To be done in Aquas:* enable safety/security analysis of embedded OSs (with a stress on PikeOS) speeding up development of applications based on such systems, light-weight timing analysis applicable in early development stages.

- **OpenCert (Tecnalia)**
  - An Eclipse based tool and open platform for evolutionary certification of safety-critical systems.
  - *To be done in Aquas:* strengthened and enhanced support for modelling safety, security, and performance aspects within assurance cases.