Deliverable 5.3

Communication/dissemination material (V2)

This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737475. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Spain, France, United Kingdom, Austria, Italy, Czech Republic, Germany.

DISSEMINATION LEVEL		
X	**PU**	Public
	CO	Confidential, only for members of the consortium (including the Commission Services)

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	AQUAS
Project Full Name:	Aggregated Quality Assurance in Systems
Grant Agreement No.:	737475
Programme	ICT-1: Cyber-Physical-Systems
Instrument:	Research & innovation action
Start date of project:	01-05-2017
Duration:	36 months
Deliverable No.:	D5.3
Document name:	Communication/dissemination material (V2)
Work Package	WP5
Associated Task	Task(s) 5a.3
Nature [1]	DEC
Dissemination Level [2]	PU
Version:	2.0
Actual Submission Date:	31-01-2019
Contractual Submission Date	31-01-2019
Editor: Institution: E-mail:	Bohuslav Křena BUT krena@fit.vutbr.cz

[1] **R**=Report, **DEC**= Websites, patents filling, etc., **O**=Other
[2] **PU**=Public, **CO**=Confidential, only for members of the consortium (including the Commission Services)

Change Control

Document History

Version	Date	Change History	Author(s)	Organisation(s)
	21-01-2019	Concept and structure of the deliverable agreed	Bohuslav Křena Filip Veljković	BUT TASE
	25-01-2019	Call for inputs	Bohuslav Křena	BUT
1.1	29-01-2019	Dissemination material summarised	Bohuslav Křena	BUT
1.2	29-01-2019	Internal review and text polishing	Ondřej Lengál	BUT
1.3	30-01-2019	Additional improvements	Bohuslav Křena	BUT
2.0	31-01-2019	Final version	Filip Veljković	TASE

Distribution List

Date	Issue	Group
29-01-2019	Internal review	Ondřej Lengál (BUT) David Bařina (BUT)
31-01-2019	Final version	EC AQUAS.ALL

Table of Contents

Executive Summary

This deliverable describes the dissemination material created or updated from the last version of this deliverable (i.e., v1 from January 2018, M9). The previous version is appended at the end of this document to support grouping of different versions of the same deliverable. The Annex is not a subject of evaluation as it was accepted by the reviewers in year 1. However, it can help the reviewers in recognizing the progress made in the past 12 months of AQUAS.

Dissemination material provides information about the AQUAS project, its progress, and achieved results. As the project evolves, the dissemination material needs to be updated according to the current project progress. This deliverable is therefore considered to evolve during the project duration. This is its second version whereas its last version will be released in January 2020 (V3, M33).

More about the dissemination activities that are supported by the dissemination material described in this deliverable can be found in deliverable D5.4: Reports on communication and dissemination activities (V1, M23), which release is planned within two months after the submission of this deliverable (March 2019).

1 Introduction

Dissemination and communication activities are a strong contributor to the project success. To support dissemination and exploitation, several kinds of dissemination material need to be prepared in order to present the project and its results to the general public and stakeholders from the ECSEL focused areas: ‘Design Technology’, ‘Cyber-physical Systems’, and ‘European Asset Protection’. In particular, communication and dissemination activities should raise the public awareness of the challenges faced with the provision of safe, secure, and efficient cyber-physical systems.

As the project evolves, different information may be used for the dissemination—in the first stages, the existence and main ideas of the project have been communicated, while now, we report more about the project progress and the achieved results. The status of the dissemination material has to be summarised and reported three times during the project:

- First (V1) in month 9,
- Second (V2) in month 21 (the current version),
- Final (V3) in month 33.

2 Dissemination material

Different forms of dissemination material are needed to present the project at different events and using different channels. In the following, we report about the dissemination material that has been created or updated from the last version of this deliverable.

2.1 Project poster

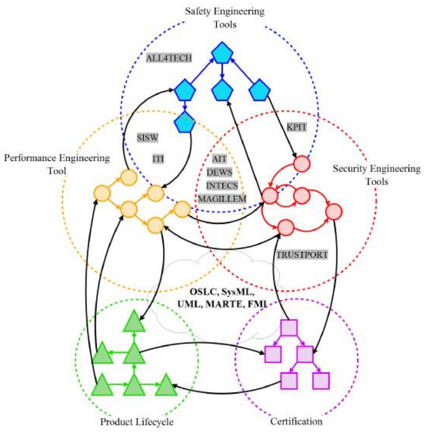
The project poster is useful for booth presentations at fairs as well as for poster sessions at conferences and workshops. Within the last year, it has been adjusted for and used at the ECSEL JU symposium in Brussels (June 2018) and at Euromicro DSD 2018 conference in Prague (August 2018). Pictures of the posters follow (the first one is from the ECSEL JU symposium, the second one from the Euromicro DSD conference).

AQUAS

AQUAS SAFETY SECURITY PERFORMANCE

Project idea

Growing complexity of the systems we engineer in modern society creates increasing difficulty with providing assurance for factors including safety, security and performance, particularly for safety critical systems such as the transportation, medical devices, aerospace or the industrial control domains.



Approach

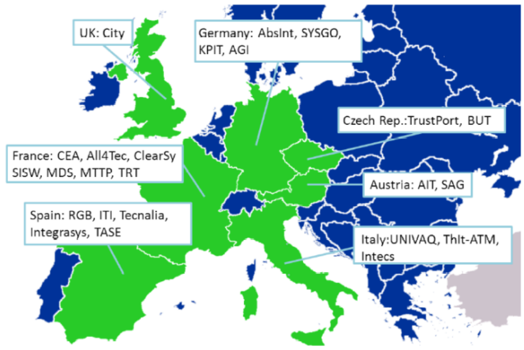
- Modelling and analysis methods and tools to capture safety, security and performance requirements and threats holistically.
- Model-based co-design for safety, security and performance, including modelling the effectiveness of intrusion detection, combining levels of defence, modelling of interdependence between subsystems and considering evolution of effectiveness of defence in view of evolving threats.
- Analysis of design decisions and their impact on safety, security and performance via design space exploration, quantitative modelling and sensitivity analysis.
- Assuring that the threats are effectively handled by state of the art certification strategies and automated HW/SW joint verification techniques.

Start	5/2017	Duration	36 months
Type	ECSEL-RIA	Costs	15.5 M€
Partners	23	Countries	7

Coordinator: Filip Veljković filip.veljkovic@thalesaleniaspace.com

Coordinator: Filip Veljković
Thales Alenia Space
Czech coordinator: Tomáš Vojnar
Brno University of Technology

safety – security – performance trade-offs • co-engineering

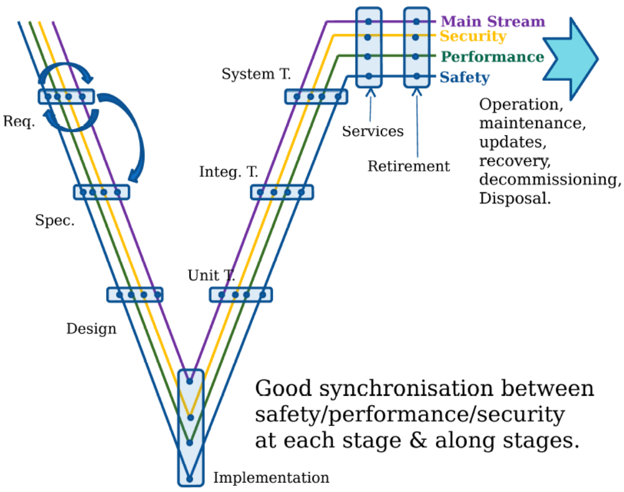


Growing complexity of the systems we engineer in modern society creates increasing difficulty with providing assurance for factors including safety, security and performance, particularly for safety critical systems.

The AQUAS approach: Co-Engineering

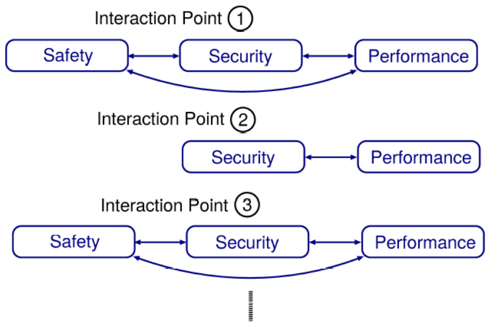
- Model-based co-design for safety, security, and performance.
- Modelling and analysis methods and tools handling safety, security, and performance requirements holistically.
- Analysis of design decisions and their impact on safety, security, and performance.
- Effective use of state of the art certification strategies and combined automated verification techniques.

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

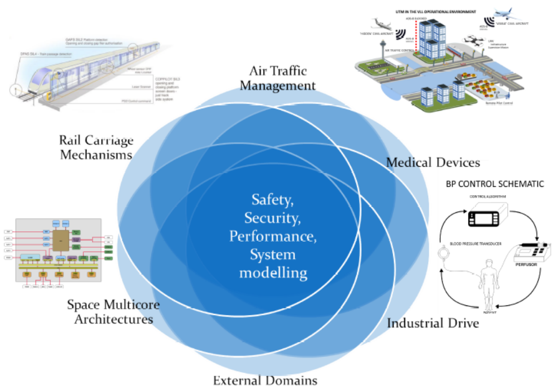


Interaction Points

- Design decisions must rely on a holistic view of the system (safety, security, and performance).
- Through the development cycle, initial decisions and allocation of goals and properties are refined.
- 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 to get a new trade-off.



Application Domains



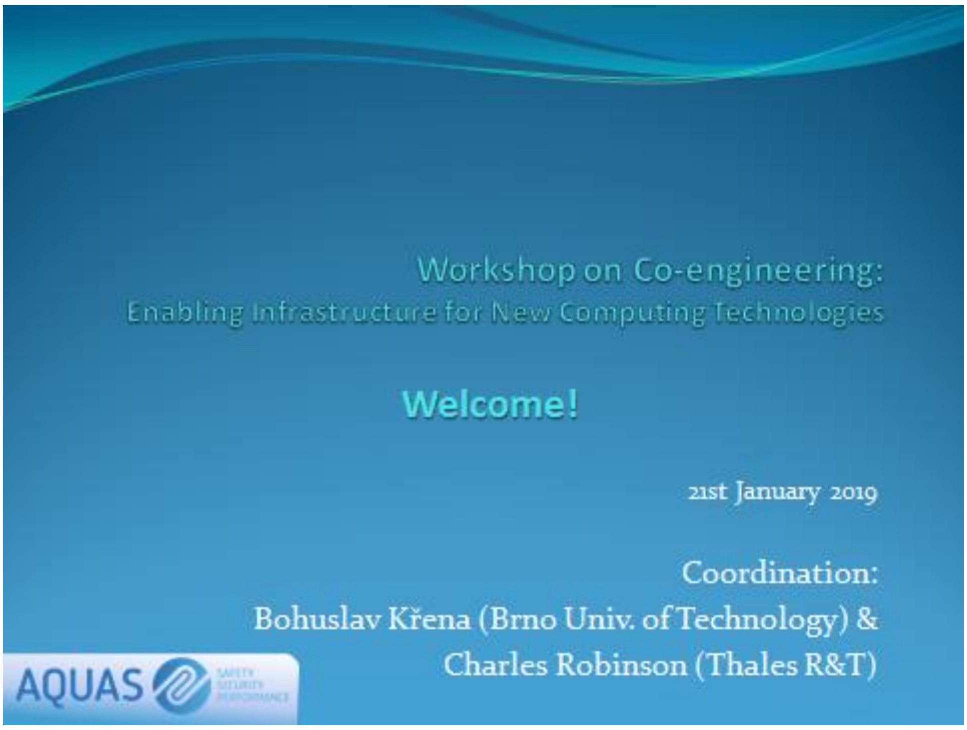
2.2 Project presentation

An important dissemination activity that we have performed within the second year of the project was the organization of the **CE-ELITE: Workshop on Co-engineering – Enabling Infrastructure for New Computing Technologies** (https://www.hipeac.net/2019/valencia/#/schedule/sessions/7638/) within the HiPEAC'19 conference (High Performance and Embedded Architecture and Compilation).

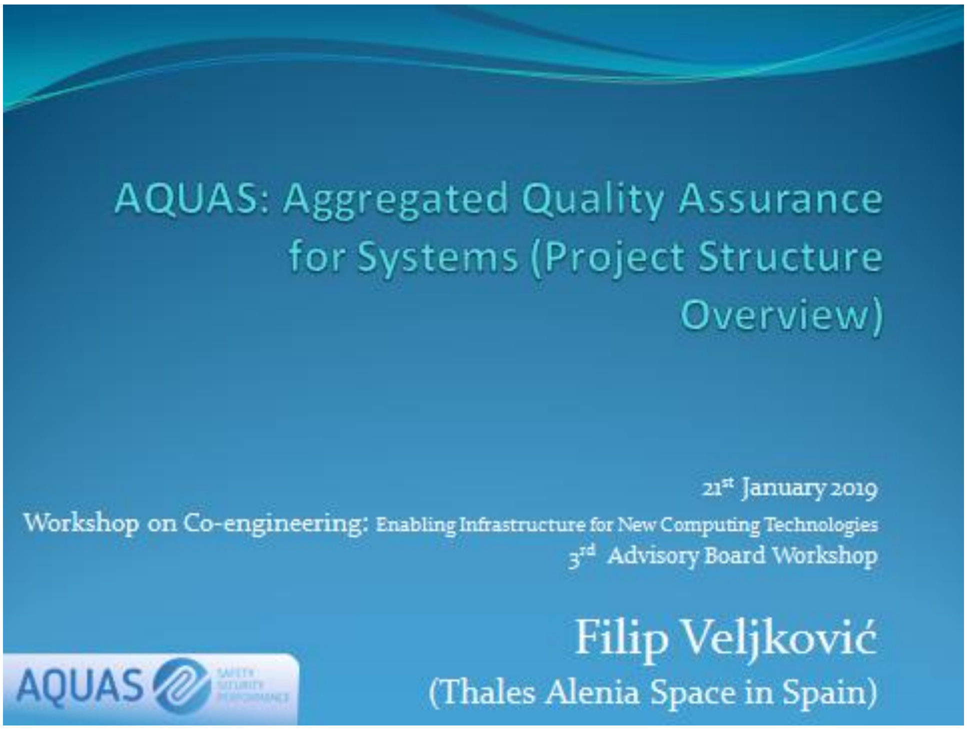
This workshop was connected also with a face-to-face meeting with the External Advisory Board (EAB) of the project. Because not all members of the EAB could participate personally, remote access was provided to them as well.

To make this workshop possible, several presentations were prepared. These presentations were used not only within the workshop, but they will also be available at the web page of the conference. Thus, we see them as an important dissemination material describing the current status of the project and therefore, we list them here.

2.2.1 Welcome



2.2.2 Overview



Co-Engineering into mainstream practices

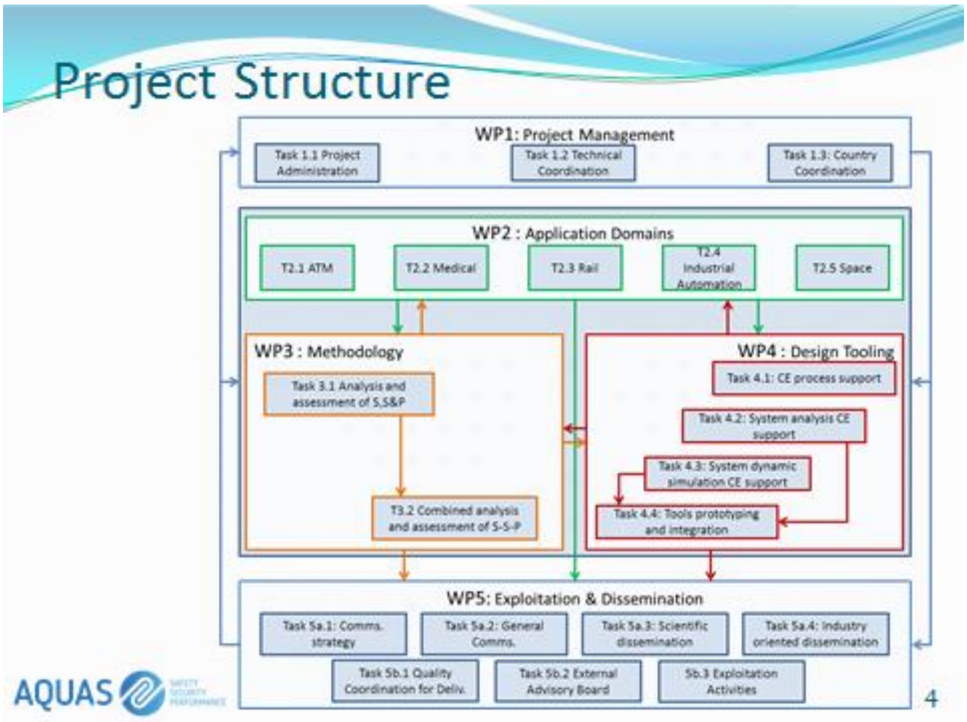
We are investigating Co-Engineering techniques for safety, security and performance of critical and complex embedded systems

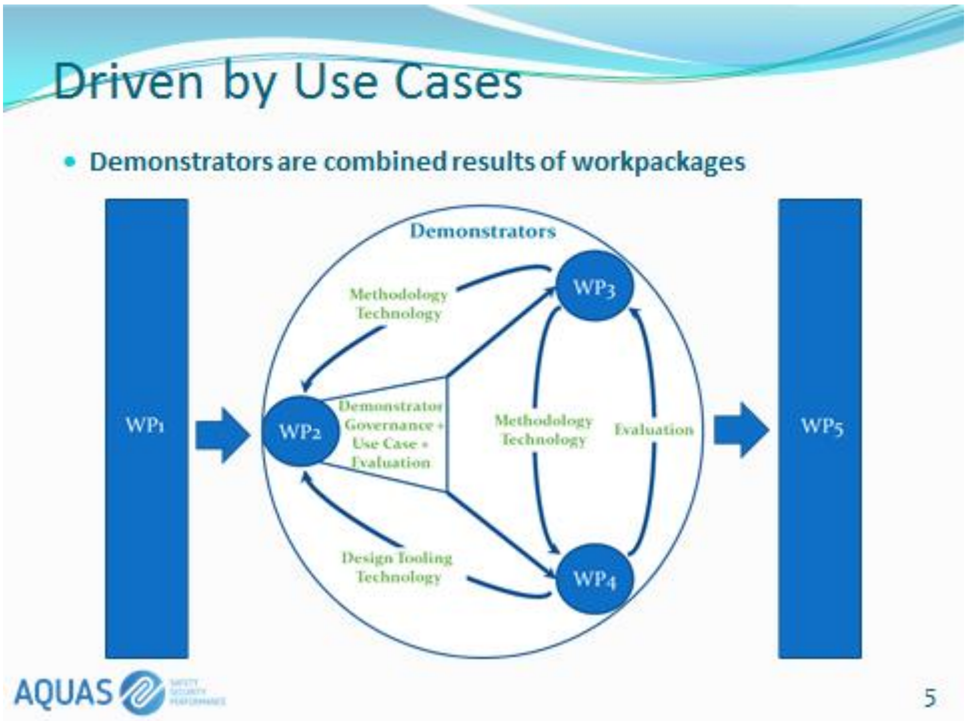
AQUAS SAFETY SECURITY PERFORMANCE 2

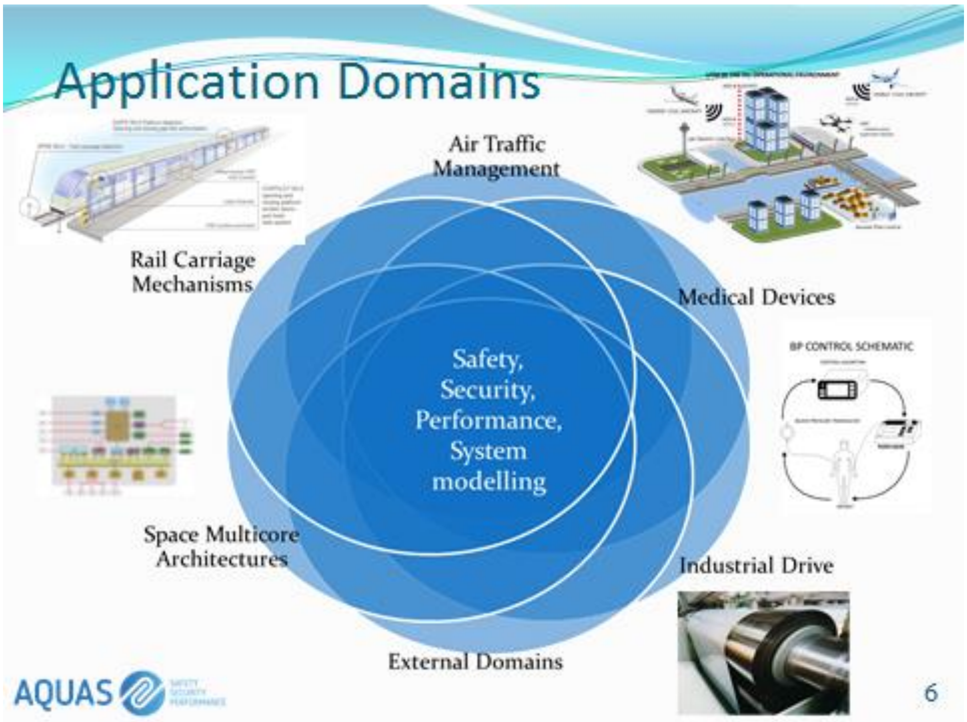
Main Goals

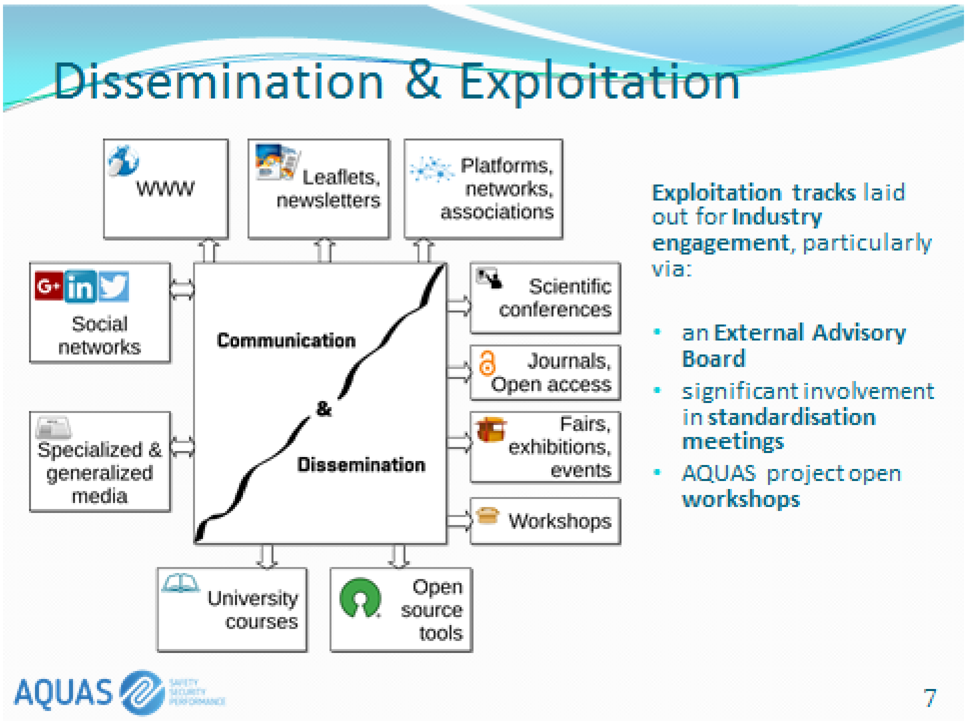
- **Co-engineering inside and across product lifecycle phases. Standards evolution. The three key goals: CE, PLC4CE, SE4CE**
- **Achieved by establishing a global concept framework for safety, security, and performance co-engineering:**
  - Based on the needs of **industrial application** domains
  - 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**

AQUAS SAFETY SECURITY PERFORMANCE 3

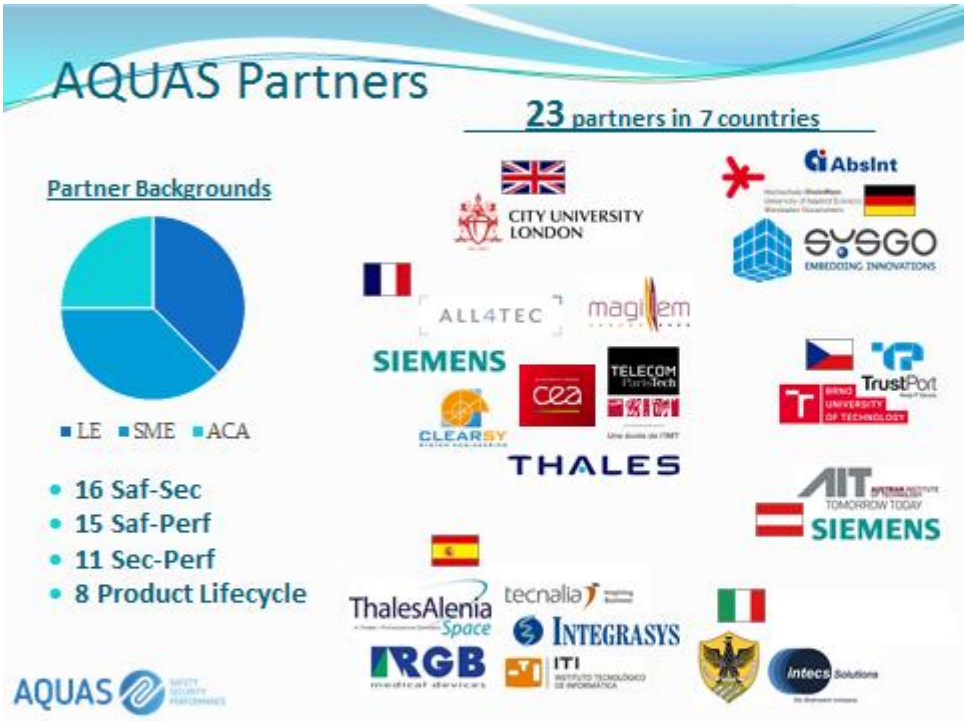

Project Structure
WP1: Project Management
Task 1.1 Project Administration
Task 1.2 Technical Coordination
Task 1.3: Country Coordination
WP2 : Application Domains
T2.1 ATM
T2.2 Medical
T2.3 Rail
T2.4 Industrial Automation
T2.5 Space
WP3 : Methodology
Task 3.1 Analysis and assessment of S,S&P
T3.2 Combined analysis and assessment of S-S-P
WP4 : Design Tooling
Task 4.1: CE process support
Task 4.2: System analysis CE support
Task 4.3: System dynamic simulation CE support
Task 4.4: Tools prototyping and integration
WP5: Exploitation & Dissemination
Task 5a.1: Comms. strategy
Task 5a.2: General Comms.
Task 5a.3: Scientific dissemination
Task 5a.4: Industry oriented dissemination
Task 5b.1 Quality Coordination for Deliv.
Task 5b.2 External Advisory Board
5b.3 Exploitation Activities
AQUAS
4

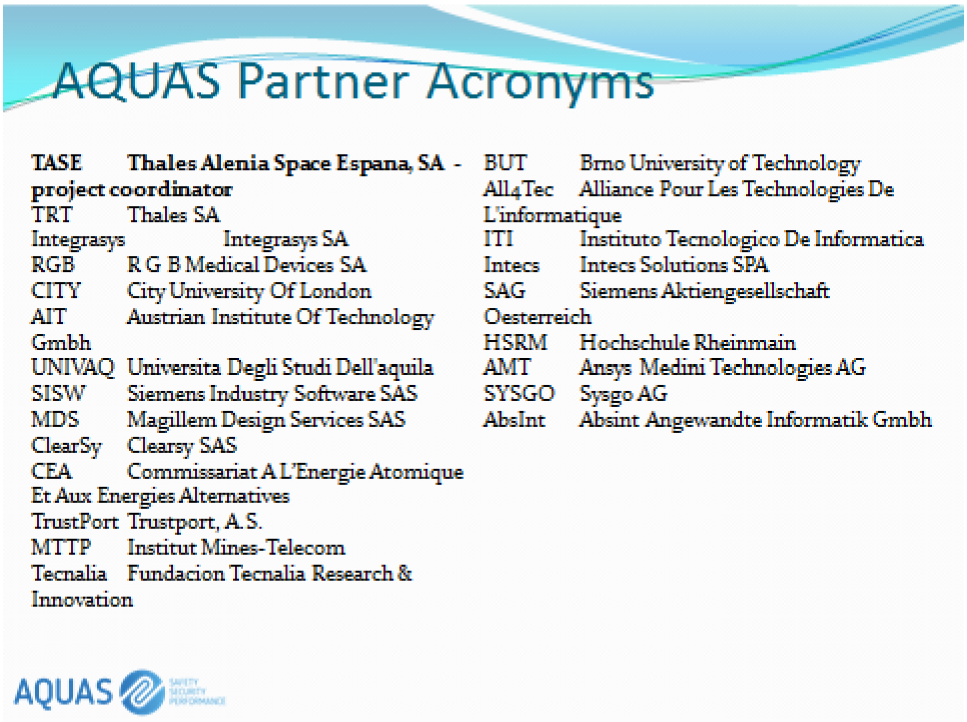

Driven by Use Cases
Demonstrators are combined results of workpackages
WP1
Demonstrators
Methodology Technology
WP3
WP2
Demonstrator Governance + Use Case + Evaluation
Methodology Technology
Evaluation
Design Tooling Technology
WP4
WP5
AQUAS
5


Application Domains
Air Traffic Management
Rail Carriage Mechanisms
Medical Devices
Safety, Security, Performance, System modelling
Space Multicore Architectures
Industrial Drive
External Domains
BP CONTROL SCHEMATIC
AQUAS
6

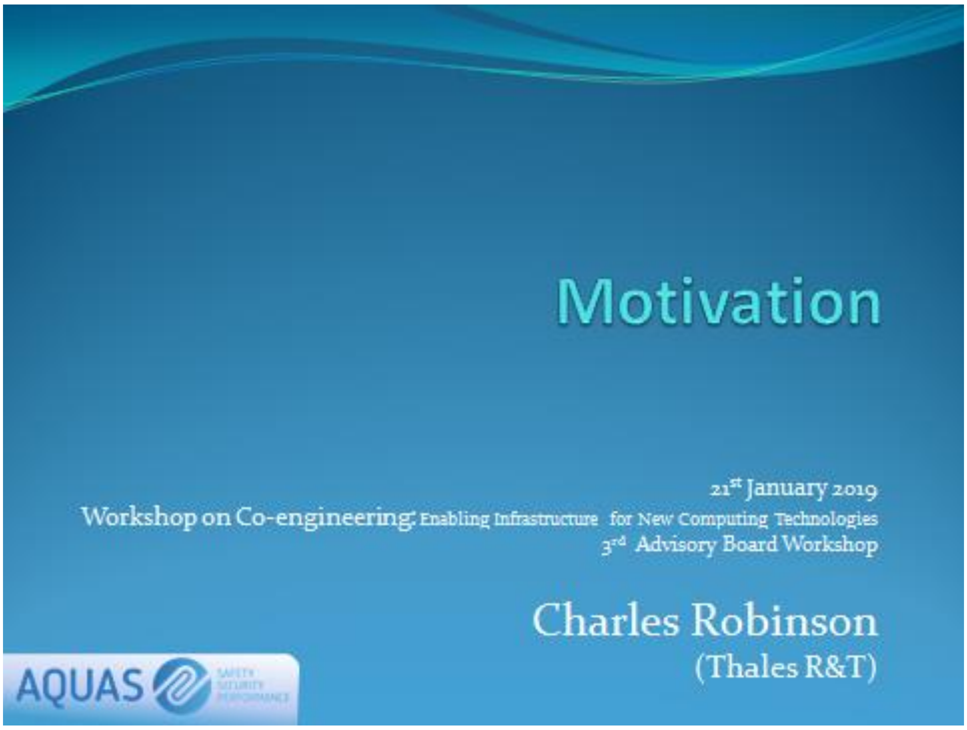

Dissemination & Exploitation
WWW
Leaflets, newsletters
Platforms, networks, associations
Social networks
Communication
&
Dissemination
Scientific conferences
Journals, Open access
Fairs, exhibitions, events
Workshops
Specialized & generalized media
University courses
Open source tools
Exploitation tracks laid out for Industry engagement, particularly via:
an External Advisory Board
significant involvement in standardisation meetings
AQUAS project open workshops
AQUAS
7

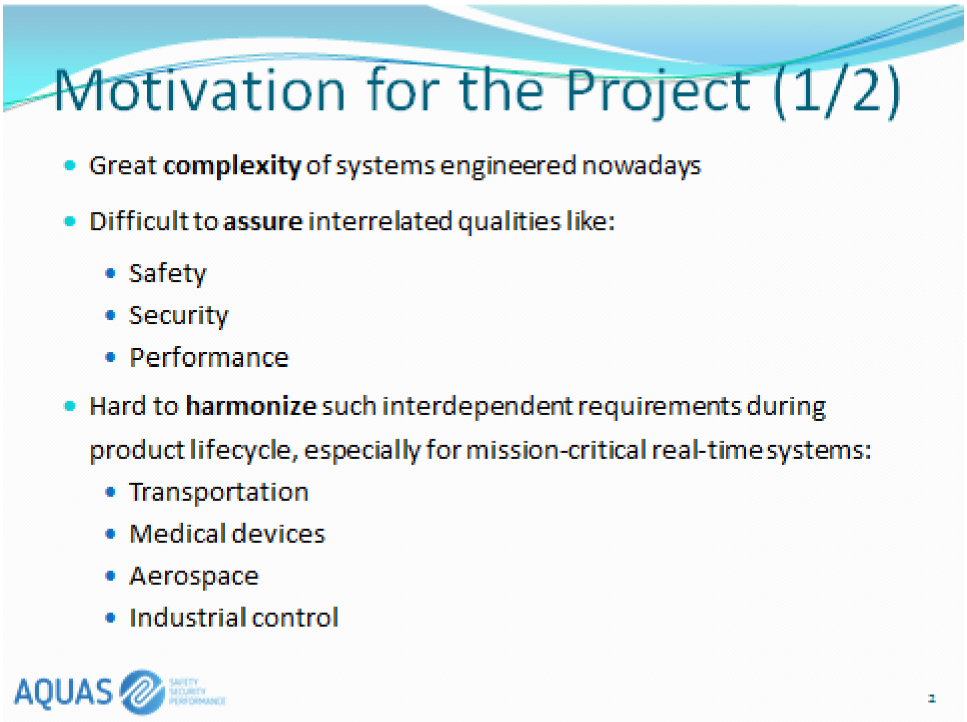

AQUAS
THANK YOU
ECSEL JU

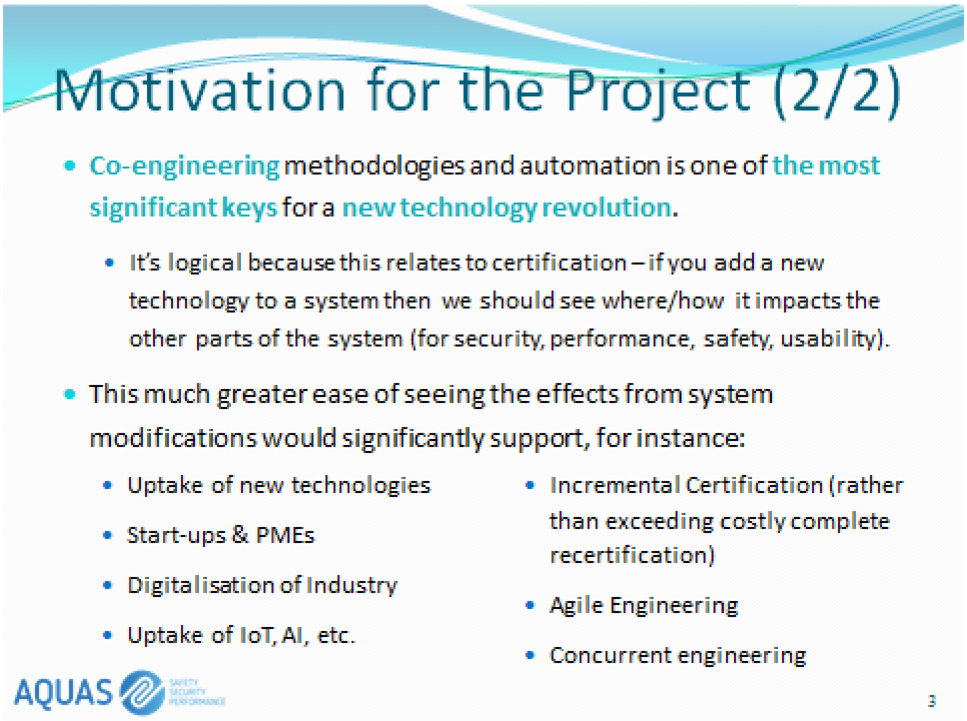

AQUAS Partners
23 partners in 7 countries
Partner Backgrounds
LE
SME
ACA
16 Saf-Sec
15 Saf-Perf
11 Sec-Perf
8 Product Lifecycle
CITY UNIVERSITY LONDON
AbsInt
SYSGO
ALL4TEC
SIEMENS
cea
TELECOM ParisTech
CLEARSY
THALES
TrustPort
AIT
TOMORROW TODAY
SIEMENS
ThalesAlenia Space
tecnalia
INTEGRASYS
RGB
ITI
intecs
AQUAS

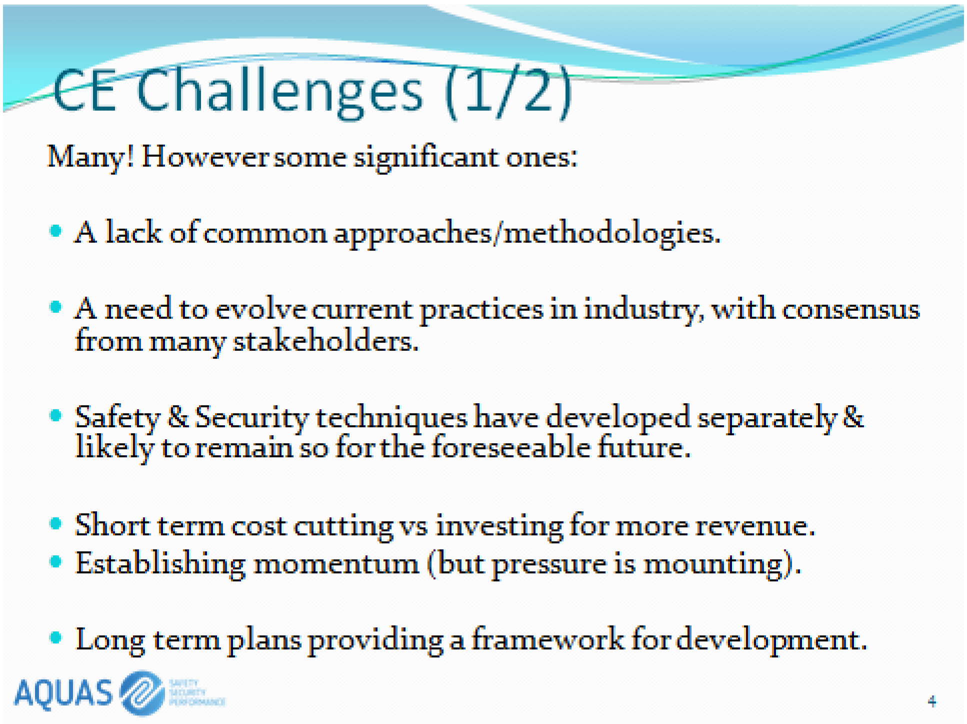


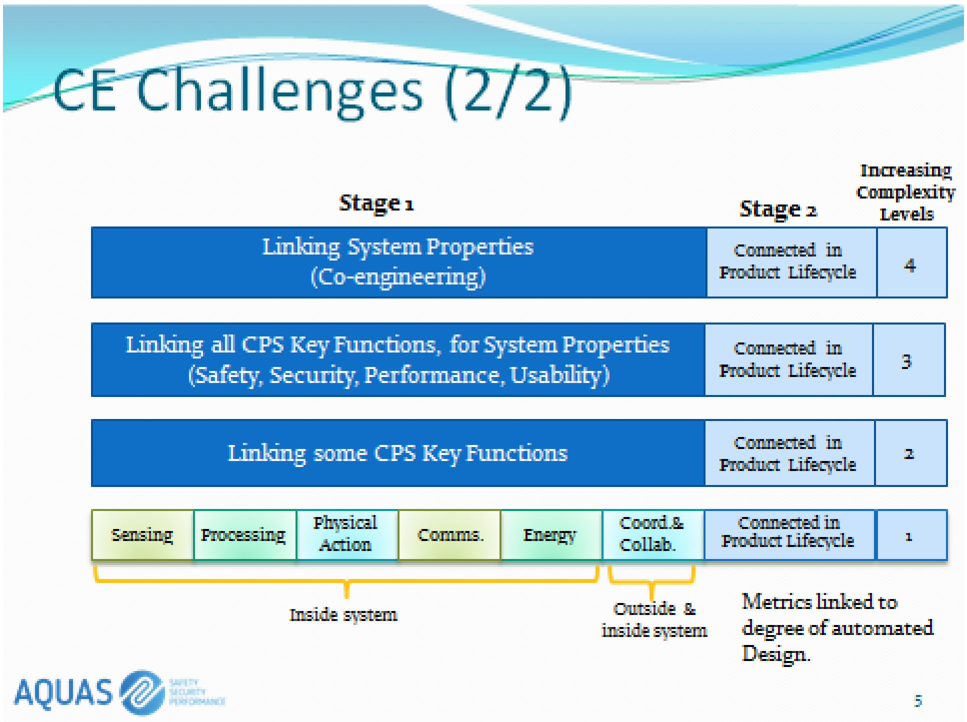
2.2.3 Motivation

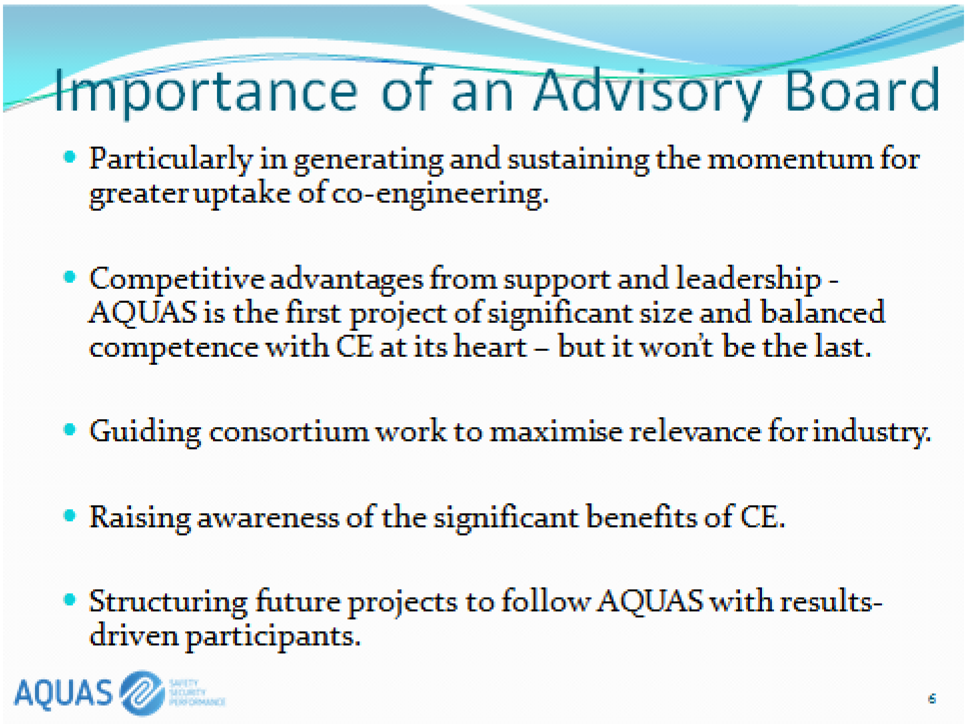



Motivation for the Project (1/2)
Great complexity of systems engineered nowadays
Difficult to assure interrelated qualities like:
Safety
Security
Performance
Hard to harmonize such interdependent requirements during product lifecycle, especially for mission-critical real-time systems:
Transportation
Medical devices
Aerospace
Industrial control
AQUAS
2

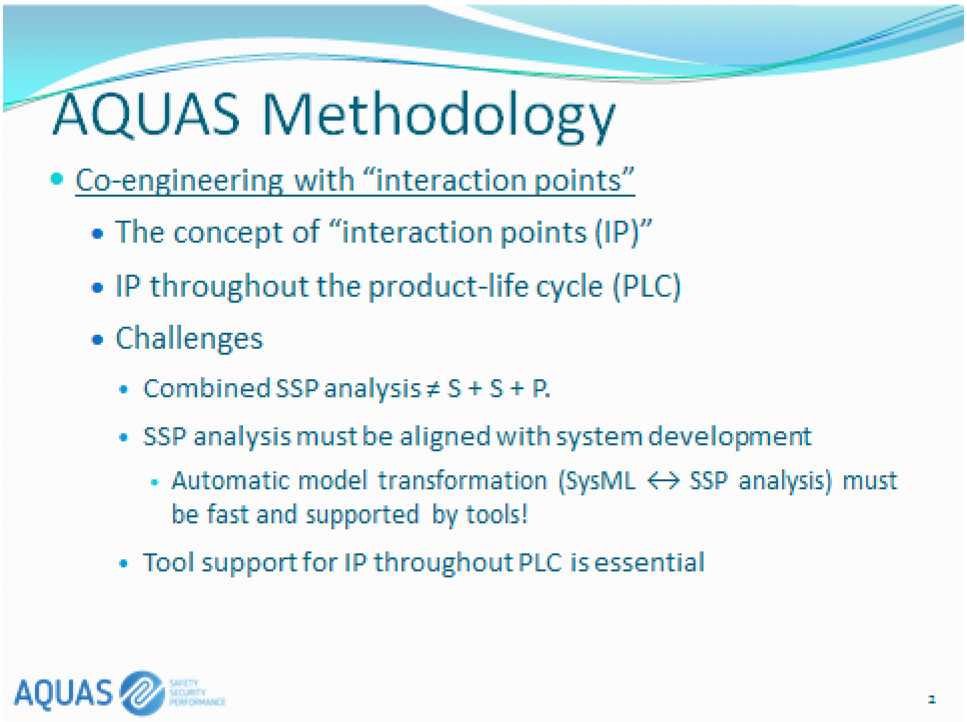

Motivation for the Project (2/2)
Co-engineering methodologies and automation is one of the most significant keys for a new technology revolution.
It's logical because this relates to certification – if you add a new technology to a system then we should see where/how it impacts the other parts of the system (for security, performance, safety, usability).
This much greater ease of seeing the effects from system modifications would significantly support, for instance:
Uptake of new technologies
Start-ups & PMEs
Digitalisation of Industry
Uptake of IoT, AI, etc.
Incremental Certification (rather than exceeding costly complete recertification)
Agile Engineering
Concurrent engineering
AQUAS
3

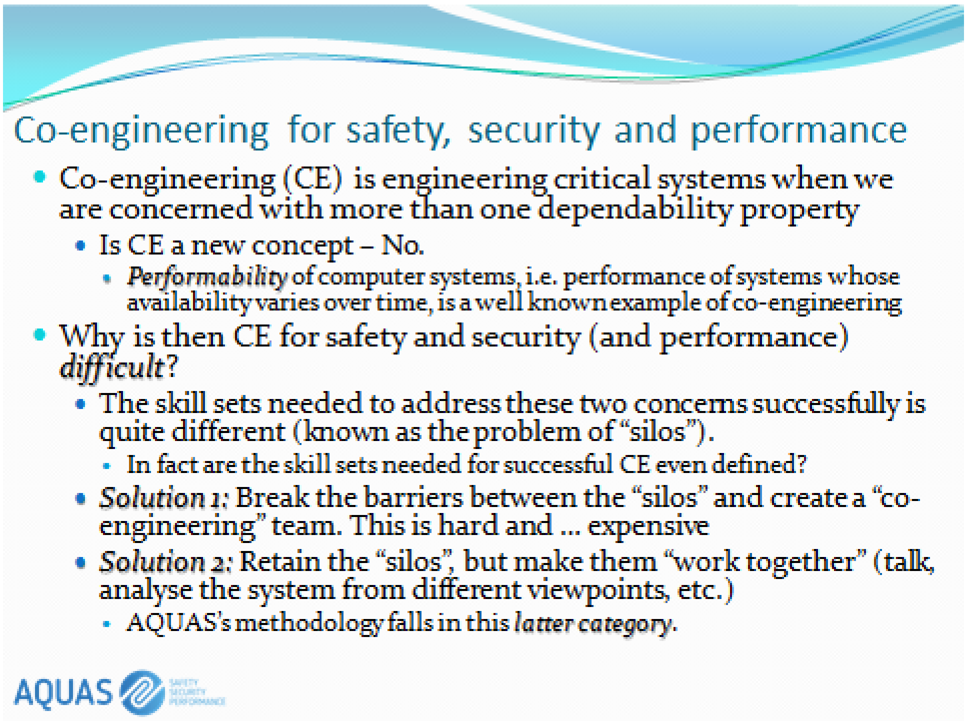

CE Challenges (1/2)
Many! However some significant ones:
A lack of common approaches/methodologies.
A need to evolve current practices in industry, with consensus from many stakeholders.
Safety & Security techniques have developed separately & likely to remain so for the foreseeable future.
Short term cost cutting vs investing for more revenue.
Establishing momentum (but pressure is mounting).
Long term plans providing a framework for development.
AQUAS
4


CE Challenges (2/2)
Stage 1
Stage 2
Increasing Complexity Levels
Linking System Properties (Co-engineering)
Connected in Product Lifecycle
4
Linking all CPS Key Functions, for System Properties (Safety, Security, Performance, Usability)
Connected in Product Lifecycle
3
Linking some CPS Key Functions
Connected in Product Lifecycle
2
Sensing
Processing
Physical Action
Comms.
Energy
Coord.& Collab.
Connected in Product Lifecycle
1
Inside system
Outside & inside system
Metrics linked to degree of automated Design.
AQUAS
5



2.2.4 Methodology


AQUAS Methodology
Co-engineering with "interaction points"
The concept of "interaction points (IP)"
IP throughout the product-life cycle (PLC)
Challenges
Combined SSP analysis ≠ S + S + P.
SSP analysis must be aligned with system development
Automatic model transformation (SysML ↔ SSP analysis) must be fast and supported by tools!
Tool support for IP throughout PLC is essential
AQUAS
2


Co-engineering for safety, security and performance
Co-engineering (CE) is engineering critical systems when we are concerned with more than one dependability property
Is CE a new concept – No.
Performability of computer systems, i.e. performance of systems whose availability varies over time, is a well known example of co-engineering
Why is then CE for safety and security (and performance) difficult?
The skill sets needed to address these two concerns successfully is quite different (known as the problem of "silos").
In fact are the skill sets needed for successful CE even defined?
Solution 1: Break the barriers between the "silos" and create a "co-engineering" team. This is hard and … expensive
Solution 2: Retain the "silos", but make them "work together" (talk, analyse the system from different viewpoints, etc.)
AQUAS's methodology falls in this latter category.
AQUAS

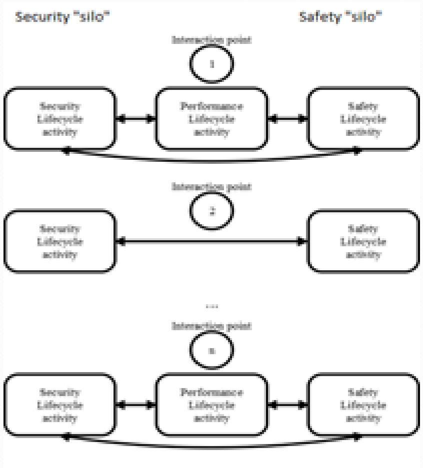
The AQUS: Interaction points

At certain points in the product life-cycle (PLC), system developers/operators *take decisions* about how to progress with the development/apply patches/etc. These decisions require a *holistic view on the system*, i.e. account simultaneously for all attributes of interest, safety, security and performance. Need for *combined analysis*.

As development progresses, the initial decisions and allocation of goals and properties to components are *subjected to refinements*. Each refinement step may or may not trigger an interaction point.

If as a result of a refinement *significant deviations* from the previous allocation of goals/properties are detected, a new trade-off has to be established between the assigned *goals and component properties*.

A similar concept is adopted in *SAE J3061: CYBERSECURITY GUIDEBOOK FOR CYBER-PHYSICAL VEHICLE SYSTEMS*



AQUAS SAFETY SECURITY PERFORMANCE

Combined analysis ≠ S + S + P

- Combined analysis is not just ***safety-only*** + ***security-only*** analyses.
- A truly ***combined SSP analysis*** *requires* an explicit and credible ***model of dependence*** between the properties of interest, e.g.:
  - Conflicting Safety and Security requirements lead to the need for trade-off analysis:
  - successful attacks may *impair safety* against accidental faults, e.g. by eliminating the ***safe state*** (real attacks on safety are well documented)
    - "If it is not secure it is not safe"
  - strengthening security controls typically affects performance (e.g. response time)
    - and increases the likelihood of missing a hard real-time deadline

Credible trade-off analysis is impossible without credible combined analysis

AQUAS SAFETY SECURITY PERFORMANCE

Qualitative combined SSP analysis

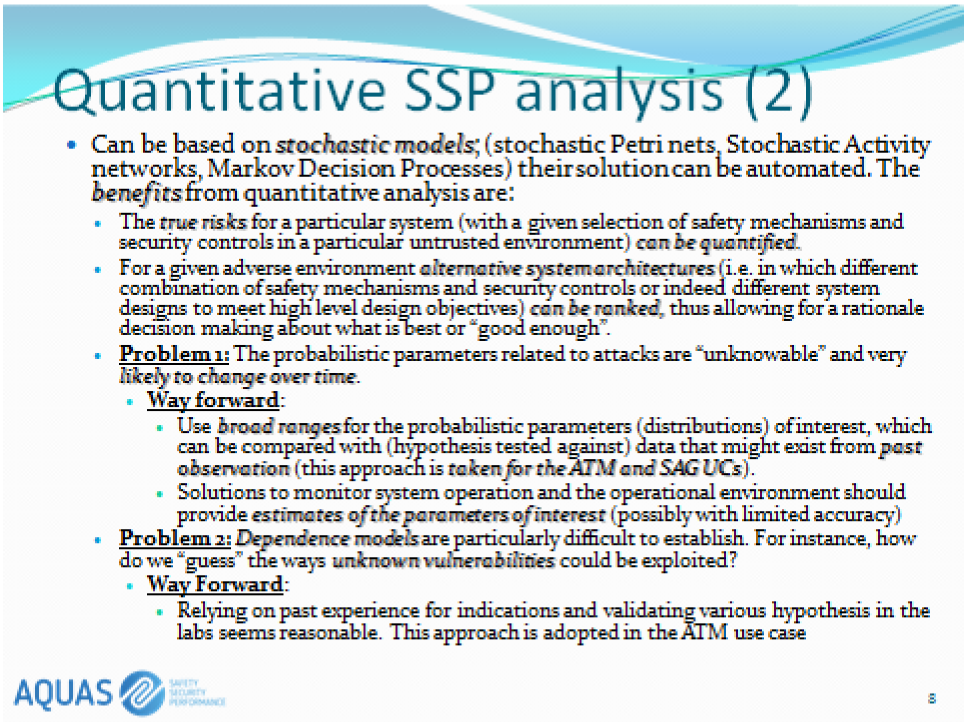
- Apply hazard analysis to identify the security incidents with impact on safety and performance.
  - A range of well established methods – FTA/Attack trees, FME(C), HAZOP developed for form safety engineering *have been extended* to account for security (some are covered in the later talks today).
  - Build "*interference matrices*". These should be analysed by safety and security experts (ideally in joint sessions).
  - Eventually, the experts seek to resolve all elements in the "interference matrix" until "good enough" resolutions are found.
    - **Problem 1:** How do we know that that the resolutions are "good enough". We rely on ***engineering judgement***, which may be deficient.
    - **Problem 2:** Even for systems of moderate size "interference matrices" quickly become quite large and analysing them becomes difficult and error-prone, especially if done manually.
- Qualitative analyses are covered further in a separate talk later today.

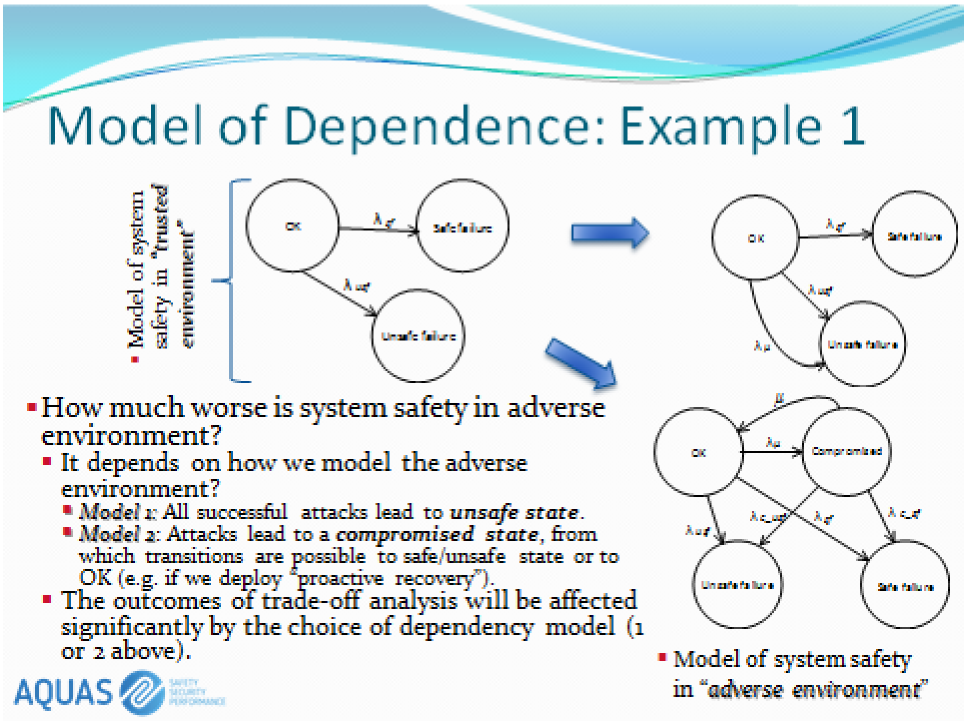
AQUAS SAFETY SECURITY PERFORMANCE 6

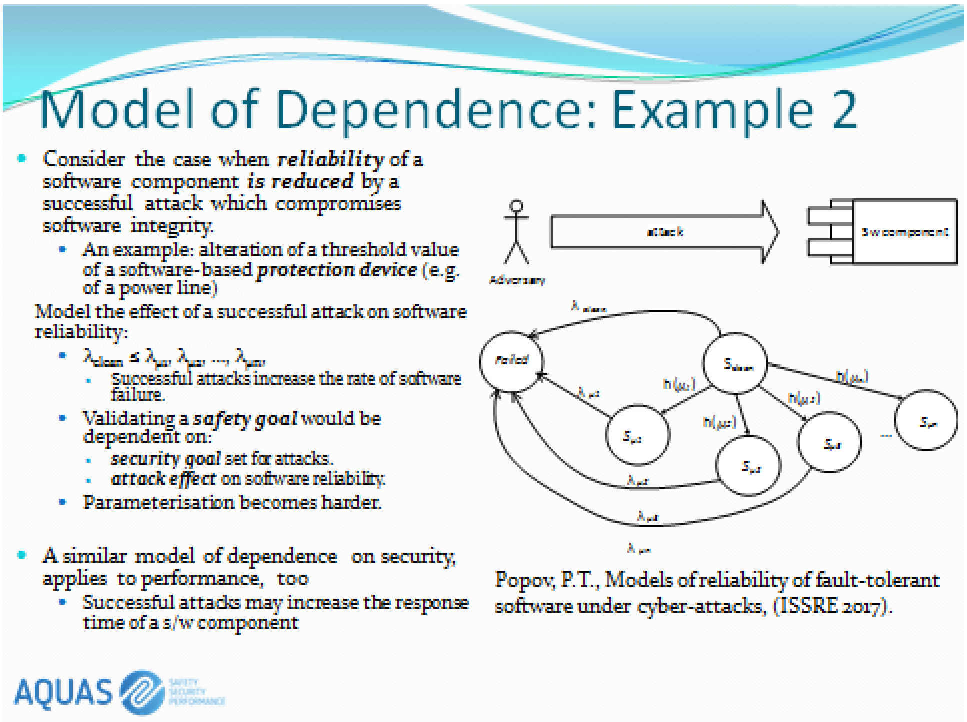
Quantitative Combined SSP analysis

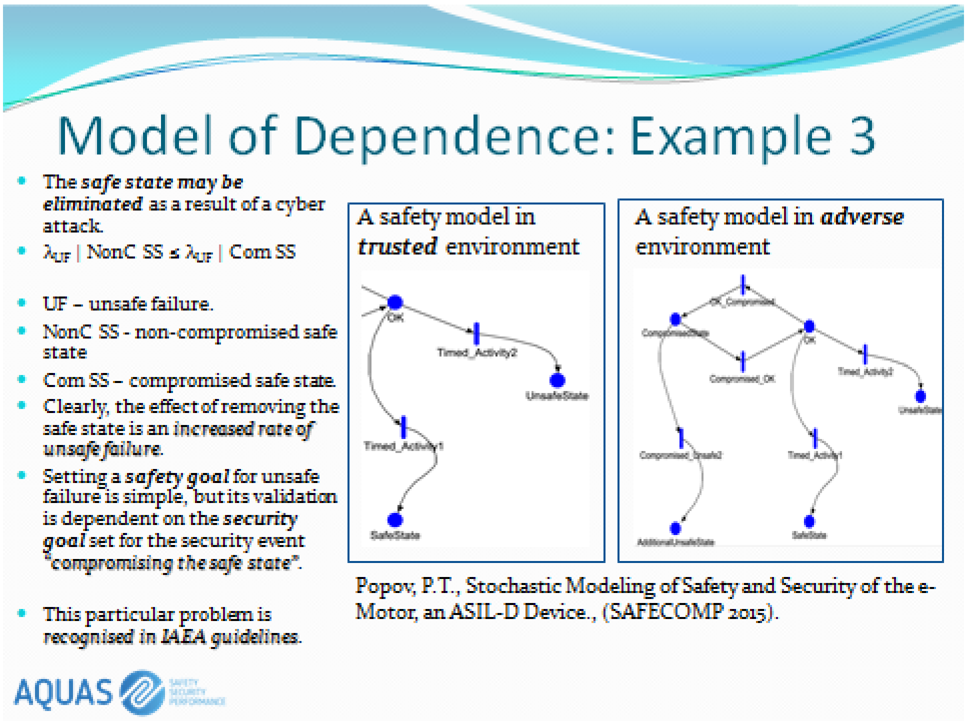
- Hazard analyses to identify the security threats that may impact the safety and performance is complemented by:
  - Judgement about the *likelihood* of various events.
    - Attack occurrence
    - Attack success
  - An explicit ***model of dependence*** between non-functional properties of interest is *needed*. Successful attacks may:
    - affect (eliminate) the functionality of a *safe state*, or
    - increase the *rate of failure* of software components, thus increasing the likelihood of *unsafe system failures*, established by safety analysis conducted for trusted environment
    - The questions that we need to resolve are:
      - *How likely* is a compromise of a safety mechanism?
      - Given an attack on a software component is successful *how much* will the performance of the compromised component *deteriorate*?
      - The answers of these questions are subject to *uncertainty*. Can we quantify credibly this uncertainty, or at least establish *bounds* on it.

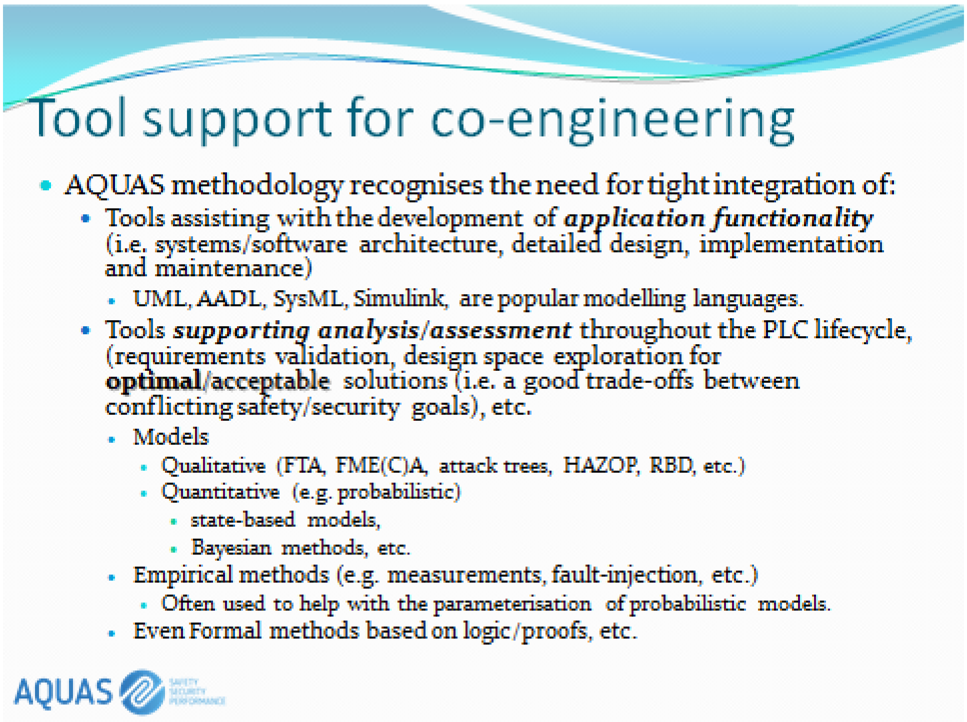
AQUAS SAFETY SECURITY PERFORMANCE 7

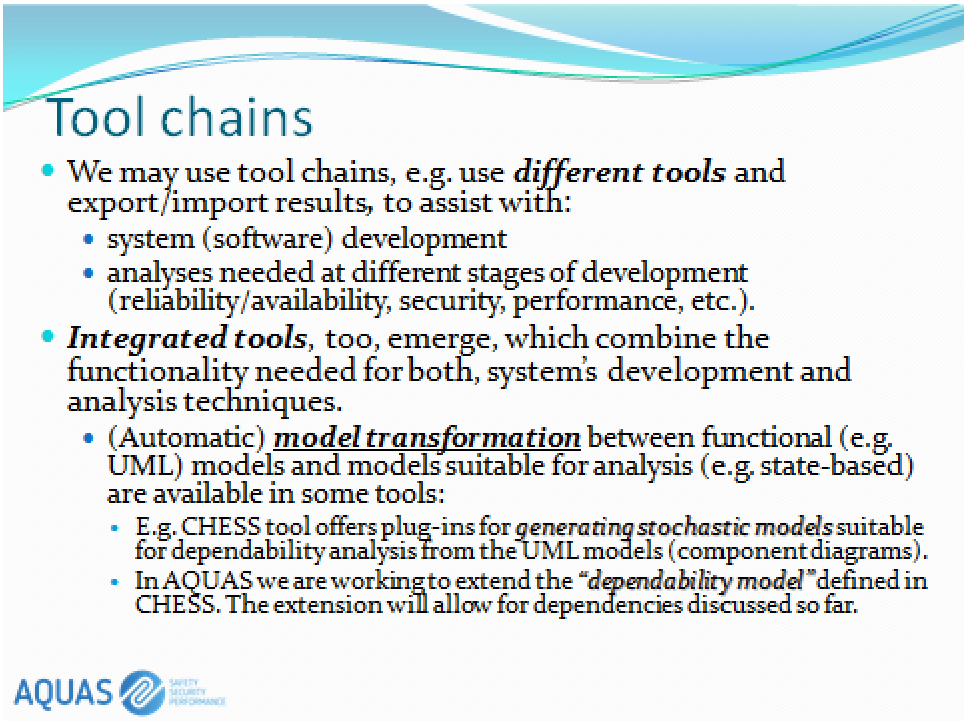

Quantitative SSP analysis (2)
Can be based on stochastic models; (stochastic Petri nets, Stochastic Activity networks, Markov Decision Processes) their solution can be automated. The benefits from quantitative analysis are:
The true risks for a particular system (with a given selection of safety mechanisms and security controls in a particular untrusted environment) can be quantified.
For a given adverse environment alternative system architectures (i.e. in which different combination of safety mechanisms and security controls or indeed different system designs to meet high level design objectives) can be ranked, thus allowing for a rationale decision making about what is best or "good enough".
Problem 1: The probabilistic parameters related to attacks are "unknowable" and very likely to change over time.
Way forward:
Use broad ranges for the probabilistic parameters (distributions) of interest, which can be compared with (hypothesis tested against) data that might exist from past observation (this approach is taken for the ATM and SAG UCs).
Solutions to monitor system operation and the operational environment should provide estimates of the parameters of interest (possibly with limited accuracy)
Problem 2: Dependence models are particularly difficult to establish. For instance, how do we "guess" the ways unknown vulnerabilities could be exploited?
Way Forward:
Relying on past experience for indications and validating various hypothesis in the labs seems reasonable. This approach is adopted in the ATM use case
AQUAS
8

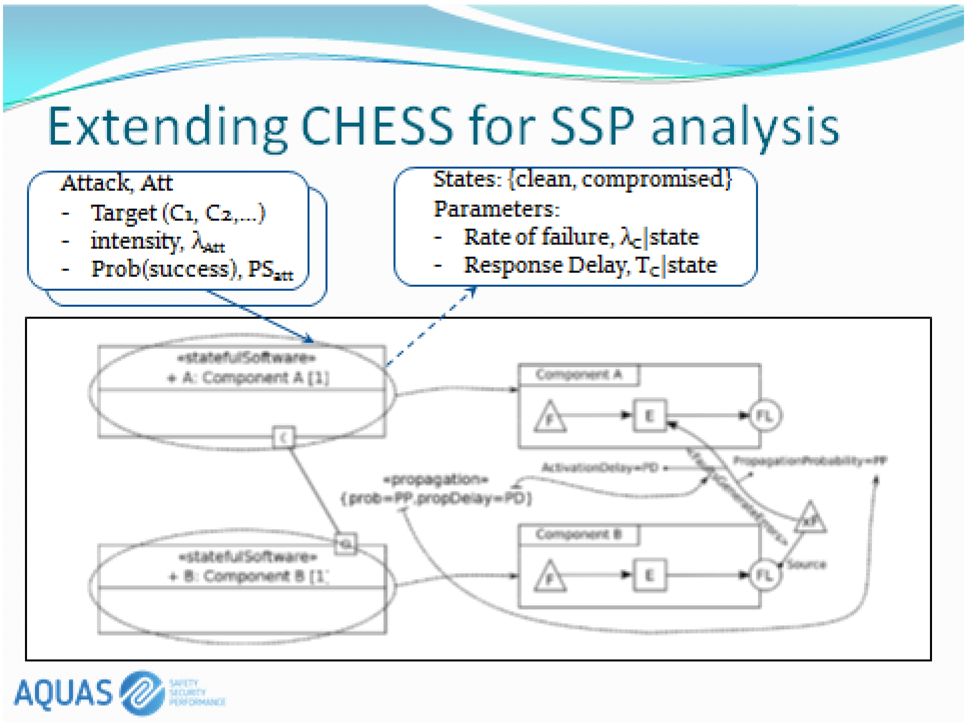

Model of Dependence: Example 1
Model of system safety in "trusted environment"
OK
Safe failure
Unsafe failure
OK
Safe failure
Unsafe failure
OK
Compromised
Unsafe failure
Safe failure
How much worse is system safety in adverse environment?
It depends on how we model the adverse environment?
Model 1: All successful attacks lead to unsafe state.
Model 2: Attacks lead to a compromised state, from which transitions are possible to safe/unsafe state or to OK (e.g. if we deploy "proactive recovery").
The outcomes of trade-off analysis will be affected significantly by the choice of dependency model (1 or 2 above).
Model of system safety in "adverse environment"
AQUAS

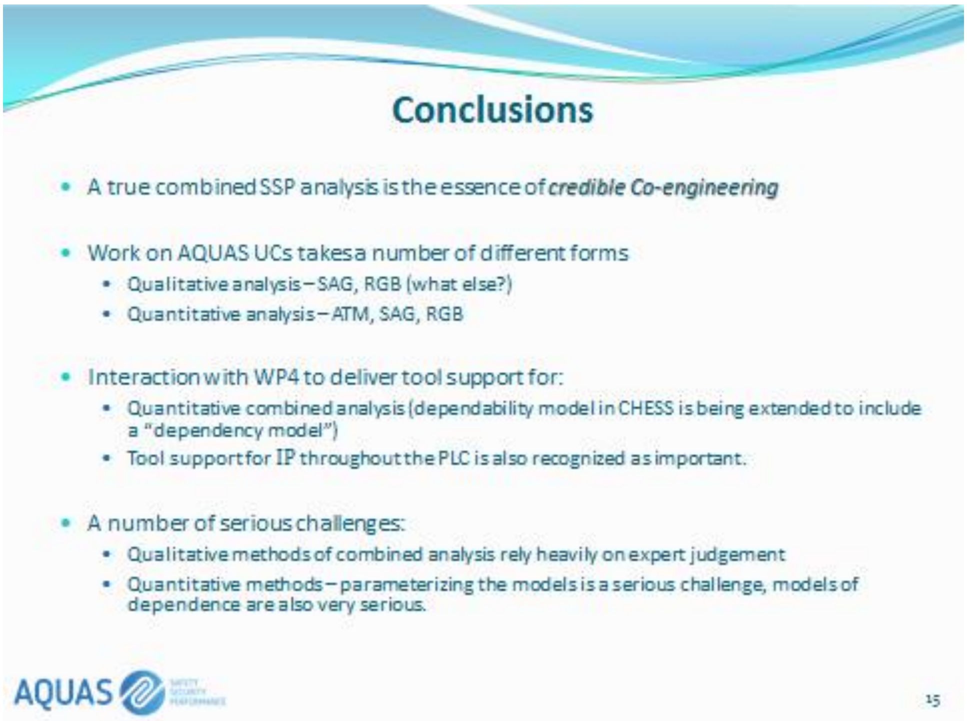

Model of Dependence: Example 2
Consider the case when reliability of a software component is reduced by a successful attack which compromises software integrity.
An example: alteration of a threshold value of a software-based protection device (e.g. of a power line)
Model the effect of a successful attack on software reliability:
λclean ≤ λμ1, λμ2, …, λμn
Successful attacks increase the rate of software failure.
Validating a safety goal would be dependent on:
security goal set for attacks.
attack effect on software reliability.
Parameterisation becomes harder.
A similar model of dependence on security, applies to performance, too
Successful attacks may increase the response time of a s/w component
attack
S/w component
Adversary
Failed
Popov, P.T., Models of reliability of fault-tolerant software under cyber-attacks, (ISSRE 2017).
AQUAS


Model of Dependence: Example 3
The safe state may be eliminated as a result of a cyber attack.
λUF | NonC SS ≤ λUF | Com SS
UF – unsafe failure.
NonC SS - non-compromised safe state
Com SS – compromised safe state.
Clearly, the effect of removing the safe state is an increased rate of unsafe failure.
Setting a safety goal for unsafe failure is simple, but its validation is dependent on the security goal set for the security event "compromising the safe state".
This particular problem is recognised in IAEA guidelines.
A safety model in trusted environment
A safety model in adverse environment
OK
Timed_Activity2
UnsafeState
Timed_Activity1
SafeState
Popov, P.T., Stochastic Modeling of Safety and Security of the e-Motor, an ASIL-D Device., (SAFECOMP 2015).
AQUAS


Tool support for co-engineering
AQUAS methodology recognises the need for tight integration of:
Tools assisting with the development of application functionality (i.e. systems/software architecture, detailed design, implementation and maintenance)
UML, AADL, SysML, Simulink, are popular modelling languages.
Tools supporting analysis/assessment throughout the PLC lifecycle, (requirements validation, design space exploration for optimal/acceptable solutions (i.e. a good trade-offs between conflicting safety/security goals), etc.
Models
Qualitative (FTA, FME(C)A, attack trees, HAZOP, RBD, etc.)
Quantitative (e.g. probabilistic)
state-based models,
Bayesian methods, etc.
Empirical methods (e.g. measurements, fault-injection, etc.)
Often used to help with the parameterisation of probabilistic models.
Even Formal methods based on logic/proofs, etc.
AQUAS


Tool chains
We may use tool chains, e.g. use different tools and export/import results, to assist with:
system (software) development
analyses needed at different stages of development (reliability/availability, security, performance, etc.).
Integrated tools, too, emerge, which combine the functionality needed for both, system's development and analysis techniques.
(Automatic) model transformation between functional (e.g. UML) models and models suitable for analysis (e.g. state-based) are available in some tools:
E.g. CHESS tool offers plug-ins for generating stochastic models suitable for dependability analysis from the UML models (component diagrams).
In AQUAS we are working to extend the "dependability model" defined in CHESS. The extension will allow for dependencies discussed so far.
AQUAS


Extending CHESS for SSP analysis
Attack, Att
- Target (C1, C2,...)
- intensity, λAtt
- Prob(success), PSatt
States: {clean, compromised}
Parameters:
- Rate of failure, λC|state
- Response Delay, TC|state
«statefulSoftware»
+ A: Component A [1]
«statefulSoftware»
+ B: Component B [1]
Component A
Component B
«propagation»
{prob=PP,propDelay=PD}
AQUAS


Conclusions
A true combined SSP analysis is the essence of credible Co-engineering
Work on AQUAS UCs takes a number of different forms
Qualitative analysis – SAG, RGB (what else?)
Quantitative analysis – ATM, SAG, RGB
Interaction with WP4 to deliver tool support for:
Quantitative combined analysis (dependability model in CHESS is being extended to include a “dependency model”)
Tool support for IP throughout the PLC is also recognized as important.
A number of serious challenges:
Qualitative methods of combined analysis rely heavily on expert judgement
Quantitative methods – parameterizing the models is a serious challenge, models of dependence are also very serious.
AQUAS
15


AQUAS
THANK YOU
ECSEL JU

2.2.5 Tooling


Aggregated Quality Assurance for Systems
Design Tooling
21st January 2019
Ken Sharman, Pacôme Magnin
Instituto Tecnológico de Informática – ITI, Siemens PLM
AQUAS

Tooling in AQUAS

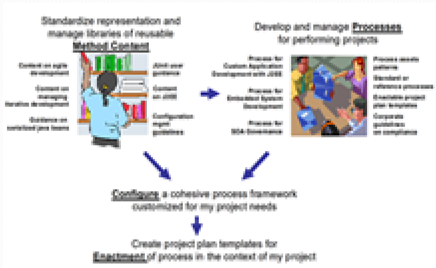
- Develop a set of tools supporting
  - Co-engineering and PLC for safety, security and performance
  - The methodology of co-engineering using interaction points
  - Use cases demonstrations

AQUAS SAFETY SECURITY PERFORMANCE

2

Co-engineering process support

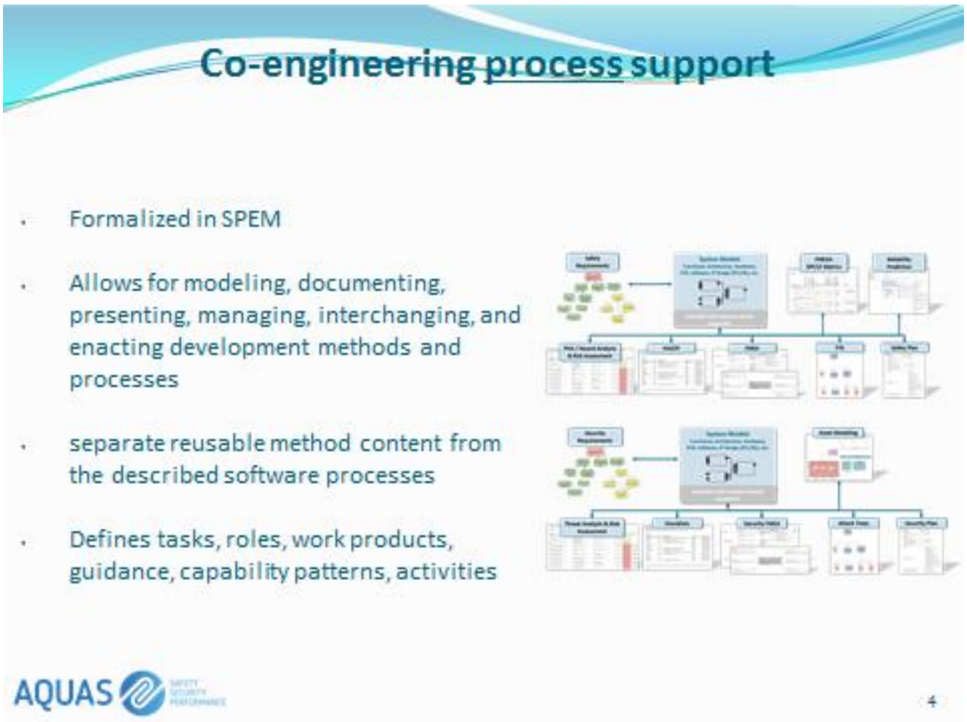
- Define how the co-engineering process could be supported by the tooling
- meta model for interaction point support & tracking
- Use-Case-specific foreseen tools case interaction points

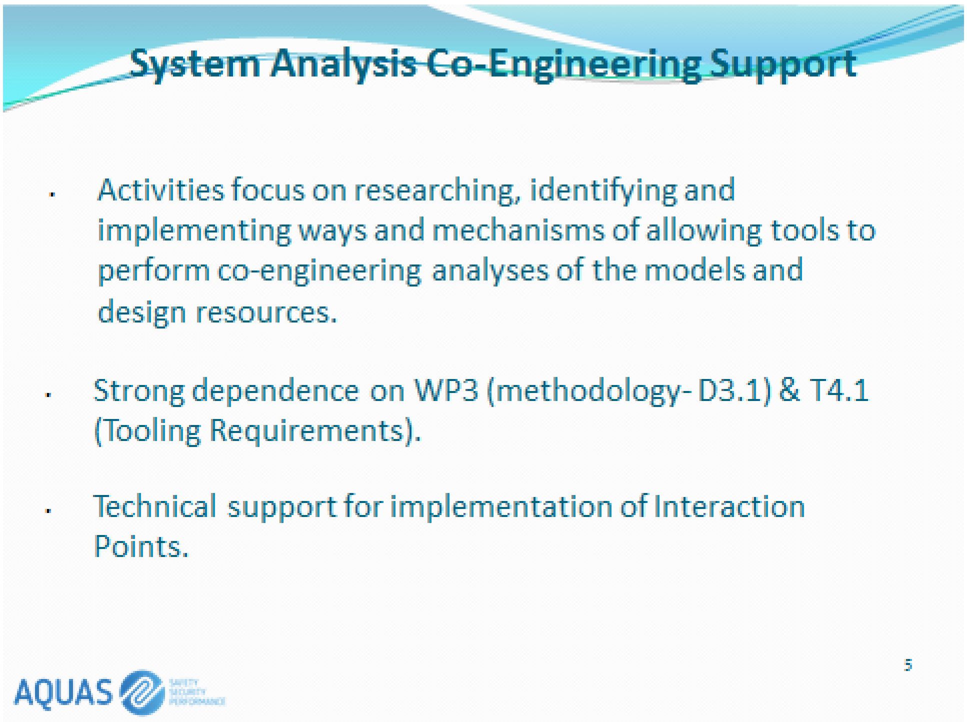


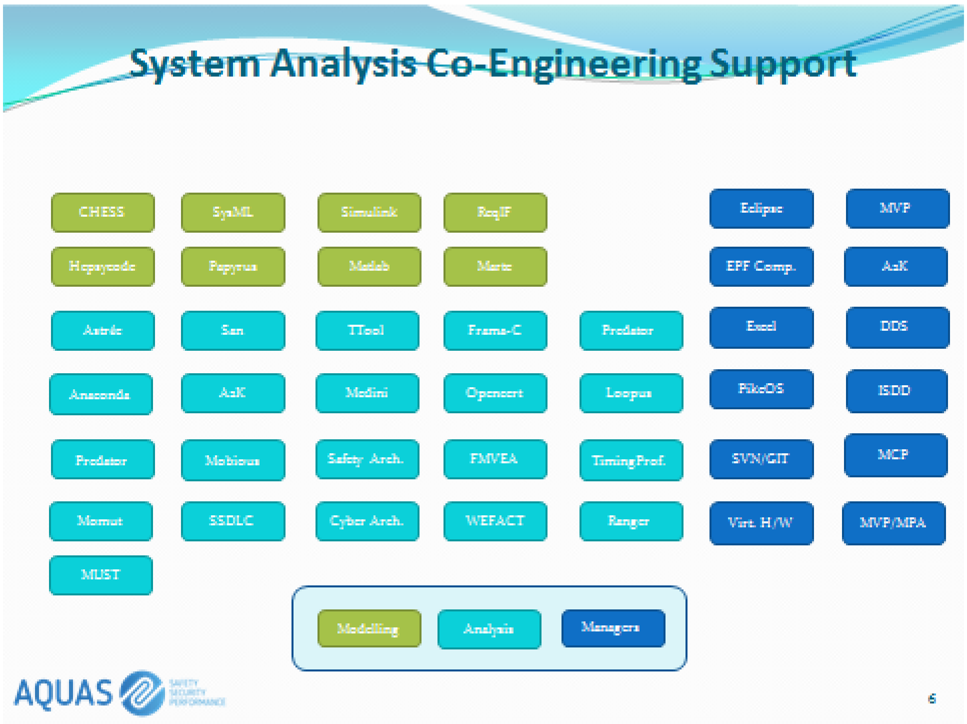
- Generic tooling approach foreseen by tools providers

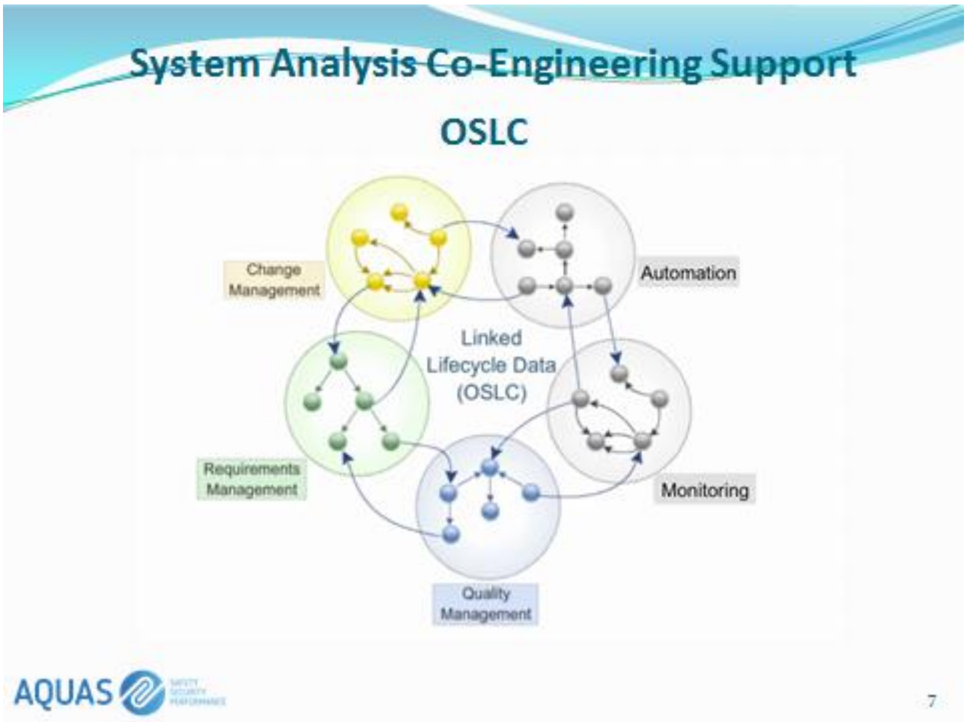
AQUAS SAFETY SECURITY PERFORMANCE

3

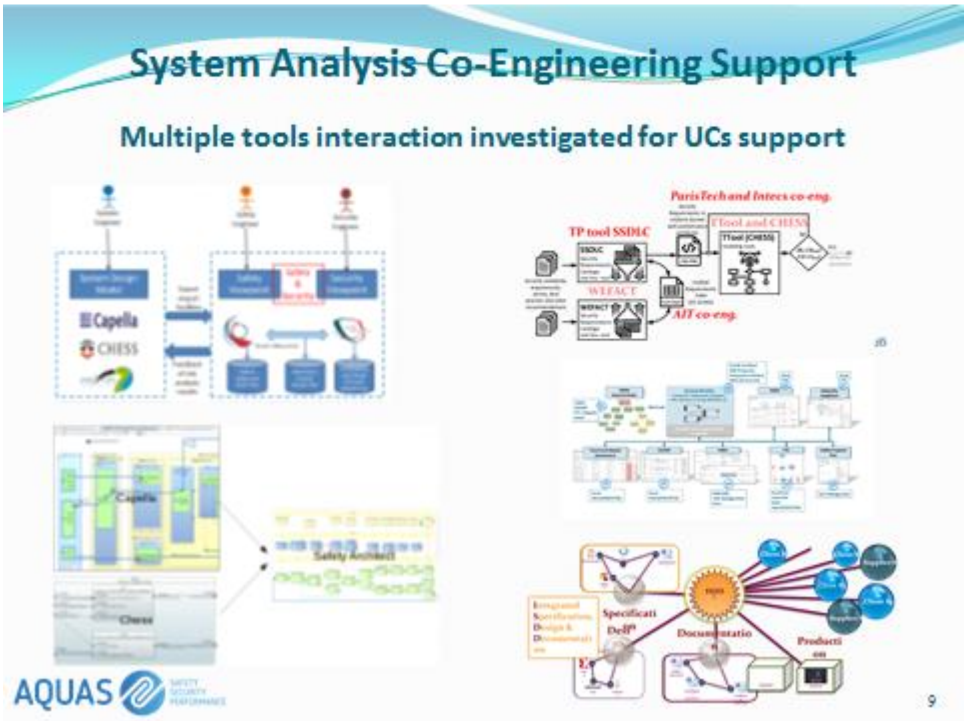

Co-engineering process support
Formalized in SPEM
Allows for modeling, documenting, presenting, managing, interchanging, and enacting development methods and processes
separate reusable method content from the described software processes
Defines tasks, roles, work products, guidance, capability patterns, activities
AQUAS
4

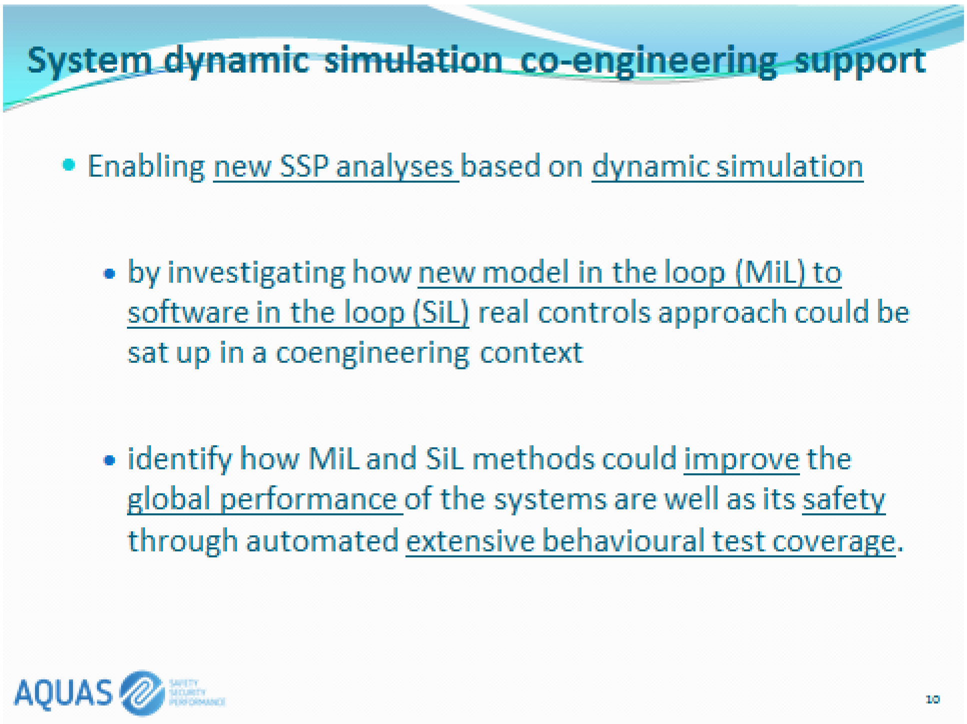

System Analysis Co-Engineering Support
Activities focus on researching, identifying and implementing ways and mechanisms of allowing tools to perform co-engineering analyses of the models and design resources.
Strong dependence on WP3 (methodology- D3.1) & T4.1 (Tooling Requirements).
Technical support for implementation of Interaction Points.
AQUAS
5

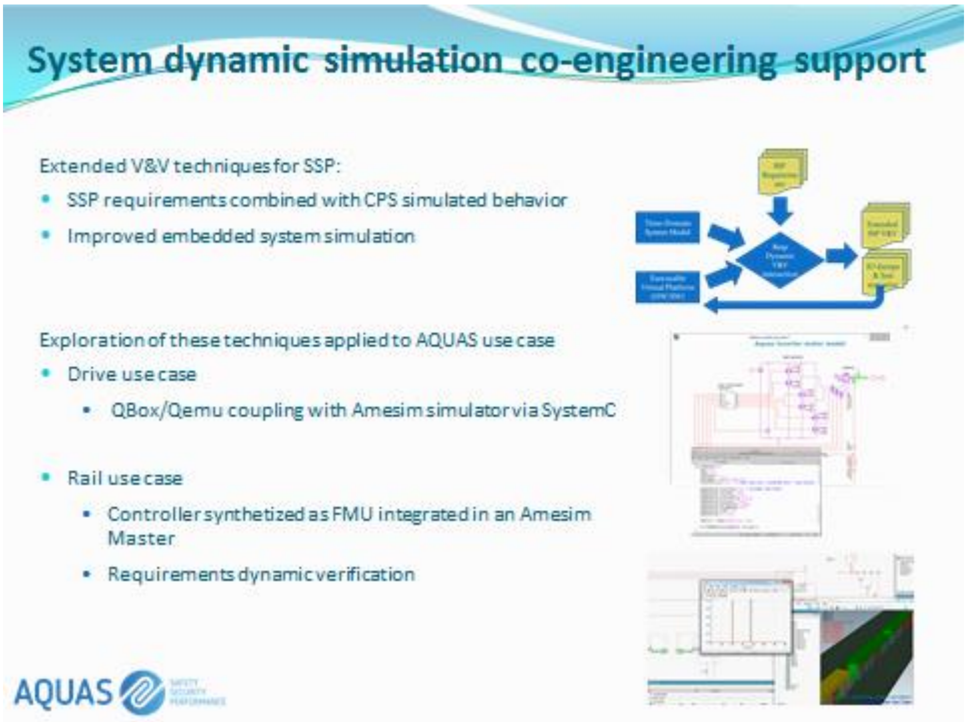

System Analysis Co-Engineering Support
CHESS
SysML
Simulink
ReqIF
Hepsycode
Papyrus
Matlab
Marte
Astrée
San
TTool
Frama-C
Predator
Anaconda
AsK
Medini
Opencert
Loopus
Predator
Mobious
Safety Arch.
FMVEA
TimingProf.
Momut
SSDLC
Cyber Arch.
WEFACT
Ranger
MUST
Eclipse
MVP
EPF Comp.
AsK
Excel
DDS
PikeOS
ISDD
SVN/GIT
MCP
Virt. H/W
MVP/MPA
Modelling
Analysis
Managers
AQUAS
6

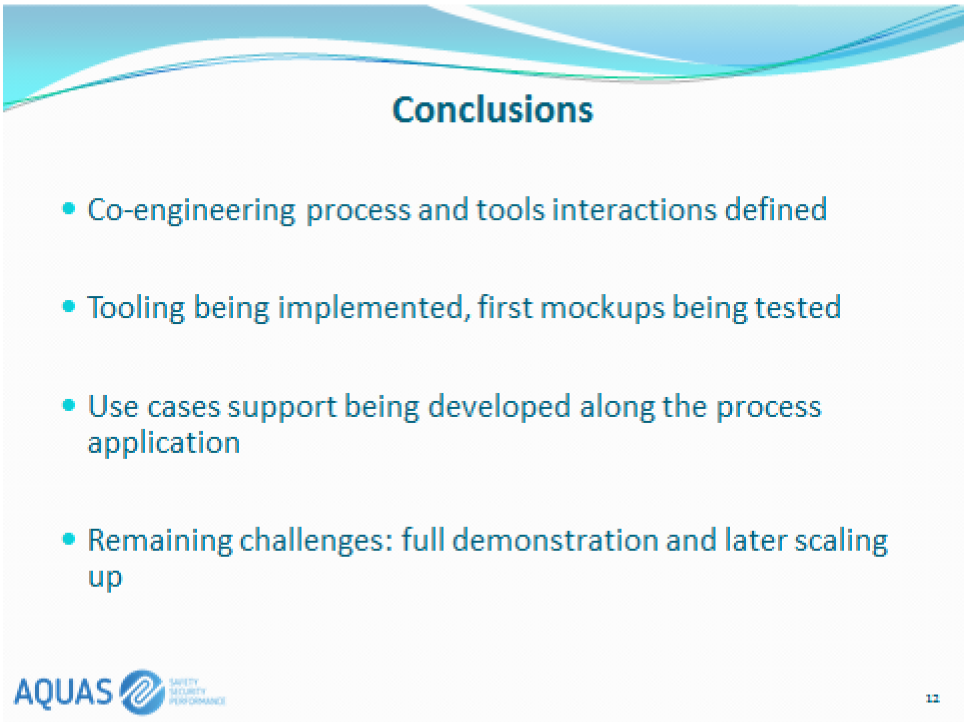

System Analysis Co-Engineering Support
OSLC
Change Management
Automation
Linked Lifecycle Data (OSLC)
Requirements Management
Monitoring
Quality Management
AQUAS
7


OSLC
Discovery: discover what services a server provides on what domains and how to access those services through REST APIs.
Resource Preview: provide icon, label, small and/or large preview dialogs for visualizing information from another tools.
Delegated Dialogs: provide dialogs for creating new resources, or selecting existing resources from other tools.
Attachments: Attach documents to resources, typically used to attach binary or non-RDF files to RDF resources.
Query: query OSLC resources with a simple, implementation independent query language
Common Vocabulary: specify recommended vocabulary and constraints common across OSLC domains.
Domain Specifications: domain vocabularies and constraints for various areas of interest including Requirements Management, Change Management, Configuration Management, Architecture Management, Quality Management, etc.
AQUAS
8


System Analysis Co-Engineering Support
Multiple tools interaction investigated for UCs support
Capella
CHESS
ParisTech and Intecs co-eng.
TP tool SSDLC
AIT co-eng.
AQUAS
9

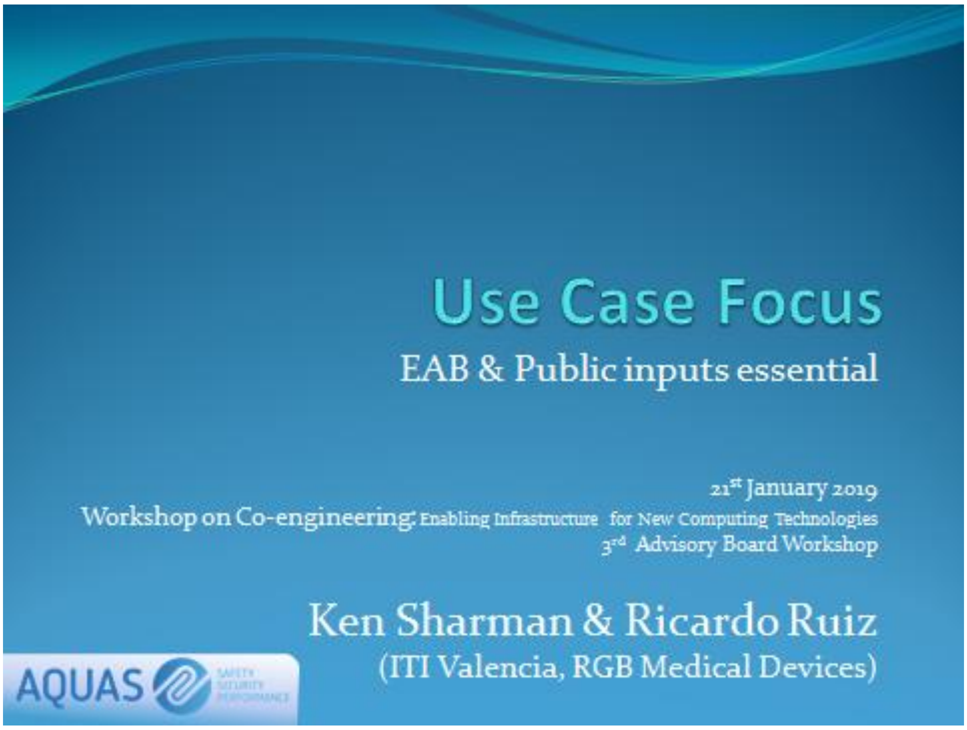

System dynamic simulation co-engineering support
Enabling new SSP analyses based on dynamic simulation
by investigating how new model in the loop (MiL) to software in the loop (SiL) real controls approach could be sat up in a coengineering context
identify how MiL and SiL methods could improve the global performance of the systems are well as its safety through automated extensive behavioural test coverage.
AQUAS
10

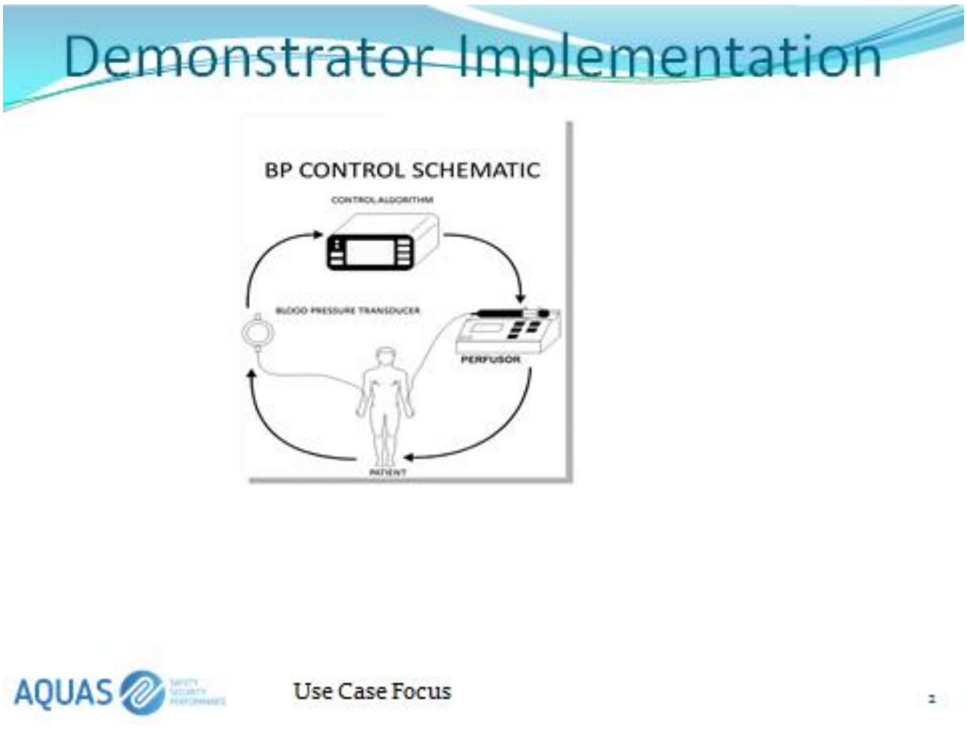

System dynamic simulation co-engineering support
Extended V&V techniques for SSP:
SSP requirements combined with CPS simulated behavior
Improved embedded system simulation
Exploration of these techniques applied to AQUAS use case
Drive use case
QBox/Qemu coupling with Amesim simulator via SystemC
Rail use case
Controller synthetized as FMU integrated in an Amesim Master
Requirements dynamic verification
AQUAS


Conclusions
Co-engineering process and tools interactions defined
Tooling being implemented, first mockups being tested
Use cases support being developed along the process application
Remaining challenges: full demonstration and later scaling up
AQUAS
12


AQUAS
THANK YOU
ECSEL JU

2.2.6 Use Case Focus – UC2





Demonstrator Implementation

This document includes basic instructions for the use of the different devices of the AQUAS demonstrator, according to the current status of development:

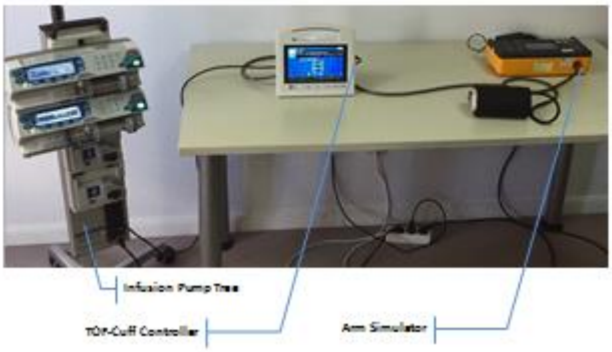
- TOF-Cuff Controller.
- Arm Simulator. It is the PROSIM 8 Vital Signs Simulator used to simulate real NIBP measurements.
- Infusion Pump Tree. It is composed of two infusion pumps (AITECS 2016 model) and the dock station (AITECS IDS-04) with Ethernet connection for remote control.

AQUAS Use Case Focus 3

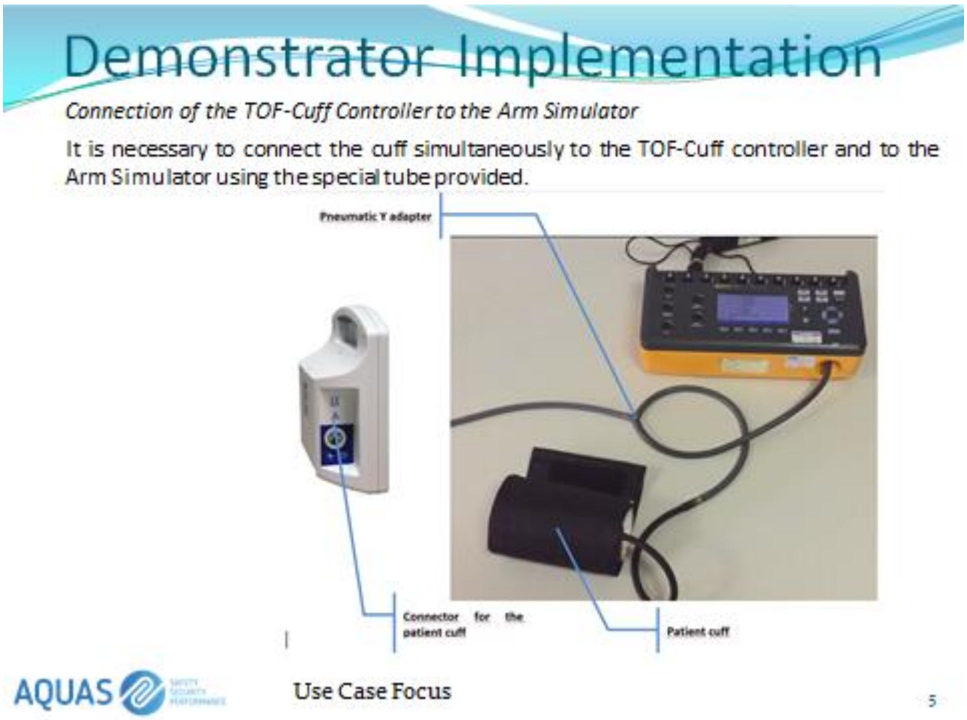
Demonstrator Implementation

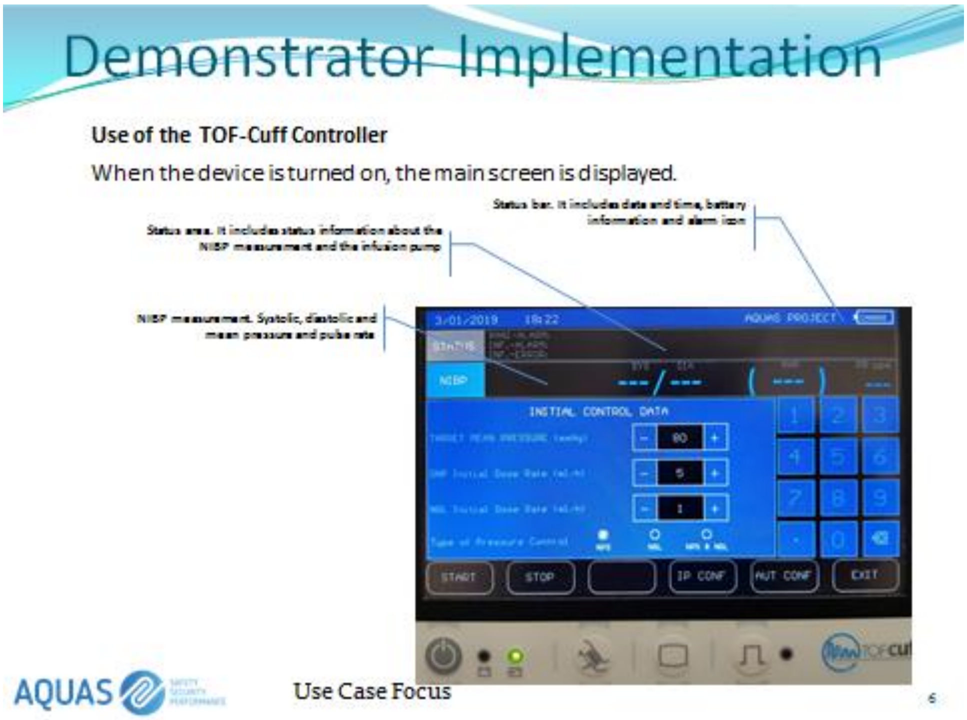
Connection of the TOF-Cuff Controller to the Infusion Pump Tree

It is necessary to connect an Ethernet cable between both devices.



AQUAS Use Case Focus 4


Demonstrator Implementation
Connection of the TOF-Cuff Controller to the Arm Simulator
It is necessary to connect the cuff simultaneously to the TOF-Cuff controller and to the Arm Simulator using the special tube provided.
Pneumatic Y adapter
Connector for the patient cuff
Patient cuff
AQUAS
Use Case Focus
5


Demonstrator Implementation
Use of the TOF-Cuff Controller
When the device is turned on, the main screen is displayed.
Status bar. It includes date and time, battery information and alarm icon
Status area. It includes status information about the NIBP measurement and the infusion pump
NIBP measurement. Systolic, diastolic and mean pressure and pulse rate
INITIAL CONTROL DATA
START
STOP
IP CONF
AUT CONF
EXIT
AQUAS
Use Case Focus
6

Demonstrator Implementation

Use of the TOF-Cuff Controller

When the device is turned on, the main screen is displayed.

Main menu

Input of initial data for the pressure control. Four data can be selected:
- Target mean pressure for the control. Patient's pressure to be maintained during the control session.
- SNP initial dose rate. SNP dose rate to start the control
- NGL initial dose rate. NGL dose rate to start the control
- Type of control. There are three options:

AQUAS Use Case Focus 7

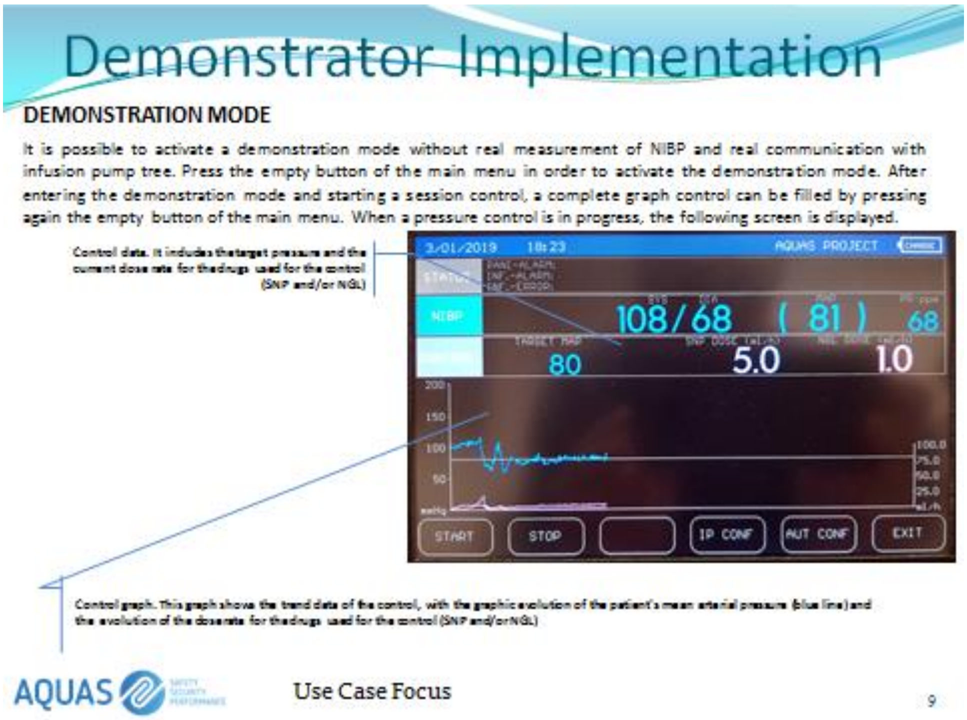
Demonstrator Implementation

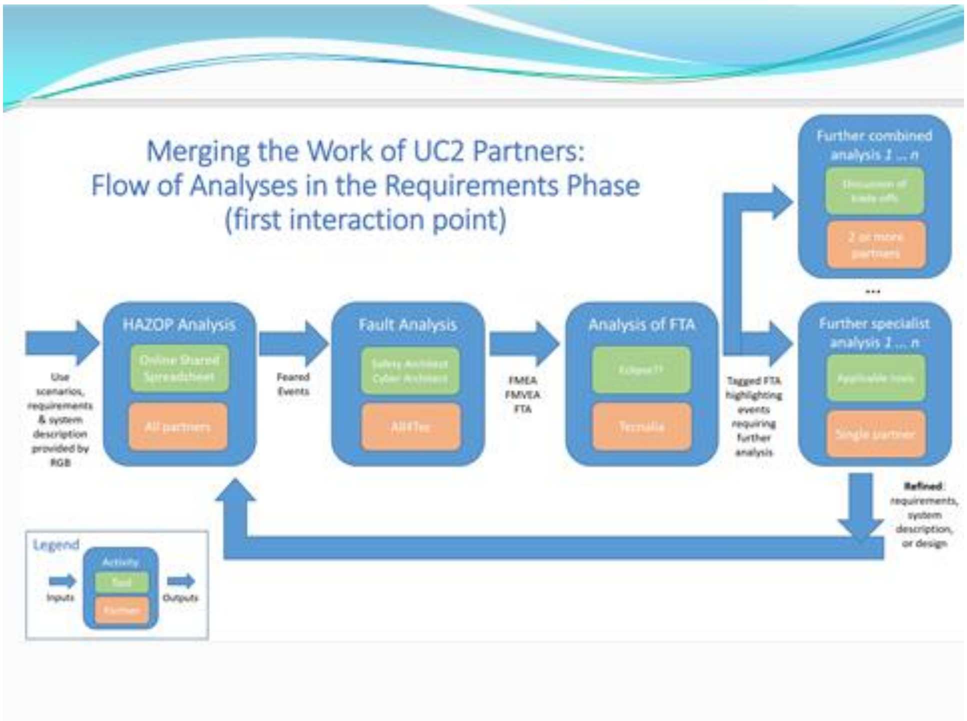
Connection of the TOF-Cuff Controller to the Arm Simulator

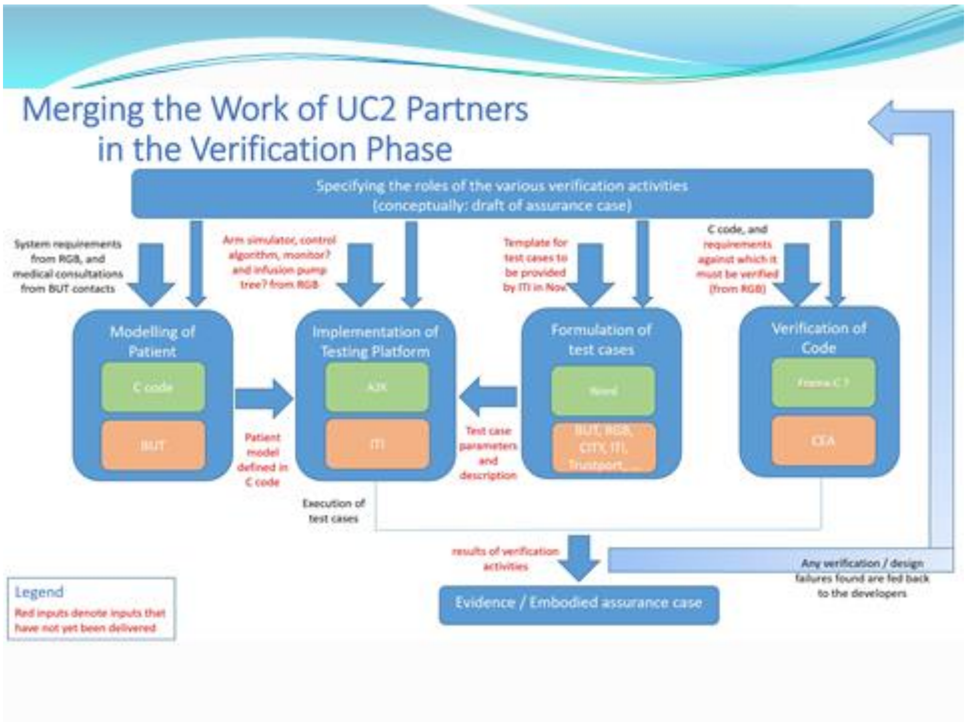
It is necessary to connect the cuff simultaneously to the TOF-Cuff controller and to the Arm Simulator using the special tube provided.

When the upper status bar is touched, a configuration screen is entered as shown in the following picture.

AQUAS Use Case Focus 8


Demonstrator Implementation
DEMONSTRATION MODE
It is possible to activate a demonstration mode without real measurement of NIBP and real communication with infusion pump tree. Press the empty button of the main menu in order to activate the demonstration mode. After entering the demonstration mode and starting a session control, a complete graph control can be filled by pressing again the empty button of the main menu. When a pressure control is in progress, the following screen is displayed.
Control data. It includes the target pressure and the current dose rate for the drugs used for the control (SNP and/or NGL)
3/01/2019 18:23
AQUAS PROJECT
NIBP
108/68
(81)
68
TARGET MAP
80
5.0
1.0
START
STOP
IP CONF
AUT CONF
EXIT
Control graph. This graph shows the trend data of the control, with the graphic evolution of the patient's mean arterial pressure (blue line) and the evolution of the dose rate for the drugs used for the control (SNP and/or NGL)
AQUAS
Use Case Focus
9


Merging the Work of UC2 Partners:
Flow of Analyses in the Requirements Phase
(first interaction point)
Use scenarios, requirements & system description provided by RGB
HAZOP Analysis
Online Shared Spreadsheet
All partners
Feared Events
Fault Analysis
Safety Architect
Cyber Architect
All4Tec
FMEA
FMVEA
FTA
Analysis of FTA
Tecnalia
Tagged FTA highlighting events requiring further analysis
Further combined analysis 1 ... n
2 or more partners
Further specialist analysis 1 ... n
Applicable tools
Single partner
Refined: requirements, system description, or design
Legend
Activity
Tool
Partner
Inputs
Outputs



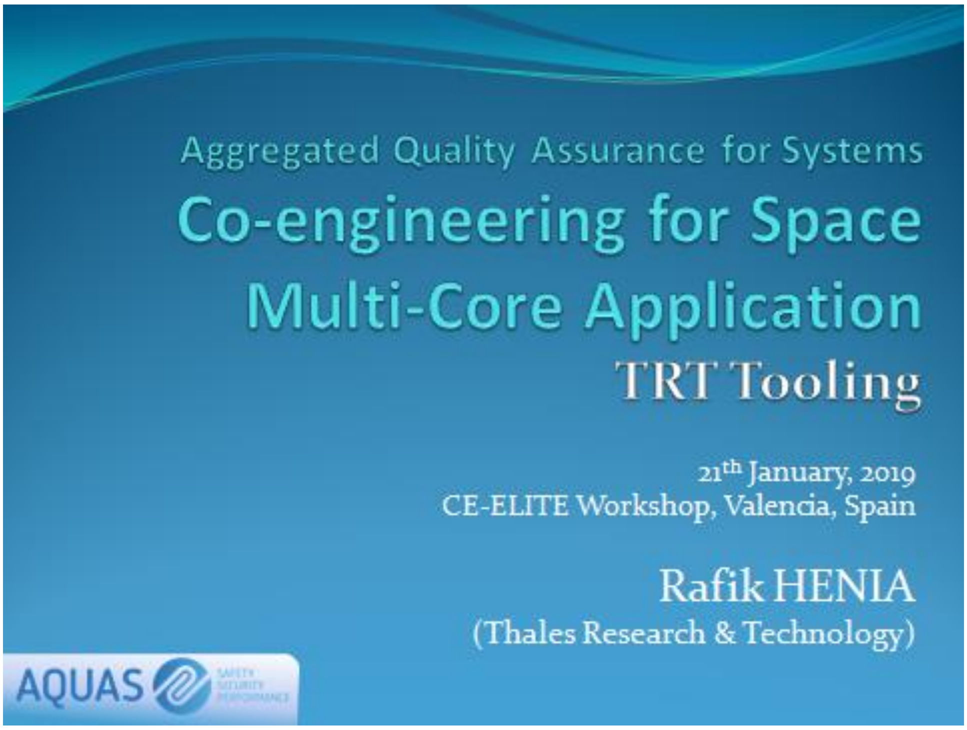
Comments Regarding the Verification Phase

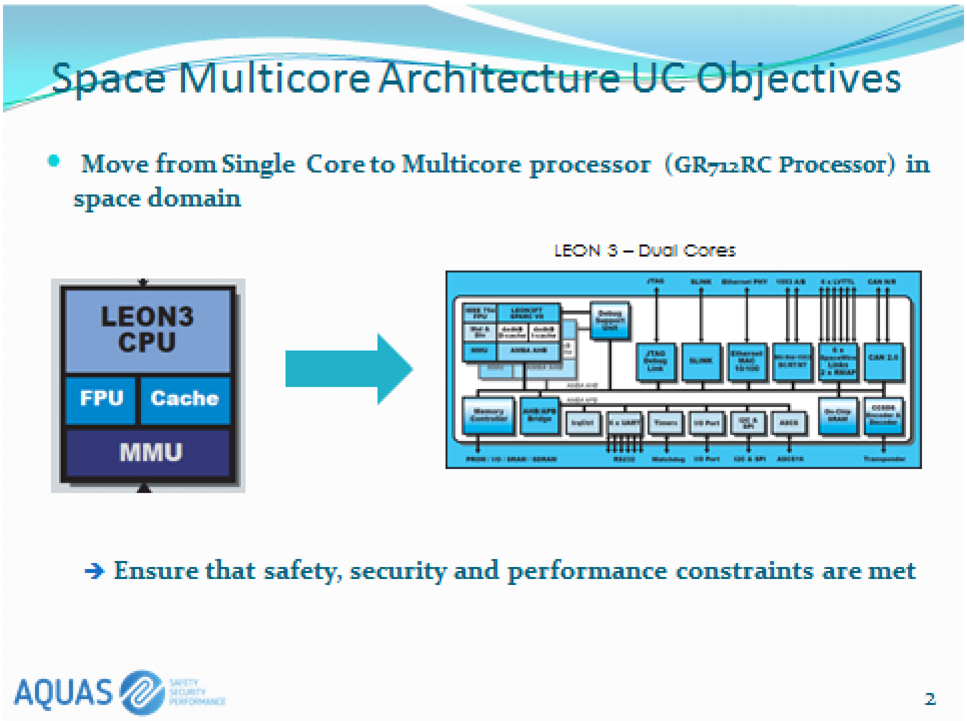
- Different partners plan to contribute test cases addressing different viewpoints. For example:
  - Trustport: security-related test cases
  - City: usability tests especially with regards to exception cases
  - ITI: robustness of the algorithm
  - BUT: robustness of algorithm for various patient physiological parameters
- Challenge: Current plan for testing platform does not support connection to hospital system to verify potential security-related test cases
- Starting with a unified goal (specific use scenario in the requirements phase; specific aspect of the assurance case in the verification phase) means the effort by all partners helps achieve a unified goal and that within the short timeframe of the AQUAS project, results can reveal how the methodology/lessons learned can be applied to a meaningful subset of the system

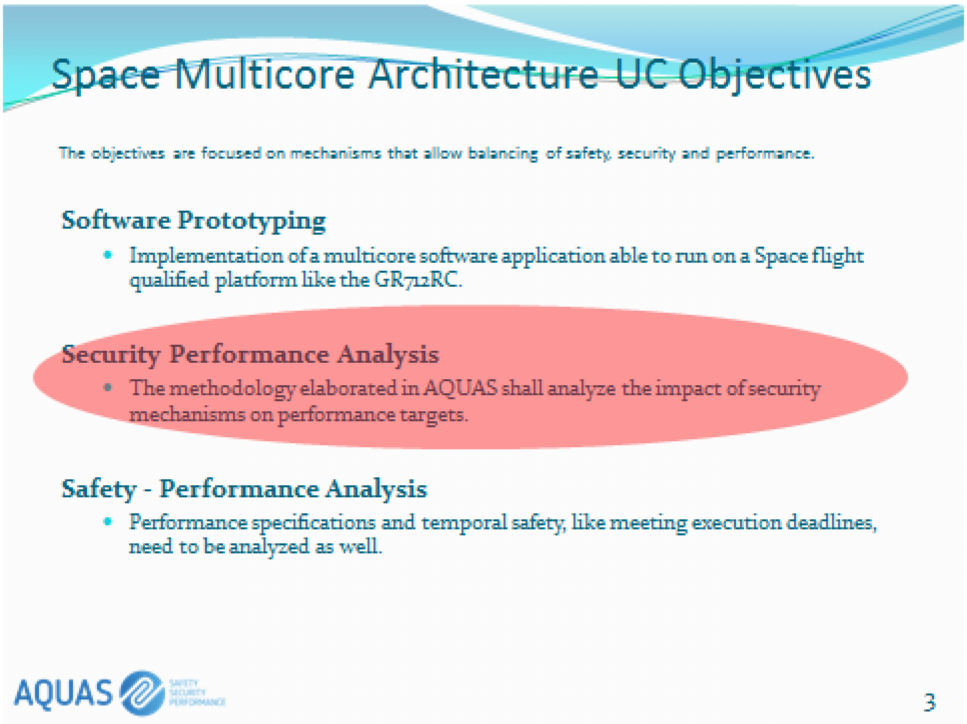

Comments Regarding the Verification Phase
RGB, Trustport and City have started analysing the security-safety-performance trade-offs that are introduced by the possible requirement for users to authenticate themselves in order to enter safety-critical adjustments.
Ability to make some adjustments quickly is crucial for patient safety;
medical staff time needs to be used most efficiently.
The activity has reached the stage of
1. Enumerating possible authentication mechanisms and
2. Agreeing criteria for identifying those potentially suitable, to be subjected to a thorough trade-off analysis to reach design decisions.
AQUAS

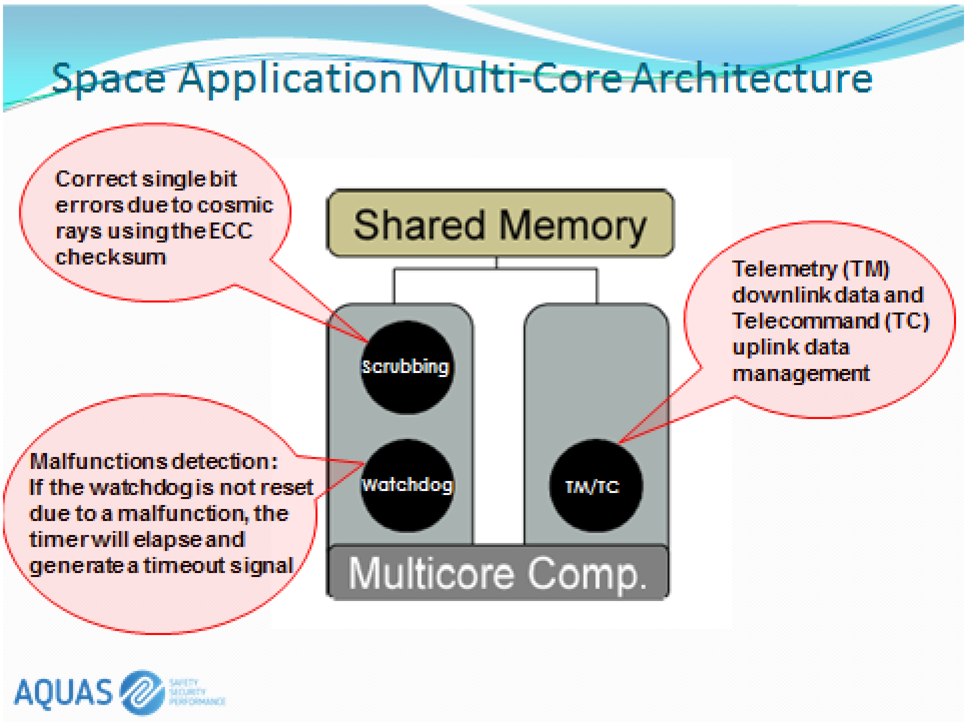

Thank you!
Comments & question?
AQUAS
14

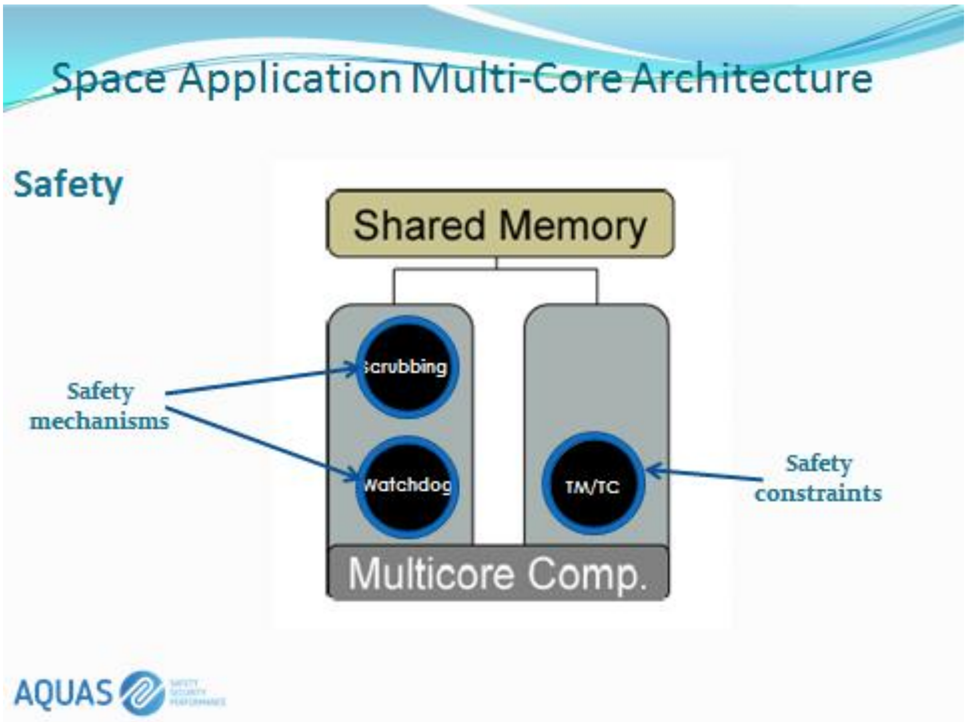
2.2.7 Use Case Focus – UC5

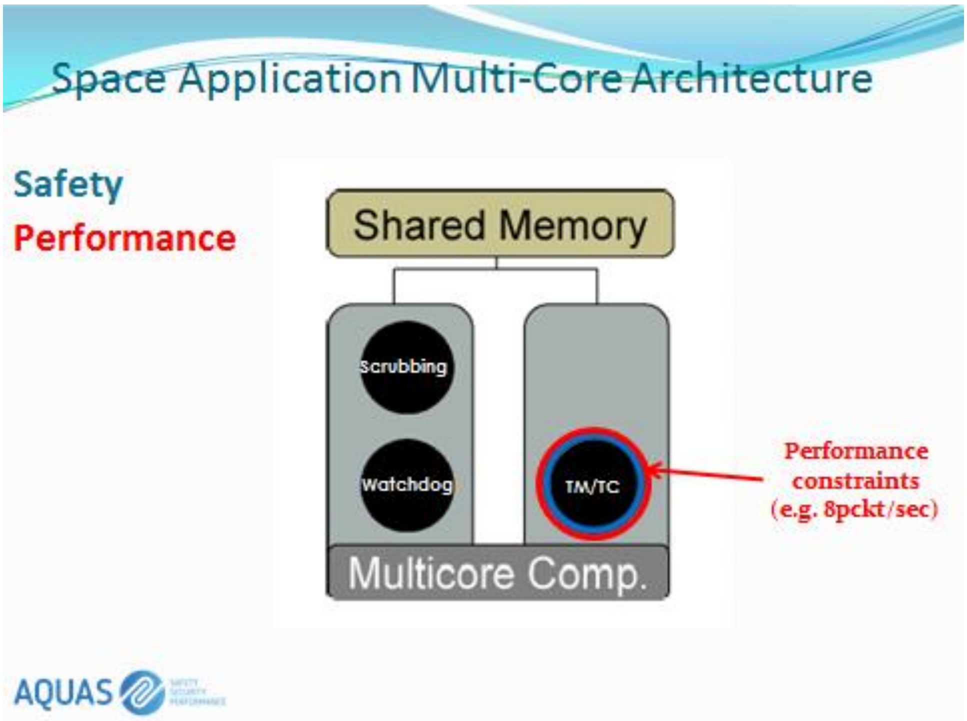


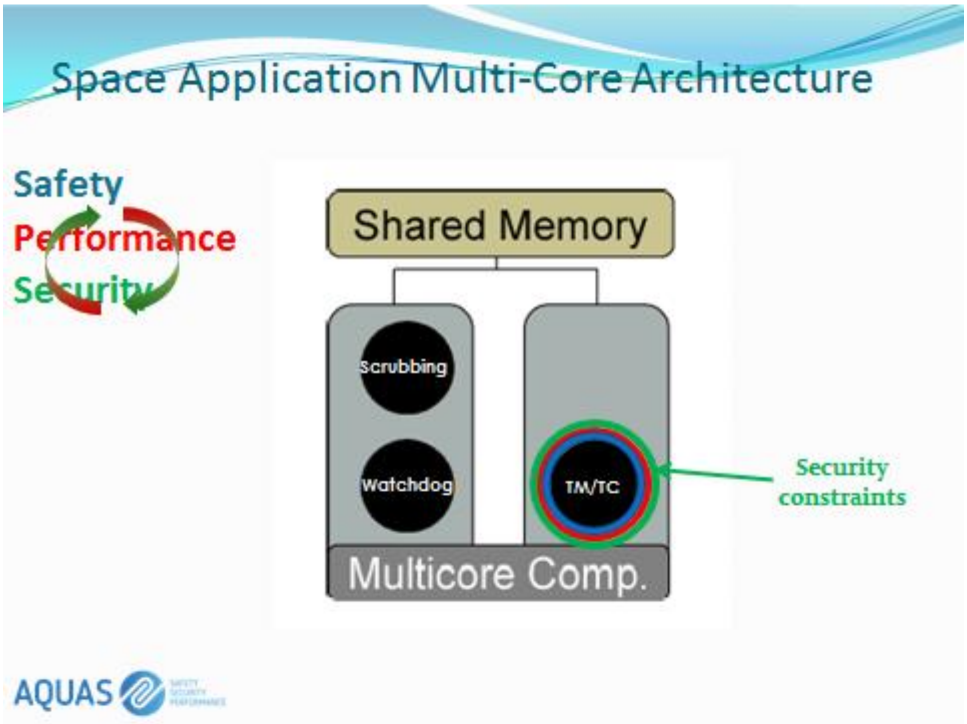


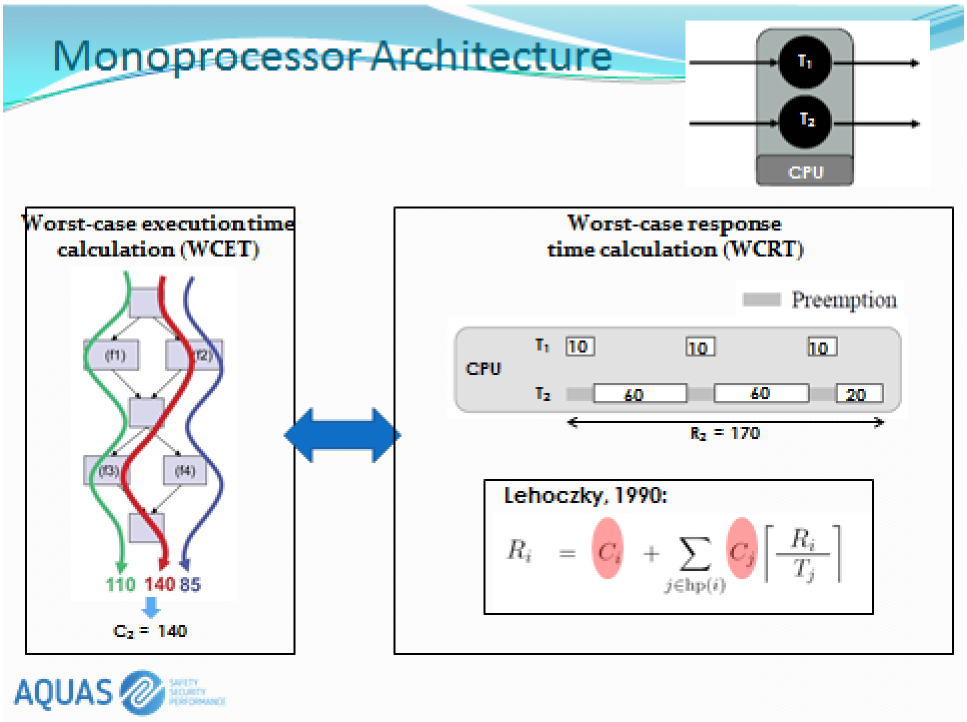

Space Multicore Architecture UC Objectives
The objectives are focused on mechanisms that allow balancing of safety, security and performance.
Software Prototyping
Implementation of a multicore software application able to run on a Space flight qualified platform like the GR712RC.
Security Performance Analysis
The methodology elaborated in AQUAS shall analyze the impact of security mechanisms on performance targets.
Safety - Performance Analysis
Performance specifications and temporal safety, like meeting execution deadlines, need to be analyzed as well.
AQUAS
3

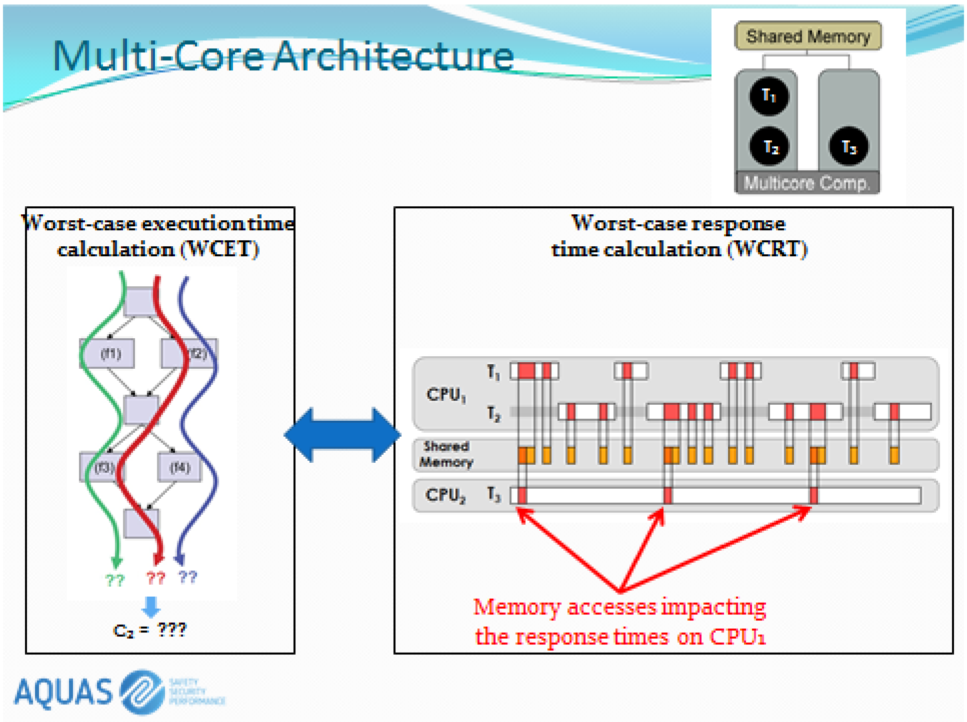

Space Application Multi-Core Architecture
Correct single bit errors due to cosmic rays using the ECC checksum
Shared Memory
Telemetry (TM) downlink data and Telecommand (TC) uplink data management
Scrubbing
Malfunctions detection: If the watchdog is not reset due to a malfunction, the timer will elapse and generate a timeout signal
Watchdog
TM/TC
Multicore Comp.
AQUAS

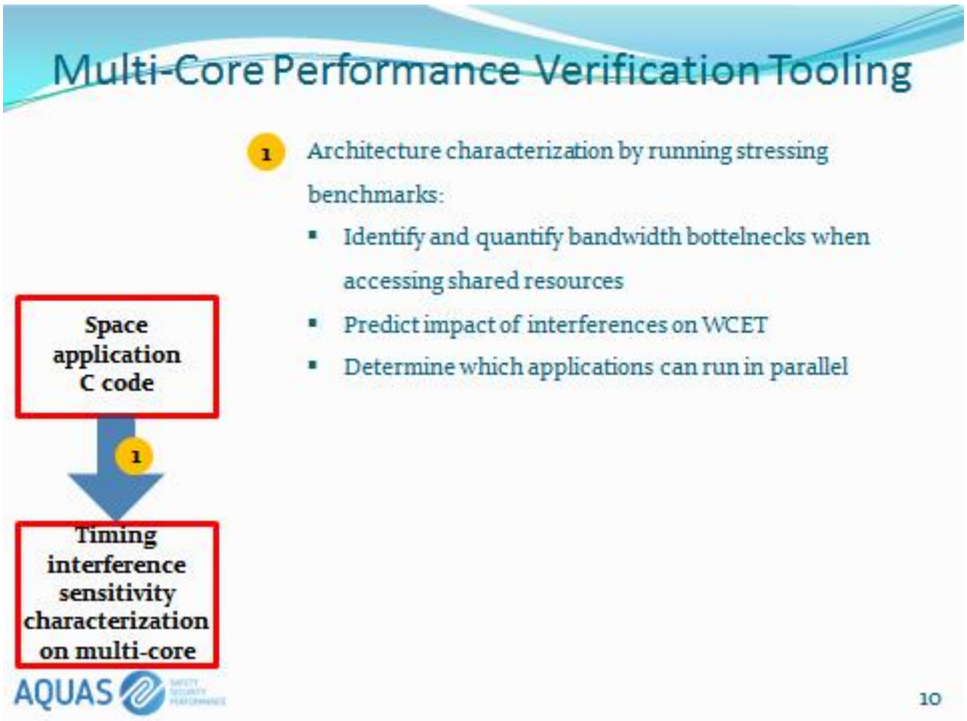

Space Application Multi-Core Architecture
Safety
Shared Memory
Safety mechanisms
Scrubbing
Watchdog
TM/TC
Safety constraints
Multicore Comp.
AQUAS

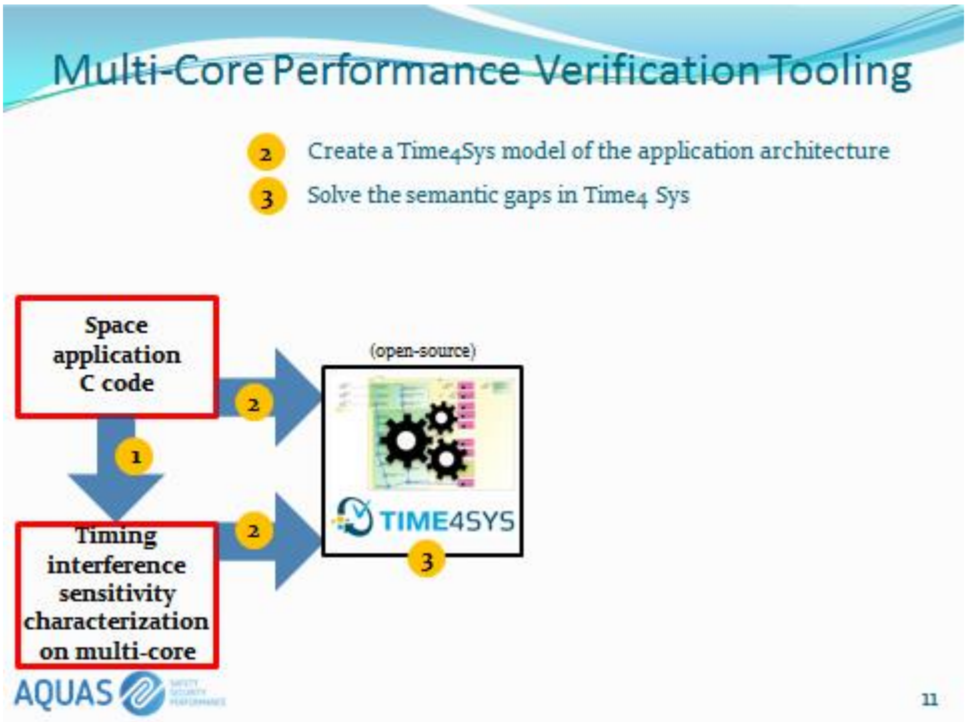

Space Application Multi-Core Architecture
Safety
Performance
Shared Memory
Scrubbing
Watchdog
TM/TC
Performance constraints (e.g. 8pckt/sec)
Multicore Comp.
AQUAS

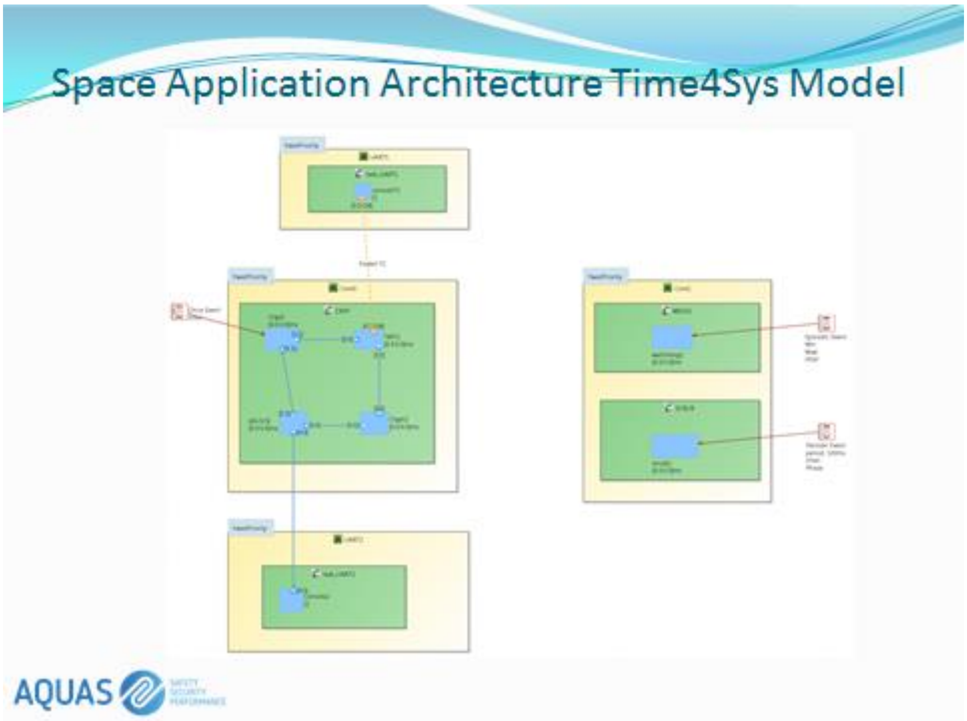

Space Application Multi-Core Architecture
Safety
Performance
Security
Shared Memory
Scrubbing
Watchdog
TM/TC
Multicore Comp.
Security constraints
AQUAS

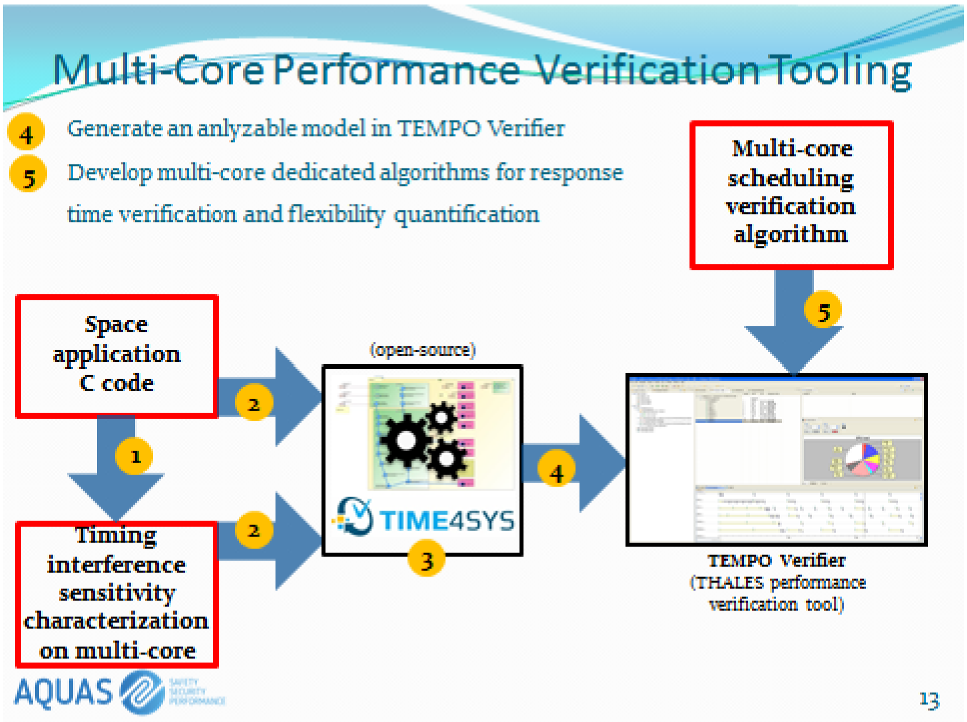

Monoprocessor Architecture
CPU
Worst-case execution time calculation (WCET)
110 140 85
Worst-case response time calculation (WCRT)
Preemption
CPU
10
10
10
60
60
20
Lehoczky, 1990:
AQUAS


Multi-Core Architecture
Shared Memory
T1
T2
T3
Multicore Comp.
Worst-case execution time calculation (WCET)
(f1)
(f2)
(f3)
(f4)
?? ?? ??
C2 = ???
Worst-case response time calculation (WCRT)
CPU1
T1
T2
Shared Memory
CPU2
T3
Memory accesses impacting the response times on CPU1
AQUAS

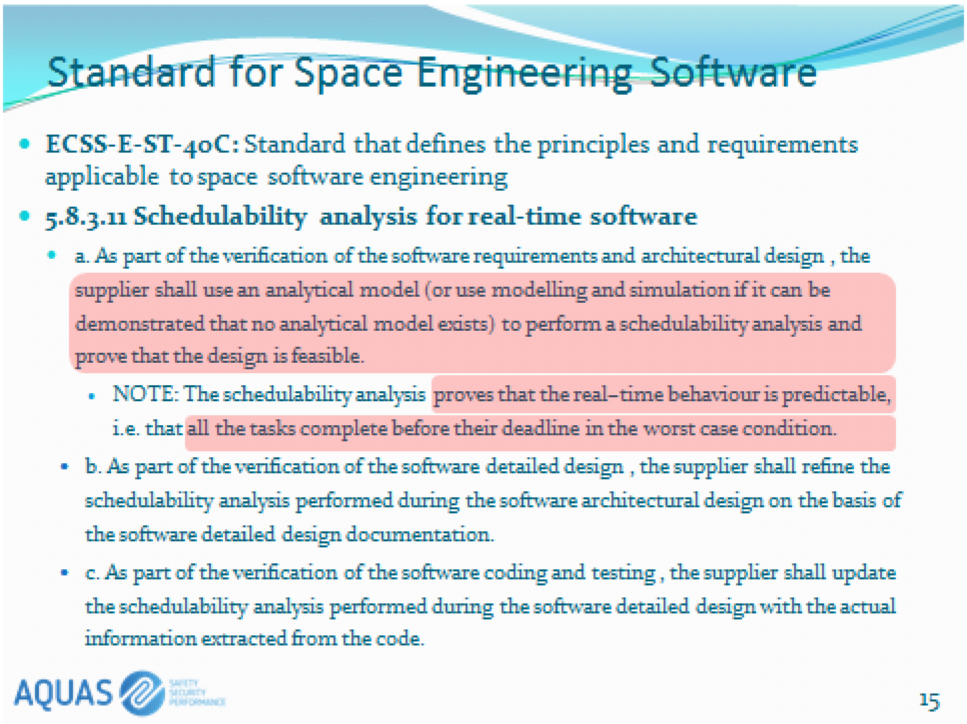

Multi-Core Performance Verification Tooling
1
Architecture characterization by running stressing benchmarks:
Identify and quantify bandwidth bottelnecks when accessing shared resources
Predict impact of interferences on WCET
Determine which applications can run in parallel
Space application C code
1
Timing interference sensitivity characterization on multi-core
AQUAS
10


Multi-Core Performance Verification Tooling
2 Create a Time4Sys model of the application architecture
3 Solve the semantic gaps in Time4 Sys
Space application C code
1
Timing interference sensitivity characterization on multi-core
2
2
(open-source)
TIME4SYS
3
AQUAS
11

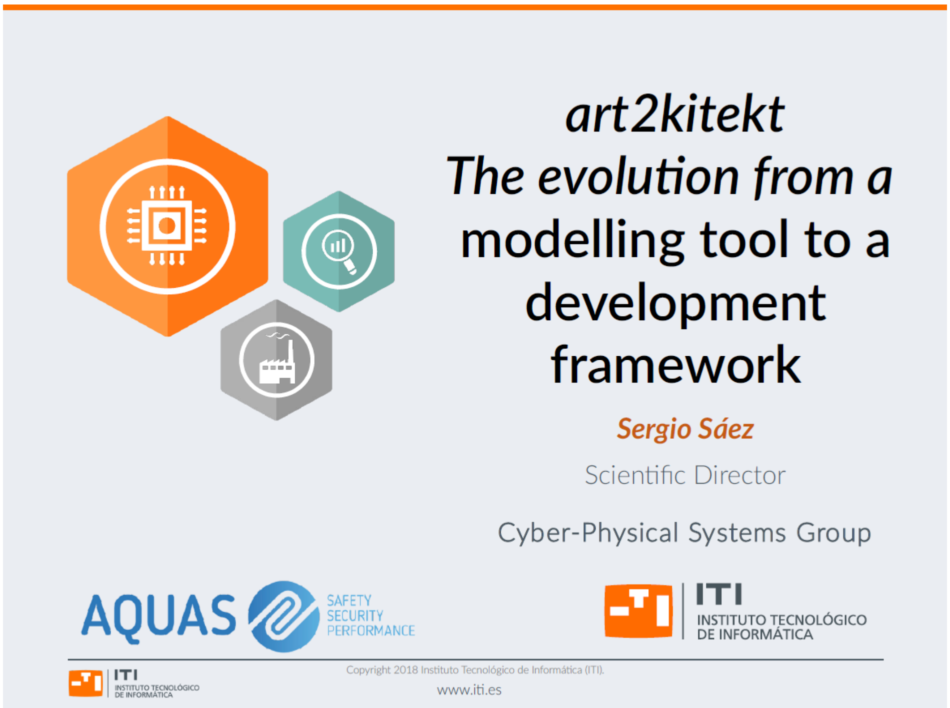

Space Application Architecture Time4Sys Model
AQUAS


Multi-Core Performance Verification Tooling
4 Generate an anlyzable model in TEMPO Verifier
5 Develop multi-core dedicated algorithms for response time verification and flexibility quantification
Multi-core scheduling verification algorithm
Space application C code
(open-source)
TIME4SYS
Timing interference sensitivity characterization on multi-core
TEMPO Verifier
(THALES performance verification tool)
AQUAS
13


AQUAS
THANK YOU
ECSEL JU



2.2.8 art2kitekt



Agenda

- **Introduction**
- Internal architecture
- Internal Data Flow
- Possible interactions / extensions

AQUAS SAFETY SECURITY PERFORMANCE

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

Introduction

- An integrated tool chain that allows the engineer to:
  - **Define** the execution platform with the application specific details, e.g. physical devices, resources, RTOS overheads, …
  - **Model** the software according to a domain-specific application model
  - **Map** the software components to execution platform resources
  - **Analyse** extra-functional requirements of the system
  - **Generate** the low-level software code/configuration from the analysis results
  - **Simulate**, **Monitor**, …

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

Agenda

- Introduction
- ***Internal architecture***
- Internal Data Flow
- Possible interactions / extensions

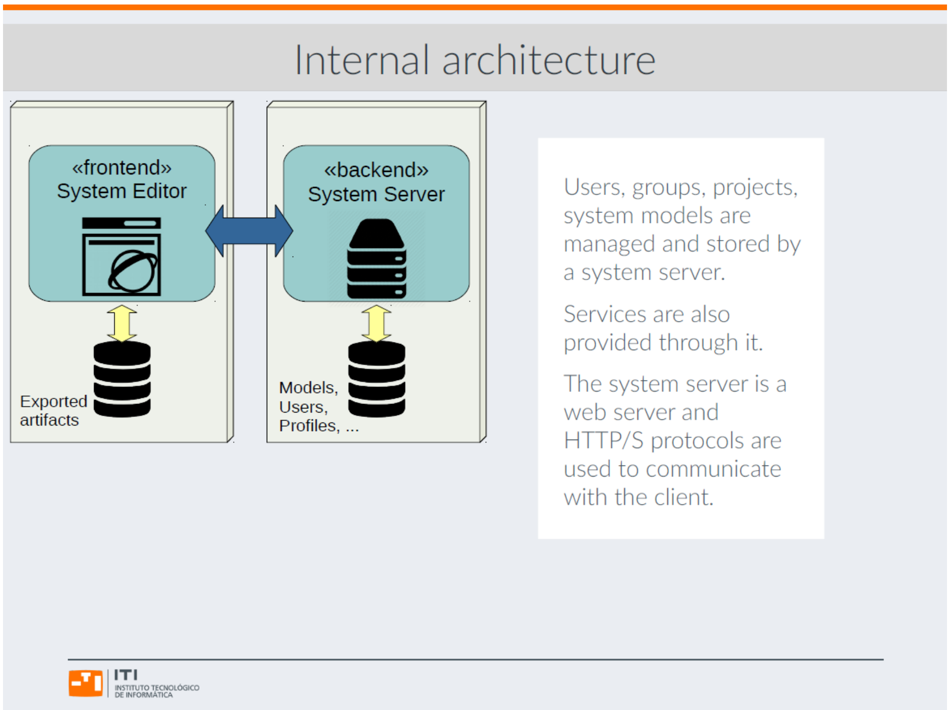
AQUAS SAFETY SECURITY PERFORMANCE

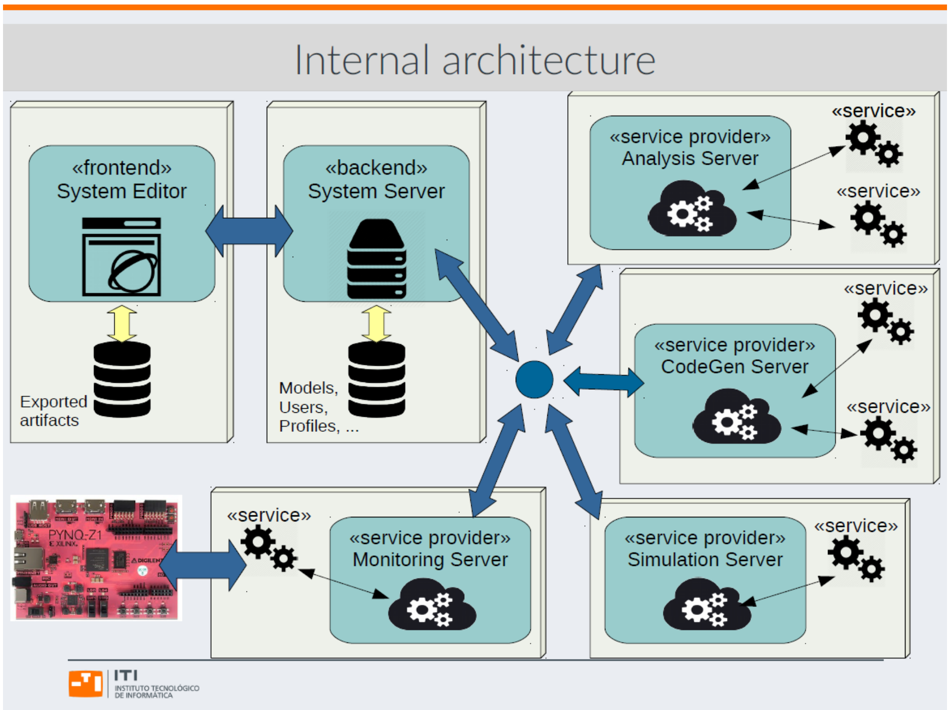
ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

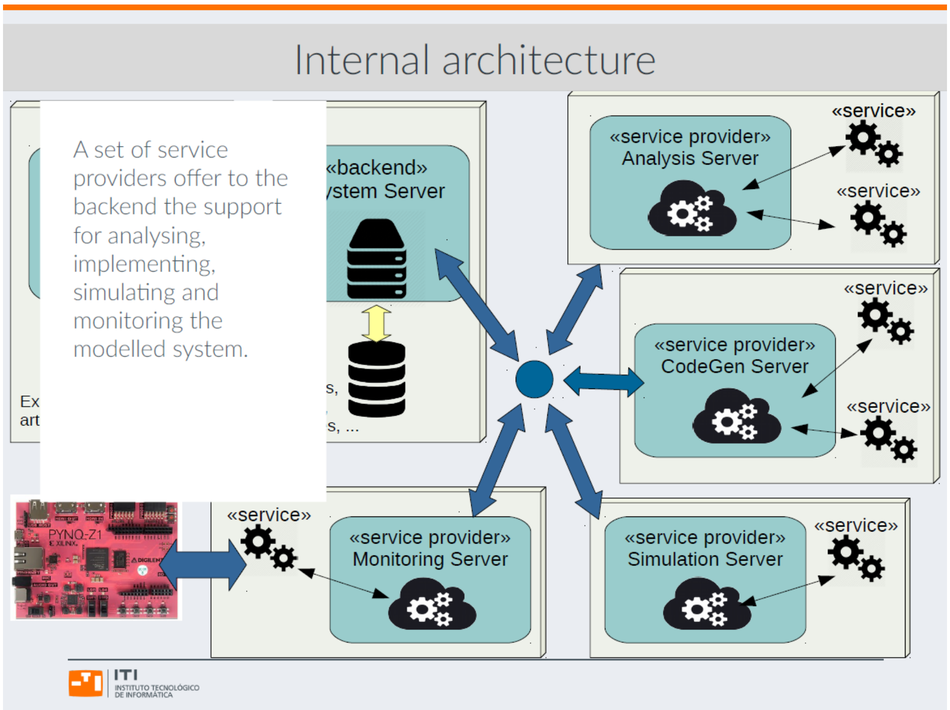
Internal architecture

System is modelled using a web browser in the engineer's computer

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA


Internal architecture
«frontend»
System Editor
«backend»
System Server
Exported artifacts
Models, Users, Profiles, ...
Users, groups, projects, system models are managed and stored by a system server.
Services are also provided through it.
The system server is a web server and HTTP/S protocols are used to communicate with the client.


Internal architecture
«frontend»
System Editor
«backend»
System Server
Exported artifacts
Models, Users, Profiles, ...
«service provider»
Analysis Server
«service»
«service»
«service provider»
CodeGen Server
«service»
«service»
«service provider»
Monitoring Server
«service»
«service provider»
Simulation Server
«service»

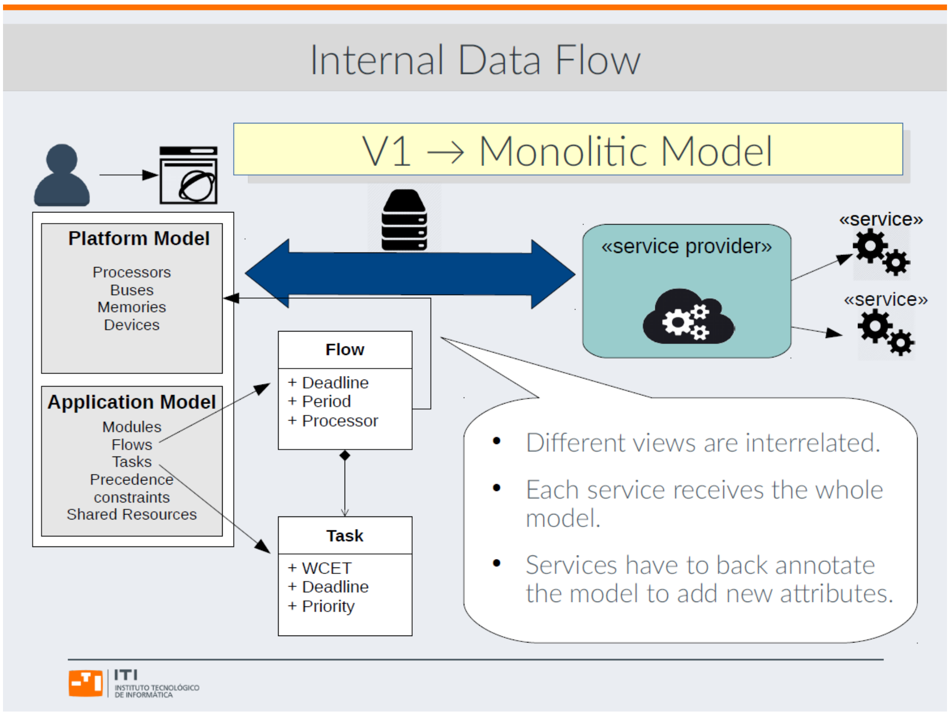


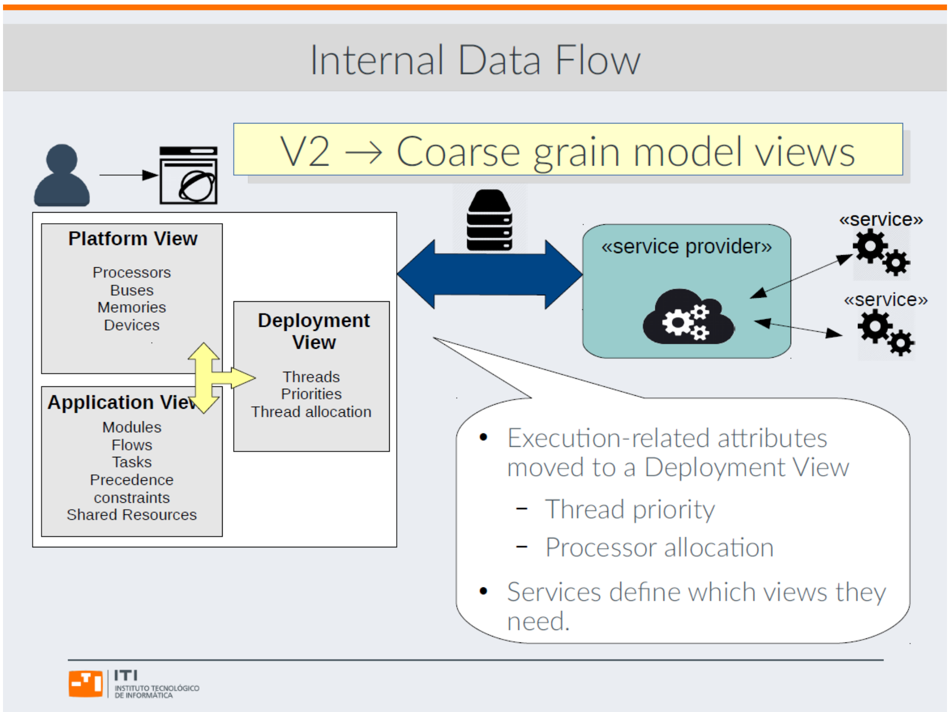
Agenda

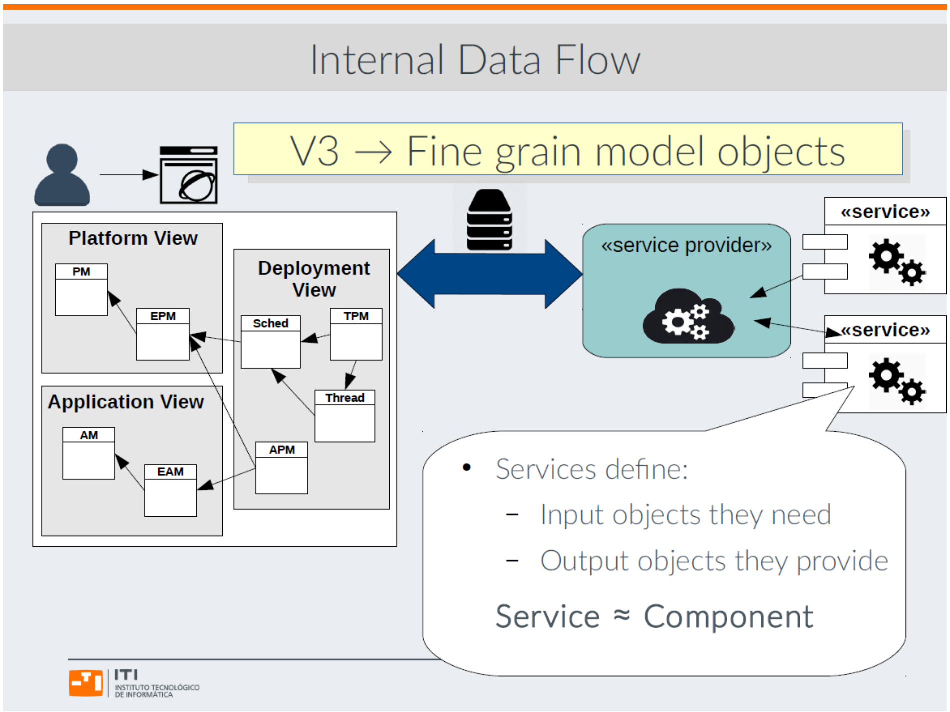
- Introduction
- Internal architecture
- ***Internal Data Flow***
- Possible interactions / extensions

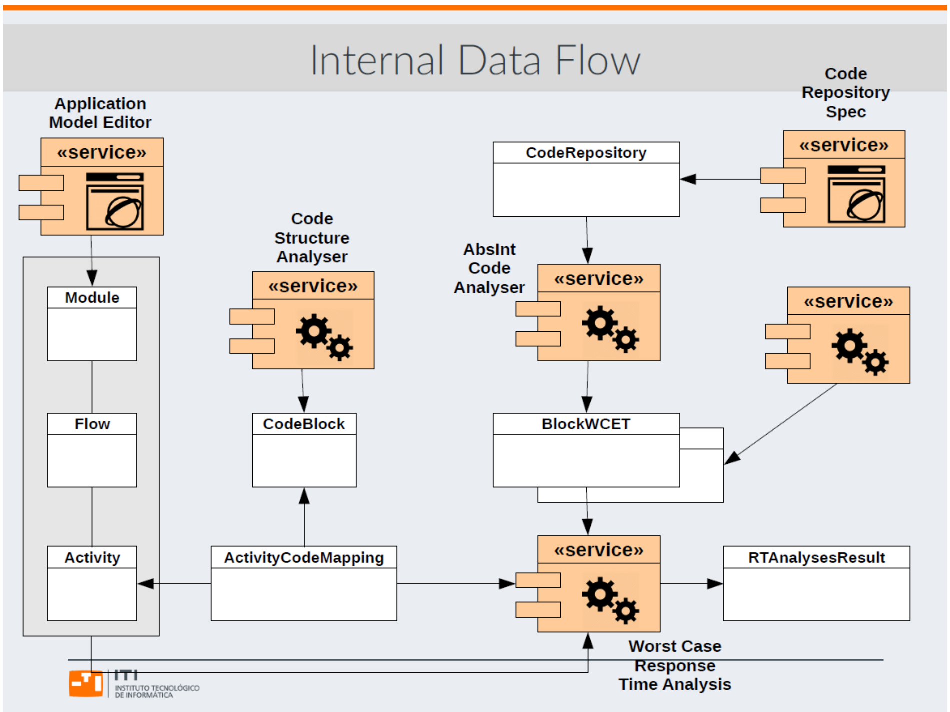
AQUAS SAFETY SECURITY PERFORMANCE

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA


Internal Data Flow
V1 → Monolitic Model
Platform Model
Processors
Buses
Memories
Devices
Application Model
Modules
Flows
Tasks
Precedence constraints
Shared Resources
Flow
+ Deadline
+ Period
+ Processor
Task
+ WCET
+ Deadline
+ Priority
«service provider»
«service»
«service»
Different views are interrelated.
Each service receives the whole model.
Services have to back annotate the model to add new attributes.
ITI
INSTITUTO TECNOLÓGICO DE INFORMÁTICA


Internal Data Flow
V2 → Coarse grain model views
Platform View
Processors
Buses
Memories
Devices
Application View
Modules
Flows
Tasks
Precedence constraints
Shared Resources
Deployment View
Threads
Priorities
Thread allocation
«service provider»
«service»
«service»
Execution-related attributes moved to a Deployment View
– Thread priority
– Processor allocation
Services define which views they need.
ITI
INSTITUTO TECNOLÓGICO DE INFORMÁTICA


Internal Data Flow
V3 → Fine grain model objects
Platform View
PM
EPM
Deployment View
Sched
TPM
Thread
APM
Application View
AM
EAM
«service provider»
«service»
«service»
Services define:
Input objects they need
Output objects they provide
Service ≈ Component
ITI


Internal Data Flow
Application Model Editor
«service»
Module
Flow
Activity
Code Structure Analyser
«service»
CodeBlock
ActivityCodeMapping
CodeRepository
AbsInt Code Analyser
«service»
BlockWCET
«service»
Worst Case Response Time Analysis
RTAnalysesResult
Code Repository Spec
«service»
«service»
ITI

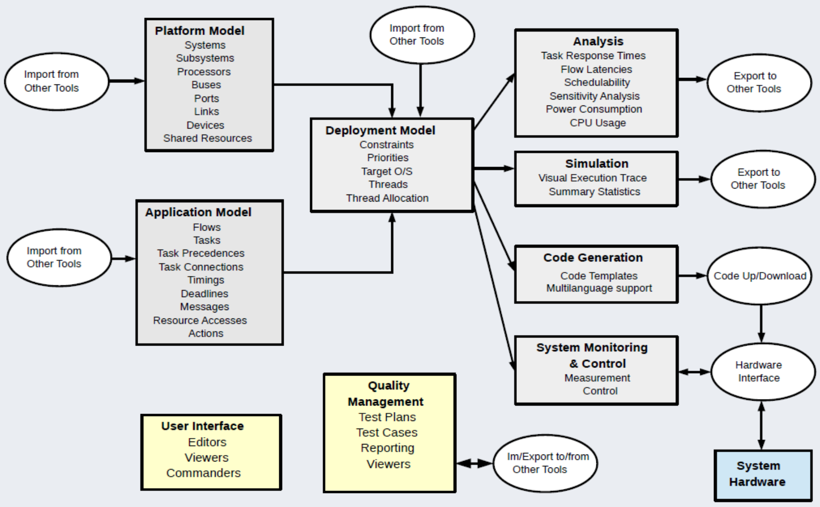
Agenda

- Introduction
- Internal architecture
- Internal Data Flow
- ***Possible interactions / extensions***

AQUAS SAFETY SECURITY PERFORMANCE

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

Internal/External Data Flow



ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

art2kitekt characteristics

- Application domain profiles
  - Execution platform, application model and analysis methods are strongly coupled.
  - Different platform/application/analysis profiles will be provided for each kind of system.
- Interoperability and extendibility
  - Interoperability with external tools should be possible, e.g. WCET analysis, high-level application modelling, etc.
  - Importing/exporting system models using common formats, e.g. JSON, XML ...
  - Data-binding and APIs for common tool programming languages, e.g. C/C++, PHP, Python, *Ada*, ...
- A simple and fast tool deployment based on web technologies

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

Cyber-Physical Systems Group
Research and Development Department

ssaez@iti.es
+34 963 877 069
http://www.iti.es

Follow us

AQUAS SAFETY SECURITY PERFORMANCE

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA
Advanced Technology for Business

ITI INSTITUTO TECNOLÓGICO DE INFORMÁTICA

2.2.9 HEPSYCODE

INTRODUCTION

UNIVERSITÀ DEGLI STUDI DE L'AQUILA

- The next ***HEPSYCODE Tutorial*** faces the problem of the **HW/SW co-design of dedicated** (embedded and real-time) **Systems** based on **Heterogeneous Parallel** architectures and presents a framework (with related methodology and prototypal tools), called **HEPSYCODE**, able to support the development of such systems in different application domains.

Hepsy Code

HW/SW CO-DEsign of HEterogeneous Parallel dedicated SYstems
www.hepsycode.com

2

TUTORIAL HEPSYCODE (23TH JANUARY)

UNIVERSITÀ DEGLI STUDI DE L'AQUILA

14.00 - 15.00
Topic 1
A System-Level Methodology for HW/SW Co-Design of Heterogeneous Parallel Dedicated Systems
Speaker: Vittoriano Muttillo

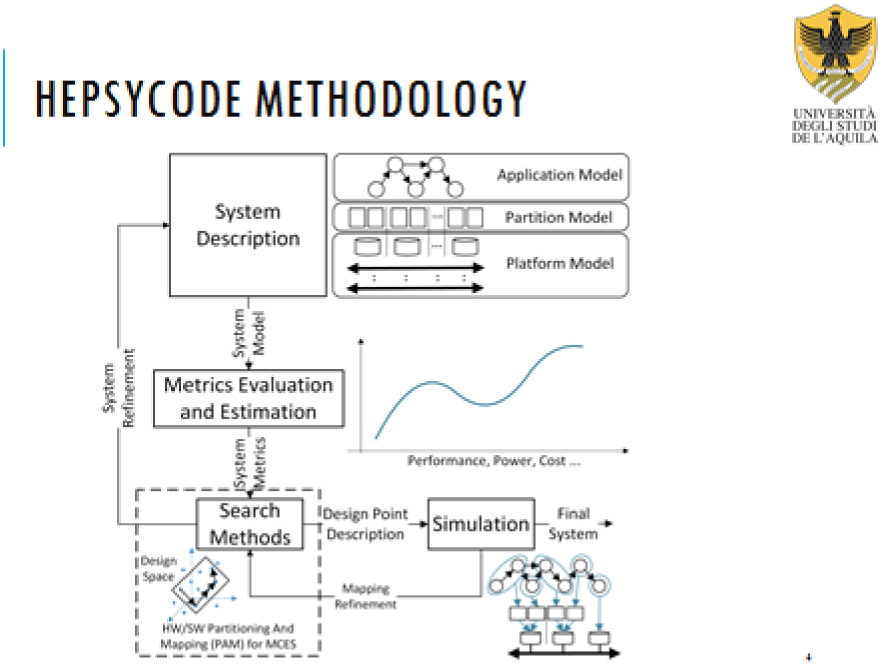
15.00 - 15.30
Topic 2
HEPSIM: an ESL HW/SW Co-Simulator Tool for HW/SW Co-Design flow
Speaker: Marco Santic

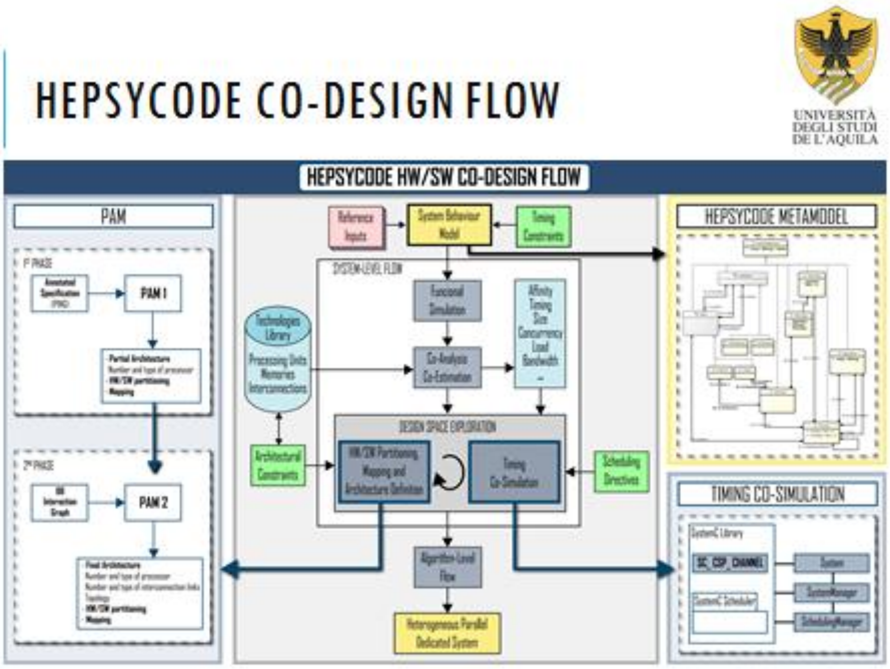
15.30 - 16.00 Coffee Break

16.00 - 17.00
Topic 3
Real-Time and Mixed Criticality Extensions for the HepsyCode Methodology: Past, Present, and Future work
Speaker: Vittoriano Muttillo

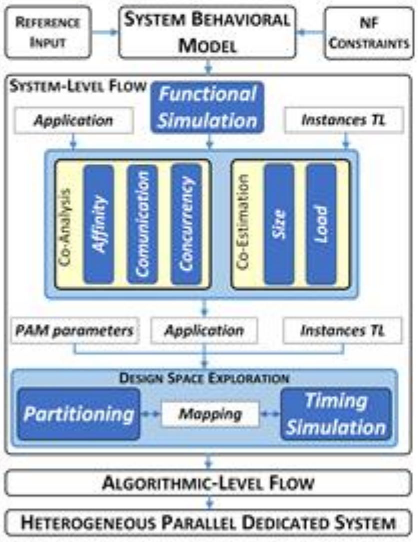
17.00 - 17.30
Topic 4
A HW/SW Unified approach for embedded system monitoring
Speaker: Giacomo Valente

3

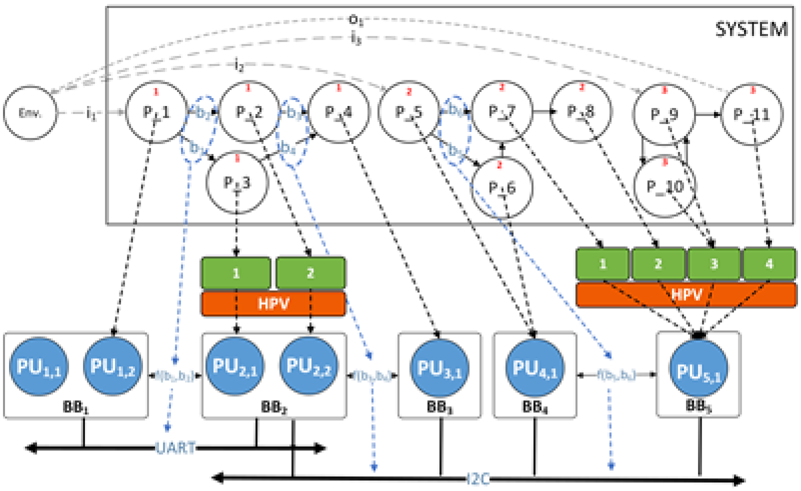

HEPSYCODE METHODOLOGY
UNIVERSITÀ DEGLI STUDI DE L'AQUILA
System Description
Application Model
Partition Model
Platform Model
System Model
System Refinement
Metrics Evaluation and Estimation
Performance, Power, Cost ...
System Metrics
Search Methods
Design Point Description
Simulation
Final System
Design Space
Mapping Refinement
HW/SW Partitioning And Mapping (PAM) for MCES

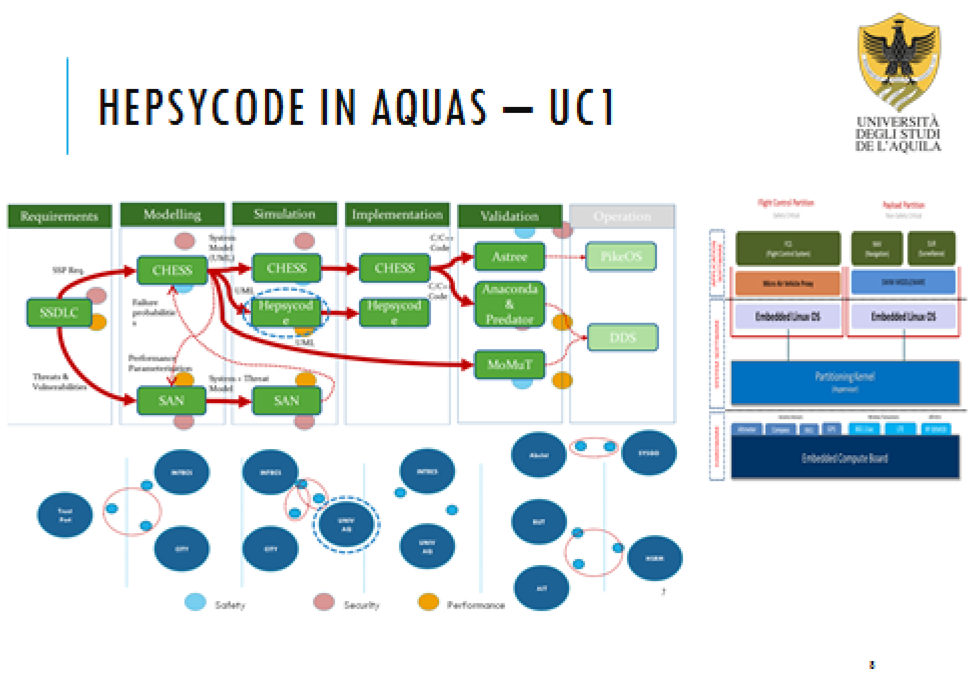

HEPSYCODE CO-DESIGN FLOW
UNIVERSITÀ DEGLI STUDI DE L'AQUILA
HEPSYCODE HW/SW CO-DESIGN FLOW
PAM
PAM 1
PAM 2
HEPSYCODE METAMODEL
TIMING CO-SIMULATION
DESIGN SPACE EXPLORATION

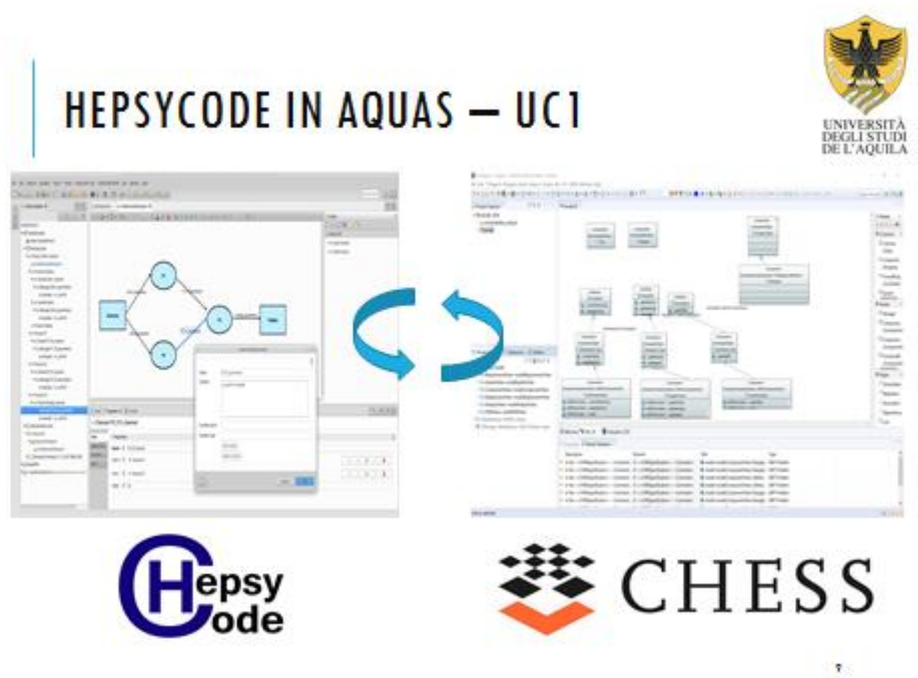
HEPSYCODE FRAMEWORK

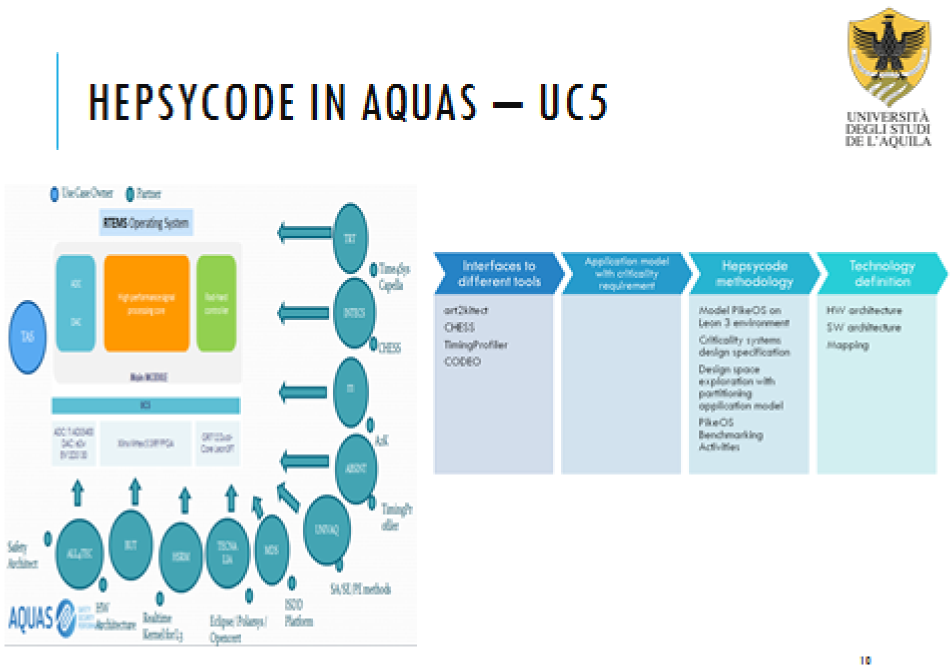


HEPSYCODE SOLUTION



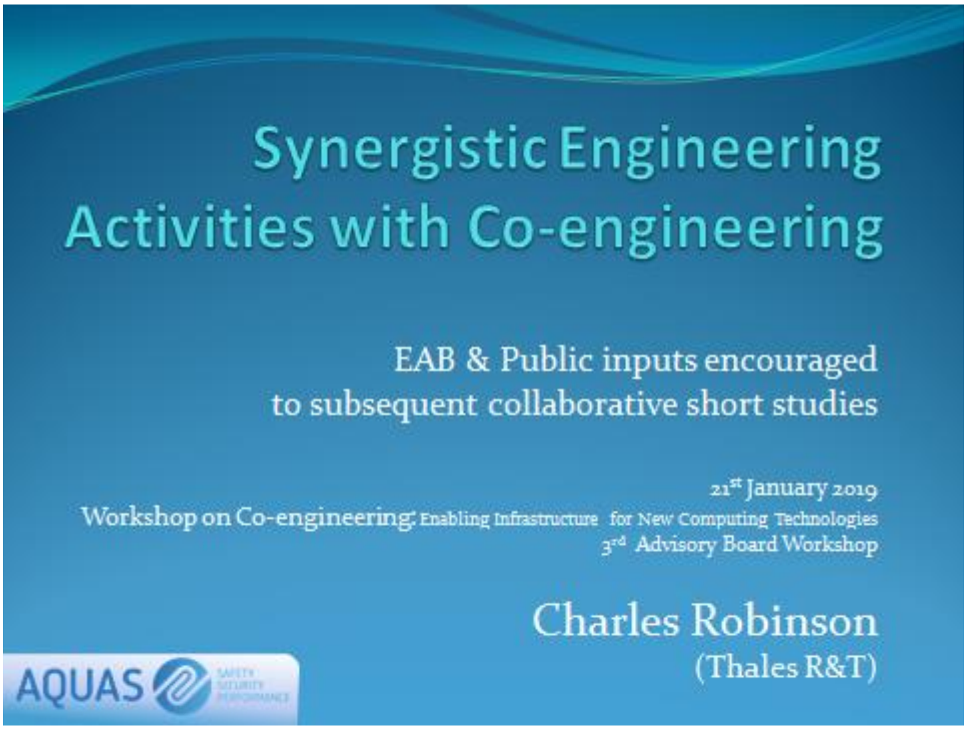

HEPSYCODE IN AQUAS – UC1
UNIVERSITÀ DEGLI STUDI DE L'AQUILA
Requirements
Modelling
Simulation
Implementation
Validation
Operation
SSDLC
CHESS
CHESS
CHESS
Hepsycode
Hepsycode
SAN
SAN
Astree
Anaconda & Predator
MoMuT
PikeOS
DDS
Safety
Security
Performance
Embedded Linux OS
Embedded Linux OS
Partitioning kernel
Embedded Compute Board

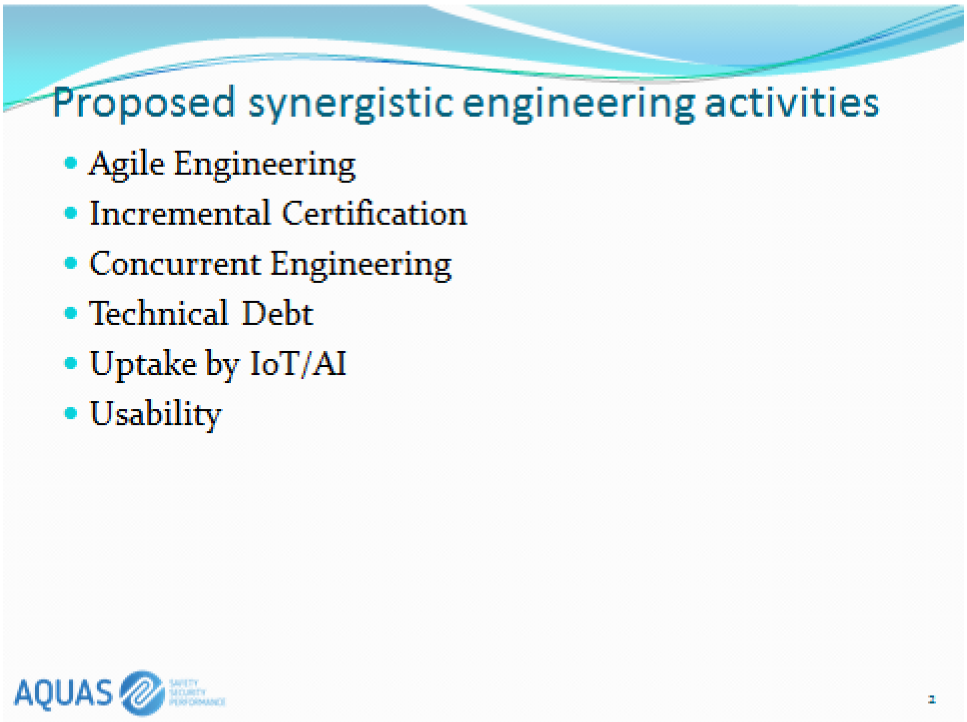

HEPSYCODE IN AQUAS – UC1
UNIVERSITÀ DEGLI STUDI DE L'AQUILA
Hepsycode
CHESS


HEPSYCODE IN AQUAS – UC5
UNIVERSITÀ DEGLI STUDI DE L'AQUILA
RTEMS Operating System
AQUAS
Interfaces to different tools
art2kitect
CHESS
TimingProfiler
CODEO
Application model with criticality requirement
Hepsycode methodology
Model PikeOS on Leon 3 environment
Criticality systems design specification
Design space exploration with partitioning application model
PikeOS Benchmarking Activities
Technology definition
HW architecture
SW architecture
Mapping
10


UNIVERSITÀ DEGLI STUDI DE L'AQUILA
UNIVERSITÀ DEGLI STUDI DE L'AQUILA
THANKS!
Questions?
Not miss the tutorial!!!

2.2.10 Synergistic Engineering Activities with Co-engineering





Purpose

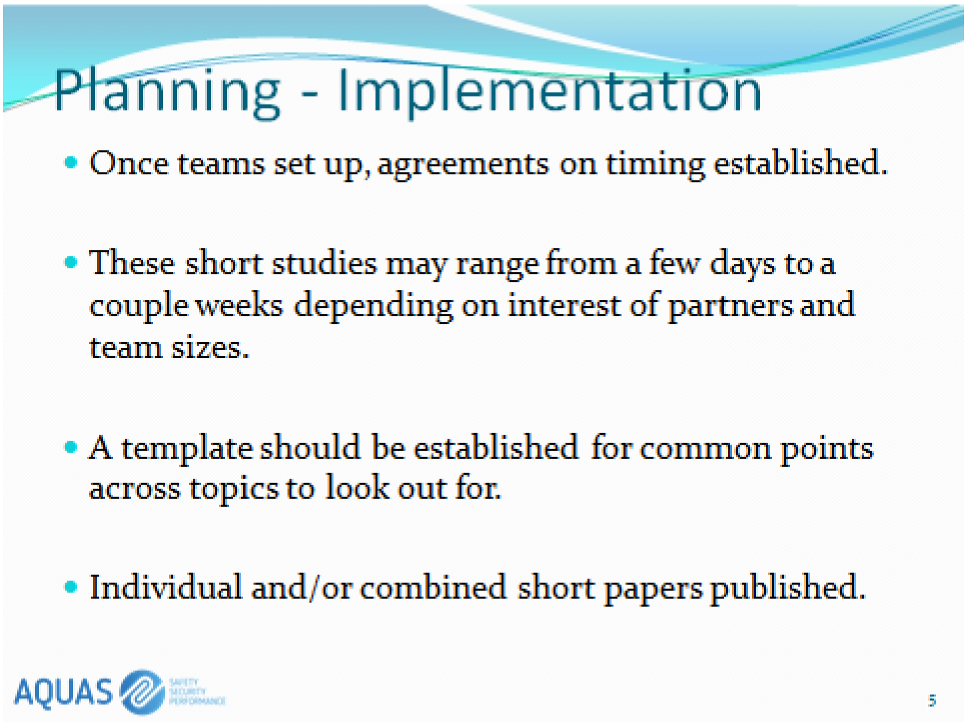
- Uptake of co-engineering is encouraged by showing its value. Some market research is part of project activities – which is where the short studies on synergistic activities fits in.
- Identifying what CE can bring to these activities strengthens the reasons showing why much more focus is needed on CE.
- Identifying what these activities can bring to the AQUAS CE will strengthen our approach.
- These themes may be important to advance further in follow-up projects.

AQUAS SAFETY SECURITY PERFORMANCE 3

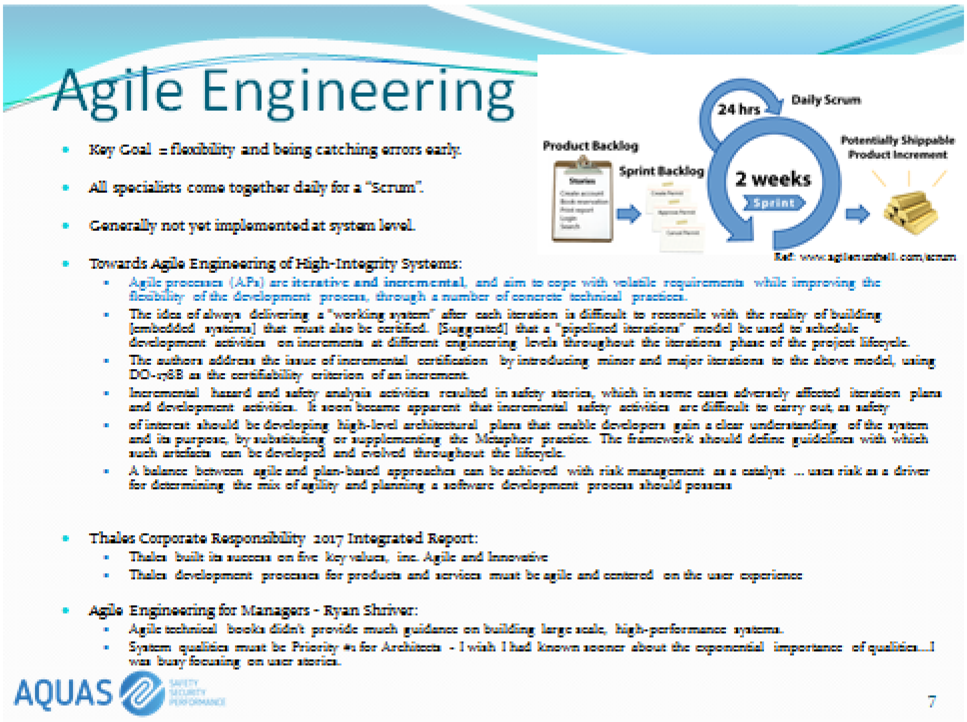
Planning - teams

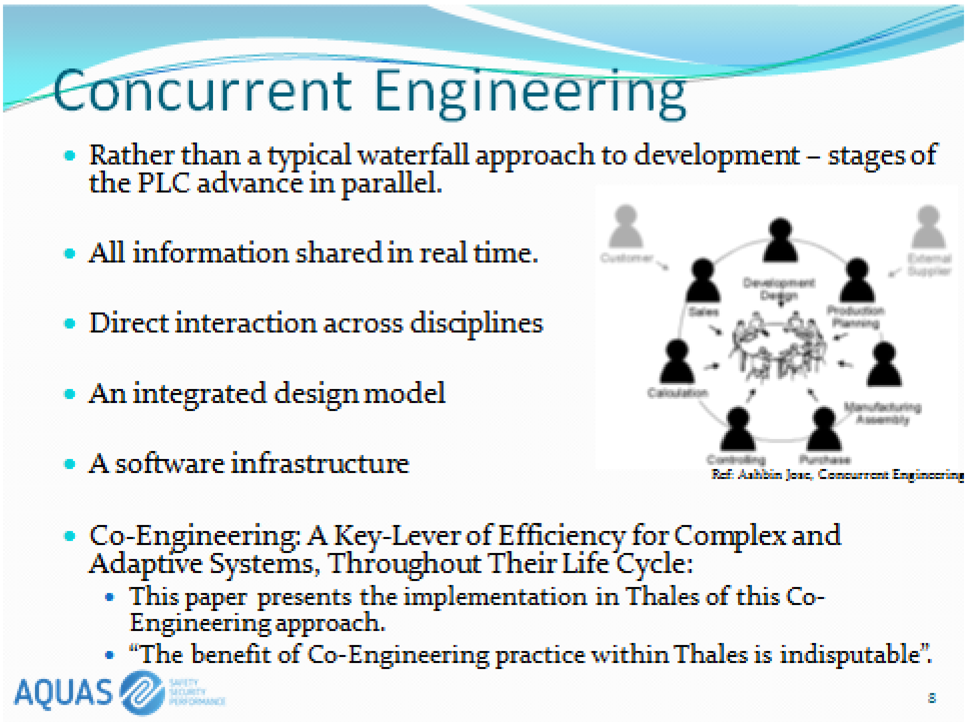
- Contributions welcome from EAB
- Teams materialise / proposed in next few weeks.
- Action plans established by end of February.
- Small studies take place over the following year.

AQUAS SAFETY SECURITY PERFORMANCE 4


Planning - Implementation
Once teams set up, agreements on timing established.
These short studies may range from a few days to a couple weeks depending on interest of partners and team sizes.
A template should be established for common points across topics to look out for.
Individual and/or combined short papers published.
AQUAS
5


Brief Oerview of Synergistic Engineering Activities
AQUAS
6

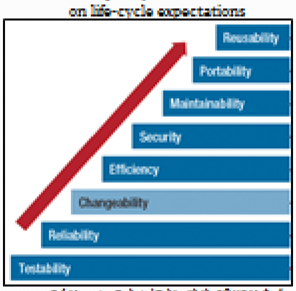

Agile Engineering
Product Backlog
Sprint Backlog
24 hrs
Daily Scrum
2 weeks
Sprint
Potentially Shippable Product Increment
Ref: www.agilenutshell.com/scrum
Key Goal = flexibility and being catching errors early.
All specialists come together daily for a "Scrum".
Generally not yet implemented at system level.
Towards Agile Engineering of High-Integrity Systems:
Agile processes (APs) are iterative and incremental, and aim to cope with volatile requirements while improving the flexibility of the development process, through a number of concrete technical practices.
The idea of always delivering a "working system" after each iteration is difficult to reconcile with the reality of building [embedded systems] that must also be certified. [Suggested] that a "pipelined iterations" model be used to schedule development activities on increments at different engineering levels throughout the iterations phase of the project lifecycle.
The authors address the issue of incremental certification by introducing minor and major iterations to the above model, using DO-178B as the certifiability criterion of an increment.
Incremental hazard and safety analysis activities resulted in safety stories, which in some cases adversely affected iteration plans and development activities. It soon became apparent that incremental safety activities are difficult to carry out, as safety
of interest should be developing high-level architectural plans that enable developers gain a clear understanding of the system and its purpose, by substituting or supplementing the Metaphor practice. The framework should define guidelines with which such artefacts can be developed and evolved throughout the lifecycle.
A balance between agile and plan-based approaches can be achieved with risk management as a catalyst ... uses risk as a driver for determining the mix of agility and planning a software development process should possess
Thales Corporate Responsibility 2017 Integrated Report:
Thales built its success on five key values, inc. Agile and Innovative
Thales development processes for products and services must be agile and centered on the user experience
Agile Engineering for Managers - Ryan Shriver:
Agile technical books didn't provide much guidance on building large scale, high-performance systems.
System qualities must be Priority #1 for Architects - I wish I had known sooner about the exponential importance of qualities...I was busy focusing on user stories.
AQUAS
7


Concurrent Engineering
Rather than a typical waterfall approach to development – stages of the PLC advance in parallel.
All information shared in real time.
Direct interaction across disciplines
An integrated design model
A software infrastructure
Customer
External Supplier
Development Design
Sales
Production Planning
Calculation
Manufacturing Assembly
Controlling
Purchase
Ref: Ashbin Jose, Concurrent Engineering
Co-Engineering: A Key-Lever of Efficiency for Complex and Adaptive Systems, Throughout Their Life Cycle:
This paper presents the implementation in Thales of this Co-Engineering approach.
"The benefit of Co-Engineering practice within Thales is indisputable".
AQUAS
8

Technical Debt

- Tradeoff Decisions Across Time in Technical Debt Management: A SystematicLiteratureReview:
  - Technical Debt arises **from decisions that favour short-term out comes at the cost of longer-term disadvantages**. They may be taken knowingly or based on missing or incomplete awareness of the costs; they are taken indifferent roles, situations, stages and ways.
  - Whatever technical or business factor motivate such decisions, they always imply a trade-off in time, a 'now vs later'.

Software quality assessment based on life-cycle expectations



Ref. Managing Technical Debt with the SQALE Method

AQUAS SAFETY SECURITY PERFORMANCE

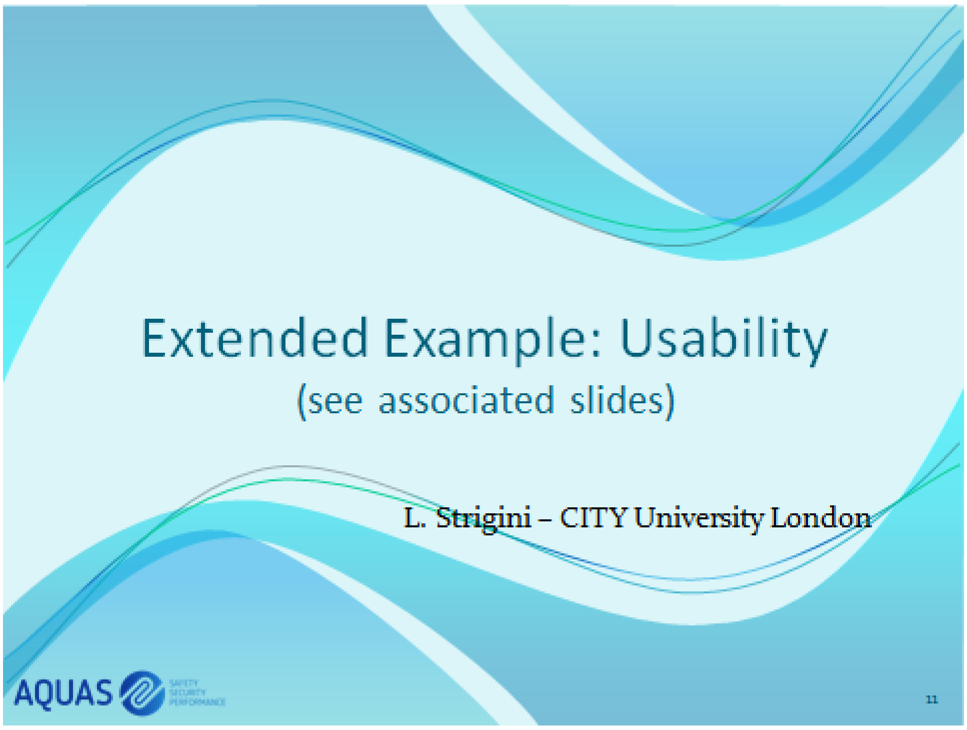
9

Uptake by IoT/AI

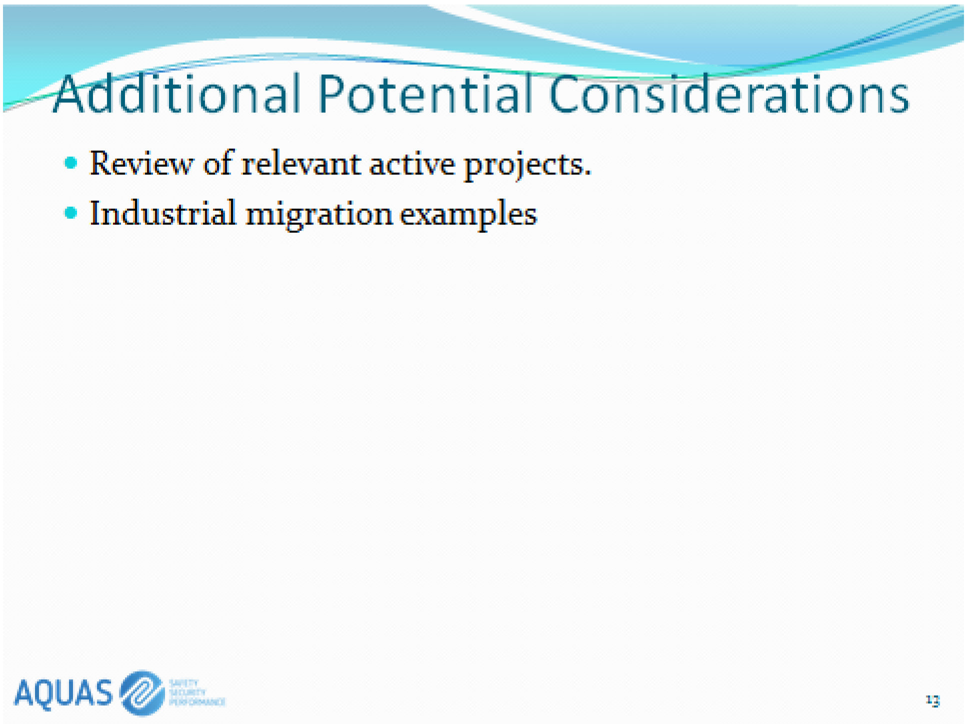
- EU investment in IoT
  - 18 Dec 2018 - The European Commission approved a plan by France, Germany, Italy, and the UK to give €1.75 billion in public funds to support a joint research and innovation project in microelectronics.
- EU investment in AI
  - Goal beyond 2020: Increasing investments from €4-5 billion / year today to €20 billion / year.
  - Desire AI to be a core technology in most cyber-physical systems.
- These technology classes are expected hold significant promise for the future of Europe.
  - However success will be limited without research investment in industrial processes/methodologies – particularly for CPS and managing the safety-security-performance co-engineering to have system dependability.

AQUAS SAFETY SECURITY PERFORMANCE

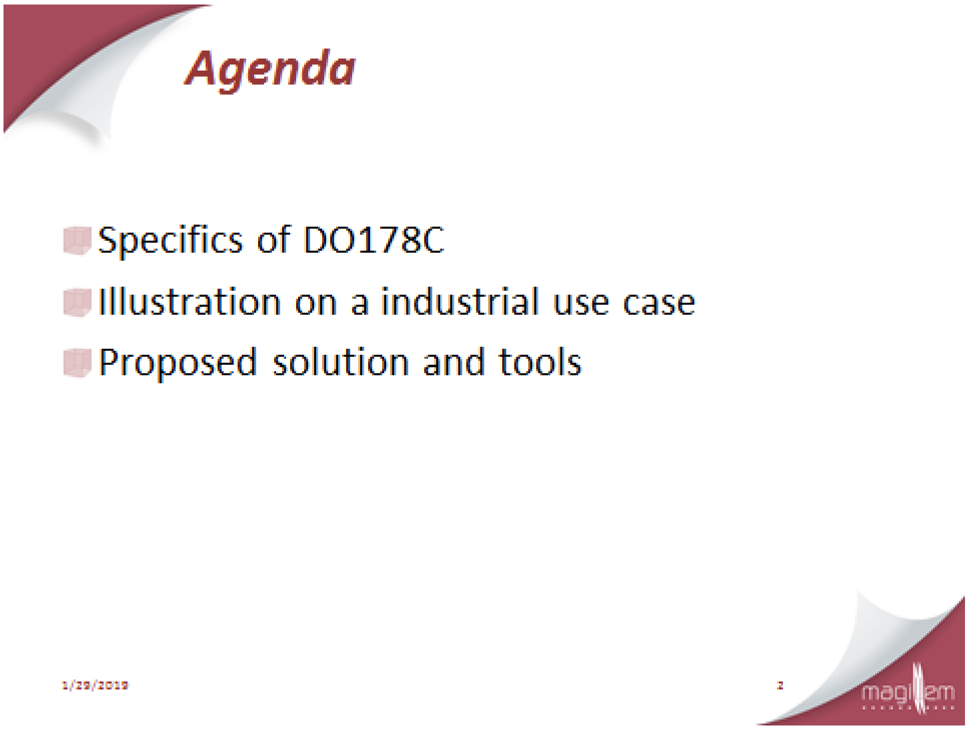
10

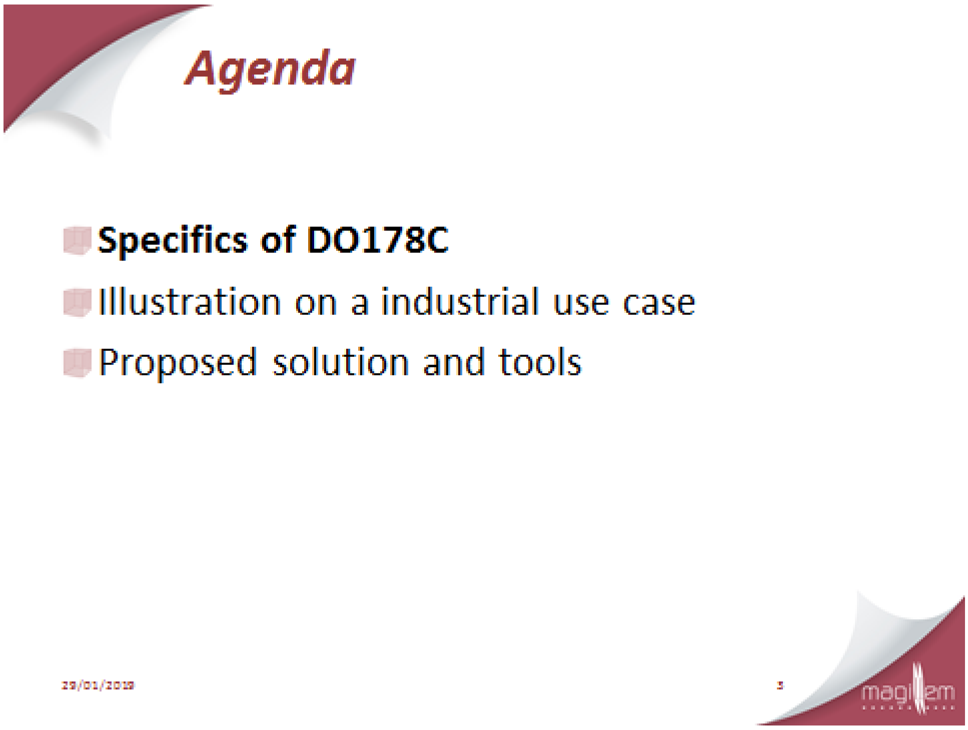

Extended Example: Usability
(see associated slides)
L. Strigini – CITY University London
AQUAS


Extended Example: Incremental Certification
(see associated slides)
E. Vaumorin/M. Pfeiffer - Magillem
AQUAS



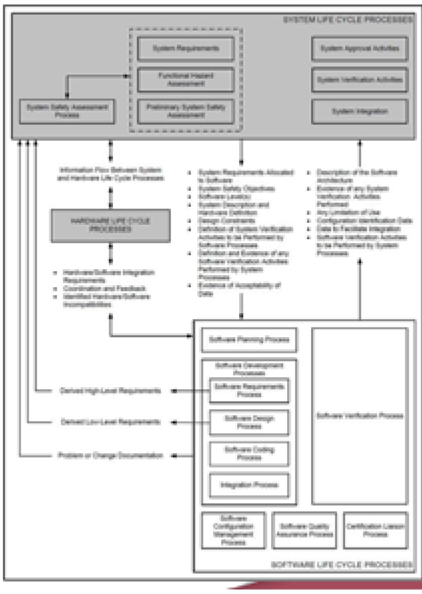
2.2.11 Incremental Certification


Agenda
Specifics of DO178C
Illustration on a industrial use case
Proposed solution and tools
1/29/2019
2
magillem


Agenda
Specifics of DO178C
Illustration on a industrial use case
Proposed solution and tools
29/01/2019
3
magillem

DO-178C (RTCA) and other certification domains

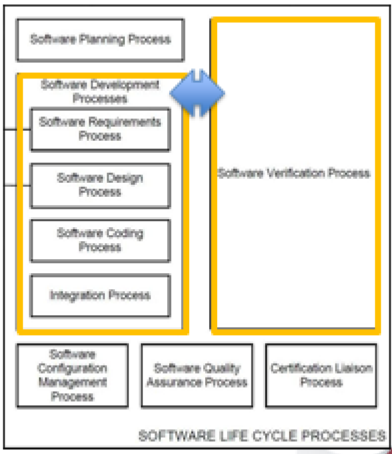
- DO178C is a guide for the production of SW for airborne systems
  - Guidance for satisfying certification requirements
  - Give main objectives for SW life cycle
  - Describe activities for achieving those objectives
  - Data showing that objectives have been satisfied
    - List of SW life cycle data for certification
    - Planned activities have been performed
- Interactions with System and HW life cycle
  - Need system description and HW definition
    - Needs for HW/SW integration process
  - Need for verification process/activities
    - Verify compatibility between HW and SW
- In SW life cycle, HW will influence:
  - HW/SW integration process
  - Verification process
    - Reviews and Analysis
    - Test environment



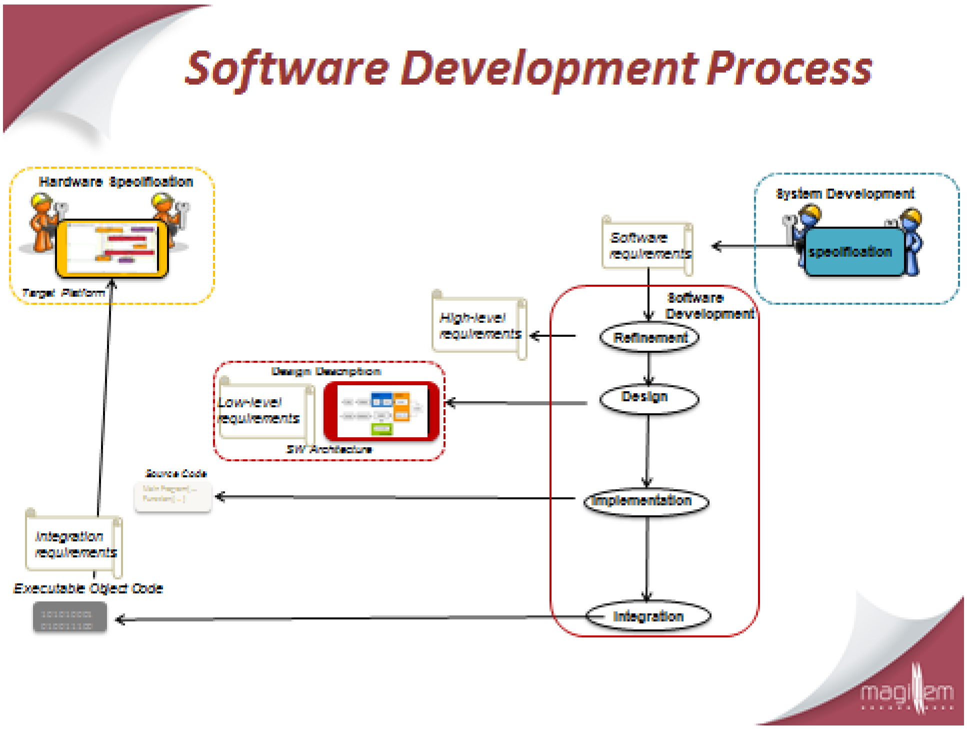
29/01/2019

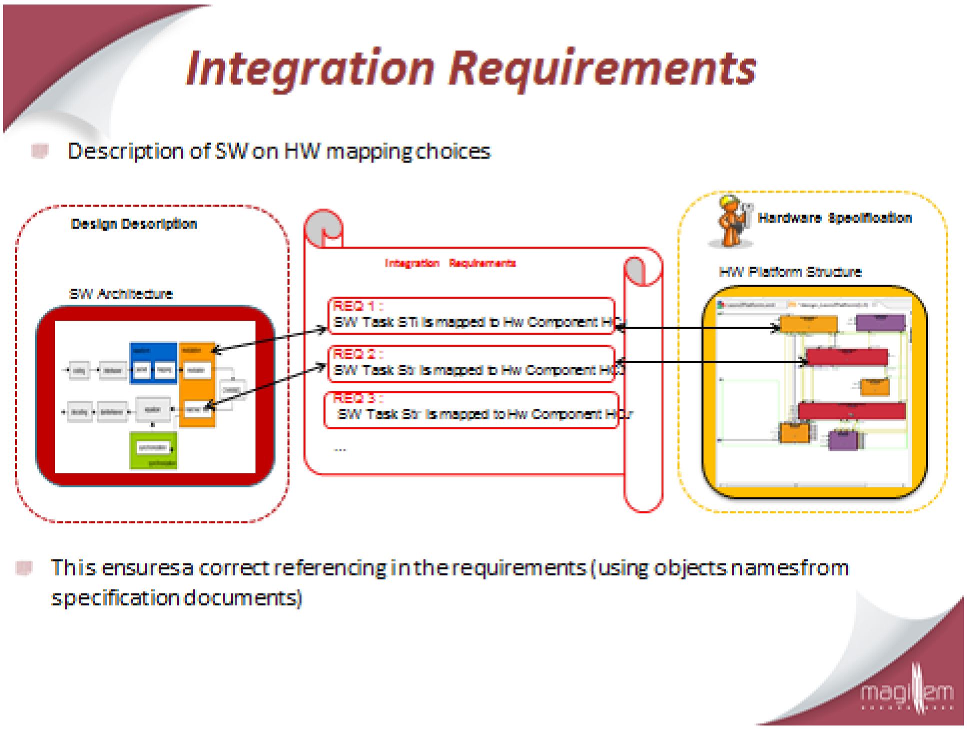
DO-178C - Software Development and Verification Processes

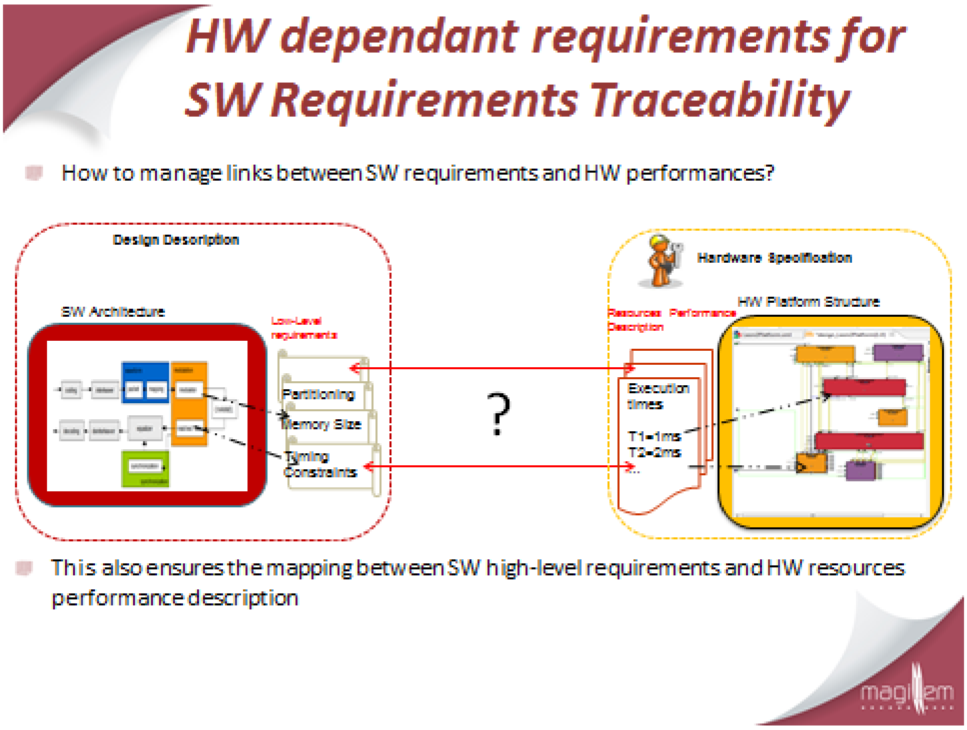
- Detect and report errors that may have been introduced during SW development process
  - High level requirements
  - Low level requirement
  - Source Code
  - Integration, test coverage
- Costly
- Removal of errors is an activity of SW development process
- Activities
  - Reviews and analysis
  - Testing for further assessment
- Can we simplify verification process for re-certification purpose?

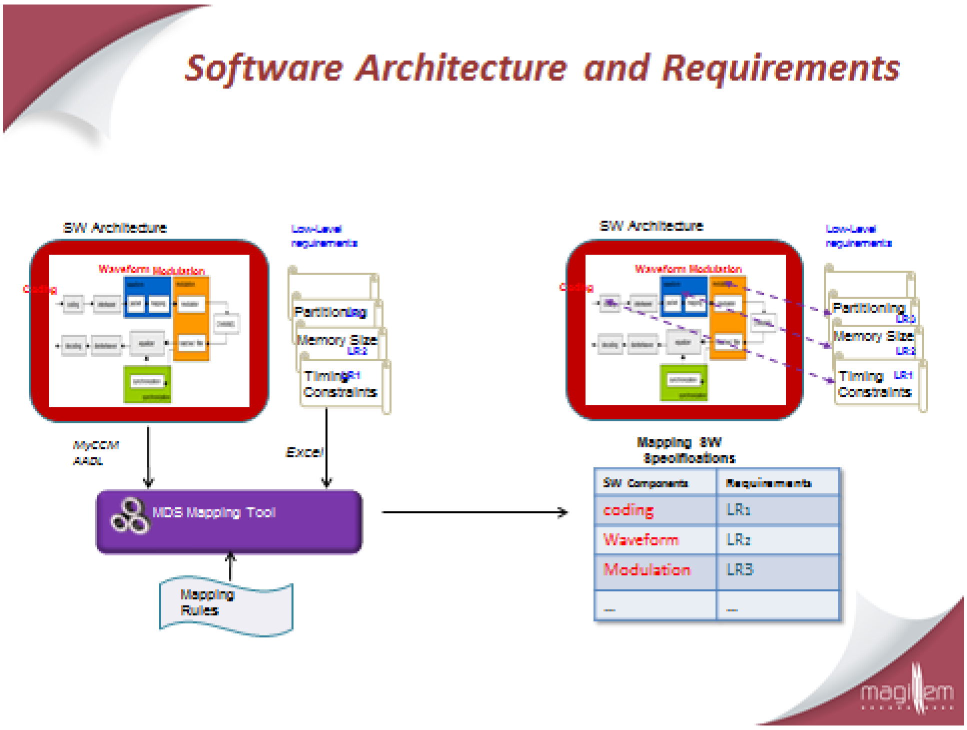


29/01/2019 5

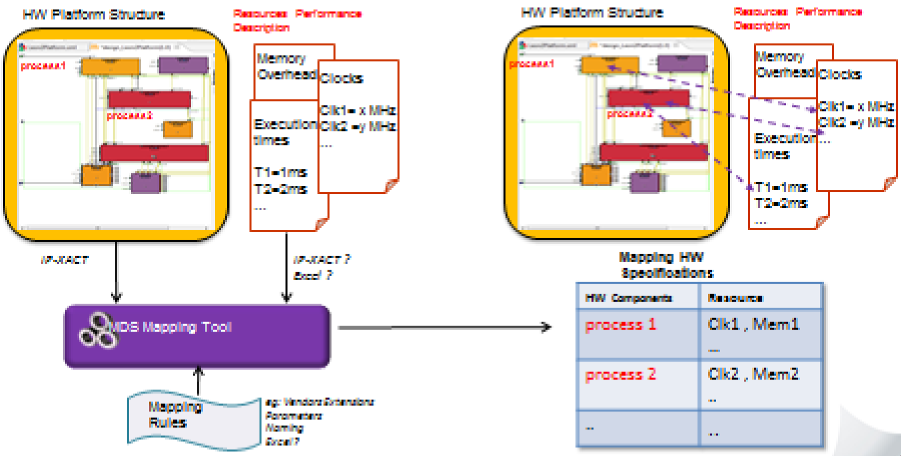

Software Development Process
Hardware Specification
Target Platform
System Development
specification
Software requirements
Software Development
High-level requirements
Refinement
Design Description
Low-level requirements
SW Architecture
Design
Source Code
Implementation
Integration requirements
Executable Object Code
Integration
magillem


Integration Requirements
Description of SW on HW mapping choices
Design Description
SW Architecture
Integration Requirements
REQ 1 :
SW Task STi is mapped to Hw Component H
REQ 2 :
SW Task Sti is mapped to Hw Component H
REQ 3 :
SW Task Str is mapped to Hw Component H
...
Hardware Specification
HW Platform Structure
This ensures a correct referencing in the requirements (using objects names from specification documents)
magillem


HW dependant requirements for SW Requirements Traceability
How to manage links between SW requirements and HW performances?
Design Description
SW Architecture
Low-Level requirements
Partitioning
Memory Size
Timing Constraints
?
Hardware Specification
Resources Performance Description
HW Platform Structure
Execution times
T1=1ms
T2=2ms
This also ensures the mapping between SW high-level requirements and HW resources performance description
magillem

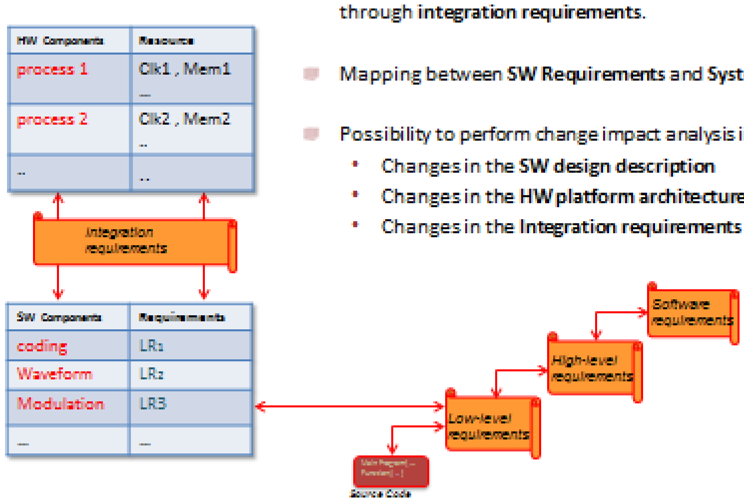

Software Architecture and Requirements
SW Architecture
Low-Level requirements
Waveform Modulation
Partitioning
Memory Size
Timing Constraints
MyCCM
AADL
Excel
MDS Mapping Tool
Mapping Rules
Mapping SW Specifications
SW Components
Requirements
coding
LR1
Waveform
LR2
Modulation
LR3
magillem

HW platform and resources



Traceability Impact Management

- Mapping between **HW ressources** and **SW requirements** through **integration requirements**.
- Mapping between **SW Requirements** and **System Requirements**
- Possibility to perform change impact analysis in case of
  - Changes in the **SW design description**
  - Changes in the **HW platform architecture**
  - Changes in the **Integration requirements**



Agenda

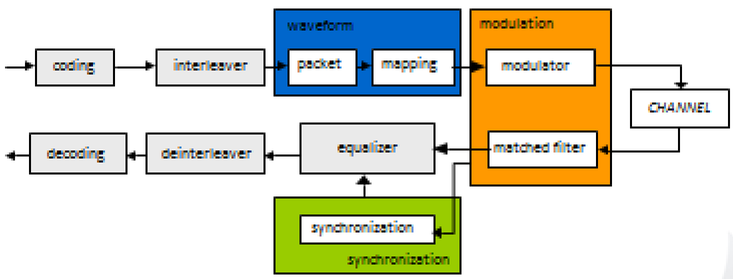
- Specifics of DO178C
- **Illustration on a industrial use case**
- Proposed solution and tools

1/29/2019 12

magillem

Avionics demonstrator

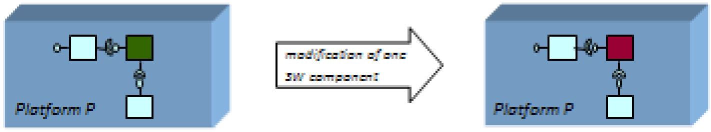
- Software application: a physical layer waveform for SDR communication system
  - is subject to evolution (market needs: more QoS, more throughput & bandwidth, ...)
  - needs revalidation of processes for recertification to be DO-178C compliant



magillem

Incremental scenarios (1/3)

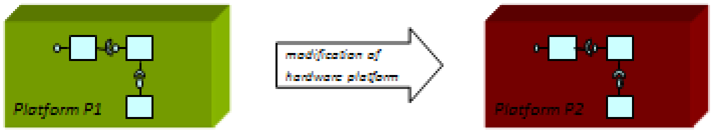
- Scenario 1: Modification of application **SW**, same **HW platform**



- Re-verification efforts (considering timing constraint only) required for
  - SW high level requirements
  - SW low level requirements
  - SW integration (see section 6.4.3.b in D0-178C)
  - Components contracts/properties verification
  - Data flow, control flow, timing, performance analysis

Incremental scenarios (2/3)

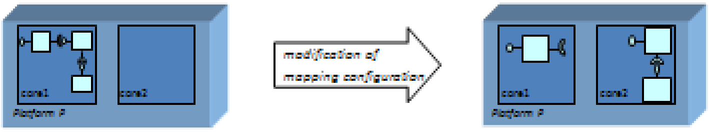
- Scenario 2: Modification of **HW platform**, same application SW



- Re-verification efforts (considering timing constraint only) required for:
  - SW high & low level requirements
  - SW/HW integration (see section 6.4.3.a in D0-178C)
  - Timing & performance analysis
  - Stack overflow, memory size, ... (and ptf related features)

Incremental scenarios (3/3)

- Scenario 3: Modification of **mapping**, same **HW platform** & same **application SW**



- Re-verification efforts (considering timing constraint only) required for:
  - SW high & low level requirements
  - SW integration (see section 6.4.3.b in D0-178C)
  - SW/HW integration (see section 6.4.3.a in D0-178C)
  - Timing & performance analysis
  - Stack overflow, memory size, ... (and ptf related features)
  - Shared memory acces

magillem

Agenda

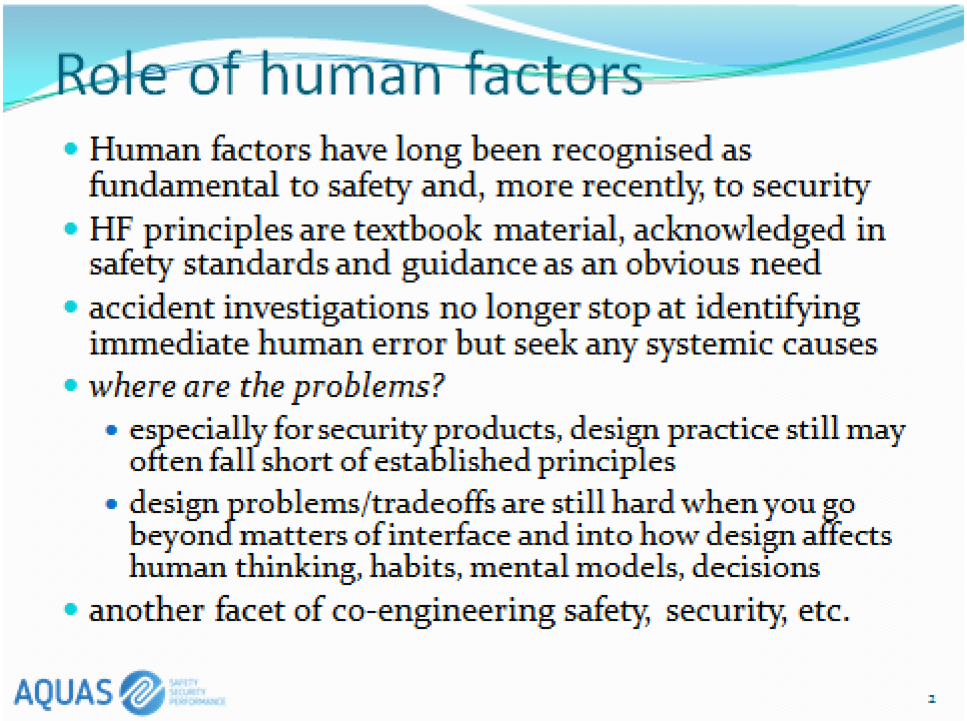
- Specifics of DO178C
- Illustration on a industrial use case
- **Proposed solution and tools**

1/29/2019 17

magillem

2.2.12 Usability and Human Factors


Usability and Human Factors
co-engineering aspects
21st January 2019
Workshop on Co-engineering: Enabling Infrastructure for New Computing Technologies
3rd Advisory Board Workshop
Lorenzo Strigini
(City, University of London)
AQUAS


Role of human factors
Human factors have long been recognised as fundamental to safety and, more recently, to security
HF principles are textbook material, acknowledged in safety standards and guidance as an obvious need
accident investigations no longer stop at identifying immediate human error but seek any systemic causes
where are the problems?
especially for security products, design practice still may often fall short of established principles
design problems/tradeoffs are still hard when you go beyond matters of interface and into how design affects human thinking, habits, mental models, decisions
another facet of co-engineering safety, security, etc.
AQUAS
2

Co-engineering of safety, security and performance – with human factors

Example: human-operated equipment often includes automated alerts for potentially dangerous conditions

- to harm safety, attackers could try to disable alarms
- but could instead tamper with the alarm's settings to
  - make *false alarms* frequent
  - making it a habitual "reflex" to ignore/reset the alarm
    - even when proper human response would confirm the danger
    - "cry wolf" effect, known from experience, including accidents
- to deal with this, analyses need to link security, safety aspects *through* human behaviour patterns
  - to include even such attacks meant to cause
    - not accidents directly
    - but "safe" conditions that yet cause unsafe actions
  - safety-only or security-only analyses may easily miss this risk

AQUAS SAFETY SECURITY PERFORMANCE

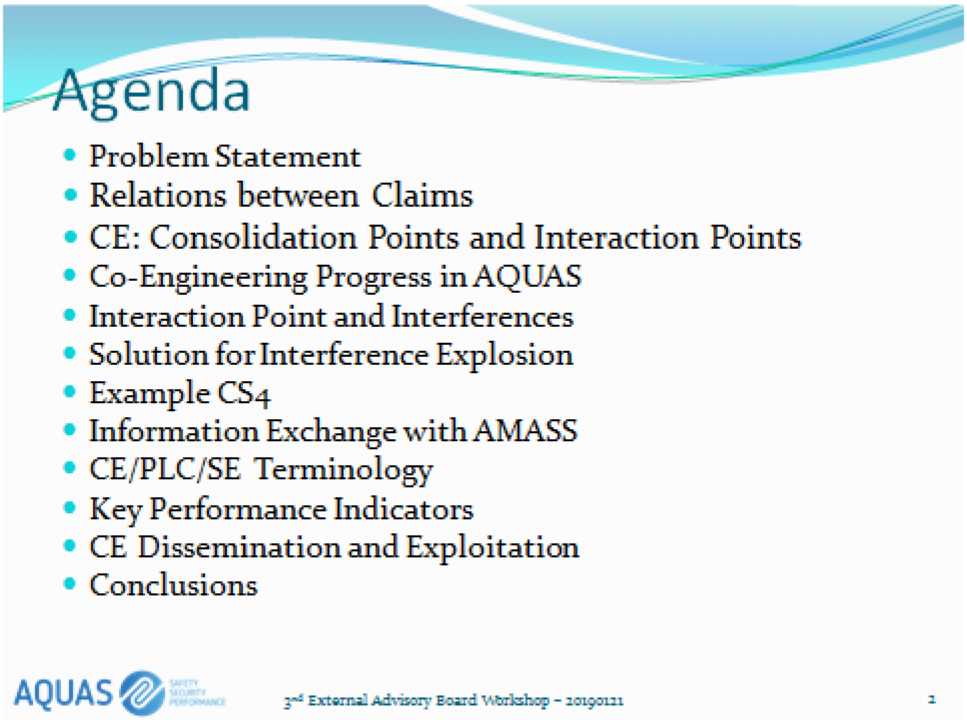
Some activity in AQUAS

- in the Medical Use Case
  - the device design applies standard usability precautions
  - combined AQUAS analysis includes reasoning about human effects
    - e.g. trade-offs around possible authentication of users
    - e.g. how the novel capabilities of the device may affect response to alarms
  - these HF considerations are included in overall risk analysis
  - we are also analysing pertinent standards to suggest possible improvements

AQUAS SAFETY SECURITY PERFORMANCE 4


Thank you!
immediate comments, question?
if interested in discussing in depth, collaboration, ways to move forward, please do contact us:
strigini@csr.city.ac.uk
AQUAS
5

2.2.13 Inside Product Life Cycle Stages



Co-Engineering Problem Statement

- Different quality attributes (in AQUAS focus on safety, security and performance) require different (mitigation) measures
- Safety and security cultures are very diverse and sometimes almost incompatible
- Safety & security people speak different languages
- Safety systems were constructed based on the assumption that they are isolated from the outer world
- Until recently, tools were not very interoperable
- Until few years ago there was only disjoint standardization

- But reality is:
  - There are mutual influences between different quality attributes causing expensive and time-consuming trade-off analyses between them and iterations in lifecycle processes
  - Safety & security people still work independently with partly incompatible results

AQUAS SAFETY SECURITY PERFORMANCE 3rd External Advisory Board Workshop – 20190121 3

Relations between Claims wrt. Quality Attributes

Dependency relationship.

- The claim A of one attribute depends on the fulfillment of claim B of another attribute.
- E.g. a fail-safe claim (safety) depends on safety system not tampered (security).

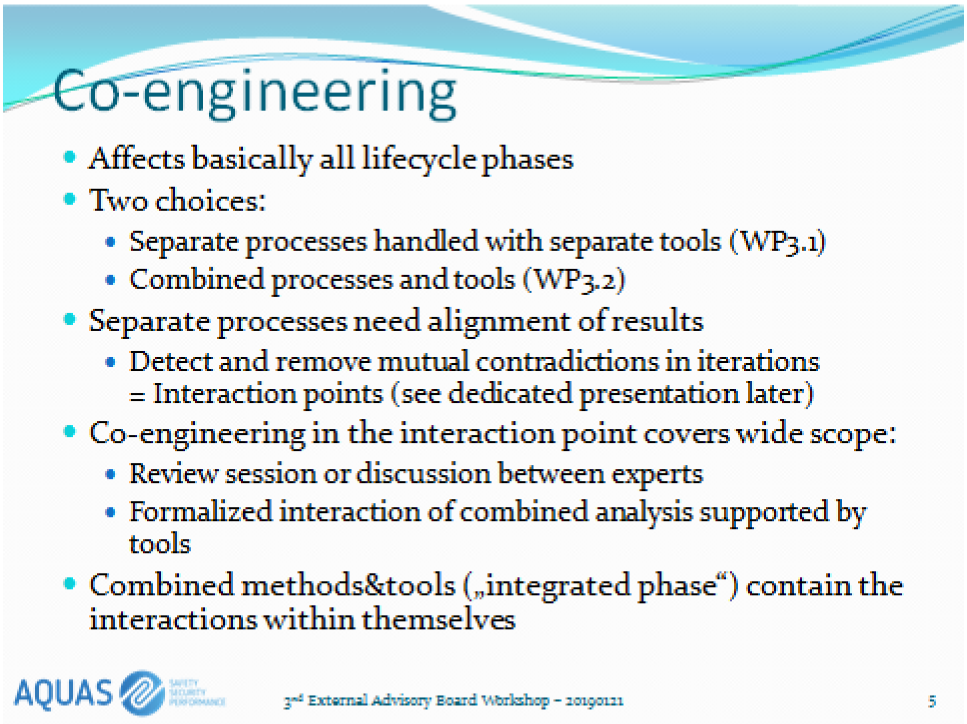
Conflicting relationship.

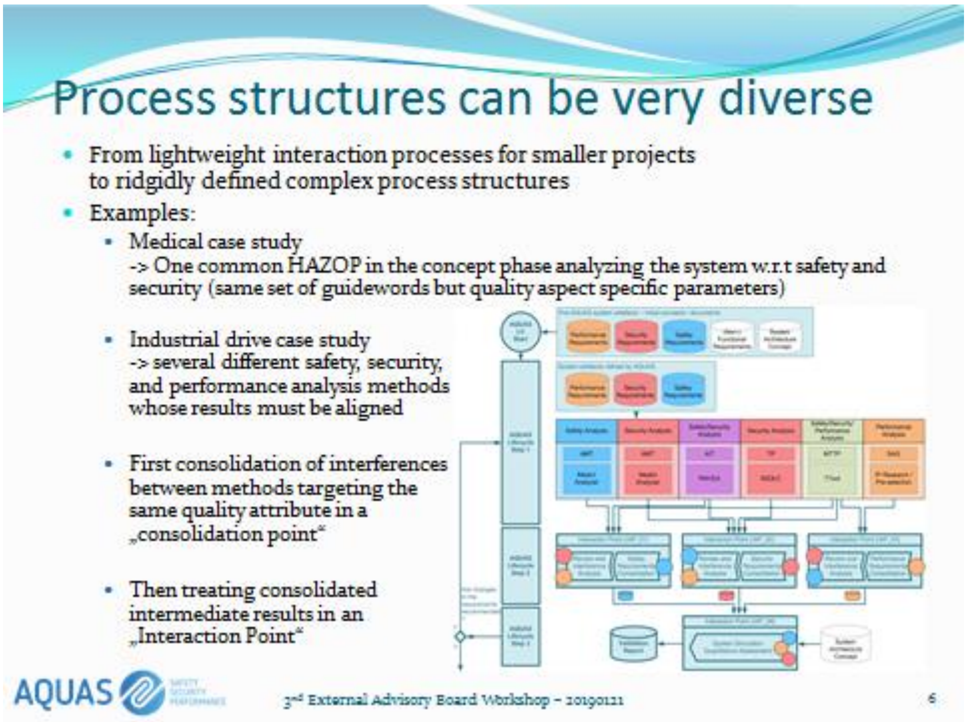
- The assurance measure of attribute A is in conflict with the assurance measure of attribute B.
- E.g. "strong password or blocking a terminal after several failed login attempts" (security) conflicts with "emergency shutdown" (safety).
- Resolution of such a conflict needs to be noted in the Assurance Case.

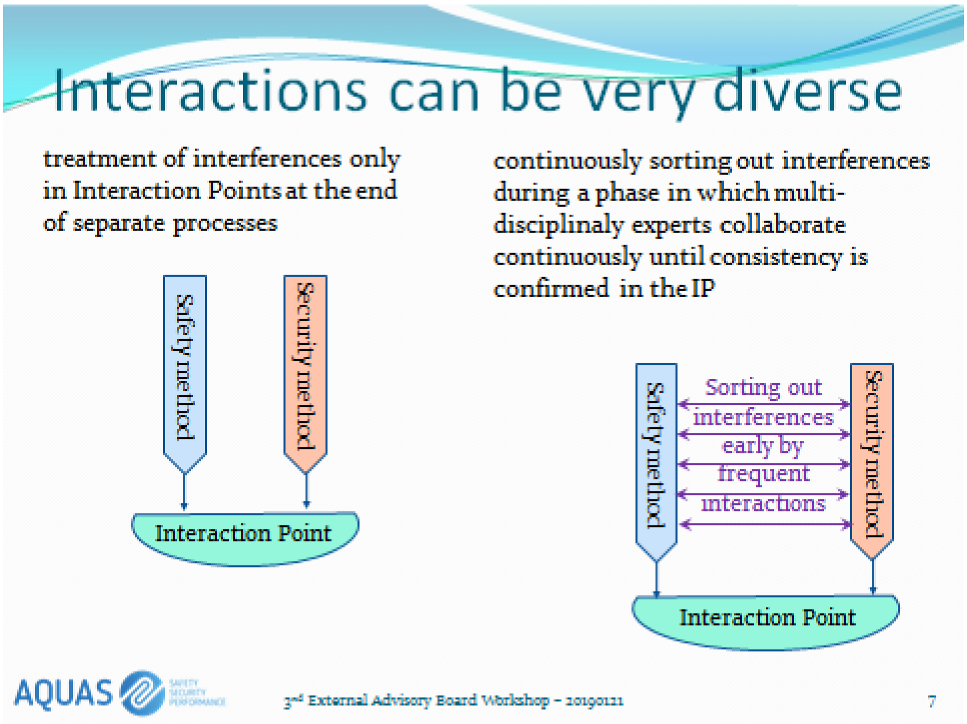
Supporting relationship.

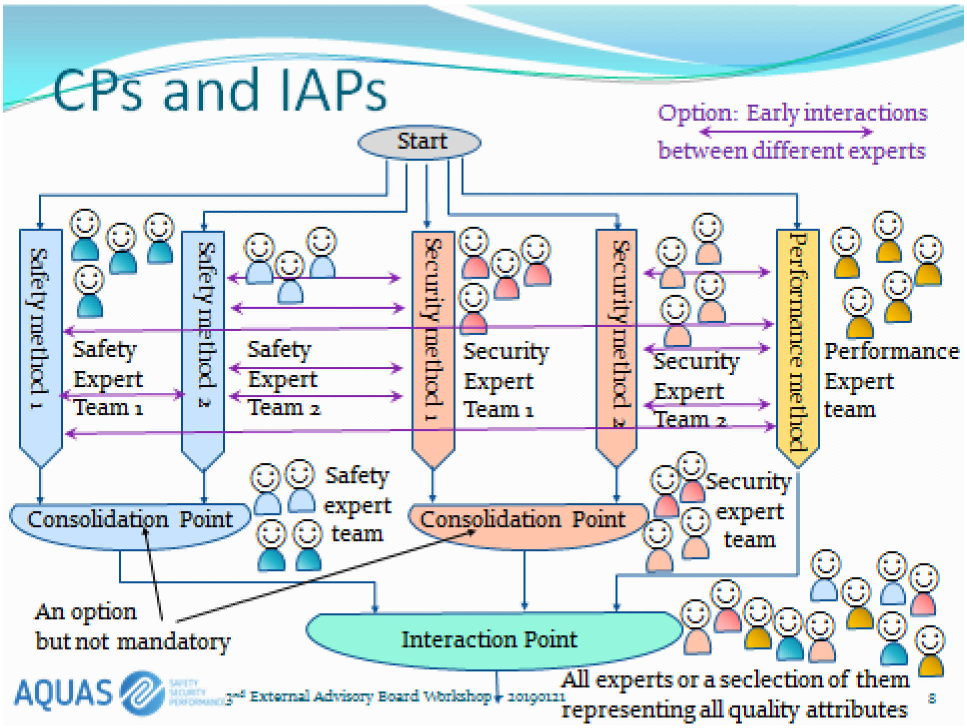
- Assurance measure of attribute A is also applicable to assurance of attribute B => one assurance measure can be used to replace two separate ones.
- E.g., encryption can be used for both confidentiality (security) and to check data integrity instead of checksum (safety).
  => This means two goals can be addressed by one argumentation.

AQUAS SAFETY SECURITY PERFORMANCE 3rd External Advisory Board Workshop – 20190121 4


Co-engineering
Affects basically all lifecycle phases
Two choices:
Separate processes handled with separate tools (WP3.1)
Combined processes and tools (WP3.2)
Separate processes need alignment of results
Detect and remove mutual contradictions in iterations
= Interaction points (see dedicated presentation later)
Co-engineering in the interaction point covers wide scope:
Review session or discussion between experts
Formalized interaction of combined analysis supported by tools
Combined methods&tools („integrated phase“) contain the interactions within themselves
AQUAS
3rd External Advisory Board Workshop – 20190121
5


Process structures can be very diverse
From lightweight interaction processes for smaller projects to ridgidly defined complex process structures
Examples:
Medical case study
-> One common HAZOP in the concept phase analyzing the system w.r.t safety and security (same set of guidewords but quality aspect specific parameters)
Industrial drive case study
-> several different safety, security, and performance analysis methods whose results must be aligned
First consolidation of interferences between methods targeting the same quality attribute in a „consolidation point“
Then treating consolidated intermediate results in an „Interaction Point“
AQUAS
3rd External Advisory Board Workshop – 20190121
6


Interactions can be very diverse
treatment of interferences only in Interaction Points at the end of separate processes
continuously sorting out interferences during a phase in which multi-disciplinaly experts collaborate continuously until consistency is confirmed in the IP
Safety method
Security method
Interaction Point
Safety method
Sorting out interferences early by frequent interactions
Security method
Interaction Point
AQUAS
3rd External Advisory Board Workshop – 20190121
7


CPs and IAPs
Option: Early interactions between different experts
Start
Safety method 1
Safety Expert Team 1
Safety method 2
Safety Expert Team 2
Security method 1
Security Expert Team 1
Security method 2
Security Expert Team 2
Performance method
Performance Expert team
Consolidation Point
Safety expert team
Consolidation Point
Security expert team
An option but not mandatory
Interaction Point
All experts or a seclection of them representing all quality attributes
AQUAS
3rd External Advisory Board Workshop – 20190121
8

Interaction Point (IP) and Interferences

- First concrete approach developed in CS4 (Industrial Drive – with complex processes)
- IPs typically occur between lifecycle phases or activities but it depends on domain and project specific parameters.
- IP treats the potential mutual influences („interferences") of atomic, aspect related phase or activity results
  - Example: the influence between one security and one performance related requirement derived during (parallel) security and performance analyses.
  - Consequence: High overall number of interferences

$$n_{Intererences} = n_{SecurityRequirements} * n_{PerformanceRequirements}$$

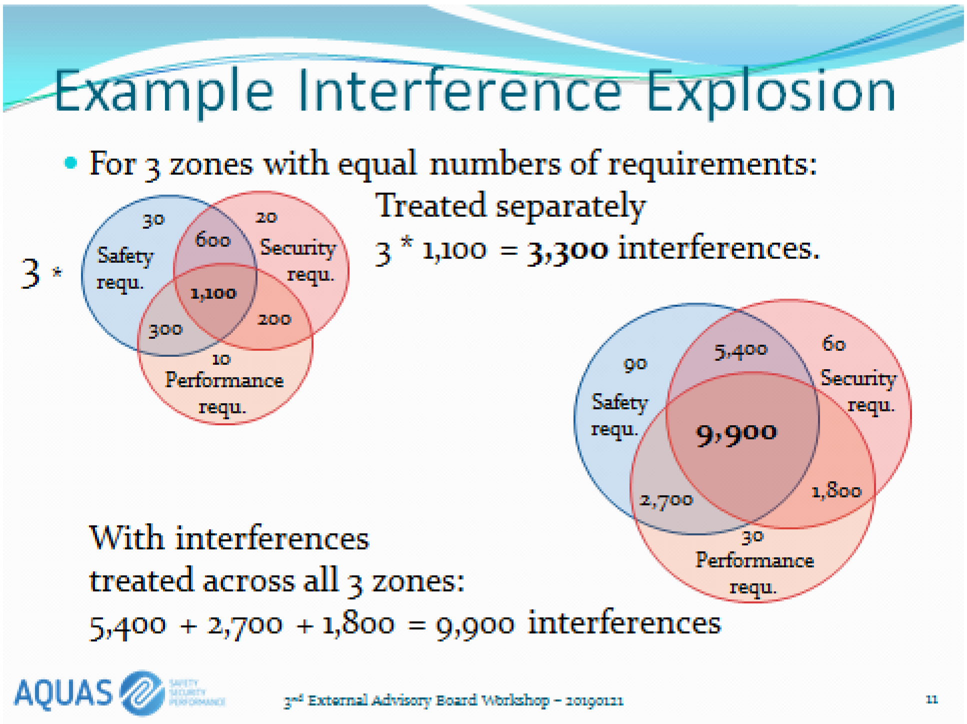
„**Interference explosion**" → >>1,000

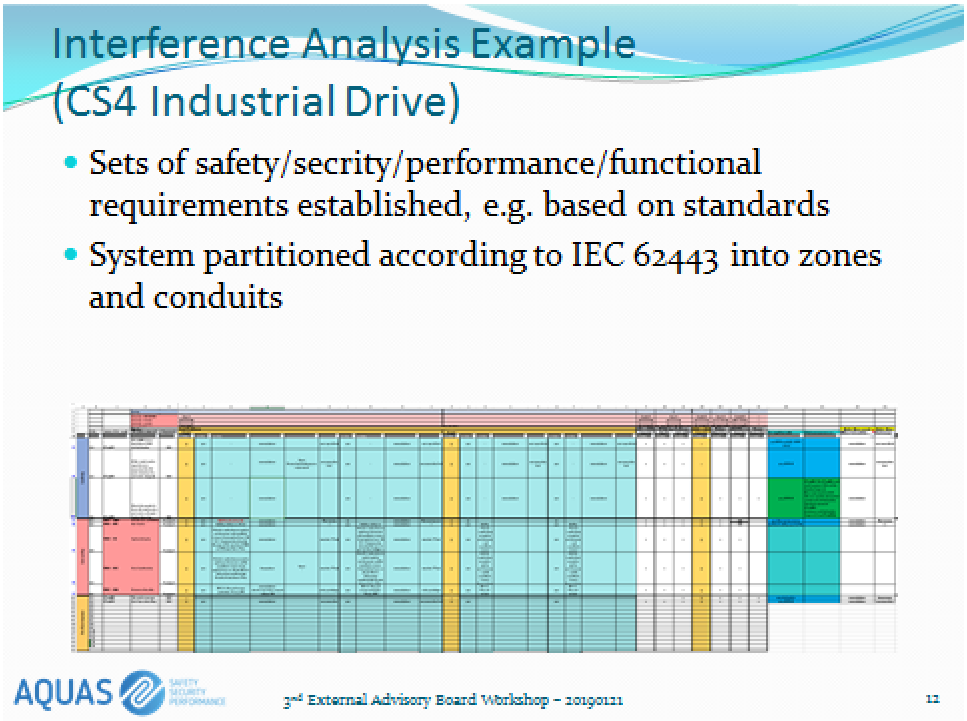
AQUAS 3rd External Advisory Board Workshop – 20190121 9

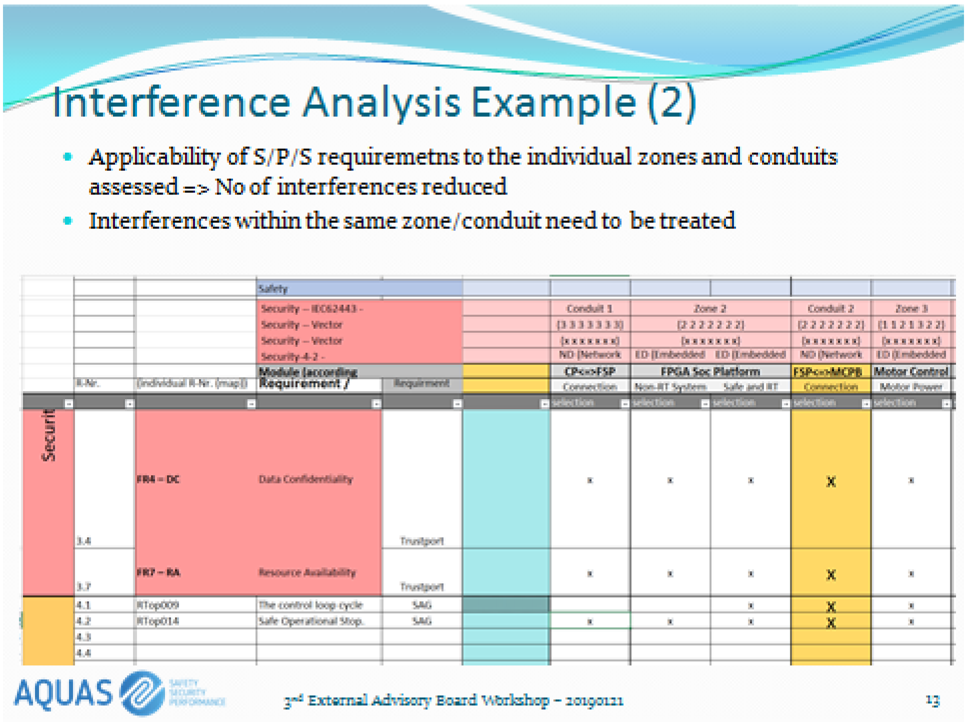
Solution for Interference Explosion

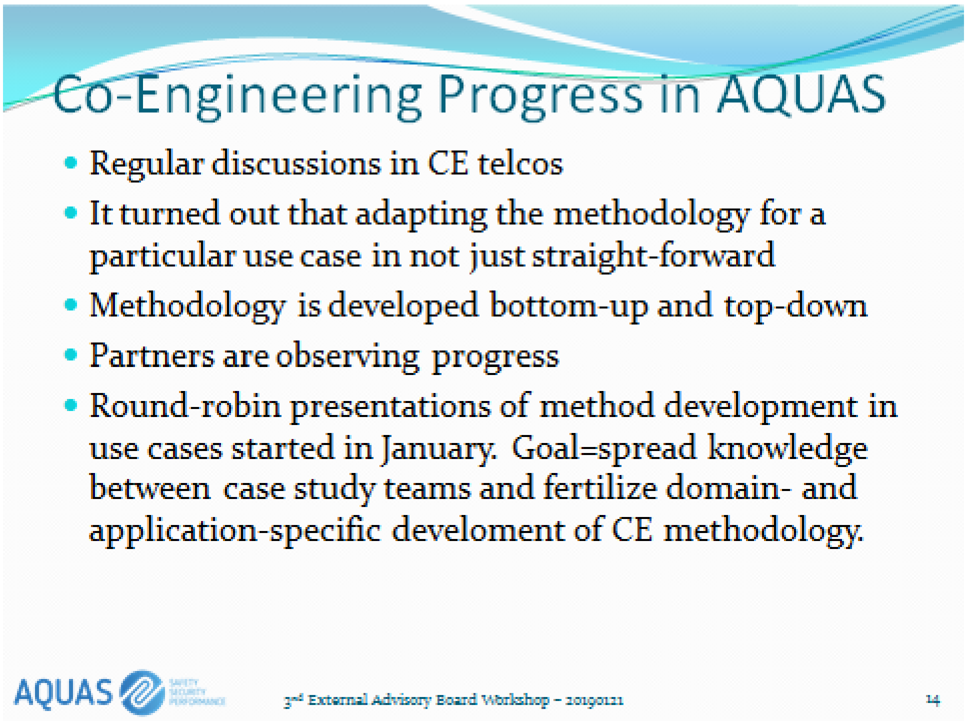
- Not all potential interferences can come into effect:
- System is partitioned into disjoint units and communication channels between them
- HW and SW requirements are usually independent of each other
- E.g. CS4 Industrial Drive: Partners applied IEC 62443 and partitioned the system into zones and conduits
- Each zone and each conduit analyzed separately.
- Assign requirements to groups:
  - Consider pairs of requirements only within one zone or within one conduit
  - Exclude influence between HW and SW requirements
- But important: Also functional requirements play a role.
- Another effort reducing factor: **Early interactions**

AQUAS 3rd External Advisory Board Workshop – 20190121 10

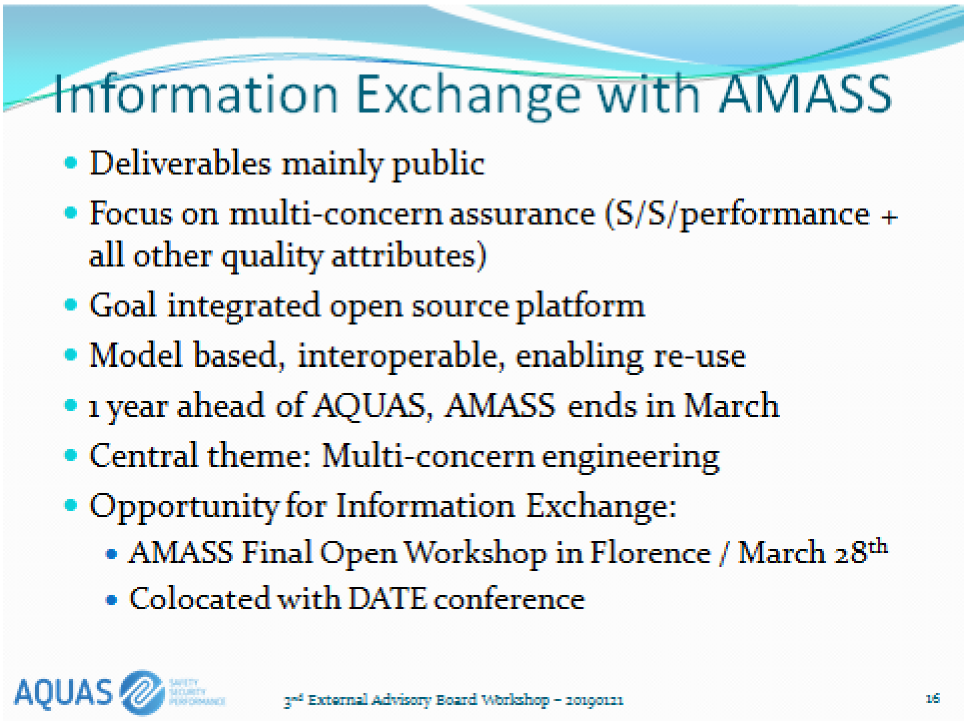

Example Interference Explosion
For 3 zones with equal numbers of requirements:
Treated separately
3 * 1,100 = 3,300 interferences.
3 *
30
600
20
Safety requ.
Security requ.
1,100
300
200
10
Performance requ.
90
5,400
60
Safety requ.
Security requ.
9,900
2,700
1,800
30
Performance requ.
With interferences
treated across all 3 zones:
5,400 + 2,700 + 1,800 = 9,900 interferences
AQUAS
3rd External Advisory Board Workshop – 20190121
11

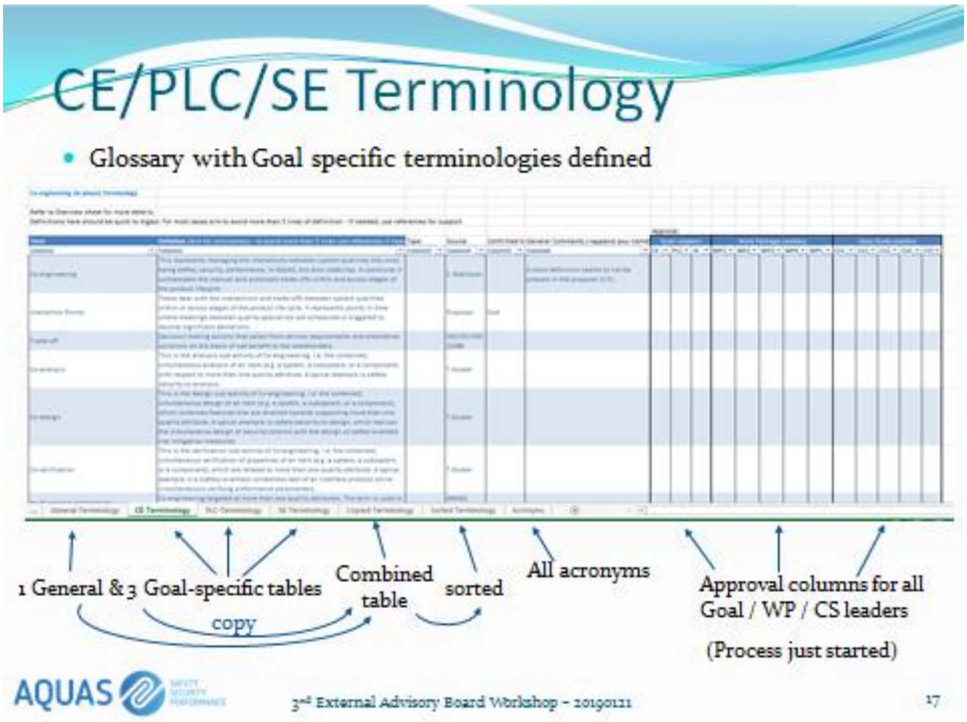

Interference Analysis Example
(CS4 Industrial Drive)
Sets of safety/secrity/performance/functional requirements established, e.g. based on standards
System partitioned according to IEC 62443 into zones and conduits
AQUAS
3rd External Advisory Board Workshop – 20190121
12

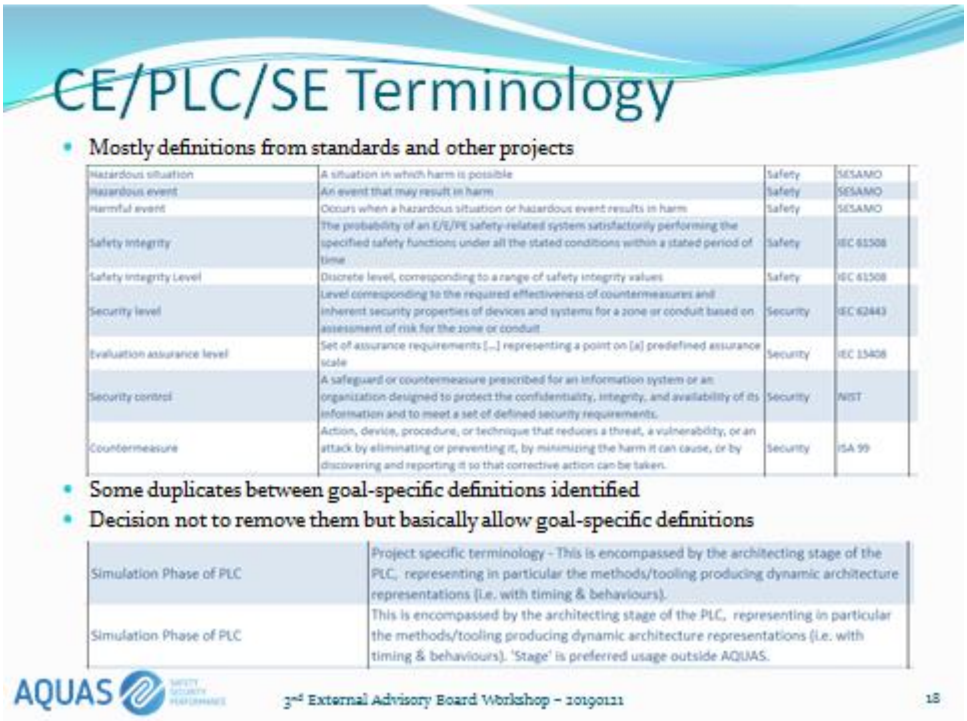

Interference Analysis Example (2)
Applicability of S/P/S requiremetns to the individual zones and conduits assessed => No of interferences reduced
Interferences within the same zone/conduit need to be treated
Safety
Conduit 1
Zone 2
Conduit 2
Zone 3
CP<=>FSP
FPGA Soc Platform
FSP<=>MCPB
Motor Control
FR4 – DC
Data Confidentiality
Trustport
FR7 – RA
Resource Availability
RTop009
The control loop cycle
RTop014
Safe Operational Stop.
SAG
AQUAS
3rd External Advisory Board Workshop – 20190121
13


Co-Engineering Progress in AQUAS
Regular discussions in CE telcos
It turned out that adapting the methodology for a particular use case in not just straight-forward
Methodology is developed bottom-up and top-down
Partners are observing progress
Round-robin presentations of method development in use cases started in January. Goal=spread knowledge between case study teams and fertilize domain- and application-specific develoment of CE methodology.
AQUAS
3rd External Advisory Board Workshop – 20190121
14


CE Developments in Standardization
tbs
AQUAS
3rd External Advisory Board Workshop – 20190121
15


Information Exchange with AMASS
Deliverables mainly public
Focus on multi-concern assurance (S/S/performance + all other quality attributes)
Goal integrated open source platform
Model based, interoperable, enabling re-use
1 year ahead of AQUAS, AMASS ends in March
Central theme: Multi-concern engineering
Opportunity for Information Exchange:
AMASS Final Open Workshop in Florence / March 28th
Colocated with DATE conference
AQUAS
3rd External Advisory Board Workshop – 20190121
16


CE/PLC/SE Terminology
Glossary with Goal specific terminologies defined
1 General & 3 Goal-specific tables
copy
Combined table
sorted
All acronyms
Approval columns for all Goal / WP / CS leaders
(Process just started)
AQUAS
3rd External Advisory Board Workshop – 20190121
17


CE/PLC/SE Terminology
Mostly definitions from standards and other projects
Hazardous situation | A situation in which harm is possible | Safety | SESAMO
Hazardous event | An event that may result in harm | Safety | SESAMO
Harmful event | Occurs when a hazardous situation or hazardous event results in harm | Safety | SESAMO
Safety integrity | The probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time | Safety | IEC 61508
Safety integrity Level | Discrete level, corresponding to a range of safety integrity values | Safety | IEC 61508
Security level | Level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit | Security | IEC 62443
Evaluation assurance level | Set of assurance requirements [...] representing a point on [a] predefined assurance scale | Security | IEC 15408
Security control | A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. | Security | NIST
Countermeasure | Action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. | Security | ISA 99
Some duplicates between goal-specific definitions identified
Decision not to remove them but basically allow goal-specific definitions
Simulation Phase of PLC | Project specific terminology - This is encompassed by the architecting stage of the PLC, representing in particular the methods/tooling producing dynamic architecture representations (i.e. with timing & behaviours).
Simulation Phase of PLC | This is encompassed by the architecting stage of the PLC, representing in particular the methods/tooling producing dynamic architecture representations (i.e. with timing & behaviours). 'Stage' is preferred usage outside AQUAS.
AQUAS
3rd External Advisory Board Workshop – 20190121
18

CE/PLC/SE Terminology

- Review of all terms initiated
  → goal-, work package-, case study-leaders invited to approve or comment
- Process is currently ongoing
- Result will finally be included in D3.2 .

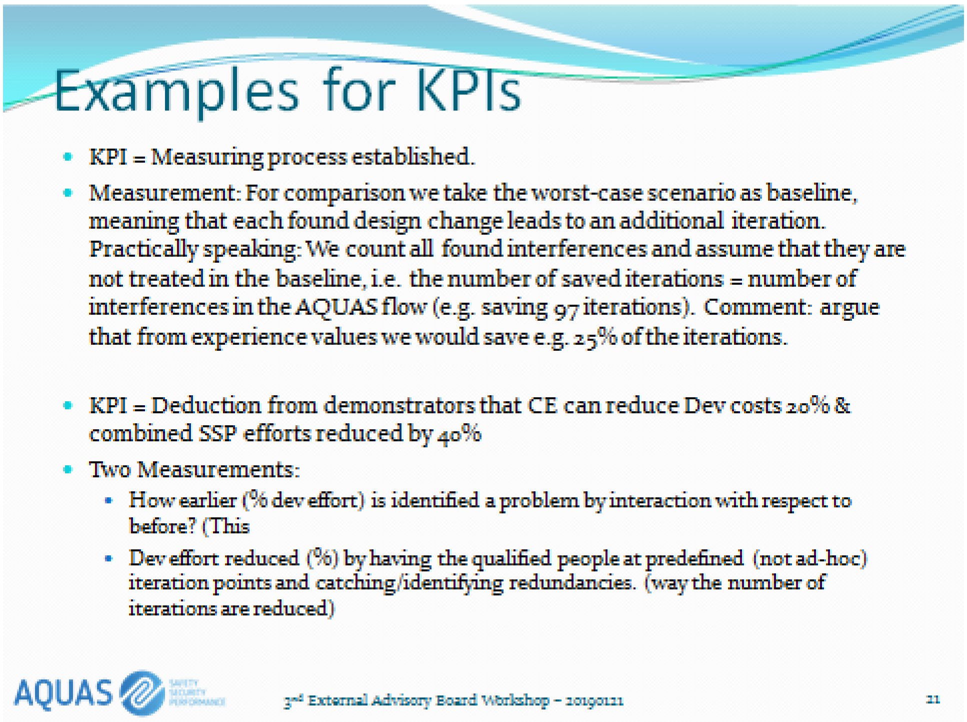
AQUAS SAFETY SECURITY PERFORMANCE 3rd External Advisory Board Workshop – 20190121 19

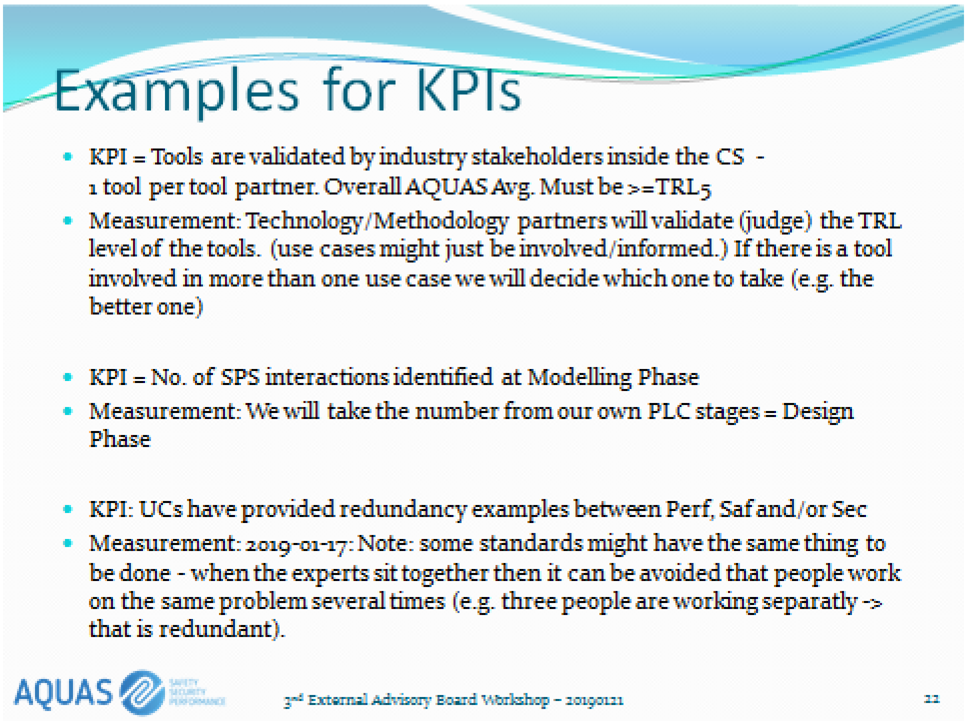
Key Performance Indicators

- Draft of KPIs per goal (CE/PLC/SE) provided
- Some cannot clearly be assigned to only one goal, respective interferences were discused and clarified
- Details about whether the KPIs can be reasonbly measured are discussed with the case study teams
- up to now improvements achieved in particular in CS4.
- Further case study discussions ongoing
- It is often difficult to establish a reasonable interpretation how we will measure the KPI
- On the following slides some examples

O2	Measuring process established.	Avg. no. of tradeoff meetings for Modelling Phase	Estimated no. of SPS tradeoffs for Modelling Stage with updated process and tools (tradeoffs = treated (.i.e solved, provided guide for later phases, resolved (verified that the compromise taken is realized as intended before))
ATM			
Medical			
Rail Carriage Mechanisms			
Industrial Drive	For comparison we take the worst-case scenario as baseline, meaning that each found design change leads to an additional iteration. Practically speaking: We count all found interferences and assume that they are not treated in the baseline, i.e. the number of saved iterations = number of interferences in the AQUAS flow (e.g. saving 97 iterations). Comment: argue that from experience values we would save e.g. 20% of the iterations.	Why only the simulation/modeling phases? (we also trade-off in the concept phase). Practically: We will take the #trade-off meetings that we would have needed in the SESAMO flow (generic baseline PLC)	UC4 Design Phase #trade-off-meetings with the new tools/methods (AQUAS flow)
Space			

AQUAS SAFETY SECURITY PERFORMANCE 3rd External Advisory Board Workshop – 20190121 20


Examples for KPIs
KPI = Measuring process established.
Measurement: For comparison we take the worst-case scenario as baseline, meaning that each found design change leads to an additional iteration. Practically speaking: We count all found interferences and assume that they are not treated in the baseline, i.e. the number of saved iterations = number of interferences in the AQUAS flow (e.g. saving 97 iterations). Comment: argue that from experience values we would save e.g. 25% of the iterations.
KPI = Deduction from demonstrators that CE can reduce Dev costs 20% & combined SSP efforts reduced by 40%
Two Measurements:
How earlier (% dev effort) is identified a problem by interaction with respect to before? (This
Dev effort reduced (%) by having the qualified people at predefined (not ad-hoc) iteration points and catching/identifying redundancies. (way the number of iterations are reduced)
AQUAS
3rd External Advisory Board Workshop – 20190121
21


Examples for KPIs
KPI = Tools are validated by industry stakeholders inside the CS - 1 tool per tool partner. Overall AQUAS Avg. Must be >=TRL5
Measurement: Technology/Methodology partners will validate (judge) the TRL level of the tools. (use cases might just be involved/informed.) If there is a tool involved in more than one use case we will decide which one to take (e.g. the better one)
KPI = No. of SPS interactions identified at Modelling Phase
Measurement: We will take the number from our own PLC stages = Design Phase
KPI: UCs have provided redundancy examples between Perf, Saf and/or Sec
Measurement: 2019-01-17: Note: some standards might have the same thing to be done - when the experts sit together then it can be avoided that people work on the same problem several times (e.g. three people are working separatly -> that is redundant).
AQUAS
3rd External Advisory Board Workshop – 20190121
22

CE Dissemination and Exploitation

- Safecomp Publication on Co-Engineering in the Loop
- Journal paper on AQUAS methodology in preparation
- Link to standardization groups ongoing to spread the methodology in industry
- Information exchange with AMASS („Multiconcern engineering“)

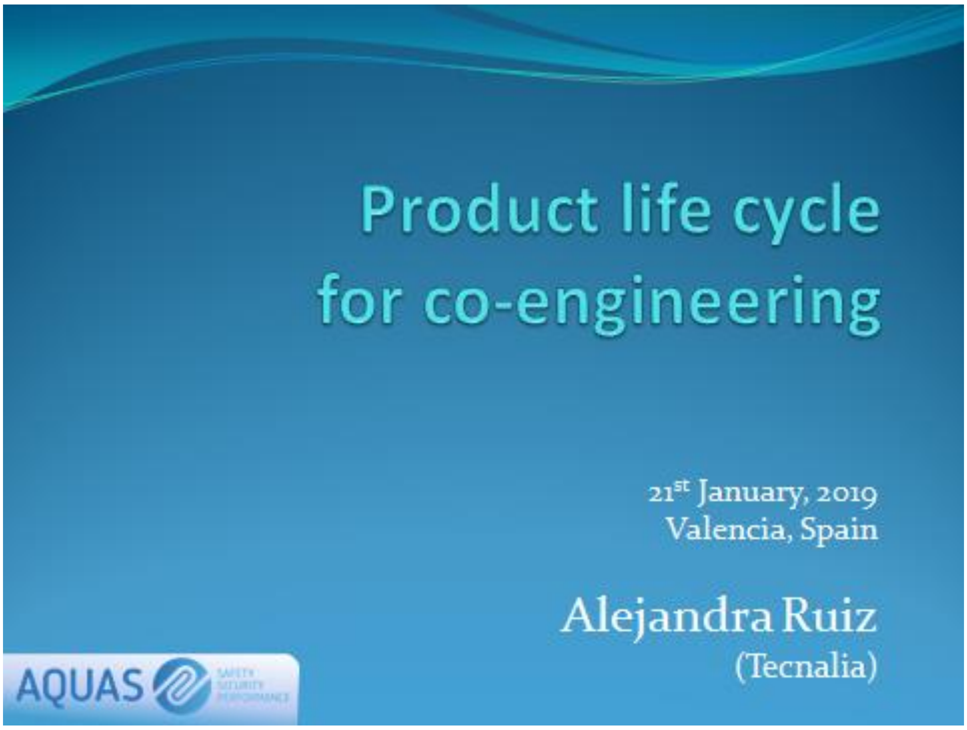
AQUAS 3rd External Advisory Board Workshop – 20190121 23

Conclusions

- Realization of Co-engineering and Interaction Point approach in use cases ongoing.
- Very diverse process structures in case studies.
- High number of interactions is an important topic.
- Terminology discussed and consolidation initiated.
- Key Performance Indicators definitions are ongoing.

AQUAS 3rd External Advisory Board Workshop – 20190121 24

2.2.14 Across the Product Lifecycle Stages



Product life cycle

- (an overview of AQUAS Use Cases diversity)

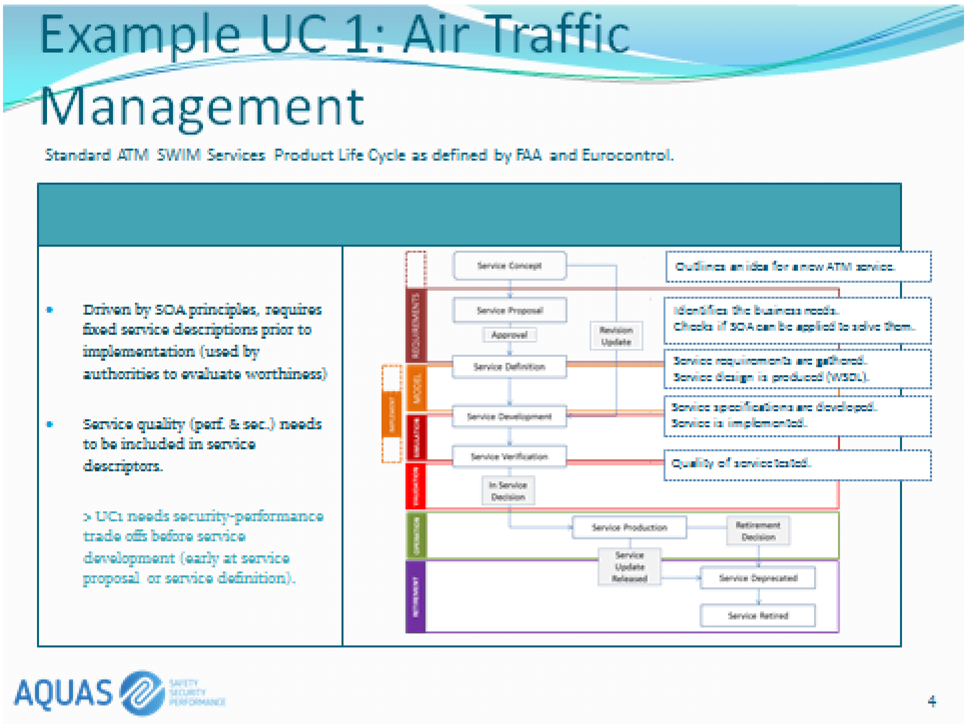
AQUAS 2

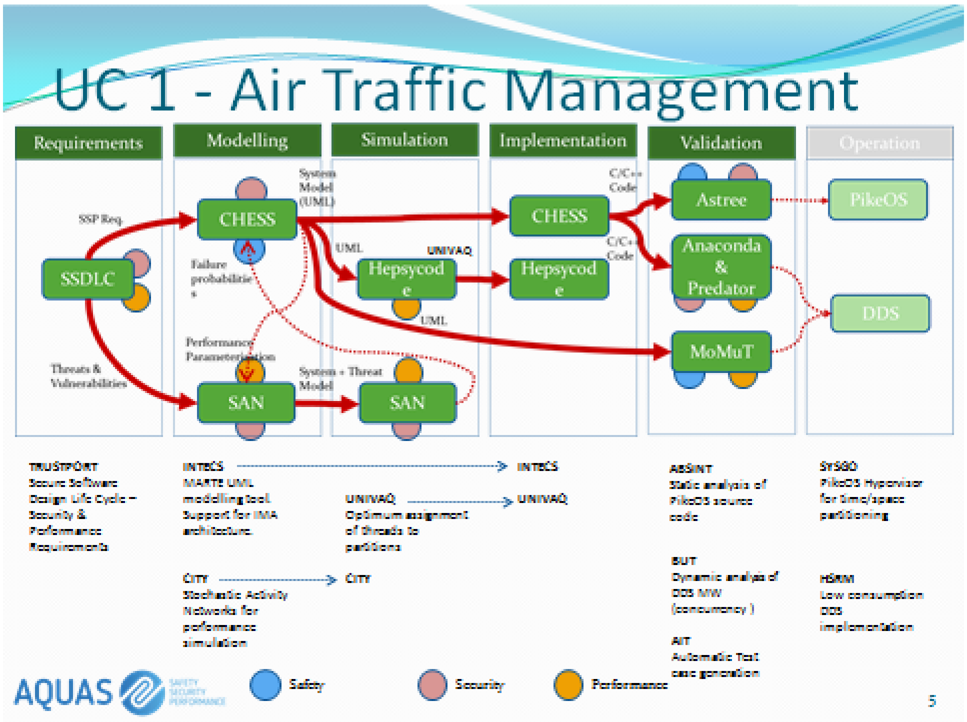
Product life cycle for co-engineering

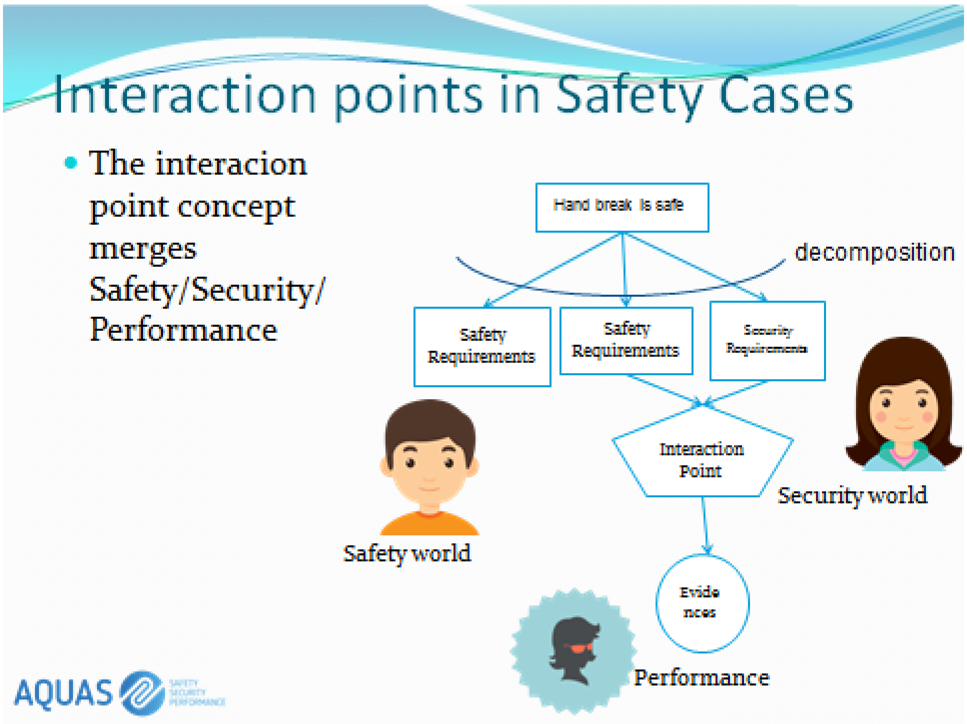
- Use cases: Diversity of **PLC** standards

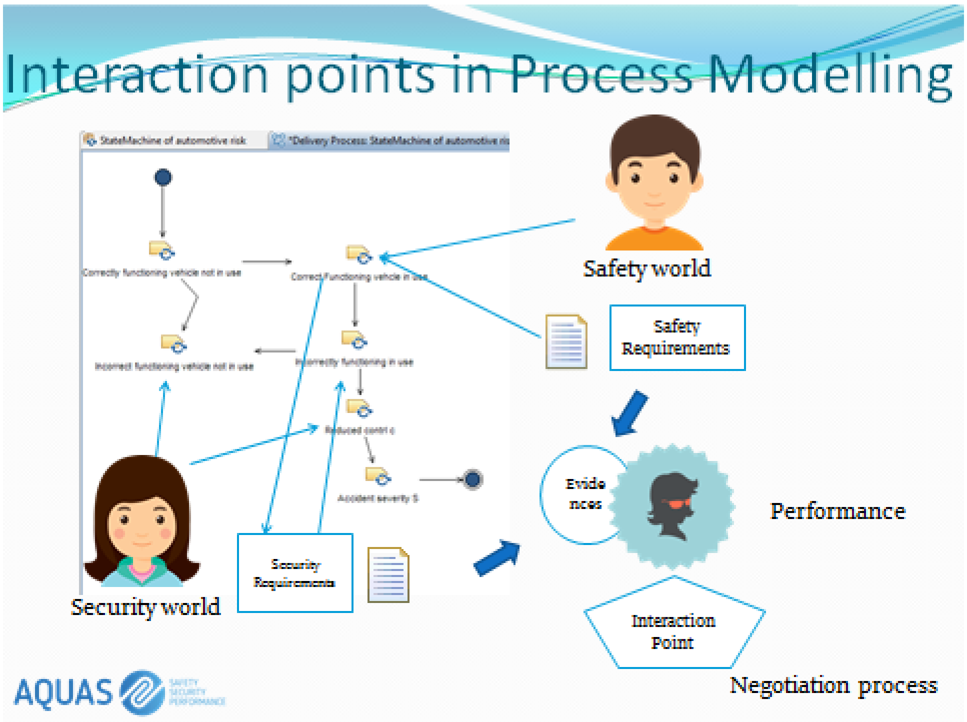
UC1 Air Traffic Management	UC2 Medical	UC3 Railway	UC4 Industrial	UC5 Space
ATM SWIM Services Product Life Cycle (Federal Aviation Administration (US) and Eurocontrol)	IEC 62304:2006 Medical device software life cycle processes	Domain independent generic Process Model derived from SESAMO Project Aligned to IEC 61508	Domain independent generic Process Model derived from SESAMO Project Aligned to IEC 61508	ECSS-E40 Space Software Engineering ECSS-Q80 Space Product Assurance

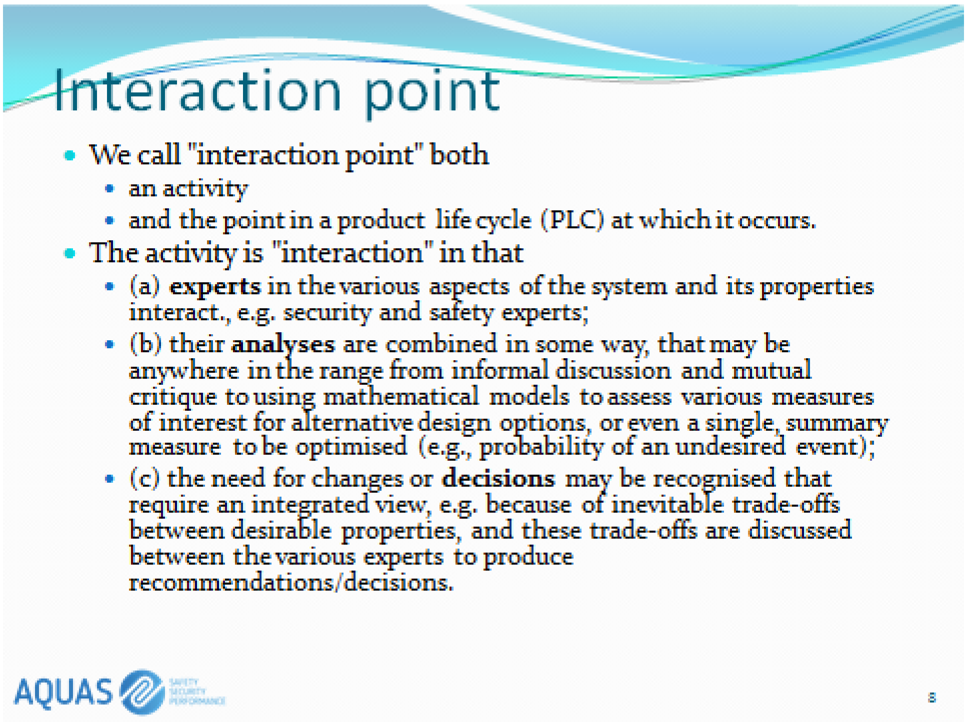
AQUAS 3

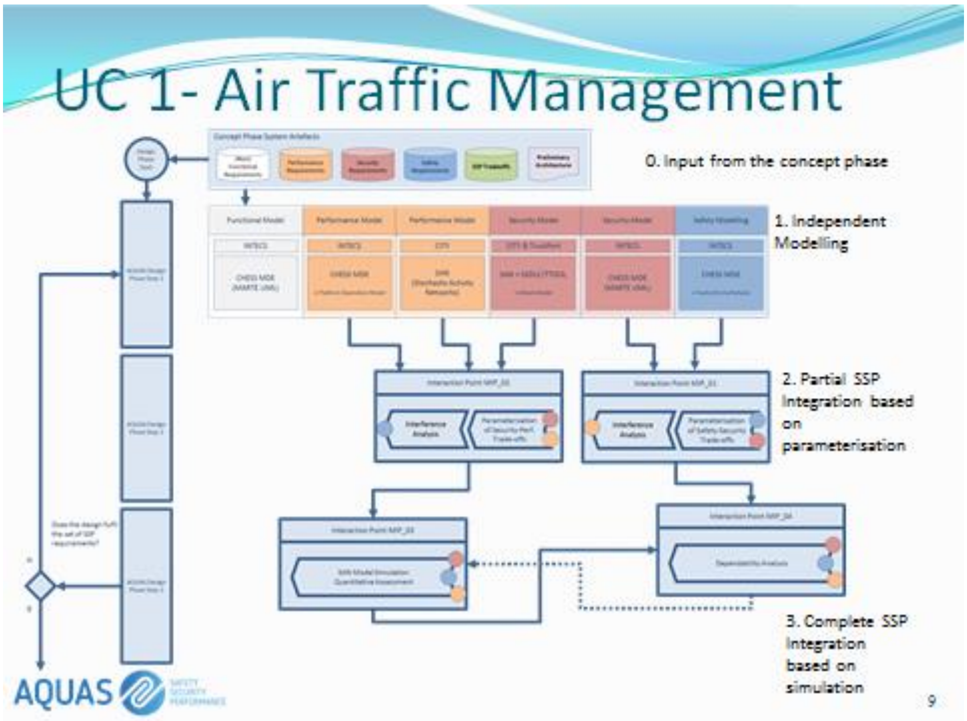

Example UC 1: Air Traffic Management
Standard ATM SWIM Services Product Life Cycle as defined by FAA and Eurocontrol.
Driven by SOA principles, requires fixed service descriptions prior to implementation (used by authorities to evaluate worthiness)
Service quality (perf. & sec.) needs to be included in service descriptors.
> UC1 needs security-performance trade offs before service development (early at service proposal or service definition).
Service Concept
Service Proposal
Approval
Revision Update
Service Definition
Service Development
Service Verification
In Service Decision
Service Production
Retirement Decision
Service Update Released
Service Deprecated
Service Retired
Outlines an idea for a new ATM service.
Identifies the business needs.
Checks if SOA can be applied to solve them.
Service requirements are gathered.
Service design is produced (WSDL).
Service specifications are developed.
Service is implemented.
Quality of service tested.
AQUAS
4

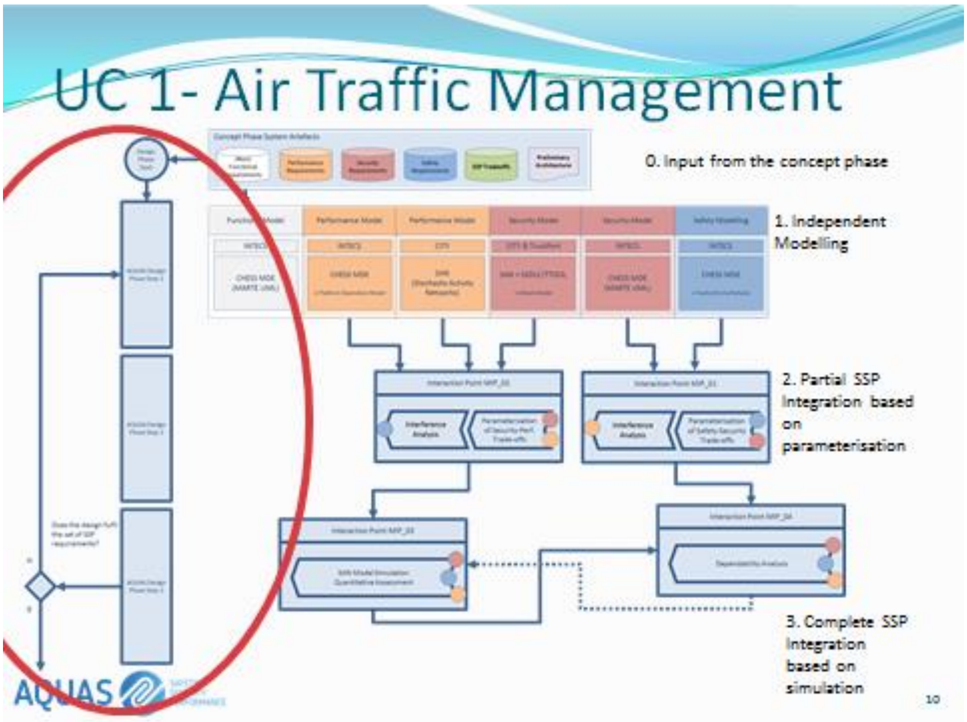

UC 1 - Air Traffic Management
Requirements
Modelling
Simulation
Implementation
Validation
Operation
SSP Req.
SSDLC
Threats & Vulnerabilities
CHESS
System Model (UML)
Failure probabilities
Performance Parameterisation
SAN
UML
UNIVAQ
Hepsycode
System + Threat Model
C/C++ Code
Astree
Anaconda & Predator
MoMuT
PikeOS
DDS
TRUSTPORT
Secure Software Design Life Cycle – Security & Performance Requirements
INTECS
MARTE UML modelling tool. Support for IMA architecture.
INTECS
UNIVAQ
Optimum assignment of threads to partitions
UNIVAQ
CITY
Stochastic Activity Networks for performance simulation
CITY
ABSINT
Static analysis of PikeOS source code
BUT
Dynamic analysis of DDS MW (concurrency)
AIT
Automatic Test case generation
SYSGO
PikeOS Hypervisor for time/space partitioning
HSRM
Low consumption DDS implementation
AQUAS
Safety
Security
Performance
5

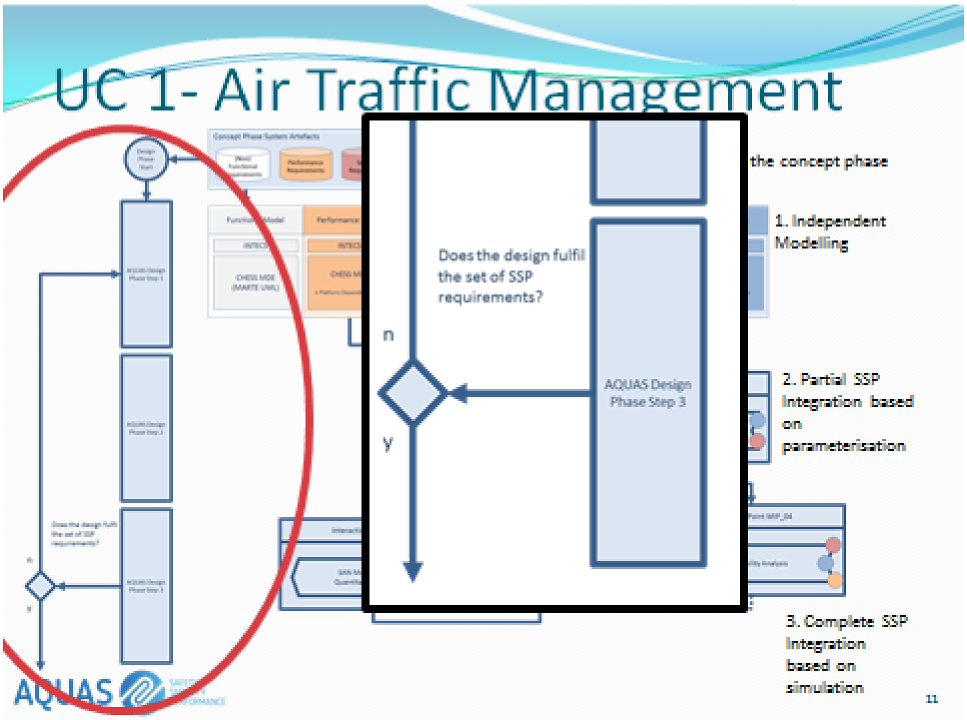

Interaction points in Safety Cases
The interacion point concept merges Safety/Security/ Performance
Hand break is safe
decomposition
Safety Requirements
Safety Requirements
Security Requirements
Interaction Point
Safety world
Security world
Evide nces
Performance
AQUAS

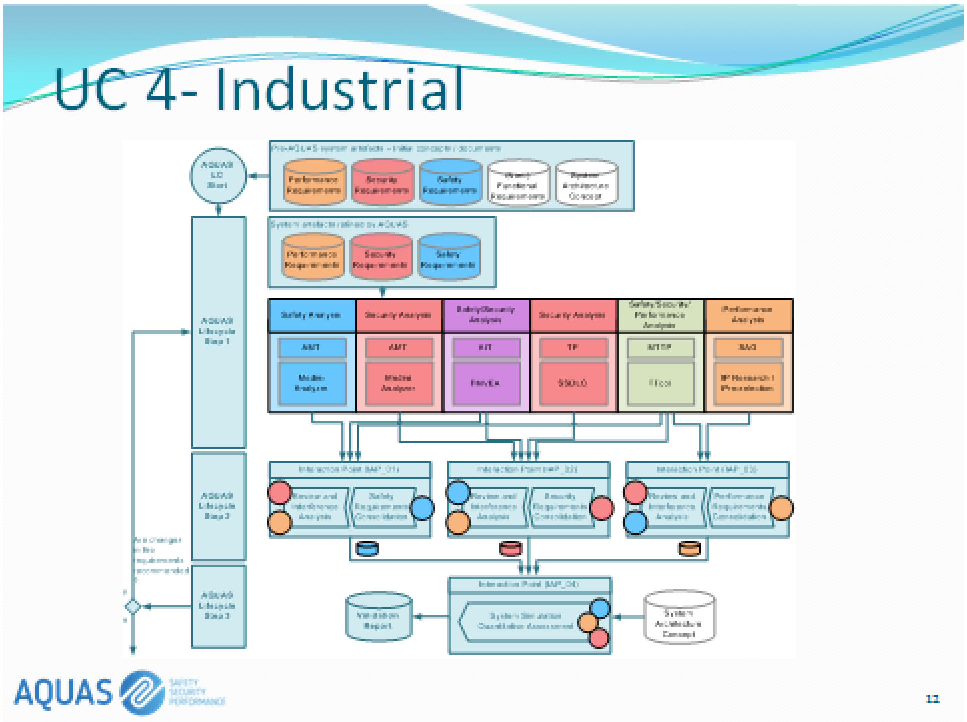

Interaction points in Process Modelling
Safety world
Safety Requirements
Security world
Security Requirements
Evide nces
Performance
Interaction Point
Negotiation process
AQUAS

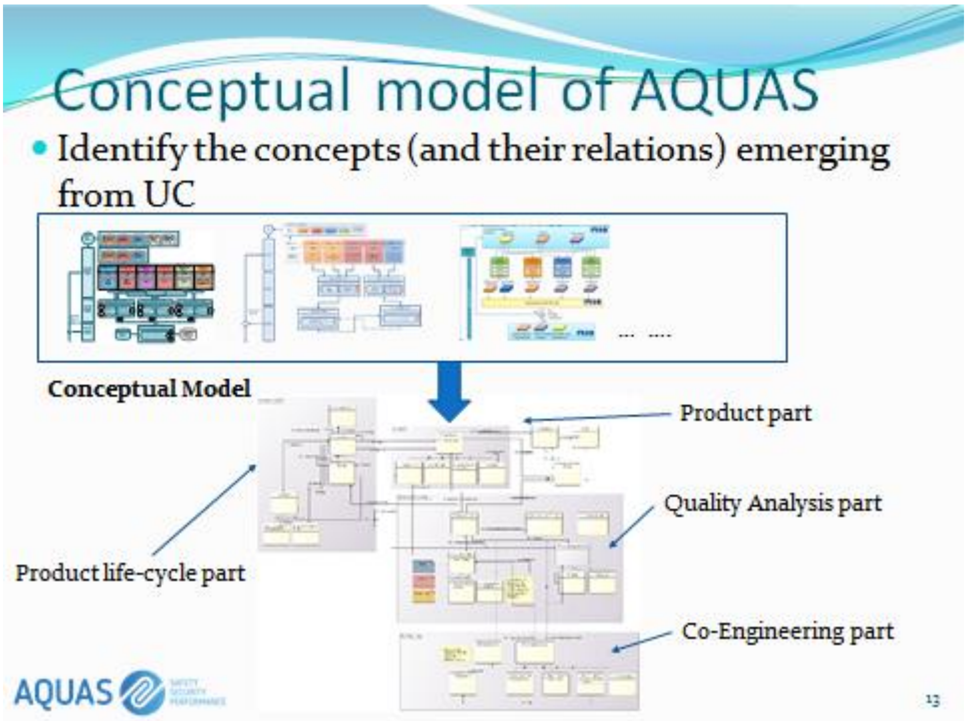

Interaction point
We call "interaction point" both
an activity
and the point in a product life cycle (PLC) at which it occurs.
The activity is "interaction" in that
(a) **experts** in the various aspects of the system and its properties interact., e.g. security and safety experts;
(b) their **analyses** are combined in some way, that may be anywhere in the range from informal discussion and mutual critique to using mathematical models to assess various measures of interest for alternative design options, or even a single, summary measure to be optimised (e.g., probability of an undesired event);
(c) the need for changes or **decisions** may be recognised that require an integrated view, e.g. because of inevitable trade-offs between desirable properties, and these trade-offs are discussed between the various experts to produce recommendations/decisions.
AQUAS
8

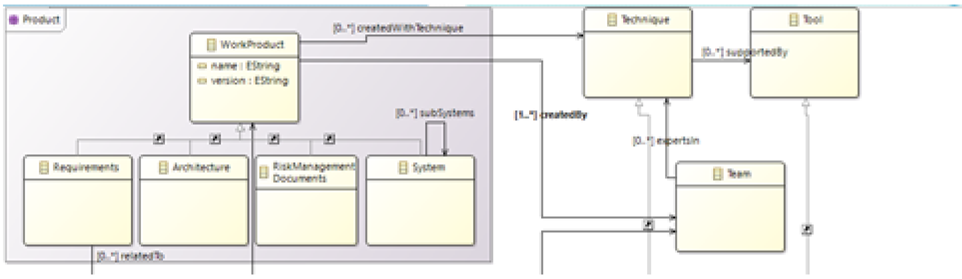

UC 1- Air Traffic Management
0. Input from the concept phase
1. Independent Modelling
2. Partial SSP Integration based on parameterisation
3. Complete SSP Integration based on simulation
AQUAS
9

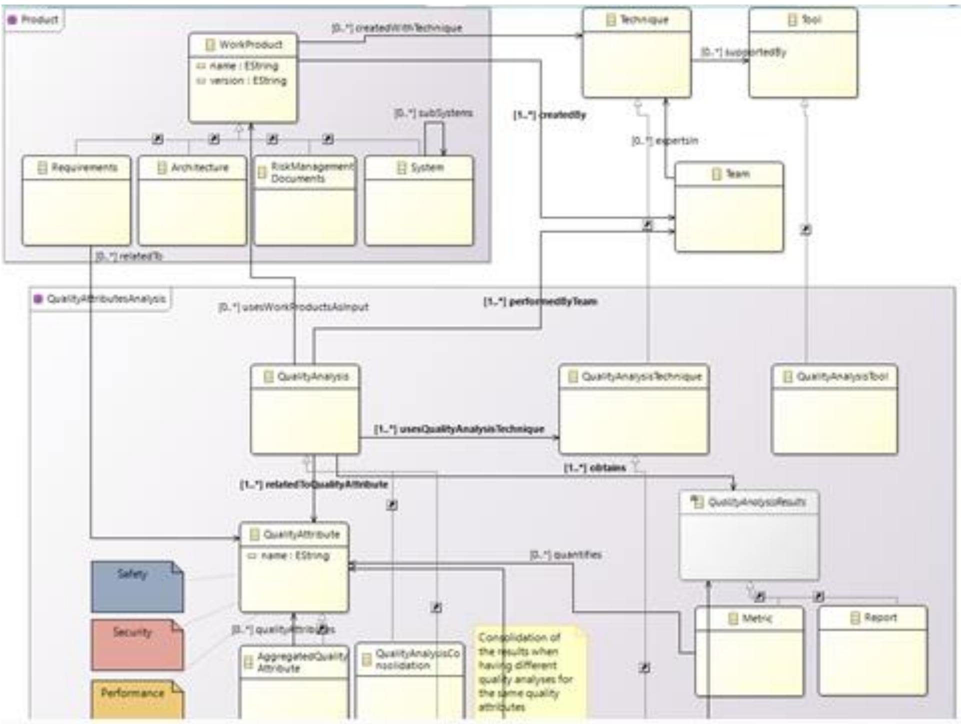

UC 1- Air Traffic Management
0. Input from the concept phase
1. Independent Modelling
2. Partial SSP Integration based on parameterisation
3. Complete SSP Integration based on simulation
AQUAS
10

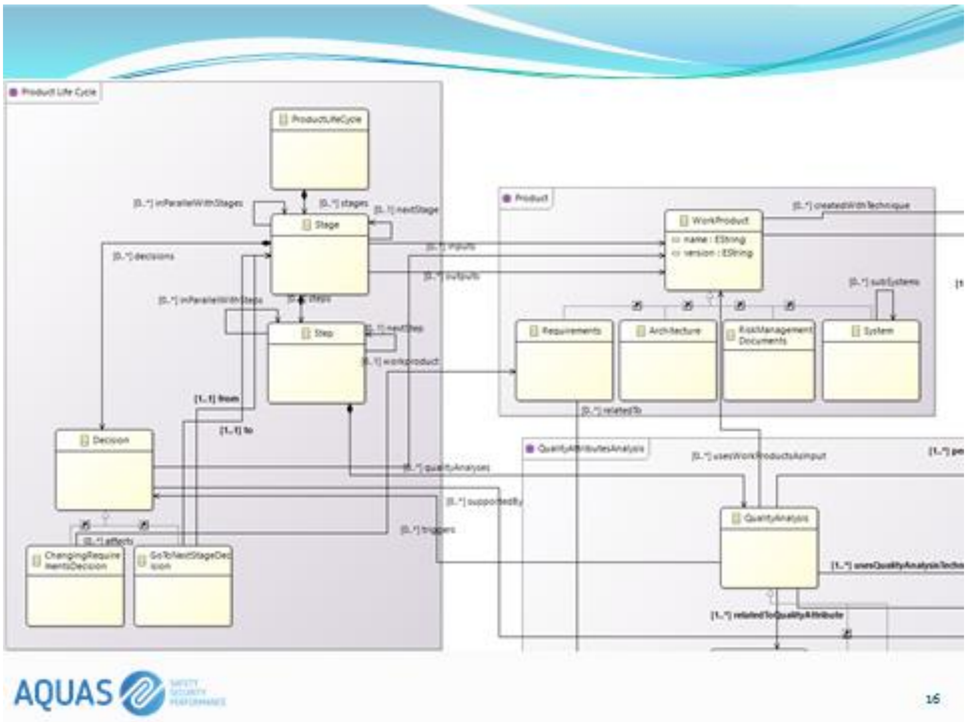

UC 1- Air Traffic Management
the concept phase
1. Independent Modelling
2. Partial SSP Integration based on parameterisation
3. Complete SSP Integration based on simulation
Does the design fulfil the set of SSP requirements?
n
y
AQUAS Design Phase Step 3
AQUAS
11

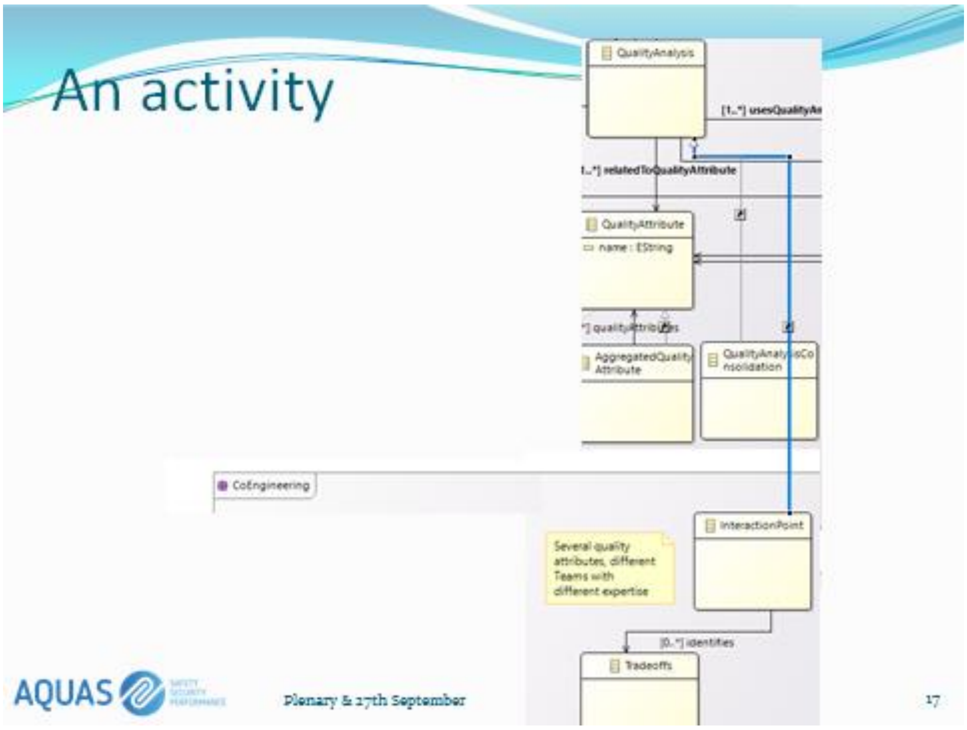

UC 4- Industrial
AQUAS
12

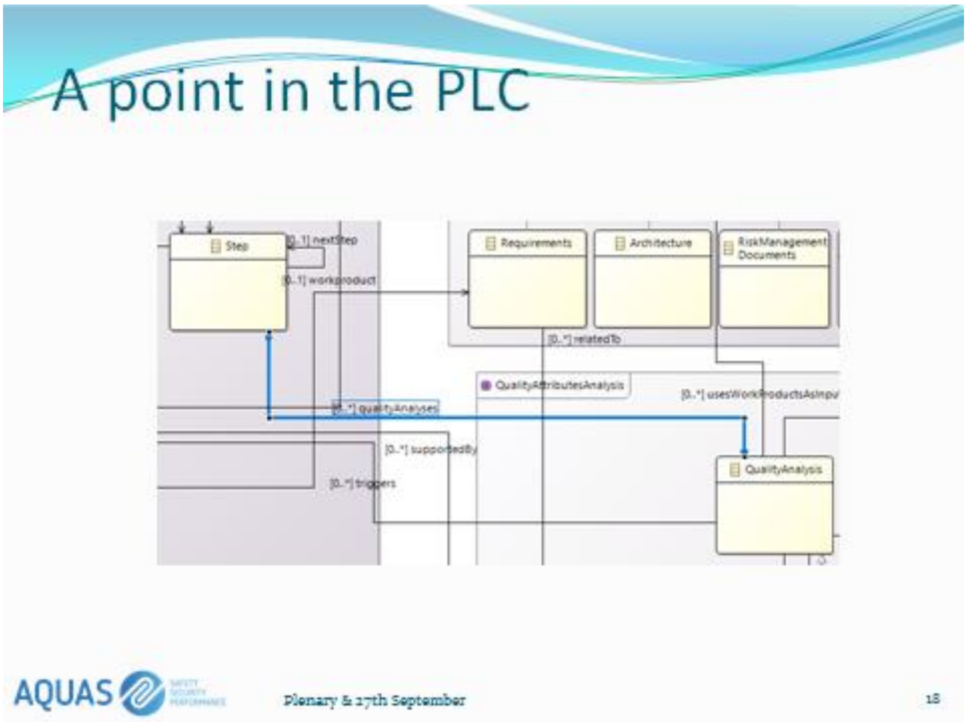

Conceptual model of AQUAS
Identify the concepts (and their relations) emerging from UC
Conceptual Model
Product part
Quality Analysis part
Product life-cycle part
Co-Engineering part
AQUAS
13

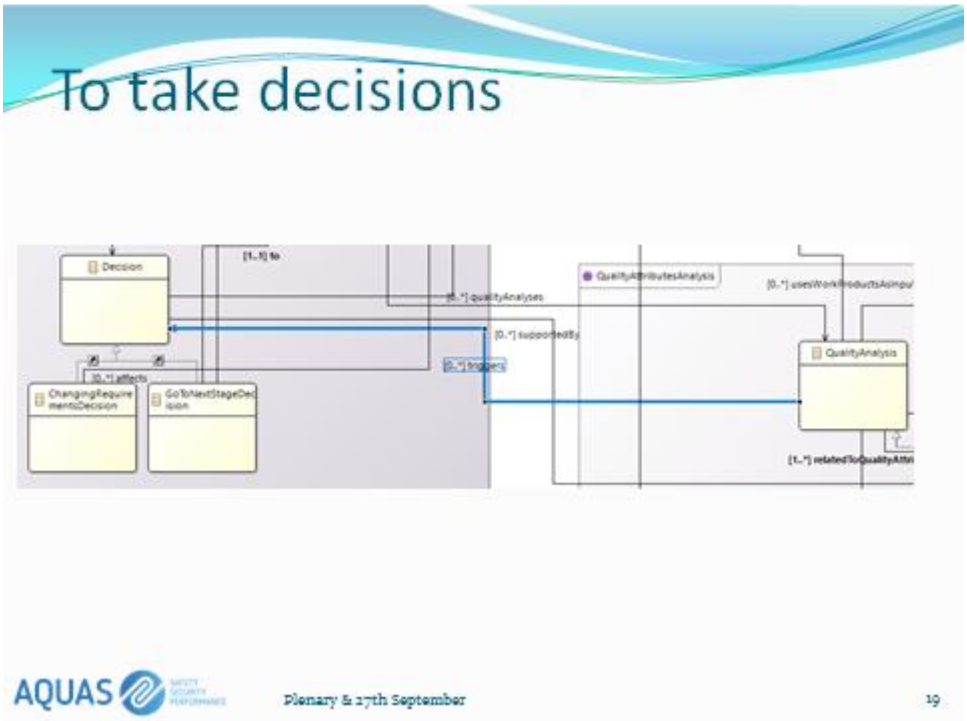

Product
WorkProduct
name : EString
version : EString
[0..*] createdWithTechnique
Technique
Tool
[0..*] supportedBy
[1..*] createdBy
[0..*] subSystems
[0..*] expertsIn
Team
Requirements
Architecture
RiskManagement Documents
System
[0..*] relatedTo

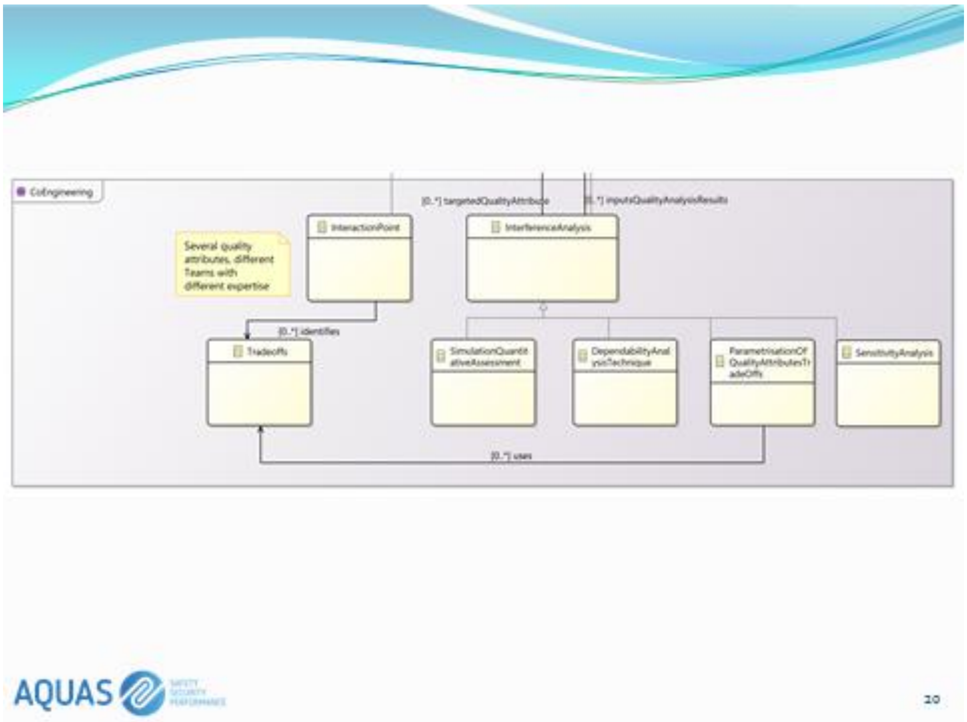

Product
WorkProduct
name : EString
version : EString
[0..*] createdWithTechnique
Technique
Tool
[0..*] supportedBy
[1..*] createdBy
[0..*] subSystems
[0..*] expertsIn
Team
Requirements
Architecture
RiskManagement Documents
System
[0..*] relatedTo
QualityAttributesAnalysis
[0..*] usesWorkProductsAsInput
[1..*] performedByTeam
QualityAnalysis
QualityAnalysisTechnique
QualityAnalysisTool
[1..*] usesQualityAnalysisTechnique
[1..*] obtains
[1..*] relatedToQualityAttribute
QualityAnalysisResults
QualityAttribute
name : EString
[0..*] quantifies
Safety
Security
Performance
[0..*] qualityAttributes
AggregatedQuality Attribute
QualityAnalysisConsolidation
Consolidation of the results when having different quality analyses for the same quality attributes
Metric
Report


Product Life Cycle
ProductLifeCycle
Stage
Step
Decision
Product
WorkProduct
Requirements
Architecture
System
QualityAnalysis
AQUAS
16


An activity
QualityAnalysis
[1..*] usesQualityAn
relatedToQualityAttribute
QualityAttribute
name : EString
AggregatedQualityAttribute
QualityAnalysisConsolidation
CoEngineering
InteractionPoint
Several quality attributes, different Teams with different expertise
[0..*] identifies
Tradeoffs
AQUAS
Plenary & 17th September
17


A point in the PLC
Step
[0..1] nextStep
[0..1] workproduct
Requirements
Architecture
RiskManagement Documents
[0..*] relatedTo
QualityAttributesAnalysis
[0..*] usesWorkProductsAsInput
[0..*] qualityAnalyses
[0..*] supportedBy
[0..*] triggers
QualityAnalysis
AQUAS
Plenary & 27th September
18

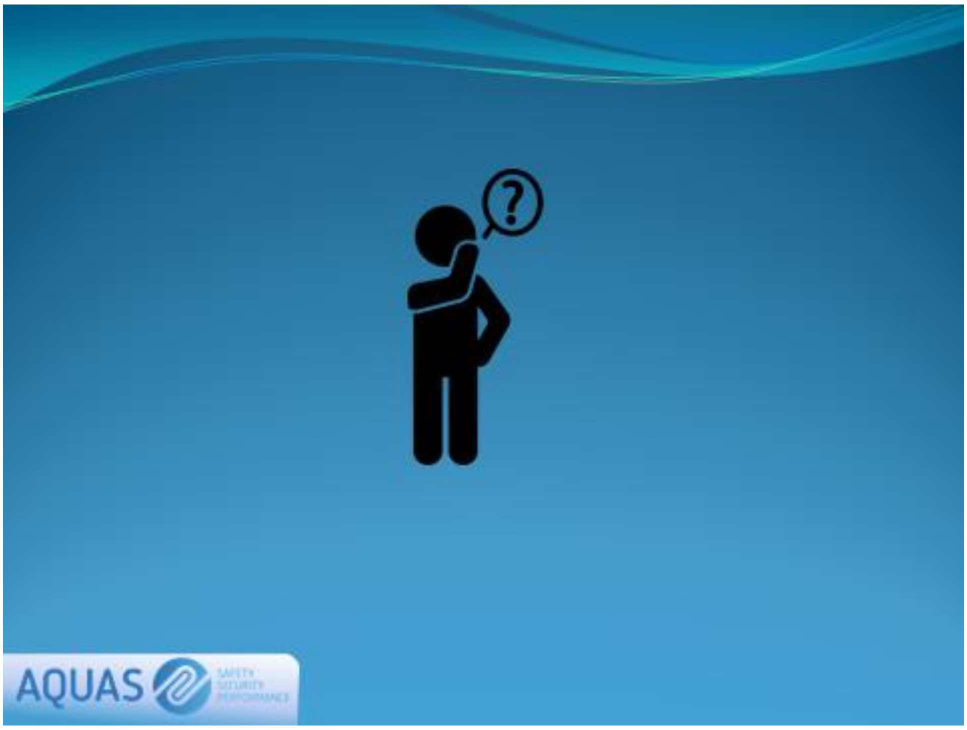

To take decisions
Decision
[1..1] to
[0..*] qualityAnalyses
QualityAttributesAnalysis
[0..*] usesWorkProductsAsInput
[0..*] supportedBy
[0..*] triggers
[0..*] affects
ChangingRequirementsDecision
GoToNextStageDecision
QualityAnalysis
AQUAS
Plenary & 27th September
19



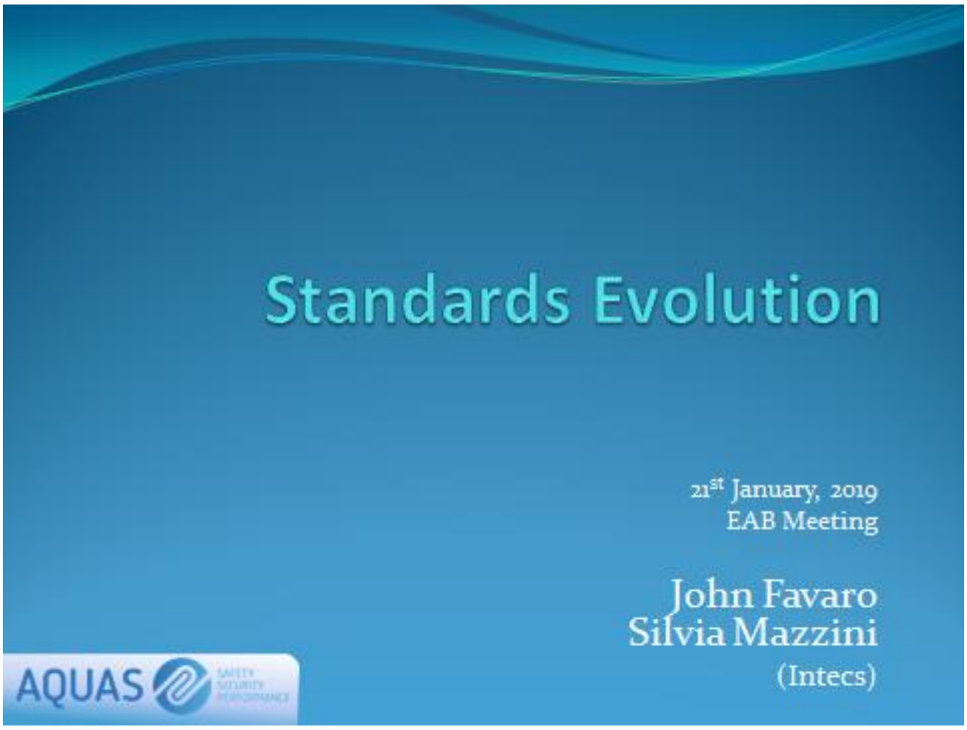
How to measure the improvements?

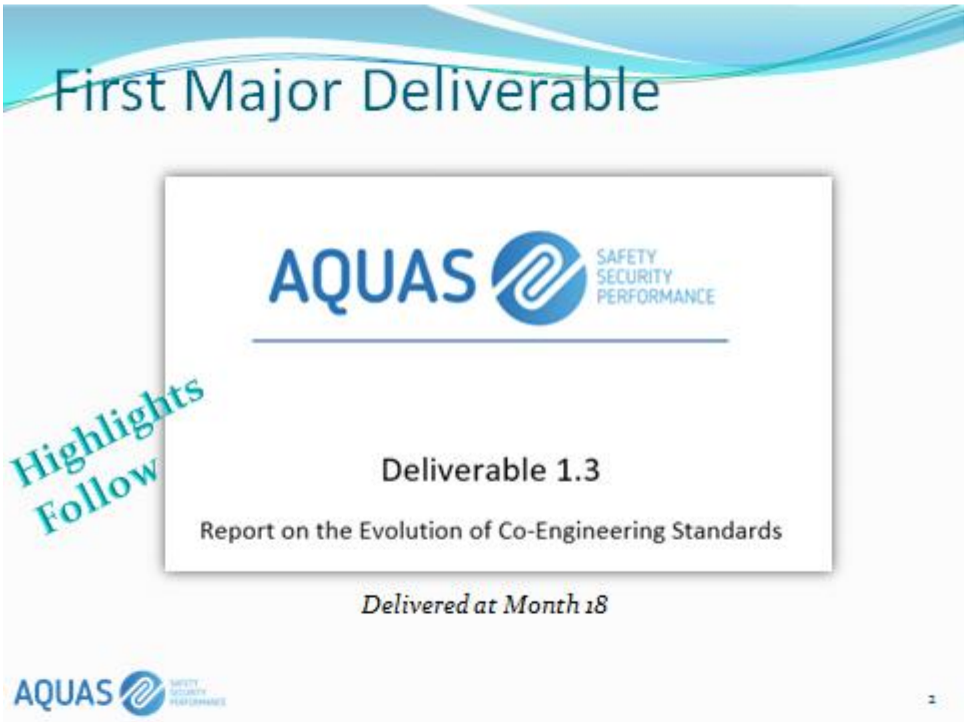
Concepts	Progress indicators
Traceability	Traceability between all phases established (inter-deps + Attributes)
Interaction between PLC phases.	Initial level of PSS-interaction data exchanged between phases Current level of PSS-interaction data exchanged between phases
Visibility for a stakeholder in a particular phase to see how changes impact other PLC phases	Visibility of which phase(s) to which other phases chosen Some impact visibility established. Specialist can see change impact from their phase to other phases.
Reduction of developments costs	From demonstrators developed, no./% redundancies, iterations, costs reduced. (r=x,i=y,c=z) How earlier is identified a problem by interaction with respect to before? (This way the number of iterations are reduced) (% dev effort) Dev effort reduced (%) by having the qualified people at predefined iteration points
TRL improvement	TRL assessments of tech by use cases completed (indicate average with assessment location as comment) Tools are used in CS which are industry relevant including real world problems

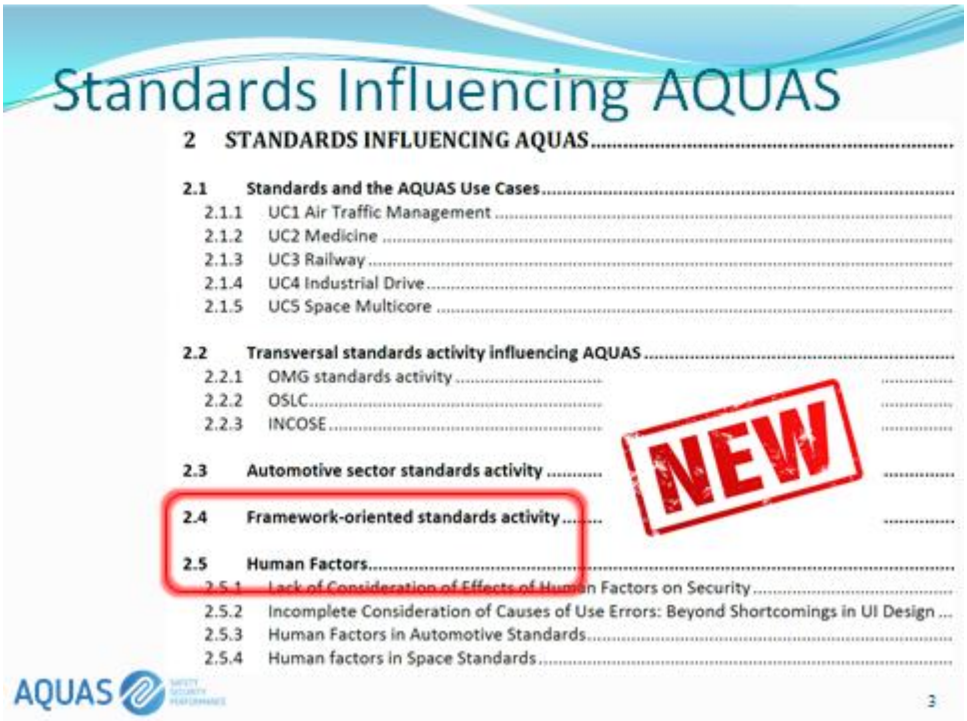
AQUAS 21

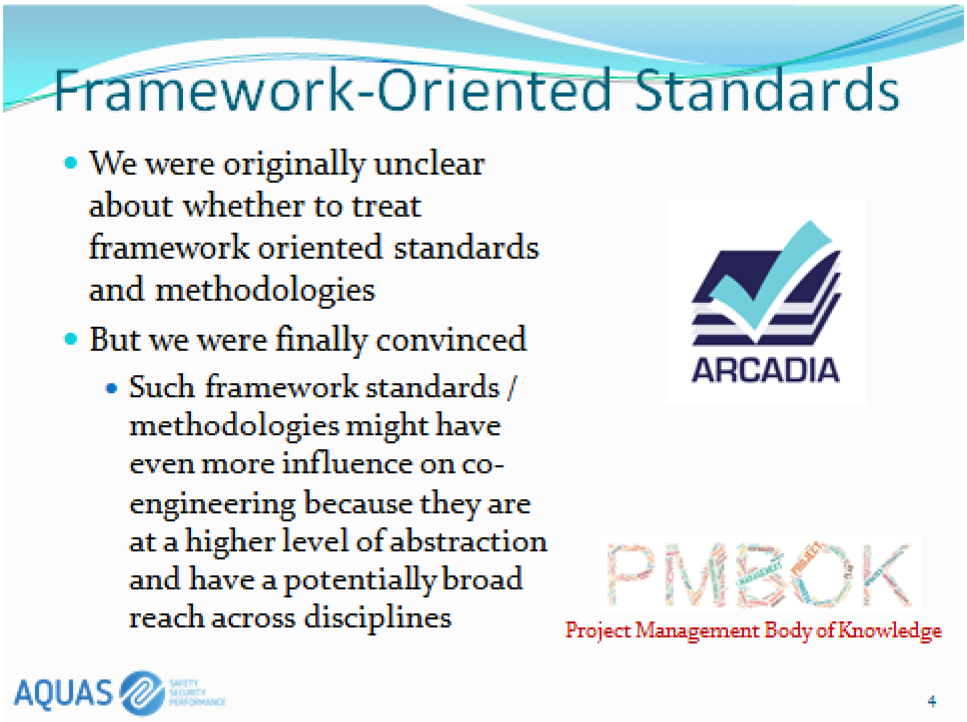


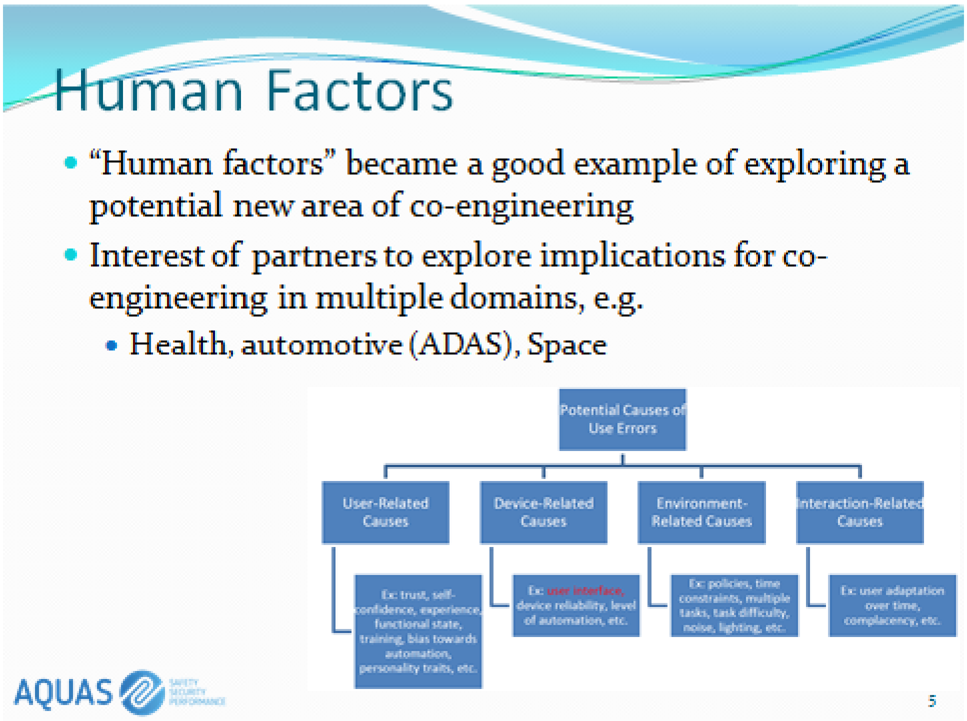
2.2.15 Standards Evolution

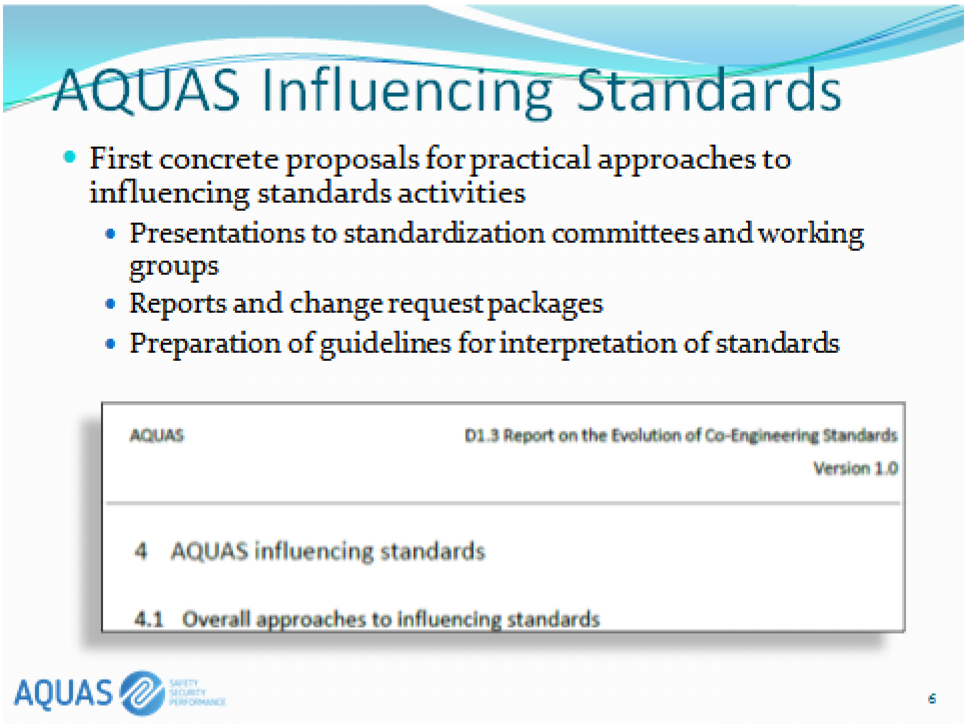


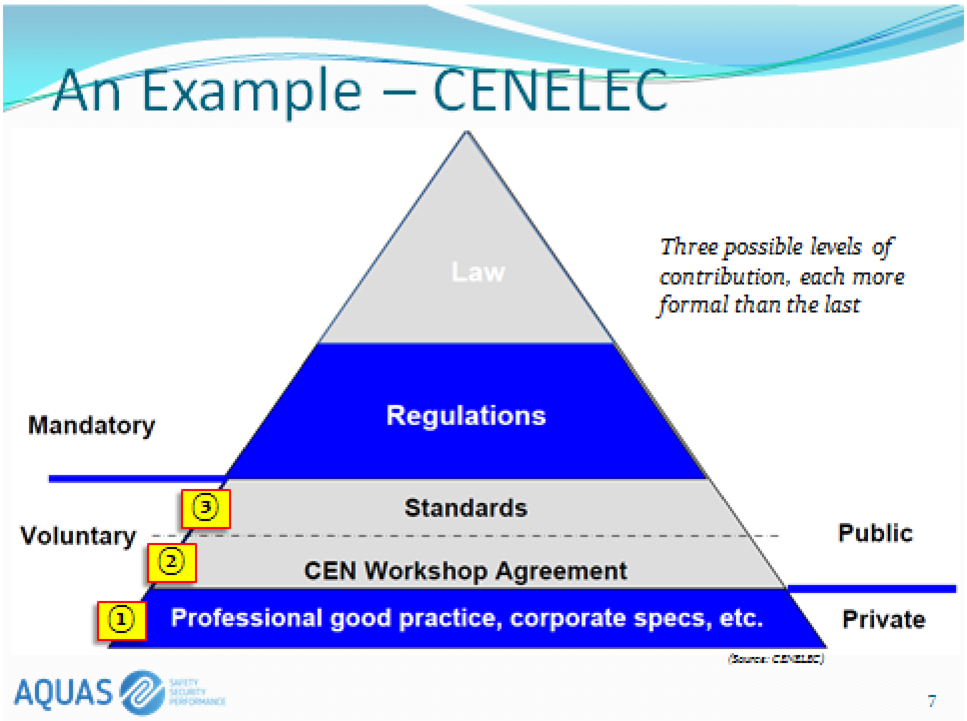

First Major Deliverable
AQUAS SAFETY SECURITY PERFORMANCE
Highlights Follow
Deliverable 1.3
Report on the Evolution of Co-Engineering Standards
Delivered at Month 18
AQUAS
2


Standards Influencing AQUAS
2 STANDARDS INFLUENCING AQUAS
2.1 Standards and the AQUAS Use Cases
2.1.1 UC1 Air Traffic Management
2.1.2 UC2 Medicine
2.1.3 UC3 Railway
2.1.4 UC4 Industrial Drive
2.1.5 UC5 Space Multicore
2.2 Transversal standards activity influencing AQUAS
2.2.1 OMG standards activity
2.2.2 OSLC
2.2.3 INCOSE
2.3 Automotive sector standards activity
2.4 Framework-oriented standards activity
2.5 Human Factors
2.5.1 Lack of Consideration of Effects of Human Factors on Security
2.5.2 Incomplete Consideration of Causes of Use Errors: Beyond Shortcomings in UI Design
2.5.3 Human Factors in Automotive Standards
2.5.4 Human factors in Space Standards
NEW
AQUAS
3


Framework-Oriented Standards
We were originally unclear about whether to treat framework oriented standards and methodologies
But we were finally convinced
Such framework standards / methodologies might have even more influence on co-engineering because they are at a higher level of abstraction and have a potentially broad reach across disciplines
ARCADIA
PMBOK
Project Management Body of Knowledge
AQUAS
4


Human Factors
"Human factors" became a good example of exploring a potential new area of co-engineering
Interest of partners to explore implications for co-engineering in multiple domains, e.g.
Health, automotive (ADAS), Space
Potential Causes of Use Errors
User-Related Causes
Device-Related Causes
Environment-Related Causes
Interaction-Related Causes
Ex: trust, self-confidence, experience, functional state, training, bias towards automation, personality traits, etc.
Ex: user interface, device reliability, level of automation, etc.
Ex: policies, time constraints, multiple tasks, task difficulty, noise, lighting, etc.
Ex: user adaptation over time, complacency, etc.
AQUAS
5


AQUAS Influencing Standards
First concrete proposals for practical approaches to influencing standards activities
Presentations to standardization committees and working groups
Reports and change request packages
Preparation of guidelines for interpretation of standards
AQUAS
D1.3 Report on the Evolution of Co-Engineering Standards
Version 1.0
4 AQUAS influencing standards
4.1 Overall approaches to influencing standards
AQUAS
6


An Example – CENELEC
Law
Three possible levels of contribution, each more formal than the last
Mandatory
Regulations
Standards
Voluntary
Public
CEN Workshop Agreement
Professional good practice, corporate specs, etc.
Private
(Source: CENELEC)
AQUAS
7

Ongoing Activities

- The Standards Evolution activities continue, including study of new areas for investigation
  - E.g. recent presentation and study of the **Variability Exchange Language** (VEL) as a potential enabler for exploration of alternative with respect to Safety-Security-Performance parameters
- Vocabulary / terminology harmonization efforts continue

OASIS
Nonprofit, global consortium for standards and open source projects

VEL
Variability Exchange Language (VEL)

AQUAS SAFETY SECURITY PERFORMANCE

8

Project-Level Progress Indicators

- **O9**: Contribute to the improvement of standards to address co-engineering, by submission of change requests to at least 1 standard for each of the AQUAS use case domains.
  - This may be addressed by preparing change request packages for potential consideration in new revision rounds of standards
- **O10**: To promote awareness and bring results of AQUAS into at least two international standards in the functional safety and security area with respect to safety, security and performance co-engineering.
  - Partner AIT in particular is involved in several of the standards working groups where co-engineering is relevant and addressed
- **O11**: To influence actively in two international standardization groups focused on frameworks for the coordination of safety, security and reliability of automation
  - AIT is involved in relevant working groups; Thales is involved in Arcadia; Intecs is involved in PMBOK.
- **O12**: To promote awareness and bring results of AQUAS into at least two other engineering international standards, such as the Object Management Group (OMG), or the Functional Mock-Up Interface (FMI) standard.
  - Several AQUAS partners are actively involved in OMG initiatives, and the VEL initiative is an example of reaching out to a new standardization group

AQUAS SAFETY SECURITY PERFORMANCE

9

General Progress Indicators

- A preliminary set of general indicators for progress against the major overall challenges has been identified
- Suitability of these indicators will be evaluated as work progresses

Challenge	Progress Indicator
How to provide visibility of challenges and progress, addressing priorities and decisions (supported in AQUAS or later).	Number of presentations either in AQUAS related meetings (e.g. EAB) or public conferences
Industry may have reservations to adopt an approach which is not reflected in current standards.	Number of explicit contacts established with companies on the question of standards-based co-engineering
There are domains in which integrated approaches to safety and security are not fostered by the governing standards –or even implicitly discouraged.	Number of papers or public reports (including AQUAS deliverables) arguing integrated standards approaches

AQUAS 10

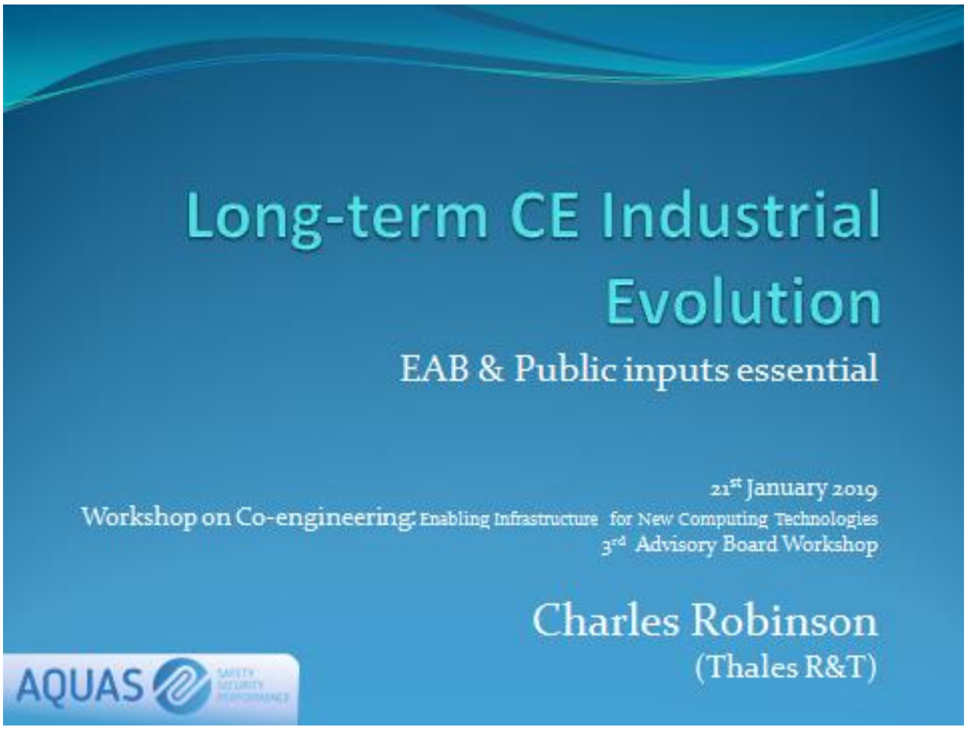
Definition Challenges

- Many problematic areas in achieving convergence
  - "**Risk**" – can we converge on a harmonized definition?
  - "**Performance**" – few standards talk about it precisely

Term	Definition	Type	Source
Safety	State where an acceptable level of risk is not exceeded. This may apply to the system or its environment (particularly to people).	Safety	ECSS / CRR
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.	Transverse	FIPS 200
Safety Integrity Level	Discrete level, corresponding to a range of safety integrity values	Safety	IEC 61508
Security level	Level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit	Security	IEC 62443
Performance limitation	Insufficiencies of the function itself	Performance	SOTIF
Trade-off	Decision-making actions that select from various requirements and alternative solutions on the basis of net benefit to the stakeholders	Transverse	ISO/IEC 15288:2015

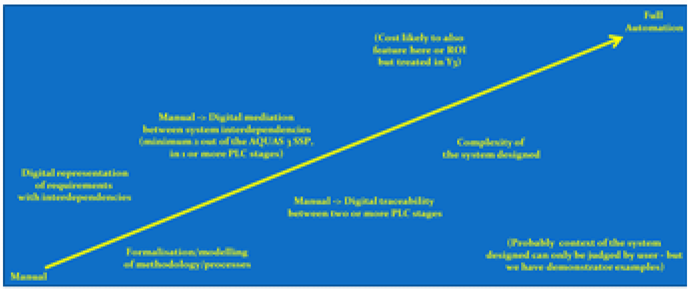
AQUAS 11

2.2.16 Long-term CE Industrial Evolution



Migration of Existing Processes to more Automated CE

- Technical migration depends on one's methodology and tooling already established for system engineering.
- For CE we start by asking what level am I currently at and what level should I advance too?
  - Primarily linked with traceability and mediation of interdependencies, but also size of the system and application context.



AQUAS SAFETY SECURITY PERFORMANCE

Challenges & Enablers

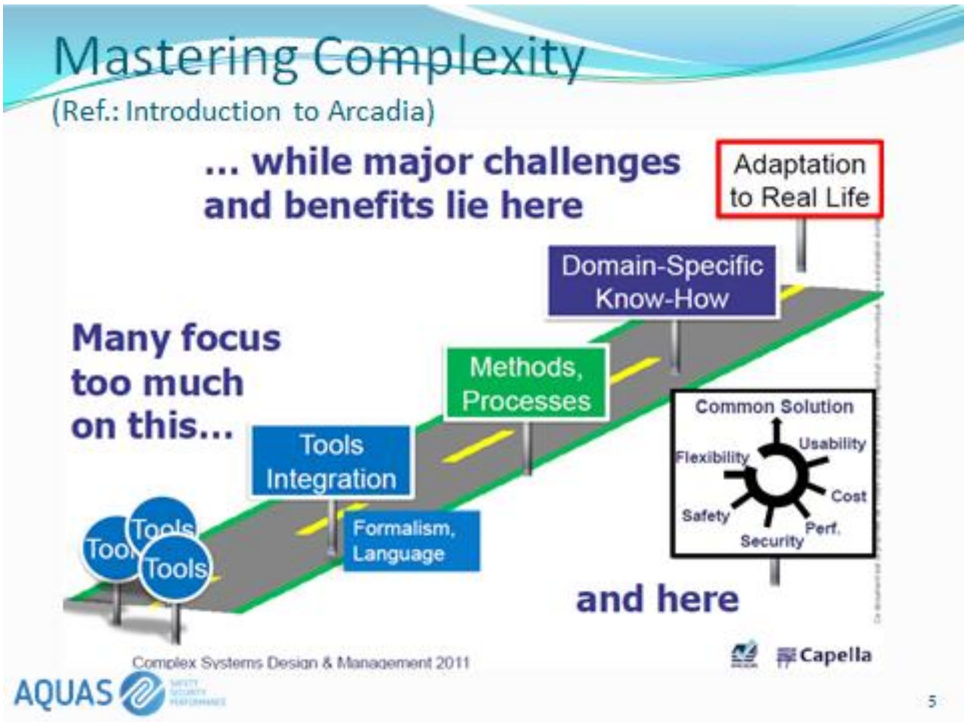
- Key point: Bringing S-P-S (automated) co-engineering into mainstream development.

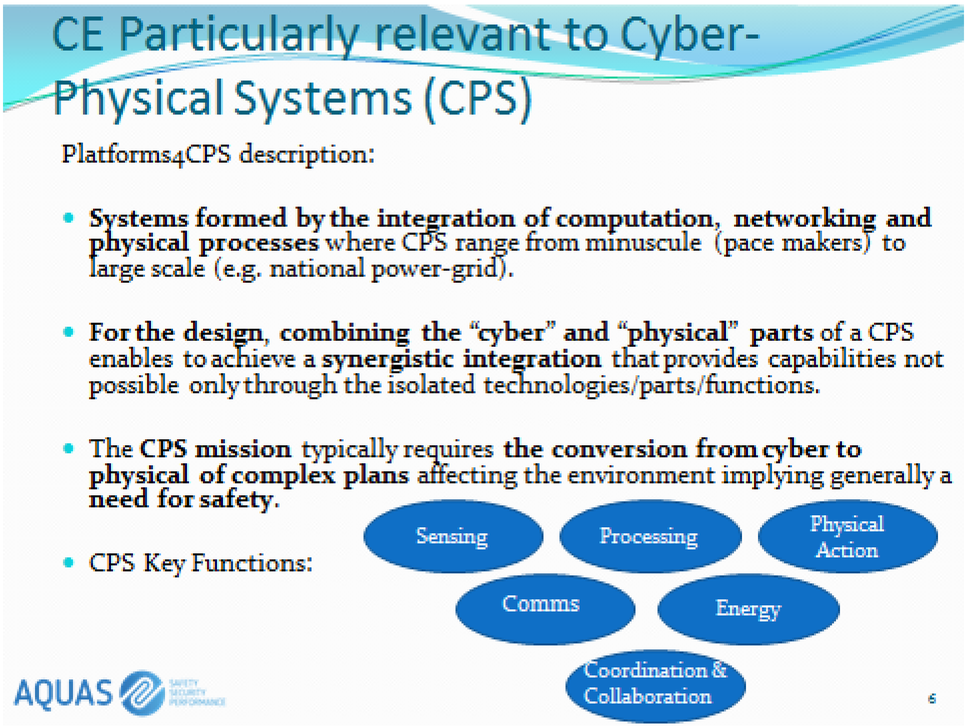
- How to provide visibility of challenges and progress
- Market research: Identifying complementary synergies with other engineering methods.
- Evolving Standards
- Strengthening the External Advisory Board (EAB)
- Supporting EAB to encourage more engagement from their organisation.
- Convincing policy makers
- Convincing higher management

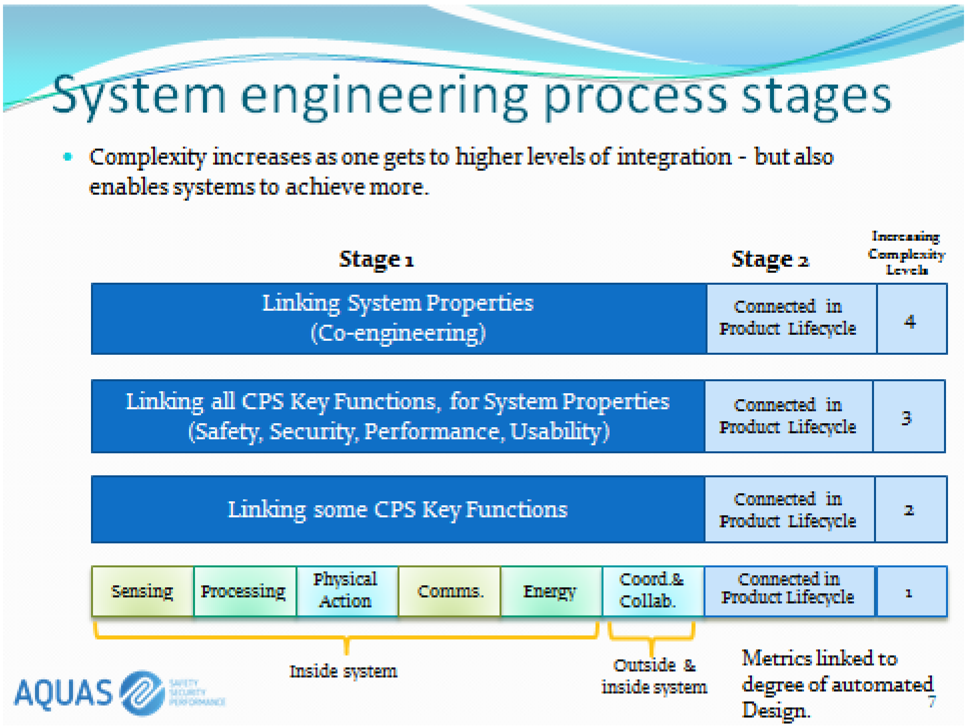
- The target of providing trans-domain solutions may not be well perceived in certain domains.
- The lack of a correct, and single, definition of the data exchange formats may cause certain co-engineering interactions between tools to become difficult or even impractical.
- Both safety and security standards impose technical and process constraints on developers.
- "Companies may stick to established processes and shy back from training expenses.Companies may suspect an immediate change of development paradigms required, which can cause a period of reduced staff productivity."
- Need for confidentiality may render difficult the cooperation between partners.

- Augmenting resources to treat CE.
- Identifying/extending funding options
- Sustainability (believed evolving standards during project was a good approach)
- Proliferation of projects. Should tools provide overviews of where projects contribute?
- Programme for CE projects to challenges.

AQUAS SAFETY SECURITY PERFORMANCE 4

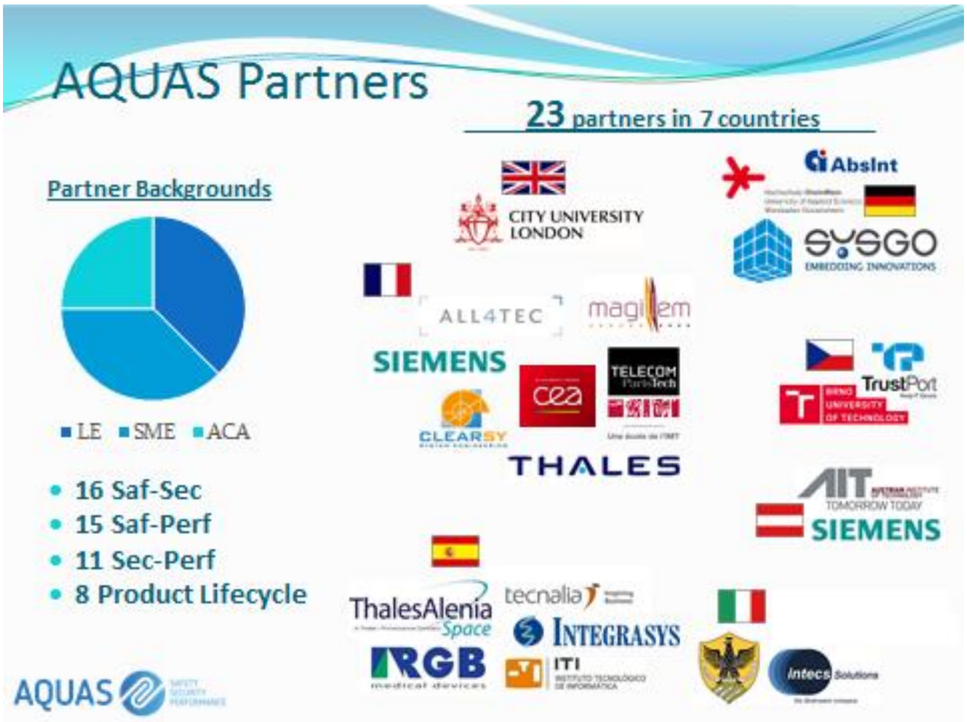

Mastering Complexity
(Ref.: Introduction to Arcadia)
... while major challenges and benefits lie here
Adaptation to Real Life
Domain-Specific Know-How
Many focus too much on this...
Methods, Processes
Common Solution
Flexibility
Usability
Cost
Safety
Perf.
Security
Tools Integration
Formalism, Language
Tools
Tools
and here
Complex Systems Design & Management 2011
Capella
AQUAS
5


CE Particularly relevant to Cyber-Physical Systems (CPS)
Platforms4CPS description:
Systems formed by the integration of computation, networking and physical processes where CPS range from minuscule (pace makers) to large scale (e.g. national power-grid).
For the design, combining the "cyber" and "physical" parts of a CPS enables to achieve a synergistic integration that provides capabilities not possible only through the isolated technologies/parts/functions.
The CPS mission typically requires the conversion from cyber to physical of complex plans affecting the environment implying generally a need for safety.
CPS Key Functions:
Sensing
Processing
Physical Action
Comms
Energy
Coordination & Collaboration
AQUAS
6

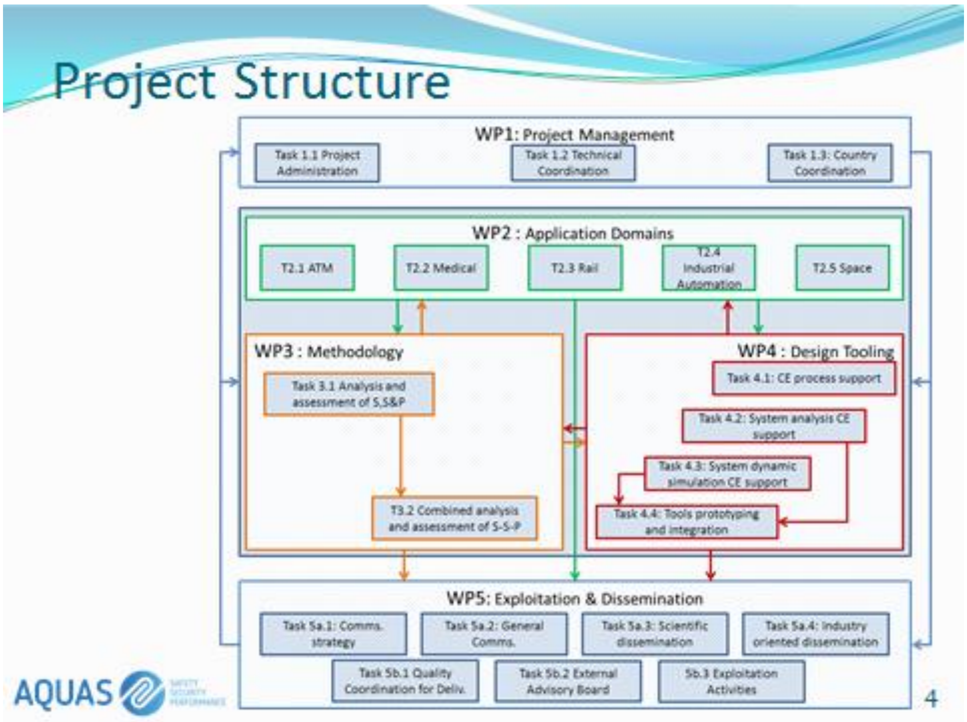


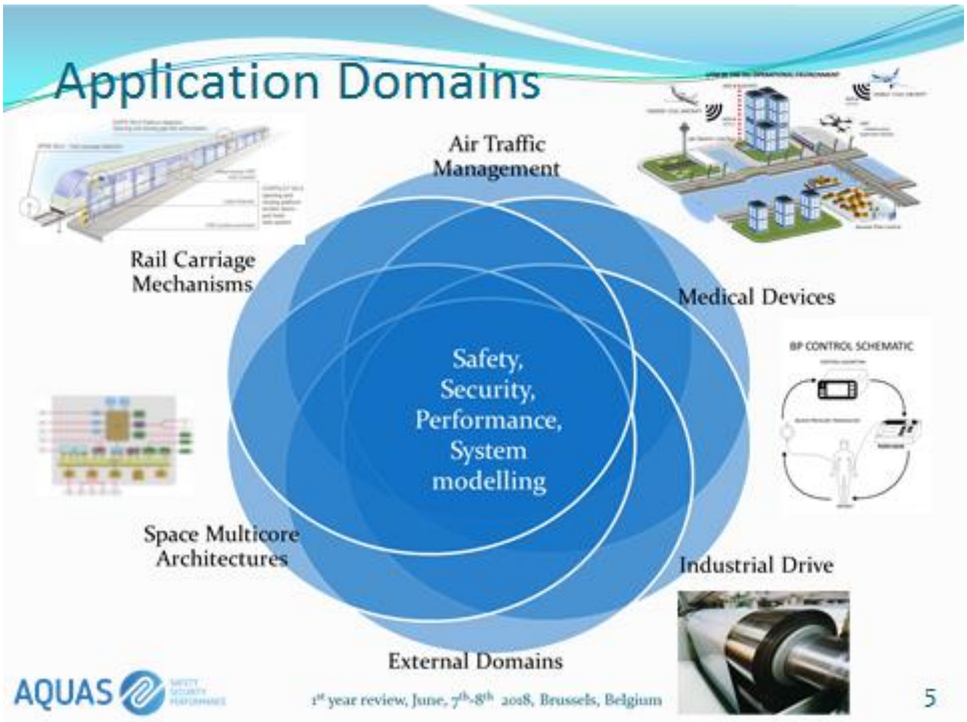
2.2.17 Presentation at ECSEL JU symposium 2018

Here, we show an overview presentation used at ECSEL JU symposium 2018 in Brussels. A slideshow video based on this presentation has been created and used to support the AQUAS booth there.

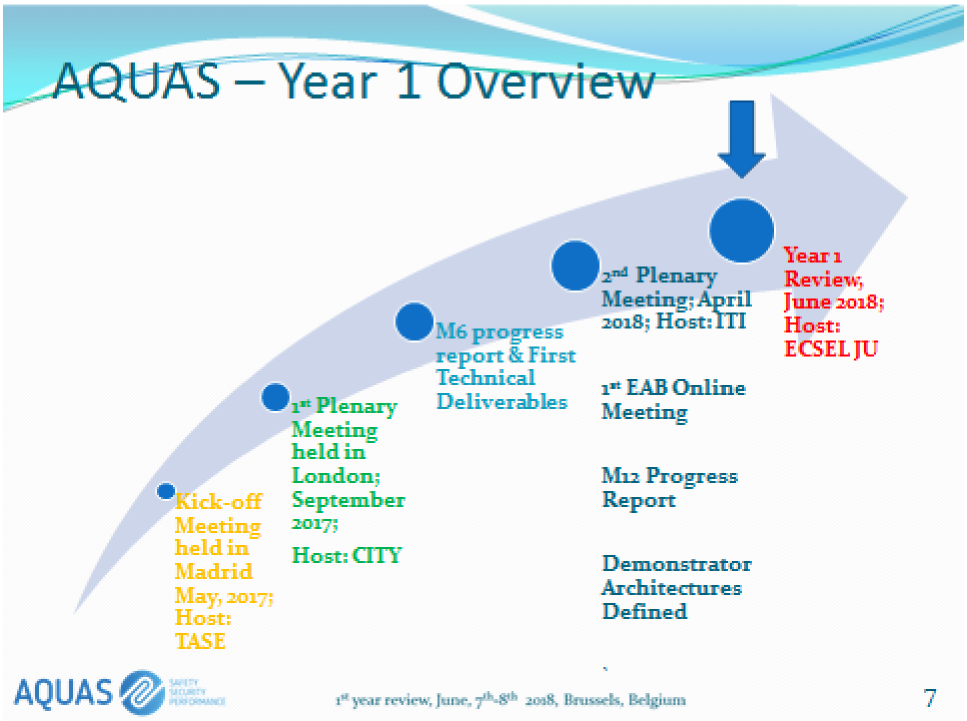

AQUAS Partners
23 partners in 7 countries
Partner Backgrounds
LE
SME
ACA
16 Saf-Sec
15 Saf-Perf
11 Sec-Perf
8 Product Lifecycle
CITY UNIVERSITY LONDON
AbsInt
SYSGO
EMBEDDING INNOVATIONS
ALL4TEC
magillem
SIEMENS
cea
TELECOM ParisTech
CLEARSY
THALES
TrustPort
BRNO UNIVERSITY OF TECHNOLOGY
AIT
TOMORROW TODAY
SIEMENS
ThalesAlenia Space
tecnalia
INTEGRASYS
RGB medical devices
ITI
INSTITUTO TECNOLÓGICO DE INFORMÁTICA
intecs Solutions
AQUAS

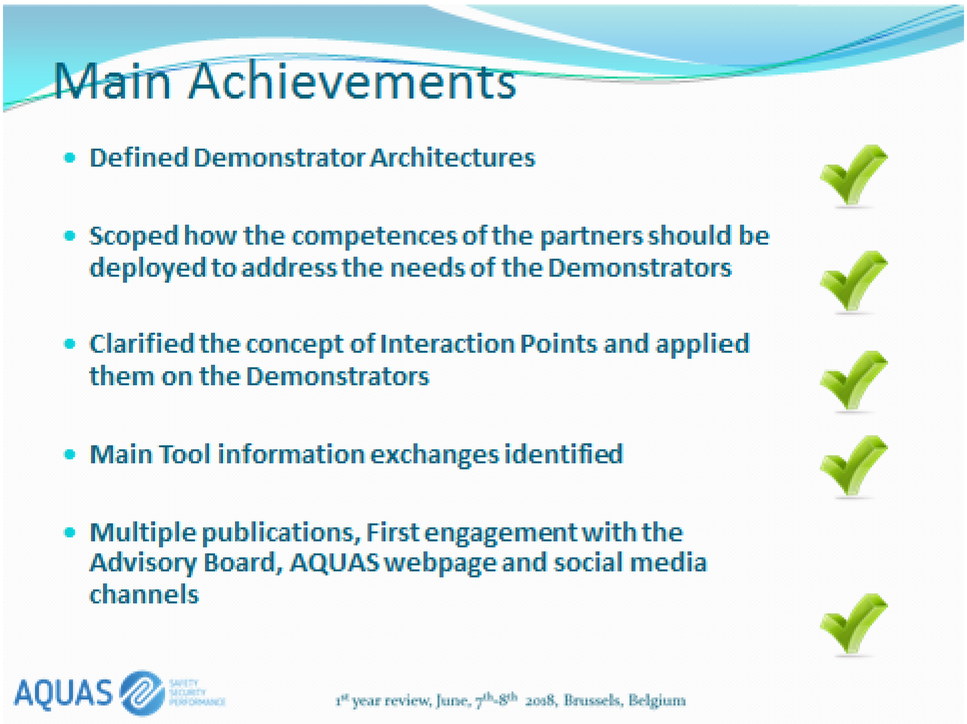

Co-Engineering into mainstream practices
We are investigating Co-Engineering techniques for safety, security and performance of critical and complex embedded systems
AQUAS
1st year review, June, 7th-8th 2018, Brussels, Belgium
3

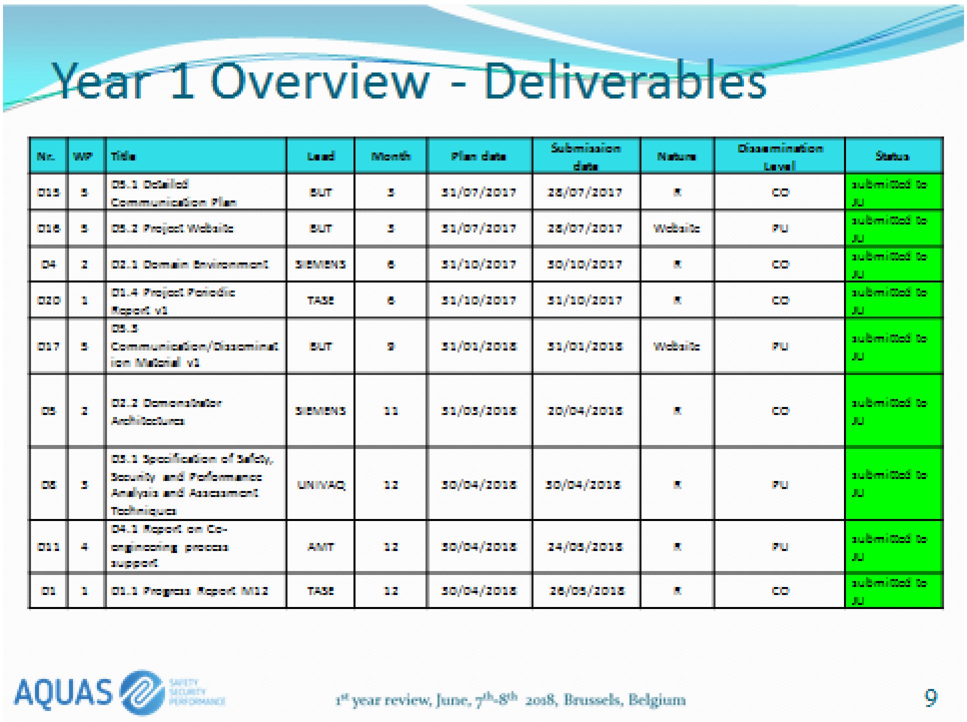

Project Structure
WP1: Project Management
Task 1.1 Project Administration
Task 1.2 Technical Coordination
Task 1.3: Country Coordination
WP2 : Application Domains
T2.1 ATM
T2.2 Medical
T2.3 Rail
T2.4 Industrial Automation
T2.5 Space
WP3 : Methodology
Task 3.1 Analysis and assessment of S,S&P
T3.2 Combined analysis and assessment of S-S-P
WP4 : Design Tooling
Task 4.1: CE process support
Task 4.2: System analysis CE support
Task 4.3: System dynamic simulation CE support
Task 4.4: Tools prototyping and integration
WP5: Exploitation & Dissemination
Task 5a.1: Comms. strategy
Task 5a.2: General Comms.
Task 5a.3: Scientific dissemination
Task 5a.4: Industry oriented dissemination
Task 5b.1 Quality Coordination for Deliv.
Task 5b.2 External Advisory Board
5b.3 Exploitation Activities
AQUAS
4


Application Domains
Air Traffic Management
Rail Carriage Mechanisms
Medical Devices
BP CONTROL SCHEMATIC
Safety, Security, Performance, System modelling
Space Multicore Architectures
Industrial Drive
External Domains
AQUAS
1st year review, June, 7th-8th 2018, Brussels, Belgium
5


Project Status
AQUAS
1st year review, June, 7th-8th 2018, Brussels, Belgium
6


AQUAS – Year 1 Overview
Kick-off Meeting held in Madrid May, 2017; Host: TASE
1st Plenary Meeting held in London; September 2017;
Host: CITY
M6 progress report & First Technical Deliverables
2nd Plenary Meeting; April 2018; Host: ITI
1st EAB Online Meeting
M12 Progress Report
Demonstrator Architectures Defined
Year 1 Review, June 2018; Host: ECSEL JU
AQUAS
1st year review, June, 7th-8th 2018, Brussels, Belgium
7





Nr.	WP	Title	Lead	Month	Plan date	Submission date	Nature	Dissemination Level	Status
D15	5	D5.1 Detailed Communication Plan	BUT	3	31/07/2017	28/07/2017	R	CO	submitted to JU
D16	5	D5.2 Project Website	BUT	3	31/07/2017	28/07/2017	Website	PU	submitted to JU
D4	2	D2.1 Domain Environment	SIEMENS	6	31/10/2017	30/10/2017	R	CO	submitted to JU
D20	1	D1.4 Project Periodic Report v1	TASE	6	31/10/2017	31/10/2017	R	CO	submitted to JU
D17	5	D5.3 Communication/Dissemination Material v1	BUT	9	31/01/2018	31/01/2018	Website	PU	submitted to JU
D5	2	D2.2 Demonstrator Architectures	SIEMENS	11	31/03/2018	20/04/2018	R	CO	submitted to JU
D8	3	D3.1 Specification of Safety, Security and Performance Analysis and Assessment Techniques	UNIVAQ	12	30/04/2018	30/04/2018	R	PU	submitted to JU
D11	4	D4.1 Report on Co-engineering process support	AMT	12	30/04/2018	24/05/2018	R	PU	submitted to JU
D1	1	D1.1 Progress Report M12	TASE	12	30/04/2018	28/05/2018	R	CO	submitted to JU

Year 1 Overview - Milestones

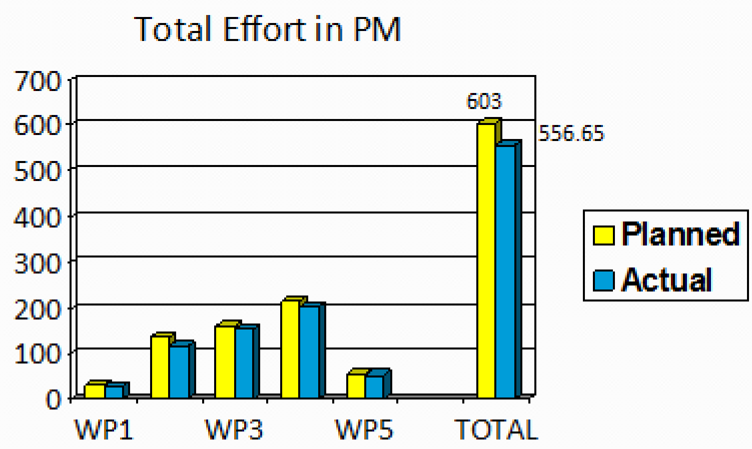
Milestone number	Milestone title	WP	Lead	Due date (month)	Comment
MS1	Launch of the Project	1	TASE	1	Kick-off Meeting successfully held in THALES building in Madrid, Spain on the 29th and 30th of May 2017. All partners attended the Kick-off meeting and elaborated on their activities.
MS2	Use Case Requirements and Environment defined	2	SIEMENS	6	D2.1 Domain Environment submitted to ECSEL JU
MS3	AQUAS Demonstrator Architectures defined	2-3-4	SIEMENS	11	D2.1 Demonstrator Architectures submitted to ECSEL JU
MS4	AQUAS Awareness and Uptake established	5	TRT	11	There is already 61 % of the consortium involved (over the expected 40 %). More information available in the Progress Report
MS5	Year 1 complete	1	TASE	12	Plenary Meetings held; First Year Review in Progress

AQUAS SAFETY SECURITY PERFORMANCE

1st year review, June, 7th-8th 2018, Brussels, Belgium

10

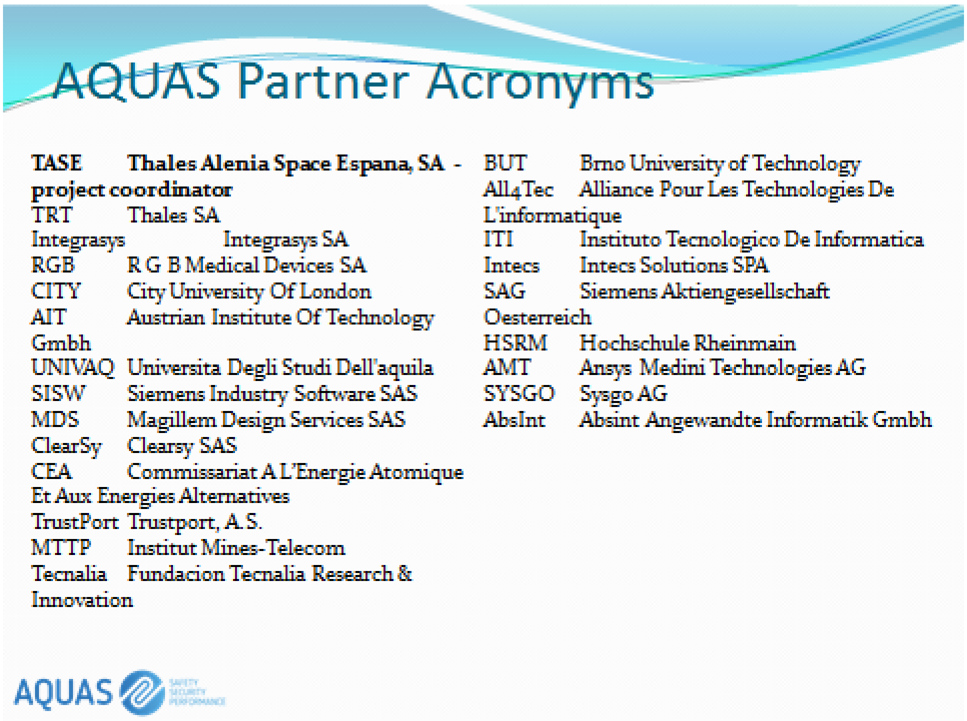
Planned vs. Actual Effort in 1st reporting period – Preliminary



AQUAS SAFETY SECURITY PERFORMANCE

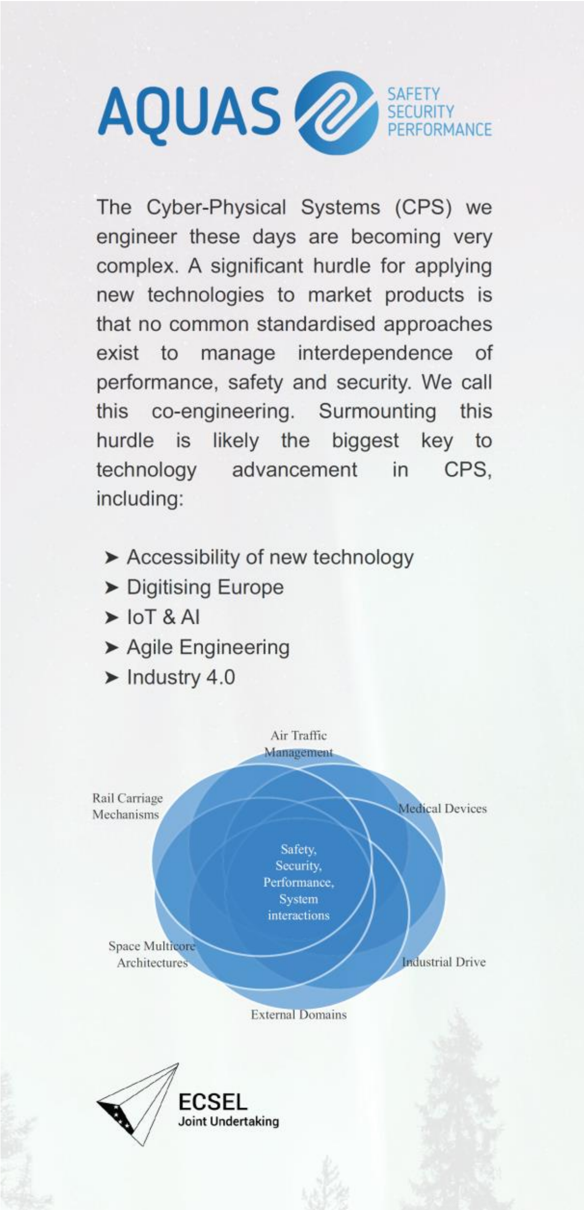
1st year review, June, 7th-8th 2018, Brussels, Belgium


AQUAS
THANK YOU
ECSEL JU


AQUAS Partner Acronyms
TASE Thales Alenia Space Espana, SA - project coordinator
TRT Thales SA
Integrasys Integrasys SA
RGB R G B Medical Devices SA
CITY City University Of London
AIT Austrian Institute Of Technology Gmbh
UNIVAQ Universita Degli Studi Dell'aquila
SISW Siemens Industry Software SAS
MDS Magillem Design Services SAS
ClearSy Clearsy SAS
CEA Commissariat A L'Energie Atomique Et Aux Energies Alternatives
TrustPort Trustport, A.S.
MTTP Institut Mines-Telecom
Tecnalia Fundacion Tecnalia Research & Innovation
BUT Brno University of Technology
All4Tec Alliance Pour Les Technologies De L'informatique
ITI Instituto Tecnologico De Informatica
Intecs Intecs Solutions SPA
SAG Siemens Aktiengesellschaft Oesterreich
HSRM Hochschule Rheinmain
AMT Ansys Medini Technologies AG
SYSGO Sysgo AG
AbsInt Absint Angewandte Informatik Gmbh
AQUAS

2.3 Project leaflet

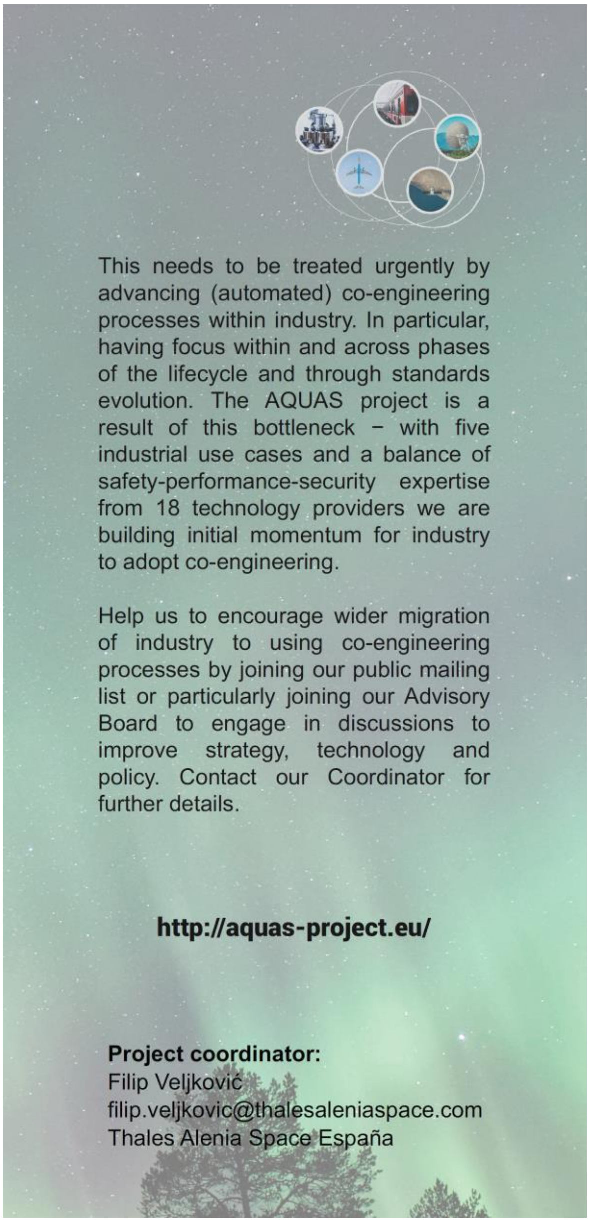
The leaflet describes the project and its goals and provides basic contact information. It can be freely circulated to inform about the project and to promote it at workshops, trade shows, technical fairs, congresses, and other events. Since the last year, it has been updated, professionally printed in 2000 copies, and distributed to all project partners to be used for project dissemination. Here is the printed version of the leaflet:



AQUAS SAFETY SECURITY PERFORMANCE

The Cyber-Physical Systems (CPS) we engineer these days are becoming very complex. A significant hurdle for applying new technologies to market products is that no common standardised approaches exist to manage interdependence of performance, safety and security. We call this co-engineering. Surmounting this hurdle is likely the biggest key to technology advancement in CPS, including:

- Accessibility of new technology
- Digitising Europe
- IoT & AI
- Agile Engineering
- Industry 4.0



This needs to be treated urgently by advancing (automated) co-engineering processes within industry. In particular, having focus within and across phases of the lifecycle and through standards evolution. The AQUAS project is a result of this bottleneck – with five industrial use cases and a balance of safety-performance-security expertise from 18 technology providers we are building initial momentum for industry to adopt co-engineering.

Help us to encourage wider migration of industry to using co-engineering processes by joining our public mailing list or particularly joining our Advisory Board to engage in discussions to improve strategy, technology and policy. Contact our Coordinator for further details.

http://aquas-project.eu/

Project coordinator:
Filip Veljković
filip.veljkovic@thalesaleniaspace.com
Thales Alenia Space España

2.4 Project video

The first version of the project video created by professional creative studio FILMONDO (http://www.filmondo.cz/) was finished in August 2018 to be used as a part of a booth presentation at Euromicro DSD conference. This version was also shown to project partners within the project plenary meeting in Vienna (September 2018). After that, several project partners provided valuable comments and suggestions that were not clear within the story line phase. BUT therefore raised several issues to FILMONDO and recently, the second version of the video has been finished. Naturally, we do not include the video directly to this deliverable. It can be simply found at the project web page (https://aquas-project.eu/).

3 Conclusion

In the above, we presented dissemination material that have been created or updated to support the AQUAS project dissemination activities during the last year, namely, a project poster, project presentations, a project leaflet, and a project video.

The progress of the dissemination material since the current moment will be next reported in month 33 of the project, i.e., in January 2020.

Deliverable 5.3

Communication/dissemination material (V1)

This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737475. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Spain, France, United Kingdom, Austria, Italy, Czech Republic, Germany.

DISSEMINATION LEVEL		
X	PU	Public
	CO	Confidential, only for members of the consortium (including the Commission Services)

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	AQUAS
Project Full Name:	Aggregated Quality Assurance in Systems
Grant Agreement No.:	737475
Programme	ICT-1: Cyber-Physical-Systems
Instrument:	Research & innovation action
Start date of project:	01-05-2017
Duration:	36 months
Deliverable No.:	D5.3
Document name:	Communication/dissemination material (V1)
Work Package	WP5
Associated Task	Task(s) 5a.3
Nature [1]	DEC
Dissemination Level [2]	PU
Version:	1.0
Actual Submission Date:	31-01-2018
Contractual Submission Date	31-01-2018
Editor: Institution: E-mail:	Bohuslav Křena BUT krena@fit.vutbr.cz

[1] **R**=Report, **DEC**= Websites, patents filling, etc., **O**=Other
[2] **PU**=Public, **CO**=Confidential, only for members of the consortium (including the Commission Services)

Change Control

Document History

Version	Date	Change History	Author(s)	Organisation(s)
(p1)	23-05-2017	Poster for ECSEL JU symposium at Malta	Bohuslav Křena, Tomáš Vojnar	BUT
(p2)	25-08-2017	Poster for Euromicro	Pribyl Johannes	AIT
(sb2)	05-12-2017	Slides for Brussels	Bohuslav Křena	BUT
(sb3)	06-12-2017	Slides for Brussels	Tomáš Vojnar	BUT
(sb4)	07-12-2017	Slides for Brussels	Charles Robinson	TRT
(sb5)	08-12-2017	Slides for Brussels	Matthieu Pfeiffer	MDS
(s0.3)	17-01-2018	Industrial Drive UC slides update	Martin Matschnig	SAG
(s0.3)	20-01-2018	Medical Devices UC slides update	Ricardo Ruiz	RGB
(s0.3)	23-01-2018	Air Traffic Management UC slides update	Juan Luis Manas	ISYS
(l1)	25-01-2018	Leaflet created	David Bařina	BUT
(s0.3)	29-01-2018	Space Multicore Architecture UC slides update	Jaime Gonzalez Martinez	TASE
0.1	29-01-2018	Dissemination material summarised	Bohuslav Křena	BUT
0.2	30-01-2018	Internal review	Tomáš Vojnar	BUT
1.0	31-01-2018	Final version	Filip Veljković	TASE

Distribution List

Date	Issue	Group
29-01-2018	Internal review	Tomáš Vojnar (BUT) David Bařina (BUT)
31-01-2018	Final version	EC AQUAS.ALL

Table of Contents

Executive Summary

This deliverable describes the dissemination material created so far to support dissemination of information about the AQUAS project, its progress, and results. It comprises a project poster, a project presentation, and a project leaflet. As the project evolves, the dissemination material will be updated according to the project progress. This deliverable is therefore considered to evolve as well. This is the first version of the deliverable while two other versions that will report about the current status of the dissemination material will follow in January 2019 (V2, M21) and in January 2020 (V3, M33).

1 Introduction

Dissemination and communication activities are a strong contributor to the project success. To support dissemination end exploitation, several kinds of dissemination material need to be prepared in order to present the project and its results to the general public and stakeholders from the ECSEL focused areas: 'Design Technology', 'Cyber-physical Systems', and 'European Asset Protection'. In particular, communication and dissemination activities should raise the public awareness of the challenges faced with the provision of safe, secure, and efficient cyber-physical systems.

As the project evolves, different information may be used for the dissemination – in the first stages, we can communicate the existence and main ideas of the project while later, we will report about the project progress and the achieved results. The status of the current dissemination material should be summarised and reported three times during the project:

- First (V1) in month 9 (the current version),
- Second (V2) in month 21,
- Final (V3) in month 33.

2 Dissemination material

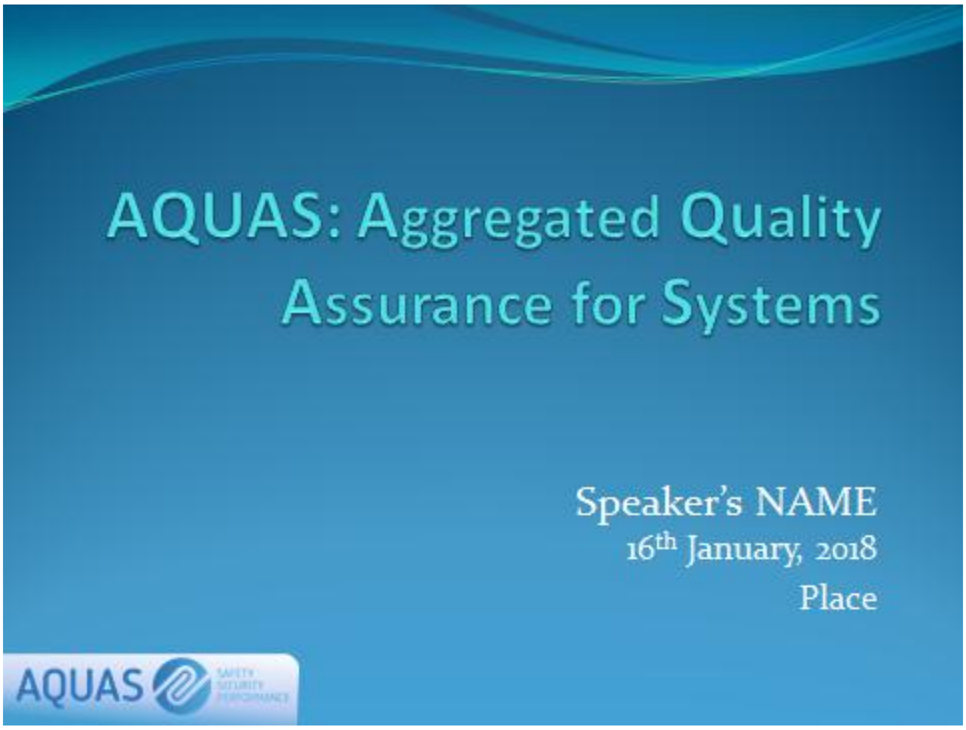
Different forms of dissemination material are needed to present the project at different events and using different channels. In the following, we report about the dissemination material that has been created to present the AQUAS project so far.

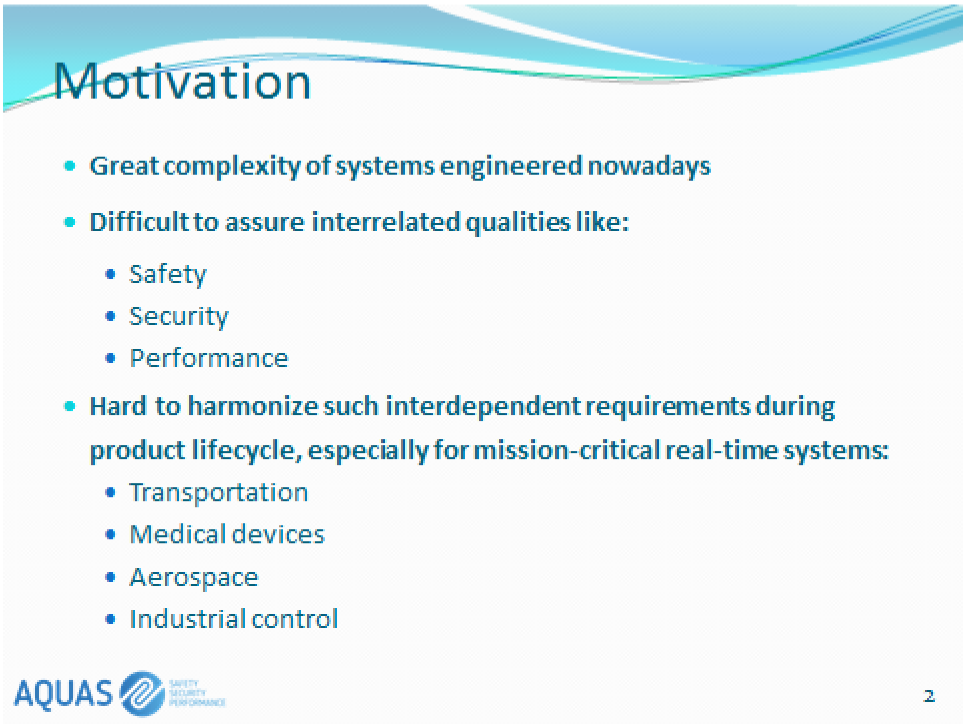
2.1 Project poster

The project poster is useful for booth presentations at fairs as well as for poster sessions at conferences and workshops. So far, it has been used twice, first by BUT at the ECSEL JU symposium in Malta and second (in a slightly updated form) by AIT at Euromicro 2017 in Vienna. A picture of the poster – in its version from Euromicro – follows:

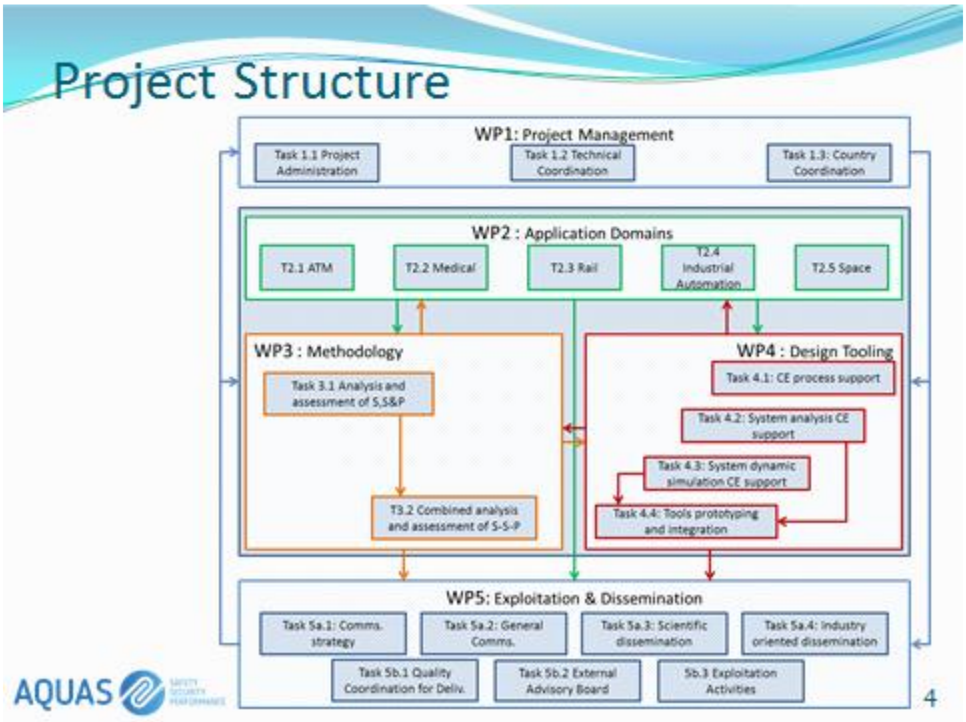
2.2 Project presentation

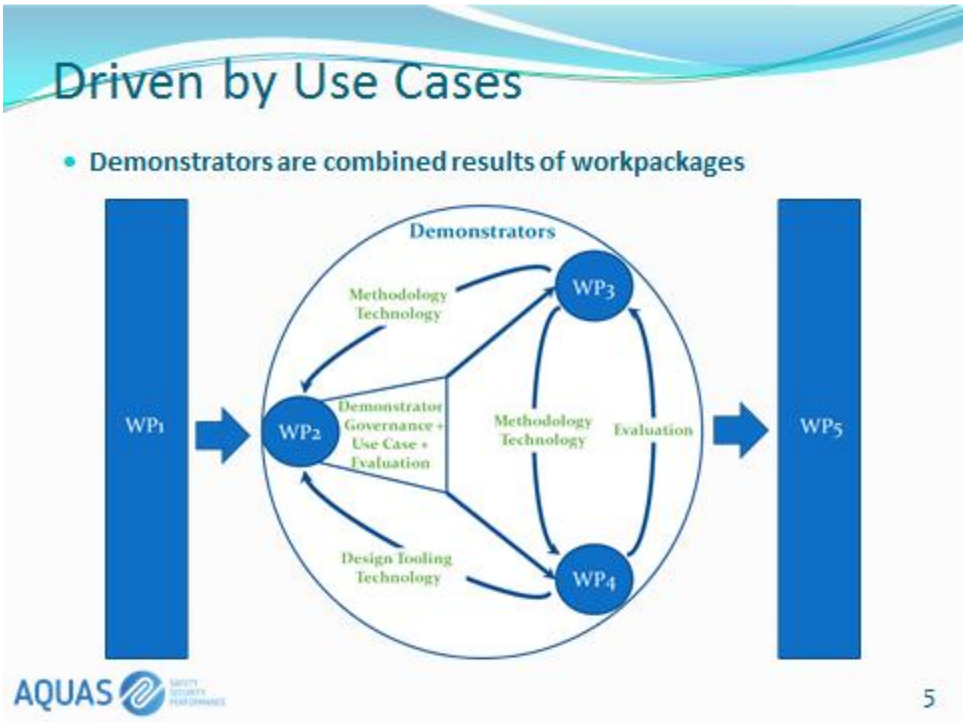
A project presentation using slides is useful for events when a presenter speaks to the audience. Of course, various versions of the presentation are needed depending on the focus as well as the time slot dedicated for the talk. The following slides are an extended version of the presentation already used by MDS in Brussels:

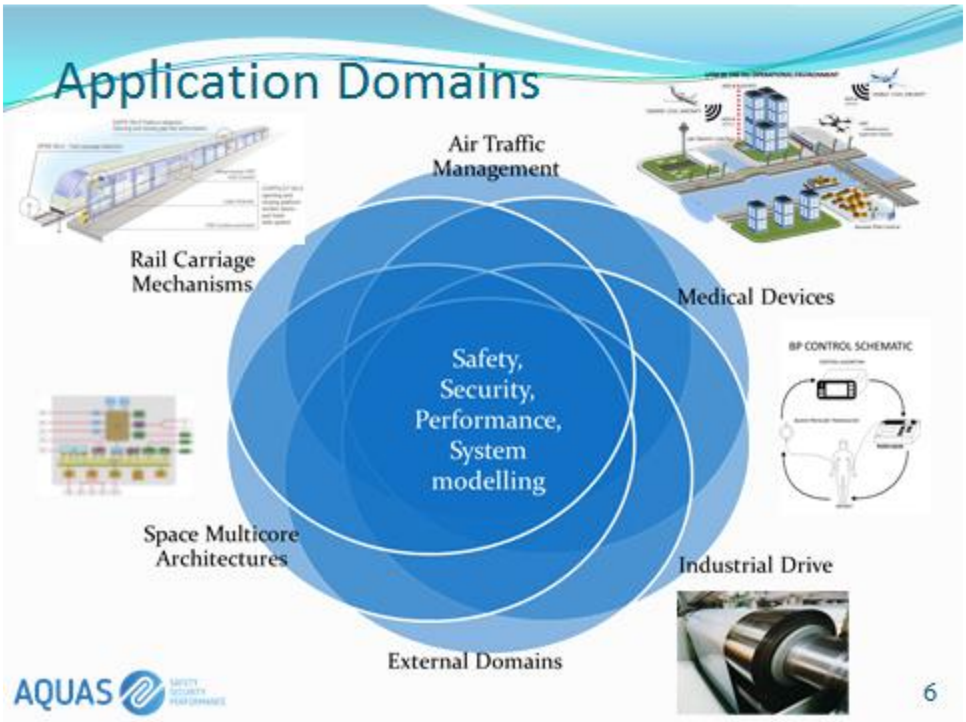


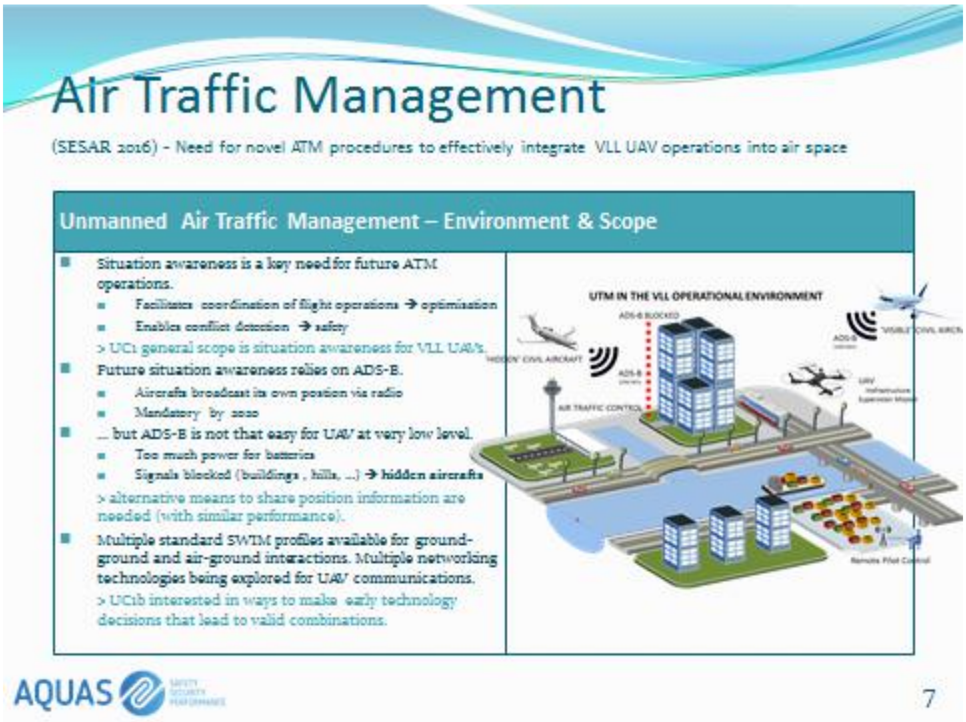

Motivation
Great complexity of systems engineered nowadays
Difficult to assure interrelated qualities like:
Safety
Security
Performance
Hard to harmonize such interdependent requirements during product lifecycle, especially for mission-critical real-time systems:
Transportation
Medical devices
Aerospace
Industrial control
AQUAS
2


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
AQUAS
3

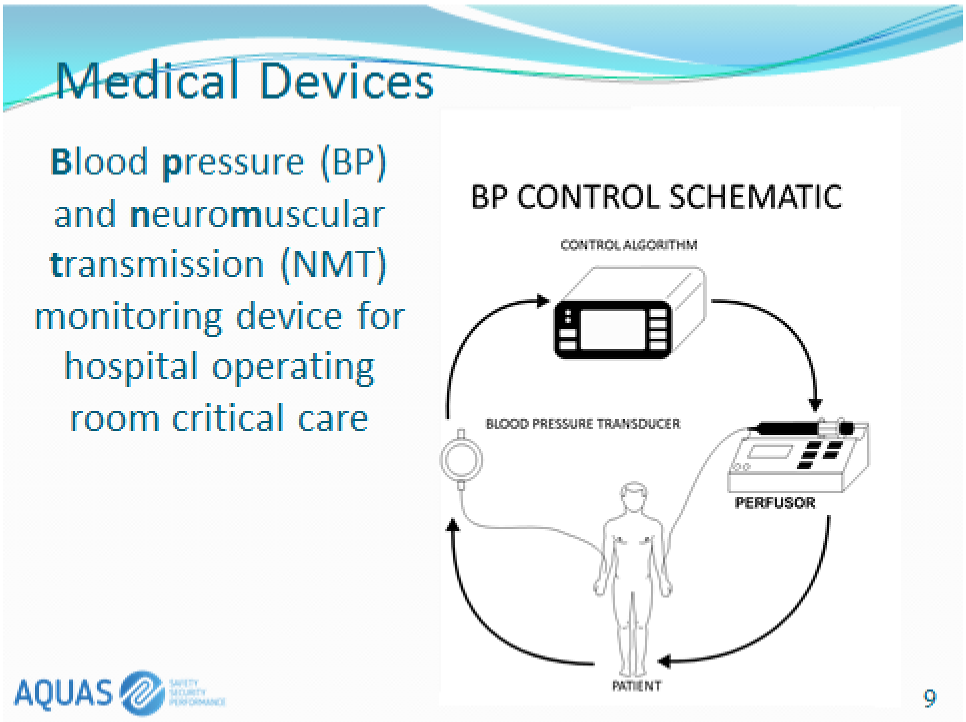

Project Structure
WP1: Project Management
Task 1.1 Project Administration
Task 1.2 Technical Coordination
Task 1.3: Country Coordination
WP2 : Application Domains
T2.1 ATM
T2.2 Medical
T2.3 Rail
T2.4 Industrial Automation
T2.5 Space
WP3 : Methodology
Task 3.1 Analysis and assessment of S,S&P
T3.2 Combined analysis and assessment of S-S-P
WP4 : Design Tooling
Task 4.1: CE process support
Task 4.2: System analysis CE support
Task 4.3: System dynamic simulation CE support
Task 4.4: Tools prototyping and integration
WP5: Exploitation & Dissemination
Task 5a.1: Comms. strategy
Task 5a.2: General Comms.
Task 5a.3: Scientific dissemination
Task 5a.4: Industry oriented dissemination
Task 5b.1 Quality Coordination for Deliv.
Task 5b.2 External Advisory Board
5b.3 Exploitation Activities
AQUAS
4


Driven by Use Cases
Demonstrators are combined results of workpackages
Demonstrators
WP1
WP2
WP3
WP4
WP5
Methodology Technology
Demonstrator Governance + Use Case + Evaluation
Methodology Technology
Evaluation
Design Tooling Technology
AQUAS
5

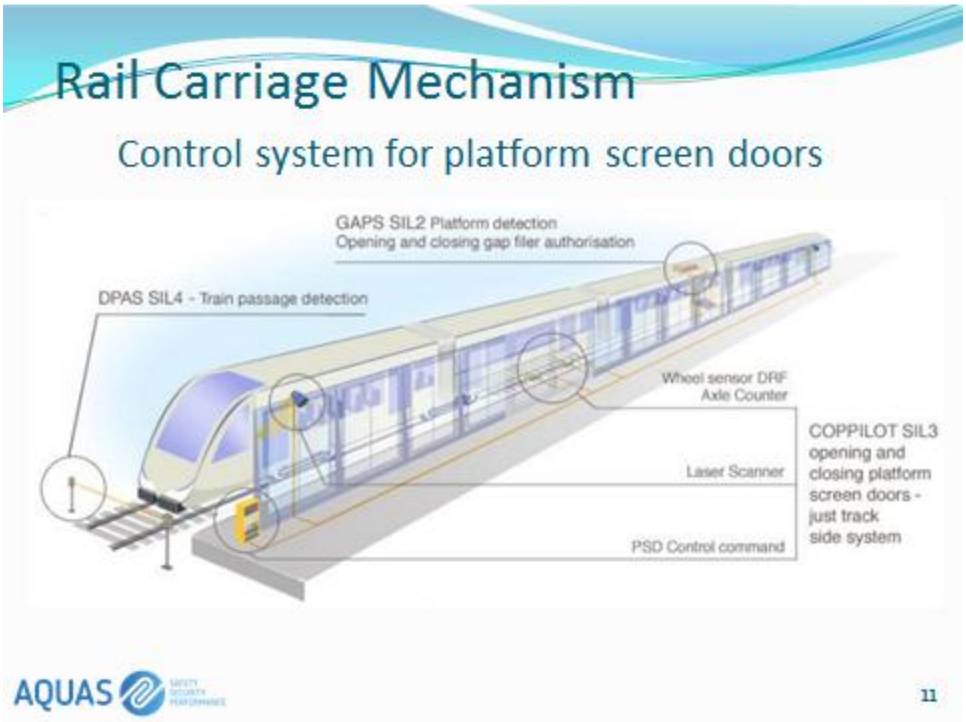

Application Domains
Air Traffic Management
Rail Carriage Mechanisms
Medical Devices
Safety, Security, Performance, System modelling
Space Multicore Architectures
Industrial Drive
External Domains
BP CONTROL SCHEMATIC
AQUAS
6


Air Traffic Management
(SESAR 2016) - Need for novel ATM procedures to effectively integrate VLL UAV operations into air space
Unmanned Air Traffic Management – Environment & Scope
Situation awareness is a key need for future ATM operations.
Facilitates coordination of flight operations → optimisation
Enables conflict detection → safety
> UC1 general scope is situation awareness for VLL UAVs.
Future situation awareness relies on ADS-B.
Aircrafts broadcast its own position via radio
Mandatory by 2020
... but ADS-B is not that easy for UAV at very low level.
Too much power for batteries
Signals blocked (buildings , hills, ...) → hidden aircrafts
> alternative means to share position information are needed (with similar performance).
Multiple standard SWIM profiles available for ground-ground and air-ground interactions. Multiple networking technologies being explored for UAV communications.
> UC1b interested in ways to make early technology decisions that lead to valid combinations.
UTM IN THE VLL OPERATIONAL ENVIRONMENT
AQUAS
7


Air Traffic Management
Unmanned Air Traffic Management demonstrator based on the Intel Aero platform
Unmanned Air Traffic Management - Objectives & Partners
Novel security-performance co-engineering methods and tools will be applied to optimise communication throughput and reduce battery consumption while keeping the high security and safety levels demanded in these scenarios.
AbsInt
AIT
BRNO UNIVERSITY OF TECHNOLOGY
CITY UNIVERSITY LONDON
intecs
INTEGRASYS
Hochschule RheinMain
SYSGO
TrustPort
AQUAS
8


Medical Devices
Blood pressure (BP) and neuromuscular transmission (NMT) monitoring device for hospital operating room critical care
BP CONTROL SCHEMATIC
CONTROL ALGORITHM
BLOOD PRESSURE TRANSDUCER
PERFUSOR
PATIENT
AQUAS
9


Medical Devices
BP and NMT Device – Testing Environment
AQUAS


Rail Carriage Mechanism
Control system for platform screen doors
GAPS SIL2 Platform detection
Opening and closing gap filer authorisation
DPAS SIL4 - Train passage detection
Wheel sensor DRF
Axle Counter
COPPILOT SIL3
opening and
closing platform
screen doors -
just track
side system
Laser Scanner
PSD Control command
AQUAS
11


Platform Screen Doors
Requirement: Open platform doors if and only if a passenger train is stopped on the platform at its correct position and train doors are opening
Detection-based: redundant, diverse sensors to detect the arrival of the train
Different possibilities:
Human drivers have different driving profiles
System that can interact with manual or automated metro trains
Digital communication with automated metros
...
Stop signal sensor
Wheel sensor
AQUAS


Industrial Drive
The heart of every automated industrial process are industrial drives.
Industrial Drives and Motion Control
Industrial drives are usually integrated in an industrial network.
> UC4 is located on the field level
There are several e-motor types such as synchronous and asynchronous motors, ranging from standard electric motor systems and servomotors for motion control applications (including linear and torque motors) over motors for use in hazardous explosion areas, to high voltage, DC and customized electric motors.
> UC4 intends to use servo motor models
Motion Control products cover a large variety of variable frequency inverters for electric motors.
> UC4 contains a virtual prototype of a motion control platform and a connected electronic motor.
The large variety of communication and sensor interfaces of such embedded systems adds significant security challenges to the safety mechanisms already implemented in today's commercial industrial products.
Virtual Prototype
AQUAS
13

Standards and Guidelines

Most important standards and guidelines for the industrial domain are IEC 61508 for functional safety and IEC 62443 for industrial network and system security.

Industrial Drives Use Case – Relevant Standards and Guidelines

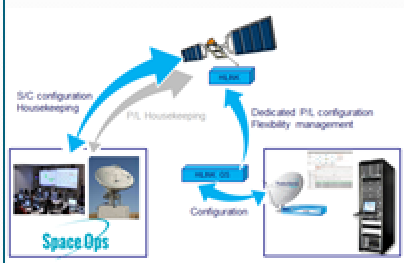
- **IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems**
  - For the use case demonstrator only the phases until Realization are of interest.
- **IEC 61800 - Adjustable speed electrical power drive systems**
  - Defines safety requirements for electric motor control such as Safely-Limited Speed
  - The use case intends to realize a subset of these (e.g. SLS, SSM, SDI)
- **IEC 62443 – Industrial Network and System Security**
  - Defines processes and security measures for networks and products
  - The use case falls into the role of a "Product Supplier".
  - Parts 62443-4-1 and 62443-4-2 are most relevant.
  - The use case motion control platform has device category PLC.
  - The use case should be compatible to the standard.

AQUAS SAFETY SECURITY PERFORMANCE

Space Multicore Architecture

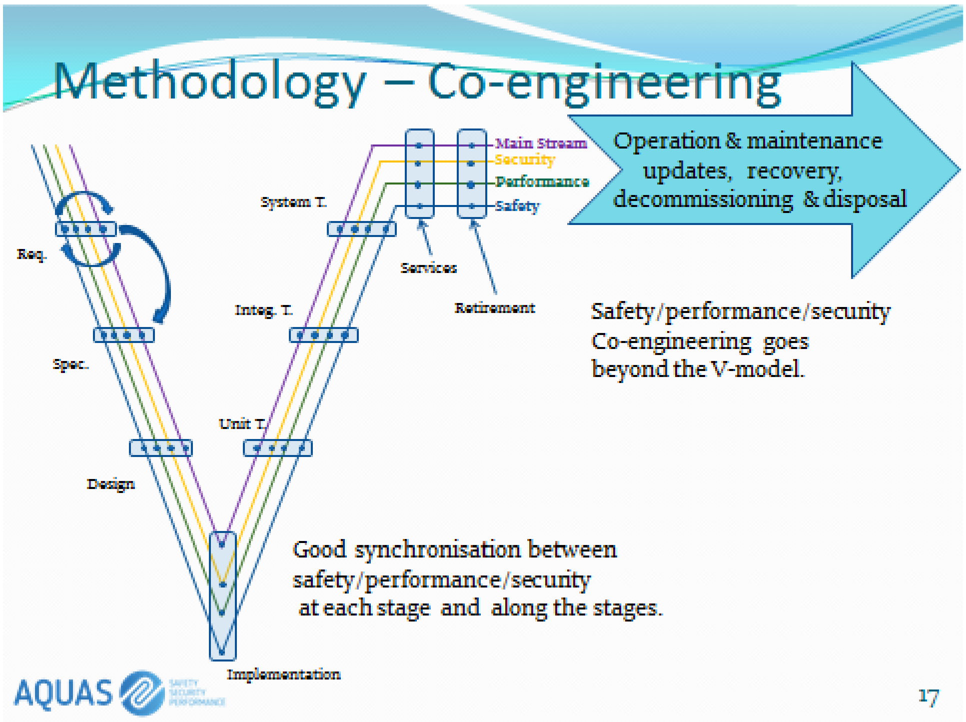
Space Multicore Architecture

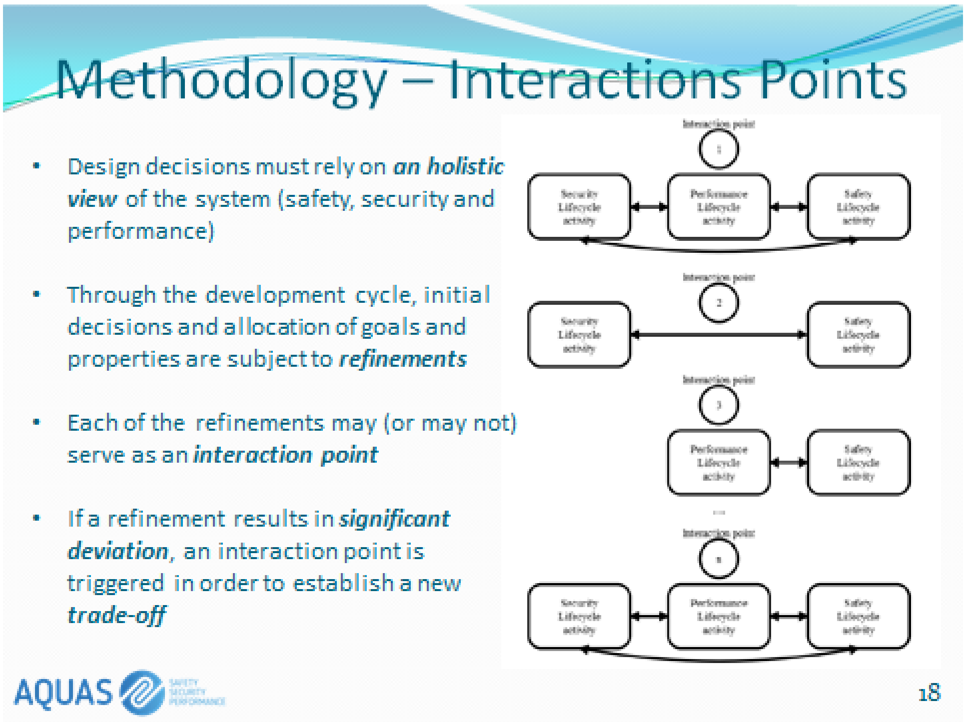
- Space projects are composed of three main components, those being Payload, Operations Center and Ground Segment.
- > UC5 will develop as demonstrator an architecture based on an integrated multicore, high performance module for the Payload. Safety, Security and Performance have to be evaluated with the environmental constraints of an orbiting piece of hardware/software.
- Software is not extremely complex, as it is not easily updated/upgraded and it must not fail.
- Safety, Security and Performance standards for a Space Project are currently segregated in different ECSS standards
- > UC5 aims to study and improve the interdependency of Safety, Security and Performance throughout the Life Cycle of a Space Project, which are currently defined in segregated ECSS standards and considered separately. Studying the relationship could lead to unifying standards and improving the consideration of these aspects along the whole Product Life Cycle.

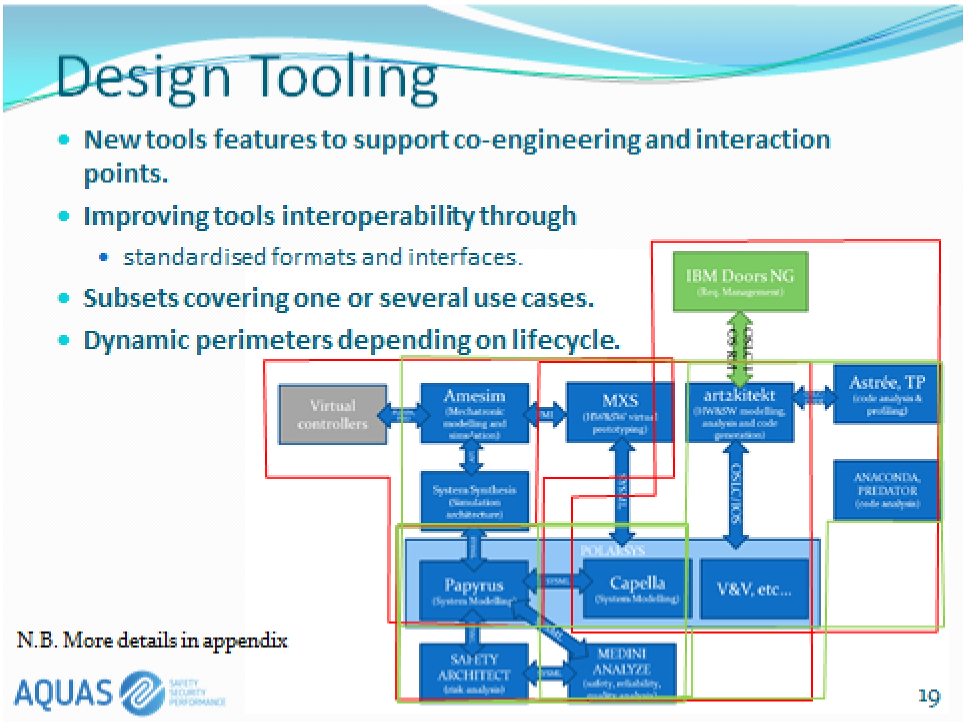


AQUAS SAFETY SECURITY PERFORMANCE 15

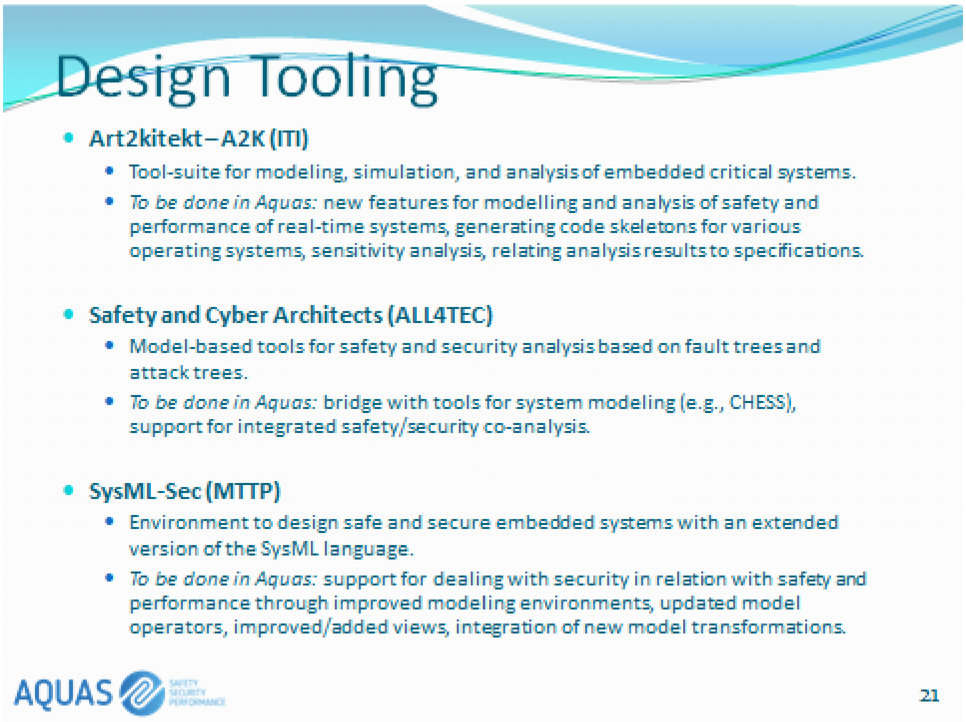

Space Multicore Architecture
Relevant Safety/Security/Performance Standards and Guidelines
Safety Standards
Safety and Dependability (SW reliability, availability and maintainability) are defined in ECSS-Q-ST-40 and ECSS-Q-ST-30 standards. These documents contain the definition, but there is also a guideline on how to apply them which is ECSS-Q-HB-80-03. One of the fundamental methods of assessing the Dependability and Safety of a software product is a Software FMECA (Failure Mode, Effects and Criticality Analysis).
Security Standards
The ECSS-E-ST-40C and ECSS-Q-ST-80C require the identification and definition of security requirements in the software specification; however, as security can be a broad subject, they do not offer a guideline for specific cases, it depends on the field of application of the SW
Performance Standards
For UC5, there are no performance control systems in the broad sense of the word; therefore, only SW execution, scheduling and parallel computation are to be considered. For real-time software, it is necessary to perform a schedulability analysis, that verifies that all tasks can meet their deadlines.
In addition, it is necessary to ensure that shared resources are protected and that there are no parallel computing issues that might affect the correct functioning of the SW product, e.g. deadlocks, starvation, race conditions, etc...
AQUAS

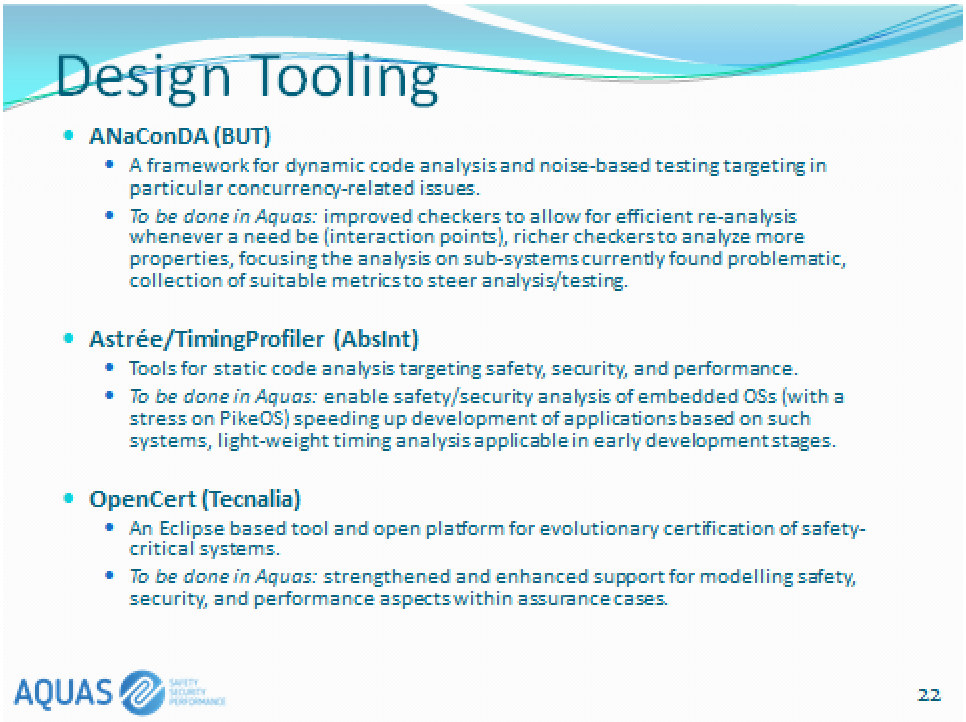

Methodology – Co-engineering
Operation & maintenance
updates, recovery,
decommissioning & disposal
Main Stream
Security
Performance
Safety
System T.
Services
Retirement
Req.
Integ. T.
Spec.
Unit T.
Design
Implementation
Safety/performance/security
Co-engineering goes
beyond the V-model.
Good synchronisation between
safety/performance/security
at each stage and along the stages.
AQUAS
17

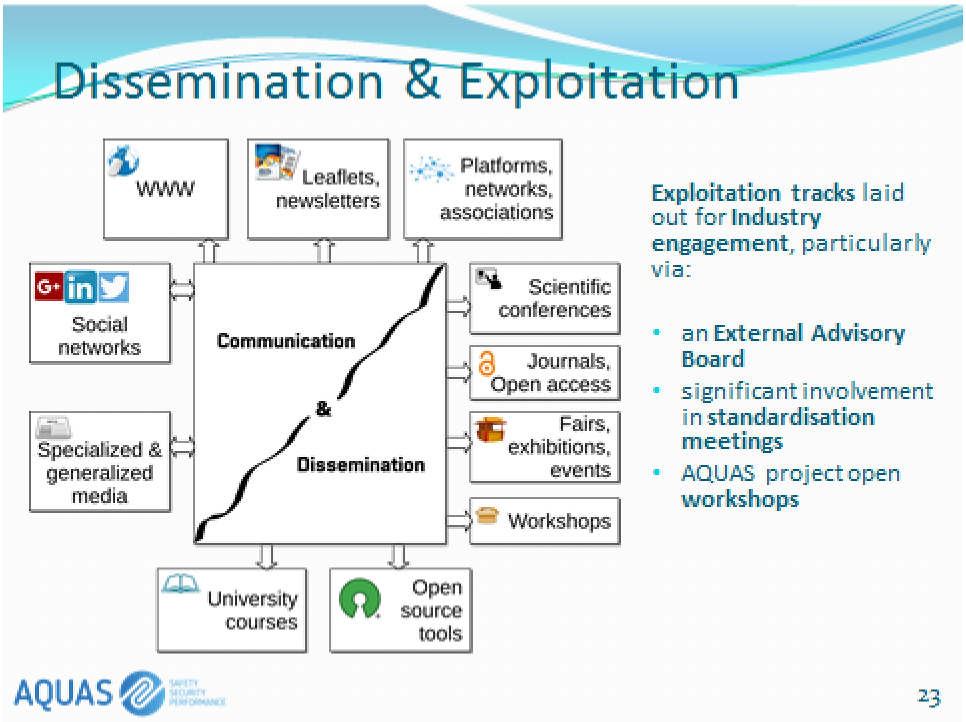

Methodology – Interactions Points
Design decisions must rely on *an holistic view* of the system (safety, security and performance)
Through the development cycle, initial decisions and allocation of goals and properties are subject to *refinements*
Each of the refinements may (or may not) serve as an *interaction point*
If a refinement results in *significant deviation*, an interaction point is triggered in order to establish a new *trade-off*
Interaction point
Security Lifecycle activity
Performance Lifecycle activity
Safety Lifecycle activity
AQUAS
18

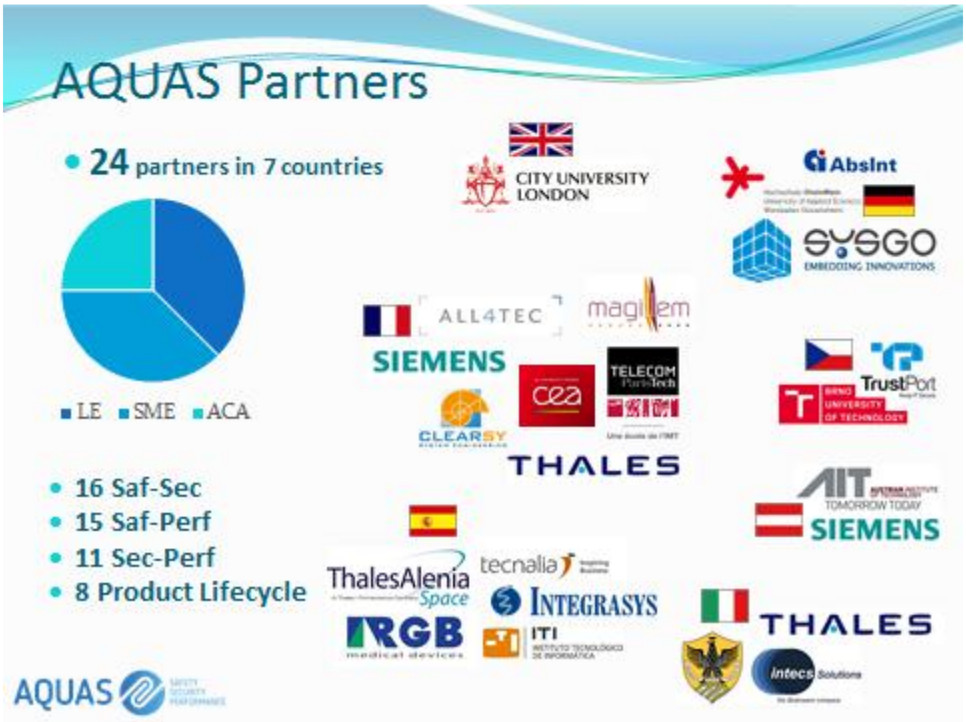

Design Tooling
New tools features to support co-engineering and interaction points.
Improving tools interoperability through
standardised formats and interfaces.
Subsets covering one or several use cases.
Dynamic perimeters depending on lifecycle.
IBM Doors NG
Virtual controllers
Amesim
MXS
art2kitekt
Astrée, TP
ANACONDA, PREDATOR
System Synthesis
POLARSYS
Papyrus
Capella
V&V, etc…
SAFETY ARCHITECT
MEDINI ANALYZE
N.B. More details in appendix
AQUAS
19

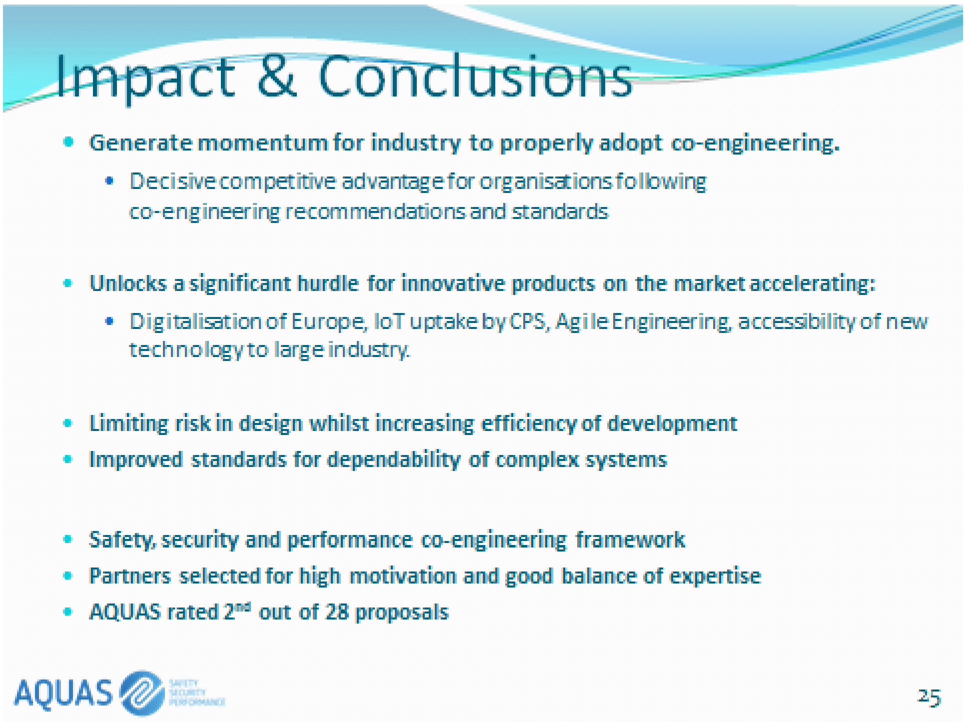

Design Tooling
New tools features to support co-engineering and interaction points.
Improving tools interoperability through
standardised formats and interfaces.
Subsets covering one or several use cases.
Dynamic perimeters depending on lifecycle.
Examples of Involved Tools and Their Improvements
CHESS (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.
AQUAS
20


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.
AQUAS
21


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.
AQUAS
22


Dissemination & Exploitation
WWW
Leaflets, newsletters
Platforms, networks, associations
Social networks
Communication
&
Dissemination
Scientific conferences
Journals, Open access
Fairs, exhibitions, events
Workshops
Specialized & generalized media
University courses
Open source tools
Exploitation tracks laid out for Industry engagement, particularly via:
an External Advisory Board
significant involvement in standardisation meetings
AQUAS project open workshops
AQUAS
23


AQUAS Partners
24 partners in 7 countries
LE
SME
ACA
16 Saf-Sec
15 Saf-Perf
11 Sec-Perf
8 Product Lifecycle
CITY UNIVERSITY LONDON
AbsInt
SYSGO
EMBEDDING INNOVATIONS
ALL4TEC
magillem
SIEMENS
cea
TELECOM ParisTech
CLEARSY
THALES
TrustPort
AIT
TOMORROW TODAY
SIEMENS
ThalesAlenia Space
tecnalia
INTEGRASYS
RGB
medical devices
ITI
THALES
intecs Solutions
AQUAS


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 2nd out of 28 proposals
AQUAS
25

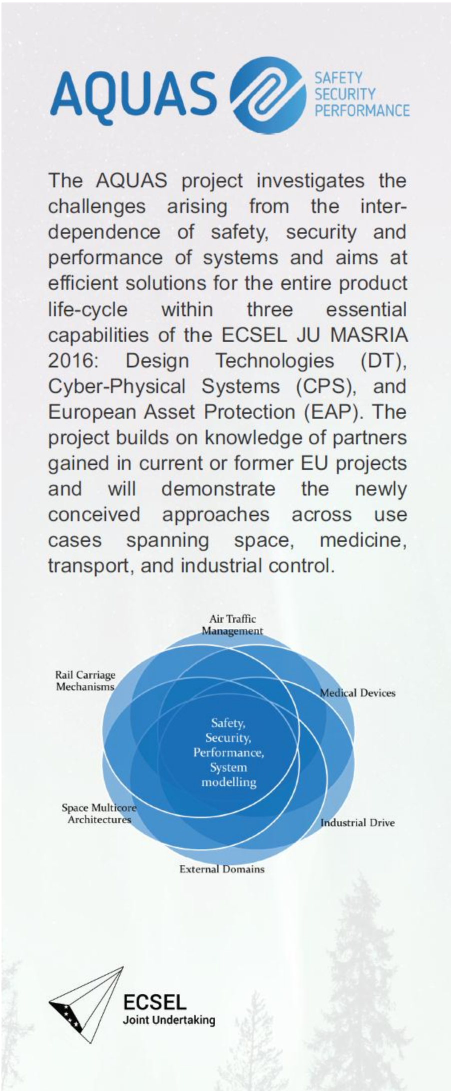
AQUAS Partner Acronyms

TASE Thales Alenia Space Espana, SA - project coordinator
TRT Thales SA
Integrasys Integrasys SA
RGB R G B Medical Devices SA
CITY City University Of London
AIT Austrian Institute Of Technology Gmbh
UNIVAQ Universita Degli Studi Dell'aquila
SISW Siemens Industry Software SAS
MDS Magillem Design Services SAS
ClearSy Clearsy SAS
CEA Commissariat A L'Energie Atomique Et Aux Energies Alternatives
TrustPort Trustport, A.S.
MTTP Institut Mines-Telecom
Tecnalia Fundacion Tecnalia Research & Innovation
BUT Brno University of Technology
All4Tec Alliance Pour Les Technologies De L'informatique
ITI Instituto Tecnologico De Informatica
Intecs Intecs Solutions SPA
SAG Siemens Aktiengesellschaft Oesterreich
HSRM Hochschule Rheinmain
AMT Ansys Medini Technologies AG
SYSGO Sysgo AG
AbsInt Absint Angewandte Informatik Gmbh

AQUAS

2.3 Project leaflet

The leaflet briefly describes the project and its goals and provides basic contact information. It can be freely circulated to inform about the project and to promote it at workshops, trade shows, technical fairs, congresses, and other events. It is intended to be printed on both sides of a small sheet of paper (e.g., 1/3 A4):


AQUAS SAFETY SECURITY PERFORMANCE

The AQUAS project investigates the challenges arising from the inter-dependence of safety, security and performance of systems and aims at efficient solutions for the entire product life-cycle within three essential capabilities of the ECSEL JU MASRIA 2016: Design Technologies (DT), Cyber-Physical Systems (CPS), and European Asset Protection (EAP). The project builds on knowledge of partners gained in current or former EU projects and will demonstrate the newly conceived approaches across use cases spanning space, medicine, transport, and industrial control.


AQUAS will aid the technological progress required to provide solutions capable of meeting the challenges of the ever increasing complexity of the systems we engineer in modern society, which includes facing the convergence between embedded world and open world. This complexity creates increasing difficulties, particularly for safety critical systems such as the transportation, space, medical and industrial control domains. Meeting the continuously growing requirements on security and performance, while maintaining safety, requires a coordinated engineering approach. Such a coordinated engineering approach, making available leading edge design for Electronic Components and Systems (ECS) technologies, will increase the competitiveness of key European industrial domains.

http://aquas-project.eu/

Project coordinator:
Filip Veljković
filip.veljkovic@thalesaleniaspace.com
Thales Alenia Space España

3 Conclusion

In the above, we have presented dissemination material that has been created to support the AQUAS project dissemination activities so far, namely, a project poster, a project presentation using slides, and a project leaflet. All these material are expected to be updated according to the progress of the project as well as to the current dissemination needs.

We have already started a preparation of a project video by discussing its content and drawing a so-called story line. The video is, however, not ready yet. We intend to distribute this video via on-line channels. It can be used also as a support for booth presentations.

The progress of the dissemination material since the current moment will be next reported in month 21 of the project, i.e., in January 2019, and finally, in month 33 of the project, i.e., in January 2020.