2018 21st Euromicro Conference on Digital System Design

The AQUAS ECSEL Project

Luigi Pomante
Università degli Studi dell'Aquila
Center of Excellence DEWS
Italy
luigi.pomante@univaq.it

Bohuslav Křena
Brno University of Technology
IT4Innovations Centre of Excellence
Czech Republic
krena@fit.vut.cz

Tomáš Vojnar
Brno University of Technology
IT4Innovations Centre of Excellence
Czech Republic
vojnar@fit.vut.cz

Filip Veljković
Thales Alenia Space in Spain
Spain
filip.veljkovic@thalesaleniaspace.com

Pacôme Magnin
Siemens PLM
France
pacome.magnin@siemens.com

***Abstract*— There is an ever-increasing complexity of the systems we engineer in modern society, which includes facing the convergence of the embedded world and the open world. This complexity creates increasing difficulty with providing assurance for factors including safety, security and performance. In such a context, 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. The project builds on knowledge of partners gained in current or former EU projects and will demonstrate the newly developed methods and techniques for co-engineering across use cases spanning Space, Medicine, Transport and Industrial Control.**

Keywords—cyber-physical systems, safety, security, performance

I. Introduction

There is an ever-greater complexity of the systems we engineer in modern society. This includes facing the convergence of the embedded world and the open world. The complexity creates increasing difficulty to provide assurance for interrelated system quality attributes including safety, security and performance. This is particularly the case for real-time systems where human life is at stake such as in the transportation, aerospace, medical and industrial control domains. Safety, security and their relation are essential for these kinds of systems. However, their interdependence and with performance is poorly understood not least because traditionally different teams within the same organization have had responsibilities for safety and security.

Modern systems require that we sufficiently master the methods of dealing with the complexity of interacting system-level qualities to build and maintain them effectively. It is therefore of the outmost importance that we bring co-engineering into mainstream practices.

In AQUAS, the focus is on the following issues:

- safety/security/performance considered together during the overall life cycle of the products;
- flexibility across domains;
- consolidation of the industrial market by reducing costs, increasing system quality and maintaining compliance with more and more exacting standards;
- improvement of tool features and their capabilities.

The project has started on May 1st, 2017 and its duration is three years. In the following, we highlight project goals, explain selected approach, describe application domains, and discuss implementation issues.

II. Project Objectives

AQUAS will aid the technological progress required to provide solutions capable of meeting the challenges of the ever-increasing complexity of the systems. It includes facing the convergence between embedded world and open world. This complexity creates increasing difficulties, particularly for critical systems. 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. This will be done by providing solutions for a holistic approach to *Safety/Security/Performance Co-Engineering* (CE) through a domain-flexible framework, supporting the entire *Product Life-cycle* (PLC) and contributing to *Standards Evolution* (SE). These three points represent the core goals of the AQUAS project. More in detail, key outputs that we expect from this project are:

- A global concept framework for safety/security/performance co-engineering:
  - based on an analysis of the needs of industrial application domains;
  - giving support for balancing existing safety & security requirements with application specific performance requirements;
  - consisting of established tools and platforms, which will be upgraded to implement and test the

978-1-5386-7377-5/18/$31.00 ©2018 IEEE
DOI 10.1109/DSD.2018.00104

co-engineering approaches and improved processes and methods;

  - considering the complete product lifecycle and influencing the evolution of standards.

- Demonstrators derived from tools and best practices:
  - solutions for major co-engineering challenges will be tested and evaluated in use cases;
  - improvement of tool capabilities to manage co-engineering;
  - improved ability for tool integration into the product life cycle tool-chain;
  - flexibility of tools supporting co-engineering across domains;
  - improved capability of systems to recover from safety or security software and hardware problems;
  - the challenges faced and overcome fed back into the concepts framework.
- A public domain document at the end of the project describing:
  - short/mid-term challenges still to be addressed for co-engineering with recommendations;
  - identification of the long-term challenges;
  - implications for Systems of Systems.
- Improved standards for dependability of complex systems:
  - positively influencing standards with feedback based on the challenges addressed in the project and those foreseen based on results;
  - where appropriate giving our tool providers a head start on the market as the first to offer support for new dependability requirements from standards bodies.

It should be noted that for standards the timeframe for completing or updating is normally longer than the duration of a research project. Also, alongside the above objectives, a complementary action will be carried out looking at the transferability of the co-engineering results to the case of Systems of Systems.

III. CONCEPT AND APPROACH

Safety, Security and Performance are interrelated concerns for developers of dependable systems and for embedded safety-critical/related systems with hard real-time constraints. The AQUAS project builds on and extends the concepts and practices developed recently on design for safety and security (e.g. [1][2][3][4]).

Central for AQUAS is the concept of co-engineering for safety, security and performance. Tools and - even more - standard practices for analyzing these aspects - security, safety, performance - are often disjoint and unable to shed light on their interactions, e.g. whether a design change against a certain security threat will enhance or reduce safety in the absence of attacks. Thus, expensive iterations may be required before a design is found acceptable from all these viewpoints. The concept of co-engineering systems for safety, security and performance essentially means that throughout the development lifecycle there will be "interaction points" addressing simultaneously several concerns (Figure 1).

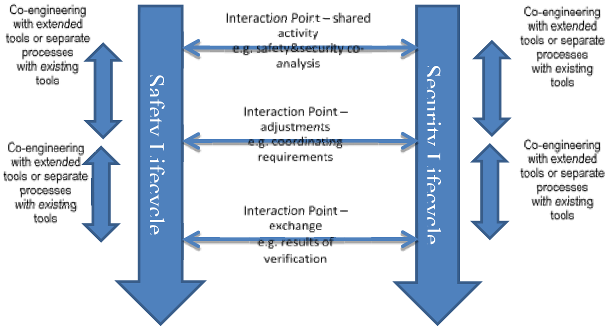
Co-engineering with extended tools or separate processes with existing tools
Co-engineering with extended tools or separate processes with existing tools
Safety Lifecycle
Interaction Point – shared activity e.g. safety&security co-analysis
Interaction Point – adjustments e.g. coordinating requirements
Interaction Point – exchange e.g. results of verification
Security Lifecycle
Co-engineering with extended tools or separate processes with existing tools
Co-engineering with extended tools or separate processes with existing tools

Figure 1: AQUAS PLC with separate/combined processes.

The point here is that during the development lifecycle, there will be points in time when the developers will take decisions about how to progress with the development. These decisions, according to the AQUAS proposed methodology, should be taken with a holistic view on the system, i.e. account simultaneously for safety, security and performance. The decisions at the level of requirements will concentrate on defining the preliminary architecture and the functional and non-functional requirements about the system safety, security and possibly performance (e.g. in case system response time is a concern) about the high-level requirements, apportionment of goals to the components used in the preliminary architecture, etc.

These initial high-level decisions ideally should be based on an analysis whether the safety, security and performance goals are achievable together. The analysis will provide an insight about the needed compromises (trade-offs) between the goals and how these system wide goals should be achieved by allocating requirements on the properties (e.g. reliability/availability, security controls and performance indicators) to the components envisaged in the preliminary architecture. At later stages of development, the initial decisions and allocation of goals and properties are subjected to refinements and each of the refinements may serve as an interaction point. If because of some refinement significant deviations from the previous allocation of the goals/properties are detected, then an interaction point will be triggered so that a new trade-off is established between the assigned goals and component properties.

The methods of analysis, which will be needed at each interaction point, will be dependent on the context. We envisage that the analysis will be supported by a range of tools appropriate for the context. The tools will also range in terms of the level of detail that they operate at: e.g. from tools for building and solving probabilistic models such as Mobius [6], which operate typically at system level, to tools suitable for more detailed analysis, such as CHESS [7], static analysis of the source code, etc. We envisage that a combination of tools, provided by the partners in the consortium, will be needed at most of the interaction points.

This process of co-engineering for safety, security and performance using interaction points requires a clear coordination between the personnel responsible for the concerns, which in turn may require organizational changes, e.g. delegating the combined analysis at interaction points to a "co-engineering" team. Industry so far has been quite reluctant to adopt a similar idea and the "silos" (e.g. safety and security) are well established and difficult to overcome. If the organizational difficulty, however, is overcome in part thanks to the improved tools facilitating the joint analysis required by the interaction points, then co-engineering promises several benefits:

- Despite the appearance that the process being iterative and may require multiple interaction points of analysis with their associated costs, we expect that some savings will be possible in comparison with having security, safety and performance largely done independently. This hope is justified, as at least to some extent avoiding duplication of the effort in analysis will be possible when combined analysis is undertaken. In other words, co-engineering offers scope for more cost-effective development. The project will collect data on savings and share them widely.

- Applying combined analysis during the interaction points offers scope for finding better trade-offs between safety, security and performance, than would be possible if the analysis of safety, security and performance is done by separate teams with limited communication between them. The fact that during the interaction points a holistic analysis is applied will give the developers and managers higher confidence that the found trade-off is better than if the solutions were achieved focusing on a single concern at a time, e.g. only on safety or only on security or only performance. This confidence will come from the fact that the search for good trade-offs has been sought systematically exploring the space of possible trade-offs of all three dimensions – safety, security and performance.

- Finally, the concluding phase of a development is Validation, which may include assessment and/or compliance with standards. The regimes for assessment/compliance vary greatly by industrial domain with a number of relevant standards. If the process of co-engineering is documented adequately, the output from the analysis done at the different interaction points will provide evidence, which can be fed into the validation (assessment/compliance) activities according to the respective industry domain regime. For instance, building an assurance case using the *Claim, Argument, Evidence* (CAE) framework [5], will naturally use the results from the interaction points as evidence.

This systematic generation of evidence and its direct coupling with the assurance case will contribute to its becoming a living artefact, capable of evolving together with the system and preserving assurance/compliance status.

IV. Domain Environments to Realize Project Goals

Co-engineering techniques and tools for safety-security-performance have yet to significantly take off for a variety of reasons described in previous sections. AQUAS aims to bridge the many resistances between specialists' domains and bring co-engineering into mainstream practice. Demonstrators from across many domains are key for the leverage needed to achieve this and to prove validity and value. AQUAS has five domains (Figure 2) which like the consortium were selected for balance (there were initially 12 proposed use cases), with differing focal points in the product life cycle. They cover transport infrastructure, health, satellite systems and manufacturing. All use cases are based on CPS and at least two of them (i.e., ATM, Railways) deal with the design of typical "constituent systems" of *Systems-of-Systems* (SoS). Also, some SoS concerns (e.g., long lifetime, evolution after entry into service, multiple stakeholders) are shared by all 5 domains. The demonstrators are described in the following sections, providing a domain market analysis, details of each use and finishing with the expected impact on their business and generally on the market.

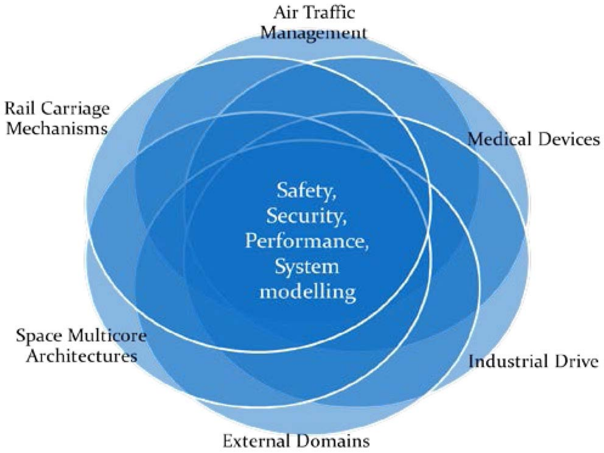

Figure 2: Co-engineering reinforced by many domains.

A. *Air Traffic Management*

The use case in which *Integrasys* (ISYS) applies and evaluates the AQUAS technology is focused on the customization of SWIM (*System Wide Information Management*) services. We intend to establish several requirements that may be tagged as Safety requirements and thus have some impact in the co-engineering process. These requirements are mainly related to the implementation of mixed criticality architectures. The safety requirements are established at the high level (architecture level) and are mainly entrusted to the Operating System level (certified hypervisor layer and RTOS). In such architectures, the isolation of different partitions allows to define different and independent performance and security requirements for each partition.

The concept of SWIM covers a complete change in paradigm of how aeronautical information (flight trajectories, meteorological, surveillance, air traffic flow, etc.) is managed along its full lifecycle and across the whole European ATM (*Air Traffic Management*) system, and how these systems communicate with each other. The goal is to move from system-centric to information-centric operations and to achieve global interoperability by defining new standardized services and data models implemented upon *Service Oriented Architecture* (SOA) and open and standard mainstream technologies. Therefore, the ATM industry is making a great effort to switch from legacy and closed systems to a whole plethora of interconnected systems sharing information through SWIM.

In this sense, security is a major concern and SWIM, as the main ATM information management layer, needs to offer solutions for it (service access control management, encryption of data, etc.). Currently, the adaptation of legacy systems to SWIM concepts and operations is being implemented mainly in the ATM ground systems, but some research is being already done in the airborne segment. Several years ago, ISYS implemented a SWIM compliant Real Time Communication middleware for ground systems, but in recent years, they have been exploring also the implementation of the SWIM concepts in the airborne segment. The different requirements for this constrained environment force us to completely change the architecture and implementation approach of existing SWIM layer profile. The nature of this layer, which might be thought of as a middleware layer, forces us to develop also some legacy applications that demonstrate to our clients the full benefits of applying the SWIM concepts to airborne platforms and applications.

However, the different requirements imposed by different airborne applications require also defining different profiles of the SWIM layer. In this sense, the ISYS use case in AQUAS considers airborne applications where the performance, security and safety are relevant properties of the whole system. Specifically, the applications that will be exploited by the SWIM layer in AQUAS are related to surveillance and navigation systems and will be used to build a SWIM-enabled situational awareness service for a simulated UAV (*Unmanned Aerial Vehicle*).

In a UAV, the space and weight of the systems on-board play a critical role, so we intend to apply the IMA (*Integrated Modular Avionics*) concept to deploy all the systems in the same embedded board. Following this architecture, several systems with different levels of safety need to co-exist and share the resources of the board, thus normally requiring a clear separation of time and space. In such architectures the co-engineering becomes especially important and critical; balance between different non-functional properties need to be assured. In the ISYS' use case we will focus on the performance-security trade-off, but without neglecting safety requirements and possibly others like energy efficiency or resource utilization.

Among other properties, the SWIM concept includes service design and run-time security controls to enforce security policies at the service and message level. Some of those security requirements include providing authorization-based access to data and services, boundary protection or cryptographic key services. At ISYS we have been working the last years on developing a SWIM profile for air to ground communications. Such profile needs to consider the non-functional properties inherent to the physical, operational and governance aspects of the avionic systems. Up to now we have focused on some of those properties, such as performance, power aware, safety, real-time metrics, etc.

However, security is one of those key aspects that we have not explored yet. This way, we intend to take advantage of the technology to be created in AQUAS to integrate and evaluate in our existing SWIM profile different security approaches and techniques, analyzing at the same time the impact on performance while maintaining the required levels of safety. Security aspects are considered to protect the integrity of the data and to guarantee the authenticity of the transmitters.

B. Medical Devices

In this context, *RGB Medical Devices* has developed and CE marked a neuromuscular transmission (NMT) device for *Hospital Operating Room* critical care performance. This device is using a very innovative technology to support the anesthesiologist in controlling muscle relaxation during an operating room intervention. Muscle relaxation is, together with depth of anesthesia and pain the three key parameters to be controlled by the anesthesiologist. The company is now confronted with the challenge to develop a closed-loop controller for muscle relaxation that will perform in AUTOMATIC PILOT mode. This is the use case we provide to AQUAS.

An experience gained in the process of these products has been the understanding of the enormous effort required in the verification and validation stages to obtain required safety and security levels through the life-cycle of these complex products. In our case, RGB has already developed the hardware. It is composed of two different components that integrate the features mentioned above: NMT monitor and injection pump tree. The system will deliver drugs with the ultimate goal of keeping the muscle relaxation at the required level during each stage of the operation. The device performance requires diagnosis and therapeutic capabilities to provide means for enhancing patient care and safety. The system should also be interoperable with the HIS (*Hospital Information System*), and security issues arise.

The proposed use case has the following alignment with AQUAS goals:

- Safety, Security and Performance considerations:
    - model of SW (control algorithm) embedded in existing NMT controller HW to reduce development time and costs;
    - model of patient to avoid clinical trials in the first stage;

- tools to comply with requirements specification and validation processes of the V-Model in development cycle;
- communication between the different components of the system must be secure, with robust communication protocols that do not compromise the integrity of the system;
- use of verification and validation tools to gain performance evidence in test cases which cover most possible real situations in real life.

- Standardization

  As result of the mentioned work, it will be possible to detect and propose improvements in standardization issues. In particular:

  - norms related to interoperability between medical devices such as IEEE11073 (section on remote control and security);
  - SW development of medical equipment (EN 62304);
  - co-lateral norm EN 60601-1-10 applied in closed –loop control systems.

- Cross Fertilization

  This type of Medical application has a great deal of things in common with regards to space and transport use cases, in terms of:

  - technology for model-based engineering;
  - managing complexity, safety & security;
  - managing diversity;
  - increase yield, robustness and reliability, generate system openness.

C. *Rail Carriage Mechanisms*

ClearSy has developed several safety systems controlling the opening and closing of the *Platform Screen Doors* (PSD) installed in Metro stations to insure passengers' protection. These systems have the advantage of being independent of the train signaling and automatic operating systems; they can be installed in a Metro which is already in service. They offer a speed of execution which seems instantaneous (simultaneous opening of train doors and PSD). Safe functioning is guaranteed by the Level 3 and 4 SIL Standards depending on the system, such as Lines 1 and 13 of the Paris Metro and Lines 2 and 3 of the Sao Paulo Metro. PSD are deployed all over the world in particular on driverless new lines, and also on modernized existing lines. ClearSy has developed independent systems, without necessity to install CBTC (Communication based Train Control), and for controlling automatic platform gates with a short delay of 300 milliseconds.

ClearSy develops both hardware and software of these systems in conformance with EN50126, 8&9 standards, including devices for fine-tuning sensors and supervision facilities. Being operated remotely, these systems must provide both safety and security functions that require cross-domain skills and knowledge and dedicated/diverse engineering tooling. The case-study perfectly fits with the AQUAS needs as railways systems must deliver a function with a given level of safety/security and within a time window.

These systems are real CPS, using various sensors (radar, laser, IR, etc.) for measurement, performing signal processing/pattern recognition/decision functions, and commanding actuators. Our systems are most of the time developed in 6 to 12 months, every new system being new (very limited reuse). They are operated remotely, mainly for maintenance. Improvements of the development cycle are expected right after the end of the project with the integration of one or several features developed and adapted during the lifetime of the project. Main expectations are to reduce development time by using improved system level tools) and to reduce guarantee costs (by limiting unexpected behavior during exploitation).

D. *Industrial Drive*

Motion Control products cover a large variety of variable frequency inverters for synchronous and asynchronous motors ranging from standard electric motor systems and servomotors for Motion Control applications including linear and torque motors to motors for use in hazardous explosion areas, to high voltage, DC and customized electric motor systems.

The Industrial Drive use case focuses on a generic commercial motion control platform solution for permanent magnetic synchronous motors (PMSM). Typical application is within e.g. tooling machines. Since this application is based on a generic control reference platform it is also possible to target applications in similar domains like Electric Drive Trains in automotive.

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 control products, where the most relevant standards are IEC 61508 and IEC 61800. Industrial automation systems are more and more moving away from an isolated operation island towards interconnected systems, in order to let companies make fast and cost-efficient decisions, based on accurate and up-to-date information about the processes under control.

The use case originates from the Artemis SESAMO project [8], where safety and security interdependencies were in focus. Besides safety and security also real-time performance is an essential criterion within this cost driven and competitive domain. This makes the Industrial Drive a perfect demonstration example for the technology developed within AQUAS.

The demonstrator shall elaborate enhancements to the current design flow, which will increase productivity and quality for future products:

- System Modelling

  - The methodology elaborated in *SESAMO* shall be enhanced with performance considerations in early stages. In particular, the CHESS tool shall be extended with code generation features and WCET analysis capabilities.

- Virtual Prototyping
  - Even though virtual HW prototyping for SW development is common industrial practice, the usage for verification of safety features is not yet state of the art. In AQUAS we work on a seamless flow from System Level Model to the Virtual HW Prototype. Since the FPGA (*Field Programmable Gate Array*) based demonstrator from SESAMO is available, a direct comparative analysis of VP vs. FPGA approach (effort, benefits, accuracy) shall be conducted.

- Safety-Security Analysis
  - We want to evaluate applicability of the FMVEA (*Failure Mode Vulnerability and Effects Analysis*) for combined safety and security analysis.

- Certification Support
  - We will use WEFACT (Workflow Engine for Analysis, Certification and Test) in this demonstrator as framework for supporting a general assurance case covering all relevant dependability attributes (safety, security and performance).

E. *Space Multicore Architectures*

Design of data handling systems and data processing systems for space applications is currently introducing technologies quite new to the space market as multi-core processors or SoC (System-on-Chip). In the space business, the SoC are newcomers that are entering the market at an extremely slow speed, especially when compared with the promised advantages that such systems may bring in terms of performances improvement. The main reason for this small adoption ratio is the criticality of the space borne systems and the associated validation and certification procedures. One of the elements blocking this certification is the lack of adequate tools for managing the complexity and mixed criticality of such systems. There is a lack of methodologies and tools to support the exploitation of these new technologies in the scope of systems which are compliant to the strict requirements of performance under critical conditions, safety, timeliness, security and reliability peculiar to the space applications.

The target of this use case is to proof the validity of the different architectures and a related development methodologies and tool chains proposed by AQUAS project and previous projects such as *OPENCoss* [9] and *NsafeCer* [10], opening new application domains to the use of multicores. This use case is clearly targeted to a final product application and, therefore, it must be guaranteed not only compliance with the functional requirements, but also, to the applicable space standards such as the *European Cooperation for Space Standardization* (ECSS) family of standards for Space Software (ECSS-Q-80 and ECSS-E-40) peculiar to space applications, pushing forward these requirements pointing to the larger flexibility provided by heterogeneous systems.

The use case of *TASE* (*Thales Alenia Space Espana*) is mainly focalized in including multicore architectures capable of in-flight reconfiguration in actual payload data processing equipment for video processing in Earth Observation missions. The target is to replace legacy designs in present flight missions using multicore improved performances to overcome the limitations imposed by classic ASIC (*Application Specific Integrated Circuits*) designs. To achieve this, TASE needs to define the requirements derived from actual mission scenarios in terms of performances, safety, security and certification needs and to support the architecture definition and validation activities. Once selected the architectures, TASE will implement them in the available processing modules based on the multicore elements both HW and SW. The reconfigurability of the proposed solution brings into the use case the need to manage variability and lifecycle for the different versions and evolutions of the SW and the synthetized HW considering that some of these versions will be loaded and modified during flight operation of the satellite.

This use case is focused on the multicore architectures available in the market and the possibilities of implementing them in *Space Worth* systems that can withstand the space environment and that can follow the stringent design rules specified for Space equipment. In the same way, in-flight reconfiguration techniques either by SW modifications for LEON processor-based architectures or by FPGA reconfiguration for *Xilinx Zynq* platforms are considered.

The core of the proposed architectures will be the processor selected by the European Space Agency for the next generation of data handling systems for space applications, i.e. the LEON3 FT which is based on a SPARC-V8 RISC architecture. This processor will be used as base to implement the Scalable Sensor Data Processor Breadboard (SSDP) architecture already under development for ESA (*European Space Agency*) to satisfy the needs of the applications that request the fast processing of a high amount of data for smart sensors to be used in future space exploration missions. This architecture combines fixed point DSP IP with a LEON controller. The inherent scalability of the *Network-on-chip* (NoC) architecture, as well as the efficient combination of GPP (*General Purpose Processor*) and DSP (*Digital Signal Processor*) cores are very interesting for future large and ultra-powerful processor ASICs, however, a strict validation and certification strategy will be key to allow the widespread usage of such a powerful device in different scenarios with very different criticality constraints.

For demonstration purposes, the following SW architecture for Video Compression is considered: the proposed solutions will be used to recode and test the performances of Video Compression algorithms commonly used in the space domain, such as CCSDS122 and 123 which are spatialized versions of the JPEG2000 standards. Being a multilayer compression algorithm, it is prone to be parallelized into an MPSoC (*Multi*

Processor System-on-Chip) structure and, as such, AQUAS results should show a clear impact on the overall validation and certification of the algorithm. A typical SW architecture of the proposed algorithms is prone to parallelization and modularization and as such can be easily linked to in flight reconfiguration procedures to adapt it to the particularities of the processed images as well as to the evolution of customer needs.

The different elements developed in the technical tasks will be implemented in the corresponding test benches, one for LEON processors and other for Reconfigurable FPGA, implementing the proposed architectures and certification procedures. These test benches will be designed to reproduce as close as possible the actual environmental and operational conditions that will be found in an actual commercial space project to guarantee representatively. The proposed co-engineering techniques and procedures will be compared against previous solutions in the space domain as well as against state of the art solutions in other domains.

A final test report will be prepared including all the information generated during the test and an evaluation of their acceptability and compliance against the ECSS Space standards.

V. Implementation

A. *Work plan — Work packages, deliverables and milestones*

The work structure and responsibilities of AQUAS are broken down into work packages and tasks. Before detailing these, an overview is provided in the following by means of Figure 3 showing their interactions. It is important to note that this is where the AQUAS management diverges from the traditional WP structure. The work packages 2, 3 and 4 should not be interpreted as the more common implementation in projects where partners divide their work on concept/tool/demonstrator development. A different approach has been taken in AQUAS to encourage a more collaborative and use case driven environment to maximize domain impact: none of the work should be done without some reference to the use cases. For this purpose, the demonstrator is not part of any WP but has been explicitly defined as a collaborative result between WP2/WP3/WP4. This helps to avoid work arising unrelated to the demonstrators. Management of the demonstrators is provided by WP2 along with provision of the use cases definitions, requirements and analysis/testing of the technologies. Methodology and design tool providers equally contribute to the demonstrators through their work in WP3 and WP4.

Partners are distributed across WP2/WP3/WP4 specifically in terms of associated collaborative tasks. This is in terms of collaboration within a WP and to other WPs. As a result, many partners are positioned only on one WP meaning inter-WP collaboration is essential. It is expected that there will be some methodology and tooling development by individual partners that does not require collaboration, but this can fit in either WP2/WP3/WP4 because it is independent and not manageable at WP level.

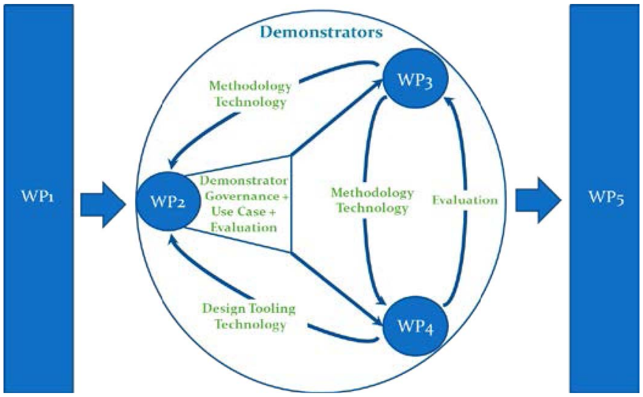

Figure 3: Interaction between Work Packages

B. *Consortium as a whole*

The initial impetus for the AQUAS consortium formation came from the projects SESAMO [8] and MERGE [11] each having tasks specific for co-engineering. Coming from these projects a *decision steering committee* (DSC) was formed with two members from each Project. The DSC has been charged with taking votes on proposal direction and consortium constitution to maximize the project effectiveness in achieving our results.

Co-engineering needs a technology rupture to pull away from the traditional compartmentalized engineering approaches. It needs long-term sustainable support, which is difficult across industry (where goals can change every 3-4 years as people change jobs). There is also a need to have a sufficient critical mass of organizations working together with this objective to push the market in the right direction.

The demand for co-engineering solutions is increasing rapidly as evidenced following a brokerage event with over 60 organizations wishing to participate in such a project. To ensure optimum cohesion with the project goals, whilst also gathering sufficient organizations together, it was believed we should not pass 20-25 partners. A short questionnaire was circulated requesting data about each organization's background and work interests within the scope of AQUAS. Approximately two thirds responded which the DSC evaluated and selected partners to balance:

- Research, SME, Industry
- Safety, security and performance expertise
- Tools, concepts and use cases
- Product lifecycle expertise and positioning
- Ability to affect standards
- Management capacity
- The scope of domains they could address

Also, to an extent the motivation and organizational capacity has been considered. The target number of AQUAS partners was achieved with a good distribution of expertise and work interests.

With this fair balance, the next driving factor has been the integration of all the organizations. This commenced by fusing and distributing the initial information from the organizations enabling everyone to review the expertise of other partners and identify their synergies, particularly with the use cases. Given co-engineering for safety, security and performance covers a vast spectrum of domains and disciplines, this phase was important for identifying exactly where our strengths lay and to generate refined objectives based on the project goals.

Just as we limited the size of the consortium, the domains addressed were also limited – maximizing impact is a trade-off between advancing in a sufficient number of domains, whilst keeping a sufficient number of partners on each domain to build momentum. The selection of the use cases was based on their work focus alignment with the competence of other partners as well as having sufficient domain diversity and coverage of the three core goals. The expertise of partners has also been carefully aligned with the needs of the use cases.

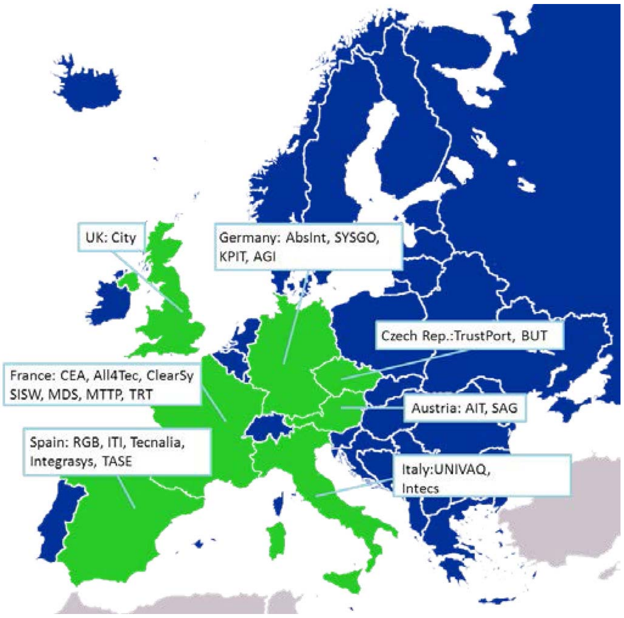
UK: City
Germany: AbsInt, SYSGO, KPIT, AGI
Czech Rep.:TrustPort, BUT
France: CEA, All4Tec, ClearSy SISW, MDS, MTTP, TRT
Austria: AIT, SAG
Spain: RGB, ITI, Tecnalia, Integrasys, TASE
Italy:UNIVAQ, Intecs

Figure 4: Country distribution.

Of equal importance to having sufficient spread across domains is having a suitable partner distribution across Europe. Within AQUAS we have organizations coming from seven countries: Italy, Austria, the Czech Republic, Germany, the UK, France and Spain. The spread of partners is indicated in Figure 4. Having cooperation across European countries is critical for bringing the practice of co-engineering into the mainstream development processes for the markets of each country. This form of collaboration is needed to ensure we can build sufficient moment.

VI. Conclusions

This paper has presented the AQUAS ECSEL JU project. It 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. The project builds on knowledge of partners gained in current or former EU projects and will demonstrate the newly conceived approaches to co-engineering across use cases spanning Space, Medicine, Transport and Industrial Control. As the paper is written after the first year of the project, it concenrates rather on the project introduction while project results – expected mainly in the field of co-engineering – will be presented later.

Acknowledgment

A special thanks to all the AQUAS consortium people that have worked on the AQUAS proposal on which this paper is based on, especially to Charles Robinson (TRT), the proposal coordinator, and to Martin Matschnig (SAG), the demonstrator's leader. The AQUAS project is funded from the ECSEL Joint Undertaking under grant agreement n° 737475, and from National funding.

References

[1] M. Steiner and P. Liggesmayer, Combination of safety and security analysis-finding security problems that threaten the safety of a system, 2013.

[2] S. Paul and L. Rioux, "Over 20 Years of Research in Cybersecurity and Safety Engineering: a short Bibliography," in 6th International Conference on Safety and Security Engineering (SAFE)., Opatija, Croatia, 2015.

[3] J. Brunel, D. Chemouil, L. Rioux, M. Bakkali and F. Vallée, "A Viewpoint-Based Approach for Formal Safety & Security Assessment of System Architectures.," in in 11th Workshop on Model-Driven Engineering, Verification and Validation, Spain, 2014.

[4] J. Osborne, "Survey of Concurrent Engineering Environments and the Application of Best Practices towards the Development of a Multiple Industry, Multiple Domain Environment" (2009). All Theses. Paper 635," in All Theses, vol. Paper 635, T. Prints, Ed., 2009.

[5] Adelard. Claim, Arguments, Evidence. Available from: http://www.adelard.com/asce/choosing-asce/cae.html.

[6] Mobius, https://www.mobius.illinois.edu/

[7] CHESS, http://www.chess-project.org/

[8] SESAMO, http://sesamo-project.eu/

[9] OPENCoss, http://www.opencoss-project.eu/

[10] NSafeCer, https://artemis-ia.eu/project/40-nsafecer.html

[11] MERGE, http://www.merge-project.eu/