Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

The AQUAS ECSEL Project Aggregated Quality Assurance for Systems: Co-Engineering Inside and Across the Product Life Cycle

Luigi Pomante[a,*], Vittoriano Muttillo[a], Bohuslav Křena[b], Tomáš Vojnar[b], Filip Veljković[c], Pacôme Magnin[d], Martin Matschnig[e], Bernhard Fischer[e], Jabier Martinez[f], Thomas Gruber[g]

[a] Università degli Studi dell'Aquila, Center of Excellence DEWS, Italy
[b] Brno University of Technology, IT4Innovations Centre of Excellence, Czech Republic
[c] Thales Alenia Space in Spain, Spain
[d] Siemens PLM, France
[e] Siemens AG, Austria
[f] Tecnalia, Spain
[g] AIT Austrian Institute of Technology, Austria

ARTICLE INFO

Article history:
Received 21 January 2019
Revised 6 May 2019
Accepted 28 May 2019
Available online 31 May 2019

Keywords:
Cyber-physical systems
Safety
Security
Performance
Co-engineering
Product life-cycle

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 e.g., 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 Aerospace, Medicine, Transport and Industrial Control.

1. Introduction

System safety considerations have a very long tradition. As an early example, the classical bottom-up safety analysis method FMECA (*Failure Modes, Effects and Criticality Analysis*) was developed by the US Department of Defense in the 1940s, and the top-down method FTA (*Fault Tree Analysis*) was invented by Bell Laboratories in the early 1960s. Guidance comes also from safety norms since long ago; the generic Functional Safety standard IEC 61508 [1] was issued in 1998, and many others followed. None of the functional safety standards, however, gave detailed guidance on how to treat potential security risks. Security was, if at all, only mentioned in a small remark. Instead, it was assumed that safety-critical systems are separated from the outside world preventing potential attackers from compromising them. Today, however, also safety-critical systems are more and more integrated in networks and, thus, the old paradigm of isolated systems is not longer valid (e.g., *Industry 4.0* [2]), and attackers can target safety-critical functions in a dangerous way. The risk is real as events like the attacks to the SCADA system at nuclear facilities in Iran [3], the steel mill attack in Germany [4], or attackers causing power outages in Ukraine [5] prove. Security considerations are therefore indispensable also for safety-critical control systems.

Moreover, 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 and security interdependence, and with performance, is poorly understood not least because traditionally different teams within the same organization have had responsibilities for safety and security.

It is acknowledged that security is usually a requirement in order to ensure safety [6], but still standardization for safety and

[*] Corresponding author.
E-mail addresses: luigi.pomante@univaq.it (L. Pomante), vittoriano.muttillo@univaq.it (V. Muttillo), krena@fit.vut.cz (B. Křena), vojnar@fit.vut.cz (T. Vojnar), filip.veljkovic@thalesaleniaspace.com (F. Veljković), pacome.magnin@siemens.com (P. Magnin), martin.matschnig@siemens.com (M. Matschnig), bernhard.bf.fischer@siemens.com (B. Fischer), jabier.martinez@tecnalia.com (J. Martinez), thomas.gruber@ait.ac.at (T. Gruber).

https://doi.org/10.1016/j.micpro.2019.05.013

security is mostly separate. Safety experts and security experts are traditionally regarded as distinct groups which “think differently”, they even “speak different languages”. This causes misunderstandings and lack of integrative treatment of interactions between different quality attributes. Only since recently a couple of standardization working groups have been tackling with the interactions between safety and security and they are for the first time trying to give guidance for this in new editions of standards.

When defining the architecture for a safety-critical system, the design has to care for both safety and security (e.g., safety and security in aerospace [7]). A safety and a security analysis at the beginning of the development lifecycle yield additional requirements for mitigation measures to keep the system sufficiently safe and secure. However, mitigation measures targeted at safety may negatively influence security, and vice versa. As an example, an additional diagnostic channel can improve failure detection and, thus, safety. But, on the other hand, the diagnostic channel increases the vulnerable surface and therefore deteriorates system security. Such problems need to be addressed in system development. Moreover, also other aspects play a role and can interfere with safety or security, like performance with respect to various properties, availability or reliability. For instance, Fujdiak et al. [8] investigated the relation between performance and security in modern systems. In addition, there are specific aspects like human factors or the system use in the operation phase, which should be seen in context with different quality attributes.

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* (SSP) 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 for the previous points.

The project has started on May 1st, 2017 and its duration is three years.

This paper is an extension of a previous conference paper (i.e., [9]) that adds details about the description and the status of the project. Its structure is the following one: Section 2 highlights the project objectives, Section 3 extends the description of the main concepts and the adopted approach, while Section 4 (completely new) focuses on the expected extensions to the state of the art. Then, Section 5 focuses on the selected application domains by extending their description and providing also the main project results currently obtained in the context of the considered use cases. Finally, Section 6 presents main implementation issues and Section 7 draws out some conclusions.

2. Project objectives

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* (SSP) *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 objectives of the AQUAS project. More in detail, key outputs that we expect from this project are:

- a global concept framework for SSP-CE:
  - 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 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* (SoS).
- 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 SoS.

3. 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., [10–13]).

AQUAS [9] is building momentum for industry to adopt significantly improved CE approaches that are applicable to the entire PLC across many domains[1]. The idea is to learn how the methodology can be applied in different use cases from five domains, and then derive a general approach with sufficient flexibility to cover all relevant domains. The basic idea is to have quality attribute- or aspect-specific processes in parallel and analyze, after their completion or partial completion, whether the results are compatible or consistent. In AQUAS, we call this activity of analyzing the results of several processes an “Interaction Point” (IP).

[1] AQUAS Project Website: http://aquas-project.eu/.

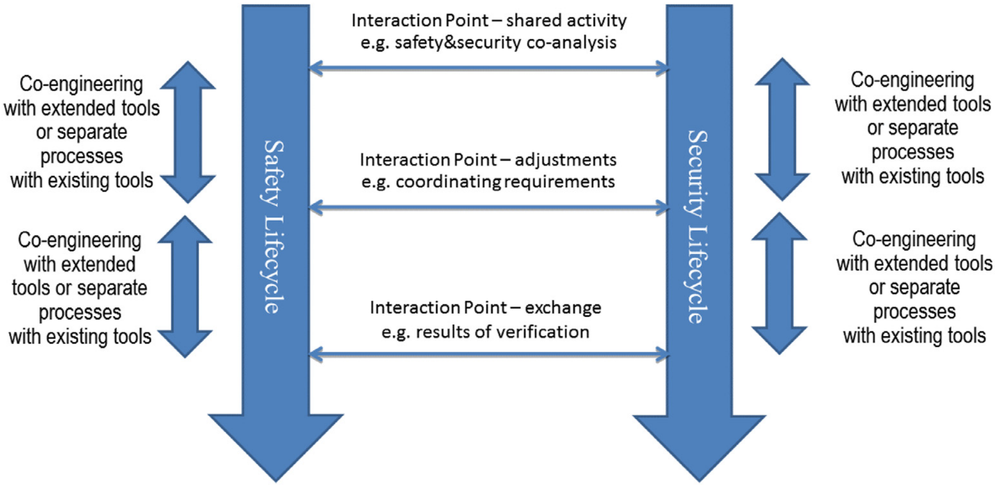
Interaction Point – shared activity
e.g. safety&security co-analysis
Interaction Point – adjustments
e.g. coordinating requirements
Interaction Point – exchange
e.g. results of verification
Safety Lifecycle
Security Lifecycle
Co-engineering with extended tools or separate processes with existing tools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

Fig. 1. AQUAS PLC with separate/combined processes.

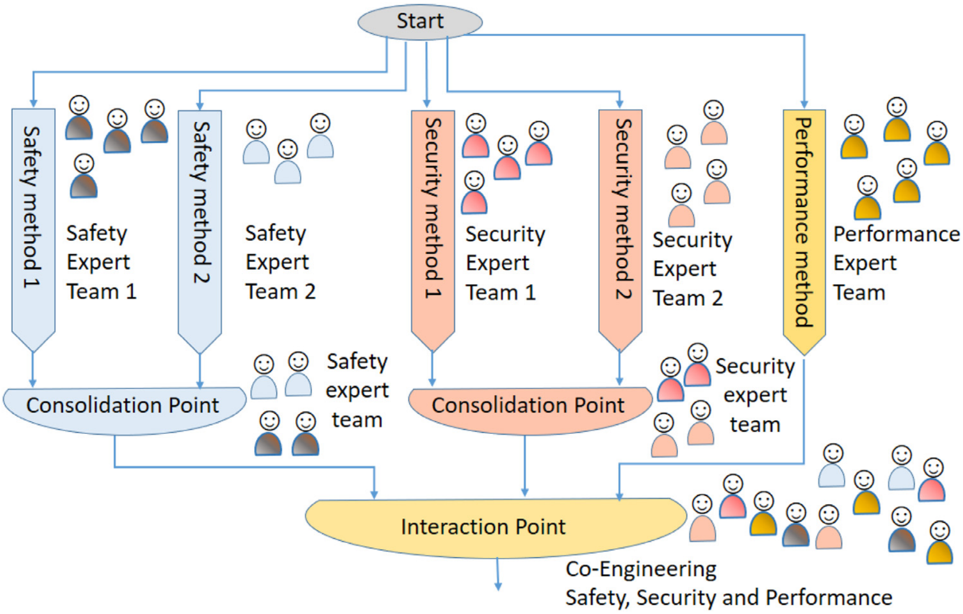

Fig. 2. Illustration of safety, security and performance co-engineering through an interaction point. Consolidation points are represented as previous steps which are specific to a quality attribute.

The purpose of an IP, where experts of the various quality attributes come together, is detecting whether the latest steps of refinement or implementation performed have violated constraints or requirements established in previous stages, or have revealed new conflicts among the various requirements of SSP that require trade-offs, or backtracking to redefining the trade-offs established at previous stages. An example for such an issue is an encryption algorithm introduced in order to support security, which, on the other hand, increases CPU load and, thus, decreases performance. This may cause a violation of the worst case execution time, and thereby deteriorate safety.

Many methods for combined analysis of safety and security have been proposed since this need was first recognized (see for example the survey by Kriaa et al. [14]), however, the main practical problems now concern the use by specialists in the different communities, and the cost-effective integration in the PLC of analysis methods and tools supporting these combined analyses. The methodology an organisation applies here relates to how often these combined analyses occur and how much can be automated.

The point here (Fig. 1) 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.

Fig. 2 illustrates an example of the process structure of an interaction point in a fictitious case. The interaction point is located at the bottom of the figure. We illustrate also the possibility to have previous “consolidation points” tackling the concerns of a specific quality attribute in an isolated way by the experts on the analysis of this quality attribute (i.e., no safety/security/performance co-engineering).

Fig. 3 illustrates the parallel processes for the different quality attributes (safety/security/performance) run through all stages of the classical V-model, and even beyond it along the operations, maintenance and retirement stages. At certain points in the life-cycle, interactions are inserted between the quality attribute-specific parallel processes. This can be done at the end of each

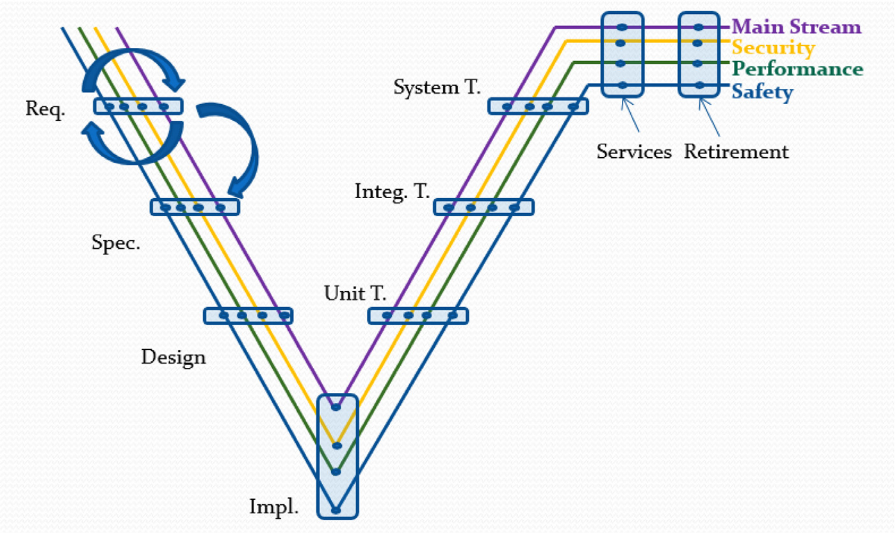

Fig. 3. Illustrative example of a product life cycle based on the v-model where the main stream cohabits with safety, security and performance streams.

stage, where a review is supposed to take place, but it can as well be at other locations.

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 Möbius [15], which operate typically at system level, to tools suitable for more detailed analysis, such as CHESS [16], 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 safety, security 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 [17] or the Goal Structuring Notation (GSN) [18], 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.

4. AQUAS extensions to the state-of-the-art

While trying to reach the objectives described in Section 2, by means of the approach described in Section 3, the AQUAS project will provide several results that will extend the state of the art in the field of *Co-Engineering, Product Life Cycle* and *Standards Evolution*. Such potential extensions are described in the following paragraphs.

4.1. Co-Engineering

Safety, security and performance are important issues for critical systems in multiple domains. With an increasing trend towards complex, open and dynamic highly automated and networked systems such attributes can no longer be considered separately. In order to develop dependable *Cyber-Physical-Systems* (CPS) and SoS, the mutual influences and constraints of each dependability attribute and their interdependencies must be taken into account through the entire development process.

The increased relevance of safety- and security-co-engineering with systems getting more complex and more networked has found its way into standardization groups. To date, several standards which promote security-aware safety-engineering are available or in preparation. SAE J3061 'Cybersecurity Guidebook for Cyber-Physical Vehicle Systems' [19] provides guidance for safety and security co-engineering in the automotive domain and has been used in the EMC2 project: the concept described in the SAE standard is compatible with the safety and security interaction point approach, which was already used in the EMC2 project, and which provides a foundation for further elaboration and extension in AQUAS. In particular, we will look ahead at the upcoming new Automotive Cybersecurity standard SAE/ISO/IEEE 21434, which builds on and refines SAE J3061 and is intended to be compatible with the Functional Safety standard ISO 26262. For the industrial control domain, IEC 62443 [20–23] gives guidance how security threats for safety-critical control systems shall be treated. The standard identifies zones and conduits of different level and elaborates on appropriate security measures, taking into account safety risks for the determination of security levels. In addition to IEC62443, IEC TC65 WG20 'Industrial-process measurement, control and automation- Framework to bridge the requirements for safety and security' is also working on the issue of safety and security co-engineering. This new working group is looking into standards for safety and security for industrial systems from the industrial and other domains to define an applicable framework for bridging safety and security. For the railway domain, a cybersecurity extension of the CENELEC standards EN 50128/29 and EN 50159 has been elaborated by the German Association of electrotechnicians VDE, named DIN/VDE V 0831-104, 'Electric signalling systems for railways - Part 104: IT Security Guideline based on IEC62443' [24]. The standard uses concepts of IEC 62443 and demands an extension of the safety case to include security measures.

The mutual dependence of safety and security has been recognized by the research community for many years and in different domains, for instance by Steiner and Liggesmayer [25], Schmittner [26] or Kriaa [14]. Several respective publications come from the ITEA2 project "MERgE", like Paul [27,28], and Brunel [12], and even a targeted deliverable [29] is available. Likewise, previous work was elaborated in the SeSaMo project with two deliverables in the area of safety and security (namely, D2.1 – Specification of Safety and Security Mechanisms and D3.1 – Specification of Safety and Security Analysis and Assessment Techniques, both accessible at http://sesamo-project.eu/documents) and a number of publications, e.g., Popov [30], Mazzini [31], Born [32], and Paulitsch [33].

One of the first systematic studies how safety and security interact on the requirements level was given in [33]. Requirements can be contradictory and need resolving or requirements can be caused by the other domain (e.g., from a "threat which can cause a hazard" can follow a "safety-based security requirement caused by a security and safety risk"). In order to identify this, a phase for conflict resolution and integration of requirements was proposed. As described in Section 2, AQUAS is focusing on developing practical co-engineering methods and tools for such shared activities and interaction points among safety, security and performance during the complete Product Life-Cycle. While safety and security interdependencies were already considered in projects like SeSaMo, Arrowhead, EVITA and EMC2, performance was largely neglected and the approach towards security was mostly done on a case by case basis.

AQUAS will develop approaches, utilizing system modelling techniques, for a security- and performance-aware design, development and testing of safety-critical systems. This extends to the operational phase, where systems need to scope with an increasing rate of changes and updates which requires re-verification or increasing and updating the security. Tools which only support, safety, security or performance will be extended to include the additional dependability requirements and interconnected to form a holistic tool chain for safety, security and performance co-engineering beyond existing safety & security co-engineering paradigms.

An overview of combined approaches for safety and security, focusing on analysis techniques and the industrial domain was presented in [14]. While these are useful first steps, which are incorporated into AQUAS, it is necessary to look at the complete system life-cycle, define co-engineering points and identify, extend and develop methods and tools for each co-engineering point. Working on a holistic system view, either with tools able to consider multiple system quality attributes or with interacting tools will reduce the necessary design concept iterations to balance safety, security and performance. Such holistic methods and processes make the effects of changes on other system quality attributes visible and support the detection of beneficial and detrimental influences between system quality attributes.

The AQUAS project will investigate all these different scenarios in the earliest possible life-cycle phase, thus avoiding costly iterations over several life-cycle stages or even overlooking critical design or implementation flaws as a consequence of disregarding the mutual dependence.

AQUAS will combine aspects of the unification and the integration approaches. The balancing among approaches will be achieved not only by checking requirements but also by inherently combined methods and tools. In addition, AQUAS plans the use of patterns whose influence on the different quality attributes is known; this allows an a priori correct design in relation to the different concerns.

The AQUAS life-cycle model allows to keep the threshold for adapting the technology low, encouraging industry to change to the novel approach early because the risk is low. Established and well-proven tools can still be used, new tools for additional concerns can be added and processes extended with interaction points and shared activities. Despite of the ambition to establish a holistic and comprehensive approach targeting the common treatment of all relevant quality attributes, AQUAS is nevertheless open for a smooth transition from well-introduced to novel life-cycle processes. Existing tools and established separate (i.e., parallel) processes for treating the individual quality attributes are joined at the interaction points. It is expected that companies will initially adapt the AQUAS approach with the yet separate safety, security and performance improvement processes. Team members responsible for the single quality attributes will learn from each other, slowly merge their knowledge and advance to experts for all quality attributes. With appropriate co-engineering tools coming up, the parallel processes can be replaced by multiple concern-aware methods allowing further efficiency increase by avoiding the otherwise necessary conflict resolution iterations between interaction points. Fig. 1 shows the choices how the processes between the interaction points can be designed.

As mentioned above, AQUAS allows two alternatives for co-engineering, namely continuous integrated co-engineering as well as concurrent engineering for treating the different quality attributes separately with synchronization at the interaction points, where the balancing is done. Osborne [13] describes approaches for concurrent engineering taken in the Aerospace industry and provides examples from eight aerospace centers which are using this technique. Here AQUAS has the potential to integrate smoothly and provide support in a domain with classified equipment and data and, thus, with the highest security requirements.

As may have become clear, in addition to advancing general approaches for co-engineering, there are two particularly critical aspects. These are the product life-cycle and standards evolution, which due to their importance for realising co-engineering have also been set as project level goals. Co-engineering concepts are gaining momentum in standardization and will require methodical and tool support for realization. Our vision for these is described in the next two sections. Co-engineering will be technically supported by tools interoperability using open standards as presented previously.

4.2. Product life-cycle

During the nineties Product Data Management was an ICT driven approach focused on product design data management. However the process has evolved to management of the product lifetime meaning the processes and applications for the entire life of the product and not just product design data [34]. The Product Life-Cycle (PLC) is thus treating a product from the initial concept all the way to disposal [35]. PLC management is intended to be an integrated data and process metamodel in order to provide models for every stakeholder across the PLC. Usually it is a set of processes, tools and models that cover certain stages, activities and information. The set of processes, tools and models are used in a phase to generate outcomes (models, files, etc.) to be used in the next stage and so on.

A seminal paper on PLC [36] discusses the main life cycle stages of a product, and it highlights the nature of the systemic approach to the PLC. A product development should comprise, not only the product development itself, but also other relationships such as customers and providers interactions. In this sense, systemic approaches have been applied in order to develop a wide set of products. There are some industrial experiences such as [37] where electronic design automation is used along a PLC.

Some papers, such as [38], outlines a structure for a so-called PLC Simulation System. From an industrial production perspective we need to manage the value [39] generated among PLC stages. This means that reuse strategies should be set up, among others. Standards such as ISO/IEC/IEEE 26531 [40] also highlights the value of PLC, reuse strategies, and metadata and workflows concepts. Therefore PLC management is an integral part of total quality management system [41], and therefore it should take into account quality aspects such as safety, security and performance.

An additional benefit from managing effectively PLC phases is that requirements changes are reduced [42]. Tests are considered one of the largest costs [43]. Therefore model based techniques are suggested to manage, for example, test requirements throughout the PLC [44]. Product's data management throughout the entire life cycle [45] is also a key element in complex product developments. This is especially relevant in safety critical scenarios where methods are defined in order to control requirements flow in PLC (e.g., [46]). Other proposal are focused on project planning practices [47] for developing complex projects such as unmanned aerial vehicles. Modelling is relevant for managing PLC, and several contributions are aligned with modelling data and resources [45,48,49].

A major focus of this goal is the better connectivity of the PLC through its various stages with respect to co-engineering for system quality attributes. This means partners and use cases with a particular competence (e.g., modelling) will be looking to improve their understanding of other stages (e.g., requirements, implementation) and providing linking mechanisms (tooling/conceptual) to these during the course of the project. The Standards Evolution goal will reinforce work particularly related to the vertical aspect of safety and security of the complete PLC.

The PLC will consider and face these challenges from several perspectives, especially when taking into account safety, security, and performance. These concepts have a direct impact on the product life cycle of any company developing safety critical systems. Safety Engineering is a mature discipline and typically rigorous processes are applied, e.g., the V-model. More recently, agile methods of different flavours have been proposed and practiced in safety related industries (e.g., the European Space Agency, the Lean Development, etc.) However these concepts have been widely studied separately due to the difficulty of integrating relationships among them but also because many domains have been trusted in the past but are now increasingly open. Industrial applications use a wide diversity of PLC models taking into account several characteristics which are not standardised, and they are not systematically applied. Traditionally "ISO/IEC 12207:2008, Systems and software engineering Software life cycle processes" indicates and establishes a common framework for software life cycle processes without taking special considerations of safety-critical development processes. In particular ISO/IEC/IEEE 15288 "Systems and software engineering System life cycle processes" defines four groups of processes: agreement processes, organisational project-enabling processes, project processes and technical processes.

In fact technical processes also highlight the need to define user requirements including safety considerations during the requirement analysis process. Other guides such as [50] do not intend to ensure safety nor security aspects. These kinds of standards and guidelines do not prescribe any specific approach to tackle safety, security and performance considerations at the same time in a coherent PLC approach. In AQUAS we propose a particular type of mechanism – interaction points – which is orthogonal to any model of life-cycle and can occur at different stages of the life-cycle and allow for combined analysis to be applied and take into account simultaneously the concerns relevant for the particular development context. Interaction points are necessary throughout the PLC. In particular, security threats evolve during operation, and require re-analysis of system security and often changes to elements of a system to restore it (e.g., to correct newly discovered vulnerabilities), sometimes with tight deadlines as changes of threat environment are unpredictable and may be such that operation becomes unsafe. Both changes of threat environment and possible required system changes may have knock-on effects. E.g., a security "patch" may violate a performance requirement dictated by safety requirements. However, current patterns of safety analysis and documentation do not fit this reactive, evolving, quick-response model: they are typically focused on showing that a system is safe despite the threats posed by a static, non-malicious environment. Thus a challenge for AQUAS is how to ensure effective, efficient combined analyses at these interaction points that occur during operation.

One of the questions is where, in the timeline of the PLC, interaction points should be placed. Combined analyses could be continuously repeated every time that any of the development artefacts changes, giving a guarantee of spotting early any risk of violating requirements and any opportunity for optimization; but this will not be cost-effective; if on the other hand much design refinement or change takes place without cross-checks, the costs of backtracking if problems are found, or the opportunity cost of missed optimization chances, may be large. The concern is analogous to what is sometimes called “technical debt” [51]: if rapid software implementation is pursued without the software engineering investment that makes for longer-term cost-effectiveness, extra costs will be incurred in maintenance, late refactoring, operational failures. On the other hand, early over-investment is also a risk, for instance if a product turns out to be short-lived.

For co-engineering for safety, security and performance, the limiting case, still present in some development processes nowadays, is that of no interaction points. The resources and design precautions dedicated to ensuring adequate safety, security and performance are decided early on, conservatively to give a good chance of the final product being adequate without any further co-engineering activities (detailed joint analysis). The only verification that the requirements are jointly satisfied is at some phase of testing the complete product, or even in its operation. The early conservatism gives good confidence that the requirements will be indeed satisfied, paid for by a somewhat wasteful design. If requirements are not satisfied, often due to having not spotted some complex interaction - for instance if security controls degrade performance so as to violate system performance goals or to create safety risks - then substantial re-work is required, and without combined analysis this rework amounts to another trial-and-error cycle.

We expect that the schedule of interaction points can in part be decided before development, at pre-defined points in the development process used by a company (the AQUAS use cases will experiment with this static scheduling of interaction points); while others will need to be introduced reactively to respond to exogenous change; for instance a decision to extend the operation of a product to new environments or regimes of operation, or when discovery of a vulnerability or unforeseen attack behaviour requires updates of security controls. One critical PLC stage is the Disposal Process, widely known as Decommissioning process, the purpose of which is to end the existence of a system entity. This removal implies several changes affecting requirements, the global architecture, and maintenance and, at the end, stakeholders need to revise their complete product life cycle. Another critical process is the Integration process when different vendors aim to integrate their solutions. Several assumptions are typically made by the respective vendors when developing their own products and a type of contract base can indicate that some assumptions are violated or not. This is the point where the implicit contract under which the product has been developed may be violated when the product is applied in a different context. ISO/IEC/IEEE 15288 specifies a set of technical processes and next figure outlines these processes including a link safety, security and performance concepts from a conceptual point of view. This integration can be done by modelling Safety Cases (e.g., using GSN (Goal Structuring Notation)/CAE (Claim - Argument - Evidence) tools) including facilities to define and trace these concepts (safety, security and performance). For doing this we can use the Opencoss platform [52] released under Eclipse/Polarsys initiative.

AQUAS aims at incorporating safety, security and performance concepts in a common approach in order to reconcile and harmonise them within a product life cycle in a safety critical domain. In this sense AQUAS investigates the relationships among these concepts (safety, security and performance) and their relationships among standards such as ISO 26262, IEC 61508, or DO-178C. In addition AQUAS provides a product life-cycle model containing analysis methods such as FMEA, FTA, HAZOP, HW-Metrics, re-engineering of requirements using formal or semi-formal methods where/when possible, and the use of model based approaches for safety assurance analysis including ‘safe’ code analysis (e.g., Tests Generation Tools). A holistic product life cycle approach enables a comprehensive development, considering system dependability issues, and the use of statistics and applied probability approaches (e.g., stochastic model-checking techniques) confers a measurement approach appropriate to safety, security and performance.

Finally the resulting product life cycle approach guarantees the whole software development process integrity with respect the requirements for a safety-critical application. This approach can reuse cross-domain, and skills and knowledge can be used from one domain into others. AQUAS results will impact evolving new standard editions, and communities such as Eclipse/Polarsys.

4.3. Standards evolution

One of the most important AQUAS goal is to promote co-engineering standards derived from the project results by collecting feedbacks and suggestion for evolution during the project and provide recommendations for improvements aiming at the standardization of co-engineering technologies focused on dependability. It will help alleviating a major roadblock to co-engineering - little or no presence in standards in turn has meant little drive from organizations to address this issue. A consequence of standardization for dependability is to enable assessment and certification; however the major focus of AQUAS will be the inputs to standards rather than the outputs from standards. We aim at having a substantial impact on the mission-critical systems community reducing costs and time for assurance and promoting migration of dependable subsystems across multiple applications domains (e.g., avionics, railway, industrial automation, medical). This will include aspects enabling faster evolution whilst preserving prior certification.

In particular, AQUAS intends to have an impact on the standards for mission-critical systems where traditional safety oriented requirements are being joined by new requirements for security and, in specialized cases, also performance. The predecessor project SESAMO has begun addressing these concerns with the introduction of ‘security informed safety’ in critical systems, and provides a foundation of results that will be extended by AQUAS both in depth and in dimension (i.e., addition of performance-related concerns) to be applied across several domains.

The following is an overview of current governing standards and their status with respect to safety and security considerations.

4.3.1. Cross-domain

IEC 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems) is the umbrella standard for E/E/PE functional safety applicable across a wide variety of industries. It is the basis for a number of domain-specific safety standards. The first security related aspects have been integrated into the last version 2.0 of the standard. IEC 61508 was the first functional safety standard taking into account security aspects particularly in risk and hazard analysis phases and the safety manual. Since November 2014 preparations have started for version 3.0 and more in-depth requirements and guidance to include cybersecurity issues with safety impact have been proposed and taken up to be developed further by partners (AIT).

4.3.2. Performance and dependability

IEC TC56, Dependability (formerly: Reliability), has recently issued interesting drafts or standards covering the dependability aspects of systems and open adaptive systems (AIT is member of the national group VE EG56 for IEC TC56):

- IEC 62853/Ed1: Open Systems Dependability (CD, comments closed July 2015; it addresses particularly the "assurance case"));
- IEC 62628/Ed1: Guidance on Software Aspects of Dependability,
- IEC 62741/Ed1: Reliability of systems, equipment and components. Guide to the demonstration of dependability requirements.
- The dependability case: this is of importance to AQUAS because the focus is here on general dependability properties and not primarily on safety and security as in IEC TC65 and ISO. Dependability is defined as a quality attribute that "includes availability, reliability, recoverability, maintainability and maintenance support, performance, and, in some cases, other characteristics such as durability, safety and security".

4.3.3. Cross-domains and cross-standards

IEC TC65 started end of Oct. 2014 an Ad-Hoc Group 1 "Framework towards coordination of safety and security (in industrial automation and control)" which should provide recommendations how to further proceed in a coordinated manner with respect to safety and cybersecurity standardization. The scope includes, but is not limited to, recommendations regarding the information security of safety-related systems. A second recently founded IEC TC65 AHG2 covers the relation between reliability and safety, thus closing the gap to IEC TC56, Dependability (AIT).

4.3.4. Ground transport domain (railway and motorway)

The standard CENELEC EN 50129 covers the safety aspects of the railway applications for communication, signalling and processing systems, while the CENELEC EN 50159 addresses the safety-related communication in the transmission systems. An update of the CENELEC standard is underway (CLC TC9X WG14 Working Group for safety-related standards). For signalling between traffic measurement equipment, traffic infrastructure on the motorways and the traffic management and information system only a directive is applied and realized: TLS 2002 (Technical Conditions on Delivery of Roadway Section Control Units 2002). For security purposes a regulation will be proposed for more secure signalling via SSL between road equipment in the forthcoming draft for TLS. Particularly VDE in Germany is just now working on an update of these standards taking into account and integrating requirements of IEC 62443, SL 1 (Security Level 1) directly into the update proposal for a new version of EN 50129 and EN 50159.

4.3.5. Air transport domain

The Safety Regulation Commission for the EUROCONTROL Agency has recently published a body of European Safety Regulatory Requirements (ESARR) in order to develop, maintain and promote common Safety Management policy, procedures, methods and tools for the European Civil Aviation Conference (ECAC) area. SC-205/WG-71 is re-considering safety-critical standards for aerospace especially with respect to guidelines on the safe use of model-based development and leveraging verification approaches towards aircraft certification. DO 178B (Software Considerations in Airborne Systems and Equipment Certification) is a major standard applied by the Federal Aviation Administration. An update of DO-178B (known as DO-178C) now exists. Multiple Independent Levels of Security/Safety (MILS) exists for security aspects. Complementary cybersecurity standards have been issued just recently, namely DO 326A/ED 202A 'Airworthiness Security Process Specification' and DO 255/ED 204 'Information Security Guidance for Continuing Airworthiness', by RTCA SC-216, Aeronautical Systems Security, in collaboration with EUROCAE WG-72.

4.3.6. Medical devices domain

The U.S. Food and Drug Administration (FDA) requires that manufacturers of medical devices establish and follow quality systems to help ensure that their products consistently meet applicable requirements and specifications. The quality systems for FDA-regulated products such as medical devices are known as current good manufacturing practices (CGMPs). The ISO standards for medical devices are covered by ICS 11.100.20 and 11.040.01. The quality and risk management regarding the topic for regulatory purposes is convened by ISO 13485 and ISO 14971. The standard for medical software is IEC 62304, the functional safety standard IEC 60601 which is referenced in the European Medical Devices Directive 93/42/EEC of 14 June 1993, revised 2007/47/EC. In context of hospital information systems, networked devices and remote patient health monitoring cybersecurity is becoming a critical issue as well.

4.3.7. Space domain

The European Cooperation for Space Standardisation (ECSS) commission of the European Space Agency maintains the standards ECSS-Q-30, containing guidelines to perform failure modes effects and criticality analysis, and ECSS-Q-40 for the safety space products assurance. The mere existence of two separated standards shows that safety and criticality analyses are treated independently. Furthermore, these standards are mere recommendations heavily subjected to final interpretation by the user and the customer. Present evolution in the complexity of space worth CPSs calls requests the maturing of these standards to define a clear set of tools and methodologies to be applied to guarantee the final performance of equipment and to remove as far as possible the subjective part of the analysis that implies delays and overcosts in all the review points of a project;

4.3.8. Process industry and industrial automation

IEC TC65 WG 10 and ISA 99 have issued the series of standards around IEC 62443 'Industrial communication networks - Network and system security - Security for industrial automation and control systems', consisting of several parts with subparts, including e.g., System security requirements and security assurance level, Patch management and Certification of IACS supplier security policies and practices. This standard is taken as reference for cybersecurity in industrial systems and in several functional safety standards.

4.3.9. IEC TC44, safety of machinery, electro-technical aspects

Considerations how to take care of cybersecurity in context of machinery safety have started:

- cybersecurity shall not interfere with the safety objectives of the plant and shall protect their realisation;
- for functional safety in the automotive domain ISO 26262 is relevant. In January 2015 at the meeting for Ed. 2.0 proposals were made for 'Consideration of security concerns in ISO26262' which is becoming of importance taking into account developments like 'connected cars', 'highly automated driving including V2V, V2I communication' and 'autonomous vehicles'. This was taken up and has become part of the DIS. In the meantime there is a new work item on Automotive Cybersecurity engineering.

Partners of the AQUAS consortium are members of several committees and very engaged to influence standards by promoting relevant project results to be reflected in the standards.

Further on, involvement in related ARTEMIS projects (SESAMO, EMC2, ARROWHEAD) and standardisation support actions (ProSE, CP-SETIS) and (pre-) standardization working groups (ARTEMIS Standardization WG, EWICS TC7) is supporting this goal. Our work

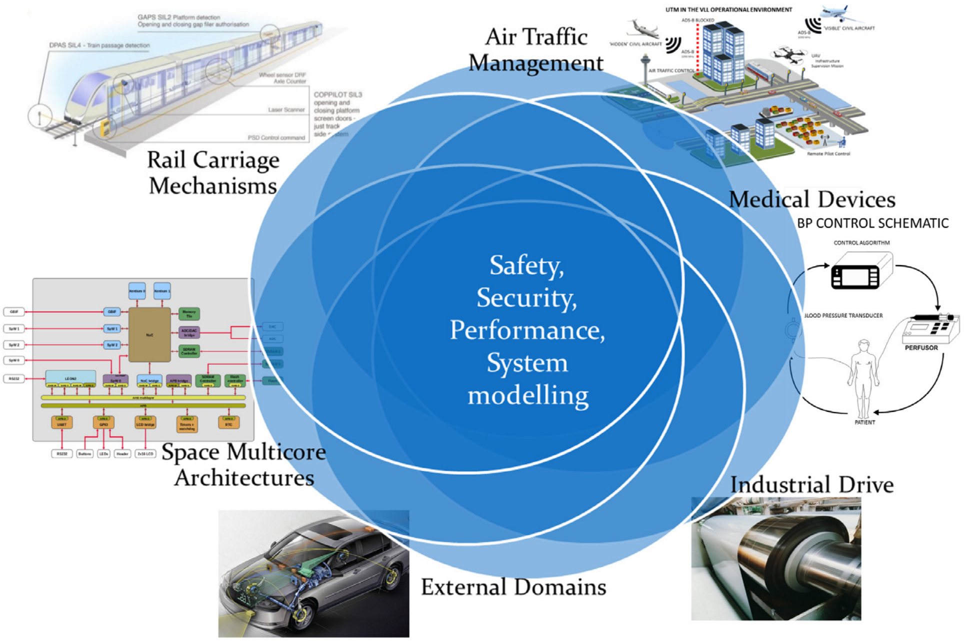
Air Traffic Management
UTM IN THE VLL OPERATIONAL ENVIRONMENT
Rail Carriage Mechanisms
GAPS SIL2 Platform detection Opening and closing gap filler authorisation
DPAS SIL4 - Train passage detection
Wheel sensor DRF Axle Counter
COPPILOT SIL3 opening and closing platform screen doors
Laser Scanner
PSD Control command
Medical Devices
BP CONTROL SCHEMATIC
CONTROL ALGORITHM
LOOD PRESSURE TRANSDUCER
PERFUSOR
PATIENT
Safety, Security, Performance, System modelling
Space Multicore Architectures
Industrial Drive
External Domains

Fig. 4. Co-engineering reinforced by many domains.

with standards evolution is also a crucial contribution to *Cyber-Physical Systems of Systems* (CPSoS), who need standardization in order to control the autonomy of management and operations. As an example, the ISO 15288 standard on Systems Engineering has much to say about SoS, but is known to be weak on extra-functional properties. AQUAS members intend to provide change request inputs for this Standard, among others.

Indeed, a key contribution of AQUAS will be to advance, where relevant, a combined approach for standards beyond the current state of the art. This will be done by evolving the concept and practice of the security informed safety case with impact on performance taken into consideration. As described in the Concept section, joint evidence gathered on security and safety through co-engineering activities will feed into the continuously maintained assurance case, which tracks the evolution of the system and maintains its dependability status. This procedure for constructing and maintaining the assurance case will be integrated seamlessly into the product life-cycle defined in AQUAS, taking into particular consideration the interaction points at which intense co-engineering activities are carried out. Much of the evidence will be directly generated by the AQUAS tools (e.g.formance analysis results from the CHESS toolset).

The results of these improvements in the non-functional development process will be directly measurable through observation of the capabilities of the AQUAS tools and life-cycle activities to generate automatically the evidence needed to prove their significance for standardization. Note that this decouples the measurement process from the actual evolution of the standards (which can be slow and unpredictable) and makes it objective and achievable as a concrete result of the project.

5. 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 as illustrated in Fig. 4 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., Air Traffic Management, Railways) deal with the design of typical “constituent systems” of SoS. Also, some SoS concerns (e.g., long lifetime, evolution after entry into service, multiple stakeholders) are shared by all five domains. The demonstrators are described in the following sections.

5.1. Air traffic management

This use case focuses on the provisioning of surveillance services to unmanned aerial vehicles (UAV) that operate on very low-level airspace and third parties such as law enforcement. The advances in unmanned aerial vehicles (UAV) and their numerous applications have contributed to the increasing air traffic density over the last years. Improvements in air traffic management are needed to address the need for appropriate situational awareness and required safety levels. In shared airspace, UAVs cannot always report their presence using standard means (e.g. ADS-B - Automatic Dependent Surveillance Broadcast) due to various reasons such as power constraints. An appropriate situational awareness can only be attained by the cooperation of ground services with airborne applications, as information on every surrounding aircraft will not be available at either side alone. The proposed approach in this use case promotes sharing UAV missing parameters (coordinates, heading, speed, etc.) using a data distribution system (DDS) middleware implementation based on the requirements of the existing System Wide Information Management (SWIM) [53] infrastructure. UAVs following this approach would mutually benefit by creating an using this common knowledge. By additionally leveraging current air traffic coordination services offered by governmental and trans-national agencies (such as the US FAA and Eurocontrol), it is feasible to determine the presence of hidden traffic, thus increasing awareness of potential conflicts that would remain unknown otherwise. The current results show that the introduction of AQUAS methodology and tools in the current work methodology can reduce the effort and improve the quality of the use case.

The next AQUAS potential benefits for this use case are support for generating input data for unit testing, support for schedulability analysis with realistic platform models, support for platform partitioning, support for generating system-level test inputs and outputs for exploration testing, support for confirming the absence of safety violations and support to design better security controls e.g. by identifying compromising situations.

5.2. Medical devices

A neuromuscular transmission (NMT) device is developed to support the anesthesiologist in controlling muscle relaxation during hospital operating room interventions. Muscle relaxation, depth of anesthesia, and pain are the three key parameters to be controlled by the anesthesiologist. The challenge is to develop a closed-loop controller for muscle relaxation that performs in automatic pilot mode. The use case hardware consists of two main components, an NMT monitor and a pump tree. The goal is to keep the muscle relaxation at the required level at each stage of the operation by delivering the right amount of drugs to the patient. The system requires diagnosis and therapeutic capabilities to enhance patient care and safety. When interfacing the system to a hospital information system security issues arise. Experience values show that the effort for safety and security verification and validation to reach the required safety and security levels is enormous. Within AQUAS, SSP shall be considered during the development life-cycle by various measures, such as modeling control software in the NMT controller hardware to reduce development time and costs, modeling the patient, applying tools for verification and validation to gain performance evidence in test cases that cover most possible real situations in real life, and securing the communication between the different components making them robust and not prone to compromising the integrity of the system. In this context, important standards are IEEE 11073 [54] (related to the interoperability between medical devices), EN 62304 [55] (related to software development of medical equipment), and EN 60601-1-10 [56] (related to closed-loop control systems). A goal is that by applying combined analysis methods for SSP evidence for assurance cases is systematically created. This will contribute to the system becoming an artifact capable of evolving whilst preserving its assurance/compliance status. Currently, this use case shows evidence of development of a first test platform that will allow to yield results and test evaluations. It will also show partner's technology considered by this Medical Devices use case as the spinal column to include operational tooling with Co-Engineering and tool interoperability means.

5.3. Rail carriage mechanisms

The opening and closing of Platform Screen Doors (PSD) installed in metro stations must be controlled in ways that ensure passengers protection. Actual implementations of PSD systems have a short delay of 300 milliseconds and operate independently of train signaling and automatic operating systems. Safety is of utmost importance with Safety-Integrity Levels (SIL) often reaching level 3 and 4. PSDs are deployed widely for either upgrading existing lines or establishing new, usually driverless, metro lines. Such systems are operated remotely, which imposes the need for security measures next to safety. Railway system functions are also time-critical, which leads to the need of tools and methods to analyze cross-effects between SSP. Hardware and software are developed in conformance to EN 50126 [57] and PSD systems require various sensor subsystems (e.g., radar, laser, infra-red, etc.), processing functions and actuators, and have a development cycle that is usually between six and twelve months. In general, each developed system is new, which makes it hard to reuse parts for design and development. Major goals of the use case within AQUAS are to reduce the time needed for the development cycle and to guarantee cost reduction by limiting unexpected behaviors at advanced stages in the PLC. At the current stage of the use case the work flow concerning safety and performance does not suffer heavy changes, but the ability to detect and reason about interaction points can greatly help anticipating the potentially costly nodes. Also, the AQUAS methodology eases significantly the introduction of new categories. The current focus lies on safety, security and performance, but any new category (ergonomics or process constraints for instance) could be introduced in the same meta-framework.

5.4. 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 large variety of communication and sensor interfaces of such embedded systems adds significant security challenges to the safety mechanisms already implemented in commercial industrial control products, where the most relevant standards are IEC 61508 [58], IEC 61800 [59] and IEC 62443 [60]. Besides safety and security, also real-time performance is an essential criterion within this cost driven and competitive domain. Finding the right balance between these attributes while staying within tight budget constraints is a challenge for this use case. This makes the Industrial Drive a relevant demonstration example for the technology developed within AQUAS. The approach taken is based on Virtual Prototyping. Even though virtual HW prototyping for SW development is common industrial practice, its usage for verification of safety features is not yet state of the art. In AQUAS, a seamless flow from System Level Model to the Virtual HW Prototype will be investigated with main focus on early concept validation. One of the major goals was to seek and manage dependencies (interferences) between requirements, thus detecting potential conflicts between safety/security/performance. At the current stage, a spreadsheet-based method for identification, management and reduction (of the huge number) of potential interferences of requirements was developed. This approach will undergo refinement accompanied by some tool support for automation.

5.5. Space multicore architectures

Spaceborne missions have very strict requirements on performance under critical conditions, as well as on other system quality attributes such as safety and security. The validation procedures for such systems are long and there is also a lack of tools and methodologies that allow quick exploitation of technology. This makes it hard for new technology to find its way into space applications (e.g., multi-processor architectures and Systems-on-Chip are still being seen as newcomers in this domain). The use case focuses on the payload of an earth observation space project by applying a multicore architecture for video processing equipment. SSP requirements are derived from actual mission scenarios. The defined architecture should enable in-flight reconfiguration with new versions of software and hardware (SW modifications for a LEON processor-based architecture or FPGA reconfiguration). One major goal is to replace legacy design systems with multicore architectures to improve performance. Parallelizable video compression algorithms that are commonly used in space domain will be taken to test the performance of the system. A possible core for the architecture is the LEON3FT [61], which will be used as base to implement the Scalable Sensor Data Processor Breadboard architecture. The use case must support compliance to the European Cooperation for Space Standardization (ECSS) family of standards for Space Software (ECSS-Q-ST-80C [62] and ECSS-E-ST-40C [63]). The tools and methods developed in AQUAS should show an impact on certification and validation of the algorithms. Currently, the relevant interaction points are being elaborated in their respective PLC phase and that will potentially lead to trade-off decisions for the design. The demonstrator SW is composed by the Boot SW and the Application SW, this last one is the subject of study in AQUAS. A safety-security-co-design was done by code developers, trying to consider during design phase the needed security features with the design of safety-oriented risk mitigation mechanisms. The application software is implemented with a real-time operating system toolchain. The schedulability of the whole software is analyzed with tools specialized on timing analysis in order to check if security features do not negatively influence the performance.

6. Implementation

6.1. Work plan - Work packages, tasks and interactions

The work structure and responsibilities of AQUAS are broken down into work packages (WPs) and tasks. Although AQUAS contemplates a number of five different Work Packages (WP), the project diverges from the traditional Concept/Tool/Demonstrator WP structure to encourage a more collaborative and use case driven environment. Consequently, the demonstrators do not form part of any WP in particular but represent a result of a joint work among WP 2, 3 and 4. This bottom-up approach is depicted in Fig. 5. WP2 on Application Domains is in charge of demonstrator management including the use case definitions, requirements, analysis, and testing of different technologies. It comprises a number of use cases corresponding to 5 application domains including air traffic management, railway, industrial drive, health, and space. Methodology and Design tool providers contribute to the demonstrators through their work in WP3 on Methodology and WP4 on Design Tooling. Both project management and technical coordination are performed in the scope of WP1 on Project Management whereas WP5 on Exploitation and Dissemination takes care of spreading the AQUAS outputs internationally and ensuring the uptake of the obtained results.

6.2. Consortium as a whole

The initial impetus for the AQUAS consortium formation came from the projects SESAMO [64] and MERGE [65] 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 that the Consortium should not pass 25 partners. A short questionnaire was circulated requesting data about each organization's background and work interests within the scope of AQUAS. The DSC evaluated replies 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

Moreover, 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. Today, the AQUAS consortium gathers 23 institutions including academy, research institutions and industry from 7 European countries.

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

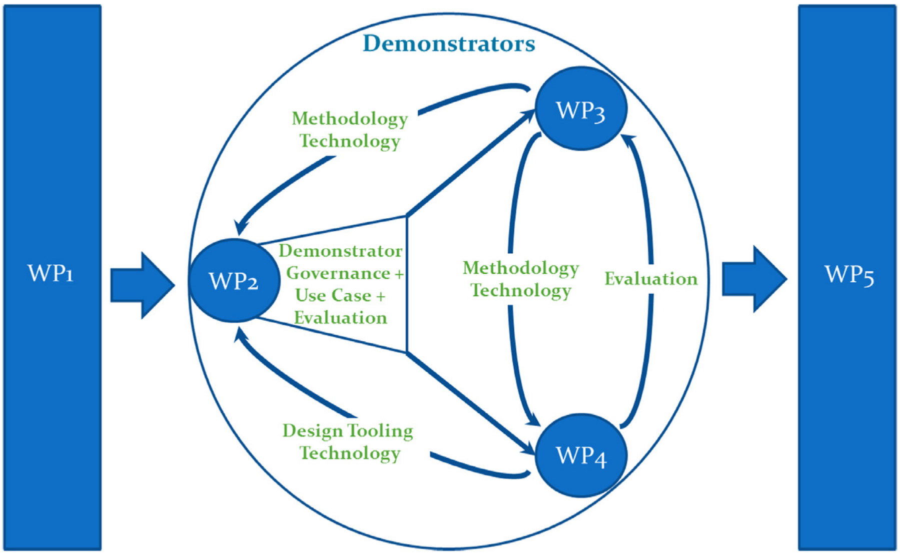

Fig. 5. Interaction between Work Packages.

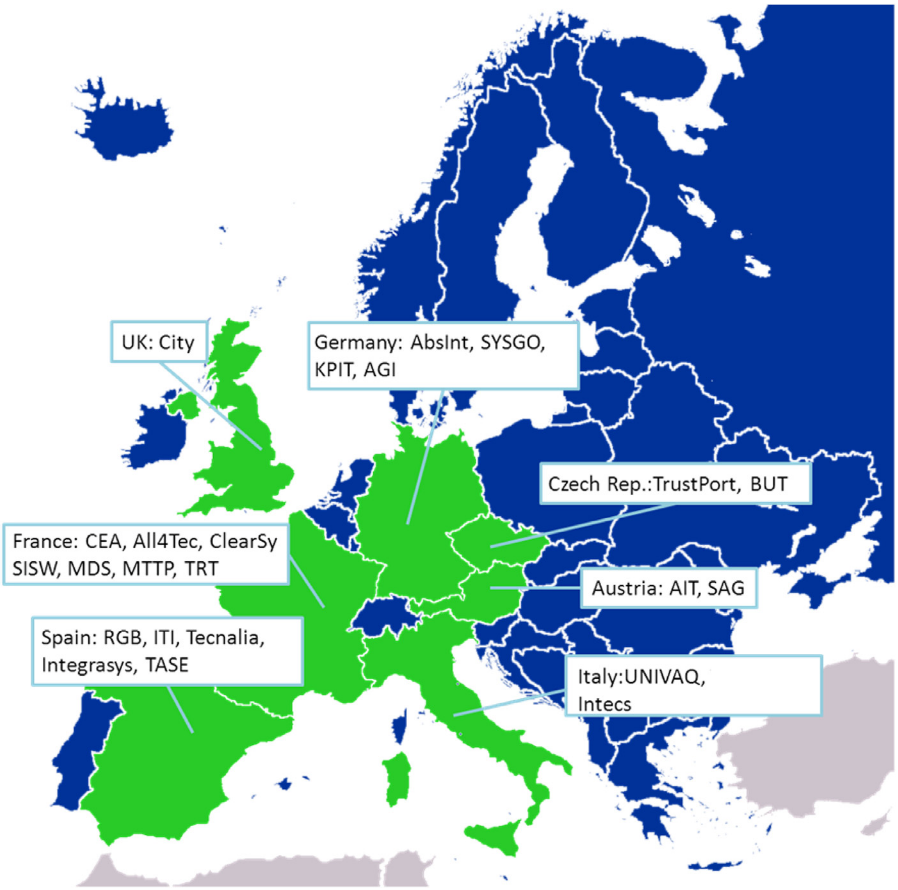
UK: City
Germany: AbsInt, SYSGO, KPIT, AGI
Czech Rep.:TrustPort, BUT
France: CEA, All4Tec, ClearSy SISW, MDS, MTTP, TRT
Austria: AIT, SAG
Spain: RGB, ITI, Tecnalia, Integrasys, TASE
Italy:UNIVAQ, Intecs

Fig. 6. Country distribution.

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.

Not only the size of the Consortium was limited. The same was done with the number of applications domains. Maximizing impact is a trade-off between advancing in a sufficient number of domains, whilst keeping a sufficient number of partners in 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 on having sufficient domain diversity and coverage of the three core goals. Partners' expertise has also been carefully aligned with the needs of the use cases.

Of equal importance to having sufficient spread across domains is having a suitable partner distribution across Europe. The spread of partners is shown in Fig. 6. Having cooperation across European countries is essential for bringing the practice of co-engineering into the mainstream development processes. This form of collaboration is intended to ensure building momentum on the markets of these countries.

7. 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 (sub)systems and components 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 (e.g. [66,67]) and demonstrates the newly conceived approaches to co-engineering across use cases spanning Space, Medicine, Transport and Industrial Control.

Conflict of interest

None.

Acknowledgement

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

References

[1] IEC, IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, 1998,
[2] Y. Lu, Industry 4.0: a survey on technologies, applications and open research issues, J. Indus. Inf. Integrat. 6 (2017) 1–10, doi:10.1016/j.jii.2017.04.005.
[3] BBC, Timeline: how Stuxnet attacked a nuclear plant, 2010https://www.bbc.com/timelines/zc6fbk7, (accessed May 2019).
[4] BBC, Hack attack causes 'massive damage' at steel works, 2014, http://www.bbc.com/news/technology-30575104, (accessed May 2019).
[5] D. Goodin, Hackers trigger yet another power outage in Ukraine, 2017 https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/, (accessed May 2019).
[6] K. Netkachova, R.E. Bloomfield, Security-informed safety, IEEE Comput. 49 (6) (2016) 98–102, doi:10.1109/MC.2016.158.
[7] M. Paulitsch, R. Reiger, L. Strigini, R.E. Bloomfield, Evidence-based security in aerospace: from safety to security and back again, in: 23rd IEEE International Symposium on Software Reliability Engineering Workshops (ISSRE), IEEE, 2012, pp. 21–22, doi:10.1109/ISSREW.2012.37.

[8] R. Fujdiak, P. Mlynek, P. Blazek, M. Barabas, P. Mrnustik, Seeking the relation between performance and security in modern systems: metrics and measures, in: 2018 41st International Conference on Telecommunications and Signal Processing (TSP), 2018, pp. 1–5, doi:10.1109/TSP.2018.8441496.

[9] L. Pomante, B. Křena, T. Vojnar, F. Veljković, P. Magnin, The AQUAS ECSEL project, in: 21st Euromicro Conference on Digital System Design (DSD), IEEE, 2018, pp. 592–599, doi:10.1109/DSD.2018.00104.

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

[11] S. Paul, Over 20 years of research in cybersecurity and safety engineering: a short bibliography, in: 6th International Conference on Safety and Security Engineering (SAFE), 2015, p. 15.

[12] J. Brunel, D. Chemouil, L. Rioux, M. Bakkali, F. Vallée, A viewpoint-based approach for formal safety & security assessment of system architectures, in: Proceedings of the 11th Workshop on Model-Driven Engineering, Verification and Validation, 2014, pp. 39–48. http://ceur-ws.org/Vol-1235/paper-06.pdf (accessed May 2019).

[13] J. Osborne, Survey of concurrent engineering environments and the application of best practices towards the development of a multiple industry, multiple domain environment, in: All Theses, 635, 2009, pp. 1–168. https://tigerprints.clemson.edu/all_theses/635, (accessed May 2019).

[14] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, Y. Halgand, A survey of approaches combining safety and security for industrial control systems, Reliab. Eng. Syst. Saf. 139 (2015) 156–178, doi:10.1016/j.ress.2015.02.008.

[15] W.H. Sanders et al., Möbius – model-based environment for validation system reliability, avalability, security, and performance, 2019https://www.mobius.illinois.edu/, ©2019 (accessed May 2019).

[16] S. Hansen et al., CHESS: composition with guarantees for high-integrity embedded software components assembly, 2019 http://www.chess-project.org/, (accessed May 2019).

[17] ADELARD, Claims, arguments and evidence (CAE), http://www.adelard.com/asce/choosing-asce/cae.html (accessed May 2019).

[18] T. Kelly, R. Weaver, The goal structuring notation – a safety argument notation, in: Proc. of Dependable Systems and Networks 2004 Workshop on Assurance Cases, 2004, p. 6.

[19] SAE, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, Standard, SAE, 2016.

[20] IEC, Industrial communication networks - network and system security - Part 1-1: terminology, concepts and models, Standard, IEC, 2009.

[21] IEC, Industrial communication networks - network and system security - Part 2-1: establishing an industrial automation and control system security program, Standard, IEC, 2010.

[22] IEC, Industrial communication networks - network and system security - Part 3 1: security technologies for industrial automation and control systems, Standard, IEC, 2009.

[23] IEC, Industrial communication networks - network and system security - Part 3-3: system security requirements and security levels, Standard, IEC, 2013.

[24] IEC, Electric signalling systems for railways - part 104: IT security guideline based on IEC 62443, Standard, IEC, 2015.

[25] M. Steiner, P. Liggesmeyer, Combination of safety and security analysis - finding security problems that threaten the safety of a system, in: International Conference on Computer Safety, Reliability and Security (SAFECOMP), 2013.

[26] C. Schmittner, T. Gruber, P. Puschner, E. Schoitsch, Security application of failure mode and effect analysis (FMEA), in: A. Bondavalli, F. Di Giandomenico (Eds.), Computer Safety, Reliability, and Security, Springer International Publishing, Cham, 2014, pp. 310–325.

[27] S. Paul, On the meaning of security for safety (s4s), in: 6th International Conference on Safety and Security Engineering (SAFE), 2015, p. 1, doi:10.2495/SAFE150321.

[28] S. Paul, Over 20 years of research in cybersecurity and safety engineering: a short bibliography, in: WIT Transactions on The Built Environment, 2015, p. 15.

[29] J. Brunel, S. Paul, L. Rioux, F. Vallée, J. de Oliveira, G. Gailliard, J.-L. Gilbert, T. Wiander, M. El Bakkali, A. Faucogney, D. Chemouil, Recommendations for security and safety co-engineering (Release n 3) - Part B, 2016, 10.13140/RG.2.1.3649.1923.

[30] P. Popov, A. Povyakalo, V. Stankovic, L. Strigini, Software diversity as a measure for reducing development risk, in: 2014 Tenth European Dependable Computing Conference, 2014, pp. 106–117, doi:10.1109/EDCC.2014.36.

[31] S. Mazzini, J. Favaro, A. Martelli, Security and safety modelling in embedded systems, in: Embedded Real Time Software and Systems Conference, 2014, p. 1.

[32] M. Born, An approach to safety and security analysis for automotive systems (oral presentation), in: SAE World Congress, 2014, p. 1.

[33] M. Paulitsch, R. Reiger, L. Strigini, R. Bloomfield, Evidence-based security in aerospace: from safety to security and back again, in: 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops, 2012, pp. 21–22, doi:10.1109/ISSREW.2012.37.

[34] F.-L. Krause, in: The Future of Product Development: Proceedings of the 17th CIRP Design Conference, 1st, Springer, 2007, doi:10.1007/978-3-540-69820-3.

[35] J. Stark, Product Lifecycle Management: 21st Century Paradigm for Product Realisation, Decision engineering, Springer, 2005, doi:10.1007/978-0-85729-546-0.

[36] L. Finkelstein, A.C.W. Finkelstein, The life cycle of engineering products–and analysis of concepts, Eng. Manag. J. 1 (3) (1991) 115–121, doi:10.1049/em:19910031.

[37] B. Stallard, M. Silverman, Using electronic design automation throughout the product life cycle, in: 2010 Proceedings - Annual Reliability and Maintainability Symposium (RAMS), 2010, pp. 1–5, doi:10.1109/RAMS.2010.5447999.

[38] K. Sakita, T. Mori, Product life cycle simulation system for ecodesigners, in: 2005 4th International Symposium on Environmentally Conscious Design and Inverse Manufacturing, 2005, pp. 527–528, doi:10.1109/ECODIM.2005.1619285.

[39] G.L. Kovács, Evaluation of value changes between different phases of the product life-cycle, in: 2013 IEEE 9th International Conference on Computational Cybernetics (ICCC), 2013, pp. 101–106.

[40] ISO/IEC/IEEE, 26531-2015 ISO/IEC/IEEE international standard for systems and software engineering – content management for product life-cycle, user, and service management documentation, 2015, 10.1109/IEEESTD.2015.7106441.

[41] D.S. Nguyen, Total quality management in product life cycle, in: 2014 IEEE International Conference on Industrial Engineering and Engineering Management, 2014, pp. 754–758.

[42] C. Ebert, Understanding the product life cycle: four key requirements engineering techniques, IEEE Softw. 23 (3) (2006) 19–25, doi:10.1109/MS.2006.88.

[43] B. Sutton, Board test and the product life cycle. get wise to board test strategies, IEEE Design Test Comput. 16 (3) (1999) 28–33, doi:10.1109/54.785826.

[44] E. Bukata, D.C. Davis, L. Shombert, The use of model-based test requirements throughout the product life cycle, in: 1999 IEEE AUTOTESTCON Proceedings (Cat. No.99CH36323), 1999, pp. 53–58.

[45] G. Chen, S. Su, Y. Gong, M. Zhu, The product life cycle-oriented modeling method, in: Third International Workshop on Advanced Computational Intelligence, 2010, pp. 373–378, doi:10.1109/IWACI.2010.5585152.

[46] S. Kumari, G. Kondeti, S. Pakki, T. Chandrasekhar, S. Balu, Method of safety critical requirements flow in product life cycle processes, in: 2011 Integrated Communications, Navigation, and Surveillance Conference Proceedings, 2011, pp. N2-1–N2-4, doi:10.1109/ICNSURV.2011.5935349.

[47] A. Sharon, D. Dori, A project–product model–based approach to planning work breakdown structures of complex system projects, IEEE Syst. J. 9 (2) (2015) 366–376, doi:10.1109/JSYST.2013.2297491.

[48] H. Jun, D. Kiritsis, P. Xirouchakis, Product life-cycle metadata modeling and its application with RDF, IEEE Trans. Know. Data Eng. 19 (12) (2007) 1680–1693, doi:10.1109/TKDE.2007.190661.

[49] K. Nagorny, A.W. Colombo, J. Barata, A survey of service-based systems-of-systems manufacturing systems related to product life-cycle support and energy efficiency, in: 2014 12th IEEE International Conference on Industrial Informatics (INDIN), 2014, pp. 582–587.

[50] IEEE CS, 24748-3-2012 – IEEE guide: adoption of ISO/IEC TR 24748-3:2011, systems and software engineering-Life cycle management-Part 3: guide to the application of ISO/IEC 12207 (Software life cycle processes), 2012, 10.1109/IEEESTD.2012.6189321.

[51] Carnegie Mellon University, Software Engineering Institute, Manag. Tech. DebtData-Driven Anal, 2017https://www.sei.cmu.edu/architecture/research/arch_tech_debt/, (accessed May 2019).

[52] OPENCOSS: open platform for EvolutioNary certification of safety-critical systems, http://www.opencoss-project.eu/, 2011–2015 (accessed May 2019).

[53] EUROCONTROL, System wide information management (SWIM), https://www.eurocontrol.int/swim (accessed May 2019).

[54] ISO, ISO/IEEE 11073 personal health data (PHD) standards.

[55] EN, IEC/EN 62304 medical device - software life cycle processes.

[56] EN, EN 60601-1-10 medical electrical equipment – part 1–10: general requirements for basic safety and essential performance – collateral standard: requirements for the development of physiologic closed-loop controllers.

[57] EN, EN 50126 railway applications - the specification and demonstration of reliability, availability, maintainability and safety (RAMS).

[58] IEC, IEC 61508-1:2010 edition 2.0. Functional safety of electrical/electronic/programmable electronic safety-related systems, 2010.

[59] IEC, IEC 61800 adjustable speed electrical power drive systems.

[60] IEC, IEC 62443 Industrial communication networks -security for industrial automation and control systems.

[61] Cobham Gaisler AB, LEON3FT fault-tolerant processor, https://www.gaisler.com/index.php/products/processors/leon3ft (accessed May 2019).

[62] European Cooperation for Space Standardization, ECSS-Q-ST-80C Rev.1 – software product assurance, 2017 https://ecss.nl/standard/ecss-q-st-80c-rev-1-software-product-assurance-15-february-2017/, (accessed May 2009).

[63] European Cooperation for Space Standardization, ECSS-E-ST-40C – software general requirements, 2009 https://ecss.nl/standard/ecss-e-st-40c-software-general-requirements/, (accessed May 2009).

[64] SESAMO: security and safety modelling, http://sesamo-project.eu/, 2012–2015 (accessed May 2019).

[65] MERGE: multi-concerns interactions system engineering, http://www.merge-project.eu/, 2012–2016 (accessed May 2019).

[66] P. Pop, D. Scholle, I. Šljivo, H. Hansson, G. Widforss, M. Rosqvist, Safe cooperating cyber-physical systems using wireless communication: the safecop approach, Microprocess. Microsyst. 53 (2017) 42–50, doi:10.1016/j.micpro.2017.07.003.

[67] W. Afzal, H. Bruneliere, D.D. Ruscio, A. Sadovykh, S. Mazzini, E. Cariou, D. Truscan, J. Cabot, A. Gómez, J. Gorroñogoitia, L. Pomante, P. Smrz, The megam@rt2 ECSEL project: megamodelling at runtime – scalable model-based framework for continuous development and runtime validation of complex systems, Microprocess. Microsyst. 61 (2018) 86–95, doi:10.1016/j.micpro.2018.05.010.

Luigi Pomante has received the "Laurea" (i.e. BSc+MSc) Degree in Computer Science Engineering from "Politecnico di Milano" (Italy) in 1998, the 2nd Level University Master Degree in Information Technology from CEFRIEL (a Center of Excellence of "Politecnico di Milano") in 1999, and the Ph.D. Degree in Computer Science Engineering from "Politecnico di Milano" in 2002. He had been a Researcher at CEFRIEL from 1999 to 2005 and, in the same period, he had been also a Temporary Professor at "Politecnico di Milano". From 2006, he is an Academic Researcher at Center of Excellence DEWS ("Universitá degli Studi dell'Aquila", Italy). From 2008 he is also Assistant Professor at "Universitá degli Studi dell'Aquila" (he is responsible of the "Embedded Systems" course). His activities focus mainly on Electronic Design Automation (in particular Electronic System-Level HW/SW Co-Design) and Networked Embedded Systems (in particular Wireless Sensor Networks). In such a context, he has been author (or co-author) of more than 100 articles published on international and national conference proceedings, journals, and book chapters. He has been also session chair, reviewer, and member of several TPCs related to his research topics. From 2010, he has been in charge of scientific and technical issues on behalf of DEWS in several European and national research projects.

Vittoriano Muttillo received his Bachelor's degree and Master's Degree (summa cum laude) in Computer Science Engineering from the University of L'Aquila. In 2014 he was a researcher at Centre of Excellence DEWS (Design Methodologies for Embedded controllers, Wireless interconnect and System-on-chip), working on development of middleware for FPGA's embedded multi-core architectures in the context of CRAFTERS (Constraint and Application driven Tailoring Framework for Embedded Real-time Systems) ARTEMIS-JU European Project. Currently he is a PhD student in the area of Information and Communication Technologies (ICT) at the Department of Information Engineering, Computer Science and Mathematics (DISIM), University of L'Aquila. He's advised by Prof. Luigi Pomante. His research interests focus on Embedded Systems, with a particular emphasis on Electronic Design Automation and Model-Based System Level HW/SW Co-Design area. He Currently work on the development of EDA tools, mainly oriented to properly manage Mixed-Criticality and Cyber-Physical application on heterogeneous multi/many-core platform.

Bohuslav Křena is an Assistant Professor at the Faculty of Information Technology of the Brno University of Technology (FIT BUT). His research focuses on formal analysis and verification, especially on analysis of concurrent programs. He received his Ph.D. at FIT BUT in 2004. In 2002, he visited the Central Laboratory for Parallel Processing of the Bulgarian Academy of Science, Sofia, Bulgaria; in 2003, he visited the Edinburgh Parallel Computing Centre at the University of Edinburgh in Scotland; and in 2004 and 2005, he worked as a researcher at the Software Testing and Analysis Laboratory of the Universita degli Studi di Milano-Bicocca, Milano, Italy. Since 2004, he has been working at FIT BUT.

Tomáš Vojnar is a full-time Professor at the Faculty of InformationTechnology of the Brno University of Technology (FIT BUT). His research focuses on computer-aided verification, including, in particular, automata-based and logic-based symbolic formal verification of infinite-state systems (especially programs with dynamic linked data structures); model checking, dynamic analysis, and intelligent testing of concurrent programs; as well as formal verification of modern hardware designs. He received his Ph.D. at the Faculty of Electrical Engineering and Computer Science of the Brno University of Technology in 2001. In 2001–2003, he worked as a post-doctoral researcher at LIAFA, Universite Paris Diderot/CNRS in France. Since 2003, he has been working at FIT BUT. He defended his habilitation thesis in 2007 and became a full-time Professor of Computer Science and Engineering in 2012.

Filip Veljković is a Project Manager at Thales Alenia Space in Spain. He is managing both commercial and R&D projects within the space industry. Previously he has been working as an ASIC/FPGA engineer in several R&D projects within company. He received a B.Sc. and M.Sc. degree in Electrical Engineering from School of Electrical Engineering, University of Belgrade, Serbia. In 2011, he joined COSIC research group at Katholieke Universiteit Leuven, Belgium as a visiting researcher where he was working on securing FPGA-based Random number generators. Following this research path he joined Technical University of Madrid where he worked as a Researcher and a PhD candidate in several projects related to fault tolerance in reconfigurable FPGAs for space applications.

Pacôme Magnin, R&D Manager after computer science degrees and over 10 years in electronic entertainment software technology development and management, he moves in 2007 to embedded systems industry, first on the research programs management in the field of critical systems for rail, aerospace, defence and automotive, and then move to Siemens Industry Software in 2011, in order to manage the research activities and projects in the field of system simulation.

Martin Matschnig has received his Diploma degree in electrical engineering and computer science from Vienna University of Technology in 2000 and joined Siemens in 2001. He was with the R&D department for ASIC and FPGA design for industrial, medical, consumer and communication applications. Starting as design engineer beside implementation he was focused on advanced verification, safety critical chip design and security aspects of electronics, Electronic System Level Design and Design Flow. He holds patents and contributed to publications in the field of ASIC Design. In Siemens Corporate Technology he continues driving safety and security for embedded electronics. He is IPMA Level C certified Project Manager.

Bernhard Fischer graduated in computer science at the Vienna University of Technology in 2011. Since joining Siemens AG (R&D department for Electronic Design, Vienna) in 2011, he has been working in the fields of Electronic System Level Modeling, High-Level Power Modeling, Safety/Security Modeling, Design Flows, and Formal Verification. He contributed to industrial projects and EU-funded research projects in the Industrial Drives domain.

Jabier Martinez joined the Digital Trust Technologies (TRUSTECH) area of Tecnalia in 2018. His background is on providing methods and tools for systems modelling, and for achieving systematic reuse covering all the artefacts that conform a system life-cycle. He obtained the title of computer engineering from the University of the Basque Country in 2007 and, after several years of industrial experience, he received his PhD in 2016 from the Luxembourg University (SnT, Interdisciplinary centre for Security and Trust) and Sorbonne University (Lip6, Laboratory of Computer Sciences, Paris 6) with an awarded thesis about mining software artefacts for product line migration and analysis. He participated in several European research projects. He co-organizes the Reverse Variability Engineering series of workshops, the Control of Alternatives and Quality workshop, and his interests are mainly related to modelling, software reuse, variability management and software product lines.

Thomas Gruber received his Diplomingenieur degree in electrical and telecommunications engineering at the TU Vienna in 1982. He has more than 25 years of experience in the area of railway safety engineering; as Senior engineer and project manager he is currently responsible for or involved in several research projects (Artemis project EMC2, ECSEL projects AMASS, ENABLE-S3, IoSense, SemI40) and customer projects (project planning tools for railway interlocking system, safety analysis for tramway driver assistance system). His main research areas are Safety and hazard analysis methods, Safety critical / fault tolerant system architectures, functional safety standards and safety certification across industry domains, and inter-dependence of safety and security in critical systems.