Detailed overview of AQUAS Results

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

Table of Contents

1 Summary of the context and overall objectives 3
2 Work performed 4
2.1 Methodology Development 4
2.2 Tooling Support 5
2.3 Exploration via application use cases 6
2.4 Awareness, Community development and exploitation support 6
3 Progress beyond the state of the art and potential impact 7
3.1 Methodology advances 7
3.2 Tooling Advances 8
3.3 Industrial Process Evolution 8
3.4 Impact through evolution of standards 8
3.5 Building towards advanced dependability co-engineering in industry 9

1 Summary of the context and overall objectives

Some of the most difficult decisions in system development relate to the coupling or interaction between safety, security and performance (SSP). Key reasons for this difficulty include too little automation support, the multi-disciplinary nature of the problems, and the prevalence, in safety and security activities, of qualitative, rather than quantitative, representations. These decisions are critical because they affect all aspects of a system, with potential serious impact on peoples' lives; they are constrained by regulation and policies as well as by the current production processes. The current scarcity of automation support is partly due to the aforementioned points. Another reason is that integrative technologies take longer to mature (everything else being equal) than component technologies, with the time to maturity dependent on how much they have to take into account. On the other hand, they also return much greater value, through their pervasive effect on multiple parts and qualities of the system.

Improved techniques for these kinds of decisions, with especially improved automation, will enable massive improvements for system development, reducing risk regarding both system operation and development costs. These techniques provide advanced forecasts of the consequences of changes in design or in operation. Automation of SSP and their coupling will enhance technology transfer. It will enable a more robust system environment for applying artificial intelligence. These are strong motivators for adoption of the improved techniques.

To give an idea of this SSP interaction, one can consider that security features are necessary to ensure performance and safety. Therefore, attacks can compromise the other two; conflicts may arise between the means for satisfying these requirements, e.g., a security feature like encryption or authentication may slow down operation in ways that impair safety; synergies may be present, as e.g. a precaution taken for safety also improves security. Management of these interactions is a serious concern in current industrial practice: in particular, conflicts that are not detected and managed early in the lifecycle may require expensive redesigns, or worse trigger product recalls or cause mishaps (accidental or due to attacks) during operation of these products.

The AQUAS project has provided major contributions towards this highly complex challenge, investigating the interactions between safety, security and performance. This includes a methodology with supporting techniques that will support the process of adoption for mainstream industrial practices. We have named this Dependability Co-Engineering (DCE). In AQUAS a DCE methodology of 'interaction points' and 'combined analysis' has formalised the engagements between SSP experts and stake-holders, with the support of these techniques. The AQUAS methodology is supported by a large set of software tools, mostly provided by industrial partners, the functionality of which was significantly extended within the project. The interaction point concept is orthogonal to the specific product lifecycle (PLC) used, and thus could be adopted in industrial practice by different companies, whatever the specific process each uses.

DCE was explored via demonstrators involving product development in the domains of Air Traffic Management, Medical Devices, Rail, Industrial Automation and Space. This included (a) refining the methodology by creating concrete instances of it, in different companies and with different sets of combined analyses and supporting tools as appropriate for those companies, and (b) evaluate the methodology. The AQUAS consortium comprised 23 organisations (manufacturers and research and technology organisations). The lessons learned from AQUAS are summarised in a publicly available document (see Report on the future challenges to be overcome for co-engineering).

The work in AQUAS has been foundational not only for advancing on the technical bottlenecks but also for addressing the non-technical ones. The key outputs from AQUAS support the uptake of DCE by industry and comprise:

- development of a DCE methodology suitable for the entire product lifecycle.
- demonstrators to advance current practices, methods and tools via five industrial use cases.
- analysis of the challenges for industry to adopt automated DCE. A community has been consolidated to advance on technical and non-technical factors with foundations established.
- supported evolution of relevant standards, particularly on mediation between SSP focuses.

Contributions involved more than 10 analysis methods and 40 tool features documented in 19 reports, 60 symposiums and conferences, and 50 publications. The public results are available at https://aquas-project.eu/documents/ and at https://cordis.europa.eu/project/id/737475/results.

Exploitation of AQUAS work is underway on individual bases, through smaller collaborations and also at consortium level. Collaboration agreements have been developed by several partners to build on the AQUAS results, examples including SYSGO and AbsINT, Siemens Austria with Ansys for the use of Medini Analyze. For using AQUAS results in the DCE adoption process, an intermediary committee is currently active to support discussions between the industrial research community and the funding and regulatory authorities. A public-private collaboration is considered as a next step towards DCE automation in industry.

In summary, AQUAS made important steps towards practical adoption of co-engineering of safety, security and performance (dependability co-engineering).

2 Work performed

Demonstrator development was centred around the methodology, tooling and use cases. A technical coordination committee supported the synchronisation of work with the expected project outputs and long-term vision for advanced DCE automation. There were twelve targets with associated key performance indicators guiding the progress and performance assessment. These included addressing use case SSP dependencies with quality specialists aware of their impact on, and impact from, other system quality attributes; full traceability of trade-off artefacts across all product lifecycle phases; and supporting DCE evolution of one standard per domain amongst international standards on functional safety, security and engineering frameworks. The supporting coordination environment including long-term challenges plays an important role for making good headway with research and development for DCE.

2.1 Methodology Development

The AQUAS approach to dependability co-engineering is based on the concept of “interaction points” (IP), points in the product lifecycle when non-functional requirements of safety, security, performance (SSP) are dealt with *together*, by applying suitable methods of "*combined analysis*". Combined analyses are used to check whether these system properties meet their respective requirements, and more importantly to detect conflicts and manage trade-offs between them. Interaction points contain the cost of DCE by limiting the combined analyses to specific points in the lifecycle.

The AQUAS approach allows developers to:

- identify potential conflicts between safety, security and performance requirements of the system under development *earlier in the lifecycle* than would be otherwise possible;

- scope the space of trade-offs between safety, security and performance, and check if an acceptable compromise exists between the conflicting properties for the particular system;
- detect possible synergies, such that e.g. a design feature engineered for safety actually makes it unnecessary to add a separate security control;
- when multiple forms of combined analysis can be applied at each IP are used to achieve better coverage of potential problems, this is done cost-effectively: a “cost model” was developed to forecast the likely costs/benefits from the application of combined analyses and their combination early in the life-cycle.
- The AQUAS methodology seeks thus:

- To improve *System quality.* Safety, security, and performance are improved because the combined analyses allow a *holistic* analysis of systems when needed in the product lifecycle, reducing the risk of neglecting subtle problems due to the interdependencies between safety, security and performance. Thus, methods and tools for combined analyses are a large part of the outputs of AQUAS; much of the effort in the project went into their development and trial use. Appropriate modelling formalisms and analysis methods are applied at each interaction point, from analysis of *coarse-grained models* during requirements specification and conceptual design to progressively more detailed analyses as the design is refined and progresses towards implementation. Since requirements (design decisions) established or confirmed at one IP have to be implemented, and their satisfaction verified, at later IPs, “IP traceability” is an important aspect of the AQUAS methodology.
- To build systems with the desired quality more *cost-effectively*. Early resolution of conflicts between requirements is seen as a major advance of the state-of-the-art, which promises to reduce the whole-lifecycle cost of developed systems – including the cost of development and the cost of maintaining the systems after their deployment. This benefit comes from the combined analyses; the cost of the combined analyses is contained by locating them at the *interaction points only*, rather than repeating them more extensively through the PLC. AQUAS has demonstrated the feasibility of these methods for early detection, analysis and resolution of problems. Assessing the gain so obtained is difficult in a single project, so AQUAS has reported the observations made in the trial application to industrial development use cases, and has developed a “cost model” to help estimate the cost reduction on development, verification and maintenance. The other aspect of cost reduction, which is application-specific, is reduced probability of flaws remaining in deployed products causing accidents, unavailability due to stops and recalls, environmental damage etc.

2.2 Tooling Support

To support the AQUAS's methodology, partners developed, extended and combined tools, covering:

- Support for combined analysis at different stages of PLC, which makes the adoption of respective methods easy. Among examples are several tools which offer a combination of Fault/Attack trees, the TTool (https://ttool.telecom-paris.fr/) which allows one to verify a system architecture against given set of security requirements, and many more.
- Tools which do not support a combined analysis per se (e.g. provers of correctness, comprehensive checks of lack of races in multi-threaded software, or providing highly specialised instrumentation of systems for performance measurement), but are useful in getting assurance that a particular aspect of system development is addressed well or, in combination with other tools (i.e. via creation of a “tool chain”), allow for a sophisticated combined analysis.

- Tools which support system engineering (e.g. based on SysML) with integrated support for analysis of non-functional properties. A noticeable example here is the extension of the CHESS (https://www.eclipse.org/chess/index.html) tool to allow for the generation of SAN (stochastic activity networks) models from a given system architecture (as a SysML model) and a description of the cyber-attacks anticipated to be applied to a given system.
- Tools that provide support for early validation by emulating the intended *operational environment*, particularly important for cyber-physical systems.
- Support for the integration of the interaction points within the PLC4CE (Product Lifecycle for Co-Engineering), which extends concept of traceability to include interaction points and the decisions taken at them.

2.3 Exploration via application use cases

The AQUAS project's approach to developing the methodology was strongly *empirical*. The general concepts of interaction points and how they would affect the PLC were specified at project level, but this philosophy was then applied in practice in the five use cases (UCs), developing “demonstrator” systems in five application domains. Over the duration of the project, each use case went through a segment of the product life cycle for its demonstrator system. In each use case, the company that developed the demonstrator product selected suitable combined analysis techniques and supporting tools (available from project partners) and assembled them in interaction points following their own lifecycle, dictated by the company's and industrial sector's experience and standards.

One practical example for combining various tools and techniques for the Industrial Drives use case is a tool chain consisting of three tools to carry out complementary analyses. medini analyze (http://www.medini.eu/) enables SysML-based modelling of the industrial drives system architecture together with (non-)functional requirements capturing, management and analysis for dependencies (interferences). With the tool’s automation support an initial set of potential interferences is generated. Based on this set experts (e.g. safety/security expert) decide when (in which phase of the PLC) and how (method and tool to apply for analysis) to analyse the identified potential conflicts or synergies (interference analysis). The SysML architecture and requirements are exported into CHESS (https://www.eclipse.org/chess/index.html) where safety and security models are added (sequence diagrams and state machines) for performance (worst-case execution time) analysis. CHESS supports the creation of Stochastic Activity Network (SAN) models that are imported into the tool Möbius (https://www.mobius.illinois.edu/) where the SAN model is enhanced for conducting systematic safety/security experiments based on Monte Carlo simulation. The system architecture is explored by running several scenarios with security attacks and various security and safety measures. The results are used to decide when to deploy “software cleansing” to enhance the overall reliability of the system. Research and development efforts spent for developing this toolchain for co-engineering enables system architecture optimization early in the product life cycle without the need for real-world hardware.

2.4 Awareness, Community development and exploitation support

Awareness is essential for establishing industry momentum towards a common approach, of course for the public and potential customers, but in the case of DCE, especially for consolidating an active community and reaching policy makers and national regulators. Several project communication channels were established through Facebook, LinkedIn, Twitter, a public mailing list and our website. During AQUAS there were over 3000 unique visitors, spending on average 1.24 minutes. Consortium members contributed to awareness and community building through over 50 publications, involvement at 68 industrial events (booths, fairs, and exhibitions), 21 presentations to customers

and business partners and also 10 internal dissemination events. Over 30 stakeholders joined the DCE community.

While AQUAS has been driven by the question of DCE exploitation (uptake to mainstream practice), we also had additional support actions. An Advisory Board with 23 members from academia, industry and government contributed to awareness, community development and exploitation support. There were six workshops with the Advisory Board, which were very useful for guiding and validating the direction of our work, finding weaknesses and also identifying challenges and enablers to be considered for DCE. Another action provided preliminary studies of other engineering activities on the market to identify synergies and mutual benefits for future investigations. This is useful to identify what can be learned from them to avoid reinventing the wheel, and showing what DCE can bring to these topics. Five key areas were selected in discussion with the consortium: Agile Engineering, Incremental Certification, Concurrent Engineering, Technical Debt, Uptake by AI/IoT, Usability.

An important point is that several AQUAS tools are available as Open Source (see https://aquas-project.eu/links/).

Finally, standards evolution represents a key action for exploitation support. More about this is described under Potential Impact.

3 Progress beyond the state of the art and potential impact

3.1 Methodology advances

The AQUAS methodologies, as trialled in the AQUAS use cases (see Report on the future challenges to be overcome for co-engineering), offer these advances:

- shifting some dependability co-engineering activities to *take place earlier* in the PLC (a primary objective for AQUAS). In the use cases, AQUAS methods made it possible to perform early trade-off analyses and verification of properties that otherwise would be delayed until after implementation, multiplying the cost of correcting any flaw discovered.
- Techniques for identifying interdependencies between safety, security and performance problems appeared *effective and productive*, leading to early analysis of possible design improvements to mitigate risk.
- Costs of adoption of the methods were seen as being certainly *non-zero*, but not such as to prevent adoption. For instance, some models may require effort of the order of person-months to produce/maintain them as needed, but the reduced risk of serious problems in operation, potentially affecting huge numbers of installed units, would justify the expenditure. For costs in the PLC before deployment, the cost model developed was trialled on two use cases. Besides confirming that AQUAS-style DCE is an affordable improvement, it was observed that it could actually reduce costs for organisations needing to newly introduce security concerns in their processes.
- Support of the methods by mature tools was seen as an *essential factor* for accelerating the adoption of the AQUAS methods. Hence the provision of tools was seen as a substantial contribution to the credibility and exploitability of the methodology.

Indications for work after AQUAS to complete an IP-based co-engineering approach concern further extensions to the tooling support; exploring the potential for dynamic scheduling of interaction points; application of the techniques to re-assurance or re-certification; extending the techniques to further support software implementation.

The AQUAS methods and tools provide building blocks that adopters can combine into their own instantiations of the AQUAS methodology. In general, the choice of combined analyses at each PLC phase is a natural extension, towards co-engineering of dependability properties, of the analyses commonly applied in pre-AQUAS PLCs. According to the AQUAS experience, these extensions facilitate the early resolution of co-engineering problems; and in turn depend on the availability of mature tooling to ease adoption of these methods.

3.2 Tooling Advances

During this project, we developed 16 novel tool prototypes driven by the new AQUAS methodology. These prototypes involved either the creation of unique and new tools or the modification of existing ones. We built 46 new tool features during these activities.

With AQUAS we demonstrated a new way to accelerate and improve systems DCE. The AQUAS results show that tools are able to tackle other applications where SSP is a critical blocking point. Tool providers will (and already have) use the AQUAS basis for future research initiatives and advanced projects for their customers.

3.3 Industrial Process Evolution

The advancements of tools and methods for Dependability Co-Engineering during AQUAS enabled enhancements of product lifecycles in all use case domains. Through the introduction of the concept of Interaction Points together with Combined Analysis as part of the industrial process, system quality attribute engineering was raised to a new level where safety, security and performance attributes as part of requirements and system architecture could be studied, analysed and explored concurrently. Applying the AQUAS methodology in the demonstrators has shown that efforts are moved from later PLC phases (such as verification) to earlier phases related to system concept and system design. This led to a positive impact on the overall development effort since mistakes detected in late phases are potentially more costly than those detected in an earlier PLC phase.

Another advantage of the AQUAS methodology lies in the incorporation of Interaction Points in the PLC that is inherently forcing quality domain experts to analyse cross-effects and interdependencies between system quality attributes. Results of such analyses raise the awareness of the potential impact of design decisions and act as anchor points for thorough system analysis together with consideration of safety and security standards. Additionally, the AQUAS methodology adds towards contradiction-free and complete sets of requirements. The orchestration of co-engineering methods and tools together with the PLC concept (Interaction Points) increases the confidence in system design and thus lowers the probability of unexpected changes late in the product life-cycle up to operation and maintenance. The systematic approaches with Combined Analysis and Interaction Points taken in the demonstrators indicate that adaptions to product solutions and the preparation of the certification are eased as well.

The demonstrators served as vehicles for elaborating the AQUAS methodology and thus built a foundation on an experimental base for the migration of AQUAS technology for co-engineering with system quality attributes in industry-grade processes for application domains such as air traffic management, medical devices, railways, industrial automation and space.

3.4 Impact through evolution of standards

AQUAS partners have recognised the benefits of standardisation for co-engineering purposes during the project and established collaborations to improve the European and global framework of standards and maximise the uptake of the project results by Industrial, Regulatory, Academic and other stakeholders (see Report on the evolution of co-engineering standards).

Significant results of the collaboration effort are:

- The analyses of CE gaps in representative standards, including standards that were either undergoing updates now or identified by AQUAS as needing improvements for DCE.
- Dedicated strategies for building consensus and actively influence the evolution of the development processes supported by the standards, according to their states in the revision cycles.
- A number of actionable requirements, interactions and published papers to influence standards and raise awareness for SE beyond the end of the project.

For example, AQUAS partners contributed to updates to IEC 61508-3 and IEC 61508-1/2, that make consideration of cybersecurity during Risk and Hazard Analysis Phase a normative requirement, with the necessary follow-up processes if an impact of security threats on safety is identified.

Related standards in multiple domains are currently under revision or (especially for security standards) for the first time under development, or even lacking (as in the case of performance). The interplay between SSP dependability attributes is being increasingly acknowledged by involved stakeholders and discussions on how to react to this development in standardization is still ongoing.

Major impact of the standardisation effort will be derived from the provided foundations and clear directions for standardisation and alignment between the outcomes of the project and standards in the near future.

3.5 Building towards advanced dependability co-engineering in industry

AQUAS has worked towards a vision of integrated, automation supported DCE in mainstream industrial development. This implies significant benefits but also challenges, because we are seeking to trigger the evolution of engineering processes across industry. AQUAS has laid down foundations that will support industry to evolve towards their desired levels of automated DCE. It will likely take 10-15 years to have a comprehensive common approach to industry adoption. The hurdles include selecting directions of research and advancement where there is a combinatorial explosion of possibilities; including harmonised training across Europe, and the specific mechanisms for DCE coordination with individual projects as steps in an industrial evolution process.

In relation to the immediate actions following the project, for consensus the consortium has reached out to other parties interested in more extensive adoption of advanced, automation-supported DCE in industry. The priorities appear to be for cross-project coordination support and wider recognition of DCE. So to support establishing a DCE central coordination committee, an interim team has been formed to sustain the network developed via AQUAS and involve the relevant authorities to consider public-private collaborations. Direct involvement of such authorities could balance industry's short-term pressures by encouraging development of a culture and community with longer-term focuses. A broader recognition by industry of DCE as a research and technical domain in its own right, with provision of courses on DCE, would encourage a positive feedback loop with increasing recognition of DCE by standards, journals and technical associations. On top of the founding principles for an adoption process and methodology, enterprises would add their own specific DCE. These actions would extend existing academic and industrial DCE cultures and develop means to share best practices, like a publicly funded repository of case studies with technical implementation in the form of open source tools, examples, and a knowledge database, thus promoting the ubiquitous deployment of DCE. Such activities would provide a common basis on which enterprises will add their specific layers.

The work in AQUAS has made foundational advances on important technical aspects of DCE and also to some extent on non-technical ones. These advances are valuable for use in industry now as well as creating the basis for more extended automation and adoption of Dependability Co-Engineering and its automation.