International Journal of Systems and Software Security and Protection
Volume 11 • Issue 2 • July-December 2020

Towards a Secure DevOps Approach for Cyber-Physical Systems:
An Industrial Perspective

Pekka Abrahamsson, University of Jyväskylä, Finland
Goetz Botterweck, LERO, Ireland
Hadi Ghanbari, Aalto University, Finland
https://orcid.org/0000-0002-9725-3025
Martin Gilje Jaatun, SINTEF Digital, Norway
https://orcid.org/0000-0001-7127-6694
Petri Kettunen, University of Helsinki, Finland
https://orcid.org/0000-0002-2928-5885
Tommi J. Mikkonen, University of Helsinki, Finland
Anila Mjeda, LERO, Ireland
https://orcid.org/0000-0003-1311-6320
Jürgen Münch, Reutlingen University, Reutlingen, Germany
https://orcid.org/0000-0003-0327-8094
Anh Nguyen Duc, University of South Eastern Norway, Notodden, Norway
https://orcid.org/0000-0002-7063-9200
Barbara Russo, Free University of Bozen-Bolzano, Italy
Xiaofeng Wang, Free University of Bozen-Bolzano, Italy

ABSTRACT

With the expansion of cyber-physical systems (CPSs) across critical and regulated industries, systems must be continuously updated to remain resilient. At the same time, they should be extremely secure and safe to operate and use. The DevOps approach caters to business demands of more speed and smartness in production, but it is extremely challenging to implement DevOps due to the complexity of critical CPSs and requirements from regulatory authorities. In this study, expert opinions from 33 European companies expose the gap in the current state of practice on DevOps-oriented continuous development and maintenance. The study contributes to research and practice by identifying a set of needs. Subsequently, the authors propose a novel approach called Secure DevOps and provide several avenues for further research and development in this area. The study shows that, because security is a cross-cutting property in complex CPSs, its proficient management requires system-wide competencies and capabilities across the CPSs development and operation.

KEYWORDS

Aerospace, Agile Development, Automotive, Continuous Deployment, CPS, Development Methodologies, Empirical Research, Energy, Healthcare, Secure Software Engineering, Software Security

DOI: 10.4018/IJSSSP.2020070103

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

1. INTRODUCTION

In recent years, with the emergence of Cyber-Physical Systems (CPSs), societies have become interconnected (Müller, 2017). This increased connectivity is associated with greater concerns related to various quality attributes, such as safety and security. The incidents and risks of operating CPSs are essential nowadays due to the expansion of CPSs across critical and regulated industry sectors such as energy, aerospace, automotive, and healthcare, where even minor failures may lead to devastating human and financial loss. Therefore, higher levels of security and reliability must be achieved in developing CPSs, and these systems must also stay continuously updated to remain resilient in operation, especially during critical events such as cyber-attacks (Yasar & Kontostathis, 2016).

At the same time, production organizations in critical and regulated domains, e.g., automotive, aerospace, and healthcare express an increasing interest in utilizing the DevOps approach for developing and maintaining consumer CPSs (e.g., wearables, virtual reality), as it enables them to shorten time-to-market and be more responsive to operational demands of customers and the market in general (Foehr et al., 2017; Stirbu & Mikkonen, 2010). However, adopting DevOps in industrial domains is extremely challenging due to the complexity of critical CPSs and the devastating costs associated with their downtime, as well as strict requirements demanded by regulatory authorities within those domains (Giaimo, Yin, Berger, & Crnkovic, 2016; Törngren & Sellgren, 2018, Morales, Yasar & Volkmann, 2018). Therefore, there is an increasing need for novel solutions and technologies enabling organizations to benefit from DevOps and, at the same time, maintain the required high levels of security and reliability in critical CPSs.

The objective of our study was to obtain a better understanding of what these novel solutions and technologies entail. To this end, a set of research questions were formulated as below:

RQ1: What are the needs of critical and regulated industries for integrating security into DevOps?
RQ2: What are the benefits and characteristics of such systematic integration expected by these industries?
RQ3: What is the impact of such systematic integration on the company's business?

To answer the research questions, we conducted a qualitative survey of 33 companies active in a variety of critical and regulated industrial sectors to explore the gap in the state-of-practice on DevOps-oriented continuous development and maintenance of CPSs. As such, we make three contributions to research and practice. First, we provide an empirical insight into a set of key needs of and expected benefits from implementing DevOps while complying with required security standards in CPSs development and deployment, as well as the business impacts that it can produce on the implementing companies. Second, based on these identified needs, benefits and impacts, we envisioned a new approach, called Secure DevOps, which encompasses human factors, tools, technologies and processes for adopting DevOps integrated with security across industrial domains. Finally, we propose three main areas which deserve future scientific research as well as further development in practice.

The remainder of the paper is organized as follows. Section 2 provides a review of literature related to CPSs and security in critical and regulated industries, and DevOps in such a context. The research methodology is explained in Section 3, and the findings are reported in Section 4. In Section 5, we present the envisioned Secure DevOps approach based on the findings of the study. Section 6 concludes the paper with highlights for future work.

2. LITERATURE REVIEW

2.1. CPSs in Critical and Regulated Industries

CPSs have been defined as the integration of calculation and physical processes, which involves embedded computers and networks monitoring and controlling the physical processes (Lee, 2007).

As an emerging research area with the overlapping and integration of multiple fields of science and engineering, CPSs require software and system engineers, computer scientists, and network professionals to collaborate closely with experts in various fields such as automation and control, civil engineering, mechanical engineering, and biology.

The generic architecture of an Internet of Things (IoT) system proposed largely defines the elements of modern CPSs (Taivalsaari & Mikkonen, 2017), including 1) client devices; 2) gateways; 3) backend cloud, including databases and other storage systems; 4) analysis applications; and 5) end-user applications. All of these elements rely on computers and computing. Additionally, in many setups, they can all be safety-critical for various reasons. Furthermore, CPSs built for critical and regulated domains such as healthcare, aerospace and automotive have additional complexities and strict requirements (Khaitan & McCalley, 2015, Morales, Yasar & Volkmann, 2018). CPSs in such domains often rely on thousands of live sensors and field devices that must be functional and constantly monitored to control physical systems. However, since these systems are distributed rather than centralized in nature, monitoring, diagnosing, and analyzing these systems becomes more challenging. Finally, failure of critical CPSs are associated with significantly high costs and may, in some cases, be lethal to human beings or even lead to global catastrophes. Therefore, the construction of critical CPSs is often subject to strict certification, which is time-consuming and requires formal software development processes. For instance, the European Space Agency requires software companies to comply with standards such as ECSS-E-40 and ECSS-Q-80.

To set baseline requirements associated with quality, standardization organizations, such as the International Organization for Standardization (ISO), have created standards that describe the processes and requirements for developing software in such a manner that regulatory authorities will accept the product to the markets. By proving compliance with these standards, a company can show to the authorities that the software has been developed with a process that ensures safety and security

2.2. Security in CPSs

Securing CPSs against malicious attacks is of utmost importance, as otherwise, malfunctioning and insecure CPSs can cause enormous damage to individuals, businesses, nations, and the humankind. With the growing importance of CPSs in our daily operations, concerns regarding their security and resiliency have also been raised (Yasar & Kontostathis, 2016). Due to their complexity and interconnectivity, the new generation of CPSs have to deal with new vulnerabilities and threats (Diaz. & Muñoz, 2020), which makes these systems more susceptible to attacks. A framework proposed represents CPSs security from a three-dimensional perspective (Humayed, Lin, Li, & Luo, 2017):

1. The security perspective considering well-known taxonomies of threats, vulnerabilities, attacks, and controls;
2. The CPSs components perspective considering cyber, cyber-physical, and physical components; and
3. The CPSs systems perspective, including general CPSs features and representative systems, such as smart grids and smart cars.

In addition to address core security principles such as confidentiality, integrity, and availability (Merkow & Raghavan, 2010), other security concerns must also be considered in the context of CPSs, including resilience to attacks (Merkow & Raghavan, 2010, Yasar & Kontostathis, 2016), data authentication (Merkow & Raghavan, 2010; Duc, Jabangwe, Paul, & Abrahamsson, 2017), access control (Merkow & Raghavan, 2010), client privacy (Merkow & Raghavan, 2010; Duc et al., 2017, Henkel, 2017), multiple layers of security (Suo, Wan, Zou, & Liu, 2012), certifiability (Farroha & Farroha, 2014), the influence of humans on the maintenance and operating security-related aspects of CPSs (Duc et al., 2017), and integrating security into system development lifecycle as well as when it is deployed and becomes operational (Merkow & Raghavan, 2010).

Previous research on CPSs security mainly focuses on threat detection and prevention, attack modeling, trust management, and detection and assessments of faults and vulnerabilities, while proposing various security controls for protecting the new generation of CPSs (Khaitan & McCalley, 2015). However, there is a lack of systematic research on security in CPSs (Humayed et al., 2017), especially from a software engineering perspective which plays a key role in CPSs implementation. Novel approaches are needed to leverage modern methods, such as DevOps, in developing secure and resilient CPSs that comply with regulatory requirements (Laukkarinen, Kuusinen, & Mikkonen, 2017, Yasar & Kontostathis, 2016). However, potential security issues to be exacerbated by using such approaches must be taken into consideration and dealt with appropriately.

2.3. DevOps and CPSs

Due to regulatory requirements, the development of CPSs in critical domains has typically suffered from long development life-cycles. A common misconception is that regulated software development needs waterfall-like development where phases follow each other in a strict order, and no agile approach is applicable. However, this claim is questionable when agile approaches are tailored to fit regulation needs (Cawley, Wang, & Richardson, 2010, Leppänen, Rindell & Hyrynsalmi, S., 2018, Mohan & Othmane, 2016).

The term DevOps emerged a decade ago as an amalgamation of Development and Operations (Virmani, 2015). It was a reaction to a perceived disconnect between developers and operators within the same organization and has been particularly highlighted in later years in companies that develop and operate software solutions in the cloud (Jaatun, Cruzes, & Luna, 2017, Mohan & Othmane, 2016).

DevOps is closely related to the concept of continuous delivery and deployment, and virtualized infrastructure enables infrastructure as code, where major parts of the deployment and configuration effort are done using pre-configured scripts (Düllmann, Paule & v. Hoorn, 2018). This allows organizations employing the DevOps paradigm to deploy new versions several times a day. The other part of the equation, the operations, is configured to provide feedback from daily operations, which in turn supports the development and deployment of new and enhanced features at a rapid pace.

However, the increased speed could easily come at the expense of security. The quick turnaround expected in DevOps makes it difficult to enforce security gates and testing regimes that are part of many Secure Software Development Lifecycles (S-SDLCs). In the context of regulated development, such as IEC 62304 (Medical device software life cycle processes) and IEC 82304 (Health software product safety), these gates are an essential requirement for any system. On one hand, DevOps practices make it easier to fix security flaws when they are discovered, since there is essentially no difference between a security patch and any other deployment. In the DevOps approach, security has generally been under the umbrella of operations. However, security must be prioritized as a key concern throughout the development process and even after deployment (Merkow & Raghavan, 2010). Therefore, to integrate security and improve DevOps, it is essential to perform security tests as a part of the automated test that applies to all software. On the other hand, continuous monitoring is necessary for identifying security vulnerabilities and breaches and addressing them rapidly (Farroha & Farroha, 2014, Mohan & Othmane, 2016).

3. RESEARCH METHODOLOGY

A qualitative survey (Robson, 2011) approach was deemed suitable to answer our three research questions, which aimed at exploring the perceptions of companies operating in critical and regulated domains on applying DevOps while addressing security concerns. A qualitative survey allows multiple levels of analysis (Jansen, 2010) and is widely used in the Software Engineering research community (Andersson & Runeson, 2002; Ayala et al., 2018).

The qualitative questionnaire was designed that reflected the three main research questions, i.e., RQ1-3 in Section 1. It gathered data on the needs and the benefits of systematically integrating

security with DevOps and the impacts that such integration can have on the business of the companies. In addition, there were also questions concerned with the company profile, i.e. application domains, number of employees, headquarters, and key development processes, to provide the organizational contexts of responding companies.

A convenience sampling strategy was adopted due to the difficulties in recruiting company subjects. The survey was conducted within the scope of a European research initiative within the H2020 Framework Programme. We sent the questionnaire to a group of companies that were involved in this initiative. These companies are based in Europe, but many of them are multi-national and have businesses across the globe. They are all actively developing CPSs in critical and regulated industry sectors. The data collection lasted three months, from January 2017 to March 2017. In total, we have received responses from 33 companies. A follow-up communication was performed in April 2017 to clarify companies' responses.

The survey responses were first analysed individually and then aggregated for text coding. In coding, the key concepts in the responses (i.e., codes) of each main research question were identified. A reference from each code to the original responses has also been stored to be used as quotes and examples. Codes are then categorized as needs, benefits, and characteristics of a Secure DevOps approach as described in the following. The results are first summarized (Sections 4.1-4.3) and then illustrated by sector (see Table 1). The Secure DevOps approach we propose is finally derived from the characteristics in Table 1 and graphically illustrated in Figure 3. In particular, Table 1 details the needs, benefits and characteristics per sector. Codes that are shared among two or more sectors are reported only for the sector from which we received more responses. For this reason, the sector Data analytics and Big Data (DABD) does not appear in Table 1. Figure 3 illustrates the different components of Secure DevOps according to the results of our qualitative analysis.

4. RESULTS

Figure 1 shows the geographical distribution of the companies that participated in the survey. As shown in Figure 1, these companies are distributed across Europe, spanning from North to South and East to West. Figure 2 illustrates the business sectors. The main business domains these companies operate in are automotive, aerospace, healthcare, and energy, where CPSs play an increasingly crucial role. The surveyed companies are consumers, producers, or consultants of CPS technologies and related services.

In the following subsections, we provide answers to the research questions, based on the empirical data we have collected. The section is structured as follows. We first present the needs and the benefits of integrating security in DevOps and then report the impact of Secure DevOps on the CPSs industry.

4.1. The Needs for Secure DevOps (RQ1)

4.1.1. Security is Critical for Both Hardware and Software

The survey results demonstrated in a clear manner that the continued convergence of IT and OT (Operational Technology) systems, along with expanding connectivity to the Internet, exasperated by the growth of the Industrial IoTs, has introduced a larger threat landscape for potential exploitation by adversaries. The new generation of embedded systems interconnected via Internet through wired or wireless connections is more vulnerable to cyber-attacks, especially in critical domains (Sharma et al. 2017). As such, both hardware and software security are critical for existing and new CPSs as one respondent operating in the healthcare sector stated:

The security of our solutions, both at the component level, network level and application level are of paramount value. Not only is our hardware being used in highly sensitive scenarios, but also they are being used to test vulnerabilities in other systems.

Table 1. Key concerns in integrating security in DevOps and characteristics of secure DevOps per CPSs domain as envisioned by the survey respondents

Company Sector (see Abbreviations in Figure 2)	DevOps-Related Needs and Benefits	Security-Related Needs and Benefits	Secure DevOps Impact and Characteristics
HMT	• Large installed base of products be serviced and upgraded in short times; • Improve the overall handling costs while ensuring the required safety and security needs; • Adaptation of the DevOps architecture in existing models, working instructions	• Data access needs to be secure to a high level; • Safety and security by executing the DevOps actions on the equipment; • Security-by-design; • Maintain a well-organized development and release cycle with satisfactory levels of security	• Continuous monitoring and delivery for hospital-based systems; • Devices connected to cloud and network services; • Multitude of semi-professional devices
AE	• Distributed systems including multiple software and firmware levels must be easily reconfigurable in a fully distributed fashion	• Integrate security considerations from its very initial conception; • Security of the system, the entire set of system users while allowing several degrees of access privilege; • Space systems have to be validated against the standards • Distributed systems including multiple software and firmware levels must be securely reconfigurable in a fully distributed fashion	• Deploying the system, a high level of security be maintained in a multi-user, multi-connected environment; • New validation and test procedures to guarantee the proper performance and security of the system in the new complex environment
AU	• Cloud with telematics interfaces, CAN bus;] • Electricity distribution network, sub-stations, transformation posts and other equipment	• Managing security issues after the development phase is expensive and time-consuming; • Adding cyber security to the current service; • Security assessment and penetration testing; • Security problems have an impact on the safety; • Qualified vendors to introduce new and advanced cyber security features	• Car technology adoption; • Security-by-design, automotive market; • Connected Car
E	• Car technology adoption; Security-by-design, automotive market;	• Qualified vendors to introduce new and advanced cyber security features	• Regulated distribution and supply businesses; • Transformational process regarding Smart Grid security
S	• Hardware, applications, own devices; • Autonomous pre-processing of the acquired data, communication with server/cloud, local storage/ retrieval of the data	• Increased security needs arise in application areas; • Robustness of systems against attacks, digital signatures, reliable and certified source of sensor information	• Implementation of the security concepts; • Integrate security features in the embedded solutions; • Application development processes (and skills) to the new environment

continued on following page

Table 1. Continued

Company Sector (see Abbreviations in Figure 2)	DevOps-Related Needs and Benefits	Security-Related Needs and Benefits	Secure DevOps Impact and Characteristics
T	• Data from the network to enable early and automatic detection; • Dynamically balance an IT network	• Securing the systems against cyber threats; • Security requirements from the initial architecture definition	• Complement conventional networks with satellite market and its technology evolving satellite broadband communications
SS	• Reduce the time of the testing process	• Combining security as an integral part of continuous operations; • Incorporate safety and security in the toolchain; • Implement security both as part of the normal operation and as part of the DevOps activity to provide secured field upgrades for application code, middleware and real-time operating systems • Adopt and adapt guidelines al- ready developed in other domains (as the ICT one OSSTMM, NIST and OWASP) for a completely connected car	• Adopt product architectures that enable safety and security compliance; • Adopt new processes and tools that incorporate safety and security in the toolchain; • Feed new requirements to standards and certification bodies; • Introduce team-building and new roles for security integration;
CSI	• Develop fast and seamless Dev- Ops approach without having to compromise on security aspects • Build communities for design thinking, DevOps and advanced analytics; • Integrate customer processes, applications, and people in service provider technology and service ecosystem; • Reduced cost and improve collaboration between development and deployment teams; • Keep up with the needs of the new tools and technologies to enhance DevOps	• Increase and ensure focus on security at the service design and transition processes; • Need of personalized training and evaluation of cybersecurity capabilities of both Development and Operations Teams • Structurally improve security of customer environment by applying best agile development practices and requirements; • Make the solution distinctive when compared to other actors in the software industry and hence guarantee competitiveness; • Deepen the co-operation with developers, IT, Security and Risk Management	• Create a platform to train and evaluate trainees for Secure DevOps • Adopt policies, concepts and security mechanism to ensure the right level of cybersecurity • Integrating development process to customer business processes, technology and continual improvement in order to leverage effect; • Define and develop solutions for remote upgrade of security components; • Define automatic security reporting tools and procedures tailored to CPS (different means of communications, lower processing power etc.); • Integrate security safety and privacy procedures in development IDEs; • Develop solutions for predicting security downtimes

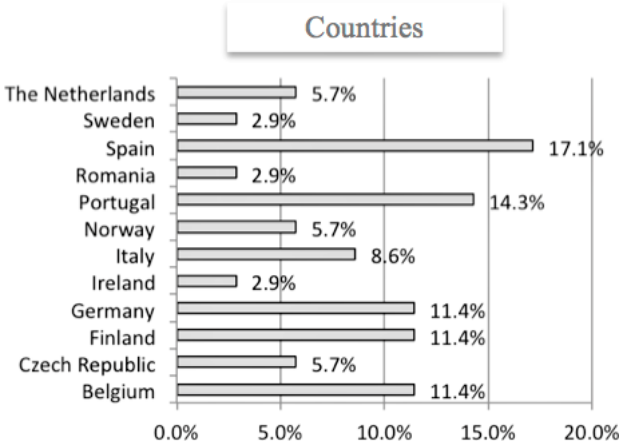
continued on following page

Table 1. Continued

Company Sector (see Abbreviations in Figure 2)	DevOps-Related Needs and Benefits	Security-Related Needs and Benefits	Secure DevOps Impact and Characteristics
TIoT	• Develop proprietary solutions to control and monitor integrated ystems	• Define security requirements • Implement continuous real-time risk management and scalable security measures by established PDCA-cycles in threat modeling (STRIDE method) during the whole CPSs lifecycle; • Reduce costs and time by avoiding implementation bugs and architectural flaws due to the integrated risk management and security view during the whole CPSs lifecycle; • Co-operation between the CPSs- design and security experts during the whole lifecycle	• Optimize a comprehensive threat mod- eling and scalable security measures to CPSs-specifics • Adapt and create new toolsets (e.g. for an automatically threat modeling process and improved risk managment); • Integrate cryptographic schemes and intrusion detection system in DevOps

Note: Duplicate concerns and characteristics among sectors have not been reported. DADB is not reported as no specific information.

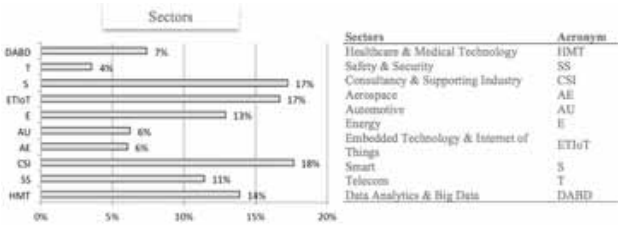
Figure 1. Geographical distribution of the surveyed companies



4.1.2. Security Concerns Must be Strategically and Systematically Incorporated in the Whole System Development Process

For companies developing or using automotive and aerospace software, the respondents sense the urge to be proactive and prepared to address these concerns and incorporate them into their software development processes. This is particularly relevant for companies that intend to open access of their systems to a third party. Integrating security in DevOps is specifically needed as reported by service providers:

Figure 2. Distribution of business sectors of the surveyed companies (some companies are in multiple sectors)



DevOps-driven services rely on automation, virtualization and smart tool choices, which require security aspects to be included in the DevOps pipeline.

As by now, companies need a more thorough strategy for security integration involving the entirety of their system development:

In the current [solutions], the security is often limited to data security or to the middle-ware as isolated pieces. Securing the whole system remains a project-by-project specific task requiring specialized know-how.

4.1.3. Security Must be Integrated by Design at the Earliest Phases of Development in a Semi-Automated Manner

There is the need to improve security features with an integrated approach that covers all development and validation phases of a product in a simple, fast and flexible way. Therefore, security must be integrated by design: security must be considered and handled from the beginning of system development in a systematic and holistic way. A service provider in the healthcare sector further suggests:

It is fundamental that we apply the same security by design methodology and put it to the test, to every system we develop to ensure that our solutions can be easy yet very securely, re-configurable in a fully distributed fashion.

The integration of security in development processes must follow the modern development practice where automation is essential (Casola, De Benedictis, Rak, & Villano, 2019 Casola, De Benedictis, Rak & Villano, 2020). Of course, as any human-centric activity in development, full automation is not conceivable. A semi-automated approach where security specifications are designed by developers and checks of such specifications are automated is the most viable solution today:

As companies become bit by bit more aware of the relevance and importance of security during the development of their products, we have seen a slow but steady move from performing security-related activities late in the development life-cycle (for example penetration testing before release) to earlier phases of the life-cycle (for example secure code reviews). However, there is a long way to go - understanding how development and security-related activities can be combined in a semi-automated way.

4.1.4. Balancing Between Speed and Security

The increase of security concerns and certification, however, does not overshadow the need for speed and agility. That is why the DevOps approach is appealing to many companies. The typical example

is the aerospace sector. The respondents from this sector reported that development activities could account from 35% up to 80% of product development cost once certification is included. The cost would further increase with re-certification that also slows down implementation and maintenance activities. A new, more flexible process is essential. As such, companies in our sample see DevOps as an opportunity to boost innovation and increase the agility of their development processes and Secure DevOps cannot invalidate such benefits.

Currently, security and DevOps are two parallel worlds and due to a lack of supporting tools, security requirements are handled manually rather than automatically. In this setting, integrating speed and agility with security requirements imposes a big burden on companies that might not be able to satisfy all their needs in security while adopting DevOps:

It is a significant burden to maintain a well-organized development and release cycle with satisfactory levels of security in the released products while at the same time being able to respond to customer requests for new features.

4.1.5. Teams must be Trained for Secure DevOps

There is a lack of a comprehensive approach for the competencies that are related to cyber-security. There is a need to develop events like "cyber security capture the flag" that put together security professionals and/or students learning about cyber-security, which can be an opportunity since they can be applied in various social environments and audiences:

A competency framework with a holistic approach including technical and non-technical skills such as team collaboration and time responsiveness, but also psychological and pedagogical competences.

4.2. Expected Benefits and Characteristics of Secure DevOps (RQ2)

4.2.1. Secure DevOps Involves the Whole CPS Lifecycle

According to Table 1, applying Secure DevOps would impact on the whole lifecycle of CPSs development processes by extending the security coverage to all phases, including system development, device deployment and provisioning, standard operations, maintenance, and system dismissing. By adopting Secure DevOps, most surveyed companies expect to achieve faster, more cost-effective, and more efficient development and maintenance of secure CPSs and be able to provide more frequent and safe updates to software, under a wide range of circumstances with increased reliability of the process.

4.2.2. Secure DevOps Eases the Certification Process

For those companies that are constrained by regulations, they also expect that certification processes are carried out more quickly and evidence needed for certification are gathered more easily, should the Secure DevOps approach be adopted. It also implies that proactive actions could be taken based on the collected evidence to ensure:

forthcoming regulatory changes and evolution by being a forerunner in regulatory advisory process.

They also foresee:

reduced costs and pain associated with certified mission-critical software development.

4.2.3. Secure DevOps Speeds Up Continuous Deployment

A closer collaboration between software development and operation teams promoted by the Secure DevOps approach enables us to deploy features into production quickly and to detect and correct problems when they occur, without disrupting other services. The development, deployment and testing processes are accelerated for updates and can be easily monitored. Additional benefits are improved tooling and system support for collaboration and security-centered development. As a service provider company specialized in data analytics and big data explains:

in our view, we are not only moving security earlier in the development cycle but also ensuring that at operation time the security aspects of the application are being kept, by monitoring anomalies and applying the appropriate countermeasures, either automatically when feasible, or with human intervention.

4.2.4. Secure DevOps is Inherently an Agile Process

Quite a few surveyed companies expect similar benefits from Secure DevOps as from agile methods, including better iteration management and sustainable pace in system development through regular iterations. The companies constrained by heavy regulations are also keen to experiment with Secure DevOps to better understand how to adopt agile methods effectively. Adopting a Secure DevOps approach could boost agile and continuous development in companies ensuring the same level of security.

4.2.5. Secure DevOps Increases the Overall Quality of Services, Products, and Processes

From the perspective of products / services, the surveyed companies expect to produce comprehensive and flexible, constantly evolving services with fused security and obtain significant quality improvements in many measures: functionality, extensibility, defect rates. The product is expected to be scalable in terms of implementing new technologies into the already installed systems, and comply to existing and upcoming standards for CPSs. A service provider company foresees that a Secure DevOps approach can:

support its customers in the stages of their cloud application development process: continuous architecting, development, deployment as well as continuous improvement during the exploitation and operation phase of secured CPS applications.

4.2.6. Secure DevOps Decreases Cost

Reduced cost and time of development, operation and maintenance are also expected, since implementation bugs and architectural flaws will be reduced due to the integrated risk management and security view during the whole CPS lifecycle. A surveyed company underlined that:

a realistic estimate is that both of these efforts can be reduced by 10% as a result of the improved security technology for both development and operations.

4.2.7. Secure DevOps' Effects go Beyond an Individual CPS's Development

A Secure DevOps approach can have greater influence that goes beyond the scope of CPSs products and processes, and produce real business value. The surveyed companies see a great opportunity in a Secure DevOps approach to CPSs to drive price competitiveness through automation, optimized cost structure in a revolutionary way. The improved quality of service (better security and hence stability) at a more competitive cost will enhance the competitive advantages of the companies in the CPS market, and enable a significant increase in the business volume and the range of services offered to the market. As one surveyed company puts it:

Security within the organization is seen as a business enabler. As such we see a driving need to ensure our solutions meet and exceed the needs of the market with security.

The ability to address security effectively, enabled by a Secure DevOps approach, brings cutting-edge competitive advantages to the companies and their customers as well. As a service provider in the healthcare sector responds:

to us, a source of competitiveness is the high level of security shown by our solutions, both at the component level, network level and application level.

One surveyed company, an embedded system manufacturer that oriented its core business in the last ten years in the areas of CPSs and industrial IoT, reports that Secure DevOps has the potential to:

demolish the barriers that characterize today the acceptance of IoT solutions.

A Secure DevOps approach requires a close collaboration among CPS-design experts, software development and operation teams, and security experts during the whole lifecycle. Secure DevOps is:

a security-enhanced DevOps platform with an end-to-end security mindset between different functions inside the company.

This increases employees' ability to work in multidisciplinary teams and, in turn, pushes team members to be creative and innovative. Thus, Secure DevOps can cause a change of internal organizational culture.

4.3. Industry Impacts of Secure DevOps (RQ3)

As we mentioned, implementing Secure DevOps produces impacts that go beyond a company's internal assets. Increase innovation, strengthen market position, ensure competitive advantage and create new business opportunities are the major impacts that motivate the European industry.

Increasing the innovation capacity of companies helps maintain their reputation and ensures their sustainability. For the surveyed consultancy companies, being the forefront of innovation helps consolidate their internal research and development line and their role as experts in the field. More in general, innovation is a means to strengthen the market position and create a competitive advantage for companies operating in the technological sector. Integrating security in DevOps further creates leadership of such companies in a market dominated by the provision and consumption of IoT services and concerns on cyber-security. Companies consider a secure IoT infrastructure capable of reducing barriers that characterize the acceptance of IoT solutions.

Integrating security-by-design in the development of solutions that can be distributed across architectures and locations over the Internet enables the companies to target new types of customers, growing their client base, and be distinctive in the IT market. Safe and stable products or infrastructures provide new market opportunities, increase service portfolio (e.g., security coaching with DevOps) or business sector coverage (e.g., the Smart Home field), as one surveyed company puts it:

enter new business segments or markets where today we have no footprints yet.

Finally, the sole DevOps paradigm opens up a new form of cooperation with customers who, in turn, get a long-lasting competitive edge.

In summary, some of the findings of this work are well-known problems with DevOps and security. The new concepts we gathered from the survey are related to whole life-cycle management, security-by-design, tool-chain integration, and people training and roles. Many companies seem to be struggling with adapting their current processes and development environments for the new security requirements of more complex CPSs.

5. DISCUSSION

CPSs are becoming more and more commonplace. This poses new needs and opportunities for innovation both in product and service solution companies, including consultant companies. However, the complexity of CPSs tends to be increasing, which is a particular challenge considering their stringent security and compliance requirements. While the basic DevOps approach supports the new product development needs of fast innovation and continuous evolution, the domain-specific security constraints and certifications are still a challenge. Thus, the industrial needs and expectations for Secure DevOps have significant managerial as well as research implications.

Based on the answers to our research questions, especially the characteristics of Secure DevOps we derived from them, in this section, we discuss our envisioned approach.

5.1. Enabling Secure DevOps

Overall, based on our survey findings, we can suggest the following aggregated areas for improvement actions in response to industrial needs and to advance the current state of the art in order to successfully apply DevOps for secure, resilient CPSs' development:

- **Understanding of Business and Regulatory Needs:** It is necessary to define the critical requirements and constraints on the technological, process, and organizational improvements that enable secure continuous deployment in CPSs settings, such as safety and security, and regulatory inhibitors and facilitators. These requirements should be derived through a business value-driven analysis of the business needs and use cases of companies, taking into account their specific CPSs domain characteristics and future development trajectories;
- **Security-Enabling/Enabled DevOps Processes:** New or adapted processes to support Secure DevOps in the context of CPSs are needed to perform continuous security deployment (i.e., continuous deployment to address security concerns), and their relationship / seamless integration with already existing (agile) development processes inside companies. These processes cover not only methodological and technical aspects but also the organizational culture of the development, including, for instance, team compositions, roles and responsibilities, and even taking multi-organizational ecosystem development into account (e.g., component vendors and service partners);
- **Architecture and Technologies for Secure DevOps:** Revising existing and introducing new architectures and technologies is necessary to develop CPSs products in a DevOps manner, where security is an integral part of the development process and product throughout the development and deployment cycle. Such technologies and architectures act as a reference for building safe and secure CPSs. In addition, since monitoring of the deployed systems is a key concept of DevOps, also the feedback loop from actual use to the development shall be considered both at conceptual and technological level (e.g., integrated into development platforms) to fit the regulatory aspects of the development;
- **Supporting Tools and Infrastructure:** Concrete tooling and infrastructure (e.g., development platforms) are indispensable to develop, ship, and operate CPSs in a secure manner using DevOps, and enabling the deployment and operation pipelines. Such tooling and infrastructure must support key DevOps concepts such as continuous delivery monitoring of system operations

with end-to-end visibility of security, and enrich them with CPSs concerns such as a plurality of operational environment software and hardware platforms, and certification;

- **People/Organizational Development:** It is not straightforward to make the DevOps approach work fully effectively in industrial software organizations. In CPSs domains, this is further complicated by the many complexities inherent in such software-intensive systems. Moreover, the security requirements must be adhered to at all times and in all related activities. It follows that the Secure DevOps approach should be designed and fabricated into the entire software organization in comprehensive and capability-based ways. Basic DevOps must be augmented with industry-strength systems engineering and management capabilities coupled with organization-wide security awareness. The key competencies and mindsets must be developed and fostered accordingly.

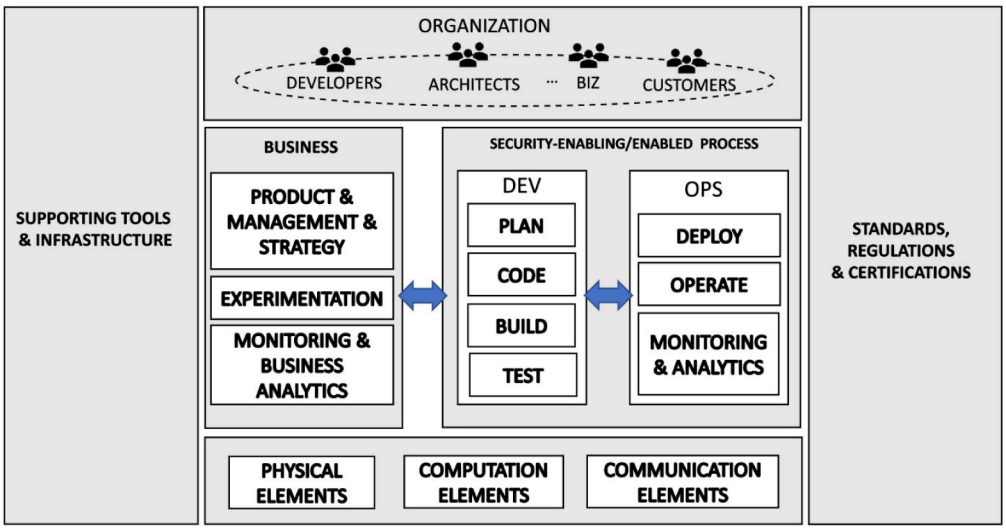
5.2. The Secure DevOps Approach

Figure 3 illustrates the Secure DevOps approach we envisioned based on the findings we discussed in the previous section. It is shown how the above-mentioned main elements work together for secure construction and updating of CPSs. The essence is that Secure DevOps contributes to deliver and maintain compliant and competitive CPSs in operation. In addition, it exhibits how the business demands for fast new product development can be supported. Continuous feedback for both security and functionality is essential. In summary, the Secure DevOps approach would support the following:

- Continuous identification of business/regulatory requirements;
- Continuous monitoring of emerging security threats;
- Coordinating the collaboration between Security and DevOps personnel with other stakeholders.

Arguably, it requires strategic organization design and major developmental efforts to realize all the components in Figure 3 in real industrial companies. Many modern CPSs domains – especially in Industry 4.0 – are currently under rapid technological advancements (e.g., automotive), but at the same time, their security concerns and regulatory requirements become more stringent (e.g., Smart Grids). Consequently, more extensive theoretical principles and methods are needed (e.g., systems

Figure 3. Secure DevOps: Developing, shipping and operating competitive CPSs in a secure manner with DevOps



modelling of heterogeneous cyber and physical components). Modern Industry 4.0 smart factories and manufacturing systems, smart grids, smart vehicles, and smart health environments are complex CPS constellations with multiple connections and accesses. Dependable and secure architectures by design and secure management and governance of operational services and systems must be realized. Our envisioned Secure DevOps approach embraces such research challenges.

A Secure DevOps approach coordinates various elements of CPSs development, including people, organization, process, business, and infrastructure, as seen in Figure 3. These elements are generally described so that they can fit into the different contexts of application. We do not focus on specializing the process for one application domain. Hence, not many relationship links are shown in Figure 3. The framework should be seen as a collection of necessary elements to build a Secure DevOps process for the modern CPS project.

5.3. Threats to Validity

Like any other empirical study, we also faced some validity threats. We were aware that information collected from the survey participants might tend to subjective perception. We had initiatives to reduce the bias as much as possible, i.e. following-up interviews, brainstorming, and several meetings among key participants. Much internal communication in participating organizations occurred to make sure the information truly reflects the actual situations in organizations. Given the fact that participation is a part of a larger research initiative, the participants had nothing to gain by giving false information. Furthermore, focusing on one data source for each case also allows us to inquire further and analyze specific contexts (Dybå, 2013).

Regarding data analysis, we documented and stored all feedback from the participants. The documentation enabled us to track changes, which allowed us to keep track of updated information. This allows replication of the analysis by others. We also made the set of data and the analyzed spreadsheet available to all the research participants for correction if needed.

Regarding external validity, a qualitative survey does not aim at quantitative generalization but characterizing the research topics in their contexts. In this work, our cases are from various industry domains, with diverse company sizes. The findings from our survey shape the perspective for companies active in the CPSs' business. Another potential threat to external validity is that the surveyed companies are all from Europe, even though they have a global presence. The generalizability of the findings to companies in other geographic locations is subject to validation.

6. CONCLUSION

In this paper, we have investigated both conceptually and empirically what secure, competitive CPSs development and operation entail. Based on the industrial survey data, we have identified practitioners' needs for that. Accordingly, we have envisioned and characterized a Secure DevOps approach. We see a lot of promise in the field of high-performing development and delivery of resilient, secure CPSs. However, there is a wide gap in research, calling for more attention in the following research and developmental areas:

1. Holistic, domain-specific deep understanding of what CPSs and their software development needs are;
2. Following that, systematic comprehension of what safety and security entails in them, including specific regulations associated with different CPS domains;
3. Based on such foundations, well-justified suggestions regarding how DevOps would support their secure (software) development.

The key characteristic is that modern CPSs in such use environments as Industry 4.0 are increasingly interconnected software-intensive systems. Hence, for instance, IoT platform providers

could serve multiple CPS business domains and consequently support security features in general, rather than satisfying domain-specific requirements. Therefore, based on our industrial survey, we propose future research and development:

- To improve the capability of industrial ecosystems to enable development, deployment, and delivery of new and innovative cyber-physical products and services;
- To enable the industry to develop secure, safe, and reliable CPSs based on sound design guidelines and toolchains that satisfy regulatory needs, based on the ability to adapt, tailor, and scale processes that facilitate DevOps adoption in critical domains;
- To enable and empower industry by overcoming organizational barriers and challenges that inhibit the effective adoption of DevOps;
- To revise the suggested approach to include domain-specific elements for specific CPS domains such as medical devices, transportation systems or smart grids.

Multidisciplinary development and systematic improvements are needed to achieve these goals, as the needs proposed by standardization and other regulatory authorities exceed any boundaries of technology, processes, and industry domains and practices.

ACKNOWLEDGMENT

This work was supported, in part, by Science Foundation Ireland grant 13/RC/2094; the Norwegian Research Council, grant number 247678 (SoS-Agile); a Contract for research project “Industry 4.0 for Smart*” funded by Systems Srl and the Free University of Bozen/Bolzano; and the European Commission grant number 856602 (Finest Twins).

REFERENCES

Andersson, C., & Runeson, P. (2002). Verification and validation in industry - a qualitative survey on the state of practice. In *Proceedings international symposium on empirical software engineering* (pp. 37–47). doi:10.1109/ISESE.2002.1166923

Ayala, C., Nguyen-Duc, A., Franch, X., H¨ost, M., Conradi, R., Cruzes, D., & Babar, M. A. (2018). System requirements-OSS components: Matching and mismatch resolution practices an empirical study. *Empirical Software Engineering*, *23*(6), 3073–3128. doi:10.1007/s10664-017-9594-1

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2019). Toward the automation of threat modeling and risk assessment in IoT systems. *Internet of Things*, *7*. doi:10.1016/j.iot.2019.100056

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2020). A novel Security-by-Design methodology: Modeling and assessing security by SLAs with a quantitative approach. *Journal of Systems and Software*, 163.

Cawley, O., Wang, X., & Richardson, I. (2010). Lean/Agile Software Development Methodologies in Regulated Environments State of the Art. In P. Abrahamsson & N. Oza (Eds.), *Lean Enterprise Software and Systems* (pp. 31–36). Springer Berlin Heidelberg. doi:10.1007/978-3-642-16416-3_4

Diaz, E., & Muñoz, M. (2020). Strategy for Performing Critical Projects in a Data Center Using DevSecOps Approach and Risk Management. *International Journal of Information Technologies and Systems Approach*, *13*(1), 61–73. doi:10.4018/IJITSA.2020010104

Duc, A. N., Jabangwe, R., Paul, P., & Abrahamsson, P. (2017). Security Challenges in IoT Development: A Software Engineering Perspective. In *Proceedings of the XP2017 Scientific Workshops* (pp. 11:1–11:5). New York, NY: ACM. doi:10.1145/3120459.3120471

Düllmann, T. F., Paule, C., & v. Hoorn, A. (2018). Exploiting DevOps Practices for Dependable and Secure Continuous Delivery Pipelines. *2018 IEEE/ACM 4th International Workshop on Rapid Continuous Software Engineering (RCoSE)*, 27-30.

Dybå, T. (2013). Contextualizing empirical evidence. *IEEE Software*, *30*(1), 81–83. doi:10.1109/MS.2013.4

Farroha, B. S., & Farroha, D. L. (2014). A Framework for Managing Mission Needs, Compliance, and Trust in the DevOps Environment. In *2014 IEEE Military Communications Conference* (pp. 288–293). doi:10.1109/MILCOM.2014.54

Foehr, M., Vollmar, J. C. A., Leitão, P., Karnouskos, S., & Colombo, A. W. (2017). Engineering of next generation cyber-physical automation system architectures. In S. Biffl, A. Lüder, & D. Gerhard (Eds.), *Multi-disciplinary engineering for cyber-physical production systems: Data models and software solutions for handling complex engineering projects* (pp. 185–206). Springer International Publishing. doi:10.1007/978-3-319-56345-9_8

Giaimo, F., Yin, H., Berger, C., & Crnkovic, I. (2016). Continuous experimentation on cyber-physical systems: Challenges and opportunities. In *Proceedings of the scientific workshop proceedings of XP2016* (pp. 14:1–14:2). ACM. doi: 10.1145/2962695.2962709

Henkel, J. (2017). Cyber-Physical Systems Security and Privacy. *IEEE Design & Test*, *34*(4), 4. doi:10.1109/MDAT.2017.2713356

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security - A Survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831. doi:10.1109/JIOT.2017.2703172

Jaatun, M. G., Cruzes, D. S., & Luna, J. (2017). DevOps for Better Software Security in the Cloud (Invited Paper). In *Proceedings of the 12th International Conference on Availability, Reliability and Security* (pp. 69:1–69:6). New York, NY: ACM. doi:10.1145/3098954.3103172

Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. Forum Qualitative Sozialforschung / Forum: Qualitative. *Social Research*, *11*(2).

Khaitan, S. K., & McCalley, J. D. (2015). Design Techniques and Applications of Cyberphysical Systems: A Survey. *IEEE Systems Journal*, *9*(2), 350–365. doi:10.1109/JSYST.2014.2322503

Laukkarinen, T., Kuusinen, K., & Mikkonen, T. (2017). DevOps in Regulated Software Development: Case Medical Devices. In *2017 IEEE/ACM 39th International Conference on Software Engineering: New Ideas and Emerging Technologies Results Track (ICSE-NIER)* (pp. 15–18). IEEE.

Lee, A. (2007). *Computing Foundations and Practice for Cyber-Physical Systems: A Preliminary Report | EECS at UC Berkeley* (Technical Report No. UCB/EECS-2007-72). University of California, Berkeley.

Leppänen, V., Rindell, K., & Hyrynsalmi, S. (2018). Fitting Security into Agile Software Development. *International Journal of Systems and Software Security and Protection*, *9*(1), 47–70. doi:10.4018/IJSSSP.2018010103

Merkow, M. S., & Raghavan, L. (2010). *Secure and resilient software development* (1st ed.). Auerbach Publications. doi:10.1201/EBK1439826966

Mohan, V., & Othmane, L. B. (2016). SecDevOps: Is It a Marketing Buzzword? - Mapping Research on Security in DevOps. *11th International Conference on Availability, Reliability and Security (ARES)*, 542-547. doi:10.1109/ARES.2016.92

Morales, J., Yasar, H., & Volkmann, A. (2018). Weaving Security into DevOps Practices in Highly Regulated Environments. *International Journal of Systems and Software Security and Protection*, *9*(1), 18–46. doi:10.4018/IJSSSP.2018010102

Müller, H. A. (2017). The Rise of Intelligent Cyber-Physical Systems. *Computer*, *50*(12), 7–9. doi:10.1109/MC.2017.4451221

Robson, C. (2011). *Real world research* (3rd ed.). Wiley.

Sharma, K., Bala, S., Bansal, H., & Shrivastava, G. (2017). Introduction to the Special Issue on Secure Solutions for Network in Scalable Computing. Scalable Computing. *Practice and Experience*, *18*(3), iii–iv.

Stirbu, V., & Mikkonen, T. (2018). *Towards agile yet regulatory-compliant development of medical software. In 2018 IEEE international symposium on software reliability engineering workshops*. ISSREW. doi:10.1109/ISSREW.2018.00027

Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the Internet of Things: A Review. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 3, pp. 648–651). doi:10.1109/ICCSEE.2012.373

Taivalsaari, A., & Mikkonen, T. (2017, January). A Roadmap to the Programmable World: Software Challenges in the IoT Era. *IEEE Software*, *34*(1), 72–80. doi:10.1109/MS.2017.26

Törngren, M., & Sellgren, U. (2018). Complexity challenges in development of cyber-physical systems. In M. Lohstroh, P. Derler, & M. Sirjani (Eds.), *Principles of modeling: Essays dedicated to Edward A. Lee on the occasion of his 60th birthday* (pp. 478–503). Springer International Publishing. doi:10.1007/978-3-319-95246-8_27

Tuma, K., Calikli, G., & Scandariato, R. (2018). Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software*, *144*(October), 275–294. doi:10.1016/j.jss.2018.06.073

Virmani, M. (2015). Understanding DevOps bridging the gap from continuous integration to continuous delivery. In *Fifth international conference on the innovative computing technology (INTECH 2015)* (pp. 78–82). doi:10.1109/INTECH.2015.7173368

Yasar, H., & Kontostathis, K. (2016). Where to Integrate Security Practices on DevOps Platform. *International Journal of Secure Software Engineering*, *7*(4), 39–50. doi:10.4018/IJSSE.2016100103

Pekka Abrahamsson (PhD) works as a full professor of information systems and software engineering at the University of Jyväskylä in Finland. He received his PhD on Software Engineering in 2002 from University of Oulu. His research is in the area of emerging software technologies, empirical software engineering, software startups, and the ethics of artificial intelligence. Before his current position, he has served as full professor in University of Helsinki (Finland), Free University of Bolzano (Italy), Norwegian University of Science and Technology (Norway). He also worked at VTT Technical Research Centre of Finland as a research professor of software technologies. He has published broadly in his fields of expertise and received many awards and recognitions. He received the Nokia Foundation Award in 2007, Aminer.org selected him as Top-100 Most Influential Scholar in software engineering in 2016, and he co-authored the best paper of 2018 in Journal of Systems and Software. He is the co-founder of the Software Startup Research Network (SSRN) and a seasoned expert in leading large research projects.

Hadi Ghanbari is a postdoctoral researcher at the Department of Information and Service Management, Aalto University, Finland. Dr. Ghanbari received his Ph.D. in Computer Science from the University of Jyväskylä, Finland (2017) and received M.Sc. in Information Systems from the University of Oulu, Finland (2012). He also holds a B.Eng. in Software Engineering (2005). Ghanbari conducts empirical research in the area of information systems development and digital innovation. During his academic career, he has been involved in several industry-driven R&D projects both as a project manager and a researcher. Prior to his academic career, he has worked in several positions in IT industry for more than eight years.

Martin Gilje Jaatun is a Senior Scientist at SINTEF Digital in Trondheim, Norway. He graduated from the Norwegian Institute of Technology (NTH) in 1992, and received the Dr.Philos degree in critical information infrastructure security from the University of Stavanger in 2015. He is an adjunct professor at the University of Stavanger, and was Editor-in-Chief of the International Journal of Secure Software Engineering (IJSSE). Previous positions include scientist at the Norwegian Defence Research Establishment (FFI), and Senior Lecturer in information security at the Bodø Graduate School of Business. His research interests include software security, security in cloud computing, and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org), vice chair of the IEEE Technical Committee on Cloud Computing (TCCLD), an IEEE Cybersecurity Ambassador, and a Senior Member of the IEEE. Most of his published papers are available here: http://jaatun.no/papers.

Petri Kettunen is a university researcher at the University of Helsinki, Department of Computer Science. His current research interests include digitalization in industries, software futures research, future software development organizations and high-performing software teams, and continuous innovation in software-intensive organizations. Kettunen received his D.Sc. (Tech.) degree from the Helsinki University of Technology (now Aalto University) in 2009.

Tommi Mikkonen is a full professor at University of Helsinki, Department of Computer Science, and acts as the Head of Research at Solita. He has published over 250 peer-reviewed articles of different types and supervised 24 doctoral and over 400 MSc. theses. During his career as a professor, Mikkonen has visited Sun Microsystems (2006-08) Mozilla (2016-17) and Solita Ltd. (2018-19) as a visiting professor, giving him valuable insight to the state-of-practice of this field in the industry. He has been rewarded twice for successful thesis supervision and once for fostering industry-university collaboration.

Anila Mjeda is a full-time researcher in Lero - The Irish Software Research Centre at the University of Limerick. Her work focuses on model-driven engineering with a focus on testing and verification of large and complex software systems. Research interests: model-driven engineering, formal methods, testing, verification, safety-critical systems, automotive software, software engineering education.

Jürgen Münch (PhD) is a Professor of Software Engineering, Entrepreneurship, and Innovation at Reutlingen University, Germany. Furthermore, he is associated with the Faculty of Faculty of Business, Economics and Social Sciences at University of Hohenheim. Prior to this position, he has been the first Finland Distinguished Professor in the field of Software Systems at the University of Helsinki and head of its Software Systems Engineering Research Group. Prof. Münch's research interests include product management, product strategy, product design, startup methods, and measurement. Münch has been a principal investigator of numerous research and industrial development projects. Münch is the method creator of the WHEELS OF VALUE MODEL and has co-invented the GQM+Strategies method for aligning organizations through measurement. Münch has been awarded the Distinguished Professor Award FiDiPro (endowed with €1.900.000) of Tekes, the IFIP TC2 Manfred Paul Award for Excellence in Software Theory and Practice, several best paper awards, the art and technology innovation award sponsored by the Rhineland-Palatinate Lotto Foundation and the community award of the Software Startups Global Research Network (SSRN). He has been chair of several renowned software engineering conferences such as the ACM/IEEE Symposium on Empirical Software Engineering and Measurement (ESEM).

Anh Nguyen-Duc (PhD) is an Associate Professor at the University of South Eastern Norway. He teaches fundamental programming, capstone projects and software engineering. His research interests include Empirical Software Engineering, Cybersecurity, Software Startup, and Internet-of-Thing.

Barbara Russo is full professor in Computer Science at the Free University of Bozen-Bolzano. She holds a PhD in pure mathematics from the university of Trento, Italy. She was visiting researcher at the Max Plan Institute for Mathematics, Bonn, Germany. She published more than 120 articles in pure mathematics and computer science. She is reviewer for the most relevant journals and conference in software engineering. Her research interest is in AI applied to systems engineering.

Xiaofeng Wang is an associate professor at the Computer Science Faculty of Unibz. Her main research areas include software startups, agile and lean software development and innovation, and human factors in software engineering. She is actively publishing in Software Engineering venues, including IEEE Software, Journal of Systems and Software, Empirical Software Engineering, etc. She is also active in serving various Software Engineering conferences and workshops.