

10-9-2023

Software in the Manufacturing Industry: A Review of Security Challenges and Implications

Yannick Landeck
fortiss GmbH, Germany, landeck@fortiss.org

Dian Balta
fortiss GmbH, Germany, balta@fortiss.org

Martin Wimmer
Siemens AG, Germany, martin.r.wimmer@siemens.com

Christian Knierim
Siemens AG, Germany, christian.knierim@siemens.com

Follow this and additional works at: <https://aisel.aisnet.org/wi2023>

Recommended Citation

Landeck, Yannick; Balta, Dian; Wimmer, Martin; and Knierim, Christian, "Software in the Manufacturing Industry: A Review of Security Challenges and Implications" (2023). *Wirtschaftsinformatik 2023 Proceedings*. 40.

<https://aisel.aisnet.org/wi2023/40>

This material is brought to you by the Wirtschaftsinformatik at AIS Electronic Library (AISeL). It has been accepted for inclusion in Wirtschaftsinformatik 2023 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Software in the Manufacturing Industry: A Review of Security Challenges and Implications

Research Paper

Yannick Landeck¹, Dian Balta¹, Martin Wimmer², and Christian Knierim²

¹ fortiss GmbH, Munich, Germany

{landeck, balta}@fortiss.org

² Siemens AG, Munich, Germany

{martin.r.wimmer, christian.knierim}@siemens.com

Abstract. Software defines digital infrastructures in the manufacturing industry, connecting services and computation resources to machines and devices. These infrastructures aim at increased flexibility, scalability, and a wider application portfolio for automated manufacturing processes. At the same time, the complexity of securing software increases dramatically. Threats to confidentiality, integrity, and availability of software can result in critical losses for automated industrial production and impact manufacturing companies. In order to map existing and emerging security challenges, we present the results of a hermeneutic literature review structured along abstraction levels and vertical integration of software. Based on this structure, we derive implications for academia and practice focused on system integrators, developers, and security auditors of digital infrastructures. Thereby, we discuss courses of action mapped to software security black boxes, infrastructure heterogeneity, and the adaptation of security for operational usage.

Keywords: Software Security, Manufacturing, Literature Review.

1 Introduction

As software is transforming the manufacturing industry, production is increasingly defined by digital infrastructures. Out of this transformation emerges an ecosystem that is comprised of software suppliers for manufacturing processes (cf. e.g. Alcácer and Cruz-Machado (2019)) and technological innovations such as infrastructure-as-code (cf. e.g. Rahman et al. (2019)). Due to the heterogeneity of software suppliers, this ecosystem is similar to established Cloud service platforms like Amazon Web Services¹ or Microsoft Azure².

The transformation increases the dependency of the manufacturing industry on software along two key dimensions. On one hand, the **abstraction of software increases** (cf. e.g. Baldini et al. (2017)). For instance, software functionality is not defined in a piece of code or imported as a library any more, but rather consumed as an abstract service. On the other hand, the boundaries of **vertical integration of software** are

¹ <https://aws.amazon.com/>

² <https://azure.microsoft.com/>

blurring (cf. e.g. Boyes et al. (2018)). For instance, software controlling a machine can be managed in the Cloud rather than being installed from a disk or a USB stick.

Although both academia and practice have recognised the increasing dependency of manufacturing on software and its consequences in terms of security, no mapping between the aforementioned key dimensions exists. For instance, extant work investigates Cloud computing security (Tabrizchi and Kuchaki Rafsanjani, 2020) or analyses the applicability of the IEC 62443 standard (Leander et al., 2019). Furthermore, topics of interest are software supply chain risk management issues (cf. NIST (2023)) and the need for a high common level of security in the European Union as constituted in the NIS2 Directive (cf. Negreiro (2023)).

To address this shortcoming, we focus on the research question: **What are security challenges and implications for the manufacturing industry in the light of increased abstraction and vertical integration of software?** The paper presents the results of a hermeneutic literature review on security challenges associated to the two dimensions. We derive implications that these challenges will have on the work of salient stakeholders related to software in manufacturing: system integrators, developers, and security auditors. The analysis dimensions and relevant stakeholders were identified by critically assessing the security challenges during our review process (cf. Section 3). To argue the implications for stakeholders, we propose courses of action towards current and emerging security challenges.

The paper is structured as follows. In Section 2, we describe the background of architectural software patterns, vertical software integration in manufacturing, and software security. In Section 3, we describe the methodology we follow. Section 4 frames software security in manufacturing and gives an overview on related literature studies. In Section 5, we summarise the security challenges found in our literature review. Section 6 discusses the implications that we derive from our findings and presents courses of actions for stakeholders. Finally, Section 7 concludes the paper.

2 Background

2.1 Development of Architectural Software Patterns

Architectural software patterns express a fundamental structural organization schema for software systems (Buschmann et al., 1996). There is a recognisable evolution of software architectures from monolithic applications towards microservices and lately minimal coupling of functional components (Dragoni et al., 2017; Leitner et al., 2019).

Software Monoliths: Dragoni et al. (2017) define a monolith as "a software application whose modules cannot be executed independently". Monoliths are characterised by tight coupling, vertical scaling and strong dependence (Ibrahim et al., 2019). Lewis and Fowler (2014) highlight two problems of evolving monoliths: the difficulty to keep a modular structure and that scaling of a module requires scaling of the entire application.

Service-oriented Architecture: Service-oriented architecture (SOA) is structuring software as services which are centered around representing certain business capabilities (Papazoglou, 2003). SOA services achieve flexibility by decoupling their interfaces from their implementation (Dragoni et al., 2017).

Microservices emerged as an evolution of SOA. They reduce the complexity of applications and focus on the programming of simple services that effectively implement a single functionality (Dragoni et al., 2017). Lewis and Fowler (2014) give a definition of microservices and highlight their characteristics of being organised around business capabilities, characterised by decentralised governance, and designed to evolve.

Minimal Coupling of Functional Components: Function as a Service (FaaS) emerged as an implementation of software architectures that trend towards minimal coupling of functional components (Perez et al., 2019). It separates the writing of application code from the management of its deployment and underlying infrastructures (Bocci et al., 2021). The short-running functions in a FaaS environment are triggered by events, and then executed on-demand in an isolated environment (Leitner et al., 2019).

Development Towards Higher Levels of Software Abstraction: Even prior to the development of FaaS, the shift from monoliths to SOA has introduced new concepts of software abstraction. Thus, systems became more modular and interchangeable (Dragoni et al., 2017). Therefore, monoliths usually represent a **low level**, SOA a **medium level**, and FaaS a **high level** of software abstraction. With increased abstraction, more of the service and function implementation is hidden from other components.

2.2 Vertical Software Integration in Manufacturing

A frequently used model for the hierarchical framing of manufacturing is the **Reference Architectural Model Industrie 4.0 (RAMI 4.0)**. RAMI 4.0 is an abstract three-dimensional reference model capturing the dimensions of system hierarchy levels, information layers, and the lifecycle and value stream (Hankel and Rexroth, 2015). "Vertical integration" of information systems refers to the technological support of organisational units across multiple system hierarchy levels of RAMI 4.0, from products and field devices up to enterprise level and the connected world (Jasperneite et al., 2020). Since software plays an essential role in these systems (Hasselbring, 2000), we present different technological approaches to **vertical software integration** and analyse their impact on security.

Cloud: The National Institute of Standards and Technology (NIST) defines Cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" (Mell and Grance, 2011). These resources (e.g. servers, applications, services) can be rapidly provisioned and released with minimal efforts for management and little service provider interaction (Mell and Grance, 2011).

Edge: Edge computing is a paradigm used to move computation to the edge of the network (Donno et al., 2019). It was introduced to leverage Cloud computing infrastructures and process data closer to its source (Shi et al., 2016). Edge computing also presents benefits regarding data security and privacy, since sensitive information stays inside the network boundaries of a company (Roman et al., 2018).

Fog: Fog computing can arguably be considered as an implementation of Edge computing (Donno et al., 2019). It was introduced as an extension to Cloud computing, e.g. through content delivery networks (Shojafar et al., 2017). It provides computation,

storage and networking services between end devices, Edge computing and Cloud servers (Roman et al., 2018; Satyanarayanan, 2017).

IIoT: The Internet of Things (IoT) comprises the extension of network connectivity and computing capability to devices and sensors (Rose et al., 2015). The Industrial Internet of Things (IIoT) is the use of IoT technologies for the promotion of goals distinctive to industry (Boyes et al., 2018). Academia and practice established several reference architectures (cf. e.g. Lin et al. (2017)) to describe the integration of IIoT devices, with software playing a major role in these systems.

IACS: Industrial Automation and Control Systems (IACS) or Industrial Control Systems (ICS) is a collective term typically used to describe different control systems (Boyes et al., 2018). In a guide to ICS security, the NIST states that, initially, ICS were isolated systems running proprietary protocols and specialised hardware and software (Stouffer et al., 2014). Since ICS have many characteristics that differ from traditional IT systems, vertically integrating software across hierarchy levels in manufacturing (cf. RAMI 4.0) poses challenges to security (Stouffer et al., 2014).

PERA: The Purdue Enterprise Reference Architecture (PERA) (Williams, 1994) is another well-recognised model to frame software in manufacturing environments into hierarchical levels (Chen et al., 2008) and analyse security (cf. e.g. Zografopoulos et al. (2021)). Levels 0 to 2 of PERA comprise IACS. Level 3 describes manufacturing operation systems for site management. Level 4 consists of systems for business operations, e.g. planning and logistics. Finally, level 5 comprises enterprise service management targeting functionalities such as analytics and reporting (Williams, 1994).

2.3 Software Security

Furnell et al. (2021) indicate a growing trend for senior business management to be held answerable for the reliable and secure operation of their information systems. The manufacturing domain is affected by this trend and is required to guarantee security in the context of technological advances that cause changes to IT infrastructures (Chhetri et al., 2018). Security approaches need to identify risks to critical infrastructures before they are victim to attacks (Chhetri et al., 2018). Information system security is commonly measured by the **CIA triad**: confidentiality, integrity, and availability (Samonas and Coss, 2014; Basu et al., 2018). These aspects represent the building blocks for designing secure systems (Zissis and Lekkas, 2012).

Confidentiality, often discussed in the context of privacy, refers to security activities that only grant authorised parties or systems access to protected data (Zissis and Lekkas, 2012). **Integrity** targets the protection of system assets against modifications that harm information structures, sabotage processes, or reduce the value of data (Samonas and Coss, 2014). **Availability** refers to the property of a system being accessible upon demand by an authorised entity and to carry on operations even in atypical situations (Zissis and Lekkas, 2012).

With software serving as the foundation of digital infrastructures, the confidentiality, integrity and availability (CIA) triad frames the view on software security. Moreover, the latter needs to be driven by analysing protective mechanisms, assurance, and emerging challenges (Furnell et al., 2021).

3 Methodology

In this paper, we follow a qualitative and hermeneutic research approach (Klein and Myers, 1999). Based on the methodology of Boell and Cecez-Kecmanovic (2014), we conducted a literature review following the process of two major hermeneutic circles: "*search and acquisition*" and "*analysis and interpretation*". We selected this approach in accordance with Klein and Myers (1999), since it suits the nature and context of our research in terms of depth, breadth and heterogeneity of research disciplines involved. We decided against a systematic review (Kitchenham and Charters, 2007), since the definition of a comprehensive research question was not feasible at the beginning of our research and the analysis dimensions had to be identified first.

We followed the initial idea of analysing the security challenges of software in manufacturing. Consequently, we entered the "**search and acquisition**" circle to select, acquire, and read literature from the multi-dimensional field of software security (Boell and Cecez-Kecmanovic, 2014). We gathered initial input by combining the keywords "security" and "security challenges" with terminology identified in our problem analysis (e.g. Cloud, IIoT, SOA) in Google Scholar. As recommended by Webster and Watson (2002), we started with highly cited papers of leading journals (e.g. Combe et al. (2016); Marin et al. (2022)) and pursued backward and forward search. By this, we identified central terms and main authors of the research field and refined our approach to searching (Boell and Cecez-Kecmanovic, 2014).

Next, we entered the "**analysis and interpretation**" circle of the hermeneutic approach. By this, we accumulated knowledge and experience that was used as a starting point for additional "search and acquisition" iterations. As suggested by Boell and Cecez-Kecmanovic (2014), there was not a clear timely separation between the two circles. We rather followed an iterative approach towards reaching a point of saturation. After seven iterations, we reached a point of saturation indicated by diminishing novelty (Boell and Cecez-Kecmanovic, 2014) regarding the challenges for software security in manufacturing.

The second circle involved a deeper interaction with extant work. It involves the following iterative steps: **(1) reading; (2) mapping and classifying; (3) critical assessment; (4) argument development; (5) research problem/questions; and (6) searching** (Boell and Cecez-Kecmanovic, 2014). In total, we read (1) and reviewed 134 publications published between 2005 and 2023. We mapped and classified (2) each publication by identifying major concepts, conceptual frameworks, and historical developments (cf. Boell and Cecez-Kecmanovic (2014)) of software security in manufacturing. For instance, the analysis of Shafiei et al. (2021) motivated us to include the concept of Function as a Service (FaaS) in our next search iteration, since it is crucial for current developments of software architectures.

Next, by critically assessing (3) the security challenges addressed by each publication, we identified the two dimensions of our analysis: abstraction levels and vertical integration of software. Furthermore, we identified a research gap in the lack of intersection coverage in literature when analysing both dimensions and the concept of security (cf. Section 4). Thus, we gained additional knowledge on the research field and applied it to subsequent search iterations. Based on the assessment of literature, we developed

arguments (4) on how to address the discovered gap. We gathered security challenges for software in manufacturing and pursued an argumentative-deductive analysis (Wilde and Hess, 2007) to derive implications for system integrators, developers, and security auditors. Similar to the analysis dimensions, the relevance of these stakeholders was also identified during the critical assessment of literature.

These implications shaped the research problem/question (5) of our review. In particular, we analysed courses of action for each of the stakeholders addressing software security black boxes, infrastructure heterogeneity, and the adaptation of security for operational usage (as described in Section 6). Similar to the preceding steps of the hermeneutic circle, newly generated knowledge and experience influenced the subsequent "*search and acquisition*" (6) circle.

4 Framing Software Security in Manufacturing

4.1 Literature Coverage Along the Two Analysis Dimensions

Figure 1 sketches the coverage in literature for software security in manufacturing. First, it aligns technological approaches to vertical software integration with levels of the PERA model. Our analysis showed that the distinction between operational technology (OT) and information technology (IT) is blurring. For instance, the Industrial Internet of Things (IIoT) is a characteristic concept that is merging the two technologies (Boyes et al., 2018). Nevertheless, the IIoT reflects software systems which are no longer dedicated to one level of the PERA model, but can be vertically integrated from the field level (level 0) up to the enterprise services level (level 5). Second, Figure 1 presents the intersection coverage in literature regarding security of software abstraction and vertical integration. In this representation, we aggregate software security literature of the PERA levels 3, 4, and 5 since the concepts of Edge and Fog computing complemented by Cloud computing cause software to be vertically integrated already (Donno et al., 2019). A distinct view on security of the individual levels and their coverage in literature is subject of future work, but not in the scope of our research.

Our analysis shows that the security of software monoliths is well discussed since we found an extensive coverage in literature (84 publications) addressing either the challenges of monoliths in particular or software security in general, which we assigned to a low abstraction level. For instance, software integration in manufacturing usually requires security to focus more on integrity and availability than on confidentiality. The latter being important on higher integration levels (Tuptuk and Hailes, 2018).

SOA (20 publications) is well-established for levels 4 and 5 (Dragoni et al., 2017) and is increasingly integrated on level 3 as well (cf. e.g. Hoday et al. (2019)). We found an extensive coverage in literature regarding security of SOA on these levels. On the contrary, SOA is usually not found on the levels 0-2 (Komoda, 2006) which is reflected by the identified literature only somewhat covering the topic of security.

FaaS (30 publications) causes software to be even more vertically integrated along all levels (Leitner et al., 2019). Consequently, FaaS shifts into the focus of research on the levels 3-5 (Eismann et al., 2021). However, the literature we identified only somewhat covered FaaS security. Thus, our analysis shows that the investigation of security for

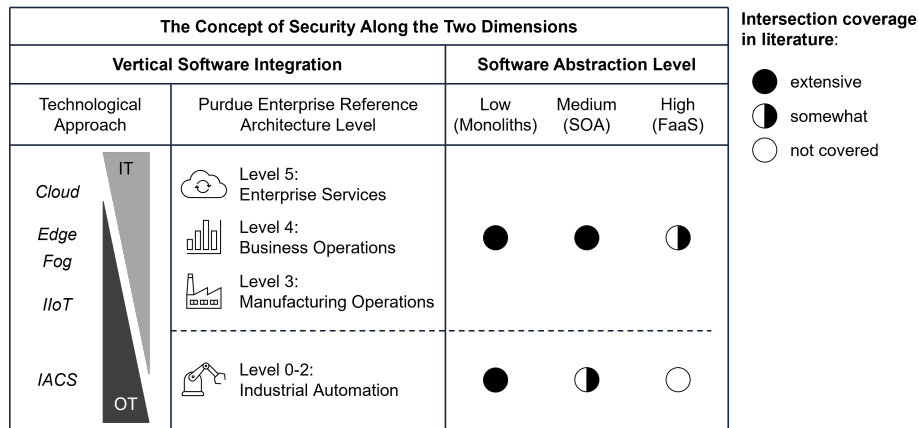


Figure 1. A sketch of literature coverage on the concept of security for software in manufacturing

FaaS implementations is extendable. As for FaaS security on levels 0-2, the identified literature did not cover the intersection of the two dimensions, possibly caused by FaaS considered to not fit the uses cases on lower levels. Additionally, work on FaaS security is often focusing on confidentiality (cf. e.g. Bocci et al. (2022)), which is often secondary for manufacturing compared to integrity and availability (Tupa et al., 2017).

In summary, there is a lack of coverage in literature on security when considering the intersection of higher abstraction levels and increased vertical integration of software. We address this gap by reviewing security challenges for software in manufacturing and derive implications for stakeholders in the industry.

4.2 Related Work

There are several literature reviews on the security of IoT. For instance, Kouicem et al. (2018) conduct a top-down survey and propose a taxonomy of security solutions in IoT. Aly et al. (2019) present guidelines to IoT security issues and describe threats, challenges, solutions, and countermeasures proposed in literature. Tange et al. (2020) conduct a systematic survey of IoT security and present a range of security requirements and discuss Fog computing opportunities. Although these reviews highlight several security challenges addressed in this paper, they are missing a manufacturing perspective and stakeholder-dependent implications. Furthermore, they are not reviewing developments towards higher levels of software abstraction.

Literature reviews on (smart) manufacturing security discuss cyber-physical security efforts (Elhabashy et al., 2019) or strategies, methodologies, and techniques to mitigate attacks (Junior et al., 2021). Bahrami and Rouzbahani (2021) conduct a bibliometric analysis on cybersecurity of smart manufacturing execution systems and present an empiric analysis. These reviews put emphasis on manufacturing systems, but lack in the analysis of software integration approaches and developments towards FaaS. In this paper, we are aiming to fill this gap by analysing literature from the perspective of both analysis dimensions.

5 Findings: Security Challenges for Software in Manufacturing

5.1 Security Challenges Related to the Software Abstraction Level

Below, we will present the results of our literature review on security challenges in terms of confidentiality, integrity, and availability regarding the software abstraction level, summarised in Table 1.

Table 1. Summary of derived security challenges related to software abstraction levels

Software Abstraction Level	Summarised Security Challenges	Exemplary Sources
Low (Monoliths)	Delayed integration of security patches hampering CIA triad	Ahmadvand and Ibrahim (2016); Sun et al. (2015); Fritzscht et al. (2019)
	Preserving CIA triad for highly dependent systems	Merkel (2014); Dragoni et al. (2017); Sun et al. (2015)
	Hampered availability due to difficult maintenance	Villamizar et al. (2015); Fritzscht et al. (2019); Sun et al. (2015)
Medium (SOA)	Network vulnerabilities can compromise CIA triad	Yu et al. (2019); Combe et al. (2016); Makris et al. (2022)
	Application segregation and isolation to preserve CIA triad	Caprolu et al. (2019); Varghese et al. (2016); Yu et al. (2019)
	Evaluating integrity of third-party components	Takabi et al. (2010); Enck and Williams (2022); Ibrahim et al. (2019)
High (FaaS)	Large attack surfaces hampering integrity of functions	Marin et al. (2022); Schleier-Smith et al. (2021); Candel et al. (2023)
	Confidentiality and availability of platform orchestration	Li et al. (2021); Wen et al. (2022); Mondal et al. (2022)
	Unknown sources for event triggers hampering integrity	Marin et al. (2022); Shafei et al. (2021); O’Meara and Lennon (2020)

Security Challenges of Monoliths: Monoliths struggle with limited scalability due to their architectural constraints (Fritzscht et al., 2019). Delayed release cycles (Ahmadvand and Ibrahim, 2016) can prolong the integration of security patches and thus hamper the CIA triad. Furthermore, monolithic systems suffer from dependencies (Merkel, 2014), hampering the adaptation of security practices and the CIA triad (Sun et al., 2015). The rigid structure of monoliths causes their deployment and maintenance to be complex (Ahmadvand and Ibrahim, 2016). Every change made requires a rebuild of the entire system, hampering availability (Villamizar et al., 2015).

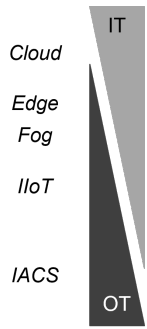
Security Challenges of SOA: SOA is decoupling systems and thus introducing security concerns to the CIA triad caused by vulnerabilities of networks and communications (O’Brien et al., 2005; Subashini and Kavitha, 2011). To secure microservices and preserve all aspects of the CIA triad, researchers have highlighted the importance of achieving application segregation and isolation (Caprolu et al., 2019; Yu et al., 2019; Ibrahim et al., 2019). Managing the security of containers, which are commonly used for microservice deployment, is a prominent challenge in research and practice (Combe et al., 2016; Sultan et al., 2019; Bui, 2015). Furthermore, Enck and Williams (2022) and others highlight the challenge of evaluating the integrity of third-party components and the software supply chain (Takabi et al., 2010; Hashizume et al., 2013).

Security Challenges of FaaS: FaaS exposes larger attack surfaces than regular SOA, hampering the integrity of functions (Schleier-Smith et al., 2021). Research points out the challenge of guaranteeing confidentiality and availability regarding FaaS deployment platforms and their orchestration (Wen et al., 2022; Mondal et al., 2022). Securing those platforms poses a challenge (Candel et al., 2023) since the statelessness of functions hinders policy enforcement (Li et al., 2021). O’Meara and Lennon (2020) highlight the danger of execution flow manipulation that harms integrity, also reflecting the challenge of handling unknown sources for event triggers (Marin et al., 2022; Shafiei et al., 2021).

5.2 Security Challenges Related to Vertical Software Integration

In the following, we will present the results of our review on security in terms of confidentiality, integrity, and availability of vertical software integration, summarised in Table 2.

Table 2. Summary of derived security challenges related to vertical software integration

Vertical Software Integration	Summarised Security Challenges	Exemplary Sources
 Cloud Edge Fog IIoT IACS	Data confidentiality of multi-tenant applications	Zissis and Lekkas (2012); Hashizume et al. (2013); Behl and Behl (2012)
	Confidentiality and availability of obscure platform orchestration	Jegan et al. (2020); Wen et al. (2021); Jonas et al. (2019)
	Preserving CIA triad with limited resources of devices	Zeyu et al. (2020); Xiao et al. (2019); Roman et al. (2018)
	Mitigating cyber and physical threats to preserve integrity	Yaacoub et al. (2020); Makris et al. (2022); Ibrahim et al. (2019)
	Ensuring availability, reliability and resilience of critical systems	Wells et al. (2014); Ashibani and Mahmoud (2017); Yaacoub et al. (2020)
	Protecting hardware and networks in order to preserve CIA triad	Wen et al. (2021); Jegan et al. (2020); Ly and Jin (2016)
	Achieving availability of connections to legacy systems	Krotofil and Gollmann (2013); Ly and Jin (2016); Humayed et al. (2017)

Preserving confidentiality for multi-tenant applications is a frequently mentioned security challenge in Cloud computing (Almorsy et al., 2016; Hashizume et al., 2013; Takabi et al., 2010). Furthermore, it is challenging to evaluate the obscurity of Cloud platform orchestration and management regarding confidentiality and availability (Marin et al., 2022; Jegan et al., 2020; Jonas et al., 2019).

Edge, Fog, and IIoT systems are characterised by a high heterogeneity of devices and networks (Roman et al., 2018; Bhat et al., 2020; Xiao et al., 2019). These devices often have limited computational resources which makes security mechanisms like policy enforcement, authentication, and authorisation a challenge (Sicari et al., 2015; Shafiei et al., 2021; Zeyu et al., 2020). This hampers all aspects of the CIA triad. Vulnerabilities of devices and endpoints pose cyber and physical threats to systems that hamper integrity (Kim et al., 2018; Ashibani and Mahmoud, 2017; Yaacoub et al., 2020). Additionally, Jegan et al. (2020) address the urgency of preventing attacks from new attack vectors that get exposed by vertical software integration.

Due to their criticality, IACS require high availability, reliability and resilience (Wells et al., 2014; Yaacoub et al., 2020). IACS pose the challenge of efficiently protecting hardware, function endpoints, and interfaces (Wen et al., 2021; Ly and Jin, 2016) to preserve all aspects of the CIA triad in an increasingly connected environment (Ashibani and Mahmoud, 2017; Chhetri et al., 2017). Availability of legacy systems, which are generally difficult to maintain and evolve, has to be preserved (Krotofil and Gollmann, 2013; Humayed et al., 2017).

6 Discussion: Implications for Stakeholders in Manufacturing

The results of our literature review highlight the challenges to software security in manufacturing from two perspectives: software abstraction levels and vertical software integration. Moreover, our results highlight the temporal perspective of software security. Short term challenges are faced in practice and handled in research (e.g. software monoliths for OT are existing for decades) (Tuptuk and Hailes, 2018; Stouffer et al., 2014). On the contrary, studies of emerging, long-term challenges are still in their infancy (e.g. FaaS has yet to impact OT) (Bocci et al., 2021; Li et al., 2021).

We argue that the basis for tackling security challenges has to be set in order to address long-term goals of securing software for manufacturing (cf. Table 3). Due to the characteristics of the gathered security challenges in Section 5, we group the derived security challenges along three dimensions: software security black boxes, heterogeneity of devices and networks, adaptation of security approaches for OT.

Table 3. Courses of action for stakeholders regarding each dimension of security challenges

	Software Security Black Boxes	Heterogeneity of Devices and Networks	Adaptation of Security Approaches for OT
System Integrator	Make security measurable at the deepest possible system level in order to evaluate black boxes	Define system boundaries and describe the required/allowed device interactions	Analyse and formulate security requirements of OT environments
Developer	Be able to provide as much evidence on software security as possible	Make software adaptable to dynamic security environments	Design software that adapts to OT security requirements
Security Auditor	Define a language to communicate and assess security of software	Target the automation of assurance assessments regarding software security	Make security requirements of integration environments comparable

Additionally, we map the implications to three salient stakeholders. **System integrators** have domain-specific knowledge of manufacturing facilities and are also responsible for the task of software integration. **Developers** refer to software developers that define vertical software integration by designing applications for multiple PERA levels. **Security auditors** are third-party stakeholders that are associated with the task of assessing and evaluating software security in systems. Their role is increasingly established to provide assurance of system security (Rushby and Bloomfield, 2022), e.g. to assure compliance to industrial security standards (Leander et al., 2019).

6.1 Software Security Black Boxes

The obscure security of software, e.g. in the context of FaaS, can be seen as "software security black boxes", since system integrators are not able to evaluate software security (Li et al., 2021). Therefore, they are inclined to make software security measurable at the deepest possible level. They are inclined to define thresholds for security compliance which the black boxes can be tested against (Wen et al., 2022). Halabi and Bellaiche (2017) propose an approach to making Cloud service provider security quantifiable. Its applicability in manufacturing is subject to future research.

Developers face the challenge to prove secure development and suitable software security to make themselves trustworthy. They must be able to provide as much evidence on security of their product as possible without reducing its value (Enck and Williams, 2022). The software bill of materials (SBOM) is a promising approach to providing application metadata but covers only very specific aspects of security and lacks in terms of performance and adaptability (Xia et al., 2023).

Finally, the obscurity of software security makes it difficult for auditors to assess a systems' compliance to security requirements. A security auditor needs to pursue activities in order to define a policy language for communication and assessment of software security (Li et al., 2021). The three-dimensional model for software security evaluation proposed by Han et al. (2014) can serve as a first step in this direction.

6.2 Heterogeneity of Devices and Networks

The heterogeneity of devices and networks, e.g. in the Industrial Internet of Things (IIoT), is introducing several security challenges. System integrators are required to define physical and logical boundaries of systems and describe the required/allowed software interactions (Ashibani and Mahmoud, 2017). Following this thought, Giarretta et al. (2019) propose Security-by-Contract and Fog computing to secure IoT systems.

For developers, we believe that engineering activities have to put emphasis on making software adaptable to dynamic security environments (Kim et al., 2018). Neureiter et al. (2016) discuss the topic of domain-specific security-by-design using a model based approach, which could serve as one way to guide developers.

Finally, security auditors need to target the continuous assurance of software security, e.g. by following the concept suggested by Rushby and Bloomfield (2022). We believe that the challenge of heterogeneity cannot be dealt with by one stakeholder, but has to be approached jointly across the manufacturing industry.

6.3 Adaptation of Security Approaches for OT

Security demands in manufacturing require the adaptation of security approaches when targeting vertical software integration. System integrators are required to specifically analyse and formulate the security requirements of their domain (Krotofil and Gollmann, 2013). Giorgini et al. (2005) propose a combination of ownership, permission, and delegation to model security requirements. This could be a starting point for investigations in the manufacturing domain.

Correspondingly, developers need to adapt software to security requirements of lower vertical integration levels, e.g. a higher focus on integrity and availability (Pennekamp et al., 2019). We highlight the evaluation of software supply chain security since integrated vulnerabilities can harm aspects of the CIA triad (Enck and Williams, 2022).

Finally, activities of security auditors have to put their focus on making software security requirements of different integration environments comparable (Wang et al., 2010). A formal modelling approach regarding domain-specific security requirements can set the direction of further research (Giorgini et al., 2005).

7 Conclusion

This paper presents the results of a hermeneutic literature review of security challenges for software in manufacturing.

We pursue an interpretative approach to the review of literature. As a basis for our analysis, we studied publications from different disciplines with focus on security of software in manufacturing. We interpreted the results along two derived dimensions: increased software abstraction and vertical integration of software. Our interpretation shows that there is a clear lack of research on FaaS for OT. Moreover, it shows that research on security regarding SOA for OT as well as FaaS for IT is still developing.

In a consequent hermeneutic cycle of analysis and interpretation, we derived three dimensions of security challenges (software security black boxes, heterogeneity of devices and networks, adaptation of security approaches for OT) and mapped them to three salient stakeholders (system integrators, developers, and security auditors). Moreover, we interpreted potential courses of action for these stakeholders and mapped them to the challenges' dimensions.

Although we followed the principles of interpretation (Klein and Myers, 1999) and hermeneutic review of literature (Boell and Cecez-Kecmanovic, 2014), we acknowledge that our research has a number of limitations and presents perspectives for future research endeavors. First, the scope of our literature review is broad which implies that we might not have achieved the level of detail necessary for tackling particular and detailed security issues and threats in practice. This leaves room for future work to narrow down the latter and analyse as well as prescribe concrete actions. For instance, concrete protection and assurance mechanisms (Furnell et al., 2021) for the emerging challenges could be studied. Second, our research provides projections of security challenges that are yet to be supported by empirical evidence in practice. This is the case, since the nature of security implies multiple managerial and technological perspectives (cf. Furnell et al. (2021)). Our research covers both intensively studied intersections (e.g. security of monoliths for IT) as well as emerging intersections (e.g. security of FaaS in OT). This should be of value for researchers towards building concrete hypothesis for empirical studies as well designing artefacts for constructivistic studies.

We believe that our results are beneficial for both academia and practice. We encourage future research to build on our findings and the described limitations of our study. Practitioners can apply our results to guide stakeholders towards the definition of a mid-to long-term security strategy and particular courses of action.

References

- Ahmadvand, M. and Ibrahim, A. (2016), Requirements Reconciliation for Scalable and Secure Microservice (De)composition, in '2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)', IEEE, Beijing, China, pp. 68–73.
- Alcácer, V. and Cruz-Machado, V. (2019), 'Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems', *Engineering Science and Technology, an International Journal* **22**(3), 899–919.
- Almorsy, M., Grundy, J. and Müller, I. (2016), 'An analysis of the cloud computing security problem', *arXiv preprint arXiv:1609.01107*.
- Aly, M., Khomh, F., Haoues, M., Quintero, A. and Yacout, S. (2019), 'Enforcing security in Internet of Things frameworks: A Systematic Literature Review', *Internet of Things* **6**, 100050.
- Ashibani, Y. and Mahmoud, Q. H. (2017), 'Cyber physical systems security: Analysis, challenges and solutions', *Computers & Security* **68**, 81–97.
- Bahrami, A. H. and Rouzbahani, H. M. (2021), 'Cyber security of smart manufacturing execution systems: A bibliometric analysis', *AI-Enabled Threat Detection and Security Analysis for Industrial IoT* pp. 105–119.
- Baldini, I., Castro, P., Chang, K., Cheng, P., Fink, S., Ishakian, V., Mitchell, N., Muthusamy, V., Rabbah, R. and Slominski, A. (2017), 'Serverless computing: Current trends and open problems', *Research advances in cloud computing* pp. 1–20.
- Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S. and Sarkar, P. (2018), Cloud computing security challenges & solutions-A survey, in '2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)', IEEE, Las Vegas, NV, pp. 347–356.
- Behl, A. and Behl, K. (2012), An analysis of cloud computing security issues, in '2012 World Congress on Information and Communication Technologies', IEEE, Trivandrum, India, pp. 109–114.
- Bhat, S. A., Sofi, I. B. and Chi, C.-Y. (2020), 'Edge Computing and Its Convergence With Blockchain in 5G and Beyond: Security, Challenges, and Opportunities', *IEEE Access* **8**, 205340–205373.
- Bocci, A., Forti, S., Ferrari, G.-L. and Brogi, A. (2021), 'Secure FaaS orchestration in the fog: How far are we?', *Computing* **103**(5), 1025–1056.
- Bocci, A., Forti, S., Ferrari, G.-L. and Brogi, A. (2022), Type, pad, and place: Avoiding data leaks in Cloud-IoT FaaS orchestrations, in '2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid)', IEEE, Taormina, Italy, pp. 798–805.
- Boell, S. K. and Cecez-Kecmanovic, D. (2014), 'A Hermeneutic Approach for Conducting Literature Reviews and Literature Searches', *Communications of the Association for Information Systems* **34**.
- Boyes, H., Hallaq, B., Cunningham, J. and Watson, T. (2018), 'The industrial internet of things (IIoT): An analysis framework', *Computers in Industry* **101**, 1–12.
- Bui, T. (2015), 'Analysis of Docker Security'.

- Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P. and Stal, M. (1996), *Software Patterns*, Wiley: Eaglewood Cliffs, NJ, USA.
- Candel, J. M. O., Elouali, A., Gimeno, F. J. M. and Mora, H. (2023), Cloud vs Serverless Computing: A Security Point of View, in 'International Conference on Ubiquitous Computing and Ambient Intelligence', Springer, pp. 1098–1109.
- Caprolu, M., Di Pietro, R., Lombardi, F. and Raponi, S. (2019), Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues, in '2019 IEEE International Conference on Edge Computing (EDGE)', IEEE, Milan, Italy, pp. 116–123.
- Chen, D., Doumeingts, G. and Vernadat, F. (2008), 'Architectures for enterprise integration and interoperability: Past, present and future', *Computers in Industry* **59**(7), 647–659.
- Chhetri, S. R., Faezi, S., Rashid, N. and Al Faruque, M. A. (2018), 'Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0', *Journal of Hardware and Systems Security* **2**(1), 51–68.
- Chhetri, S. R., Rashid, N., Faezi, S. and Al Faruque, M. A. (2017), Security trends and advances in manufacturing systems in the era of industry 4.0, in '2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)', IEEE, pp. 1039–1046.
- Combe, T., Martin, A. and Di Pietro, R. (2016), 'To Docker or Not to Docker: A Security Perspective', *IEEE Cloud Computing* **3**(5), 54–62.
- Donno, M. D., Tange, K. and Dragoni, N. (2019), 'Foundations and Evolution of Modern Computing Paradigms: Cloud, IoT, Edge, and Fog', **7**, 13.
- Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R. and Safina, L. (2017), 'Microservices: Yesterday, today, and tomorrow', *Present and ulterior software engineering* pp. 195–216.
- Eismann, S., Scheuner, J., van Eyk, E., Schwinger, M., Grohmann, J., Abad, C. L. and Iosup, A. (2021), 'Serverless Applications: Why, When, and How?', *IEEE Software* **38**(1), 32–39.
- Elhabashy, A. E., Wells, L. J. and Camelio, J. A. (2019), 'Cyber-Physical Security Research Efforts in Manufacturing – A Literature Review', *Procedia Manufacturing* **34**, 921–931.
- Enck, W. and Williams, L. (2022), 'Top Five Challenges in Software Supply Chain Security: Observations From 30 Industry and Government Organizations', *IEEE Security & Privacy* **20**(2), 96–100.
- Fritzsch, J., Bogner, J., Zimmermann, A. and Wagner, S. (2019), From Monolith to Microservices: A Classification of Refactoring Approaches, in J.-M. Bruel, M. Mazzara and B. Meyer, eds, 'Software Engineering Aspects of Continuous Development and New Paradigms of Software Production and Deployment', Vol. 11350, Springer International Publishing, Cham, pp. 128–141.
- Furnell, S., Haskell-Dowland, P., Agrawal, M., Baskerville, R., Basu, A., Bishop, M., Cuellar, J., Foresti, S., Fletcher, L. and Gal-Oz, N. (2021), Information security and privacy—challenges and outlook, in 'Advancing Research in Information and Communication Technology', Springer, pp. 383–401.
- Giaretta, A., Dragoni, N. and Massacci, F. (2019), Protecting the Internet of Things with Security-by-Contract and Fog Computing, in '2019 IEEE 5th World Forum on Internet of Things (WF-IoT)', IEEE, Limerick, Ireland, pp. 1–6.

- Giorgini, P., Massacci, F., Mylopoulos, J. and Zannone, N. (2005), Modeling security requirements through ownership, permission and delegation, in '13th IEEE International Conference on Requirements Engineering (RE'05)', IEEE, Paris, France, pp. 167–176.
- Halabi, T. and Bellaïche, M. (2017), 'Towards quantification and evaluation of security of Cloud Service Providers', *Journal of Information Security and Applications* **33**, 55–65.
- Han, Z., Li, X., Feng, R., Hu, J., Xu, G. and Feng, Z. (2014), A Three-Dimensional Model for Software Security Evaluation, in '2014 Theoretical Aspects of Software Engineering Conference', IEEE, Changsha, pp. 34–41.
- Hankel, M. and Rexroth, B. (2015), 'The reference architectural model industrie 4.0 (rami 4.0)', *Zvei* **2**(2), 4–9.
- Hashizume, K., Rosado, D. G., Fernández-Medina, E. and Fernandez, E. B. (2013), 'An analysis of security issues for cloud computing', *Journal of Internet Services and Applications* **4**(1), 5.
- Hasselbring, W. (2000), 'Information system integration', *Communications of the ACM* **43**(6), 32–38.
- Homay, A., Zoitl, A., de Sousa, M. and Wollschlaeger, M. (2019), A Survey: Microservices Architecture in Advanced Manufacturing Systems, in '2019 IEEE 17th International Conference on Industrial Informatics (INDIN)', IEEE, Helsinki, Finland, pp. 1165–1168.
- Humayed, A., Lin, J., Li, F. and Luo, B. (2017), 'Cyber-Physical Systems Security—A Survey', *IEEE Internet of Things Journal* **4**(6), 1802–1831.
- Ibrahim, A., Bozhinoski, S. and Pretschner, A. (2019), Attack graph generation for microservice architecture, in 'Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing', ACM, Limassol Cyprus, pp. 1235–1242.
- Jasperneite, J., Sauter, T. and Wollschlaeger, M. (2020), 'Why We Need Automation Models: Handling Complexity in Industry 4.0 and the Internet of Things', *IEEE Industrial Electronics Magazine* **14**(1), 29–40.
- Jegan, D. S., Wang, L., Bhagat, S., Ristenpart, T. and Swift, M. (2020), 'Guarding Serverless Applications with SecLambda'.
- Jonas, E., Schleier-Smith, J., Sreekanti, V., Tsai, C.-C., Khandelwal, A., Pu, Q., Shankar, V., Carreira, J., Krauth, K., Yadwadkar, N., Gonzalez, J. E., Popa, R. A., Stoica, I. and Patterson, D. A. (2019), 'Cloud Programming Simplified: A Berkeley View on Serverless Computing'.
- Junior, A. A. D. S., Pio, J. L. D. S., Fonseca, J. C., De Oliveira, M. A., Valadares, O. C. D. P. and Da Silva, P. H. S. (2021), 'The State of Cybersecurity in Smart Manufacturing Systems: A Systematic Review', *European Journal of Business and Management Research* **6**(6), 188–194.
- Kim, N. Y., Rathore, S., Ryu, J. H., Park, J. H. and Park, J. H. (2018), 'A Survey on Cyber Physical System Security for IoT: Issues, Challenges, Threats, Solutions', *Journal of Information Processing Systems* **14**(6), 1361–1384.
- Kitchenham, B. and Charters, S. (2007), 'Guidelines for performing systematic literature reviews in software engineering EBSE Technical Report EBSE-2007-01', *Keele, Staffs, and Durham, UK*.
- Klein, H. K. and Myers, M. D. (1999), 'A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems', *MIS Quarterly* **23**(1), 67.

- Komoda, N. (2006), Service Oriented Architecture (SOA) in Industrial Systems, in '2006 IEEE International Conference on Industrial Informatics', IEEE, Singapore, pp. 1–5.
- Kouicem, D. E., Bouabdallah, A. and Lakhlef, H. (2018), 'Internet of things security: A top-down survey', *Computer Networks* **141**, 199–221.
- Krotofil, M. and Gollmann, D. (2013), Industrial control systems security: What is happening?, in '2013 11th IEEE International Conference on Industrial Informatics (INDIN)', IEEE, Bochum, Germany, pp. 664–669.
- Leander, B., Čaušević, A. and Hansson, H. (2019), Applicability of the IEC 62443 standard in Industry 4.0 / IIoT, in 'Proceedings of the 14th International Conference on Availability, Reliability and Security', ACM, Canterbury CA United Kingdom, pp. 1–8.
- Leitner, P., Wittern, E., Spillner, J. and Hummer, W. (2019), 'A mixed-method empirical study of Function-as-a-Service software development in industrial practice', *Journal of Systems and Software* **149**, 340–359.
- Lewis, J. and Fowler, M. (2014), 'Microservices: A definition of this new architectural term', *MartinFowler.com* **25**, 14–26.
- Li, X., Leng, X. and Chen, Y. (2021), 'Securing Serverless Computing: Challenges, Solutions, and Opportunities'.
- Lin, S.-W., Miller, B., Durand, J., Bleakley, G., Chigani, A., Martin, R., Murphy, B. and Crawford, M. (2017), 'The industrial internet of things volume G1: Reference architecture', *Industrial Internet Consortium* **10**.
- Ly, K. and Jin, Y. (2016), Security Challenges in CPS and IoT: From End-Node to the System, in '2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)', IEEE, Pittsburgh, PA, USA, pp. 63–68.
- Makris, A., Tserpes, K. and Varvarigou, T. (2022), 'Transition from monolithic to microservice-based applications. Challenges from the developer perspective', *Open Research Europe* **2**, 24.
- Marin, E., Perino, D. and Di Pietro, R. (2022), 'Serverless computing: A security perspective', *Journal of Cloud Computing* **11**(1), 69.
- Mell, P. and Grance, T. (2011), 'The NIST definition of cloud computing'.
- Merkel, D. (2014), 'Docker: Lightweight linux containers for consistent development and deployment', *Linux j* **239**(2), 2.
- Mondal, S. K., Pan, R., Kabir, H. M. D., Tian, T. and Dai, H.-N. (2022), 'Kubernetes in IT administration and serverless computing: An empirical study and research challenges', *The Journal of Supercomputing* **78**(2), 2937–2987.
- Negreiro, M. (2023), 'The NIS2 Directive - A high common level of cybersecurity in the EU', *EPRS | European Parliamentary Research Service*.
- Neureiter, C., Engel, D. and Uslar, M. (2016), 'Domain Specific and Model Based Systems Engineering in the Smart Grid as Prerequisite for Security by Design', *Electronics* **5**(4), 24.
- NIST (2023), 'NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework'.
- O'Brien, L., Bass, L. and Merson, P. (2005), Quality Attributes and Service-Oriented Architectures:, Technical report, Defense Technical Information Center, Fort Belvoir, VA.

- O'Meara, W. and Lennon, R. G. (2020), Serverless Computing Security: Protecting Application Logic, in '2020 31st Irish Signals and Systems Conference (ISSC)', IEEE, Letterkenny, Ireland, pp. 1–5.
- Papazoglou, M. (2003), Service-oriented computing: Concepts, characteristics and directions, in 'Proceedings of the 7th International Conference on Properties and Applications of Dielectric Materials (Cat. No.03CH37417)', IEEE Comput. Soc, Rome, Italy, pp. 3–12.
- Pennekamp, J., Henze, M., Schmidt, S., Niemietz, P., Fey, M., Trauth, D., Bergs, T., Brecher, C. and Wehrle, K. (2019), Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective, in 'Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy - CPS-SPC' 19', ACM Press, London, United Kingdom, pp. 27–38.
- Perez, A., Risco, S., Naranjo, D. M., Caballer, M. and Molto, G. (2019), On-Premises Serverless Computing for Event-Driven Data Processing Applications, in '2019 IEEE 12th International Conference on Cloud Computing (CLOUD)', IEEE, Milan, Italy, pp. 414–421.
- Rahman, A., Mahdavi-Hezaveh, R. and Williams, L. (2019), 'A systematic mapping study of infrastructure as code research', *Information and Software Technology* **108**, 65–77.
- Roman, R., Lopez, J. and Mambo, M. (2018), 'Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges', *Future Generation Computer Systems* **78**, 680–698.
- Rose, K., Eldridge, S. and Chapin, L. (2015), 'The internet of things: An overview', *The internet society (ISOC)* **80**, 1–50.
- Rushby, J. and Bloomfield, R. (2022), 'Assessing Confidence with Assurance 2.0'.
- Samonas, S. and Coss, D. (2014), 'The CIA strikes back: Redefining confidentiality, integrity and availability in security.', *Journal of Information System Security* **10**(3).
- Satyanarayanan, M. (2017), 'The Emergence of Edge Computing', *Computer* **50**(1), 30–39.
- Schleier-Smith, J., Sreekanti, V., Khandelwal, A., Carreira, J., Yadwadkar, N. J., Popa, R. A., Gonzalez, J. E., Stoica, I. and Patterson, D. A. (2021), 'What serverless computing is and should become: The next phase of cloud computing', *Communications of the ACM* **64**(5), 76–84.
- Shafiei, H., Khonsari, A. and Mousavi, P. (2021), 'Serverless Computing: A Survey of Opportunities, Challenges and Applications'.
- Shi, W., Cao, J., Zhang, Q., Li, Y. and Xu, L. (2016), 'Edge Computing: Vision and Challenges', *IEEE Internet of Things Journal* **3**(5), 637–646.
- Shojafar, M., Pooranian, Z., Naranjo, P. G. V. and Baccarelli, E. (2017), 'FLAPS: Bandwidth and delay-efficient distributed data searching in Fog-supported P2P content delivery networks', *The Journal of Supercomputing* **73**(12), 5239–5260.
- Sicari, S., Rizzardi, A., Grieco, L. and Coen-Porisini, A. (2015), 'Security, privacy and trust in Internet of Things: The road ahead', *Computer Networks* **76**, 146–164.
- Stouffer, K., Falco, J. and Scarfone, K. (2011), 'Guide to industrial control systems (ICS) security', *NIST special publication* **800**(82), 16–16.
- Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M. and Hahn, A. (2014), 'Guide to Industrial Control Systems (ICS) Security', *NIST Special Publication* .

- Subashini, S. and Kavitha, V. (2011), 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications* **34**(1), 1–11.
- Sultan, S., Ahmad, I. and Dimitriou, T. (2019), 'Container Security: Issues, Challenges, and the Road Ahead', *IEEE Access* **7**, 52976–52996.
- Sun, Y., Nanda, S. and Jaeger, T. (2015), Security-as-a-Service for Microservices-Based Cloud Applications, in '2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)', IEEE, Vancouver, BC, Canada, pp. 50–57.
- Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020), 'A survey on security challenges in cloud computing: Issues, threats, and solutions', *The Journal of Supercomputing* **76**(12), 9493–9532.
- Takabi, H., Joshi, J. B. and Ahn, G.-J. (2010), 'Security and Privacy Challenges in Cloud Computing Environments', *IEEE Security & Privacy Magazine* **8**(6), 24–31.
- Tange, K., De Donno, M., Fafoutis, X. and Dragoni, N. (2020), 'A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities', *IEEE Communications Surveys & Tutorials* **22**(4), 2489–2520.
- Tupa, J., Simota, J. and Steiner, F. (2017), 'Aspects of Risk Management Implementation for Industry 4.0', *Procedia Manufacturing* **11**, 1223–1230.
- Tuptuk, N. and Hailes, S. (2018), 'Security of smart manufacturing systems', *Journal of Manufacturing Systems* **47**, 93–106.
- Varghese, B., Wang, N., Barbhuiya, S., Kilpatrick, P. and Nikolopoulos, D. S. (2016), 'Challenges and Opportunities in Edge Computing'.
- Villamizar, M., Garces, O., Castro, H., Verano, M., Salamanca, L., Casallas, R. and Gil, S. (2015), Evaluating the monolithic and the microservice architecture pattern to deploy web applications in the cloud, in '2015 10th Computing Colombian Conference (10CCC)', IEEE, Bogota, Colombia, pp. 583–590.
- Wang, C., Wang, Q., Ren, K. and Lou, W. (2010), Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, in '2010 Proceedings IEEE INFOCOM', IEEE, San Diego, CA, USA, pp. 1–9.
- Webster, J. and Watson, R. T. (2002), 'Analyzing the Past to Prepare for the Future: Writing a Literature Review', *MIS Quarterly* **26**(2), xiii–xxiii.
- Wells, L. J., Camelio, J. A., Williams, C. B. and White, J. (2014), 'Cyber-physical security challenges in manufacturing systems', *Manufacturing Letters* **2**(2), 74–77.
- Wen, J., Chen, Z. and Liu, X. (2022), 'Software Engineering for Serverless Computing'.
- Wen, J., Chen, Z., Liu, Y., Lou, Y., Ma, Y., Huang, G., Jin, X. and Liu, X. (2021), An empirical study on challenges of application development in serverless computing, in 'Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering', ACM, Athens Greece, pp. 416–428.
- Wilde, T. and Hess, T. (2007), 'Forschungsmethoden der Wirtschaftsinformatik'.
- Williams, T. J. (1994), 'The Purdue enterprise reference architecture', *Computers in industry* **24**(2-3), 141–158.
- Xia, B., Bi, T., Xing, Z., Lu, Q. and Zhu, L. (2023), 'An Empirical Study on Software Bill of Materials: Where We Stand and the Road Ahead'.
- Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J. and Lv, W. (2019), 'Edge Computing Security: State of the Art and Challenges', *Proceedings of the IEEE* **107**(8), 1608–1631.

- Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A. and Malli, M. (2020), 'Cyber-physical systems security: Limitations, issues and future trends', *Microprocessors and Microsystems* **77**, 103201.
- Yu, D., Jin, Y., Zhang, Y. and Zheng, X. (2019), 'A survey on security issues in services communication of Microservices-enabled fog applications', *Concurrency and Computation: Practice and Experience* **31**(22).
- Zeyu, H., Geming, X., Zhaohang, W. and Sen, Y. (2020), Survey on Edge Computing Security, in '2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)', IEEE, Fuzhou, China, pp. 96–105.
- Zissis, D. and Lekkas, D. (2012), 'Addressing cloud computing security issues', *Future Generation Computer Systems* **28**(3), 583–592.
- Zografopoulos, I., Ospina, J., Liu, X. and Konstantinou, C. (2021), 'Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies', *IEEE Access* **9**, 29775–29818.