UNIVERSITÄT BAYREUTH

Digital Transformation in the Manufacturing Sector - Tackling Business and Technology Challenges

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Bastian Léon Stahl

aus

Aschaffenburg

Dekan:	Prof. Dr. Michael Grünberger
Erstberichterstatter:	Prof. Dr. Maximilian Röglinger
Zweitberichterstatter:	Prof. Dr. Björn Häckel
Datum der mündlichen Prüfung:	23.03.2023

„Die Zukunft kann man am besten voraussagen, wenn man sie selbst gestaltet."

Alan Kay

Mit dem Abschluss dieser Dissertation geht für mich eine der bewegendsten Phasen meines bisherigen Lebens zu Ende. Neben den inhaltlichen Einblicken und vielzähligen fachlichen Erfahrungen, die ich sammeln durfte, blicke ich insbesondere auf eine Zeit voller Zusammenhalt in Freundschaften, Familie und Partnerschaft zurück.

Ich bin daher unglaublich stolz und dankbar, für die wunderbaren Menschen, die mir diesen Weg ermöglicht haben, immer an mich geglaubt haben und in Momenten der Rück- und Fehlschläge für mich da waren.

Danke an meine akademischen Mentoren und Doktorväter Max und Björn. Ich danke euch für die Hilfestellung und Freiheit in der Betreuung, für die Menschlichkeit und das Vertrauen in allen Projekten. Danke, dass ihr an mich geglaubt habt.

Danke an alle Freunde, Kollegen und Kolleginnen und Wegbegleiter. Ich danke all denjenigen, die mich aus Nähe oder Ferne immer unterstützt haben. Und ich bin dankbar, dass aus so vielen großartigen Menschen wahre Freunde und treue Wegbegleiter wurden.

Danke an meine Familie. Ihr habt mir diesen Weg durch eure Erziehung, eure Werte und den stetigen Glauben an mich eröffnet. Ihr habt mich auf diesem Weg durch eure uneingeschränkte Liebe und Unterstützung begleitet. Ich danke euch für die unendlichen Möglichkeiten, die ihr mir eröffnet habt.

Danke an Michelle. Danke für deinen Glauben an mich. Danke für deine Warmherzigkeit, deine bedingungslose Unterstützung und deine Nachsicht, wenn mich die Promotion mal wieder viel Zeit, Energie oder gute Laune gekostet hat. Danke, dass du mein Ruhepol und meine Energiequelle bist.

Danke.

Abstract

Many incumbents in the manufacturing sector strive to leverage the various opportunities offered by digital technologies and therefore embark on digital transformation. Afforded by digital technologies, the development of digital business models represents a central field of action for manufacturers to counter increasing competitive pressure and declining margins. However, manufacturers face, among others, *business and technology challenges* when moving toward digital business models.

Especially for incumbent manufacturers, *business challenges* include the structured *exploration of digital business models* and identifying the *organizational capabilities* required for such new business models. Coming from hitherto mainly hardware-centric business models, this implies far-reaching changes for many companies, in which management must give structure and direction. In addition, in the wake of digital transformation, *technology challenges* arise from the broad adoption of digital technologies. Here, *IT security* is a central area of action and a crucial requirement for the successful implementation and sustainable operation of digital business models. Especially in the manufacturing sector, IT security incidents can paralyze entire value chains or threaten a company's existence through a drain of technical knowhow. Thus, manufacturers need to define *proactive and reactive measures* to enhance their IT security along with their digital transformation.

Many incumbent manufacturers are still struggling to meet *business and technology challenges* and thus call for applicable research artifacts that provide prescriptive knowledge and offer guidance. However, while existing research provides a valuable base of descriptive knowledge, for example, in archetypal business models or case studies about manufacturers' digital transformation, there is a research need for prescriptive knowledge with real-world applicability. To address this need, this cumulative dissertation sheds light on manufacturers' digital transformation and comprises five research articles that include research artifacts to assist in tackling these challenges.

First, regarding *business challenges*, this dissertation examines ways for incumbents to *structure the exploration* of digital business models. Therefore, research article #1 presents the case study of *WashTec*, an incumbent car washer manufacturer, revealing how the company successfully explored three digital business models utilizing a structured approach. Hence, the key artifact of research article #1 is a four-phase approach that complements core elements of

existing exploration approaches, for example, Design Thinking, with the aspects of strategy and monetization of digital business models.

Research articles #2 and #3 address *what capabilities* manufacturers need to develop based on an identified target digital business model. The two articles use established digital business model archetypes to develop and evaluate maturity models that assist in identifying the technical and non-technical capabilities required.

Second, this dissertation examines how manufacturers can meet the *technology challenges* of increasing IT security requirements associated with moving toward digital business models. In the area of *proactive measures*, a framework for the strategic consideration of IT security in digitalization projects is presented (research article #4). This artifact enables manufacturers to prioritize IT security according to identified drivers and individual requirements and, thus, to design-in IT security in digital solutions. However, since IT security incidents can never be prevented entirely, research article #5 addresses the area of *reactive measures* for IT security. Here, a maturity model is developed that provides organizations with a comprehensive perspective on capabilities for developing effective incident response management.

In sum, this work contributes to the existing body of knowledge about manufacturers' digital transformation consisting of both business and technology challenges. This work strives to empower manufacturers in tackling their digital transformation challenges by developing and evaluating applicable artifacts that offer notably prescriptive knowledge. In addition, this work stimulates future research on understanding digital transformation. For instance, by applying the developed artifacts as analytical lenses on a broad scale to generate new descriptive (e.g., by identification of transformation paths and associated theories) and prescriptive knowledge (e.g., deriving industry best practices) in the digital transformation of manufacturers.

Table of Contents

I Introduction

1 Motivation

The manufacturing sector represents a central driver of the German economy (Statistisches Bundesamt, 2022). However, while manufacturing high-quality machinery and equipment has been a differentiating feature of this industry for decades, the industry's market conditions have been changing recently. In particular, global competition is growing steadily and increases market pressure on incumbent firms. For instance, in 2021, China's machinery sales exceeded €1 trillion, outperformed Germany (~ €311 billion) by a mere factor of three - and the trend is rising (VDMA, 2022). Therefore, the manufacturing sector is characterized by high competition and shrinking profit margins, especially at the core of product sales (Björkdahl, 2020).

To withstand global competitive pressure, manufacturing executives focus on digital technologies as a strategic opportunity promising positive impacts on overall organizational performance, enhanced competitive advantage, and new ways of generating value (Devaraj & Kohli, 2003; Goldfarb & Tucker, 2019). Thus, for many executives in the manufacturing sector, embarking on digital transformation by leveraging digital technologies to enhance their profitability is a strategic response to changing environmental conditions (Vial, 2019; Volberda et al., 2021).

Digital transformation in the manufacturing sector is often associated with the concept of Industry 4.0 and cyber-physical systems (CPS), enabling to enhance efficiency in the existing business models (exploitation) or to unfold completely new value propositions and business models (exploration) (Björkdahl, 2020; Herden, 2020). Industry 4.0 refers to manufacturers increasingly utilizing digital technologies in industrial applications to leverage competitive advantages (Culot et al., 2020). This fuels the rise of CPS, where physical components (such as machines and sensors) and software (e.g., intelligent manufacturing execution systems) exchange information, become increasingly blended, and trigger automated actions to enhance their productivity (Kagermann et al., 2013; Waschull et al., 2020). To enable CPS, manufacturers must connect their production assets like robots and machines via the Industrial Internet of Things (IIoT) and process the resulting data using digital technologies such as Big Data Analytics and Artificial Intelligence. Accordingly, many manufacturers invest substantially in adopting and rolling digital technologies. Not surprisingly, in 2021, every second executive of German manufacturers planned substantial investments in rolling out digital technologies (PWC, 2021). With the rising trend of digitally connected production assets

in the industrial sector, the number of globally active IIoT-connections is expected to grow to 27 billion by 2025 (Hasan, 2022). Leveraging CPS and Industry 4.0 for efficiency gains in existing business models (exploitation) is associated with lower machine downtimes and reduced quality costs. For instance, CPS can reduce downtime in manufacturing lines by anticipating problems and resolving them without human intervention (Margherita & Braccini, 2020). CPS can also increase the flexibility of production processes: for example, through automatic tool changeovers or additive manufacturing processes such as 3D printing (Simons, 2018). In this way, highly individualized products can be manufactured in small quantities. According to a 2020 McKinsey report, this may yield a 10 to 30 % increase in throughput and a 10 to 20 % reduction in quality costs (de Boer et al., 2020).

While exploitation attempts to optimize the existing business model, digital technologies also unleash the potential of exploring new opportunities to extend a company's value proposition beyond its existing product core (exploration) (Oberländer et al., 2021; Porter & Heppelmann, 2014). For machinery and equipment manufacturers, digital technologies are the key to expanding their business models beyond selling physical products and offering digitally enabled services (Hunke et al., 2021). Digitally connecting sold machines enables insight into usage data and allows manufacturers to position themselves with new, digital business models and move toward servitization of business (Favoretto et al., 2022; Gebauer et al., 2021). In this way, the advantages of CPS can not only be exploited in the manufacturer's production but can also be marketed to customers in the form of digital business models and services. The laser-based metal processing machine manufacturer *Trumpf* is a prominent example of this explorative development. In addition to selling machines to customers, *Trumpf* developed a "pay-per-part model" for metal processing solutions (Schuh et al., 2021). *Trumpf* uses an equipment-as-a-service model enabled by digital technologies. This model allows customers to access a machine at *Trumpf's* production facilities remotely. Therefore, the machine's production planning, programming, and maintenance are entirely managed by *Trumpf*. A significant advantage is created by the fact that several customers can use the same machine, allowing *Trumpf* to operate it at increased capacity. Especially for customers with low equipment utilization, the "pay-per-part model" is advantageous as customers only pay for the parts produced instead of buying the entire asset (Ringel, 2022).

Another example is *Kaeser*, a manufacturer of compressor systems and services (Kaeser Kompressoren, 2022). While the company hitherto sold compressors to its customers, the "*Sigma Air Utility*" is an entirely service-based business model. Leveraging Industry 4.0

technologies to enable digital machine health monitoring and the billing of consumption units, *Kaeser* takes care of compressor operation at the customer's facility. This allows the customer to pay a monthly, variable fee based on the compressed air consumption instead of buying and maintaining the compressor. For *Kaeser*'s customers, this business model allows more flexibility as they only pay for their consumption. For *Kaeser*, the advantages are enhanced customer retention and a reduced number of service calls, as the company can proactively manage the health status of the equipment (Bock et al., 2019).

In summary, while exploitation helps reduce costs in the existing business model, exploring digital business models can even enable tapping into new revenue opportunities and dampening competitive pressure. Moreover, digital business models promise to strengthen customer loyalty, help garner competitive advantages, and even open up new markets (Kowalkowski et al., 2017; Voigt et al., 2021). Concordantly, a McKinsey report indicates that companies that invest at least as much in developing new business models as in maintaining their core business can achieve above-average growth (McKinsey Digital, 2019).

So while there are many reasons for manufacturers to explore digital business models, their realization in the wake of digital transformation is fraught with two central challenges, especially for incumbent firms (Favoretto et al., 2022; Zheng et al., 2019). First, manufacturers face *business challenges* when endeavoring in their transformation toward digital business models. These challenges refer to managing the transformation toward a business logic of digitally-enabled value creation, delivery, and capture (Davenport & Westerman, 2018; Ibarra et al., 2018). Especially for incumbent manufacturers, transitioning from a previously product-centric organizational logic to a digital business model is a considerable transformation effort (Favoretto et al., 2022). According to a BCG report, only about 30 % of organizations fully embrace the potential of digitally-empowered business (Forth et al., 2020). However, the report also indicates success is less dependent on the company's starting position than the structuring and commitment to this transformation (Forth et al., 2020). Thus, an initial task is *exploring a target digital business model* that fits existing and future customers based on established organizational assets like the products or market position (Sund et al., 2021). While a clear vision of a pursued digital business model can then provide the strategic polestar for this transformation, all areas of an enterprise must be aligned to fulfill it (M. Wessel et al., 2016). Consequently, the organization undergoes a far-reaching transformation that requires it to develop new organizational capabilities to embrace digital business models (Vial, 2019). In this context, organizational capabilities represent repeatable patterns of action, including technical

and non-technical aspects (Kerpedzhiev et al., 2021; Wade & Hulland, 2004). To structure such organization-spanning transformative changes, layered enterprise architecture models have proven valuable tools in the information systems domain (Rashed & Drews, 2021). These models provide an integrated and aligned perspective on business and IT to facilitate and standardize communication between different organizational stakeholders (Kotusev, 2018). Besides the widely applied *The Open Group Architecture Framework (TOGAF)*, many other enterprise architecture frameworks have been developed for specific application areas (Kotusev, 2018; Winter & Fischer, 2006). For instance, the *Reference Architectural Model Industry 4.0 (RAMI 4.0)* helps manufacturers to structure the capabilities required for Industry 4.0 (Hernández et al., 2020). These enterprise architecture models typically use a hierarchical, multilevel layered structure to comprehensively cover the organization's elements (Winter & Fischer, 2006). As such, the five-layered digital transformation model of Urbach and Röglinger (2019) offers a socio-technical concept (Appelbaum, 1997; Baxter & Sommerville, 2011) to examine an organization's digital transformation. In their representation, the outward-facing business layer (i.e., *business model*) represents the top, while the bottom layer is represented by technical equipment (i.e., *infrastructure*) (Urbach & Röglinger, 2019). In between the edges, the models possess various technical and non-technical intermediary layers connecting these two edges (i.e., *business processes*, *people & applications*, *and data & information*) (Urbach et al., 2021).

Especially in manufacturing, where profound socio-technical transformation efforts are needed to overcome product-centric business models and organizational logic, the newly required capabilities become visible at all organizational layers. For instance, when *Kaeser* established their offering of *Sigma Air Utility*, the company needed to adapt and develop the required capabilities (Bock et al., 2019; Kaeser Kompressoren, 2022). At the *business model* layer, the rationale for sales shifted, as *Kaeser* was now offering "compressed air" instead of a simple product (i.e., compressors). Thus, sales became increasingly solution-oriented, and the offering became a service. This required new capabilities to successfully market and monetize the offering (Baltuttis et al., 2022). Also, the company's *business processes* had to be adapted to the new business model. For example, the company had to establish new processes for consumption-based billing, which is now in use (Kaeser Kompressoren, 2022). In the area of *people & applications*, the new business model also changed requirements. Due to *Kaeser's* role as operator of assets at the customer's site, the customer relationship changed from a transactional to a partnership-based one. This changed role must be supported and maintained

by the employees (e.g., regular customer meetings). At the same time, with this layer, the transition to the technological aspects of the transformation becomes evident: New application systems (i.e., the *Kaeser Plant Control Center*) for monitoring customer assets and managing service calls are needed to fulfill the business model (Bock et al., 2019; Kaeser Kompressoren, 2022). Operating equipment at the customer's site also resulted in new requirements for *Kaeser* regarding the *data and information* needed. The manufacturer now relies on information about the operating status, usage, and health of its machines at the customer's site (Parvinen et al., 2020). For this purpose, monitoring points had to be defined, and the secure transport and storage of the data had to be ensured. Consequently, this also meant the adoption of new *infrastructure*. For instance, the customer's on-site equipment was connected to a Kaeser database and linked directly to the Enterprise Resource Program (ERP) to store spare parts. Thus, the customer's networked plants also represent additional remote assets in *Kaeser's* IIoT network (Bock et al., 2019).

As seen in *Kaeser's* example, moving toward digital business models implies a tremendous shift in the organizational rationale and requires the *structured development of new capabilities* for incumbent firms (Comuzzi & Patel, 2016). Consequently, organizations must structure their transformation in alignment with a target digital business model, define the required capabilities for realization, and execute the organizational change (Favoretto et al., 2022; Wißotzki et al., 2021).

While the last section addressed the business challenges, manufacturers also face *technology challenges* when moving toward digital business models and broadly adopting digital technologies (Vial, 2019). The adoption of CPS entails connecting machines and equipment in internal production facilities and at external customer production sites to access the sold machines (Wang et al., 2015). This leads to a steadily growing attack surface for cyberattacks as the number of networked and digital assets increases. Consequently, the likelihood of an incident occurring and the potential extent of the damage grow, too (D. Wu et al., 2018). Furthermore, IT security incidents can result in direct costs due to data loss or system failure and indirect costs such as reputational damage (Knight & Nurse, 2020). Particularly in manufacturing, the drain of know-how is critical to competition and can threaten a company's existence (Tuptuk & Hailes, 2018). Internally, IT security poses a challenge to manufacturers, as their networked production facilities in Industry 4.0 are particularly vulnerable to IT security threats (Berger et al., 2022; Tupa et al., 2017). Externally, attacks on connected machines, systems, and digital services represent new vectors for cyberattacks on customers. Thus, intra-

and inter-organizational networking increase IT security risks to the entire value network (Berger et al., 2020). The failures in the production environment caused by IT security incidents can thus affect entire value networks (Berger et al., 2022). Hence, *IT security* has been positioned as one of the biggest technology challenges and is a top priority for many IT executives (Kappelman et al., 2020). *Kaeser* also faced this challenge as part of its new business model: The network infrastructure connecting the compressor stations at customer sites to the central *Kaeser* database raised the need to secure this connection against unauthorized access to data and the network (Bock et al., 2019).

With the trend of cyberattacks being on the rise, the entire German economy faces annual damage of around €203 billion due to the theft of IT equipment and data, espionage, and sabotage (Berg, 2022). Nearly every second company (45 %) in Germany agreed that cyber-attacks threaten their business existence (Berg, 2022). To avoid such substantial consequences, companies must find ways to manage the technology-induced security issues with both *proactive* (e.g., when securely developing or implementing new digital assets) or *reactive measures* (e.g., when implementing an effective incident response management) to boost resilience. In practice, however, many organizations have a shortage of cybersecurity talent, knowledge, and expertise, and thus, addressing IT security sufficiently is challenging (Boehm et al., 2022). Especially in the context of digital transformation, the strategic integration of IT security is a key prerequisite but also a substantial challenge for many companies (Abolhassan, 2017; S. P.-J. Wu et al., 2015). Therefore, management must consider the challenges of adopting digital technologies and define *proactive and reactive measures* for risk mitigation.

In sum, digital transformation to enable digital business models offers manufacturers a strategic response to ever-increasing competitive pressure (Vial, 2019). However, this transformation is beset with *business challenges*, including the structured *exploration of digital business models* and the development of *required capabilities*. In addition, with the growing adoption of digital technologies, *technology challenges*, such as the growing demand for *proactive and reactive* IT security measures, arise. Therefore, these two challenges emphasize that digital transformation must be understood as a comprehensive, socio-technical change process spanning all organizational levels (Urbach & Röglinger, 2019; Vial, 2019) (Figure 1).

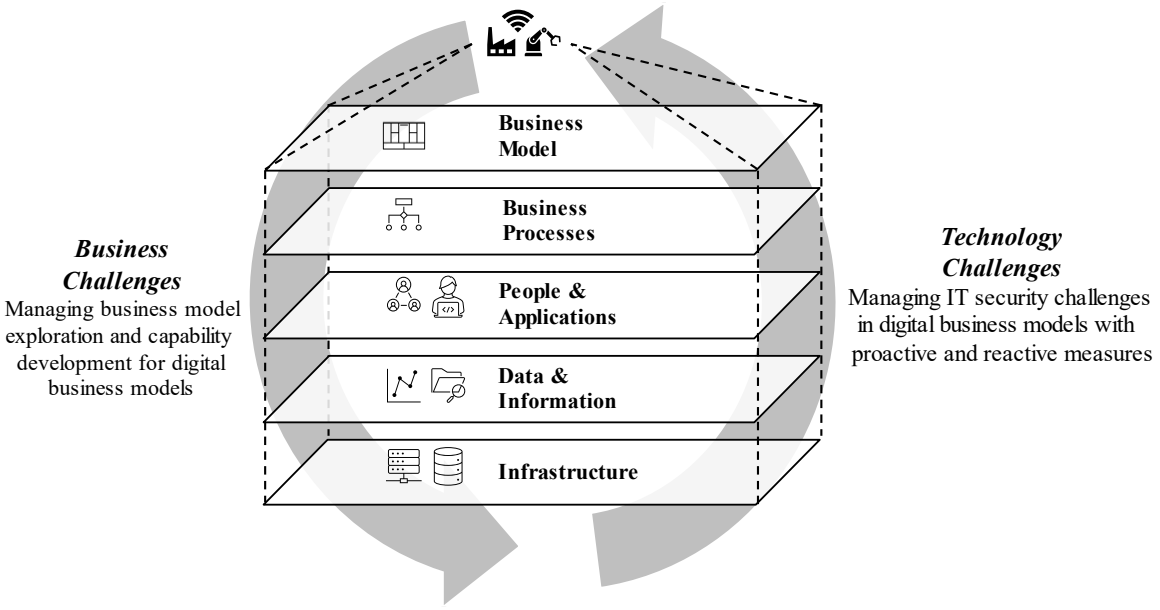

Figure 1. Conceptualization of Business and Technology Challenges in Digital Transformation in Manufacturing Based on Urbach and Röglinger (2019)

2 Research Objectives and Structure of This Dissertation

This dissertation aims to address the two challenges described in the previous section as two main research objectives. It, therefore, builds on existing research, such as business model archetypes and descriptive studies, to develop applicable artifacts that deliver prescriptive knowledge.

First, regarding *business challenges*, previous research conceptualizes possible target states of digital business models in manufacturing or generic transformation paths towards CPS and Industry 4.0 (Duraivelu, 2022). However, there is still a need for research in the field of digital transformation to connect these two aspects to work out how manufacturers can *structure exploration endeavors for digital business models* and *which capabilities* are necessary for the respective digital business model (Hunke et al., 2021; Verhoef et al., 2021). This work, therefore, aims to contribute to this challenge by developing artifacts for structuring the transformation toward digital business models in manufacturing. These artifacts embed themselves in previous research and unify existing knowledge under the focal point of specific digital business models to apply this knowledge in practice. Furthermore, this can lay the foundation for further research by being applied as an analytical lens to understand how companies transform toward digital business models and develop the associated capabilities (Favoretto et al., 2022).

Second, the *technology challenges*, especially those addressing IT security, receive little attention in combination with the strategic considerations of transforming toward digital business (Vial, 2019). While the literature suggests many approaches, especially technical ones, for improving IT security, these insights have rarely been applied in the context of digital transformation. As manufacturers introduce many digital technologies in their digital transformation and thus create new attack surfaces for IT security, these companies must understand IT security as an integral part of the digital transformation (Mendhurwar & Mishra, 2021). In this way, IT security can be developed in alignment with digital transformation, and the development of "technical debt" (i.e., the expensive catching up on necessary investments) can be avoided (Martinez et al., 2021). Therefore, this dissertation aims to provide concrete artifacts demonstrating how manufacturers can leverage *proactive and reactive measures* to enhance IT security during their digital transformation.

The overarching objective of this work is to examine digital transformation in manufacturing from both a *business* and a *technology* perspective and thus to provide artifacts that tackle arising challenges in both domains. In addition, this dissertation strives to enhance the understanding of both aspects as part of the integrated management of digital transformation in manufacturing.

As a cumulative dissertation, this work consists of five research articles that address the two issues raised before: (1) *business challenges* and (2) *technology challenges* in the wake of digital transformation (Figure 2). The research articles in both pillars use *design science research (DSR)* methodology to answer the respective research questions (Hevner et al., 2004). As such, applicable artifacts built on the extant research knowledge base to resolve real-world problems are designed and evaluated (vom Brocke et al., 2020). The results provide conceptual and theoretical lenses on the respective phenomenon under investigation in the form of artifacts.

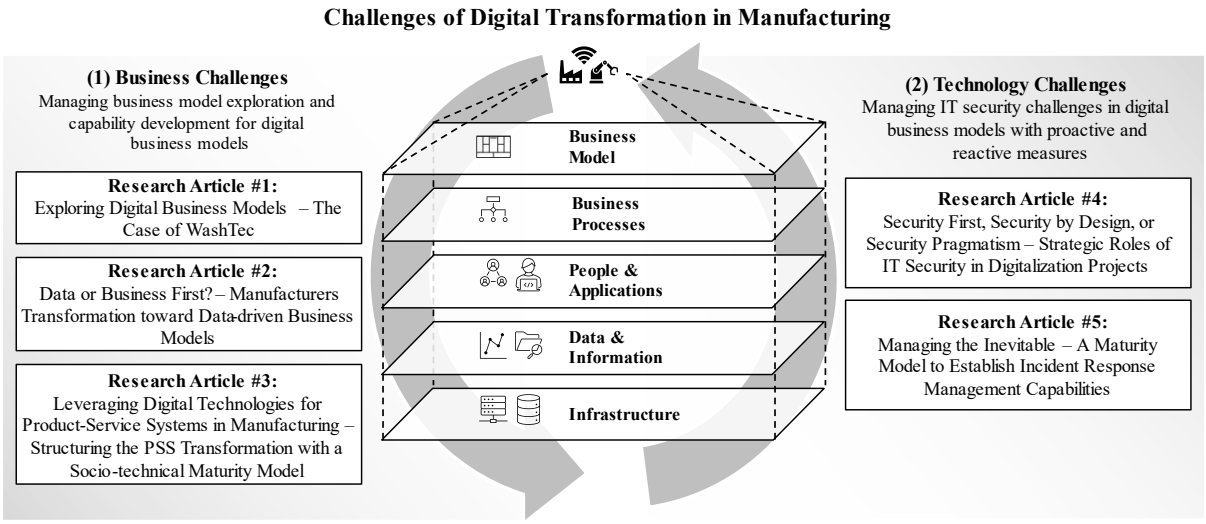

Figure 2. Structure of This Dissertation

Section II.1 presents research articles #1, #2, and #3 that address *business challenges*. Research article #1 uses the case study of the incumbent car wash manufacturer *WashTec* to outline the exploration journey toward digital business models. In particular, this paper addresses the issue of *how* the exploration of digital business models can be structured in manufacturing. The core result of this study is a structured, four-phase methodological approach that supports incumbent manufacturers in identifying and initially evaluating digital business models. Here, manufacturing-specific challenges of digital transformation, such as how to explore structurally beyond the existing product core or monetize digital business models, are addressed in a dedicated manner. Once manufacturers have identified a potential digital business model, they need to determine *which capabilities* are required for these business models. In this context, based on digital business model archetypes, research article #2 outlines which capabilities manufacturers need to develop along their entire organization to successfully offer specific archetypal digital offerings (e.g., digital dashboards to visualize machine's performance indicators for customers) (Hunke et al., 2021). The central result of this work is a maturity model that links digital business model archetypes with necessary capabilities. However, digital business models in manufacturing are often associated with increasing servitization, resulting in a blended offering of products and (digital) services. Therefore, the concept of so-called product-service systems (PSS) strives to merge a tangible component (e.g., the sold machine) and non-tangible components (e.g., remote maintenance services) in a bundle that yields increased customer utility (Lerch & Gotsch, 2015; Tukker, 2004). As different archetypal PSS offerings have established themselves as digital business model offerings achieved by digital transformation, research article #3 leverages archetypal PSS typologies to elaborate on which

capabilities are necessary to offer certain digitalized PSS. The central result of this work is a socio-technical maturity model based on PSS archetypes.

Addressing the *technology challenges* of manufacturers' digital transformation, section II.2 presents two papers (research articles #4 and #5) focusing on IT security. Research article #4 provides an artifact enabling companies to define the strategic role of IT security in digitalization projects as a *proactive measure*. The paper leverages existing research on various drivers for integrating IT security in digitalization projects to develop a framework that offers decision support for this issue. Research article #5 focuses on *reactive measures* of IT security by addressing the issue of Incident Response Management (IRM). The work develops a maturity model for necessary IRM capabilities. This unifies existing practices from the literature into a comprehensive framework to provide a perspective on IRM capabilities and to stimulate further development.

Section III concludes this paper with a summary of key findings, limitations, and directions for future research. Section IV lists the references used in this dissertation. Finally, the Appendix in section V provides an index of the research articles presented in this dissertation (V.1), my individual contributions (V.2), and the research articles themselves (V.3 to V.7).

II Tackling Business and Technology Challenges in the Manufacturing Sector

In the course of manufacturers' digital transformation, organizations are changing the company's offers, organizational logic, structures, and technologies used (Legner et al., 2017; Urbach et al., 2021). To master this comprehensive endeavor in manufacturing, management must overcome two interdependent issues: in *business challenges*, management is called upon to identify a targeted digital business model and define the required capabilities to enable this new business model. Furthermore, steering toward new business models fueled by digital technologies entails adopting novel technologies, such as IIoT. Therefore, building new digital solutions and adopting emerging technologies, such as IT security, gives rise to *technology challenges* (Vial, 2019). This makes the digital transformation in manufacturing, whose starting position is often strongly product-centric, a complex challenge that must be met in an integrated manner.

1 Business Challenges

Based on CPS and Industry 4.0, digital technologies enable new digital business models in manufacturing (Luz Martín-Peña et al., 2018). However, the logic of value creation strongly differs between traditional product-centric business models and new service-oriented value propositions (Linde et al., 2021). As a result, the digital transformation of these companies entails considerable *business challenges* in practice and is an intriguing research object for study. Existing research reveals and structures the various options for digital business models in manufacturing. A joint study by the VDMA and PWC supports the growing trend of these business models. It predicts that the market share in the plant engineering sector of solution-oriented business models will quadruple from 10 to 40 % by 2025 (VDMA & PWC, 2019). While existing works vividly portray possible visions through archetypal examples, structuring the transformation remains challenging for many executives. It implies leaving the well-trodden paths of hitherto product-centric business and innovation practices to deal with the high ambiguity of digital business models (Sjödin et al., 2022). For instance, many manufacturers struggle to sense exploration opportunities and assess the strategic value of new, digital business models, to what extent existing business can be strengthened or expanded, and how it can be monetized (Favoretto et al., 2022; Linde et al., 2021). For example, pay-per-use models imply a change from capital expenses (CapEx) to operating expenses (OpEx) (Böttcher et al., 2022; Linde et al., 2021). Thus, management is faced with the issue of *identifying a desirable target*

digital business model based on an existing product core and business for which there is a lack of systematic approaches (Sjödin et al., 2022; Verhoef et al., 2021; Wißotzki et al., 2021).

Against this backdrop, research article #1 outlines the case of *WashTec*, an incumbent manufacturer of car wash systems. *WashTec*, like many other incumbents, excelled in enhancing its existing business models (exploitation) but struggled to develop new digital business models (exploration) (Oberländer et al., 2021). Exploration for manufacturing means that digital technologies allow novel ways of value creation, delivery, and capture past the limits of an existing product or service core (Hunke et al., 2021). Before *WashTec* started its exploration journey toward digital business models, the management set up two central requirements: First, the exploration endeavor must be evaluated according to the strategic value of allowing exploration beyond an established product core. Second, the exploration must include an evaluation of the monetization potential of the firm. Although many existing and established innovation and exploration approaches exist, these fail to meet these two key requirements set by *WashTec*'s management. On the one hand, established and well-structured innovation processes, such as the Stage-Gate-process of Cooper (1990), are very efficient approaches for developing solutions to clear requirements. However, these structured approaches are limited in their suitability for exploring new digital business models, driven more by an opportunity perspective than by clearly defined solution requirements (Acar et al., 2019). On the other hand, there are creative, problem-oriented innovation paradigms like Design Thinking and associated processual representations (Brown, 2008; Naiman, 2019). The Design Thinking process model can be characterized by two central phases of divergence and convergence (i.e., the definition of customer challenges and the design and evaluation of solutions) (Clune & Lockrey, 2014). As the customer-centric process starts from identifying customer challenges, it is more suited to explorative endeavors. However, this approach lacks strategic considerations and doesn't evaluate monetization potentials (Linde et al., 2021).

Against this backdrop, research article #1 uses an Action Design Research approach (Mullarkey & Hevner, 2019) to develop a guiding structure to assist *WashTec* in exploring digital business models. The artifact of this paper is a four-phase approach (i.e., *Activation, Inspiration, Evaluation,* and *Monetization*) that enhances established Design Thinking patterns (Naiman, 2019) to identify, conceptualize and evaluate digital business models (Figure 3).

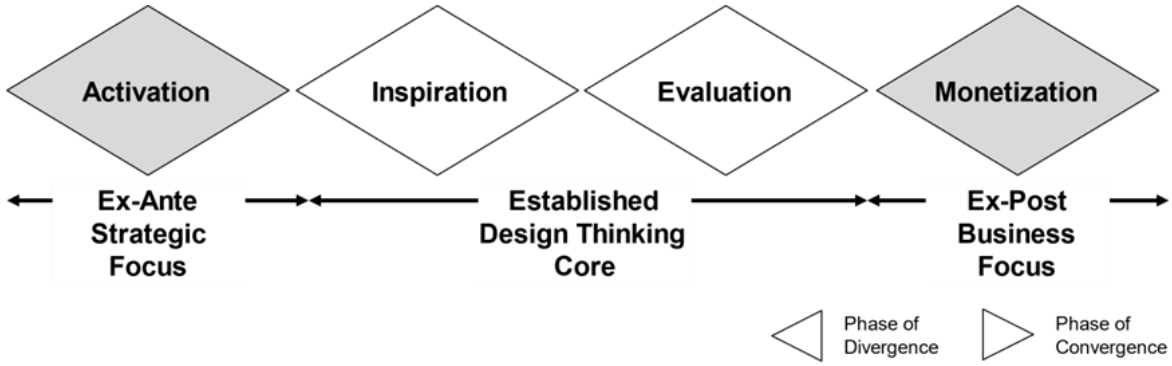

Figure 3. The Four-phase Exploration Approach of WashTec

In the initial *Activation* phase, *WashTec* laid an ex-ante strategic focus and evaluated different strategic opportunities for exploration. This included the development of so-called "value pools," which represent business model opportunities in strategically relevant markets. These can be grouped into strategic clusters and evaluated in terms of their distance from the core business model. This phase thus enabled *WashTec's* management to focus on those business model opportunities that go beyond the existing product core but match the company's strategy and existing product portfolio. Based on this analysis, strategically valuable value pools were prioritized and transferred to the subsequent *Inspiration* phase. In this phase, *WashTec* developed innovative ideas within the prioritized value pools utilizing the expertise and creativity of their workforce as well as external innovation sources through cooperation with universities. As a result, these ideas were further refined and prioritized. In the subsequent *Evaluation* phase, prototypes were developed to evaluate the remaining ideas for digital business models. Here, three main criteria were used to assess the value of the ideas – desirability (i.e., alignment with customer expectations), feasibility (i.e., technical feasibility), and viability (i.e., in terms of overall financial potential) (Ries, 2011). Lastly, *WashTec's* exploration approach also includes the so-called *Monetization* phase. This phase aims to evaluate the detailed business cases and derive an overarching monetization strategy for the digital business models (Baltuttis et al., 2022).

In sum, research article #1 presents a four-phase approach to exploring digital business models as the article's key artifact. Based on this structure, the case company, *WashTec*, successfully developed three digital business models. For practitioners, the developed approach can serve as a blueprint to structure their exploration of digital business models, thus offering prescriptive knowledge. In addition, the article also offers lessons learned and recommendations for incumbents to approach exploration more effectively. For research purposes, the work offers descriptive knowledge about the challenges and lessons learned along the case company's

exploration journey. It highlights the complexity of the socio-technical transformation required to move from hardware-centric organizational logic to new, digital business models. The artifact and the embedded prescriptive knowledge may stimulate further design-oriented research to build on and enhance this structure.

However, once a target of transformation has been set, manufacturers must develop appropriate capabilities aligned to the aspired digital business model archetype (Favoretto et al., 2022; Hunke et al., 2021). Therefore, unraveling *what* capabilities a company needs to offer specific archetypal digital business models remains a pressing challenge for executives in this sector (M. Yang & Evans, 2019).

Research already offers approaches that structure the multitude of digital business opportunities in this sector. For example, existing studies provide an overview of various archetypal ways manufacturers can use digital services and CPS to develop new value propositions (Hunke et al., 2021; Ibarra et al., 2018; Jovanovic et al., 2022). Hence, digital business models can be classified by focusing on embedded digital services. For instance, Hunke et al. (2021) propose a typology of digital business models characterized by their data-driven service (i.e., *data provider*, *insight provider*, *recommendation provider*, and *digital solution provider*). In the first archetype, manufacturers provide customers with (product) data beyond the physical product (*data provider*). The data is only moderately processed, for instance, when visualized in dashboards (Hartmann et al., 2016). The *insight provider* processes the data to meet specific objectives associated with a customer's needs (Heinz et al., 2022); for instance, to trigger alarms when machines or processes malfunction. As a *recommendation provider*, a manufacturer offers tailored decision support for customers. Predictive maintenance services are an example of this type of offering. Finally, manufacturers can act as *digital solution providers*, opening up novel ways of doing business by turning into smart data platform providers (Beverungen et al., 2021; Beverungen et al., 2022).

While there are manifold contributions to research on technical capability development, an integrated and aligned perspective on business and technology capabilities for distinct data-driven business model archetypes is needed (Hunke et al., 2021). This perspective promises to enhance research's understanding of this transformation and offers guidance for practitioners.

To guide transformative endeavors and structure capability development, maturity models are valuable artifacts offering guidance for research and practice (Becker et al., 2009; Mettler, 2011). From a research perspective, maturity models represent theories of how organizational

capabilities develop progressively along an expected, desired, or logical maturation path (Pöppelbuß & Röglinger, 2011). As such, maturity models strive to disentangle required capabilities and offer prescriptive knowledge (Gregor & Hevner, 2013). In practice, maturity models help assess an organization's status quo, determine the desired target state, and identify fields of action (Pöppelbuß & Röglinger, 2011).

Against this backdrop, research article #2 proposes a maturity model for transforming toward archetypal data-driven business models in manufacturing. The development follows the procedure model of Becker et al. (2009) that specifies the DSR methodology for maturity models regarding their design and evaluation. Based on eight interviews with practitioners, research article #2 outlines three key requirements for the maturity model to be developed: First, the model should integrate established business model archetypes to offer clear guidance on the target state of transformation. Second, the model should allow comprehensive coverage of socio-technical capabilities on all enterprise architecture layers. Third, the model should include complete capability descriptions to enhance the model's prescriptive value and usability for practice.

Based on these requirements, the data-driven business model maturity model (DDBM3) was developed using the archetypal digital business models of Hunke et al. (2021) as maturity levels (columns). In addition, it uses the layered enterprise architecture model of Urbach and Röglinger (2019), presented in section I.1. to structure the model's 22 capability dimensions (rows) in five major focus areas. Finally, as a continuous maturity model, it offers capability descriptions for every cell in the resulting matrix.

In the DDBM3 (Figure 4), the first focus area *business model* includes four capabilities dimensions (i.e., "value proposition," "customer interaction," "monetization and pricing," and "sales and channel management"). These outward-faced capability dimensions are essential for manufacturers to define, market, and monetize digital business models based on the archetypal offerings of Hunke et al. (2021). The second focus area, *business processes*, covers specific processual capabilities that create, deliver, and capture the value of data-driven services and outlines how manufacturers can manage the required activities. This focus area includes four capability dimensions (i.e., "strategy and vision for data-based business," "data-centric process management," "knowledge sharing and management," and "product life cycle management"). The next focus area is *people and applications*. It includes cultural aspects (capability dimension "recognition and mindset"), soft and hard skills ("methods," "data analytics

competencies"), responsibilities ("roles and responsibilities"), and tools ("data analytics tooling") for data-driven business models at the employee level and seeks to empower the workforce for digital business models. The next focus area, *data and information,* includes a focus on mechanisms of data management and the extraction of information. It, therefore, comprises four capability dimensions (i.e., "applied forms of analytics," "data management, " "data governance and quality," and "horizontal and vertical data integration"). Lastly, the focus area *infrastructure* covers the technological enablers that organizations need to provide digital business models and includes software and hardware's secure and scalable operation. It comprises five capability dimensions (i.e., "data analytics software management and operations, " "data-driven service integration and deployment," "data architecture and scaling," "cybersecurity and -privacy," and "cyber-physical systems and connectivity").

Along with the development procedure of Becker et al. (2009), the DDBM3 was also evaluated. The artifact was evaluated artificially by an academic focus group (Tremblay et al., 2010). Additionally, a naturalistic evaluation was performed by applying the model to two manufacturers (i.e., *Alpha* and *Beta*) to assess their status quo and target the state of transformation toward digital business models (Sonnenberg & vom Brocke, 2012). Research article #2 finds that the two manufacturers took very different approaches to transform toward digital business models, namely "data first" and "business first." For *Alpha*, a "business first" approach was observed. *Alpha's* transformation was mainly driven from the business side as customers demanded data delivery from connected machines. Consequently, *Alpha* possessed more maturity capabilities in the upper levels of the DDBM3 (e.g., strategic initiatives and new roles). In contrast, weaknesses were identified in the bottom capability dimensions of the DDBM3, for instance, in the data analysis capability or the scaling of networked machines.

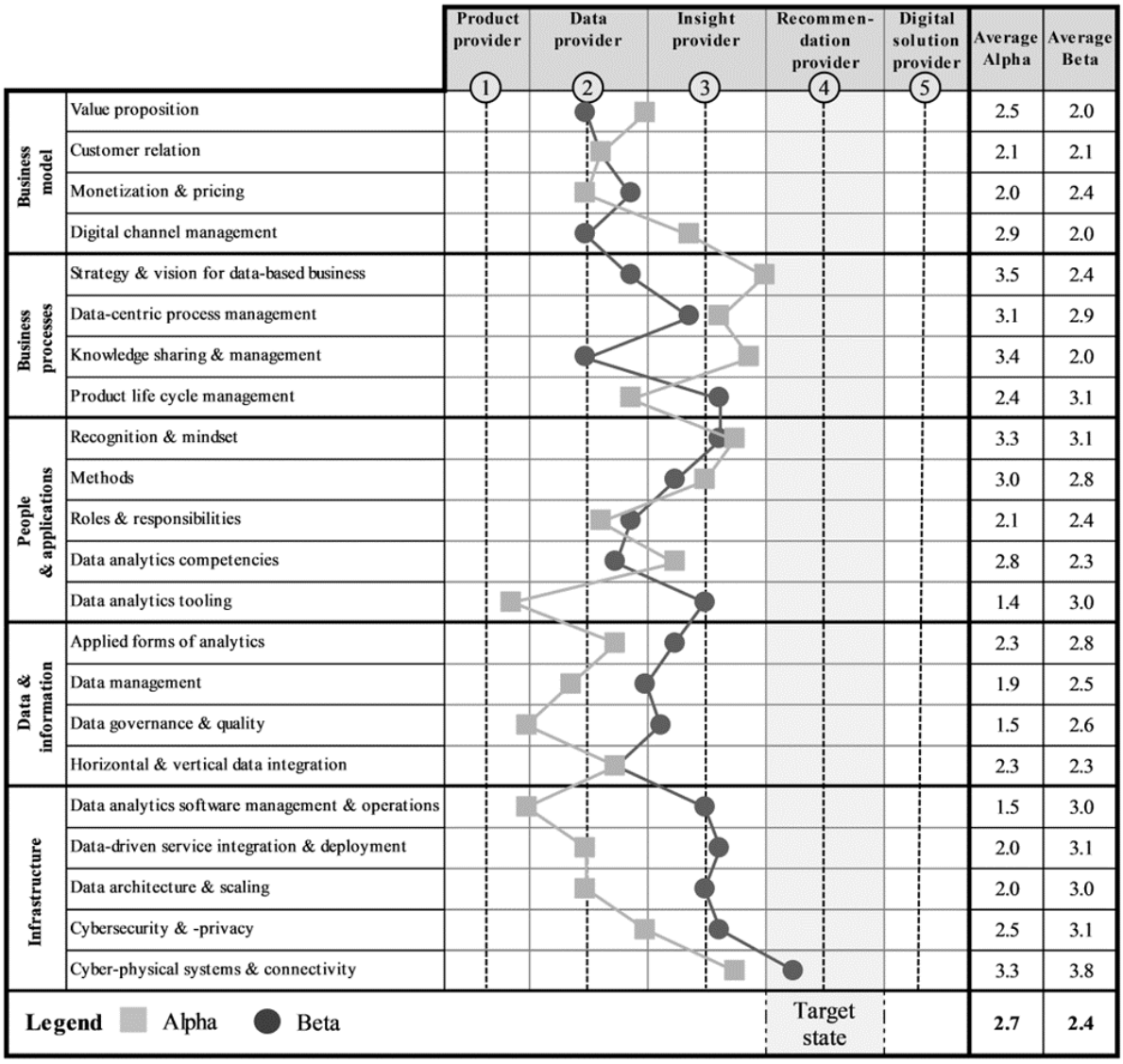

Figure 4. The Data-driven Business Model Maturity Model (DDBM3)

In contrast, *Beta*, with the "data first" approach, has more mature capabilities in the technological and data areas of the DDBM3 (e.g., "cyber-physical systems" or "data analytics software management and operations"). However, *Beta* showed weaknesses in the upper capability dimensions, such as monetization and pricing capabilities, and knowledge sharing within the organization.

In sum, research article #2 uses the typology of Hunke et al. (2021), which focuses on data-driven services, to structure the transformation of manufacturing toward digital business models. The contribution of research article #2 is twofold: First, the naturalistic demonstration of the model highlights the artifact's applicability and usefulness for practitioners. Thus, the DDBM3 was used for a status quo and target state assessment. With its continuous design, the model provides prescriptive knowledge of the required capabilities for digital business models

(Gregor & Hevner, 2013). Second, the insights gained from the application of the model highlight the model's integrative perspective's value for research to improve the understanding of this transformation as different paths of manufacturers moving toward digital business models become apparent. Thus, the model offers an analytical lens for research, including the potential of descriptive knowledge on transformative actions in manufacturing (Favoretto et al., 2022).

Since many manufacturers have an established, product-centric business model, research article #3 uses a different typology to assist these companies in defining relevant capabilities for digital business models. Thus, after all, especially in manufacturing, a trend toward offering bundles of physical equipment and digital services, dubbed as digitalized PSS, can be observed (Lerch & Gotsch, 2015). Therefore, research article #3 focuses not only on the aspect of data-driven services but also on how physical products and (digital) services can be combined in the value proposition. These offerings go beyond traditional service complements to physical products (e.g., spare parts management) (Favoretto et al., 2022). Digital technologies (e.g., IIoT and data analytics) enable digitized PSS that can be offered proactively. Digitalized PSS can enhance the customer utility of machines by offering predictive maintenance services (Gebauer et al., 2021; Lerch & Gotsch, 2015). To structure possible target business models associated with digitalized PSS, Tukker (2004) proposes a classification according to their customer value proposition (M. Yang & Evans, 2019; Zheng et al., 2019): In (1) *product-oriented PSS*, the business model focuses mainly on selling products, and a few additional services, such as maintenance services, are added (M. Yang & Evans, 2019), which in CPS can be provided remotely (Lerch & Gotsch, 2015). In (2) *use-oriented PSS*, the use or availability of a product is sold (Baines et al., 2007) - an example of this is the fleet management of *Hilti*, a global company that provides construction tools. However, instead of just selling tools, *Hilti* offers a comprehensive bundle of products and complementary services in a "pay-per-use model" (vom Brocke et al., 2014). In (3) *result-oriented PSS*, the customer and the supplier agree in advance on the outcome to be delivered by the supplier and the price to be paid by the customer (Selviaridis & Wynstra, 2015). Central to this PSS type is that customers purchase a function or result rather than purchasing a machine necessary for the function or its use over a period of time (L. Yang et al., 2010). An example of this is the "pay-per-part model" presented above, where *Trumpf* directly offers metal processing instead of selling machines (Schuh et al., 2021).

However, with PSS types outlining archetypal digital business models for manufacturers, organizations need to define which capabilities are needed to embrace the aspired PSS type successfully. Coming from predominantly hardware-centric business logic, the transformation toward a desired PSS target state often requires manufacturers to develop technical capabilities (e.g., to achieve remote access to machines) and non-technical capabilities (e.g., to market and monetize the PSS offer) (Favoretto et al., 2022; Paschou et al., 2020). Using the PSS types of Tukker (2004), guidance is needed to pinpoint which capabilities are needed for each PSS type (Favoretto et al., 2022). Therefore, RA #3 develops a maturity model to support product manufacturers in transforming to a specific PSS type.

Although numerous maturity models in the context of PSS exist (e.g., Exner et al. (2018)), current research lacks in mapping established PSS types with the required socio-technical capabilities. This makes it challenging for manufacturers to determine the required capabilities for an aspired PSS type and map them to their current "status quo." Hence, the created PSS maturity model (PSSMM) in research article #3 bridges the gap between common PSS types and a comprehensive socio-technical perspective on required capabilities. The artifact was developed following the development procedure of Becker et al. (2009), including the design and evaluation of the maturity model. The PSS types of Tukker (2004) were used to structure the PSSMM and indicate the maturity levels in columns. As many incumbent manufacturers initially offer the "pure product" (first column), this was chosen as the initial maturity level. In contrast, the three main PSS types (i.e., *product-oriented*, *use-oriented*, and *result-oriented PSS)* represent the remaining maturity levels. The model's rows use the focus areas proposed by Cleven et al. (2014) to leverage a comprehensive, socio-technical perspective on required capabilities for dedicated PSS types: *strategy*, *culture*, *structure*, *practices*, and *IT*. The PSSMM is a continuous maturity model, and the intersection of rows and columns describes a typical proficiency of a capability required for a PSS type. In contrast to many other maturity models, for example, the servitization maturity model proposed by Adrodegari and Saccani (2020), the PSSMM does not imply that a higher degree of maturity is to be aspired to by any applying organization. Instead, the PSSMM offers a self-assessment tool that allows manufacturers to define an aspired PSS type beforehand and use the PSSMM to structure the transformation toward this aspired target state. The PSSM includes 20 capability dimensions in five focus areas (Figure 5), described in the following paragraph. First, the focus area *strategy* represents the extent to which a company focuses on enhancing its value generation with services (capability dimension "service focus"). In addition, customer centricity is required for the co-creation of

service value with the customer ("customer involvement") (Exner et al., 2018). To be successful in the PSS transformation, management must devote significant resources to managing the shift ("management commitment to PSS") (Oliveira et al., 2018). Second, the focus area *culture* captures capabilities for efficient and effective collaboration ("internal collaboration") and guarantees commitment to the PSS vision of the organization ("employee commitment to PSS") (Waschull et al., 2020). Lastly, the area captures capabilities to enable the development of necessary soft and hard skills ("skills training") (Lund & Karlsen, 2020). Moving to the focus area *structure*, modifications to the marketing and value delivery are needed ("sales channels") (Kiel et al., 2017). As PSS focus on customer utility and digital interaction, capabilities that allow partners' integration into the design of value propositions are becoming increasingly important ("partner integration") (Benitez et al., 2020). Finally, the capability dimension of "capital management" refers to a shift in cash flow from one-time product purchases to ongoing service payments (Zhang & Banerji, 2017). Next, the focus area *structure* includes the capabilities needed to change existing routines and processes. With mature PSS focusing on proactive services (e.g., predictive maintenance), the first capability dimension, "customer interaction and service initiative," refers to shaping customer interaction and defining the service initiative (Brambila-Macias et al., 2018). The second capability dimension is concerned with the design of new or improved PSS, emphasizing methods and tools ("PSS design methods and tools") (Weking et al., 2020). As mature PSS rely on a defined availability or result for customers, "product performance measurement" becomes increasingly important for providing and pricing services (Kamal et al., 2020). In line with this capability, PSS providers must develop "automated service provision," allowing continuous service availability (Müller et al., 2018). Additionally, PSS providers must develop "pricing mechanism" capabilities that rely on the defined availability (Porter & Heppelmann, 2014). Finally, manufacturers need to enhance their "life cycle management" capabilities for PSS, as in many PSS, the product needs to be maintained after the point of sales at customer sites (Fargnoli et al., 2018). As the last focus area, *IT* provides the foundation for creating and operating digitalized PSS. Its role determines whether IT supports the business or goes beyond by enabling the organization's strategic goals (L. Wessel et al., 2021). Second, "IT security and compliance" are essential capabilities for mature PSS, as with digitally connected products, the attack surface grows (Preuveneers et al., 2018). In addition, PSS providers must develop "connectivity and data access" capabilities to access and remote-control products at customer sites (Wagire et al., 2020). Additionally, to provide data-driven services (e.g., prediction of machine failure), manufacturers need to collect and analyze relevant data ("data collection" and "data analysis") (Frank et al., 2019).

Focus area	Capability dimension	Maturity level / PSS type			
		1. Pure product	2. Product-oriented PSS	3. Use-oriented PSS	4. Result-oriented PSS
Strategy	Service focus	Focus on the physical product; no additional services	Limited focus on PSS; product-related additional services like consulting, maintenance, or recycling	Focus on PSS; warranty of the availability of the physical product along with services	Focus on mature PSS as core BM; highly integrated product-service bundles to offer result as a service
	Customer involvement	No or little involvement in the design of the product	Growing participation in designing and evolving the product and additional services	Increasing cooperation with the customer and integration into PSS design processes	Partner-like collaboration and intense communication on PSS development
	Management commitment for PSS	No resource allocation for PSS development and implementation	Little effort to create additional services to the product; ad hoc resource allocation in organizational changes	Medium effort for creating well-functioning PSS; continuous resource allocation	Significant efforts to achieve a high-performance PSS; substantial and continuous resource allocation
Culture	Internal collaboration	Independent work or partly homogenous teams	Occasional work in interdisciplinary teams	Work in interdisciplinary teams	Team-oriented, cross-team, -domain, and -organizational work, continuous exchange with value-adding partners
	Employee commitment for PSS	Product-oriented way of thinking; working to develop and sell physical products	Product-oriented way of thinking; working to offer complementary services to the product	Thinking in terms of customer use; working to provide PSS solutions with a higher level of service integration	Thinking in terms of customer results; working to deliver the result as a service
	Skill training	No training or further education regarding PSS skills	Occasional training in terms of PSS development, training for product-related consultation	Selective training courses on specific topics for PSS development and implementation	Structured training courses on all relevant PSS topics such as development, implementation, sales, customer contact, leadership, and management
Structure	Sales channels	Traditional and web-based channels for product sales	Traditional and web-based channels for product and service sales	Traditional and web-based channels or products as a point of sale	Traditional and web-based channels and products as a point of sale that allow tracking results achieved
	Partner integration	Only suppliers as value-adding partners; clear organizational boundaries	Additional value-adding partners for service-creation and initial involvement of and cooperation with the customer as a partner	Blurred boundaries between company, suppliers, and partners involved in service-creation; close cooperation with customer as a partner	Strong collaboration and integration of value-adding partners and customers for PSS co-creation; company is deeply integrated into customers' processes and BM
	Capital management	Bearing all costs until the point of sale; management of one-time payments for each product sale	Bearing all costs until the point of sale; management of one-time payment for the product and demand-driven service provision income	Bearing of production and development costs for products and services until a predefined point of time; continuous payments for use	Bearing all the costs for PSS until the end-of-life cycle; continuous and success-related payments for the operation of PSS
Practices	Customer interaction and service initiative	Interaction focuses on product purchase and emerging operation problems; customers are responsible for operations	The customer drives interaction; interactions are predefined in the service contract; mostly topic-driven services related to maintenance	PSS provider initiates services and is responsible for ensuring perpetual availability; planned interactions	Proactive and automated service interaction; connected through predefined touchpoints and processes; result as continuously monitored parameter for service initiative
	PSS design methods and tools	No approach for service or PSS development	Standard (management) approaches for product development; partial use of PSS methods and tools	Selected approaches and formalized development processes for PSS; appropriate tools for development and implementation	Company-specific and individualized PSS approaches plus fast development cycles and prototyping; continuous improvement and use of methods
	Product performance measurement	No need for measuring product performance; measuring product quality by internal tests only	No need to measure product performance but occasional insights through maintenance services; measuring product quality to provide advice and guidance to customers	Measurement of product performance and use to guarantee and optimize product availability	Well-defined measures and feedback loops are used for payments, maintenance, and new service development
	Automated service provision	No service provision	Almost no automation; rule-based, or instinct-driven service provision	Partly automated or modularized services are provided	Most services with the customer or value-creation partners are automated and/or modularized; optimization towards minimizing the human interaction in the service process
	Pricing mechanism	Fixed one-time payment (pay for the product)	One-time payment for the product and situational service fees (pay for the product or service order)	Continuous payments such as leasing, renting, or sharing (pay on availability)	Customer-specific, result-based payments based on service level agreement (pay on production)
	Life cycle management	Development, production, sale, and shipment; no responsibility for the operation	Development, production, sale, and shipment; no responsibility for operation but a reactive provision of services	Development, production, sale, shipment, maintenance, and usage phase; responsible for guaranteeing the usability of the product	Managing everything until the end of the product life cycle; responsible for delivering results and productivity
IT	Role of IT	IT plays a supporting role; intra-organizational focus	Supporting function, partly as the driver of value creation and change; intra-organizational focus	IT as an enabler and driver of value creation and change; enabler of product availability; inter-organizational focus	IT as an enabler and driver of value creation and change; enabler of enhanced product-performance, inter-organizational focus
	IT security and compliance	Security of highly critical assets; isolated IT security activities	Protection of highly critical assets and, initially, external processes	Intra- and inter-organisational IT security activities	Intra- and inter-organisational IT security activities; security by design in product and service development process
	Connectivity and data access	No access to the product after the point of sale	Indirect, situational data access to customers; possible manual data exchange	Frequent data exchange with OEM; mainly reading rights	Continuous data exchange; full access to the product
	Data collection	No collection of customer's product data	Reactive and manual collection of data; no defined data collection strategy	Partly automated collection of data; high-level requirements of the data that needs to be stored	Highly automated collection of data; specific requirements for data that requires storage regarding volume, velocity, and variety
	Data analysis	No analysis of product use or descriptive analysis of internal product testing	Descriptive and diagnostic analysis of product data; initially for service provision	Diagnostic and predictive analysis of product data; focus on keeping the promise of availability	Predictive and prescriptive analysis; focus on result optimization

Figure 5. The Product-service Systems Maturity Model (PSSMM)

To evaluate the PSSMM, a twofold evaluation strategy was used: First, using an academic focus group (Tremblay et al., 2010) and second, using a case study demonstration at *VacuumCo*, a manufacturer of vacuum pumps (Yin, 1992). In the case study demonstration, a total of three workshops with the *VacuumCo* team responsible for PSS and 14 expert interviews were conducted to determine the current status quo of the company and the target state of the PSS transformation based on the PSSMM (Schultze & Avital, 2011). The application of the model indicated that the manufacturer currently holds the typical capabilities of a product-oriented PSS provider. As a target state, no distinct positioning of the company was identified, which ranged between "*use-oriented*" and "*result-oriented.*" In further investigation, it became clear that the target state depended on which customer segment of *VacuumCo* was considered by the respective experts. Overall, the application of the PSSMM helped *VacuumCo* better understand its status quo and target state and identify areas where its capabilities were particularly immature. This model application also provided an impetus for further research: analyzing multiple target state PSS transformations for different customer segments in one company may enable a more nuanced understanding of PSS transformation.

In sum, research article #3 and the developed PSSMM combine established PSS types and a socio-technical perspective of required capabilities underpinning the transdisciplinary character of PSS. A case study demonstration reveals that the PSSMM offers an appropriate tool for manufacturers to capture their current and intended target state.

To conclude section II.1., the three research articles #1, #2, and #3 contribute to the understanding of *business challenges* in the digital transformation of manufacturing. More precisely, the works offer guidance on *how to structure the transformative endeavor* and *identify the required capabilities* needed for digital business models in manufacturing.

2 Technology Challenges

While digital transformation is primarily associated with positive effects, such as new digital business models, it also entails, among other things, *technology challenges,* such as IT security (Abolhassan, 2017; Vial, 2019). With the pervasive adoption of digital technologies, the attack surface of organizations is constantly growing and is accelerated by digitalization (Mendhurwar & Mishra, 2021). The issue is additionally fueled by cyber threat actors steadily becoming more professional (Cui et al., 2022). Consequently, around two-thirds of companies are affected by cyberattacks yearly, some even several times (Barreuther et al., 2022). Thus, IT security is becoming increasingly important (Ahmad et al., 2021; Thangavelu et al., 2021). In

organizations, IT security aims to ensure three main principles: *confidentiality*, *integrity*, and *availability* (Saltzer & Schroeder, 1975); this is often dubbed the "*CIA-triad*" (e.g., Bitzer et al. (2021), Parekh et al. (2018)). *Confidentiality* aims to prevent unauthorized information disclosure. *Integrity* strives to prevent the unauthorized modification of information. *Availability* refers to systems and information that are accessible and usable (Samonas & Coss, 2014). To ensure IT security and compliance with the CIA-triad, organizations enact measures that cover socio-technical aspects, including technologies, processes, and practices (Craigen et al., 2014; Malatji et al., 2020). The vulnerability of digital services in the manufacturing sector was demonstrated by a hack attack in 2022 that disabled around 5.800 wind turbines made by the German manufacturer *Enercon*. The manufacturer used *Viasat* satellite modems for remote maintenance services on several turbines in the field. In the course of a hacker attack, the *Viasat* system failed, and the turbines became uncontrollable and had to be powered down (Boschetti et al., 2022).

Organizations can mitigate security incidents by taking *proactive and reactive measures* (Benaroch, 2018). In *proactive measures*, organizations strive to enhance a system's properties to dampen the likelihood or impact of an incident (Thompson, 2018). For instance, when using multiple-factor authentication or systems with inherent integrity properties, such as blockchain (Rieger et al., 2019). A key challenge here is that IT security must be considered as early and as continuously as possible in digitalization initiatives, for instance, product development projects (Payette et al., 2015). Although research indicates that IT security measures can be an attractive investment option to ensure competitive advantage (Cardholm, 2016), in practice, they are often considered a restraint in digitalization projects (Grahn et al., 2021). Especially in initiatives with tight budgets, security measures might consume scarce resources and time, exacerbating the iron triangle's trade-off between time, cost, and quality (Atkinson, 1999; Lech, 2013). For this reason, organizations must decide for every digitalization project whether putting effort into IT security measures is feasible and beneficial. In this way, it can be considered whether putting effort into IT security will hinder the progress of the digitalization project (e.g., by increasing time-to-market) (Payette et al., 2015; Pinto & Prescott, 1988). Therefore, to leverage the potential of *proactive measures* for IT security, management is faced with the issue of defining an adequate role of IT security for each digitalization initiative of the company.

Research article #4 addresses this issue by introducing a tool to strategically consider IT security in digitalization projects using a DSR approach (Gregor & Hevner, 2013; Hevner et

al., 2004). More precisely, the paper relies on the four-phase DSR evaluation patterns (i.e., Eval 1-4) of Sonnenberg and vom Brocke (2012). Initially, this paper's problem-to-solve was defined as a guide in defining the role of IT security in digitalization projects aligned with relevant IT security drivers. Next, the research gap is justified (Eval 1) by providing a brief literature review to evaluate its theoretical importance and novelty. Thereby, it was found that existing literature introduces different approaches to align IT security with business needs (S. P.-J. Wu et al., 2015). While some papers consistently prioritize IT security and warn of harmful effects (Angst et al., 2017), others also weight the "slowing down" of digitalization through additional resource expenditure (Grahn et al., 2021). A third approach is the continuous integration of IT security into digitalization projects to drive both domains forward coherently (Payette et al., 2015). Finally, by drawing on insights into the decision-making processes for IT security investments (Dor & Elovici, 2016; Heidt et al., 2019b), the paper conceptualizes the different approaches to integrating IT security as *alignment paths*. The alignment path of *security first* (SF) describes the prioritization of IT security. Second, *security by design* (SD) refers to progress in both domains under the maxim of continuous alignment. Third, *security pragmatism* (SP) refers to the postponement or de-prioritization of IT security. While these strategic options can be derived from the existing literature, practice lacks a tool to support one of the three options based on relevant drivers.

Therefore, in line with existing research on IT security decision processes (Heidt et al., 2019a; Heidt et al., 2019b), several internal and external drivers impact the choice of these strategic alignment paths from an organizational and project domain were identified. To develop an applicable artifact that allows high applicability in practice, general design criteria were evaluated (e.g., the level of detail and applicability) by conducting an interview study with 14 industry experts from eleven organizations of different industries (Eisenhardt, 1989) (Eval 2). Next, the artifact was constructed in four major iterations. Finally, within the construction process, the artifact was refined using the feedback of twenty industry experts and scientists (Eval 3).

The final artifact maps the drivers from an organization and project domain to the alignment paths for IT security (SF, SD, and SP) (Figure 6). The drivers are categorized into "internal governance" (e.g., "To what extent does your organization strive to avoid technical debt?"), "industry standards" (e.g., "Is there a high level of established industry-wide IT security standards independent of mandatory legal regulations?"), "market & competition" (e.g., "To what extent is 'good' IT security presupposed or expected by the project's customers?"), and

"technology" (e.g., "To what extent did IT security incidents reveal your organization's vulnerabilities or attack vectors during the last two years?"). The artifact assigned each driver a fit to the identified alignment paths SF, SD, and SP based on literature and expert knowledge derived from Eval 2. This fit is indicated by a five-staged ordinal scale (–, -, 0, +, ++). While '0' indicates a non-existing dependency, '+' and '++' indicates that a driver supports the specific strategic alignment path. Consequently, '-' and '–' indicates that the driver has counterproductive effects on the specific alignment path. For instance, high regulatory standards do not fit SP since SP fosters a stronger focus on digitalization while focusing less on IT security. To focus on the organization's individual needs and to support the operational use of the artifact, each driver is weighted in terms of its relevance using a five-staged ordinal scale (i.e., none, low, medium, high, and obligatory). Thereby, "none" indicates that the driver is irrelevant to an organization. For instance, "none" doesn't meet the requirements of regulated industries with regulatory industry standards. "Obligatory" indicates that the corresponding driver is essential for the organization. Last, an exemplary instantiation was conducted using two real-world cases to demonstrate the artifact's usability and proof of its usefulness (Eval 4).

By consolidating this knowledge into an applicable artifact, this research article helps explain organizational action patterns. Moreover, it provides a managerial tool to evaluate and decide on appropriate IT security for digitalization projects. The artifact can support managers in two ways: First, managers can use it to identify a suitable *alignment path* for their digitalization project. Organizations must go through each driver and fill in their specific relevance weight to apply the artifact in this way. Then, organizations should carefully consider the drivers that were considered obligatory. According to the drivers' fit, the organizations should focus on SD or even SF if the obligatory weighted drivers fit with these strategic alignments. Organizations can look at the less weighted drivers to clarify their findings in close decisions between two strategic alignments. Second, organizations that want to follow a specific strategic alignment, for instance, a management philosophy, may start with the drivers' alignment. They may use the provided drivers matching a strategic alignment path to deriving requirements. In this case, the artifact primarily supports managers in convincing other stakeholders within the organization to undertake specific actions by explicitly illustrating relevant drivers.

Domain	Focus Area	No.	Driver	Driver's Relevance	Fit to Alignment Path		
					SF	SD	SP
Organization	Internal Governance	1	To what extent does your organization have a high security awareness and emphasis on IT security in early phases of IT project management?	To be evaluated by applying organization	++	++	-
		2	To what extent does your organization strive to avoid technical debt?		--	++	--
	Industry Standards	3	How strong or critical is your organizations interconnectedness with other organizations (focusing on suppliers (B2B))?		+	++	-
		4	How strong or critical is your organizations interconnectedness with other organizations (focusing on customers (B2B))?		+	++	-
Project		5	Is there a high level of established industry-wide IT security standards independent of mandatory legal regulations?		++	+	-
		6	Is there a high level of established IT security standards at your project's customer(s) independent of mandatory legal regulations?		++	+	-
		7	How strongly is the particular field (scope of the project) legally regulated in terms of IT security?		++	+	--
		8	How strongly is the the operational application at the customer (result of the project) legally regulated in terms of IT security?		++	+	--
	Market & Competition	9	To what extent is 'good' IT security presupposed or expected by the projcet's customers?		++	++	-
		10	To what extent does 'good' IT security within the projects offer you a possible access to new/future markets or customers?		+	0	-
		11	To what extent does 'good' IT security within the projects offer you direct competitive advantages?		++	++	-
		12	How vulnerable is your competitive advantage to IT security incidents?		++	+	-
		13	To what extent does your market position create higher pressure to improve IT security than digitalization?		++	+	--
		14	To what extent do first-mover advantages of innovations outweigh IT security requirements?		--	-	++
	Technology	15	To what extend did IT security incidents revealed your organization's vulnerabilities or attack vectors during the last two years?		++	+	--
		16	How large is the utilization of technologies that are secure by their inherent properties in the project?		++	++	-

Figure 6. Framework to Define a Strategic Role of IT Security in Digitalization Projects

In sum, research article # 4 encourages managers to proactively consider IT security measures while conducting digitalization projects that enhance digital maturity. Furthermore, especially with the path of SD, the paper strives to offer a perspective on how to design-in security in digital solutions.

However, even companies that massively invest in proactive IT security measures fall victim to security incidents (Hiscox, 2021). Furthermore, since attack vectors and tactics constantly evolve, incidents cannot be prevented completely (Kuypers et al., 2016; Lallie et al., 2021). Accordingly, the mitigation of these incidents plays a decisive role in reducing the extent of damage and restoring the operability of systems as quickly as possible (Ahmad et al., 2021). Consequently, organizations need to establish *reactive measures* that help to recover after being affected by IT security incidents.

Therefore, effective *Incident Response Management (IRM)* has been established as an effective tool for reactive IT security (He et al., 2022; van der Kleij et al., 2022). IRM aims to maintain the continuity of business processes, reduce the impact of security incidents, and respond to security incidents effectively (Ruefle et al., 2014). Organizations must enhance their efficiency and effectiveness in incident preparation, incident detection, incident remediation, and post-incident activities (Ab Rahman & Choo, 2015). Timely recovery from a security incident is essential, especially in highly networked production environments with high losses at production shutdown. In May 2022, for instance, the tractor manufacturer *AGCO/Fendt* had to shut down an entire German production site for ten days after a ransomware attack until the systems were restored (AGCO, 2022). According to a McKinsey report reducing the mean time to resolve (MTTR) significantly contributes to a company's resilience (Agarwal et al., 2020). Thus, during manufacturers' digital transformation, the continuous development of effective IRM capabilities is a crucial challenge. However, research still lacks a practice-grounded and socio-technical conceptualization of those capabilities and their development. To tackle this issue, the central artifact of research article #5 is an IRM maturity model (IRM3) closely aligned with practical requirements. The development follows a research approach composed of both the eight-phase development process according to Becker et al. (2009) and the evaluation patterns according to Sonnenberg and vom Brocke (2012) (i.e., Eval 1-4).

First, five expert interviews were conducted to derive the need for the IRM3 and elicit three design requirements: First, applicability to organizations with immature IRM. Second, consideration of the social-technical perspective. And third, practice-grounded evaluation. Next, the research gap was justified by screening existing models based on recommendations of practitioners during the interviews and a literature search (Eval 1). A structured literature review and expert interview revealed that the existing models (e.g., the Security Incident Management Maturity Model 'SIM3' of Stikvoort (2019)) could not fulfill all three outlined requirements. Hence, building on and enhancing existing works, a new model was developed (Becker et al., 2009). The developed IRM3 possesses, like the SIM3 (Stikvoort, 2019), four focus areas (i.e., *organization*, *human*, *tools*, and *processes*) and possesses in total 29 capability dimensions (Figure 7). As a focus area maturity model, the IRM3 does not use uniform and aligned maturity levels based on columns but measures the maturity for each capability dimension in each line (Lasrado et al., 2015). To indicate that more mature capabilities build on their predecessors and complement these, a plus sign "+" in front of some capabilities was added. At the end of the development process, the IRM3's design was evaluated regarding

fidelity with the real-world phenomena, completeness, and internal consistency (Eval 2) (Sonnenberg & vom Brocke, 2012) using an academic focus group (Tremblay et al., 2010). The focus area o*rganization* contains seven dimensions describing the pre-defined interaction of humans, resources, infrastructures, and processes (e.g., "management support," "service description," or "responsibility"). It is about specific and strategic goals related to IRM. It includes fundamental principles and organizational measures to structure and implement IRM. The realization of these organizational aspects requires the involvement of decision-makers. Second, the focus area *human* consists of six dimensions that describe how employees work together to realize organizational goals (e.g., "security awareness," "communication culture"). This focus area considers the collective values and behaviors of individuals or teams and, thus, the human factor. Consequently, the area covers dimensions that affect or require employee participation to respond appropriately to incidents. The focus area *tools* contains eight dimensions and concentrates on the applications, programs, services, and other parts of equipment to conduct incident response (e.g., "IT resources," "work equipment"). These tools enable the company to achieve the goals described in the focus area organization. With their help, an organization can improve its IRM regarding time, granularity, or quality. Last, the focus area *processes* consists of eight dimensions and defines IRM procedures carried out by tools or humans (e.g., "incident prevention," "incident detection"). The procedures support the incident management or services, which are part of the incident response process. To increase the effectiveness of IRM, procedures need to be repeatable, measurable, adaptable, and documented.

Focus Area	Capability Dimension	Maturity Capabilities				
Organization	Management Support	De-prioritization & Negligence	Management Awareness	+ Active Management Support	+ Sufficient Resources	
	Service Description	No Service Description	Implicit Service Description	Explicit Service Description	+ Regular Reviewing of Service Description	
	Responsibility	Responsibility Unclear	Clearly Assigned Responsibilities		+ Regular Review & Adjustment of Responsibilities	
	Emergency Availability	Undefined Contact Points	Defined Contact Points	+ Publicity of Contact Points	+ Ensured Reachability of Contact Points	
	Incident Classification	Ad-hoc & Intuitive Classification	Case-by-Case Classification	Developed Classification Scheme	+ Institutional Application of Classification Scheme	+ Permanent Improvement of Classification
	Security Policy	Focus on Damage Avoidance	+ Adherence to Legal Guidelines	+ Defined Internal Guidelines	+ Adaption towards Internal Guidelines	+ Consideration of Changing Requirements
	External Collaboration	No Collaboration	Case-by-Case Collaboration	+ Involvement of External Service Providers	+ Acquisition of Cyber Insurance	
Human	Security Awareness	No IT Security Awareness	Awareness of Existence	+ Awareness of Importance	+ Training and Awareness Raising	
	Communication Culture	Reactive Communication	Proactive Communication	+ Know-how-Transfer	+ Competence Sharing	
	In-House Cooperation	Occasional Interaction	Proactive Interaction & Teamwork	+ Cooperation across Departments		
	Personnel Resilience	Insufficient IT Workforce	Insufficient Security Workforce	Dedicated Security Workforce	+ Absence-resilient Workforce	
	Personnel Characteristics	Pro-forma Assignment in IT	Dedicated Competence Profile	+ Skilled & Trained Personnel	+ Experienced Personnel	
	Training Opportunities	No Training Opportunities	Demand-oriented Training	Training for Person in Charge	+ Training for IT Members	+ Company-Wide Training
Tools	IT Resources	No IT Resource & Asset Management	Regular Inspection of Resources	+ Classification of Resources	+ Documentation & Description of Critical Resources	
	Work Equipment (Systems)	Vulnerable IT Systems	Protected IT Systems	+ Implementation of Redundancies	+ Highly Resilient and Scalable Systems	
	Work Equipment (Personnel)	Vulnerable Work Equipment	Protected Work Equipment	+ Equipment for Replacement	+ Seamless Recovery	
	Prevention Toolset	Unestablished Prevention Tools	Integrated Antivirus Programs & Firewalls	+ Access Control & Management	+ Tools for Patch Management	
	Detection Toolset	No Detection Tools	Unestablished Detection Tools	Tools for NetFlow & Traffic Analysis	+ Tools for Endpoint Detection and Response	
	Tracking System	No Tracking of Incidents	Manual Tracking of Incidents	Incident Tracking System		
	Resolution Toolset	Unestablished Resolution Tools	Integrated Logging Tools	+ Tools for Configuration & Backup Management	+ Established Forensic Tools	+ Integration of Sandboxing Tools
Processes	Documentation System	Unsystematic Collection of Data & Knowledge	System for Knowledge Management	+ Encouragement of Documentation	+ Time for Documentation & Reflection	
	Incident Prevention	No Prevention Measures	+ Defined Prevention Measures	+ Established Prevention Measures	+ Permanently Reviewed Prevention Measures	
	Incident Detection	Unsystematic Detection Measures	+ Defined Detection Measures	+ Established Detection Measures	+ Permanently Reviewed Detection Measures	
	Escalation	Unsystematic Escalation	Implicit Escalation	Systematic Escalation	+ Defined Escalation Criteria	+ Continuous Process Improvement & Learning
	Incident Resolution	Unsystematic Resolution Measures	Defined Resolution Measures	+ Established Resolution Measures	+ IT Business Continuity Management	+ Permanently Reviewed Resolution Measures
	Incident Reflection	No Reflection of Incidents	Case-by-Case Learning	+ Change Management Process	Permanent Improvement	
	Audit	No Revision Measures	Self-Assessment & Learning	+ Integrated Audit Management	+ Internal & External Assessment	+ Certification
	Knowledge Acquisition	Implicit Knowledge Acquisition	Systematic Research		+ Exchange & External Networking	
	External Communication	Negligence for Security	Unsystematic PR Activity	Market Observation	+ Systematic & Proactive PR Activity	

Figure 7. The Incident Response Management Maturity Model (IRM3)

After the development process, the IRM3 was transferred into an online survey tool to allow *ease of use* and *feasibility* for its target group (i.e., practitioners in the IT security field) (Eval 3). Finally, f a naturalistic evaluation and to assess its *practical value* in applicability, effectiveness, and generality, the IRM3 was applied in a case study demonstration at seven organizations (Yin, 1992) (Eval 4).

Aside from the IRM3's prescriptive value confirmed throughout the demonstration, it provided descriptive insights into the assessed organization's IRM capability maturity (Gregor & Hevner, 2013). It appeared that IRM maturity is affected by drivers and challenges that can mainly be traced back to the contextual factors of an organization. Based on the case study demonstration, three main classes of maturity and contextual factors were found (i.e., *Classes A-C*): First, *Class A* organizations had mature IRM capabilities rooted in certification and auditing as a contextual factor. Second, *Class B* organizations possessed average IRM capabilities driven by customer requirements, cyber insurance, or a business model focusing on IT or security. Third, *Class C* includes organizations with immature IRM. These companies use IT only as a supporting component and are not driven by customer requirements due to their industrial sector.

To conclude section II.2, research article #5 addresses the need for practical guidance on reactive measures in IT security by examining IRM capabilities in a holistic, socio-technical perspective across 29 capability dimensions. In sum, the model offers prescriptive knowledge on relevant IRM capabilities but can also be used as a status quo assessment tool for descriptive purposes.

III Summary and Future Research

1 Summary

In the wake of continuously increasing global competitive pressure, the market environment in the manufacturing sector has undergone major upheaval (Björkdahl, 2020). To withstand this market pressure, many manufacturers seek to leverage digital technologies to offer new digital business models associated with high margins and potent competitive advantages. Driven by these opportunities and as a strategic response to the new market conditions and technological affordances, many manufacturers are embarking on their digital transformation (Vial, 2019). However, pursuing digital transformation and enabling digital business models in manufacturing bears *business and technology challenges*. These challenges are most pressing for incumbent manufacturers whose established market position was carved out decades ago and primarily rooted in the engineering, production, and sales of high-quality equipment but not software and digital services.

On the one hand, these companies face *business challenges* when endeavoring digital transformation. First, in the form of lacking guidance on the structured *exploration of digital business models* that allows the company to leave well-trodden paths of hardware-centric business logic and consequently identify a strategic polestar of future digital business models. Second, by struggling to *identify and develop the capabilities* required to embrace their digital business vision.

On the other hand, as digital business models require the broad adoption of digital technologies, this also gives rise to *technology challenges*. These challenges become evident, for instance, in the field of *IT security*, as threats in this area will increase because of intensifying digital business and intra- and inter-organizational connectivity. To mitigate those emerging security threats, *proactive and reactive IT security measures* must be considered in the wake of digital transformation.

Against this backdrop, the phenomenon of digital transformation yields considerable research potential for the information systems domain as it stimulates the development of artifacts that can help to tackle dedicated challenges (Gregor & Hevner, 2013; March & Storey, 2008). This dissertation and the research contributions presented therein utilize the DSR paradigm to contribute to the prescriptive knowledge on resolving both business and technology challenges associated with digital transformation. Additionally, by applying these artifacts, for instance,

as analytical lenses on capability development, descriptive knowledge on how manufacturers manage their transformation is being generated (Favoretto et al., 2022; Verhoef et al., 2021).

Regarding the *business challenges,* section II.1 sheds light on *how to explore digital business models* and *what capabilities* need to be developed to embrace these business models in manufacturing.

Research article #1 underpins the relevance of this issue by outlining the case of *WashTec*, an incumbent manufacturer of car wash systems. *WashTec* strived to explore new digital business models to enhance its market position. However, existing methodological approaches for exploration did not fulfill the requirements set by *WashTec'*s management rooted in the desire to build on existing resources and strengths and develop monetization metrics for digital business models. Thus, this study uses Action Design Research to develop a guiding structure (Mullarkey & Hevner, 2019). This article's artifact is an approach to the structured exploration of digital business models in incumbent firms. With its four main phases (i.e., *Activation, Inspiration*, *Evaluation,* and *Monetization*), this approach is rooted in established Design Thinking literature (Brown, 2008; Naiman, 2019). However, based on established companies' requirements, the approach extends existing Design Thinking patterns. First, it considers an upstream *Activation* phase that assesses strategic exploration options based on an incumbent's established resources and products. Second, the approach includes a dedicated *Monetization* phase that focuses on developing monetization metrics for the explored digital business models. The work's contribution is twofold, as it, first, offers descriptive knowledge about digital transformation at the case company. It highlights the complexity of the socio-technical transformation required to move from hardware-centric organizational logic to a new business model. Second, it provides prescriptive knowledge that offers guidance for the defined real-world problem (i.e., structuring the exploration activities of manufacturers) and lessons learned from *WashTec*'s case that could make the application at other manufacturers even more effective (Gregor & Hevner, 2013).

Research articles #2 and #3 shed light on the *capability development* required for manufacturers' digital business models. Both research articles use archetypal digital business model designs to examine required capabilities comprehensively. While research article #2 focuses on business models whose value proposition is fulfilled by data-driven services and thus does not presuppose a specific bundle between product and digital services, research article #3 draws on archetypal PSS and thus includes bundling of hardware and services. Both use

existing, descriptive research findings (i.e., about archetypal business models) to generate prescriptive knowledge describing how these archetypal business models can be achieved. To fulfill this goal, both articles develop continuous maturity models as core artifacts drawing on a socio-technical lens to identify the technical and non-technical capabilities necessary for archetypal business models.

Research article #2 builds on Hunke et al. (2021) archetypal data-driven business models (i.e., *data provider, insight provider, recommendation provider,* and *digital solution provider*) and identifies relevant capabilities along Urbach and Röglinger's (2019) five-layered enterprise architecture model. Along with the development of the model, the existing literature is reviewed, structured, and aggregated in the maturity model. Finally, the model is applied to two manufacturers to evaluate the model properly following Becker et al. (2009). During the application, the model serves as an analytical lens that offers insights into the manufacturer's digital transformation. This offers intriguing avenues for further research, which can be more empirical, to understand better the transformation processes toward digital business models (Favoretto et al., 2022).

Research article #3 focuses on archetypal PSS business models enabled by digital technologies. The paper builds on the established PSS business model typology of Tukker (2004). This typology allows the classification of PSS according to their core logic of value creation and value proposition to customers (i.e., *product-oriented, use-oriented, and result-oriented* PSS). Research article #3 leverages this systematization to represent target states of manufacturers' digital transformation. The article thereby answers the research question of which socio-technical capabilities manufacturers need to offer the respective PSS archetypes. Like research article #2, the research design is based on developing a maturity model as the central artifact. To this end, by combining the PSS archetypes and a socio-technical perspective on the organization, a continuous maturity model is developed to assist manufacturers in identifying the status quo of capability development and deriving a target state of transformation. The model is evaluated in a case study demonstration at *VacuumCo*, an incumbent manufacturer of vacuum pumps. The central artifact contributes mainly to prescriptive knowledge, while the insights of the case study demonstration contribute to the general understanding of digital transformation in manufacturing.

Regarding *technology challenges*, section II.2 outlines how manufacturers can *proactively and reactively* enhance their mitigation of IT security threats. It is assumed that manufacturers are

increasingly adopting digital technologies to implement digital business models. Thus, the attack surface for IT security incidents increases. Research article #4 examines this issue from the perspective of digitalization projects, which are commonly used to drive the digital maturity of enterprises. Using theory on driving factors for IT security investments (Heidt et al., 2019a; Heidt et al., 2019b), this research article examines strategic roles that IT security can take in digitalization projects (i.e., *security first, security by design,* and *security pragmatism*). As a central artifact, a framework is developed that identifies established drivers for these strategic roles. In addition, the artifact was applied to two organizations, yielding insights into the strategic role of IT security in these organizations. Thus, this paper contributes to the area of prescriptive knowledge by directly mapping the drivers to the various strategic roles of IT security.

Despite proactive measures, IT security incidents cannot be prevented entirely due to a constantly expanding attack surface and the increasing number of hacker attacks. Against this background, research article #5 examines the risk perspective by considering IRM as the ability of organizations to regain business operations after suffering IT security incidents. The work analyzes what capabilities organizations need to establish effective IRM. For this purpose, a socio-technical maturity model is developed, which takes a comprehensive view of the organization and thus considers technical and non-technical aspects of IRM. The artifact is applied to seven different organizations to investigate their status quo and target state of incident response management capabilities. The contribution of the work lies especially in merging technical and non-technical capabilities for IRM and, thus, in prescriptive knowledge. At the same time, the results of the application of the artifact in the companies studied indicate a relatively low average maturity of incident response capabilities, thus emphasizing the need for action.

2 Future Research

As with any research endeavor, this dissertation and the associated findings are subject to limitations. While the individual research articles have already addressed their respective limitations (see Appendices V.3-V.7), this section focuses on an aggregated perspective of business and technology challenges in manufacturing. In addition, stimuli for future research in the field of digital transformation of manufacturers are to be provided.

First, in the area of *business challenges,* this work builds in particular on established archetypes of digital business models (e.g., Hunke et al. (2021), Tukker (2004)) and therefore uses a mainly

deductive approach (Bhattacherjee, 2012). While these archetypes serve as established structures, they bring some limitations. First, when considering different archetypal business models, it is not initially considered whether they are appropriate for the company in its context (i.e., regarding the size of the company or its industrial focus). This could be an impetus for future research to question the qualitative suitability of a certain archetype for the company and the associated context. Furthermore, archetypal business models are subject to a limitation in that they represent a simplified form of the complex reality. Although this makes it possible to identify a target business model, it also implies giving up the potential for innovation and individualization. As illustrated by Chiu et al. (2019), the multitude of existing classifications also points out individual weaknesses of the abstractions. Future research could therefore strive for inductive approaches to investigate meta-characteristics of digital business models that go beyond typologies (Bhattacherjee, 2012). A cross-sectional analysis of existing archetypes could identify overarching patterns and yield prescriptive knowledge (e.g., success factors, best practices) so that practical guidance based on them is not limited to the logic of specific typologies.

Second, limitations and resulting stimuli for future research can also be derived in the area of *technology challenges*, which addresses the topic of IT security in particular. This work examines *proactive and reactive measures* companies can use to enhance their IT security. However, this work, like many other studies in this domain, is limited because these two areas are not considered in an integrated way. Especially with the increasing networking of machines and systems, an integrated approach seems to be more viable. While manufacturers can continuously interact with their own IT infrastructure, networked production systems, and employees, this influence is limited to machines and systems operating at the customer's site. Manufacturers must, therefore, not only take responsibility for their assets and systems but also extend this responsibility to digitally networked products. For this, a combination of proactive and reactive measures can be adopted throughout the product development process: On the one hand, products should be designed proactively from the perspective of IT security to make them resilient to hacker attacks or misuse. On the other hand, it seems appropriate to implement reactive measures to ensure the ability to act in the event of an incident that affects the networked machine. Thus, impulses for future research arise that IT security must be integrated proactively and reactively during product development. For instance, the approaches described in this paper could be integrated into the product development process giving rise to "security by design"-approaches.

Thirdly, this work offers a hitherto rarely considered *integrated perspective* of *business and technology challenges* in the digital transformation of manufacturing. For this purpose, this dissertation provides research articles that address the respective issues of both challenges. While this perspective allows addressing both issues sequentially, this dissertation is limited in offering integrated tools. Future research could therefore leverage this combined perspective to explore the technological challenges associated with specific digital business models and the associated implications (e.g., expected risk). This might broaden manufacturing executives' decision-making basis to include the associated technology challenges when evaluating the opportunities of digital business models.

In sum, this work contributes to the existing knowledge of digital transformation in manufacturing by presenting artifacts and approaches that help tackle business and technology challenges in developing new digital business models. In doing so, I hope that this work will both provide practical guidance in the digital transformation of this relevant industry and inspire researchers to investigate this phenomenon in an integrated manner and from both a business and technology perspective.

IV References

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A Survey of Information Security Incident Handling in the Cloud. *Computers & Security*, *49*, 45–69. https://doi.org/10.1016/j.cose.2014.11.006

Abolhassan, F. (2017). Security: The Real Challenge for Digitalization. In F. Abolhassan (Ed.), *Management for Professionals. Cyber Security. Simply. Make it Happen: Leveraging Digitization Through IT Security* (pp. 1–11). Springer International Publishing. https://doi.org/10.1007/978-3-319-46529-6_1

Acar, O. A., Tarakci, M., & van Knippenberg, D. (2019). Creativity and Innovation Under Constraints: A Cross-Disciplinary Integrative Review. *Journal of Management*, *45*(1), 96–121. https://doi.org/10.1177/0149206318805832

Adrodegari, F [Federico], & Saccani, N [Nicola] (2020). A Maturity Model for the Servitization of Product-centric Companies. *Journal of Manufacturing Technology Management*, *31*(4), 775–797. https://doi.org/10.1108/JMTM-07-2019-0255

Agarwal, H., Agarwal, R., Kayyali, B., & Stephens, D. (2020, September 1). *Four Ways to Improve Technology Service Resiliency.* McKinsey. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/four-ways-to-improve-technology-service-resiliency

AGCO. (2022, May 16). *AGCO Provides Update on Recovery from Ransomware Cyber Attack: News Releases.* AGCO. https://news.agcocorp.com/news/agco-provides-update-on-recovery-from-ransomware-cyber-attack

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How Can Organizations Develop Situation Awareness for Incident Response: a Case Study of Management Practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, *41*(3), 893–916. https://doi.org/10.25300/MISQ/2017/41.3.10

Appelbaum, S. H. (1997). Socio-technical Systems Theory: an Intervention Strategy for Organizational Development. *Management Decision*, *35*(6), 452–463. https://doi.org/10.1108/00251749710173823

Atkinson, R. (1999). Project Management: Cost, Time and Quality, Two Best Guesses and a Phenomenon, its Time to Accept Other Success criteria. *International Journal of Project Management*, *17*(6), 337–342. https://doi.org/10.1016/S0263-7863(98)00069-6

Baines, T. S., Lightfoot, H. W., Evans, S [S.], Neely, A [A.], Greenough, R., Peppard, J., Roy, R., Shehab, E., Braganza, A., Tiwari, A., Alcock, J. R., Angus, J. P., Bastl, M., Cousens, A., Irving, P., Johnson, M., Kingston, J., Lockett, H., Martinez, V., . . . Wilson, H. (2007). State-of-the-art in Product-service Systems. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture*, *221*(10), 1543–1552. https://doi.org/10.1243/09544054JEM858

Baltuttis, D., Häckel, B., Jonas, C. M., Oberländer, A. M., Röglinger, M., & Seyfried, J. (2022). Conceptualizing and Assessing the Value of Internet of Things Solutions. *Journal of Business Research*, *140*, 245–263. https://doi.org/10.1016/j.jbusres.2021.10.063

Barreuther, P., Wanke, K., Cichon, F., Klüh, S., & Halusa, S. (2022, January 1). *Cyber-Security-Risk-Report 2021*. MHP Management- und IT Beratung GmbH. https://www.mhp.com/de/insights/was-wir-denken/cyber-security-risk-report/download#whitePaper-75

Baxter, G., & Sommerville, I. (2011). Socio-technical Systems: from Design Methods to Systems Engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Benaroch, M. (2018). Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision Making. *Information Systems Research*, *29*(2), 315–340. https://doi.org/10.1287/isre.2017.0714

Benitez, G. B., Ayala, N. F., & Frank, A. G. (2020). Industry 4.0 Innovation Ecosystems: an Evolutionary Perspective on Value Cocreation. *International Journal of Production Economics*, *228*, 107735. https://doi.org/10.1016/j.ijpe.2020.107735

Berg, A. (2022, August 31). *Wirtschaftsschutz 2022*. Berlin. Bitkom e.V. https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf

Berger, S., Bürger, O., & Röglinger, M. (2020). Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy. *Computers & Security*, *93*, 101790. https://doi.org/10.1016/j.cose.2020.101790

Berger, S., van Dun, C., & Häckel, B. (2022). IT Availability Risks in Smart Factory Networks – Analyzing the Effects of IT Threats on Production Processes Using Petri Nets. *Information Systems Frontiers.* Advance online publication. https://doi.org/10.1007/s10796-022-10243-y

Beverungen, D., Hess, T., Köster, A., & Lehrer, C. (2022). From Private Digital Platforms to Public Data Spaces: Implications for the Digital Transformation. *Electronic Markets*, *32*(2), 493–501. https://doi.org/10.1007/s12525-022-00553-z

Beverungen, D., Kundisch, D., & Wünderlich, N. (2021). Transforming into a Platform Provider: Strategic Options for Industrial Smart Service Providers. *Journal of Service Management*, *32*(4), 507–532. https://doi.org/10.1108/JOSM-03-2020-0066

Bhattacherjee, A. (2012). *Social Science Research: Pinciples, Methods and Practies* (2. ed.). Creative Commons Attribution 3.0 License.

Bitzer, M., Brinz, N., & Ollig, P. (2021). Disentangling the Concept of Information Security Properties: Enabling Effective Information Security Governance. *ECIS 2021 Research Papers*, *134*.

Björkdahl, J. (2020). Strategies for Digitalization in Manufacturing Firms. *California Management Review*, *62*(4), 17–36. https://doi.org/10.1177/0008125620920349

Bock, M., Wiener, M., Gronau, R., & Martin, A. (2019). Industry 4.0 Enabling Smart Air: Digital Transformation at KAESER COMPRESSORS: How Organizations Rethink Their Business for the Digital Age. In M. Röglinger & N. Urbach (Eds.), *Management for Professionals. Digitalization Cases: How Organizations Rethink Their Business*

for the Digital Age (1st ed., pp. 101–117). Springer International Publishing; Imprint: Springer. https://doi.org/10.1007/978-3-319-95273-4_6

Boehm, J., Lewis, C., Li, K., Wallance, D., & Dias, D. (2022, March 10). *Cybersecurity Trends: Looking Over the Horizon.* McKinsey. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Boschetti, N., Gordon, N. G., & Falco, G. (2022, October 24). *Space Cybersecurity Lessons Learned from the ViaSat Cyberattack*. AIAA Ascend 2022, Las Vegas. https://doi.org/10.2514/6.2022-4380

Böttcher, T. P., Weking, J., Hein, A., Böhm, M., & Krcmar, H. (2022). Pathways to Digital Business Bodels: the Connection of Sensing and Seizing in Business Model Innovation. *The Journal of Strategic Information Systems*, *31*(4), 101742. https://doi.org/10.1016/j.jsis.2022.101742

Brambila-Macias, S. A., Sakao, T., & Kowalkowski, C. (2018). Bridging the Gap between Engineering Design and Marketing: Insights for Research and Practice in product/service system design. *Design Science*, *4*, 1. https://doi.org/10.1017/dsj.2018.3

Brown, T. (2008). Design Thinking. *Harvard Business Review*, *86*(6), 84.

Cardholm, L. (2016). Demonstrating Business Value of Security Investments in the Age of Digitalization. *International Journal of Innovation in the Digital Economy*, *7*(3), 1–25. https://doi.org/10.4018/IJIDE.2016070101

Chiu, M.-C., Chu, C.-Y., & Kuo, T. C. (2019). Product Service System Transition Method: Building Firm's Core Competence of Enterprise. *International Journal of Production Research*, *57*(20), 6452–6472. https://doi.org/10.1080/00207543.2019.1566670

Cleven, A. K., Winter, R., Wortmann, F., & Mettler, T. (2014). Process Management in Hospitals: an Empirically Grounded Maturity Model. *Business Research*, *7*(2), 191–216. https://doi.org/10.1007/s40685-014-0012-x

Clune, S. J., & Lockrey, S. (2014). Developing Environmental Sustainability Strategies, the Double Diamond Method of LCA and Design Thinking: a Case Study from Aged Care. *Journal of Cleaner Production*, *85*, 67–82. https://doi.org/10.1016/j.jclepro.2014.02.003

Comuzzi, M., & Patel, A. (2016). How Organisations Leverage Big Data: a Maturity Model. *Industrial Management & Data Systems*, *116*(8), 1468–1492. https://doi.org/10.1108/IMDS-12-2015-0495

Cooper, R. G. (1990). Stage-gate Systems: A New Tool for Managing New Products. *Business Horizons*, *33*(3), 44–54. https://doi.org/10.1016/0007-6813(90)90040-I

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Cui, L., Cui, J., Hao, Z., Li, L., Ding, Z., & Liu, Y. (2022). An Empirical Study of Vulnerability Discovery Methods Over the Past Ten Years. *Computers & Security*, *120*, 102817. https://doi.org/10.1016/j.cose.2022.102817

Culot, G., Nassimbeni, G., Orzes, G., & Sartor, M. (2020). Behind the Definition of Industry 4.0: Analysis and Open Questions. *International Journal of Production Economics*, *226*, 107617. https://doi.org/10.1016/j.ijpe.2020.107617

Davenport, T. H., & Westerman, G. (2018). Why so Many High-profile Digital Transformations Fail. *Harvard Business Review*, *9*, 15.

de Boer, E., Fritzen, S., Khanam, R., & Lefort, F. (2020, April 10). *Preparing for the Next Normal via Digital Manufacturing's Scaling Potential*. https://www.mckinsey.de/capabilities/operations/our-insights/preparing-for-the-next-normal-via-digital-manufacturings-scaling-potential

Devaraj, S., & Kohli, R. (2003). Performance Impacts of Information Technology: Is Actual Usage the Missing Link? *Management Science*, *49*(3), 273–289. https://doi.org/10.1287/mnsc.49.3.273.12736

Dor, D., & Elovici, Y. (2016). A Model of the Information Security Investment Decision-making Process. *Computers & Security*, *63*, 1–13. https://doi.org/10.1016/j.cose.2016.09.006

Duraivelu, K. (2022). Digital Transformation in Manufacturing Industry – A Comprehensive Insight. *Materials Today: Proceedings.* Advance online publication. https://doi.org/10.1016/j.matpr.2022.07.409

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.5465/amr.1989.4308385

Exner, K., Balder, J., & Stark, R. (2018). A PSS Maturity Self-assessment Tool. *Procedia CIRP, 73*, 86–90.

Fargnoli, M., Costantino, F., Di Gravio, G., & Tronci, M. (2018). Product Service-systems Implementation: A Customized Framework to Enhance Sustainability and Customer Satisfaction. *Journal of Cleaner Production, 188*, 387–401. https://doi.org/10.1016/j.jclepro.2018.03.315

Favoretto, C., Mendes, G. H. d. S., Filho, M. G., Gouvea de Oliveira, M., & Ganga, G. M. D. (2022). Digital Transformation of Business Model in Manufacturing Companies: Challenges and Research Agenda. *Journal of Business & Industrial Marketing, 37*(4), 748–767. https://doi.org/10.1108/JBIM-10-2020-0477

Forth, P., de Laubier, R., Reichert, T., & Chakraborty, S. (2020, October 29). *Flipping the Odds of Digital Transformation Success.* Boston Consuling Group. https://www.bcg.com/publications/2020/increasing-odds-of-success-in-digital-transformation

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 Technologies: Implementation Patterns in Manufacturing Companies. *International Journal of Production Economics, 210*, 15–26. https://doi.org/10.1016/j.ijpe.2019.01.004

Gebauer, H., Paiola, M., Saccani, N [Nicola], & Rapaccini, M [Mario] (2021). Digital Servitization: Crossing the Perspectives of Digitization and Servitization. *Industrial Marketing Management, 93*, 382–388. https://doi.org/10.1016/j.indmarman.2020.05.011

Goldfarb, A., & Tucker, C. (2019). Digital Economics. *Journal of Economic Literature, 57*(1), 3–43. https://doi.org/10.1257/jel.20171452

Grahn, S., Granlund, A., & Lindhult, E. (2021). Barriers to Value Specification when Carrying out Digitalization Projects. *Technology Innovation Management Review, 11*(5). https://timreview.ca/article/1442

Gregor, S., & Hevner, A. R. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly, 37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A [Andy] (2016). Capturing Value from Big Data – a Taxonomy of Data-driven Business Models Used by Start-up Firms.

International Journal of Operations & Production Management, *36*(10), 1382–1406. https://doi.org/10.1108/IJOPM-02-2014-0098

Hasan, M. (2022, May 18). *State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally.* IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile Incident Response (AIR): Improving the Incident Response Process in Healthcare. *International Journal of Information Management*, *62*, 102435. https://doi.org/10.1016/j.ijinfomgt.2021.102435

Heidt, M., Gerlach, J., & Buxmann, P. (2019a). A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions. In T. Bui (Ed.), *Proceedings of the Annual Hawaii International Conference on System Sciences, Proceedings of the 52nd Hawaii International Conference on System Sciences.* Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2019.739

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019b). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Heinz, D., Benz, C., Bode, J., Hunke, F., & Satzger, G. (2022). Exploring the Potential of Smart Service Systems: A Multi-Actor View on Affordances and Their Actualization. *Journal of Service Management Research*, *6*(2), 132–146. https://doi.org/10.5771/2511-8676-2022-2-132

Herden, T. T. (2020). Explaining the Competitive Advantage Generated from Analytics with the Knowledge-based View: the Example of Logistics and Supply Chain Management. *Business Research*, *13*(1), 163–214. https://doi.org/10.1007/s40685-019-00104-x

Hernández, E., Senna, P., Silva, D., Rebelo, R., Barros, A. C., & Toscano, C. (2020). Implementing RAMI4.0 in Production - A Multi-case Study. In H. A. Almeida & J. C. Vasco (Eds.), *Lecture Notes in Mechanical Engineering. Progress in Digital and Physical Manufacturing* (pp. 49–56). Springer International Publishing. https://doi.org/10.1007/978-3-030-29041-2_6

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, Article Vol. 28 No. 1, 75–105.

Hiscox. (04/2021). *Hiscox Cyber Readiness Report 2021: Don't Let Cyber Be a Game of Chance* (No. 5). Hiscox Ltd. https://doi.org/10.1016/S1361-3723(21)00049-X

Hunke, F., Heinz, D., & Satzger, G. (2021). Creating Customer Value from Data: Foundations and Archetypes of Analytics-based Services. *Electronic Markets.* Advance online publication. https://doi.org/10.1007/s12525-021-00506-y

Ibarra, D., Ganzarain, J., & Igartua, J. I. (2018). Business Model Innovation Through Industry 4.0: A Review. *Procedia Manufacturing*, *22*, 4–10. https://doi.org/10.1016/j.promfg.2018.03.002

Jovanovic, M., Sjödin, D., & Parida, V. (2022). Co-evolution of Platform Architecture, Platform Services, and Platform Governance: Expanding the Platform Value of Industrial Digital Platforms. *Technovation*, *118*, 102218. https://doi.org/10.1016/j.technovation.2020.102218

Kaeser Kompressoren. (2022, November 18). *SIGMA AIR UTILITY: Just Buy the Air You Need*. https://www.kaeser.com/int-en/download.ashx?id=tcm:17-3180

Kagermann, H., Wahlster, W., & Helbig, J. (2013, April 1). *Recommendations for Implementing the Strategic Initiative Industrie 4.0* (No. 0). https://www.acatech.de/projekt/industrie-4-0/

Kamal, M. M., Sivarajah, U., Bigdeli, A. Z., Missi, F., & Koliousis, Y. (2020). Servitization Implementation in the Manufacturing Organisations: Classification of Strategies, Definitions, Benefits and Challenges. *International Journal of Information Management*, *55*, 102206. https://doi.org/10.1016/j.ijinfomgt.2020.102206

Kappelman, L., L. Johnson, V., Maurer, C., Guerra, K., McLean, E., Torres, R., Snyder, M., & Kim, K. (2020). The 2019 SIM IT Issues and Trends Study. *MIS Quarterly Executive*, *19*(1), 69–104. https://doi.org/10.17705/2msqe.00026

Kerpedzhiev, G. D., König, U. M., Röglinger, M., & Rosemann, M. (2021). An Exploration into Future Business Process Management Capabilities in View of Digitalization. *Business & Information Systems Engineering*, *63*(2), 83–96. https://doi.org/10.1007/s12599-020-00637-0

Kiel, D., Arnold, C., & Voigt, K.-I. (2017). The Influence of the Industrial Internet of Things on Business Models of Established Manufacturing Companies-A Business Level Perspective. *Technovation*, *68*, 4–19.

Knight, R., & Nurse, J. R. (2020). A Framework for Effective Corporate Communication after Cyber Security Incidents. *Computers & Security*, *99*, 102036. https://doi.org/10.1016/j.cose.2020.102036

Kotusev, S. (2018). TOGAF-based Enterprise Architecture Practice: An Exploratory Case Study. *Communications of the Association for Information Systems*, 321–359. https://doi.org/10.17705/1CAIS.04320

Kowalkowski, C., Gebauer, H., & Oliva, R. (2017). Service Growth in Product Firms: Past, Present, and Future. *Industrial Marketing Management*, *60*, 82–88. https://doi.org/10.1016/j.indmarman.2016.10.015

Kuypers, M. A., Maillart, T., & Paté-Cornell, E. (2016). *An Empirical Analysis of Cyber Security Incidents at a Large Organization.* Stanford University. https://fsi.stanford.edu/publication/empirical-analysis-cyber-security-incidents-large-organization

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-crime and Cyber-attacks During the Pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Lasrado, L. A., Vatrapu, R., & Andersen, K. N. (2015). Maturity Models Development in IS Research: A Literature Review. *Selected Papers of the IRIS*, *6*(6). https://doi.org/10.13140/RG.2.1.3046.3209

Lech, P. (2013). Time, Budget, and Functionality?—IT Project Success Criteria Revised. *Information Systems Management*, *30*(3), 263–275. https://doi.org/10.1080/10580530.2013.794658

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., & Ahlemann, F. (2017). Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. *Business & Information Systems Engineering*, *59*(4), 301–308. https://doi.org/10.1007/s12599-017-0484-2

Lerch, C., & Gotsch, M. (2015). Digitalized Product-Service Systems in Manufacturing Firms: A Case Study Analysis. *Research-Technology Management*, *58*(5), 45–52. https://doi.org/10.5437/08956308X5805357

Linde, L., Sjödin, D., Parida, V., & Gebauer, H. (2021). Evaluation of Digital Business Model Opportunities. *Research-Technology Management*, *64*(1), 43–53. https://doi.org/10.1080/08956308.2021.1842664

Lund, H. B., & Karlsen, A. (2020). The Importance of Vocational Education Institutions in Manufacturing Regions: Adding Content to a Broad Definition of Regional Innovation Systems. *Industry and Innovation*, *27*(6), 660–679. https://doi.org/10.1080/13662716.2019.1616534

Luz Martín-Peña, M., Díaz-Garrido, E., & Sánchez-López, J. M. (2018). The Digitalization and Servitization of Manufacturing: A Review on Digital Business Models. *Strategic Change*, *27*(2), 91–99. https://doi.org/10.1002/jsc.2184

Malatji, M., Marnewick, A., & Solms, S. von (2020). Validation of a Socio-technical Management Process for Optimising Cybersecurity Practices. *Computers & Security*, *95*, 101846. https://doi.org/10.1016/j.cose.2020.101846

March, & Storey (2008). Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research. *MIS Quarterly*, *32*(4), 725. https://doi.org/10.2307/25148869

Margherita, E. G., & Braccini, A. M. (2020). Industry 4.0 Technologies in Flexible Manufacturing for Sustainable Organizational Value: Reflections from a Multiple Case Study of Italian Manufacturers. *Information Systems Frontiers.* Advance online publication. https://doi.org/10.1007/s10796-020-10047-y

Martinez, J., Quintano, N., Ruiz, A., Santamaria, I., Soria, I. M. de, & Arias, J. (2021). Security Debt: Characteristics, Product Life-Cycle Integration and Items. In *2021 IEEE/ACM International Conference on Technical Debt (TechDebt)* (pp. 1–5). IEEE. https://doi.org/10.1109/TechDebt52882.2021.00009

McKinsey Digital. (2019, September 16). *Mastering the Duality of Digital: How Companies Withstand Disruption*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/mastering-the-duality-of-digital-how-companies-withstand-disruption

Mendhurwar, S., & Mishra, R. (2021). Integration of Social and IoT Technologies: Architectural Framework for Digital Transformation and Cyber Security Challenges. *Enterprise Information Systems*, *15*(4), 565–584. https://doi.org/10.1080/17517575.2019.1600041

Mettler, T. (2011). Maturity Assessment Models: a Design Science Research Approach. *International Journal of Society Systems Science*, *3*(1/2), Article 38934, 81. https://doi.org/10.1504/IJSSS.2011.038934

Mullarkey, M. T., & Hevner, A. R. (2019). An Elaborated Action Design Research Process Model. *European Journal of Information Systems*, *28*(1), 6–20. https://doi.org/10.1080/0960085X.2018.1451811

Müller, J. M., Buliga, O., & Voigt, K.-I. (2018). Fortune Favors the Prepared: How SMEs Approach Business Model Innovations in Industry 4.0. *Technological Forecasting and Social Change*, *132*, 2–17.

Naiman, L. (2019). Design Thinking as a Strategy for Innovation. *The European Business Review*, *53*, 72–76.

Oberländer, A. M., Röglinger, M., & Rosemann, M. (2021). Digital Opportunities for Incumbents – A Resource-centric Perspective. *The Journal of Strategic Information Systems*, *30*(3), 101670. https://doi.org/10.1016/j.jsis.2021.101670

Oliveira, M., Mendes, G., Albuquerque, A., & Rozenfeld, H. (2018). Lessons Learned from a Successful Industrial Product Service System Business Model: Emphasis on Financial Aspects. *Journal of Business & Industrial Marketing*, *33*(3), 365–376. https://doi.org/10.1108/JBIM-07-2016-0147

Parekh, G., DeLatte, D., Herman, G. L., Oliva, L., Phatak, D., Scheponik, T., & Sharman, A. T. (2018). Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes. *IEEE Transactions on Education*, *61*(1), 11–20. https://doi.org/10.1109/TE.2017.2715174

Parvinen, P., Pöyry, E., Gustafsson, R., Laitila, M., & Rossi, M. (2020). Advancing Data Monetization and the Creation of Data-based Business Models. *Communications of the Association for Information Systems*, *47*(1), 25–49. https://doi.org/10.17705/1CAIS.04702

Paschou, T., Rapaccini, M [M.], Adrodegari, F [F.], & Saccani, N [N.] (2020). Digital Servitization in Manufacturing: A Systematic Literature Review and Research Agenda. *Industrial Marketing Management, 89*, 278–292. https://doi.org/10.1016/j.indmarman.2020.02.012

Payette, J., Anegbe, E., Caceres, E., & Muegge, S. (2015). Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. *Technology Innovation Management Review, 5*(6), 26–34. https://doi.org/10.22215/timreview/904

Pinto, J. K., & Prescott, J. E. (1988). Variations in Critical Success Factors Over the Stages in the Project Life Cycle. *Journal of Management, 14*(1), 5–18. https://doi.org/10.1177/014920638801400102

Pöppelbuß, J., & Röglinger, M. (2011). What Makes a Useful Maturity Model? A Framework of General Design Principles for Maturity Models and its Demonstration in Business Process Management. *Proceedings of the 19th European Conference on Information Systems (ECIS 2011), 28*.

Porter, M. E., & Heppelmann, J. E. (2014). How Smart, Connected Products are Transforming Competition. *Harvard Business Review, 92*(11), 64–88.

Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2018). Policy Reconciliation for Access Control in Dynamic Cross-enterprise Collaborations. *Enterprise Information Systems, 12*(3), 279–299. https://doi.org/10.1080/17517575.2017.1355985

PWC. (2021, May 1). *PwC Maschinenbau-Barometer Q1 2021 - Schwerpunkt: Investitionen.* PricewaterhouseCoopers. https://www.pwc.de/de/industrielle-produktion/pwc-maschinenbau-barometer-q1-2021.pdf

Rashed, F., & Drews, P. (2021). How Does Enterprise Architecture Support the Design and Realization of Data-Driven Business Models? An Empirical Study. In F. Ahlemann, R. Schütte, & S. Stieglitz (Eds.), *Lecture Notes in Information Systems and Organisation. Innovation Through Information Systems* (Vol. 48, pp. 662–677). Springer International Publishing. https://doi.org/10.1007/978-3-030-86800-0_45

Rieger, A., Guggenmos, F., Lockl, J., Fridgen, G., & Urbach, N. (2019). Building a Blockchain Application that Complies with the EU General Data Protection

Regulation. *MIS Quarterly Executive*, *18*(4), 263–279. https://doi.org/10.17705/2msqe.00020

Ries, E. (2011). *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses* (First edition). Currency, an imprint of the Crown Publishing Group.

Ringel, A. (2022, September 21). *Pay-Per-Part: Das neue Geschäftsmodell von Trumpf: Kunden bezahlen für gefertigte Bauteile.* Produktion- Technik und Wirtschaft für die deutsche Industrie. https://www.produktion.de/wirtschaft/pay-per-part-das-neue-geschaeftsmodell-von-trumpf-81-775.html

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer Security Incident Response Team Development and Evolution. *IEEE Security & Privacy*, *12*(5), 16–26. https://doi.org/10.1109/MSP.2014.89

Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. *Proceedings of the IEEE*, *63*(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939

Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, *10*(3), 21–45.

Schuh, G., Frank, J., Holst, L., Müller, D., Leiting, T., & Bruhns, L. (2021). Digitalization as an Enabler of Subscription Business Models in the Manufacturing Industry. In K.-I. Voigt & J. M. Müller (Eds.), *Future of Business and Finance. Digital Business Models in Industrial Ecosystems* (pp. 49–70). Springer International Publishing. https://doi.org/10.1007/978-3-030-82003-9_4

Schultze, U., & Avital, M. (2011). Designing Interviews to Generate Rich Data for Information Systems Research. *Information and Organization*, *21*(1), 1–16. https://doi.org/10.1016/j.infoandorg.2010.11.001

Selviaridis, K., & Wynstra, F. (2015). Performance-based Contracting: a Literature Review and Future Research Directions. *International Journal of Production Research*, *53*(12), 3505–3540. https://doi.org/10.1080/00207543.2014.978031

Simons, M. (2018). Additive Manufacturing—a Revolution in Progress? Insights from a Multiple Case Study. *The International Journal of Advanced Manufacturing Technology*, *96*(1-4), 735–749. https://doi.org/10.1007/s00170-018-1601-1

Sjödin, D., Parida, V., & Visnjic, I. (2022). How Can Large Manufacturers Digitalize Their Business Models? A Framework for Orchestrating Industrial Ecosystems. *California Management Review*, *64*(3), 49–77. https://doi.org/10.1177/00081256211059140

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the Science of the Artificial– reconsidering the Build-evaluate Pattern in Design Science Research. In *International Conference on Design Science Research in Information Systems* (pp. 381–397). Springer.

Statistisches Bundesamt. (2022, June 2). *Inlandsprodukt Detaillierte Jahresergebnisse: Inlandsproduktberechnung - Detaillierte Jahresergebnisse.* Statistisches Bundesamt. https://www.destatis.de/DE/Themen/Wirtschaft/Volkswirtschaftliche-Gesamtrechnungen-Inlandsprodukt/Publikationen/Downloads-Inlandsprodukt/inlandsprodukt-vorlaeufig-pdf-2180140.pdf?__blob=publicationFile&v=6

Stikvoort, D. (2019). *SIM3: Security Incident Management Maturity Model* (SIM3 mkXVIIIc1). Open CSIRT Foundation (OCF) et al. http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf

Sund, K. J., Bogers, M. L., & Sahramaa, M. (2021). Managing Business Model Exploration in Incumbent Firms: A Case Study of Innovation Labs in European Banks. *Journal of Business Research*, *128*, 11–19. https://doi.org/10.1016/j.jbusres.2021.01.059

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of Comprehensive Information Security Awareness and Cognitive Characteristics on Security Incident Management – an Empirical Study. *Computers & Security*, *109*, 102401. https://doi.org/10.1016/j.cose.2021.102401

Thompson, E. C. (2018). Cyber Risks and the Attack Life Cycle. In E. C. Thompson (Ed.), *Cybersecurity Incident Response* (pp. 71–85). Apress. https://doi.org/10.1007/978-1-4842-3870-7_6

Tremblay, M. C., Hevner, A. R., & Berndt, D. J. (2010). Focus Groups for Artifact Refinement and Evaluation in Design Research. *Communications of the Association for Information Systems*, *26*. https://doi.org/10.17705/1CAIS.02627

Tukker, A. (2004). Eight Types of Product–service System: Eight Ways to Sustainability? Experiences from SusProNet. *Business Strategy and the Environment*, *13*(4), 246–260. https://doi.org/10.1002/bse.414

Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of Risk Management Implementation for Industry 4.0. *Procedia Manufacturing*, *11*, 1223–1230. https://doi.org/10.1016/j.promfg.2017.07.248

Tuptuk, N., & Hailes, S. (2018). Security of Smart Manufacturing Systems. *Journal of Manufacturing Systems*, *47*, 93–106. https://doi.org/10.1016/j.jmsy.2018.04.007

Urbach, N., & Röglinger, M. (2019). *Digitalization Cases*. Springer International Publishing. https://doi.org/10.1007/978-3-319-95273-4

Urbach, N., Röglinger, M., Kautz, K., Alias, R. A., Saunders, C. S., & Wiener, M. (Eds.). (2021). *Management for Professionals: vol. 2. Mastering Digital Transformation for Global Business*. Springer. https://doi.org/10.1007/978-3-030-80003-1

van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing Decision Support for Cybersecurity Threat and Incident Managers. *Computers & Security*, *113*, 102535. https://doi.org/10.1016/j.cose.2021.102535

VDMA. (2022, April 1). *Mechanical Engineering - Figures and Charts 2022*. https://www.vdma.org/documents/34570/6128644/Maschinenbau%20in%20Zahl%20und%20Bild%202022.pdf/43a31467-dc91-1bd9-41ee-97413c4e769d

VDMA, & PWC (Eds.). (2019, May 1). *Digital Business Models in Plant Engineering and Construction in an International Comparison*. https://www.pwc.de/de/industrielle-produktion/pwc-vdma-studie-digital-business-models-in-plant-engineering-and-construction.pdf

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital Transformation: A Multidisciplinary Reflection and Research Agenda. *Journal of Business Research*, *122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Vial, G. (2019). Understanding Digital Transformation: A Review and a Research Agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Voigt, K.-I., Brechtel, F., Schmidt, M.-C., & Veile, J. (2021). Industrial Data-Driven Business Models: Towards a Goods-Service-Data Continuum. In K.-I. Voigt & J. M. Müller (Eds.), *Future of Business and Finance. Digital Business Models in Industrial Ecosystems* (pp. 137–153). Springer International Publishing. https://doi.org/10.1007/978-3-030-82003-9_9

Volberda, H. W., Khanagha, S., Baden-Fuller, C., Mihalache, O. R., & Birkinshaw, J. (2021). Strategizing in a Digital World: Overcoming Cognitive Barriers, Reconfiguring Routines and Introducing New Organizational Forms. *Long Range Planning*, *54*(5), 102110. https://doi.org/10.1016/j.lrp.2021.102110

vom Brocke, J., Debortoli, S., Müller, O., & Reuter, N. (2014). How In-memory Technology Can Create Business Value: Insights from the Hilti Case. *Communications of the Association for Information Systems*, *34*. https://doi.org/10.17705/1CAIS.03407

vom Brocke, J., Hevner, A., & Maedche, A. (Eds.). (2020). *Progress in IS. Design Science Research. Cases*. Springer International Publishing. https://doi.org/10.1007/978-3-030-46781-4

Wade, & Hulland (2004). Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research. *MIS Quarterly*, *28*(1), 107. https://doi.org/10.2307/25148626

Wagire, A. A., Joshi, R., Rathore, A. P. S., & Jain, R. (2020). Development of Maturity Model for Assessing the Implementation of Industry 4.0: Learning from Theory and Practice. *Production Planning & Control*, *226*, 1–20. https://doi.org/10.1080/09537287.2020.1744763

Wang, L., Törngren, M., & Onori, M. (2015). Current Status and Advancement of Cyber-physical Systems in Manufacturing. *Journal of Manufacturing Systems*, *37*, 517–527. https://doi.org/10.1016/j.jmsy.2015.04.008

Waschull, S., Bokhorst, J., Molleman, E., & Wortmann, J. C. (2020). Work Design in Future Industrial Production: Transforming Towards Cyber-physical Systems. *Computers & Industrial Engineering*, *139*, 105679. https://doi.org/10.1016/j.cie.2019.01.053

Weking, J., Stöcker, M., Kowalkiewicz, M., Böhm, M., & Krcmar, H. (2020). Leveraging Industry 4.0 – A Business Model Pattern Framework. *International Journal of Production Economics*, *225*, 107588. https://doi.org/10.1016/j.ijpe.2019.107588

Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Blegind Jensen, T. (2021). Unpacking the Difference Between Digital Transformation and IT-Enabled Organizational Transformation. *Journal of the Association for Information Systems*, *22*(1), 102–129. https://doi.org/10.17705/1jais.00655

Wessel, M., Levie, A., & Siegel, R. (2016). The Problem with Legacy Ecosystems. *Harvard Business Review*, *94*(11), 68–74.

Winter, R., & Fischer, R. (2006). Essential Layers, Artifacts, and Dependencies of Enterprise Architecture. In *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)* (p. 30). IEEE. https://doi.org/10.1109/EDOCW.2006.33

Wißotzki, M., Sandkuhl, K., & Wichmann, J. (2021). Digital Innovation and Transformation: Approach and Experiences. In A. Zimmermann, R. Schmidt, & L. C. Jain (Eds.), *Intelligent Systems Reference Library. Architecting the Digital Transformation* (Vol. 188, pp. 9–36). Springer International Publishing. https://doi.org/10.1007/978-3-030-49640-1_2

Wu, D., Ren, A., Zhang, W [Wenhui], Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for Digital Manufacturing. *Journal of Manufacturing Systems*, *48*, 3–12. https://doi.org/10.1016/j.jmsy.2018.03.006

Wu, S. P.-J., Straub, D. W., & Liang, T.-P. (2015). How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers. *MIS Quarterly*, *39*(2), 497–518. https://doi.org/10.25300/MISQ/2015/39.2.10

Yang, L., Xing, K., & Lee, S.-H. (2010). A new Conceptual Life Cycle Model for Result-Oriented Product-Service System Development. In *Proceedings of 2010 IEEE International Conference on Service Operations and Logistics, and Informatics* (pp. 23–28). IEEE. https://doi.org/10.1109/SOLI.2010.5551621

Yang, M., & Evans, S [Steve] (2019). Product-service System Business Model Archetypes and Sustainability. *Journal of Cleaner Production*, *220*, 1156–1166. https://doi.org/10.1016/j.jclepro.2019.02.067

Yin, R. K. (1992). The Case Study Method as a Tool for Doing Evaluation. *Current Sociology*, *40*(1), 121–137.

Zhang, W [Wanrong], & Banerji, S. (2017). Challenges of Servitization: A Systematic Literature Review. *Industrial Marketing Management, 65*, 217–227. https://doi.org/10.1016/j.indmarman.2017.06.003

Zheng, P., Wang, Z., Chen, C.-H., & Pheng Khoo, L. (2019). A Survey of Smart Product-service Systems: Key Aspects, Challenges and Future Perspectives. *Advanced Engineering Informatics*, *42*, 100973. https://doi.org/10.1016/j.aei.2019.100973

V Appendix

1 Index of Research Articles

Research Article #1: Exploring Digital Business Models – The Case of WashTec

Ritter C., Häckel B., Klees C., Koeppe R., Oberländer A.M., Röglinger M. & Stahl B. Exploring Digital Business Models – The Case of WashTec. *Working Paper in 1st Revision.*

Research Article #2: Data or Business First? – Manufacturers' Transformation toward Data-driven Business Models

Stahl B., Häckel B., Leuthe D. & Ritter C. Data or Business First? – Manufacturers' Transformation toward Data-driven Business Models. *Schmalenbach Journal of Business Research (SBUR) (2023).*

(VHB-Jourqual 3: Category B)

Research Article #3: Leveraging Digital Technologies for Product-Service Systems in Manufacturing – Structuring the PSS Transformation with a Socio-technical Maturity Model

Häckel B., Huber R., Stahl B., Stöter M., Berger T. & Faßl J. Leveraging Digital Technologies for Product-Service Systems in Manufacturing – Structuring the PSS Transformation with a Socio-technical Maturity Model. *Submitted Working Paper*. Earlier version published in *Proceedings of the 16th The International Conference on Business Information Systems (WI 2021). Duisburg, Germany.*

Research Article #4: Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects

Guggenmos F., Häckel B., Ollig P. & Stahl B. Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects. *Computers & Security* (2022) *118, 2022, 102747.*

(VHB-Jourqual 3: - Impact Factor (2023): 5.105)

Research Article #5: Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities

Bitzer M., Häckel B., Leuthe D., Ott J., Stahl B. & Strobel J. Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security* (2023) *125, 2023, 103050.*

(VHB-Jourqual 3: - Impact Factor (2023): 5.105)

During my Ph.D., I also contributed to other publications, which are listed below. These publications are not part of this dissertation.

Berger, M., Lange, T. & Stahl, B. (2022). **A digital push with real impact–Mapping effective digital nudging elements to contexts to promote environmentally sustainable behavior**. *Journal of Cleaner Production,* VHB-Jourqual 3: B

Fabri L., Häckel B., Stahl B., Beck S. & Gabele M. (2022). **How Agile is Your IT Department? – Development and Application of a Framework-independent Agile Scaling Maturity Model**. *Proceedings of the 30th European Conference on Information Systems (ECIS),* Timisoara, Romania. VHB-Jourqual 3: B

Bitzer, M., Stahl, B. & Strobel, J. (2021). **Empathy for Hackers-an IT Security Risk Assessment Artifact for Targeted Hacker Attacks**. *Proceedings of the 29th European Conference on Information Systems (ECIS),* Marrakesh, Morocco. VHB-Jourqual 3: B

Berger, S., Häckel B., Niesel, O. & Stahl, B. (2021). **The Digital 'War for Talents': A Conceptual Framework of Technology-Driven Factors in Digital Personnel Selection Systems**. *Proceedings of the 42nd International Conference on Information Systems (ICIS)*. - Austin, USA. VHB-Jourqual 3: A

Huber, R., Niesel, O., Oberländer, A. M., Stahl, B. & Übelhör, J. (2021). **Intelligent Innovation Processes: The Potential Of AI for Digital Innovation Processes**. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS).* Dubai, UAE. VHB-Jourqual 3: C

Häckel, B., Huber, R., Stahl, B. & Stöter, M. (2021, March). **Becoming a Product-service System Provider – A Maturity Model for Manufacturers**. *Proceedings of the 16th The International Conference on Business Information Systems (WI 2021).* Duisburg, Germany. VHB-Jourqual 3: C

Huber, R., Renner, J. & Stahl, B. (2021). **Combining Individual and Organizational Capabilities: An Integrated Maturity Model for Ambidexterity**. *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS)*. Oahu, Hawaii VHB-Jourqual 3: C

Oberländer, A. M., Stahl, B., Watkowski, L., Braadt, S. & Scherer, P. (2021). **A Two-Sided Approach for Digital Innovation at SCHOTT**. In *Digitalization Cases Vol. 2* (pp. 227-247). Springer, Cham.

2 Individual Contribution to the Research Articles

This cumulative dissertation comprises five research articles that comprise the main body of work. All articles were developed in teams with multiple co-authors. This section details the respective research settings and highlights my individual contributions to each article.

Research article #1:

I co-authored this research paper with Christian Ritter, Björn Häckel, Carsten Klees, Ralf Koeppe, Anna Maria Oberländer, and Maximilian Röglinger. As the paper was developed in action design research, I closely engaged in the conceptual development and evaluation of the paper's main artifact. Regarding the development of the manuscript, I co-developed the initial draft of the research paper and was mainly engaged in the methodological development and conceptualization of the practical observations. Additionally, I engaged in the further development and revision of the research idea as well as textual elaboration. Christian Ritter is the lead author of this research paper.

Research article #2:

This research article was developed by a team of four co-authors (Bastian Stahl, Björn Häckel, Daniel Leuthe, and Christian Ritter). As the leading author, I developed the artifact's basic research idea and concept and was responsible for elaborating the research method, model development, and evaluation. Additionally, I was in charge of preparing the article's refinement and preparing it for the rounds of revisions. While, to a large extent, this article reflects my work, all co-authors promoted the advancement of the paper throughout the entire project.

Research article #3:

I co-authored this research paper with Björn Häckel, Rocco Huber, Maximilian Stöter, Tom Berger and Jan Faßl. An earlier version of the article was presented at the 16th International Conference on Business Information Systems (WI 2021) in Duisburg, Germany. The author's team decided to extend the article's scope by overhauling the theoretical embedding and conducting a thorough evaluation in a case study demonstration. Throughout the development of both papers, I was primarily responsible for developing the theoretical embedding, developing and evaluating the maturity model by organizing and conducting the case study demonstration. In the paper's re-submissions, I was engaged in the further development of the research idea as well as textual elaboration. All co-authors contributed equally to the article's content and supported the project throughout its duration.

Research article #4:

I co-authored this research paper with Florian Guggenmos, Philipp Ollig, and Björn Häckel. All co-authors jointly developed the IT security decision framework for digitalization projects. I was mainly involved in developing the framework and its evaluation by conducting several interviews with industry experts. Furthermore, regarding crafting the manuscript for this article, I engaged in the initial draft of the paper and its further textual elaboration throughout the revisions. Björn Häckel holds a subordinate co-authorship in this research article, while the other three co-authors contribute equally to this research article.

Research article #5:

Research article #5 was developed by the author's team of Björn Häckel, Michael Bitzer, Daniel Leuthe, Joshua Ott, Bastian Stahl, and Jacqueline Strobel. All co-authors jointly developed the incident response management maturity model. I dedicatedly focused on the development method and engaged the framework's design and refinement and its evaluation with several organizations. Additionally, I engaged in the first draft of the paper and its additional textual refinement throughout the revisions. All six co-authors contributed equally to the article's content and supported the project throughout its duration.

3 Research Article #1

Exploring Digital Business Models – The Case of WashTec

Working Paper

Authors: Ritter C., Häckel B., Klees C., Koeppe R., Oberländer A., Röglinger M. & Stahl B.

Extended Abstract[1]:

Digital technologies allow manufacturers to tap into new digital business models that promise to enhance their competitive advantage (Luz Martín-Peña et al., 2018; Oberländer et al., 2021). However, the value creation logic strongly differs between traditional product-centric offerings and new service-oriented digital business models (Linde et al., 2021). As a consequence, many executives of incumbent manufacturers are faced with the issue of identifying a desirable target digital business model based on an existing product core and business for which there is a lack of systematic approaches (Verhoef et al., 2021; Wißotzki et al., 2021). Especially sensing exploration opportunities and assessing the strategic value of new, digital business models, to what extent existing business can be strengthened or expanded, and how it can be monetized, is a challenge (Favoretto et al., 2022; Linde et al., 2021).

This challenge is addressed by presenting the case study of WashTec, a manufacturer of car wash systems. The article highlights the need for exploration beyond an established product core and the evaluation of monetization potential to develop successful digital business models. The article evaluates established innovation and exploration approaches, but also diagnoses missing methodological guidance throughout the exploration process for digital business models. To address the issue, the paper uses an action design research approach (Mullarkey & Hevner, 2019) to develop a four-phase approach for exploration (i.e., *Activation, Inspiration, Evaluation,* and *Monetization*). This approach enhances existing approaches, such as the established Stage-Gate-process (Cooper, 1990) or Design Thinking patterns (Naiman, 2019), by including a dedicated upstream focus on strategy (i.e., the *Activation* phase) and a downstream phase dedicated on development of business cases (i.e., the *Monetization* phase).

[1] At the time of writing, this research article is under review for publication in a scientific journal. Therefore, an extended abstract, taken from the research article, is provided here.

The four phases are presented in detail, starting with the *Activation* phase, which evaluates different strategic opportunities for exploration and identifies strategically valuable opportunity spaces for digital business models (*value pools*). The *Inspiratio*n phase develops innovative ideas within the prioritized value pools, utilizing the expertise and creativity of the workforce and external innovation sources. The *Evaluation* phase assesses the remaining ideas based on three criteria: desirability, feasibility, and viability (Ries, 2011). Lastly, the *Monetization* phase evaluates detailed business cases and derives an overarching monetization strategy for the digital business models (Baltuttis et al., 2022).

The four-phase approach offers a blueprint for practitioners to structure their exploration of digital business models and provides lessons learned and recommendations to approach exploration more effectively drawn from the case. The work also offers descriptive knowledge about the challenges and lessons learned along WashTec's exploration journey, highlighting the complexity of the socio-technical transformation required to move from hardware-centric organizational logic to new, digital business models.

Keywords: Exploration, Digital business models, Strategy, Digitalization, Innovation

References:

Baltuttis, D., Häckel, B., Jonas, C. M., Oberländer, A. M., Röglinger, M., & Seyfried, J. (2022). Conceptualizing and Assessing the Value of Internet of Things Solutions. *Journal of Business Research*, *140*, 245–263. https://doi.org/10.1016/j.jbusres.2021.10.063

Cooper, R. G. (1990). Stage-gate Systems: A New Tool for Managing New Products. *Business Horizons*, *33*(3), 44–54. https://doi.org/10.1016/0007-6813(90)90040-I

Favoretto, C., Mendes, G. H. d. S., Filho, M. G., Gouvea de Oliveira, M., & Ganga, G. M. D. (2022). Digital Transformation of Business Model in Manufacturing Companies: Challenges and Research Agenda. *Journal of Business & Industrial Marketing*, *37*(4), 748–767. https://doi.org/10.1108/JBIM-10-2020-0477

Linde, L., Sjödin, D., Parida, V., & Gebauer, H. (2021). Evaluation of Digital Business Model Opportunities. *Research-Technology Management*, *64*(1), 43–53. https://doi.org/10.1080/08956308.2021.1842664

Luz Martín-Peña, M., Díaz-Garrido, E., & Sánchez-López, J. M. (2018). The Digitalization and Servitization of Manufacturing: A Review on Digital Business Models. *Strategic Change*, *27*(2), 91–99. https://doi.org/10.1002/jsc.2184

Mullarkey, M. T., & Hevner, A. R. (2019). An Elaborated Action Design Research Process Model. *European Journal of Information Systems*, *28*(1), 6–20. https://doi.org/10.1080/0960085X.2018.1451811

Naiman, L. (2019). Design Thinking as a Strategy for Innovation. *The European Business Review*, *53*, 72–76.

Oberländer, A. M., Röglinger, M., & Rosemann, M. (2021). Digital Opportunities for Incumbents – A Resource-centric Perspective. *The Journal of Strategic Information Systems*, *30*(3), 101670. https://doi.org/10.1016/j.jsis.2021.101670

Ries, E. (2011). *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Successful Businesses* (First edition). Currency, an imprint of the Crown Publishing Group.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital Transformation: A Multidisciplinary Reflection and Research Agenda. *Journal of Business Research*, *122*, 889–901. https://doi.org/10.1016/j.jbusres.2019.09.022

Wißotzki, M., Sandkuhl, K., & Wichmann, J. (2021). Digital Innovation and Transformation: Approach and Experiences. In A. Zimmermann, R. Schmidt, & L. C. Jain (Eds.), *Intelligent Systems Reference Library. Architecting the Digital Transformation* (Vol. 188, pp. 9–36). Springer International Publishing. https://doi.org/10.1007/978-3-030-49640-1_2

4 Research Article #2

Data or Business First? – Manufacturers' Transformation toward Data-driven Business Models

Authors: Stahl B., Häckel B., Leuthe D. & Ritter C.

Published in: *Schmalenbach Journal of Business Research (SBUR) (2023)*

Abstract: Driven by digital technologies, manufacturers aim to tap into data-driven business models, in which value is generated from data as a complement to physical products. However, this transformation can be complex, as different archetypes of data-driven business models require substantially different business and technical capabilities. While there are manifold contributions to research on technical capability development, an integrated and aligned perspective on both business and technology capabilities for distinct data-driven business model archetypes is needed. This perspective promises to enhance research's understanding of this transformation and offers guidance for practitioners. As maturity models have proven to be valuable tools in capability development, we follow a design science approach to develop a maturity model for the transformation toward archetypal data-driven business models. To provide an integrated perspective on business and technology capabilities, the maturity model leverages a layered enterprise architecture model. By applying and evaluating in use at two manufacturers, we find two different transformation approaches, namely 'data first' and 'business first'. The resulting insights highlight the model's integrative perspective's value for research to improve the understanding of this transformation. For practitioners, the maturity model allows a status quo assessment and derives fields of action to develop the capabilities required for the aspired data-driven business model.

Keywords: Data-driven business models, Data-driven services, Data analytics, Manufacturing, Enterprise architecture.

5 Research Article #3

Leveraging Digital Technologies for Product-Service Systems in Manufacturing – Structuring the PSS Transformation with a Socio-technical Maturity Model

Working Paper

Authors: Häckel B., Huber R., Stahl B., Stöter M., Berger T. & Faßl, J.

Extended Abstract[1]:

With increasing servitization in the manufacturing sector, the emerging growth of product-service systems (PSS) as the combination of physical products and complementary services has been observed in recent decades (Baines et al., 2017). Nowadays, servitization and digitalization are two merging trends in manufacturing, allowing to upgrade physical products with digital services leading to integrated or digitalized PSS (Favoretto et al., 2022; Gebauer et al., 2021). In this context, digital technologies like the internet of things, cloud computing, and artificial intelligence are leveraged to empower the service components of PSS (Ardolino et al., 2016). This allows manufacturers to offer proactive services, for instance by providing predictive maintenance for their machinery (Zonta et al., 2020). As a consequence, PSS promise great strategic potential for manufacturers, for instance through higher customer loyalty and increased competitiveness (Gebauer et al., 2021).

Generally, PSS can be classified, regarding their intended value offering (Yang & Evans, 2019). The established typology of Tukker (2004), for instance, distinguishes between *product-oriented*, *use-oriented*, and *result-oriented PSS*. However, the transformation from a pure product manufacturer to becoming a provider of mature PSS, goes in line with the development of new technical and non-technical capabilities (Favoretto et al., 2022). Thus, while the provided PSS archetypes allow manufacturers to identify a target state of their PSS transformation, it remains unclear, what technical and non-technical capabilities manufacturers require for providing a defined PSS type.

As maturity models are an established tool for structuring capability development in transformative processes (Pöppelbuß & Röglinger, 2011), this paper develops a

[1] At the time of writing, this research article is under review for publication in a scientific journal. Therefore, an extended abstract, taken from the research article, is provided here.

maturity model with a socio-technical lens on established PSS types to identify required technical and non-technical capabilities (Baxter & Sommerville, 2011; Bostrom & Heinen, 1977). By following the development procedure of Becker et al. (2009), the paper uses a rigorous design science research approach (Hevner et al., 2004) to build and develop the PSS maturity model (PSSMM) as the central artifact based on existing literature.

The PSSMM is structured in two central dimensions: On the horizontal axis, it includes the PSS typology of Tucker (2004) as maturity levels (i.e., *pure product, product-oriented, use-oriented,* and *result-oriented PSS*). The vertical axis structures the required capabilities along five socio-technical focus areas (i.e., *strategy, culture, structure, practices,* and *IT*) proposed by Cleven et al. (2014). In sum, the continuous maturity model describes 80 capabilities in 20 capability dimensions.

The model was evaluated using both an *ex ante* and *ex post* evaluation methods (Sonnenberg & vom Brocke, 2012). A focus group discussion with academic scholars on the developed model was used as an *ex ante* evaluation proving the model's completeness and internal consistency. The *ex post* evaluation of the model was performed as a case study demonstration (Yin, 1992) at VacuumCo, a German manufacturer of vacuum pumps. In this case study, the PSSMM was first used to define the manufacturer's status quo and target state. Second, based on the assessment, the model was used to derive a project roadmap to track progress in relevant capability dimensions for PSS, showcasing the model's ability to structure the path toward a defined PSS type. The case study demonstration yields insights into the case company's digital transformation and challenges associated with developing towards mature PSS.

In conclusion, the developed model contributes to existing PSS literature and offers a foundation for further theory-building and design actions. Additionally, the model has practical value, as it guides manufacturers in their PSS transformation and describes the required capabilities.

Keywords: Product-service systems, Maturity model, Manufacturing, Digital transformation, Capability development, Case study demonstration.

References:

Ardolino, M., Saccani, N., Gaiardelli, P., & Rapaccini, M. (2016). Exploring the Key Enabling Role of Digital Technologies for PSS Offerings. *Procedia CIRP*, *47*, 561–566. https://doi.org/10.1016/j.procir.2016.03.238

Baines, T., Ziaee Bigdeli, A., Bustinza, O. F., Shi, V. G., Baldwin, J., & Ridgway, K. (2017). Servitization: Revisiting the State-of-the-art and Research Priorities. *International Journal of Operations & Production Management*, *37*(2), 256–278. https://doi.org/10.1108/IJOPM-06-2015-0312

Baxter, G., & Sommerville, I. (2011). Socio-technical Systems: From Design Methods to Systems Engineering. *Interacting with Computers*, *23*(1), 4–17. https://doi.org/10.1016/j.intcom.2010.07.003

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-technical Perspective. Part I: The Causes. *MIS Quarterly*, 17–32.

Cleven, A. K., Winter, R., Wortmann, F., & Mettler, T. (2014). Process Management in Hospitals: an Empirically Grounded Maturity Model. *Business Research*, *7*(2), 191–216.

Favoretto, C., Mendes, G. H., Oliveira, M. G., Cauchick-Miguel, P. A., & Coreynen, W. (2022). From Servitization to Digital servitization: How Digitalization Transforms Companies' Transition towards Services. *Industrial Marketing Management*, *102*, 104–121. https://doi.org/10.1016/j.indmarman.2022.01.003

Gebauer, H., Paiola, M., Saccani, N., & Rapaccini, M. (2021). Digital Servitization: Crossing the Perspectives of Digitization and Servitization. *Industrial Marketing Management*, *93*, 382–388. https://doi.org/10.1016/j.indmarman.2020.05.011

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Pöppelbuß, J., & Röglinger, M. (2011). What Makes a Useful Maturity Model? A Framework of General Design Principles for Maturity Models and its Demonstration in Business Process Management. In *Proceedings of the European Conference on Information Systems (ECIS)*.

Sonnenberg, C., & vom Brocke, J. (2012). Evaluations in the Science of the Artificial–reconsidering the Build-evaluate Pattern in Design Science Research. In *International Conference on Design Science Research in Information Systems* (pp. 381–397). Springer.

Tukker, A. (2004). Eight Types of Product–service System: Eight Ways to Sustainability? Experiences from SusProNet. *Business Strategy and the Environment*, *13*(4), 246–260. https://doi.org/10.1002/bse.414

Yang, M., & Evans, S. (2019). Product-service System Business Model Archetypes and Sustainability. *Journal of Cleaner Production*, *220*, 1156–1166. https://doi.org/10.1016/j.jclepro.2019.02.067

Yin, R. K. (1992). The Case Study Method as a Tool for Doing Evaluation. *Current Sociology*, *40*(1), 121–137.

Zonta, T., Da Costa, C. A., Da Rosa Righi, R., Lima, M. J. de, Da Trindade, E. S., & Li, G. P. (2020). Predictive Maintenance in the Industry 4.0: A Systematic Literature Review. *Computers & Industrial Engineering*, *150*, 106889. https://doi.org/10.1016/j.cie.2020.106889

6 Research Article #4

Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects

Authors: Guggenmos F., Häckel B., Ollig P. & Stahl B.

Published in: *Computers & Security (2022)*

Abstract:

Although digital transformation is geared to achieving strategic goals such as efficiency or competitive advantages, it involves digital threats. IT security is an overarching task for managers and specialists that currently receives little attention in digitalization projects. Therefore, the strategic potential of IT security mostly remains untapped due to a lack of appropriate decision-making and communication tools that support project managers to address IT security consciously. This work tackles this issue by introducing a method to strategically consider IT security in digitalization projects using a design science approach. As a result, three strategic variants of IT security in digitalization projects and their underlying drivers were identified. By consolidating this knowledge into an applicable artifact, this work helps explain existing action patterns in organizations. Moreover, it provides a managerial tool to evaluate and decide on appropriate IT security for digitalization projects.

Keywords: IT security, Digitalization projects; IT security strategy, Strategic interplay.

7 Research Article #5

Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities

Authors: Bitzer M., Häckel B., Leuthe D., Ott J., Stahl B. & Strobel J.

Published in: *Computers & Security (2023)*

Abstract:

Although the ongoing digital transformation offers new opportunities for organizations, more emphasis on information security is needed due to the evolving cyber-threat landscape. Despite all preventive measures, security incidents cannot entirely be mitigated. Organizations must establish incident response management to treat inevitable incidents in a structured manner and under considerable time pressure. If not handled, incidents can result in reputational or financial losses and disrupt business continuity. Especially organizations that have not addressed incident response management extensively need to understand which capabilities are required to develop their incident response management. However, research still lacks a practice-grounded and socio-technical conceptualization of those capabilities and their development. For such challenges, maturity models have proven valuable in practice and research. This paper follows a design science research approach to develop an incident response management maturity model (IRM3) closely aligned with practice requirements under a socio-technical lens. Iteratively applying and evaluating the IRM3 with seven real-world organizations leverages its comprehensive view based on four focus areas and 29 capability dimensions to understand which capabilities organizations need to approach incident response management. Building on existing research, this work provides a comprehensive perspective on incident response management and its associated capabilities. For practitioners, especially in organizations with initial incident response maturity, the IRM3 offers descriptive value when used as a status quo assessment tool and prescriptive value by outlining capabilities for successful incident response management.

Keywords: Design science research, Incident response management, Information security, Maturity model, Socio-technical.