Digital Technologies in the Industrial Sector: Technology-driven Threats and Opportunities

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft

der Rechts- und Wirtschaftswissenschaftlichen Fakultät

der Universität Bayreuth

Vorgelegt

von

Stephan Berger

aus

Augsburg

Dekan:	Prof. Dr. Jörg Gundel
Erstberichterstatter:	Prof. Dr. Maximilian Röglinger
Zweitberichterstatter:	Prof. Dr. Björn Häckel
Tag der mündlichen Prüfung:	06. Mai 2020

Abstract

Digitalization is driven by the rapid emergence and adoption of digital technologies. At unprecedented speed, technological advancements are triggering disruptive changes that affect individuals, organizations, and society on a global scale. In the industrial sector, the rise of new digital technologies such as Cyber-physical Production Systems and the Industrial Internet of Things accelerates the transition from traditional production facilities towards so-called smart factories. These self-organizing and self-optimizing production systems enable more flexible and efficient processes to produce higher quality products at reduced cost. With this, the fourth industrial revolution is profoundly influencing the competitiveness of organizations and regions, affecting productivity, economic growth, and working profiles. Despite their growing importance, the nature of digital technologies – in terms of similarities and differences in their characteristics – remains poorly understood. This hampers scientific progress and practical application, while technology-driven threats and opportunities remain largely opaque. Against this backdrop, this thesis first elaborates on the fundamental understanding of digital technologies, before applying an industrial perspective in order to focus on Cyber-physical Production Systems as the core technology in smart factories. This understanding builds the foundation for the identification, analysis, and management of IT security threats and ecological opportunities in the industry.

This thesis provides two perspectives on the technological foundation of digitalization, developing an in-depth understanding of digital technologies, *per se*, and Cyber-physical Production Systems as a specific technology applied in the industrial sector. Based on a sample of real-world technologies, research article #1 presents a low-level taxonomy of digital technology characteristics, and high-level archetypes representing technology groups. These classification schemes provide long-lasting insights that are much needed in the fast-moving field of digitalization. Focusing on digital technologies in the industry, research article #2 defines and classifies entities of Cyber-physical Production Systems and illustrates their relationships using a terminology, taxonomy, and reference model. Both research articles provide descriptive knowledge of technology, on which further advancements in research and practice can build.

Within the industrial sector, the high degree of cross-linking and decentralization of applied digital technologies brings new complexity and increases the vulnerability of systems to IT (security) threats. Focusing on technology-driven threats, research article #3 proposes a taxonomy of attacks on the Industrial Internet of Things. Drawing on an inductively and deductively compiled sample of attacks, the taxonomy enables the classification of both conventional and emergent attacks. The analysis of an attacked steel facility in Germany provides insights on the use of the taxonomy, which supports the intra- and inter-organizational identification, documentation, and communication of incidents. Analyzing the impact of IT threats within smart factory networks, research article #4 focuses on the

effects of attack and error propagation on production processes. Based on Petri Nets, the presented modeling approach enables organizational stakeholders to compare different smart factory architectures in terms of the impact of IT threats on the availability of information components and production machines. The approach thus provides support for layout decisions and the derivation of appropriate IT security mitigation measures.

With regard to technology-driven opportunities, the thesis offers a technology-driven perspective on ecological sustainability in the industry. Research article #5 develops and evaluates a Benefits Dependency Network which can be used to systematically identify and structure cause-effect relations between digital technology, associated business changes, and ecological benefits. Several artificial and real-world instantiations indicate its practical applicability. As a result, the framework supports decision-making about technology investments, and serves as a basis for planning, executing, and evaluating digitalization projects towards ecological sustainability.

Keywords: *Digitalization, Digital Technology, Industrial Sector, IT Threats, Ecological Opportunities*

Table of Contents

I. Introduction[1]

With wave after wave of disruption, digitalization brings about massive changes affecting individuals, economy, and society (Fitzgerald et al., 2014; Gimpel et al., 2018; Steininger, 2019). Driven by the rapid emergence and adoption of digital technologies, digitalization has launched a paradigm shift in both research and practice (Berger et al., 2018). Having been a value driver for over half a century (Lucas Jr et al., 2013), today, the integration of digital technologies such as virtual reality, big data, cloud computing, or the Internet of Things (IoT) into everyday life happens at unprecedented speed and scale – transforming entire industries (Buck and Eder, 2018; Clark, 2003; Iansiti and Lakhani, 2014) as well as accelerating innovation in business and society alike (Legner et al., 2017). In the case of the IoT, for example, McKinsey estimates that 127 new objects or devices connect to the internet every second (Baroudy et al., 2018). The economic impact of associated IoT applications may exceed $11 trillion per year by 2025 (Ménard, 2017). What can also be observed is an ever-faster rate of commoditization and a shorter time-to-market. While upcoming social networks such as Instagram reached 100 million users in only about two years, mature technologies like the telephone required 75 years to achieved comparable coverage (Statista, 2017).

With their tremendous speed and impact, digital technologies enable the smartification of established products and services as well as the development of new ones. This not only disrupts extant business models and processes but also creates new ones, while opening up entirely new markets (Fitzgerald et al., 2014; Gimpel and Röglinger, 2015; Legner et al., 2017). For instance, the world's leading accommodation and transportation providers – Airbnb and Uber – do not possess any lodging or vehicles, but merely act as brokers (McRae, 2015). Since digital technology has long been at the front and centre of business models, and is now "applied to almost every part of a company's value chain" (Furr and Shipilov, 2019, p. 96), an in-depth technological understanding is essential in order to tap the economic and societal potential of digitalization (Bharadwaj et al., 2013).

The acronym SMAC – i.e., social, mobile, analytics, and cloud computing – relates to the most disruptive technologies in recent years (Evans, 2016). These technologies are already established and have long been part of everyday life. Today, the DARQ technologies, i.e., distributed ledger technology, artificial intelligence, extended reality, and quantum computing, are ringing in the new 'post-digital' age (Accenture, 2019b). Additionally, concepts such as cyber-physical systems combine multiple different technologies to merge the virtual world with physical reality. Meanwhile, rapidly-changing trends in the market bring forth a multitude of new technologies at ever-shorter intervals. For instance, the Gartner Hype Cycle for Emerging Technologies lists over 40 upcoming technologies every year. However, organizations increasingly face uncertainty when making assessments about whether

[1] This section partly comprises content from the thesis' research articles. To improve the readability of the text, I omit the standard labelling of these citations.

technologies will enter mainstream adaption or disappear into oblivion. Causing greater confusion is the opacity that results from the great variety and sheer number of available technologies (Adomavicius et al., 2008). Despite being the key driver of digitalization, digital technology remains a poorly understood phenomenon. The lack of understanding about similarities and differences – which also applies in the case of groups of digital technologies – not only hampers scientific progress but also hinders clear-headed decision-making in industry when it comes to digital transformation. In order to sustain or enhance their competitive position, executives must understand digital technologies as a prerequisite to recognize the technological impact on products, services, business models, and markets (Ciriello et al., 2018; Davenport and Westerman, 2018; Fang et al., 2018; Fichman et al., 2014).

In the industrial sector, the widespread use of digital technologies has led to a new industrial age, known as Industry 4.0. This new age is typified by changes in the industry structure, customer demands, and market competition (Dalenogare et al., 2018), as the uptake of digital technologies affects productivity, economic growth, and working profiles. The integration of digital technologies – particularly the IoT – into manufacturing systems forms the Industrial Internet of Things and Cyber-physical Production Systems (CPPSs) (Sisinni et al., 2018), accelerating the transformation of traditional production facilities into so-called smart factories (Lasi et al., 2014). On an operational level, highly self-organizing and self-optimizing production systems within smart factories increase flexibility, production efficiency, and product quality by monitoring and controlling production processes in real-time (Brettel et al., 2014; Lasi et al., 2014; Radziwon et al., 2014). At the same time, set-up and processing times and material and labour costs can be reduced (Dalenogare et al., 2018). Furthermore, technology integration enables the three main benefits of Industry 4.0: vertical integration, i.e., connecting different hierarchy levels within a smart factory; horizontal integration, i.e., collaboration between organizations; and end-to-end engineering, i.e., engineering throughout a product's entire value chain (Brettel et al., 2014; Kagermann et al., 2013). This increasingly enables organizations to provide their customers with individual service solutions rather than standardized physical products (Govindarajan and Immelt, 2019). Today, customers expect new products and services to incorporate the latest technological advancements (Römer et al., 2017). By pivoting towards customer orientation (Buschmeyer et al., 2016), organizations are able to remain competitive within dynamic markets with shorter research and development cycles for customer-specific products, growing resource and energy efficiency requirements, and constantly changing demands (Kagermann et al., 2013; Lasi et al., 2014). As a result, industrial organizations spent over $220 billion on digital transformation in 2019 (IDC, 2019). In this new industrial age, technology has long been the major driver of transformation and innovation, entailing new threats and opportunities for organizations (Kagermann et al., 2013; Lucas Jr et al., 2013).

Across all industries, established organizations, such as Burberry, Ford, GE, Lego, Procter & Gamble, and Nike, struggle with digital transformation (Davenport and Westerman, 2018), while others, such as Kodak, fail completely (Lucas Jr and Goh, 2009). Hence, it is not surprising that a recent survey of

413 senior executives, carried out by the Center for Information Systems Research of the MIT, found that digital disruption will threaten, on average, 28% of revenue from the executives' enterprises in the next five years (Weill and Woerner, 2018). For large organizations (with more than $7 billion in annual revenue), this figure is as high as 46% (Weill and Woerner, 2018). The reasons are manifold: while companies like Procter & Gamble want to become the most digital organization in the world, they may lose sight of their actual stable business (model). Furthermore, digital transformation is not just about digital technology but also about people and processes adapting to substantial organizational and cultural change (Davenport and Westerman, 2018). Due to their high profits and inability to rapidly adapt, this is particularly true for large organizations, which are increasingly threatened by external digital disrupters (Weill and Woerner, 2018). As a result, IT security has become a critical success factor and main competitive differentiator for digital transformation (Porter and Heppelmann, 2014). An Accenture risk survey (2018a) among Chief Information Security Officers revealed that 71% considered cyber-attacks to be a black box – without being able to estimate the impact on their organization. Nevertheless, only one out of eight organizations includes future cyber threats in their security budgets (Accenture, 2018b), and cybersecurity is often an 'afterthought', with strategic considerations, such as transformation paths, business models, or product mix, taking priority (Doan, 2019). Yet, as systems and threats become more complex and attacks become more sophisticated and professional, this is no longer sufficient (Doan, 2019). Current attitudes suggest a need for organizations to enhance their cybersecurity knowledge and research tools in order to stay ahead of IT threats (Accenture, 2018b). Ultimately, only secure processes and business models will enable a successful digital transformation and prove viable and competitive in the long run.

The fact that their production processes are increasingly reliant on information leaves smart factories particularly vulnerable to IT security threats (Tupa et al., 2017). The multitude of connected technologies, machines, and products in the Industrial Internet of Things open entry points for intentional attacks and unintentional errors which affect the availability of information systems and production machines. In contrast to formerly isolated systems, today, organizations are highly interconnected with their supply chain partners and customers via the internet, forming digitized value networks. As stated in Symantec's *Internet Security Threat Report* (2019), cyber-attacks on value networks increased by 78% in 2018. The high degree of intra- and inter-organizational cross-linking and dependencies favours the spread and propagation of attacks and errors across value chains and networks. Cascading failures amplify the vulnerability within highly connected networks and cause instability in smart factories and their supply chains (Smith et al., 2007), eventually leading to the collapse of entire value networks (Amiri et al., 2014). Hence, "with cyberattacks increasingly threatening businesses, executives need new tools, techniques, and approaches to protect their organizations" (Huang et al., 2019, p. 1). This includes both anticipating potential attacks and developing proactive mitigation measures to protect business (Accenture, 2018b).

On the upside, digital transformation creates a plethora of new opportunities through technological change (Steininger, 2019). Aiming for business growth and expansion (Lucas Jr and Goh, 2009), technology-driven innovation creates new products, services, business models, and markets. With this, organizations are able to strengthen their customer relations and leverage cross-selling opportunities (Weill and Woerner, 2015). In industry, the integration of technology into manufacturing systems is generally used to achieve higher performance (Kagermann et al., 2013; Wang et al., 2016) in terms of the product and operations, i.e., better quality and higher efficiency, as discussed above, or general concepts, such as sustainability (Dalenogare et al., 2018; Fitzgerald et al., 2014; Gimpel and Röglinger, 2015). While there is an extensive body of literature on technology-based process automation and efficiency, and product mass customization and innovation, technology-driven sustainability is still in its infancy. At the same time, public and governmental awareness is constantly increasing, forcing the industry to react. Investigating the reinvention of the industry, a study involving 1,200 executives in 14 industries and 17 countries identified the 'drumbeat to go green' – which is increasingly becoming reality – as one of six major forces responsible for change in this new industrial age (Accenture, 2019a). In his annual letter to corporate executives, the CEO of BlackRock – the world's largest fund manager, holding $7 trillion in assets – recently put pressure on organizations to address environmental sustainability, stating that BlackRock would no longer support organizations that "are not making sufficient progress on sustainability-related disclosures and the business practices and plans underlying them" (BlackRock, 2020). However, the industrial sector still accounts for more than half of global energy consumption (U.S. Energy Information Administration, 2017). Although digitalization and the internet consume increasing amounts of energy themselves (International Energy Agency, 2017), digital technologies – if used intelligently – offer significant opportunities to reduce the industry-related environmental disruption, including global warming, pollution, and the processing of nonrenewable resources (Wang et al., 2016).

Although Industry 4.0 holds the potential to substantially improve environmental performance, it has not yet delivered its full capability to industry (Dalenogare et al., 2018; Wang et al., 2016). Ecological aspects are still not the primary objective of technological investments but are instead seen as positive side effects (Dalenogare et al., 2018). Hence, ecological benefits are neither well understood or explored in the industry (Elsevier, 2019; Ford and Despeisse, 2016) nor linked to digital technologies (Despeisse et al., 2012; Geng et al., 2017) and associated organizational changes. As "technology changes faster than organizations do" (Relihan, 2019), many organizations struggle to realize digital transformation projects due to missing (re)definitions of new organizational structures (Davenport and Westerman, 2018; Denner et al., 2018). Hence, organizations need to be aware of the impact of technology on their business and production processes. In sum, a framework is needed to identify and manage interrelations between digital technologies and ecological benefits, along with necessary business changes, in a

structured manner in order to support organizations' attempts to reduce negative impacts on the environment.

This doctoral thesis is cumulative and consists of five research articles. Based on an in-depth understanding of the nature of digital technologies, it sheds light on associated threats and opportunities in the industrial sector. Accordingly – and as outlined in Figure 1 – the research articles are structured in terms of three overarching topics: *Understanding Digital Technology* as a foundation for *Identifying and Analyzing Technology-driven Threats*, and *Identifying and Managing Technology-driven Opportunities*. Providing novel insights into technological advancements and their effects on industry, the key findings of this thesis are relevant for both researchers and practitioners.

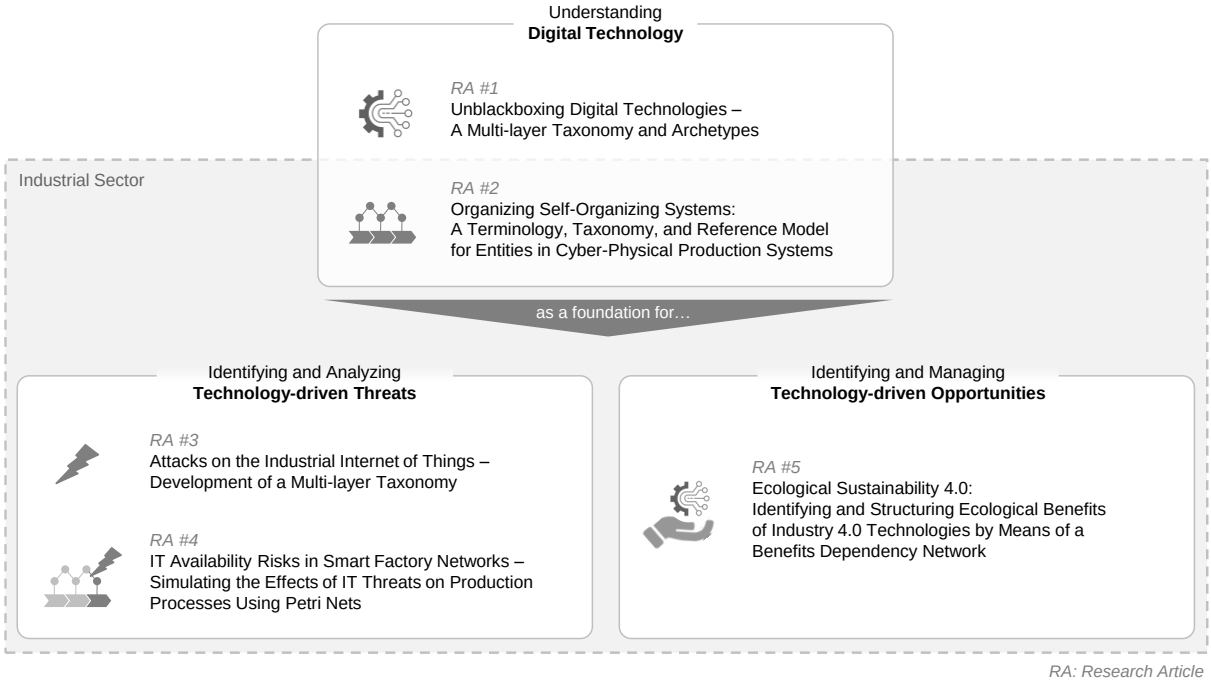

Figure 1. Assignment of the Research Articles to the Structure of the Doctoral Thesis

Digital technologies are the foundation of digitalization, and an in-depth understanding of such technologies is key when exploiting their economic and societal potential. The current lack of sufficient academic and professional literature leaves researchers and practitioners struggling to effectively leverage digital technologies. In response to this problem, this thesis firstly provides a basic technological overview that supports the overarching goal of *Understanding Digital Technology* (Section II.1, comprising research articles #1 and #2). This overview involves two perspectives: research article #1 elaborates on characteristics and groups of digital technologies in general, while research article #2 focuses on the industrial sector and discusses CPPSs in terms of entities and their interactions. Based on these insights, the thesis further discusses threats and opportunities that arise with the increasing application of emerging technologies in the industry. It considers how, due to a high degree of cross-linking and decentralization, technologies such as CPPSs and the Industrial Internet of Things

create new vulnerabilities, particularly when it comes to IT (security) threats. Elaborating on cyber-attacks and the associated effects on production processes, the thesis addresses the challenge of *Identifying and Analyzing Technology-driven Threats* (Section II.2, comprising research articles #3 and #4). In contrast, technologies also offer a multitude of new opportunities. In this regard, the thesis provides a technological perspective on ecological benefits, by *Identifying and Managing Technology-driven Opportunities* (Section II.3, comprising research article #5).

Section III concludes with a summary and an outlook on future research. Section IV includes the publication bibliography. Finally, the appendix in Section V comprises further details on all research articles (Section V.1), my corresponding individual contributions (Section V.2), and the research articles themselves (Section V.3 to V.7).

II. Overview and Context of the Research Articles[2]

1 Understanding Digital Technology

Digitalization is primarily driven by the emergence of digital technologies, and their increasingly rapid adoption in various contexts (Gimpel et al., 2018). Ever-faster commoditization, time-to-market, and increases in user numbers reflect the exponential pace of technology-driven digital disruption. In this regard, Nintendo's application game 'Pokémon Go', which combines location-based and augmented reality technology, broke several records: launched in summer 2016, the application achieved 130 million downloads within the first month and over 1 billion downloads by the end of 2018 (Iqbal, 2019). It was also the fastest game to reach $100 million in sales, which it did after only 20 days (Guinness World Records, 2016). Regarding its social and behavioral impact, the application affected the physical health of users by changing their walking routines and increasing their steps per day by an average of 26% (McFarland, 2016). Despite the initial success of this 'social experiment', experts were unsure about the lifetime of the game and its popularity – which they predicted would last from a few weeks to several years (Kollar and Allegra, 2016). Although today the hype about Pokémon Go has noticeably decreased, in 2019 – three years after its launch – the game generated $894 million, exceeding its revenue from 2016 (Chapple, 2020). Hence, digital technologies hold considerable economic and social potential to transform the way business is practiced.

Applications like 'Pokémon Go' also contribute to the growth of available data, which is doubling every three years (Henke et al., 2016). This affects competition on the market: using data analytics, artificial intelligence, and automation to enable strategic business decisions in real-time, data-driven businesses transform into insights-driven organizations with an expected revenue of $1.8 trillion a year in 2021 (Hopkins et al., 2018). In addition, the integration of digital technologies into products and services disrupts established business models and creates new ones (Fitzgerald et al., 2014; Matt et al., 2015) while opening up new markets. A study of over 50 companies revealed that smart products and services make it possible to increase and modify value propositions (Gimpel et al., 2018). Hence, if organizations are to remain competitive in this fast-moving field, they must develop a clear understanding of the nature of digital technologies and use them to realize company needs (Ciriello et al., 2018; Fang et al., 2018; Fichman et al., 2014). However, as digital technologies "do not necessarily create economic value themselves; […] they need to be leveraged and exploited" (Steininger, 2019, p. 364).

Many organizations nonetheless remain unsure about the technological impact on business models and markets (Davenport and Westerman, 2018) that will result from the use of technology within their products, processes, production, and supply chains (Kagermann et al., 2013), and its capitalization (Denner et al., 2018). Although intuitively and frequently used, 'digital technology' remains an umbrella

[2] This section partly comprises content from the thesis' research articles. To improve the readability of the text, I omit the standard labelling of these citations.

term which is not consistently defined (Denner et al., 2018). At the same time, the number of available technologies is constantly growing thanks to ever-shorter research and development cycles (Berger et al., 2018). This effect is further amplified by combinatorial evolution (Arthur, 2009). That is, new devices and functionalities develop through combining existing technologies, i.e., technology is technology itself. As a result, a broad variety of different technologies exists, such as machine learning, smart dust, 4D printing, and natural language question answering.

Although there have been calls to structure the field (Bharadwaj et al., 2013), digital technologies remain poorly understood. Academic literature primarily discusses topics such as big data (Fahad et al., 2014) or smart things (Püschel et al., 2016) on the level of individual technologies. As digital technologies must not be reduced to a few features (Mathiesen et al., 2013), research lacks a sufficient level of abstraction upon which to build theory. In contrast, professional literature is mainly market-driven and refers to high-level classification schemes like SMAC, i.e., social, mobile, analytics, and cloud (Evans, 2016), and DARQ, i.e., distributed ledger, artificial intelligence, extended reality, and quantum computing (Accenture, 2019b). This leaves organizational stakeholders puzzled about technology selection and adoption decisions, as the first step in selecting a concrete technology involves a consideration of its potential benefits, application cases, and affordances, i.e., action possibilities provided by a technology. Academics and practitioners agree that a common technological understanding is a prerequisite and foundation for theorizing and building appropriate modeling approaches with which to guide further explorations of technology-driven threats and opportunities (Berger et al., 2018).

Against this backdrop, research articles #1 and #2 contribute to the understanding of digital technologies as a prerequisite for developing sound scientific methods and making practical advances: while research article #1 elaborates on digital technologies in general, research article #2 is focused on the industrial sector and discusses CPPSs as the core technology applied in smart factories.

In line with McKelvey's (1978) 'organizational systematics' approach, and based on the iterative development processes as per Nickerson et al. (2013), research article #1 elaborates on the similarities and differences of digital technologies by means of a taxonomy. To identify general classes of digital technologies, the article also provides archetypes. The results are deductively and inductively derived.

The taxonomy of digital technologies (Figure 2) comprises eight dimensions – i.e., role of technology, scope, multiplicity, direction, data treatment, input, output, and human involvement – which are structured using the layered architecture of Yoo et al. (2010) – i.e., device, network, content, and service. Each dimension distinguishes two to five characteristics that are mutually exclusive (exactly one characteristic applies), or non-exclusive (one or multiple characteristics apply). The taxonomy builds on an extensive literature review of current knowledge and a sample of 92 digital technologies from the

Gartner Hype Cycles for Emerging Technologies of 2009 to 2017 (Gartner Inc., 2017, 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2009).

Layer	Dimension	Characteristic					Exclusivity *
Device	Role of Technology	Application			Infrastructure		ME
	Scope	Cyber			Cyber-Physical		ME
Network	Multiplicity	One-to-One		One-to-Many		Many-to-Many	ME
	Direction	Uni-directional			Bi-directional		ME
Content	Data Treatment	Collection	Aggregation	Analysis	Execution	Transmission	NE
	Input	Digital			Physical		NE
	Output	Digital			Physical		NE
Service	Human Involvement	Active Usage			Passive Usage		ME

* ME: Mutually Exclusive; NE: Non-Exclusive

Figure 2. Multi-layer Taxonomy of Digital Technologies

Based on the classification of the sample, a hierarchical cluster analysis resulted in nine digital technology archetypes (Figure 3), each representing a group of digital technologies with similar characteristics.

Archetype	Relative Frequency	Device		Network		Content			Service	Examples
		Role of Technology	Scope	Multiplicity	Direction	Data Treatment	Input	Output	Human Involvement	
Connectivity & Computation	15.2%	Infrastructure (100%)	Cyber (93%)	Many-to-Many (100%)	Bi-Directional (100%)	Transmission (100%)	Digital (100%)	Digital (100%)	Passive Usage (100%)	802.11ax, Quantum Computing
Platform Provision	10.9%	Infrastructure (100%)	Cyber (100%)	One-to-Many (80%)	Bi-Directional (100%)	Transmission (100%)	Digital (100%)	Digital (100%)	Active Usage (100%)	(Mobile) Application Store, Cloud/Web Platform
Mobile Device	5.4%	Infrastructure (100%)	Cyber-Physical (100%)	One-to-One (100%)	Bi-Directional (100%)	Collection / Transmission (100%)	Digital / Physical (100%)	Physical (100%)	Active Usage (100%)	E-Book Reader, Media Tablet
Sensor-based Data Collection	12.0%	Application (100%)	Cyber-Physical (100%)	One-to-One (100%)	Uni-Directional (100%)	Collection (91%)	Physical (100%)	Digital (91%)	Active Usage (100%)	Gesture Recognition, Smart Dust
Actor-based Data Execution	6.5%	Application (100%)	Cyber-Physical (100%)	One-to-One (100%)	Uni-Directional (100%)	Execution (83%)	Digital (100%)	Physical (100%)	Active Usage (100%)	3D Printing, 4D Printing
Analytical Insight Generation	17.4%	Application (100%)	Cyber (100%)	One-to-One (100%)	Bi-Directional (94%)	Analysis (75%)	Digital (100%)	Digital (100%)	Active Usage (100%)	In-memory Analytics, Machine Learning
Self-dependent Material Agency	2.2%	Application (100%)	Cyber-Physical (100%)	One-to-Many (100%)	Bi-Directional (100%)	Col. / Ana. / Exe. / Tra. * (100%)	Digital / Physical (100%)	Digital / Physical (100%)	Active Usage (100%)	Autonomous Vehicle
Augmented Interaction	13.0%	Application (100%)	Cyber-Physical (100%)	One-to-One (100%)	Bi-Directional (100%)	Transmission (92%)	Digital (100%)	Physical (100%)	Active Usage (100%)	Augmented Data Discovery, Virtual Personal Assistant
Natural Interaction	17.4%	Application (100%)	Cyber-Physical (100%)	One-to-One (100%)	Bi-Directional (100%)	Collection (100%)	Physical (100%)	Digital (69%)	Active Usage (100%)	Conversational User Interface, Natural-language Question Answering

For each dimension, we illustrate the relative frequency of the characteristic which occurs most frequently
* Col. / Ana. / Exe. / Tra.: Collection / Analysis / Execution / Transmission

Figure 3. Archetypes of 92 Digital Technologies from the Gartner Hype Cycle for Emerging Technologies

One group of archetypes comprises technologies that build the foundation for applications and add value by supporting, enabling, and enhancing their functionality. *Connectivity & computation* relates to digital technologies that enable the coordination and execution of distributed work (Alter, 2018) in terms of collaboration and information sharing (Levermore et al., 2010; Silver et al., 1995). *Platform provision*

covers infrastructure, software development, and application platforms (Fichman, 2004), which ensure data availability and distribution (Bharadwaj et al., 2013). Finally, *mobile device* represents hardware components that allow for human-computer interaction (Bødker, 1987; Nardi, 1996) and enable the use of digital data independent of the user's location.

The next group of archetypes is involved with the physical world yet does not rely on or interact with humans: *sensor-based data collection* focuses on gathering real-world data by observing changes in the physical environment and transforming this data into digital signals for further analysis (Akyildiz and Kasimoglu, 2004). In contrast, *actor-based data execution* encompasses digital technologies that use digital input to intervene in their physical surrounding (Akanmu et al., 2012).

Other digital technology archetypes are equipped with distinctive analytical skills: *analytical insight generation* deals with data in the course of big data analysis, e.g., extracting useful knowledge using data-mining techniques (Witten et al., 2017), data warehousing (Watson et al., 2002), data-driven business processes, or decision making (Lycett, 2013). *Self-dependent material agency* combines sensors and actors in digital technologies such as smart things, which possess self-x capabilities (e.g., self-configuration, -dependence, -optimization, -diagnosis, or -healing) enabling them to perform autonomous actions.

Finally, interaction-driven archetypes support humans in their tasks: while *augmented interaction* aims to generate insights from data and presenting these to humans, *natural interaction* is focused on social interaction (Al-Natour and Benbasat, 2009) in terms of conversations between users and technology.

The taxonomy and archetypes were developed and evaluated by classifying the sample of 92 digital technologies. The reliability, validity, and usefulness of the results was then assessed by applying the Q-sort method (Nahm et al., 2002), both internally among the co-authors and externally with focus groups (Krueger and Casey, 2014; Tremblay et al., 2010) and industry experts (Rowley, 2012).

In line with IS literature on theory building (Gregor, 2006; Gregor and Hevner, 2013), the results add to descriptive knowledge on the nature of digital technologies and serve as a basis for sense-making and design-oriented research. While the taxonomy enables the identification of similarities and differences on a low level, the archetypes provide a sufficiently abstract and stable foundation for investigating action possibilities, as well as drivers of and barriers to the adoption of digital technologies in future research. On a more practical level, the archetypes support the innovation process of new technologies. As the taxonomy and archetypes were also inductively derived, they provide insights into what is currently going on in the market. This reduces the uncertainty surrounding technology selection and increases the transparency of associated decisions.

The IoT is among the most disruptive technologies and describes "the connectivity of physical objects equipped with sensors and actuators to the Internet via data communication technology" (Oberländer et al. 2018, p. 488). The IoT serves as the basis for cyber-physical systems, which merge the cyber world

with physical reality (Kagermann et al., 2013; Lucke et al., 2008; Schuh et al., 2014). Beyond their application in domains like avionics, health care, and energy distribution (Ahmed et al., 2013), cyber-physical systems are primarily applied in industry. These so-called CPPSs accelerate the transformation of traditional production sites into smart factories (Lasi et al., 2014), which act within interconnected value networks. As CPPSs are adaptive, self-organizing, and cooperative (Broy et al., 2012; Hellinger and Seeger, 2011; Yoon et al., 2012), they allow for flexible and automated production processes, resource efficiency, vertical and horizontal integration (Kagermann et al., 2013; Yoon et al., 2012), and product mass-customization (Lasi et al., 2014; Tjahjono et al., 2017).

Due to the high level of cross-linking and multifunctionality, these technology-driven systems are becoming increasingly complex and opaque. The lack of a common understanding of CPPS characteristics, entities, and system behavior (Ullrich et al., 2016; Wang et al., 2015) hampers design, implementation (Hellinger and Seeger, 2011; Pétrissans et al., 2012; Zuehlke, 2010), and innovation activities in industry (National Instruments, 2014). To date, extant CPPS models vary in their level of abstraction and granularity. As "heterogeneity and isolated solutions prevail" (Hellinger and Seeger, 2011, p. 12), research and practice lack a holistic perspective on CPPSs. Modeling approaches are required that "describe the structure, communication interfaces, and capabilities of the different entities inside a CPPS and the functionalities of the production facilities and their components and the specification of products" (Vogel-Heuser et al., 2014, p. 714). A common understanding is a prerequisite to overcoming complexity and opacity in CPPSs (Kagermann et al., 2013) and serves as a foundation for creating general models of machines, processes, and production (Hellinger and Seeger, 2011; Kagermann et al., 2013). This is especially important as CPPSs are an interdisciplinary construct, combining aspects of (production) engineering, informatics, and automation (Kagermann et al., 2013; Karnouskous and Colombo, 2011).

To address this need, research article #2 elaborates on CPPSs as the core technology in smart factories. Based on an extensive review of current CPPS literature (e.g., Chen, 2017a, 2017b; Monostori et al., 2016), the contribution of this article is three-fold: firstly, a terminology based on a consideration of the diverse nomenclature in literature is introduced in order to unify, define, and standardize CPPS entity terms. Secondly, a taxonomy classifies the identified terms using 'is-a relationships'. Thirdly, based on the terminology and taxonomy, a reference model (Figure 4) illustrates abstract relations – i.e., associations and aggregations – between CPPS entities using Unified Modeling Language (UML) class diagrams.

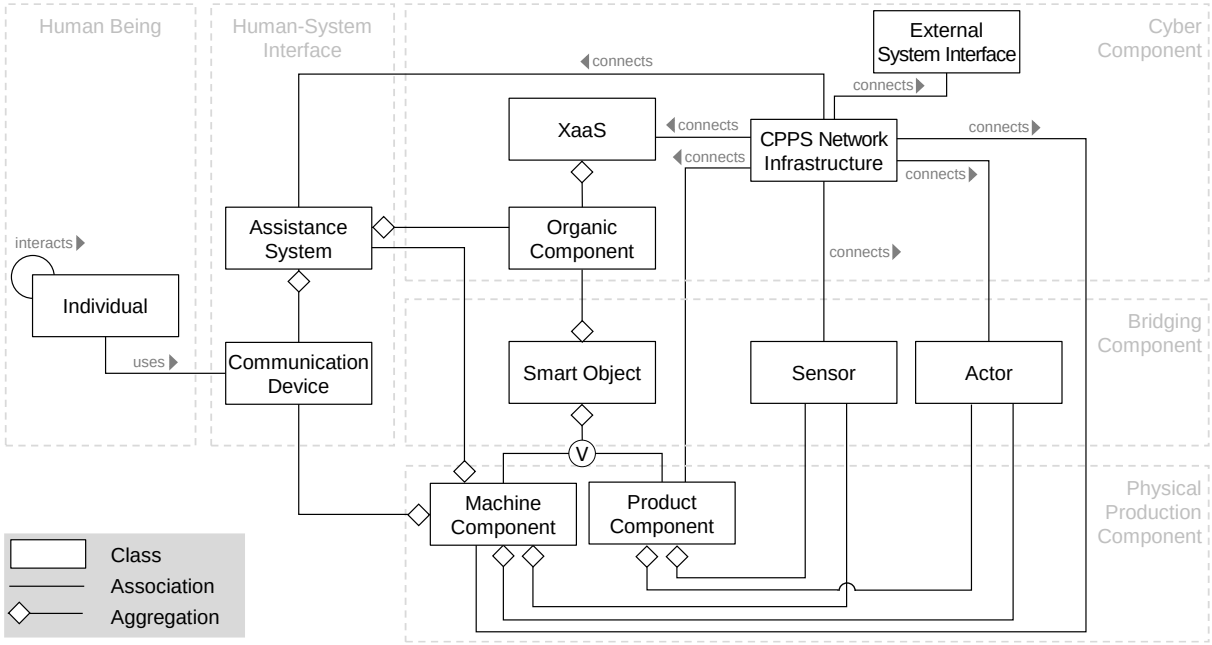

Figure 4. Reference Model for Cyber-physical Production Systems

The proposed artefacts for CPPSs were developed and evaluated based on the iterative development process of Nickerson et al. (2013). The iteration steps build on an extensive literature review, the co-authors findings from internal discussions, and the feedback from focus group discussions and interviews with industry experts. To demonstrate its efficacy and general applicability, the reference model was instantiated in the course of three fictional application scenarios featuring differing levels of distributed smartness. In order to demonstrate its practical relevance, the reference model was also used to illustrate a CPPS from a real-world model factory.

In sum, research article #2 concretizes the idea of CPPSs with regard to more mature modeling approaches. The combination of detailed definitions and classification of CPPS entities, as well as the abstract illustration of their relationships, enables the modeling of various CPPS layouts and associated capabilities. CPPSs are the core technology in smart factories, making a better understanding of CPPSs a necessary starting point for further exploration of technology-driven threats and opportunities in the industrial sector.

In particular, architectural knowledge about the structure and functioning of CPPSs supports the identification of possible risk sources, such as attacks and errors, along with the analysis of their propagation and associated effects on the overall system, e.g., in terms of availability (Section II.2). Improved risk management thereby reduces the potential of financial losses and supports profound decision-making regarding prioritization in risk control and investments in mitigation measures. At the same time, insights about CPPS entities and their capabilities enable the identification of opportunities, such as ecological benefits (Section II.3), and the corresponding changes in production and business processes necessary in order to realize those benefits.

2 Identifying and Analyzing Technology-driven Threats

As discussed in the previous section, digital technologies are changing individuals, organizations, and society at unprecedented speed and scale. Organizations are riding the digital wave, attempting to increase their profitability by adopting digital technologies that enable new operating and business models. Today, almost everything that improves the efficiency and competitiveness of an organization involves digital systems and networks. However, these technology-driven systems are increasingly vulnerable to IT security threats (Tupa et al., 2017).

In industry, smart factories rely on technologies such as CPPSs or the Industrial Internet of Things, which significantly differ from conventional IT systems (Alaba et al., 2017; Frustaci et al., 2018). Due to the high number, heterogeneity, openness, and interconnectedness of decentralized products, machines, and devices, smart factories are complex and opaque systems (Frustaci et al., 2018). Moreover, industrial production often builds on existing systems featuring outdated security technologies (Sadeghi et al., 2012), and adds components with limited hardware and software resources (Frustaci et al., 2018; Jing et al., 2014) that are linked through insecure connections (Lu et al., 2014). This expands the 'surface area' exposed to cyber-attacks by offering targets and entry points for conventional and technology-specific, emerging IT attacks (Alaba et al., 2017). Thereby, conventional attacks might have different impacts on CPPSs or the Industrial Internet of Things than on conventional IT systems, especially because air gaps, i.e., the physical or logical separation of two or more IT systems, are increasingly being removed. At the same time, the probability of unintentional or negligent disruptions and errors occurring increases (Broy et al., 2012).

From a risk management perspective, the continuing trend towards more sophisticated, multi-stage security incidents (Ervural and Ervural, 2018) complicates the implementation of appropriate mitigation measures. As a consequence, more than half of successful attacks lead to operational interruptions such as downtimes within production processes (BSI, 2017), eventually entailing physical damage or even posing a threat to human life (Bhamare et al., 2020). Since digital technologies are deeply embedded in highly connected and automated operation systems, a single security incident increases the potential damage (Accenture, 2018a). Hence, organizations increasingly face the challenge of protecting their production systems. A structuring approach is therefore required to support the systematic identification, analysis, and documentation of conventional and emerging attacks.

Although the current literature encompasses a variety of classification schemes for conventional attacks, it lacks an integrated and systematic approach that elaborates on the particularities of smart factory technologies and considers conventional and emerging attacks alike. As a result, organizations still lack an overview of potential attacks and associated characteristics (Kaspersky, 2017), which is nonetheless needed to identify and analyze attacks and to derive appropriate mitigation measures (Shirazi et al., 2014; Spreitzer et al., 2018). In order to address this need, research article #3 proposes a multi-layer

taxonomy of attacks on the Industrial Internet of Things, which can be used to distinguish relevant attack characteristics. In line with the iterative development process of Nickerson et al. (2013), the taxonomy was developed deductively and inductively by drawing on an extensive literature review, insights from expert interviews with practitioners from ten organizations involved in IT security, and the classification of a sample including over 50 real-world attacks. The taxonomy was evaluated in discussions with co-authors and industry experts, using established evaluation criteria from design science research.

As there is a continuing trend toward more sophisticated, multi-stage incidents (Ervural and Ervural, 2018), the taxonomy ensures consistency by focusing on individual attacks as the smallest unit of an incident. Hence, incidents have to be subdivided into attacks to be analyzed in more detail. The taxonomy (Figure 5) comprises three layers, which allow it to characterize attacks in detail: the 'method of operation' describes the procedure used by an attacker (Kjaerland, 2005) to achieve an 'impact' (CERT, 2004; Howard and Longstaff, 1998) on a desired 'target' (Howard and Longstaff, 1998). Each layer includes several dimensions, whereby the 'method of operation' specifically focuses on the procedure and behavior of the attacker, and tools and ways used to perform an attack (CERT, 2004; Kjaerland, 2005). The 'target' level illuminates the attack surface from an organizational and architectural perspective. Finally, the effect of an attack is summarized in the 'impact' layer.

Layer	Dimension	Characteristic				Exclusivity *
Method of Operation	Technique	Physical		Logical		ME
	Mechanism	Active		Passive		ME
	Executability	Stand-alone		Coupled		ME
	Focus	Undirected		Directed		ME
Target	Vulnerability	Technical		Social		NE
	IoT Level	Perception Level	Network Level	Application Level		NE
Impact	Consequence	Disclosure	Deception	Disruption	Usurpation	NE
	Scope	Cyber		Cyber-physical		ME

* ME: Mutually Exclusive; NE: Non-Exclusive

Figure 5. Multi-layer Taxonomy of Attacks on the Industrial Internet of Things

To demonstrate the applicability and practical relevance of the results, a real-world incident was analyzed. As it is one of the rare multi-stage incidents about which information is publicly available, the incident in a German steel facility from 2014 (Lee et al., 2014) was selected. The example demonstrates that the taxonomy is suitable for the detailed analysis of such incidents.

The results of this study further the understanding of attacks on the Industrial Internet of Things and provide insights for IT security management. From an academic point of view, the article adds to the descriptive knowledge, providing the first approach capable of consistently describing and comparing complex attacks and incidents in technology-driven, highly interconnected systems. From a practical

perspective, the taxonomy enables organizations to systematically identify, collect, and analyze information on attacks. As uniform guidelines for incident reporting among various security teams have not yet been established (Zuech et al., 2015), the taxonomy supports the standardized intra- and inter-organizational documentation and communication of attacks. The subdivision of incidents into attacks enables the recognition of attack patterns, which is beneficial for the derivation of appropriate countermeasures in IT security.

In smart factories, physical production processes increasingly require information from underlying information networks to enable the flexible production of customized products (Radziwon et al., 2014). Due to the increasing use of information in production processes, the information network within smart factories is, in particular, vulnerable to disruption (Pasqualetti et al., 2013). These disruptions may result from intentional IT attacks – as discussed in research article #3 – or unintentional errors, and can affect the availability of both the information and the production network (Broy et al., 2012). To protect systems from disruptions, the goals of traditional IT security management followed the CIA-triad, whereby (1) *confidentiality* involves restrictions on access to and disclosure of data, (2) *integrity* ensures protection against the improper alteration or destruction of data, and (3) *availability* describes the timely and reliable access to and use of data (Dempsey et al., 2011). With (close to) real-time requirements and the high degree of interconnectivity, smart factories become most vulnerable to availability threats (Amiri et al., 2014; Cardenas et al., 2008; Lee, 2008).

The high level of interconnectivity within smart factories facilitates threat propagation (Smith et al., 2007), eventually resulting in the collapse of entire systems (Amiri et al., 2014). Concepts like just-in-time and just-in-sequence additionally amplify propagation effects, further increasing the potential damage. As extant approaches have proven insufficient for depicting the specific characteristics of smart factory networks and simulating propagation effects, a modeling approach is needed to grasp availability risks as a basis for decision-making regarding information and production network layouts and the derivation of mitigation measures (Amin et al., 2013; Dempsey et al., 2011; Frustaci et al., 2018; Vavra and Hromada, 2015).

Against this backdrop, research article #4 addresses the issue of analysing and simulating availability risks of IT threats in smart factory networks. In line with the design science research methodology of Peffers et al. (2007), the modeling approach elaborates on the effects that IT threats have on production processes by enabling the modeling of smart factory network architectures and the simulation of attack and error occurrence and propagation. Using Petri Nets (Petri, 1966) and multiple extensions, e.g., Timed Coloured Petri Nets (Ha and Suh, 2008) and Generalised Stochastic Petri Nets (Valk, 2008), the modeling approach offers modular components to model smart factory networks which comprise an information network and a production network (Figure 6). The information network is formed of modular information components that build information layer hierarchies. Once an information component is affected by an attack or error,

the failure propagation follows an exponential distribution and cascades through the information network and may even extend to the production network.

The article also identifies and discusses various factors influencing propagation effects, i.e., redundancy within the production network, redundancy within the information network, and the smartness of production machines; these serve as a basis for modeling and analyzing different smart factory network architectures.

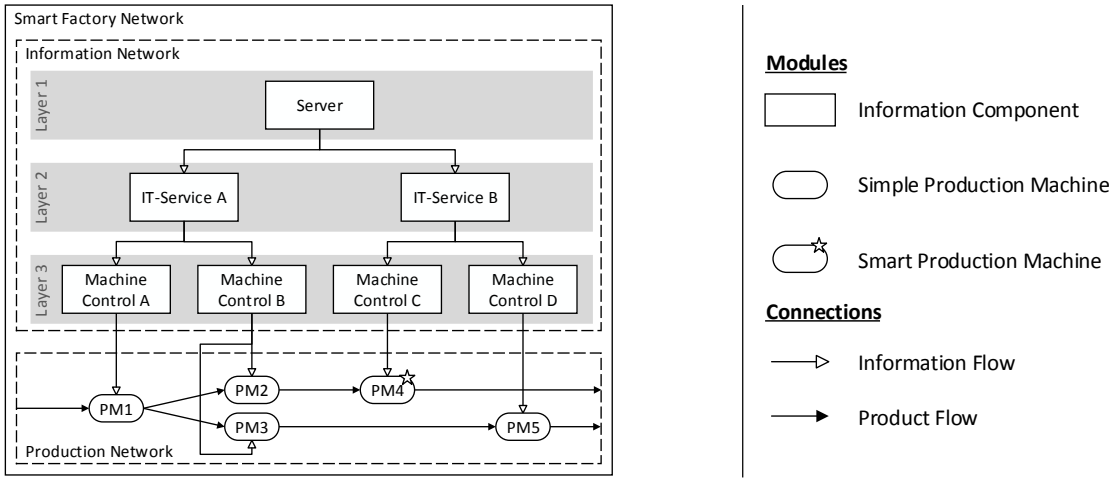

Figure 6. Exemplary Layout of a Smart Factory Network

The modeling approach was evaluated via its application in artificial and naturalistic settings. For the real-world scenario, the production environment of a German manufacturer of customized milling and turning machines was simulated and analyzed in terms of productivity and the availability of information components and production machines under varying conditions. By enabling the modeling and analysis of IT availability threats, the modeling approach supports production managers and IT security experts in their efforts to identify critical components and dependencies within smart factory networks. The approach thus enables risk managers to make well-founded decisions on appropriate mitigation measures.

3 Identifying and Managing Technology-driven Opportunities

In addition to the threats described in the previous section, technologies present manifold opportunities in industry. The main idea of Industry 4.0 relates to the integration of digital technologies into manufacturing systems in order to increase performance (Kagermann et al., 2013; Wang et al., 2016). In this context, performance is operations-related, product-related, or represents general performance in terms of global challenges such as sustainability (Dalenogare et al., 2018; Fitzgerald et al., 2014; Gimpel and Röglinger, 2015). With concepts like decentralization, autonomy, and self-organization in real-time, industrial technologies (e.g., CPPSs) enable more efficient and flexible processes, raising the operational performance of an organization (Brettel et al., 2014; Lasi et al., 2014; Radziwon et al., 2014). At the same time, organizations are able to raise the quality and diversity of customized products via the use of digital technologies. General performance often relates to sustainability, which is divided into ecological, economical, and social aspects. In times of climate change, the industry is, in particular, responsible for reducing its ecological footprint. The industrial energy demand, which already accounts for more than 55% of the global energy consumption, is expected to grow by a further 18% in the next twenty years (U.S. Energy Information Administration, 2017).

Although the technological advancements in industry hold huge potential for reducing environmental impact (Dalenogare et al., 2018; Wang et al., 2016), industrial production still uses nonrenewable resources and contributes to pollution and climate warming. When it comes to technological investment decisions, ecological benefits are still rarely seen as the primary objective, but as merely a positive side-effect (Dalenogare et al., 2018). In literature, the topics of technology (Atzori et al., 2010; Chan et al., 2018; Tao et al., 2018) and ecology (Despeisse et al., 2012; Geng et al., 2017) are being discussed in isolation from one another, with an integrated approach still lacking. As the dependencies between these two domains are complex, it remains unclear how technology and ecology are related. In addition, becoming digital includes more than plugging in technology: the redefinition of processes and the organizational structure is a key element for successful digital transformation (Davenport and Westerman, 2018). Hence, it must be examined how organizations might transform their processes in order to realize desired ecological benefits. This is especially important as technology changes faster than organizations (Relihan, 2019).

In this regard, research article #5 aims to systematically identify ecological benefits, associated digital technologies, and necessary business changes in the manufacturing context. In line with the design science research methodology of Peffers et al. (2007), the article takes a triple-punch approach: firstly, the Benefits Dependency Network (Ward and Daniel, 2006) from benefits management is introduced, which is designed to "improve the likelihood of successful results in digital investments" (Peppard, 2016). The framework asks the intended users to answer the following questions: why is an investment being made, what changes are needed to achieve desired benefits, and how are these changes enabled by technology? In line with Ward and Daniel (2006), the Benefits Dependency Network distinguishes

five dimensions: the ‘Investment Objectives’ address the organization’s drivers, i.e., internal and external aspects of the business environment, such as financial benefits or market trends, and ensure that a project contributes to the organization’s strategic future goals. ‘Business Benefits’ represent advantages which are associated with corresponding ‘Investment Objectives’. Those benefits and objectives will only be realized if permanent changes – i.e., ‘Business Changes’ – or one-off changes – i.e., ‘Enabling Changes’ – are implemented. These (structural) changes affect the business and production processes of organizations. Finally, ‘IS/IT Enabler’ represents the technological foundation for the realization of the described changes. In general, the Benefits Dependency Network is developed from right to left in order to align the applied technology with the organization’s goals. In line with King (2011), however, this approach also enables a technology-driven development direction from left to right.

In a second step, the Benefits Dependency Network is transferred to the context of ecological sustainability in the industry. To guide intended users in identifying technology-driven opportunities in terms of ecological benefits and underlying technologies, building blocks are provided (Figure 7). Building on and extending the literature on green manufacturing principles (Despeisse et al., 2012) and technological advancements in the industry (Dalenogare et al., 2018), the building blocks represent exemplary technologies, organizational changes, and ecological benefits for each dimension. Although the building blocks do not depict every possible technology, change, or benefit, and have to be adapted to specific use cases, they simplify the application of the Benefits Dependency Network for intended users and support such users in creating instantiations of their own projects.

Thirdly, the feasibility and effectiveness of the Benefits Dependency Network are demonstrated by providing instantiations from practice. In particular, the case of a company that uses additive manufacturing – i.e., 3D sand printing to produce sand moulds – shows that the framework not only supports the identification of technology-based ecological benefits but also reveals at what stage of the product lifecycle these benefits are realized. In this case, the ecological benefits were generated not during the production process but as part of the product and material life cycle.

The framework was evaluated from ex-ante and ex-post perspectives by applying the four evaluation activities as per Sonnenberg and vom Brocke (2012). Thus, the Benefits Dependency Network was developed and evaluated in multiple rounds with both researchers – i.e., discussions with focus groups – and practitioners – i.e., interviews with experts. Furthermore, the Benefits Dependency Network was applied in both artificial and naturalistic settings. The interdisciplinary approach combines the knowledge of different domains and contributes to the descriptive knowledge of technology-driven opportunities. The overall contribution is a framework that guides intended users in taking novel perspectives on the ecological benefits of digital technologies in the industry. With this, the Benefits Dependency Network provides a basis for sound investment decisions, in which ecological considerations play an increasingly important role.

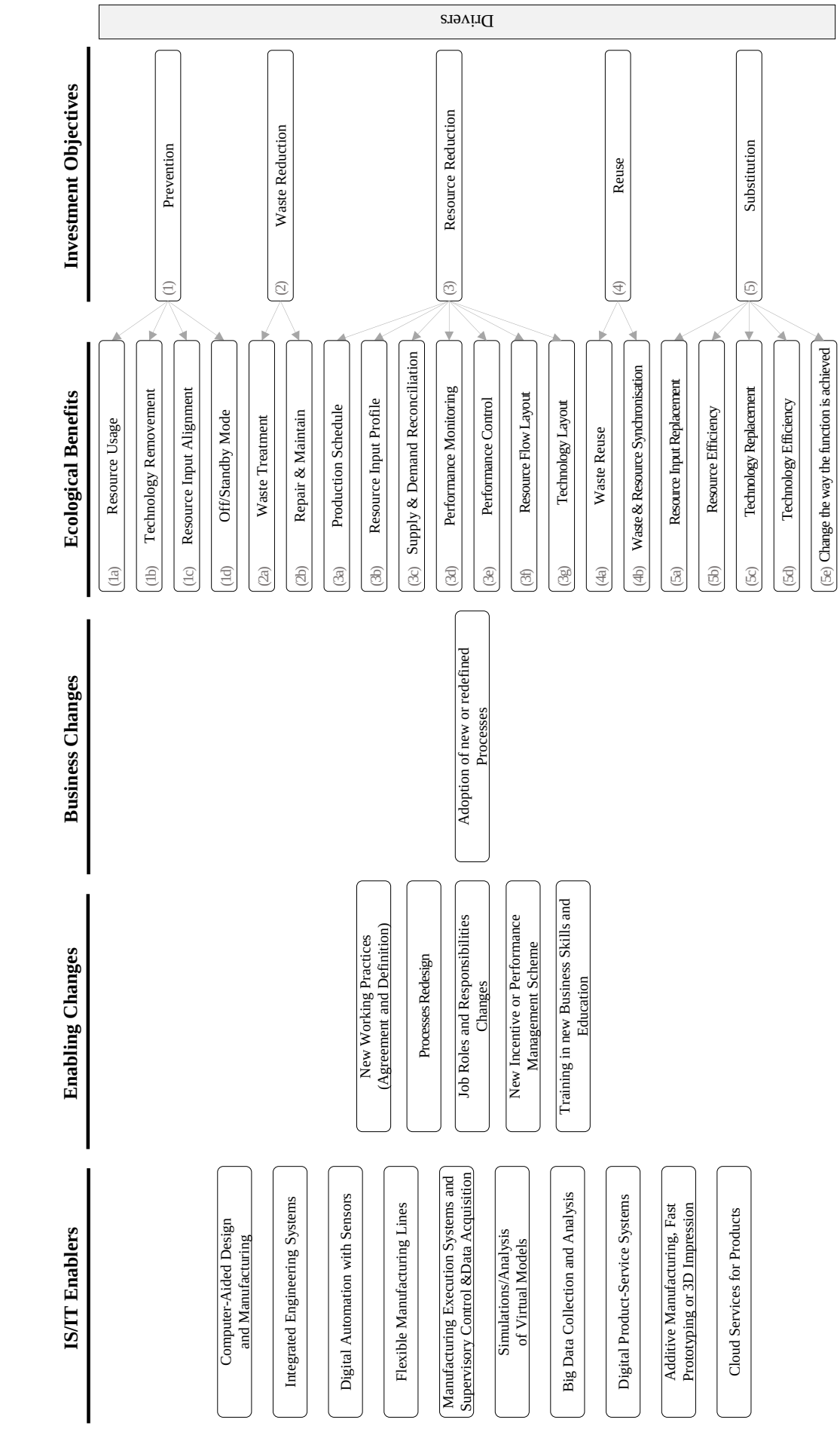

Figure 7. Resulting Benefits Dependency Network with exemplary Building Blocks

III. Conclusion[3]

1 Summary

Digitalization is driven by the rapid emergence and adoption of digital technologies, changing individuals, organizations, and society on a global scale. Although digital technologies have been around for almost half a century, increases in their number, variety, impact, and diffusion are all currently gaining further momentum. Within this highly volatile environment, researchers and practitioners increasingly struggle to understand and leverage digital technologies. This hampers scientific progress and decision-making in industry. Addressing calls for structure to be brought to the field (Bharadwaj et al., 2013), this doctoral thesis provides a common understanding of digital technologies as a foundation for taking different perspectives on technology-driven threats and opportunities in the industrial sector. Firstly, organizations have to understand digital technologies in general, and manufacturing technologies in particular, to fully tap their economic and social potential. Secondly, the high degree of cross-linking and decentralization accompanying different technologies increases the complexity of industrial systems. Therefore, the thesis examines vulnerabilities and threats evoked by technology. Thirdly, this thesis elaborates on ecological opportunities enabled by digital technologies in the industry.

Regarding the overarching topic of *Understanding Digital Technology*, Section II.1 examines digital technologies by providing in-depth insights on their nature, and by discussing entities and relations within CPPSs as the most important technologies in manufacturing. Research article #1 aims to provide a clear understanding of digital technologies via the identification of similarities and differences as a prerequisite for their further use in sound scientific methods and applications (McKelvey, 1978; Posey et al., 2013). Drawing on a sample of 92 digital technologies from the Gartner Hype Cycle for Emerging Technologies (Gartner Inc., 2017, 2016, 2015, 2014, 2013, 2012, 2011, 2010, 2009) and an extensive literature review as justificatory knowledge, the resulting taxonomy distinguishes eight dimensions and associated characteristics, which are structured cross four layers of an established digital technology architecture (Yoo et al., 2010). Based on the subsequent classification of the sample, the hierarchical cluster analysis (Ward, 1963) results in nine digital technology archetypes, each representing a group of digital technologies with similar characteristics. Both the taxonomy and archetypes add to the descriptive knowledge of digital technologies and serve as a foundation for further sense-making and design-oriented research (Gregor, 2006; Gregor and Hevner, 2013). Focusing on the industrial sector, research article #2 deepens the technological perspective by elaborating on CPPSs which are applied within smart factories. Building on and extending current CPPS literature, a terminology, taxonomy, and reference model are presented as a foundation for creating general models of machines, processes, and production (Hellinger and Seeger, 2011; Kagermann et al., 2013). Thereby, the terminology unifies,

[3] This section partly comprises content from the thesis' research articles. To improve the readability of the text, I omit the standard labelling of these citations.

defines, and standardizes the CPPS nomenclature, while the taxonomy groups the identified CPPS entities. As the core of this article, the reference model illustrates abstract relationships between CPPS entities using UML class diagrams. With this, research article #2 meets the demand for more mature and appropriate CPPS modeling approaches (Vogel-Heuser et al., 2014) and creates a common technological understanding, which enables the modeling of various CPPS layouts and associated capabilities. With this, the further exploration of technology-driven threats – e.g., the identification of risk, such as attacks, errors, and their propagation – and opportunities – e.g., the benefits of technology use – becomes feasible in the industrial sector.

On the topic of *Identifying and Analyzing Technology-driven Threats*, Section II.2 discusses the vulnerabilities of new systems based on digital technologies and associated challenges of IT security in the industry. Taking a risk perspective, IT attacks and their effects on highly cross-linked information and production systems are discussed in detail. In this regard, research article #3 elaborates on the typical characteristics of attacks on industrial technologies and systems. The developed taxonomy conceptualizes characteristics, dimensions, and layers of attacks on the Industrial Internet of Things, drawing on a sample of over 50 attacks, interviews with researchers and practitioners, and relevant work on IT attacks as justificatory knowledge. Splitting IT security incidents into single attacks enables the recognition of attack patterns, which is useful for the derivation of appropriate countermeasures. As there are, so far, no established, uniform guidelines for incident reporting (Zuech et al., 2015), the taxonomy supports researchers and organizational stakeholders in systematically identifying, collecting, analyzing, and sharing information on attacks. Thereby, the taxonomy adds to the descriptive knowledge in the field of IT security. Research article #4 complements the risk perspective on technology-driven threats by analysing and simulating availability risks in smart factory networks. In particular, the Petri Net-based modeling approach elaborates on the effects of IT attacks on production processes by enabling the modeling of various smart factory network architectures, and the simulation of attack and error occurrence and propagation. The modeling approach supports production managers, security experts, risk managers, and IT architects in identifying critical network components and dependencies as a basis for sound and transparent decisions on appropriate mitigation measures.

With regard to *Identifying and Managing Technology-driven Opportunities*, Section II.3 elaborates on the industrial application of technology for environmental purposes. More precisely, research article #5 supports the identification of cause-effect relationships between ecology and technology by applying and further developing the Benefits Dependency Network (Ward and Daniel, 2006) from benefits management. This framework structures drivers of change along with associated objectives, business changes, and underlying technologies. Drawing on relevant literature from sustainability and technology, e.g., green manufacturing principles (Despeisse et al., 2012) and digital technologies in the industry (Kang et al., 2016), the article introduces exemplary building blocks for technologies, business changes, and ecological benefits to support intended users from research and practice in creating

concrete Benefits Dependency Network instantiations of their specific use-cases. In addition to supporting the identification phase, the framework can also be used to evaluate the progress of digitalization projects in industrial organizations. Thereby, the framework helps to provide structured descriptions of the interrelationships between technology and ecological benefits, and thus provides additional transparency for investment decisions. It also forces intended users to identify and understand the changes required for a successful digital transformation. By combing and extending knowledge from different domains, this interdisciplinary approach contributes to the descriptive knowledge of technology-driven opportunities.

2 Future Research

As any research project, this doctoral thesis is beset with some limitations that will stimulate future research. In the following, an overview is provided which discusses these limitations and makes recommendations for advancing research about information systems on digital technology, and associated threats and opportunities in the industry. Further details are described in the individual research articles.

In the section on *Understanding Digital Technologies*, research article #1 and #2 deductively and inductively develop and evaluate the resulting artefacts – i.e., terminology, taxonomy, archetypes, and reference model – and draw on academic and professional literature as justificatory knowledge. This includes, *inter alia*, state-of-the-art definitions of and literature on digital technologies (e.g., Yoo et al., 2010) and CPPSs (e.g., Penas et al., 2017), technology reports and trends compiled by management consultancies and market research institutions (e.g., Deloitte, Forbes, or Forrester), and a sample of 92 digital technologies from the Gartner Hype Cycle for Emerging Technologies from 2009 to 2017. Digitalization, however, is a fast-moving field. Ever-shorter development cycles and time-to-market result in the emergence of countless new technologies every year, which is further reinforced by the combination of extant technologies (Arthur, 2009). At the same time, once-hyped technologies disappear, e.g., ‘broadband over power lines’ (Gartner Inc., 2010). To cope with this highly volatile, uncertain, complex and ambiguous environment (Bennett and Lemoine, 2014), efforts to advance research activities should focus on repeatedly adjusting and re-evaluating the presented artefacts, and should also integrate new insights from theory and practice. This is in line with organizational systematics (McKelvey, 1982, 1978), which proclaims that the ‘theory of diversity’ includes the development of taxonomies and archetypes, as well as tracking the evolution of objects of interest, i.e., digital technology, over time. Follow-up research should therefore update and enlarge the sample size, including extant and emerging technologies. Moreover, the application of technology in additional real-world use-cases and studies is encouraged. In particular, the archetypes of digital technologies, as well as the CPPS reference model, should be used in defined fields of application in order to test their robustness and practical relevance. This increases the stability and generality of the results and helps to

obtain a holistic view on the diversity of digital technologies. Finally, the use of emerging digital technologies opens up new possibilities regarding the design of innovative products and processes, which should be explored.

In the manufacturing industry, in particular, technological advancement and digital disruption entail massive changes (Govindarajan and Immelt, 2019; Urbach and Röglinger, 2019). This puts pressure on industrial organizations to transform themselves in order to remain competitive (Ciriello et al., 2018; Fang et al., 2018; Fichman et al., 2014). However, digitalization concepts and digital technologies do also affect multiple other industries, such as the automotive, avionics, energy, transportation, and health care industries (Ahmed et al., 2013). Hence, future endeavours should transfer the findings of this thesis regarding digital technologies and Cyber-physical (Production) Systems to other industries, and *vice versa*, in order to promote the sharing of experiences and knowledge among researchers and practitioners.

In the industry, *Identifying and Analyzing Technology-driven Threats* is a first step towards risk and IT security management within smart factories. Research article #3 and #4 focus on the description and simulation of intentional attacks, unintentional errors, and their propagation within industrial systems such as the Industrial Internet of Things and smart factory networks. Future research should use this as a starting point for the further development of IT security management concerning the derivation of mitigation measures. Moreover, the concepts lack validation with real-world data and in real-world settings. This is because the majority of organizations conceal information on attacks to avoid image loss. Initially, future research should, therefore, concentrate on investigating IT security threats to model factories, and thereby convince organizations of the added value of IT security research for industrial application. In addition, IT security always lags behind technological innovation, which increases the risk posed by new, unknown vulnerabilities, targets, and attacks. Hence, there is an urgent need for continuous research activities regarding the expansion and adjustment of extant models and their transformation into suitable IT security tools. In particular, there is a need for research involving organizations themselves. Only by working closely together will research and practice be able to keep up with the growing number and increasing power of attackers. On the other hand, professional cooperation with hackers is also conceivable, as they have considerable knowledge in the area of attacks and are experienced in dealing with the latest technology. Research article #4 focusses on availability risks. Although availability is the most critical threat within smart factories (Amiri et al., 2014; Cardenas et al., 2008; Lee, 2008), future works should incorporate other IT security goals, such as integrity and confidentiality, as violations of such goals often remain unnoticed for a longer time and might, therefore, cause more damage. On a more general level, the threats to digital technologies discussed herein mainly concern IT risk and security management. However, multiple other areas in manufacturing are likewise disrupted and well worth exploring, e.g., technology-driven change of work and employment, including work design, qualification measure, and employment-oriented work and qualification policy.

With regard to sustainability, *Identifying and Managing Technology-driven Opportunities* is an increasingly important field emerging in global awareness. The Benefits Dependency Network is an appropriate tool for identifying and managing cause-effect relations between technologies, associated business changes, and ecological benefits. However, the efficient use of resources by means of 'green' technology often implies side-effects such as the rebound effect, which should be subject to further research. The rebound effect refers to the phenomenon that new technologies, which increase resource use efficiency, might cause behavior that reduces or even reverses its expected benefits. Ideally, future endeavors should focus on embedding the Benefits Dependency Network into a corporate sustainability strategy. In addition to ecological activities, this strategy should also pool, link, and control economic and social sustainability initiatives. While economic sustainability aims to support long-term economic growth by purchasing local goods or using recycled material without harming the environment or society, social sustainability refers to practices that support cultural aspects, such as social and health equity, human and labor rights, and social justice. Only a holistic view of the three pillars of sustainability enables the meaningful depiction of a company's sustainability efforts and serves as a basis for well-founded strategy and investment decisions. Just as with threats, there are other worthwhile technology-driven opportunities besides sustainability, such as the digital transformation and innovation of business models and processes, which should be examined and researched in the future.

In sum, the unprecedented speed and scale of technological advancement continue to increase. As a result, research and practice will face novel threats and opportunities in the near future. With this thesis, I hope to encourage researchers and practitioners to join the interdisciplinary endeavour of shedding light on the highly relevant field of digitalization in order to leverage digital technologies and move towards fully tapping their economic and social potential.

IV. Publication Bibliography

Accenture, 2018a. Build pervasive cyber resilience now: Securing the future enterprise today - 2018. https://www.accenture.com/_acnmedia/pdf-81/accenture-build-pervasive-cyber-resilience-now-landscape.pdf (accessed 22 January 2020).

Accenture, 2018b. Cyber threatscape report 2018: Midyear cybersecurity risk review. https://www.accenture.com/_acnmedia/pdf-83/accenture-cyber-threatscape-report-2018.pdf (accessed 21 January 2020).

Accenture, 2019a. Industry X.0: The remaking of industries, explained. https://www.accenture.com/gb-en/insights/industry-x-0/reinvention-of-industries (accessed 21 January 2020).

Accenture, 2019b. Technology vision 2019: The post-digital era is upon us. Accenture. https://www.accenture.com/_acnmedia/pdf-97/accenture-technology-vision-2019-executive-final-brochure.pdf (accessed 27 January 2020).

Adomavicius, G., Bockstedt, J.C., Gupta, A., Kauffman, R.J., 2008. Making sense of technology trends in the information technology landscape: A design science approach. MIS Quarterly 32 (4), 779–809. https://doi.org/10.2307/25148872.

Ahmed, S.H., Kim, G., Kim, D., 2013. Cyber physical system: Architecture, applications and research challenges, in: Proceedings of the IFIP 2013 Wireless Days, Valencia, Spain, pp. 1–5.

Akanmu, A.A., Anumba, C.J., Messner, J.I., 2012. An RTLS-based approach to cyber-physical systems integration in design and construction. International Journal of Distributed Sensor Networks 8 (12), 1–11. https://doi.org/10.1155/2012/596845.

Akyildiz, I.F., Kasimoglu, I.H., 2004. Wireless sensor and actor networks: Research challenges. Ad Hoc Networks 2 (4), 351–367. https://doi.org/10.1016/j.adhoc.2004.04.003.

Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F., 2017. Internet of Things security: A survey. Journal of Network and Computer Applications 88, 10–28. https://doi.org/10.1016/j.jnca.2017.04.002.

Al-Natour, S., Benbasat, I., 2009. The adoption and use of IT artifacts: A new interaction-centric model for the study of user-artifact relationships. Journal of the Association for Information Systems 10 (9), 661–685. https://doi.org/10.17705/1jais.00208.

Alter, S., 2018. System interaction theory: Describing interactions between work systems. Communications of the Association for Information Systems 42 (9), 233–267. https://doi.org/10.17705/1CAIS.04209.

Amin, S., Schwartz, G.A., Hussain, A., 2013. In quest of benchmarking security risks to cyber-physical systems. IEEE Network 27 (1), 19–24. https://doi.org/10.1109/MNET.2013.6423187.

Amiri, A., Cavusoglu, H., Benbasat, I., 2014. When is IT unavailability a strategic risk? A study in the context of cloud computing, in: 35th International Conference on Information Systems, Auckland, New Zealand.

Arthur, W.B., 2009. The nature of technology: What it is and how it evolves, 1st ed. Free Press, New York.

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of Things: A survey. Computer Networks 54 (15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010.

Baroudy, K., Kishore, S., Nair, S., Patel, M., 2018. Unlocking value from IoT connectivity: Six considerations for choosing a provider. McKinsey & Company.

Bennett, N., Lemoine, G.J., 2014. What a difference a word makes: Understanding threats to performance in a VUCA world. Business Horizons 57 (3), 311–317. https://doi.org/10.1016/j.bushor.2014.01.001.

Berger, S., Denner, M.-S., Röglinger, M., 2018. The nature of digital technologies - Development of a multi-layer taxonomy, in: Proceedings of the 26th European Conference on Information Systems, Portsmouth, UK, pp. 1–18.

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., Meskin, N., 2020. Cybersecurity for industrial control systems: A survey. Computers & Security 89, 101677. https://doi.org/10.1016/j.cose.2019.101677.

Bharadwaj, A., El Sawy, O.A., Pavlou, P.A., Venkatraman, N.V., 2013. Digital business strategy: Toward a next generation of insights. MIS Quarterly 37 (2), 471–482. https://doi.org/10.25300/MISQ/2013/37:2.3.

BlackRock, 2020. A fundamental reshaping of finance. https://www.blackrock.com/uk/individual/larry-fink-ceo-letter (accessed 30 January 2020).

Bødker, S., 1987. Through the interface: A human activity approach to user interface design. DAIMI Report Series 16 (224). https://doi.org/10.7146/dpb.v16i224.7586.

Brettel, M., Friederichsen, N., Keller, M., Rosenberg, M., 2014. How virtualization, decentralization and network building change the manufacturing landscape: An Industry 4.0 perspective. International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering 8 (1), 37–44.

Broy, M., Cengarle, M.V., Geisberger, E., 2012. Cyber-physical systems: Imminent challenges, in: Large-Scale Complex IT Systems. Development, Operation and Management. Monterey Workshop 2012. Lecture Notes in Computer Science, vol. 7539. Springer, Berlin, Heidelberg, pp. 1–28.

BSI, 2017. Cyber-Sicherheits-Umfrage 2017: Cyber-Risiken, Meinungen und Maßnahmen. https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3 (accessed 27 January 2020).

Buck, C., Eder, D., 2018. The impact of digitization on business models: A systematic literature review, in: Proceedings of the 24th Americas Conference on Information Systems, New Orleans, USA, pp. 1–10.

Buschmeyer, A., Schuh, G., Wentzel, D., 2016. Organizational transformation towards product-service systems — Empirical evidence in managing the behavioral transformation process. Procedia CIRP 47 (1), 264–269. https://doi.org/10.1016/j.procir.2016.03.224.

Cardenas, A.A., Amin, S., Sastry, S., 2008. Secure control: Towards survivable cyber-physical systems, in: 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, pp. 495–500.

CERT, 2004. Insider threat study: Illicit cyber activity in the banking and finance sector. http://www.cert.org/archive/pdf/bankfin040820.pdf (accessed 12 January 2018).

Chan, H.K., Griffin, J., Lim, J.J., Zeng, F., Chiu, A.S.F., 2018. The impact of 3D printing technology on the supply chain: Manufacturing and legal perspectives. International Journal of Production Economics 205, 156–162. https://doi.org/10.1016/j.ijpe.2018.09.009.

Chapple, C., 2020. Pokémon GO has best year ever in 2019, catching nearly $900 million in player spending. https://sensortower.com/blog/pokemon-go-has-best-year-ever-in-2019-catching-nearly-900m-usd-in-player-spending (accessed 18 February 2020).

Chen, H., 2017a. Applications of cyber-physical system: A literature review. Journal of Industrial Integration and Management 2 (3), 1750012. https://doi.org/10.1142/S2424862217500129.

Chen, H., 2017b. Theoretical foundations for cyber-physical systems: A literature review. Journal of Industrial Integration and Management 2 (3), 1750013. https://doi.org/10.1142/S2424862217500130.

Ciriello, R.F., Richter, A., Schwabe, G., 2018. Digital innovation. Business & Information Systems Engineering 60 (6), 563–569. https://doi.org/10.1007/s12599-018-0559-8.

Clark, G., 2003. The disruption opportunity. MIT Sloan Management Review 44 (4), 1–27.

Dalenogare, L.S., Benitez, G.B., Ayala, N.F., Frank, A.G., 2018. The expected contribution of Industry 4.0 technologies for industrial performance. International Journal of Production Economics 204, 383–394. https://doi.org/10.1016/j.ijpe.2018.08.019.

Davenport, T.H., Westerman, G., 2018. Why so many high-profile digital transformations fail. Harvard Business Review 9 (15), 1–5.

Dempsey, K., Chawla, N.S., Johnson, A., Johnston, R., Jones, A.C., Orebaugh, A., Scholl, M., Stine, K., 2011. Information security continuous monitoring for federal information systems and organizations. U.S. Department of Commerce.

Denner, M.-S., Püschel, L., Röglinger, M., 2018. How to exploit the digitalization potential of business processes. Business & Information Systems Engineering 60 (4), 331-349. https://doi.org/10.1007/s12599-017-0509-x.

Despeisse, M., Ball, P.D., Evans, S., 2012. Modelling and tactics for sustainable manufacturing: An improvement methodology, in: Seliger, G. (Ed.), Sustainable Manufacturing. Springer, Berlin, Heidelberg, pp. 9–16.

Doan, M., 2019. Companies need to rethink what cybersecurity leadership is. Harvard Business Review. https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is (accessed 21 January 2020).

Elsevier, 2019. New technologies in operations and supply chain: Implications for sustainability. Call for papers. https://www.journals.elsevier.com/international-journal-of-production-economics/call-for-papers/new-technologies-in-operations-and-supply-chain-implications (accessed 10 October 2019).

Ervural, B.C., Ervural, B., 2018. Overview of cyber security in the Industry 4.0 era, in: Ustundag, A., Cevikcan, E. (Eds.), Industry 4.0: Managing The Digital Transformation. Springer, Cham, pp. 267–284.

Evans, N.D., 2016. Future skills. ITNOW 58 (1), 50–51. https://doi.org/10.1093/itnow/bww022.

Fahad, A., Alshatri, N., Tari, Z., Alamri, A., Khalil, I., Zomaya, A.Y., Foufou, S., Bouras, A., 2014. A survey of clustering algorithms for big data: Taxonomy and empirical analysis. IEEE Transactions on Emerging Topics in Computing 2 (3), 267–279. https://doi.org/10.1109/TETC.2014.2330519.

Fang, Y., Henfridsson, O., Jarvenpaa, S.L., 2018. Editorial on generating business and social value from digital entrepreneurship and innovation. Journal of Strategic Information Systems 27 (4), 275–277. https://doi.org/10.1016/j.jsis.2018.11.001.

Fichman, R.G., 2004. Real options and IT platform adoption: Implications for theory and practice. Information Systems Research 15 (2), 132–154. https://doi.org/10.1287/isre.1040.0021.

Fichman, R.G., Dos Santos, B.L., Zheng, Z.E., 2014. Digital innovation as a fundamental and powerful concept in the information systems curriculum. MIS Quarterly 38 (2), 329–353. https://doi.org/10.25300/MISQ/2014/38.2.01.

Fitzgerald, M., Kruschwitz, N., Bonnet, D., Welch, M., 2014. Embracing digital technology: A new strategic imperative. MIT Sloan Management Review 55 (2), 1–12.

Ford, S., Despeisse, M., 2016. Additive manufacturing and sustainability: An exploratory study of the advantages and challenges. Journal of Cleaner Production 137, 1573–1587. https://doi.org/10.1016/j.jclepro.2016.04.150.

Frustaci, M., Pace, P., Aloi, G., Fortino, G., 2018. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet Things Journal 5 (4), 2483–2495. https://doi.org/10.1109/JIOT.2017.2767291.

Furr, N., Shipilov, A., 2019. Digital doesn't have to be disruptive: The best results can come from adaptation rather than reinvention. Harvard Business Review 97 (4), 94-103.

Gartner Inc., 2009. Hype Cycle for Emerging Technologies 2009. Gartner Inc. https://www.gartner.com/documents, ID: G00169368.

Gartner Inc., 2010. Hype Cycle for Emerging Technologies 2010. Gartner Inc. https://www.gartner.com/documents, ID: G00205757.

Gartner Inc., 2011. Hype Cycle for Emerging Technologies 2011. Gartner Inc. https://www.gartner.com/documents, ID: G00215650.

Gartner Inc., 2012. Hype Cycle for Emerging Technologies 2012. Gartner Inc. https://www.gartner.com/documents, ID: G00233931.

Gartner Inc., 2013. Hype Cycle for Emerging Technologies 2013. Gartner Inc. https://www.gartner.com/documents, ID: G00252762.

Gartner Inc., 2014. Hype Cycle for Emerging Technologies 2014. Gartner Inc. https://www.gartner.com/documents, ID: G00264126.

Gartner Inc., 2015. Hype Cycle for Emerging Technologies 2015. Gartner Inc. https://www.gartner.com/documents, ID: G00289755.

Gartner Inc., 2016. Hype Cycle for Emerging Technologies 2016. Gartner Inc. https://www.gartner.com/documents, ID: G00299893.

Gartner Inc., 2017. Hype Cycle for Emerging Technologies 2017. Gartner Inc. https://www.gartner.com/documents, ID: G00314560.

Geng, R., Mansouri, S.A., Aktas, E., 2017. The relationship between green supply chain management and performance: A meta-analysis of empirical evidences in Asian emerging economies. International Journal of Production Economics 183, 245–258. https://doi.org/10.1016/j.ijpe.2016.10.008.

Gimpel, H., Hosseini, S., Huber, R., Probst, L., Röglinger, M., Faisst, U., 2018. Structuring digital transformation: A framework of action fields and its application at ZEISS. Journal of Information Technology Theory and Application 19 (1), 31-53.

Gimpel, H., Röglinger, M., 2015. Digital transformation: Changes and chances – Insights based on an empirical study. Project Group Business and Information Systems Engineering of the Fraunhofer Institute for Applied Information, 1–21.

Govindarajan, V., Immelt, J., 2019. The only way manufacturers can survive. MIT Sloan Management Review 60 (3), 24–33.

Gregor, S., 2006. The nature of theory in information systems. MIS Quarterly 30 (3), 611–642. https://doi.org/10.2307/25148742.

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.

Guinness World Records, 2016. Pokémon Go catches five new world records. Guinness World Records. https://www.guinnessworldrecords.com/news/2016/8/pokemon-go-catches-five-world-records-439327?fb_comment_id=1042775672485563_1042869635809500 (accessed 26 January 2020).

Ha, S., Suh, H.-W., 2008. A timed colored Petri nets modeling for dynamic workflow in product development process. Computers in Industry 59 (2-3), 193–209. https://doi.org/10.1016/j.compind.2007.06.016.

Hellinger, A., Seeger, H., 2011. Cyber-physical systems: Driving force for innovation in mobility, health, energy and production. Acatech Position Paper, National Academy of Science and Engineering.

Henke, N., Bughin, J., Chui, M., Manyika, J., Saleh, T., Wiseman, B., Sethupathy, G., 2016. The age of analytics: Competing in a data-driven world. McKinsey Global Institute. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world (accessed 23 August 2018).

Hopkins, B., McCormick, J., Schadler, T., 2018. Insights-driven businesses Set the pace for global growth: The vision report of the insights-driven business playbook. Forrester.

Howard, J.D., Longstaff, T.A., 1998. A common language for computer security incidents. Sandia national laboratories albuquerque report. https://doi.org/10.2172/751004.

Huang, K., Siegel, M., Pearlson, K., Madnick, S., 2019. Casting the dark web in a new light. MIT Sloan Management Review 60 (4), 1–9.

Iansiti, M., Lakhani, K.R., 2014. Digital ubiquity: How connections, sensors, and data are revolutionizing business. Harvard Business Review 92 (11), 90–99.

IDC, 2019. Businesses will spend nearly $1.2 trillion on digital transformation this year as they seek an edge in the digital economy, according to a new IDC spending guide. https://www.idc.com/getdoc.jsp?containerId=prUS45027419 (accessed 25 January 2020).

International Energy Agency, 2017. Digitalisation and energy: Technology report. https://www.iea.org/reports/digitalisation-and-energy (accessed 18 February 2020).

Iqbal, M., 2019. Pokémon GO revenue and usage statistics. https://www.businessofapps.com/data/pokemon-go-statistics/ (accessed 24 February 2020).

Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D., 2014. Security of the Internet of Things: Perspectives and challenges. Wireless Networks 20 (8), 2481–2501. https://doi.org/10.1007/s11276-014-0761-7.

Kagermann, H., Wahlster, W., Helbig, J., 2013. Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing Industury. Final report of the Industrie 4.0 working group.

Kang, H.S., Lee, J.Y., Choi, S., Kim, H., Park, J.H., Son, J.Y., Kim, B.H., Do Noh, S., 2016. Smart manufacturing: Past research, present findings, and future directions. International Journal of Precision Engineering and Manufacturing-Green Technology 3 (1), 111–128. https://doi.org/10.1007/s40684-016-0015-5.

Karnouskous, S., Colombo, A.W., 2011. Architecting the next generation of service-based SCADA/DCS system of systems, in: Proceedings of the 37th Annual Conference on IEEE Industrial Electronics Society, Melbourne, Australia, pp. 359–364.

Kaspersky, 2017. The state of industrial cyber security 2017: Global report. https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf (accessed 27 January 2020).

King, N., 2011. A benefits dependency network as the bridge between requirements and business objectives: An ODE perspective. International Journal of Organisational Design and Engineering 1 (3), 185–208. https://doi.org/10.1504/IJODE.2011.041161.

Kjaerland, M., 2005. A classification of computer security incidents based on reported attack data. Journal of Investigative Psychology and Offender Profiling 2 (2), 105–120. https://doi.org/10.1002/jip.31.

Kollar, P., Allegra, F., 2016. Pokémon Go review. Polygon. Vox media. https://www.polygon.com/2016/7/14/12183956/pokemon-go-review-ios-android-nintendo-niantic-company-mobile-game (accessed 26 January 2020).

Krueger, R.A., Casey, M.A., 2014. Focus groups: A practical guide for applied research, 5th ed. SAGE, Thousand Oaks, California.

Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., Hoffmann, M., 2014. Industry 4.0. Business & Information Systems Engineering 6 (4), 239–242. https://doi.org/10.1007/s12599-014-0334-4.

Lee, E.A., 2008. Cyber physical systems: Design challenges, in: IEEE International Symposium on Object Oriented Real-Time Distributed Computing, Orlando, Florida, USA, pp. 363–369.

Lee, R.M., Assante, M.J., Conway, T., 2014. German steel mill cyber attack. Industrial control systems.

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.

Levermore, D.M., Babin, G., Hsu, C., 2010. A new design for open and scalable collaboration of independent databases in digitally connected enterprises. Journal of the Association for Information Systems 11 (7), 367–393. https://doi.org/10.17705/1jais.00233.

Lu, T., Zhao, J., Zhao, L., Li, Y., Zhang, X., 2014. Security objectives of cyber physical systems, in: Proceedings of the 7th International Conference on Security Technology, Hainan Island, China, pp. 30–33.

Lucas Jr, H., Agarwal, R., Clemons, E.K., El Sawy, O.A., Weber, B., 2013. Impactful research on transformational information technology: An opportunity to inform new audiences. MIS Quarterly 37 (2), 371–382. https://doi.org/10.25300/MISQ/2013/37.2.03.

Lucas Jr, H.C., Goh, J.M., 2009. Disruptive technology: How Kodak missed the digital photography revolution. Journal of Strategic Information Systems 18 (1), 46–55. https://doi.org/10.1016/j.jsis.2009.01.002.

Lucke, D., Constantinescu, C., Westkämper, E., 2008. Smart factory - A step towards the next generation of manufacturing, in: Mitsuishi, M., Ueda, K., Kimura, F. (Eds.), Manufacturing Systems and Technologies for the New Frontier. Springer, London, pp. 115–118.

Lycett, M., 2013. Datafication: Making sense of (big) data in a complex world. European Journal of Information Systems 22 (4), 381–386. https://doi.org/10.1057/ejis.2013.10.

Mathiesen, P., Bandara, W., Watson, J., 2013. The affordances of social technology: A BPM perspective, in: Proceedings of the 34th International Conference on Information Systems, Milan, Italy, pp. 1–11.

Matt, C., Hess, T., Benlian, A., 2015. Digital transformation strategies. Business & Information Systems Engineering 57 (5), 339–343. https://doi.org/10.1007/s12599-015-0401-5.

McFarland, M., 2016. Pokemon Go could add 2.83 million years to users' lives. CNN money. https://money.cnn.com/2016/10/11/technology/pokemon-go-exercise-health/index.html (accessed 26 January 2020).

McKelvey, B., 1978. Organizational systematics: Taxonomic lessons from biology. Management Science 24 (13), 1428–1440. https://doi.org/10.1287/mnsc.24.13.1428.

McKelvey, B., 1982. Organizational systematics: Taxonomy, evolution, classification. University of California Press, Berkeley, California.

McRae, H., 2015. Facebook, Airbnb, Uber, and the unstoppable rise of the content non-generators. http://www.independent.co.uk/news/business/comment/hamish-mcrae/facebook-airbnb-uber-and-the-unstoppable-rise-of-the-content-non-generators-10227207.html (accessed 27 January 2020).

Ménard, A., 2017. How can we recognize the real power of the Internet of Things? McKinsey & Company.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W., Ueda, K., 2016. Cyber-physical systems in manufacturing. CIRP Annals 65 (2), 621–641. https://doi.org/10.1016/j.cirp.2016.06.005.

Nahm, A.Y., Rao, S., Solis-Galvan, L.E., Ragu-Nathan, T.S., 2002. The Q-sort method: Assessing reliability and construct validity of questionnaire items at a pre-testing stage. Journal of Modern Applied Statistical Methods 1 (1), 114–125. https://doi.org/10.22237/jmasm/1020255360.

Nardi, B., 1996. Context and consciousness: Activity theory and human-computer interaction. MIT Press, Cambridge.

National Instruments, 2014. NI trend watch 2014 - Technology trends that accelerate your productivity.

Nickerson, R.C., Varshney, U., Muntermann, J., 2013. A method for taxonomy development and its application in information systems. European Journal of Information Systems 22 (3), 336–359. https://doi.org/10.1057/ejis.2012.26.

Pasqualetti, F., Dorfler, F., Bullo, F., 2013. Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control 58 (11), 2715–2729. https://doi.org/10.1109/TAC.2013.2266831.

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A design science research methodology for information systems research. Journal of management information systems 24 (3), 45–77. https://doi.org/10.2753/MIS0742-1222240302.

Penas, O., Plateaux, R., Patalano, S., Hammadi, M., 2017. Multi-scale approach from mechatronic to cyber-physical systems for the design of manufacturing systems. Computers in Industry 86, 52–69. https://doi.org/10.1016/j.compind.2016.12.001.

Peppard, J., 2016. A tool to map your next digital initiative. Harvard Business Review. https://hbr.org/2016/06/a-tool-to-map-your-next-digital-initiative (accessed 27 January 2020).

Petri, C.A., 1966. Communication with automata. Diploma Thesis.

Pétrissans, A., Krawczyk, S., Cattaneo, G., Feeney, N., Veronesi, L., Meunier, C., 2012. Final study report: Design of future embedded systems. http://cordis.europa.eu/fp7/ict/embedded-systems-engineering/documents/idc-study-final-report.pdf (accessed 13 October 2018).

Porter, M.E., Heppelmann, J.E., 2014. How smart, connected products are transforming competition. Harvard Business Review 92 (11), 64–88.

Posey, C., Roberts, T.L., Lowry, P.B., Bennett, R.J., Courtney, J.F., 2013. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. MIS Quarterly 37 (4), 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.09.

Püschel, L., Röglinger, M., Schlott, H., 2016. What`s in a smart thing? Development of a multi-layer taxonomy, in: Proceedings of the 37th International Conference on Information Systems. Dublin, Ireland, pp. 1-19.

Radziwon, A., Bilberg, A., Bogers, M., Madsen, E.S., 2014. The smart factory: Exploring adaptive and flexible manufacturing solutions. Procedia Engineering 69, 1184–1190. https://doi.org/10.1016/j.proeng.2014.03.108.

Relihan, T., 2019. 5 digital insights from MIT Sloan Management Review. MIT Sloan Management. https://mitsloan.mit.edu/ideas-made-to-matter/5-digital-insights-mit-sloan-management-review (accessed 21 January 2020).

Römer, M., Röglinger, M., Linhart, A., Schmidl, J., Utz, L., Venus, M., 2017. Designing IT setups in the digital age. AT Kearney and Project Group Business and Information Systems Engineering of Fraunhofer Institute for Applied Information Technology FIT.

Rowley, J., 2012. Conducting research interviews. Management Research Review 35 (3/4), 260–271. https://doi.org/10.1108/01409171211210154.

Sadeghi, A.-R., Wachsmann, C., Waidner, M., Haider, W., 2012. A survey of password attacks and comparative analysis on methods for secure authentication. World Applied Sciences Journal 19 (4), 439–444. https://doi.org/10.1145/2744769.2747942.

Schuh, G., Potente, T., Varandani, R., Hausberg, C., Fränken, B., 2014. Collaboration moves productivity to the next level. Procedia CIRP 17, 3–8. https://doi.org/10.1016/j.procir.2014.02.037.

Shirazi, N.-u.-h., Schaeffer-Filho, A., Hutchison, D., 2014. Attack pattern recognition through correlating cyber situational awareness in computer networks, in: Zhu, H., Blackwell, C. (Eds.), Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns. Springer International Publishing, Cham, pp. 125–134.

Silver, M.S., Markus, M.L., Beath, C.M., 1995. The information technology interaction model: A foundation for the MBA core course. MIS Quarterly 19 (3), 361–390. https://doi.org/10.2307/249600.

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., Gidlund, M., 2018. Industrial Internet of Things: Challenges, opportunities, and directions. IEEE Transactions on Industrial Informatics 14 (11), 4724–4734. https://doi.org/10.1109/TII.2018.2852491.

Smith, G.E., Watson, K.J., Baker, W.H., Pokorski II, J.A., 2007. A critical balance: Collaboration and security in the IT-enabled supply chain. International Journal of Production Research 45 (11), 2595–2613. https://doi.org/10.1080/00207540601020544.

Sonnenberg, C., Vom Brocke, J., 2012. Evaluations in the science of the artificial – Reconsidering the build-evaluate pattern in design science research, in: Design Science Research in Information Systems. Advances in Theory and Practice. Proceedings of the 7th DESRIST Conference. Springer, Berlin, Heidelberg, Las Vegas, Nevada, pp. 381–397.

Spreitzer, R., Moonsamy, V., Korak, T., Mangard, S., 2018. Systematic classification of side-channel attacks: A case study for mobile devices. IEEE Communications Surveys & Tutorials 20 (1), 465–488. https://doi.org/10.1109/COMST.2017.2779824.

Statista, 2017. Internet of Things connected devices installed base worldwide from 2015 to 2025. The statistics portal. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed 27 January 2020).

Steininger, D.M., 2019. Linking information systems and entrepreneurship: A review and agenda for IT-associated and digital entrepreneurship research. Information Systems Journal 29 (2), 363–407. https://doi.org/10.1111/isj.12206.

Symantec, 2019. Internet security threat report.

Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H., Sui, F., 2018. Digital twin-driven product design, manufacturing and service with big data. The International Journal of Advanced Manufacturing Technology 2018 (94), 3563–3576. https://doi.org/10.1007/s00170-017-0233-1.

Tjahjono, B., Esplugues, C., Ares, E., Pelaez, G., 2017. What does industry 4.0 mean to supply chain? Procedia Manufacturing 13, 1175–1182. https://doi.org/10.1016/j.promfg.2017.09.191.

Tremblay, M.C., Hevner, A.R., Berndt, D.J., 2010. The use of focus groups in design science research, in: Hevner, A., Chatterjee, S. (Eds.), Design Research in Information Systems, vol. 22. Springer US, Boston, Massachusetts, pp. 121–143.

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.

U.S. Energy Information Administration, 2017. International energy outlook 2017. https://www.eia.gov/outlooks/ieo/pdf/0484(2017).pdf (accessed 18 January 2020).

Ullrich, J., Voyiatzis, A.G., Weippl, E.R., 2016. Secure cyber-physical production systems: Solid steps towards realization, in: Proceedings of the 1st International Workshop on Cyber-Physical Production Systems, Vienna, Austria, pp. 1–4.

Urbach, N., Röglinger, M., 2019. Introduction to digitalization cases: How organizations rethink their business for the digital age, in: Digitalization Cases. Springer, pp. 1–12.

Valk, R., 2008. Generalizations of Petri nets, in: Mathematical Foundations of Computer Science, vol. 118, pp. 140–155.

Vavra, J., Hromada, M., 2015. An evaluation of cyber threats to industrial control systems, in: 2015 International Conference on Mechatronics Technology, pp. 1–5.

Vogel-Heuser, B., Diedrich, C., Pantförder, D., Göhner, P., 2014. Coupling heterogeneous production systems by a multi-agent based cyber-physical production system, in: 12th IEEE International Conference on Industrial Informatics System, Porto Alegre, Brasilia, pp. 713–719.

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.

Wang, S., Wan, J., Di Li, Zhang, C., 2016. Implementing smart factory of Industrie 4.0: An outlook. International Journal of Distributed Sensor Networks 4, 1–10. https://doi.org/10.1155/2016/3159805.

Ward, J., Daniel, E., 2006. Benefits management: Delivering value from IS and IT investments. John Wiley & Sons Ltd, Hoboken.

Ward, J.H., 1963. Hierarchical grouping to optimize an objective function. Journal of the American Statistical Association 58 (301), 236–244. https://doi.org/10.1080/01621459.1963.10500845.

Watson, J.W., Goodhue, D.L., Wixom, B.H., 2002. The benefits of data warehousing: Why some organizations realize exceptional payoffs. Information & Management 39 (6), 491–502. https://doi.org/10.1016/S0378-7206(01)00120-3.

Weill, P., Woerner, S., 2018. What's your digital business model? Six questions to help you build the next-generation enterprise. Harvard Business Review Press.

Weill, P., Woerner, S.L., 2015. Thriving in an increasingly digital ecosystem. MIT Sloan Management Review 56 (4), 27–34.

Witten, I.H., Frank, E., Hall, M.A., Pal, C.J., 2017. Practival machine learning: Tools and techniques, 4th ed. Morgan Kaufmann, Cambridge.

Yoo, Y., Henfridsson, O., Lyytinen, K., 2010. Reserach commentary - The new organizing logic of digital innovation: An agenda for information systems research. Information Systems Research 21 (4), 724–735. https://doi.org/10.1287/isre.1100.0322.

Yoon, J.-S., Shin, S.-J., Suh, S.-H., 2012. A conceptual framework for the ubiquitous factory. International Journal of Production Research 50 (8), 2174–2189. https://doi.org/10.1080/00207543.2011.562563.

Zuech, R., Khoshgoftaar, T.M., Wald, R., 2015. Intrusion detection and big heterogeneous data: A survey. Journal of Big Data 2015 (2). https://doi.org/10.1186/s40537-015-0013-4.

Zuehlke, D., 2010. SmartFactory—Towards a factory-of-things. Annual Reviews in Control 34 (1), 129–138. https://doi.org/10.1016/j.arcontrol.2010.02.008.

V. Appendix

1 Index of Research Articles

Research Article #1: Unblackboxing Digital Technologies – A Multi-layer Taxonomy and Archetypes

Berger S., Denner M.-S., & Röglinger M. Unblackboxing Digital Technologies – A Multi-layer Taxonomy and Archetypes. *Submitted working paper*. Earlier version published in *Proceedings of the 26th European Conference on Information Systems (ECIS), Portsmouth, United Kingdom.*

Research Article #2: Organizing Self-organizing Systems: A Terminology, Taxonomy, and Reference Model for Entities in Cyber-physical Production Systems

Berger S., Häckel B., & Häfner L. (2019). Organizing Self-organizing Systems: A Terminology, Taxonomy, and Reference Model for Entities in Cyber-physical Production Systems. In: *Information Systems Frontiers* (in press).

Research Article #3: Attacks on the Industrial Internet of Things – Development of a Multi-layer Taxonomy

Berger S., Bürger O., & Röglinger M. (2020). Attacks on the Industrial Internet of Things – Development of a Multi-layer Taxonomy. In: *Computers & Security, 2020, 93 (2020), 101790*.

Research Article #4: IT Availability Risks in Smart Factory Networks – Simulating the Effects of IT Threats on Production Processes Using Petri Nets

Berger S., Häckel B., & van Dun C. IT Availability Risks in Smart Factory Networks – Simulating the Effects of IT Threats on Production Processes Using Petri Nets. *Submitted working paper*. Earlier version published in *Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm and Uppsala, Sweden.*

Research Article #5: Ecological Sustainability 4.0 – Identifying and Structuring Ecological Benefits of Industry 4.0 Technologies by Means of a Benefits Dependency Network

Berger S., Graf V., & Häckel B. Ecological Sustainability 4.0 – Identifying and Structuring Ecological Benefits of Industry 4.0 Technologies by Means of a Benefits Dependency Network. *Submitted working paper.*

2 Individual Contribution to the Research Articles

This thesis is cumulative and consists of five research articles that build the main body of work. All included research articles were developed and written in teams with multiple co-authors. This section provides details on the research settings and highlights my individual contribution to each article.

Research article #1 (Berger et al.) was developed in a team of three co-authors. All three jointly developed the key concept of the taxonomy and archetypes of digital technologies. A former version of the article was presented at the 26th European Conference on Information Systems (ECIS), Portsmouth, United Kingdom. After incorporating feedback, we significantly advanced our work. All co-authors jointly elaborated on the identification of a sample of real-world technologies, taxonomy development, the underlying literature work, as well as the conduction of internal and external Q-sorts in course of the evaluation. I particularly focussed on the design of the research method and the use of statistical methods to inductively derive archetypes from our sample.

Research article #2 (Berger et al. 2019) was developed in a team of three co-authors. The three co-authors jointly worked on the main idea and the key contributions, i.e., terminology, taxonomy, and reference model. I played a key role in reviewing the extant literature and in the method design. With regard to our artefacts, I was, in particular, responsible for the development of the taxonomy and reference model, along with their application. I was also responsible for preparing the article for re-submission.

Research article #3 (Berger et al. 2020) was developed in a team of three co-authors. As the leading author, I brought in the idea and key concept of the article and was responsible for the elaboration of the research method, model development, and application. I also prepared, organized, and conducted expert interviews for our evaluation. While, to a large extent, this article reflects my efforts, all co-authors promoted the advancement of the paper throughout the entire project.

Research article #4 (Berger et al.) was developed in a team of three co-authors. A former version of the article was jointly developed by a former team of four co-authors and presented at the 27th European Conference on Information Systems (ECIS), Stockholm and Uppsala, Sweden. After one new co-author joined the team and two co-authors left, we revised our modeling approach, incorporating the feedback from the conference and extending its evaluation. In particular, I was responsible for reviewing the extant literature, further developing the methodology, and clarifying the contribution. All three co-authors supported the project throughout its duration and made equal contributions to the article.

Research article #5 (Berger et al.) was developed in a team of three co-authors. As the leading author of this article, I developed the basic idea and, to a large extent, created its content. In particular, I set up the research method and developed our framework within multiple iterations. I also carried out the comprehensive evaluation of the framework and conducted several interviews with industry experts. The analysis of the interviews enabled me to draw insights about both the application and contribution

of our work. Although I am the leading author of this project, the co-authors were involved in the literature review and discussions throughout the project.

3 Research Article #1: Unblackboxing Digital Technologies – A Multi-layer Taxonomy and Archetypes

Authors: Berger S., Denner M.-S., Röglinger M.

Status: Submitted working paper.
Earlier version published in *Proceedings of the 26th European Conference on Information Systems (ECIS), Portsmouth, United Kingdom.*

Extended Abstract

With their rapid emergence and adoption, digital technologies are the key driver of digitalization, affecting individuals, organizations, and society as a whole on a global scale. Despite their major importance for research and practice, digital technologies remain poorly understood. The lack of knowledge about their very nature hampers scientific progress and clear-headed decisions on digital transformation in practice. While academia mainly elaborates on individual technologies, professional literature primarily lists multiple technology compilations and provides high-level classifications. Hence, a literature-backed and empirically validated approach is required, which identifies similarities and differences as well as provides a sufficient level of abstraction from individual technologies as a basis for further sense-making and design-oriented research. Against this backdrop, we ask the following research question: *How can digital technologies be classified?*

In response to this research question, we adopt an 'organizational systematics' approach in line with McKelvey (1978) to make a two-fold contribution: First, we apply the established iterative taxonomy development process of Nickerson et al. (2013) to inductively and deductively develop a taxonomy of digital technologies. Drawing on an extensive literature review of current knowledge and a sample of about 90 digital technologies from the Gartner Hype Cycle for Emerging Technologies of 2009 to 2017, the taxonomy comprises eight dimensions – i.e., role of technology, scope, multiplicity, direction, data treatment, input, output, and human involvement – and corresponding characteristics of digital technologies, which are structured along the establish layered architecture of Yoo et al. (2010). Enabling the structured classification of individual technologies, the taxonomy addresses similarities and differences of digital technologies. Second, we inductively infer digital technology archetypes, each of which reflects a typical combination of digital technology characteristics. After classifying the entire sample of digital technologies by means of the taxonomy, we conducted a hierarchical cluster analysis and received nine archetypes: connectivity & computation, platform provision, mobile device, sensor-based data collection, actor-based data execution, analytical insight generation, self-dependent

material agency, augmented interaction, and natural interaction. These archetypes abstract from individual technologies and provide a profound basis for further research.

Regarding the evaluation, we classified the sample of 92 digital technologies. As for the archetypes, we conducted a Q-sort among the co-authors and a panel of twelve industry experts with a digitalization background. To evaluate the robustness of the archetypes, we conducted a longitudinal analysis to examine the occurrence of archetypes over time. Finally, we asked the industry experts for potential use cases to elaborate on the archetypes applicability. In sum, the evaluation results confirmed the reliability and validity of the taxonomy and archetypes.

Overall, the taxonomy and archetypes build on and extend discussions in the IS community about the nature of digital technologies and add to the descriptive knowledge in this field. While the taxonomy enables the classification of individual digital technologies, the archetypes provide a profound basis for industrial use cases and future research.

References

McKelvey, B., 1978. Organizational systematics: Taxonomic lessons from biology. Management Science 24 (13), 1428–1440. https://doi.org/10.1287/mnsc.24.13.1428.

Nickerson, R.C., Varshney, U., Muntermann, J., 2013. A method for taxonomy development and its application in information systems. European Journal of Information Systems 22 (3), 336–359. https://doi.org/10.1057/ejis.2012.26.

Yoo, Y., Henfridsson, O., Lyytinen, K., 2010. Reserach commentary - The new organizing logic of digital innovation: An agenda for information systems research. Information Systems Research 21 (4), 724–735. https://doi.org/10.1287/isre.1100.0322.

4 Research Article #2: Organizing Self-organizing Systems: A Terminology, Taxonomy, and Reference Model for Entities in Cyber-physical Production Systems

Authors: Berger S., Häckel B., Häfner L.

Published in: *Information Systems Frontiers* (in press).

Abstract: Ongoing digitalization accelerates the transformation and integration of physical production and traditional computing systems into smart objects and their interconnectivity, forming the Internet of Things. In manufacturing, the cross-linking of embedded systems creates adaptive and self-organizing Cyber-Physical Production Systems (CPPSs). Owing to ever-increasing cross-linking, rapid technological advances, and multifunctionality, the complexity and structural opacity of CPPSs are rapidly increasing. The development of urgently needed modeling approaches for managing such complexity and structural opacity, however, is impeded by a lack of common understanding of CPPSs. Therefore, in this paper, we contribute to a common understanding of CPPSs by defining and classifying CPPS entities and illustrating their relations. More precisely, we present a terminology, a taxonomy, and a reference model for CPPS entities, created and evaluated using an iterative development process. Thereby, we lay the foundation for future CPPS modeling approaches that make CPPS complexity and structural opacity more manageable.

Keywords: Digitalization, Cyber-Physical (Production) Systems, Terminology, Taxonomy, Reference Model, Smart Objects

5 Research Article #3: Attacks on the Industrial Internet of Things – Development of a Multi-layer Taxonomy

Authors: Berger S., Bürger O., Häckel B.

Published in: *Computers & Security*, 2020, 93 (2020), 101790.

Abstract: The Industrial Internet of Things (IIoT) provides new opportunities to improve process and production efficiency, which enable new business models. At the same time, the high degree of cross-linking and decentralization increases the complexity of IIoT systems and creates new vulnerabilities. Hence, organizations are not only vulnerable to conventional IT threats, but also to a multitude of new, IIoT-specific attacks. Yet, a literature-based and empirically evaluated understanding of attacks on the IIoT is still lacking. Against this backdrop, we develop a multi-layer taxonomy that helps researchers and practitioners to identify similarities and differences between attacks on the IIoT. Based on the latest literature and a sample of about 50 attacks, we deductively and inductively determine attack characteristics and dimensions. We demonstrate the usefulness and practical relevance of our taxonomy by applying it to a real-world incident affecting a German steel facility. By combining IT security, IIoT, and risk management to form an interdisciplinary approach, we contribute to the descriptive knowledge in these fields. Industry experts confirm that our taxonomy enables a detailed classification of attacks, which supports the identification, documentation, and communication of incidents within organizations and their value-creation networks. With this, our taxonomy provides a profound basis for the further development of IT security management and the derivation of mitigation measures.

Keywords: Industrial Internet of Things, Industry 4.0, IT Security, Attacks, Taxonomy

6 Research Article #4: IT Availability Risks in Smart Factory Networks – Simulating the Effects of IT Threats on Production Processes Using Petri Nets

Authors: Berger S., Häckel B., van Dun C.

Status: Submitted working paper.
Earlier version published in *Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm and Uppsala, Sweden.*

Extended Abstract

In manufacturing, concepts like the Internet of Things and Cyber-physical Systems accelerate the development from traditional production facilities towards smart factories. Thereby, the high degree of cross-linking and information exchange between information components and production machines forms complex smart factory networks. Due to their increasing reliance on information flows and the openness, complexity, and interconnectedness of components, smart factory networks are, in particular, vulnerable to IT availability risks caused by cyber-attacks and errors (Tupa et al., 2017). As the number attacks and errors is rising and existing literature lacks an integrated model for analysing availability risks in smart factory networks, our research question is: *How can availability risks of IT attacks and errors in smart factory networks and their impact on production be modelled and simulated?*

To answer this research question, we adopt the Design Science Research Methodology of Peffers et al. (2007): Drawing on an extensive literature review, we infer formal and functional design objectives, i.e., modelling requirements, for iteratively developing our modelling approach as an artefact. In line with these design objectives, we introduce classical Petri Nets (Petri 1966) and multiple extensions to provide modular information and production components, representing specific features of smart factory networks for analysing IT availability risks and associated impacts on production. More precisely, these components enable the modeling of (existing) smart factory network architectures, and the simulation of stochastic attack and error occurrence and propagation.

To evaluate our artefact and demonstrate its applicability, we follow the evaluation activities as per Sonnenberg and vom Brocke (2012). After justifying the research gap from scientific and practical view, we conduct a feature comparison discussing our artefact's specification against the design objectives and competing artefacts. In addition, we demonstrate the real-world fidelity and applicability of our modeling approach in artificial and naturalistic settings: As for the artificial setting, we implemented an instantiation of our modeling approach as a software prototype and simulated multiple fictional scenarios. With this, we provide a proof of concept and enable the modelling of various smart factory

network layouts. As for the naturalistic setting, we recreated and parameterised real-world scenarios with industry experts. After simulating these scenarios, we analyzed and compared the result regarding availability and productivity.

Overall, our modeling approach creates transparency by providing a scalable depiction of smart factory networks and its components. At the same time, our approach allows for the analysis and comparison of threat scenarios by simulating the occurrence of errors and the spread of attacks from the information network down to machine level. By comparing different network layouts, the identification of weak points and critical dependencies becomes feasible. With this, the proposed modeling approach supports preventive risk management and the derivation of suitable mitigation measures, serving the specific needs of different organizational stakeholders such as IT security experts, production and risk managers, and IT architects.

References

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A design science research methodology for information systems research. Journal of management information systems 24 (3), 45–77. https://doi.org/10.2753/MIS0742-1222240302.

Petri, C.A., 1966. Communication with automata. Diploma Thesis.

Sonnenberg, C., Vom Brocke, J., 2012. Evaluations in the science of the artificial – Reconsidering the build-evaluate pattern in design science research, in: Design Science Research in Information Systems. Advances in Theory and Practice. Proceedings of the 7th DESRIST Conference. Springer, Berlin, Heidelberg, Las Vegas, Nevada, pp. 381–397.

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.

7 Research Article #5: Ecological Sustainability 4.0 – Identifying and Structuring Ecological Benefits of Industry 4.0 Technologies by Means of a Benefits Dependency Network

Authors: Berger S., Graf V., Häckel B.

Status: Submitted working paper.

Extended Abstract

Driven by the integration of digital technologies into manufacturing systems, digitalization accelerates the development of the industrial sector towards Industry 4.0. With concepts like self-organization, self-optimization, decentralization, and autonomy, industrial technologies such as Cyber-physical Production Systems and the Industrial Internet of Things enable highly flexible and efficient (production) processes at reduced costs. Until now, the benefits of Industry 4.0 are primarily described from a product or operations perspective. Performance improvement in terms of sustainability is merely seen as positive side effect of technology use (Dalenogare et al., 2018). In times of ongoing environmental deterioration and climate change, however, the industrial sector is, in particular, responsible for reducing its ecological footprint as it accounts for more than half of the worldwide energy consumption (U.S. Energy Information Administration, 2017). As current literature discusses technologies and ecologic benefits individually rather than from an integrated point of view, researchers and practitioners are still struggling to systematically identify cause-effect relations. Hence, our research question is: *How can ecological benefits of Industry 4.0 technologies be identified in a structured way?*

To answer this question, we follow the design science research methodology as per Peffers et al. (2007) and propose a triple-punch approach: First, we iteratively develop a Benefits Dependency Network (Ward and Daniel, 2006) as a framework from benefits management to support organizational stakeholders in identifying and correlating ecological benefits, associated Industry 4.0 technologies, and necessary organizational changes in a structured way. Second, we introduce building blocks, i.e., exemplary elements of the Benefits Dependency Network derived from literature on topics such as green manufacturing principles (e.g., Despeisse et al., 2012) and technological advancements in the industry (e.g., Dalenogare et al., 2018), to increase the utility of the Benefits Dependency Network and guide intended users in developing instantiations. Third, we demonstrate the feasibility and effectiveness of the Benefits Dependency Network and its building blocks.

Regarding the validation of the framework, we follow the evaluation activities as per Sonnenberg and vom Brocke (2012), which are in line with the design science research paradigm. We demonstrate our artefact in artificial, i.e., literature-based instantiations, and naturalistic, i.e., real-world use cases,

settings. For the iterative development process and the validation of the artefact, we included feedback from multiple discussions with focus groups and interviews with industry experts.

In sum, the Benefits Dependency Network contributes to the descriptive knowledge regarding the interdisciplinary research field of ecological sustainability. The framework guides researchers and practitioners in systematically identifying, structuring, and correlating Industry 4.0 technologies and ecological benefits under consideration of associated organizational changes. The integrated view on technology and ecology serves as a basis for the ex-ante, ex-nunc, and ex-post evaluation of technology-driven projects and corresponding ecological objectives. With this, we support profound decision-making on investments and the monitoring and control of projects to accelerate ecology-driven transformation.

References

Dalenogare, L.S., Benitez, G.B., Ayala, N.F., Frank, A.G., 2018. The expected contribution of Industry 4.0 technologies for industrial performance. International Journal of Production Economics 204, 383–394. https://doi.org/10.1016/j.ijpe.2018.08.019.

Despeisse, M., Ball, P.D., Evans, S., 2012. Modelling and tactics for sustainable manufacturing: An improvement methodology, in: Seliger, G. (Ed.), Sustainable Manufacturing. Springer, Berlin, Heidelberg, pp. 9–16.

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A design science research methodology for information systems research. Journal of management information systems 24 (3), 45–77. https://doi.org/10.2753/MIS0742-1222240302.

Sonnenberg, C., Vom Brocke, J., 2012. Evaluations in the science of the artificial – Reconsidering the build-evaluate pattern in design science research, in: Design Science Research in Information Systems. Advances in Theory and Practice. Proceedings of the 7th DESRIST Conference. Springer, Berlin, Heidelberg, Las Vegas, Nevada, pp. 381–397.

U.S. Energy Information Administration, 2017. International energy outlook 2017. https://www.eia.gov/outlooks/ieo/pdf/0484(2017).pdf (accessed 18 January 2020).

Ward, J., Daniel, E., 2006. Benefits management: Delivering value from IS and IT investments. John Wiley & Sons Ltd, Hoboken.