2nd Conference on Production Systems and Logistics

Identification of Cyber Security Risks in Subscription-based Business Models for Manufacturing Companies and Derivation of Suitable Measures

Günther Schuh[1], Volker Stich[1], Jan Hicking[1], Lars Kaminski[1], Jacques Engländer[1], Anna Majchrzak[1]

[1]*Institute for Industrial Management, FIR at RWTH Aachen University, Campus-Boulevard 55, Aachen 52074, Germany*

Abstract

In the age of digitalization, manufacturing companies are under increased pressure to change due to product complexity, growing customer requirements and digital business models. The increasing digitization of processes and products is opening up numerous opportunities for mechanical engineering companies to exploit the resulting potential for value creation. Subscription business is a new form of business model in the mechanical engineering industry, which aims to continuously increase customer benefit to align the interests of both companies and customers. Characterized by a permanent data exchange, databased learning about customer behavior, and the transfer into continuous innovations to increase customer value, subscription business helps to make Industry 4.0 profitable. The fact that machines and plants are connected to the internet and exchange large amounts of data results in critical information security risks. In addition, the loss of knowledge and control, data misuse and espionage, as well as the manipulation of transaction or production data in the context of subscription transactions are particularly high risks. Complementary to direct and obvious consequences such as loss of production, the attacks are increasingly shifting to non-transparent and creeping impairments of production or product quality, which are only apparent at a late stage, or the influencing of payment flows. A transparent presentation of possible risks and their scope, as well as their interrelationships, does not exist. This paper shows a research approach in which the structure of subscription models and their different manifestations based on their risks and vulnerabilities are characterized. This allows suitable cyber security measures to be taken at an early stage. From this basis, companies can secure existing or planned subscription business models and thus strengthen the trust of business partners and customers.

Keywords

Cyber Security, Subscription Business, Manufacturing Companies, Digital Transformation

1. Introduction

1.1 Initial situation

National initiatives such as the National Climate Protection Plan 2050 are driving the goal to achieve high standards of economic, social, or environmental sustainability. Individual components that contribute to increasing sustainability, such as the circular economy, are therefore highly relevant to all social sectors in Germany [1]. Enterprises in the field of mechanical and plant engineering have recognized this fact and are

DOI: https://doi.org/10.15488/11246

setting goals for the sustainable orientation of their corporate activity [2], since a long time of use has a major impact on CO2-emissions generated during the product life cycle of machinery and equipment [3]. This, however, contradicts the prevailing business model in the manufacturing industry - the transactional business model, which consists of the one-off sale of products. Therefore, the manufacturer faces the challenge of maximizing two conflicting goals, i.e., increasing the useful life of its machines and, at the same time, maintaining profit through one-time sales.

As trends, both a circular economy and digitalization have a significant impact on markets and core elements of enterprises' business models. It is apparent that the mere sale of goods, i.e. the core business, delivers a significantly lower contribution margin than services and after-sales services in the enterprises of the machinery and plant-engineering sector [4]. The shift from manufacturing to software- and data-driven services shape the view of how and for what customers pay. This leads to a turn from revenue to user fees. The convergence of software and hardware components acts as a catalyst and foundation for these developments. The associated networking and resulting databased services open up considerable potential for digitization. Digital business models such as subscriptions are ultimately the logical consequence of this development. Numerous machine and plant manufacturers are already developing corresponding solutions today. Moreover, in current times of crisis, it is evident that those enterprises that pursue subscription business models are performing better than other enterprises in navigating the COVID 19 crisis. Their revenue grew by 9.5% in the first quarter of 2020 whereas the S&P 500 only posted 1.9% growth [3].

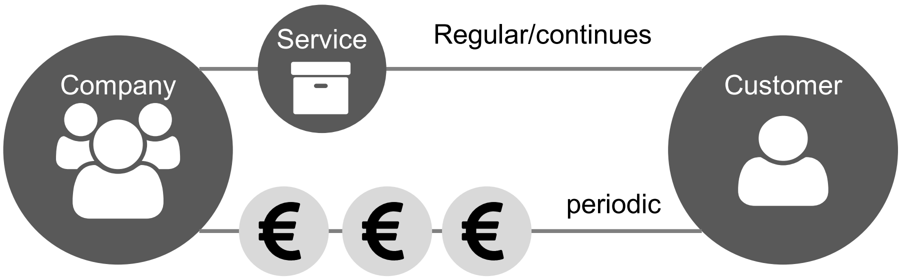

Figure 1: Subscription business model scheme

An enterprise enters a long-term relationship with its customers by providing services. Since this relationship has a great impact on the output and performance of manufacturing companies, it thrives on the mutual trust relationship between the partners involved [1]. Currently, the lack of trust in the context of cross-company data flows is a major obstacle to the implementation of new business models [2]. The increasing number of partners in a value network requires joint responsibility.

Besides, databased services and digital business models, such as subscription, require cross-linking of machinery. Existing machines (legacy) and modern machines are considered separately for this purpose. First, legacy machines are retrofitted, whereby the retrofitted solution must be guaranteed concerning cyber security. Even modern machines are not safe per se, even if they are based on existing standards (e.g., OPC-UA) and norms (e.g., IEC 62443). After all, only properly configured solutions offer the best possible protection. The integration of machines into the customer's network and transmission of the data to the machine and plant manufacturer are complex questions that have yet to be answered.

Digital transformation means that enterprises need to increasingly provide proof of trust to participate in value creation networks and to remain competitive [4]. Thus, appropriate cyber security will become a success factor for machine and plant manufacturers and manufacturing companies with digital business models in the future. A lack of expertise in the IT area and a lack of assistance, especially for small and medium-sized enterprises (SMEs) on which this paper will focus, prevent an efficient approach. Solution approaches, especially for SMEs, need an appropriate level of complexity, necessary investment, and applicability to enable efficient protection. To develop their business models and help shape their markets, the need for tried-and-tested solution patterns for their technical design is a necessity.

Software companies such as Microsoft with its Office 365 product and production enterprises such as the car manufacturer Volvo with its "Auto-Abo" demonstrate that subscription business models will increasingly prevail despite the aforementioned challenges. It is no longer sufficient to simply ensure IT security of individual components; instead, the need for action at the level of the overall system is necessary. This ensures that communication paths and corresponding technologies are designed to be as secure as possible across the entire value chain from the provider to the customer.

The research presented in this paper addresses the above issues by proposing the examination of subscription business models based on constituent characteristics from a cyber security perspective. It describes an approach to investigate the resulting attack vectors and their interaction with resulting measures. This perspective intends to sensitize subscription service providers as well as their customers to the relevance of cyber security and to contribute to accelerating acceptance and implementation in SMEs.

1.2 Structure of the paper

Firstly, basic terminology is explained to provide a general basis of understanding regarding the introduced issues. This is followed by an explanation of the potential and relevance of subscription business models and a more detailed description of the specific challenges involved. Subsequently, we describe existing management and security frameworks, as well as their focus on the described topic. On this basis, we present a systematic approach to solving the challenges described at the beginning. This approach is divided into four parts. First, we present different specifications of subscription business models, whereupon possible attack vectors are derived. Based on these attack vectors, an approach for determining suitable measures for these attack vectors is presented to subsequently describe them concerning their interactions. Finally, we highlight how to classify the findings from the previous steps using thread modeling.

2. State of the art

2.1 Terminology

Cyber security

Cyber security deals with protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also referred to as information technology security or electronic information security [5]. Additionally, it deals with various fields of application such as network security, application security, information security, disaster recovery, and business continuity, and end-user education.

Digital business ecosystems

From a business point of view, “[...]ecosystems encompass a set of actors that contribute to the focal offer’s user value proposition” [6]. A digital ecosystem is an assemblage of interconnected information technology resources and diverse stakeholders that can function as a cohesive unit. These include customers, research and collaboration partners, suppliers, external service providers, software and hardware, as well as third-party data service providers [7]. As such, it is understood as an environment of digital platforms that enable enterprises to position their products and services in the digital world [8].

Digital business models

A digital business model is a form of value creation that is based on developing added value and benefits for customers utilizing innovative digital technologies. Such a business model aims to generate a significant advantage for which customers are willing to pay [9]. As such, it is understood as a set of rules created by a company to organize its business processes in the most profitable way possible. It includes all aspects relevant to value creation, such as the respective range of products and services, addressed customers and target groups, how customer communication is performed, how services are rendered, revenue is generated, and transactions are carried out. All these aspects generate information that is collected, processed, analyzed, or communicated further using digital technologies. As a result, all processes are automated, and process chains are better coordinated. In this way, digital technologies streamline process chains, increase efficiency and maintain a company's competitiveness [10]. The transformation to digital business models is shifting the focus of attention towards customers, making it increasingly important to collect their data in the form of user profiles to adapt products and services more closely to their wishes and needs and even to anticipate them.

Threat Modeling

A threat model is a structured representation of all the information affecting the security of an application. Threat modeling is a process for capturing, organizing, and analyzing all information relevant to cyber security. As a result, it enables an informed decision-making process regarding the security risk of an application. Also, a priority list of cyber security enhancements is created for the concept, requirements, design, or implementation of each application. By identifying targets and vulnerabilities and then defining countermeasures to prevent threats or reduce their impact, the security of the system is holistically improved. [11]

2.2 Norms, standards and methods

Cyber security is referred to as a moving target in constant motion, 100% protection cannot be achieved. New measures are implemented with a certain delay and in an insufficient form. Moreover, the relevance to specific applications is often not sufficiently considered. As a result, there exist numerous frameworks with a different focus for securing cyber security like ISO IEC 27001:2015, NIST, or the IEC 62443, which are either too extensive, too complex, or not designed for the needs of companies.

ISO IEC 27001

The ISO IEC 27001 as an international and cross-sector standard supports companies to manage their information security. This standard contains requirements and specifications for the implementation, maintenance, and continuous improvement of information management systems (ISMS). Besides, methods are described to make the handling of risks related to information security controllable. The presentation of this information is at a generic level to ensure the broadest possible applicability to all stakeholders. [12]

IEC62443

The international series of standards IEC 62443 defines standards and guidelines for the cyber security of "Industrial Automation and Control Systems" (IACS) and provides basic guidelines for operators, integrators, and manufacturers concerning the design, implementation, management, manufacture, and operation of IACS [13]. The core areas are general principles, safety requirements for operators and service providers, safety requirements for automation systems, and safety requirements for automation components. The general principles describe, for example, basic concepts such as defense-in-depth or even fundamental requirements and refer to other parts of the standard for concrete implementation. Guidelines for the implementation of organizational measures are contained in security requirements for operators and service providers. It provides technical aspects such as security level and security requirements for automation systems. The fourth area aims specifically at the product and component view (sensors, interfaces, chips, etc.) and focuses more on manufacturers. [14]

IDS - An approach to securing digital ecosystems

The International Data Spaces (IDS) initiative aims to create a secure data space that enables enterprises of all sizes and from different industries to manage their data assets in a self-sufficient way. The IDS reference architecture model includes all components required for secure exchange and combination of data in ecosystems. The overall architecture consists of four sub-architectures: business architecture, software architecture, security architecture, and data and service architecture. [15] The IDS are distributed networks of data endpoints, provide standardized interfaces and define technical terms of use for data. In addition to legal and organizational contractual rules, it is also possible to formulate and implement technical terms of use. This enables data providers to retain sovereignty over their data when exchanging it. [16]

2.3 Potentials of subscription business models

Subscription business models are characterized by a consistent focus on customer benefits. The aim is no longer to sell the customer individual products or services, but rather to offer access to a constantly improving service. Thus, the subscription business changes the supplier-customer relationship in many respects. In the traditional transaction business, everything was geared to the sale and conclusion of high volumes. In the subscription business, the nature of the business relationship changes fundamentally. Due to the continuous data-technical connection to the customer and thus the insight into the use of the service offers in the field, the provider now has the opportunity for continuous, customer-specific service improvement. This enables customer and provider to enter into a participatory business relationship. We assume that both benefit directly in monetary terms from successful use or an increase in the customer's productivity. HARLAND AND WENGER characterize subscription businesses based on the following four constituent features along the business model dimensions described by GASSMANN ET AL. [17–19]:

1. Revenue mechanics: A subscription is characterized by periodic, unit-of-performance payment streams.
2. Value proposition: A subscription strives for the continuous performance increase of the customer benefit. To this end, the customer benefit is quantified.
3. Value architecture: Subscription is based on knowledge of changes in individual customer benefits. This requires integrating service bundles with customers, improving service delivery through continuous releases, and analyzing individual customer user data based on a customer ID.
4. Customer: A subscription describes a long-term, collaborative partnership. For this purpose, the target systems of provider and customer must be harmonized.

2.4 Research gap

Although many enterprise security frameworks exist, as can be seen in the state of the art section, they are either designed for universal application and thus often too broad for SMEs, or they take only a general perspective without directly addressing the security needs of digital business models. The paradigm shift from business models to collaborative value networks with active data exchange requires a new perspective from an information security point of view. Subscription business models, in particular, are characteristically predestined to represent this change since they are based on highly frequent, condensed data exchange, a high degree of dependence of the partners on each other, and trust. Therefore, an investigation of information security in subscription models needs a target-oriented approach to conclude the security requirements of new digital business models.

3. Research Results

3.1 Identification of cyber security challenges in subscription business models

The motivation and structure of subscription business models described above suggest the need for intensive cyber security consideration. Figure 2 illustrates the various attack vectors that result from the way subscription business models work.

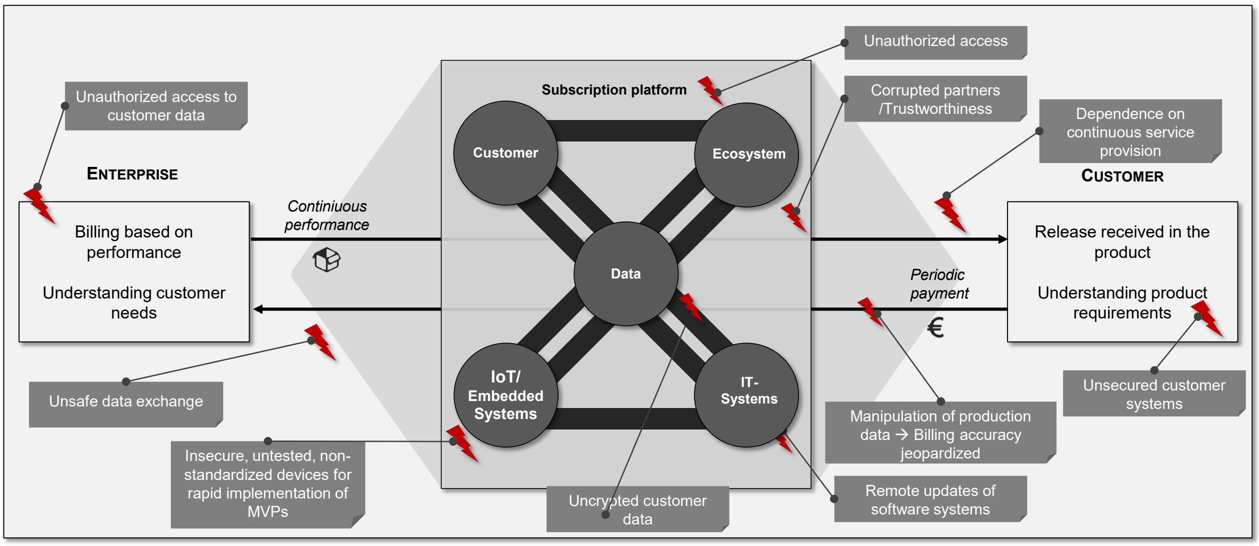
Unauthorized access
Subscription platform
Corrupted partners /Trustworthiness
Unauthorized access to customer data
Dependence on continuous service provision
ENTERPRISE
Customer
Ecosystem
CUSTOMER
Continiuous performance
Billing based on performance
Understanding customer needs
Release received in the product
Understanding product requirements
Data
Periodic payment
€
Unsafe data exchange
IoT/ Embedded Systems
IT-Systems
Unsecured customer systems
Manipulation of production data → Billing accuracy jeopardized
Insecure, untested, non-standardized devices for rapid implementation of MVPs
Uncrypted customer data
Remote updates of software systems

Figure 2: Attack vectors on subscription business models

The features presented in section 2.3 result in properties that require end-to-end protection. To ensure continuous service provision, we examine the dependencies on other systems and the interdependencies between the Stakeholders. In complex structures, continuous service provision is a critical factor for success on the customer side. As a result, this service provision is inevitably guaranteed constantly. It is also important to ensure correct billing depending on the type of subscription. This is done based on the time of usage, the number of units produced, or purely on a performance basis. The integrity and correctness of the data play a critical role. To bring a continuous increase in customer use in the sense of the value proposition, frequent exchange of, for example, production data, and performance data are necessary. This data is primarily used to optimize the product or the processes. On the buyer's end, there is a fear of intrusion into the protected corporate network and thereby endangering or losing sensitive product and production data. For this reason, enterprises prevent communication in and out of their network. In cases where this is inevitable (e.g., condition monitoring or remote maintenance), extensive legal safeguards are implemented. On the vendor or supplier end, the consumption volumes and correctness of usage information are indispensable to falsify payment information and save costs. Although buyers are merely users of the product, they have far-reaching access and thus also manipulation options. These options include data manipulation through unauthorized access to IT systems. This compromises the accuracy of production data and the associated invoice data, resulting in significant monetary damage. Since the financial damage caused by incorrect usage information or faulty configuration is substantial, it is in the vendor's best interest to secure the product against unauthorized manipulation by the customer or by third parties. This results in a paradigm shift in the area of facility operation: neither the physical access to the facility nor the IT network in which the facility is located is considered trustworthy anymore. The close relationship and connection between provider and customer make both sides potential gateways for hackers who can significantly influence the other party. It is becoming apparent that the interests of customers and providers are moving closer together. Information security must therefore shift from a purely singular view of one's own company to a holistic view as an ecosystem.

3.2 Top-down approach

In the following, we explain the schematic approach of the method developed in the future and the individual steps briefly. We divided the procedure for achieving a suitable method into four phases (Figure 3). First, we describe subscription business models based on their constituent characteristics from a cyber security perspective to derive use cases and resulting attack vectors based on these requirements. For this purpose, we assign subscription models to different types, based on STOPPEL supplemented by cyber security relevant aspects [20].

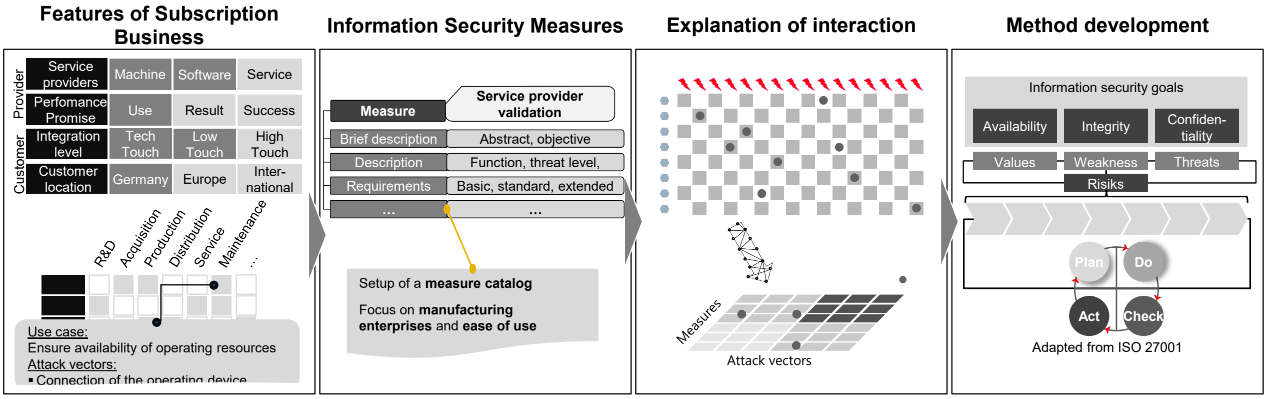

Figure 3: Components of the method development

The first type describes the pure availability of a product and represents the classic subscription model. At this stage, the supplier provides the customer with the machine or its service provision and maintenance in exchange for a periodic continuous payment. In addition to the transmission of payment data, there is no extensive data storage or transmission. Possible attack vectors on this type are, for example, manipulation of the payment information or influencing the machine at the customer's site, physically or via digital interfaces, to interrupt service provision.

The second type, usage-based, refers to billing based on effective production time or usage tracked in the payment interval. Terms such as pay-per-use or pay-per-hour are common in this context [21]. To enable this type of subscription, highly accurate tracking of machine usage is required. This is often measured in terms of uptime, to enable error-free and unambiguous billing. There is a risk that the transmitted usage time is manipulated and thus the billing does not correspond to the performed usage time. This can happen both by manipulating the machine itself, or the responsible functions and sensors and by manipulating the data itself.

This is followed by the third, result-dependent type. The reference figure used is the result of the use of infrastructure. Such systems are known as pay-per-unit or pay-per-part solutions, especially in operator models [22]. Whereas in usage-based models, the primary interest of the provider lies in the most intensive use of the infrastructure by the customer. In contrast, in outcome-based pricing systems, the provider focuses on achieving the outcome as efficiently as possible, according to which the provider is paid and for which he must pay. A possible attack vector is represented by the manipulation of the provided environment. There is the risk that the efficiency of the environment, as well as the quality and quantity of production, is negatively influenced, resulting in the need to prevent manipulation.

We describe the last type as performance-based. The reference of the value of the systems is the economic success resulting from interactions between supplier and customer. Customers pay a price for economic success, which is measured, for example, in terms of cost reductions, higher contribution margins, or profits. With a performance-based system, the provider also partially assumes the value risk in addition to the risks already discussed. The customer only has to pay if economic success is generated at all from the interaction with the provider. If this success is lower, the customer also pays a lower price. Preventing value creation or optimization through hacker attacks, denial of service or other attacks are critical variables to consider here, which greatly increase the risk on the provider's side.

In the second phase, after the features of the respective subscription model characteristics and their possible attack vectors have been discussed, we identify measures that minimize the described attack surface. To this end, we describe measures and their precise characteristics and scope concerning one or more attack vectors and classified them based on an evaluation catalog yet to be developed. This evaluation and description, which is still being prepared, is based on KÖNIGS [23]. Subsequently, in phase three, we explain cause-effect relationships between the identified attack vectors and the cataloged measures. We develop influence diagrams and influence matrices, based on the approach by PROBST AND GOMEZ [24], that make the relevance of the relationships for users transparent and understandable.

Based on the fundamentals now obtained, a method (phase 4) will be designed that secures the individual characteristics of subscription business models. To achieve this goal, we combine existing management approaches such as the ISO 27001 and the ISIS12 [25] procedure with a procedure based on the threat modeling described above. This method is composed of four core components:

1. Modeling of the targeted system to be built or modified based on characteristic properties
2. Use existing models such as STRIDE [26] to identify threats to the system described in step one
3. Addressing the identified threats based on the model applied in step two
4. Validation of completeness and efficiency

This approach of threat modeling serves to design methods and frameworks that are as close to the application as possible and that can efficiently deal with specific cyber security challenges. The intended result is a method that allows determining the own expression of the subscription model including the resulting attack vectors, corresponding measures, and their interaction to ensure a deployment roadmap for the implementation of the measures and transparency.

4. Contribution and Discussion

The contribution of this paper is a new way of looking at digital business models, especially subscription business models, from a cyber security perspective. We highlighted the motivation and necessity of these business models and described the resulting challenges. Furthermore, we explained the constitutive features of subscription transactions in more detail and, based on this, described different types and their characteristics. On this basis, specific cyber security challenges were described and their potential impact highlighted. In doing so, we have emphasized the criticality of the need for more intensive consideration. Finally, we presented an approach on how we want to solve this issue methodically. To this end, we outlined a four-step approach. The components will be detailed in the future and molded into a methodological procedure. The overall goal is to secure provider competitiveness on the one hand, and on the other hand, how customers are facilitated in their decision to use and accept subscription business models.

References

[1] Bundesministerium für Wirtschaft und Energie (BMWi), 2020. IIoT Value Chain Security – The Role of Trustworthiness, Berlin.

[2] Lassnig, M., Stabauer, P., Breitfuß, G., Müller, J.M., 2019. Erfolgreiche Konzepte und Handlungsempfehlungen für digitale Geschäftsmodellinnovationen, in: Meinhardt, S., Pflaum, A. (Eds.), Digitale Geschäftsmodelle – Band 1. Geschäftsmodell-Innovationen, digitale Transformation, digitale Plattformen, Internet der Dinge und Industrie 4.0. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 201–219.

[3] Widjaja, R., 2020. Focus: Subscription Economy: The Future of Business Models. https://cigp.com/insights/focus-subscription-economy-the-future-of-business-models. Accessed 12 February 2021.

[4] Henke, M., Schulte, A.T., Jakob, S., 2020. Blockchain-basiertes Supply Chain Management, in: Hompel, M. ten, Bauernhansl, T., Vogel-Heuser, B. (Eds.), Handbuch Industrie 4.0. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 599–615.

[5] Kaspersky, 2021. What is Cyber Security? https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. Accessed 9 March 2021.

[6] Kapoor, R., 2018. Ecosystems: broadening the locus of value creation. J Org Design 7 (1).

[7] Brush, K., 2019. Definition Digital Ecosystem. https://searchcio.techtarget.com/definition/digital-ecosystem. Accessed 9 March 2021.

[8] Canteli, A., 2018. Digital business ecosystem. OpenKM. https://www.openkm.com/blog/digital-business-ecosystem.html#:~:text=Written%20by%20Ana%20Canteli%20on,into%20clients%20and%2For%20subscribers. Accessed 18 March 2021.

[9] innolytics.ag, 2020. What is a digital business model? https://innolytics-innovation.com/digital-business-model/#:~:text=A%20digital%20business%20model%20is,customers%20are%20willing%20to%20pay. Accessed 18 March 2021.

[10] Bundesministerium für Wirtschaft und Energie (BMWi), 2017. Digitale Geschäftsmodelle: Themenheft Mittelstand-Digital, Berlin. https://www.bmwi.de/Redaktion/DE/Publikationen/Mittelstand/mittelstand-digital-digitale-geschaeftsmodelle.pdf?__blob=publicationFile&v=16.

[11] OWASP Foundation, 2021. Threat Modeling. https://owasp.org/www-community/Threat_Modeling. Accessed 23 March 2021.

[12] TÜV Süd, 2021. ISO/IEC 27001 - ISMS-Zertifizierug. https://www.tuvsud.com/de-de/dienstleistungen/auditierung-und-zertifizierung/cyber-security-zertifizierung/iso-27001. Accessed 27 March 2021.

[13] Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (DKE), 2020. IEC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung. https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung. Accessed 22.02.21.

[14] Seipel, C., 2020. EC 62443: Die internationale Normenreihe für Cybersecurity in der Industrieautomatisierung. DKE. https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung. Accessed 19 March 2021.

[15] Otto, B., Jürjens, J., Schon, J., Auer, S., Menz, N., Wenzel, S., Cirullies, J., 2016. Industrial Data Space - Digitale Souveränität über Daten (White Paper). White Paper, München, 40 pp.

[16] Forschungszentrum Data Spaces, 2020. Allgemeine Fragen zu den International Data Spaces. Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. https://www.dataspaces.fraunhofer.de/de/faq.html. Accessed 23 March 2021.

[17] Ebi, M., Hille, M., Doelle, C., Riesener, M., Schuh, G., 2019. Methodology for the risk and reward evaluation of industrial subscription models, in: Lehnert, Wulfsberg (Eds.), Production at the leading edge of technology. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 613–622.

[18] Gassmann, O., Csik, M., Frankenberger, K., 2014. The business model navigator: 55 models that will revolutionise your business. Pearson, Harlow, 387 pp.

[19] Wenger, L., 2019. Informationslogistik für Subskriptionsmodelle im Maschinen- und Anlagenbau: Vorstudiengespräch zum Dissertationsvorhaben. FiR an der RWTH Aachen, Aachen.

[20] Stoppel, E., 2016. Nutzungsabhängige Preissysteme auf industriellen Märkten. Springer Fachmedien Wiesbaden, Wiesbaden, 207 pp.

[21] Thiesse, F., Kohler, M., 2008. An Analysis of Usage-Based Pricing Policies for Smart Products. Elec. Markets 18 (3), 232–241.

[22] Decker, C., Paesler, S., 2004. Financing of Pay-on-Production-Models, in: Knorr, A., Lemper, A., Sell, A., Wohlmuth, K. (Eds.), Berichte aus dem Weltwirtschaftlichen Colloquiumder Universität Bremen, pp. 1–15.

[23] Königs, H.-P., 2017. Methoden und Werkzeuge für das Informations-Risikomanagement, in: Königs, H.-P. (Ed.), IT-Risikomanagement mit System. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 247–281.

[24] Probst, G., Gomez, P. (Eds.), 1991. Vernetztes Denken: Ganzheitliches Führen in der Praxis, 2., erweiterte Auflage ed. Gabler Verlag, Wiesbaden, Online-Ressource.

[25] IT-Sicherheitscluster e.V., 2020. Über ISIS12 - InformationsSicherheitsmanagementSystem in 12 Schritten, Regensburg. https://isis12.it-sicherheitscluster.de/ueber-isis12/. Accessed 27 March 2021.

[26] Wadhwa, M., 2020. A Beginners Guide to the STRIDE Security Threat Model. https://www.ockam.io/learn/blog/introduction_to_STRIDE_security_model. Accessed 15 March 2021.

Biography

Prof. Dr.-Ing. Dipl.-Wirt. Ing Günther Schuh (*1958) has held the chair of production systems engineering at RWTH Aachen University since 2002. Furthermore, he is the director of the Institute of Industrial Management (FIR) and a member of the board of directors of the Machine Tool Laboratory WZL at RWTH Aachen and the Frauenhofer Institute for Production Technology (IPT). He is co-founder of the electric vehicle manufacturers Streetscooter and e.GO Mobile.

Prof. Dr.-Ing Volker Stich (*1954) has been head of the Institute of Industrial Management (FIR) at the RWTH Aachen University since 1997. Prof. Dr.-Ing Volker Stich worked for 10 years for the St. Gobain-Automotive Group and led the management of European plant logistics. Also, he was responsible for the worldwide coordination of future vehicle development projects.

Jan Hicking (*1991) has been head of the division Information Management at FIR at RWTH Aachen University since 2020. Starting in 2016, he received his Ph.D. in 2020 in the field of intelligent products. As head of the division, he is responsible for multifaceted consulting and research projects.

Lars Kaminski (*1993) started working as a project manager at FIR at RWTH Aachen University in 2019. In his current position within the technical group IT complexity management, he specialized within IT architecture management and the development of transformation strategies concerning information security.

Jacques Engländer (*1992) has been working as a project manager at FIR at RWTH Aachen University since 2018. In his current position as part of the Information Management division, he supports companies in the design of IT strategies and information security management for organizational, technical, and cultural aspects.

Anna Majchrzak (*1990) has been a research student assistant at FIR at RWTH Aachen University since 2020. As a sociologist with an emphasis on the sociology of technology and organization, her primary research interests include organizational development, sociotechnical systems, and the impact of digital transformation in enterprises.