Journal of Machine Engineering, 2020, Vol. 20, No. 1, 117–126
ISSN 1895-7595 (Print) ISSN 2391-8071 (Online)

Received: *22 November 2019* / Accepted: *03 February 2020* / Published online: *05 March 2020*

distributed ledger,
service ecosystem,
cyber-pysical production system,
value networks

Gordon LEMME[1]
Diana LEMME[2*]
Kilian Armin NÖLSCHER[1]
Steffen IHLENFELDT[1,3]

TOWARDS SAFE SERVICE ECOSYSTEMS FOR PRODUCTION FOR VALUE NETWORKS AND MANUFACTURING MONITORING

In a global sales market with networked production steps and increasing complex machine tools, scaling service ecosystems for production provide an adequate solution for handling the generated data. The existing sensor equipment at current and the extension possibility by the System-of-Systems approach for existing machine tools can offer value-added services by the smart handling of production-related data. It is important to make these data validatable and exchangeable, taking into account to different protection goals. The trust of the individual actors in such a volatile value chain and the different (partly cross-border) value creation partners play an important role. The participation of a large number of these actors creates an attractive overall system (ecosystem) with lots of services and network effects. Concerning data security there are numerous aspects, which have not been adequately answered or taken into account in the use of a service ecosystem in the production environment. The paper discusses a distributed ecosystem for production on a distributed ledger-based service ecosystem, in which services can be mapped in the machine tool environment (e.g. calibration). This technology can be used for secure data exchange in order to discuss traceability and unchangeability of data while maintaining data sovereignty.

1. INTRODUCTION

The effectiveness of machine tools and the individuality of products have been gaining in importance in the last few years [1]. These characteristics of mechanical and plant engineering currently form a fundamental knowledge lead for Germany as a production location in view of the global market situation [2]. The most important components are a growing automation of the value chain as well as an increasing product individualization [3] with a successively improved quality. Companies are increasingly operating on global sales and procurement markets in order to exploit the economies of scale there, such as market size and cost advantages. In addition, new growth potential is opening up for these companies

[1] Fraunhofer Institute for Machine Tools and Forming Technology (IWU), Dresden
[2] Technische Universität Dresden – Institute of Software and Multimedia Technology, Dresden
[3] Technische Universität Dresden – Chair of Machine Tools Development and Adaptive Controls, Dresden
[*] E-mail: Diana.Lemme@tu-dresden.de
https://doi.org/10.36897/jme/118218

thanks to a significantly enlarged sales market. As a result of the increasing digitalization of individual processes, this globalization is characterized by more complex production and service networks and significantly increased information transparency. A traditional customer-supplier relationship that has existed for decades is no longer defined in such a form, which is why a previously existing basis of trust between the individual players does not necessarily have to exist. The digitalization and networking of mechanical and plant engineering forms the basis for an integrated process digitalization over the entire production life cycle and various value creation location (within the company and outside). In this way, volatile properties can be effectively considered throughout the entire process chain, processes can be stabilized or automated, and the increasing quality requirements can be met. At the same time, the individualization of service offerings is increasing, leading to a growing complexity of production and logistics processes. This complexity is no longer manageable with an increasing number of product features, shorter product life cycles, shorter delivery times, legal requirements and increasingly global value-added processes. The growing value creation networks require a redesign of the (digital) interface between producer and consumer, whereby a complete picture of the product creation process as well as the provision of information without media discontinuity is required. In order to meet these requirements, the amount of data provided, data quality and data security play an important role. Only then services can be offered on this data basis and the product development process be accelerated and individualized. This necessity turns data into an asset that needs to be increasingly valued and managed. Data thus forms the link between industrial production and product-accompanying services via smart services. In this paper a conceptual approach shall be presented to provide such services on data sets from the industrial environment (e.g. calibration data). The focus is on data sovereignty and data security as well as on later verifiability towards third parties.

2. ECOSYSTEM

In ancient Greek, “oikos” means the “house” and “sýstema” the “connection”. According to Kurt Jax, an ecosystem thus represents the combination of organisms of different categories in space and time [4]. A digital ecosystem pursues the overarching goal of overcoming complex, dynamic challenges in a scalable and efficient way [5]. A digital ecosystem imitates the behavior of biologically complex systems in order to build a dynamically adaptive overall system [5]. The characteristic of digital ecosystems is the combination of the economic and technological interpretation of the ecosystem concept, extended by the openness of the system. Since digital ecosystems combine a number of heterogeneous actors from different sectors and disciplines, it is also advisable to consider the network dimension [6]. In many cases, a platform forms the basis of such a network. If additional technical systems are actors, then one speaks of “smart ecosystems” [7]. Just like the individuals of a natural ecosystem, the actors also try to achieve certain goals. For this purpose, they are dependent on interaction with other actors of the digital ecosystem, but they also have to take into account predetermined framework conditions that can hardly be influenced.

Within an ecosystem, "things" are needed that the individual organisms contribute to the preservation and "justification of their being". In digital ecosystems, this is the infrastructure (e.g. marketplace) for the consumers [8] on the one hand that is as free of media discontinuity as possible, but in particular the provision of services on the other hand (e.g. machine calibration, process data analysis). Due to the increasing merging of consumers and producers into so-called prosumers [9], the clear demarcation between service recipient and service provider also becomes blurred. In this context, the term "smart service" refers to data-based, individually configurable offerings of services, digital services and products [10]. Platforms or digital marketplaces take over the tasks of bringing service providers with their various offers together with the service consumer. At present, digital services in mechanical and plant engineering are carried out on the basis of inventory data and data analyses is performed after process execution [11]. In the future, it will be important to bring services in mechanical and plant engineering as close as possible to the machine so that services can be provided more quickly and data can be analyzed as close as possible to real-time [12]. Digital ecosystems offer great potential in particular because they bring together growing networks with many different players and, alongside large mechanical engineering companies and control manufacturers, make it easier for small and medium-sized enterprises and start-ups to enter the mechanical engineering market. Within the industrial sector, production systems are usually cyber-physical production systems (CPPS) that allow the coupling and coordination of computing power and mechanical elements. Anke and Krenge [13] therefore also define smart services as "digital services for technical products that are provided as product service systems based on cyber-physical systems". While networked smart products and cyberphysical production systems represent the components and infrastructure of industry 4.0, smart services represent the services that can be provided through the further processing of the data collected by smart products [14].

2.1. SMART SERVICES

Allmendinger and Lombreglia [15] emphasize that Smart Services go beyond traditional product-related services such as maintenance in terms of their value to the customer and internal efficiency. They see three essential requirements for the provision of intelligent services. Basically, a connection to the Smart Product or to the data-generating machines for data acquisition must be established. In addition, the service provider must be able to interpret the collected data. In the case of corresponding automation of processes using smart services in the field of mechanical and plant engineering, the stored algorithms or models must be individually parameterized so that the collected data can be converted into valuable information. This creates a corresponding smart data management system in which the data can be assigned a (monetary) value. Finally, it is necessary to respond appropriately to the information generated, e.g. by initializing a calibration process on machine tools. For this type of automation, the operational processes must be designed and the (machine) systems involved qualified. The combination of a digital ecosystem and smart services offers great potential for optimizing machines and manufacturing processes in mechanical and plant engineering. With regard to implementation in mechanical and plant engineering, such

partial/full automation by smart services must never endanger machine safety. In addition, solutions must be developed to validate the correct provision or use of a service. This is the only way to realize a real data management with cash flow. Currently, there is a lack of implementation without media discontinuity where both data security and data sovereignty are ensured. The first approaches and concepts for this can be seen in the International Data Space project [16], although a corresponding practical implementation is still pending.

2.2. INFORMATION SECURITY

In order to make the service as such, the handling of the data provided for it and the use of calculation models transparent and secure for the parties involved, new approaches are needed in the handling of (process) data. Traditionally, the data is only exchanged between two parties (e.g. by e-mail, online platform), without a corresponding holistic evaluation being carried out and taken into account. Thus, it is conceivable that the data, which, as mentioned above, is an asset, may be transmitted unencrypted, accessible to everyone and usable as a result of digitisation, without the two parties being aware of it.

For the evaluation of security in IT systems, protection objectives are defined, which are subdivided into the following three main objectives Confidentiality, Integrity and Availability (CIA-Triad). These protection goals form the generic terms and can be differentiated more finely in order to allow a more detailed evaluation of data processing systems (see Table 1) [17]. Confidentiality describes the fact that data may only be changed or viewed by persons who are authorized to do so. If data is to be treated confidentially, it must be clearly defined who has access to this data and how. This can be done, for example, by suitable encryption of the data during transmission or persistence. Integrity guarantees the completeness of the data on the one hand and the correctness of the data on the other. It is irrelevant whether the data has been damaged by transmission or storage errors or altered by unauthorised persons. Changes to the data can be detected using cryptographically secure hash functions, for example. The protection goal "availability" includes the avoidance of system failures that lead to data or services not being usable.

Typically, availability is the ratio of the time the IT system is expected to function properly to the time it is expected not to function properly, with a value of 100% desirable. An appropriate measure to ensure availability is, for example, some degree of data redundancy or functionality.

The challenge is therefore to enable machine tools and equipment to provide data in a secure digital ecosystem pseudonymised and encrypted in order to use suitable smart services without losing data sovereignty. At the same time, it is necessary to be able to trace the provision of services, check data validity and initiate a payment flow. For this purpose, additional systems (e.g. embedded systems) with the corresponding interfaces both to the machine control system and to the digital ecosystem or machine controls themselves must have the ability to correspond directly to the digital ecosystem via an interface. Through a direct system connection, the targets for attacks by hackers are reduced solely to the machine control, which must be thoroughly protected by cryptographic procedures and equipped with sufficient computing power.

Table 1: Extended protection goals [18]

Privacy	Confidentiality requires appropriate measures for access control and encryption of data and information on data flows. It must be ensured that no information can reach unauthorized persons.
Unlinkability	If the observation of different events does not result in the observer being able to connect these events with an entity, it is the unlinkability of the events. The aim is to establish the confidentiality of actions or communication by concealing the affiliation of events in a system to entities.
Non traceability	Less general than unlinkability means that untraceability means that actions, events and communication content cannot be traced back to a single, identifiable entity. Measures for this are, for example, anonymization or aggregation.
Anonymity	As soon as the assignment of data to individual entities is no longer possible or disproportionately difficult, anonymity is given. It is the counterpart to authenticity.
Pseudonymity	A compromise between anonymity and authenticity can be created by pseudonymity. Thus it is not possible for unauthorized persons to assign the substitute entities and real entities to each other. However, it remains possible to assign the data to the individual substitute entities. Basis for the pseudonymity is an assignment of real entities to be replaced. If the assignment is lost or destroyed, pseudonymity becomes anonymity, because without suitable assignment rules or authentications, control over the substitute entities is not guaranteed beyond doubt.
Transparency	The protection objective of transparency is understood as a counterpart, but not necessarily as an opponent, to confidentiality. For example, it is necessary for an encryption procedure to be transparent (or verifiable) so that the resulting confidentiality can be classified as secure. In connection with legal aspects, it may also be necessary that certain processes be traceable.
Attributability	Attributability refers to the demonstrable, unambiguous assignment of actions, events and communications to one entity or, in the case of communication, to several entities. Proofability and non-deniability are synonymous with imputability.
Revision capability	If it is possible to document the actions and events in a system in a comprehensible and verifiable manner, the system has audit capability. There is a great similarity to accountability where the auditability is understood as a property of the system, but accountability focuses more on the entities of a system.
Authenticity	The authenticity protection objective ensures that data originates from a specific, identifiable entity. For this purpose, appropriate measures must ensure the unambiguous identification of the entities. Examples of such methods are passwords or proof of a signature.

2.3. BLOCKCHAIN TECHNOLOGY

The blockchain technology offers cryptographic approaches to achieve the various protection goals, whereby it is characterized by the fact that individual blocks consisting of a header and several transactions with process data are stored in a linearly concatenated list and connected by backward linking of the headers. Based on the distributed ledger technique, all participants (nodes) are able to have a local copy of the list (ledger). This enables manipulations of individual lists in the entire network to be detected and data integrity to be ensured. The agreement between all parties on a synchronized update of the list is made through appropriate distributed consensus mechanisms (e.g. Proof of Stake, Proof of Work, Proof of X). Distributed consensus-building mechanisms are methods that more or less randomly give the right to add a valid block to the existing chain in different ways. The blockchain technology also uses cryptographically secure hash methods to protect the data

structure from manipulation [19]. With the exception of the initial block, all subsequent blocks have a cryptographic reference to the previous block in the chain and can thus enable a secure order of all blocks. The second cryptographic tool for designing IT systems is digital signatures in addition to hash functions. Digital signatures can be compared analogously with handwritten signatures. To confirm this analogy, two criteria [19] must be fulfilled. On the one hand, only one person may use one's own signature to sign; on the other hand, each person can check the authenticity of this signature. The signature is thus firmly attached to the signed data record and cannot be transferred to other content. Digital signatures therefore authenticate the exchange of information between individuals or individual IT systems. In this way, everyone can determine whether the message sent was actually sent by the actual sender and whether the content was not manipulated. A functional extension of the transaction-oriented blockchain technology can be realized by so-called smart contracts. This development of Szabo [20] represents the basis for a digital, intermediate-free equivalent to conventional contracts, but could only be implemented as a suitable environment with the advent of blockchain technology. A smart contract within the framework of blockchain technology implements a digital, distributed process for the automated handling of if-then conditions. These are programs with a limited range of functions. For example, an assurance of claims can be made within the framework of a relationship between several parties that is not necessarily based on trust. Smart Contracts are stored in the blockchain and receive their own address or account, for example. To be able to use the process, a transaction with corresponding parameters is sent to this address. In addition, the results of a smart contract are stored decentrally on the block chain using a transaction and are therefore persistent and irreversible. After their creation, the Smart Contracts are written to the blockchain and are therefore final and unchangeable, which is why it is necessary that the corresponding program part has been carefully checked and saved. For the execution security of smart contracts it is also important that the program code is executed in a runtime environment. This runtime environment ensures that the program code does not gain unauthorized access to local resources, binds it to the block chain for reading and writing, and guarantees the deterministic execution of the smart contract.

2.4. CONCEPT & APPLICATION SCENARIO

As described above, the challenges for service ecosystems in the area of production technology are high complexity, fast data provision and the need for scaling. This complexity is furthered by the necessary use of edge devices or master computers to provide or calculate machine-oriented and time-determined information. In the production environment a shift of computing power from the (cloud) backend to the devices themselves (edge computing) increases this complexity enormously. Digital service ecosystems are complex per se, comprise numerous dynamic components, unite different stakeholders and realize their added value on provided data. Applications in the production environment are both business-critical, as they have a direct impact on the product or on the associated customer satisfaction, and on personal safety in the direct machine environment, as machine operators interact directly with the machines. Smart Services must therefore never lead to production downtimes or

disruptions. In addition to heterogeneous control systems and the underlying concepts, a holistic view of the machine environment also includes numerous other different data sources. These are individual sensors for recording context information (e.g. temperature), monitoring devices (e.g. tablets), complex Manufacturing Execution Systems (MES) and any other conceivable hardware in between. Digital service ecosystems therefore require sufficient flexibility to be able to collect and process the large amount of data.

The following picture is attached as a possible architectural model for an appropriate implementation concept. On the one hand, an embedded system is used to process the machine tool data and store the block chain contents (see Fig. *1*). This architecture enables context information, such as additional sensors (e. g. hall temperature [21]) via corresponding sensor nodes [22] for manufacturing monitoring, to be captured and merged at a central location. In addition, this approach allows older machines to be connected to a secure service platform by means of a retrofit, with temporary use (e.g. machine calibration, data acquisition for commissioning) to provide services. As a second architectural concept, all data (e.g. control data, context data from measuring system) are merged directly on the machine control system (see Fig. *1* without retrofit add-on), whereby the real-time capability of data acquisition and data synchronization is realized by the control system at the same time. For this a powerful control system is necessary to collect the data from different sources, preprocess them and encrypt or authenticate them according to the specifications of the blockchain. Such an implementation would make an additionally required embedded system superfluous and at the same time eliminate an attack vector (embedded system). The type of data storage is a question that has not yet been considered but is still relevant. Due to the expected sampling rates of several kHz on machine tools (e.g. measuring system), it is necessary to create the possibility to temporarily store these data in the sense of the application, to preprocess them depending on the service application, so that the necessary data quality for providing the service is maintained and to store them in encrypted form. To secure this data, symmetrical encryptions (e.g. one-time-pad, AES) can be used, which cannot be broken in terms of information theory and demonstrably. This data can then be stored on an available server in the Internet and a corresponding path can be saved in the blockchain. Nevertheless, solutions such as those discussed by the International Data Space are possible, in which data can be exchanged directly between the service recipient and the service provider (and vice versa), so that no storage space is required on servers available worldwide. With this solution, it is not possible to provide services based on historically multiple data (e.g. anomaly detection in machine tool behavior) and differently involved service providers without providing the complete data sets again. The same applies if several service providers are able to provide a service on one data set, in which case a corresponding increase in traffic becomes necessary. In order to reduce the pure amount of data within the blockchain, only the necessary meta information (e.g. keys, paths, partners) and smart contracts are stored to automate the entire system. The symmetric key for data access, the data end point (where the data is located) and the necessary access authorization (e.g. number of accesses) are stored in the block chain by asynchronous encryption and signature of the participating partners. This allows data access regulations for different service providers to be granted by several entries in the block chain or by means of smart contracts on one and the same data record. By means of suitable interfaces to the machine tool or embedded system and with the aid of an attractive

front-end for a marketplace, this architecture creates an infrastructure for a digital ecosystem in which the parties involved do not necessarily have to trust each other, but can nevertheless operate a verifiable and secure economic relationship. By mapping the process via the blockchain, it is possible to track the data transfer via the hashed values without being able to conclude on the data and thus also to realize a later payment flow after completion of the service. This payment flow can also be completely self-sufficient through the use of a smart contract. In addition, the machine operator can determine the storage location of the data provided himself, so that his own server can also be taken into account and data sovereignty is secured. With symmetric encryption (e.g. one-time-pad, AES) of the process data, it is impossible to decrypt the data without the corresponding symmetric key, so that it can be stored securely from attackers and third parties.

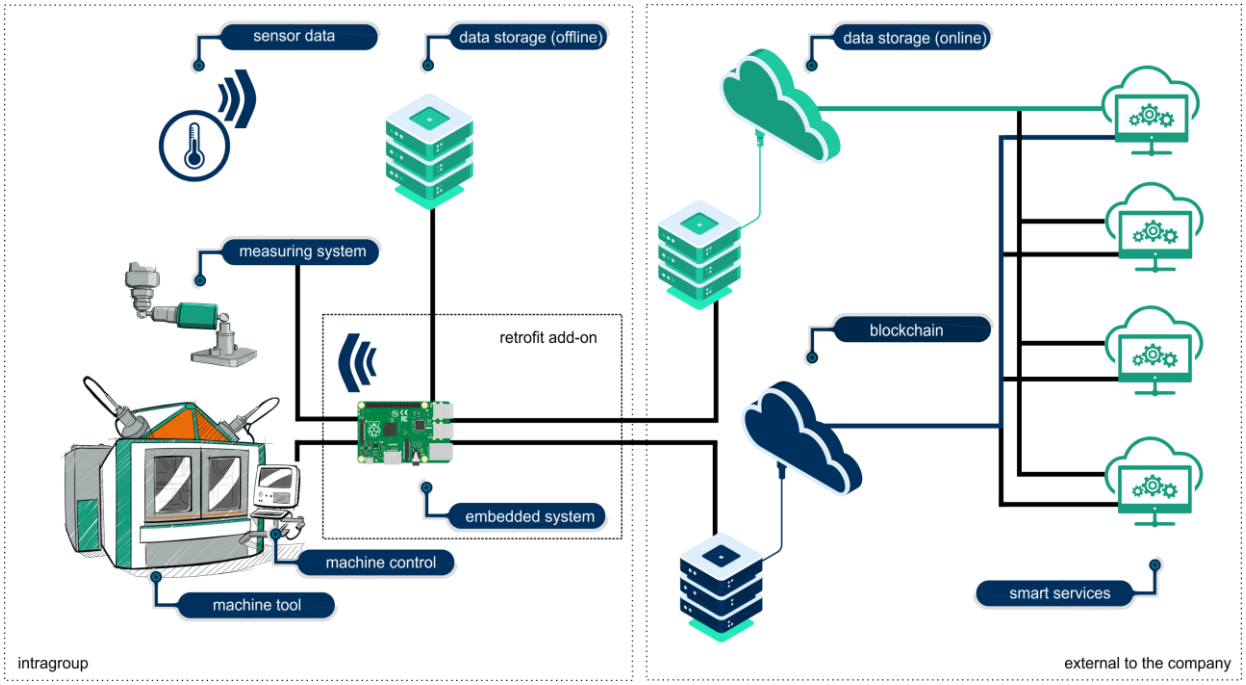

Fig. 1. Architecture with embedded system (retrofit)

In order to validate such an IT infrastructure in the machine tool environment, corresponding qualitative as well as quantitative criteria must be defined by the end application. Due to the heterogeneity in machine and plant engineering, these can also be very divergent. In principle, such systems can be evaluated by pure performance criteria, flexibility and cost reduction, using methods of utility value analysis, cost comparison or benchmark tests. In benchmark tests, quantitative criteria are defined which compare a distributed ledger-based system with a conventional service system. Aspects such as latency (especially runtime delay, transmission delay, processing delay, queue delay) and serialization delay (corresponds to data quantity/data rate) are used for a quantitative comparison. At the same time, however, the added value created by such an architecture must be evaluated. In a distributed ledger-based system, aspects of information security (confidentiality, availability, integrity) exist per design, whereby confidentiality can be "openly designed" (public vs. private distributed

ledger). In addition, competitive advantages and productivity increases result, which must be considered individually with an impact chain analysis or a utility value analysis. These added values must be included in a system validation to ensure a holistic view.

3. SUMMARY

The paper presented an approach for securely storing production-related data and making it available for verifiable services. For this purpose, two architectures were presented in which the protection goals of confidentiality, integrity and availability are taken into account using Blockchain Technology. These concepts follow on from the considerations on International Data Space and security by design through blockchain technology. Existing machine tools that can be connected to a corresponding ecosystem using an embedded system were also taken into account. In addition, the paper also points out possibilities for storing context information from sensor nodes securely and traceably, so that options for media-break-free digitalization can be provided by means of services on the hall floor. The young technology of the blockchain still poses numerous challenges in mechanical and plant engineering. These include the lack of standards as well as proof of practical suitability on the hall floor. In particular, the consensus procedures to be used for data validation, the associated consensus-building time and aspects relating to participation (permissioned vs. permissionless blockchain) as well as rule-setting in the digital ecosystem remain unanswered for the time being. Furthermore, there is no knowledge about the scaling of such a blockchain-based ecosystem. Here we can only fall back on experience in dealing with crypto currencies, whereby the number of transactions is probably considerably lower than in a digital service ecosystem for machine and plant construction with thousands of machine tools and countless smart services. This requires explorative investigations and reliable projections in order to implement such a system sustainably. In addition, the statements made are based on the assumption that the data can be collected within the framework of discrete manufacturing processes or measurement processes and that corresponding block formations can be carried out. Further research is needed to encrypt and verifiably store the data of a continuous process for use in order to be able to offer condition monitoring services, for example.

ACKNOWLEDGEMENTS

This Paper has been financed by BMWi Program "Smarte Datenwirtschaft" – Project "AUDlo-Auditlösung für ML-basierte, datengetriebene Dienstleistungen" Reg.-Nr.: 01MD19005, Germany. It was supported by the Federal Ministry for Economic Affairs and Energy (BMWi) based on a decision taken by the German Bundestag. This work was also supported by the Fraunhofer Internal Programmes under Grant No. MEF 836273.

REFERENCES

[1] DISPAN J., 2017, *Entwicklungstrends im Werkzeugmaschinenbau*, Hans-Böckler-Stiftung.
[2] NEUGEBAUER R., 2012, *Werkzeugmaschinen*, Springer-Verlag Berlin Heidelberg.

[3] BARNER A., 2013, *Perspektivenpapier der Forschungsunion: Wohlstand durch Forschung – Vor welchen Aufgaben steht Deutschland?*, Wirtschaft-Wissenschaft.
[4] JAX K., 2010, *Ecosystem Functioning*, Cambridge University Press.
[5] MASAK D., 2008, *Digitale Ökosysteme,* Springer-Verlag Berlin Heidelberg.
[6] ALVEDALEN J., BOSCHMA R., 2017, *A critical review of entrepreneurial ecosystems research*: towards *a future research agenda*, European Planning Studies, 25/6, 887–903.
[7] DIECKHOFF P., 2018, *Biologische Transformation und Bioökonomie*, Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., München.
[8] BULLINGER H.J., MEIREN T., NÄGELE R., 2015, *Smart Services in Manufacturing Companies*, International Conference on Production Research, ICPR, Manila, Philippines, 23.
[9] TAPSCOTT D., WILLIAMS A.D., 2010, *How Mass Collaboration Changes Everything*, Penguin Random House.
[10] Fraunhofer IAO, 2019, Smart_Services, https://wiki.iao.fraunhofer.de/index.php/Smart_Services, (Accessed 20 11 2019).
[11] Arbeitskreis Smart Service Welt, 2015, *Smart Service Welt – Umsetzungsempfehlungen für das Zukunftsprojekt internetbasierte Dienste für die Wirtschaft*, Abschlussbericht, Berlin, acatech.
[12] TOMBEIL A.S., NEUHÜTTLER., GANZ J.W., 2016, *Dienstleistungsproduktivität und qualität*: eine kritische *Würdigung*, EXIS, In book: Kundenbindung durch kosteneffiziente Service Excellence, 51–68.
[13] ANKE J., KRENGE J., 2016, *Prototyp eines Tools zur Abschätzung der Wirtschaftlichkeit von Smart Services für vernetzte* P*rodukte*, Multikonferenz Wirtschaftsinformatik (MKWI), Ilmenau, Germany, 1275–1286.
[14] QUACK K., 2015, *Smart Services – die nutzerorientierte Schwester der Industrie 4.0*, CeBIT-Nachrichten.
[15] ALLMENDINGER G., LOMBREGLIA R., 2005, *Four Strategies for the Age of Smart Services*, Harvard Business Review, 83/10, 131–134, 136, 138.
[16] International Data Space Association, 2019, Available: https://www.internationaldataspaces.org/, (Accessed 20 11 2019).
[17] BEDNER M., ACKERMANN T., 2010, *Schutzziele der IT-Sicherheit*, DuD, Datenschutz und Datensicherheit, 323–326.
[18] BLESS R., MINK S., BLAß E.O., CONRAD M., HOF H.J., KUTZNER K., SCHÖLLER M., 2010, *Datenschutz und Datensicherheit, in Sichere Netzwerkkommunikation – Grundlagen*, Protokolle und Architekturen, 323–328.
[19] NARAYANAN A., BONNEAU J., FELTEN E., MILLER A., GOLDFELDER S., 2016, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.
[20] SZABO N., 1997, *The Idea of Smart Contracts*, Satoshi Nakamoto Institute.
[21] LEMME G., NÖLSCHER K.A., 2019, *Demo: Wireless sensor network for retrofitting production systems*, 18 Fachgespräch Sensornetze der GI/ITG Fachgruppe, Kommunikation und Verteilte Systeme, Magdeburg.
[22] LEMME G., NÖLSCHER K.A., 2019, *Wireless sensor network for retrofitting production systems*, 18 Fachgespräch Sensornetze der GI/ITG Fachgruppe, Kommunikation und Verteilte Systeme, Magdeburg.