2nd Conference on Production Systems and Logistics

Dedicated Data Sovereignty as Enabler for Platform-Based Business Models

Sander Lass[1], Benedict Bender[1]
[1] *Chair of Business Informatics, esp. Processes and Systems, University of Potsdam, Germany*

Abstract

The digitalization of value networks holds out the prospect of many advantages for the participating companies. Utilizing information platforms, cross-company data exchange enables increased efficiency of collaboration and offers space for new business models and services. In addition to the technological challenges, the fear of know-how leakage appears to be a significant roadblock that hinders the beneficial realization of new business models in digital ecosystems. This paper provides the necessary building blocks of digital participation and, in particular, classifies the issue of trust creation within it as a significant success factor. Based on these findings, it presents a solution concept that, by linking the identified building blocks, offers the individual actors of the digital value network the opportunity to retain sovereignty over their data and know-how and to use the potential of extensive networking. In particular, the presented concept takes into account the relevant dilemma, that every actor (e. g. the machine users) has to be able to control his communicated data at any time and have sufficient possibilities for intervention that, on the one hand, satisfy the need for protection of his knowledge and, on the other hand, do not excessively diminish the benefits of the system or the business. Taking up this perspective, this paper introduces dedicated data sovereignty and shows a possible implementation concept.

Keywords

information gateway; data security; information flow control; platform acceptance

1. Introduction

Digitalization provides technologies and concepts for realizing the integration of business-relevant information across the entire value chain. In particular, cross-company information platforms are a general approach in this respect. In conjunction with the Internet of Things (IoT), there is potential for manufacturing companies to ensure their competitiveness in the future. IoT-based systems and their integration by means of information platforms make it possible to link a large number of data sources and network them into advantageous value creation networks. Cross-company networking in production has already demonstrated its fundamental potential in the automotive industry [1]. By participating in platform ecosystems, companies can encounter cost pressure in the core business. Digital business models allow internal product and process optimization for the platform players machine suppliers, machine users, suppliers and the customer.

With numerous IoT-based platforms and various clouds, solutions exist that are already available as a usable product, at least from the perspective of their providers [2], [3]. Hyperscalers (AWS, Microsoft Azure and Google Cloud Platform) also offer basic functions in terms of computing power, storage and networks. Looking at actual use in practice, the potential users do not seem to share this optimism: deployment occurs hesitantly and use of information platforms, despite their potential, is low.

The result is a low level of information exchange between value creation partners and level of digitization across entire industrys [4], [5]. Since companies as actors in value chains are shaping socio-technical systems, possible reasons are the perceived risks which, from the companies' point of view, have not yet been addressed to a sufficient extent and are working against actual comprehensive use. According to Gartner, IoT platforms are in the phase through of disillusionment [6]. The task is to identify solutions based on key challenges that will help to implement digitized value networks in a targeted manner. Taking up this perspective, this article introduces dedicated data sovereignty and shows a possible variant of implementation.

1.1. Research question and expected results

Experience with cloud-based ERP shows that the fear of a know-how leak is a relevant roadblock among potential users [7]. This leads to the thesis that trust creation plays a significant role and that ensuring perceptible data sovereignty is therefore an important success factor for the effective establishment of future value creation networks. The implication of this thesis is that the cross-company exchange of information as a fundamental part of digital value networks must be designed in such a way that the participating companies do not have to fear a leakage of their know-how. This makes controlled communication indispensable. The dilemma: It must be ensured that every actor (e.g., the machine users) can control the communicated data at any time and at an effort-adequate level, and that there are sufficient options for intervention that satisfy the need for protection on the one hand and do not excessively diminish the system benefits on the other. For SMEs in particular, this is a challenging task that has to be mastered in addition to day-to-day business.

Thus, there is a need for suitable concept of principles that serves as a basis for the development of such solutions. Solutions that avoid the perceived loss of control if data is passed on to external systems (e.g., cloud-based services or SaaS applications) and still make the aforementioned positive aspects usable. Solutions that create trust through the appropriate regulation of information flows bring acceptance for the active co-design of future ecosystems. In this respect, the following relevant research questions arise with regard to the establishment of platform-based business models in future value creation networks: **Is the fear of know-how outflow actually a misson-critical obstacle? How can the data sovereignty of individual actors within shared platforms be achieved with reasonable effort?** Subsidiary results from the knowledge process are: What is the significance of trust creation for the establishment of digital value networks? Which building blocks are success factors for connection to IoT platforms?

Taking up the above thesis, the identification of the obstacles confirms the high importance of trust creation within value networks. A reference model of the necessary building blocks systematizes the implementation of the platform connection. In this context, the reference model is to be understood as a model which, on the one hand, concretizes certain aspects of the mapping space (delimitation of metamodel) and, on the other hand, offers room for adaptation to concrete use cases (delimitation of model). It serves as a basis for a systematic approach and forms a framework for further operationalization to concrete use cases. With the goal of effective trust creation, we introduce dedicated data sovereignty, a concept that ensures appropriate know-how protection. Part of the dedicated data sovereignty is the concept of a controlling entity - an information firewall. This element acts as part of the corporate network and provides extensive control of information flow. This avoids the creation of another external actor that appears to be independent, but results in respect to its viable business model in additional cost and effort. The Information-Firewall provides the concept which takes over the tasks of information flow control within the corporate structure. Synergistically, the device also offers the prospect of further added value (e.g. retrofit).

1.2. Methodology of research process

The first part of the research process is the problem analysis with an identification and structuring of the obstacles that hinder the use of cross-company information platforms and platform-based business models. It starts with investigating the lack of participation in cross-company information platforms, carried out in

the first instance by means of interviews with companies to identify practical obstacle reasons. For the purpose of consolidation and supplementation, a focused literature research follows in the second instance. The latter forms part of the state of Research. It follows by the elaboration of trust creation as an essential key factor follows. The resulting findings are then used to identify relevant fields of action. Based on this, the development of a solution approach follows. This begins with the data privacy approach and shows the current state of research in this area. Subsequently, security-relevant model elements are determined and linked in the concept of information firewalls. In addition, an implementation proposal results, which carries out the operationalization and enables the implementation for existing systems.

2. Problem analysis

The analysis begins with a practical perspective, considers possible solutions and derives implications. Thus, it links practical needs and theoretical solutions to a model of the relevant solution modules.

2.1. Practitioner's perspective

The situation from a practical perspective is documented in the results of 18 interviews with players in manufacturing SMEs (managing directors, IT managers, production managers; end of 2019). The guideline-based design allows sufficient freedom in the choice of areas of observation and their detailing, while still maintaining the focus. With regard to the use of platforms, the guideline covers the perception of the potentials, the experiences to date and the status of implementation, viewed from the perspectives of people, technology and organization. In summary, the following findings result.

The existing heterogeneous IT and automation landscape and the lack of integration capability of the production objects make the holistic implementation of platform projects difficult. There are too few standardized interfaces that allow the configuration and comprehensive connection of the systems involved in a way that is commensurate with the effort involved and overcomes the partial closeness of proprietary isolated solutions. Implementation also fails because of the specifics of the situation at hand. Although there is consensus on the theoretical application potential, difficulties arise in the individual adaptation. The selection and configuration of the appropriate technological and organizational elements and their sustainable combination represent hurdles. This also includes the lack of migration strategies that enable systematic and targeted further development of the existing systems (brown field), as well as the provision of human resources, since all employees are typically tied up in day-to-day business in SMEs.

Furthermore, the individual benefits of digitizing processes cannot be adequately demonstrated without suitable evaluation tools for potential investment decisions. The only partial evaluation of possible solution modules leads to false expectations and misjudgments on the part of those responsible and decision-makers. In addition to these technical and organizational reasons, the psychosocial dimension is also part of the problem with the fear of a know-how drain. Since control of the data actually communicated to the platform during operation cannot be adequately ensured, these concerns lead to the decision not to connect to and use the platform. In summary, significant obstacles exist within the enabling prerequisite, the implementation as well as the operation. This general structuring into this issue areas is applied in the following for further elaboration.

2.2. Detailing the issue areas

The next step of the knowledge process aims at a supplementary consideration of the reasons for obstacles by means of literature research and their systematization. The guiding question of the literature research is that of building blocks that make an essential contribution within the issue areas mentioned.

From a technological point of view, IoT systems arise from the connection of people, objects and systems [8], which interact as actors in a communication structure. Industry 4.0 as the production-related manifestation of the IoT names cyber-physical systems (CPS) and their extensive networking as essential elements that use embedded systems (ES) to equip objects with the necessary capabilities and upgrade them to IoT devices [9], [10]. Consequently, high penetration is a prerequisite for the economic implementation of CPS and their linkage to cyber-physical production systems (CPPS). The same applies to other technologies (e.g., AutoID, localization with GPS or beacons, algorithms for search and analysis such as deep learning) that realize essential capabilities of the IoT system elements. Thus, **technology availability** emerges as part of the issue area enabling prerequisite.

Networking to form an IoT communication architecture implies three potential levels of action for the system elements involved: environmental interaction with sensing by sensors and action by actuators, the gateway level as an essential network element, and the IoT platform as a higher level of data storage and processing [11]. Grounded in their ability to process information locally, IoT devices can not only be used for mere data collection, but can also act as an IoT gateway, if necessary, which handles communication to the next higher level (typically a cloud) (e.g., via HTTP/REST-based data transfer or via MQTT protocol) [12]. These gateways are equipped with various network interfaces and, in addition to pure data transmission, can also act as translators or intermediaries and perform preprocessing of the data (e.g., filtering, aggregation) locally [13]. Within the cloud, the cross-element evaluation of the accruing data and integration of the results into the company's business processes takes place. Possible variants are the private cloud on premise in the company or the external variant using cloud service providers [14]. Existing IT architectures must therefore have a suitable architecture concept that fundamentally permits this distribution of tasks for the system elements mentioned. **Architecture concepts** forms a further component of the issue area enabling prerequisite.

Taking up the above IoT communication structure, IoT platforms are software systems that connect objects or devices [15] and provide or allow the development of applications for data storage, analysis or visualization. To structure the architecture of IoT, typical models concretize the three task domains into a five-layer model with typically device, connectivity, processing, application, and security layers [16]. The latter three form the IoT platform in a narrow sense. The processing layer includes device management (with identification and health monitoring) and data preparation, among others. The application layer provides applications for information retrieval, some of which cover domain-specific use cases or can be created by external actors. Also part of an IoT platform is a security concept. Other reference models make further differentiation into functions and tasks or directly include business models and processes (e.g., ten task areas [14], eleven criteria [17]) and thus offer a broader perspective. In existing platform offerings, the aforementioned tasks are implemented or configurable to varying extents. Particularly relevant components are standardized interfaces to third-party systems, IoT data analytics and the provision of mobile applications, as well as support for a wide range of communication protocols [18]. This shows success-critical factors for the implementation of IoT platforms. The component IoT platform offer, i.e. **portfolio available on the market**, is also part of the enabling prerequisites issue area.

For the demonstration of use and validation of potential solutions, a suitable set of tools for evaluation is needed. The demand for such testing and validation tools is also evident from the increasing address in the relevant funding programs of science and practice as well as in political and industrial initiatives: As so-called "test centers", they are an essential part of the respective intended solution strategy [19], [20]). In terms of the structuring used, the **solution evaluation** is located in the implementation issue area.

In particular, the topics of interfaces and communication protocols point to the technical challenges of integration within heterogeneous and evolved IT and automation landscapes. Since it cannot be assumed that existing systems will be replaced by new copies without further ado, the implication arises that existing systems must be enabled in a suitable form to act as part of an IoT platform. In particular, the integration of closed legacy systems forms a typical use case [21], [22]. Reasons are the necessary investment protection,

the new acquisition of machines or systems is rarely a real option for SMEs. An implementation within existing systems is inevitable. Thus, **brownfield** is part of the problem area implementation.

Various middleware concepts (such as the Reference Architecture Model Industry 4.0 (RAMI 4.0) [23]) exist to enable existing production facilities. These work on a very abstract level and offer little help for operational implementation. Thus, these general concepts require further concretization (e.g., in the form of configurable migration strategies). They must also address the specifics of the situation at hand, but at the same time follow standards in order to avoid isolated solutions or lock-in effects. Target-oriented **individualization** is another building block within the issue area of implementation.

The use of the Internet Protocol (IP) in the IoT gives the impression of simple implementation of global end-to-end communication. Looking at the differentiation into signal, data, information and aggregation levels [24], this is largely true only on the first two levels. On the information or aggregation level, this is not the case. The inclusion of semantic aspects or complex data structures, preprocessing and aggregation, or the provision of functions at a high level of abstraction for communication and operation is not sufficiently available and requires further concerted work [25]. This means production objects can only exchange data, but no full interoperability has been implemented at the application level of the IoT structural model in a practical way. Currently, there are only islands of interoperability provided by the individual reference architectures from different application domains [26]. In other words, objects just talk but do not understand each other sufficiently. After all, some commonly used application-level protocols have been established for connecting machines to cloud services, which provide a basis for solving the lack of communication capabilities. These include MQTT (Message Queue Telemetry Transport) for message exchange between devices, LWM2M (Lightweight Machine-to-Machine) for IoT device management, and OPC-UA (Open Platform Communication Unified Architecture) for communication between machines. Thus, **semantic interoperability** is also part of the implementation problem domain.

The commitment of the stakeholders is an important success factor in the introduction and use of innovations and counteracts possible negative consequences such as the deliberate delaying or slowing down of the change or even the failure of the project [27]. Acceptance is also characterized by the perception of risks and barriers when (potential) customers use IoT and cloud computing [28]. In particular, the assessment of the trustworthiness of the provider is a critical factor for success in this respect [29]. The fact that shop-floor IT is no longer an isolated entity that can only be accessed physically means that new threat scenarios are emerging (see Stuxnet, Duqu, etc.). As a consequence, new challenges arise for security concepts and their practical implementation in the factory [30]. On the other hand, a security concept must protect the know-how about production processes and manufacturing methods from uncontrolled outflow [31], which is also essential in the ecosystem [32]. Know-how protection is particularly important due to the high degree of networking of the IoT and its need for communication relevant to its use. Suitable measures are not only important in the initial design (cf. security by design). Rather, in daily operation, maintenance and necessary adaptation are highly relevant. For this reason, **know-how assurance** is classified as an essential component of subject area operation, as is **user acceptance** especially its upholding, which promotes a high degree of utilization of the system element in question.

The required ability to adapt to changing conditions during operation addresses adaptability. As the adaptation to changing conditions by the system itself, it is, in addition to efficiency, a further requirement with regard to the competitiveness of companies [33]. Concepts of adaptability provide more suitable design means and solution paths for permanent and rapid adaptation of the internal organization and technology [34]. Also in the context of digitalization, platform-based ecosystems and new business models, mutability is a desirable property of the overall enterprise system, whose architecture forms the basis for changing business models from within and changes due to competition and new technologies from outside [35]. Consequently, the system as well as the system element must offer internal user suitable options for implement-

ing future change requirements in an effort-appropriate manner. Since not all change requirements are foreseeable during implementation, **adaptability** is taken into account as a further component of the issue area "operation". Figure 1 summarizes the resulting elements from the identified obstacle reasons and influencing factors, structured into the three issue areas prerequisites/enablers, implementation and operation. Also included are the perceived levels of maturity, which was part of the insight validation with the interview partners.

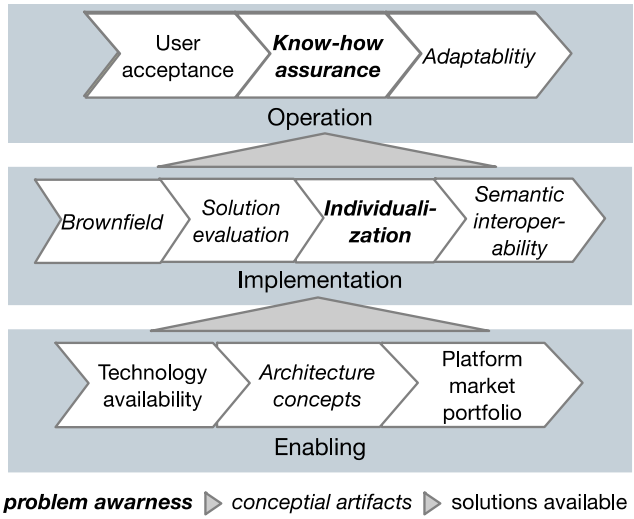

Figure 1: Building blocks for platform application and maturity

2.3. Implications

In line with the fact that psychosocial aspects are also relevant within change management for the actual use of innovations in addition to the technical and organizational perspective, concerns and worries on the part of potential users are important for acceptance and the probability of benefits. In the case of external information platforms, this relates in particular to fears of a loss of know-how. To counter these, it must be ensured that every actor (e.g., the machine users) can control the communicated data at any time and that there are sufficient intervention options which, on the one hand, satisfy the need for protection and, on the other hand, do not excessively diminish the system benefits. Existing authorization concepts must be checked in this respect or adapted to the extended data availability. A suitable data structuring with associated rights and appropriate data granularity is still missing.

The control of the actually communicated data is an essential consequence. The implication for action is therefore to ensure appropriate data sovereignty with respect to the platform connection by means of controlled communication that is transparent to the data owner at all times. Ensuring data sovereignty becomes an effectiveness-determining task in the use of information platforms and the realization of platform-based business models in this regard. Furthermore, this task does not have a "static" problem solution, but requires an adaptable solution that implements control loops, if necessary, in order to be able to make adjustments and further developments during operations and to react appropriately to new external and internal requirements. A particular challenge for SMEs is both the implementation and operation of these control loops, which implies the use of appropriate automation and configuration. These control loops need an effective runtime environment within the overall architecture and external knowledge of the business transactions at the meta-model level.

3. Dedicated data sovereignty

The particular challenge is to restrict the flow of information without impairing the functions of the platform ecosystem, i.e., without too much or too little data flowing out of the company. Thus, suitable mechanisms are required that on the one hand realize the fundamental data sovereignty, but on the other hand also address

the information needs of the network partners in an expedient manner and adapt the communicated data to this purpose. This tailored data sovereignty is referred to as dedicated data sovereignty. The dedicated data sovereignty approach takes up the influencing factors that have been identified and derives a reference model of the necessary building blocks for implementation.

3.1. Starting point data privacy

Trust creation as a basis for acceptance and application is well recognized. Trust and Privacy is one of the key challenges in respect of the adoption of Internet of Things [36], wich is the collective term for future connecting system concepts. Likewise, the Gaia-X initiative of the BmWI points to trust, digital sovereignty and self-determination as relevant goals and recommends addressing them within modern cross-company data infrastructures [37]. In this respect, this initiative names digital sovereignty as a part of the implementation. An essential element here is data sovereignty, which concretizes the goal: complete control over stored and processed data and also the independent decision on who is permitted to have access to it.

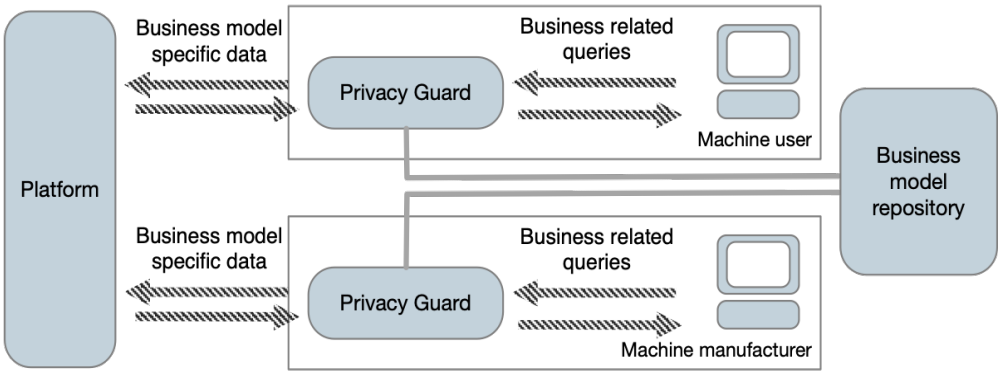

Figure 2: Implementation by using information gateways with a firewall function

Starting point data privacy: There are already approaches from data protection (e.g. BSI-Grundschutz) which can serve both methodically and in terms of content as a basis for developing an adequate adaptation to the IoT in the area of discourse being worked on. Various principles and paradigms exist here that serve as the starting point for further conceptualization of the reference model. A first operationalization is provided by [38]. The basic principle is data sparseness (minimize) with the restriction to the provision of the actually required data of the respective business activity. This implies the sufficient definition and delimitation of the respective use cases. In addition, encryption and anonymization (hide) ensure secure communication and appropriate information reduction. Distributed data storage and analysis (seprate) can reduce the risk of knowledge leakage by scattering information fragments, since the complete picture is not fully accessible to anyone, as can early aggregation into groups (aggregate) through local data aggregation. Both measures require appropriate data classification. Organizationally, transparency with regard to data collection, processing and dissemination as well as loss through attacks (inform) and the maintenance of control by the data owner (control) must be realized. The enforcement of data protection laws (enforce) and the demonstration of enforcement (demonstrate) also have an effect in this sense and may have a regulatory requirement. All building blocks are to be anchored in the architecture through technical and organizational measures (privacy by design).

The requirements of data economy in combination with the diversity of platform-based business transactions give rise to the need for scalable anonymization, i.e., the implementation of different degrees of anonymization and pseudonymization. Approaches are provided, for example, by Marnau with k-anonymity [39] and Ulbricht [40]. The differential privacy approach (cf. [41]) implies the multi-level design using gateway-like software elements. The gateway element allows security and pre-processing at the user's end. Figure 2 shows this approach. It extends the classic firewall with business related abilities, replacing static blocking of information flows with customized business case dependent filtering. The question remains open as to how

the gateway element must be designed and how it can be ensured with regard to the requirement of appropriate integration and low-effort operation. Building on these basic approaches results in the concept of the information firewall. This concept of an information-firewall provides a solution to control the communicated data regarding actor-specific requirements for high transparency of the data flows as well as necessary interventions by the respective stakeholders.

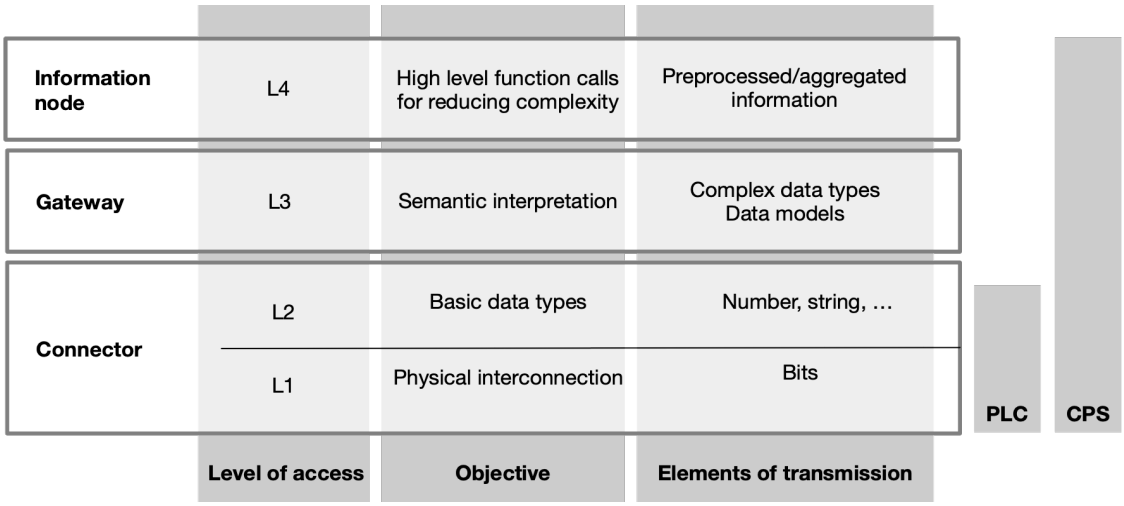

Figure 3: Classification and requirements for an information gateway

Figure 3 shows the requirements for such a component and makes a classification as well as a distinction from typical device classes. An information gateway with firewall function operates at the level of an information node. These capabilities can be realized, for example, as an independent component between production objects (e.g., machine) and platform by an edge controller device (see [20]).

3.2. Reference model

In addition to the hardware and software concepts for an information gateway, further building blocks are required which, as elements of the surrounding overall system, represent the prerequisites for effective deployment. Applying the structure of organization, technology and human, the building blocks shown in Figure 4. As an example, the user access module is detailed here (Figure 5). The data sources (left) and the platform (right) are visible. In between, the information firewall is realized by means of the information gateways and I4.0 box, which regulate the flow of information as a connecting element and in this case provide the necessary functions by means of agents and automate them appropriately.

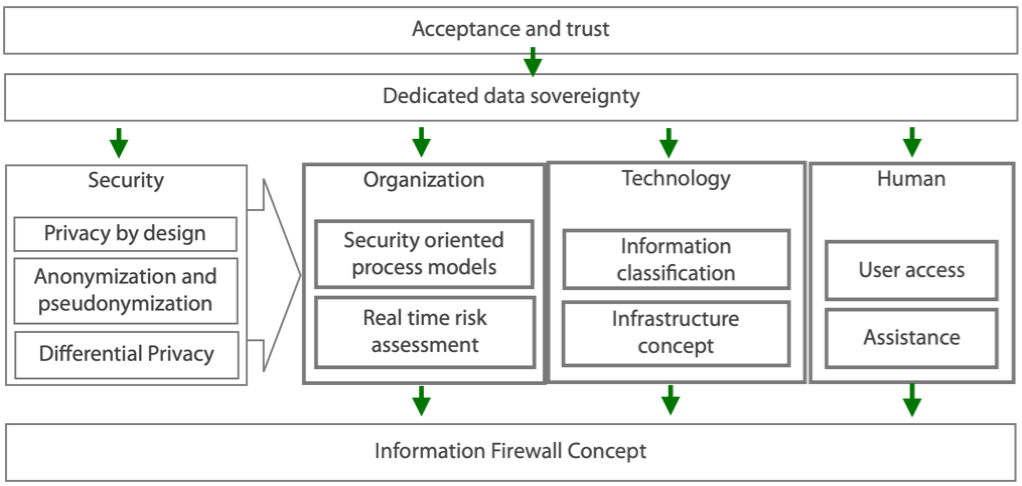

Figure 4: Result for the realization of an information firewall

4. Hardware concept

The deployment of the information firewall concept needs a hardware concept that enables the implementation in existing infrastructures. In reference to the presented building blocks this concept have to fulfill several requirements. Accordingly, potential data sources must be enabled in a proper way to act as CPSs. In particular, from brownfield perspective (see section Influencing factors) the integration of closed legacy systems is a typical use case. The concept envisages a component which enables the required properties to be retrofitted and equips a production object with CPS capabilities. The implementation of the information firewall function follows Industry4.0's ideas of complexity reduction through decentralized elements with capabilities for local information processing. It is therefore obvious to design this component as a typical CPS in accordance with I4.0. Thus, the device acts on the information node level (see section 3.1).

Figure 5: User access with mobile dashboard and I4.0-Box device

The term I4.0 box is used in reference to the Industry 4.0 concept. Also picking up on this aspect, the reference architecture model Industry4.0 (RAMI 4.0) also describes such an approach under the conceptual term management shell [23]. The management shell as an interoperable profile of the technical actor (e.g., the machine) provides information about the data supplied, among other things. Thus, by comparison in combination with the description of the business model, a classification can be made with regard to adaptations of the communicated data. The use of local information processing also contributes to the flat communication hierarchy of IoT. Figure 5 shows a an actual implementation of this hardware concept. CPS enablement, data source with local information processing and communication capability: the device gains access to the production object's installed sensors by connecting them via discrete cabling, using existing fieldbus via the controller/PLC, or alternatively via additional sensors installed at a suitable location. Actuators are connected via fieldbus or via direct cabling to the controller. In analogy to operating systems and their tasks - the abstraction of the operating equipment from the underlying hardware and the management of hardware resources - the software components of the boxes are summarized under the term factory operating system (FaBS). The ConnectionService realizes the communication of the components. Similar to a driver, it abstracts technical details and provides access to FaBS functions. It allows the implementation of a gateway function between the internal communication of the system components and the respective protocol of the external component. This can be done using standards (such as OPC-UA in the case of linking different runtime levels) or using things, specifically defined by the provider.

5. Conclusion

The individual and situational protection needs of data owners are juxtaposed with the need to share information regarding the effectiveness of platform-based business models. By creating dedicated data sovereignty through scalable transparency, this paper addresses this issue and provides an approach to address this problem. It systematically shows the necessary building blocks. The reference model provides a framework for further activities to operationalize the identified building blocks. It offers a basic procedure whose principles serve as a basis for the development of such solutions. An obvious and further approach is to

establish the analysis of information flows as an important part of securing the IT infrastructure and to implement the detection of dynamic structures as well as the detection of irregularities and anomalies in suitable systems. To adequately master these tasks, AI-based methods are possible tools for technical operationalization, e.g., to design self-learning (security) systems. The CPS-based hardware concept offers a usable runtime environment in this respect.

Acknowledgements

The IGF project 20664 BG "IoT-Business Model Evolution - Development of a stage-oriented IoT strategy for SMEs in the injection molding industry for the establishment of interoperable platform ecosystems" is funded by the German Federal Ministry for Economic Affairs and Energy via the AiF as part of the program for the promotion of joint industrial research (IGF) on the basis of a resolution of the German parliament.

References

[1] IDG, 2018, Internet of Things 2018. Key findings, IDG Business Media GmbH

[2] Bender, B., Lass, S., Habib, N. et al., 2020, Platform deployment strategies in mechanical and plant engineering: strategies of German companies in the Industry4.0 context. HMD (2020). DOI: 10.1365/s40702-020-00648-1.

[3] Dremel C., Herterich M., 2018, Digital cloud platforms as enablers for the analytical use of operational product data in mechanical and plant engineering. InCloud Computing 2018 (pp. 73-88). Springer Vieweg, Wiesbaden.

[4] Naderer, B., (ed.), 2017, Latest news from kunststoffland NRW e.V. Focus: Opportunities of digitalization (Issue 2), https://www.kunststoffland-nrw.de/download/publikationen/nrw_report_2017-02- screen_5mb.pdf, last checked on 16.04.2021.

[5] Vassiliadis, M. (ed.), 2017, Digitalization and Industry 4.0. Technology alone is not enough. Hannover: Industrygewerkschaft Bergbau Chemie Energie.

[6] Velosa, A., Schulte, W, R., Lheureux, B., 2020, Hype Cycle for the Internet of Things, Gartner.

[7] Gao, L. ,2019, Exploring the Data Processing Practices of Cloud ERP - A Case Study. Journal of Emerging Technologies in Accounting, 17(1):63–70.

[8] VDI 2014, Industry 4.0-On the way to a reference model. VDI Status Report.

[9] Bauernhansl, T., ten Hompel, M.,; Vogel-Heuser, B., 2014, Industry 4.0 in production, automation and logistics: application, technologies, migration: Springer-Verlag Berlin Heidelberg.

[10] Bauer, W., Schlund, S., Marrenbach, D., Ganschar, O., 2014, Industry 4.0 - Economic potential for Germany. Ed. by BITKOM and Frauenhofer IAO.

[11] Vogel-Heuser, B., Bauernhansl, T., ten Hompel, M., 2017, Handbook Industry 4.0 Bd. 4: Springer.

[12] Hasan, H. and Mohammed, B. (2018). Evaluation of MQTT Protocol for IoT Based Industrial Automation. International Journal of Engineering Science, 8:19364–19369.

[13] Theuer, H., 2019, Market overview of IoT gateways. Factory Software, 24(3):58-62, Gito Berlin.

[14] Krause et al, 2017, IT platforms for the internet of things (IoT), IT platforms for the Internet of Things (IoT): Basis of intelligent products and services. Stuttgart: Fraunhofer Verlag.

[15] Andreev, S., Koucheryavy, Y., Baladin, S., (ed.), 2012, 12th International Conference NEW2AN. Springer.

[16] Sethi, P., Sarangi, S. R., 2017, Internet of things: architectures, protocols, and applications. In: Journal of Electrical and Computer Engineering 2017.

[17] Vogt, A., 2017, IoT Vendor Benchmark 2017 Germany: Experton Group AG.

[18] IDG Research Services 2016, IDG Business Media GmbH.

[19] BMWi, 2016, Announcement for the funding initiative Mittelstand 4.0 - further competence centers for innovative solutions for the digitalization and networking of the economy. BAnz AT 26.08.2016: Federal Ministry for Economic Affairs and Energy.

[20] Lass, S., 2017, Benefit validation of cyber-physical systems in complex factory environments - A hybrid simulation concept for Industry 4.0. GITO Berlin.

[21] Strauß et al., 2018, Enabling of predictive maintenance in the brownfield through low-cost sensors, an iiot-architecture and machine learning. In 2018 IEEE International conference on big data (big data), pages 1474–1483. IEEE.

[22] Gronau, N., 2014, The influence of cyber-physical systems on the design of production systems. In Kersten, W., Koller, H., and Lödding, H., editors, Industry 4.0 - How intelligent networking and cognitive systems are changing the way we work, p. 279-295. GITO Berlin.

[23] Adolphs, P., Epple, U., 2015, Status Report Reference Architecture Industry 4.0 (RAMI4. 0).

[24] Lass, S. and Gronau, N., 2020, A factory operating system for extending existing factories to industry 4.0. Computers in Industry, 115:103128.

[25] Eylers, K., 2020, Proposal for the systematic classification of interactions in Industry 4.0 systems. Technical report, German Association for Information Technology, Telecommunications and New Media.

[26] Herzog et al. 2016. Semantic interoperability in IOT-based automation infrastructures: How reference architectures address semantic interoperability. at-Automatisierungstechnik, 64(9):742–749.

[27] Stahl, J.: Accepting Change, Effecting Change-The Role of Employees in Strategic Renewal. In: Krüger, W. (Ed.) ; Bach, N. (Ed.): Excellence in Change. Springer, 2014, pp. 129-161.

[28] Gebauer, L. et al., 2012, Barriers to the use of cloud computing in B2B and the allocation of these to the different trust relationships. In: ConLife 2012 Academic Conference, Cologne, Germany.

[29] Repschlaeger J, Wind S, Zarnekow R, Turowski K., 2012, A reference guide to cloud computing dimensions: infrastructure as a service classification framework. In; 45th Hawaii International Conference on System Sciences 2012 Jan 4 (pp. 2178-2188). IEEE.

[30] Lass, S. and Fuhr, D., 2013, IT-Sicherheit in der Fabrik. Productivity Management, 18(4):29–32.

[31] Wirsam, J., 2008, Know-how as an object of protection in the context of innovation management. In: Spectrum of Production and Innovation Management: Springer, pp. 233- 242.

[32] Bender B, Gronau N., 2017, Coring on Digital Platforms-Fundamentals and Examples from the Mobile Device Sector. InICIS 2017.

[33] Gronau, N., 2014, Adaptability in Production and Logistics. In: Productivity Management 19 (2014), No. 2, pp. 23-26.

[34] Westkämper, E., Zahn, E., 2009, Transformable Production Companies: The Stuttgart enterprise model. Springer, 2009.

[35] Kaufmann, T. and Servatius, H.-G., 2020, The Internet of Things and Artificial Intelligence as Game Changers. Springer. S. 105.

[36] Wadhwa, P., Puri, A., 2016, Internet of Things: Challenges and impact. International Journal of Engineering Research and General Science, 4(3), 781-786. http://pnrsolution.org/Datacenter/Vol4/Issue3/109.pdf:

[37] GAIA-X, 2020. Driver of digital innovation in Europe - Featuring the next generation of data infrastructure Federal Ministry for Economic Affairs and Energy (BMWi) 2020,

[38] Steinbach, M. et al., 2016, Data Protection and Data Analytics: Challenges and Approaches. In: Data Protection and Data Security, Issue 7, 2016; pp. 440 - 445.

[39] Marnau, N., 2016, Anonymization, pseudonymization and transparency for Big Data. In: Data Protection and Data Security, Issue 7, 2016; pp. 428 - 433.

[40] Ulbricht, C., 2015, Anonymization and pseudonymization; encryption. In: Dorschel, Joachim (Ed.), Handbook of Practice Big Data. Springer Fachmedien Wiesbaden, pp. 185 - 189.

[41] Jain, P. et al., 2016, Big data privacy: a technological perspective and review. In: Journal of Big Data, Heft 1, 2016; S. 1 – 25.

Biography

Sander Lass, Dr. (*1976) studied at the Technical University of Berlin and received his doctorate in applied computer science from the University of Potsdam. He conducts post-doctoral research in the field of factory software and is the technical director of the Center Industry 4.0 Potsdam. The focus of his work is the transfer of Industry4.0 building blocks and concepts into practical applications.

Benedict Bender, Dr. (*1989) studied business informatics at the University of Potsdam, the Humboldt University of Berlin as well as the University of St. Gallen. His research interests include Industry 4.0 and aspects of IT security and privacy. Furthermore, he deals with digital platforms and business ecosystems.