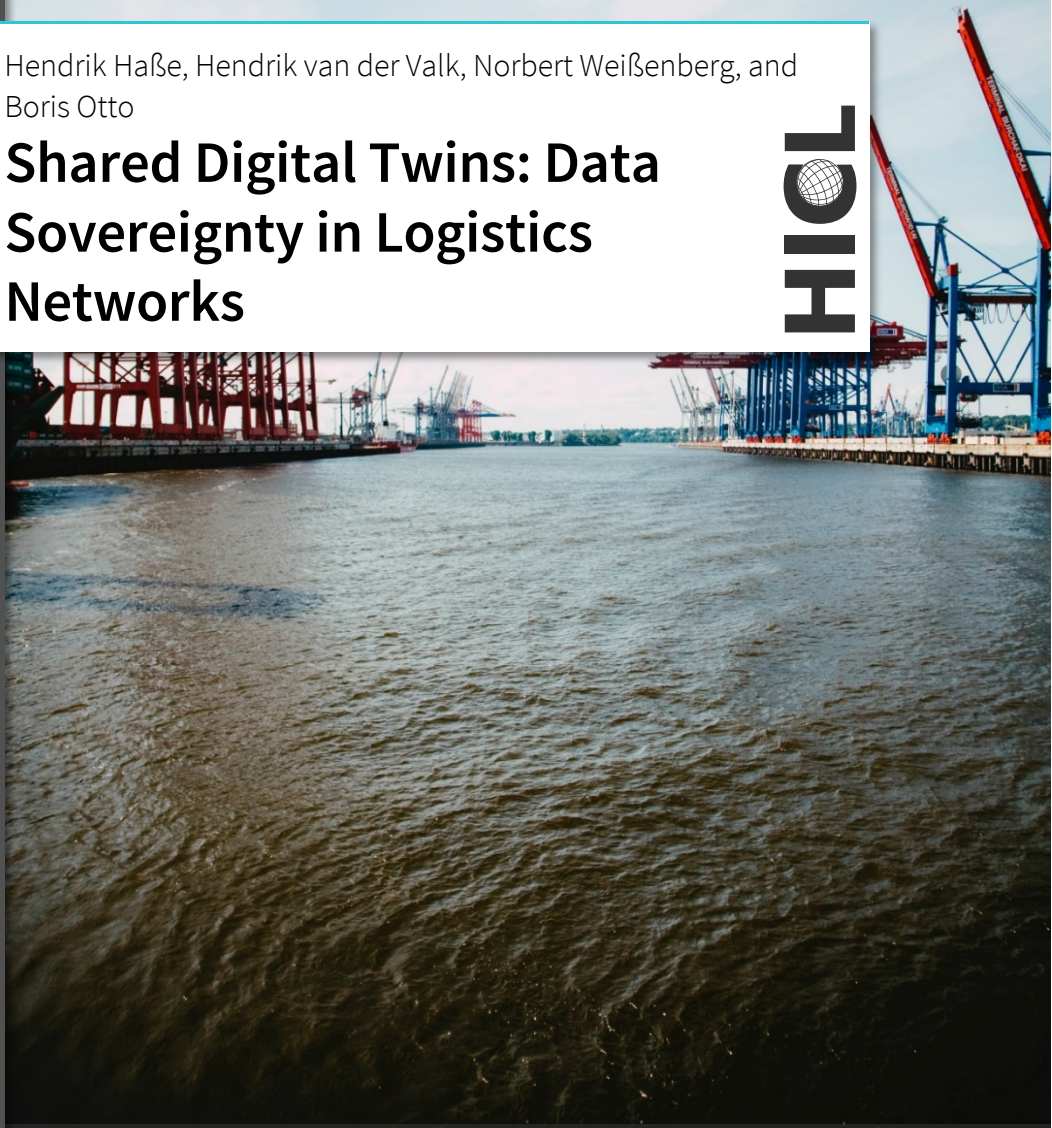
Haße, Hendrik; van der Valk, Hendrik; Weißenberg, Norbert; Otto, Boris

Conference Paper

Shared Digital Twins: Data sovereignty in logistics networks

Hendrik Haße, Hendrik van der Valk, Norbert Weißenberg, and Boris Otto

Shared Digital Twins: Data Sovereignty in Logistics Networks



Published in: Data science and innovation in supply chain management
Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.)
ISBN: 978-3-753123-46-2 , September 2020, epubli

Shared Digital Twins: Data Sovereignty in Logistics Networks

Hendrik Haße [1], Hendrik van der Valk [2], Norbert Weißenberg [1], and Boris Otto [1]

1 –Fraunhofer-Institut für Software- und Systemtechnik ISST

2 – TU Dortmund Lehrstuhl für Industrielles Informationsmanagement

Purpose: Digital Twins attract much attention in science and practice, because of their capability to integrate operational data from a wide variety of sources. Thus, providing a complete overview of an asset throughout its entire life cycle. This article develops and demonstrates a Digital Twin, which enables a sovereign and multilateral sharing of sensitive IoT data based on proven standards.

Methodology: The design described in this paper is developed following the design science research methodology. Current challenges and solution objectives are derived from literature and the solution approach is implemented and demonstrated in a central artefact. The findings are evaluated and iterated back into the design of the central artefact.

Findings: For multilateral data exchange of sensitive operational data, standards are needed that allow for interoperability of several stakeholders and for providing a secure and sovereign data exchange. Therefore, the designs of the Plattform Industrie 4.0 Asset Administration Shell and the International Data Spaces are merged in this contribution. In this way, Digital Twins can be used in cross-company network structures.

Originality: Multilateral data sharing is still associated with considerable security risks for the companies providing the data. Therefore, the consideration of data sovereignty aspects for Digital Twins is very limited. Furthermore, Digital Twins are seldom addressed in the context of cross-company data sharing.

First received: 14. Feb 2020 Revised: 15. Jun 2020 Accepted: 07. Jul 2020

1 Introduction

A Digital Twin integrates and provides data from a wide variety of sources and in a multitude of formats over the entire life cycle of an asset or process. Besides static data, Digital Twins also contain dynamic process data and are therefore able to generate a comprehensive digital representation of a real object or process (Schroeder, et al., 2016, p. 13). Thus the Digital Twin forms an integrated and centralized knowledge base, which makes a valuable contribution to the improvement of business processes (Wang and Wang, 2019, p. 3895). In addition to the extensive generation of information and knowledge, a Digital Twin is characterized by the combination of information with meta-information, which allows a complete semantic description of an asset (Rosen, et al., 2015, p. 568). Therefore, a Digital Twin is a valid tool for data collection and data integration and a viable technology to solve the problem of data disruption between distributed systems. (Wang and Wang, 2019, p. 3894).

Currently, the use of Digital Twins is mainly limited to internal organizational processes, in which the Digital Twin is used to exchange data between different systems within a company (Schroeder, et al., 2016; Tao, et al., 2019, pp. 2409). Digital Twins also offer the opportunity to improve cross-company collaboration processes and represent a feasible instrument for data exchange between different stakeholders (Wagner, et al., 2017, p. 7; Schleich, et al., 2018, p. 7). However, inter-organizational data sharing is largely unconsidered in the literature on Digital Twins, which is reflected in the limited number of relevant examples on this subject. One example is the contribution by Wang and Wang (2019, p. 3894) describing the sharing of a Digital Twin between different stakeholders. In particular,

the consideration of security concepts to restrict access to the contents of the Digital Twin plays a decisive role (Steinmetz, et al., 2018, p. 157; Tao, et al., 2019, p. 2412). An essential building block for implementing collaborative data sharing is the Shared Digital Twin (SDT). An SDT is a specific instance of a Digital Twin that allows for sharing sensitive operational data within a production or supply network or even within a data ecosystem (Cappiello, et al., 2020). However, this lack of concepts for inter-organizational data sharing based on Digital Twins forms the problem-centered approach and thus the research entry point based on the Design Science Research Methodology (DSRM) according to Peffers et al. (2007). In this context, Capiello et al. (2020) encourage an expansion of the research effort in the area of SDTs, leading to the first research objective:

RO1: Development of an SDT based on standards and existing concepts for data sovereignty and interoperability.

Even a bilateral data exchange requires extensive agreements between the partners involved. In the case of multilateral data sharing, the effort involved is more extensive and requires the consideration of uniform standards (Fukami, 2019, p. 1; Wagner, et al., 2019, p. 93). This applies in particular to Digital Twins, requiring a uniform framework for their holistic use (Wagner, et al., 2019, p. 93). Efforts to achieve uniform standardization are ongoing within the Industrial Internet Consortium (IIC) and the German Plattform Industrie 4.0 (Lin, et al., 2017; Seif, Toro and Akhtar, 2019, p. 498). With the Asset Administration Shell (AAS), the Plattform Industrie 4.0 develops a logical construction that consists of several submodels and is explicitly not designed as an encapsulated object based on a monolithic data model (Wagner, et al., 2017, p. 5). In particular, the platform-independent interface of the AAS is a decisive component, as it offers various services

and properties, which in turn are associated with the asset (Wenger, Zoitl and Muller, 2018, p. 75). The development of an SDT based on existing concepts and standards is the central artefact of this paper according to the DSRM by Peffers et al. (2007). Therefore, RO1 serves as the prime objective of this contribution.

RO2: Application of the SDT in a logistics scenario.

This scenario demonstrates how an SDT enables data sharing in a collaborative logistics network. For the implementation of such a scenario, the authors define the roles of data consumer and data provider sharing data via the SDT. The basis for this approach is an IoT-architecture, which processes raw data into key performance indicators (KPIs) in real-time. The IoT-architecture is, in turn, connected to an AAS, providing all data generated. In combination with security gateways, described in DIN SPEC 27070, the data provider controls the consumer's access to data by using AAS mechanisms (Teuscher, et al., 2020, p. 11). This experiment aims to demonstrate the feasibility and to highlight the benefits of an SDT for the individual roles of the collaborative network. The AAS enables data sharing, but for secure multilateral collaboration, it needs a multi-sided platform. Here the authors employ the approaches of the International Data Spaces (IDS) and show how a combination of AAS standards and IDS standards provides a sound basis for SDTs. RO2 bases on the development of an SDT within RO1 and describes the demonstration of the central artifact according to the DSRM by Peffers et al. (2007).

2 Theoretical Background

Based on the DSRM, according to Peffers et al. (2007), this chapter deals with the identification of standards and approaches for inter-organizational interoperability and data sovereignty. Before discussing these approaches in more detail, the concept of the Digital Twin must first be explained. The technologies identified in this chapter serve as the framework for instantiating an SDT and therefore forms the objective of a solution according to the DSRM.

2.1 Digital Twins: Origin and Definitions

The Digital Twin was introduced by Michael Grieves (2014) as a concept for the product life cycle. In 2003, Grieves (2014) proposed a concept of a physical product with a corresponding virtual product and a linkage through data and information connections between both products. Later Grieves and Vickers (2017) extended the concept, stating that the virtual product describes the physical product in every detail and contains information from a micro to a macro level, integrating all current data into the virtual product.

Coming from first usages of the twin concept at NASA during the Apollo project, Glaessgen and Stargel (2012, p. 7) define the Digital Twin "as an integrated multiphysics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin" (Rosen, et al., 2015, p. 568). This definition of a Digital Twin is the most common one and appears in numerous publications (Karakra, et al., 2019, p. 2).

Furthermore, Glaessgen and Stargel (2012) stress the importance of integrating data sources like historical data, sensor data or complementary data (Glaessgen and Stargel, 2012, p. 7). Finally, the definition given by Tao, et al. (2018) is equally important, according to which "a Digital Twin consists of three parts: physical product, virtual product, and connected data that tie the physical and virtual product" (Tao, et al., 2018, p. 3566). All definitions stress the data connection between a physical and a digital part, as well as the integration of additional data from various sources. In summary, the authors consider a virtual model of a physical system containing a bidirectional data link between the virtual and the physical part as the archetypal core of a Digital Twin. Therefore, the further use of the term Digital Twin in this publication refers to the content described in this section.

The concept of a Digital Twin is characterized by its permanent connection between the real asset and its virtual representation. This, in turn, requires an extensive IoT environment to ensure this connection (Koulamas and Kalogeras, 2018, p. 96). Particularly well-known IoT reference architectures come from the international organization Industrial Internet Consortium (IIC) and the German strategic initiative Plattform Industrie 4.0 (Lin, et al., 2017, p. 1).

International Internet Consortium (IIC)

The IIC developed the Industrial Internet Reference Architecture (IIRA), which is a standards-based open architecture for Industrial Internet of Things (IIOT-)systems (Lin, et al., 2017, p. 4). IIRA is characterized by its focus on different business and technical perspectives and emphasizes broad applicability and interoperability (Lin, et al., 2017, pp. 1-3). IIC considers the concept of Digital Twins as a central component of the IIOT and identifies

eight general reference characteristics for Digital Twin data models, described by assets, components, environment, models and descriptions, control parameters, behavioral data, environmental data and finally connectivity parameters. Depending on the particular use case, Bächle and Stefan (2019, p. 10) emphasize that Digital Twin data models must also be interoperable across company boundaries.

Plattform Industrie 4.0

The endeavors of the IIC and the Plattform Industrie 4.0 are closely linked together (Lin, et al., 2017, p. 2)**.** The Plattform Industrie 4.0 proposes the Reference Architectural Model Industrie 4.0 (RAMI 4.0) as a guideline for the adaption of Industry 4.0 and its related technologies (Chilwant and Kulkarni, 2019, p. 15). In contrast to IIRA, RAMI 4.0 focuses on digitization and interoperability in the area of manufacturing. RAMI 4.0 comprises three dimensions, consisting of *layers*, *hierarchy levels* and *life cycle value stream*. Whereas *layers* and *hierarchy level* deal with properties and system structures respectively with the functional hierarchies of a factory, the dimension *life cycle value stream* focuses on life cycle aspects of an asset (Lin, et al., 2017, pp. 3-5).

The AAS is a central component of the Plattform Industrie 4.0 and describes the most mature data model of a Digital Twin (Bächle and Stefan, 2019, p. 3). The AAS describes different assets in a standardized format over their entire life cycle. This specification is an important basis for interoperability. It enables the digital integration of assets, creates the technical prerequisites of a decentralized industry 4.0 and is the concept of a Digital Twin as an open accessible and interoperable interface. The AAS is intended to become the central standardized integration plug of any asset to digital ecosystems, using a common language.

The information model of the AAS supports a modular asset description with formally describable semantics and is defined by using UML class diagrams (Bader, et al., 2019). These classes allow for the creation of a concrete AAS data model. The AAS covers a wide variety of data formats like XML, JSON, RDF, AutomationML or OPC-UA in order to share information between different systems (Bader, et al., 2019).

Figure 1 illustrates the principles of this coming AAS data standard and shows how to transform proprietary data models to AAS-conformant models. On the left side, it shows a straightforward proprietary data model, named *MODEL*, representing a proprietary Digital Twin of a machine and below it an instantiation of that model to describe a machine *m1*. The authors only display one attribute to focus on the mechanisms of how to translate this model to an AAS submodel. The simplified generic AAS model is shown in the middle column of Figure 1, whereas the right side shows its instantiation to describe the sample model. Each submodel, which is composed of *SubmodelElements,* has an Internationalized Resource Identifier (IRI), an *idShort*, *descriptions in different languages* and a *kind,* distinguishing type from instances.

For all attributes of the given model an AAS Property is added to the AAS submodel. A Property is a name-value pair with additional metadata. Here, the semantic annotation via attribute *semanticId* is very important for automatic interpretation.

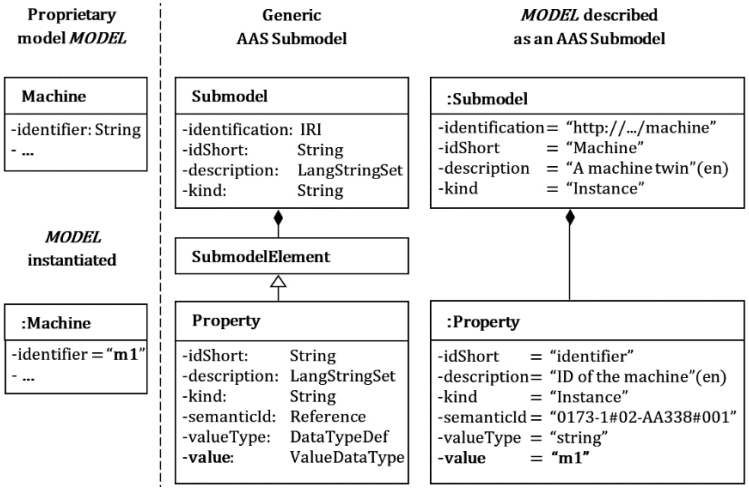


Figure 1: Transformation of proprietary models to AAS models

In this example, an International Registration Data Identifier (IRDI) points to an attribute defined by the eCl@ss standard. Alternatives for semantic annotation are an IRI referencing a standard property of a well-known ontology, or an IEC 61360-1 conformant *ConceptDescription* stored within the AAS (IEC 61360-1, 2017). The last attributes are *valueType* and *value*. The value appears only if *kind=Instance*.

An asset can be composed of other assets, leading to the construction of a composite AAS, listing all its parts. These contained assets are either co-managed by the composite AAS or are self-managed, by having their own AAS. In this way, complex AAS structures evolve, reflecting the physical asset structure.

An essential aspect of the AAS is to enable data exchange between different stakeholders. However, this requires taking into account various security

aspects that protect the data of the AAS from unauthorized access (Bächle and Stefan, 2019, p. 3). Therefore, the AAS uses attribute-based access control (ABAC), a security model protecting e.g., the REST-API of an AAS. ABAC is an extension of role-based access control, considering not only the role of the subject but also attributes of the subject, the objects and the context conditions holding when checking access right (Wang, Wijesekera and Jajodia, 2004, p. 45). For each subject, being role or user, it can be specified, which object, submodels or even properties, the user is allowed or denied to read or to modify. This can even be specified using expressions over attributes of the subject, the object and the context.

2.2 Concepts for Sovereign Data Sharing

The ongoing digitization process and the associated increase in data volume present companies with the challenge of reconsidering their business models and sharing data across companies (Zrenner, et al., 2019, p. 477). According to a PWC study, the majority of the companies surveyed recognize a steadily increasing need for cross-company data exchange, but at the same time express concerns about non-existent data sovereignty (PwC, 2018, p. 40). Data sovereignty is the ability of a natural and legal person to exercise exclusive self-determination over the economic asset data (Otto, et al., 2019, p. 116). With the objective of data sovereignty in business ecosystems, the IDS initiative provides key concepts and technologies that enable companies to exchange and to share data with business partners while retaining the right of self-determination over their data (Otto, et al., 2019, p. 116).

Data sharing describes a vertical and horizontal collaboration between companies to achieve common goals and therefore differs from the term data exchange, where the exchange of data takes place in the sense of vertical cooperation between companies. One example of collaborative data sharing is predictive maintenance, in which both the company providing the data and the company consuming it benefit from each other through improved services and an improved data basis, leading to a mode of collaboration towards coopetition (Otto, et al., 2019, p. 15).

International Data Spaces (IDS)

The IDS represents a multi-sided platform for secure and trusted data exchange (Otto and Jarke, 2019, p. 561). This initiative is governed by an institutionalized alliance of different stakeholder organizations bundled in the International Data Spaces Association (IDSA). To ensure the self-determination with regard to data, the IDS initiative proposes a Reference Architecture Model (IDS-RAM). It describes a software architecture for enforcing data sovereignty in business ecosystems and value-added networks. IDS-

RAM includes the IDS Information Model and the architecture of IDS Connectors.

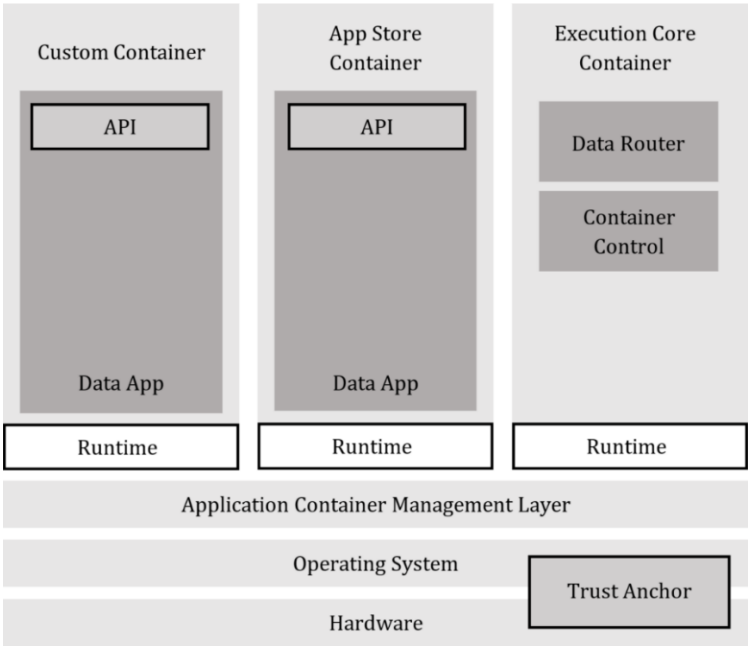


Figure 2: Building Blocks of a Security Gateway according to DIN SPEC 27070 (Teuscher, et al., 2020, p.11)

The IDS information model describes all concepts and artifacts needed for the implementation of IDS-based ecosystems and networks, including conditions for the usage of data and for describing the IDS Connector as a software component. The IDS Connector, representing standardized interfaces for receiving, sending and transforming data sets (Otto and Jarke, 2019;

Zrenner, et al., 2019, p. 481). It has three key functions comprising of exchanging data between a data provider and a data consumer, enabling secure and trusted execution of software and finally executing trusted software packages. It therefore acts as a secure, trusted gateway and a secure, trusted execution environment for apps (Otto, et al., 2019; Otto and Jarke, 2019; Teuscher, et al., 2020, p. 11). The DIN-compliant IDS Connector architecture appears in Figure 2.

3 Research Methodology

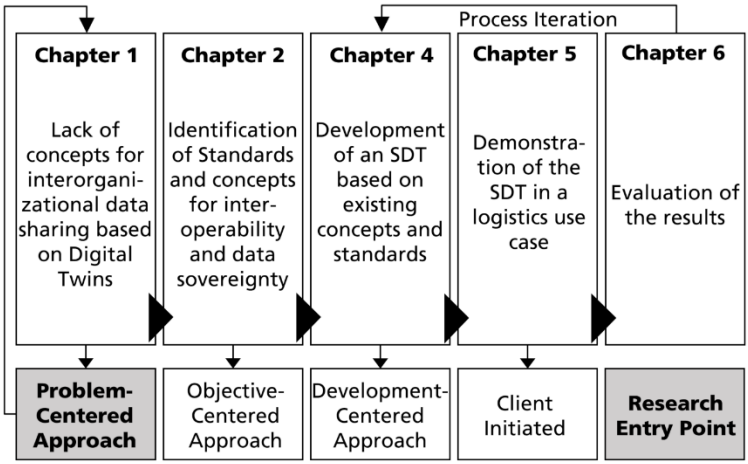


Figure 3: The DSRM for the development of an SDT by Peffers et al. (2007)

For this contribution, the authors follow the DSRM by Peffers et al. (2007). This Methodology synthesizes common steps of design science research and is divided into six different steps (Rhyn and Blohm, 2017, p. 2660). These steps consist of problem identification and motivation, the definition of the objectives for a solution, the design and development of a central artefact, the demonstration of the central artefact, the evaluation and finally the communication of the results (Peffers, et al., 2007, pp. 12-14). This paper focuses on the development and instantiation of an SDT, representing the central artifact in this contribution. The approach corresponds to the order of the chapters, where Chapter 1 addresses the lack of concepts for using Digital Twins in collaborative networks. Chapter 2, therefore, examines various concepts and approaches for the implementation of an SDT

which are finally designed and instantiated in Chapter 4. A demonstration in the context of a logistics use case follows in Chapter 5. The final evaluation of the results leads to a process iteration step, including the reconsideration of policy enforcement concepts. Step 6 of the DSRM consists of communicating the results, which is fulfilled by presenting the findings in this publication.

4 Development of a Shared Digital Twin

The focus of this research project is the development of an SDT, which follows the approaches and concepts mentioned in Chapter 2. The aim is to connect the information model of an AAS with that of an IDS Connector. The SDT represents the central artefact according to the DSRM by Peffers et al. (2007).

The foundation for the development is a proprietary Digital Twin in combination with an IoT-architecture, which processes sensor data into KPIs in real-time. In addition to the generated KPIs, the raw data and the corresponding metadata are also provided in this proprietary Digital Twin. Building on this, it is now a matter of making these data sets available in a B2B data ecosystem while preserving data sovereignty. The authors argue that proprietary approaches cannot offer a suitable solution, especially regarding the existing interoperability requirements. The bilateral exchange of data already requires high implementation effort, as well as the agreement on common interfaces (Elgarah, et al., 2005, p.19). If, as described here, a collaborative approach to sharing data is pursued, it is necessary to use existing approaches that allow for easy implementation of the framework. For this purpose, the authors adopt the AAS concept and combine it with the architecture for security gateways described in DIN SPEC 27070 in order to ensure the necessary interoperability on the one hand and the required data sovereignty of the data provider on the other (Teuscher, et al., 2020, p. 11). The implementation of such a system requires three steps:

1. Mapping the Proprietary Data Model to the AAS Data Model

Figure 1 illustrates the mapping of data models of a proprietary Digital Twin

to an AAS-conformant data model. Here, additional metadata and semantic annotations of all concepts and properties need to be added, which a proprietary Digital Twin often does not yet provide. A further prerequisite for the combination of AAS and IDS is the integration of their data models. IDS messages contain AAS-compliant data with references to IDS resources.

2. Implementing an AAS-conformant REST-API using IDS
The second step is the implementation of the AAS-REST API. However, since IDS controls the AAS-REST API and all AAS resources, for example the files described in the *Documentation* submodel, there are some IDS-specific additions necessary. These include the verification of REST headers.

3. Implementing an AAS ABAC Model synchronized with IDS
The AAS ABAC security model protects the AAS-REST API and is synchronized with the IDS contracts. These contracts are used to protect the IDS resources by defining usage control rules. IDS resources describe the data exchanged via the IDS, namely the AAS submodels and the documents contained in the AAS *Documentation* submodel. The submodels of the AAS are thus protected by both mechanisms.

Resulting Architecture

Figure 4 shows the resulting architecture of this approach, which turns a proprietary Digital Twin into a standardized SDT that supports data sovereignty by combining AAS and IDS standards based on DIN SPEC 27070. It uses a proprietary Digital Twin that obtains raw data via MQTT to implement an AAS-compliant REST-API as an IDS Data App, which in turn is accessed over the IDS-managed HTTPS endpoint. This design complies with DIN SPEC 27070. The authors argue that this pattern suits for developing SDTs for data ecosystems. It allows to convert proprietary Digital Twin to a

sovereign Digital Twin according to the standard (AAS) by providing an IDS-AAS wrapper. By skipping the step of data model conversion, even newly developed Digital Twins can apply this framework. Any number of ecosystem participants can access the data in a standardized way, while the data owner retains control of the data. The data owner determines who is allowed to access which data and for what purposes.

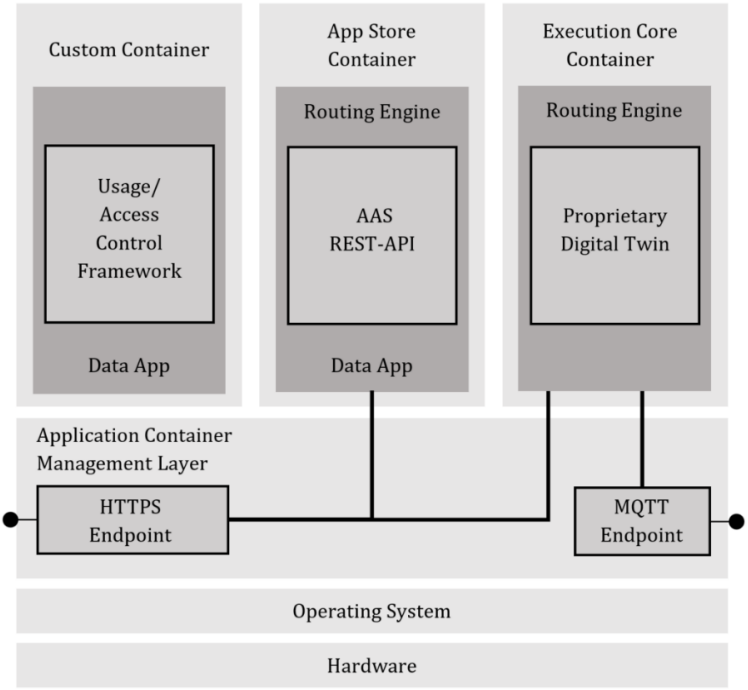


Figure 4: Architecture of an IDS-AAS for a proprietary Digital Twin

5 Demonstration of the Shared Digital Twin

In order to validate the functionality of the developed architecture, the authors conduct an experiment within the scope of this research endeavor, which demonstrates, in particular, the implementation of combined AAS and IDS security concepts. In the context of the DSRM by Peffers et al. (2007), this section aims to prove the developed SDT in a logistics use case. In general, the demonstration of the central artefact developed in the previous step aims to show that the proposed solution solves one or more instances of the problem (Peffers, et al., 2007, p. 13). An essential aspect is to enable multilateral data sharing on the basis of a Digital Twin, which is possible with the artefact developed.

In this experiment, the authors equip remote control (RC) forklifts with a sensor system that records their acceleration values. An IoT architecture captures the raw data of the RC forklifts and processes this data to KPIs. These KPIs include, primarily, workload, the detection of shocks and the calculation of maintenance intervals based on the current workload. The basis for the real-time calculation of KPIs is RIOTANA® (Real-Time Internet of Things Analytics), an IoT architecture that captures all data in a proprietary Digital Twin (Haße, et al., 2019, p. 20). Here, the main purpose of the proprietary Digital Twin is to provide a real-time virtual representation of the forklift trucks. RIOTANA® uses an ontology to describe all relationships between forklifts, the sensors attached to them and the KPIs determined from raw data, which eased the semantic annotation of AAS data.

The aim of this attempt is the sovereign sharing of the KPIs generated by the IoT architecture. This exchange takes place between a server and a cli-

ent. With this experiment, the most diverse roles of a collaborative ecosystem can be assumed. The concept of collaborative data sharing describes an innovative approach that creates added value for all participants within the value chain (Tavanapour, et al., 2019, p. 7). The logistics use case described here takes into account a two-tier value chain that is expandable to any extent due to the use of neutral standards. The test simulates the interaction between a manufacturer of industrial trucks and an operator of industrial trucks. The operator purchases the industrial trucks from the forklift manufacturer. All forklift trucks continuously generate data via an active sensor system, which RIOTANA® processes into KPIs.

Forklift Fleet Operator

The utilization of the forklift fleet generates data, which in turn is available in the AAS of the fleet, where each forklift is a co-managed asset. Via a user interface, the operator of the fleet has a complete overview of all data generated. In addition, the forklift operator has full control over all data and can, therefore, restrict access to it by defining ABAC rules (Figure 6).

Forklift Manufacturer

The forklift manufacturer can access the AAS of the operator's forklift fleet using the AAS-REST-API. The manufacturer can access some submodels of the AAS, which contain the KPIs, the master data and a complete meta-data description. The manufacturer can only access the data authorized by the operator using ABAC. With authorized access to the operator's data, the

manufacturer gains insight into the use of its assets and is thus able to analyze this data (Figure 5).

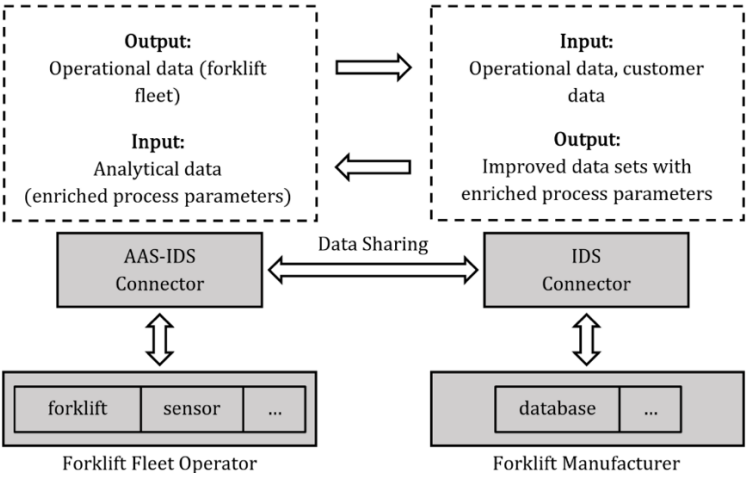
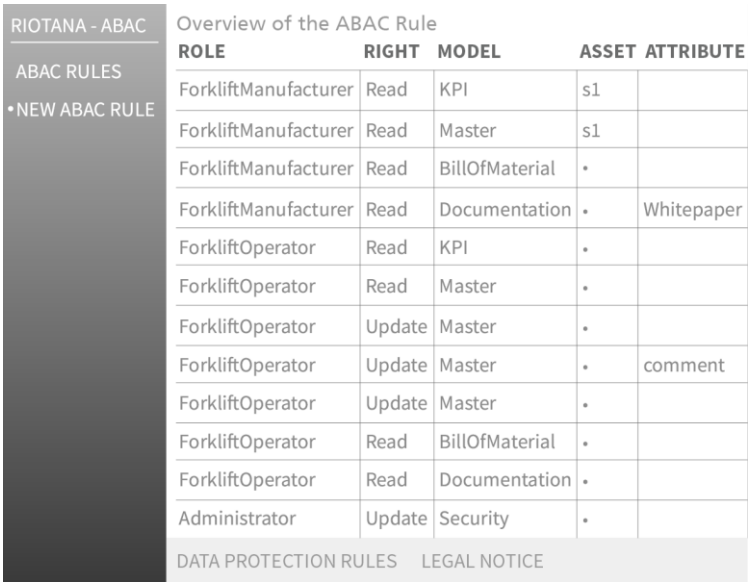


Figure 5: Application Scenario

Benefits

The operator can benefit from the manufacturer's additional services without disclosing its operational confidentiality. The operator decides which data to release and which services the operator wants to receive from the forklift manufacturer. In principle, the operator benefits from the controlled release of operating data, which in turn results in an optimization of

the fleet management, improved reliability of the forklift fleet and the possibility of optimizing the environmental parameters of the warehouse.



ROLE	RIGHT	MODEL	ASSET	ATTRIBUTE
ForkliftManufacturer	Read	KPI	s1	
ForkliftManufacturer	Read	Master	s1	
ForkliftManufacturer	Read	BillOfMaterial	•	
ForkliftManufacturer	Read	Documentation	•	Whitepaper
ForkliftOperator	Read	KPI	•	
ForkliftOperator	Read	Master	•	
ForkliftOperator	Update	Master	•	
ForkliftOperator	Update	Master	•	comment
ForkliftOperator	Update	Master	•	
ForkliftOperator	Read	BillOfMaterial	•	
ForkliftOperator	Read	Documentation	•	
Administrator	Update	Security	•	

Figure 6: Defining ABAC Rules via a user interface

In general, the forklift manufacturer benefits greatly from the operating data of the forklifts, to which the manufacturer would otherwise never have had access. The forklift manufacturer gains a deep insight into the use of the industrial trucks and can thus improve the requirement profiles of its products. Based on the actual utilization, the forklift manufacturer can offer improved maintenance intervals. By evaluating this data, the forklift manufacturer can establish proactive spare parts management and, at the

same time, optimize its warehouse logistics. In principle, this form of collaboration increases customer loyalty, which results in improved service performance.

6 Discussion and Conclusion

Companies increasingly recognize the relevance of cross-company data sharing but hesitate to implement it due to security concerns. Together, companies can extract more value from their data. That is especially the case for companies whose core competence is not in data management, but whose processes generate a large amount of data. In the future, these companies will be increasingly dependent on drawing more information and knowledge from their process data and will thus be dependent on strategic partners. This necessity may be expressed by the fact that companies collaborate more closely with each other along a value chain, associated with added value for all actors involved. However, this requires technological building blocks that enable interoperability across companies while at the same time preserving the sovereignty of the companies providing the data. With an SDT based on standards, the authors develop a concept of a Digital Twin that is particularly suitable for such collaborative networks.

Two aspects in particular play an essential role in this regard. On the one hand, in the context of collaborative data sharing, there are high requirements for multilateral interoperability. Becoming a standardized data ecosystem plug, the AAS is an important entry point for this. On the other hand, there are special requirements for security and usage control for data sharing. The information model of the IDS plays a decisive role here. By combining the information models of the IDS and the AAS, it is expected that it will not only be possible to regulate access to the data, but also to provide the data with usage policies. In this way, it will be possible to ensure that the company providing the data remains sovereignty over its data and at the

same time profit from its data. In summary, this contribution addresses two main research objectives.

RO1 addresses the development of an SDT based on existing standards and approaches for data sovereignty and interoperability. In addition to the actual development of an SDT, the main focus is on the description of existing approaches for the realization of these requirements. Here the authors identify the data model and REST-API of the AAS of the Plattform Industrie 4.0 to ensure interoperability across companies, and additionally the concepts of IDS to ensure data sovereignty. The authors have succeeded in combining both information models and both security concepts to instantiate an SDT.

RO2 addresses the application of the SDT developed in this research project in a logistics scenario. Here the authors describe the possible collaboration between a forklift manufacturer and a forklift operator within a simulated IoT environment. By using the results of RO1, an existing proprietary logistics Digital Twin was converted to a standard-conformant sharable SDT. The emphasis of this project lies in particular in the description of security concepts, which are implemented in this pilot with attribute-based access control, an AAS concept which was integrated with the corresponding IDS concepts (namely IDS contracts).

Key Findings

The SDT is an essential component for implementing collaborative data sharing. It is based on the fundamental concepts of a general Digital Twin, which are essentially characterized by the integration of various data formats from distributed data storage and by the description of data with meta information (Cappiello, et al., 2020, p. 120). Hence, an SDT describes

the extension of the archetypal characteristics of a Digital Twin by the functions of interoperable and sovereign use in collaborative networks. This extension essentially includes the consideration of a standardized data model, which in particular contains the uniform description of interfaces. The respective data model must enable manufacturer-neutral and cross-company interoperability.

Scientific Implications

Several scientific implications result, which, in addition to the creation of an SDT based on the combination of existing approaches, also manifest themselves through the integration of a proprietary Digital Twin into a standardized data model of a Digital Twin. In this way, existing Digital Twin approaches can be subsequently adapted to the AAS data model. The authors moreover propose a combination of AAS data models with IDS data models. The application possibilities of SDTs are very extensive and cover a wide range of different use cases.

Managerial Implications

Managerial implications result mainly from the ability of collaborative data sharing and the associated possibility of participating in a data ecosystem. By using an SDT as described, for example by combining AAS and IDS, the data owner retains sovereignty over provided data. The concepts and approaches described in this paper are particularly of a technical nature. Nevertheless, the authors argue that the strong emphasis on data sovereignty aspects is crucial to create incentives for collaborative data sharing. As already described in the introduction of Chapter 6, it is having security concerns that make companies hesitant to share data with other companies.

Limitations

Limitations of the work described arise, primarily through the application of access control instead of usage control. While access control describes the terms that apply to data before it is released, usage control describes how the data is handled after its release (Bussard, Neven and Preiss, 2010, p. 1).

Future Research

Since usage control is essential for the implementation of data sovereignty, the future implementation of usage control is an iteration step according to the DSRM by Peffers et al. (2007) (Zrenner, et al., 2019, p. 486). In addition, the concept of the AAS is currently undergoing continuous development, resulting in a correspondingly high implementation effort. Furthermore, research in the field of digital twins continuously expands. There are already contributions dealing with the basic dimensions and characteristics of Digital Twins (van der Valk, et al., 2020). It is therefore of fundamental importance to investigate the extent to which an SDT differs from the basic characteristics of Digital Twins. Further implications for future research include the systematic collection of requirements for SDTs and the derivation of design principles for them.

Acknowledgement

This research was supported by the Excellence Center for Logistics and IT funded by the Fraunhofer-Gesellschaft and the Ministry of Culture and Science of the German State of North Rhine-Westphalia

References

Bächle, K. and Stefan, G., 2019. Digital Twins in Industrial Applications: Requirements to a Comprehensive Data Model. [online] Available at: <https://www.iiconsortium.org/news/joi-articles/2019-November-JoI-Digital-Twins-in-Industrial-Applications.pdf> [Accessed 23 March 2020].

Bader, S., Barnstedt, E., Bedenbender, H., Billmann, M., Boss, B. and others, 2019. Details of the Asset Administration Shell: Part 1 - The exchange of information between partners in the value chain of Industrie 4.0 (Version 2.0). [online] Available at: <https://www.zvei.org/presse-medien/publikationen/details-of-the-asset-administration-shell/> [Accessed 25 March 2020].

Bussard, L., Neven, G. and Preiss, F.-S., 2010. Downstream Usage Control. IEEE International Symposium on Policies for Distributed Systems and Networks. http://dx.doi.org/10.1109/POLICY.2010.17.

Capiello, C., Gal, A., Jarke, M., Rehof, J., 2020. Data Ecosystems: Sovereign Data Exchange among Organizations (Dagstuhl Seminar 19391). http://dx.doi.org/10.4230/DAGREP.9.9.66.

Chilwant, N. and Kulkarni, M. S., 2019. Open Asset Administration Shell for Industrial Systems. Manufacturing Letters, [e-journal] 20, pp. 15-21. http://dx.doi.org/10.1016/j.mfglet.2019.02.002.

Elgarah, W., Falaleeva, N., Saunders, C. C., Ilie, V., Shim, J. T. and Courtney, J. F., 2005. Data exchange in interorganizational relationships. ACM SIGMIS Database, [e-journal] 36(1), pp. 8-29. http://dx.doi.org/ 10.1145/1047070.1047073.

Fukami, Y., 2019. Standardization for Innovation with Data Exchange. International Conference on Data Mining Workshops (ICDMW), pp. 1-4. http://dx.doi.org/10.1109/ICDMW.2019.00008.

Glaessgen, E. and Stargel, D., 2012. The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles. In: Structures, Structural Dynamics, and Materials and Co-located Conferences. 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference. Reston, USA: American Institute of Aeronautics and Astronautics, pp. 1-14.

Grieves, M., 2014. Digital Twin: Manufacturing Excellence Through Virtual Factory Replication. [online] Available at: <https://www.researchgate.net/publication/275211047_Digital_Twin_Manufacturing_Excellence_through_Virtual_Factory_Replication> [Accessed 26 March 2020].

Grieves, M. and Vickers, J., 2017. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behaviour in Complex Systems. In: F.-J. Kahlen, S. Flumerfelt, and A. Alves, eds. 2017. Transdisciplinary Perspectives on Complex Systems. New Findings and Approaches. Cham, Switzerland: Springer, pp. 85-113.

Haße, H., Li, B., Weißenberg, N., Cirullies, J. and Otto, B., 2019. Digital Twin for real-time data processing in logistics. http://dx.doi.org/10.15480/882.2462.

International Electrotechnical Commission, 2017. IEC 61360-1:2017 Standard data element types with associated classification scheme - Part 1: Definitions - Principles and methods. [online] Available at: < https://webstore.iec.ch/publication/28560#additionalinfo> [Accessed 26 April 2020].

Karakra, A., Fontanili, F., Lamine, E. and Lamothe, J., 2019. HospiT'Win: A Predictive Simulation-Based Digital Twin for Patients Pathways in Hospital. In: 2019 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI). Chicago, IL, USA: IEEE, pp. 1-4.

Koulamas, C. and Kalogeras, A., 2018. Cyber-Physical Systems and Digital Twins in the Industrial Internet of Things. *Computer*, [e-journal] 51(11), pp. 95-98. http://dx.doi.org/10.1109/MC.2018.2876181.

Lin, S.-W.; Murphy, B., Clauer, E., Loewen, U., Neubert, R., Bachmann, G., Pai, M.; Hankel, M., 2017. Architecture Alignment and Interoperability: An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper. [online] Available at: <IIC:WHT:IN 3:V1.0:PB:20171205> [Accessed 10 March 2020].

Otto, B., ten Hompel, M., Wrobel, S., 2019. Industrial Data Space. Referenzarchitektur für die Digitalisierung der Wirtschaft. In: R. Neugebauer, ed. 2019. Digitalisierung. Schlüsseltechnologien für Wirtschaft & Gesellschaft. München: Springer Vieweg. pp. 113-133.

Otto, B. and Jarke, M., 2019. Designing a multi-sided data platform: findings from the International Data Spaces case. *Electronic Markets*, [e-journal] 29(4), pp. 561-580. http://dx.doi.org/10.1007/s12525-019-00362-x.

Otto, B.; Steinbuß, S.; Teuscher, A., Lohmann, S., 2019. Reference Architecture Model of the International Data Spaces. [online] [Accessed 27 March 2020].

Peffers, K; Tuunanen, T., Rothenberger, M. A., Chatterjee, S., 2007. A Design Science Research Methodology for Information Systems Research, [e-journal] 24 (3), pp. 45 - 77. https://doi.org/10.2753/MIS0742-1222240302.

PwC, 2018. Data exchange as a first step towards data economy. [online] Available at: <https://www.pwc.de/en/digitale-transformation/data-exchange-as-a-first-step-towards-data-economy.pdf> [Accessed 26 March 2020].

Rhyn, M and Blohm, I., 2017. Combining Collective and Artificial Intelligence: Towards a Design Theory for Decision Support in Crowdsourcing. In: Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017, pp. 2656-2666. ISBN 978-0-9915567-0-0 Research-in-Progress Papers.

Rosen, R., Wichert, G. von, Lo, G., Bettenhausen, K. D., 2015. About The Importance of Autonomy and Digital Twins for the Future of Manufacturing. IFAC-PapersOnLine, [e-journal] 48(3), pp. 567-572. http://dx.doi.org/10.1016/j.ifacol.2015.06.141.

Schleich, B., Wärmefjord, K., Söderberg, R., Wartzack, S., 2018. Geometrical Variations Management 4.0: towards next Generation Geometry Assurance. Procedia CIRP, [e-journal] 75, pp. 3-10. http://dx.doi.org/10.1016/j.procir.2018.04.078.

Schroeder, G. N., Steinmetz, C., Pereira, C. E. and Espindola, D. B., 2016. Digital Twin Data Modeling with AutomationML and a Communication Methodology for Data Exchange. *IFAC-PapersOnLine*, [e-journal] 49(30), pp. 12–17. http://dx.doi.org/10.1016/j.ifacol.2016.11.115.

Seif, A., Toro, C., Akhtar, H., 2019. Implementing Industry 4.0 Asset Administrative Shells in Mini Factories. Procedia Computer Science, [e-journal] 159, pp. 495-504. http://dx.doi.org/10.1016/j.procs.2019.09.204.

Steinmetz, C., Rettberg, A., Ribeiro, F. G. C., Schroeder, G., Pereira, C. E., 2018. Internet of Things Ontology for Digital Twin in Cyber Physical Systems. Symposium on Computing Systems Engineering (SBESC), pp. 154-159. http://dx.doi.org/10.1109/SBESC.2018.00030.

Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H. and Sui, F., 2018. Digital Twin-Driven Product Design, Manufacturing and Service with Big Data. The International Journal of Advanced Manufacturing Technology, 94(9-12), pp. 3563-3579. http://dx.doi.org/10.1007/s00170-017-0233-1.

Tao, F., Zhang, H., Liu, A. and Nee, A. Y. C., 2019. Digital Twin in Industry: State-of-the-Art. *IEEE Transactionson Industrial Informatics*, [e-journal] 15(4), pp. 2405-2415. http://dx.doi.org/10.1109/TII.2018.2873186.

Tavanapour, N., Bittner, E. A. C. and Brügger, M., 2019. Theory-Driven-Design for Open Digital Human Collaboration Systems. In: *Americas Conference on Information Systems* (AMCIS 2019). Cancún, Mexico.

Teuscher, A., Brost, G., Brettner, U., Böhmer, M., Fraune, B., Haas, C. and others, 2020. DIN SPEC 27070:2020-03. Anforderungen und Referenzarchitektur eines Security Gateways zum Austausch von Industriedaten und Diensten. [online] Available at: <https://www.beuth.de/de/technische-regel/din-spec-27070/319111044> [Accessed 12 February 2020].

Van der Valk, H.; Haße, H.; Möller, F.; Arbter, M.; Henning, J.-L. and Otto, B., 2020. A Taxonomy of Digital Twins. *26th Americas Conference on Information Systems (AMCIS 2020)*. Salt Lake City, USA.

Wagner, C., Grothoff, J., Epple, U., Drath, R., Malakuti, S., Gruner, S., Hoffmeister, M. and Zimermann, P., 2017. The role of the Industry 4.0 asset administration shell and the digital twin during the life cycle of a plant: Septmeber 12-15, 2017, Limassol, Cyprus, pp. 1-9. http://dx.doi.org/10.1109/ETFA.2017.8247583.

Wagner, R., Schleich, B., Haefner, B., Kuhnle, A., Wartzack, S., Lanza, G., 2019. Challenges and Potentials of Digital Twins and Industry 4.0 in Product Design and Production for High Performance Products. Procedia CIRP, [e-journal] 84, pp. 88-93. http://dx.doi.org/10.1016/j.procir.2019.04.219.

Wang, L., Wijesekera, D. and Jajodia, S., 2004. A logic-based framework for attribute based access control. FMSE '04: Proceedings of the 2004 ACM workshop on Formal methods in security engineering, [e-journal], pp. 45-55. http://dx.doi.org/10.1145/1029133.1029140.

Wang, X. V. and Wang, L., 2019. Digital twin based WEEE recycling, recovery and remanufacturing in the background of Industry 4.0. *International Journal of Production Research*, [e.journal] 57(12), pp. 3892-3902. http://dx.doi.org/10.1080/00207543.2018.1497819.

Wenger, M. Zoitl, A., Müller, T., 2018. Connecting PLCs With Their Asset Administration Shell For Automatic Device Configuration. In: 2018 IEEE 16th International Conference on Industrial Informatics (INDIN), pp. 74-79. http://dx.doi.org/10.1109/INDIN.2018.8472022.

Zrenner, J., Möller, F. O., Jung, C., Eitel, A. and Otto, B., 2019. Usage Control architecture options for data sovereignty in business ecosystems. *Journal of Enterprise Information Management*, [e-journal] 32(3), pp. 477-495. http://dx.doi.org/10.1108/JEIM-03-2018-0058.