







Advancing Industry 4.0: Integrating Data Governance into Asset Administration Shell for Enhanced Interoperability

Mario Angos-Mediavilla^{1,2}^a, Michael Gorenzweig^{1,2}^b, Gerome Pahnke²^c, André Pomp¹^d,
Matthias Freund³^e and Tobias Meisen¹^f

¹*Institute for Technologies and Management of Digital Transformation, University of Wuppertal, Lise-Meitner-Str. 27-31, 42119, Wuppertal, Germany*

²*Digital Transformation Office, Coroplast Group, Wittener Straße 271, 42279, Wuppertal, Germany*

³*Festo SE & Co. KG, Rüter Str. 82, 73734, Esslingen, Germany*


Keywords: Asset Administration Shell, Digital Twin, Data Governance, Industry 4.0, Digital Transformation.


Abstract: The concept of Asset Administration Shell (AAS) is gaining attention in both the scientific community and manufacturing enterprises within the context of digital transformation and Industry 4.0. AAS enables the digital representation of information and services related to assets, facilitating their use and optimization in specific use cases. Standardization and the use of AAS as a vehicle for data transfer enables the collaborative exchange of information between value chain participants throughout the product life cycle. In this sense, it is essential to define and conceptualize the data governance (DG) aspects necessary to enable the use of the AAS concept in industry. Despite its significance, this topic has so far been insufficiently addressed in the scientific community. Therefore, this paper aims to identify the relevant aspects of DG needed in the AAS ecosystem, through a literature review. Based on these identified aspects, this paper addresses in detail, access control, role and rights management, and data management principles. Next, we suggest solutions for integrating these conceptual approaches into the current AAS metamodel. This approach lays the foundation for the adoption of AAS in industry, encouraging standardized data sharing practices among industry stakeholders.


1 INTRODUCTION


The ongoing digitalization of assets, i.e. physical and/or digital objects of an organization in the form of information and services, is currently an omnipresent and central topic and represents the basis for digital transformation and Industry 4.0 (I4.0) (Adolphs et al., 2015; Fleckenstein and Fellows, 2018; Boss et al., 2019). Further, as part of I4.0, digitalization advancements aim to facilitate collaboration between participants in the value chain, among other objectives. Nevertheless, this objective faces challenges due to the constant increase in the complexity of business processes, the need to individualize the products to be manufactured, and especially the growth in the


shared use of information and services in the manufacturing industry. In order to meet these challenges, the concept of asset orientation is being developed. Its goal is to systematically organize the increasing quantity of information and services associated with the exchange of data between manufacturers and to ensure a standardized structure for this information and services (DIN EN IEC, 2022). The Asset Administration Shell (AAS) is a concept that has received a lot of attention in this context. It is being developed to enable standardized representation and integration of assets into the information world, considered as the totality of all available data, digitalized systems, and people, in a virtual environment (Hertterich et al., 2015; Boss et al., 2019; Belyaev et al., 2021). Accordingly, the AAS aims to create a uniform standard for the digital twin for I4.0 and thereby attempts to define and establish the potential of the networked digital world in future industries. One important aspect addressed by the AAS is the semantic interoperability for cross-manufacturer data exchange (Adolphs et al., 2016; Boss et al., 2019; Bader et al.,


^a <https://orcid.org/0000-0003-3021-5515>

^b <https://orcid.org/0009-0003-3356-4320>

^c <https://orcid.org/0009-0009-5040-7697>

^d <https://orcid.org/0000-0003-0111-1813>

^e <https://orcid.org/0009-0008-4531-7817>

^f <https://orcid.org/0000-0002-1969-559X>

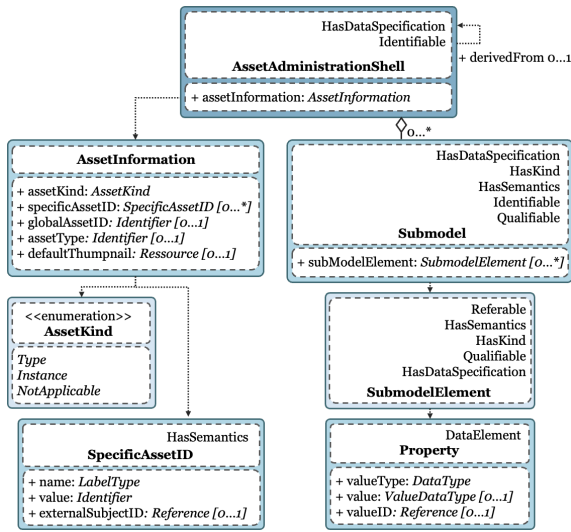


Figure 1: Metamodel of Asset Administration Shell (DIN EN IEC, 2022).

2019; DIN EN IEC, 2022). In data exchange along the value chain using the AAS, data governance (DG) plays a pivotal role in the successful development and establishment of the AAS in industrial organizations, particularly regarding data security and interoperability (Bader et al., 2019; Angeli et al., 2019). Given this context, the AAS faces the challenge of supporting cross-manufacturer data exchange, where manufacturers and their vendors have individual and partly informal DG concepts (DIN EN IEC, 2022; Zimmermann and Schäffer, 2023). Additionally, data exchange must comply with future legal and internal security regulations (Bader et al., 2019; DIN EN IEC, 2022). To fulfill the main objective, we address the following questions as guidelines throughout our work:

- Q1. What are the relevant aspects of DG for cross-manufacturer data exchange in the AAS ecosystem?**
- Q2. What options does the AAS offer for the integration of aspects of DG?**
- Q3. What could a possible DG approach for cross-manufacturer data exchange in the AAS ecosystem look like?**

In light of the above, the main objective of this work is to propose a solution for cross-manufacturer data exchange using the AAS, while considering specific aspects of DG. To achieve this objective, we initially define the concepts of AAS and DG in Section 2 (cf. Section 2). In Section 3 (cf. Section 3), we analyze the current state of the art. Based on a methodology (cf. subsection 3.1), in which we

develop and establish the criteria for the evaluation of the current literature, we present our results in the form of a corpus analysis (cf. subsection 3.2). Here, relevant aspects of DG are derived and identified. In Section 4 (cf. Section 4), we elaborate on and clarify the fulfillment conditions of the identified aspects of DG to ensure secure cross-manufacturer data exchange using the AAS. Based on this, we introduce the initial approach for the concept of DG for the existing structure of the AAS (cf. Section 5), represented by a Unified Modeling Language (UML) class diagram. Lastly, the key ideas of this study are summarized, and future research directions are provided (cf. Section 6).

2 FUNDAMENTALS

2.1 Asset Administration Shell

The Reference Architecture Model for Industry 4.0 (RAMI4.0) provides a three-dimensional framework for mutual understanding and communication among participants in the value chain. Additionally, RAMI4.0 serves as a guideline for the integration of I4.0 components (Adolphs et al., 2015; Heidel et al., 2019). The structure of an I4.0 component consists of an AAS, representing the concrete implementation of a digital twin (Boss et al., 2019), and its corresponding asset, a physical or logical object with value for a company (Heidel et al., 2019). The I4.0 component aligns with the principles of RAMI4.0 (Adolphs et al., 2015; Heidel et al., 2019) and is distinguished by a unique identifier (ID) (Heidel et al., 2019; Plattform Industrie 4.0, 2021). The architecture of the I4.0 component enables a digital representation of the associated asset. As discussed earlier, the AAS constitutes an integral part of the I4.0 component, embodying the standardized digital representation and characterization of an asset (Adolphs et al., 2015; Heidel et al., 2019; DIN EN IEC, 2022). To achieve this standardization, the general concept and existing structure of an AAS are defined in the IEC 63278-1 standard (DIN EN IEC, 2022). In order to describe the structure of an AAS from a technical point of view, a metamodel is used. This metamodel is created using a UML class diagram to define the hierarchical structure and relationships between the classes used and the associated instances, which are called objects (Czuchra, 2010; Bader et al., 2019; Industrial Digital Twin Association, 2023). As seen in Figure 1, the AAS consists of the classes *AssetInformation*, *Submodel (SM)*, *SubmodelElement (SME)* and *Property*. The *AssetInfor-*

mation class describes the specifications of the represented asset of the AAS. In addition, the AAS consists of several SMs, which represent a group of properties required to implement a specific use case (Boss et al., 2019). In this context, a dependency exists between the *SM* class and the *SME* class, because the *SME* class contains the actual specifications of the SM. Furthermore, an SME can assume various standardized SME types, such as property, blob or file, in which the data type and the respective value are contained (DIN EN IEC, 2022).

2.2 Data Governance

As outlined by Hildebrand (Hildebrand, 2011) and Khatri (Khatri and Brown, 2010), the concept of DG holds escalating significance in the evolving landscape of digitalization, assuming a pivotal role for contemporary organizations while simultaneously presenting novel challenges. In light of the recognition of data as a crucial asset within modern organizations and the exponential growth in data volumes, the implementation of a DG emerges as imperative for efficient data management, storage, and utilization (Khatri and Brown, 2010; Hildebrand, 2011; Fleckenstein and Fellows, 2018). Given the multitude of definitions associated with DG, the following adheres to an established definition proposed by Mosley (Mosley and Brackett, 2010) and Fleckenstein (Fleckenstein and Fellows, 2018), chosen for its alignment with the international, standardized, and formalized approach provided by the Data Management Body of Knowledge DMBOK (Mosley and Brackett, 2010). In accordance with Mosley (Mosley and Brackett, 2010) and Fleckenstein (Fleckenstein and Fellows, 2018), a DG is defined as “a framework for exercising authority and control (planning, monitoring, and enforcement) over the management of data assets”. A fundamental objective of DG lies in the handling and maintenance of data in harmony with organizational goals (Mosley and Brackett, 2010; Fleckenstein and Fellows, 2018; Zimmermann and Schäffer, 2023). DG encompasses various dimensions, including role and rights management, data life cycles, data quality, and data security (Mosley and Brackett, 2010; Hildebrand, 2011). Effective utilization of DG provides clarity regarding roles, responsibilities, and permissible actions at all times (Khatri and Brown, 2010; Mosley and Brackett, 2010; Hildebrand, 2011). This, among other benefits, can fortify trust in data exchange and ensure data availability (Khatri and Brown, 2010; Mosley and Brackett, 2010). It is essential to distinguish between DG and data management principles. While the DG defines roles, responsibilities and priorities

for the data management principles, the execution and implementation of policies, standards and or guidelines on aspects such as data security, confidentiality, interoperability, data quality, or data sovereignty, fall under the scope of the data management principles (Khatri and Brown, 2010; Mosley and Brackett, 2010; Fleckenstein and Fellows, 2018; European Commission, 2020). In order to establish a formalized and actionable DG, detailed data management principles are first required (Fleckenstein and Fellows, 2018).

3 RELATED WORK

3.1 Methodology

This work presents a systematic literature review in order to ascertain and evaluate the presence of the DG topic within the scientific community in the context of data exchange through a digital twin or an AAS. This review, inspired by the methodologies proposed by Snyder (Snyder, 2019), Heil (Heil, 2020), and Tercan (Tercan and Meisen, 2022), provides a supportive guide for the identification and evaluation of publications relevant to a specific theme, aligning with the defined scope of this work. The literature review is conducted using well-established databases such as *Web of Science*, *IEEE Explore*, *ACM Digital Library*, and *Semantic Scholar* as well as the leading institution *Plattform Industrie 4.0* in the context of I4.0. To guarantee search reproducibility and delimit its scope, the following set of keywords was defined in the form of boolean operators: “asset administration shell” AND (“data governance” OR “data policy” OR “data exchange” OR “access control” OR “access permission” OR “authorization” OR “authentication” OR “security”). Since the earliest publications in the AAS domain incorporating these selected keywords date back to 2017, this work restricts the publications to those from that year up to the present, i.e., the year 2023 in which this review is conducted. The systematic review, illustrated in Figure 2, encompasses key stages such as database search, removal of nonrelevant publications such as wrong subject area, target or category, and review of the remaining publications. From the initial database search, 50 relevant publications were identified, distributed as follows: *IEEE Explore* (23), *Web of Science* (11), *ACM Digital Library* (8), *Semantic Scholar* (7) and *Plattform Industrie 4.0* (1). Subsequently, the refinement process involved preselection, criteria selection, and snowballing. Preselection focused on obtaining full texts, eliminating nine publications due to restricted access. A detailed review of the remaining 41 publications centered on

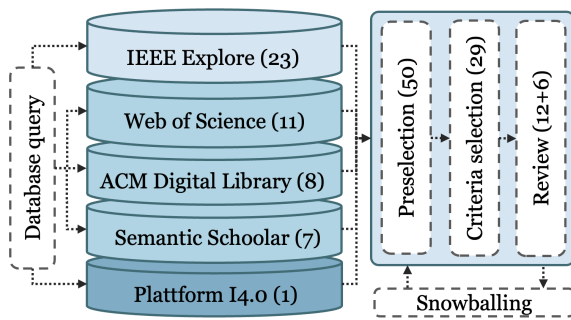


Figure 2: Overview of the systematic literature search process - own figure based on (Terçan and Meisen, 2022).

those originating from the manufacturing industry, resulting in the exclusion of 12 publications that pertained to a different sector such as biological engineering, smart cities, and/or agriculture. As a result of preselection, 29 publications remained as potential candidates. In the second step, the remaining publications were thoroughly examined, categorized, and consolidated based on various criteria, including publication target and aspects considered regarding DG. This categorization process, aided by an Excel tool and a text document for consolidating key passages, revealed that 17 publications lacked sufficient depth in DG content, i.e. the possible partial aspects of DG were only dealt with superficially in the main body of the publication and did not reveal any new or concrete statements or results so they were consequently excluded. In step three, based on the 12 remaining publications, an iteration was carried out using the snowballing principle, which identified six additional publications. This iterative process scrutinized source references and bibliographies in more detail, as inspired by (Claes, 2014). In the final step, based on the refined set of 18 publications, a detailed review is conducted to derive insights into the consideration of DG aspects in the AAS ecosystem.

3.2 Corpus Analysis

In this section, the identified publications are analyzed using two categories, as illustrated in Table 1. The first category outlines the target of the publications, where three subcategories are identified: *state of the art* (5), *conception* (9), and *proposal* (10). Publications categorized as *state of the art* delve into theoretical advancements in the realms of AAS and DG. Furthermore, nine publications present conceptual frameworks based on literature analysis, while another ten offer practical proposals for the concepts discussed in the literature. The second category highlights the aspects related to DG that are addressed in the publications. These aspects include *data security*

(15), *authentication* (15), *authorization* (10), *confidentiality* (8), *role and rights management* (10), *data sovereignty* (5), and *data integrity* (9). The publications explore and discuss these facets within the context of DG, contributing valuable insights to the current discourse on these critical topics. The aspect of *data security* appears in 15 publications and pertains to the security needed in the cross-manufacturer exchange of data. In this context, the data management principles outline the agreed-upon and/or legally prescribed rules and conditions to ensure data security (Moreno et al., 2023). Data security requirements encompass establishing mutual trust and/or authenticating the involved parties, managing information securely, and ensuring data integrity, which includes employing data encryption (Mosley and Brackett, 2010; Bedner and Ackermann, 2010; Hosseini et al., 2021). Compliance with the additional requirements of the General Data Protection Regulation (GDPR) is mandatory for the cross-manufacturer exchange of personal data. While the aspect of *authentication* appears in 15 of the publications, the aspect of *authorization* is mentioned in only ten of them. An interesting observation is the diversity of methods described, with eight distinct authentication methods such as *X.509*, *OAuth2.0* or *Decentralized Identifiers* and six distinct authorization methods such as *RBAC*, *ABAC* or *OAuth2.0*. Authentication serves as the initial verification step and grants the initial approval to access the respective system for data exchange and querying (Hosseini et al., 2022; Moreno et al., 2023). Authentication aims to verify the user's identity, utilizing certificates, passwords, or usernames to confirm the accessing user's authenticity (Ding et al., 2021; Dogan et al., 2022; Moreno et al., 2023). Following successful authentication, authorization determines which user can access specific data and content (Ding et al., 2021; Hang et al., 2022; Moreno et al., 2023). To define the granularity of data access, roles and rights can be assigned to corresponding users. Access rights regulate and restrict the actions that roles and users can execute. In this context, access control focuses on ensuring the authentication, authorization, and reliability of all value chain participants seeking access to AAS data (Angeli et al., 2019; Hang et al., 2022; Moreno et al., 2023). It is, therefore, a fundamental basis for compliance with data security, confidentiality, and integrity (Angeli et al., 2019; Jacoby et al., 2021; Hang et al., 2022). The aspect of *confidentiality* appears in eight publications and plays a pivotal role in securing cross-manufacturer data exchange, ensuring that only authorized users have access to pertinent information (Oh et al., 2019; Broring et al., 2022; ISO/IEC, 2022).

Table 1: Overview of the publications found in the literature (2017-2023), indicating their target and the aspects identified in the scope of the GD - own table based on (Webster and Watson, 2002).

Publication	Target			Aspect DG						
	State of the art	Conception	Proposal	Data security	Authentication	Authorization	Confidentiality	Role and rights management	Data sovereignty	Data integrity
[1] (Moreno et al., 2023)	●			●	●	●		●	●	
[2] (Broring et al., 2022)	●	●		●	●		●			●
[3] (Dogan et al., 2022)	●	●		●	●	●	●	●		●
[4] (Hang et al., 2022)		●	●	●	●			●	●	
[5] (Hosseini et al., 2022)		●	●	●	●			●		●
[6] (Dogan et al., 2021)		●			●	●				
[7] (Bröring et al., 2021)			●				●		●	●
[8] (Ding et al., 2021)			●	●	●	●				
[9] (Hosseini et al., 2021)	●			●	●					
[10] (Jacoby et al., 2021)			●	●				●	●	
[11] (Leander et al., 2021)		●		●	●	●		●		●
[12] (Redeker et al., 2020)	●				●	●	●		●	●
[13] (Angeli et al., 2019)		●		●	●	●	●	●		●
[14] (Lewin et al., 2019)			●	●			●			●
[15] (Oh et al., 2019)			●	●	●	●	●	●		●
[16] (Schmitt et al., 2019)		●	●	●	●	●		●		
[17] (Alonso et al., 2017)			●	●	●	●	●	●		
[18] (Tantik and Anderl, 2017)		●	●	●	●					

Additionally, various techniques are presented for ensuring data confidentiality, such as classifying information based on its security level and employing encryption methods (Angeli et al., 2019; Ding et al., 2021; Moreno et al., 2023). Meanwhile, the aspect of *role and rights management* is discussed in ten publications. Ding (Ding et al., 2021) and Moreno (Moreno et al., 2023) link the assignment of roles and rights directly with the previously mentioned authorization aspect, allowing access to specific information. The role and rights management aspect aims to ensure granularity of access to data by different users, roles, and/or attributes (Angeli et al., 2019; Hang et al., 2022; Moreno et al., 2023). To guarantee the release of appropriate and authorized data for exchange between manufacturers, data can also be classified based on sensitivity and importance as part

of role and rights management (Angeli et al., 2019; Ding et al., 2021; Moreno et al., 2023). In this aspect, access control concepts play an indispensable role. Several authors systematically introduce the concepts of attribute-based access control (ABAC) and role-based access control (RBAC) (Alonso et al., 2017; Angeli et al., 2019; Oh et al., 2019; Leander et al., 2021; Dogan et al., 2022). These concepts are employed to restrict access to data, with RBAC opting for the use of defined roles that grant access to specific information (Angeli et al., 2019; Dogan et al., 2022; Leander et al., 2021; Oh et al., 2019; Alonso et al., 2017). In contrast to this, ABAC provides more granularity by considering individual attributes along with roles (Alonso et al., 2017; Angeli et al., 2019; Oh et al., 2019; Leander et al., 2021; Dogan et al., 2022). Regarding rights management, the Platform

I4.0 (Angeli et al., 2019; Hosseini et al., 2022; Oh et al., 2019), and Moreno (Moreno et al., 2023) propose distinguishing between read access rights and write access rights. Additionally, Plattform I4.0 (Angeli et al., 2019) provides a comparative analysis between RBAC and ABAC access control. In this context, the authors opt for the ABAC method due to its dynamism and present it as a possible implementation in the AAS standard. However, they acknowledge the significant administrative effort required to implement the ABAC concept. On the other hand, RBAC represents a well-known and easy-to-manage solution with low administrative overheads, making it a viable candidate for managing information access within the AAS (Alonso et al., 2017; Angeli et al., 2019; Oh et al., 2019; Leander et al., 2021). The aspect of *sovereignty* holds significance in nine of the selected publications. In the context of a DG proposal for the AAS concept, data sovereignty refers to ensuring that participants in the value chain maintain control, data ownership, and entitlement over their data during data exchange (Redeker et al., 2020; Jacoby et al., 2021; Moreno et al., 2023). The goal is to ensure data sovereignty regardless of the number of participating organizations or systems. Consequently, in the course of data sovereignty, organizations must be able to decide independently what data is shared, to what extent, and with whom (Jacoby et al., 2021; Hang et al., 2022; Moreno et al., 2023). Finally, the aspect of *data integrity* is addressed in nine of the publications. Data integrity implies that ensuring the quality of data throughout its life cycle is a crucial requirement (Mosley and Brackett, 2010; Rahul and Banyal, 2020; Moreno et al., 2023). The diversity of requirements, both internally between departments and externally between organizations, poses challenges for data quality (Khatri and Brown, 2010; Hildebrand, 2011; Zimmermann and Schäffer, 2023). Due to the heterogeneity of user requirements, data classification is proposed. This involves categorizing the data to prioritize and protect the most sensitive data, ensuring data quality according to specific needs (Mosley and Brackett, 2010; Hildebrand, 2011; Fleckenstein and Fellows, 2018). Additionally, completeness, accuracy, immutability, availability, and timeliness of data play an indispensable role in terms of integrity and must be ensured in the exchange of data between manufacturers, during both data exchange and storage (Broring et al., 2022; Moreno et al., 2023). Thus, integrity refers not only to the quality of the data but also to the security of the data during their exchange (Bedner and Ackermann, 2010; Hosseini et al., 2021; Moreno et al., 2023).

4 RELEVANT ASPECTS OF DG FOR CROSS-MANUFACTURER DATA EXCHANGE IN THE AAS ECOSYSTEM

The corpus analysis, as explored in subsection 3.2 (cf. subsection 3.2), highlights a notable gap in introducing a comprehensive concept of DG and its associated aspects within the AAS ecosystem. While specific aspects of DG have been discussed, often in a highly theoretical manner, there is a distinct absence of concrete implementations. Hence, drawing on foundational principles (cf. Section 2), we advocate for approaching the DG concept through three key aspects crucial for information exchange in the value chain: data management principles, access control, and role and rights management. In the realm of data management principles, the authors underscore the significance of upholding confidentiality, data sovereignty, security, and integrity in their publications. For this purpose, the consensus is that data exchange between collaborating organizations must conform to valid data management principles. However, there is currently no specific concept or approach that describes how data management principles should be structured within the existing AAS metamodel. Therefore, we propose considering data management principles to be an aspect that encompasses the fulfillment of the requirements identified in the context of data security, interoperability, data integrity, data sovereignty, access control, and role and rights management. Moreover, the topic of access control has not yet been dealt with in depth in the analyzed publications. To ensure the authenticity of the respective user and/or system requesting access to the AAS, the principles of data management are complemented by access control. In this regard, we propose considering access control in conjunction with authentication and authorization aspects. The final aspect discussed in this paper is role and rights management, which guarantees and authorizes access to the respective AAS information based on defined roles and rights.

4.1 Aspect: Data Management Principles

Along with access control, and role and rights management, data management principles represent one of the most comprehensive aspects that enables exchange of data among value chain participants when considering DG. This section presents the conditions and organizational requirements necessary for successful cross-manufacturer data exchange, consider-

ing the identified aspects within the scope of DG. The premise is that the data management principles are interdependent with other aspects, each relying on the fulfillment of their respective requirements. It is crucial to underscore that while each aspect is interlinked, this paper acknowledges their independent consideration. To derive a possible solution, it is assumed that the following fulfillment conditions for the requirements are generally valid and must be met to ensure basic data security in the cross-manufacturer data exchange and to create a foundation for efficient and secure data exchange among different organizations and systems. In this process, data management principles are defined and created by the data provider and must be accepted by the data user before the exchange and use of data. To ensure that the requirements and fulfillment conditions of data management principles for access and data exchange are met, they can be incorporated into the Non-Disclosure Agreement (NDA) between the two parties. The following section describes the fulfillment conditions for the identified requirements. The fulfillment of the requirement *data security* hinges on the adherence to the agreed data management principles for cross-manufacturer data exchange, encompassing the necessary data security prerequisites, including authentication and authorization. Furthermore, strict compliance with the stipulations of the GDPR is paramount, and automated exchange of personal data via AAS is strictly prohibited. The manual review and approval processes for personal data must align with the prescribed role and rights management procedures. The requirement for *interoperability* is considered fulfilled if the AAS allows the transfer of data between different systems and organizations and uses standardized data formats, structures, and/or communication protocols. Additionally, it must be ensured that the data in the AAS has a common and unambiguous meaning and can be interpreted by all involved actors. The requirement *data integrity* is considered fulfilled if the data in the AAS meet the specified criteria. For this purpose, authentication methods and/or role and rights models for access to submodels (SM) and their properties can be taken into account and applied. The fulfillment of this requirement is contingent upon the proper classification of data destined for the AAS. This classification should not only align with the intended use case but also consider the sensitivity and significance of the data. Furthermore, enhancing data quality and upholding data integrity requires the implementation of authentication and authorization methods. Leveraging role and rights models for accessing SM and their properties contributes significantly to refining the param-

eters that define data quality. These measures are vital for maintaining the integrity of the data throughout its life cycle within the AAS. The requirement of *data sovereignty* is considered fulfilled when the security of data is taken into account, and compliance with contractual/organizational approaches described in the data management principles is guaranteed concerning the storage, processing, and transfer of data. This implies that the data management principles must be accepted by the data user before any data exchange takes place. The requirement *access control* is considered fulfilled if access to the AAS data is restricted by an access time and by means of access control. Authentication must successfully verify the identity of the user. Authorization must successfully define the access roles and access rights that regulate and restrict the actions of users. The access time must restrict or terminate access after expiry. The requirement *role and rights management* is considered fulfilled if the role and rights management ensures granularity for data access and defines and records roles, rights and attributes in the data management principles.

4.2 Aspect: Access Control

In terms of access control to AAS repositories, which involve information or services digitally represented in the AAS, the need for authentication and authorization is identified based on corpus analysis (cf. Section 3.2). To access the AAS, a basic level of trust has to be established between organizations, i.e., participants, through standards such as ISO 27001 or user authentication. This is a necessary condition in order to obtain proof of which user wishes to access the content and structure of the AAS and for how long they need access. For this work, we have evaluated various methods including *distributed ledger technology*, *X.509*, *OpenAuthorization 2.0*, *Blockchain*, *Asset Administration System* and *Object Memory Model*. Evaluation criteria included method maturity, decentralization, integration into the AAS structure, open source, identifiability with DIN 91406, and authentication and authorization capabilities. Based on the criteria evaluation we determined the X.509 Method to be a suitable candidate for authentication. The main advantage of X.509 over other methods is that X.509 is a decentralized, open-source method that provides an existing and established certification without requiring any additional specific adaptation to integrate it into the existing AAS structure, and it can be used for certificate-based authentication as described next (Angeli et al., 2019; Broring et al., 2022; Moreno et al., 2023). Furthermore, X.509 carries out a quick verification of the

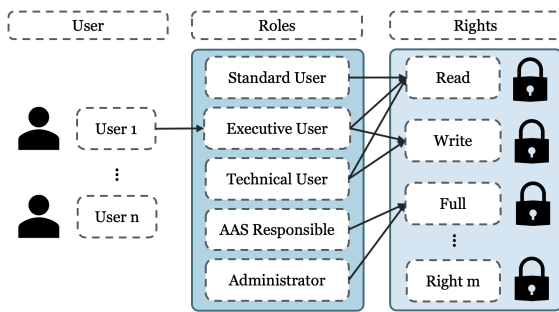


Figure 3: Overview of a possible solution for role and rights management - own figure based on (Ferraiolo, 2007).

certificate and, therefore, authentication can be performed, since this certificate confirms the identity and authenticity of the user from a trusted certification authority (Moreno et al., 2023). To integrate the method of X.509 into the existing AAS metamodel, both the signed certificate and the public key of the respective user are required. The authenticity of the user can be confirmed and guaranteed by comparing both objects. With regard to the fulfillment condition of access control, a time stamp of the authentication is also required for the subsequent steps, which should make it possible to define and manage access time.

4.3 Aspect: Role and Rights Management

The restriction of access to information and services within the AAS through the specification and use of roles and rights is crucial to ensure the successful exchange of information in the value chain necessary for the execution of a use case. Additionally, the data classification process is considered fundamental for effective management of roles and rights. In this regard, reference is made to the DG framework by (Fleckenstein and Fellows, 2018), emphasizing the need to prioritize the protection of critical business data. To achieve this, we propose precise classification of an organization's existing data into critical and noncritical business data, essentially a binary classification. In the context of AAS, we specifically propose the classification of data, namely SME, which will be stored or referenced in the respective SM of an AAS. This classification is performed manually in this work, emphasizing high and low sensitivity of the data. We propose two perspectives for the classification. One concept involves duplicating the same SM, i.e., an SM X.1 for high-sensitivity data and another SM X.2 for data that poses no risk to the company. Another perspective is the idea of sharing only non-sensitive data for the company, using only the AAS concept in this case. In the case of sensitive data,

the use of the AAS structure will be avoided. Currently, due to the present state of implementation of the AAS concept and its structure, the creation and generation of an AAS with its respective SMs and SMEs entails a large amount of manual and administrative work, mainly at the industrial level. Thus, our objective is to restrict the access to all the information relating to a specific SM, without differentiating its SMEs. It is important to note that the AAS concept provides the opportunity to restrict access at the AAS or SME level, but that is not the focus of this work. Similarly, the binary classification, which we focus on in this work, is a first step toward introducing DG aspects into the AAS. It is anticipated that the classification will be more detailed in various dimensions regarding AAS information and services. The management of roles and rights, complemented by binary classification, advocates for an RBAC concept, where access to AAS information is granted through the definition of user roles. Thus, RBAC provides a secure, easily manageable, and efficient solution for data access among manufacturers, aligning with organizational requirements (Ferraiolo, 2007; Emig, 2008). User assignment and rights allocation, separated by roles, facilitates access control without requiring changes for each user as organizational structures evolve. Figure 3 illustrates the interplay between user assignment, roles, and rights assignment. The implementation of RBAC involves more users than roles and rights. A relational $N \times M$ relationship accommodates this, allowing multiple role assignments for users and rights assignments for roles. In the AAS context, we propose basic roles, including administrator, AAS manager, standard user, technical user, and executive user. Each role aligns with specific rights, such as read access, write access, and full access. Administrator privileges encompass full access to the AAS, primarily managing user administration. AAS-responsibles possess extensive knowledge in a particular area, equivalent to organizational data stewards, managing AAS elements and data. Standard users have read access to the information and services represented in the SMs of the AAS. Technical users, on the other hand, have access to standardized technical SMs such as Provision of Simulation Models and Time Series Data. Executive users have additional authorizations beyond standard functions, such as the generation and visualization of reports based on the information from the relevant SMs. The rights allocation follows a successive structure: read access is highly limited, allowing only viewing and reading AAS content; write access includes read access, and full access encompasses both read and write access, along with the right to add, modify, and

delete information. The proposed concept requires at least one administrator and one AAS-responsible for each AAS, ensuring functionality and user creation. While we provide a basic concept of roles and rights, specific and more detailed roles and rights of the organization should be defined beyond this framework.

5 PROPOSAL FOR THE INTEGRATION OF DATA GOVERNANCE ASPECTS INTO THE METAMODEL OF THE AAS

To integrate the possible aspects of a DG, namely data management principles, access control, as well as role and rights management, into the ecosystem of the AAS, two options are discussed. The first option would be to integrate DG aspects in the form of an SM, using a template SM as proposed by the Industrial Digital Twin Association (IDTA) and subsequently standardizing it. This would require incorporating the SM that presents DG aspects into each AAS instance before proceeding with data exchange. Since DG is a concept that encompasses all SMs, this idea is susceptible to errors and unnecessary complexity, as DG aspects, such as role and rights management, would need to be manually referenced to each respective SM. On the other hand, the option of integrating the identified aspects related to DG directly into the structure of the AAS is considered, i.e., extending the AAS metamodel. In this way, the AAS concept would inherently contain the identified DG aspects, eliminating the need for additional integration. Therefore, we propose expanding the AAS metamodel with the identified DG aspects. This approach offers a more cohesive and efficient solution by avoiding redundancies and simplifying the process of integrating DG aspects into the AAS environment. For the integration, the existing metamodel of the AAS is used in the format of a UML class diagram. Further basics of a UML class diagram are not explained in detail and can be found in (Czuchra, 2010; Bader et al., 2019; Industrial Digital Twin Association, 2023). The extension of this metamodel by the proposed aspects of a DG is based on the DIN EN IEC 63278-1 in which the structure and specification of the third version of the AAS metamodel is described (DIN EN IEC, 2022). Specifically, the third version of the AAS metamodel does not take into account or include any aspects of a DG. Nevertheless, the existing structure of the AAS represents a significant advantage for integration, as the necessary structures and aspects are

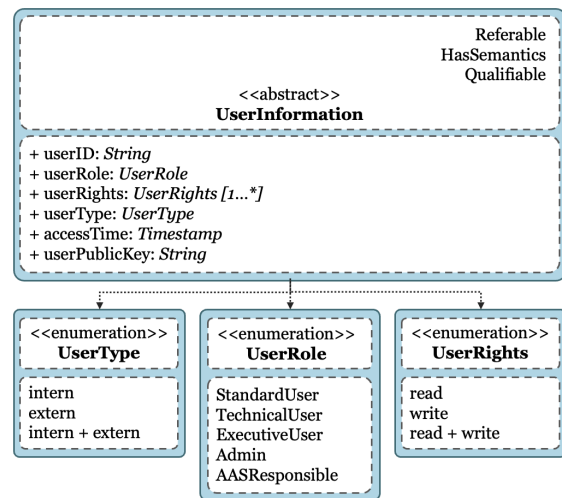


Figure 4: Overview of the `UserInformation` superclass - own figure.

defined and standardized so that they can be supplemented with new classes and attributes that follow the schema. Accordingly, Figure 6 shows a proposal for the integration of a DG into the existing metamodel of the AAS. Existing classes are shown in normal text. Extended classes and new classes are shown in bold text. In order to create an understanding of the extension of the existing metamodel in view of the new classes and attributes, the integrated superclasses (SC) `UserInformation` and `Authorizable` are explained first.

5.1 Superclass `UserInformation`

Figure 4 shows an overview of the SC `UserInformation`. This SC can be used to reference the user information to an element of the AAS metamodel so that it can contain information about the user, such as identification, roles or rights, if this is required for the further process. The SC `UserInformation` inherits all attributes from the classes `Referable`, `HasSemantics` and `Qualifiable` for a concrete specification, referencing and further information about the user's creator. The information about the user is made up of the attributes `userId`, `userRole`, `userRights`, `userType`, `accessTime` and `userPublicKey`. The `userId` contains a locally unique ID of the user in the form of a `string`, i.e. a character string, so that the user can be uniquely identified and referenced in the respective system. The attribute `userRole` represents the role of the user from the defined roles. This attribute is of the type of the class `UserRole`. This class in turn contains an enumeration of the user's roles. This is used to specify whether the user is a `StandardUser`, `TechnicalUser`, `ExecutiveUser`, `Administrator` or `AASResponsible`. In

order to maintain the consistency of the concept, each user is assigned a role in accordance with the specifications, as otherwise the assignment of the rights associated with the respective role can lead to inconsistencies and ambiguity. Analogous to the roles, the attribute *userRights* represents the user's rights from the defined rights. This attribute has the type *UserRights*, which contains an enumeration of the user's rights that are anchored in the user's role. It therefore specifies whether the user has *read*, *write* or *full* access to the SM. According to the specifications outlined in Section 4 (cf. Section 4), these rights are structured in an incremental manner, building upon each other. This delineates the roles eligible to receive these rights, ensuring alignment with the user's assigned role. In addition to roles and rights, each user is associated with a user type. The *userType* attribute denotes, for a specific user instance, its classification among the predefined user types. This attribute is of the class type *UserType*, which includes an enumeration of possible user types, indicating whether the user is *internal*, *external*, or both *internal and external*. Another attribute of the SC *UserInformation* is the *accessTime*. This attribute contains a timestamp with the time of the user's access to the information or services of the respective SM. The access time is saved and then overwritten each time the user is authenticated and is intended to manage and restrict the access period in a specific implementation. The final attribute is *userPublicKey*. This contains the user's public key in the form of a *string*, which is compared with a certificate for authentication.

5.2 Superclass Authorizable

Figure 5 shows an overview of the extended SC *Authorizable*. For further specifications the SC *Authorizable* inherits from the SC *HasSemantics*, *Referable* and *Qualifiable*. Specifically, the class *Authorizable* represents the authorization of the user. To do this, the class contains the attributes *authenticationCheckpoint*, *authorizeUser* and *SubmodelAccessRestriction*. To eliminate inconsistencies and security gaps, the *authenticationCheckpoint* attribute checks whether the user has been successfully authenticated. Consequently, this checkpoint is represented by the type *Boolean*. Similarly, the attribute *authorizeUser* is represented by a *Boolean*. This attribute authorizes the user if their characteristics match the authorization restrictions. The class *Authorization* contains the attribute *submodelAccessRestriction* for defining possible restrictions on authorization for data access. This attribute represents the restrictions for the authorization of the user and is of the type of the class *Submod-*

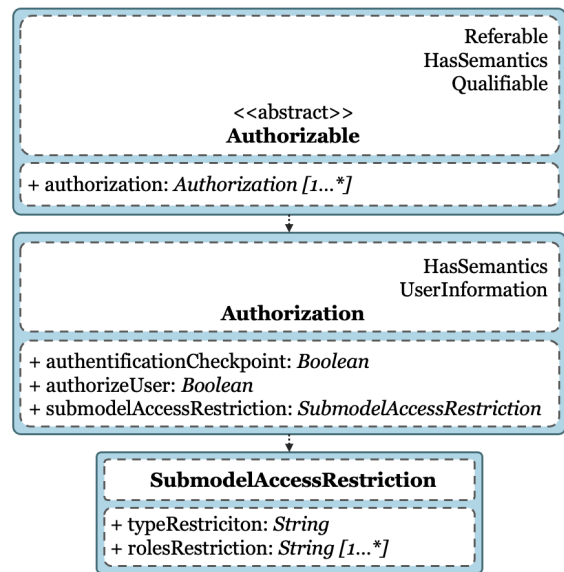


Figure 5: Overview of the Authorizable superclass - own figure.

elAccessRestriction. The class *SubmodelAccessRestriction* defines the restrictions for the authorization of the user. For this purpose, the class contains the attributes *typeRestriction* and *rolesRestriction*. The rights are not restricted because, as previously mentioned, these are associated with the respective role of the user. The *typeRestriction* attribute contains the permitted user types, i.e. the visibility for the SM, for data access. The permitted user types from the permitted set of user types are defined in this *string*. Analogous to visibility, the permitted roles for data access are defined via the *rolesRestriction* attribute.

5.3 Overview of the Extended Metamodel

Figure 6 illustrates the integration of a DG into the AAS structure. The extended metamodel incorporates the *accessControl* attribute, addressing security aspects such as authentication and data management principles for AAS access control. The *accessControl* attribute belongs to the *AccessControl* class, managing *authentication* methods and *datamanagementPrinciples*. The *AccessControl* class inherits from the SC *UserInformation* which provides information for user authentication and for authentication of checkpoints. Additionally, *AccessControl* inherits from the *Referable* class for local reference. The *datamanagementPrinciples* attribute signifies attachment of required data management principles and user confirmation, belonging to the *DatamanagementPrinciples* class. The *authentication* attribute denotes the au-

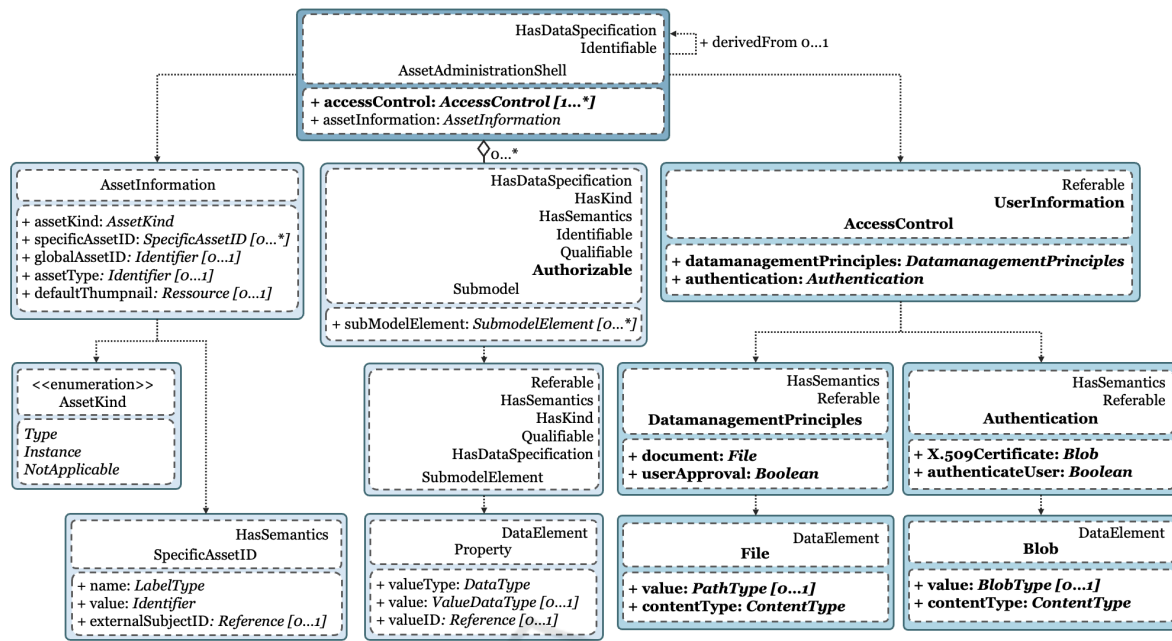


Figure 6: Overview of the integration of data governance aspects identified into the existing metamodel of the asset administration shell - own figure based on (Industrial Digital Twin Association, 2023); Existing elements of the asset administration shell shown in normal text; Extended elements for data governance shown in bold text.

Authentication method for data access and user authentication, belonging to the *Authentication* class. The *DatamanagementPrinciples* class includes the *document* attribute of type *File* for data guidelines and the *userApproval* attribute for user confirmation. *File* class attributes *value* and *contentType* represent the document path and content, respectively. The *Authentication* class features *X.509Certificate* for user authentication using certificates and *authenticateUser* for user authentication as a Boolean. The *Blob* class, concluding AAS access control, encompasses *value* and *contentType* attributes for blob instances. Finally, for user authorization, the *SM* class is extended by *SC Authorizable*. *SM* class inherits from *SC Authorizable* to impose access restrictions, allowing individual assignment based on role and rights management specifications. Notably, the assumption of data classification by sensitivity remains integral. *SM* can be replicated and created multiple times, each with distinct access restrictions and permissible visibility according to *SC Authorizable* specifications.

6 CONCLUSION AND OUTLOOK

The main objective of this scientific publication was to specify and develop a concept for integrating identified aspects of a DG into the existing structure of the AAS to ensure secure cross-manufacturer data exchange. To outline the relevance of the topic and

the main objective based on existing findings and research, we first conducted an exhaustive literature review. The literature review revealed that the number of publications on the topic of AAS in combination with a DG is very limited due to the newness of the subject. As a result, no publication could be identified that provided an initial proposal or concept for implementing a DG for data exchange among manufacturers using AAS. However, through the literature review, three potentially relevant aspects for DG compliance during data exchange among manufacturers were identified. These aspects are data management principles, access control, and role and rights management. These aspects formed the basis for specifying DG integration into the AAS structure. By achieving the main objective of the paper, we offer an initial proposal for future research in this area. Thus, the integration of a DG into the existing structure of the AAS aimed to restrict access to the AAS through access control, where users must first undergo an authentication and authorization procedure before gaining access to information and services stored in AAS repositories. Regarding **Q1**, seven relevant aspects for conceiving a DG for cross-manufacturer data exchange in the AAS ecosystem were identified: data management principles, data security, interoperability, data integrity, data sovereignty, access control, and role and rights management. Furthermore, not only necessary requirements are described, but also compliance definition to consider these aspects within

a DG framework. It is indicated that these aspects cover the most important organizational requirements to restrict and ensure the access to data and its use through AAS. For this reason, these requirements were integrated into the data management principles of the concept and must be accepted by users before accessing the data. The answer to **Q2** shows that the current AAS metamodel does not yet consider DG aspects. However, it offers specifications, definitions, and elements suitable for integrating potential DG aspects. The existing metamodel includes classes, SC, attributes, data elements, and relationships, allowing the addition of new elements that incorporate potential DG aspects. In answering **Q3**, possible aspects of a DG were initially specified for integration into the AAS metamodel. Regarding conceptualization, the necessity for a binary classification of the data was first demonstrated. This classification was required because the authorization in our concept was implemented using RBAC. To enable the RBAC to sensibly restrict access and granularity to the SM, the data was classified into business-critical and non-business-critical data. In the course of this, it was shown that different roles and rights for data access can be assigned depending on the type of data. The concept also includes the introduction of SC, such as *UserInformation* and *Authorizable*, as well as the creation of the class *AccessControl*. The *AccessControl* class was the foundation for ensuring that a user first authenticates himself with an X.509 certificate and accepts the organization's most important data management principles before accessing the AAS. To do this, the *AccessControl* class received the attributes of the user by inheriting them from the *UserInformation* class. If these two aspects of access control were fulfilled, the authorization of the user could continue. This was ensured by means of the *Authorizable* class, which also inherits the attributes from the *UserInformation* class. This concept will be tested and validated in future work. The remaining unanswered questions revolve around handling sensitive user data in the AAS, since our concept is based on the consumption and persistence of this user data in the AAS. One idea would be to integrate encryption concepts into user information to ensure data security and prevent it from being readable by any type of user.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support from The German Federal Ministry for Economic Affairs and Climate Action through the VWS4LS project (Grant No.13IK005A).

REFERENCES

- Adolphs, P., Auer, S., Bedenbender, H., and Billmann, M. (2016). Structure of the asset administration shell: further development of the reference model for the industry 4.0 component. *Federal Ministry for Economic Affairs and Climate Action*.
- Adolphs, P., Bedenbender, H., Dirzus, D., ..., and Wollschlaeger, M. (2015). Referenzarchitekturmodell industrie 4.0. *Association of German Engineers VDI*.
- Alonso, Á., Fernández, F., Marco, L., and Salvachúa, J. (2017). Iot application-scoped access control as a service. *Future Internet*.
- Angeli, C., Boss, B., Braunmandl, A., Brost, G., and ..., Schmitt, M. (2019). Access control for industrie 4.0 components for application by manufacturers, operators and integrators. *Federal Ministry for Economic Affairs and Climate Action*.
- Bader, S., Barnstedt, E., and Bedenbender, H. (2019). Details of the asset administration shell. *Plattform Industrie 4.0*.
- Bedner, M. and Ackermann, T. (2010). Schutzziele der it-sicherheit. *Datenschutz und Datensicherheit - DuD*.
- Belyaev, A., Diedrich, C., and Espen, D. (2021). Aas reference modelling: Exemplary modelling of a manufacturing plant with aasx package explorer based on the aas metamodel. *Plattform Industrie 4.0*.
- Boss, B., Bader, S., Orzelski, A., and Hoffmeister, M. (2019). Verwaltungsschale. *Handbuch Industrie 4.0*.
- Bröring, A., Belyaev, A., Trsek, H., Wisniewski, L., and Diedrich, C. (2021). Secure asset administration shell exchange with distributed ledger technology. *Plattform Industrie 4.0*.
- Bröring, A., Ehrlich, M., Wisniewski, L., Trsek, H., and Heiss, S. (2022). Towards an asset administration shell integrity verification scheme. In *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE.
- Claes, W. (2014). Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Blekinge Institute of Technology*.
- Czuchra, W. (2010). *UML in logistischen Prozessen: Graphische Sprache zur Modellierung der Systeme*. Studium. Vieweg + Teubner Verlag, 1st edition.
- DIN EN IEC (2022). DIN EN IEC 63278-1: Verwaltungsschale fuer industrielle Anwendungen. *DIN EN International Electrotechnical Commission[IEC]*.
- Ding, K., Fan, L., and Liu, C. (2021). Manufacturing system under i4.0 workshop based on blockchain: Research on architecture, operation mechanism and key technologies. *Computers & Industrial Engineering*.
- Dogan, A., Fay, A., Rijo, G., Diedrich, C., Block, C., and Bondza, A. (2021). Distributed ledger-basierte infrastruktur für verwaltungsschalen. *VDI Congress Automation*.
- Dogan, A., Schnakenbeck, A., and Fay, A. (2022). Distributed ledger-based authentication and authorization for industrie 4.0 components. In *IEEE 20th International Conference on Industrial Informatics (INDIN)*. IEEE.

- Emig, C. (2008). Access control in service-oriented architectures. *Karlsruhe Institute of Technology*.
- European Commission (2020). Data governance and data policies at the european commission.
- Ferraiolo, D. F. (2007). *Role-Based Access Control*. Artech House Computer Security Series. Artech House.
- Fleckenstein, M. and Fellows, L. (2018). *Modern Data Strategy*. Springer International Publishing.
- Hang, J. H., Charles, D. S., Gan, Z. H., Gan, S. K., Lim, Y. M., Lee, W. P., Wong, T. L., and Goh, C. P. (2022). Constructing a real-time value-chain integration architecture for mass individualized juice production. *Information*.
- Heidel, R., Hoffmeister, M., Hankel, M., and Döbrich, U. (2019). *Industrie 4.0: The reference architecture model RAMI 4.0 and the Industrie 4.0 component*. Beuth Verlag GmbH and VDE Verlag GmbH.
- Heil, E. (2020). Methode der systematischen literaturrecherche. In *Justus-Liebig-Universität Giessen*. Universitätsbibliothek Gießen.
- Herterich, M., Uebernickel, F., and Brenner, W. (2015). Nutzenpotentiale cyber-physischer systeme für industrielle dienstleistungen 4.0. *HMD Praxis der Wirtschaftsinformatik*.
- Hildebrand, K., editor (2011). *Daten- und information-squalität: Auf dem Weg zur information Excellence*. Praxis. Vieweg + Teubner Verlag, 2nd edition.
- Hosseini, A. M., Sauter, T., and Kastner, W. (2021). Towards adding safety and security properties to the industry 4.0 asset administration shell. In *2021 17th IEEE International Conference on Factory Communication Systems (WFCS)*. IEEE.
- Hosseini, A. M., Sauter, T., and Kastner, W. (2022). A safety and security reference architecture for asset administration shell design. In *2022 IEEE 18th International Conference on Factory Communication Systems (WFCS)*. IEEE.
- Industrial Digital Twin Association (2023). Specification of the asset administration shell - part 1 metamodel. *Industrial Digital Twin Association*.
- ISO/IEC (2022). ISO/IEC 27002:2022-02 Information security, cybersecurity and privacy protection - Information security controls. *International Organization for Standardization [ISO], International Electrotechnical Commission [IEC]*.
- Jacoby, M., Volz, F., Weißenbacher, C., Stojanovic, L., and Usländer, T. (2021). An approach for industrie 4.0-compliant and data-sovereign digital twins. *Automatisierungstechnik*.
- Khatri, V. and Brown, C. V. (2010). Designing data governance. *Communications of the ACM*.
- Leander, B., Causevic, A., Hansson, H., and Lindstrom, T. (2021). Toward an ideal access control strategy for industry 4.0 manufacturing systems. *IEEE Access*.
- Lewin, M., Dogan, A., Schwarz, J., and Fay, A. (2019). Distributed-ledger-technologien und industrie 4.0. *Informatik Spektrum*.
- Moreno, T., Almeida, A., Toscano, C., Ferreira, F., and Azevedo, A. (2023). Scalable digital twins for industry 4.0 digital services: a dataspace approach. *Production & Manufacturing Research*.
- Mosley, M. and Brackett, M. (2010). *The DAMA guide to the data management body of knowledge*. Technics Publications.
- Oh, S.-R., Kim, Y.-G., and Cho, S. (2019). An interoperable access control framework for diverse iot platforms based on oauth and role. *Sensors*.
- Plattform Industrie 4.0 (2021). The asset administration shell in detail - from the idea to the implementable concept.
- Rahul, K. and Banyal, R. K. (2020). Data life cycle management in big data analytics. *Procedia Computer Science*.
- Redeker, M., Volgmann, S., Pethig, F., and Kalhoff, J. (2020). Towards data sovereignty of asset administration shells across value added chains. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE.
- Schmitt, J., Gamer, T., Platenius-Mohr, M., Malakuti, S., and Finster, S. (2019). Authorization in asset administration shells using opc ua. *Automatisierungstechnik*.
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*.
- Tantik, E. and Anderl, R. (2017). Integrated data model and structure for the asset administration shell in industrie 4.0. *Procedia CIRP*.
- Tercan, H. and Meisen, T. (2022). Machine learning and deep learning based predictive quality in manufacturing: a systematic review. *Journal of Intelligent Manufacturing*.
- Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *JSTOR*.
- Zimmermann, L. and Schäffer, T. (2023). Interorganisatorische data governance: Vorschlag eines rollenmodells für einen kooperativen datenaustausch im kontext von logistik 4.0. *HMD Praxis der Wirtschaftsinformatik*.