Chapter 19
Industrial Data Spaces

Thomas Usländer and Andreas Teuscher

Abstract This chapter describes the application of the IDS principles, architectural artifacts, and technologies to the application domain of industrial production and smart manufacturing, in particular as drafted by the Platform Industrie 4.0 in their Reference Architecture Model Industrie 4.0 (RAMI4.0) and follow-on specifications about the Asset Administration Shell (AAS). It elaborates on the working approach of the IDS-Industrial Community (IDS-I) for the analysis of requirements on data sovereignty. This activity is motivated by the vision 2030 of the Platform Industrie 4.0 that states autonomy, including data sovereignty, as one strategic field of action.

The chapter presents how IDS-I aims at systematically deriving and analyzing data sovereignty aspects from the two reference use cases, Collaborative Condition Monitoring (CCM) and Smart Factory Web (SFW), in order to identify architectural and technological synergies and gaps between the International Data Spaces (IDS) and the specifications of the Platform Industrie 4.0.

19.1 Motivation for Industrial Data Spaces

Digitalization leads to the creation and usage of data. In the context of this social, economic, and technical development, data has become an independent product, also in the domain of industrial production and smart manufacturing. As an economic good, they form the basis for new value-added processes and business models. In daily business practices, data are used very often, however, exchanged rather rarely. Companies are still too worried about losing control over their data—and thus their valuable corporate knowledge. This is where International Data Spaces (IDS) come

T. Usländer (✉)
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Karlsruhe, Germany
e-mail: thomas.uslaender@iosb.fraunhofer.de

A. Teuscher
SICK AG, Waldkirch, Germany
e-mail: andreas.teuscher@sick.de

B. Otto et al. (eds.), *Designing Data Spaces*,
https://doi.org/10.1007/978-3-030-93975-5_19

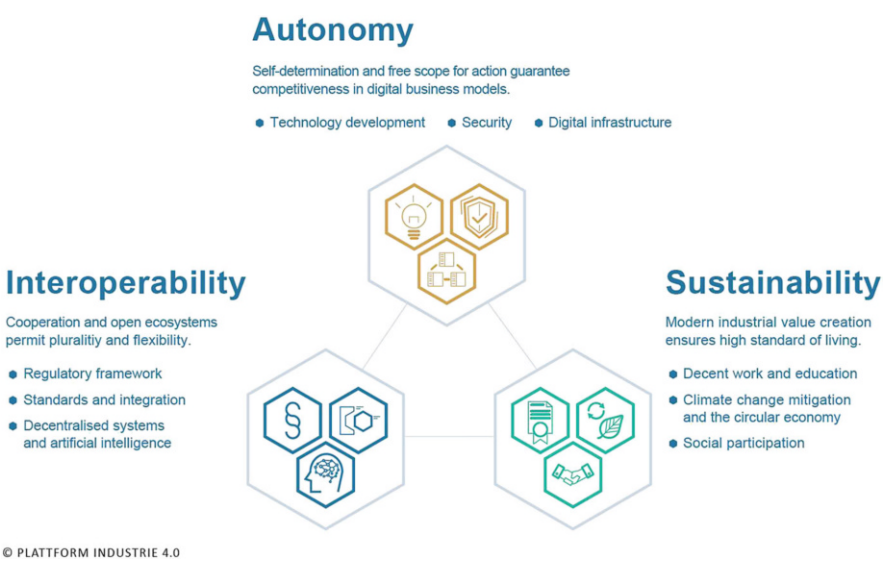

Fig. 19.1 Strategic fields in the Vision 2030 of the Platform Industrie 4.0 [1]

into play: with an architecture for virtual data spaces that guarantees the secure and sovereign exchange of their data.

The overriding objective of the IDS is to help companies and institutions to take advantage of the benefits of digitalization without increasing their risks. The means for this is a trustworthy architecture for data management with standards for sovereignty and secure data exchange.

The International Data Spaces Association (IDSA) represents the interests of more than 120 international companies and institutions. The IDSA bundles the requirements for all IDS application domains, organizes the exchange of knowledge between research and industry, and develops guidelines for the certification, standardization, and utilization of the results resulting from the various IDSA-related research projects at European and national level.

In its vision for 2030, published in August 2019, the Platform Industrie 4.0 formulated a holistic approach to the shaping of digital ecosystems and re-orientated the further development of Industrie 4.0 according to this vision [1]. At the heart of the design of digital ecosystems are the three strategic fields of action autonomy, interoperability, and sustainability (see Fig. 19.1).

For data sovereignty the strategic field of autonomy is highly relevant:

- Autonomy is the freedom to take independent decisions and to interact in conditions of fair competition—from a chosen business model to an individual's decision to make a purchase.
- Autonomy requires an open digital infrastructure for everyone, data protection, IT and information security, and technology-neutral research, development, and innovation.

The freedom to take independent decisions and the request for fair conditions are key characteristics of the demand for digital sovereignty—on the technological and infrastructural level as well as on the data level. The European initiative GAIA-X [2] focuses on the former level and aims at creating a secure, federated infrastructure that meets the highest standards of digital sovereignty while promoting innovation. The data level, however, is the key concern of the IDS.

Within IDSA, the application domain of networked industrial production and smart manufacturing, hence Industrie 4.0, is represented by a dedicated community entitled IDS-Industrial, abbreviated by IDS-I. This chapter describes how IDS-I handles the problem of analyzing the requirements on data sovereignty for Industrie 4.0.

As a consequence, the mission of the IDS-Industrial Community is summarized as follows:

1. To gather requirements on data sovereignty incl. Data sharing, data usage monitoring and control, as well as data provenance tracking by means of reference use case specifications.
2. To map these requirements systematically to the standards, capabilities, and recommended technologies of the International Data Spaces Association and the Platform Industrie 4.0.
3. To derive profiles of IDS/Industrie 4.0 specifications that support the requirements in industrial business ecosystems based upon standards and by means of common governance models.
4. To validate and demonstrate the applicability of these specifications by means of reference testbeds, e.g., Smart Factory Web and GAIA-X use cases.
5. To contribute to the outreach of the IDS architecture and specifications to the community of industrial production and smart manufacturing.

In this chapter, it is described how the individual statements of this mission are carried out.

19.2 Industrial Perspective

Establishing globally accepted framework conditions for possession, ownership, transfer, and usage of data is a basic prerequisite for the realization of an efficient digital ecosystem.

In order to meet the requirements for the networking of industrial equipment, machinery, and sensors with cloud/data services in the Internet, going hand in hand with digitalization, “smart machinery” or “cyber-physical systems (CPS)” must become part of the Internet of Things (IoT). The production environment, in particular, is becoming increasingly digital and intelligent. Especially automation, mobility, flexibility, and individuality are pushed. Digitalization is thus becoming the key to making things in the cyberspace addressable, visible, and, in this way, usable, e.g., for applications such as condition-based monitoring, predictive

analytics, and maintenance. It increases efficiency as well as attractiveness of a location for business development and competitiveness.

From the industrial perspective, there are the following central requirements:

1. **Identification of users without doubt when they access equipment, machinery, and sensor data.**

   In the real world, this problem is addressed with documentary proof such as an identity card or an employee badge. In the digital world, a one-to-one digital identity, which is accepted beyond a security domain, is necessary. Examples of this exist in telecommunications technology, which allows a mobile phone user to be identified in the telecommunications network via a subscriber identity module. Subsequently, the mobile communications provider provides data connections to the user.

2. **Upon successful identification, the transfer of data must be safeguarded against manipulation before the data flow starts.**

   In view of the increasing data volumes, the transfer must be at the same time secure and reliable as well as efficient (high throughput) and scalable. Ideally, as these objectives may be contradictory, the users themselves should be able to define the required level of the technical security. Thus, it would be possible to select the security mechanisms to the match the data protection class.

3. **Usage characteristics shall be assigned to the data itself, further-on communicated to the recipient, and, in an ideal case, enforced and monitored.**

   As a consequence, data could be linked to a dedicated contract associated with a data usage control policy, e.g., to delete the data elements after a certain period of use or number of accesses in order to prevent any further use. However, this would require the data user to receive, understand, and confirm the terms of use. It lies in the nature of digital data that reproduction without any technical problems and quality loss results in a transfer of possession that is undesirable to the owner. This can only be prevented and controlled by clear rules and their technical implementation. These measures must be transparent and trustworthy for all economic actors. To this end, it is necessary to create independent institutions and technologies ensuring compliance with the socially necessary and accepted rules.

The IDS-Industrial Community has come to entertain the view that an individual company that centrally controls and manages data and its possession and/or the transfer of data ownership cannot fulfill the conditions of a free market economy, because such an approach would result in a global monopoly on data.

The current practice of signing bilateral contracts and bilateral technical agreements to lay the foundation for secure data sharing generates high costs for establishing and maintaining a contract and, consequently, high transaction costs, and it would hinder further digitalization.

If we aim at leveraging a diversified, competition-driven global economy, we need to standardize in terms of laws and regulations and technically implement a data ecosystem for the transfer of ownership and the associated transfer of possession.

The IDS-Industrial Community is convinced that the International Data Spaces promotes digital sovereignty of data owners in the industrial data economy and thus provide the basis for an open, generally accepted technical procedure for all data transactions. The development of such a trust level with the label "Made in EU" could not only significantly promote global data sharing and thus the growth of future data-based business models but in general support easy value creation as an enabler for the economy.

19.3 Requirements Analysis in the IIoT

The question of how to handle requirements on data sovereignty in joint Industrie 4.0/IDS and GAIA-X service-oriented environments falls into the general problem of Agile Service Engineering in the Industrial Internet of Things (IIoT) [3].

As illustrated in Fig. 19.2, an agile approach is recommended to reduce the conceptual and terminological gap between the views of the thematic expert (typically an industrial, mechanical, and/or an electrical engineer) and the IT expert (typically, a computer scientist). Driven by the business strategy, the thematic expert expresses his/her functional and non-functional requirements about the system's behavior and characteristics, whereas the IT expert "answers" in terms of (mostly technical) system capabilities and service registries. Usually, both descriptions cannot be matched without additional, tedious discussions and additional explanations.

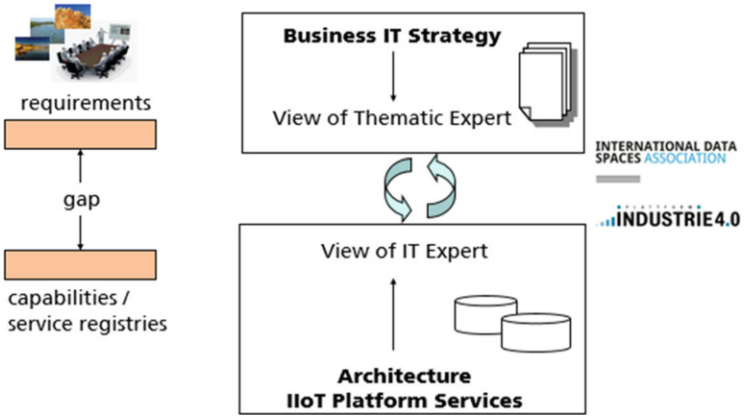

Fig. 19.2 Mapping of requirements in IoT platform environments

ID	<<will be defined later>>
Name	Name of the use case
Priority	[Low, medium, high]
Reference use case	[Smart Factory Web, Collaborative Condition Monitoring or other...]
Description	Textual description of the use case: • motivation • involved stakeholders • objective • constraints • ...
Comment	Optional further comments
Preconditions	what is required before the use case may be started or deployed
Workflow	The following steps are required to perform the use case: 1. ... 2. ... 3. ... ... Note: may have loops and jumps (if ... then go to step X)
Postconditions	Describe the situation after the use case was carried out
Sources	Literature or references
Authors	Name of the authors
Date	Date of last change

Fig. 19.3 Use case template as used in the IDS-Industrial Community

The idea of the SERVUS methodology [3] is to use semi-structured descriptions of use cases for this activity, following semi-structured use case templates [4] (see Fig. 19.3). With SERVUS, this idea of a semi-structured description of analysis and design artifacts applies, too, when mapping the use cases step-by-step to other design artifacts such as requirements and when matching them with abstract, technology-independent capability descriptions of IIoT platforms.

The terminological gap is approached by attaching semantic annotation labels to the basic terms used. The IIoT platforms of interest are those specified by the Platform Industrie 4.0, IDS, and GAIA-X. In order to master this stepwise mapping

process, all the analysis and design artifacts are stored in an IIoT Platform Engineering Information System (IIoT-PEIS), which also provides documentation, information retrieval, and visualization support [3].

19.4 IDS-I Reference Use Cases

The IDS-I Community decided to describe use cases stemming from two so-called reference use case domains (Fig. 19.4), also used by other initiatives:

- Collaborative Condition Monitoring (CCM), provided by the Platform Industrie 4.0 applied as GAIA-X use case.
- Smart Factory Web (SFW), an accepted IIC Testbed of the Industrial Internet Consortium (IIC).

19.4.1 Collaborative Condition Monitoring (CCM)

The CCM reference use case deals with the collection and use of operating data to optimize the reliability and service life of machines and their components during operation [5]. In the real world, installed machines come from different machine suppliers that are equipped with different products from different component suppliers. In these multi-stakeholder environments, the exploitation of the data of components, machines, and the factory plant to provide higher-level services such as predictive maintenance is still a challenge.

This is due not only to the lack of interoperability, which may be solved by encapsulating the assets by the concept of the Asset Administration Shell (AAS), but also due to the uncertainty of how to control the access and usage of the datasets

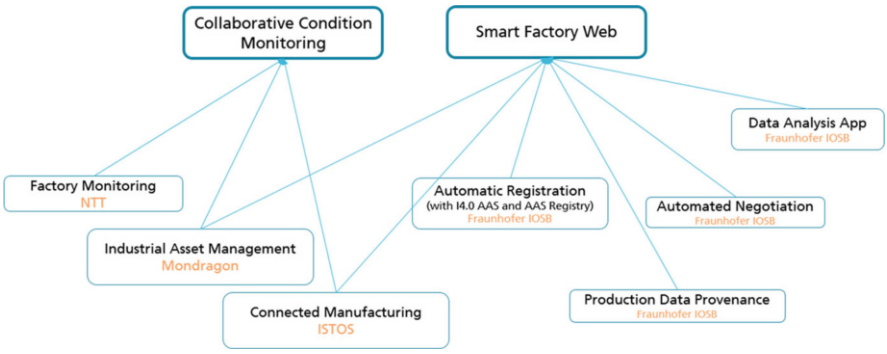

Fig. 19.4 Usage control as an extension to access control. ©2020, International Data Spaces Association (IDSA)

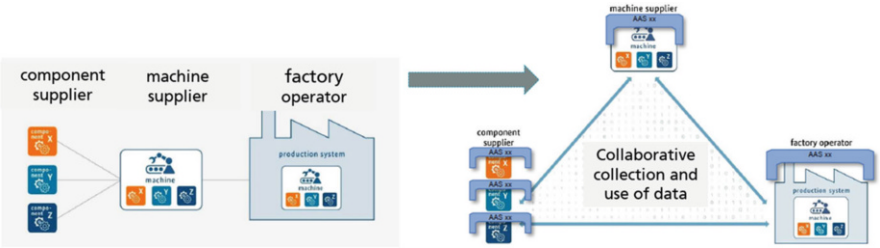

Fig. 19.5 CCM and SFW use cases under investigation in IDS-I

associated with and provided by the assets. IDS-I aims at investigating the detailed requirements and concerns (Fig. 19.5).

19.4.2 Smart Factory Web (SFW)

The SFW reference use case provides a blueprint architecture for open sustainable and resilient production ecosystems [6]. One important SFW application is an industrial marketplace for industrial production following the platform-driven economy of other branches such as tourism or mobility. As illustrated in Fig. 19.6, the demands of higher resilience, sustainable production, more flexibility, higher product variance, manufacturing on demand, and smaller lot sizes do not only address the factory level, e.g., the shop floor environment, but also the supply chain level, the so-called connected world of the Reference Architecture Model Industrie 4.0 (RAMI4.0).

A marketplace is highly needed that does not impose business dependency constraints upon the suppliers, but is designed on the principles of openness,

Fig. 19.6 Problem illustration of the Collaborative Condition Monitoring use case [5]. ©2020, Platform Industrie 4.0

fairness, and transparency. It allows a user to quickly search for new and alternate suppliers in a supply chain network. More flexibility is demanded in case a given supply chain is at risk or about to fail due to broken transport lines, natural catastrophes, pandemics, or material shortage.

In order to enable searching for alternate suppliers and matchmaking by the marketplace, adequate data about the capabilities and assets of factories in the supply chain is required. IDS-I aims at investigating the detailed requirements and concerns about sharing this type of data in a marketplace and within the supply chain network.

19.5 Requirements Analysis for Data Sovereignty

When considering and analyzing the requirements for data sovereignty in case of scenarios spanned by these two reference use cases, one has to distinguish between the classical aspects of access control (to data and operations) and data usage control.

Usage control is an extension to traditional access control [7]. After access to data and operations has been permitted, the question remains what happens to the data after the access and delivery of the data (as part of operation results). Hence, usage control is about the specification and enforcement of restrictions regulating what must (not) happen to data. Usage control is concerned with requirements that pertain to data processing (obligations), rather than data access (provisions) as illustrated in Fig. 19.7. In general, usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management.

As IDS-I aims to ensure data sovereignty in industrial value chains, requirements on data usage control are analyzed according to a common scheme, following the list of obligations proposed by [7]:

- **Secrecy:** Classified data must not be forwarded to nodes which do not have the respective clearance.
- **Integrity:** Critical data must not be modified by untrusted nodes as otherwise their integrity cannot be guaranteed anymore.
- **Time to live**: A prerequisite for persisting data is that it must be deleted from storage after a given period of time.

Fig. 19.7 Problem illustration of the Smart Factory Web use case

- **Anonymization by aggregation**: Personal data must only be used as aggregates by untrusted parties. A sufficient number of distinct records must be aggregated in order to prevent de-anonymization of individual records.
- **Anonymization by replacement**: Data which allows a personal identification must be replaced by an adequate substitute in order to guarantee that individuals cannot be de-anonymized based on the data.
- **Separation of duty:** Two data sets from competitive entities (e.g., two automotive OEMs) must never be aggregated or processed by the same service.
- **Usage scope:** Data may only serve as input for data pipes within the connector, but must never leave the connector to an external endpoint.

The IDS-Industrial Community has started a process to analyze the two reference use cases in more detail by means of use case descriptions that fall into these categories. For each of the use cases, requirements on access control (both role-based and attribute-based), usage control (according to the obligation categories described above), and data provenance tracking (where does the data come from) are gathered and analyzed.

19.6 Major Concepts of the International Data Spaces (IDS)

In order to understand the use case analysis below, the major architectural concepts of the International Data Spaces (IDS) are described [8] in the following and illustrated in Fig. 19.8.

- **Data spaces** unlock the value of data.
- An **IDS Connector** is a dedicated software component that allows participants to attach usage policies to their data in a data space, enforce the usage policies, and seamlessly track the provenance of received data. Hence, an IDS Connector acts as a kind of gateway for data and services. Furthermore, it provides a trusted environment for the execution of apps.
- **Data owner and data provider**: The data provider is a device that transfers the owner's data to the data space via the IDS Connector. It allows others to use the data while retaining control over the who, how, when, why, and at what price.
- **Data user and data consumer**: The data consumer is a device that processes data on behalf of the user. The data is offered by data providers by their usage policies and with confidence in the data quality and reliability.
- An **Identity Provider** creates, maintains, manages, and validates identity information of and for participants in the data space such as data providers and data consumers.
- **App Stores** provide software applications that can be deployed in IDS Connectors.
- **Apps** may be downloaded from the App Store into the trusted environment of the IDS Connector. Apps perform tasks such as transformation, aggregations, or analytics of data.

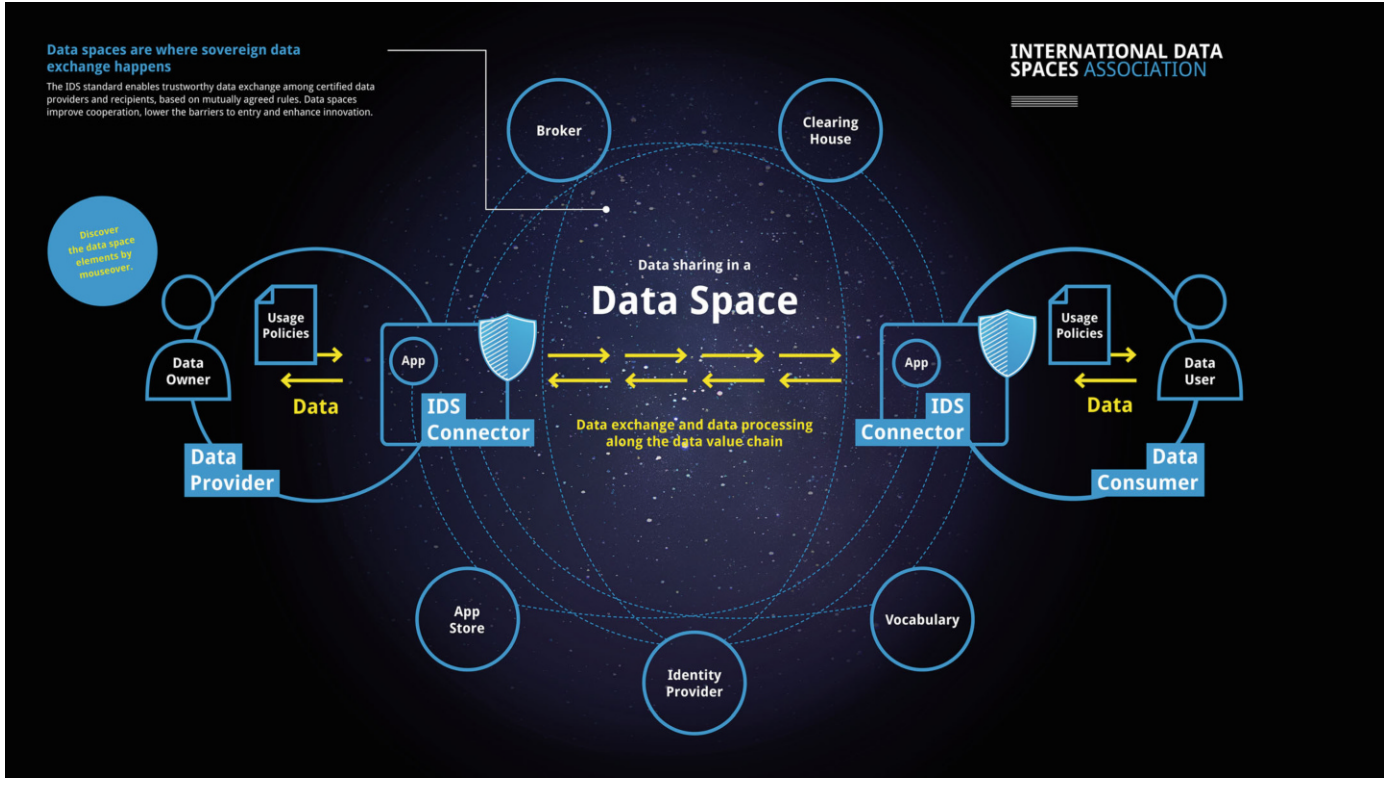

Fig. 19.8 Basic Architectural Concepts of the International Data Spaces (IDS). ©2021 International Data Spaces Association (IDSA)

- A **Broker** provides information about data sources in terms of content, structure quality, currency, and other features.
- A **Clearing House** provides clearing and settlement services for all data exchanges and financial transactions within a data space.
- **Vocabularies** provide standardized descriptors for data based on accepted best practices.

19.7 Exemplary Use Case Analysis

As an example for a detailed use case analysis, we take the "Automated Negotiation" use case in the context of the Smart Factory Web.

Name	Automated Negotiation
Priority	Medium
Referenceuse case	Smart Factory Web (SFW)
Description	**Motivation** The Smart Factory Web enables the design of an open matchmaking platform for industrial production to find new business partners and negotiate with them (Manufacturing as a Service—Maas). In most industries today, this negotiation is carried out by manual agents with telephone and e-mail. During the negotiation, sensitive information such as price, availability, capacity, and process durations are revealed. There is a need for a data infrastructure to let automatic negotiation agents handle the negotiation without revealing any information to potential partners. Negotiation should take place in isolated data containers (e.g., connectors) that interact with each, but cannot leak any information elsewise. After negotiation, the successful terms of a contract are presented, but dynamic variables about the production shall remain hidden. The companies then have the opportunity to sign the contract proposed by the negotiation. **Involved Stakeholders** Smart Factory Web portal, Company A, Company B **Objective** Hide sensitive data during negotiations **Constraints** The negotiation apps need to be compatible with each other, meaning that successful negotiation is usually achieved in the same industry branch, where variables and prices can be compared. Additionally, these apps need to be licensed by some authority so that information cannot be extracted
Pre-conditions	When realized in an IDS environment: both companies have IDS Connectors deployed with negotiation apps downloaded from certified IDS app stores.
Workflow	The following steps are required to perform the use case: 1. The production capabilities and/or production assets of company B are registered in the SFW portal. 2. Company A searches for an adequate production capability and issues a search request to the SFW portal. 3. Company A finds Company B on the SFW portal and places an order for a component or service.

(continued)

	4. The SFW portal performs the search and returns an endpoint address of company B to company A. 5. Company A contacts Company B via the IDS Connector and initiates the negotiation. 6. Negotiation data is exchanged between the IDS connectors involved according to the negotiation needs. 7. The negotiation is handled by the negotiation app without sensitive information ever leaving the IDS connectors including their apps. 8. The information gets deleted and the result of the negotiation presented (contract with terms). 9. Company A and B sign the contract, or they may proceed to the next negotiation step.
Post-conditions	Successful negotiation and contract between previously unknown partners.
Sources	https://www.smartfactoryweb.de
Authors	Employees of Fraunhofer IOSB

When reflected at the data sovereignty aspects presented before, this use case covers the following aspects:

- **Secrecy:** Negotiation data must not leave the IDS connectors and the negotiation apps.
- **Integrity:** Negotiation data must not be modified.
- **Time to live**: Negotiation data shall be deleted after the negotiation process.
- **Anonymization by aggregation/replacement**: not necessarily required.
- **Separation of duty:** Negotiation data shall only be used for the negotiation between companies A and B.
- **Usage scope:** Negotiation data may only serve as input for the negotiation process.

Looking at basic architectural patterns when realizing this use case in the context of an Industrie 4.0/IDS System environment, one option is as follows:

1. The capabilities and/or assets of company B are represented to the SFW portal according to the meta-model and constraints of the Industrie 4.0 asset administration shell and related AAS sub-models.
2. The SFW portal accesses the capabilities and/or assets of company B by means of one of the AAS application programming interfaces (e.g., RESTful API or OPC UA).
3. The SFW portal just acts as mediator between the search request of company A and is not directly involved in the negotiation process.
4. The negotiation process is carried out in a trusted IDS industrial data space by means of interacting IDS connectors.

Please note that other architectural patterns are possible. For instance, the SFW portal may also be connected to the industrial data space via IDS connectors and may act as active negotiation broker including a negotiation policy. In such a setting, the SFW portal may also learn from previous negotiations based on anonymized data in order to improve the negotiation based upon additional information. In this case, the data sovereignty aspects need to be interpreted and applied in a different manner.

This use case analysis shows that the level and aspects of data sovereignty are dependent on the use case to be supported. The basic IDS architecture is designed in a generic manner such that a multitude of use cases may be implemented. By means of a detailed use cases analysis, the IDS-Industrial Community validates this approach and proposes reusable architectural options in the context of a joint Industrie 4.0/IDS system environment.

19.8 Outlook

The mission of the IDS-Industrial (IDS-I) Community is to enable the design, setup, and operation of International Data Spaces tailored to the needs of the application domain of industrial production and/or smart manufacturing. IDS-I is an open community associated with the IDS Association, currently comprising 47 companies and research institutes around the world. The IDS-I Community is convinced that the handling of data sovereignty according to international regulations and standards will become a critical success factor for the European manufacturing industry [8], or may be even world-wide. After the requirements analysis on data sovereignty was published in an IDS-I position paper in June 2022 [9], IDS-I will consider the architectural and technological consequences in joint Industrie 4.0/IDS and GAIA-X system and infrastructure environments.

References

1. Platform Industrie 4.0 (Ed.). *Position Paper 2030 Vision for Industrie 4.0*. https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Positionspapier%20Leitbild%20(EN).html
2. GAIA-X. https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html
3. Usländer, T., & Batz, T. (2018). Agile service engineering in the industrial internet of things. *Future Internet, 10*, 100. https://doi.org/10.3390/fi10100100
4. Cockburn, A. (2001). *Writing effective use cases*. Addison-Wesley.
5. Platform Industrie 4.0: CCM Webinar, 2020. https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/Webseminar-Collaborative-data-driven-business-models.pdf?__blob=publicationFile&v=8
6. Fraunhofer IOSB (Ed.) (2020). *IIC testbed smart factory web*. https://www.smartfactoryweb.eu
7. IDS Association. (2019, November). *Usage control in the international data spaces*. Position paper of the IDSA, Version 2.0. Accessible at https://www.internationaldataspaces.org/wp-content/uploads/2019/11/Usage-Control-in-IDS-V2.0_final.pdf
8. Hillermeier, O., Punter, M, Schweichhart, K., & Usländer, T. (Eds.). *Data sovereignty - Critical success factor for the manufacturing industry*. Position Paper of the IDS-Industrial Community Accessible at https://internationaldataspaces.org/download/21213/
9. Usländer, T. (Ed.). *Data sovereignty – Requirements analysis of manufacturing use cases*. Position Paper of the IDS-Industrial Community. Accessible at https://internationaldataspaces.org/download/32789/