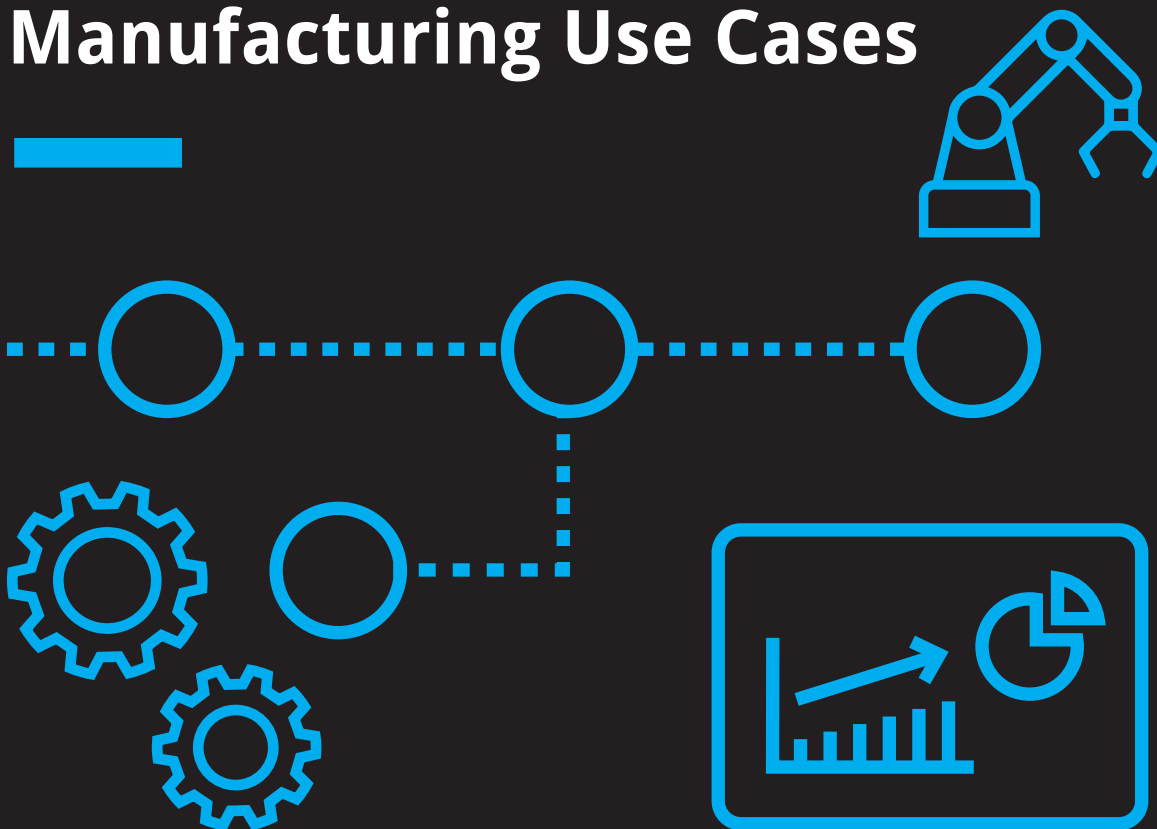**Position Paper | Version 1.0 | May 2022**

Data Sovereignty – Requirements Analysis of Manufacturing Use Cases

- ● Position Paper of members of the IDS Association and of the IDS-Industrial Community
- ○ Position Paper of bodies of the IDS Association
- ○ Position Paper of the IDS Association
- ○ White Paper of the IDS Association

Table of Content

List of figures

1   Motivation

The increasing digitization in the manufacturing industry within and between production companies raises the question of secure and interoperable data sharing between companies in virtual enterprises or between enterprises that work together for joint businesses. Although there is a wish to share data, there is a clear request to keep the control over the usage of data by the distributing entity throughout the whole usage phase of that data by other entities. However, data sovereignty and especially data usage control is a complex and multi-faceted aspect of data sharing infrastructure and difficult to enforce in a truly distributed environment. Hence, there is a need to analyze the concrete needs for data usage control and to set priorities motivated by user requirements.

This paper follows a use case driven approach to reveal a structured and prioritized set of requirements on a conceptual level, abstracting from the options and constraints of underlying technology and operational infrastructures.
Three reference use cases for smart production systems are used for this analysis:

1. Collaborative Condition Monitoring (CCM)
2. Smart Factory Web (SFW)
3. Evaluation of the Impact on UN Sustainability Development Goals (SDG)

Based on these three reference use cases, several sub-use cases are derived which serve to study the requirements needed on data sovereignty including access control, data usage monitoring and control as well as data provenance tracking.

By gathering requirements derived from use cases, this position paper contributes to the issue of how to unify the architectural models of the Platform Industrie 4.0 (RAMI 4.0) and the International Data Spaces (IDS-RAM).

The Asset Administration Shell (AAS) as one core concept of the RAMI 4.0 is currently being standardized on international level in the IEC TC65 Industrial-Process Measurement, Control and Automation as IEC CD 63278-1. On the one hand, the AAS offers a unified and standardized information model that allows data to be securely shared across industries while covering the whole life cycle of a product. However, on the other hand, the involved parties in data sharing have a high demand in establishing rules on how their data is used even after granting access. The IDS-RAM provides means for such a data access and usage control. As a consequence, a way must be found such that both architectural models can coexist with each other, especially in the context of the emerging GAIA-X data sharing infrastructure upon which both architectural models are mapped.

2   Data Spaces Context

The development of data spaces and their governance is significant as the European data economy continues to grow rapidly – from 301 billion euros (2,4 % of GDP) in 2018 to an estimated 829 billion euros (5,8 % of GDP) by 2025[1].

In February 2020, the European Commission published the **European Strategy for Data**[2], aiming at creating a single market for data to be shared and exchanged across sectors efficiently and securely within the EU. This strategy enforces the European data economy following European values of self-determination, privacy, transparency, security and fair competition. The rules of accessing and using data must be fair, clear and practicable. The EU Strategy for Data and the Data Governance Act are essential cornerstones of this evolution, which will lead to a new organization of digital market forces.

The **Data Governance Act** is proposing a two-tier governance structure:

1. a governance entity required for each data space, and
2. an overall governance organization concerned with all common aspects of data space interoperability and data sovereignty, thereby creating the de-facto 'soft infrastructure'.

This position paper aims at supporting the fundamentals of such data spaces and the expectations to meet European standards and viewpoints on data sovereignty. It aims at deriving user requirements on data access and usage control to be met by building blocks of a data space infrastructure and its governance.

Among the most recent endeavors on setting a common ground to establish successful European Data Spaces it is worth to mention the position paper "Design Principle for Data Spaces" [3] developed within the Horizon 2020 project "OPEN DEI Aligning Reference Architectures, Open Platforms and Large-Scale Pilots in Digitising European Industry", under the coordination and leadership of the International Data Spaces Association (IDSA). It embodies a collaboration of more than 40 data spaces and industrial domain experts representing more than 25 organizations from thirteen Horizon 2020 projects and related initiatives, representing the four main sectors of manufacturing, energy, agri-food and healthcare.

The OPEN DEI position paper presents some convergence pathways on how to sustainably establish data spaces. Sustainable data spaces leverage their economic potential in the long run considering functional, operational and legal agreements, asking for new technical standards which together provide the foundation for interoperability across data spaces, steered by the market developments which will be voiced and prioritized by the market participants.

Furthermore, it raises the necessity to harmonize common aspects in every data space into a software infrastructure to enable users (citizens, businesses, governments) to stay in

---

[1] https://datalandscape.eu/sites/default/files/report/D2.9_EDM_Final_study_report_16.06.2020_IDC_pdf.pdf
[2] https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf
[3] https://design-principles-for-data-spaces.org/

control of their data even across different sectors and applications (i.e., across different data spaces).

The Horizon 2020 **AI REGIO**[4] project made a deep study on Ethics Assessment and Data Management Strategy. The main result is that a holistic approach is desirable in such a contest, adopting in a coherent way the regulatory framework for deriving the legal and ethical requirements and for defining guidelines on how to cope with the identified boundaries and constrains. Such approach entails Ethics, Fairness, Privacy and Security by design. Among them it is worth to highlight, in the context of such document, the relevance of fairness and privacy by design.

Starting with the Fairness dimension of the approach, the so-called "Fairness Principle" is mentioned by the European General Data Protection Regulation (GDPR) itself, besides other principles such as the "Lawfulness and Transparency Principle" (Art. 5[5], c. 1 a). The concept of fairness, which might have different interpretations, refers to loyalty and good faith to be respected in all the steps of any personal data processing, but in the industrial domain we can even extend such definition to non-personal data: it requires that data must be used in a fair way. Any handling that is unduly detrimental, unexpected or misleading to the individuals/organizations concerned or that could have adverse impact on them is not allowed. The "**Fairness by Design**" is considered as a straightforward requirement to ensure privacy and real control over their data, as well as their well-being and empowerment.

On the other hand, "**Privacy by Design**"[6] addresses the design process of the technological artefacts as well as the business processes, relying on the idea to put privacy principles into such process since the very beginning and throughout the whole process. The GDPR incorporates such approach and also includes the Privacy-by-Default principle, seeking to deliver the maximum degree of privacy by ensuring that personal data are automatically protected, "by default", without the need of any action from the individual.

The initiation of **GAIA-X**[7] by German and French government officials in 2020 and the subsequent founding of the GAIA-X AISBL in 2021 in Belgium by 22 companies has ignited interest in and accelerated the development of decentralized, federated data technology as well as first services called data spaces using such technology. For example, an early, prominent example of data space technology is the IDS-RAM (5).

GAIA-X enables federations to create an interconnected, provider-neutral data infrastructure that supports secure data storage (data at rest), sovereign data exchange as well as the possibility to use data and services collaboratively, autonomous data sharing and for the collaborative use of data and services. Each company decides for itself where its data is stored, by whom and for what purpose it may be processed. The privacy classification and use restrictions desired by the data producer must be guaranteed. One potential way of categorizing data in this way could be: public, private, semi-public.

GAIA-X has the potential to lay the basis for a marketplace for monetizing operational data within industrial value networks. At the same time, it can provide incentives for stakeholders to share data. On the one hand, GAIA-X shall support portability, i.e., the ability to port a

---

[4] https://www.airegio-project.eu/
[5] https://gdpr-info.eu/art-5-gdpr/
[6] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
[7] https://www.gaia-x.eu

customer's business from one cloud infrastructure to another (no vendor lock-in), on the other hand, it shall support interoperability between several cloud infrastructures. As there is an overlap in objectives and functionality, GAIA-X and IDS concepts and technologies should be harmonized.

Another area that drives development and adoption of data spaces is the automotive and mobility sector. Examples include the **Mobility Data Space**[8] launched by the German government (6) as well as the industry-lead **Catena-X automotive network**[9] that is utilizing a government funded project with 28 partners, including leading automakers and tier-1 suppliers, to develop a data space as central and integral component of an operating system for a data driven value chain. This network operating system will be designed to enable innovative and much needed applications that require data chains across multiple organizations, such as CO_2 footprint proof and parts traceability. Another aspect of Catena-X is its built-in international dimension. For one, the automotive industry is a global one with international supply chains. For another, internationalization has been explicitly recognized with dedicated expansion activities in the Catena-X project. Furthermore, Catena-X has institutionalized an ongoing working relationship with the Gaia-X AISBL to ensure Gaia-X compliance of the Catena-X technology stack as well as helping Gaia-X AISBL better understand industry and implementation specific considerations.

The importance of the data spaces and their governance is recognized not only in Europe but also in other regions. The Society 5.0 concept brought up by Japan pursues a human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyberspaces and physical spaces. Society 5.0 connects and analyzes data from various stakeholders in cyberspaces, creating feedback to the physical spaces and solving previously unsolvable social issues. Data space development is central to such value-creating activities through trusted data exchange.

---

[8] https://mobility-dataspace.eu
[9] https://catena-x.net/en

3   Methodology

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) (1)(2). As illustrated in Figure 1, an agile approach is recommended to reduce the conceptual and terminological gap between the views of the thematic experts (typically industrial, mechanical and/or electrical engineers) and the IT experts (typically computer scientists). Driven by the business strategy, the thematic experts express their functional and non-functional requirements about the system's behavior and characteristics, whereas the IT experts "answer" in terms of (mostly technical) system capabilities and service registries. Usually, both descriptions cannot be matched without additional, tedious discussions and additional explanations.
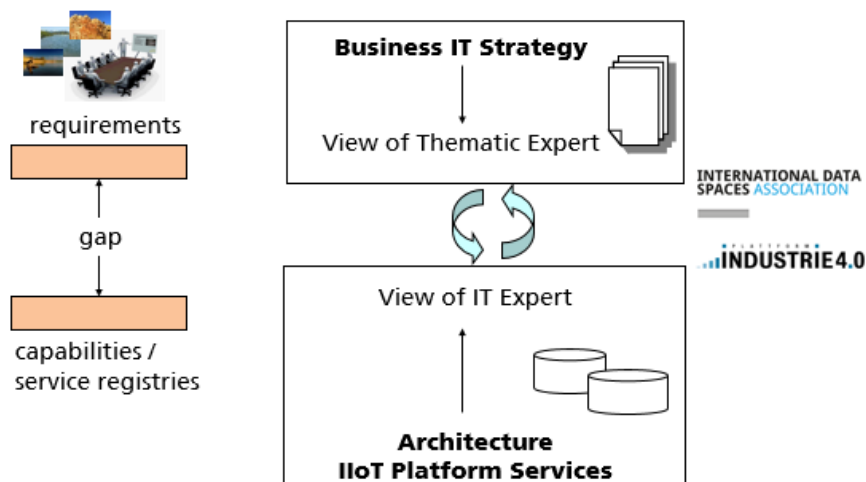
Figure 1: Mapping of requirements in IoT platform environments

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

When considering and analyzing the requirements for data sovereignty in case of scenarios spanned by the three reference use cases specified in section 4, one has to distinguish between the classical aspects of access control (to data and operations) and data usage control.

According to (3), access control restricts access to resources. The term authorization is the process of granting permission to resources. Several access control models exist, such as

- Discretionary Access Control (DAC),

- Mandatory Access Control (MAC),

- Role-based Access Control (RBAC), and

- Attribute-based Access Control (ABAC).

Although such a plethora of access control models exists, RBAC and ABAC are most commonly used.

Usage control is an extension to traditional access control (3). After access to data and operations has been permitted, the question remains as to what happens to the data after access and delivery (as part of operation results). Hence, usage control is about the specification and enforcement of restrictions regulating what may happen to the data and what must not happen. Usage control is concerned with requirements that pertain to data processing (obligations), rather than data access (provisions) as illustrated in Figure 2. In general, usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management.
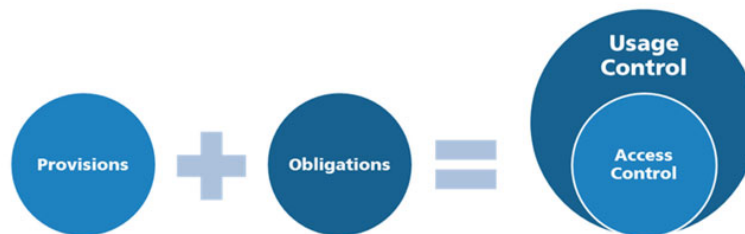
Figure 2: Usage control as an extension to access control

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 a subset of the list of obligations proposed by (3):

- **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.

- **Anonymization by aggregation:** Data on assets 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 on assets which allows an identification must be replaced by an adequate substitute in order to guarantee that individuals cannot be de-anonymized based on the data.

- Note: Originally, these obligations have just been postulated for personal data, i.e., data that is related to a human with a personal identification. In this position paper, we extend this consideration to asset data in general, being human or machine data, assuming that also machines will be considered as juridical person in future with rights and obligations.

- **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.

Furthermore, we consider the obligations on **data provenance tracking**. According to (3), data provenance tracking is closely related, but also complementary to distributed data usage control. It has its origins in the domain of scientific computing, where it was introduced to trace the lineage of data. Data provenance tracking thereby allows finding out when, how and by whom data was modified, and which other data influenced the process of creating new data items.

In general, these obligations should be applicable to any volume of data from small to **big data**. Big Data means data with a high volume, high variety, veracity or velocity, coming either from one data provider or several providers working in a collaborate environment and should support the corresponding technologies/frameworks (e.g., Spark & Hadoop). As a consequence, related technologies to realize the obligations shall be scalable from small to big data.

4 IDS-Industrial Reference Use Cases

Figure 3 illustrates three reference use cases and their major sub-use cases that are described and analyzed in this position paper as part of the task force work in the IDS-I community.
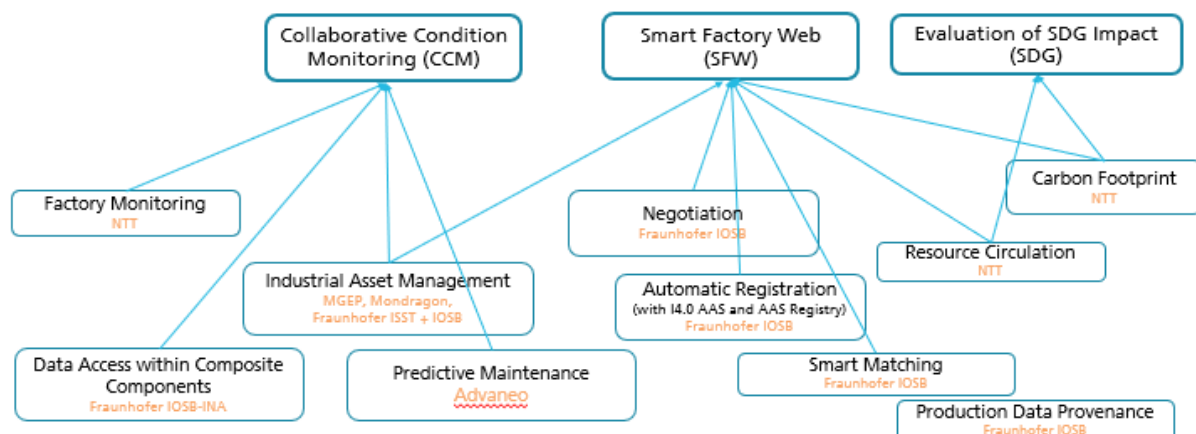

Figure 3: IDS-Industrial Reference Use Cases

4.1   Collaborative Condition Monitoring (CCM)

The reference use case Collaborative Condition Monitoring (CCM[10]) was defined by the German Platform Industrie 4.0 (8) as it is both driven by practical needs of industrial production plants and requires an open, integrated solution that responds interoperability, IT security and data sovereignty demands based upon Industrie 4.0 concepts such as the Asset Administration shell (AAS). CCM Business models are described in (9).

The manufacturer of an automation component would like to access the operational data pertaining to one of their products, which is installed in a machine operated by a third company. Collecting data on the machine condition on a permanent basis supports the manufacturer in optimizing the safety and efficiency of both their component and the entire machine.

This very simple constellation occurs frequently in industrial business relations. It does however, entail a number of questions e.g. Who is the owner of the component manufacturer's data and who is entitled to access it for what purpose? How can data be monetized? Is the data available in a standardized format?

Issues of this nature are currently being resolved bilaterally along a defined value chain. However, the data of interest to the manufacturer is not available in aggregated form across various operators.

This renders it impossible to scale up across value-creation networks.

In order to be able to collaborate on condition monitoring (i.e., the continuous aggregation, analysis and presentation of operational and condition data by means of sensors), the manufacturer and the operators need a trusted data sharing infrastructure, shared rules on cross-company authentication as well as access control.

4.2   Smart Factory Web (SFW)

The Smart Factory Web[11] aims to set up a web-based platform to allow factories to offer production capabilities and share resources to improve order fulfilment in a much more flexible way than is currently possible with available technology. The Smart Factory Web seeks to provide the technical basis for new business models, especially for small lot sizes, with flexible assignment of production resources across factory locations. In particular, this testbed is designed as a step towards establishing an open marketplace for manufacturing where one can look for factories with specific capabilities and assets to meet production requirements. Factories offering those capabilities can then register to be located and participate in the marketplace.

This requires up-to-date information about the capabilities and status of assets in the factory. The characteristics of the products, e.g., availability, quality and price, provide a basis for possible negotiation between competing offers.

---

[10] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Artikel/UseCases/collaborative-condition-monitoring.html
[11] The Smart Factory Web system and further media material (podcasts, publications, videos, …) is accessible at https://www.smartfactoryweb.de.

International standards such as OPC UA and AutomationML as well as Industrie 4.0 and International Data Spaces (IDS) specifications are applied to link factories into the Smart Factory Web in order to provide information about the factories in a standardized and trusted way. Originally started as a testbed of the Industrial Internet Consortium (IIC) with the Korean research partner KETI, it has since then attracted global IT players such as Microsoft and SAP to join and to jointly leverage commercial business cases.

An overview description about the requirements, the architecture and usage scenarios of the Smart Factory Web is provided in (4).

4.3   Impact on the UN Sustainability Development Goals (SDG)

The need for building a sustainable society is growing globally. In 2015, the United Nations General Assembly adopted the Sustainable Development Goals (SDGs), which define concrete action goals for sustainable development and are intended to be achieved by the year 2030. Also, following the Paris Agreement adopted at the 21st session of the Conference of the Parties to the United Nations Framework Convention on Climate Change (COP 21) in 2015, and the Special Report on Global Warming of 1.5°C published in 2018 by the Intergovernmental Panel on Climate Change (IPCC), concrete actions have begun to reduce greenhouse gas emissions to net-zero by 2050 in order to keep temperature increase below 1.5°C.

Various efforts are accelerating around the world toward the realization of a low-carbon and resource circular society. In the manufacturing industry the government, investors, shareholders, customers, etc. need to evaluate in addition the degree of contribution to social issues. This requires to disclose information along the entire value chain about the impact on the environment and the society that constitutes the business they run.

For example, as represented by initiatives such as the SDG Impact Standards, the Greenhouse Gas Protocol Scope 3, the Science Based Targets, and the recommendations on climate-related financial disclosures of the Task Force on Climate-Related Financial Disclosures (TCFD), formulation of evaluation criteria for information disclosure has begun in various countries and regions. Also, in order to meet this demand, product manufacturers need to obtain various data from the companies that constitute the value chain, and the need for data sharing between companies is growing.

However, since these data contain information important for competition for each company, data providers have a need to limit the scope of data disclosure to specific trusted companies with which they have contracts, to limit the purpose of use and period of use of the data, and to detect violators in case of unauthorized use. This is because information such as trade secrets (sensitive production data) and data generated during operation which can be used to estimate production capability need to be protected from other competitors in the market. Data must be provided safely, taking into consideration the format of information, disclosure scope, disclosure conditions, verification means, etc., based on international rules, laws and regulations, and contracts. Also, when sharing data, we need to be able to flexibly meet the diverse demands of the entire value chain, such as connection methods suitable for each industry and corporate system, and data formats and verification methods that comply with the rules of each government. In addition, it is necessary to establish a unified standard for the meaning and interpretation of data so that all companies in the value chain can share accurate information.

Therefore, this reference use case realizes secure and trusted data sharing across multiple companies that constitute the international value chain. This reference use case makes the business contributions to the achievement of SDGs comparable by collecting, evaluating, scoring, and indexing data on the use of human resources, goods, money and energy (quantity and quality) through secure and trusted data sharing across international industrial value chain. Sharing data implies the necessity to specify, control, and limit the format, disclosure scope, disclosure conditions, verification means, etc. of information based on international rules, laws, regulations, and contracts, features such as access control, usage control, and data provenance are required.

There are various indicators of SDGs, but this use case targets the measurement of the impact on the reduction of greenhouse gas emissions and the realization of resource recycling. Since there are cases where resource recycling efforts, such as paper recycling, involve excessive greenhouse gas emissions, we will make it possible to confirm such situations by evaluating both indicators. In the future, we will realize an "SDGs certification service" in which a third-party organization comprehensively evaluates and scores the achievement level of SDGs of each business based on data, aiming to expand to various other SDGs indicators such as protection of human rights and elimination of inequality, and to apply to the entire value chain including non-manufacturing industries.
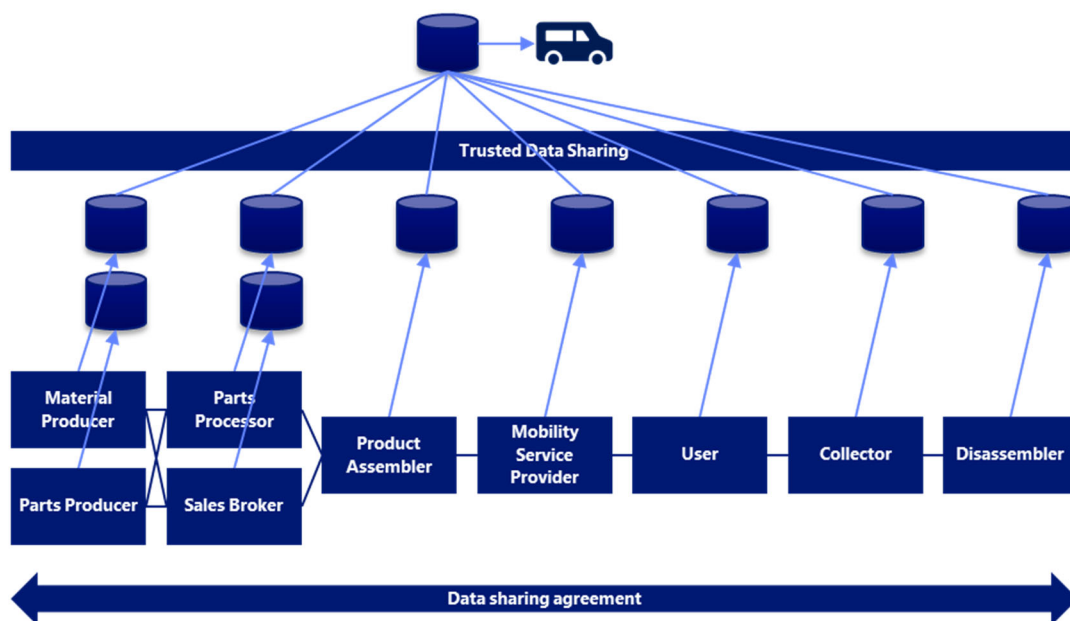

Figure 4: Evaluation of the SDG Impact in Industrial Value Chains

The overall reference use case is illustrated in Figure 4. It is structured into the following sub-use cases:

- Visualization of Carbon Footprint

- Visualization of Resource Circulation

- Usage Control for Data Analysis Apps

- Smart Factory Web Negotiation (Fraunhofer IOSB)

5   Requirements on Access and Usage Control

Following the methodology described in section 3 the reference use cases, introduced above and broken down to several sub-use cases, were analyzed in detail. The use case descriptions including their requirements on access and usage control are contained in Annex B. i.e. section 11. The result is illustrated below in Figure 5. It shows the number of mentions of the access and usage control obligation for the individual workflows in the sub-use case descriptions, following the methodology described in section 0. Each mention in a use case description means that there is a need for a capability in the underlying infrastructure for the given obligation.
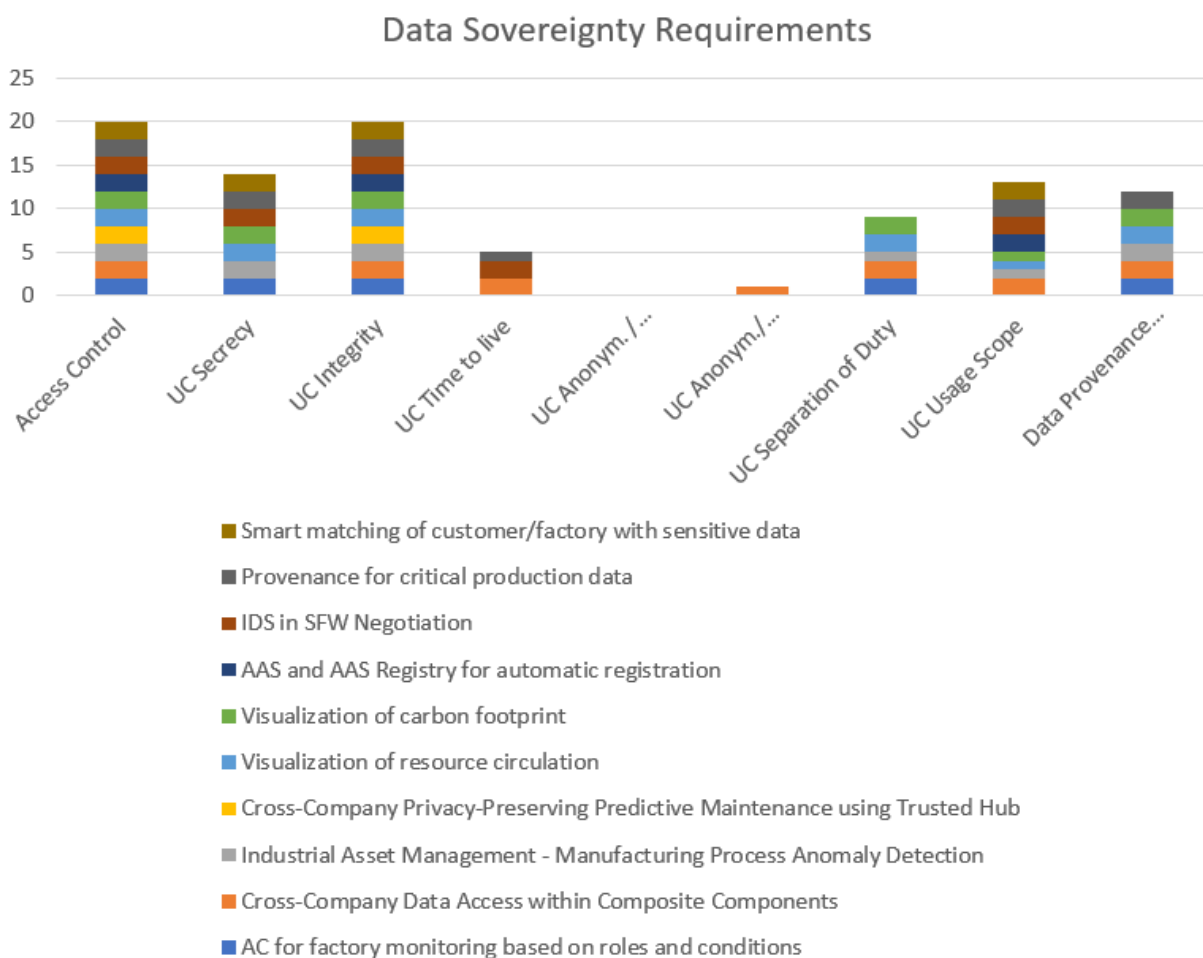
Figure 5: Data Sovereignty Requirements - Result of the Use Case Analysis

The spread of the results provides hints to the designers and development managers of data space infrastructures which of the obligations have the highest priority to be offered as capabilities. This analysis follows the assumption that the AC/UC requirements of the three reference use cases including their sub-use cases are representative for the set of all relevant use cases. A four-priority classification scheme of obligations is chosen:

- Urgent obligations (76-100% coverage)

  - **AC (Access control) (100%)**: restriction of access to resources

  - **UC integrity (100%)**: critical data must not be modified by untrusted nodes as otherwise their integrity cannot be guaranteed anymore

- High-priority obligations (50-77% coverage)

  - **UC secrecy (70%)**: Classified data must not be forwarded to nodes which do not have the respective clearance.

  - **UC Usage scope (65%)**: Data may only serve as input for data pipes within the connector, but must never leave the connector to an external endpoint.

  - **Data provenance tracking (60%)**: finding out when, how and by whom data was modified, and which other data influenced the process of creating new data items.

- Medium-priority obligations (25-49% coverage)

  - **UC Separation of duty (45%):** Two data sets from competitive entities must never be aggregated or processed by the same service.

  - **UC Time to live (25%):** A prerequisite for persisting data is that it must be deleted from storage after a given period of time.

- Low priority obligations (0-24% coverage)

  - **UC Anonymization by aggregation (5%):** Data on assets 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.

  - **UC Anonymization by replacement (0%):** Data on assets which allow an identification must be replaced by an adequate substitute in order to guarantee that individuals cannot be de-anonymized based on the data.

6   Conclusions

The first position paper of the IDS-Industrial Community (7) published in April 2021 has formulated and justified the hypothesis that data sovereignty is a critical success factor for the manufacturing industry. In its call for action it was requested, among others,

- to deepen the knowledge on data sovereignty,

- to analyze relevant scenarios, the involved players, and the components that are necessary to offer data sovereignty capabilities, as well as

- to discuss the usage of data sovereignty concepts with business and engineering partners.

The purpose of this second IDS-I position paper is to contribute to this discussion by the analysis of requirements and by breaking down what is meant by data sovereignty in terms of access control, usage control and data provenance tracking. Usage control is the main value proposition of IDS-compliant data sharing infrastructures, but rather difficult to enforce in its full scope. Therefore, for the requirements analysis carried out in this position paper, usage control has been broken down into distinct obligations following the scheme defined in (3).

The scenarios that were analyzed are taken from three prominent reference use cases being globally discussed:

1. Collaborative Condition Monitoring (CCM)
2. Smart Factory Web (SFW)
3. Evaluation of the Impact on UN Sustainability Development Goals (SDG)

The analysis of further reference use cases, e.g. the tendency towards individualized and even personalized production, i.e., a lot size of 1, may be worthwhile.

The result of the analysis shows that besides access control it is the requirement of preserving data integrity across value chains that is of utmost importance. Next, it is highly important keep the secrecy and to observe the usage scope of the data, i.e., to keep the data within the connector-defined data space, one of the most prominent value propositions of the IDS-RAM. Furthermore, the capability to track the data provenance has high priority, too, followed by the need to separate duties and to delete data items after a given period of time. Finally, it is argued that the anonymization of data is of low priority, at least in the manufacturing industry.

The objective of this classification is to set priorities when thinking about the design and implementation of data sharing infrastructures for the manufacturing industry in projects of the manufacturing domain of GAIA-X. As an outlook, it may be useful to think about a classification of data associated to assets, e.g., open data, anonymized data, public data and private data (for example without personal data), and to link them to the data sovereignty capabilities discussed in this position paper.

Furthermore, it has to be evaluated how the emerging European Data Governance Act (DGA)[12] and the tendency towards data altruism will also influence the behavior of the companies in the industrial production domain.

However, becoming more sovereign over your own data is not a technical exercise only. Regulation, way of working and technical solutions shall be integrated in one overall approach. IDS give an answer for the current data sovereignty issues. Within the Industrie 4.0 domain data sovereignty is key to improve the way of collaborative working in supply chains if and only if access and usage control is possible for each of the players in the manufacturing supply chain, as it is, for instance, discussed in the Manufacturing-as-service (MaaS) use case of the Catena-X Automotive Network.

All IDS-I Use Cases presented and assessed in this position paper have one thing in common, the creation of data space deployment scenarios and use cases, including a minimal viable data space offering. It has the functionality for deploying the data space capabilities, in a trustful data space ecosystem. As such, the IDS Reference Testbed[13] may be used for new data space deployments, providing the basis for system development and assessment together with data space partners, e.g. on integrating and interacting with the ecosystem of data space partners providing various IDS components and on the development of data apps and services. The IDS Reference Testbed consists of a set-up with open-source IDS components complying to the IDS specifications for establishing connections and communication.

---

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767
[13] https://internationaldataspaces.org/use/reference-testbed

7   Join the IDS-Industrial Community

IDS-I comprises an international community of industrial partners that unites more than 60 organizations from around the world. It is a verticalization community of the International Data Spaces Association (IDSA)[14].

The IDS-I objective is to analyze the mapping of IDS concepts and principles of data sovereignty to the requirements of the industrial sector. In this sense, the mission of the IDS-Industrial Community is:

- 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.

- To map these requirements systematically to the standards, capabilities and recommended technologies of the IDSA and the Platform Industrie 4.0.

- To derive profiles of IDS/Industrie 4.0 specifications that support the requirements in industrial business eco-systems based upon standards and by means of common governance models.

- To validate and demonstrate the applicability of these specifications by means of reference testbeds, e.g. Smart Factory Web[15] and GAIA-X use cases.

- To contribute to the outreach of the IDS architecture and specifications to the community of industrial production and smart manufacturing.

For more information please contact the authors or join the IDS-Industrial (IDS-I) Community by expressing your interest in an email to info@internationaldataspaces.org.

---

[14] https://internationaldataspaces.org/make/communities/
[15] https://www.smartfactoryweb.de

8   Abbreviations

AAS	Asset Administration Shell
ABAC	Attribute-based Access Control
AISBL	Association internationale sans but lucratif
DAC	Discretionary Access Control
DGA	Data Governance Act
GDPR	General Data Protection Regulation
IDSA	International Data Spaces Association
IDS	International Data Spaces
IDS-RAM	International Data Spaces – Reference Architecture Model
MAC	Mandatory Access Control
MaaS	Manufacturing-as-a-service
RBAC	Role-based Access Control
RAMI4.0	Reference Architectural Model Industrie 4.0
SDG	Sustainability Development Goals
SFW	Smart Factory Web
TCFD	Task Force on Climate-Related Financial Disclosures

9   References

(1) Usländer, T.; Batz, T.: Agile Service Engineering in the Industrial Internet of Things. Future Internet 2018, 10, 100. https://doi.org/10.3390/fi10100100

(2) Usländer, T.; Teuscher, A.: Industrial Data Spaces. Chapter in book "Data Spaces" (to be published by Springer Verlag)

(3) Steinbuss, S., IDS Association (Ed.): Usage Control in the International Data Spaces. Position Paper of the IDSA, Version 2.0, November 2019. Accessible at https://www.internationaldataspaces.org/wp-content/uploads/2019/11/Usage-Control-in-IDS-V2.0_final.pdf

(4) Usländer, T.; Schöppenthau, F.; Schnebel, B.; Heymann, S.; Stojanovic, L.; Watson, K.; Nam, S.; Morinaga, S. Smart Factory Web—A Blueprint Architecture for Open Marketplaces for Industrial Production. Appl. Sci. 2021, 11, 6585. https://doi.org/10.3390/app11146585

(5) Otto B., Steinbuss S., Teuscher A., Lohmann S. et al. (2019): IDS Reference Architecture Model (Version 3.0). International Data Spaces Association. http://doi.org/10.5281/zenodo.5105529

(6) Drees, H., D. O. Kubitza, J. Lipp, S. Pretzsch, and C. Schlueter Langdon. 2021. Mobility Data Space – First Implementation and Business Opportunities. Technical Paper ID 909, 27th ITS World Congress

(7) Hillermeier, O., Punter, M., Schweichhart, K., Usländer, T. (Eds.): Data Sovereignty – Critical Success Factor for the Manufacturing Industry. Position Paper of members of the IDSA and of the IDS-Industrial Community. Version 1.0, April 2021. Accessible at https://internationaldataspaces.org/download/21213/ .

(8) Platform Industrie 4.0: Multilaterales Datenteilen in der Industrie - Zielbild am Beispiel des Collaborative Condition Monitoring als Basis für neue Geschäftsmodelle. Publication of the Platform Industrie 4.0, project group CCM, publication in German and English announced for May 2022.

(9) Platform Industrie 4.0: Collaborative data-driven Business Models. Publication of the Platform Industrie 4.0, Accessible at https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/collaborative-data-driven-business-models.html

10   Annex A: Use Case Template

The following use case template is applied in the IDS-Industrial Community.

ID	Unique ID of the use case in a given scope
Name	Name of the use case
Reference use case	[Smart Factory Web, Collaborative Condition Monitoring, Evaluation of SDG Impact, or other…]
Motivation	Textual description of the motivation of the use case
Stakeholders	List of stakeholders involved
Objective	Objective of the use case
Constraints	Constraints to be obeyed
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. …
	
	Note: may have loops and jumps (if … then go to step X)

Postconditions	Describe the situation after the use case was carried out

Requirements	Indicate which, and in which workflow steps, access control (AC) and usage control (UC) requirements are relevant.
	AC: yes/no/conditional (workflow steps x.y)
	UC Secrecy: yes/no/conditional (steps)
	UC Integrity: yes/no/conditional (steps)
	UC Time to live: yes/no/conditional (steps)
	UC Anonymization
	   • by aggregation: yes/no/conditional (steps)
	   • by replacement: yes/no/conditional (steps)
	UC Separation of duty: yes/no/conditional (steps)
	UC Usage scope: yes/no/conditional (steps)
	Data provenance tracking: yes/no/conditional (steps)

Sources	Literature or references
Authors	Name of the authors

11 Annex B: IDS-I Use Case Descriptions

11.1 Collaborative Condition Monitoring

11.1.1 Cross-Company Data Access within Composite Components

ID	CCM-01
Name	Cross-Company Data Access within Composite Components
Motivation	Data Scientists are dependent on high quality, high context and high-volume data, e.g. for an AI-based monitoring of machine components. Not only internal component sensor data is of interest, but also supplementary data points within the machinery hierarchy. The additional data points can help to provide more useful information. It is common that component manufacturers ask for data insights but can only provide a few data sets since they neither know where the components are put into operation nor are they able to collect the data.
Stakeholders	• Component Supplier / Manufacturer • Component Integrator • Operator • Data Scientist
Objectives	The operational data of components and machines should be accessible for all participants. This is only applicable when all participants, especially the factory operator, agree to share the data. The data acquisition and the data exchange itself must met requirements regarding confidentiality, integrity and authenticity. The involved stakeholders must be identifiable and able to establish a trust relationship. The objective of the workflows is to collect data for a temperature sensitive component type.
Comment	Stakeholders can act either as Data Consumer or Data Provider. Naturally, the Operator should be seen as Data Owner during the operation phase, but this can vary due to different possible (data) business models. Owner and Provider do not have to be the same entity.
Preconditions	All stakeholders are uniquely identifiable and can provide trustful information about their roles, intentions and/or relationships.
Workflow A	1. Data Providers publish meta-data about the component type and historicized sensor data. In this case, the Data Providers are multiple Operators.

	2. Data Scientist queries for a specific machine type and filters for sources who can also provide environmental temperature data and energy data. 3. Data Scientist selects and requests data based on metadata. 4. The Data Provider reviews the request and decides whether or not to authorize data access based on the Data Scientist identity and other information attached to the request. 5. If authorized, the Data Consumer collects historicized data.
Workflow B	1. The Component Supplier acquires, historicizes and merges data for his product via a trusted connection to the operating instance. 2. The Component Supplier delivers all data directly to the Data Scientist. 3. Based on attached metadata, the Data Scientist can query supplementary data points from Operators or Component Integrators. 4. The Data Scientist selects and requests data based on metadata. 5. Operators or Component Integrators review the request and decide whether or not to authorize data access based on the Data Scientist identity and other information attached to the request. 6. If authorized, the Data Consumer collects historicized data.
Postconditions	After aggregating data from several components of the same type, the Data Scientist is able to provide data insights, e.g. for a condition monitoring application. The newly created condition monitoring application can be offered to stakeholders to use it directly or to act as a distributor for that application.
Requirements	AC: A.4, A.5, B.2, B.5, B.6 UC Integrity: in general UC Time to live: up to postcondition holds UC Anonymization by replacement: B.1 UC Separation of duty UC Usage scope: A.4, B.5 Data provenance tracking: postcondition
Sources	Collaborative data-driven Business Models (8)(9)
Authors	Bastian Rössl, Fraunhofer IOSB-INA

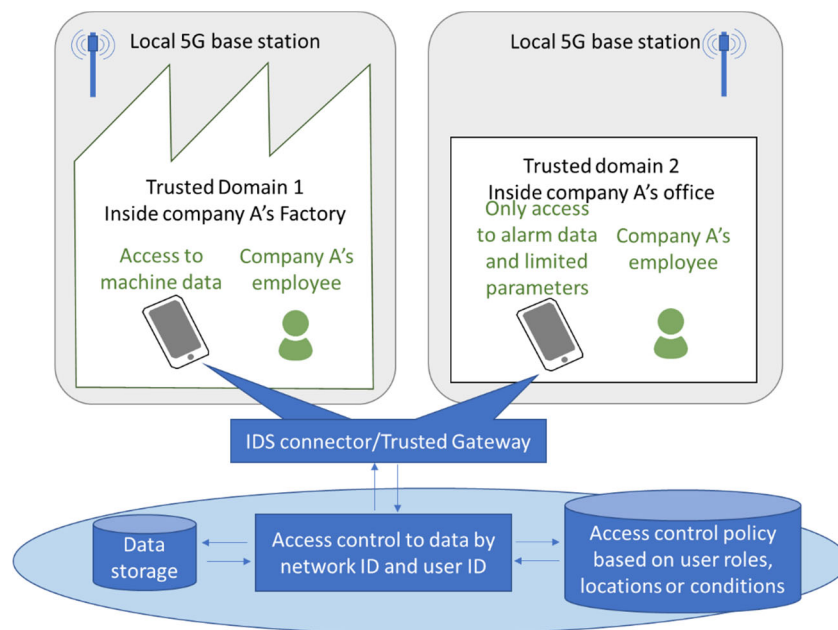### 11.1.2 Factory Monitoring

ID	CCM-02
Name	Data access control for factory monitoring based on roles and conditions
Motivation	To enable industrial data utilization between companies while preserving the data sovereignty of factory data owners
Stakeholders	• Manufacturers • Producers/Machine Tool Builders • Maintenance personnel of machine maker • Factory automation systems/solutions providers • Telecommunications carriers
Objective	To realize network-based data access control with data sovereignty in the industrial data sharing system between companies
Constraints	Data access control and data provenance control require identification information of network facilities such as local 5G networks, internet gateways, wireless networks, or IoT SIM cards of manufacturing machines and devices.
Comment	none
Preconditions	• Manufacturing system provider should be queried about data catalogs of connectors or controllers of manufacturing machines and sensors. • Manufacturers should be queried about policy rules for each factory locations, machines or data class based on conditions such as users' roles or locations via GPS or wireless beacon ID, device ID, network ID or 5G base station ID. • Company A (manufacturer) has a factory and office building. Company A's factory uses multiple machines manufactured by multiple machine tool builders, including company B (machine tool builder). • Company C (computerized numerical controller maker) manufactures control devices of machines used in the product of Company B (machine tool builder). The maintenance personnel of company C maintain the control devices built in the machines at the factory of Company A. • Company A shares data on the related parts of the machine manufactured by company B in order to receive maintenance services from company B and company C. • Company A has different data usage rules depending on the locations such as factories, offices, and outside. Company A divides trusted domains with specific data usage rules according to the usage and role of each location.

	• Since company A, B and C are different companies, their data usage rules and trusted domains are different. • Company A allows company B to access data only about machines manufactured by Company B. Company A allows company B to access limited data remotely, but more detailed data locally. Company A allows company C to access data only about control devices via company B. Company C is allowed to access only limited data remotely, but more detailed data locally. • Company D is a manufacturer which uses Company A's product as parts. • Company E is a manufacturer which produces the materials or parts of company A's product. • Supply chain managers of company D are allowed to access machine operation status data related to the products that will be delivered to company D in company A's factory. • Supply chain managers of company E are allowed to access machine operation status data related to the production lines using materials or parts provided by company E at company A's factory. • This case includes 7 trusted domains with different data usage rules for each location as factory A, office A, outside company A, company B, company C, company D, company E. Communications between these trusted domains must be done through the IDS connector with inter-company agreements. • Though data is managed using AAS of Industrie4.0 inside the factories of each company, but it is not connected across companies by using AAS.

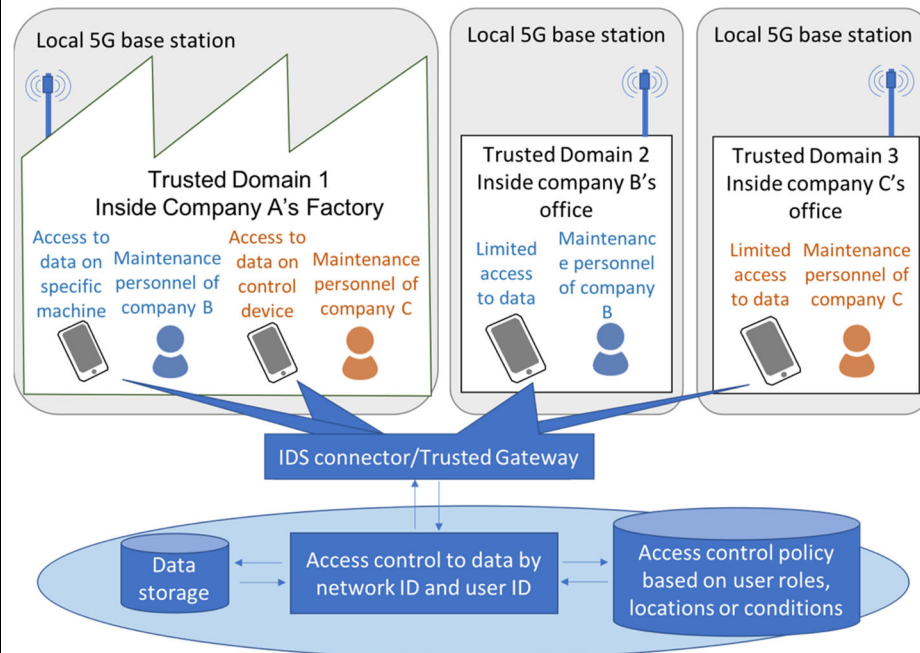| Workflow 1	

Use case of the access control over different trusted domains inside the company

1. Factory managers of company A (manufacturer) add metadata indicating data types, etc. to data generated in their factory. They also decide access control policy of each data types for all trusted domains based on companies, roles, user locations, network ID of display devices, base station ID, or conditions.
2. Trusted domain examples:
   - Trusted domain 1: Inside company A's factory
   - Trusted domain 2: Inside company A's office
3. Policy example:
   - Factory employees inside company A's factory (via registered 5G local base station ID) are allowed to access all machine data and alarm data of company A's factory.
   - Factory employees inside company A's office (via another 5G local base station IDs) are allowed to access only alarm data and limited monitoring parameters.
4. Manufacturing system of company A's factory send machine data to data sharing cloud via IDS connector.
5. Users such as employee of company A request data on machines used in company A's factory and send user information and network information that their display device connects.
6. Required data will be provided to users based on the access control policy set in step 1.
7. Result example:
   - Factory employees of company A inside the factory of company A (via registered 5G local base station ID) are able to access all machine data. |

	8. Request to access data will be refused if conditions such as wireless beacon ID, 5G base station ID or network ID do not match the registered information allowed in the policy set in step 1. 9. Result example: • Company A's employees inside the office of company A (via another 5G local base station ID) can only access alarm data and limited monitoring parameters and cannot access other machine data.

Workflow 2	
	
	Use case of collaborative condition monitoring across multiple companies
	1. Factory managers add metadata indicating data types, etc. to data generated in their factory. They also decide access control policy of each data types for all trusted domains based on companies, roles, user locations, network ID of display devices, base station ID, or conditions.
	2. Trusted domain examples:
	   • Trusted domain 1: Inside the company A's factory
	   • Trusted domain 2: Inside the office of company B (machine tool manufacturer)'s maintenance personnel
	   • Trusted domain 3: Inside the office of company C (computerized numerical controller maker)'s maintenance personnel
	
	3. Policy example:
	   • Maintenance personnel of company B (machine tool manufacturer) are allowed to access data only on machines manufactured by company B and used in company A's factory when they are inside the factory (via registered 5G local base station ID). They are allowed to access more

> limited data such as alarm data and limited monitoring parameters remotely.
> - Maintenance personnel of company C (computerized numerical controller maker) are allowed to access data via company B only on control devices manufactured by company C that is assembled in machines in company A's factory when they are inside the factory (via registered 5G local base station ID). They are allowed to access more limited data such as alarm data and limited monitoring parameters remotely.

4. Manufacturing system send machine data to data sharing cloud via IDS connector. Data can be sent in batches or streams.

5. Data examples:
   - Machine data for predictive maintenance continues to be streamed to the machine manufacturer while the machine is running
   - Data such as blueprints of products are sent in batch every time needed.

6. Users such as maintenance personnel of company B or company C request data on machines used in company A's factory and send user information and network information that the display device connects.

7. Required data will be provided to users based on the access control policy set in step 1.

8. Result examples:
   - Maintenance personnel of company B inside the company A's factory (via registered 5G local base station ID) are able to access data on machines manufactured by company B.
   - Maintenance personnel of company B outside the company A's factory are able to access only limited data such as alarm data and limited monitoring parameters on machines manufactured by company B.
   - Maintenance personnel of company C inside the company A's factory are able to access data via company B only on control devices manufactured by company C that is assembled in machines in company A's factory.
   - Maintenance personnel of company C outside the company A's factory are able to access limited data such as alarm data and limited monitoring parameters via company B on control devices manufactured by company C that is assembled in machines in company A's factory.

9. Request to access data will be refused if conditions such as wireless beacon ID, 5G base station ID or network ID do not match the registered information allowed in the policy set in step 1.

10. Result example:
    - Maintenance personnel of company B cannot access data on machines not manufactured by company B and used in company A's factory.

	• Maintenance personnel of company B outside the company A's factory (via not registered 5G local base station ID) cannot access detailed data except alarm data and limited monitoring parameters on machines manufactured by company B and used in company A's factory. • Maintenance personnel of company C cannot access data on parts of machines not manufactured by company C and used in company A's factory. • Maintenance personnel of company C outside the company A's factory (via not registered 5G local base station ID) cannot access detailed data except alarm data and limited monitoring parameters on control devices manufactured by company C and used in company A's factory.

Workflow 3	
	
	Use case of collaborative condition monitoring across supply chains
	
	1. Factory managers add metadata indicating data types, etc. to data generated in their factory. They also decide access control policy of each data types for all trusted domains based on companies, roles, user locations, network ID of display devices, base station ID, or conditions.
	2. Trusted domain examples:
	  • Trusted domain 1: Inside the company A's factory
	  • Trusted domain 2: Inside the office of company D (manufacturer using company A's product as parts)
	  • Trusted domain 3: Inside the office of company E (Supplier of the materials or parts of company A's product)
	3. Policy examples:

	• Supply chain managers of company D are allowed to access machine operation status data related to the products that will be delivered to company D in company A's factory.
	• Supply chain managers of company E are allowed to access machine operation status data related to the production lines using materials or parts provided by company E at company A's factory.
	4. Manufacturing system of company A's factory send machine operation status data to data sharing cloud via IDS connector.
	5. Users such as supply chain managers of company D or company E request data on machines related to the specific production lines of company A's factory and send user information and network information that the display device connects.
	6. Required data will be provided to users based on the access control policy set in step 1.
	7. Result examples:
	    • supply chain managers of company D inside the company D's office (via specific 5G local base station ID) are able to access machine operation status data related to the products that will be delivered to company D in company A's factory.
	    • supply chain managers of company E inside the company E's office (via specific 5G local base station ID) are able to access machine operation status data related to the products that uses materials or parts provided by company E in company A's factory.
	8. Request to access data will be refused if conditions such as wireless beacon ID, 5G base station ID or network ID do not match the registered information allowed in the policy set in step 1.
	
	9. Result example:
	    • supply chain managers of company D outside the company D's office (via specific 5G local base station ID) cannot access machine operation status data in company A's factory.
	    • supply chain managers of company E inside the company E's office (via specific 5G local base station ID) cannot access machine operation status data related to the products that don't use materials or parts provided by company E in company A's factory.

Postconditions	• Factory managers can analyze machine data from different locations or countries and utilize data for production control or quality management, etc. • Factory managers can limit data access period for machine manufacturers or supply chain managers. (e.g. The precise data on specific machine failure is shared to the machine maker only for a limited time of repair.

	• Factory managers can limit data access period for supply chain managers. It is possible to prove the source of each data (where the data was generated) until data in the supply chain expires. • Machine maintenance personnel from different companies can repair machine quickly at customer factory. • Machine Tool Builders can get data for improving their machine tool products or predicting machine tool failure and providing predictive maintenance. • Producers can integrate third-party data provided under their access control policy. • Supply chain managers can use machine operation status data of their supplier's or customer's production lines related to their own company's products for automatically adjusting supply amount or production plan in their factory or changing contracts.
Requirements	AC: W1.1, W1.4, W2.1, W2.4, W3.1, W3.4 UC Secrecy: W1.all, W2.all, W3.all UC Integrity: W1.all, W2.all, W3.all UC Separation of duty: W1.1, W1.4, W2.1, W2.4, W3.1, W3.4 Data provenance tracking: W1.2, W1.4, W2.2, W2.4, W3.2, W3.4
Sources	
Authors	Koki Mitani, Yui Saito (NTT Corporation)

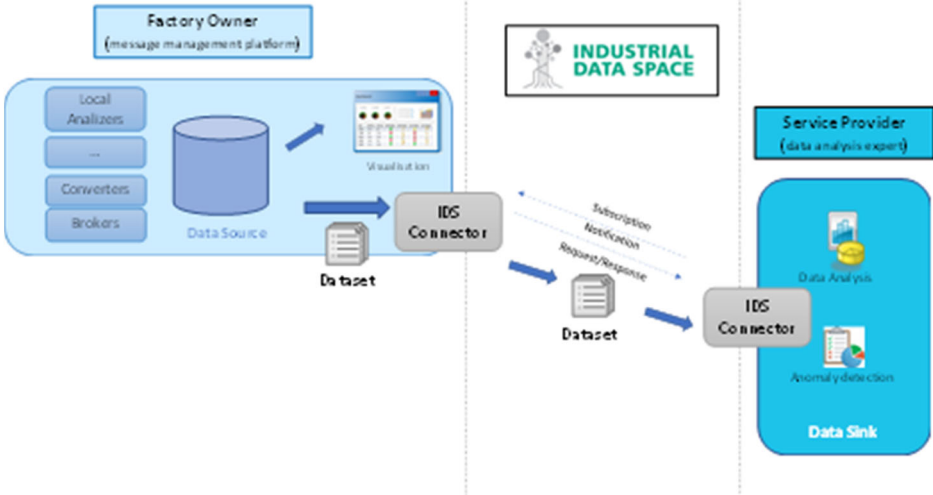### 11.1.3 Manufacturing Process Anomaly Detection

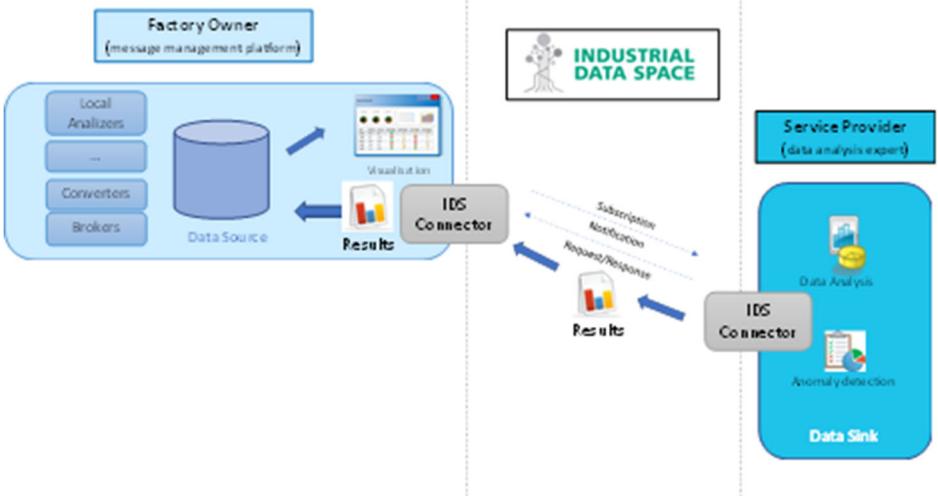| ID	CCM-03
Name	Industrial Asset Management - Manufacturing Process Anomaly Detection
Motivation	Devices in a production plant collaborate in producing goods in a process. They work according to a given sequence of tasks. The sequence is repeated many times to comply with the production requests. During production, those devices or assets produce messages related to 1. parameters measured by the machines involved, and 2. process data collecting timestamps for production process events (start time, end time, time in a machine, time in stock …). These data are collected and used to monitor and evaluate industrial processes. Performance is satisfactory when parameter values are within certain thresholds. Results might even be valid when some of those values are above/below the thresholds. Faulty products might

	appear at any time. In those cases, it is essential to determine the cause for defective products. Process data can be analyzed to detect anomalies that might impact on the final result. Factory owners like to separate production data analysis from anomaly detection analysis. The technologies and tools for anomaly detection analysis are not always available within the company and 3rd party experts and algorithms are required to analyze those data. The IDS platform could assure that those data is used only by the desired company agreeing to the terms established in the contract.
Stakeholders	• Factory owner • Data analysis expert
Objective	To demonstrate successful data sovereignty for critical production data to mitigate trust issues between unknown partners
Comment	---
Preconditions	 Company A (Factory Owner) collects information from different industrial processes. The information is collected in the form of messages in a platform (message manage platform). Exchanged messages hold information about processes, events or logs. Messages follow a common format based on AAS to transport values, files or events. Messages are stored for monitoring, analysis and anomaly detection. Company A monitors processes with its own software applications but needs support from third parties to detect anomalies from the information collected.

	Company B provides data analysis and anomaly detection services based on their algorithms.
	All companies are uniquely identifiable and can provide trustful information about their roles, intentions and/or relationships.
	They rely on IDS for data exchange.
	Blocks of messages needs to flow from data source to data sink through the IDS infrastructure. Company A needs to publish those blocks of messages with a frequency or for a given period of time.
	Company B can collect blocks of messages and by applying its algorithms obtain results related to anomalies.
Workflow A	 1. Data/factory owner (data source) selects a period of time and puts together all the messages in that period in a file or dataset. 2. Data/factory owner and consumer (Data Sink) use certificates issue by the IDS certificate authority and they agree on the contract to exchange data. 3. The Data Sink subscribes through its IDS Connector to the resource announce by the Data Source IDS Connector. 4. The Data Source produces a dataset in the IDS connector installed in its premises. 5. The provider IDS Connector notifies the other end about the availability of a resource update. 6. The dataset flows from the Data Source to the Data Sink once requested. 7. Usage Policies are checked so that the dataset can only flow into the IDS connector of the consumer.

Workflow B	 1. Service Provider detects anomalies from latest dataset using its algorithms. 2. Data/factory owner and service provider use certificates issue by the IDS certificate authority, and they agree on the contract to exchange data. 3. Factory Owner subscribes through its IDS Connector to the resource announce by the Service Provider IDS Connector. The resource is associated to the results obtained after running the anomaly detection algorithm. 4. The Service Provider produces the results and updates the resource associated in the IDS connector installed in its premises. 5. The Service provider IDS Connector notifies the other end (Factory Owner) about the availability of a resource update (new results). 6. The results flow from the Service Provider to the Factory owner once requested. 7. Usage Policies are checked so that the results can only flow into the IDS connector of the factory owner.
Postconditions	Data is hidden and can only be used by the App specified by the consumer
Requirements	AC: A.2, A.3, A.5, A.6, A.7, B.2, B.3, B.5, B.6 and B.7 UC Secrecy: in all steps in A and B UC Integrity: in all steps in A and B UC Separation of duty: yes UC Usage scope: yes((7) Data provenance tracking: A.1 and B.1
Sources	QU4LITY European Project Co-funded by the Horizon 2020 Framework Programme of the European Union Under grant agreement No 825030 Use Case Participants: Fagor Arrasate, Danobat Group, Ideko, Ikerlan, Mondragon Corporation, ISST Fraunhofer and Mondragon University
Authors	Felix Larrinaga, Jon Legaristi, Javier Cuenca, Alain Perez – MGEP, Michel Iñigo - MONDRAGON,

	Marcel Altendeitering, Stephan Duebler, Ronja Quensel, Fraunhofer ISST

11.1.4 Cross-Company Privacy-Preserving Predictive Maintenance using Trusted Hub

ID	CCM-04
Name	Cross-Company Privacy-Preserving Predictive Maintenance using Trusted Hub
Motivation	To train a holistic Predictive Maintenance (PdM) model to forecast the failure of a specific component/machine in future, data scientists and solution providers need to have access to high quality, high context, and high-volume Machine Generated Data (MGD) ideally from multiple factories operated by different operators. Note that the process of combining and aggregating various data sources results in new insights, and better PdM models. Although operators, as the owner of MGD, understand the benefits of collaboration and data sharing, they might be reluctant to share raw MGD, even using traditional IDS protocol, because of the potential risks of leakage of highly privacy-sensitive information. This causes a series of significant challenges to fully benefiting from the power of Artificial Intelligence and Machine Learning. To address this challenge, a novel Privacy-Preserving Machine Learning (PPML) framework, known as Trusted Hub, will be integrated into IDS protocols to enable collaborative data analysis, just as if there is a shared database between participants without ever revealing raw privacy-sensitive data. In other words, sensitive data sources held by multiple participants (operators) can be linked together in a secure manner while parties gain no additional information about each other's sensitive data.
Stakeholders	• Component Suppliers • Machine Suppliers • Integrators • Operators • Data Scientist and Solution Provider
Objectives	The combination of Asset Administration Shell (AAS) and IDS technologies provide a comprehensive solution for data acquisition and the data exchange among Component Suppliers, Machine Suppliers, Integrators, Operators, and Data Scientists, enabling a collaborative industrial data economy. However, this collaborative environment is hindered by concerns around privacy. The objective of this workflow is to demonstrate how PPML can be incorporated into IDS to tackle the challenge of privacy, enabling participants to conduct analysis on

	private data held by multiple data owners without ever revealing those privacy-sensitive data.
Comment	Messages or blocks of messages need to flow into an IDS Connector, in which they will be encrypted and then will be transferred to a secure infrastructure, known as Trusted Hub. In the Trusted Hub, all data are securely processed in a protected environment. Trusted Hub is a hardware-software solution with only volatile memory providing a tamper-resistant physical and logical encapsulation to tackle both internal (i.e., attacks from operators and administrators) and external attacks. The Trusted Hub is equipped with several smart sensors (e.g., radar and motion sensors that also stream the readouts to blockchains) to detect unauthorized access and inform participants that an unauthorized access is detected. Trusted Hub simply adds an intelligent privacy layer as well as a multi-party collaboration environment on top of the IDS usage control, ensuring that neither the Operator of the infrastructure nor the Provider of services, nor the other participants has the opportunity to access the MGD - not even during processing-while allowing multi-party data analysis.
Preconditions	
Workflow A	 1. Data Providers (Operates) collect the data and via AAS send them to the IDS connector. Next, they publish metadata about the component type and historicized sensor data in IDS broker. 2. Data Scientists, component providers, or machine providers, who are working on a PdM project, query the broker for a specific machine type and filter for sources who can provide MGD. 3. Data Scientists select and request data based on metadata stored in the broker. 4. Data Providers review the request and decide whether or not to collaborate on the PdM project as a participant. They also specify the usage policies which will be enforced in the next steps.

	5. Participants transfer and transfer their MGD, encrypted individually by unique user-specific keys, via IDS connector to Trusted Hub. 6. In the Trusted Hub, PdM algorithms, provided by data scientists, will be trained on top of the MGDs (collected and aggregated from several data owners), while bridging the gap between privacy and utility. No one, neither the operator of the Trusted Hub nor data scientists can see any raw data. All operations, including data ingestion, aggregation, processing and analysis are conducted on a safe, secure, and privacy-preserving environment and only the result of the machine learning will be shared. 7. The result of the model training will be downloaded by data scientists that can be deployed to the corresponding components/machines to predict future failures. 8. All shared data will be permanently deleted from the Trusted Hub.
Requirements	AC: W1, W2, W3, W4, W5, WP6, WP7 UC Integrity: in general This use case extends the traditional IDS usage control by including the following requirements: **Privacy (W4, W5)**: In some specific use cases, due to regulations, raw data is not allowed to be transferred from provider to consumer even over a secure channel in the presence of strict usage policies. **Multi-Party (W6):** Stakeholders should be able to jointly compute a function or train a machine learning model over the combined privacy-sensitive data while keeping those data private. **Privacy-Preserving Computing (W6):** This feature enables the secure computation of the data without revealing the content of the data.
Authors	Farshad Firouzi

11.2 Smart Factory Web

11.2.1 Factory Registration

ID	SFW-01
Name	AAS and AAS Registry for automatic registration in the SFW
Motivation	The Smart Factory Web offers interesting opportunities to find new business partners and securely interact with them over the IDS. However, registration in the SFW requires some initial effort to properly describe the plant and capabilities. A solution could be the automatic registration via an on-premise AAS Registry. Each machine or production line in the plant could register the digital AAS description in the registry. To register the plant, the SFW will connect to the IDS Factory Connector and import the structure of the factory

	in the SFW. Another use-case includes the life-cycle management of plants in the SFW. Instead of updating the profile in the SFW manually, an AAS could be used to automatically update changes of the factory.
Stakeholders	factory owner service broker (Smart Factory Web)
Objective	automatic import and registry in SFW
Constraints	not all information can be extracted from AAS descriptions alone
Comment	Automatic registry of factories in the SFW is currently done via AutomationML. However, not all companies design their factories with AutomationML. The Asset Administration Shell is a promising new standard in the Industry 4.0 landscape that will be adopted in many next generation factories. Using the Asset Administration Shell for registration in the SFW might be the key to reach critical mass.
Preconditions	AAS or AAS Registry is used in the factory
Workflow	1. Factory owner wants to register in SFW to offer production capabilities to new customers 2. He starts the import in the SFW by providing the URL of the AAS Registry 3. The SFW connects to the AAS Registry and imports the factory structure into the SFW 4. Some data is manually added and corrected
Postconditions	The factory owner is now successfully registered in the SFW without much effort.
Requirements	AC: 3 UC Integrity: 3 UC Usage scope: 3
Sources	IDS Reference Architecture
Authors	Ljiljana Stojanovic, Friedrich Volz, Fraunhofer IOSB

11.2.2 Negotiation

ID	SFW-02
Name	Smart Factory Web Negotiation
Motivation	The Smart Factory Web is an industrial platform to find new business partners and negotiate with them. In most industries this negotiation is done by manual agents with telephone and e-mail. During the negotiation, sensitive information like price, availability, capacity and process durations are revealed. The IDS could be the ideal solution to let automatic negotiation agents handle the negotiation without revealing any information to potential partners. This is realized by isolated negotiation containers in the IDS Connectors, that interact with other negotiators, but cannot leak any information elsewise. After negotiation, the successful terms of a contract are presented, but dynamic variables about the production are still hidden. The companies then have the opportunity to sign the contract proposed by the negotiation.
Stakeholders	• Service broker (Smart Factory Web) • Company A • Company B
Objective	Hide sensitive data during negotiations with IDS
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 the IDS so that information cannot be extracted.
Comment	

Preconditions	Both companies have IDS Connectors with Negotiation Apps deployed
Workflow	1. Company A finds Company B on SFW and wants to order a component or service 2. Company A contacts Company B via the IDS Connector and initiates the negotiation 3. The negotiation is handled by the Negotiation Apps without sensitive information ever leaving the Apps. 4. The information gets deleted and the result of the negotiation presented (contract with terms) 5. Company A and B sign the contract
Postconditions	Successful negotiation and contract between previously unknown partners.
Requirements	AC: 2 UC Secrecy: 3 UC Integrity: 3 UC Time to live: 4 UC Usage scope: 3
Sources	https://www.smartfactoryweb.de/servlet/is/65421/Smart_Factory_Web-20191021-PU.pdf
Authors	Ljiljana Stojanovic, Friedrich Volz

11.2.3 Smart Matching

ID	SFW-03
Name	Smart matching of customer/factory with sensitive data
Motivation	Production data can be analyzed by 3rd parties to enhance their service, but normally sharing critical data could compromise confidentiality. The IDS with Usage Control could make sure, that this critical data is only processed in certain Apps and that data is hidden. For example, the Smart Factory Web aims to match customers with a suitable factory. However, the data in this case is sensitive price and production data from the factory. Without IDS, filtering the search results based on this sensitive data is too risky for factory owners.
Stakeholders	• Factory owner • Service broker (Smart Factory Web) • Customer looking for factory

Objective	demonstrate successful data sovereignty for critical production data to mitigate trust issues between unknown partners
Constraints	the critical production data cannot leave the IDS network, e.g. it must be analyzed by the data analysis provider in an IDS App
Comment	"Fraunhofer IOSB" is registered on the Smart Factory Web with several machines capable of providing material for other customers. Fraunhofer also provides critical data about the factory capacity, availability and depending on these parameters the price for a certain amount of material. This data is highly sensitive in a competitive market and Fraunhofer wants this data protected so that the data is only used to enhance the search function of the Smart Factory Web. This allows SFW users to better find a suitable factory in accordance to their price and time constraints. The IDS is used so that the sorting on the Smart Factory Web hides this sensitive data of all factories but the result list is still sorted by price or availability.
Preconditions	Production data needs to flow into an IDS Connector. SFW also uses IDS Connectors and an IDS App to sort the search result list according to the hidden factory data.
Workflow	1. Data owner provides an endpoint in the IDS Connector to retrieve production data 2. Data owner is registered on SFW 3. SFW retrieves data with IDS Connector 4. Usage Policies are checked so that the data can only flow into the SFW Sorter App
Postconditions	Data is hidden and can only be used in SFW Sorter App
Requirements	AC: 3 UC Secrecy: yes (4) UC Integrity: yes (3) UC Usage scope: yes (4)
Sources	www.eur3ka.eu , www.smartfactoryweb.de
Authors	Ljiljana Stojanovic, Friedrich Volz

11.2.4 Provenance

ID	SFW-04

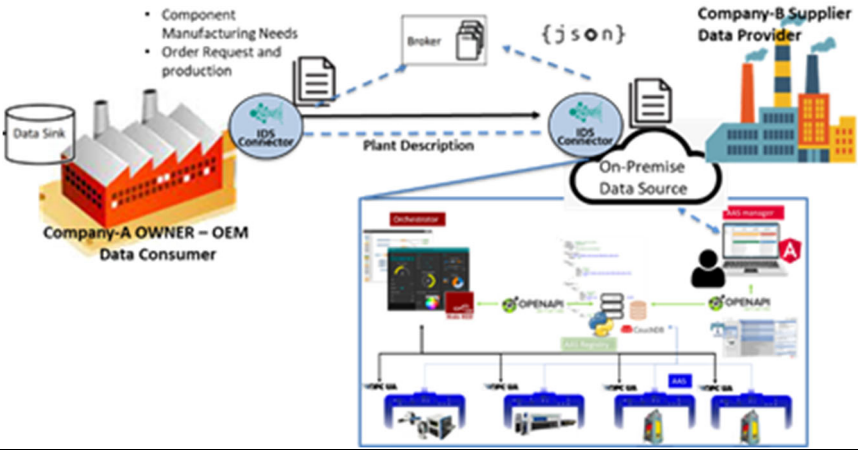| Name	Provenance for critical production data
Motivation	Production data is rarely shared because confidentiality might be compromised. In the case of a data leak or illicit sharing, the data owner does not know who leaked the data and where it went. With data provenance it is possible to trace critical data in the information network. The Smart Factory Web provides a platform to find new partners and interact with them. Data provenance also allows billing of data usage and allows new business models by charging for data usage.
Stakeholders	• Data owner (producer) • Data consumer (partner)
Objective	demonstrate successful data provenance for critical production data to mitigate trust issues, trace data across different companies and allow billing for IDS Clearing House
Constraints	critical production data may not leave the IDS network
Comment	
Comment	Data owner "Fraunhofer IOSB" uses a bulk sorter with valves from Company V. Company V accesses the valve actuations via an IDS Connector to conduct predictive maintenance. Fraunhofer IOSB allows Company V to share and sell the statistics of valve actuations with other companies to improve the process of predictive maintenance. With data provenance, Fraunhofer IOSB will be notified if Company V shares the data. Additionally, a small fee will be paid by Company V if data is sold to other companies.
Preconditions	Production data needs to flow into an IDS Connector, for example the "IOSB OPC UA Factory Connector" supports retrieval of data by OPC UA. The data consumers need IDS Connectors.
Workflow	1. Data owner provides an endpoint in the IDS Connector to retrieve production data 2. Data consumer retrieves data with his IDS Connector 3. Usage Policies are checked so that the data can only flow in ways the data owner allows 4. Every data transfer is tracked (Provenance) and a bill is created for data consumers
Postconditions	Data owner successfully tracked data in the network (Provenance) and billed data consumers
Requirements	AC: 2 UC Secrecy: 2

	UC Integrity: 2 UC Time to live: conditional (required in some cases) UC Usage scope: 3 Data provenance tracking: 4
Sources	IDS Reference Architecture, www.smartfactoryweb.de
Authors	Ljiljana Stojanovic, Friedrich Volz

11.2.5 Industrial Asset Management - Plant Description

ID	SFW-05
Name	Industrial Asset Management - Plant Description Service
Motivation	Automation is evolving from a hierarchical model towards an integrated network of smart automation devices. Furthermore, an I4.0 compliant automation system is characterized by its ability to provide a defined and standardized mechanism for locating, accessing, and semantically understanding the standardized and even manufacturer-specific information and manufacturing devices. In that sense, OEMs needs to control the whole component production in their suppliers and its semantic information for future and current schedule production. There is a sequence of tasks to satisfy in a distributed production environment for specific components: 1) Verify the possibility of the production in suppliers knowing the semantic and plant description and 2) sharing the plant description to know the semantic capabilities and characteristics for satisfying the requirements production. To overcome such integration challenges the AAS concept may be used for the automatic self-conducted semantic machine data and for interaction and integration with the industrial environment and IDS connector to share the plant description.
Stakeholders	• Factory - Company A – Data Consumer • Supplier - Company B – Data Producer - Owner • Production Management System
Objective	Demonstrate the successful data sovereignty for production management capabilities through OEMs and suppliers
Comment	---
Preconditions	Messages or blocks of messages and system needs to be deployed into an IDS Connector.

	Company A (Data Consumer) collects information from ERP to know which components and requirements associated are needed to produce specific industrial product

Company B (OWNER - Supplier) produce Home Appliance components based on Asset Administration Shell manufacturing line. AAS Registry and AAS manager stored the AAS capabilities and models from Machine Tool Digital Twin (FAGOR ARRASATE and DANOBAT) |
| Workflow | 1. Factory – Company A - Data Consumer provides an endpoint in the IDS Connector to store information for knowing what manufacturing capabilities needs to produce
2. Supplier - Company B – Data Producer - Owner provides an endpoint in the IDS Connector to provide plant description. Digital Twins of Stamping Machine and Digital Twin of Cutting Machine through OPC-UA for Home appliance operations (oven door and a refrigerator door) provide the schema of plant description following AAS Standard.
3. Data owner (data source) and consumer (data sink) use certificates issue by the IDS certificate authority and the agree on the contract to exchange data.
4. Consumer retrieves data with IDS Connector
5. Usage Policies are checked so that the data can only flow into the App specified by Factory Owner.

 |
| Postconditions | Data is hidden and can only be used by the App specified by the consumer/Factory plant |
| Requirements | AC: yes (workflow steps)
UC Secrecy: yes (steps)
UC Integrity: yes (steps)
UC Separation of duty: yes
UC Usage scope: yes
Data provenance tracking: yes/no/conditional (steps) |

Sources	Digital Twin Stamping Machine – FAGOR ARRASATE
	Digital Twin Laser Cutting Machine - DANOBAT
Authors	Michel Iñigo - MONDRAGON, Felix Larrinaga – MGEP, Blanca Kramer-IKERLAN, Elena Montejo - IDEKO

11.3 Impact on Sustainability Development Goals

11.3.1 Visualization of carbon footprint

Name	Visualization of carbon footprint
Priority	Medium
Reference use case	International data sharing for evaluating SDG impact across industrial value chain
Motivation	The following issues need to be solved for achieving SDGs (Sustainable Development Goals founded by United Nations), and this can be accelerated by promoting international data sharing between businesses. • Since it is not possible to quantitatively measure the SDG Impact of the businesses of each company that provide services / products, investors and regulators cannot confirm whether the business of the company that provides or uses the service / product contributes to the achievement of SDGs. • In the value chain for manufacturing industry, the following three goals out of 17 goals of SDGs are highly needed to be considered: Goal 9 Industry, Innovation and Infrastructure, Goal 12 Responsible consumption and production, and Goal 13 Climate action
Stakeholders	All participants of supply chain, and all stakeholders in the same circular strategy
Objective	Make the business contributions to the achievement of SDGs comparable by collecting, evaluating, scoring, and indexing data on the use of human resources, goods, money and energy (quantity and quality) through secure and trusted data sharing across international industrial value chain. There are various indicators of SDGs, but this use case targets the measurement of the impact on the reduction of greenhouse gas emissions.
Comment	-
Preconditions	The automobile manufacturer (such as electric vehicle manufacturer) requests all companies in the value chain (including electric power

	energy supplier) to share the data related to the use of human resources, goods, money, and energy (e.g. the amount of greenhouse gases emitted through production, distribution, recovery) necessary for evaluating the SDG Impact, and obtain their consent for data sharing. This request is for calculating the SDG Impact on the reduction of greenhouse gas emissions of the entire value chain built for the manufacture and sale of motor vehicles, the provision and use of mobility services utilizing motor vehicles, and the resource recycling of materials and parts of the motor vehicles.
Workflow	The following steps are required to perform the use case: 1. Companies involved in manufacture of one motor vehicle measure the amount of the greenhouse gases emitted for acquisition (collection, mining, cultivation) of all materials, procurement and manufacture of parts. Then, they store the data of the greenhouse gas emission into their internal system in a format that cannot be tampered with. 2. Materials and parts processors and sales brokers measure the amount of greenhouse gases emitted during processing and brokerage. Then, they store the data of the greenhouse gas emission into their internal system in a format that cannot be tampered with. 3. A company that finally assembles and sells a motor vehicle (an automobile manufacturer) measures the amount of greenhouse gases emitted during the final assembly and sale of a motor vehicle. Then, the company stores the data of the greenhouse gas emission into its internal system in a format that cannot be tampered with. 4. A company or individual who purchases and uses a motor vehicle measures the amount of greenhouse gases emitted during the use, maintenance, inspection, and operation of the purchased motor vehicle. Then, the company or the individual stores the data of the greenhouse gas emission into the company's internal system, the system the individual is using, or the system of the automobile manufacturer, in a format that cannot be tampered with. 5. Companies that provide mobility services that utilize motor vehicles measure the amount of greenhouse gases emitted during the use, maintenance, inspection, and operation of the motor vehicles they use. Then, they store the data of the greenhouse gas emission into their internal system in a format that cannot be tampered with. 6. Companies that collect discarded motor vehicles measure the amount of greenhouse gases they emit when collecting their parts. Then, they store the data of the greenhouse gas emission into their internal system in a format that cannot be tampered with. 7. Companies that disassemble collected motor vehicles and sort, process, and resell their parts measure the amount of greenhouse gases emitted during the disassembly, sorting, processing, and sale of their parts. Then, they store the data of the greenhouse gas emission into their internal system in a format that cannot be tampered with.

	8. The automobile manufacturer accesses all of the above systems in a secure and trusted manner to obtain greenhouse gas emission data. Then, the automobile manufacturer calculates the amount of greenhouse gases emitted by the business of manufacturing and selling one motor vehicle or providing mobility services utilizing one motor vehicle, as an index of SDG Impact, by using a universal calculation method. 9. The automobile manufacturer can only access data on greenhouse gas emissions from the manufacture of its products, and never access data on the value chain for other automobile manufacturers. 10. An audit and certification body authorized to verify the emissions of greenhouse gases in the industry has access to data for all value chains of all client companies.
Postconditions	An automobile manufacturer submits the calculation result of the SDG Impact of the amount of greenhouse gas emission to a third-party certification body to obtain a digital certificate. Then, the aggregated value and average value of the SDG Impact will be disclosed and provided, to stakeholders such as investors, customers, regulators, and corporate rating agencies together with digital certificates. Stakeholders such as investors, regulators and corporate rating agencies evaluate and rank the contribution of each company to the achievement of SDGs, and publish the results.
Requirements	AC: yes (step 8) UC Secrecy: yes (all steps) UC Integrity: yes (all steps) UC Separation of duty: yes (step 8) UC Usage scope: conditional (step 8) Data provenance tracking: yes (all steps)
Sources	-
Authors	Koki Mitani (NTT Corporation)

11.3.2 Visualization of resource circulation

Name	Visualization of resource circulation
Priority	Medium
Reference use case	International data sharing for evaluating SDG impact across industrial value chain
Motivation	The following issues need to be solved for achieving SDGs (Sustainable Development Goals founded by United Nations), and this can be accelerated by promoting international data sharing between businesses. • Since it is not possible to quantitatively measure the SDG Impact of the businesses of each company that provide services / products, investors and regulators cannot confirm whether the business of the company that provides or uses the service / product contributes to the achievement of SDGs. • In the value chain for manufacturing industry, the following three goals out of 17 goals of SDGs are highly needed to be considered: Goal 9 Industry, Innovation and Infrastructure, Goal 12 Responsible consumption and production, and Goal 13 Climate action
Involved stakeholders	All participants of supply chain, and all stakeholders in the same circular strategy
Objective	Make the business contributions to the achievement of SDGs comparable by collecting, evaluating, scoring, and indexing data on the use of human resources, goods, money and energy (quantity and quality) through secure and trusted data sharing across international industrial value chain. There are various indicators of SDGs, but this use case targets the measurement of the impact on the realization of resource recycling.
Comment	-
Preconditions	The automobile manufacturer (such as electric vehicle manufacturer) requests all companies in the value chain (including electric power energy supplier) to share the data related to the use of human resources, goods, money, and energy (e.g. the information about reuse and recycle of materials and parts) necessary for evaluating the SDG Impact, and obtain their consent for data sharing. This request is for calculating the SDG Impact on the realization of resource recycling of the entire value chain built for the manufacture and sale of motor vehicles, the provision and use of mobility services utilizing motor

	vehicles, and the resource recycling of materials and parts of the motor vehicles.
Workflow	The following steps are required to perform the use case: 1. Companies that procure the materials and parts needed to manufacture motor vehicles identify whether the procured materials or parts are reused or recycled from used products. Then, they store the data of the evidence of reuse and recycle into their internal system in a format that cannot be tampered with. 2. The material or part processors identify whether the materials or parts used during processing are reused or recycled. Then, they store the data of the evidence of reuse and recycle into their internal system in a format that cannot be tampered with. 3. A company that finally assembles and sells a motor vehicle (an automobile manufacturer) identifies whether the materials and parts used in the final assembly of motor vehicles are reused or recycled. Then, the company store the data of the evidence of reuse and recycle into their internal system in a format that cannot be tampered with. 4. A company or individual who purchases and uses a motor vehicle records the history of repairing the purchased motor vehicle, reusing it for various purposes, and collecting or disposing of part or all of it when it is no longer needed. Then, the company or the individual stores the data of the evidence of repair, reuse, collection, and disposal into the company's internal system, the system the individual is using, or the system of the automobile manufacturer, in a format that cannot be tampered with. 5. Companies that provide mobility services record the history of repairing the purchased motor vehicle, reusing it for various purposes, and collecting or disposing of part or all of it when it is no longer needed. Then, they store the data of the evidence of repair, reuse, collection, and disposal into their internal system in a format that cannot be tampered with. 6. Companies that collect obsolete motor vehicles record information about where they are reused (sold) or where they are disposed of. Then, they store the information into their internal system in a format that cannot be tampered with. 7. Companies that disassemble a collected motor vehicle and sort, process, and resell its parts record the history of the reuse of its materials and parts. Then, they store the information into their internal system in a format that cannot be tampered with. 8. The automobile manufacturer accesses all of the above systems in a secure and trusted manner to obtain data on the origin of materials and parts. Then, the automobile manufacturer calculates the usage rate of reused or recycled materials and parts in the business of manufacturing and selling one motor vehicle or providing mobility services utilizing one motor vehicle, as an index of SDG Impact, by using a universal calculation method.

	9. The automobile manufacturer can only access data on the resources used to manufacture its products and never access data on the value chain for other automobile manufacturers. 10. An audit and certification body authorized to verify the circulation of industry resources has access to all value chain data for all client companies
Postconditions	An automobile manufacturer submits the calculation result of the SDG Impact of the usage rate of reused or recycled materials and parts to a third-party certification body to obtain a digital certificate. Then, the aggregated value and average value of the SDG Impact will be disclosed and provided, to stakeholders such as investors, customers, regulators, and corporate rating agencies together with digital certificates. Stakeholders such as investors, regulators and corporate rating agencies evaluate and rank the contribution of each company to the achievement of SDGs, and publish the results.
Requirements	AC: yes (step 8) UC Secrecy: yes (all steps) UC Integrity: yes (all steps) UC Separation of duty: yes (step 8) UC Usage scope: conditional (step 8) Data provenance tracking: yes (all steps)
Sources	-
Authors	Koki Mitani (NTT Corporation)

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Emil-Figge-Str. 80
44227 Dortmund | Germany

phone: +49 231 70096 501
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

@ids_association

international-data-spaces-association