A European Common Digital Manufacturing Infrastructure and Data Space Pathway for Connected Factories 4.0 Data Value Chain Governance

Digital Europe EU Grant Agreement: 101083939

Title	D4.2 Blueprints for Data Spaces 4.0
Document Owners	ENG
Contributors	SQS, INNO
Dissemination	Public
Date	27/09/2024
Version	2.0

Document History

07/07/2023	ToC
31/08/2023	ENG's Contribution to Ch. 2 and Ch. 4
20/09/2023	UNP's Contribution to Ch. 3 and Ch. 7, ENG's Contribution to Ch. 5
09/11/2023	SQS's Contribution to Ch.,
10/11/2023	First draft of the document
26/11/2023	Quality Revision of the Deliverable
30/11/2023	Final version 1.0
06/09/2024	Revision of the document
27/09/2024	Final version 2.0

Document Fiche

Authors	Angelo Marguglio, Marta Calderaro (ENG), Begoña Laibarra (SQS), Oscar Lazaro, Lucia Castiñera (INNO)
Internal Reviewers	Oscar Lazaro (INNO), Sergio Gusmeroli (POLIMI), Golboo Pourabdollahian (IDC)
Workpackage	4 – Manufacturing Data Space Building Blocks and Blueprint Certification
Task	T4.3 - Manufacturing Data Space Blueprints for Dynamic Asset Management, Predictive Maintenance and Agile Supply Chain T4.4 - Manufacturing Product and Process Data Space Blueprint Certification Strategy
Nature	Report
Dissemination	Public

Project Partners

Participant organisation name	Acronym
ASOCIACIÓN DE EMPRESAS TECNOLÓGICAS INNOVALIA	INNO
FONDAZIONE POLITECNICO DI MILANO	FPM
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	CEA
VDI TECHNOLOGIEZENTRUM GMBH	VDI TZI
BRAINPORT INDUSTRIES COOPERATIE UA	BPI
INDUSTRIE 4.0 OSTERREICH – DIE PLATTFORM FUR INTELLIGENTE PRODUKTION	PIA
CHALMERS TEKNISKA HOGSKOLA AB	CHALMERS
INTERNATIONAL DATA SPACES EV	IDSA
ENGINEERING - INGEGNERIA INFORMATICA SPA	ENG
UNPARALLEL INNOVATION LDA	UNPARALLEL
SOFTWARE QUALITY SYSTEMS SA	SQS
FIWARE FOUNDATION EV	FIWARE
IDC ITALIA SRL	IDC ITALIA
SIEMENS AKTIENGESELLSCHAFT	SIE

Executive Summary

The deliverable *D4.2 Blueprints for Data Spaces 4.0* aims at designing the main elements characterising a Manufacturing Data Spaces, and Data Value Journey and the Data Business Journey experienced in participating in a Data Space. It furtherly identifies main elements and principles related to the design, development and deployment of a Manufacturing Data Space, by providing a taxonomy of Data Spaces Building Blocks and their relationship with RAMI 4.0 as the main Reference Architecture in the Manufacturing context; the conceptualisation of a preliminary checklist of the main key points to be followed for the creation of a Manufacturing Data Space; the definition of the main phases of the creation of a Manufacturing Data Space; and the certification models and strategy designed by Data Space 4.0.

Lastly, it supports the Blueprint adoption in a concrete Manufacturing Data Value Chain via the example provided by the Use Cases part of one of the European Data Space Deployment projects in the Manufacturing domain, the SM4RTENANCE project.

Keywords: *Manufacturing, Blueprint, Building Blocks, Checklist, Reference Architecture, RAMI 4.0, OSS Catalogue, Certification Strategy*

Disclaimer

Acknowledgement

This document is a deliverable of EU DATA SP4CE project. This project has received funding from the European Union's Digital Europe programme under grant agreement N° 101083939.

Table of Contents

List of Figures

Abbreviations and Acronyms

Acronym	Meaning
AAS	Asset Administration Shell
ADRA	Artificial Intelligence, Data and Robotics Association
API	Application Programming Interface
APP	Application
BAE	Business API Ecosystem
BBs	Building Blocks
BDVA	Big Data Value Association
BLOFT	Business, Legal, Operational, Functional and Technical
CAB	Conformity Assessment Bodies
CAGR	Compound annual growth rate
CoCs	Codes of Conducts
CPRF	Certification Program Reference Framework
CX	Catena-X initiative
DFA	Digital Factory Alliance
DS	Data Space
DS 4.0	EU DATA SP4CE - Data Space 4.0
DSBA	Data Spaces Business Alliance
DSSC	Data Space Support Centre
DTDL	Digital Twin Definition Language
DVC	Data Value Chain
EBSI	European Blockchain Services Infrastructure
EDIH	European Digital Innovation Hub
EIT	European Institute of Innovation and Technology
EFFRA	European Factories of the Future Research Association
ENISA	European Union Agency for Cybersecurity
ET	Engineering Technology
ETSI	European Telecommunications Standards Institute
EU	European
FAIR	Findable, Accessible, Interoperable and Reusable
GDPR	General Data Protection Regulation
ICANN	Internet Corporation for Assigned Names and Numbers

IDS	Industrial Data Space
IDSA	International Data Space Association
IIoT	Industrial IoT
IM	Identity Manager
IoT	Internet of Things
IT	Information Technology
MaaS	Manufacturing as a Service
MDS	Manufacturing Data Space
MiE	Made in Europe
MQTT	Message Queuing Telemetry Transport
NGSI	Next Generation Service Interfaces
NGSI-LD	NGSI Linked Data
ODRL	Open Digital Rights Language
OEM	Original Equipment Manufacturer
OPC	Open Platform Communications
OPC UA	OPC Unified Architecture
OSS	Open-Source Software
OT	Operational Technology
ParIS	Participant Information Service
P4P	Process for Planet
PSD2	2nd Payment Services Directive
RA	Reference Architecture
RAM	Reference Architecture Model
RAMI 4.0	Reference Architectural Model Industrie 4.0
RCPF	Reference Certification Programme Framework
SCADA	Supervisory Control and Data Acquisition
XACML	eXtensible Access Control Markup Language

Introduction

This deliverable *D4.2 Blueprints for Data Spaces 4.0* represents a key milestone devoted to achieving one of the main results of EU DATA SP4CE project. It relates to *MS5 - Certifiable blueprints and common/specific building blocks for DS continuity available in a catalogue* and it unveils the Data Space 4.0 Blueprint dedicated to the Manufacturing Industry, both Discrete and Process Industry. The analyses, the activities and the methodologies pursued during the project lifetime, with specific reference to the *Work Package 4 – Manufacturing Data Spaces Building Blocks and Blueprint Certification*, and its main tasks, namely *T4.3 Manufacturing Data Space Blueprints for Dynamic Asset Management, Predictive Maintenance and Agile Supply Chains* and *T4.4 Manufacturing Product and Process Data Space Blueprint Certification Strategy* have been included as annexes to the proposed Blueprint.

The document objective is to share useful recipes and guidelines to support the design, development and deployment of a Manufacturing Data Space, covering common scenarios and key aspects related to the Manufacturing Industry.

The Blueprint is designed as a CookBook, guiding the organisation in the identification of key values and necessary steps to design a Data Space, as described by the following items:

1. *The concepts behind a Manufacturing Data Space and the reasons behind the participation in a data space.*
2. *the Data Value Journey and Business Value Journey that an organisation will experience in participating in a Data Space.*
3. *the main Building Blocks to design a Data Space.*
4. *the technical convergence with Industry 4.0 main principles, and the available innovative solutions.*
5. *the main BLOFT dimensions to be pursued to design a Manufacturing Data Space within a useful checklist*
6. *main steps to design and deploy a Manufacturing Data Space.*
7. *Certification strategy in a Manufacturing Data Space.*

1 What is a Manufacturing Data Space

The European strategy for data aims to speed up the development of the European data ecosystems and economy to harness the societal value of data, and to ensure Europe's global competitiveness and data sovereignty.

At the core of the proposed measures to ensure the successful achievement of its objectives, it designed the development and deployment of the *Common European Data Spaces.*

According to the pioneer initiative *Data Space Support Centre* (DSSC), a Data Space is defined as "A distributed system defined by a governance framework that enables secure and trustworthy data transactions between participants while supporting trust and data sovereignty. A data space is implemented by one or more infrastructures and enables one or more use cases" [1].

A Manufacturing Data Space might deal with different aspects of the manufacturing lifecycle:

- the design of products and processes - with the Product Lifecycle Management (PLM), the Process Simulation and Supply Chain optimisation,
- the operation, production, maintenance and control – mainly devoted to MES, MOM, Factory Automation and Control, Supply Chain management, Asset Management as well as Warehouse Management System, Transportation Management System and Quality Control,
- the Product Performance monitoring and maintenance, Sale and After Sale management, and the Customer Relationship Management.

Therefore, a Manufacturing Data Space has the capacity to enable Data sharing among different actors as manufacturing companies, service providers, suppliers, end-users and clients (from an individual to a Public Administration), influencing business-to-business, business-to-government and business-to-consumer related services and ecosystems.

In the Manufacturing Data Space companies can share, integrate and use data collaboratively and securely to improve operational efficiency and transparency in commercial relationships. Data Spaces also facilitate improved decision-making and innovation processes, ensuring flexibility and efficiency via cost savings and faster operations, and circularity. They also

facilitate the creation of new business models, through the optimisation of the user experience through personalised services or even mass customisation. Ultimately, collaboratively sharing data across the supply chain allows companies to identify and mitigate risks.

Data value chains will enable Industry 4.0 services as dynamic asset management, predictive/prescriptive maintenance, and support the effective deployment of the most innovative enabling technologies as AI-based analytics, IIoT and optimisation applications that are capable to influence internal processes, as well as processes across organisations and value chains.

2 Manufacturing Data Space Value Journeys

When designing, operating or simply joining a Manufacturing Data Space, every organisation will realise both a "*Data Value Journey*" and a "*Business Value Journey*" as part of the continuous Digital Transformation journey that every modern company has now to go through to remain competitive in the EU Digital Single Market.

These two journeys are briefly presented also in the following Figure 1. These journeys represent what the Data Space Support Center's glossary[1] specifies as Data space value, the cumulative value generated from all the data transactions and use cases within a data space.

The Data Value Journey starts from the top with the identification of all the actors of the *Data Value Chains* of interest (e.g. manufacturing companies, OEM providers, suppliers, operators, …). These actors (and especially the manufacturing companies) have already access to several *Manufacturing Process and Asset 4.0 Data Sets*, coming from their systems operating at Engineering Technology (*ET*), Operational Technology (*OT*), Information Technology (*IT*), and Industrial IoT (*IIoT*) level. Most of these datasets are usually underexploited if left in silos, within a company or even within a single department. Only when *Individual Companies* start adopting trusted technologies to share data (via *Trusted Network*s, *Data Marketplaces* or *Open Data* portals) in their Data Value Chains, their Business Value Journey begins.

The Business Value Journey, depicted on the left-hand side of on the Figure 1, represents how digital infrastructures can impact every business, thankful to data sharing practices in trustful European Data Spaces. The journey starts from the bottom where a edge-cloud *Federated Trusted Ecosystem* will be established to offer access and usage services to High-Value Data Sets (mostly data sets built within a single organisation and made available upon the FAIR principles, see point above) within Cloud Infrastructures, able to host Data Platforms and

[1] DSSC Glossary is a curated set of terms ('names' of the entities) and definitions ('criteria' enabling to check if something qualifies as an instance of the term). The current version of the glossary can be found at Data Spaces Glossary.

relevant *Data Services* and *Federation Services*. The existing *Digital Manufacturing Platform* of an individual company will be extended to support *Collaborative Industrial Data Sharing* capabilities, while keeping the full control on the *Factory Systems and APPS*, as well as hosting new *Industrial Data-driven Services* enabled by a larger data pool available for intelligent applications. The federation of different sovereign digital platforms enables extensive data sharing capabilities facilitating and enhancing advanced processes and solutions, benefiting from the established *Manufacturing Data Spaces* (e.g. for *Dynamic Asset Management and Predictive/Prescriptive Maintenance*, for *Agile Supply Chain Management and Execution*, for *Data Sharing for Circularity*, or any other). Therefore, the interactions among Manufacturing Data Platforms into *European Data Spaces* will contribute to the wider impact on the European Data Economy and the whole *EU Digital Single Market*.

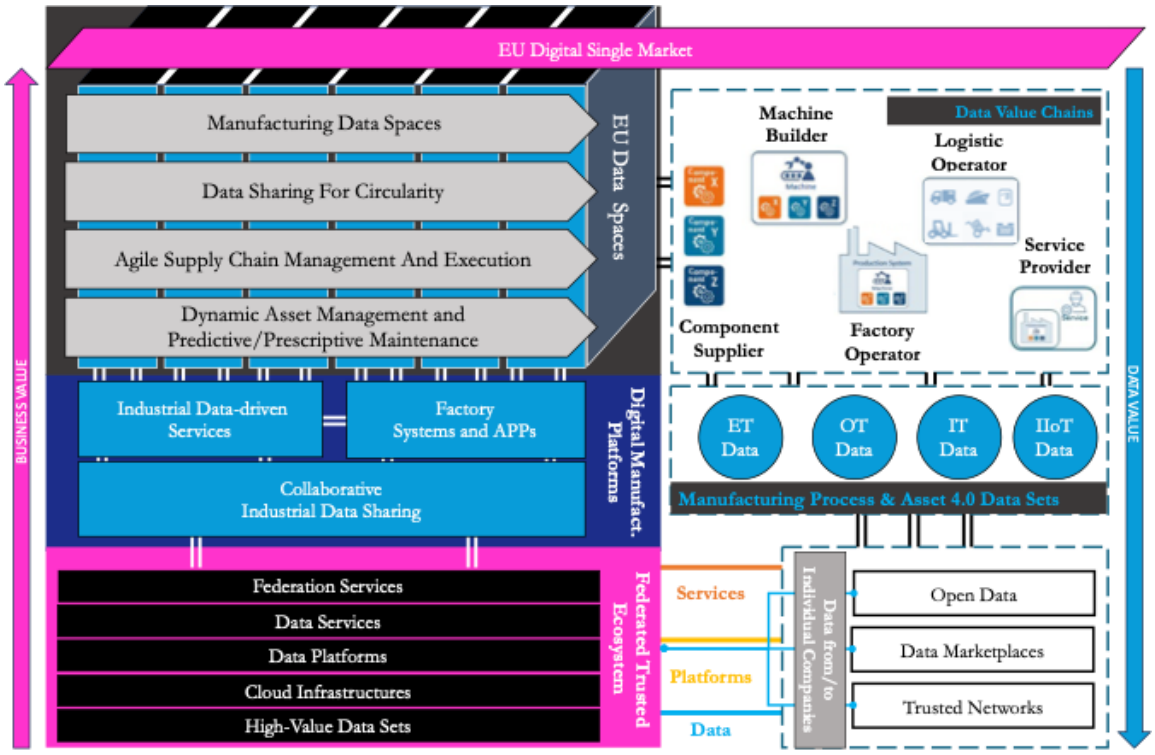

Figure 1. Conceptualization of a Data Space for Manufacturing

3 Main Building Blocks of a Manufacturing Data Space

As part of the Data Space Support Centre's Data Spaces Blueprint, the following concepts represent the main baseline for the design of a Data Space:

- Conceptual Model: a model of the data space domain which represents the concepts (entities) and the relationships between them. The Conceptual Model can be found at DSSC Data Space Conceptual Model.
- Data Spaces Building Blocks: a basic unit or component that can be implemented and combined with other building blocks to achieve the functionality of a data space. For each building block specifications and reference implementations are identified, especially for technical building blocks, at the Data Space Building Blocks.

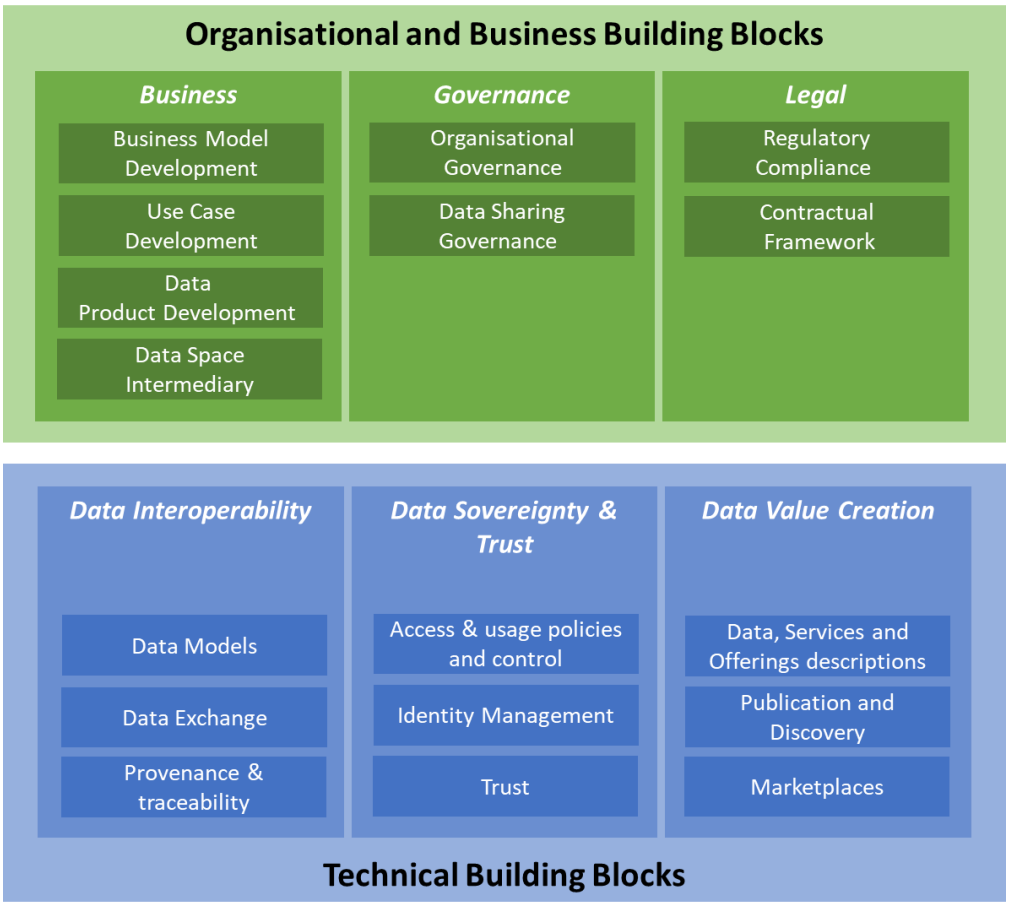

Figure 2. Data Space Building Blocks

There are choices to be made for each building block. The DSSC wants to enable data spaces to reach a higher maturity-level faster: enabling data spaces to focus on their business or societal objectives. In addition, it wants to ensure future benefits from synergies and to foster data space interoperability, making it easier to connect to multiple data spaces and enable economies of scale for data space intermediaries.

The Building Blocks represent the backbone of a Data Space, specified in two interlinked categories:

- Business and Organisational building blocks: these relate to business models of data spaces, the governance of data spaces and the legal frameworks for data spaces. While the focus may differ, the four key outcomes mentioned below still apply, albeit with a slightly different approach. For more information about the Governance building blocks, please refer to: Business and Organisational Building Blocks
- Technical building blocks: These relate to the technical aspects of a data space, i.e. the technical agreements which individual participants and trusted data space intermediaries need to adhere to. The technical specifications outline the use of specific technology solutions and processes that are necessary for ensuring the desired functionality of a given building block. For more information about the Governance building blocks, please refer to: Technical Building Blocks

In the Manufacturing context, for both Discrete and Process Industries, the Building Blocks does not change from the DSSC's vision, but assume a deeper relevance due to level of abstraction necessary for the different actors and value chains in the manufacturing context.

The convergence among standards, technological and business innovations across the different building blocks represents a key activity to be pursed in the design and development of a Data Space.

4 Convergence with Industry 4.0

The RAMI 4.0 Reference Architecture [2], in a three-dimensional way, defines how to approach the deployment of Industry 4.0 principles in a structured manner. RAMI 4.0 is able to support all participants involved in the Industry 4.0 processes through a common understanding, simplifying the complexity thanks to the three dimensions:

- Layers responsible for describing all the IT components in a structured manner.
- Life Cycle Value Stream represents the life cycle of the product.
- Hierarchy Levels details all the hierarchy levels of the organisation and its functionalities.

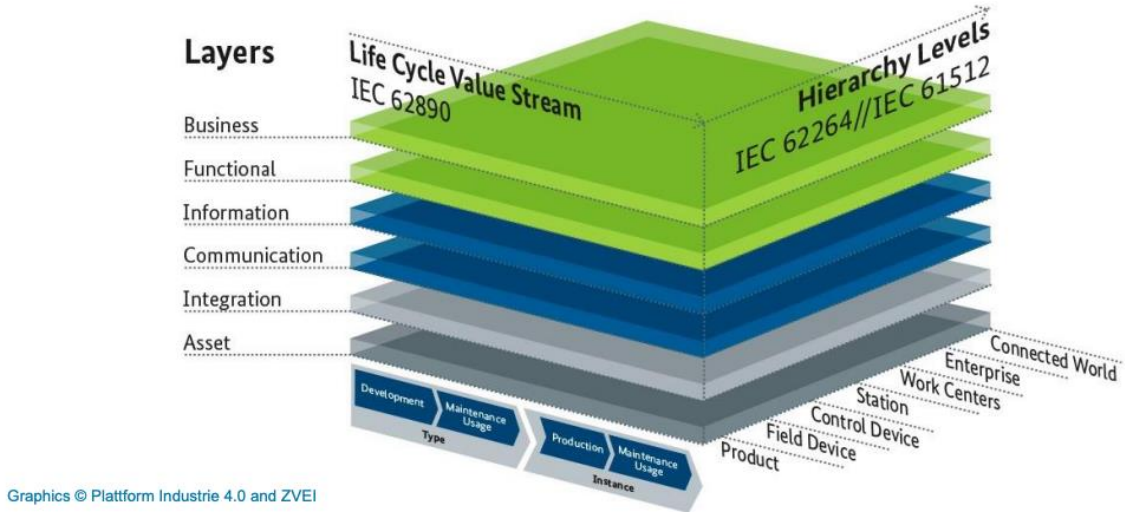

Figure 3. RAMI 4.0 Architecture

Based

on Data Spaces Support Centre (DSSC) Building Block Taxonomy, a mapping exercise is intended to ease the understanding of the *Data Spaces Building Blocks* to any system architect already experienced in designing and implementing manufacturing platform based on RAMI 4.0.

Furthermore, a deep analysis regarding how those building block can be customised, implemented and used and with which available solutions can be tailored in the manufacturing sector has been performed.

In the rest of the section, a mapping analysis between *Data Spaces Building Blocks* and RAMI 4.0 has been presented to describe how the Data Space elements can impact the RAMI 4.0 dimensions. These mappings are intended to ease the understanding of the *Data Spaces*

Building Blocks to any system architect already experienced in designing and implementing manufacturing platform based on RAMI 4.0. Furthermore, referring to a reference model will streamline also the communications among different stakeholders of the Data Space, especially at (eco)system level.

Furthermore, several manufacturing-specific standardised technologies and innovative solutions have been included in the Building Block's related section.

It is worth to mention that, as described in the *D4.1 Pan-European Data Platform Catalogue,* a selection of the best in place and latest innovative technologies available for each Building Block has been included in the Digital Factory Alliance's Catalogue of Open-Source Software service.

In the rest of the document, we have adopted the convention of using *italic font* whenever a specific term can be retrieved the DSSC Glossary for further clarification [1].

Data models

The common semantic understanding is necessary for the different architecture layers described from RAMI 4.0: business processes, functions of the assets, data access and representation, physical things and related transition to the digital world need to have a vocabulary to describe and interpret data in a proper way. Same considerations can be done for the hierarchy levels considering the semantic needs through the entire enterprise or factory covering different types of functions (restricted, wide range, real-time, etc.).

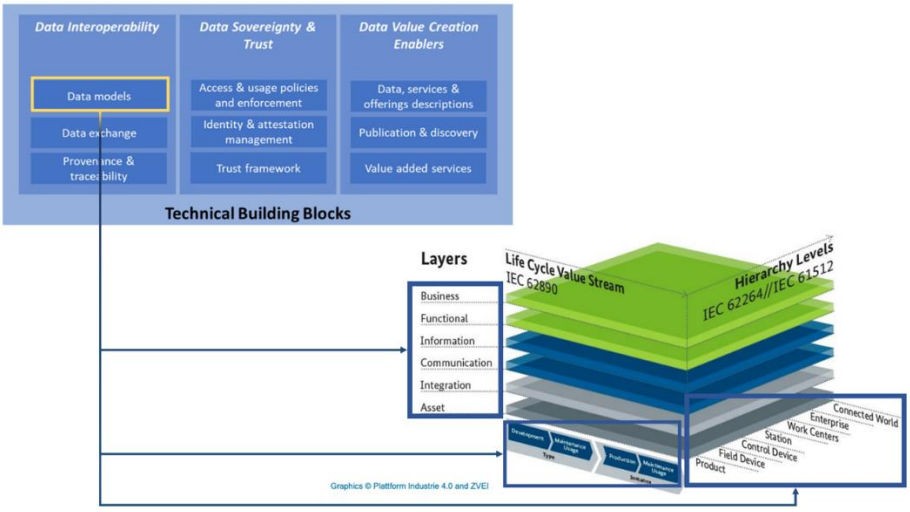

Figure 4. DSSC Taxonomy vs. RAMI 4.0 - Data models analysis

Therefore, Data Models and Format enables a common semantic understanding of data in a Data Space, guaranteeing a data consumer is able to interpret data in a proper way for reaching the semantic interoperability. Several manufacturing-specific data interoperability standards exist; a not exhaustive list is reported below:

- *Digital Twin Definition Language (DTDL)* is a language for describing digital twin models of smart devices, assets, spaces, and environments. It allows manufacturers to capture the rich semantics of their IoT solutions, including the relationships between different devices, their properties, commands, and telemetry.
- *MQTT Sparkplug* is an interoperability protocol that works perfectly for smart manufacturing and industrial automation use cases offering a specification that enables OEM device manufacturers and application developers to build comprehensive and interoperable SCADA/IIoT solutions, leveraging MQTT as the core messaging technology.
- *OPC UA* is a set of standards developed by the OPC Foundation for industrial information exchange. It promotes a unified approach for interacting with different data sources in an industrial setting.
- *AAS - Asset Administration Shell*, conceptualised within the context of the German Industrie 4.0 initiative, is a digital representation or digital twin of a physical asset in the production process.
- *Smart Data Models (SDM)* - The Smart Data Models Program (smartdatamodels.org) includes more than 1100 open-licensed documented data models in 13 different domains, documented with technical specifications translated into 7 languages and with technical resources for the validation of compliance.

Data exchange

Data must be exchanged following specific rules and guidelines to enable the interaction between systems and/or data counterparts. It complements the Data Model and Formats component: defined common models and data representation are used during the data exchange. Data exchange building block impacts the architecture layers from the communication up to the business one, considering the component nature for defining the

access to information, the necessary data, functions of assets and business processes. On the other hand, the entire hierarchy level is involved, due to the need of communication among all participants of the network.

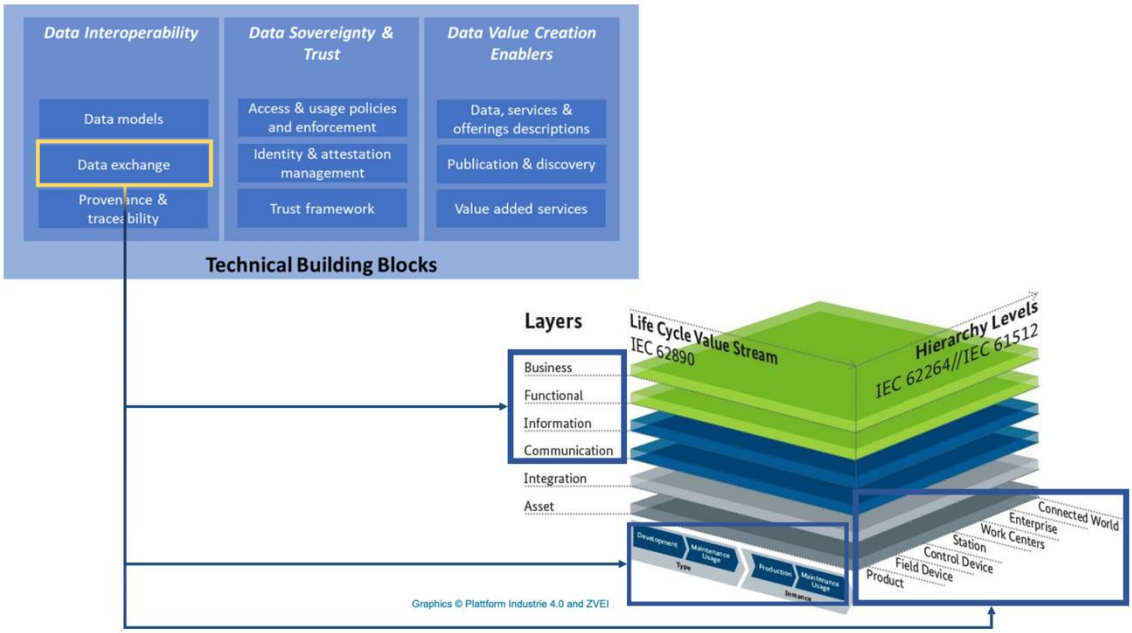

Figure 5. DSSC Taxonomy vs. RAMI 4.0 - Data exchange analysis

Data Exchange API allows data sharing and exchange between Data Space participants. It enables the control phase (contract negotiation) as a preliminary step before the data exchange. After the analysis of the existing Manufacturing Data Spaces based on IDSA and FIWARE several components can be listed as examples:

- *Data Space (IDS) Connectors* compliant with the IDS Reference Architecture Model (RAM) implement both control phase and physical data exchange.
- *FIWARE Context Broker* based on NGSI-LD API specifications for managing context data and related (standardised by ETSI) services.

Provenance and traceability

Data must be monitored to support the data sovereignty operations implementing the no-repudiation. Data sharing has to be observable for legal and business reasons (data economy). The component impacts mainly to the three upper levels of the architecture layers, starting from the information layer and to the entire hierarchy levels embracing the entire connected network.

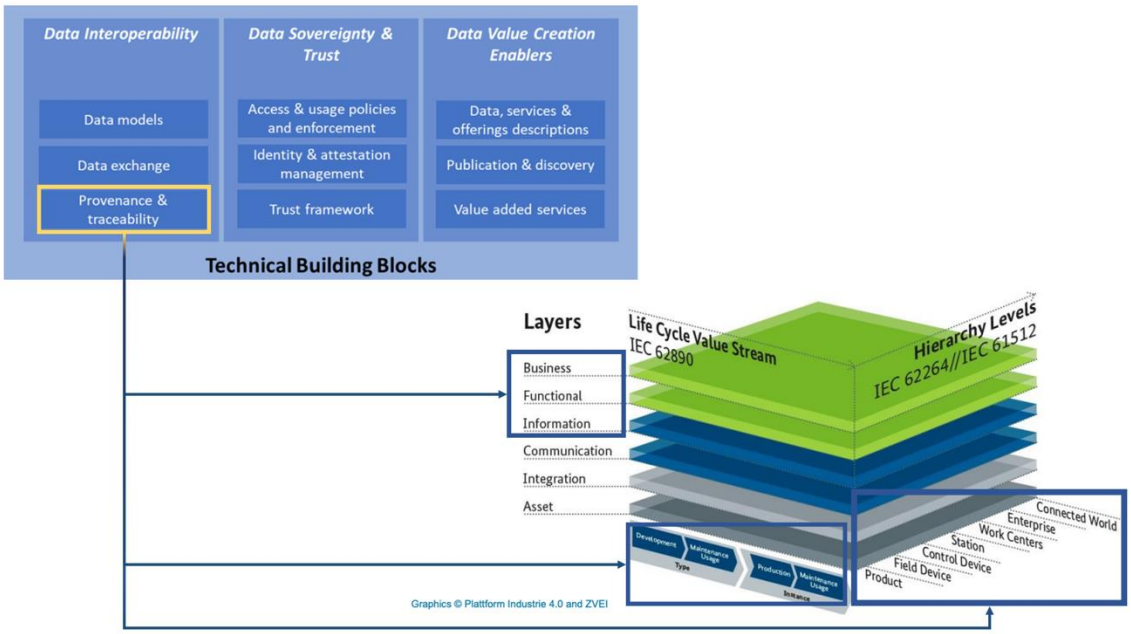

Figure 6. DSSC Taxonomy vs. RAMI 4.0 - Provenance and traceability

Provenance and Traceability observes the data sharing process managing transactions through the implementation of auditing and logging services.

- *IDS Clearing House* consists of an IDS Connector and bases all its functions on a logging service that records information relevant for clearing and billing as well as usage control.

Access & usage policies and enforcement and Trust framework

The *Access & usage policies and enforcement* component is crucial for the Data Spaces definition. The *Trust framework* component refers to a set of common agreed rules, standards and technology enablers in order to establish trust among Data Space participants. Indeed, they represent one of the foundations for the data sovereignty implementation: the counterparts have to make an agreement related to the data access and usage in order to guarantee that data can be accessed only by the authorised "consumers" and used according to the usage control rules have been exchanged during the contract negotiation phase. In this case, the mapping with RAMI4.0 impacts on the Enterprise and Connected World hierarchy levels, considering the "openness" of a factory/enterprise to be a *Data space participant*.

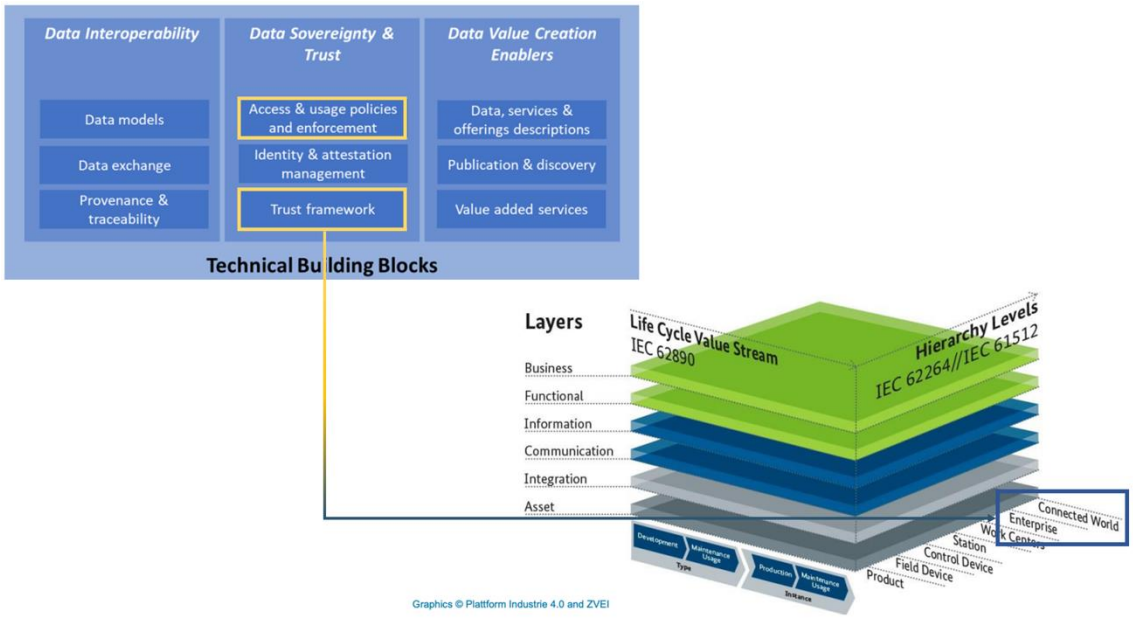

Figure 7. DSSC Taxonomy vs. RAMI 4.0 – Access & usage policies and enforcement and Trust framework

Access and Usage Policies Control guarantees enforcement of data access and usage policies defined as part of the terms and conditions established when data resources or services are published or negotiated between counterparts. Using the Identity Management services, data provider can verify the access rights, while the usage policies can be enforced on both sides.

- *ODRL (Open Digital Rights Language)* is an international standard aiming to represent and communicate rules and permissions to the use of data products and services. It defines vocabulary and syntax for permissions, obligations and constraints through a machine-readable format.
- *XACML (eXtensible Access Control Markup Language)* is an open standard to express and enforce access control policies, providing a framework able to manage conditions and permissions for the resource access.

Trust Services realises the Data Space Registry provided by a Data Space Authority. Manufacturing companies (and counterparts) are part of the Data Space Registry.

- *Trusted Issuers Registry* provides both an EBSI Trusted Issuers Registry implementation [20] and an iShare implementation [21]. The service provides data from an NGSI-LD compliant backend and configuration files.

- *IDS Participant Information Service (ParIS)*, a registry for IDS Participant self-description documents.

Identity & attestation management

The Identity & attestation management block is crucial for managing Data Space counterparts. Each participant has to be registered and identified, supporting in a prelaminar way the access control. From the RAMI4.0 perspective, there is a clear mapping between the three upper architecture layers (information, functional and business) since the counterparts are already able to communicate one each other: data will be consumed only if the rules are satisfied. As the previous components, all hierarchy levels are involved, considering the transversal application of the data spaces.

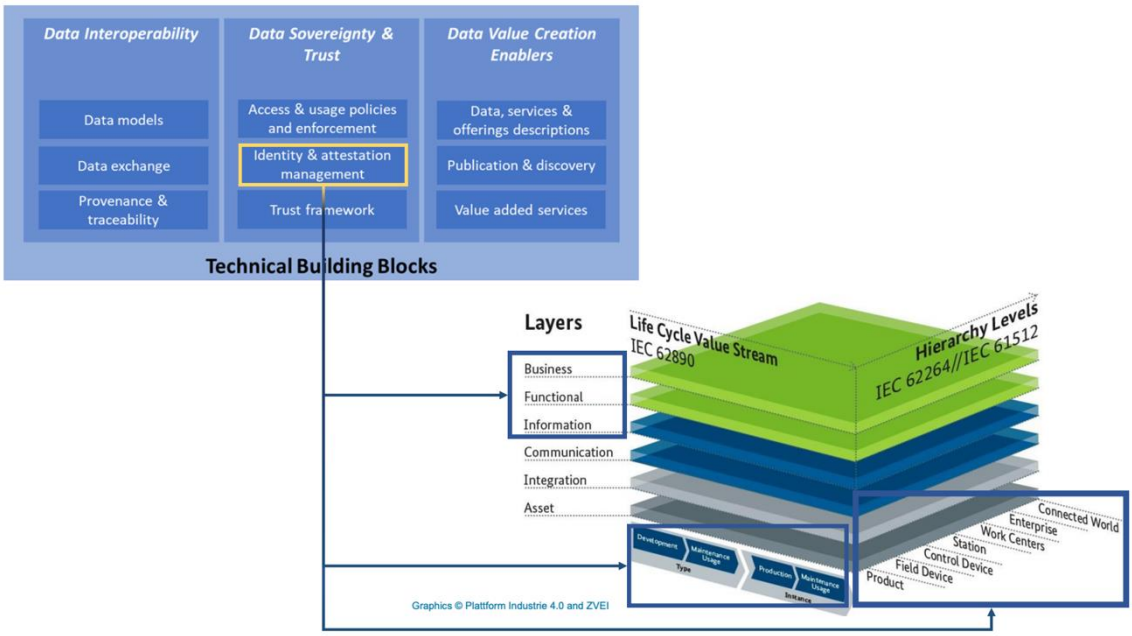

Figure 8. DSSC Taxonomy vs. RAMI 4.0 - Identity management and Trust

Identity Management allows identification, authentication, and authorisation of stakeholders operating in a Data Space. Manufacturing companies can be identified for implementing the access control through several components:

- *FIWARE Trust Framework* allows to manage authentication and authorisation in applications and backend services.
- *IDS Identity Provider* offers a range of services to create, maintain, manage and validate identity information of and for IDS participants, and

components. Collective trust in the provable identity of all IDS participants is imperative to the successful functioning of IDS-based exchanges and economies.

Data Services & offering descriptions, Publication & discovery, Value added services

Data Value Creation building blocks are related to the data description and services (to make them FAIR - Findable, Accessible, Interoperable and Reusable), publication, discovery and marketplace (to enable monetisation).

This “vertical” embraces all hierarchy levels impacting to the entire enterprise, and the three upper architecture layers, from information to business, considering information has to be produced before the publishing.

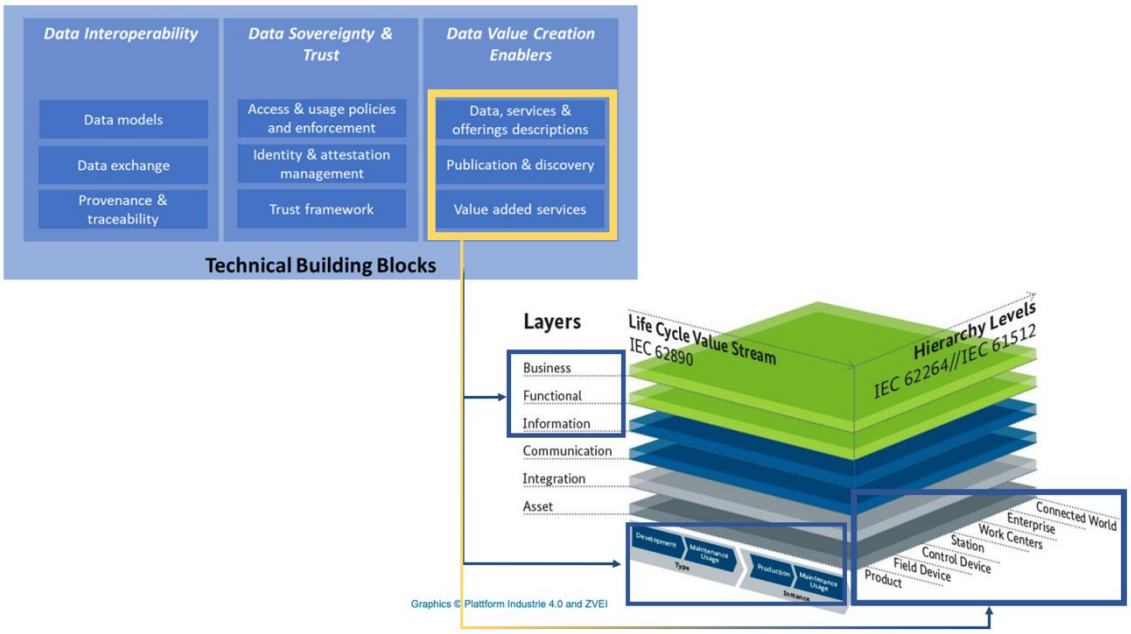

Figure 9. DSSC Taxonomy vs. RAMI 4.0 - Data Services & offering descriptions, Publication & discovery, Value added services

Data, Services and Offering Descriptions includes the definition of data products to create a link with potential consumers. Industrial counterparts have to use a common language to describe metadata and data to enable the data exchange and semantic understanding.

- *Data Space Information Model*

- *IDS Vocabulary Provider* manages and offers vocabularies (including ontologies, reference data models, metadata elements) which can be used to annotate and describe datasets.
- *Dataspace Protocol* is a set of specifications designed to facilitate interoperable data sharing between entities governed by usage control and based on Web technologies in order to ensure the Data Space interoperability.

Publication and Discovery Services includes publishing and discovery mechanisms for data products.

- *IDS Metadata Broker* a registry for IDS Connector self-description documents.

Marketplace and Usage Accounting provides the way to generate value out of sharing data, through the description of services/application to access and process data. Furthermore, mechanisms for usage accounting are defined.

- *IDS Clearing House* provides decentralised and auditable traceability of all transactions if needed. In addition, this intermediary provides clearing and settlement services for all financial and data-exchange transactions within the IDS.
- *FIWARE BAE (Business API Ecosystem)* provides sellers the means for managing, publishing, and generating revenue of their products, apps, data, and services, relying on TM Forum APIs

Governance Building Blocks

Governance building blocks have not a direct impact to the RAMI 4.0 components, however we can consider a wide indirect impact through the correlated technical building blocks have been analysed in the previous sections.

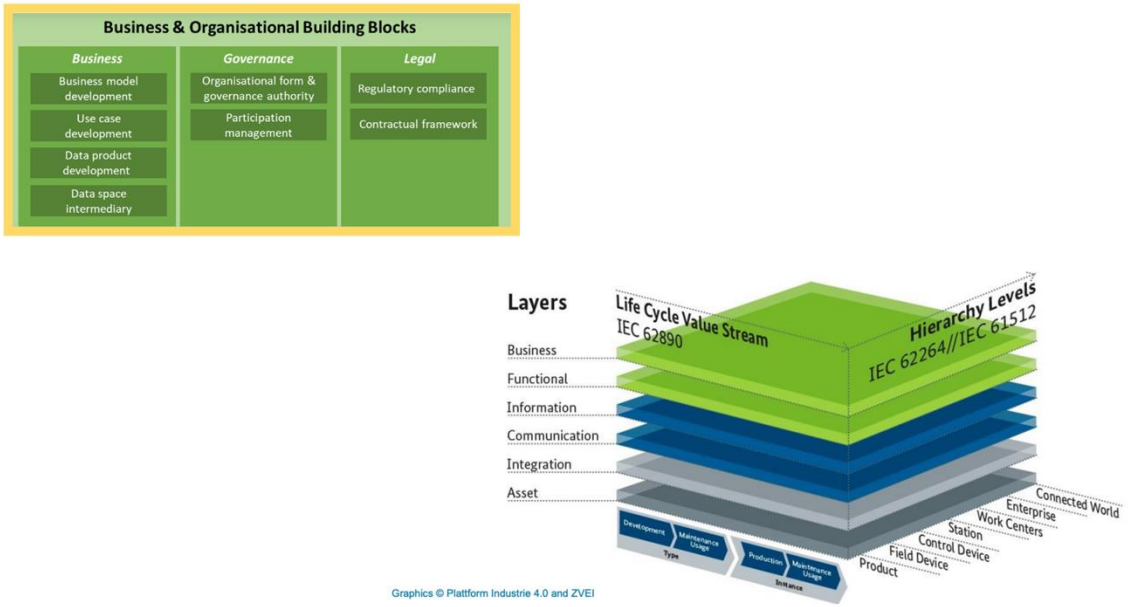

Figure 10. DSSC Taxonomy vs. RAMI 4.0 - Governance Building Blocks

Business Agreements specify what kind of terms and conditions can regulate the sharing of data between participants and the legal framework supporting contracts established through the Data Space.

Operational Agreements regulate policies that have to be enforced during data space operation like, for example, compliance with GDPR (General Data Protection Regulation) or the 2nd Payment Services Directive (PSD2) in the finance sector.

Organisational Agreements establish the governance bodies (very much like ICANN for the Internet). They deal with the identification of concrete specifications that products implementing technology building blocks in a data space should comply with, as well as the business and operational agreements to be adopted.

Despite DSSC provides a deepen analysis and relevance to Data Space Governance Building Blocks, a major focus on the essential Building Blocks on Data Governance have been extensively supported via Work Package 3 “Sustainability Business Models for Data Economy in Manufacturing” activities and has been furtherly detailed under D3.2 “– Business Model (BM) navigator and data space 4.0 maturity assessment model”.

5 Manufacturing Data Space Design and Adoption

The following sub-chapters identify the outcomes of EU DATA SP4CE Work Package 4 activities in terms of Manufacturing Data Space Checklist and Data Space Design Approach.

The following resources would like to guide the Data Space Design processes via a useful checklist, relevant to understand the value pursued by the Data Space per se, and the necessary steps to support the creation of the Data Space and its development phases.

5.1 Checklist to design a Manufacturing Data Space

In this section, we aim to provide some questions, to contemplate and answer when setting up a data space. The questions are derived from the DSSC checklist [5], and initially categorised across five dimensions: business, legal, operational, functional, and technical. Then, considering the specificities of Manufacturing Data Spaces, and the added value to refer them to the RAMI 4.0 model, we introduced a sixth dimension given by the life cycle, mainly to consider one of RAMI 4.0 axis less developed within the Data Sharing Coalition's BLOFT framework [25], adopted by DSSC Starter Kit.

The Checklist supports the design processes of the Manufacturing Data Space following the main items described in Figure 11.

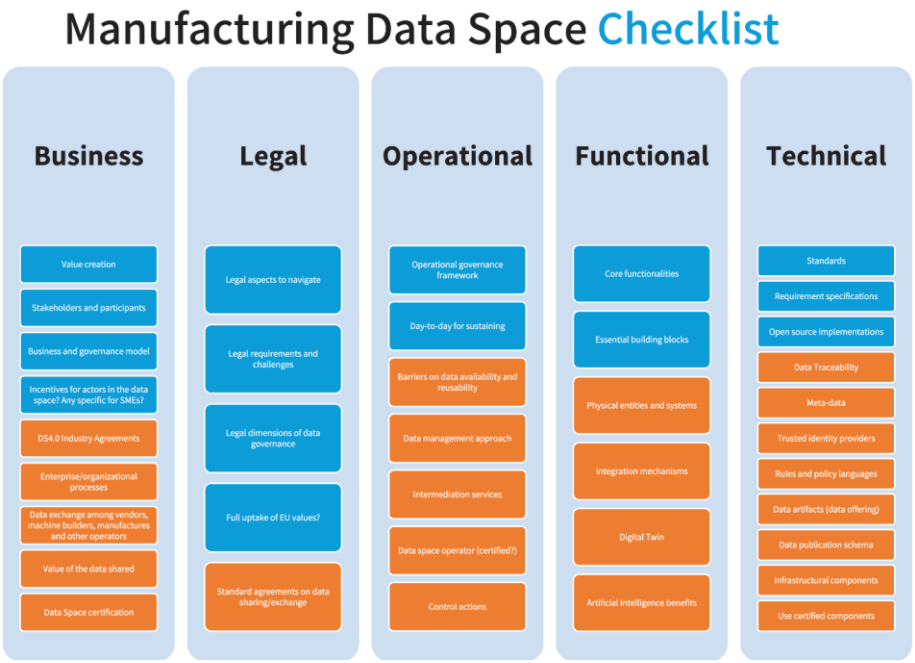

Figure 11. Manufacturing Data Space Checklist

In the following text, we have left the original questions by DSSC Starter Kit in *italic* font, adding new questions or detailing the existing ones to make them more effective for our stakeholders in the manufacturing domain.

- *Business*
  - *How does the data space create value?*
  - *Who are the active stakeholders or participants of the data space?*
  - *What is the business and governance model of the data space?*
  - *What are the individual and collaborative business models (Incentives) for actors in the data space?* Any specific need coming from the SMEs of the target ecosystem?
  - Have you checked the DS4.0 online Repository of Industry Agreements?
  - Which are the enterprise/organisational processes impacted by the data space?
  - Which are the needs for exchanging data among vendors, machine builders, manufactures and other operators in your ecosystem?
  - How would you estimate the impact and value of the data shared? Do you foresee specific methodologies?
  - Are you interested in obtaining a Data Space certification as a “secure” organisation?

- *Legal*
  - *What legal aspects are relevant to navigate when setting up a data space?*
  - *What are the legal requirements and challenges?*
  - *What are the legal dimensions of data governance?*
  - *How can data spaces ensure the full uptake of EU values?*
  - Have you identified standard agreements on data sharing/exchange for users interested in joining the data space?
- *Operational*
  - *What is the operational governance framework for the data space?*
  - *What day-to-day activities and processes are essential for sustaining a data space?*
  - Have you already identified some barriers that may limit data availability and reusability across platforms?
  - What is the data management approach adopted in the target Data Value Chains (DVC)?
  - Which Data space intermediary or Value-added services are in use in your data space?
  - Have you already identified the Data space governance authority, responsible for developing, maintaining, operating and enforcing the governance framework? If yes, do they have any (cyber)security certification? Are they interested in Data Space Organisational Certification?
  - How existing control actions may be augmented using information shared within the data space?
- *Functional*
  - *What core functionality should a data space offer?*
  - *What are the essential building blocks that make up each functionality?*
  - What are the physical entities and systems you have to connect to the data space?
  - What are the integration mechanisms to support your business at tactical/operational/strategic level?

- How Digital Twin (and other simulation/modelling elements) will be integrated in the data space? Are you using DTDL? AAS? Or any other industrial smart data models?
- How Artificial Intelligence applications will benefit from:
  - the data pools available in the data space acting as a data consumer
  - the exchange of AI algorithms/parameters (data prosumer)
  - the sharing of the processed data (data provider)

- *Technical*
  - *What are the formal and de-facto standards that should be followed when deploying a data space?* Are you using OPC UA? MQTT? Others?
  - *What software requirement specifications to use as references when implementing a data space?*
  - *Which opensource software implementations are compliant with the recommended standards and specifications?*
  - Do you need to trace exchanged data and involved participants of the data space?
  - Are you interested to have detailed meta information about data you can access through a data space?
  - In your ecosystem, which are the most used trusted identity providers?
  - What are the rules you plan to apply to your data? Are you familiar with policy languages (e.g., ODRL, XACML, etc.)?
  - What are the data artifacts (data offering) to be shared in the data space by the data providers? What are the related vocabularies (if any) the data consumer needs to process data?
  - In your sector, do you have a well-recognised data publication schema?
  - If needed, are you available to host and manage data space infrastructural components (i.e., identity provider, metadata broker, clearing house, etc.)?
  - Are you going to use existing certified components? If needed, are you interested in the design and implementation of solutions compliant with data space certification requirements?

- Life Cycle
  - How may product/process design benefit from the data space?

- How assets may be connected (at both OT and IT level) to the data space?
- How may manufacturing/supply chain processes be impacted by the data space?
- How may maintenance processes benefit from the data space?

5.2 Manufacturing Data Space Design Approach

Every *Data space initiative* or in general every Data Value Chain (DVC) ecosystem needs to define and adopt specific technologies and a *Data space infrastructure* to deploy and operate a data space, i.e. following a *Data spaces blueprint* that enables all the data sharing/exchange capabilities required for the specific DVCs. This could be a daunting task because:

- Every ecosystem has a unique set of requirements for the data space.
- Building Block implementations are difficult to compare because every vendor provides a unique set of features, adopting emerging (and not yet consolidated) standards and methodologies.
- Several *Data space initiatives* and closed communities are interested in getting as large a footprint as possible.
- Some *Data space component* and their *implementations* of different building blocks offer the same functionalities.
- Some implementations are just not compatible.
- Certification programmes and standards are still far to be adopted in the data space arena.

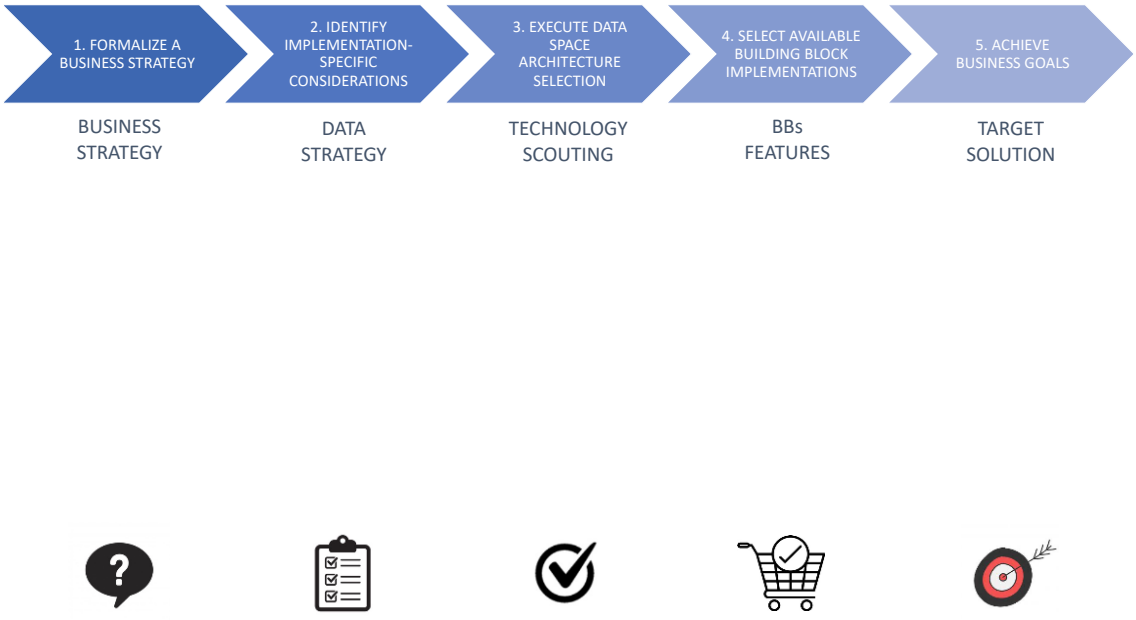

Figure 12. Data Space design approach

Data Space design and adoption start with the analysis and a common agreement on the business goals for the whole federated ecosystem. Building Blocks and their implementations should be based on common best practices and, at the same time, be optimised for the ecosystem's specific needs and they should support an evolutionary (centralised, decentralised, federated, …) data space development.

Understand your current environment and use proven architectural patterns can expedite building the Data Space that matches your needs:

- Use a pragmatic approach, considering that what is best for one organisation may be totally unacceptable for another – all for very valid reasons.
- Understand your goals and priorities.
- Picture your target-state architecture.
- Identify the current technology coverage and maturity level (based on the prioritised business cases to implement).
- Select the software (Building Block implementations) covering the gaps in technology enablement based on feature/functional enablement descriptions as well as vendor and deployment preferences.

6 Data Space 4.0 Blueprint Certification Strategy

The analysis of the existing certification programs performed in Section 6 indicates:

- IDSA model is focused on the certification of "IDS Core Components" and "Operational Environments".

  IDSA has defined a reference architecture model for secure data sharing, implemented by a set of technical core components (Connector, Broker, Daps, Clearing house, App store and Paris). Each of these components implements a defined functionality and a secure data protocol. The certification guarantees that any of those Core Components can be used in a secure and reliable way to deploy an IDS Compliant Space.

  IDSA intends to create a marketplace of IDS Core Components that can be used in an interoperable and secure manner in any specific Data Space.

  IDS Certification Scheme does not cover domain specific requirements or standards (i.e., data models, …).
- CATENA-X has already designed, implemented, and maintains an architecture based on IDS and GAIA-X reference models, focusing only on automotive domain.

  The certification process is focused on guaranteeing functional and technical interoperability of components, applications and service providers operating in that specific data space.

  A component or application certified for CATENA-X does not necessarily meet the requirements of other data space.
- IDSA and GAIA-X incorporate the concept of Security Levels: in these two programs, the requirements and scope of the certification are linked to security requirements of the specific data space.

  This opens an interesting discussion: the possibility to integrate domain specific security requirements to the certification process.

In fact, the three certification programmes are complementary and, in fact, they could be benefited by agreements of mutual recognition. Interoperability between domain-specific data spaces is a crucial issue to avoid silos and develop a real data-driven economy.

A detailed analysis of the three certification programmes has been provided in *Annex II Data Space Available Certification Programmes and relevant Code of Conducts*.

The DSSC describes a Data Space as a composition of building blocks. Each of these building blocks has a well-defined Mission and:

- In the technological related Building Blocks, it is supported/implemented by one/several core or enabling technologies or methods, which are not domain specific. For instance, an IDS Compliant Connector
- It can be customised or configured to meet the specific requirements and standards/regulations of a specific domain. For instance, specific Data Models in the connector.
- Are operated by entities that play different roles. For instance, service providers of Connectors as a service

The assembly of these building blocks on reference architectures that specify a role model and the distribution of building blocks among roles.

A reference certification strategy proposed by Data Space 4.0 should comply with the following objectives:

- Objective 1: Guarantee Trust in all technologies and parties involved in a data sharing process.
- Objective 2: Accelerate the secure and fast design and development of data spaces.
- Objective 3: Market Recognition

The Data Space 4.0 Reference Certification Programme Framework (RCPF) should take into account:

- Be based and supported by reference standards, reference specifications and open specifications. Therefore, it has to provide transparent information on compliance with those standards or specifications.
- Provide transparent information of the area of application and intended used.

- Modular approach, guaranteeing functional and technical interoperability. At the moment, there is no single Reference Architecture and no single set of Reference Technical Components. The Certification and Compliance scheme has to be ready to validate and certify technology against its capacity to be interoperable and operate in a secure manner but without strict limits or constraints in functionality.
- Cover both technology and participants.
- Role-based. No every participant has the same role: data consumer, data provider, service provider or application developer do not have the same impact on the data sharing process. Therefore, the certification scheme for participants has to be role and risk-based.
- Differentiate between Core Components (in the form of interoperable generic enabling technology with a cross-domain applicability) and Domain Specific Applications and Assets. This means that we should distinguish between Certification (cross-domain) and Qualification (domain-specific)
- As far as possible, be compliant and aligned with market standards (i.e., ISO 27001). The data spaces are a new approach to data sharing but many existing standards (at technology and process level) can be used as reference to guarantee the required trust. Let´s use that to avoid extra costs. Mutual recognition of certifications and standards should be taken into consideration.

As a reference Certification Scheme for the Data Space 4.0 Blueprint, Data Space 4.0 takes the Building Blocks as a high-level reference specification and proposes as pathway for mission centric data space certification programme design; i.e. asset management, predictive maintenance, circular economy:

- Step 1: Define and Select Reference Specifications and Standards that support the implementation of each Building Block
- Step 2: Identify Reference Technologies (Core components and generic applications) per building block
- Step 3: Elaborate a Reference Catalogue Criteria and standards criteria per Reference Technology
- Step 4: Develop a certification process

Data Space Certification Program Reference Framework (CPRF) is divided in two type of processes (Certification and Qualification) and three different topics (Core technologies; generic applications and partners), depicted in Figure 24.

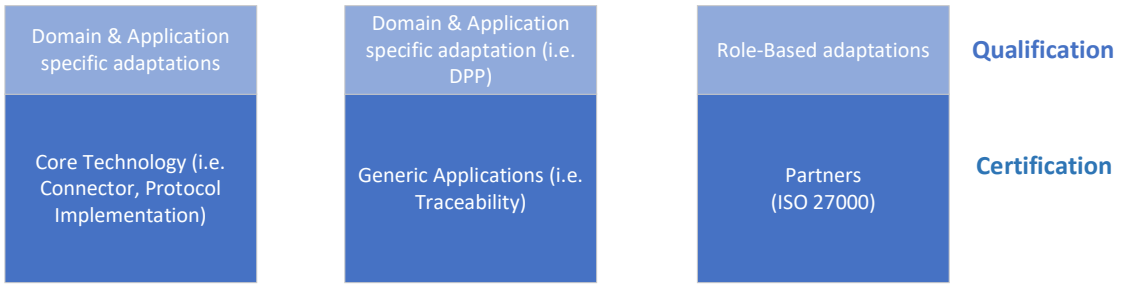

Figure 13. Data Spaces 4.0 Certification Reference Programme

The Processes:

- Certification guarantees domain-agnostic applicability of technology, compliance with the reference specifications of a building block.

  The certification process will be operated by the DSSC and carried out by qualified accredited entities. Certification criteria will be maintained by the DSSC.

- Qualification means compliance with domain-specific requirements or with a specific role, in case of partners.

  The qualification process will be managed by the data space operators or owners. Qualification criteria will be specified at domain level.

The Three Topics

The Certification Framework is focused on different parts of the data space ecosystem/DSSC/Data Space 4.0 environment, and the three of them are necessary to any manufacturing domain.

- Core Technology: all technological components/solutions used in the data space architecture must be certified following the principle of “secure by design”, interoperability capacities and security in operations.
- Generic (Collaborative) Manufacturing Applications: all technological components that provide solutions on top of the data sharing architecture and blueprint.

- Partners: all entities (companies, experts) that play a role in the design, operations and management of a Data Space.

All those certification processes are based on common ground and are composed of a set of requirements that will be extended with the domain specific requirements. All these requirements are selected from several sources:

- Catalogue Criteria: refer to a set of standardised guidelines, best practices, and requirements used to evaluate and assess the effectiveness and quality of testing processes, methodologies, and tools. These criteria help in the certification or accreditation of testing practices and ensure that they meet industry standards. Catalogue criteria are created based on the building blocks defined and industry standards compliance. Catalogue criteria provide a structured framework for evaluating DSSC components, processes, and practices. They help establish a benchmark for quality and competence in testing and are often used in the certification or accreditation of testing professionals and organisations. These criteria contribute to the ongoing improvement of testing processes and the delivery of high-quality software products.
- Industry Standards Compliance: these processes should adhere to recognised industry standards and best practices, such as ISO/IEC 27001 or ISO/IEC 62443. We will select them among the standards related to the specific domain of the certification scope.
- Domain Testing Cases: considering the scope of the certification, several Domain Testing Cases will be created. These cases will be based on specific domain criteria.

Additionally, the certification process should cover:

- Test Documentation: quality of test documentation, including test plans, test cases, test data, and test reports, is assessed to ensure that they are clear, well-structured, and traceable.
- Test Data Management: Adequate provisioning, generation, and management of test data are essential. Catalogue criteria evaluate how well test data is handled to ensure comprehensive testing.

- Risk-Based Testing: The effectiveness of risk assessment and risk-based testing is evaluated to ensure that critical areas of the software are tested rigorously.

7 Applying DS4.0 Blueprint in a concrete Manufacturing Data Value Chain

EU DATA SP4CE Blueprint checklist, as presented in Chapter 5.1, represents a valuable tool for fostering data-sharing collaborations. It focuses on specific use-cases, allowing partners to identify data-sharing needs, define purposes, and outline essential components spanning from business, legal, operational, functional and technical dimensions.

EU DATA SP4CE identified key relevant questions to support the creation and the deployment of a Manufacturing Data Space and support its Data Value Chain. To provide *a concrete Manufacturing Data Value Chain* example*,* the SM4RTENANCE project coordinator [32], representing one of the two deployment projects supported by the European Commission, has been interviewed.

SM4RTENANCE counts 42 full partners, 5 associated partners, distributed across 11 EU countries. The partnership supports the actions calls for deployment of the data spaces, for both discrete manufacturing (e.g. automotive, electronics and e-batteries, machinery tool, textile and aeronautics) and process industry (e.g. steel and aluminum).

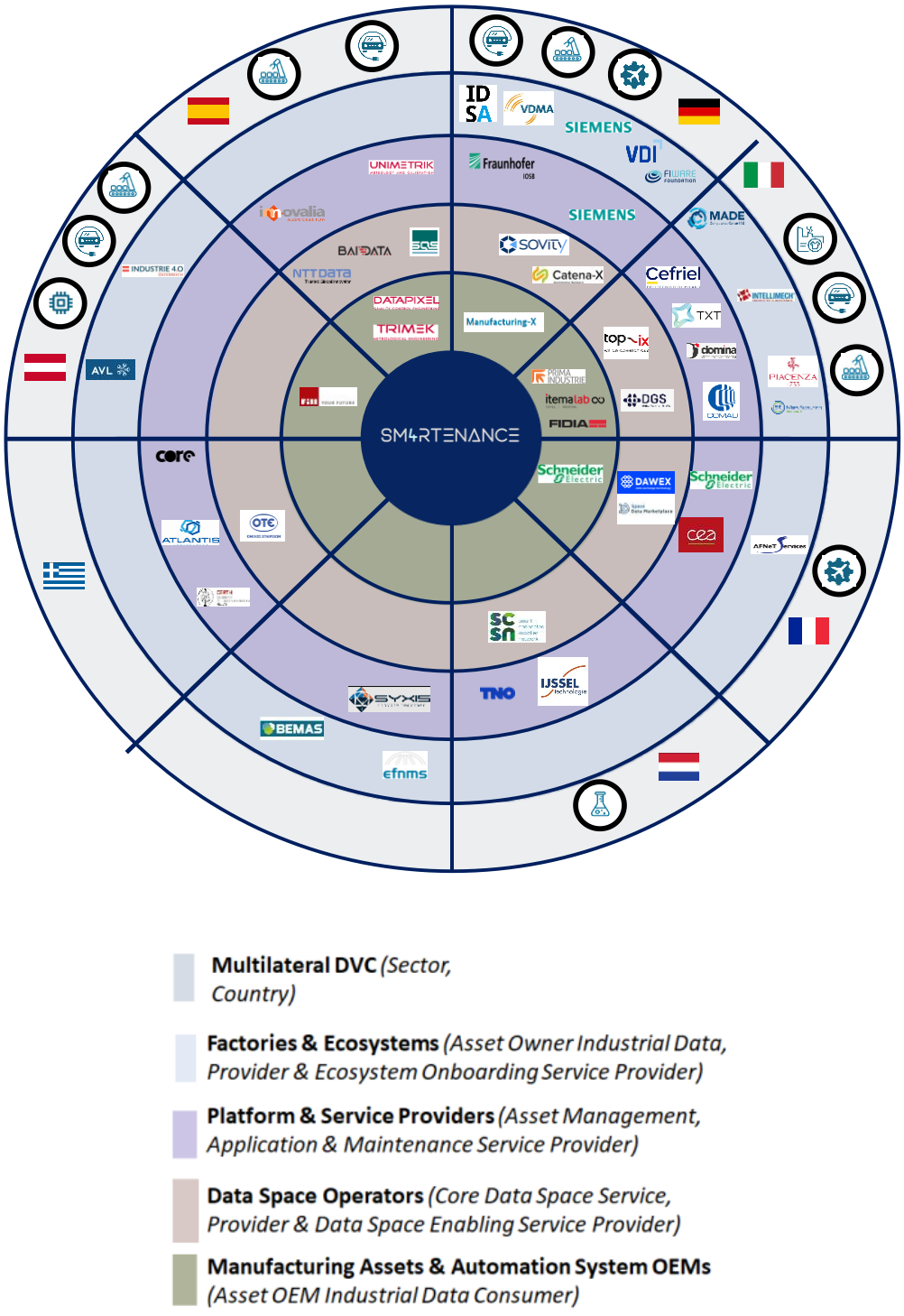

Figure 14. SM4RTENANCE Consortium

As depicted in Figure 23, SM4RTENANCE Consortium demonstrates a well-balanced mix of different Data Service Providers (distinguished in Core Data Exchange Service Providers and DS Enabling Service Provider), Industrial Data Providers (as Asset Owners and Asset & Automation OEM), Asset Management Application & Maintenance Service Providers, and Ecosystem On-Boarding (mainly represented by Consulting Service Provider).

Among SMARTENANCE's activities, different demonstrators will be implemented along multilateral data value chains, encompassing trials in terms of data space federation and in terms of interworking level. These interworking and federation trials are the baseline for the SM4RTENANCE assessment and validation of the data space business application trials roll out of (1) generative co-engineering and commissioning services of manufacturing assets (2) collaborative net-zero operation services (3) cooperative autonomous condition monitoring services and (4) circular asset management services. This should result in increased benefits for the factories facilitating access to data in this trusted environment benefiting from increased asset resilience, lower energy consumption, lower CO2 footprint, optimised OEE and extended asset lifetime by new means of retrofitting and reuse of components and subsystems in manufacturing assets. Furthermore, Data Value Chains will be investigated also in terms of supply chain management.

As key findings from SM4RTENANCE's interview, it must be underlined the Data Space's relevance identified in the field of process optimisation, material resource efficiency, asset resilience, asset energy efficiency, optimised OEE and asset lifetime. The integration of digital twins should be performed through data space connectors, enabling AI services in the Data Spaces. Predictive Maintenance has been deemed as an essential service for SMEs accessing Manufacturing Data Spaces. Furthermore, the Data Space demonstrates its value in designing and running smarter, cheaper and more flexible supply processes.

The definition of a data governance model capable to provide standardised APIs for plug and play on a decentralised federated Operating System for data value chain set-up seems essential in the manufacturing domain. Key relevant principles should be identified to support the Data Space deployment: decentralisation, openness, transparency, sovereignty and interoperability. The latter can be furtherly supported via distributed technologies and shared vocabularies created by different parties.

The complete interview to SM4RTENANCE project is available at Annex I.

Annex I - Data Space 4.0 Interview to SM4RTENANCE deployment initiative

Data Space 4.0 Interview to SM4RTENANCE deployment initiative

1. Data Space 4.0: How does the data space create value to your stakeholders? How would you estimate the impact and value?

SM4RTENANCE: The 80% of industrial data is never used. We still have in our brain the misconception that set of data has only one use. Nowadays the potential of data access and sharing will help companies to create and develop new products and services. For example, the potential value of manufacturing data sharing has been estimated at €83 billion just in the field of process optimisation and better leveraging machine-generated data can lead to up to 20% improvements in material resource efficiency. The total value that companies can create in five key areas of data sharing is estimated to be more than $100 billion according to World Economic Forum white paper. Conceptually the value for stakeholders derived from data sharing services will be in asset resilience, asset energy efficiency, optimised OEE and asset lifetime.

2. Data Space 4.0: Do you foresee individual and collaborative business models (Incentives) for all the stakeholders in your data space? Any specific need for SMEs?

SM4RTENANCE: In the actual socioeconomic context, the big industrial players are transforming their business into a full vertical and horizontal integration of systems and components. We have pioneer projects like Catena-X. The implementation of data space concept inside the companies will let them to be more competitive and more flexible to any market changes. It will be essential to have innovative services like predictive maintenance or autonomy of processes. SMEs should understand as quick as possible the data value chain concept and start playing the game.

3. Data Space 4.0: What are the legal requirements and challenges? Are there any legal requirements on the specific verticals related to your Data Space?

SM4RTENANCE: In general terms, SM4RTENANCE and other projects referring to Data Space must be aligned to the Europe Data governance Act and most recent Data Act.

Basically, legal data aspects of data are fixed in three work lines: legal compass, data governance matrix and smart contractual models.

4. Data Space 4.0: Have you already identified the organisation in charge of operating the data space and acting as a trustworthy data broker? If yes, do they have any (cyber)security certification? Are they interested in Data Space Organisational Certification?

SM4RTENANCE: There are lots of coordination and management challenges. One of the most relevant is to scale up the process from the component or machine at factory level to the Data Space environment. There we already have some embryonic projects like Catena-X, BAIDATA, SCSN, Manufacturing X. It is necessary to articulate and define a model in order to provide standardised APIs for plug and play on a decentralised federated Operating System for data value chain set-up. This is the SMA4RTENANCE vision.

5. Data Space 4.0: What core functionality should a data space offer? Which core services will be provided?

SM4RTENANCE: For a data space to function properly, it is necessary to have sufficient actors to cover a set of roles and a set of technological components. These elements enable a common governance framework to be established for secure data sharing, ensuring the sovereignty of the participants over their own data. In this sense, the EU-funded report "Design Principles for Data Spaces" provides the fundamentals that data spaces should follow to act in accordance with EU values: decentralisation, openness, transparency, sovereignty and interoperability.

6. Data Space 4.0: How Digital Twin (and other simulation/modelling elements) will be integrated in the data space? How Artificial Intelligence applications will benefit from this enriched data ecosystem?

SM4RTENANCE: In discrete manufacturing today, most components are already designed digitally using computer-aided design (CAD) software. Even if manufacturers originate the product design using a CAD model, paper records are still used to document and communicate the actual dimensions of the product created in different production steps. Because records are kept by individual stakeholders along the value chain, in many cases, it is necessary to manually exchange records. Manufacturers must also conduct audits and quality checks to confirm that selected dimensions will meet the tolerances specified. Digital product twins provide a solution to these challenges. These are digital

representations of a product, including its actual dimensions and shape characteristics. A digital product twin expands upon the original CAD model by adding information on actual dimensions and quality from various production steps – creating a merged model of design data and actual characteristics. Yet creating a digital twin that follows the whole life cycle of the product, combining data on components, requires a high level of cooperation and coordination. The integration of digital twins will be through data space connectors.

The AI applications will access a big amount of integrated data so mainly efficacy and efficiency of maintenance works will be improved.

7. Data Space 4.0: What are the data artifacts (data offering) to be shared in the data space by the data providers? What are the related standards and/or vocabularies (if any) the data consumer needs to process data?

SM4RTENANCE: The best way to illustrate this is the DDD (digital Data Package exchange) concept, defined in the following figure:

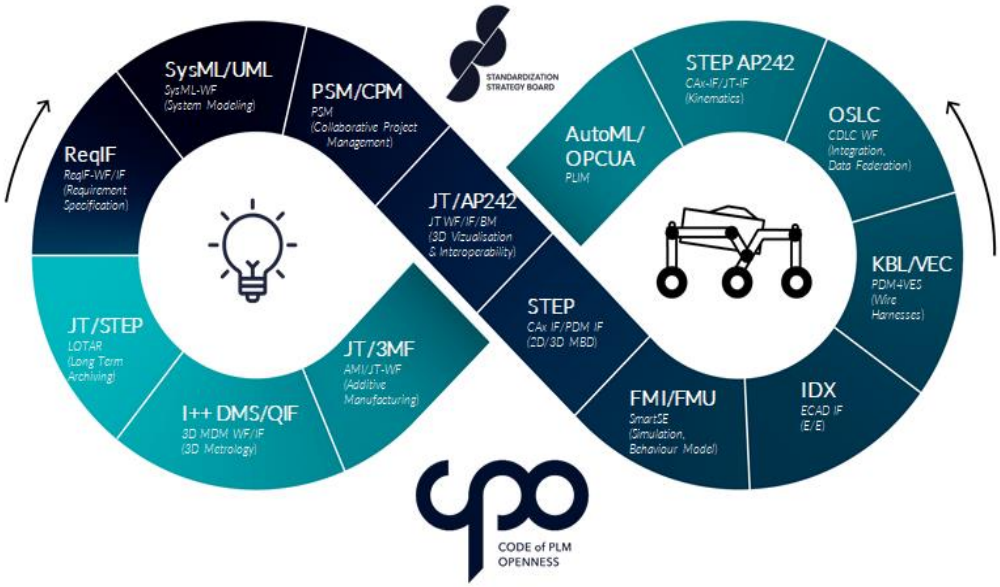

Figure 15. Digital Data Package exchange

Data spaces are expected to be built in a decentralised manner and with distributed efforts, hence necessary shared vocabularies will also be created by different parties. This gives rise to the need of certain governance to ensure the interoperability of the domains involved in the respective use cases and solutions. For example, if a supplier wants to notify a company of an imminent delivery bottleneck, this information should not be published or disseminated in an uncontrolled manner. And data space control and data exchange

technologies could be providing the information in real time to the appropriate managerial team.

1. Data Space 4.0: How may manufacturing/supply chain processes be impacted by the data space?

SM4RTENANCE: Data Space technology will help supply chain analytics to describe the use of new data sources and analytical techniques to help companies design and run smarter, cheaper and more flexible supply processes. One of the most significant benefits is that with data space concept, companies could gain access to better data-driven predictions of obstacles in their supply chain to potentially avoid disruption scenarios altogether. Supply chain disruptions include natural disasters, labor shortages, cyberattacks, and global crises like COVID-19.

In dealing with disruptions like these, for example AI (artificial intelligence) can also be used as a proactive communication tool between shipping partners and their clients in cases of delayed freight by providing weather updates, reasons for delay, or alternate routing in case of unforeseen challenges.

Annex II Data Space Available Certification Programmes and relevant Code of Conducts

Three different certification schemes have been analysed: IDSA Certification Scheme; CATENA-X Certification Programme and GAIA-X Labelling programme. For each scheme the scope and the process are outlined.

IDSA Certification Scheme

IDS is an ecosystem for data exchange. The exchange of data with known and unknown entities requires trust that the recipient of the information will not use it in a way that was not intended. IDS certification provides transparent information about the security level of the communication partner and this information is verified by independent parties (Evaluation and Certification Bodies). Based on this information, IDS participants can sovereignly decide with whom they want to share their data. IDS Certification is therefore the basis for establishing trust and sovereign data sharing in the IDS ecosystem.

This IDS certification is conceived to guarantee trust in the implementation of a data space. However, the first layer of trust is “Trust By design”, where the security concept and associated security requirements, architectures and even technologies, are considered.

The IDS certification scheme has been designed to provide evidence of compliance of technological components and entities with the IDS Reference Architecture Model and the rules and governance Models designed by IDSA.

The IDS Certification Scheme is aligned with the specifications of IDSA.

Scope of the Certification and Certification Schemes

To build a data space we need:

1. Technological components (so-called Core Components) that allow the secure data sharing. In the case of an IDS Architecture, these components are: Connectors, Broker, DAPs, Clearing House and PARIS. Each of them has its own role to implement an IDS Compliant architecture.
2. Entities or Participating Organisations that, using these components, provide data, consume data and/or provide services (for example, provision of digital certificates, infrastructure providers).

The IDS Certification Scheme is designed to provide evidence of "trust" in the technical core components of the infrastructure and Trust in the partners operating those components.

Therefore, The IDS Certification Scheme is composed of two complementary Certification Programmes.

1. The Certification Programme of Core Components: It is designed to validate functionality, interoperability and security aspects. A catalogue criteria per core component exists based in ISO62443-4-2 criteria, complemented with IDS-specific criteria and secure development process.
2. The Certification Programme of Operational Environments: It is designed to guarantee the trustworthiness of the physical environment, processes, and organisational rules of the entity operating a Core Component. It seeks for evidence that the environments are operated under appropriate security practices. It is based on the ISO27001 and the BSI C5 Catalogue [26].

Thinking that not all data spaces will require the same levels of security (sharing health data is not the same as sharing data on the weather conditions of a city) and that not all parties have the same role (data consumer vs service provider of identity), both programs have defined and establish different levels of Trust (specifically 3), with an increasing extent in the security requirements that need to be fulfilled.

Higher Trust Level represent the increasing amount of criteria which needs to be fulfilled for a successful certification.

Additionally, three Assurance Levels are established. Higher Assurance Level represent the increasing demand for more reliable evidence that needs to be presented in different evaluation methods to prove compliance with the certification criteria.

1. Assurance Level 1 is implemented through a Self-Assessment process.
2. Assurance level 2 and 3 the engagement of a third party is required, and the extent of analysis increases with the level.

The next figures show the different Trust and Assurance Levels for Core Components:

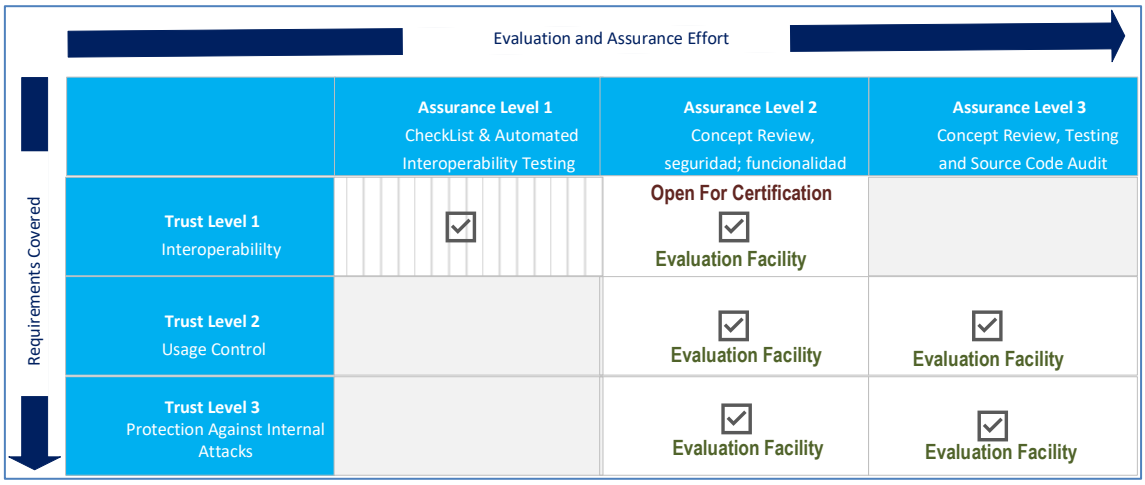

Figure 16. Trust and Assurance Levels for Core Components

Following, relation between Trust and Assurance Levels for Participating Organisations:

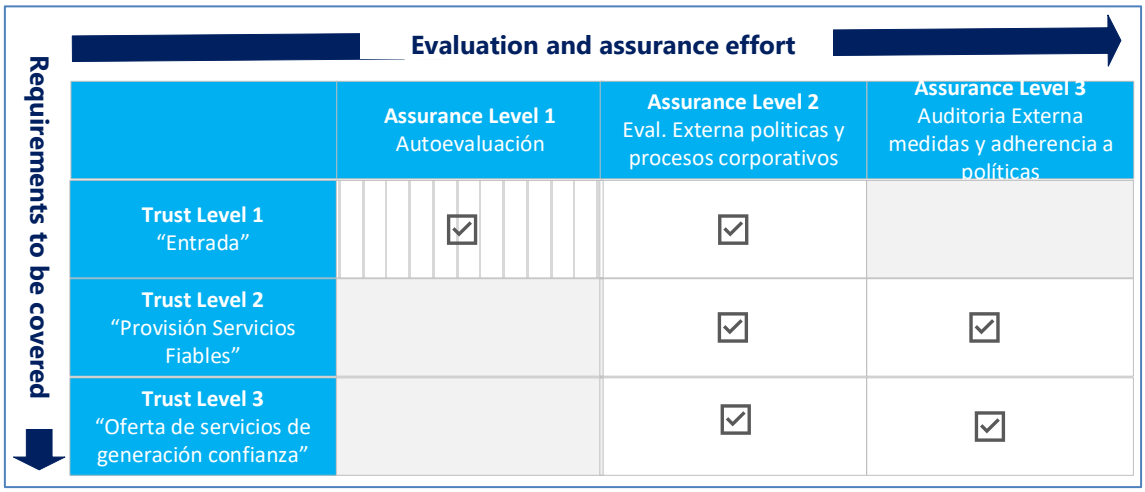

Figure 17. Trust and Assurance Levels for Operational Environments

Trust Levels

Trust Levels in Operational Environments

The operational environment certification defines three different trust levels, with an increasing extent of the security requirements that need to be fulfilled.

- Trust 1: covers only the basic security requirements that every participant of the International Data Space needs to fulfil. The entry level therefore serves as a low barrier for companies (especially SMEs) interested in trying out International Data Space participation.
- Trust 2: covers additional security requirements, ensuring an advanced level of security. This level is suit-able for most core participants.
- Trust 3: includes special security requirements that are necessary for International Data Space participants providing key services within the International Data Space.

Trust Levels in Components

Three different trust levels, with an increasing extent of the security requirements that need to be fulfilled, are defined:

- Trust 1: offers basic security features to protect against attackers from outside, to ensure integrity and availability. It is therefore designed for use in scenarios with only low security requirements. A Connector meeting this profile is suitable for exchanging data with limited trust and security needs, for exchange of data in a contained environment or for demonstration purposes.
- Trust 2: includes strict container isolation, integrity-protected logging, encryption of all persisted data, protection against accidental misuse by administrators. This profile is used for scenarios in which the protection of the processed and transmitted data is essential.
- Trust 3: offers additional protection against misuse of privileged access, i.e., manipulation by administrators. This includes the protection against insider attacks as well as against external attackers who could gain privileged access. This is achieved by actively monitoring users and data on behalf of the data owner.

Certification Process

The actors

Among the certification process, we can find three different actors:

- Certification Body: the Certification Body oversees the certification process regarding quality assurance and framework governance. It defines standard evaluation procedures and supervises the actions of the Evaluation Facilities. A certificate is granted only if both the Evaluation Facility and the Certification Body have concluded that all preconditions for certification are fulfilled.
- Evaluation Facilities: contracted by an Applicant (see below), the Evaluation Facility is responsible for carrying out the detailed technical and/or organisational evaluation work during a certification process. The Evaluation Facility issues an evaluation report for the respective organisation/individual or core component, listing details regarding the evaluation process and an assessment whether all requirements are properly fulfilled. Evaluation Facilities are accredited by IDSA following an accreditation process.
- Applicant: the Applicant is not just the subject of the evaluation and certification process but plays an active part in it. An Applicant needs to actively submit an application to trigger the certification process. This applies to organisations/individuals that develop software components intended to be deployed within the International Data Spaces (i.e., prospective Software Providers) and to organisations that intend to operate components in the IDS. During the certification process, the Applicant provides all necessary material needed for the evaluation and certification of its component or organisation and supports with questions or issues arising.

The process

- Preparation: the organisation must ask IDSA a formal request for the certification. The organisation also needs to have a clear understanding of the IDS specifications and guidelines. The organisation will gather all documentation needed and can perform a self-assessment using the Testbed and the Test Suite before starts the certification.

The component or the operational environment must be ready to initiate the certification process.

- Request: the process starts with a request from the Applicant to the CB and with a negotiation with one of the Evaluation Facilities. Once both contracts are signed, the Evaluation Process can start.
- Evaluation: the Evaluation Facility will perform the testing and validation. This involves working with Applicant and Certification Body. Several tests are performed to ensure that the organisation's infrastructure, systems, and processes conform to IDS standards. These tests are performed based on the catalogue criteria depending on the scope of the certification. The result of the Evaluation is reflected in an Evaluation Technical Report that is submitted to the Certification Body.
- Certification: The certification body reviews the application and the results of the tests. They may also perform additional examinations to verify the assessment. Based on the results of the documentation review, self-assessment, and third-party audits (if conducted), the CA decides regarding certification. If the organisation meets the requirements, the CA issues a certificate as proof of compliance. If the organisation passes the certification review, it will receive IDS certification.

CATENA-X Certification Programme

The Catena-X Automotive network is built on two major principles: Interoperability and Data Sovereignty.

Cross company interactions highly rely on mutual trust. The certifications provide trust via transparency and reliability based on Catena-X standards. By setting up a certification process, Catena-X guarantees that network major principles are considered in every component of the network. From the core service providers to the data. Therefore, certification plays a crucial role in the success of Catena-X by establishing trust and transparency within the network.

Catena-X data ecosystem has defined and maintains a set of standards prescribing how the exchange of data and information in the Catena-X network should work. They are the basis for ensuring that the technologies, components, policies, and processes used are developed and operated according to uniform rules. All standards developed for the Catena-X data

ecosystem are based on the technological and industry-specific requirements of the automotive industry.

The Catena-X Association publishes standards for generic core and enabling services as well as for domain-specific business applications (the so-called KITS). These standards and artifacts form the basis for the development and operation of software components in the Catena-X network to ensure interoperability and data sovereignty between different software components and providers. All relevant standards are accessible in the Catena-X standard library.

Catena-X association is responsible for the standardisation, certification and qualification within the Catena-X data space. Catena-X association does not carry out the conformity assessment process itself, but delegates it to selected conformity assessment bodies (CAB

s). The conformity assessment process can be applied to all certification objects. Only the certification criteria and the certification validity change.

Scope of the Certification and the Qualification

Catena-X certification is done in a modular, role-based way, to fulfill different requirements of participants in the ecosystem, whether IT application providers, service providers or onboarding partners. The modularity allows high flexibility and lowers the efforts and redundancies for all parties involved.

Catena-X issues four different labels to help customers find suitable and legitimate providers for their needs. Each label is issued to the relevant role after achieving successful certification and/or qualification. Labels are associated with the offered services of the provider.

1. Certified Operating Company: Core Service Provider
2. Certified Provider, such as: Onboarding Service Provider, Business Application Provider or Enablement Service Provider
3. Certified Solution, such as Business app or Service
4. Qualified Advisor for Advisory providers

This Certification Process involves the identification of the relevant role, determination of the certification scope, and provision of certification modules, including the required Solution Base and Provider Base.

This modular approach includes specific standards and conformity assessment criteria related to specific areas (Product Carbon Footprint, Sovereign Data Exchange, etc.), known as CXs. All relevant standards and conformity assessment criteria are accessible in the Catena-X standard library.

Based on the role and use case, participant should select the relevant standards from standard library. The use cases describe the concrete benefits within Catena-X. Standards already published are currently divided into:

2. Traceability: continuous data chains over the life cycle.
3. Sustainability: standards and methods for saving CO2.
4. Behavioral Twin: behavioral forecasts from the network.
5. Demand & Capacity Management: fewer bottlenecks, more security.
6. Live Quality Loops: consistency instead of parts tourism.
7. Circular Economy: maximum use of resources.
8. Product Carbon Footprint: primary data for precise CO2 recording.

For the audit and the issuing of the certification, Catena-X relies on proven auditing companies, as conformity assessment bodies (CABs). A CAB must be nominated by the Catena-X Association and comply with the Catena-X certification framework.

A CAB carries out the conformity assessment process in accordance with the Catena-X Certification Framework on behalf of the Catena-X Association. The Certification Framework consists of the certification manual and the certification catalog (derived from the Catena-X standards). A CAB is nominated by the Catena-X Association to ensure an independent, trustworthy, and secure conformity assessment process. A CAB is responsible for:

1. creating offers for the conformity assessments.
2. carrying out the conformity assessment process for various certification objects (e.g., provider, solutions).

3. informing the Catena-X Association and the certification candidate about the certification results.
4. issuing, reissuing, and revoking of certificates on behalf of the Catena-X Association

The Qualification Process applies to Advisory Services. These services are hard, if not impossible, to standardise. Consequently, conformity assessment of qualified advisory services cannot take place through certification. To maintain a consistent level of quality among advisory service providers in the Catena-X data space, the Catena-X Association offers a qualification process that is mandatory for all advisory service providers that want to get listed in the marketplace.

There are two ways to become a Catena-X qualified advisory service provider.

1. Qualification through training
2. Qualification through existing experience

The involvement of a CAB is not required.

The Certification Process

The Catena-X Association creates and publishes the standards that form the foundation of the network. For the audit and certification issuance Catena-X rely on auditing companies, known as Conformity Assessment Bodies (CABs).

The certification process [27] ensures that all participants in the Catena-X network are compliance with the established standards and principles, fostering trust, transparency, and interoperability in cross-company processes within the automotive industry.

- Request: the participant create and submit a certification request to Catena-X via homepage for its software component. Inside this page, all the accredited CABs are listed, in order for the certification applicant to contact the CAB directly, which will send the participant essential information using the CX Standards Conformity Assessment Template, obtaining then the Certification Submission.
- Review of certification request: using the Certification Submission, the CAB reviews the information, regarding the fulfilment of the CX requirements. In case the certification object does not meet the certification criteria, but the request can be

corrected, the CAB will provide assistance for certification. The conformity assessment body helps in resolving shortcomings that can be corrected. Both participant and CAB agree on the scope of the certification project and create the Certification Contract.

- Kick-Off: CAB presents the certification project to the participant, clarifying details and organisation topics about coordination and communication.
- Certification by CAB: The CAB carries out the certification according to the certification framework and informs the applicant about the result. In case of findings that It can be corrected, the participant has the opportunity to revise his application together with the CAB.
- Catena-X approval: the CAB sends to Catena-X and the results of the certification with the adequate feedback (all certification criteria are met) the CAB awards and sends the certification and publish the results on the homepage.

The Qualification Process

As indicated above, there are two ways to become a Catena-X qualified advisory service provider. “Qualification through training” and “Qualification through existing experience”

1. The process the process for Qualification through Training has yet to be established.
2. If a company is interested in Qualification and/or the proof of qualification through Experience, the first step is to contact the Catena-X Association. Further information and a first questionnaire to collect basic information about the company will then be made accessible. The assessment of the questionnaire will be the basis for the qualification.

GAIA-X Labelling Programme

The main objectives of Gaia-X can be summarised as follows:

- Build a new ecosystem for European innovation.
- Create a compelling environment to develop new European digital services.
- Enable the creation of common European data spaces in a trustworthy environment.

- Reduce the dependency from non-sovereign and non-European technologies.

The trust framework is the set of rules that define the minimum baseline to be part of the Gaia-X ecosystem. Those rules ensure a common governance and the basic levels of interoperability across individual ecosystems while letting the users in full control of their choices.

The Gaia-X labelling framework introduced a set of core principles that are being refined by the criteria. The criteria list brings together the policies and requirements from the committees –policies and rules committee, technical committee, data Spaces and business committee –along with comprehensive verification means to ensure that these requirements can be met.

Gaia-X developed a Compliance and Labelling technological Framework automating all the tests and verifications needed to give a service a specific Label. These labels may come in different levels, indicating varying degrees of trustworthiness. These levels represent the trust associated with a particular service provider. These label levels are designed to provide a standardised way to assess and communicate the level of compliance with Gaia-X standards and requirements.

Labelling Criteria

Gaia-X labels reflect the objectives and concepts of the ecosystem. These labels are determined through decisions made by Gaia-X committees and approved by the Board of Directors. The labelling criteria are aligned with Gaia-X's key documents, such as the architecture document, policy rules document, and principles for data spaces.

Label Level 1

- Compliance Criteria: This level ensures compliance with basic requirements related to data protection, transparency, security, portability, and flexibility.
- Source of Requirements: These requirements are based on the rules defined in the Gaia-X Policy Rules Document and a set of technical requirements derived from the Gaia-X Architecture Document.
- Cybersecurity: For cybersecurity, the minimum requirement is to meet ENISA's European Cybersecurity Scheme - Basic Level [28].

Label Level 2

- Compliance Criteria: This advanced label extends the basic requirements from Label Level 1 and includes a higher level of security and transparency regarding applicable legal rules and potential dependencies.
- Service Location: The option of a service location in Europe must be provided to the consumer.
- Cybersecurity: For cybersecurity, the minimum requirement is to meet ENISA's European Cybersecurity Scheme - Substantial Level [28].

Label Level 3

- Compliance Criteria: This level aims to meet the highest standards for data protection, security, transparency, portability, and flexibility, as well as European control.
- Requirements: It extends the requirements of Label Levels 1 and 2 and includes criteria that ensure immunity to non-European access and a strong degree of control over vendor lock-in.
- Service Location: A service location in Europe is mandatory at this level.
- Cybersecurity: For cybersecurity, the minimum requirement is to meet ENISA's European Cybersecurity Scheme - High Level [28].

These labels offer a clear way for consumers to understand the level of data protection, security, and other attributes provided by a service or solution within the Gaia-X ecosystem. The detailed criteria for each level are found in the Gaia-X Labelling Criteria Catalogue, which is composed of different attributes categorised under data protection, transparency, security, portability, flexibility, and European control. This catalogue can be updated periodically to reflect evolving standards and requirements.

Gaia-X labels can be extended to meet new requirements, including country and domain-specific needs. Extension profiles can add and define additional criteria for specific purposes. The authorisation of new labels and extensions is the responsibility of the Gaia-X Association.

Gaia-X labels are issued and verified in a federated manner. The concept of modularity allows the reuse of existing certifications. Verification processes within Gaia-X are based on a federation of responsibilities.

Labelling Framework

The Gaia-X Labelling Framework is designed to provide a standardised way of assessing and certifying the trustworthiness of digital services and data hosting providers within the Gaia-X ecosystem. It aims to help users and organisations make informed decisions when selecting service providers for data storage, processing, and other digital services.

Service providers within the Gaia-X ecosystem can voluntarily apply for trust labels to demonstrate their commitment to meeting certain standards and criteria related to data protection, security, and compliance.

Verification of the label criteria can be done through self-assessment or external Conformity Assessment Bodies (CAB). Verification includes the use of W3C verifiable credentials. The list of trusted verifiable credential issuers is maintained in the Gaia-X registry.

The framework defines a set of criteria and requirements that service providers must meet to obtain trust labels. These criteria typically encompass data protection, security, and regulatory compliance. Some of the specific criteria may include:

- Data Protection: Compliance with data protection regulations, such as GDPR in Europe, and the ability to provide data sovereignty and control to the users.
- Security: Implementation of robust security measures, including encryption, access control, and auditing.
- Interoperability: Ensuring that the service or data is compatible with other services and data sources within the Gaia-X ecosystem.
- Data Portability: Allowing users to move their data between different service providers within the ecosystem without encountering data lock-in.

The certification process is typically carried out by independent third-party organisations or certification bodies. These organisations assess the service providers' adherence to the criteria specified in the framework. The Gaia-X Association reserves the right to select its own CAB for its basic labels. A detailed document will be issued on the process for choosing

relevant CAB. When Gaia-X lacks reference to accepted standards, it will define a dedicated verification process and appoint an adequate CAB.

References

[1] A. Poikola, B. Verdonck, R. Joosten, T. Guggenberger and S. Salminen, "DSSC Glossary," September 2023. [Online]. Available: https://dssc.eu/space/BVE/357073672/DSSC+Glossary.

[2] “OPEN DEI Project,” [Online]. Available: https://www.opendei.eu/.

[3] “Data Space Business Alliance,” [Online]. Available: https://data-spaces-business-alliance.eu/.

[4] “Gaia-X - European Association for Data and Cloud AISBL,” [Online]. Available: https://gaia-x.eu/.

[5] "BDVA - Big Data Value Association," [Online]. Available: https://www.bdva.eu/.

[6] “FIWARE Foundation,” [Online]. Available: https://www.fiware.org/.

[7] “IDSA - International Data Spaces Association,” [Online]. Available: https://internationaldataspaces.org/.

[8] “DSSC – Data Space Support Centre,” [Online]. Available: https://dssc.eu/.

[9] “EFFRA - European Factories of the Future Research Association,” [Online]. Available: https://www.effra.eu/.

[10] “Connected Factories 2,” [Online]. Available: https://www.connectedfactories.eu/.

[11] “Manufacturing-X Initiative,” [Online]. Available: https://www.plattform-i40.de/IP/Navigation/EN/Manufacturing-X/Manufacturing-X.html .

[12] “Brainport Industry “Factories of the Future” program,” [Online]. Available: https://www.brainportindustries.com/en/factoryofthefuture.

[13] "Brainport Industries Campus - official website," [Online]. Available: https://www.brainportindustriescampus.com/en/.

[14] "Funding and Tender Opportunities Portal - Data space for manufacturing (deployment) Call for Proposals," [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cloud-ai-03-ds-manuf.

[15] “European Data Market Study 2021-2023,” IDC and the Lisbon Council Research, 2022.

[16] "DataBench project," [Online]. Available: https://www.databench.eu/.

[17] DIGITALEUROPE, “Manufacturing data-sharing as driver for sustainability in Europe,” 2021.

[18] P. Gronlier, J. Hierro and S. Steinbuss, “DSBA Technical Convergence document,” 2023.

[19] L. D. Nagel L., Design Principles for Data Spaces. Position Paper. Version 1.0., Berlin: , 2021.

[20] "EBSI Trusted Issuers Registry," [Online]. Available: https://api-pilot.ebsi.eu/docs/apis/trusted-issuers-registry/v4#/.

[21] "iShare - Trust Framework for Data Spaces," [Online]. Available: https://ishare.eu/.

[22] “DFA - Digital Factory Alliance,” [Online]. Available: https://digitalfactoryalliance.eu/.

[23] "IDS RAM 4.0," [Online]. Available: https://docs.internationaldataspaces.org/knowledge-base/ids-ram-4.0. [Accessed 28 March 2023].

[24] “Data Space Support Centre checklist,” [Online]. Available: https://dssc.eu/space/SK/35586053/2+Data+Spaces+Start-up+Checklist.

[25] “Data Sharing Canvas - A stepping stone towards cross-domain data sharing at scale,” Data Sharing Coalition, 2021.

[26] “Cloud computing C5 criteria catalogue,” [Online]. Available: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html#:~:text=The%20C5%20(Cloud%20Computing%20Compliance,providers.

[27] “CATENA-X Certification Programme,” [Online]. Available: https://catena-x.net/en/catena-x-introduce-implement/certification.

[28] “European Cybersecurity Certification Scheme,” [Online]. Available: https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework.

[29] "Digital Factory Alliance - Innovation Catalogue," [Online]. Available: https://digitalfactoryalliance.eu/innovation-catalogue-2/.

[30] “IoT-Catalogue.com,” [Online]. Available: https://www.iot-catalogue.com/.

[31] "International Data Space Association - Data Space Radar," [Online]. Available: https://internationaldataspaces.org/adopt/data-space-radar/.

[32] "SM4RTENANCE project," [Online]. Available: https://sm4rtenance.eu/.