D2.1 REFERENCE ARCHITECTURE FOR CROSS-DOMAIN DIGITAL TRANSFORMATION V1

14 October 2020

Abstract

This report corresponds to Deliverable D2.1 of the "WP2 - OPEN DEI cross-Industry Digital Platforms federation" of the OPEN DEI project and provides useful insights to the most relevant work in the field of Reference Architecture for building Digital Platforms to support the Digital Transformation journeys in the four sectors targeted by OPEN DEI (i.e. manufacturing, agriculture, energy, and healthcare).

The State of the Art presented in Chapter 2 describes general purpose architectures as well as standard architectures, while Chapter 3 presents some examples of relevant projects in the fields addressed by OPEN DEI. Chapter 4 represents the foundation of the OPEN DEI Reference Architecture Framework (RAF) specifications, defining the underlying principles, the interoperability needs and the first release of the RAF specifications.

The OPEN DEI RAF will be built upon 6 main underlying principles (INTEROPERABILITY, OPENNESS, REUSABILITY, AVOID VENDOR LOCK-IN, SECURITY&PRIVACY, SUPPORT TO A DATA ECONOMY) and following a 6C Architectural Model.

The insights described here will be then used in later activities of the OPEN DEI project (e.g. the cross-domain Task Forces), while further advances and lesson learnt will be captured in the next iteration of this report due by M24 (May 2021).

D2.1 REFERENCE ARCHITECTURE FOR CROSS-DOMAIN DIGITAL TRANSFORMATION V1

Work Package	WP2 - OPEN DEI cross-Industry Digital Platforms federation
Task	T2.1 Cross-domain Digital Transformation Reference Architecture
Due Date	31/05/2020
Submission Date	29/09/2020
Version	2.0
Type	Report
Dissemination Level	Public
Deliverable Lead	Engineering Ingegneria Informatica S.p.A.
Authors	Angelo Marguglio (ENG)
Reviewers	Jesús Martínez Gadea (ATOS), Silvia Castellvi (IDSA)
Project website address	www.opendei.eu

Keywords

Reference Architecture Framework, Reference Architecture, Digital Platform, Digital Twin, Asset Administrative Shell, Digital Transformation, Digitizing European Industry, Openness, Reusability, Security, Interoperability

Disclaimer

This document reflects the authors view only. The European Commission is not responsible for any use that may be made of the information this document contains.

CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

Within OPEN DEI, Task 2.1 aims at harmonizing and coordinating different Digital Transformation (DT) approaches under a common **Reference Architecture Framework** (RAF), which combines knowledge and tools to foster effective sharing and assessment of experiences and lessons learned on how systems supporting DT can be architected, crossing the boundaries of specific applicative sectors. Reference models represent, in fact, a common structure and language to describe and specify system architectures and, therefore, are beneficial to enable common understanding and lay down the foundations for achieving interoperability between applications running on top of platforms, as well as the portability (replicability) of applications across platforms, complying with the reference architecture. In the architectural definition of a Digital Platform, the alignment to these reference models is positive because they provide a basis for the standardization of relevant technical elements across the lifecycle of systems, from development, through integration, to operation. Thus, the definition of reference architecture models provides the right orientation to system architecture definitions, fosters component integration, and provides the basis for a dialogue towards collaboration with relevant organizations, as well as for dissemination and internationalization of a technical vision.

This report aims to investigate and identify the current practices (including definition, concepts, processes, models, and templates) for the development of a Reference Architecture Framework relevant to the four sectors targeted by OPEN DEI (namely Manufacturing, Energy, Healthcare and Agrifood), as well as providing recommendations (based on the identified principles) to successfully design and operate Digital Platforms supporting DT journeys.

The following list tries to summarize the main challenges addressed by this report:

- **Problem space**: Digital Platform building activities of interest in the Innovation Actions dealing with Digital Transformation paths.
- **Mission statement**: Systemically develop a coherent set of instruments for exploiting knowledge sharing among sectors on standard and project-related reference architectures.
- **Vision statement**: In 2-3 years, the majority of new Innovation Actions active in the DT area will use the OPEN DEI RAF to achieve a common understanding and communication of the overall system among its diverse stakeholders, which will aid in system deployment and significantly enhance system interoperability across industrial sectors.

The State of the Art presented in Chapter 2 describes general purpose architectures as well as standard architectures, while Chapter 3 presents some examples of relevant projects in the fields addressed by OPEN DEI. Chapter 4 represents the foundation of the OPEN DEI Reference Architecture Framework (RAF) specifications, defining the underlying principles, the interoperability needs and the first release of the RAF specifications.

The insights described here will be then used in later activities of the OPEN DEI project (e.g. the cross-domain Task Forces), while further advances and lesson learnt will be captured in the next iteration of this report due by M24 (May 2021).

1 INTRODUCTION

The digital economy, defined by fundamental changes in the characteristics of information, computing, and communications, is now the preeminent driver of economic growth, social change, and sharing economy. In the digital economy, platform models have strongly proliferated over the past years, providing services on the top of technological building blocks used as a foundation to deal with competitive pressures.

From an economic viewpoint, Digital Platforms are restructuring the global economy, contributing to the digitalization of organizations, value chains and whole sectors, by resetting entry barriers, changing the logic of value creation and value capture. From a commercial viewpoint, Digital Platforms ease the creation of ecosystems of stakeholders, supporting new forms of innovation and value creation, as well as related business and commercial models, focused on Digital Platforms' underlying vision and value proposition.

In 2016 the European Commission started the Digitizing European Industry initiative (DEI) aimed to reinforce the EUs competitiveness in digital technologies. The European Commission strategy defines four pillars[1]: Digital Innovation Hubs, regulatory framework, skills, and Digital Platforms. The EU has launched several calls in the Horizon 2020 program to advance in the development of digital platforms like DT-ICT-07 2018–2019 and 2019–2020 with a budget over €100 M. As an example, digital platforms in the manufacturing sector play a key role in addressing competitive pressures and integrating new technologies, apps and services. The challenge is to make full use of new technologies that enable manufacturing businesses, particularly mid-caps and small and medium-sized enterprises (SMEs) to meet the requirements of evolving supply and value chains. Besides Innovation and Research actions there are also Coordination and Support Actions in order to cross-fertilize the industrial platform communities, facilitating the adoption of digital technologies from ongoing and past research projects to real-world use cases and encouraging the transfer of skills and know-how between industry and academia. Within this context, Digital Transformation (DT) has been largely recognize as one of the most important preconditions for EU industries to fully benefit from the adoption of new technologies.

This report tackles different Digital Platform building approaches under a common **Reference Architecture Framework** (RAF), which combines knowledge and tools to foster effective sharing and assessment of experiences and lessons learned on how systems supporting DT can be architected, crossing the boundaries of specific applicative sectors. Reference models represent, in fact, a common structure and language to describe and specify system architectures and, therefore, are beneficial to promote common understanding and system interoperability. In the architectural definition of a Digital Platform, the alignment to these reference models is positive because they provide a framework for the standardization of relevant technical systems, from development, through integration, to operation. Thus, the liaison with reference models provides the right orientation to system architecture definitions and fosters component orchestration, collaboration with relevant organizations, and internationalization.

[1] European Commission. Pillars of the Digitising European Industry Initiative. 2018. Available online: https://ec.europa.eu/digital-single-market/en/pillars-digitising-european-industry-initiative (accessed on 3 April 2019).

2 DT REFERENCE ARCHITECTURES: A STATE OF THE ART

This chapter presents the most known Reference Architectures, used in several sectors and in most of the cases enabling Digital Transformation pathways for their adopters. The first examples refer to Domain-Specific Reference Architectures (DS-RA), even if some of them are also used cross-sectors; then we will move toward more general-purpose architectures and reference frameworks.

2.1 Reference Architectural Model Industrie 4.0 (RAMI 4.0)

The Reference Architectural Model Industrie 4.0 (RAMI 4.0) was developed by the Platform 4.0 in 2015 and focuses on the IoT and Cyber-Physical Systems (CPS) in the industrial manufacturing domain. RAMI4.0 is a three-dimensional model, which describes the Industrie 4.0 space and organizes the lifecycle/value streams and the manufacturing hierarchy levels across the six layers of the IT representation of Industry 4.0. It outlines a comprehensive view of manufacturing related implications to any IoT landscape. The primary topic, the integration of the physical asset and its digital representation, is proposed relying on a common representation called the Administration Shell.

Reference models, such as the Reference Architecture Model for Industry 4.0 (RAMI 4.0), provide a solution-neutral reference architectural model for applications that make use of Internet of Things (IoT), big data analytics, and other technologies advancements in manufacturing processes, what is known as smart manufacturing, intelligent manufacturing, or simply Industry 4.0. One of the main objectives once adopted is to be able to communicate the scope and design of the system, to foster collaboration and integration with other relevant initiatives by framing the developed concepts and technologies in a common model.

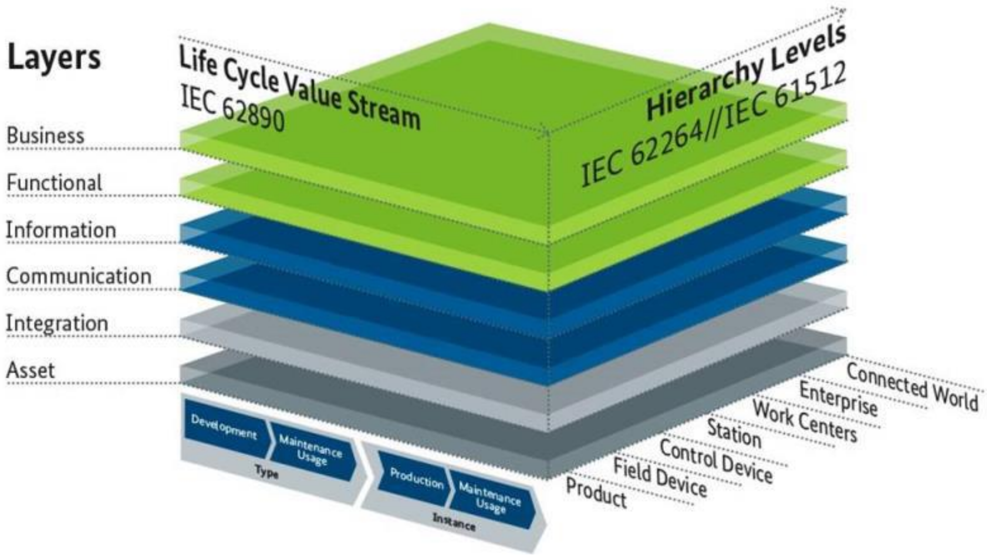

FIGURE 1. THE THREE DIMENSIONS OF THE RAMI 4.0 (SOURCE: PLATFORM I4.0 AND ZVEI)

The three-dimensional matrix can be used to position standards and describe use-cases. It addresses integration within and between factories, end-to-end engineering and human value-stream orchestration. This model is complemented by the Industrie 4.0 components and both have been described in DIN SPEC 91345[2].

In RAMI4.0, each component consists of six layers. Starting with the lowest layer, the structure consists of asset, integration, communication, information, functional and business and represents a layered IT system structure, as shown in the figure below.

[2] Reference Architecture Model Industrie 4.0 (RAMI4.0) - DIN SPEC 91345:2016-04. (2016). Retrieved from https://www.din.de/en/wdc-beuth:din21:250940128

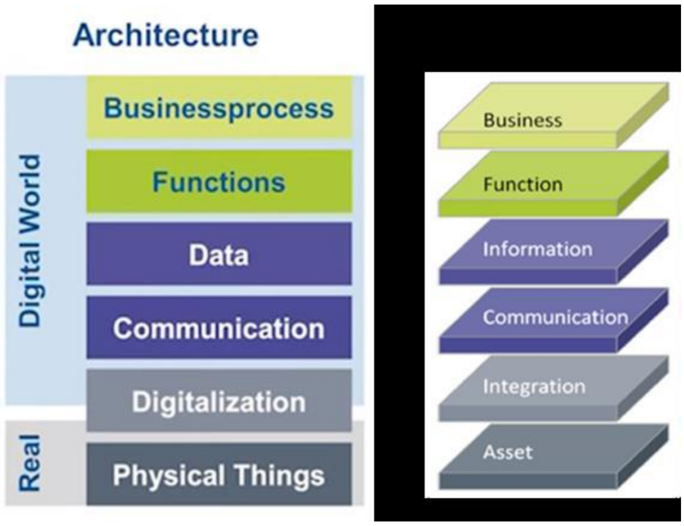

FIGURE 2. THE IT LAYERS OF RAMI 4.0 (SOURCE: PLATFORM I4.0 AND ZVEI)

The function of each layer is:

- The asset layer describes the physical components of a system, for example production equipment, product part, sensors, documents, as well as humans. For every asset represented in this layer there must be a virtual representation in the above layers. Among the physical assets, this layer includes the digital interface with humans and the relationship to elements in the integration layer.
- The integration layer deals with easy to process information content and can be considered as a bridge between the real and the IT world. It contains all elements associated with the IT, including field buses, HMIs, necessary to implement a function, as well as the properties and process related functions required to use an asset in the intended way and generates events based on the acquired information.
- The communication layer is responsible for the standardized communication between integration and information layer. Therefore, it performs transmission of data and files and standardizes the communication from the Integration Layer, providing uniform data formats, protocols and interfaces in the direction of the Information Layer. It also provides services to control the integration layer.
- The information layer holds the necessary data in a structured and integrated form and provides the interfaces to access this structured data from the functional layer. It is responsible for processing, integrating and persisting the data and events, as well as for describing the data related to the technical functionality of an asset. It can be considered the run-time environment for Complex Event Processing (CEP) where rule-based (pre-) processing of events takes place, data APIs and data persistence mechanisms. So, events are received from the communication layer, transformed and forwarded accordingly.
- The functional layer describes the logical and technical functions of an asset providing a digital description of its functions and a platform for horizontal integration of various functions; it also describes the business model mapping, business processes which can be adjusted based on inputs from the functional layer, providing models with runtime data of processes, functions and applications.
- The business layer is in charge to orchestrate the services provided by the functional layer. It maps the services to the business (domain) models and the business process models. It also models the business rules, legal and regulatory constraints of the system. The processes to ensure of the economy are located on this level.

In order to represent the Industry4.0 needs, the functionalities of IEC62264 have been expanded to include two new levels, at the bottom, the "product" (both the type and the instance, through the entire lifecycle) which are active elements within the production system due to their ability to communicate. They provide information on their individual properties and necessary production steps. At the top there is the "connected world", which represents its outer networks or the ecosystem, e.g. collaboration with business partners and customers, suppliers or service providers, as well as Internet-based services.

This allows moving from the typical pyramid, with rigid hierarchical structures, to a composite of networked objects and systems as reflected in the figure below.

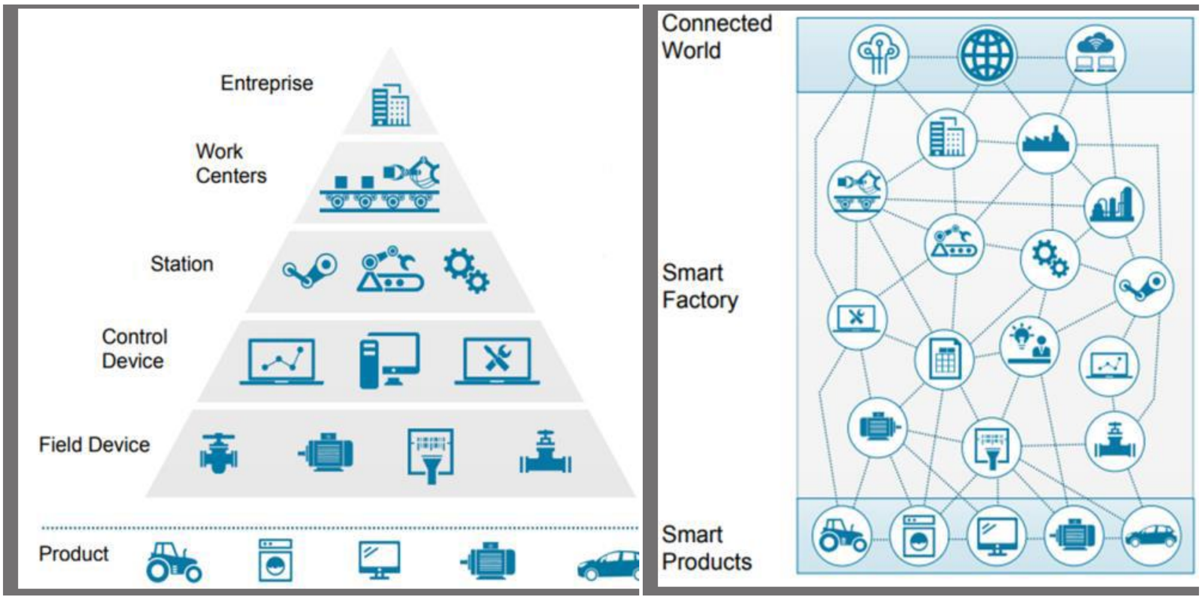

FIGURE 3. HIERARCHY LEVELS OF INDUSTRY 3.0 AND RAMI 4.0 (SOURCE: PLATFORM I4.0 AND ZVEI)

Asset Administration Shell

The Asset Administration Shell (AAS) is a standard model aiming to create a bridge between the real world and the IoT world integrating assets into the world of information.

An asset is everything that can be connected for implementing an Industrie4.0 solution (i.e. machinery, parts, supply material, documents, contracts, etc.). The AAS also defines the data models for the exchange of information between partners in the value chain (see Figure 4) and a package file format (the Asset Administration Shell Package, AASX), to exchange the full or partial structure of the administration shell.

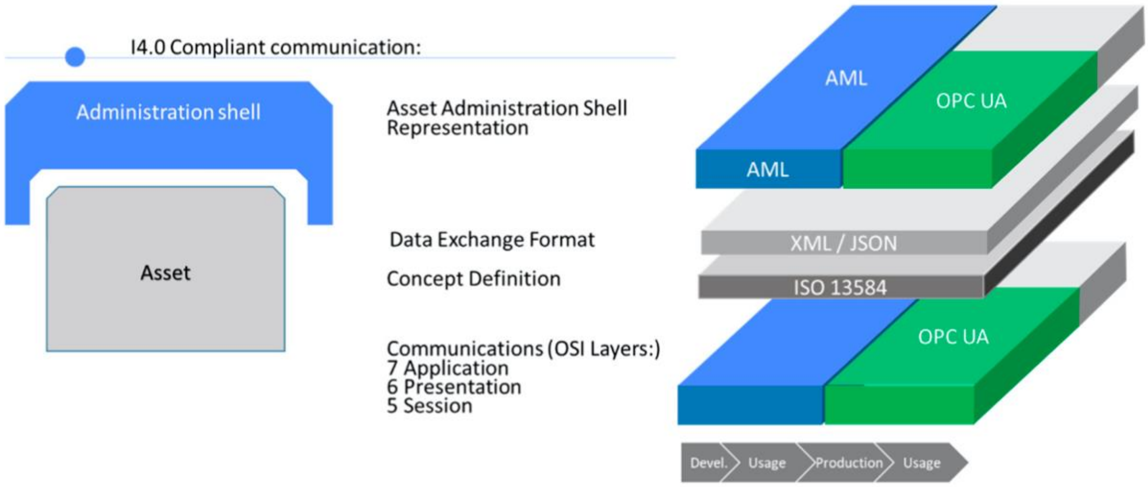

FIGURE 4. I4.0 COMMUNICATION PROTOCOL STACK

The AAS implements the Digital Twin concept meeting requirements of different use cases coming from several domains guaranteeing:

- **Interoperability**, companies can communicate and exchange information
- **Availability**, for every kind of product (non-intelligent and intelligent)
- **Integration** of value chains
- **Covering** of the complete life cycle of products, devices, facilities, etc.
- **Basis** for autonomous systems and AI

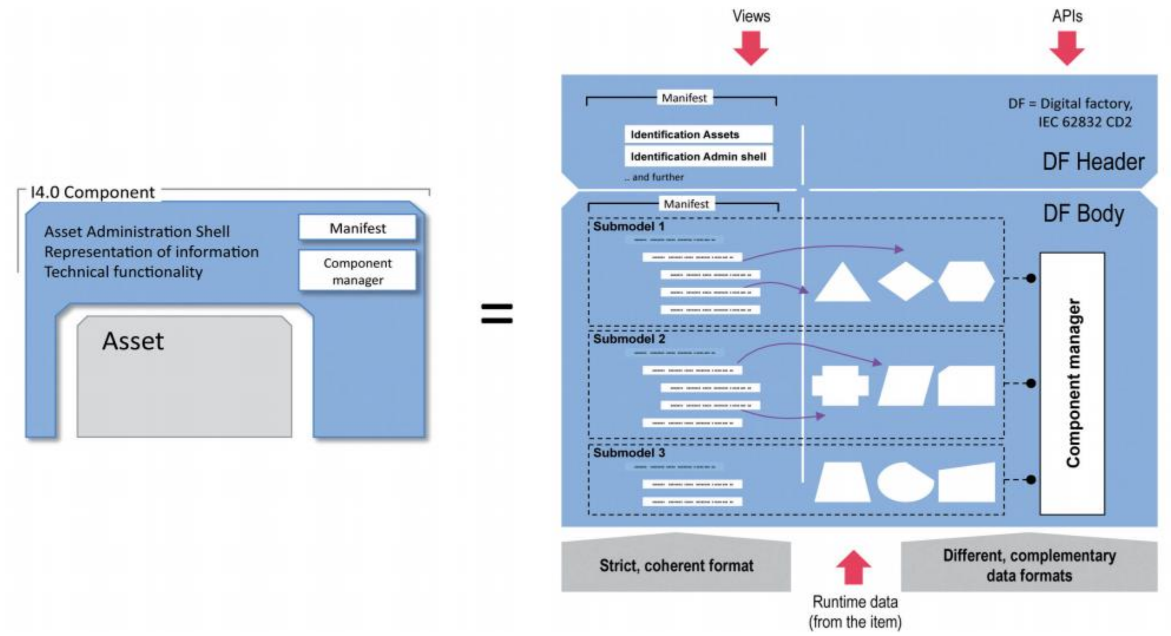

FIGURE 5. ASSET ADMINISTRATIVE SHELL

The AAS can be provided in different implementation variants:

- **Passive** for example if the information is provided using a file or with IP/API-based access. In that case, the requested AAS is provided using a client/server pattern.
- **Active** corresponds to the peer-to-peer interaction pattern. The Administrative shells can communicate with each other using the Industry 4.0 language.

Starting from the above classification AAS implementation can be assigned in the RAMI4.0 Model covering different layers[3].

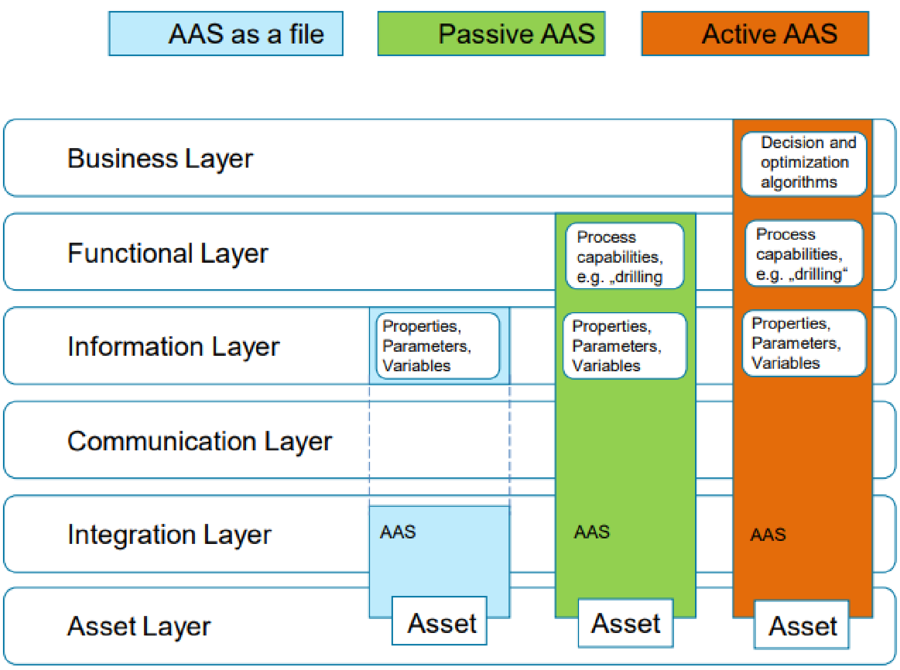

FIGURE 6. ASSIGNMENT OF THE ACTIVE AAS IN THE RAMI4.0-MODEL

[3] Belyaev, Alexander & Diedrich, Christian. (2019). Specification "Demonstrator I4.0-Language" v3.0.

Benefits: Defining different layers for both the life cycle value stream and the hierarchy, RAMI4.0 is able to describe and support different user perspectives, use cases and standards. RAMI4.0 offers more potential to various stakeholders in industrial production.
Risks: The RAMI4.0 supports different standards in different layers. Regarding the communication layer, the OPC UA is the de facto standard, however companies can use unofficial or internal standards. Furthermore, there are some inconsistencies regarding the concept of the Layers and how the Hierarchy Levels fit to the Life Cycle & Value Stream. Finally, the role of processes and how they should be mapped to the framework are subject to further research[4].

2.2 Industrial Internet Reference Architecture (IIRA)

The Industrial Internet Reference Architecture (IIRA) has been published by the Industrial Internet Consortium (IIC) in the document "The Industrial Internet of Things Volume G1: Reference Architecture"[5] and contains architectural concepts, vocabulary, structures, patterns and a methodology for addressing design concerns. The document identifies the fundamental architecture constructs and specifies design issues, stakeholders, viewpoints, models and conditions of applicability defining a framework by adapting architectural approaches from the ISO/IEC/IEEE 42010-2011 Systems and software engineering - Architecture description standard.

This international standard outlines the requirements regarding a system, software, and enterprise level architecture. The ISO/IEC/IEEE 42010 standard recommends identifying the perspectives of the different stakeholders that can be: system users, operators, owners, vendors, developers, and the technicians who maintain and service the systems. The aim is to describe system properties as seen from their viewpoint. Such properties include the intended use and suitability of the concept in terms of its implementation, the implementation process itself, potential risks, and the maintainability of the system over the entire lifecycle.

IIC addresses concerns about IIoT across industries broadly, while RAMI4.0 focuses mainly on manufacturing in depth. Essentially, the IIRA attempts to identify the most important and common architecture concerns. It then provides an architectural template and methodology that engineers can use to examine and resolve design issues. In addition, the template and methodology suggest ways of addressing the top concerns, allowing designers to glean insights by examining architecture patterns, helping Industrial Internet of Things (IIoT) system designers to avoid missing important architecture considerations and this also helps them to identify design gaps of missing important system functions or components.

IIRA represents an architectural template to categorize IIoT system requirements and design concrete architectures to address them. Using this common approach to architecture design, IIRA assists in consistent architecture implementation across different use cases in various industrial sectors meeting unique system requirements. The core of the IIRA's methodology lies in a set of system conceptualization tools called viewpoints that enable architects and engineers to identify and resolve key design issues. Thus, the IIRA design starts with defining the shapes and forms of an Industrial Internet of Things Architecture by starting with the viewpoints of the stakeholders. These IIRA's viewpoints are arranged in a particular order to reflect the pattern of interactions that occurs between the four elements, because the decisions from a higher-level viewpoint impose requirements on the viewpoints below it. In this sense, the IIRA is a layer model that takes into consideration four different viewpoints (business, usage, functional, and implementation). It focuses on the capabilities from the perspective of the software and their business processes. Each of the four viewpoints outlined in IIRA can be compared with the respective layers on the vertical axis of RAMI 4.0; RAMI 4.0 supplements the model with the axes 'Lifecycle' (with types and instances) and 'Hierarchical Levels'.

[4] J. Frysak, C. Kaar and C. Stary, "Benefits and pitfalls applying RAMI4.0," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, 2018, pp. 32-37, doi: 10.1109/ICPHYS.2018.8387633.
[5] The Industrial Internet of Things Volume G1: Reference Architecture Version 1.9. (2019, June 19). Retrieved from https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf

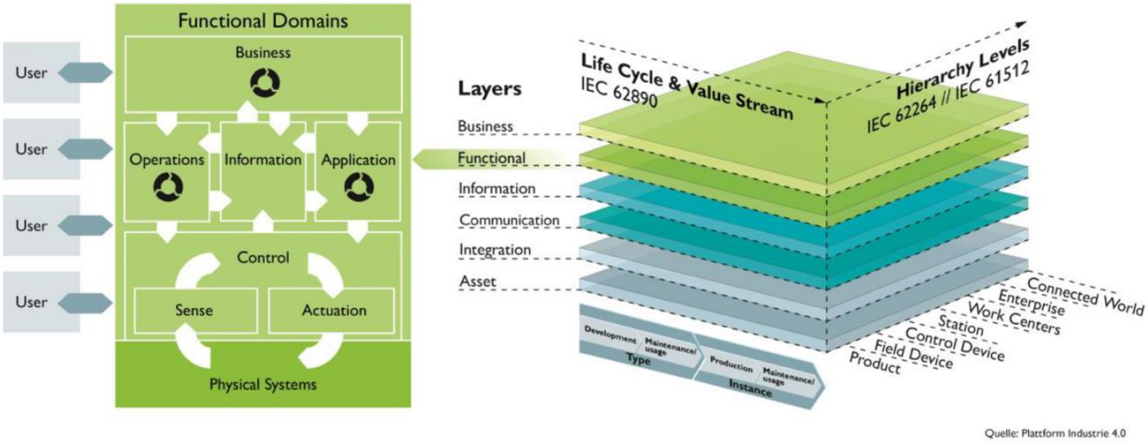

FIGURE 7. THE VIEWPOINTS OF THE IIRA CAN BE REPRESENTED IN THE CORRESPONDING LAYERS IN THE RAMI 4.0 MODEL

The IIoT technologies core implemented in IIRA are applicable to the depth and breadth of every small, medium and large enterprise in manufacturing, mining, transportation, energy, agriculture, healthcare, public infrastructure and virtually every other industry. In addition to IIoT system architects, the plain language of IIRA and its emphasis on the value proposition and enablement of converging Operational Technology (OT) and Information Technology (IT) enables business decision-makers, plant managers, and IT managers to better understand how to drive IIoT system development from a business perspective.

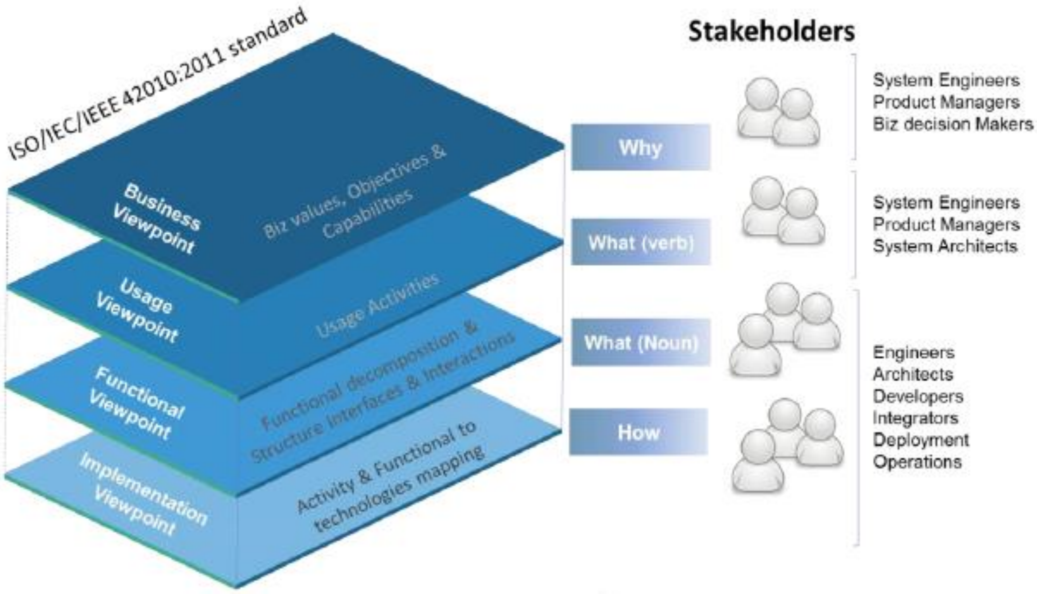

FIGURE 8. IIRA ARCHITECTURAL FRAMEWORK

Security Framework (IISF)

Additionally, if the design of the IIoT solution requires considerations within the context of all the viewpoints - crosscutting concerns- as for example security and safety issues, it exists the cross-cutting functions and the system characteristics. The figure below illustrates the relationship between functional domains, cross-cutting functions and system characteristics.

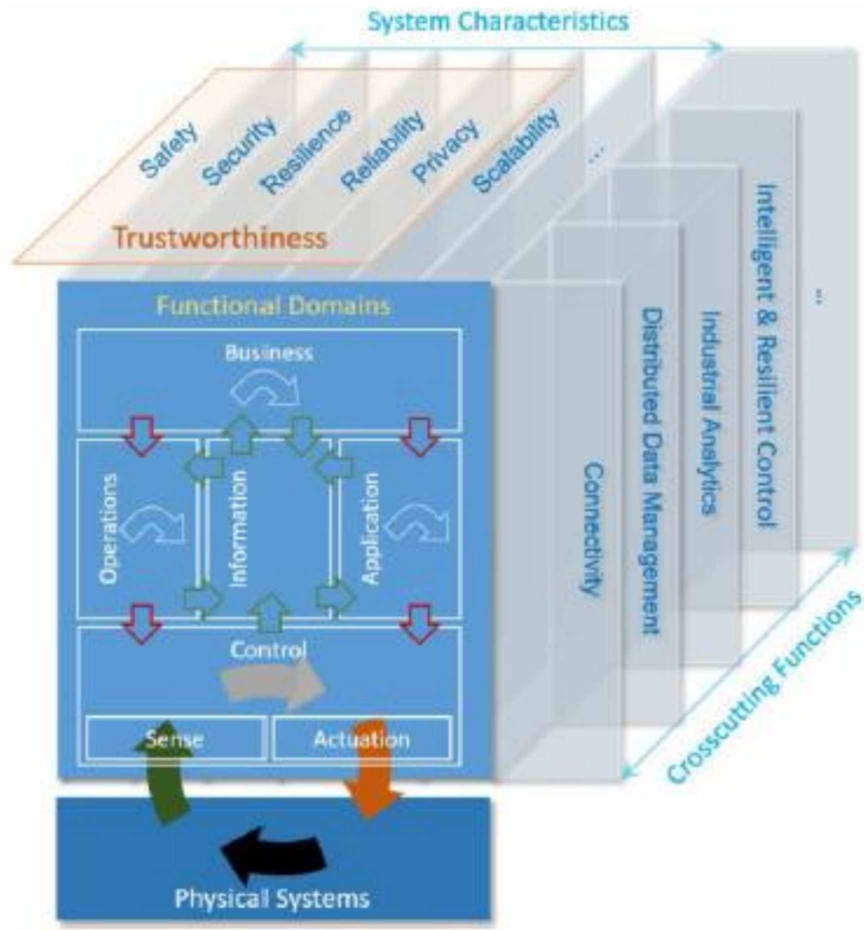

FIGURE 9. IIRA FUNCTIONAL DOMAIN, CROSSCUTTING FUNCTIONS AND SYSTEM CHARACTERISTICS (SOURCE IIC)

IIoT systems are typically systems that interact with the physical world where uncontrolled change can lead to hazardous conditions. This potential risk increases the importance of safety, reliability, privacy and resiliency beyond the levels expected in many traditional IT environments.

The "Industrial Internet of Things Volume G4: Security Framework"[6], published by the Industrial Internet Consortium (IIC), identifies, explains and positions security-related architectures, designs and technologies, as well as identifies procedures relevant to trustworthy Industrial Internet of Things (IIoT) systems. It describes their security characteristics, technologies and techniques that should be applied, methods for addressing security and how to gain assurance that the appropriate mix of issues have been addressed to meet stakeholders' expectations.

Benefits: IIRA aims at a comprehensive model of the industrial internet, independent of specific domains and industries[7]. The wide scope results in a broad coverage of topics being able to make compliant with various IIoT architectures. The main IIRA categorization is based on the aforementioned ISO/IEC 42010, introducing the four viewpoints Business, Usage, Functional and Implementation.
Risks: IIRA concrete implementation guidelines are only partly provided. Furthermore, IIRA lacks an explicit set of addressed concerns. While major concerns can be extracted by analyzing the viewpoint descriptions, a specific allocation of concerns to viewpoints is not given. This results in a certain vagueness of requirements for IIoT implementations.

[6] Industrial Internet of Things Volume G4: Security Framework - IIC:PUB:G4:V 1.0:PB:20160926. (2016). Retrieved from https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

[7] Bader, S.R., Grangel-Gonz´alez, I., Tasnim, M., Lohmann, S.: Structuring the Industry 4.0 Landscape. In: International Conference on Emerging Technologies and Factory Automation (ETFA). pp. 224–231. IEEE (2019)

2.3 Industrial Value Chain Reference Architecture (IVRA)

The Industrial Value Chain Reference Architecture (IVRA) is a similar initiative to the previous ones, the IIRA and RAMI 4.0, but coming from Japan and led by the Industrial Value Chain Initiative (IVI). The IVRA provides three perspectives to understand manufacturing industry as a whole: The knowledge/engineering flow, the demand/supply flow and hierarchical levels from the device level to the enterprise level.

A key element is the introduction of Smart Manufacturing Units (SMUs) in a way that allows to smoothly integrate human beings as elements with their autonomous nature – paying tribute to the fact that it is the human being who discovers a problem, defines a problem, and solves a problem in many cases not only in the past, but also in the foreseeable future.

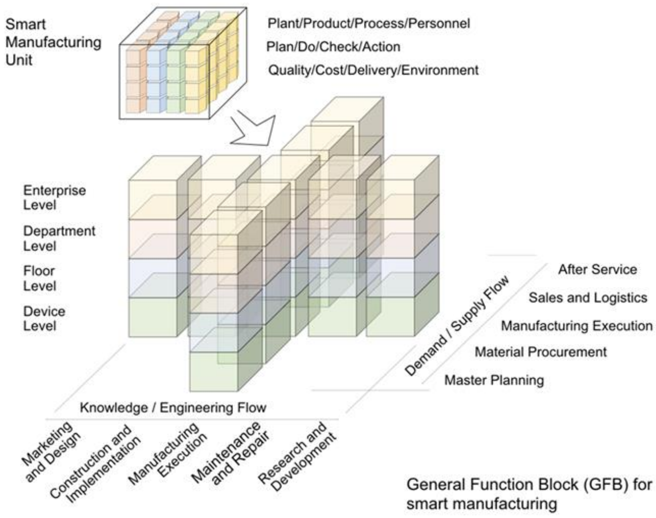

FIGURE 10. INDUSTRIAL VALUE CHAIN REFERENCE ARCHITECTURE (SOURCE: IVI)[8]

The Industrial Value Chain Reference Architecture (IVRA), consists of Smart Manufacturing Units (SMUs) and Portable Loading Units (PLUs). SMU has three views: asset view, management view, activity view. Kaizen approach can be realized in the activity view of an SMU where PDCA cycles perform for continuous improvement.

In order to implement IoT/ICT system in a manufacturing enterprise, it is necessary to keep interoperability among IoT devices, applications, data storages, and related tools. In order to achieve interoperability among such digital components, IVRA also addresses reference models of IVI platforms. The concept of Loosely Defined Standard (LDS) is applied in management of interoperability between IVI components, in which data commonality cannot be fixed unless improvement of the system as a whole is terminated.

Using LDS, IVRA allows the factory managers to describe scenarios of daily operations and inter-relations between actors. Then an SMU can be defined as a set of models including Actor, Activity, Thing, Information, Logic and Data. The talk also illustrates the procedure of bottom-up system improvement of a cyber-physical SMU. Factory floor managers, production engineers and chiefs of workers make some operational scenarios from their actual concerns. Then the scenarios are redesigned using data and logics in the cyber world. Assigning appropriate services provided by platform component suppliers to the data and logics, an IVI platform gives interoperability framework to those components.

Industrial Value Chain Initiative (IVI) provides a software tool, IVI modeler in order to facilitate a common understanding and defining scenarios and terms. Models defined by the IVI modeler can play a key role in integrating the physical world and cyber world.

In order to make collaboration and win-win relation among platformers, component suppliers, system integrators and factory managers, general rules of profile specification and distribution are identified. Since the platformers and component suppliers have their own data models and interfaces, IVI proposes a profile publication framework and a common dictionary for specifying the profiles in accordance with the concept of LDS.

---

[8] https://iv-i.org/docs/doc_161208_Industrial_Value_Chain_Reference_Architecture.pdf

Therefore, since the domain is very complex and consists of heterogeneous subsystems that can be combined in different ways including interchange, there is a need for introducing an architectural pattern which supports an abstract and composite view on the functionalities of the system as a whole (Platform of Platforms[9]). The following figure provides such a view inspired by Industrial Value Chain Reference Architecture.

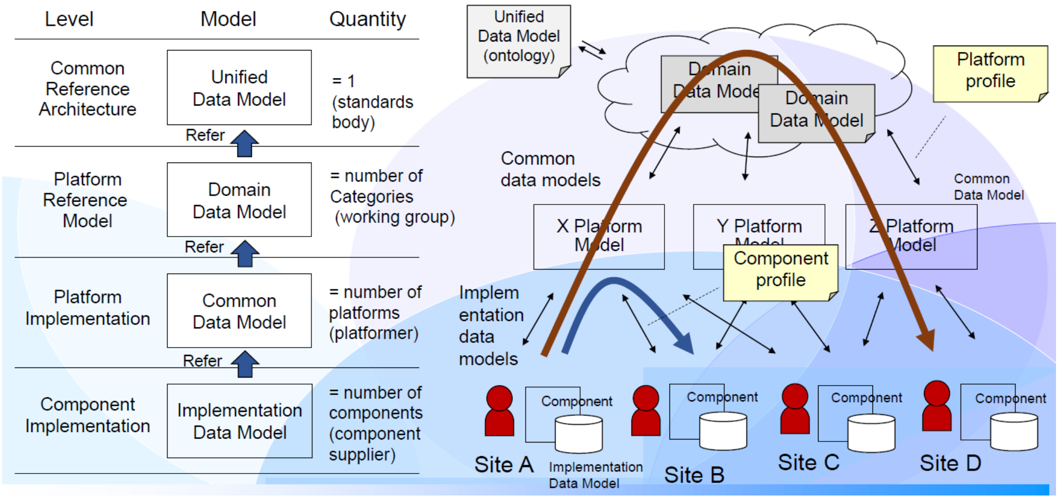

FIGURE 11. HIGH-LEVEL INTEROPERABILITY VIEW (SOURCE: INDUSTRIAL VALUE CHAIN INITIATIVE)[10]

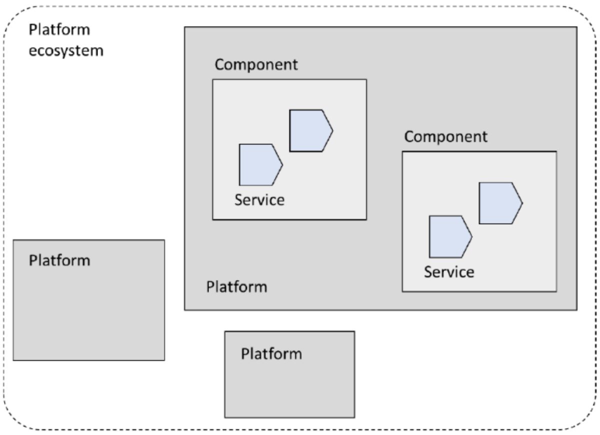

FIGURE 12. THE ANATOMY OF THE PLATFORM (SOURCE: INDUSTRIAL VALUE CHAIN INITIATIVE)

Platform ecosystem

A platform ecosystem is a state in which different constituent platforms are loosely connected by some relations. Each platform in an ecosystem is its constituting element but it is not in the position of being able to control the ecosystem. Thus, a platform ecosystem as a whole is made up based on autonomous decision makings of individual platforms.

A **platform** is a unit which beforehand ensures or supports interoperability of its components by some rule or terms. A manager of a platform (platformer) has two aspects: It collects components constituting the platform; and at the same time, it provides a service gathering users who actually utilize the platform for manufacturing.

Components include software that are designed in advance and meet a quality level to be provided as products as well as necessary hardware's. A component has some function independently which can be provided to users. But in many

[9] https://www.avnet.com/wps/wcm/myconnect/onesite/97cedd40-2ea0-414e-a091-6d844b70a487/IBM-The-Platform-of-Platforms-IoT.pdf?MOD=AJPERES&attachment=true&id=1488926185691
[10] https://iv-i.org/en/docs/Industrial_Value_Chain_Reference_Architecture_170424.pdf

cases, it is needed to connect to other components in order to execute its function. Connection among components is precisely what platforms exist for, so it is discussed at the level of platforms. The topic is explained later in this chapter.

A **service** is a unit of software that constitutes a component. It provides customers with values directly or indirectly. If a connection of services is within a component, it is provided in a form defined by the component in advance.

There are four categories of components:

- IoT device
- Application
- Service tool
- Data infrastructure

Regarding the Hierarchy of System Connection, it specifies the following:

- **Connection among Services**
  A service is a unit and its result can be evaluated by physical users or upper level users in the management layer. Connections at this level are managed by individual components.
- **Connection among Components**
  A component is a unit of multiple services which are tightly coupled. Mutual connections of components are ensured in the range assumed by the suppliers. Thus, connections among components are conducted by the users or platforms.
- **Connection among Platforms**
  In most cases, connections among platforms are autonomous decentralized systems without core management functions. Thus, it is not basically ensured connections are correctly made. However, it is possible to connect multiple platforms as an ecosystem when the platforms agree with a unified rule, terms or connection procedures.

There are two forms for interconnections of components: tight coupling inter-operation and loose coupling inter-operation.

1. Tight coupling inter-operation, the tight coupling inter-operation is a form of connection that components mutually boot a service of the other component and utilize it by using API (Application Programming Interface) and SDK (Software Development Kit). This type enables speedy and high-quality connections but has a task in serviceability for example when a function of one of the components is extended.
2. Loose coupling inter-operation (message-oriented middleware), the loose coupling inter-operation is a form which minimizes effects of future function extension of the other component as well as enables components' own function extension by losing the degree of a coupling between components. API protocols in the lower implementation level are limited to versatile ones which are already widely diffused.

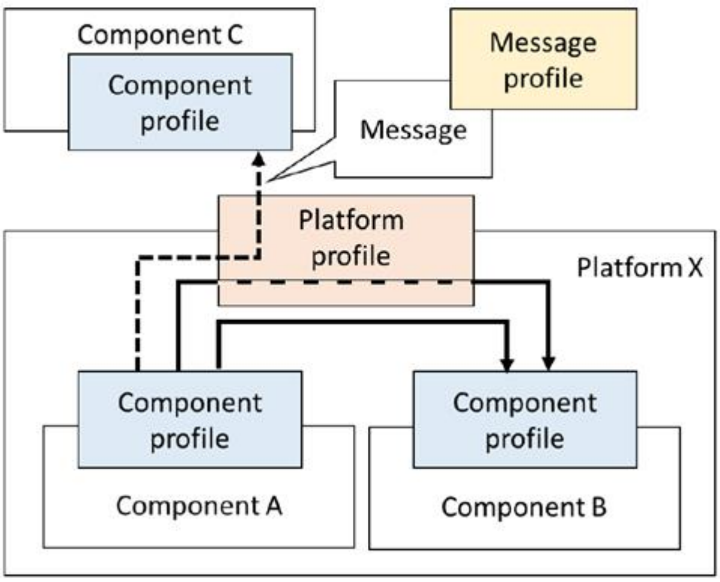

FIGURE 13. COMPONENTS INTERCONNECTION (SOURCE: INDUSTRIAL VALUE CHAIN INITIATIVE)

Benefits: The Digital Twin concept is very well described: as mentioned above, PLUs can contain a physical thing or product but also data and transaction information, therefore creating a general bracket for any transaction in both the physical and the virtual world.
Risks: In the IVRA architecture, data security and interoperability methods are less prioritized in comparison to the modeling and description of processing activities and operations.

2.4 FIWARE Open Source Reference Architecture

FIWARE[11] is a curated framework of open source platform components (also referred as Generic Enablers – GE-) which can be assembled together and with other third-party platform components to build "powered by FIWARE" platforms that accelerate the development of interoperable and portable (replicable) Smart Solutions in multiple application domains.

FIWARE tries to manage the data within a given smart vertical solution or break the existing information silos within a smart organization by supporting access to a Context / Digital Twin data representation that manages at large-scale all relevant information. FIWARE NGSI is the RESTful API used by context data providers and consumers to publish and access Context / Digital Twin data. This can be realized by interacting with the Context Broker, which is a central component of FIWARE architecture implementing the FIWARE NGSI API. The API is not only used by applications but also provides the means for integrating FIWARE components among themselves and with 3rd party software.

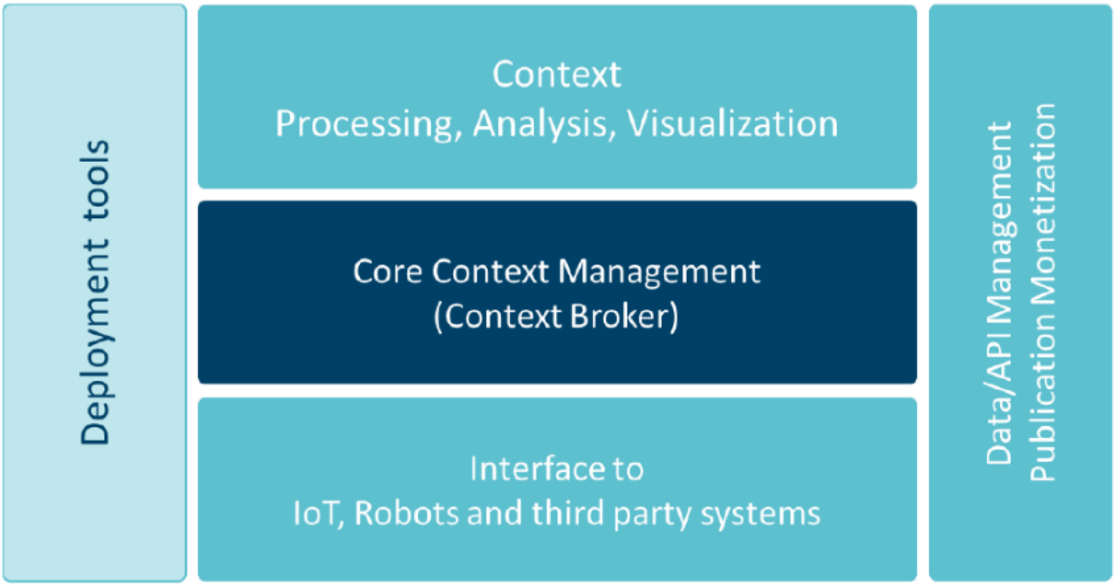

FIGURE 14. FIWARE OVERALL ARCHITECTURE

FIWARE GEs are organized in chapters as depicted in the figure above[12]. The main and only mandatory component of any "Powered by FIWARE" platform or solution is the FIWARE Context Broker Generic Enabler, which brings a cornerstone function in any smart solution: the need to manage Context / Digital Twin information, enabling to perform updates and bring access to it.

Building around the FIWARE Context Broker, a rich suite of complementary FIWARE components are available, dealing with:

- **Interfacing with the Internet of Things (IoT), Robots and 3rd Party systems**, for capturing updates on context information and translating required actuations.
- **Context Data/API management, publication, and monetization**, bringing support to usage control and the opportunity to publish and monetize part of managed context data.
- **Processing, analysis, and visualization of context information** implementing the expected smart behavior of applications and/or assisting end users in making smart decisions.

[11] FIWARE developers catalogue. (n.d.). Retrieved from https://www.fiware.org/developers/catalogue/
[12] FIWARE developers page. (n.d.). Retrieved from https://www.fiware.org/developers/

The catalogue contains a rich library of components with reference implementations that allow developers to put into effect functionalities such as the connection to the Internet of Things or Big Data analysis, making programming much easier. FIWARE core platform model facilitating IaaS and SaaS required of application domains, on this basis GEs applications achieve already defined standards, provide APIs for interoperability, represent application domains or design granularities. We can think of a GE as macroscopes were the highest level interface is a simple controller providing a wide and in scope view of operations (attributes control functions of a system); GEs from different domains are Macroscopes on the domain: implement abstract Macroscopes concretely and provide API access via REST HTTP to trigger GE behavior. Modelling a GE is identified within UML use cases. GE specification have some properties:

- Addressing: IP address and port numbers
- Recognition: control syntax, parser, interpreter and semantic rules
- Multimodal: APIs, protocols, drivers
- Structured Data: XML, JSON, IC
- Formal Operation: state machine, dispatcher, DOM nodes
- Ad hoc Network Communication: HTTP/s, request methods, asynchronous, client/server, URIs
- Modular Design: object-oriented architecture, methods and functions, listeners, callbacks
- Behavioral: multithreaded, parallel, imperative, result combining, verifying, transformation, bidirectional communications
- Security: channel encryption, message encryption, authentication, authorization
- HCI: GUI, hardware interaction, multimodal UI, accessibility, human actors
- Interoperability: networked API server, configuration parameters, legacy system integrators, RPC, REST

In 2016, the European Commission published The 2016 Rolling Plan for ICT Standardisation[13] in which ETSI was requested to create an ISG (Industry Specification Group) aimed at definition of a standard Context Information Management (CIM) API with FIWARE NGSIv2[14] (current API specification implemented by the FIWARE Orion Context Broker) as basis. In the beginning of 2017, ETSI created the CIM ISG[15] which produced a first version, in January 2019, of the so named ETSI NGSI-LD API specifications[16].

The ETSI NGSI-LD API specifications are compatible with the FIWARE NGSIv2 API specifications, adding new features bringing support to Linked Data. It is planned that the FIWARE Orion Context Broker will evolve in line with the future ETSI NGSI-LD specifications, integrating the developments carried out in Orion-LD[17].

Several implementations of the NGSI-LD API are emerging, most of which have been incorporated in the FIWARE Catalogue: Scorpio[18] or Stellio[19]. The only exception to this rule at the moment is Djane[20] despite conversations are taking place to also include it.

In 2018, the European Commission (EC) formally adopted FIWARE Context Broker technology as CEF Building Block[21] within their Digital CEF (Connecting Europe Facility) Building Blocks program. This means that the EC officially recommends Public Administration and private companies of the European Union (EU) to adopt this technology in order to foster development of digital services which can be replicated (ported) across the EU.

During 2019, the FIWARE Foundation with other relevant organizations has launched an initiative towards definition of Smart Data Models[22]. The goal is to provide a common set of data models, with their corresponding mappings into JSON/JSON-LD which, in combination with NGSIv2/NGSI-LD ensures portability and interoperability of smart applications. The initiative is experiencing a growing momentum, involving multiple organizations and projects contributing data models in multiple domains: Smart Cities, Smart Agrifood, Smart Manufacturing, Smart Energy, Smart Water, Smart Destinations, etc.

The FIWARE Reference Architecture does not only bring components for an effective exchange and management of digital twin /context data but brings a number of components for publication of data resources and its eventual

[13] https://ec.europa.eu/growth/content/2016-rolling-plan-ict-standardisation-released-0_en
[14] http://fiware.github.io/specifications/ngsiv2/stable/
[15] https://www.etsi.org/committee/cim
[16] https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.02.02_60/gs_CIM009v010202p.pdf
[17] https://github.com/Fiware/context.Orion-LD
[18] https://github.com/ScorpioBroker/ScorpioBroker
[19] https://github.com/stellio-hub/stellio-context-broker
[20] https://github.com/sensinov/djane/
[21] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Context+Broker
[22] https://github.com/smart-data-models

monetization. Concretely, components coping with:

- Data Marketplace functions enabling publication of data resource offerings, supporting the definition of terms and conditions for accessing data resources including access and usage policies as well as, eventually, adopted pricing schemas
- Business Support functions, including functions for data resources usage accounting and rating, giving the option of storing usage log records on distributed ledgers to support trustworthiness of processes, Clearing House, Payment and Billing functions

Many of these functions rely on TM Forum Open APIs[23].

Smart Industry

FIWARE for Industry (F4I) is a multi-project initiative aiming at developing an ecosystem of FIWARE-enabled software components, suitable to meet the challenges of Manufacturing Industry business scenarios, as indicated by Industry 4.0 vision. F4I originates at the end of 2015 as the exploitation booster of the FITMAN FP7 FI PPP project (www.fiware4industry.com) which developed Open Source reference implementations of Smart-Digital-Virtual Factory scenarios by integrating 14 FIWARE Generic Enablers with 15 original Manufacturing Industry Specific Enablers.

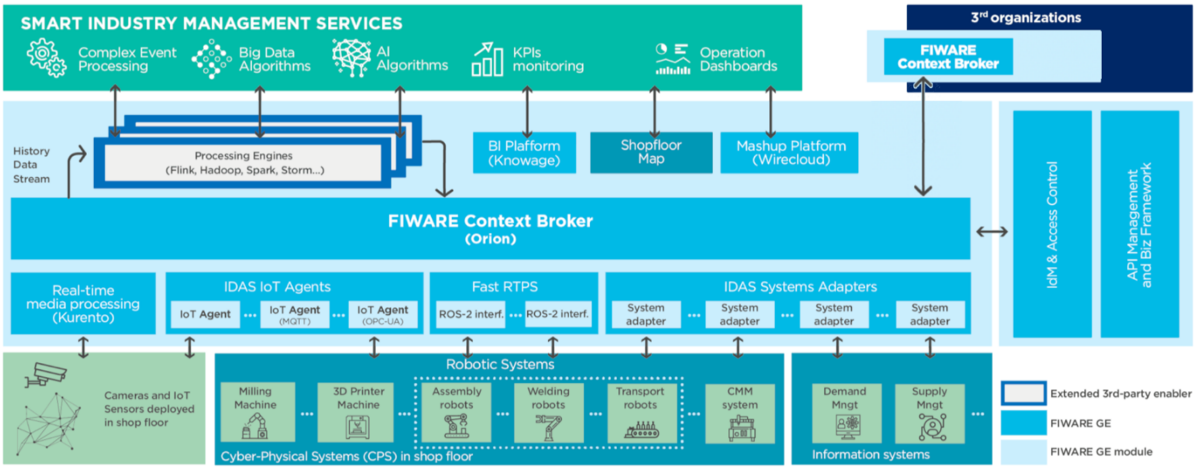

FIGURE 15. REFERENCE ARCHITECTURE FOR SMART INDUSTRY MANAGEMENT SYSTEM POWERED BY FIWARE

Starting from these 29 components, more than 15 new projects are developing their Smart Manufacturing solutions in several R&I domains. In the Factories of the Future H2020 cPPP, the recent projects CREMA, C2NET, PSYMBIOSYS, BEinCPPS, some of the ongoing FoF11 Connected Factories projects (e.g. FAR EDGE, AUTOWARE, vfOS and NIMBLE) RIAs and two I4MS Phase III Innovation Actions (MIDIH in the domain of CPS/IOT, L4MS in the domain of Mobile Robotics and Industrial Shop-floors' Logistics) are contributing in kind to the picture here below which includes 17 Enablers: 8 enhancements of FITMAN SEs, 3 enhancements of FIWARE GEs, 2 new specific enablers and 4 new releases of FIWARE GEs. Moreover, the EIT DIGITAL High Impact Initiative called OEDIPUS (Operate European Digital Industry with Products and Services) is developing platforms and components FIWARE based for the Smart Manufacturing Industry, in close collaboration with SIEMENS (OEDIPUS coordinator) and its platforms (e.g. MindSphere). In the near future, the EU-Brasil FASTEN project and some National / Regional projects will give their contributions as well to the F4I ecosystem.

During conversations with representatives of the Industrie 4.0 platform, the potential derived from adopting the ETSI NGSI-LD API as a standard API for accessing Asset Administrative Shell data has been acknowledged.

Smart Energy

The digitalization of the energy sector demands higher levels of operational excellence with the adoption of disruptive technologies to foster cross-domain data sharing and data-driven innovation. The following key elements in data

23 https://www.fiware.org/2016/04/27/fiware-and-tm-forum-at-the-dawn-of-the-data-economy/

management in support of a data economy need to be fulfilled:

- Data model/Semantics: Defining an appropriate data model beyond a single sector is a key ingredient for interoperability.
- Context Information: Defining the context is a key ingredient for bridging the gap between different verticals.
- Data Sovereignty: The ability of a data owner to define what a third party is allowed to do with his/her data.
- Open APIs: Closed solutions will not create a real open and competitive market. Open APIs offer the perfect bridge between private infrastructure spaces.

The Reference Architecture of Smart Energy Management Systems "Powered by FIWARE" relies on a "System of Systems" vision. The existence of a digital twin / context information management layer breaks the silos of information associated with the several vertical smart solutions, information systems and connected devices, enabling an overall management of an Energy ecosystem.

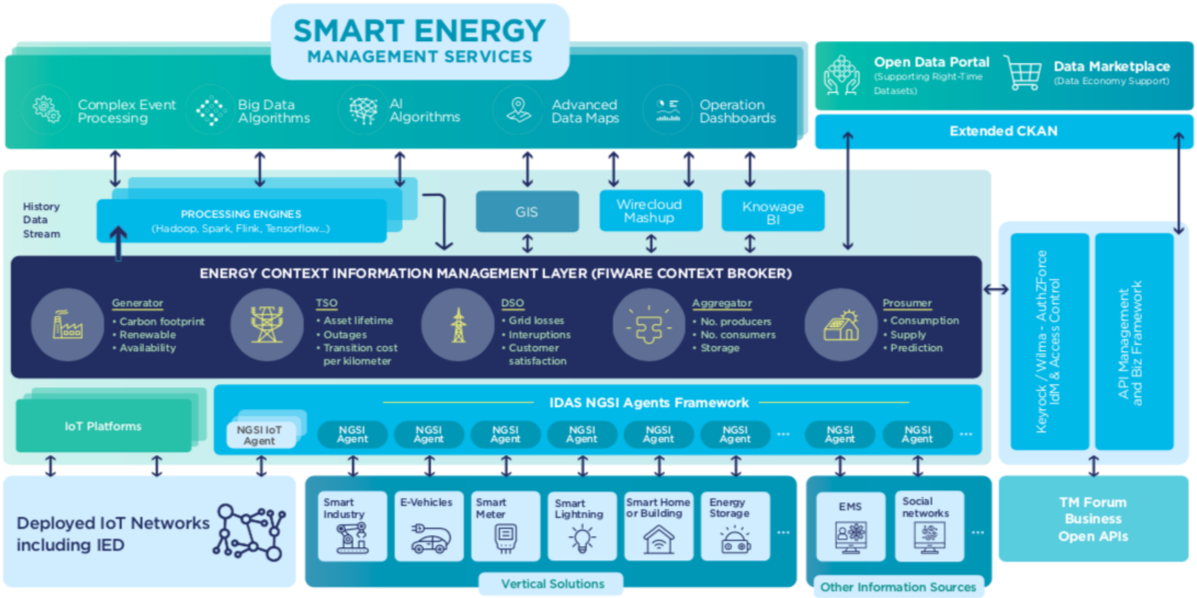

FIGURE 16. REFERENCE ARCHITECTURE FOR SMART ENERGY MANAGEMENT SYSTEM POWERED BY FIWARE

Smart Agrifood

The Reference Architecture of Smart Farm Management Systems "Powered by FIWARE" [24] also relies on a "system of systems" vision. The existence of a digital twin / context information management layer breaks the silos of information associated to the several vertical smart solutions, information systems and connected devices, enabling an overall management of Farm processes.

[24] Smart Agrifood - FIWARE Foundation Open Source Platform. (n.d.). Retrieved from https://www.fiware.org/community/smart-agrifood/

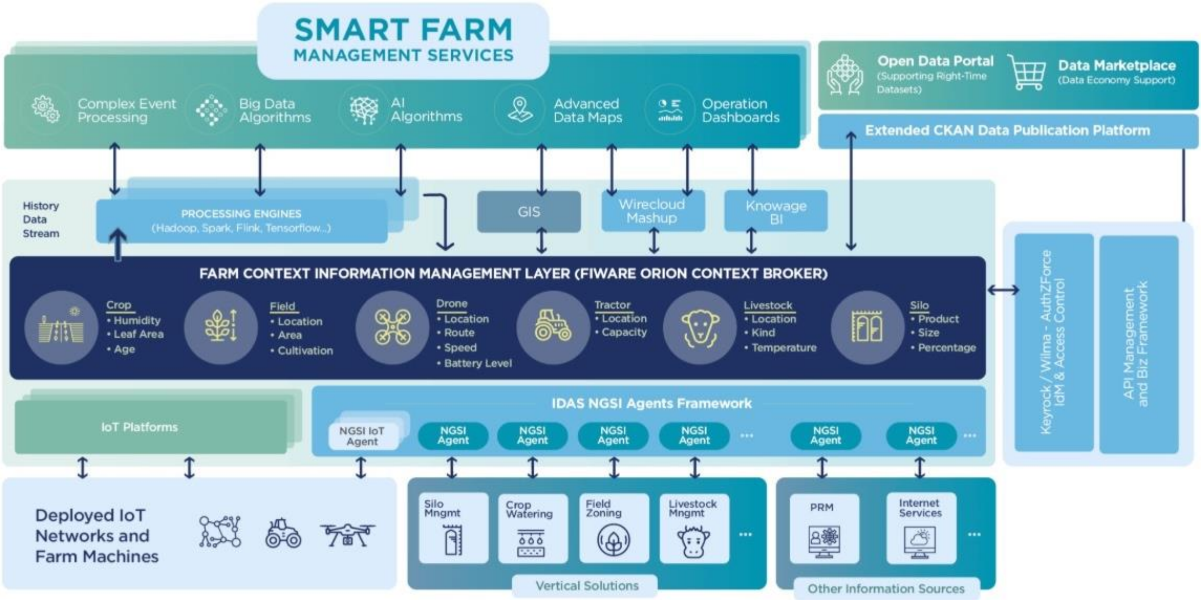

FIGURE 17. REFERENCE ARCHITECTURE FOR SMART FARM MANAGEMENT SYSTEM POWERED BY FIWARE

More specifically, the Orion Context Broker (or any other FIWARE Context Broker) collects data from sensors, drones, vertical smart solutions and information systems. In this way, the broker breaks information silos. Sensors are connected to IDAS IoT Agents, so that they can handle many IoT protocols such as MQTT, CoAP/OMA-LWM2M, OneM2M. Also, alternative IoT platforms can be used for this situation. Fast RTPS is used to interface ROS-2 robots, which is the main communication middleware in ROS-2. Different processing engines, such as Flink, Hadoop and Spark, are used in order to process historical data, so as to extract valuable insights or derive smart actions. Artificial Intelligence or Complex Event Processing functions can be used above the integrated processing engines. Wirecloud web mashup framework is used for Operating dashboards. Extended CKAN portal can offer to 3rd parties part of the current and historic context data. The API/Data access control functions enable access to the context data to parties that own certain privileges. The API management and business support layer can offer auditing of the system and monetize data access.

Benefits: The FIWARE Smart Industry RA defines a real ecosystem compliant with the main Reference Architectures in the manufacturing domain following the success in a domain like Smart Cities. The FIWARE RAs in other domains are also experiencing a growing adoption. The standardization is a strength point (i.e. support of ETSI) bringing innovation and spreading knowledge. In addition, it is worth to mention the adoption of Context Broker technology as a Connecting Europe Facility (CEF) Building Block. Last but not least, FIWARE brings a comprehensive set of components for data publication and monetization, in the latter case based on TM Forum recommendations, which pave the way for materializing Data Economy concepts.
Risks: The adoption is still lower than expected also compared with other open-source based architectures.

2.5 CREATE-IoT RA

CREATE-IoT (CRoss fErtilisation through AlignmenT, synchronization and Exchanges for IoT)[25] brings together 18 partners from 10 European countries. The objectives are to stimulate collaboration between IoT initiatives, foster the take up of IoT in Europe and support the development and growth of IoT ecosystems based on open technologies and platforms. This requires synchronization and alignment on strategic and operational terms through frequent, multi-directional exchanges between the various activities under the IoT Focus Areas (FAs). It addresses cross fertilization of the various IoT Large Scale Pilots (LSPs) for technological and validation issues of common interest across the various application domains and use cases.
The project fosters the exchange on requirements for legal accompanying measures, development of common methodologies and KPIs for design, testing and validation and for success and impact measurement, federation of pilot

[25] https://european-iot-pilots.eu/project/create-iot/

activities and transfer to other pilot areas, facilitating the access for IoT entrepreneurs/API developers/makers, SMEs, including combination of ICT & Art. CREATE-IoT builds strong connections with Member States' initiatives and other initiatives and will transfer learning points to the broader IoT policy framework that include contractual PPPs (e.g. Big Data, Factories of the Future, 5G-infrastructure), Joint Technology Initiatives (e.g. ECSEL), European Innovation Partnerships (e.g. on Smart Cities) as well as other FAs (e.g. on Autonomous transport).

During the initiative, the LSP model[26] was designed giving a significant contribution to IoT standards. The LSP model offers an extension of current architectures and is aiming at:

- Ensuring a common view of the different layers of the IoT systems from Physical up to Business.
- Providing additional viewpoints to the different stakeholders (not just to the developers) regarding some additional cross systems functions such as security, privacy or safety and the shared analysis of some properties (e.g. integrability) between different stakeholders.

This additional dimension of properties is a new way to discuss the properties of the IoT system between different involved parties (e.g. users, contractors, designers) and identify the elements in support (e.g. functional building blocks, APIs) and those missing.

The three dimensions of the proposed model are referring to different concerns in the elaboration of the functions of an IoT system. These three dimensions are described below[27]:

- **Layers**. The IoT LSPs have taken this into account together with the (specific) needs of their deployment CREATE-IoT domain, in particular:
    - Collaboration and processes, enable integration with existing enterprise and other external systems.
    - Applications, present device data in rich visuals and/or interactive dashboards.
    - Service, provide integrated development environment to simplify development of apps, support mashup of different data streams, analytics and service components and allow insights from data to be extracted and more complex data processing to be performed.
    - Abstraction, simple rules engine to allow mapping of low-level sensors events high level events and actions and provides basic data normalization, reformatting, cleansing and simple statistics.
    - Storage, cloud-based storage and database capabilities (not including on-premises solutions).
    - Processing, enable remote maintenance, interaction and management capabilities of devices at the edge and capabilities to perform processing of IoT data of devices at edge as opposed to cloud.
    - Networks & Communications, offer connectivity networks / HW modules enabling air interface connectivity and IoT gateway devices from bridge connectivity from IoT nodes into the cloud-based platform.
    - Physical / Device Layer, offers low-level system, SW managing SW/HW and runs applications, adaptable modules, drivers, source libraries that reduce development and testing time and multi-purpose programmable electronic devices at Microprocessor/Microcontroller level.
- **Cross-cutting Functions**. This dimension addresses additional functionalities that are not linked to a single layer but whose provision requires spanning across several layers. Examples of such cross-cutting functions are security and privacy that are described in all LSPs Reference Architectures as cross-layer functions.
- **Properties**. This dimension addresses the global properties of the IoT system that re (or not) provided by a proper implementation of functions (at all layers) and cross-cutting functions. As an example, trustworthiness is resulting in particular from the proper implementation of the security and privacy cross-cutting functions.

[26] https://european-iot-pilots.eu/wp-content/uploads/2019/06/IoT-_European-_Large-Scale_Pilots_Programme_eBook_CREATE-IoT_V02.pdf

[27] https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5be06018e&appId=PPGMS

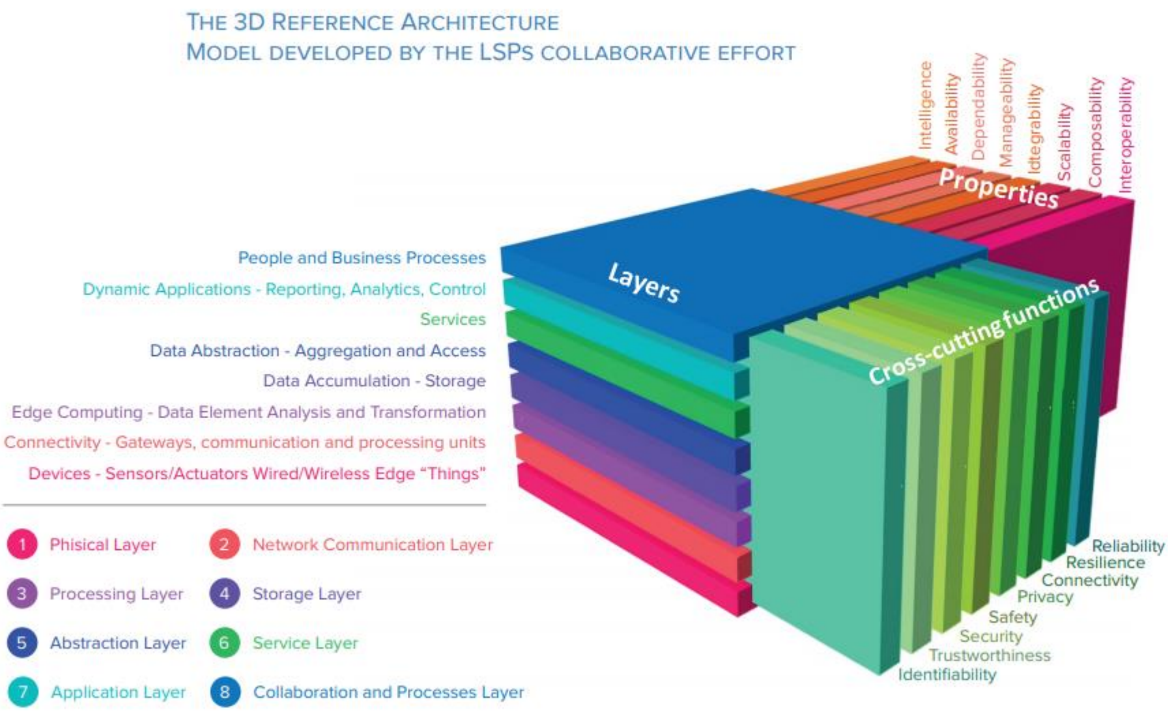

FIGURE 18. 3D REFERENCE ARCHITECTURE MODEL FROM CREATE-IOT

Benefits: The collaborative development by LSPs of a 3D Reference Architecture model expanding the reach of architecture specification and aimed at contributing to standardization.
Risks: The 3D Model is meant to be contributed to standardization (not yet another Reference Architecture)[28], the mappings with the consolidated RAs in the manufacturing domain (i.e. RAMI4.0 and IIRA) should be defined.

[28] https://oascities.org/wp-content/uploads/2019/06/20190619_ETSI_Darmois.pdf

2.6 BDVA Reference Architecture

The BDVA Reference Architecture [29] is a reference framework made by the European BDVA (Big Data Value Association) that describes logical components of a generic big data system.

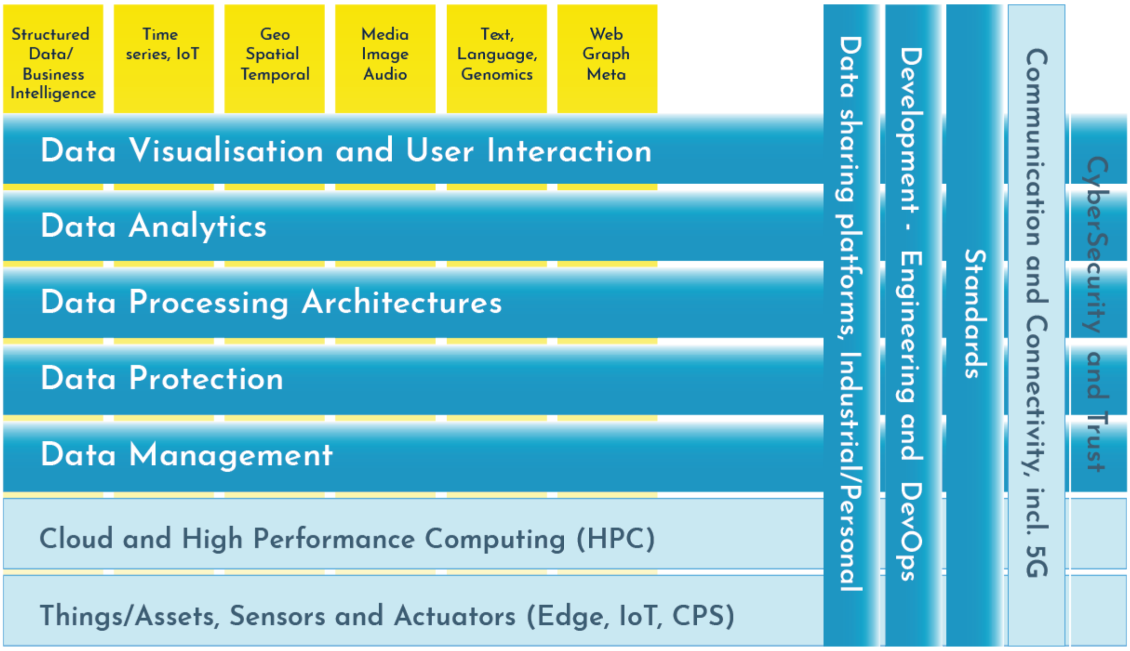

FIGURE 19. THE BDVA REFERENCE ARCHITECTURE

In fact, BDVA has proposed their initiative regarding a European Data-Driven Artificial Intelligence and their vision regarding AI and Big Data and how it can drive the European technology and economy[30]. To realize this vision, it will be necessary to address a number of challenges:

a) Data-driven AI-based solutions for the industry will require new business models.
b) Trust in AI and its results must be established; for example one should be able to explain how AI applications came to a specific result ("Explainable AI"), which would foster responsible technological development (e.g. avoid bias) and enhance transparency in how and why an AI takes a decision.
c) It is necessary to develop an AI and Big Data ecosystem, by developing data for open AI platforms and overcoming the lack of data interoperability.
d) Fuse and develop a number of technologies, as a successful industrial AI relies on the combination of a wide range of technologies, such as advanced data analytics, distributed AI, and hardware optimized for AI.

To this end, recently BDVA (together with euRobotics) has proposed the creation of an AI PPP (public-private partnership)[31]. The BDV Reference Model is structured into horizontal and vertical concerns[32]:

- Horizontal concerns cover specific aspects along the data processing chain, starting with data collection and ingestion, and extending to data visualization. It should be noted that the horizontal concerns do not imply a layered architecture. As an example, data visualization may be applied directly to collected data (the data management aspect) without the need for data processing and analytics.
- Vertical concerns address cross-cutting issues, which may affect all the horizontal concerns. In addition, vertical concerns may also involve non-technical aspects.

[29] European BDVA Strategic Research and Innovation Agenda v4.0. (2017, October). Retrieved from http://www.bdva.eu/sites/default/files/BDVA_SRIA_v4_Ed1.1.pdf

[30] Data-driven Artificial Intelligence For European Economic Competitiveness and Societal Progress. BDVA Position Statement. (2018, November). Retrieved from http://www.bdva.eu/sites/default/files/AI-Position-Statement-BDVA-Final-12112018.pdf

[31] Joint Vision Paper for an AI Public Private Partnership (AI PPP). Brussels: BDVA - euRobotics. (2019). Retrieved from http://www.bdva.eu/sites/default/files/VISION%20AI-PPP%20euRobotics-BDVA-Final.pdf

[32] European Big Data Value Strategic Research and Innovation Agenda http://bdva.eu/sites/default/files/BDVA_SRIA_v4_Ed1.1.pdf

Benefits: The BDVA reference model provides a clear and comprehensive overview of concerns at the intersection of Big Data and cloud platforms[33]. BDVA analyzes current gaps and challenges for dynamic data and formulates a list of necessary advancements.
Risks: The target group are decision-makers in companies and politics, therefore technical definitions are limited to the mentioning of according initiatives and organizations. Furthermore, interoperability, security or composition are only mentioned to a limited extend.

2.7 AI PPP Reference Architecture in SRIDA

The AI PPP SRIDA[34] recently published by BDVA and euROBOTICS PPPs puts at the center of its EU AI Framework three main boxes: the need for new skills and professions; the need for a pan-EU ecosystem of AI experiments and the need for a Data4AI platform, able to bridge the gap between AI-based analytics and the Industrial IoT.

The joint initiative aims to demonstrate the value of the Artificial Intelligence (AI) to customers and society in Europe. The AI technologies and applications can support and improve processes in many contexts, exploiting the European know-how from the industries (i.e. improving the effectiveness and efficiency of processes) to the healthcare (i.e. for data analysis and insights). The partnership represents over 400 European organizations from Industry and Research focused on achieving impact in the market: AI is transversal and cuts across sectors affecting many actors in the value chain.

A European AI Framework was defined for setting boundaries and limitation addressing the ethical values, human rights and safety in the EU and globally.

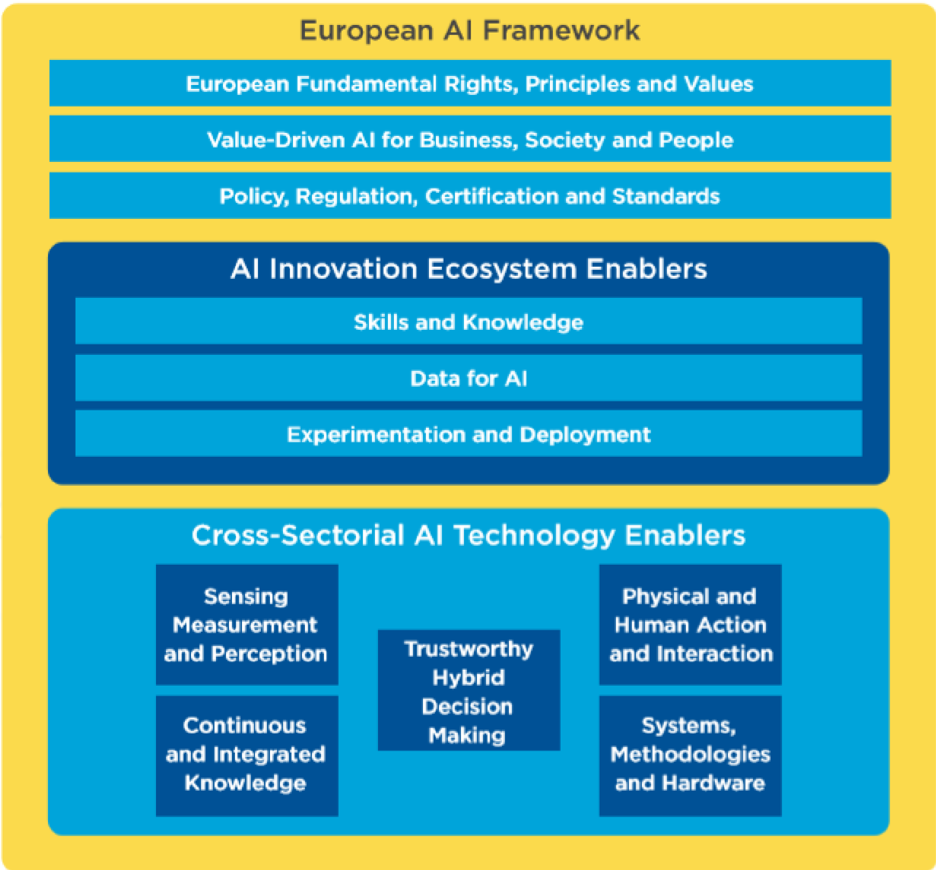

FIGURE 20. EUROPEAN AI FRAMEWORK

[33] Bader, Sebastian & Maleshkova, Maria & Lohmann, Steffen. (2019). Structuring Reference Architectures for the Industrial Internet of Things. Future Internet. 11. 151. 10.3390/fi11070151.
[34] http://www.bdva.eu/sites/default/files/AI%20PPP%20SRIDA-Consultation%20Version-June%202019%20-%20Online%20version.pdf

The AI Innovation Ecosystem Enablers represents essential resources for innovating and going from the research to the development phase. Furthermore, the Cross-Sectorial AI Technology Enablers represent the core technical competencies that are essential for the development of AI systems.

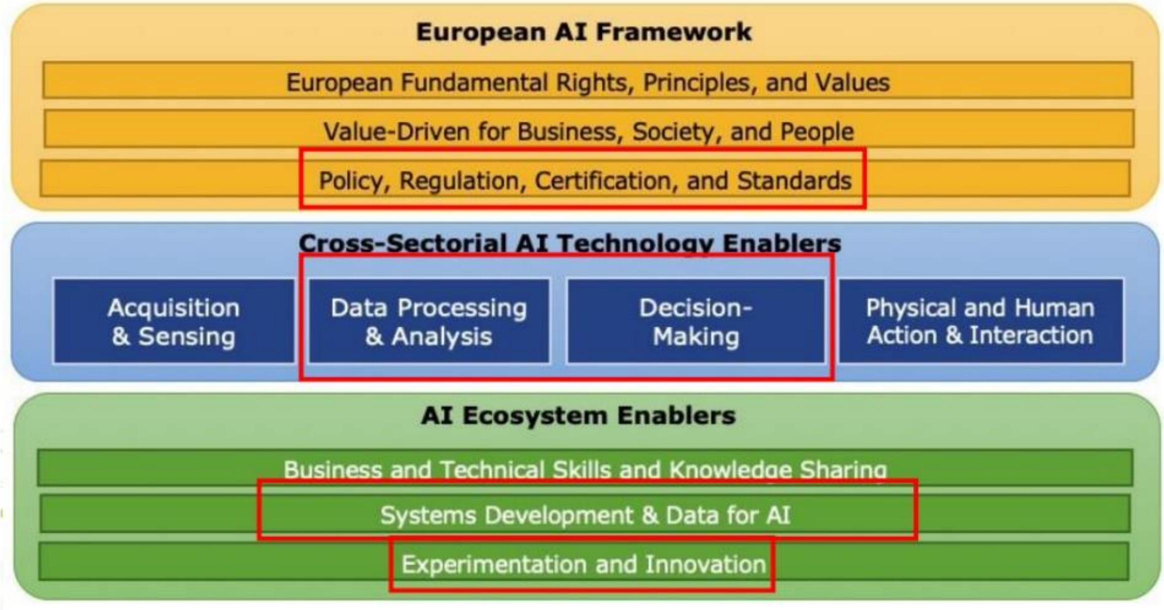

FIGURE 21. CROSS-SECTORIAL AI TECHNOLOGY ENABLERS

The AI PPP SRIDA document shows the tremendous importance of adequate high-quality Data for training AI systems. Ex-post data cleansing is often too costly and in-effective, especially in the absence of proper Metadata and domain Knowledge sources.

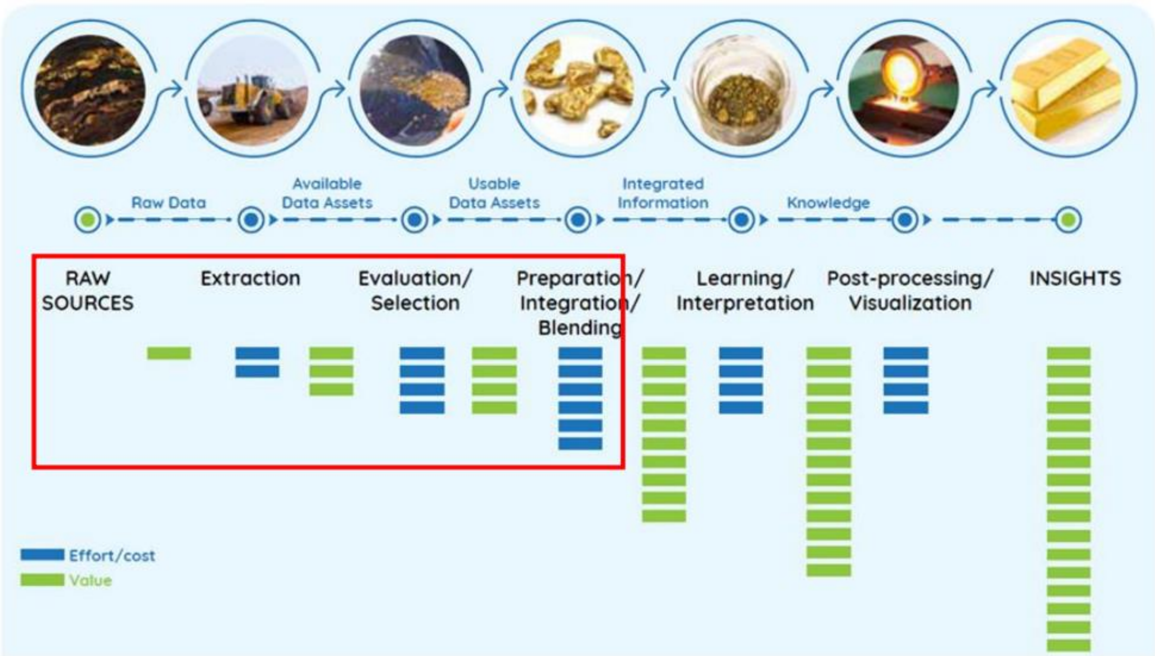

FIGURE 22. EVOLUTION OF QUALITY-RELATED VALUE IN DATA PIPELINES

Benefits: The architecture aims to drive the AI adoption in the European ecosystem defining a framework and key enablers for making innovation.
Risks: The architecture does not provide neither technological details nor implementations guidelines to put this framework into practice, being more focused in not-technical principles.

2.8 IDS Reference Architecture Model (IDS-RAM)

The International Data Spaces Association (IDSA) is the evolution of IDS (Industrial Data Space) which itself was an initiative lead by Fraunhofer ISST and promoted by the German Federal Ministry of Education and Research. IDSA is characterized by the focus on information ownership, with the aim of enabling clear and fair exchanges between data providers and consumers. To this end it suggests a reference distributed architecture that accomplishes this goal: the IDS Reference Architecture Model Version 3.0[35].

Broadening the perspective from an individual use case scenario to interoperability and a platform landscape view, the IDS Reference Architecture Model positions itself as an architecture that links different cloud platforms through policies and mechanisms for secure data exchange and trusted data sharing (through the principle of data sovereignty). Over the IDS Connector, industrial data clouds, individual enterprise clouds, on-premise applications and individual, connected devices can be connected to the International Data Space ecosystem (see Figure 23).

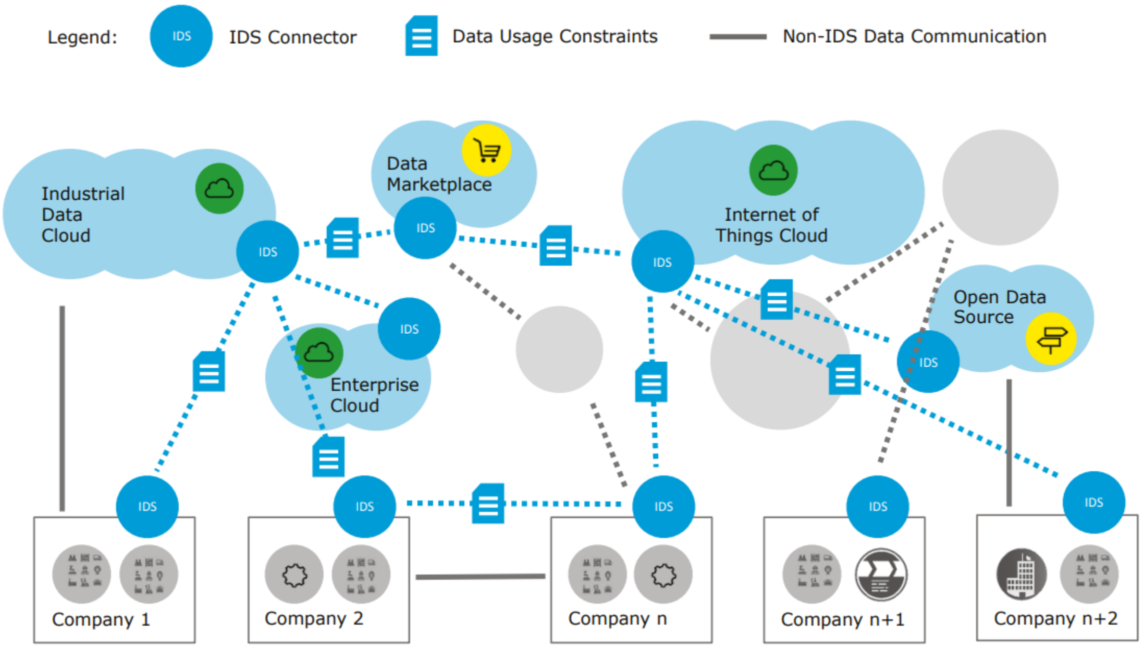

FIGURE 23. INTERNATIONAL DATA SPACES CONNECTING DIFFERENT PLATFORMS

This IDS Reference Architecture Model (IDS-RAM) is described using multiple layers, such as business, functional, process, information and system; between and common to all these layers are transversal functionalities that foster security, certification and governance, as illustrated in Figure 24. The Business Layer specifies and categorizes the different roles which the participants of IDS can assume, and it specifies the main activities and interactions connected with each of these roles. The Functional Layer defines the functional requirements of IDS, plus the concrete features to be derived from these. The Process Layer specifies the interactions taking place between the different components of IDS; using the BPMN notation, it provides a dynamic view of the Reference Architecture Model. The Information Layer defines a conceptual model which makes use of linked-data principles for describing both the static and the dynamic aspects of IDS' constituents. The System Layer is concerned with the decomposition of the logical software components, considering aspects such as integration, configuration, deployment, and extensibility of these components.

[35] https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf

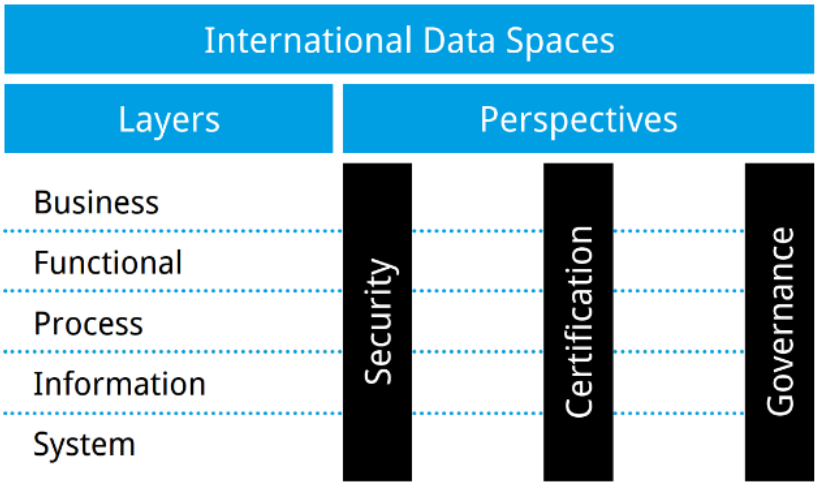

FIGURE 24. GENERAL STRUCTURE OF REFERENCE ARCHITECTURE MODEL

Comparing IDS to IoT-A ARM, the former focuses its specification of the roles for actors within the business layer that would govern the data flows between different domains or data spaces. As such, key participants (actors in the system) would be the Data Owner, Data Provider, Data Consumer, Data User or Broker Service provider. The complete landscape of roles, their functionalities and relationships result in a model depicted in the following Figure 25.

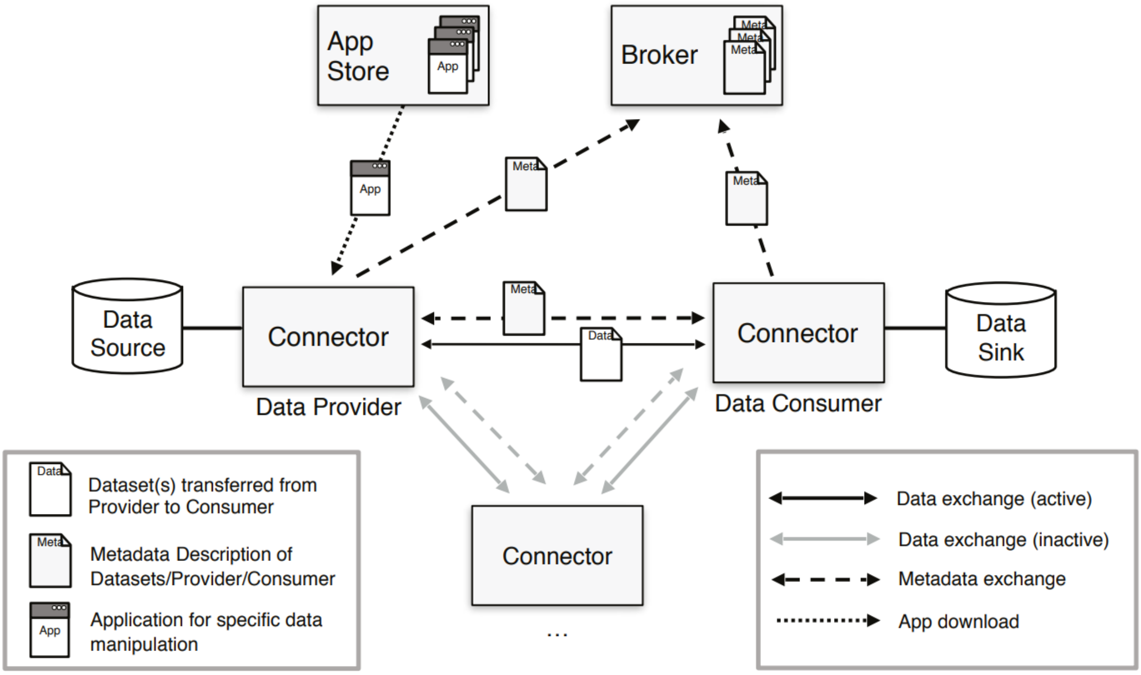

FIGURE 25. INTERACTION BETWEEN TECHNICAL COMPONENTS OF IDS REFERENCE ARCHITECTURE MODEL

The **Connector** is the central technological building block of IDS. It is a dedicated software component allowing Participants to exchange, share and process digital content. At the same time, the Connector ensures that the data sovereignty of the Data Owner is always guaranteed. The **Broker Service Provider** is an intermediary that stores and manages information about the data sources available in IDS. The activities of the Broker Service Provider mainly focus on receiving and providing metadata that allow provider and consumer connectors to exchange data. The **App Provider** role is optional in IDS, and its main role is to develop applications that can be used by both data providers and consumers in the data space. Applications are typically downloaded from the remote app store and run inside the containerized connector.

Establishing **trust for data sharing and data exchange** is a fundamental requirement in IDS. The IDS-RAM defines two basic types of trust: 1) Static Trust, based on the certification of participants and core technical components, and 2) Dynamic Trust, based on active monitoring of participants and core technical components. For data sharing and data exchange in the IDS, some preliminary actions and interactions are required. These are necessary for every participant, and involve a Certification Body, Evaluation Facilities, and the Dynamic Attribute Provisioning Service (DAPS). Figure 26 illustrates the roles and interactions required for issuing a digital identity in IDS, and these interactions are briefly listed here:

1. **Certification request**: This is a direct interaction between a participant and an evaluation facility to trigger an evaluation process based on IDS certification criteria.
2. **Notification of successful certification**: The Certification Body notifies the Certification Authority of the successful certification of the participant and the core component. Validity of both certifications must be provided.
3. **Generating the IDS-ID**: The Certification Authority generates a unique ID for the pair (participant and component) and issues a digital certificate (X.509).
4. **Provisioning of X.509 Certificate**: The Certification Authority sends a digital certificate (X.509) to the participant in a secure and trustworthy way and notifies the DAPS.
5. **Register**: After the digital certificate (X.509) is deployed inside the component, the component registers at the DAPS.
6. **DTM Interaction**: The Dynamic Trust Monitoring (DTM) implements a monitoring function for every IDS Component, and DTM and DAPS then exchange information on the behavior of the component, e.g. about security issues (vulnerabilities) or attempted attacks.

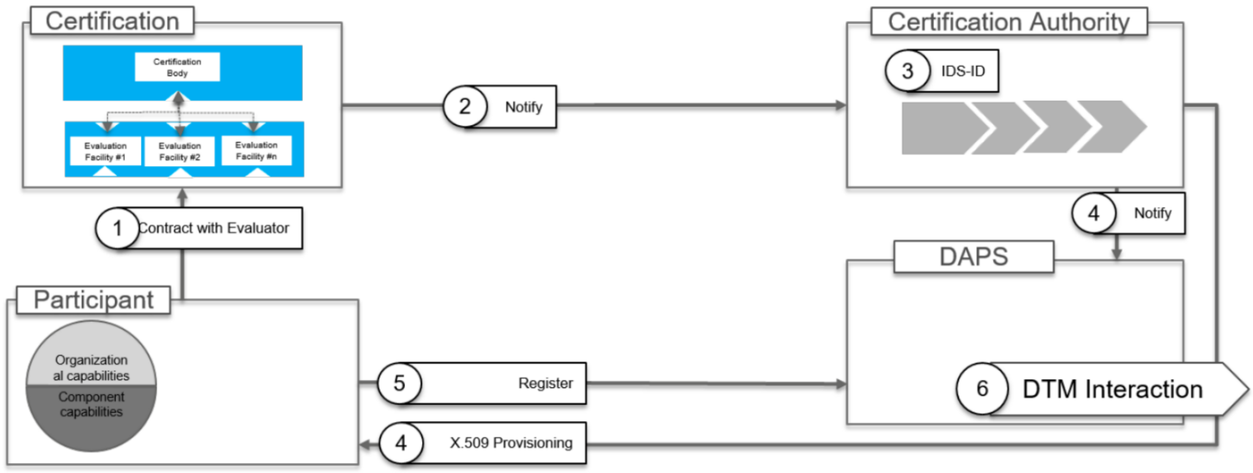

FIGURE 26. INTERACTIONS REQUIRED FOR ISSUING A DIGITAL IDENTITY IN THE IDS

The IDS Reference Architecture contains an internal structure that is strongly supported by the containerization for the development of IDS connectors. It relies on IDS Communication Protocol to enforce security in data exchanges, as it is depicted in the figure below.

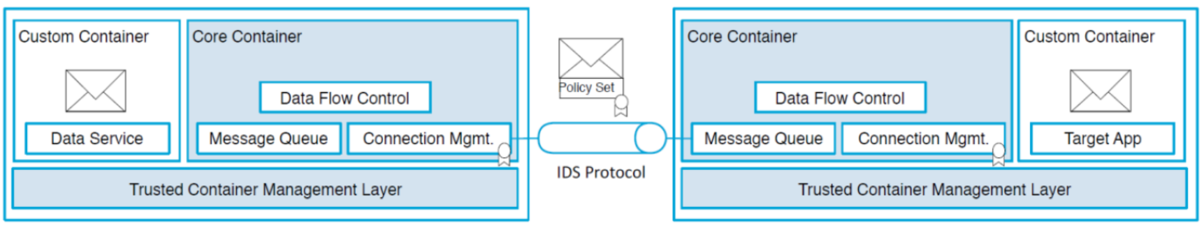

FIGURE 27. ENFORCING SECURITY IN DATA EXCHANGES: THE IDS COMMUNICATION PROTOCOL (IDS-RAM V3)

To sum up, the security implications that guarantee reliable and trusted transfer of information between independent entities in IDS are the following:

- **Secure communication.** The concept of Trusted Connector is introduced as depicted in the figures above.
- **Identity Management** for identification/authentication/authorization enhancing. There is use of certificates issued by a Certificate Authority (CA).
- **Trust Management** that uses Cryptographic methods such as PKI (Public Key Infrastructures).
- **Trusted Platform** for trustworthy data exchange, which defines the minimal requirement for Security

Profiles that should be verified by IDS connectors. It also defines the capacity to perform integrity verification of the rest of the involved connectors.

- **Data Access control**. IDS defines authorization criteria based on the previously defined Security Profiles.
- **Data Usage Control**. IDS checks and regulates that data processing is according the intended purposes defined by the original data owner.

IDSA RAM is a **blueprint** for the European Data Spaces in order to speed up its implementation in nine strategic areas. IDSA is working on the definition of functional building blocks for smart data sharing to guide the path to make fully interoperable data spaces creating the European Data Space.

Basically, functional building blocks for data sharing must enable three major functional groups:

1. Interoperability.
2. Trust between companies, platforms, and data ecosystems.
3. Enabling Governance for the data economy.

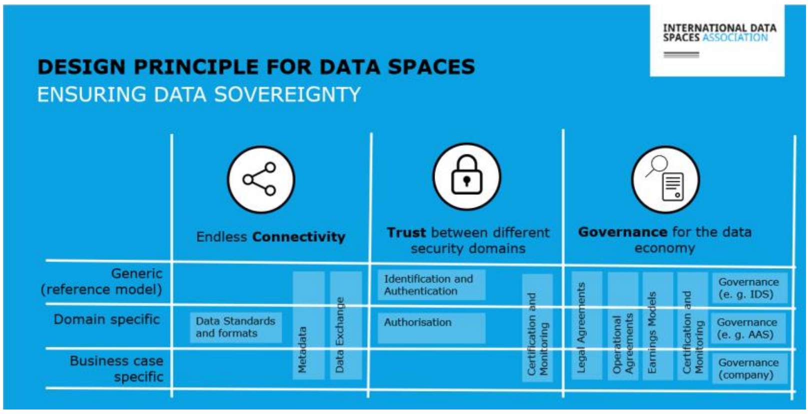

FIGURE 28. DESIGN PRINCIPLE FOR DATA SPACES (SOURCE: IDSA)

Benefits: The IDS RAM defines the way for creating a trusted environment for data exchange, implementing data economy services and data sovereignty principles.
Risks: There is a need for more market ready solutions and broad adoption. IDSA is working to make IDS components clearly defined in order to build an ecosystem ready for market and rapidly adopted.

3 RELEVANT CASES FROM THE OPEN DEI ECOSYSTEM

This chapter presents some relevant examples coming from the project activities, related to Reference Architecture for Digital Platforms, within the Innovation Actions falling within the project scope and supported by OPEN DEI.

For each sector targeted by OPEN DEI, we have identified only one example, selecting some of the most advanced projects dealing with building Digital Platforms focusing on data spaces and IoT interoperability, but other examples and alignment work will be carried on in the next iteration of this deliverable to provide a full picture of the supported IAs.

This chapter is going to address the approach to Reference Architecture from the point of view of these Use Cases. This approach will allow for the identification of commonalities and differences both across the various Use Cases of a single Innovation Action, as well as across several projects as further described in Chapter 4.3.

3.1 Manufacturing Sector – QU4LITY Reference Architecture

- Project Name: QU4LITY - Digital Reality in Zero Defect Manufacturing
- Website: https://qu4lity-project.eu/
- Grant ID and CORDIS url: **825030** - https://cordis.europa.eu/project/id/825030
- Relevant Deliverable(s): D2.11[36]

QU4LITY is developing and deploying solutions for the next generation of Zero Defect Manufacturing (ZDM) capabilities in the Industry4.0 era. The project's solutions will therefore leverage Cyber Physical Systems (CPS) and advanced digital technologies (e.g. Big Data, Edge/Fog Computing, Artificial Intelligence). QU4LITY is concerned not only with demonstrating Industry4.0 ZDM solution in productions lines, but also with providing reusable building blocks for developing and integrating such solutions.

The QU4LITY RA is aligned to the implementation needs envisaged in the Autonomous Quality (AQ) vision defined in the project, where processes and solutions are developed toward innovative digital ZDM solutions for smart manufacturing, based on best in class technologies and on relevant sector standards. To this end, the QU4LITY RA has not been designed from scratch, being strongly based on the most relevant outcomes of other Research and Innovation activities and strongly rooted back on the Plattform Industrie 4.0 initiative (RAMI 4.0) and the Industrial Internet Consortium (IIRA and OpenFog RA).

On the other hand, several research projects have already been executed by many of the Consortium partners, providing a wide set of background knowledge on the topic and providing solid backgrounds. Following this experience, the Digital Shopfloor Alliance Reference Framework has been adopted as the main input to further enhance it for ZDM scenario, exploiting its adherence to standards and the openness toward the integration of multiple digital enablers.

Figure 29 illustrates different components and views of the QU4LITY Reference Architecture (QU4LITY RA).

[36] Main contributors: Angelo Marguglio (ENG), Olga Meyer (FHG), John Soldatos (AIT), Irune Mato (INNO), Javier Hitado Simarro (ATOS), Martijn Rooker (TTT), Xiaochen Zheng (EPFL), Vassilis Tsolekas (ATLAS)

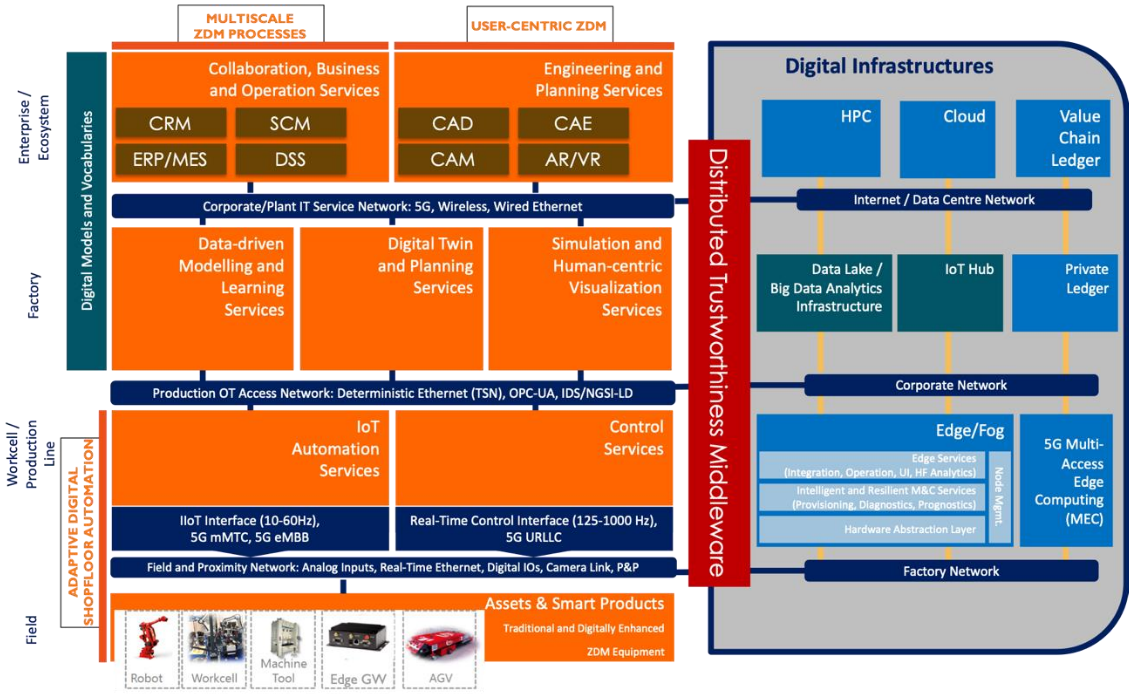

FIGURE 29. QU4LITY REFERENCE ARCHITECTURE

QU4LITY RA as a Four-Tier design, where the main Tiers (Field, Line, Factory and Ecosystem) are hierarchically stacked according to their scope with respect to the physical processes in the factory, and one Digital Infrastructures providing common services such as connectivity and distributed processing capabilities. Moreover, the QU4LITY RA groups system functionality into three distinct Functional Domains (Adaptive Digital Shopfloor Automation, Multiscale ZDM Processes and User-Centric ZDM), which are orthogonal to the Tiers, and four Crosscutting Functions (Security, Digital Infrastructures and Digital Models) that are domain-agnostic. To better clarify the role of all these elements, they are mapped, whenever possible and relevant, to the corresponding concepts in RAMI 4.0.

3.2 Agriculture Sector – DEMETER Reference Architecture

- Project Name: DEMETER - Building an Interoperable, Data-Driven, Innovative and Sustainable European Agri-Food Sector
- Website: http://www.demeter-eu-project.eu/
- Grant ID and CORDIS url: **857202** - https://cordis.europa.eu/project/id/857202
- Relevant Deliverable(s): D3.1[37]

There are a variety of smart farming systems and platforms already deployed, employing many different communication, sensing and data processing technologies. However, building a new master system that has the ability to also incorporate other existing systems is a near impossible task, also due to the complexity/heterogeneity of the agrifood sector, when it comes to issues such as scalability and governance. To tackle these, DEMETER proposes an overarching approach that integrates heterogeneous technologies, platforms and systems, while supporting fluid data exchange across the entire agrifood chain, addressing scalability and governance of ownership. As described in the previous section, these goals are delivered through the Agricultural Interoperability Space. The proposed approach enables existing Agriculture Knowledge Information Systems (AKISs) to continue their operation, but also allows those systems to make available and consume data from other cooperating systems. Additionally, newer technologies and services can be exposed that may be of interest to cooperating AKISs. This is more realistic and viable in terms of usability, market adoption, and sustainability. In order to realize this approach, the following two core objectives need to be fulfilled by the proposed solution:

[37] Main contributors: Ioanna Roussaki (ICCS), Thanasis Poulakidas (INTRA), Ioannis Oikonomidis (INTRA), Angelo Marguglio (ENG), Antonio Caruso (ENG), Antonio Skarmeta (UMU), Arne Berre (SINTEF), Tomas Pariente Lobo (ATOS), Nenad Gligoric (DNET), Raul Palma (PSNC)

- Allow existing AKISs to offer their data to and consume data from their counterparts, providing also the means to incentivize AKISs for sharing data by ensuring data integrity and valorization, giving them also the chance to make some profit.
- Extensive use of virtualization containers for services should be made to ensure rapid deployment, portability and scaling once required.

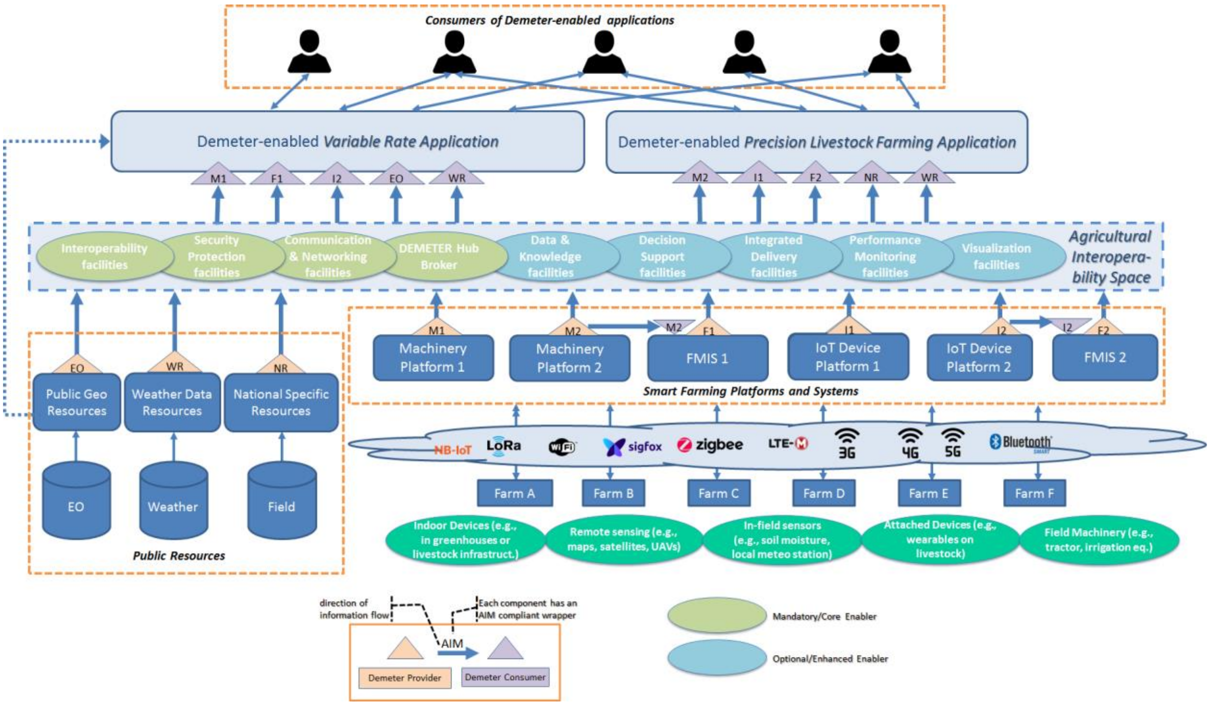

FIGURE 30. DEMETER REFERENCE ARCHITECTURE

The DEMETER architecture consists of a DEMETER Provider and a DEMETER Consumer service based on the architecture model introduced by the Industrial Data Space (IDS), then further specified by the International Data Space Association (IDSA), which is the continuation of IDS. However, DEMETER Provider and DEMETER Consumer services further extend their applications by supporting AKISs to also expose and consume data. Rapid deployment and decommissioning are highly beneficial for survey services that might not require a continuous feed from a particular AKIS. Such a service would deploy and start a DEMETER Consumer service for that particular AKIS, gather necessary information, and then stop the service. The service will be packaged into a lightweight container along with all the software necessary to support self-contained deployment of the service (runtime environment, libraries for supported communication protocols, encryption techniques, etc.).

As data interoperability is of critical importance, the proposed solution provides the necessary data translation mechanisms combining the use of a semantic data model (Agriculture Information Model — AIM) developed by DEMETER, along with the respective data translation/management/inference mechanisms adopting widespread standardized solutions such as NGSI-LD , Saref4Agri , ADAPT , etc. In order to enable interoperability of heterogeneous data handling approaches, the DEMETER provider-consumer services, deployed on various AKISs, translate and exchange data based on the AIM common data format with the utilization of lightweight data wrappers/translators. For this conversion to be feasible, each AKIS needs to provide the specifications of the utilized data model-semantics, or it should parse returning content in the AIM format. The AIM is not built ab initio but incorporates and extends existing ontologies and vocabularies already available for this domain.

DEMETER provider-consumer services maintain the necessary mechanisms for satisfying data security and privacy concerns (cf. below). They need to be trusted to be deployed and hosted by the AKIS on their own cyber-premises (i.e. hosting environments) following the principle that moving processing capabilities is easier than moving data themselves. This is also an inherent data privacy protection feature as the owner of the data maintains the control/decision of which data are allowed to be shared with other entities. The services need to provide privacy and security functionalities, including user authentication and access authorization. Once a DEMETER-enabled application is implemented, the final version at a production level can be discovered by consumers (e.g. Farmers, Agronomists, Cooperatives, etc.) through the DEMETER Dashboard, which is also used by these stakeholders to provide their feedback regarding the perceived experience and added value.

For simplicity, the picture presents only some of the platforms that can be integrated in the DEMETER Reference Architecture, thus representing a specific instantiation of the architecture deployed to serve the needs of one pilot site for example. However, apart from platforms, DEMETER service logic blocks are made available and can be used by the interested parties (e.g. data/knowledge facilities), as well as any other 3rd Party resource. All the registered resources are made available to the developers through the DEMETER Enabler Hub, presented in the next subsection of this deliverable report; these are annotated with rich metadata that describe the capabilities (or constraints) of these resources thus guiding the deployment of DEMETER apps based on the adopted technologies as well as information regarding ownership of resources that are available and the restrictions that their locations might impose during this process.

3.3 Energy Sector – PlatOne Open Framework

- Project Name: PlatOne - PLATform for Operation of distribution NEtworks
- Website: https://www.platone-h2020.eu/
- Grant ID and CORDIS url: **864300** - https://cordis.europa.eu/project/id/864300
- Relevant Deliverable(s): D2.1[38]

The energy system is facing an incredible revolution. End target is the creation of a new energy scenario widely dominated by renewable energy sources and mostly based on distributed energy generation working in synergy with electric cars inside the smart city ecosystem. In the middle of this process is the distribution network where the majority of the new sources are and will be connected, renewable resources that are mainly unpredictable and high peak loads related to fast and superfast e-car recharging. Flexibility is a key resource in a scenario in which the grid is more and more changing from being a load driven system to a generation driven system, given the partial control on energy intake from renewable energy sources. This process implies also that the changes are not only related to the operational aspects but also to the market element. Digitalization is a key enabler of this process opening the way to smart and efficient management of data sources in a secure way. In a nutshell, actually, digitalization is making the separation between market and operation less and less meaningful.

The world envisioned by the European project PlatOne will provide a seamless integration of operation and market simplifying the life of customers (both prosumers and citizens), distribution grid operator and aggregators, thanks to a multilayer platform architecture collecting data on the edge and delivering secure information both to distribution management systems and to an open marketplace for service provision. PlatOne aims to develop an architecture for testing and implementing a data acquisitions system based on a two-layer approach that will allow greater stakeholder involvement and enable an efficient and smart network management. The tools used for this purpose will be based on platforms able to receive data from different sources, such as weather forecasting systems or distributed smart devices spread all over urban areas. These platforms, by communicating with each other and exchanging data, will allow collecting and elaborating information useful for Distribution System Operators (DSOs), Transmission System Operators (TSOs), customers and aggregators.

The PlatOne open framework aims to create a fully replicable and scalable system that enables distribution grid flexibility/congestion management mechanisms through Peer-to-peer (P2P market models involving all the possible actors at many levels (DSOs, TSOs, customers, aggregators). The key components for an open framework are a secure shared data management system, standard and flexible integration of external solution (e.g. legacy solutions), and openness to external services through standardized open application program interfaces (APIs). The PlatOne open framework offers a two-layer platform and innovative components (illustrated in Figure 31) that allow targeting all the PlatOne goals. These components are:

- *DSO technical platform*: it allows DSOs to manage the distribution grid in a secure, efficient and stable manner. It is based on an open-source extensible microservices platform and allows to deploy, as Docker containers, specific services for the DSOs and execute them on Kubernetes. The Data Bus layer, included on the DSO Technical Platform allows to integrate both other components of PlatOne framework and external components (e.g. DMS, LFC) with a

[38] Main contributors: Vincenzo Croce (ENG), Ferdinando Bosco (ENG)

direct connection to the classical supervisory control and data acquisition (SCADA) system adopted by the DSO wrapped by standard communication protocols.

- *Blockchain service layer*: it is a blockchain-based infrastructure that enables the deployment of blockchain-based components as the PlatOne market platform.
- *Market platform*: it allows the support of wide geographical area flexibility requests from TSOs and local flexibility requests from DSOs. These are matched with offers coming from aggregators resolving conflicts according to pre-defined rules of dispatching priorities. All the market operations are registered and certified within the blockchain service layer, ensuring a higher level of transparency, security and trustworthiness among all the market participants.
- *Blockchain access layer*: it is a layer that adds a further level of security and trustworthiness to the framework. It is an extension of the physical infrastructure and performs multiple tasks, among which the data certification and automated flexibility execution through Smart Contracts.
- *Shared customer database*: it contains all the measurements, set points and other needed data collected from customer physical infrastructure. It allows the other components of the PlatOne open framework to access data in an easy way and without compromising security and privacy.
- *Aggregator platform*: it is not included as core components of the PlatOne Open Framework but it is an integral part of it. The aggregator platform allows the aggregators to participate in the PlatOne market offering the resources of them aggregated customers.

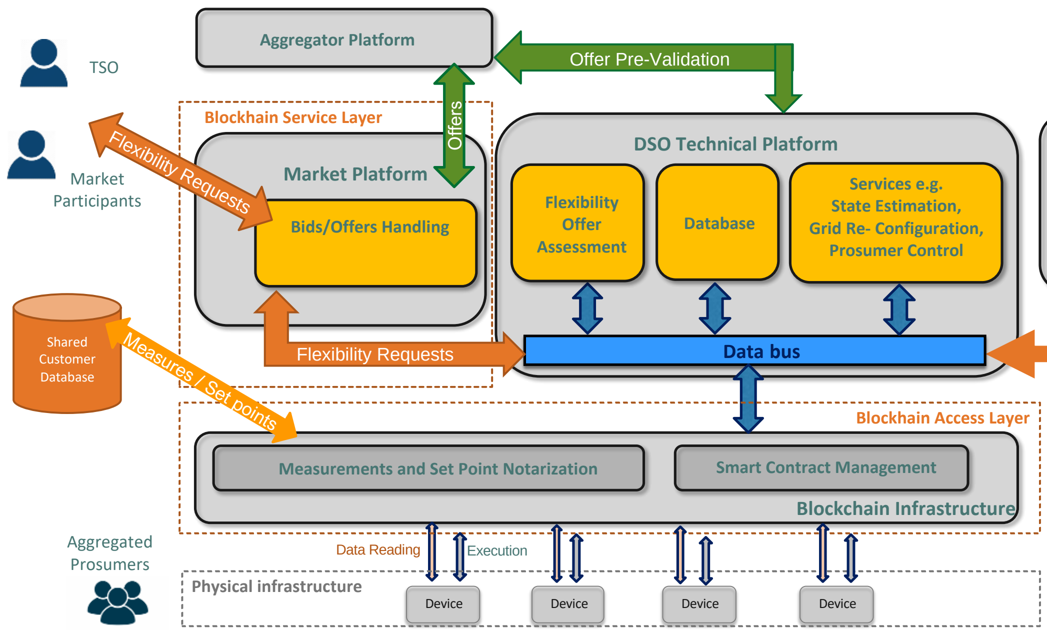

FIGURE 31. PLATONE OPEN FRAMEWORK

The core components of the PlatOne Open Framework will be released as open- source to support a rapid market uptake at European level. IT integrators are then expected to release on top commercial version with proper Service Level Agreement.

3.4 Healthcare Sector – ACTIVAGE IoT Ecosystem Suite

- Project Name: ACTIVAGE - ACTivating InnoVative IoT smart living environments for AGEing well
- Website: https://www.activageproject.eu/
- Grant ID and CORDIS url: **732679** - https://cordis.europa.eu/project/id/732679
- Relevant Deliverable(s): D3.7[39]

[39] Main contributors: Alejandro Medrano (UPV), Giuseppe Fico (UPV), Clara Isabel Valero-Lopez (MYSPHERA), Regel G. Usach (MYSPHERA), Carlos Palau (MYSPHERA), Sergio Guillén (UPM)

The ACTIVAGE project, from its start, has worked towards implementing the idea of innovating the Active and Healthy Ageing (AHA) sector by both, designing solutions introducing IoT technology and by using IoT technology to improve current healthcare services. One of its ambitious objectives is to build the first European IoT ecosystem across 9 Deployment Sites (DS) in seven European countries. The ecosystem must be replicable by means of reusing underlying open and also proprietary IoT platforms, and scaling up software technologies and promote standards. ACTIVAGE at the same time aims to integrate new necessary interfaces for enabling interoperability across heterogeneous platforms. The ACTIVAGE project's ecosystem by definition will set the foundations for connecting providers, service providers, and users.

ACTIVAGE project focuses on the need to overcome a fundamental barrier and technical limitations of IoT ecosystems: the lack of interoperability across IoT platforms and things. In today's society where people rely on the Internet as one of the most powerful communication means, we are dealing with vertically oriented and mostly closed systems. IoT architectures are built on heterogeneous standards or even proprietary interfaces. This causes interoperability problems when developers aim to create cross-platform and cross-domain applications, hiding the creation of broadly accepted IoT ecosystems. Service and application providers who want to use services in the ecosystem need to adapt to the platform-specific API and information models and therefore, can only provide application and services for a small number of platforms creating barriers and limiting business opportunities. This concerns especially small innovative enterprises, which cannot afford to provide solutions across multiple platforms.

In addition, ACTIVAGE not only focuses on providing interoperability through the previously mentioned European platforms but also the architecture should be able to support other future platforms and services, providing a common framework for allowing to deploy IoT services in any Deployment Site platforms that comply with the standards of the architecture.

ACTIVAGE architecture, as shown in Figure 32, is designed to serve as common framework to build interoperable smart living solutions in the form of apps, software tools and services that can be deployed, extended and replicated at Deployment Sites across Europe. In other words, to allow future support of any additional platforms and services as far as they comply with defined interoperability framework and standards. The design of this architecture is based on the analysis carried out, which included IoT Reference Architectures such as oneM2M, Big IoT or Inter-IoT. Issues such as security, privacy, semantics, data processing and data sharing should be taken into account so as to develop the ACTIVAGE architecture. In addition to these gaps, it should be noted that the Deployment Sites architectures and the selected IoT Platforms are extremely heterogeneous therefore the architecture should efficiency and effectively integrate a wide spectrum of open and commercial platforms and IoT devices. Furthermore, ACTIVAGE architecture has been designed to provide semantic interoperability. Moreover, the ACTIVAGE architecture is in compliance with the IoT-A reference model which has been developed as a reference model for IoT systems in general. It could be seen as one of the most generic and comprehensive model.

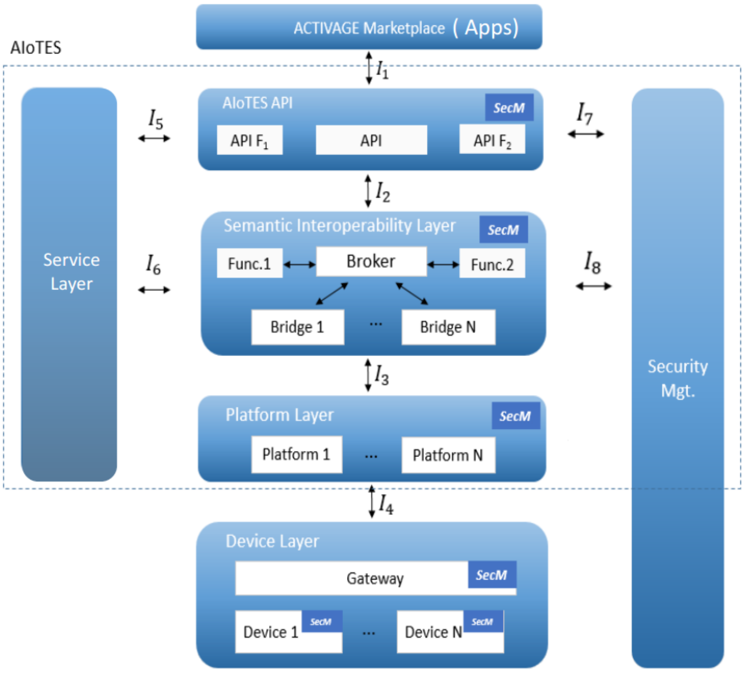

FIGURE 32. ACTIVAGE HIGH-LEVEL ARCHITECTURE

ACTIVAGE architecture from top to bottom, will enable a set of tools and services and will provide them in the form of a marketplace where developers and entrepreneurs make use of the advantages of the ACTIVAGE ecosystem.

ACTIVAGE IoT Semantic Interoperability Layer plays an important role in the ACTIVAGE architecture. It enables and orchestrates the interconnection of heterogeneous IoT devices, European platforms and smart living services within a common ecosystem of solutions. It will enable application developers, integrators, service providers a common framework to build interoperable smart living apps and services that can be deployed, extended and replicated at Deployment Sites available across Europe.

The *ACTIVAGE Platform Layer* rely on multiple solutions mainly to enable technical exchange of protocols data and configurations to enable the processing of the IoT data ether in edge or cloud, based on the demands of the deployment sites using this layer for integration. The device layer represents the set of smart objects such as sensors and actuators that are associated to specific platforms and are responsible of the collection of valuable data from the Smart Homes in Deployment Sites.

The security and privacy protection are crucial components of the AIoTES since they span across all the above layers and suites and guarantee both the protection of sensitive information of users and also comply with ethical and legal requirements for privacy and confidentiality. Furthermore, the security module is responsible for the protection of the intellectual property of application developers.

The **ACTIVAGE IoT Ecosystem Suite** consists of a set of Techniques, Tools and Methodologies for interoperability between heterogeneous IoT Platforms and an Open Framework for providing Semantic Interoperability of IoT Platforms for AHA while addressing trustworthiness, privacy, data protection and security.

Currently, interoperability is a complex challenge in IoT, and more in particular, the interoperability among IoT platforms is a major concern. ACTIVAGE aims to enable the federation of available platforms within an ecosystem of applications. Regarding this goal, AIoTES enables interoperability among different IoT platforms from Deployment Sites and applications within the ACTIVAGE ecosystem, and specifically targets issues related to the AHA domain.

AIoTES pursues the separation of concerns to facilitate interoperability among the project DS and provide a complete independent and accessible software suite. Its objective is to create an abstraction layer inside of ACTIVAGE architecture that encapsulates the content of the API, IoT Semantic Interoperability layer and Platforms Layer as well as the Security Management Framework and the AIoTES Management module. Thus, using this suite, any platform belonging to the Active & Healthy Ageing IoT Deployment ecosystem will be able to establish seamless communication with all the applications and services located in the Marketplace. In other words, thanks to this suite, it is achieved interoperability across heterogeneous platforms and consequently applications are independent of platforms, obtaining a less fragmented AHA market.

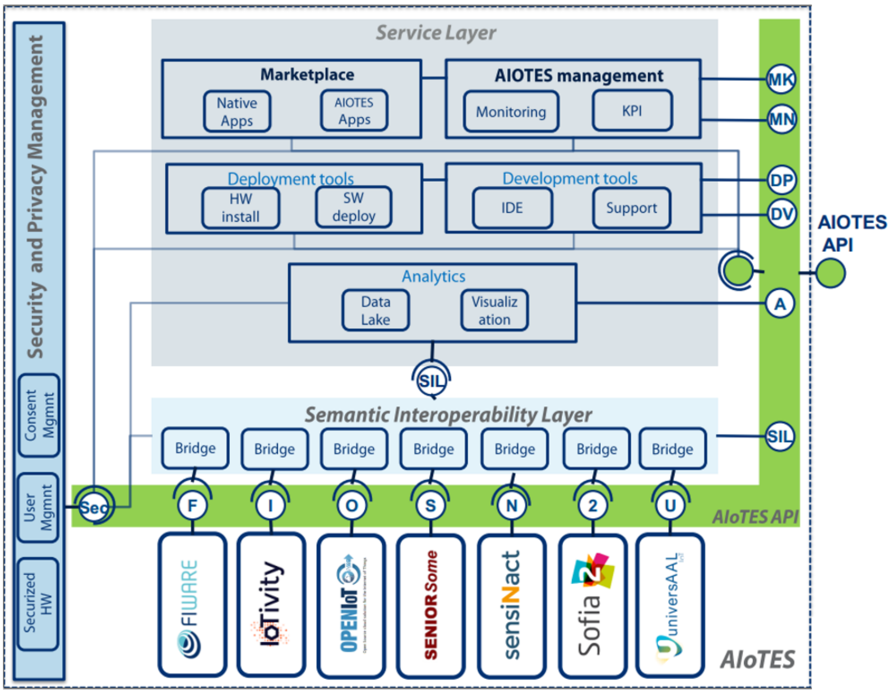

FIGURE 33. ACTIVAGE-AIOTES HIGH-LEVEL BLOCK SCHEME

The structural blocks of AIoTES can be seen in Figure 33. AIoTES is divided in 2 layers, the Semantic Interoperability Layer, that provides interoperability and allows communication with the Deployment Sites, and the Service Layer, in which the AIoTES management, Data Lake and Marketplace module are included. There is a vertical module for security and privacy that guarantees security and privacy within the framework. AIoTES will expose an API that can be accessed externally by Marketplace applications. Also, within the AIoTES frame, there are tools being developed that support the development of applications over AIoTES and the deployment of AIoTES architectural components and several services.

As it can be seen in Figure 32 AIoTES groups together most of the building blocks of the architecture. The AIoTES block scheme drawn in Figure 33 leverages the general ACTIVAGE architecture.

4 OPEN DEI REFERENCE ARCHITECTURE FRAMEWORK (RAF)

This chapter describes the performed activities for the analysis, design, and validation of the OPEN DEI **Reference Architecture Framework** (RAF in short). The objective is to harmonize and coordinate different DT approaches, analyzed in the previous chapter, under a common Reference Architecture Framework so that experiences and lessons learned could be shared and assessed.

To this end a short list of underlying principles will be described, before providing the high-level specifications of the OPEN DEI RAF, as well as some example mappings between existing Digital Platforms (adopted in some of the Innovation Actions under the OPEN DEI umbrella) and the defined OPEN DEI RAF.

4.1 Underlying principles

This section sets up the fundamental principles which will drive the design and implementation of the OPEN DEI RAF. They are relevant to the process of creating data-driven services enabling digital transformation and building Digital Platform supporting such services.

4.1.1 Underlying principle 1: INTEROPERABILITY THROUGH DATA SHARING

Syntactic interoperability between two or more systems is achieved by means of using common data formats and communication protocols. Semantic interoperability between two systems, on the other hand, is achieeved when the information exchanged can be interpreted meaningfully and accurately at both ends, producing useful results as defined by the end users of both systems.

A major obstacle to interoperability arises from legacy systems. Historically, applications and information systems in business organizations were developed in a bottom-up fashion, trying to solve domain-specific and local problems. This resulted in fragmented ICT islands which are difficult to interoperate. Due to the fragmentation of ICT solutions, the plethora of legacy systems creates an interoperability barrier at technical level.

There are different paradigms for achieving interoperability. Sharing of a digital representation of assets from the real world (physical objects like a car or a citizen as well as digital entities like a claim ticket in a CRM system) is the paradigm adopted in the OPEN DEI RAF. In this case, the "coin of exchange" in order to achieve effective interoperability is the information about attributes linked to the digital representation of assets. Interoperability enables to break information silos within an organization and the creation of innovative data value chains and the creation of multi-side markets involving different organizations. Effective interoperability through data sharing requires the definition of standard data models and often a standard API, as well as mappings of these data models into data structures compatible with the API. Such standard data models specify the unique identifiers and shortnames, valid value types and semantics associated to attributes of classes of real/digital objects.

***Recommendation 1**: OPEN DEI RAF should foster technical interoperability at syntactic and semantic levels, via the use of data sharing mechanisms, grounded on well-established standards and design/implementation patterns.*

4.1.2 Underlying principle 2: OPENNESS

In the context of data-driven services, the concept of **openness** mainly relates to data, data/API specifications and software.

Open data refers to the idea that all sharable data should be available (for free or under fair conditions) for use and reuse by others, unless restrictions apply e.g. for protection of personal data, confidentiality, or intellectual property rights. Innovation Actions within the OPEN DEI ecosystem collect and generate huge amounts of data. This data should be published with as few restrictions as possible and clear licenses for its use to allow better scrutiny of administrations' decision-making processes and realize transparency in practice.

The use of **open source software technologies** and products can help to save development cost, reduce the total costs of ownership (TCO), avoid a lock-in effect and allow fast adaptation to specific business needs because the developer communities that support them are constantly adapting them. On the other hand, development of open source reference implementations of API specifications is the basis for definition of most widely "de facto" standards nowadays, following a "driven by implementation" as opposed to "design by committee" approach. OPEN DEI should not only use open source software but whenever possible contribute to the pertinent developer communities.

Specifications of APIs and data models are crucial in the development of systems. By openness of a specification we refer to the public and royalty-free nature of the specification. The level of openness of a given **specification** (particularly when it is intended to be adopted as **standard**) is decisive for the reuse of software components implementing or using that specification. In this way, all stakeholders can contribute to the development of the specification, and it will be available in a way that allows several implementations in both proprietary and open source solutions. These open standards and specifications can and should be used more widely beyond the domain for which they were originally developed.

Recommendation 2: *OPEN DEI RAF should ensure a level playing field based on open source datasets/software/standards and demonstrate active and fair consideration of the coverage of functional needs, maturity and market support and innovation.*

4.1.3 Underlying principle 3: REUSABILITY

Reuse means that system architects confronted with a specific problem seek to benefit from the work of others by looking at what is available, assessing its usefulness or relevance to the problem at hand, and where appropriate, adopting solutions that have demonstrated their value elsewhere. This requires the involved stakeholders to be open to sharing its interoperability solutions, concepts, frameworks, specifications, tools and components with others.

Reusability of IT solutions (e.g. software components, Application Programming Interfaces, standards), information and data, is an enabler of interoperability and improves quality because it extends operational use, as well as saves money and time. This makes it a major contributor to the development of Digital Transformation culture in the EU. Sharing and reuse of IT solutions fosters also the adoption of new business models, promoting the use of open source software for key ICT services and when deploying digital service infrastructure.

Recommendation 3: *OPEN DEI RAF must support reusing and sharing of data and solutions, enabling cooperation in the collaborative development of data models and solutions when implementing Digital Transformation pathways.*

4.1.4 Underlying principle 4: AVOID VENDOR LOCK-IN

When establishing Digital Platforms, system architectures should focus on functional needs and defer decisions on technology as long as possible in order to minimize dependencies on vendors, to avoid imposing specific technical implementations or products on their constituents and to be able to adapt to the rapidly evolving technological environment. The OPEN DEI RAF should be able to support the adoption of concrete open standard technologies to use for the effective sharing of data for example, while at the same time choose technologies that will not impose any specific technical implementation and avoid vendor lock-in. The functioning of an implementation-independent technology requires data to be easily transferable among different sub-systems independently of how and who has implemented those subsystems, in order to support the free movement of data. This requirement relates to data portability - the ability to move and reuse data easily among different applications and systems, which becomes even more challenging in cross-border scenarios.

Recommendation 4: *OPEN DEI RAF should foster access and reuse of their digital services and data irrespective of specific technical implementations or products.*

4.1.5 Underlying principle 5: SECURITY and PRIVACY

Organizations and businesses must be confident that when they interact with other stakeholders they are doing so in a secure and trustworthy environment and in full compliance with relevant regulations. The identified technologies must guarantee all the stakeholders' privacy, and the confidentiality, authenticity, integrity and non-repudiation of information provided by organizations and businesses.

To establish trust between different security domains requires a common data sharing infrastructure based on agreed standards, policies and rules that are acceptable and usable for all domains. In addition to secure solutions, it is necessary to build a trust ecosystem that includes identification, authentication, authorization, trust monitoring and certification of solutions.

Recommendation 5: *OPEN DEI RAF must define a common security and privacy framework and establish processes for digital services to ensure secure and trustworthy data exchange between the involved stakeholders and in interactions with organization and businesses.*

4.1.6 Underlying principle 6: SUPPORT TO A DATA ECONOMY

Data-driven applications will benefit citizens and businesses in many ways. As a consequence, data has become an essential resource for economic growth, competitiveness, innovation, job creation and societal progress in general. Actually, the value of the Data Economy in the EU is estimated to grow from 301 € billions (2,4% of the EU GDP) up to 829 € billions (5,8% of the EU GDP).

In a data economy, data becomes a key asset that businesses provide as a way to generate value. And where businesses do not have the exact data that is valuable to their customers, they use their platform base to connect to other platform partners who DO have that data. Consumers and businesses then become more willing to pay for access to data if that data provides them with greater value: if they get premium access to high quality or exclusive content for example, or if the data is available in real-time. As life speeds up and more demands are placed on our time, people and businesses are increasingly willing to pay for access to the data that will give to them an advantage or will save costs or time.

Common data sharing infrastructures should come with marketplace functions enabling data providers to publish their offerings associating terms and conditions which, besides data and usage control policies to be enforced, may include different formulas for payment: single payment, subscription fees, pay-per-use, etc. In order to support monetization of data, it should also include the necessary backend processes supporting data usage accounting, rating, payment settlement and billing. Standards enabling publication of data offerings across multiple compatible marketplaces will be highly desirable.

Recommendation 6: *OPEN DEI RAF must define a data marketplace framework enabling parties to publish open and priced data, supporting the creation of multi-side markets and innovative business models which bring support to the materialization of a Data Economy.*

4.2 Reference Architecture Framework (RAF) specifications

This chapter proposes a conceptual model for integrated data-driven services for Digital Transformation pathways, to guide their planning, development, operation and maintenance by adopting organizations. The model is modular and comprises loosely coupled service components interconnected through a shared common data infrastructure.

The conceptual model promotes the idea of interoperability by design. It means that for the to-be integrated services to be interoperable, they should be designed in accordance with the proposed model, or at least mapped to it, and with certain interoperability and reusability requirements in mind.

The **Reference Architecture Framework** (RAF) proposed promotes reusability as a driver for interoperability, recognizing that the data-driven services for DT should reuse information and services that already exist and may be available from various sources inside or beyond the organizational boundaries of the adopting organizations. Information and services should be retrievable and be made available in interoperable formats (e.g. adhering to the FAIR principles[40]). To this end, the core reusable **Model Building Blocks** (MBBs), mainly representing information sources and services, should make their data or functionality accessible through well-defined services supporting data-oriented and event-driven interactions. The reusable building block approach finds a suitable application by mapping solutions against the conceptual building blocks of a Reference Architecture that allows reusable components to be detected, which also promotes rationalization.

Starting from the Reference Architecture case analysis (presented in Section 2) and relying on the requirements coming from the Innovation Actions under the CSA umbrella (presented in Section 0), the OPEN DEI project has defined the approach for designing a common Reference Architecture Framework able to describe the Cross Domain Digital Transformation.

The extensive use of sensors and connected devices is a common scenario in the implementation of many Digital Transformation solutions and in many industrial sectors. The huge amount of available data is able to cover many business scenarios. Data-driven pipelines and workflows management is nowadays crucial for data gathering, processing, and decision support. To cope with this complexity OPEN DEI has adopted the following 6C architecture,

[40] https://www.go-fair.org/fair-principles/

adapted from the one suggested by the German Industrie 4.0 initiative, and based on the following pillars (using a bottom-up reading):

- **Connection**, making data available from/to different networks, connecting systems and digital platforms, among several IT culture and cross organizations' boundaries, start from the capability to make data available from/to different physical and digital assets. Different devices or sensors are used to acquire a variety of IoT data, but also many systems are based on unstructured or multi-media files. Data and information may also come from existing IT systems, using sector-specific protocols or more common standards coming from the Internet of Things (IoT) world used to realize data transfers.
- **Cyber**, modeling and in-memory based solutions to convert data into information, leveraging several information conversion mechanisms. Digital representations (of assets, data and information) will be then shared with upper layers of the pyramid in order to improve the self-healing properties of the overall system.
- **Computing**, storing and using data on the edge or on cloud. Many of modern digital platforms use a combination of cloud and edge computing models, based on driving factors for established a more centralized and powerful computation capabilities, or faster, connectivity-friendly and secure computing at the edge of the digital networked platform. The forces fueling the demand for distributing computing technologies are advancing rapidly. This will create a paradigm shift for organizations moving along new digital transformation pathways, with potential changes affecting all players in the target business ecosystem.
- **Content/Context**, correlating collected data for extracting information, creating a digital space for data-information continuum, not something to push out to one side of the adopted information architecture. Modern businesses need a holistic approach with the end goal of driving the data (processing) and information needs. However, exploiting data is not as straightforward. So, data needs to be acquired (captured, entered via a data pipeline) and processed with a goal and context in mind, making it information, which essentially is about processed data, before moving to the next levels.
- **Community**, sharing data between people and connecting stakeholders for solving collaboration needs. Networked organizations will be able to collect and share knowledge and opportunities in the widest number of sectors so that its members can make the right decisions. The community around organizations could become increasingly important to collect and share information in a push&pull fashion.
- **Customization**, personalizing allows to add value to data following each own user perspective and to match their expectations. Multiple strategies can make it possible to address all aspects of the end user expectations and empower an individual to progress through platform functionalities in a natural way. Democratizing access to data is a promising approach to help unlock the value of data, but even the most advanced technology is of little value if people do not embrace it. This is a lesson that many businesses have learned the hard way; in order to avoid pitfalls, it is paramount to properly understand end user expectations and build the platform from the ground up while keeping in mind that the intended audience, even within a single organization, can be very diverse and must be properly segmented and with specific and varying needs.

In this scenario, complex systems based on distributed intelligence will be increasingly designed and operated based on accurate data sharing and analysis techniques. But as one of the upper layers is showing, the "smart" functions of the platforms will gain more power by leveraging the network and community effects, such that organizations' habits are changed while their dimensions of business are expanded.

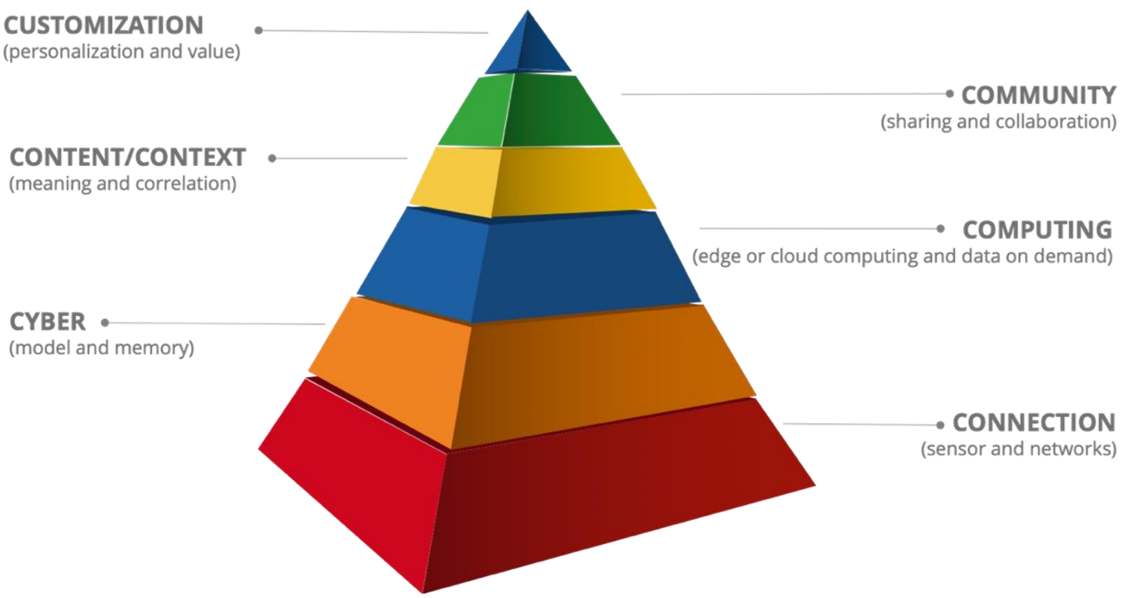

FIGURE 34. 6C ARCHITECTURAL MODEL

The above-mentioned 6C Architecture principles have driven the design of the OPEN DEI RAF, developed around the main concept of Data Spaces in which data is shared (published and accessed), identifying three main different layers described in the following using a bottom-up reading approach:

- **Field Level Data Spaces**, it includes the Smart World Services able to collect data and support the interaction with the IoT Systems (configuration, calibration, data acquisition, actuation, etc.), Automation and Smart Assets (robots, machinery, and related operations) and Human Systems (manual operations, supervision, and control, etc.).
- **Edge Level Data Spaces**, it defines the typical edge operations from the data acquisition (from the logical perspective) to the data processing through the data brokering. The edge services will play a key role also for data analytics (i.e. validating and improving models for data analysis).
- **Cloud Level Data Spaces**, it includes data storage, data integration and data intelligence operations on the cloud. The cloud services will process big data, deploy algorithms, integrate different source platforms and services, provide advanced services such as AI prediction and reasoning.

•

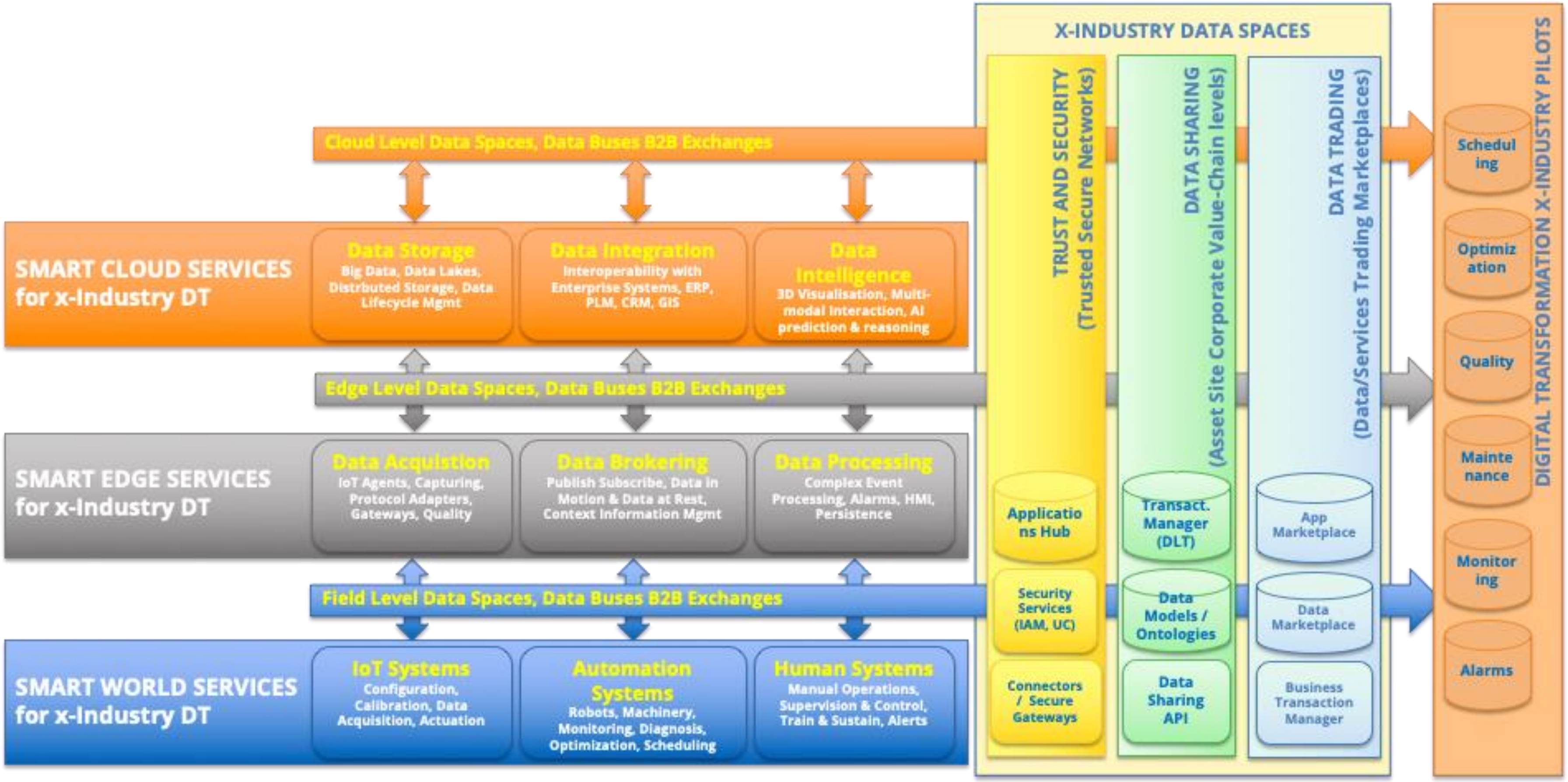

FIGURE 35. OPEN DEI REFERENCE ARCHITECTURE FRAMEWORK

Furthermore, all these horizontal Data Spaces spines will feed the OPEN DEI Reference Architecture Framework a main orthogonal dimension, named **X-Industry Data Spaces**, characterized by following components:

- **Trusted and Security**, incorporating technical frameworks and infrastructures that complements the previous to support trusted and secure exchange, which embraces:
    - **Applications Hub**, an infrastructure which collects the recipes required for the provision of applications (e.g. deployment, configuration and activation) in a manner that related data access/usage control policies can be enforced.
    - **Security Services**, a technical framework to support Identity Access Management, Usage Control and other security services.
    - **Connectors and Secure Gateways**, a technical framework for trusted connection among involved parties.
- **Data Sharing**, incorporating technical frameworks and infrastructures for an effective and auditable data sharing, which more in details embraces:
    - **Transaction Manager**, a distributed ledger/blockchain infrastructure for logging selected data sharing transactions.
    - **Data Models and Ontologies**, to leverage common standard and information representations.
    - **Data Sharing API**, a technical framework for effective data sharing: a data sharing API.
- **Data Trading**, incorporating technical frameworks and infrastructures for the trading (offering, monetization) of data, which embraces:
    - **App Marketplace**, enabling the offering of applications and application building blocks which can be integrated plug&play to enrich existing data spaces.
    - **Data Marketplace**, enabling the offerings around data resources with associated terms and conditions including data usage/access control policies as well as pricing schemas.
    - **Business Support Functions**, enabling data/applications usage accounting as well as implementing Clearing House, Payment and Billing functions.

Finally, all the mentioned layers serve the realization of **Digital Transformation X-Industry Pilots**, for enabling applications (sometimes sector specific) for supporting business scenarios from experiments.

4.3 Mapping existing sector-specific Digital Platforms to the RAF

This section aims to provide an easy mapping framework among the OPEN DEI RAF and the selected sector specific Digital Platforms described in Chapter 3, by adopting easy tools intended to highlight the important functional building blocks common to data-driven Digital Platforms across industries.

The first tool adopted is a high-level mapping table to cross-reference the OPEN DEI RAF service layers to the ones included in the compared Digital Platform. Secondly, a graphical representation of the main mappings is provided in the form of a picture comparing the approaches.

OPEN DEI RAF	QUALITY Digital Platform
Smart World Services	"Assets & Smart Products"
Smart Edge Services	"IoT Automation Services" and "Control Services" deployed on the edge/fog nodes (or 5G MEC)
Smart Cloud Services	"Data-driven Modelling and Learning Services", "Digital Twin and Planning Services", "Simulation and Huma-centric Visualization Services", running on cloud/HPC infrastructures
X-Industry Data Spaces	"Distributed Trustworthiness Framework" and "Data Lake", as well as "Digital Models and Vocabularies"
X-Industry Data Buses	External communication networks ("Internet / Data Centre Network") and "Value Chain Ledger"
Digital Transformation X-Industry Pilots	"Adaptive Digital Shopfloor Automation", "Multiscale ZDM Processes", and "User-centric ZDM"

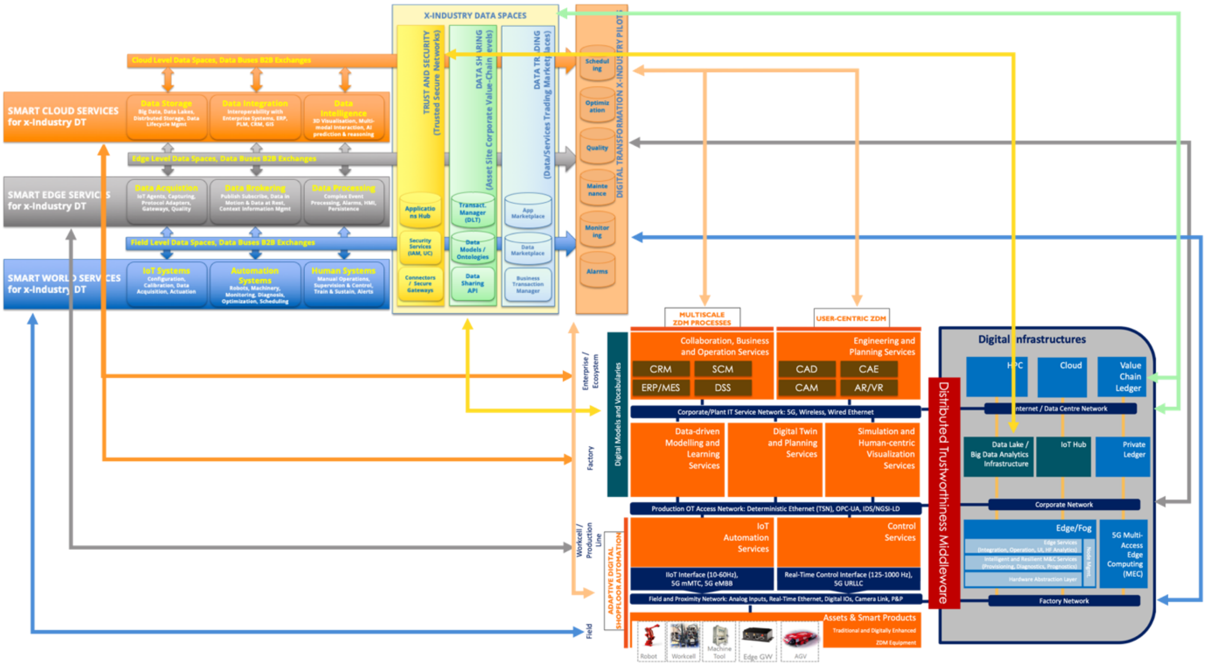

FIGURE 36. OPEN DEI RAF VS. QU4LITY RA MAPPING

OPEN DEI RAF	DEMETER Digital Platform
Smart World Services	“Indoor Devices”, “Remote Sensing”, “In-field sensors”, “Attached Devices”, “Field Machinery”, “FMIS”
Smart Edge Services	“Smart Farming Platforms and Systems” southbound agents (i.e. Lora, Sigfox, Zigbee, Bluetooth, 4G, 5G, etc.), and “Machinery Platforms”
Smart Cloud Services	“Decision Support facilities”, Integrated Delivery facilities”, “Performance Monitoring facilities”, “Visualization facilities”
X-Industry Data Spaces	“Public Resources” (for EO, Weather, Field information), “Data and Knowledge facilities”, “Security Protection facilities”
X-Industry Data Buses	“Interoperability facilities”, “DEMETER Hub Broker”, “Agricultural Interoperability Space”
Digital Transformation X-Industry Pilots	“Demeter-enabled Variable Rate Applications” and “Demeter-enabled Precision Livestock Farming Applications”

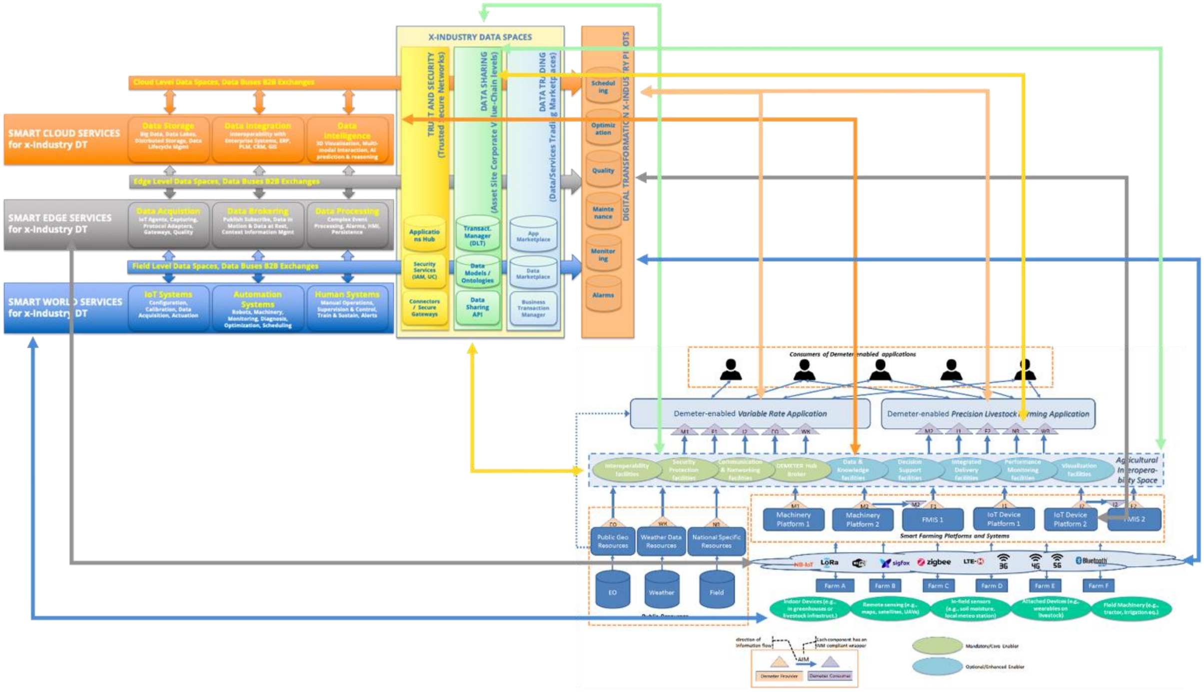

FIGURE 37. OPEN DEI RAF VS. DEMETER DIGITAL PLATFORM MAPPING

OPEN DEI RAF	PlatOne Digital Platform
Smart World Services	"Physical infrastructure"
Smart Edge Services	"Measurements and Set Point Notarization" and "Smart Contract Management"
Smart Cloud Services	"Shared Customer Database", "Flexibility Requests"
X-Industry Data Spaces	"DSO Technical Platform" and "Services for Prosumer Control"
X-Industry Data Buses	"Blockchain Infrastructure"
Digital Transformation X-Industry Pilots	"Aggregator Platform" and "Market Platform"

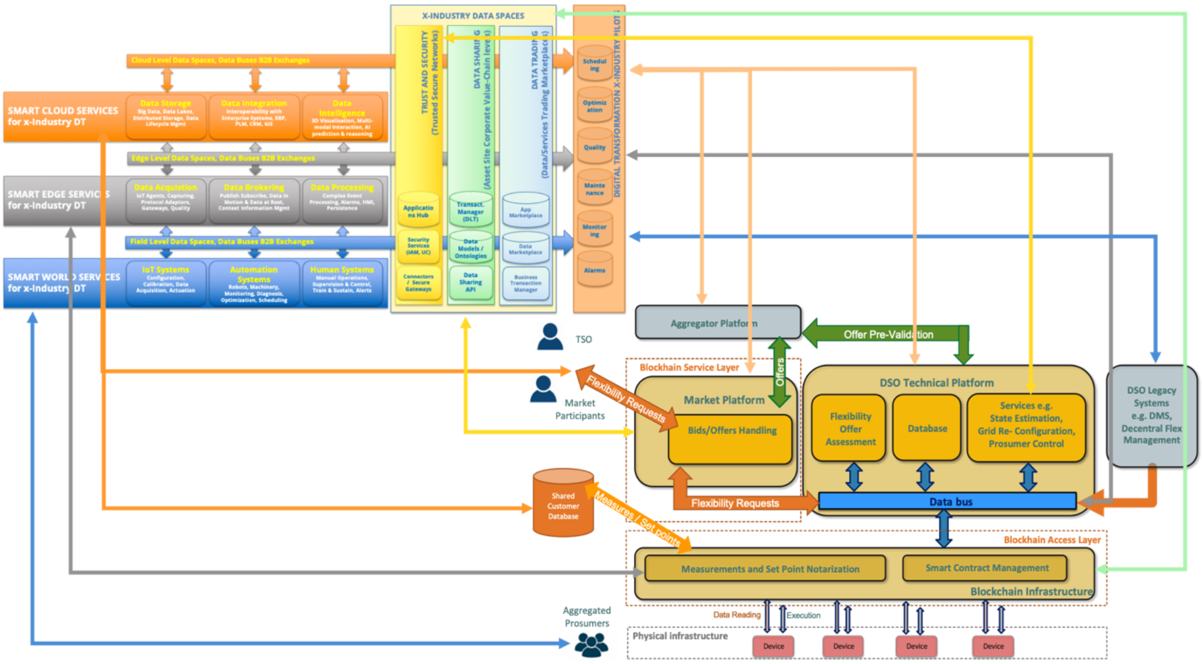

FIGURE 38. OPEN DEI RAF VS. PLATONE DIGITAL PLATFORM MAPPING

OPEN DEI RAF	ACTIVAGE IoT Ecosystem Suite
Smart World Services	"Device Layer"
Smart Edge Services	"Semantic Interoperability Layer" bridges
Smart Cloud Services	"Development tools" and "Analytics"
X-Industry Data Spaces	"Security and privacy Management", "AIoTES Apps" and "Native Apps"
X-Industry Data Buses	"AIoTES API"
Digital Transformation X-Industry Pilots	"ACTIVAGE Marketplace" and "AIoTES management"

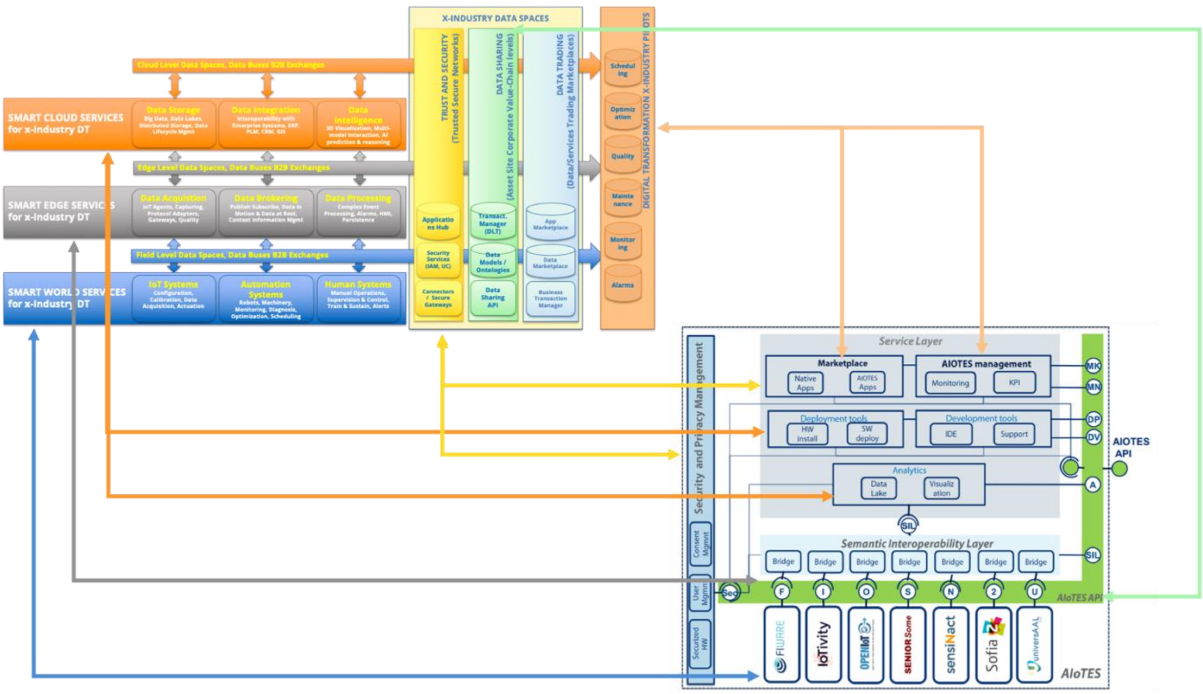

FIGURE 39. OPEN DEI RAF VS. ACTIVAGE IOT ECOSYSTEM SUITE MAPPING

5 FUTURE OUTLOOK AND CONCLUSIONS

In recent decades, many business organizations have invested in ICT to modernize their internal operations, reduce costs and improve the services they offer to citizens and businesses. Despite the significant progress made and benefits obtained already, organizations still face considerable barriers for exchanging information and collaborating electronically, and to fully exploit the Digital Transformation challenges. These include legislative barriers, incompatible business processes and information models, and the diversity of technologies used. This is because, historically, information systems were set up independently of each other and not in a coordinated way. The diversity of institutional configurations across extended value networks adds another layer of complexity trespassing the organization boundaries (e.g. in a supply chain).

Interoperability is a prerequisite for enabling exchange and reuse of information between different stakeholders. This makes it also a prerequisite for achieving the famous European Digital Single Market. Interoperability programmes in the EU have evolved over time. At first, they were concerned with achieving interoperability at syntactic level, focused in particular domains or between just a few well-known a priori set of systems, putting in place common infrastructure. More recently, they have started to address interoperability at the semantic level and with a bigger ambition (cross domain, supporting dynamic multi-side markets where actors are not known a priori). Governance, compatibility of legal regimes, alignment of business processes and secure access to data sources are some of the issues to be addressed next, to provide fully fledged public services.

The OPEN DEI RAF promotes 5 core principles on data/service exchange and reuse for the Digital Transformation by providing a set of common models, principles and recommendations. It acknowledges and stresses the fact that interoperability is not only an ICT matter, as it has layers of implications ranging from the legal to the technical. Addressing issues through a holistic approach in all these layers and at different cross-domain levels remains a challenge. The OPEN DEI RAF identifies an integrated approach to interoperability challenges at the same time pointing out the essential role of governance to ensure coordination of relevant activities across all levels and sectors of interest.

This report will serve as a starting point for the work to be carried out in relevant communities supported by OPEN DEI, especially the cross-domain Task Force 3 **"Digital Platforms & Pilots"**, already in its planning phase and going to be started in the upcoming months. The results of such activities will be used to validate the proposed approach, further conclusions and the lesson learnt during these activities will be reported in the next release of such report due by M24 (May 2021).