D 1.4
Report summarizing main contributions to other WPs – Second iteration

Action acronym	ConnectedFactories 2
Action Full Title	Global-leading smart manufacturing through digital platforms, cross-cutting features and skilled workforce
Grant Agreement Number	873086
Instrument	CSA: Coordination and Support Action
Deliverable Number	[D1.4]
Deliverable Title	Report summarizing main contributions to other WPs – Second iteration
Work package	#1
Work package leader	TECNALIA R&I
Dissemination level[1]	Public
Type[2]	R
Due date according to DoA	Sept 30th 2022
Actual submission date	Oct 19th 2022

[1] PU: Public, CO: Confidential, only for members of the consortium (including the Commission Services)

[2] RE: Report, OT: Other; ORDP: Open Research Data Pilot

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

VERSION MANAGEMENT		
	Name	**Beneficiary**
Author(s):	Luis Usatorre	TECNALIA
Contributor(s):	Alison Krauskopf, Olga Meyer, Jorge Martins, Katri Valkokari, Chris Decubber, Carlos Montalvo, Ilina Georgieva, Kosmas Alexopoulos, Ulrich Seldeslachts, Luis Usatorre	MTC, Fraunhofer (FHG), VTT, EFFRA, TNO, LMS, LSEC, TECNALIA
Reviewed by:	Ulrich Seldeslachts	LSEC

List of Abbreviations:

The following is a list of initialisations and acronyms used within the body of this report.

TERMS, ABBREVIATIONS AND ACRONYMS	
CCF	Cross-Cutting Factor
CE	Circular Economy
CF1	Connected Factories 1
CF2	Connected Factories 2
CS	CyberSecurity
CSA	Coordinated and Support Action
DMP	Digital Manufacturing Platform
EC	European Commission
GA	Grant Agreement / General Assembly
GDPR	General Data Protection Regulation
WP	Work package
ZDM	Zero Defects Manufacturing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Table of Content

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

List of Figures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Executive Summary

This deliverable D1.4 (Report summarizing main contributions to other WPs – Second iteration) is the continuation of D1.2 (as a **Second iteration**). We have maintained what it is already written on D1.2 improving it with new contributions, mainly reporting the meetings the Connected Factories 2 project partners have had with the DT-ICT-07-2018-2019 project representatives, industry representatives, policy makers and other related projects related or relevant to Digital Manufacturing Platforms and connected factories and conclusions.

1 Introduction

The aim of this work package is to identify and establish a structured understanding of key factors and new cross-cutting aspects on digitalization as well as reinforcing existing ones already defined in Connected Factories previous Coordinated and Support Action (CSA) project.

Connected Factories 1 (CF1) identified a number of key enablers and cross-cutting factors (CCF). These have been further refined in Connected Factories 2 (CF2) as shown in Figure 1

- Digital Tools and Technology (Technology – building blocks),
- Skills and Knowledge Transfer (previously skills and engineering tools and skills for the operation of the technologies),
- Business Models and Strategy (previously Business models / financial investment),
- Value Assessment and Optimisation (previously Added value / optimisation focus),
- Standards and Standardisation,
- Interoperability,
- Security.

These serve both as generic guidance for enterprises wishing to engage in a pathway towards digitalisation, and as a mapping/analysis framework for existing projects that serve as case studies. CCFs are key enablers that need to be systematically addressed in all the respective activities and deliverables.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

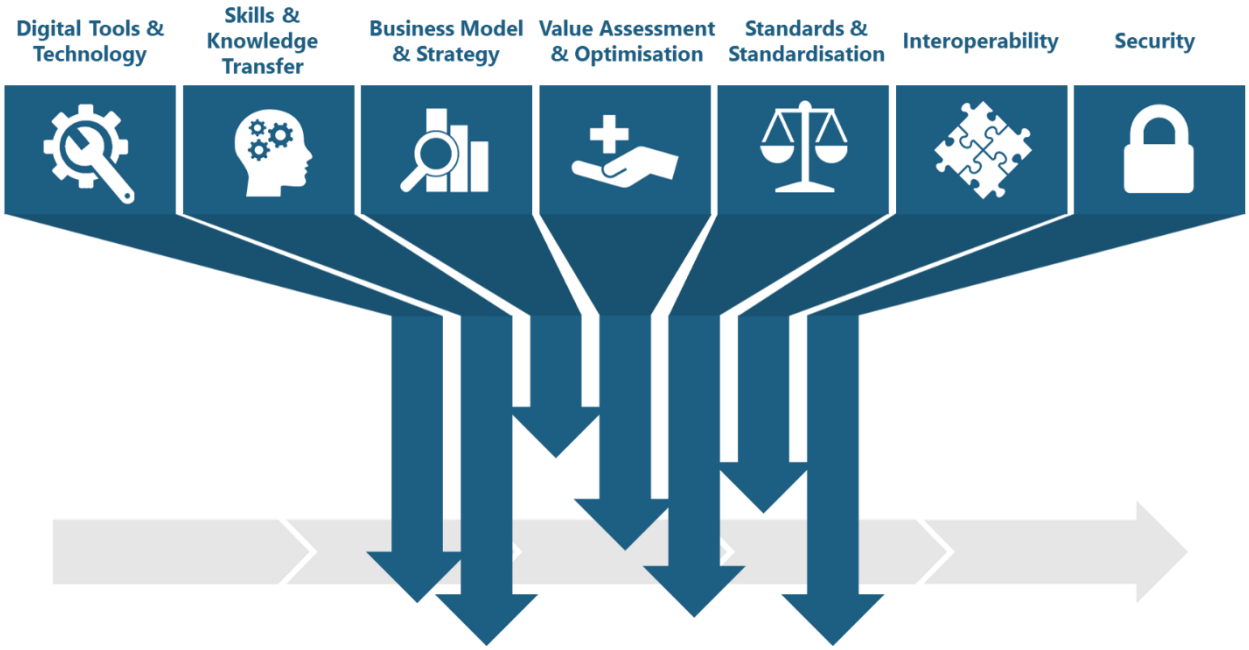


Figure 1: Connected Factories cross-cutting factors (CCF).

CF2 Work Package 1 (WP1) will focus on the following aspects that feed these CCFs:

- Added value and business models (Section 2);
- Industrial agreements and legal aspects (Section 3);
- Standards and Standardisation (Section 4);
- Interoperability (Section 5);
- Cybersecurity (Section 6);
- Humans in manufacturing (Section 7).

WP1 (Key enablers & Cross-cutting Factors) has a close relationship with WP2 (Pathways), WP3 (Cases), WP4 (Skills and Transfer of Knowledge) and WP5 (Outreach), as detailed in **Fout! Verwijzingsbron niet gevonden.** and builds further on Connected Factories 1 as shown in Figure 3.

Within this framework, WP1 will study the building blocks that WP2 will use to develop the pathways. Those pathways will be broken down into five stages or levels of increasing maturity. The pathway will then be mapped across several key operations and milestones will be identified for each operation at each level (see Figure 3 and Figure 4).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

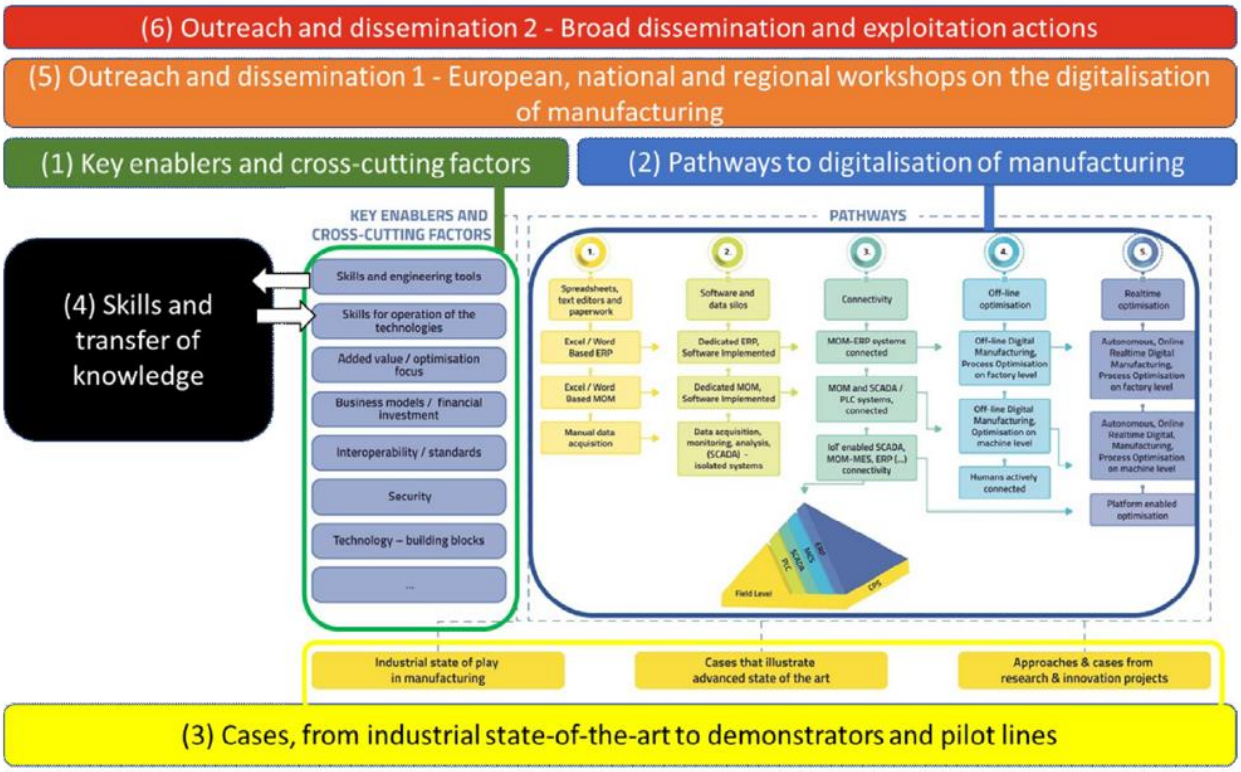


Figure 2: WP1 relationships

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

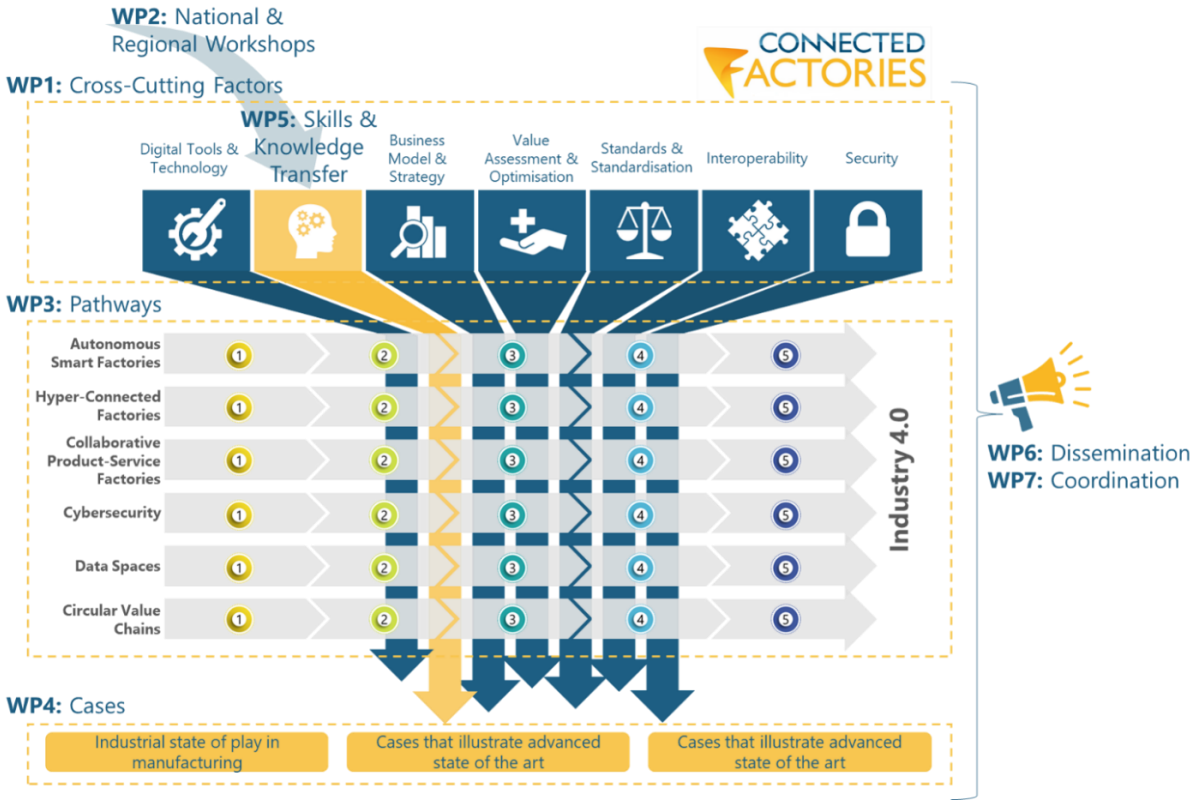


Figure 3: CF2 work package breakdown.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

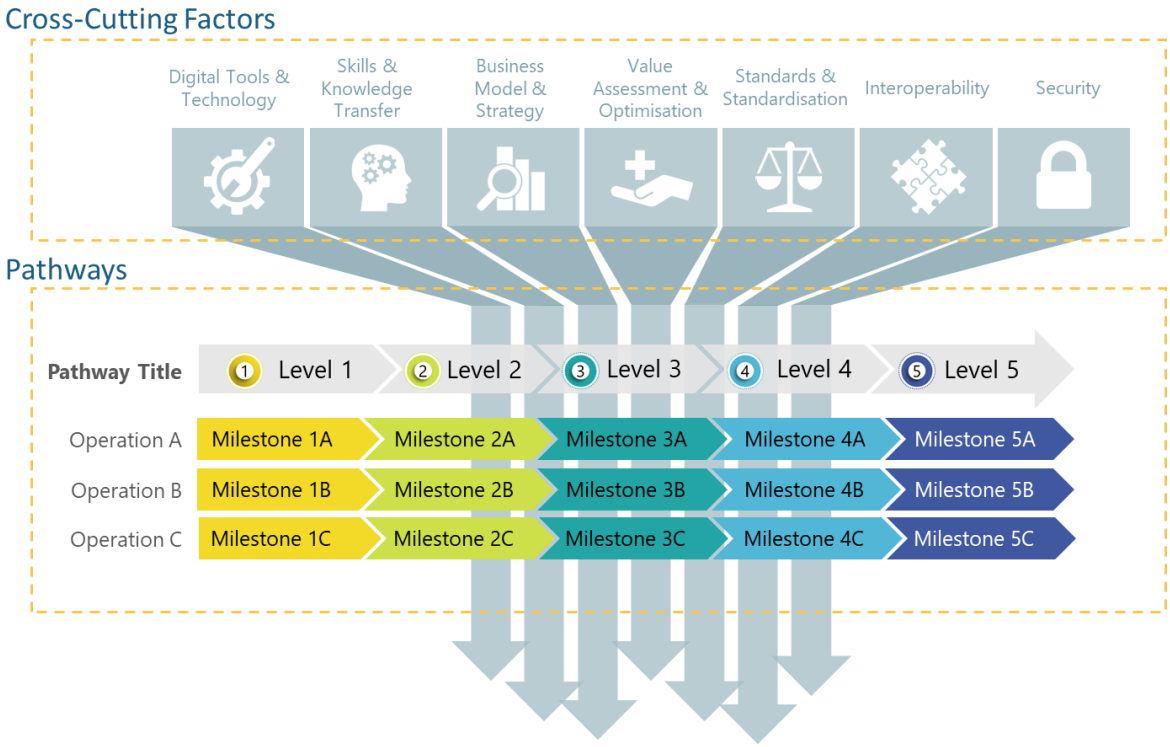


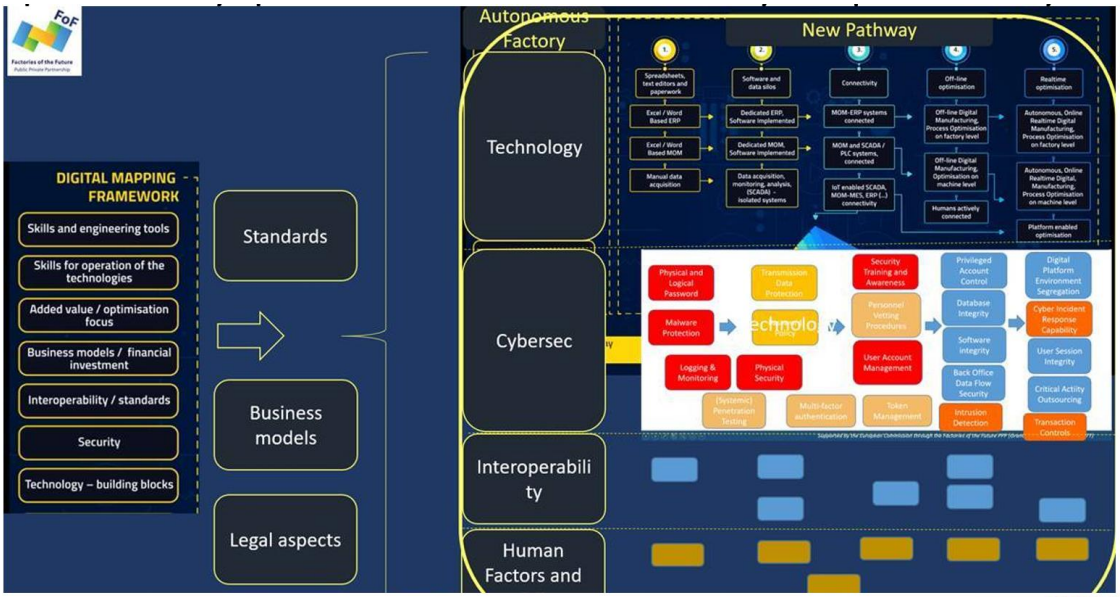
Figure 4: Connected Factories pathway development.

At the beginning of the project, several questions were identified:

- Will the CCFs shape the building blocks of the pathways or become separate pathways?
- Are the CCFs common to all pathways or specific to certain ones?

An initial approach taken by CF2, as shown in Figure 5, was to identify standards, business models or legal aspects as key support tools for all of the pathways, to separate cybersecurity as an individual pathway, and to further investigate 'Interoperability' and 'Human Factors' as new pathways.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.



Supported by European Commission grant number 873086

Figure 5: Different CCFs use in pathways

In any case, it was agreed that answering these questions falls outside the scope of WP1. The role of WP1 role is to both feed WP2 and WP3 and receive feedback from them via national and regional workshops. See the explanation on the Figure 6 below:

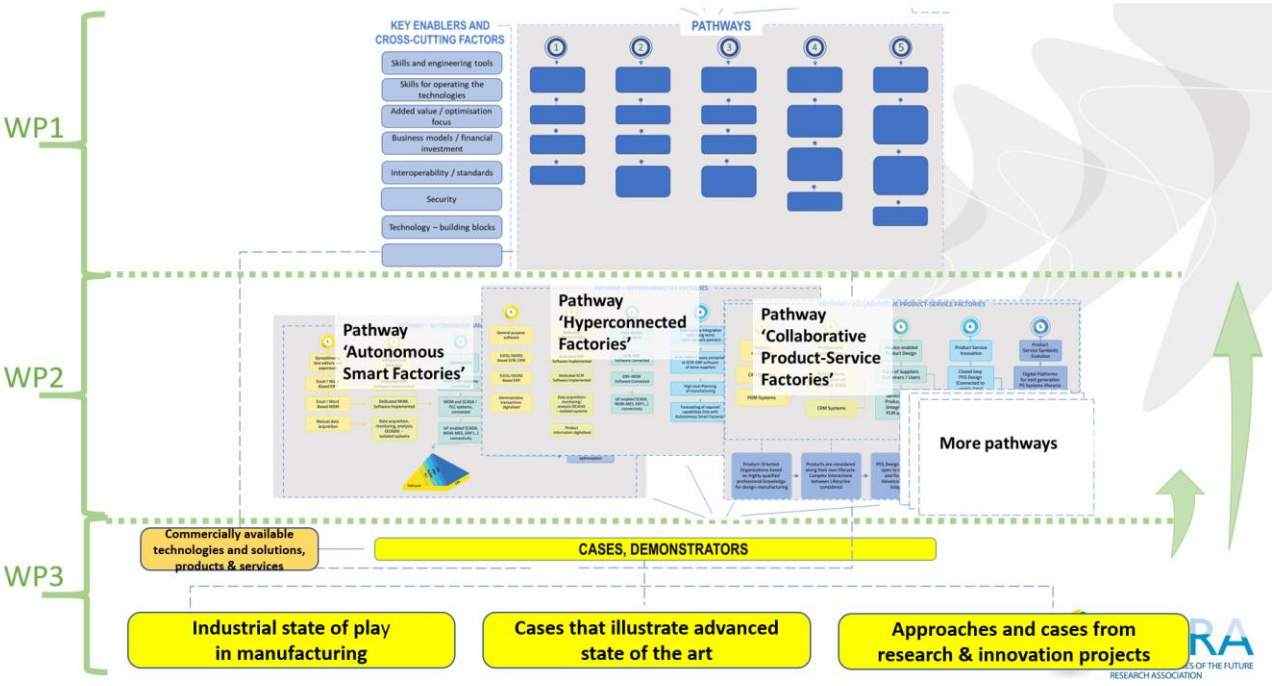


Figure 6: CF2 WPs relationship

This WP will build on top of Connected Factories 1 (CF1) outputs on business models, ownership, standardisation, security and liability. Some of the CCFs have already been discussed in CF1. Others are new. The relationship between CF1 and CF2 WP1 is depicted in Figure 7 below:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Figure 7: Inter-relationship between CF1 and CF2 WP1.

1.1 Cross Cutting Factors definition

The meaning of 'cross-cutting factors' within the context of the ConnectedFactories projects (1&2) and in particular in relation to the pathways to digitalisation of manufacturing has been described in CF1 - 'Deliverable 4.7 Revised set of consolidated pathways':

> *There are a lot of **cross-cutting aspects that enable progress along the pathways,** such as engineering skills and tools and also skills that are required for operating and managing the digital systems and tools.*
>
> *Another example are the many **technological building blocks** need to be put into place and need to be integrated: from data communication infrastructure such as field busses, industrial wireless or cabled networks to data storage, simulation tools, high performance computing, big data technologies, artificial intelligence, etc…*

*The ConnectedFactories 2 project endeavours to cover all or at least the most important of these different aspects, which is implemented also as a self-standing **structured glossary, which** is embedded in the structured wiki of the EFFRA Innovation Portal.*

1.2 Cross Cutting Factors subdivision

Each section of this deliverable is structured according to CCF subdivision. In most of the cases, the CCF has been subdivided in a different way from the one already done in CF1. The reasons are thoroughly explained in each chapter.

1.3 Structured Wiki

The wiki is the part of the portal that includes the structured items ('taxons') with an short explanation and some references to key resources. The wiki is accessible at: https://portal.effra.eu/wiki.

The wiki is software and has been identified as D.1.1 OTHER in the DoW. **D1.1** describes the modifications on the wiki for each of the CCFs.

Projects and their use case can be described (mapped) using these items (taxons) as framework and this is then visible in different ways in the EFFRA Innovation Portal (for instance like this).

In deliverable 1.2, this mapping was initially presented considering some of the projects were just started so the information was still not very relevant,yet and only some project and cases had been mapped on the portal. (This information can even be extracted from the portal). Now, in D1.4, a much more intensive analysis

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

and mapping of the projects have been carried out. You can find the analysis of each CCF for each project in a separate section.

Videos and tutorials on how to take benefit of the portal can be found here: https://www.effra.eu/tutorials.

1.4 Examples from projects (mapping of projects) introduction

There is a need for a solid structured approach for describing and analysing solutions and approaches to digitalisation of manufacturing, including the deployment of digital manufacturing platforms. Therefore, one of the activities of the ConnectedFactories Coordination Action is **gathering of the key information** about projects, enablers, and cross-cutting aspects.

For example, **engineering skills and tools** are required, and employees need to have adapted skills for operating and managing the digital systems and tools.

Another important aspect is the **value or benefit** obtained while progressing towards the right hand side of the pathway. (See D2.4) For instance, the factory would gain responsiveness and speed, improved quality and reduced down-time, resource-efficiency. These gains do not only apply to the milestones on the right side, but also to the milestones that are situated on the left-hand side. These benefits will need to be analysed by the companies according to their financial resources or **investment needed**.

From a more technical point of view, **interoperability** is extremely relevant; not only since systems and since tools will very likely come from **different vendors**, but also since many **legacy systems** have to be integrated. In addition, many **technological building blocks** need to be put into place and need to be integrated: from data communication infrastructure such as fieldbuses, industrial wireless or cabled networks to data storage, simulation tools, high performance computing, big data technologies, artificial intelligence, etc…

Cyber Security is a requirement that became increasingly important while progressing on the different pathways The CyberSecurity Pathway in relation to the othe Pathways has been described in the D2.6 (Pathways cross-fertilization with Digital Technologies) and the different workshop (such as the introductionary one found here – others will be documented throughout the CyberSecurity chapter).

The following video presents a guidance on how to Map projects and use cases on the cross-cutting aspects (which builds on the content of WP3) and Cases with commercial approaches.

https://www.youtube.com/watch?v=sodfn_RI5u4

The following links lead to search results on project level and result-demonstrator level on the EFFRA Innovation Portal for a number of aspects that are crucial .to the development and deployment of digitalisation in manufacturing:

- Cybersecurity – **project search** – **results and demonstrator search**
- Interoperability – **project search** – **results and demonstrator search**
- Business model aspects – **project search** – **results and demonstrator search**
- Humans and digitalisation aspects – **project search** – **results and demonstrator search**
- Architectures – **project search** – **results and demonstrator search**

Cross-cutting aspects are described through a comprehensive set of structured lists, which also can be seen as a self-standing 'structured glossary'. These lists are included in the structured Wiki (see picture below) of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

the EFFRA Innovation portal, such that the collection and sharing of information about R&D projects, demonstrators and use cases is more structured and accessible.

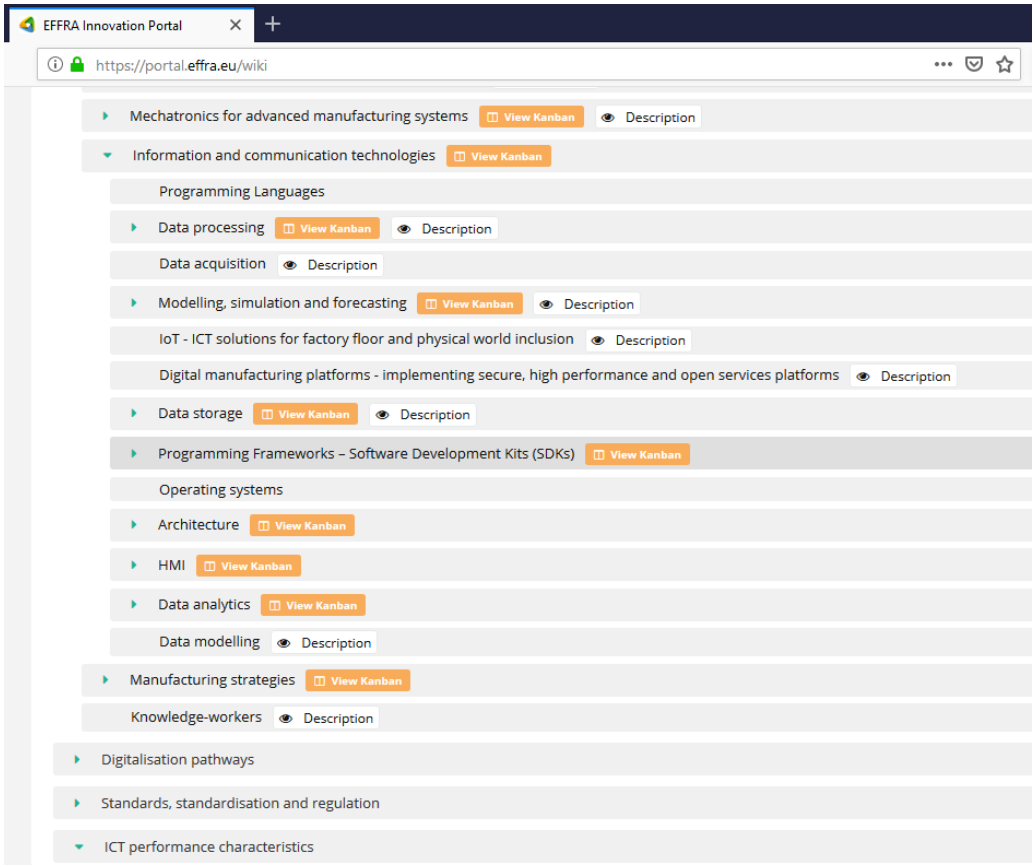


Figure 8: Wiki view

1.5 Reference documents introduction

In each of the chapters, the reference documents related to each CCF are named.

In the following video, it is possible to view how to Create reference documents as results and tag these as ReferenceDocuments: https://www.youtube.com/watch?v=l8eb8uT_S1s

1.6 Digital Manufacturing Platform (DMP) Cluster

Projects financed under the call "H2020-DT-ICT-07-2018- 2019 have created a cluster called "Digital Manufacturing Platforms for Connected Smart Factories". Its objective is to define a common cluster strategy for cooperating, dissemination and outreach of the cluster projects results.

The following Table 1 shows the projects' names, acronyms, coordinators and their details.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Name	Acronym	Coordinator	Logo	Coordinator contact
European Connected Factory Platform for Agile Manufacturing	eFactory	AIDIMME - Instituto Tecnologico Valencia	eFactory	Maria Jose Nunez; Usman Wajid
Zero Defect Manufacturing Platform	ZDMP	Information Catalyst		Stuart Campbell
Joining forces towards an European Industrial Autonomous Quality	Qu4lity	ATOS	QUALITY	Jorge Rodriguez
An Advances Circular and Agile Manufacturing Ecosystem based on rapid reconfigurable manufacturing process and individualised consumer preferences	Kyklos 4.0	TECNALIA	KYKLOS 4.0	Jason Mansell
Digital Platform for Circular Economy in Cross-sectorial Sustainable Value Networks	digiPRIME	POLIMI	DigiPrime	Marcello Colledani
Smart Human Oriented Platform for Connected Factories	SHOP4CF	TECHNISCHE UNIVERSITAET MUENCHEN	SHOP4CF	Meri Maghlakelidze

Table 1: DMP Cluster projects overview.

Along the CF2 project life, EFACTORY was renamed as EFPF and the logo was also renamed. Find the new one here down:

Figure 9: EFPF logo

Initially, the DMP cluster had defined the following working groups (WGs):

- WG1 Standardisation; (direct match with CF2 CCFs)
- WG2 Dissemination; *
- WG3 Joint Research; *
- WG4 Performance; *
- WG5 Business; *(direct match with CF2 CCFs)
- WG6 Open Calls; *
- WG7 Platforms; *
- WG8 Pilots; *

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

** for cross-domain DT topics OPEN DEI CSA can be addressed*

During the initial phase of the DMP cluster, there were direct links amongst these working groups and the CF2 WP1 cross-cutting factors. CF2 took the opportunity to discuss this undertaken during the joint meetings that were held with representatives of the DMP cluster and CF2 task leads. As the result, the mapping matrix has been established and the responsible task leads could be identified for the further transfer activities (see the Table 2).

DMP CLUSTER		CF2 WP1 TASKS	
WG	**LEADER**	**TASK**	**LEADER**
•WG1 Standardisation; *	Ingo Martens Olga Meyer	**•Task 1.3 Standards (task lead Fraunhofer)**	OLGA MEYER
•WG2 Dissemination; *	Joao Sarraipa UNINOVA	**WP6 - Dissemination**	EFFRA
•WG3 Joint Research; *	Joao Sarraipa UNINOVA Usman Wajid (ICE)		
•WG4 Performance; *	Usman Wajid (ICE) Luis Usatorre (DIGIPRIME)		
•WG5 Business; *	Gerardo Pagalday IKER	**•Task 1.1 Added value and business models (task lead VTT)**	**•VTT** -INNOLAB +INESC+STEINBEISS + RISE
•WG6 Open Calls; *	Carmen Polcaro INNOVALIA		
•WG7 Platforms; *	Usman Wajid (ICE)		
•WG8 Pilots; *	Carmen Polcaro INNOVALIA	**WP3 - Use cases**	INNOVALIA
		•Task 1.2 Industrial agreement and **Legal aspects**	TNO
		•Task 1.4 Interoperability (task lead Tecnalia)	TEC +FHG +CEA + UNOTT
		•Task 1.5 Cybercsecurity (task lead LSEC)	LSEC
		Task 1.6 Humans and manufacturing (task lead LMS)	**LMS** +MTC+SIRRIS+I.4.0+POLIMI

Table 2. Crossover from DMP Clusters to CF2 WP1 Tasks.

So, in recent discussions of the DMP cluster, the WGs have been accordingly realigned. Find here down (Figure 10) the new structure:

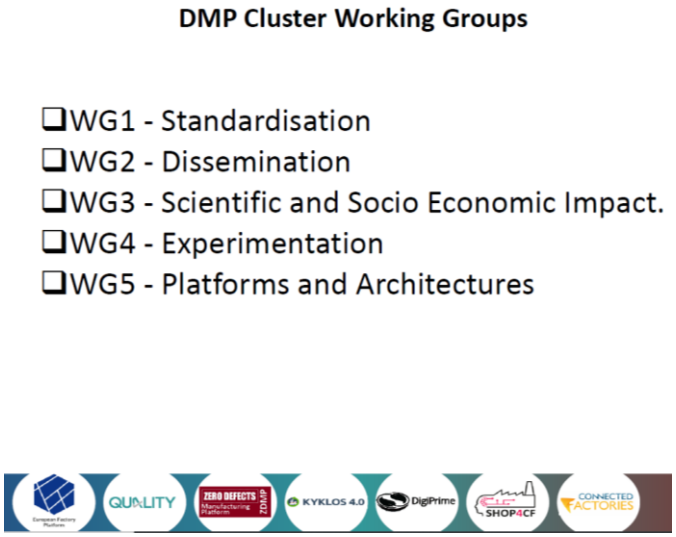


Figure 10: DMP cluster WGs

Find here down a list of the main events and workshops interacting CF2 and DMP cluster.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

1.6.1 Events:

1.6.1.1 Standards for digital manufacturing Webinar:

When: 20 October 2020

Short description: The Webinar focused on use cases and best practices that illustrate how standards are used in research & innovation in digital manufacturing. Special attention has been dedicated to the added value as well as gaps and needs.

- 236 Registrants
- 128 Participants

Agenda: https://cloud.effra.eu/index.php/s/3ZSPeg9tsLr0IXw

09:30 – 09:45	Participants connecting to the webinar
09:45 – 09:55	Opening – Overview of the Agenda
09:55 – 10:10	Industrial requirements for standards in manufacturing by Michel Iñigo Ulloa, MONDRAGON Corporation
10:10 – 10:30	ISO 10303 in EU projects like Kyklos4.0, Arrowhead Tools, Change2Twin by Kjell Bengtsson, Jotne
11:30 – 11:40	Standardisation and Research & Innovation, Luc Van den Berghe, CEN- CENELEC
11:40 – 11:50	The Digital Manufacturing Platform Cluster (DMP Cluster) and standardisation, Olga Meyer, Fraunhofer IPA
10:50 – 11:35	More use cases and pilots: how standards are used, identified gaps EFPF, Standards as trusted glue to federate digital platforms in the digital manufacturing domain, Karl Grün, Austrian Standards ZDMP, Standardisation Activities and the Role of CEN-CENELEC Workshop Agreements, Christian Grunewald, DIN QU4LITY, Application of Reference Architecture Model (IDS-RAM), Giulia Giussani, IDSA
11:35 – 11:50	The new edition of the German Standardisation Roadmap Industry 4.0 by Olga Meyer, Fraunhofer IPA, head of the Working Group Standardization Roadmap at Standardization Council Industrie 4.0
11:50 – 12:05	Cybersecurity standards and de-facto standards relevant for digital manufacturing by Ulrich Seldeslachts, LSEC

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

12:05 – 12:10	Collection and analysis of standards by ConnectedFactories, Chris Decubber, EFFRA
12:10 – 12:30	Q&A

Presentations: https://cloud.effra.eu/index.php/s/gPgyduCZldwbY6g

Recordings: https://www.youtube.com/playlist?list=PLpaccoqg8rxav7-sdcOIkTuDMe-Kb7g7

1.6.1.2 Cybersecurity Workshop:

When: 20 January 2021

Short description: The online workshop has provided an insight into the recent developments of projects that focus on cybersecurity in manufacturing: SeCoIIA and COLLABS project and into how cybersecurity aspects are addressed in other projects that focus on the digitalisation of manufacturing and the deployment of digital platforms. In addition, the workshop has provided an insight into European and international industrial cybersecurity standard (including de-facto) developments.

- 118 Registrants
- 65 Participants

Agenda: https://cloud.effra.eu/index.php/s/pbiKdHxSlMvFmd8#pdfviewer

09:45-10:00	Participants connecting to the webinar and opening with the overview of the agenda
10:00-10:10	Welcome & introduction by **Ulrich Seldeslachts**, CF2 - LSEC
10:10-11:40	**European industrial CS standard (and de-facto) developments:** - ENISA Industrie 4.0 developments & CyberAct Certification : **Renate Verheijen**, ENISA - Current focus of the working group and sub-working group and on international cooperation: **Detlef Houdeau,** Member of the Networks Systems Security, Platfform Industrie 4.0, Germany -
11:40-14:20 11:40-13:20	**European Digital Manufacturing Projects activities on CyberSecurity & Certification** - **Digital Manufacturing Project work on Cybersecurity** 1. QU4LITY, **Trujillo Salvador** & **Jose Francisco Ruiz** 2. ConnectedFactories2 3. SHOP4CF, **Morten Kühnrich** 4. ZDMP, **Artem Nazarenko**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

13:20-14:20	5. Other European projects with relevant security standardization works Panel discussion - **European Cybersecurity for Manufacturing projects** 1. CyberSecurity developments and Standards analysis by SECOIIA, **Reda Yaich** 2. CyberSecurity developments towards standardization by COLLABS, **Armand Puccetti** Panel discussion
14:20-16:00	**International industrial CS standard developments** - SBOM – Security Bill of Materials, **Allan Friedman**, NTIA - CSA IoT Taking Control of IoT - **Brian Russell**
	Panel discussion
16:00	**Close the webinar**

Presentations: https://cloud.effra.eu/index.php/s/pbiKdHxSlMvFmd8

Recordings: https://www.youtube.com/playlist?list=PLpaccoqg8rxaSN-DbE3frMjJBEBUE7h7a

1.6.2 DMP Cluster meetings:

- **DMP Cluster meeting**
  - When: 25 September 2019, During the World Manufacturing Forum
  - General information: among the 3 DT-ICT-07-2018 projects Qu4lity, ZDMP, EFPF
- **DMP Cluster + CF2 meeting** (online) - facilitated by ConnectedFactories 2
  - When: 12 March 2020
  - General information: 38 Registrants - 35 Participants
- **DMP Cluster + CF2 meeting** (online) - facilitated by ConnectedFactories 2
  - When: 4 June 2020
  - General information: 58 Participants
- **DMP Cluster + CF2 meeting** (online) - facilitated by ConnectedFactories 2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- When: 25 September 2020
- General information: 48 Participants

- **DMP Cluster + CF2 meeting (online)** - facilitated by ConnectedFactories 2
  - When: 2/3 December 2020
  - General information:
    - 02 December 2020 – 45 participants
    - 03 December 2020 – 49 participants
  - Presentations:
    - 02 December 2020:
      - https://cloud.effra.eu/index.php/apps/files?dir=/CF2_Cluster/Meetings/20201202_CF_DMP_Cluster_Plenary&fileid=8941
    - 03 December 2020:
      - https://cloud.effra.eu/index.php/apps/files?dir=/CF2_Cluster/Meetings/20201203_CF_DMP_Cluster_Plenary&fileid=8948
  - Recordings: https://www.youtube.com/playlist?list=PLpaccoqg8rxah7W6Nzi_yjTwHXL01uF6U

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

2 Added value and business models

Implementation of digital technologies in manufacturing companies is very much related with the **renewal of their business models**, or digitalization is seen as a means to implement the business model at hand. For a manufacturing company, becoming more sustainable and digital from typically quite linear efficiency-oriented operation models of manufacturing networks, there is first need to make strategic decision and consider renewal of its business model and modify its culture moving towards understanding added value at level of networked business.

The purpose of the section is to review and understand the prevailing and future business models[3] that are relevant to manufacturing in order to understand their linkage to other success factors. These future business models include examples of the following: cloud-based business models, platform-based business, product-service models, manufacturing as a service as well as business models related to transition towards Circular Economy (CE). Strategic perspectives and cost- and benefit-sharing between actors in CE will be paid attention to, i.e. different earning logics such as renting, payment according to performance, use, profit, availability.

The benefits and difficulties of adopting new business models enabled by digitalisation and circular economy will be analysed further. Therefore, **commonalities and differences** in the digitalization process of different types of companies in different markets and different sectors will be investigated (see section 2.3 positioning of the cluster projects). As for the other key enablers and crosscutting factors, there is a section on Business models in the structured wiki of the EFFRA Innovation Portal. Based on the analyses, the portal has been enriched with a number of new examples of business model change enabled by digital transformation.

Task 1.1 has deepened and updated the insight into the role of business models for digitalised manufacturing and in particular in relation to the deployment of digital manufacturing platforms and CE business models. Thus, the business impacts of digital technologies are **complex and multifaceted**, and seldom simply positive or negative. Comprehensive understanding of this issue is still limited.

2.1 General observations on added value and business models.

In **traditional** manufacturing network, operations of suppliers, lead producers (such as OEMs) and customers are seen as independent sequential tasks, which **form a value chain**. Already since the 1990s, however, this pattern has been changing and the theoretical discussion has emphasised the transfer from value chains to value networks. The trend among customers, lead producers (OEMs), and suppliers seems to be to engage in **forward transfer in their value chains**. This means that customers, lead producers or OEMs outsource manufacturing (give up earlier value chain phases), and their suppliers have increased services (add later value chain phases and give up some of the earlier phases). Concurrently, the interpretation of value has changed, and the intangible aspects of value added have emphasized.

Interdependency of operations and co-creation between the actors have been emphasized from several theoretical viewpoints, such service and data business. Furthermore, digitalisation of manufacturing networks has enhanced and enabled the **change in roles** as well as transparency in networks. Adoption of technologies also indicate evolutions regarding business models and, on the other hand, business models typically cause challenges or requirements to the technologies. As an example, CE business models pose

[3] A business model describes the rationale of how an organization creates, delivers, and captures value, in economic, social, cultural or other contexts. Business model can be seen as an integrating element between strategy and operations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

requirements to digital platforms in terms of **transparency** in the value chain or to application interfaces to enable industrial symbiosis. Circular Economy business models in particular will be analysed including network approaches integrating both upstream and downstream dimensions towards CE within the overall product life cycle (closed-loop supply chain, remanufacturing, recycling, and other activities. When possible, examples of transformation **from manufacturing driven business towards innovation driven service** business will be highlighted.

2.2 Reference documents on added value and business models.

CE has the potential to revolutionize many industries as companies begin to develop their business models around the ideas of extending product life cycles, expanding from products to services, and focusing on renewability and resource efficiency, or closing the loop. The use of data and IT has the potential to change the way value is created and to enable better resource efficiency for business. Many CE solutions are supported or even enabled by data and digital platforms. They ensure the availability, reliability, and transparency of the solutions to the relevant actors and stakeholders. Therefore, the traditional presentation of two CE circles (biological and technical cycles) could be complemented with the third necessary cycle of the CE: the information cycle (see Figure 1, presented by Valkokari et al. 2019[4]).

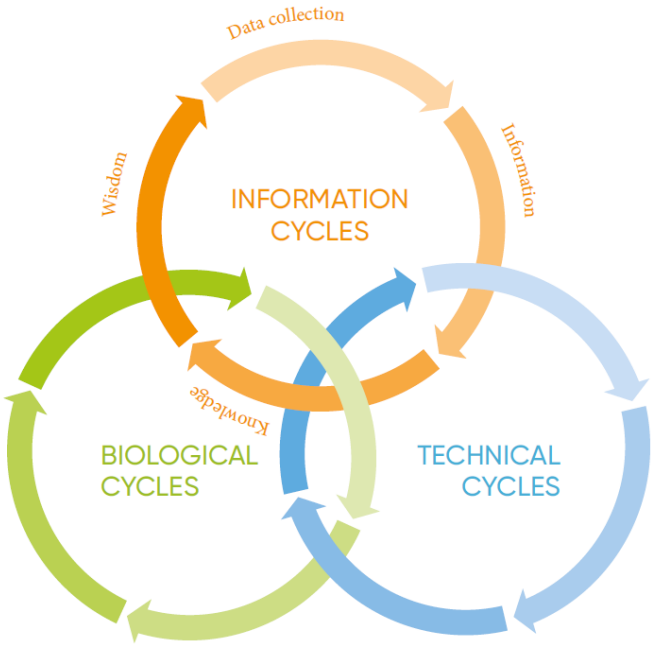


Figure 11: Information as a third dimension of CIRCULAR ECONOMY

In order to become more circular from typically quite linear operation models of manufacturing networks, a manufacturing company needs to first make strategic decision and consider **renewal of its business model and modify its culture moving towards a sustainable attitude and understand the core of the CE principles**. Embracing these principles require to modify internally the companies' business model, anyhow, there are

[4] *Valkokari, P et al. (2019). Advancing Circular Business.*

https://www.vtt.fi/sites/datatowisdom/PublishingImages/publications/FINAL%20Advancing%20circular%20business.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

several possible ways to change. Indeed, only once strategic agenda and the mindset of the entire company (and its network) has been changed, it is possible to efficiently move towards the adoption of Circular Manufacturing strategies (such as closing-the-loop or remanufacturing). Furthermore, the change of their current business model quite often requires also change on position within value network or even broader change (or disruption) of network.

2.3 Examples from projects (mapping of projects)

Industry 4.0 technologies contribute to sustainable operations management decisions and new business models through integrating value chains based on data collection and data sharing. Following this principle of sustainability-oriented management of manufacturing operation highlights the connection between digital manufacturing platforms and circular economy approaches. Consequently, Industry 4.0 ensures a framework for industry that combines competitiveness and sustainability, allowing industry to realise its potential as one of the pillars of transformation.

In practical terms, this entails an **integration of the more traditional understanding of efficiency management with a more comprehensive awareness of production operations impacts on the environment**, giving way to the emergence of sustainable products, sustainable production processes, and sustainable logistics decisions. Furthermore, this will require a business level transformation of product/service/system design, supply chain reconfiguration that moves beyond a singular focus on cost optimisation or linearity, towards business models and value creating systems.

From the perspective of efficiency management, the combination of technical enablers such as CPS, IoT, and smart factories introduces a shift from mass production to mass customisation, enhanced coordination between demand and supply, and the transformation of linear supply chains into digitally connected value networks. The search for added value by manufacturing firms aiming at closer customer contact, more stable revenue streams, and improved resource utilisation is also shifting their role from product seller into becoming solution and service providers.

The variety of business models therefore ranges from isolated use of data for differentiation (where the product is the primary source of value and product data is used strategically to improve both product and service offerings) to a gradual transition wheredata from multiple sources are combined to create additional value. The latter ultimately leads to platform-based delivery networks where companies collaborate to leverage data opportunities to reduce costs and extend product-service offerings.

Our theoretical synthesis of the projects proposes an evolutionary identification of value generation conceptual components. The general view is that the components illustrate each project's focus by describing the dominant logic they apply both to capturing economic value and to create value to customers. This is a typological flexible view that outlines components in a value-oriented activity system that is made up of interdependent activities, where possible configurations build-up on each other and grow in complexity.

The dimensions of digital sustainable manufacturing reflects the intersection of two main dimensions: (1) the use of digital technologies to exploit and explore information on manufacturing processes and the performance of manufacturing equipment; and (2) the applied use of that information to strategically direct either the improvement of existing company level processes or building broader sustainability impact through value network level thinking.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

At the level of the two top quadrants (of Figure 12 see further below), value creation and delivery is determined by a focus on streamlining resources and capabilities, channels, partners and technology for the maximisation of efficiencies. At the level of the two bottom quadrants, value is mapped to different value circle actors (suppliers, partners, competitors, and customers) to attain a novel sustainable value proposition.

Crucially, **across all projects the focus is on the optimisation of the value creation architecture in terms of key resources and activities**. This entails the use of new enabling technologies increasing efficiency and improving performance at the levels of reducing costs, time and manufacturing failures. Value creation occurs through production, logistics management and quality control that become more efficient. Machine to machine interaction controls internal processes and connects them with suppliers. The delivery of value is on the individualisation and customisation of production.

In addition, **common across projects**, is the **aim to enhance the delivery of value through better understanding of customers' needs and experiences, achieved through data analysis-based segmentation and improved self-service digital channels** that aim to implement new revenue streams, generate time, and cost savings. This is particularly evident in the EFPF project.

Emphasis on **platforms that collect information** about the use of physical assets and make this information available for further processing are also a common feature of the projects. In particular, the emphasis is on the technical implementation of platforms that collect information about manufacturing processes and potentially about products throughout their entire lifecycle, so manufacturing firms can exploit **additional revenue sources through offering data-driven services** and act on feedback to improve process and product (e.g. projects QU4LITY and ZDMP). However, there is also concern with the development of platform infrastructure that allows the deployment of **human-centric industrial applications**, combining in a complementary way machine capability such as high accuracy and precision, with human assets such as creativity and adaptability (project SHOP4CF). The importance of platform and possibilities for platform based novel business were discussed with all projects during the first half of year 2022. As a general note, it can be considered that the different aspects of data or platform-based business are considered at the projects but it is challenging to find a clear business model for platform ownership and maintenance. Therefore, following the most recent findings of platform business, it can be summarized that **APIs** and other technical solutions enabling **integration between platforms** and other enterprise data systems are **crucial**.

Finally, a set of projects takes a differentiated look at new value creation models where data and services become products in themselves, composing **new value circles through new channels, new markets and customers**. Thus, the project KYKLOS looks at product servitisation strategy through the proposal of maintenance services, and product recycling/ reuse. Project DIGIPRIME, on the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

other hand, supports the future systematic creation of cross-sectorial circular value-chains for the remanufacturing and re-use of high added-value components.

On a second level of analysis, Figure 12 below further develops the conceptualisation of the integration of digital manufacturing platforms and CE business models. This is premised on the transformation of the way in which resources are utilised, i.e. the goal is closed production systems where resources are reused and kept in a production/ consumption loop that maximises the efficient use of resources through product-life extension, redistribution/reuse, remanufacturing, and recycling. Again, possible configurations determine a company's positioning along what might be considered an evolutionary pathway with increasing levels of complexity, supported by a close integration of the biological, technical and data cycles introduced in 2.2.

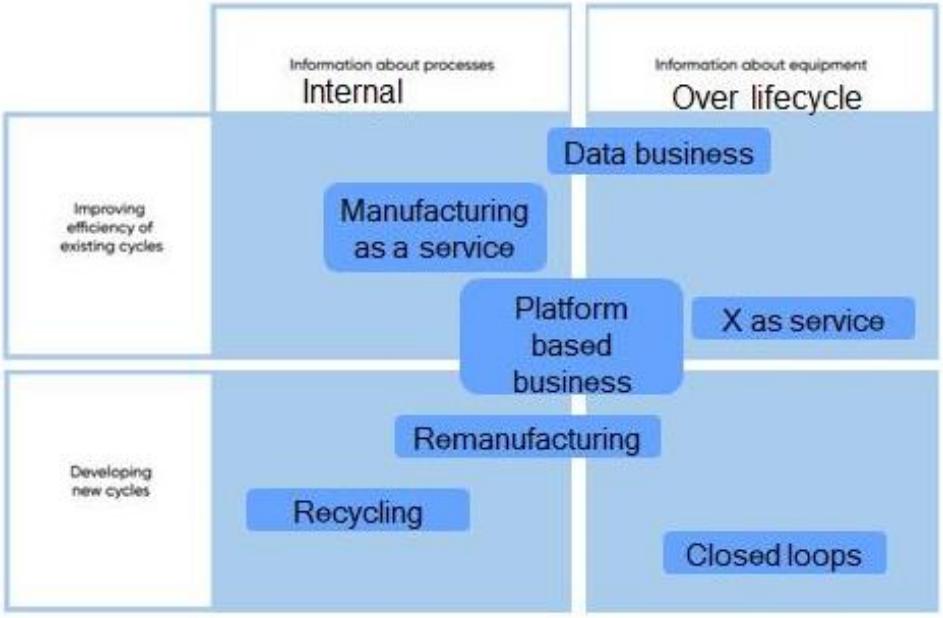


Figure 12: Mapping of business models

Data business concerns the adaptation of design and product decisions based on the active use of planning, monitoring and control data (e.g. in the form of sensors and apps), in a manner that reduces resource consumption to improve manufacturing productivity.

'**Manufacturing as a service**' and '**X as a service**' trigger the shift from resource- and order-orientation towards service- and requirements-orientation. This is possible because of platform-based business that enables parties to connect and share information related to supply and demand. In addition, based on parameters of resource production and consumption, firms can monitor and control the performance of operations, intervene in the process, and assess in real time the performance of machines, in order to plan adequate maintenance.

The use of similar sensor technology for performance monitoring is also fundamental for '**Remanufacturing**', where the goal is failure detection without the need to completely disassemble the product or components for effective repair; as well as for 'Recycling', where the tracking,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

recycling and management of manufacturing materials and waste are optimised. In both cases, the production and logistics of **sustainable operations management** are adaptable and based on the data provided by the resources of cyber-physical systems.

Finally, '**Closed Loops**' represents the broadest perspective on circular economy, with greater emphasis on significant extension of energy and materials circularity and a comprehensive use of data. The latter is used to **inform** not only **production**, but also on **product use** (i.e. through products embedded with information on components, materials, disassembly and recycling) **and post-consumption logistics** to enable manufacturers to more easily reuse, remanufacture, or recycle components of the product and its packaging.

2.3.1 EFPF- European Connected Factory Platform for Agile Manufacturing

The EFPF project has established a **federated digital platform to interlink manufacturing platforms**, smart **factory toolsets and Industry 4.0 concepts through an interoperable data spine** (Figure 13). This is enabling an **ecosystem of small smart factory platforms** to compete and cooperate to deliver customer value. An **integrated EFPF Platform and Marketplace** interlinks digital manufacturing platforms, smart factory tools and Industry 4.0 concepts. Unified access and single-sign-on is provided to interoperable tools and services. Cross-domain embedded pilot cases demonstrate how the integrated marketplace framework connects with external marketplaces in the EFPF ecosystem using API interfaces. This allows the filtered listing of products from external marketplaces. An **agent-based marketplace** performs marketplace negotiations in online bidding processes, therefore automating existing manual procedures. In terms of governance, the **European Factory Foundation** was established as a **legally independent body** that maintains, manages, and grows the EFPF digital platform and federated ecosystem, with an emphasis on **growing business opportunities for members and maximise trade, connectivity, communication and interoperability across the ecosystem.**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

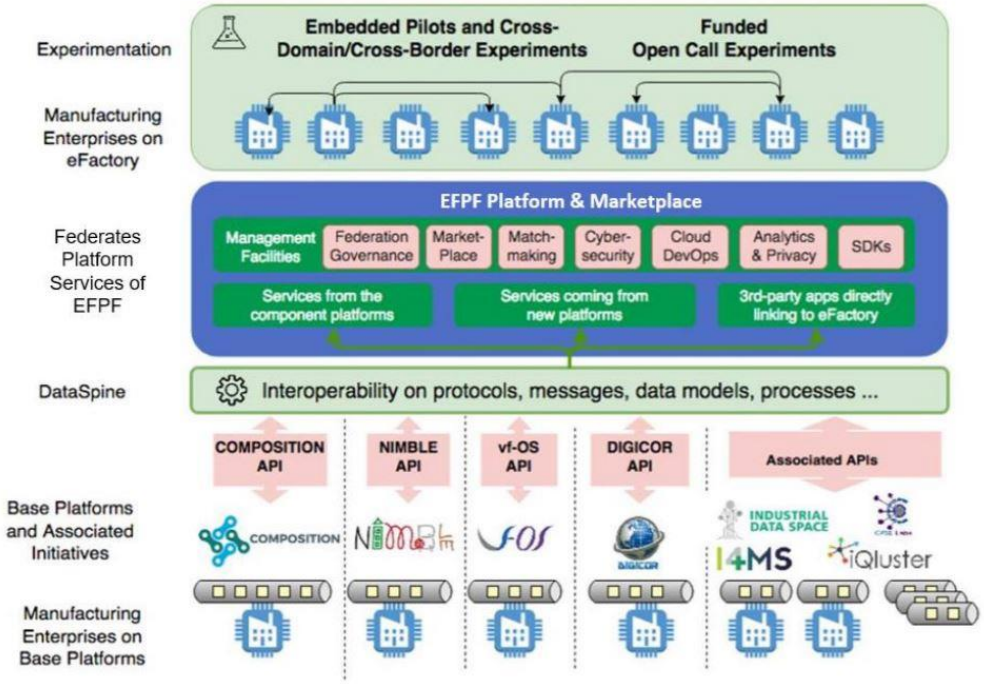


Figure 13: EFPF architecture

The **federated marketplace infrastructure** presented in figure above set up by the project allows multiple marketplaces to be connected. This provides a unified interface to multiple marketplaces, from where it is possible to search for different products listed on different marketplaces, and complete transactions. A **back-end business mechanism** allows the economic interactions between **different marketplaces**, so if a transaction is made through the marketplace, a commission is taken. The platform provides federated search mechanisms, so a manufacturing firm can search for a product on four connected marketplaces. This is a brokerage business model, as the platform allows connectivity between different types of products, different types of systems, platforms and protocols. The **platform's data spine enables** connectivity and interoperability between different existing systems and platforms, all of which with their own business models and their own user communities. Not being focused on developing the tools and services that other platforms would define as their value proposition, EFPF is focused on **developing a brokerage model that enables connectivity between different kinds of existing systems**, where the value is in enabling different systems to communicate, and different user communities to use the functionalities and services from different platforms.

An example can be found in data management platforms focused on zero-defect manufacturing, which are implemented within a shop floor environment, where manufacturers can see that the production system is relying on tools or services originating in a supply chain. To ensure consistency and quality in products, it is necessary that the supply chain is aware of quality constraints put in place for the product, and that there is compliance with regulations and certifications. EFPF has developed an **end-to-end supply chain management solution that ensures compliance and transparency**, as well as **visibility of activities that are taking place across supplier network**.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Manufacturers can **connect their quality system with the supply chain management system** and connect suppliers with their supply chain management system to make sure that the products that on the shop floor are compliant and developed in completeness with ability and transparency, following specified protocols. So being part of a federation, that solution should be accessible to the **DMP users** because it becomes **searchable on the marketplace**.

2.3.2 QU4LITY – Joining forces towards an European Industrial Autonomous Quality

QU4LITY provides factories and manufacturing equipment vendors **a one stop-shop platform for a comprehensive assessment of autonomous quality processes and digital continuity enablers** focused on the deployment of zero-defect manufacturing. QU4LITY relies on an **ecosystem** of **orchestrated open platforms** that span all phases of product and lifecycle to leverage advanced autonomous decision and control loops— i.e. multi-stage deep process analytics, digital twin orchestration and simulation-based control, embedded intelligence and real-time control, as well as augmented human-centred decision support capabilities. Drawing on **fourteen pilot lines**, the ecosystem demonstrates a standardised and certifiable, data-driven zero-defect manufacturing product and service model, which effectively operates a shift from current production quality methods into the disruptive concept of autonomous quality. This **enables manufactures and solution providers to develop, validate, deploy and adopt cognitive collaborative quality assurance solutions** throughout an entire supply chain, ultimately leading to cost and resource-efficient goods that are responsive to market and customer needs.

Q4ALITY's platform business model is premised on the concept of a one-shop-stop marketplace for autonomous zero-defect manufacturing solutions, providing a single-entry point to the project's intellectual property, and allowing users to explore, access, test and market services and solutions, as well as to access a portfolio of potential clients and partners. Alongside network building and the facilitation of collaboration of matchmaking, the interoperability of solutions and their compatibility with recognised standards are at the core of the platform's value proposition. A concrete example of the platform's impact on the project's pilot business models is the integration of novel analytical conformity inline inspections systems within the production line of (industrial ceramics manufacturer). Q4LITY is enabling the implementation of in-line automation components that are capable of automatically removing defective produce from production lines and introducing recycling/ re-introduced raw materials into the production line. In practical terms, this means that this novel in-line automation component is not only capable of early **of early product defect detection and warning, but also of self-readjusting for corrective action**, therefore effectively increasing the overall production effectiveness through facilitating process adjustment decisions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

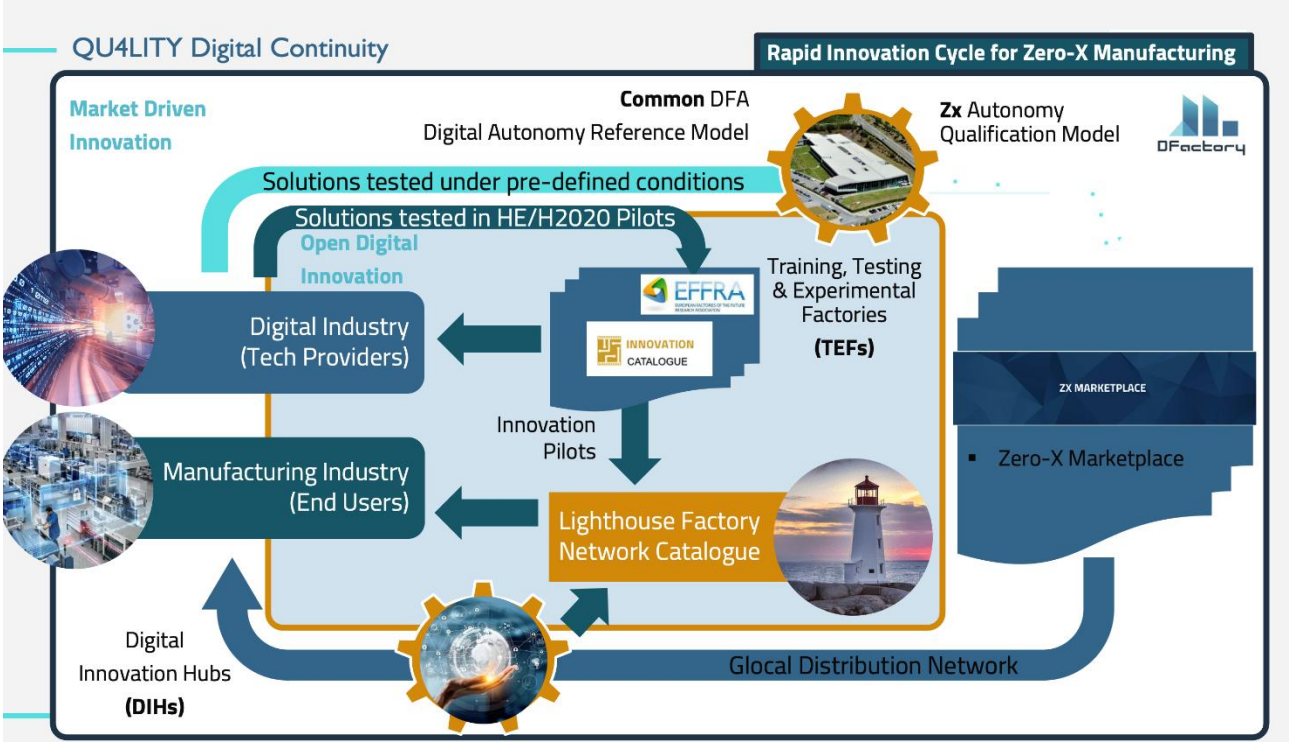


Figure 14: QU4LITY digital continuity

2.3.3 ZDMP – Zero Defect Manufacturing Platform

ZDMP is developing a digital platform for connected smart factories to **enable excellence in manufacturing through zero-defect processes and zero-defect products**. The project connects end users' systems (e.g. shop-floor and Enterprise Resource Planning systems) to enhance product and production quality assurance through data acquisition into a ready-built, open, reference platform, which ultimately simplifies the development of zero defect applications to deliver enhanced business value comparatively to do-it-yourself platforms. ZDMP has a **value-chain focus** that ensures the quality of a product through deploying modelling, detection, inspection and predictive techniques. Starting with the automotive, electronics, machine tools and construction sectors, the initial ecosystem will be extended through **open calls** that will **allow SMEs and start-ups to produce, pilot and adapt technical solutions through the platform**.

One example of such supply chain collaborative business development enhanced by digital platform of ZDMP project is the pilot case of construction industry[5]. This use-case involves 3 industrial partners: FLEX – the steel tubes producer, ALONG – the stone slabs produces and CONS – the construction company. The pilot showed that it is important that all the parties have an early access to information about potential delays and about the quality of supplies to act quickly and, if needed, to reschedule activities. ZDMP platform allows automated exchange of the critical information that

[5] https://portal.effra.eu/result/show/4511#structured-details-1937

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

can affect the schedule. Ability to adjust the activities regarding potential delays has significant impact on the construction consortia performance.

Aiming to service the **whole manufacturing community irrespective of specific sectors**, the project is concerned with making applications from technology components – software and hardware - which can improve the processing of products and improve quality. The components are of a generic nature and encompass messaging, data transfer and analytics related to process or product quality. There is a focus on specific zero-defect software components and inspection algorithms for process optimisation, the core principle being that other actors can take and build them into applications, which are then sold on the project's marketplace. The solutions developed through the project in terms of components will enable applications to be built faster, especially originating in small-size software companies, which provide services to manufacturing companies in a quicker way that is often developed in conjunction with existing customers and then placed on the marketplace. The effect of a **more accelerated development of tools and components** achieved through the project is that it contributes to an overall more cost-effective solution acquisition through the reduction of development and ownership costs. Post-project business sustainability will be assured by the constitution of IPFS, a company managing the project's IPR and operating as a marketplace. Taking commissions on applications sold, the marketplace will provide an environment where developers can acquire components, build new applications, and put them back on the marketplace.

Especially, the challenges faced by manufacturing **SME companies** has been raised up by the ZDMP project. Due to limited resources the SME companies do **not always have a strategic development agenda**. Consequently, they focus more on individual customers that re-thinking their offering to markets. This generates a broad portfolio of mixed technologies and products rather than longer-term development of unique offerings. Thus, the potential solutions for these challenges of manufacturing SMEs are identified: starting from understanding customer requirements to product architecture and manufacturing process improvements. The recording of the ZDMP presentation at the ConnectedFactories 2 event on 18 February 2022, provides insight on the value proposition of ZDMP and the goals of I4FS in the exploitation strategy. This presentation includes insights on different collaboration models between the customers, software developers and manufacturing SMEs.

2.3.4 KYKLOS4.0 – An advanced circular and agile manufacturing Ecosystem based on rapid reconfigurable manufacturing process and individualized consumer preferences.

KYKLOS4.0 is focused on the development of an **ecosystem that autonomously creates the configurations, methodologies, production techniques, autonomous decision-making processes and actions at all levels and stages of the manufacturing value chain**. This addresses the interrelated goals of increased energy efficiency, decreased use of raw materials through second use of materials such as manufacturing process waste, customer-centricity, and on-demand manufacturing. Through **cross-sector** pilots, the project adopts a **life cycle management approach** to devise and enable a set of product strategies for reconfigurable and reusable products, using a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

set of set of intelligent tools for real time analytics and prediction, as well as recommendation systems. Within the KYKLOS4.0 ecosystem (Figure 15), the customised open production system framework includes a set of **production – service simulation models** that enable responses to: product specifications, produce to order or make to stock requirements, product usage based on customer-profiling, product servitisation strategy through the proposal of maintenance services, and product recycling/ reuse. The vision is that though digital platform data and AI will allow a possibility to talk between the production equipment and operate alone without the intervention of the operator.

A concrete example of the synergies between manufacturing-as-a-service and product-as-a-service business models is explored in the pilot currently developing a new methodology and approach to design, produce and deliver the next generation of customisable wheelchairs integrating a system with postural device. The medical pilot is developing a fully automatized process where users can configure the chairs through web modelling tools according to individual specifications, where unique components of the wheelchair are 3D printed; and where augmented reality manuals are available to users. In complement to this, blockchain certification of the wheelchair components ensures product standards and quality, and predictive maintenance is employed to identify repair needs and prioritise replaceable/ reusable components[6].

Another pilot at the food industry aims to Reduction of Energy Consumption and Waste Management[7]. The goal is to control the variables that ensure the quality of the production and therefore the quality of the final product offered to the consumer. By monitoring the production variables, KYKLOS 4.0 platform will support PINDOS optimizing the resources needed through the production process; particularly, the resource optimization will be focused on ensuring the minimum energy consumption while maintaining high quality of the final product.

[6] https://portal.effra.eu/result/show/4537

[7] https://portal.effra.eu/result/show/11306

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

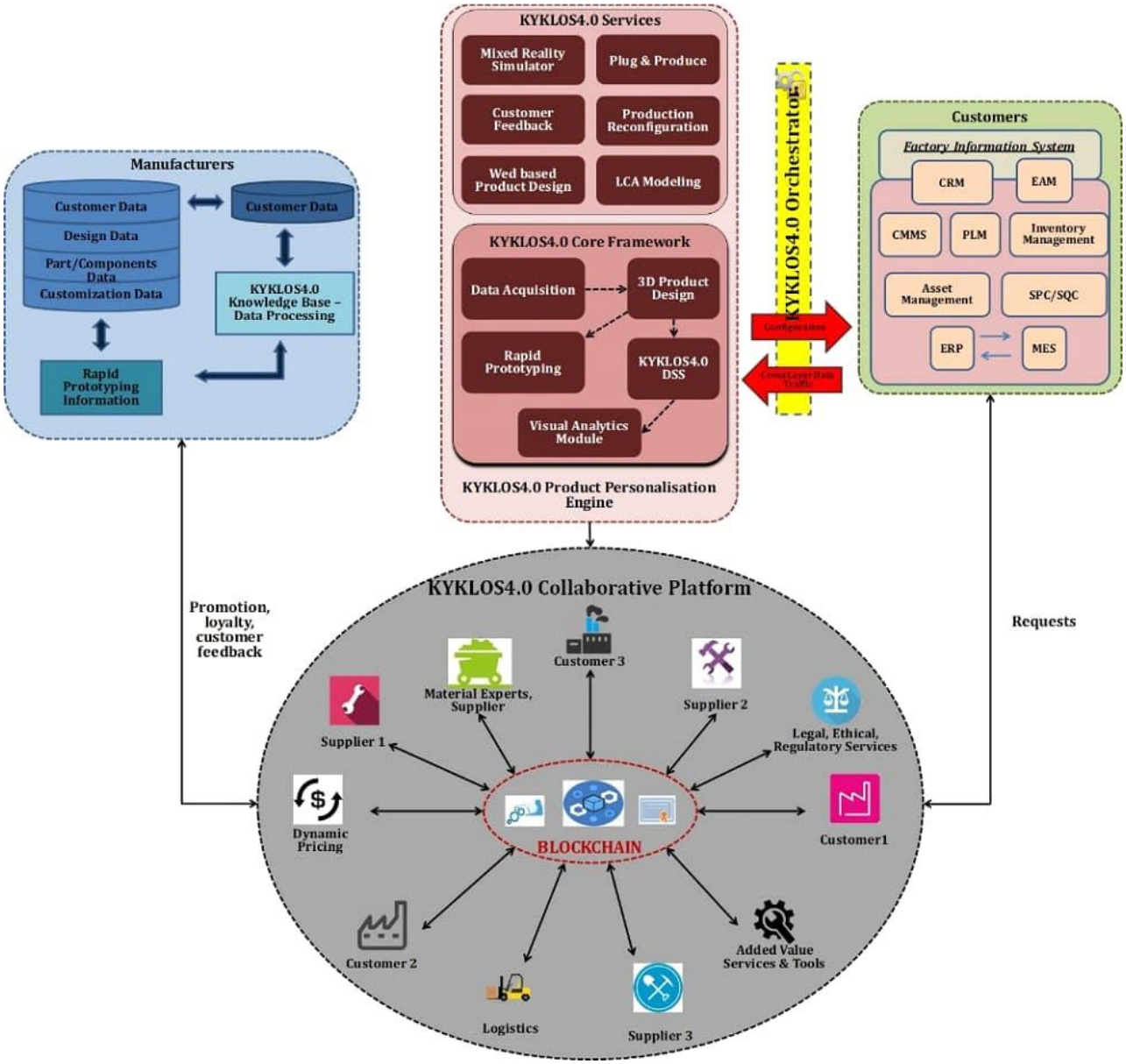


Figure 15: KYKLOS4.0 collaborative architecture

To ensure the continuity of the developed platform solutions, at the KYKLOS, the platform components are shared and used in several pilots. Thus, the pilots show that there is quite often need for tailoring of solutions as the circumstances, value network actors as well as their aims differ. The consortium is actively working to develop service packages based on the development solutions, there are different components from three different partners focusing on: predictive maintenance, virtual reality& maintenance, and sub-optimisation services.

Concurrently, there is an on-going discussion on how these components are enabled and supported after the project. Within these considerations, different business and operation models has been identified such as launching an association, developing company-oriented ownership etc. Furthermore, testbeds for learning, resource pooling and risk sharing access to complementary

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

competences are identified as cross-industrial collaboration opportunities enhanced by the digital platform.

2.3.5 DIGIPRIME – Digital Platform for Circular Economy in Cross Sectorial Sustainable Value networks.

DigiPrime is focused on the **development of a circular economy digital platform** that enables the **creation of circular business models based on the data-enhanced recovery and reuse of functions and materials**[8] .

A federated model of digital platforms for cross-sector business in the circular economy will be validated through cross-sectoral pilots and use cases in multiple industries including automotive, renewable energy, electronics, textile, and construction. The platform will help overcome current information asymmetry among value-chain stakeholders, thus contributing to unlock new circular business models based on the data-enhanced recovery and re-use of functions and materials from high value-added post-use products across manufacturing sectors. Through deploying a **multi-node federation structure** that is replicable on different, existing and prospective sectorial platform instances, DigiPrime supports the future systematic creation of cross-sectorial circular value-chains for the remanufacturing and re-use of high added-value components (i.e., batteries, composite and techno-polymer parts, textile components, and mechatronics / electronics).

Textile pilot[9] is a good example demonstrating the role of the DigiPrime platform to support the creation of a robust circular economy for textile-made components through a **cross-sectorial** approach between automotive (especially for interior trim) and other textile sectors (e.g., furniture, technical textiles, etc.). The aim of the pilot is reducing the information gap among textile industries, automotive industries, and other possible production sectors. This requites several actions: identify and characterise specific composition of the main automotive textile waste, define and test their dismantling procedure and define and test recovery, reuse and recycle practices for them to select and validate cross-sectoral applications. Furthermore, validation of best potential second life scenarios for automotive textile materials is a key aspect, which should be made on the base of materials characteristics and of markets needs and availability. Thus, the pilots have shown that the waste regulation may bring additional challenges to such close-the-loop strategies. The use of second life material requires region-specific permissions, i.e., reuse is hindered, as there is need to go through the authorisation process at each region separately.

[8] <https://www.digiprime.eu/the-digiprime-concept-and-objectives/>

[9] https://portal.effra.eu/result/show/4497

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

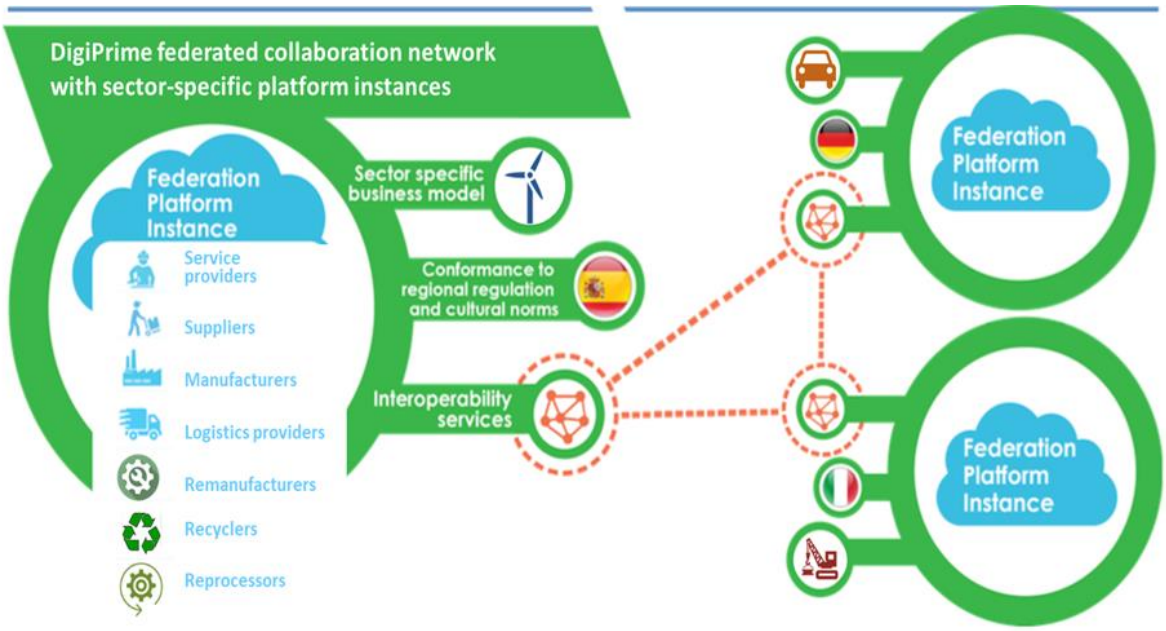


Figure 16: DigiPrime collaboration network

DigiPrime develops a multi-sided platform pursuing the **goal that all relevant actors of circular economy scenarios** - i.e., Products and materials manufacturers, de-manufacturers, re-manufacturers, material recyclers, Consultancy, Research and Innovation centres and ICT providers **are placed in a common space** thereby **facilitating contact between two or more sides** that would otherwise be unlikely to interact. The platform **facilitates transactions (data and services)** among those actors by **reducing transaction costs**: that's the real value DigiPrime business model relies on. In fact, the platform provides a convenient way of matching the different sides of an interaction (e.g. search or recommendation function), a virtual space to interact, a code of conduct, instruments that increase transparency and trust (i.e. comprehensive information, feedbacks, Material flow monitoring and aggregated system-oriented KPIs, Barriers Identification and legislation support, Circular Innovation Hubs integration, De- and re-manufacturing oriented product information formalization, Reverse Logistics and value-chain integration, Demand and supply forecasting, Circular production planning and control, Material characterization and certification), methods of secure transaction, etc. to which both sides agree.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

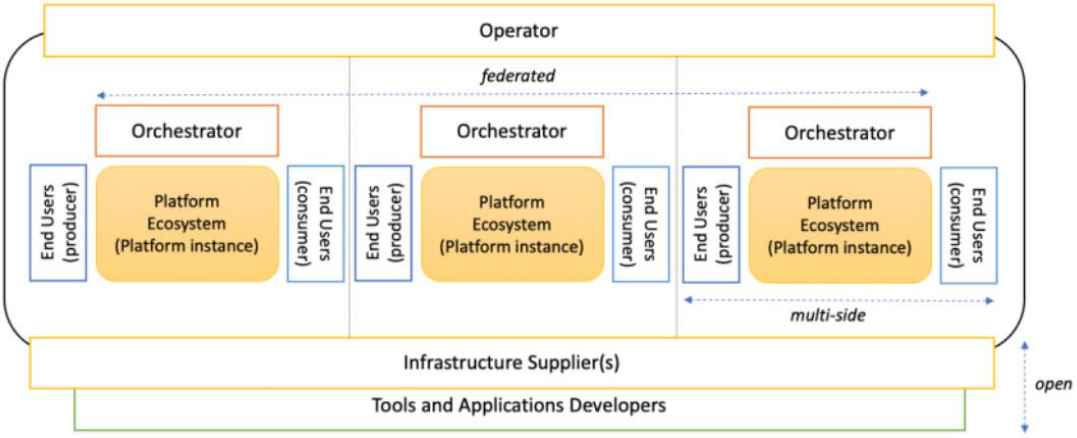


Figure 17: DIGIPRIME federated view

Moreover, the concept and availability of federated agile business collaboration platforms for the circular economy is at the core of the DigiPrime vision. The proposed federated platform model will lead to disruption and business benefits in all the above areas of circular economy impact. Unlike platform monopolies, federated platforms offer diversity and demand-led development in a wide range of industry sectors, yet they all adopt a common architecture, standards, and core technologies to facilitate interoperability and economies of scale.

In their simplest shape, existing online platforms do not intervene in the transaction (still guaranteeing its correct execution), except by asking for a fee from one or multiple sides of the transaction to make profit. Those kinds of platforms do not take control over the object of the transaction, nor on the transaction price. Considering preliminary investigations performed, the heterogeneous variety of requirements DigiPrime wants to address requires a more complex approach. For this reason, our platform needs to adopt a hybrid business model, choosing to act as a platform operator mediating between different market participants in one area of activity and as something like a distributor in another. Hybrid value creation is defined as the innovation strategy of generating additional value by innovatively combining products, data and services. To support such a vision, we currently foreseen a **model where a permissioned network of actors can be created on top of the platform**. To be in the network each actor will pay a minimal annual fee. Then each actor might earn incomes by selling products, data, and services on the platform and/or need to pay additional fees once consuming/acquiring products, data and services.

To further define the business model of the DigiPrime platform, the project has started to define key elements of the **Platform Design ToolKit**[10] a tool inspired initially by the business model canvas but extended with a set of tools especially thought for Platforms with several actors and with a distributed value generation. In the following only the Ecosystem mapping canvas and the final Business Canvas are reported for page limits; the overall canvas will be used as first reference for the business model generation and a key guideline for implementations, so to have always a clear vision shared among all the consortium partners.

[10] https://platformdesigntoolkit.com/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

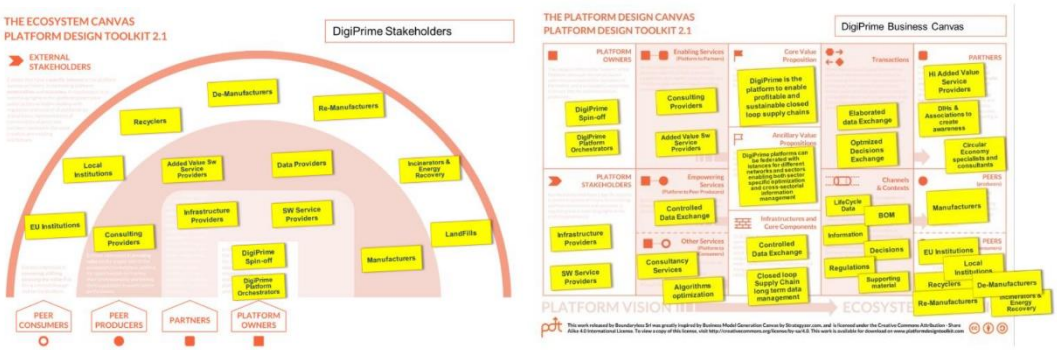


Figure 18: DIGIPRIME CANVAS

Also DigiPrime-project reported during the interviews 2022, that there is ongoing work related to the platform business model. Consequently, it is not yet sure who will be platform orchestration, how will have access to services or guidelines to levels of information sharing and what is the earning logic related to platform and services. The critical mass needs to be gained, linking the users and service providers together. Similarly, to other ICT-07 cluster projects possibilities of joint-venture, alliance or company-centric model are analysed. The final decisions are depended on use of services (i.e., their business potential) and pilots are currently starting to test cross-sectoral material flows and related business models

2.3.6 SHOP4CF – Smart Human Oriented Platform for Connected Factories

The SHOP4CF project is developing **an open architecture platform encompassing technologies based on RAMI 4.0 and FIWARE Technologies to support human workforce in manufacturing activities**, and providing basic implementation as a free, open-source solution. The project operates through the implementation pilots combining large-scale industrial leaders and smaller pilots selected through competitive calls. The focus of the **human-oriented technological platform** in on supporting human workers in the production activities of the manufacturing industry, with an emphasis on technological solutions that improve well-being and working conditions, automates repetitive tasks and increases workforce productivity. Operating as a **one-stop-shop marketplace** for developers and users and based on the **unification of interfaces for easy integration and cross-industry application**, the platform makes available a set of augmented / virtual reality tools including virtual planning of safety behaviour, augmented reality projection of assembly instructions, and digital twins of production lines.

From a business model perspective, SHOP4CF builds upon the **RAMP marketplace** to extend current functionalities with twenty additional technology components and tools – currently under development - to validate the impact of digitised processes and operate as a check list to assist in safety assessment of manufacturing digitisation. As a point in case, the introduction of automated guided vehicles in the shop floor prompts the need to perform safety assessments, which the project addresses with the development of a checklist tool that will be publicly available. In complement to this, an online learning platform will assist SMEs with integration. Finally, in terms of sustainability of the marketplace, the project aims to establish an association funded by membership, transaction, and consultancy fees to manage the app store, connect technology providers with user requests and offer consultancy as a service. The ambitious aim is to pursue the highly connected factory model to reap the benefits of all the data generated within the factory.

The consideration of continuity is ongoing also at the context of SHOP4CF project. However, the business model of platform and the different components provided are two separate streams. According to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

consortium rules the ownership of components belongs to partners and licencing the components is up to their decision. On the other hand, three different scenarios around the platform ownership are discussed: i) non-profit association, ii) spin-off company and iii) Integration to other platforms/marketplaces from other projects. Each of these options have its strengths and weaknesses and the decision requires agreement between the consortium members.

2.4 Key elements of platform-based business

As the ICT-07 cluster project examples show to create value added, a **platform needs to attract, involve, and interconnect value creators on both the supply and demand sides**. The core three elements – value and participants including both users and producers – describe the most important activity of the platform: the core interaction. **Matchmaking** between the value propositions of service components and their providers and users, i.e., manufacturing companies is a crucial starting point. The platform should provide an easy access to manufacturing companies, so that they can find appropriate digital solutions for development of their production system as well as be able implement these solutions.

After defining the rules for core interaction and the value the participants need or want to exchange, it is relatively easy to define the key enablers of platforms' network effects. To put it short, direct network effects explain how a platform attracts others to participate whereas indirect network effects arise from attracting others to contribute to in value creation. In all ICT-07 projects the **pilots and demonstrators are the key driver** for building the networks around the developed solutions and related services. However, the developed platforms are in most of the cases at the piloting phase and there is a need to agree on technical and co-operative resources after the project. This is closely linked to sustainability of platforms' business model and building the critical mass of providers and users when network effects as they set the rules of participating and sharing within the platform.

At the same time, **overall governance** practices define in more detail how the collaboration within the platform ecosystem is orchestrated. Open interfaces of solutions or between the platforms can enable network effects and create new interaction, which may not be directly controlled by the platform owner. Therefore, collaboration and coordination between the platform initiatives could enhance the broader impact and sustainability of platforms.

Finally, the last and crucial element of platform is the **value capture**, i.e., monetizing as it a critical question from the viewpoint of business model of platform ownership and maintenance. At the moment, most of the above-mentioned platform initiatives are comparing the different operation and ownership models. Thus, their thoughts on earning logics are quite traditional such as subscription or transaction-based models. The transparency in benefit sharing is critical, although the earnings within the platform economy are not or neither will always be shared equally. Each actor should take account of this in their business model, i.e., **platform operations should be profitable also to providers of technical components or business services as well as intermediators and platform owners**.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3 Industrial agreement and Legal aspects

Exploring and identifying the different regulatory frameworks, legal aspects, GDPR aspects and free data flow constraints.

3.1 General observations on legal aspects.

3.1.1 Types of industrial relations

Industrial agreements are at the **core of industrial organisation and innovation ventures**. In any industrial activity, agreements are codified in contracts. Such **contracts** are **standardised into several clauses** that ensure the provision and compensation of exchanges incurred between the parties in the agreement as well as provisions for failure to fulfil the contractual obligations agreed upon.

The form of the agreements and the formal contracts vary greatly considering the type of relationship between the parties and main features of the relationship (objectives, operational area involved, and the main mean of relational exchange that integrate the parties in the agreement). Figure 19: Type of agreements

The main types of industrial relations outlined at the top the figure 20 are expanded in the section of generic types of industrial contracts in section 3.3 further below. The figure above intends to make explicit the new nature of data flows that in the near future, in digital factories, become the main integration vehicle across many industries. In the remaining of this chapter some of the key challenges that this brings for industrial organisation and the governance of data flows are discussed.

gives an indication of the generic type of agreements. As will be seen bellow each of these agreements present particularities that must be considered to make explicit legal issues.

characteristics	**Supply relationships**	**Agreements Joint-Ventures**	**Regional industrial systems**
main objective	operational synergies	technological/ functional synergies	strategic synergy
main area involved	operating core 	support staff 	strategic apex 
main integration vehicle	material flow	expertise flow, skills exchange	associative and consortial bonds

Figure 19: Type of agreements[11]

[11] Nassimbeni, G. (1998). Network structures and co-ordination mechanisms: a taxonomy. International journal of operations & production management. 18, 6.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The main types of industrial relations outlined at the top the figure 20 are expanded in the section of generic types of industrial contracts in section 3.3 further below. The figure above intends to make explicit the new nature of data flows that in the near future, in digital factories, become the main integration vehicle across many industries. In the remaining of this chapter some of the key challenges that this brings for industrial organisation and the governance of data flows are discussed.

3.1.2 Challenges of I4.0 for data protection

Issues of data protection can be divided into three areas: the first one refers to the safety against disruption of the operations; the second refers to the protection of personal data; and the third to the protection of non-personal data at the different operational levels of the data pyramid.[12] The former is related to the risks that arise from the interconnectedness of the elements of the factory among each other and to the Internet of Things. When all the supply chain is aided by an advanced IT system that usually is situated on a cloud, this makes the whole production process exposed to the threats of hacking and sabotage. The protection of personal data is a tricky topic in the Smart Factory, because very often operators in these environments think that the only informational risks are those related to production, sales and supply-chain related data.

Personnel data: I4.0 requires an increasing level of integration of data from different sources, including data from not only workers, but also from different providers and sources. This enforces Privacy by design (PbD) requirements, due to both company security rules and regulatory requirements. A major aspect of the GDPR are the so-called legal grounds for lawfully processing personal data, one of which is consent. In several IoT applications where consent is used, it may even need to be explicit consent.[13] There are still some issues with personal data beyond GDPR:

- data consistency and the use of different sources of information and/or different time periods or geographical positions.
- data storage: although properly scrambled, masked, or blurred, the related persons probably are not aware such pieces of information do exist related to them; and
- problems related to EU citizens when requesting products or services outside of the EU. The harder problem is the service request mainly due to the absence of accountability, as a user never knows who gathers information about them and they cannot ask for access, erasure, or modification. Thus, there are two types of accountabilities:
    - Accountability regarding users; but also,
    - Accountability within the organization.

[12] Automation pyramid to the automation network. The former is made of five levels. Starting from the top, there is the Enterprise Resource Planning (ERP), a tool which refers to a variety of management activities. Then the Manufacturing Execution System (MES) follows, that manages production from scheduling to maintenance operations, to resource allocation. The third and fourth level aims at process control, based on Supervisory Control and Data Acquisition (SCADA) and the physical controllers known as Programmable Logic Controllers (PLCs). The last level is the production level, where interactions of machines, equipment and sensors (non-personal data) interact with personnel (personal data). This last stage generates issues that fall into the realm of the GDPR.

[13] Sun, S., Zheng, X., Villalba-Díez, J., & Ordieres-Meré, J. (2020). Data handling in industry 4.0: Interoperability based on distributed ledger technology. *Sensors*, *20*(11), 3046.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.1.3 Context of industrial "contract" agreements in relation to data generation, storage, transfer and analytics

Following (CARSA, 2021) **"Industry Agreements"** are tools designed to address the barriers that hinder the development of industry data ecosystems to enable industry stakeholders to enjoy the full benefits of the data revolution. They target economic gains for all participants and the creation of new market opportunities, new ecosystems and standards. Industry agreements may encompass three types of solutions:

- Federated Digital Infrastructures – FDI (e.g., reference architecture and reference models);
- Common Vocabulary Standards – CVS (e.g., common ontology, taxonomy, semantics, etc);
- **Relational Contractual Agreements – RCA** (e.g., rules for accessing and storing data, limitations on aggregation, and the use and further sharing of data, beyond a typical discussion on data ownership).[14]

Much of the current work developed under the programme "Factories of the Future" under Horizon 2020 has been focusing on developing and reaching agreements on FDIs and CVS while leaving RCAs underdeveloped. The form and content of the contract agreement will be strongly affected by the functionalities of industrial data infrastructures (e.g., Industrial data spaces). In the following in section 3.2 an exploration of the policy and legal framework is explored with an analysis of its limitations to guide in detail industrial agreements and their legal implications. In section 3.3 the notion of general forms and content of legal contracts agreements are outlined.

3.2 Reference documents on legal aspects data protection and data flows.

This section aims to briefly introduce a number of regulatory intiatives oriented to address and give regulatory framework to several aspects of data protection and data flow. The rationale of this section is to make aware the novice reader of the very many legal issues that are inherent to the deployment and implementation of digital factories across Europe. Legal issues that until recently industry is becoming aware of.

3.2.1 European Data Strategy

The vision

The EU should create an attractive policy environment so that, by 2030, the EU's share of the data economy – data stored, processed and put to valuable use in Europe - at least corresponds to its economic weight, not by fiat but by choice. The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. It should be a space where EU law can be enforced effectively, and where all data-driven products and services comply with the relevant norms of the EU's single market. To this end, the **EU should combine fit-for-purpose legislation and governance to ensure availability of data**, with investments in standards,

[14] (Carsa (2021) Background document shared for expert validation workshop within the "Study on technological and economic analysis of industry agreements in current and future digital value chains". A study prepared for the European Commission DG for Communications Networks, Content & Technology

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

tools and infrastructures as well as competences for handling data. This favourable context, promoting incentives and choice, will lead to more data being stored and processed in the EU.

The challenges

- *Availability of data:* The value of data lies in its use and re-use. Currently there is not enough data available for innovative re-use, including for the development of artificial intelligence. The issues can be grouped according to who is the data holder and who is the data user, but also depend on the nature of data involved (i.e., personal data, non-personal data, or mixed data sets combining the two).
- *Imbalances in market power*: Beside the high concentration in the provision of cloud services and data infrastructures, there are also market imbalances in relation to access to and use of data, for example when it comes to access to data by SMEs.
- *Data interoperability and quality*: Data interoperability and quality, as well as their structure, authenticity and integrity are key for the exploitation of the data value, especially in the context of AI deployment.
- *Data governance*: There have been calls to further reinforce the governance of data use in society and the economy.[15] For these data spaces to become operational, organisational approaches and structures (both public and private) are needed that enable data-driven innovation based on the existing legal framework.
- *Data infrastructures and technologies*: The digital transformation of the EU economy depends on the availability and uptake of secure, energy-efficient, affordable, and high-quality data processing capacities, such as those offered by cloud infrastructures and services, both in data centres and at the edge.
- *Empowering individuals to exercise their rights*[16]: Individuals value the high level of protection granted by the GDPR and ePrivacy legislation. However, they suffer from the absence of technical tools and standards that make the exercise of their rights simple and not overly burdensome.
- *Skills and data literacy*: Currently, big data and analytics are top of the list of critical skills shortages.
- *Cybersecurity*: In the area of cybersecurity, Europe has developed an already comprehensive framework to support Member States, businesses, and citizens to tackle cybersecurity threats and attacks, and Europe will continue to develop and improve its mechanisms to protect its data and the services building on it. The safe and widespread use of data-fuelled products and services will also depend on the highest cybersecurity standards. The EU Cybersecurity Certification Framework and the EU Agency for Cybersecurity (ENISA)34 are expected to play an important role towards that endeavour.

The roadmap for EU Data Strategy implementation (5 key actions)

The vision and challenges are supported by several key actions organised around five pillars that give coherence to the EU Data Strategy.

[15] 'Common European data spaces' is one of initiatives used as spearhead to generate a governance framework for industrial data. See https://ec.europa.eu/digital-single-market/en/news/report-european-commissions-workshops-commoneuropean-data-spaces.

[16] Same logic applies for companies

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

1. Key actions supporting the *development of a cross-sectoral governance framework for data access and use:*
   - Propose a legislative framework for the governance of common European data spaces, Q4 2020
   - Adopt an implementing act on high-value datasets, Q1 2021
   - Propose, as appropriate, a Data Act, 2021
   - Analysis of the importance of data in the digital economy (e.g., through the Observatory of the Online Platform Economy), and review of the existing policy framework in the context of the Digital Services Act package (Q4 2020).
2. Key actions to enable investments in data and strengthening Europe's capabilities and infrastructures for *hosting, processing, and using data, interoperability*:
   - Invest in a High Impact project on European data spaces, encompassing data sharing architectures (including standards for data sharing, best practices, tools) and governance mechanisms, as well as the European federation of energy-efficient and trustworthy cloud infrastructures and related services, with a view to facilitating combined investments of €4-6 billion, of which the Commission could aim at investing €2 billion. First implementation phase foreseen for 2022;
   - Sign Memoranda of Understanding with Member States on cloud federation, Q3 2020;
   - Launch a European cloud services marketplace, integrating the full stack of cloud service offering, Q4 2022;
   - Create an EU (self-)regulatory cloud rulebook, Q2 2022.
3. Key action to develop European digital competences by *empowering individuals, investing in skills and in SMEs:*
   - Explore enhancing the portability right for individuals under Article 20 of the GDPR giving them more control over who can access and use machine-generated data (possibly as part of the Data Act in 2021).
4. Key action to establish *Common European data spaces in strategic sectors and domains of public interest*.
   - Building in the experience of the European Open Science Cloud the Commission will support the establishment of nine data spaces (Manufacturing, green deal, mobility, health, financial, energy, agriculture, public administration, and data science skills.
5. Key action to promote *international data flows*:
   - To this end, the Commission will create a European analytical framework for measuring data flows (Q4 2021). This should be a durable framework that provides the tools to conduct a continuous analysis of data flows and the economic development of the EU's data processing sector, including a robust methodology, economic valuation, and data flows collection mechanisms.

3.2.2 European Data Governance (Data Governance Act)

A key pillar of the European strategy for data, the Data Governance Act seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data. The Data Governance Act will also support the set-up and development of common European data spaces in strategic domains, involving both private and public players, in sectors such as health, environment, energy,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

agriculture, mobility, finance, manufacturing, public administration and skills. The Data Governance entered into force on 23 June 2022 and, following a 15-month grace period, will be applicable from September 2023.

The data governance act aims support the development of data sharing systems with four sets of measures:

- Mechanisms to facilitate the reuse of certain public sector data that cannot be made available as open data. For example, the reuse of health data could advance research to find cures for rare or chronic diseases.
- Measures to ensure that data intermediaries will function as trustworthy organisers of data sharing or pooling within the common European data spaces.
- Measures to make it easier for citizens and businesses to make their data available for the benefit of society.
- Measures to facilitate data sharing, in particular to make it possible for data to be used across sectors and borders, and to enable the right data to be found for the right purpose.

3.2.3 OECD Guidelines

The main result of the expert committee was the identification of eight fundamental principles that still today influence the discourse on privacy and data protection:

Collection limitation: This principle entails that data collection should be limited as possible and that, when **personal or non-personal data** are obtained, it happens by lawful and fair means, with the awareness and approval of the data subject.

- *Data quality*: This principle refers to the relevance of personal data for the purpose for which they are obtained and, relative to that purpose, to accuracy, completeness, and veracity of the data.
- Purpose specification: This principle states that the data subject should be made aware of the purpose for which personal data are collected not later than the moment of the collection and that then the use of data should be limited to the fulfilment of the purpose. Every change in the subject should be specified too.
- *Use limitation*: Personal data should not be disclosed, made available or used for purposes other than those specified as according to the previous principle, unless required by the law or with the approval of the data subject.
- *Security safeguards*: There must be security safeguards that protect data against loss, unauthorised use, destruction, use, modification, and disclosure.
- *Openness*: This principle refers to the fact that it should always be possible to know the nature and use of personal data, as well as the identity of data controller and his usual residence. In general, all developments, practices, and policies relative to personal data have to be kept open.
- *Individual participation*: This principle lists all the ways in which an individual can be responsible for his own data. He must be able to have confirmation from a data controller that the data controller has data relating to him. Then, data relative to an individual should be communicated to him in a timely manner, at an inexpensive charge, in a reasonable way and in an intelligible form. Moreover, the individual should be able to act in case the previous rights are denied to him and finally, if the challenge is successful, data should be erased, updated or corrected.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- *Accountability*: The data controller must comply with measures that ensure the previous rights and held accountable for compliance. As mentioned before, these guidelines were the first impressive step towards data regulation.

The reach of this document can be explained by three main aspects. First, they are technologically neutral, i.e., they are not limited to automated data or to any industry, as well as to no sector, whether private or public. Secondly, they are written in a language that makes them both non-binding, as it appears from the use of the verb should and of structures non-typical of treaties, and very easy to understand, with a simplicity that ended up being perfect for the kind of complex evolution of the subject. Moreover, the guidelines add the principle of accountability, which had never appeared in earlier works. Finally, the most important point is that the eight principles call Member States to action but leaving space for flexibility.

3.2.4 European Data Protection Directive[17]

The Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data and the free movement of such data constitutes the first appearance of the right to data protection in European secondary law. This new set of rules, promulgated in 1995, was fuelled by the increased use of data in many industries and fields, consequent to the spread of Information Communication Technologies in the 1970s. The content of the Directive is not particularly innovative, as it follows closely that of the OECD Guidelines. However, two main aspects are relevant in this case. First, the protection granted by the principles addresses the freedom of individuals and their privacy, especially relative to data processing. Secondly, it promotes the free flow of information in the internal market of data. By the time the Directive was promulgated, the European data protection framework was far from being harmonised. Consequently, the Directive was conceived as a tool that, by harmonising the data protection practices in Europe, could promote the existence of an internal market of data too.

3.2.5 Article 16 of the Treaty on the Functioning of the European Union[18]

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals regarding the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted based on this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

[17] EU (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L 281/31. Brussels: European Commission

[18] Article 16 of the Treaty on the Functioning of the European Union (TFEU)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.2.6 The General Data Protection Regulation[19]

In principle, the GDPR has its roots on the Data Protection Directive, which was adopted by the EU in 1995. The GDPR is characterized by an extended scope on data protection as it affects all individuals and organizations, regardless of their geographical location, that record data and process information related to European citizens. Furthermore, the GDPR considers 'personal data' in an extended context covering information and identifiers like Internet Protocol (IP) addresses and cookies. The former directives were vaguely accepting as personal information any information that could directly or indirectly link to specific individuals. Moreover, notifications about discovered data breaches is now mandatory within 72 h of the incident, with imposed penalties ranging from 2–4% of an organization's global annual turnover during the previous fiscal year[20]. For companies involved in intense data processing activities, the appointment of a data protection officer is being provisioned. **GDPR requires that an impact assessment is performed to identify data security risks and mitigation strategies adopted by every organization.**

The GDPR also foresees that individuals have the right to: (1) provide their consent to organizations for processing their data, and (2) access any stored information related to them.

The GDPR is expected to result in substantial fines while the need to comply with the imposed regulations was anticipated to significantly increase business cost. To accommodate the GDPR ramifications would require an increase in business budgets of about 10%. [21]

The goal of the GDPR is to reinstate trustiness with consumers through transparency and security. GDPR addresses issues of personal data: Hacking—Use of stolen credentials and use of backdoor or command-and-control servers; Social phishing; Malware like spyware/keylogger, command-and-control servers and export data; and Services classification vagueness. GDPR addresses these challenges by:

- harmonizing of data-protection rules;
- fostering transparency and reporting obligations and updating the legal basis for processing personal information;
- allowing the switch of service providers in an easy and cost-effective manner;
- imposing the use of an advanced web application firewalls;
- detecting mobile app tampering;
- taking advantage of scalable multi-cloud advances;
- preventing malware from stealing credentials from victims' devices.

Concerning non-personal data in industrial applications, the GDPR is still in its infancy and CF2 waits to see further implications in different sectors.

3.2.7 European Cybersecurity Act

The EU Cybersecurity Certification Framework and the EU Agency for Cybersecurity (ENISA) are to give structure and enforce cybersecurity regulations in the single market. A European cybersecurity certification

[19] The General Data Protection Regulation (GDPR)

[20] Rodger A (2017) Ovum's mini-guide to GDPR. Ovum TMT Intelligence, London. https://ovum.informa.com/~/media/Informa-Shop-Window/TMT/Files/Brochure/Ovum-MiniGuide-to-GDPR-Sept-2017.pdf

[21] Sydekum R (2018) Can consumers bank on financial services being secure with GDPR? Comput Fraud Secur 6:11–13. https://doi.org/10.1016/S1361-3723(18)30054-X

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

framework. The EU Cybersecurity Act introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services, and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes, and services only once and see their certificates recognised across the European Union.

More information on the European Cybersecurity Act related to Cybersecurity can be found in Chapter 6 : Cybersecurity. Also other legal frameworks and regulatory components have been detailed in that Chapter.

3.2.8 Cybersecurity: EU COM Briefing

Digitising Industry (Industry 4.0) and Cybersecurity: EU COM Briefing

The New General Data Protection Regulation – Privacy in the Industry 4.0

For cybersecurity aspects, please refer to chapter #6.

3.3 Industrial contract types

The form of the agreement between two or more industrial entities will depend on the type of relation and type exchange conducted between the parties participating in the industrial agreement (Figure 20). The most common forms of industrial contract agreements are displayed and outlined in this section further below.

The **formalization of industrial contracts** in the context of industrial digitalization is **still in its infancy** and there is little to **no information as to the form and contents of the contract that ensure the protection of property, ensure delivery and quality of services, liabilities, etc**. These issues will be outlined in the sections further below.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

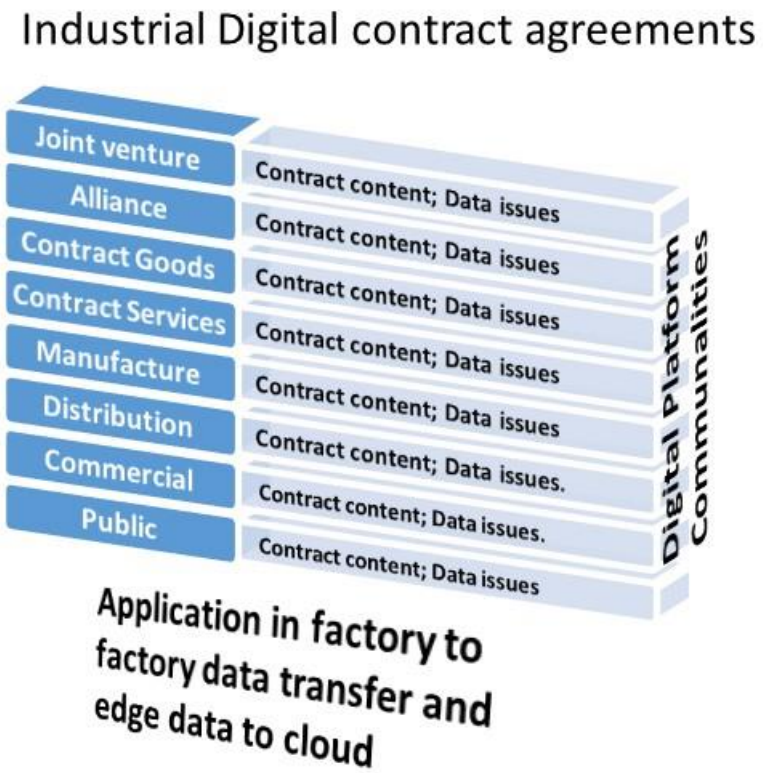


Figure 20: Industrial Digital Contract agreements

Factories of the future are developing in that context of industrial organisation landscape that is changing rapidly enabled by digital technologies. The notion of edge-to-cloud reflect advances that cover the collection of data connect several levels of the data pyramid. Connecting from the sensor level (in equipment, machinery and manufacturing or production cells) to PLCs to SCADA to Enterprise Resources Processing (ERP). Most of these operations are currently occurring within a single factory (or business) but are moving and striving to enable a more autonomous flow of data across different factories and business units. This level of sophistication in data gathering storage, transfer and associated analytics is currently embodied in the concept of *digital platform* whereby the connecting rod for all levels of business manufacturing operations is the flow and analytics of data. This new paradigm generates a new landscape of contractual issues that to a large extent is to be defined.

Industrial agreements on data accumulation (storage) data flows, data analytics and exploitation by third parties of data must be formalised in a way that the parties involved in such agreements are protected. The type of contracts varies depending on the aim of the relationship between parties in the agreement. With the new wave of servitisation of industrial operations (like manufacturing) often industrial agreements can take the form of one the following most common forms of Industrial contract agreements are: Alliances, Corporate Joint Venture, Commercial Sale of Goods, Long-Term Supply of Goods, Supply of Services, Manufacture Agreement, Distribution of Goods, Commercial Agency. These are briefly defined below

- **Alliance**: A framework for an alliance or collaboration between parties.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- **Corporate Joint Venture** (short form): A framework for a joint venture between two parties to establish a jointly owned company.
- **Commercial Sale of Goods**: An agreement for the sale of manufactured goods between a seller and a buyer. It contains added specifications and explanations on issues such as lack of conformity and limitation of the sellers' liability.
- **Long-Term Supply of Goods**: An agreement for the long-term supply of manufactured goods between a supplier and a customer.
- **Manufacture Agreement**: An agreement under which the client wants the manufacturer to design, manufacture and deliver certain goods, which the client intends to integrate into its own final products or its services.
- **Distribution of Goods**: An agreement for the distribution of manufactured goods, between a supplier and a distributor, whether the supplier is the manufacturer of the goods.
- **Commercial Agency**: An agreement under which a commercial agent negotiates the sale or purchase of goods on behalf of another person (the principal).
- **Supply of Services**: An agreement under which a service provider provides certain services to a client.

Each Model Contract indicates has a number of basic elements that should be considered when entering into an agreement in order to identify and make explicit existing and potential legal issues. Although there are many commonalities between different forms of contracts, the differences between them require attention according to the goals of the agreement. Such differences have legal implications of benefits, responsibilities, and liabilities. Table 3.1 below shows the **most common components of a contract agreement** for each of the industrial relations listed above. Here is important to highlight these particularities are not defined in sufficient detail in current legal instruments that provide guidelines for data protections (of citizens and companies).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Table 3.1 Digital industrial agreements generic taxonomy content

Alliance	Joint Venture	Supply of Goods	Supply of Services	Manufacture Agreement	Distribution of Goods	Commercial Agency
Objectives and key principles	Interpretation Business of JVC	Supply of the Goods	Supply of the service – Qualifications of the Supplier	Manufacture and supply of the Goods	Appointment of the Distributor	Scope of appointment
	Establishment of JVC: Conditions precedent	*Procedure for ordering*	*Procedure for ordering*		*Procedure for ordering the Goods*	*Obligations of the Principal and the Agent*
Management Committee	Directors and Management	Delivering the Goods			*Supply of the Goods*	Minimum orders
Joint Projects	Additional contributions of the Parties	*Price of the Goods*	*Payment of fees*	*Payment of price*	*Price of the Goods*	Agent's commission – right to commission
Contributions of the Parties	Dividend policy, Transfer of Shares	*Payment*	*Late payment and interest*	*Late payment and interest*	*Payment*	*Method of calculating commission and payment*
	Capital and further finance	Quality of the goods	Quality of the service	Quality of the goods	Quality of the service	Advertising, fairs and exhibitions
Data: transfers, storage, analytics	*Data: transfers, storage, analytics*	*Data: reliability, accuracy, periodicity, velocity*	*Storage: access, security, reliability, capacity, upload and retrieval speed*	*Data: transfers, storage, analytics*	*Data: transfers, storage, analytics*	*Data: transfers, storage, analytics*
Alliance costs	Costs	*Warranties relating to the Goods* General warranties	*Warranties and*	*Warranties relating to the Goods*	*Warranties relating to the Goods* General warranties	*Restriction of territory*
Lack of conformity (with agreed standards)	*Lack of conformity (with agreed standards)*	*Lack of conformity (with agreed standards)*	*Lack of conformity (with agreed standards)*	*Lack of conformity (with agreed standards)*	*Lack of conformity (with agreed standards)*	*Lack of conformity (with agreed standards)*
Intellectual Property	*Intellectual Property*	*Transfer of property*		*Intellectual property and trademarks*	*Intellectual Property*	*Trademarks and property rights*
Secondments and personnel (security and privacy)	Secondments and personnel (security and privacy)	Non-performance of the Buyer's obligation to pay the price at the agreed time		Cooperation of the Parties for improvements and modifications	Support and training	
Preferred supplier/distrib utor	General meetings	Non-performance of the Seller's obligation to deliver the Goods at the agreed time			Distribution of the Goods	Financial responsibility (Option)
	Reserved Matters	*Documents and manuals*	*Documents and manuals*	*Documents and manuals*	*Documents and manuals*	*Documents and manuals*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Confidentiality	Confidentiality	*Confidentiality*	*Confidentiality*	*Confidentiality*	*Confidentiality*	*Confidentiality*
Restrictions on the Parties	Restrictions on the Parties	Effects of contract avoidance in general				Exclusivity, non-competition
Duration and termination	*Establishment of JVC: Closing Deadlock or termination*	*Duration, termination and consequences of termination*	*Term, termination and consequences of termination*	*Duration and termination Consequences of termination*	*Duration and termination Consequences of termination*	*Term, termination and consequences of termination*
Change of circumstances (hardship)	*Change of circumstances (hardship)*	*Change of circumstances (hardship)*	*Change of circumstances (hardship)*	*Change of circumstances (hardship)*	*Change of circumstances (hardship)*	*Change of circumstances (hardship)*
Force majeure	*Force majeure*	*Force majeure*	*Force majeure*	*Force majeure*	*Force majeure*	*Force majeure*
Liability	Supremacy of this contract	*Liability* Restitution	*liability*	*liability*	*Liability*	*Indemnity or compensation on termination*
Entire Agreement	*Entire agreement/variations*	*Entire agreement*	*Entire agreement*	*Entire agreement*	*Entire agreement*	*Entire agreement*
Notices	*Notices*	*Notices and writing*	*Notices*	*Notices*	*Notices and writing*	*Notices*
No partnership or agency	*No partnership or agency*	*No partnership or agency*	*No partnership or agency*	*No partnership or agency*	*No partnership or agency*	*No partnership*
Assignment and subcontracting	*Assignment and subcontracting*	*Assignment and subcontracting*	*Assignment and subcontracting*	*Assignment and subcontracting*	*Assignment and subcontracting*	
Effect of invalid or unenforceable provisions	*Effect of invalid or unenforceable provisions*	*Effect of invalid or unenforceable Articles*	*Effect of invalid or unenforceable provisions*	*Effect of invalid or unenforceable provisions*	*Effect of invalid or unenforceable Articles*	*Effect of invalid or unenforceable provisions*
Authorizations		*Authorizations*	*Authorizations*	*Authorizations*	*Authorizations*	*Authorizations*
Dispute resolution procedure	*Dispute resolution procedure*	*Dispute resolution procedure*	*Dispute resolution procedure*	*Dispute resolution procedure*	*Dispute resolution procedure*	*Dispute resolution procedure*
Language of agreement	*Language of agreement*	*Language of contract*	*Language of contract*	*Language of contract*	*Language of contract*	*Language of contract*
Applicable law	*Applicable law*	*Applicable law*	*Applicable law*	*Applicable law*	*Applicable law*	*Applicable law*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.3.1 Digital industrial agreement common elements

Table 3.1 in previous page indicates many item clauses to the considered when conducting an industrial digital contract agreement. The variation across forms of industrial agreements as displayed in Table 3.1 is apparently low but there will be significant differences in most clauses depending on aims of the relation, the specification of the type of digital goods (data, infrastructures, storage facilities, etc.) or services (data curation, analytics, storage, etc.). The full outlining of the legal implications of digital industrial agreements still very much on its infancy. The list of clauses below is not exhaustive but must serve as examples and guidelines to identify variation and a more nuanced analysis of rights, responsibilities, and liabilities. These rights, responsibilities and liabilities might not be otherwise identified when considering entering an industrial business relationship involving digital goods and services supporting or underpinned by the follow of industrial personal and non-personal data.

3.3.1.1 Definition of the supply of the goods (or service) (this can be considered Clause 1)

This article must define the goods or service subject to the agreement. This one of the most important clauses in the agreement. This clause defines functions, interfaces, and technologies to realize digital products and services. Such definition will help to identify and make explicit the different regulatory frameworks and legal aspects that are relevant to secure industrial data flows free of constraints. In addition, it will help define responsibilities and liabilities.

3.3.1.2 Delivering the Goods

The agreement must define the place of delivery, date or period of delivery, carrier (logistics or telecom network provider), third parties involved.

3.3.1.3 Price of the Goods

This clause must indicate the total price, price per unit of measurement, currency, and the method for determining the price.

3.3.1.4 Payment

The payment clause must specify (latest) time for payment and whether this is done in advance, delivery of goods (or services). The Buyer must arrange for an irrevocable documentary credit in favor of the Seller to be issued by a bank, subject to the Uniform Customs and Practice for Documentary Credits published by the International Chamber of Commerce (ICC). The issue must be notified at least 14 days before the agreed date for delivery, or before the beginning of the agreed delivery period specified (see 3.3.1.2).

3.3.1.5 Data: reliability, accuracy, periodicity, velocity

The provision of goods (or services) should define the characteristics of the data and data flows in relation to their volume, reliability, accuracy, periodicity, and velocity of data transfers. The agreement should specify the needs of the buyers and what the supplier can fulfill considering the intrinsic characteristics of data flows (required and offered).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.3.1.6 Warranties relating to the Goods (or services) and liabilities

The Supplier warrants to the Client that the service will be provided as is customary for the provision of similar services on the Client's market. The goods (or services) will be provided in accordance with the specification agreed in clause one, and on the delivery time *[At the intervals and within the times]* expressly agreed in clause addressing deliveries. *Third party supplier*: Where the Supplier supplies in connection with the provision of the service any goods supplied by a third party, the Supplier does not give any warranty, guarantee or other term as to their quality, fitness for purpose or otherwise, but shall, where possible, assign to the Client the benefit of any warranty, guarantee or indemnity given by the person supplying the goods to the Supplier. *Goods or services client specifications*: The Supplier shall have no liability to the Client for any loss, damage, costs, expenses or other claims for compensation arising from any material or instructions supplied by the Client which are incomplete, incorrect, inaccurate, illegible, out of sequence or in the wrong form, or arising from their late arrival or non-arrival, or any other fault of the Client, provided the Supplier has duly notified the Client within agreed time of receipt of such material or instructions.

3.3.1.7 Lack of conformity (with agreed standards)

Lack of conformity refers to the non-compliance with the characteristics of the goods (or services) agreed to deliver. This includes amounts, quality, quantity, standards, functionalities, support and training, duration of supply, and any other features described in clause one.

3.3.1.8 Intellectual property and transfer of property

Transfer of Property: Following the definition of the goods and services to be provided to the Buyer (done in clause one), the Seller must deliver to the Buyer the Goods free from any right or claim of a third person.

3.3.1.9 Documents and manuals

Documents and manuals refer to the Seller duty to make available to the Buyer (or representative specified by the Buyer) the following documents: Commercial invoice, transport or transfer, packing list documents (specify any detailed requirements); Insurance documents; Certificate of origin (to be defined for data transfers as first or second party originating the data); Certificate of inspection; Handbooks and manuals for operation, maintenance and repair of the goods supplied. The documentation should be made available according to the specified delivery of goods and services.

3.3.1.10 Confidentiality

This clause refers to all reasonable efforts that each party in the agreement shall use to keep confidential all commercial and technical information that it may acquire in relation to the customers, business, or affairs of the other party. No party shall use or disclose any such information except with prior consent of the other party. This restriction shall not apply to any information: which is or becomes publicly available through no default of that party; is already in that party's possession without any obligation of confidentiality; to the extent that it is required to be disclosed by applicable law or by the rules of any recognized regulatory body. Each party shall use all reasonable efforts to ensure that its employees, agents, and any affiliates observe these confidentiality obligations. No announcement in connection with the Alliance shall be made by either party without the prior approval of the other party (such approval not to be unreasonably withheld or delayed) except as may be required by law or by any stock exchange or by any governmental authority. Bridging the confidentiality clause will apply the clause on liabilities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.3.1.11 Force majeure

"Force majeure" refers to war, emergency, accident, fire, earthquake, flood, storm, industrial strike or other impediment which the affected party proves was beyond its control and that it could not reasonably be expected to have taken the impediment into account at the time of the conclusion of this contract or to have avoided or overcome it or its consequences. A party in an industrial agreement affected by force majeure shall not be deemed to be in breach of this the agreement, or otherwise be liable to the other, by reason of any delay in performance, or the non-performance, of any of its obligations under the contract to the extent that the delay or non-performance is due to any force majeure of which it has notified the other party.

3.3.1.12 Liability

Strongly related to clause one, for example in relation to quality of data, data, security breaches, delivery, data analytics misuse or misrepresentation, loss of stored data, access, or retrieval of data, etc. *Liability Clause*: Except in respect of death or personal injury caused by the Supplier's negligence, the Supplier shall not be liable to the Customer by reason of any representation (unless fraudulent), or any implied warranty, condition or other Term, for any loss of profit or any indirect, special or consequential loss or damage (whether caused by the negligence of the Supplier, its servants or agents or otherwise) in relation to the supply of the Goods (or any failure to supply them) or their resale by the Customer, or otherwise arising out of or in connection with the agreement.

3.3.1.13 Dispute resolution procedure

For any dispute, controversy or claim arising out of or relating to the goods or services under agreement, including its conclusion, interpretation, performance, breach, termination or invalidity, the parties dispute shall be finally settled under agreed rules of arbitration. Such rules must specify the arbitration institution and number of arbitrators appointed, the place of arbitration and language shall be specified in the agreement.

3.3.1.14 Applicable law

In the context of industry agreements developing workable functionalities and data flows often will involve entities from different jurisdictions and hence subject to different regulators. The agreement must specify the national or international law that the agreement will follow for its implementation.

3.3.2 Strategic alliances and Joint Venture common features (applicable to research ventures)

Industrial agreements under the form of alliances and joint ventures hold similar features but each alliance or collaboration agreement is different. A contract agreement must consider the following issues depending on the purpose of the Alliance or joint venture. Provisions that are not relevant to the agreement should not be considered. Provisions that could be included are:

- The formation of a Management Committee on which the Parties involved are represented.
- Share of costs and risks implicit in the alliance or joint venture
- Definition of areas of responsibility to contribute towards the success of the Alliance. In some cases, responsibilities will be expressed in general terms – and not involve formal legal commitment. In other cases, specific legally binding commitment and liabilities will be appropriate.
- Definition of what knowhow and technical development will be shared by each party (e.g., where Intellectual Property), more detailed license or other contracts might be necessary.
- Duration of the Alliance and setting conditions for renewal requiring mutual agreement.
- Definition of dividend shares if there is a clear imputation of (potential) profits.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.4 Examples from projects (mapping of projects)

In most of the ICT-07 projects, industrial agreements and legal aspects are still at a very embryony level. To study the awareness of the pilots of the upcoming regulatory changes, as well as their readiness to address those changes in their operations, we asked a number of questions during a series of bilateral meetings with each project. The questions covered among other issues of liability, data protection and IT security, and are listed further below in this section.

The underlying idea was to uncover specific project needs – definitions, typical hurdles, recurrent challenges – that are not met by the current EU framework, and whether/ how the projects have dealt with those issues. Further, the questions aimed at facilitating a conversation on the types of industrial agreements that will be needed in the future to accomplish the connectivity between CF and the respective data flows, and to do so in a manner that avoids liability issues and secures IP. We were also hoping to receive indication on how specific data issues are handles in contractual clauses.

What can be said before the presentation of the individual results is that all pilots have a rather low TRL, which means that a lot of the risks, liabilities and warranties we were inserted in learning about are not yet considered; we thus often established a lack of awareness or capacity to look into these issues.

The questions we addressed to the pilots can be read below.

Liability

- How does the pilot deal with risks that stem from the integration of external partners (e.g. R&D partners, suppliers and customers) in the supply chain of companies, with regards to data protection, security and agreements on liability?
- What is the form of engagement or industrial contract type that is used to secure a (Alliance, joint venture, supply of goods, supply of services, manufacture agreement, distribution of goods, other…specify)
- What type of *data operations* are involved in your project? Transfer, storage, analytics, other?
- What type of legal /contractual issues are the more pressing in your project? Rate importance: high (1), medium (2), low (3)

Supply of the Goods or service (Data: transfer, storage, access, analytics)	**Rank**
Definition of the goods, product or service	
Procedure for ordering	
Delivering the Goods or service	
Price	
Payment	
Quality of the goods (setting the standard)	
Data: reliability, accuracy, periodicity, velocity	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Warranties relating to the Goods/service General warranties	
Lack of conformity (with agreed standards)	
Transfer of property (Intellectual property)	
Non-performance of the Buyer's obligation to pay the price at the agreed time	
Non-performance of the Seller's obligation to deliver the Goods at the agreed time	
Provision of documents and manuals	
Confidentiality	
Effects of contract avoidance in general	
Duration, termination and consequences of termination	
Change of circumstances (hardship)	
Force majeure	
Liability general	
Liability Restitution	
Notices and writing	
No partnership or agency	
Assignment and subcontracting	
Effect of invalid or unenforceable Articles	
Authorizations	
Dispute resolution procedure	
Language of contract	
Applicable law	

Data protection and IT security

- What data and privacy regulations are relevant to your project? Why? (e.g.,The General Data Protection Regulation, the European Cybersecurity Act, etc.)

- How does the pilot deal with legal aspects of the digital transformation of processes, in particular the collection/ use of production data (i.e. the ways in which data analytics create a new type of relationship with customers)?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- Based on the experience of the pilot, how do you think regulatory frameworks can be adjusted (e.g. data protection, data flows) to help businesses to digitally transform?

Below we present the answers to these questions we received during the bilateral workshops with the pilot's participants. Some of the answers are very short, others are more elaborate. It should be also noted that very few of the pilots had been engaged with data governance and regulation, or with issues surrounding the digitalization of industrial agreements. Before providing their answers, we first give some context about the pilot and its operations.

3.4.1 EFPF- European Connected Factory Platform for Agile Manufacturing

The EFPF platform aims to provide access to services and solutions that are currently dispersed. For that purpose, it realises a federated smart factory ecosystem by interlinking smart factory platforms through an open and interoperable Data Spine. In parallel, the platform provides the necessary infrastructure, tools and support for novel service creation and validations by third parties.[1] In essence, the EFPF connects multiple service providers.

3.4.1.1 Liability and risks related to data protection, security and integration of external partners

To avoid risks related to data storage on the system, EFPF's model is to channel the information from one point to another; EFPF is in its own words a 'facilitator'. This way, service providers – the ones the platform connects – keep the data in their domain; the project itself only creates repositories or pipelines. The data pipelines remain in the control of the data owners, who also specify the privacy and security privileges during the transfer phase. EFPF sees what pipelines exist but does not know who the owner is or what the user specifications are; it therefore does not see any risks or liabilities, unless there is a hack, which is a usual risk. Open source landscape of the data spine is supported by a security component that allows data handlers to have control over the data.

This means that any sensitive data such as addresses or names are effectively handled (and kept) by those who have collected or generated it for their business purposes. EFPF keeps minimal data to protect itself from liability, and if they do, they are very clear on how the data is used or managed. How the concept of the platform works with real use cases and whether new risks arise when real cases establish connectivity in the data spine, will become clear in the course of autumn 2022.

If necessary, EFPF would use ISO standards for data management. The latter is the case, for instance, when it manages and handles user data – the data on the users of the platform; however, the latter is a general profile data and not high-risk. Thereby, EFPF has also minimized the opportunities for cyberattacks.

3.4.1.2 Form of engagement or industrial contract type used

From a policy-maker or regulator point of view, EFPF's business is an infrastructure. Channelling data by means of this infrastructure is a novel type of service, for which industrial type agreements as they exist are not straightforwardly fitting or at least the community does not know how to address them at this point. EFPF understands its service more in line with what the Amazon model does – it adds expertise to how services can be pulled together; data is too big of a responsibility to take.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.4.1.3 Data and privacy regulations relevant to the project

The project is concern with architectural governance and therefor considers regulation as very important. It has taken into consideration the GDPR, as well as the NIS directive and its provisions on digital platforms; further, the HLEG ethics guidelines for trustworthy AI and scholarly works on ethically aligned design have been considered.

3.4.2 ZDMP – Zero Defect Manufacturing Platform

ZDMP aims to provide an extendable platform to support factories with a high interoperability level to cope with the concept of CF in reaching the zero defects goal. In this context, ZDMP envisions to allow end-users to connect their systems (i.e. shopfloor and ERP Systems) to benefit from the features of the platform. These benefits include among other products and production quality assurance.[2] ZDMP's concept can be thus seen as a feedback and control system as those employed in domains ranging from human/autonomous driving to electronics. The platform will be steered by the ZDMP app using the projects SDK and additional components. These receive (and present/actuate) information from sensors/APIs and then process the data, allowing to influence the material, the process and to avoid errors which create defects. The ecosystem thus created by ZDMP will: 1) build applications to monitor, manage, and control connected devices; 2) collect and analyze data from those connected devices; 3) enable secure connectivity and privacy between devices and throughout the platform; 4) manage the interconnectivity of device/sensors, machines, factories and partners; 5) offer core API services to facilitate use; 6) allow integration with 3rd party systems/services and provide interoperability with other platforms.; and 7) automate and provide services for the intelligent Zero Defects ecosystem of the platform.

During the bilateral meeting with ZDMP, current risks and encountered data issues were discussed.

3.4.2.1 Liability and data operations

When it comes to issues of liability and concerns about potential risks that may stem from the integration of external partners in the platform's supply chain, the pilot stakeholders identified the data stemming from operators as a risk, as well as the certification data. An additional risk or challenge at the moment was reported to be the handling of the different data sets, as well as the setting-up of a data repository. Those risks are addressed mostly by individual contractual relationships.

3.4.2.2 Type of industrial agreement

The pilot has not been able to conceptualize the type of industrial contract specific to their operations. For the time being, there are a number of (simpler) contractual relationships, established to introduce limitations and restrictions to the data access on the platform. However, the pilot participants reported that they are covering merely aspects of what is actually necessary to be fully compliant, and that they have not implemented a comprehensive solution yet, which is much needed.

One of the reasons for that is that the types of commitment among the parties have been difficult to further narrow down. There are some rules defined but those are not enough, as clearer definitions are required on all operational aspects and the commitments they imply from the parties. This has also further implications for the terms and conditions under which third parties can join the platform.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.4.2.3 *Data and privacy regulation relevant to the project*

The pilot participants are aware that the Data Act, which aims to make more data available for the purposes of the data economy in line with EU values and rules,[3] will largely affect the stakeholders of the platform once introduced. Further, the GDPR is mentioned as a relevant legal instrument, especially in reference to the data exchange and processing conducted by the platform, as well as in relation to issues of confidentiality.

3.4.3 KYKLOS4.0 – An advanced circular and agile manufacturing Ecosystem based on rapid reconfigurable manufacturing process and individualized consumer preferences.

To demonstrate the transformative effects of CPS, PLM, LCA, AR and AI technologies on the Circular Manufacturing (CM) Framework, KYKLOS4.0 runs seven pilots to test the respective environmental, economic and technical viability of its ecosystem on intra-factory processes and services.[4] The idea of the pilots is thus to demonstrate the penetration and response of the CM market to the KYKLOS4.0 Ecosystem.

Of the seven pilots, we gathered input regarding the legal aspects of their operations from three of the pilots – GRC, PROMEDICARE and PINDOS – which we address in turn below. It should be noted that all pilots solve concrete practical problems and thereby create new data. We therefore, asked a number of questions relating to the data gathering, storage, processing, and other related regulation and governance aspects. Importantly, KYKLOS4.0 does not share data with external companies, and its overall contribution is the digitalization of the aspects the pilots require it for.

3.4.3.1 *Aerospace pilot (GE Research)*

Within the GE Aviation Services group's maintenance of jet engines, periodic overhaul is a key process. In the pilot, KYKLOS 4.0 is used to help in the estimation of which engine parts and when to replace them. Its overall goal is thus to make jet engine overhaul more efficient through reusing as many engine parts as possible, and to make it quicker in order to reduce the production of additional engines that are used as temporary replacements during the process of overhaul.

To achieve both goals, an overhaul operation requires complex processes of prediction and planning. This use case addresses two of these processes: Maintaining just-enough levels of spare part inventory through predicting which parts would be required for each engine, based on its service history; and scheduling the maintenance activities to achieve high throughput and responsiveness. Importantly, the pilot has already moved on from the test environment into the working environment – it is possible to move directly from the simulation model to the physical model, and to directly connect the digital twin to the physical twin. Therefore, one first commercial case is underway.

3.4.3.1.1 Liability and data operations

When asked about whether and how the pilot has dealt with risks that stem from the integration of external partners in the supply chain of company, data protection, security or agreements on liability, it appears that at least at this point no new risks have been experienced/encountered by the pilot participants. The pilot uses data of GE's customers and external partners, as has always been the case. The pilot thus transfers, stores, analyses and snapshoots operational data. GE Research does not see liability or product issues.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.4.3.1.2 Data protection and IT security

When it comes to data protection and privacy regulations, the pilot appears to not be including personal information, as the data it works with is commercial. As such, the data and its security are subject to internal GE procedures and the contractual agreements within partners and customers. We were not able to obtain any further information on whether and how the pilot considers upcoming changes in EU data and privacy regulations, and to what extents it anticipates the changes in its operations.

3.4.3.2 PROMEDICARE

Current wheelchair customization is not yet a fully automated process, requiring hours of technical time and many additional fitting sessions. The PROMEDICARE system creates orders for customized wheelchairs by sending the patients' specifications to the prototype designer to start the actual customized design process. The prototype designer takes advantage of the KYKLOS4.0 platform to follow a new and advanced methodology in designing the different custom parts of the wheelchair.[5] The production of a customized product based on the real physical needs of the patient reduces the adaptability error of the product with respect to the patient's needs, also reducing time and cost of production, and delivery time to the end customer.

3.4.3.2.1 Liability

When it comes to issues of liability and concerns about potential risks that may stem from the integration of external partners in its supply chain, data protection issues or security, the pilot has managed most issues by means of concluding confidentiality agreements with the necessary project partners. For reasons of data protection, information on the executive design of the wheelchair, technical drawings of the product and other detailed information, have not been shared with anyone except in cases of extreme necessity.

3.4.3.2.2 Type of industrial agreement

The pilot has not further conceptualized the form of engagement or industrial contract type that is used. The way in which data relating to confidential information is shared, or information on purchase orders is shared, is managed through the signing of specific confidentiality agreements.

3.4.3.2.3 Type of data operations

During the development of the pilot project, data transfers such as CAD models, product BOMs or BOMs of only final product components have taken place. Some of the collected data has been transferred to carry out data analysis.

3.4.3.2.4 Most pressing legal/ contractual issues encountered during the pilot

The pilot party reports that the legal issues encountered as most pressing or challenging to solve have been such relating to the procedures of ordering, definition and quality of the goods and delivery, warranties, authorizations, change of circumstances, lack of conformity with the agreed standards, transfer of IP. Less of an issue are considered or experienced confidentiality, properties of the data (reliability, accuracy, periodicity, velocity), dispute resolution procedures or subcontracting. Not an issues at all for the pilot have been issues of payment, liability, language of the contract and applicable law.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.4.3.2.5 Data protection and IT security

The pilot works with data based on the patient's anthropometric measurements or analysis of the patient's habits. The storage of this data is essential in order to activate a production cycle of a product that can be customized according to the needs of the consumer. The handling of the data, however, appears unclear. On the one hand, it is stored for production purposes; on the other hand, the pilot claims that the storing of sensitive patient data is avoided in order to maintain a high level of patient privacy and anonymity. It appears that it has not been investigated to what extent the anthropometric data can be turned into *identifiable* or personal data and lead to the identification of the patient. Accordingly, data protection regulation is not considered at largen, save for data security for process purposes.

3.4.3.3 PINDOS

The PINDOS pilot aims to incorporate a number of tools into one single platform and it uses KYKLOS4.0 to monitor the process and resources. The purpose of the pilot is complex ecosystem monitoring and environmental footprint reduction in the water domain. The monitored values are recorded during production processes and pertain to normal water, hot water, steam, or air compressors. The data is derived through ICS equipment such as sensors and PLCs, installed on the external of the engines (pumps, flowmeter, energy meter) to monitor their proper operation and to prevent damage by human error, external factors or through malicious intervention. The goal is to control the variables that ensure the quality of the production and therefore the quality of the final product offered to the consumer.

3.4.3.3.1 Liability

When it comes to issues of liability and concerns about potential risks that may stem from the integration of external partners in its supply chain, data protection issues or security, the pilot has managed most issues by means of concluding confidentiality agreements with the project partners. Agreements have been concluded with all partners that deal with the pilot's sensitive data.

3.4.3.3.2 Type of industrial agreement

The pilot has not further conceptualized the form of engagement or industrial contract type that is used.

3.4.3.3.3 Type of data operations

During the development and implementation of the pilot project, data has been stored and processes. For that purpose, attention has been given to the security of the network(s).

3.4.3.3.4 Most pressing legal/ contractual issues encountered during the pilot

The pilot party reports that the legal issues encountered as most pressing or challenging to solve have been such relating to data (and its reliability, accuracy, periodicity, velocity) and warranties. Less of a challenge but not entirely unproblematic have been issues of defining the delivered good/ service, its quality, lack of conformity, and provisions of documents or manuals. Not an issue at all or not experienced as such during the pilot are questions related to procedures of ordering, delivery of good, payment, price, transfer of IP or non-conformity.

3.4.3.3.5 Data protection and IT security

The pilot reports awareness of the GDPR, but not of other data protection regulatory instruments. Further, as customers and the market do not appear to be connected in the pilot's initial concept, the pilot has not

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

looked into processes of digital transformation (such as whether the data analytics used/ deployed create new relationships, pathways to the customer, etc..)

3.4.4 DIGIPRIME – Digital Platform for Circular Economy in Cross Sectorial Sustainable Value networks.

3.4.4.1 Most pressing legal/ contractual issues encountered during the pilot

In the moment DIGIPRIME is focusing on legal aspects in relation to plastics and batteries; the rest of the subsectors such as textile, mechatronics, etc. will be analysed further along the project.

When it comes to plastic, following sources of rules are being taken into account:

- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the reduction of the impact of certain plastic products on the environment. 2018/0172 (COD)
- Directive 1994/62/EEC of the European Parliament and of the Council of 20 December 1994 on
- packaging and packaging waste
- DIRECTIVE 2000/53/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 September2000 on end-of life vehicles
- DIRECTIVE 2005/64/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on the type-approval of motor vehicles with regard to their reusability, recyclability and recoverability and amending Council Directive 70/156/EEC
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A European Strategy for Plastics in a Circular Economy

When it comes to batteries, the Batteries Directive (2006/EC/66) is the only piece of EU legislation that is entirely dedicated to batteries, addressing the lifecycle of batteries and the recycling of spent batteries, and therefore considered by the pilot. Further the pilot is aware that the environmental issues linked to batteries can be traced back to the poor functioning of the EU's internal market, including the absence of a comprehensive set of rules for batteries placed on the market and the uneven implementation of obligations.

In this regard, DIGIPRIME is actively working on the Feedback on the Proposal for a Regulation of the European Parliament and of the Council concerning batteries and waste batteries, repealing Directive 2006/66/EC and amending Regulation (EU) No 2019/1020 to translate the pilot's key concerns regarding reuse, repurposing, remanufacturing, battery passport, EPR and labelling into the provisions.

3.4.5 SHOP4CF – Smart Human Oriented Platform for Connected Factories

3.4.5.1 Liability

When it comes to issues of liability, the pilot sees a challenge in the current lack of regulation of data ownership. What contributes to the challenge is that there is also no common European framework on liability that can be applied in this context, as each member state applies its own rules. Therefore, the contractual agreements need to be very clear.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

3.4.5.2 Most pressing legal/ contractual issues encountered during the pilot

The pilot participants report that a pressing issue is the combination of personal and non-personal data, and the implications of bundling it and how to apply then the GDPR provisions. Further, the wearables in the factory, such as smart gloves or AR glasses require special attention as they reveal the state of health, the location of the worker, their performance etc.

Further, licensing of AI components is an issue as it falls between IP law and contract law, and is currently treated as software. Software, however, is not protected by patents but by copyright law, which falls under the competence of member states. Therefore, the EU has made an attempt to harmonize software protection by means of the Computer Programs Directive, but the latter is not applicable to contracts. There are also different types of software contracts (licenses, transfer of IPR, SaaS), which may all be applicable to the same case.

3.4.5.3 Data and privacy regulation relevant to the project

The pilot participants are looking ahead and already aware of the implications of the Data Governance Act,[6] which will be applicable as of September 2023 and introducing the legal framework for data sharing infrastructures, re-use of public sector information, and rules for the provision of data exchange services between private actors.

The pilot participants are also aware of the relevance of the draft Data Act[7] for the pilot, which will have implications for data ownership, and therefore industrial contract will have to pay better attention to who the owner of the data is that has been generated by the machine or online service. In the future, once the Data Act is in force, the (business) user will have the right to request the disclosure of the data generated by his use of the product, as well as the right to request the transfer of such data to third parties. Further, manufacturers or service providers will be required to provide information to users about the data itself and the ability to access it. All those issue are to be addressed contractually for the time being.

The draft AI Act[8] is also of relevance for the pilot, as the Act covers biometric identification and categorization systems and management and operation of critical infrastructure, which are often used in smart factories, as well as AI systems that are intended as safety components of products. The pilot participants envision necessary work around Art. 10 of the Act – training, validation and test data; Art. 12 – keeping event logs throughout the lifecycle of the system; and Art. 13 of the Act – ensuring sufficient transparency of the operations and providing users with information that allows them to interpret the results of the system.

[1] EFPF (European Factory Platform) European Connected Factory Platform for Agile Manufacturing | EFFRA Innovation Portal

[2] Concept | Zdmp

[3] Data Act: measures for a fair and innovative data economy (europa.eu)

[4] IoT Catalogue (iot-catalogue.com)

[5] IoT Catalogue (iot-catalogue.com)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

[6] EUR-Lex - 52020PC0767 - EN - EUR-Lex (europa.eu)

[7] Data Act: measures for a fair and innovative data economy (europa.eu)

[8] EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)

3.5 Reflection

Recent initiatives and research have developed an architecture of nine **building blocks to organise and develop Industrial agreements on data spaces**. Such structure has nine pillars that **facilitate the dialogue** across the stakeholders that participate in the development and deployment of data spaces. The nine pillars are namely: Data standards, exchange protocols, identification and authentication, authorization, metadata, operational agreements, governance, business models and legal agreements. These pillars are depicted in the figure below. Over the last five years the pillars in the left side of the picture have been advancing to consolidate several industrial agreements and the creation of data spaces. The right side of the having elements like business models, governance and legal agreements have advanced at a slower pace. Specially the issue of digital contracts and legal agreements has not received sufficient attention.

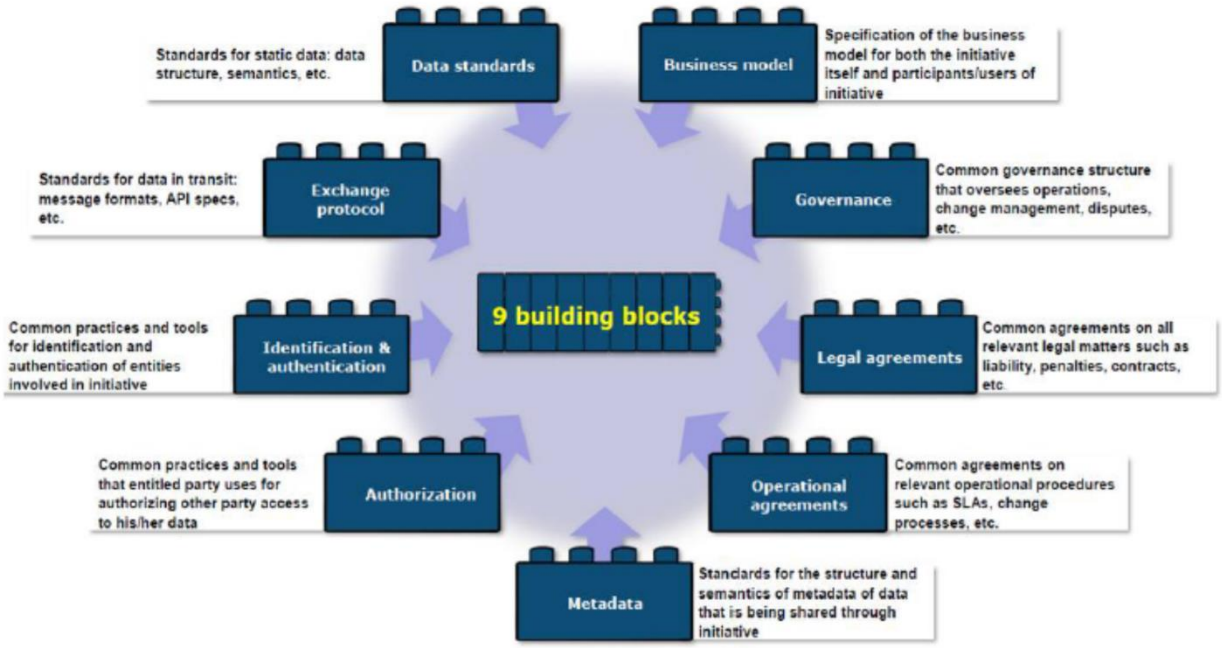


Figure 21: Source: Source: European Commission — DG CNECT, 2020

The advent of massive data flows across industrial organisations is likely to generate new business models while at the same time bring unknown risks in legal terms. It is likely that entire value chains could be affected by new business models that are data driven, this will demand clear definitions of contracts contents that protect the parties involved and those receiving services based in data analytics. The recent initiatives from the European Commission on the upcoming data regulations aim to be the first step to bring some regulatory framework for the production, storage, transfer, and analytics of big data generated in industrial activities. The actual implementation of commercial contracts on data flows and analytics will to a large extent left to businesses.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The advent of new initiatives governing data at the EU level (e.g., EU Cybersecurity Act, EU Data Governance Act, EU Data Act, EU Digital Markets Act, EU Machinery Regulation, EU AI Act) has taken industry unprepared.

The interaction with the example projects developing technologies and applications that support the digital connection of industrial operations provided rich detail onto how the contractual and legal implications of data production, transfer, storage and analytics are seen by researchers and organisations. Given the relative novelty of the topic in relation to data transfers the most salient issues are:

- Generalized **lack of awareness** of current and upcoming regulatory framework addressing data governance;
- Current **regulatory framework on industrial data transfers not adequate** (focuses on data protection individuals rights, i.e., B2C not B2B, B2G and G2B);
- Non-personal data on edge-to-edge systems not addressed;
- Non-personal data can be transformed into personalized data during interaction with operators or management generating potential liabilities for operators and/or management;
- Standard clauses of existing templates of legal contracts must be adapted to specific requirements of contractual industrial relations. Critical to achieve this is a good definition of the nature of the goods or service to supply (this can be considered Clause 1 of any contract. See sections on contracts above).

Some urgent need that derives from this exploratory research is that there must be an awareness raising effort to inform digital technology developers and companies on the legal implications of the new regulatory and governance initiatives at the EU level. This effort must stem from the instances issuing regulatory and governance of data flows and industrial associations that have a stake in the development and exploitation of new technologies where data flows and analytics are part of their operations and business model.

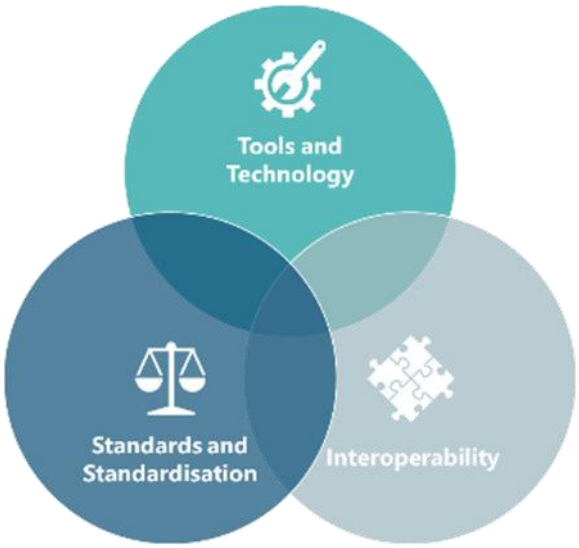
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

4 Standards

Standards and standardization are the driving force of innovation and sustainable technological development. Standards practically guide the work of the CF2 project developers and help to channel the needs and expectations of the stakeholders. Particularly, technical experts of the projects accumulate information that is valuable for drafting of future standards and, thus, express their future expectations in the standardisation work.

4.1 General observations on standardization

From the group of cross-cutting factors identified as key enablers for increased digitalisation and connectivity introduced in Figure 1, '**Standards and Standardisation'** operates within a unique triad. At a foundational level, the digital 'Tools and Technology' that forms each level of the automation pyramid must be implemented, the presence of 'Standards and Standardisation' bodies for that technology is a measure of its maturity, which in turn helps enable and ensure the 'Interoperability' of the solutions or strategies being deployed. However, while these CCFs are often interdependent, they remain separate. Technologies can be interoperable without codified open standards. Likewise, technologies may be standardised yet not interoperable. Additionally, open standards for interoperability may be drafted for technologies that have not yet reached a level of maturity for mass-distribution. These interrelationships are visualised in the Venn diagram below (see Figure 22).



The presence of standards and accepted standardisation bodies are a key enabler and CCF to facilitate the broad implementation of innovative tools and processes across an entire industry. The Connected Factories project (both CF1 and CF2) provides support for the standardisation of projects across regional, national, and international boundaries. This support primarily takes the form of a wiki that was introduced in CF1. The wiki provides useful information to aid and inform new projects being initiated, and serves as a vehicle to collect information. In this way the wiki can both support and evolve with manufacturing (industry, research, supply, demand, …) as it engages with the envisioned transformation.

Figure 22: Venn diagram of technology, standards and interoperability

The last few years have seen lively debates about which areas of standardization are the most important in the digital transformation. This question will not yet find a clear answer for the moment and will definitely need further elaboration from the standardization community. As adopted by IEC Strategic Group 12, Digital transformation is "the profound transformation of business and organizational activities, processes, competencies and models to fully leverage the changes and opportunities of a mix of digital technologies and their accelerating impact across society in a strategic and prioritized way, with present and future shifts in mind".

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

4.2 DMP Cluster WG 1 Standardization

4.2.1 Goals

The DMP (Digital Manufacturing Platform) cluster is a project cluster that was established with the aim of promoting cooperation between the projects of "DT-ICT-07-2018-2019: Digital Manufacturing Platforms for Connected Smart Factories". It also includes upcoming projects focusing on AI and CSA, which were funded under the 2019 call.

Across the four main pillars: (1) Platform Building; (2) Large Scale Piloting; (3) Ecosystem Building; and (4) Standardization, the cluster strategy builds on various collaborative topics, which discover common interests, i.e. potential synergies, among all cluster participants. The key topics include joint activities regarding standardization, research, dissemination of events, performance management and KPIs, market analysis and business models, pilots and open calls.

Standardization is one of the key topics of the cluster.

The **DMP Working Group 1** *Standardization* is focusing on common standardization work with the goal to exchange on standardization results of the projects and push common standardization activities in order to reach a wider spectrum in a joint work. Thus, the key aim of the WG 1 is to **organize the cluster framework in such a way that the projects will be able to cooperate freely in developing common strategies for interoperability and the development of/contribution to current standards including ZDM technologies**. In particular, the impact of ConnectedFactories2 can be summarized as follows:

- coordination of joint activities in the field of standardization among the member projects to increase the overall impact in standardization;
- facilitation of the exchange of best practices and experiences among the projects to promote the rapid development of standards and their application in large-scale pilots;
- coordination of the joint dissemination activities with the standardization focus to promote joint results.

4.2.2 Tasks

The coordination and support of ConnectedFactories2 applies to the following key tasks of the WG 1:

❑ **TC1.0: Common standardization strategy (Ambassador: O.MEYER, FHG, CF2)**

Main goals:	The main goal of this task is to analyse the overall goals of the cluster regarding standardization and help the participants to align on a common standardization strategy for Zero-Defect Manufacturing.
Outputs:	The result of the task includes a list of relevant tasks and selection of tools to enable the necessary exchange between the members of the working group.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

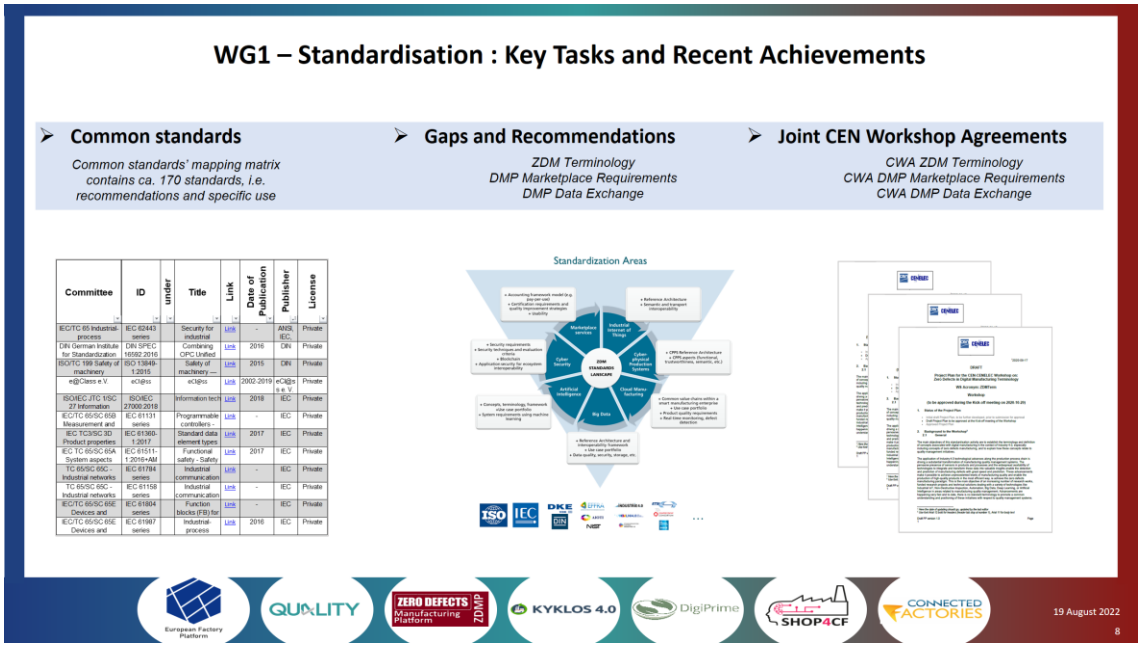


Figure 23: Key tasks of the DMP Cluster WG 1 Standardization

Notable results: During the first working group meetings, the list of required tasks for joint activities was defined (see key task in Figure 23). These include TC1.1 - TC1.6. The working group agreed on the roles of ambassadors to support and monitor the tasks. Some of the tasks were established as a bridging activity to other working groups in the cluster.

To facilitate the necessary exchange between members, it was decided to introduce a regular update based on a round table. The regular exchange between the projects is intended to establish a common understanding and assistance on standardization activities and progress between the projects. The results complement a common zero-defect manufacturing strategy and help members get a fast start on standardization work.

One of the notable results of this round table is the collection of status updates on completed standardization activities from all members. This activity was included as a fixed agenda item. In this context, each project presents not only the results from their projects but also shares valuable experiences they gained executing this or another activity.

- ❑ **TC1.1: Link to EC activities (Ambassador: C.GRUNEWALD, DIN, ZDMP)**

Main goals: The main objective is to establish a link with the activities of the European Commission and to collect up-to-date information on other relevant activities at the European level.

Outputs: The main outputs of this task include short reports on the relevant activities of the European Commission and current news, as well as information on interesting future events related to standardization. This includes not only events organized by the European Commission, but also related events, e.g., by EFFRA or internal events of the participating projects or workshops that were of interest to the objectives of the Cluster.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Notable results: One of the notable results of this task is the participation of consortium members at standardization events triggered by the European Commission and the European standardization organizations.

Activity: *Workshop "Boosting Innovation through standards - Your gateway to the market"*[22]

This event took place on the 13 November, 2019 and aimed at boosting the market uptake of innovation and research outcomes by using standardization as an enabler. The attendees were leading experts in innovation and standardization (e.g. CEN and CENELEC, the European standardization organizations) who got the opportunity to present their experiences highlighting the linkage between innovation and standards.

The event was structured in thematic parallel sessions as follows: a) innovative researchers interested in enhancing their understanding of standards and how it helps their ideas to reach the market; b) researchers, eager to learn how to integrate standardization in research programmes; c) entrepreneurs looking to break into a market of 600 million consumers; d) experts keen to understand how patents and standards support researchers and innovators; e) those interested in expanding their network within industry as well as the research and innovation community; f) research and innovation enablers (NCPs, European Federations, ETPs and other multipliers).

Activity: *EU-Workshop: „ Stakeholder consultation on the future Guiding Principles for Knowledge Valorisation"*[23]

As part of the implementation of the Communication on "A new ERA for Research and Innovation" the European Commission developed Guiding Principles for knowledge valorisation. A set of codes of practice have been proposed to implement these Guiding Principles. One of these codes of practice is planned to be utilized as a Code of Practice for researchers on standardisation. To create the Code of Practice relevant stakeholders were identified to ensure its usefulness, relevance and ownership. As part of this exercise, the European Commission (Directorate General for Research and Innovation) has launched a comprehensive on-line survey to collect and understand the experiences and views of beneficiaries on the role of standardisation in valorising R&I results. As the result the ConnectedFactories2 project has been selected as relevant for standardisation as means of valorisation of R&I results.

To facilitate the design of the code, the consortium contributed to the work by taking part in the survey and also took part in the following workshop organized under the umbrella of EU.

Activity: *EU-Workshop: „DG R&I Stakeholder Workshop | A Code of Practice for researchers on standardisation"*

[22] https://www.eu-ems.com/agenda.asp?event_id=4417&page_id=10277

[23] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/stakeholder-consultation-future-guiding-principles-knowledge-valorisation-2021-12-13_en

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The event was held on December 13, 2021 in a closed circle of participants from various projects involving an element of standardisation, national standardisation organisations with strong R&I focus, academics active. The main objective was to discuss how standards enable the dissemination of knowledge in projects and how they can bridge the gap between research and products/services to enable technology diffusion, facilitate the adoption of new technologies, and make it easier for innovations to gain market acceptance and consumer confidence. The goal of the discussion was to develop a code of conduct for researchers in the field of standardization, which includes a set of recommendations on how beneficiaries of public R&I programs can best identify opportunities and techniques for valorising their project results through standardization.

During this stakeholder workshop CF2 jointly discussed and reflected on the following topics: a) the success factors, operational steps and outputs of projects that are relevant to the development of standards; b) the recurring challenges linked to standardisation and ways to overcome those; d) the recommendations to design and implement projects in a way that their results can be valorised through standardisation; e) the possible indicators for monitoring and evaluating the success factors and impacts related to the use of standardisation to valorise R&I results.

Activity: *Guest contribution to CEN-CENELEC-ETSI Coordination Group 'Smart manufacturing' (CEN-CLC-ETSI/SMa-CG)*

To coordinate the European standardization activities relating to new technologies in the field of manufacturing, the CEN-CENELEC-ETSI Coordination Group 'Smart manufacturing' (CEN-CLC-ETSI/SMa-CG)[24] was established. It is a joint group of CEN, CENELEC and ETSI which advises the CEN-CENELEC Technical Boards and the ETSI Board. Decision ref: CEN/BT C143/2019 and CLC/BT D163/C081, applicable from: 2019-08-28 CCMC (Source: CEN/CENELEC newsletter, Nov. 2019[25]). The SM-CG advises on standardisation needs related to smart manufacturing to CEN, CENELEC, and ETSI. The Group doesn't develop standardization deliverables itself, but may produce information material intended for the public domain after approval by the CEN/CENELEC/ BTs and ETSI Board. Furthermore, the SMa-CG aim is to provide information exchange with relevant initiatives including relevant EU projects.

On this base the representatives of the DMP WG 1 (O. MEYER, FHG) attended on October 3, 2022 the 10th general meeting of the Sma-CG and presented the overall goal of the DMP Cluster and in particular the standardization strategy of the WG 1, showing the recent results.

On this basis, the representatives of DMP WG 1 (Olga Meyer, Fraunhofer IPA) attended the 10th General Meeting of Sma-CG on October 3, 2022, presented the general objectives of the DMP cluster and, in particular, the standardization strategy of WG 1, and showed the latest results of the joint work (see Figure 24).

[24] https://www.cencenelec.eu/areas-of-work/cenelec-sectors/mechanical-and-machines-cenelec/

[25] https://www.cencenelec.eu/News/Newsletters/Newsletters/BT_Newsletter_November2019_Final.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The experts of the group were very interested in the current activities of WG 1. It was agreed, if possible, to discuss the regular update in the forthcoming meetings of the Sma-CG.

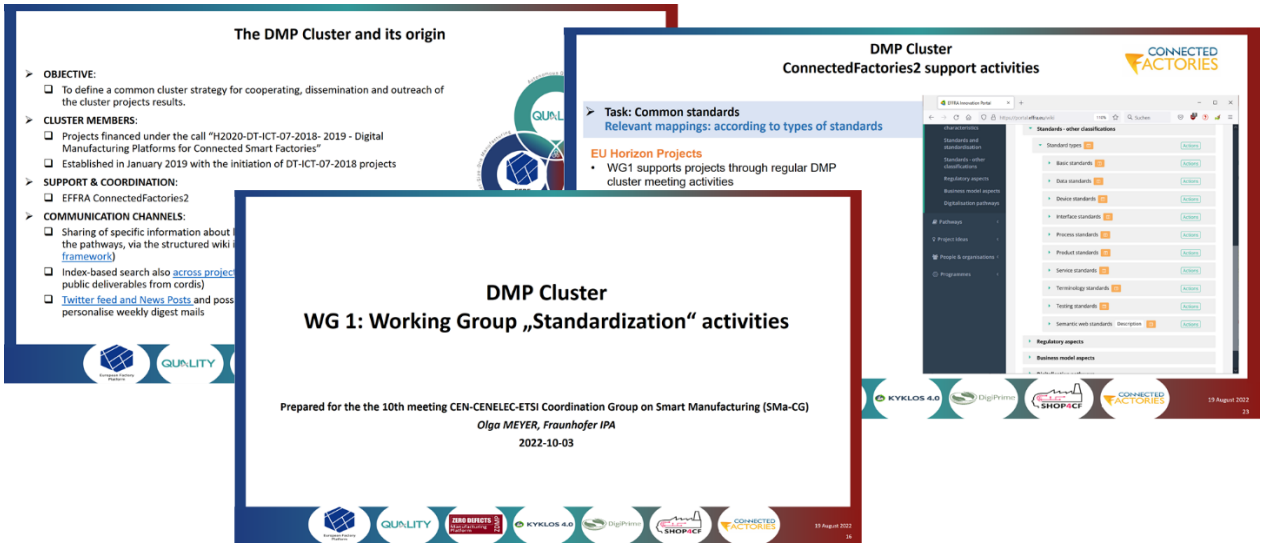


Figure 24: Presentation at CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing (SMa-CG)

- ❑ **TC1.2: Common standards (Ambassador: O.MEYER, FHG, QU4LITY)**

Main goals: The main goal is to identify common standards used by projects and analyse, classify, and migrate these to the wiki in accordance to the updated framework taxonomy.

Outputs: The output of this task includes a list of common standards and a classification roadmap according to the taxonomy. It was decided to perform this task on a recursive basis, asking members to submit new information on common standards or update old ones every six months.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

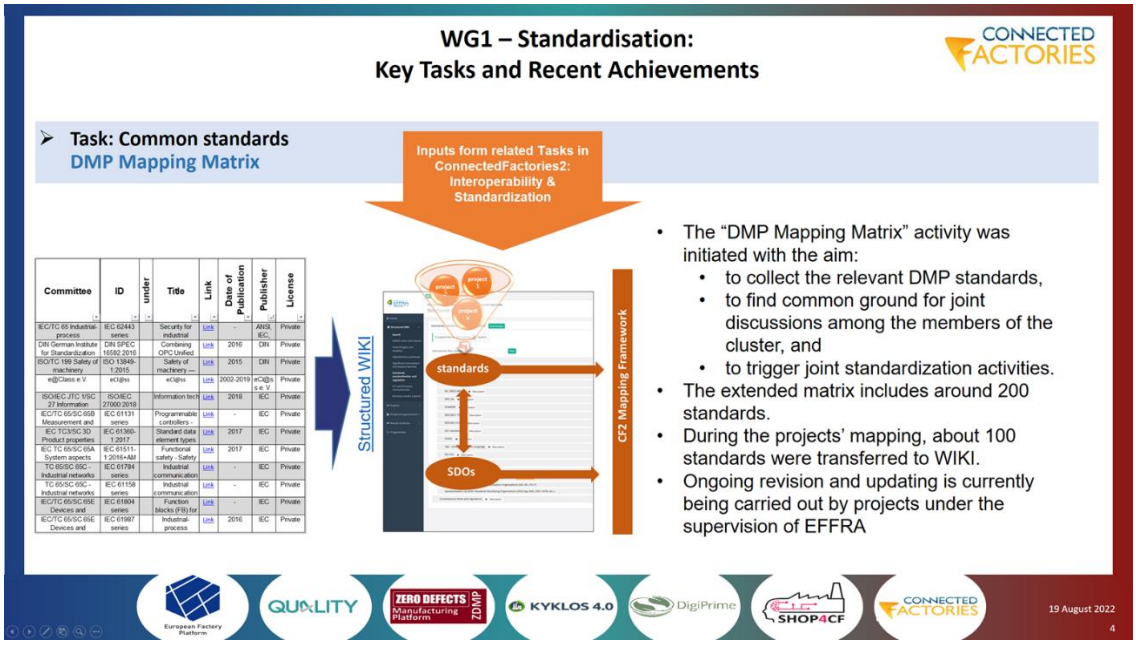


Figure 25: The mapping matrix strategy

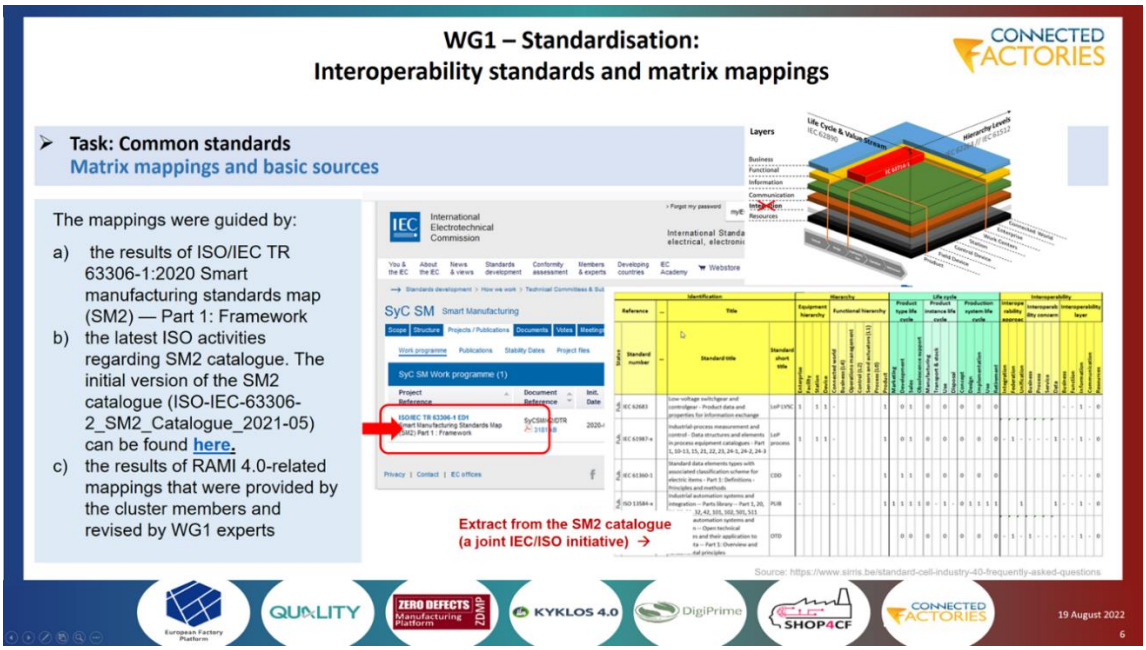


Figure 26: Approach for the taxonomy structure

Notable results: The participation of the projects in this task is based on the progress of the standardization activities of the individual projects. Thus, initially three projects (EFPF, ZDMP and QU4LITY) contributed their results. In this sense, it was assumed at the beginning of the work that in the long term other members would also be able to contribute their results to the matrix (in long-term on the EFFRA wiki portal) once their standardization activities had reached an advanced level (see Figure 25).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The basic list of standards and the initial analysis was performed by the QU4LITY experts. To accomplish the task, the QU4LITY experts performed a detailed analysis of more than 200 potential standards (see the slide presenting the approach for used taxonomy in Figure 26 and an example from the first draft of the matrix in Figure 26).

The first draft of the matrix was created in Excel format and was publicly available during the initial design phase. Subsequently, the first draft of the matrix was successfully commented on and finalized by all project experts in the working group during the first review phase. The results were documented and distributed to all members and interested parties within the projects for comment.

The first draft of the matrix served as input for the wiki structure and its content was successfully transferred in the first version stage. One of the most important works was the creation of different classifications and taxonomy structures for the matrix content. This procedure as well as the final taxonomy structure and classification are described in detail in Deliverable 1.3 "Structured wiki update on Business models, Legal aspects, Interoperability, Standardization, Cybersecurity and Human aspects – Second iteration".

								RAMI4.0 transfer to EFFRA/WIKI						Factors							EFPF			ZDMP			QU4LITY		
Committee	ID	under development	Title	Link	Date of Publication	Publisher	License	Asset Layer	Integration Layer	Communication Layer	Information Layer	Functional Layer	Business Layer	(tbd)	Human	Security & safety	Interoperability &	Quality	RA	AI	EFPF "in usage"	EFPF RA	EFPF Details	ZDMP "in usage"	ZDMP RA	ZDMP Details	QU4LITY "in usage"	QU4LITY RA	QU4LITY Details
DIN German Institute for	EN 61069 series		Industrial-process	Link	-	_	Private									x	x								---	---			Distributed Trustworthiness	Cyber Security in Industrial Environments
ANSI	B11.0 - 2020		Safety of Machinery	Link	2020	ANSI	Private									x									---	---			Digital models and Vocabularies	Description of industrial plants and components in
ANSI	B11.Tr10—20 2x	x	Functional Safety of Artificial	Link	-	ANSI	Private									x				x					---	---			Control Service	Control Service; design and integration of safety-
IEC/TC 65 Industrial-process	IEC 62443 series		Security for industrial	Link	-	ANSI, IEC,	Private									x					x		Two partners	x	Secure installation,	Information Security		Digital models and Vocabularies	e@Class: Supports the digital
CEN/TC 459/SC 3 Structural steels	EN 10219-1:2006		Cold Formed Welded structural	Link	2006	CEN	Private																		none	none		Digital models and Vocabularies	Information security management systems;
CEN/TC 459/SC 10 Steel tubes and iron	EN 10305-3:2016		Steel Tubes for precision	Link	2016	CEN	Private																		none	none		Control Service	PLC,HMI (Part 3: PLCOpen XML)
CEN/TC 459/SC 10 Steel tubes and iron	EN 10305-5:2016		Steel tubes for precision	Link	2016	CEN	Private																		none	none		Digital models and Vocabularies	CDD, Definition of the properties and associated
CEN/TC 319 Maintenance	EN 13306:2018		Maintenance – Maintenance	Link	2018	CEN	Private											x						x	Prediction and optimisation	Maintenance		Collaboration, Business and	SIS design: Specification, design,
CEN/TC 319 Maintenance	EN 16646:2014		Maintenance – Maintenance	Link	2014	CEN	Private											x						x	none	Maintenance		Factory Network/ Field and Proximity	Profiles for industrial communication networks

Figure 27: Common standards of the Mapping Matrix (sample of the first draft)

- **TC1.3: Common feedback and recommendations (Ambassador: M.LORENZ, Austrian Standards, EFPF)**

Main goals: The main goal of this task is to collect and analyse the common feedback and recommendations for standardization in the projects and, based on the results, compose recommendations for actions for the relevant standardization bodies and organisations.

Outputs: The key output of this task is a list of normative recommendations for actions.

It was decided to perform this task on a recursive basis, asking members to submit new information on common standards or update old ones every six months.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Notable results: Due to the fact, that the analysis of major (standardization) results in a project is commonly planned towards the end of a project, it was decided to align the task activities with the planned timelines of contributors.

To accomplish the task, a working group of three projects, i.e. QU4LITY, ZDMP, and EFPF, was established to set up the first strategic steps of the task and then discuss these during the joint regular meetings on a regular basis. The results were documented and distributed to all members and interested parties within the projects for comment.

To complete the task, it was suggested that a publicly available document be created for all members to submit their recommendations and provide comments. An Excel document was created for this task with the following structural elements:

- *General information* about the submitted recommendation, such as: the ID of the recommendation; information about the particular member of a cluster that submitted the recommendation (e.g. in case further questions or more detailed information is needed); the actual text of a recommendation for action (e.g. to be submitted to a desired standards body or taken into further discussion); and the type of the recommendation and specific objective covered by the recommendation as e.g. digital twin, circular economy, big data, human, security, safety, interoperability , quality, reference architecture, system, system requirements, etc. .

  Note: With regard to the type of recommendation, it was suggested that the experience of the German standardization experts of the German Standardization Roadmap for Industry 4.0 (supervised by the Standardization Council Industrie 4.0) be used, who distinguish between two types of recommendations: 1) a fundamental recommendation for action (R) that can be a topic for standardization bodies and consortia; 2) and a user-specific recommendation (UR) that is more informative in nature and provide a feedback (e.g., news about upcoming standards or references to specific standards that may be of interest to one or another topic or industry).

- *Analysis details*, addressing such key questions as: What is the actual need ("short gap description")? How can the achievement of the recommendation be estimated? What other national or international bodies/standards/standards committees are affected / concerned?
- *Concrete actions* derived / executed after the analysis, which specifically answer the question: What has been already done to initiate the activity?

The following recommendations were identified and discussed in the first round:

ID:	001	**Submitted by:**	EFPF, QU4LITY, ZDMP
Type:	R	**Objectives:**	Interoperability; digital twin, AAS
Recommendation for action:		Broken consistency of concept digital factory framework and asset administration shell for industrial applications.	
Details:		Broken consistency between IEC TS 62832-1 Industrial-process measurement, control, and automation - Digital factory framework - Part 1: General principles and IEC 63278-1 ED1 Asset administration shell for industrial applications - Part	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

	1: Administration shell structure as well as the other planned parts of the standard.
Requirements:	Standard update IEC 63278-1 or synchronization with running /planned activities of IEC TC 65 WG24.
Affected bodies:	IEC/TC65 WG 24
Current progress:	QU4LITY members participated in the recent general meetings of the TC 65 WG 23 focusing on Smart Manufacturing and established contact to the newly established Task Group “Gap analysis and recommendations for standardization actions”.

ID:	002	**Submitted by:**	EFPF, QU4LITY, ZDMP
Type:	R	**Objectives:**	Promotion & Guidelines
Recommendation for action:		Provide better promotion of official guidance to research projects, including information on how standardization can be addressed in an appropriate/useful manner in the respective project tasks, including appropriate linkage to responsible coordination and support activities (CSAs).	
Details:		Specific guideline with concrete KPIs is expected. For instance, already available results of the relevant activities as e.g., project BRIDGEIT could be used more actively in the promotion.	
Requirements:		Currently under discussion: 1) Report to European Commission. It can be very useful to inform projects responsible for standardization activities about relevant mechanisms or contacts at the EU level before starting the project. 2) Possibly contact the MSP WG to clarify on who is responsible for such kind of a linkage. 3) There may be helpful guidance in CEN/CENELEC Guideline 23 in BRIDGEIT2. 4) EFFRA role in providing support, e.g., it may be helpful to further support EFFRA with DMP Cluster WG 1.	
Affected bodies:		EU MSP WG 1; BRIDGEIT; EFFRA	
Current progress:		1) Experts got into the first discussion with the WG MSP contact to appoint the gap here. 2) Experts form the BRIDGEIT project have been involved into the discussion of this recommendation. 3) EFFRA is actively promoting such information and can promote the guidelines if needed on the EFFRA portal.	

ID:	003	**Submitted by:**	EFPF, QU4LITY, ZDMP
Type:	R	**Objectives:**	Architecture
Recommendation for action:		It is suggested that upcoming projects, especially those focusing on the development of an Industrie 4.0 or Smart Manufacturing compliant reference architecture, follow the latest developments in standardization on this topic.	
Details:		Investigate on possibility to map to the Smart Manufacturing Meta-model developed in the Technical Report (TR) Smart Manufacturing Meta-model " A Meta-modelling analysis approach to Smart Manufacturing Reference Models (SMRM)". The standard should be included as a primary concept within the project to avoid mapping to specific reference architecture models.	
Requirements:		1) Creation of an understanding of the topic; 2) Presentation of the concept from TR to projects; 3) possibly inclusion in the H2020 portfolio within the related calls.	
Affected bodies:		EC and projects	

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

Current progress:	Monitoring of the current activities around the Technical Report (TR) Smart Manufacturing Meta-Model

ID:	004	**Submitted by:**	EFPF, QU4LITY, ZDMP
Type:	R	**Objectives:**	Practical advise
Recommendation for action:		It is advised that project consortia carry out a comprehensive gap analysis regarding current standardization needs as early as the application phase in order to establish a direct link to relevant standardization activities and to be able to contribute in a targeted manner in a later phase.	
Details:		In doing so, EU should identify ways in which the applicant can be supported with regard to relevant gaps or bodies that regularly revise current standardization needs (e.g. EFFRA innovation portal wiki; StandICT).	
Requirements:		1) The regular activities of DIN/DKE and SCI 4.0 as part of the German standardization roadmap on Industrie 4.0 are an example of where the relevant information on the existing need for standardization can be found. 2) ICT Rolling Standardization Plan could be considered.	
Affected bodies:		Projects writing proposal	
Current progress:		Initial discussion has shown that it is not easy to implement due to the estimated resources planned at the proposal stage. The biggest challenge is that the initial understanding of the contribution efforts is very limited. Standardization contacts and activity types may change or vary with the development of the project.	

ID:	005	**Submitted by:**	EFPF, QU4LITY, ZDMP
Type:	R	**Objectives:**	Support action
Recommendation for action:		There should be a central contact person at EU level to liaise and make a recommendation to existing committees at EU level.	
Details:		*tbd*	
Requirements:		Under discussion: How to accelerate the connection to relevant entities, e.g., a TC, and find relevant contacts right after the project starts?	
Affected bodies:		EC, projects and standardization bodies	
Current progress:		Recommendation is under development.	

ID:	006	**Submitted by:**	QU4LITY
Type:	R	**Objectives:**	Practical advice
Recommendation for action:		Brief revisions and updates should be made periodically in the project	
Details:		The standardization landscape changes significantly with respect to SDO activities during the project lifetime, so it is not possible to provide a complete roadmap of all future standardization activities for a period of more than one year. From our experience, we can recommend that brief revisions and updates be made periodically during the active work phases (e.g., at three- or six-month intervals)	
Requirements:		Under discussion: What is the right time for standardization in the project? When to approach standardization bodies? Is there a global approach that a project can easily apply for its standardization needs?	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Affected bodies, initiatives, etc.:	Leaders of standardization tasks / activities in a project, *tbd*
Current progress:	Collecting lessons learned from the projects.

ID:	007	**Submitted by:**	QU4LITY
Type:	R	**Objectives:**	Support action
Recommendation for action:		Support action is needed to address challenges regarding membership, fees, and involvement possibilities for projects in SDOs	
Details:		1) Each member represents the international SDO in his or her country. Individuals or companies cannot simply become members of the international SDO for a short period. However, the right ways must be found to give the projects the opportunity to present their results to the interested bodies during the project period without high fees and long-term involvement. 2) The standardization activities at the European and international level are usually fee-based, which limits the project active involvement. 3) Other constrains e.g. Participation in committees is limited to a certain number (e.g., ISO up to five).	
Requirements:		Under discussion: 1) Find out in advance about the international SDO and its members in the respective country; 2) Establish a direct contact to the chairperson and elaborate on possibilities for participation rights in the development of international standards. 3) Projects should check participation rights before applying for membership and paying the expensive fees. Full ISO members can for instance influence the development of ISO standards and guidelines by attending and voting at ISO technical and policy meetings. 4) We recommend checking budget options during the proposal phase as membership fees cannot be determined from available online information and are based on the country's gross national income and trade figures. 5) A very effective way to contribute to standardization activities and initiate valid discussions is to attend the face-to-face meetings as a guest (e.g., participating in discussions and presenting results). Participation as a guest is usually limited to one or two meetings (i.e., free of charge). However, depending on the schedule of WG/TC meetings, intercontinental travel expenses may be incurred.	
Affected bodies:		Future leaders of standardization tasks / activities in a project	
Current progress:		Collecting lessons learned from the projects.	

ID:	008	**Submitted by:**	QU4LITY
Type:	R	**Objectives:**	
Recommendation for action:		It is recommended to estimate the time needed for committee work very accurately before joining a working group and developing the standard.	
Details:		Experience shows that the effort is very high, which often has to be compensated by the company and internal budget.	
Requirements:		It is advisable to check the planned meeting schedule in advance. The number of meetings depends primarily on the intensity of the work planned by the working group. In addition to face-to-face meetings (e.g., two or more per year), weekly or monthly conference calls may be held. It is also important to calculate in advance all other important tasks of a member, such as commenting or voting on standards. Working on standards documents is very time-consuming and	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

	depends on the size of the document and the technical level, which may also require additional research.
Affected bodies:	Partners contributing to standardization in the project
Current progress:	Collecting lessons learned from the projects.

❑ **T1.4: Joint CWA proposals and guidelines (Ambassador: C.GRUNEWALD, DIN, ZDMP)**

Main goals: The main goal of this task is to identify and coordinate the joint CWA activities.

Outputs: The main output of this task is the joint strategy of WG 1 with regard to CWA proposals (incl. joint discussions, collecting of inputs, regular updates, etc.)

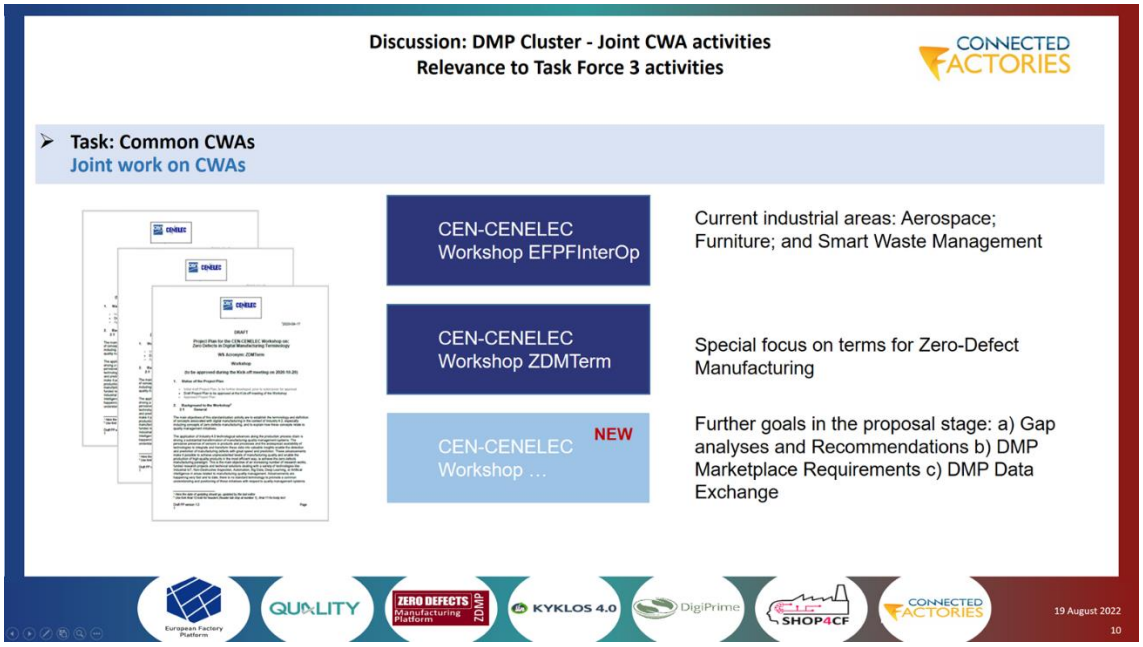


Figure 28: Joint CWA activities

Notable results: The main results of the task (see also Figure 28) can be summarized as follows:

Activity: *CEN/CLC/WS ZDMTerm - Zero Defects in Digital Manufacturing Terminology*

- Project reference: **prCWA 17918** (pr=WSZDM001)
- Title: Zero defects manufacturing in digital manufacturing terminology
- Scope: The CWA defines and collates terms for zero defects manufacturing in digital manufacturing with correlation to Industry 4.0 and quality management
- Project link: https://standards.cencenelec.eu/dyn/www/f?p=305:22:0::::FSP_ORG_ID,FSP_LANG_ID:2842664,25&cs=17B0879A0B26FAEEFB0FAAF7B302607DE
- Status: Under drafting
- Initial date: 2020-10-29

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Activity: *CEN/CLC/WS ZDMTerm - Zero Defects in Digital Manufacturing Terminology*

- Project reference: **prCWA 17907** (pr=WSEFP001)
- Title: European Connected Factory Platform for Agile Manufacturing Interoperability (EFPFInterOp)
- Scope: This CEN-CENELEC Workshop Agreement (CWA) defines a reference architecture for federating manufacturing platforms focusing on the interoperability on Service-Oriented Architecture (SOA), Protocol, Security and Data Model level. Additionally, a reference implementation in the form of the EFPF Data Spine and associated components will be described including Best Practices identified. This CWA will not define requirements related to safety aspects.
- Project link: https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:76335,25&cs=1C5EA6E502A43AF91A051D4BC2F94ECF3
- Status: Under drafting
- Initial date: 2020-10-29
- Date of availability: 2022-12-01 (7)

Activity: *Further CWAs under discussion and preparation*

During the WG 1 meetings the experts also discussed other possibilities for joint work:

- DMP Marketplace requirements (Decision: Proceed preparation, is ongoing)
- DMP Data Exchange (Decision: Investigating possible collisions with other activities)
- DMP Gap Analyses and Recommendations (Decision: to change from CWA format to joint report)

Activity: *Short analysis of the joint work*

In general, the following considerations can be derived from the task:

- The members of WG 1 showed a high motivation and willingness to participate in the CWAs;
- Joint dissemination activities show high acceptance of responsible TCs;
- The expert work in CWA working group is very time consuming and can take more time as it is agreed in the original plan;
  In particular, the management of a CWA may require much more effort than expected. This should definitely be included in the considerations and management of project resources.

❑ **T1.5: Joint standardization events (Ambassador: O.MEYER, FHG, CF2)**

Main goals: The main goal of this task is the coordination and support of joint standardization events for WG 1 members.

Outputs: The key output of the task is a report on standardization events related to WG 1 activities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Notable results:

Activity: *Joint events with regard to standardization*

The following events with regard to standardization activities of WG 1 as well as the dissemination of the specific standardization results of the projects were coordinated in the task:

- Cybersecurity workshop organised by ConnectedFactories 2 on the 20th of January 2020
- ConnectedFactories Webinar - Standards for digital manufacturing organised in association with the ConnectedFactories CSA on the 20th of October 2020.

More details on events are reported in section **Fout! Verwijzingsbron niet gevonden.**.

Activity: *General exchange and news about interesting events*

Another support activity in this task was to inform WG 1 members about interesting events with regard to standardization and exchange on news (see Figure 29).

Figure 29: (Example) Informing WG 1 members about interesting upcoming and past events.

❑ T1.6: Joint dissemination work (Ambassador: O.MEYER, FHG, CF2)

Main goals: The main goal of this task is the coordination and support of joint dissemination activities (joint work with the DMP Cluster WG Dissemination).

Outputs: The key output of the task is to discuss and support DMP WG 2 Dissemination activities that link to standardization and prepare contributions based on joint results in WG 1.

Notable results: The first discussions and coordination of the joint dissemination topics took place in the regular joint meetings. The common strategy still needs to be aligned with all partners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The key effort was concentrated on the joint CWA publications.

Further topics of joint publications are still under discussion and will be addressed in the upcoming meetings in September and October 2022. Till then more concrete results will be available from the projects that started later.

The last discussion was about the results of WG 1 and the current list of recommendations. There was discussion on how to make the results publicly available. Concrete ideas were developed to include the possibility of the EFFRA platform.

4.2.3 Meetings and scope

Since the launch of the DMP Cluster several WG 1 meetings and workshops took place (see Table 3). According to the latest resolutions of the WG 1, the meetings are to be held regularly at three-month intervals. Intermediate meetings with regard to any internal work of the tasks are admissible at any time.

The coordination and organisation of the meetings is the responsibility of the ConnectedFactories2 Task 1.3 lead. The convenor of the WG 1 is O. MEYER (Fraunhofer IPA).

Table 3: Relevant CSA activities in the DMP Cluster.

DMP Cluster / Plenary

Date	Activities	References
19-09-25, 20-03-12, 20-05-13, 20-06-04, 20-12-02/ 20-12-03, *21-02-26*	Presentation / WG 1 report on current status and results	Presentation WG 1

DMP Cluster / Leads

Date	Activities	References
20-09-16 *21-01-28*	Discussion / WG 1 report on current status and results	Presentation WG 1
20-09-25 20-11-20	Discussion / Alignment between DMP Cluster and ConnectedFactories2 activities; WG 1 / CF2 Task 1.3 alignment	

DMP Cluster / WG 1 Standardization

Date	Agenda	References
20-01-23 1st meeting	• General update on actions (MEYER, CF2) • Task 1.0: General strategy • Task 1.1: Event "Boosting Innovation through standards - Your gateway to the market"	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

20-05-12 2nd meeting	• General update on actions (MEYER, CF2) Task 1.0: Update of the projects' activities ○ EFPF ○ ZDMP ○ QU4LITY • Task 1.4: CWA preparation	Meeting minutes
20-05-18 3rd meeting	• General update on actions (MEYER, CF2) • Task 1.0: Update of the projects' activities ○ EFPF ○ ZDMP ○ QU4LITY ○ KYKLOS 4.0 ○ digiPRIME ○ SHOP4CF • Presentation of the CWA drafts (Ch. GRUNEWALD, ZDMP), incl. discussion points: ○ Titles, members and participants, timeframe ○ Targeted committees ○ "Scope narrowing" (project contribution) ○ other related topics	Meeting minutes
20-06-04 4th meeting (first round)	• General update on actions (MEYER, CF2) • Task 1.0: Update of the projects' activities • New WG 1 member Change2Twin • Task 1.4: CWA preparation (GRUNEWALD, ZDMP) ○ Titles, members and participants, timeframe ○ Targeted committees ○ "Scope narrowing" (project contribution) ○ other related topics	Meeting minutes
20-06-23 4th meeting (second round)	• General update on actions (MEYER, CF2) • Task 1.0: Update of the projects' activities ○ EFPF ○ ZDMP ○ QU4LITY ○ KYKLOS 4.0 ○ digiPRIME ○ SHOP4CF • Task 1.2: Common standards (MEYER, CF2) • Presentation: Standardization in KYKLOS4.0 (BENGTSSON, KYKLOS4.0) • Presentation: Standardization in QU4LITY (MEYER, QU4LITY) • Presentation: Standardization activities/RAMI 4.0 (NAZARENKO, UNINOVA)	• Meeting minutes; • Presentation "Standardization activities/RAMI 4.0"; • Presentation "KYKLOS on standards" • Presentation "CWA status update"

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

	• Task 1.4: CWA preparation (GRUNEWALD, ZDMP)	

20-09-15
5th meeting
	• General update on actions (MEYER, CF2)
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ KYKLOS 4.0
	  ○ digiPRIME
	  ○ SHOP4CF
	  ○ Change2Twin
	• Task 1.6: Joint papers update (cooperation with WG3 "Joint research activities")
	• Task 1.2: Common standards (MEYER, NAZARENKO, Report)
	• Task 1.5 Webinar preparation
	• Task 1.4: CWA preparation (GRUNEWALD, ZDMP)
		• Meeting minutes
		• Excel "Status update"
		• Excel "Standards matrix"
		• Presentation "CWA status update"

20-12-09
6th meeting
	• General update on actions (MEYER, CF2)
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ KYKLOS 4.0
	  ○ digiPRIME
	  ○ SHOP4CF
	  ○ Change2Twin
	• Task 1.2 Common standards (MEYER)
	• Task 1.3 Collection of gaps and recommendations (MEYER)
	• Task 1.6 & T1.5: Events and joint dissemination activities (MEYER)
	• Task 1.4: CWA preparation (GRUNEWALD, ZDMP)
		• Meeting minutes
		• Excel "Status update"
		• Excel "Standards matrix" (online)
		• Presentation "CWA status update"

21-02-17
7th meeting
	• General update on actions (MEYER, CF2)
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ KYKLOS 4.0
	  ○ digiPRIME
	  ○ SHOP4CF
	  ○ Change2Twin
		• Meeting minutes
		• Excel "Status update"
		• Excel "Standards matrix" (online)
		• Presentation "DigiPrime Standards"
		• Presentation "KYKLOS40 Horizon Europe and more"

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

	• Task 1.3 Collection of gaps and recommendations (MEYER) • Task 1.6 & T1.5: Events and joint dissemination activities (MEYER) • Task 1.4: CWA preparation (GRUNEWALD, ZDMP)	

21-05-10
8th meeting
	• General update on actions (MEYER, CF2)
	• New WG 1 member DAIS and DRYADS
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ KYKLOS 4.0
	  ○ digiPRIME
	  ○ SHOP4CF
	  ○ Change2Twin
	  ○ DAIS and DRYADS
	• Task 1.2 Common standards (MEYER)
		• Meeting minutes
		• Excel "Status update"
		• Excel "Standards matrix" (online)
		• Presentation "Change2Twin standards support survey"
		• Presentation "Europe fit for the digital age AI"
		• Presentation "FORSEE webinar #4 – standardization session"

21-08-09
9th meeting
	• General update on actions (MEYER, CF2)
	• New WG 1 member DAT4.ZERO
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ KYKLOS 4.0
	  ○ Change2Twin
	  ○ DAIS and DRYADS
	  ○ DAT4.ZERO
	• Task 1.2 Common standards (MEYER)
		• Meeting minutes
		• Excel "Status update"
		• Excel "Standards matrix" (online)

21-11-08
10th meeting
	• General update on actions (MEYER, CF2)
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ digiPRIME
	  ○ SHOP4CF
	  ○ DAT4.ZERO
	• Task 1.2 Common standards (MEYER)
	•
		• Meeting minutes
		• Excel "Status update"
		• Excel "Standards matrix" (online)
		• Deliverable "D1.2 First report on standardization relevant for digital twins"
		• Presentation "ForeSee roadmap to the predictive maintenance technologies production systems"

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

		• Presentation "Interoperability - InterOpera project"

22-02-07
11th meeting
	• General update on actions (MEYER, CF2)
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ KYKLOS 4.0
	  ○ digiPRIME
	  ○ SHOP4CF
	  ○ Change2Twin
	  ○ DAIS and DRYADS
	  ○ DAT4.ZERO
	• Task 1.2 Common standards (MEYER)
	•
		• Meeting minutes
		• Excel "Status update"
		• Excel "Standards matrix" (online)
		• Presentation "SHOP4CF standardization activities"
		• Deliverable "D2.8 QU4LITY"

22-08-01
12th meeting
	• General update on actions (MEYER, CF2)
	• Task 1.0: Update of the projects' activities
	  ○ EFPF
	  ○ ZDMP
	  ○ QU4LITY
	  ○ KYKLOS 4.0
	  ○ digiPRIME
	  ○ SHOP4CF
	• Task 1.6 & T1.5: Events and joint dissemination activities (MEYER)
		• Meeting minutes
		• Excel "Standards matrix" (online)
		• Deliverable "QU4LITY D9.6 Contributions to SDOs and Clusters" (final)

4.3 Reference documents on standards

With regard to commonly used standards for Zero-Defect Manufacturing, ConnectedFactories2 has set several tasks to fulfil during the project: 1) Consultation of projects on current standards, 2) Identification of standards used in projects, 3) Gathering information on the specific application of standards, 4) Providing means for classifying and assigning standards to individual projects and cases, 5) Regular exchange of experiences in the application of standards, possible standardization gaps and resulting standardization activities.

The complete list of collected standards and other reference documents were transferred to EFFRA innovation portal and can be accessed via: https://portal.effra.eu/wiki. The list of standards is the result of the work of the WG 1 in DMP Cluster in *Task TC1.2: Common standards* (see section 4.2.2).

Furthermore, the portal provides helpful shortcuts that help a user to apply mapping functions on e.g., projects and standards or demonstrator and standards (see Figure 30).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

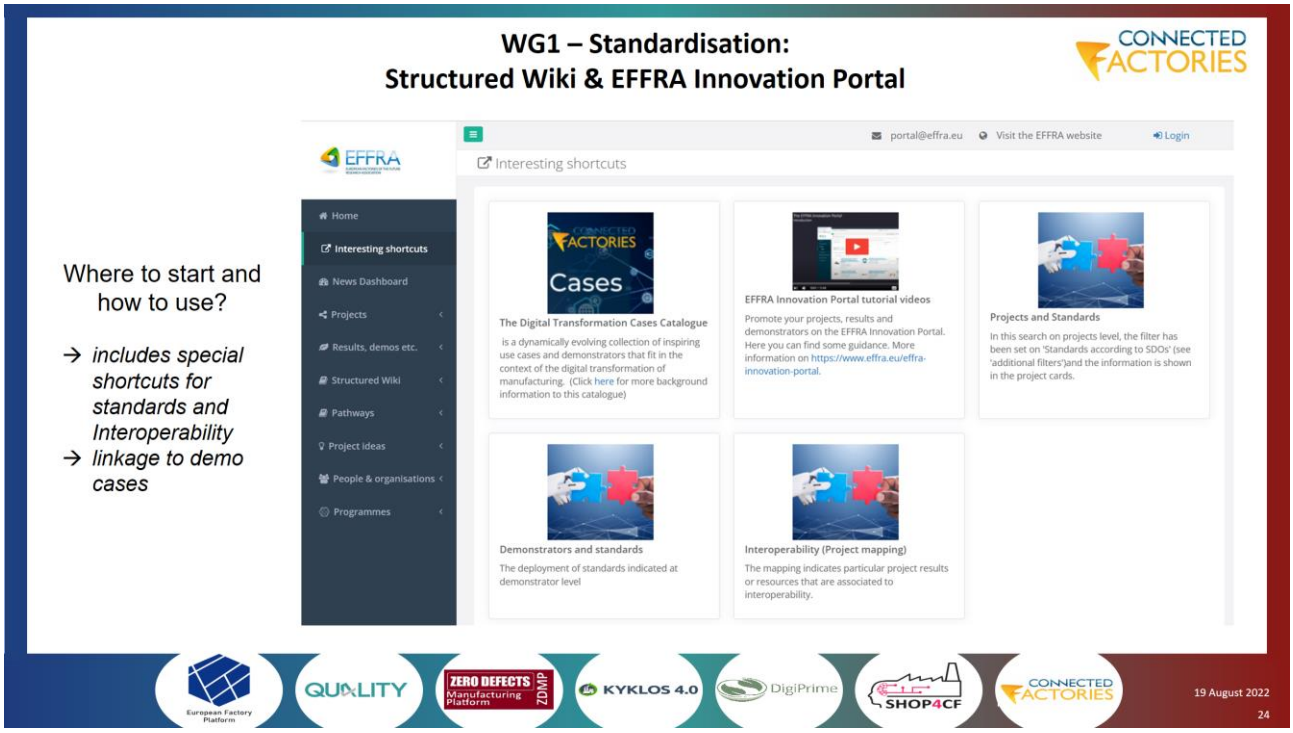


Figure 30: Using shortcuts for standards

More information is provided in the ConnectedFactories2 Deliverable *D1.3 Structured wiki update on Business models, Legal aspects, Interoperability, Standardization, Cybersecurity and Human aspects*.

4.4 Examples from projects (mapping of projects)

As part of the project, ConnectedFactories2 held individual workshops with thematic sessions - including the session on standardization - dedicated to each of the six projects. Herewith the main questions that were addressed regarding standardization that were inspired by the developed Guiding Principles for knowledge valorisation of the European Commission.

1. **Standardization approach:**
   - Has your project developed a specific standardization approach or involved a review or assessment of existing standards? If YES, please give a short description of this activity.
   - Have there been an SDO, SNB or TA directly involved in the consortium and how did these contribute to the methodology of the work package?
   - Have the standardisation activities in your project led to specific deliverables? If YES, which ones?
2. **Addressing standardization bodies:**
   - Has your project liaised with standards developing organisation (SDO), national standardisation body (NSB) or technical committee (TC)? If YES, which ones?
   - How did you choose cooperation with the SDO, NSB or TCs?
   - Did the involvement of the SDO or NSB influence the technological choices in the project?
3. **Timing of standardization activities:**
   - When were standardisation activities addressed / implemented in the project (e.g. in a dedicated work package / task / across the work packages / etc.)?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- At what stage did you liaise with SDOs, NSBs or TCs and what did you expect from this collaboration?

4. **Context:**
   - How important do you consider standardisation in your project?
   - How have consortium members integrated standardization activities into their work and what were the main reasons for including standardization in your project (e.g. requirement from market, legislation, organisation, project call; critical for research, exploitation and market strategy; etc.)?
   - Which standards were addressed by your project?
5. **Experience and lessons learned:**
   - Have you experienced any difficulties or obstacles in carrying out standardization activities during the project?
   - Has your project directly involved or led to a specific recommendation or proposal?
   - Are you participating in clustering with other projects?

The following subchapters integrate the results of the workshop according to the structure described above.

4.4.1 EFPF- European Connected Factory Platform for Agile Manufacturing

This subchapter summarizes the key mapping results regarding EFPF project.[26]

4.4.1.1 Standardization approach

Within EFPF, standardisation activities are derived by the experts within the consortium to provide two-way communication between EFPF RTD activities and ongoing standardisation activities. Among others the project also promotes the use of "Standardisation guidelines for IST research projects interfacing with ICT standards organisations" by the Cooperation Platform for Research and Standards (COPRAS[27]).

In its standardization strategy, the EFPF follows a specific approach based on the following principles:

a) identification of stakeholder interests;
b) derivation of related activities (listing and road mapping of key standardization activities under the project) and voluntary/mandatory schemes;
c) mapping of results to project needs: e.g., to a task, pilot project, etc.;
d) specific focus on EU regulations, including harmonization of standards and conformity complaints; and
e) focus on improving market solutions by demonstrating the application of standards.

Overall, the standardization strategy was reinforced by the use of a standardized approach called PDCA ("plan-do-check-act"). The standardisation plan contributed to updates and helped to establish the link to pilots keeping them and information updated

[26] https://www.efpf.org/

[27] https://www.w3.org/2004/copras/docu/D15.html

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Under this premise, the project closely monitored the progress of standardization. For this reason, a special regulatory survey was conducted among all pilots at the very beginning of the project. ASI, as lead of the respective task on standardization, has prepared a survey of the relevant and active standardisation initiatives that EFPF partners could leverage, participate, and contribute towards. The results were subsequently published.

Another survey was then conducted to update the information and identify new standards. The survey also addressed limitations of existing standards in the project, e.g., barriers, needs for standardization, experiences of partners (also related to innovations). These gaps were collected and analysed by standardization experts. As a result, new standardization initiatives could be launched in the form of CWAs.

Collaboration with pilots was also closely integrated. For example, the pilots were involved in the development of standards (e.g., role allocation between taker and producer). This allowed pilots to share their experiences with standards. Standardisation experts aided strengthen the cooperation with pilots.

Several methods were used to "translate" the latter into the “language of standardization”. For instance, the numbering of the standards was specifically adapted to the expectations of the pilots. Moreover, standardization experts held educational webinars for project partners, explaining overall standardization process of CEN, CENELEC, ISO, and IEC in a nutshell; showing the contribution methods; clarifying the role of EFPF in DMP Cluster WG 1; etc.

The projects’ activities in standardization are coordinated in the WP11: Dissemination, Collaboration and Standardisation, Task 11.3 (Regulatory Alignment, Compliance and Standardisation Strategies). The Austrian Standards was directly involved in the consortium and supported the methodology in the Task. Inputs form project partners who were directly involved in TCs etc. were taken into consideration

So far, the work has included regular reports provided by EFPF partners to guide standardization activities:

- D11.11 - Standardisation Plan: The purpose of this EFPF deliverable is to provide a plan for standardisation activities in the EFPF project. This document describes the rational for standardisation in the EFPF project, lists relevant standards, describes the standardisation plan, and provides an overview of general standardisation procedures.
  D11.7 - Regulatory Alignment, Compliance and Standardisation Strategies-I.: This EFPF deliverable provides a strategy for standardisation activities in the EFPF project and an overview on relevant regulations. This document describes the degree of participation of EFPF project partners in the standardization process and which regulations need to be considered in the project activities.

4.4.1.2 Addressing standardization bodies

The EFPF consortium carries out important interactions with the national and European regulation and standardisation bodies on smart factory automation, data processing and analytics to facilitate the sharing of data and standardisation processes.

As for liaisons, the project focused mainly on collaborations. A list of the collaborations is published in the project deliverables. It includes, for example, ISO, ISO/IEC JTC1 and others. A special collaboration took place with CEN/CENELEC regarding EFPF activities in the CWA format. The project has been very active in cluster activities (e.g. OPEN DEI, DMP Cluster, etc.) that have contributed on the whole to the improvement of the normative ecosystem of the project.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

The focus for the committees identified in the proposal, as well as for the collaborations, evolved over the course of the project. Here, the research was very helpful in finding new consortia and identifying others (e.g., the Gaia-X Foundation).

The project liaised with SDOs, NSBs or TCs during the whole project. The involvement of SDOs and other consortia did not have a particular impact on the technological choices. However, the EFPF made its experience based on a requirement, i.e., the project kept track of integrity and security, which were important and served as a filter for new changes.

The experts report that the technical evaluation influenced the decision on which standards to use. Even after some implementation work, the decision was made to support the solution with standards as it was implemented.

4.4.1.3 Timing of standardization activities

In the individual workshop with ConnectedFactories2, EFPF addressed the question "When should standards be reviewed?" The project reports that the first draft focused primarily on the standards landscape with respect to project management verification. For this reason, EFPF began analysing standards and technical specifications very early in the project. At the halfway point, it was important to familiarize the partners with the standardization process. EFPF experts emphasized the importance of general normative training for the pilots, e.g., in the form of workshops for technical partners. These workshops contributed a lot to understanding and getting the partners to the same level of comprehension.

4.4.1.4 Context and focus objectives

Due to the nature of the technical activities (i.e., the implementation of a federated digital manufacturing platform connecting multiple platforms, tools, and services via a standardized interoperable Data Spine), several EFPF priority objectives are considered relevant to ongoing standardization and regulatory activities. Among these are e.g. shop floor automation; reference architecture modelling; cybersecurity; blockchain; digital twin for manufacturing; safety in workplace and human machine interaction.

Thus, EFPF recognizes an urgent need for the convergence of different tools/solutions towards a networked, interoperable federation. This is due to the common problem of increasingly overlapping standards and the challenge of finding suitable standards for specific platform solutions. The approach taken in the EFPF is to closely monitor ongoing developments in various standardization initiatives and, through expert support, to align RTD activities with ongoing standardization activities. The main goal here is to adopt existing standards and, where possible, contribute to the development of standards. Based on this approach, a standardization plan was developed to better plan the project's standardization activities on a strategic and tactical level.

A data gathering exercise was organised within the project to raise partner awareness about relevant standards and to collect partner input on EFPF related standards. As the result, EFPF identified more than 40 standards references that were classified and listed in the D11.11. The outcomes are transferred in the Mapping Matrix (see section 4.2.2). An updated list of standards used by EFPF is listed in D11.7 (Regulatory Alignment, Compliance and Standardisation Strategies-I.), which is regularly updated.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

EFPF launched an EN-CENELEC Workshop on European Connected Factory Platform for Agile Manufacturing Interoperability (EFPFInterOp[28]). The invitation was spread among the WG 1 members. The motivation of EFPF for creating the CEN-CENELEC Workshop is to have a standardized interoperability framework enabling an open market infrastructure for European manufacturing, interlinking digital manufacturing platforms, smart factory tools and Industry 4.0 concepts to realise and support a connected and smart ecosystem of the future.

4.4.1.5 Experience and lessons learned

The experts consider standardization to be an important element of the project. The experience of a user in EFPF shows a very practical character. They report that the more standards are followed, the more complicated and expensive it can become in practice. Also, using a standard raises expectation among partners, which can create some challenges during the development phase.

Some observations were done regarding the difference between technical and industrial standards. Users have experienced that some of the industry standards were difficult to implement (e.g., the standard for data security and trust), which ultimately led to uncalculated effort and inconsistency.

Less understanding was noted for technical standards. It took additional iterations with pilots to achieve the same level of understanding. E.g., industry specifications were of interest - large ecosystem is hard to describe - too many standards. With this in mind, the experience of project leaders suggested that a distinction should be made between industry standards and technical standards.

One of the findings is the need to train partners on the normative context. For example, EFPF has found the internal webinars to be very helpful. They were met with a positive response. As a result, several webinars have been organized to capture partner feedback, highlight areas of interest and ongoing developments in standardization, and support partners in their standardization activities.

With respect to the issue of patterns and licensing (SAPs), which was also addressed in the project activities related to standardization, the need to verify certain patterns in advance was identified. If not done properly, the review can become a challenge in the project. For instance, in communications, a patent holder needs to be contacted to grant a free license which can be very time consuming.

Besides, also poor accessibility of standards was also pointed to be an issue, e.g., the conditions for licence fees can be difficult to agree upon in the context of a project.

Other experiences and recommendations were summarized within the Task 1.3 of the WG 1 described in the section 4.2.2.

4.4.2 QU4LITY – Joining forces towards an European Industrial Autonomous Quality

This subchapter summarizes the key mapping results regarding QU4LITY project.

28 https://standards.cencenelec.eu/dyn/www/f?p=305:110:0::::FSP_PROJECT,FSP_LANG_ID:76335,25&cs=1C5EA6E502A43AF91A051D4BC2F94ECF3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

4.4.2.1 Standardization approach

The projects' activities in standardization were coordinated in the QU4LITY Task 9.2 Standardization and Clustering led by Fraunhofer IPA. The work includes periodical reporting among which two specific deliverables could be highlighted in the context of standardization, i.e.:

- Deliverable 9.6 - Contributions to SDOs, Associations and Clusters: (Final version) the document provides an overview of the project's standardization activities and contributions to standardization bodies, associations and clusters, describes the current standardization landscape within the QU4LITY scope, and exhibits critical standardization gaps with regard to Industry 4.0.
- Deliverable 2.8 - Standards Compliance and Interoperability Specification: (Final version) this document defines common specifications for standards compliance and interoperability for zero-defect production within the QU4LITY project and gives general recommendations for the use of these standards.

The standardization strategy of the project foresees several important tasks:

- setting of the overall standardization strategy of the project and specifying the common standardization landscape;
- active participation and reporting on various standardization activities (also including monitored activities) based on the activities and contributions of the project consortium at international, national, and European level;
- active participation and reporting on the project's clustering activities regarding standardization, listing the recent standardization work and cluster roadmap activities; and
- involvement in and provision of related network events pursuing a specific standardisation purpose;
- provisioning of a detailed overview and summary of the work done, including some useful information on limitations and lessons learned, and future work.

To achieve the tasks, experts developed the standardization roadmap, in which they identified the central challenges of the task and derived appropriate measures. These activities helped to create a clear workflow among the experts involved and to identify important standardization objectives of the projects as well as the next steps. An open and easy interaction between the pilots and the experts was one of the main goals. In doing so, the project placed an important requirement on its internal work, namely, to bring pilots and experts to a round table and provide as much support and training as possible in order to achieve a uniform result and understanding of the normative framework.

Overall, the experts of the standardization task acted as an important link between the project and standardization activities on the national, international and European levels. They provided reviews and recommendations for specific project activities regarding possible standardization gaps, including helpful references and recommendations. Standardization experts were constantly involved in the key concepts of the project

To coordinate the activities of the more than 25 project partners who were very active in this task, internal (remote) workshops were held regularly by the task lead. These made it possible to follow the current activities of all participants between workshop periods and to exchange information on the status and recent developments in the field of the identified standardization objectives. Although the overall strategy was based on a concrete roadmap (whose foundation consisted of standardization goals), the task included agile

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

working principles within the task. This involved discussing and adjusting the roadmap where necessary to accommodate the new activities.

All current relevant activities were collected in the standardization activities matrix and regularly updated internally. At the end of the work, this matrix gave a very good overview of the KPIs of the standardization activities in the project. The internal standardization workshops were supplemented by direct exchanges with other task managers and experts, who provided more detailed information on various aspects of the standardization activities.

4.4.2.2 Addressing standardization bodies

QU4LITY experts have actively contributed to more than 19 different SDOs and SSOs and started collaborations with 4 clusters. The main achievements related to contributions to standards at ISO/IEC JTC 1, IEC, IDSA, euRobotics, CEN/CENELEC, ETSI, as well to the corresponding German and Italian national bodies such as DIN/DKE, SCI 4.0 and many others. D9.6 provides a very detailed description of project impact referring to concrete contributions to standards.

Regarding networking with standards-focused associations and clusters, several respective activities were included in the deliverables. Here it is worth to emphasize the active role of QU4LITY experts in the DMP Cluster contribution to a common standardization strategy in various topics. On the other hand, the project reports on a constant exchange with other relevant associations and industry initiatives, EU H2020 DIATOMIC, OPEN DEI, MIDIH, BOOST4.0 and other activities. Further details are also described in the D9.6.

4.4.2.3 Timing of standardization activities

The standardization activities of the project started very early and concentrated mainly on the research and analysis of normative references and standards, consolidation, and management of the standardization strategy in the first phase of the project. The progress of the activities was carried out according to the standardization plan and in alignment to the project phases (see Figure 31). However, this was revised and updated during the project development.

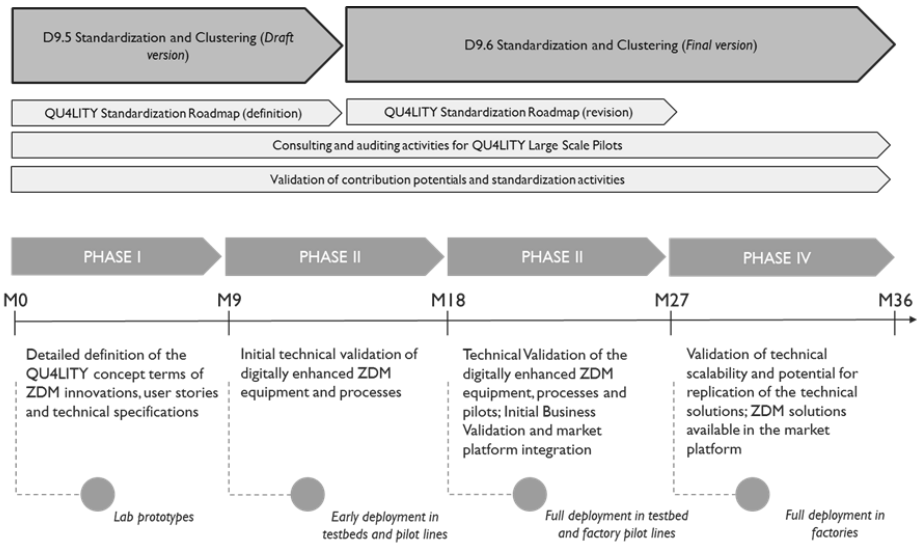


Figure 31: QU4LITY - Standardization activities across the project phases (Source: QU4LITY, D9.6 p. 11)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Collaboration with related EU-funded projects and other networking activities (e.g. participation in standardization workshops, conferences, thematic webinars, etc.) were carried out throughout the whole period.

4.4.2.4 Context and focus objectives

In its initial research, the project identified the following focus objectives to be addressed in its standardization activities in the ZDM field, see Figure 32. The research includes not only the focus objectives in standardization, but also points out the activities of interest in one or another area.**Fout! Verwijzingsbron niet gevonden.**

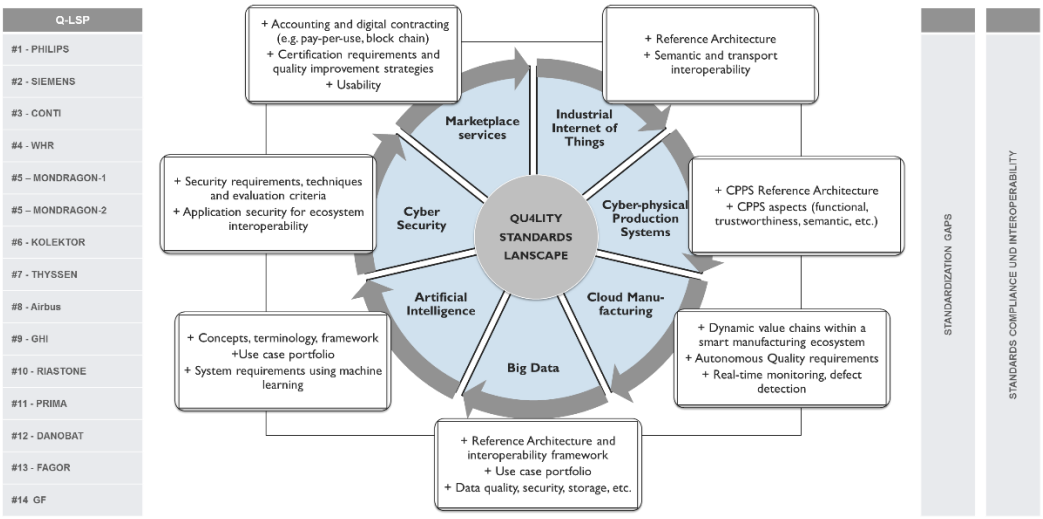


Figure 32: Focus objectives across the QU4LITY's ZDM technology fields and identified standards (Source: QU4LITY, D2.8)

In its strategy, the project also analysed the key areas across RAMI 4.0 layers and maps these to pilots' technological requirements and needs (see Figure 32 and Figure 33).

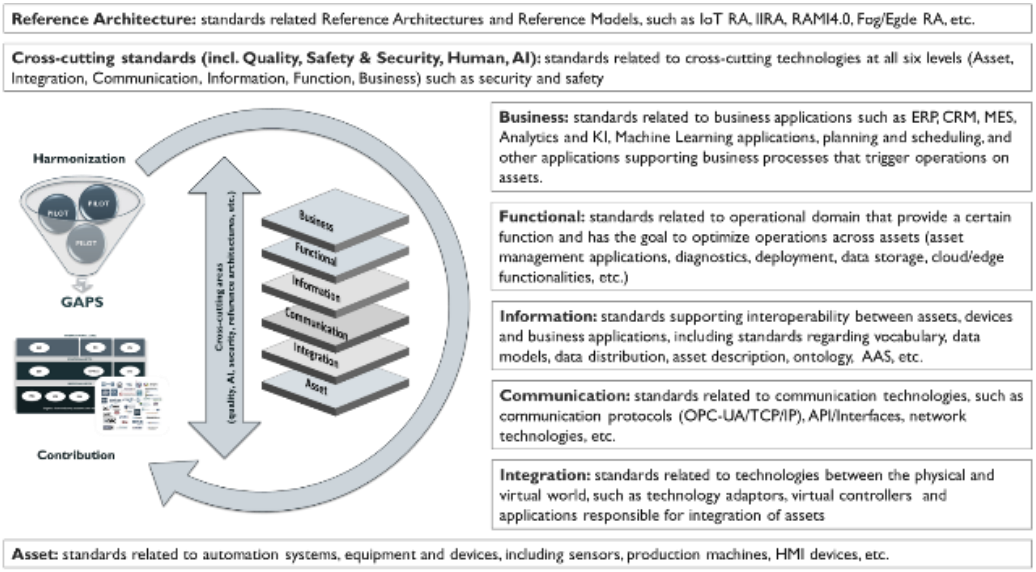


Figure 33: Standardization areas identified across RAMI 4.0 layers (Source: QU4LITY, D9.6 Appendix B)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The final report on standardization activities of the project indicates that experts participated in more than 140 activities, including more than 80 general assembly meetings (one to two-day meetings) of the SDOs/SSOs, more than 60 remote working sessions and workshops with standardization focus. The final work was intensively done around such key standardization objectives as Cybersecurity, Artificial Intelligence, Interoperability and Administration Asset Shell, Zero Defect Manufacturing Terms and Definitions, New Market Technologies, and Trends, Industrial IoT and Use Cases, and other.

4.4.2.5 Experience and lessons learned

The key lessons learned have been already transferred in the joint work of the WG 1 of the DMP Cluster (see section 4.2.2., Task 1.3: Common feedback and recommendations). Other recommendations can be found in QU4LITY deliverable D9.6 in respective sections "Recommendations and exploitation of results" included in the analysis of each activity.

4.4.3 ZDMP – Zero Defect Manufacturing Platform

4.4.3.1 Standardization approach

The open ZDMP ecosystem relies on a standardized interface to ensure an open and transparent environment. Building on this foundation, the project has several main goals, whereby standards and standardization play a key role in supporting extensibility, interoperability, and openness. To ensure this, the project has defined three standardization goals: 1) *Interaction*, to engage with the relevant standards groups and standardising bodies for information exchange; 2) *Input*, to actively contribute to the standardisation processes to exploit the project results; and 3) *Compliance*, to monitor the use of standards and standardisation within the project to foster compliant results.

The overall methodological approach of the project can be further defined by several key activities:

- **Horizon Scanning** – First step included the definition of the current standards landscape. This led to horizon scanning activities to identify key standards, standardized tools, and standards bodies and/or committees.
- **Identification of Standards** - Existing standards were then evaluated at the regional, national, European, and international levels. The standards were divided into several categories of relevance to ZDMP: general, zero defect, smart manufacturing, cloud and platforms, and predictive maintenance.
- **Involvement** - It was then necessary to contact the various relevant standardization groups or bodies. This process was facilitated by several project partners who were already members of various consortia involved in standardization.
- **Process Assessment** - Next, it was important to understand the process of participating in the creation or modification of current standards within the standards bodies. For many of the most important standards, it was determined that the primary path was through a European Committee for Standardization (CEN) workshop and the creation of a CEN Workshop Agreement (CWA).
- **Workshops** - CEN workshops were considered the cornerstone for communicating standardization needs and developing standardization proposals, both within the ZDMP project and in collaboration with others. The primary objective of these workshops was to identify potentials in standardization and needs for activities within the project. Initially, a workshop was conducted at the ZDMP project level. As a result of this activity, a series of CEN workshops were planned to discuss specific

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

standardization topics: Terminology, Requirements for Applications, and Guidelines for Data Exchange.

On the readiness of the standardization strategy the experts report that it was operational from the beginning of the project. The focus at the beginning was more on the research activities. Other work included partner evaluation of standards and adaptation to platform requirements. To facilitate work with the pilots, EFPF experts organized workshops to discover standardization potential, network, and conduct activities. Overall, the experts reported that the general plan created at the beginning of the project to meet the needs of the project worked very well.

The work includes periodic reporting for standards and standardisation activities outlined in the following deliverables:

- D4.6a - Standardisation Plan and Status Report The document discusses the main standardization objectives of ZDMP and describes how the defined standardization goals will be reached.
- D057 - Standardisation Plan and Status Report (Informal Pre-Version of D4.6b): This informal M18 interim report gives updated results on the ZDMP standardization plan.
- D2.4 - Manufacturing Reference Model Analysis: This document provides guidance for the identification of relevant standards for project and standardization activities, provides recommendations for the development of platform architecture models consistent with state-of-the-art reference models and standards for digital manufacturing platforms, and thus sets an appropriate framework for the definition of the ZDMP architecture
- Article and Publications: Analysis of relevant standards for industrial systems to support zero defects manufacturing process.(https://doi.org/10.1016/j.jii.2021.100214).

4.4.3.2 Addressing standardization bodies

The ZDMP is one of the few projects where SDO experts were directly involved in the consortium. This had a major impact on the standardization plan and brought a good approach and expertise to the development of the project's standardization activities. In addition, SDO experts brought useful networks and connections to advance their own standardization activities, e.g., in the implementation of CWAs.

ZDMP was a very active contributor to the DMP Cluster work. The experts led the Task 1.4: Joint CWA proposals and guidelines and contributed with their experience to the overall process. It is worth to mention that ZDMP undertook many efforts to drive the pre-phase of the three CWA projects. These activities are also very well described in the deliverables.

In addition, the ZDMP experts brought new methods to the overall approach, namely training activities with the consortium. This was done to help the consortium understand the process of participating in the creation or modification of current standards within the standards bodies. For this reason, the standardization approach and standardization were explained very well to the partners from the beginning.

There have been no direct links to SDOs, NSBs or TCs, but the project has had several collaborations, e.g., DIN, CEN-CENELEC, DMP Cluster, which are explained in detail in the deliverables.

4.4.3.3 Timing of standardization activities

The standardization activities started right at the beginning of the project. They are motivated by the need to provide useful information on standards to the partners.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The committees were selected at the very beginning. Particular attention was paid to those working on ZDM standards. The involvement of the SDO did not influence the technological decisions of the project, but triggered more thinking about standards among the project partners, i.e., the partners were motivated to work on standards.

The ZDMP experts started their work with the CWA through the participating SDO and used its network as well as the joint ideas developed in the DMP Cluster WG 1. In addition, the work of standardization task was also supported by the consortium's network in various standardization activities.

4.4.3.4 Context and focus objectives

The ZDMP aims to create an industrial software platform capable of analysing data from various machines and sensors to actively reduce the number of defective parts or optimize processes. Accordingly, the ZDMP investigated the areas of Zero Defects, Smart Manufacturing, Industrie 4.0, Cloud Platforms, Predictive Maintenance and Platform Services.

As a basis for the standardization work, the ZDMP uses the recommendations of COPRAS and the recommendations currently being developed in the H2020 project HARMONI. Another important source for the ZDMP research was StandICT.eu, which provides a selection of the most important standards in this area.

The deliverable “Standardisation Plan and Status Report” provides detailed information on the focus objectives and lists respective standards from the research in this field. It is also worth to consult the chapter describing standardization tools and standardization process as it includes very valuable information for “beginners”.

4.4.3.5 Experience and lessons learned

In the individual workshops with ConnectedFactories2, the experts emphasized that the most unexpected part was finding common ground for the CWA work. This required more work than originally expected. Although there was a lot of collaboration between the projects, the experts had difficulty bringing the different ideas together.

Another difficulty arose during the analysis phase. The broad standardization landscape led to challenges because there were too many standards to analyse.

It is, for example, beneficial to gain the participation of experts who are members of standardisation committees, as they provide access to their networks, increase the quality of the documents, and increase the chance of the CWAs to be integrated into standards.

Although the work with the consortium partners and pilots was strongly supported by the workshops and trainings, it was still difficult to track how the standards were implemented at the end. The experts recommend that more effort be put in at the end of the project to reserve time for follow-up.

4.4.4 KYKLOS4.0 – An advanced circular and agile manufacturing Ecosystem based on rapid reconfigurable manufacturing process and individualized consumer preferences.

This subchapter summarizes the key mapping results regarding KYKLOS 4.0 project.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

4.4.4.1 Standardization approach

KYKLOS 4.0 is developing an Advanced Circular and Agile Manufacturing Ecosystem based on rapid configurable manufacturing processes and individualized consumer preferences. Regarding the role of standards in KYKLOS 4.0 in relation to the project scope, the task experts involve external stakeholders' perspectives on standards; focus on each partner's standards needs to achieve the project vision; engage work on specific standards of recognized importance, build interactions with organizations developing standards and conduct dissemination activities focused on the use of standards.

KYKLOS 4.0 bases its standardization strategy on several results of the three main activities:

- Standards identification and analysis,
- Collaboration with standardization committees, and
- Contributions to standards.

In the form of a list of standards with high relevance to the project goals, KYKLOS 4.0 experts create recommendations. The standards are then grouped into technology categories for better usability. The experts then create user guides in the form of short best-practice documents for standards with high relevance for which there is good expertise in the project. For standards with high relevance, improvement and extension proposals addressed to the relevant standardization bodies, the experts plan to provide active feedback as part of the project's standardization activities. To disseminate the results and share success stories related to the application of specific standards by the project, the experts are planning events and presentations. These will be aimed not only at the community of standards developers, but also at a wider audience.

The related standardization activities are described in the Following deliverables are of interest in connection to standardization work:

- D12.7 Analysis of Standardization Context as the first of two reports on the KYKLOS 4.0 standards context, it presents project activities; recommendations for partners on standards; SDOs, organizations, and initiatives that identify standards relevant to industry or gaps in standardization; the results of an internal project survey on standards use and needs; standards already identified as of high interest; project partner contributions to SDOs; and dissemination activities of standards use in the project.
- During task T12.5, “Standardization Activities”, KYKLOS 4.0 identified common needs with Task T5.3, “Interoperability Requirements for Compliance to International Standards”.
- A related paper and presentation were given to the NAFEMS World Congress in 2021. The Standard Based Digital Twin - making the foundation for smarter manufacturing and creating better products, CIRTES/France (M. Prado-Motta, C. Abel, Dr. C. Pelaingre) and Jotne/Norway (Dr. R. Lanza, H. Galtung, M. Chaure), NAFEMS World Congress 2021, 2021-10-27

4.4.4.2 Addressing standardization bodies

KYKLOS 4.0 experts are very well networked within related standardization committees and use own consortium network to address standardization bodies. In its strategy regarding the collaboration with standardisation bodies, the project focuses on SME needs concerning standards through “Small Business Standards” (SBS).

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

KYKLOS 4.0 wants to facilitate the acceptance and utilization of the developed solutions by the market in alignment with standardization. On the one hand, the project aims to ensure capability and interoperability with existing solutions on the market through standards. On the other hand, it wants to use the "standardization system" as a powerful tool to disseminate the project results and start interaction with the market stakeholders. Following considerations regarding standardization activities were provided to CF2 by the KYKLOS 4.0 experts:

- Through using international standard formats for the data storage, the PLM Module will be key to KYKLOS 4.0 enabling consumer products manufacturers to integrate products and components that have been independently designed, produced and used, in addition to the manufacturing system itself.
- Using ISO 10303 standards for data exchange, sharing and archiving the PLM module will provide a central repository for all applications in the project, at the same time allowing any legacy system to be connected in commercialization's of the project results.
- Further, the project will significantly contribute to the standardization efforts in Industrial Data systems taking place in ISO TC 184/SC4 and its counterparts in CEN/CENELEC to work as a transfer channel of new industrial participation opportunities.
- At the same time, the standards will promote innovations, ensure quality of products, enhanced visibility, increase safety and environmental protections

4.4.4.3 Timing of standardization activities

The standardization activities started from the very beginning of the project. The project showed also great engagement in the DMP Cluster WG1 work. To the time of this deliverable the projects' activities have proceeded from the early stage to operational mode.

4.4.4.4 Context and focus objectives

KYKLOS 4.0 investigates relevant standards for smart manufacturing, digital twin, and circular economy. Here, KYKLOS 4.0 conducted an extensive internal survey with the goal of creating best practice guides for the critical standards. The standards research includes information from the external sources as well collects experience support by internal partners from pilot owners and technology providers.

Based on the project goals KYKLOS 4.0 aims to provide a set of product-service simulation models. The main interest of KYKLOS 4.0 is, therefore, related to the work of ISO TC 184/SC, especially ISO 10303 standard for Industrial Data. In particular, the following aspects are of great interest: a) Product specifications, standards, and regulatory compliance; b) Product design & materials, the suppliers, the manufacturing strategy (produce to order or make to stock), the product usage (profiles of customers), and the product servitisation (type of maintenance services proposed), and eventually product recycling/reuse and c) Security requirements.

Within the focus objectives, KYKLOS 4.0 also explores generally applicable standards that support the KYKLOS 4.0 platform. These concern, for example, reference architectures, the Internet of Things, hardware interfaces, low-level network protocols including cloud communication, data interoperability (low-level), data archiving, cybersecurity including blockchain, data quality, sensors, Big Data, artificial intelligence, and machine learning, and, last but not least, the specific aspects of circular manufacturing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The project experts identify EFFRA portal mapping matrix as "the most comprehensive overview of standards relevant to KYKLOS 4.0" needs. The mapping list of KYKLOS 4.0 standards have been transferred to EFFRA portal and can be found for example, here: https://portal.effra.eu/project/1943/taxonomy-list-taxon/814 (see Figure 34).

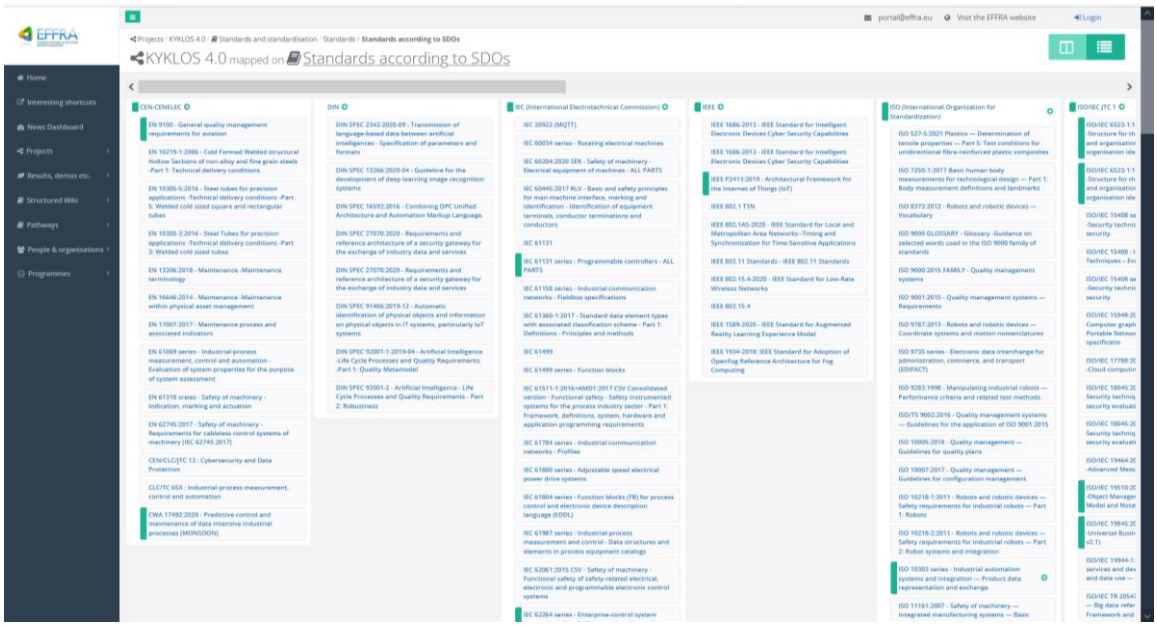


Figure 34: EFFRA page with information on the use of standards by KYKLOS 4.0

4.4.4.5 Experience and lessons learned

Currently the project is still collecting the first lessons learned.

Regarding the survey on standards, the experts emphasize that most of the identified standards are complementary and can generate synergy effects when integrated. However, particularly in data exchange, the various standards propose different solutions.

The project also applied internal trainings. Thus, a training was provided to project partners for the use of ISO 10303. A TV-streamed webinar presented project experiences of using ISO 10303 in KYKLOS 4.0 to a wide (300 attendees) and global audience.

4.4.5 DIGIPRIME – Digital Platform for Circular Economy in Cross Sectorial Sustainable Value networks.

4.4.5.1 Standardization approach

The standardization approach of the project involves is briefly outlined in Figure 35. It concerns review and alignment to standards and policies in three different strands: a) Industrial Standards, including standards linked to digital industry; b) Circular Economy Standards; and c) Sector Specific Standards (e.g., related to the Energy/Batteries sector).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

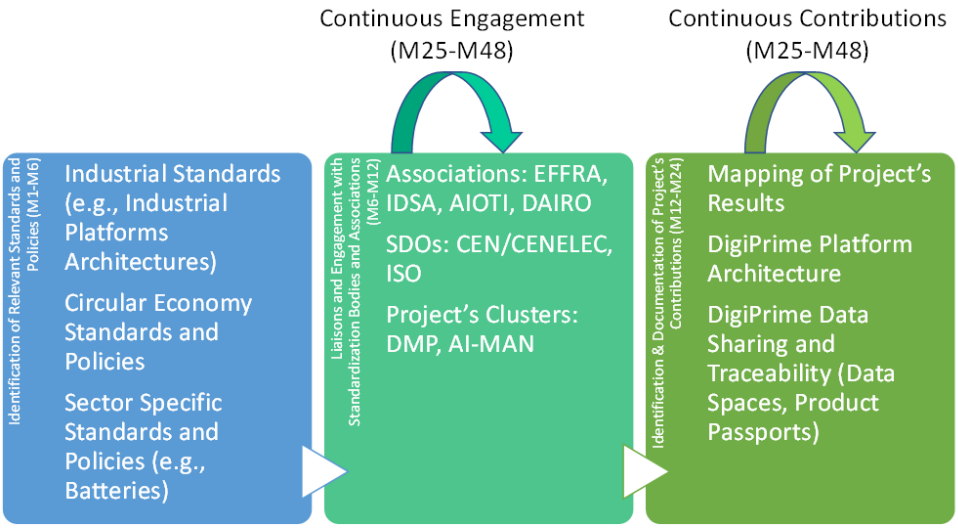


Figure 35: DIGIPRIME - The standardization roadmap

The project experts view standards as critical to ensure the success of the project's exploitation and/or market strategy. Standardization is important for the exploitation and market acceptance of the outcome and provides DIGIPRIME with the opportunity to engage in emerging standardization efforts and policy/regulatory developments (such as the EU Battery Regulation).

In its standard search the project applied a bottom-up not top-down approach. Regarding the internal process, the expert team relied mainly on the brought/earlier experiences, while the deliverables were based on the current standards.

There is no SDO or SNB involved in the project consortium. The technical partners of the project have contributed to the alignment of the project's architecture to different standards based on their experience with the use of digital and industrial standards.

Specific deliverables within standardization activities were addressed in a dedicated task:

- D9.5: Standardization plan and results. The deliverable reports on the project's standardization activities during the first two years of the DIGIPRIME lifetime. It also provides an outlook and a plan for future activities.

4.4.5.2 Addressing standardization bodies

It is noteworthy that DIGIPRIME has established liaisons and collaborations with associations, clusters and SDOs since the first semester of the project's lifetime, even though the standardization task of the DIGIPRIME work plan was scheduled for later in time.

The project's review and alignment to different standards, as well as its contributions are based on liaisons with associations (e.g., European Batteries Association), SDO's and clusters of EU projects (like the DMP cluster).

The project has not established liaisons up to the current stage, but it has contributed its proposal to the EC Public Consultation on the EU Battery Regulation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

4.4.5.3 Timing of standardization activities

Standardisation activities were divided into three phases and started at the beginning of the project. More details can be seen in the figure above of the previous subsection.

4.4.5.4 Context and focus objectives

DIGIPRIME is an interdisciplinary project that develops and validates a digital platform for the Circular Economy, with emphasis on the management of the circular chain, including cross-sector interactions. It identifies standards and standardization activities of major importance for the project. The project's standardization approach is also interdisciplinary and aims at covering standards and policies in multiple areas including various standards and regulations as e.g., EU Batteries Regulation; various Data Modelling Standards (e.g., ISO/IEC 19845:2015, OASIS Universal Business Language (UBL)); various Industrial Architectures Standards (e.g., Industrial Internet Reference Architecture (IIRA)). The project used open-source standards such as REST API and Swagger; part of the architecture also relies on such standards.

The project investigates on:

- **Standards relating to the project's Digital platform**: The project adopts standards-based approaches for the development of its Digital platform. Specifically, standards associated with Industrial Internet of Things (IIoT) applications (e.g., the Industrial Internet Reference Architecture, RAMI 4.0) are considered, in conjunction with standards and guidelines for the development of data spaces (e.g., design guidelines from the Industrial Data Spaces Associations (IDSA)). Most of these standards focus on the architectural aspects of the platform. Nevertheless, the project also develops and use standards-based components such as Lifecycle Assessment components based on MIMOSA standards and ISO55000 standards for asset management. Likewise, the data models of the platform adhere to standards and related guidelines (e.g., of the Industrial Ontology Foundry (IOF)).
- **Standards relating to the project's Circular Economy aspects**: The applications, services and pilots that are developed and deployed over the platform adhere to circular economy standards and guidelines, such as guidelines from the European Batteries Alliance (EBA) regarding the Recycling of batteries, composite standards for the certification of recovered materials, as well as materials efficiency aspects (e.g., IEC TC21 on Secondary cells and batteries, IEC TC69 on Electric Road Vehicles).
- **Regional/National Level Policy Making**: DIGIPRIME has an active role in circular policy making at regional level based on the consortium's liaisons with regional clusters and Digital Innovation Hub (DIH). The project will provide relevant policy making guidelines for the circular economy, while developing a tool for supporting policy makers in identifying and resolving legal barriers to circular innovation at regional level.

Meanwhile, the project experts have provided detailed and concrete input to the EU Batteries Regulation consultation, reflecting DIGIPRIME approach to batteries circularity and including a Digital Product Passport (DPP) outlook.

4.4.5.5 Experience and lessons learned

The project experts reported on the main difficulties and obstacles encountered so far.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

In terms of resources, the lack of adequate resources for standardization could be identified. The DIGIPRIME GA and work plan includes a task to align with standards but does not provide for active participation in standardization organizations and working groups.

Since there is no SDO in the consortium, the experts believe that this fact makes the links to standardization working groups more time consuming and labour intensive. Standardization is performed by organizations whose main activity is not standards development.

Regarding the alignment of standardization schedules and activities, experts emphasize that these may not always match project deadlines and deliverables. For example, the project's policy proposals on batteries had to be submitted at an early stage, before the initial implementation of the battery pilot project.

4.4.6 SHOP4CF – Smart Human Oriented Platform for Connected Factories

This subchapter summarizes the key mapping results regarding SHOP4CF project.

4.4.6.1 Standardization approach

The project's activities in standardization are dedicated in a separate task. This task focuses on the issues regarding pre-regulatory aspects of human-robot collaboration.

The standardization approach foresees several activities. These include the identification of all relevant stakeholders and the accompanying use-cases. In the next step, the project cross-references the goals with current standards to identify gaps. The best practice guidelines are to be delivered at the end. These include then the experimental data gathered by the user-experience experts in the project, as well as according to the current standardization and regulatory situation.

Based on the approach, the project prepares a document in which it clearly defines rules of engagement for different situations where humans come in contact with collaborative robots, specifically including adults in industrial settings, as well as children or the general public in industrial, civil (e.g., on the street) and domestic (e.g., in the home) settings. These rules of engagement include both expected robot behaviours as well as specific instances of how humans can intervene in normal robot operation (e.g., cause the robot to slow down, re-plan and change its trajectory, stop the robot, or have the robot initiate communication with the human with the goal of reducing any unintended process interruptions.

In is standardization plan, the project gives a detailed description of the activities taken to get SMEs involved in the standardization process, such as polling, training/information workshops and any feedback collected from SMEs that is intended to influence standardization bodies. It also includes description of the activities taken by the consortium to contribute to standardization processes, including any best-practice publications and or suggestions regarding current gaps in standardization and safety regulations.

The projects' activities in standardization are coordinated in the SHOP4CF T7.1 pre-regulatory aspects of human-robot collaboration within work package 7, Standardization, legal and ethical aspects. The work includes periodical reporting, i.e.:

- Deliverable D7.1: Contributions to standardization bodies: This is a public report about all activities within the project which contribute to standards.
- D3. 3 SHOP4CF Architecture 2: This document presents the SHOP4CF framework architecture that aims at ensuring coherence and interoperability of the SHOP4CF software components under

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

development. Interoperability of the components is addressed with logical views on the platform and data aspects that together facilitate and standardize communication among the components. Separately, interoperability of the architecture with existing standards is discussed.

4.4.6.2 Addressing standardization bodies

The project is active in clustering activities and has liaison with the DMP Cluster to also participate in standardization activities initiated through that organization and that match with SHOP4CF project profile. Currently this involves active contributions to the WG 1 Standardization in the DMP Cluster, as well as concrete participation in the CEN-CWA proposal on the topic "Digital Manufacturing Platform – Marketplace requirements".

Regarding the contribution to digital twin standards the experts used opportunities to contact Industrial Digital Twin Association IDTA[29]. Moreover, the experts submitted a proposal for the development of the Asset Administration Shell sub models within the cooperation of IDTA and InterOpera project.

4.4.6.3 Timing of standardization activities

Standardization activities started at the beginning of the project.

4.4.6.4 Context and focus objectives

Several activities have been reported in the meantime.

Among these is ADRA (AI, Data and Robotics Association, asbl), which was founded in 2021 by joint forces of BDVA, CLAIRE, ELLIS, EurAI and euRobotics. This joint work integrates a wide range of stakeholders into the activities of the Partnership. The recent focus of on validation activities was the main focus in Open Standards Forum with EC.

Digital twin and related standards is one of the central standardization objectives in the project. Thus, the experts attended in 2021 four respective sessions in open workshop sponsored by ISO/IEC JTC 1/SC 41 /AG27/N42 "Digital Twin workshop report JTC 1/SC 41/AG27" that were conducted in the following time: 2021-09-16, 2021-09-21, 2021-09-23, 2021-09-28. The key input of the project in the standardization of digital twins focuses on robotics. To do so, respective use-cases and discussions with technology providers have been started in the project as well as collection of digital twin requirements have been addressed by the task.

One of the next objectives in standardization activities is the collection of needs through FSTP projects. Here experts plan several activities in the next period in 2022. This includes not only the analysis, but also the transfer of the collected results to standardization committees.

In this term, the project will continue work on validation through TC 299, WG8 "Validation of collaborative applications" and will begin its work on recommendations for design of collaborative workspaces (analog Safety traffic rules).

Another important standardization focus lies on standardization of marketplaces. Here the experts report on some open questions regarding FIWARE and RAMP. RAMP - Robotics and Automation MarketPlace -

[29] https://industrialdigitaltwin.org/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

functions as a marketplace bringing together suppliers and Manufacturing SMEs and offers digital infrastructure and services for robotics and automation on top of FIWARE.

4.4.6.5 Experience and lessons learned

So far SHOP4CF collected only few experiences in standardization. Nevertheless, the project identifies standards and standardization as of major importance in the project.

The current user experiences from the pilots show that e.g., the data model and also the interfaces (REST, OPC UA) that were integrated were very helpful and easy to use in the project.

Open standards like ROS, FIWARE, IDSA and their integration brought helpful experiences and will allow pilots to integrate more components in the future.

Some pilots report very good experiences with the use of ISA-95 and emphasize that the use of a set of standards can also prevent limitations.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

5 Interoperability

The following Chapter is reporting on the task defining the best practices in interoperability,

- and **looking for new forms of cooperation amongst companies and sectors,**
- addressing **enhanced transparency** across manufacturing cells, production lines, factories and even between different manufacturing companies
- suggesting **actions to address the cooperation** challenges.

Interoperability amongst manufacturing companies relies on several aspects that will be analysed. These include: material, resources and product **traceability** as well as questions and improvements related to **quality control or logistic improvements**. And **technical constraints on** Transparency and interoperability. Leaving legal and business models aspects to be analysed in T1.1 or T.1.2 (and reported in Chapters 2 and 3 of this D1.4).

This task is closely related with the Hyperconnected Factories pathway (developed under ConnectedFactories 1) but also with Lot-size-1 and sustainable-value-networks in the current and future ICT 07 projects.

To address all this interoperability views, it is necessary to define a taxonomy that permits clustering of the different aspects.

5.1 General observations on interoperability

Europe has a good position and could win the "second half" of the digital match against global competitors (Commissioner Oettinger, 2015). In these considerations the important role of platforms and B2B-platforms are receiving more attention among policy makers and businesses (1). A first wave of commercial platforms is launched to the market (e.g., GE Predix, Siemens Mindsphere). **Commission and member states are investing in** developments of platforms and **interoperability.**

Vision of the Plattform I4.0: Interoperability is a huge thing in Germany this year. The key word here would be "Ecosystems", especially to the new for Industrie 4.0 till 2030 (Figure 36.

Figure 36: 2030 vision for I4.0 (Source: Plattform 4.0)

On the 5th and 6th February 2018, before this CF2 CSA, EFFRA hosted a dissemination event on digital platforms in manufacturing in association with the ConnectedFactories Coordination and Support Action. A

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

specific session addressed standardisation and interoperability aspects of the FoF 2016-11 projects (this call topic is associated with that ConnectedFactories CSA). More information and presentations from the respective sessions can be downloaded here: https://www.connectedfactories.eu/events/5-6-february-2018-connectedfactories-dissemination-event.

In the following sections, we have analysed different projects according to RAMI and IIRA concluding they would be a complementary way to define and map initiatives.

5.1.1 INTEROPERABILITY at RAMI 4.0 Vertical layers

INTEROPERABILITY can be defined in many ways and from many perspectives:

- Interoperability is create a knowledge representation of an agent/asset in modular production.
- Interoperability is the seamless movement of data along different levels of knowledge.

Looking for a new way to define interoperability, it is important to look at the RAMI 4.0[30] in first place (Figure 37):

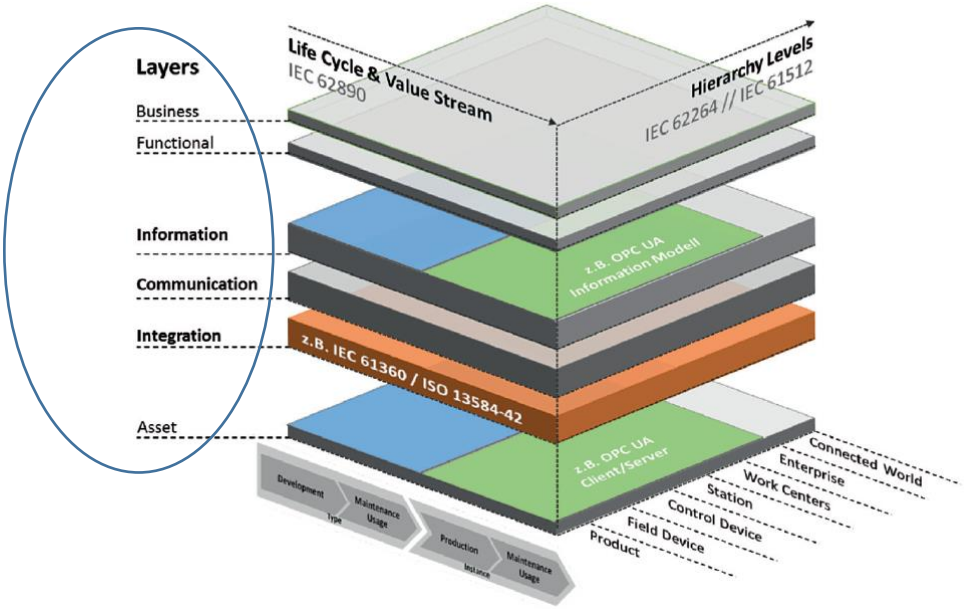


Figure 37: Interoperability layers in RAMI 4.0

RAMI 4.0 provides 6 vertical layers

- Business
- Functional
- Information
- Communication
- Integration

[30] Reference architecture model industry 4.0 (RAMI 4.0)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- Asset

However, **there are many ways to look at the interoperability, so the following appoach tries to link them with RAMI 4.0 and use its architecture from now on.**

The first exaple shows how to describe each of RAMI 4.0 vertical layers with the help of MIDIH (Figure 38).

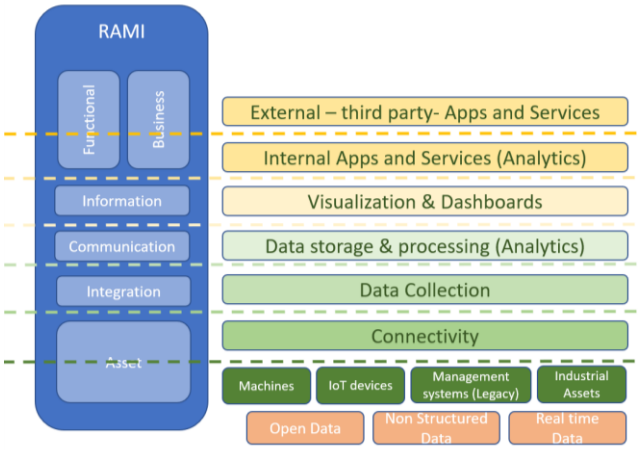


Figure 38: Interoperability comparison: MIDIH and RAMI 4.0

MIDIH RA provides similar RA with Functional layers and capabilities. In this case, the data sources (ASSETS in RAMI 4.0) are IOT devices, machines, legacy systems, industrial assets.. Other aspects to take into account are:

- open data;
- real time data;
- non structured data (streaming).

The MIDIH approach is shown in Figure 39.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

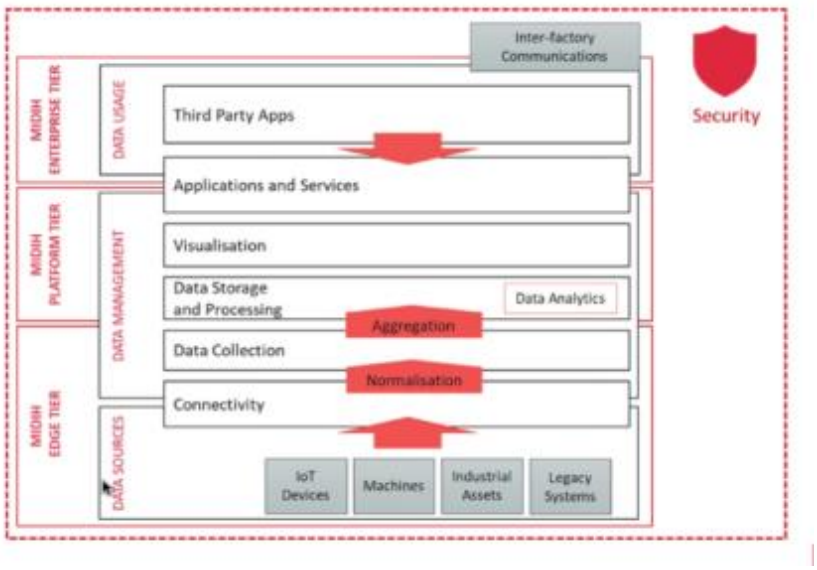


Figure 39: MIDH approach

But there are other ways to address interoperability, for example, through distinguishing three aspects:

1. DATA GENERATION: Data is generated on an ASSET, and INTEGRATED filtering the data (usually on the EDGE).
2. DATA MANAGEMENT: Then it is COMMUNICATED through the INFORMATION layers, transforming in structured data. This is usually the FOG at PLATFORM level.
3. DATA USAGE: And then is analyzed either for improving FUNCTIONAL aspects (performance, quality, productivity….) or BUSINESS aspects. This is the CLOUD. See the picture below:

In the following Figure 40, this different approach and RAMI 4.0 are mapped.

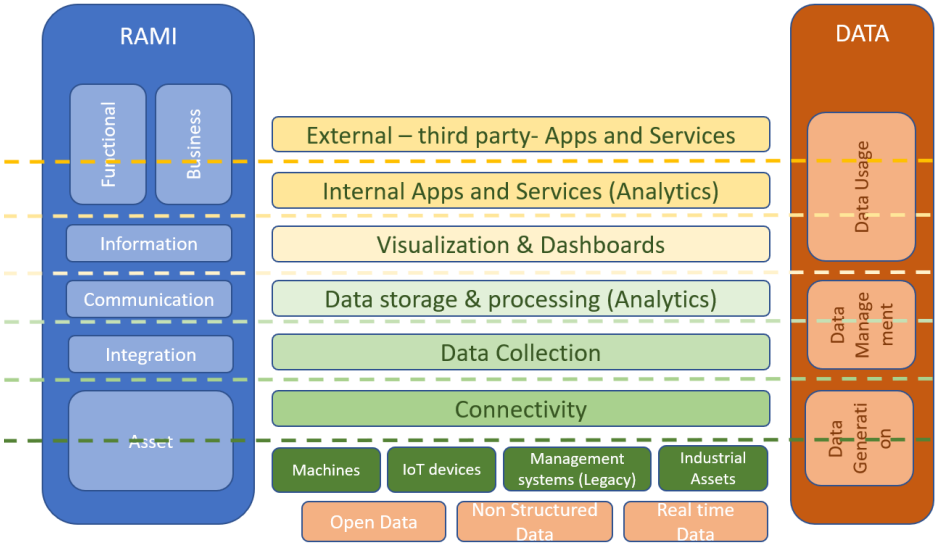


Figure 40: Data mapped in RAMI 4.0

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

In MIDIH, data sources along with connectivity, normalization, data collection and aggregation are made at EDGE level. It is also called DATA IN MOTION. Data storage and processing (analytics) are made at PLATFORM level (FOG). Also called DATA AT REST. While applications, services and third party apps are at enterprise level. See Figure 41 below.

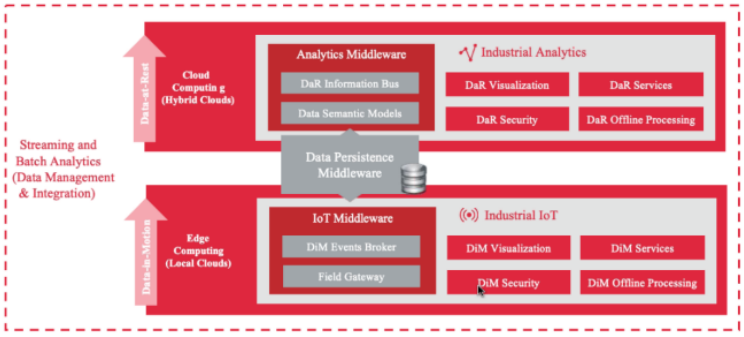


Figure 41: MIDIH data approach

The following shows the mapping results of both approaches (Figure 42):

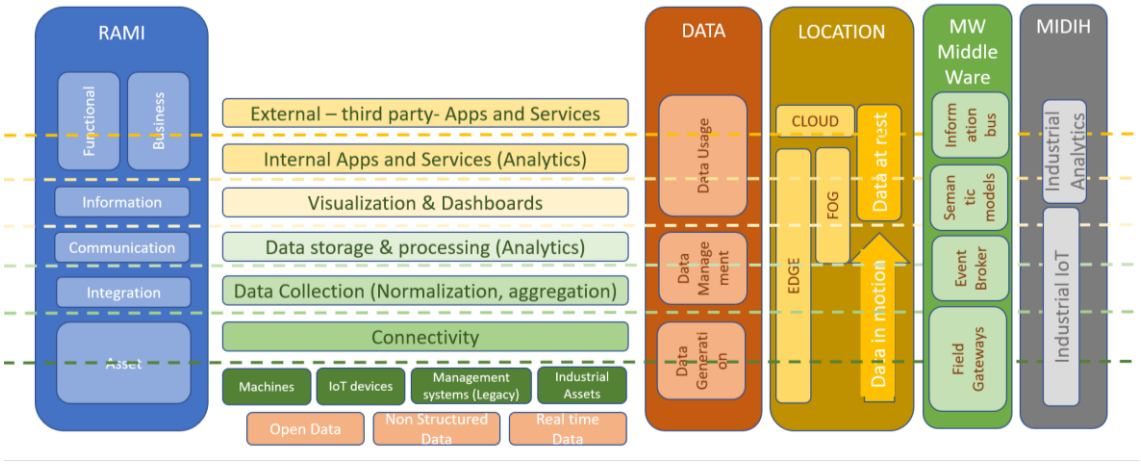


Figure 42: MIDIH data approach mapped in RAMI 4.0

At last, another way to look at interoperability (DIMOFAC, AAS, and EIF – see Figure 43) is:

- Technical interoperability: ability to exchange data (ISO/OSI);
- Syntactic interoperability: Description of the data with all its type attributes in uniform formats (OPC UA);
- Semantic interoperability: ability to interpret the exchanged data in such a way that intended actions can be recognized and triggered;
- Organizational interoperability: ability to act in non-technical processes.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

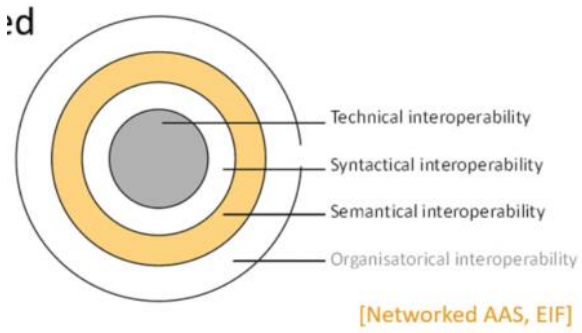


Figure 43: AAS approach to interoperability

After mapping of this definition into the RAMI 4.0, the following result is displayed (Figure 44):

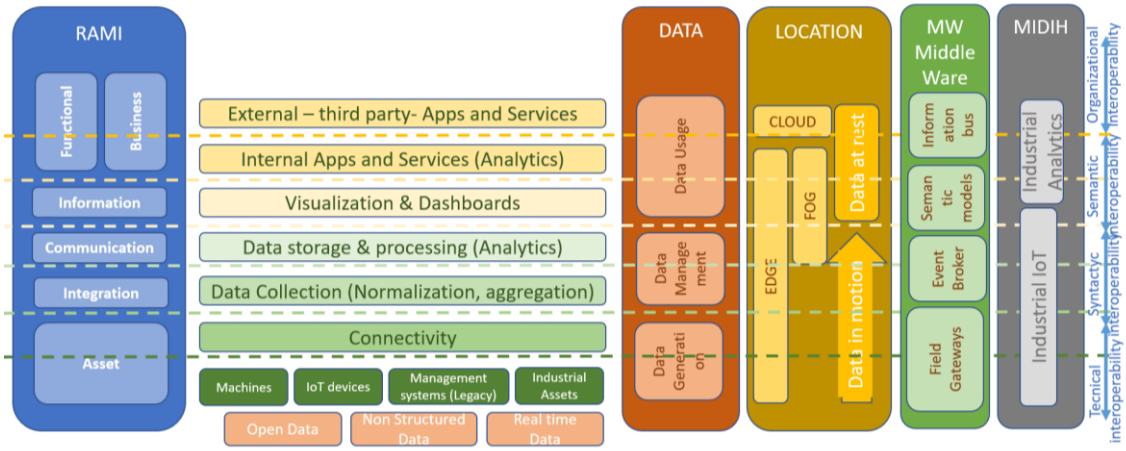


Figure 44: AAS approach mapped in RAMI 4.0

As a preliminary conclusion of this chapter, we could say that RAMI permits the mapping of the different interoperability approaches of different projects and initiatives.

5.1.2 Interoperability at RAMI 4.0 Horizontal Hierarchy levels

It is also possible to look at INTEROPERABILITY from the Horizontal perspective of RAMI 4.0 (Figure 45). In this way, it is possible to address not only a vertical flow, but also interconnecting with other devices, controls, stations, enterprise.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

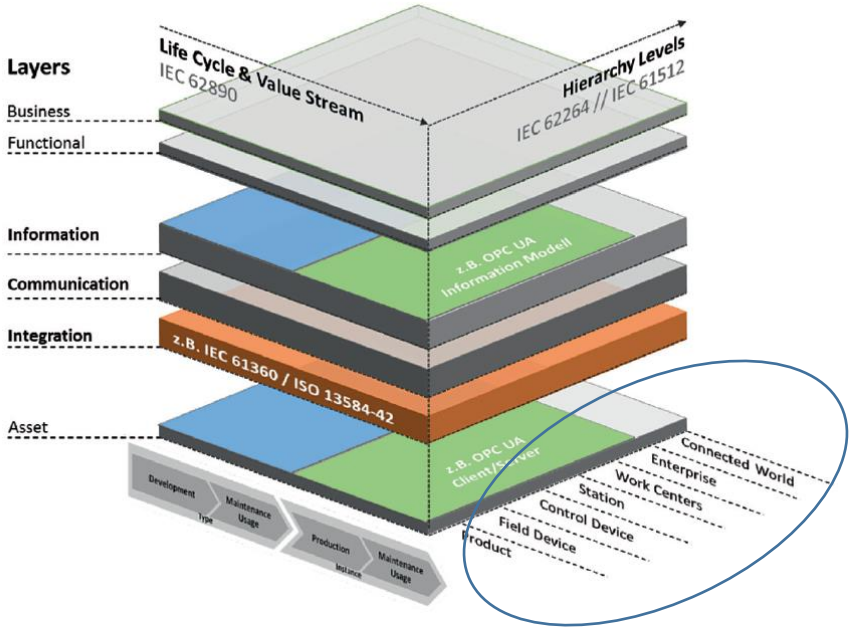


Figure 45: RAMI 4.0 horizontal layers - Hierarchy levels in RAMI 4.0

1. **Product:** Interoperability amongst products at use phase. RAMI 4.0 is much focused on the manufacturing than on use. Industrial products (where RAMI 4.0 applies) appear in multiple industries (where IIRA applies) so they must interoperate.
2. **Field device**: Interoperability amongst field devices (sensors, actuators…)
3. **Control device**: Interoperability amongst control devices (PLCs, PCs, AI based control tools…)
4. **Station**: Interoperability amongst stations (production cells, robots and machines, machines and humans…)
5. **Work centre**: Interoperability amongst work centres (production lines within a factory, departments within a plant…)
6. **Enterprise**: Interoperability amongst enterprises (different factories of a company)
7. **Connected world**: Interoperability amongst field devices (different companies, companies of the supply chain, customers-suppliers…)

In the following Figure 46 a sketch of the different levels is presented:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

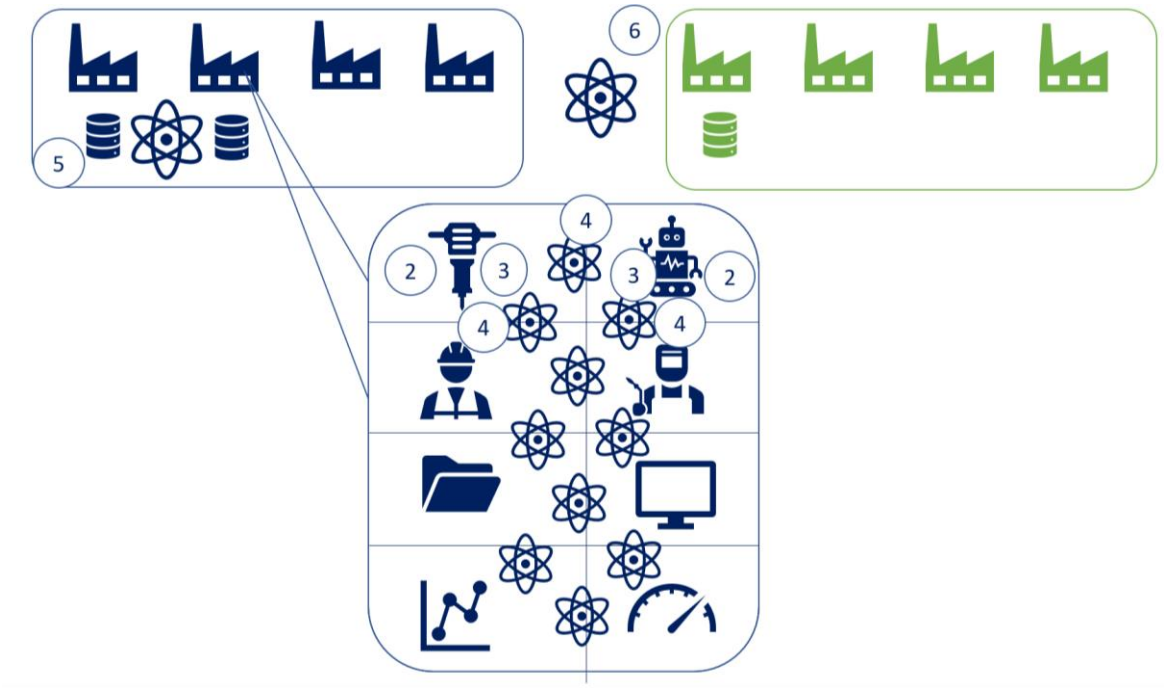


Figure 46: Sketch of different levels

The following Figure 47 highlights the relation amongst companies according to the vertical layer of RAMI. Exchanging data not only at high level (enterprise) but also amongst their machines, stations.

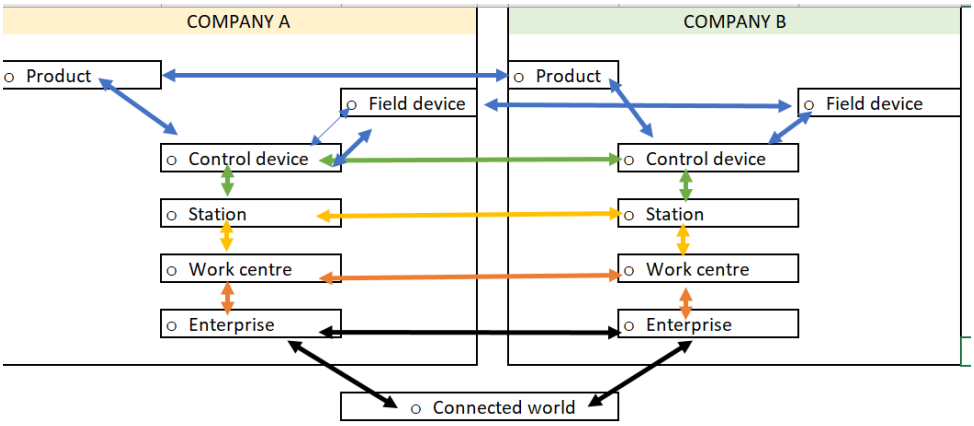


Figure 47: Horizontal interoperability

This interoperability concept was already addressed in the HYPERCONNECTED FACTORY pathway.

5.1.3 Interoperability in IIRA: Layered databus and architectural pattern

Industrial Internet consortium provides a similar reference architecture (IIRA) based on a data driven approach. The mapping of IIRA and RAMI 4.0 shows the following results Figure 48

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

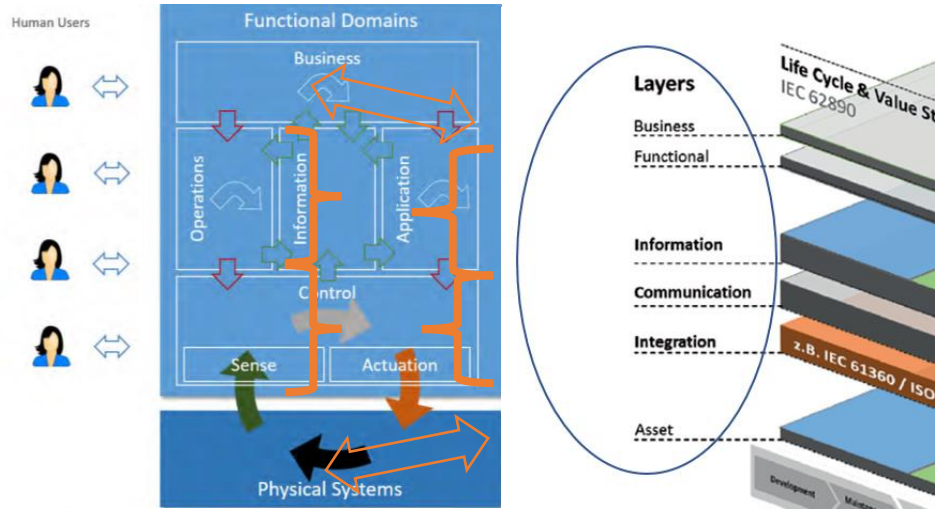


Figure 48: IIRA-RAMI 4.0 relationship

The three tier mapping defined by IIC, can also easily match it with RAMI 4.0 and the previous sketch (Figure 49)

Figure 49: Three Tier IIoT system architecture

The rotation of the image allows its fitting in the previous sketch (Figure 50**Fout! Verwijzingsbron niet gevonden.**):

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

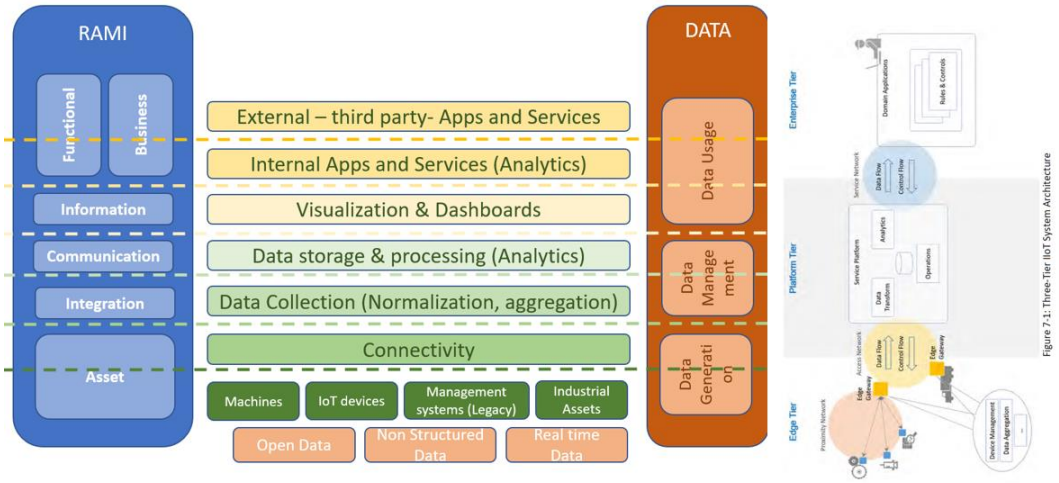


Figure 50: RAMI 4.0 and the the 3Tier IIoT

Furthermore, it allows its matching even clearer in the **Fout! Verwijzingsbron niet gevonden.** Figure 51 and matching it with the sketch as shown in Figure 52

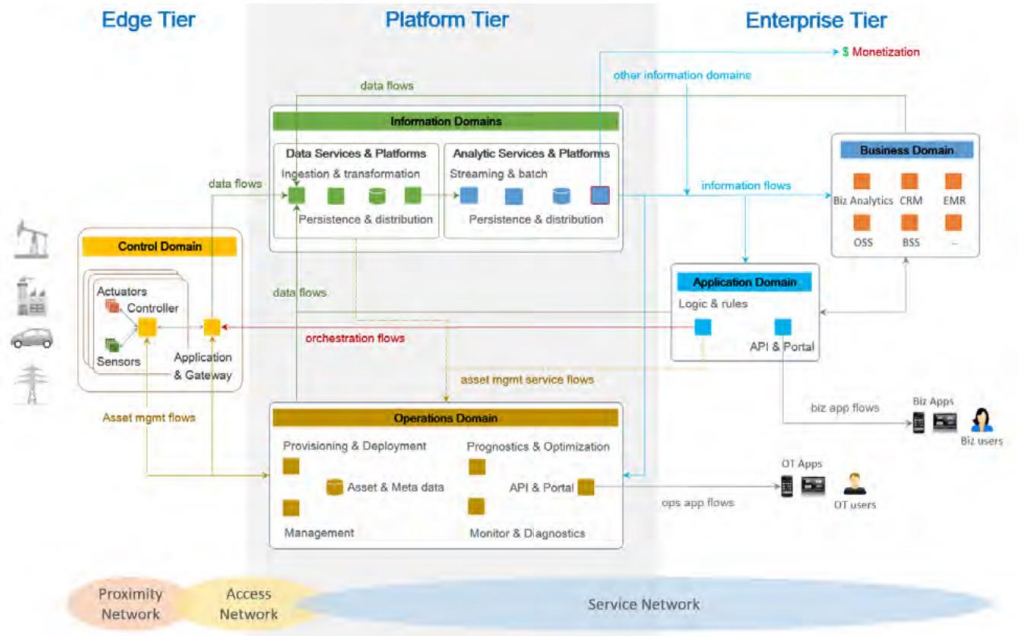


Figure 51: Three-tier architecture and the functional domain mapping.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

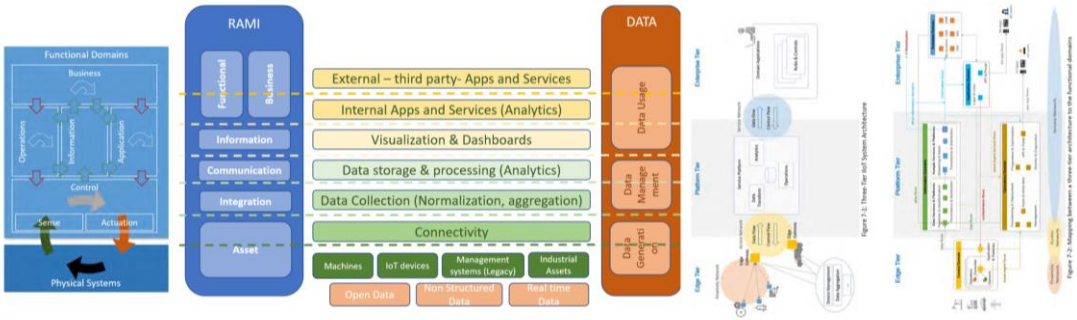


Figure 52: IIRA mapping

Continuing the evaluation of IIC RA, a layered databus architecture could be analysed (Figure 53). The lower level (smart machines) is the real world: sensors, actuators, objects, devices machines. It could even be a CPPS (e.g. a car, a robot).

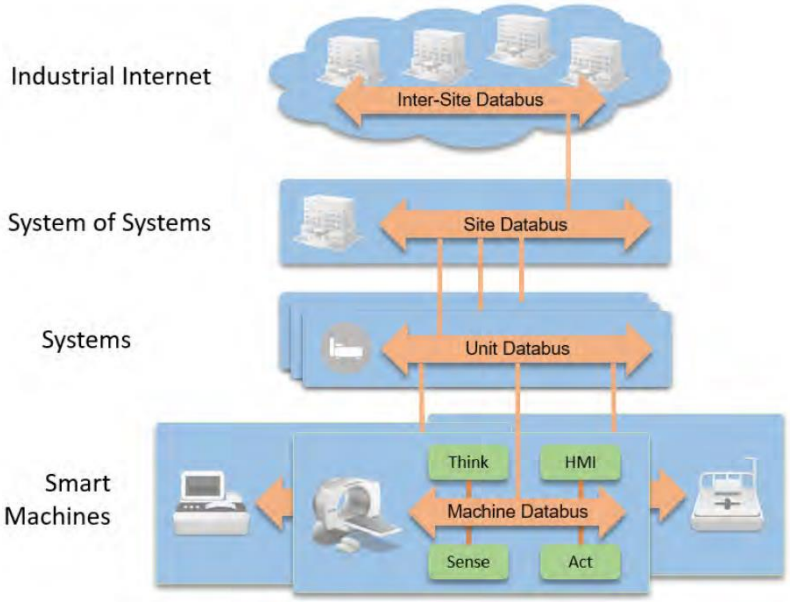


Figure 53 IIRA layered databus architecture

This architecture matches with the hierarchy layer in RAMI 4.0, as it is shown in the Figure 54 below.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

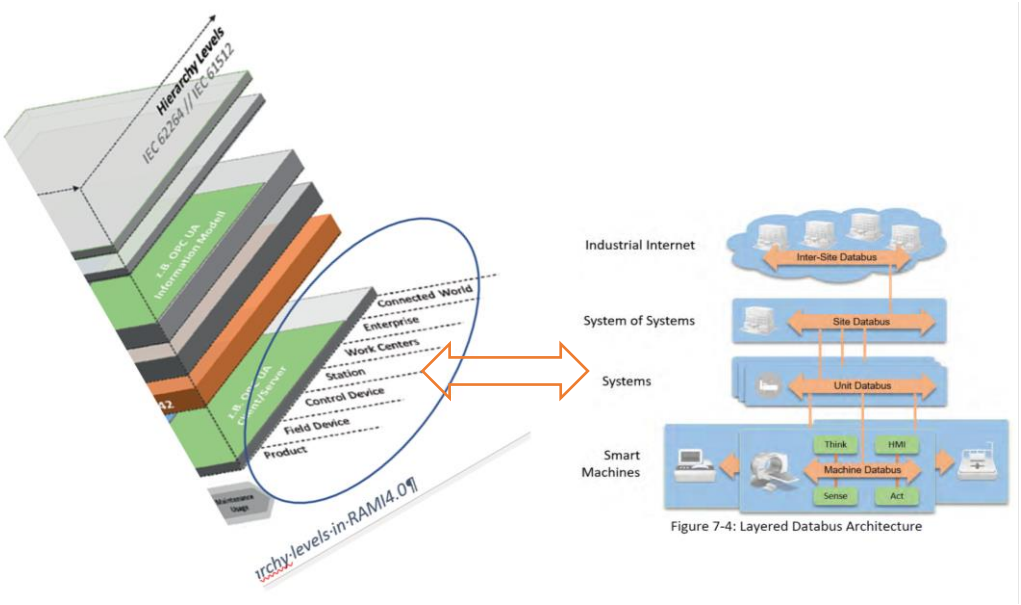


Figure 54: Mapping IIRA layered databus architecture in the RAMI 4.0 hierarchical layer

5.1.4 Interoperability approaches and goals mapped on RAMI 4.0

There are several **approaches to the interoperability topic** that need to be addressed when implementing interoperability:

1. **Proprietary approach:** Decision of Interoperation of different commercial tools and platforms (against data protectionism). From a more technical point of view, **interoperability** is extremely relevant. This is not only since systems and tools will very likely come from **different vendors**, but also since many **legacy systems** have to be integrated.
2. **International approach:** Data exchange amongst borders.
3. **Sector approach**: Cross-sectorial reference architectures.
4. **Data resiliency approach:** to guarantee the integrity of common repositories. (Blockchain technology).
5. **Integration approach: A**mongst levels on the plant: Edge, fog, cloud.
6. **Semantic/information approach**: Modelling correlation between information sources. Like Open ontologies. Or AAS Asset administration shell.
7. **Data sovereignty approach:** to guarantee the trust amongst participants on data transactions (Industrial Data Space Association).
8. **Digital Twin & Digital Factory:** exchanging data between real and virtual assets?
9. **R**eal time communication.

The approached can be matched in the Horizontal layer of RAMI 4.0 as depicted in Table 5.

RAMI 4.0 vertical layer / **Interoperability approach**	**Asset**	**Integration**	**Communication**	**Information**	**Functional**	**Business**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Proprietary					x	x
International					x	x
Data resiliency				x		
Sector approach					x	x
Integration		x	x			
Semantic				x		
Data sovereignity				x	x	x
Digital twin			x	x	x	
Real time comm	x	x	x			

Table 4: Interoperability approaches

At the same time, interoperability can be implemented considering different company goals (see Table 5):

1. **Quality goals:** improvements on quality control.
2. **Productivity goals:** improvements on productivity control.
3. **Maintenance goals**: improvements on maintenance control.
4. **Traceability goals** for material, resources and products.
5. **Production visibility goal:** M2M & HMI in factory environment: evaluation of human machine interfacing HMI.
6. **Cooperation approach** new forms of cooperation amongst companies and sectors either at supply chain or value chain.
7. **Logistic approach:** improvements on logistics control.

RAMI 4.0 horizontal layer / **Interoperability Goals**	**Product**	**Field device**	**Control Devide**	**Station**	**Work Centre**	**Enterprise**	**Connected World**
Quality		x	x	x			
Productivity				x	x	x	
Maintenance			x	x	x	x	
Traceability			x	x	x	x	x
Production visibility				x	x	x	
Cooperation (supply side)						x	x
Cooperation (value side)						x	x
Logistics						x	x

Table 5: Interoperability goals

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

5.1.5 Interoperability requirements

Several requirements need to be taken into account when addressing interoperability, as e.g.:

- Safety when addressing the interoperability amongst human and machines/ robots.
- Privacy when addressing interoperability amongst different companies.
- Reliability when data are required for very accurate decisions (i.e. at machine level).

Some of these requirements are already mapped in the IIRA, calling them “system characteristics” (Figure 55).

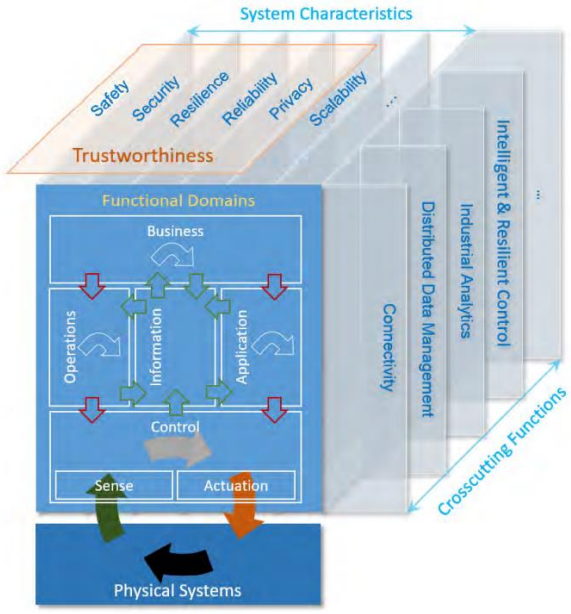


Figure 55: IIRA system characteristics

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

5.2 Reference documents on interoperability.

The following Table 6 shows the main reference documents on interoperability. The list is not exhaustive but highlights only some current work in the area.

Document title	Short description	Link
Progress report 2019. Shaping Industrie 4.0. Autonomous, interoperable and sustainable.	Publication of the Plattform Industrie 4.0: This report reflects the past developments, but also proposes future scenarios along technological and non-technological lines. At the core of the 2030 vision of Industrie 4.0 are the three pillars "autonomy, interoperability and sustainability".	Link
German Standardization Roadmap Industrie 4.0.	The Standardization Roadmap for Industrie 4.0 is one of the pivotal communication media for Industrie 4.0. It enables the national and international exchange of information between standardization, industry, associations, research, and politics. It is a guide showing the way for individuals and organizations active in various sectors of technology and presents the outcomes from current work and discussions, as well as an overview of standards and specifications relevant to Industrie 4.0. It sketches out the requirements placed on standardization and lays down effective measures for their successful implementation.	Link
Usage View of the Asset Administration Shell	Publication of the Plattform Industrie 4.0: This discussion paper highlights the applications and benefits of the administration shell	Link
Structure of the Administration Shell	Trilateral perspectives from France, Italy and Germany - Publication of the Plattform Industrie 4.0: The 4th industrial revolution is radically transforming our economies, as innovation and digitization call for a paradigm shift in industrial production and products. Therefore, integrating the digital revolution is the new road ahead for industry.	Link
Relationships between I4.0 Components – Composite Components and Smart Production	Continuation of the Development of the Reference Model for the I4.0 SG Models and Standards-Publication of the Plattform Industrie 4.0: The RAMI4.0 model can be used to describe any I4.0 asset. The I4.0 component allows you to create an information technology link, using the administration shell, between any asset and Industrie 4.0. This document aims to describe an information technology structure that can be used to interrelate various I4.0 components and then organise these components into composites for specific purposes.	Link
Details of the Asset Administration Shell - Part 1	The exchange of information between partners in the value chain of Industrie 4.0 (Version 3.0RC01): The publication states how companies can use the Asset Administration	Link

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

	Shell to compile and structure information. In this way, all information can be shared as a package (set of files) with partners at several levels of the value chain. It is not necessary to provide online access to this data from the very beginning.	
Examples of the Asset Administration Shell for Industrie 4.0 Components – Basic Part. Continuing Development of the Reference Model for Industrie 4.0 Components	The aim of the publication is to provide examples relating to the recently agreed "structure of the asset administration shell" and thus to strengthen a common understanding of the content. This applies to the collaboration with VDI/VDE GMA FA 7.21 and the Ontology sub-working group of Plattform Industrie 4.0.	Link
Industrie 4.0 Communication Guideline Based on OPC UA	Guidance for German small and medium sized companies: An important basis for the successful introduction of Industrie 4.0 is the manufacturer-independent exchange of data in production. For this purpose, the open interface standard OPC UA is increasingly established.	Link
I4.0-Sprache (engl.: Industry 4.0 Language)	Vocabulary, message structure and semantic interaction protocols of the I4.0 language: The publication of the Plattform Industrie 4.0 promises a new level of organization and control of value chains. Networking to form an Internet of Things using data and services, as well as extensive cooperation between components of an Industrie 4.0 system, will create dynamic, self-organizing, self-optimizing, and cross-company value creation networks.	Link
Industrie 4.0 Plug-and-Produce for Adaptable Factories: Example Use Case Definition, Models, and Implementation	The document provides a use case specification, a conceptual model for its realization, as well as the high-level mapping to different technologies. It also provides the description of an example realization to make the concepts more tangible. Still, the description may not be detailed enough to illustrate all facets of the use case. The aim is to use only standards for the implementation of the scenario, so that a vendor-neutral Plug&Produce becomes possible. At the end the document discusses standards useful for the example implementation and provides a first evaluation.	Link
Position Paper Interoperability	The vision for Industrie 4.0: Interoperable communication between machines within networked digital ecosystems In the industrial world, new forms of cooperation have replaced rigid value chains. The borders between countries, industry sectors and companies are becoming increasingly blurred. Machines, products, and plants are able to communicate autonomously in digital, globally networked ecosystems that are dynamic, self-optimising and composed of multiple decentralised stakeholders.	Link

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Which criteria do Industrie 4.0 products need to fulfill?	Publication of the Plattform Industrie 4.0: ZVEI and the working group 1 on reference architectures, standards and norms of Plattform Industrie 4.0 have developed general and universal criteria for Industrie 4.0 products. These criteria are described in this guideline.	Link
Submodel Templates of the Asset Administration Shell - ZVEI Digital Nameplate for industrial equipment (Version 1.0)	Publication of the Plattform Industrie 4.0: The Submodel template "Nameplate" for the Asset Administration Shell aims at interoperable provision of nameplate information of an asset by means of a standardised property structure. It targets equipment for process industry and factory automation.	Link
Details of the Asset Administration Shell - Part 2	Interoperability at Runtime – Exchanging Information via Application Programming Interfaces (Version 1.0RC01). This part extends Part 1 and defines how information provided in the Asset Administration Shell (AAS) (e.g. submodels or properties) can be accessed dynamically via Application Programming Interfaces (APIs).	Link
Industrial Internet Consortium and Plattform Industrie 4.0 Explore the Application of Digital Twin and Asset Administration Shell Concepts	The Industrial Internet Consortium® (IIC™) and Plattform Industrie 4.0 announced the publication of a new whitepaper that explores digital twin technology concepts and their practical application in an organization. The joint whitepaper, Digital Twin and Asset Administration Shell Concepts and Application, provides clear and concise definitions of digital twin technologies, standards, and use cases. It also describes how the Plattform Industrie 4.0 Asset Administration Shell, an implementation of a digital twin for industrial applications, enables cross-company-interoperability across the complete value stream.	Link
I4.0 x Industrial Internet: Practices and Findings	White Paper of the Sino-German Expert Group on Industrial Internet: The Industrial Internet is a key enabler to the digital transformation of manufacturing. Working at the industry and expert level, the Sino-German Company Working Group on Industrie 4.0 and Intelligent Manufacturing (AGU) Expert Group Industrial Internet (EG II) aims to foster mutual understanding on technological concepts and develop a joint conclusion and recommendations. As the result of the initial phase of the EG II, the 2019 edition of the White Paper presents the preliminary findings of the joint work of German and Chinese companies and experts, builds the foundation for future cooperation, and specifies topics for the future work of the AGU EG II.	Link
Sino-German White Paper on Functional Safety for	The paper surveys and analyses existing standards, specifications, and research to give an overview of safety for Industrie 4.0 and Intelligent Manufacturing.	Link

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Industrie 4.0 and Intelligent Manufacturing		
Guidance for the Construction and Promotion of Industrial Internet Platforms & Evaluation Method for Industrial Internet Platforms.	Policy Update of the Sino-German Industrie 4.0 Project, August 2018: This Policy Update focuses on the "Guidance for the Construction and Promotion of Industrial Internet Platforms" and the "Evaluation Method for Industrial Internet Platforms". Whilst the former introduces measures to standardise and optimise platform development, the latter outlines specific capability requirements for a unified assessment to guide the application and development.	Link
Interoperabilität hoch zwei für Simulationsmodelle (available in German)	In this presentation, the simulation and standardization experts of Plattform Industrie 4.0 explain what lies behind the simulation submodel and show how they develop and expand a solution step by step using use cases.	Link
Der digitale Zwilling in der Industrie 4.0 (engl: The digital twin in Industrie 4.0)	In this presentation, the standardization experts from Plattform Industrie 4.0 explain what lies behind the management shell concept and how it works in practice.	Link
Shaping Europe's digital future. Interoperability	POLICY: The Commission has adopted a list of standards and specifications for harmonised electronic communications networks to ensure that consumer choice is not restricted because of incompatibilities	Link
2030 Vision for Industrie 4.0. Shaping Digital Ecosystems Globally	A holistic approach to the shaping of digital ecosystems: In this 2030 Vision, the stakeholders of Plattform Industrie 4.0 present a holistic approach to the shaping of digital ecosystems. Working from the specific situation and established strengths of Germany's industrial base, their aim is to create a framework for a future data economy in line with the requirements of a social market economy: emphasising open ecosystems, diversity and plurality and supporting competition between all the stakeholders on the market. The Vision is primarily addressed to industry and commerce in Germany, but explicitly highlights the importance of openness and a willingness to work together with partners in Europe and around the world.	Link
Industrie 4.0 Service Architecture - Basic concepts for interoperability	This status report provides the foundation for a reference model of the Industrie 4.0 Service Architecture.	Link
A Review of Interoperability Standards for Industry 4.0.	The focus of this paper is to examine the progress that is being made to establish interoperability across a diverse set of systems and also to identify the challenges in establishing this level of interoperability. To achieve this a literature review of current Industry 4.0 technologies and	Link

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

	current interoperability standards was be undertaken, to identify and categorise potential frameworks capable of providing an Industry 4.0 global interoperability standard. (https://doi.org/10.1016/j.promfg.2020.01.083)	
Industry 4.0 Interoperability, Analytics, Security, and Case Studies	(Edited By G. Rajesh, X. Mercilin Raajini, Hien Dang; ISBN 9780367501129). The book provides an understanding of the drivers and enablers of Industry 4.0; includes real case studies of various applications for different fields; discusses technologies such as cyber physical systems (CPS), Internet of Things (IoT), cloud computing, machine learning, virtualization, decentralization, blockchain, fog computing, and many other related areas; covers design, implementation challenges, and interoperability; offers detailed knowledge on Industry 4.0 and its underlying technologies, research challenges, solutions, and case studies.	
The Industrial Internet of Things Volume G1: Reference Architecture	The document is refining and advancing the 'Industrial Internet Reference Architecture'	Link
Architecture Alignment and Interoperability	An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper IIC:WHT:IN3:V1.0:PB:20171205	Link

Table 6: Recent publications regarding interoperability

It is important to highlight the first document "Plattform Industrie 4.0 Germany. Progress report 2019". This report reflects the past developments, but also proposes future scenarios along technological and non-technological lines. At the core of the 2030 vision of Industrie 4.0 are the three pillars "autonomy, interoperability and sustainability".

In the interim period between D1.2 and D1.4, two interesting white papers have been published:

- OPENDEI position paper: REFERENCE ARCHITECTURES AND INTEROPERABILITY IN DIGITAL PLATFORMS
- AIOTI report about semantic interoperability

Find here down the main contributions of these papers:

5.2.1 OPENDEI position paper

This paper analyses the different Reference architectures and its implementation in the different sectors, particularly:

- Health
- Manufactuirng

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- Agrifood
- Energy

There is a very close connection between CF2 and OPENDEI manufacturing industry analysis. The contributions from TECNALIA, INNOVALIA, POLIMI have tried to align both projects, addressing RAMI, IDSA RA, AAS, FIWARE…. As in CF2 D1.2.

5.2.2 AIOTI report on semantic interoperability

AIOTI WG has created an Ontology Landscape that currently includes 30 ontologies from different application areas of IoT. This overview gives a first indication, which ontologies could be suitable candidates in each use case

The Ontology Landscape visualization shown below is structured according to the different IoT application domains. Generic IoT ontologies that do not target a specific application domain are shown in the vertical box below. The colour identifies the maintainer of the ontology. The colour intensity shows the maturity of the ontology based on the Technology Readiness Level as it is also used in European Projects

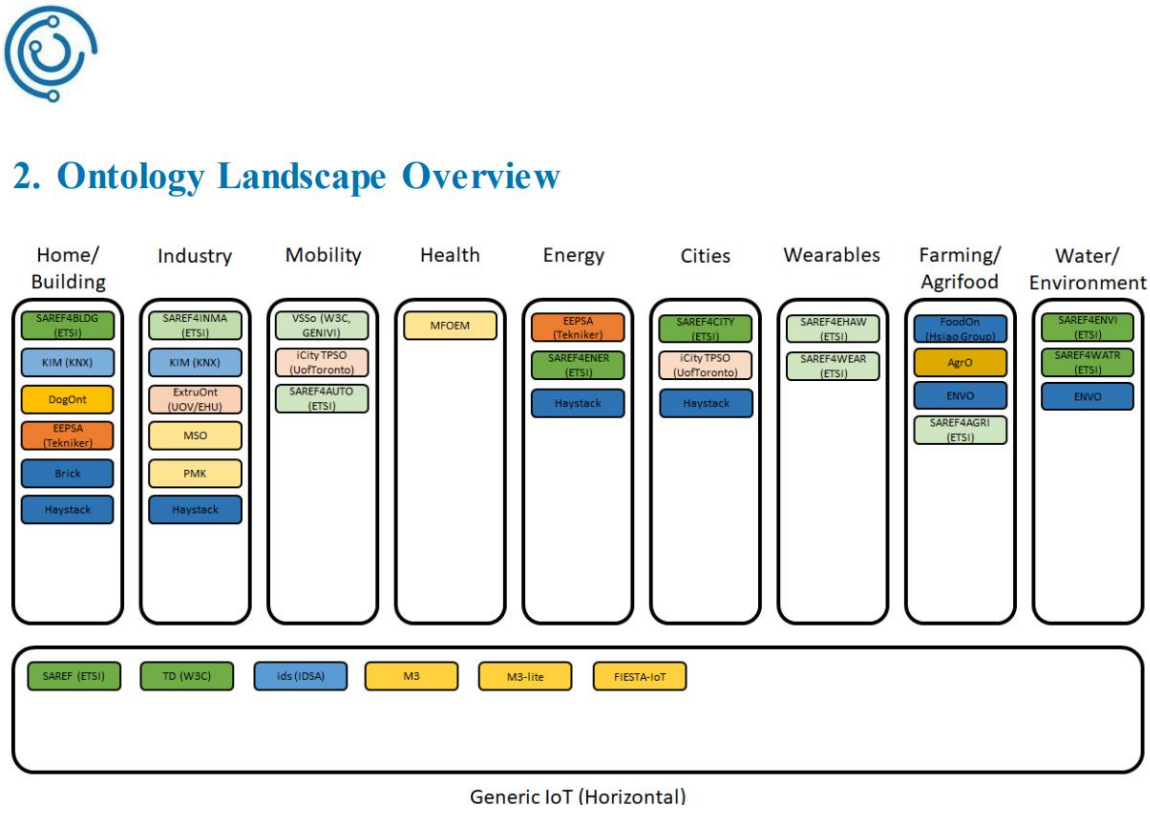


Figure 56: AIOTI ontology landscape overview

It is worth mentioning that AAS has not been even mentioned on this doc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

5.3 Examples from projects (mapping of projects)

5.3.1 EFPF- European Connected Factory Platform for Agile Manufacturing

The following describes the interoperability approach of EFPF, as was presented in Dec 2020 DMP CLUSTER-CF2 workshop (Figure 57 and Figure 58):

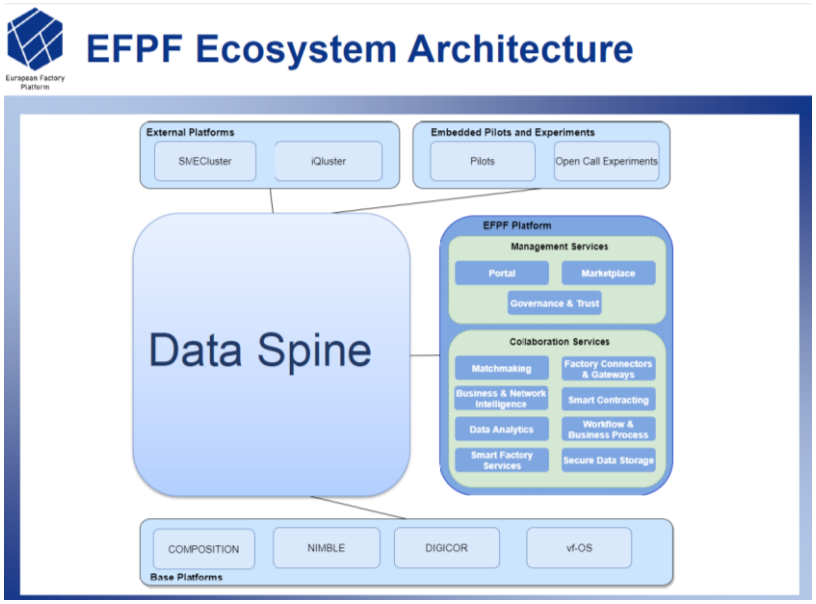


Figure 57: EFPF ecosystem architecture

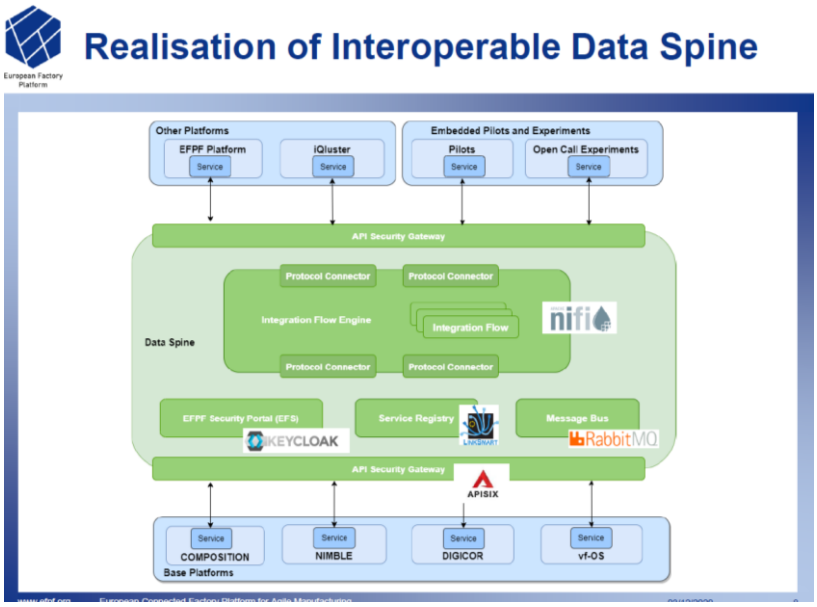


Figure 58: Interoperable Data SPine

- at Protocol level (Figure 59):

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

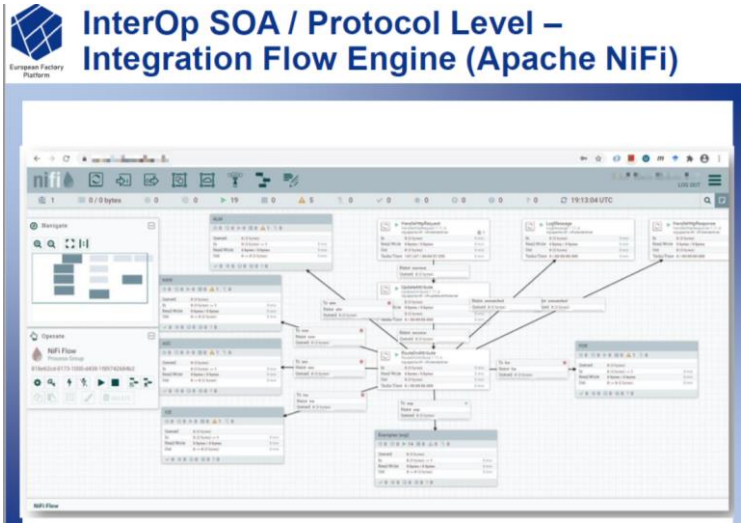


Figure 59: Interop SOA

- at data model level (Figure 60):

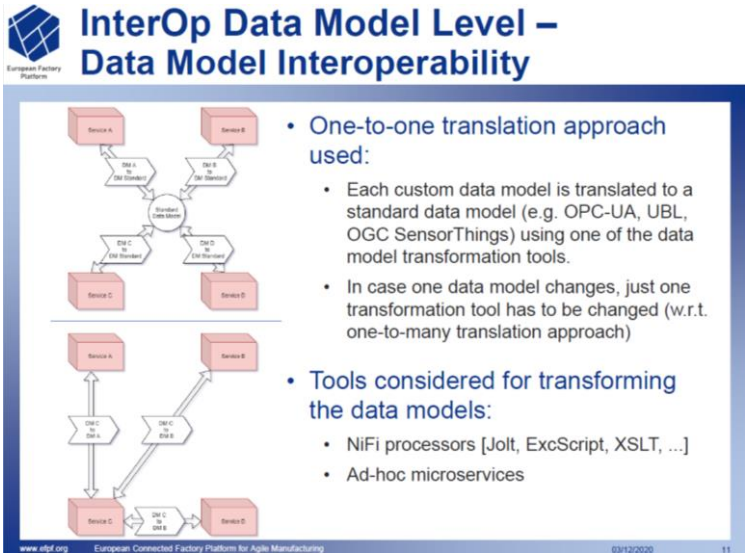


Figure 60: Interop Data model

- and giving as a result the following components interaction and implementation (Figure 61):

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

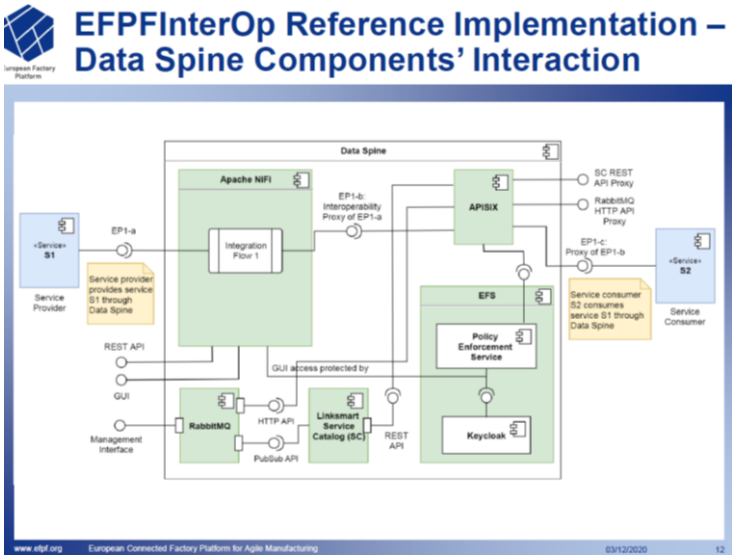


Figure 61: EFPF interoperability implementation

Relevant public deliverables generated by the EFPF project so far include:

- D2.3 - Requirements of Embedded Pilot Scenarios (M5)
- D3.11 - EFPF Data Spine Realisation
- D2.2 - Platform Interoperation Challenge Report (M5)

5.3.2 QU4LITY – Joining forces towards an European Industrial Autonomous Quality

QU4LITY approach to interoperability will be further analysed in the second half of CF2.

QU4LITY does not provide a digital platform, for the reason that it looks imposible to cover all pilot needs, but on the other hand provide a RA with different layers, creating DIGITAL enablers and applying them in 14 pilots.

The infrastructure that will facilitate 1-the integration of two or more digital enablers in ZDM/AQ solutions, in ways that facilitate the deployment, release, packaging and distribution of the results and 2- the interoperability across different modules and platforms that comprise a ZDM/AQ solution, given that the various components/platforms tend to produce digital data in different formats and based on different semantic

The pilots are the following:

USE CASE	DESCRIPTION
WHIRLPOOL	vertical integration of data management (from data gathering to visualization and decision-making),
GF	detecting, diagnosing, and fully compensating deviations on accuracy, productivity and sustainability of a machining cell based on the aggregation of information from milling and EDM machinery health, process performance and geometrical part characterisation, using AQ control loops and a common data space
PRIMA	¿?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

RiaStone	integration of new inline inspections systems and AQL control loops into the current production line. Perform Artificial Vision
Kolektor (KOL)	(i) Collect moulding process parameters; (ii) Monitor environmental parameters; Based on the collected data and by applying control loops, advanced analytics and artificial intelligence methods we will better understand the moulding process
SIEMENS	implementing a closed control loop approach via the deep analysis of process data and the implementation of digital twins for products and production. Data from control loops throughout the manufacturing lines are to be collected and analysed via data mining and machine learning techniques, allowing to systematically identifying faulty products and the respective failure causes, providing the base for the intended improvements.
THYS	acoustic control: specific treatment and analysis of the signal, component as the root cause can be isolated.
PRIMA	Additive Manufacturing : enhance process monitoring and control. Real time detection, collect data, communicate data
CONTI	automotive electronics - PCBs) Sensing and combining data from a variety of source recognition a management of unstructured data for multi-stage production lines through introduction of deep analysis and decision-making control loops, for capturing, communicating, secure storing and visualizing real-time holistic data Big Data technology in supervisory and strategic decision-making
FAGOR	FAGOR. A press machine collecting press machine critical parameters and identifying exactly the process developed in the manufacturing of pieces. acquisition, measurement and transmission of the parameters and variables
DANOBAT	use grinding machine operational data to relate machine-use with evolution of machine components condition
GHI	industrial furnaces for melting, heat treating and heating any type of metal. reduce fuel consumption, assuming a reduction in CO2 emissions hot stamping?? What is the goal of the pilot?
AIRBUS	A Model-based systems engineering (MBSE) design an industrial system at high level (Supplier network, Factories, Machines and processes) for near Zero-Defect Manufacturing
MONDRAGON	FAGOR+DANOBAT
PHILLIPS	

Table 7: QU4LITY pilots

Some info regarding QU4LITY pilots.

Link to the pilot descriptions in the portal:

https://portal.effra.eu/results/list/result?result_search%5Btaxon%5D=&result_search%5BtextQuery%5D=&result_search%5Bproject%5D=1864&result_search%5Bsort%5D=Relevancy&result_search%5BsortDirecti

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

on%5D=Descending&result_search%5Blist__1045%5D%5B%5D=all&result_search%5Blistcheckbox__1045%5D=1045&result_search%5Bpublishable%5D=1

The reference arquitecture provided by QU4LITY is very coherent with the previous analysis done by CF2 in the first part of the project. See picture below.

The orange part is very similar to RAMI VERTICAL: RA describes "data in motion" and "data at rest". This definition comes from MIDIH project, that was already analyzed in CF2

Regarding the blue part, it is like the horizontal layers in RAMI and describes 3 networks.

- Factory
- Corporate –private ledger
- Internet –value chain ledger – for multiple organizations
- Data space- multiple transactions has NOT been addressed.

The ledger connects with the DISTRIBUTED LEDGER TECHNOLOGIES block and provides data sovereignty tools: privacy, security, trustworthiness…

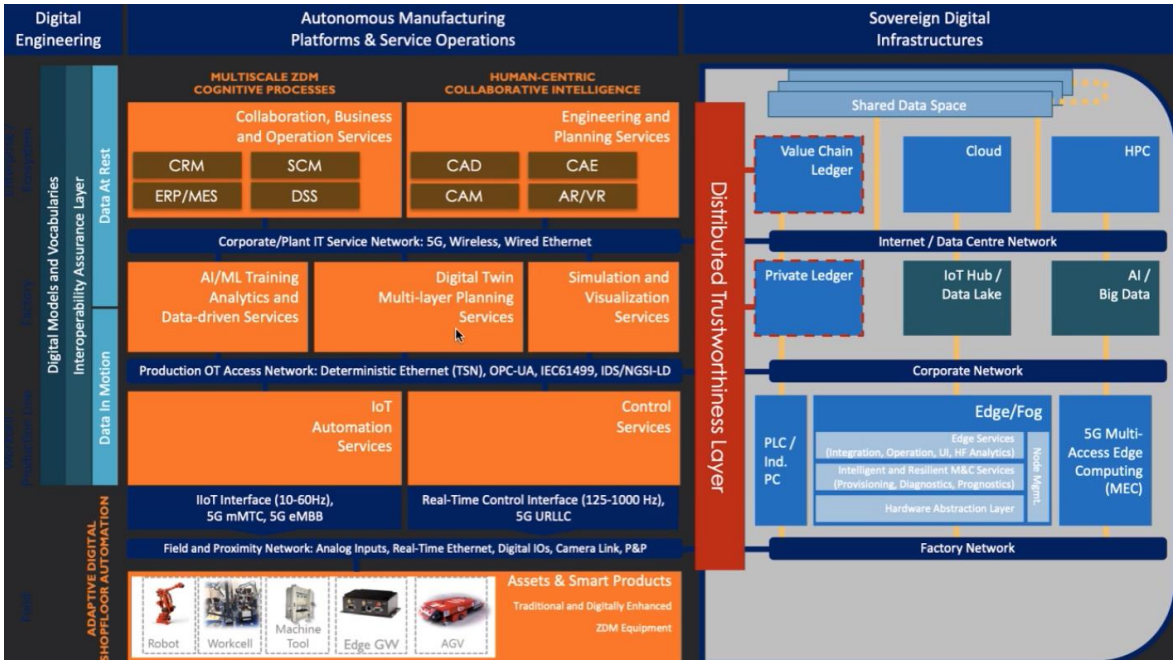


Figure 62: QU4LITY RA.

During our meetings with QU4LITY we have tried to answer the following questions:

1. Which interoperability challenges need to be addressed as a priority or are the most challenging?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

PHILIPS: The biggest challenge lies in making state-of-the-art systems interact with legacy systems throughout the factory. Mostly all data is available, however, retrieving this data can cause problems due to its high velocity and the impact collection from data has on legacy systems. For example, robot encoder data used as an input for predictive algorithms causes a decrease in performance of assets (e.g.robot) because these are not made for high velocity data streaming resulting in "abusing" the robots buffer causing it to slow down.
SIEMENS: Security, performance, not to interrupt the automated production flow (no bottleneck with additional modules).
CONTINENTAL: Globally accessible Cloud Platform and the connection to it.
WHIRLPOOL: Many shop floor system not homogeneous in term of technologies and semantic.
MONDRAGON: Integrate data from heterogeneous systems for standardized output, integrate applications for unique Dashboard, interchange data ensuring governance properties.
KOLEKTOR: In our pilot we had to address the problem of standard communication interfaces between various system (Smart IoT agents and various other systems)
THYSS: Interoperability between additional assets sensors monitoring is the main problematic for our non-intrusive IoT system, these sensors have to be interchangeable while measuring several aspects of the shopfloor environment. Also, a large interoperability between different production line PLC has to be developed in order to keep the same level of integration for each application use-case.
GHI: Data models and secure protocols for data exchange across various digital platform (SCADA for manufacturing process and quality control platform).
RIASTONE: The relevant interoperability changes that we have faced in the RiaStone Pilot were the need to transport contextualized logical commands through different operating Systems, and application layers in order to be able to build a complete AQL System, from individual shopfloor machines that use different OS´s, Applications, and languages.
IDEKO: Integration of different devices/assets, from different manufacturers defining the assets in a standardized way using common data models and enabling the data exchange between different stakeholders through a secure and trusted data space.
FAGOR: Interoperability between cloud platforms.
GF: High frequency data transmission and collection from machines in standard, secure mode. OPC UA does not enable this in real time

2. How are the challenges addressed and solved in your pilot by taking into account the particular context and requirements of your business case?
   PHILIPS: This challenge discovered during the course of the qu4lity project is solved by manually extracting the data for as far as possible, however, in order to really tackle this problem, long-term solutions are needed that are not in the scope of the Qu4lity project.
   SIEMENS: Defined interfaces to machine PC, modules running on Edge device.
   CONTINENTAL: Interoperability is not the primary focus of the Pilot. In one Business Process a Semantic Search engine overcomes language barriers and makes use of a cloud platform

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

WHIRLPOOL: Creating a semantic MPFQ-R model able to conceptualize all the objects (process, material, function etc.) needed for our use case.
MONDRAGON: Integrate data from heterogeneous systems and Manufacturing production lines.
KOLEKTOR: In our pilot case we are primarily addressing the interoperability challenge of the IoT world regarding the traceability goals for material, resources, and products. We decided to adhere to the MQTT Sparkplug B specification. Sparkplug B is a specification for MQTT that defines how data is sent and received. IoT agents at the edge of a network can use Sparkplug B to communicate with applications like SCADA systems, historians, and analytics programs. In our case that is Kolektor's IIoT.Sinapro system. For interoperability between smart IoT agents and robotic workers, we chose ROS communication protocol.
THYSS: Interoperability between additional assets sensors monitoring is the main problematic for our non-intrusive IoT system, these sensors have to be interchangeable while measuring several aspects of the shopfloor environment. Also, a large interoperability between different production line PLC has to be developed in order to keep the same level of integration for each application use-case
GHI: Data models are based on standard models (avoiding proprietary formats; e.g. ISO23952:2022). Piloting DIN 27070 reference architecture for secure information gateway.
RIASTONE: In the RiaStone case we have used a number of different solutions, namely interoperability buses (Kafka Bus), Built to purposes API´s, and ETL (Extract_Transfor_load) data systems, namely due to Real-time requirements, Productivity control or visibility/interfaces for human interaction, and Traceability goals for material, resources and products.
IDEKO: Exploring AAS and IDS technologies for standardization and data sharing making a proof of concept with the machine pilot for predictive maintenance purposes.
FAGOR: Building flexible solutions with the capacity of interacting with other services of different natures (REST, MQTT, OPC, Industrial Bus).
GF: The pilot provides a proprietary solution combining OPC UA with real time M2M, real time control, communication protocols

3. On which layers or system levels do you have to address in particular the interoperability?
PHILIPS: Asset level.
SIEMENS: Machine PC, Edge device and cloud.
CONTINENTAL: Functional level of Parts Analysis recording.
WHIRLPOOL: Integration level.
MONDRAGON: The interoperability was addressed between Integration, Information and Business Level.
KOLEKTOR: Integration level, Communication Level.
THYSS: • Asset Level, Integration Level, Communication Level • Field device level, Control Device level, Station level, Work Centre level, Edge
GHI: We are focusing on data layer interoperability for shopfloor operation optimization.
RIASTONE: All these challenges were addresses mostly @ M2M (Machine-to-Machine) levels, namely at Integration level / Communication level / Functional level / Control Device level / and Edge – fog - cloud.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

IDEKO: Asset Level.
FAGOR: Asset level, Communication level. GF: Machine to Machine, Asset, Communication and Information level

4. Do you use existing (interoperability) frameworks or do you need to develop new technological solutions?
   PHILIPS: Currently no existing / previously developed frameworks are used because, to my knowledge, these do not solve the challenges faced.
   SIEMENS: We use Industrial Edge and SSH
   CONTINENTAL: We are using inhouse legacy applications. In the future an AWS Cloud Service will be used.
   WHIRLPOOL: We use a database MariaDB to standardize data flow as per MPFQ model.
   MONDRAGON: Open-Source Solutions based on Publish/Subscribe broker architecture and DevOps.
   KOLEKTOR: We have integrated the eclipse sparkplug framework.
   THYSS: We have developed each interoperability modules needed for the project.
   GHI: We are using DFA reference framework for integration and interoperability.
   RIASTONE: In the RiaStone Pilot we have used standard tools to address interoperability (ex: Kafka Bus), but we have also used customised built to purpose API´s.
   IDEKO: Asset Administration Shell (AAS).
   FAGOR: The solution is based on standard architectures such as RAMI4.0 but the implementation is proprietary.
   GF: Mainly OPC UA and UMATI specifications for machine tool communication
5. In your business case, have you tackled interoperability aspects dealing with international data exchange challenges,sectoral or cross-sectoral approaches, data resiliency?
   PHILIPS: No.
   SIEMENS: No.
   CONTINENTAL: Yes, Language barriers are tackled by a Fraunhofer Semantic Search algorithm.
   WHIRLPOOL: No.
   MONDRAGON: International data exchange challenges.
   KOLEKTOR: No. THYSS: Not concerned. GHI: No. we are focusing on data sharing and integrated visualization and decision support processes
   RIASTONE: Not at this point in time, but it is foreseen in the future that RiaStone will apply distributed ledger technologies, specially Blockchain, and particularly using DPOS based Blockchain frameworks.
   IDEKO: No. Only for testing in lab environment.
   FAGOR: No.
   GF: Mainly with OPC UA protocols, less popular in the US and in Asia than in Europe
6. How did you incorporated standardization activities (if this is the case) in your pilot work and what were the main initial reasons for addressing standardization in your business case?
   PHILIPS: N/A
   SIEMENS: It was a requirement from your organization.
   CONTINENTAL: Standardization is a cost reduction means.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

WHIRLPOOL: It was a key requirement of the call for projects.
MONDRAGON: Standardization was a requirement from the market
KOLEKTOR: It was seen as critical to ensure the success of the project's exploitation and/or market strategy.
THYSS: It was a requirement from your organization.
GHI: • It was a requirement from your organization • It was seen as critical to conduct the research activities during the projects (e.g. for agreeing on terminology or methodology)
RIASTONE: It was seen as critical to ensure the success of the project's exploitation and/or market strategy.
IDEKO: N/A
FAGOR: It was a key requirement of the call for projects.
GF: It was seen as critical to ensure the success of the project's exploitation and/or market strategy

5.3.3 ZDMP – Zero Defect Manufacturing Platform

ZDMP approach to interoperability will be further analysed in the second half of CF2.

It was not meant to follow RAMI arquitecture but to focus on Interplatform interoperability: ADAMUS, BOSCH, SERVITLY platforms and their intereoperability with ZDMP

The following slide presents how they have been addressed in the different USE CASES/PILOTS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

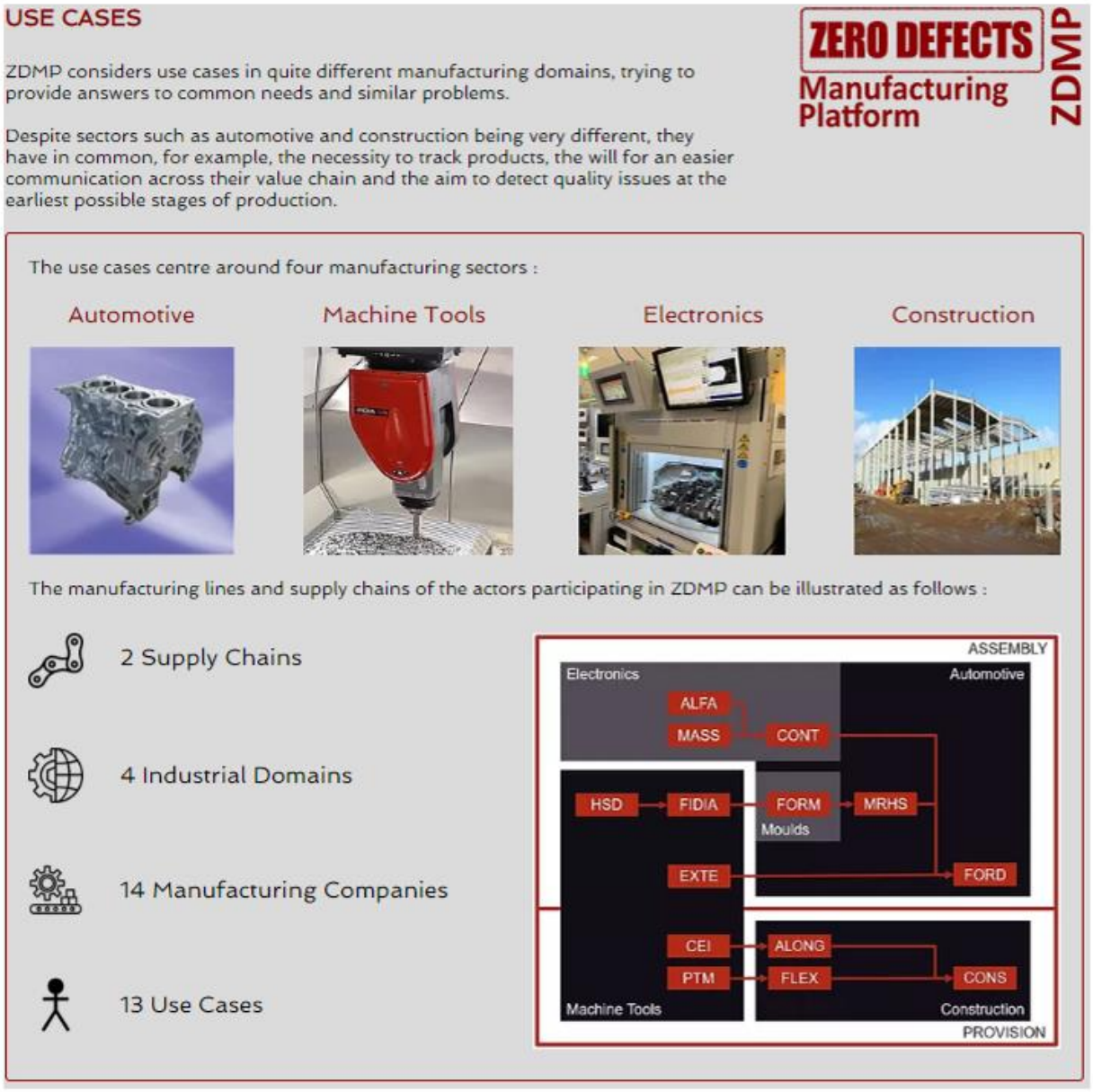


Figure 63: EFPF use case summary

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

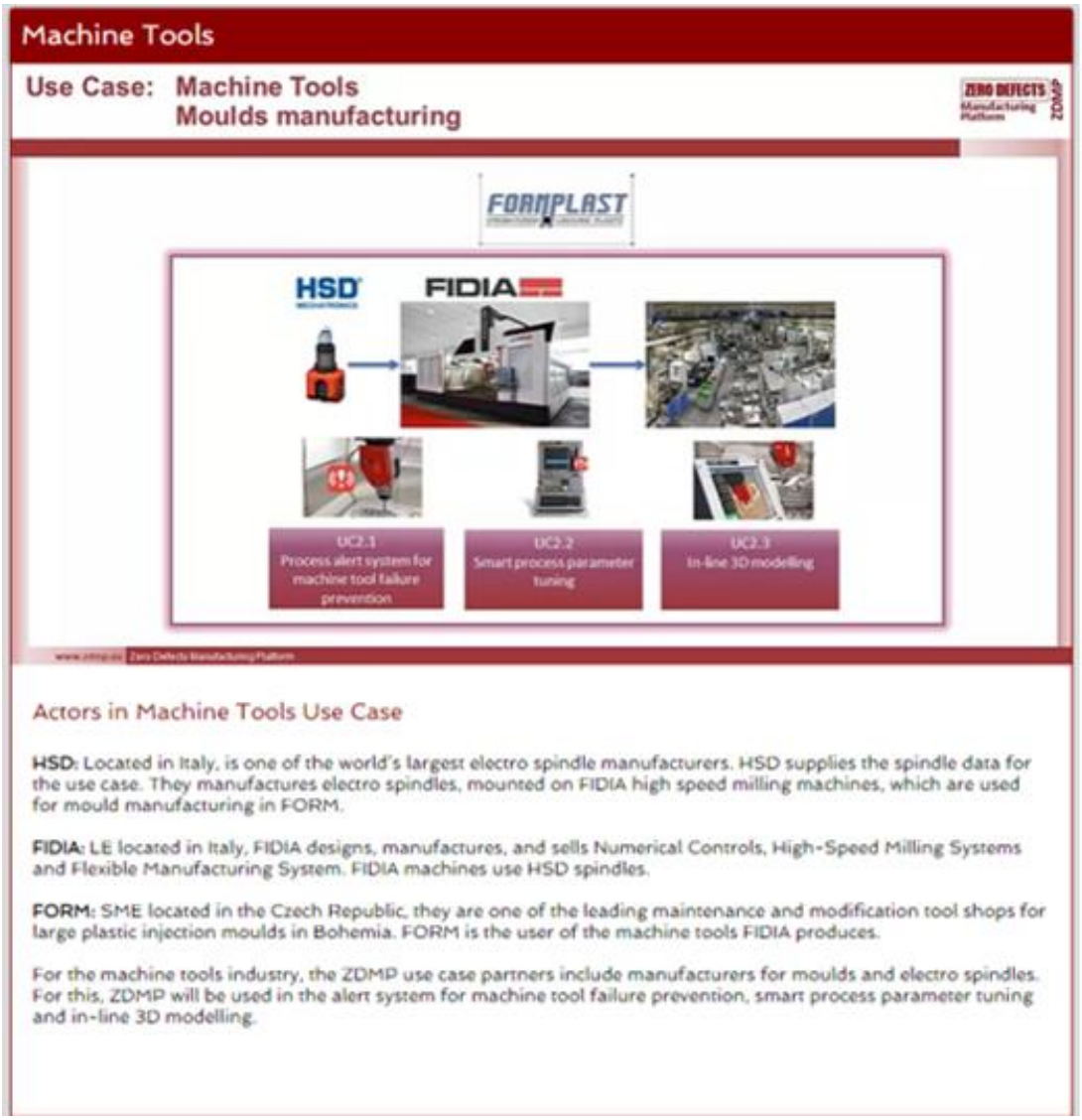


Figure 64: EFPF use case 1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Figure 65: EFPF use case 2

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

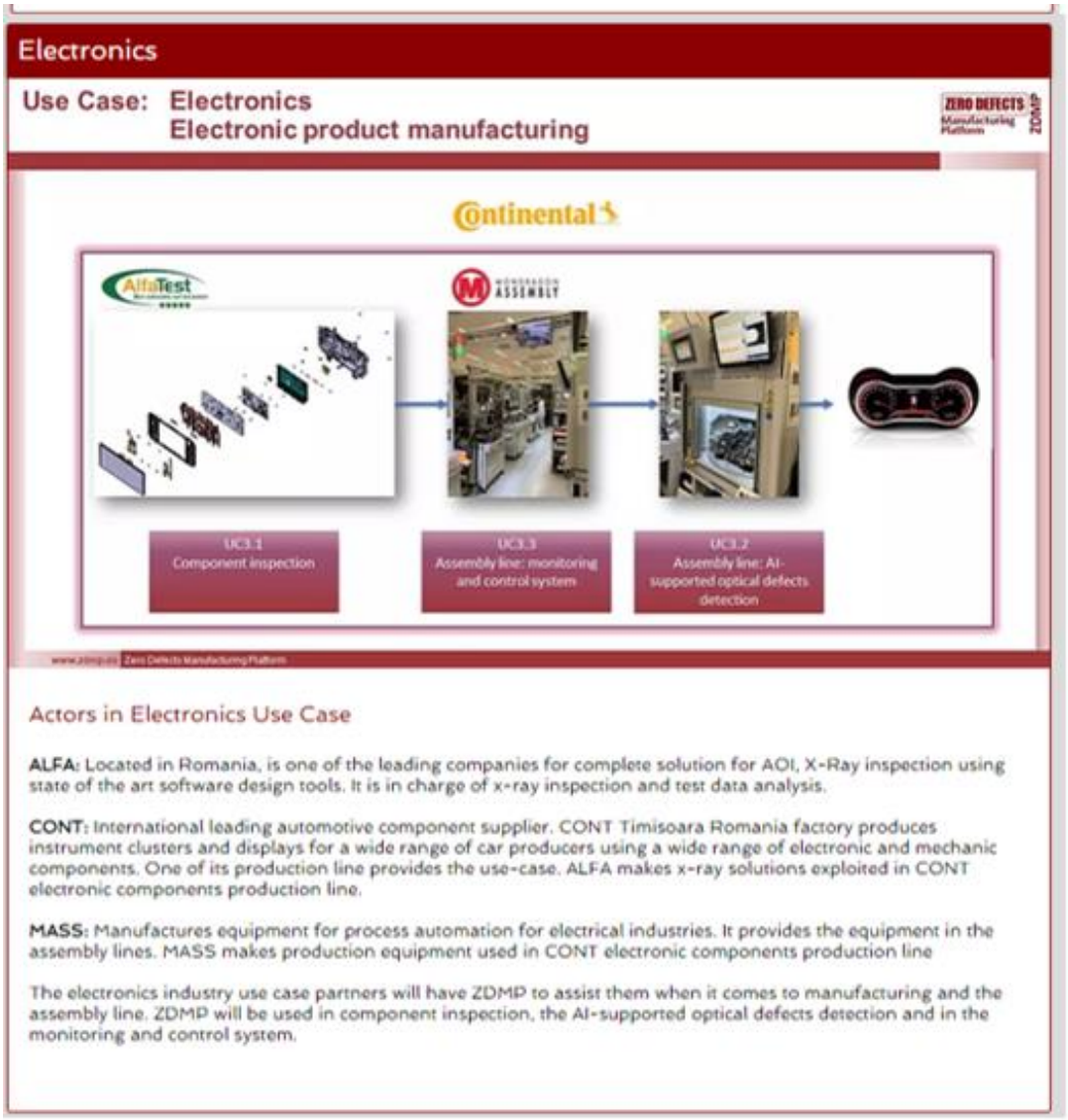


Figure 66: EFPF use case 3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

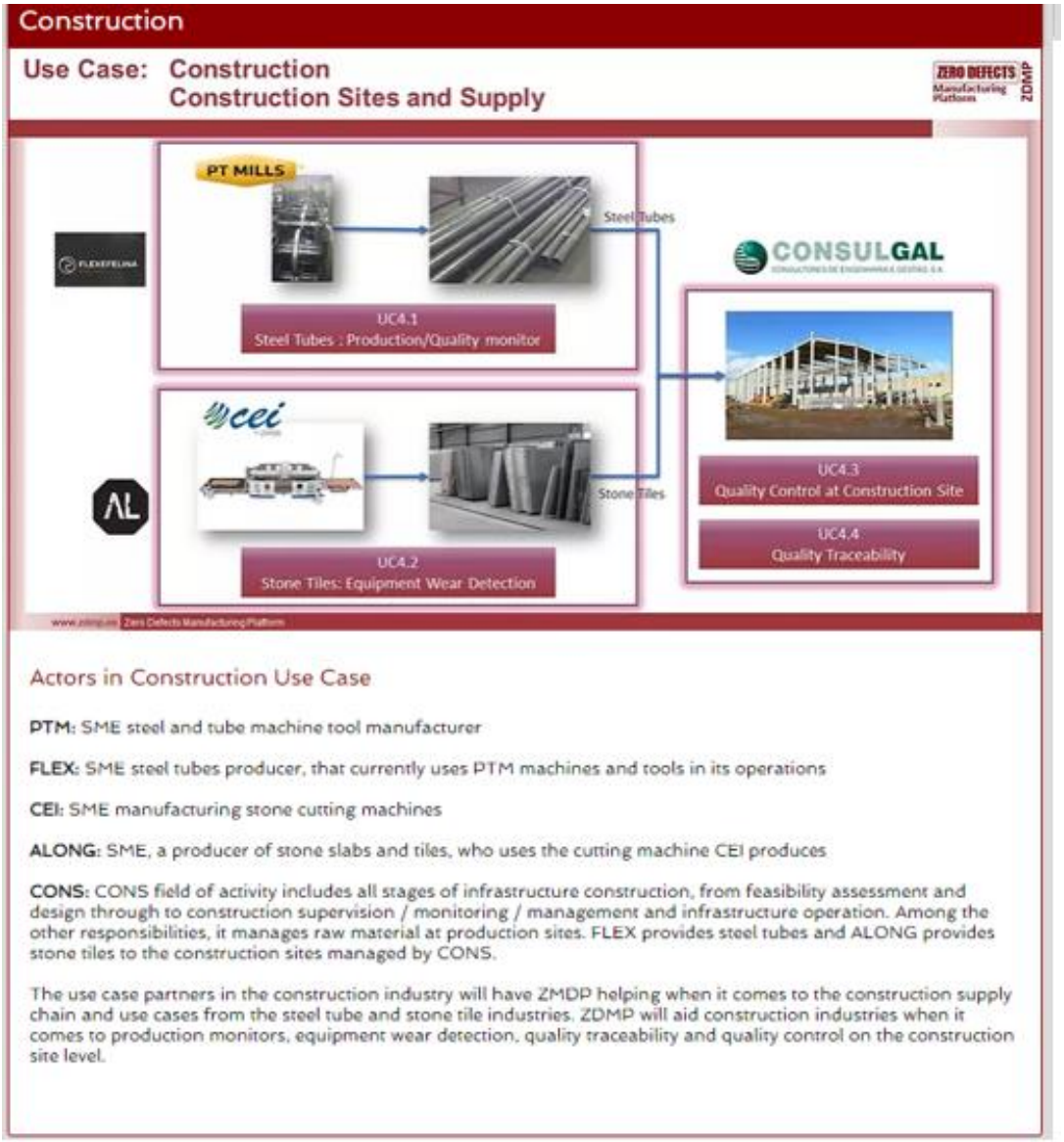


Figure 67: EFPF use case 4

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

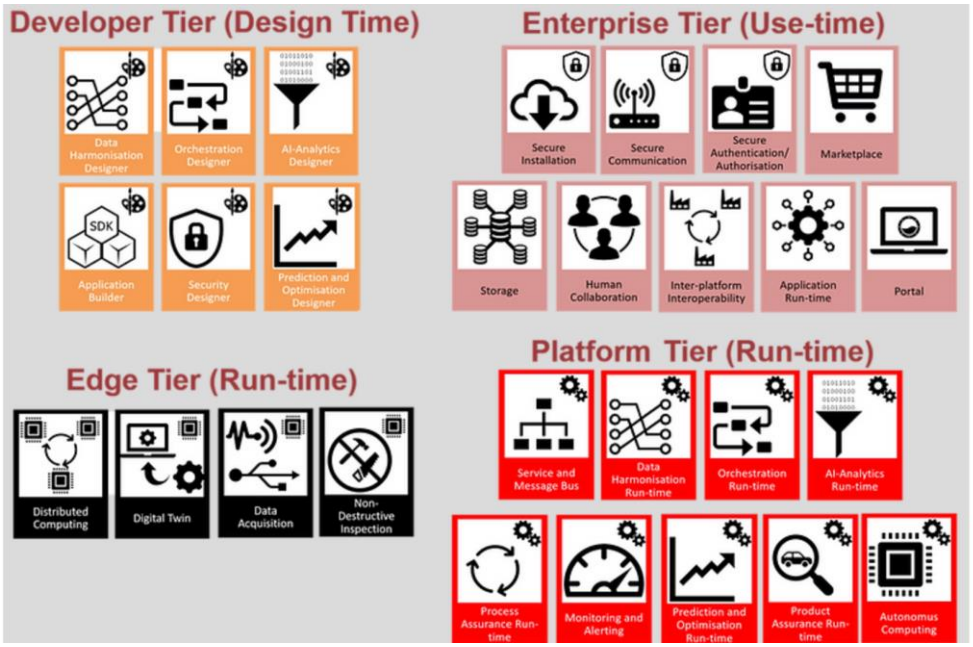


Figure 68: ZDMP tiers: Developer, Enterprise, Edge, Platform

Regarding the questions raised during our interviews on interoperability, these are the answers provided….

- Which interoperability challenges need to be addressed as a priority or are the most challenging?
  - Interoperability at Platform level SUPPORTING COMPONENTS AND DATA HARMONIZATION considering data is in different formats for different platforms.
  - Security aspects related with Authorization
  - Data capture was a challenge solved using standard protocols, but it is not considered an interoperability challenge in their WP.
- How are the challenges addressed on project level, or how are these challenges solved pilots by taking into account the particular context and requirements * of the pilots?
  - Considering NO critical data is running through the demonstration, implementation has been carried out in the different pilots using
    - Public APIs (commercial products) to be used
    - REST APIs
    - Opc ua
    - No use of AAS or semantics….

5.3.4 KYKLOS4.0 – An advanced circular and agile manufacturing Ecosystem based on rapid reconfigurable manufacturing process and individualized consumer preferences.

In D1.2, KYKLOS 4.0 was still in the initial phases of the project and the interoperability approach had not been properly defined. In the picture below, the general architecture was presented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

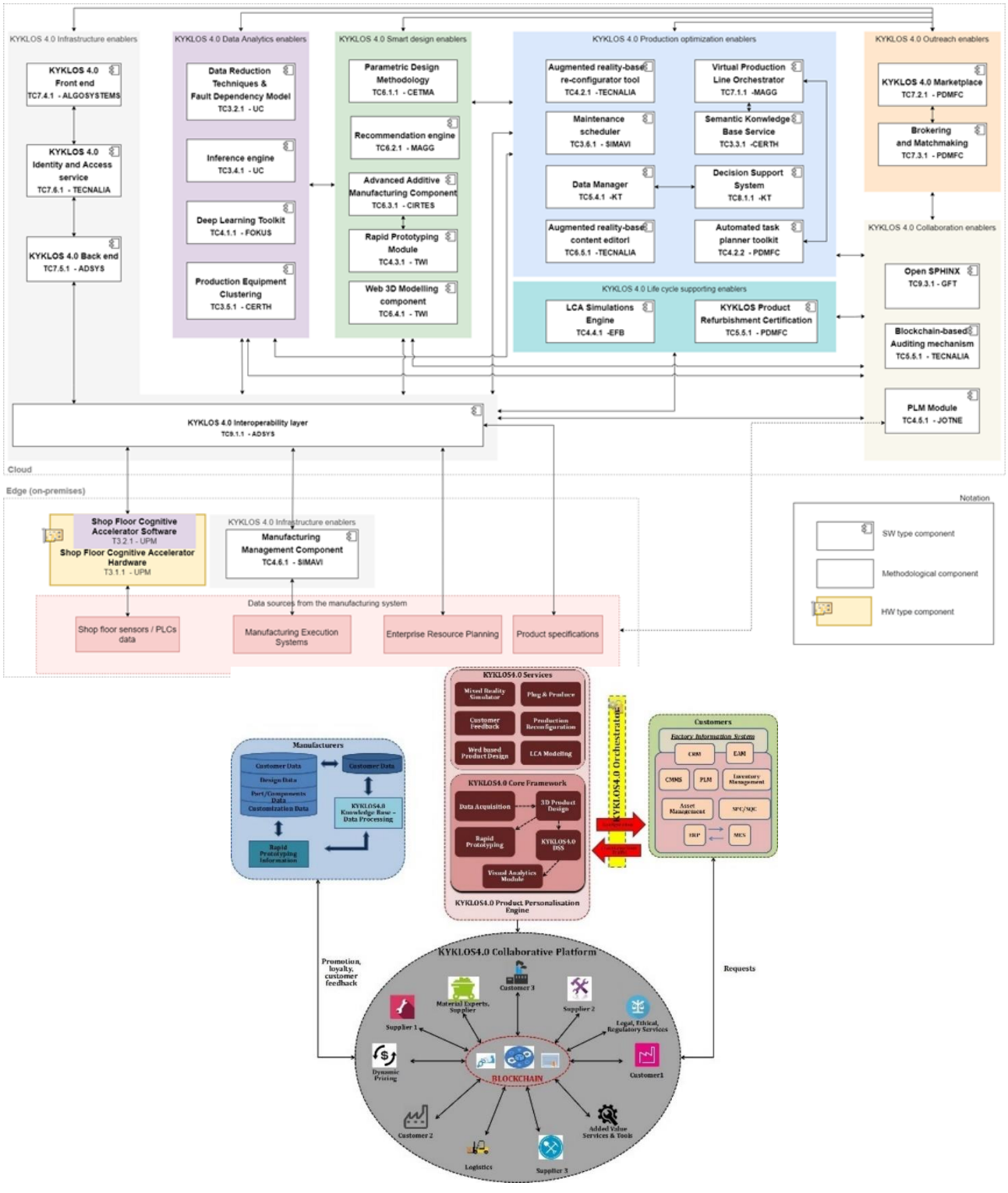


Figure 69: KYKLOS4.0 General Architecture

The interoperability approach has been analysed properly in the second half of CF2.

KYKLOS 4.0 has four pilots:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- UC.1: Medical pilot –
- Custom and smart wheelchair systems manufacturing (PROMEDICARE) Pro Medicare s.r.l. (PROMEDICARE) designs and manufactures postural systems for users who need customized wheelchairs. PROMEDICARE's customers are qualified dealers, i.e., Orthopaedic workshops.
- UC.2: Aerospace Pilot – Additive manufacturing technology for aerospace - aircraft part customization systems (KANFIT3D)
- KANFIT3D offers the latest solutions in Metal AM and hybrid manufacturing (combining AM with CNC), using advanced equipment and the latest manufacturing technologies to achieve accuracy and precision, to meet the top-most international standards. Most of KANFIT3D's manufacturing is for aerospace and medical customers. While in aerospace domain various high-precision parts of aircrafts are manufactured, in the medical domain Patient-Specific Implants are produced.
- 3.2.3 UC.3: Aerospace Pilot – Jet engine manufacturing & maintenance (GRC)
- GE Research (GRC) is General Electric's corporate research group, based in Israel. It supports the work of GE's business groups by performing research aligned with GE's business needs. Among the research interests of the GE Research team is collaborating with GE's Aviation business group to innovate in the domain of jet engine maintenance. With more than 33,000 engines in commercial service, GE is a world leader not just in engine manufacturing but in also in jet engine maintenance, repair, and overhaul (MRO).
- 3.2.4 UC.4: Electronic Devices/Equipment Pilot – Electrical Equipment Manufacturers (VESTEL) Television is the main final product of Vestel Electronics (VESTEL). In fact, VESTEL is one of the top 3 global TV producers. VESTEL manages four factories for the manufacturing of different parts of the final product, and a factory for the assembly of the final product. One of mentioned factories is a Metal Press factory and the KYKLOS use case pilot will take place in this factory.
- 3.2.5 UC.5: Electronic Equipment Industry Pilot (CONTINENTAL)
- CONTINENTAL develops pioneering technologies and services for sustainable and connected mobility of people and their goods. Founded in 1871, the technology company offers safe, efficient, intelligent, and affordable solutions for vehicles, machines, traffic, and transportation.
- 3.2.6 UC.6: Shipyard Pilot – Product Service solutions in Shipyards (ASTANDER)
- Astilleros de Santander S.A.U. (ASTANDER) was founded in 1872 as a forge by Mr. Bernardo Lavín. In 1913 the company made its first repair afloat of a vessel and in 1922 dry dock No 1 was inaugurated. Currently, ASTANDER is providing all the technical and human capacity needed to carry out all kinds of conversion and ship repair projects under the most demanding quality standards in the sector.
- 3.2.7 UC.7: Food Industry Pilot – Reduction of Energy Consumption and Waste Management (PINDOS)
- PINDOS is the largest first-degree agricultural cooperative and one of the five largest food companies in Greece. Some of the most important features that represent Pindos are shown below. • Over 500 poultry farmer – producer members • 43% of the members are women • 1200 employees • generations of poultry farmers who combine tradition with know-how • Working with 50 producer partners Despite the rapid growth of PINDOS in the last years, Pindos aims at protecting the environment while keeping up with the production demand. For that purpose, they enhance the quality of their products by optimizing the resources and utilizing all waste from the production process

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- UC.8: Automotive Pilot – Addressing the critical components of each piece in automotive industry (DIGRO)
- DIAD Group is a fast-growing company in the sector of advanced automotive and aeronautic components and finds its success factor in the constant transformation of the knowledge produced by applied innovation into products, technologies, and services for the automotive and the manufacturing industrial sectors. The main activities of DIAD Group are the design, development, testing and application of advanced components for the automotive and the aerospace sectors, using the most advanced engineering tools and innovative materials such as high-performance composites, hyper functionalized surfaces, bio - based thermoplastics, nanostructured based massive materials, and multi-functional coatings. DIAD is proposing as case study in automotive field a windshield cowl cover at present produced by injection molding and that in KYKLOS 4.0 project will be manufactured by Additive Manufacturing through the pilot AM Stratoconception owned by CIRTES.

The answers from the PILOTS to the questionnaire have been the following:

- Which interoperability challenges need to be addressed as a priority or are the most challenging?
  - In general, the need to establish a variable pace input system which follows industry standards, to provide a heterogeneous-potentially-unknown-source-capable system with homogeneous, standarised sharing methods, in a resilient way.
  - ASTANDER: The most efficient change of data by change of automatons does not have to start from scratch and automatically recognizes the new data and integrates them. The goa lis to have more data and a better understanding of the cranes that has changed their PLC and integrated sensors.
  - PINDOS: The ability to share information and services between production machines and an integration platform Pindos use case optimizes energy and water consumption. CONECTABLE (Another company) has created a common data model for both use cases with particular rules for each of them.
  - PROMEDICARE: Surely the biggest challenge is represented by the need to manage time for the development of platforms/tools that can allow correct interoperability between the different project partners. Once the different toolkits have been presented, they will then be processed for validation to allow rapid sharing of the data that it intends to carry out. Particular attention was also paid to the regulations that define what data can be shared.
- How are the challenges addressed on project level, or how are these challenges solved pilots by taking into account the particular context and requirements * of the pilots?
  - In general, the challenges are:
    - to know and establish the incoming pace and a definition -model- of the data.
    - To check how these restrictions can fit given the provided resources (templates), either by systems provided by the pilot partner or by us.
    - To test incoming signal values and associated troubleshooting [IL services and tune-up].
  - ASTANDER: FTP data retrieval, ADSYS server, CSV files. Signals have been mapped by ADSYS experts on-premises to iterate on the problems arisen from the bit-wise signals. For partner UPM a subset of signals has been defined, mapped, and tested as well.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

    - PINDOS: MQTT data retrieval, with broker provided by ALGOSYSTEMS, hence the connection parameters; JSON file format. Process has been driven by email exchange with ALGOSYSTEMS – Ioannis to test the links and to define the data layout. Afterwards a tune-up of the signals has been driven. Additional signal and signal values maintenance has been performed (data deletion, addition of specific signals). For partner UPM a subset of signals has been defined, mapped, and tested as well.
- other aspects may be relevant, such as international data exchange challenges, sectoral or cross-sectoral approaches, data resiliency (eg. is blockchain technology). Etc…
    - In general, As for the international data considerations, a particular user has its own date zone and "culture". The date zone allows to have a static reference by treating them as UTC+00, and delivering them as such or depending on the users' preferences. The *culture* affects to those items inherent to each side of the world (commas, etc.). Further than that, each datasource can be configured to follow a set of specific configurations regarding the aforementioned topics. Finally, it is possible to adapt the incoming signals by means of mathematical operations or unit assignation, in a way that they are meaningful to consumers.
    - No quality restrictions have been specified from partners further than security issues. Data processsing is monitorised by the application itself by means of its UI, enhancing quick reaction if problems are detected. The data are delivered via a de-facto standard REST API, using JSON content. A performance document regarding real-time data has been filled up with information from several tests oriented to challenge the extraction capabilities, using the most performant protocol available (MQTT). They have proven to be more than enough not only for the pilots but for the Open Call projects.
    - AVIATION GRC: The most relevant way that these questions relate to the pilot is through interoperability of service and supply chains. This is known to be challenging, especially for assets such as jet engines where the volume is comparatively low, and where the lifetimes of designs and units may span multiple decades. This pilot may be able to benefit from substantial research and standardization activities related to these challenges.
- On which layers or system levels ** do you have to address the interoperability? ** layers could be identified as Asset level **,, Integration level ** , Communication level ** , Information level **, Functional level **, Business level
    - In general, the Rationaleis that data are necessary **assets** to be exploited ideally from a single, reliable source. The IL allows to **integrate** heterogeneous systems by abstacting interested components from data particularities
    - At **communication** level, the IL creates a homogeneous way to interact between components, making them agnostic or semi-agnostic in terms of data exchange
    - At **information** level, the IL leverages data exploitation by making them available to any interested stakeholder, and allowing data owners to check on their gathered data
    - Lastly, from the **functional** level perspective, enables the information exploitation and, therefore, create functionalities considering the data
- ... and also, the hierarchy levels (as indicated in the RAMI 4.0 cube) may be relevant: Product level o Field device level, Control Device level o Station level **, Work Centre level, Enterprise level **, Connected World level **, Edge – fog – cloud. **
    - The Rationale here is:
        - As a control means by allowing to monitor and access the information
        - At an enterprise asset to create the functionalities to exploit the data
        - As connected world for ovbious reasons
        - As a cloud actor to drive the data independently of its origin

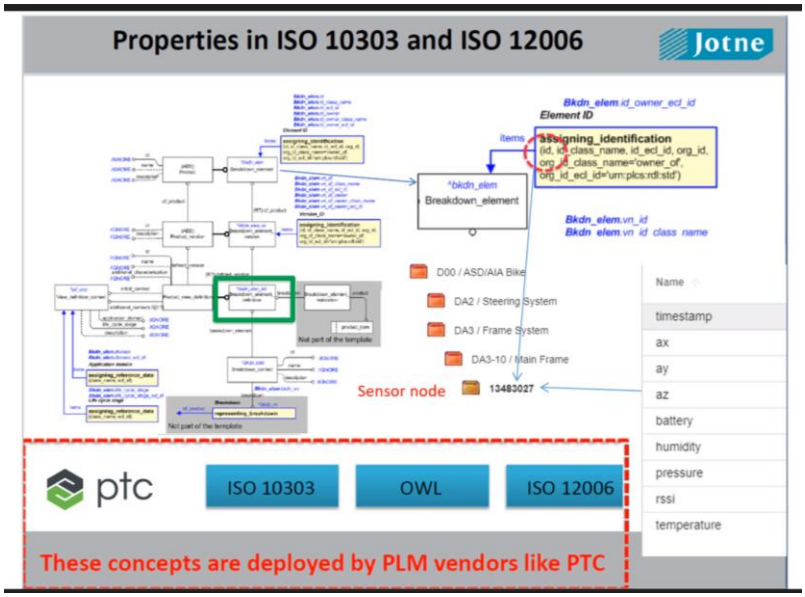
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- Do you use existing (interoperability) frameworks, or do you need to develop new technological solutions?
    - In general, a range of technologies have been used to implement the components and match both needs and existing protocols, first off to communicate with remote systems and later on to gather and process the input data by means of a standalone (visualisation, deployment, components, security) development. Services have been built from scratch with Java and available libraries such as PAHO.
    - PROMEDICARE: New frameworks have been developed for interoperability between the various companies, in which innovative forms of product customization have been introduced within the toolkits and which also allow real-time sharing of the operations carried out within platforms developed ad hoc (an example can be represented by the development of a web editor that allows the development of activities that exploit the AR technology).
- Does the project for instance use previously developed or deployed frameworks (such as ARROWHEAD (used in the FAR-EDGE project), etc…)
    - Project components do not use external frameworks
    - PROMEDICARE: The main frameworks used have been developed or are still under development, in which there is the integration of contents that facilitate the sharing of data between the end user and the company, or even between companies.

No issues have been addressed in Kyklos with:

- Data sovereignty (IDS)
    - KYKLOS will not share data with external companies.
    - GRC: Inside the company. No data sharing
    - PROMEDICARE
        - Not Using patients' critical data
        - Inside the company. No data sharing
- Data ontology and semantics (AAS)
    - DSS data model has been developed using 2 use cases reqs
    - Semantics has not been used
    - STEP information model – semantics built in
    - PLM module- reference data library
        - Module xxxxx store a metamodel of the semantics
            - Translate the company references to standardize references

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- 

- Real time decision making
  - In PINDOS
  - Real time data capture
  - AR deals with real time
    - Data goes through the PLM
    - Problems with data transactions due to network protocols

5.3.5 DIGIPRIME – Digital Platform for Circular Economy in Cross Sectorial Sustainable Value networks.

The following figures present DIGIPRIME approach to interoperability.

Figure 70 shows the relation amongst the company data and the services data through two types of data management, local and global.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

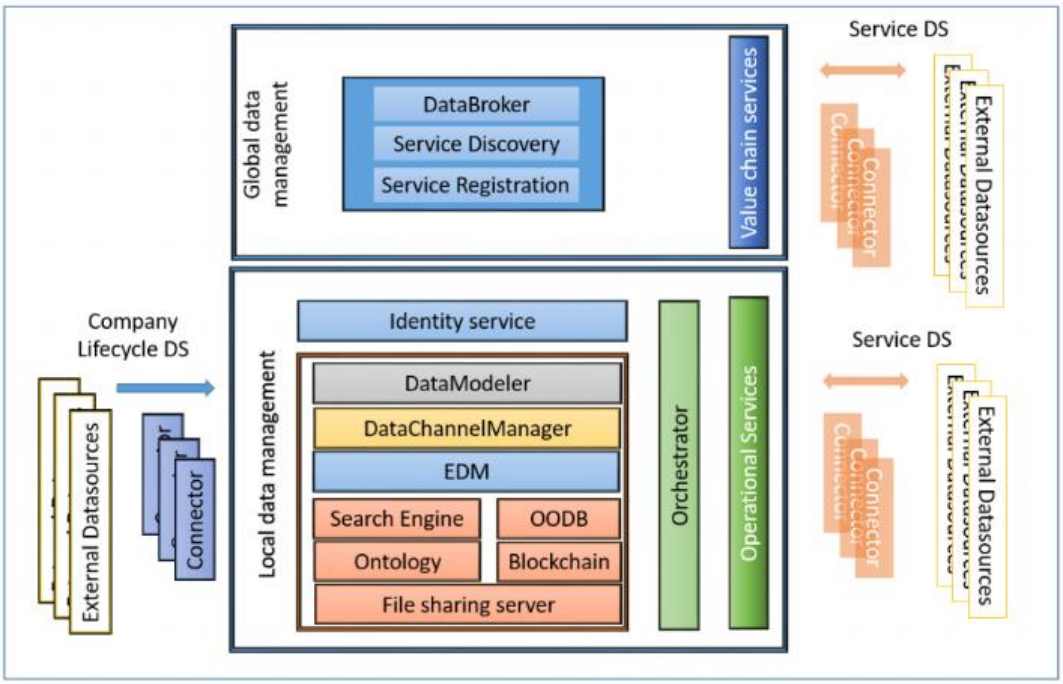


Figure 70: DIGIPRIME data management

Figure 71 presents the relation amongst the remanufacturing processes and the IT layers.

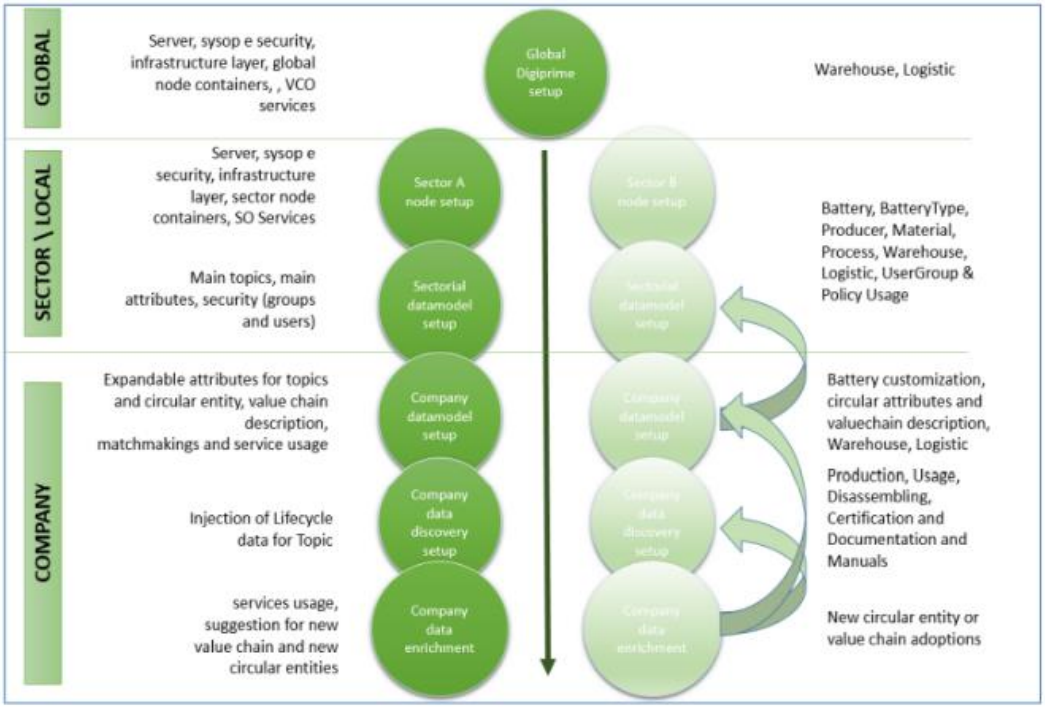


Figure 71 The DigiPrime Data Platform Infrastructure (left picture) and the lifecycle of the DigiPrime data model (right picture)

Figure 72 presents the key components in the interoperability architecture, and how services and data brokers are connected.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

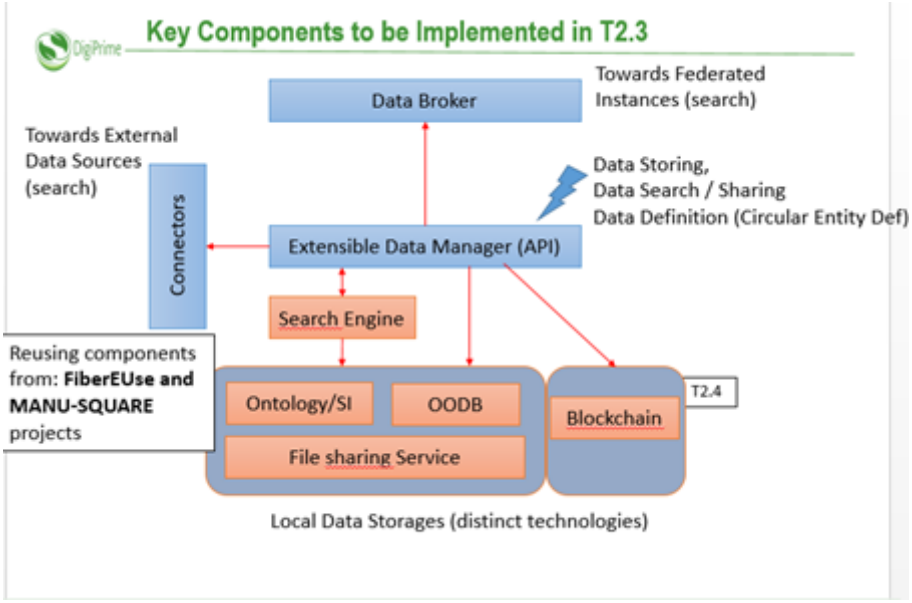


Figure 72: DIGIPRIME key IT components

This picture below (Figure 73) presents the semantic infrastructure overall approach.

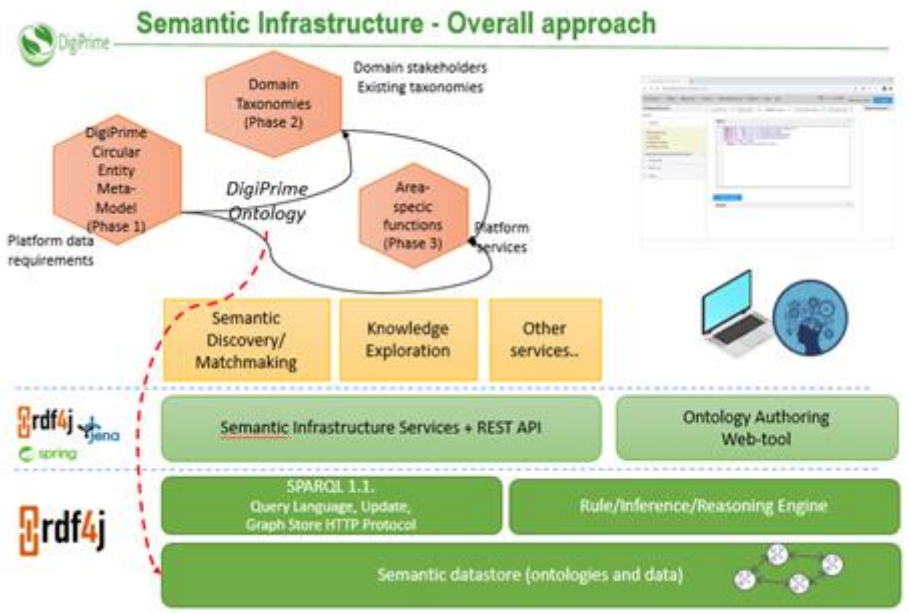


Figure 73: DIGIPRIME semantic infrastructure

At last, the final picture (Figure 74) presents the different applications and services, both operation and value chain services, on open and closed loop, along with the data buses and routing and incorporating security and ledger services.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

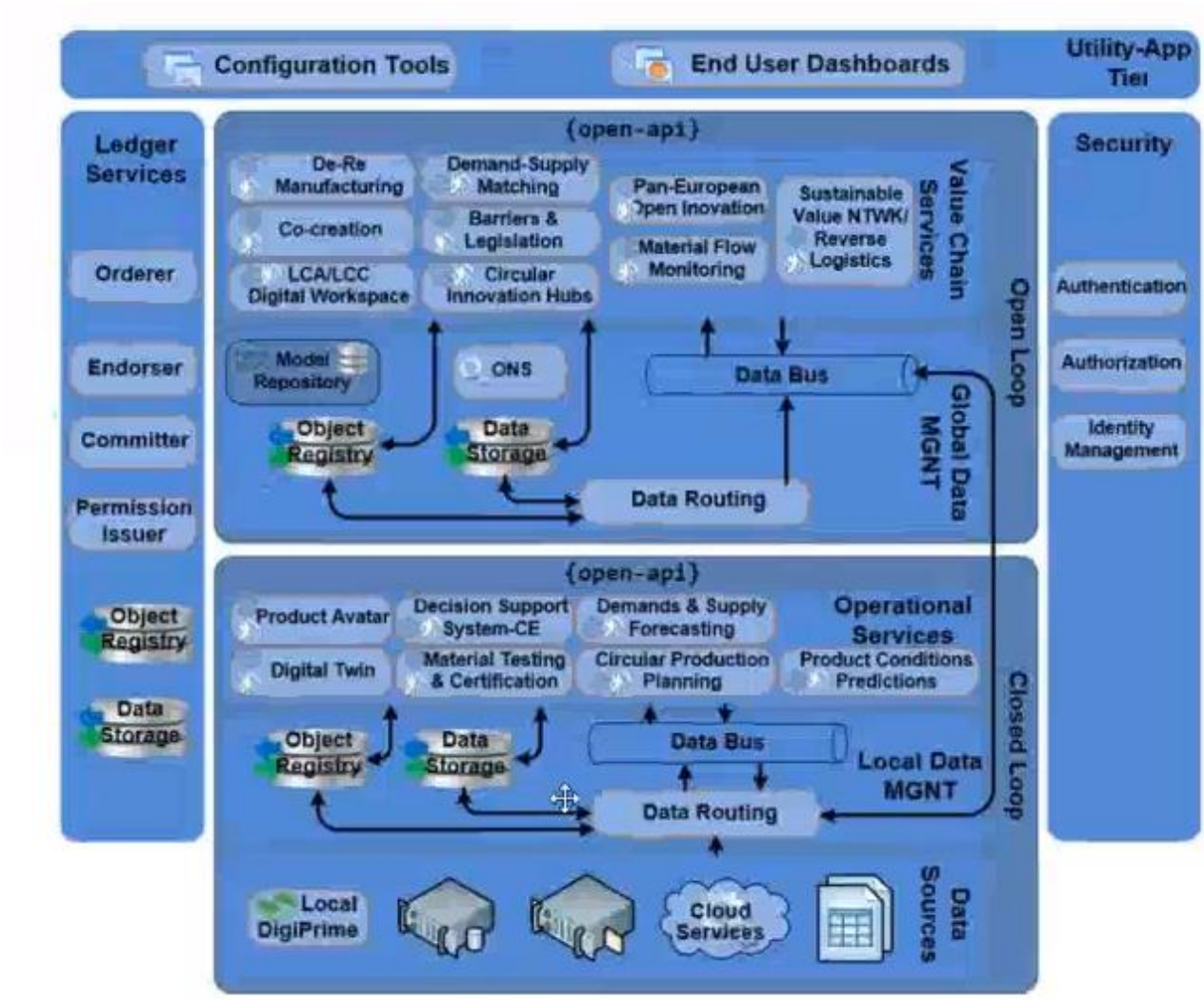


Figure 74: DIGIPRIME services interoperability schema

Relevant Digiprime public deliverables:

- D2.1:Description of the platform architecture and integration guidelines.
- Deliverable 2.2 (Data Models) and D2.3 (Implementation aspects) are confidential

5.3.5.1 Link between ARROWHEAD and DIGIPRIME. Challenges on data interoperability.

Eclipse arrowhead is actually moving on very nicely developing open-source set of services for the digitalization and automation in the different type of factories.

ARROWHEAD has been more focus on the vertical type services, for example building MES systems with nice connexion to business layers, but also Connections to lower layers below underneath the MES.

DIGIPRIME defines very similar concepts being used when it comes to service-oriented architecture and microservices use or industrial automation although DIGIPRIME don't explicitly refer to eclipse but considering microservices was very nicely align with the sort of ideas already in the rest of their project like nimble and other projects in general that have been moving towards this type of Federated platform.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

As an example the contractual interactions and demad supply matchmaking service, where there is a contractual sort of interaction that is heavily influenced and inspired by something called the contract boxes which is one of the eclipse arrowhed services as well, so common ground here is definitely there and microservices use eclipse services like registry orchestration… it's already set the different ways you can make those secure arrowhead use certificates using API keys.

While Arrowhead was more focused on the factory lower layers, DIGIPRIME is more focused on circularity and value chain interactions.

Regarding DATA INTEROPERABILITY, the existing status is that different services are being adapted or configured to fit the different pilot according to deliverable 2.2(not public) defining the data, the data model and how to use polymorphic approaches to address interoperability issues. And D3.2 which is the implementation of semantic data infrastructure for searching and sharing of information.

Probably the biggest challenge on data interoperability has been the definition of a common ontology for all pilots that need to be validated now on WP6, on the Pilots making sure that the services work for the different pilots that will sort of force into this thinking about how does DIGIPRIME actually structure information FOR sharing an interoperability so information interoperability is the challenge. (Semantics)

5.3.6 SHOP4CF – Smart Human Oriented Platform for Connected Factories

ZDMP approach to interoperability will be further analysed in the second half of CF2.

5.3.6.1 SHOP4CF use case introduction.

SHOP4CF has 4 use cases that could be summarized as follow:

1 BOSCH: Support its workers to reduce the error rate
2 Arcelik: Utilisation of AR/VR communication & remote sensing Technologies for Technical Support between Remote Plants of Arçelik
3 SIEMENS: Improve automatic data acquisition, storage, traceability with user-friendly interfaces and human safety
4 Volkswagen: Upfront challenges faced by the assembly workers and engineers

5.3.6.2 SHOP4CF general introduction.

As a general introduction, the main challenges on Interoperability are

- Network connectivity
- Scalability
    - Because all robots are different: kuka, UR,…
    - Using a GUI to configure and scale up.
- Data connectivity amongs different comercial tools

Regarding the focus and goals, SHOP4CF is addressing mainly:

- Human factores

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- Ramp up reduction
- Productivity

Key facts

▪ SHOP4CF wants to simplify the integration of human factors into manufacturing via pre-existing components

▪ The SHOP4CF architecture was designed to ensure interoperability between components using the FIWARE middleware at the communication layer

▪ Interoperability with the asset layer was not foreseen. However, two components are dealing with that Interoperability within SHOP4CF

Initial findings

▪ The SHOP4CF architecture has guarantee interoperability between components in the pilot use cases

▪ The vast amount of use cases uses the degree 3 of the OSI definition focusing in the execution of the use cases

▪ Pilots are open to data sharing and the IDSA architecture is investigated for this matter

As a final general comment, SHOP4CF is keener on using FIWARE central bróker than on MQTT

5.3.6.3 SHOP4CF interoperability approach

Shop4CF will be a human centered platform for designing and deploying human centered manufacturing applications. The cloud-based platform will contain different components to cover a broad spectrum of industrial requirements. The components require very limited programming skills. Expandability / Reconfigurability of the application will be possible in short time through containerization technologies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

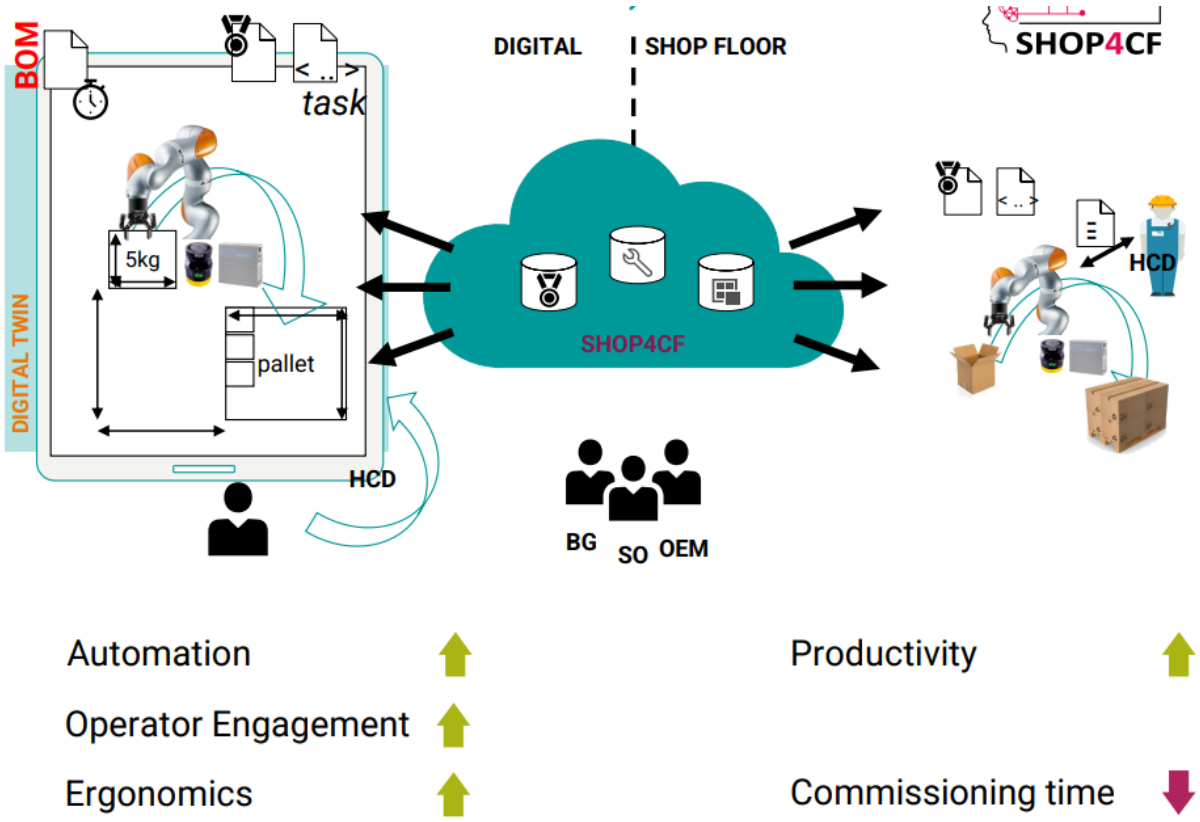


Figure 75: SHOP4CF project sketch

Three vertical layers have been distinguished: Design, Execute and Analyze. Moreover, two horizontal layers have been distinguished: Global and Local. To connect this last two a middleware layer based on Fiware LD is selected. Through this design, the architecture enables a common structure for the SHOP4CF components. See schema below:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

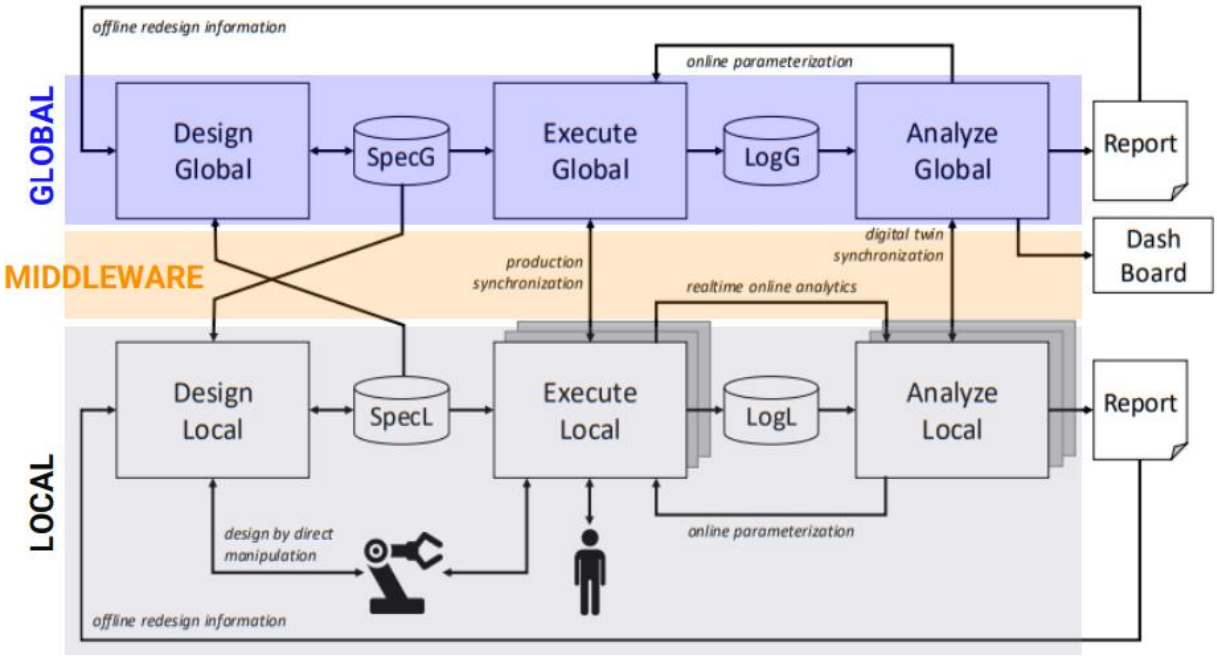
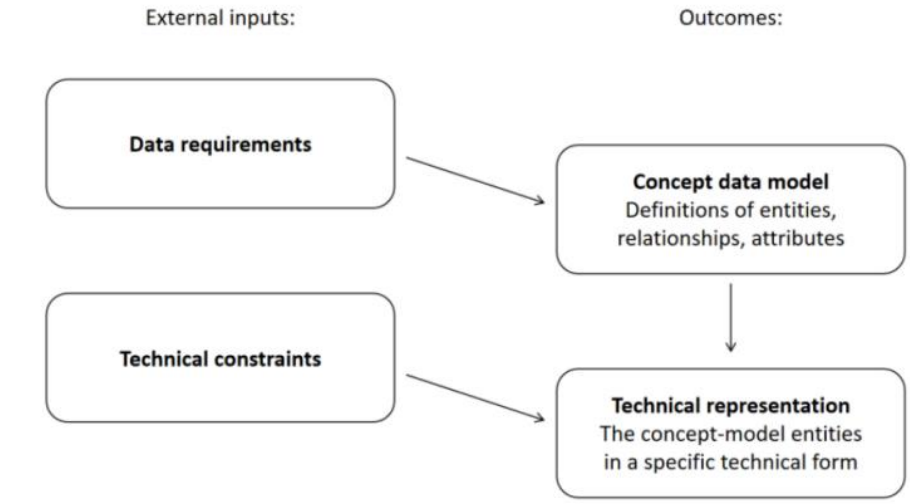


Figure 76: SHOP4CF interoperability concept.

Data models were selected to ensure that mapped SHOP4CF components can communicate between each other easily independently on the implementation language and platform levering the FIWARE middleware. Through this we addressed our main priority which was to have a common understanding between SHOP4CF components (actual and future)

On the following Figure we can visualize the Approach taken for the creation of the data models, at first the data requirements are considered for creating the concept data models. Afterwards, the technical constraints are used to obtain the technical representation based on the concept data model. This approach is based on [1] and has been well documented in the SHOPCF reference architecture deliverable [2].

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.



[31]

Figure 77: Interoperability across components

This modelling ended up in the following data models [1]. The models were selected for representing real manufacturing flows following also the definitions from ISA-95 [2]. However, considering that most components are in the execution layer, only the execution data models were used for the technical representation. Through these data models representation the components can ensure interoperability across them. Examples of the technical representation are in GitHub [3].

Through these data models we can track the lifecycle of assets and resources during production as long entities exist in the context broker.

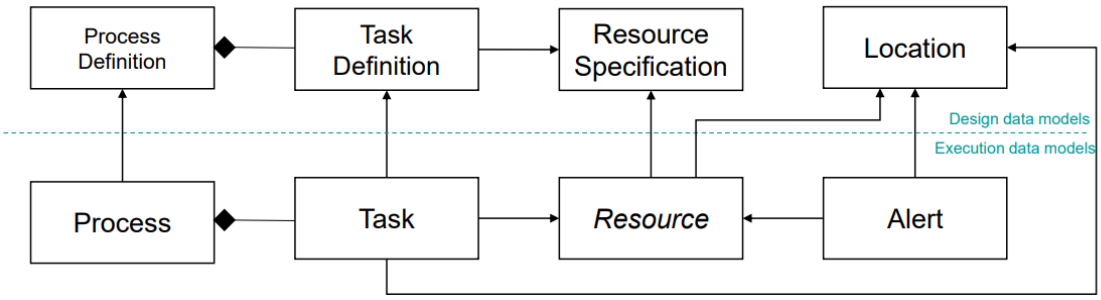


Figure 78: Data models of the SHOP4CF project, in depth description is given in [1]. The data models were inspired by the ISA-95 standard [2

Put of the 30+ SHOP4CF components more than 90% is a software component developed in Linux and containerized through the usage of Docker. Therefore, the selection of Fiware as middleware was a simple way to integrate the different data model while guaranteeing a simple R/W from the components through a

[31] [1] West, Matthew. Developing high quality data models. Elsevier, 2011.

[2] SHOP4CF, Deliverable 3.2 – SHOP4CF architecture, 2021. Available online https://elk.adalidda.com/2021/05/SHOP4CF-WP3-D32-DEL-210119- v1.0.pdf (accessed on 15/06/2022)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

REST API. However, the selection was for the FIWARE LD (Linked Data) version as long it is the version supporting data with context based on the NGSI-LD specification [1].

The usage of REST APIs and the Fiware LD context brokers allowed a almost seamless integration among the different SHOP4CF components. Therefore, targeting the need of the Communication layer considering the RAMI4.0 cub

[32]On the following figure, example of the task data model. The task data model contains important information like which actor should consider the task, its definition and which actor should consider the task. For more information visit [2]


```
{
    "id": "urn:ngsi-ld:Task:company-xyz:im834wyoen78w37",
    "type": "Task",
    "isDefinedBy": {
        "type": "Relationship",
        "object": "urn:ngsi-ld:TaskDefinition:company-xyz:hybrid-transportation-x"
    },
    "involves": {
        "type": "Property",
        "value": [
            {
                "type": "Relationship",
                "object": "urn:ngsi-ld:Device:company-xyz:agv-5"
            },
            {
                "type": "Relationship",
                "object": "urn:ngsi-ld:Person:company-xyz:person-x"
            },
            {
                "type": "Relationship",
                "object": "urn:ngsi-ld:Material:company-xyz:pallet"
            }
        ]
    },
```


Figure 79: SHOP4CF task data model.

The selection of the 30+ SHOP4CF components are tied to specific hardware. Therefore, at a project level effort in making the standardization cross different devices has not been conducted (while this is in evaluation with the project Interopera). Despite this, two components in SHOP4CF aimed to pose some bridges to existing technologies. More specifically for OPCUA and ROS [1]. For the ROS to Fiware communication we have one adapter which translates tasks into ros topics and working with NGSI-LD (the

[32] Sources:

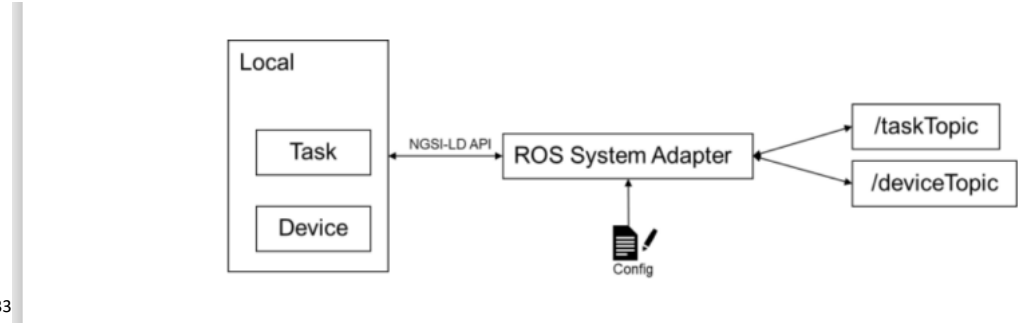
[1] ETSI, ETSI GS CIM 009 V1.4.1 (2021-02), Available online https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.04.01_60/gs_cim009v010401p.pdf (accessed on 15/06/2022)

[2] SHOP4CF, Technical data models, Available online https://github.com/SHOP4CF/data-models (accessed on 15/06/2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

previous ros to Fiware was just for NGSI-v2). For the OPC-UA to ROS we have the WoT component which can migrate any OPC-UA data into Fiware device entities using the OpenAPI W3C [2].

Within the SHOP4CF components, just two are related to the integration of information regarding the asset level.



[33]

Figure 80: Example of the integration between ROS and Fiware. For more information visit [1]

Figure 81: Example of usage of the WoT component. For more information visit [1,2] (source www.w3.org)

OPENNESS TO DATA SHARING

To understand the needs of the pilots and needs for interoperability of the SHOP4CF architecture with existing infrastructures, an open-end question survey was conducted. The survey was integrating questions regarding both general Manufacturing Execution System (MES) information and capabilities of connection. More than half of the pilots would be open to data sharing but defined interfaces for each MES are necessary.

[33] Sources:

[1] SHOP4CF, Deliverable 3.2 – SHOP4CF architecture, 2021. Available online https://elk.adalidda.com/2021/05/SHOP4CF-WP3-D32-DEL-210119- v1.0.pdf (accessed on 15/06/2022)

[2] UPM, WoT component, Available online https://gitlab.lst.tfo.upm.es/shop4cf/wot-il-opc-ua-to-fiware (accessed on 15/06/2022)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

	Yes	No
Open to data sharing	75%	25%
Established supplier connection	75%	25%
MES supports APIs	75%	25%

Table 8: High level results from the SHOP4CF internal pilot interviews

IDSA architecture Integration with FIWARE ORION LD

To overcome the need the IDSA architecture is being tested for the purpose. The architecture will enable the integration of data sharing coming from the FIWARE CB.

FIWARE TRUE Connector (source: fiware-trueconnector.readthedocs.io) is an example of how IDSA can be integrated in FIWARE based systems

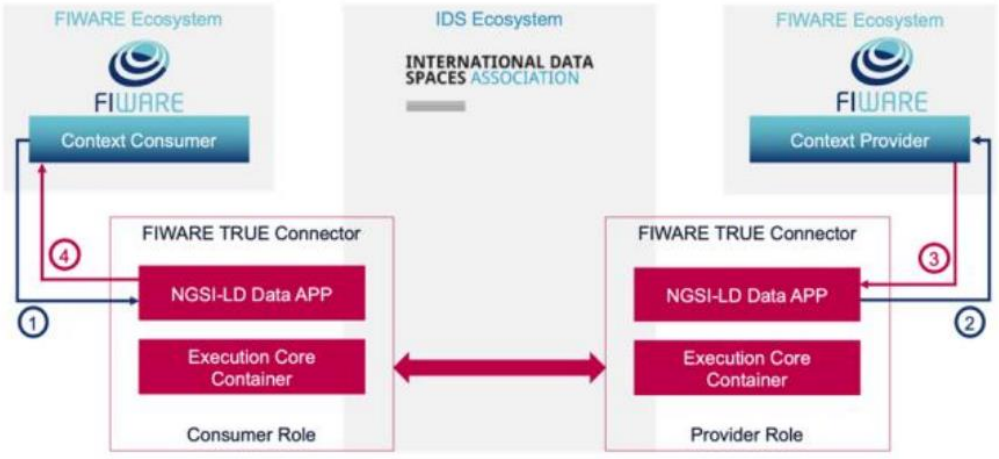


Figure 82: FIWARE true connector

5.3.6.4 SHOP4CF interoperability in the different use cases.

SIEMENS USE CASE

Departs from the ideas that 1.Human operators are flexible 2. Human operators have experience with manufacturing processes 3. Human operators could bridge between automation and requirements for high mix – low volume productions if aided by tools.

The used hardware in this pilot is:

- Linux PC to install docker SHOP4CF apps with local network connection to Fiware CB. More specifically the Linux PC is used for the MPMS. SAG-DOME and SAG-SCAN to interface between Fiware and real hardware. A different Linux PC is used for running Design components
- Camera a simple USB cam to record images
- UR10 robot a UR 10 robot controlled in ROS for the camera movement
- Windows PC to host any windows based SHOP4CF docker apps. More specifically, M2O2P and the MES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- Glove a glove recognizing gestures which is connected via Bluetooth to the windows pc
- PLC for managing a IO-Link gripper and input from laser scanner
- Gripper for taking any parts related to the use case
- Laser scanner to detect operators entering the workspace

The important requirements are:

- Productivity control or visibility/interfaces for human interaction
- Safety

The sub-cases in SIEMENS are:

UC1: Assembly Challenge

- The manufacturing engineer struggles to create manufacturing flows because no tool is available for human robot collaboration
- GOAL: Simplify the way how collaborative manufacturing flows are created for the shopfloor METHODOLOGY: Use a tool to simplify the risk analysis and connected to the MES to get the resource parametrization. Finally, control the robot to avoid collisions
- COMPONENTS: MES, RA, F-TPT, DTS

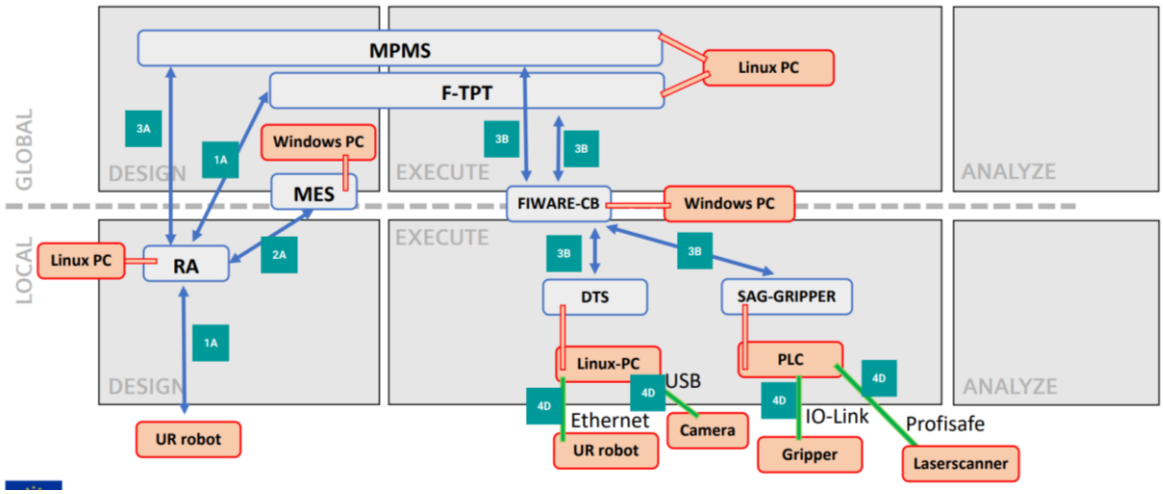


Figure 83: SIEMENS UC1 Architecture adaptation

UC2: SortBot Challenge

- The human operator struggles to program a bin picking system due to complex human-machine interface
- GOAL: Reduce the time to teach a bin picking system application by empowering operators using existing bin picking application
- METHODOLOGY: Use a personalized glove interface to send control commands to the robot to retrieve data for the teaching while ensuring operator safety
- COMPONENTS: M2O2P, SAG-DOME, SAG-SCAN, RA

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

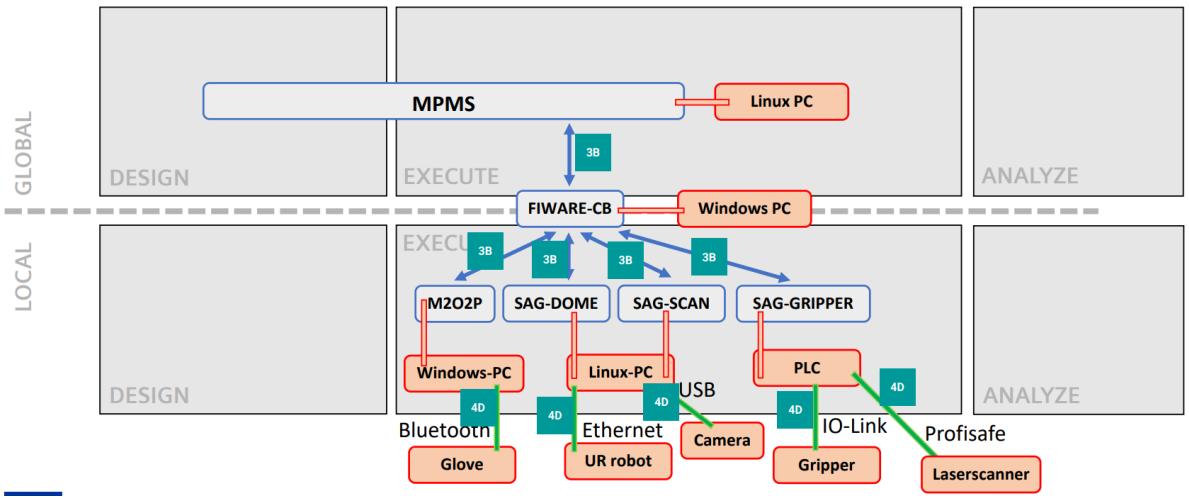


Figure 84: SIEMENS UC2 Architecture adaptation

UC3: Frames Challenge

- The human operator struggles in visualizing the frames of the robot because displayed on a flat display

BOSCH USE CASE

UC1.1: carts that are transported through the production area by the collaborative robot

- GOAL: reduce the non added value time of workers when transferring the finished PCBs manually
- METHODOLOGY: Use a collaborative robot for transporting the PCBs carts avoiding overlaps with the milkrun [1] that circulates in production
- COMPONENTS: F-TPT, HA-MRN, Wi-POS

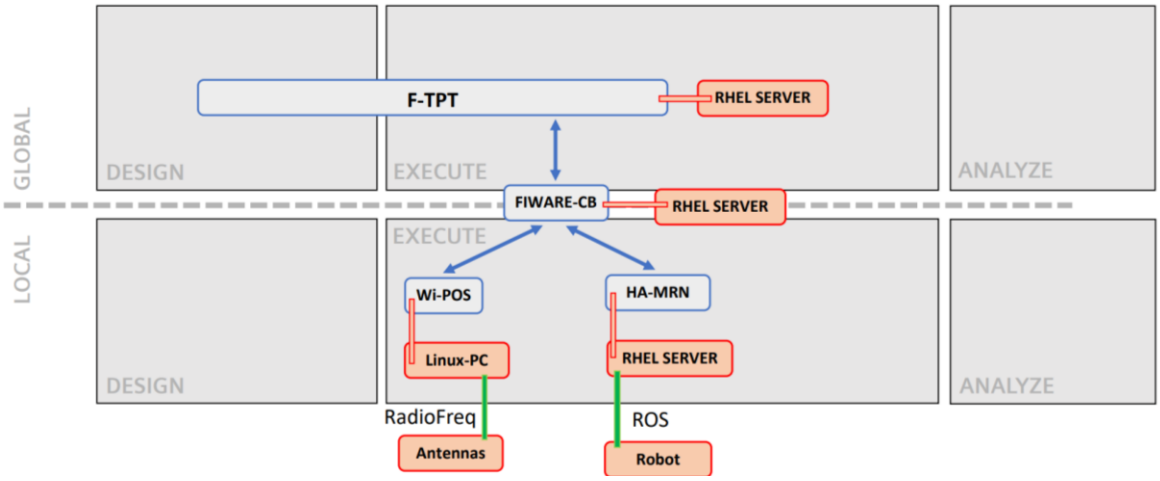


Figure 85: BOSCH UC1.1 Architecture adaptation

UC1.2: manual assembly working station

- GOAL: reduce the cognitive load of the workers while the worker is assembling the PCBs, reducing the risk of errors

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- METHODOLOGY: When the operator scans the PCB to be mounted, the assembly instructions are displayed on the monitor. Afterwards, he places it under the camera and takes the picture, and it will instantly show on the same monitor whether it has been mounted correctly or not.
- COMPONENTS: VQC, AR-CVI, Bosch SW

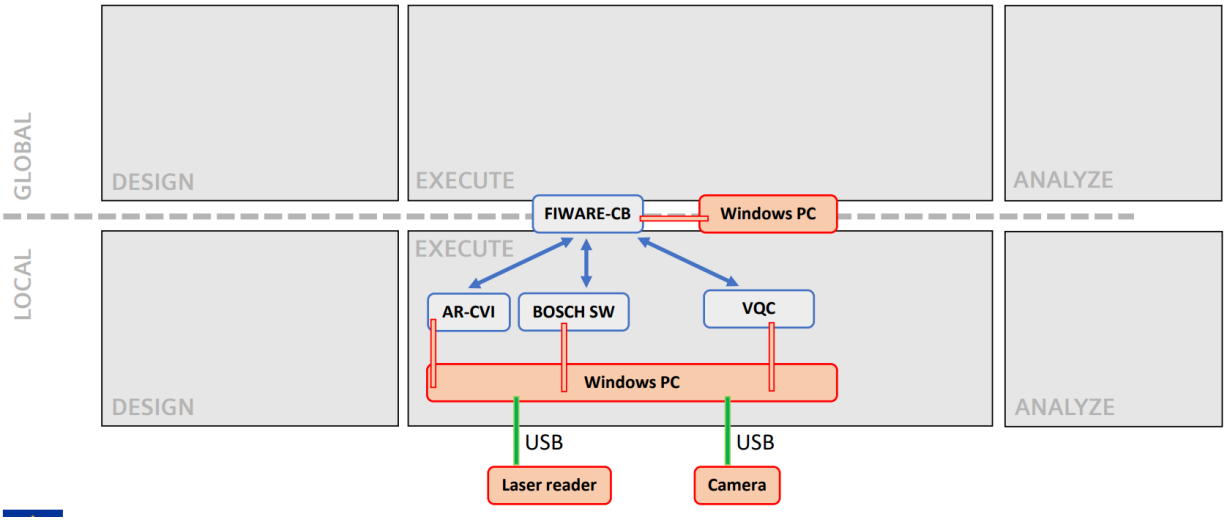


Figure 86: BOSCH UC1.2 Architecture adaptation

The used hardware in this pilot is:

- RHEL server to install docker SHOP4CF apps with local network connection to Fiware CB.
- Linux PC is used for Wi-POS, as we need an equipment to connect the hardware of Wi-POS component.
- Camera a simple USB cam to record PCB images
- Laser reader to scan the PCB DMCs to be assembled
- Windows PC to host any windows based SHOP4CF docker apps. More specifically, VQC, AR-CVI and Fiware CB
- ER-FLEX 250 a collaborative robot formed by an AGV MiR250, a robotic arm UR10e, a calibration camera and a gripper

The important requirements are:

- Productivity control or visibility/interfaces for human interaction
- Particular quality requirements
- Safety

UC2:

- GOAL: To provide the right material to the production lines upon the request. Autonomous mobile robotic solution would relieve the human operator from the tedious loading task
- METHODOLOGY: Use a collaborative robot for feeding the machines based on automatic material request
- COMPONENTS: HA-MRN, MPMS, WoT-IL

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The used hardware in this pilot is:

- RHEL server to install docker SHOP4CF apps with local network connection to Fiware CB.
- ER-FLEX 250 a collaborative robot formed by an AGV MiR250, a robotic arm UR10e, a calibration camera and a gripper
- 2x Linux PC to display MPMS user interface on a touch screen placed at the operator working station

The important requirements are:

- Productivity control or visibility/interfaces for human interaction
- Maintenance control or Real-time requirements
- Safety

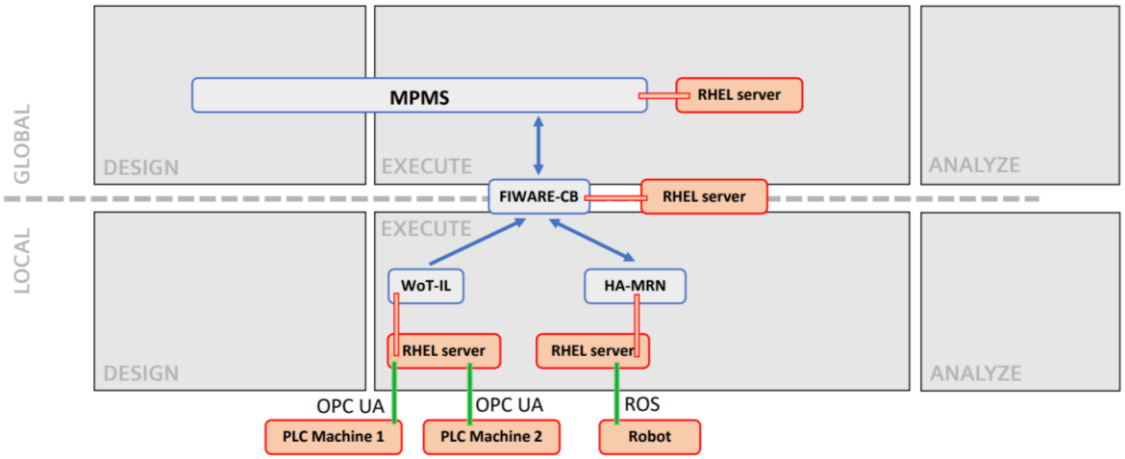


Figure 87: BOSCH UC2 architecture

VOLSKSWAGEN USE CASE

- GOAL: Reduction of time needed to analyze the correctness of body painting in the event of a production disruption.
- METHODOLOGY: Use of ML algorithms used to detect anomalies (quality assessment painting) such as: Autoencoder.
- COMPONENTS: MPMS, FLINT, PMDAI

The used hardware in this pilot is:

1. Windows PC to host any windows based SHOP4CF docker apps

The important requirements are:

2. 1. Greater production awareness
3. 2. Quality

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

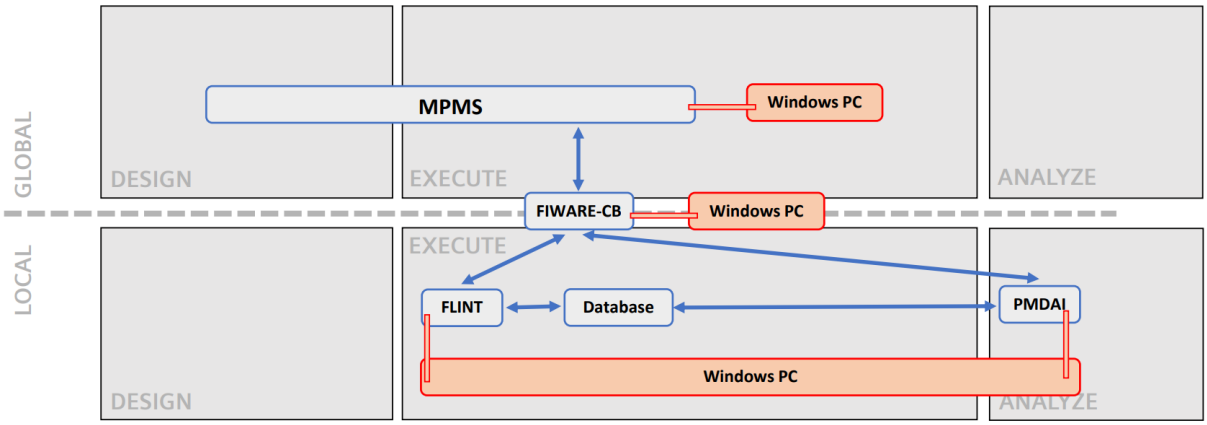


Figure 88: VOLKSWAGEN UC Architecture

ARCELIK USE CASE

- GOAL: Improve the working conditions of operators by preventing overload on assembly lines.
- METHODOLOGY: Data from the communication hardware of the line will be used to detect and address possible issues regarding ergonomics and unbalanced workload.
- COMPONENTS: DCF,DT-CP

The used hardware in this pilot is:

- Linux PC to install docker SHOP4CF apps and Orion context broker with local network connection.
- PLC is used to gather operation data (button and pallet) from shop-floor and broadcast it to the Fiware CB via a web service

The important requirements are:

- Productivity control or visibility/interfaces for human interaction

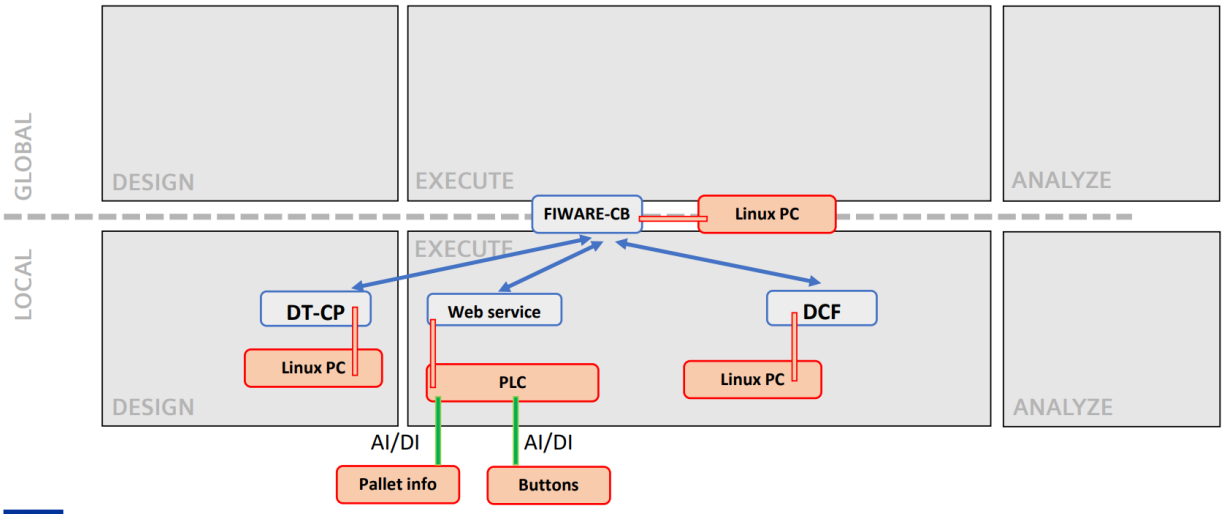


Figure 89: ARCELIK UC Architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

6 CyberSecurity

The role of this task is to ensure that CyberSecurity (CS) challenges are considered and addressed as needed along all the lines of the developments of the Digital Manufacturing Platforms, the Digital Manufacturing Pathways and overall digital manufacturing and Factory of the Future developments and this project.

A CyberSecurity Pathway was also described in the Connected Factories (1) project and the evolved version in D2.6 Pathways cross-fertilisation with Digital Technologies - Second Iteration of this Connected Factories 2 project.

6.1 General observations on cybersecurity

CyberSecurity is a broad and complex domain of interacting technologies that cause individually and in combination vulnerabilities that could lead to adverse effects to the company operating the Digital Platforms or the manufacturing companu and could impact the whole manufacturing chain, the production company, the ecosystem it operates in, the environment, the economies to which it belongs and the society as a whole. CS evolves continuously alongside the developments of Information and Communication Technologies (ICT), on which it is based and to which it has an immediate impact. In manufacturing, CS must be considered for legacy (industrial control systems, PLC, decision support systems, inspection and vision, ERP, product lifecycle management, Manufacturing Execution Systems, …) and other cyberphysical systems. Both are evolving to (Industrial) Internet of Things (IIoT) and utilize both internet, Edge- and Cloud based computing considerations and technologies such as distributed architectures, agile development, virtualization technologies, AI and big data.

CyberSecurity in Digital Manufacturing Platforms in this Report is being considered both from a Risk perspective, from architectural, systems, application and end point perspective trying to protect and preserve both the information flows from availability, integrity, and confidentiality (CIA principle). CS in manufacturing should also preserve impact on the manufacturing itself, but mainly through the protection of the information and commands steering the automation and information and communication systems guiding, managing, and controlling the production systems.

In 2020 and 2021, most harm on production companies was caused by ransomwares, an evolved form of malware that was distributed by email (through phishing attacks, malicious links leading to download and execute these malwares), targeted attacks, USB- and other portable memory, network and system intrusions and trusted supply chains (eg Solarwinds).

These observations suggest the ongoing need and requirement for a transversal approach to CyberSecurity, in the form of a further evolving Pathway, maximally based upon industry leading standard approaches with a view on future approaches whereby considerations of transparent supply chains, shared responsibilities and reliability based upon certified fundamental components and methodologies should be utilized.

In the following Chapters additional documentation can be found on the relevance for Digital Manufacturing from different (developing) standards and de-facto standards, and legislation.

6.2 Relevant documents for Cybersecurity on Digital Manufacturing

The following developments and documents are relevant and important for companies considering Digital Manufacturing. They are and refer to standards (ISO27k) and de-facto standards (IEC62443) and to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Regulatory requirements and ongoing regulatory developments that have a direct and indirect impact on Digital Manufacturing Platforms, digital manufacturing and connected factories, manufacturing operations and the production process.

Most relevant and reference standards and de-facto standards:

1. IEC62443 and derivatives
2. ISO27k series
3. NIST CyberSecurity standards , CSF for Manufacturing Profile and CyberSecurity for Manufacturing standards
4. CSA CAIQ and CSA Cloud Matrix

Most relevant and reference regulatory works and works in progress:

1. Cyber Security Act
    a. Common Criteria
    b. Cloud Service Provider
2. Cyber Resilience Act (under development)
3. NIS2
4. GDPR
5. ePrivacy Regulation (under development)
6. Radio Equipment Directive
7. Revision of the Machine Directive (Machine Regulation under development)
8. AI Act (under development)

6.3 Most relevant and reference standards and de-facto standards

6.3.1 IEC62443 and derivates

The ISA/IEC 62443 series of standards **define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS**). These standards set **best practices for security** and provide a way to assess the level of security performance. Their approach to the cybersecurity challenge is a **holistic** one, bridging the gap between operations and information technology as well as between process safety and cybersecurity.

The ISA/IEC 62443 standards are submitted to the International Electrotechnical Commission (IEC) for global adoption as international standards ISA/IEC 62443. The ISA/IEC 62443 series of standards are endorsed by the United Nations. With use cases from more than 20 different industries, the ISA/IEC 62443 series of standards have demonstrated their utility in all industry verticals that use operational technology. In 2021, IEC recognized the series as a horizontal standard, meaning that the standards have been proven to apply to a broad range of different industries.

The final published documents are available from both IEC and ISA. The ISA editions of the standards and reports in the series have a naming convention written as “ISA-62443-x-y,” while the IEC Editions appear as “IEC 62443-x-y.” The ISA and IEC editions of each document are identical, however, and both are released as concurrently as possible.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

The following are the **published ISA-62443 standards and technical reports relevant for Digital Manufacturing and Connected Factories**:

- ISA-TR99.00.01-2007, Security technologies for industrial automation and control systems
- ISA-62443-1-1-2007, Security for industrial automation and control systems, Part 1-1: Terminology, concepts, and models
- ISA-62443-2-1-2009, Security for industrial automation and control systems, Part 2-1: Establishing an industrial automation and control systems security program
- ISA-TR62443-2-3-2015, Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment
- ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT)
- ANSI/ISA-62443-3-2-2020, Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design
- ANSI/ISA-62443-3-3-2013, Security for industrial automation and control systems, Part 3-3: System security requirements and security levels
- ANSI/ISA-62443-4-1-2018, Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements
- ANSI/ISA-62443-4-2-2018, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components

The "Technical Security requirements for IACS components" provides the most practical suggestions for technical measures to be put in place for CyberSecurity in Digital Manufacturing:

1. Identification and authentication control purpose and SL-C(IAC) descriptions
    a. Human user identification and authentication
    b. Software process and device identification and authentication
    c. Account management
    d. Identifier management
    e. Authenticator management
    f. Wireless access management
    g. Strength of password-based authentication
    h. Public key infrastructure certificates
    i. Strength of public key-based authentication
    j. Authenticator feedback
    k. Access via untrusted networks
    l. Strength of symmetric key-based authentication
2. Use control
    a. …
    b. Auditable events
    c. Use of physical diagnostic and test interfaces
    d. Security functionality verification
    e. integrity
3. System integrity
    a. …
    b. Input validation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

   c. Deterministic output
   d. Error handling
   e. Session integrity
4. Data confidentiality
   a. Information confidentiality
   b. Information persistence
   c. Use of cryptography
5. Software application requirements
6. Embedded device requirements
   a. Mobile code
   b. Use of physical diagnostic and test interfaces
   c. Protection from malicious code
   d. Support for updates
   e. Physical tamper resistance and detection
   f. Provisioning product supplier roots of trust
   g. Provisioning asset owner roots
   h. Mapping of CRs and REs to FR SL levels 1 -4
7. Network device requirements
   a. …
   b. Wireless access management
   c. Access via untrusted networks
   d. Use of physical diagnostic and test protection from malicious code
   e. Support for updates
   f. Physical tamper resistance and detection
   g. Provisioning product supplier roots of trust
   h. Provisioning asset owner roots of trust
   i. Integrity of the boot process
   j. Zone boundary protection
   k. General purpose, person-to-person communication restrictions

6.3.2 IS027000 and derivates

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an **information security management system** within the context of the organization. It also includes **requirements for the assessment and treatment of information security risks tailored to the needs of the organization**. The requirements set out in ISO/IEC 27001:2013 are **generic** and are intended to be applicable to all organizations, regardless of type, size or nature.

This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as: 1) Security requirements capture methodology; 2) Management of information and ICT security; in particular information security management systems, security processes, and security controls and services; Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information; 3) Security management support documentation including terminology, guidelines as well as procedures for the registration of security components; 4) Security aspects of identity management, biometrics and privacy; 5) Conformance assessment, accreditation and auditing requirements in the area of information security management systems; 6) Security evaluation criteria and methodology.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

6.3.3 NIST CyberSecurity standards and CyberSecurity for Manufacturing standards

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges.

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity.

6.3.3.1 NIST CyberSecurity Framework

The NIST CyberSecurity Framework (CSF) was first published in 2014 after a year-long, collaborative process in which NIST convened industry, academia, and government stakeholders. The CSF is now widely viewed as foundational to securing organizations and technology, because it provides a common vocabulary for the cybersecurity community. NIST moves to CSF 2.0.

The **voluntary Framework** consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

The Framework Core and Informative References are available as separate downloads in two formats: spreadsheet (Excel) , and alternate view (PDF). A companion Roadmap discusses future steps and identifies key areas of cybersecurity development, alignment, and collaboration.

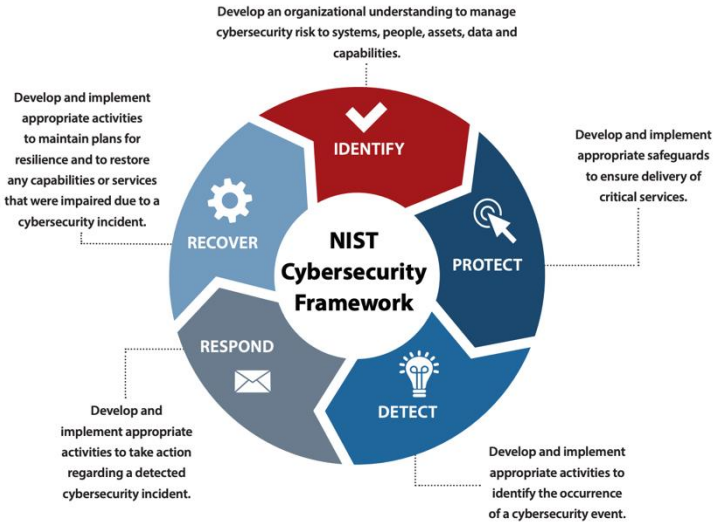


Figure 90 : the NIST CS framework is widely used in the CyberSecurity industry as a reference model to be able to maintain a full scope of CyberSecurity activities, which are necessary also for manuyfacturing companies to consider, in the derivate NISTIR 8183 (see below) CyberSecurity Framework for Manufacturing Profile, this is applied to manufacturing companies.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

6.3.3.2 NIST CyberSecurity Framework for Manufacturing Profile (NISTIR 8183)

NISTIR 8183[34] is the Cybersecurity Framework (CSF) implementation details developed for the manufacturing environment. The "Manufacturing Profile" of the Cybersecurity Framework can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices. This Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing. The latest version dates from October 2020 but is still relevant and provides an excellent baseline for manufacturing companies that aim to embrace CyberSecurity in their organization.

Draft NISTIR 8183
Revision 1

Cybersecurity Framework Version 1.1
Manufacturing Profile

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Management
PR	Protect	PR.AC	Identity Management, Authentication and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 91 : NIST CS Framework Manufacturing Profile - NISTIR 8183

The Framework provides the basic Identify, Protect, Detect, Respond and Recover CyberSecurity functions allowing manufacturing companies to ensure a better handle on potential incidents and risks. The manufacturing profile takes this framework and applies it so the five Framework functions can be performed **concurrently** and **continuously** to form an operational culture that addresses the **dynamic cybersecurity risk**. The Profile was developed to be an actionable approach for implementing the CSF customized to the manufacturing domain using relevant informative references. Control Objectives for Information and Related Technologies (COBIT) 5 is sourced for subcategories that have no corresponding 800-53 or ISA/IEC 62443 references. Additional input came from NIST SP 800-82, Rev. 2, both in section 6.2 (Guidance on the Application of Security Controls to ICS) and in Appendix G (ICS Overlay) [3]. For informative references to an entire control family or set of controls (such as subcategory ID.GV-1's informative reference to all "policy and procedures" controls), the approach took a holistic view of the controls comprising the family/set. It provides a **customized CSF subcategory language** developed using informative references relevant to the manufacturing domain, some examples :

- ID.AM-3 : Document all connections within the manufacturing system, and between the manufacturing system and other systems. All connections are documented, authorized, and reviewed. Connection information includes, for example, the interface characteristics, data characteristics, ports, protocols, addresses, description of the data, security requirements, and the nature of the connection.
- ID.SC-3 : Implement contractual cybersecurity requirements for suppliers and third-party partners requiring access to sensitive information or providing information technology, operational technology, services, technology-based input products, or non-technology-based input products

[34] https://csrc.nist.gov/publications/detail/nistir/8183/rev-1/final

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

supporting the manufacturing system. Cyber supply chain risk assessment results should be used in the development of cybersecurity requirements.

- PR.DS-5 : Protect the manufacturing system against data leaks. Monitor the manufacturing system at the external boundary and at key internal points to detect unauthorized access and use. Develop and document access agreements for all users of the manufacturing system.
- …

The Profile expresses tailored values for cybersecurity controls for the manufacturing system environment. These represent the application of the Categories and Subcategories from the Framework based on domain-specific relevance, business drivers, risk assessment, and the manufacturer's priorities. Users of the Profile can also add Categories and Subcategories as needed to address unique and specific risks.

6.3.3.3 NIST 1800-10B CyberSecurity for Manufacturing (Industrial Control Systems) standards

Documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

Cybersecurity guidance that empowers manufacturers to protect their operations from data integrity attacks in Industrial Control System environments. To keep a competitive edge, manufacturers are connecting their operational technology (OT) systems to their information technology (IT) systems. While integrating IT and OT networks has helped manufacturers boost productivity and gain efficiencies, it has also made them more vulnerable to cybersecurity threats posed by malicious actors.

Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. The solutions implement standard cybersecurity capabilities such as behavioral anomaly detection (BAD), application allow listing (AAL), file integrity-checking, change control management, and user authentication and authorization. The solution was tested in two distinct lab settings: a discrete manufacturing work cell, which represents an assembly line production, and a continuous process control system (PCS), which represents chemical manufacturing industries.

An organization that is interested in protecting the integrity of a manufacturing system and information from destructive malware, insider threats, and unauthorized software should first conduct a risk assessment and determine the appropriate security capabilities required to mitigate those risks. Once the security capabilities are identified, the sample architecture and solution presented in this document may be used.

A Mapping of Device Cybersecurity Capabilities and Nontechnical Supporting Capabilities to NIST Cybersecurity Framework Subcategories of the ICS Project is a Table in the document referring to Device Cybersecurity Capabilities and linking them with CSF Subcategories. The list runs over 100 pages, and allows for reference checking with Digital Manufacturing Platforms Cybersecurity Capabilities.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

6.4 Most Relevant regulatory works and relevant regulatory works in progress

6.4.1 EU Cybersecurity Act

The Cybersecurity Act creates a framework for EU certification schemes that are only voluntary and not mandatory. The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services and processes. Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognized across the European Union. The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. The framework will be based on agreement at EU level on the evaluation of the security properties of a specific ICT-based product or service. It will attest that ICT products and services that have been certified in accordance with such a scheme comply with specified requirements.

The assurance levels are used to inform users of the cybersecurity risk of a product, and can be basic, substantial, and/or high. They are commensurate with the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident. A high assurance level would mean that the certified product passed the highest security tests. The resulting certificate will be recognized in all EU Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

6.4.2 Cyber Resilience Act (under development)

The Radio Equipment Directive and the Medical Devices Regulation cover only certain types of products, leaving the vast majority of digital products without any cybersecurity guidelines. Current legislation does not address non-embedded software products and does not prescribe cybersecurity requirements that cover the whole product lifecycle.

The initiative aims at ensuring that vendors put in place adequate cybersecurity safeguards on the digital products they sell. By providing cybersecurity requirements before and after a product is placed on the market, the CRA will strengthen security and resilience of whole supply chains for the benefit of companies and final consumers.

During the State of the Union (SOTEU) address of 15 September 2021, the President of the European Commission Ursula von der Leyen announced a “European Cyber Resilience Act to establish common cybersecurity standards for products”, now being transformed into a legislative draft by DG CNECT.H.2. Objective of the proposal is to create a horizontal legislation to define common European cybersecurity standards for [digital] products and [ancillary] services that are placed on the EU internal market

6.4.3 NIS2 (under development) : Networks & Information Security Directive

NIS2 is a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (the NIS Directive). The NIS directive mainly establishes cybersecurity requirements for operators of essential services. The NIS2 Directive (EU) 2022 sets additional measures.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

This Directive applies to public and private entities of a type referred to as essential entities in Annex I (from NIS 1) and as important entities in Annex II (the extended list of NIS 2, such as Manufacture, production and distribution of chemicals, Food production, processing and distribution, Manufacture of medical devices and in vitro diagnostic medical devices, Manufacture of computer, electronic and optical products, Manufacture of electrical equipment, Manufacture of machinery and equipment n.e.c., Manufacture of motor vehicles, trailers and semi-trailers, Manufacture of other transport equipment, Providers of online marketplaces, …). This Directive does not apply to entities that qualify as micro and small enterprises (but there are exceptions). Regardless of their size, this Directive also applies to entities : … where (c) the entity is the sole provider of a service in a Member State; (d) a potential disruption of the service provided by the entity could have an impact on public safety, public security or public health; (e) a potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact; (f) the entity is critical because of its specific importance at regional or national level for the particular sector or type of service, or for other interdependent sectors in the Member State …

There is still a level of discretion by the Member States in the implementation, but it is clear that companies related to Digital Manufacturing platforms (either exploiting or operating them) could be impacted by NIS2, and will have to abide by its directions.

Those computing resources include resources such as networks, servers or other infrastructure, operating systems, software, storage, applications and services. The service models of cloud computing include, amongst others, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS) and Network as a Service (NaaS).

Cybersecurity risk management and reporting obligations need to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. They shall include at least the following: (a) risk analysis and information system security policies; (b) incident handling; (c) business continuity, such as backup management and disaster recovery, and crisis management; (d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures ▌to assess the effectiveness of cybersecurity risk management measures; (fa) basic computer hygiene practices and cybersecurity training; (g) policies and procedures regarding the use of cryptography and, where appropriate, encryption; (ga) human resources security, access control policies and asset management; (gb) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate.

Essential and important entities need to **notify**, without undue delay, the **CSIRT** or, where relevant, the **competent authority of any incident having a significant impact on the provision of their services.** Entities need to use particular **ICT products, services and processes**, either developed by the essential or important entity or procured from third parties, that are **certified** under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881, to use **qualified trust services** pursuant to Regulation (EU) No 910/2014.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Entities should address cybersecurity risks stemming from their interactions and relationships with other stakeholders within a broader ecosystem, including to counter industrial espionage and to protect trade secrets. Similarly, given the importance and value of data for the activities of the entities, when relying on data transformation and data analytics services from third parties, the entities should take all appropriate cybersecurity measures. (art 45)

Entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, and organise training for their staff, and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine learning systems to enhance their capabilities and the protection of networks. (art 45b)

In duly justified cases where the competent authority is aware of a significant cyber threat or a pending risk, the competent authority should be able to take immediate enforcement decisions with the aim to prevent or respond to an incident. (art 70d).

6.4.4 GDPR : General Data Protection Regulation

Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. This text includes the corrigendum published in the OJEU of 23 May 2018. The regulation strengthesn individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market. This single European Regulation reduces fragmentation in different national systems and removes unnecessary administrative burdens. The regulation entered into force on 24 May 2016 and applies since 25 May 2018. Rules for business and organisations, how they must do to comply with EU data protection rules and how companies can help citizens exercising their rights under the regulation is complex, but extensively documented.

6.4.5 ePrivacy

New players: privacy rules will in the future also apply to new players providing electronic communications services such as WhatsApp, Facebook Messenger and Skype. This will ensure that these popular services guarantee the same level of confidentiality of communications as traditional telecoms operators.

Stronger rules: all people and businesses in the EU will enjoy the same level of protection of their electronic communications through this directly applicable regulation. Businesses will also benefit from one single set of rules across the EU.

Communications content and metadata: privacy is guaranteed for communications content and metadata. Metadata — data that describes other data, such as author, date created and location— has a high privacy component and should be anonymised or deleted if users did not give their consent, unless the data is needed for billing.

New business opportunities: once consent is given for communications data to be processed, traditional telecoms operators will have more opportunities to provide additional services and to develop their

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

businesses. For example, they could produce heat maps indicating the presence of individuals. These could help public authorities and transport companies when developing new infrastructure projects.

Simpler rules on cookies: the cookie provision, which has resulted in an overload of consent requests for internet users, will be streamlined. The new rule will be more user-friendly as browser settings will provide an easy way to accept or refuse tracking cookies and other identifiers. The proposal also clarifies that no consent is needed for non-privacy intrusive cookies that improve internet experience, such as cookies to remember shopping-cart history or to count the number of website visitors.

Protection against spam: this proposal bans unsolicited electronic communications by email, SMS and automated calling machines. Depending on national law people will either be protected by default or be able to use a do-not-call list to stop marketing phone calls. Marketing callers will need to display their phone number or use a special prefix that indicates a marketing call.

More effective enforcement: the enforcement of the confidentiality rules in the Regulation will be the responsibility of data protection authorities, already in charge of the rules under the GDPR.

6.4.6 Revision of the Machine Directive

The machinery directive 2006/42/EC was published on 9 June 2006 and became applicable on 29 December 2009. It was amended by Directive 2009/127/EC of the European Parliament and of the Council of 21 October 2009, with regard to machinery for pesticide application, and by Regulation (EU) No 167/2013 of he European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles, among others.

On 21 April 2021, the Commission put forward a proposal for a new Regulation on machinery products, as part of a wider 'AI package'. The proposal on machinery products addresses several problems identified in the current EU framework: insufficient coverage of new risks stemming from the new digital technologies (such as AI, the IoT and robotics); insufficient coverage for 'high risk machines'; inconsistencies with other pieces of product-safety legislation; and divergences in interpretation across Member States due to transposition (hence the choice of a Regulation instead of a Directive). The proposed new regulation will ensure the safe integration of AI systems into machines and thus encourage innovation. The aim of this proposal is to improve and adapt the existing Machinery Directive to the new needs of the market and risks originating from emerging technologies, such as Digital Platforms. One of the major resulting aspects is the definition of safety component has been clarified to include non-physical components such as software. This proposal contains only a marginal part of cybersecurity about the safety aspect linked with the correct functioning of machines' software. But the proposal is coherent with and complementary to other EU legislation on AI and cybersecurity, making the link with the cybersecurity certification schemes of the Cyber Security Act of 20194 and the AI Act. The consideration is that if the product is certified by a cybersecurity scheme under the Cyber Security Act, it is also compliant for this regulation. However, there is a consideration for high-risk machinery.

6.4.7 Radio Equipment Directive

The delegated act to the Radio Equipment (in October 2021) aims to make sure that all wireless devices are safe before being sold on the EU market. This act lays down new legal requirements for cybersecurity safeguards, which manufacturers will have to take into account in the design and production of the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

concerned products. It will also protect citizens' privacy and personal data, prevent the risks of monetary fraud as well as ensure better resilience of our communication networks.

The measures proposed cover wireless devices such as mobile phones, tablets and other products capable of communicating over the internet. The new measures will help to 1) Improve network resilience: Wireless devices and products will have to incorporate features to avoid harming communication networks and prevent the possibility that the devices are used to disrupt website or other services functionality. 2) Better protect consumers' privacy: Wireless devices and products will need to have features to guarantee the protection of personal data. 3) Manufacturers will have to implement new measures to prevent unauthorised access or transmission of personal data. 4) Reduce the risk of monetary fraud: Wireless devices and products will have to include features to minimise the risk of fraud when making electronic payments. For example, they will need to ensure better authentication control of the user to avoid fraudulent payments.

6.4.8 Artificial Intelligence (AI) Act (under development)

Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Artificial Intelligence (AI) is a fast evolving family of technologies that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities. AI can also bring about new risks or negative consequences for individuals or the society. It is legislation for a coordinated European approach on the human and ethical implications of AI. The current proposal presents a balanced and proportionate horizontal regulatory approach to AI that is limited to the minimum necessary requirements to address the risks and problems linked to AI, without unduly constraining or hindering technological development or otherwise disproportionately increasing the cost of placing AI solutions on the market.

The objectives of the proposal are 1) to ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values, 2) to ensure legal certainty to facilitate investment and innovation in AI, 3) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems, 4) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

The Commission proposed to enshrine in EU law a technology-neutral definition of AI systems. The Commission proposes as well to adopt different set of rules tailored on a risk-based approach with four levels of risks: 1) Unacceptable risk AI : harmful uses of AI that contravene EU values (such as social scoring by governments) will be banned because of the unacceptable risk they create. 2) High-risk AI: a number of AI systems (listed in an Annex) that are creating adverse impact on people's safety or their fundamental rights are considered to be high-risk. In order to ensure trust and consistent high level of protection of safety and fundamental rights, a range of mandatory requirements (including a conformity assessment) would apply to all high-risks systems. 3) Limited risk AI: some AI systems will be subject to a limited set of obligations (e.g. transparency). 4) Minimal risk AI: all other AI systems can be developed and used in the EU without additional legal obligations than existing legislation.

In the current Annex, the following Manufacturing and related applications are being considered of High Risk: (a) Biometric identification and categorisation of natural persons: AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons; (b) Management and operation of critical infrastructure: AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity; (c) Education and vocational training: (a) AI systems intended to be used for the purpose of determining access or assigning natural

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

persons to educational and vocational training institutions; (d) Employment, workers management and access to self-employment: AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

Those AI systems will have to comply with a set of horizontal mandatory requirements for trustworthy AI and follow conformity assessment procedures before those systems can be placed on the Union market. Predictable, proportionate and clear obligations are also placed on providers and users of those systems to ensure safety and respect of existing legislation protecting fundamental rights throughout the whole AI systems' lifecycle.

6.5 Examples from projects (mapping of projects)

Attemps have been undertaken to both provide and collect examples towards and from a diversity of projects working on CyberSecurity in manufacturing, and projects which are working on CyberSecurity having a spillover effect on CyberSecurity for manufacturing. This is an ongoing process, but is already happening.

6.5.1 CS standards for projects to consider

As part of the focus of the Digital Manufacturing Platforms interactions, the CyberSecurity track and this task has been identifying and compiling different applicable standards which are being applied by manufacturers, technology providers and research projects working towards cybersecuring the environment and looking to apply existing methodologies, policies and technological standards which they can relate to. Some of the listed standards were presented to the projects and have been both selected and expanded by different project partners and their respective coordinators.

Not all projects under the Digital Manufacturing Platforms (DT-ICT-07-2018-2019) have already contributed to the following lists or overviews since a number of them are still in progress of development, however participating in the collaboration activities of the CF2 project.

1. International industrial CS standard developments : IEC62443, NIST, CSA, …
2. European industrial CS standard developments : CEN/CENELEC, RED, Machiner Directive, GDPR, ETSI IoT, CyberAct, ..
3. De-Facto standards : Industrial IoT CS Framework, Industry4.0, IDSA, Platform I4.0 WG Sicherheit, RAMI Security model developments, CSA Taking Control of IoT, OWASP, OPC – OPC/UA, SROS, …
4. Industry specific
    a. User orientation driven – Sector oriented (process industry / aerospace / energy) : Namur, WG 4.18 Automation Security, EEMUA, WIB,
    b. Technology orientation driven (IoT / cloud / OPC / Web application / …)
    c. Cybersecurity technology (TLS / HTTPS /
5. Non-industry-specific
    a. Standard organisation driven : NIST / ISO / IEC / CEN-CENELEC
    b. Regulated : NIS / GDPR / CIP
6. Governmental – regulated
    a. Sector Specific : nuclear, air traffic, health, telecom, …
    b. Country specific – Member State specific: Grundschutz, BSI, …

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

7. New approaches :
    a. Software Bill of Materials – SBOM,
    b. Reference Integrity Manifest – RIM, & RIMM,
8. Cybersecurity specific Vulnerability databases & Responsible Disclosure information sharing …

6.5.2 CS standards, standardisation participation – cross project analysis (part 2)

Standards can be important for organizations to save costs, be better aligned to facilitate cooperations and learn from best practices from others. Standards can also be a burden and a challenge to adhere to, trying to be compliant following methodologies which could be much heavier for smaller organisations with limited resources and expertise.

The CF2 project had the intention to first do stock-taking of available and relevant standards, to support the different projects in their choice, but equally asking the various projects which standards they have been considering for the execution of their developments. During the interactions, projects can learn from each other's experiences and improve on the results being achieved from those developments. The first table indicates the assessment done by the CF2 project on the various CS standards the respective projects have considered, or are following with additions thanks to the contributions by the projects. This table will be further enhanced and completed, while the references will be added in the online Structured Wiki, with additional comments and considerations from the field

Connected Factories 2 CS & Privacy Standardization & Industry Standards															
CS Standard Analysis															
		DT-ICT-07-2018-2019							DT-ICT-08-2018-2019		ECSEL		DT-ICT-02-2018-2019		
		CF2	Kyklos 4	DigiPrime	Qu4lity	EFPF	SHOP4CF	ZDMP	SeCollA	COLLABS	Industry4.E	Productive4.0	DIH2	TRINITY	
IEC62443		X				X		X	X	X					
NIST		X				X		X	X	X					
	NIST SP800-82	X				X									
	NIST CSF	X				X									
NISTIR8183	CS for Manufacturing	X													
NISTIR 8259	CS for IoT Device Manufacturers	X													
CSA CAIQ		X													
CSA GDPR COC		X													
CSA ICS		X													
ISO13849						X									
ISO27	27000:2018	X				X									
	JTC1/SC27	X				X									
	27017:2015	X				X									
ISO33052:2016	PRM					X									
CIS-ICS		X													
ETSI IoT		X													
ETSI TS103 457	Trusted Cross-Domain					X									
CISA		X													
NIS		X							X	X					
STRIDE		X													
CVE		X							X	X					
ATT&CK		X							X						
Industrie4.0		X													
GDPR		X							X						
SBOM		X													
RIM		X													
ENISA	IS & P standards for SME	X				X									
	Procure Secure	X				X									
OPC	IEC/TR 62541-2:2016	X				X									
ISO/TC 262															
TLS		X													
HTTPS		X													
IDSA		X		X											

Table 9: Mapping of ICT-07 projects in CS standards

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The different DMP-projects and other projects trying to secure automation and digital manufacturing activities apply similar standards. The Work in Progress (WIP) indicate how the projects have published and reported their use of various CyberSecurity standards. Analysis from the DMP Standardization workshop from October 20th 2020[35] shows that some projects are focusing more on specific aspects of CyberSecurity such as identification and authorization, but are not taking into account considerations such as device security, data transport, security monitoring, data protection, incident management and other cybersecurity perspectives that would allow for a more consistent holistic approach on CyberSecurity. Some projects (like SHOP4CF, SECOIIA, COLLABS, QU4LITY, …) apply first an enterprise risk assessment related approach and relate some of the challenges back to the underlying factories before identifying specific technology approaches and methodologies. For this they apply usually similar standard approaches such as the **NIST Cybersecurity Framework, IEC62443 and ISO 27k-series.**

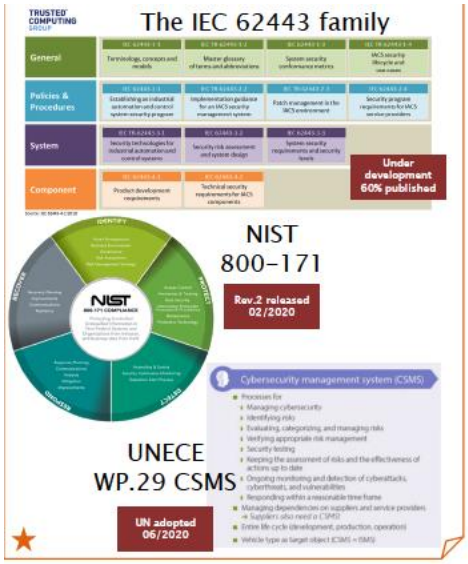


Figure 92 assessment of CyberSecurity standards being used by the COLLABS project, indicating the main use of NIST and IEC62443, adding the perspective from UNECE

Projects also refer to developing standards, indicating also that many current standards are not completely covering the requirements of digital manufacturing. Approaches refer to the Industrial Internet of Thing Consortium (IIC) and the CyberSecurity Framework (IISF)[36]. During the analysis and the subsequent workshops, additional CS standards and de facto standards were added to the list, whether to be considered only for specific verticals (SECOIIA and COLLABS on automotive) or general CS developments such as the ETSE 303645 for component design (SHOP4CF)-project.

[35] https://www.connectedfactories.eu/news/standards-digital-manufacturing-webinar-recordings-and-presentations-are-now-available

[36] https://www.iiconsortium.org/IISF.htm

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

CS Standards with DMP & FoF - WIP

Connected Factories 2 CS & Privacy Standardization & Industry Standards

CS Standard Analysis

		DT-ICT-07-2018-2019							DT-ICT-08-2018-2019		ECSEL		DT-ICT-02-2018-2019	
		CF2	Kyklos 4	DigiPrime	Qu4lity	EFPF	SHOP4CF	ZDMP	SeCollA	COLLABS	Industry4.E	Productive4.0	DIH2	TRINITY
IEC62443		X				X		X	X	X				
NIST		X				X		X	X	X				
	NIST SP800-82	X				X								
	NIST CSF	X				X								
NISTIR8183	CS for Manufacturing	X												
NISTIR 8259	CS for IoT Device Manufacturers	X												
CSA CAIQ		X												
CSA GDPR COC		X												
CSA ICS		X												
ISO13849						X								
ISO27	27000:2018	X				X								
	JTC1/SC27	X				X								
	27017:2015	X				X								
ISO33052:2016	PRM					X								
CIS-ICS		X												
ETSI IoT		X												
ETSI TS103 457	Trusted Cross-Domain					X								
CISA		X												
NIS		X							X	X				
STRIDE		X												
CVE		X							X	X				
ATT&CK		X							X					
Industrie4.0		X												
GDPR		X							X					
SBOM		X												
RIM		X												
ENISA	IS & P standards for SME	X				X								
	Procure Secure	X				X								
OPC	IEC/TR 62541-2:2016	X				X								
ISO/TC 262														
TLS		X												
HTTPS		X												
IDSA		X		X										

Adding :
+ ID&AM : ISO 24760, UMA, XACML, SAML 2, OpenID,…
+ Identity Assurance : NIST 800-63
+ AAA : OAUTH, …

+ DIN27070 : security gateway for exchange of industry data

Source : LSEC, 2020

Supported by the European Commission (Grant Agreement Number 873086)

Table 10: New CS standards incorporated

During a series of activities by the CF2 project in collaboration with the DMP projects, additional discussions on the use of standards have been used. This resulted in the presentation of additional standards that were considered by the projects, or considerations from developing standard organizations which are relevant for the DMP and related manufacturing projects and which serve to support the developing CyberSecurity Pathway.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

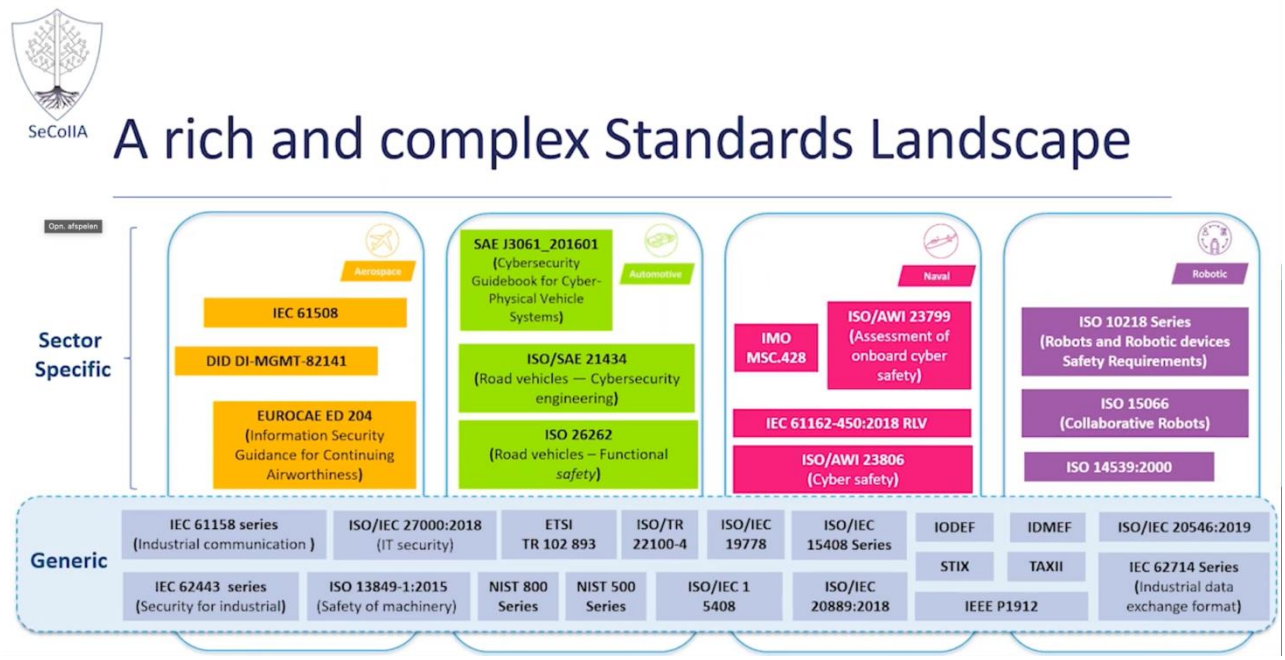


Figure 93 : assessment of security, safety and CyberSecurity standards investigated and applied in the SECOIIA-project, © SECOIIA project, 2021

This standards overview from the SECOIIA project indicates the importance of sector-specific CyberSecurity standards that need to be considered from the project to be able to serve its pilots. In addition, a number of traditional safety and security standards are also been considered that impact also the CyberSecurity approach. SECOIIA applied a transformation journey for standardization from the current state of the manufacturing environments, using an assessment to identify the need for alignment to the project objectives on the basis of a gap analysis.

For more information on the specific standards to be followed and the details of the standards, we refer to the structured Wiki and additional reference materials which will be added to the Structured Wiki as some of the additional standards are also to be considered by other DMP projects and related projects.

6.5.3 H2020-ICT-08-2019 : Security and resilience for collaborative manufacturing environments

Our listing and reference starts with the two projects which were selected under this program “Security and resilience for collaborative manufacturing environments”, as it indicates that the core focus of these projects is security, next to the manufacturing. In the two selected projects, the DMP serves the functioning of the manufacturing companies and their digital operations but mainly from the intention and the business intentions of the manufacturing companies, which are being supported by the security mechanisms.

6.5.3.1 SECOIIA : Secure Collaborative Intelligent Industrial Assets [37]

Also SECOIIA approaches manufacturing with different vertical industries (automotive, aerospace, robotics, maritime) and various manufacturing partners, with different levels of expectations and risk exposure levels.

[37] https://secoiia.eu/

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 873086.

With a mission of bringing higher levels of security and safety to the manufacturing industries while utilizing digitalization and collaboration in production and manufacturing techniques.

The security requirements of the SECOIIA project are in the first place driven by the specific use cases related to interconnectivity of factories belonging to the same group, to relations with suppliers providing maintenance and the considerations of the physical production of highly sensitive products and technologies. In addition specific safety and human-interaction with robots resulting from CyberSecurity are being considered. Finally it considers challenges for CyberSercurity from a product lifecycle management. At the same time it is considering the CyberSecurity of the systems from for instance ransomware. The project takes into consideration training and education of various persons / persona's in the factory.

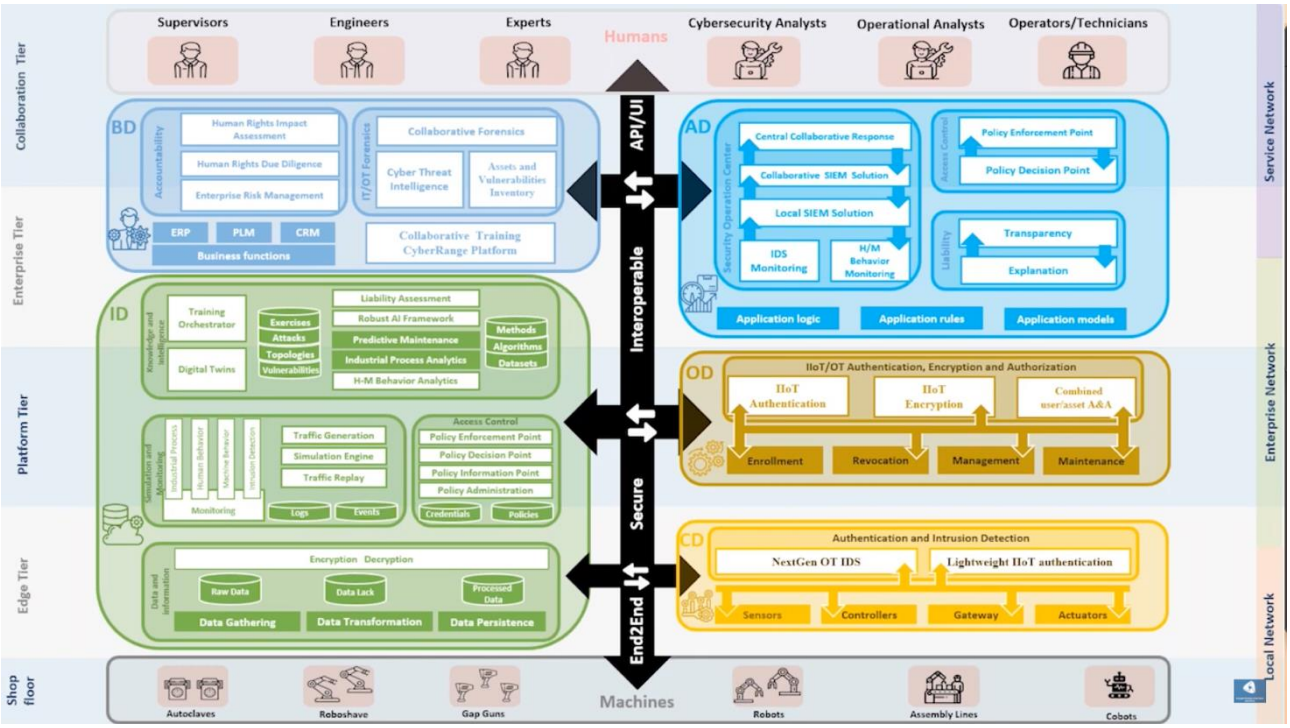


Figure 94 : overview of the current SECOIIA CyberSecurity approach in progress identifying a wide area of focus areas for CyberSecurity both from a functional – operational perspective, system perspective, persons/personas perspective and trying to apply various technology, process and skills-considerations. © SECOIIA project 2021

The SECOIIA project partners are aiming to produce CyberSecurity improvements on various levels, such as the identification and use of different CyberSecurity standards, considering the continuous evolutions and ongoing work on standardization. SECOIIA identifies the challenges related to the use of AI or Forensics which

Figure 95 : the CyberSecurity solutions approach by SECOIIA aiming to deliver impact on various interaction levels and for different identified entities which are involved in the manufacturing activities. © SECOIIA project 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

are currently not fully being covered by either standards or technologies and require specific additional attention. SECOIIA identified 16 key capabilities to enforce security of Factories of the Future at 4 collaboration levels (organization, human, machine) and in 4 challenges (human preparedness, information security, process safety and social liability). The project has been building a generic functional architecture based upon secure cloud / edge manufacturing backbone and collaboration services, facilitating training and simulation capacity and a collaborative Security Operatations Center (SOC) supporting the collaborative manufacturing value chains of the difference verticals. Finally it aims to provide a security ccountability framework.

Key learnings from this project are the scope and breadth of CyberSecurity in manufacturing environments, clearly indicating the complexity of CyberSecuring different activities, processes and entities and identifying challenges related to this and gaps that are already appearing (AI and forensics). The key use for projects under the DMP and other digital manufacturing environments or factories transforming towards digital relate to the enterprise and sectorial risk-based approach, the use of standards, the identification of a CyberSecurity-wide architecture on top of the current standard framework and particular technologies and methodologies towards continuous improvements, skills and education and analysis of intelligence coverage.

6.5.3.2 COLLABS : a COmprehensive cyber-intelligence framework for resilient collaborative manufacturing Systems[38]

The other project under the ICT-08-2019 program "Security and resilience for collaborative manufacturing environments" is COLLABS. Equally working with different production companies and manufacturing use cases, it considers also the factories from the inside with their transforming infrastructures evolving to digital and include challenges related to their supply chain relations.

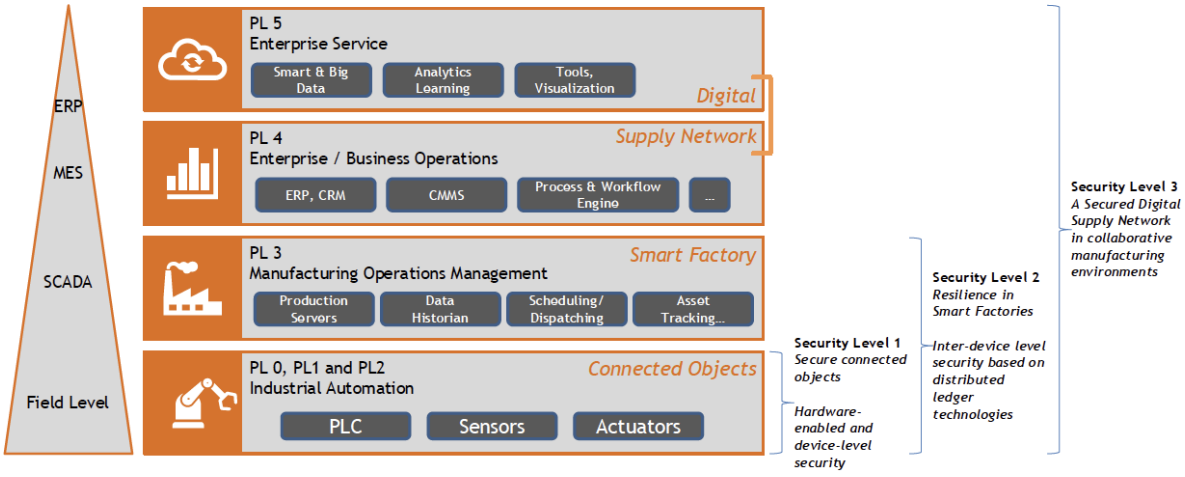


Figure 96 : COLLABS use of the Purdue model for segregation of functions

COLLABS can inspire other projects in many different ways. It applies the Purdue-model (IEC-62443) to segment the different operations from field level up to enterprise services. Next, it applies an enterprise wide

[38] https://www.collabs-project.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

perspective on layers of security: data protection, system integrity and workflow security covering not only multiple partners and connected enterprise interworking components, but also looking into the supply chain and supporting compliance in manufacturing. COLLABS is taking abstraction from the various underlying systems while still focusing on a wide security perspective. Finally it aims to integrate different security functionalities from COLLABS technologies into a 3ACEs data integration layer and to finally arrive to a Trusted Execution Environment (TEE) within the supply chain.

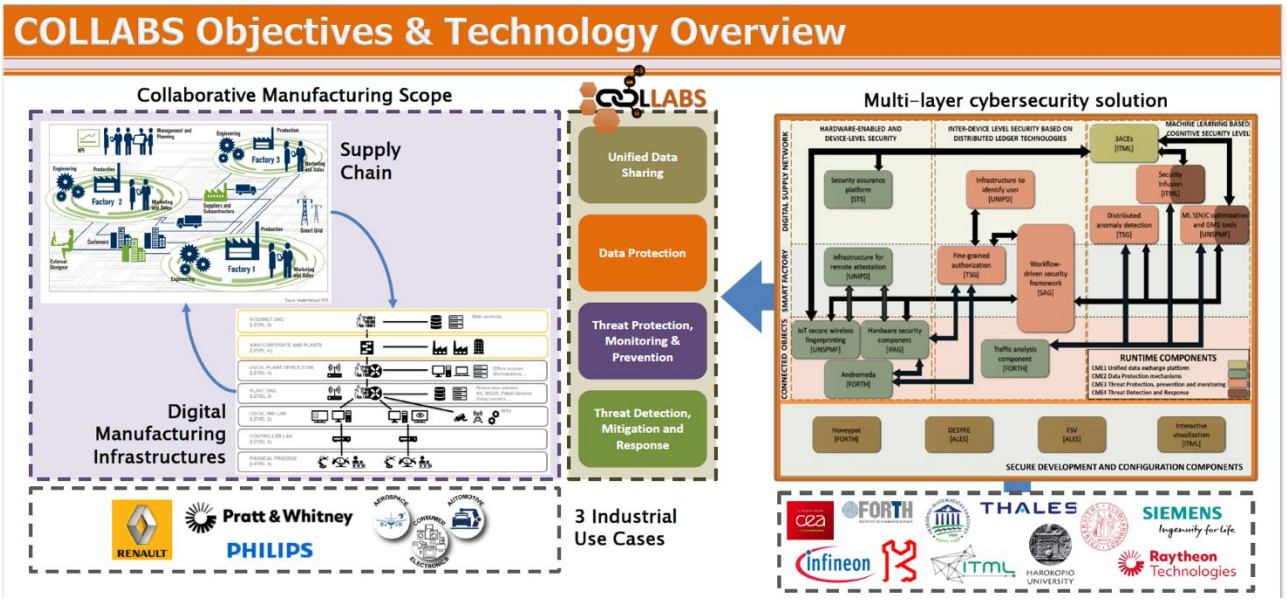


Figure 97 overview of the multi-layer CyberSecurity approach on the different business challenges derived from the different manufacturing environments © COLLABS project 2021

The ongoing work on the applied CyberSecurity architecture represents a similar approach, where both from the systemic level, the enterprise level and the manufacturing company in relation to its environment is being considered, and where the approach is to take a holistic perspective in trying to apply CyberSecurity on these different levels with specific approaches. For some of these approaches existing technologies will be applied, but COLLABS is aiming to derive a framework approach from this, in order to apply it into various factory environments.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

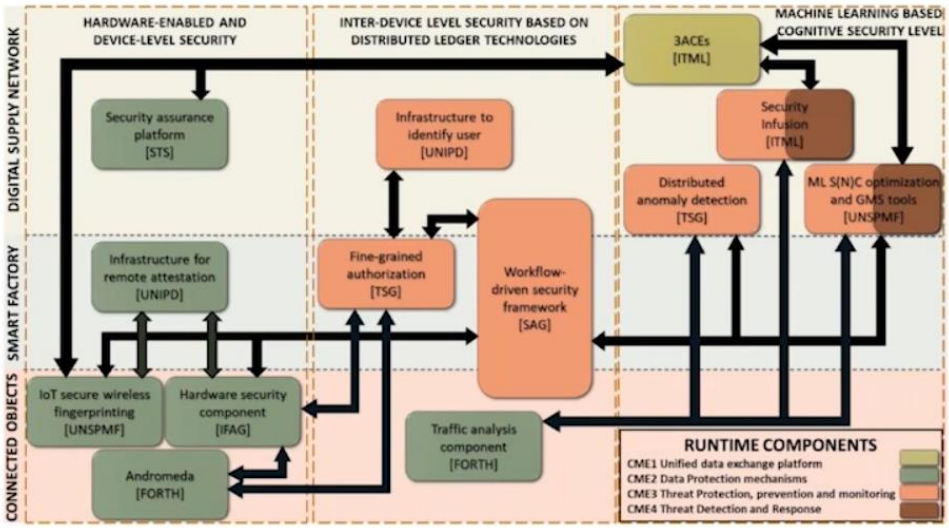


Figure 98 the COLLABS three-layered architecture and the interconnectivity of different CS-components © COLLABS project 2021

The security architecture being constructed indicates a complex interaction of developments on the basis of existing systems and technologies, aiming to serve different security functionalities that can be applied in the manufacturing companies following a series of scenarios. Specific technologies (minimal viable products – MVPs) which are being developed and could be considered by other DMP projects and related manufacturing companies building their digital manufacturing activities, such as 1) agent-based traffic analysis; 2) SE-based endpoint protection, 3) remote attestation mechanisms, 4) distributed anomaly detection and 5) fine-grained process-driven access control.

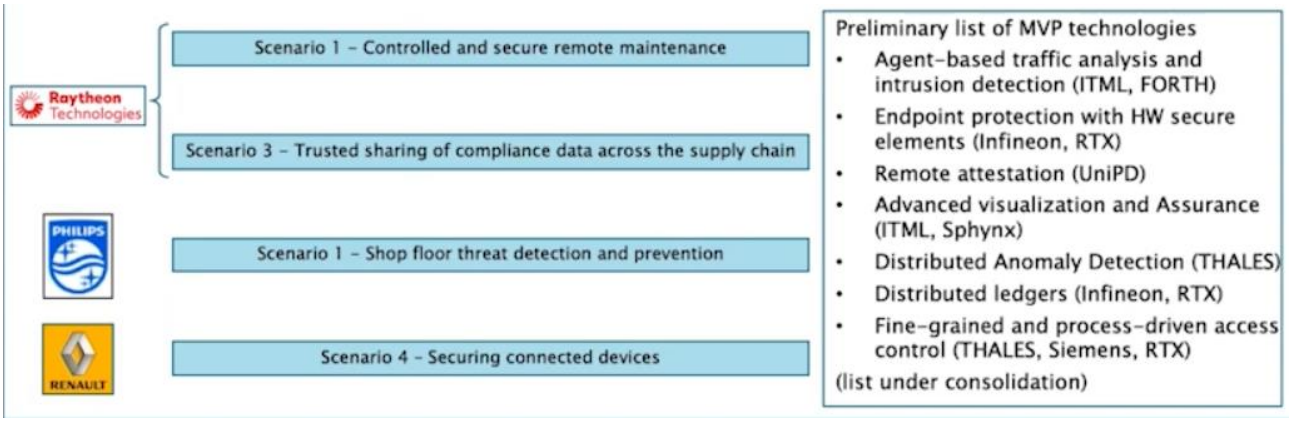


Figure 99 : COLLABS technologies that will be applied in a series of scenario's, scenario's which can be run in the pilot manufacturing companies, but equally in other manufacturing and digital manufacturing environments. © COLLABS project 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

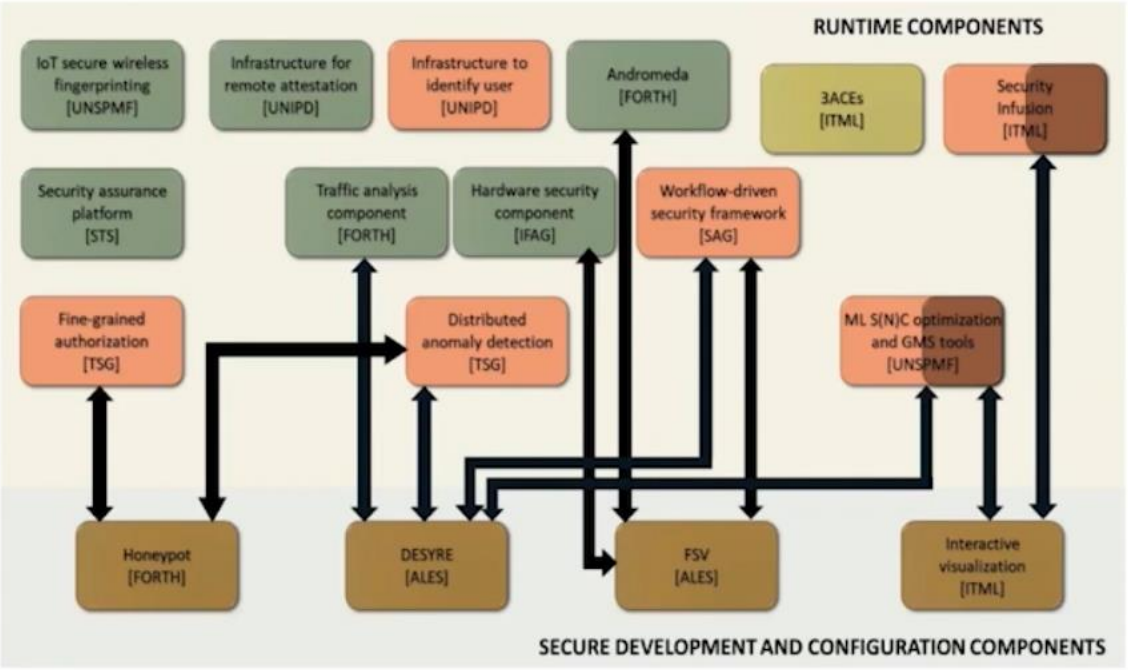


Figure 100 : COLLABS insight in the functioning of the CyberSecurity runtime components and the relation between the core functionalities of the CyberSecurity activities that can relate to a wider CyberSecurity framework © COLLABS project 2021

The different components identified by the CyberSecurity architecture indicate the complexity and the potential approach for Digital Manufacturing Platforms to consider in a production facility environment. Some indicators for the CyberSecurity Pathway are considerations of the 1) Fine grained authorization, 2) Remote attestation, 3) Distributed (anomaly) detection, 4) Traffic analysis, 5) (In)Fusion and ML optimization and visualisation.

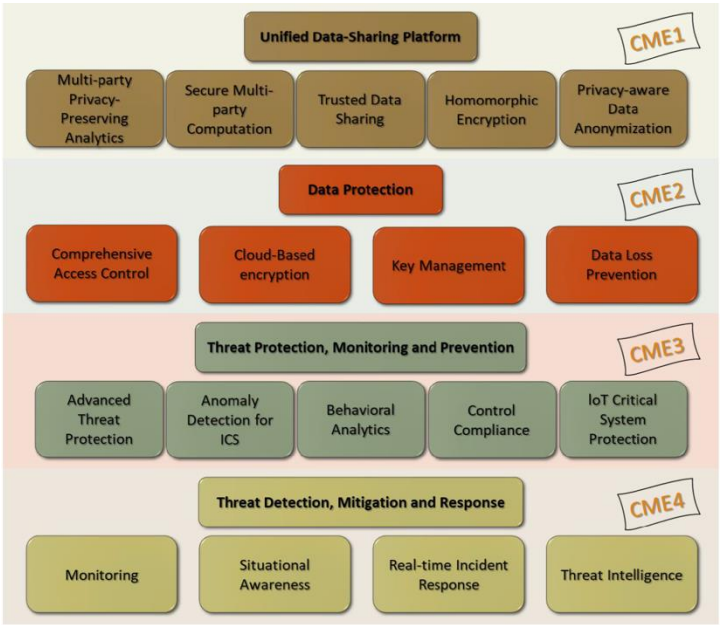


Figure 101 : COLLABS project functional element © COLLABS project 2022

Tools and techniques are being represented in the COLLABS functional elements, components which can eventually also be mapped to the CF2 security pathway. The unified data exchange platform will be using secure multiparty computation, in order to protect sensitive data coming from cyber-incidents sych as attacks, untrusted infrastructure attempts and unauthorized acces attempts to be shared amongst partners. Context-based cloud access control will be used to authenticate users and ensure data protection. Remote attestation and mechanisms relying on deep learning methods to detect and prevent threats will be used in the Threat Protection, Monitoring and Prevention capabilities. Finally in the System, runtime components on hardware, inter-

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

device and machine learning are fundamental to the final operational environment. In the IoT devices, COLLABS inserted wireless fingerprinting to develop dynamic behavioural models for device and device data inspection. Additional hardware security components were inserted in the frameworks to provide a secure execution environment (SEE) to allow for secure processing, identifiable and secured datatransmitters and remote attestation. COLLABS also introduced the use of a trusted OS and analysis of encrypted data transmissions.

Some basic components such as Honeypots, ID & AM and intelligence components could also be re-used by the DMP projects and manufacturing companies transforming to digital manufacturing.

The COLLABS project identifies that the main challenge is to derive from this approach a common security framework that can fit to several industrial settings and accommodate the constraints and variety of applications, functionalities, systems and devices. As they have the idea to validate this on different use-cases, the different DMP projects and related pilots and activities can have a benefit in closely following the requirements in order to use their environments to have the COLLABS frameworks being validated against.

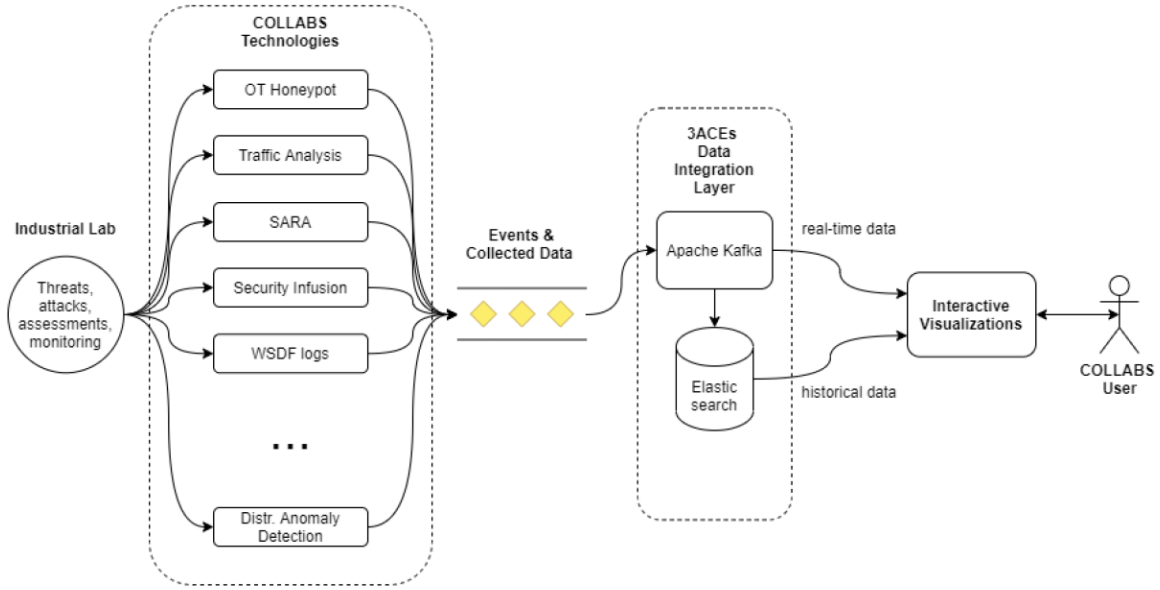


Figure 103 : COLLABS components 3ACE's integration

The project also identifies the challenge of labelling datasets (metadata) for machine learning and use in supervised learning algorithms, also pointing to the related CyberSecurity challenges.

6.5.4 Critical Infrastructure Protection Best Practices

Horizon2020 has invested quite extensively into research in Critical Infrastructure Protection, into various domains including utilities production and transport, logistics, telecoms and financial services. During the CF2 activities, some of these projects were invited to represent some of the outcomes relevant for the manufacturing industry in terms of resilience, cybersecurity challenges related to legacy and new digitalisation trends.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

Similar to critical infrastructure requirements for CyberSecurity, we must be creative in investing methods and technique for fully unleashing the power of Digital Manufacturing Platforms, while ensuring that ultimate control stays with the human.

6.5.4.1 *ANASTACIA : Advanced Networked Agents for Security and Trust Assessment in CPS / IoT Architectures*

The consideration that cyber-attacks on IoT are getting more widespread, causing the emergence of new types of attacks and zero-day vulnerabilities without the current cybersecurity solutions being able to react swiftly and dynamically requires the consideration of a new context-aware security framework to allow orchestration by virtual agents across IoT domains.

An interoperable and scaleable IoT security management, based upon a learning decision model for detecting, hybrid security monitoring and optimal selection of virtual agent-based security mechanisms, their orchestration are being considered.

6.5.4.2 *SATIE[39] : Security of Air Transport Infrastructure of Europe*

Similar to the aviation industry, within Digital Manufacturing there is currently no turnkey cyber-physical security management system operational addressing a modular approach connecting any imaginable sensor (from drones to agents on devices), where the system is capable to learn on the job and to provide for a central overview for security operators allowing for threat prevention and decision support for security operators to work with.

The SATIE proposed architecture can inspire Digital Manufacturing operators from an architectural perspective focusing on a central alerting system and supporting systems, that can be distributed towards the connected factories from within the enterprise and a connection to the factories in the ecosystem. The joint crisis alerting system allows to escalate incidents beyond the existing operators and exchange intelligence and information.

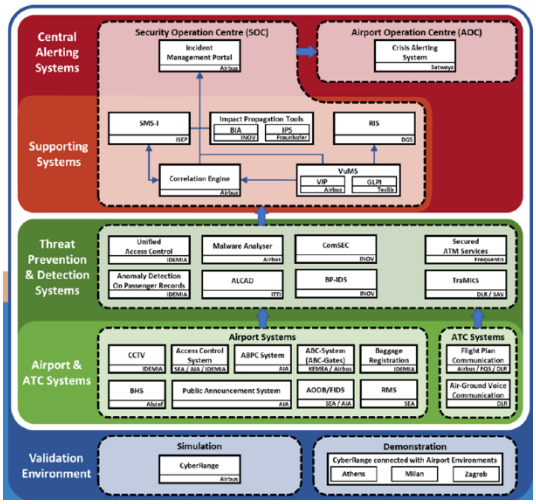


Figure 104 : the SATIE architecture, © SATIE-project 2022

6.5.4.3 *CyberSEAS[40] : Cyber Securing Energy Data Services*

The CyberSEAS project is relevant for the Digital Manufacturing Platforms and operators in multiple ways. It focuses on the highest impact attacks possible, on protecting consumers privacy and security and on the security of a common data space. The project has developed several Methodological (policies, design techniques, governance) and Technical Measures (risk assessments, real time asset monitoring, information

[39] https://satie-h2020.eu/ (H2020-SU-INFRA-2018-2019-2020)

[40] https://cyberseas.eu/ (H2020-SU-DS-2018-2019-2020)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

exchange, triage, prioritization, training, …) to increase the security level based on situational awareness. The resulting 100+ attack scenarios allowing for categorization of attacks, identification of impact on personal data (breaches) and emerging threats.

`

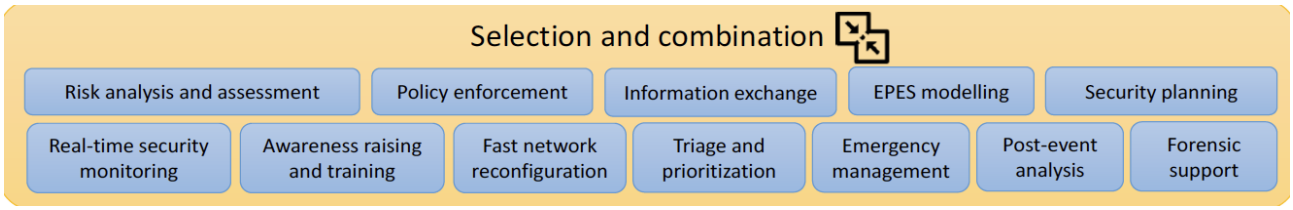


Figure 105 : excerpt from the CyberSEAS ecosystem approach – cybersecurity for securing energy data services © CyberSEAS project 2022

Key learning aspects for digital manufacturing include the development of multiple attack scenarios, both strategic and technical measures, which are also apparent in the Toolbox[41] approach for 5G cybersecurity, developed by mobile operators and ENISA.

6.5.4.4 Other relevant Critical Infrastructure (CI) project contributions : serious gaming, digital twin, AI

In PRECINCT[42], considerations are being made to use Serious Gaming techniques, to represent cascading effects in interdependent critical infrastructures. Serious Gaming involves the gamification of a potential event or series of events, and playing them like a real life scenario. This allows to stimulate interactions, train a series of activities, learn from reactions, impact, potential side effects and how to deal with these; next to the resulting effects of the counteractions. While in a virtual scenario, the game can be played in a real life setting in order to enlarge the direct impact on the participants. Such games can also support designated participants to follow specific guidelines and train them in executing them, according to preset scenarios. This is to avoid potential mistakes from happening, which increases the chances on adverse effects and results. Overall most CI activities are being focused towards Cyber Physical attacks, the result from a hybrid approach of physical an natural hazards, that can be affected and can have an effect on operational and information technology (OT/IT) and cyber-systems.

Both Norcic[43]s (the Norwegian Centre for CyberSecurity in Critical Sectors) and the PRECINCT project consider the impact of unified IT&OT modelling; with PRECENT specifically considering the use of Digital Twins supporting the cyber-physical security. Digital Twins can provide a unified IT&OT model or a cyber-physical system that can be analyzed for CyberSecurity. The Twin can be a physical clone a or a virtual representation of a live system allowing for additional investigations, to evaluate and assess the effect of hardened materials. It will include integration of physical and logical assets, that represents an interaction with the components.

Advanced analytics and AI are at the core of the IRIS[44] project aim to create a framework to support incident response teams (CERT, CSIRT) in detecting, sharing, responding and recovering from cybersecurity threats

[41] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

[42] https://www.precinct.info/ (SU-INFRA01-2018-2019-2020)

[43] https://www.ntnu.edu/norcics

[44] https://www.iris-h2020.eu/ (SU-DS02-2020 Intelligent security and privacy management)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

and vulnerabilities of IoT and AI-driven ICT systems. The IRIS platform will be made available free of charge to European national CERT and CSIRTs; and can serve from the focus on smart cities as example for Digital Manufacturing platforms.

6.5.5 DT-ICT-02-2018 : Robotics – Digital Innovation Hubs (DIH) - TRINITY[45]

Under the Leadership in enabling and industrial technologies (LEIT) program of ICT the project Digital Innovation Hubs are being developed for Digital Technologies, where one of the selected projects is TRINITY. The TRINITY project focuses on Advanced Robotics, CyberSecurity and IoT for agile production. The project builds a series of pilot activities and technologies as demonstrators for European manufacturing companies. Next to this, the project is support innovative European projects with a Financial Support to Third Parties (FSTP)-program, a cascade funding project.

Within TRINITY, there are 17 different technology development activities, which are aimed to progress beyond the State of the Art by themselves, but also offer the results to manufacturing companies throughout Europe. An additional 19 innovative projects have been selected in the first Open Call which took place in 2020. A second Open Call will be launched in 2021 aiming to support an additional 10 – 15 projects.

The variety of innovative projects is a typical similar challenge to manufacturing companies looking to further improve their production environment. Many of these projects are applying digital technologies, or are using robotics to further improve their operations.

The project has applied a CyberSecurity assessment of the various technologies developed within the project, that resulted in an alarming result after the analysis of the overall approach towards CyberSecurity. Close to none of the pilot actions had performed any significant CyberSecurity assessment, and realized during the exercise the number of potential vulnerabilities and impact these could cause. While many project partners indicated that their main pilot development was only running within the lab environment (TRL 4-7), the aim of the project was to facilitate the uptake of the technologies by SMEs, and some even with the plan on going into production in factories. On the basis of the existing architecture and additional hardening exercise took place, in some cases improving the network security layer, the identity and access control layer, and monitoring of the activities on the endpoints, or limiting the direct access to the industrial equipment by utilizing secured hosts.

[45] https://trinityrobotics.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

UseCase CyberSecurity Analysis (ß-stage)

High Level Analysis of Use Cases	Applicable Nr TR Use Cases	% of total nr of use cases
1. A CyberSecurity Risk Analysis defining potential risks and vulnerability threat assessment has been done and documented during DESIGN or PRIOR to the development of the use case?	none	0
2. CyberSecurity concerns and have been taking into account, and have been documented?	3, 4, 14, 15	24
3. Robotic System Developers and Engineers are aware of CyberSecurity concerns in the use case?	3, 4, 6, 7, 11, 12, 13, 14, 17	53
4. Our robotic systems are designed and operated only by vendor specific controllers.	1,10, 11, 16, 13, 14	35
5. Our robotic systems have been programmed, created and operated by PLC's	10, 14	12
6. Our robotic systems have been programmed and /or are being controlled and operated by ROS – ROS2, DDS, OPC, OPC-UA, or other available interfaces	1, 2, 3, 4, 6, 7, 9, 12, 13, 17	59
7. Our robotic systems have a web interface, can be accessed via intranet, mobiles, internet or can be operated via the cloud	6, 7, 8, 11, 12, 14	35

Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance

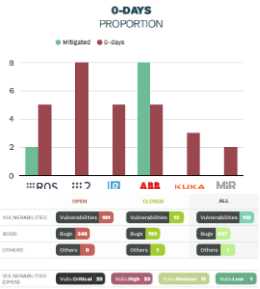
CASE OF STUDY
MIR-100
THREAT: SAFETY PLC IS DIRECTLY CONNECTED TO THE ROBOT INTERNAL NETWORK

TRINITY

Figure 106 the original assessment of the various components of the TRINITY project presented an alarming image of the CyberSecurity state of the various use cases during the first review period. This resulted in a holistic approach to all pilot actions to design ways to further improve the CyberSecurity standing © TRINITY project 2021

UseCase CyberSecurity Analysis (ß-stage)

The following cybersecurity measures have been taken into account:	Applicable Nr TR Use Cases	% of total nr of Use Cases
1. Isolation : the robotic systems has been taken offline, or has been implemented on a segregated network	1, 3, 4, 7, 10, 11, 12, 13, 16, 14, 17	65
2. White Listing : the robotic system, has been integrated in the network, but can only be accessed by a specific set of network operations and other machines	14	6
3. Access, Identity & Authentication Management : access to the robotics systems (development and operations) has been limited to a specific set of users, and other applications requiring access, to be granted upon authentication	1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17	88
4. A vulnerability assessment (pentest) of the robotic system has taken place and all vulnerabilities have been reported and are being dealt with	3, 4	12
5. The application logic of the robotic system has been developed on the basis of security by design principles, taking into account application security	none	0
6. We are aware of the security capabilities offered by ROS2, and have implemented those measures, or at least have considered them in the use case	3, 4, 7, 12, 17	29
7. We are getting aware of CyberSecurity issues thanks to TRINITY (and others), we didn't yet take any serious preventative measures, but intend to do so	3, 4, 6, 9, 10, 11, 13, 14, 15, 17	59



TRINITY

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

The following list indicates an overview of potential hardening activities that can take place on the industrial automation systems, which are being integrated in the Digital Manufacturing activities of the factories.

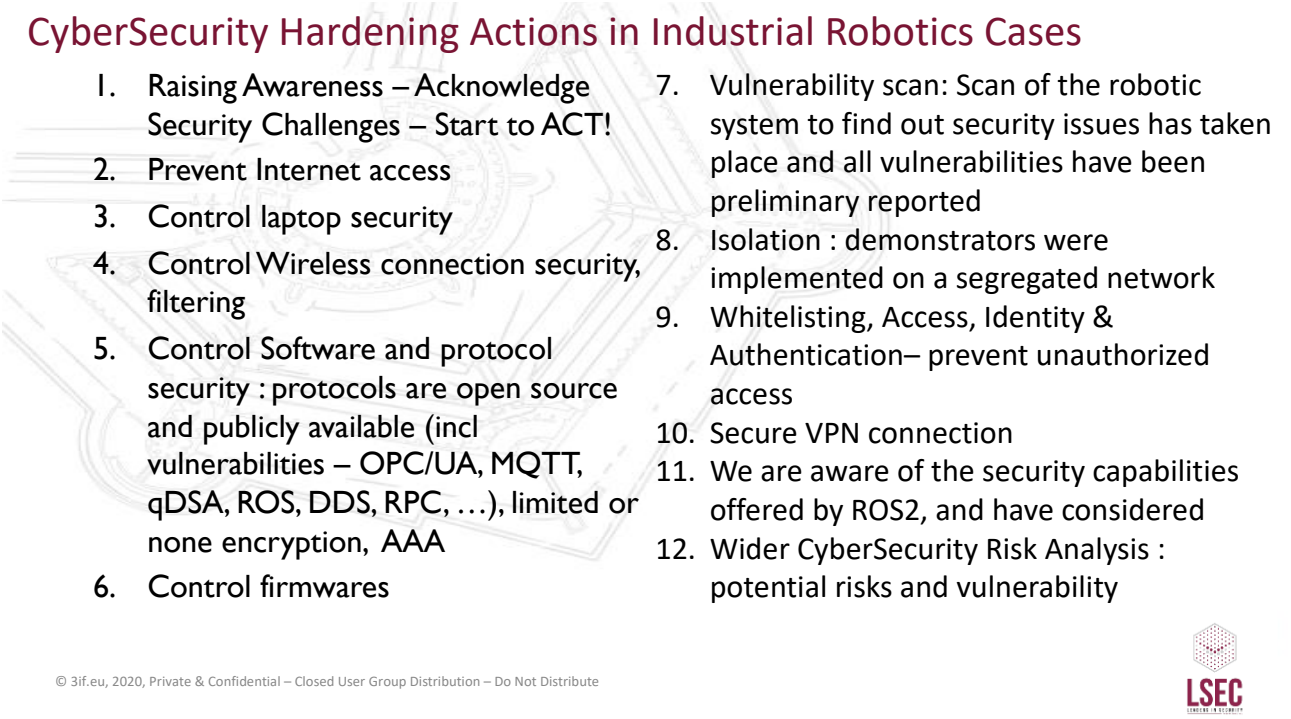


Figure 107 : series of actions to be followed by Digital Manufacturing transformation activities to harden the security layers of the various industrial components for automation and production. Specific attention was paid to the utilization of robotic systems which are either legacy environments working on industrial pc which have not been hardened, or the use of open source ROS (Robotic Operating System) – which is only gradually improving on CyberSecurity © TRINITY project, 2021

Key learnings for Digital Manufacturing Projects are the use of assessments and the sanitization of some of the basic components before applying additional CyberSecurity measures. The CyberSecurity is only as strong as the weakest link in the whole chain or environment. Different specific actions had been presented and hardening mechanisms proposed which can be applied into other Digital Manufacturing Platforms and digital manufacturing environments.

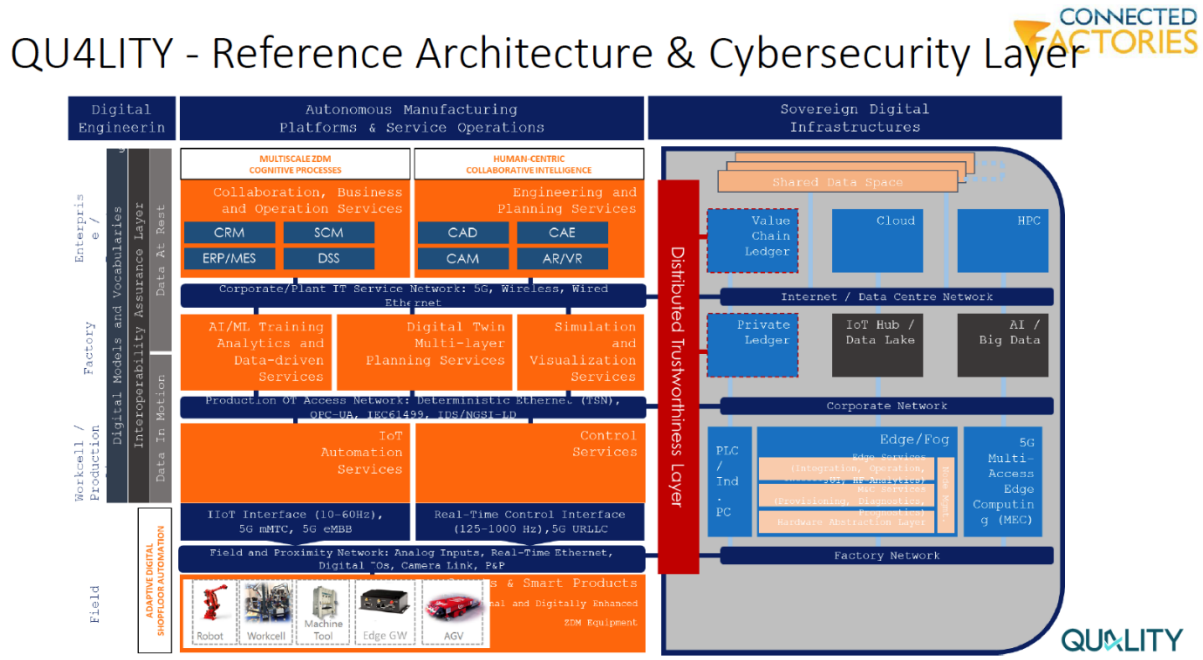
The next steps for the TRINITY project is to apply a similar top-down approach to the Open Call projects selected under the first Open Call and to provide a bottom-up (security by design) support to the projects selected under the second open call. The overall principles are to be proposed as a standardized approach for manufacturing companies increasing their use and applications of digital manufacturing systems and the use of robotics.

6.5.6 QU4LITY – Joining forces towards an European Industrial Autonomous Quality

The QU4LITY project aims to demonstrate a data-driven Zero Defect Manufacturing (ZDM) product and services model for Factory4.0 through 14 pilot lines, with 9 production lighthouse facility pilots and 5 strategic ZDM. The project aims to provide a modular cybersecurity framework for manufacturing covering

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

CyberSecurity, Privacy and Trust[46]. It aims to provide integration of different tools in order to support the pilot factories and support distributed and critical functionality. Under consideration are challenges such as Digital Sovereignity and opportunities provided through Standardization.



The system architecture considers a separate CyberSecurity Layer (Distributed Trustworthiness) considering a Sovereign Digital Infrastructure (SDI), whereby the Autonomous Manufacturing platform would be distributing data and intelligencey to the SDI. The project aims to utilize an Open Secure IDS connecting the various manufacturing pilots (PRIMA, Philips, Siemens, Mondragon, Conti, Danobat, …) to the central Data platform, utilizing context-based authentication and digital traceability.

The project started with an enterprise (production company / factory) risk perspective and tries to provide additional security layers to facilitate the interaction between different manufacturing companies and other related entities. The identification of the persons and systems are important components, as well as the security layer for the data transmission. Other considerations and the CF2 cybersecurity activities will further support additional perspectives on CyberSecurity for the manufacturing companies and the DMP being considered by the manufacturing companies. QU4LITY activities will enable manufacturing companies to mature on the CyberSecurity Pathway from level 3 to partial level 4, whereas components of level 3 might not have been completed.

6.5.7 DIGIPRIME – Digital Platform for Circular Economy in Cross Sectorial Sustainable Value networks.

DigPrime aims to be focused on the digitization of the circular chain and hence general cybersecurity standards and supply chain security standards are applicable, factory/shopfloor security is mostly relevant to internal systems of manufacturing partners, not to the DigiPrime platform per se. The platform leverages

[46] https://www.effra.eu/events/cybersecurity-workshoppresentations-and-recordings

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

KeyCloak / OAuth for the authentication, aims to comply to GDPR (mandatory), and adopts principles from IDSA (secure communication layer) in our platform design. For next version of the deliverable, DIGIPRIME will focus a bit further on the Supply Chain Management, for instance the use of TPRM – SIG – assessments for supply chain security.

6.5.8 SHOP4CF – Smart Human Oriented Platform for Connected Factories

The SHOP4CF, Smart Human Oriented Platform for Connected Factories - project, pursues a highly-connected factory model aiming to create a platform with 30 components based on RAMI 4.0 and FIWARE Technologies on Automation MarketPlace, which also includes Financial Support to Third Parties – cascade funding for selected SMEs. Its industrial partners include manufacturing companies such as Bosch, Volkswagen, Arcelik and Siemens. For CyberSecurity, the project is at the time of this analysis assessing which target security levels with the Asset Owners (the Manufacturing companies) require in their environment, on the basis of interview methods. From this on this project will also consider both System Integrators and Product Suppliers in CyberSecurity conversations. In addition, the project is considering specific integrations with cloud infrastructure. The expected outputs will include best practice guidelines and specifically a risk assessment tool for integrators or component developers.

The SHOP4CF project will be able to utilize some of the works being prepared by CF2 and the Security and Resilience for Manufacturing projects, by means of the assessment and maturity frameworks and mechanisms to evaluate the CyberSecurity requirements from the Manufacturing environment on the basis of existing standards.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

7 Humans and manufacturing

7.1 General observations on human aspects.

With the advent of the fourth industrial revolution called Industry 4.0, the industrial world has shifted further towards automation, where advanced workplaces are replacing existing working stations. Moreover, human-machine collaboration has taken a big leap forward, placing human operators in the centre of attention. In the past, people were expected to adapt to machine requirements. Now, automation systems are being designed and developed so that they can recognise the users, remember their capabilities, skills, and preferences, and adapt accordingly. Humans and automation are therefore taking advantage of each other's strengths, having a symbiotic relationship for enhancing the capabilities, skills, and quality of their work[47]. factory floor solutions addressed by the five projects that make up the ACE Factories cluster reinforce the concepts introduced by the original Operator 4.0 topology by Romero et al. (2016). Figure 108 illustrates the ACE Factories cluster Operator 4.0 concepts. The Super-strong as well as the Augmented and virtual operator illustrate how new technologies empower operators with new capabilities and enhanced sensing. The Social and collaborative operator illustrates how operators and the whole work community can be engaged to influence on the work environment and work practices. The one-of-a-kind operator illustrates how manufacturing environments can empower workers by adapting to the different characteristics, skills and preferences of workers. The Healthy and happy operator emphasises that all the Industry 4.0 solutions should have positive impact on operator wellbeing.

Figure 108: ACE Operator 4.0 Topology (modified from Romero et al (2016)).

[47] Ace factories cluster white paper on "Human-centred factories from theory to industrial practice. Lessons learned and recommendations", October 2019.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

7.2 Reference documents on human aspects.

- Ace factories cluster white paper on "Human-centred factories from theory to industrial practice. Lessons learned and recommendations", October 2019.
- World Economic Forum, 2020, The Future of Jobs Report, October 2020.

7.3 Examples from projects (mapping of projects)

7.3.1 EFPF- European Connected Factory Platform for Agile Manufacturing

The EFPF platform interlink digital manufacturing platforms, smart factory tools and Industry 4.0 concepts to realise and support a connected and smart ecosystem of the future. The platform is offered to users through a unified Portal with value-added features to hide the complexity of dealing with different platform and solution providers.

Aerospace Pilot: The Aerospace Pilot in the EFPF project addresses the ad-hoc setup of a production network involving Airbus Hamburg and local SME suppliers represented by the HanseAerospace (HAW) association. The Aerospace plot of EFPF focuses on B2B procurement type of interactions between SMEs and OEMs (or SMEs) in the aerospace industry. Hence "human factors in manufacturing" in this pilot case have rather low relevance.

Furniture Pilot: The furniture manufacturing pilot in the EFPF project, envisions the creation of a Lot Size 1 Consolidation Center to control small scale stocking and consolidation points for large manufacturers, such as LAGRAMA. In the Furniture pilot several user roles are foreseen. The Production Manager role should be supported with mechanisms to configure and optimise production processes.

Circular Economy Pilot: In this pilot, the partner KLEEMANN (KLE), a global manufacturer of Lift Systems, Escalators, Moving Walks and a specialist in lot-size-one projects such as anti-vandal lifts, oil rigs, marine solutions, requires agile relationships with different partners and suppliers in the waste management domain in order to be compliant with Life Cycle Assessment (LCA) regulations. The "Operations manager" role responsible for the production management will be supported with solutions to bring more visibility and real-time support across the supply-chain. Smart and analytics dashboards are expected to support this role in decision making.

A workshop took place with the EPFP project participants to discuss on Human Factor issues in the project. A summary of the workshop is presented hereafter.

Question (CF2): Based on the experience of the pilot case do you think that new job profiles should be defined to master the new technologies, practices etc?

Answer (EPFP): Personnel with the job profile needed but are may not be available could be contracted if needed from the labor market.

Question (CF2): Based on the experience of the pilot case is there a need for re-skilling/up-skilling of personnel to master the new technologies, practices etc.? If yes, can you name a few skills that are missing or needed? For example, IT skills, data analysis skills, management skills etc.

Answer (EPFP):

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- In the furniture industrial case IT skills are needed and missing, especially for elderly. Moreover, data analysis skills are needed.
- In the aerospace pilot case project managers, mid-management need some SW development and IT skills that are now missing.

Question (CF2): What type of knowledge delivery mechanisms (e.g., vocational training, on the job training, MOOCs, AR/VR) would be more adequate for re-skilling/up-skilling purposes of the final users of the pilot case results?

Answer (EPFP):

- In the furniture pilot case the technology provider (e.g. AIDIMME) is providing training to the manufacturing company (how to put the sensors, how to analyse the data) via online ad-hoc training sessions). More and more vocational training is covering the needs of using the technologies.
- In the aerospace pilot case there short on-the-job training session may facilitate the need for training. Typically, the companies have not the capacity for a e.g. half-a year training.

Question (CF2): Are you aware of any learning and training initiatives in Europe that fit to the re-skilling/up-skilling needs of the pilot case?

Answer (EPFP):

- Platzi Ibero-American
- Furniture: AIDIMME offers training courses in different areas, for example, Industry 4.0, Additive Manufacturing, Circular Economy, …: https://www.aidimme.es/@formacion-oferta-formativa#00 with the scope of the target audience manufacturing companies.
- There is a list of specialized Vocational Training Centers in Wood, Cork, Furniture, Carpentry and Installations (for blue-collar-workers) at regional and national level with qualified certifications for the student (a job bank available if the company requires specific skills):
    - https://labora.gva.es/es/web/cipfp-catarroja/inicio
    - https://labora.gva.es/es/web/crnfp-paterna
    - https://labora.gva.es/es/web/cipfp-benicarlo/inicio

Question (CF2): Which types of operators does the pilot support or augment their capabilities and how?

Answer (EPFP):

- In the furniture case related to Production Optimization at the edge bending machine avoiding human error when attempting to interpret a barcode label on a product, which can cause mistakes and production delays. The operator just verified what the system displays avoiding stress, the category health and happy operator is relevant.
- For the Aerospace case the Collaborative Operator and the Health and Happy operator are relevant.
- In general, the proposed taxonomy is adequate.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

7.3.2 QU4LITY – Joining forces towards an European Industrial Autonomous Quality

Qu4lity will realise a radical shift from state-of-the-art production quality methods to the disruptive Autonomous Quality (AQ) concept, through enabling manufacturers and solution providers (including SMEs) to develop, validate, deploy and adopt innovative Cognitive Manufacturing solutions for ZDM. Qu4lity supports 14 industrial pilot cases. 9 pilot cases focus on manufacturing companies/pilot factories in a diverse range of the industries and 5 cases focus on equipment suppliers. In QU4lity the Analytics Operator and Augmented and Virtual Operator requirements are pertinent.

7.3.3 ZDMP – Zero Defect Manufacturing Platform

ZDMP offers an open Industry 4.0 environment where a new generation of developed zero-defect service applications will be available in a marketplace contributing to create an ecosystem where ZDMP stakeholders would be able to interact with each other.

Automotive pilot case -1: The automotive pilot case involves the collaboration for the supply of casted engine parts from MRHS to Ford[48]. This case involves data sharing between FORD and MHRS as well as zero-defect prediction algorithms/solutions for the casted parts of MRHS. Human factors are related to information display through dashboards. In formation should be communicated to the user so that the model results are understandable, the rationale behind the model results is explained (i.e. explainable AI approaches are applied), recommendations for process parameter adjustments are delivered in a comprehensive manner.

Automotive pilot-case-2: The second automotive plot case involves the collaboration of FORD with EXT (machine provider). This is a Condition Based Monitoring / Predictive Maintenance case. In this case human factors are related to the delivery and interpretation of models' information (i.e. Analytical Operator).

Moulds manufacturing case-1: In this case a value chain between HSD, FIDIA and FORM is employed for moulds production. It is a typical condition monitoring and predictive maintenance case and the human factors are similar to the automotive case-2 above.

Moulds manufacturing case-2: In this case a value chain between HSD, FIDIA and FORM is employed for moulds production. The objective of this case is to optimize the process parameters so as to avoid quality defects. A key issue in this case is to create trust between the digital twin model and the operator. Moreover, the UI should provide clear indications on the parameter's modification (i.e. Analytical Operator).

A workshop took place with the ZDMP project participants to discuss on Human Factor issues in the project. A summary of the workshop is presented hereafter.

Question (CF2): Based on the experience of the pilot case do you think that new job profiles should be defined to master the new technologies, practices etc?

Answer (ZDMP)*:* In order to help the users use ZDMP results the project has developed the documentation of zComponents that includes text, figures, video etc. This will be partially documented in "D083 - Human Collaboration Environment" of the project. Moreover, a specific forum for interaction with the developers

[48] ZDMP Deliverable D2.3 - Industry Scenarios and Use Cases

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

has been setup. For example, the construction case requires no specific knowledge or some specific new employee profile.

Question (CF2): Based on the experience of the pilot case is there a need for re-skilling/up-skilling of personnel to master the new technologies, practices etc? If yes, can you name a few skills that are missing or needed? For example, IT skills, data analysis skills, management skills etc.

Answer (ZDMP)*:* Some of the skills missing and are required by the ZDMP developments are

- Interaction and use of AR technologies.
- Quality management, and quality control skills.
- System integrator skills
- Basic knowledge is required Kubernetes, virtualization; Skills for the zApps developers
- Data analytics skill, big-data, AI etc is needed but are not necessary (not needed for the operator level but on the higher level)

Question (CF2): What type of knowledge delivery mechanisms (e.g. vocational training, on the job training, MOOCs, AR/VR) would be more adequate for re-skilling/up-skilling purposes of the final users of the pilot case results?

Answer (ZDMP):

- AR is required to support maintenance tasks
- Documentation, videos etc of zComponents are used for training purposes.
- Virtual Academia (tutorials) how to install and use the zComponents and zApps
- Human Collaboration Environment such as Git can be used to deliver training content to developers (to be documented in Deliverable D083)

Question (CF2): Which types of operators does the pilot support or augment their capabilities and how?

Answer (ZDMP): In the construction case AR/VR operator and Smart and Analytical operator are relevant. In general, the taxonomy of operator types seems pertinent.

7.3.4 KYKLOS4.0 – An advanced circular and agile manufacturing Ecosystem based on rapid reconfigurable manufacturing process and individualized consumer preferences.

KYKLOS 4.0 aims to develop an innovative Circular Manufacturing ecosystem based on novel CPS and AI based technologies, enhanced with novel production mechanisms and algorithms, targeting on personalised

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

products with extended life cycle and promoting energy efficient and low material consumption intra-factory production processes, resulting reduced greenhouse gas emissions and air pollutants.

In KYKLOS4.0 the pilot cases need further analysis in terms of the human factors involved towards smart manufacturing (Aerospace Pilot 1, Aerospace Pilot 2) and circular manufacturing (Electronic Devices/Equipment Pilot, Heavy Equipment Industry, Shipyard Pilot, Food Industry Pilot, Automotive Pilot). At this point of time KYKLOS4.0 pilot cases cannot be analysed in terms of human factors addressed in the project.

A workshop took place with the KYKLOS4.0 project participants to discuss on Human Factor issues in the project. A summary of the workshop is presented hereafter.

Question (CF2): Based on the experience of the pilot case do you think that new job profiles should be defined to master the new technologies, practices etc?

Answer (KYKLOS4.0):

- **Pindos industrial case:** Yes, there is a need for new job profiles (see answer in the second question below)
- **GRC industrial case:** Probably not. However, the profiles of existing roles may need to be enriched with understanding of the high potential value of data, analytics and optimization (but not necessarily requiring related skills).
- ***PROMEDICARE industrial case:*** Within the interventions envisaged for the development of this pilot case, various professional figures were identified, so that the development of the entire project could be continued. First of all it was necessary the intervention of mechanical and biomedical engineers who dealt with the design of the entire integrated posture system, providing a general picture of the level of customization and adjustment that the product can provide. Obviously at the base there is an in-depth study of what are the pathologies of the patient who needs a wheelchair and how to act on the correction of the patient's posture. Following a discussion with Promedicare on the technical specifications relating to the product, research work was carried out on the current state of the art, necessary to identify in detail the points on which to act in order to improve the entire production cycle of a customizable product. As specified in other points, the customer can proceed directly from his home to share his anthropometric data which will then be transformed into production input and delivery of the final product. In order to obtain a usable web interface, the collaboration of IT engineers and software technicians was necessary. In addition, the contribution of CAD modelers was necessary for the creation of parametric models of the product and software developers expert in AR technology for the development of a web platform on which to design an interactive manual and a mobile application for reading the manual. AR developed. For the activities carried out so far it does not seem necessary to create a new professional figure.
- **Astander industrial case:** Training on how to manage, obtain data in addition to the new operation of the crane.

Question (CF2): Based on the experience of the pilot case is there a need for re-skilling/up-skilling of personnel to master the new technologies, practices etc? If yes, can you name a few skills that are missing or needed? For example, IT skills, data analysis skills, management skills etc.

Answer (KYKLOS4.0):

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- **Pindos industrial case:** Yes, automation engineering skills, data analysis skills, IT and IIoT infrastructure engineers.
- **GRC industrial case:** (See previous answer)
- ***PROMEDICARE industrial case:*** It might be useful to think of increasing project management skills for all professionals involved in the pilot project. Furthermore, it would also be useful for all project partners to have a clear idea of how a software architecture (relative to the case study examined) can be developed and managed, and how it can be interfaced both with AR technologies and with the management of parametric CAD modules. A further important aspect is certainly that of being able to have access to an update on one's skills related to ergonomics and anthropometric standards.
- **Astander industrial case:** IT skills, data analysis skills and cybersecurity

Question (CF2): What type of knowledge delivery mechanisms (e.g. vocational training, on the job training, MOOCs, AR/VR) would be more adequate for re-skilling/up-skilling purposes of the final users of the pilot case results?

Answer (KYKLOS4.0):

- ***Pindos industrial case:*** On the job training.
- **GRC industrial case:** On-the-job training
- ***PROMEDICARE industrial case:*** End users will not need to access specific IT or technological skills, as the interaction they will have with the results of the pilot case will be made extremely intuitive and simple to use. It will be necessary to have technological devices to be able to share their data which will be the input of a customized production of the product.
- **Astander industrial case:** crane operation- AR/VR , data- job training

Question (CF2): Are you aware of any learning and training initiatives in Europe that fit to the re-skilling/up-skilling needs of the pilot case?

Answer (KYKLOS4.0): It would be useful if each company participating in a European project could receive information in advance on any re-skilling / up-skilling sessions in relation to the topics that will be addressed within the project.

Question (CF2): Which types of operators does the pilot support or augment their capabilities?

Answer (KYKLOS4.0):

- ***Pindos industrial case:*** Augmented and virtual operator, one-of-a-kind operator, Smarter and analytical operator
- **ADSYS industrial case**: Smarter and analytical operator.
- **GRC industrial case:** Smarter and analytical operator – for example, providing human planners with the analytics and intelligence to identify potential issues in the flow of parts, and suggest solutions.
- ***PROMEDICARE industrial case:*** Augmented and virtual operator, one-of-a-kind operator.
- **Astander industrial case:** Augmented and virtual operator, Social and collaborative operator, Smarter and analytical operator.
- In general, the proposed taxonomy is adequate.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

7.3.5 DIGIPRIME – Digital Platform for Circular Economy in Cross Sectorial Sustainable Value networks.

Digital technology plays a big role in our transition to a circular economy, which aims to make optimum use of resources within industries. Investing in innovation is good for the protection of the environment, and it also contributes to Europe's competitiveness. The EU-funded DigiPrime project will develop the concept of a circular economy digital platform to create circular business models based on the data-enhanced recovery and reuse of functions and materials. Specifically, it will create and operate a federated model of digital platforms for cross-sector business in the circular economy. DigiPrime will be validated through several cross-sectoral pilots, further detailed in 20 use cases covering different European industrial sectors (automotive, renewable energy, electronics, textile, construction), and by additional pilots in new sectors, funded through an open call mechanism.

A workshop took place with the DIGIPRIME project participants to discuss on Human Factor issues in the project. A summary of the workshop is presented hereafter.

Question (CF2): Based on the experience of the pilot case do you think that new job profiles should be defined to master the new technologies, practices etc?

Answer (DIGIPRIME):

- Skills to manage batteries and more general energy storage systems production are missing.

Question (CF2): Based on the experience of the pilot case is there a need for re-skilling/up-skilling of personnel to master the new technologies, practices etc? If yes, can you name a few skills that are missing or needed? For example, IT skills, data analysis skills, management skills etc.

Answer (DIGIPRIME):

- To acquire skills for batteries' production a combination of both training of engineers for example in Technical Universities and targeted reskilling activities could be employed. Curricula are adapted in manufacturing engineering course to address those needs.
- It is not a matter of how digital technologies work but also how to adapt the work process to interact properly with the technologies.
- In traditional production sectors, such as composites, it is even more difficult to find the skills and for the people in such industry to understand the importance of data.

Question (CF2): What type of knowledge delivery mechanisms (e.g., vocational training, on the job training, MOOCs, AR/VR) would be more adequate for re-skilling/up-skilling purposes of the final users of the pilot case results?

Answer (DIGIPRIME):

- On the job training is the most relevant mechanism especially from the operator point of view.
- At the managerial level other mechanism could be relevant such as MOOCs.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- Regional level training through Competence Centres and Digital Innovation Hub that "speak the same language".

Question (CF2): Are you aware of any learning and training initiatives in Europe that fit to the re-skilling/up-skilling needs of the pilot case?

Answer (DIGIPRIME):

- BEPA (PPP on batteries) are developing some L&T activities.

Question (CF2): Which types of operators does the pilot support or augment their capabilities?

Answer (DIGIPRIME):

- Keep the proposed classification and maybe consider adding a new role of the "Environment conscious operator", in general an operator that understands the environmental impact of the manufacturing task, and there are technologies around him/her to support on this objective.

7.3.6 SHOP4CF – Smart Human Oriented Platform for Connected Factories

SHOP4CF, Smart Human Oriented Platform for Connected Factories, aims to find the right balance between cost-effective automation, repetitive tasks and involve the human workers in areas such as adaptability, creativity, and agility where they create the biggest added value. SHOP4CF aims to pursue the highly connected factory model to reap the benefits of all the data generated within the factory[49].

SHOP4CF platform will provide technological solutions that will **improve the well-being and working conditions of human workers**, automatizing monotonous and exhaustive tasks and increasing their productivity due to technological support. To contribute to the human-robot collaboration on the shopfloor, SHOP4CF develops and integrates components and supporting tools to the platform that lead to a great support in the different stages of the manufacturing process. Moreover, the supporting tools will facilitate the design and deployment of the human-centric manufacturing processes. The components and supporting tools are highly designed to best complement the collaboration between human & technology. SHOP4CF fosters the ability to swiftly adapt the manufacturing capacities and will ensure the safety of the human operators while working in a highly robotic and digitized environment.

To mitigate such challenges, a set of augmented / virtual reality tools were developed in various projects by different partners associated in the SHOP4CF project. Those components include, for example, virtual planning of safety behavior, augmented reality projection of assembly instructions or digital twins of production lines to monitor the condition. The relevance of those tools has been already validated in different research projects and verified in various research scenarios.

SHOP4CF foresees pilot cases in four industrial users.

- ARCELIK case: The second ARCELIC case involves a central team of engineering experts that remotely support the local factories through augmented reality (AR) and virtual reality (VR) tools. The

[49] https://www.shop4cf.eu/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

SHOP4CF augmented reality interface environment using interactive computer monitors and AR/VR glasses will be used. This will enable the efficient use of expert human resources to solve technical problems, reduce the efforts (site visiting, equipment transport and travel needs) and reduce the error-rate caused by humans.

- The Volkswagen Wrzesnia factory case aims at supporting workers to eliminate ergonomically incorrect work postures during Chassis Shielding. In the same manner, visual inspection of paint quality issues will relief workers from eye-tiredness and allow them to concentrate on other tasks that require more advanced human decision-making capabilities.
- Robert Bosch España Fábrica Madrid case aims to employ collaborative robot that picks up the Printed Circuit Boards (PCB) and transfers them to the working stations and/or to the testing stations. The human, assisted with an AR system which provides real-time instructions and records any action thus, improving quality and reducing errors, places the electronic components on the board, to be then transferred to the soldering station by the collaborative robot.
- Siemens pilot aims at supporting human operator during the assembly of a medical product with the use of collaborative robots.

A workshop took place with the SHOP4CF project participants to discuss on Human Factor issues in the project. A summary of the workshop is presented hereafter.

Question (CF2): Based on the experience of the pilot case do you think that new job profiles should be defined to master the new technologies, practices etc?

Answer (SHOP4CF):

- IT-skills: AR technology. E.g., remote support, assembly
- Use of remote support tools (AR) require new competence and new working methods. Remote support sessions will be a novel work task.
- Robot programming skills / human-robot collaboration skills
- Planning / management skills
- System maintenance skills (IT-skills…)
- Management skills
- Related to increasing autonomy of the workers
- Process management skills related to new systems
- Data analysis skills

Question (CF2): Based on the experience of the pilot case do you think that new job profiles should be defined to master the new technologies, practices etc?

Answer (SHOP4CF):

- For new work tasks:
  - Training responsible role,
  - Process responsible role – should consider changes of work from all relevant persons viewpoint (worker involvement in planning)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

- One goal is the up skilling of personnel (robot programming, digital twin creation…), so that external experts would not be needed. Shift from *normal* operator to more *skilled expert*.
- Monitoring role: Analysis skills

Question (CF2): *Which types of operators does the pilot support or augment their capabilities?* **Answer (SHOP4CF):** All types of operators are relevant.

Question (CF2): What type of knowledge delivery mechanisms (e.g., vocational training, on the job training, MOOCs, AR/VR) would be more adequate for re-skilling/up-skilling purposes of the final users of the pilot case results?

Answer (SHOP4CF):

- On the job training
- Flexible microlearning processes (small learning units and short-term learning activities); collaborative learning with peer support
- RAMP marketplace should provide training material

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.

8 Conclusions

This deliverable has summarized the work carried out on CCFs along the project.

During this first half of the project, an important work has been developed describing and dividing the different CCFs. As a result, the structured wiki has been deeply modified.

On the second phase of the project, the analysis of CCF in the different ICT-07 projects has been carried out.

The connection between CF2 and the DMP cluster is working properly and lots of interactions and collaborations are coming out of it.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 873086.