
# D4.1

# Early Deployment of Eur3ka R3 Service Platforms and Infrastructures

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016175

# D4.1 Early Deployment of Eur3ka R3 Service Platforms and Infrastructures

| | |
|---|---|
| **Work Package:** | WP4 |
| **Lead partner:** | INTRASOFT International S.A (INTRA) |
| **Author(s):** | John Soldatos (INTRA), Nikos Kefalakis (INTRA), Georgios Makantasis (INTRA)<br>INTRA, ENG, IOSB, IMECH, INNO, VIS, SIEL |
| **Due date:** | 28/02/2021 |
| **Deliverable Type:** | Report |
| **Version number:** | 1.0 **Status:** Final |

| | |
|---|---|
| **Project Number:** | 101016175 **Project Acronym:** Eur3ka |
| **Project Title:** | *EUropean Vital Medical Supplies and Equipment Resilient and Reliable Repurposing Manufacturing as a Service NetworK for Fast PAndemic Reaction* |
| **Start date:** | December 1st, 2020 |
| **Duration:** | 24 months |
| **Call identifier:** | H2020-SC1-PHE-CORONAVIRUS-2020-2-NMBP |
| **Topic:** | SC1-PHE-CORONAVIRUS-2020-2A<br>Repurposing of manufacturing for vital medical supplies and equipment. |
| **Instrument:** | IA |

| **Dissemination Level** | |
|---|---|
| PU: Public | ✓ |
| PP: Restricted to other programme participants (including the Commission) | |
| RE: Restricted to a group specified by the consortium (including the Commission) | |
| CO: Confidential, only for members of the consortium (including the Commission) | |

# Revision History

| Revision | Date | Who | Description |
|---|---|---|---|
| 0.1 | 18/01/2021 | INTRA | First release of the ToC, identified partners responsibilities |
| 0.2 | 29/01/2021 | INTRA | Added FAR-EDGE platform |
| 0.3 | 01/02/2021 | ENG | Added TRUE connector |
| 0.4 | 02/02/2021 | IOSB | Added SFW Platform and Factory Trusted connector |
| 0.5 | 03/02/2021 | IMECH | Makers and Fablabs connectors |
| 0.6 | 10/02/2021 | INTRA | Added deployment strategy and infrastructures & tools |
| 0.7 | 15/02/2021 | INNO | Added M3 Workspace, M3 Trusted IDS Connector |
| 0.8 | 16/02/2021 | INTRA | Added the introduction |
| 0.9 | 17/02/2021 | VIS | Added Visual Components 4.0 |
| 0.10 | 02/03/2021 | INTRA | Added Infrastructure topology of the Eur3ka Ecosystem |
| 0.11 | 04/03/2021 | INTRA | Added executive summary and conclusions |
| 0.12 | 08/03/2021 | INTRA | Prepared the deliverable for internal review |
| 0.13 | 10/03/2021 | STAM | Provided internal reviewer comments |
| 0.14 | 10/03/2021 | ETHZ | Provided internal reviewer comments |
| 0.15 | 11/03/2021 | INTRA | Addressed Reviewers comments. |
| 0.16 | 19/03/2021 | SIEL | Added AMN Trusted+ Connector |
| 0.17 | 19/03/2021 | INTRA | Integrated additional contributions, prepared the deliverable for final submission |
| 1.0 | 19/03/2021 | ENG | Final coordinator review before submission |

# Quality Control

| Role | Date | Who | Approved/Comment |
|---|---|---|---|
| Internal review | 10/03/2021 | STAM | Approved |
| Internal review | 10/03/2021 | ETHZ | Approved/provided comments |

# Disclaimer

# Executive Summary

The main goal of the Eur3ka project is to develop, provide and validate a pool of smart production services that will boost the manufacturers' ability to respond to large-scale disruptions of their production processes rapidly and successfully. Eur3ka is largely motivated by the disruption caused by the COVID19 pandemic and aims at providing a complete manufacturing Plug & Response framework that will enable manufacturing enterprises to cope with the adverse implications of the healthcare crises on their production. The development and deployment of the Eur3ka framework leverages existing manufacturing platforms of the partners. Specifically, the project aims at integrating diverse platforms for flexible production lines and supply chains towards easing the trusted sharing of production information across different stakeholders. Trusted data sharing is therefore at the very core of the Eur3ka solution. In this context, this deliverable illustrates the ways existing platforms will be deployed in the scope of Eur3ka, including information on how they will be integrated in a coherent solution.

Trusted information exchange takes place through the Eur3ka data space, which will be established in-line with the principles of International Data Spaces (former Industrial Data Space). The deliverable illustrates the structure and topology of the Eur3ka data space, along with the infrastructures that will enable stakeholders to join the data space and exchange data through it. The latter include the Eur3ka identify management and access control infrastructures, as well as monitoring and control tools. Along with these infrastructures, the deliverable presents the main deployment tools that will be used, notably tools for the packaging and distribution of digital manufacturing components.

Various platforms will be deployed around the International Data Space infrastructure. These platforms include for example the Smart Factory Web (SFW) platform for flexible supply chain management operations, the M3Workspace solution for metrological operations and quality control assurance, the Visual 4.0 3D simulation platform, as well as a distributed data analytics platform. The integration of these platforms in the data space will be based on the implementation and deployment of trusted connectors, which will support the secure and reliable exchange of data with the data space. The deliverable presents the main connectors that will be developed and used.

The deliverable provides an outline of the main platforms to be used and the way they will be integrated with the data space. In several cases, these platforms are available and deployed as Docker component i.e., they are almost ready for integration in the Eur3ka platform. Nevertheless, the technical details are provided at a high level only. More technical details will be provided in a subsequent version of this deliverable i.e., deliverable D4.2 of the project. Likewise, some important technical details for the platforms and the data spaces are elaborated in other work packages of the project and their respective deliverables. For instance, the overall architecture of the Eur3ka platform that will drive the integration of the Eur3ka services is currently under development in WP2, while the semantics of the information to be exchanged via the connectors is being elaborated in WP3. These on-going work streams will help completing the deployment of the Eur3ka service platforms as part of deliverable D4.2.

# Table of Contents

# List of figures



# List of Tables

# Definitions and acronyms

| | |
|---|---|
| AMN | Additive Manufacturing Network |
| CAD | Computer-Aided Design |
| CCE | Clinical Care Equipment |
| CE | Community Edition |
| CLI | Command Line Input |
| CNC | Computer Numerical Control |
| CPPS | Cyber Physical Production Systems |
| CSV | Comma-Separated Values |
| DDA | Distributed Data Analytics |
| DMP | Data Management Plan |
| EAE | Edge Analytics Engine |
| EC | European Commission |
| ECC | Execution Core Container |
| EU | European Union |
| GUI | Graphical User Interface |
| IDS | International Data Spaces |
| LDAP | Lightweight Directory Access Protocol |
| OPC UA | OPC Unified Architecture |
| P&R | Plug & Respond |
| PAAS | Platform As A Service |
| PPE | Personal Protection Equipment |
| PPE | Personal Protection Equipment |
| RAM | Reference Architecture Model |
| RBAC | Role-Based Access Control |
| SAML | Security Assertion Markup Language |
| SFW | Smart Factory Web |
| SMMA | Smart Matching Mediation App |
| TRUE | TRUsted Engineering |
| UC APP | Usage-Control Application |
| VIS | Visual Components |
| VR | Virtual Reality |
| WP | Work Package |
| XML | eXtensible Markup Language |
| YAML | YAML Ain't Markup Language |

# 1 Introduction

## 1.1 Scope and Purpose

Following the pandemic outbreak, manufacturers, industrial managers, and policy makers focused on the implementation of strategies for revamping production patterns and meet consumer demand for specific products, such as Clinical Care Equipment (CCE) and Personal Protection Equipment (PPE). Likewise, manufacturers and their suppliers started analysing supply chain operations to support the new requirements. Furthermore, it become apparent that production should become more agile and flexible against future disruptions. In this direction, digital manufacturing technologies and Cyber Physical Production Systems (CPPS) could play a key role through unlocking the flexibility potential of Industry 4.0 (I4.0).

Eur3ka is a joint effort of manufacturers and I4.0 experts to provide a Plug & Respond (P&R) framework for flexible manufacturing that could enable the rapid adaptation and repurposing of production in the scope of disruptive events such as the COVID19 healthcare crises. The Eur3ka P&R framework will be empowered by a range of digital manufacturing technologies, which will be integrated and will interact with each other in-line with an open, standardized, modular, digital manufacturing architecture.

The present deliverable is destined to provide an outline of the main platforms to be used as an early deployment of the Eur3ka provided services. Moreover, it lists available connectors that can be used as part of the applications to manipulate data from the available platforms. Additionally, deliverable provides/references installation and usage guidelines of the offered platforms and connectors. Finally, it provides information on the deployment architecture based on the IDS reference model and the access control schemes that are also provided there.

## 1.2 Relevance to Other Deliverables

The deliverable describes the initial platforms and connectors along with the deployment schemes that are going to be offered by the Eur3ka ecosystem. As such it is relevant to most of the technical deliverables of the project, as most of them are referencing the utilization of the infrastructure that is listed in D4.1. However, there are two deliverables with similar development timelines as D4.1, which are the most closely related to the present deliverable. Specifically:

- Deliverable D2.1 “Eur3ka Manufacturing Repurposing Reference Framework & Data Management Plan (DMP)” is the deliverable that specifies the reference architecture of the project. D4.1 should be generally aligned to D2.1 i.e., the services presented in this deliverable must be aligned to the structuring principles for the Eur3ka components that will be specified in D2.1.
- Deliverable D3.1 “Early Rapid Medical CCE/PPE Production Specifications & Eur3ka R3 Service Definition”, which provides the specification of the Eur3ka ecosystem. As such D3.1 provides the specification of the services that are going to be offered thru the Eur3ka ecosystem along with the different platforms and tools.

Overall, the three deliverables listed above (i.e., D2.1, D3.1, D4.1) will provide a sound basis for implementing and integrating the Eur3ka framework.

## 1.3 Structure of the Document

The rest of the deliverable is structured as follows:

- Section 2 following this introductory paragraph, presents the deployment strategy and describe how it can be utilized by external applications. It provides information about the infrastructure topology but also tools that are going to be utilised for the platform management, monitoring and access control.
- Section 3 presents the different platforms and connectors that are going to be used for an early deployment of the Eur3ka services along with installation and usage guidelines and references to detailed documentation of the different platforms and connectors in order to facilitate their deployment and setup.
- Section 4 is the final and concluding section of the deliverable. It draws main conclusions and provides an outlook for the future developments.

# 2 Infrastructure Deployment Strategy

This section presents the deployment strategy and describe how it can be utilized by external applications. It provides information about the infrastructure topology but also tools that are going to be utilised for the platform management, monitoring and access control.

## 2.1 Infrastructure topology of the Eur3ka Ecosystem

As mentioned in D3.1 “Early Rapid Medical CCE/PPE Production Specifications & Eur3ka R3 Service Definition” deliverable, Eur3ka is going to adopt the International Data Spaces (IDS) initiative (former Industrial Data Space) RAM (Reference Architecture Model) which propose an architecture for secure data exchange and trusted data sharing. IDS position itself as an architecture that links different cloud platforms through policies and mechanisms for secure data exchange and trusted data sharing. Over the IDS Connector, the International Data Space’s central component, industrial data clouds, as well as individual enterprise clouds, on-premises applications and individual, connected devices can be connected to the International Data Spaces (see Figure 2-1 below).

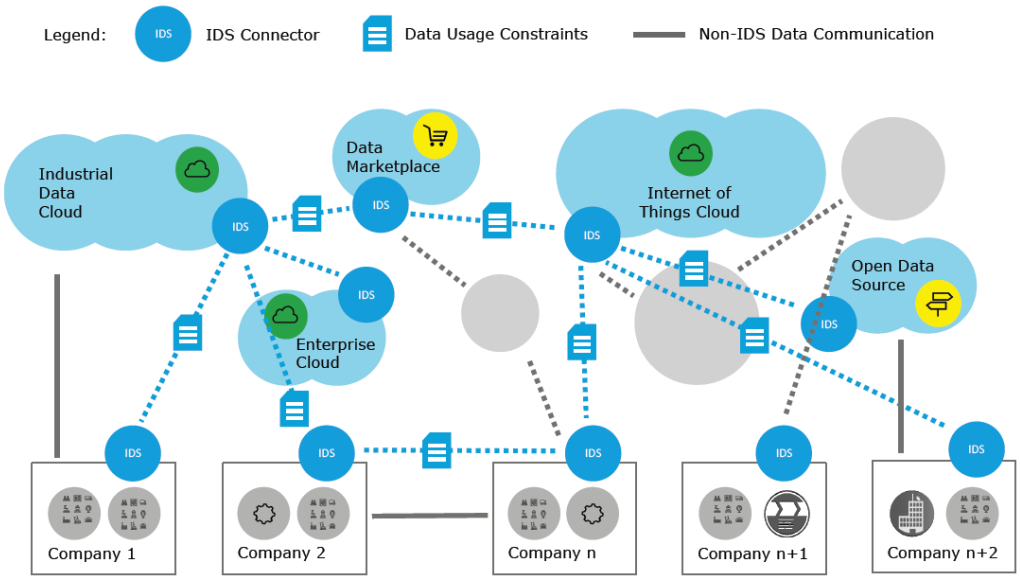


*Figure 2-1 International Data Spaces Connecting Different Cloud Platforms[1]*

To this end, in this early deployment of the Eur3ka service platform and Infrastructures, we are going to use some readily offered solutions that are brought to the project form the partners of the Eur3ka consortium. These solutions are consisted from Platforms and connectors that following the IDS paradigm can be deployed as cloud services and can be utilized at this point thru the offered connectors.

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

### 2.1.1 IDS Connector

The IDS MA identifies the System Layer, which is the technical core of the International Data Spaces. Figure 2-2 below depicts the interaction of the components that consist the System layer which are the Connector, the Broker and the App Store.

A distributed network like the International Data Spaces relies on the connection of different member nodes where Connectors or other core components are hosted. The Connector is responsible for the exchange of data or as a proxy in the exchange of data, as it executes the complete data exchange process from and to the internal data resources and enterprise systems of the participating organizations and the International Data Spaces.

Two fundamental variants are the Base Connector and the Trusted Connector (see Section 4.1) as they differ in the capabilities regarding security and data sovereignty. Connectors can be further distinguished into External Connectors and Internal Connectors where:

- An External Connector executes the exchange of data between participants of the International Data Spaces
- An Internal Connector is typically operated in an internal company network (i.e., a network which is not accessible from outside)

Some of these types of connectors are provided from Eur3ka partners and are listed in section 3.2. More details on the IDS Connector can be found at the IDS RAM.

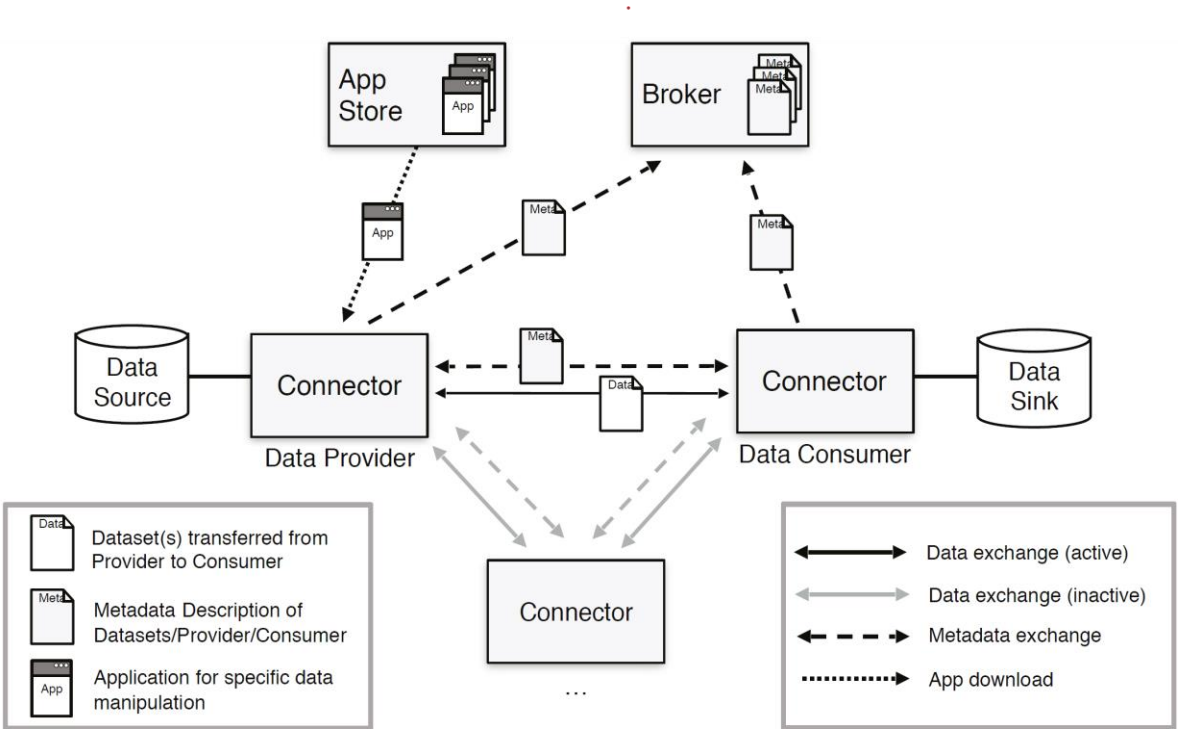


*Figure 2-2 IDS technical components interaction*[2]

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

## 2.2 Deployment and Packaging Strategy

From the different artefacts distribution and deployment methodologies, described in section 3, it becomes evident that the most common packaging strategy is Docker containers and deployment strategy is Docker Compose. Docker is an open platform for developing, shipping, and running applications. With Docker, an infrastructure can be managed in the same way's applications are managed. Docker offers shipping, testing, and deploying methodologies easily and quickly, where time between writing code and running it in production can be significantly reduced. Finally Docker offers container isolation which allows implementation of additional security features, such as time-to-live policy enforcement for complete container instantiations as described in IDS RAM[3].

Docker compose uses YAML files to configure the application's services and performs the creation and start-up process of all the containers with a single command. The docker-compose.yml file is used to define an application's services and includes configuration options. Information on how to edit a docker-compose.yml file can be found at Docker Docs and more specifically at the Get started with Docker Compose[4]

## 2.3 Infrastructure Tools

In this section, we provide a list of tools that can be deployed to the Eur3ka infrastructure to facilitate the deployment and runtime of the platform. These tools may enable management, monitoring and access control capabilities.

### 2.3.1 Access Control

In order to offer secure access to the infrastructure and more specifically for the platforms and services that does not implement authentication the option of a SSO (Single Sign On) identity and access management will be offered. One of the Most commonly used Open-Source identity and access management software is the Keycloak[5]. Some of the Key features of Keycloak are that it:

- Provides Single-Sign On functionality,
- Offers standard protocols like OpenID connect, OAuth 2.0 and SAML 2.0,
- Offers centralized management,
- Offers adapters for applications and services,
- Provides LDAP and active directory to connect existing user directories.

[3] https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf
[4] https://docs.docker.com/compose/gettingstarted/
[5] https://www.keycloak.org/

Directions on how to install Keycloak using Docker can be found at the Keycloak on Docker page[6]. Moreover, all the information related with the Keycloak functionalities, deployment and usage can be found at the Keycloak's documentation[7].

#### 2.3.1.1 Authorization Policies

Keycloak supports fine-grained authorization policies[8] and can combine different access control mechanisms one of which is the Role-based access control (RBAC). RBAC can be utilised in specifying the roles identified in the International Data Spaces. Some of the core IDS[9] roles are:

- **Data Owner**: which is a legal entity or natural person creating data and/or executing control over it.
- **Data Provider**: which possesses data sources and offers data from these sources to be used by other participants in the International Data Space.
- **Data Consumer**: which receives data from a Data Provider
- **Data User**: is the legal entity that has the legal right to use the data of a Data Owner as specified by the usage policy.
- **Broker**: which acts as a mediator between Data Providers offering data and Data Users requesting data.
- **App Provider**: which is a participant of the IDS ecosystem that develops software to be offered thru the AppStore.
- **Certification Authority**: which makes sure that the software components of the International Data Space meet the requirements jointly defined by the participants and rules and standards are observed.

Figure 2-3 below identifies some of the basic interactions taking place between the different roles in the International Data Spaces that will be considered in the Keycloak setup (X --> mandatory interaction, (X) --> optional interaction).

[6] https://www.keycloak.org/getting-started/getting-started-docker
[7] https://www.keycloak.org/documentation
[8] https://www.keycloak.org/docs/latest/authorization_services/
[9] https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf

| | Data Owner | Data Provider | Data Consumer | Data User | Broker | Clearing House | Identity Provider | Service Provider | App Provider | App Store | Vocabulary Provider | Certification Body | Evaluation Facility |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Data Owner | - | X | - | - | - | (X) | - | (X) | (X) | (X) | (X) | - | (X) |
| Data Provider | X | - | X | | X | (X) | X | (X) | (X) | (X) | (X) | - | X |
| Data Consumer | - | X | - | X | (X) | (X) | X | (X) | (X) | (X) | (X) | - | X |
| Data User | - | - | X | - | - | (X) | - | (X) | (X) | (X) | (X) | - | (X) |
| Broker | - | (X) | (X) | - | - | - | X | (X) | - | - | ? | - | X |
| Clearing House | - | (X) | (X) | - | - | - | (X) | - | (X) | (X) | (X) | - | X |
| Identity Provider | - | X | X | - | X | (X) | Federation | - | (X)? | (X)? | - | - | X |
| Service Provider | (X) | (X) | (X) | (X) | (X) | - | - | - | (X) | (X) | (X) | - | X |
| App Provider | (X) | (X) | (X) | (X) | - | (X) | (X) | (X) | - | (X) | - | - | (X) |
| App Store | (X) | (X) | (X) | (X) | - | (X) | (X)? | (X) | (X) | - | (X) | - | (X) |
| Vocabulary Provider | (X) | (X) | (X) | (X) | ? | (X) | - | (X) | (X) | (X) | - | - | X |
| Certification Body | - | - | - | - | - | - | - | - | - | - | - | - | X |
| Evaluation Facility | (X) | X | X | (X) | X | X | X | X | (X) | X | X | X | - |

*Figure 2-3 Interactions between roles in the IDS*[10]

## 2.3.2 Infrastructure Management & Monitoring

Since the preferred deployment strategy is the Docker containerization in order to facilitate the ecosystem management and monitoring there are various offerings one of which is the Community Edition (CE) of Portainer.[11]

Portainer CE is a lightweight management toolset that allows you to easily build, manage and maintain Docker environments. Portainer offers a GUI (Graphical User Interface) which alleviates the complexity of using CLI (Command Line Input) commands. Portainer offers the following features which can be used over the Eur3ka infrastructure:

- UI that covers all of essential docker CLI actions
- Enhanced functions, not available from the command line
- Expert configuration built into the software
    - Including pre-validation checks for complex deployments
- Management of access control and LDAP authentication
- Aggregation view of swarm clusters
- Log viewer
- Remote console with process performance viewer

Directions on how the technology providers can install Portainer environment in a local Docker instance can be found at the Portainer's Deployment[12] documentation.

[10] https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf
[11] https://www.portainer.io/products-services/portainer-community-edition/
[12] https://portainer.readthedocs.io/en/stable/deployment.html

# 3 Eur3ka Infrastructure Deployment & Setup

In this section we provide an overview of the different platforms and connectors that are going to be used for an early deployment of the Eur3ka services. Within this section we also provide high level installation and usage guidelines and references to detailed documentation of the different platforms and connectors to facilitate their deployment and setup.

## 3.1 Platforms

### 3.1.1 SFW Platform

#### 3.1.1.1 Requirements

To get started you need to install Docker on your system. Information about the Docker installation can be found here[13]

#### 3.1.1.2 Login to the Docker registry

After a successful installation you need to login to the Fraunhofer IOSB docker registry to get access to the Docker image.

Open a command line interface of your operating system. In the following example, it is shown for Windows. The steps for Linux are analogous.

Open the Windows terminal (cmd.exe):

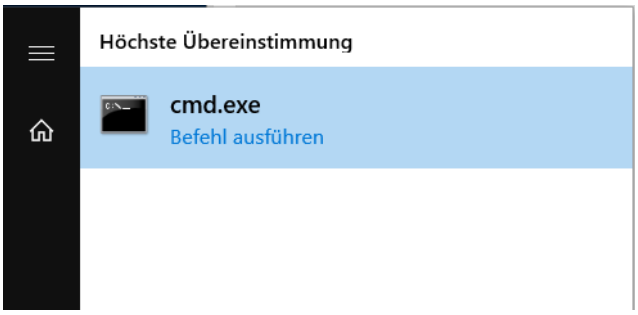


*Figure 3-1 Command terminal for Windows*

In the Windows terminal, execute the following command:

“docker login gitlab-ext.fraunhofer.iosb.de:4567” and enter your username and password.

#### 3.1.1.3 Downloading the Docker image

Open the Fraunhofer IOSB repository (https://gitlab-ext.iosb.fraunhofer.de/) and login with the provided credentials. You should see the smartFactoryWeb4Eur3ka group with the sFw4Eur3ka repository. Download the files as zip archive:

[13] https://docs.docker.com/compose/install/

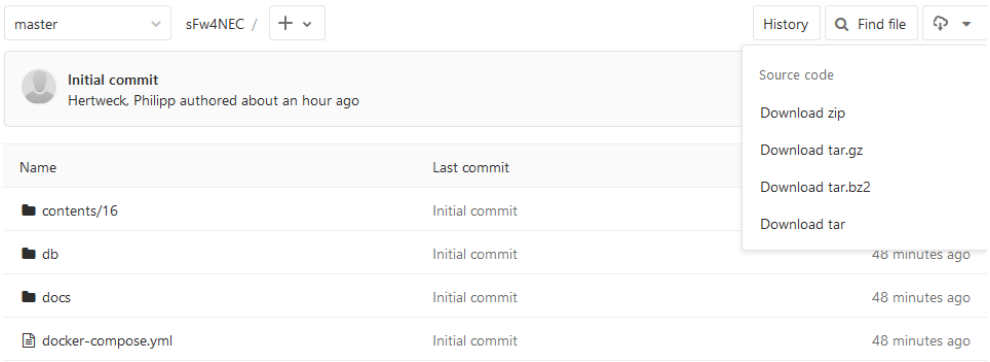


*Figure 3-2 Content of the Docker repository for Eur3ka*

Extract the zip file and move it to a suitable location on your system. Open the "docker-compose.yml" in a text editor. You need to adapt the path (actually "C:\sfw") to the extracted folder. All data will be stored inside this directory.

The image includes an executable of WebGenesis®, a product of Fraunhofer IOSB that provides a framework for the generation and support of web-based information systems[14]. The Smart Factory Web ontology and functions to manage assets are also included. The ontology can be can adjusted in the running instance.

#### 3.1.1.4 Start the server

To start SmartFactoryWeb open a command line and navigate to the extracted folder. Running "docker-compose up –d" starts the server. You can access it by opening "localhost" (host name of computer where command was executed) in your web browser.

To shut down the server, open a command line in this folder and execute "docker-compose down".

## 3.1.2 Visual 4.0 Platform

### 3.1.2.1 Description

Visual Components 4.0 is the fourth generation of a well-known commercial 3D simulation platform developed and commercialized by Visual Components (VIS). Compared to the previous versions, which were based in COM technology, the product family 4.0 offers a totally redesigned 3D simulation and visualization set of digital tools for factory simulation based in .Net technology.

Visual Components' simulation platform implements open interfaces and is brand independent supporting the simulation and validation in the virtual environment of products from different vendors, supporting the users' manufacturing virtualization requirements from concept until decommissioning.

The simulation is based on parametric virtual components which allows easy tailoring and configuration to the different simulation demands. The open interfaces, which enables

[14] https://www.iosb.fraunhofer.de/servlet/is/21107/?highlight=webgenesis

creating the digital twin in the virtual environment, allow to design and connect the virtual environment to most of the automation solution providers in the market. Open APIs (Python and .Net) facilitate to extend the capabilities of the simulation environment with new extensions to reach the production demands. The available communication interface supports virtual commissioning technologies and big data analysis, providing connectivity for OPC UA, Siemens S7, Beckhoff ADS, UR RTDE, SIMIT, WinMOD Net and can be extended with FIWARE connectivity.

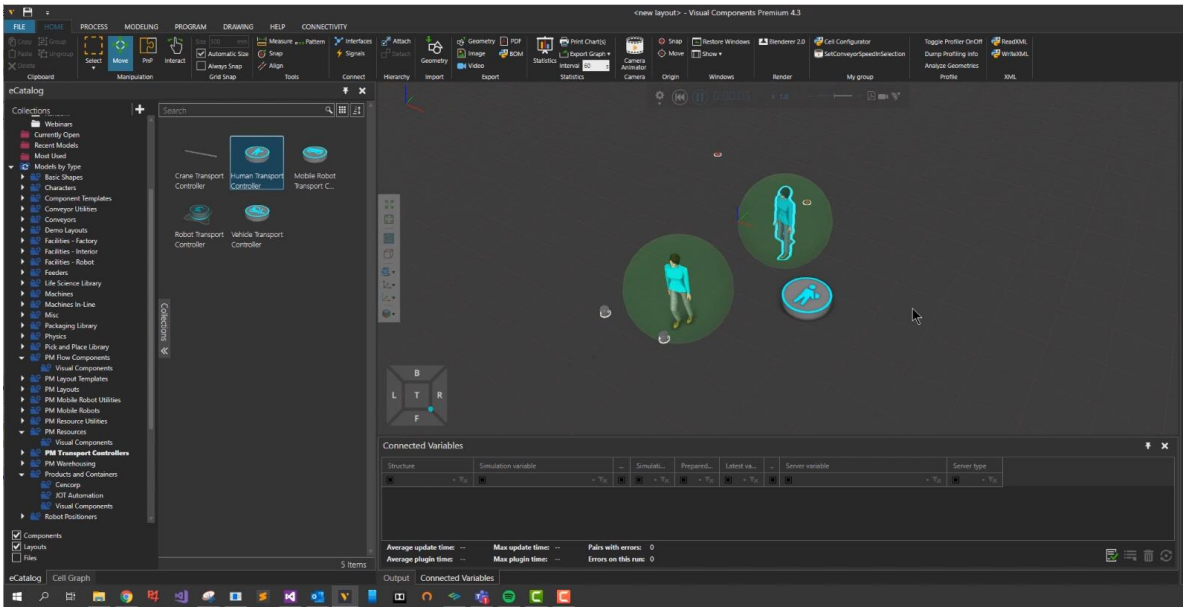

***Figure 3-3 Screenshot of Visual Components 4.0 (R4.3), simulating a production scenario to validate interpersonal distance.***

Visual Components 4.0 can be connected to the most popular VR systems using Visual Components Experience[15]. Visual Components Experience provides an immersive interactive 3D environment, also known as Virtual Factory (concept developed at Factory2Fit project), where designers can interact with the virtual manufacturing systems to improve the design and detect errors already in the initial states of the design, even before the real system has been started to be built. Operators can start training parallel to the initial design phases providing their feedback, and accelerating ramp up when new products start to be manufactured. The VR data sets can be used in 3rd party providers to be used in collaborative VR environments where several operators or engineers can meet simultaneously.

[15] https://www.visualcomponents.com/visual-components-experience/

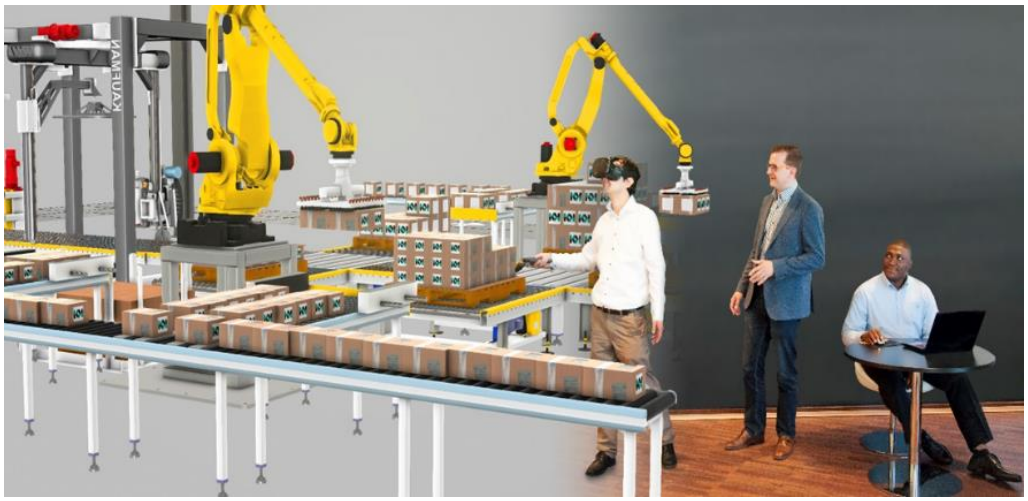

*Figure 3-4 Detail of a virtual factory layout generated in Visual Components 4.0 and VR interaction*

#### 3.1.2.2 Availability

Visual Components 4.0 is distributed as standalone solution and requires a valid license and acceptance of the EULA[16] to be used. The installers of the latest release can be downloaded from Visual Components website[17]. The solution is Windows based and requires 64-bit operation system, Windows 8.1 or preferable Windows 10.

Hardware recommended specifications comprises Intel i7-8xxx processor or equivalent with a minimum of 8GB of RAM and 3GB of available space at the HDD. Graphical requirements include a graphic card, Nvidia GPU with at least 4GB of dedicated memory. To properly handled the virtual models three buttons mouse is recommended and 3D mouse is also supported.

For using VR headsets to visualize and interact within the virtual factory, it is required to install Visual Components Experience, available in the same download link, where it is possible to also find the SIMIT external coupling for Siemens SIMIT software for virtual commissioning. Visual Components experience is also available for downloading in mobile devices in the Google play and Apple store.

While installing Visual Components, internet access is recommended for product activation and component catalog download.

#### 3.1.2.3 Deployment

Once installation is completed the public electronic catalog (eCat) is automatically downloaded and available to be used. Visual Components has created and maintains an extensive eCat of +2500 virtual components. The eCat contains the most demanded components required to build any factory layout. The models are parametric which allows to easily configure in the virtual space with the real systems characteristics. In addition, in the eCat are available virtual components from the most demanded automation providers.

[16] https://www.visualcomponents.com/legal-information/

[17] https://www.visualcomponents.com/products/downloads/

If the virtual component is not available, the model tab of Visual Components 4.0 allows to import most of the commercial CAD formats. The creation of a virtual component is very intuitive and supported by wizards and pre-defined behaviours that the user can tailor using the Python API.

The creation of a new virtual factory or new production layout in the virtual environment follows a pick & place workflow. Once the virtual components are in the virtual environment, can be interconnected using plug & play and defining their operation parameters, which are pre-defined with the standard design parameters provided by the systems manufacturers. Despite the intuitive process, there is an on-line academy that supports the users[18] from the initial steps towards more specialized tasks. The users are supported by a strong Visual Components community built around the forum[19].

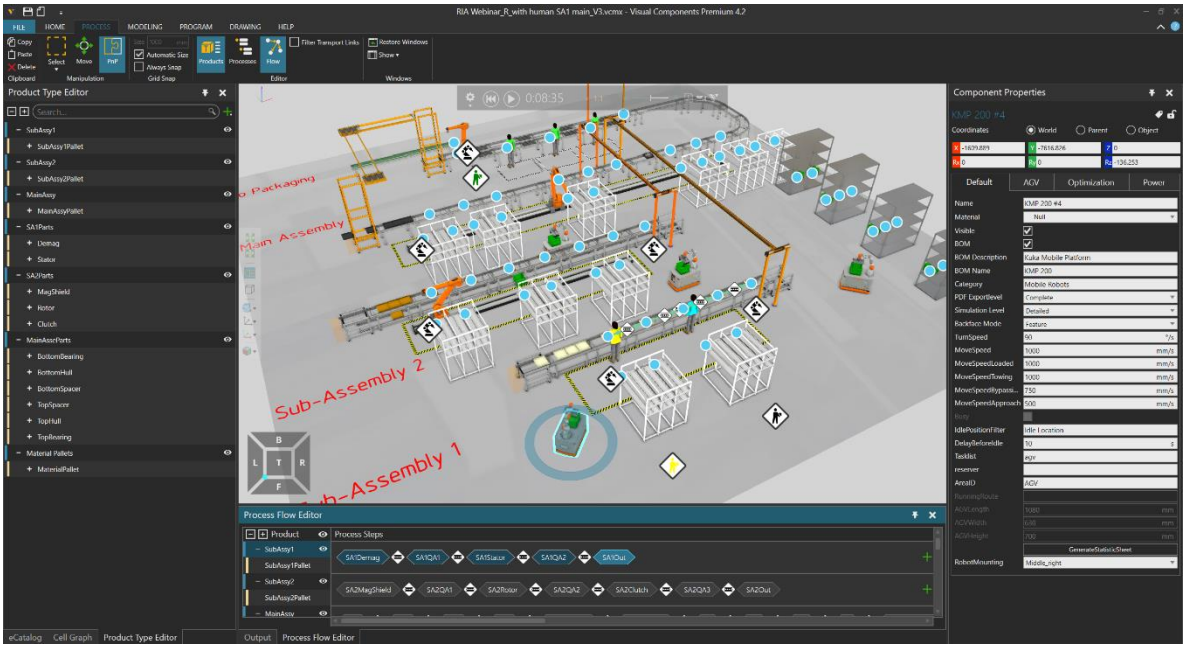


***Figure 3-5 Screenshot of Visual Components 4.3 showing the creation of the virtual factory using virtual components available in the eCat. The processes are created using the process modelling library defining the process tasks between the stations.***

## 3.1.3 M3 Workspace

### 3.1.3.1 Description

M3Workspace is a solution from M3 Platform, the metrological high-performance software developed by Innovalia, that consists on a Platform As A Service (PAAS) cloud-based solution providing metrological after-sales assistance services, it consists mainly on a customer-manufacturer collaborative space for sharing metrology data in a secure way during the manufacturing process, allowing the correct management and monitoring of the quality control process but also to manage all customer needs across their quality control process.

[18] https://academy.visualcomponents.com/
[19] https://forum.visualcomponents.com/

In this way, M3 Workspace was born as a platform through which it was intended to give customer support for a user service desk but also to share M3 license administration and that over time and analysing the customer's needs, other functionalities began to be included such as Software user guides, operative measurement guidelines, trainings and above all the My Workspace service, a collaborative space for the trusted sharing of metrological, product design and manufacturing data.

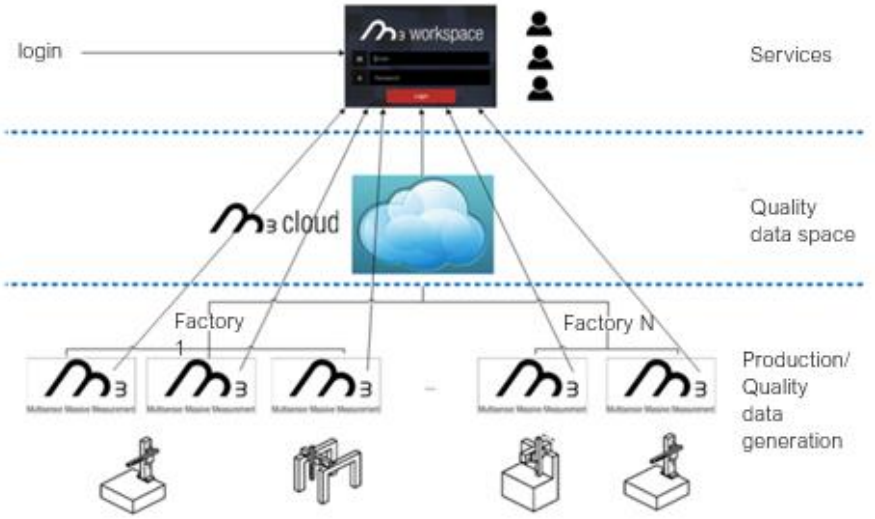


*Figure 3-6M3 Workspace architecture*

### 3.1.3.2 Availability

M3 Workspace is part of the licensed M3 Software. It is one of the set of services offered within M3 Software as a cloud-based service for quality control service assistance.

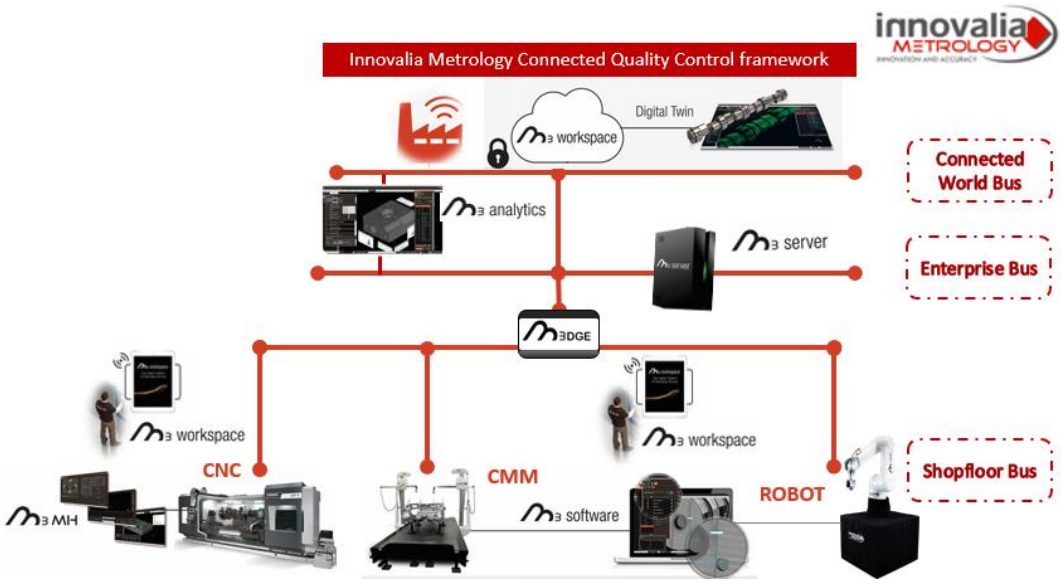


*Figure 3-7 M3 Platform components portfolio for a complete Connected Quality Control Framework.*

More information about the M3 Platform can be found here[20].

#### 3.1.3.3 Functionalities

As it has been described at the beginning, M3 Workspace is a PAAS providing the following services to Innovalia customers (see Figure 3-8 below):

- Licenses → for user/customer M3 license management.
- Support → as a help desk service chat to solve incidences and customers problems while interacting with M3 services.
- Documentation → Space kept for documentation referring to M3 user guides
- My Contacts → Customer contacts within their quality control supply chain
- Messages → Mail service as a communication channel with M3 users regarding software updates, license expiring awareness…
- Training → Space kept for M3 user guidance webinars, specific measurement steps webinars, … almost generated in different languages (English, Spanish, Chinese, Russian, Japanese)
- My Workspace → this is the tool where the work in Eur3ka will be focused. This is the tool for the secure data exchange, in which the information provider can establish the limitations on the use of this data, securely through IDS connectors.


*Figure 3-8 M3 Workspace services*

Through this tool it is allowed to carry out the following activities:

- Upload/download of documents, mainly concerning to products design, measurement projects, measured parts or even metrological and statistical reports, supporting any format with which you work and depending on the type of file (CAD, STEP, XML, CSV, txt…), This process can be both done by the customer and by Innovalia (see Figure 3-9 below).
- Direct upload of measurements results from M3 software interface.

[20] https://m3.innovalia-metrology.com/

- Visualization of files on the proper M3 Workspace interface, either CAD files, point clouds or metrological reports.


*Figure 3-9 File uploading process*

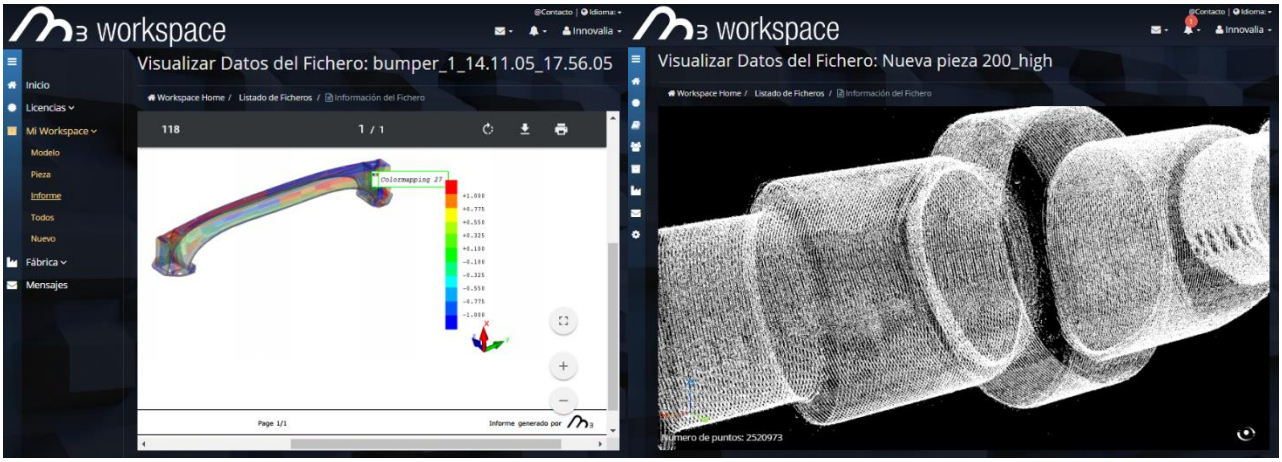


*Figure 3-10 Files visualization in M3 Workspace interface.*

In this manner, with this tool, available data from different heterogeneous products, metrological sources and different locations will be integrated, managed and stored in the M3 Workspace. The secure data exchange will be carried out between the M3 Trusted IDS connector and the customer IDS connector.

## 3.1.4 FAR-EDGE Platform

### 3.1.4.1 Description

The FAR-EDGE Distributed Data Analytics (DDA) platform is consisted from two core components which are the Edge Analytics Engine (EAE) and the Distributed Analytics Engine (DAE). The EAE, as implied by the name, resides within the Edge Gateways of the FAR-EDGE infrastructure and is responsible in processing low level data streams collected from one Edge Gateway. The DAE resides within the Cloud tier and is responsible in processing data coming from the different EAEs. It is capable to provide more complex and consolidated analytics from the whole infrastructure (multiple Edge Gateways).

#### 3.1.4.2 Availability

FAR-EDGE DDA is an Open-Source software and is offered both as source code at GitHub[21] but as well as a containerized solution at DockerHub[22]. The platform deployment scripts can be found here[23].

#### 3.1.4.3 Deployment

**Start Everything.**

Run the following command.

```
docker-compose -f test.yml -p test up -d
```

**Deployment Test.**

Run the following command.

```
docker ps --filter name=test --format "table {{.Image}}\t{{.Names}}"
```

Make sure you see the following deployed containers.

| IMAGE | NAMES |
|---|---|
| faredge/analytics-dashboard:1.0.1 | test_analytics-dashboard_1 |
| faredge/edge-analytics-engine:1.0.3 | test_edge-analytics-engine_1 |
| faredge/open-api-for-analytics:1.0.3 | test_open-api-for-analytics_1 |
| faredge/data-router-and-preprocessor:1.0.3 | test_data-router-and-preprocessor_1 |
| confluentinc/cp-enterprise-kafka:5.0.0 | test_streams_1 |
| aksakalli/mqtt-client:latest | test_message-echoer_1 |
| faredge/mqtt-random-data-publisher:1.0.3 | test_random-data-publisher_1 |
| faredge/model-repository:1.0.3 | test_model-repository_1 |
| mongo:3.6.4 | mongo:3.6.4 |
| confluentinc/cp-zookeeper:5.0.0 | confluentinc/cp-zookeeper:5.0.0 |
| mongo:3.6.4 | mongo:3.6.4 |
| eclipse-mosquitto:latest | eclipse-mosquitto:latest |

*Table 3-1 FAR-EDGE deployed containers*

[21] https://github.com/far-edge
[22] https://hub.docker.com/u/faredge
[23] https://gitlab.com/prophesyEuH2020/data-router-and-processor/-/tree/develop/docker-deployment

**Sample System Configuration Test**

- Go to http://localhost:8000.
- Select **Overview** from the menu on the left.
- Make sure you see the following.
    - There is 1 edge gateway.
    - There are 2 data kinds.
    - There are 2 data interfaces.
    - There are 2 data source definitions.
    - There is 1 analytics processor definition.
    - There are 3 data sources.
    - There is 1 analytics instance.
- Select **Analytics instances** from the menu on the left.
- Make sure the state of the single instance is **Stopped**.
- Press the **|>** button.
- Make sure the state of the single instance has changed to **Running**.
- Select **Data** from the menu on the left.
- Select **Bob temperature in JSON over Kafka** from the **Data source** drop-down.
- Make sure that you see new values coming in every 10 seconds.
- Select **Bob temperature (again) in JSON over Kafka** from the **Data source** drop-down.
- Make sure that you see new values coming in every 10 seconds.

**Stop Everything.**

Run the following command.

```
docker-compose -f test.yml -p test down
```

**Clean Everything.**

Run the following command. (**at your own risk**).

```
docker system prune --volumes
```

Please note that this command erases all the unused system volume so execute it only if you are sure useful system volumes are not going to be deleted.

# 3.2 Connectors

## 3.2.1 Factory Trusted Connector

The Factory Trusted Connector is based on the IDS Trusted Connector. A fully documentation you find on the official documentation site[24]. The core platform is the connector's application layer part for managing containers, message routes, and usage control policies. It is based on the Apache Karaf framework and can be started as a standalone application, within a docker container or as a trust|me a0 container.

### 3.2.1.1 Installing Docker

See chapter 3.1.1 or check the official docker installation documentation[25].

### 3.2.1.2 Starting Trusted Connector

Download the Trusted Connector files as .zip archive, unzip it and start it with docker compose:

```
$wget https://github.com/industrial-data-space/trusted-connector/blob/develop/examples/trusted-connector-examples_develop.zip?raw=true -O examples.zip
$ unzip examples.zip
$ cd example-getting-started
$ docker-compose up
```

The web console of the connector is available at "http://localhost:8181/". The login is "ids:ids".

### 3.2.1.3 Development of Trusted Connector Core

If you want to manually change the trusted connector you can clone/download the project from Github.and build it at your own.

Clone it with git:

```
$git clone https://github.com/industrial-data-space/trusted-connector.git
```

or download the zip archive.

[24] https://industrial-data-space.github.io/trusted-connector-documentation/docs/overview/
[25] https://docs.docker.com/compose/install/

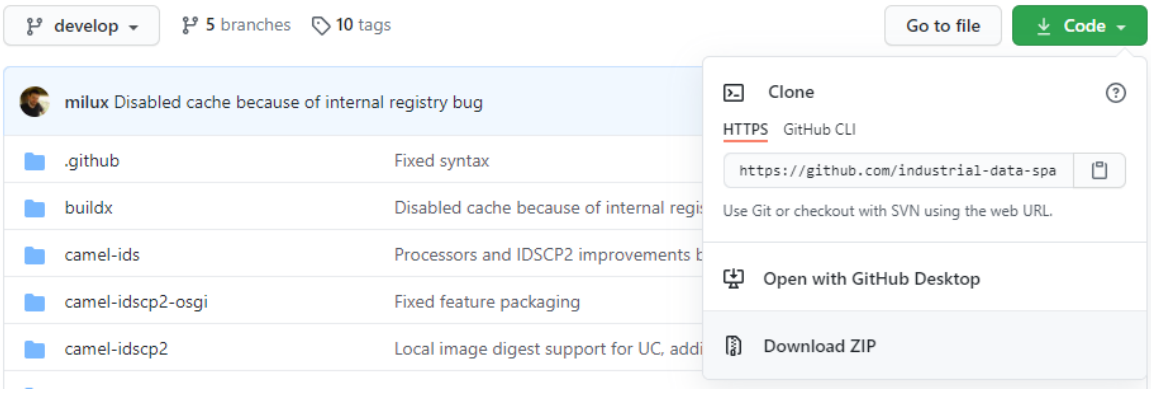


*Figure 3-11 Download .zip archive of git repository*

Now you can do your changes in the code. If you are ready to deploy, change (cd) into the cloned directory, then start the build using the build.sh script.

Make build.sh executable and start the build script:

```
$chmod +x build.sh
$ ./build.sh
```

After a successful build, the core platform can be launched with the following command:

```
$karaf-assembly/build/assembly/bin/karaf clean debug
```

Confirm that the management console is available at “http://localhost:8181/”.

#### 3.2.1.4 Installing Apps within the Factory Connector

The Trusted Connector could integrate individual images and launch them as applications. and ensures a secure communication and usage control within the data exchange. Applications come in the form of Docker containers. Any image from a Docker registry can be pulled into the Trusted Connector and launched as an application. Without further configuration, application containers are initially isolated from each other and restricted in a virtual network with the Core Platform which blocks outbound traffic. That is, even malicious applications cannot interfere with the running system.[26]

[26] https://industrial-data-space.github.io/trusted-connector-documentation/docs/overview/

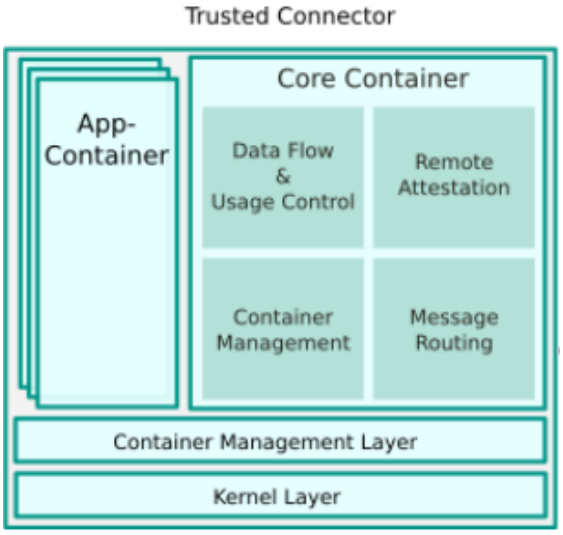


*Figure 3-12 General architecture of the Trusted Connector*

The Smart Matching Mediation App (SMMA) is such an app and will be delivered as a Docker image which then needs to be related to a Trusted Connector instance.

IOSB will provide a download link to the SMMA Docker image in near future. Then the Dockerfile must be adjusted to connect to the Trusted Connector instance. After configuration the Docker container can be started, and the application is running within the Trusted Connector.

## 3.2.2 AMN Trusted+ Connector

### 3.2.2.1 What is Siemens Additive Manufacturing Network (AMN)

Few years ago Siemens launched AMN as a cloud ready solution able to digitalize the order to delivery process over a collaboration platform. Key values of this product is the increased speed to connect suppliers of additive manufacturing capabilities to real world demand and transparency offered to buyers, able now to control feasibility of parts design and receive feedback from manufacturing process.

Whole additive manufacturing process, otherwise asking for intensive collaboration aiming to select fitted supplier, material and alignment between design and execution capabilities, including quotation is now placed in an enterprise grade environment with increased level of security and trust between participants.

As for specific demand of Eur3ka and all COVID-19 challenges, AMN promotes close to real time capability of individual or large volume custom parts buyers to react in an agile manner but keeping transparent view on production. Another added value aspect worth to mention is the offered scalability leaving the buyers and suppliers to focus on what makes sense for their own interests and leave AMN to boost productivity with shorter time to evaluate feasibility of execution and quotation.

#### 3.2.2.2 Technical background of current AMN implementation

AMN has been designed and implemented with the aim to reduce at maximum the volume of development on both buyers and suppliers' side. Same time was observed the need ot have access to various degrees of knowledge regarding design of parts where individual design ownership is still protected. Therefore, here are few questions considered where the platform was designed and built.

- Dependencies to 3rd party software: AMN is fully independent of any outer provider and offer the access to all available stakeholder via a web user interface. All current software solution is self-consistent and end users do not need to consider anything else to use it.
- Availability: Platform is directly available in Amazon Web Services (AWS) cloud. This approach promotes high availability and reducing the dependency of end users of their own on-premises deployment. Also, updates and upgrades and more easily controlled, validated and made available.
- Local, on premises dependencies: AMN do not request any local HW or SW investments or maintenance costs for buyers and suppliers
- Setup effort on user side: This aspect is reduced to a minimum and is focused on use case specific needs, if the standard process needs to be adapted. This includes the connection to Siemens NX platform for sophisticated CAD/CAM/CAE support in a pre-production phase. A specific feature for Eur3ka is considered and explained below.
- Easy to use user documentation is made available on a web-based manner

#### 3.2.2.3 Technical aspects considered for Trusted+ connector

As previously detailed, AMN was designed and implemented with a specific focus on the easiness of user access and operation, therefore no Open API was considered to be offered. For the specific case of Trusted+ connected further analysis and developments are performed and some technical solutions are under evaluation.

As for current state of the work most prominent implementation is related to possibility to use Mendix[27] connectors securely deployed in Trusted Connector containerized environment. This low code platform reduces consistently the time to deliver specific connectivity to ingest semantically specified product descriptions in addition to design files and providing insights on deep customer needs. Taking into account Eur3ka expressed need for quick generation of production ecosystems Mendix will be used via its cloud ready features and in conjunction with the semantically enabled DataHub capable to share and govern knowledge.

Additional features considered are related to custom developments where the heterogeneity of data spaces is relevant, asking for connectors ready for various data sources like IoT devices, databases or widely used AWS S3 data storage.

[27] https://www.mendix.com

### 3.2.3 Makers and FabLabs Trusted Connector

Makers and FabLabs could play a crucial role in response to unpredictable events. Usually, these entities own automated and flexible production equipment based on contemporary technologies, including but not limited to additive manufacturing (3D printing) printers, Computer Numerical Control (CNC) machines, and laser cutters. Thus, in the view of the Eur3ka project, they could significantly extend the manufacturing network providing additional manufacturing capabilities distributed throughout the European area. Given that, Makers and FabLabs should ideally make available the following information within the network:

- Manufacturing capability and tuneable parameters: owned technologies, with a detailed description of the manageable materials, size, achievable levels of accuracy, and eventual support tools such as temperature controllers.
- Quality certification: the provider should assess the truthfulness of the declared ability in the specific technological field;
- Location: this information is essential to organize the delivery and assess the shipment costs and timing based on the clients' and eventually the suppliers' position;
- Machine availability: this feature should be declared and updated based on the incoming orders. The availability could be expressed by illustrating the reservable time slots or including in the offer the expected delivery period calculated by the platform taking into account the logistic system organization;
- Inventory availability: real-time and traceable data on the raw material provision and usage are needed to monitor the consumption rates and manage the supply chain. In the case of modular system whose parts are produced by different manufacturers, it could be also useful to declare the on-site availability of eventual complementary components, especially concerning the entities dedicated to the assembly process;
- Order status: ideally, the clients could benefit from receiving updates on the progress of their personal order, such as the start and the conclusion of the manufacturing process.

Thus, while the first three points are static data, that can be uploaded only once during the registration to the platform, the machine and inventory availability should be updated based on the agreed orders, and eventually modified by the technology provider in the case of necessities external to the platform. Note that, given security issues, it is not advisable to provide direct access to the machine. Thus, the presence of an intermediate agent that manages the production process should be considered. This intermediate acts as a link between the Eur3ka platform and the manufacturing equipment. Based on the competences of the named agent, this person could also serve as an emergency contact in the case of necessity.

In this context, from the perspective of Makers and FabLabs, the main issues associated with the platform connectors are:

- Transparency: the identity of both the suppliers and the clients should be reliable;

- Data privacy and security: this could concern personal and financial data inserted in the platform during the registration process, as well as data produced during the platform exploitation, such as preferences and connection established with other stakeholders. The users should be aware of the accessibility of these data and the eventual exploitation for analysis purposes;
- Traceability: the localization of the raw materials and products, as well as the distance covered and the intended journey should be visible;
- Data ownership: This issue is highly significant if the platform aims to build a cooperative system, where expertise and knowledge can be shared to face critical situation. For instance, it could be useful to provide a common accessible catalogue of previously produced components, conceivably with variable parameters tunable to the client's needs. In this case, the intellectual and data properties should be well defined to avoid possible conflicts;
- Data coherence: standard forms should be defined to exchange design specifications and further useful information to define the order, the payment and the shipment timing. -
- Quality: note that the clients might not be aware of the technical knowledge needed to define the design requirements and to evaluate the manufacturing feasibility. Thus, a preliminary collaborative phase could be beneficial. This collaboration could occur with the producer or with a third part devoted to the feasibility control.

## 3.2.4 M3 Trusted IDS Connector

### 3.2.4.1 Description

The M3 Trusted IDS Connector is an open-source FIWARE-based component based on the IDS Trusted Connector following IDS RA, with the functionality to connect the M3 Workspace cloud services with Innovalia customers cloud services using other IDS connectors.

As it has been previously described, the M3 IDS Connector is the essential component through which metrological and manufacturing data exchange between Innovalia and their customers can be carried out complying with the IDS RA. This connector contains a series of services/apps that allows this connection between the M3 Workspace platform services and the customer IDS Connector following as indicated in the figure below.

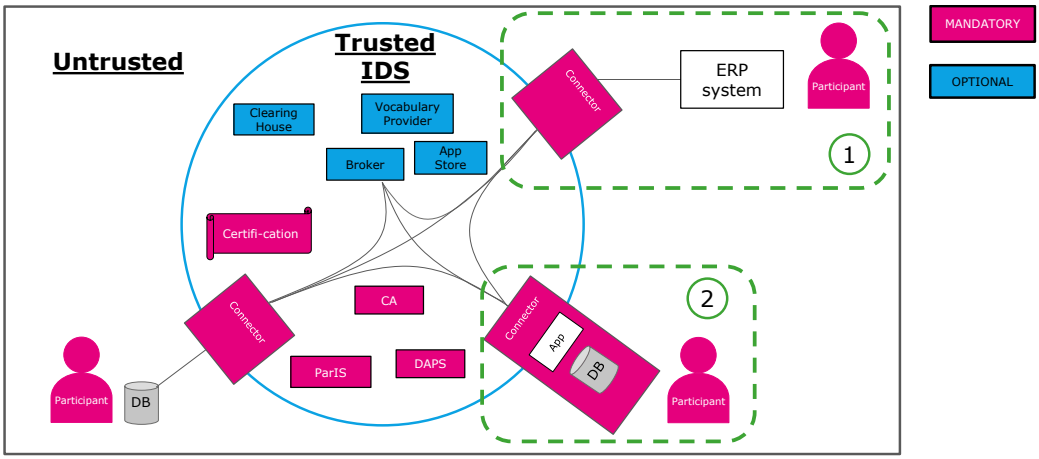


*Figure 3-13Schema for the IDS connector connection between BD Analytics Apps/Platforms*

### 3.2.4.2 Main features

One of the main characteristics of the M3 Trusted IDS connector is that it is FIWARE enabled, this means that it is composed by a system adapter, from the QIF standard, as the data model applied among the whole metrological framework, to the NGSI standard, in order to easily connect to the Orion Context Broker, the Broker entity that will handle the management of all communication between Innovalia and their customers. This system adapter is deployed and configured in the M3 Trusted IDS Connector.

This system adapter allows that the GD&T results can be accessed and offered to data apps, using QIF standard in order to leverage metrology information interoperability using industry consensus standards to communicate data between component producers and consumers of manufacturing quality systems. For this reason, INNOVALIA is integrating and developing QIF schema as the data model of the GD&T results (an XML data file).

This is an example of part of the GD&T information model Innovalia obtains on every measurement:

```
<MeasurementResults>
    + <FileUnits>
    + <InspectionTraceability>
      <DatumDefinitions> </DatumDefinitions>
      <DatumReferenceFrames> </DatumReferenceFrames>
    + <MeasurementResources>
    + <ProductGeometriesDefinitions>
    + <Products>
    - <Features>
        + <FeatureDefinitions>
        + <FeatureNominals>
        + <FeatureActuals>
        + <FeatureInstances>
      </Features>
    + <Characteristics>
    + <InspectionStatus>
</MeasurementResults>
```

*Table 3-2 Example of part of the GD&T information model*

This is just considering the measurement results, but it also contains modules for units transformation, measurements and machine traceability, geometries definition, part register.

This QIF data model makes it easier to adapt this information into NGSI standard considering the NGSI Context Management Information Model based on the definition of entities, attributes, domains and context elements with a similar data structure as QIF does.

This is an example of GD&T NGSI formatted publications made available through the M3 Trusted IDS Connector:

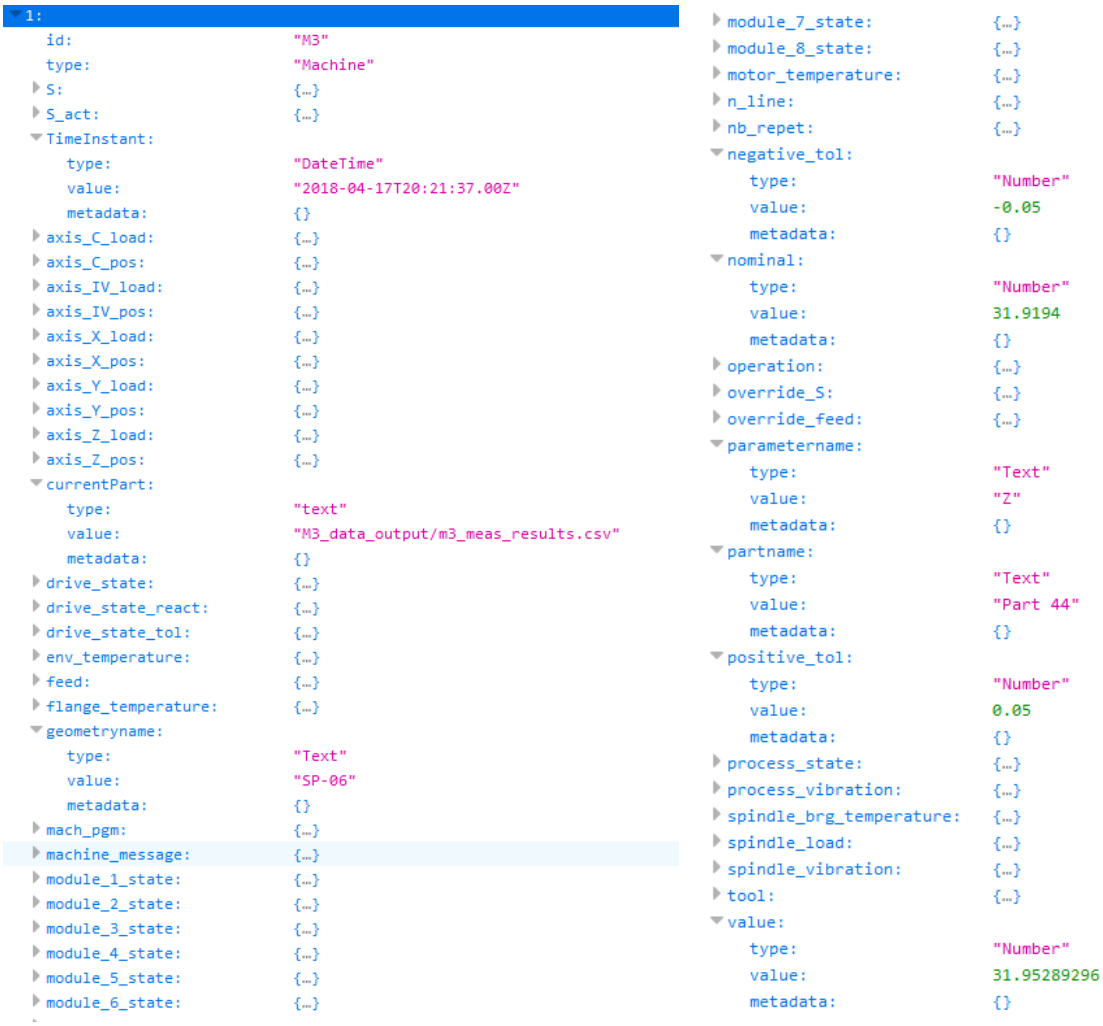


*Figure 3-14 NGSI formatted publications made available through the M3 Trusted IDS Connector*

### 3.2.4.3 Development of FIWARE-based IDS Trusted Connector

These are the steps followed in order to implement this FIWARE-based IDS Connector:

1. Dockerized tools relying on Docker Hub Services enabling automated deployment and configuration of Data Apps.
2. Analyze the proper data model NGSI compliant to be adopted to adapt from QIF standard.

3. Data Apps mapping to NGSI system adapters processing context information.
4. Consider that also the External (Customer) IDS Connector implements and uses FIWARE Context Broker components.

### 3.2.5 TRUE Connector

The TRUE (TRUsted Engineering) Connector[28] is an open-source component defined, implemented and maintained by Engineering. It is aligned to the IDS base security profile and it represents a multi-protocol connector aiming to exchange data with several representations (IDS-like) through different communication protocols.

The architectural overview is depicted in Figure 3-15 considering a couple of connectors describing the roles of consumer and provider.

The TRUE Connector is composed of three components:

- **Execution Core Container (ECC)**, an open-source project designed by ENG. It is in charge of the data exchange through the IDS ecosystem representing data using the IDS Information Model and interacting with an external Identity Provider. It is also able to communicate with an IDS Broker for registering and querying information.
- **Data Application (Data APP)**, an open-source project designed by ENG. It represents a trivial data application for generating and consuming data on top of the ECC component.
- **Usage-Control Application (UC APP)**, a customized version of the Fraunhofer IESE base application for integrating the MyData Framework (a Usage Control Framework designed and implemented by Fraunhofer IESE) in a connector.

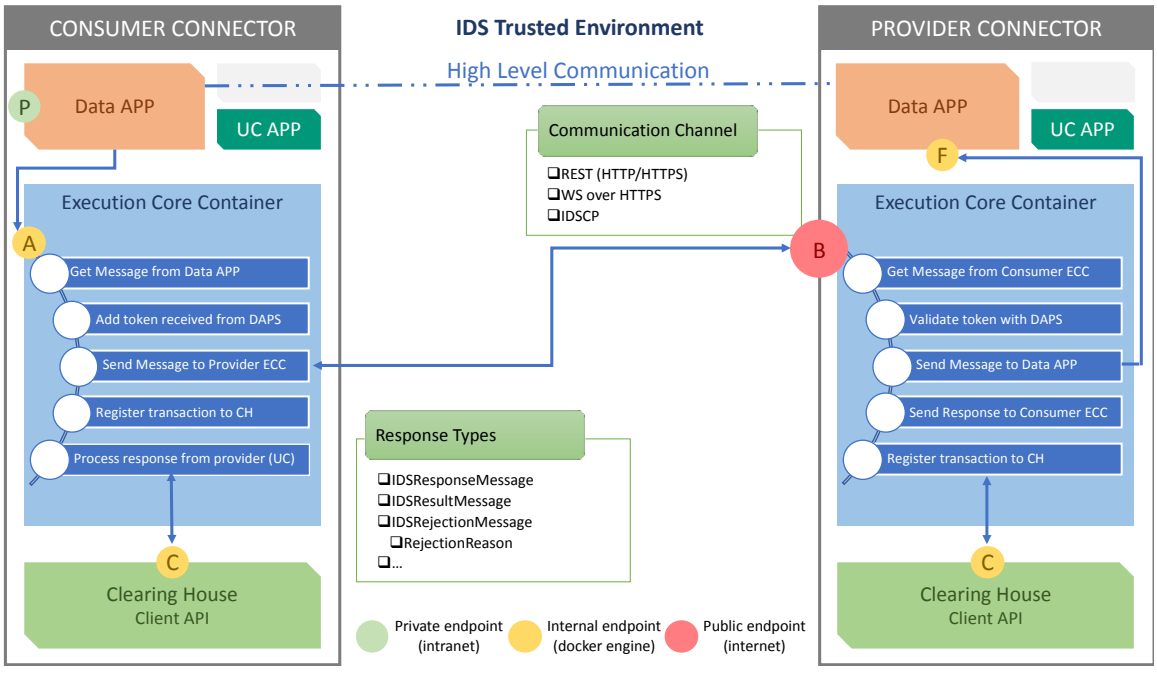


*Figure 3-15 TRUE Connector Architecture*

[28] https://github.com/Engineering-Research-and-Development/true-connector

The TRUE Connector supports the following data formats for data exchange between connectors and also internally (between Execution Core Container and Data APP):

- **Multipart/mixed**, composed of a mix of different data types. Each body part is delineated by a boundary. Typically, the message is represented by the header part (IDS Message) and a free-format body (payload of the message).
- **Multipart/form**, each value is sent as a block of data ("body part"), with a user agent-defined delimiter ("boundary") separating each part. The message is composed of a header and a payload.
- **HTTP-header**, the header part of the message (IDS Message) is described using HTTP headers, the body contains the payload of the message.

The data formats described above are totally configurable using dedicated properties for describing the way data will be exchanged between connectors and inside the connectors themselves.

Furthermore, the connector can be configured to activate several kinds of communication protocols starting from the user needs:

- **HTTP/HTTPS**, activating the proper endpoint type (B in Figure 3-15) for accepting HTTP/HTTPS communications and implementing the related client side (for sending data).
- **Web Socket over HTTPS**, implementing the web socket technology for exchanging information, useful for large data communication.
- **IDSCPv1**, partially integrated for communicating with existing trusted connectors, implementing advanced security features.

The proper communication protocol can be configured before deploying the connector, aiming to satisfy business requirements that can be related to user (i.e., large file exchange) or technical needs (i.e., integration with existing connectors).

The TRUE Connector implements the Access Control integrating the state-of-the-art IDS Identity Provider services, in particular the Fraunhofer AISEC v1, v2, and Orbiter even they are not aligned regarding the certificate types for identifying users.

The Usage Control has implemented thanks to the integration of the Fraunhofer MyData Framework. The Usage Control APP was customized and improved in order to support several kinds of usage control rules[29] (location-based, purposed-based, temporal-based, modifiers, etc.).

Moreover, the connector is able to register itself and to interact with an IDS Broker, in particular, it was tested during the IDS Integration Camps[30] with the Fraunhofer EIS Metadata Broker.

Finally, the connector is able to register transactions to the ENG Clearing House, a distributed Clearing House service, for logging exchanged messages.

[29] https://github.com/Engineering-Research-and-Development/true-connector/blob/main/doc/USAGE_CONTROL_RULES.md
[30] https://www.sqs.es/q-idsa-itc/?lang=en

# 4 Conclusions and Future Outlook

The Eur3ka approach to provide a pool of services for manufacturing response during event that disrupt production operations is based on the integration of existing digital manufacturing platforms and components around a data space. This approach is in-line with the project's strategy to use the partners' background IP (Intellectual Property) towards accelerating the project's developments. Furthermore, it is in-line with state-of-the-art data sharing best practices and supply chain management systems i.e., the practices of International Data Spaces. This deliverable has introduced this approach along with the infrastructures and tools that will be used to support it.

A significant part of the deliverable is devoted to presenting the platform to be integrated, along with their alignment to the selected infrastructures and tools. The project leverages modern approaches to digital components packaging, deployment and distribution, such as Docker images. Most of the existing platforms are compatible to the project's approach, while some of them are already available as Docker containers. Thus, the deliverable is accompanied by an early prototype deployment of the platforms as well.

The deliverable has also illustrated various connectors that will be used to integrate individual platforms and components to the data space. Initial technical specifications for these connectors are provided, yet a detailed specification of their data semantics is on-going as part of work in other Eur3ka work packages. Note also that the Eur3ka service deployment architecture will be compliant to the Eur3ka reference architecture, which is specified in WP2 of the project. Therefore, there are still several missing pieces in the Eur3ka deployment architecture, which is the reason why the present deliverable is providing guidelines and information about the early deployment of the Eur3ka services.

The next steps to the development of these deliverable include:

- More detailed specification of the platforms and the connectors that will enable the integration of the Eur3ka platform.
- Alignment of the deployment architecture to outcomes of other work packages, notably the reference architecture of WP2 and semantic data models of the project.
- Packaging and distribution of the platforms in-line with the containerization approach of the project.
- Implementation of the specified connectors to the International Data Space.

The developments entailed in these steps will be reflected in the next version of this deliverable i.e., D4.2 according to the Eur3ka deployment architecture.


*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101016175*