QU4LITY

DIGITAL MANUFACTURING PLATFORMS FOR

D3.8 Fog Nodes and Edge Gateways for ZDM deployments (Final Version)

Deliverable Id :	**QU4LITY-D3.8**
Deliverable Name :	**Fog Nodes and Edge Gateways for ZDM deployments (Final Version)**
Status :	**Final**
Dissemination Level :	**PU**
Due date of deliverable :	**30/06/2021**
Actual submission date :	**30/06/2021**
Work Package :	**WP3**
Organization name of lead contractor for this deliverable :	**TTT**
Author(s):	**Martijn Rooker (TTT), Elena Urkia (IDEKO), Márcio Mateus (UNP), Irune Mato (INNO)**
Partner(s) contributing:	**IDEKO, UNP, SQS**

Abstract: This deliverable presents the edge solutions and validation framework enablers of the QU4LITY project. It describes the implementation and extensions of the enablers and their deployment within their respective pilots and additionally, how edge solutions can be of benefit to manufacturers for ZDM problems.

Contents

HISTORY

Version	Date	Modification reason	Modified by
0.1	10/02/2021	Initial Table of Contents shared with WP leader and contributors	TTT
0.2	31/03/2021	Initial description of digital enabler	TTT
0.3	15/04/2021	Draft version of Section 1	TTT
0.4	19/04/2021	Description of digital enabler	IDEKO
0.5	07/05/2021	Draft version of Section 2	TTT
0.6	25/05/2021	Description of digital enabler	UNP
0.7	26/05/2021	Description of digital enabler	SQS
0.8	27/05/2021	Introduction and conclusions	TTT
0.9	02/06/2021	Final inputs	TTT, SQS, UNP, IDEKO
0.10	07/06/2021	Ready for review	TTT, SQS, UNP, IDEKO
0.11	18/06/2021	Updates based on review from CEA	TTT, SQS, UNP, IDEKO
1.0	30/06/2021	Finalization and submission	TTT

Executive Summary

The deliverable D3.8 "Fog Nodes and Edge Gateways for ZDM deployment (Final Version)" reports on the overall work performed in and the final results of Task 3.4 (Fog/Edge Computing Technologies Adaptation and Cyber-Physical Systems Integration). The main focus of Task 3.4 has been on the development of edge devices targeting the deployment and hosting of ZDM applications at the edge of the network, direct at the machines and thus close the data sources, thereby significantly reducing latency in data processing and potentially machine actuation.

The task comprises in the first part of three partners (TTT in cooperation with TIAG, IDEKO and UNP) that have been working on the (further) individual development of their respective edge solutions for manufacturing solutions and enabling the hosting and deployment of ZDM applications. The solutions will be integrated in either pilot lines or experimental facilities. The edge devices have not all been completely developed completely from scratch, but the involved partners already had a basis which has been extended within the QU4LITY project to fulfil the requirements from the different pilots inside the project. Only partners UNP started the development of their edge device from scratch. Additionally, SQS has been involved in Task 3.4, focusing on the development of a ZDM V&V Framework that is capable of certifying Autonomous Quality (AQ) solutions. This framework will enable end users to certify the solutions, including edge devices and AI solutions and bring them into their manufacturing solutions.

The deliverable provides an overview of the requirements for the development and the deployment of edge devices in industrial environments. These requirements are coming from the requirements phase inside the project and additionally from interaction with the targeted pilots and the developments partners involved in the respective pilots.

Following on this, it describes developments of the three edge devices that have been performed inside this task. Partners TTT (in cooperation with TIAG), DANOBAT and UNP have focused their work in this task on extending their existing or newly developed edge devices for ZDM deployment and the deployment of the devices in their respective pilots and/or experimental facilities. It will highlight specific developments focusing on the improving the hosting, deployment and access to data needed to establish ZDM.

The final part of the deliverable focuses on the ZDM V&V framework developed by partner SQS, where a certification framework will enable that will use a modular approach. This framework will certify ZDM components for specific usage scenarios and specific adaptation to deploy the validated or certified solutions at the factory shopfloor.

In the rest of the project, the results of Task 3.4 will be integrated in the respective pilots and experimental facilities and minor modifications can still take place to fine-tune the actual deployment and hosting of ZDM applications. Furthermore, the solutions will be validated in these pilots and experimental facilities (cf. WP6 and

WP7) and will be evaluated for potential offering in the marketplace established in WP8.

1. Introduction

1.1 Scope and Purpose of the Deliverable

One of the main important factors of realizing Zero Defect Manufacturing (ZDM) is to have the data quickly available, potentially directly at the source, which means the manufacturing line of machines. The QU4LITY project proposes data-driven, digitally enabled mechanisms for ZDM. To make data directly available at the machines (or so-called edge of the network), the QU4LITY project provides different fog and edge solutions, enabling the hosting of applications at the edge for faster handling of data to enable ZDM.

It needs to be reported here that edge systems provide an infrastructure enabling ZDM. The edge solutions are not explicit solutions that will analyse or handle data but can host applications that can perform these tasks directly at the edge of the network, thereby avoiding the expensive transfer of data into the cloud.

The aim of this deliverable is to present the final versions of the edge solutions that were under development within the QU4LITY project, including their deployment in an industrial pilot or an experimental facility. The classification of the deliverable has been changed from DEM to OTHER, as the main result of the task, as mentioned before, are edge infrastructures that can be deployed in factories and these infrastructures will host applications that can provide ZDM functionalities to the production lines. The demonstration of infrastructure solutions is not as straightforward and easy as demonstrating ZDM applications. Therefore, this deliverable will mainly focus on the developments of the infrastructures and how it can support the companies in integrating ZDM functionalities closer to the machine, thus at the edge of the network.

Next to the development of the edge devices, Task 3.4 also focused on a ZDM V&V framework that aims to certify Autonomous Quality solutions taking into account the regulations established by the European Commission for environments with AI.

Each of the enablers developed within Task 3.4 and mentioned in this deliverable will be described according to the following perspectives:

- **Business perspective:** This perspective describes what the benefits are for manufacturing companies introducing the edge solution to their manufacturing process. Edge solutions don't immediately provide a technology for establishing ZDM but provide an infrastructure that enable the hosting of such technologies. This perspective will describe how companies can benefit from deploying edge solutions into their production facilities and how they can support them into establishing ZDM.

- **Technology perspective:** The technology perspective provides a description of the technical developments that have been performed on the edge solutions available in the project. As in two of the three edge solutions were already in a certain development stage before the start of the project, the technology perspective will mainly highlight the developments that have taken place in the course of the project and describe how they can add to the concept of ZDM, for example through remote access to the system, improved performance (real-time virtual PLCs), better data access, etc.

- **Demonstrator perspective:** Within this perspective it is highlighted how the available edge solutions are integrated in the designated pilots. It will provide a highlight on how the edge infrastructures are included in the already existing pilot infrastructures (e.g., the network infrastructure). Additionally, it will be described which dedicated ZDM applications will be hosted on the edge. A detailed description of the overall pilot will be provided in the designated deliverables for these pilots (i.e., D7.X), so the aim of this deliverable is not to present the overall pilot. The aim of this deliverable is to present the functionality and applicability of the edge solutions, thus that will be the focus of the description in this section.

1.2 Methodology

The methodology applied for the developments in Task 3.4 varies a bit from the other tasks where digital enablers are being developed. First of all, there are two different types of digital enablers developed within this task, namely three different edge solutions and an ZDM validation framework. The developments coming out of this task are not direct solutions that enable ZDM, but are infrastructures that support the deployment of ZDM solutions to the edge of the network, very close to the location where the data is being generated, which is of crucial importance to the concept of ZDM. In the first deliverable D3.5, the existing edge solutions were presented, and which concepts would be further developed to make them available for the pilots to deploy ZDM applications. The pilots where the edge solutions will be deployed provided requirements and specifications in the first phase of the task. Additionally, the QU4LITY-RA provided requirements on how edge solutions can be deployed in manufacturing plants and how they can add to ZDM.

As some of the edge solutions were already available at the beginning of the task, an early deployment was possible. This provided the pilot partners to work in an earlier stage with the edge devices and provided feedback and input to the new developments. Based on the feedback from the pilot partners, modifications and fine tuning of the developments and the deployments in the pilot lines were made possible.

At the end of the Task, the final implementations for the edge devices and their internal software have been made available to the pilot and will be used in the pilot implementations tasks (Task 7.x). The edge solution providers will closely interact with the pilot partners performing the final integration and validation of the technologies.

1.3 Relation Deliverable D3.7 (Version 1)

This deliverable is a continuation of the work described in the predecessor deliverable D3.7. The deliverable D3.7 provided an overview of some of the more accepted frameworks that are currently available for fog and/or edge computing. Additionally, it introduced the edge solutions that will be targeted inside the QU4LITY projects and that will be further developed inside this task. Additionally, it will focus on the added value of having edge solutions in the pilots and what the economic benefit is of these solutions.

This deliverable presents the implementation, integration and demonstration of the enablers that were introduced in deliverable D3.7. Compared to the previous deliverable, here the developments that have taken place during the duration of the task will be highlighted.

1.4 Relation to Other Deliverables

This deliverable is closely related to various other deliverables inside the project:

- **D2.1/D2.2 Analysis of User Stories and Stakeholders' Requirements (Version 1 & Final Version).** The requirements and user stories provided by these deliverables have formed the basis for the work of the enablers described in this deliverable.
- **D2.11/D2.12 Reference Architecture and Blueprints (Version 1 & Final Version).** The QU4LITY-RA provides a detailed description on how the digital enablers can be deployed within pilots and factories. There was a close interaction with these deliverables in a two-sided way. Task 3.4 was providing input to these deliverables with technical input to the architecture, whereas the architectures were describing how to possibly deploy edge devices and host ZDM enables on the devices.
- **Deliverables from WP3.** The deliverables coming out of the task of WP3 describe different digital enablers. A big part of these digital enablers can be deployed to and hosted on the edge technologies developed in Task 3.4.
- **D7.1/D7.2 Detailed Pilot Specification and Report on Pilot Sites Preparation (Version 1 & Final Version)**. These deliverables describe the various pilot site being exploited inside the QU4LITY project. A selection of these pilots will be equipped with the solutions described in this deliverable.

There are other related deliverables as well, but the above-listed ones are the most closely linked to D3.8.

1.5 Deliverable Structure

This deliverable is structured as follows:

- Section 2 describes the requirements that were identified for the development of the digital enablers within Task 3.4. As mentioned before, the technologies coming from this task are not directly enabling ZDM but provide the restructurers to deploy ZDM solutions. Therefore, these requirements are focused on providing optimal edge solutions support ZDM.

- Section 3 presents the three different fog and edge solutions that have been designed and further developed within the QU4LITY project. The descriptions of these solutions are separated in three different sections focusing on business perspective, technology description and deployment. Additionally, it will provide some links where more information can be found regarding literature, tutorials, and additional solution information.
- Section 4 describes the ZDM Validation Framework defined by SQS. This service is based on Q-Digital Automation, a framework that advocates for the validation of the Autonomous Qu4lity Solutions.
- Section 5 is the final section and concludes the deliverable. It summarizes the enablers developed within Task 3.4 of the QU4LITY project and the usage of the enablers within the project. It further summarizes the applicability of the enablers beyond the project.

2. Driving Requirements and Reference Use Cases

2.1 Driving Requirements for Development and Deployment of Edge Computing Solutions

As mentioned before, the edge technologies developed in this task are not specific digital enablers for ZDM. The solutions are infrastructures that are developed to deploy ZDM technologies close to the machines, at the edge of the network. The advantage of having the ZDM technologies at the edge is that a more direct access to data can be guaranteed, without any delay of data transfer into the cloud. Additionally, applications that are interacting with the machines (e.g., perform control operations) can even do this in (semi) real-time as there is hardly any delay in sending data back to the machine. Therefore, to deploy and optimally use edge computing solutions in machines or manufacturing lines, different requirements have been identified based and the developed edge solutions should address them:

- **Northbound Connectivity:** Edge computing is often closely connected to cloud computing. With edge computing there is quite often a trade-off between what needs to be computed on the edge (i.e., in real-time) and what can be computed in the cloud (i.e., non-real time). Therefore, edge solutions must have a northbound connection, either up to the cloud, to on premise computing centres or to other edge devices. Additionally, this northbound connection can also be exploited to have good remote access to the nodes, to exchange data between different nodes via a cloud solution. A solid northbound connection is therefore of importance to a good edge solution.
- **Southbound Connectivity:** Similar to northbound connectivity, an edge solution needs to have multiple southbound connections. The southbound connectivity is mostly used for collecting data from sensors and sending data to actuators. Especially in the domain of ZDM, it is important that enough data is being collected (potentially in real-time). Additionally, sensors are not all connected using the same interface, so ideally the edge solutions would also support multiple (open) interfaces so that as much data as possible can be collected.
- **Application Hosting:** Collecting data is not enough. It is important that there are applications available at the edge, so that the data can be interpreted, modified and be used to improve the manufacturing process to establish ZDM. Hosting of applications on edge devices can be accomplished using different approaches, like virtualization (enabling support of legacy applications), containerization, etc.
- **(Real-Time) Data Handling:** The applications hosted on the edge devices must have direct access to the data coming from the sensors if they want to be effective on the edge. Multiple interfaces to different sensors have to be made available to access the data sources. Additionally, the result of the analysis sometimes has to be fed back into the machine, e.g., by updating parameters of a manufacturing process to improve it. This interaction between

the edge and the machine have to be performed in real time, so the downtime of the machines is as small as possible.

- **Remote access and Configurability:** In most situations, edge devices are either connected to the internal network and quite often also to the Internet, providing the possibility to remotely access them. Remote access to edge devices to monitor connected machines, perform maintenance and updates and deploy applications significantly improves the usability of such devices and reduces the costs associated with
- **Machine Learning Support:** As Machine Learning (ML) is becoming more and more important for the field of ZDM, edge devices must have the possibility to support ML on the edge of the network, instead of having all the ML applications in the cloud. Providing this possibility at the edge, will significantly reduce the latency of the data transfer. A selection of the digital enablers developed within QU4LITY use ML techniques and will be deployed at the edge.

These identified requirements were the driving force behind the developments performed for the edge and fog devices inside QU4LITY. The partners developing the platforms have taken these requirements as the basis for the implementations and tried to implement these requirements as well as possible. As in some of the edge devices, an already existing platform was already available at the start of the project,

2.2 Driving Requirements for Validation

This part of task T3.4 focuses on the development of a ZDM V&V Framework that is capable of certifying Autonomous Quality solutions. To find out the necessary requirements to validate solutions of this type, an analysis has been made of the new regulation of the European Commission for systems that make use of artificial intelligence. One of the main goals of the new framework called "Regulation on a European approach for artificial intelligence" is to guarantee people's trust in systems that use AI, on that account the EC (European Commission) embraced a total product lifecycle (TPLC) approach; AI technologies will be subject to inspection before they are placed in the market and throughout their lifecycle, putting special attention to the risks assessment and transparency. The EC has classified AI environments according to the intended use, in the case of 'high-risk' must be preventively evaluated with the aim to ensure that the system comply with all the requirements, before being released to the market.

More information will be given in section 4 called QU4LITY Validation Strategy.

3. QU4LITY Fog Nodes and Edge Gateways

3.1 Overview of Fog Nodes and Edge Gateways

Within the QU4LITY project, many digital enablers are being developed and deployed in pilot lines or experimental facilities. These digital enablers vary from reliable communication solution, cloud infrastructures, AI and big data analytics, cybersecurity solutions, etc. One of the problems, manufacturing companies still see nowadays is the access to the actual data coming from the machine. As depicted in the QUALITY Reference Architecture, the edge solutions coming from Task 3.4 will be deployed to host various digital enablers (developed in the other tasks in WP3) at the edge of the network, thus having direct access to the data coming from the machines.

The following table provides an overview of the three edge solutions that have been developed/provided within the project and that will be deployed in either a pilot or an experimental facility. The following section will describe the developments on the edge solutions and how they are deployed within the designated pilots or experimental facilities to reach the goals of the QU4LITY project.

Platform	Description	IP Owner
Nerve Blue	A radically open edge computing platform that promotes vendor independence and flexibility, allowing users to deploy their own software, or applications developed by third parties.	TIAG
Danobat Box	The Danobat Box is the solution used by Danobat for the monitoring and provision of associated services related to their machines. It is a robust solution that enables heterogeneous data acquisition and provides a safe channel to send this information to the cloud.	IDEKO
FOOTPRINT	The Fog Node that supports data acquisition from an arbitrary number of sensors and use the available data to create a set of profiles for each pair of machine/part to monitor the production quality and automatic detect and identify problems or defects during manufacturing.	UNP

Table 1: Overview of QU4LITY Fog Nodes and Edge Gateways

3.2 Nerve Blue

3.2.1 Digital Enabler Overview

Nerve Blue is a versatile software that enables machine builders to deliver data and offer services to their customers from machines installed anywhere in the world. For plant owners, Nerve Blue can be used to optimize the processes running in the plant, enabling faster access to data, as data can be used directly at the edge of the network and no latency is created by sending all the data to the cloud.

Nerve Blue allows users to collect, store and analyse machine data direct on the edge of the network. It offers the possibility to host multiple applications on a single device and remotely manage the software deployed on multiple devices.

Nerve provides connectivity to multiple PLCs or remote I/O modules using Ethernet fieldbuses, such as PROFINET and EtherCAT. The data that is collected from the I/O modules is modelled in OPC UA, which allows information to be shared in a standardized way.

3.2.2 The Business and ZDM perspective

The Nerve Blue solution has a high business value for each manufacturing process and machine builder. Edge solutions are not explicitly designed only for the ZDM domain but have a huge added value for each manufacturing process.

- **Reduced Hardware Costs:** By using virtualization, multiple Operating Systems (OSs) can be supported on a single device, thus combining multiple IPC functions on a single IPC.
- **Reduced Developments Costs:** The use of virtualization allows users to deploy their Operating System of their choice. This also allows to deploy legacy software solutions, thus no chance in software is required, thereby drastically reducing the developments costs for deploying their existing technology onto the new solution.
- **Reduced Service Costs:** Nerve Blue remote access features enable system developers to access the solutions and the deployed applications from their own offices. System developers don't have to perform expensive site visits to access the applications and can perform maintenance tasks and update quickly.
- **Speed up time to market:** Nerve Blue offers a complete solution which can be directly integrated into a pilot system. The possibility to integrate legacy systems into the machines significantly speeds up the time to market as no modifications to the applications are needed to have them running on the devices.

As mentioned before, edge solutions are not explicitly designed for ZDM, but are an infrastructure that have a large added value for ZDM. Hosting ZDM applications directly on the edge of the network and on the machine, reduces latency of data transfer and faster access to the machines can significantly improve the performance of the machines and add to the concept of ZDM.

3.2.3 The Technological Perspective

The objective of the Nerve Blue solution is to optimize edge connectivity, edge application management and data usage in machines and production lines. Bringing the data and applications to the edge of the network, thus closer to the machine, enables the machine to react faster to changes in the data, reduce latency of data transfer and thus overall improve the manufacturing process. Therefore, edge computing can be seen as a major cornerstone of realizing ZDM in manufacturing.

Updated Architecture

For the new developments of the Nerve solution, a new architecture has been defined to optimize the performance of the system. The architecture is depicted in Figure 1 and in detail in Figure 4.

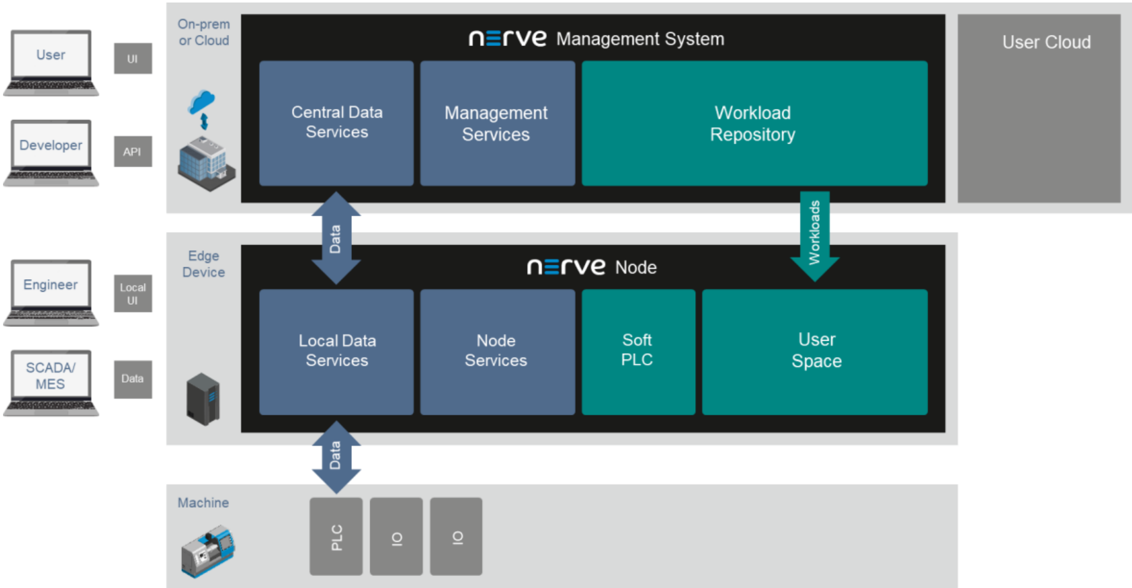


Figure 1: Nerve System Architecture

The Nerve System consists of two parts, where one part is located at the edge device and the other part runs in the cloud, which could be any specific cloud solution. The edge device will host different services, which are:

Data Services

Data services are a collection of services and interfaces that enable the system to collect, store, analyse, visualize and distribute data. These services are available on the individual edge devices, as well as in the management system in the cloud or on premises. Using these services, data can be collected in fast real-time cycles on the edge devices and be stored or visualized locally at the device or also centrally in the management system. The data services are divided into two solutions, namely Local Data Services (on the node) and Central Data Services (in the Cloud or on premise), which is also depicted in Figure 1. This can be interpreted as a distributed system, where the edge offers the input path including evaluation and possible data uses and the cloud offers output paths.

Local data services are located and directly accessible on the edge node. These data services use the local data gateway, local data storage and local data visualization, which are all present at the node. Compared to this, the central data services have a central data gateway, central data story and central data visualization. This concept is depicted in a high-level graphical overview in Figure 2. The local data services on each individual node can be exploited by accessing the node directly and using access the data to the devices and sensors the node is connected to. The central data services have access to the data stored in the management system (e.g., the cloud or on premises). The local data services also enable the processes hosted on the node to access the data directly on the node and perform (near real-time) processing and control of the machines, thus providing the possibility to react faster to changes required in the production process.

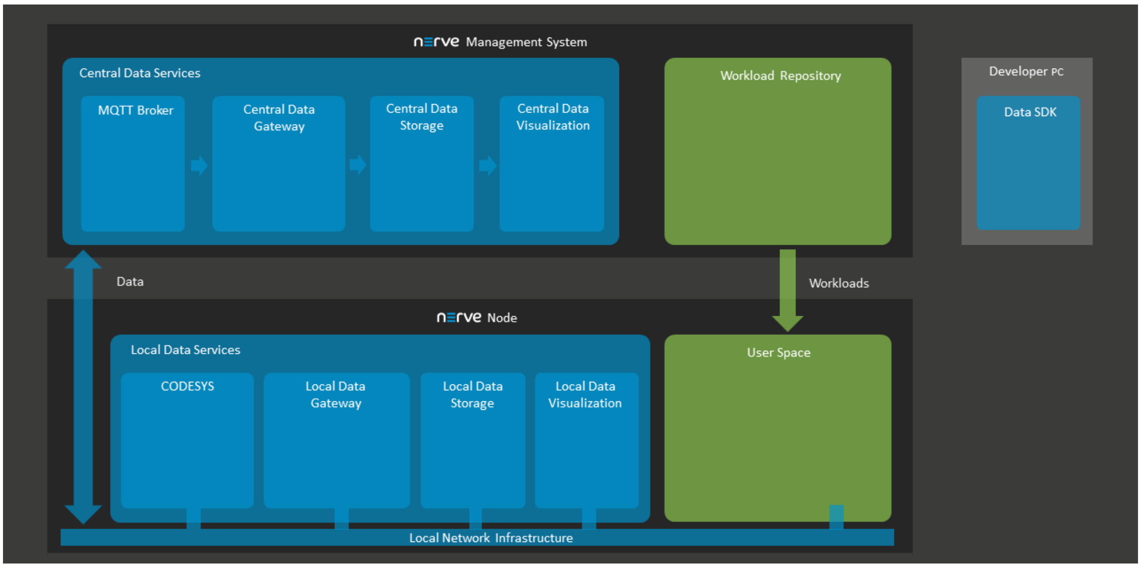


Figure 2: Local and central data services

The data services in the Nerve system support data ingestion from different, well-accepted industrial protocols, so that it can be easily integrated into legacy systems. The following input/output protocols are currently being supported (see Table 2).

Table 2: Nerve supported protocols

Inputs	Outputs
MQTT subscriber	MQTT publisher
OPC UA PubSub over MQTT	OPC UA PubSub over MQTT
OPC UA PubSub over UDP	OPC UA PubSub over UDP
OPC UA Client	OPC UA Server
Modbus Server	ZeroMQ publisher
S7 server	TimeScale DB
	Influx DB

Node Services

The nodes offer additional services, called node services. The node services are running locally on the node and enable the user to access and control the node. This is made possible by a local User Interface (UI) on the node. The node offers the following services directly on the node: network configuration, node registration and password management, workload management, local workload deployment, local workload repository and management of remote connections (see below).

The local UI provide the user an overview of the node and can show different functionalities, like how long the node has been online, how much space is still available on the node, RAM usage, etc. (see Figure 3).

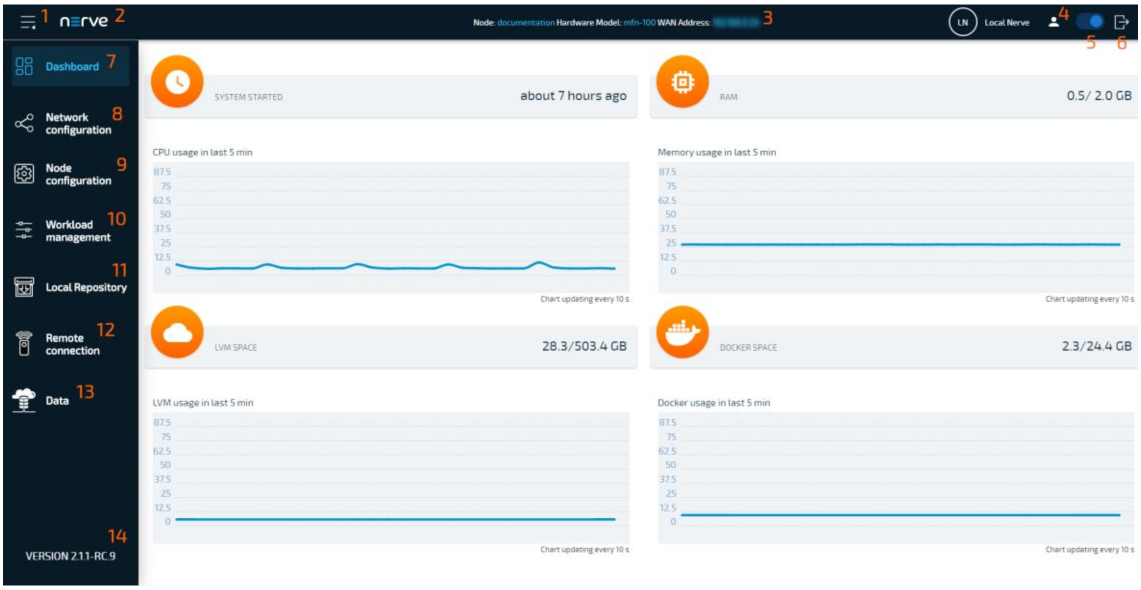


Figure 3: Local node UI

Management Services

Management services are hosted by the Management System in the Cloud or on premises. The Management system is a web-based service and enables the management of the nodes that are registered to this specific management system. The management system offers the following services: monitoring (and logging) of nodes, deployment and control of workloads to the registered nodes and the management of workloads (see Figure 4).

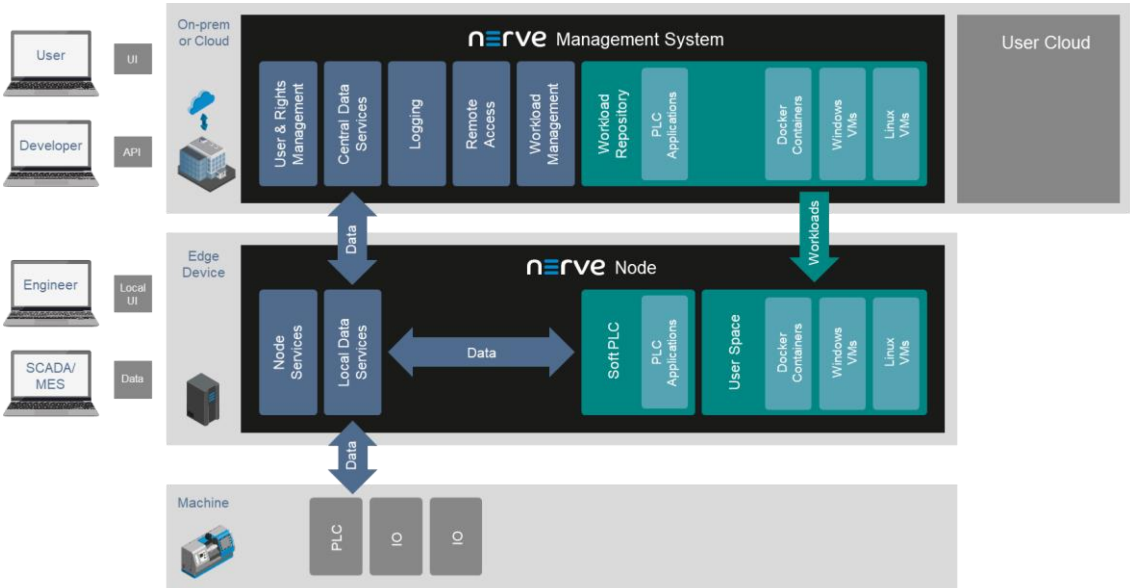


Figure 4: Nerve System Architecture Detail

Remote connections

To have a direct connection into a node located at a factory or a machine or even a direct connection into a virtual machine on the edge device, an improved remote connection to the edge device has been established. The advantage of having a direct remote connection to the edge device or even to the virtual machine on the device, is that deployment and maintenance can also be performed remotely, thereby significantly reducing costs.

There are two options available for these remote connections, namely remote screens and remote tunnels.

- Remote screens are connections that are established between the Management System and a target (e.g., a machine). These remote screens are configured and visualized within the Management System (see Figure 5) and support the following protocols: SSH, RDP and VNC protocols.
- Remote tunnels are connections that are created from a local workstation to a target (see Figure 6). This is similar as a VPN connection. Tunnels allow access to services and servers on the target directly from the user's local workstation. Remote tunnels are managed and established in a connection manager system and the Management System. The locally opened connection endpoint can then be leveraged in a web browser, with SSH clients, or with a remote desktop application, depending on the target.

The targets for these remote connections are either the node itself, the workloads on the nodes or even external devices that can be connected via the edge node itself.

The remote connection is established via the management system. A web socket connection is established for the tunnel between the edge device and the workstation, through the management system.

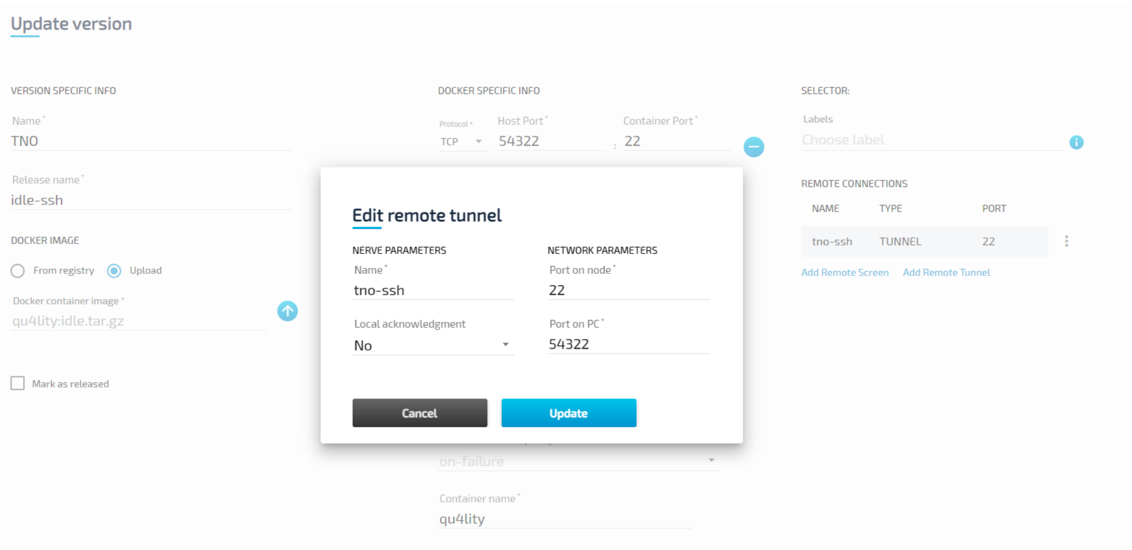


Figure 5: Remote tunnel configuration

A remote screen can be established from the Management System directly to the target. This can be established either via SSH, VNC or RDP connections to nodes or workloads in the Management System (Figure 6).

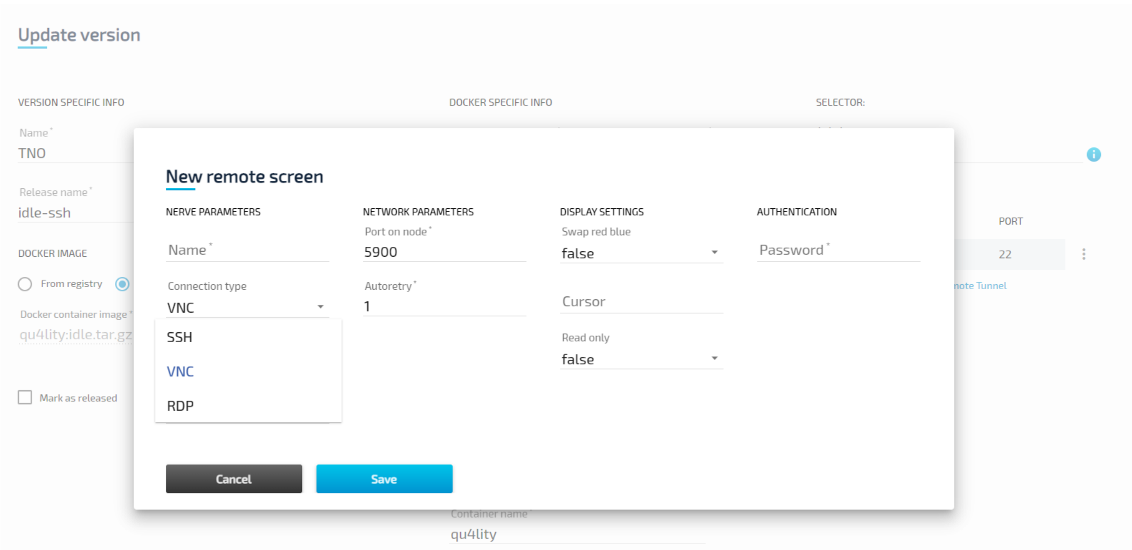


Figure 6: Remote screen configuration

Virtual/Soft PLC

Nerve Blue can be used to host and manage multiple virtual/soft PLCs on one edge device, enabling convergence of control on the plant floor. Nerve Blue can be used to control multiple real-time applications with a single device using soft PLCs from multiple vendors. As seen in Figure 1, a soft PLC can be included into a single virtual machine on the node. If you have multiple virtual machines, each one can host a soft PLC, thus making the node capable of hosting multiple soft PLCs. Within the soft PLC, control programs can be hosted for real-time applications with cycle times down to 500 µs, making it an excellent solution for directly interacting or controlling machines on the shopfloor.

Real-time workloads can be developed as CODESYS applications. A CODESYS runtime environment (RTE) is being hosted in the real-time virtual machine (RTVM) to execute these real-time workloads.

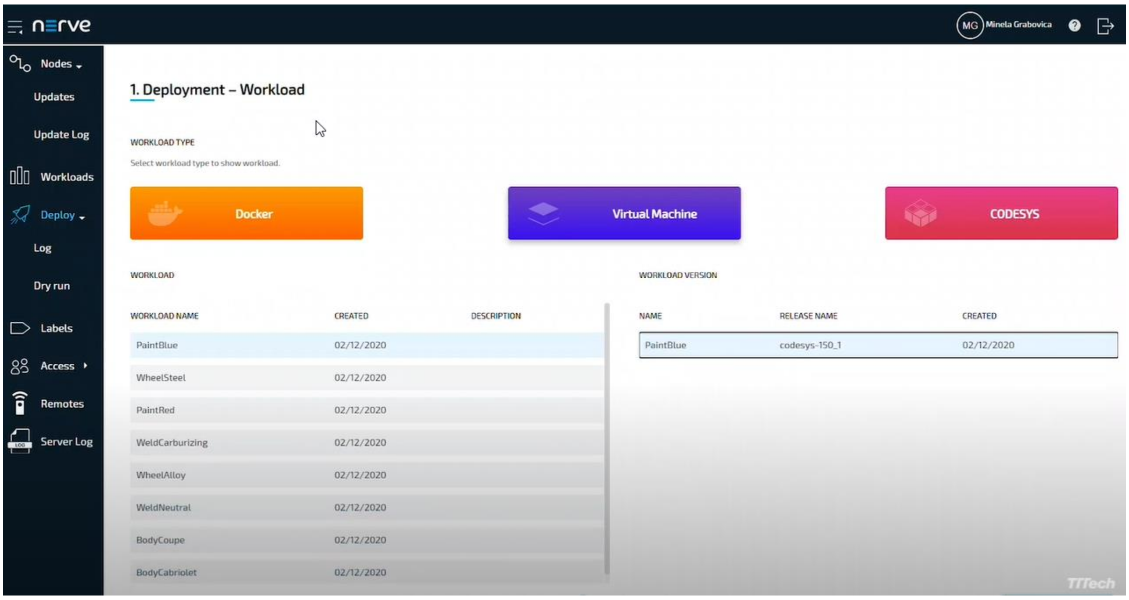


Figure 7: CODESYS real-time workloads can be deployed from the Management System

For the implementation and the hosting of soft PLCs, a hypervisor has been integrated into the Nerve Blue system. For this solution, the Xen hypervisor has been integrated into the architecture for hosting real-time applications. Xen is a type-1 hypervisor, which is also called a Bare-Metal-Hypervisor. It runs direct on the hardware and is also referenced as the hardware virtualization engine.

3.2.4 Documentation

A free trial version of Nerve Blue can be acquired from the product website. One can find this on the following page:

https://www.tttech-industrial.com/products/nerve/free-trial/

A quick start guide and documentation regarding Nerve Blue can be found on the following website: https://docs.nerve.cloud

3.2.5 Deployment

The Nerve Blue solution will be deployed in the pilot #1 – PHILIPS OneBlade shaving unit production line. Within the PHILIPS pilot line, Nerve Blue will be deployed to collect data directly at the machines and to host the applications from partners TNO and Fraunhofer to improve the quality measurements of the production line and to improve the overall performance of the system.

The pilot line is the PHILIPS OneBlade shaving unit product line, which is being developed as a new production line with increased capacity to meeting the increasing market demand. The aim is to improve the main metrics: Time to market, Production costs and Product/component quality.

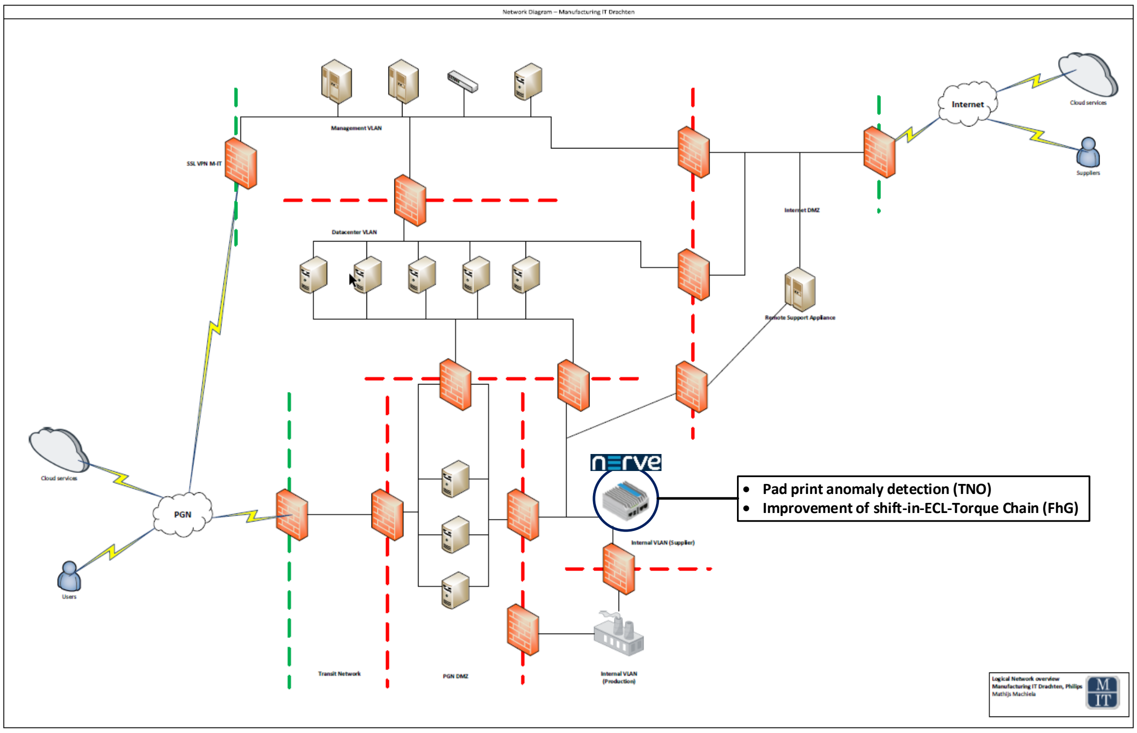


Figure 8: Nerve Blue at Philips Pilot

Together with partners Philips, TNO and Fraunhofer, TIAG has been working on the Philips pilot, where Nerve Blue will be deployed as the infrastructure for hosting the ZDM application developed by TNO and Fraunhofer.

TNO – Anomaly detection for pad printing process

TNO has developed an anomaly detection algorithm for the Philips Pilot line. One of the production steps in this line is the pad printing process in which a grid is printed onto a metal shaving blade. To support the prediction of potential pad printing issues and thereby the remaining ink lifetime, insight into defect trends are desired, also for small anomalies in the pad print that do not lead to actual rejections. A state-of-theart supervised deep learning network can be trained to detect these defects but that will require a lot of annotated training data. Moreover, such a network cannot cope with anomalies that have not been included in the training set. As retraining can be costly and time consuming, TNO proposed to create an unsupervised algorithm that should meet the following requirements:

- Model normal variation
- Easy to implement (within 1 day) and maintain
- Easily accessible by production personnel
- Can be trained with contaminated dataset
- Should be fast enough for inline application

These requirements can be met by an adversarial auto-encoder. The encoder maps an image of the shaving blade after the pad-print process to a latent space. Next an image is reconstructed by the decoder network. Since only a small fraction of the training set corresponds to defects, the decoder will not be able to reproduce such anomalies. Hence, the difference between the original image and the reconstruction will show any imperfections in the printed grid. If the reconstruction error exceeds certain threshold, the print is considered to be anomalous.

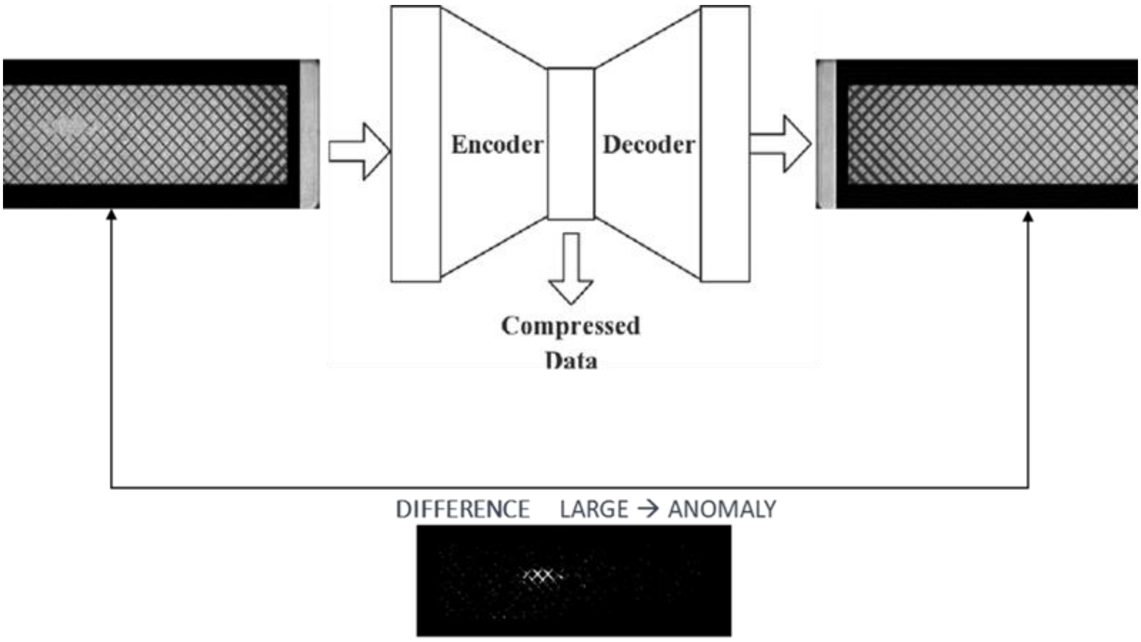


Figure 9: Product images are processed with an adversarial auto-encoder. The reconstructed image outputted by the decoder or compared to the original image. As the network is not able to reconstruct product defects, large difference between input and output indicate the presence of such a defect.

The actual application that is going to be tested in the Pilot line will run in a docker on a Nerve Blue solution. For each produced shaving blade, an image will be sent to the docker environment and analysed by the anomaly detection algorithm. The results will be logged so that they can be viewed when desired.

Fraunhofer IPA – Anomaly detection for assembly process / shift-in movement

Fraunhofer IPA is developing an anomaly detection system that is applied to an assembly process in the Philips pilot (shift-in movement), based on time-series data from process-integrated non-visual sensors. The shift-in movement takes place as an intermediate process step in the production line. A misalignment between the two assembled parts results in a reduced performance of the final product. Today, this issue is identified in an end-of-line tester at the end of the production line. In order to improve the production process, the anomaly detection system focuses on two aspects: First, identification of critical work pieces directly after the shift-in movement. Second, avoidance of faulty work pieces at all by an intelligent process control system that identifies anomalies before they become critical.

The system for anomaly detection utilizes supervised and unsupervised algorithms for anomaly detection. Input data comprises e.g., force-way-measurements with high sample rate and differences of programmed and actual positions of the tool centre point (TCP) of the assembly robots. Rare process failures e.g., unsuccessful gripping activities along the production line are also considered. Moreover, unsupervised methods based on the statistical cluster analysis are utilized to identify yet unrecognized anomalies.

The anomaly detection requires an edge device close to the shop floor in order to evaluate sensor data in real time and to take corrective actions if necessary. From a data flow point of view, machine and sensor data is collected from different stations in the production line, mainly for the assembly station and the end-of-line tester. Product tracking is ensured by a data matrix code (DMC) on each product. The evaluation utilizes machine learning algorithms and models. The machine learning inference is realized on the computing unit / edge device next to the production line. An update of the ML model is performed on the edge device or by a specialized cloud service from Fraunhofer IPA, depending the frequency and the data intensity of the update process.

The system for anomaly detection advises or performs corrective actions in a run-2-run manner, i.e., they are applied in the subsequent assembly cycle. This implies real-time ability for the edge device, but with rather mild real time constraints (~500ms).

3.2.6 Future Work

There is continuous updates and improvement performed on the Nerve Blue edge solution. A small subset of future developments that are planned for the edge solution are the following:

- Improved flexibility of the hypervisor, which would improve the real-time performance of the edge solution.

- Make the system hardware agnostic, being independent on the hardware where the edge solution is deployed. Currently, a small set of hardware is supported, but the aim is that in the future more and more hardware solutions are running Nerve Blue, making the system open for any solution what the customer is supporting.
- Improved remote viewing of the edge devices, enabling system integrators or end users to monitor worldwide more easily the deployed edge devices. Providing the possibility to remotely view the virtual machines running on edge devices directly on the monitor of the system integrator.
- High availability and improved support of Machine Learning and Artificial Intelligence directly running on the edge.

3.3 Danobat Box

3.3.1 Digital Enabler Overview

The Danobat Box is the solution used by Danobat for the monitoring and provision of associated services related to their machines. It is a robust solution specially designed for machine tool and process industry manufacturers. It captures and makes use of all the information generated by the Danobat Machines. The platform enables heterogeneous data acquisition made simple and it also provides a safe channel, in order to send this information to the cloud.

It is a “Plug & Run” system, easy to install and compatible with a big number of industrial automation protocols. It is interoperable, as it allows to share information with third party systems and software. It is a non-intrusive system as it works in parallel avoiding overloading the CNC or PLC of the machine.

The Danobat box allows to deploy software in the edge through a dockerized system. Because of the volume of data in IoT environments, some processing and management functions have to be pushed closer to the devices in order for them to scale. That extension to the edge requires more complex operational management – another layer must be integrated into the operational model, and the IoT platform needs to have the architectural support for it. Functions such as identity validation and data processing can be projected out to edge elements to distribute the work required to operate at IoT scale.

Even though the cloud computing paradigm seems ideally suited for addressing the increased demand for computation power at the edge, this comes at the expense of an additional abstraction layer that imposes significant overhead to the software stack. Danobat Box edge computing offers computation and storage at the very edge of the network where data is produced, reducing latency and limiting the load that is carried to higher layers of the infrastructure hierarchy.

3.3.2 The Business and ZDM perspective

The Danobat Box has been developed and customized in the Quality project to exploit the possibilities of the Edge Computing for ZDM manufacturing.

It provides the following advantages:

- Modular and scalable architecture based on virtualization applied to different functionalities at machine and plant level, which allows moving services directly to the edge device where the data is locally acquired. Overcoming the reluctance of the customers of Danobat to connect the machines to the cloud.
- With the provided container-based technology that acts as the platform for edge computing, advanced analytics, or even third parties' algorithms from the cloud, can be deployed. New functionalities on containers configure a new digital value proposal from Danobat.
- Computing of some functionalities in an environment independent from the machine operation. Optimal technical solution that protects the main function of the machine from possible failures associated to new digital features.

It is applied to the following functions that configure the digital value proposal of Danobat:

- Machine condition analysis cycles pre-processing and persistence
- Interoperability with plant software, allowing the integration with business systems from edge level.
- Application of communication standards
- Machine learning algorithms and associated diagnosis

Advantages from the Business point of view:

- Easy connectivity of industrial devices. Thanks to the "Plug & Run" design, the Danobat Box data-capture device can be installed and connected to any industrial asset (machine tool, component, robot) in a matter of minutes.
- Flexibility to adapt the solution to the needs of each industrial case in terms of connectivity to other software, customized smart functions and algorithms, etc. The Danobat Smart functions can be installed and run even with no or very restricted connection to the cloud.
- Remote management of the developed solutions
- Offers an inclusive all-in-one service for both monitoring and edge computing, among others. Other commercial gateway product and solutions are most purely focused on data acquisition.

- Reduce costs. Production digitization helps businesses gain better insight into production issues like, use conditions of the machines or use of the tools. This increased visibility helps reducing unnecessary risks and costs related
- Customers leveraging the Danobat Box can expect to see a substantial decrease on their required IT & computational resources for digesting their monitored machine tool and process data

3.3.3 The Technological Perspective

The Danobat solution consist of the Danobat Box and the Danobat Cloud. The box is not only the gateway that allows to gather key data for the machine monitoring but an edge device that multiplies the developing capabilities for the machine tool manufacturer. The cloud allows the gathering of historical data for learning and analysis purposes and is also the management point for the lifecycle of the devices, data and applications.

By using the system's automatic deployment tools, the Danobat Box can connect any machine or process line to Danobat Cloud regardless of its site while ensuring the security of the platform and the facilities and machines being monitored.

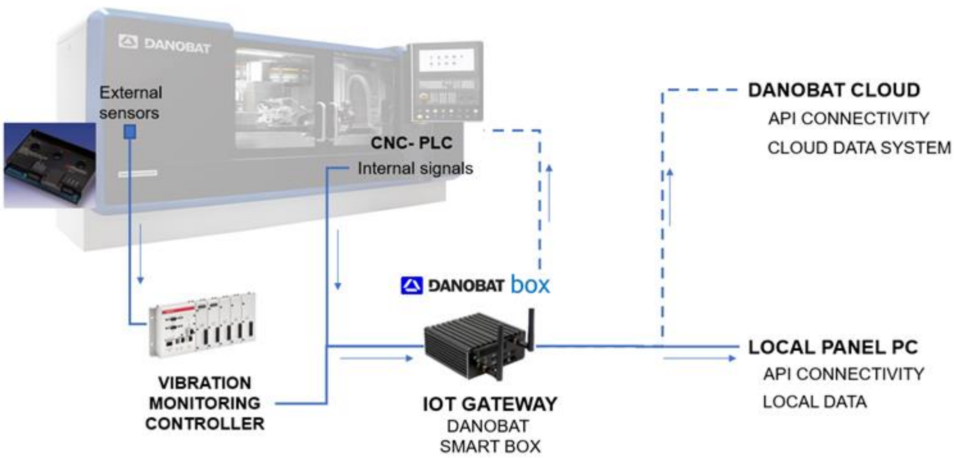


Figure 10: Schema of installation of the Danobat Box

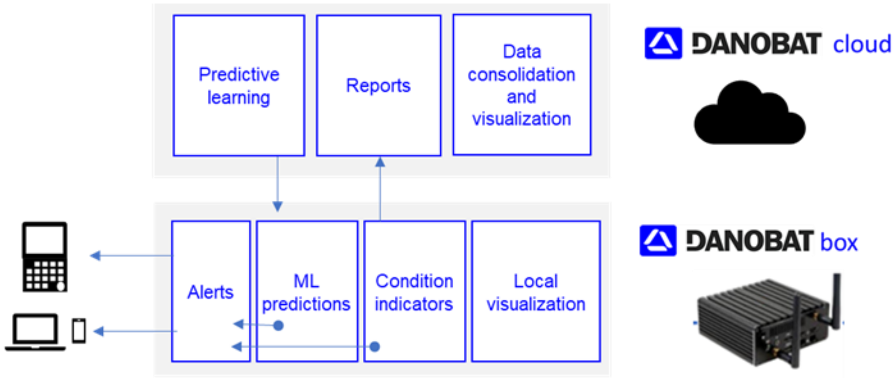


Figure 11: General architecture of the Danobat Solution

The Danobat Box is connected to the rest of the industrial environment through three layers. The box is really easy to connect to any data source thanks to the connectivity layer, that is prepared with the most important industrial protocols and standards.

Thanks to multi-level API data, any information can be obtained using standard protocols for use by third-party systems either on-site or in the Cloud:

- Streaming Data: Steady stream of data in standard format. Multiple protocols available.
- Data On Demand: Request time ranges, filtered by machine, factory or any requirement.
- Aggregate Data: Value-added information pre-processed and shared with third parties.

The data can also be provided following the latest industrial standards like UMATI or IDS among others. The box also provides local visualization through a flexible interfaces' configuration tool.

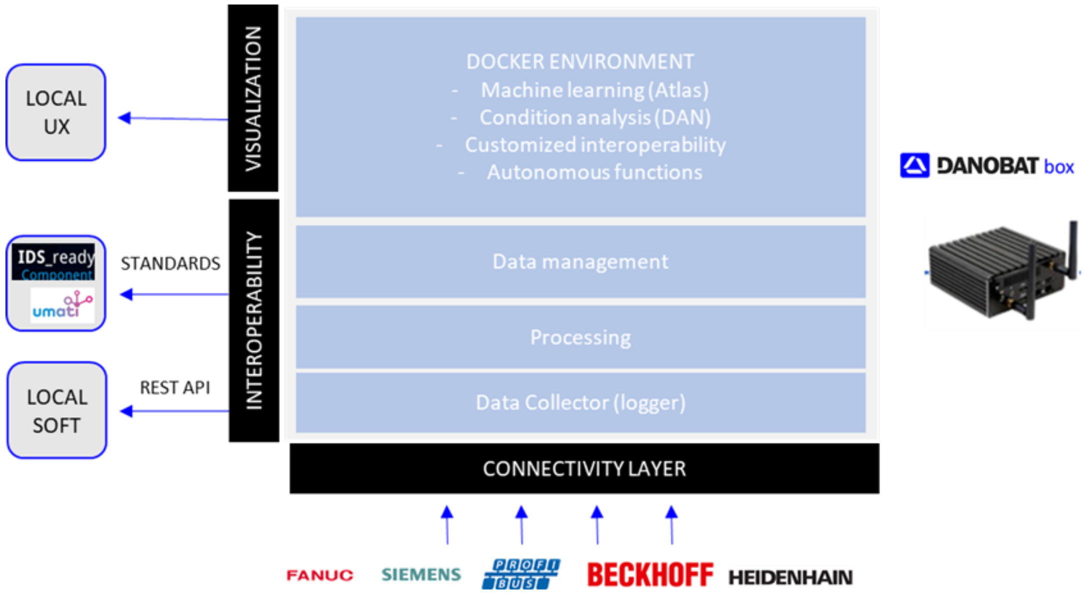


Figure 12: Capabilities of the Danobat Box at Edge Level

The microservices-based architecture and container-based application make the solution flexible and enable the edge computing. The docker containers enable the virtualization of the implemented applications in the Danobat solution, which can be deployed as isolated executed avoiding dependencies with other software

This provided modularity combined with the orchestration supplied by Docker technology, simplifies the management and enables distributed deployments, creating a highly dynamic system.

All the containers are managed from the Danobat Cloud platform. As each model/algorithm is running in the box, we should enter the Applications tab in the specific section of the box installed in the shopfloor.

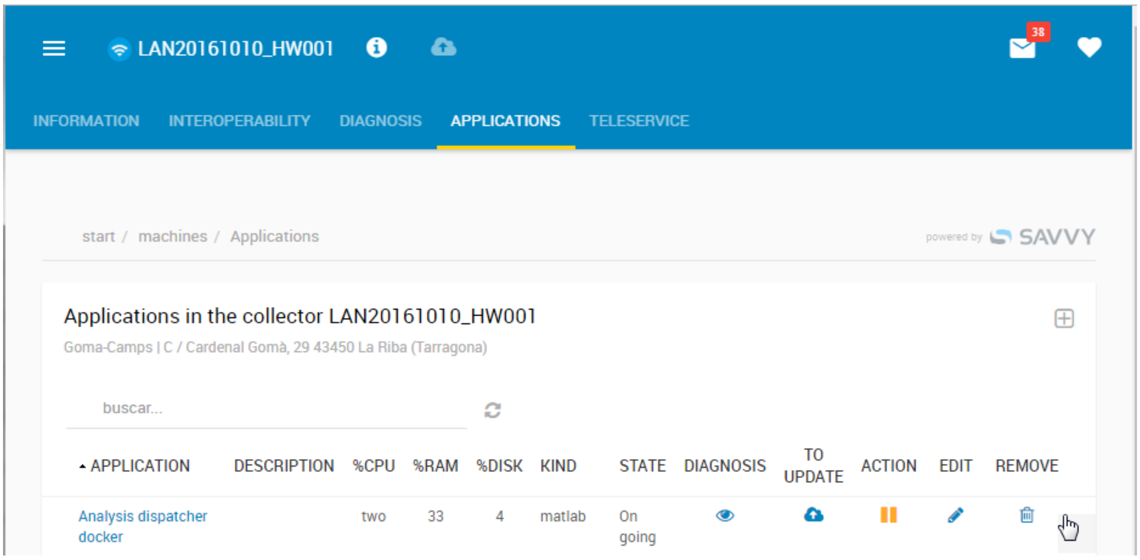


Figure 13: View of applications section in the Danobat Box

The Danobat solution offers also teleservice, a native remote access functionality which enables users to communicate with the Danobat Box and production equipment by means of secure connections established over Danobat's cloud servers.

3.3.4 Documentation

Information related to the commercial hardware and software that is the base for the Danobat Solution can be found at: https://www.savvydatasystems.com

3.3.5 Deployment

The system is being deployed in two pilots in the Quality project:

- Pilot #5: Zero defect and Autonomous Quality in Machinery Building for Capital Goods sector
- Pilot #12: Danobat Digital Machine for zero-defects at high precision cutting/grinding

In both cases the Danobat Box is used to collect and process information related to the condition of the machines and processes.

Pilot 12 is an application centred in one griding machine and besides data collection, some of the applications that are containerized in the box , also by other partners in the project can be seen in Figure 14.

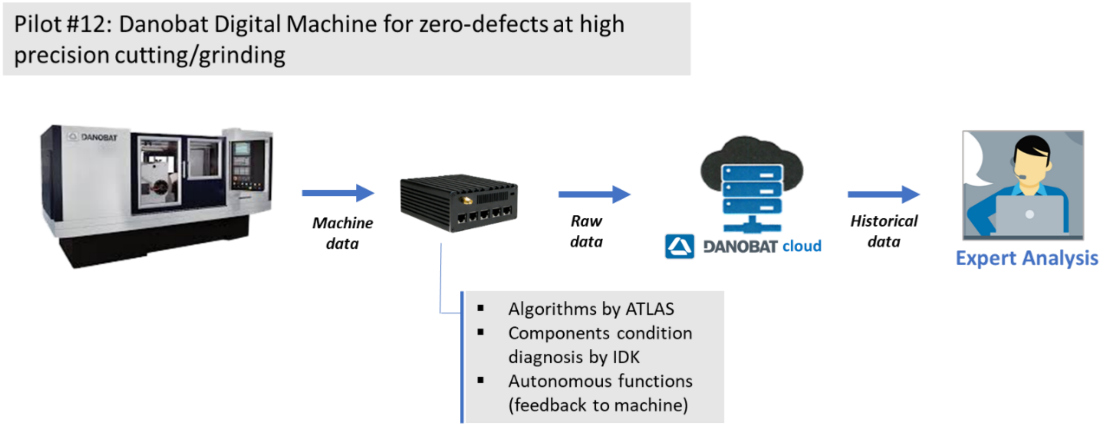


Figure 14: Danobat Box at Pilot #12

In the case of the Pilot #5, the box is used for all the machines in the line and it also allows the connection with other software that is key for the pilot development as can be seen in Figure 15.

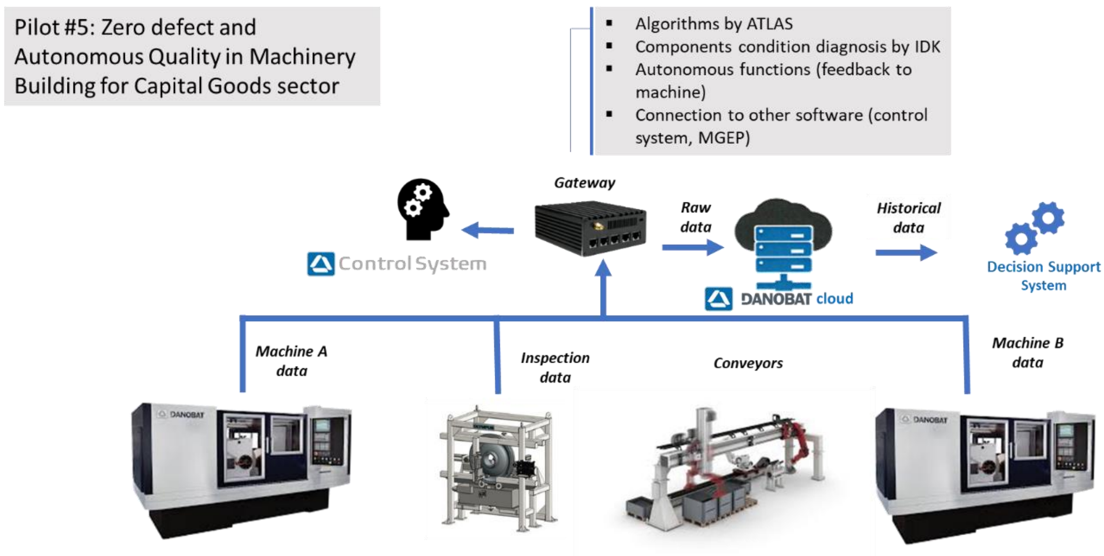


Figure 15: Danobat Box at Pilot #5

3.3.6 Future Work

The future research lines on the edge applications are related to:

- Distributed applications: node autodiscovery, master/slave containers
- Security layers (i.e., SDK technologies)
- Installed base applications monitoring (real time logs, management of a big number of boxes and applications).

3.4 FOOTPRINT

3.4.1 Digital Enabler Overview

FOOTPRINT is an edge device that enables a high-level monitoring of the production quality, automatic detection and identification of problems or defects during manufacturing. It uses voltage and current sensors to create energy profiles, for a machine doing a specific job.

A bundle of datasets is used to create a profile for the machine's action being well performed, without any detectable problems, and other profiles for each type of possible defect or manufacturing fault, that is desired to be monitored and detected. In the simplest case, where the algorithm has been trained by a dataset that does not specify any faults or defects, the tools will only monitor if the machine's job is being performed as expected or if something unexpected has happened, indicating that a problem might have occurred, without identifying which type of fault has happened.

The edge device provides energy monitoring and detection of the machine's job or action based on the energy profiles used to train the model. Additionally, automatic detection and identification of problems or defects during manufacturing and maintenance forecasts can also be supported.

3.4.2 The Business and ZDM perspective

Automatically identifying faults on produced parts, and even predicting when maintenance is needed on certain machines, is essential in industrial environments, so that simple problems can be fixed prior to production defects or failures on the production line occur.

Detection production faults early would reduce the number of faulty products manufactured in the long term and reduce wasted raw materials used and consequently reduce costs overall. The proposed ZDM implementation is focused on improving the detection of faults or issues on machines throughout the production pipeline, helping to quickly identify issues that could cause a product to not comply the quality standards of the company.

Additionally, reducing longs stops in machinery to fix issues leads to more uptime in production and consequently more income. Eventually, shorter and frequent maintenance in the machinery can also prevent faulty products to be manufactured and prevent a more costly intervention in the machinery. It is anticipated that a machine's maintenance needs could also be detected by identifying deviations on certain behaviours of the machine's energy profile, which could be used to forecast and alert that a maintenance check should be performed, prior to the usual periodic maintenance, to avoid degradation on the machine performance and quality of the produce.

This can be achieved through improvements in advanced detection of defective products, and integration with the production line control systems for autonomous defect mitigation, by using available data acquired from edge devices to generate pattern recognition models, that can detect when the product quality has differed from what is expected. FOOTPRINT deep learning analytics generate statistics and alert decision support systems assisting them to react fast when shift in quality occurs.

3.4.3 The Technological Perspective

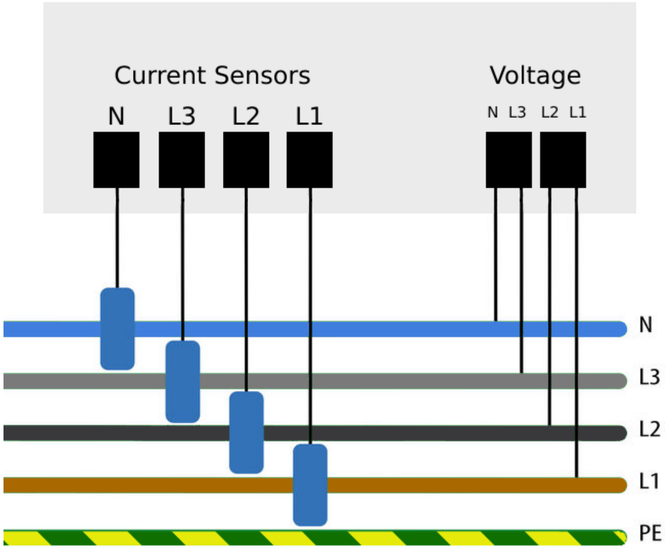
The FOOTPRINT edge device has 4 inputs for current measurement (L1, L2, L3, N) and three inputs for voltage measurement. This allows measurements on all three phases and the neutral conductor.

Figure 16: FOOTPRINT edge device

The system is supplied with the required operating voltage via the L1 voltage connection, thus a separate power supply is not required. All interfaces to the system are galvanically isolated to ensure maximum safety. The housing has a mounting bracket on the back for mounting the system on a DIN rail, allowing easy installation.

Measured parameters:

- Current
- Voltage
- Power
  - Active power
  - Reactive power
  - Apparent power
- Energy consumption
- Energy production
- Power consumption
- Power production
- Frequency
- Power factor



The measured parameters are read out every second and sent to the configured MQTT broker, for persistent storage of historical data in an external database. The data is also stored in an internal database every minute, which is convenient in case of offline usage. The measurement periods can be configured if needed, to match the requirements of the specific application scenario.

Dashboard

A dashboard, built with Grafana, is provided to view real time and historical data. The dashboard can be customized to display the most relevant info, as needed by the user, and alerts can be defined, to notify the user when a parameter exceeds a threshold or certain conditions are met. The dashboard also supports exporting the historical data as CSV files, for chosen time frames, to allow usage of the datasets with other tools.

Figure 18: FOOTPRINT data explorer

RESTful API

With the integrated RESTful service, it is possible to read all relevant values directly out of the edge device.

Table 3: Allowed parameters for <valueid>

current	Current [A] (available for phase 1,2,3, neutral conductor)
voltage	Voltage [V] (available for phase 1,2,3)
power	Power [W] (available for phase 1,2,3)
cosphi	cos φ (available for phase 1,2,3)
frequency	Frequency [Hz] (available for phase 1,2,3)
all	Get all Values

Table 4: Allowed values for <phaseid>

1	Phase 1
2	Phase 2
3	Phase 3
4	Neutral conductor (only for use with <valueid> current)
all	All phases

The RESTful API can also serve historical:

Table 5: Historical parameters for <valueid>

current	Current [A] (available for phase 1,2,3, neutral conductor)
voltage	Voltage [A] (available for phase 1,2,3)
power	Power [W] (available for phase 1,2,3)
cosphi	cos φ (available for phase 1,2,3)
energy_pos	Energy [Wh] (energy consumption)
energy_neg	Energy [Wh] (energy production)

Table 6: Historical parameters for <phaseid>

1	Phase 1
2	Phase 2
3	Phase 3
4	Neutral conductor (only for use with <valueid> current)
123	All phases

Pattern recognition capabilities

At an initial stage the device is deployed, without any trained models and recognition capabilities, to collect data that will then be analyzed and arranged into datasets to train the models. The general workflow for enabling the pattern recognition capabilities on the edge device is depicted on the diagram below, Figure 19.

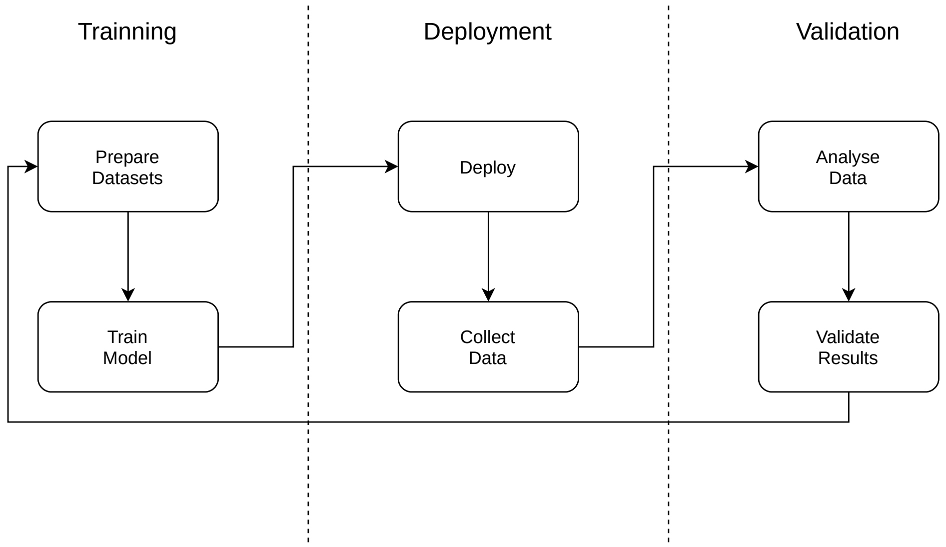


Figure 19: Training, deployment, and validation sequence

To train the pattern recognition models, besides the current and voltage sensor data, it is needed to know what job or action the machine was performing, and what faults might have occurred, to allow matching the energy profiles with a job, action, or fault. Initially, the edge device is deployed to collect the energy parameters needed to model the machine's energy profile. Then the models can be trained, using the collected sensor data together with timestamped annotations, provided by the manufacturing company. These annotations provide context to the training algorithms and allows the categorization of the datasets, according to what action was being performed by the machine, enabling the models to know how to detect and identify a fault, that could happen during production.

The trained models are then deployed, along with the ongoing data collection. The collected data along with the results of the first-stage recognition capabilities, are then analysed and used to validate and refine the models, that are then retrained and redeployed. This training, deployment and validation sequence can be repeated until the models have the desired performance.

When the models are deployed, the recognized events are shown as annotations on the dashboard, together with historical data, automatically providing context of what was happening to the product manager. The device itself will not perform any direct control on the monitored machine, however alerts can then be configured, to generate notification for specific events, such as when a fault is detected and alert can be generated, notifying the PLC that is controlling the machine. The PLC can then decide to trigger an action, like discarding the produce due to a possible defect or stopping the machine to avoid further damage.

3.4.4 Deployment

The edge device is intended to be deployed at tested at the Experimental Facilities at a later stage.

3.4.5 Future Work

The advance of the edge node technology within QU4LITY will focus on the following aspects:

- Generation of energy profiles for each machine job, action, or fault.
- Enhancement and refinement of the model building algorithms.
- Integration with dashboards and decision support systems

4. QU4LITY Validation Strategy

The following table provides an overview of the QU4LITY Validation strategy that have been developed/provided within the project and that will be deployed in either a pilot or an experimental facility. The following section will describe the developments on the validation strategy and how it is being used within the designated pilots or experimental facilities to reach the goals of the QU4LITY project.

Platform	Description	IP Owner
Q-Digital	The certification framework advocates for a modular approach, where core components are certified for concrete usage scenarios and the specific adaptation to tailor the solutions deployed is actually validated or certified at the factory shopfloor.	SQS

Table 7: Overview of Validation Framework

4.1 Q-Digital Automation Framework

4.1.1 Digital Enabler Overview

SQS is developing Q-Digital Automation service, an enabler that allows the validation process to be carried out.

This enabler is founded on the idea of a Digital Automation Validation Laboratory, the architecture of the core enabler is shown in Figure 20. The goal of Q-Digital Automation is to supply a certification framework that advocates for a modular approach, where core components are certified for concrete usage scenarios and the specific adaptation to tailor the solutions deployed is actually validated or certified at the factory shopfloor.

This enabler consists on a certification laboratory flexible to validate performance, scalability, OT/IT safety and security of Industry 4.0 base technologies and can be customized to the validation of application specific deployments in any industrial sector. Among the different industrial sectors addressed by Q-Digital Automation are Manufacturing, Production Facilities, Metrology, Industrial Automation, Railway and Pharma.

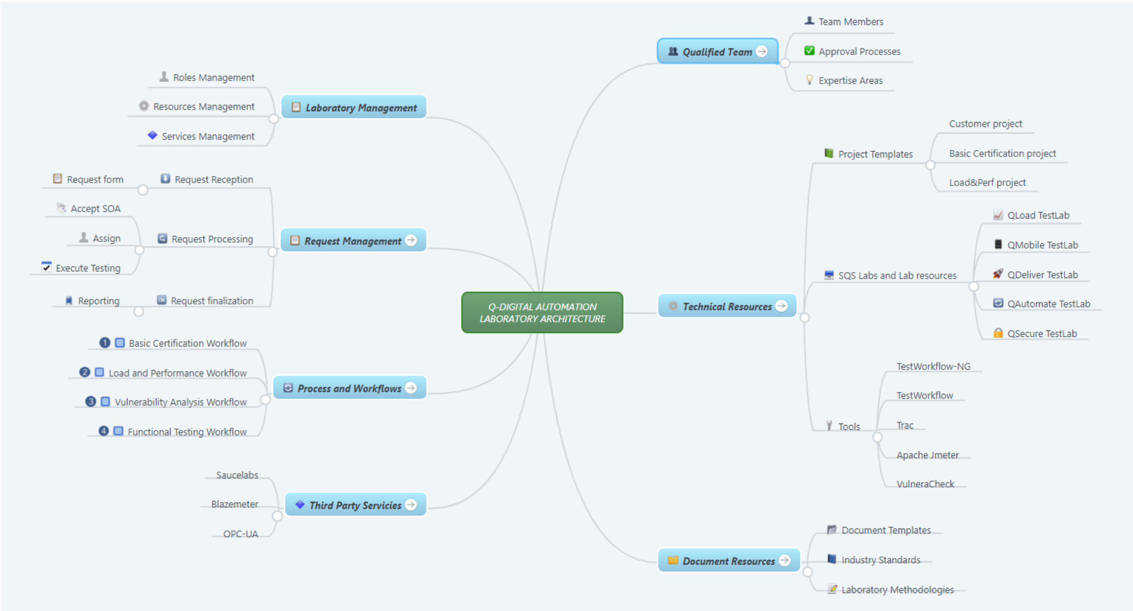


Figure 20: SQS Testlab Architecture

To carry out this validation process through Q-Digital Automation, it is necessary to follow a series of steps defined by this certification framework. The validation process is made up of the following phases:

- The owner of the component requests the certification and the acceptance requested is registered in MangoApps, which is a platform like a workplace that integrates the applications that SQS uses along the whole validation process.

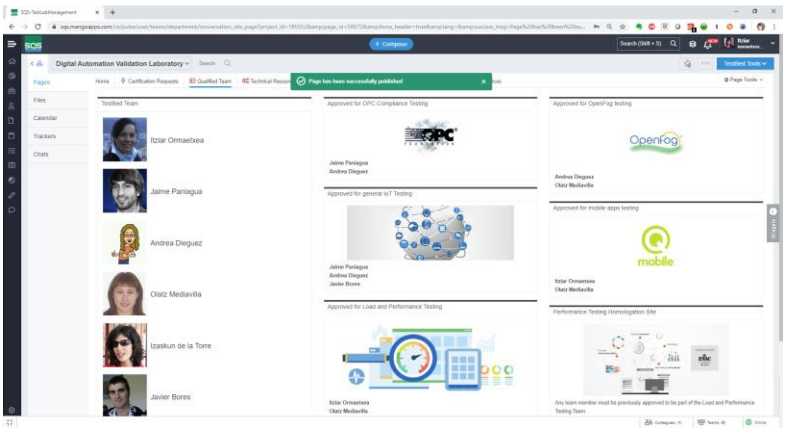


Figure 21: MangoApp Interface

- The next step is the conformity assessment. The SQS Testlab Manager receives the request and begins the certification procedure, accepting the assignment.

- The next step is to upload the document and make the Hardware/Software request. The SQS Testlab Manager assigns the specific tasks to the SQS team and uploads the certification templates. Afterwards, the declaration of applicability is sent to the client and when final approval is obtained, the component is requested to be sent to be tested.

- The next step is the installation and configuration of the component for test development in the SQS lab (and not at Pilot premises: this is important). The SQS Testlab Team configures the component so that testing can begin.

- The next step consists of reviewing the documentation generated in the previous steps and determining: the certification strategy, the work team in the certification process and the selection of the necessary tools to carry it out.

- Component testing begins. The first are called White-Box testing, which consists of a review of the internal structure, design and code of the software. It mainly focuses on verifying the flow of inputs and outputs through the application, improving the design and usability, strengthening security. Through these tests, the code evaluation report is generated, reporting the errors identified.

- The next test is the functional assessment. Bump testing is a quality assurance (QA) process that bases your test cases on the specifications of the software component under test. Through this test the functional evaluation report is generated.

- The final tests are related to vulnerability analysis and consists of penetration tests. These tests are intended to exploit vulnerabilities in a system to determine if unauthorized access or other malicious activity is possible and to identify which cracks pose a threat to the application. Through this test the Vulnerability Assessment Report is generated.

- Finally, the SQS Testlab Manager collects all the previous reports, reviews them and generates the final validation report of the component, determining if it meets the established requirements. This report is sent to the client through MangoApps.

The deadlines established to carry out this entire validation process depends on the complexity of the component and what needs to be validated. For this, and summarized in the chart of Figure 22, three possible scenarios have been established, from the faster to the most conservative one, giving a deadline for each phase of the process:

Phase	Low (days)	Medium (days)	High (days)
Phase 0: SOA	Owner	Owner	Owner
Phase 1: Conformance	2	4	5
Phase 2: Upload	Owner	Owner	Owner
Phase 3: Installation	1	3	5
Phase 4: Documentation	3	5	7
Phase 5: White Box (if req.)	3	7	10
Phase 6: Functional	5	7	10
Phase 7: Vulnerability	5	5	10
Phase 8: Reporting	3	5	7
Total (days)	22	36	54

Figure 22: Possible scenarios for the Validation process

Where Owner means that this step depends on the customer, for when they decide or manage to do it. This means that it is not actually inherent to SQS.

4.1.2 The Business and ZDM perspective

QU4LITY aims to reach a ZDM stage. This stage is a capable giver to increase the quality and reduce cost. ZDM is applicable in any manufacturing domain and area, making its structure more intelligence using Autonomous Quality solutions.

An industrial environment using Autonomous Quality solutions is complex, and it is essential to ensure that the tool fulfils the purpose for which it was created, and even more so in the cause of Autonomous Quality solutions based on AI/ML algorithms since there are continually changes and new data inputs. Having a ZDM validation and verification framework that will confirm that the implemented Autonomous Quality solutions will work as they should, not only at the time of installation/configuration/security, but also during their execution. The advantages offered by Q-Digital Automation are the following:

- **Trustworthy process**, the V&V framework will ensure that Autonomous Quality solution works correctly for specific usage scenarios. The validation will be adapted to the SUT (Specifications and Usage Testing) needs.
- **Versatility**, it is a tool that can be applied in a wide range of Industry 4.0 technologies such as Industrial Communications, Fog / Edge Computing, Robotic Systems, Cybersecurity & Safety, Cloud Computing, Big data and analytics and Mobile Solutions.

- **A more secure environment**, it is safe because a user and password are provided for each client, and it is reliable because the customer can see the status of the certification, as well as the tests that have been executed.

4.1.3 The Technological Perspective

Developing a V&V framework for intelligent technologies is a great challenge, since most of the time a system is watertight, that is, a system that does not have information alterations, nor does it have changes of intended use. In this type of environment, the V&V of the component is very simple, since it would only be necessary to do it once to see if its installation, security and configuration is adequate.

In the case of Industry 4.0 technology environments, more specifically in autonomous quality environments using AI/ML algorithms, this is not the case, they are very **dynamic environments that are continuously receiving information**; therefore, it is a system that must be validated continually. We could say that this occurs because an algorithm that receives information results in a new algorithm. The objective of the framework developed by SQS is none other than to ensure the validation of the autonomous process during the total lifecycle.

Change in an Autonomous Quality solution can be due to three situations:

- <u>Performance:</u> Improvements to analytical and clinical performance that could follow from a number of changes. This may include re-training with new data sets within the intended use population from the same type of input signal, a change in the Autonomous Quality solution architecture, or other means.

- <u>Inputs:</u> These types of modifications are those that change the inputs used by the Autonomous Quality solution. These alterations could involve modifications to the algorithm for use with new types of input signals, but do not change the product use claims.

- <u>Intended use:</u> These types of modifications include those that result in a change in significance of information provided by the Autonomous Quality solutions.

For each of the possible changes in the Autonomous Quality solution, the result must be validated to check if the change is trustworthy or not. This evaluation will be carried out taking into account the **Assessment List for Trustworthy Artificial Intelligence 4.0** (ALTAI4.0).

The goal of ALTAI4.0 is to provide an evaluation process for Trustworthy AI self-evaluation. Companies could be able to draw elements relevant to the particular AI system from ALTAI4.0 or add elements to it as they seem fit (taking into account the sector). This self-assessment will allow the organizations to know what Trustworthy AI is, particularly what risks an AI system might generate and to identify what kind of active measures are needed to avoid and reduce risks.

To assess the AI solutions, the European Commission has established questions for each of the 7 requirements that ensure AI reliability. These requirements are:

- **Human Agency and Oversight**: "AI systems should support human agency and decision making, as dictated by the principle of respect for human autonomy". In this section, organizations should reflect on the effects that AI systems can have on:
    - Human behaviour, in a broad sense.
    - Human perception and expectations when confronting AI systems that act like human beings.
    - Human affection, trust and (in) dependence.

  The issues arising from these topics will help companies decide the most conducive governance and control measures and mechanisms, as well as different approaches, such as:

    - Human-in-the-Loop (HITL) or the capacity for human intervention in each decision cycle of the system.
    - Human-on-the-Loop (HOTL) or the capacity for human intervention during the System design cycle and for the control of system operations.
    - Human-in-Command (HIC) or the ability to monitor the entire activity of the AI system and decide on when and how to use the AI system in each particular situation.

  The questions in this part are primarily developed around the interaction of AI systems with end users and their learning and training process.

- **Technical Robustness and Safety**: "Technical robustness requires that AI systems are developed with a preventive risk approach and that they behave safely and as expected, so that unintended and unforeseen damage is reduced and avoided where possible". In this section, organizations should reflect on the following elements:
    - Resilience to attack.
    - Safety.
    - Precision.
    - Reliability, alternative support plans and reproducibility.

  There are two aspects that are key to obtaining positive results in the areas mentioned above:

    - Dependency, which encompasses the ability of AI systems to offer services that can be trusted.
    - Resilience, which means the robustness of AI systems to cope with changes, both in their environment or external, when there is the

presence of other agents, human or artificial, that may adversely interact with AI.

The questions in this part are primarily developed around undesirable and unexpected behaviours of AI systems, certification mechanisms, threat forecasting, documentation procedures, and risk metrics.

- **Privacy and Data Governance**: "Closely related to the harm prevention principle is privacy, a fundamental right that is greatly affected by AI systems". In terms of data protection, the harm prevention principle involves the following:
  - Adequate data governance that covers the quality and integrity of the data used.
  - Relevance of the data in light of the context in which the AI systems will be developed.
  - Data access protocols
  - The ability of AI system to process data in a way that protects privacy.

The questions in this part are mainly developed around the type of personal data used for training and development, the implementation of the measures and requirements of the RGPD, and the alignment of AI systems with important standards such as ISO standards.

- **Transparency**: "A crucial component to achieving trustworthy AI is transparency, which encompasses three elements: 1) traceability; 2) explicability; and 3) open communication about the limitations of the AI system".
  - Traceability: the AI systems development process should be properly documented.
  - Explicability: explicability refers to the ability to explain both the technical process of AI systems and the reasoning behind the decisions and predictions made by it, which in turn would have to be easily understandable by all those who saw it. Affected both directly and indirectly.
  - Communication: the capabilities and limitations of the AI system should be communicated to users in a manner appropriate to the use case and could include information on the level of accuracy of the AI system and its limitations.

The questions in this part are mainly developed around traceability measures, registration practices, user interviews, reporting mechanisms, and the provision or training material.

- **Diversity, Non-discrimination and Fairness**: "In order to achieve reliable AI, you must advocate for inclusion and diversity throughout the AI system lifecycle". Regarding AI systems, discrimination can be derived from the following aspects, both in the training phase and in the implementation phase:
  - Inclusion of inadvertent biases.

- Imperfections
- Bad models of government.
- Intentional exploitation of consumer biases.
- Unfair competition.

The questions in this part are primarily developed around procedures to avoid bias, education and awareness initiatives, accessibility, user interfaces, Universal Design principles, and stakeholder engagement.

- **Societal and Environmental Well-being**: "In accordance with the principles of justice and prevention of harm, society in general, other living beings and the environment should be taken into account as stakeholders throughout the entire life cycle of the AI system".
  The following factors should govern decisions in this regard:
  - Environment well-being
  - Impact on work and skills
  - Impact on Society as a whole and democracy.

  The questions in this part are mainly developed around the mechanisms to assess the social and environment impact, the measures to manage this impact, the risk of disqualification of the workforce and the promotion of new digital skills.

- **Accountability**: "The principle of accountability requires that mechanisms be established to ensure the distribution of responsibilities in the development, implementation and use of AI systems." Closely linked to risk management, there are three key elements for these purposes:
  - Measures to identify and mitigate risks.
  - Mechanisms to manage these risks.
  - Regular audits.

  The questions in this part are mainly developed around audit mechanisms, third party audit processes, AI ethics committees and protection for whistle-blowers, NGOs and associations.

Below are ALTAI4.0 questions for each of the requirements mentioned before:

❖ Transparency

Traceability:

- Did you put measures in place that can ensure traceability? This could entail the documentation of:
  - Methods used for designing and developing the algorithmic system:
    In case of a rule-based AI system, the method of programming or how the model was built should be documented;
    In case of a learning-based AI system, the method of training the algorithm, including which input data was gathered and selected, and how this occurred, should be documented.

- Methods used to test and validate the algorithmic system:

  In case of a rule-based AI system, the scenarios or cases used in order to test and validate should be documented;

  In case of a learning-based model, information about the data used to test and validate should be documented.

- Outcomes of the algorithmic system:

  The outcomes of or decision taken by the algorithm, as well as potential other decisions that would result from different cases (e.g., for other subgroups of users) should be documented.

Explainability:

- Did you assess the extent to which the decisions and hence the outcome made by the AI system can be understood?
- Did you ensure that an explanation as to why a system took a certain choice resulting in a certain outcome can be made understandable to all users that may desire an explanation?
- Did you assess to which degree the system's decision influence the organisation's decision-making process?
- Did you assess why this particular system was deployed in this specific area?
- Did you assess the business model concerning this system (e.g., how does it create value for the organisation)?
- Did you design the AI system with interpretability in mind from the start?
- Did you research and try to use the simplest and most interpretable model possible for the application in question?
- Did you assess whether you can analyse your training and testing data? Can you change and update this over time?
- Did you assess whether you have any options after the model's training and development to examine interpretability, or whether you have access to the internal workflow of the model?

Communication:

- Did you communicate to (end-)users – through a disclaimer or any other means – that they are interacting with an AI system and not with another human? Did you label your AI system as such?
- Did you put in place mechanisms to inform users on the reasons and criteria behind the AI system's outcomes?
- Is this clearly and intelligibly communicated to the intended users?
- Did you establish processes that take into account users' feedback and use this to adapt the system?
- Did you also communicate around potential or perceived risks, such as bias?
- Depending on the use case, did you also consider communication and transparency towards other audiences, third parties or the general public?

- Did you make clear what the purpose of the AI system is and who or what may benefit from the product/service?
- Have the usage scenarios for the product been specified and clearly communicated, considering also alternative forms of communication to ensure that it is understandable and appropriate for the addressed user?
- Depending on the use case, did you think about human psychology and potential limitations, such as risk of confusion, confirmation bias or cognitive fatigue?
- Did you clearly communicate characteristics, limitations and potential shortcomings of the AI system:
  - In case of development: to whoever is deploying it into a product or service?
  - In case of deployment: to the end-user or consumer?

❖ Technical robustness and safety

Resilience to attack and security:

- Did you assess potential forms of attack to which the AI system could be vulnerable?
- In particular, did you consider different types and natures of vulnerabilities, such as data pollution, physical infrastructure, cyber-attacks?
- Did you put measures or systems in place to ensure the integrity and resilience of the AI system against potential attacks?
- Did you assess how your system behaves in unexpected situations and environments?
- Did you consider whether or not, and to what degree your system could be dual-use? If so, did you take suitable preventative measures against this case (including for instance not publishing the research or deploying the system)?

Fall-back plan and general safety:

- Did you ensure that your system has a sufficient fall-back plan should it encounter adversarial attacks or other unexpected situations (e.g., technical switching procedures or asking for a human operator before proceeding)?
- Did you consider the level of risk raised by the AI system in this specific use case?
- Did you put any process in place to measure and assess risks and safety?
- Did you provide the necessary information in case of risk for human physical integrity?
- Did you consider an insurance policy to deal with potential damage from the AI system?
- Did you identify the potential safety risks of (other) foreseeable uses of the technology, including accidental or malicious misuse thereof? Is there a plan to mitigate or manage these risks?

- Did you assess whether there is a probable chance that the AI system may cause damage or harm to users or third parties? If so, did you assess the likelihood, potential damage, impacted audience and severity?
- In case there is a risk of the AI system causing damage, did you consider liability and consumer protection rules, and how did you take these into account?
- Did you consider the potential impact or safety risk to the environment or to animals?
- Did your risk analysis consider whether security or network problems (for example cybersecurity hazards) pose safety risks or damage due to unintentional behaviour of the AI system?
- Did you estimate the likely impact of a failure of your AI system that leads to providing wrong results, that leads to your system being unavailable, or to your system providing societally unacceptable results (e.g., discriminatory practices)?
- Did you define thresholds and governance for the above scenarios to trigger alternative/fall-back plans?
- Did you define and test fallback plans?

Accuracy:

- Did you assess what level and definition of accuracy would be required in the context of the AI system and use case?
- Did you assess how accuracy is measured and assured?
- Did you put in place measures to ensure that the data used is comprehensive and up to date?
- Did you put in place measures to assess whether there is a need for additional data, for example to improve accuracy or to eliminate bias?
- Did you assess the harm that would be caused if the AI system makes inaccurate predictions?
- Did you put in place ways to measure whether your system is making an unacceptable number of inaccurate predictions?
- If inaccurate predictions are being made, did you put in place a series of steps to resolve the issue?

Reliability and reproducibility:

- Did you put in place a strategy to monitor and test that the AI system meets the goals, purposes and intended applications?
- Did you test whether any specific contexts or particular conditions need to be taken into account to ensure reproducibility?
- Did you put in place processes or methods for verification to measure and ensure different aspects of reliability and reproducibility?
- Did you put in place processes for describing when an AI system fails in some types of settings?
- Did you clearly document and operationalise these processes for the testing and verification of the reliability of AI systems?

- Did you put in place a mechanisms or communication to assure (end-)users of the reliability of the AI system?

❖ Privacy and data governance

Respect for privacy and data Protection:

- Depending on the use case, did you establish a mechanism that allows others to flag issues related to privacy or data protection issues concerning the AI system's processes or data collection (for training as well as operation) and data processing?
- Did you assess the type and scope of data in your data sets (e.g., whether they contain personal data)?
- Did you consider ways to develop the AI system or train the model without or with minimal use of potentially sensitive or personal data?
- Did you build in mechanisms for notice and control over personal data depending on the use case (such as valid consent and possibility to revoke, when applicable)?
- Did you take measures to enhance privacy, such as via encryption, anonymisation and aggregation?
- Where a Data Privacy Officer (DPO) exists, did you involve this person at an early stage in the process?

Quality and integrity of data:

- Did you align your system with potentially relevant standards (e.g., ISO, IEEE) or widely adopted protocols for your daily data management and governance?
- Did you establish oversight mechanisms for data collection, storage, processing and use?
- Did you assess the extent to which you are in control of the quality of the external data sources used?
- Did you put in place processes to ensure the quality and integrity of your data? Did you consider other processes? How are you verifying that your data sets have not been compromised or hacked?

Access to data:

- What protocols, processes and procedures were followed to manage and ensure proper data governance?
- Did you assess who can access users' data, and under what circumstances?
- Did you ensure that these persons are qualified and required to access the data, and that they have the necessary competences to understand the details of data protection policy?
- Did you ensure an oversight mechanism to log when, where, how, by whom and for what purpose data was accessed?

❖ Diversity, non-discrimination and fairness

Unfair bias avoidance:

- Did you ensure a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design?
- Did you assess and acknowledge the possible limitations stemming from the composition of the used data sets?
- Did you consider diversity and representativeness of users in the data? Did you test for specific populations or problematic use cases?
- Did you research and use available technical tools to improve your understanding of the data, model and performance?
- Did you put in place processes to test and monitor for potential biases during the development, deployment and use phase of the system?
- Depending on the use case, did you ensure a mechanism that allows other to flag issues related to bias, discrimination or poor performance of the AI system?
- Did you consider clear steps and ways of communication regarding how and to whom such issues can be raised?
- Did you consider not only the (end-)users but also other potentially indirectly affected by the AI system?
- Did you assess whether there is any possible decision variability that can occur under the same conditions?
- If so, did you consider what would be the possible causes of this?
- In of variability, did you establish a measurement or assessment mechanism of the potential impact of such variability on fundamental rights?
- Did you ensure an adequate working definition of "fairness" that you apply in designing AI systems?
- Is your definition commonly used? Have you considered other definitions before choosing this one?
- Did you ensure a quantitative analysis or metrics to measure and test the applied definition of fairness?
- Did you establish mechanisms to ensure fairness in your AI systems? Did you consider other potential mechanisms?

Accessibility and universal design:

- Did you ensure that the AI system accommodates a wide range of individual preferences and abilities?
- Did you assess whether the AI system usable by those with special needs or disabilities or those at risk of exclusion? How was this designed into the system and how is it verified?
- Did you ensure that information about the AI system is accessible also to users of assistive technologies?
- Did you involve or consult this community during the development phase of the AI system?

- Did you take into account the impact of your AI system on the potential user audience?
- Is the team involved in building the AI system representative of your target user audience? Is it representative of the wider population, considering also of other groups who might tangentially be impacted?
- Did you assess whether there may be persons or groups who might be disproportionately affected by negative implications?
- Did you get feedback from other teams or groups that represent different backgrounds and experiences?

Stakeholder participation:

- Did you consider a mechanism to include the participation of different stakeholders in the AI system's development and use?
- Did you pave the way for the introduction of the AI system in your organisation by informing and involving impacted workers and their representatives in advance?

❖ Human agency and oversight

Fundamental rights:

- In those use cases where there can potentially be a negative impact on fundamental rights, did you carry out a fundamental rights impact assessment? Did you identify and document potential trade-offs made between the different principals and rights?
- Does the AI system interact with decision-making by human end users (e.g., recommended actions or decisions to take, presenting of options)?
- In those cases, is there a risk that the AI system affects human autonomy by interfering with the end user's decision-making process in an unintended way?
- Did you consider whether the AI system should communicate to users that a decision, content, advice or outcome is the result of an algorithmic decision?
- In case the AI system features a chat bot or conversational system, are the human end users made aware of the fact that they are interacting with a non-human agent?

Human agency:

- In case the AI system is implemented in work and labour processes, did you consider the task allocation between the AI system and human workers for meaningful interactions and appropriate human oversight and control?
- Does the AI System enhance or augment human capabilities?
- Did you take safeguards to prevent overconfidence or overreliance in the AI system in work processes?

Human oversight:

- Did you consider what would be the appropriate level of human control for the particular AI system and use case?
- Can you describe the level of human control or involvement, if applicable? Who is the "human in control" and what are the moments or tools for human intervention?
- Did you put in place mechanisms and measures to ensure such potential human control or oversight, or to ensure that decisions are taken under the overall responsibility of human beings?
- Did you take any measures to enable audit and to remedy issues related to governing AI autonomy?
- In case there is a self-learning or autonomous AI system or use case, did you put in place more specific mechanisms of control and oversight?
- What kind of detection and response mechanisms did you establish to assess whether the something could go wrong?
- Did you ensure a "stop button" or procedure to safely abort an operation where needed? Does this procedure abort the process entirely, in part or delegate control to a human?

❖ Societal and environmental well-being

Sustainable and environmentally friendly AI:

- Did you put in place mechanisms to measure the environmental impact of the AI system's development, deployment and use (e.g., energy used by data centre, type of energy used by the data centres, etc.)?
- Did you ensure measures to reduce the environmental impact of your AI system's life cycle?

Social impact:

In case the AI system directly interacts with humans:

- Did you assess whether the AI system encourages humans to develop attachment and empathy towards the system?
- Did you ensure that the AI system clearly signals that its social interaction is simulated and that is has no capacities of "understanding" and "feeling"?
- Did you ensure that the social impacts of the AI system are well understood? For example, did you assess whether there is a risk of job loss or de-skilling of the workforce? What steps have been taken to counteract such risks?

Society and democracy:

- Did you assess the broader societal impact of the AI system's use beyond the individual (end-)user, such as potentially indirectly affected stakeholders?

❖ Accountability

Auditability:

- Did you put in place mechanisms that facilitate the system's auditability by internal and/or independent actors, such as ensuring traceability and logging of the AI system's processes and outcomes?

Minimising and reporting negative Impact:

- Did you carry out a risk or impact assessment of the AI system which takes into account different stakeholders that are directly and indirectly affected?
- Did you put in place training and education frameworks to develop accountability practices?
- Which workers or branches of the team are involved? Does it go beyond the development phase?
- Do these trainings also teach the potential legal framework applicable to the AI system?
- Did you consider establishing an 'ethical AI review board' or a similar mechanism to discuss overall accountability and ethics practices, including potentially unclear grey areas?
- In addition to internal initiatives or frameworks to oversee ethics and accountability, is there any kind of external guidance or were auditing processes set up as well?
- Are there any processes in place for third parties (e.g., suppliers, consumers, distributions/vendors) or workers to report potential vulnerabilities, risks or biases in the AI system/application?

Documenting trade-offs:

- Did you establish a mechanism to identify relevant interests and values implicated by the AI system and potential trade-offs between them?
- What process do you use to decide on such trade-offs? Did you ensure that the trade-off decision was documented?

Ability to redress:

- Did you establish an adequate set of mechanisms that allows for redress in case of the occurrence of any harm or adverse impact?
- Did you put mechanisms in place both to provide information to (end-)users/third parties about opportunities for redress?

Moreover, the European Commission has developed in April 2021 a new regulation to guarantee fundamental rights and safety on AI environments. The new rule regulates the types of risks in AI solutions, classifying them as unacceptable risk, high risk, limited risk and minimal risk, making true trustworthy AI.

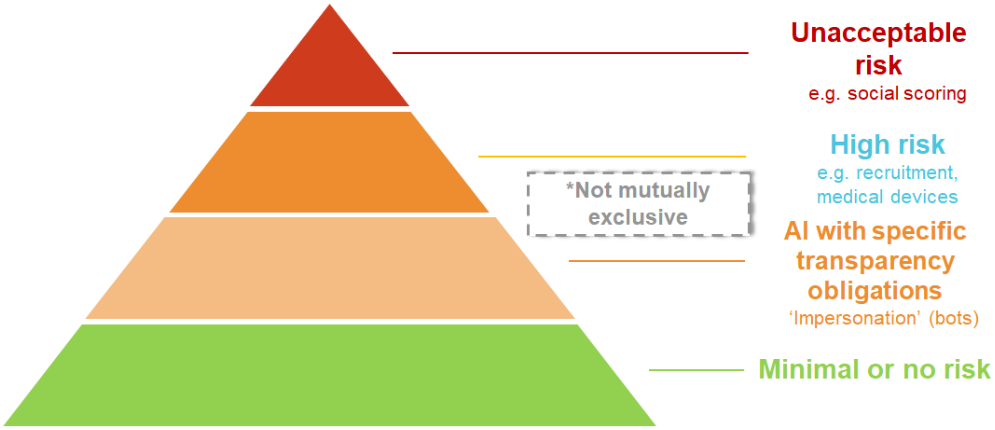


Figure 23: Risk classification according to EC AI framework

- Unacceptable risk: AI environments considered a clear threat to the safety, livelihoods and rights of people will be banned. This category includes AI systems or applications that manipulate human behaviour and systems that allow 'social scoring' by governments.
- High-risk: AI systems identified as high-risk include AI technology used in: Critical infrastructures, educational or vocation training, safety components of products, employment, workers management and access to self-employment, essential private and public services, law enforcement, migration, asylum and border control management, administration of justice and democratic processes.

  Risks in this category have to meet a series of requirements established by the regulatory framework of the European Union in AI in order to be marketed.

  - Adequate risk assessment and mitigation systems;
  - High quality of the datasets;
  - Logging of activity to ensure traceability of results;
  - Detailed documentation;
  - Clear and adequate information;
  - Appropriate human oversight;
  - High level of robustness, security and accuracy.

- Minimal risk: The legal proposal allows the free use of applications such as AI-enabled video games or spam filters. The vast majority of AI systems fall into this category.

Taking into account the types of changes that may occur, the assessment of the changes to avoid dangerous risk considering the new AI regulations released by the EC, a modification approach has been defined by SQS to address possible alterations within an Autonomous Quality solution. This ZDM framework is able to V&V Autonomous Quality solutions across total product lifecycle.

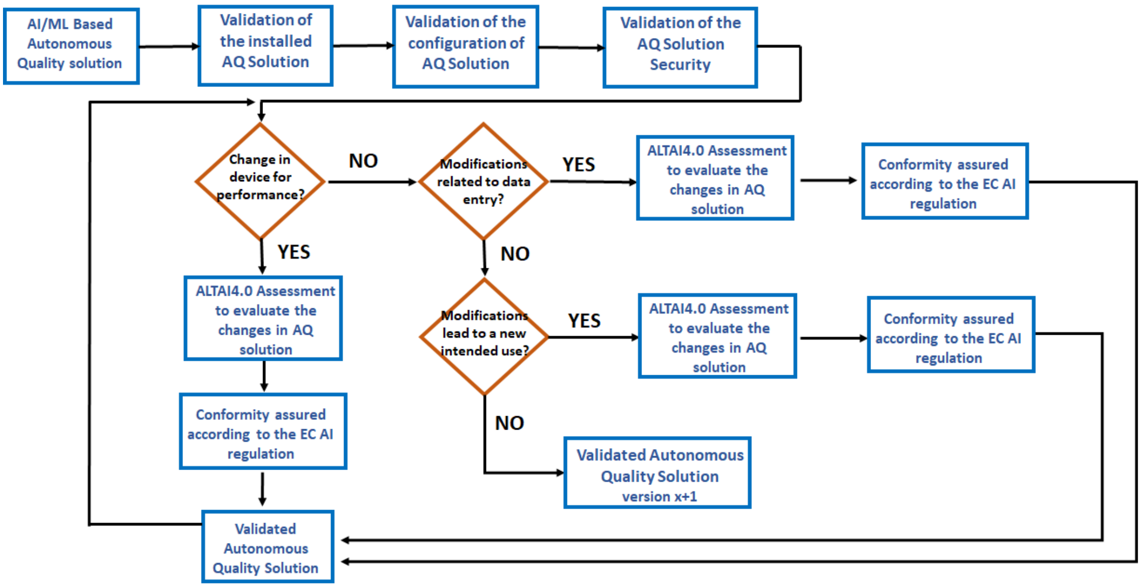


Figure 24: Total product lifecycle approach

4.1.4 Documentation

Link to the Digital Factory Alliance (DFA) website, where QU4LITY solutions will be certified according to the ZDM Validation Framework:

https://digitalfactoryalliance.eu/certification/

4.1.5 Deployment

Link to the Digital Factory Alliance (DFA) website, where QU4LITY solutions will be certified according to the ZDM Validation Framework:

https://digitalfactoryalliance.eu/certification/

Link to the SQS website, more specifically to the Q-Digital Automation section:

https://www.sqs.es/q-digital-automation/

4.1.6 Future Work

SQS will work on the continuous updating of the defined ZDM framework based on the certification needs that may arise in the future and have not been identified at the present time.

5. Conclusions

This deliverable has provided an overview of the enablers for edge computing, which can be deployed directly at the manufacturing machines on the shopfloor, thus at the edge of the network. Additionally, the validation of the edge computing solutions was an important topic within this task. The presented components developed in this task can be divided into the two following categories:

- **Edge solutions** for collecting data and hosting ZDM applications at the edge of the network close to the data coming from the machine. These solutions can host multiple legacy applications and provide data coming direct from the sensors in the machine and feed them back into the actuators from the machines.
- **Q-Digital Automation Framework** which will be able to validate and verify Autonomous Quality solutions whatever the change, guaranteeing at any time the Autonomous Quality solution will work as it should.

The deliverable highlights the functionalities of the different edge solutions developed inside the project and how it can be deployed in a factory setting. It outlines the developments that have taken place specifically during the project and how companies can benefit from these solutions. Additionally, it presents how the different edge solutions are deployed and integrated in their respective pilots and what kind of ZDM applications are being hosted on the edge solutions. The deployment of the edge solutions is being performed in WP7.

The solutions described within this deliverable will be mainly exploited by the individual partners. The solutions will be further developed after the project and new features will be added to support among other ZDM in manufacturing plants, but also for other functionalities like improved data usage, hosting AI at the edge, etc.

Concluding it can be stated that the results developed within Task 3.4 and presented in this deliverable provide excellent solutions for deploying in factories and machines for hosting various ZDM applications. The components developed and extended within this work can be used in various situations for performing fast data handling at the edge and directly at the machine, supporting machine learning functionalities and even controlling the machines. The deployment of the solutions at their respective pilots have shown the benefits and the added value to the manufacturing process. The partners will continue to further develop their respective solutions, thereby significantly contributing the future manufacturing solutions.

List of figures

List of tables

List of Abbreviations

Acronym	Abbreviation
AI	Artificial Intelligence
ALTAI4.0	Assessment List for Trustworthy Artificial Intelligence 4.0
API	Application Programming Interface
CNC	Computerized Numerical Control
CSV	Comma-Separated Values
DB	Database
DFA	Digital Factory Alliance
DMC	Data Matrix Code
DPO	Data Privacy Officer
EC	European Commission
HIC	Human-in-Command
HITL	Human-in-the-Loop
HOTL	Human-on-the-Loop
I/O	Input/Output
IDS	Industrial Data Space
IoT	Internet of Things
IPC	Industrial PC
ISO	International Organization for Standardization
IT	Information Technology
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
OPC UA	Open Platform Communications Unified Architecture
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controller
QA	Quality Assurance
QU4LITY-RA	QU4LITY Reference Architecture
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RGPD	Règlement Général pour La Protection des Données (French: General Regulations for Data Protection)
RTE	Runtime Environment
SSH	Secure Shell
SUT	Specifications and Usage Testing
TCP	Tool Centre Point
TPLC	Total Product Life Cycle
UDP	User Datagram Protocol
UI	User Interface
UMATI	Universal Machine Technology Interface
URL	Uniform Resource Locator
V&V	Verification and Validation
VNC	Virtual Network Computing
VPN	Virtual Private Network
WP	Work Package
ZDM	Zero Defect Manufacturing
ZeroMQ	Zero Message Queue

Partners: