D4.3b AUTOWARE Open CPPS ecosystem development

Document Owner	TTT		
Contributors	SFKL, FhG, CNR, UMH, imec, Robovision, JSI		
Reviewers	UMH		
Dissemination level	Public	**Dissemination nature**	Report
Date	14/02/2019	**Version**	V1.0

European Commission

Version History

Nr.	Date	Author (Organization)	Description
0.1	15/11/2018	TTT	Deliverable structure and ToC
0.2	22/11/2018	TTT	Configuration Open Platform, Network configuration enabler
0.3	03/12/2018	SFKL, TTT	Usability Enabler descriptions
0.4	06/12/2018	FhG, CNR, UMH	Usability Enabler descriptions
0.5	07/12/2018	TTT	Executive Summary, Introduction
0.6	13/12/2018	Imec, Robovision	Usability Enabler description
0.7	17/12/2018	JSI	Usability Enabler description
0.7R	15/01/2019	UMH	Internal review
1.0	17/01/2019	TTT	Finalization based on review
1.0R	14/02/2019	SQS, INNO	Certification enabler description Final version reviewed

Table of Contents

List of Figures

List of Tables

Acronyms

ADOMe	Active Digital Object Memories
AMQP	Advanced Message Queuing Protocol
AP	Access Point
AR	Augmented Reality
CAD	Computer-Aided Design
CN	Communication Node
CPPS	Cyber-Physical Production System
DMP	Dynamic Movement Primitive
ERP	Enterprise Resource Planning
GPU	Graphical Processing Unit
HPC	High Performance Computing
I4.0	Industry 4.0
IEEE	Institute of Electrical and Electronic Engineers
M2M	Machine to Machine
MES	Manufacturing Execution System
MQTT	Message Queuing Telemetry Transport
OPC	Open Platform Communication
OPC UA	Open Platform Communication Unified Architecture
PL	Performance Level
PLr	Performance Level risk
PLM	Product Lifecycle Management
RA	Reference Architecture
RFID	Radio-Frequency Identification
ROS	Robot Operating System
SEV	Secure Encrypted Virtualization
SGX	Software Guard Extensions
SLRT	Sequential Likelihood Ratio Test

SME	Small and Medium Enterprise
TPU	TensorFlow Processing Unit
VR	Virtual Reality
WP	Work Package

Executive Summary

This public deliverable (D4.5) presents the continuation of the development related to the AUTOWARE Open CPPS ecosystem, based on the results from the other (technical) work packages (WP1-WP3). It is the final deliverable of the work performed in Task 4.2 "Definition and Specification of Open Platform Configuration and usability enablers". As the name of the task already states, the focus in this task is on the definition and specification of the open platform. The predecessor deliverables D4.2 and D4.3 introduced and specified the open platform that is being applied inside the project, namely the edge node platform introduced by TTTech. As the specification of the open platform has been provided in the previous deliverables and this specification still is valid, this deliverable will not go into this aspect anymore.

The focus of this deliverable is more targeted towards the second aspect in the title of the task, namely the usability enablers. In the AUTOWARE Framework, a collection of usability enablers has been defined as components/tools that will enable potential users of the tools, be it end users, system integrators or software developers, to easily apply the developed technical enablers to their daily work. In other words, the usability enablers ensure that the technical enablers are actually applicable, without causing too much effort/training to apply the developed technical enablers and thereby support their introduction to the market.

Finally, verification, validation and certification enablers will be introduced. Developing technical and usability enablers and bringing them to the market is not a straightforward task, and companies are more tended to introduce new technologies that have officially been validated and certified. Introducing new technologies into the production process is always a risk, especially for small and medium enterprises (SME). Verification, validation and certification enablers can support this process and reduce the barriers for introducing technologies to the market.

Keywords

Open CPPS ecosystem, open platform, fog node, usability enablers, verification, validation, certification

1. Introduction

1.1 Purpose and Scope

The AUTOWARE Open CPPS (Cyber-Physical Production System) ecosystem has already been introduced in deliverable D4.2 (Reference Architecture for AUTOWARE Open CPPS Ecosystem) and the actual open CPPS platform that will be used for the implementation of the pilots. Another aspect that is targeted in Work Package 4 (AUTOWARE Open CPPS ecosystem) and especially in Task 4.2 (Definition and Specification of Open Platform Configuration and usability enablers) is the definition of the usability enablers.

Usability enablers are closely related to the technical enablers developed in WP2 and WP3 and will guarantee the usability of the technical enablers, making them easy to access and to operate. It has quite often been experienced that new technologies that are made available for SMEs lack usability, thus making them useless for these companies. The goal of AUTOWARE is not only to develop new technical enablers giving SMEs tools to introduce the Industry 4.0, but also to easy the use of these tools and make new and unexperienced employees use these tools in an intuitive way.

Additionally, this deliverable will provide an overview of verification, validation and certification enablers. These enablers will evaluate and certify the applicability of the developed technical and usability enablers, fulfilling the requirements of the AUTOWARE approach.

This deliverable will provide a high-level description of the available usability enablers developed inside the project and how they will be applied inside the different neutral or industrial pilots.

1.2 Contributions to other WPs and deliverables and document structure

This deliverable gathers contributions from the technical Work Packages 2-4. WP2 and WP3 provide technical enablers, but to use these technical enablers, so called usability enablers are required to ease the use of these technical enablers. WP2 focuses on the usability enablers for communication (wireless and wired) and data management, whereas WP3 will provide usability enablers in the area of machine learning, dual reality, robot programming and active digital object memories. Additionally, WP4 focuses more on the open CPPS ecosystem, providing the open CPPS platform (i.e. the fog node architecture) and verification, validation and certification methods applicable for the AUTOWARE technologies.

This deliverable has close relations with all deliverables from WP2-4, where the different technical enablers, open CPPS platform and verification and validation enablers are described. Within this document, you will find multiple references to other deliverables.

This deliverable is built up as follows:

- Chapter 2 gives an overview of the version of the open CPPS platform that is being applied inside the AUTOWARE project. This is based on a fog node architecture together with its configuration approach, which is the usability enabler for the open CPPS platform.
- Chapter 3 provides an overview of the other usability enablers developed inside the AUTOWARE project. It will provide a high-level overview of the functionality of the enablers and will shortly describe in which neutral or industrial pilot this enablers is applied.
- Chapter 0 presents the verification, validation and certification enablers that are developed and applied inside the project.
- Finally, chapter 5 concludes this deliverable.

1.3 Target Audience

The deliverable is intended for potential end-users of the AUTOWARE platform and ecosystem. This deliverable will provide a high-level overview of the available usability enablers developed inside the project and their functionality. Additionally, system integrators and technology developers can benefit from the description on what kind of features are available and can be integrated in the final system.

2. AUTOWARE Open CPPS Ecosystem

The AUTOWARE project has defined an updated Framework and Reference Architecture in deliverable D1.3b (see Figure 1). The Framework captures the overall concept of the AUTOWARE Project, thereby also encapsulating the AUTOWARE Open CPPS Ecosystem. As defined in the previous deliverable in work package 4 (deliverable D4.2 and D4.3), the AUTOWARE Open CPPS Ecosystem is identified as the CPPS platform that will be used within the project at the implementation of different industrial and neutral facilities.

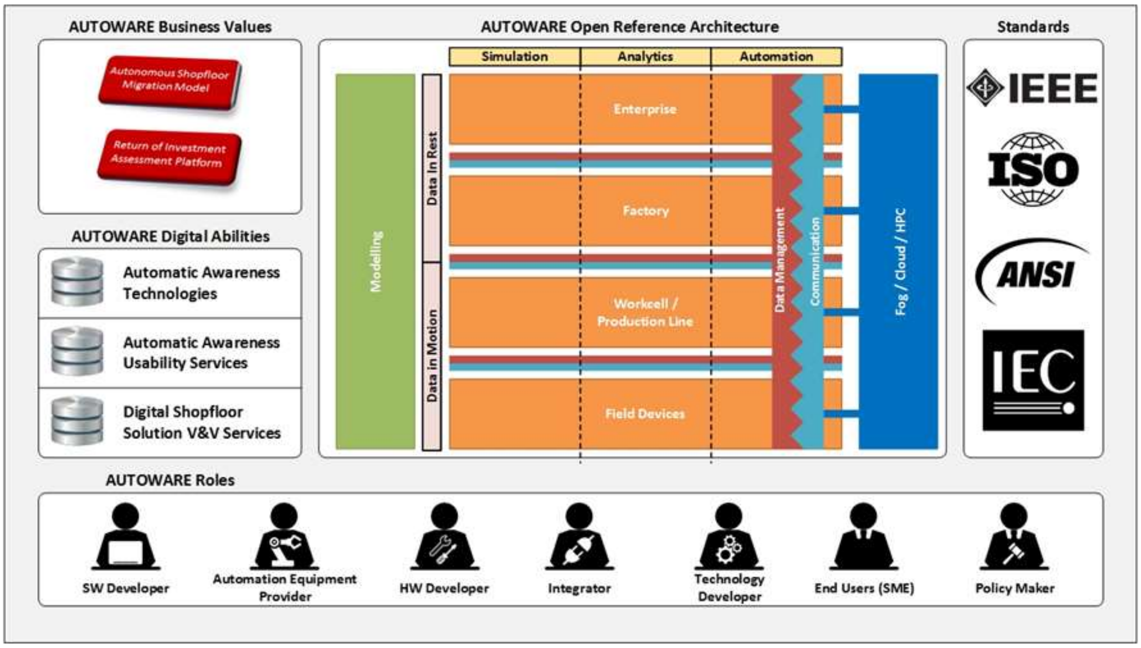


Figure 1: Updated AUTOWARE Framework [1]

The open CPPS platform is based on a fog/edge node architecture, which is positioned in the AUTOWARE Open Reference Architecture (RA), on the right side of the RA, combined with the Cloud and HPC (High Performance Computing) concept. The open CPPS platform will enable the integration of processing at the edge of the network, instead of performing all the calculations in the cloud, thereby enabling a more direct access to the machine, lower latency times and the possibility of performing real-time control and communication on machine level.

Another important concept of the AUTOWARE Framework, and thereby also targeting the AUTOWARE Open CPPS ecosystem, are the AUTOWARE Usability Enablers, or as they are called in the Framework, AUTOWARE Awareness Usability Services. The Usability Enablers are closely related to the Technical Enablers (Automatic Awareness Technologies in the Framework), where the Technical Enablers focus on the actual developed technologies (e.g. robotic systems, smart machines, (wired and wireless) communication, Augmented Virtuality) and the Usability Enablers focus on how the technology can be used in an intuitive manner (i.e. tools, user interface, interaction possibilities, etc.).

Finally, the ecosystem will provide Certification, Verification & Validation enablers, that will provide services that will verify and validate the functionality of the technical enablers, making them official available for interesting companies.

2.1 Open Platform Configuration

The Open Platform architecture has been introduced and described in the previous deliverable D4.3a. Since this deliverable, no updates in the platform architecture have taken place and the development is continuously striving forward. Therefore, this deliverable will not provide any additional information on the status of the open platform architecture, as the information would be similar to the one presented in deliverable D4.3a.

The (intuitive) configuration of the AUTOWARE Open Platform is defined as an important usability enabler, targeting different roles within the AUTOWARE Framework. Figure 2 provides a schematic overview of how the System Manager works in a centralized way for controlling fog devices and deploying applications to the distributed devices.

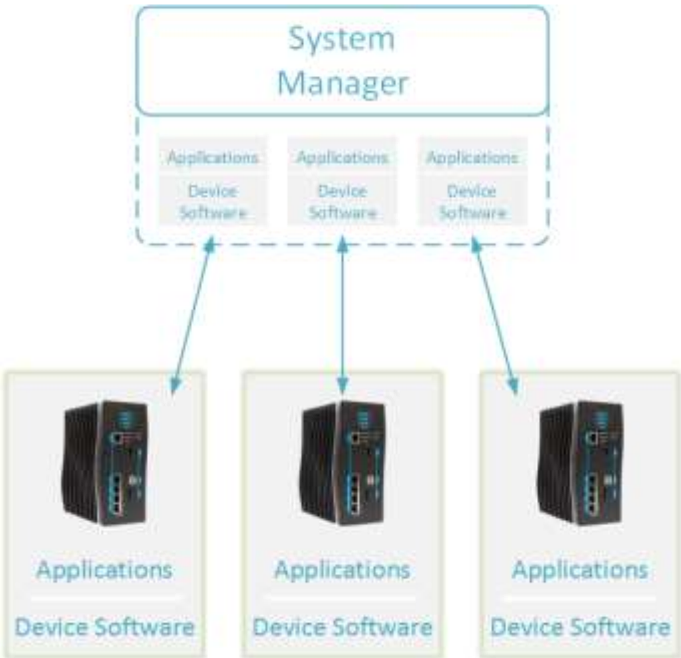


Figure 2: Open Platform Centralized Management

The System Manager is a centralized management system for updating device software and deploying applications to the fog devices. It can either be hosted remotely in the cloud, or locally on a company internal server or even on one of the deployed fog devices. The System Manager is intended to be used for a collection of different management tasks that are required to have a system working properly.

Figure 3 provides an overview of the System Manager. With this overview depicted in the figure, you can have a world-wide overview of where your fog devices are deployed, which are up and running and where there are currently problems.

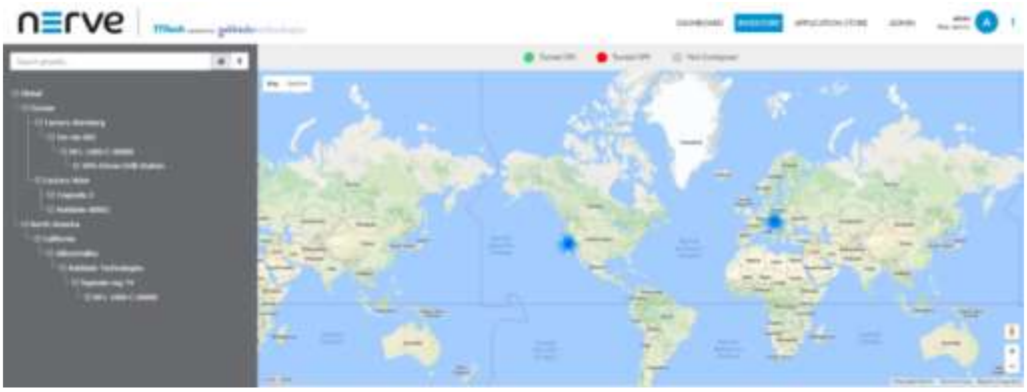


Figure 3: System Manager: Overview of deployed fog nodes

Figure 4 provides the view of a specific fog device selected inside the System Manager. This view provides you a general overview of the functionality of the selected fog device. This view enables the user to configure the selected fog device. A major advantage for companies is that they don't have to be present at the actual facility where the fog device is deployed. The configuration of the device can be performed from their own premises and the device can be deployed somewhere completely else. Additionally, there is an app store available, where you can upload your applications (e.g. docker, windows applications, etc.) and you can select, in a centralized manner, where you want to deploy the applications. One of the major advantages here also is, that the fog device supports virtual machines (e.g. Linux, Windows), so the legacy applications that are currently running in the factory, can be deployed to the fog device and no re-programing is required.

The deployment of applications to the devices can be done simultaneously to multiple devices, thereby reducing time and assuring that the same application is running on various devices (consistency) and thus in various factories.

Figure 4: System Manager: fog node information

2.2 Open Platform Applications in AUTOWARE

2.2.1 SmartFactoryKL – Neutral Cognitive Digital Automation Process Experimentation Infrastructure

In the neutral test factory SmartFactoryKL, the fog node is attached in the edge layer. This is integrated with the infrastructure of the individual production modules, more precisely with the industrial M2M (Machine-to-Machine) communication protocol according to the OPC (Open Platform Communication) specification, with which the production modules communicate with the higher-level MES (Manufacturing Execution System) system. These transmitted messages can be evaluated and processed in the fog node. The basic arrangement of the production modules with the fog node can be seen in Figure 5.

Figure 5: Fog node in the SmartFactoryKL production line

The fog node has several virtual machines that are used to realize the different applications scenarios in the SmartFactoryKL.

In the first case, Tomcat is installed on the fog node server running the visualization software DyVisual. The DyVisual software represents a real-time capable visualization of the production plant (a "digital twin" of the plant) and can be accessed via compatible web browsers at any time and from any location. This makes it possible to obtain information remotely about the current status of the system. The implementation of the server close to the machine on the edge device makes it possible to update it at any time by means of current information about the OPC UA (Open Platform Communication Unified Architecture) messages, so that the web model of the plant can be animated in almost real time. This Tomcat server runs on the operating system Windows 10 with 64bit.

In addition to the visualization of the system, the operator is also supported by an augmented reality solution. A data goggle (in this case a Microsoft Hololens) is used to provide the operator with an insight into the internal processes of the modules without having to actively shut them down and open them. This, however, requires an overlay of the real production modules with their digital 3D model. Real-time data from the modules are also used here to enrich the Augmented Reality 3D representation with further information. Since visualization with the help of data glasses are very susceptible to latencies (the 3D representation must always be compared with the viewing direction and angle of the viewer, which can change very quickly), the communication of the data with the glasses must take place as quickly as possible. A software on the fog node is used for this purpose, which records the OPC UA messages from the modules, processes them and transmits them to the data glasses via a binary communication protocol (such as MQTT - Message Queuing Telemetry Transport - or AMQP - Advanced Message Queuing Protocol -).

Another use case of the fog node results from the application of the Active Product Memory. This communicates via binary communication protocols with a "Trac 'n Trace" software, which records current information from the product memory, compares it with the information stored in the server (or ERP - Enterprise Resource Planning - system) and updates it according to the level of information. It includes all the information transmitted by the production modules via OPC-UA (current operating status, machining process, consumption data), the information transmitted via the Trac 'n Trace software from the active digital product memories (identification of the respective product, localization information, pending machining processes, already executed production processes) and information from the ERP system (change in the prioritization of an existing order, new orders received, discontinuation of a product due to quality problems) in order to determine an optimum sequence. Based on this algorithm executed on the fog node, information is transmitted to the active digital product memories about when, and where, the sequence in the flow chain must change. Thus, the product memories automatically reorganize themselves with the help of the fog node.

Furthermore, highly digitized production facilities, such as the SmartFactoryKL, are highly susceptible to damage caused by malicious intruders into the network. Such intruders or malicious software (computer viruses) must be detected in time and removed from the system. As the fog node is an important interface in the plant for the communication between the modules, the MES and ERP system and the product memories, it is the optimal place for monitoring the network communication. For this purpose, the security software "Red Border" is installed on a virtual machine, which examines the traffic generated in the network. This traffic is checked for anomalies that could indicate malicious software or attackers. The fog node thus plays an important role in the security of the infrastructure for digitized production facilities.

2.2.2 Tekniker – Neutral Experimentation Infrastructure for Intelligent Automation Applications for Robotic Industrial Scenarios

For the integration of the open platform in the Tekniker pilot, partners UMH, CNR, Tekniker and TTT are still in discussion on how to integrate all the available components. The aim is to use the communication technologies from WP2 (wired and wireless) and data management into the dual-arm robot and mobile robot scenario.

The potential solution that is being studied is presented in Figure 6. The open CPPS platform (i.e. fog node) will be integrated as central station, where the configuration of the open platform will be performed with the usability enablers for programming and controlling the fog node. The node will act as central point, where the different applications (e.g. data management) will be hosted on. The robot controller and available access points (AP) will be connected to the fog node and enable communication between the different components in the production cell.

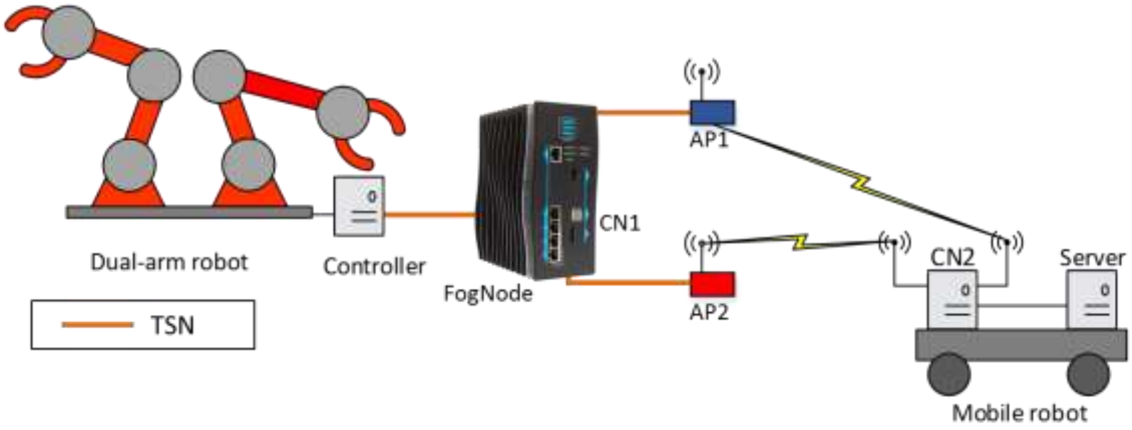


Figure 6: Potential integration of fog node in Tekniker pilot

As mentioned, this concept is still under development, as this approach was not foreseen in the first phase of the project and is an initiative of the WP2 partners (TTT, CNR and UMH) in cooperation with Tekniker. The aim is to establish an integrated solution until the end of the project.

3. Usability Enablers

In addition to technology enablers (i.e. innovative technologies that can increase/improve the production capacity of companies), AUTOWARE also focuses on so called usability enablers, which are approaches/concepts or interaction modalities to improve the applicability of the developed technologies.

The before described centralized system manager is also an important usability enabler, focusing on the open CPPS platform. The following subsections will provide an overview of the available usability enablers inside the AUTOWARE project. It will contain a short description of the enablers, with a reference to the technical enablers which it supports. Finally, it will provide a reference to the neutral and/or industrial use case where the enablers are being applied.

3.1 (Re-)configuration tool for network scheduling

The configuration of a (deterministic) communication network is always a challenging topic, and creating the actual schedule for the sending of the messages over the network is always a challenge.

A Deterministic Ethernet network configuration and scheduling tool is under development by TTT that will support and alleviate the end user/system integrator in defining the network and schedule requirements for the defined and deployed network. The tool is a browser-based, user-friendly software tool that gives the user the possibility to intuitively create network topologies with a selection of pre-defined network components (i.e. switches, end systems, etc.). The tool automatically generates network schedules based on the parameters of network components and the connection between the different components. Schedules are calculated and generated with just one click via our own-developed built-in scheduling engine [3].

For the topology modelling of the network structure, there are two possibilities to model it:

- **Graphical modelling:** The graphical view is ideal for modelling small and medium sized network topologies. New components can be added by dragging and dropping them into the topology. Data streams can also be represented as logical connections between components.
- **Table-based modelling:** The table editor is designed for modelling large network topologies and mass editing. Components, data streams and other parameters (e.g. timing) can be inserted into tables and viewed in the graphical mode.

The configuration of a network can be depicted in two different formats:

- **Physical Configuration:** The physical configuration depicts the actual real-life, physical structure of the network and shows which device is connected to which other device. This doesn't show yet which device is communicating with which device. A physical configuration of a network is depicted in Figure 7.

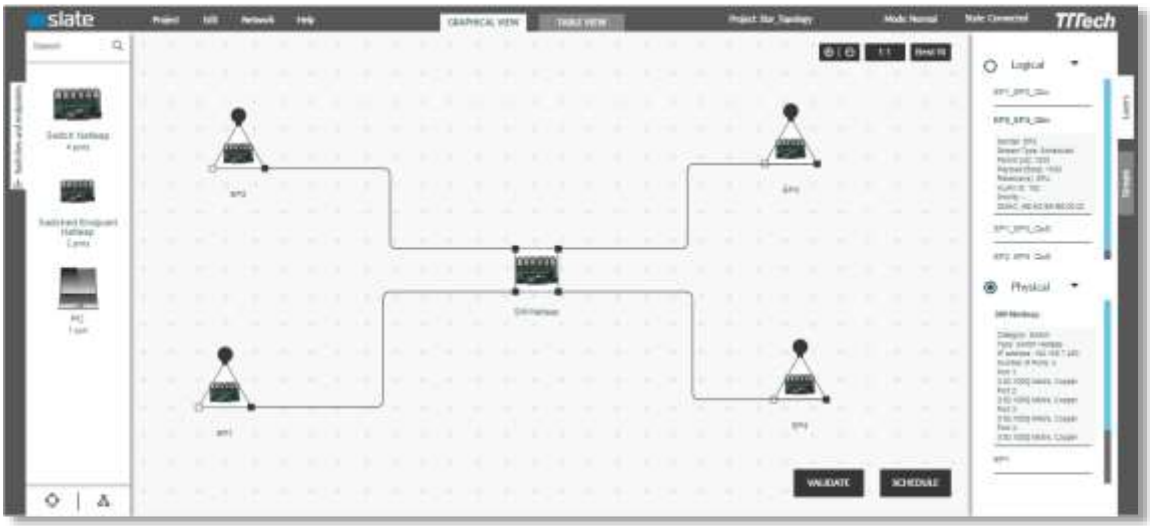


Figure 7: Physical configuration of a network

- **Logical Configuration:** The logical configuration view depicts the actual connection between devices, showing which devices are communicating with each other. Figure 8 shows the logical links within a network.

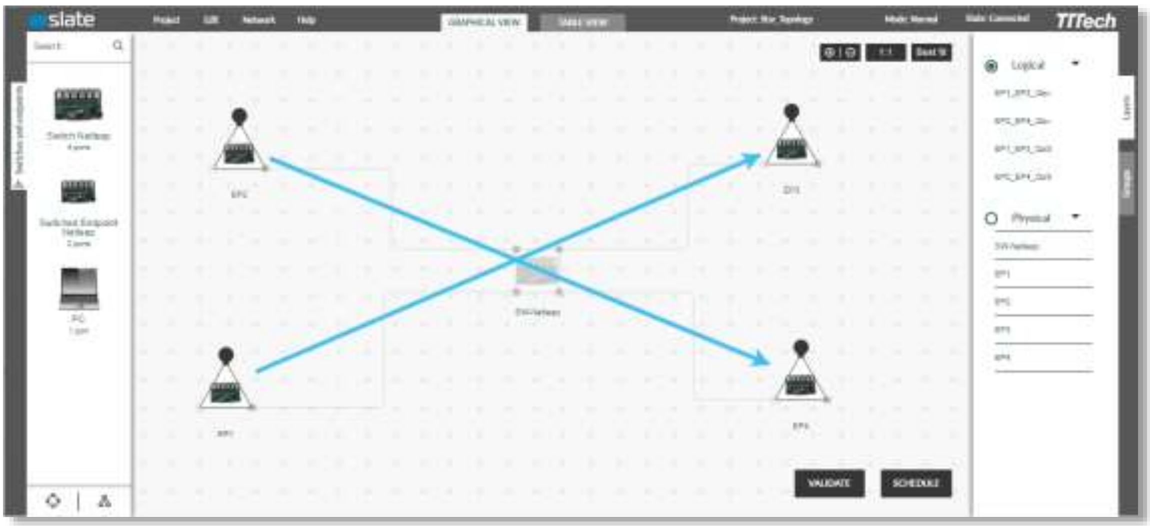


Figure 8: Logical configuration of a network

After modelling the complete network configuration, the information about the devices, the message information (i.e. priority) can be included in the network description. After finalizing the total network, the tool automatically generates a communication schedule for the defined network (see Figure 9).

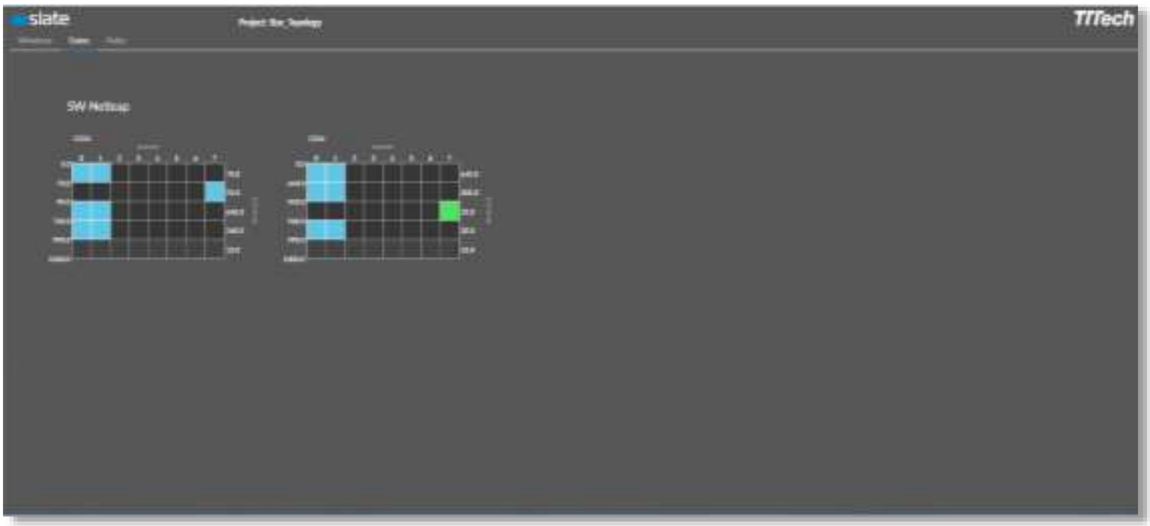


Figure 9: Schedule Visualization

More detailed information regarding this usability enabler for configuring communication network will be provided in the updated deliverable D2.2, which is due in Month 30.

Use Case Applicability

The configuration tool for network scheduling will be applied in the following use cases:

- *SmartFactory^KL – Neutral cognitive digital automation process experimentation infrastructure:* A fog device will be integrated in the SFKL neutral facility and the tool will be applied to schedule the communication within the application that will be deployed inside the fog device.
- *Tekniker – Neutral experimentation infrastructure for intelligent automation application for robotic industrial scenarios:* The partners from WP2 are, at the moment of writing, looking for possibilities to integrate the technologies from the respective work package (i.e. deterministic communication, wireless communication and smart data distribution) and apply the integrated solutions in the robotic work cell.

3.2 Smart Data Distribution

The Smart Data Distribution enabler (introduced in deliverable D2.4) is a core component in the AUTOWARE communications and data management framework. It implements the logic of a control plane for cognitive data distribution across all communication layers of AUTOWARE architecture, it is based on the available communication technologies and it is supporting the needs of the higher-level services and applications. The main Data Management functions provided by the Smart Data Distribution enabler are depicted in Figure 10 in orange colour.

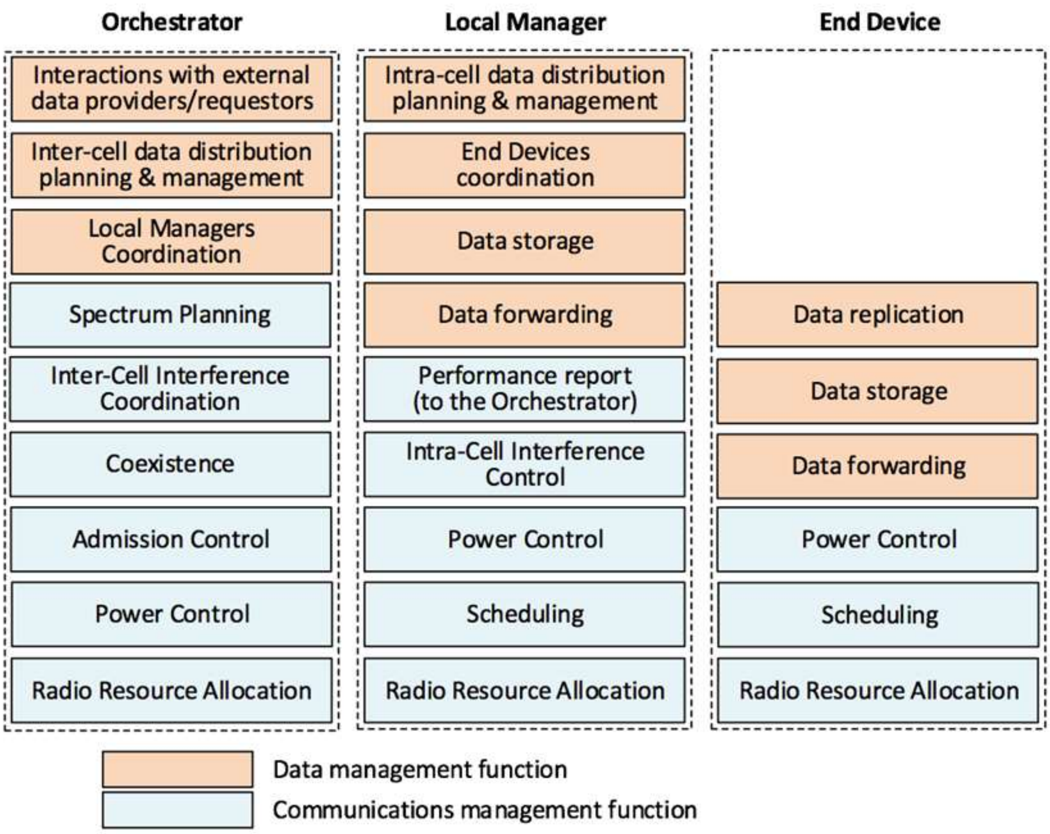


Figure 10: Data Management functions (in orange colour)

The AUTOWARE Smart Data Distribution enabler is decentralized, dynamic and hierarchical, so as to support cooperation with cloud-based service provisioning and communication technologies. More specifically, it provides decentralized data distribution among the various nodes of the AUTOWARE ecosystem. This decentralization is targeting the efficient management of massive data generation and consumption and the exploitation of resources available locally at individual nodes. Then, it copes with dynamically changing network parameters by employing adaptive data placement and replication techniques. Finally, it provides a hierarchical data management, by employing a mix of centralized and decentralized control processes and a hierarchy of data managers.

Use Case Applicability

The Smart Data Distribution enablers will be demonstrated at the IK4-Tekniker industrial environment. A typical scenario at IK4-Tekniker is shown in Figure 11. A mobile robot is responsible for fetching objects to a robotic bi-manipulator. The objects are located at a set of shelves, where a human operator is responsible for manually loading the objects on the mobile robot. Both the robot and the operator are aware of which object is currently needed at the bi-manipulator, as there is a centralized wireless or wired communication infrastructure, coordinated by a central controller and the data can be sent and received through the communication links. However, due to the harsh conditions in several industrial environments, it is not unusual for the main centralized operational network to go offline, for a variety of reasons. Where there is a situation like this in the current scenario, the mobile robot and human operator cannot be aware of which object is currently needed at the bi-manipulator, which in turn results in a failure of the production process.

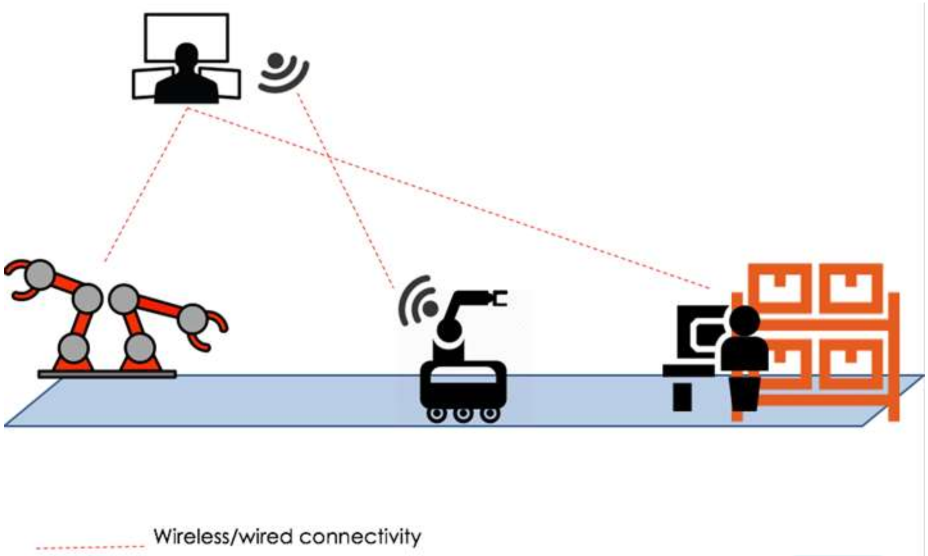


Figure 11: Centralized network functional

In order to address this problem, the Smart Data Distribution approach is applied. More specifically, we employed a secondary, lightweight data distribution layer and implemented it by using small, low-cost wireless sensor motes. The proof of concept was showcased by placing three motes in the network as shown in Figure 12, one on the bi-manipulator, one on the mobile robot and one on the set of shelves. The motes used were IEEE 802.15.4 enabled, a fact that renders them compatible with typical industrial networking protocols, such as IEEE 802.15.4e and WirelessHART. This demonstration is proving that the Smart Data Distribution enabler can achieve high fault tolerance and reliability with low-cost.

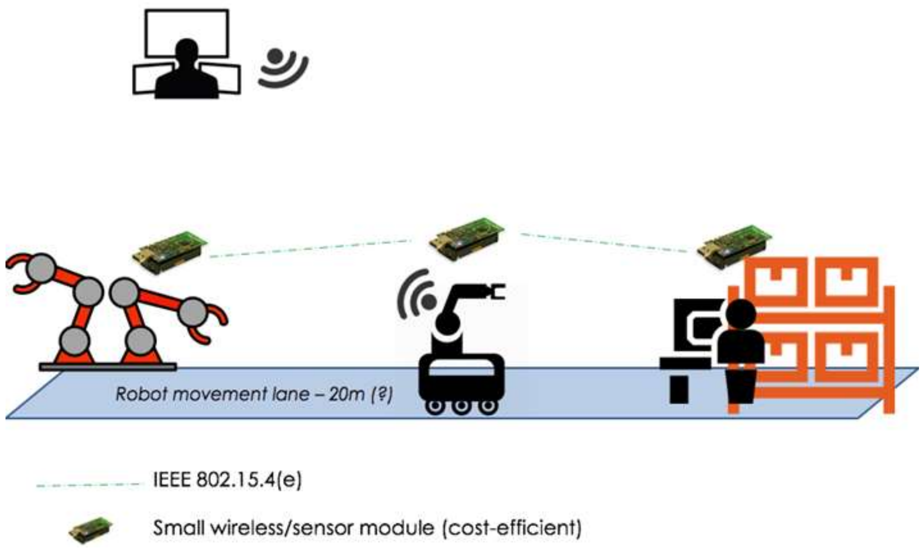


Figure 12: Centralized network, not functional

3.3 Wireless Communication

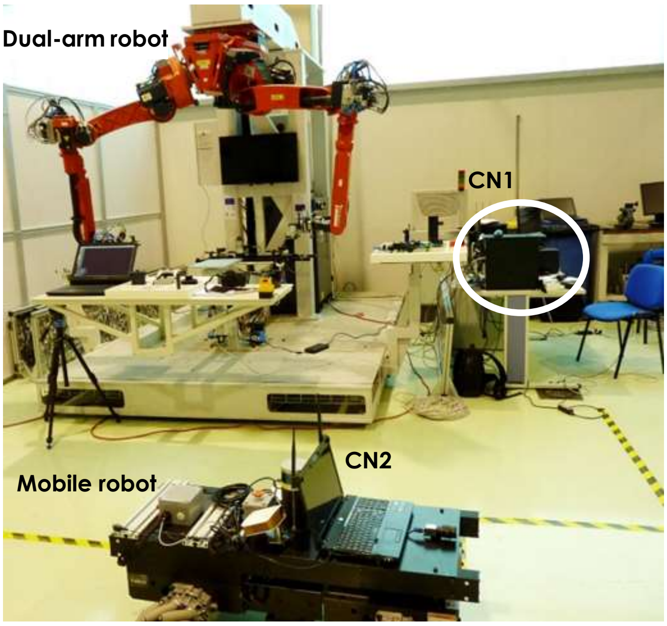
UMH has developed a wireless communication solution to provide reliable industrial wireless communications to support mobile industrial applications. This wireless communication solution is implemented in communication nodes (CNs) that are integrated in the entities/devices that want to communicate. The CNs establish two independent wireless links between the two entities/devices that want to communicate. Data packets are sent over both wireless links increasing the reliability of the communication and decreasing the latency experienced in the end-to-end communication. This wireless communication solution allows two different operation modes:

1. The first one aims at exploiting diversity to ensure a resilient, high reliable and low latency industrial wireless communication. In this case, the CNs establish the two wireless links, and data is sent through the link with the best estimated quality at each time.
2. The second operation mode exploits redundancy. In this case, the CN implemented in the transmitter side sends duplicated data through both wireless links simultaneously. The CN in the receiver side processes first data packets received, and discards duplicated data.

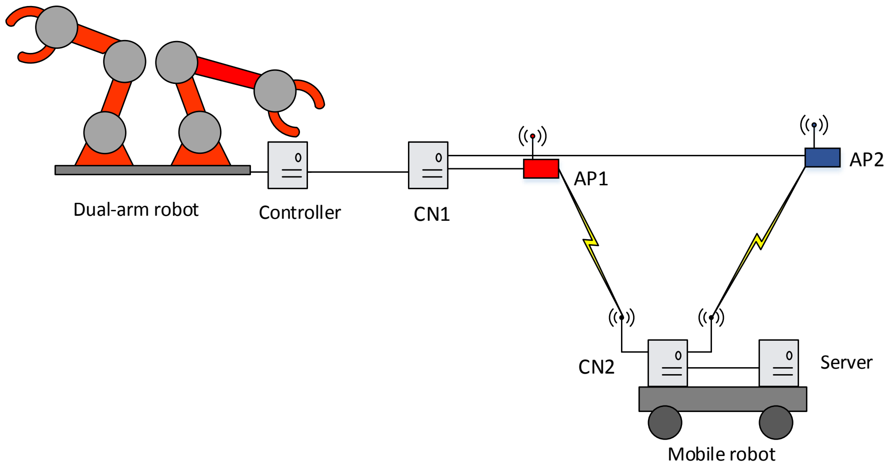
The current implementation of the wireless communication solution uses IEEE 802.11 or WiFi for the wireless links. It is important to highlight that this solution is not restricted to this wireless technology, and others could be implemented. The CNs are also ready to integrate heterogeneous wireless technologies. Additional information can be found in deliverable D2.3a.

Use Case Applicability

The UMH wireless solution has been integrated into the Tekniker neutral experimental infrastructure for intelligent automation applications for robotic industrial scenarios. This facility is a standalone workcell deployed in an industrial shopfloor. It includes a dual-arm robot, a tool changer, interaction devices, and multiple sensors for safety and interaction. Tekniker aims at incorporating into the neutral facility a mobile robotic platform that will act as a component supplier for the dual-arm robot. To ensure coordination and interoperability of the dual-arm robot and the mobile robot, a highly reliable communication between both robots is required. To this end, the UMH CNs have been implemented in the dual-arm robot and the mobile robot. Figure 13 shows the Tekniker neutral experimentation facility. In this picture, it is possible to see the developed CNs (CN1 and CN2) integrated with the mobile robot and the dual robot controller.



a) Tekniker neutral experimentation facility



b) Schematic representation

Figure 13: Reliable wireless communication solution integrated in the Tekniker neutral experimentation infrastructure for intelligent automation applications

The above figure illustrates the wireless solution developed by UMH applied to provide reliable wireless communications between the dual-arm robot and the mobile robot. In this case, both CNs communicate through two APs located at two different locations in the plant. The conducted experiments carried out in the Tekniker facilities have shown that this solution can help overcome some of the limitations traditionally affecting wireless communication in harsh industrial environments (e.g. link outages), and improve the reliability and latency of industrial wireless communications.

3.4 Active Digital Object Memories

The Active Product Memory services as an extension of the common product memory used in SmartFactory. This consists of an RFID chip attached to the test product (a business card holder) as shown in Figure 14.

Figure 14: Product with product memory

This product memory stores all the information required to manufacture this individual product when an order is received. In the further course of production, RFID readers/writers are attached to the processing stations, which are divided into production modules in the SmartFactory. They read the RFID chip of the product and check which production step they have to carry out and whether they are capable of doing so. Once the associated machining process has been completed, this is recorded in the locally stored product memory of the associated product. In this way, the product independently finds its way through the production process. Missing or superfluous processing steps can therefore not happen. Likewise, no information can be lost or incorrect processes carried out on the product, if, for example, the sequence of the products on the assembly line is changed manually in the event of a defect.

However, this form of product memory is purely passive in nature. The products themselves are not able to communicate with a higher-level system, but are dependent on the RFID readers of the processing modules. Since the production modules are also only able to process the product read out in each case, a superordinate, automatic coordination between the products is not possible. This would become necessary, for example, if the prioritization of the order were to be changed. Using a "priority" tag, the products would have to be able to change their processing sequence in the production modules so that urgent orders are processed first. In order to enable such communication with each other and with the higher-level system, the product memory was extended by an active component in the workpiece carrier, as can be seen in Figure 15.

Figure 15: Prototype of the Active Product Memory (ADOMe)

The components of the Extended Active Product Memory thus enable an ontology to be stored on the product and to communicate with it at any time via the AMQP binary network protocol.

Use Case Applicability

In the SmartFactory, different use cases for the Active Product Memory are tested. In the first case, the sequencing of the processing sequence is defined for an incoming order, the products are described and production is started. After a fixed time T, however, a product is prioritized which must be manufactured as quickly as possible. With the help of the active product memory, the products in production must be reorganized accordingly so that on the one hand the lead time of the prioritized product is minimized and on the other hand, the lead times of the remaining products are not neglected. This is done using an algorithm that permanently monitors the production sequence in the edge layer and communicates with the products via the active product memory.

In the second use case, a defect is discovered in a module already in production that affects the manufacturing quality. The active product memory can be used to automatically check which product was processed by this production module in the corresponding period of time. In the event that the product has been processed by the faulty module, it is automatically reorganized and controls the next processing station, the manual workstation for quality control. The aim is to detect defective products as early as possible and to remove them from the process in order to avoid further waste (unnecessarily executed machining processes for a defective product).

3.5 ROS-based Cognitive Planning & Control Services for Reconfigurable Robot Workcells

JSI instantiated the AUTOWARE architecture for the example of the CPPSs involving robots. We defined a control architecture with special emphasis on functional levels from supervision down to hard real-time control, which is needed to sense and control the shop floor devices as robots, machines and other equipment that is physically executing the production processes. At the same time, we defined a connection layer that enables connection of the production cell control to the external edge/fog and cloud, where planning, MES and ERP type functionalities are typically implemented.

The main bonding component is ROS (Robot Operating System), an open source middleware containing a set of tools and libraries. The main functionalities ROS provides are unified message passing between processes and hardware abstraction, so that processes can run on a single or more computers. We conceived and developed a number of enablers that execute functionalities for robot based CPPSs. We describe these in the following sections. Modules implementing these enablers can be included into any application based on the ROS core.

Real-time and robot abstraction enabler. We have developed an enabler that solves two issues:

- ROS does not provide hard real-time, necessary for low level robot control, especially for more intelligent (or cognitive) manipulation, where force or vision sensory information must be taken into account synchronously to achieve adaptive operation.
- Most (industrial) robot suppliers today use proprietary control systems, each having different basic robot control commands.

We developed a methodology to configure and deploy a so-called SLRT (Sequential Likelihood Ratio Test) server, one per proprietary robot included in a production cell. In operation, it executes all robot real-time sensing and control; at the same time, it provides a standardized robot control interface between the ROS environment modules and the proprietary robot(s) controller(s).

Robot teaching-by-showing enabler. One of the obstacles to robot automation for smaller production lots is the overhead of robot programming for each new application, new task or each production change. To address this issue, we have developed a module, which in conjunction with the SLRT module enables simple teaching or robot transfer and assembly trajectories just by taking the top of the robot and moving it through the trajectory being taught. The enabler takes care of controlling the robot during the teaching phase, so that the operator led movement is effortless and smooth as possible. Internally, we synthesized sophisticated kinesthetic guidance, which enables incremental learning. This control lets the operator refine the previously learned trajectory, by giving him hints about changes: operator movements of the robot that are coincident with the previous trajectory are easier, while larger changes require more effort (by controlled force/torque). The enabler encodes the motion in a special parametric form (DMP) (see Figure 16).

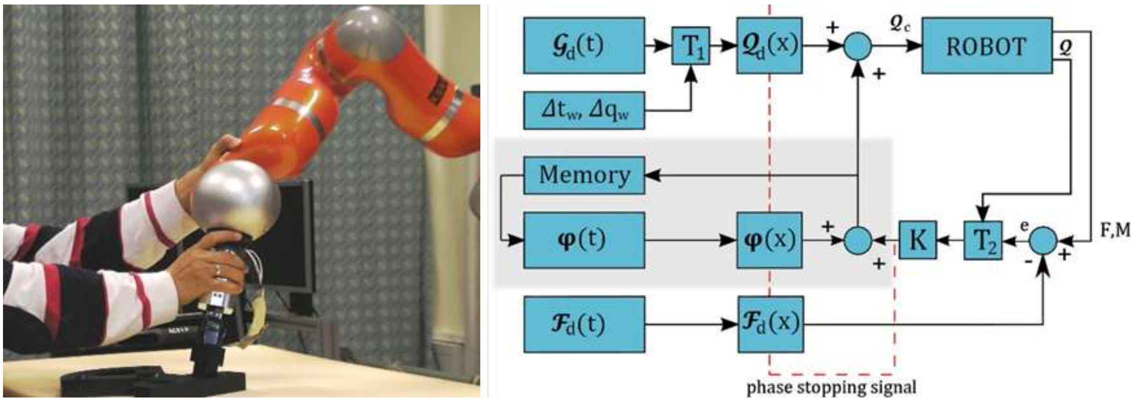


Figure 16: Teaching-by-showing enabler user for an assembly tight insertion operation involving position and force. Left: operator during one demonstration. Right: scheme of learning system.

Robot trajectory generalization enabler. Using ordinary robot controllers, the whole trajectory must be usually re-learned if the beginning or endpoint change (by position or by orientation) or if tools or workpieces change, even slightly. We have developed a so-called trajectory generalization module, which computes such a new trajectory automatically, for example when the start and/or end points change. This automated generation is based on a number of previously used trajectory for the same task category. Example of such task classes are: a) a transfer from A to B; b) insertion of a component into a (tight) opening in another work piece (that is, plug-in-hole type assembly operation).

We have developed or in process of finalizing development of other enablers, e.g.:

- **A ROS communication layer enabler**. It implements standard communication protocols, e.g. MQTT and OPC UA; it functions as an interface from ROS control to external fog/edge and cloud services using previously mentioned, standard IoT protocols.
- **An enabler for deep learning network training.** The typical use for the developed enabler is pretraining of a neural network, based on a number of test images.

Essentially, it achieves a semantic segmentation capability by using a deep learning approach. This enabler runs on a dedicated HPC edge node, as this task requires a considerable computation and takes some time. The pretrained network is then transferred to the on-line ROS based robot control system. There, it is used in operation for real-time robot vision tasks, e.g., for quality control or for object identification.

Use Case Applicability

The enablers described above will be demonstrated at the neutral experimentation infrastructure at JSI. Specifically, we will demonstrate the inclusion of enablers listed above in two or three use cases listed in the following. All use cases represent real-life examples given by actual production companies. The activities on the neutral demonstration facilities that are related mainly to the mechanical/hardware disposition and component design has been done in a parallel, soon to be finished project (ReconCell) [3], while the design and implementation of appropriate service as a software architecture and the design and inclusion of specific enablers is being done as part of the AUTOWARE project.

Some facility's construction structural characteristics are easily reconfigurable main mechanical frame system, specially developed plug-in units dedicated to various sub-tasks, and inclusion of two manipulator robots that can be placed in various positions, depending on the cell layout design for individual production tasks.

The main characteristics of the use cases for demonstration of enabler's applicability are a) necessity to execute several assembly operations (matching, inserting, affixing, orienting, and exerting controlled force) in an effective way, and b) requirements for input and output dimensional and quality controls. Beside this, individual product variants are produced in small batches, resulting in requirements for fast design, control set-up (e.g., fast robot task learning), fast design and construction of required tools (e.g. grippers) and fast assembly of cell elements – that is, there is a strong requirement for fast and effective robot cell reconfiguration capability.

Case A. The first use case will be the assembly of a mechanical subsystem that includes a gearbox (see Figure 17). A total of 5 parts have to be assembled, each residing in different storage device. As individual parts require different gripping and assembly operations, each of these components require different manipulation tools (robot grippers) and different assembly trajectories and operations.

Figure 17: Demonstration of enablers in a use case involving gearbox assembly

Case B. The second use case involves assembling drive actuator elements (see Figure 18). These are components for electronically adjustable furniture. The production company has high volume products, but with several customization possibilities for each customer. This leads to many different product types, based on few basic versions. The basic versions are produced in high volumes on specific production lines and then manually finalized before packing. In this use case, the basic, partially assembled versions of drive actuator elements will be brought to the facility on trolleys, positioned to the cell mechanical frame structure using developed plug-ins production connectors. Specific tools and grippers for the variant presently produced will be concurrently conveyed and positioned to the main cell structure on other plug-in stations. A sequence of operations previously synthesized will be downloaded to the cell control station and executed by the two robots. During the assembly, the robots do change end effectors-grippers and end effector tools. In addition, the application use vision for part location and inspection.

Case C. The third use case will be the assembly of car lightning parts, e.g., headlamps, rear lights and indicator lights. The use case comes from a company that is supplying various car producers, each having different models and variants. Beside this, they must be able to produce – on short notice orders – not only lamps/lights for the current models but also for all individual past models during the time period in which the car producer assures availability of spare parts. Each of these variants needs specialized tools for operations from molding to final assembly. The production, maintenance and stocking of tools require, beside others, a large warehouse. This is problematic especially for past models, where the costs of this is high in comparison with batch sizes, directly influencing profit margins. In this use case, we are achieving two goals: a) to find technical solutions to replace specialized fixture tools with a universal, rapidly reconfigurable device; b) to automate the final assembly operations. When a new product is introduced, some cell planning and set up is similar to the previous two use cases. Additionally, a number of fixture devices must be set up. First, an appropriate fixing device (e.g., a gripper) is mounted on the top of the fixture device (a passive Stewart platform mechanism); second, the position and orientation of the top is set accordingly to the generated assembly plan and sequence. These operations – mounting the device and positioning it – are performed automatically by the cell robots for all fixture tools used in the application.

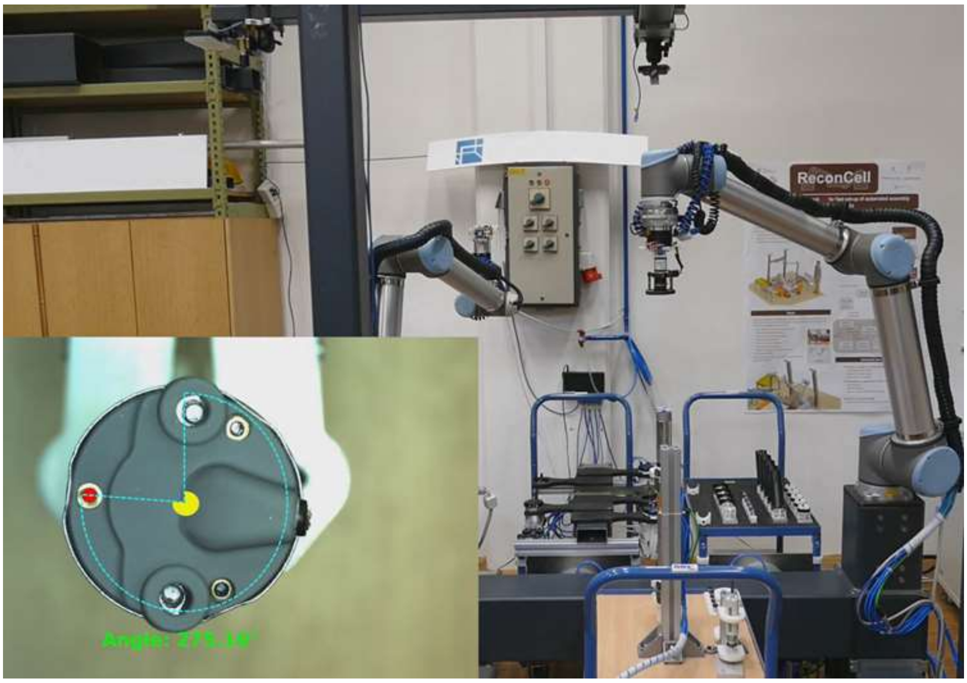


Figure 18: Demonstration of enablers in a use case of drive actuator product customization

General Applicability. The enablers are implemented in the JSI neutral facility cell and the applicability is demonstrated and presented in use cases with emphasis on assembly oriented production. Nonetheless, the nature of the enablers make them useful and operable in any CPPS scenario using ROS based control and involving robots.

3.6 Dual Reality Services

Dual Reality Services comprise Virtual Reality (VR)/Augmented Reality (AR) technologies, which belong to the key-enabler for Industry 4.0 and their application supports effective assistance for assembly, maintenance and repair tasks, training, quality control and commissioning as well as monitoring and visualization [4]. At this time, we propose four different dual reality services to enable new CPPS technology for SMEs while maintaining and improving the usability.

Semantic Workflow Modelling Service

Although knowledge from product engineering and production planning is available in companies and could potentially be reused for different applications, a concept for integration of all this data is still missing. The semantic workflow modelling service foresees to make existing product engineering and production planning data available for a secondary use, namely for cooperative assembly tasks. By retrieving product engineering data (i.e. 3D CAD files) and production planning data (i.e. structured textual data describing the manufacturing execution and the assembly process) from a company's Product Lifecycle Management (PLM) system, the service will generate a semantic description of the assembly process incorporating the 3D representations of the assembly steps (Figure 19). This semantic description can then be queried to learn and to gain cognitive planning and control capabilities. Based on this semantic description the system will be able to identify the next assembly steps and adapt its behaviour accordingly.

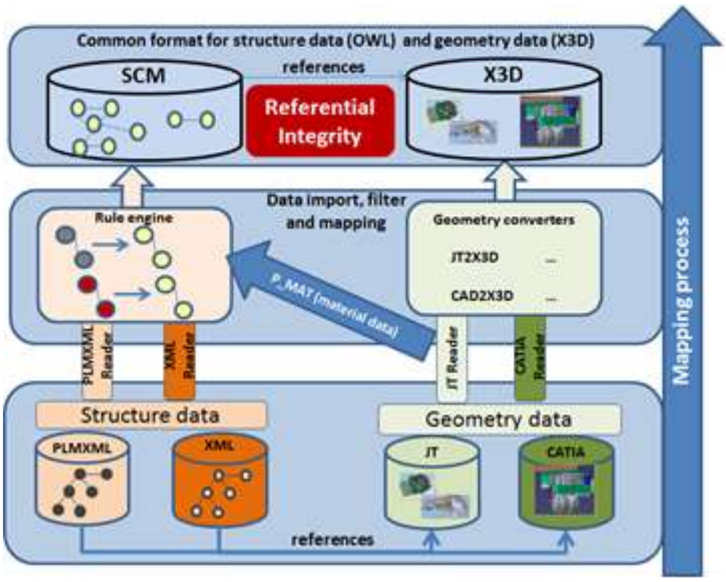


Figure 19: Component diagram showing an overall view of the processing pipeline to create a semantic workflow representation

Dual Reality Modelling Service

In order to apply modern algorithms defined in virtual context to a real world production environment and still benefit from intuitive usability, careful merging between real and virtual data is required.

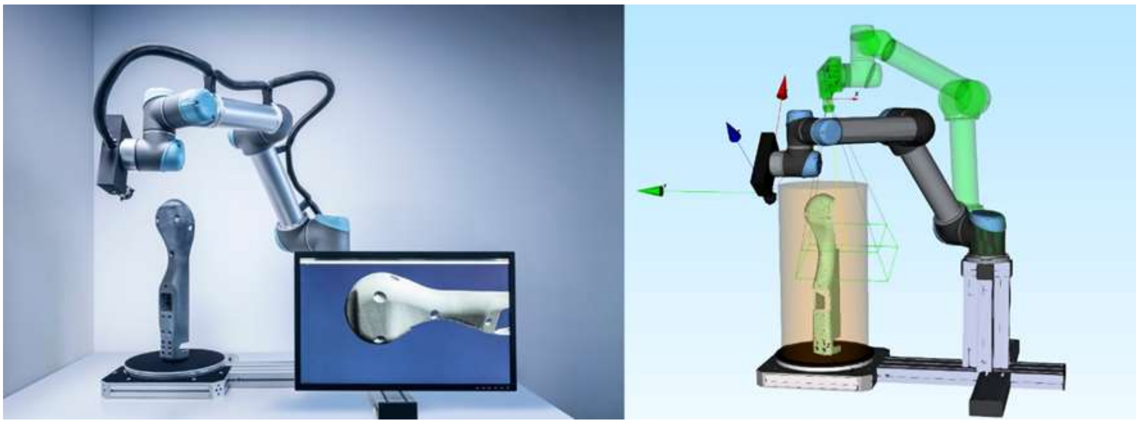


Figure 20: Robot station for 3D laser scanning shown in dual reality

Figure 20 shows an example of applied dual reality modelling within the AUTOWARE project: a 3D laser scanning station developed by Fraunhofer IGD to address the SMC use case of collaborative assembly and quality assessment. The left side of the figure shows a photo of the real scanning station, consisting of a laser scanner mounted on a robot arm scanning an object on a turntable. The virtual representation on the right side shows exactly the same setup and relies on real world sensor data, such as robot arm joint configurations and 3D point clouds, to represent and enrich the real world setup in an intuitive way. E.g., the real object's 3D scanning data is directly reconstructed on the virtual turntable, therefore, it is much easier for an operator to visually monitor the progress of complex autonomous scanning tasks.

To make use of this functionality of dual reality, the system must be initially calibrated. This typically requires high user expertise and involves the sensor type knowledge and its mounted position and orientation on the kinematic chain. Within the dual reality modelling service, we plan to automate the whole calibration process and make it available on the cloud.

3D Object Retrieval and Object Recognition Service

Most shape representations describe the shape of an object, with visual and material properties. However, autonomous and cognitive applications often require enhanced shape properties to relate the parts of a shape to each other. The 3D Object Retrieval and Object Recognition service can use engineered, but also learned features in order to classify and recognize 3D objects. This involves also semantic segmentation by fitting geometric primitives in discrete geometric representations and mapping them to related parts in CAD models (see Figure 21). By providing a 3D CAD model reference database containing the 3D geometry of parts and tools used in the assembly process and 3D point clouds of the real object, the service can identify the CAD model representing the assembly state. This allows for an automatic state recognition and enables the alignment of real world conditions with the digital world.

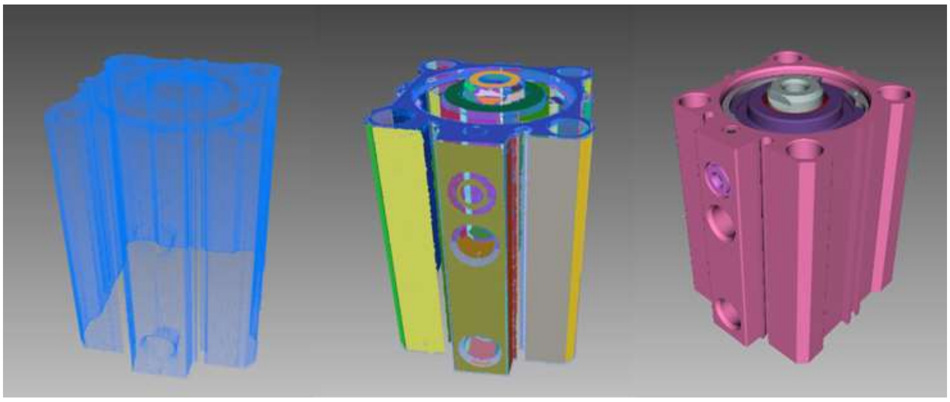


Figure 21: From left to right: The scan from a real world objects, the result after the semantic segmentation, the classified CAD model representing the state of the real world object

3D Quality Control Services

One primary aspects of autonomous 3D quality control is comprised of target/current comparison of point clouds generated from real world objects with digital CAD models. With this service, the user is relieved from doing manual check of dimensions after the completion of assembly steps. The quality control service requires an annotated 3D CAD model with measurement details and a 3D point cloud of the real object. The service automatically retrieves the measurement details, which are involved primitives e.g. planar segments, the expected distance between the primitives and allowed tolerances. Therefore, this service realizes the automatic transfer of information embedded in CAD models to qualify services. As an output, the user receives the results of the measurement and a statement whether the measurement result is in the predefined tolerance range. By adding annotations in the CAD model, the requirements can be easily extended without changing the workflow providing the user and easy to handle measurement tool.

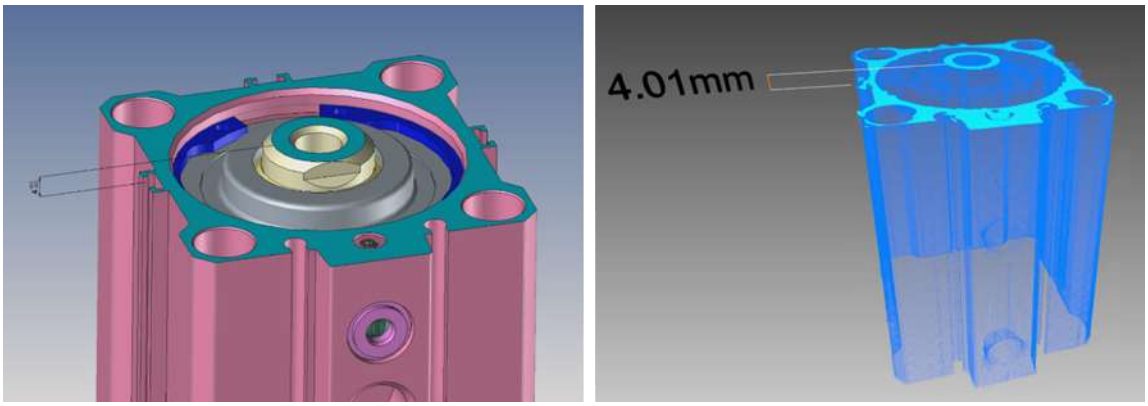


Figure 22: Based on measurement annotations in a CAD model (left), the scan of the real world object (right) is semantically segmented and registered to automatically perform the desired measurements.

Use Case Applicability

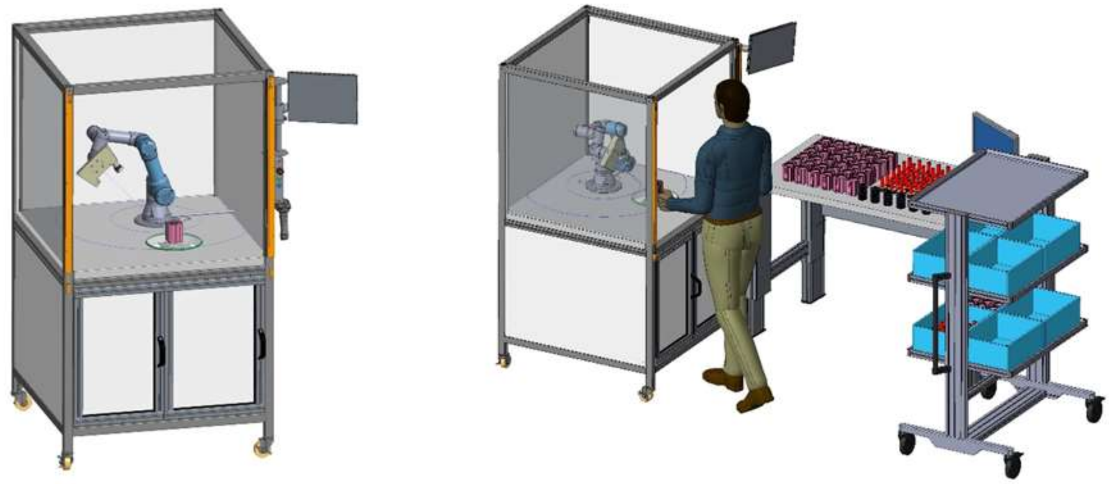


Figure 23: Robot scanning station within the SMC use case of collaborative assembly and quality assessment

All enablers are included in the use case of industrial cooperative assembly of pneumatic cylinders by SMC Pneumatik GmbH. Figure 23 shows the designed 3D laser scanning station within the SMC use case. The initial self-configuration of the system is part of the dual reality modelling service and is essential for robot trajectory and view planning that enables autonomous 3D scanning and quality control for this use case. The required user interaction is reduced to placing a known calibration target board on the turntable. Then the robot autonomously carries out the calibration procedure and captures the board from various angles. After the calculation, 3D scanning data can be reconstructed and merged within the common turntable coordinate system and forwarded to other processing services. By exploiting the knowledge of the semantic model generated from the semantic workflow modelling service, the scanning system and related services are provided with a knowledge base to autonomously perform tasks like object recognition and measurement.

3.7 Machine Learning

Machine learning and machine vision are disruptive new key technologies currently being adopted in Industry 4.0. They enable further automation in production processes, specifically in cases where manual programming of the system is not possible due to the complexity to transform domain knowledge into rule-based systems. Well known examples of this include predictive maintenance, the recognition of objects and process optimization. ROBOVISION and IMEC describe two enablers in this field:

- Deep learning based computer vision
- Rapid reconfiguration of deep learning vision systems

Both technologies are applied in the STORA ENSO use case.

Deep learning based computer vision

Traditional vision systems used in industry rely on the extraction of simple human engineered features which are then used as input of a rule-based system to make decisions. Such systems are highly limited in their applicability. Firstly, the decision process must be easily transformable into a set of rules with optimal inputs and secondly, the input features of the rules must be able to be extracted in real-time and with high precision from the video stream.

Therefore in reality, such use cases only make up for a very small fraction of production processes, restricting the adoption of vision based systems and resulting in the need for manual labour and lower quality metrics. In addition, manual feature engineering is a difficult and costly process with limited re-usability in case the production process changes slightly.

In Industry 4.0, there is a clear trend towards the production of smaller batches of different products as opposed to a single product being produced. This evolution results in the need for rapid changeovers and versatile systems. Further increasing the need of new vision based technology which can cope with these changing production requirements.

Deep learning is a specific field of machine learning which investigates the use of large and layered neural network architectures to enable automatic feature engineering based on data. This technology has rapidly evolved in the last years and has enabled a revolution in *inter alia,* image and video processing, speech synthesis, generative models and natural language processing. The success of this technology can be largely attributed to its ability to automatically extract relevant input features related to the problem at hand, removing the need for costly and often sub-optimal manual feature engineering.

Figure 24: Vision Technology and Robovision's Deep Learning models applied towards segmentation of paper versus cardboard. See lowest part, the centre points of cardboard pieces are marked – for removal by one of the techniques described.

Within AUTOWARE, ROBOVISION has configured deep learning systems and associated tools to create novel machine vision systems, which are applied in the use-cases. More specifically, in a first phase, the machine learning system data needs to be collected related to the process. This data can be separated in two categories: human annotation (labels) and associated image data. Obtaining relevant labels is a costly process, for this ROBOVISION has developed solutions in its RVAI platform. In a second phase, the system needs to be trained, for which ROBOVISION uses the latest deep learning advances. This novel technology offers the possibility to use vision based algorithms based on combinations of complex features such as shape, form, colour and can be reconfigured to recognize new products, as demonstrated in the STORA ENSO use case (see Figure 24).

Rapid reconfiguration of deep learning vision systems

The adoption of deep learning vision systems effectively removes the need for manual feature engineering, however, it introduces the need to tune the deep neural network to the specific problem. This tuning process requires specialist knowledge and is often criticized to be an ad-hoc process. In addition, during set-up, it may require extensive computing power in the form of specific hardware (GPU, TPU). Both problems hinder the adoption of such systems in a manufacturing setting where rapid changeover times are critical.

IMEC has developed specific software to mitigate these problems in the form of the software framework GPFlowOpt. In traditional deep learning network set-up, the domain expert will select and try out different neural network architectures and settings which can be described as 'hyperparameters' of the system. This process is traditionally performed by random searches or grid searches of certain values. In contrast, GPFlowOpt is a novel framework which relies on a set of machine learning methods called Gaussian Processes to perform Bayesian Optimization. Bayesian optimization is a particularly useful method for expensive optimization problems. This includes optimization problems where the objective (and constraints) are time-consuming to evaluate: measurements, engineering simulations or in this setting: hyperparameter optimization of deep learning models.

The software package will tackle the problem by exploring at the start a limited set of settings for the deep learning vision problem and will continue by exploring regions of hyperparameter settings in the most optimal regions. Throughout this iterative process, a fine balance between exploitation and exploration is struck, allowing the system to converge to a more accurate machine vision system. In addition, less domain knowledge is needed to utilize such systems and shorter changeover times can be obtained.

Use Case Applicability

These technologies are actively used in the novel STORA ENSO use case, which was found as a replacement for the original proposed PWR industrial pilot. Briefly, the envisioned main outcome of the use case is the adoption of AUTOWARE technologies to allow more accurate paper-cardboard separation by among others deep learning vision technology and the ability to process diverse compositions of paper-cardboard of varying quality by rapid reconfiguration of such systems to the incoming batches.

In the off-site testing facility, a conveyor belt system has been set up*, equipped with a camera bridge and a robot gripper. During the set-up phase, images of paper-cardboard mixes have been generated and labelled using the developed software (see* Figure 25*).*

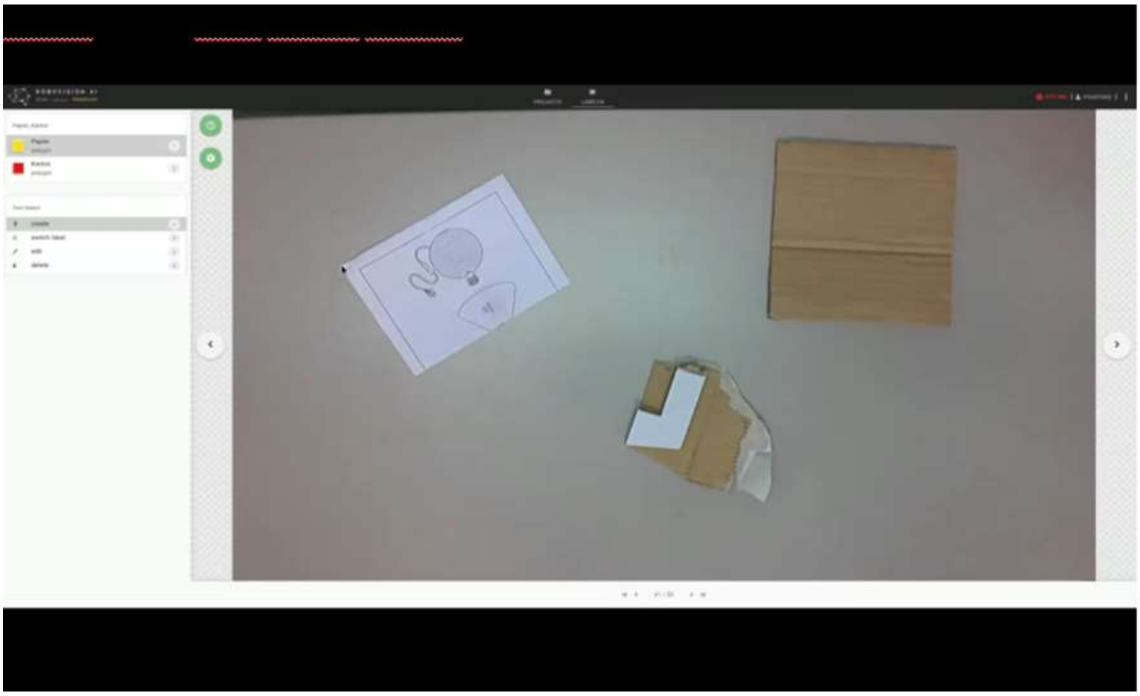


Figure 25: Labelling process of the data set

In a next phase, the deep learning vision system has been trained and validated offline with good results. During further testing, work will be done towards the integration of the system in a live setting and the rapid reconfiguration will be performed using the GPFlowOpt technology.

4. Verification, Validation and Certification Enablers

The evolution of the industry 4.0 leads us to plants of flexible and reconfigurable structure through modularization, leaving behind the serialized and mass production. With an increasingly personalized consumption, more and more lots of single pieces are carried out in the manufacturing plants. After the configuration of our plant in order to produce our single piece batch, we will have to carry out the certifications related to safety manually.

In order to avoid manual verification, validation and certification, new adaptative safety concepts regardless of the machines used should be developed. This system must allow the insertion or elimination of modules without having to stop production and without this change affecting the rest of the plant. The achievement is the automatic update of the changes on the parameters related to the safety of the manufacturing line.

In the following chapter it is explained the development that has been carried out to achieve a simple and partially or fully automated certification process. The implementation of these advances has been carried out in SmartFactory facilities.

The core of SmartFactory is to be the culmination of everything that encompasses Industry 4.0, pretends that factories are able to adapt continuously and immediately to different tasks, change the products that are manufactured and adapt them to the specific needs of each client.

Therefore, SmartFactory is the perfect place to test the development of automated security due to the fact that if the developed system works in SmartFactory, it will meet the specifications mentioned above.

4.1 Machine Learning

The first step in the development of modular systems in terms of safety is to make the modules safe themselves. Dedicated production modules with their own control system are responsible for the execution of the individual process steps. Each of these production modules represents a complete machine according to the machinery directive and has its own CE conformity. As already mentioned at the beginning of this chapter, the creation of a network of machines from these production modules requires in certain cases a new consideration related to the security of the whole due to the existing relevant interfaces.

As a result, it cannot be derived from the combination of several production modules compatible with CE to any global CE compliance for the resulting machine network. The entire 4.0 industrial system of the SmartFactory KL technology initiative is based on paradigms such as plug & production, vertical networks and decentralized production control to enable individualized production in batch size one “on demand”. These paradigms and intelligent neighbourhood detection allow modules to be replaced during operation without significantly affecting production. However, in practice, a security assessment must be performed when changing the configuration of a group of machines. These revaluations are contrary to the objective of flexibility and, therefore, form a bottleneck.

The challenge within this context is to verify as automatically as possible if it is necessary to reexamine security after having assembled two or more modules. The general certification is given when the modules are not related to each other in terms of security, especially if the system is not an interlinked system. If there are dependencies, however, between the modules, a new examination is necessary according to the current state of the art. Only the security risks caused by the combination of the modules and the resulting interfaces are considered. The requirements for an analysis of the conformity the before mentioned network of machines include, therefore, the following questions:

- Is the machine interconnected?
- If so, what interdependencies related to the safety exist?
- What consequences result from the evaluation of the security units?

4.2 Requirements

The goal is that any combination of I4.0 module machines from different manufacturers will automatically result in a network of certified machines. For this certification process, the obligations of the manufacturer of the interlinked plant are summarized in extracts in the following table:

Table 1 Obligations of the manufacturer of the interconnected plant

Machinery Directive-obligations	Source
Risikobeurteilung (risk assessment)	MRL 2006/42/EG Anhang I
Maschinenkennzeichnung (machine identification)	MRL 2006/42/EG Anhang I.1.7.3
Betriebsanleitung (operating manual)	MRL 2006/42/EG Anhang I.1.7.4
Konformitätserklärung (declaration of conformity)	MRL 2006/42/EG Anhang II
CE-Kennzeichnung (CE-labeling)	MRL 2006/42/EG Anhang III
Technische Dokumentation (technical documentation)	MRL 2006/42/EG Anhang VII

In order for the rules indicated in the previous table to be met automatically, different basic requirements must be met. As for example, CE compatible machine modules with basic risk assessment provided. In addition, a clear and complete description of the interface of each module of the machine is required. The modules of the machine, at the same time, must be able to communicate with each other and with the central production servers. The use of machine modules from different manufacturers requires a communication protocol independent of the service-oriented platform, such as, for example, OPC-UA through TPC/IP.

After the addition and/or the removal of modules in the production line, the risk assessment is automatically adapted to the reorganized production line. This saves us resources by not having to assess risks manually. Analogous to the modules of the machine, the modules must meet the same requirements: description of the interface and communication oriented to the service.

4.3 Concept for automatic conformity assessment

The following concept describes how the implementation and use of the described requirements can lead to an automatic evaluation of the interlinked systems. A distinction is made between different phases, which operationalize the manual procedure for conformity assessment and make it manageable for IT processing.

- **Discovery phase**

  During this phase, a connection is established with a new machine module, this connection is identified and the properties of the module are transferred. It is not necessary to transmit all the content of the management shell, it is sufficient to transmit the header that serves as a link to a table of contents within the administrative shell that contains all the information, data and functions.

- **Validation phase**

  The validation phase essentially consists of two steps: determination of the configuration of the new production plant and validation that configuration using profiles. These profiles represent partial models of the assets of the shell administration and contain relevant information in relation to security aspects of the mold. That will form the basis for future conformity assessments. During this phase, in which the configuration is determined, it is decided which module is coupled to which module.

- **Plausibility check**

The communication parameters for a secure cyclic communication are read from the management shell and subject to plausibility check. This compares, for example, network times and ensures that reliable response times can be maintained in all security functions.

- **Digital conformity assessment (proof of CE conformity)**

This phase is carried out parallel to the plausibility check. The information exchanged between the components is transmitted to a cloud service. This cloud includes security measures such as SEV, SGX, etc.

If the cloud service concludes that the network of modules of the machine meets the requirements with respect to the safety of the machine, the declaration of conformity is created and also archived and the keys are generated. The keys contain the logical IDs of all safety actuators and sensors involved, the ID of the safety control, the typology and the level of performance achieved.

- **Approval of the machine group**

In this automated concept, a bidirectional communication is implemented since an expert may request some document that is generated during the process to review it.

The following figure illustrates the phases described for the automated integration of a new machine module into a production line using a flow diagram:

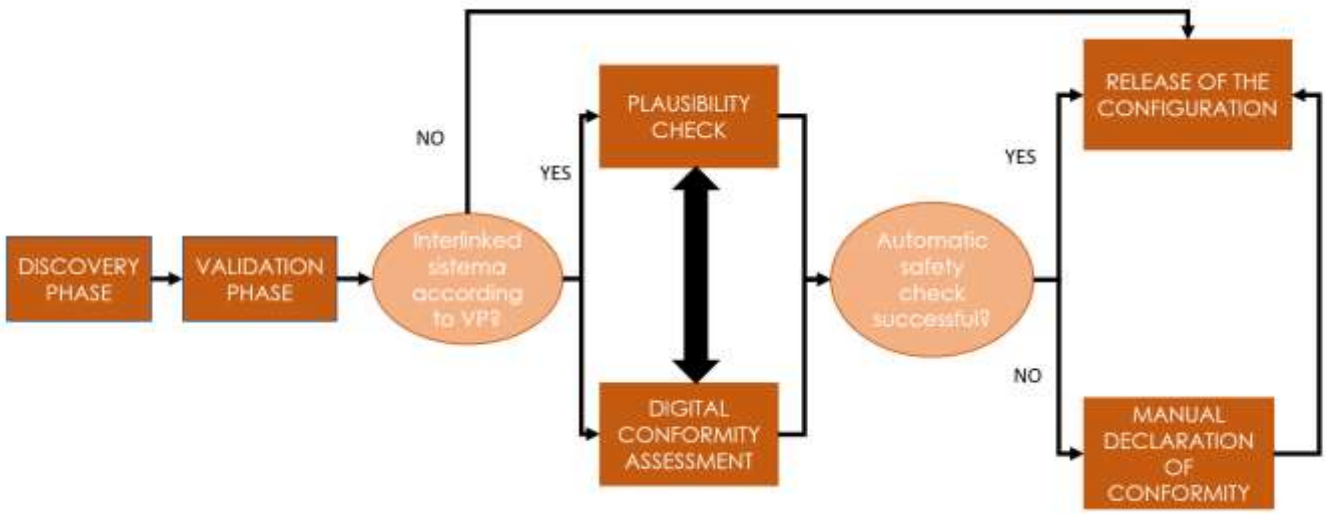


Figure 26 Phase diagram

4.4 Structure of the modules and applications

The modules of SmartFactory KL are identical with respect to the internal transport of their parts. The transport is carried out through two conveyor belts that turn in the opposite direction, each of which is secured at its ends by doors. The doors controlled by pneumatic cylinders can have the "open" a "closed" states.

Protection/maintenance doors and emergency stop switches have been installed in each module as physical protection devices. A necessary step has been taken with respect to modular security by dynamically expanding the emergency stop circuit of the modules that belong to it from a local point of view. In addition to the modules already described, there are special transfer modules (hereinafter, coupling stations) that carry that workpiece transport at the end of a production line to the "Robotino" driverless transport system. These docking stations do not have their own doors, as there is no immediate danger from the functional assembly of this module. In order to avoid a possible danger due to the intervention in an adjacent module door and, due to its height, makes it impossible to reach it. Robotino himself has an emergency stop switch that stops only the Robotino not the entire production line.

All the relevant security functions are connected wirelessly to the security system. During the coupling phase in one of the various production lines, a piece is transferred from the line to the Robotino , which, from a safety perspective, must be temporarily assigned to the corresponding line.

Subsequent versions are limited to interfaces to link the described system modules. The following figure shows the protection devices "door" and "protection tunnel" that have been implemented":

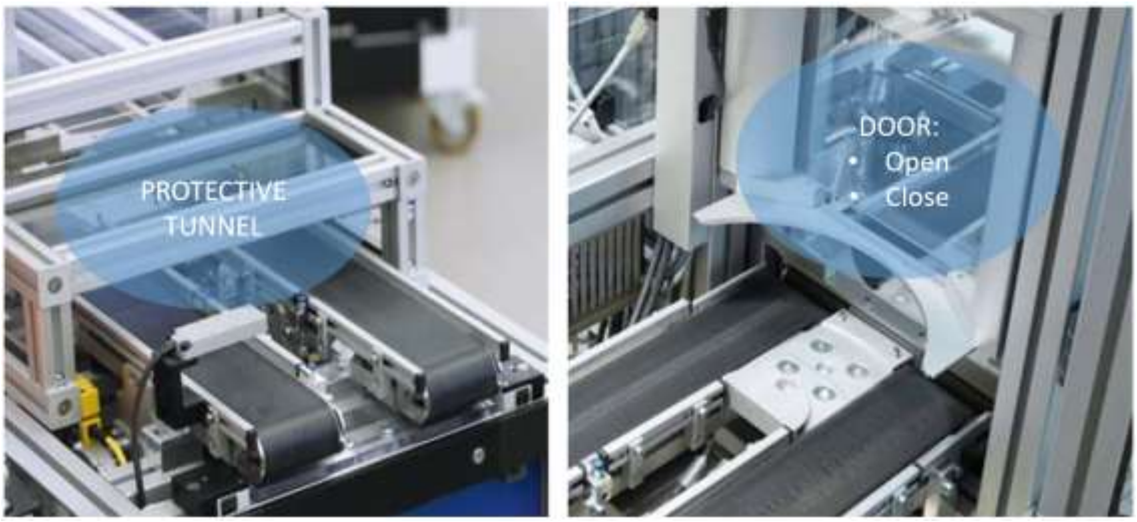


Figure 27 Protective tunnel & door

From this described structure of the modules and the resulting properties of a concatenation of these, different cases arise, which require a consideration related to safety.

Case 1

A problem with the modules of the adjacent machine arises when trying to access another module by opening a v through the doors. If the neighbouring modules have different PL (Performance Level), restrictions may arise. For example, the module with the highest performance level could affect the security assessment of the module with the lowest performance level.

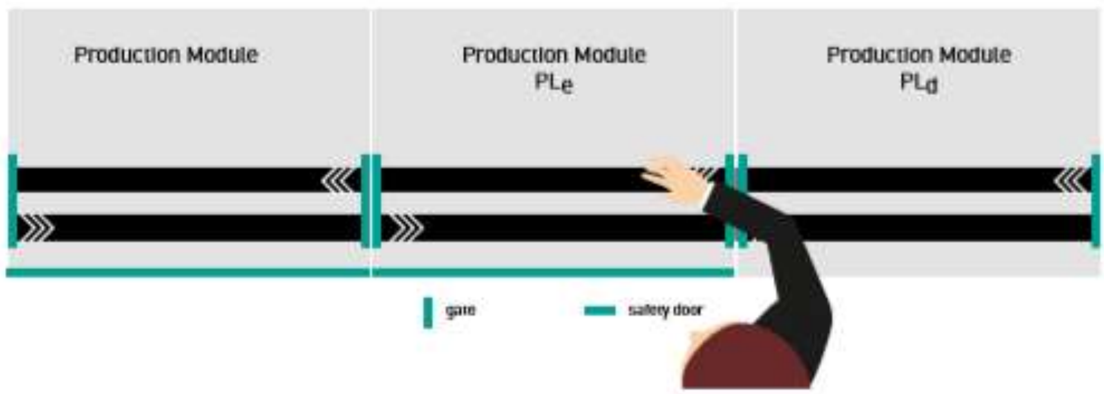


Figure 28 Case 1

Case 2

There is another conceivable case, if a module has a door lock and the neighbour module does not. This case is derived directly from the considerations in case 1 and the results of different PL of the modules. If the maintenance and/or safety door is opened without a blockage of the module, the gates must be closed immediately if a module with a PLr greater than the PLr of the module in question is adjacent to prevent penetration during the operation of the neighbouring module. If the PLr of all adjacent modules is equal to or less than the module under consideration without blocking, it is not necessary to close the gates immediately.

Case 3

If the neighbouring modules are in different operating modes (for example, manual, automatic operation, coupling or decoupling), there is another case of a possible additional danger in the interlaced operations. In this case, the doors between the modules must always be kept closed.

4.5 Safety profile definition

Through the described structure of the modules and the consideration of the interfaces related to the security, as well as the resulting risks, different profiles can be defined that should allow an automatic evaluation of the conformity when linking the modules. For a SmartFactory KL production module, the profiles are "Performance level", "Emergency stop", "Doors" and "Protection door", regardless of the module considered.

Performance level of the security profile

The risk assessment is used to determine the PLr of the machine module, which must be evaluated through the profile for an interconnected machine. As mentioned above, the production modules are intrinsically safe, so PLr = PL is applied. This means that all the protection measures used in and on the module, interfaces comply with the requirements resulting from the module functions.

Profile definition performance level:

PL = PLr = x ε [a, b, c, d, e]

Safety profile emergency stop

The emergency stop switch must be present in each module. Therefore, each module also has an emergency stop safety profile. The emergency stop acts on the module itself and, in the case of an interconnected machine, on the entire line.

A red light on the switch indicates that the emergency stop switch is in the active state. There is a second ring of additional light around the switch, whose colour indicates functional affiliation. The emergency stops switches that are functionally assigned to the same group of machines have the same colour.

Profile definition emergency stop:

- Emergency stops available

Safety profile security door

The security door allows access to the interior of the module. If there are dangerous points or dangerous movements in the module, the system should turn off when the security door is opened. If a timely closing is not possible, the safety protection must be equipped with a locking device. Let's say that if it is not possible to stop the machine from hitting when the door is opened, it will be necessary to block the door so that it cannot be opened until the line is stopped.

Profile definition of the safety door:

- safety door available
- door locks available
- PL

Safety profile doors

The material is transported through the modules through the doors of these modules. When these doors are closed, they prevent access to the dangerous movement that may be happening inside the module. If no dangerous movement occurs within a module, those doors are not necessary. If a machine operates alone, that is, the process only needs to go through that module, both doors will be closed. And if a machine is at the end of the line, the last door must also be closed. The protection tunnel that is in the docking stations is included in the "gate" profile pq has the same functions.

Profile definition:

- Gate on the left side available
- Gate on the right side available
- Gate == protective tunnel
- PL
- Operating mode

As explained above, the profiles describe the structure, behaviour and interfaces of a machine. For use case "doors", this means that a profile "gate" presupposes the existence of a physical gate, which is displayed in the asset management shell. It also means that the profile must be implemented for monitoring the security door.

If all the machines of a group have implemented the profile mentioned above, the group can be certified as safe with respect to the security functions established in this profile. If the necessary information is lacking (e.g., a machine that has not analysed the safety profiles that it would need or special situations) qualified personnel should evaluate the possible guidelines to follow regarding safety. These new manually certified machines are stored and can be automatically certified in the future on the basis of the new security parameters stored dynamically in the asset management Shell.

4.6 Summary

This chapter describes a concept for the automatic certification of the production modules of Industry 4.0. The objective is to provide greater flexibility when changing the groups of machines. Changes in the machine group are accepted as safe (machinery directive) if the individual components have the expected safety profile for the higher protection function in which the safety functions are described and implemented by all the machines in the group. If there are machines in the group that have not yet implemented the required profiles, or if these profiles are obsolete, they must be re-evaluated manually. These are stored in the asset administrative shell and will be available to the group of machines in the future.

The technical chapter provides an impulse for the automatic certification of the modules of the machine, but there are still work packages that must be elaborated before the implementation. Security profiles must be created uniformly, they must not differ from one machine to another, so the uniform Ind4.0 validation requirements can be considered for automatic certification. In addition, the cloud is a central component of the concept. However, this also imposes special requirements on them. It should be clarified how communication between the machine and the cloud should be designed to meet the security requirements for the desired certification.

5. Conclusions

This deliverable provides an overview of the developed usability and verification, validation and certification enablers. The work presented in this deliverable is closely related to the technical work coming from WP2, WP3 and WP4 where the different technical enablers are being developed. The usability enablers are responsible for the user friendliness of the technical enablers and that the technical developments are actually applicable for the targeted companies (mostly SMEs).

The description of the usability enablers is provided on a high level in this deliverable. In the related technical deliverables (coming from WP2-WP4, describing the technical enablers) also include a more detailed description of the usability enablers. The goal of this deliverable is more to provide an overview of the available enablers and to refer the potential users (e.g. end-users, technology developers or system integrators) to the technical description. Additionally, the overview of the enablers also provide a description of the neutral or industrial pilot, where the enablers is applied and especially, how the enabler will be applied in the specific pilot. This will provide a potential user with an overview of how the different enabler can be applied is a specific scenario.

As a final remark, the reader has to keep in mind that the usability enablers presented in this deliverable are not the final ones. The AUTOWARE project is still on-going and developments to the technical enablers (and indirect to the usability enablers) will take place. This can have as a result that modifications can take place and that there will be implementations available that are not presented yet in this deliverable.

References

[1] AUTOWARE Deliverable D1.3b – AUTOWARE Cognitive Digital Automation Framework, Public Deliverable, 2018

[2] R. Serna Oliver, S.S. Craciunas, and W. Steiner - **IEEE 802.1Qbv Gate Control List Synthesis using Array Theory Encoding** In Proc. 24th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), pp. 13-24, IEEE, 2018.

[3] ReconCell – A Reconfigurable robot WorkCell for fast set-up of automated assembly processes in SMEs, EU Project, [Online], http://www.reconcell.eu/, last visited: January 2019

[4] ZDNet, Retrieved from Ten industries using augmented reality and virtual reality: http://www.zdnet.com/article/ten-industries-using-augmented-reality-and-virtual-reality/