ICT-56-2020 "Next Generation Internet of Things"
Grant Agreement number: 957218

IntellioT

Deliverable D2.4
Use Case specification & Open Call definition (final version)

Deliverable release date	30/04/2022
Authors	1. SIEMENS: Andreas Zirkler, Arne Bröring, Vivek Kulkarni 2. EURECOM: Jérôme Härri 3. AAU: Beatriz Soret, Lam Nguyen 4. UOULU: Sumudu Samarakoon, Mohamed Abdelaziz 5. TTC: Martijn Rooker 6. TSI: Andreas Brokalakis, Babis Savvakos 7. Philips: Nancy Irisarri Mendez, Anca Bucur 8. SANL: Konstantinos Fysarakis, Ioannis Vezakis 9. HSG: Simon Mayer, Jérémy Lemée 10. HOLO: Carina Pamminger, Nour Fendri 11. AVL; Holger Burkhardt, Wolfgang Hollerweger, Sandro Perla-Steinhuber 12. PAGNI: Maria Marketou 13. STARTUCOLORS: Berkay Kabay, Maren Lesche
Editor	Martijn Rooker (TTC)
Reviewer	Arne Bröring (SIEMENS), Konstantinos Fysarakis (SANL)
Approved by	PTC Members: (Vivek Kulkarni, Konstantinos Fysarakis, Sumudu Samarakoon, Beatriz Soret, Arne Bröring, Maren Lesche) PCC Members: (Vivek Kulkarni, Jérôme Härri, Beatriz Soret, Mehdi Bennis, Martijn Rooker, Sotiris Ioannidis, Anca Bucur, Georgios Spanoudakis, Simon Mayer, Filippo Leddi, Holger Burkhardt, Maren Lesche, Georgios Kochiadakis)
Status of the Document	Final
Version	1.0
Dissemination level	Public

Table of Contents

ACRONYMS AND DEFINITION

Acronym	Definition
5G NR	5th Generation New Radio
AAA	Authentication, Authorization and Accounting
A&E	Accident and Emergency
AGV	Autonomous Ground Vehicle
AI	Artificial Intelligence
AODV	Ad-hoc On-demand Distance Vector
API	Application Programming Interface
AR	Augmented Reality
B.A.T.M.A.N.	Better Approach To Mobile Adhoc Networking
CAD	Computer Aided Design
CAGR	Compound Annual Growth Rate
CAM	Computer Aided Manufacturing
CAN	Controller Area Network
CNC	Computerized Numerical Control
CNN	Convolutional Neural Network
D2D	Device to Device
DLT	Distributed Ledger Technology
ECG	Electrocardiogram
ETCS	E-Tractor Control System
FAO	Food and Agriculture Organization
FOV	Field of View
GDPR	General Data Protection Regulation
GIS	Geographic Information System
gNB	gNodeB
GPS	Global Positioning System
HIL	Human in the Loop
HyperMAS	Hypermedia Multi-Agent System
IAKM	Infrastructure Assisted Knowledge Management

ICT	Information and Communication Technology
IDS	Intrusion Detection System
IMU	Inertial Measurement Unit
IoT	Internet of Things
IPR	Intellectual Property Right
IPSec	Internet Protocol Security
IT/OT	Information Technology / Operation Technology
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LBS	Location-based Services
MEC	Multi-Access Edge Computing
MES	Manufacturing Execution System
ML	Machine Learning
MTD	Moving Target Defences
NN	Neural Network
OLSR	Optimized Link State Routing
QoS	Quality of Service
RFID	Radio-Frequency Identification
ROI	Return on Investment
RTLS	Real-Time Locating System
SAP	Security Assurance Platform
SME	Small and Medium Enterprise
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
UC	Use Case
UE	User Equipment
UML	Unified Modeling Language
VPN	Virtual Private Network
VR	Virtual Reality
W3C WoT TD	World Wide Web Consortium Web of Things Things Description

EXECUTIVE SUMMARY

This deliverable summarizes the work that has been done in the whole of Task 2.1 (which covers cycle 1 and updates for cycle 2 of the project), related to the use case definitions and the technical scoping of the second Open Call of IntellIoT. As such, this deliverable presents the final results of Task 2.1, organized in two parts: the first part defines the three use cases (agriculture, healthcare and manufacturing) in detail, including its objectives, description, market situation, technical components and the defined scenarios that cover the three key IntellIoT concepts, namely Collaborative IoT, Human-in-the-Loop and Trustworthiness. The second part defines the second IntellIoT Open Call, allowing third parties to further extend the ecosystem of IntellIoT by building up on and contributing to the use cases and the overall framework. This is the final deliverable of Task 2.1 and with this deliverable, this task has been finalized.

1 INTRODUCTION

The IntellIoT project targets three use cases in the areas of agriculture, healthcare and manufacturing. These areas have been selected because they feature heterogeneous IoT enabling technologies, device types, network deployments and performance requirements. Due to these dimensions of variability, the use cases provide broad coverage of technical challenges that need to be considered during the development of Next Generation IoT applications, and consequently of IntellIoT's architecture, providing an effective foundation for evaluating and demonstrating IntellIoT's outcomes. In addition, by specifying and analysing the three use cases and related to the three conceptual pillars (Section 1.2), we were able to identify and formulate a key technical challenge for IntellIoT on which to focus the project's efforts:

Enable **collaborative IoT** environments to execute **de-centralised AI-driven** applications interacting with the **human-in-the-loop**.

While this main challenge provides focus and guidance for our research work, the definition of the use cases forms the basis for our developments, demonstrations and evaluation activities taking place within the project across the associated work packages (namely, WP3, WP4, and WP5). The use cases will provide a high-level story about what and how the functionalities will be demonstrated in the three different selected domains.

To present the above, Section 2 of this deliverable provides the descriptions of the three different use cases. Each description of a use case starts with highlighting its scope and objectives, stating why the specific domain has been selected as an appropriate area for intelligent IoT. Next, the high-level story line of the use cases is provided, describing what will be demonstrated in the use cases and how the technologies will fit in. An overview of the specific domain is also provided, together with some main challenges inside the targeted domain. It will be described here which challenges each use case targeting within the domain. An overview of the different entities that are being applied or further developed inside the use cases will be provided, describing the functionalities of these entities and what their role is going to be inside the specific use case. These include use case specific entities (e.g., the tractor for the agriculture use case, robots for the manufacturing use case and health devices for the healthcare use case) and entities that are core IntellIoT framework components that will be deployed in multiple use cases, demonstrating the cross-domain applicability of the IntellIoT solution. Additionally, there will be a description of the contribution of the first Open Call winners for the respective use cases. Four SMEs have been added to the consortium, one for each use case to add new functionality, and the fourth one as a contributor to the general framework. The last part of each use case description provides the specification of different scenarios for each individual use case. The decision was made that the use cases are targeting a specific domain (i.e., agriculture, healthcare and manufacturing), while the scenarios of each use case demonstrate key activities, functionalities and technologies within said domain. Therefore, for each use case, three scenarios are identified based on the pillars of the IntellIoT project (Collaborative IoT, Human-in-the-Loop, Trustworthiness), as will be described in Section 2.

Section 3 describes the technical scoping of the 2nd Open Call. While the purpose of the 1st Open Call has been primarily to enhance the project's technological and use case coverage towards the 2nd cycle, the purpose of the 2nd Open Call is the initiation of an ecosystem that carries on beyond the project. The contributions from the 1st Open Call are described in each use case section.

Finally, section 4 concludes this deliverable and will summarizes the results of task 2.1 and how these will impact the rest of the project.

1.1 Modifications compared to deliverable D2.1

This deliverable is the follow-up of deliverable D2.1. The decision was made to not write a whole new document but instead, update the predecessor with the experiences and feedback from cycle 1, that will influence the definition of the three use cases. The use case teams have been working extensively on the development of the individual technologies (WP3 & WP4) and the first integrations of the technologies and their validation within the use case demonstrators (WP5). Feedback from these activities resulted in changes in the specifications of the use case

definitions (e.g., usage of technologies, scenarios descriptions, key scenes, etc.). The updated use case specifications will be presented in the following sections for each use case.

Furthermore, end user workshops have taken place, which are described in deliverable D2.2. The feedback we received from the end users has been validated and considered in the updates of the three use cases. Additionally, the use case specifications have been extended by the results of the first Open Call. For each use case, a description of the contribution from the respective Open Call winner is provided in each chapter, presenting their contributions and how the contributions will extend the overall use case.

As mentioned, the individual use case definitions are updated based on the results of the first cycle. This mainly can be found in the description of the three scenarios for each use case. In the updated scenario descriptions, one can also find an additional field in the corresponding tables describing the updates of the specific scenario.

Finally, the description of the Open Call (see Section 3) has been updated. As the first Open Call is now over and the winners are contributing to the use cases, we are already preparing for the second Open Call in the project. This chapter has been updated and provides first information and ideas for the upcoming Open Call and will be the basis for the further work to be performed in Work Package 6.

1.2 Pillars of IntellIoT

The overarching objective of IntellIoT is to develop a reference architecture and framework to enable IoT environments for (semi-) autonomous IoT applications endowed with intelligence that evolves with the human-in-the-loop based on an efficient and reliable IoT/edge – (computation) and network- (communication) framework that dynamically adapts to changes in the environment and with built-in and assured security, privacy, and trust. This reference architecture and framework will be applied in the heterogeneous use cases encompassed in the project, covering agriculture, healthcare, and manufacturing environments. It is therefore of major importance that clear requirements are derived from the use cases. But to create the definitions of the use cases, it is also important that we uphold the defined targets of IntellIoT. The IntellIoT project focuses on three research aspects and associated next generation IoT capability pillars, namely collaborative intelligent systems (IoT), human interaction with the intelligent systems and that all these activities are performed in a trustworthy and secure way. These aspects result in three pillars, which are depicted in Figure 1, and are shortly described below.

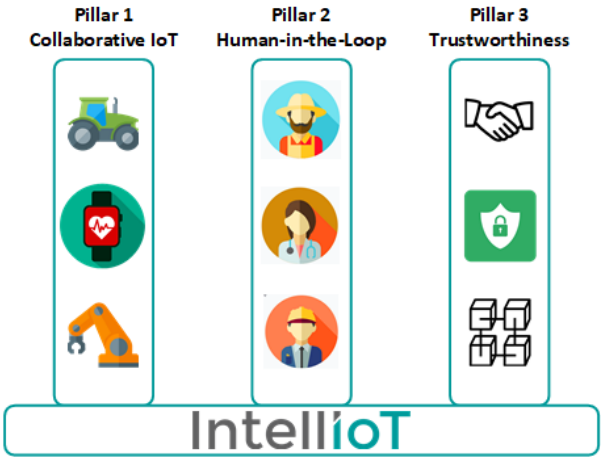


Figure 1: Three pillars of IntellIoT

1) **Collaborative IoT:** Various semi-autonomous entities (e.g., tractors, robots, healthcare devices, etc.) need to cooperate in order to execute multiple IoT applications. These entities have to be self-aware, and all have a different amount of knowledge of the task at hand and their environment where they are located. Unfortunately, it is not always possible to provide all the necessary knowledge to the entities, especially in

changing environments. To keep the knowledge of the entities up-to-date, they need to extend it by applying learning technologies based on Artificial Intelligence and Machine Learning. New knowledge can either be acquired by interacting with the environment (via sensors) or by interacting with the other entities in the environment. By exchanging information via a reliable and secure communication network, the entities in the environment need to collaborate with each other to update their own knowledge to fulfil their assigned task.

2) **Human-in-the-Loop**: The human within the system will keep on playing a crucial role in the whole process. The aim is not to remove the human from the system but use his/her experience and knowledge to overcome unknown situations, where the system does not have the knowledge (yet) to handle the situation and the collaboration with the other entities in the field also does not provide the required information. The interaction with the human (be it either the machine operator, the farmer, the physician, or any other person) will enable the intelligent system to expand its knowledge about the environment or the application through machine learning technologies and use the experience from the human operator to learn new features or information about the overall process. Therefore, human will remain a vital element of the system and will interact with the IoT elements in the system to overcome the current limitations of the system.
3) **Trustworthiness**: Security, privacy and, ultimately, trust are considered as indispensable preconditions for reliability and the wider acceptability of distributed, collaborative IoT systems and applications. Trust of the human (e.g., a patient or farmer) in the system is key, as the system's (autonomous) decisions need to be trusted, and the end-users' data need to be handled with utmost care, by providing appropriate levels of security and privacy safeguards. In this context, and in addition to well-understood security and privacy best practices, IntellIoT will adopt advanced security intelligence to protect unsupervised device-to-device interactions, based on self-adaptable, security-related operations. Furthermore, the overall trust will be fortified by continuous monitoring, real-time assurance assessment, and primitive enabling transparency of performed actions. Distributed ledger technologies (DLT) and smart contracts will be made accessible by IoT devices and other actors in the use cases to show transparency of performed actions, create trustworthy supply chains, and build trust between parties.

The above three pillars also help group the activities within the use cases. As mentioned before, all the use cases have identified three different scenarios each, that will be used to demonstrate the different technologies applied within the use case areas (i.e., agriculture, healthcare, and manufacturing). In the first scenario, the focus in all the use cases will be on the collaborative IoT concepts, where the entities in the use cases will collaborate to achieve their goals. The second scenario in each use case will focus on the interaction between the systems and the humans involved in the use cases. Examples of humans involved are plant operators, physicians, or remote operators of tractors. The third scenario, that focuses on trustworthiness, has a special place within the use cases. To demonstrate the trustworthiness of the systems, the technologies developed have to be applied to the solutions in the other scenarios, namely collaborative IoT and Human-in-the-Loop. Therefore, the pillar Trustworthiness is in fact overlapping ("horizontal") over the other two pillars.

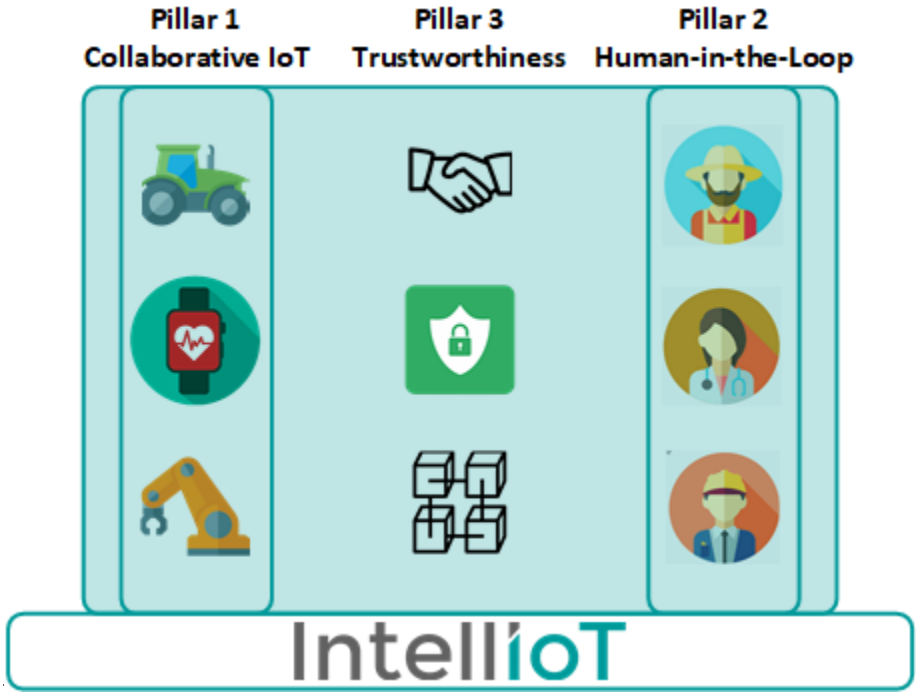


Figure 2: Three pillars of IntellIoT and associated scenarios (Trustworthiness overlapping other two)

2 USE CASE DESCRIPTIONS

This section aims to present and provide an in-depth analysis of the three different use cases that the IntellIoT project will focus on.

2.1 Use Case 1 – Agriculture

2.1.1 SCOPE AND OBJECTIVES

Within the agricultural domain, the industry has already successfully implemented "smart farming" features, which focus on the detection of the crop's needs and problems, e.g., fertilizer and water application and crop spraying according to the needs of individual plants, rather than treating large areas in the same manner. These features have already introduced a high level of automation and have saved millions of tons of fertilizer, pesticides, insecticides, etc.[1] The missing link for optimizing farming activities (e.g., ploughing, spraying, harvesting etc.) is heading in the direction of autonomous operations, in order to optimize resources, increase the level of efficiency, improve the safety and security of autonomous vehicles in the field of farming, and additionally reduce costs significantly.

Nowadays, farmers are driving agricultural vehicles for many hours during the day, resulting in fatigue and finally in (potentially deadly) accidents[2]. The ultimate aim is to remove the farmer from the cabin and have the agricultural vehicles drive autonomously over the farming fields, performing their tasks (e.g., harvesting) by themselves, thereby using the available data to optimize their required behaviour. However, the aim of having a human operator completely taken out of the loop and have the tractor perform its tasks completely autonomous is still not completely feasible. Therefore, currently much research is on the topic of autonomous operation. Nevertheless, within the agricultural use case, we will investigate concepts related to bringing more and more autonomy to agricultural vehicles.

The scope of the agriculture use case is to investigate future autonomous features of farming vehicles, like autonomous driving, decision making and interaction and reliable communication with other (smart) entities (e.g., vehicles, drones, sensors, manipulators) in the field. The interaction between the different entities in the field will create an intelligent IoT environment, where the different entities securely interact with each other and use this knowledge to update their own internal knowledge of the environment. Such knowledge is utilised to enhance the decision-making capabilities and communication aspects. Although the goal is to remove the farmer from the cabin, humans should still play a big role in the control or supervision of the overall system. In this context, the aim of this use case is to incorporate the human-in-the-loop in the intelligent IoT environment of a semi-autonomous agricultural vehicle in collaboration with other devices on the field, while improving safety, reliability, and security. Human intervention is needed in uncertain situations (e.g., animals on the path, dust or other particles, obstacles) and it is especially valuable in the initial deployments of smart farming. Since the agriculture use case is dealing with dynamic environments and fluctuating availability of devices (e.g., tractors, drones), these dynamics should be handled by the system. To accomplish this, we introduce autonomous agents that can be programmed in a no-code environment by a user with relevant domain knowledge (e.g., a farming engineer).

To validate the above, the objective of the agriculture use case is to deploy and demonstrate a prototype of a self-driving tractor in a connected environment by equipping a fully electrified tractor with new technologies, like cameras, communication, machine learning, interaction capabilities, etc. To validate the above, the objective of the agriculture use case is to deploy and demonstrate a prototype of a self-driving tractor in a connected environment by equipping a fully electrified tractor with new technologies, like cameras, communication, machine learning, interaction capabilities, etc. These will be augmented by a set of innovative security enablers, aiming to provide a trustworthy-by-design environment for all involved stakeholders.

---

[1] Lieder, S., Schröder-Schlaack, C., „Smart Farming Technologies in Arable Farming: Towards a Holistic Assessment of Opportunities and Risks.", Sustainability 2021, 31, 6783. https://doi.org/10.3990/su13126783

[2] Health and Safety Authority, "Fatal accidents," December 2019. [Online]. Available: https://www.hsa.ie/eng/Your_Industry/Agriculture_Forestry/Further_Information/Fatal_Accidents

2.1.2 DESCRIPTION OF THE USE CASE

As mentioned above, the agriculture use case will investigate different technologies for future autonomous farming activities, but in the first place mainly focusing on improving autonomous operation for agricultural vehicles. The consortium has identified different technologies (e.g., machine learning, 5G communication, security, human-machine interaction, hypermedia multi-agent systems) that will be further developed and applied to the identified scenarios for the agriculture use case (see Section 2.1.6).

The high-level concept of the agriculture use case is depicted in Figure 3. The use case will cover multiple facets of a smart agriculture deployment, where a tractor is driving over a farming field. The tractor will be equipped with sensors and computing resources to perform the mission assigned to it. The computing resources integrated into the tractor will enable it to perform computation tasks locally, thus acting as an edge device. Besides the tractor, there will be other edge devices in this use case, like the mobile platform from the Open Call winner or an infrastructure 5G MEC.

Concretely, in this use case, a farm engineer first configures a Hypermedia Multi-agent System (HyperMAS) with the required procedural as well as organizational knowledge to appropriately react to user tasks. The procedural knowledge includes specifications of which services need to be invoked by autonomous agents that run in the HyperMAS, where the interfaces of these devices are described by means of W3C WoT Thing Descriptions; the organizational knowledge specifies the roles of these agents to allow decomposition of tasks at run time. Then, the end user (i.e., the farmer in this UC) specifies a goal (e.g., that "Field A shall be harvested") using a Web front end. This goal is sent to the HyperMAS for execution by the configured agent organization. The central aspects of these tasks are way points in the field where the tractor should move, together with information about what action it should perform at these way points and in-between (e.g., harvesting). If an unknown obstacle is encountered, the AI will try to identify a way to bypass the obstacle using a pre-trained model. If the confidence of this decision is below a pre-defined threshold, the AI will trigger a human operator to remotely navigate it. Via the HIL Service, the human operator gets notified and will take control of the tractor.

In the situation where an unknown situation is detected and the vehicle does not know how to overcome it, it will first try to collect complementary information or knowledge from possible other entities via the Infrastructure Assisted Knowledge Management (IAKM) component. If required or compatible information cannot be found, the vehicle will stop and request help from the human operator. Utilizing a 5G NR connection, data from the tractor's sensors is sent to the VR glasses of the human operator. Part of the sent data is a video feed which will allow a view of the situation of the vehicle. The human operator will execute strategies where he can directly interact with the vehicle (i.e., moving the vehicle forwards or backwards) using VR controllers. The information coming from the human operator will be stored along with the associated video frames. The vehicle will refine its own local AI model by learning from the stored data after enough human interventions have been collected.

Distributed Ledger Technologies (DLTs) will further ensure that the data and information, and interactions between agents and edge apps are transparently recorded and immutable, covering both cases of operation (with or without human intervention). Besides, smart contracts allow timely processes of exchange and payments between stakeholders that can be triggered by data changes appearing in the ledger.

Furthermore, security concepts will be applied to allow access only to authorized devices but also to mitigate any intrusions to the network. While the vehicle is performing a mission, and a malicious entity (e.g., another tractor that has been compromised by an attacker) tries to harm that mission, the security mechanisms should be activated. The vehicle or its peers must identify the malicious entity and notify the backend infrastructure, taking measures to isolate the malicious entity, while making sure the vehicle, as well as any other legitimate entities continue functioning. To pre-emptively protect the network, periodic actions will be taken to dynamically reconfigure it, thus making any knowledge an attacker might have gathered, obsolete. Finally, for potential limited-resource devices that are placed on the field (e.g., smart-sensor type devices) that require co-operative communication mechanisms in order to reach the main computing infrastructure, secure routing algorithms will be used to relay packets from source to destination.

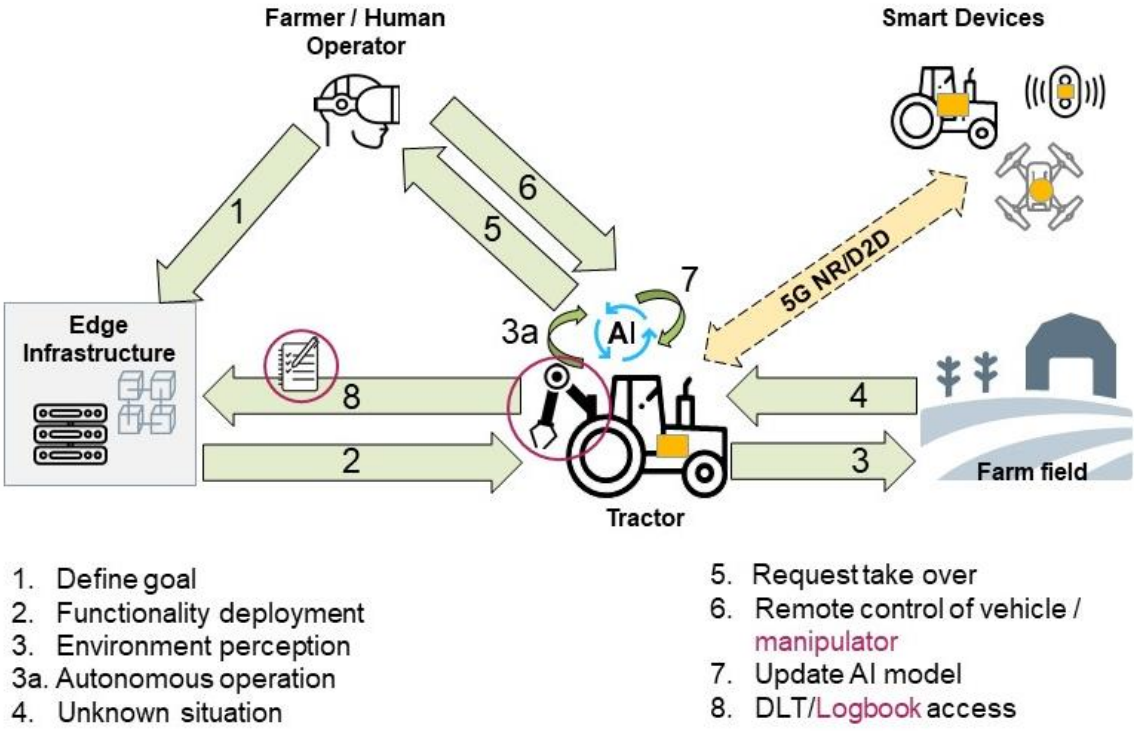


Figure 3: Agriculture use case (in red the contribution from the Open Call)

2.1.3 MARKET SITUATION AND CHALLENGES

Farming employment in the European Union has been steadily declining for decades and has fallen from 13.1 million Annual Work Units in 2003 to 9.1 million Annual Work Units in 2018 across the EU-27, representing an impressive 30% decrease in the last fifteen years[3]. Additionally, the average age of the farmers has been rising drastically, with only one in ten EU farmers (11%) were under the age of 40 years old in 2016[4]. Nevertheless, the amount of people living on earth will steadily increase and all need food to live. Farmers will have to produce 70 percent more food for an additional 2.3 billion people by 2050 to sustain the whole world population, according to the UN Food and Agriculture Organization (FAO)[5]. Therefore, farms and agricultural operations will have to be run very differently from nowadays, which will also be influenced by advancements in technology such as sensors, devices, (mobile) machinery and information technology. Future agriculture will use sophisticated technologies such as robotics, temperature and moisture sensors, aerial images, and GPS technologies. These advanced devices and precision agriculture and robotic systems will allow farms to be more profitable, efficient, safe, and environmentally friendly.

Unfortunately, the integration and usage of new technologies, or even existing technologies, also bring dangers with it, especially in the agriculture domain. The large machinery is difficult to control, especially with the growing age of farmers. Many fatal accidents happen in the agriculture area, especially with tractors and other vehicles[6], be it either in conjunction with other vehicles or caused by the human operator of the device. Discussing this topic also in the end-

[3] The EU Farming employment: current challenges and future prospects, [online], https://eprints.glos.ac.uk/7629/1/IPOL_STU(2019)629209_EN.pdf
[4] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Farmers_and_the_agricultural_labour_force_-_statistics
[5] https://www.fao.org/news/story/en/item/35571/icode/
[6] https://www.hsa.ie/eng/Your_Industry/Agriculture_Forestry/Further_Information/Fatal_Accidents/Fatal_Accidents.html

user workshops of the project, this appears to be one of the main challenges in this domain. Making the work with agricultural vehicles safer is a very challenging and difficult task to solve. One of the approaches is to bring more autonomy onto the farm, thus creating future autonomous vehicles. First approaches are being made or are available on the market[7], but are still not available for many farmers, especially the smaller farmers in Europe. New solutions must be made available that bring this improved autonomy to the market for the smaller farmer.

Another challenge risen during the end-user workshop is that the agricultural machine manufacturing industry has been showing declining figures. Only since the last year, the numbers are rising again[8], but still not as impressing as it used to be. Instead of coming up with completely new vehicles, which are most often expensive, it is better to come up with smaller solutions that can be integrated in legacy systems, which makes it more affordable for the smaller farmer to keep up with the developments offered by the market.

With a growing planet population and significant challenges due to health issues, climate change and other factors, the agriculture sector will become the centre of attention in the years to come. Not only the quality of the crops has to be improved but also the efficiency and overall output of the production is estimated to arise between 40-54 percent till 2050 compared to 2012, as estimated by the United Nations' Food and Agriculture Organization[9]. Among the proposed solutions to achieve this overly ambitious (yet extremely important) milestone, smart farming and precision agriculture stands at the epicentre. This puts significant pressure on the development of technology solutions at the device, network, and application layers in order to produce highly precise, safe and efficient systems that will enable the farming industry to maximize food production under diverse environmental conditions, reduced costs, minimal waste and increased safety for all working personnel.

Furthermore, the wide application of ICT technologies in the agricultural domain (usually falling under the broad category of Internet-of-Things (IoT) applications because of their interconnected nature that spans from the tiniest devices to cloud computing infrastructures) and the expected high reliance on the services that they will provide, creates a number of challenges10. Securing the infrastructure, protecting core data, and ensuring the integrity and trustworthiness of information exchanged and stored at all levels is crucial11. As agriculture is of vital importance to the population, any disruptions in food production systems may have consequences that cannot only be measured in terms of financial costs or losses and this only makes them a more esteemed attack target from malicious entities, that may include terrorist activities, state-sponsored attacks, blackmailing efforts, and other rising threats. Cyber-security, therefore, emerges as a design consideration that must be included in all steps of ICT infrastructure development for the agricultural domain. It comprises of a combination of techniques, skills and processes required to ensure a high degree of protection for network, computers, programs, and data, against malware, attacks, damage, and unauthorized access. It exists to counter threats that include ransomware, endpoint attacks, phishing, third party attacks, supply chain attacks, artificial intelligence and Machine Learning-driven attacks, crypto-jacking, cyber physical attacks, IoT attacks, threats to smart devices, attacks on connected, semi-autonomous or autonomous vehicles and more. It needs to account for defenses against both well-known kinds of the attacks as well as possible future types of malicious acts that target yet undiscovered vulnerabilities of the computing and network infrastructure.

2.1.4 TECHNOLOGIES OF THE USE CASE

Actors, components, and associated technologies playing a considerable role in the use case are described in the following subsections.

---

7 https://www.deere.com/en/news/all-news/autonomous-tractor-reveal/

8 https://www.cema-agri.org/images/publications/press_releases/2022-03-21-CEMA_Economic_Press_Release_Tractor_Registrations_2021.pdf

9 https://www.fao.org/publications/sofa/sofa-2021/en/ The state of Food and Agriculture 2021, p.4

10 https://doi.org/10.3390/s20226458 Survey on Security Threats in Agricultural IoT and Smart Farming

11 https://doi.org/10.1007/978-3-030-31703-4 Cyber Security: The Lifeline of Information and Communication Technology

2.1.4.1 ETRACTOR

AVL provides a fully electric vehicle (see Figure 4) that is the platform for the implementation of semi-autonomous functions. Using a sensor array it is possible to provide a digital representation of the local environment. Data can be sent or received via the Tractor Controller, which acts as an IoT-Gateway. The tractor has two electric driven axles - each of them with a maximum power of 25 kW, as well as a hydraulic steering system. The various components appear in Figure 5, and some additional details are provided below.

Figure 4: AVL e-tractor platform

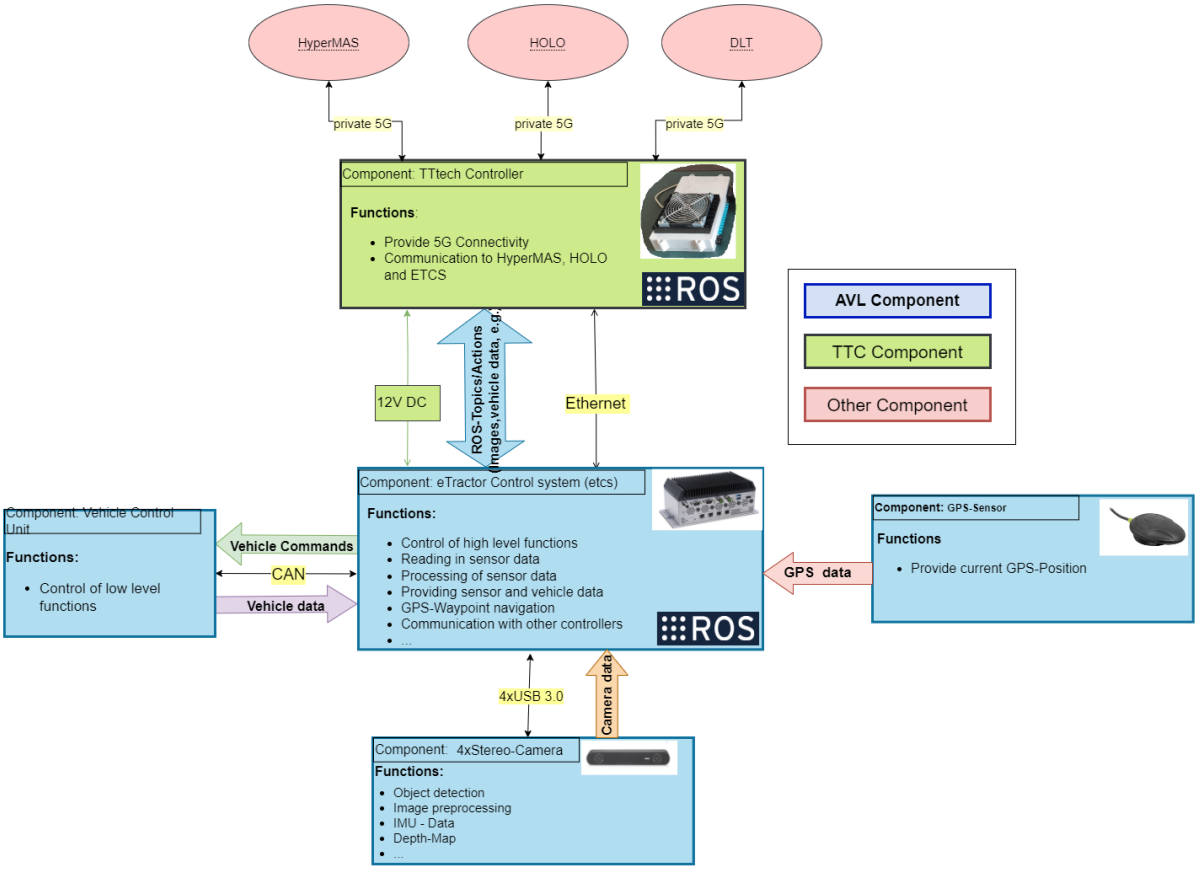


Figure 5: Signal Flow Tractor Control

Vehicle Control:

A vehicle controller is installed on the tractor to control the low-level functions – hydraulic management, cooling management, energy management, driving and steering. The controller provides a CAN-interface that allows to get signals from the eTCS and to control the driving functions. The eTCS enables other members of the IoT infrastructure to take control of the tractor and operate it remotely. Three operating modes are available for this purpose.

- **Waypoint-operated:** The eTractor receives mission targets (1 … n), which consists of GPS points (latitude, longitude, heading) and an action (spraying, ploughing, etc.), which are tried to be accomplished
- **Manual-operated:** The tractor can be controlled by cyclically obtaining a target speed, as well as a target steering angle.
- **Routine-operated:** The tractor can be controlled by time-triggered move commands

Perception:

Mounted on the tractor are four 4k Stereo cameras which provide a 3D-representation of the local environment (see Figure 6). In addition, the eTractor has a compass, GPS and IMU sensors. The respective sensors are provided as a topic and can be requested via the IoT gateway from the individual clients

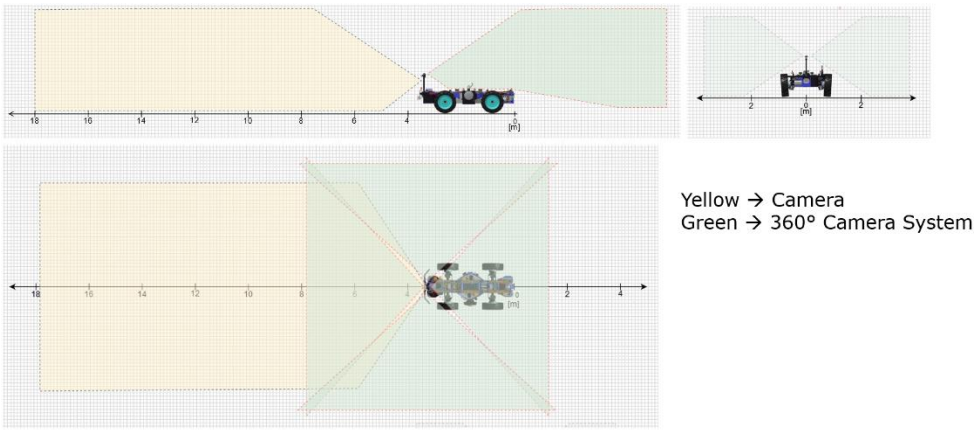


Figure 6: Camera system of the tractor

2.1.4.2 ARTIFICIAL INTELLIGENCE FOR OBSTACLE BYPASSING

AI is integrated into the use case to facilitate the autonomy of the system. The goal of the AI model is to help the tractor bypass the detected obstacles. In the presence of obstacles, the tractor controller requires a command sequence that corresponds to a tractor maneuver without collisions.

Training of the AI model is carried out in a supervised learning fashion. In this view, an AI model is pre-trained using labelled data corresponding to navigations around obstacles (by a human operator). These data include the recorded information related to sensing (e.g., video data from onboard camera) and controlling (e.g., linear, and angular velocity components that are normalized into a scale from 0 to 100). Here, the former is used as the input and the latter is used as the label. First, to reduce the computation complexity with high-dimensional sensing information, the video data is rescaled and compressed to generate low-complex inputs. Then, a convolutional NN (CNN) model is trained to regress the labelled control information and a measure of its confidence from the input sensory data. The choice of the NN architecture is to extract the higher order features from the time-dependent visual data and the selected regression loss function will ensure that the output of the trained CNN model is almost equivalent to the labelled control information.

The inference initiates with a manoeuvre request. During the inference, using the sensory information (e.g., camera feed), the AI model generates a sequence of control information that are to be used by the tractor controller to safely bypass the obstacle. The confidence inferred by the AI model is compared with a predefined confidence target, in which, human support is requested when the confidence drops below the target as a safety measure. With a human takeover, during the remote control, both the sensory and control information that have the same structure as the training data is stored as a new labelled training sample. Over time, using enough new data, the AI model is retrained to improve its performance.

2.1.4.3 HIL APPLICATION & HUMAN OPERATOR

Human Operator refers to the user of the HIL Application. The Human Operator will connect to the HIL Application through the ISAR Client installed on the Oculus Quest 2. Once connected, the application's content will be streamed to the VR device where the user will be greeted with a tractor's dashboard containing data describing the real tractor's status. The Human Operator will have a surround view of the real environment through the camera streams. At this point, the Operator has already taken over the control of the tractor and will remotely try to solve the issue it encountered. Once successful, he returns the control back to the AI.

2.1.4.4 MALICIOUS OPERATOR

We define as malicious operator an adversary that tries to hamper normal system operation. For example, a malicious operator could gain access to a tractor and seize its operation. The implications of such an action could range from damaging the tractor itself, the crops or even driving it outside of the desired area.

2.1.4.5 IOT INFRASTRUCTURE

The IoT infrastructure is responsible of allocating service resources that enable the cooperation among components and the execution of the IoT application functions. This allocation must be highly dynamic to adapt to the changes in the intelligent IoT environment. This is supported through three components that interact to achieve the IntellIoT goals:

2.1.4.5.1 HYPERMEDIA MULTI-AGENT SYSTEM (HYPERMAS)

The functional integration between the components will be based on interacting agents within a HyperMAS. The components of the use case (tractor, drones, sensors) will be tethered to software agents that will be able to, together, proactively plan component behaviour while staying reactive to environment changes. These agents will in turn be integrated with each other, with (physical) artifacts, and with their environment using proven mechanisms from the Web architecture -- specifically, uniform hypermedia interfaces -- where we aim for a conceptual integration rather than merely a technological integration: the resulting multi-agent system is not merely layered on top of the Web but is integrated in the Web's hypermedia fabric to enable the inheritance of its desirable architectural properties (e.g., scalability and evolvability).

2.1.4.5.2 EDGE INFRASTRUCTURE / PRIVATE 5G MEC INFRASTRUCTURE

The private 5G MEC infrastructure provides an Edge service to the tractor and the UC. The Private 5G MEC is deployed next to the Private 5G infrastructure (5G gNB) and will provide APIs to control the 5G network characteristics. Moreover, it will enable hosting of edge microservices, such as the AIKM server, the global AI or the DLT manager.

2.1.4.5.3 INFRASTRUCTURE ASSISTED KNOWLEDGE MANAGEMENT (IAKM)

The IAKM server component will be deployed on the Private 5G MEC infrastructure and will provide local storage for AI/ML models. The IAKM client component will be deployed on the tractor and will offer HTTP APIs to the local AI agent to query for a particular AI/ML model. If the AI/ML model is found in the IAKM database, it will be provided to the tractor over the 5G network. Optionally, if not, an appropriate AI/ML will be queried to another IAKM server on a different Private 5GMEC and provided to the local AI agent. AI/ML semantics will be used to identify the AI/ML and its usability context.

2.1.4.6 TRUST COMPONENTS

Several components are also deployed that support the trustworthiness aspects of the agriculture use case, as presented in the subsections that follow.

2.1.4.6.1 SECURITY ASSURANCE PLATFORM

The Security Assurance Platform (SAP) will provide runtime, continuous assessments of the monitored agriculture UC deployment. In general, this enabler will form a core integration point of all trust enablers within IntellIoT.

In the context of the specific use case the role of the Assurance Platform will be to provide the operator with the capability to carry out assessments (e.g., vulnerability assessments), while also providing a view of the assurance posture of the deployment. SAP will also facilitate response to changes in said posture, as detected by the integration with the needed event captors and the trust-based IDS enabler (see sect. 2.1.4.6.2). The timely and efficient response will be achieved by triggering changes in the MTDs (sect. 2.1.4.6.5) deployed in the UC environment. All such events will be relay to the SAP. Throughout its operation, the Assurance Platform will also interface with the DLT building blocks, allowing the evidence-based operation of the assurance scheme.

2.1.4.6.2 TRUST-BASED INTRUSION DETECTION SYSTEM (IDS)

In the Agriculture Use Case, all devices that participate in the functioning of the system (e.g., tractors, smart sensors, drones) are pre-validated and initially configured by trusted authorities. No ad-hoc connections from external entities are generally allowed. As such, the way for a malicious user to infiltrate the network is to gain access to a certain node that used to be considered trustworthy. The security components need to account for such a break-in attempt. To do so, a Trust-based Intrusion Detection System continuously monitors the behaviour of all nodes in order to validate that they keep on performing untampered. Each node in the network maintains a trust table for all the nodes that it has direct communication. If a node is observed to behave improperly according to some predefined properties (e.g., send an extraordinary number of packets) will have its trust value reduced by all other nodes it communicates with and eventually this will lead towards alarms to security components (Security Assurance Platform and MTD) that can perform proper actions to block or isolate the misbehaving node.

2.1.4.6.3 SECURE ROUTING

Wireless sensor networks are wireless ad-hoc networks that mainly contain sensors with limited resources, e.g., computation, storage, and power. The IoT Edge of the agriculture environment is expected to contain such networks. This prevents us from using conventional cryptography to establish a trusted communication channel between nodes. It is necessary for the routing protocols to establish trust relationships to guarantee the validity of the transmitted data.

2.1.4.6.4 AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

AAA provides centralized authentication, authorization, and accounting services. External entities employ these services to communicate with nodes that are part of an IntellIoT scenario in a safe and controlled manner. Two deployment types are available in order to facilitate services that support OAuth2 protocol as well as those that do not. The first case is straightforward; this kind of services communicate directly with the AAA component. For the second case, a reverse proxy is employed. It handles the OAuth2 protocol and acts as a middleman between the services and the external entities. For the agriculture use case, AAA will be used to secure the backend API calls.

2.1.4.6.5 MOVING TARGET DEFENCE (MTD)

Moving Target Defence (MTD) is a technology that changes the network configuration (or certain of the properties of the communication channels such as encryption algorithms or keys) dynamically over time, in order to interrupt and mitigate possible attacks because of the resulting increase in complexity and time costs for the attacker. Even if the attacker succeeds in compromising the system in a specific configuration, its benefit will be low due to the limited lifetime of that configuration and the diversity of the system.

In the agriculture scenario, when the Security Assurance platform identifies a malicious node (through an IDS notice or otherwise), the MTD is called upon to change the network configuration in order to isolate the attacker and sustain normal system operation. Beyond this reactive way to protect the network, the MTD component periodically performs changes to the network configuration to proactively deter potential attacks.

2.1.4.6.6 DISTRIBUTED LEDGER TECHNOLOGY (DLT)

A DLT system offers a tamper-proof ledger distributed on a collection of communicating nodes, all sharing the same initial block of information, synchronizing the common states.

In order to add information to the DLTs , a client formats information in DLT transactions in a block with a pointer to its parent block, this creates a chain of blocks, hence called "Blockchain". The terms Blockchain and DLT can be used interchangeably. To create a block, a node usually needs to solve a crypto-puzzle and provides the solution as a proof of its work to get a reward. This process is called mining. The difficulty of the crypto puzzle is adjusted based on the total computational power or mining power of the DLTs network which use Proof-of-Work Consensus. Each correctly behaving miner needs to adhere to the same protocol for creating and also validating new blocks. Upon successfully mining a block, a miner broadcasts it for validation.

Based on the nature characteristics of DLTs e.g., DLTs can contribute to building a trusted and transparent distributed IoT system applied in agriculture domains. DLTs promise a reliable source of truth about the state and work progress of farm workspaces, and inventories via DLT-based smart contracts towards smart agriculture, where the collection of such data is often significantly expensive. The DLTs can also track the provenance of goods and help create trustworthy supply chains and build trust between producers and consumers. In specific, we implement the integration of DLT with tractor controller to accounting the activities of tractors, e.g., position, task activities.

2.1.5 OPEN CALL #1 CONTRIBUTION

The company IKnowHow (IKH) from Athens, Greece has been the winner of the Open Call #1 for the agriculture use case. IKH is developing "Greenbot"; a self-navigating ground vehicle, fitted with a robotic manipulator for performing activities in the frame of precision agriculture. The platform is depicted in Figure 7.

Figure 7: IKH's precision agriculture robot (Greenbot)

Within IntellIoT, IKH will develop the following distinct components to expand the foreseen developments of IntellIoT:

1. Trusted Farmer's logbook that will be used for certification procedures, thereby using the Security Assurance Platform and Distributed Ledger Technologies.
2. Remote operation of the manipulator and the AGV by the human operator – use of VR.

3. 5G connectivity

More details on the above are provided in the subsections that follow.

2.1.5.1 FARMER'S LOGBOOK

IKH will develop a web-based, mobile friendly application for enabling farmers to log their daily activities on the farm. These activities may include application of fertilizer, pesticides or other special treatments, observations, harvesting, etc. The application will also log activities performed by the robot, e.g., the scanning of a specific pest. It will be built upon IntellIoT's DLT-based monitoring capabilities, to ensure trustworthiness and tamper proof records. Connectivity with the SAP will also be examined, in cases that the DLT and associated Logbook data can be used to detect trust-related incidents that must be recorded & mitigated.

2.1.5.2 REMOTE VR BASED OPERATION

IKH will develop a VR application (see Figure 8) based on the IntellIoT's developments in Unity3D for the teleoperation of the vehicle itself and the robotic arm mounted on top of it. The user using either keyboard/mouse controls or a more natural interface based on hands movement will be able a) to see through the AGVs cameras the environment of the robot, b) move the AGV in any direction and c) control the robotic arm in order to move the actuator closer to a point of interest. This development will further develop IntellIoT's human in the loop concept allowing the robot to notify a human operator when reaching a situation, it cannot handle.

Figure 8: UR10e digital twin in VR

2.1.5.3 5G CONNECTIVITY

IKH will integrate its robot in the 5G infrastructure provided by IntellIoT and provide to the consortium any ROS module developed for that purpose.

2.1.5.4 ARCHITECTURE

In Figure 9 below one can see an initial proposition on how Greenbot can be integrated into IntellIoT's high-level architecture. In addition to the components described in the previous subchapter, optional integration with IoT sensors is foreseen as also off-loading of the DL computation to the edge infrastructure.

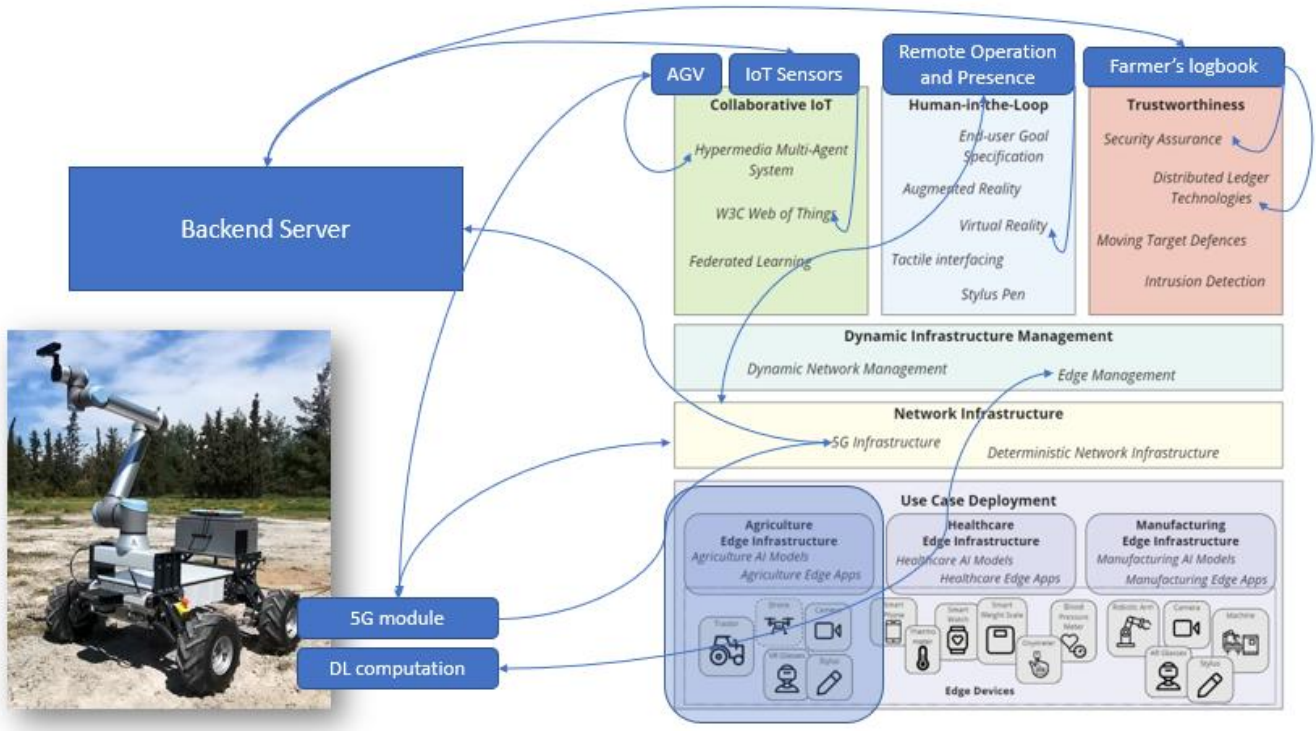


Figure 9: Architecture integration proposition

2.1.5.5 INTEGRATION AND DEMONSTRATION

IKH's robot and all the developed software will be demonstrated in Austria at AVL's premises during September 2022. Software integration between the different components, developed by IKH, and the infrastructure provided by IntellIoT will be performed throughout the duration of the project following a continuous interaction with other partners involved in the use case.

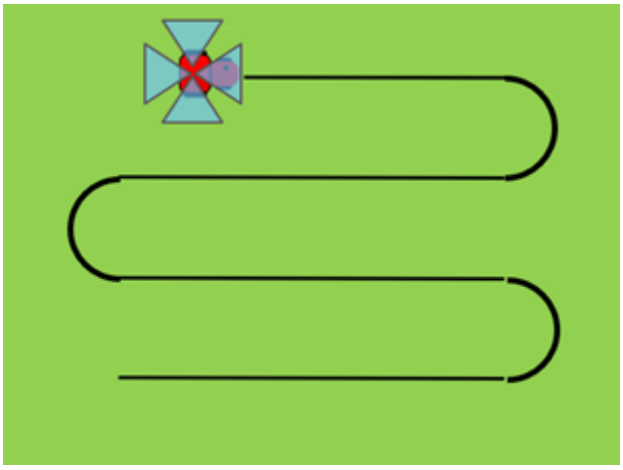
2.1.6 SCENARIOS

2.1.6.1 SCENARIO 1.1 – COLLABORATIVE IOT

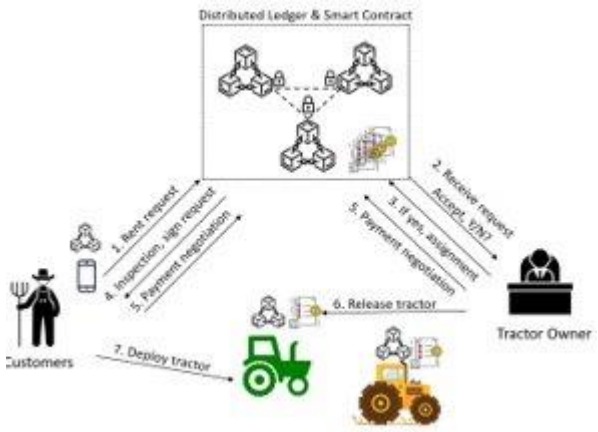
Scenario Name	Collaborative IoT
Scenario ID	UC1-Scenario1
Partners	TTC, AVL, EURECOM, HOLO, HSG, SANL, AAU, TSI, UOULU

Description	This scenario deals with the operation of the tractor in the field. The farmer will specify a goal for the tractor, which could be e.g., ploughing or spraying of a field. The mission consists of an assigned field, where a waypoint service calculates waypoints that the tractor needs to follow. These waypoints are assigned to the tractor by agents within the HyperMAS. The tractor platform is equipped with sensors to recognize the tractor environment and an E-tractor control system (ETCS) to operate the tractor. The sensor input is pre-processed and when an obstacle is detected within the FOV (Field of View) of the tractor, this can be reported. The data corresponding to the obstacle bypassing AI, will then be used to infer the control information by utilizing the obstacle bypassing AI in the tractor. Towards improving the success of the mission completion, the tractor utilizes the 5G-Infrastructure to potentially collaboratively update its internal knowledge with other entities in the same or different fields through the IAKM component. DLTs enable the trackability and traceability of information that various actors and stakeholders generate throughout the entire value-added process, from seed to sale. The DLT ensures that the data and information are transparently recorded and are immutable. Besides, smart contracts allow timely processes of exchange and payments between stakeholders that can be triggered by data changes appearing in the ledger.
Key Scene	**Key Scene 1.1**: The farmer specifies a goal to be performed by the agricultural vehicle and transmits it to the HyperMAS. This goal defines the task to be performed by the vehicle, the components (e.g., which tractor, what kind of implement, etc), and the targeted field/area. A dedicated user interface will be made available where the farmer can specify the goal and the field that needs to be processed.  **Key Scene 1.2**: An agent that runs in the HyperMAS detects available resources (i.e., vehicles, implements, etc.) and allocates them to the tasks at hand. Additionally, it uses a waypoint service to find waypoints, and continually sends these waypoints to the tractor which will automatically drive there. Additionally, it uses a waypoint service to find waypoints, and continually sends these waypoints to the tractor which will automatically drive there.

Key Scene 1.3: The tractor automatically navigates to the given waypoints continuously received from the agent and performs the assigned tasks. (e.g.: plough, cultivator, planter, sprayer).



Key Scene 1.4: During the task operation, it can happen that an unknown situation occurs, for example that an obstacle is in front of the tractor and it doesn't know how to pass by it. Based on trained model, the AI inside the vehicle should be capable of proposing a solution to bypass the obstacle. When the AI fails to make a reliable decision, if available, the tractors refer to the IAKM for the supported AI technologies on the IoT-Infrastructure having access to all cooperative devices. Depending on the requirement, the tractor and Edge Infrastructure securely shares either raw/processed data (e.g., vehicle data, GPS position, video data (3D), detected objects) or update obstacle bypassing AI models via the IAKM component. If the problem persists, the tractor stops and sends a message to the operator (see scenario 1.2).

	 **Key Scene 1.5:** The tractor fleet has at least one tractor from a third-party service provider. This key science can be shown by simulations. Distributed ledger and smart contract are used for contractual agreements, to confirm the ownership and agreement of the tractor for rent services. 
Potential Variation of the Scene	[1] Different weather or environmental conditions (e.g., dust particles, rain) can influence the information coming from the sensors, causing false-positives or false-negatives. [2] Parallel driving behaviour between multiple vehicles, for example a harvester and a tractor for unloading.
Purpose	The purpose of this specific scenario is to establish AI driven tractors and potentially other farming entities (e.g., sensors, drones) that are actively collaborating. They will learn based on their experiences in the field and interact with each other to overcome unknown situations, without any human interaction.
Sources of Risk	[1] No reliable communication connection between the vehicle and the other entities or the IoT-Infrastructure [2] Poor GPS signals, resulting in a situation where the vehicle doesn't know where it is located and therefore can't move to the correct waypoint [3] Controller fails to make a reliable decision

	[4] Controller issues a wrong command [5] Sensor misalignments [6] Overloaded IoT-Infrastructure [7] Humans that are entering the field and are challenging the vehicles (standing in front of it) and see if the vehicle reacts accordingly to the (mobile) obstacle.
Threats	[1] Malicious external parties can take over control of the vehicles and create dangerous situations by moving the vehicles in areas where it is not allowed to go. [2] Wrong/inconsistent input signals from external devices can lead to wrong decisions. [3] Misalignments or damaged sensors due to intentional (malicious external party) or unintentional (animals, trees, dirt) situations.
Precondition for the Scenario	[1] Wireless Connection [2] GPS Signal [3] Mission defined by the operator [4] Moderately trained controller
Successful end condition	Mission is completed as initially planned by the operator.
Failed end condition	Tractor stops and cannot finish the mission – e.g., tractor is blocked.
Fatal end condition	The tractor is damaged, or the environment (e.g., field, crops) is damaged.
Frequency of occurrence	This is the standard behaviour of the tractor, so this is a scenario that will constantly occur. Each time the tractor is set out on a mission, this scenario will take place.
Actor(s)	Tractor, 5G private infrastructure, Agents in the HyperMAS, Human operator DLT
Information exchange between actors	[1] Human → Agents in the HyperMAS: definition of the goal [2] Agents in the HyperMAS → Tractor: definition of the path [3] Edge Infrastructure → Tractor: updated AI Model [3] Tractor → DLT Manager: Status information about the tractor. This information can include telemetry, sensor information, process information, etc. [4] Tractor → IAKM: requests for additional information, like e.g., map data including unidentified obstacles, ML object/AI models.
Challenges for scenario validation (T5.3)	[1] Reliability of the environment perception with the 360 degrees camera and the 3D camera [2] Providing image/video data in a suitable format and data size [3] Accuracy of the trajectory calculation of the tractor [4] Communication reliability [5] Data exchange and learning capabilities of the individual entities in the field
Changes with respect to D2.1	• Deleted former key scene 1.5, which is covered by scenario 2. In scenario 1, the tractor is not transmitting the data to the human operator, so it can be deleted.

	• Updated key scene 1.4, explaining how the obstacle bypassing AI could be updated using other AI models if available in the system. • Updated scenario description by deleting the explicit usage of the drone. The target was to have an Open Call partner that would provide a drone to the use case, which didn't happen. As there is no drone available in the use case, the description was updated accordingly.

Figure 10 provides a UML-based diagram of the scenario. This figure shows the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

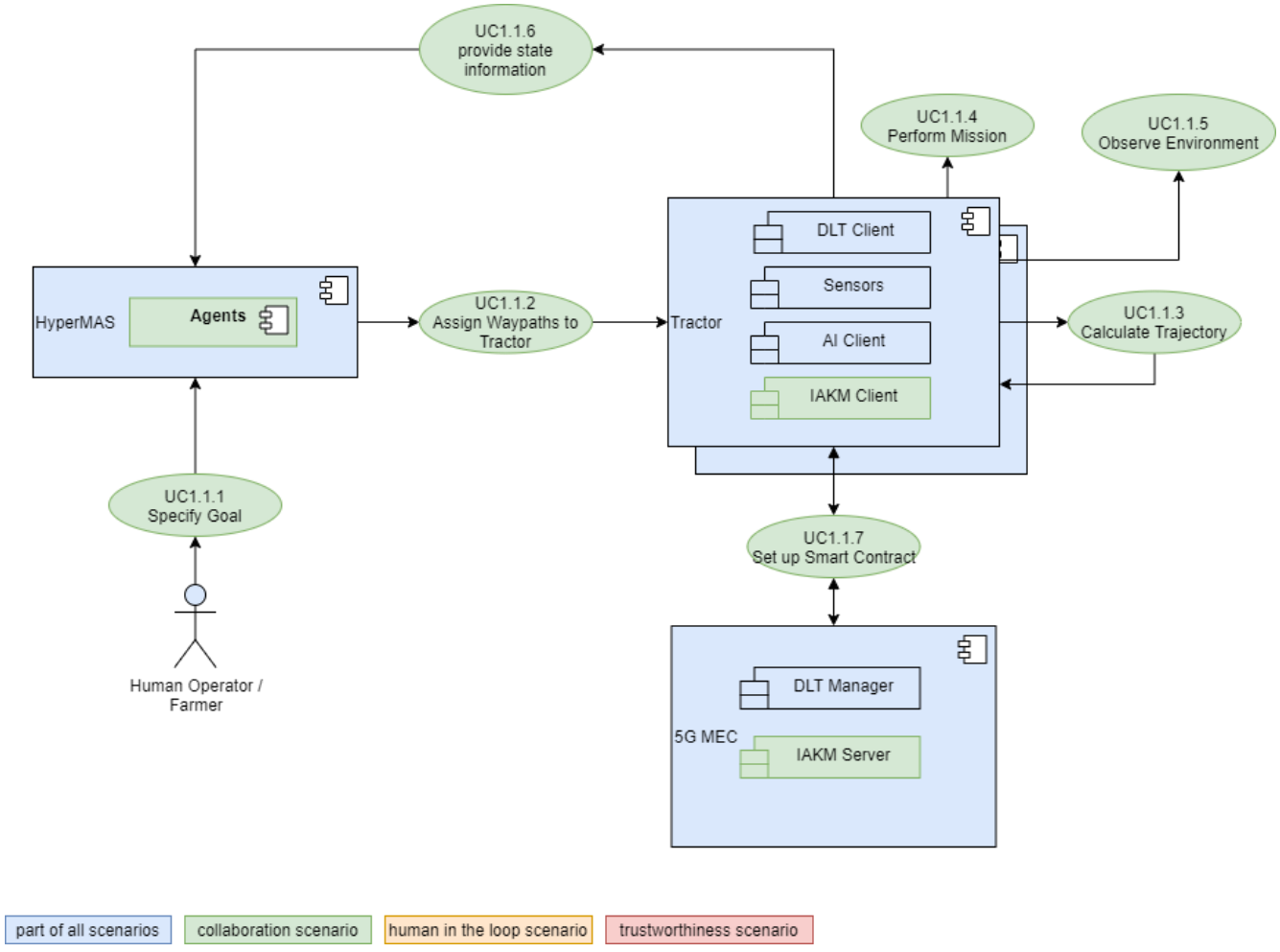
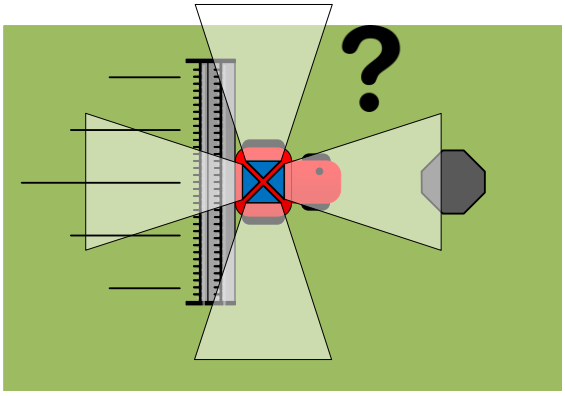
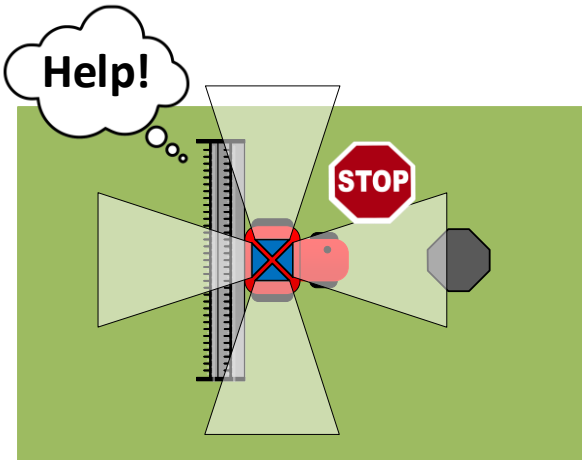


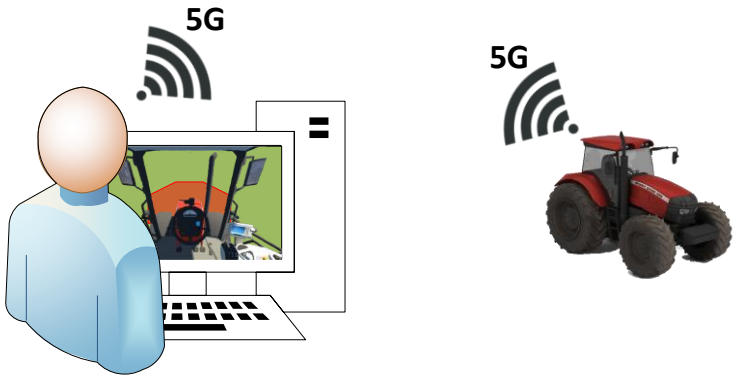
Figure 10: UC1 – Collaborative IoT Scenario

2.1.6.2 SCENARIO 1.2 – HUMAN-IN-THE-LOOP

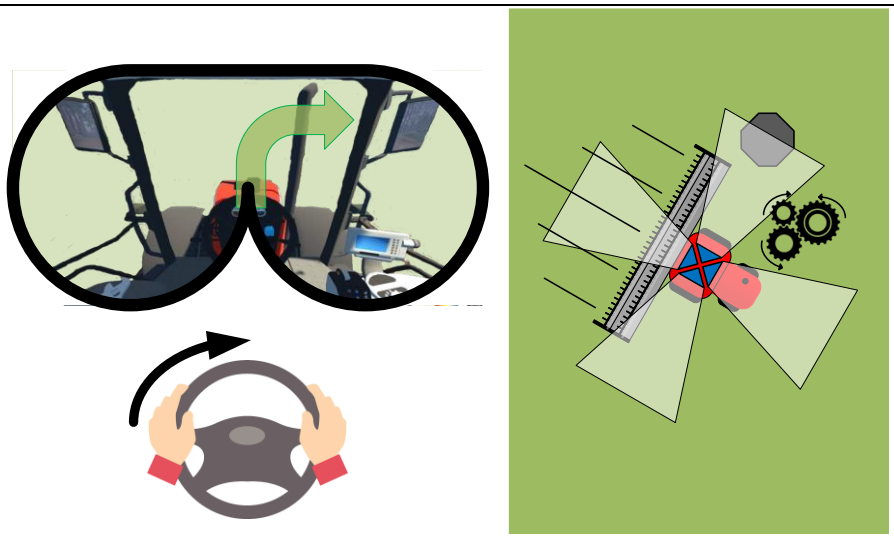
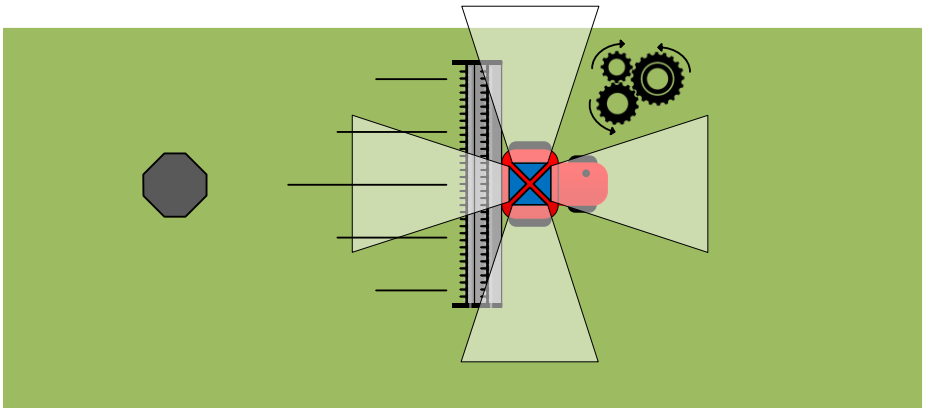
Scenario Name	Human-in-the-Loop
Scenario ID	UC1-Scenario2
Partners	TTC, AVL, EURECOM, HOLO, HSG, SANL, AAU, TSI, UOULU
Description	The semi-autonomous tractor encounters a situation (e.g., an obstacle) that it does not know how to handle (e.g., it does not recognize the obstacle or does not know how to drive around it). The tractor goes into a safe state and makes a request for a handover to the human operator. The human operator receives the request from the HIL service and creates a secure connection to the tractor. Via the connection, the human operator receives visual data from the tractor to clarify the situation. With the aid of virtual reality, the human operator will directly control the tractor around the obstacle to overcome the unknown situation. After the situation has been solved, control is given back to the agent and the human operator closes the connection.
Key Scene	**Key Scene 2.1**: Tractor is stuck in an unidentified situation (e.g., an obstacle was detected) and is not able to clear the situation within given constraints.  **Key Scene 2.2**: Tractor goes into a safe state and performs a request for handover to the human operator. The safe state will be a position where the tractor cannot endanger anybody and will not drive further until the situation is solved. The request for handover can be a message to the human operator stating the fact that the specific vehicle (potentially with tractor ID) is stuck in GPS-position and can also optionally send raw data to explain the situation.



Key Scene 2.3: The human operator creates a secure connection to the tractor and receives data coming from the tractor. The tractor publishes the required data.



Key Scene 2.4: The human operator uses VR to aid the tractor through the unidentified situation. The operator identifies the problem using the information available (i.e., data from different sensors) and will use VR technology to get a clear view of the environment. VR glasses will be applied to create a surround view of the tractor. Based on this information, the operator will take direct control of the tractor and will remotely drive it around the obstacle.

	 **Key Scene 2.5**: After successfully handling the unidentified situation, the human operator gives control back to the tractor and it continues its semi-autonomous behaviour. During the remote controlling, the control information similar to the training labels are stored along the corresponding sensory data as a new labelled data sample. After sufficient amount of newly accumulated data, the obstacle bypassing AI model is updated. 
Potential Variation of the Scene	[1] Additional information coming from external sources (e.g., a drone, sensors on the field, etc.) [2] The obstacle is not a stationary object, but is moving around (e.g., an animal) [3] Different weather or environmental conditions (e.g., dust particles) can influence the information coming from the sensors, causing false-positives or false-negative.
Purpose	The purpose of this specific scenario is the generation of a plan for the semi-autonomous tractor, so that in the future it can overcome similar situations. The human operator will teach the tractor how to handle such a situation and after collecting sufficient amount of such new data samples, the tractor will learn from it over time.
Sources of Risk	[1] No reliable communication connection between the vehicle and the VR device used by the human operator [2] Not enough data available to get a clear picture of the situation

	[3] No possibility is available for driving around the obstacle. Either the human operator has to come to the field to manually remove the obstacle, or a completely new trajectory has to be planned for the tractor. [4] Bad weather or environmental conditions (dust, sun flare, etc.) can cause sensors to not correctly detect its environments, rendering them incapable of detecting the obstacles in front of the vehicle. [5] A saturated IoT-Infrastructure cannot process requests.
Threats	[1] Malicious external parties can take over control of the vehicles and create dangerous situations by moving the vehicles in areas where it is not allowed to go. [2] External people could create a conflicting situation to see if the tractor can handle it (e.g., like pedestrian stopping in the middle of the road to see if a highly automated vehicle will actually stop); Operator needs to differentiate between legitimate and non-legitimate situations. [3] A malicious user may eavesdrop over the process and use the data to train its own competing AI.
Precondition for the Scenario	The tractor is capable of performing its task semi-autonomously (e.g., ploughing) and has a set of cameras that is capable of assessing the environment. Additionally, a reliable connection must be available between the tractor and the human operator to successfully interact and allow the human operator to take over control. Additionally, the communication channel must be capable of providing a good enough data stream to the human operator to assess the unknown environment. Finally, the human operator must have sufficient knowledge and experience to remotely control the tractor.
Successful end condition	The tractor has overcome the unidentified situation in a safe and secure way, with the aid of the human operator. Control is given back to the vehicle, and it performs its autonomous task again.
Failed end condition	The human operator is not capable of guiding the tractor around the unknown objects, caused either by insufficient data or not being capable of planning a path around the object. The tractor will remain stationary, and the human operator/farmer has to go outside to the field and drive the tractor personally to a situation, where it can continue its autonomous task.
Fatal end condition	The tractor is damaged because it collided with the obstacle obstructing its path. Additionally, the tractor could move in a wrong direction, causing potentially damage to other objects located in the field.
Frequency of occurrence	In the worst case, this situation can occur quite frequently, especially if the tractor is not capable of identifying certain objects. Additionally, the tractor can misinterpret the data from the sensors resulting in frequent unknown situations. The frequency should become less, as the tractor should learn from previous experiences how the deal with such situations.
Actor(s)	Tractor, HyperMAS, human operator and potentially other entities in the field (e.g., sensors providing data to the human operator.
Information exchange between actors	[1] Tractor → Human operator: Request message for takeover, brokered by the HyperMAS. The message will be configurable and adaptable to the situation and can either only contain the request for takeover, or it can also include tractor state and situation information.

	[2] Tractor → Human operator: Situational data for deciding what to do with the tractor stuck in its current position. The message will be highly configurable, potentially supporting raw data from the tractor sensors (video images). This data will be used for creating the virtual reality stream for the human operator, so it gets a view of the surrounding of the vehicle, and it can aid in the remote driving of the tractor. The message can also include processed data in order to provide an overview of the environment the tractor currently faces, or finally also ML models. Accordingly, the human operator can have access to a wide range of information to take a decision. [3] Human operator → tractor: Actuation commands or trajectory. The human operator drives the tractor directly (via remote control) or within an augmented environment. [4] Human operator → tractor: return of control. The human operator closes the connection to the tractor. The tractor will receive a message that it will have to continue with its predefined path.
Challenges for scenario validation (T5.3)	[1] Reliable communication [2] Identification of new situations based on the newly learned ones, showing that the tractor has actually learned new knowledge over time. [3] Reliable and secure human-machine interaction [4] Precise translation of VR movement to AI – Tractor movement.
Changes with respect to D2.1	Key Scene 2.5: Updated to indicate that obstacle bypassing AI can be learned over time by collecting data. General update, by explaining in more detail how the interaction between the human operator and the tractor is triggered by the HyperMAS.

Figure 11 provides a UML-based diagram of the scenario. This figure shows the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

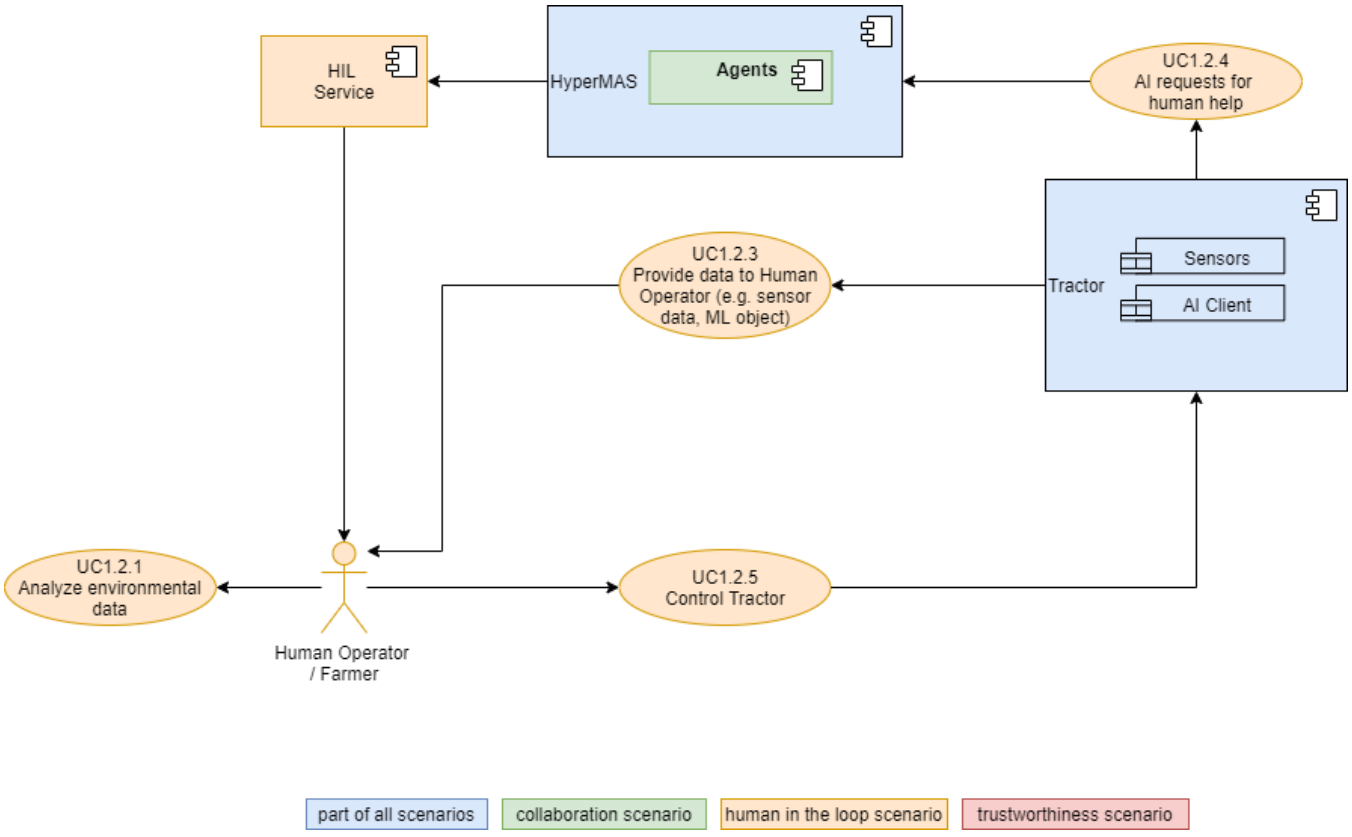
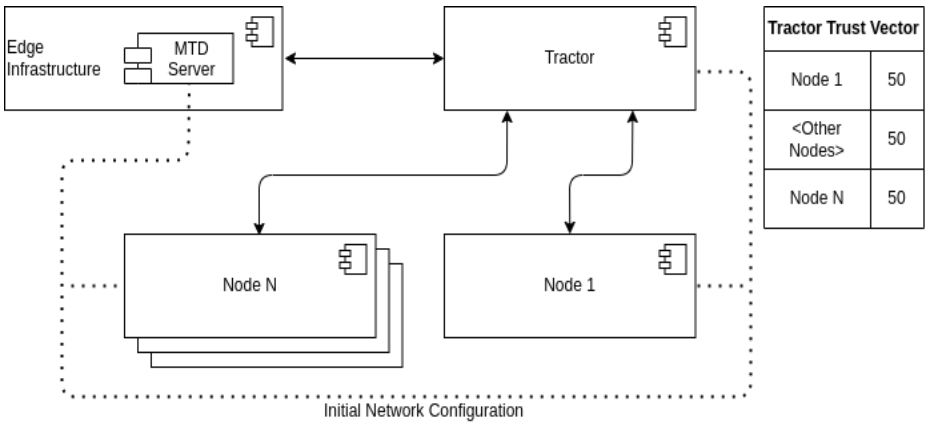
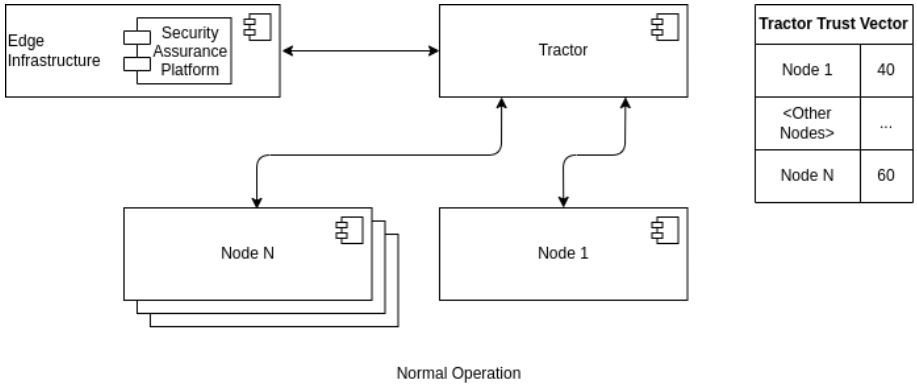
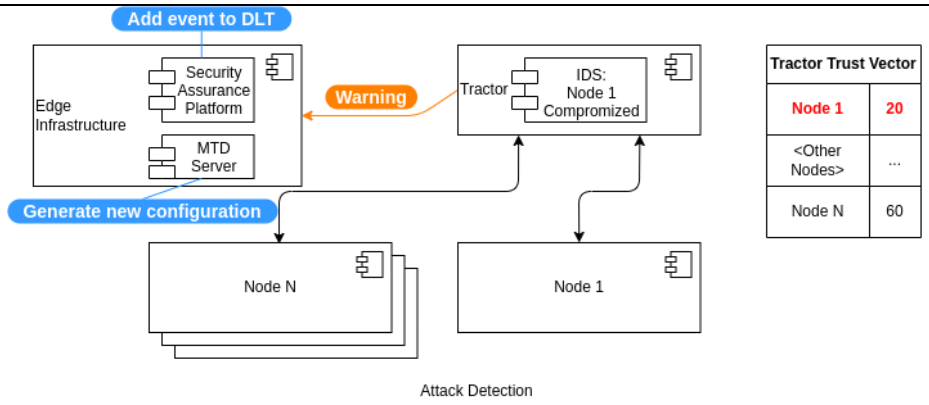


Figure 11: UC1 – Human-in-the-Loop Scenario

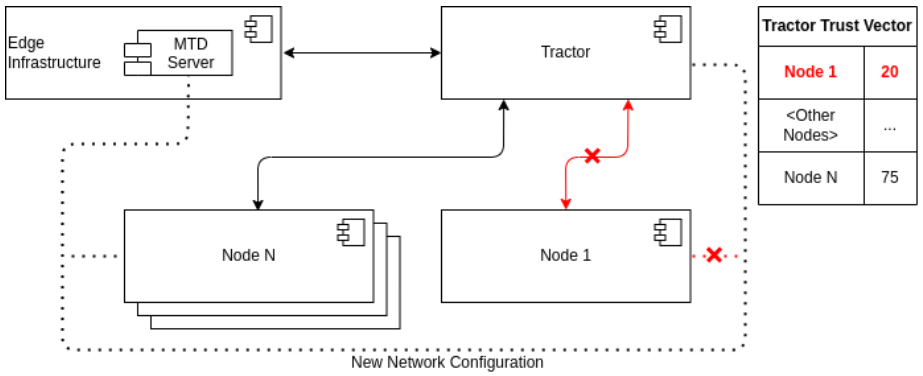
2.1.6.3 SCENARIO 1.3 – TRUSTWORTHINESS

Scenario Name	Trustworthiness
Scenario ID	UC1-Scenario3
Partners	TSI, SANL
Description	During deployment to the field, all participating parties initialize their Intrusion Detection System (IDS) components and establish a secure connection with the SAP and the MTD through a broker. For the agriculture scenario, a key actor is the tractor itself. We assume there are at least two more participants for the most basic scenario acting as computation and communication nodes. Additional entities could participate such as other tractor(s), other autonomous machinery, smart sensors & actuators present on the field, drone(s), etc. The trust-based network is established after the distributed IDS is initialized and executed on each participant. As the system is used in everyday tasks, the IDS builds trust between participants, establishing this as the normal operation of the system. IDS is now in place to detect malicious/malfunctioning participants. When one is detected, the SAP is notified, while also triggering the MTD mitigation process. Consequently, the

	MTD changes network parameters as needed, based on pre-defined defence strategies, to stop the offending participant from further affecting the rest of the system. The aim here is to showcase completely autonomous detection and response processes, relying on trust established from peer monitoring (through the Trust IDS) and MTDs, while the operator remains informed of these changes in the security posture through the SAP.
Key Scene	**Key Scene 3.1**: Initial Phase: build an initial network that is considered trusted. The drone is in the picture to represent the possible additional participants.  Initial Network Configuration **Key Scene 3.2**: Normal Operation: the tractor operates in collaboration with the other actors and the network builds trust as long as everything operates in a predictable manner.  Normal Operation **Key Scene 3.3:** Attack Detection: a participant node is compromised and sends information that lowers its trust to the point that the IDS mechanisms are triggered. Both the MTD Server and the Security Assurance Platform are notified of the event.



Key Scene 3.4: Mitigation Phase: The Moving Target Defense mechanism is activated, and all nodes are notified to change their mode of operation according to a predefined plan. This aims to isolate the malicious node by making it impossible to communicate with the other nodes in an acceptable fashion. The Security Assurance Platform is also notified of this incident to inform operator.



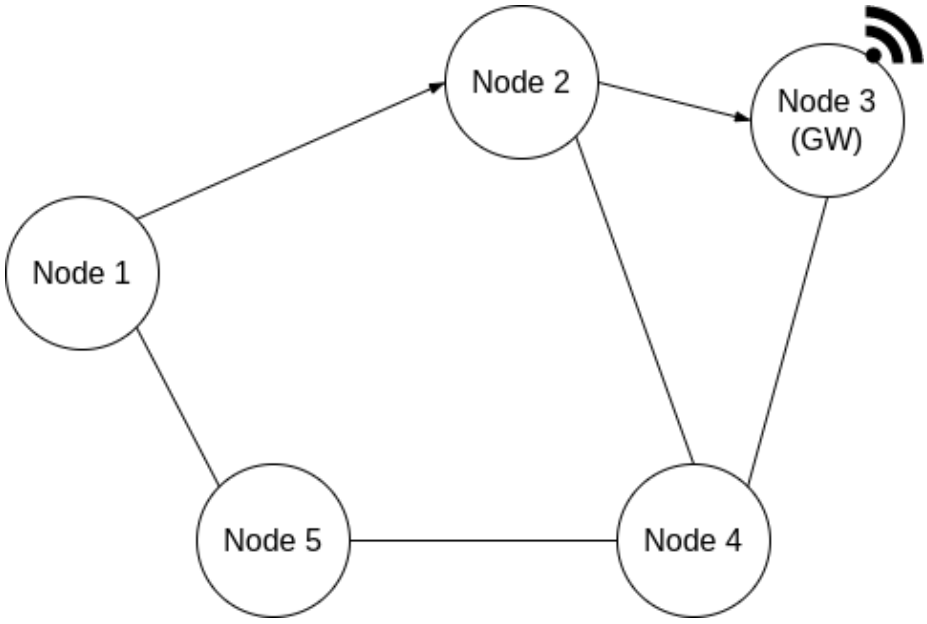
Variation Scene

When we consider the agriculture use case in a bigger scale, there will be multiple autonomous vehicles as well as a significant number of devices forming a smart farming infrastructure. At this scale, these IoT devices will employ adhoc networks to communicate with each other or reach the 5G network access points to connect to remote infrastructure. It is expected that to achieve those communication goals, at least one gateway node will be required. These nodes are at the same time part of the adhoc network and the 5G network providing internet access. In the adhoc network part, all nodes participate in the routing process by using appropriate protocols such as AODV, OLSR and B.A.T.M.A.N. These protocols focus on performing routing tasks in an efficient way; however they do not consider security issues.

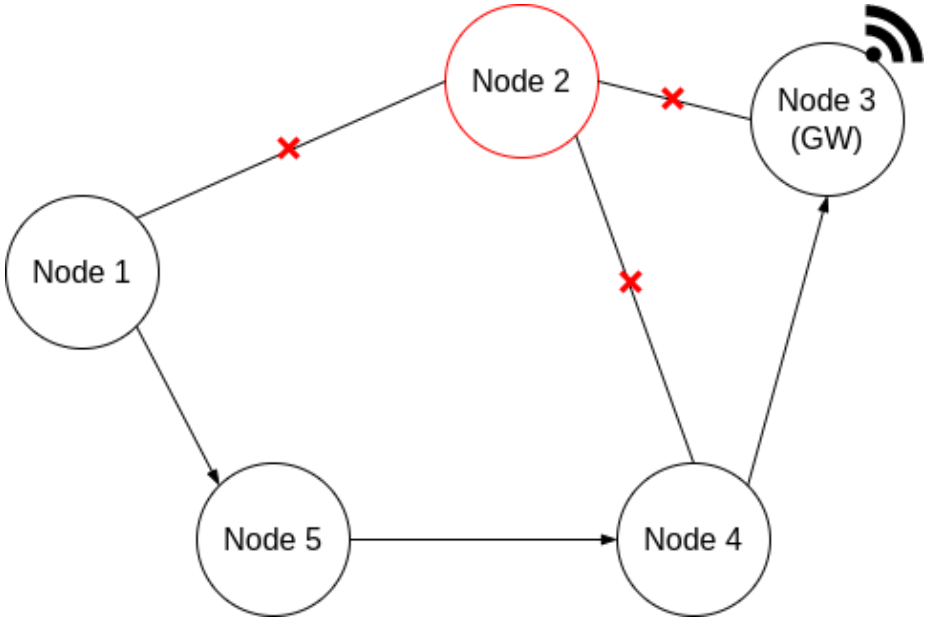
In this scene, we use multiple nodes represented by Single-Board Computers. We do not consider their actual role in the agriculture domain. The purpose of this scene is to add and showcase security on existing adhoc routing protocols. Security will be based on computing trust values of neighbour nodes and whether they are trustworthy enough to be part of the routing process. Detection and mitigation are decentralized as each IoT node handles them locally.

For this type of networks, the nodes topology affects the routing process. We will consider both stationary and moving nodes.

Initially all nodes are considered trustworthy. Therefore, all possible routes can be used. The radius in which a node communicates affects the available routes:



Since all nodes are considered trustworthy, Node 1 can route traffic towards the Gateway through Node 2. If Node 2 starts misbehaving e.g., by dropping received packets, Node 1 will eventually lower its respective trust value. After reaching a certain threshold, an alternative route will be chosen in order to bypass Node 2. For this misbehaving node, all neighbor nodes will eventually lower their trust towards it resulting in its isolation as demonstrated in the figure below:



Purpose	The purpose of this specific scenario is the successful mitigation of an attack on the network without interrupting normal functionality.
Sources of Risk	[1] No reliable communication connection between the components to set up a stable Trust network [2] Nodes that are not malicious might be falsely flagged as such, due to not communicating correctly with their neighbours because of high load. See the other scenarios for the potential sources of risk.
Threats	[1] Loss of confidentiality, integrity and/or availability of system data [2] Compromise of assets (e.g., tractor) [3] Use of compromised assets to perform malicious actions
Precondition for the Scenario	The first two scenes describe normal functionality. For the rest of the scenario to occur, another participant must act in a malicious manner (due to malfunction, external attack, etc.).
Successful end condition	The malicious participant has been identified and isolated, and the rest of the network continues to function.
Failed end condition	If the malicious participant is not identified: [1] It can have access to sensitive data [2] It can avoid detection while providing inaccurate data and altering the behaviour of other participants [3] It might lead to a fatal condition as described below.
Fatal end condition	The malicious participant gains control of the tractor. Even if the tractor is isolated from the rest of the network, it could pose a physical threat.
Frequency of occurrence	Any time someone attacks the network or a device malfunction
Actor(s)	Tractor, IoT nodes
Information exchange between actors	[1] The IoT-Infrastructure sends to all other participants the network configuration [2] The drone sends inaccurate data to the tractor [3] The tractor sends to the IoT-Infrastructure the IDS warning
Challenges for scenario validation (T5.3)	[1] Reliable communication between participants [2] Reliable identification of compromised participants [3] Reliable isolation of compromised participants
Changes with respect to D2.1	[1] Removed the drone node. No partner or Open Call winner could provide this. All additional nodes, apart from the tractor, will be simulated by using Single Board Computers, focusing on their network activity (not their role in the farming process, e.g., actual measurements). The diagrams have also been updated to reflect that.

	[2] Removed IDS from the Edge Infrastructure as it might not be at the same network with the Security Assurance Platform and the MTD Server [3] Focus on autonomous interaction between IDS and MTD using the broker. Security Assurance Platform will still be in the loop about what actions take place [4] Replaced the old variation scenes with secure routing description

Figure 12 provides a UML-based diagram of the scenario. This figure shows the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

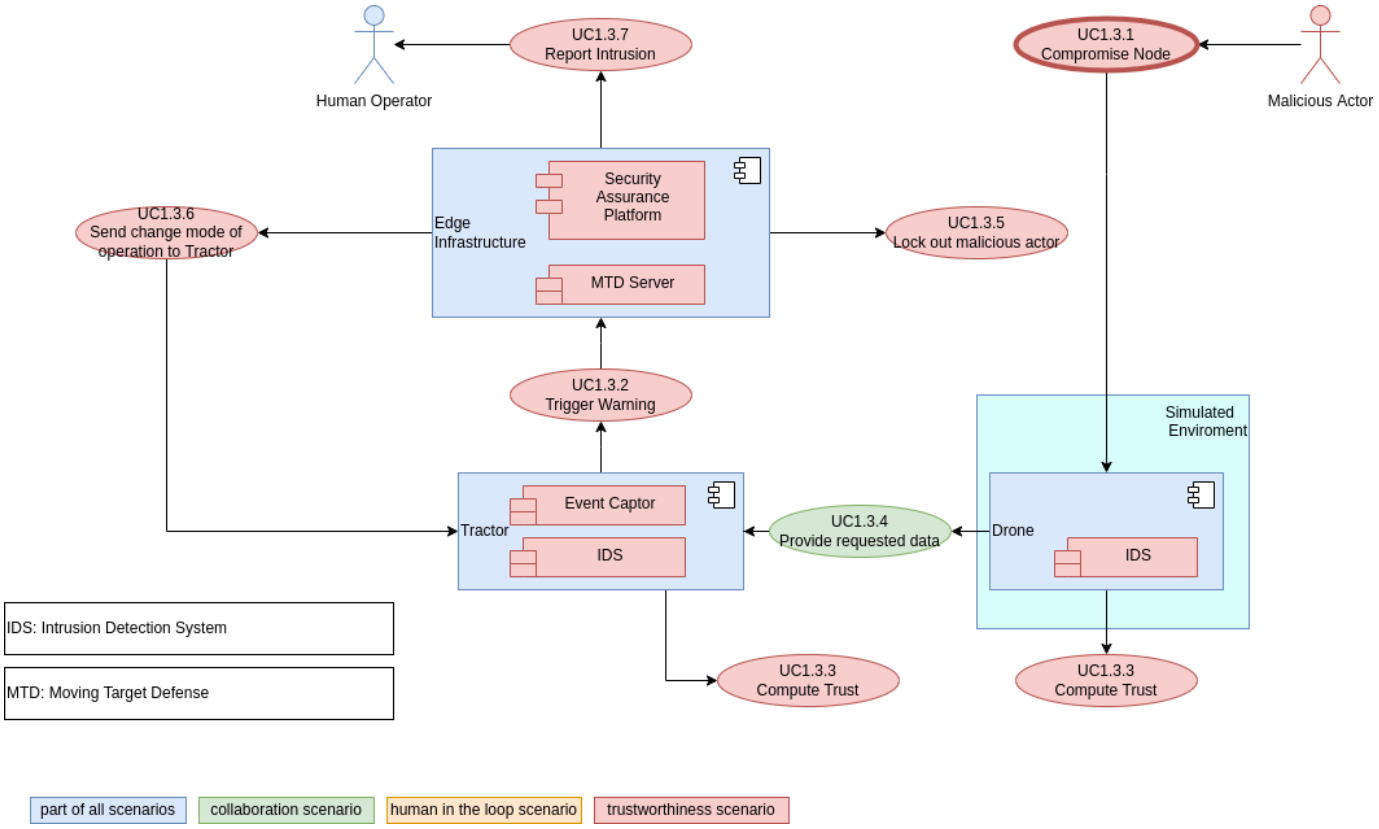


Figure 12: UC1 – Trustworthiness Scenario

2.2 Use Case 2 – Healthcare

2.2.1 SCOPE AND OBJECTIVES

Chronic diseases are a significant social and financial burden and the main cause of death world-wide[12][13] through an increasingly large range of validated IoT devices and wearables, combined with the implementation of AI technologies have the potential to address the stringent needs of this large group of patients. Novel technologies can empower patients to become active partners in the treatment of their disease and contribute to effective strategies for secondary and tertiary prevention.

The scope of the healthcare use case is to investigate collaborative semi-autonomous systems with the human in the loop, that leverage artificial intelligence, wearable devices and sensors, and communication technologies to provide more accurate information to clinicians about the health status of their patients, while enabling patients to carry out normal activities in their home environment with limited disruption related to the management of their chronic disease. We will as well investigate the use of these technologies to implement strategies for recovery and prevention at home, such as support for improved diet and guidance within safe physical exercise programs. The intelligent IoT environment incorporates devices, sensors and algorithms that interact using novel communication technologies to provide continuous active support, personalized to the needs of the individuals, providing specific interventions and recommendations, and fulfilling relevant information needs.

Human intervention is needed in two cases: (a) when an AI algorithm detects a potential health emergency, predicts a deterioration that requires the intervention of the clinician, receives a patient request that involves reaching out to a clinical expert, or when the defined workflow defines the involvement of the clinician; and (b) when the system encounters an exception that it does not know how to address, or in case of technology failure.

The main objectives of the healthcare use case are to design, develop and evaluate a platform combining novel IoT, communication and 5G technologies with an artificial intelligence framework and models enabling semi-autonomous collaborative patient support, with clinical oversight. We will apply and evaluate this platform to facilitate the guidance of heart failure patients and empower them in the management of their own disease, and to assess the effectiveness of a range of technology-assisted interventions.

2.2.2 DESCRIPTION OF THE USE CASE

The healthcare use case will explore the implementation of an intelligent IoT environment to provide efficient AI-supported interventions to patients, and effective interaction with their clinicians, in the context of remote care management. This use case will focus on the needs of heart failure patients and develop a system enabling them to take a key role in improving their health and guiding them through the management plans provided by the clinical experts. We aim to demonstrate that such a remote and continuous support system can provide effective recommendations and guidance, empower patients to reach better outcomes, and reduce costs while never compromising on safety. To enable adoption by healthcare organizations, the solution needs to use the increased information (from sensors, devices, etc.) and the AI models to deliver effective and safe semi-autonomous interventions, without overwhelming the healthcare professional with large amounts of additional (and non-actionable) data.

Figure 13 depicts key components, actors, and interactions of the proposed intelligent semi-autonomous system. IoT devices (wearables, sensors) will collect data that will be used by the AI infrastructure and models to provide

12 https://www.who.int/news-room/fact-sheets/detail/noncommunicable-diseases

https://www.healthdata.org/news-release/lancet-latest-global-disease-estimates-reveal-perfect-storm-rising-chronic-diseases-and

https://www.cdc.gov/chronicdisease/about/costs/index.htm

13 https://www.sciencedirect.com/science/article/pii/S1386505618309821

http://venus-pro-bucket.s3.amazonaws.com/journal/RCM/22/2/10.31083/j.rcm2202046/2153-8174-22-2-403.pdf

recommendations and drive interventions, and to extract accurate information on the health status of the patients that are monitored in the out-of-hospital setting. The AI-assisted system will guide the patients through their daily activities and through their care plan, with clinical expert oversight.

In more detail, referring the steps in Figure 13, patients will be equipped with wearable devices measuring relevant data that is transferred to a personal IoT device (smart phone) via step (1). The AI application will analyse the collected data in step (2) to identify the need for interventions or recommendations, according to the initial AI models and the care plans and goals previously defined by the clinicians responsible for treating the patients. When the need for an intervention is detected, either a recommendation is sent to the patient via step (3a) (with all the information sent to the patient, shared with the clinician as well for review), or the case is escalated to involve the clinician directly (e.g., when potential safety risks are detected), leading to the human-in-the-loop intervention depicted by step (3b). The solution will implement personalization approaches, tailoring interventions to the clinical needs and preferences of the individual patients and enable efficient and effective remote care. The goal is to both improve outcomes and increase adherence.

We will as well test our federated/distributed learning framework in the scenario of distributed collaborative hospital networks (step 9). Additionally, the system may implement a model for monitoring and diagnosing technical issues with the constrained devices as depicted by step (4).

In the planned solution, when an escalation takes place and the clinical expert in the loop is notified, the clinician may decide to contact the patient as shown in step (5a), respond to the personal device shown by step (5b), send a notification to another specialist, or raise an alarm by step (5c). The feedback or recommendation provided by the clinician is persisted in the dataset. The local dataset is used as well to validate and re-train the AI model locally on a personal IoT device as shown in step (6), in order to increase personalization, potentially improve performance, and avoid performance degradation. Model updates are then contributed to the aggregated model at the Global AI Component that is deployed at the central infrastructure (e.g., of a hospital) shown by step (7) to enable its continuous improvement. This distributed AI framework will implement federated and active learning. Model updates are communicated to all personal IoT devices (e.g., using 5G Cellular IoT or D2D communications), through distribution of the aggregated model via step (8).

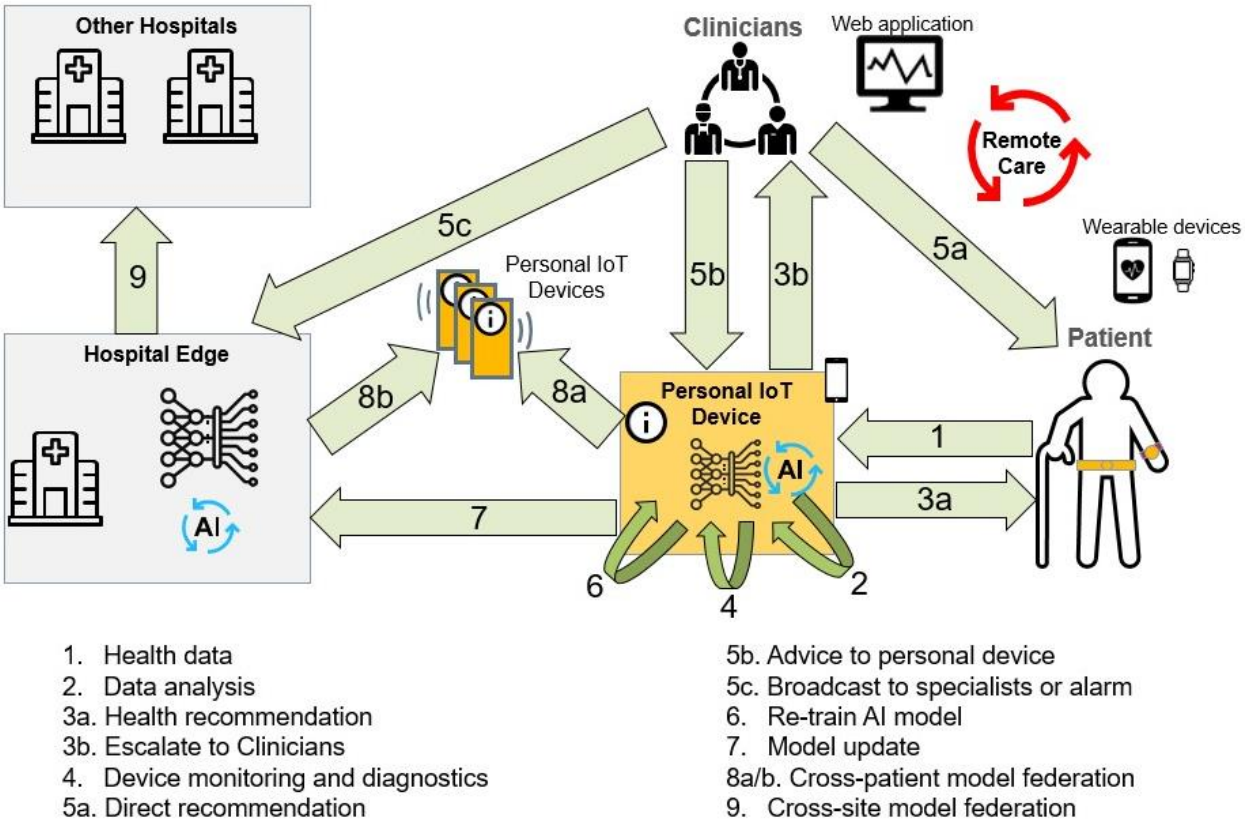


Figure 13. Healthcare Use Case

In terms of security, privacy, and trust, all the involved communications and interactions need to be covered by state-of-the-art security and privacy provisions, catering for the intricacies of the private-sensitive user data. Continuous, evidence-based monitoring will also be employed, with added trust through integration with DLTs, while focusing on requirements (e.g., compliance) and threats (e.g., ransomware) that are most pertinent for the healthcare environment. In variations of the use case, digital consent management to drive the interactions of the system (patients, clinicians, devices) could also be managed e.g., via smart contracts.

2.2.3 MARKET SITUATION AND CHALLENGES

The healthcare market dynamic has been dominated during the past 2 years by the COVID-19 pandemic. The pandemic has highlighted several issues of the structure of the market. According to the 2022 Global Health Care Outlook published by Deloitte[14], issues around health equality and outcomes have been quantified through studies that show the disproportionate impact that COVID-19 has had on certain racial and ethnic minority groups and underserved and marginalized populations. Low vaccination rates, even in developed economies, also show issues such as hesitancy, scheduling, transportation, and convenient hours. In addition, workplace stress caused by the pandemic combined with the projected shortage of health workers by the World Health Organization[15] indicate areas that need improvement.

[14] https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-health-care-outlook-Final.pdf

[15] https://www.who.int/health-topics/health-workforce#tab=tab_1

As was mentioned in D2.2, leaders in the healthcare market interviewed for the Philips Future Health Index[16] indicate that they plan to expand investments in AI three years from now to integrate diagnostics, predict outcomes, and for clinical decision support. They also estimate that a higher amount of routine care delivery will take place outside of the walls of a hospital or healthcare facility three years from now, driven by the increased demand from patients for remote and at-home care. The role of the home is expected to increase from 11% currently to 17% of total routine care delivery.

The main challenges in healthcare according to the participants of an End-User Workshop held by the IntellIoT Consortium can be arranged into 3 categories: the ability of patients to use technology, the creation of useful interactions with technology, and the regulation of patient data. These challenges are well-aligned with the 3 main archetypes that will redefine the healthcare sector as reported in the Future of Health by Deloitte[17], namely data and platforms, well-being and care delivery, and care enablement. Regarding the specific heart failure patients that will be enrolled as part of the clinical investigation of IntellIoT, the European Society of Cardiology reports that cardiovascular disease causes 45% of all deaths and is the leading cause of mortality under 65 years in Europe, while death rates from two types of the disease are generally higher in Central and Eastern Europe than in Northern, Southern and Western Europe[18].

In addition to the above challenges, healthcare systems also face a significant uptick in cyber-attacks, especially during the COVID-19 pandemic. As highlighted in ENISA's Threat Landscape 2021 report[19], healthcare emerges as one of the critical infrastructure sectors impacted by cyberattacks, notably also facing targeted attacks by sophisticated threat actors. In fact, a surge has been observed in healthcare- related data breaches during 2021 that exceeds the increase reported other critical domains[20]. Data breaches may also trigger outages to the system until operations are deemed secure again, as was the case when hackers gained access to the records of 1.4M people who took the COVID-19 test in the Paris region in 2020[21]. An equally notable surge is noted in ransomware attacks[22], which can cause significant disruptions and can also cause cascading effects. For example, a recent analysis[23] of the 2017 WannaCry ransomware's impact on the National Health Service (NHS) in the United Kingdom revealed that, among hospitals infected with WannaCry ransomware, there was a £5.9 million loss in hospital activity, due to the significant decrease in the number of attendances and admissions, including lost inpatient admissions, lost accident and emergency (A&E) attendances, and cancelled outpatient appointments. Apart from disruptions, ransomware attacks can also lead to fatal consequences, like the tragic incident in Düsseldorf University Hospital, Germany, where in September 2020, 30 servers were held to ransom causing the emergency room to shut down and surgeries to be cancelled. Additionally, regulatory compliance -related threats cannot be overlooked, considering the criticality and sensitivity of data handled within hospitals. In fact, fines are increasingly being imposed to hospitals for GDPR infringements (e.g., the Karolinska

[16] https://www.philips.com/a-w/about/news/future-health-index
[17] https://www2.deloitte.com/be/en/pages/life-sciences-and-healthcare/articles/future-of-health.html
[18] https://www.escardio.org/The-ESC/Press-Office/Fact-sheets
[19] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape (ETL) Report 2021", Oct. 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[20] CrowdStrike, "2021 Global Threat Report", Feb. 2021. https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
[21] https://www.rfi.fr/en/france/20210916-hackers-steal-covid-test-data-of-1-4-million-people-from-paris-hospital-system
[22] Europol, "Catching the virus cybercrime, disinformation and the COVID-19 pandemic", Dec. 2021. https://www.europol.europa.eu/publications-events/publications/catching-virus-cybercrime-disinformation-and-covid-19-pandemic
[23] Ghafur, S., Kristensen, S., Honeyford, K. et al. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digit. Med. 2, 98 (2019). https://doi.org/10.1038/s41746-019-0161-6

University Hospital in Sweden, Dec. 2020, €390.100 fine[24]; an undisclosed public hospital in Portugal, July 2018, €400.000 fine[25]; the Haga Hospital in The Netherlands, June 2019, €460.000 fine[26]).

IntellIoT's focus on the pillar of Collaborative IoT will enable the adoption of AI as well as help preserve the privacy of patient data. Meanwhile, the Human-in-the-Loop pillar is mainly centered on supporting health workers. We will as well perform a pilot including patients of heart failure and perform a technical validation of the IntellIoT system under this context. The Trustworthiness pillar will mitigate cyberattacks and data breaches that impede a safe and normal flow of work in healthcare.

2.2.4 TECHNOLOGIES OF THE USE CASE

Actors, components, and associated technologies playing a considerable role in the use case are described in the following subsections.

2.2.4.1 AI FRAMEWORK AND ALGORITHMS

Within this use case, the AI Framework has the role to enable training and deployment of AI-based models providing prediction, interventions, recommendations, and fulfilling the information needs of the users. Due to the intrinsically distributed nature of the system, we will implement a distributed/federated learning solution. Continuous and active learning components will be implemented as well to enable personalization to individual users and their specific needs.

The framework will be used to develop models for interventions relevant in our use case and to predict and early detect potential health degradation or negative events when clinical intervention is needed. We will as well assess the effectiveness of the interventions, guide patients through their clinician-provided plans for diet, exercising, and home management of their disease. The solution will collect the information provided by devices and sensors, presenting it to the healthcare providers, and triggering requests when the intervention of the clinician is needed for a particular patient, implementing the concept of human-in-the-loop, and enabling the remote care of patients.

The framework and the models will be developed and tested in the lab in phase 1, with input from the clinical experts to design and evaluate the interventions to be implemented and will be evaluated with patients in phase 2 of the project.

2.2.4.2 ADVANCED COMMUNICATION INFRASTRUCTURE

The advanced communication infrastructure takes the form of a private 5G MEC architecture hosting various microservices connected to a network controller entity.

In the context of this use case, the advanced communication infrastructure will host IAKM. It provides a means of reliable IoT services to discover, subscribe, and disseminate knowledge (in the form of ML models) for coordination and is required by the other components, such as the AI Framework. In particular, it will host the Federated ML Global AI Component specified in the AI framework.

In the context of health data being gathered in silos, the IAKM will also be in charge of brokership between various IoT gateways from various sensor technologies.

2.2.4.3 IOT ENVIRONMENT: WEARABLE DEVICES AND SENSORS

Sensors and wearable devices are the main source of information and will include an Edge device for advanced processing and storage capacity. It will be connected to the IoT-Infrastructure entity by an IoT client entity and to various microservices hosted on the Edge device.

[24] https://gdprhub.eu/index.php?title=Datainspektionen_-_DI-2019-3839
[25] https://iapp.org/news/a/portugal-fines-hospital-400k-euros-for-gdpr-violation/
[26] https://www.hipaajournal.com/netherlands-hospital-hit-with-e460000-gdpr-data-breach-fine/

In the context of this use case, wearables and other sensors will gather health related data (e.g., vital signs, physical activity, sleep quality, indoor air quality). Depending on the sensor technology, they either will transmit data to a dedicated IoT gateway, which will then act as an Edge device, or locally consolidate data through a local AI on the Edge device, and coordinate with other wearables via the IAKM service from the advanced communication infrastructure for privacy preserved, decentralized AI.

Processed and consolidated data and knowledge will be made available to subscribed and authorized participants through the IoT-Infrastructure entity.

2.2.4.4 TRUST COMPONENTS

Several components are also deployed that support the trustworthiness aspects of the healthcare use case, as presented in the subsections that follow.

2.2.4.4.1 SECURITY ASSURANCE PLATFORM

The Security Assurance Platform will provide runtime, continuous assessment of the monitored healthcare UC deployment, while also acting as a key integration point between the trust enablers.

In the context of the specific use case the role of the Assurance Platform will be to provide the operator with a view of the assurance posture of the deployment, while also responding to changes in said posture, as detected by the integration with the needed event captors. The timely and efficient response to attacks (ransomware and botnet, in this case) will be achieved by triggering changes in the MTDs deployed in the UC environment. This will be achieved through the integration of Playbooks, encoding the defence strategies to be employed.

Throughout its operation, the Assurance Platform will also interface with the DLT building blocks, allowing the evidence-based operation of the assurance scheme. Furthermore, also leveraging this integration, the Assurance Platform will be used as a point for generating trustworthy evidence needed for auditing pertinent to the healthcare environment (e.g., for GDPR audit purposes).

2.2.4.4.2 MOVING TARGET DEFENCES (MTDS)

Moving Target Defence (MTD) is a technology that changes the network configuration dynamically over time, to interrupt and mitigate possible attacks because of the resulting increase in complexity and time costs for the attacker.

In the healthcare scenario, MTDs will be leveraged to mitigate both ransomware and botnet attacks at the clinician and patient premises, respectively. The aim will be to allow the system to continue normal operation, where possible, and to safeguard the private sensitive data present in the healthcare environment.

2.2.4.4.3 AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

AAA provides centralized authentication, authorization, and accounting services. External entities employ these services to communicate with nodes that are part of an IntellIoT scenario in a safe and controlled manner. Two deployment types are available in order to facilitate services that support OAuth2 protocol as well as those that do not. The first case is straightforward; this kind of services communicate directly with the AAA component. For the second case, a reverse proxy is employed. It handles the OAuth2 protocol and acts as a middleman between the services and the external entities.

In the healthcare use case, AAA will be used to authenticate users that have access to patient data. It will be integrated with the solution of the 1st Open Call winner Vidavo.

2.2.4.4.4 DISTRIBUTED LEDGER TECHNOLOGY (DLTS)

DLTs possess key characteristics, such as immutability, decentralization, and transparency, which potentially address pressing issues in healthcare systems, for example, incomplete records at the point of care and difficult access to health data patients. An efficient and effective healthcare system requires interoperability, which allows software and technology platforms to communicate securely and seamlessly, exchange data, and use the exchanged data across

health organizations and development vendors. Besides, the integration of DLTs and smart contract technology open new opportunities to heal insurance, telemedicine, and health records interoperability.

In the specific use case and associated scenarios, DLTs will be leveraged to provide an additional layer of trust on the multi-layered evidence aggregated by SAP.

2.2.5 OPEN CALL #1 CONTRIBUTION

The first Open Call winner in the Use Case Healthcare was Vidavo. The contribution of this new collaborator of the IntellIoT Consortium will focus on the Human-in-the-Loop pillar and the remote care of patients, which is illustrated in Figure 11. Vidavo is a digital health company established in 2002. All these years it has consistently invested in scientifically proved, market focused products. Our solutions cover a wide range of connected health and self-management (mobile apps and web platforms) for supporting chronic disease (medical), nutrition and weight management (wellness). Vidavo's main product, Vida24© is a connected care suite, where citizens can log and keep health records and healthcare professionals manage and process patient data, enjoy personalization tools, effective time management, and create care plans. Vida24© CE0653 Class IIa certified as a medical device according to EU MDR 2017/745 and GDPR compliant. During the project, Vidavo will support the Healthcare Use Case by providing the technical infrastructure to perform the pilot study. Vida24© mobile and web applications will allow the continuous monitoring of patients' vitals and ensure that patients are following their treatment plans by integrating medical devices and IntellIoT machine learning models. Also, Vidavo will integrate Vidavo's custom wearables to IntellIoT framework in order to measure a set of metrics including respiration rate, steps and calories.

2.2.6 SCENARIOS

2.2.6.1 SCENARIO 2.1 – COLLABORATIVE IOT

Scenario Name	Autonomous collaborative IoT scenario with federated learning to provide personalized interventions
Scenario ID	UC2-Scenario1
Partners	PAGNI, PILIPS, AAU, EURECOM, HSG, SANL, TSI, UOULU
Description	Regular day-to-day interventions can be autonomously supported by the IntellIoT solution. The relevant data is collected from the deployed devices and via manual input of the patient and is locally aggregated and used as input to the AI model that monitors and provides recommendations to the patient. The AI algorithm is executed on the Edge Device that provides sufficient computational power. The Edge Device will most likely be a mobile phone. Wearable devices and other mobile devices (like e.g., smart watches) connected by an IoT network will take measurements from patients and communicate with the Edge Device. A subset of data is transmitted to the data repository and will be leveraged to provide information to the physician and for analytics. The AI algorithm is implemented as federated learning, improving personalization to each individual patient, and reducing the connectivity requirements (as model computation is mostly carried out locally) and the volume of data that is transferred to the central repository. During training, the local model is transferred to the Global AI and updates are received from the Global AI. The global model is regularly validated with a validation dataset to ensure performance preservation. A researcher inspects the results of the validation and rolls back to a previous version when issues occur.
Key Scene	**Key Scene 1.1:** Data is collected to train the algorithm. The algorithm is trained and validated in a development phase, before becoming operational. A federated learning approach is

	implemented, including Local AI workers and a Global AI at the central IntellIoT infrastructure. **Key Scene 1.2:** After validation, the algorithm is applied during system operation on data acquired from devices and from patient input. When needed recommendations/interventions are provided directly to the patient and presented on the mobile application based on the predefined and personalized thresholds set by the clinicians. **Key Scene 1.3:** The algorithm is regularly re-trained locally, and updates are sent to the Global AI Component. Accepted updates are propagated to the local deployments. **Key Scene 1.4:** The algorithm is regularly validated, and the results are inspected by a researcher.
Potential Variation of the Scene	The scenario also explores active learning settings that would allow the model to be regularly updated post deployment. Low quality or inaccurate data is collected and used in training or during operation for active learning. The performance drifts, outliers and deviations are detected. The issue is detected and corrected.
Purpose	The purpose of this specific scenario is to describe the autonomous operation of the system. This includes the training phase of the AI algorithm and the deployment and operational/production phase of the solution.
Sources of Risk	[1] Delayed or unreliable communication [2] Unreliable measurements or communication connection between the wearable device and the smart phone [3] Not enough data available for training [4] The collected data is low quality or inaccurate and the system fails to detect it, or the algorithm provides the wrong recommendation based on bad data [5] Damage of the IoT or wearable devices during a possible fall [6] Damage of the smart phone during a possible fall [7] Problems with the wireless connection [8] Failure of device [9] Patient does not use the IoT or wearable devices or the smart phone correctly [10] Cybersecurity incidents
Threats	[1] The device is hacked, and data is stolen or distorted [2] The system is hacked, and the wrong information/recommendations are provided [3] Data is exposed or distorted in transit
Precondition for the Scenario	Users are recruited in the pilot and are using the system. Sufficient data is generated to train the algorithm.
Successful end condition	The collected data is accurate and of sufficient quality. The algorithm interprets the data correctly and provides the suitable intervention/recommendation.

	Adequate clinical and physical parameters are sent with accuracy to the doctor. Data is stored safely in the patient record. Sufficient data of suitable quality is available to train and validate the algorithm. Any device faults are correctly identified and reported.
Failed end condition	When not all the relevant clinical parameters are measured or recorded or are recorded with artefacts or wrong values. The smart watch cannot detect the wearable device, or the device is broken/not used. The algorithm provides a wrong intervention.
Fatal end condition	A health alert is missed or is incorrectly managed by the system.
Frequency of occurrence	We expect that the system will mostly function in this scenario.
Actor(s)	Wearable devices, IoT or smart devices, smart phone, patient, physician
Information exchange between actors	Patient data, recommendations/interventions
Challenges for scenario validation (T5.3)	Reliable communication Interaction between the devices Complexity of situation, measured data insufficient to discern between situations that require different interventions (device defective or inadequately placed, or health issue) Safety of data storing Safe and sufficient AI algorithm development that minimize the physician's intervention Provide support to the patient at the right time, avoid technology fatigue or information overloading.
Changes with respect to D2.1	• In Key Scene 1.2, we now mention the mobile application that will be used by patients as well as the predefined and personalized thresholds that will be set by physicians.

Figure 14 provides a UML-based diagram of the scenario. This figure shows the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

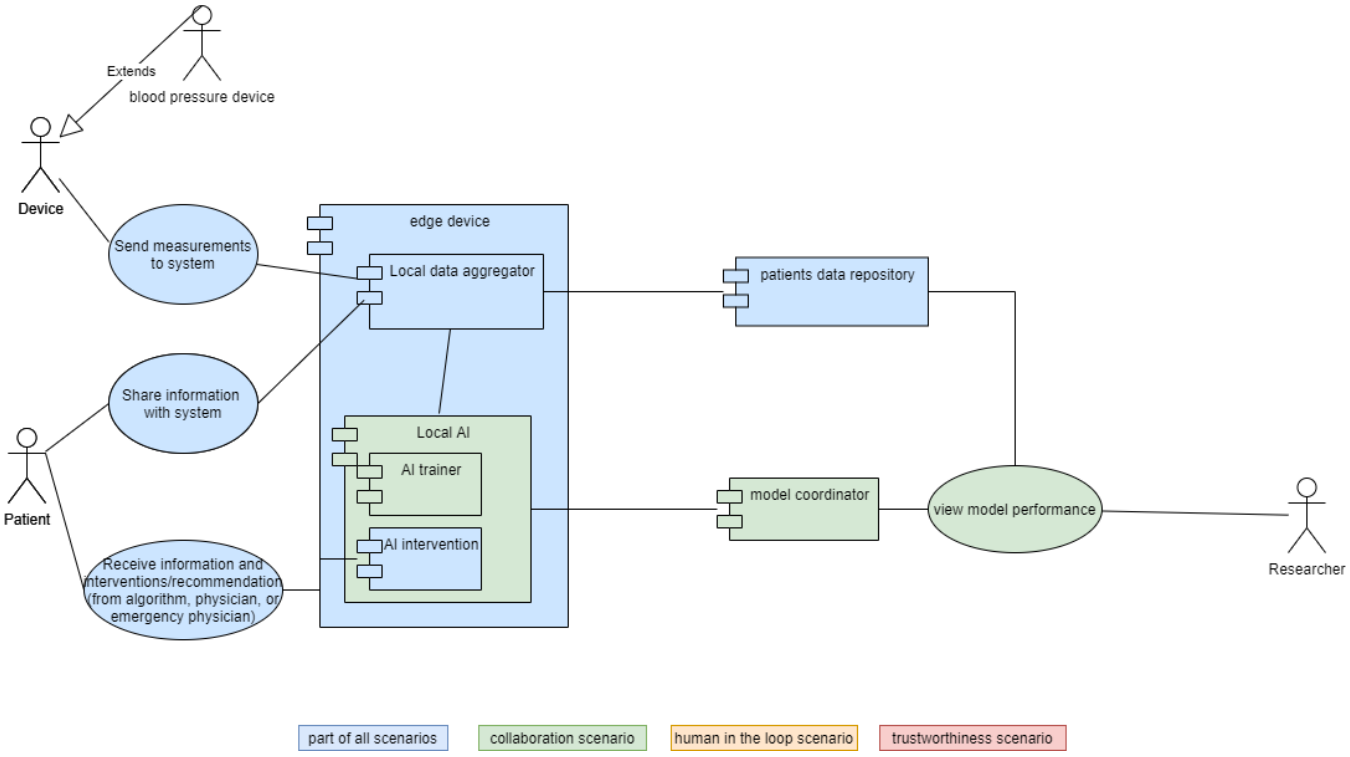


Figure 14. UC2 - Collaborative IoT Scenario

2.2.6.2 SCENARIO 2.2 – HUMAN-IN-THE-LOOP

Scenario Name	Human Take Over during normal operation for interventions that require human involvement
Scenario ID	UC2-Scenario2
Partners	PAGNI, PHILIPS, AAU, EURECOM, HSG, SANL, TSI, UOULU
Description	Specific interventions will require the involvement of the physician in the patient management to ensure safety. This is the case for all potentially dangerous degradations of patients' status. For instance, a patient with heart failure experiences dizziness while walking or exercising. The wearable devices measured patient's vital signs, ECG, patient recorded information, etc. and this data is transmitted to a mobile phone. The AI algorithm is applied to the collected data, and it detects an issue for which the intervention requires that the physician should be contacted. The physician receives alerts from the application and gives instruction to the patient (e.g., via smart watch or mobile phone). This task is very critical for patients whose access to the hospital is difficult.
Key Scene	**Key Scene 2.1**: The algorithm is applied on collected data during system operation. When possible, recommendations and interventions are sent directly to the patient's mobile application. Meanwhile, some recommendations and interventions produced by AI models

	should be approved by the authorized physician through the web application before they are sent to the patient's mobile application. **Key Scene 2.2**: The patient experienced a pre-syncopal episode or a symptom which they are able to report through a questionnaire on the mobile phone. The wearable device measures abnormalities in heart rhythm that are detected by the AI algorithm. The algorithm assesses that the probability of a device malfunction or connectivity issue is low. As this is a potentially dangerous situation, the application is not allowed to give instructions to the patient, sending an alert to the physician instead., **Key Scene 2.3**: The patient takes an ECG with the smart watch and generates a PDF of it in the mobile phone app. The patient sends the PDF to the physician by email or instant messaging application. Then, the physician uploads the PDF to the physician web platform. **Key Scene 2.4*:*** Real time connection to the physician is established. The physician receives real time data regarding patient's clinical condition and provides instructions to the application. Also, some additional information is required. The physician sends his input to the application. **Key Scene 2.5:** The mobile application provides the physician's instructions to the patient. **Key Scene 2.6:** The physician contacts the patient and provides advice through a) the web platform; or b) phone call. The physician ensures that the patient is stable. The application collects data to support further training/validation of the algorithm.
Potential Variation of the Scene	The patient might be sweating due to previous exercise and the vital signs cannot be accurately measured. The wireless connection is not good enough for the reliable and low latency transmission of data. One of the devices may fail and the measurements are out of expected range. -The device sends an error notification to the mobile application and requests that the patient repeat the measurement.
Purpose	The purpose of this specific scenario is to describe the normal operation of the system and the involvement of the physician in defined cases when the algorithm alone should not provide a recommendation. When potential issues are detected, the algorithm contacts a healthcare professional to avoid putting the patient at risk with a wrong advice or by ignoring a serious situation. The physician should be involved in the decision process at an early stage. The doctor will provide input to the application and the patient will receive the correct advice. The clinical input will be used to train and improve the algorithm.
Sources of Risk	[1] Delayed or unreliable communication [2] Unreliable measurements or communication connection between the wearable device and the smart phone. [3] Not enough data available to get a clear picture of the situation. [4] The collected data is low quality or inaccurate and the system fails to detect it, or the algorithm provides the wrong recommendation based on bad data. [5] Damage of the device during a possible fall [6] Damage of the smart watch during a possible fall [7] Problems with the wireless connection

	[8] Failure of device [9] Patient does not use the IoT or wearable devices or the smart phone correctly. [10] Cybersecurity incidents
Threats	[1] The device is hacked, and data is stolen or distorted [2] The system is hacked, and the wrong information/recommendations are provided. [3] Data is exposed or distorted in transit
Precondition for the Scenario	The system is operational and deployed, the users are recruited in the pilot and have been using the system.
Successful end condition	The collected data is accurate and of sufficient quality. The algorithm interprets the data correctly and provides the suitable intervention/recommendation. Adequate clinical and physical parameters are sent with accuracy to the doctor. The mobile application gives the alarm and the correct advice to the patients as needed. The doctor sends instructions to the patient for next steps either directly or via the application and these are correctly received by the patient. Sufficient data of suitable quality is available to train and validate the algorithm. Any device faults are correctly identified and reported.
Failed end condition	When not all the relevant clinical parameters are measured or recorded or are recorded with artefacts or wrong values. The smart watch cannot detect the device, or the device is broken/not used. The doctor does not receive the alert or request for intervention. The doctor cannot send to the patient instruction for the next steps, or the patient does not receive the instructions. The algorithm provides a wrong intervention.
Fatal end condition	A health alert is missed or is incorrectly managed by the system.
Frequency of occurrence	We expect that most of our patients will experience such an event during the pilot.
Actor(s)	Wearable devices, IoT or smart devices, smart phone, patient, physician, emergency physician
Information exchange between actors	Patient data, recommendations/interventions
Challenges for scenario validation (T5.3)	Reliable communication Interaction between the devices Complexity of situation, measured data insufficient to discern between situations that require different interventions (device defective or inadequately placed, or health issue). Safety of data storing

	Safe and sufficient AI algorithm development that minimize the physician's intervention. Provide support to the patient at the right time, avoid technology fatigue or information overloading.
Changes with respect to D2.1	• In the Description, we mention that the collected data is transmitted to the mobile phone. • In Key Scene 2.1, we distinguish between recommendations and interventions that are sent directly to patients and those that need to be approved by the authorized physician. • Key Scene 2.2 is expanded to include symptoms that a patient can report through questionnaires that will be available on the mobile phone. • Key Scene 2.3 has been added. • Key scene 2.6 (previously Key Scene 2.5) now mentions the two ways in which the physician can access patients. Also, it mentions that the physician ensures that the patient is stable. • A Potential Variation of the Scene was rectified to mention that when one of the devices fails, an error notification will be produced by the mobile application used by patients and ask them to repeat the measurement. • Additions to Failed end condition.

Figure 15 provides a UML-based diagram of the scenario. This figure shows the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

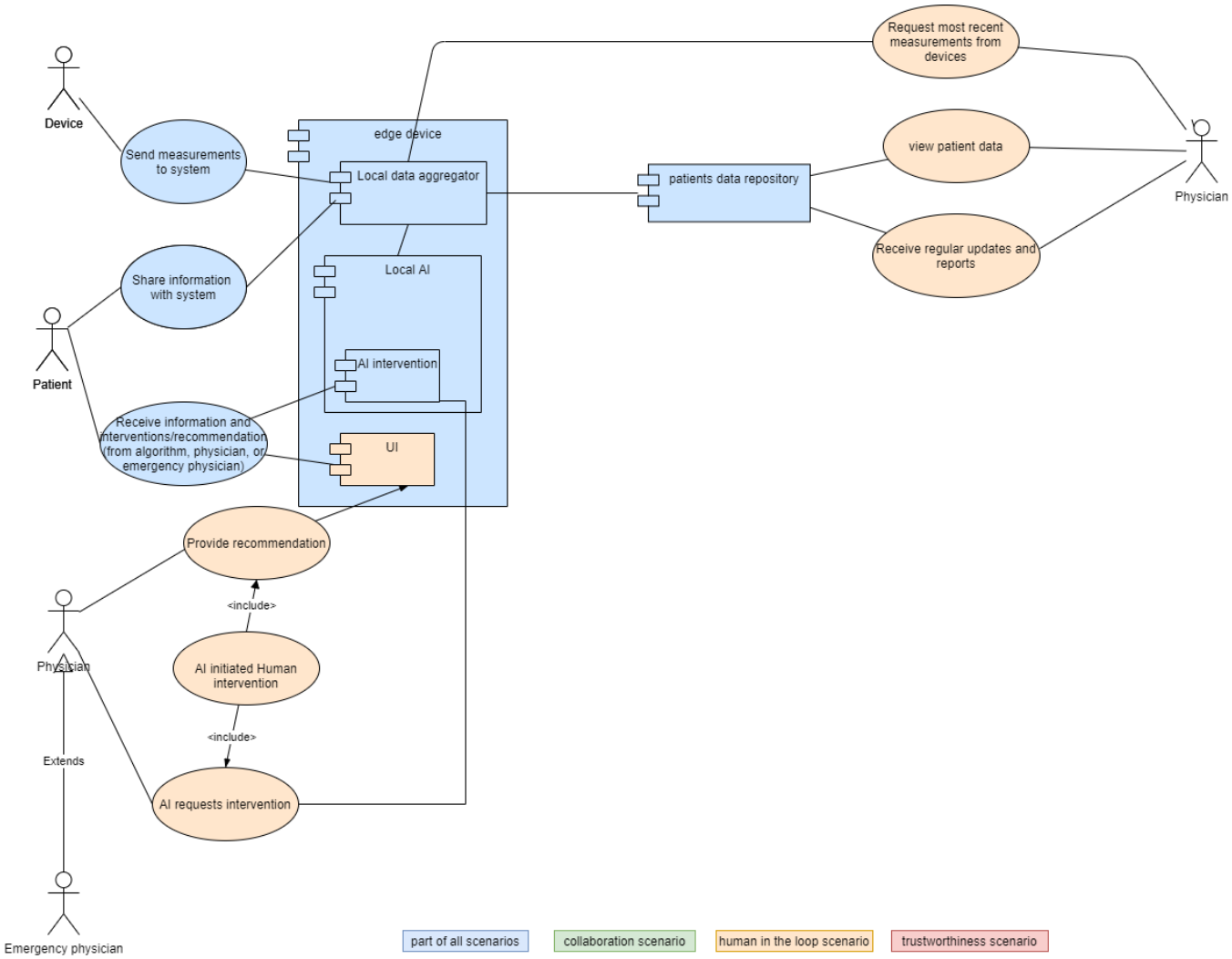
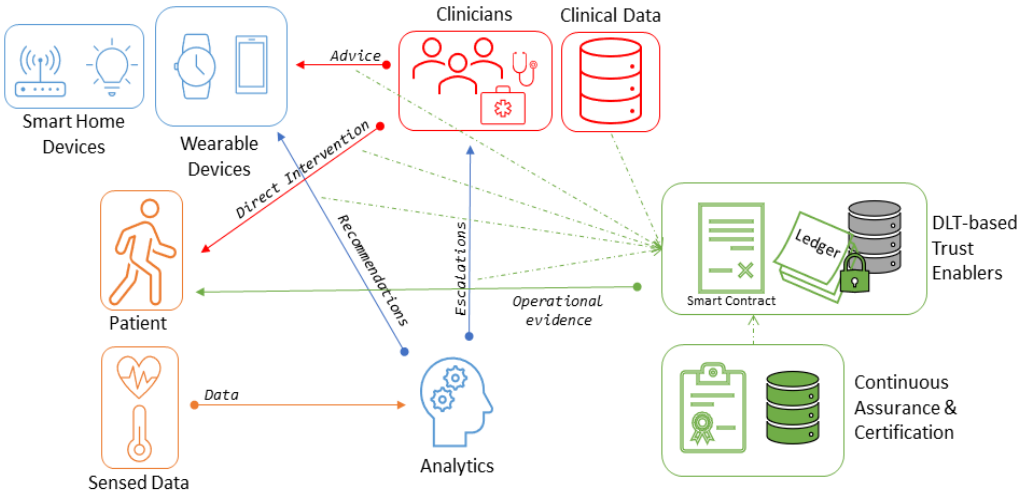
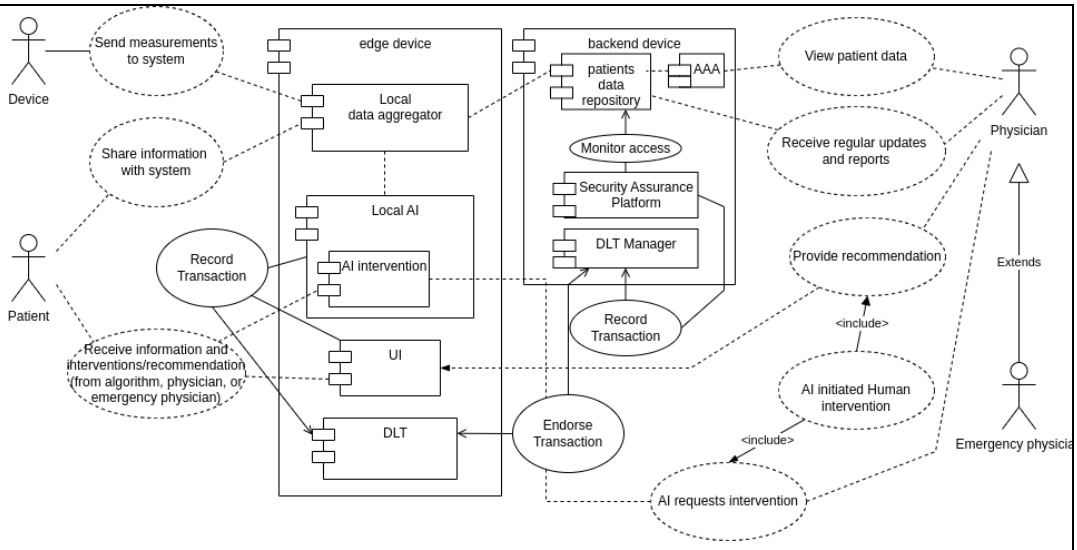


Figure 15. UC2 – Human-in-the-Loop Scenario

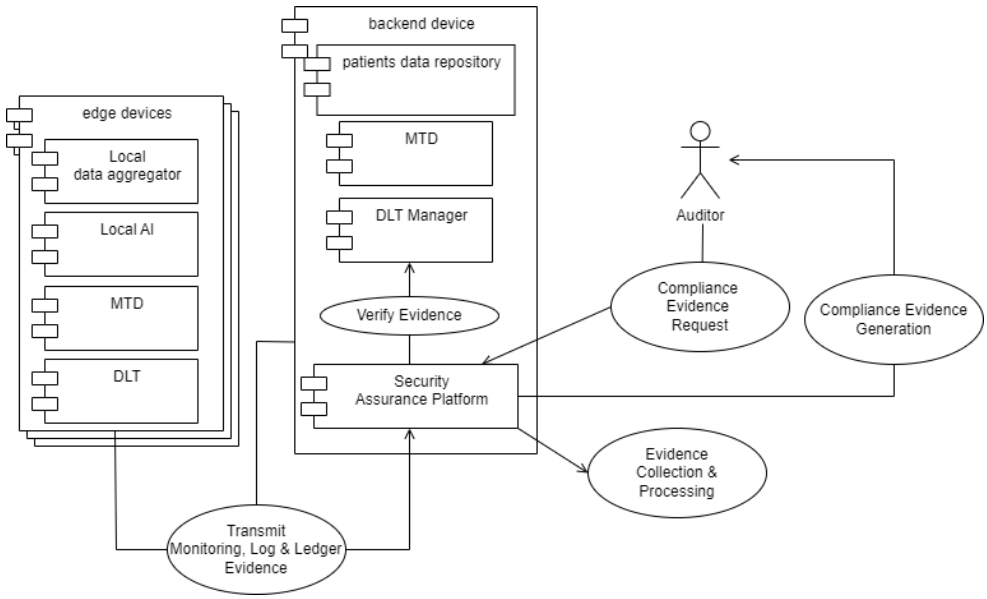
2.2.6.3 SCENARIO 2.3 – TRUSTWORTHINESS

Scenario Name	Security, Privacy & Trust in NGIoT-enabled remote patient care
Scenario ID	UC2-Scenario3
Partners	SANL, TSI, AAU, EURECOM
Description	During the events taking place in the two previous scenarios (i.e., Scenario 1 & Scenario 2), trust and transparency-related evidence are generated via Event Captors and relayed to the DLT-based enablers of IntellIoT via SAP. The patient retrieves said evidence of compliance with agreed upon terms for handling (transport, sharing and analytics) of her data (Key Scene 3.1).

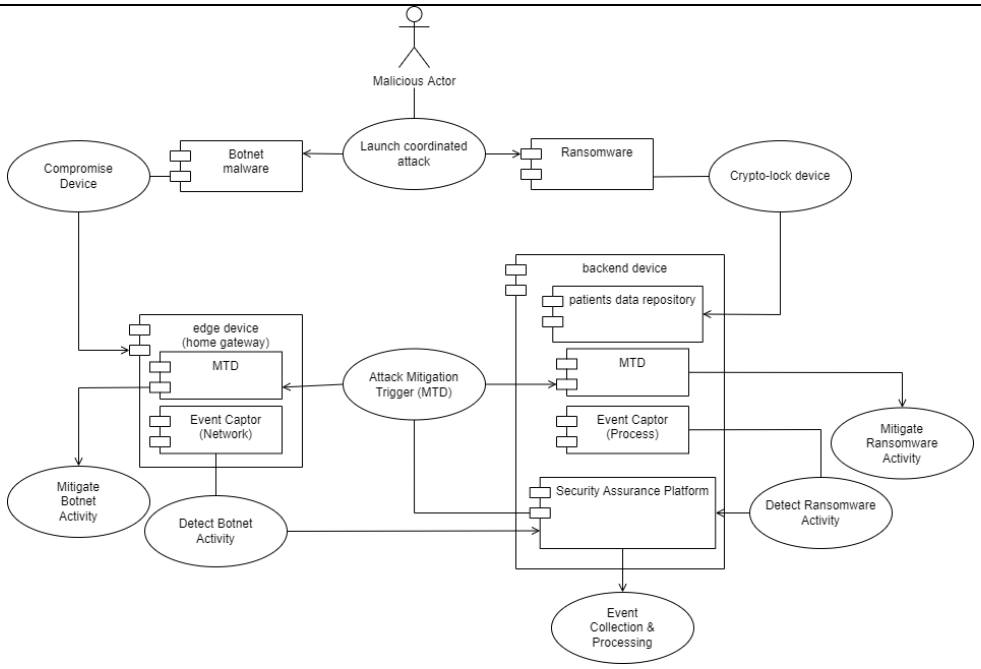
	A few days later an auditor visits the IntellIoT healthcare deployment to conduct a GDPR compliance audit and issue the corresponding certification. The Assurance Platform retrieves and delivers the requested evidence (Key Scene 3.2). Finally, when a coordinated cyberattack takes place (Key Scene 3.3), targeting both the patient's network with a malware tailored to attack her smart devices and make them part of a botnet network, as well as the responsible clinician, with ransomware malware. The IntellIoT security mechanisms detect the two attacks and trigger the necessary defence mechanisms to mitigate them, based on the defence strategies encoded in relevant executable Playbooks. The aim here is to showcase the autonomous operation of security mechanisms tailored to the main threats and pain points of cybersecurity in the healthcare domain, while also facilitating the generation of auditable evidence to support the compliance with relevant certifications & regulations. 
Key Scene	**Key Scene 3.1**: Initial (normal) Phase – Trustworthy intelligent monitoring & interventions for patient remote care, leveraging IntellIoT's innovative DLT-based enablers for transparent framework operation.



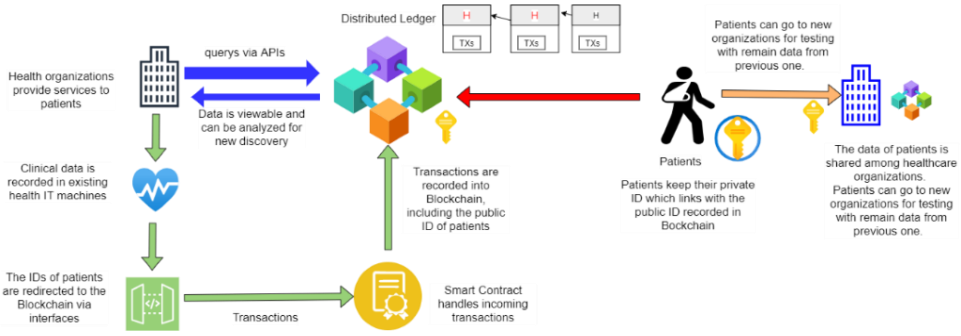
Key Scene 3.2: Audit Phase – Privacy and GDPR compliance. Generation of evidence needed for auditing & certification.



Key Scene 3.3: Attack Phase – Smart device & health data protection. Detection and mitigation of attacks on smart devices (botnet takeover) and data storage (ransomware).

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Potential Variation of the Scene</td><td>Variation/expansion on 3.1 to highlight the benefit of DLTs as an enabler for new business models, by enabling secure, privacy-aware, and trustworthy data monetization.

Health organization records clinical data and public ID of patients in Blockchain via APIs. The organization can directly query the data from the ledger for analysis and discover new insight data. Among organizations, they can have a common ledger to allow patients to share their identity with new health organizations for testing.

 
</td></tr>
<tr><td>Purpose</td><td>The scenario focuses on highlighting the security, privacy, and trust enablers of IntellIoT in the context of the NGIoT-enabled remote patient care environment of the healthcare use case.

The key involved enablers to be showcased include:

[1] Security Assurance Platform:</td></tr>
</table>

	Event & log monitoring in real-time and batch mode to aggregate indicators of attack and compliance evidence from other trust enablers and system components (purpose-built Event Captors, AAA system, native logging, etc.). Generation of compliance evidence to support auditing and certification. Triggering of defence techniques encoded in Playbooks, by interacting with other trust enablers. [2] Patient-side & clinical-side security controls (Event Captors, MTDs, AAA): Protecting the smart home environment and smart assets in said environment. Protecting the clinical environment and patient data stored there. Applying AAA, MTD and monitoring techniques (through dedicated Event Captors) on both environments to identify and respond to pertinent threats (e.g., malware, unauthorised access). [3] DLTs / Smart Contracts: First, the DLT-based E-Healthcare system allows all participants to access the distributed ledger to maintain secure exchange without complex brokered trust. Second, decrease the cost of making transactions. Besides trustworthiness, due to disintermediation, the cost of making transactions is reduced, and more efficient. Third, DLT allows patients and health organizations to share data real-time or near real-time updates across the network to all parties involved. Next, DLT-based smart contracts system creates consistent, and rule-based methods for accessing health record data of patients which can be permissioned or permission-less to specific health organizations. In the above scenarios, DLTs are leveraged to provide an additional layer of trust to the evidence aggregated by SAP.
Sources of Risk	[1] Communication failures between trust components [2] Misconfiguration of components, policies etc. [3] Complexity leads to disabling and/or hindering operation of clinical processes
Threats	[1] Loss of confidentiality, integrity and/or availability of system data, including patient data [2] Legal/regulatory compliance violations [3] Compromise of client-side and clinical-side assets [4] Use of compromised assets to issue erroneous recommendations to patients
Precondition for the Scenario	Scenarios 1 & 2 of the UC will need to have taken place (setting up the environment etc.).
Successful end condition	When all 3 scenes have been demonstrated as intended, focusing on the operation of the DLTs in key scene 3.1, the generation of valid compliance evidence in key scene 3.2 and the detection and mitigation of the two attack types in key scene 3.3.
Failed end condition	[1] DLT scalability issues and solution (On-chain and off-chain solutions) [2] Not adequate or pertinent monitoring evidence generation [3] Not adequate or pertinent log evidence generation [4] Not adequate or pertinent ledger transaction evidence generation [5] Failure to detect ransomware attack at clinical side [6] Failure to mitigate ransomware attack at clinical side [7] Failure to detect botnet (malware) attack at patient side

	[8] Failure to mitigate botnet (malware) attack at patient side
Fatal end condition	Realization of threats [1]-[4] mentioned above.
Frequency of occurrence	Key scene 3.1 continuously takes place upon system operation. Key scene 3.2 happens at predefined intervals depending on audit frequency (e.g., once per year) Key scene 3.3 happens when the system is targeted by malicious actors or due to human negligence (e.g., accidental installation of malware) – so frequency may vary a lot and cannot be estimated.
Actor(s)	IntellIoT Analytics engine, DLT Manager, Security Assurance Platform, Patient-side security controls (Event Captors, MTDs), Clinical-side security controls (Event Captors, MTDs), (emulated) Botnet Malware, (emulated) Ransomware, (emulated) Patient smart home devices, Patient data repository, Auditor
Information exchange between actors	Monitoring, logs and ledger transactions evidence Malicious activity indicators Defence techniques' triggers
Challenges for scenario validation (T5.3)	Identification and deployment of relevant event captors Accurate malware activity simulation Audit evidence accurate specification and validation Efficacy validation of defence mechanisms
Changes with respect to D2.1	• Inclusion of playbooks to automate & orchestrate defenses • Refinement of DLT involvement • Update on diagrams to better reflect actual IntellIoT architecture & deployment

Figure 16 provides a UML-based diagram of the scenario. This figure shows the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

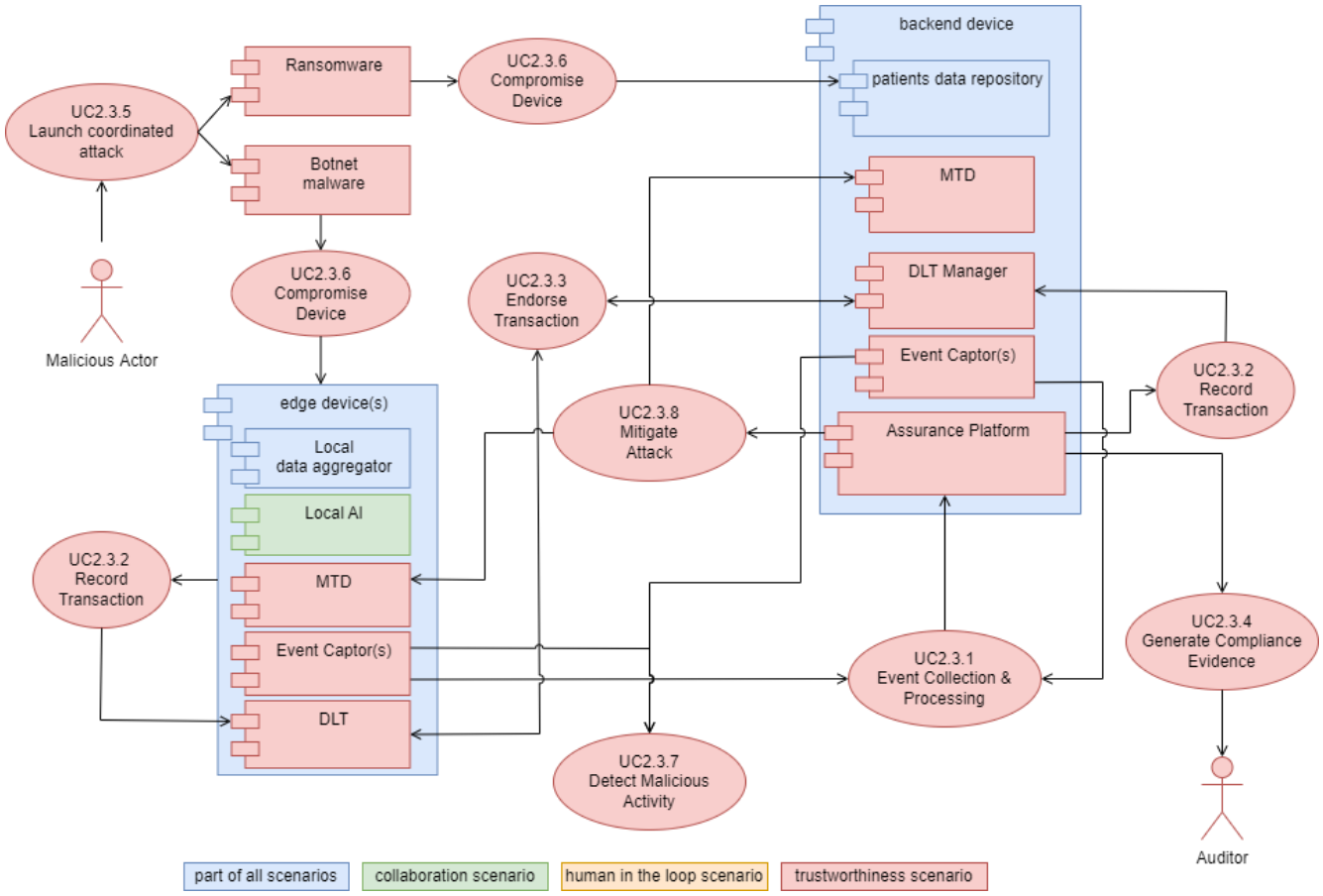


Figure 16. UC2 – Trustworthiness Scenario

2.3 Use Case 3 – Manufacturing

2.3.1 SCOPE AND OBJECTIVES

Industry 4.0 is seen as the most disruptive change emerging in manufacturing industry. Shrinking lot sizes, with orders directly coming from the customer and being manufactured without or very little human intervention is one of the main focus areas. The *aim* of this use case is to enable flexible and individualized (up to lot-size one) production, which is widely recognized as a crucial feature of Industry 4.0 for the manufacturing plant of the future. Thinking such a demand even further, this use case considers a shared manufacturing plant with multiple customers utilizing manufacturing-as-a-service. Machines in the shared manufacturing plant are provided by multiple machine vendors and operators, which offers production flexibility and potential for novel and disruptive business models.

2.3.2 DESCRIPTION OF THE USE CASE

The *intelligent IoT environment* in this use case derives a production plan from product data received from a **customer**, selects machines for the planned production steps and plans optimized transport paths for workpieces. Smart contracts are concluded between customers, **machine owner**s and **plant operator** – where at least the latter two are represented by digital agents. Transport is done by a UR5 robot. Whenever AI is not sufficiently confident about a production step or workpiece handling, the intelligent IoT environment will involve a human-in-the-loop to take over control remotely. Using AR technologies, the human-in-the-loop assists the AI, which is concurrently trained with

these new inputs. The infrastructure of IoT/edge and networking (within the machines and robots and to the operator) will enable tactile, reliable, secure and safe operation.

The *approach* of this use case is summarized in Figure 17 and entails the following components and actors, including their respective interactions: Instead of ordering a standard product, a customer (tenant) provides a specification for a product, i.e., a production goal, e.g., CAD-drawing and CAM-data, see step (1). A great variety of products can be built depending on the machines available in the shared manufacturing plant. Using additive manufacturing in addition to conventional machines (e.g., for drilling, milling, or welding), almost arbitrary products can be made. In a small-scale, but fully featured demonstrator of this use case, the customer provides text to be engraved or lasered on a wood slice. In step (2), a Hypermedia-based Multi-Agent System takes care of orchestrating different machines to fabricate the desired product, by searching for suitable artifacts that represent available machines and assembling them according to Agent procedural knowledge ("Agent plans") that are configured by the plant operator, who is considered as the "domain expert" from HyperMAS point of view, using a no-code development environment for Agents. If the Agents are unable to reach the production goal, they can ask the customer or the plant operator to reconfigure the production goal or to update the Agent knowledge (3).

In the proposed demonstrator, a wood slice (as raw material) is selected, and the HyperMAS decides how to place it in which machine(s) to engrave and/or laser text on it. Human help might be needed e.g., if the text is too large and must be cut or resized. Next, a robot or AGV is tasked to transport the workpiece (4) to the next production step. As a machine may be operated by the **plant operator** or a third-party **machine owner**, contractual arrangements are set up using a distributed ledger. Further, comprehensive security mechanisms are applied to ensure privacy and security of customer data. When a robot interacts with a machine, e.g., moves a part in the working area of a machine, a safe peer-to-peer communication relation between both can be setup ad hoc to protect from collisions. In step (5), the manufacturing edge AI decides how the robot picks a workpiece from a machine.

If the confidence-level of the AI is low and it cannot pick the workpiece safely, a connection to a human is established (6). Utilizing AR, the human can **virtually select the grab spot of the workpiece** to support the robot. A **tactile communication** is established for this interaction, under consideration of security and privacy. Grabbing and haptic feedback will be realized with the Holo-Stylus developed by HOLO. If support from a remote operator is needed, a tactile communication may not be possible through long-distance internet connection. Hence, the operator can **control a virtual robot** rendered in the local edge, with delayed movement of the real robot. An accurate enough reconstruction of the surroundings in the AR space is generated, which allows the full control and visual information about the robot. From the human handling of the work piece, the **AI at the plant edge re-trains** itself using the human feedback as target (7). During the whole process the location of the RFID-tagged workpieces is tracked using RFID sensors. From location and movement data, TRACCIA software will derive location-based KPIs.

In terms of trust, the use case focuses on providing a real-time view of the security posture of the manufacturing deployment, with holistic assessments covering all assets within said deployment. Furthermore, in addition to the standard security & trust provisions deployed across UCs, a novel incident response mechanism will be leveraged that will allow the operator (human-in-the-loop) to be informed in real time of incidents, and trigger the appropriate defence mechanisms, based on executable playbooks.

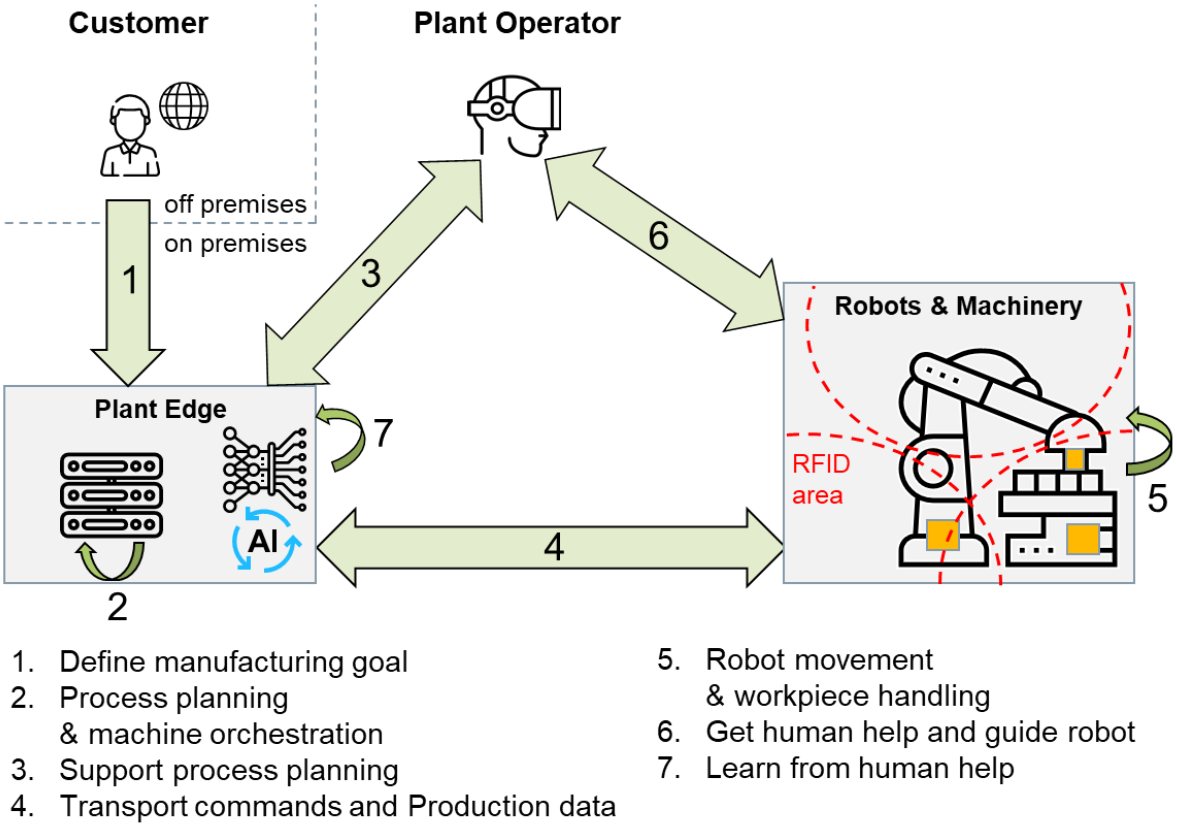


Figure 17: Manufacturing use case

2.3.3 MARKET SITUATION AND CHALLENGES

The EU's manufacturing sector employs over 30 million people, contributes 21.4% to the EU's employment, and generated €1,912 billion of economic value added in 2016[27]. Thus, manufacturing is the *largest industry from an IoT investments perspective*[28], accounting for $183 billion in 2017, while a 3.17% increase to this number was forecasted for 2018[29]. This economic branch is currently amid an immense transition, which has been termed the 4th industrial revolution. However, many challenges still exist in this market transition. Below, we name those challenges that are considered most important in context of the IntellIoT project (these challenges have also been identified and confirmed by domain experts in the exploitation workshops whose outcomes are analyzed in D6.3):

A crucial challenge for the manufacturing domain is protection of data privacy. While many companies made progress in employing "Industrie 4.0" technologies, a recent survey[30] shows that a large number of enterprises are still lagging behind, e.g., in Ireland only 43% of the manufacturing companies surveyed have defined a digital strategy. This is often caused by a reservation towards cloud platforms because of the privacy and dependability concerns for manufacturing companies.

27 https://ec.europa.eu/eurostat/statistics-explained/index.php/Manufacturing_statistics_-_NACE_Rev._2

28 https://www.i-scoop.eu/internet-of-things-guide/iot-investments-2017-2021/

29 https://www.i-scoop.eu/internet-things-spending-2018

30 https://new.siemens.com/ie/en/company/topic-areas/digitalization/digitalization-trends-and-solutions.html

Related to the privacy concerns is the challenge of unreliable public internet connections that are used by manufacturing plants to establish connectivity to the cloud. Besides concerns over possible outages, the public network may show inadequate latencies that undermine the reliability of plant automation systems. Particularly for industrial facilities in remote locations, connections to a cloud platform are not capable of handling the amounts of data that would need to be transferred. This challenge can be overcome by using more local infrastructure in the plant and avoiding the communication with the cloud. Therefore, edge computing capacities need to be established locally and reliable networking (e.g., through TSN) needs to connect the edge servers and local machinery.

A further challenge relates to the ability of facilitating smaller manufacturing lot sizes, as there is a demand from the customer side for more individualized products. To fulfil this customer desire smaller lot sizes will become reality in the production process. In turn, this results in the requirement for highly flexible production facilities. The ability to quickly re-arrange parts of a plant to produce in different ways becomes important. Besides a reliable communication & computation infrastructure, methods from artificial intelligence are needed to enable adaptivity of machines and production lines/cells.

Finally, a crucial challenge is acceptable cybersecurity levels. As highlighted in ENISA's Threat Landscape 2021 report[31], adversaries have increasingly invested resources to target industrial networks in the past 10 years, and these investments are certain to continue to grow, with objectives varying from information collection and long-term persistence to disruption of ICS operations and potential physical destruction. In fact, according to a recent report by Palo Alto[32], manufacturing was one of the industries with the highest increase in security incidents (230% up) during the COVID-19 pandemic. Typically, industrial organisations focus less on monitoring their internal networks (e.g., ICS networks), compared to their IT networks, as these were considered "trusted". Nevertheless, the old paradigm of perimeter defenses and trusted internal networks is obsolete, as IT and OT networks merge, and the trust boundaries become blurred by the "digital transformation" and the move to the Industrial IoT, cloud-connected ICS, "smart" manufacturing devices, and complex supply and value chains (e.g., requiring access to assets from external, third parties)[33] [34] [35]. The move to more complex, IIoT -enabled, ecosystems also increases the attack surface in terms of vulnerabilities, including in the equipment (e.g., security vulnerabilities in manufacturing robots[36] [37]) and in third-party software components[38]. ENISA highlights that software supply chain attacks are the most frequent type of supply chain attacks[39] [40]. The recent SolarWinds[41] supply chain compromise is a prominent example of how impactful such attacks can be, affecting ~18.000 organisations, including Fortune 500 companies, governmental organisations, and critical infrastructures. Such vulnerabilities are typically the main means (along with phishing attacks) that ransomware is also delivered; another important threat to manufacturing environments, with a significant increase in ICS-aware (e.g., tailored to stop industrial processes) ransomware targeting industrial environments being noted[42].

---

31 European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape (ETL) Report 2021", Oct. 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

32 Palo Alto Networks, Unit 42 - Cloud Threat Report, 1H 2021

33 https://www.microsoft.com/security/blog/2020/10/21/addressing-cybersecurity-risk-in-industrial-iot-and-ot/

34 Accenture - 2020 Cyber Threatscape Report - https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf

35 https://www.dragos.com/blog/industry-news/manufacturing-sector-cyber-threats/

36 Yaacoub, JP.A., Noura, H.N., Salman, O. et al. Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations. Int. J. Inf. Secur. 21, 115–158 (2022). https://doi.org/10.1007/s10207-021-00545-8

37 https://www.iiot-world.com/artificial-intelligence-ml/robotics/industrial-robots-gone-rogue-staying-ahead-of-ics-security-vulnerabilities/

38 Trend Micro, Securing the Pandemic Disrupted Workplace, 2020

39 https://www.dragos.com/year-in-review/#section-recommendations

40 European Union Agency for Cybersecurity (ENISA), Threat Landscape for Supply Chain Attacks, Jul. 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

41 https://www.solarwinds.com/sa-overview/securityadvisory

42 https://www.dragos.com/blog/industry-news/manufacturing-sector-cyber-threats/

The Colonial Pipeline's ransomware attack[43] (with an estimated $5M paid in ransom) is a very recent, high-impact incident that triggered policy initiatives (including US President Joe Biden signing an Executive Order to enhance cybersecurity[44]). Other, less high-profile, cases exist as well; e.g., in 2017 a Honda plant in Japan was hit by the WannaCry ransomware, forcing a halt to domestic production for a day (>1000 cars), costing millions of dollars[45]. Of course, less sophisticated attacks (e.g., getting access to credentials of valid accounts, which is the most common technique used by threat agents targeting industrial systems[46]) also show a lack of adoption of best practices and a lack of security prioritisation (with uptime and production rates being a top priority, affecting e.g., the patching schedule), that is not appropriate in the current IIoT landscape, whereby attacks can have an impact on human safety and business operations, causing significant damage. Overall, industrial environments need increased visibility of internal networks (monitoring, logging, etc.), processes and mechanisms allowing them to identify and prioritise assets, better vulnerability management, and a boost to incident response capabilities, while also focusing on getting the basics right (e.g. better credential management, such as no credential sharing, separate IT & OT credential management).

2.3.4 TECHNOLOGIES OF THE USE CASE

Figure 17 summarized the general approach of the manufacturing use case. Figure 18, Figure 19, Figure 20, Figure 21 and Figure 22 show use case diagrams for the scenarios described in chapter 2.3.6**.** Actors, components, and associated technologies playing a considerable role in the use case are described in the following subsections.

2.3.4.1 AR GLASSES AND STYLUS INPUT DEVICE

AR glasses, i.e., Microsoft HoloLens 2, will be used by the plant operator to view a live video feed coming from the robot. Depending on the scenario, 3D replicas of the robot as well as the workpiece can be displayed in addition or instead of the live video of the real robot. The Holo-Stylus will be used to move the robot arm and instruct the robot on the best action plan, i.e., grab workpiece here. Models of the robots and workpiece can be rendered directly on a local computational unit on the glasses up to a certain complexity. For more complex models, rendering might be offloaded to the edge.

2.3.4.2 HYPERMEDIA MULTI-AGENT SYSTEM

Agents that are running in a HyperMAS orchestrate available artifacts to fabricate the desired product by searching for suitable artifacts that encapsulate available machines and combining services that are provided by these artifacts. In this component, we integrate multi-agent-oriented programming on top of a hypermedia-based infrastructure so that we may achieve a flexible yet scalable system, while providing an end-user programming framework that allows domain experts (i.e., plant operators in UC3) to specify procedural knowledge of Agents. In Cycle 2 of the project, we extend this component to permit the creation of semantic multi-agent organizations to coordinate the individual agents towards the production goal.[47] If our system is unable to find a solution for a given production goal, it can request the customer to modify the goal specification or can notify the plant operator to update the specified Agent knowledge.

2.3.4.3 ROBOT

A robot arm is tasked to transport the workpiece to the next production step. It is a commercial UR5 robot, composed of rotative joints linked together with a gripper at the end-effector. AI decides how the robot picks a workpiece and places it in the next machine. The different joints are connected to a central computing unit referred to UR5 controller.

43 https://www.powermag.com/colonial-pipeline-ransomware-attack-rattles-power-industry-renews-vulnerability-concems/

44 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

45 https://www.wired.co.uk/article/nhs-cyberattack-ransomware-security

46 Dragos - Year in Review - https://hub.dragos.com/2020-year-in-review-download

47 A. Ciortea, S. Mayer, F. Michahelles: Repurposing Manufacturing Lines on the Fly with Multi-agent Systems for the Web of Things. In Proceedings of the International Conference on Autonomous Agents and Multiagent Systems, pp. 813-822, 2018.

The central computing unit is responsible for commanding the joints in real-time in order to execute the task, communicating with other components.

2.3.4.4 AI

The AI to support the manufacturing process is realized as an edge app. The main purpose of the AI is to identify the engraving areas of workpieces and to compute the grabbing points of workpieces from the images obtained from cameras deployed over the work bench/machines. Towards achieving these two objectives, the AI additionally requires image pre-processing, camera lens distortion correction and object (workpieces and markers placed on the surfaces) recognition. During the inference, the AI may fail to accurately determine the grabbing points for some workpieces. Under which, a human operator intervenes to carry out the grabbing tasks and the corresponding grabbing points and camera images are stored as new labelled training data. Followed by several such failures, the edge AI model will initiate retraining using the newly accumulated labelled data. This will update the AI model and reduce the frequency of human interventions over the plant operational time.

2.3.4.5 MACHINES

A great variety of products can be built depending on the machines available in the shared manufacturing plant. Using additive manufacturing in addition to conventional machines (e.g., for drilling, milling, or welding), almost arbitrary products can be made. A laser-cutter and -engraver and a 2D milling machine will be available in the demo setup for this use case. A machine-readable machine description, e.g., W3C WoT TD capability descriptions, enables the HyperMAS to store machine properties and capabilities and Agents to make use of particular machines in a production plan.

2.3.4.6 EDGE ORCHESTRATOR

The Edge Orchestrator is the central component to distribute tasks as edge apps inside the edge infrastructure. The Edge Orchestrator determines when and where (on which edge device) to start edge apps to be optimal with respect to service levels. It integrates with the Siemens SIMATIC Industrial Edge suite.

The Computational Resource Manager determines optimal allocations and is part of the Edge Orchestrator. It comprises an algorithm for the optimized allocation of individual Edge Apps or parts of Edge Apps composed of functions onto edge devices, while considering the network configuration. The deployment of Edge App functions can be tuned towards different optimization goals, e.g., reliability of compute nodes, response time of the application, or energy consumption. The Computational Resource Manager takes the IoT application configuration, its constraints, as well as the current edge and network configuration as input. After determining an optimal allocation, it returns a specification of it as output. During the whole allocation of an edge app, the Computational Resource Manager monitors whether optimality criteria for Edge Apps are still met.

As part of the optimization, the Edge Orchestrator also initiates the reservation resources with TSN Network Controller and the Communication Resource Manager.

2.3.4.7 TSN CONTROLLER

TSN controller is responsible to compute network schedules and reserve network resources in order to guarantee Quality for communication services. Communication services are requested through its northbound interface. For example, when human help is needed to guide a robot, Edge orchestrator requests a **tactile communication** between the robot and the helping human. TSN controller will plan and enforce this communication relation considering real-time and reliability constraints. Additionally, when security assurance platform detects suspicious operations from a potentially malicious actor, it triggers TSN controller to lock out the concerned device, i.e., to cut the according communication relation.

2.3.4.8 COMMUNICATION RESSOURCE MANAGER

The Communication Resource Manager enables allocation of wireless 5G resources based on the requests and requirements of each user. When a process like the Edge Orchestrator makes a request for a user to have a certain

data rate or latency, the Communication resources Manager receives it through its southbound interface. It then enforces an allocation policy that attempts to guarantee the requested resources and returns whether or not the requested resources could be guaranteed.

2.3.4.9 TRUST COMPONENTS

Several components are also deployed that support the trustworthiness aspects of the manufacturing use case, as presented in the subsections that follow.

2.3.4.9.1 SECURITY ASSURANCE PLATFORM

Furthermore, the integration of the Security Assurance Platform within the manufacturing environment will provide runtime, continuous assessment of the monitored manufacturing assets comprising the UC deployment. The platform will monitor the operation of both critical assets and the deployed security mechanisms, providing the operator at the backend with a view of the assurance posture of the whole deployment and enabling the timely response to changes in said posture. The evidence related to the changes to the assurance posture over time, as well as the evidence related to the timely and efficient response to attacks stemming from malicious actors' activities, will be stored in the DLT component. Furthermore, the SAP will integrate incident response mechanisms that, based on executable playbooks, will allow the operator to trigger defence strategies, when an incident is detected.

2.3.4.9.2 DISTRIBUTED LEDGER TECHNOLOGIES (DLTS)

DLTs are predicted to disrupt the manufacturing industry over the next few years with its high potential to fundamentally redesign core manufacturing and supply chains. Major manufacturers incur enormous time and expense in managing their complicate global supply chains, for example, identifying and selecting trusted providers, negotiating, and enforcing agreements, tracking products during production and delivery, and ensuring timely payments. These standard cumbersome processes are now largely manual, for example, still requiring human activities, such as, e-mails, phone calls and meetings for closure, which do not guarantee reliability and trustworthiness of the overall process. DLTs support the manufacturing industry to have transparency, and immutable communication and accounting systems which can provide trusted evidence and records of activities. By automating manual processes, a DLTs/blockchain network could ensure product quality and authenticity, accelerate transactions, and reduce processing fees.

In addition to comprehensive security mechanisms that are applied to ensure privacy and security of customer data (and which will also aggregate evidence from the DLT), whenever a machine or robot is tasked, contractual arrangements are set up using a distributed ledger.

2.3.4.9.3 MOVING TARGET DEFENSES (MTD)

In this Use Case, MTDs will not be autonomously triggered, but will require human intervention to take place (to isolate malicious entities). This intervention and triggering will be encoded and executed through the corresponding playbooks at the SAP (see above). Isolation in this use case can also take advantage of the TSN controller API.

2.3.4.9.4 AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA)

AAA provides centralized authentication, authorization, and accounting services. External entities employ these services to communicate with nodes that are part of an IntellIoT scenario in a safe and controlled manner. Two deployment types are available in order to facilitate services that support OAuth2 protocol as well as those that do not. The first case is straightforward; this kind of services communicate directly with the AAA component. For the second case, a reverse proxy is employed. It handles the OAuth2 protocol and acts as a middleman between the services and the external entities.

For the manufacturing use case, AAA will be used to secure the backend API calls.

2.3.4.9.5 INTEROPERABILITY BOX (IO BOX)

Interoperability Box (IO Box) enhances the connectivity of low end IoT devices by abstracting technical, syntactic and semantic interoperability issues. IoT devices can vary in the communication protocol, e.g. I2C or BLE, in the data exchange format, e.g., raw or CoAP, as well as the semantics used in the provided data. IO Box acts as a gateway for devices with limited capabilities. It is hosted on a device, e.g., RPi, providing the necessary physical interfaces to communicate with them. The selected host handles the device-specific low-level communication drivers. The IO Box uses those drivers to connect with the IoT devices. It then leverages the host's networking and computational capabilities to expose a high-level HTTP API. The API is described using W3C WoT TD. This results into a system where limited IoT devices can be accessed in a high-level manner.

For the manufacturing use case, IO Box will at least interface with MiroCard. MiroCard is a solar powered BLE device with integrated sensors. This is a device with significant resource limitation. When interfaced with IO Box, the data it provides will be accessible by HyperMAS which can then make decisions about the safety of the manufacturing equipment and trigger appropriate actions.

2.3.5 OPEN CALL #1 CONTRIBUTION

2.3.5.1 UC3 CONTRIBUTION BY TRILOGIS

The contribution given by Trilogis is focused on the computation of manufacturing KPIs that are based on position/movement data. Toward this end, the activities address the detection and localization of workpieces throughout the different production steps using identification/localization technologies. Among the potential technological solutions (e.g., UWB, BLE, Computer Vision, etc.), RFID is selected to detect the presence of workpieces within predefined working areas in UC3 demo site. Accordingly, multiple RFID readers will be deployed to define different detection areas where tagged workpieces are placed and moved. The localization approach is based on the proximity principle since each reader defines a delimited area with coverage proportional to the transmission power. The real-time update of position and movement of the workpieces enables the computation of different location-based KPIs useful to analyse the performance of the process. For example, some potential indicators are: waiting time in buffer, end-of-line time, occupation time, process productivity, cycle time, phase duration, handling time, handling sequence, etc. Other indicators can be defined in cooperation with stakeholders and/or partners involved in the UC3 demo.

The software platform TRACCIA by Trilogis (background IPR) will be used to manage the acquired position data, convert positions in geographic coordinates, and exploit Geographic Information System (GIS) technologies to extract proper information for the computation and visualization of the performance. Toward this end, a configurable dashboard is used to show graphs and gauges in the combination preferred by the user, and position data are shown in real-time on the interactive map where the layout of the UC3 demo is geolocalized.

2.3.5.2 FRAMEWORK CONTRIBUTION APPLIED IN UC3, BY MYWAI

MYWAI S.r.l. will contribute to the IntellIoT project by selecting a set of suitable enabling modules and services from its technological baseline, to be further specified and adapted for integration into the IntellIoT architecture, with the aim of extending its existing features in terms of advanced functionalities for supporting the emerging Equipment-and-Infrastructure-as-a-Service (EIaaS) business model and delivering edge intelligence to any equipment through the integration of sensors, hardware and software hybrid cloud-edge AI enablers, the adoption of innovative information interoperability models, the DLT-based storage and management of certified and secured equipment and process-related information. More in detail, from its flagship Edge Intelligence platform MYWAI will select a set of enabling modules and services suitable for integration into the IntellIoT architecture to support:

- Management of equipment "as a service", by delivering edge/very edge intelligence to any machine, orchestrating procedures execution, notifying anomalies/events/alarms, exporting/importing interoperable information models, offering dashboarding and analytics functionalities.
- Acquisition of multivariate data time series and images, Human in The Loop smart data labelling and detection of anomalies approval workflows. Dashboarding of real-time and/or historical data.

- Modeling, training and deployment of ML/AI algorithms from Cloud to remote CPU, FPGA and/or ASIC-empowered edge computers suitable for delivering low cost and low consumption artificial intelligence at the very edge of equipment and machinery.
- DLT-based storage and certification of sensors data, detected anomalies and process information using a new generation blockchain topology (IOTA, https://www.iota.org/) and a distributed file system (IPFS, https://ipfs.io/), to extend the offer of enhanced equipment-related technical (e.g. predictive maintenance, machines performance monitoring) and non-technical (e.g. fintech, insurtech) services.
- Multipurpose data acquisition IoT devices, embedding in a battery-powered enclosure an IMU combined with a flexible/reconfigurable set of additional application-dependent sensors (e.g., temperature, humidity, etc.) and supporting multichannel communication (e.g., cellular, BLE, WiFi).

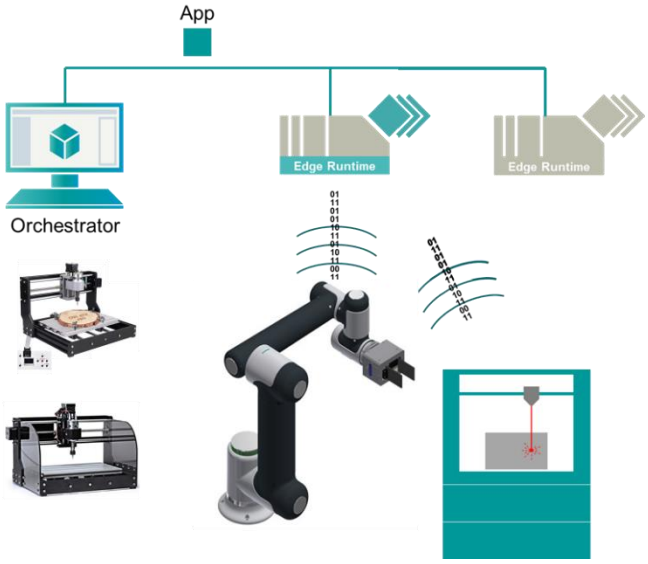
Selected MYWAI technologies will be integrated into the design of the IntellIoT architectural framework and mapped to each of the three use case storylines. With specific reference to UC3, MYWAI aims at showcasing open interoperability of production operational and technical data within the IntellIoT framework by enabling the flexible integration of equipment, sensor systems and data intelligence modules to offer new services and business models in the emerging Equipment-as-a-Service market.

2.3.6 SCENARIOS

2.3.6.1 SCENARIO 3.1 – COLLABORATIVE IOT

Scenario Name	Collaborative IoT
Scenario ID	UC3-Scenario 1
Partners	SIEMENS, HSG, HOLO, EURECOM, TTC, SANL, TSI, UOULU, AAU
Description	Our shared manufacturing plant receives a *goal* formulated by a customer. Agents that run in a HyperMAS together achieve this goal by assembling their individual plans, the plant has a flexible production cell, in our demo case equipped with a robot arm for grabbing workpieces and placing it in machines for cutting and engraving. A process plan consists of multiple tasks. A task can comprise models (e.g., a CAD-model), required resources (e.g., computing, network bandwidth), required device functions (e.g., cutting) as well as further constraints (e.g., dependability on other processes, completion time). A task is represented by a data structure (e.g., in JSON), which can be interpreted by an appropriate app, i.e., an agent representing a robot or a machine. Multiple agents, representing machines and robots, collaborate on fulfilling the plan. The execution of a task might include steps where a job is sent to a machine. A job is derived from a task and could e.g., be a cutting job sent to a laser cutter. In contrast to a task, the job might be represented in a machine-specific format which was generated from the task description by a machine specific app. The execution also relies on machine availability in the production cell, as well as on the computation and communication infrastructure for edge offloading. The different components of the manufacturing plant (robots, machines, interoperability box, humans, edge infrastructure) are connected via wired and wireless network, with robots, machines and humans taking the role of User Equipment (UE) and the edge infrastructure being composed of base stations and computation devices.

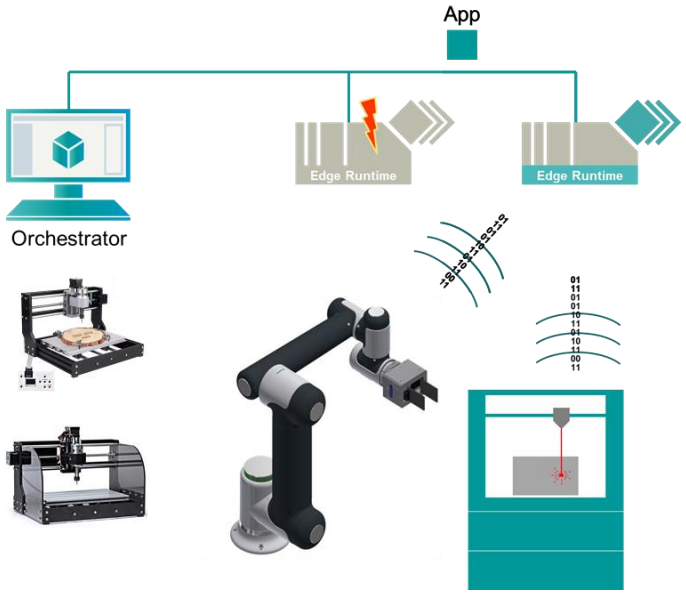
	In the scope of an IoT edge cloud environment, offloading is performed by web requests to specific edge apps. Accordingly, a production process step might require the deployment of an edge app. An example could be the offloading of AI-based image classification to an edge app. During the execution of the task, an image could be sent to the AI edge app, which returns the optimal grabbing position. Edge apps are deployed on edge devices, which might be deployed anywhere in the plant. The location and the properties of communication links to the edge devices is taken into account when choosing an edge device for offloading. Both are managed by an Edge Orchestrator, which takes care of app and device lifecycle management (start, stop, deploy, update, etc.). An edge app is a bundle of metadata plus a set of orchestrated containers, which run isolated microservices. An edge app could be an end user application (e.g., an AGV navigation app) or a service for other edge apps (e.g., AI inference). The differentiation between tasks and apps is that a task describes in a specific data format what is to do while an app is a program which executes actions or provides services. For example, an app could contain the application logic to execute a task. This scenario shows how offloaded computation tasks are distributed in a multi-edge environment. A management system schedules tasks to dedicated machinery and edge devices taking network conditions into account. With the management system being a decentral, agent-based system running on all involved assets, the term collaboration of assets in order to reach the given goal becomes meaningful.
Key Scenes	**Key Scene 1.1**, see Figure 18: A customer requests a new product to be manufactured by the shared manufacturing plant and specifies the production goal using a dedicated interface. In our proof of concept, the customer specifies a desired engraving on a specific material, which together represent the desired product. This goal is submitted to a HyperMAS where several agents collaborate to achieve it. They do this by relating the goal to formal descriptions of machine interfaces through agent plans. For example, this could be the steps required to achieve the goal: 1. **Agent in HyperMAS** requests **computation** of best grabbing spot at an **AI edge app** 2. **Agent in HyperMAS** instructs **robot** to grab the workpiece at that grabbing spot 3. **Robot** grabs the workpiece 4. **Agent in HyperMAS** instructs **robot** to transport the workpiece to a laser cutter 5. **Robot** transports the workpiece to the **laser cutter** 6. **…** **Key Scene 1.2**, see Figure 18**:** The agents execute these steps in a continuous reasoning cycle while making use of available and suitable artifacts (e.g., the robot and laser cutter as well as compute resources such as the AI edge app). An AI application deployed in the edge environment is processing the images from the camera on the concerned machine and computes the best grabbing spot autonomously.



Key Scene 1.3, see Figure 18**:** Similar as in key scene 2, the derived plan is deployed to an execution environment for plans on the edge. According to the tasks of the plan, resources are optimally allocated on available and suitable machinery (robots or CNC), and edge devices (for computing tasks within the plan).

Computing, such as computing the best grabbing spot of a workpiece, is provided by an edge app. Multiple apps to realize functionality (e.g., HIL service, machine control, AI) are deployed in the edge infrastructure and optimally allocated to edge resources (also taking into account the network specifics and failover constraints) while making their services available to agents in the HyperMAS.

Key Scene 1.4, see Figure 18: During production, the connection between the robot and the edge device is not the optimal choice anymore (e.g., the performance is getting worse due to network congestion or the edge device even fails), for which it is decided move the edge app with its state to another edge device.

	
Potential Variation of the Scene	**Variation Scene 1:** In a variation, a production step is to be carried out on a more distant production cell. Accordingly, an AGV moves the workpiece there. The path is predicted and required edge apps and states are transferred to the edge devices close to the new location. **Variation Scene 2:** Interoperability box is also deployed. It is coupled with MiroCard which monitors the environment e.g., temperature. The data gathered are exposed through Interoperability Box using an HTTP API accessible by the HyperMAS Agents. When critical conditions are detected, the Agents trigger the appropriate actions.
Purpose	The purpose of this scenario is to show how the production plan is transformed to tasks for different actors in the production process. It shows the interplay between the production world and the IoT world.
Sources of Risk	Network disruptions (link failures, interference) as well as hardware faults on edge devices and IT infrastructure can cause service outages affecting crucial process steps. For example, it is not possible to determine the optimal grabbing spot because the AI fails to infer accurately. In the event of those problems, the production might be disturbed or even stopped. Downstream fallback mechanisms should guarantee that every machine is going to safe state on failures. Those mechanisms are part of a production system which is not addressed in this project.
Threats	[1] Physical manipulation of edge devices, machines and IT infrastructure [2] Eavesdropping on network link (e.g., wireless link) [3] Manipulation of network traffic [4] Network attacks on IT/OT infrastructure from Internet [5] Malware on edge apps
Successful end condition	The scenario is accomplished when edge apps are deployed, so that productions steps can use required services.
Failed end condition	One goal of the scenario is to show resilience. However, all attempts to relocate an app to another edge device could fail or no connection could be established or there might be a hardware fault which cannot be replaced by another hardware component. In that case, the

	process continues as long process steps don't require communication or task offloading. Else, the process stops, and safety critical machines go in a safe state. In any case of failure, service personnel are alerted via notification mechanisms.
Frequency of occurrence	The scenario has continuous aspects regarding the deployment of tasks to the edge infrastructure. This mostly happens when the production process changes. Reorganization on failures or heavy utilization should occur from time to time.
Actors	Customer, Agents in the Hypermedia MAS Planner, Machines and Robot
Information exchange between actors	Customer sends goal to Hypermedia MAS Infrastructure (i.e., the Agents' runtime). Agents assign jobs to machines and robots, which provide state information and interface descriptions. HyperMAS components able to discover and access W3C WoT TD capability descriptions of machines. HyperMAS components able to interact with machine APIs based on these capability descriptions.
Challenges for scenario validation (T5.3)	Definition of a process plan comprised of multiple tasks, which can be distributed in the process line. Deterioration of network condition, so that rescheduling has to occur. Definition of KPIs of production efficiency. Implementation of offloading infrastructure and edge apps, in such a way that offloading shows a benefit. Interoperability of machines and components in demo setup.
Changes with respect to D2.1	• Deleted the former Key Scene 1.5, which was related to updating local AI models of multiple robots using federated learning, since the setup includes a single robot that carries out the manufacturing tasks.

Figure 18 provides a UML-based diagram of the scenario. This figure shows the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

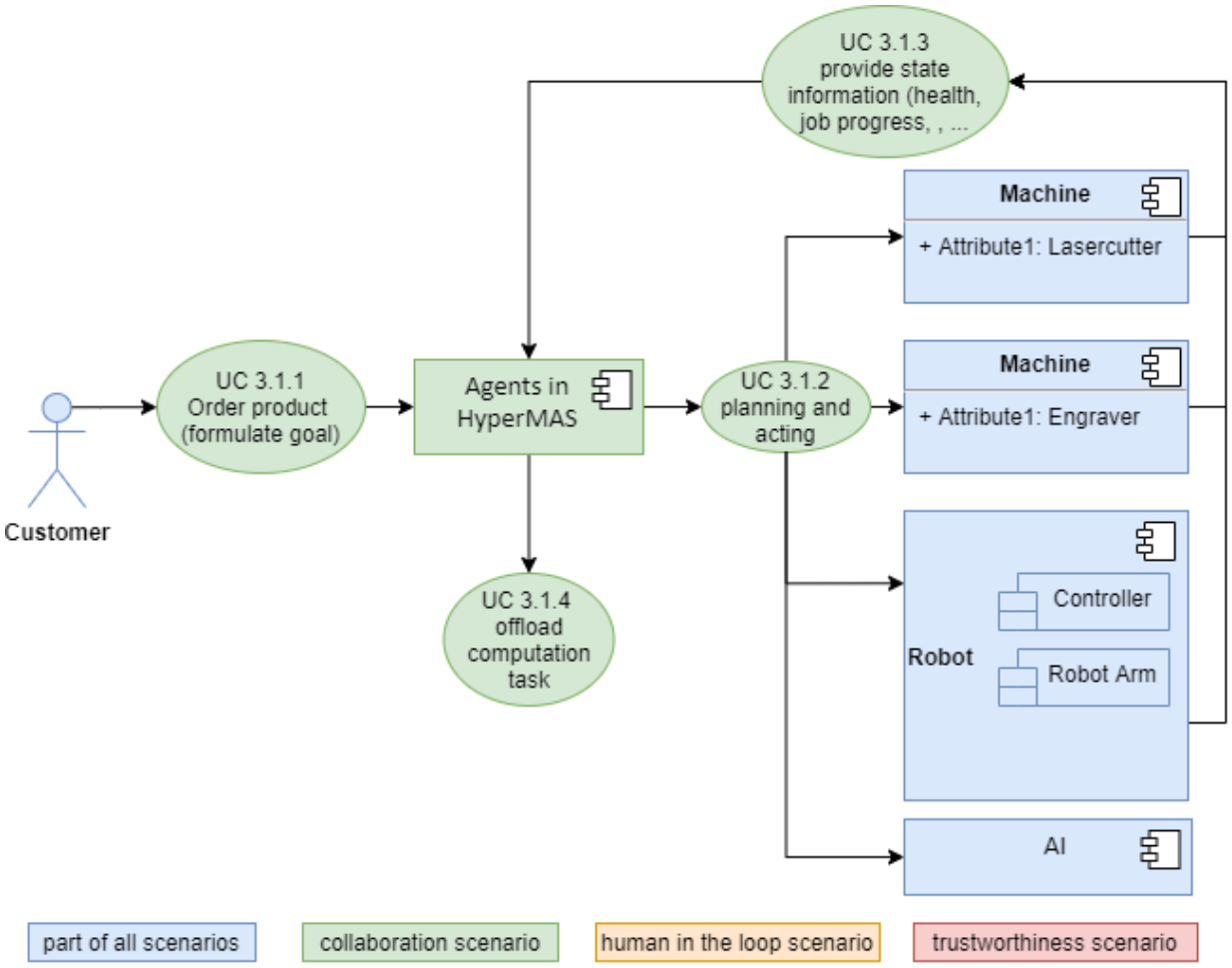
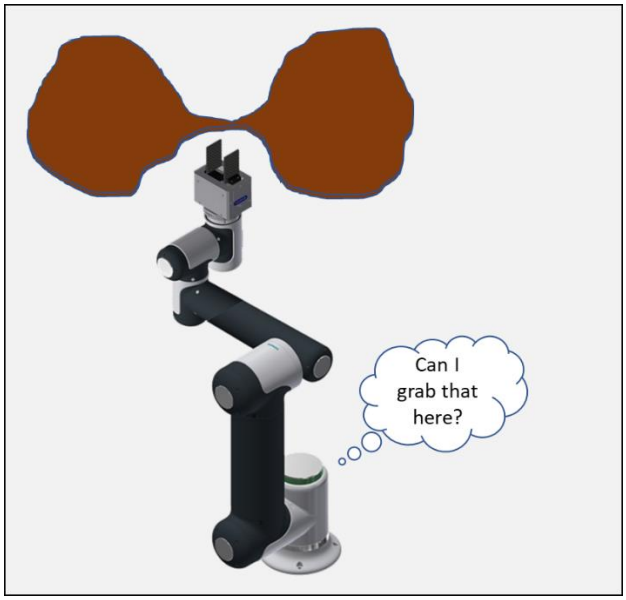
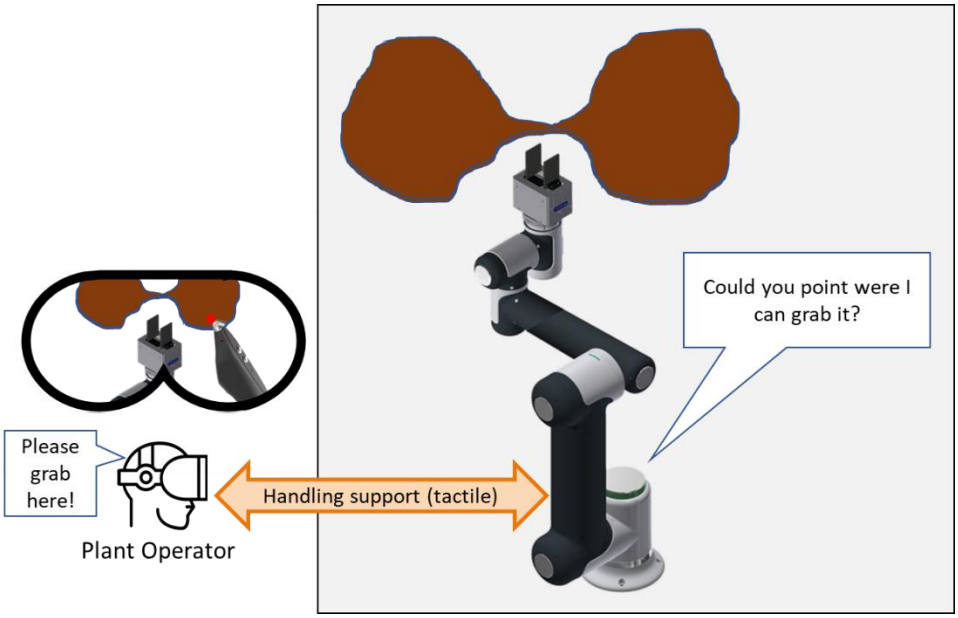


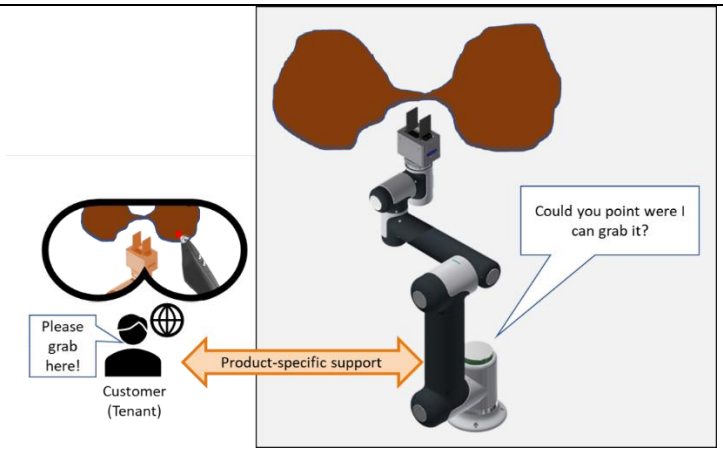
Figure 18: UC3 Collaborative IoT scenario diagram

2.3.6.2 SCENARIO 3.2 – HUMAN-IN-THE-LOOP

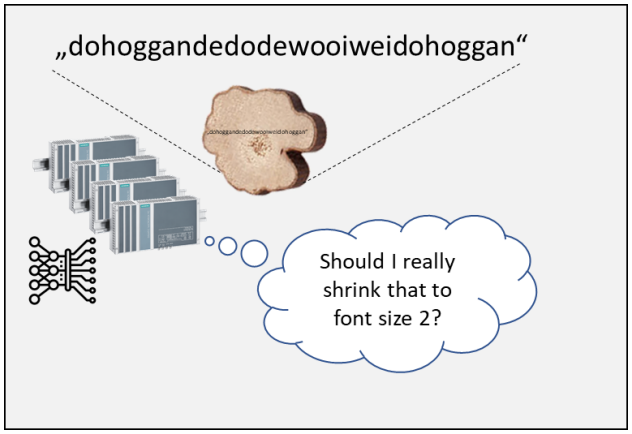
Scenario Name	Human-in-the-Loop for shared manufacturing
Scenario ID	UC3-Scenario 2
Partners	SIEMENS, HSG, HOLO, EURECOM, TTC, SANL, TSI, UOULU, AAU
Description	Our shared manufacturing plant produces products based on production plans. Agents that have been configured through a no-code agent programming environment automatically execute production plans from a) a formal specification of a manufacturing goal by a customer and b) explicit formal descriptions of the available production capabilities in the form of W3C WoT Thing Descriptions. During the running manufacturing process, edge AI has an insufficient level of confidence in a decision, e.g., on about how to grab a workpiece. To solve its issue, HyperMAS asks the Human-in-the-loop (HIL) service for help. The latter passes this help request to a human, e.g., the plant

	operator or machine owner, who is connected to the HIL infrastructure. At this time, production has already been started, i.e., the concerned machine and robot are blocked. Thus, this task is time critical with respect to machine outage times. After the human solves the issue, the grab spot used by the human operator is stored along the image of the workpiece as new labelled training data. Over time, after accumulating a sufficient amount of new labelled data (e.g., 10% of new data samples w.r.t. the training dataset), the edge AI is re-trained to overcome similar situations in the future. In another key scene, the automatic creation of a production plan fails because: a) There is no solution: there is no production plan for the given goal with the existing production capabilities and shopfloor environment. b) The system is unable to infer a production plan because it cannot relate the formal specification of the goal to the available production capabilities or the state of the environment. This is either because of: • a fault in the physical world or the modelling of the production capabilities or environment. • a system design choice in the physical world or the modelling of the production capabilities or environment. c) The system is unable to infer a production plan because this takes too much time or computational resources. For (a), the human might be asked to verify or to adapt or state the goal more precisely. For (b) and (c), the human is asked to help to correct the situation. This problem will typically occur before the manufacturing starts. Whenever changes occur during manufacturing, e.g., in machine availability, HyperMAS might need to react to this, which also might require human help. In this case getting that help is time-critical.
Key Scenes	**Key Scene 2.1,** see Figure 19: The AI which is responsible to compute a grab spot is unsure how to grab a workpiece. Thus, it calls a component of the HyperMAS, which invokes the HIL service in order to contact the plant operator for clarification. 

	A real-time tactile AR connection to the plant operator is established as follows: Plant operator receives real-time image streaming from the camera on the robot. The image stream is displayed on AR glasses. The plant operator supports the decision on how to grab and positions the robot through guiding the robot by grabbing and moving the robot arm through the camera image visible in his glasses with the stylus pen (Thanks to the QoS guarantees provided by the communication network, the operator does not feel any delay between his actions and the reaction of the robot, what re refer to as tactile feedback). Alternatively, the operator might directly point the grab spot with the stylus pen. After receiving help from the human, the robot completes its task. The manufacturing process can continue with short delay.  **Key Scene 2.2,** see Figure 19**:** In order to get a more detailed view of the current situation from different observation angles, the plant operator moves the robot without grabbing the workpiece, while receiving the image stream from the associated camera on the AR glasses. **Key Scene 2.3,** see Figure 19**:** The edge AI will store the decision of the human operator along the image of the workpiece as new labelled data to retrain the AI model in future. **Key Scene 2.5,** see Figure 20: The uncertainties of grabbing a workpiece could be due to unseen shapes and textures of the workpiece. In this case, help from the *customer* having provided this workpiece might be required. The customer might not be as trustworthy as the plant operator or a machine owner, as everybody can easily act as a customer. Additionally, a customer might be unexperienced controlling a robot. Therefore, the customer will only be allowed point to the grab spot he wants to recommend, without moving the real robot.



Key Scene 2.6, see Figure 19: While HyperMAS attempts to derive a work plan and machine orchestration from a customer goal, HyperMAS is unsure how to interpret the goal formulated by the customer and contacts the customer for clarification. A reason could be, that the provided text is too long for the available work pieces.



A connection to the customer is established and the customer supports the decision by refining his goal description. HyperMAS is now able to plan the manufacturing process.

Potential Variation of the Scenario	**Variation Scene 1:** Whenever an off-premises actor (customer, machine owner, etc.) is contacted (instead of the plant operator) by a component of the HyperMAS it might be possible to set up a tactile AR communication link over a long-distance network, e.g., if a dedicated high-performance infrastructure is available, maybe including 5G technologies. This would also introduce stringent security requirements to avoid that an external human harms the workpiece, the robots or other parts of the plant. **Variation Scene 2**: Uncertainties regarding the capabilities of available machines or robots or the availability of raw material could occur. In this case, HyperMAS shall contact the plant operator instead of the customer for help.
Purpose	The purpose of this specific scenario is to solve blockings in the process of manufacturing products, typically in very small lot sizes, based on goals defined by customers. Such a blocking could occur while HyperMAS attempts to derive a production plan from a customer goal or while a robot tries to grab a workpiece.

	If HyperMAS is unsure how to interpret the customer's goal, instead of taking the risk of an unsatisfying product for the customer, he is involved in the decision process at an early stage. If a robot is stuck while grabbing a workpiece, the purpose of this specific scenario is to solve a blocking of cost-intensive production machines and robots as fast as possible, i.e., without requiring the plant operator, customer or machine owner to physically move to the concerned machine and robot. Now, the human will teach the robot, whose associated AI will learn from this help over the time for future decisions.
Sources of Risk	**All possible sources of risk in terms of safety and functionality** [1] Wrong interpretation of machine capabilities by HyperMAS and/or plant operator, machine owner respectively, could result in damages of machines, robots, and the workpiece. [2] Wrong interpretation of the options presented to the customer could lead to wrong decisions and subsequently to an unsatisfying product. [3] Actions derived from wrong decisions or wrong interpretations of human interaction might bring the product-in-progress to an undesirable state irreversibly. [4] Long delay or large jitter on the tactile communication link between human and robot might lead to unintended movement, which might lead to damage of robots, machines, or workpieces. Poor picture quality is less critical, as this is obvious to the human operator and should lead him to very careful movement; to the extent of stop in worst case. Therefore, communication QoS shall be monitored (or predicted) and image resolution shall be adapted if necessary (Quality of experience for the user). [5] Abrupt interruption of the end-to-end connection for a sustained duration, which leaves the robot in a state that is not well-defined. This can be addressed by suitable timeout mechanism and definition of fallback states. [6] Giving control over the robot to potentially unexperienced machine owners could lead to unintended movement, which might lead to damage of robots, machines, or workpieces.
Threats	**All possible threats in terms of security.** [1] When manufacturing a product for a customer, the goal description needs to be shared with the plant operator and eventually with 3rd party machine owners, at least partly. This is potentially sensitive data; e.g., if the goal is a prototype for an undisclosed invention. [2] Plant operator and machine owners will get to see the semi-manufactured product of a customer. This might be critical, e.g., if the goal is a prototype for an undisclosed invention. Therefore, the video stream shall be prevented from being seen by others. [3] Malicious or counterfeit plant operators or 3rd party machine owners could lead the HyperMAS to decisions which result in damages of machines, robots, and workpieces. [4] Malicious or counterfeit plant operators or 3rd party machine owners could intentionally move the robot to damage machines, robots, and workpieces or could spy out images from workpieces, machines, and the whole plant. [5] ICT assets could be compromised by malicious actors or human error.
Precondition for the Scenario	AI is trained to be able to grab a set of workpieces. During the running manufacturing process, a workpiece occurs, which differs significantly from the ones the AI has been trained on, which triggers AI to ask for human help.

	Agents in the HyperMAS are configured to interpret goal descriptions from customers and to derive a process plan and machine orchestrations from that. A goal description significantly differing from previous goals, and / or comprising ambiguities, causes HyperMAS to be unable to derive a confident decision, which triggers it to ask for human help.
Success end condition	Robot is enabled to grab and/or place a workpiece with the help of the plant operator, machine owner or customer and the edge AI has accumulated new data to learn from this help for future decisions.
Failed end condition	Plant operator, machine owner and customer were not able to support the robot. Thus, production could not be continued. Maybe, it was in fact not possible to grab the workpiece with the available robot. Customer, plant operator or machine owner were not able to support MES; or MES was not able to interpret the help. Thus, no production plan could be computed. Maybe, it was in fact not possible to produce the desired product with the available machines, or the customer had conflicting requirements.
Fatal end condition	Robot has damaged, with or without human intervention, a workpiece, a machine, or itself, due to a wrong decision on grabbing or placing a workpiece. MES computed, with or without human help, a production plan which leads to an unsatisfying product or to damage of robots or machines.
Frequency of occurrence	In worst case, it could occur for every pick and place operation, for every new goal defined by a customer respectively. The goal is to be having it occur much less frequent, additionally decreasing by learning from human help.
Actors	Customer, plant operator and machine owner; Agents in the HyperMAS, AI, HIL Service, HIL application, Edge Orchestrator, TSN controller, communication resource manager, and robot.
Information exchange between actors	Image stream of current situation from the camera on the robot to the AR glasses at the operator (where the robot struggles to grab a workpiece); Help from plant operator or customer in the form of movement commands in form of destination coordinates. In variation: Description of the issue HyperMAS has with the customer goal (or machine capability description); Help from customer or plant operator in the form of goal clarification.
Challenges for scenario validation (T5.3)	• Provision of new workpieces to the plant edge AI to prove that it recognizes uncertainties in its decision and requests human help. • Provision of slight variations of the former workpieces to the plant edge AI to prove that it learns from human help. We might use a simulated environment to avoid repetitive manual interventions by the human operator. • Provision of ambiguous goals to the HyperMAS to prove that is recognizes uncertainties in its decision and requests human help. • Provision of imprecise machine ability descriptions (W3C WoT Thing Descriptions) to the HyperMAS to prove that it recognizes uncertainties in its decision and requests human help. • Provision of new goals to the HyperMAS to prove that it recognizes uncertainties in its decision and requests human help. • Provision of slight variations of the former goals to the MES to prove that it learns from human help.

Changes with respect to D2.1	• Revised key scene 2.3, which could be misinterpreted as the model can be retrained with a single additional support from the human operator. The revised scene specifies the need of accumulating multiple samples over the failures of AI inference prior to model training. • Deleted former key scene 2.4, which was invoking the machine owner when AI is unsure how to place a workpiece in a machine. This is not feasible, because AI is not concerned for placing a workpiece in a machine. • Adapted key scene 2.5, so that the customer cannot directly move the robot, but point the grab spot. • Deleted variation scene 3, which explains the transfer of AI models between different robots. It is no longer applicable for the setup with a single robot. • Removed key scene 2.7 because trustworthiness is demonstrated in scenario 3.

Figure 19 and Figure 20 provide UML-based diagrams of the scenario. These figures show the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) have been described in more detail in deliverable D2.5.

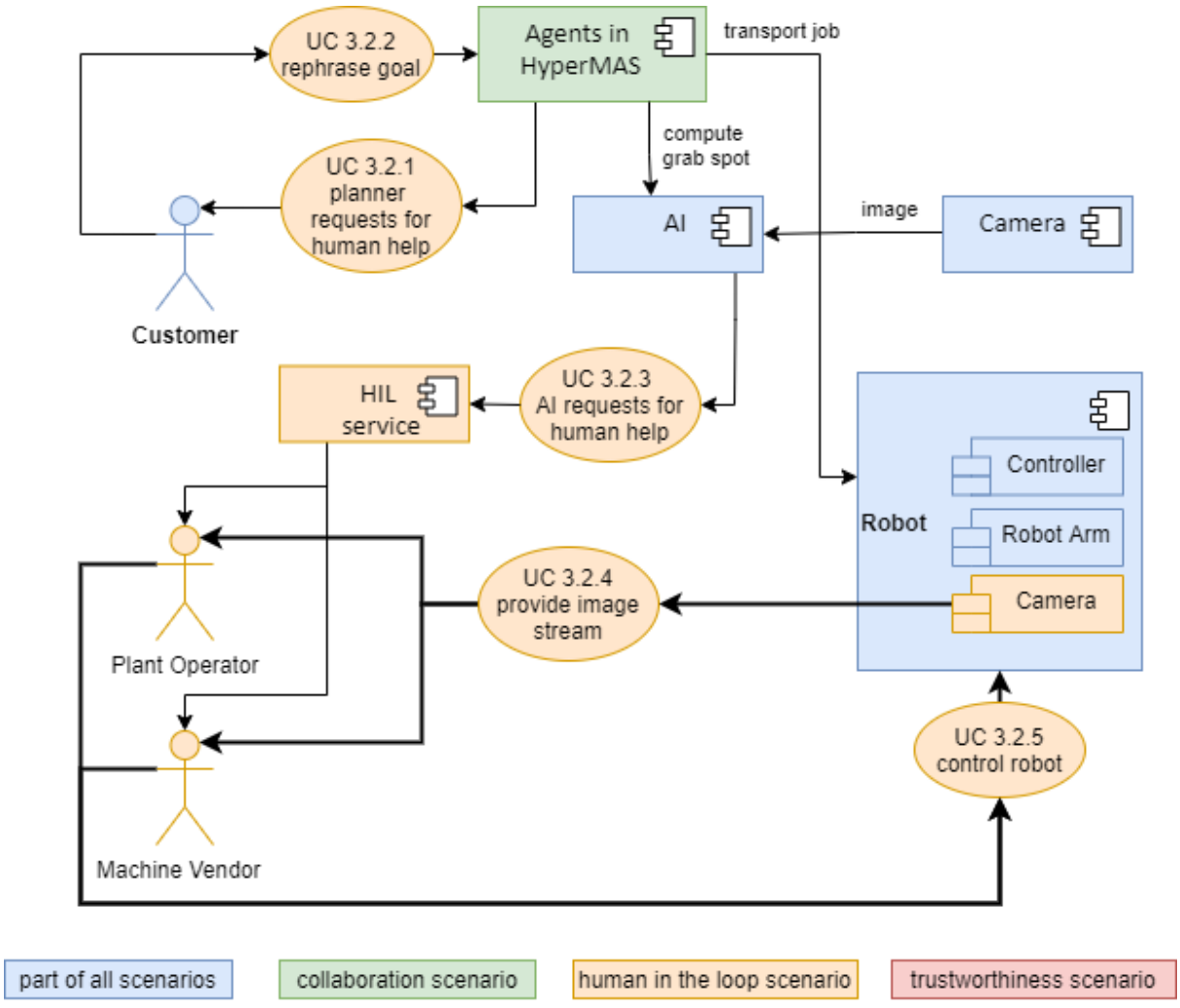


Figure 19: UC3 human-in-the-loop scenario diagram

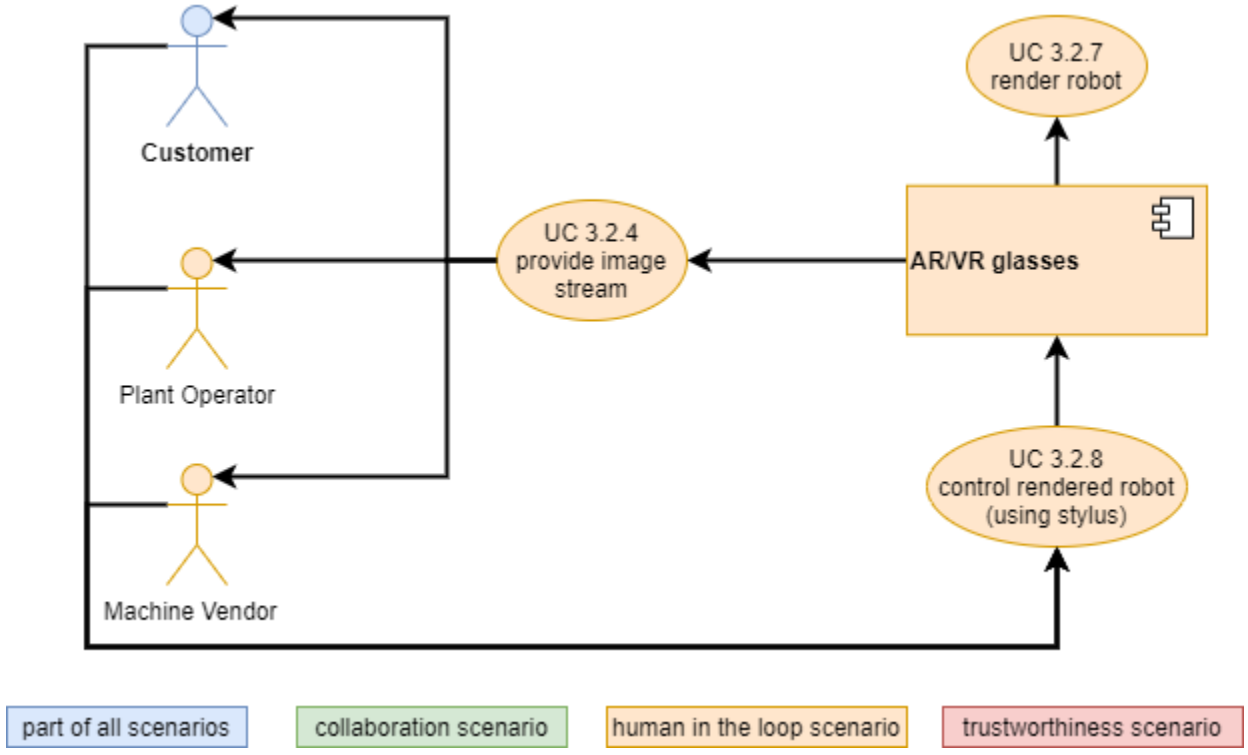
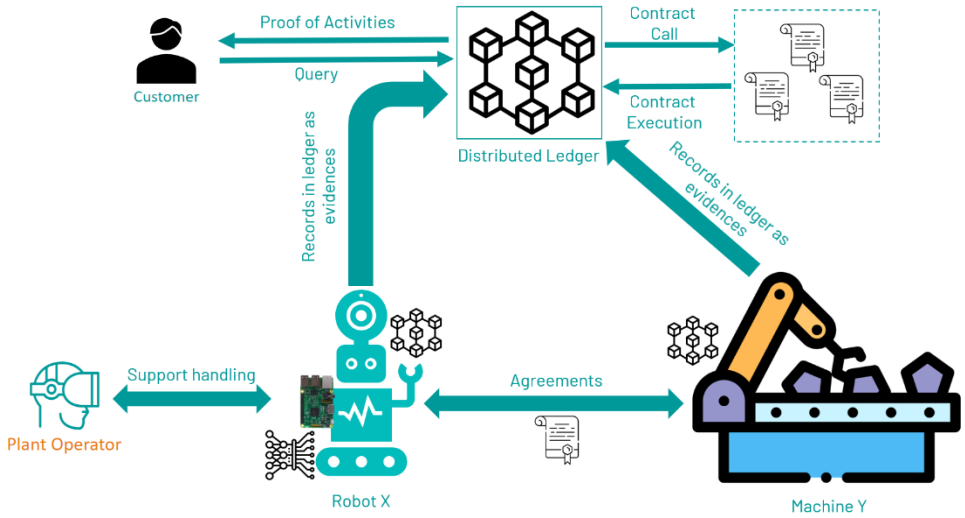
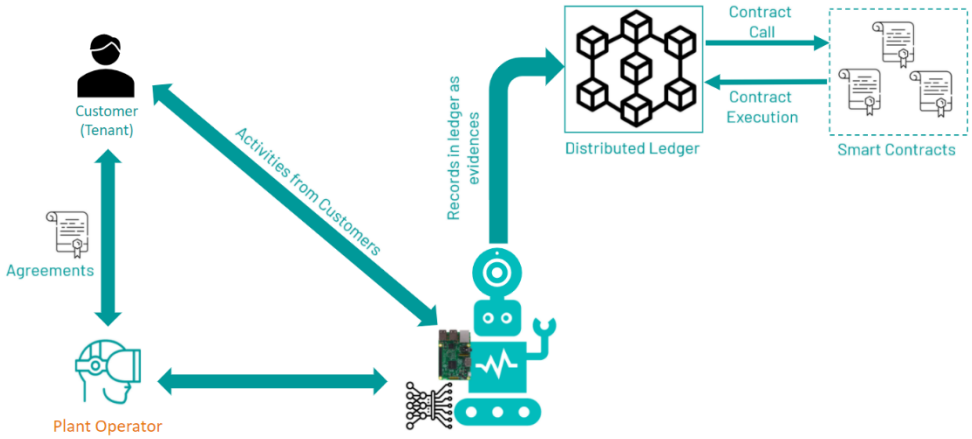
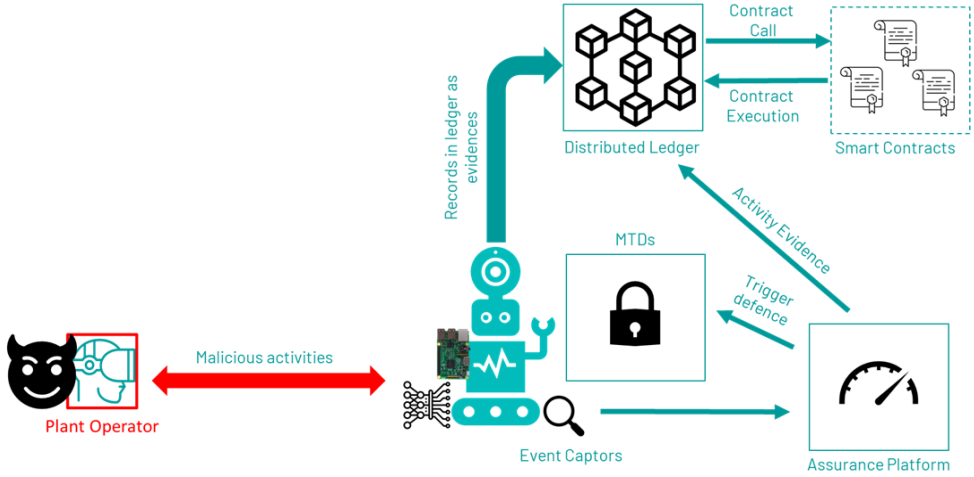


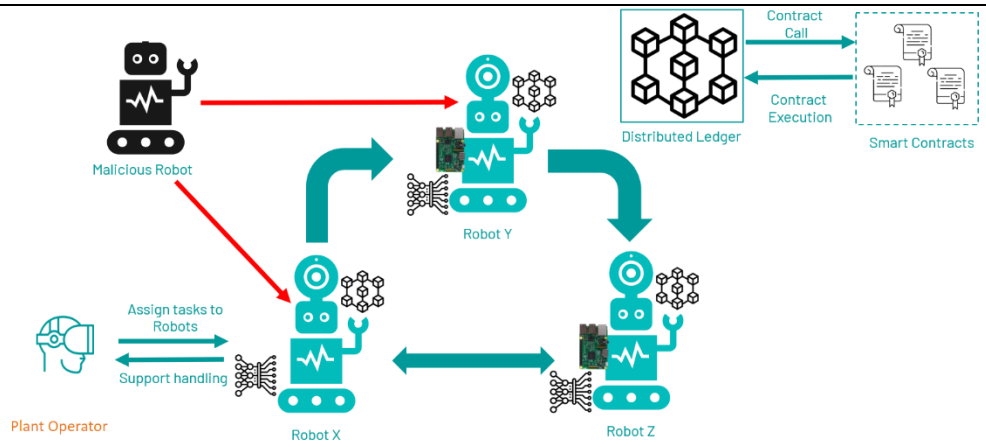
Figure 20: UC3 human-in-the-loop scenario diagram with rendered robot

2.3.6.3 SCENARIO 3.3 – TRUSTWORTHINESS

Scenario Name	Trust by design for shared manufacturing
Scenario ID	UC3-Scenario 3
Partners	SANL, TSI, AAU, EURECOM
Description	The shared manufacturing plant is producing a product according to customer specifications, using the processes demonstrated in the previous scenarios. Nevertheless, the customer requires that the whole process is trustworthy, accountable, and auditable. To achieve this goal, the third scenario revolves around the integration of the following elements: (1) Providing contractual arrangements or confidential handling with a smart contract for (audit of) authentication and authorization actions, for example when a robot wants to manipulate one of the machines, eventually from a third-party; (2) Providing recording of the operations with DLT: sequence and timing of processes and events (e.g., component handling failures, delays). This is important in solving disputes (e.g., delayed delivery of orders, claims of unnecessary billing) and in analysing safety-related events that may occur (post-incident analysis). (3) Providing evidence from the operation, for which the security assurance platform provides continuous security and privacy by deploying event captors at the different edge, machines and robot components that provide continuous security monitoring and reporting of potential threats, triggering defense mechanisms based on pre-defined Playbooks encoding these strategies and orchestrating other trust enablers (e.g., MTDs);

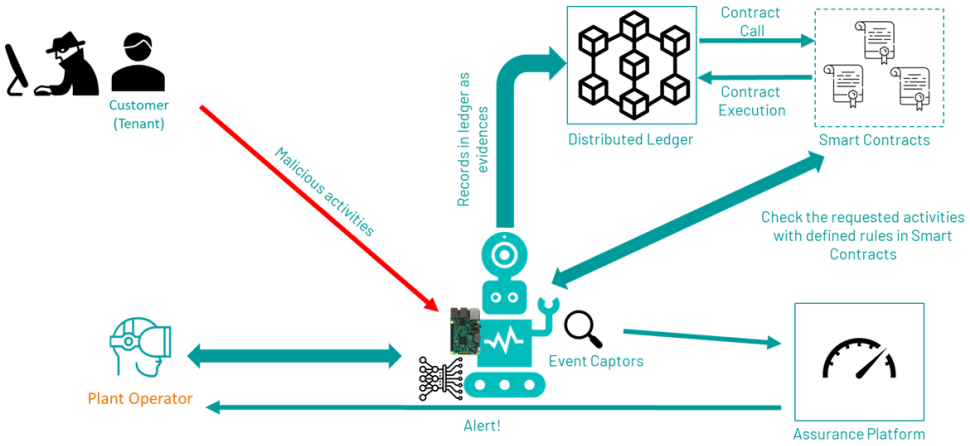
	(4) Providing secure remote access to machines and robots only for eligible users by adding a AAA component. A reverse proxy is used as a middleman to take care of the OAuth2 protocol.
Key Scenes	**Key Scene 3.1** (Figure 21): In this key scene, the DLT-based smart contracts can play as a key actor, which is executed autonomously based on the agreement between customers and plant operators, e.g., time running, task detail, etc. In order to use the machine, a smart contract is arranged beforehand between the plant owner and the machine owner. After the contract is arranged, the Agents in a Hypermedia MAS can use services from the third-party machine, for example, data or specific actions. All these activities are recorded in the ledger as a proof.  **Key Scene 3.2** (): A customer request has been completed, but there is a delayed delivery, and the customer does not agree with the total amount in the bill. The customer requests explanations from the plant owner. The plant owner uses an HMI to request information recorded in the DLT, where all the transactions, agreements and smart contracts have been registered. This can be used as the proof in the dispute with the customer, e.g., to prove that robot "X" and machine "Y" were used for "T" hours, and this has a total cost of "S" EUR. This information is retrieved from the DLT and available to all parties in the DLT. 

	Key Scene 3.3 (Figure 22): At various intervals, the plant operator (IT staff) carries out assessments to verify the security posture of the infrastructure (e.g., to identify configuration errors or systems needing patching). **Key Scene 3.4** (Figure 22): Considering the possibility of malicious employees within the manufacturing environment (e.g., a disgruntled employee), the system can detect & defend against malicious activity coming from internal users, i.e., a realization of an insider threat. Exploiting the human-in-the-loop mechanisms giving her control over the robot, the malicious actor moves the robot in a non-standard pattern (e.g., to damage the equipment and otherwise obstruct the manufacturing process on the factory floor). The DLT event captor associated with robot "X" provides continuous monitoring of the robot's telemetry, sending an alert to the Security Assurance Platform. The Security Assurance Platform, through its continuous monitoring feature, immediately informs the plant (security) operator, and triggers the associated incident response playbook, giving her the option to cut the control connection to the malicious operator. 
Potential Variation of the Scenario	**Variation Scene 1:** Agents in a Hypermedia MAS assign tasks to group of robots and machines, and they need to agree on decisions. In general, to make a collective decision, robots in a swarm need to share their information and to aggregate this information using a distributed consensus protocol. Consensus agreement is a vital capability for robots in manufacturing plants, for instance, for path selection, spatial aggregation or collective sensing services. However, the presence of a malicious robot, called Byzantine robot, could prevent connected robots to achieve consensus using traditional consensus protocol. The emerging of distributed ledger enables these robots to achieve consensus in a distributed manner and defend against Sybil Attacks.



Variation Scene 2:

In a variation of Key Scene 3.4 above, a black hat acting as a customer interacts with the plant with the intention of describing a special goal, which causes the AI to face issues while handling it. This results in the AI asking the machine owner for help. When being asked for help, the black hat, now acting as machine owner, moves the robot in a non-standard pattern (e.g., to use the camera on the robot to spy out technical details of competitors products within the plant). The DLT event captor associated with robot "X" provides continuous monitoring of the robot's telemetry, sending an alert to the Security Assurance Platform. The Security Assurance Platform, through its continuous monitoring feature, immediately informs the plant operator, and also triggers the associated incident response playbook, giving the operator the option to cut the control connection to the malicious customer.



Purpose	The purpose of this scenario is to design a trusted communication system for shared manufacturing. DLTs create a transparency and immutability environment and allow all participants to access the distributed ledger to maintain transactions without the need of third party or untrust entity. With the inherent trackability and traceability features, DLTs provide some advantages to this UC:

	(i) reduce the cost of execution. In the DLT-based manufacturing systems, the central hub is eliminated, so the cost of generating transactions is reduced and more secured. (ii) enhanced traceability and transparency. All transactions are executed and recorded in the common distributed ledger transparently and immutably, so that within a supply chain, all history transactions are real-time or near real-time audited. Besides, the transactions are secured against modifications, so DLTs are ideal for industries with strict compliance requirements. (iii) Secured connectivity: DLTs allow the storage of all transactions into immutable records and every record is distributed across many participants. Thus, security in DLTs comes from the distributed characteristic, but also the use of strong public-key cryptography and strong cryptographic hashes. Furthermore, in the case of detected malicious incidents, and in contrast to the other UCs, here the focus is on execution of defence strategies that involve a human-in-the-loop (operator) at runtime, who can view and judge if the next steps in the strategy should be executed.
Sources of Risk	• The communication connection is not reliable or fast enough • Scalability issues of DLTs in manufacturing systems. Since the limited storage of robots or devices, while the number of DLT transactions generated increases significantly, so the potential solution could be used as an off-chain storage (e.g., IPFS) • Accessibility, anonymity, and authentication and access control of devices. • Sensors and Robots can be compromised to transmit wrong information to a blockchain
Threats	All possible threats in terms of security. Compromised robots, Sybil attacks, 51% attacks, other insider threats
Precondition for the Scenario	The key scenes describe the DLT-based manufacturing system which requires every participant installs and owns a version of ledger and synchronizes with the rest of network. For that, all involved participants need enough storage and computing capabilities and secured connection with others.
Success end condition	The scenario is successful when (i) the communication between the involved parties is secured and guaranteed; (ii) the collected data and information uploaded to distributed ledger are correct and trusted; (iii) the smart contract is implemented among partners to agree on common rules and contracts, and (iv) the malicious insider attacks are detected and mitigated.
Failed end condition	In key scene 1, the smart contract is not defined / instantiated properly, failing to record critical manufacturing transactions to the ledger. In key scene 2, the DLT fails to report and produce evidence that are adequate to provide the customer with the needed guarantees regarding the manufacturing process. In key scene 3, the system fails to detect the malicious activity and/or fails to mitigate the attack once it is detected.
Fatal end condition	Lack of capabilities of devices Scalability issues of DLTs The communication between actors is not secured Successful 51% attack from malicious nodes
Frequency of occurrence	Key scene 1 is base-line of overall system for recording and monitoring when there is a need for exchanging and trading
Actor(s)	Customer, Distributed Ledger, Robots, Machines, Malicious entities (compromised robots, malicious employee), Security Assurance Platform, MTDs

Information exchange between actors	Exchange of control data and handling request between planner and robots and machine The data uploaded to Distributed Ledger for recording data Query requests for verification between machines and distributed ledger
Challenges for scenario validation (T5.3)	The loss of communication among the devices in shared manufacturing The noise in communication, and the correctness of information
Changes with respect to D2.1	• Added key scene 3.3 to showcase the assessment capabilities of the SAP • Exchange of key scene 3.4 and variation scene 2 in order to demonstrate the more challenging insider-attack with less overhead. • Inclusion of playbooks in key scene 3.4 to specify, automate & orchestrate defence strategies (including involving the human-in-the-loop for incident response). • Update of sequence diagrams to better reflect actual IntelllioT architecture & deployment

Figure 21 and Figure 22 provide a UML-based diagram of the scenario. These figures show the activities of the individual entities and the interaction between the different entities within the scenario. The individual activities (bubbles in the diagram) will be described in more detail in deliverable D2.5.

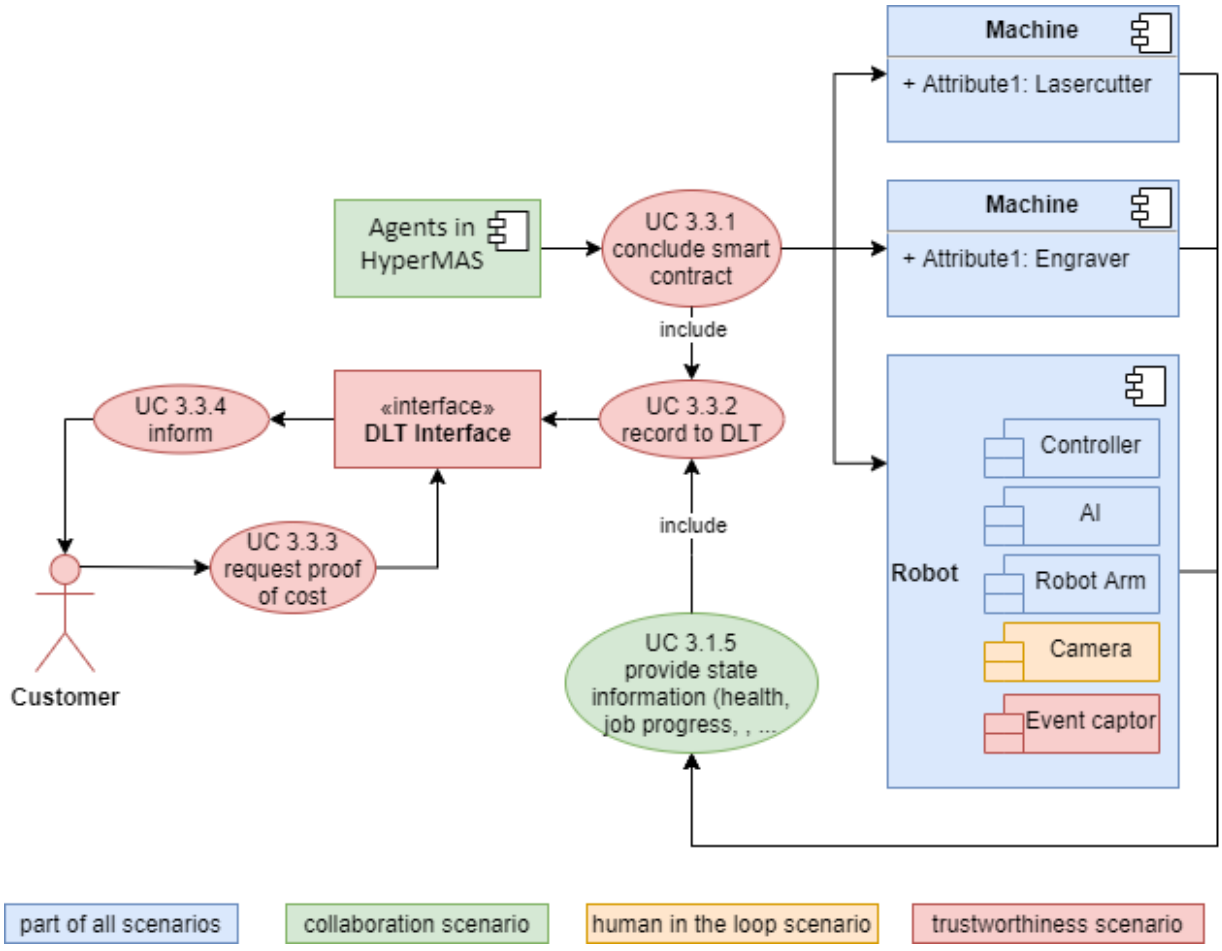


Figure 21: Use case diagram trustworthiness - proof (key scenes 3.1 & 3.2)

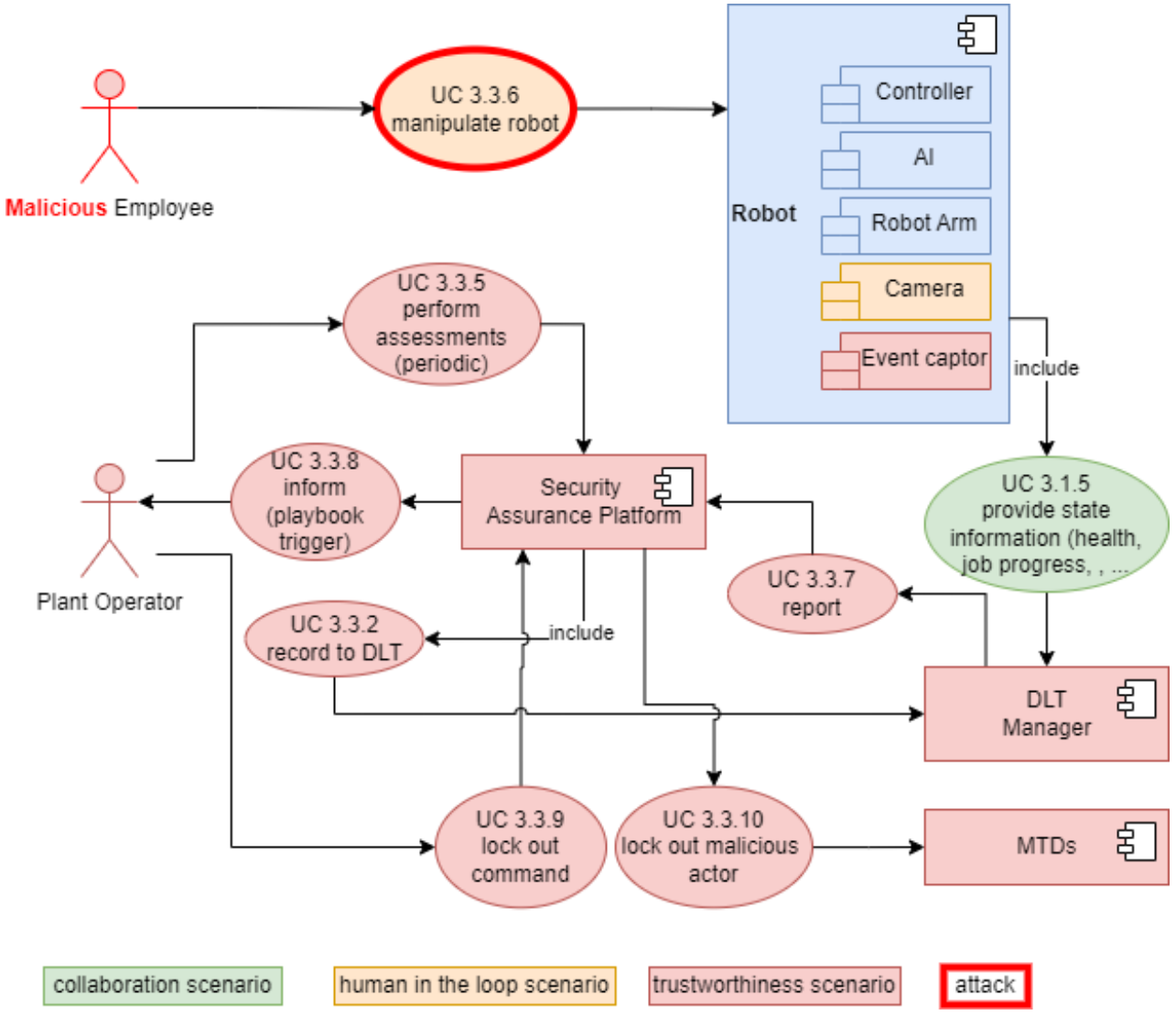


Figure 22: Use case diagram trustworthiness - assessment, attack- attack detection & mitigation (key scenes 3.3 & 3.4)

3 SECOND OPEN CALL DEFINITION

While the purpose of the 1st Open Call was to primarily enhance the IntellIoT framework and/or the three use cases, the purpose of the 2nd Open Call is to further evaluate the final version of IntellIoT framework, as well as to contribute to building a sustainable ecosystem in the existing or new application domains that carries on beyond the project. Hence, in comparison with the 1st Open Call, the contributions to the 2nd Open Call should emphasize their potential for longevity beyond the project lifetime.
As within the 1st Open Call, the details on expectations towards applicants will be specified in a dedicated "Guide for Applicants"[48] Below, initial expectations and contribution ideas for the 2nd Open Call are described.

3.1 Expectations for participating entities

Entities taking part in the 2nd Open Call are expected to:

- clearly integrate with the IntellIoT framework (e.g., through the HyperMAS, or the computation & communication infrastructure),
- develop and provide scalable and future proof technologies / solutions, e.g., software or hardware, based on existing solutions of the applicant,
- keep deployed components alive at least until the final project review,
- provide access to collected data for the consortium of IntellIoT,
- demonstrate and present the final outcomes (and plans on their exploitations),
- provide feedback to the IntellIoT team,
- outline arguments for potential longevity of the developed components beyond the project lifetime.

3.2 Contribution Ideas

The below mentioned list of ideas shall give Open Call applicants an understanding of what could be contributed through their Open Call applications. The described ideas do not preclude submission of alternative suggestions. In fact, new ideas from interested entities to join the Open Call are encouraged and welcome.

3.2.1 IDEAS FOR NEW USE CASES / DOMAINS

In the 2nd Open Call, we also encourage the development and deployment of the IntellIoT framework in new use cases, even within domains other than the ones covered in the three IntellIoT use cases. For example:

- **Transportation:** A proposal could target to utilize (parts of) the IntellIoT framework for realizing IoT applications in the transportation domain. E.g., to implement communication/computation infrastructures for vehicles.
- **Logistics:** E.g., to use (parts of) the IntellIoT framework for management of fleets of autonomously guided vehicles.
- **Utilities:** E.g., to use (parts of) the IntellIoT framework for managing electrical grid usage.
- **Smart Buildings:** E.g., to use (parts of) the IntellIoT framework for the control and management of a building's actuators (e.g., control of HVAC or lighting) based on sensory input (e.g., detection of humans). Novel communication (e.g., 5G NR or NB-IoT) and computation (e.g., edge servers) could be integrated. This could also involve the "human-in-the-loop" concept by allowing the building users to override control decisions by the AI.

[48] https://intelliot.eu/open-calls

3.2.2 IDEAS FOR ALL USE CASES

Besides contributions for a specific use case, we welcome contributions that are more general and can be applied in all use cases. Examples:

- **Digital Twin tooling:** Software that allows to create a digital copy of a physical object to enable simulations, advanced designing, and planning. Such a digital twin could make sense for example for the tractor in use case 1 or the robot arm in use case 3.
- **Blockchain-based marketplace:** Software that implements a user interface and underlying marketplace exchange to support service business based on IntellIoT's blockchain components (e.g., 3rd party agriculture or manufacturing machinery vendors).

3.2.3 IDEAS FOR AGRICULTURE USE CASE

- **Drones:** Hardware (e.g., drone devices) and software for unmanned aerial vehicles (UAV) that are integrated by the Open Call participant into the IntellIoT framework (e.g., through HyperMAS adaptors). Drones could then be used in collaboration with the tractor to support for example in the circumvention of obstacles, by providing imagery data around the tractor and of the obstacle. A challenge will then be the implementation of coordinating the drone's flight with the driving path of the tractor, or even other drones.
- **Smart farming:** Contributions from an external partner could integrate equipment, devices and services (e.g., measuring soil humidity through beacons and small scale meteobot etc.) to an agricultural field and interconnect it with our infrastructure.

3.2.4 IDEAS FOR HEALTHCARE USE CASE

- **Data:** Access to data (e.g., historical and anonymized medical data or live data from sensors). Generated or simulated data that is representative of patient populations and diagnoses or exemplifies device data, as well as anonymous data that can be reused according to GDPR regulations.
- **Analytics:** Software (e.g., machine learning models) that can be utilized to analyse the medical data.

3.2.5 IDEAS FOR MANUFACTURING USE CASE

- **Edge applications:** Development of additional / novel manufacturing applications that are executed on the IntellIoT edge infrastructure (e.g., painting, welding) or more complex manufacturing management tasks, such as predictive maintenance for machinery.
- **Process industry machinery:** Hardware and software to adapt the IntellIoT framework in a scenario from process industries (e.g., textile or food & beverages), which can meaningfully employ the developed technologies, e.g., to achieve modular designs and thereby contribute to a circular economy.
- **Additive manufacturing machinery:** Hardware (e.g., 3D printers) and software to integrate with the IntellIoT framework and contribute with advanced machinery to the manufacturing use case, e.g., by integration with robots.
- **New sensor technologies:** Hardware (e.g., radar or LIDAR) and software to integrate with IntellIoT framework and to support the manufacturing use case, for example to improve the robot arm interaction with the machinery.

4 CONCLUSIONS

The IntellIoT project has chosen a use-case based approach for the validation of the developed framework and its underlying technologies. This deliverable describes the final design of the three use cases, that are defined for the demonstration of the results of IntellIoT. The use cases target the three heterogeneous domains of agriculture, healthcare and manufacturing, focusing on the topics of distributed intelligent machines, tactile human machine interaction and safety and security, while considering the intricacies of each of these domains. The definition of the use cases highlights the scope of the individual use case within the specific domain, describing what will be demonstrated and what the realistic problem definition and the market situation for the respective domain is. Additionally, this document highlights the different technologies (e.g., tractors, robots, mobile devices, etc.) that are targeted inside the use cases and that will be extended to become intelligent devices in the context of the overall IntellIoT framework.

Furthermore, the above efforts also highlighted the three pillars of the IntellIoT project, namely (1) collaborative IoT, (2) human-in-the-loop, and (3) trustworthiness. These pillars cover the main research topics of the project and will be applied in the three uses cases. To cover these pillars inside the use cases, a scenario-based approach has been introduced in the use cases. Each scenario in its use case will cover one of the pillars and will demonstrate a certain functionality presenting the targeted pillar.

As this deliverable is the final deliverable of Task 2.1, it reflects the final results of the work performed in this task, updating the previous version (D2.1), and integrating feedback from the first cycle of IntellIoT's development, integration, demonstration & validation activities. This includes the feedback from WP3, WP4 and WP5, where the technologies have been developed and first integration and demonstration efforts have taken place, as all these WPs and associated tasks have provided feedback to the work in Task 2.1, thus kicking off Cycle 2 of the project. Additionally, the results from the first Open Call are also mentioned in this deliverable, integrating the contributions from the Open Call winners. Similar to deliverable D2.1, D2.4 will form the basis for the second and final cycle of the IntellIoT project and will be the document describing the use cases and providing the foundations for what still needs to be developed and integrated to demonstrate the final results of the IntellIoT project.