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

IntellioT

Deliverable D2.1
Use case specification & Open Call definition (first version)

Deliverable release date	31/03/2021
Authors	1. SIEMENS: Andreas Zirkler, Andreas Ziller, Arne Broering 2. EURECOM: Jérôme Härri 3. AAU: Beatriz Soret, Lam Nguyen 4. UOULU: Sumudu Samarakoon 5. TTC: Martijn Rooker 6. TSI: Andreas Brokalakis, Vassilis Amourgianos, Babis Savvakos 7. PHILIPS: Anca Bucur 8. SANL: Konstantinos Fysarakis, Ioannis Vezakis 9. HSG: Simon Mayer 10. HOLO: Carina Pamminger, Nour Fendri 11. AVL: Holger Burkhardt 12. PAGNI: Maria Marketou
Editor	Martijn Rooker (TTC)
Reviewer	Dominik Krabbe (STARTUPC), Holger Burkhardt (AVL)
Approved by	PTC Members: (Vivek Kulkarni, Konstantinos Fysarakis, Sumudu Samarakoon, Beatriz Soret, Arne Bröring, Dominik Krabbe) PCC Members: (Vivek Kulkarni, Jérôme Härri, Beatriz Soret, Mehdi Bennis, Martijn Rooker, Sotiris Ioannidis, Anca Bucur, Georgios Spanoudakis, Simon Mayer, Filippo Leddi, Harshitha Chandregowda, Maren Lesche, Fragkiskos Parthenakis)
Status of the Document	Final
Version	1.0
Dissemination level	Public

Table of Contents

ACRONYMS AND DEFINITIONS

Acronym	Definition
5G NR	5th Generation New Radio
AGV	Automated Guided Vehicle
AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
BDI	Belief-Desire-Intention
CAD	Computer Aided Design
CAM	Computer Aided Manufacturing
CAN	Controller Area Network
CNC	Computerized Numerical Control
COVID-19	Corona Virus Disease of 2019
D2D	Device to Device
DLT	Distributed Ledger Technology
ECG	Electrocardiogram
EMS	Edge Management System
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HMI	Human Machine Interface
HyperMAS	Hypermedia Multi-agent System
IAKM	Infrastructure Assisted Knowledge Management
ID	Identification
IDS	Intrusion Detection System
IO	Input Output
IoT	Internet of Things
IPFS	Inter Planetary File System
IPSec	Internet Protocol Security
IT/OT	Information Technology/Operation Technology
JSON	JavaScript Object Notation

MES	Manufacturing Execution System
MTD	Moving Target Defences
NGIoT	Next Generation Internet of Things
OEM	Original Equipment Manufacturer
PLC	Programmable Logic Controller
PROFInet	Process Field Network
QoS	Quality of Service
TLS	Transport Layer Security
TSN	Time Sensitive Networking
UC	Use Case
UE	User Equipment
UML	Unified Modeling Language
URLL	Ultra-Reliable and Low Latency
VDMA	Verband Deutscher Maschinen- und Anlagenbau
VPN	Virtual Private Network
VR	Virtual Reality
W3C WoT TD	World Wide Web Consortium Web of Things Things Description
WiFi	Wireless Fidelity
WP	Work Package
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie

EXECUTIVE SUMMARY

This deliverable summarizes the work that has been done in the first cycle of Task 2.1, related to the use case definitions and the first open call definition of IntellIoT. As such, this deliverable presents the first results of Task 2.1. A final, updated version of this deliverable is due in Month 19 of the project and will include the final definition of the use cases and the definition of the second open call.

This deliverable summarizes the work that has been done in the first cycle of Task 2.1, related to the use case definitions and the first open call definition of IntellIoT. As such, the deliverable presents the first results of Task 2.1, organized in two parts: the first part defines the three project use cases (agriculture, healthcare, manufacturing) in detail, including scope, potential end users, components, and scenarios, covering the three key IntellIoT concepts, namely Collaborative IoT, Human-in-the-loop and Trustworthiness; the second part aims to define the first IntellIoT Open Call, allowing third parties to contribute and enhance the project's use cases. A second, and final, updated version of this deliverable is due in Month 19 of the project and will include the final definition of the use cases and the definition of the second open call.

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 issues that need to be considered during the development of the IntellIoT architecture and infrastructure and provide an effective foundation for evaluating and demonstrating IntellIoT's outcomes.

The definition of the use cases will form the basis for most of the developments, demonstrations and evaluation activities taking place within the project. The use cases will provide a high-level story about what and how the functionalities will be demonstrated in the three different selected domains.

Section 2 provides the descriptions of the three different use cases. The description of the use cases starts with highlighting the scope and objectives of the individual use cases, 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 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 agricultural use case, robots for the manufacturing use case and health devices for the healthcare use case) and entities that are core IntellIoT framework entities/components that will be deployed in multiple use cases, demonstrating the cross-domain applicability of the IntellIoT solution. 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.

Moreover, the IntellIoT vision involves two open calls that will be used to validate the applicability of the results of the project in real-world scenarios, as well as allow to create solutions developed on the IntellIoT framework and to create an ecosystem around the technology for exploitation beyond the project lifetime. While the purpose of the 1st open call is primarily to enhance the project's technological and use case coverage towards the 2nd cycle, the purpose of the 2nd open call is the building of an ecosystem that carries on beyond the project. In this context, section 3 will provide the definition of the 1st open call based on the definition of the use cases.

Finally, section 4 concludes this deliverable and presents the future work for the use case definition, open call definitions and the work towards the second (and final) version of this deliverable, that will follow at Month 19 of the project.

1.1 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 smart 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 will mainly focus 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.

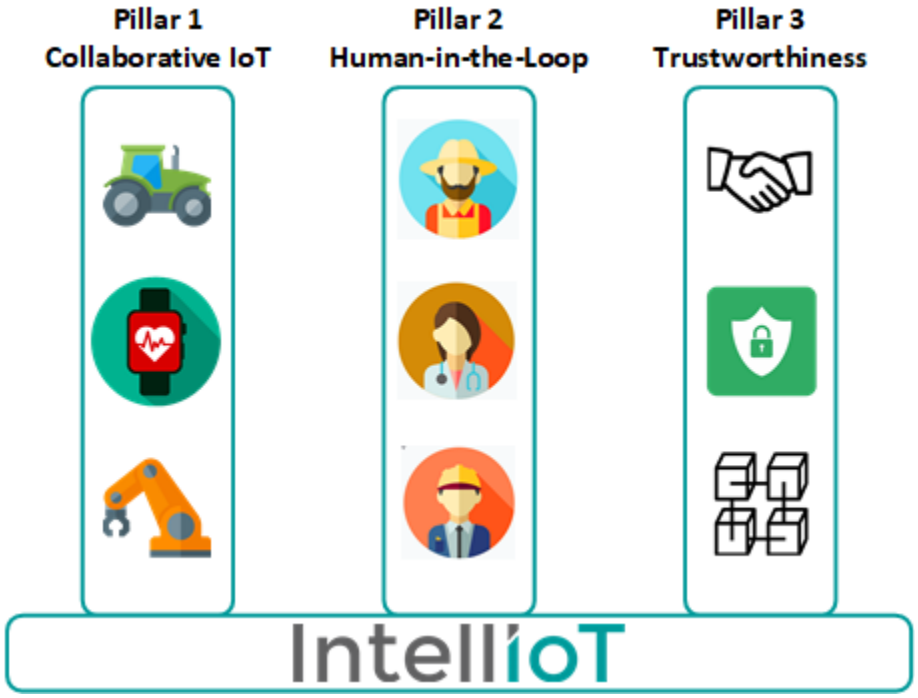


Figure 1: Three pillars of IntellIoT

1) **Collaborative IoT:** Various semi-autonomous entities (e.g., tractors, robots, healthcare devices, etc.) will need to cooperate in order to execute multiple IoT applications. These entities will have to be self-aware and will 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 will 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 to not 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, humans 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 primitives 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, it has been decided that the pillar Trustworthiness is more of an overlapping pillar over the other two pillars and will be covering the technologies developed and applied in scenarios covering pillars 1 and 2. Figure 2 depicts this approach where pillar 3 is overlapping the other two pillars.

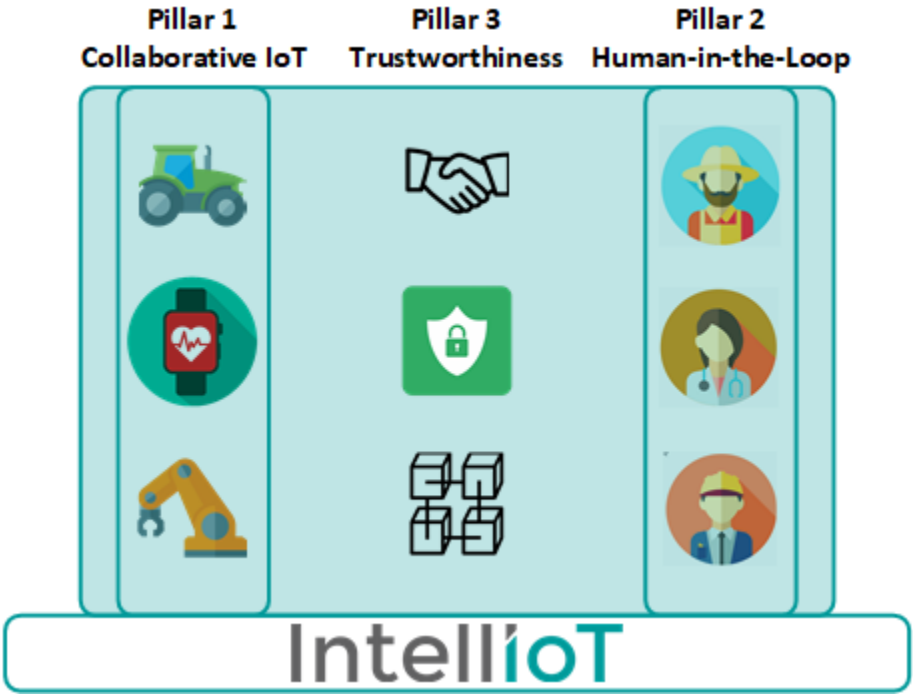


Figure 2: Three pillars of IntellIoT and associated scenarios (Trustworthiness overlapping other two)

2 USE CASE DESCRIPTIONS

This section will go into deeper details on the three different use cases that have been identified within the IntellIoT project.

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. 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 days, resulting in fatigue and finally in (potential deadly) accidents[1]. The 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.

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 entities (e.g., vehicles, drones, sensors) 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 future aim 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 (e.g., drones, sensors, other tractors), 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.

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

2.1.2 DESCRIPTION OF THE USE CASE

As mentioned above, the agriculture use case will investigate different technologies for future autonomous farming activities. The consortium has identified different technologies (e.g., machine learning, 5G communication, security, human-machine interaction) that will be further developed and applied to the identified scenarios for the agriculture use case (see Section 3.1.5).

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

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 a drone or an infrastructure edge. Tasks that cannot be performed on the vehicle will be offloaded to an available cloud infrastructure.

The tractor is programmed with a mission by the human operator by having the operator specify a goal through the Hypermedia Multi-agent System (HyperMAS). The system then plans how this goal can be achieved and instructs the tractor by assigning tasks to it. 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). Additionally, it could be possible that new/updated functionalities (e.g., object recognition, navigation, hazard detection) are uploaded to the tractor before it starts performing its assigned tasks. These functionalities can be made available to an infrastructure by technology providers (e.g., tractor OEMs, system integrators) from where vehicle owners can deploy these functionalities to the specific vehicles. While the vehicle is driving over the field, it observes the environment and uses the gathered information to update its internal knowledge of the environment. Other entities (e.g., other vehicles, drones, sensors, etc.) can also be present in the field and a network is created between these entities to exchange information and update the internal knowledge of the entities. The connected entities will use the information to collectively train their own models (i.e., local AI) and identify unknown obstacles in a faster and more robust manner. In the particular case of drones, which can be used in the use case to increase the field of view of tractors, there is currently no partner in the consortium with real drones, so the interaction and information exchange will be performed using a simulated drone.

In the situation where an unknown obstacle is detected and the vehicle does not know how to traverse it, it will first try to collect complementary information or knowledge from the 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. If the provided feed does not provide enough information to allow finding a solution, the human operator can also access other entities in the field (other tractors, drones) to view the situation from different angles. The human operator will execute direct or indirect strategies. In the direct control, the human operator can directly interact with the vehicle (i.e., moving the vehicle forwards or backwards) using VR controllers. This will require a reliable, high-speed and low-latency connection that enables real-time interaction between operator and the vehicle. When using indirect control, a feasible trajectory around the obstacle has to be defined. Once this action is completed, the control needs to be given back to the vehicle. In this case, the human operator supervises the vehicle through the video feed to ensure that the newly defined trajectory is executed correctly. The indirect strategy has more relaxed latency and timing requirements for the communication. Based on the information coming from the human operator (be it either direct or indirect control), the vehicle will refine its own local AI models by continuously learning how to overcome such obstacles in the future, in addition to sharing the learned information (in an AI model) with other vehicles. The latter will be achieved by announcing the availability of the updated AI model tailored to the specific environment (using adapted semantics) via the IAKM. To this end, the IAKM will provide publish/subscribe mechanisms to exchange knowledge (in the form of AI models) or to seek environments required to learn or apply knowledge. Structured semantics will be used to describe various parameters related either to the model, to the environment, or to validity and applicability of the shared knowledge.

Distributed Ledger Technologies (DLTs) will further ensure that the data and information 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., a drone that has been infiltrated by an attacker) tries to harm that mission, the security assurance mechanisms should be activated. The vehicle or its peers must identify the malicious entity and notify the cloud infrastructure. The infrastructure will then take 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.

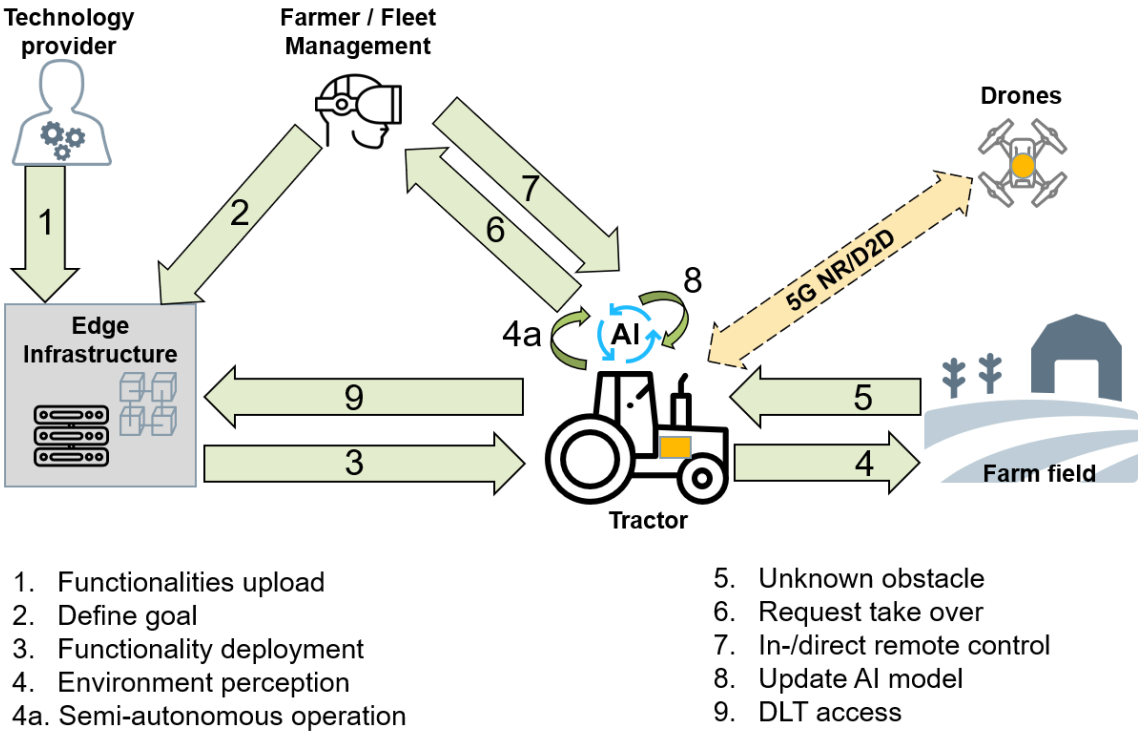


Figure 3: Agriculture use case

2.1.3 COMPONENTS / ACTORS OF THE USE CASE

The following components will be investigated and further developed within the scope of the agriculture use case.

2.1.3.1 TRACTOR (AVL)

AVL provides a fully electric vehicle that is the platform for the implementation of semi-autonomous functions. It contains sensors and cameras for the perception of the surrounding area. This data will be shared with all the devices of the IoT-Infrastructure. The tractor has two electric driven axles - each of them with a maximum power of 25 kW. The steering angle of the front and the rear axle can be controlled separately. The tractor has interfaces to provide hydraulic and electric power to implements and additional devices.

Figure 4: AVL E-Tractor platform

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 tractor and to control the driving functions.

signals sent by the tractor*	**Signal received by the tractor**
Actual vehicle speed	Set point vehicle speed
Actual curvature	Set point for curvature
Actual e-motor data (speed, torque, ...)	Steering method (front axle, rear axle, both)
Actual steering angle	E-motor limitations (speed, torque)
	Emergency off (emergency brake)

*actual signals, additional signals can be added during development phase.

At the moment, this interface is used by a remote control that allows the operator to manoeuvre the tractor. In the next step, a superordinated controller which is calculating the trajectory will use this interface to control the vehicle. Therefore, the vehicle is receiving signals waypoints and tasks from a mission planning tool sent using a 5G connection. An additional autonomous function controller is processing this request and evaluates the path by using GPS-data, data from the IoT-Infrastructure and information of the surrounding area.

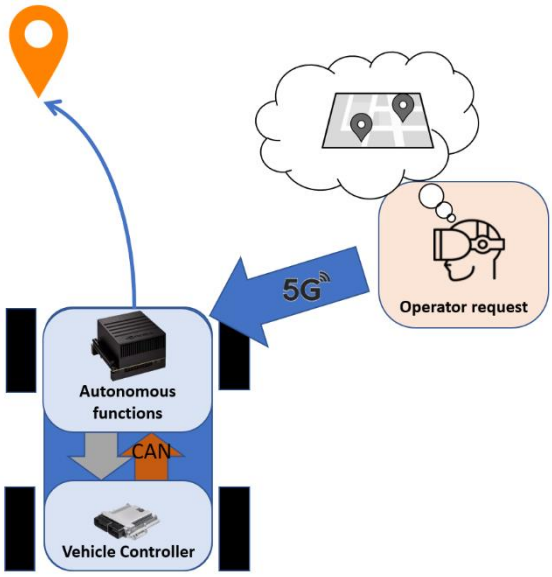


Figure 5: Controlling the tractor via 5G

The autonomous controller allows other members of the IoT-Infrastructure to take over the control of the tractor and operate it remotely. Especially in unexpected situations, when the internal intelligence is not able to find a suitable and safe action (e.g., tractor is blocked by an obstacle), the operator can resolve the situation. Therefore, the operator is connected with the device and is receiving image data from the surrounding area via VR-Glasses.

Perception:

Mounted on the tractor is a sensor box, that is equipped with several cameras. Four wide angle 4K-cameras are aligned on each side to capture the surrounding area with 120deg each. The images of these cameras are processed and stitched together by the controller to achieve a 360deg panoramic view. A stereoscopic camera is used for the perception of structures and objects and for the evaluation of their distances.

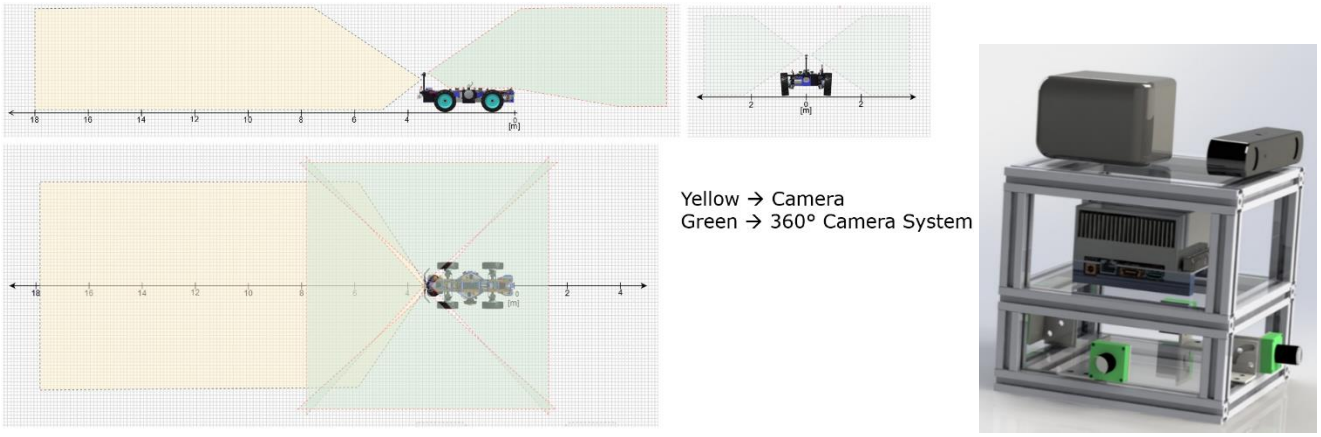


Figure 6: Camera system for the tractor

The processed data from the vehicle will be provided via ethernet connection to the 5G-interface. This interface is connected via 5G to the IoT-Infrastructure and allows other devices to use the information.

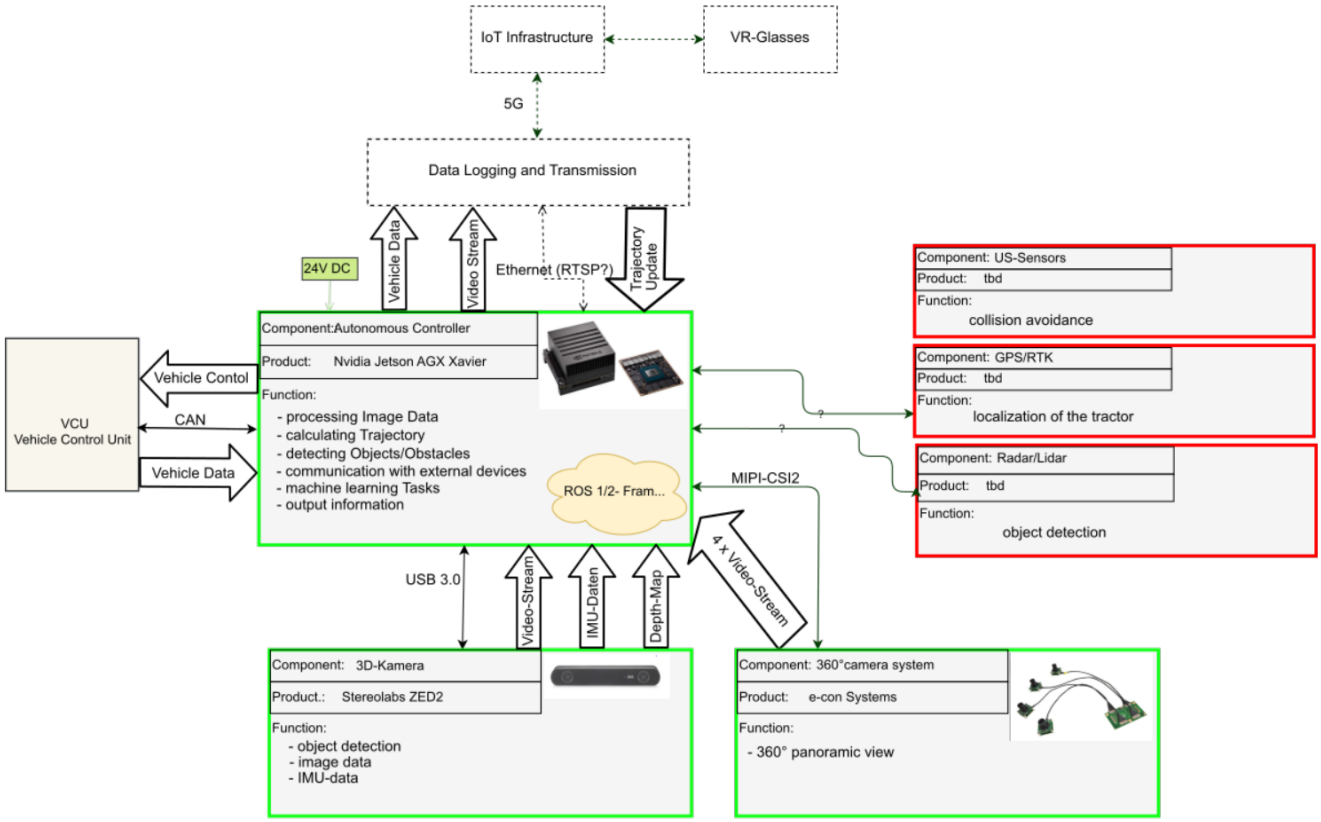


Figure 7: Signal Flow Tractor Control

Furthermore, the vehicle will be equipped with additional processing solutions allowing it to perform edge-based computing on the vehicle. The processing solution will be able to host different applications, including AI, safety based and standard controlling processes for the vehicle and make sure that the safety specific applications will not interfere with non-safety applications. Finally, communication capabilities (e.g., 5G, WiFi) will be deployed to the tractor, enabling the tractor to exchange data with the IoT-Infrastructure, other entities in the field (e.g., drones, other vehicles in the field or the human operator) and use this data exchange for updating its knowledge of the field and better perform the task at hand.

2.1.3.2 DRONE

The drones serve two purposes:

i) Act as a sensor network on the air: The tractors' visibility is limited to the ground level and is prone to be obscured by various types of obstacles. Hence, drones can assist tractors by providing real-time data in terms of visuals from the bird's-eye point of view.

ii) Providing connectivity among tractors and the infrastructure: Benefitting the line-of-sight connectivity between both ground (tractors, infrastructure) and air (drones) nodes, an overlaid drone network can act as a secondary relaying network connecting tractors with the infrastructure

The flexibility of deployment, control, and operation in large numbers under moderately low energy consumption is the key motivation behind adopting a drone network to serve aforementioned purposes. Within the scope of IntellIoT, the drone network is deployed in a simulated environment adopting air-to-air[2] and air-to-ground[3] communication models from the existing literature.

2.1.3.3 HUMAN OPERATOR

A human operator is a person that can either directly or indirectly take over control of the tractor in case a situation occurs where human intervention is necessary. The human operator has to be skilled enough and requires access credentials. Once these are provided, the human operator will gain situational awareness through a video feed sent to a VR headset. The VR headset's controllers will allow direct interaction with the tractor.

2.1.3.4 MALICIOUS OPERATOR

A malicious operator is an adversary that tries to hamper normal system operation. For example, the malicious operator could gain access to the tractor and seize its operation to damage the tractor itself or the crops or drive it outside of the desired area.

2.1.3.5 IOT INFRASTRUCTURE

The communications and computation infrastructure is responsible of allocating communication and computation 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. In the communications part, the link must support reliable data transmission and low latency between the human operator and the machines.

The functional integration between the components will be based on 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) artefacts, 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 inheriting its desirable architectural properties (e.g., scalability and evolvability). To jointly plan and execute behaviours in this use case, our software agents will require access to shared knowledge via an Infrastructure Assisted Knowledge Management (IAKM) entity.

2.1.3.6 TRUST COMPONENTS

2.1.3.6.1 SECURITY ASSURANCE PLATFORM

The Assurance Platform will provide runtime, continuous assessment and certification of the monitored agriculture UC deployment. In general, this enabler will form the core of the assurance and certification capabilities of IntellIoT.

---

[2] N. Goddemeier and C. Wietfeld, "Investigation of air-to-air channel characteristics and a UAV specific extension to the rice model," in Proc. IEEE Globecom Workshops (GC Wkshps), San Diego, CA, USA, Dec. 2015, pp. 1–5.

[3] 3GPP TR 36.777, Study on enhanced LTE support for aerial vehicles (Release 15), 3GPP, Dec. 2017.

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 agriculture deployment, while also responding to changes in said posture, as detected by the integration with the needed event captors and the trust-based IDS enabler. The timely and efficient response will be achieved by triggering changes in the MTDs deployed in the UC environment. Throughout its operation, the Assurance Platform will also interface with the DLT building blocks, allowing the evidence-based operation of the assurance scheme.

2.1.3.6.2 TRUST-BASED INTRUSION DETECTION SYSTEM (IDS)

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. The Intrusion Detection System (IDS) is used to build trust between nodes and isolate those that are less trustworthy.

In the agriculture scenario, if a malicious operator takes over control of a drone and starts working against the legitimate scenario, it would gradually lose its reputation. Thus, the rest of the nodes will stop using it and the Assurance Platform will be informed to take further actions.

2.1.3.6.3 MOVING TARGET DEFENCES (MTDS)

Moving Target Defence (MTD) is a technology that changes the network configuration 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, her benefit will be low due to the limited lifetime of that configuration and the diversity of the system.

In the agriculture scenario, when the IDS detect the malicious node, MTD is called upon to change the network configuration in order to isolate the attacker and sustain normal system operation.

2.1.3.6.4 DISTRIBUTED LEDGER TECHNOLOGIES (DLTS)

A Blockchain system offers a tamper-proof ledger distributed on a collection of communicating nodes, all sharing the same initial block of information, the genesis block. In order to add information to the Blockchain, a node includes information in a block with a pointer to its parent block, this creates a chain of blocks, hence called Blockchain. 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 Blockchain network. 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. DLTs promise a reliable source of truth about the state of farm workspaces, inventories and contracts towards smart agriculture, where the collection of such data is often significantly expensive. The DLTs can track the provenance of goods and thus help create trustworthy supply chains and build trust between producers and consumers.

2.1.4 TARGET MARKETS / END USERS

The solutions that are developed, integrated and validated within the agriculture use case can be applied in many other domains, like the general off-highway domain for mobile machinery. (Semi-) autonomous vehicles are entering more and more fields, like construction areas, municipal, forestry, etc. The goal is to remove the human from the cabin and bring more and more autonomy into the vehicles, but nevertheless keep the human in the loop. The agriculture use case, will primarily target the farming domain, thus focusing on farming vehicle OEMs or companies developing technologies for these OEMs. Nevertheless, new companies or business concepts can also appear based on these

solutions, like companies renting out this kind of machinery and performing the remote control. These so-called Farming-as-a-Service (FAAS) solutions could create completely new markets.

Additionally, we will look at the user groups that will use or deploy these future vehicles. In the agriculture domain, these will mainly be the farmers that will be the target end users of this use case. They have the most experience with this machinery and can provide the best feedback about these solutions.

In addition to the field of agriculture, the AI developed within the scope of IntellIoT has several other potential end users. The distributed AI solutions on autonomous navigation can be adopted for the navigation in factories, storage yards, distribution lines (posts, packages) and construction sites with relevant minor modifications. Apart from autonomous navigation, the distributed AI for object recognition developed under on-device as well as communication constraints can be adopted for other object recognition applications using memory and energy limited devices (rescue robots, explore/expedition devices). These solutions can be of interest for technology providers or system integrators.

Finally, we will look into organizations and governmental entities, which can have a major influence on the success of new technologies on the market. The earlier we include them into the discussions, the earlier we can use their input in developments and potentially prepare the market for these future solutions.

Summarizing, the following potential end users for the IntellIoT agriculture use case are identified:

- OEMs for agricultural vehicles and mobile machinery.
    - Technology providers developing new technologies for the agricultural domain, that can be integrated into farming solutions. These are suppliers to the OEMs, therefore they are marked as a subgroup of the OEMs.
- Farmers, where the final system/technologies will be deployed and who will be using these systems.
- System integrators, that will integrate the overall system at the farms/fields.
- Companies that are lending out agricultural vehicles (Farming-as-a-service) and are also performing the remote control of the vehicles
- Farmer associations that will advise farmers about new technologies available on the market. Although associations are not direct end users of the technologies, they can still have major influence by reaching out to other end users and support bringing technologies on the market.
- Governmental entities that advise farmers on solutions. These entities can make or break a solution and therefore have to be included in discussions as soon as possible to inform them about new technologies being developed for these domains.

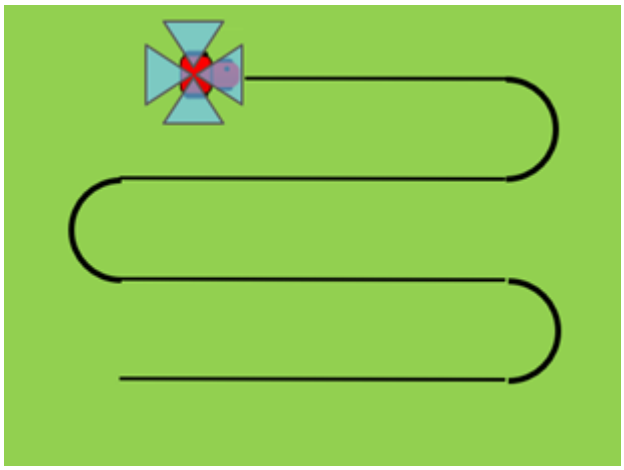
2.1.5 SCENARIOS

2.1.5.1 SCENARIO 1.1 – COLLABORATIVE IOT

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

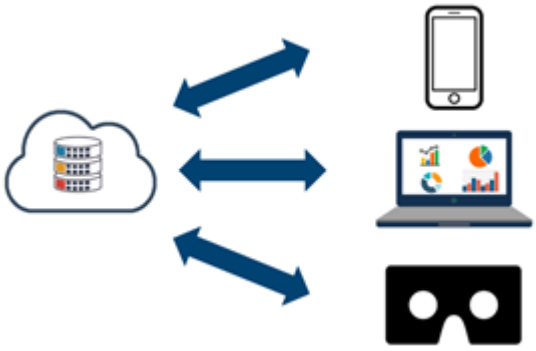
Description	This scenario deals with the standard behaviour of the tractor. The human operator will plan a mission for the tractor, which could be the ploughing or spraying of a field. The mission consists of an assigned field, where the trajectory planner calculates waypoints that the tractor needs to follow. These waypoints are assigned to the tractor by the IoT-Infrastructure. The tractor platform is equipped with sensors to recognize the tractor environment and an AI-driven controller unit to operate the tractor. The sensor input is pre-processed and when an object is detected, the distance to this object is calculated. All these data and additional tractor data (e.g., speed, GPS position, operation status, etc.) are fed into the controller to infer the control commands as well as to actively update its AI. Towards improving the success of the mission completion, the tractor utilizes an overlaid drone network and the IoT-Infrastructure for two purposes: i) to extend its field-of-view via external sensors on the field and ii) to collaboratively update its AI with other tractors in the same or different fields. Occasionally, the collected data is transmitted via 5G to a cloud service to provide task status updates to the operator. In addition, 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 human operator plans a mission and securely transmits the data to the IoT-Infrastructure. The operator defines the task, the process, the time and the area.  **Key Scene 1.2**: The IoT-Infrastructure detects available resources and allocates them to the tasks in an efficient way, calculates the best path and sends the tractors to the defined positions.

Key Scene 1.3: The tractor moves to the given waypoints and performs the requested tasks. Here, the tractor automatically navigates and carries out the assigned task (plough, cultivator, planter, sprayer, etc.).

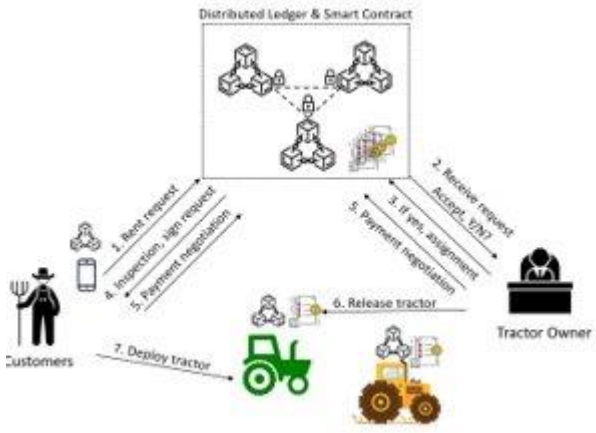


Key Scene 1.4: When the controller fails to make a reliable decision, the tractors refer to the IAKM for the supported AI technologies on the IoT-Infrastructure having access to all cooperative devices. Depending on the requirement, the tractor and IoT-Infrastructure securely shares either raw/processed data (e.g., vehicle data, GPS position, video data (3D), detected objects) or updated AI models.
If the problem persists, the tractor stops and sends a message to the operator (see scenario 1.2).

Key Scene 1.5: IoT-Infrastructure transmits important data to the operator in a trustworthy manner. All members (drones, tractors, etc.) can obtain signals from the other devices (drones, tractors, etc.).



Key Scene 1.6: The tractor fleet has at least one tractor from a third-party service provider. 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. The vehicles need direct interaction with each other in real-time communicating their current position and status.
Purpose	The purpose of this specific scenario is to establish AI driven tractors and 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, IoT-Infrastructure, Human operator, Drones
Information exchange between actors	[1] Human → IoT-Infrastructure: definition of the task [2] IoT-Infrastructure → Tractor: definition of the path, updated AI Model [3] Tractor → IoT-Infrastructure: Status information about the tractor. This information can include telemetry, sensor information, process information, etc. [4] Tractor → IoT-Infrastructure: requests for additional information, like e.g., map data including unidentified obstacles, ML object/AI models. [5] Tractor ↔ Drones: sensor data, updated AI models
Challenges for scenario validation (T5.3)	[1] Reliability of the environment perception with the 360-degree 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

Figure 8 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 D2.2.

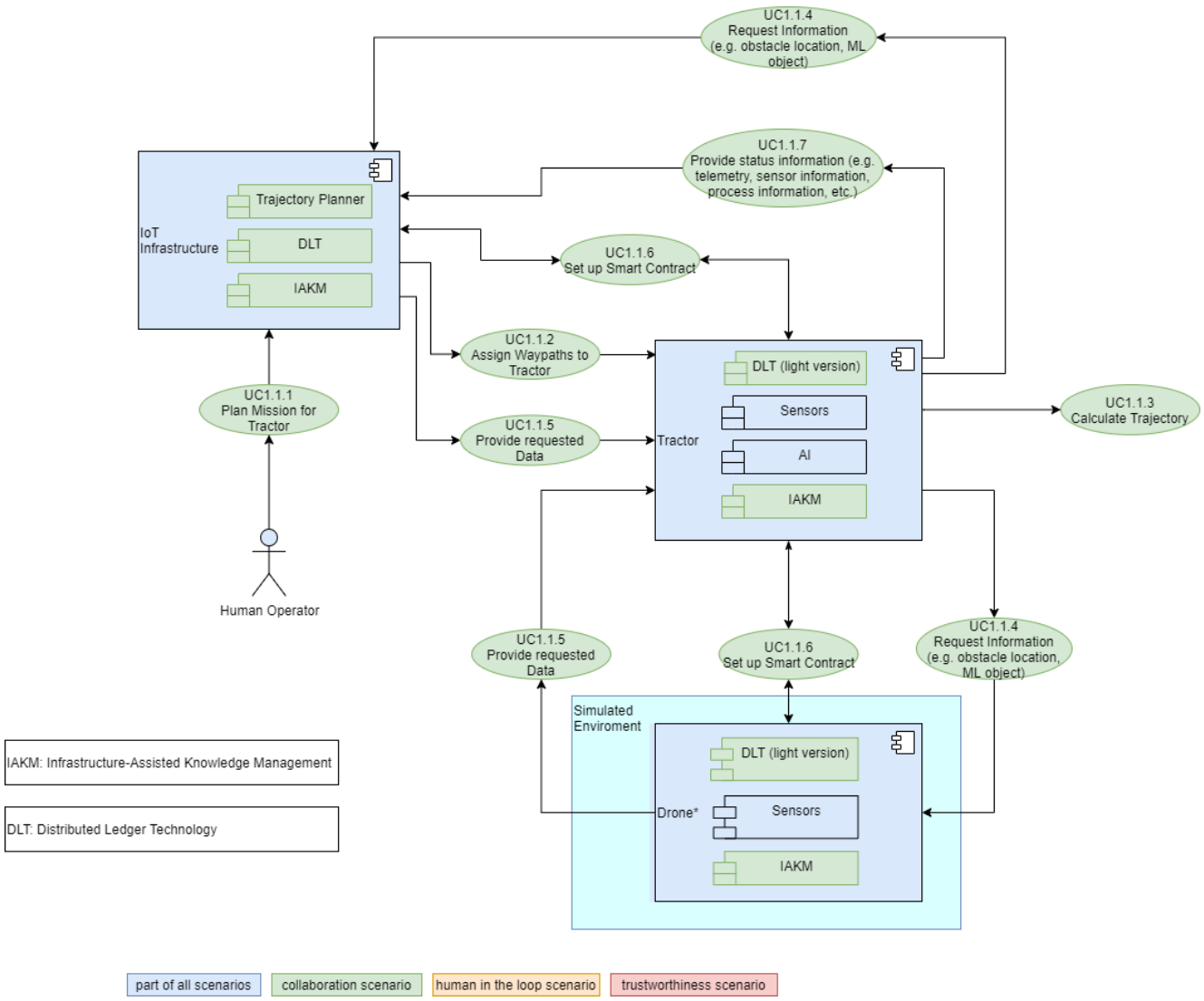
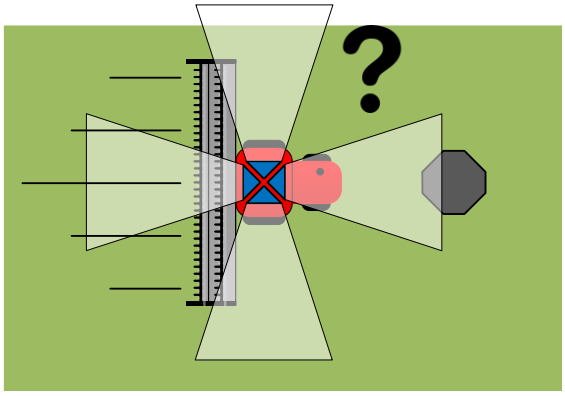
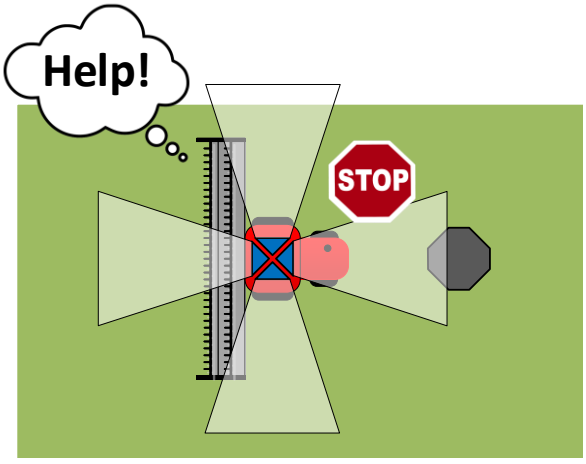


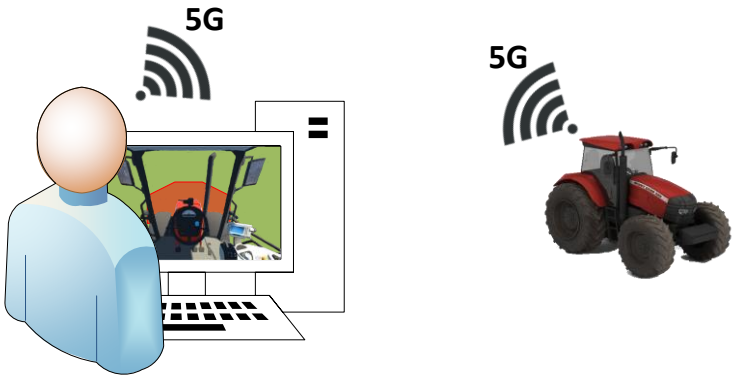
Figure 8: UC1 – Collaborative IoT Scenario

2.1.5.2 SCENARIO 1.2 – HUMAN-IN-THE-LOOP

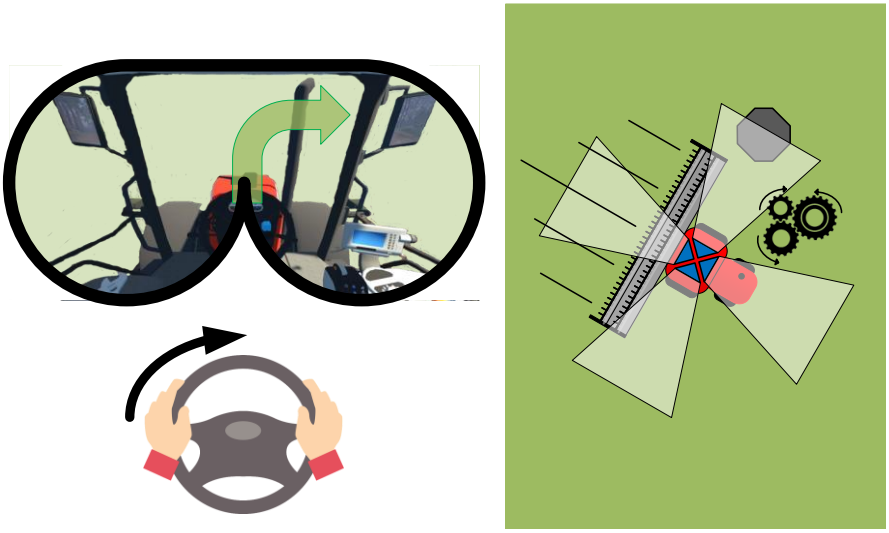
Scenario Name	Human-in-the-Loop
Scenario ID	UC1-Scenario2
Partners	TTC, AVL, EURECOM, HOLO, HSG, SANL, AAU, TSI, UOULU
Description	The semi-autonomous tractor encounters a situation (e.g., an obstacle) that it does not know how to handle (e.g., it does not recognize the obstacle or does not know how 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 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 either directly control the tractor

	or plan a trajectory around the obstacle to overcome the unknown situation. The tractor uses the information from the operator to update its image of the world and learns new behaviour on how to overcome a comparable situation in the future. After the situation has been solved, control is given back to the tractor and the human operator closes the connection.
Key Scene	**Key Scene 2.1**: Tractor is stuck in an unidentified situation (e.g., an obstacle that was not present on any map or incomplete map data) and the tractor doesn't know how to move around the obstacle. Interaction with other entities in the field (e.g., tractors, drones, or sensors) does not provide sufficient additional information, so the vehicle is stuck in the current position.  **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 position XY 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 (visual) data coming from the tractor. The data from the tractor can either be extracted from the IoT-Infrastructure (e.g., progress, trajectory, position) or is direct real-time information coming from the sensors on the tractor. If these sensors don't provide enough information, potentially other

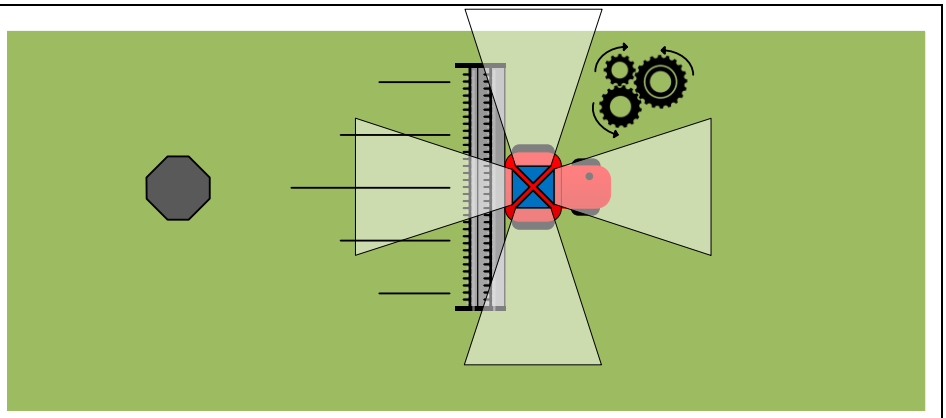
entities in the field can be contacted to provide additional information about the situation of the tractor.



Key Scene 2.4: The human operator uses VR to aid the tractor through the unidentified situation and the tractor learns from the interaction. The operator identifies the problem using the information available (i.e., data from different sensors, entities or even meta-data from the machine) 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 either plan a trajectory for the tractor and set new waypoints for the tractor or will even take direct control of the tractor and will remotely drive the tractor around the obstacle. The tractor will record the activities from the operator and will update its AI via learning processes. Using this information, the tractor will be able to traverse similar situations in the future and assist other tractors in similar situations (see scenario "Collaborative IoT")



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.

	
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 (either direct or indirect) how to handle such a situation and the tractor will learn from it.
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 (I.e., the data provided by the sensors must be in real-time). 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, human operator and potentially other entities in the field (e.g., sensors, tractors drones) providing data to the human operator.
Information exchange between actors	[1] Tractor → Human operator: Request message for take over. 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, trajectory, or an updated AI model. Either the human operator drives the tractor directly (via remote control) or within an augmented environment to update the AI model. Otherwise, the operator creates a path around the obstacle, and this is then sent to the vehicle. [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 [3] Reliable and secure human-machine interaction [4] Precise translation of VR movement to AI – Tractor movement.

Figure 9 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 D2.2.

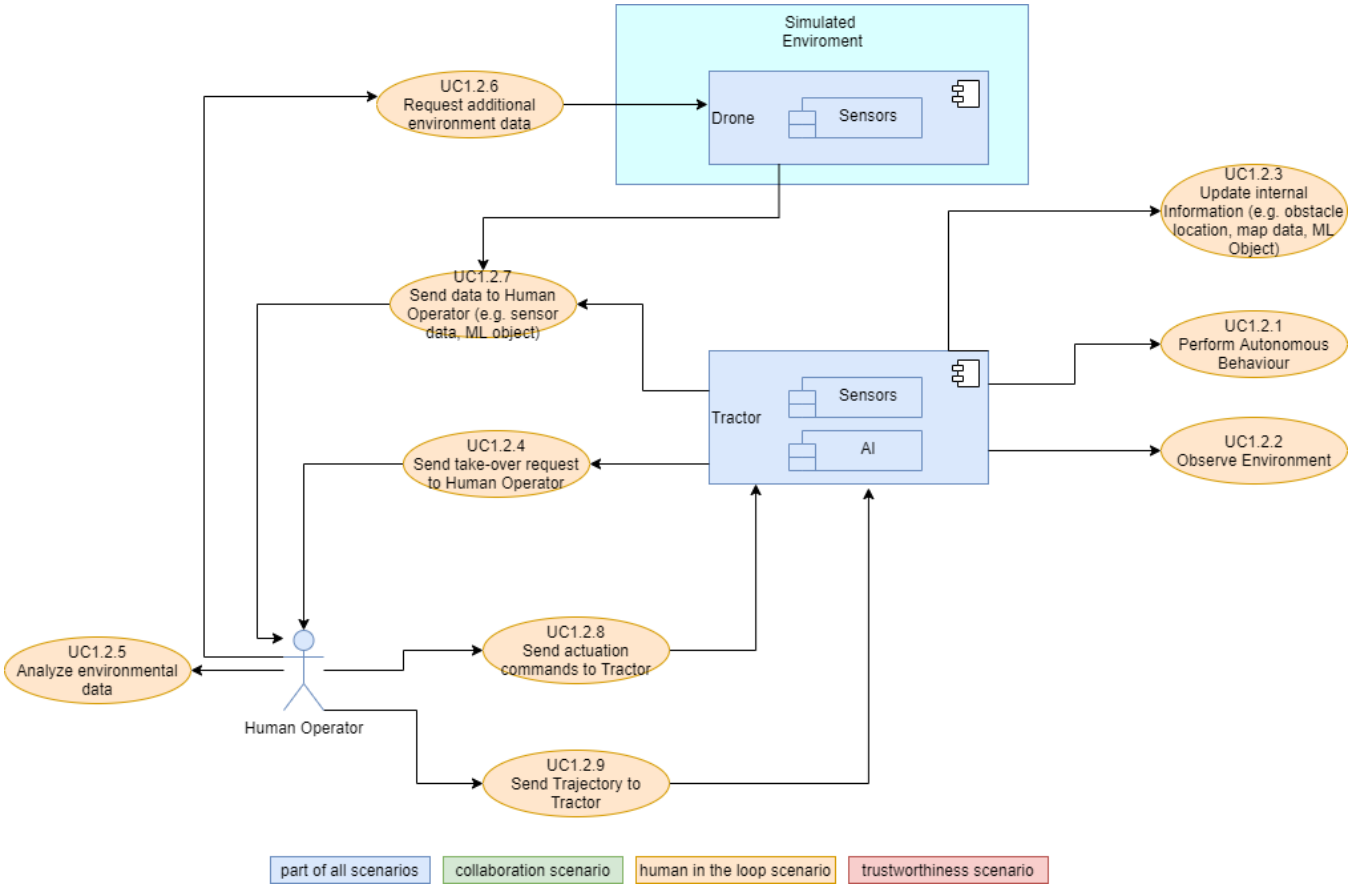
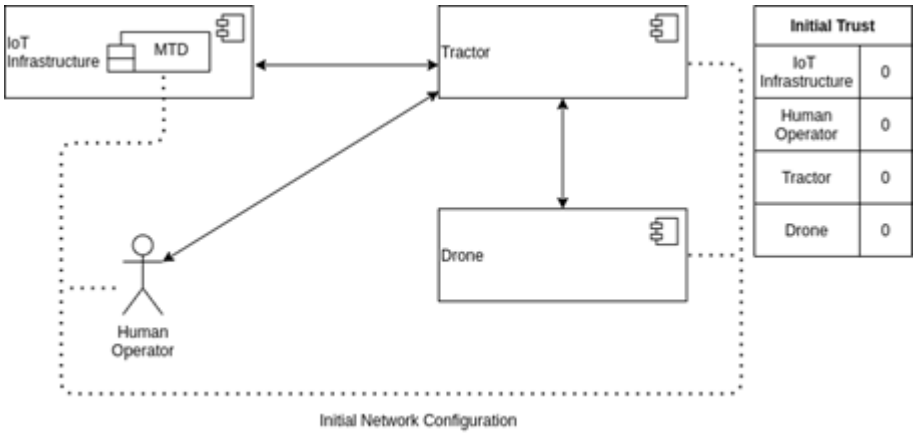
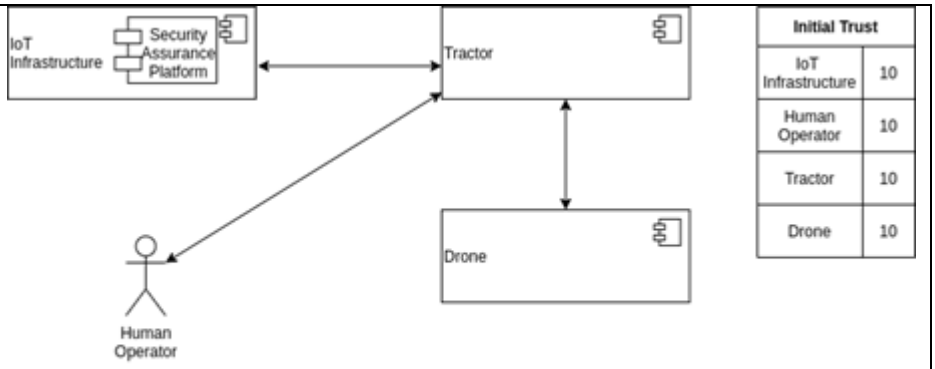


Figure 9: UC1 – Human-in-the-Loop Scenario

2.1.5.3 SCENARIO 1.3 – TRUSTWORTHINESS

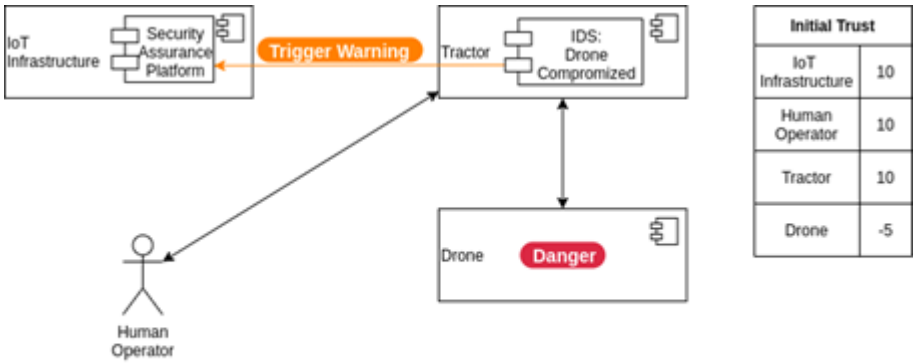
Scenario Name	Trustworthiness
Scenario ID	UC1-Scenario3
Partners	TSI, SANL

Description	During deployment to the field, all participating parties need to initialize their distributed Intrusion Detection System (IDS) component through secure channels to establish a trust-based network. For the agriculture scenario, a key role is that of the tractor. We assume there are at least two more participants for the most basic scenario. The one is the human operator and the other is a computation and communication node (IoT infrastructure). Additional entities could participate such as other tractor(s), sensor(s), actuator(s), 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 security assurance platform is notified. The security assurance platform initiates a Moving Target Defense (MTD) mitigation process. Consequently, the MTD changes network parameters as needed, based on pre-defined defence strategies, making it impossible for the offending participant to further affect the rest of the system.
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.



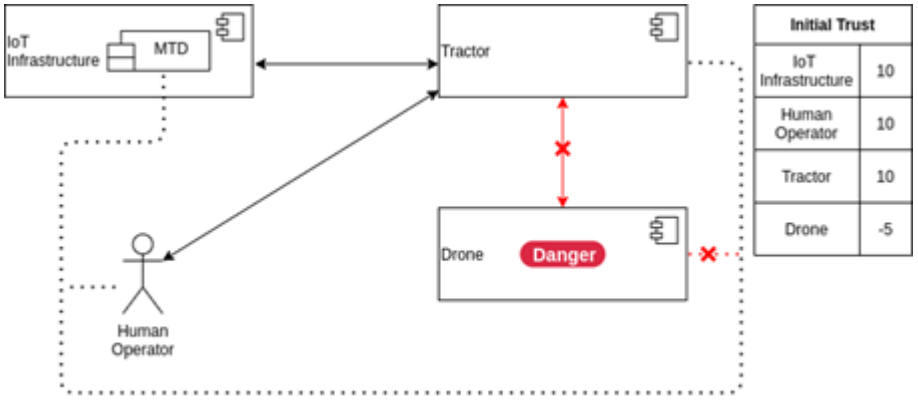
Normal Operation

Key Scene 3.3: Attack Detection: a participant (drone) is compromised and sends information that lowers its trust to the point that the IDS mechanisms are triggered. The Security Assurance Platform is notified of the event.



Attack Detection

Key Scene 3.4: Mitigation Phase: The Moving Target Defense mechanism is activated by the Security Assurance Platform, 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.



New network configuration

Potential Variation of the Scene	[1] If participants were added in an already functioning network, trust would have to be built and defences would be higher until trust was established for the new participants as well. [2] If an attack was detected on a crucial element of the network, for example the human operator proved to be malicious or his equipment had been compromised and an attacker tried to control the tractor which could be considered an insider attack, upon detection, the Security Assurance Platform would need to bring the entire system to a failsafe state. [3] When the tractor requests an AI model to tackle a specific problem (e.g., obstacle detection), the malicious participant might send an altered AI model, to modify the tractors behaviour. This action would be recognized by the Infrastructure-Assisted Knowledge Management and reported to the Security Assurance Platform. The Security Assurance Platform would then take the necessary measures to mitigate the attack.
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, the drone (or any other 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, drone, IoT-Infrastructure and human operator

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

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 D2.2.

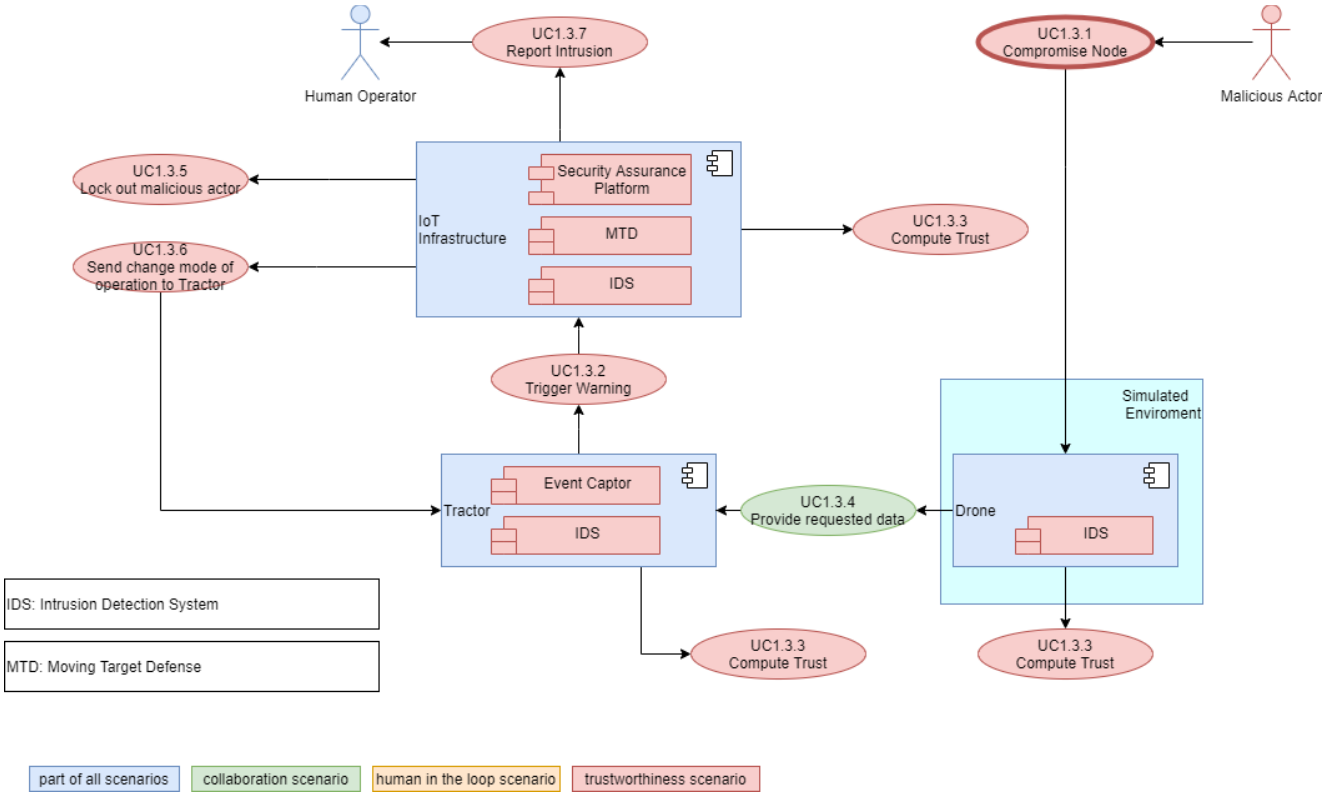


Figure 10: UC1 – Trustworthiness Scenario

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[1]. There is a need for more effective strategies for patient management to improve patient outcomes and reduce healthcare costs.

Remote patient monitoring[2] 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 home 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 11 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 recommendations and drive interventions, and to extract accurate information on the health status of the patients that are monitored in their home environment. The AI-assisted system will guide the patients through their daily activities and through their care plan, with clinical expert oversight. Patients will be equipped with wearable devices measuring relevant data that is transferred to a personal IoT device (e.g., smart watch or 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. The goal is to both improve outcomes and increase adherence.

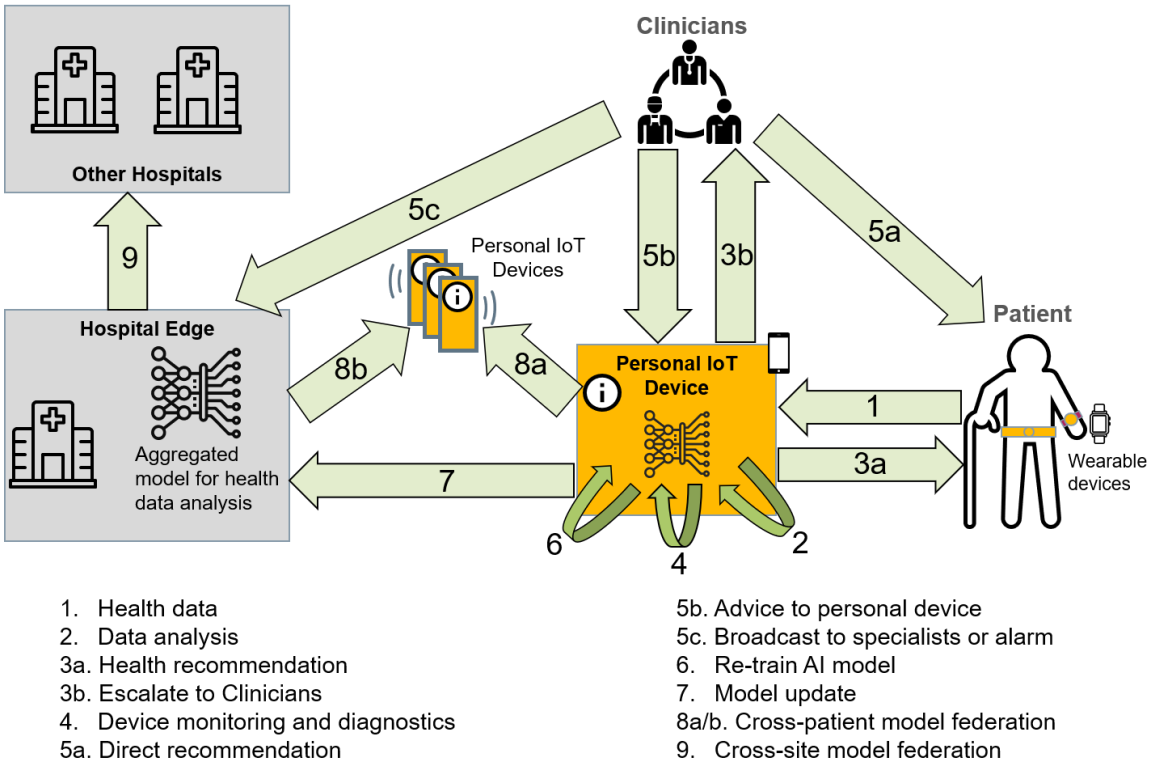


Figure 11: Healthcare Use Case

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 coordinator 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). 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. Digital consent management to drive the interactions of the system (patients, clinicians, devices) can be managed e.g., via smart contracts.

2.2.3 COMPONENTS / ACTORS OF THE USE CASE

2.2.3.1 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).

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.

2.2.3.2 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 coordinator 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.

2.2.3.3 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.

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.

2.2.3.4 TRUST COMPONENTS

2.2.3.4.1 SECURITY ASSURANCE PLATFORM

The Assurance Platform will provide runtime, continuous assessment and certification of the monitored healthcare UC deployment.

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. Throughout its operation, the Assurance Platform will also interface with the DLT building blocks, allowing the evidence-based operation of the assurance scheme. Furthermore, the Assurance Platform will be used as a point for generating evidence needed for auditing and certification pertinent to the healthcare environment.

2.2.3.4.2 MOVING TARGET DEFENCES (MTDS)

Moving Target Defence (MTD) is a technology that changes the network configuration dynamically over time, in order 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.

2.2.3.4.3 DISTRIBUTED LEDGER TECHNOLOGIES (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.

2.2.4 TARGET MARKETS / END USERS

The overall solution developed in IntellIoT and demonstrated in the domain of cardiovascular diseases has applicability in many other clinical domains where patients require support at home and guidance for recovery and disease management. The infrastructure can be applied for the development and deployment of new algorithms, with customized apps and sensors, to support elderly care with exercising, diet and cognitive capacity training, to support behaviour change for healthy sleep, to support efficient management of mental illness such as depression and anxiety, and many other clinical applications. When validated and proven in these promising areas, the concept of remote care can be applied to many other clinician-patient interactions. This trend has been significantly accelerated in 2020 during the COVID-19 pandemic, when for instance remote consultations with General Practitioners have become common practice for non-emergency issues.

We have identified several classes of end users for the IntellIoT infrastructure developed in the healthcare use case:

- Our key end users are clinicians and their patients. A successful implementation of such a system and its acceptance by users will enable healthcare systems to reach better outcomes at lower costs.
- Components and concepts of the solution can be applied in the consumer market, with AI-enabled personalized recommendations.
- The infrastructure could be generalized and opened to new use cases which would create opportunities for new algorithms and devices.

- Governments are well aware of the need to improve outcomes of healthcare delivery while reducing costs. With healthcare costs becoming unsustainable, many healthcare systems are moving towards prevention and decentralization of care. It is likely that the COVID-19 crisis will accelerate this trend.

2.2.5 SCENARIOS

2.2.5.1 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 coordinator and updates are received from the coordinator. 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 coordinator 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 to the patient. **Key Scene 1.3:** The algorithm is regularly re-trained locally, and updates are sent to the coordinator. 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.

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 D2.2.

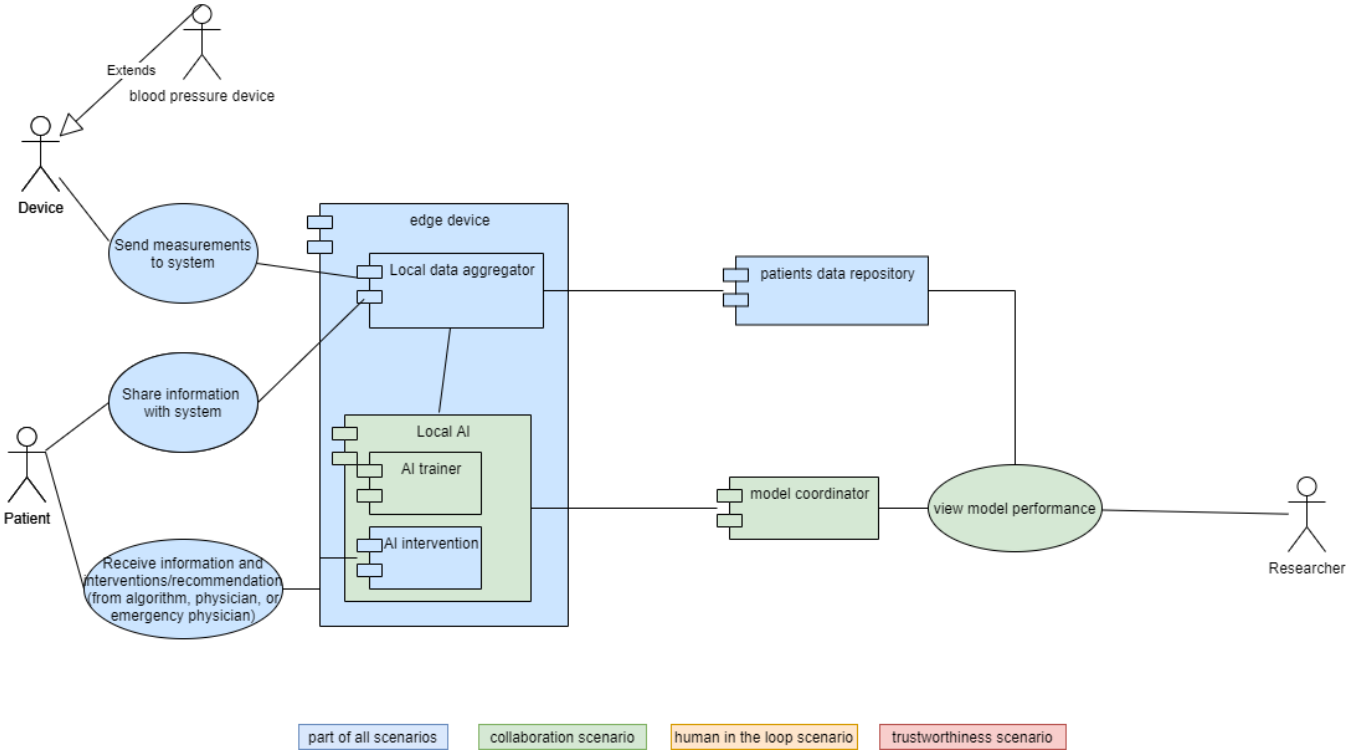


Figure 12: UC2 - Collaborative IoT Scenario

2.2.5.2 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. data is transmitted to the smart watch. 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 needed, recommendations/interventions are provided to the patient. **Key Scene 2.2**: The patient experienced a pre-syncopal episode. 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:** 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 2.4:** The application provides the physician's instructions to the patient. **Key Scene 2.5:** The physician contacts the patient and provides advice. 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 application contacts the patient who confirms that the device does not work.
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 smart watch 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 the majority 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.

Figure 13 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 D2.2.

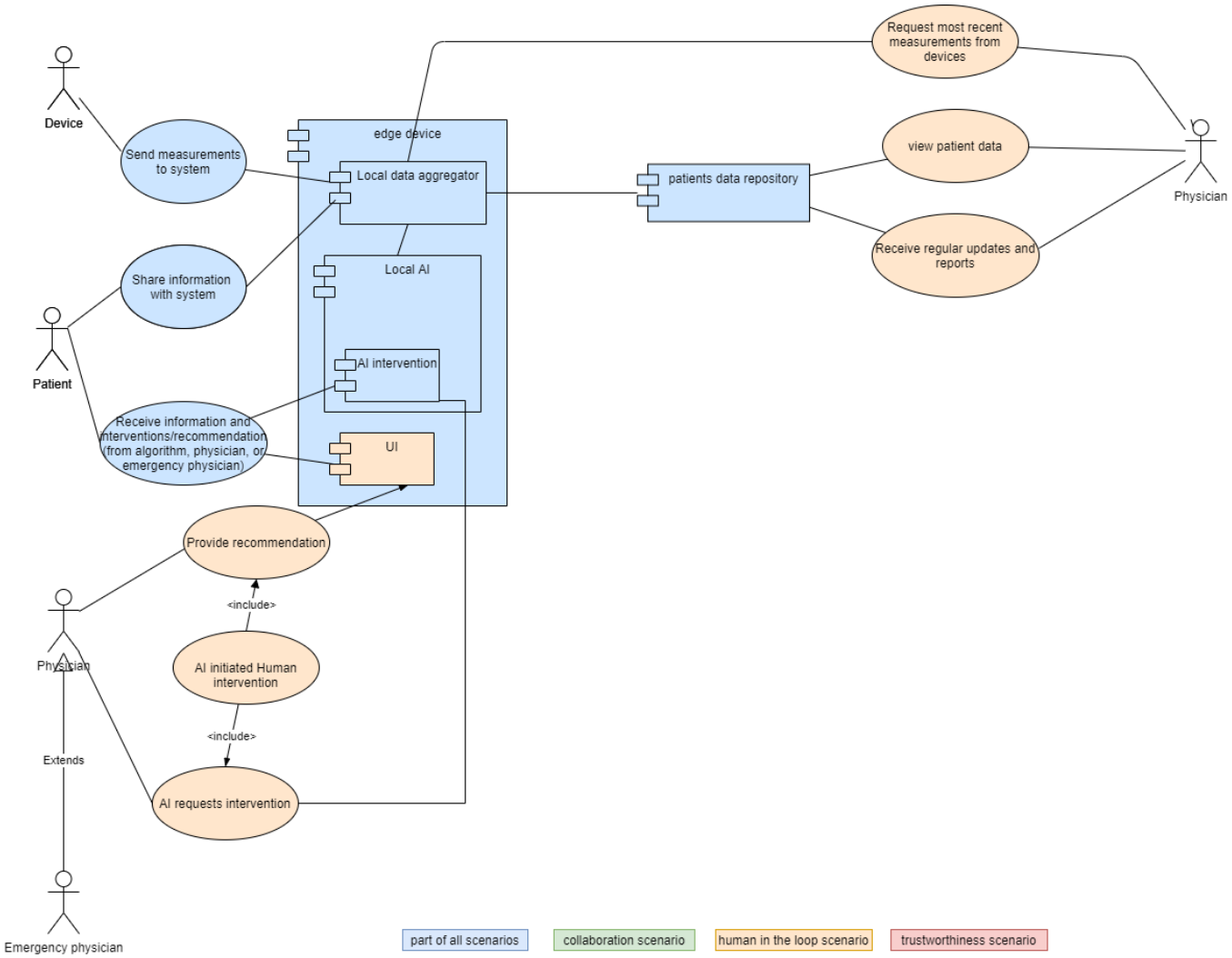
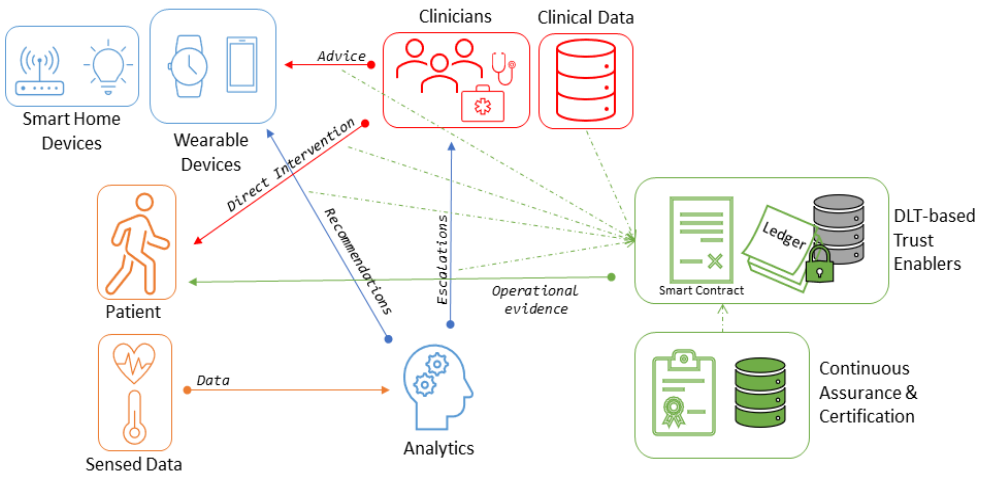
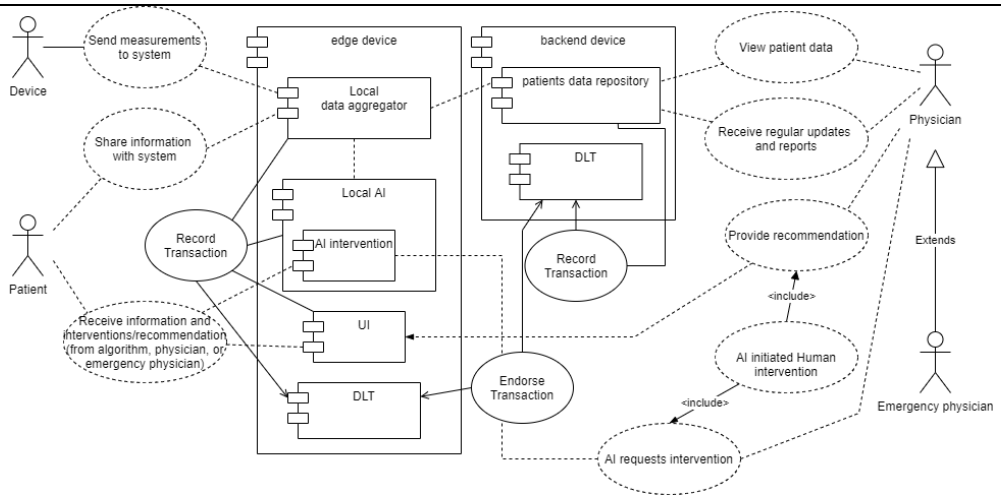


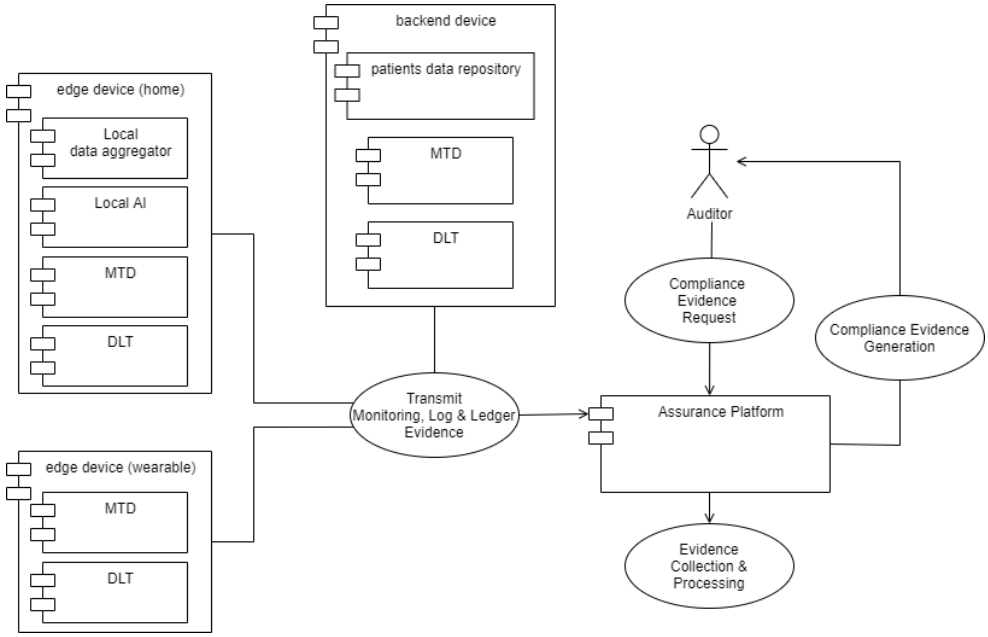
Figure 13: UC2 – Human-in-the-Loop Scenario

2.2.5.3 SCENARIO 2.3 – TRUSTWORTHINESS

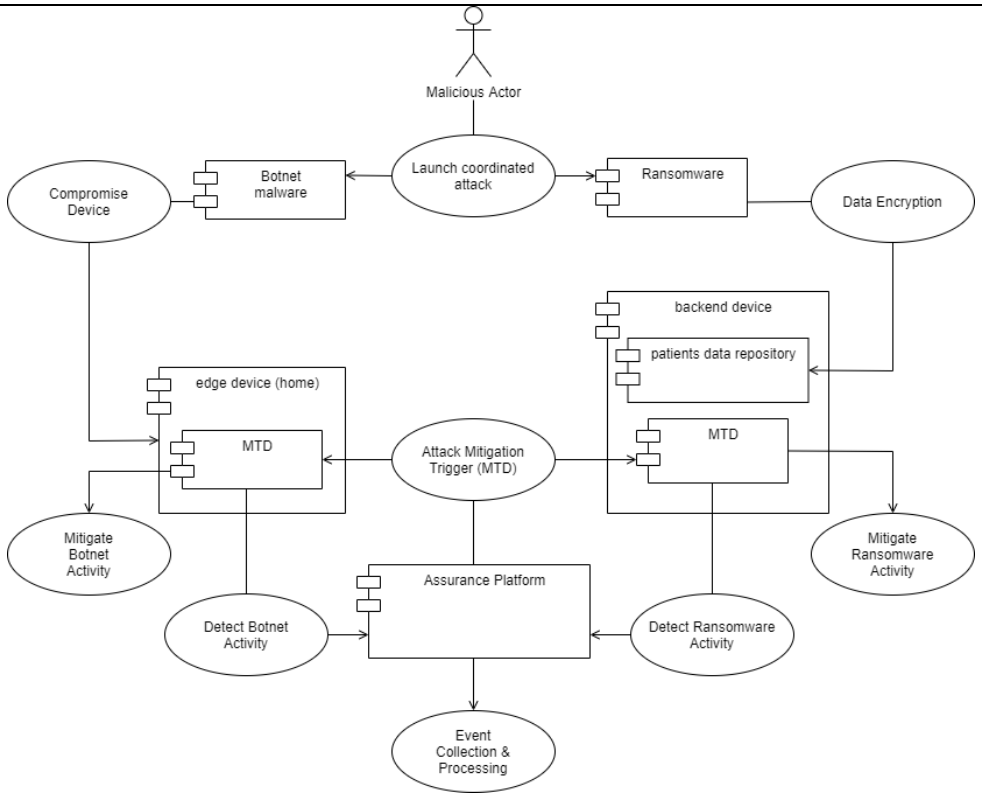
Scenario Name	Security, Privacy & Trust in NGIoT-enabled remote patient care
Scenario ID	UC2-Scenario3
Partners	SANL, TSI, AAU, EURECOM
Description	During the events taking place in the two previous scenarios (i.e., Scenario 1 & Scenario 2), trust and transparency-related evidence are generated via the DLT-based enablers of IntellIoT. 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, 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 a phishing email fabricated to deploy a ransomware malware. The IntellIoT security mechanisms detect the two attacks and trigger the necessary defence mechanisms to mitigate them. 
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.



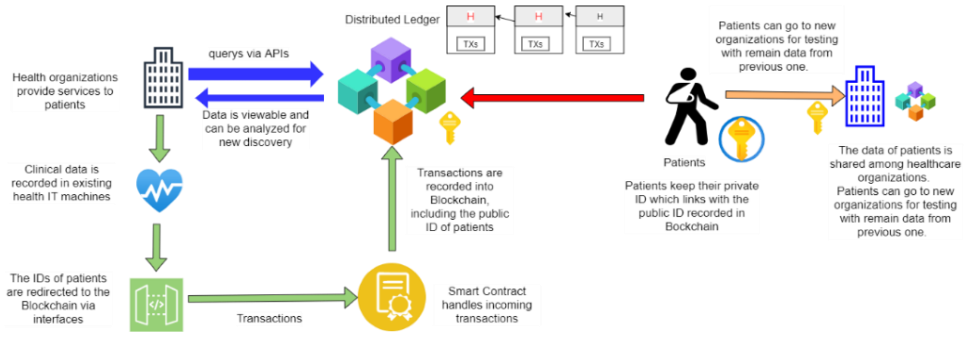
Key Scene 3.3: Attack Phase – Smart device & health data protection. Detection and mitigation of attacks on smart devices (botnet takeover) and data storage (ransomware).



Potential Variation of the Scene

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.



Purpose	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] 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. [2] Assurance Platform: Event & log monitoring in real-time and batch mode to aggregate indicators of attack and compliance evidence from other trust enablers and system components. Generation of compliance evidence to support auditing and certification. Triggering of defense techniques by interacting with other trust enablers [3] Patient-side & clinical-side security controls: 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 on both environments
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, Ledger, Assurance Platform, Patient-side security controls, Clinical-side security controls, Botnet Malware, Ransomware, Patient smart home devices, Patient smart wearable devices, Patient data repository, Auditor
Information exchange between actors	Patient vitals/measurements Analytics recommendations 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

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 D2.2.

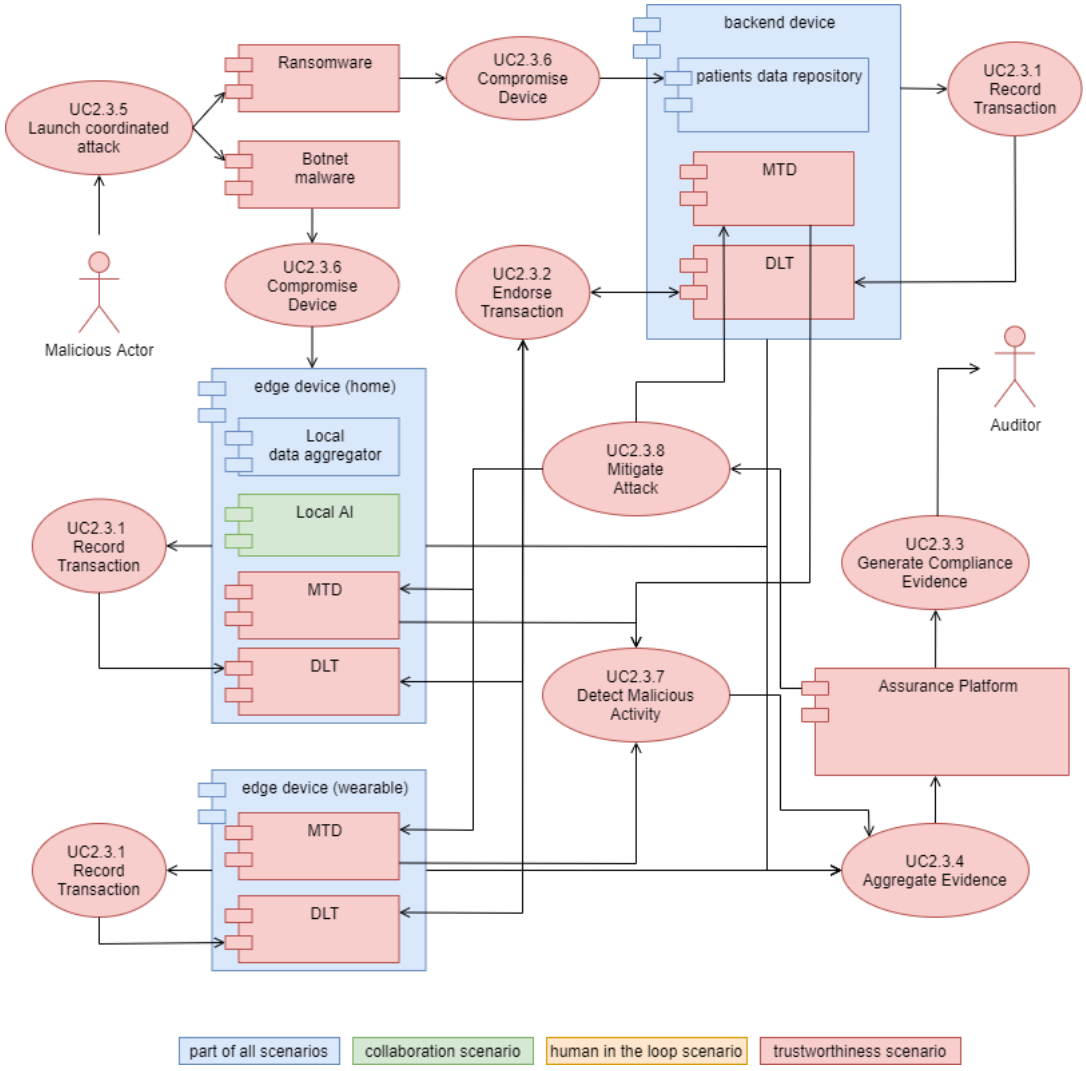


Figure 14: UC2 – Trustworthiness Scenario

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 operators and plant operator – where at least the latter two are represented by digital agents. Transport is done by robots and Automated guided vehicles (AGVs), guided by in-built AI. Whenever built-in computing resources are insufficient, computation tasks are automatically offloaded to the edge cloud. 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 15 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 or an image to be engraved or lasered on a wood slice. In step (2), the Reactive Planner creates a machine orchestration plan to fabricate the desired product, by searching for suitable artefacts that represent available machines. If the Reactive Planner cannot find a solution for the production goal, it can request support from a human plant operator or customer (3). In the proposed demonstrator, a wood slice (as raw material) is selected, and the AI decides how to place it in which machine(s) to engrave and/or laser text or image on it. Human help might be needed e.g., if the image 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 owner or a third-party operator, 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. E.g., 5G communication is setup that supports wireless TSN and supports URLL not only in Uplink or Downlink, but also in Sidelink (D2D). In step (5), a local AI on board of the robot decides how the robot picks a workpiece and places it in the next machine. If the confidence-level of the local AI is low and it cannot pick and place the workpiece safely, a connection to a human is established (6). Utilizing AR, the human can **virtually grab the workpiece** to support the robot. A **tactile communication** is established for this interaction, under consideration of security and privacy. Cameras will generate an accurate enough reconstruction of the surroundings and the robot itself which allows the full control and visual information about the parameters of every joint. 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 (overlaying the scanned model with the CAD model)**, rendered in the local edge, with delayed movement of the real robot. From the human handling of the work piece, the **local AI re-trains** itself using the human feedback as target (7) and **federates the learned parameters** to other robots (8).

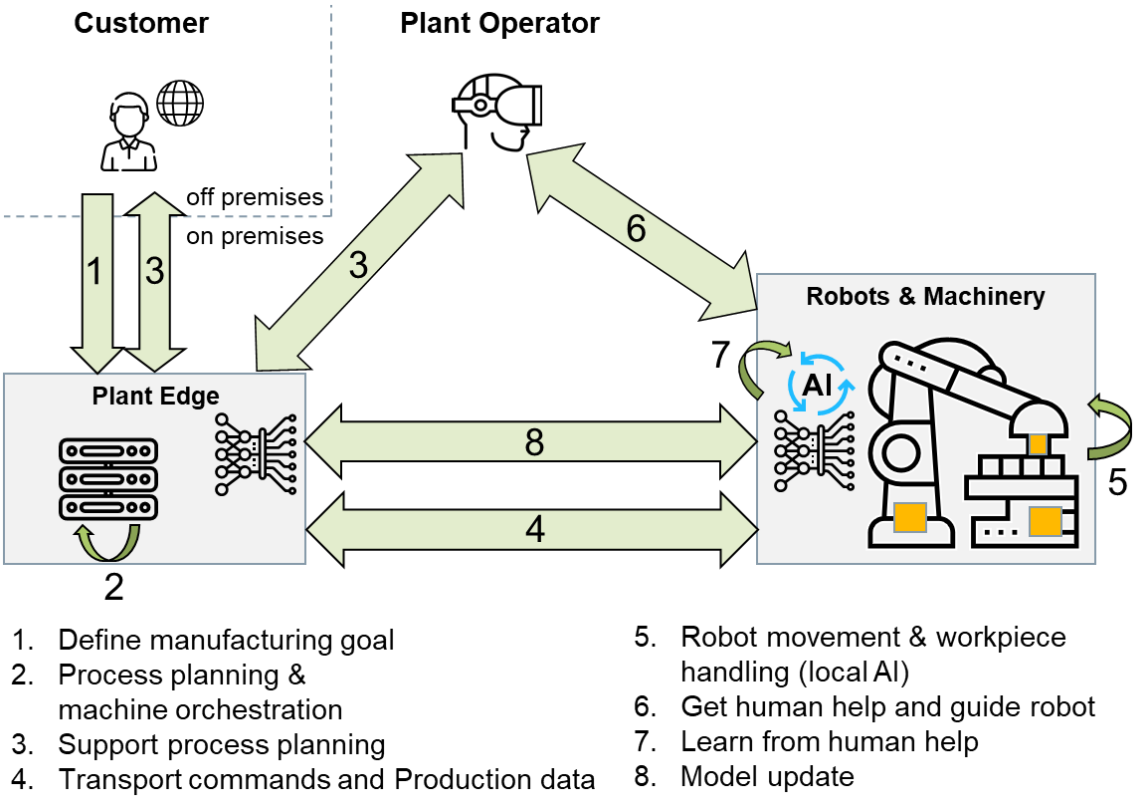


Figure 15: Manufacturing use case

2.3.3 COMPONENTS / ACTORS OF THE USE CASE

Figure 15 summarized the general approach of the manufacturing use case. Figure 16, Figure 17, Figure 18, Figure 19 and Figure 20 show use case diagrams for the scenarios described in chapter 2.3.5**.** Actors and components playing a considerable role in the use case diagrams are described in the following:

2.3.3.1 CUSTOMER

A customer provides a specification for a product, i.e., a production goal. The customer will be asked for help if the Reactive Planner component is unsure interpreting his goals. The interface to the customer is an HMI provided by the Reactive Planner.

2.3.3.2 PLANT OPERATOR

A plant operator is asked for help whenever AI faces uncertainties handling a workpiece. The plant operator is equipped with AR glasses and a Stylus device to interact with the robot.

2.3.3.3 MALICIOUS ACTOR

Other than the typical actors interacting with the manufacturing environment, from the trustworthiness perspective it is important to consider the presence of malicious actors interacting with the infrastructure and services; be it external actors (e.g., customers with malicious intent) or internal actors (e.g., a disgruntled employee or another

malicious actor with access to valid credentials of a plant operator). The potential presence of these actors introduces a number of security (and safety)-related threats that the system must be able to mitigate in an effective manner.

2.3.3.4 MACHINE OWNER

The machine owner is asked for help whenever the Reactive Planner has issues due to insufficient or incomplete machine descriptions or a robot is unsure about how to place a workpiece. The machine owner might be equipped with AR glasses and a Stylus device for the latter.

2.3.3.5 AR GLASSES AND STYLUS INPUT DEVICE

AR glasses, i.e., Microsoft HoloLens 2, will be used by the plant operator in order 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.

2.3.3.6 REACTIVE PLANNER

The HyperMAS Reactive Planner creates a machine orchestration plan to fabricate the desired product by searching for suitable artefacts that encapsulate available machines and combining services that are provided by these artefacts. In this component, our aim is to integrate automated planning with multi-agent-oriented programming on top of a hypermedia-based infrastructure so that we may achieve a flexible yet scalable system. To accomplish this, we use multi-agent planning: we integrate Belief-Desire-Intention (BDI) agents with first-principles planning over Web-based artefacts, and we use semantic multi-agent organizations to coordinate the individual agents towards the production goal.[4] If our system is unable to find a solution for a given production goal, it can request support from a human plant operator, machine owner, or customer. Note that the Reactive Planner is distributed over several computing components, even if depicted as a box for the sake of simplicity.

2.3.3.7 ROBOT

A robot arm is tasked to transport the workpiece to the next production step. It is an arm composed of rotative joints linked together with a gripper at the end-effector. Local AI on board of the robot decides how the robot picks a workpiece and places it in the next machine. Additional cameras will generate an accurate enough reconstruction of the surroundings and the robot itself. The different joints and the camera are connected to a central computing unit. The central computing unit is responsible for commanding the joints in real-time in order to execute the task, communicating with other components.

2.3.3.8 DISTRIBUTED AI

Each robot is equipped with a local AI. The main purpose of the AI is for object recognition including dimensions and physical properties (e.g., brittleness, fatigue under stress). Since robots are exposed to a limited number of samples,

[4] 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.

initially, the local AI at each robot will be trained in a collaborative/federated manner to improve its performance. Thereby it is important that no training data is exchanged between the local AI components to protect the privacy of the production tasks submitted by the different customers of the shared manufacturing plant. Towards such distributed AI learning, the network edge acts as a mediator for collaboration.

During the inference, the local AI will be actively updated using the new observations, decisions and the corresponding reward-based feedback. Under the circumstances of the local AI failing to infer reliable decisions, robots may offload the local AI towards the network edge. In this case, the edge can aid by allowing AI model sharing among the robots providing access to the updated AI model. When there is no AI model that can resolve the issue, a request for human intervention is issued.

In addition to the requests generated from the network, human intervention can take place when a new or modified procedure is introduced to the robots (e.g., change of instructions on the existing procedure as well as integrating a new product into the system). During human intervention, an operator will generate a sequence of actions to introduce the desired procedure. Using this procedure, the **local AI re-trains** itself using the feedback as the target. Once the robot of interest updates its local AI, it will disseminate the updated model allowing other robots to **federate the learned parameters**.

2.3.3.9 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. Laser cutter and engraver will be available in the demo setup for this use case. A machine-readable machine description, e.g., W3C WoT TD capability descriptions, enables Reactive Planner to gather machine properties and capabilities and make use of particular machines in a production plan.

2.3.3.10 NETWORK MANAGER

When human help is needed to guide a robot, Reactive Planner requests a **tactile communication** between the robot and the helping human. Network manager will plan and enforce this communication relation, not only considering real-time and reliability constraints, but also security and privacy. When a robot interacts with a machine, e.g., moves a part in the working area of a machine, network manager establishes a safe peer-to-peer communication relation between both to protect from collisions. When security assurance platform detects suspicious operations from a potentially malicious actor, it triggers network manager to lock out this human, i.e., to cut the according communication relation.

2.3.3.11 TRUST COMPONENTS

2.3.3.11.1 SECURITY ASSURANCE PLATFORM

Comprehensive security mechanisms are applied to ensure privacy and security of customer data. Whenever a machine or robot is tasked, contractual arrangements are set up using a distributed ledger.

The integration of the Security Assurance Platform within the manufacturing environment will provide runtime, continuous assessment and certification 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.

2.3.3.11.2 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 evidences and records of activities. By automating manual processes, a DLTs/blockchain network could ensure product quality and authenticity, accelerate transactions and reduce processing fees.

2.3.4 TARGET MARKETS / END USERS

The AI developed within the scope of IntellIoT UC3 is focused on two main tasks: object detection for pick-and-place applications and continuous improvements via human-in-the-loop. The distributed AI for object recognition and identification of its physical properties developed under on-device as well as communication constraints can be adopted for the applications beyond manufacturing that use memory and energy limited devices such as rescue robots, explore/expedition devices, automatic parcel/package sorting. AI improvement mechanisms via human-in-the-loop are used to enable the usage of AI-based decision mechanisms in applications, where mistakes due to wrong decisions could lead to expensive damage of products or production facilities. Input from the human is used to solve acute blockings due to uncertainties and to enhance the AI model robustness over time. These solutions can be adopted for various AI-driven applications outside factory automation, including navigation, control and communication. In the main focus as end users for the IntellIoT manufacturing use case are:

- Plant owners and operators, which deal with flexible automation, particularly for small lot sizes. Besides the typical application in the factory automation domain, other domains like e.g., logistics and automated storage are imaginable.
- System integrators building and maintaining plants for flexible automation.
- Machine Builders, which integrate their machines in shared manufacturing plants, particularly those following new business models like pay per use.
- Automation component vendors, delivering e.g., PLCs, edge devices, robots being used in aforementioned machines and plants.
- Industrial workers collaborating with machines and robots controlled by AI.
- End user associations, e.g., PROFInet International, VDMA, ZVEI that will advise end users about new technologies available on the market. Although associations are not direct end users of the technologies, they can still be of major influence for reaching out to other end users and be of support for bringing technologies on the market.

2.3.5 SCENARIOS

2.3.5.1 SCENARIO 3.1 – COLLABORATIVE IOT

Scenario Name	Collaborative IoT
Scenario ID	UC3-Scenario 1

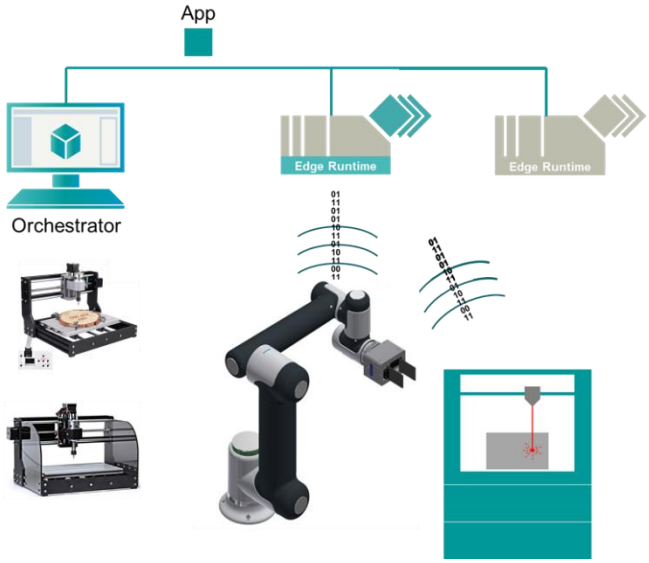
Partners	SIEMENS, HSG, HOLO, EURECOM, TTC, SANL, TSI, UOULU, AAU
Description	Our shared manufacturing plant receives a *goal* formulated by a customer. A Reactive Planner component translates the goal into a process plan. To execute the plan, the plant has a flexible production cell, in our demo case 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, continuously check for open tasks and pick them when they are able to fulfil them, i.e., the agents 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, 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 management system (EMS), 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 16: A customer requests a new product to be manufactured by the shared manufacturing plant. Therefore, the production goal is designed by the customer (e.g., using a dedicated HMI).

Thereby, as a Proof of Concept, the customer specifies a desired shape and engraving on a specific material, which together represent the desired product.

The *goal* defined by the customer is then transformed into a *plan* that comprises multiple tasks, which give a formal description of machine actions and the required resources. For example, this could be a stepwise definition required to achieve the goal:

1. a **robot** positions itself at X
2. a **robot r**equests **computation** of best grabbing spot at an **AI edge app**
3. a **robot** grabs the workpiece at Z
4. a **robot** puts workpiece in a **laser cutter**

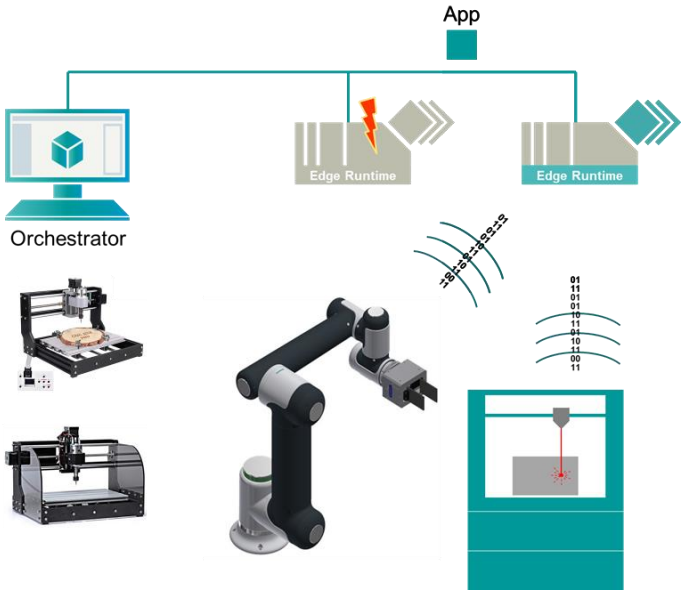
Key Scene 1.2, see Figure 16**:** The above derived plan is then deployed to an execution environment for plans on the edge. According to the tasks of the plan, resources are optimally allocated on available and suitable machinery (robots or CNC), and edge devices (for computing tasks within the plan). A local AI pipeline is processing the images from the camera on the robot and computes the best grabbing spot autonomously. If parts of the AI pipeline are executed on the robot, it will showcase AI on a constrained device.



Key Scene 1.3, see Figure 16**:** 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., image processing, or inference AI) are deployed in the edge infrastructure and optimally allocated to edge resources (also taking into account the network specifics and failover constraints).

Key Scene 1.4, see Figure 16: During production, the wireless connection between the robot (UE) and the base station is not the optimal choice anymore (e.g., the performance is getting worse due to network congestion), for which it is decided to handover to another base station. Accordingly, the edge app with its state is moved to another edge device.

	 **Key Scene 1.5**: After the model of the local AI controlling the robot is updated (e.g., through input from the user; see Section 2.1.5.2) the difference of the updated model to its original state is shared with other local AIs.
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.
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 offloaded AI capabilities at edge nodes cannot be accessed. In the event of those problems, the production might be disturbed or even stopped. Downstream fallback mechanism 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 → site access control, tamper proof housings, limited IO ports, access protected terminals [2] Eavesdropping on network link (e.g., wireless link) → Encryption [3] Manipulation of network traffic → Security protocols (TLS, IPSec, VPN) [4] Network attacks on IT/OT infrastructure from Internet → Firewalls, physical network separations [5] Malware on edge apps → App isolation concepts, signed apps, app auditing
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, Reactive Planner, Machines and Robot
Information exchange between actors	Customer sends goal to Reactive Planner. Reactive Planner assigns jobs to machines and robots, which provide state information to Reactive Planner. 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.

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 D2.2.

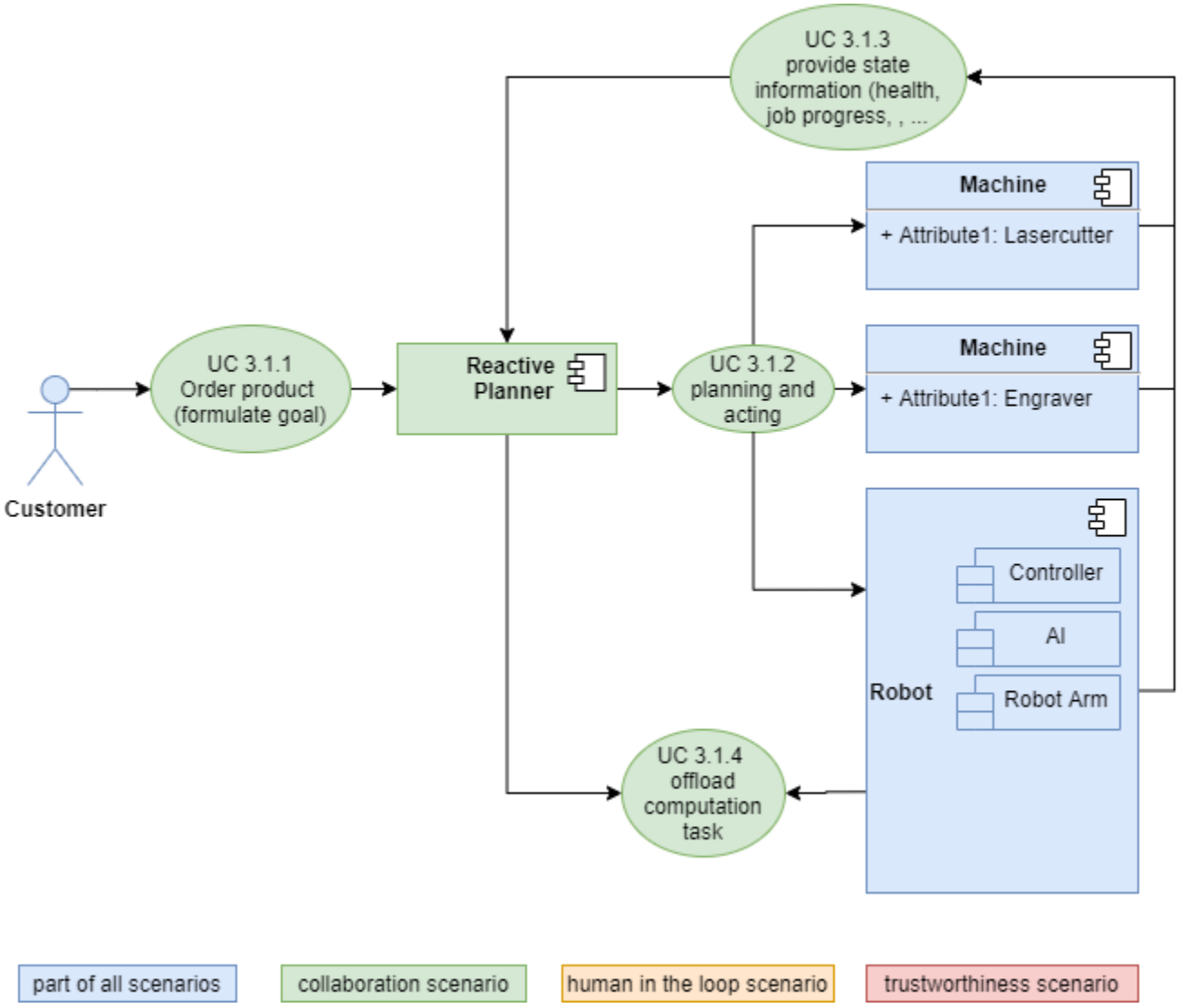
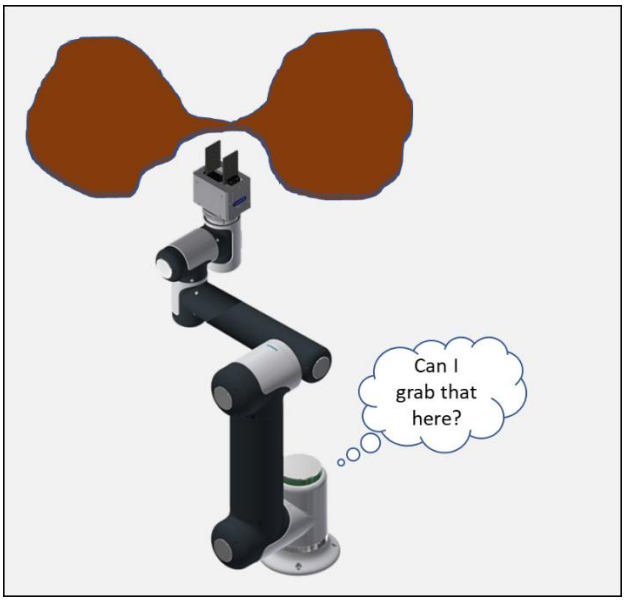


Figure 16: use case diagram collaboration

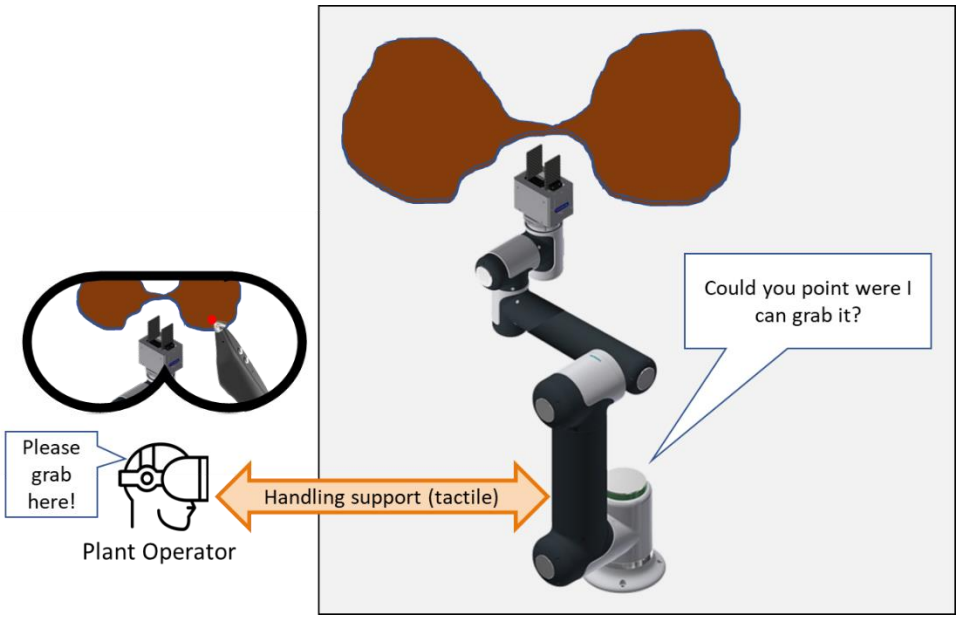
2.3.5.2 SCENARIO 3.2 – HUMAN-IN-THE-LOOP

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. A Reactive Planner component automatically computes production plans from a) a formal specification of a manufacturing goal by a customer and b) explicit formal descriptions of the available production capabilities.

	During the running manufacturing process, local AI on a robot has an insufficient level of confidence in the decision about how to grab a workpiece or how to insert and place a workpiece in a machine. To solve its issue, the robot asks a human, e.g., the plant operator or machine owner, for help. 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, AI is re-trained based on the human input and then capable of overcoming 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 17: Local AI associated with the robot is unsure how to grab or place a workpiece. Thus, a component of the HyperMAS contacts the plant operator for clarification. 

A real-time tactile AR connection to the plant operator is established in a secure manner 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 how to grab and positions the robot through guiding the robot by grabbing and moving the robot arm projected in his glasses with the stylus pen (tactile feedback).

After receiving help from the human, the robot completes his task. The manufacturing process can continue with short delay.



Key Scene 2.2, see Figure 17**:** 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 17**:** Later, when producing another product, a workpiece similar to the one before occurs. Now, the robot is able to grab the workpiece without human help, because it has learned from the previous human help.

Key Scene 2.4, see Figure 18**:** The uncertainties about placing a workpiece could also relate to a third-party machine, then the *machine owner* could directly be contacted instead of the plant operator.

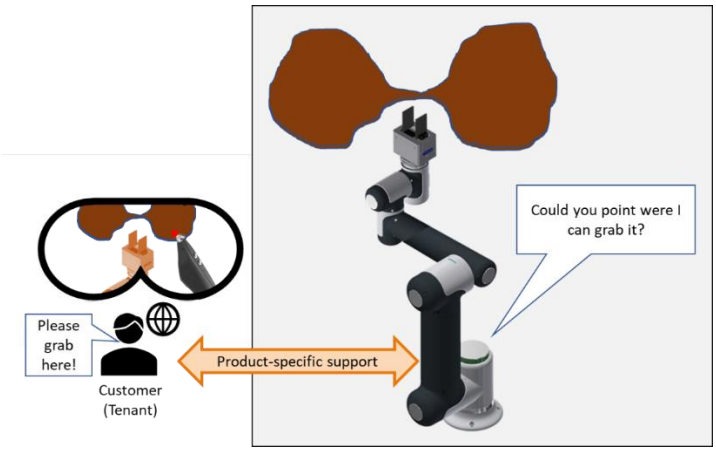
In such cases, an off-premise actor (e.g., machine owner) is contacted (instead of the plant operator) by a component of the HyperMAS.

Alternatively, the plant operator can also forward the issue to the off-premise actor (customer, machine owner, etc.) when he does not know the solution.

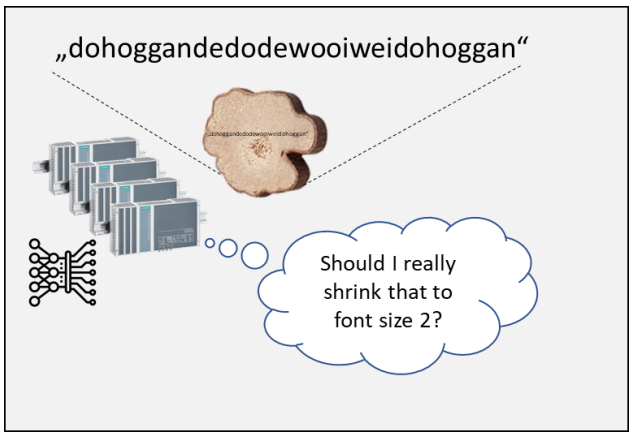
The key challenge of this scene compared to the original key scene is that machine owner or customer are (usually) off-premise. Since a tactile AR communication link over a long-distance public network is usually not possible, the rendered robot comes into play, which allows for remote handling with slightly delayed movement of the real robot.

Key Scene 2.5, see Figure 18**:** The uncertainties of grabbing a workpiece could concern properties of the workpiece, e.g., stability or centre of gravity of a mixed material semi-finished product provided by the *customer*. In this case, help from the *customer* would be required. The

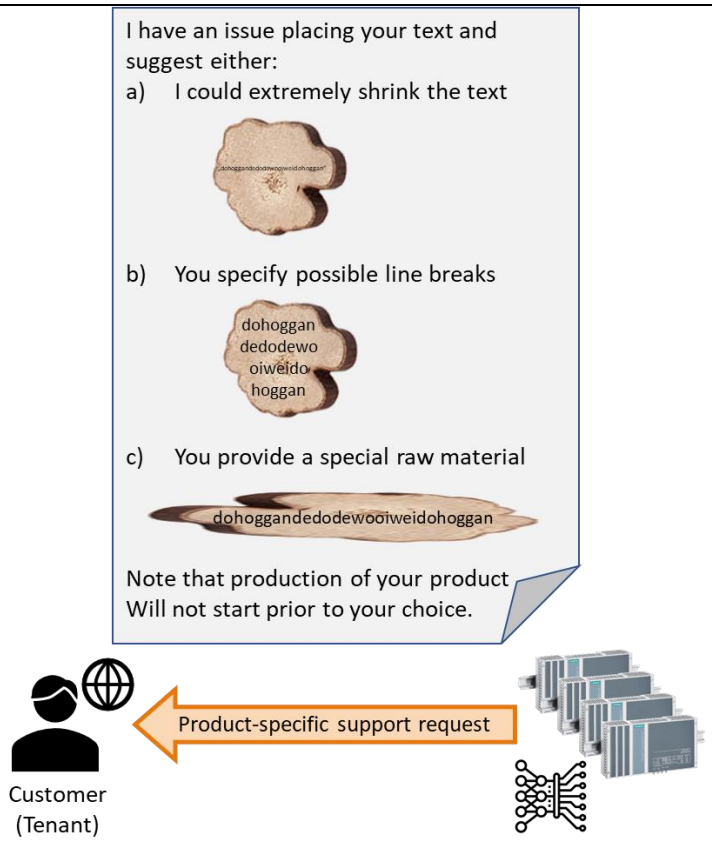
customer might not be as trustworthy as the plant operator or a machine owner, as everybody can easily act as a customer. Additionally, a customer might be unexperienced controlling a robot. Therefore, the customer will only be allowed to control the rendered robot. Before movements proposed by a customer are executed by the real robot, a plant operator has to clear them.



Key Scene 2.6, see Figure 17: While the 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 connection to the customer is established and customer supports the decision, e.g., by selecting from two or more presented interpretations or by refining his goal description. HyperMAS is now able to plan the manufacturing process.

	 **Key Scene 2.7,** see Figure 17: In case uncertainties about machine capabilities concern a third-party machine, the third-party machine owner could directly be contacted through a trustworthy connection instead of the plant operator.
Potential Variation of the Scenario	**Variation Scene 1:** Whenever an off-premise 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. **Variation Scene 3,** see Figure 17: In a scenario with multiple robots, all robots have learned from human help one of the robots has experienced. That means, if robot A got help on the handling of a special workpiece, all other robots will be able to handle similar workpieces after the updated model has been shared.
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 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	Local AI on a robot 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.

	HyperMAS is trained 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 has learned from this help for future decisions. HyperMAS is enabled to compute a production plan for the desired goal with the help of the customer, plant operator or machine owner and has learned 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, or to place it into the selected machines. 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, 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; Reactive Planner 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 AI in the robot to prove that it recognizes uncertainties in its decision and requests human help. • Provision of slight variations of the former workpieces to the AI in the robot to prove that it learns from human help. • 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 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.

Figure 17 and 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 D2.2.

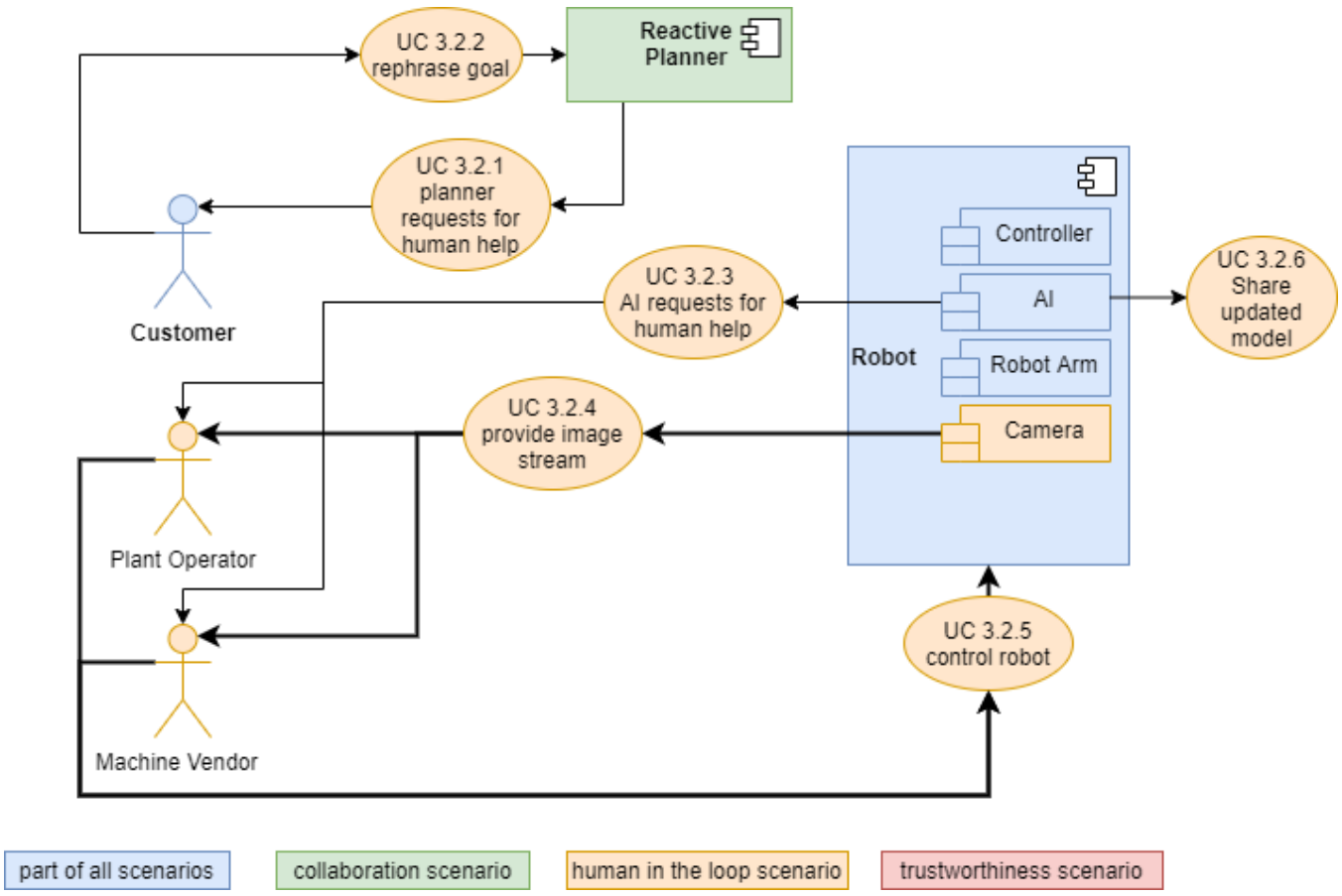


Figure 17: use case diagram human-in-the-loop

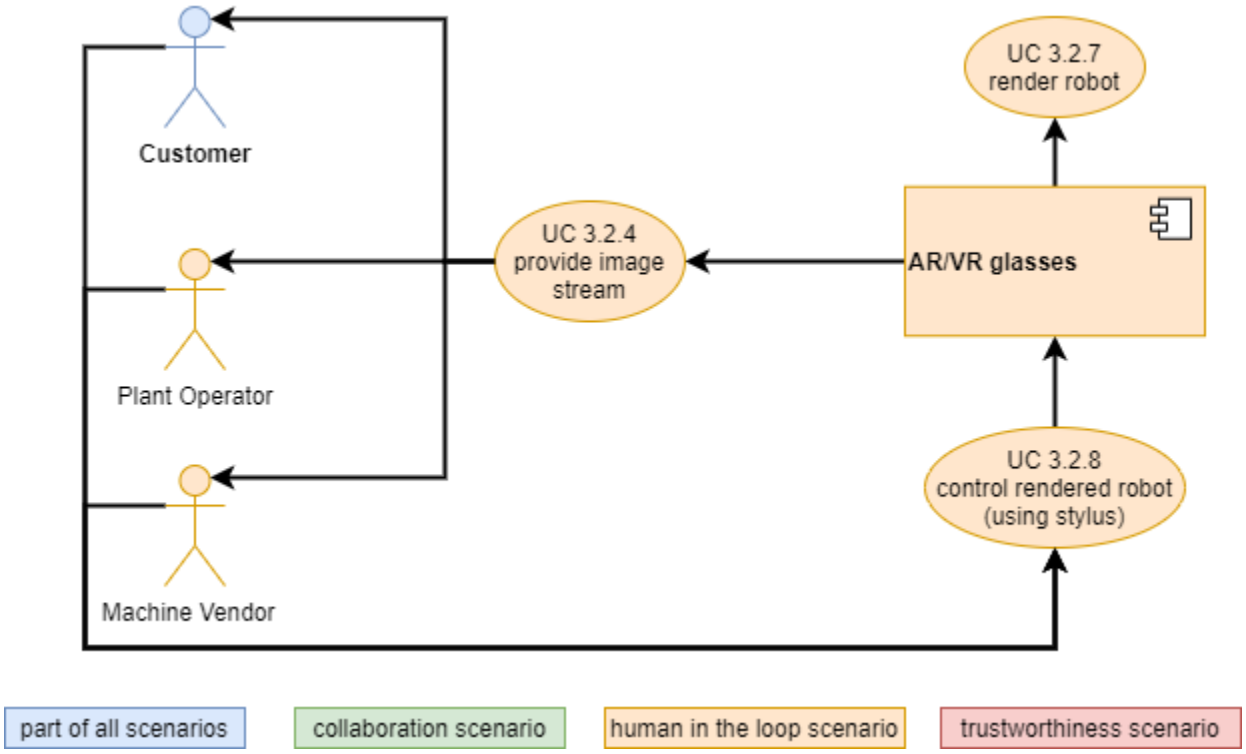
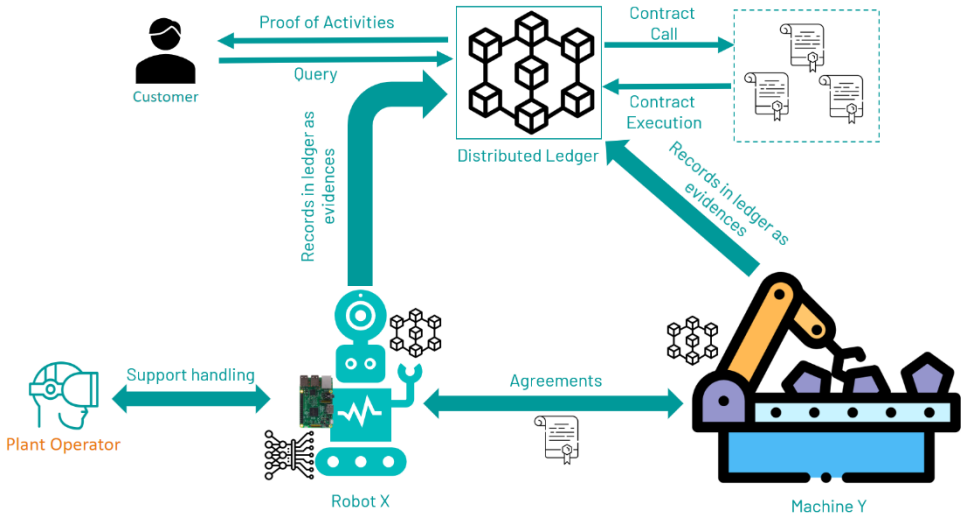
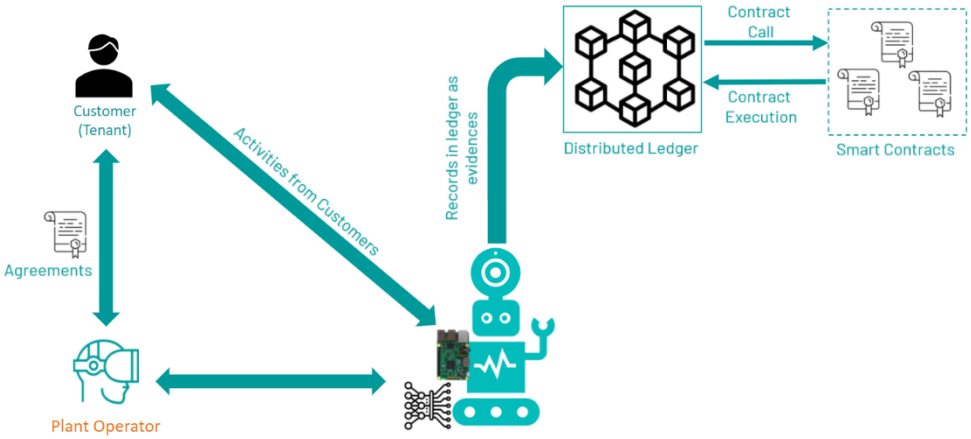
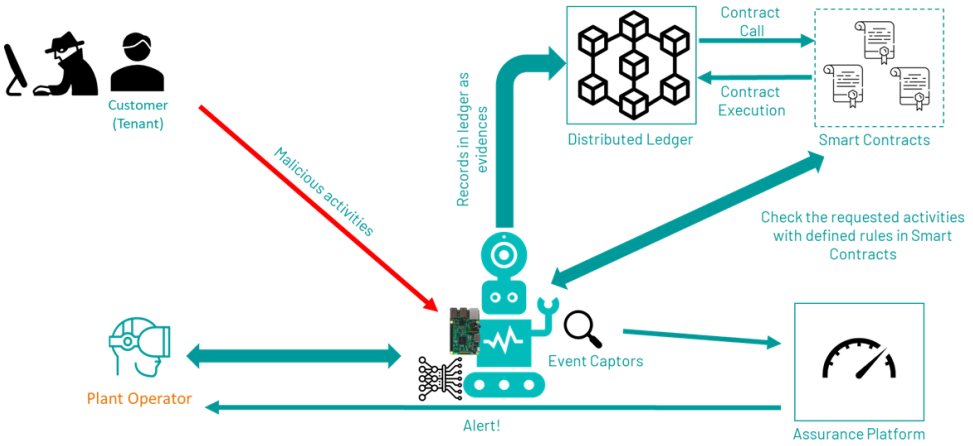
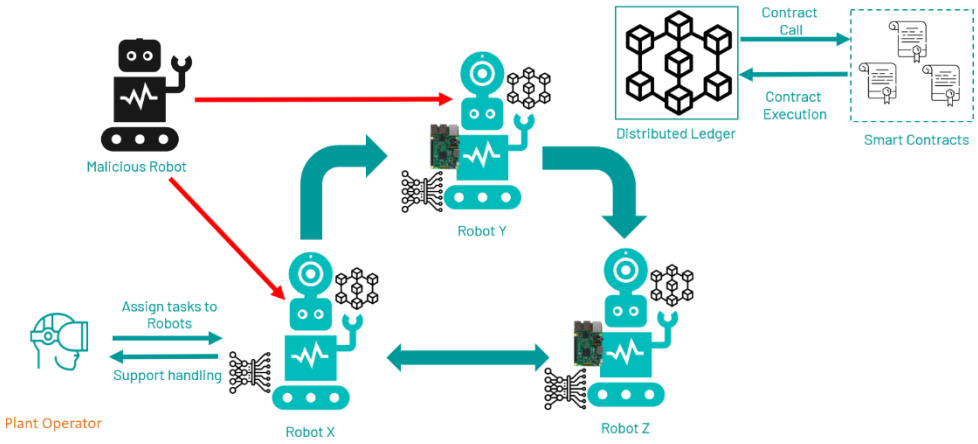


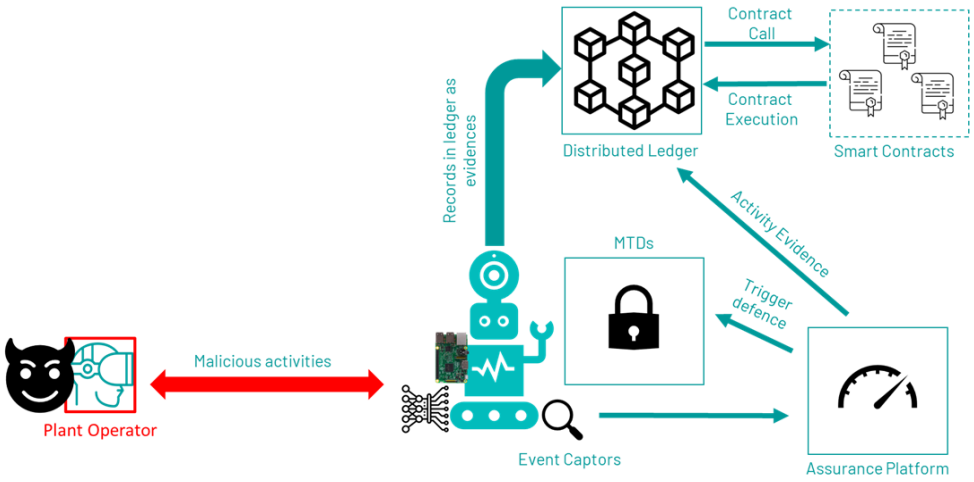
Figure 18: use case diagram human-in-the-loop with rendered robot

2.3.5.3 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 three elements: (1) 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; (2) 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; (3) 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).

Key Scenes	**Key Scene 3.1**, see Figure 19: A production plan computed by the Reactive Planner is used by a machine for producing a product, which is currently located in the plant but it is owned by a third-party machine owner. In order to use the machine, a smart contract is arranged beforehand between the plant owner (represented by the Reactive Planner) and the machine owner. When the contract is arranged, the Reactive Planner 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**, see Figure 19: 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, see Figure 20: A black hat acting as customer interacts with the plant with the goal of describing a special workpiece, which causes the robot to face issues placing it in a machine. This results in the robot asking the machine owner for help. When being asked for help, the black hat, now acting as machine owner, uses the camera on the robot and the possibility to move the camera to spy out technical details of competitors products within the plant. The event captor associated with robot "X" provides continuous monitoring of security, recognizes suspicious robot movements and reports to the Security Assurance Platform. The Security Assurance Platform immediately informs the plant operator, who cuts the control connection to the malicious customer. 
Potential Variation of the Scenario	**Variation Scene 1:** Reactive Planner assigns 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 above, the malicious activity could come from an employee of the plant operator, i.e., a realization of an insider threat. The process is similar to Key Scene 3 but involves malicious activity without involvement of a malicious client. In this case automated defences (through triggering of MTDs), along with recording of the relevant evidence in the ledger, counter the attack automatically. This automated defence is relevant in this case, as notification of the operator may not be desirable (broken trust with - now compromised - operator). 
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.
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; and (iii) the smart contract is implemented among partners to agree on common rules and contracts.
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 robots and machines
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

Figure 19 and Figure 20 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 D2.2.

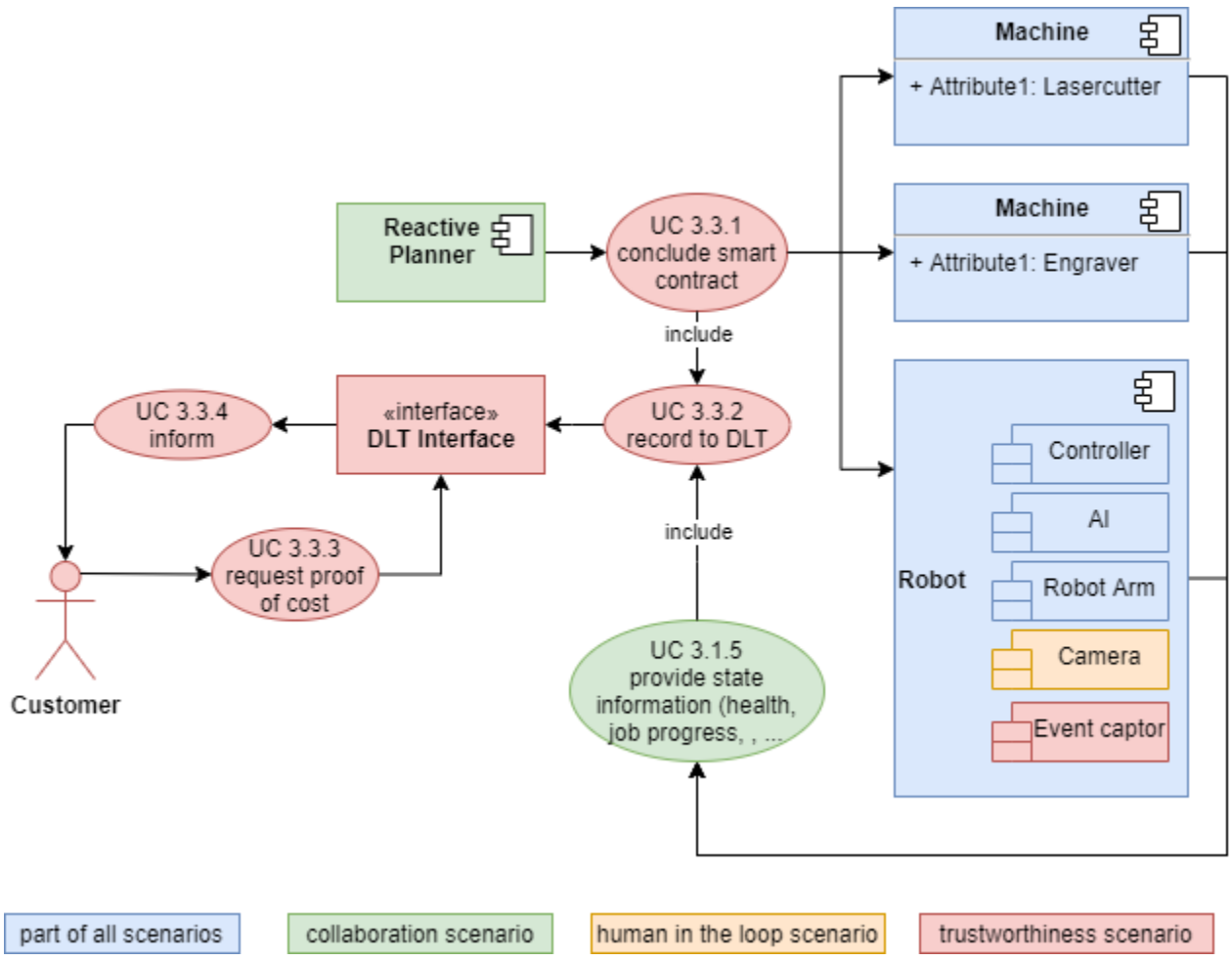


Figure 19: use case diagram trustworthiness - proof

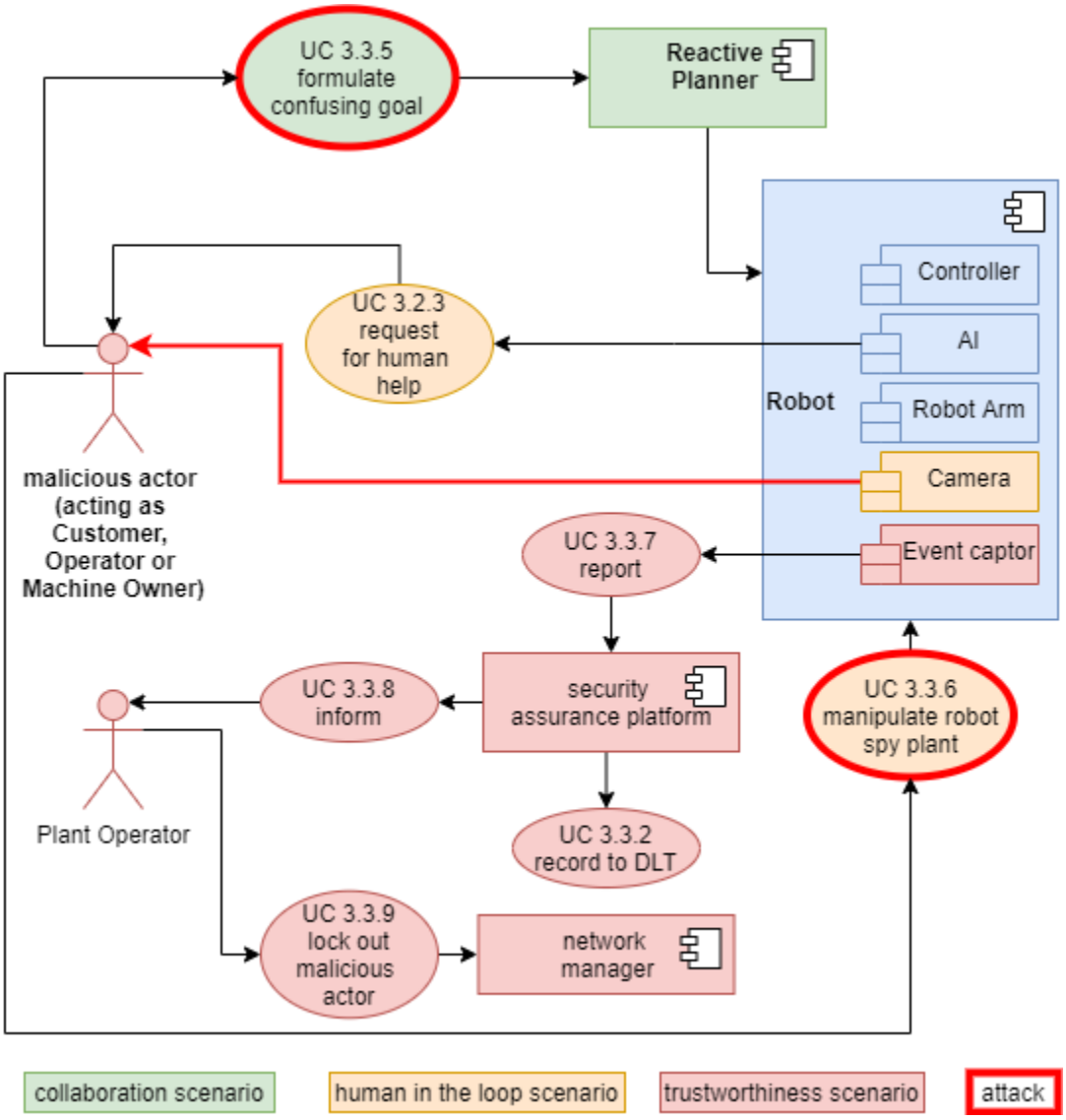


Figure 20: use case diagram trustworthiness - spy

3 OPEN CALLS DEFINITION

The two Open Calls will focus on attracting startups and SMEs to build applications, services and extensions on the IntellIoT technical framework within special 6-month pilots (for each open call) that will be aligned with IntellIoT's 3 use cases. The main objective of the Open Calls is testing the IntellIoT framework and components by integrating new, external components, i.e., software (e.g., AI tools) or hardware components (e.g., IoT devices).

The purpose of the 1st Open Call is primarily to enhance technological toolkit and/or use case coverage and refinement of the IntellIoT framework towards its 2nd cycle. These pilots will help to validate IntellIoT results and components in the 3 use cases.
The purpose of the 2nd Open Call is to further evaluate the final version of IntellIoT framework, as well as building a sustainable ecosystem in the existing or new application domains that carries on beyond the project.

3.1 Expectations for participating entities

Entities taking part in the 1st Open Call are expected to

- 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 end of the project lifetime,
- provide access to collected data for the consortium of IntellIoT,
- demonstrate and present the final outcomes (and plans on their exploitations),
- provide feedback to IntellIoT technologies as input for the 2nd cycle.

3.2 Contribution Ideas

With the Open Calls the use cases aim to widen the range of new and innovative IoT applications and devices of their specific IoT environments. To assure a consistent development of sustainable solutions throughout the use case implementations and upcoming activities in Open Call 1 and 2, clear integration points with the IntellIoT framework need to be described in the Open Call proposals and realized during their execution. Moreover, it is intended to further develop the use cases already specified by providing additional tools, services, applications or devices.

The below mentioned list of ideas shall give Open Call applicants an understanding of what could be contributed through their Open Call proposals. 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 CONTRIBUTION 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.
- **5G Infrastructure:** Software and hardware that is able to setup a prototype 5G private network. IntellIoT will have its own 5G infrastructure setup, however, to test interoperability on that level, a further 5G network testbed could be meaningfully included.

- **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).
- **Devices to support human-machine interaction:** Hardware (e.g., HMI devices such as AR gloves) and software that enables intuitive remote machine or vehicle interaction, for example to control a robot arm in the manufacturing use case or to control the tractor in the agricultural use case. The solution should consider the cooperation with the AR/VR solution from Holo-Light. This could also involve the realization of simulation environments to train and validate the remote control of vehicles or machines.

3.2.2 CONTRIBUTION 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 Solution:** Hardware and software solutions for smart farming could be integrated with the IntellIoT framework (e.g., via the HyperMAS) to support the agriculture use case. Solutions could range for example from the integration of in-situ sensor networks or aerial imagery sensors to the analysis of such collected data to improve the efficiency of the farming.

3.2.3 CONTRIBUTION IDEAS FOR HEALTHCARE USE CASE

- **Next generation Medical AI devices:** Hardware (medical devices) and software (e.g., analytics) to integrate with the IntellIoT framework and support the healthcare use case through patient monitoring and guidance.
- **Data & analytics:** Access to data (e.g., historical and anonymized medical data or live data from sensors) as well as software (e.g., machine learning models that can be utilized to analyse the medical data).
- **Wearables:** Hardware (e.g., smart garments) and software to integrate them into the IntellIoT framework to provide data for support in the healthcare use case.

3.2.4 CONTRIBUTION IDEAS FOR MANUFACTURING USE CASE

- **Automated guided vehicle (AGV):** Hardware (e.g., an AGV platform) and software to integrate the AGV into the IntellIoT framework (e.g., through HyperMAS adaptation) and to coordinate with other machinery/robots (potentially the AGV could also carry a robot arm).
- **Localization / navigation in manufacturing IoT environment:** Hardware (e.g., indoor positioning system) and software to integrate with the IntellIoT framework. After integration, this contribution could for example provide accurate positioning information.
- **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 AND FUTURE WORK

The IntellIoT project has chosen a use-case based approach for the validation and demonstration of the developed framework and its underlying technologies. This deliverable introduced 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 for the domain is. Additionally, the document highlights the different actors or entities (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 deliverable identified the three pillars of the IntellIoT project, namely (1) collaborative IoT, (2) human-in-the-loop, and (3) trustworthiness. These three pillars cover the main research topics of the project and will be applied in the three use 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.

The above, as documented within this deliverable, are only the first iteration, reflecting the current status of the IntellIoT efforts. Nevertheless, the definitions provided in this deliverable will form the basis for the rest of the work in the project, especially in defining the functional, non-functional and technical requirements (to be specified within T2.2 and documented in D2.2) and the technology developments that will follow. During the work in technology development work packages (WP3 and WP4), these use case definitions will be regularly revisited and elaborated upon. Additionally, the input from the user workshops (Task 2.2) and the 1st open call will have major influence on these definitions. The final version of this deliverable (D2.4, which is due in M19) will describe these updates and will provide the final definition of the use cases and the latest Open Call developments.