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

IntellioT

Deliverable D2.2
Technology Analysis & Requirements Specification (first version)

Deliverable release date	31/05/2021
Authors	1. Siemens: Andreas Zirkler, Andreas Ziller, Arne Broering, Vivek Kulkarni 2. EURECOM: Jerome Harri 3. AAU: Beatriz Soret, Lam Nguyen 4. UOULU: Sumudu Samarakoon 5. TTC: Martjin Rocker, Gerald Fritz 6. TSI: Andreas Brokalakis, Vassilis Amourgianos, Charalampos Savvakos 7. Philips: Nancy Irisarri Mendez, Anca Bucur 8. SANL: Konstantinos Fysarakis, Ioannis Vezakis 9. HSG: Simon Mayer 10. HOLO: Carina Pamminger 11. AVL: Holger Burkhardt, Wolfgang Hollerweger 12. STARTUPC: Dominik Krabbe 13. PAGNI: Maria Marketou, Ioannis Anastasiou
Editor	Andreas Brokalakis (TSI)
Reviewer	Martijn Rooker (TTC), Nancy Irissari Mendez (Philips), Beatriz Soret (AAU)
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	5G New Radio
AAA	Authentication, Authorization, and Accounting
AAMAS	Autonomous Agents and MultiAgent Systems
AR	Augmented Reality
CAGR	Compound Annual Growth Rate
D2D	Device to Device
DLT	Distributed Ledger Technology
DRL	Deep Reinforcement Learning
ECG	Electrocardiogram
ETSI	European Telecommunications Standards Institute
FL	Federated Learning
GUI	Graphical User Interface
HIL	Human In the Loop
HMD	Head-Mounted Display
IAKM	Infrastructure Assisted Knowledge Management
ICT	Information and Communication Technology
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IPFS	InterPlanetary File System
KPI	Key Performance Indicator
LL-MEC	Low Latency Multi-access Edge Computing
MAS	Multi-Agent System
MEC	Multi-access Edge Computing
ML	Machine Learning
mMTC	massive Machine-Type Communication
MTD	Moving Target Defense
NB-IoT	Narrow Band IoT
NFV	Network Function Virtualization

NG IoT	Next Generation Internet of Things
OEM	Original Equipment Manufacturer
RAN	Radio Access Network
RL	Reinforcement Learning
RPC	Remote Procedure Call
RPM	Remote Patient Monitoring
SGD	Stochastic Gradient Decent
TSN	Time Sensitive Networking
URLLC	Ultra Reliable Low Latency Communication
WoT	Web of Things

1. INTRODUCTION

This deliverable summarizes the work that has been carried out as part of Task 2.2. This is intended to be a two-version process. The current deliverable is the first version aiming to cover initial research and preliminary requirements carried out during the first eight months of the project. A re-iteration of the deliverable (second version) is planned for the second half of the project and will include the final analysis and specifications, ingesting results from the evaluation of the first version of the IntellIoT framework.

Deliverable D2.2 has two distinct parts. The first one aims to provide insights on the business value drivers for NG-IoT technologies and an analysis of the state-of-the-art solutions for said systems. Providing this market and technology-oriented analysis, IntellIoT's vision and positioning is revealed and the connection between the three chosen use cases, their requirements and measurements of success of the project effort (evaluation) can be formed.

It should be noted that the state-of-the-art technology analysis presented in the original research carried out during the preparation of the proposal of IntellIoT forms the basis of the state-of-the-art update provided herein. This is further extended to provide insights to the most recent developments since the proposal-writing phase.

The second part of the deliverable is based on the initial outcomes of Task 2.1 as described in Deliverable D2.1 and includes the specifications of the requirements of the three use cases that will be developed as part of the project. Deliverable D2.1 provides the definitions of each use case and this deliverable unfolds those definitions in order to produce a set of requirements that the framework developed within Work packages 3 and 4 (as well as integration and implementation efforts within Work package 5) should cover. Two main sets of requirements are defined within the scope of this work: functional and non-functional requirements. These cover the requirements from a user perspective and that is why they are specified in tight connection with the use cases. A third set of requirements covering internal functionalities and technicalities of the framework and its components is going to be specified in Deliverable D2.3.

Besides the requirements, this deliverable defines two sets of baseline performance measures or Key Performance Indicators (KPIs). These KPIs are going to form the basis of evaluation criteria for the success of the project and cover two main aspects: project objectives and project impact. The KPIs are specified in accordance with the project objectives and expected impact, as defined in the IntellIoT's Description of Action.

2. BUSINESS VALUE DRIVERS FOR NGIOT

In this chapter, we review different business drivers and technology enablers for creating value in NGIoT ecosystems (i.e., plans of the way in which an organisation can create, capture and deliver business value in an NGIoT ecosystem, which includes the End-users, customers, value chains and revenue models) and the role that technology plays in this context. Our review considers also different types of stakeholders in the NGIoT ecosystem as well as regulatory aspects (e.g., related to Trustworthiness, including privacy and security) that may affect the operation of the NGIoT ecosystem, application and the creation of value.

The value of NGIoT lies in connecting the real world with the virtual world of data. Digitalisation technologies offer new business models. In the Internet of Things, billions of things have addresses and are linked to the Internet. They can transmit data to the Edge device for processing and be managed and controlled via applications. This scenario will become a reality thanks to increasingly miniaturized computers, affordable sensors and actuators, tactile networking, and the increasing availability of "intelligent" IoT devices in many areas. With well-designed IoT solutions, one can harness data from already owned machines and physical infrastructure to find transformative insights across the entire business. And the users can immediately develop, deploy and run digital services, create own applications, or even new business models. In the following, we examine the above factors in more detail with the focus on the three sectors showcased in IntellIoT: agriculture, healthcare and manufacturing.

2.1. Customer needs and pain-relieving products & services

Value propositions describe the benefits that the end customers expect from NGIoT products. From the opposite side, they also quantify the expected return of investment for NGIoT technology providers. The business model demonstrates how to bring that value to market. Therefore, it is vital to combine both aspects for a successful product.

In the *agriculture sector*, the agricultural machine manufacturing industry in the EU accounts for a total annual revenue of €42.9 billion with the major share in tractor manufacturing. It is furthermore a major driver of EU exports, as EU tractor manufacturers export one third of the produced volume of 187,000 tractors to non-EU member states. Consequently, this industry is dependent on integration of novel technologies for sustaining its competitiveness internationally. However, declining revenue figures[1] during the past years have challenged the industry. Thus, there is a strong requirement to further boost innovation to gain global market share via increasing productivity, sustainability and efficiency. In this regard, semi-autonomous behaviour of electrical agricultural vehicles and associated technology drivers provide great potential. Farm owners, as customers, can profit from novel farming-as-a-service models with a pay-per-use revenue stream. Its main value pro-po--sition is shar-ing- or renting of semi-autonomous agri-cul-tural equipment and the service to provide farming activities such as land preparation or crop harvesting. This can make the cost structure of such services more attractive, as a remote controller can be potentially in charge of a fleet of vehicles.

In the *healthcare sector*, the European eHealth market is rapidly growing and is projected to reach €7 billion by 2023[2]. Chronic heart diseases, diabetes, and chronic respiratory diseases are the leading cause of mortality and morbidity in the world. Chronic care management accounts for 75% of the healthcare costs. Continuous and self-managed health monitoring and interventions have been shown to reduce the risk for chronic illnesses by 60-80% and reduce the chronic care costs. Thus, it reduces the readmissions and prevents avoidable hospitalizations. This is critical given the EU-wide increase of healthcare costs due to the aging society. The increase in prevalence of chronic conditions places an enormous financial burden on the caregivers. Multi Parameter Monitors Segment to grow with the highest CAGR of 38.6% during 2019-30. Remote Patient Monitoring (RPM) Market is segmented by type as Heart Monitors, Breath

[1] https://www.cema-agri.org/images/publications/brochures/2019_CEMA_report_priorities_key_figures_web.pdf
[2] https://www.marketdataforecast.com/market-reports/e-Health-market

Monitors, Hematology Monitors, Multi-parameter Monitors, and Other. The Heart Monitor segment is estimated to lead the market with a share of over 80.0% of Remote Patience monitoring market in 2018 and this trend is expected to continue during the forecast period. There is an urge for IoT applications to look beyond. The vision is the connection of a variety of different wearable devices and the addition of intelligence, autonomy, and security to the IoT edge node, close to the patients, and preserving the privacy of the health data. For semi-autonomous health advise to the remote patients, the basic enabler is the use of distributed AI over IoT devices, instead of uploading data to a cloud. Even AI model training needs to be done locally through privacy- and resource-aware federated learning. This opens greater potential for novel healthcare services that enable outside/home care, with a value proposition in increased quality of patients' lives and reduction of cost of care.

In the *manufacturing sector*, which accounts for 16% of Europe's GDP, ICT-based solutions applied across the manufacturing value chain help to make processes more efficient, leading to Smart Manufacturing bringing information technology closer to the manufacturing centers to help them boost their productivity, maximize their resources, and help them innovate products. Production process needs to be more agile in future to quickly adjust to market demands with higher degree of utilization of installed production capacity, improvement in transparency and price discovery. There is a need to integrate ICT innovations into factories to make transform them into more digital, smart, and virtually controlled. New product models need to be produced in shorter cycles and end-users want individualized products (lot-size one production). There is a huge potential for manufacturing-as-a-service aiming at sharing (parts of) production facilities, e.g., with a pay-per-use revenue stream. Such plants need to be flexible to allow production of various goods. Providing flexible NGIoT infrastructures, an edge-as-a-service business model (like the established cloud infrastructure-as-a-service) will gain traction with business value proposition. Intelligent combination of both wired and wireless connectivity together with dynamic infrastructure management enable the creation of flexible IoT environments required to execute those business models.

Revenue models are an important aspect for the successful development of NGIoT ecosystems. Typically, there are three revenue streams: (i) fixed one-time transaction; (ii) One-time or ongoing service, and; (iii) outcome based. Operators seeking to attract ecosystem partners need to define the right model for generating and distributing revenue. What is needed is business models encouraging partners to join the ecosystem, reducing the risks for innovation partners and be consistent with each partner's business model. Some partners are attracted by a revenue-sharing model, while others prefer a licensing model or a fixed royalty-based model. This means that operators need to support multiple revenue and partnership models, which in turn requires new decision-making and management systems.

Table 1. End-users for the Agriculture, Healthcare and Manufacturing sectors.lists the end-users for each one of the three targeted sectors: Agriculture, Healthcare and Manufacturing.

Table 1. End-users for the Agriculture, Healthcare and Manufacturing sectors.

Agriculture	Healthcare	Manufacturing
1. OEMs for agricultural vehicles and mobile machinery 2. Farmers 3. System integrators 4. Farming-as-a-Service companies 5. Farmer associations 6. Governmental Entities	1. Clinicians and patients 2. Personalized care consumer market 3. New marketplace for AI algorithms and devices 4. Governments	1. Plant owners and operators 2. System integrators 3. Machine Builders 4. Automation component vendors 5. Industrial workers 6. End user associations

2.2. Business value drivers for NGIoT

Below are the generic business value drivers identified for NGIoT systems:

- **Cost reduction**: Monitoring of IoT devices regarding variety of data such as usage, uptime etc. enable equipment owners to take immediate action if something goes wrong. Instead of scheduled maintenance, NGIoT brings no more unexpected equipment downtime with predictive maintenance.
- **Usability**: NGIoT systems need to be simple to use and rich in user experience. To achieve such goals, they need to inspire faith and trust in the semi-autonomous operations that they provide.
- **Ease in installation, integration, and maintenance**: NGIoT systems provide ease in installation, both in greenfield and brownfield systems; and their capabilities are immediately known in the system via semantic integration.
- **Quality control and reproducibility**: NGIoT systems help in quality control of the data they sense and take immediate action (e.g., calibration) if necessary. Reproducibility of the data is an important aspect of NGIoT for end-user trust.
- **Asset utilization**: NGIoT system bring transparency by logging their own utilization and offering their services to other stakeholders in the system for optimal asset utilization.
- **Data quality and automated learning**: NGIoT systems brings quality data for AI/ML algorithms to act in a correct and expected way in local or distributed learning setup.
- **Augmented reality and digital twin**: NGIoT support simulating future behaviour via digital twin and together with augmented reality can bring value added services like training, worker safety and remote maintenance.
- **Scalability**: NGIoT systems provide scalability to support large number of field devices with their local edge computing capacities.
- **Reliability**: NGIoT systems are reliable enough for fail-over scenarios of their important system components.
- **Interoperability**: NGIoT system are interoperable with other systems in both greenfield and brownfield installations to avoid vendor lock-in scenario.
- **Data ownership**: NGIoT should bring clarity on the data ownership and data domains from the end-user perspective.
- **Security and safety**: NGIoT add further value when those systems are designed with security, privacy and trust by design. By deploying AI/ML and Robotics for semi-autonomous operation, NGIoT systems should focus on risk-based safety challenge associated with it to increase users' trust in the new, versatile generation of NGIoT products.

2.3. Business value drivers for IntellIoT's Use Cases

2.3.1 BUSINESS VALUE FROM AUTONOMOUS OPERATION OF AGRICULTURAL VEHICLES

The introduction of (semi-) autonomous operation of agricultural vehicles provides a major potential for farmers, but also for companies, like OEMs and technology providers. Autonomy in farming vehicles is likely to emerge as one of the most revolutionary aspects of the agricultural domain. The size of the market for autonomous farm equipment is set to grow from its current market value of $55 billion to over $180 billion by 2024, as reported in the latest study by Global

Market Insights, Inc.[3] Increasing labour shortage (also caused by the COVID pandemic) showed a shift towards more autonomy in the farming equipment, like e.g., autosteering, smart farming, etc.).

The uptake of technology for (semi-)autonomous operator of agricultural vehicles offers many possibilities for companies, not only for the large OEMs, but also for SMEs that are developing individual technologies, like sensors, actuators, but also Artificial Intelligence for the autonomous operation. The final goal of the autonomous operation is to remove the human operator from the cabin and have the operator control perform its task from its own offices, and possible only interacting with the system when the need arises (e.g., when the vehicle gets stuck in an unknown situation).

Many new technologies that are currently under heavy development can make a large impact on the agricultural domain and provide new business values for the domain. AI can add more autonomy to the vehicles, so that it can learn more about its environment and its task at hand, thus opening the market for new companies focusing on new AI technologies. For autonomous operation, collaboration and human in the loop, reliable and low-latency (wireless communication) is of vital importance. However, most agriculture fields are in rural or remote areas with limited/poor connectivity. This is where 5G comes into play and open another business perspective for telecom companies that did not find a business value in those areas before the arrival of NGIoT.

2.3.2 BUSINESS VALUE FROM REMOTE PATIENT MONITORING

As mentioned, chronic diseases are a significant social and financial burden and the main cause of morbidity and mortality world-wide. Remote patient monitoring 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. Furthermore, the overall solution developed in IntellIoT and demonstrated in the domain of cardiovascular diseases has applicability in the other Remote Patient Monitoring market segments. The infrastructure can be applied for the development and deployment of new algorithms, with customized apps and sensors.

According to the Philips Future Health Index[4], healthcare leaders are prioritizing investment in AI to optimize administrative tasks. Healthcare leaders also plan to expand these investments in AI three years from now to integrate diagnostics, predict outcomes, and for clinical decision support. Given their sentiment that patients are driving an increased demand for remote and at-home care, healthcare leaders estimate that a higher amount of routine care delivery will take place outside of the walls of a hospital or healthcare facility three years from now. The role of the home is expected to increase from 11% currently to 17% of total routine care delivery. This trend has been significantly accelerated in 2020 during the COVID-19 pandemic.

2.3.3 BUSINESS VALUE FROM MANUFACTURING-AS-A-SERVICE:

Even a minor bottleneck in a manufacturing process can result in a huge loss of resources. Manufacturing-as-a-service will empower flexible and individualized production using collaborative IoT based on AI. This solution will open new business opportunities by enabling shared manufacturing plants with multiple customers (external or internal) utilizing manufacturing machines as-a-service. This brings flexibility in the productions, enabling profitable production of small lot sizes, down to lot size one. It fosters better asset utilization, continuous quality control and provides semi-autonomous operation for repetitive tasks in manufacturing leading to deployment of human capital to do better jobs.

[3] https://marketersmedia.com/autonomous-farm-equipment-market-size-to-go-past-180-billion-dollar-mark-by-2024/88901140
[4] https://www.philips.com/a-w/about/news/future-health-index

Reliable, low-latency and high-rate wireless communication is required to make the flexible smart factory a reality. This opens new business opportunities for telecom operators that can provide private 5G network solutions.

3. TECHNOLOGY ANALYSIS

IntellIoT proposes the creation of *intelligent IoT environments* as an answer to the challenges of Next Generation IoT applications. As such, it considers the implementation of a framework that binds together heterogeneous devices of varying capabilities and constraints that can collaboratively execute semi-autonomous IoT applications. Its target is to advance the adoption of Artificial Intelligence in such applications while keeping the human-in-the-loop as an integral part of the system in order to guarantee safe and well-predictable operation on all occasions.

To achieve those ambitions, IntellIoT aims to build upon a number of key technical solutions and through the collective work carried out during the project to move beyond the state-of-the-art that is currently available. The next subsections present those key technologies and the current state-of-the-art in each one of them.

3.1. IoT Architectures and Interoperability

To enable the Internet of Things to reach its full potential, virtual services and physical devices need to be interoperable on the network and transport layers (i.e., connected to the Internet via TCP/IP), and we further need to guarantee that such Internet-enabled soft (virtual)- and hardware artifacts can discover, manage, and interact with one another on the application layer [1]. A first major step towards accomplishing this goal has been made through the Web of Things [2] where interactions between devices are based on the architecture of the World Wide Web, and its architectural principles. Through integration of physical devices and virtual services into a common application layer, the WoT (and other approaches, such as OneM2M) provide a higher degree of interoperability, but this by itself is still insufficient to empower devices and services to automatically and meaningfully interact with one another - that is, to reach semantic interoperability. Today, this challenge is typically circumvented through a platform approach: so-called IoT Platforms (by Amazon, IBM, Samsung, Siemens, and others) accomplish interoperability within their respective platform environment but constitute semantically walled gardens when viewed from the outside.

Crucially, however, interoperability on the semantic level and across such platforms is a central requirement in the future evolution of the Web. This is because the reliance of Web-based systems on developers to manually integrate Web APIs across service providers and to program explicitly all system behaviour is, today, becoming a pressing bottleneck [3]. The explosive growth in the number of Web APIs, particularly in the context of the WoT, together with the dynamic nature of cyber-physical systems in pervasive computing environments, requires components to be deployed and to evolve independently from one another. Thus, the use of static Web APIs that are manually integrated by developers becomes impractical. This motivates the need for dynamic Web APIs that can evolve over time and for software clients that can autonomously discover, consume, and cope with the evolution of such APIs - using hypermedia not only as a general linking mechanism, but furthermore to drive the evolution of application state (this principle is termed HATEOAS). Based on efforts such as the W3C WoT Thing Description (WoT TD) and initiatives such as Hydra to create declarative specifications of interactions on the Web, researchers and practitioners are already looking for new means to use hypermedia for designing evolvable Web APIs and general-purpose clients (e.g., [4]), and for new paradigms and languages for programming more flexible Web systems (e.g., [5, 6, 7, 8, 9, 10]).

This declarative specification and enactment of interactions between autonomous agents has been studied to large extent in research on Multi-agent Systems (MAS). However, these efforts are at the moment not coordinated with the architecture of the Web and, thus, not aligned with the Internet of Things' de-facto application layer [10]. Early attempts to integrate MAS and the Web would often just juxtapose the two [10], e.g., by using Web standards as message formalisms in MAS [11]. When service-oriented computing took off in the early 2000s, the AAMAS community turned to integrating MAS and Web services to engineer large-scale MAS [10]. These approaches included the tunnelling of RPC-like method invocations through HTTP using SOAP and the WS-* standards, and generally relied on RPC-like architectures. This led to FIPA (Foundation of Intelligent Physical Agents) proposing a specification for using HTTP as a transport protocol for messages exchanged among agents [12], which was implemented by several MAS platforms [10] - many researchers in the AAMAS community still view the Web merely as a transport layer for messages in MAS, thereby remaining in juxtaposition with core principles of the Web architecture as it is conceived of today [10].

Regarding the engineering of world-wide systems, however, they have shortcomings as compared to REST-style, resource-oriented architectures [13]. This is true for instance regarding world-wide scalability and openness. Regarding scalability, intermediaries (e.g., caches) have played a central role but can hardly be used by RPC-style systems. Regarding openness, HATEOAS enables new and (design-time) unanticipated uses of services and devices and supports the serendipitous use of resources [10] especially when combined with the Linked Data initiative [14].

Web services have thus evolved drastically over the past decade and it is widely accepted that using the Web merely as a transport layer entails important drawbacks in open and long-lived Web systems [10]. It is therefore highly relevant to integrate the research done in the Web community over the past decade with current research in MAS with so-called Hypermedia-based Multi-agent Systems (or HyperMAS, [10]).

Progress beyond the state of the art

Within IntellIoT, we aim to support this development, and thereby to inherit these favourable architectural properties (e.g., scalability, loose coupling) across the project's technologies and use cases, where we aim to prove that our approach enables decentralized systems that evolve at runtime (e.g., to adapt to dynamic environments) and can be rapidly reconfigured by engineers [15]. Since there is no generally accepted way of measuring and quantifying the flexibility and interoperability of a system [16], we furthermore aim to establish a benchmark that can be used to compare approaches and systems that claim these properties.

3.2. Edge Computing

IoT applications are moving from the cloud into the edge, closer to the devices producing and consuming data. I.e., applications move from the scalable and homogeneous cloud environment into a heterogeneous IoT/edge infrastructure. Previous work introduced concepts such as micro data centres [17, 18], cloudlets [19], fog computing [20], or Multi-access Edge Computing (MEC) [21] where computing resources are part of a 5G network. We define "edge" as any computing and network resources along the path between data sources and cloud datacentres so that computing happens in closer proximity of the data sources [22]. For example, in a manufacturing plant or a hospital the edge can consist of heterogeneous networked computing devices including dedicated edge devices [23], IoT devices, or even network gateways. Utilizing edge computing has the potential to address the concerns of response time requirement, battery life constraints, bandwidth cost saving, or safety and privacy. Previous work showed (for example in the case of face recognition [24] or cognitive assistance [25]) that application response time could be reduced by 60-80 % when moving computations from cloud to edge. In context of *IntellIoT*'s use cases, a key challenge for the computation infrastructure is to decide on which computing resource to handle a specific workload of an IoT application (e.g., execute an AI algorithm). There are multiple existing allocation strategies, e.g., [26, 27, 28, 29], which optimize different performance metrics, e.g., response time, bandwidth, availability, or energy consumption.

With the advent of high-speed access technologies as 5G, edge computing becomes more and more crucial. Low latency requires proximity to the data producers and high data rates advise data preprocessing at the edge in order not to overload backend infrastructure. ETSI introduces with multi-access edge computing a standard [30], which is the link between the wireless communication and the edge computing world. It defines an application enablement framework, which allows the registration, notification and discovery of applications as well as the authorization and authentication within the MEC system. Accordingly, a web API is specified, which exposes network context information for edge apps. Edge apps can discover network capabilities and manage traffic, DNS and mobility. Furthermore, own services can be registered, so that they can be discovered by other apps as well.

The MEC exploits several enablers within the 5G System for local routing and traffic steering [31], [32]. The 5G Core System is able to select traffic to be routed to the application. Traffic steering is supported by uplink classifiers matching steered traffic. Other enablers are used for, e.g., session and service continuity in mobility scenarios.

Managed MEC services are planned as commercial offerings by various telco providers, typically in partnership with established cloud providers [33]. A free implementation for MEC is available from Mosaic5G [34]. Mosaic5G is a non-profit initiative for open-source software development to realize 5G systems. Among others, they offer LL-MEC as a low-latency computing platform with mobile network core controller.

Progress beyond the state of the art:

The computation side of the infrastructure will be innovated by developing components for advanced, dynamic resource management (T4.1), which can be flexibly applied in various private edge environments of the 3 *IntellIoT* use cases. This includes functionalities for private MEC integration within a 5G network to enable plug & play Cellular IoT services to the 5G network architecture. Thereby, a key component will be the optimized allocation of workload to computing resources (i.e., mapping of HyperMAS artifacts of an IoT application to devices). Building up on prior work [35], we will develop a flexible algorithmic framework (adjustable to different optimality criteria) based on integer linear programming to calculate the allocations at runtime and able to dynamically adjust to changes of the network. As the response time of an application is not only determined by computation time, but also by network delay, we will develop mechanisms to transmit high-level application requirements [36] to the network management in order to adapt to the (executed/planned) applications, i.e., establishing *closed-loop* infrastructure management.

3.3. Networking Infrastructure Towards Tactile IoT

While IoT/edge devices can provide the computation side of the infrastructure, the communication side is driven by novel networking technology. Current research is mostly focused on 5G, which has introduced major radio access network (RAN) innovation with the 5G New Radio (NR) as a redesign of the radio access toward radically new capabilities, such as Ultra-Reliable Low Latency Communications (URLLC), massive Machine-type Communication (mMTC), and enhanced Mobile Broadband (eMBB) [37, 38, 39]. Network Function Virtualizations (NFV) [40] and native support for end-2-end network slicing capabilities have been introduced in 5G. Also, extensions of 5G NR towards private networks and Industrial IoT have been introduced: narrow-band IoT (NB-IoT) [41] has been integrated and targets energy efficient operations for massive sensor communications. Further, 5G NR in unlicensed bands (NR-U) [42] enables 5G networks to be operated without an actual network operator. The 5G eV2X [43] is a complete redesign of the LTE V2X [44] for cooperative automated mobility and robotics. Together, 5G reaches unprecedented ubiquitous communication capabilities required by IoT verticals seeking URLLC, sensory exchanges with Cellular IoT, or 'sidelink' communications between robots and humans with eV2X as realization of D2D [45].

The support of tactile IoT with 5G technologies relies on the support of URLLC traffic and its promise of a reliability of "5 nines" with a maximum latency below 1 ms. This value is justified by studies on Quality of Control (QoC) [46], which show that even such a small delay can be perceptible as a difference in the perceived hand's position in high-precision applications (for example Augmented Reality (AR) aided surgery [47]). However, most applications can tolerate higher latencies and a number of lost packets with negligible loss of performance [48]. A recent survey [49] proposed a hierarchy of desirable properties: while full QoC requires millisecond latency, systems with latency in the tens of milliseconds can appear transparent to humans engaged in less critical and high-precision tasks, and even delays of hundreds of milliseconds are tolerable in some cases. A model of haptic system transparency to losses and delay using control theory is presented in [50]. Interestingly, delay is perceived more in stiff contact, and a certain delay can only ensure smooth operation below a maximum virtual environment stiffness. It is also possible to adaptively change the perceived responsiveness of the environment to adapt to high latency and maintain transparency [51], although this has a performance cost. Packet loss has a small but linear effect on perception of simultaneity between haptic and visual events [52]. However, a high packet loss can result in annoying artifacts and "jumps" in the user perception, as the packet loss degrades the receiver system's tracking capabilities [53]. The negative impact of loss highlights another critical issue: while UDP transmission of haptic packets provides no delivery guarantees, and losses can be arbitrarily high (as well as time-correlated), TCP can often cause long delays while waiting for retransmission. The development of appropriate codec to reduce the throughput of haptic signals [54] is another active area of research. Two useful surveys on the subject, which cover topics from the required communication architecture to a taxonomy of Tactile Internet applications in various contexts, can be found in [49]- [55].

Progress beyond the state of the art

The communication side of the infrastructure will be leveraging 5G networking for IoT [56, 57]. Thereby, *IntellIoT* will progress beyond the state-of-art towards the following directions: tactile IoT support and industrial IoT support.

Concerning the former, the first goal is to investigate the timing relations and the interplay of the different traffic flows involved in tactile applications specifically in combination with AR/VR, where audio-visual and data traffic co-exist with real-time transmission of haptic information (i.e., touch, actuation, motion, etc.). Although 5G took the first step with the definition of URLLC, this represents a simple one-way requirement that cannot satisfy the broad range of 5G real-time and control systems and tactile applications, as it was explained before. Besides the latency/reliability requirement, IntellIoT will consider: (1) the synchronization of outputs (e.g., in mixed systems with visual and tactile feedback, the image needs to be presented approximately 50 ms before the haptic feedback for the users to perceive the two as simultaneous [52]); (2) the contribution of the computation to the latency budget and its interplay with the communication [58]; (3) the timeliness requirements of the video-control-haptic loop, captured for example in the Age of Information metric and (4) the correlations in the traffic and dynamicity of future intelligent edge environments, by adopting a contextual and data-driven approach to the network configuration. The result of this research will be the design of a steer-/control-based communication framework to support tactile Internet.

The tactile traffic must co-exist with the rest of traffic of intelligent IoT environments, e.g., sensory data and AI models exchange among nodes. Some of these traffic flows have also strict latency/reliability/massiveness requirements. The interplay of different technologies, such as NR and Cellular IoT communications is a natural candidate for increased reliability/latency requirements, and especially challenging in terms of allocation decisions in the *IntellIoT* use cases, with a huge traffic heterogeneity. The provided solutions will enable efficient spectrum usage and joint URLLC control [59, 60, 61] in downlink, with massive sensory feedback on the uplink, targeting 1ms downlink, 10ms uplink with 99.99% availability.

Towards Industrial IoT, in order to support URLLC towards Time-Sensitive Networking (TSN) for 5G Industrial IoT [62], 5G mmWave radio providing fiber data speed, real-time reactivity and massive sensorics capacity [63, 64], as well as support for IEEE TSN will be investigated. Further, toward distributed networking support, functions for ad-hoc scheduling capabilities for enhanced device-to-device (D2D) communication will be finalized soon [65]. Yet no specific scheduler has been designed, hence, *IntellIoT* will develop a Wireless TSN-grade D2D scheduler providing deterministic QoS for decentralized computing in IoT context. Finally, we will enhance relaying support [66] to improve wireless coverage, which is typically challenging in indoor facilities (e.g., factories or hospitals), and provide energy efficient IoT communications for decentralized networking.

3.4. Distributed AI and the Human-in-the-Loop

The high-stake IoT applications of IntellIoT (including autonomous tractors, robot arms, AR/VR, or drones) require a novel paradigm change from classic ML calling for distributed, low-latency and reliable ML at the wireless network edge [67]. The key benefits of distributed ML at the edge are reduced latency and reduced cost of sharing training data, improved privacy, and higher inference accuracy due to the ability of training over data including privacy-sensitive information. Towards this goal, server-assisted [68] and peer-to-peer [69, 70] distributed learning and optimization techniques are investigated in the existing literature. Federated learning (FL) was proposed as a decentralized learning technique where privacy sensitive training data is distributed (possibly unevenly) across learning agents, instead of being centralized [68, 67]. FL allows each agent to compute a set of local learning parameters from the available training data (e.g., local model or local function's gradient with respect to a global model). Instead of sharing the training data, agents share their locally computed parameters with a central entity that, in turn, computes a global model that is sent back to the agents. Since models/gradients are much more compact than training data, FL can reduce the communication latencies during ML training process. Except a few works such as [71, 72, 73, 74], the vast majority of the existing literature assumes ideal client-server communication conditions, overlooking channel dynamics and uncertainties. In [73], authors study the impact of conventional scheduling policies (e.g., random, round robin, and proportional fair) on the accuracy of FL over wireless networks without deriving the optimal scheduling policy. The works of [71, 72, 74] propose various client scheduling and resource allocation methods to reduce either the communication overhead, the computational burden, or the loss of accuracy during the model training. In addition to the client-server communication aspects, FL has been used for various applications [75, 76, 77] and has been combined with different technologies [78, 79, 80, 81]. Similar to many other ML training methods, FL utilizes stochastic gradient decent (SGD) technique within agents for local training. In the existing literature, a variety

of SGD techniques such as centralized parallel SGD, local SGD, elastic SGD, entropy SGD, and stochastic variance reduced gradient can be found. These techniques have different requirements in terms of local computation as well as global communication iterations, which influence the convergence, accuracy, and robustness of the trained model. However, the impact of different choices of SGD techniques in FL, specifically in the agriculture, industrial, and healthcare use cases, in terms of the availability of local computing power and communication resources for model sharing (in addition to privacy preservation) is an untapped research area highly relevant for the Next Generation IoT. To further reduce communication overhead, model algorithms that consider quantization before transmission were proposed for both parameter-based and fully decentralized FL [82], [83]. Therefore, it is essential to analyse the effect of such communication cost reduction on the next generation IoT.

The learning process involving discovery and interaction in the reinforcement learning (RL) is one of the key benefits over supervised and unsupervised learning methods [84]. Here, each action is associated with a return, and the agent takes an action that maximizes its predicted cumulative return. However, the larger state dimensions requiring more computation may degrade the performance, known as *curse of dimensionality*. With the recent advancements in neural network-based ML, the branch of deep RL (DRL) is developed by addressing the above issue. The model-free, value/policy-based, and actor-critic RL within DRL exhibit efficient and accurate decision-making capabilities over the classical RL [85, 86]. The wide array of applications based on RL and DRL are seen in the existing literature [87, 88, 89, 90, 91]. Yet the aspects of computation-communication limitations and the privacy in distributed multi-agent RL need to be well investigated.

The involvement of the human expert in data collection, training, testing, and validation to achieve high accuracy and robustness of the ML systems is the fundamental philosophy behind the human-in-the-loop for ML. The conventional approach is to use the human expert to detect and correct the flaws on the ML systems by manipulating data and training process [92]. The improvements therein require quick feedbacks, continuous monitoring, utilizing intermediate result utilization and analysis of the impacts due to the changes. With distributed AI techniques, the interaction between the agents and the human expert needs to consider the time sensitivity, learning procedure and ability to control and train remotely in the scalable systems. Hence, it is mandatory to investigate various transfer learning methods (imitation, knowledge distillation) [93] as well as optimizers (Tabu Search, genetic algorithms, simulated annealing and ant colony optimization) [94].

Progress beyond the state of the art

Within the scope of *IntelIIoT* project, the distributed ML focusing on FL and RL is mainly investigated from the viewpoints of project's use cases: agriculture, healthcare, and manufacturing. In this regard, scalable ML techniques will be developed with the application-specific target accuracies and worst-case training latencies under the tolerable number of failures (reliability and robustness guarantee). For training and inference accuracy and reliability, server-client/human-machine communication and computation limitations have a significant impact. Therefore, the proposed ML solutions in the *IntelIIoT* project will be accounting for the wireless resources availability, on-device energy, storage and computing restrictions, human-machine/machine-machine interactions as well as the mobility and dynamics of the system (T3.2). In addition, control aspects are crucial in the IoT applications analysed in *IntelIIoT*. Hence, studying the control stability (plant, string, swarm- stabilities) of both single and multi-agent systems is mandatory within the project scope. In this view, investigating the co-design of ML, communication-computation and control will be the basis of *IntelIIoT* for developing the novel distributed AI solutions. Additionally, the codesign of communication-computation-control is beneficial from novel communication protocols allowing devices to exchange different messages to cooperatively and autonomously achieve their goals (T3.1). As highlighted above, the importance of human-in-the-loop for improved accuracy and reliability in ML will be adopted in *IntelIIoT* (T3.3). The fusion between transfer learning, optimization and FL/RL will be a key contribution of *IntelIIoT* towards the field of multi-agent distribution ML.

3.5. Security, Privacy and Trust by Design

The wide adoption of IoT technologies in a plethora of domains, often involving private-sensitive and critical applications, necessitates the provision of secure and trustworthy communications and interactions. This involves

considering security and trust early in the design phase, enabling the integration of mechanisms safeguarding crucial aspects such as the detection of physical tampering of the interacting devices, intrusion detection mechanisms that detect malicious entities and expel them from collaborative tasks, and AI-driven defence strategies that administer the overall system to counter ongoing attacks at runtime (e.g. [95, 96]).

While a preliminary line of defence may lie in the secure initialization of an IoT system by adding only trusted devices under specific protocols and procedures, this can eventually be compromised by online attacks that aim to hijack those devices. Except from the data breach in the device itself, an active attacker could also attack the rest of the connected devices and the network itself and manipulate the collaborative applications (e.g., perform denial-of-service attacks, disrupt distributed computational/communicational tasks, poison the data of a federated learning process, etc.) [97, 98].

For IoT systems that interact with the environment by receiving data from external sensors, another attack vector that can be realized is the emission of information by malicious systems masked as sensors. As such an evaluation model over the data received needs to be put in place in order to quantify the building of trust [99]. In this direction, intrusion detection functionality based on trust-based mechanisms can be adopted to mitigate pertinent risks. Such mechanisms monitor the behaviour of each participant and evaluate its legitimacy and cooperativeness, revealing selfish or malicious entities [100, 101].

In most current IoT applications, the system configurations are set once and are rarely changed. Such systems are considered as 'seating ducks' for the attackers, as they have the required time to examine them, analyse their weak points, and exploit their vulnerabilities. Therefore, apart from detecting and expelling misbehaving nodes, a next generation IoT network must also have the intelligence to protect itself proactively and respond to ongoing attacks automatically. Moving Target Defence (MTD) form a novel offensive defence strategy that promote this vision [102, 103]. AI security-sensitive procedures administrate the system (i.e., via smart agents). These processes are aware of the provided security level of the different system configurations. At normal operation, they periodically alter the network topology and/or configuration in order to harden its analysis by wily entities. When an attack is launched, they perform pre-defined defence strategies to counter it or at least mitigate its malicious effects. Possible drawbacks of this defence mechanism, such as the cost of movement between different modes of operation, have been identified [104] and several techniques have been proposed to address them by using dynamic schedulers to perform movement only when necessary or reduce the cost of the moving process [105], [106].

While automated assurance, continuous monitoring, evidence aggregation and evaluation have long been hot topics for both industry and academia, assurance evaluation of IoT systems is in its infancy. Most of the works are based on research carried out in the context of cyber-physical systems (e.g., [107, 108]) and some preliminary assurance approaches have emerged (e.g., [109, 110]). A number of works also exists on security and privacy assessment based on compliance (e.g., [111, 112, 113]) and audit (e.g., [114, 115]).

In parallel, research on security and privacy assurance models has followed the whole IT evolution initially providing approaches for software-based (e.g., [116]) and service-based (e.g., [117]) systems, consequently evolving to cover cloud (e.g., [118]) and IoT environments (e.g., [119]). These assurance and certification solutions typically employ testing and monitoring techniques to verify the behavior of the protected system [120].

The difficulties in defining new approaches to IoT assurance are due to the fact that the peculiarities of IoT applications make existing assurance approaches (e.g., for typical organisations or the cloud) unusable. Nevertheless, more recently, security assessment approaches started covering the peculiarities of IoT environments (e.g., [121, 108]). Of particular interest are security-focused approaches tailored to IoT environments (more specifically Industrial IoT where vulnerabilities might have devastating effects) that try to make use of Blockchain technologies due to their intrinsic trust properties and distributed nature [122] [123]. These aspects make blockchain particularly useful from a trust perspective (e.g., establishing trust in IoT-based manufacturing systems [124]), as well as for providing cybersecurity-related certification of the IoT devices (e.g., [125]).

Progress beyond the state of the art

IntellIoT aims to provide a secure and trustworthy by design IoT environment, via the tight integration of a number of innovative security, privacy and trust enablers; namely:

1. a novel, evidence-based continuous security assurance and certification solution, integrating hybrid assessments tailored to next generation IoT environments and which will consider different attacks surfaces and attacker capabilities, gathering detailed contextual information (e.g., configuration changes, network and middleware behaviour), as well as maintaining an up-to-date view of all known vulnerabilities across the complex IoT deployments, from field to backend;
2. trust-based computing mechanisms that will act as a distributed intrusion detection system (IDS) and discriminate the legitimate networking entities from the malicious (e.g., compromised) ones;
3. MTD strategies that administrate the overall legitimate system with AI security-context aware processes, performing self-adaptive behaviours to counter attacks or mitigate their side-effects at runtime, and;
4. integration of state-of-the-art security and trust building blocks, including security primitives (AAA, encryption, etc.) also suitable for resource-constrained devices, secure-by-default and fail-secure configuration of devices, as well as multi-layer monitoring of the security posture of the IoT environment and the operation of said primitives.

3.6. Distributed Ledger Technologies and Smart Contracts for the IoT

Starting with the revolutionary adoption of Bitcoin, blockchain or distributed ledger technologies (DLT) have received a lot of attention in the realm of IoT, as they have the potential to help address some of the IoT security and scalability challenges [126, 127, 128]. 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 publish data to the ledger, a node includes data formatted in transactions in a block with a pointer to its previous block, which creates a chain of blocks, so called Blockchain. A block generated by a node usually needs to solve a mathematical crypto-puzzle and gives the solution as a proof of its workload 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 network. Each correctly behaving miner needs to adhere to the same protocol for creating and also validating new blocks. Until successfully mining a block, a miner broadcasts it for validation. In a nutshell, there are two basic types of DLT: permissionless and permissioned. *Permissionless ledgers*, or public blockchains, are maintained by users (miner or minters) that do not register/authenticate themselves to a certification authority and they do not know each other – not even by a pseudonym. Instead, everyone can freely jump into the system and start maintaining it (and possibly benefitting from it) as long as he/she is willing to invest resources into it. Examples of these blockchains are modern-day cryptocurrencies like Bitcoin, Ethereum or Cardano. In the *permissioned ledger* category, or private blockchains, every party maintaining a ledger needs to register with the system - either by contacting a certification authority or by receiving credentials from the already registered parties - and all these parties know the digital identities, e.g., the public keys, of other registered parties. Permissioned blockchains tend to be more scalable and operate faster.

A smart contract is a distributed app that lives in the blockchain. This app is, in essence, a programming language class with fields and methods, and they are executed in a transparent manner on all nodes participating in a blockchain. Smart contracts are the main blockchain-powered mechanism that is likely to gain a wide acceptance in IoT, where they can encode transaction logic and policies, which include the requirements and obligations of both the party requesting access and the IoT resource/service provider as well as in supporting data trading over wireless IoT networks [129].

DLT can lead to a wave of completely new applications as the enabler of trusted access to edge computing resources. However, the implementation of DLT and smart contracts at the edge still requires further research. Besides, the trust provided by DLTs is greatly valuable in IoT monitoring applications with a large number of devices. As an example,

consider an urban IoT application that monitors the air quality and gas emissions. The data generated by this application is critical, so it must be protected while being tractable, immutable, and transparent.

However, in a typical monitoring system such as the aforementioned, the inter-organization sharing of data may be untrusted, complex, unreliable, and non-transparent. On top of that, the storage of data is centralized, which leads to a single point of failure, where data can be lost or modified. Even in cases where data are spread to different heterogeneous parties, issues may be raised. Firstly, it becomes difficult to validate their origin and consistency. Secondly, querying and performing operations on the data becomes a challenge due to the incompatibility between different application programming interfaces (APIs). For instance, Non-Governmental Organizations (NGOs), Public and Private sectors, and industrial companies may use different data types and databases, which leads to difficulties when sharing the data. Therefore, the way information from IoT-based monitoring systems is stored and collected raises concerns about data integrity, trust, security, transparency, and public availability [130].

In Blockchain-enabled IoT networks, transactions are recorded and synchronized in a distributed manner in all the participants of the system. These participants are called miners or peers and, in some specific DLTs, users are charged a transaction fee to perform (crypto) transactions. In addition, DLTs allow the storage of all transaction into immutable records and every record is distributed across many participants. Thus, security in DLTs comes from their distributed nature, but also the use of strong public-key cryptography and strong cryptographic hashes.

Progress beyond the state of the art

The *IntellIoT* project will progress beyond the DLT state-of-the-art in three aspects (building up on our previous work [131, 132]):

1. circumventing devices' constraints in terms of processing resources, storage resources and network connectivity
2. advancing traditional network designs for uplink-dominated IoT systems
3. interoperability with third-party devices

In an IoT environment, an edge gateway with DLT solutions is equipped with the necessary computational intelligence. Yet, devices in a blockchain should keep a copy of the DLT record, which can be large and increasing over time and limits the scalability of the system. Moreover, the transactions associated with smart contracts require two-way communication traffic, which violates the common assumption that the IoT systems are dominated by an uplink traffic. An edge device in a blockchain network should be capable of verifying information in the blockchain, which is associated with the downlink traffic [133]. At the same time, we want to minimize the use of the downlink from a power-limited node. At a high level, *IntellIoT* envisions an architecture that can trade off complexity of the device, achieved trust and network capabilities, and maintain the trust when some of the devices belong to third parties or connect to the blockchain through a proxy.

4. REQUIREMENTS' SPECIFICATION

This section provides a definition of the functional and non-functional requirements for the IntellIoT framework. As the project follows a use-case driven approach, the first subsection provides an in-depth analysis of the different usage scenarios for each of the three use-cases targeted: Agriculture, Healthcare and Manufacturing. Based on those usage scenarios, a set of identifiable functional requirements are derived, while subsequently a set of non-functional requirements are provided.

It should be noted that *Functional Requirements* describe functionalities of the system from a user-level perspective. These requirements define what the user is expecting of the system during its operation or as a response to specific conditions. *Non-Functional Requirements* describe qualities and performance requirements of the IntellIoT framework, including also aspects related to the functioning of the system on issues such as safety and security.

4.1. Description of Steps in IntellIoT Use-Cases

In this section, the different operating scenarios for each use-case are described. Each scenario focuses on one of the key pillars of IntellIoT (Collaborative IoT, Human-in-the-Loop and Trustworthiness) and describes interactions between actors and components based on different events that trigger them and defines what the expected actions should be. Based on those detailed description, the functionalities of the three systems are defined and can be used to describe the user requirements (functional and non-functional) for the IntellIoT framework.

4.1.1. AGRICULTURE USE CASE

For the Agriculture use-case, three main scenarios are described: Collaborative IoT, Human-in-the-Loop and Trustworthiness. For each of the three scenarios, a number of scenes are defined. Those scenes present the different steps of operation of the overall system, describe the interactions between the actors and components involved and define the actions that need to be performed in order to successfully complete each task. More details about the different scenarios and scenes of the Agricultural use-case can be found in deliverable D2.1, section 3.1.

COLLABORATIVE IOT IN AGRICULTURE USE CASE

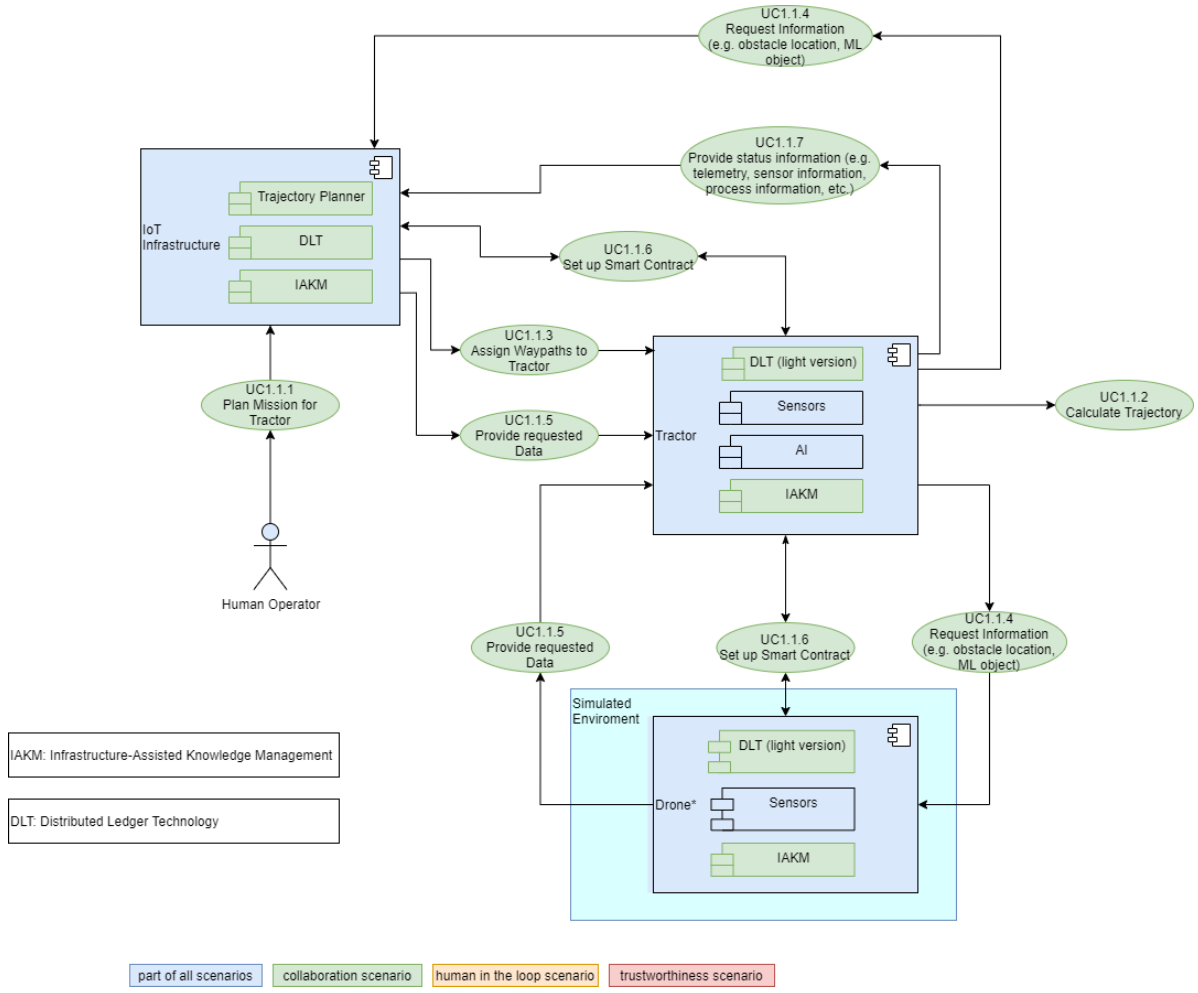

Figure 1. Use Case Diagram Collaborative IoT in Agriculture Use Case

ID:	UC1.1.1
Title:	Plan Mission for Tractor
Description:	The operator uses the End User Goal Specification Front End to create an agriculture mission (e.g., "plough field 5").
Primary Actor:	Operator
Preconditions:	Operator wants to perform a certain procedure on a field within a defined area
Postconditions:	The procedure is defined, the area is defined, borders are defined
Triggers:	Operator input

Main Success Scenario:	The operator has successfully defined a task, area and boundaries
Extensions:	
Frequency of Use:	When a new mission is planned
Status:	Final
Owner:	HSG
Justification:	This is required for the scenario to start.

ID:	UC1.1.2
Title:	Calculate Trajectory
Description:	The tractor is calculating a trajectory based on the waypoints sent by the IoT-Infrastructure, the GPS data of the tractor, data from other IoT-devices, information of the camera system and a tractor model.
Primary Actor:	Tractor (autonomous function controller).
Preconditions:	Input data from the mission planning tool (Waypoints, Tasks).
Postconditions:	The tractor reached the last waypoint and finished its task without interruption
Triggers:	The mission planning tool has sent the tractor a task which has to be performed along a defined path
Main Success Scenario:	1. The tractor receives waypoints and the operation which has to be performed 2. Based on the tractor model and additional input data (e.g., from a camera) the autonomous controller is calculating the trajectory
Extensions:	Missing GPS-Signal, no 5G connection, waypoint data are not feasible to reach (too small cornering radius, crossings or other reasons)
Frequency of Use:	When a new mission was started
Status:	Final
Owner:	AVL
Justification:	A trajectory is required for the tractor to define a course and complete any requested task

ID:	UC1.1.3
Title:	Identify Tractor and Assign Waypoint to Tractor
Description:	Depending on the configuration of the Hypermedia MAS, one or multiple Agents accept the specified mission. Using a service to find possible entry points to, reach the designated area and using another service to select, based on these entry points and the specified process (e.g., fertilizing) a suitable tractor to accomplish it, the selected tractor is tasked with the first waypoint.
Primary Actor:	Hypermedia MAS / One or multiple Agents in the Hypermedia MAS

Preconditions:	A mission was defined by the operator Agents within the system have access to the services required to accomplish the mission
Postconditions:	Suitable waypoints have been sent to a suitable vehicle
Triggers:	Operator planned a mission
Main Success Scenario:	• An agent has found a suitable vehicle for the task, e.g., an available tractor with the required tooling for the task • An agent has defined waypoints and borders for the vehicle.
Extensions:	No suitable tractor can be found (offline / in operation / no required tooling / task exceeds maximum operation area); inconsistent or missing data.
Frequency of Use:	When a new mission is initiated
Status:	Final
Owner:	HSG
Justification:	This is required for a vehicle to start operating within this scenario.

ID:	UC1.1.4
Title:	Request Information
Description:	Tractors, drones or the IoT infrastructure (later called 'initiators') require information related to a particular environment. That environment needs to be described according to a known semantic such that entities holding such information (later called 'target') may be identified. Targets holding the requested information may be identified in two ways. If targets notify other entities of their environments using a common semantic, initiators may uniquely identify the target and send the information request directly to the target. Otherwise, the initiator sends the request in multicast to all entities, including the environment description, and the target identifying to correspond that environment reply with the requested information. Request information are implemented as publish/subscribe mechanisms. Information may also take the form of knowledge, for which the request information will correspond to request knowledge.
Primary Actor:	Called 'initiator', it corresponds either to the IoT infrastructure or any entity in the field (drone or tractor), which require information it does not have for the operation of the service.
Preconditions:	The initiator requires information or knowledge of a particular context, without which the IntellIoT service cannot proceed.
Postconditions:	The initiator received the requested information for at least one target entity and may proceed with the service.
Triggers:	The IntellIoT service requires missing environmental information or knowledge.
Main Success Scenario:	The information request is sent to the right entity, which holds the appropriate information or knowledge required by the service, or authorized to be provided by the service.
Extensions:	The initiator may request knowledge in two forms:

	1. Knowledge models – ML model used directly for the service or as transfer learning to have a pretrained model. 2. Knowledge capacity – identify a target entity, which could train or assist the initiator to train a given model.
Frequency of Use:	Often at the early phase of the service, where capabilities of target entities are not known by an initiator. Less often but critical, in case of unrecognized context or environment.
Status:	Final
Owner:	EURECOM
Justification:	Not being able to identify the target holding the required information or knowledge is expected to interrupt the service.

ID:	UC1.1.5
Title:	Provide requested Data
Description:	Tractors and other entities in the field (e.g., drones, edge infrastructure, sensors, etc.) provide the information they have about the environment to the entity that has requested the data. This information can contain data about obstacles, trajectories, tasks, etc.
Primary Actor:	The entity (e.g., tractor, drone, sensor) making the data available to the entity that is requesting the information.
Preconditions:	The entity has knowledge about the environment that is different from the one requested. Additionally, the entity is connected to the overall system and received the request for information.
Postconditions:	Data has been exchanged with the requesting entity and the requesting entity will update its internal knowledge based on the received data.
Triggers:	A request for information has been received by the entity, as another entity in the field is stuck in an unknown situation and is asking for additional data
Main Success Scenario:	• Data has been provided to the requesting entity • Requesting entity is updating its internal knowledge and has received correct information for evaluating the situation.
Extensions:	Communication with other entities is not possible because of communication issues.
Frequency of Use:	In the beginning, the tractors have not a complete view of the environment, so the requests can occur more frequently. The more data is exchanged, the less likely a request for data will occur.
Status:	Final
Owner:	EURECOM
Justification:	Information exchange and update of internal knowledge is of high importance to keep the system up and running.

ID:	UC1.1.6
Title:	Set up Smart Contract
Description:	The interaction rules are defined in smart contracts between tractors, drones and the IoT infrastructure. Smart contracts provide an autonomous mechanism for operation and management between involved partners.
Primary Actor:	The tractors, drones and the IoT infrastructure are the primary entities
Preconditions:	The entities are connected and communicated via wired or wireless channels. A lightweight version of a distributed ledger is set up in every actor, then smart contracts can be executed over secured and trusted infrastructure.
Postconditions:	The pre-defined agreements and rules in smart contracts between involving partners are executed autonomously. Then, a record for every activity is formed in transaction format and stored immutably in the distributed ledger.
Triggers:	One of the actors, for example a drone, a tractor or the IoT infrastructure initiates a request for a service, e.g., renting, or sharing data. On the other hand, the actors request for a verification from the ledger and ask their neighbors.
Main Success Scenario:	• The actors with the DLT setup synchronize with each other to have a common database in the entire network. • One of the actors is rented for a particular service which is defined in smart contracts and recorded in distributed ledger • Based on the agreements in smart contracts, the provided services and payments are autonomously executed. • All activities and bills are recorded in the distributed ledger for future accounting and auditing.
Extensions:	Because of the transparency and immutability of distributed ledger technologies, the partners can query the ledger to verify the records and check the progress or history of tasks. All the activities are stored in the ledger and cannot be changed, so the partners can trust the data.
Frequency of Use:	Continuous: the smart contract is set up once, when the tractor or the IoT infrastructure initiates the request, and then it is active to record all activities
Status:	Final
Owner:	AAU
Justification:	The trustworthiness of information exchange between actors is important for communication and accounting purposes.

HUMAN-IN-THE-LOOP IN AGRICULTURE USE CASE

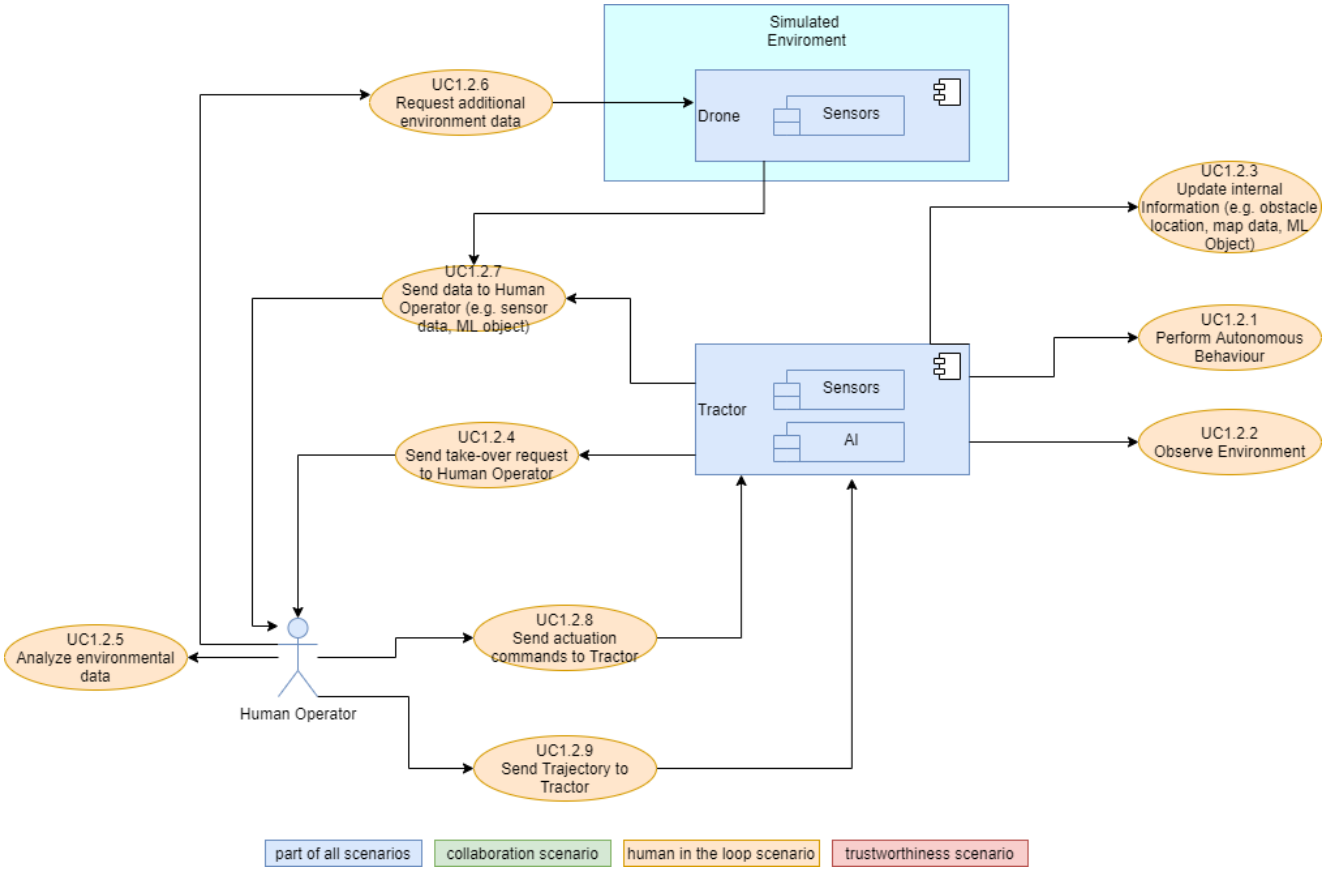

Figure 2. Use Case Diagram Human In The Loop in Agriculture Use Case

ID:	UC1.2.1
Title:	Perform autonomous behavior
Description:	The tractor is transferring the trajectory data into steering and drivetrain request. The calculated trajectory is continuously updated based on the environment information and data of other IoT-devices. Cameras on the tractor help to find a suitable path along agricultural structures without harming the crops – line detection. The cameras can detect obstacles and force the controller to find a trajectory around it.
Primary Actor:	Tractor
Preconditions:	A mission was started
Postconditions:	The tractor is moving along the waypoints and performing the task
Triggers:	Mission was started
Main Success Scenario:	• Trajectory was defined • drivetrain requests are calculated from the trajectory

	• Trajectory is continuously updated based on camera data and external inputs. • Tractor is performing the task
Extensions:	Tractor is blocked by an obstacle; operator takes over control. Deviations between tractor model and real tractor behavior, dirt/dust on camera system, bad light conditions
Frequency of Use:	When a mission was started
Status:	Final
Owner:	AVL
Justification:	Based on the precalculated information such as computed trajectory and with the assistance of monitoring tools, the tractor should be able to perform its autonomous operation.

ID:	UC1.2.2
Title:	Observe environment
Description:	The tractor is equipped with 4 cameras that are aligned to each side. The cameras capture a 360deg panorama around the tractor. This information is provided via 5G to the operator. With a VR headset the operator can perceive the surrounding area of the tractor.
Primary Actor:	Tractor
Preconditions:	The Tractor was started and is in an operational state.
Postconditions:	Sufficient amount of data was captured.
Triggers:	Tractor is in an operational state
Main Success Scenario:	1. capturing images from the 4 cameras 2. stitching the image data 3. converting the data into a suitable format (file format, resolution, compression) 4. providing the image data to the IoT-Infrastructure
Extensions:	Missing 5G Connection, dust or dirt on camera, bad light conditions.
Frequency of Use:	Continuous
Status:	Final
Owner:	AVL
Justification:	The tractor must be able to gather environmental data both for its autonomous operation and to provide proper suitable information to a remote human operator.

ID:	UC1.2.3
Title:	Update internal information

Description:	When the tractor receives the actuation commands (UC1.2.5) or the trajectory (UC1.2.6) from the human operator, it needs to improve its own model in order to be able to overcome similar situations when encountered in the future.
Primary Actor:	Tractor
Preconditions:	The tractor receives an input from the human operator, either actuation commands (UC1.2.5) or trajectory information (UC1.2.6)
Postconditions:	The tractor has successfully updated its own model, given the human operator's input. The tractor can autonomously overcome similar situations in the future.
Triggers:	Receiving actuation commands (UC1.2.5) or trajectory information (UC1.2.6) from the human operator.
Main Success Scenario:	1. Tractor successfully receives commands/trajectory from the human operator. 2. Tractor sends its state (object information, map data) and command/trajectory to its AI unit. 3. AI unit successfully carryout model updating, and hence, can autonomously resolve similar future encounters.
Extensions:	• Due to poor connectivity, operator cannot receive real-time feedback on his commands. • Operator's input is used to train a ML model of an augmented tractor at the operator's premises. Then the updated ML model is uploaded to the tractor.
Frequency of Use:	High frequency in the initial phase. As the performance of the tractor's AI improves, the frequency of occurrences lowers.
Status:	Final
Owner:	UOULU
Justification:	This is required to leverage human input in order to improve the AI models. The goal is to eventually minimize human interventions.

ID:	UC1.2.4
Title:	Send take-over request to Human Operator
Description:	The tractor is stuck in a specific situation (e.g., unknown obstacle in front of the tractor has not enough knowledge how to overcome the situation). The tractor goes into a safe state and sends a request for support to the human operator.
Primary Actor:	The tractor sending the take-over request to the human operator.
Preconditions:	The tractor has encountered a situation that it doesn't know how to handle (because of limited knowledge about the environment). The tractor is in safe state (i.e., has stopped) and is capable of sending a request for support to the operator.
Postconditions:	A connection between the human operator and the tractor has been established and the human operator can control the vehicle.
Triggers:	• Unknown obstacle on the path of the tractor

	• Limited knowledge about the environment.
Main Success Scenario:	• Tractor is in a safe state • A successful request has been made to the human operator • The human operator has received the request.
Extensions:	• The tractor doesn't identify the unknown situation • The request has not been received by the human operator
Frequency of Use:	Every time an unknown situation occurs and the knowledge of the tractor is not limited. In the beginning of a task, this will happen more often, but as the tractor updates its internal knowledge, the request will most likely become fewer.
Status:	Final
Owner:	EURECOM
Justification:	The tractor will remain stuck without the human operator knowing about it.

ID:	UC1.2.5
Title:	Analyze environmental data
Description:	An unexpected event occurs, which results in a blocking state for the system (AI). The system therefore requests the human operator (Human-in-the-loop) to take over. The human operator analyzes the situation, based on the environmental data. The environmental data consists of one or more video streams from the tractor, and possibly additional video streams from external devices (drone view) and the position on a map
Primary Actor:	A skilled person using a Virtual Reality (VR) capable Head Mounted Display (HMD), which provides an immersive view of the environmental data (ideally 360°-degree video feed).
Preconditions:	Live video feed from the tractor (and drone) is needed
Postconditions:	Latency and jitter free immersive view from the tractor in an ideally 360° experience.
Triggers:	Unexpected blocking event, for example: • obstacle in front of the trajectory • tractor get stuck inside mud • animal is crossing the field
Main Success Scenario:	• Unexpected blocking event triggers the human-in-the-loop scenario • Human operator receives a message from a tractor's AI during an VR experience or before putting on the headset • Human operator establishes connection and is requesting the environmental 360° video feed of this specific tractor • Operator can fully look around the tractor in order to visually analyze the event.
Extensions:	Error 1: Environmental video feed results in heavy motion sickness for the User (high latency) Error 2: Environmental video feed has bad resolution (low bandwidth)

	Error 3: Source of issue is outside the camera angle or is covered by other objects.
Frequency of Use:	The current assumption is, that human interaction is frequently needed during the early stages, but will steadily decrease over time, as the AI is a self-learning system.
Status:	Final
Owner:	HOLO
Justification:	The human operator needs to understand the situation so that he/she/they can make the right decisions.

ID:	UC1.2.6
Title:	Request additional environment data
Description:	The human operator has only a limited view of the environment and cannot establish the current situation. He/she will make a request to other entities in the field (e.g., other vehicles, drones, sensor) to receive more (sensor) data to get a more extensive view of the environment.
Primary Actor:	Human Operator
Preconditions:	The human operator has limited information about the situation and has a connection to other entities in the field for requesting data.
Postconditions:	The human operator has interacted with other entities in the field and performed a successful request for additional data, which will be provided.
Triggers:	• The vehicle is stuck in a specific situation, e.g., an unknown obstacle • A request has been made to the human operator for take over • The human operator inspects the data from the tractor and has limited information and cannot properly assess the situation
Main Success Scenario:	• Connection to other entities in the field has been established • The human operator has identified the entities that can provide additional information regarding the situation
Extensions:	1. Bad connectivity resulting in incomplete data 2. Other entities in the field cannot provide the required information.
Frequency of Use:	In the beginning, the human operator has potentially limited information available about the environment and will have to contact more often external entities for information. The information will then be extended and will results in less additional information requests.
Status:	Final
Owner:	HOLO
Justification:	The human operator must have access to additional information – in case the normal video feed is not sufficient – to assess the situation and not damage the environment or the vehicles.

ID:	UC1.2.7
Title:	Send data to Human Operator
Description:	The human operator performs a request for additional data (see UC1.2.2) and the contacted entity provides the requested data to the human operator.
Primary Actor:	Entity (e.g., other tractor, drone, sensor) contacted by the human operator for additional information.
Preconditions:	The entity is connected to the overall system and has the requested information for the human operator.
Postconditions:	The entity has sent successful the requested data to the human operator.
Triggers:	A request for data from the human operator has been received
Main Success Scenario:	1. The data has been identified that is requested by the human operator. 2. The entity has successfully sent the data to the human operator.
Extensions:	1. Bad connectivity resulting in incomplete data 2. Connectivity issues cause high latencies 3. The requested information is not available or not of good quality.
Frequency of Use:	In the beginning, the human operator has potentially limited information available about the environment and will have to contact more often external entities for information. The information will then be extended and will result in less additional information requests.
Status:	Final
Owner:	EURECOM
Justification:	The human operator must have sufficient and correct information available to assess the situation and not damage the environment or the vehicles.

ID:	UC1.2.8
Title:	Send actuation commands to Tractor
Description:	The human operator has identified the source of the blocking event and is capable to solve the situation by manually repositioning (driving) the vehicle.
Primary Actor:	The human operator wearing a head-mounted display (allowing to display a virtual reality representation of the field) can remotely control the tractor.
Preconditions:	The human operator has identified the source of the blocking event and found a way to solve the situation. Furthermore, the video feed is stable enough allowing the safe manual navigation for the tractor.
Postconditions:	The human operator has successfully repositioned the vehicle and returns control to the AI. The AI has learned new behavior.
Triggers:	The intention of the human operator to reposition the vehicle manually via the VR controllers.

Main Success Scenario:	1. The human operator has successfully identified the blocking event and can solve the problem by manually repositioning the vehicle 2. The human operator grabs the VR controllers and initiates movements 3. The movements are correctly shared with the AI (speed and direction), moving the tractor in accordance with the controller input 4. The AI system verifies, that the issue was solved and is given back control
Extensions:	Error 1: bad connection resulting in loss of video feed, or movement issues Error 2: manual reposition does not solve the problem Error 3: vehicle gets stuck during its repositioning
Frequency of Use:	The current assumption is, that human interaction is frequently needed during the early stages, but will steadily decrease over time, as the AI is a self-learning system.
Status:	Final
Owner:	HOLO
Justification:	The human operator will need a method to change the tractor's path.

ID:	UC1.2.9
Title:	Send trajectory to Tractor
Description:	The human operator has identified the source of the blocking event and is capable to solve the situation by adjusting the tractor's trajectory via a virtual browser version of the system.
Primary Actor:	The human operator wearing an HMD to interact with a virtual version of the system.
Preconditions:	The human operator has identified the source of the blocking event and found a way to solve the situation. The connection to the system is stable and the tractor's location is correctly recognized.
Postconditions:	The human operator has successfully adjusted the trajectory and returns control to the AI. The AI has learned new behavior.
Triggers:	The intention of the human operator to reposition the tractor manually via the VR controllers.
Main Success Scenario:	1. The human operator has successfully identified the blocking event and can solve the problem by setting a new trajectory for the tractor 2. The human operator gains access to the system via a virtual browser 3. The tractor is at the correct location, so the human operator can create a new path for the tractor 4. The AI picks up the new information and executes the instructions, while the human operator observes the taken actions through the video feed of the tractor's cameras 5. The tractor's issue has been solved and the human operator returns the control to the tractor's AI.

	6. The AI has been trained from this process and improved its performance, creating new models that can be shared with other tractors
Extensions:	Error 1: bad connection resulting in loss of video feed Error 2: indirect reposition does not solve the problem Error 3: vehicle gets stuck during its repositioning Error 4: the system does not pick up the correct location of the tractor, so new movements cannot be planned
Frequency of Use:	The current assumption is, that human interaction is frequently needed during the early stages, but will steadily decrease over time, as the AI is a self-learning system.
Status:	Final
Owner:	HOLO
Justification:	The human operator needs a method to correct the tractor's path. Nevertheless, adjustment of trajectory is the secondary solution to the issue.

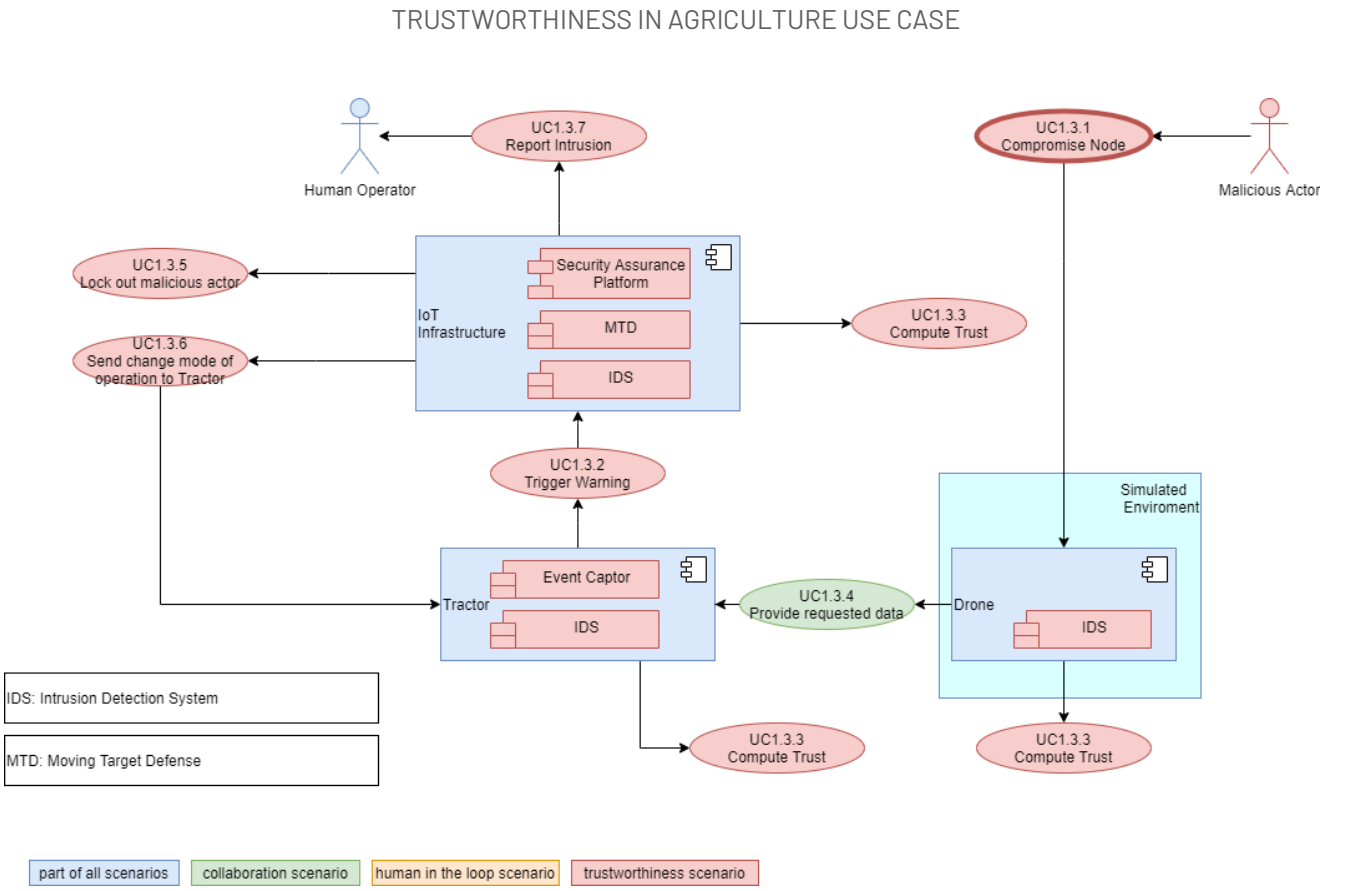

Figure 3. Use Case Diagram Trustworthiness in Agriculture Use Case

ID:	UC1.3.1
Title:	Compromise node (drone)
Description:	The drone gets compromised by a malicious actor, who gains control of the drone
Primary Actor:	The malicious actor, the drone
Preconditions:	The drone is part of the network and is operating as expected
Postconditions:	The drone is compromised. The malicious actor controls drone's actions
Triggers:	Malicious actions aiming to compromise drone
Main Success Scenario:	• The malicious actor exploits a security vulnerability of the drone • The malicious actor gains control of the drone and controls its behavior • The compromised drone attacks the rest of the network
Extensions:	Equivalent scenario can be assumed for other nodes (e.g., tractor)
Frequency of Use:	Scenario refers to misuse. Depends on the malicious actor, number of vulnerabilities, number/effectiveness of protection measures adopted etc.

Status:	Final
Owner:	TSI
Justification:	A compromised node (the drone in this case) attacking the internal network may cause severe issues to the overall operation of the system, lead to failures and even compromise safety.

ID:	UC1.3.2
Title:	Trigger Warning
Description:	The tractor identifies, through trust-based IDS, that the drone is possibly compromised and notifies the Security Assurance Platform
Primary Actor:	Detecting node (Tractor, in this case)
Preconditions:	All nodes communicate normally with each other and have built trust tables for their peers
Postconditions:	The tractor triggers a warning notification.
Triggers:	The drone behaves in a way that reduces its trust.
Main Success Scenario:	• The drone starts working in an unexpected way • The tractor decreases its trust towards the drone • When trust drops below a certain threshold, the tractor identifies the drone as compromised and sends a notification to the Security Assurance Platform
Extensions:	As a variation, the tractor could be compromised (detected by the drone). Error 1: A node compromise is not detected by the trust-based IDS (false-negative) Error 2: A non-compromised node is marked as compromised by the trust-based IDS (false-positive).
Frequency of Use:	Scenario refers to misuse. Depends on the malicious actor, number of vulnerabilities, number/effectiveness of protection measures adopted etc.
Status:	Final
Owner:	TSI
Justification:	If the tractor does not trigger the warning, the malicious drone will not be identified and will have access to the system or it will be able to interfere without being restricted.

ID:	UC1.3.3
Title:	Compute Trust
Description:	Each node in the ad-hoc network builds a trust table, with an entry for each of its neighbouring nodes, and populates the table based on successful communications, packet monitoring and profiling the behaviour of its neighbouring nodes
Primary Actor:	A node that computes trust, which could be any entity in the field (e.g., tractor or drone).
Preconditions:	More than one node is available

Postconditions:	Communication is successful and trust for all parties is computed
Triggers:	Any network communication through the ad-hoc network
Main Success Scenario:	1. A node starts communicating with another node 2. Trust is computed based on the communication according to a number of metrics
Extensions:	Various trust computation schemes can (and will be) explored, each with its own intricacies in terms of trust information exchange, computation etc.
Frequency of Use:	Continuous. Trust is computed every time there is a network communication inside the ad-hoc network.
Status:	Final
Owner:	TSI
Justification:	If trust is not computed correctly, malicious nodes might not be identified, or legitimate nodes might be falsely identified as malicious

ID:	UC1.3.4
Title:	Provide requested data
Description:	The drone provides data to the tractor
Primary Actor:	The drone, the tractor
Preconditions:	The drone and the tractor trust each other and can communicate
Postconditions:	The tractor continues normal operation using the data provided by the drone
Triggers:	The tractor requests data from the device
Main Success Scenario:	1. The tractor requests data from the drone 2. The drone receives the request 3. The drone collects the needed data 4. The drone sends the data to the tractor
Extensions:	Errors can be introduced by communication failures.
Frequency of Use:	Every time a node requests data
Status:	Final
Owner:	TSI
Justification:	The drone provides information that the tractor cannot otherwise collect and therefore if both nodes are trustworthy, it is critical to ensure continuous communication between them.

ID:	UC1.3.5
Title:	Lock out malicious actor

Description:	The Security Assurance Platform, upon receiving an intrusion warning, generates a new network configuration and sends it to the tractor, thus isolating the malicious actor.
Primary Actor:	The Security Assurance Platform
Preconditions:	The tractor has identified the drone as malicious
Postconditions:	The Security Assurance Platform generated a new network configuration that isolates the drone
Triggers:	The tractor notification to the Security Assurance Platform
Main Success Scenario:	• The Security Assurance Platform receives an intrusion/compromise warning from the tractor • The Security Assurance Platform ingests evidence of intrusion/compromise • The Security Assurance Platform generates mitigation plan (new configuration) to isolate the drone
Extensions:	Error 1: One or more involved entities are not included in the asset model of the Assurance Platform Error 2: A mitigation plan cannot be identified for a specific type of attack
Frequency of Use:	Every time a non-compliant / possible malicious node is detected
Status:	Final
Owner:	TSI
Justification:	If the malicious drone is not locked out of the system automatically, it will have time to attack the system until the human operator is notified and takes action.

ID:	UC1.3.6
Title:	Send change mode of operation to tractor
Description:	The Security Assurance Platform, upon receiving an intrusion warning, generates the new network configuration and sends it to the tractor, thus isolating the malicious actor.
Primary Actor:	The Security Assurance Platform
Preconditions:	The Security Assurance Platform has been notified about an intrusion and generated a new network configuration
Postconditions:	The tractor is using the new configuration and the drone has been isolated
Triggers:	The tractor notification to the Security Assurance Platform
Main Success Scenario:	• The Security Assurance Platform sends the mitigation action (new network configuration) to the tractor • The drone does not know the new network configuration and is isolated, while the tractor continues normal operation
Extensions:	Error 1: The receiving node (tractor) does not know how to apply configuration

	Error 2: The new configuration is erroneous, causing connectivity issues to tractor Error 3: The new configuration fails to isolate compromised/malicious node
Frequency of Use:	Every time a non-compliant / possible malicious node is detected
Status:	Final
Owner:	TSI
Justification:	If the tractor is not informed for the changes to the configuration, it will be isolated as if it were a malicious node.

ID:	UC1.3.7
Title:	Report intrusion
Description:	The Security Assurance Platform, upon receiving an intrusion warning, reports the incident to the Human Operator
Primary Actor:	The Security Assurance Platform
Preconditions:	The tractor has identified the drone as malicious
Postconditions:	The Human Operator has been informed, in order to perform any additional operations needed to ensure the normal and secure operation of the network
Triggers:	The tractor notifies the Security Assurance Platform that the drone was identified as malicious
Main Success Scenario:	1. The Security Assurance Platform receives a warning from the tractor 2. The Security Assurance Platform informs the Human Operator of the intrusion 3. The Human Operator can perform additional actions in order to investigate and mitigate the attack
Extensions:	To be explored, if mitigation actions have to be triggered/confirmed by human operator, or can be carried out autonomously.
Frequency of Use:	Every time a non-compliant / possible malicious node is detected
Status:	Final
Owner:	SANL
Justification:	The human operator must be promptly informed to investigate the attack, and possibly perform additional actions to secure the system.

4.1.2. HEALTH-CARE USE CASE

For the Healthcare use-case, three main scenarios are described: Autonomous Collaborative IoT with federated learning to provide personalized interventions, Human Take Over for interventions that require human involvement and Security and Trustworthiness in remote patient care. For each of the three scenarios, a number of scenes are defined. Those scenes present the different steps of operation of the overall system, describe the interactions between the actors and components involved and define the actions that need to be performed in order to successfully complete each task. More details about the different scenarios and scenes of the Healthcare use-case can be found in deliverable D2.1, section 3.2.

COLLABORATIVE IOT IN HEALTHCARE USE CASE

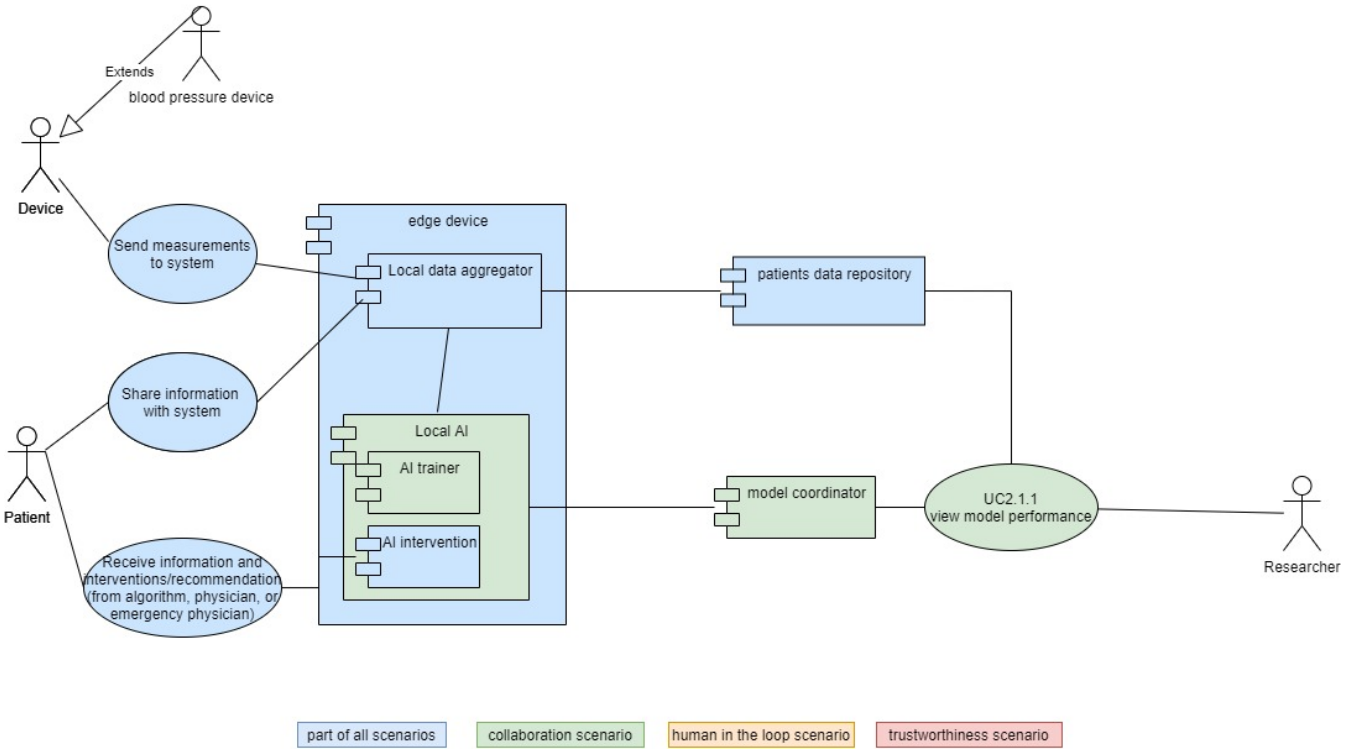

Figure 4. Use Case Diagram Collaborative IoT in Healthcare Use Case

ID:	UC2.1.1
Title:	View model performance
Description:	A researcher monitors the performance of the models created by the Global and Local AI systems. Note that there might be multiple researchers.
Primary Actor:	Researcher
Preconditions:	An evaluated base model exists. Note that there might be multiple base models.

Postconditions:	An optimized model is trained in the Global AI system, which is sent as an update to the Local AI system. Personalized models are created in the Local AI system. Note that it is possible that the Local and Global AI systems will keep learning as long as there is new data from the patients.
Triggers:	1. A researcher starts new tasks for the workers, which are a number of Local AI systems, through the Global AI coordinator. Once all the Local AI systems finish training, the coordinator will aggregate the results into an updated model for the researcher to view. The Global AI coordinator can be configured with a minimum number of Local AI systems. If the minimum is reached, an automatic trigger for the training of an updated model will occur.
Main Success Scenario:	• An evaluated base model exists. Note that there might be multiple base models. • A researcher starts new tasks for the Local AI systems through the Global AI coordinator. Alternatively, the Global AI coordinator is configured for the automated start of new tasks. • The Local AI systems finish their tasks. To achieve personalization, these local models are made available in the Local AI systems. • The coordinator will aggregate the results of the tasks into an updated global model for the researcher to view. After enough rounds, an optimized model should be achieved. 1. If the updated global model shows improved performance, it is made available to the Local AI systems.
Extensions:	Failures: • The Global AI coordinator can go into an error state. • A Local AI can fail before training finishes. • The Global AI coordinator is waiting indefinitely for the minimum number of Local AI systems. Alternatives: • Validating model updates will be a challenge, due to performance drift and outliers. • In clinical scenarios, outliers are special cases which may not be used for global updates, but which are still valid and should be accounted for. • A Local AI can take an unreasonably long time for model training. • Flexible ways for the researcher to modify the model parameters and updates need to be investigated. • The owner of a model may not be willing to share the entire model in raw form. • The impact of differences in the amount and quality of the data in the Local AI systems needs to be investigated (appropriate global model averaging, data pre-processing). • Appropriate techniques for dealing with communication overhead need to be investigated. • Support for data provenance needs to be investigated.

	• Appropriate data privacy during model updates needs to be investigated. • A workflow service so that the coordinator's scope can be limited needs to be investigated.
Frequency of Use:	On-demand as requested by a researcher. Also, as determined by the Global AI coordinator.
Status:	Final
Owner:	Philips
Justification:	Models must be optimized and retrained periodically. Local AI models are essential to enabling personalized health recommendations. Meanwhile, Global AI models leverage training from the Local AI models.

HUMAN IN THE LOOP IN HEALTHCARE USE CASE

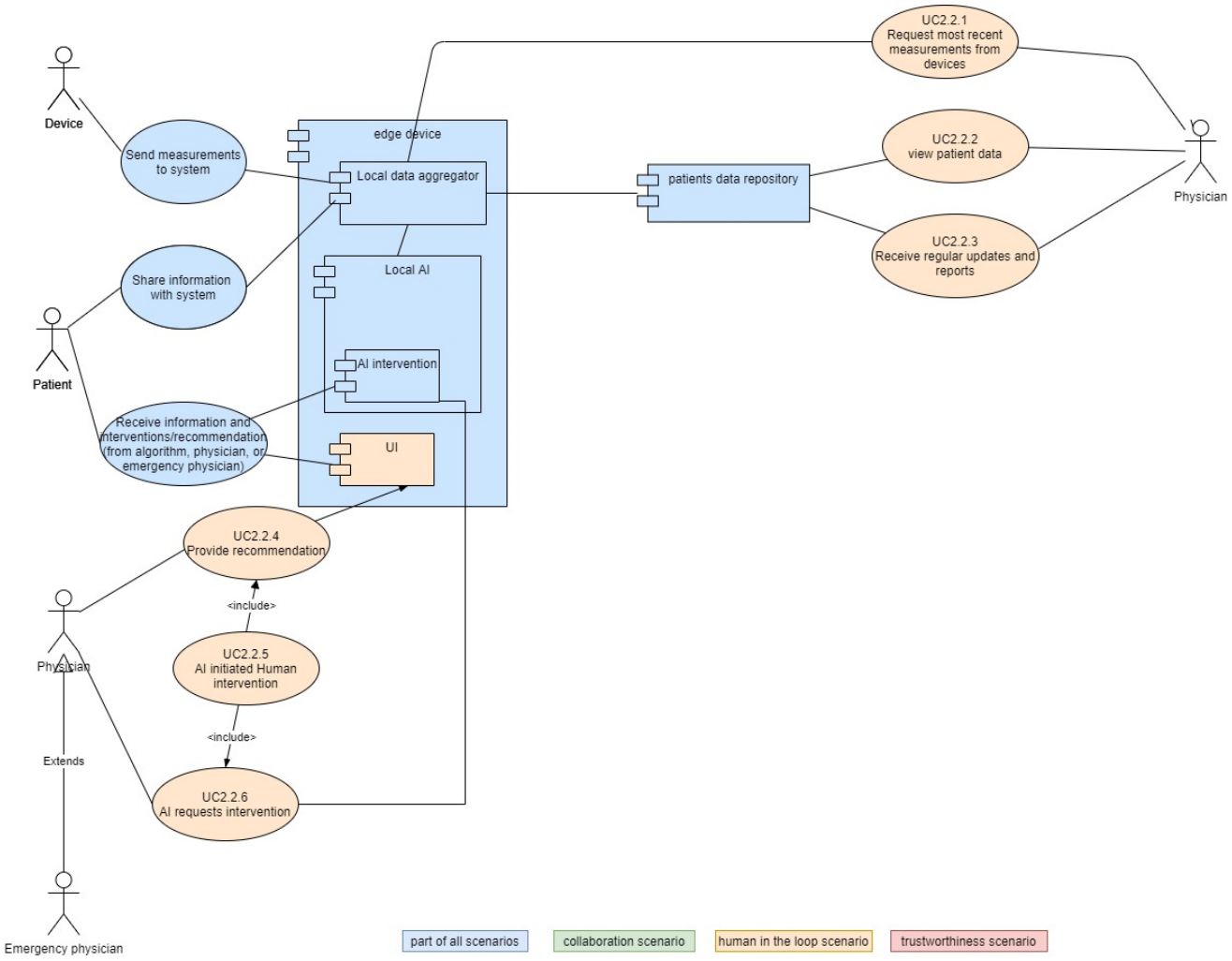

Figure 5. Use Case Diagram Human Take Over in Healthcare Use Case

ID:	UC.2.2.1
Title:	Request most recent measurements from devices
Description:	The Physician requests recent data for a particular patient
Primary Actor:	Physician
Preconditions:	The Physician is logged into the system
Postconditions:	In the case of an emergency contact or in case of a reported clinical event recent data regarding heart rate (last hour) before the event, ECG (during or immediate after the

	clinical event episode), temperature, oxygen saturation (during or immediate after the episode), blood pressure (during or immediate after the episode) are available for viewing.
Triggers:	• Patient has an appointment with Physician • Emergency contact with Physician • The patient enters data regarding 'how he feels today: better, worse or the same, symptoms: dyspnea, chest pain, dizziness, syncope, fatigue, tachycardia) and transmits them successfully to the physician transmitted successfully 1. The physician contacts the patient and provides advice.
Main Success Scenario:	• Physician selects the patient (using the pseudonym) • Physician triggers the request for recent data (last hour)
Extensions:	• If the patient reports an event, the data should be sent autonomously. The same should be performed in the case of detection of abnormalities in any clinical parameter. • In the event of the detection of one abnormal parameter, data from all the other parameters should be explored as well and transmitted. • Case of delayed transmission or communication • Case of unreliable measurement from the system Failures: • A fault in the Edge device system causes storage and/or processing of the new measurements to fail. • The patient takes a measurement incorrectly. Then, they do not retake the measurement, or they retake it multiple times
Frequency of Use:	• Once per week • On demand
Status:	Final
Owner:	Philips
Justification:	An undetected abnormality might oppose a risk for the patient

ID:	UC.2.2.2
Title:	View patient data
Description:	The Physician views the data for a particular patient
Primary Actor:	Physician
Preconditions:	The Physician is logged into the system
Postconditions:	A physician is able to see patient data.
Triggers:	• Patient has appointment with Physician 2. Emergency contact with Physician

Main Success Scenario:	1. Physician selects the patient (using the pseudonym) 2. The Physician selects a period 3. The Physician sees (pertaining to the period): a. the measurements of this patient covering blood pressure, heartrate, activity level, oxygen saturation, weight, ECG, temperature on a time scale • Given recommendations
Extensions:	• Data should be sent autonomously in case of detection of abnormalities in any clinical parameter • In case of the detection of one abnormal parameter, data from all the others should be explored as well. • Detection of changes in daily biometric parameters, inform the clinician • Alarm the patient when activity level is not reached • Alarm the patient when weight is increased, give instructions • Distinguish between deterioration of clinical condition or an alarm situation • Case of unreliable measurement •
Frequency of Use:	• Daily • On demand
Status:	Final
Owner:	Philips
Justification:	The physician can make a better diagnosis when they have access to historical as well as recent measurements. In the case of emergencies or when a recommendation should be given to a patient, the physician needs to decide what will be communicated to the patient.

ID:	UC2.2.3
Title:	Receive regular updates and reports
Description:	Regular updates and reports of a patient's condition are sent to a physician.
Primary Actor:	Physician
Preconditions:	There are new measurements for a patient, or a schedule determines that a report should be created.
Postconditions:	Regular updates and reports are sent to a physician.
Triggers:	• New measurements or all measurements needed for a report are available. 3. A report needs to be created according to a schedule.
Main Success Scenario:	• New measurements for an update of a patient's condition are available. • The new measurements should be reported in order to complete the data required for a report.

	• Alternatively, a schedule determines that a report should be sent, even if there is no new data. • The report is sent to a physician.
Extensions:	Failures: • A report is created according to a schedule, but the patient had not taken new measurements.
Frequency of Use:	Weekly.
Status:	Final
Owner:	Philips
Justification:	The physician needs updates and reports for communication with and diagnosis of the patient. For specific conditions or measurements, weekly aggregations are used.

ID:	UC2.2.4
Title:	Provide recommendation
Description:	A physician provides a recommendation to the patient.
Primary Actor:	Physician
Preconditions:	The Local AI system has a number of possible recommendations for the patient.
Postconditions:	A physician selects a recommendation that will be provided to the patient.
Triggers:	• The Local AI system has enough data on the patient to find possible recommendations. • The Local AI system uses external data sources, e.g., weather conditions, and finds possible recommendations.
Main Success Scenario:	• The Local AI system finds a number of possible recommendations. • A physician evaluates the recommendations and selects an appropriate one. • The recommendation is provided.
Extensions:	Failures: • The patient is not engaged enough with the system to receive personalized recommendations.
Frequency of Use:	• After more time of using the platform (7 months and afterwards), determined by the results of the Local AI. Also depends on useful and relevant external data sources.
Status:	Final
Owner:	Philips

Justification:	While certain recommendations can be sent to the patient automatically without human intervention, other recommendations cannot be made with sufficient confidence or offer similar options and thus require a physician to make a selection.

ID:	UC2.2.5
Title:	AI initiated human intervention
Description:	The Local AI system will be able to recognize potential extreme measurements or behaviors and raise an alert that requires human intervention. Note that there will be several alerts. The alerts may include the case of an emergency contact between the physician and the patient.
Primary Actor:	Physician
Preconditions:	The Local AI system recognizes potential extreme measurements or behaviors.
Postconditions:	The Local AI system raises an alert and a physician intervenes.
Triggers:	• The Local AI recognizes potential extreme measurements or behaviors. • After a patient uses the platform for 7 months and afterwards, the Local AI system will be able to recognize personalized deviations.
Main Success Scenario:	• The Local AI system includes decision tree algorithms, with combined multiple rule-based interventions as presented in different clinical scenarios. • Using the algorithms and rules, the Local AI system recognizes potential extreme measurements or behaviors. • After 7 months of use, personalized deviations will be recognized. • The Local AI system raises an alert and a physician intervenes.
Extensions:	Alternatives: • For very extreme measurements and behaviors, critical alerts will be raised.
Frequency of Use:	• As required, when extreme measurements or behaviors are recognized.
Status:	Final
Owner:	Philips
Justification:	The Local AI will be able to identify general and personalized extreme measurements or behaviors, which means that a patient is not adhering to the prescribed program. This will require a physician to communicate with the patient.

ID:	UC2.2.6
Title:	AI requests intervention
Description:	In some cases, the Local AI system will not know how to proceed. It will then request an intervention from a physician, who will make a decision.
Primary Actor:	Physician

Preconditions:	No feedback can be given to the patient because the Local AI system does not know how to proceed.
Postconditions:	A physician decides how the AI system should proceed.
Triggers:	• The Local AI system does not know how to proceed. • The Local AI system does not know how to proceed. • A physician is contacted and makes a decision.
Main Success Scenario:	• The system can proceed with giving feedback to the patient.
Extensions:	-
Frequency of Use:	• Depends on the conditions.
Status:	Final
Owner:	Philips
Justification:	Several situations can arise (the Local AI model does not converge, there is an error in the system, there is an error in the data, unforeseen technical errors) that cause the AI system to not know how to proceed, requiring the intervention of a physician.

TRUSTWORTHINESS IN HEALTHCARE USE CASE

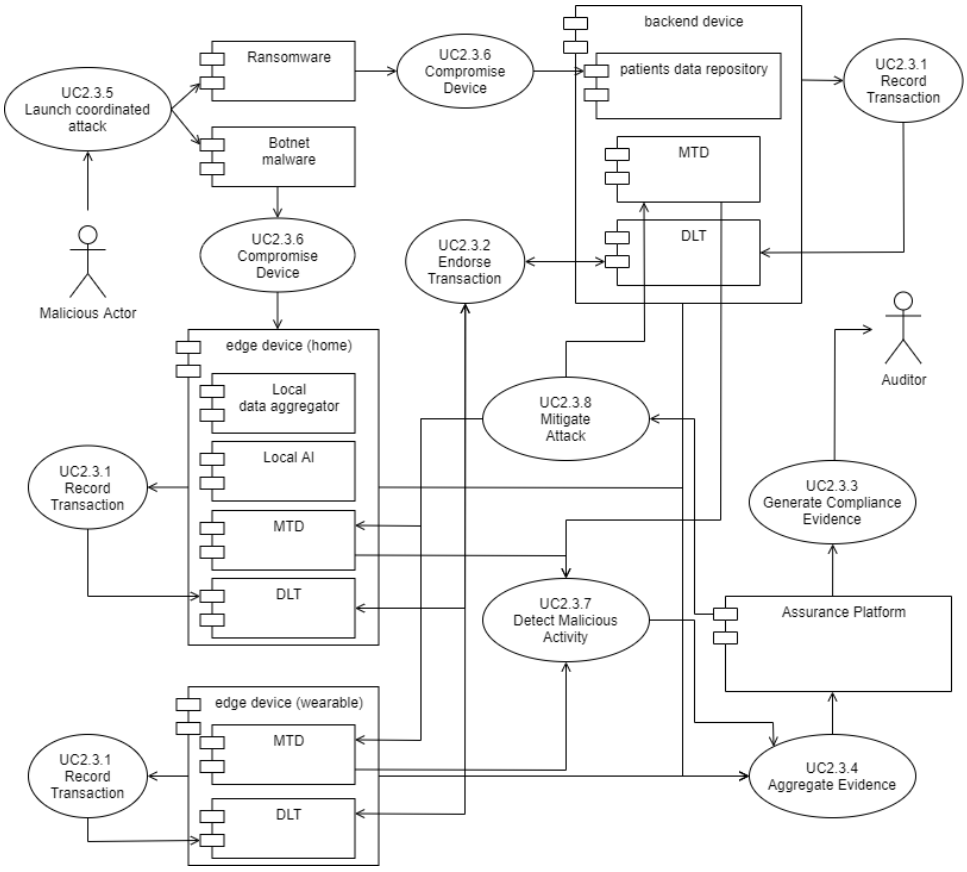

Figure 6: Use Case Diagram Trustworthiness in Healthcare Use Case

ID:	UC2.3.1
Title:	DLT transaction record
Description:	Record important events on the shared Ledger
Primary Actor:	DLT components
Preconditions:	System is authorized and operates normally
Postconditions:	All trust-pertinent events are recorded, to be sent for endorsement to peers
Triggers:	Any component (inter)actions and events that are recorded to the DLT
Main Success Scenario:	1. One of the monitored trust-related events takes place in one of the devices (edge or backend) and monitored components (e.g., DLT, MTD). 2. The corresponding DLT component creates a corresponding entry (transaction) for the ledger

Extensions:	Because of scalability issues of DLT, the data can be recorded in distributed storage, for example, IPFS, and just stored hashed of data in the distributed ledger.
Frequency of Use:	Continuous: DLT app is running during the whole use case execution. Whenever a trust-pertinent event takes place in any of the devices integrating DLT capabilities.
Status:	Final
Owner:	AAU
Justification:	Trustworthiness is important for health care data/information exchange. Recording in the ledger is a basic operation of DLT.

ID:	UC2.3.2
Title:	DLT transaction record endorsement
Description:	Approval (endorsement) of transaction by peers
Primary Actor:	DLT components
Preconditions:	UC2.3.1 has taken place
Postconditions:	All trust-pertinent events are recorded and sent for endorsement to DLT
Triggers:	Creation of a new transaction record by one of the DLT components
Main Success Scenario:	1. A newly created record is transmitted to the peers' network for endorsement 2. Peers endorse transaction 3. The transaction is added to the DLT.
Extensions:	The endorsement of transactions could be upgraded with various requirements of end-users or devices to guarantee the privacy and security.
Frequency of Use:	Continuous: DLT app is running during the whole use case execution. Whenever a trust-pertinent event takes place in any of the devices integrating DLT capabilities.
Status:	Final
Owner:	AAU
Justification:	Trustworthiness is important for health care data/information exchange. Approving transactions is a basic operation of DLT.

ID:	UC2.3.3
Title:	Generate Compliance Evidence
Description:	An auditor requests compliance evidence and the system provides them.
Primary Actor:	Security Assurance Platform
Preconditions:	System is authorized, operates normally, and Assurance Platform is able to aggregate evidence (UC2.3.4)

Postconditions:	Compliance evidence is provided to the Auditor
Triggers:	Auditor request
Main Success Scenario:	1. An auditor requests compliance evidence from the Security Assurance Platform 2. The Security Assurance Platform aggregates all relevant records 3. The compliance report is provided to the auditor
Extensions:	Can be extended to generate different kinds of compliance evidence (tailored to different regulations etc.).
Frequency of Use:	Whenever a trust-pertinent event takes place in any of the devices integrating DLT capabilities. Error: Evidence generated are not pertinent to requested compliance requested
Status:	Final
Owner:	SANL
Justification:	Compliance audits may or may not happen in the healthcare domain (and are, typically, not regularly carried out). But it is important to be able to provide such evidence when needed.

ID:	UC2.3.4
Title:	Aggregate Evidence
Description:	Security Assurance Platform aggregates all evidence needed for assessment and compliance certification
Primary Actor:	Security Assurance Platform
Preconditions:	System is authorized and operates normally
Postconditions:	All relevant evidences are aggregated at the Security Assurance Platform database
Triggers:	Any trust-pertinent event
Main Success Scenario:	1. A trust pertinent event takes place in one of the IntellIoT components (edge or backend) 2. Event captors capture details of the event and relay it to the Security Assurance Platform 3. The Assurance Platform aggregates all relevant evidence, ingesting it in relation to its assurance model, and storing it in the monitoring database.
Extensions:	Can be extended to aggregate different kinds of monitoring events / evidence. Error: Identified events are not in line with (correctly mapped to) the specified assurance model.
Frequency of Use:	Whenever a trust-pertinent event takes place in any of the devices integrating event captors.
Status:	Final

Owner:	SANL
Justification:	The operation of the assurance platform relies on this evidence aggregation.

ID:	UC2.3.5
Title:	Launch Coordinated Attack
Description:	A malicious actor launches a coordinated attack against IntellIoT deployment
Primary Actor:	Malicious actor
Preconditions:	The IntellIoT deployment is targeted by a malicious actor, who manages to identify exploitable vulnerabilities.
Postconditions:	An attack is launched on one or more IntellIoT components, using a combination of vulnerabilities/attack vectors.
Triggers:	Attack on IntellIoT assets
Main Success Scenario:	1. A malicious actor compromises or otherwise gains access in one of the edge IntellIoT assets in the patient's premises 2. The malicious actor also manages to compromise or otherwise gain access to the IntellIoT backend (clinician-side)
Extensions:	Can be extended to cover more complex attacks.
Frequency of Use:	Refers to system misuse
Status:	Final
Owner:	SANL
Justification:	Emulating a potential attacker's capabilities will help in ensuring appropriate defense mechanisms are successfully developed and tested.

ID:	UC2.3.6
Title:	Compromise Device
Description:	Compromise of IntellIoT assets at edge and/or backend instances
Primary Actor:	Malicious actor
Preconditions:	UC2.3.5 has taken place
Postconditions:	Edge and backend instances of IntellIoT are compromised and infected with malware.
Triggers:	Successful attack on IntellIoT assets
Main Success Scenario:	• Malicious actor leverages his access to compromised edge (client-side) assets to deploy a malware (botnet malware) • Malicious actor leverages his access to compromised backend (clinician-side) assets to deploy a malware (ransomware malware)

Extensions:	Can be extended to different types of malware or other types of attacks (tampering attacks, eavesdropping etc.)
Frequency of Use:	Refers to system misuse
Status:	Final
Owner:	SANL
Justification:	To emulate an attacker's actions after successfully compromising the system, and ensuring the corresponding protection mechanisms are appropriately developed and tested.

ID:	UC2.3.7
Title:	Detect Malicious Activity
Description:	Detection of malicious activity in edge and backend instances
Primary Actor:	MTDs
Preconditions:	UC2.3.6 has taken place (malicious activity in IntellIoT assets)
Postconditions:	Malicious activity is detected in edge and/or backend instances and relayed to the Security Assurance Platform
Triggers:	Malicious activity
Main Success Scenario:	1. Security mechanisms are able to detect indicators of malicious activity in edge (patient-side) IntellIoT deployment (malware activity on the network, in this case) 2. Security mechanisms are able to detect indicators of malicious activity in backend (clinician-side) IntellIoT deployment (ransomware activity on patient data repository storage, in this case) 2. 3. Upon detection, evidence of malicious activity (at edge and backend) is relayed to the Security Assurance Platform
Extensions:	Can be extended to include detection of attacks by other trust components (e.g., Trust IDS) Error 1: Malicious activity remains undetected (false negative) Error 2: Normal activity is erroneously detected as malicious (false positive)
Frequency of Use:	Whenever malicious activity takes place on IntellIoT assets
Status:	Final
Owner:	TSI/SANL
Justification:	It is important to promptly detect malicious activity in the sensitive healthcare environment

ID:	UC2.3.8
Title:	Mitigate Malicious Activity
Description:	Mitigation of malicious activity in edge and backend instances
Primary Actor:	Security Assurance Platform
Preconditions:	UC2.3.7 has taken place (malicious activity has been detected)
Postconditions:	Malicious activity is mitigated through MTDs reconfiguration
Triggers:	Detection of malicious activity
Main Success Scenario:	1. The Security Assurance Platform receives intrusion/compromise indicators from the backend and/or edge security mechanisms 2. The Security Assurance Platform ingests evidence of intrusion/compromise 3. The Security Assurance Platform generates mitigation plan (new configuration) to isolate compromised node or block malware activity 4. New configuration is relayed to corresponding security mechanism(s), 5. Changes are applied, mitigating Malicious activity
Extensions:	Can be extended to include mitigation of additional number of attacks, also involving additional security mechanisms Error 1: One or more involved entities are not included in the asset model of the Assurance Platform Error 2: A mitigation plan cannot be identified for specific type of attack Error 3: The receiving node cannot apply new configuration Error 4: The new configuration fails to mitigate malicious activity
Frequency of Use:	Whenever malicious activity takes place on IntellIoT assets
Status:	Final
Owner:	SANL/TSI
Justification:	The system should be able to automatically respond to at least a basic set of such attacks, without requiring expert input (medical personnel and patients cannot be assumed to have technical expertise).

4.1.3. MANUFACTURING USE CASE

In this section, the steps shown in the use case diagrams known from IntellIoT deliverable D2.1 (see Figure 7, Figure 8, Figure 9, Figure 10 and Figure 11) are described in more detail. Therefore, unique numbers have been added to each step in the use case diagrams. Hereafter, requirements derived from the steps are described in Section 4.2.

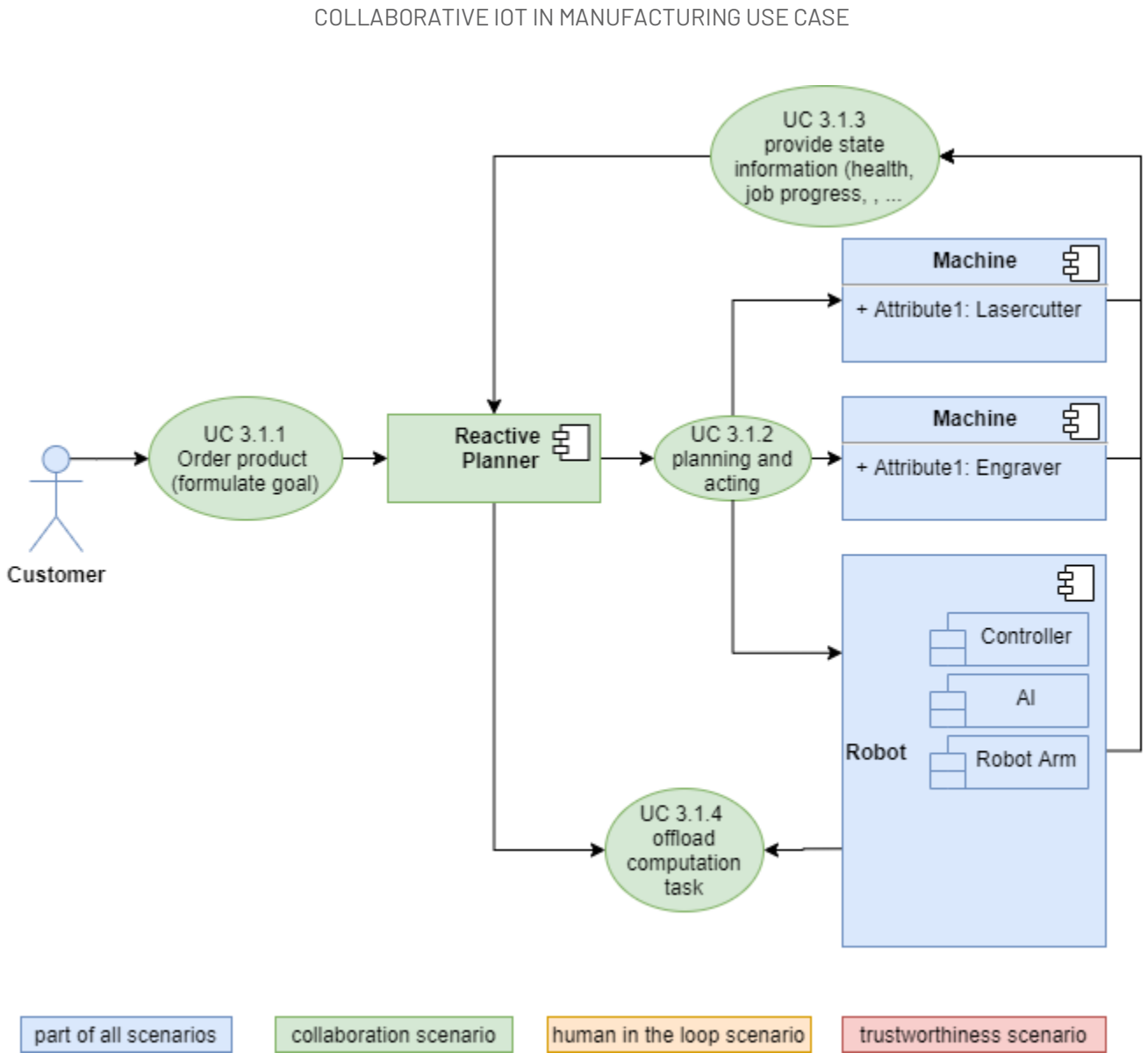

Figure 7: use case diagram collaboration

ID:	UC3.1.1
Title:	Order product (formulate goal)

Description:	The customer orders the product by using the End User Goal Specification Interface to formulate a production goal. The formulated goal is transmitted to the distributed Hypermedia MAS Infrastructure.
Primary Actor:	Customer
Preconditions:	The customer is able to access the system; the system is ready to receive new production goals; there is no precondition regarding whether or not the system is currently producing a product.
Postconditions:	The system starts to produce the specified product; the system is ready to receive new production goals; the customer is informed that the system is working.
Triggers:	The customer's desire to have a product produced.
Main Success Scenario:	The system has successfully received the production goal and was able to syntactically interpret it. The Hypermedia MAS Infrastructure returns an acknowledgement to the customer. At this stage, no semantic interpretation of the production goal has taken place.
Extensions:	If a syntactically ill-formed production goal has been transmitted to the system, the customer is alerted about this.
Frequency of Use:	With every goal formulated by the customer.
Status:	Final
Owner:	HSG / Siemens
Justification:	The system is unable to achieve its core function of producing the product without the specification of the product.

ID:	UC3.1.2
Title:	Planning and Acting
Description:	Given the specification from the End-user IDE, the agents form a choreography to achieve the production goal.
Primary Actor:	Hypermedia MAS Infrastructure
Preconditions:	The Hypermedia MAS Infrastructure has received a syntactically valid production goal. The Hypermedia MAS Infrastructure has been configured regarding the agents and their organization and procedural knowledge.
Postconditions:	The agents on the Hypermedia MAS act out the choreography to achieve the goal.
Triggers:	A production goal has been transmitted by the Goal Specification Front End.
Main Success Scenario:	The Hypermedia MAS Infrastructure is modeled as a multi-agent organization, which enables the coordination of the individual agents towards the common production goal. The Hypermedia MAS Infrastructure searches the hypermedia-based production floor for available artifacts. Each agent synthesizes a part of the production plan given the configuration of the agent system. Plans are synthesized in a non-blocking manner to

	enable the simultaneous planning and acting-out of plans. For the acting-out, agents that operate the identified artifacts are now executing their tasks according to the multi-agent organization defined for the type of production goal that had been formulated by the customer.
Extensions:	If the Hypermedia MAS Infrastructure is unable to find a solution for the given production goal, it can request support from a human plant operator, machine operator, or customer.
Frequency of Use:	With every production goal formulated by the customer.
Status:	Final
Owner:	HSG / Siemens
Justification:	The system is unable to achieve the user goal without the agents cooperating to achieve it.

ID:	UC3.1.3
Title:	Provide state information
Description:	Machines and robots provide information on their own state to the Hypermedia MAS Infrastructure. State information could be, for example, health state, progress on a job, events, maintenance requests etc.
Primary Actor:	The machine or robot itself, which pushes state changes unasked to the Hypermedia MAS Infrastructure.
Preconditions:	Machine / robot is authenticated and known to the Hypermedia MAS Infrastructure.
Postconditions:	Hypermedia MAS Infrastructure is up to date on the state of the concerned machine / robot.
Triggers:	Events on the machine, e.g., an upcoming maintenance request. Start or end of a job. Keepalive updates every predefined time interval, in order to detect lost machines and get updates on the progress of long-lasting jobs.
Main Success Scenario:	Trigger is active. Machine repeatedly sends state information to Hypermedia MAS Infrastructure until it receives an acknowledge. Timer for keepalive updates is reset.
Extensions:	Communication to Hypermedia MAS Infrastructure is not possible – machine will repeatedly send keepalive updates.
Frequency of Use:	At least in the defined interval for keepalive state updated, additionally for events.
Status:	Final
Owner:	Siemens

Justification:	The Hypermedia MAS Infrastructure is unable to react on the plant state without state information.

ID:	UC3.1.4
Title:	Offload computation task
Description:	Computation tasks, required by production steps, will be transferred to the corresponding app on the edge device.
Primary Actor:	AI on robot or Hypermedia MAS Infrastructure
Preconditions:	• The edge app, suitable for task offloading, is deployed on the edge device • The production machine and the edge device are connected via a network • The production machine is authorized as a user • A production or planning process is in progress
Postconditions:	1. The computation result is transferred to the requester 2. The edge app is ready to accept further offloading tasks
Triggers:	A certain production or planning steps is due, which requires offloading capabilities
Main Success Scenario:	• AI on robot or Hypermedia MAS Infrastructure creates a request for task offloading. This may include instructions, scripts and input data. • The request is routed to the edge app • The computation task is executed • Computation results and status are returned.
Extensions:	• If the execution of the tasks fails because of a software error, a corresponding error message is propagated back to the client. • On a system error, because of a failing network link or failing edge device or an overload, the execution of the task is transferred to another edge device • If the requesting production machine is moving outside the realm of a specific edge device, computation tasks are transferred to another edge device.
Frequency of Use:	continuous
Status:	Final
Owner:	Siemens
Justification:	Required for network and resource optimization as well as edge computing

ID:	UC3.1.5
Title:	Compute tasks locally
Description:	Local AI computes the tasks and determines how to carry out the production.
Primary Actor:	AI on robot

Preconditions:	1. The information related to the task is available at the robot 2. The input sensory data is available at the robot 3. A trained AI model is available at the robot
Postconditions:	The robot has the knowledge to proceed with the production task
Triggers:	Arrival of production item at the robot
Main Success Scenario:	• AI computes the input sensory data and identify next production steps (e.g., where to grab the workpiece and identify the usable area) • The production steps are delivered to robot arm
Extensions:	• If the computations cannot be carried out locally, task offloading event is triggered.
Frequency of Use:	continuous
Status:	Final
Owner:	UOULU
Justification:	To enable self-aware and autonomous behavior.

HUMAN IN THE LOOP IN MANUFACTURING USE CASE

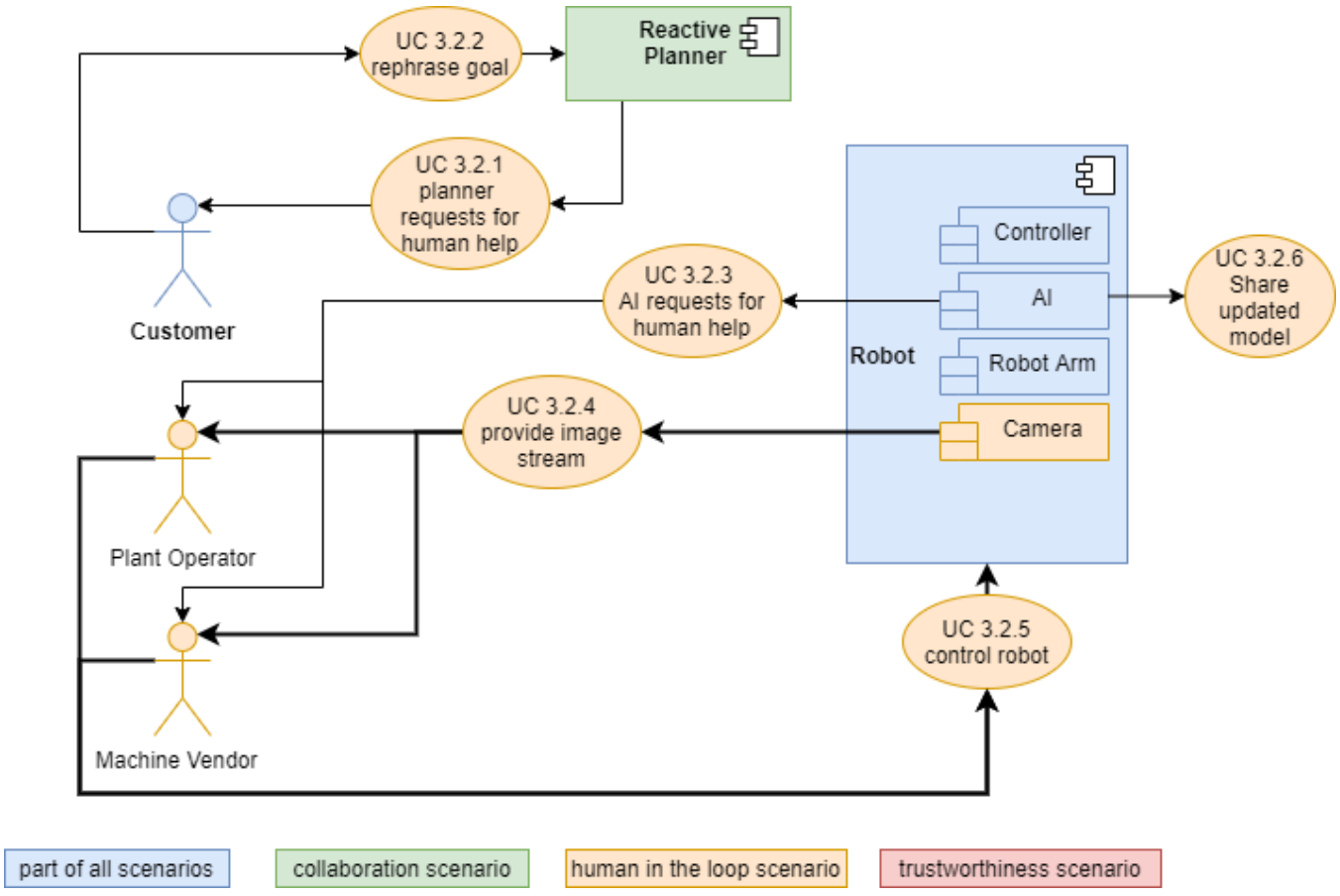

Figure 8: use case diagram human in the loop

ID:	UC.3.2.1
Title:	Planner requests for human help
Description:	Hypermedia MAS Infrastructure is unsure about how to interpret a customer's goal and requests help from the human customer.
Primary Actor:	Hypermedia MAS Infrastructure (Agent or EUP Back End)
Preconditions:	A customer has formulated a goal. Hypermedia MAS Infrastructure has knowledge about machines in the plant and their capabilities. Hypermedia MAS Infrastructure is unsure about how to interpret the customer's goal.
Postconditions:	Human in the loop has solved the issue and the process plan is computed.
Triggers:	Hypermedia MAS Infrastructure detects inability to fulfill customer's goal.
Main Success Scenario:	• Hypermedia MAS Infrastructure requests human help • Human customer receives help request and accepts

	• Human operator rephrases goal using the Goal Specification Front End
Extensions:	Human operator is not able to help and forwards the request to an operator or machine owner.
Frequency of Use:	In worst case, it could occur for every goal formulated by a customer. The goal is to have it occurring much less frequent.
Status:	Final
Owner:	Siemens
Justification:	The planner is unable to automatically complete the customer's goal

ID:	UC3.2.2
Title:	rephrase goal
Description:	The customer is given the opportunity to rephrase the production goal.
Primary Actor:	Customer
Preconditions:	The Hypermedia MAS Infrastructure was unable to find a suitable orchestration plan when given a specific production goal.
Postconditions:	The Hypermedia MAS Infrastructure receives a different production goal.
Triggers:	The Hypermedia MAS Infrastructure being unable to find a suitable orchestration plan.
Main Success Scenario:	The Hypermedia MAS Infrastructure informs the customer that it was unable to find a behavior that would reach a given production goal. The customer inputs a new, different, production goal, or a production goal that is more specific, and transmits this goal to the Hypermedia MAS Infrastructure.
Extensions:	
Frequency of Use:	Whenever the Hypermedia MAS Infrastructure is unable to find a suitable orchestration plan.
Status:	Final
Owner:	HSG
Justification:	The planner is unable to automatically complete the customer's goal, therefore action is required by the customer in order to provide a different production goal.

ID:	UC.3.2.3
Title:	AI requests for human help
Description:	AI is unsure about how to grab a workpiece and requests help from a human plant operator.
Primary Actor:	Local AI on the robot or AI offloaded to the edge

Preconditions:	A transport job has been assigned to a Robot. The robot has reached the location where a workpiece shall be picked or placed, AI is unsure how to execute the job.
Postconditions:	Human in the loop has solved the issue and the process continues.
Triggers:	AI detects insufficient confidence level on a decision how to pick or place a workpiece.
Main Success Scenario:	AI requests human help. Human operator receives help request and responds positively. Human operator receives image stream and controls robot. Human operator solves blocking.
Extensions:	Human operator is not able to help and forwards the request to another operator, machine owner or customer.
Frequency of Use:	In worst case, it could occur for every pick and place operation. The goal is to have it occurring much less frequent, additionally decreasing by learning from human help.
Status:	Final
Owner:	Siemens
Justification:	If the robot is unsure how to grab or place a workpiece, it needs help to avoid blocking of the production process.

ID:	UC3.2.4
Title:	Provide image stream
Description:	A human assistance requires to see the scene in order to provide instructions to the robot. Image streams may also be integrated into AR/VR googles and through the AR/VR control, the robot camera may move the image source. A tactile connection is provided by the 5G RRM between the human operator and the camera on the robot, according to the QoC/QoS provisions and the requested frame per second (FPS). According to the QoC/QoS, the feedback to the robot will take different strategies.
Primary Actor:	The 5G RRM actuates the camera on the robot according to the required Level-of-Service (LoS) and the network capacity available by the 5G network. The camera provides the image stream according to the requested parameters.
Preconditions:	The image stream was only used locally by the robot AI. The robot AI requests human assistance, which requires image streams to be transmitted to the human.
Postconditions:	Image streams are provided to the human assistance, which enables it to provide the right action to the robot.
Triggers:	1. Human assistance to provide advice to the robot by the Hypermedia MAS 2. Human supervision to monitor the robot operation by the Hypermedia MAS
Main Success Scenario:	The human assistance requests the 5G RRM to have image streams from the robot camera to be transmitted to its location. The 5G RRM requests the opening of a tactile link to the robot camera to the 5G network, which according to the conditions and configuration will either grant it or provide a reduced capacity. Accordingly, the 5G RRM actuates the

	camera with the appropriate stream parameters as well as target destination of the stream to match the offered 5G capacity. The camera initiates a direct stream transfer to the human assistance.
Extensions:	1. The human assistance is actually located next to the robot. A direct D2D link is provided by the 5G RRM between the robot and the human assistance. 2. A match between the required FPS and 5G capacity cannot be found. 3. The supported FPS is not sufficient for the human assistance to understand the context and help.
Frequency of Use:	Often at the beginning, as the robot AI is expected to regularly require assistance, less once the robot AI will have learned enough.
Status:	Final
Owner:	EURECOM
Justification:	Video streams are a direct request for human assistance. Failure to provide the appropriate video stream will impact the success of the UC.

ID:	UC3.2.5
Title:	Control robot
Description:	The human operator gets control over the arm and moves it remotely.
Primary Actor:	The human operator
Preconditions:	The robot has requested help. HIL Service has chosen a human to help, which is ready to take over. The video stream is up.
Postconditions:	The workpiece has been handled in the required way and the robot is ready to take new commands.
Triggers:	The AI on the robot is uncertain for its decision
Main Success Scenario:	1. A workpiece is to be handled. 2. The constrained AI does not know how to take the workpiece and ask for help to the operator. 3. The operator takes control over the robot. 4. The human operator moves the robot remotely and handles the workpiece. 5. The human operator places the workpiece remotely.
Extensions:	Error 1: The commanded position from the human operator is not possible.
Frequency of Use:	Every time AI on robot needs help handling a workpiece.
Status:	Final
Owner:	Siemens
Justification:	The human operator intervenes as the AI on the robot cannot produce an acceptable solution

ID:	UC3.2.6
Title:	Share updated model
Description:	An AI model has been updated and might be helpful to other robots or entities. The Infrastructure Assisted Knowledge management (IAKM) entity is in charge of supervising the sharing of the updated model. Either it can identify the interested party and provide such information to the robot for a direct exchange. Or it will store the updated model on its database to share with other entities indirectly.
Primary Actor:	The IAKM
Preconditions:	An AI model located at one edge entity (e.g., robot) has been updated with new knowledge. At least one interested entity subscribed to the IAKM to receive an updated version of a given model with its semantic description.
Postconditions:	The updated AI model is either stored on the IAKM database or hosted by other entities requiring it.
Triggers:	The AI model is updated according to an updated context.
Main Success Scenario:	1. the descriptive parameters of the updated AI model are updated (new context, new knowledge, updated version) 2. the entity hosting the updated model sends a push request to the IAKM with the updated model and its semantic description 3. the IAKM matches the semantic description of the updated model to any active model update subscription. If one is found, it pushes the updated model to the subscribing entities. 4. any entity having subscribed to the particular model update receives it.
Extensions:	1. no model update subscription matches the semantic description of the model. The updated model is stored in the database but not shared. 2. the model update semantic description does not match any entry in the IAKM database. A new entry is created. A separate process in the IAKM is in charge of detected duplicate models. 3. The entity hosting the updated model bypasses the IAKM and handle the subscription and publication of model update itself. 4. Subscription to updated model is open to external entities or partner of the Factory.
Frequency of Use:	Often at the beginning, as AI models are expected to be frequently updated and shared; The frequency also depends on the number of entities in the UC and their potential interest in that model.
Status:	Final
Owner:	EURECOM
Justification:	Factories may have various robots facing similar challenges. Once the AI of one robot has been updated, all robot in the factory should also be updated.

HUMAN IN THE LOOP IN MANUFACTURING USE CASE

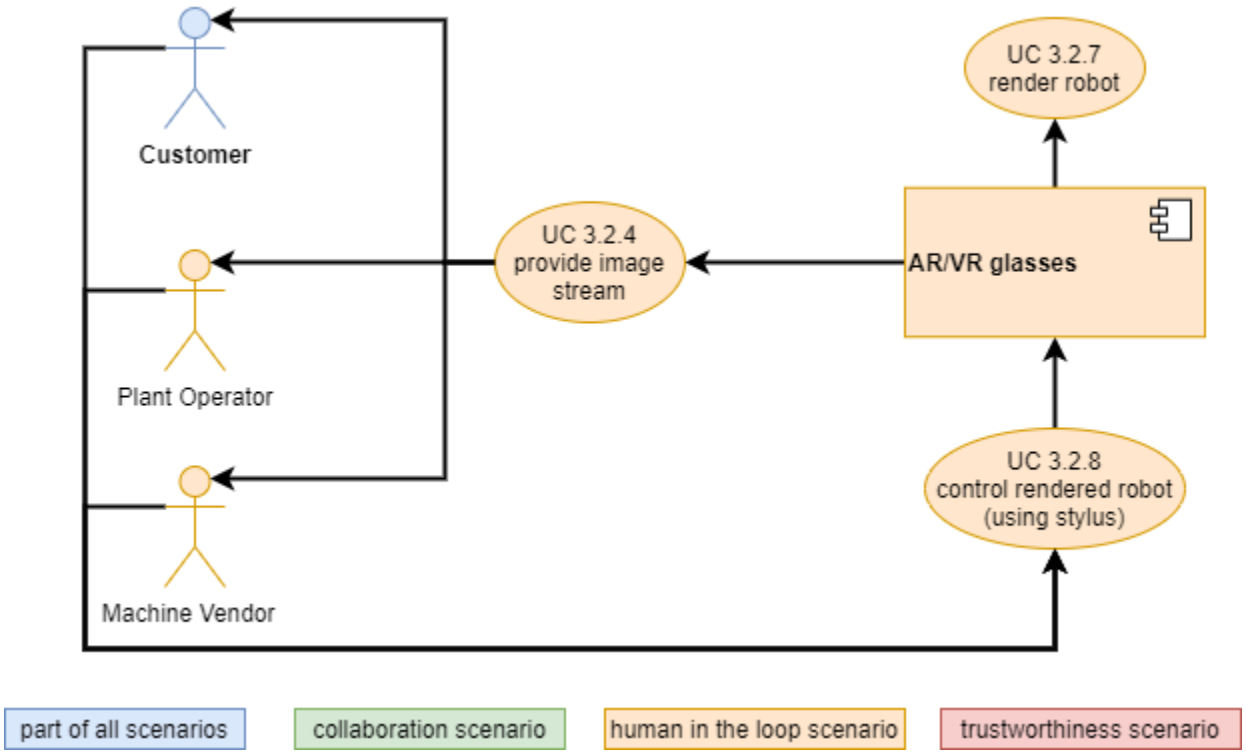

Figure 9: use case diagram human in the loop with rendered robot

ID:	UC3.2.7
Title:	Render robot
Description:	A digital twin of the robot and its near environment in its current state is available for the human operator (Human-in-the-loop)
Primary Actor:	The human operator using an Augmented Reality HMD (e.g., Microsoft HoloLens 2)
Preconditions:	The environment data needs to be available (low latency, high bandwidth)
Postconditions:	The human operator is experiencing a real-time updating digital twin and its near environment.
Triggers:	When the human operator is physically "far" away and needs to monitor or control the robot
Main Success Scenario:	• Human operator is receiving a message in his AR Experience, that a robot needs his attention • Human operator is requesting the environmental view feed of this specific robot • Operator can fully look around the robot in order to visually analyze the situation
Extensions:	Error 1: Environmental video feed result in heavy delay for the User (high latency) Error 2: Environmental video feed has bad resolution (low bandwidth)

Frequency of Use:	The current assumption is, that human interaction is frequently needed during the early stages, but will steadily decrease over time, as the AI is a self-learning system.
Status:	Final
Owner:	HOLO
Justification:	Human interaction would be nearly impossible without a rendered robot.

ID:	UC3.2.8
Title:	Control rendered robot
Description:	The human operator can control the holographic digital twin of the robot by using a special interaction tool (Stylus).
Primary Actor:	The human operator wearing an AR HMD and using a special interaction tool (Stylus).
Preconditions:	The AR experience needs to have a real time connection to the robot (upstream and downstream).
Postconditions:	The new state of the robot, which was intended by the human operator.
Triggers:	The human operator wants to set the robot position into a new state
Main Success Scenario:	1. The Operator is requesting direct control of the robot (Holographic robot is in sync with real robot) 2. The Operator can control the robot movement and set the robot into his intended new state 3. Once the action was successful the human operator will give control back to the robot's AI
Extensions:	Error 1: environmental video feed result in heavy motion sickness for the User (high latency) Error 2: environmental video feed has bad resolution (low bandwidth) Error 3: an obstacle is in its way, so the intended state cannot be reached Error 4: the view is blocked so a full analysis is not possible Error 5: the arm cannot be moved into the required position Error 6: the light conditions in the robot's room distorting the displayed colors and in result hinder the human operator from viewing all relevant details
Frequency of Use:	The current assumption is, that human interaction is frequently needed during the early stages, but will steadily decrease over time, as the AI is a self-learning system.
Status:	Final
Owner:	HOLO
Justification:	Without the interface that allows passing location data from the rendered robot to the real robot, human interaction would be impossible from a remote location.

TRUSTWORTHINESS IN MANUFACTURING USE CASE

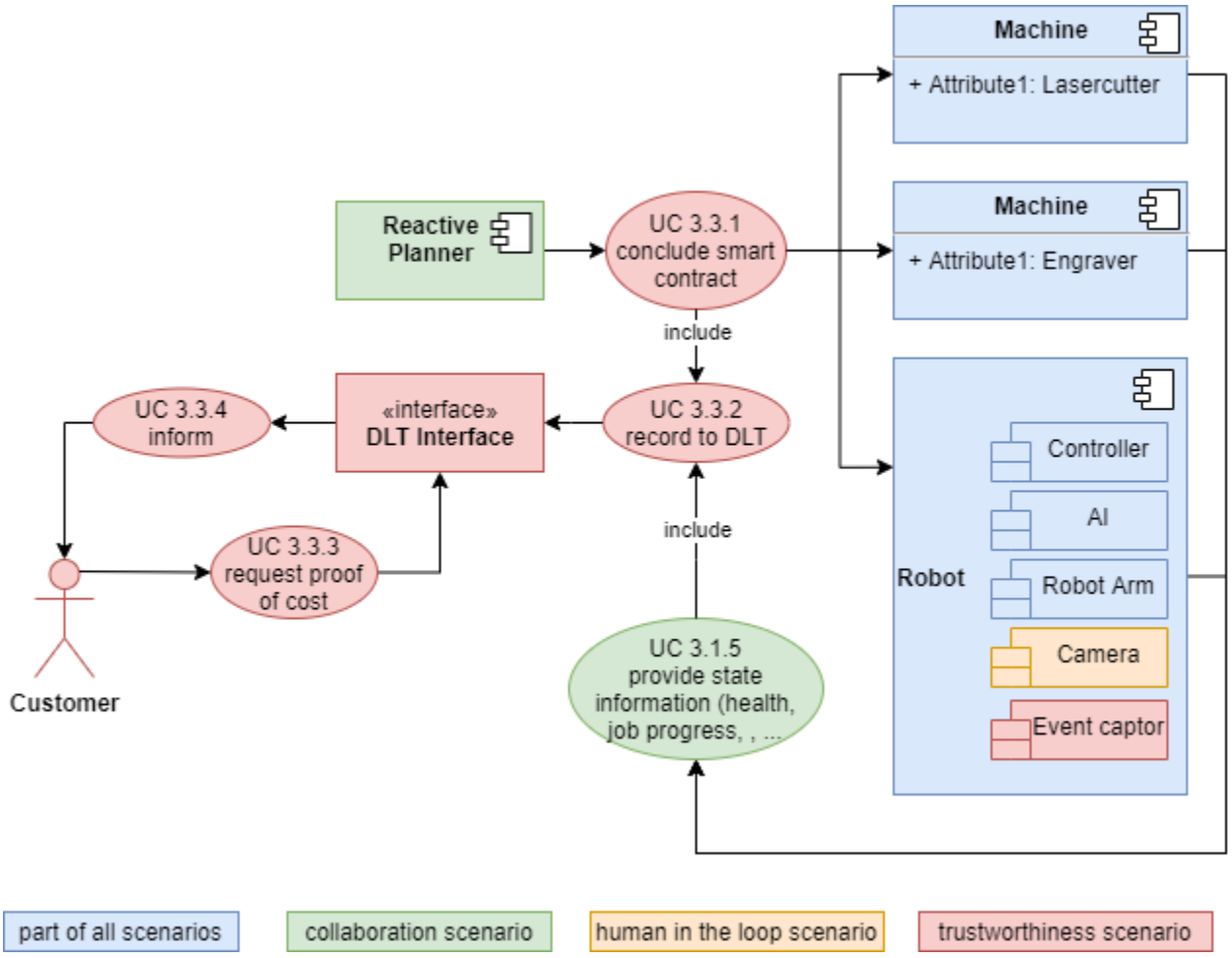

Figure 10: use case diagram trustworthiness – proof

ID:	UC3.3.1
Title:	Conclude smart contract
Description:	Smart contracts are initially generated by the human administrator of the system with rules and agreements for participants, for example machines and robots. Then, whenever an agent commits to a task it provides information about agreements to import into smart contracts. The code of smart contract and the agreements contained therein exist across a distributed, decentralized Blockchain system. The controls and the execution, and transactions are trackable and irreversible in the ledger.
Primary Actor:	The entities including an Agent, customers, machines and robots are actors in the system. The actors interact via wired or wireless connectivity.

Preconditions:	First, actors can communicate with others via communication channels and have the same DLT infrastructure. Second, the lightweight version of DLT is installed in robots and machines so the actors
Postconditions:	After the Agent in the Hypermedia MAS infrastructure creates smart contracts, the smart contracts are stored and synchronized to all the DLT nodes in the networks.
Triggers:	An agent in the Hypermedia MAS Infrastructure has a new task to a machine or robot, or agreement that needs to be announced: this will generate a new contract and publish to the ledger.
Main Success Scenario:	• An Agent in the Hypermedia MAS Infrastructure has a task that it wants to delegate to a machine or robot. Then, the Agent generates a new smart contract, and stores the contract in the ledger of the DLT node. The DLT node which stands for the Agent synchronizes the contracts to the rest of networks. • The DLT nodes of every actors now have similar contracts to interact and operate activities.
Extensions:	
Frequency of Use:	When the Agent defines a new task to be delegated to the actors, for example, machines, robots. Then, the Hypermedia MAS Infrastructure will generate smart contracts for executing the job.
Status:	Final
Owner:	AAU
Justification:	The smart contract is a vital factor of distributed and trust network where the involving entities acts based on agreements defined in smart contracts.

ID:	UC3.3.2
Title:	Record data to the DLT
Description:	After generating the smart contracts, all involved DLT nodes record the smart contracts and all operations to the ledger. The information related to the history of activities and operations are stored in the ledger, and the customers can access to the ledger to get the related information.
Primary Actor:	The entities including an Agent, customers, machines and robots are actors in the system. The actors interact via wired or wireless connectivity.
Preconditions:	The Agent created smart contracts to control the operations of machines and robots. Then, these machines and robots act as agreements defined in the contracts.
Postconditions:	In the final state, the operations and results from all actors are recorded and published in the distributed ledger. The customers can access to this information via interfaces.
Triggers:	The actors complete tasks or jobs and start publishing to the ledger.

Main Success Scenario:	• After the Agent generates smart contracts and synchronizes with other DLTs nodes of machines and robots. All the actors operate autonomously and start publishing their history of operations to the ledgers. • The data and information of actors are formatted into DLT transactions which are encrypted and signed by signatures of actors to guarantee the security and trustworthiness. • The signed transactions are then published to the distributed ledger and arranged in blocks. • Through the mining process of DLT nodes to verify the trustless of transactions in blocks, then the blocks are broadcasted to all the DLT nodes in the network via consensus protocols. • Finally, the data from actors is verified and published in the distributed ledger for further actions.
Extensions:	This scenario can be extended in the case of using multiple types of DLTs. Each actor can have different resources as well as nature capacities, so that they can use different types of DLTs for operations. The combination of multiple DLTs, for example, private DLTs and public DLTs could be considered.
Frequency of Use:	Every operation from actors is stored in the distributed ledger, so this action will happen frequently.
Status:	Final
Owner:	AAU
Justification:	Recording to the DLT is the basic operation of DLT and smart contracts.

ID:	UC3.3.3
Title:	Request proof of cost
Description:	The customers after using the services provided by the system might request for the proof of operation cost and evident of exchanges.
Primary Actor:	The customers, the agents, machines and robots are primary actors.
Preconditions:	After the Agent, machines and robots complete a required task from customers, they form the transactions and publish the results to distributed ledger. The customers can access and view the published results using his laptop or mobile device with DLT interface
Postconditions:	The customer needs to verify the trustless and verify the history of operation cost of other actors.
Triggers:	The customer sends a request to the ledger for proof of operations costs as well as historical information of a required job.
Main Success Scenario:	• All the operations of machines and robots are recorded in the distributed ledger and available for customers to check the correctness. • The customers can request for the proofs or evidence that demonstrate the operations and activities of machines/robots during the contract time between customers and Hypermedia MAS Infrastructure.

	• The distributed ledger stores all this information and provides proofs to customers.
Extensions:	The customers receive reports of operations from the Agent, but they want to verify the operations, they can proactively send verification requests to the distributed ledger to ask.
Frequency of Use:	Whenever the customers want to verify the received data/information e.g., in the bill or a report from the owner of the plant
Status:	Final
Owner:	AAU
Justification:	One of the applications of smart contracts is for accountability, where the final phase is the customer requiring the proof-of-cost and the system providing it.

ID:	UC3.3.4
Title:	Inform: the DLT reports the progress or bill of process to customers
Description:	While robots and machines are doing the requested tasks or services defined in smart contracts, and the reports of task progress are generated and available in the distributed ledger. The customers can query the reports about the progress of tasks and jobs via their personal devices such as laptop or mobile devices.
Primary Actor:	Customers.
Preconditions:	The ledger via consensus process knows about the progress of the tasks, and the customer requests a proof-of-cost using his laptop or mobile device
Postconditions:	The customer receives the update via DLT interfaces.
Triggers:	The customer proof-of-cost request.
Main Success Scenario:	1. The ledger has the information about progress of tasks from transactions of machines and robots. 2. The customer receives the update from distributed ledger via DLT interface after requesting a proof-of-cost
Extensions:	To minimize the communication overhead and interaction between customers and DLTs, we can separate the communication into multiple protocols.
Frequency of Use:	For applications which require the confirmation from providers, the confirmation message is important. The frequency of use depends on the type of applications developed in the system.
Status:	Final
Owner:	AAU
Justification:	DLT provides to customers features to query the progress of tasks, and after customer requests for the proof-of-cost, DLT is triggered to send the report to the customers regarding to progress and updates.

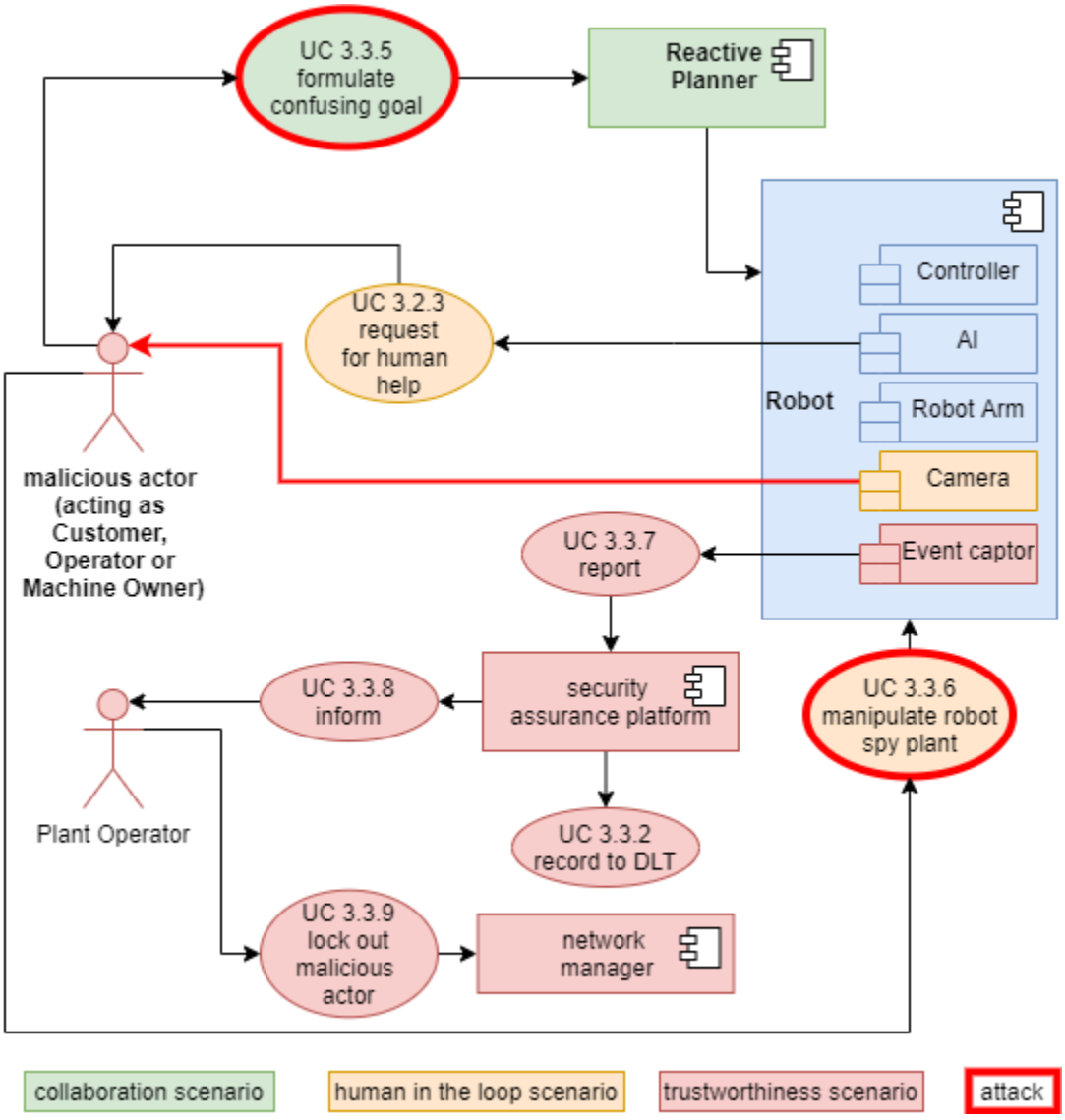

Figure 11: use case diagram trustworthiness – spy

ID:	UC3.3.5
Title:	Formulate confusing goal
Description:	A confusing goal is purposefully formulated, in a way that will necessitate human operator intervention
Primary Actor:	Malicious actor (Customer)
Preconditions:	The system is ready to process customer orders
Postconditions:	The confusing goal is accepted and forwarded for manufacturing

Triggers:	Formulation of confusing goal (UC3.1.1 by malicious actor)
Main Success Scenario:	1. Malicious actor accesses goal formulation front-end as customer 2. Confusing goal is formulated 3. The goal is received by the system and forwarded for manufacturing 4. AI on the robot is facing issues handling the workpiece
Extensions:	Malicious actor could steal and access using access existing customer credentials, editing an existing project accordingly
Frequency of Use:	Refers to system misuse
Status:	Final
Owner:	Siemens / SANL
Justification:	Emulation of system misuse through the formulation of confusing goals will help in developing and testing robust security mechanisms.

ID:	UC3.3.6
Title:	Manipulate robot / spy plant
Description:	Malicious actor controls robot and/or camera to spy the plant or otherwise affect the normal operation of the manufacturing process
Primary Actor:	Robot / Camera (controlled by malicious actor)
Preconditions:	Malicious actor (external or disgruntled employee) has access to operator credentials and human intervention is needed to complete goal (UC3.2.3)
Postconditions:	The control over robot /cameras is exploited to spy plant or otherwise affect normal operation of manufacturing process
Triggers:	UC3.2.3 by malicious actor
Main Success Scenario:	1. Operator (malicious) takes over control of robot to assist in manufacturing process 2. Malicious actor exploits control to move robot (and/or camera) around to monitor (spy) on activities, or to otherwise disrupt the manufacturing process
Extensions:	Scenario could involve spying through robot/camera or disruption of the manufacturing process (damaging other equipment, the manufactured components, or even endanger the safety of human staff in the vicinity).
Frequency of Use:	Refers to system misuse
Status:	Final
Owner:	Siemens / SANL
Justification:	Emulating an attacker's capabilities to ensure appropriate defense mechanisms are developed and tested.

ID:	UC3.3.7
Title:	Report Activity
Description:	Event captors related to robot monitoring detect and report unusual activity
Primary Actor:	Event Captor
Preconditions:	Human intervention to complete goal (UC3.2.4); the latter manipulated by malicious user (UC3.2.5)
Postconditions:	The Security Assurance Platform is notified of suspicious robot activity
Triggers:	Suspicious robot activity/movements
Main Success Scenario:	1. Indicators of suspicious/abnormal robot movements are captured by purpose-deployed event captors 2. Evidence of this activity is relayed to the Security Assurance Platform
Extensions:	Could be extended to cover camera movements Error 1: Event captor fails to detect malicious handling of robot (false negative) Error 2: Event captor detects as malicious a normal activity of robot (false positive)
Frequency of Use:	Refers to system misuse
Status:	Final
Owner:	Siemens / SANL
Justification:	Monitoring of the robotic activities is a welcome feature (as long as it does not interfere with the normal manufacturing/business process).

ID:	UC3.3.8
Title:	Inform Operator
Description:	Operator is informed of malicious activity
Primary Actor:	Security Assurance Platform
Preconditions:	UC3.3.6 has taken place
Postconditions:	The operator has real-time visibility of robot misuse/abnormal activity
Triggers:	Event Captor input (UC3.3.6, UC3.3.6)
Main Success Scenario:	1. Security Assurance Platform ingests event captor alerts / information 2. The evidence is processed using information in the relevant assurance model 3. Resulting information on the event is presented to the operator through the platform's GUI
Extensions:	Error: Information received by event captors cannot be properly ingested/processed due to erroneous or incomplete specification of assurance model
Frequency of Use:	Whenever a trust-pertinent alert is generated by event captors

Status:	Final
Owner:	SANL
Justification:	It is important to provide real-time visibility to the operators of the assurance posture of the manufacturing assets and any related malicious/suspicious activity.

ID:	UC.3.3.9
Title:	Lock out malicious actor
Description:	Plant operator triggers network manager to lock out a malicious actor after security assurance platform informed him of suspicious activities
Primary Actor:	Plant operator
Preconditions:	Security assurance platform got information about suspicious activities (via event captor and has informed plant operator. (UC3.3.7 has taken place)
Postconditions:	Malicious actions countered
Triggers:	Security assurance platform informs plant operator of suspicious activities (UC3.3.7)
Main Success Scenario:	• Plant operator observes warning issues by Security Assurance Platform • Plant operator requests network manager to lock out malicious actor access • Network manager removes access of malicious entities Malicious actor is not able to carry out attack any more
Extensions:	Lock out can focus on access needed to control specific affected robot (at the network level), but also authentication/authorization access of malicious operator's credentials, as well as authentication/authorization level access of malicious customer's credentials.
Frequency of Use:	Whenever suspicious activity is detected by security assurance platform.
Status:	Final
Owner:	TSI / SANL
Justification:	It is important for the operator to be promptly informed and have the means to respond to detected malicious/suspicious activity.

4.2. Functional Requirements

Following the use case scenarios described in the previous section, four main sets of functional requirements are derived. The first encompasses the IntellIoT framework as a whole (General Functional Requirements) and describes those requirements that are to be expected to be fulfilled by the framework regardless of the use-case scenario and are even applicable beyond the scope of the three use-cases. The other three sets of functional requirements are specific to each use-case.

All functional requirements are identified by a unique Requirement ID, so they can be traced within the scope of this deliverable, as well as throughout the development of the framework. Use-case specific functional requirements are also associated with at least one scenario as described in Section 4.1. Lastly, each functional requirement is appointed a Level, based on a MUST/SHOULD/MAY rating. Functional requirements marked as "MUST" are crucial and obligatory to be implemented. Those marked as "SHOULD" describe functionalities that are considered welcome features and the ones marked as "MAY" are optional ones.

It should be noted that the Functional Requirements described in this document, list the user-level requirements. As such, they describe user visible functionalities that the IntellIoT framework must, should or may provide. Functional requirements that describe functionalities and organizations that are internal to the functioning of the system will not be covered in this document. These functionalities, named Technical Functionalities, will be expressed in Deliverable D2.3 describing the architecture of the IntellIoT framework.

4.2.1 GENERAL FUNCTIONAL REQUIREMENTS

The general functional requirements of IntellIoT are provided in Table 2. General Functional Requirements of IntellIoT

Table 2. General Functional Requirements of IntellIoT

Requirement ID	Requirement	Level
GFR.1	When an engineer intends to setup or re-engineer the Hypermedia MAS, the Web-based IDE for Hypermedia MAS shall provide an interface to configure the agent organization and to specify procedural knowledge of agents, using an end-user programming abstraction. This IDE shall make use of the Hypermedia MAS Infrastructure to enable the engineer to monitor the current state of the Hypermedia MAS (i.e., agents, agent organizations, procedural knowledge) and of the environment (i.e., services with their capability descriptions).	MUST
GFR.2	When the operator indicates that he has finished the description of the goal, the Goal Specification Front End shall send the specification of the goal to the Hypermedia MAS.	MUST
GFR.3	When the system has successfully received a task from a user, the system shall inform the user and start executing the assigned task.	MUST
GFR.4	When the system has successfully completed a (long-running) task, the system shall inform the user that tasked it that the task has been finished.	MUST
GFR.5	While the system is performing its mission, the sensors and other data-gathering devices employed must frequently provide data/transactions to be recorded in the DLT that is hosted in the edge infrastructure.	MUST

GFR.6	The DLT must validate the operational data with those specified in the smart contract to ensure that the contractual obligations are fulfilled.	MUST
GFR.7	If the DLT identifies that the contractual obligations are not fulfilled anymore, the DLT must report this to the human operator.	MUST
GFR.8	While a service (including services that shadow physical entities) is registered to the Hypermedia MAS Infrastructure, when one of the events listed below occurs, the service shall send a state information update to the Hypermedia MAS Infrastructure. Events to be considered are: 1. The keepalive interval, with a length to be defined during system design, has expired 2. A new job was assigned 3. A job was started 4. A job was finished 5. The health state changed 6. A maintenance request occurred 7. A maintenance request was cleared 8. A smart contract concerning the machine was changed	MUST
GFR.9	When the Hypermedia MAS Infrastructure receives a state information update from a service, it shall reply with an acknowledge.	MUST
GFR.10	The End User Goal Specification Front End shall provide a Web-based interface that allows the human operator to specify, review and rephrase goals for the Hypermedia MAS.	MUST
GFR.11	If the metric used to determine the performance of the AI's decision on how to proceed with a task is smaller than a threshold to be defined during system design, then the AI shall request human help from the agent representing the HIL service. The request shall contain a necessary amount of information in order to describe properly the issue to the human operator.	MUST
GFR.12	When a human operator requests a malicious actor to be locked out, Human-in-the-Loop (HIL) service shall interrupt all communication relations to the malicious actor within a reaction time to be defined during system design. HIL service may rely on the TSN network controller or 5G network controller for that.	MUST
GFR.13	When an operator becomes available or unavailable, HIL-AR Application shall inform the HIL service about IP addresses of available servers.	MUST
GFR.14	If an operator offers help, while the help request was cancelled or taken over by another operator, the HIL service shall inform HIL-AR Application about that.	MUST
GFR.15	While an operator is controlling a machine, the HIL-AR Application shall display status related event messages to the user.	MUST
GFR.16	While an operator is controlling a machine, the HIL service shall inform HIL-AR application about relevant issues, events and data regarding this control operation, e.g., error messages, coordinates.	MUST

GFR.17	While a human operator controls the system, the latter shall provide a video stream to HIL-AR Application.	MUST
GFR.18	HIL-AR Application shall display the video feed from the camera in AR for the human operator to view.	MUST
GFR.19	When an operator indicates that he has finished his operations, HIL-AR Application shall inform HIL Service to initiate the return of control to the AI and exit user session.	MUST
GFR.20	When the human operator wants to directly control the system, the user interface shall provide a direct connection to the system.	MUST
GFR.21	When the system has successfully overcome an issue with the aid of other entities in the field or the human operator, the AI shall evaluate this newly acquired knowledge with its internal model. In case the newly acquired knowledge improves the base model, the AI shall update its internal model.	MUST
GFR.22	The user interface shall enable a human operator to manually specify parameters regarding the operation of the security modules.	MUST

4.2.2 AGRICULTURAL USE CASE-SPECIFIC FUNCTIONAL REQUIREMENTS

The functional requirement associated with the agriculture use case are presented in Table 3.

Table 3. Agriculture use-case specific functional requirements

Requirement ID	Derived from	Requirement	Level
FR.UC1#1	UC1.1.1	When an end user opens the URL of the End User Goal Specification Front End, this front end shall provide a Web-based interface that allows the human operator to specify, review and rephrase goals for the Hypermedia MAS. Concretely, this interface shall allow the operator to: - Select which field shall be processed - Select the process to be executed (e.g., fertilizing, ploughing) - Task the Hypermedia MAS with the configured goal by clicking a button	MUST
FR.UC1#2	UC1.1.2	When delegated a goal, among other tasks, depending on the configured agent organization, and by using available services, the agents shall select the concrete vehicle to be used (depending on the vehicle's location and equipped gear) and shall task this vehicle with waypoints towards fulfilling the goal.	MUST
FR.UC1#3	UC1.1.3	When the tractor receives a waypoint, the tractor must calculate a trajectory to reach the received waypoint.	MUST
FR.UC1#4	UC1.1.3	If the tractor cannot calculate a trajectory based on the waypoints, it shall inform the human operator that it cannot perform the task at hand	MUST

FR.UC1#5	UC1.2.1, UC1.2.2	While performing its autonomous operation, the tractor must scan the environment through its sensor systems in order to maintain proper course and identify potential obstacles.	MUST
FR.UC1#6	UC1.2.1	When the sensors detect a potential obstacle the control system shall trigger the AI algorithms to provide a viable solution to overcome this obstacle.	MUST
FR.UC1#7	UC1.2.4	If an unknown situation is encountered and the AI cannot calculate a solution above a predefined acceptance threshold, the tractor must go into a safe state (stop). An unknown situation could be for example an obstacle which it doesn't know how to drive around it.	MUST
FR.UC1#8	UC1.2.1	When the AI on the tractor cannot calculate a viable solution to overcome an obstacle based on its own information, the tractor shall request more information from the IAKM.	MUST
FR.UC1#9	UC1.2.4	When the AI on the tractor cannot calculate a viable solution to overcome an obstacle based on the information from the IAKM, the AI shall request help from the human operator.	MUST
FR.UC1#10	UC1.1.5	If the AI on another deployed device can provide a requested solution, then it should send to tractor's AI in order to maintain the autonomous operation.	MUST
FR.UC1#11	UC1.2.5	When the human operator is asked for support by the tractor, the operator must be made available a user interface that allows a 180° display of the video stream.	MUST
FR.UC1#12	UC1.2.8	When the human operator is requested for help by the tractor, the human operator must be able to control the tractor through VR controllers.	MUST
FR.UC1#13	UC1.2.5	The user may have the possibility to access a map of the field with all positions of all entities in the field. This map may be accessible in the user interface.	MAY
FR.UC1#14	UC1.2.5	When the human operator is planning the trajectory around the obstacle, the user interface should display a virtual environment of the surroundings of the tractor	SHOULD
FR.UC1#15	UC1.2.5	When the human operator wants to access other entities in the field for more information, the user interface shall enable the human operator to make a connection to these entities (HIL Service).	MUST
FR.UC1#16	UC1.2.5	While the human operator is accessing the program to get information from other entities, the user interface should provide the positions of the other entities in the field.	SHOULD
FR.UC1#17	UC1.2.5	When the human operator wants to have a drone fly to a certain position for observing the tractor, the user interface may provide the user the possibility to directly control the drone.	MAY

FR.UC1#18	UC1.2.6/ UC1.2.7	When a specific entity in the field has been selected by the human operator to provide additional information, this entity shall provide a data or video stream into the user interface.	MUST
FR.UC1#20	UC 1.2.9	When the human operator wants to plan a trajectory around the obstacle, the user interface shall provide the possibility to provide new waypoints for the tractor, so it knows where it should move.	MUST
FR.UC1#21	UC1.2.9	When a human operator has planned waypoints around the obstacle, the user interface may validate the proposed waypoints if it is viable solution for the tractor to move to.	MAY

4.2.3 HEALTH-CARE USE CASE

The functional requirements related to the healthcare user case are specified in Table 4.

Table 4. Healthcare use-case specific functional requirements

Requirement ID	Derived from	Requirement	Level
FR.UC2#1	UC2.2.1, UC2.2.2, UC2.2.3	The system shall measure activity level, heart rate, oxygen saturation, blood pressure and body weight	MUST
FR.UC2#2	UC2.2.1, UC2.2.2, UC2.2.3	The system shall monitor patient constantly, during both rest and high-activity (physical exercise) periods.	MUST
FR.UC2#3	UC2.2.1, UC2.2.2, UC2.2.3	The patient shall be able to mark the initiation and termination of an exercise session.	MUST
FR.UC2#4	UC2.2.1, UC2.2.2, UC2.2.3	The system shall provide electrocardiogram (ECG) tracing upon patient demand.	MUST
FR. UC2#5	UC2.2.1, UC2.2.2, UC2.2.3	The system shall provide measurements to indicate intensity of exercise. More specifically the system shall provide measurements of distance covered in meters, steps and calories consumed.	MUST
FR.UC2#6	UC2.2.1, UC2.2.2, UC2.2.3	The system should provide measurements of body composition, such as percentage of body fat and body water.	SHOULD
FR.UC2#7	UC2.2.1, UC2.2.4	The system shall store patient biometric data to enable the physician to evaluate patient's history in case of an event.	MUST
FR.UC2#8	UC2.2.5, UC2.2.6	The system's AI module shall trigger alarms in case of detection of abnormal measurements or significant changes on biometric parameters.	MUST

FR.UC2#9	UC2.3.1, UC2.3.2	The DLT components shall record all important trust-related events and accountable activities of the actors	MUST
FR.UC2#10	UC2.3.3, UC2.3.4	The Assurance platform shall provide compliance report requests for trust-related audits.	MUST
FR.UC2#11	UC2.2.5	The system shall allow the physician to manually set the values that trigger an alarm ("too high" / "too low") for all parameters measured and for different activity periods (exercise / rest).	MUST
FR.UC2#12	UC2.2.4	Diagrams with mean values of the requested biometric parameters and their variation with the previous ones should be send weekly to the clinicians.	SHOULD
FR.UC2#13	UC2.2.4	The system must be able to provide personalized recommendations to patients. For example, when to exercise or other clinical prescriptions, based on previous behaviour and/or the behaviour of similar patients.	MUST
FR.UC2#14	UC2.1.1	The system must be able to federate algorithms from a base model hosted at a global AI component or coordinator server to local AI components or workers. The algorithms must seek to minimize a given loss function while training on data at the local components.	MUST
FR.UC2#15	UC2.1.1	The system must have functionality so that the local AI components can send updates to the global AI component, which will average the results.	MUST
FR.UC2#16	UC2.1.1	The system must have functionality for comparing the base model with the updated model at the global AI component and redistributing the updated model to the local AI components as appropriate.	MUST

4.2.4 MANUFACTURING USE CASE

The functional requirements related to the manufacturing user case are specified in Table 5.

Table 5. Manufacturing use-case specific functional requirements

Requirement ID	Derived from	Requirement	Level
FR.UC3#1	UC3.2.1	If the Hypermedia MAS or the back end of its Web-based IDE are unsure how to interpret a goal formulated by a customer, then either of them shall contact the customer to rephrase the goal via the End User Goal Specification Front End.	MUST
FR.UC3#2	UC3.2.1, UC3.2.2	While a customer formulates a goal, the user interface shall display a workpiece template and allow the operator to: - select material of workpiece (only "wood" available for v1) - add one or more text boxes - upload and add one or more images - position text boxes and images on trunk	MUST

		- select process type (engrave; laser; any) per text box and image - confirm his input and thus start the creation process	
FR.UC3#3	UC3.2.1, UC3.2.2	When the user has confirmed his inputs, the front end shall generate the input for the manufacturing devices in a suitable image format (e.g., an eps file) and forward that file to the back end of the Web-based IDE. In addition to the image, it shall submit the position of the image on the workpiece (x, y) in relation to the center of the workpiece, the material type, and the process type. We refer to this data structure as the "goal".	MUST
FR.UC3#4	UC3.2.5	While an operator is controlling a robot, the HIL-AR Application shall provide the following information to the robot controller: • Coordinates of digital twin to initiate the robot arm movement • Grab commands • Release commands	MUST
FR.UC3#5	UC3.2.5	When an operator is taking over control of a robot, the HIL-AR framework shall provide the following information to the robot controller: • Handedness of the robot (left or right)	MUST
FR.UC3#6	UC3.2.5	When an operator is taking over control of a robot, the robot controller shall provide the following information to the HIL-AR Application: • Coordinates of robot to initialize the digital twin	MUST
FR.UC3#7	setup	While the reservoir for workpieces is not completely full, the operator should be able to refill workpieces at any time. The operator should not be required to place the workpieces at different places but should be able to place every workpiece at the same place.	SHOULD
FR.UC3#8	UC3.3.3	When a customer requests the proof of cost for the logs of activities of machines, the customer shall use MetaMask as a DLT client. The customer shall install MetaMask on his personal device such as laptop or mobile phone to communicate with DLT via Smart Contract to get the requested data.	MUST

4.3. Non-Functional Requirements

Similarly, to the Functional Requirements described in the previous section, two main sets of non-functional requirements are provided in the following subsections. Those cover common non-functional requirements for the overall IntellIoT framework, as well as specific requirements for each of the three use cases.

As a reminder, Non-Functional Requirements describe properties that the system functions must/should/may have. These typically include performance, scalability, usability, security and other qualitative requirements that may be defined or expressed in absolute or relative terms. For example, some performance requirements are expressed with absolute terms using a specific performance number or property value (see e.g., GNFR.8 that defines that the camera resolution has to be at least 2K) while others are expressed qualitatively in an effort to declare something less-easily quantifiable through a specific value (e.g., see UCNFR.2 where usability is expressed as an intuitive manner).

This document covers the first increment of the requirements definition. As such, a number of features have not been implemented yet and experimentations and feedback are limited. Therefore, certain non-functional requirements that are declared in the scope of this document and are expressed in relative terms, during the second increment of the document, they will be ratified and quantified more precisely.

Last but not least, in the Functional Requirements definition, each use-case specific requirement is narrowly associated with a specific usage scene (some applied to more than one). For the Non-Functional Requirements, the qualities described through them are broader than a specific use-case scenario scene and therefore while there is a distinction between general and use-case specific non-functional requirements, the non-functional requirements are broadly associated with use cases rather than specific scenes.

4.3.1 GENERAL NON-FUNCTIONAL REQUIREMENTS

The following table (Table 6) lists the non-functional requirements for the overall IntellIoT framework.

Table 6. General non-functional requirements

Requirement ID	Requirement	Level
GNFR.1	The system shall be able to capture trust-related events.	MUST
GNFR.2	The system shall ingest malicious activity alerts received from event captors.	MUST
GNFR.3	The security components of the system (including MTDs, DLT and IDS) shall have a bounded maximum response time for communication with the Security Assurance platform. The specific value shall be configurable depending on the deployment scenario, the network topology and the security/safety requirements set by the user.	MUST
GNFR.4	If a node behaves in an unexpected or malicious way, the security modules of the framework shall identify malicious, compromised, or misbehaving nodes based on a number of different criteria covering different types of potential attacks.	MUST
GNFR.5	If a node behaves in an unexpected or malicious way, the security modules of the framework should automatically exclude or isolate problematic nodes in order to ensure the functioning of the overall system under attack conditions.	SHOULD
GNFR.6	The human operator shall be notified through a proper user interface about the security posture of the system deployment, including security events and how the security components of the frameworks have responded to them.	MUST

GNFR.7	When the Security Assurance Platform receives alerts from event captors, it must visualise malicious activity alerts on its GUI, for the operator to review.	MUST
GNFR.8	The user interface should enable a human operator to manually override the responses of the security modules and define the permanent or temporary actions on specific events.	SHOULD
GNFR.9	If a human operator attempts to override the responses of the security modules, a user authentication process shall always be required.	MUST
GNFR.10	A user may set a Security Assurance platform uptime requirement (in terms of percentage of the overall system time).	MAY
GNFR.11	A secure configuration process of all devices participating in the system shall be required as part of the system startup/bootstrap phase.	MUST
GNFR.12	The composed image must have a resolution of max. 2K.	MUST
GNFR.13	If the system, e.g., robot or tractor, is requested to move to a position which it cannot reach safely, it shall stop and provide an error message to the requester. The area for safe movement might be preconfigured.	MUST
GNFR.14	All devices participating in the system may have configurable fail-safe states.	MAY
GNFR.15	When the human operator assumes control of a device in the system (e.g., the tractor or the robotic arm), the device shall respond to user commands in real-time.	MUST
GNFR.16	Users without formal programming knowledge but with domain knowledge about either of the use cases shall be able to use the Web-based IDE for Hypermedia MAS to configure the Hypermedia MAS for that use case.	MUST
GNFR.17	At run time, it shall be possible to extend the Hypermedia MAS Infrastructure with additional services and update its behaviour through the Web-based IDE for Hypermedia MAS. This may be limited while a user goal is currently being processed by the system.	MUST
GNFR.18	The Web-based IDE for Hypermedia MAS and the Hypermedia MAS Infrastructure shall be compatible with any service that satisfies the technical requirements regarding W3C WoT TD, TDT, and input/output schema specification.	MUST

4.3.2 USE CASE SPECIFIC NON-FUNCTIONAL REQUIREMENTSTable 7 presents the non-functional requirements associated with specific use cases.

Table 7. Use-case specific non-functional requirements

Requirement ID	Use Case	Description	Requirement Level
UCNFR.1	UC1	When the human operator is controlling the tractor remotely, the tractor shall react in real-time to the actuation commands.	MUST
UCNFR.2	UC1	When the human operator is controlling the tractor remotely, the user interface should give the human operator full control over the tractor (perform all driving actions such as steering, accelerating or braking) in an intuitive manner.	SHOULD

UCNFR.3	UC1	When a human operator initiates an emergency action that halts the operation of the tractor for safety reasons, the response shall be immediate (hard real-time).	MUST
UCNFR.4	UC2	The smart blood pressure monitor shall provide alarms to the physician if daily changes fluctuate more than 20%.	MUST
UCNFR.5	UC2	The system's AI components should provide an interface with proper notifications to the patients when weight, blood pressure and activity level are not the appropriate or when the patients are not adherent to their medication, lifestyle and use of the monitoring system.	SHOULD
UCNFR.6	UC3	While the robot is operating, either physical barricades shall keep people away from the robots operating area, or safety sensors shall detect any approaching person and stop the robot before the person can reach the operating area.	MUST
UCNFR.7	UC3	Maximum reaction time Hypermedia MAS takes to acknowledge an update from a machine or robot shall be short enough to avoid resending of the update.	MUST
UCNFR.8	UC3	While a machine or robot is registered to the Hypermedia MAS Infrastructure, if the machine/robot does not receive and acknowledge on a state information update within a timeout interval to be defined during system design, then it shall resend it.	MUST

5. EVALUATION CRITERIA

This section describes the evaluation criteria defined in IntellIoT's Description of Action in order to measure the success of the project. The evaluation is based on two main pillars: The first is a set of Key Performance Indicators (KPIs) that aim to assess the project's performance and ensure it meets the main objectives that have been set for the project. A second set of KPIs is defined in order to relate the project's achievements to the impacts that have been expected by the call.

In the subsequent sections, the KPIs for each objective are going to be presented and described, providing insights on how each KPI is associated with the different components of the IntellIoT framework, how the achievement of every KPI is going to be measured and validated and which are the baseline performances that need to be matched or surpassed. Section 5.7 provides in a similar manner, a description of the impact KPIs.

5.1 Objective 1: Creation of a self-aware and semi-autonomous multi-agent system

The first objective of IntellIoT aims at the creation of a self-aware and semi-autonomous multi-agent system over an optimized computation and communication infrastructure that manages compositions of IoT/edge devices in closed-loop with the network. The following KPIs are associated with this specific objective.

KPI-ID	1.1
Name	Open-Source HyperMAS
Description	Open-source software components for HyperMAS, including libraries and tooling for researchers and practitioners to design, deploy, and manage such systems.
Responsible partner(s)	HSG
Scope	IntellIoT Framework and UCs
Mapping to components & measurement points	This maps to the three main components that are created in the scope of WP3 T3.1: - Per use case, the End User Goal Specification Frontend (for Farmer/Doctor/Customer) - Across use cases, the Infrastructure for Hypermedia MAS - Across use cases, the Web-based Integrated Development Environment for Hypermedia MAS - Support libraries, e.g., for the handling of W3C WoT Thing Descriptions
Baseline	No HyperMAS software components that are published as open source.
Means of verification	Documentation
Methodology / tools	Publicly accessible repositories (e.g., GitLab/GitHub) with the code and instructions for the listed software components. Where applicable, whitepapers or research articles that document the listed software components.
Assessment Updates	Cycle 2 final release

KPI-ID	1.2

Name	Vertical and Horizontally Scaling HyperMAS
Description	Reach high vertical and horizontal scalability of the HyperMAS with respect to increasing numbers of agents, artifacts, and devices with a benchmark against existing MAS
Responsible partner(s)	HSG
Scope	IntellIoT Framework
Mapping to components & measurement points	Ability of the Hypermedia MAS Infrastructure and the Web-based IDE for Hypermedia MAS to support large numbers of agents and artifacts (i.e., devices and services) compared to existing MAS
Means of verification	Testing
Methodology / tools	Evaluation of the relevant components in the laboratory (using simulated services) as well as in the context of the IntellIoT use cases.
Baseline	Baseline values depending on what MAS framework is taken as reference.
Assessment Updates	After Cycle 1: Evaluation in laboratory. After Cycle 2: Evaluation in context of use cases.

KPI-ID	1.3
Name	HyperMAS Deployments
Description	Provide deployments (within the three use cases) of the HyperMAS and evaluate (with existing benchmarks) system flexibility & evolvability (e.g., adapt to dynamic environments).
Responsible partner(s)	HSG
Scope	IntellIoT Framework and Use Cases
Mapping to components & measurement points	- Running demonstrators across all three IntellIoT use cases, given the scope of each UC and the applicability of HyperMAS components in this scope. - Ability of the Hypermedia MAS Infrastructure and the Web-based IDE for Hypermedia MAS to apply across the heterogeneous use cases of IntellIoT.
Means of verification	Testing
Methodology / tools	Ability of the Hypermedia MAS Components (Web-based IDE and Infrastructure) to support the IntellIoT use cases without any changes, i.e., without use-case-specific adaptation. Tested through the implementation of demonstrators for the IntellIoT use cases that use equivalent and unchanged Hypermedia MAS Components.
Baseline	N/A
Assessment Updates	After Cycle 1: Evaluation in laboratory given results from WP5. After Cycle 2: Aim for evaluation in the field given results from WP5.

KPI-ID	1.4
Name	HyperMAS Reconfiguration
Description	Initial configuration as well as reconfiguration of the HyperMAS (e.g., in case of failures) will be *real-time* enabled, where concrete real-time requirements will be defined per use case.
Responsible partner(s)	HSG
Scope	IntellIoT Framework
Mapping to components & measurement points	- Ability of the Web-based IDE for Hypermedia MAS to allow engineers to design and re-design agent organizations and agent procedural knowledge while the system is running - Extent of the ability to deploy such changes while the system is running (not all changes can be deployed in this case)
Means of verification	Testing
Methodology / tools	Based on tests for KPI 1.3, ability of the Hypermedia MAS Components to allow engineers to design and re-design agent organizations based on available services and ability of the Hypermedia MAS Infrastructure to run the resulting organizations. Tested by adding/removing heterogeneous services at run time and verifying that engineers are able to update the agent organization to keep a running system (as long as this is feasible). This should be refined given the results from WP5.
Baseline	N/A
Assessment Updates	After Cycle 2: Evaluation in laboratory and, possibly, in the field.

KPI-ID	1.5
Name	Optimized allocation
Description	Optimized allocation of IoT application functions with a maximum optimality gap of 15% and implementation for 3 optimality criteria: reliability, response time and energy consumption.
Responsible partner(s)	SIEMENS
Scope	UC3
Mapping to components & measurement points	Determining the optimal allocation of IoT application functions will be done by the Computational Resource Manager. It comprises an algorithm for the optimized allocation of IoT application functions on IoT devices / edge resources while considering the network configuration. The deployment of such functions will be tuned towards different criteria, e.g., reliability of compute nodes, response time of the application, or energy consumption. Together with the Edge Orchestrator, this will automatically deploy functions of a composed IoT application to the Edge infrastructure.
Means of verification	Testing
Methodology / tools	A stepwise testing approach will be chosen:

	1. Model based test: relying on models for network, devices and application functions upon which the algorithm for optimal allocation is applied. 2. Simulation based test: based on a selected simulation environment (e.g., Omnet++) network and device infrastructure will be simulated and allocation options will be tested. 3. Operational test: using the actual network/device infrastructure of the UC3 demonstrator, tests will be conducted with different component allocations.
Baseline	The baseline is a set of randomly allocated IoT application functions.
Assessment Updates	Cycle 1: The fundamental ability to assign application functions to IoT/Edge device. Cycle 2: Quantitative evaluation of the optimal allocation and optimization gap.

5.2 Objective 2: Enable ultra-reliable low-latency communication over heterogeneous networks

The second objective of the project aims to enable dynamic network planning/management for ultra-reliable low-latency communication schemes over heterogeneous networks (LTE, 5G NR, Cellular IoT, D2D) in order to achieve tactile (real-time) and contextual (adaptive) interaction between IoT devices, humans and services. The KPIs that follow are associated with the specific targets.

KPI-ID	2.1
Name	5G URLL Communications
Description	Extending 5G network functionalities supporting URLL & eMBB for the needs of the three use cases.
Responsible partner(s)	EURECOM
Scope	UC 1 / UC3
Mapping to components & measurement points	The OAI RAN controller is in charge of configuring the required radio resources from the Edge controller. The RAN controller itself contains the configuration parameters and a data-driven optimizer will need to dynamically adjust the right parameters to the wireless conditions.
Means of verification	Testing
Methodology / tools	• Unit tests (PHY layer simulation) • Laboratory test (1-2 devices) • (if available) emulation test (under challenging conditions)
Baseline	Delay <10ms on the RAN
Assessment Updates	Cycle 1: FR1 (<6Ghz) Cycle 2: FR2 (>20Ghz)

KPI-ID	2.2
Name	TSN functions integration
Description	TSN functions integration in computation & communication infrastructure (combined with 5G).
Responsible partner(s)	SIEMENS, EURECOM, HOLO
Scope	IntellIoT framework and UC3
Mapping to components & measurement points	TSN functions are implemented in TSN switches and endpoints and controlled by the Network Controller. Network controller is mainly triggered by HIL service. HIL service integrates TSN with 5G communication services. Measurement points: • Low latency and low jitter communication between robot controller and robot arm. • High bandwidth and low latency for camera stream to human operator. • Dynamic allocation of communication services between robot and human operator.
Means of verification	Testing
Methodology / tools	Test probes are deployed to relevant end stations. These allow for end-to-end measurement of Quality-of-Service parameters.
Baseline	Current TSN-based networks are vendor-locked and have very limited support for dynamic reconfiguration. No close interaction between 5G and TSN networks.
Assessment Updates	Will be evaluated in Cycle 2

KPI-ID	2.3
Name	5G Multi-RAN
Description	Enabling heterogeneous networking technologies: LTE, 5G NR, Cellular IoT, D2D.
Responsible partner(s)	EURECOM
Scope	UC1 / UC3
Mapping to components & measurement points	The 5G RAN can support various technologies. The 5G RAN Controller can operate in a stand-alone or none-standalone mode (either with a 4G backend or with a full 5G backend). The non-standalone mode supports both 5G and LTE UEs. A RAN controller will be integrated directly in 5G UE to support D2D.
Means of verification	Testing
Methodology / tools	Cycle 1 • 5G non-standalone mode – unit test + lab test Cycle 2: • 5G standalone and non-standalone modes – unit test + lab test + demonstrator

	• D2D mode - unit test + lab test
Baseline	As function of the configured connection choice, the right mode is used by the UE.
Assessment Updates	Cycle 1: • 5G non-standalone Cycle 2: • Standalone and non-standalone • D2D

KPI-ID	2.4
Name	Industrial D2D
Description	Enabling wireless TSN-grade D2D scheduler for decentralized computing in IoT context.
Responsible partner(s)	EURECOM
Scope	UC1 / UC2 / UC3
Mapping to components & measurement points	A D2D RAN controller (called ProSE controller in 3GPP) configures the D2D wireless link. A 5G D2D scheduler is provided as an external module to the 5G 3GPP architecture. The 5G D2D scheduler provides quasi-deterministic resource allocation on the D2D link respecting the requirements configured by the D2D RAN controller
Means of verification	Testing
Methodology / tools	• Unit testing - the D2D scheduler is tested alone without the 3GPP stack • Lab test – the D2D scheduler is integrated to the OAI 5G D2D architecture and 2 UEs can connect on the D2D link. • Emulation test – the 5G D2D PHY and Channel are abstracted for multi-UE testing under challenging conditions
Baseline	D2D resources are allocated with delay and reliability guarantees
Assessment Updates	Not tested in Cycle 1

KPI-ID	2.5
Name	Application-tailored reliability
Description	Application-tailored definition and fulfilling of a reliability requirement for the three use cases, maintained under challenging network conditions and based on a data-driven prediction.
Responsible partner(s)	AAU
Scope	UC3

Mapping to components & measurement points	Dynamically determining the communications resource allocation of IoT application functions will be done by the Communications Resource Manager. It comprises an algorithm for the optimized allocation of VR/AR, IoT, control traffic. The deployment of such functions will be tuned towards different reliability-related criteria, e.g., system stability (control loop), information freshness, or latency-reliability curves.
Means of verification	Testing
Methodology / tools	Two steps: 1. Model test with simulations: relying on models for network, devices, upon which the algorithm for optimal allocation is applied. Selection of a simulation environment (e.g., Python) 2. Operational test: using the actual 5G infrastructure, tests will be conducted with different traffic and allocations.
Baseline	The baseline is a set of randomly allocated resources.
Assessment Updates	Cycle 1: Analytical models and simulations. Cycle 2: Implementation as x-apps and evaluation in the 5G infrastructure.

5.3 Objective 3: Semi-autonomous IoT applications with distributed AI while keeping human-in-the-loop

The third objective of the project is to enable semi-autonomous IoT applications by leveraging distributed AI algorithms under compute, storage, mobility and bandwidth constraints and by integrating the human-in-the-loop for safety, assistance and continuous improvement of AI. The following KPIs are associated with this specific objective.

KPI-ID	3.1
Name	Distributed training guarantees
Description	With a centralized training model as benchmark for training accuracy, enable distributed solutions achieving an accuracy beyond 95% of benchmark within 50 inter-device communication rounds.
Responsible partner(s)	UOULU
Scope	At least one out of UC1 and UC3
Mapping to components & measurement points	Resource-aware re-trainer, AI model aggregator, Agriculture/Manufacturing AI model
Means of verification	Testing
Methodology / tools	Proposed: Implementation of federated learning algorithm and carry out distributed training over the system. Benchmark: All devices upload training data to a server where centralized training is carried out.

	V1: training over artificial data, V2: training over UC-specific data
Baseline	Training accuracy of centralized training where the training takes place in a server after importing data from all devices.
Assessment Updates	V1 after Cycle1 and V2 at final Cycle 2 evaluation

KPI-ID	3.2
Name	ML model reduction
Description	At least 10 times ML model size reduction during knowledge distillation for constrained IoT devices.
Responsible partner(s)	UOULU
Scope	At least one out of UC1 and UC3
Mapping to components & measurement points	Resource-aware ML inference, Agriculture/Manufacturing AI model
Means of verification	Testing
Methodology / tools	Use the pre-trained model as the baseline Minimize ML model size subject to ML model accuracy above a predefined target
Baseline	Pre-trained model size prior to model reduction
Assessment Updates	At final Cycle 2 evaluation

KPI-ID	3.3
Name	Enabling autonomy
Description	Ensure the frequency of necessary human interventions reduces with exponential rate over time.
Responsible partner(s)	UOULU
Scope	At least one out of UC1 and UC3
Mapping to components & measurement points	Resource-aware re-trainer, AI model aggregator, Agriculture/Manufacturing AI model
Means of verification	Testing
Methodology / tools	At the interventions, human inputs are added into the training dataset Retrain the ML models with modified training data
Baseline	None
Assessment Updates	At final Cycle 2 evaluation

KPI-ID	3.4

Name	ML energy reduction
Description	At least 10% of energy reduction during distributed training while ensuring high training accuracy compared to centralized training methods.
Responsible partner(s)	UOULU
Scope	At least one out of UC1 and UC3
Mapping to components & measurement points	Resource-aware re-trainer, AI model aggregator, Agriculture/Manufacturing AI model
Means of verification	Testing
Methodology / tools	Proposed: Implementation of federated learning algorithm and carry out distributed training over the system. Benchmark: All devices upload training data to a server where centralized training is carried out. V1: training over artificial data, V2: training over UC-specific data
Baseline	Total energy consumption of centralized training where the training takes place in a server after importing data from all devices.
Assessment Updates	V1 after Cycle1 and V2 at final Cycle 2 evaluation

KPI-ID	3.5
Name	Increase accuracy of Holo Stylus
Description	Reach an accuracy of the Holo-Stylus below 5 mm in the field of view of the operator.
Responsible partner(s)	HOLO
Scope	UC3
Mapping to components & measurement points	HMU application on HoloLens; ISAR;
Means of verification	Testing
Methodology / tools	Normative-Actual value comparison.
Baseline	N/A
Assessment Updates	V1 after Cycle1 and V2 at final Cycle 2 evaluation

5.4 Objective 4: Enable security, privacy and trust-by-design

IntellIoT aims to enable security, privacy and trust-by-design with continuous assurance monitoring, assessment and certification as an integral part of the system, providing trustworthy integration of third party IoT devices and services. The following KPIs are associated with the effort to achieve those goals.

KPI-ID	4.1

Name	Continuous Assurance
Description	Delivery of a continuous assurance and certification component supporting: (a) individual risk assessment schemes; (b) incremental risk assessment schemes, and; (c) hybrid risk assessment schemes to estimate risk by combining the outcomes of the schemes in (a) and (b).
Responsible partner(s)	SANL
Scope	IntellIoT framework
Mapping to components & measurement points	Security Assurance Platform
Means of verification	Testing
Methodology / tools	Testing will cover each and every one of the core features of the Security Assurance platform that will be integrated into IntellIoT to satisfy this KPI. In more detail, it will cover: (i) each one of the individual risk assessment schemes, including: (a) vulnerability assessments; (b) static analysis; (c) penetration testing, and; (d) continuous runtime monitoring. (ii) Incremental risk assessment schemes, featuring mechanisms to will allow to build and elaborate upon previous assessments. (iii) Hybrid risk assessment, which will combine and correlate results from all of the above assessments, providing a multi-perspective analysis of the security and privacy posture of the protected systems. For testing purposes, a mock IoT infrastructure model will be developed and used, while a comprehensive validation of the above will also follow, in the context of all three of the project's use cases.
Baseline	N/A
Assessment Updates	V1 after Cycle1 and V2 at final Cycle 2 evaluation

KPI-ID	4.2
Name	DLT implementations
Description	Delivery of at least 2 DLT implementations that can adjust level of trust to capabilities of devices, can integrate proxies, and can conform to certain latency and reliability requirements, such that the level of decentralization of device participation is proportional to its computation-communication capabilities.
Responsible partner(s)	AAU
Scope	UC1/UC2/UC3
Mapping to components & measurement points	Resource aware DLT-manager
Means of verification	Simulations + experimental testing
Methodology / tools	Two phases:

	1. Simulation test: relying on models for network, devices and application functions. The steps are: a. Test with different BC platforms: Ethereum, Hyperledger fabric, IOTA and find the proper one for IntellIoT. b. Check that the system works correctly. c. Implement two protocol options: (1) lightweight nodes; (2) standard devices (no DLT-capable). d. Do performance measures: latency, throughput, robustness. e. Design APIs and integrate with other partners. 2. Experimental test: using the actual nodes for each UC (tractor, robots, wearables…). The same steps as for the simulation test phase are followed here.
Baseline	Not applicable: the baseline is not having DLT
Assessment Updates	V1 with platform decision and smart contract for the 3 UCs after Cycle1; V2 at final Cycle 2 evaluation

KPI-ID	4.3
Name	Secure Routing for Ad-Hoc IoT Networks
Description	Delivery of at least two trust-based secure routing algorithms, applicable for the IoT system, which cover the design requirements of i) relatively static networks with low mobility and ii) open networks with high mobility nodes, respectively.
Responsible partner(s)	TSI
Scope	UC1
Mapping to components & measurement points	Secure Routing / Intrusion Detection System components
Means of verification	Testing
Methodology / tools	The functionality is tested by hosting multiple entities to the network in an Ad-Hoc topology. Most of the entities generate legitimate traffic, and some entities work as malicious entities and try to compromise the network. The Intrusion Detection System will discriminate legitimate networking entities from malicious ones. The chosen routes for each legitimate entity are monitored and analysed to verify that malicious nodes are skipped and there is no data loss or breach. Several different attacks will be performed, and the successful identification to each attack and rerouting of traffic will be tested.
Baseline	N/A
Assessment Updates	Emulated proof of concept after Cycle 1 and final version at Cycle 2 evaluation

KPI-ID	4.4
Name	Moving Target Defenses for IoT systems
Description	Development of at least 2 MTD algorithms for: i) local decision making by an individual agent for its underlying system, and; ii) horizontal incorporation of trusted agents in the IoT system.
Responsible partner(s)	TSI
Scope	IntellIoT framework
Mapping to components & measurement points	Moving Target Defenses component - Security Assurance Platform
Means of verification	Testing
Methodology / tools	Two cases will be tested: one during normal operation of the overall system and one for operation of the system under ongoing attacks. During normal operation the MTDs will proactively change the system's configuration at predefined or random intervals. The goal is to increase the required effort for an attacker to analyse a specific system configuration, exploit potential vulnerabilities or gather enough information about the system. During ongoing attacks, the agents must enforce pre-defined defense strategies that can counter the malicious actions or at least mitigate their side effects. The generation of new configurations will be tested to verify the validity of each new configuration. The predefined set of defense strategies will be tested for the corresponding attacks and the mitigation will be verified.
Baseline	Not applicable
Assessment Updates	Individual agent local decision-making implementation after Cycle1 and horizontal incorporation of trusted agents at final Cycle 2 evaluation

5.5 Objective 5: Development of a reference implementation of the IntellIoT framework

Under the specific objective, the goal is to development a reference implementation of the IntellIoT framework, which will be demonstrated and evaluated in three use-case areas: agriculture, healthcare and manufacturing. The KPIs that are provided below are used as a measurement to assess the success of this effort.

KPI-ID	5.1
Name	IntellIoT Framework
Description	Delivery of the integrated *IntellIoT* framework.
Responsible partner(s)	AVL
Scope	IntellIoT framework
Mapping to components & measurement points	All components

Means of verification	Testing
Methodology / tools	Testing methodology needs to be developed during integration
Baseline	N/A
Assessment Updates	V1 after Cycle1 and V2 at final Cycle 2 evaluation

KPI-ID	5.2
Name	End-user workshops
Description	Involve end-users of three domains and conduct (at least) two requirements workshops.
Responsible partner(s)	STARTUPC
Scope	UC1 / UC2 / UC3
Mapping to components & measurement points	Not applicable
Means of verification	Documentation
Methodology / tools	The end-user workshops will be conducted in a co-creative setup, using a design thinking approach to capture end-user's needs, pain points, requirements and expectations regarding the IntellIoT applications. Input from these workshops will be collected and synthesized in a deliverable report and used for the refinement of the Use Cases.
Baseline	Not applicable
Assessment Updates	V1 after Cycle 1 and V2 at final Cycle 2 evaluation

KPI-ID	5.3
Name	Framework validation
Description	Validation of the *IntellIoT* framework in three use cases each in relevant environment.
Responsible partner(s)	TSI
Scope	IntellIoT framework
Mapping to components & measurement points	All IntellIoT framework components and KPIs
Means of verification	Testing
Methodology / tools	For each use case, the three scenarios will be evaluated to verify the basic functionality. Then controlled experiments will be performed for evaluating low level TRLs of the developed mechanisms and components of the IntellIoT framework Finally, a cross checking to assess the generality of the IntellIoT framework and approach will be performed.

	Detailed methodology and tools will be described in D5.3 for Cycle 1 and D5.6 for Cycle 2 and will depend on the architecture from D2.3
Baseline	To be defined
Assessment Updates	Validation and verification of the KPIs based on the first version of the framework after Cycle1 and validation and verification of the KPIs based on the final version of the framework at final Cycle 2 evaluation

5.6 Objective 6: Promotion and exploitation of the IntellIoT framework

This objective is associated with the promotion and exploitation of the IntellIoT framework. This will be primarily done through contribution to standards and delivery of open-source components as well as by building an active IoT ecosystem (supported by two Open Calls) and focused dissemination and exploitation activities. The following list provides the KPIs associated with these goals.

KPI-ID	6.1
Name	Open Calls
Description	Successful conduction of two Open Calls with a minimum of 40 applicants per Open Call.
Responsible partner(s)	STARTUPC
Scope	IntellIoT framework and UC1 / UC2 / UC3
Mapping to components & measurement points	Not applicable
Means of verification	Documentation
Methodology / tools	All applications to the open calls will be managed through a central tool (F6S), which will include the applicant's general information, detailed description of the planned contribution and technology, as well as the evaluation by external experts.
Baseline	Not applicable
Assessment Updates	V1 after Cycle1 and V2 at final Cycle 2 evaluation

KPI-ID	6.2
Name	Dissemination and communication
Description	Achieve dissemination and communication targets as defined in Description of Action.
Responsible partner(s)	STARTUPC
Scope	IntellIoT framework and UC1 / UC2 / UC3
Mapping to components & measurement points	Not applicable
Means of verification	Documentation

Methodology / tools	All dissemination and communication activities are monitored on a constant basis and results captured in a central dissemination file.
Baseline	Not applicable
Assessment Updates	Ongoing

5.7 KPIs related to expected impact of the project

IntellIoT will strive to address all impacts expected by the Next Generation Internet of Things call and therefore has defined a set of impact KPIs (iKPIs) for transparent performance assessment of the project. There are six main impacts expected to be addressed, namely:

1. Contribution to human-centered IoT evolution improving usability and user acceptance, notably through strengthened security and user control
2. Contribution to emerging or future standards and pre-normative activities
3. Log-term evolution of next-generation IoT infrastructures and service platform technologies and contribution to scientific progress enabling novel, future semi-autonomous IoT applications
4. Proposal of novel and disruptive business models
5. Mobilization of key IoT players in security and privacy
6. Maintenance of an active ecosystems of all relevant IoT stakeholders

For each of the above six expected impacts a number of iKPIs are defined. The iKPI IDs are used to identify uniquely each iKPI and the numbering associates each iKPI with a specific impact (e.g., iKPI-ID i2.1 is the first iKPI associated with expected impact 2: contribution to emerging or future standards and pre-normative activities).

iKPI-ID	i1.1
Description	At least 70% of end-users of the developed IoT applications (based on IntellIoT framework) state they trust and accept the smart system, based on established metrics
Lead partner(s)	STARTUPC
Mapping to components & measurement points	IoT applications in the use cases
Means of verification	Inclusion & analysis of questionnaire and/or online poll results in D5.6.
Methodology / tools	Questionnaires prepared by the consortium and distributed during the end-user workshops. Post-workshops' analysis of results.
Baseline	N/A
Assessment Updates	Final end-user workshops

iKPI-ID	i2.1
Description	Influence standardization with at least 4 contributions
Lead partner(s)	EURECOM

Mapping to components & measurement points	3GPP D2D; 3GPP RAN controller;
Means of verification	Contributions or comments added to WI documents; leadership in WI; creation of new WI; Deliverable D6.10
Methodology / tools	Identifying the key WI and SDO, where IntellIoT contributions could be beneficial; participations to WI meetings; contributions to the meetings; presentations of IntellIoT framework to the WI meetings and stakeholders;
Baseline	N/A
Assessment Updates	Continuous, end of project

iKPI-ID	i2.2
Description	Development and offering of at least three security assessment and certification models tailored to specific standards, validated in the context of IntellIoT's use cases
Lead partner(s)	SANL
Mapping to components & measurement points	Security Assurance Platform
Means of verification	Deliverable D4.8
Methodology / tools	The assessment and certification models will be specified through the Security Assurance Platform and documented in the relevant deliverable (D4.8). They will encompass vulnerability, dynamic, and hybrid assessments. All three models will be validated in each of the three use cases.
Baseline	N/A
Assessment Updates	Cycle 1 and Cycle 2 release of the platform.

iKPI-ID	i3.1
Description	At least 80% of the stakeholders involved in the use cases (without direct project involvement) express a positive view on: (a) IntellIoT facilitates deployment of semi-autonomous IoT applications; (b) IntellIoT increases trustworthiness of NG IoT infrastructures
Lead partner(s)	(a) HSG / (b) SANL
Mapping to components & measurement points	a) End-user Goal Specification Front-End (for end users) and Web-based IDE for Hypermedia MAS (for engineers)
Means of verification	Inclusion & analysis of questionnaire results in D5.6.
Methodology / tools	Questionnaires prepared by the consortium and distributed during the end-user workshops, including questions that cover both aspects (a) and (b). Post-workshops' analysis of results.
Baseline	N/A

Assessment Updates	Final end-user workshops

iKPI-ID	i3.2
Description	At least two external organizations (beyond Open Call partners) use (on trial-basis) the IntellIoT framework and build IoT applications on top
Lead partner(s)	TTC
Mapping to components & measurement points	Out of the three use-case domains at least one technical building block described in Section 3 is used by external organizations apart from the IntellIoT framework.
Means of verification	Description of the applications that are using the IntellIoT framework and its technological building block which are built on top of it in deliverable D6.8. An evaluation report from the external organizations about the IntellIoT framework and a brief assessment of the business case will complement the verification.
Methodology / tools	Technical description report on the IoT application and an assessment of the business case (e.g., business canvas or similar) from an end-user of the IntellIoT project results and/or technologies.
Baseline	State of the art IoT applications at the projects starting date.
Assessment Updates	2nd cycle of deliverable D2.2

iKPI-ID	i4.1
Description	At least 80% of expert stakeholders participating in exploitation workshops (externals and use case owners) are engaged in deriving and approving novel business models
Responsible partner(s)	TTC
Mapping to components & measurement points	The exploitation workshops will identify the specific technology or the overall system approach (IntellIoT framework) as component or system, depending on the product/service under investigation.
Means of verification	Exploitation Workshop organized and results summarized and reported in the deliverable D6.8
Methodology / tools	Report on novel business models and its product/service identified by participating parties. Questionnaire prepared by the consortium and online surveys to structure the outcome of the exploitation workshops.
Baseline	N/A
Assessment Updates	An update will be prepared after the exploitation workshops and delivered in the 2nd cycle of the affected deliverables.

iKPI-ID	i5.1
Description	Mobilise at least 5 key IoT players external to the consortium, through their participation in security and privacy-related dissemination activities organised by IntellIoT

Lead partner(s)	STARTUPC
Mapping to components & measurement points	N/A
Means of verification	Ongoing inclusion of involved stakeholders in Dissemination file, final list in D6.9
Methodology / tools	Organisation of own Meetups, inclusion of articles by IoT stakeholders in Medium Magazine, engagement with external players via Social Media Channels
Baseline	N/A
Assessment Updates	D6.9, final report on Dissemination & Ecosystem building

iKPI-ID	i5.2
Description	Highlight the potential of security and privacy as an enabler for NG IoT applications, through validation of associated business models (see i4.1) with all involved IoT players
Lead partner(s)	TTC / SANL
Mapping to components & measurement points	Security, Privacy & Trust components of IntellIoT used in the individual application domains of the project.
Means of verification	Inclusion & analysis of questionnaire and/or online poll results in D6.8.
Methodology / tools	Questionnaires prepared by the consortium and distributed during the exploitation workshops, or online polls carried out during the exploitation process (to be decided by the consortium), collecting feedback on the novel business models defined during said workshops (in line with i4.1). Post-workshops' analysis of results.
Baseline	N/A
Assessment Updates	An update will be prepared after the final exploitation workshops and delivered in the 2nd cycle of the affected deliverables.

iKPI-ID	i5.3
Description	At least 80% of surveyed end-users (without direct project involvement) confirm that IntellIoT increases security and privacy protection and thereby alleviates an important adoption barrier
Lead partner(s)	SANL / TSI
Mapping to components & measurement points	Security, Privacy & Trust components of IntellIoT
Means of verification	Inclusion & analysis of questionnaire results in D5.6.
Methodology / tools	Questionnaires prepared by the consortium and distributed during the end-user workshops, including questions that cover security and privacy as an adoption barrier and whether IntellIoT alleviates said barrier. Post-workshops' analysis of results.
Baseline	N/A
Assessment Updates	Second (final) series of end-user workshops

iKPI-ID	i6.1
Description	Demonstrate interaction with at least 20 different IoT stakeholders who are external to the IntellIoT consortium, in the context of the ecosystem building activities of the project
Lead partner(s)	STARTUPC
Mapping to components & measurement points	N/A
Means of verification	Ongoing inclusion of involved stakeholders in Dissemination file, final list in D6.9
Methodology / tools	Organisation of own Meetups, inclusion of articles by IoT stakeholders in Medium Magazine, engagement with external players via Social Media Channels
Baseline	N/A
Assessment Updates	D6.9, final report on Dissemination & Ecosystem building

iKPI-ID	i7.1
Description	Successful safety and security assessment of the developed IoT environment for semi-autonomous behaviour of the farming vehicle
Lead partner(s)	SANL / TSI
Mapping to components & measurement points	Security & Trust components of IntellIoT
Means of verification	Deliverable D5.6
Methodology / tools	Verification through satisfaction of security and safety -related requirements specified for UC1, and the tractor in specific.
Baseline	Security and safety threats identified in UC1 scenarios.
Assessment Updates	Cycle 1 and Cycle 2 UC1 validation updates.

iKPI-ID	i8.1
Description	Clinicians time saving of 5%, without any loss of information for patient or specialist
Lead partner(s)	PAGNI / Philips
Mapping to components & measurement points	Healthcare AI models; Patients Data Repository
Means of verification	Comparison of unscheduled visits and emergency calls during each stage of the protocol, during the 1st and the 2nd phase of the protocol. Including time spent on all steps, such as accessing the system. Deliverable D5.6
Methodology / tools	Prospective evaluation.
Baseline	Time spent without using the system.

Assessment Updates	At delivery of the project and system.

iKPI-ID	i8.2
Description	Higher data quality and volume compared to the current context. We will reach 90% increase in data points collection in out-of-home settings compared with current situation (measured baseline)
Lead partner(s)	Philips
Mapping to components & measurement points	Local AI Component; Healthcare AI models
Means of verification	Comparison of amount of data collected by physicians before the project, with amount of data collected during the project. Measure properties of data that determine its quality. Deliverable D5.6.
Methodology / tools	Calculate amount of data before and after the project. Properties of data such as How to measure data quality and Measuring Data Quality.
Baseline	Data quality and volume at start of project.
Assessment Updates	At delivery of the project and system.

iKPI-ID	i8.3
Description	Patients achieve a 20% increase in their activity level (steps) and out of home walking time
Lead partner(s)	PAGNI
Mapping to components & measurement points	Security, Privacy & Trust components of IntellIoT. Smartphone Applications for Patients' Health and Fitness
Means of verification	Weekly reports of activity levels from smartphone exercise applications. Deliverable D5.6
Methodology / tools	Exercise and activity applications in smartphone. Messages that encourage people to achieve health and wellness goals, and remind them when they do not meet minimum goals.
Baseline	Recruitment / Enrolment
Assessment Updates	Continuous.

iKPI-ID	i9.1
Description	External stakeholders develop five additional manufacturing IoT applications based on the IntellIoT framework, e.g., through Open Calls or hackathons
Lead partner(s)	SIEMENS
Mapping to components & measurement points	Overall IntellIoT framework will be used as basis for application development.

Means of verification	Deliverable D5.6
Methodology / tools	Final demonstration will include showcasing external applications.
Baseline	N/A
Assessment Updates	Continuous

iKPI-ID	i10.1
Description	Delivery of open-source software components for the HyperMAS including libraries and tooling for researchers and practitioners to design, deploy, and manage IoT/edge infrastructures
Lead partner(s)	HSG
Mapping to components & measurement points	Web-based IDE for Hypermedia MAS Hypermedia MAS Infrastructure
Means of verification	This impact is reached if the software from these two components is available as open-source and together with documentation that enables outside users to utilize the software for running hypermedia-based multiagent systems in their own context. Deliverable D3.5.
Methodology / tools	Verification of access to source code and documentation of these components via a public code sharing platform such as GitLab/GitHub.
Baseline	N/A
Assessment Updates	End of project

iKPI-ID	i11.1
Description	Delivery of open-source components for 5G communication and dynamic network management supporting context-based and data-driven ultra-reliable low-latency communication for the NG IoT, as defined in Obj. 2
Lead partner(s)	EURECOM
Mapping to components & measurement points	5G RAN/CN; 5G RAN controller;
Means of verification	Contributions available on the OSA software library (https://gitlab.eurecom.fr/oai), either integrated or as stand-alone modules.
Methodology / tools	Access to OAI (RAN, CN, Mosaic5G) code on EURECOM hosted/administrated GitLab https://gitlab.eurecom.fr/ ; CD/CI methodology to keep new contributions in line with the stable code. Deliverable D4.7.
Baseline	OAI GitLab devel branch
Assessment Updates	OAI yearly workshops organized by EURECOM

iKPI-ID	i12.1
Description	Delivery of open-source AI algorithms and IoT/edge infrastructure components
Lead partner(s)	UOULU
Mapping to components & measurement points	AI components of all three use cases
Means of verification	D3.6 and dissemination
Methodology / tools	Delivery of algorithms and source codes
Baseline	N/A
Assessment Updates	Cycle 2 delivery components

iKPI-ID	i13.1
Description	Delivery of more than three standalone and re-usable innovative security tools and technologies developed within IntellIoT, in a form ready-to-be-adopted in other domains (in addition to the domains covered by use cases)
Lead partner(s)	TSI / SANL / AAU
Mapping to components & measurement points	Security, Privacy & Trust components of IntellIoT
Means of verification	Security, Privacy and Trust enablers detailed within D3.8 & D4.8.
Methodology / tools	Delivery of algorithms, source code and/or binary files and deployment and usage documentation for the core security, privacy and trust enablers of IntellIoT.
Baseline	N/A
Assessment Updates	Cycle 1 and Cycle 2 delivery of components.

6. CONCLUSIONS AND FUTURE WORK

This first version of Deliverable *Technology Analysis & Requirements Specification* (D2.2) captures the work that has been carried out in Cycle 1 of the project, focusing on Task 2.2 efforts. The main goal of the Task was to capture the state-of-the-art of technical solutions aimed at NGIoT and along with the use-case definitions (carried out within Task 2.1) and define a baseline of the expectations from the framework that IntellIoT aims to develop. These expectations are captured through the requirements specifications, namely the specifications of Functional and Non-functional requirements, as set from an end-user standpoint.

This is the reason that requirements are provided in such close knitting with the use-case scenarios that have been defined. The use cases are built upon user feedback and technology enablement. For this increment of the document, user feedback is mostly provided by the different industrial partners of the project, whose R&D and commercial activities are on the field of NGIoT applications and are engaged with real customers. External users (i.e., users outside the IntellIoT consortium) have also started to be engaged through initial discussions and preliminary workshops.

Along with requirements, the evaluation criteria have been specified. To evaluate whether the requirements have been met as well as the success of the project, two main sets of KPIs have been defined. The first set associates KPIs to the objectives of the project, while the second aims to associate the work that is carried out with IntellIoT with the impacts that it is aimed to have.

As this is the first increment of the deliverable, D2.2 aims to set the stage for the forthcoming activities. The first one, already initiated, is the specification of the IntellIoT Architecture and Interoperability of its different components in order to provide a coherent framework (Task 2.3). Based on the identified business value drivers, the state-of-the-art and progress beyond that aimed by consortium's technology providers, as well as the user requirements and expected performance outcomes, D2.3 will include a detailed architecture for the framework while it will also provide an additional set of requirements; namely, the Technical Requirements, that the framework will have to satisfy. Those will drive the technical work that will be carried out with the Work packages 3, 4 and the integration efforts of work package 5.

The completion of the first version of the deliverable marks the beginning of the second round of work within Task 2.2. As the first specifications and requirements for IntellIoT are set and development of technologies and tools commences, experimentation and evaluation work begin. D2.2 has already set the mark on how to start addressing those issues and during the work of the second increment, these are expected to start providing more robust definitions. For example, non-functional requirements that describe performance characteristics will be able to be defined more accurately, as through on-field deployment it will be possible to measure and evaluate more realistically different aspects (e.g., delay issues).

The initial deployment of certain IntellIoT technologies and the testing of different features is also expected to provide a broader and more expanded use-case definition with additional scenarios, scenes and added functionalities (captured through the second round of work for Task 2.1 and specified in D2.4). These will lead in a further refinement of the user requirements and expected performances that will be ratified in the second increment of this deliverable (D2.5).

Furthermore, external users are expected to be more closely integrated into the loop, by providing more thorough meetups and workshops that are going to demonstrate the initial concepts and work carried out within IntellIoT. As such, during the second phase of Task 2.2 (captured in D2.5), external user feedback is going to have a stronger effect on the definition of requirements and expected performances.

BIBLIOGRAPHY

[1] M. Blackstock and R. Lea, "IoT interoperability: A hub-based approach," in *2014 International Conference on the Internet of Things (IOT)*, 2014.

[2] D. Guinard, V. Trifa, F. Mattern and E. Wilde, "From the internet of things to the web of things: Resource-oriented architecture and best practices," in *Architecting the Internet of things*, Springer, 2011, pp. 97-129.

[3] A. Ciortea, S. Mayer, O. Boissier and F. Gandon, "Exploiting Interaction Affordances: On Engineering Autonomous Systems for the Web of Things," in *Proceedings of the Second W3C Workshop on the Web of Things*, 2019.

[4] M. Amundsen, RESTful Web Clients: Enabling Reuse Through Hypermedia, " O'Reilly Media, Inc.", 2017.

[5] S. Stadtmüller, S. Speiser, A. Harth and R. Studer, "Data-Fu: a language and an interpreter for interaction with read/write linked data," in *Proceedings of the 22nd international conference on World Wide Web*, 2013.

[6] S. Mayer, N. Inhelder, R. Verborgh, R. Van de Walle and F. Mattern, "Configuration of smart environments made simple: Combining visual modeling with semantic metadata and reasoning," in *2014 International Conference on the Internet of Things (IOT)*, 2014.

[7] M. Kovatsch, Y. N. Hassan and S. Mayer, "Practical semantics for the Internet of Things: Physical states, device mashups, and open questions," in *2015 5th International Conference on the Internet of Things (IOT)*, 2015.

[8] A. Ciortea, O. Boissier and A. Ricci, "Beyond physical mashups: Autonomous systems for the Web of Things," in *Proceedings of the Eighth International Workshop on the Web of Things*, 2017.

[9] O. Corby, C. F. Zucker and F. Gandon, "LDScript: a Linked Data Script Language," 2016.

[10] A. Ciortea, S. Mayer, F. Gandon, O. Boissier, A. Ricci and A. Zimmermann, "A Decade in Hindsight: The Missing Bridge Between Multi-Agent Systems and the World Wide Web," in *AAMAS '19 Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, Montreal, Canada, 2019.

[11] F. Gandon, "Distributed Artificial Intelligence And Knowledge Management: Ontologies And Multi-Agent Systems For A Corporate Semantic Web," Université Nice Sophia Antipolis, 2002.

[12] F. f. I. P. Agents, "FIPA Agent Message Transport Protocol for HTTP Specification, Document number: SC00084F," 2002. [Online]. Available: http://www.fipa.org/specs/fipa00084/SC00084F.html.

[13] J. A. a. S. R. Jose Exposito, "Configuring the JADE HTTP MTP," 2010. [Online]. Available: http://jade.tilab.com/documentation/tutorials-guides/configuringthe-jade-http-mtp/.

[14] R. T. Fielding, "Architectural styles and the design of network-based software architectures, PhD Dissertation," University of California, Irvine, 2000.

[15] A. Ricci, A. Ciortea, J. F. Hubner, R. H. Bordini, O. Boissier and S. Mayer, "Engineering Scalable Distributed Environments and Organizations for MAS," in *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems*, 2019.

[16] S. K. Das, "The measurement of flexibility in manufacturing systems," *International Journal of Flexible Manufacturing Systems*, vol. 8, pp. 67-93, 1996.

[17] A. Greenberg, J. Hamilton, D. A. Maltz and P. Patel, "The cost of a cloud: research problems in data center networks," *ACM SIGCOMM computer communication review,* vol. 39, pp. 68-73, 2008.

[18] E. Cuervo, A. Balasubramanian, D.-k. Cho, A. Wolman, S. Saroiu, R. Chandra and P. Bahl, "MAUI: making smartphones last longer with code offload," in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010.

[19] M. Satyanarayanan, V. Bahl, R. Caceres and N. Davies, "The case for vm-based cloudlets in mobile computing," *IEEE pervasive Computing,* 2009.

[20] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012.

[21] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila and T. Taleb, "Survey on multi-access edge computing for internet of things realization," *IEEE Communications Surveys & Tutorials,* vol. 20, pp. 2961-2991, 2018.

[22] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal,* vol. 3, pp. 637-646, 10 2016.

[23] Siemens, "Industrial Edge: Bring IT to the field level – easily, flexibly, and securely," 2019. [Online]. Available: https://new.siemens.com/global/en/products/automation/topic-areas/industrial-edge.html. [Accessed 29 11 2019].

[24] S. Yi, Z. Hao, Z. Qin and Q. Li, "Fog computing: Platform and applications," in *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, 2015.

[25] K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai and M. Satyanarayanan, "Towards wearable cognitive assistance," in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*, 2014.

[26] A. M. Haubenwaller and K. Vandikas, "Computations on the edge in the internet of things," *Procedia Computer Science,* vol. 52, pp. 29-34, 2015.

[27] S. Sardellitti, G. Scutari and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," *IEEE Transactions on Signal and Information Processing over Networks,* vol. 1, pp. 89-103, 2015.

[28] N. Mohan and J. Kangasharju, "Edge-Fog cloud: A distributed cloud for Internet of Things computations," in *2016 Cloudification of the Internet of Things (CIoT)*, 2016.

[29] V. Cardellini, V. Grassi, F. Lo Presti and M. Nardelli, "Optimal operator placement for distributed stream processing applications," in *Proceedings of the 10th ACM International Conference on Distributed and Event-based Systems*, 2016.

[30] ETSI - Industry specification group, "Multi-access Edge Computing (MEC)," 2018 - 2020. [Online]. Available: https://www.etsi.org/committee/1425-mec.

[31] K. e. al., "MEC in 5G networks," June 2018. [Online]. Available: http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf.

[32] ETSI, "MEC 5G Integration," [Online]. Available: https://www.etsi.org/deliver/etsi_gr/MEC/001_099/031/02.01.01_60/gr_MEC031v020101p.pdf.

[33] globenewswire.com, "Global 5G and Edge Computing Market Report 2020-2024: Multi-access Edge Computing (MEC) Deployments to Proliferate as Applications Demand Decentralized Computing," 20 11 2020. [Online].

Available: https://www.globenewswire.com/news-release/2020/11/20/2130752/0/en/Global-5G-and-Edge-Computing-Market-Report-2020-2024-Multi-access-Edge-Computing-MEC-Deployments-to-Proliferate-as-Applications-Demand-Decentralized-Computing.html.

[34] "Mosaic 5G," [Online]. Available: https://mosaic5g.io/ll-mec/.

[35] J. Seeger, A. Bröring and G. Carle, "Optimally Self-Healing IoT Choreographies," *ACM Transactions on Internet Technology (TOIT); arXiv preprint arXiv:1907.04611,* 2019; to be published.

[36] J. Seeger, A. Bröring, M.-O. Pahl and E. Sakic, "Rule-Based Translation of Application-Level QoS Constraints into SDN Configurations for the IoT," in *EuCNC 2019, Valencia, Spain*.

[37] ITU-R, "Minimum requirements related to technical performance for IMT-2020 radio interface(s)," 11 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf.

[38] P. Popovski, K. Trillingsgaard, O. Simeone and G. Durisi, "5G Network Slicing for eMBB; URLLC, and mMTC: a communication-theoretic view," *IEEE Access,* pp. 55765-55779, 2018.

[39] P. Popovski, Č. Stefanović, J. J. Nielsen, E. De Carvalho, M. Angjelichinoski, K. F. Trillingsgaard and A.-S. Bana, "Wireless Access in Ultra-Reliable Low-Latency Communication (URLLC)," *IEEE Transactions on Communications,* 2019.

[40] B. Yi, X. Wang, K. Li, M. Huang and others, "A comprehensive survey of network function virtualization," *Computer Networks,* vol. 133, pp. 212-262, 2018.

[41] A. Ikpehai, B. Adebisi, K. M. Rabie, K. Anoh, R. E. Ande, M. Hammoudeh, H. Gacanin and U. M. Mbanaso, "Low-power wide area network technologies for Internet-of-things: A comparative review," *IEEE Internet of Things Journal,* vol. 6, pp. 2225-2240, 2018.

[42] 3GPP, "TR 38.889 – Study on NR-based access to unlicensed spectrum," 2018. [Online]. Available: https://itectec.com/archive/3gpp-specification-tr-38-889/.

[43] 3GPP, "Study on architecture enhancements for the Evolved Packet System (EPS) and the 5G System (5GS) to support advanced V2X services," 2019. [Online]. Available: https://www.3gpp.org/DynaReport/23786.htm.

[44] 3GPP, "Architecture enhancements for V2X services," 2016. [Online]. Available: https://www.3gpp.org/DynaReport/23285.htm.

[45] 5G americas, "5G - The Future of IoT," 2019. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_White_Paper_on_5G_IOT_FINAL_7.16.pdf.

[46] K. Polachan, J. Pal, C. Singh and P. T. V, ""Quality of Control assessment for Tactile Internet based cyber-physical systems"," *arXiv,* october 2019.

[47] E. Barsom and M. S. M. Graafland, "Systematic review on the effectiveness of augmented reality applications in medical training," *Surgical endoscopy,* vol. 30, pp. 4174-4183, 2016.

[48] J. Arata, H. Takahashi, S. Yasunaka, K. Onda and e. al., "Impact of network time-delay and force feedback on tele-surgery," *International Journal of Computer Assisted Radiology and Surgery,* vol. 3, pp. 371-378, 2008.

[49] K. Antonakoglou, X. Xu, E. Stenbach, T. Mahmoodi and M. Dohler, "Toward haptic communications over the 5G Tactile Internet," *IEEE Communications Surveys and Tutorials,* vol. 20, pp. 3034-3059, 2018.

[50] S. Hirche and M. Buss, "Human-oriented control for haptic teleoperation," *Proceedings of the IEEE,* vol. 100, pp. 623-647, 2012.

[51] C. Schuwerk, X. Xu, W. Freund and E. Steinbach, "Transparency analysis of client-server-based multi-rate haptic interaction with deformable objects," *IEEE Word Haptics Conference (WHC),* pp. 506-511, june 2015.

[52] Z. Shi, H. Zou, M. Rank, L. Chen, S. Hirche and H. Muller, "Effects of packet loss and latency on the temporal discrimination of visual-haptic events," *IEEE Transactions on Haptics,* vol. 3, pp. 28-36, 2009.

[53] F. C. B. Brandi and E. Steinbach, "On the perceptual artifacts introduced by packet losses on the forward channel of haptic telemanipulation sessions," *International Conference on Human Haptic Sensing and Touch Enabled Computer Applications,* pp. 67-78, june 2012.

[54] E. Steinbach, M. Strese, M. Eid, X. Liu, A. Bhardwaj and e. al., "Haptic codecs for the tactile Internet," *Proceedings of the IEEE,* vol. 107, pp. 447-470, 2018.

[55] D. G. R. Van Den Berg, D. De Koning and e. al., "Challenges in haptic communications over the tactile Internet," *IEEE access,* vol. 5, pp. 23502-23518, 2017.

[56] G. A. Akpakwu, B. J. Silva, G. P. Hancke and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access,* vol. 6, pp. 3619-3647, 2017.

[57] P. Schulz, M. Matthe, H. Klessig, M. Simsek, G. Fettweis, J. Ansari, S. A. Ashraf, B. Almeroth, J. Voigt, I. Riedel and others, "Latency critical IoT applications in 5G: Perspective on the design of radio interface and network architecture," *IEEE Communications Magazine,* vol. 55, pp. 70-78, 2017.

[58] F. Chiariotti, O. Vikhrova, B. Soret and P. Popovski, "Peak Age of Information distribution for edge computing with wireless links," *IEEE Transactions on Communications,* 2020.

[59] A. E. Kalør, R. Guillaume, J. J. Nielsen, A. Mueller and P. Popovski, "Network slicing for ultra-reliable low latency communication in industry 4.0 scenarios," *arXiv preprint arXiv:1708.09132,* 2017.

[60] M. Bennis, M. Debbah and H. V. Poor, "Ultrareliable and low-latency wireless communication: Tail, risk, and scale," *Proceedings of the IEEE,* vol. 106, pp. 1834-1853, 2018.

[61] G. A. P. Gerardino, "Radio Resource Management for Ultra-Reliable Low-Latency Communications in 5G," 2017.

[62] 3GPP, "Study on NR industrial Internet of Things (IoT)," 2019. [Online]. Available: https://www.3gpp.org/DynaReport/38825.htm.

[63] M. Giordani, M. Polese, A. Roy, D. Castor and M. Zorzi, "Initial access frameworks for 3GPP NR at mmWave frequencies," in *2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net),* 2018.

[64] 3GPP, "Study on NR beyond 52.6 GHz," 2018. [Online]. Available: https://www.3gpp.org/DynaReport/38807.htm.

[65] 3GPP, "Overall description of Radio Access Network (RAN) aspects for Vehicle-to-everything (V2X) based on LTE and NR," 2019. [Online]. Available: https://www.3gpp.org/DynaReport/37985.htm.

[66] 3GPP, "Enhanced relays for energy efficiency and extensive coverage," 2019. [Online]. Available: https://www.3gpp.org/DynaReport/22866.htm.

[67] J. Park, S. Samarakoon, M. Bennis and M. Debbah, "Wireless network intelligence at the edge," *Proceedings of IEEE,* vol. 107, no. 11, pp. 2204-2239, November 2019.

[68] J. Kone{\v{c}}n{\'y}, H. B. McMahan, D. Ramage and P. Richt{\'a}rik, "Federated optimization: Distributed machine learning for on-device intelligence," *arXiv preprint*, vol. arXiv:1610.02527, 2016.

[69] W. Deng, M.-J. Lai, Z. Peng and W. Yin, "Parallel multi-block ADMM with O(1/k) convergence," *Journal of Scientific Computing*, vol. 71, no. 2, pp. 712-736, 2017.

[70] A. Elgabli, M. Bennis and V. Aggarwal, "Communication-efficient decentralized machine learning framework for 5G and beyond," in *IEEE Global Communications Conference (GLOBECOM)*, Hawai, USA, 2019.

[71] T. Chen, G. Giannakis, T. Sun and W. Yin, "LAG: Lazily aggregated gradient for communication-efficient distributed learning," in *Advances in Neural Information Processing Systems*, Montreal, Canada, 2018.

[72] T. Nishio and R. Yonetani, "Client selection for federated learning with heterogeneous resources in mobile edge," in *IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019.

[73] H. H. Yang, Z. Liu, T. Q. Quek and H. V. Poor, "Scheduling policies for federated learning in wireless networks," *IEEE Transactions on Communications*, vol. PP, no. 99, pp. 1-1, 2019.

[74] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," *arXiv preprint*, vol. arXiv:1909.07972, pp. 1-30, 2019.

[75] S. Samarakoon, M. Bennis, W. Saad and M. Debbah, "Federated Learning for Ultra-Reliable Low-Latency V2V Communications," in *IEEE Global Communications Conference (GLOBECOM)*, Abu Dhabi, United Arab Emirates, 2018.

[76] S. Samarakoon, M. Bennis, W. Saad and M. Debbah, "Distributed Federated Learning for Ultra-Reliable Low-Latency Vehicular Communications," *IEEE Transactions of Communications*, vol. PP, no. 99, pp. 1-1, 2019.

[77] E. Jeong, S. Oh, J. Park, H. Kim, M. Bennis and S.-L. Kim, "Multi-hop Federated Private Data Augmentation with Sample Compression," in *International Joint Conference on Artificial Intelligence (IJCAI-19)*, Macao, China, 2019.

[78] V. Smith, C.-K. Chiang, M. Sanjabi and A. S. Talwalkar, "Federated Multi-Task Learning," in *Advances in Neural Information Processing Systems (NIPS)*, Long Beach, CA, USA, 2017.

[79] H. Kim, J. Park, M. Bennis and S.-L. Kim, "Blockchained On-Device Federated Learning," *IEEE Communications Letters*, vol. PP, no. 99, pp. 1-1, 2019.

[80] J. Park, S. Wang, A. Elgabli, S. Oh, E. Jeong, H. Cha, H. Kim, S.-L. Kim and M. Bennis, "Distilling On-Device Intelligence at the Network Edge," *arXive preprint*, vol. arXiv:1908.05895, pp. 1-7, 2019.

[81] H. Cha, J. Park, H. Kim, S.-L. Kim and M. Bennis, "Federated Reinforcement Distillation with Proxy Experience Memory," in *International Joint Conference on Artificial Intelligence (IJCAI-19)*, Macao, China, 2019.

[82] J. T. C. G. B. G. Q. Y. a. Z. Y. Sun, "Lazily Aggregated Quantized Gradient Innovation for Communication-Efficient Federated Learning," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2020.

[83] A. J. P. A. S. B. C. B. I. M. B. a. V. A. Elgabli, "Q-GADMM: Quantized group ADMM for communication efficient decentralized machine learning," *IEEE Transactions on Communications*, 2020.

[84] M. M, R. A and T. A, Foundations of Machine Language Processing, Adaptive Computation and Machine Learning, Massachusetts: The MIT Press, 2012.

[85] R. S. Sutton, D. McAllester, S. Sing and Y. Mansour, "Policy gradient methods for reinforcement learning with function approximation," in *Advances in Neural Information Processing Systems (NIPS)*, 1999.

[86] E. Briman, "CEVA's Experts Blog," CEVA, 14 April 2016. [Online]. Available: https://www.ceva-dsp.com/ourblog/artificial-intelligence-leaps-forward-mastering-the-ancient-game-of-go. [Accessed 19 November 2019].

[87] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra and M. Riedmiller, "Playing Atari with Deep Reinforcement Learning," in *Neural Information Processing Systems (NIPS)*, Nevada, USA, 2013.

[88] H. Khan, A. Elgabli, S. Samarakoon, M. Bennis and C. S. Hong, "Reinforcement Learning Based Vehicle-cell Association Algorithm for Highly Mobile Millimeter Wave Communication," *IEEE Transactions on Cognitive Communications and Networking,* vol. PP, no. 99, pp. 1-1, 2019.

[89] F. Bu and X. Wang, "A smart agriculture IoT system based on deep reinforcement learning," *Future Generation Computer Systems,* vol. 99, no. 10, pp. 500-507, 2019.

[90] A. Elgabli, H. Khan, M. Krouka and M. Bennis, "Reinforcement Learning Based Scheduling Algorithm for Optimizing Age of Information in Ultra Reliable Low Latency Networks," *arXiv preprint,* vol. arXiv:1811.06776, no. 5, pp. 1-30, 2019.

[91] R. Soni, J. Guan, G. Avinash and V. R. Saripalli, "HMC: A Hybrid Reinforcement Learning Based Model Compression for Healthcare Application," in *IEEE International Conference on Automation Science and Engineering (CASE)*, Vancouver, BC, Canada, 2019.

[92] D. Xin, L. Ma, J. Liu, S. Macke, S. Song and A. Parameswaran, "Accelerating Human-in-the-loop Machine Learning: Challenges and Opportunities," in *Proceedings of the Second Workshop on Data Management for End-To-End Machine Learning*, Houston, TX, USA, 2018.

[93] L. Sun, C. Peng, W. Zhan and M. Tomizuka, "A Fast Integrated Planning and Control Framework for Autonomous Driving," in *the 2018 Dynamic Systems and Control conference (DSCC2018)*, Atlanta, 2018.

[94] A. Holzinger, M. Plass, M. Kickmeier-Rust, K. Holzinger, G. C. Crisan, C.-M. Pintea and V. Palade, "Interactive machine learning: experimental evidence for the human in the algorithmic loop," *Applied Intelligence,* vol. 49, no. 7, pp. 2401-24214, 2019.

[95] G. Hatzivasilis, I. Papaefstathiou and C. Manifavas, "SCOTRES: secure routing for IoT and CPS," *IEEE Internet of Things Journal,* vol. 4, pp. 2129-2141, 2017.

[96] G. Hatzivasilis, O. Soultatos, S. Ioannidis, G. Spanoudakis, G. Demetriou and V. Katos, "MobileTrust: Secure Knowledge Integration in VANETs," *ACM Transactions on Cyber-Physical Systems,* vol. 4, 2019.

[97] R. H. Khokhar, M. A. Ngadi and S. Mandala, "A review of current routing attacks in mobile ad hoc networks," *International journal of computer science and security,* vol. 2, pp. 18-29, 2008.

[98] N. Saxena, S. Grijalva, V. Chukwuka and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Communications,* vol. 24, pp. 88-98, 2017.

[99] T. Q. L. S. A. K. L. A. B. M. Z. A. &. M. Y. Wang, "Edge-Computing-Based Trustworthy Data Collection Model in the Internet of Things," *IEEE Internet of Things Journal,* vol. 7, no. 5, pp. 4218-4227, 2020.

[100] D. Airehrour, J. Gutierrez and S. K. Ray, "Secure routing for internet of things: A survey," *Journal of Network and Computer Applications,* vol. 66, pp. 198-213, 2016.

[101] R. Dalal, M. Khari and Y. Singh, "Survey of trust schemes on ad-hoc network," in *International Conference on Computer Science and Information Technology*, 2012.

[102] C. Lei, H.-Q. Zhang, J.-L. Tan, Y.-C. Zhang and X.-H. Liu, "Moving target defense techniques: A survey," *Security and Communication Networks*, vol. 2018, 2018.

[103] X.-L. Xiong, L. Yang and G.-S. Zhao, "Effectiveness Evaluation Model of Moving Target Defense Based on System Attack Surface," *IEEE Access*, vol. 7, pp. 9998-10014, 2019.

[104] A. a. B. G. T. Bajic, "A critical view on moving target defense and its analogies," in *Proceedings of the 17th ACM International Conference on Computing Frontiers*, 2020.

[105] G. a. S. G. a. C. L. a. H. X. a. J. S. Chen, "A Novel Model of Mimic Defense Based on Minimal L-Order Error Probability," *IEEE Access*, vol. 8, pp. 180481--180490, 2020.

[106] Y. a. C. G. a. J. S. a. Z. Y. a. C. Z. Zhou, "Cost-effective moving target defense against DDoS attacks using trilateral game and multi-objective Markov decision processes," *Computers & Security*, vol. 97, 2020.

[107] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou and A. Bouabdallah, "A systemic approach for IoT security," in *2013 IEEE international conference on distributed computing in sensor systems*, 2013.

[108] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet of Things Journal*, vol. 4, pp. 1250-1258, 2017.

[109] C. A. Ardagna, E. Damiani, J. Schütte and P. Stephanow, "A case for IoT security assurance," in *Internet of Everything*, Springer, 2018, pp. 175-192.

[110] H. Sato, A. Kanai, S. Tanimoto and T. Kobayashi, "Establishing trust in the emerging era of IoT," in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2016.

[111] G. Koschorreck, "Automated audit of compliance and security controls," in *2011 Sixth International Conference on IT Security Incident Management and IT Forensics*, 2011.

[112] T. C. Chieu, S. Dutta, A. Gupta, A. McKay, B. Prysock, R. Ramaratnam, A. A. Shaikh, M. Singh, C. Tang, M. Viswanathan and others, *Automated Validation of Configuration and Compliance in Cloud Servers*, https://patents.google.com/patent/US20130247136A1/en: Patent, 2013.

[113] S. Parthasarathy, S. Field, M. Goertzel, D. Kays, J. Dadzie and E. Reus, *Regulatory compliance across diverse entities*, https://patents.google.com/patent/US20130145027A1/en: Patent, 2013.

[114] F. Doelitzscher, C. Reich, M. Knahl and N. Clarke, "Understanding cloud audits," in *Privacy and security for cloud computing*, Springer, 2013, pp. 125-163.

[115] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE transactions on parallel and distributed systems*, vol. 24, pp. 1717-1726, 2012.

[116] E. Damiani, C. Ardagna and N. Ioini, Open Source Systems Security Certification, Springer, 2009.

[117] e. a. M. Anisetti, "A Test-based Security Certification Scheme for Web Services," *ACM Transactions on the Web* , 2013.

[118] M. Krotsiani, G. Spanoudakis and K. Mahbub, "Incremental Certification of Cloud Services," in *Proc. of SECURWARE*, 2013.

[119] C. Ardagna, E. Damiani, J. Schütte and P. Stephanow, " A Case for IoT Security Assurance," in *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*, Springer, 2018, pp. 175-192.

[120] e. a. C.A. Ardagna, "From Security to Assurance in the Cloud: A Survey," *ACM Computing Surveys (CSUR),* pp. 1-50, 2015.

[121] M. Anisetti, R. Asal, C. A. Ardagna, L. Comi, E. Damiani and F. Gaudenzi, "A Knowledge-Based IoT Security Checker," in *European Conference on Parallel Processing*, 2018.

[122] J. a. R. S. a. B. S. D. Sengupta, "A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications,* vol. 149, 2020.

[123] H.-N. Z. Z. a. Y. Z. Dai, "Blockchain for Internet of Things: A survey," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8076-8094, 2019.

[124] Y. Zhang, X. Xu, A. Liu, Q. Lu, L. Xu and F. Tao, "Blockchain-Based Trust Mechanism for IoT-Based Smart Manufacturing System," *IEEE Transactions on Computational Social Systems,* vol. 6, no. 6, pp. 1386-1394, 2019.

[125] R. Neisse, J. L. Hernández-Ramos, S. N. Matheu, G. Baldini and A. Skarmeta, "Toward a Blockchain-based Platform to Manage Cybersecurity Certification of IoT devices," in *IEEE Conference on Standards for Communications and Networking (CSCN)*, Granada, Spain, 2019.

[126] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *http://bitcoin.org/ bitcoin.pdf*, 2008.

[127] V. Buterin, "A next-generation smart contract and decentralized application platform," *https://github.com/ethereum/wiki/wiki/White- Paper,* 2013.

[128] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things (IoT)," *IEEE Access,* May 2016.

[129] L. L.-M. I. L. A. P. P. Nguyen, "Modeling and analysis of market Blockchain data trading in NB-IoT networks," *IEEE Internet of Things Journal,* 2020.

[130] S. Xu, M. Perez, K. Yang and e. al., "Effect of latency training on surgical performance in simulated robotic telesurgery procedures," *The International Journal of Medical Robotics and Computer Assisted Surgery,* vol. 11, pp. 290-295, 2015.

[131] P. Danzi and P. Popovski, "Towards blockchain networks tailored to IoT devices," *IEEE Blockchain technical briefs,* Jan 2019.

[132] P. Danzi, A. Kalør, R. Sørensen, A. Hagelskjær, L. Nguyen, C. Stefanovic and P. Popovski, "Communication aspects of the integration of wireless IoT devices with Distributed Ledger Technology," *https://arxiv.org/abs/1903.01758,* March 2019.

[133] L. Nguyen, K. A. E., L.-M. I. and P. Popovski, "Trusted wireless monitoring based on distributed ledgers over NB-IoT connectivity," *IEEE Communications Magazine,* vol. vol. 58, no. 6, pp. 77-83, June 2020.

[134] R. T. Fielding and R. N. Taylor, Architectural styles and the design of network-based software architectures, vol. 7, University of California, Irvine Doctoral dissertation, 2000.

[135] C. Bizer, T. Heath and T. Berners-Lee, "Linked data: The story so far," in *Semantic services, interoperability and web applications: emerging concepts*, IGI Global, 2011, pp. 205-227.

[136] D. L. Nguyen, I. Leyva-Mayorga and P. Popovski, "Witness-based approach for scaling distributed ledgers to massive IoT scenarios," *IEEE 6th World Forum on Internet of Things (WF-IoT),* 2020.

[137] "Industry specification group (ISG) on multi-access edge computing (MEC)," Industry specification group (ISG) on multi-access edge computing (MEC), 2018 - 2020. [Online]. Available: https://www.etsi.org/committee/1425-mec.