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

IntelliIoT

Open Call 1
Guide for Applicants

Submission starts September 1st, 2021, at 12:00 CEST
Submission deadline is November 1st, 2021, at 16:00 CET
Version 1.0

Table of Contents

1 GENERAL OVERVIEW

1.1 Overview and summary of the Open Call

IntellIoT, a pan-European research and innovation project funded by the European Union as part of the Horizon 2020 programme ICT-56-2020 "Next Generation Internet of Things", is organizing two Open Calls with the aim to involve startups and SMEs to build applications, services and extensions on the IntellIoT technical framework within special 6-month pilots (for each open call) that will be aligned with IntellIoT's 3 use cases.

The Open Calls will be used to gain feedback from the participants on the developed framework and technologies as well as to explore different novel business models applied by the Open Call winners. In case of Open Call 1, this feedback will be considered for the evolvement of the framework in its 2nd release. The Open Call 2 results will feed into the demonstration of the 2nd release of the IntellIoT framework and will aim to build a sustainable ecosystem beyond the project.

Applicants are invited to submit a short outline of their technology and business proposition, highlighting how they may integrate with the IntellIoT framework. The submissions will be evaluated by independent and external experts based on clearly outlined criteria, resulting in the selection of the four best companies per Open Call.

The four selected companies each gain access to the IntellIoT project within a 6-month pilot to work with the IntellIoT partners on the framework and use cases. In addition, the selected organizations will receive up to 150,000 Euro for their efforts in accordance with the selection criterion on economic fairness and as necessary to achieve the objectives of the action.

IntellIoT partner Startup Colors UG is responsible for the coordination of the Open Calls.

1.2 Introduction to IntellIoT

The overarching objective of IntellIoT is to develop a reference architecture and framework to enable IoT environments for (semi-)autonomous IoT applications endowed with intelligence that evolves with the human-in-the-loop based on an efficient and reliable IoT/edge- (computation) and network- (communication) framework that dynamically adapts to changes in the environment and with built-in and assured security, privacy and trust. This reference architecture and framework will be applied in the heterogeneous use cases encompassed in the project, covering **agriculture, healthcare and manufacturing** smart environments.

The IntellIoT project will mainly focus on three research aspects and associated next generation IoT capability pillars, namely collaborative intelligent systems (IoT), human interaction with the intelligent systems and that all these activities are performed in a trustworthy and secure way. These aspects result in three pillars, which are depicted in Figure 1, and are shortly described below.

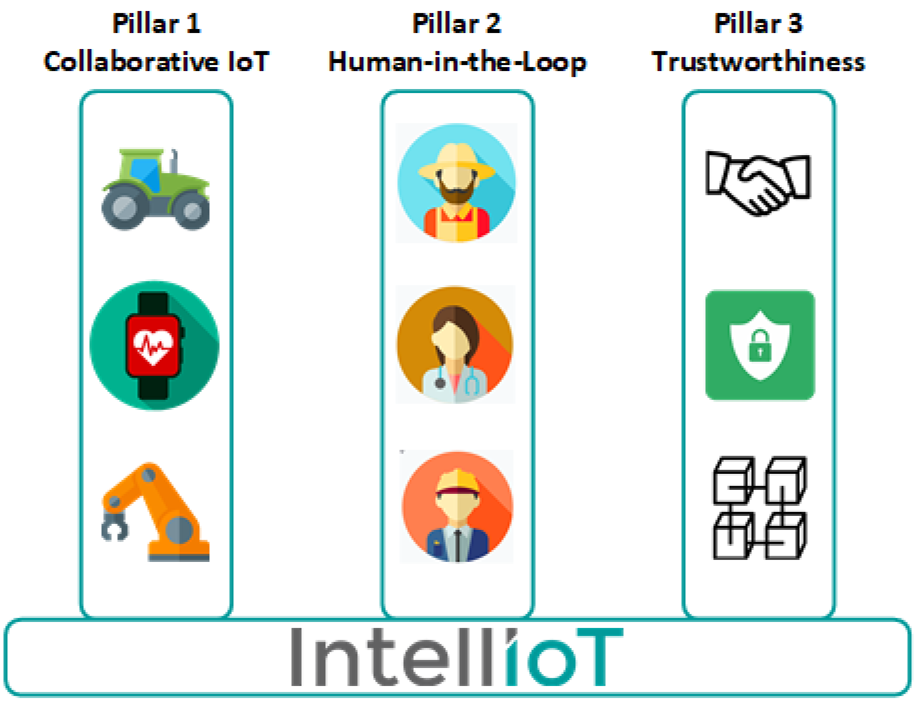


Figure 1: Three pillars of IntellIoT

1) **Collaborative IoT:** Various semi-autonomous entities (e.g., tractors, robots, healthcare devices, etc.) will need to cooperate in order to execute multiple IoT applications. These entities will have to be self-aware and will all have a different amount of knowledge of the task at hand and their environment where they are located. Unfortunately, it is not always possible to provide all the necessary knowledge to the entities, especially in changing environments. To keep the knowledge of the entities up to date, they need to extend it by applying learning technologies based on Artificial Intelligence and Machine Learning. New knowledge can either be acquired by interacting with the environment (via sensors) or by interacting with the other entities in the environment. By exchanging information via a reliable and secure communication network, the entities in the environment will need to collaborate with each other to update their own knowledge to fulfil their assigned task.
2) **Human-in-the-Loop:** The human within the system will keep on playing a crucial role in the whole process. The aim is to not remove the human from the system, but use his/her/their experience and knowledge to overcome unknown situations, where the system does not have the knowledge (yet) to handle the situation and the collaboration with the other entities in the field also does not provide the required information. The interaction with the human (be it either the machine operator, the farmer, the physician or any other person) will enable the intelligent system to expand its knowledge about the environment or the application through machine learning technologies and use the experience from the human operator to learn new features or information about the overall process. Therefore, humans will remain a vital element of the system and will interact with the IoT elements in the system to overcome the current limitations of the system.

3) **Trustworthiness:** Security, Privacy and, ultimately, trust are considered as indispensable preconditions for reliability and the wider acceptability of distributed, collaborative IoT systems and applications. Trust of the human (e.g., a patient or farmer) in the system is key, as the system's (autonomous) decisions need to be trusted, and the end-users' data need to be handled with utmost care, by providing appropriate levels of security and privacy safeguards. In this context, and in addition to well-understood security and privacy best practices, IntellIoT will adopt advanced security intelligence to protect unsupervised device-to-device interactions, based on self-adaptable, security-related operations. Furthermore, the overall trust will be fortified by continuous monitoring, real-time assurance assessment, and primitives enabling transparency of performed actions. Distributed ledger technologies (DLT) and smart contracts will be made accessible by IoT devices and other actors in the use cases to show transparency of performed actions, create trustworthy supply chains and build trust between parties.

1.2.1 THE INTELLIOT FRAMEWORK

The IntellIoT architecture is organised around the three pillars at the heart of the project's concept; i.e., Collaborative IoT, Human-in-the-loop, and Trustworthiness. Figure 2 provides a high level, simplified view of the IntellIoT framework and its building blocks.

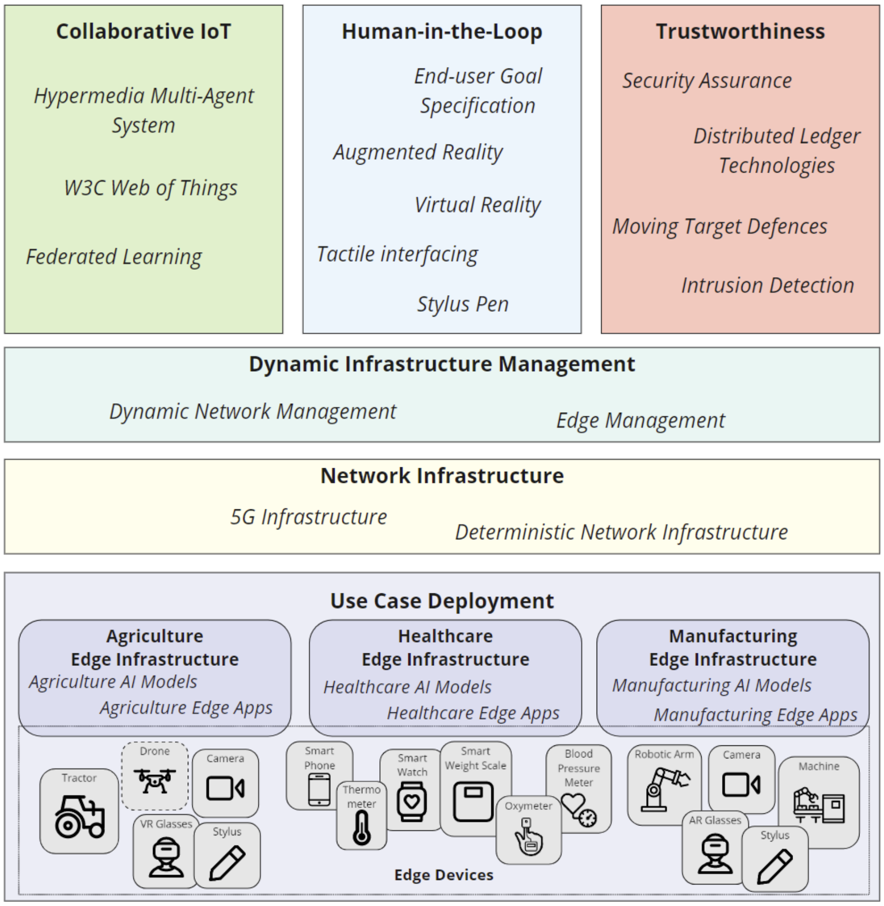


Figure 2: The IntellIoT framework – simplified view

In more detail, at the heart of the **Collaborative IoT** (system-wide AI) components is the *Hypermedia Multi-Agent System (HyperMAS) Infrastructure*; a multi-agent system that reacts to incoming end user goal specifications, managing - including discovery and search facilities - available artifacts and agents (defined in W3C WoT Thing Descriptions or W3C WoT Thing Description Templates) along with available procedural knowledge (i.e., agent plans). Moreover, *Federated Learning* is leveraged to prevent deployed model degradation, address edge cases, and implement data privacy and security.

In terms of the **Human-in-the-Loop** pillar, key elements include the *Goal Specification Front End* which enables the end user (e.g., farmer, customer, doctor) to specify the goal (e.g., "plant wheat in field 5"), sending it to the back end of the Web-based IDE that does the mapping from user goals to the input for the Hypermedia MAS and enables the systems engineer to monitor the system and to specify the agent organization and the procedural knowledge of individual agents. The IntellIoT features additional innovative Human-Machine Interface (HMI) capabilities, leveraging *Virtual Reality (VR)* and *Augmented Reality (AR)* technologies (based on Oculus Quest 2[1] and HoloLens 2[2], respectively – the

[1] https://www.oculus.com/quest-2
[2] https://www.microsoft.com/en-us/hololens

latter augmented by a *Stylus Pen*) to provide a user friendly, feedback rich and tactile way of interacting with and managing the underlying intelligent infrastructure.

Aiming to provide a solution with **trustworthiness** by design, a set of trust enablers are designed, developed, and integrated within IntellIoT. A *Security Assurance* platform acts as the trustworthiness hub within the framework, providing continuous, real-time assessment of the security and privacy posture of the underlying IoT deployment and IntellIoT itself. Moreover, novel, resource-aware *Distributed Ledger Technologies (DLTs)* are developed and integrated which are based on HyperLedger Fabric (HLF), and are leveraged to provide auditability, reliability, and accountability in all critical operations (transactions) within IntellIoT's deployed application domains. Furthermore, trust enablers include advanced (trust-based) *Intrusion Detection* systems which are augmented by *Moving Target Defence* mechanisms based on agents that administrate the IoT network at runtime to change the system's configuration both proactively and reactively when attacks are detected.

The above three pillars are supported - and their capabilities are enabled – by IntellIoT's dynamically managed network and compute infrastructure. In more detail, IntellIoT features computation resource management and edge management and orchestration capabilities, along with network choreography and management and xApp management and control features. The underlying network infrastructure supporting tactile communication is built upon *5G* (5G MEC, 5G vRAN, 5G D2D, Private 5G Core), and *Deterministic* - Time-Sensitive Networking (TSN) - technologies.

Moreover, use case-specific features are developed to support the application of IntellIoT in the project's three heterogeneous use cases, such as *UC-specific AI models* and *Edge Applications.* More details on the use cases are provided in the subsection that follows.

1.2.2 USE CASE DESCRIPTIONS

1.2.2.1 USE CASE 1 – AGRICULTURE

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

Nowadays, farmers are driving agricultural vehicles for many hours during the days, resulting in fatigue and finally in (potential deadly) accidents[3]. The aim is to remove the farmer from the cabin and have the agricultural vehicles drive autonomously over the farming fields, performing their tasks (e.g., harvesting) by themselves, thereby using the available data to optimize their required behaviour.

The scope of the agriculture use case is to investigate future autonomous features of farming vehicles, like autonomous driving, decision making and interaction and reliable communication with other entities (e.g., vehicles, drones, sensors) in the field. The interaction between the different entities in the field will create an intelligent IoT environment, where the different entities securely interact with each other and use this knowledge to update their own internal knowledge of the environment. Such knowledge is utilised to enhance the decision-making capabilities and communication aspects. Although the future aim is to remove the farmer from the cabin, humans should still play a big role in the control or supervision of the overall system. In this context, the aim of this use case is to incorporate the human-in-the-loop in the intelligent IoT environment of a semi-autonomous agricultural vehicle in collaboration

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

with other devices (e.g., drones, sensors, other tractors), while improving safety, reliability and security. Human intervention is needed in uncertain situations (e.g., animals on the path, dust or other particles, obstacles) and it is especially valuable in the initial deployments of smart farming.

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

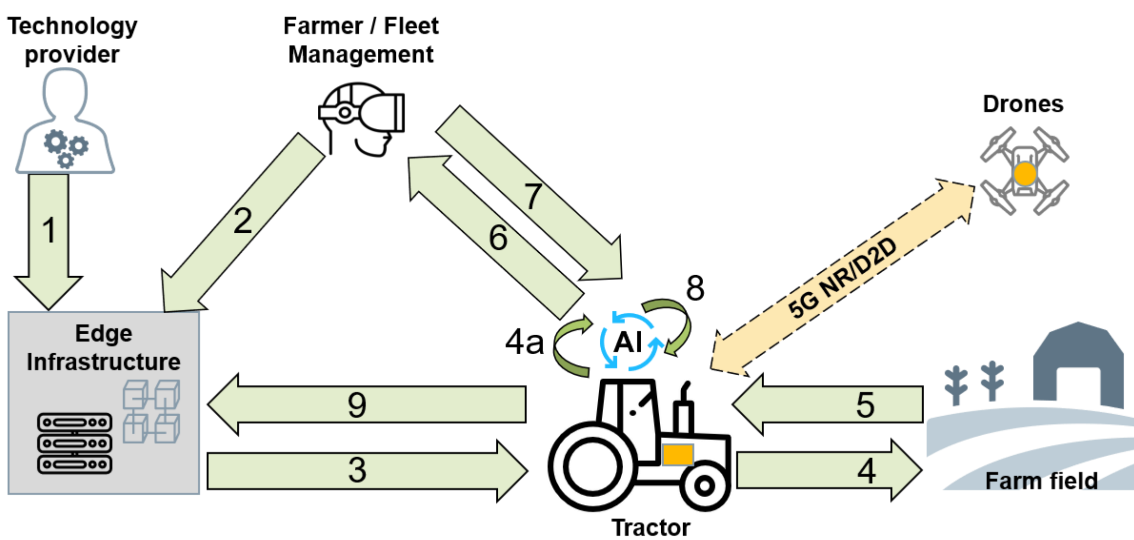
The high-level concept of the agriculture use case is depicted in Figure The use case will cover multiple facets of a smart agriculture deployment, where a tractor is driving over a farming field. The tractor will be equipped with sensors and computing resources to perform the mission assigned to it. The computing resources integrated into the tractor will enable it to perform computation tasks locally, thus acting as an edge device. Besides the tractor, there will be other edge devices in this use case, like a drone or an infrastructure edge. Tasks that cannot be performed on the vehicle will be offloaded to an available cloud infrastructure.

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

In the situation where an unknown obstacle is detected and the vehicle does not know how to traverse it, it will first try to collect complementary information or knowledge from the other entities via the Infrastructure Assisted Knowledge Management (IAKM) component. If required or compatible information cannot be found, the vehicle will stop and request help from the human operator. Utilizing a 5G NR connection, data from the tractor's sensors is sent to the VR glasses of the human operator. Part of the sent data is a video feed which will allow a view of the situation of the vehicle. If the provided feed does not provide enough information to allow finding a solution, the human operator can also access other entities in the field (other tractors, drones) to view the situation from different angles. The human operator will execute direct or indirect strategies. In the direct control, the human operator can directly interact with the vehicle (i.e., moving the vehicle forwards or backwards) using VR controllers. This will require a reliable, high-speed and low-latency connection that enables real-time interaction between operator and the vehicle. When using indirect control, a feasible trajectory around the obstacle has to be defined. Once this action is completed, the control needs to be given back to the vehicle. In this case, the human operator supervises the vehicle through the video feed to ensure that the newly defined trajectory is executed correctly. The indirect strategy has more relaxed latency and timing requirements for the communication. Based on the information coming from the human operator (be it either direct or indirect control), the vehicle will refine its own local AI models by continuously learning how to overcome such obstacles in the future, in addition to sharing the learned information (in an AI model) with other vehicles. The latter will be achieved by announcing the availability of the updated AI model tailored to the specific environment (using adapted semantics) via the IAKM. To this end, the IAKM will provide publish/subscribe mechanisms to exchange knowledge (in the form of AI models) or to seek environments required to learn or apply knowledge. Structured semantics will be used to describe various parameters related either to the model, to the environment, or to validity and applicability of the shared knowledge.

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

Furthermore, security concepts will be applied to allow access only to authorized devices but also to mitigate any intrusions to the network. While the vehicle is performing a mission, and a malicious entity (e.g., a drone that has been infiltrated by an attacker) tries to harm that mission, the security assurance mechanisms should be activated. The vehicle or its peers must identify the malicious entity and notify the cloud infrastructure. The infrastructure will then take measures to isolate the malicious entity, while making sure the vehicle, as well as any other legitimate entities continue functioning. To pre-emptively protect the network, periodic actions will be taken to dynamically reconfigure it, thus making any knowledge an attacker might have gathered, obsolete.



1. Functionalities upload
2. Define goal
3. Functionality deployment
4. Environment perception

4a. Semi-autonomous operation

5. Unknown obstacle
6. Request take over
7. In-/direct remote control
8. Update AI model
9. DLT access

Figure 3: Agriculture Use Case

1.2.2.2 USE CASE 2 – HEALTHCARE

Chronic diseases are a significant social and financial burden and the main cause of death world-wide[4]. There is a need for more effective strategies for patient management to improve patient outcomes and reduce healthcare costs. 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. Novel technologies can empower patients to become active partners in the treatment of their disease and contribute to effective strategies for secondary and tertiary prevention.

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

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

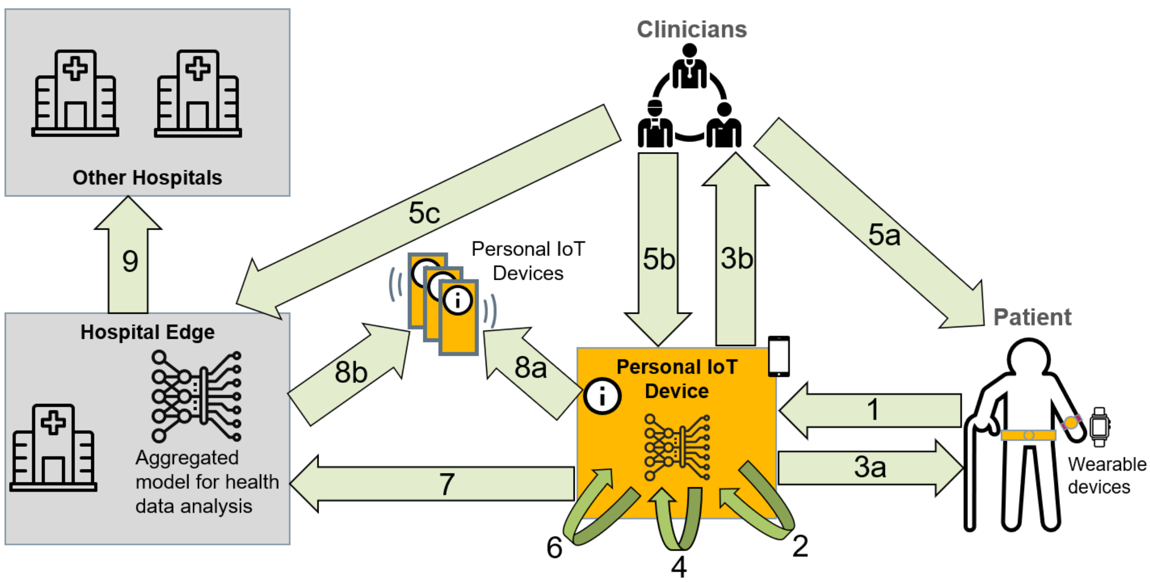
The main objectives of the healthcare use case are to design, develop and evaluate a platform combining novel IoT, communication and 5G technologies with an artificial intelligence framework and models enabling semi-autonomous collaborative patient support, with clinical oversight. We will apply and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

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

Figure 4 depicts key components, actors, and interactions of the proposed intelligent semi-autonomous system. IoT devices (wearables, sensors) will collect data that will be used by the AI infrastructure and models to provide recommendations and drive interventions, and to extract accurate information on the health status of the patients that are monitored in their home environment. The AI-assisted system will guide the patients through their daily activities and through their care plan, with clinical expert oversight. Patients will be equipped with wearable devices measuring relevant data that is transferred to a personal IoT device (e.g., smart watch or smart phone) via step (1). The AI application will analyse the collected data in step (2) to identify the need for interventions or recommendations, according to the initial AI models and the care plans and goals previously defined by the clinicians responsible for

[4] https://www.who.int/news-room/fact-sheets/detail/the-top-10-causes-of-death

treating the patients. When the need for an intervention is detected, either a recommendation is sent to the patient via step (3a) (with all the information sent to the patient, shared with the clinician as well for review), or the case is escalated to involve the clinician directly (e.g., when potential safety risks are detected), leading to the human-in-the-loop intervention depicted by step (3b). The solution will implement personalization approaches, tailoring interventions to the clinical needs and preferences of the individual patients. The goal is to both improve outcomes and increase adherence.



1. Health data
2. Data analysis
3a. Health recommendation
3b. Escalate to Clinicians
4. Device monitoring and diagnostics
5a. Direct recommendation
5b. Advice to personal device
5c. Broadcast to specialists or alarm
6. Re-train AI model
7. Model update
8a/b. Cross-patient model federation
9. Cross-site model federation

Figure 4: Healthcare Use Case

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

In the planned solution, when an escalation takes place and the clinical expert in the loop is notified, the clinician may decide to contact the patient as shown in step (5a), respond to the personal device shown by step (5b), send a notification to another specialist, or raise an alarm by step (5c). The feedback or recommendation provided by the clinician is persisted in the dataset. The local dataset is used as well to validate and re-train the AI model locally on a personal IoT device as shown in step (6), in order to increase personalization, potentially improve performance, and avoid performance degradation. Model updates are then contributed to the aggregated model at the coordinator that is deployed at the central infrastructure (e.g., of a hospital) shown by step (7) to enable its continuous improvement. This distributed AI framework will implement federated and active learning. Model updates are communicated to all personal IoT devices (e.g., using 5G Cellular IoT or D2D communications), through distribution of the aggregated model via step (8). All the involved communications and interactions need to be covered by state-of-the-art security and privacy provisions, catering for the intricacies of the private-sensitive user data. Digital consent management to drive the interactions of the system (patients, clinicians, devices) can be managed e.g., via smart contracts.

1.2.2.3 USE CASE 3 – MANUFACTURING

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

The *intelligent IoT environment* in this use case derives a production plan from product data received from a customer, selects machines for the planned production steps and plans optimized transport paths for workpieces. Smart contracts are concluded between customers, machine operators and plant operator – where at least the latter two are represented by digital agents. Transport is done by robots and Automated guided vehicles (AGVs), guided by in-built AI. Whenever built-in computing resources are insufficient, computation tasks are automatically offloaded to the edge cloud. Whenever AI is not sufficiently confident about a production step or workpiece handling, the intelligent IoT environment will involve a human-in-the-loop to take over control remotely. Using AR technologies, the human-in-the-loop assists the AI, which is concurrently trained with these new inputs. The infrastructure of IoT/edge and networking (within the machines and robots and to the operator) will enable tactile, reliable, secure and safe operation.

The *approach* of this use case is summarized in Figure 5 and entails the following components and actors, including their respective interactions: Instead of ordering a standard product, a customer (tenant) provides a specification for a product, i.e., a production goal, e.g., CAD-drawing and CAM-data, see step (1). A great variety of products can be built depending on the machines available in the shared manufacturing plant. Using additive manufacturing in addition to conventional machines (e.g., for drilling, milling, or welding), almost arbitrary products can be made. In a small-scale, but fully featured demonstrator of this use case, the customer provides text or an image to be engraved or lasered on a wood slice. In step (2), based on a given specification of the Hypermedia Multi-Agent System where a human engineer defines the system's organization and procedural knowledge using a Web-based development environment that is aware of the currently available artifacts (3), the system orchestrates suitable artifacts that represent available machines to manufacture the specified product. If the system cannot find a solution for the production goal, it can request support from a human plant operator or customer (3). In the proposed demonstrator, a wood slice (as raw material) is selected, and the AI decides how to place it in which machine(s) to engrave and/or laser text or image on it. Human help might be needed e.g., if the image is too large and must be cut or resized. Next, a robot or AGV is tasked to transport the workpiece (4) to the next production step. As a machine may be operated by the plant owner or a third-party operator, contractual arrangements are set up using a distributed ledger. Further, comprehensive security mechanisms are applied to ensure privacy and security of customer data. When a robot interacts with a machine, e.g., moves a part in the working area of a machine, a safe peer-to-peer communication relation between both can be setup ad hoc to protect from collisions. E.g., 5G communication is setup that supports wireless TSN and supports URLL not only in Uplink or Downlink, but also in Sidelink (D2D). In step (5), a local AI on board of the robot decides how the robot picks a workpiece and places it in the next machine. If the confidence-level of the local AI is low and it cannot pick and place the workpiece safely, a connection to a human is established (6). Utilizing AR, the human can **virtually grab the workpiece** to support the robot. A **tactile communication** is established for this interaction, under consideration of security and privacy. Cameras will generate an accurate enough reconstruction of the surroundings and the robot itself which allows the full control and visual information about the parameters of every joint. Grabbing and haptic feedback will be realized with the Holo-Stylus developed by HOLO. If support from a remote operator is needed, a tactile communication may not be possible through long-distance internet connection. Hence, the operator can **control a virtual robot (overlaying the scanned model with the CAD model)**, rendered in the local edge, with delayed movement of the real robot. From the human handling of the work piece, the **local AI re-trains** itself using the human feedback as target (7) and **federates the learned parameters** to other robots (8).

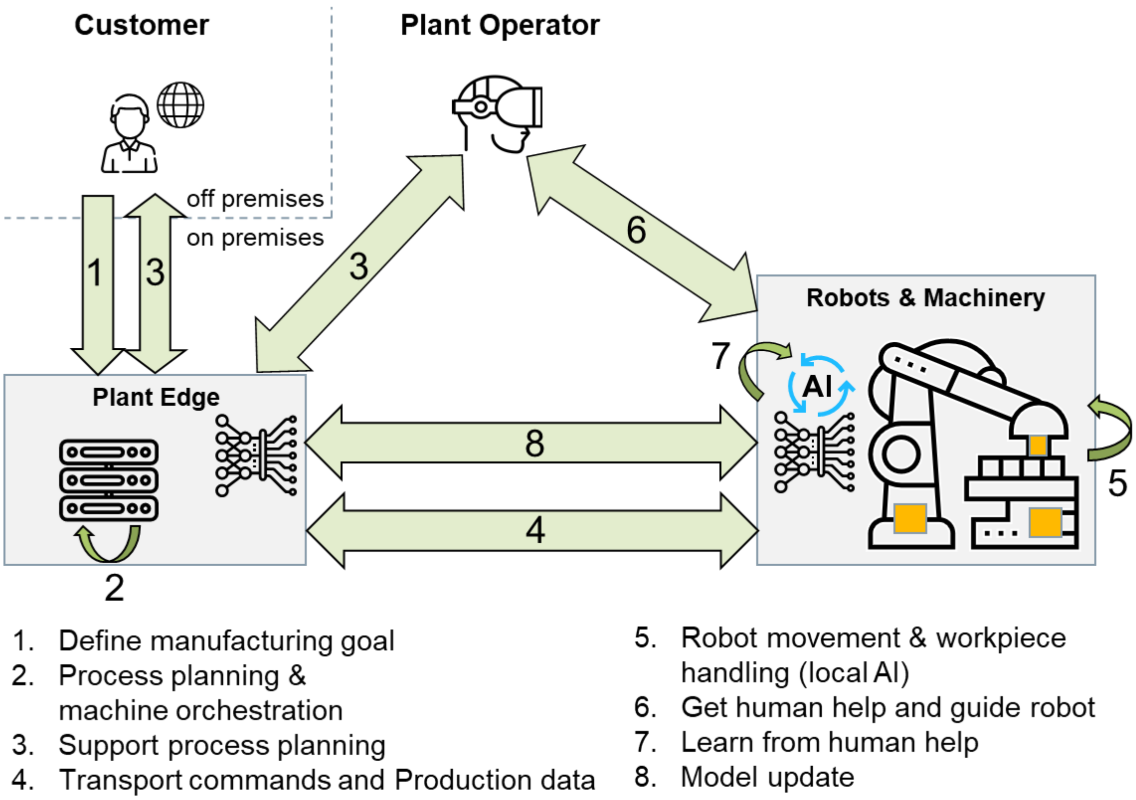


Figure 5: Manufacturing Use Case

1.3 What types of contributions are we looking for?

With the Open Calls, IntellIoT aims to widen the range of new and innovative IoT applications and devices within the framework and specific IoT environments of the use cases. To assure a consistent development of sustainable solutions throughout the use case implementations and upcoming activities, clear integration points with the IntellIoT framework need to be described in the Open Call proposals and realized during their execution. Moreover, it is intended to further develop the use cases already specified by providing additional tools, services, applications or devices. To ensure valuable addition to all use cases as well as the general framework, one proposal per use case and one proposal addressing the general framework will be selected.

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

1.3.1 EXEMPLARY CONTRIBUTIONS FOR THE GENERAL FRAMEWORK

To deliver the proposed framework, as sketched in subsection 1.2.1 above, the consortium (which includes large enterprises, SMEs/start-ups and academic institutions) brings together key expertise and heterogeneous state-of-the-art technologies for the next generation IoT. These include 5G communications, resource-aware edge computing, distributed AI, autonomous self-aware systems, DLTs, security & privacy for IoT, Tactile AR/VR HMI and vertical-specific know-how in the areas of agriculture, manufacturing, and healthcare.
Nevertheless, to further enhance the capabilities of the platform, but to also showcase the suitability of the core IntellIoT framework as a basis for an ecosystem that can be built on top of it beyond the project, we are seeking additional technological building blocks that can further expand the capabilities of the core framework and be applied horizontally across the project's use cases. Therefore, besides contributions that target one specific use case, we welcome contributions that are more general and can be applied across use case environments. Examples of such contributions are:

- **Digital Twin tooling:** Software that allows to create a digital copy of a physical object to enable simulations, advanced designing, and planning. Such a digital twin could make sense for example for the tractor in use case 1 or the robot arm in use case 3.
- **Edge and 5G Infrastructure:** IntellIoT has its own Edge orchestrator which handles placement of Edge Apps on different Edge devices. Open Call participants can bring project relevant edge applications/tasks to be handled by the Edge orchestrator. Prerequisite is for those apps to be dockerized and run in a x86 environment.
  For 5G infrastructure, Open Call participants can bring software and hardware that can setup a prototype 5G private network. IntellIoT will have its own 5G infrastructure setup, however, to test interoperability with other implementations, a further 5G network testbed could be meaningfully included. Furthermore, more MEC applications (xApps) can be added for advanced 5G MEC functionalities.
- **Blockchain-based marketplace:** Software that implements a user interface and underlying marketplace exchange to support service business based on IntellIoT's blockchain components (e.g., 3rd party agriculture or manufacturing machinery vendors).
- **Devices/tools to support human-machine interaction:** Hardware (e.g., HMI devices such as AR gloves) and software that enables intuitive remote machine or vehicle interaction, for example to control a robot arm in the manufacturing use case or to control the tractor in the agricultural use case. The solution should consider the cooperation with the AR/VR solutions used in the project. This could also involve the realization of simulation environments to train and validate the remote control of vehicles or machines.
  Web-based IDE as a tool for programming hypermedia-based multi-agent system also falls in this category. Together with a WoT Thing Description for constrained devices, the interoperability within heterogenous devices in the project can be demonstrated.
- **Data Analytics platform:** possibly a web interface, to be used by the human-in-the-loop and with log-in functionality. Data processing and Data engineering pipelines: clean and prepare the data collected by the sensors and make it available in the analytics platform, passing through the System Data Repository as appropriate.
- **Advanced sensing solutions:** The introduction of advanced sensing solutions (e.g., Sonar, Radar or LIDAR technology, Wireless Sensor Networks – WSNs) could be used horizontally across the project's use cases. E.g., in Use Case 1 to enable Precision Agriculture scenarios (e.g., deploying WSNs to monitor soil parameters), in Use Case 2 to enable Ambient Assisted Living (AAL) scenarios which consider the ambient environment of the patients, and in Use Case 3 to support additional logistics/supply chain scenarios (e.g., monitoring supply of spare parts). The Open Call participant would have to provide the hardware for scanning the environment, the software to transform the data into useful functionality and the interface that the project can link to.

- **AI models**: that can be federated, personalised and executed in Edge devices in all different use cases. Filtering 3D video data frames for minimal representation would be helpful in the federated learning approach. For the healthcare use case, AI models together with anonymized patient data from cardiovascular patients is requested to verify against the project's AI models.
- **Security and Privacy**: Mobile OS (Android) -focused security and privacy mechanisms for handling user data, Novel IoT authentication & authorisation schemes for resource-constrained environments.

1.3.2 EXEMPLARY CONTRIBUTIONS FOR THE AGRICULTURE USE CASE

In the agriculture use case, a semi-autonomous tractor will cover a field where it will traverse over and perform a simulated task like ploughing or mowing the dedicated field. A camera setup mounted on top of the vehicle will provide environmental information capable of driving it around the field and detect potential obstacles that could endanger the vehicle. The vehicle will collect environmental information and update its internal knowledge using AI algorithms to react to these situations. If an unknown situation occurs and the vehicle doesn't have the knowledge how to react to it, it will interact with other entities in the field (e.g., other vehicles or drones) or use the knowledge of a human operator to overcome the situation. To demonstrate the scalability of the developed solutions, the agriculture use case is looking for additional solutions that go beyond the available technology in the project and use these new technologies as proof that the results can be applied to a fleet of vehicles or a combination of vehicles and drones to provide additional sensory information to the overall setup of the agriculture use case. These can be combinations of real hardware of drones and/or simulated entities representing other agricultural vehicles and drones. New sensory information or other IoT technologies for improved human-machine interaction to improve the performance of the overall agricultural system are also being investigated for improving the performance of semi-autonomous and future autonomous agricultural solutions. Examples of such contributions are:

- **Digital Twin Tooling:** Digital twins of physical objects enable advanced simulations without having the actual objects available for testing purposes. In many test situations, the actual hardware is not available or only a very limited amount. Digital twins can e.g., be extended with Hardware-in-the-Loop testing equipment and provide multiple interfaces for interacting with the technologies developed inside the IntellIoT project to demonstrate the functionality of the system, without having actual access to the real hardware. Additionally, digital twins enable continuous testing, whereas deploying solutions on the real hardware reduces the testing capabilities significantly. Within the agricultural Use Case, the team is looking for an advanced simulation environment, capable of demonstrating functionalities of semi-autonomous agricultural vehicles (e.g., tractors, harvesters, but also potentially drones) and use these digital twins to demonstrate the scalability of the solutions and the cooperation capabilities between multiple vehicles to fulfil the assigned missions.
- **Drones:** Drones are being used more and more in the agricultural domain to provide among other additional sensory information to the vehicles deployed in the field. The aim of the IntellIoT project is to provide collaborative IoT, where multiple entities in the field (be it a fleet of vehicles or drones and vehicles) interact with each other by exchanging data and learn from the exchanged data to overcome situations that can not be handled by the limited data available by a single entity. The challenge here is to have the correct interaction between the drone and the designated vehicle. Additionally, exchanging data over reliable data channels (e.g. 5G) will also be investigated.
- **Smart Farming Solutions:** Hardware and software solutions for smart farming could be integrated with the IntellIoT framework (e.g., via the HyperMAS) to support the agriculture use case. Solutions could range for example from the integration of in-situ sensor networks or aerial imagery sensors to the analysis of such collected data to improve the efficiency of the farming. These new IoT technologies can also cover other topics, including improved human-machine interaction where a human operator can have improved interaction with vehicles or drones located at the field and either have better control over the vehicles or acquire more detailed information about the activities and status of the machines.

1.3.3 EXEMPLARY CONTRIBUTIONS FOR THE HEALTHCARE USE CASE

In the healthcare use case, we will implement privacy-preserving AI solutions leveraging federated learning approaches to provide personalized interventions to patients and support them and their clinicians with the effective management of the disease. Data will be collected from patients with a range of devices and will be leveraged to design, develop and apply interventions. Our goal is to propose and evaluate interventions, models and workflows that may help improve the currently available options for the home monitoring and support of heart failure patients, for better outcomes. We welcome innovative contributions with the potential to enhance the solutions provided to clinicians and patients in the IntelIoT ecosystem, including new models and datasets for model training and validation, and innovative devices and wearables that could provide valuable information on the health status of the patients. Examples of such contributions are:

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

1.3.4 EXEMPLARY CONTRIBUTIONS FOR THE MANUFACTURING USE CASE

In the manufacturing use case, a robot arm transports work pieces between machines and storages involved in the production process. A camera, mounted on the head of the robot, provides images of the scene the robot is working in, to the controlling AI and to the helping operator if needed. Thinking the use case in a bigger scale, alternative transport technologies would be required to transport different work pieces, e.g. workpieces of different shapes (from very small to very large, round, square cut and anything in between), different weights (from very light to very heavy), different materials (from soft to hard, from robust to fragile), different aggregation states (e.g. liquids, hot, not yet hardened plastic parts). Additionally, in a bigger plant with more machines, larger distances will have to be spanned. Flexible storage solutions might be required to store semi-finished products if bottlenecks occur in machine availability. New kinds of machines would be required to cover a larger range of possible production steps, potentially covering additive manufacturing or chemical or biological processing steps. New sensors might be required to detect properties of new materials in use, or to monitor the quality of completed or semi-finished products. Examples of such contributions are:

- **Automated guided vehicle (AGV):** Hardware (e.g., an AGV platform) and software to integrate the AGV into the IntelIoT framework (e.g., through HyperMAS adaptation) and to coordinate with other machinery/robots (potentially the AGV could also carry a robot arm).
- **Localization / navigation in manufacturing IoT environment:** Hardware (e.g., indoor positioning system) and software to integrate with the IntelIoT framework. After integration, this contribution could provide accurate positioning information, for example for AGVs transporting work pieces or mobile machines and storages.
- **Process industry machinery:** Hardware and software to adapt the IntelIoT framework to a process industry scenario (e.g., textile or food & beverages), which can meaningfully employ the developed technologies, e.g., to achieve modular designs and thereby contribute to a circular economy.
- **Additive manufacturing machinery:** Hardware (e.g., 3D printers) and software to integrate with the IntelIoT framework and contribute with advanced machinery to the manufacturing use case, e.g., by integration with robots.

- **New sensor technologies:** Hardware (e.g., radar or LIDAR) and software to integrate with IntellIoT framework and to support the manufacturing use case, for example to improve the robot arm interaction with the machinery or to handle work pieces with different material properties.

1.4 Financial support provided

The EC funding budget for Third Parties available for both Open Calls is 860,000 Euro. In each of the Open Calls, a total of four companies will be selected – one contributing to the general framework, and one for each of the three use cases.

The four selected companies each gain access to the IntellIoT project within a 6-month pilot to work with the IntellIoT partners on the use cases. In addition, the selected organizations will receive financial support of up to 150,000 Euro for their efforts in accordance with the selection criterion on economic fairness and as necessary to achieve the objectives of the action.

Within the Open Call 1, the funding available for selected companies is as follows:

- Up to 150,000 Euro for proposals addressing the general framework
- Up to 100,000 Euro for proposals addressing one of the three use cases

Within their application, participants have to describe the expected workplan for the 6-month pilot and the budget required for the successful execution of this workplan.

The beneficiaries will receive the funding as a fixed lump sum. The lump sum is a simplified method of settling expenses in projects financed from Horizon 2020 funds. It means that the grantee is not required to present strictly defined accounting documents to prove the cost incurred (e.g. invoices), but is obliged to demonstrate the implementation of the project in line with the milestones set for the Project. Simply speaking it means that we will assess your progress and quality of your work during Interim and Final Reviews, not your accountancy. The milestones (deliverables and KPIs) will be elaborated at the beginning of the pilot.

The lump sum does not release you from the obligation to collect documentation to confirm the costs under fiscal regulation.

In order to receive the grant, an individual Sub-Grant Agreement in accordance with Horizon 2020 funding rules has to be signed between the selected organizations and the IntellIoT consortium. SIEMENS AG, as coordinator of the IntellIoT project, will be responsible for transferring the grants in accordance with the above-mentioned process, and the following installments:

- **After contract signature**, a prepayment of **50% of the requested funding**, in order to avoid cash flow problems, will be issued.
- **One month after the end of the pilot** phase and after validation of an internally submitted progress report and Final Review, the **remaining 50% of the requested funding will be transferred**.

The Sub-Grant Agreement will include a set of obligations that beneficiaries have towards the European Commission. It is the task of beneficiaries to satisfy these obligations and of the IntellIoT consortium partners to inform beneficiaries about them.

An exemplary set of obligations:

- obligation to submit to any control measures (checks, reviews, audits or investigations) in relation to the participation in the IntellIoT project,

- obligation to keep records,
- obligation to provide information to the Coordinator or EC or other Consortium Members in order to verify proper implementation of the action and compliance with any other obligation,
- obligation to adhere to the ethics requirements of the project,
- liability for damages.

The selected companies shall be responsible for all possible taxes, wire transfer costs and other possible costs related to the payment of grants.

2 APPLICATION AND EVALUATION

2.1 Eligibility criteria

The IntellIoT Open Calls focus on involving startups and SMEs, in particular medium- and small-sized companies, as per definition from the European Commission (https://ec.europa.eu/growth/smes/sme-definition_en).

Please, be aware that while checking the company's status, if it's a SME, the linked parties of the company are also taken into consideration. SME status is calculated in accordance with the rules defined in the EU recommendation 2003/361.

As a summary, the criteria which define a SME are:

- Staff headcount in Full Time Equivalents (FTE) less than 250;
- Annual turnover less or equal to €50 million OR annual balance sheet total less or equal to €43 million.

IntellIoT partners and their related entities or entities in which IntellIoT partners have shares or other interest are excluded from participating in the Open Calls. The existence of potential conflict of interest among applicants and one or more Consortium partners will be taken into consideration.

Each proposal must be submitted by a single applicant, consortia are not allowed.

Organisations must be legally incorporated in the European Union or one of the Horizon 2020 Associated Countries to be eligible:

European Union member states (EU27):

Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

Countries associated with Horizon 2020:

Albania, Armenia, Bosnia and Herzegovina, Faroe Islands, Georgia, Iceland, Israel, North Macedonia, Moldova, Montenegro, Norway, Serbia, Switzerland, Tunisia, Turkey, UK and Ukraine. (The latest information on which countries are associated, or in the process of association to Horizon 2020 can be found at: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/3cpart/h2020-hi-list-ac_en.pdf)

Furthermore, entities taking part in the Open Call 1 are expected to:

- integrate with the IntellIoT framework (e.g., through the HyperMAS, or the computation & communication infrastructure),
- develop and provide scalable and future proof technologies / solutions, e.g., software or hardware, based on existing solutions of the applicant,
- keep deployed components alive at least until the end of the project lifetime (September 2023),
- provide access to collected data for the consortium of IntellIoT,
- demonstrate and present the final outcomes (and plans on their exploitations),
- provide feedback to IntellIoT technologies as input for the 2nd cycle.

IntellIoT

2.2 Proposal preparation

The Open Call proposal, as well as all corresponding documentation must be written in English. Proposals submitted in any other language will not be evaluated. English is also the only official language during the whole length of the pilot and, accordingly, any requested deliverables will be admitted only if submitted in English.

All applicants will have to submit an outline of their technology proposition, describing how their technology integrates with or extends the application of the IntellIoT framework within the use cases. In addition, they will have to describe how they intend to use the funding provided to realize optimal results during the 6-month pilot.

Applicants are not allowed to submit multiple applications. In case that more than one application from the same applicant is submitted, only the one submitted first will be considered and any other will be rejected.

Proposals must be submitted online through the IntellIoT Open Call submission platform on F6S. Proposals submitted by any other means will not be considered for funding.

Within the submission platform, limits for each of the proposal sections are defined which can not be exceeded.

The following sections are defined in the submission platform:

- General and company information
- Solution description
- Industrial relevance and impact
- Team
- Work plan
- Justification of resources and costs

2.3 Timeline

Each Open Call will be open for applications for at least 2 months.

Submissions for the first Open Call will be accepted from **September 1st, 2021, 12:00 CET until November 1st, 2021, 16:00 CET.**

The applications must be finally submitted through the online submission platform before the above-mentioned deadline to be accepted for the call. The Organizers might change the submission timeline at their discretion, the change in application timeline will be duly communicated.

The applicants are strongly recommended not to wait until the last minute to submit the proposal. Failure of the proposal to arrive in time for any reason, including extenuating circumstances, will result in rejection of the proposal.

After the closing of the application phase, all submissions will first be checked for eligibility. All eligible applications will then be evaluated as described below, and the winners shall be informed in December 2021. The 6-month pilots are expected to begin in February 2022.

2.4 Evaluation and selection process

The evaluation and selection process of the Open Calls is designed to create an open, accountable, multi-step selection process based solely on the merit of the submitted application. All submissions shall receive the same opportunity.

For each of the use cases and for the general framework, one proposal will be selected, i.e. four proposals in total. This means that proposals for one of the use cases are only competing with other proposals for that use case.

2.4.1 ELIGIBILITY CHECK

Submitted applications will first be checked according to the "Eligibility criteria" described in chapter 2.1., and those proposals which do not comply with those criteria will be excluded.

2.4.2 EXTERNAL EVALUATION

Each eligible submitted application shall be evaluated by a minimum of two independent and external experts. The experts will be individuals with experience in the fields of innovation linked to this Open Call and with the highest level of knowledge. All involved experts will sign a declaration of confidentiality concerning the evaluation process and the content of the proposals they evaluate. They will also declare their absence of any conflict of interest for the assigned tasks.

The experts will apply the criteria outlined below:

- **Relevance to IntellIoT**:
  - Usefulness: the degree of expected future use of the application, service or extension. The score should reflect the potential of the new component to be used by the IntellIoT technical framework or a future ecosystem build on top of it.
  - Complementarity: the degree to which the application, service or extension will provide new functionality that builds upon the functionalities provided by the consortium.
- **Impact and sustainability**: In which way the proposal contributes to further maturity and integration of NG IoT technology, and which are beneficiaries of the proposed solution. Further, there should be a guarantee of availability of the resources offered by the proposal after its open call pilot finishes and for how long.
- **Technical excellence**: Soundness of concept, quality of objectives and innovative elements of the proposal.
- **Quality of implementation**: Feasibility of the workplan, quality and effectiveness of the technical methodology, contribution to collaboration with IntellIoT to achieve objectives of the project, appropriateness of the allocation and justification of the resources to be committed (staff, equipment…).
- **Quality of the team:** Quality and relevant experience of the individual participants, quality of the team as a whole, including complementarity, balance, gender balance (applicants with female-led teams should be rated higher).
- **Economic fairness:** The requested budget should be adequate with the proposed workplan.

Each criterion will be scored between 1 and 6 points and only entire points are allowed:

- **1 (Fail):** Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
- **2 (Poor):** The criterion is addressed in an inadequate manner, or there are serious inherent weaknesses.
- **3 (Fair):** While the proposal broadly addresses the criterion, there are significant weaknesses.
- **4 (Good):** The proposal addresses the criterion well, although improvements would be necessary.
- **5 (Very Good):** The proposal addresses the criterion very well, although certain improvements are still possible.
- **6 (Excellent):** The proposal successfully addresses all relevant aspects of the criterion in question.

Each external evaluator will record his/her individual evaluation on each proposal using an individual evaluation form. The final score will be calculated as the average of the individual assessments provided by the evaluators.

Threshold for the first criterion, Relevance to IntellIoT, is 5, for all other criteria the threshold is 4. The overall threshold, applying to the sum of the individual scores, will be 27. Proposals which fail to reach these thresholds will not be considered for the funding.

In case the scores of the evaluators differ by (or more than) 3 points in at least one of the award criteria, the bias will be solved by involving the third evaluator in the process.

All proposals above the threshold will be passed to the consensus meeting.

2.4.3 CONSENSUS MEETING

After the external review, a Selection Committee formed by members of the consortium partners and external evaluators, will decide by Consensus the list of winners selected for the funding, as well as the "Reserve List". The discussion will be based on the ranking obtained as a result of the External Evaluation.

Whilst normally the highest ranked proposals will be selected for funding, the Selection Committee might have fair reasons for objecting to a specific third party, like the alignment with IntellIoT goals and scope, the ability to achieve the highest impact possible, commercial competition, as well as the existence of significant ethical concerns or a potential conflict of interest. In this case, the choice may pass to the next-ranked proposal.

In case of ties, the following criteria will be used to rank the proposals, in this order:

- Relevance to IntellIoT score
- Gender balance (female-led teams should be preferred)
- Impact and sustainability score
- Economic fairness score

The results of that consensus meeting will be recorded and applicants will be notified whether they have been selected or not.

2.4.4 SUB-GRANT AGREEMENT SIGNATURE

Before the pilot phase starts, we will ask you to sign the Sub- grant Agreement with the IntellIoT Consortium. To do so, we will ask you to provide documents regarding your formal status. Please do it within the deadlines that will be communicated to you. If you fail to deliver the requested documents on time, without clear and reasonable justification, we will exclude you from the further formal assessment and you will be replaced with a company from the Reserve List.

3 ADDITIONAL INFORMATION

3.1 Intellectual Property and Publication Rights

Participants retain full and exclusive ownership of their prior information and intellectual property rights. By submitting their application participants warrant that they hold ownership or have legally secured the right to use all elements of the technology. Participants shall indemnify and hold harmless the IntellIoT project partners, or any assignee or affiliate for any allegations or claims by third parties of infringement of intellectual property rights by the technology of participants.

Participants shall have the right to further develop, use and license their intellectual property rights for creating, making, marketing, and distributing products, services and technology.

By submitting their application forms, the selected companies agree to the possible inclusion of their technology in any media coverage by IntellIoT and its partners, such as press releases or publications. The content of such publications will be checked with the companies and only published after approval. Also, all winners agree that their personal data, such as their names and affiliations, pictures, videos and sounds may be used and processed for such purposes by IntellIoT and its partners.

The ownership of the IP rights arising from the development of a project, within the scope of this program, shall belong to the corresponding SME/consortium, as referred in the signed consortium agreement.

The following aspects will be considered in the agreement:

Knowledge management (IPR, data, and open access)

The *IntellIoT* consortium pays particular attention to the knowledge protection (background and foreground). The knowledge management and IPR protection strategy aims to be as open as possible to achieve maximum impact of the project results, so the default rule is for results to be public. The Innovation Manager together with the Technical Manager (see Section 3.2.1) will monitor this aspect closely and will initiate suitable actions in cooperation with the individual partners as well as their legal and technology transfer offices. In addition to the Grant Agreement, the partners will draw up a Consortium Agreement (CA) and address these aspects in the negotiations. Partners must follow this CA in all common or individual dissemination and exploitation activities. The knowledge produced will be continually tracked and registered to the respective owners, as follows: The mechanisms that the consortium will implement for managing knowledge and intellectual property deal with: (i) Management of both pre-existing know how brought in the project by a participant and of knowledge generated through the project; (ii) Protection of deliverables and prototypes; (iii) Publication of journal and conference papers; (iv) Open source and standards.

Background knowledge remains the property of the participant that brings it into the project. It is offered by the corresponding partner royalty free for the implementation of the project only.

Foreground knowledge is owned by the participant(s) creating it. This can be used by any of the partners for scientific/research purposes without any other obligation. It can also be used for commercial purposes by any of the partners according to the IPR agreement, which will be signed by all partners. Further, it cannot be used by others without the permission of the corresponding partner even if this is related to scientific/research purposes.

Deliverables and prototypes will be offered to the wider public through the website of the project. All other deliverables and prototypes will be protected by the IPR agreement. For all deliverables, a summary will be provided to the public through the website of the project.

Publication of journal and conference papers will be uploaded to the project website. Authors must obtain permission from the participant owning the foreground before submitting a paper for publication. Also, authors must carefully check the compatibility of the Grant Agreement with any publication agreement before signing off, and they must inform the publisher of the obligations resulting from the Grant Agreement. Regarding the latter, the project will follow an *open access* approach for all its scientific publications. It will opt for "green access" (i.e., self-archiving) whenever possible, to maximize the project's budget. Pre-prints of all scientific publications will be made available on the project website or on freely accessible online institutional websites or archives. In cases "green access" model cannot be adopted, the project will opt for a "gold open access" model (i.e., open access publishing).

Open source and standards will be influenced by the *IntellIoT* consortium in order to provide benefit for the European community. As outlined in Section 2.2.3, some of the project partners plan to contribute parts of their deliverables to open source projects and other partners plan to contribute to standardization.

Data generated or collected as part of the project will be carefully managed regarding privacy concerns of user related data, this is particularly the case for the health-related data of patients in the healthcare use case for which we have setup a dedicated ethics management in Task 1.3 that also deals with data de-identification procedures. The project will participate in the 'Pilot on Open Research Data in Horizon 2020' to make its research data available to a wide audience. Therefore, Task 1.2 will define the *Data Management Plan*, which details the types of data generated/collected, used standards, possible exploitation and data sharing for verification and re-use, as well as curation and preservation methods (and coverage of their costs).

3.2 Ethics requirements

Ethics is currently a topic in Artificial Intelligence standardization (e.g. ISO IEC JTC1 SC42), where there is a general consensus that they will not standardize ethics or ethical values. Ethical values are defined by the societal and cultural environment and may change over time. Therefore, it hardly makes sense to standardize these values and they are not a technology specific issue. What is important is that technologies may enable and provide new applications that may impact the ethical values of a society. A negative impact on these values will decrease the trust people have in the technology and hamper its acceptance by the society. Trustworthiness, the degree to which users and all stakeholders have confidence that a product or system will behave as intended, is therefore an issue for each technology. IoT trustworthiness aspects are mainly related to privacy, security and safety. *IntellIoT* therefore proposes to focus on IoT Trustworthiness.

As the use and impact of IoT and autonomous and intelligent systems become pervasive, we need to establish societal and policy guidelines for such systems to remain human-centric, serving humanity's values and ethical principles. These IoT systems must be developed and should operate in a way that is beneficial to the users and their environment, beyond simply reaching functional goals and addressing technical problems. This approach will foster the heightened level of trust between people and used IoT technology that is needed for its fruitful use in our daily lives. Typically, IoT systems are specifically designed to reduce the necessity for human intervention in our day-to-day lives. In doing so, these new systems are also raising concerns about their impact on individuals and societies. IoT systems/Machines do not, in terms of classical autonomy, comprehend the moral or legal rules they follow. They move according to their programming, following rules that are designed by humans. This requires ethical and values-based design, development, and implementation of IoT systems in *IntellIoT* use cases (Agriculture, Healthcare and Manufacturing), that should be guided by the following general principles:

- Human Rights: IoT shall be created and operated to respect, promote, and protect internationally recognized human rights.
- Well-being: IoT creators shall adopt increased human well-being as a primary success
- Data Privacy: IoT creators shall empower individuals with the ability to access and securely share their data, to maintain people's capacity to have control over their identity.
- Effectiveness: IoT shall provide evidence of the effectiveness and fitness for purpose.

- Transparency: The basis of a particular IoT decision should always be discoverable.
- Accountability: IoT needs to provide an unambiguous rationale for all decisions made.
- Awareness of Misuse: IoT creators shall guard against all potential misuses and risks of IoT in operation.
- Competence: IoT creators shall specify and IoT operators shall adhere to the knowledge and skill required for safe and effective operation.

IoT systems solve many real-life problems, but they create serious ethical concerns and legal challenges related to:

- Protection of privacy
- Data security
- Data usability
- Data user experience
- Trust
- Safety, etc.

Trustworthiness is the degree to which users and all stakeholders of IoT system have confidence that a product or system will behave as intended. Trustworthiness is a major issue for the acceptance of a technology by the society especially if applications enabled by a new technology may have negative impact on ethical values of the society. Standards can support adherence to ethical principles, while supporting a wide range of ethical value systems.

From an IoT point of view the following areas are of major importance when considering trustworthiness:

- Privacy: due to the vast amount of personal and related data that might be gathered by IoT applications
- Information security: due to the possibility to have access IoT devices from basically everywhere in the world in case they are connected to the Internet
- Safety: in case physical equipment and processes, which can lead to harm to humans, property and the environment, are controlled via IoT

It should be noted that these topics must be evaluated in a holistic view for a system taking its specific functionality/use case, the environment and all deployed technologies into account. IoT may introduce specific issues, vulnerabilities and threads related to a specific topic. ISO/IEC JTC SC41 has work items on a Trustworthiness Framework and Methodology for trustworthiness of IoT system/service.

Based on above general principles, concerns and legal challenges about Ethics, to reach the aims of the *IntellIoT* project, user and/IoT device data needs to be collected and stored, e.g., to develop distributed AI algorithms and applications in all 3 use case (Agriculture, Healthcare and Manufacturing).

Following paragraphs describe further details specifically in the healthcare use case where data needs to be extracted from existing infrastructures at the clinical site, de-identified, and processed for algorithm development and validation. Additionally, patients are enabled to access, communicate and process their health-related data. These (and related) actions can raise ethical and privacy implications. Therefore, the consortium will ensure that the proposed research activities comply with all legal and ethical requirements and that all necessary measures are taken to protect the rights of any data subject that could be involved. In no case, and under no circumstances, will the consortium do research activities that involve sensitive issues without considering EU legislation and proper authorisation from the Ethics Committee of the clinical partner, PAGNI, and of the other partners involved in the data processing tasks.

In the implementation of the healthcare use case, this work will leverage the support of PAGNI, who will drive the requirements regarding data protection, privacy, and appropriate use and management of the data. For the evaluation and for any retrospective patient data used for algorithm development, a study will be defined and submitted to the Ethics Committee of PAGNI and the Ethics Committees of the other partners that will use the data. All recommendations will be taken into account and the corresponding work will only proceed when the study is approved by the Ethics Committees. All parties will conform to the Declaration of Helsinki in its latest version and to the Convention of the Council of Europe on Human Rights and Biomedicine. The Consortium will prepare an Informed Consent Form that will be translated and enclosed in the Applications to the Local Ethical Committees. After local approval by the Ethical Committees the Informed Consent will be used in all the clinical centres participating into the project. Fully informed valid consent will be obtained from all patients participating to the study.

Approval for protocols involved in this project will be sought both at the coordinating institution ethical committee for the protocol, as well as at the ethical committees of each partner unit. No one's medical treatment is being compromised and participants know that they can withdraw or refuse their participation without this affecting their treatment in any way. Prior to the signature, the investigator, or a person designed by the investigator, fully informs the subject of all pertinent aspects of the study. In detail, subjects will receive a detailed verbal explanation in laymen's language by a trained clinician in the purpose and procedures involved in the project and will receive a written version of this explanation to take home.

Participation to the survey is entirely voluntarily. Before Informed Consent may be obtained, the patient is given ample time and opportunity to inquire about details of the study and decide whether to participate or not. Refusal to participate will have no consequences and will not involve any penalty or loss of benefits to which the subject is otherwise entitled. The subject may discontinue participation at any time without penalty or loss of such benefits. In case of withdrawal from the study, all stored material will be destroyed. The process of recruiting participants will not involve coercion in any way. The protection of privacy of the research participants, including third parties, will be ensured. Adequate level of confidentiality of the research data will be ensured.

The structure of the database will be such that individuals' anonymity is preserved. An independent reference database relating anonymized or pseudonymized codes to individual identities will be held separately in locked files which will not be accessible across network partners. Thus, files used for analysis of data by the partners will not include information that could be used to identify an individual or respective origin. Anonymity of individuals and organisations participating in the research will be ensured. Affiliations in any forms, sources of funding, as well as any possible conflicts of interests will be declared. The research will be communicated with honesty and transparency at all levels. Misleading and biased representation of data and findings will be avoided. Falsification, fabrication and misinterpretation of data will always be avoided. Works of other researchers and authors used in research will be referenced.

To further enhance our efforts concerning the implementation of the applicable EU and national regulations and the compliance with all legal and ethical requirements, our External Advisory Board includes Prof. Dr. Nikolaus Forgó who is a prominent expert on the topics of IT law, European data protection (EU regulations and their implementation in the member states), and related ethics aspects. Prof. Forgó will regularly provide feedback and recommendations on the relevant activities of the project.

Details on the procedure and criteria that will be used to identify/recruit research participants

The *IntellIoT* healthcare use case will conduct two types of tests (i) Lab tests and (ii) Controlled trials supervised by medical staff and/or caregivers. Only the second type of tests entails patient recruitment. The Lab tests aim to assess the technological properties (e.g. availability, reliability, connectivity, performance) of the system and to carry out the technical verification and validation. They will be conducted by the *IntellIoT* researchers.

On the other side, the controlled trials require the involvement of patients to assess the feasibility of the solution, the benefit to the users (in line with the defined KPIs), and the usability of the system, i.e. how the patients experience the technology and whether such solution is accepted by the envisaged target patient population.

Target group definition:

The controlled trial (an evaluation study comprising two iterations with two versions of the system) will be conducted with a group of 15-20 adult patients, living at home and for whom monitoring and physical activity for rehabilitation has been recommended by their clinicians. The participants will be recruited in Greece at the PAGNI site. End-users will be explained the objectives of the project and the details of the study and asked whether they are interested and willing to participate. The users who give consent, will be trained in the use of the system and provided with the necessary sensors and smart devices.

Inclusion criteria:

- Adult patients (>18 years old)
- Heart failure diagnosis
- Stable disease under treatment
- Good performance status and ability to be active
- Patients have received recommendation to increase physical activity
- Clinicians have found monitoring at home relevant for the patients
- Regular interaction between the patient and clinician is currently needed (e.g. patients are invited for regular meetings with their clinicians)
- Patients want to be active and aim to increase their independence and physical fitness

Exclusion criteria:

- Patients are bound to home or physical activity is not recommended
- Patients have specific issues preventing them from following the training and using the system.

General Guidelines for recruitment

The user selection process will be performed on-site by the medical experts comprising the clinical staff of PAGNI.

The details of the user selection methodology will be defined by the medical staff of PAGNI once the *IntellIoT* functionalities are established in a concrete implementation. Several expected key characteristics are:

- The patient recruitment is carried out by PAGNI staff well informed of the project and the study.
- The user is presented with the Informed Consent Form and is potentially willing to participate if found to be eligible.
- The user selection methodology includes a set of inclusion criteria and exclusion criteria to be applied in the selection/recruitment process.
- The initial visit will require approximately 1-1 ½ hour to complete, aimed to explain the study, confirm that the inclusion and exclusion criteria are met, and explain the consent form. At this visit, the relevant patient history will be collected, including medical, behavioural and social background information, and a routine physical examination will be carried out. A medical expert will decide based on the available information whether the user fulfils the recruitment criteria.

- When a user fulfils the eligibility criteria, details about the study and the *IntellIoT* solution are described to the user by their clinician (rationale behind the project, procedures, anticipated results and benefits, confidentiality, rights and obligations). This will be performed with the help of special dissemination material prepared.
- The user will be given ample time to read the 'Informed Consent Form' and to raise any project related questions. Before signing the forms, the clinician will establish that the user fully understands the study and agree with the study related procedures. A copy of the signed Informed Consent Form will be given to the user and another will be retained by PAGNI.

Details on incidental findings policy

During the project, new data and information that is potentially relevant for the patients participating in the pilot may become known to the researchers. The consent form will include a question asking the patients how they want such findings to be handled. If incidental findings occur and the patients have specified that they would like to receive the information, their clinicians will be informed. The clinicians will tell the patients about this new information and discuss as well whether and how this new information affects the patients.

Justification in case of collection and/or processing of personal sensitive data

The *IntellIoT* project aims to develop the Next Generation (NG) IoT and to enable the management of intelligent IoT environments, developing autonomous IoT systems with intelligence that evolves with the environment and with the interaction with humans as well as with the IoT devices. In the healthcare use case, we aim to demonstrate feasibility in a realistic environment and measure benefits to end-users (patients and clinicians). Measures of success target more efficient monitoring at a lower specialist resource utilization, more self-reliance and autonomy of the patients, better communication and connectivity. To convincingly evaluate these parameters, sufficient real-life data needs to be acquired and analysed.

Therefore, direct involvement of the users in the project is necessary, together with the acquisition and processing of all relevant data, which includes personal sensitive data. The users will be trained to use the system and will be provided with sensors and smart devices. During the evaluation pilots, personal sensitive data collected from sensors and devices will be de-identified, stored and analysed. The end-users will be asked as well to provide feedback on the usability of the system.

Protection of personal data

All data will be confidential, and patients will be given a Unique Patient Number, access to the data will only be allowed via a password and given to only authorized personnel involved in the Project. The coordinator will be responsible for ensuring that patient confidentiality is always respected. All these features are detailed in the Informed Consent Form presented to patients and thereafter undersigned by the patient and the researcher

Protection of personal data will follow the following principles:

1. <u>status of personal health data</u>: *IntellIoT* respects that personal health data form a part of the personality of the individual, and must not be treated as mere objects of commercial transaction.

2. <u>confidentiality / privacy:</u> *IntellIoT* investigators will ensure that the collection of, and access to, personal health data is limited to treating medical practitioners and to those third parties (non-treating medical practitioners, healthcare and social security personnel, administrators) who can demonstrate a legitimate use; this will be documented by an informed and required consent of the individual. All legitimate users of personal health data, even after death, have a duty of confidentiality equivalent to the professional duty of medical secrecy. Exceptions to this duty must be limited and provided for by legal rule.

3. self-determination: health data will be collected directly from the patient wherever possible and self-determination includes patients' right to know and to determine which personal health data are collected and recorded, to know who uses them for what purposes, and to correct data if necessary; the patient has the right to oppose the use of her/his data for secondary purposes not provided for by law;

4. principle of legitimate purpose: the principle of a strict relationship between the collection and processing of personal health data and handling and the legitimate purpose to which those data are used guides the collection of data; access to these data to third parties (e.g., insurers and employers) will be strictly denied and inaccessible within *IntellIoT*.

5. security: *IntellIoT* investigators will imperatively take care for security of individual data to ensure the respect for human rights and freedoms, in particular the confidentiality of data and the reliability in medical care; European security standards will be performed and rigorously monitored wherever an electronic transfer of person identifiable data occurs;

6. participation: the individual's right to participate in the medical decision-making process is a past and future key part of patient care, meaning accessibility of the patient will have access to his/her electronic health record.

7. transparency: standardization is a key feature of *IntellIoT* involving diagnostic procedures where classification and coding (clinical protocols, diagnostic related code, checklists, etc.) are in widespread use. As these standards are not neutral, but embody value-related choices, they will be transparent and may be subject to evaluation by independent bodies.

3.3 Data protection

The sole purpose of the collection of data is to verify the eligibility of the submitted applications and to identify the best proposals. Only for the purposes of the execution of the Open Call participants will provide name and email address ("personal data"). Startup Colors UG will process the submitted material according to the European General Data Protection Regulation (GDPR).

The evaluation of the submitted applications will be done within F6S (http://www.f6s.com), an online submission management tool by F6S Network Limited.

YOUR CONSENT TO THE USE OF F6S AS SUBMISSION AND EVALUATION TOOL: By submitting your application within this Open Call you implicitly state your consent to the F6S Terms and Conditions as well as the Privacy policy of F6S, available under https://www.f6s.com/terms and https://www.f6s.com/privacy-policy

YOUR CONSENT TO THE USE OF PERSONAL DATA: By submitting your application within this competition you consent that Startup Colors UG will collect, transfer, process, store and delete your data under above-mentioned conditions.

3.4 Coordinator & Contact

The IntellIoT Open Calls are organized by the IntellIoT project consortium. Startup Colors UG is responsible for the central coordination of the Open Calls, coordinating the dissemination, application, and evaluation process.

Open Call Coordinator is:

Startup Colors UG
Friedrichstraße 120, 10117 Berlin
Email: intelliot@startupcolors.com

For any enquiries regarding the IntellIoT Open Call topics and process, submission procedure, or any other general issues, please contact the coordinator.

3.4.1 COMPLAINTS

If, after receiving the results of one of the evaluation phases (when foreseen), you consider that a mistake has been made, you can send us your complaint. To do so please send us your complaint in English by email to: intelliot@startupcolors.com, including the following information:

- your contact details (including email address),
- the subject of the complaint,
- information and evidence regarding the alleged breach.

You have **5 calendar days** to submit your complaint starting from the day of becoming aware of the grounds for the rejection. We will review your complaint within no more than seven calendar days from its reception. If we need more time to assess your complaint, we will inform you by email about the extension.

We will not review anonymous complaints as well as complaints with incomplete information.

Please take into account that the external evaluation is run by experts in the IOT field, and we do not interfere with their assessment, therefore we will not evaluate complaints related to the results of the evaluation.

The Eligibility Check is carried out by the partners of the IntellIoT project. Should you have any concerns related to this evaluation phase, submit your complaints as described above.

3.5 Partners

SIEMENS	Siemens AG (headquartered in Berlin and Munich) is a global powerhouse in electronics and electrical engineering. Operating in the fields of automation, electrification and mainly also digitalization, Siemens holds leading market positions in all its business areas. For more than 171 years, Siemens stands for technological excellence, innovation, quality, reliability, and internationality. By discussing, sharing, and implementing ideas with scientists from outside the company, especially with 25 preferred universities and numerous research centers, Siemens researchers keep abreast of the latest findings resulting from fundamental and applied research all over the world. Concerning the IntellIoT Projects, three research groups will be involved: Industrial Networks, Wireless Networks and Mechatronic Systems. They combine research on communication technologies with applications such as (indoor) localization, as well as a holistic view on architectures and systems for the Internet of Things and mechatronics, such as robotic systems. This research finds its use in all Siemens business domains, e.g., in the definition and evaluation of the emerging 5G technology for the manufacturing shop floor, asset tracking for smart hospital management, the advanced engineering of intelligent office environments, or AI-based robot control.
EURECOM Sophia Antipolis	EURECOM is a graduate-level engineering school and research center that offers master and postmaster programs in the area of Digital Sciences and C-ITS. EURECOM is composed of three departments: Digital Security, Big Data and Communication Systems. The Communications Systems department (participating in this project) has a long expertise in cellular networks both from access stratum to cellular networking and management. EURECOM belongs to the Institut Mine Telecom and has 6 academics and 7 industrial members within its Economical Interest Group and is a founding member and strategy contributor to the Open5G Platform 'OpenAirInterface'. Thanks to its strong ties set up with the industry, EURECOM was awarded the "Institut Carnot" label jointly with the Institut Mines Telecom right from 2006.

AALBORG UNIVERSITET	Aalborg University (AAU) is a dynamic and innovative university of more than 20,000 students and 3,000 staff, with very strong engineering background and close ties with industry. AAU is engaged in more than 2600 externally funded research projects and has been continuously ranked among top institutions worldwide, e.g., according to US News World Ranking, as well as to the 2018 MIT report. The Department of Electronic Systems is one of the largest departments at AAU and is internationally recognized for the contributions in information and communication technology. Research activities are carried out in cooperation with industry and national and international research institutions. The project will be carried by Connectivity (CNT) section at the Department of Electronic Systems at AAU. CNT conducts research connectivity enablers, dominantly wireless, both in fundamental and practical aspects. CNT is well-known for its pioneering results in the field of Internet-of-Things, publishing innovative and original works on short-packet communications, advanced wireless access networking schemes for massive IoT and ultra-reliable low-latency communications (URLLC). CNT staff took part in the flagship EU research projects on 5G and IoT technology.
UNIVERSITY OF OULU	The University of Oulu is an international science university that creates innovation for the future, well-being, and knowledge through multidisciplinary research and education. The involved Centre for Wireless Communications (CWC) is a large university-based research unit operating within the Faculty of Information Technology and Electrical Engineering at the University. The objective of CWC is to provide a widely recognized, high-quality international research and learning environment for its 150 research staff members thus enabling the production of cutting-edge research results and novel innovations in cooperation with its research partners. The scope of CWC spans a comprehensive range of wireless telecommunications topics. The research builds on radio channel competence, expanding through communications signal processing and radio access technologies, finally addressing the wireless internet working domain. CWC also applies basic knowledge to the application of wireless technology in several fields, including 5G, medical ICT as well as energy and environment. The 5GTN developments serve as a major validation platform for the 5G FRINGE project. Previously, CWC has been one of the few academic partners from Europe to participate in the development process of 3G and IMT-A (4G) cellular standards.
TTControl HYDAC INTERNATIONAL	TTControl GmbH is a leading supplier in the field of safety controls, displays and connectivity solutions for mobile machinery. TTControl boasts a broad experience regarding commercial production projects in the domain of electronic control systems for mobile machinery that rely on their equipment to function under the most difficult environmental conditions. TTControl is a joint venture of the TTTech Group and HYDAC International, uniting two leading technology partners for the mobile machinery market. The TTTech Group is globally oriented and formed of high-tech companies providing leading real-time networking platforms and safety controls, while HYDAC International works with well-known global customers on projects requiring fluid technology in connection with hydraulics, electronics and engineering. TTControl is headquartered in Vienna, Austria and in Bressanone/Brixen, Italy and has access to a global sales network thanks to the HYDAC and TTTech Group offices worldwide. Including contractors and freelancers, more than 130 employees are working for TTControl.

TSI	The Telecommunication Systems Institute (TSI) is a National Research Institute founded by the Greek Ministry of Education in 1995. TSI operates within the framework of the Technical University of Crete as an administratively independent entity. Its mission is to spearhead basic and applied research in telecommunications and allied areas, contribute to graduate education, service, and outreach activities, and promote technological development at the regional and national level. TSI is entirely funded from external research and development grants and contracts in telecommunications and allied areas: telecommunication systems/networks and network services, networking hardware, sensors, RF, and high-performance computing systems, machine learning, information systems, big data analytics, signal processing for telecommunications, speech, language and image processing, and biomedical applications. TSI has had significant experience in FP6, FP7 and H2020 projects, including FET, acting on many occasions as coordinator. It has also adopted a strategy of promoting the commercial exploitation of R&D results, by providing services and contracting with industrial partners for specific products.
PHILIPS	Philips is a diversified health and well-being company, focused on improving people's lives through meaningful innovation in the areas of Healthcare and Consumer Lifestyle. The company is a leader in cardiac care, acute care, digital pathology, and home healthcare. In an increasingly connected world, the convergence of Philips' consumer technologies that facilitate healthy living, medical technologies that help clinicians to deliver better diagnosis and treatment, and cloud-based technologies that enable data sharing and analysis, will be a key enabler of more effective, lower-cost integrated health solutions. This fits very well with the core strengths of Philips in professional healthcare and in consumer health and well-being. The company brings expertise of applying IoT in healthcare, integrating consumer and clinical data to create smarter and more meaningful connected consumer and care solutions, enabling seamless patient care. Specifically, to healthcare, stringent requirements for data security, privacy, and regulatory compliance, make such integration a very challenging task as well as embedded software, supporting tailor-made solutions that maximize the performance of devices. This requires a combined expertise in the cloud, IoT security, regulatory and connectivity technologies.
Sphynx Analytics	Sphynx Analytics Ltd is a subsidiary company of Sphynx Technology Solutions AG, which offers solutions and consulting services, in the areas of big data analytics with a focus on analytics for cybersecurity, and for healthcare systems and services. The solutions offered are based on two core underlying technologies of its mother company Sphynx Technology Solutions, namely a model-driven big data analytics engine, and a complex event processing engine based in event calculus. Key innovative features of the analytics platform of the company include the realization of a model-driven data analytics approach in which analytics are embedded in the context of and driven by models that describe the decision-making based on the evidence arising from it, and the execution of trustworthy analytics (e.g., seamlessly embedded checks within the core computations of the SPARK platform services). Sphynx analytics offers also consulting services and has expertise in providing customized big data analytics and cybersecurity solutions tailored to client needs as well as more general training on analytics, security assessment and cyber intelligence.

Universität St.Gallen	The University of St. Gallen (HSG) was founded as a business academy in 1898, and is nowadays a School of Management, Economics, Law, Social Sciences, and International Affairs. While extending HSG's study programs towards Computer Science MSc and BSc degrees, it established its Institute of Computer Science in August 2018 with the creation of four initial chaired professorships. From HSG, the participating entity in the proposed project is the Chair of Interaction- and Communication-based Systems that is led by Prof. Dr. Simon Mayer. Within its research agenda, the team, which currently consists of eight individuals, explores interactions among devices and people in ubiquitous environments. Our focus is on the integration of physical things into the Web, on increasing the autonomy of Web-enabled devices and on making interactions of connected devices intelligible for people.
HOLO-LIGHT	Holo-Light is a tech company based in Munich, Germany, recognized as a pioneer in developing Augmented and Mixed Reality solutions for Enterprises, many of which are already implemented by global market leaders in several verticals and use cases. They are also pioneering in tackling the biggest issues in fully actualizing the potential of AR and MR. Through the development of deep tech, for example, they render 3D content remotely on edge computing systems and 5G infrastructures with low-latency data transmission. Their revolutionary input device Holo-Stylus (Winner in 2018 of the "German Innovation Award" and the "Auggie Award" for the best input device at Augmented World Expo in Santa Clara) allows users to naturally and precisely interact with 3D content.
AVL	AVL List GmbH is the world's largest privately-owned company for the development, simulation, and testing technology of powertrains (hybrid, combustion engines, transmission, electric drive, batteries and software) for passenger cars, trucks and large engines. AVL has about 4150 employees in Graz (Austria), and a global network of 45 representations and affiliates resulting in more than 10,000 employees worldwide. AVL's Powertrain Engineering division activities are focused on the research, design and development of various powertrains in the view of low fuel consumption, low emission, low noise and improved drivability. The Agricultural market is one of the most demanding but also exciting markets. Highest requirements and customer expectations regarding functionality, efficiency and comfort are the driving factors in this branch. One of the major challenges for the off-highway OEMs is to manage the application diversity in a cost-effective manner. Sophisticated tools and methodologies from AVL keep the development time and cost to a minimum. Based on the latest technologies, air to air communication, various sensor inputs and signal processing enable developments to optimize the complete process and increase production and quality.
Startup Colors	Startup Colors is a Berlin-based innovation and communications agency specialized in startup consulting, innovation strategy as well as ecosystem building. Founded in 2018, the agile agency is run like a startup with a team of 6 full-time and additional part-time and freelance experts. In the previous 10 years, working in the startup ecosystem in Europe, the Startup Colors team has worked with over 2000 startups. The company is a vivid supporter of international startup programs such as Startupbootcamp Digital Health Berlin, Startupbootcamp Mobility in Dubai, Techstar Retail in Berlin, Barcelona Health Hub, or enpact. Startup Colors will bring a broad, international network to technology startups into IntellIoT as well as experience in Open Call management and support. Together with very strong communication expertise, Startup Colors will be able to efficiently lead communication and

	coordinate the Open Calls as well as dissemination and ecosystem building activities. Further, Startup Colors will contribute to the exploitation and the definition of novel and disruptive business models through their experience with startups and design thinking.
ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΓΕΝΙΚΟ ΝΟΣΟΚΟΜΕΙΟ ΗΡΑΚΛΕΙΟΥ	The University General Hospital of Heraklion was founded in 1989 and is the major hospital in Crete, Greece. As a University Hospital, it shares a long-standing affiliation with the University of Crete. It covers a population of approximately 650,000 and has more than 750 beds and over 1,700 staff members. It is the referral hospital for the island of Crete and all the Aegean Islands. Cardiovascular services include heart care, heart surgery, and treatment for all types of heart disease. The Department of Cardiology at the University Hospital provides comprehensive evaluation, consultation, and medical and surgical management of diseases of the heart and circulatory system. With the latest technology, skilled physicians and compassionate staff, the department provides care for abnormalities of cardiac rhythm and conduction, coronary artery disease, cardiomyopathies, heart failure and valvular heart disease. The Hospital is also at the forefront of implementing Management Information Systems technology. Further, it is working actively in the development and advance of research in the sector of medicine and other relevant sciences. In this direction, it applies and develops research projects, scientific researches and collaborates with other relevant institutions as well as with international organizations on scientific and research projects.