D1.1 MIRAI Framework Requirements

Work Package	WP1
Dissemination level	Public
Status	Pre-release
Date	06/08/2021
Deliverable leader	Pedro Santos, ISEP
Potential Contributors	All

Contributors

Names	Organisation
Barış Bulut (BB)	Enforma
Sencer Sultanoglu	Eliar
Anna Hristoskova (AH)	Sirris
Nicolás González-Deleito (NGD)	Sirris
Sarah Klein	Sirris
Gregoire de Hemptinne	Shayp
Julien Deckx	3E
Geert Vanstraelen	Macq
Pedro Santos (PS)	ISEP
Luís Almeida	UPorto
Joana Sousa (JS)	NOS
João Tagaio	NOS
Nuno Martins	NOS

Reviewers

Names	Organisation
Baris Bulut; Burak Ketmen	Enforma
Nicolás González-Deleito	Sirris

Rev. #	Responsible	Comments
1.0	PS	First iteration.
1.1	PS	Small improvements over v1.0.
2.0	NGD, BB	Revision of version v1.1
3.0	PS	Addressed issues raised in v2.0, with all changes recorded and comments explaining options taken.
4.0	PS, JS, NGD, AH	Based as v3.0 with all changes accepted and no comments; only remaining subset of issues are commented. Reviewed and commented by JC, AH, NGD.
5.0	PS	Addressed issues raised in v4.0, with all changes recorded and comments explaining options taken.
6.0	PS	Based as v5.0 with all changes/comments accepted.

Table of Contents

List of Figures

Abbreviations

AI	Artificial Intelligence
ANPR	Automatic Number Plate Recognition
API	Application Programming Interface
AWS	Amazon Web Services
CPE	Customer Premises Equipment
DDoS	Distributed Denial-of-Service
EARS	Easy Approach to Requirements Syntax
GCP	Google Cloud Platform
HGW(s)	Home Gateway(s)
IoT	Internet of Things
IR	Infrared
MFBB	MIRAI Framework Building Blocks
ML	Machine Learning
MW	Megawatt
MWh	Megawatt-hour
NB-IoT	Narrowband Internet of Things
NN	Neural Network
OPC	Open Platform Communications
PID	Proportional-Integral-Derivative
PLC	Programmable Logic Controller
PV	Photovoltaic
UC(s)	Use Case(s)
VRU	Vulnerable Road User

Executive Summary

This document provides the deliverable of T1.1 of the ITEA3-MIRAI project, and contains the framework level requirements (i.e., global requirements) for the MIRAI Framework. Towards producing this set of global requirements, the following activities of the requirement elicitation phase were carried throughout T1.1:

1) Synchronization of the application scenarios by organizing workshops per application with all relevant project partners.
2) Provision of the basis for which the application partners can describe and refine the application scenarios and elicit the respective Business, Functional Non-Functional, and Technical requirements.
3) Identification of commonalities between the requirements of each application towards the creation of a list of requirements of the MIRAI Framework.

Found commonalities between the application requirements are to be used to focus the work in WP2-WP4 to develop the MFBB in a way that may flexibly serve a variety of end users.

This document contains the following elements produced throughout the task: the description and requirement elicitation per individual Use Case (UC) (Chapter 2), and the global list of framework requirements (Chapter 3). In both cases, produced requirements were assigned one of 4 classes: business, functional, non-functional, and technological. Support elements (template for UC description, mapping of UC requirements into global requirements) are also provided as appendices.

1 Introduction

We start this chapter by introducing terminology relevant to the comprehension of the document. The procedure followed to produce the list of Global Framework Requirements, as well as topics relevant to the classification and definition of the requirements, is presented next. The structure of the remainder of the document is also described.

1.1 Relevant Terminology

The definition of some terms is laid out for the sake of keeping the discussion throughout this document clear and unambiguous.

- **MIRAI Framework (MF, or simply "Framework"):** the Edge AI architecture being proposed under MIRAI. As stated in the **Rationale of the project** section in the FPP (or subsequent iterations): "MIRAI's mission is to design and create the first truly scalable edge computing software toolkit (MFBB) tailored for IoT and edge computing applications."
- **MIRAI Framework Building Blocks (MFBB):** components providing functionalities of the MIRAI Framework. It can refer to both conceptual specifications of MFBBs, or concrete instantiations of MFBBs in the target devices.
- **Target process/equipment:** process and/or equipment being monitored and/or controlled in each use-case (UC).
- **Business service:** the service that the UC owner currently provides and is planned for improvement by application of the MIRAI Framework.
- **Infrastructure:** the set of existing components (hardware or software; computing or communications-oriented; etc.) and any other kind of infrastructure that provide the business service. Typical key physical components are **edge nodes** and **cloud**.
- **MIRAI Service (or "Service"):** the service that the MIRAI framework is providing in each particular UC, improving the existing business service.
- **Solution:** the solution to be developed under the MIRAI project and that will provide the MIRAI service. Solutions will be composed primarily of MFBBs but builds on, and/or interfaces with, and/or integrates, components of the existing infrastructure that provide the business service. A solution can be thought of as a concrete instantiation of the MIRAI Framework. The term "solution" may refer specifically to MFBBs on the edge node, on the cloud nodes, or to all modules regardless of location (unless explicitly stated, the particular case must be inferred from context).
- **System operator:** person or agent in charge of managing the complete system, i.e., the set of the existing target process/equipment and infrastructure, and the solution provided by the MFBBs.

1.2 Use-cases Driving the MIRAI Framework

The following use-cases motivate and drive the development of the MIRAI framework.

- Use case 1: Distributed renewable energy systems (UC owner: 3E)
- Use case 2: Continuous auto configuration of industrial controllers at edge (UC owner: Eliar & Enforma)
- Use case 3: Traffic management (UC owner: Macq)
- Use case 4: Secure Internet provisioning (UC owner: NOS)
- Use case 5: Water management (UC owner: Shayp)

1.3 Procedure to Elicit Global Requirements

We describe the procedure to arrive to the Global List of Framework Requirements for MIRAI:

1) A template was prepared by the task leader and provided for partners to be filled with:
   a) Context, motivation, and description of their use case (UC)
   b) Title and definition of requirements of the UCs, organized under the following classes: **Business**, **Functional**, **Non-Functional**, and **Technological**.

   To the extent possible, the requirements definition followed the Easy Approach to Requirements Syntax (EARS) methodology (Section 1.4).
   The template provided to the partners can be found in Appendix A.
   The output of this initial step can be found in Section 2.
   On occasion, partners provided additional context or comments to motivate the requirements, that was decided to keep for informational purposes (identified as *"Additional Comments"* next to the UC requirement definition).

2) In a task meeting (held on March 30th, 2021), with most partners, the full set of requirements was reviewed and verified for common requirements, leading to an initial set of global requirements.
   The output of this meeting can be found in Appendix C.

3) The initial proposal of global requirements was improved to a first consolidated version. To do so:
   a) The title of each global requirement was revised and improved for clarity and scope.
   b) A definition was produced for each global requirement.

4) Each of the original UC requirements was mapped into one or more of the global requirements. Guidelines to this process are described in Section 1.6.
   The output of this mapping can be found in Appendix C.

5) The set of Global Requirements was further revised for:
   a) Category: the requirements were categorized into *Business*, *Functional*, *Non-Functional* and *Technological*, following the definitions of Section **Erro! A origem da referência não foi encontrada.**.
   b) Relevance: two criteria were applied: "Number of UCs that have that requirement" and "Relevance to the MIRAI vision" (as described in the **Rationale of the project** section in the FPP, or subsequent iterations).
   c) Similarity/overlap to existing requirements.

   The consolidated Global Requirements can be found in Section 3.

1.4 Requirement Identification Format

Both UC and Global Requirements were given an identifier of the type <UC owner>-<type-of-req acronym>-<number>. The acronyms are: **BR**-Business Requirement; **FR**-Functional Requirement; **NFR**-Non-Functional Requirement; and **TR**-Technological Requirement. Example: *Shayp-BR-1*.

1.5 Proposed Requirement Syntax Guideline

The Easy Approach to Requirements Syntax (EARS)[1] is a methodology for constraining the syntactic description of requirements. Examples:

- *Generic EARS syntax:* While <optional pre-condition>, when <optional trigger>, the <system name> shall <system response>.
- *Ubiquitous requirements:* The <system name> shall <system response>.

[1] https://alistairmavin.com/ears/

- *Event driven requirements:* When <trigger>, the <system name> shall <system response>.

The partners were proposed, to the extent possible, to formulate their requirements using this methodology.

1.6 Methodology for Mapping UC to Global Requirements

To map the UC requirements into Global Requirements, the following guidelines were used:

1) All UC requirements were evaluated for match with a Global Requirement. Some UC requirements may be mapped into more than one Global Requirement; likewise, Global Requirements may be supported by more than one UC requirement. There was no merging of UC requirements. Not all UC requirements were mapped into a Global Requirement.
2) Given that there is some heterogeneity in the criteria used to classify UC requirements into *Business*, *Functional*, *Non-functional* and *Technological*, and that the criteria for Global Requirements also ends up being different, an UC requirement and the corresponding Global Requirement may be of different categories. The criteria used for the Global Requirements is described in the next section.
3) Some important Global Requirements did not have a specific UC requirement onto which to map, but would be found in the UC description or implicitly in the definition of other UC requirements. In Section 3, when listing UC requirements that support a global requirement, we identify such cases by adding the tag *implicit*.

For the process of eliciting the global requirements, the criteria for assigning a class to a requirement was based on the following definitions:

- **Business:** relating to the target service from a business perspective and/or to economic aspects of the operation of the system.
- **Functional:** a functionality that the MF (and MFBB) must provide to the target system/service.
- **Non-Functional:** other types of requirements such as *operational* (what should the system do to provide the functionality; way in which the MFBB should provide a given functionality), *design* (what already existing components must be integrated, where should components be deployed [physically or logically]), among others that may be relevant.
- **Technological:** particular technologies that must be used and or integrated with MF.

1.7 Document Structure

The remainder of this document is organized as follows.

- Section 2 presents the description and requirements of each UC by the respective partners.
- Section 3 lists the Global MIRAI Framework Requirements.
- Section 4 draws some final remarks on this deliverable.

2 Definitions of Use cases

The description and requirements of each use-case (UC) by the respective partners are presented next, per UC. Each use-case subsection is composed of three parts:

- The first two parts, “Context/Motivation”, “Use-Case Description” are left at the discretion of the UC owners. Enforcement of MIRAI terminology is relaxed.
- The third part, “Requirements for the Framework”, strives to enforce introduction of MIRAI terminology (“MIRAI System”, “edge node”, etc.) as opposed to partner/UC-specific terminology.

To guide partners in the process of identifying UC requirements, the template available in Appendix A was provided to partners.

2.1 Distributed Renewable Energy Systems (UC owner: 3E)

2.1.1 Context/Motivation

With SynaptiQ, 3E provides a hardware agnostic platform-as-a-service solution for the management of distributed renewable energy assets (e.g., inverters in a photovoltaic plant). The current architecture of SynaptiQ is shown in Figure 1.

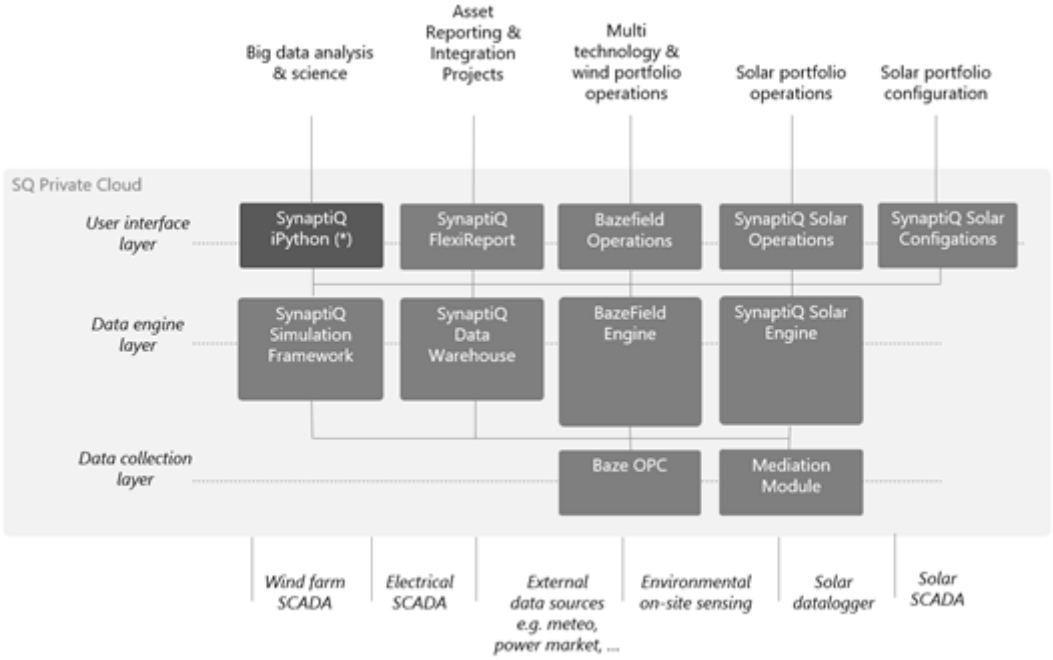

Figure 1. SynaptiQ Architecture

SynaptiQ is used by the Operations & Maintenance (O&M) responsible to the plants where such assets are deployed. Existing functionality focuses on performance optimisation for the production of solar and wind energy.

The responsibilities of O&M operators are ever increasing, from guaranteeing availability of the plants, to guaranteeing energy yield, to even guaranteeing a certain cash flow in the future. This is achieved in the following ways:

- Switching off the plant when market prices are negative (due to too high energy offer).
- Maximizing self-consumption of renewables.
- Selling flexibility on short-term and balancing markets. This means that you can get relatively high revenue for instantly turning your net energy output up or down to help balancing the total power balance of the electric grid.

To be able to provide the services listed above, the assets connected to SynaptiQ need to be flexible assets, which are able to shift energy:

- Flexible loads, like electric heating, ventilation and air-conditioning (HVAC), which can be switched off and on at different times.
- Batteries, which can be charged and discharged at different times.
- Electric vehicles (EV), which can be charged at any time throughout the day, and new generations can also be discharged (so-called vehicle-to-grid).

The abovementioned evolutions have the following impact on the functionality of SynaptiQ:

- Moving from one-directional (monitoring only) to bi-directional communication (enabling control features).
- Moving from near real-time to real-time status updates.
- Moving from aggregation of information of plant assets for monitoring purposes to optimized control of those assets.

2.1.2 Use case Description

As emphasis shifts from plant availability to revenue maximization, renewable plant operators are looking for ways to control different assets to maximize revenue. This use case focuses on optimized control.

Actors: Solar or wind plant operators (one operator is responsible for a large number of plants)

Context / Setting: multiple Photovoltaic (PV) and/or wind plants, complemented by one or more of the following assets:

- Building with flexible loads
- Industrial production with flexible loads
- Battery
- EV charging stations
- Programmable Logic Controller (PLC) programmed to react to grid signals (this PLC can also be used as edge device)

Service: maximize revenue by continuously monitoring and optimizing the control of assets mentioned above based on the following input:

- Energy production (current & forecast)
- Load (current & forecast)
- Market prices (current & forecast)
- Battery state of charge (SoC)
- EV state of charge (SoC)

The maximization of direct revenue is balanced with other constraints: maximize comfort, maximize battery lifetime, respect EV availability.

Infrastructure/equipment: solar panels, wind turbines, buffer server, EV charging stations, batteries.

Agents Involved: plant SCADA, PPC hardware, building management system, battery management system, EV charging management system, aggregator.

2.1.3 Requirements for the MIRAI Framework

2.1.3.1 Business Requirements

ID: 3E-BR-1
When wholesale market prices are negative, the solution shall turn off the plants to avoid losing revenue.

ID: 3E-BR-2
When energy production varies throughout the day due to changing meteorological conditions, the solution shall vary flexible loads in order to maximize self-consumption of generated energy.

ID: 3E-BR-3
When short-term electricity prices fluctuate throughout the day, the solution shall charge and discharge a battery to maximize revenue.

ID: 3E-BR-4
When balancing prices are high, the solution shall push settings to the local PLC (edge node) to reserve a certain amount of power for balancing services, which the System will provide as a pre-aggregator.

ID: 3E-BR-5
The solution shall continuously calculate the optimum between Reqs. 3E-BR-1 to 3E-BR-4, optimizing the control of assets both on a local level (individual plant) and on a portfolio level (group of plants owned by the same entity).

ID: 3E-BR-6
The proposed cloud-edge solution will compete with pure local solutions. As a consequence, the bi-directional real-time communication to the cloud should be as lean and cost-effective as possible.

2.1.3.2 Functional Requirements

Figure 2 below gives a rough outline of the different functional blocks. The green blocks are relevant to the MIRAI project.

ID: 3E-FR-1
The solution’s cloud forecast shall continuously forecast production, load and prices based on market input and the production and consumption data from the plants.

ID: 3E-FR-2
The cloud optimization shall continuously calculate the optimal set points to the flexible assets in order to maximize revenue based on forecast production, load and prices. These set points will be compiled into a schedule for the next time period.

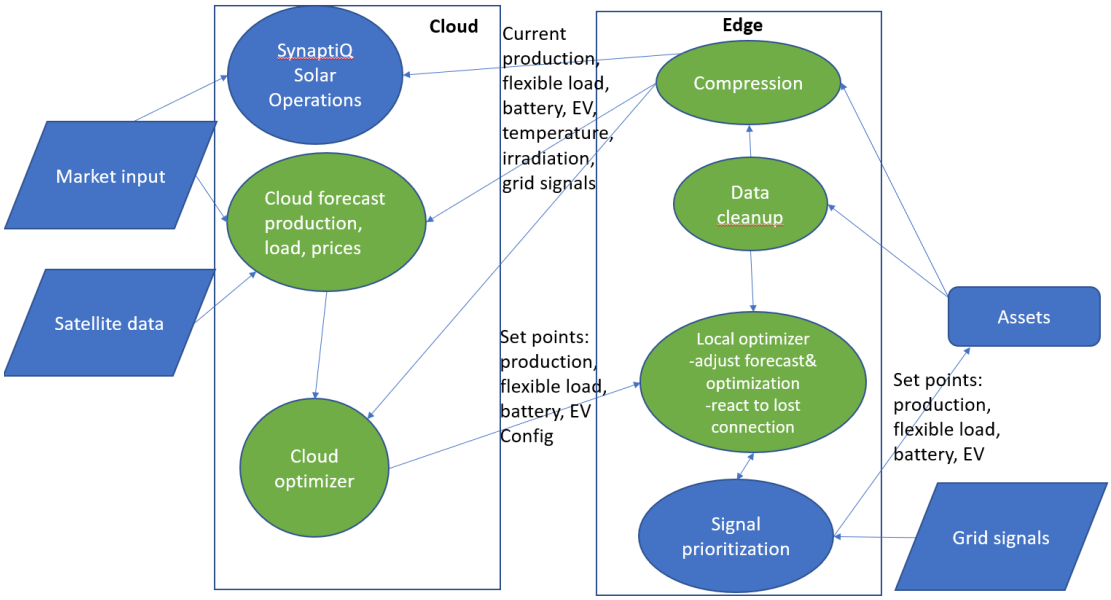

Figure 2. Functional Blocks of 3E system.

ID: 3E-FR-3
The data clean-up shall clean up the real-time data coming from the assets to correct for missing or incorrect data.

ID: 3E-FR-4
The local forecast (i.e., at edge node) shall predict the local production and load based on the local real-time data.

ID: 3E-FR-5
The local optimization (i.e., at edge node) shall continuously adjust the schedule of the cloud optimizer as a function of the real-time data. For example, it will react to instantaneous variations in production to avoid injecting power into the grid when possible.

ID: 3E-FR-6
When the edge node loses access to the cloud, the local optimization (i.e., at edge node) shall execute the locally available schedule for as long as it is available from the global optimization and then revert to the default fallback.

2.1.3.3 Non-Functional Requirements (Operational, Design, etc.)

ID: 3E-NFR-1
A portfolio of distributed energy production assets, controllable from the cloud, is a high commercial and strategic risk. The risk of intrusion should be minimized.

ID: 3E-NFR-2
If an attack is ongoing, the solution shall provide a detailed report in real time or near real time during the attack, and resume after it.

2.1.3.4 Technological Requirements

ID: 3E-TR-1
The solution shall allow for implementation on different types of generic local hardware (Industrial PC, PLC, Raspberry Pi, …).

ID: 3E-TR-2
Bi-directional real-time communication should be established between the edge devices and the cloud.

ID: 3E-TR-3
The compression module will compress the real-time data stream at the edge node with minimum information loss to reduce the required bandwidth in the connection with the cloud, reduce cost, optimize performance & storage, etc.
Additional comments: Implementation can happen in 2 steps: 1) Use existing compression algorithms on the edge 2) Implement a new algorithm with data loss Requirements for new algorithm: • The compression algorithm must preserve enough precision for performance monitoring and analytics. • A recompression must yield the same compressed data as the original compression. • There must be a reference implementation available in either Python, Java or Lisp. Decompression must be fast.

2.2 Continuous auto configuration of industrial controllers at edge (UC owner: Eliar & Enforma)

2.2.1 Context/Motivation

Textile dyeing process is a batch process which takes 5-12 hours depending on various process parameters such as fabric to be dyed, desired colour, chemicals and dye. Eliar Elektronik produces Textile machine process control devices and PLCs, which control the machine according to the desired recipe and process steps (Figure 3).

In the textile dyeing process, one of the important criteria that will ensure “right first time” is the correct temperature control of the machine. Currently, Proportional-Integral-Derivative (PID) controller parameters are tuned by technicians based on their personal experience during installation of the dyeing machine. This may lead to inconsistencies in process control and sustainability issues. It can also result in inefficient use of resources such as energy, steam, water, chemical, dye, and time.

The goal of this project is to tune PID parameters adaptively with the output of the artificial intelligence algorithm working on our process controllers and PLCs, which are IoT devices operating at the edge. The benefits and contents of the project can be described as follows:

- Resource-efficient deployment will be provided by AI algorithms.
- AI algorithms will be able to exchange data and information with each other.
- Each dyeing process is a batch process with unique definition. AI algorithms will be adapted to different processes.
- Noisy and uncertain data from a machine operating in an industrial environment will be studied.
- The installation of the machines will be easier, faster and guarantee trust.
- Results of these algorithms will be stored in the central database for data analysis on factory basis.
- A typical textile dyeing factory has 30 dyeing machines and control devices. Generally, all machines run simultaneously. The main tank liquid temperature is controlled by using PID, taking about 70% of the duration of the dyeing process.
- During the process, an average of 400 different data points is collected. These data points are various process values such as analogue input and output values, digital input and output values, alarms, operator interventions, running commands. In a typically slow dyeing process, it suffices to exchange data with PLC at 10 Hz.
- PID parameters will be set automatically during installation of the machine. After installation, the system is planned to continue learn and tune the PID parameter values when necessary.
- Daily production amount is around 30 tons in a 30-dyeing machine factory.

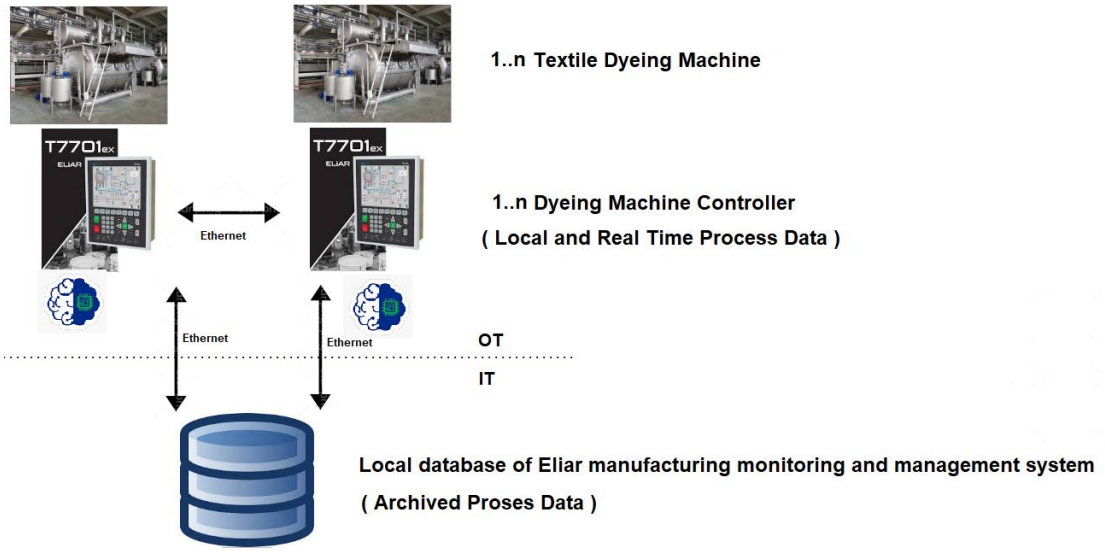

Figure 3. Eliar's manufacturing infrastructure.

2.2.2 Use-case Description

Actors: Textile dyeing process expert, Textile dyehouse machine & energy manager, Textile dyeing machine operator

Context / Setting: Textile dyehouse

Service:

- Distributed control of temperature in running dyeing process at dyehouse
- Precise reference temperature tracking depending on the process priority and availability of steam

- Increase in efficiency by optimizing steam distribution

Infrastructure/equipment/Agents: Textile dyeing machines, Eliar T7701ex operator panels & PLCs and embedded software running on them, Eliar central monitoring and control software & its database, and steam source.

2.2.3 Requirements for the MIRAI Framework

2.2.3.1 Business Requirements

ID: Eliar-BR-1
The solution shall be run as an add-on to the current Eliar products, particularly, be integrated to Eliar control panel model T7701ex (the edge node) and software Teleskop. Thus, control panel T7701ex and Teleskop must be already installed on site.

2.2.3.2 Functional Requirements

ID: Eliar-FR-1
The solution shall determine dyeing process priority.
Additional comments: Dyeing processes consist of different types of sub-processes like bleaching, dyeing, chemical dosing, washing. Process priority is an indicator of how crucial it is that a certain process is completed, in contrast to other processes (this difference may be due to client order, cost, etc.). Some of these sub-processes require more precise temperature tracking, less process delay depending also on type of fabric, type of dye chemicals. According to these characteristics, priority of dyeing process and its corresponding sub-processes must be determined in a sense like **HIGH**, **MEDIUM**, **LOW**.

ID: Eliar-FR-2
Process data such as the steam priority, steam efficiency, temperature values must be distributed among the machines to be used in tuning algorithms.

ID: Eliar-FR-3
The solution shall determine the heating performance of the machines.
Additional comments: Even though there is one main steam source in a dyehouse, heating performance of the machines can be differentiated between each other depending on factors like size, exchanger type, distance from the steam source, staleness, maintenance date, etc. By taking into consideration these factors, heating performance of each machine must be determined to enable the design and implementation of the aforementioned distributed control algorithms.

ID: Eliar-FR-4
The solution shall save long-term process data for temperature control.
Additional comments:

Temperature control takes about 70% of the duration of the overall dyeing process. Reference values of temperature, realized values of temperature, values of success metrics of temperature control must be saved at database of central monitoring system.

ID: Eliar-FR-5
The solution shall tune controller parameters offline and real-time.
Additional comments: Temperature control in dyeing processes is done by PID controllers which have several parameters to tune. These parameters must be tuned offline by using long term data and real-time by using process priority data that are distributed among corresponding machines.

ID: Eliar-FR-6
If anormal temperature values occur, the solution must ignore them. In addition, data cleaning must be done on historical data for removing low performance temperature control steps.

ID: Eliar-FR-7
The solution must warn the actors that it is impossible to control the machines if steam pressure is generally low and the solution cannot control the machines according to the given references and set point.

ID: Eliar-FR-8
The solution must report performance of control to actor textile dyehouse machine & energy manager.

2.2.3.3 Non-Functional Requirements (Operational, Design, etc.)

ID: Eliar-NFR-1
The solution shall ensure that process control continues if network connection between operator panels is broken.
Additional comments: T7701ex must, without any halt even in the case of certain failures, gracefully continue controlling dyeing machine without the need of auto-tuning add-on for the rest of the prescribed job. Add-on is not a must for controlling dyeing machine.

ID: Eliar-NFR-2
The solution shall strive to enforce fair network utilisation.
Additional comments: The auto-tuning add-on requires network communication for distributed control and data exchange. However, the network is not dedicated solely to this add-on and the transfer of the data needed to run distributed AI should not dominate the network traffic. Therefore, the solution's network bandwidth load must not block out Eliar Teleskop system and coupled machines.

ID: Eliar-NFR-3
The solution shall share data among machines every 60 seconds while performing distributed control.

ID: Eliar-NFR-4
Any actor can disable distributed temperature control for machine or a single dyeing process.

ID: Eliar-NFR-5
If power failure occurs during temperature control, after power is on, the solution (in the form of an add-on to existing infrastructure) must continue running by saving necessary data for continue.

ID: Eliar-NFR-6
The solution shall run 7/24.

2.2.3.4 Technological Requirements

ID: Eliar-TR-1
Developed software for the solution must run on Linux OS.
Additional comments (assumption): 1000 Mbps ethernet network must be installed for system operation.

ID: Eliar-TR-2
The solution must be run in T7701ex and some modules may need to run on Teleskop server.

2.3 Traffic Management (UC owner: Macq)

2.3.1 Context/Motivation

Macq offers a wide range of products ranging from sensor solutions for traffic monitoring, including advanced Automatic Number Plate Recognition (ANPR) cameras (able to operate on multiple lanes, distinguish between different types of vehicles, detect the number of passengers, estimate driving speed, etc.), to controllers for traffic light management at road intersections, to software packages for managing mobility-related data and extracting valuable insights to different types of decision makers (such as police and road authorities).

Within the MIRAI project, Macq proposes a use case in the domain of road safety for vulnerable road users (VRUs) in the vicinity of complex road intersections, linked to the following research areas:

- Leveraging the computational power of edge devices in order to extract valuable road safety analytics and react quickly when a potentially dangerous situation is detected. Several sensors and ANPR cameras are needed to properly equip complex road intersections. While the most advanced of Macq's ANPR cameras perform most of their computations locally, performing more advanced computations such as enabling to understand a given situation (possibly based on information from several other nearby data sources) and to detect potentially dangerous

situations when they occur would require relying on the cloud. Being able to perform more advanced machine learning and data mining computations at the edge would enable a better exploitation of the computational edge capabilities, a more balanced usage of computational resources and faster response times, as bandwidth-intensive image data would not need to be transferred to the cloud.

- Building robust approaches for efficiently dealing with bandwidth-intensive image data and for extracting insights even in the presence of noise and missing data. On the one hand, the intrinsic nature of Macq's ANPR camera data makes it challenging to merely transfer that data between other edge devices or to the cloud in order to perform the required computations. Being able to apply appropriate data compression techniques or to extract relevant features from the raw data would make it possible to envision more advanced applications like the ones in the considered use case without incurring into high data transmission costs and high latencies. On the other hand, Macq's ANPR cameras are deployed outdoors and are hence exposed to possibly harsh weather conditions. This result in incorrect readings, in communication problems, and, sometimes, in broken devices that need to be replaced. Being able to operate even in the presence of noise and missing data would enable to better ensure service continuity.

Determining how to scale computations based on the other devices present and operational in the immediate surroundings, their processing capabilities, their current load, the connection link to them, etc. While advanced machine learning and data mining approaches suitable for edge computing enable to leverage the computational power offered by edge devices, determining how to perform computations and split tasks between the different neighbouring edge devices available and the cloud infrastructure, remains a challenge to address before being able to fully exploit the available edge and cloud infrastructure.

2.3.2 Use-case Description

Actors: Drivers of Vehicles and Vulnerable Road Users (pedestrians and cyclists).

Context / Setting: Complex intersections, School and Railway intersections.

Service: To delivery an improved service of safety of Vulnerable Road Users at intersections, school and railway crossings.

Infrastructure/equipment: In the Macq AI ecosystem we need to distinguish three kind of processing systems. We have edge devices with sensors, edge devices with only calculation power and backend systems. In most cases the network infrastructure consists of wired Ethernet. The sensors need to be installed on the road infrastructure. This can be poles or gantries and determine the height and the angle. There are some degrees of freedom but they depend on the local situations that can be very diverse.

Agents Involved:

- Sensors (cameras and other)
    - Colour
    - B&W (near Infrared (IR))
    - Radar
    - Thermal
    - Time of Flight
- Actuators: IR Flash
- Processing elements
    - Cameras integrating the above sensors
    - AI boxes
    - M3 Backend systems
- Road Signage and Infrastructure

- Variable Message Signs
- Barriers
- Traffic lights
- Streetlights

2.3.3 Requirements for the MIRAI Framework

2.3.3.1 Business Requirements

ID: Macq-BR-1
The solution must improve the safety at: • Railway crossings • School streets • Complex intersections

ID: Macq-BR-2
The solution shall require minimal onsite configuration.
Additional comments: Although the sites are very versatile a complicated on-site configuration is not desirable because of the high involved personnel cost and difficulties to train subcontractors that install the cameras. This is a business requirement because the companies that install the cameras are the B2B customers. The end-client (city, police) writes a tender. Companies that do road infrastructure work subscribe to the tender and order the cameras at Macq or our competitors.

ID: Macq-BR-3
The solution shall run on multiple versions of the hardware platform.
The hardware platform is NVIDIA based. Cost and use of hardware are optimized for each use case. For instance, parking monitoring is less demanding than highways with multiple and high-speed vehicles. Supporting multiple software platforms comes at a high development and maintenance cost. The maintenance period exceeds 10 years.

ID: Macq-BR-4
The solution shall be perceived as privacy safe by design.
End clients need to comply to the GDPR and need to convince public opinion.

ID: Macq-BR-5
The solution shall increase availability when compared to a centralized approach.

ID: Macq-BR-6
The solution shall reduce development, deployment and operation costs for 3rd party software and embedded AI functions in edge devices.

2.3.3.2 Functional Requirements

ID: Macq-FR-1
The solution shall detect persons in image data including status and intentions (walking, crossing tracks while barrier down, …). In detail, when a VRU moves, the solution shall track him/her across sensor fields of view.
Additional Comments: This is, *strictu sensu*, not a Functional Requirement of the end-user use case but it is for the framework that is used to build it.

ID: Macq-FR-2
The solution shall enable the distributed system of edge devices to take decisions independently of the backend.
Additional Comments: The solution shall enable efficient edge processing without the need of sending images to the cloud. The edge devices can be cameras and or AI boxes.

ID: Macq-FR-3
When external conditions change, the solution shall adapt its working parameters to maintain the best working conditions.
Additional Comments: The solution shall adapt the configuration of the camera settings depending to external conditions such as weather, lighting, etc. Settings include: exposure time, gain, flash time and intensity. Not (yet) automated are the diaphragm.

2.3.3.3 Non-Functional Requirements (Operational, Design, etc.)

ID: Macq-NFR-1
The solution shall enable a modular solution supporting different solutions for various applications.
Additional Comments: Examples of applications are: • Trajectory control (focus on ANPR), • C-ITS application like Warning System for Pedestrians (WSP) and Blind Spot Detection (BSD) • Traffic light priority for cyclists Examples of modules that can be combined in a chain are: • Reading sensor data (Source) • Detection • Classification • Tracking • Regulation

- Image output (Sink)
- Data fusion
- Communication protocols

ID: Macq-NFR-2
The solution shall operate in real-time.
Real-time operation is needed to be able to issue a warning in case of a dangerous situation. In practice a delay of less than 100ms is required.

ID: Macq-NFR-3
The MIRAI system shall support explication and justification of the decisions taken during operation. Machine learning algorithms supporting explainable AI shall be supported. Decision and event logging are to be supported.

ID: Macq-NFR-4
The solution shall guarantee that data exchange between edge/IoT and cloud devices is protected; and that AI algorithms are executed in edge nodes in protected environment.

ID: Macq-NFR-5
The solution shall provide mechanisms to guarantee interoperability, efficient and easy integration of new edge devices with the core large-scale computing infrastructure (i.e., the cloud).

ID: Macq-NFR-6
The solution shall reduce bandwidth requirements.

ID: Macq-NFR-7
The solution shall minimize the sense-compute-act latency.

ID: Macq-NFR-8
The solution shall achieve high scalability thanks to the amount of pooled resources and distributed and composable ML models (bounded by the application's architecture).

ID: Macq-NFR-9
The solution shall protect privacy in images of VRUs and ensure that policies for data privacy (and, when possible, control over privacy) are applied. Images shall not leave the sensor system (edge node) for processing, and when images are processed, the System shall delete them. The solution will enforce privacy aspects across multiple cameras, in the case of deep learning.
Additional Comments:

Images are allowed to leave the edge devices when they are part of the application. For instance, an ANPR system doing trajectory control needs the images as proof in case of an infraction.

2.3.3.4 Technological Requirements

ID: Macq-TR-1
The solution shall combine information from different visual sources: • Black & White + near IR • Colour • Thermal • Time of Flight The fusion can be done on different levels: sensor data, extracted features and object detections.

ID: Macq-TR-2
The solution shall offer the possibility of combining information extracted from images with other non-visual technologies: • Radar • Sound Each sensor system can generate an object detection list. The detection lists can then be fused together.

ID: Macq-TR-3
Development in C++ and Python.

ID: Macq-TR-4
The solution shall enable the possibility to combine modules that use AI with modules that implement traditional technologies.

2.4 Secure Internet Provisioning (UC owner: NOS)

2.4.1 Context/Motivation

With the massification, globalization, digitization and the wide use of the Internet, a drastic increase in cyberattacks has been witnessed mainly using viruses and malware that exploit software and hardware weaknesses. In addition, the rise of Internet-connected equipment among the leading smart devices / IoT devices contributes to an exponential increase in network connections and, as a result, the number of cyber testing target views.

Networking equipment that is a part of the Operator Network, such as modems and routers, is a major target of major cyberattacks and is hence exposed to many threats, such as the misappropriation of user accounts from malicious servers and access to personal information and data, threatening users' privacy and security.

Currently Home Gateways (HGWs) have static firewall rules that should detect and stop some predefined attack scenarios. To update those rules, leaving the Home Gateway updated, is necessary to do a firmware install. These installations require that different Home Gateway (HGW) stakeholders (hardware manufacturer, system integrator, Operator) be synchronized to release a new version, which sometimes can take up to months. Real-time attacks cannot wait for such chain of dependence, and they must be stopped as soon as possible guaranteeing available resources to customers. Moreover, current attacks are more complex and intelligent, which makes using only this static type of defence obsolete.

Modern home networks have IoT devices, which may switch on/off some other appliances, may interoperate with other IoT devices to complement their actions, or do some predefined sets of actions without human intervention. There has been a huge increase on the number of devices per household, such as power outlets, lamps, smart fridges, other wireless gateways (Zigbee, ZWave), thermostats, smart assistants, etc., which all have access to the Internet for interaction and configuration. These IoT devices also run software, and some devices maybe updated if the manufacturer releases one. The ubiquity of these devices and their low cost (some) leads to some of the devices not being update leading to a security risk, as they can also be tampered with or attacked, as they are connected to the Home Gateway and from there to the Internet. The attacks to these devices, may be disguised as legit actions, which in fact may be malware that may infect other devices on the customer network depleting him/her from using the resources available. Moreover, as some IoT devices have specific purposes and communication patterns, going outside of those purposes or communications on the network may indicate a security an unhealthy issue.

It is necessary to use dynamic mechanisms based on field information to understand if it is occurring an attack and act on it, guaranteeing that customers are safe using their devices on their network. In a single HGW, NOS wants to provide a security solution allowing the detection of potential attacks and to have the possibility of assuring defence against these threats by processing and identifying them in order to guarantee the customer network protection.

The proposed system would be integrated directly in the HGWs, supported by intelligence in the cloud, and supplemented by mobile applications that would ensure services such as household member profiling in order to adapt browsing protection and parental control as well as privacy management.

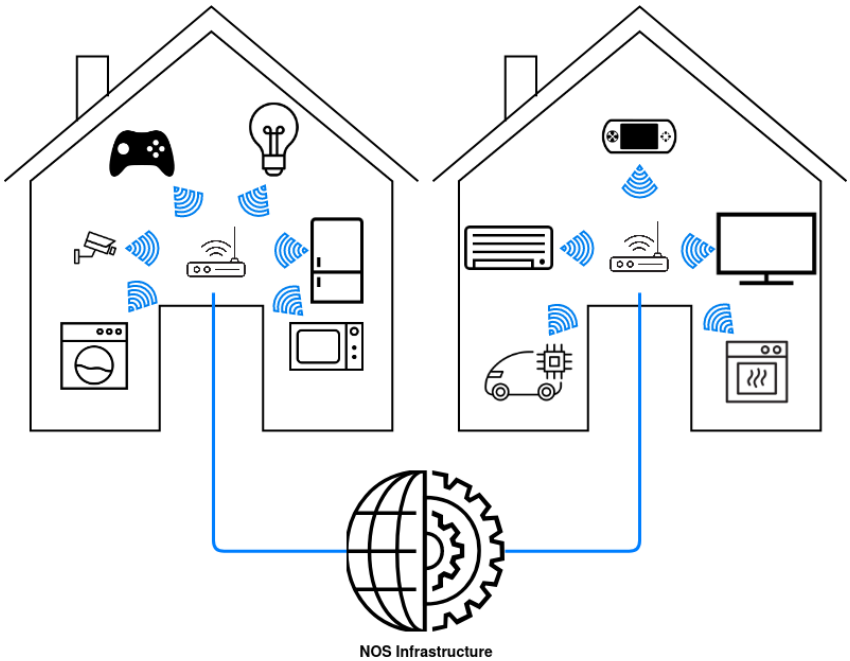

Figure 4. Customers' premises with a variety of IoT devices connect to the Internet through NOS infrastructure

2.4.2 Use-case Description

Actors: Customer; Attacker, Service Provider.

Setting: Customer home network, enabled by Service Provide Equipment & Infrastructure (Customer Network).

Infrastructure/Equipment/Agents (refer to Figure 5):

- Customer Home Gateway (HGW): equipment deployed by Telco Operator (NOS) that: (a) enables Customer Network; (b) connects Customer Network to Operator Infrastructure.
- Customer Devices: IoT Devices connected to the Customer Network (c).
- Malicious Agent (Malware): an agent (typically software) that can grant control of a Customer Device to an Attacker (d);
- Operator Infrastructure: Service and Networking Infrastructure that connects Customer Network to Internet (e).

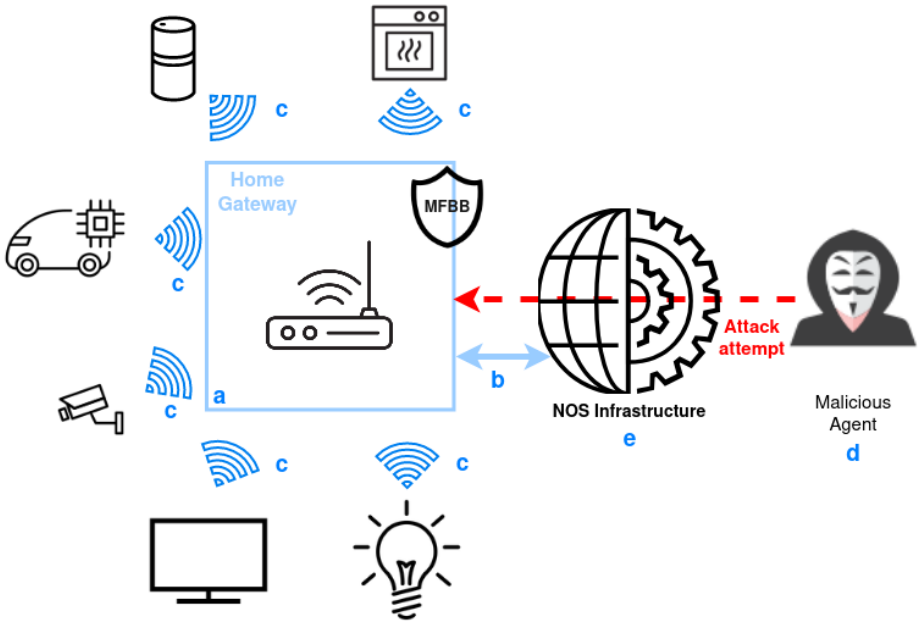

Figure 5. Summary figure of the Secure Internet Provision Use-Case.

Goal: The Service Provider wants to provide a Cyber Attack Detection/Prevention/Mitigation System (System), deployed in the Customer' Home Gateway.

Services to be provided:

1. Main service: Detect and Mitigate involvement of Customer Devices in attack attempts (e.g., DoS) to other parties (to other Devices in the Customer Network; to infrastructure of the Service Provider; to external parties).
2. Other services:
   2.1. Prevent (by Detecting pre-emptively) intrusion and installation of 'malware' on the Customer Device by Attacker (through attack agent).
   2.2. Detect and Mitigate DoS attacks to the Customer Devices.
   2.3. Detect and Mitigate involvement of Costumer Devices in intrusion attempts to other parties (to other Devices in the Customer Network; to infrastructure of the Service Provider; to external parties).

2.4.2.1 Business Requirements

ID: NOS-BR-1

The solution shall increase the perception of security of IoT devices by the Customer.

ID: NOS-BR-2
The solution shall increase the overall security of the NOS network, preventing economical loses.

ID: NOS-BR-3
The System shall have minimal impact on Customer Internet experience.

ID: NOS-BR-4
The solution shall provide privacy and anonymity of the users, and security of processes and data transfers.
Additional comments: • The communication between the Home Gateway and cloud platforms should be encrypted. • Home Gateway and cloud platforms must exchange secure verifiable identifications. • No personal/sensitive data can be sent to cloud platforms.

2.4.2.2 Functional Requirements

ID: NOS-FR-1
The solution shall monitor traffic patterns 24/7 to find indicators of DDoS security threats and attacks.

ID: NOS-FR-2
The solution shall learn applications' traffic patterns concerning IoT and other devices and use the protection profile that best suits the identified patterns ("smart and customized protection").

ID: NOS-FR-3
The solution shall provide a mitigation mechanism against large scale attacks, such as TCP SYN, UDP and ICMP flood; Amplifier attacks and fragmented attacks. The mitigation mechanism should prevent the access of the infected device to the home network and to the outside (Internet). To protect the core network of NOS alongside with the home network of the client, the mitigation mechanism should quarantine the infected devices and, when possible, clean the device.

ID: NOS-FR-4
The solution shall provide a mitigation mechanism against devices vulnerabilities.

ID: NOS-FR-5

If an attack is ongoing, the solution shall provide a brief report in real time or near real time during the attack, and a detailed one after the attack is over. The solution shall also provide a global report with information about all installed Home Gateways to have knowledge about how many Home Gateways were exposed to attacks, and which was the attack profile/type.

ID: NOS-FR-6
The solution shall compute and provide metrics related to vulnerabilities and attacks that have been identified and thwarted (or not).
Additional comments: Examples of metrics: • Characteristics per each type of attack (Flood attacks, Amplification attacks, Fragmentation attacks) on bandwidth usage, packets per second (pps), packet flags. • Number of devices that where infected (identifying the source Ips that were infected). • Values of CPU and Memory usage during the attack. • Time-to-Response. • Time-to-Detect. • Packets per second sent/received during the attack. • Communication patterns in IoT devices.

ID: NOS-FR-7
The solution shall provide the possibility for the Service Provider and/or Customer to be informed whenever a vulnerability and/or attack is detected. Circumstances: • Every time a possible attack is underway the gateway must send a notification to the system provider on a specific URL. • The Service provider from the NOC (Network Operations Center) will be able to request a report from the gateway. • Customers, from their router internal page or Internet Portal will be able to request a report from the gateway.

ID: NOS-FR-8
The solution at the Home Gateway (edge node) shall be able to continue operation even when connection to cloud is unavailable.

2.4.2.3 Non-Functional Requirements (Operational, Design, etc.)

ID: NOS-NFR-1
The solution shall be integrated directly and operate in the Home Gateways (edge nodes).
Additional comments: • An agent must run on the gateway to monitor the traffic. • An agent must run on the gateway to act upon information an attack is undergoing. • An agent must run on the gateway to report to stakeholders.

ID: NOS-NFR-2
The solution may be complemented by components deployed outside the Home Gateway, namely mechanisms to support the operation of the System deployed in edge (than not the Home Gateway) and/or cloud platforms.

2.4.2.4 Technical Requirements

ID: NOS-TR-1
The solution shall use the operating system RDK (which uses the Linux kernel), and work with packets using Ipv4 and Ipv6 protocol.

ID: NOS-TR-2
The system should be able to detect attacks in OSI layer 3, 4 and 7.

ID: NOS-TR-3
The system should be able to run in multi-cloud platform.
Additional Comments: Ideally the system should be agnostic to the cloud provider. However, the most critical ones are Google Cloud (GCP) and Amazon Web Services (AWS) platforms.

2.5 Water management (UC owner: Shayp)

2.5.1 Context/Motivation

Shayp has developed a water consumption monitoring technology made of a hardware device (Figure 6) measuring water flow in pipes[2] with 3 key features in mind:

- non-invasiveness: hardware does not require any plumbing intervention in order to read water consumption from the water supply system. This allows the solution to be highly compatible with many types of settings and easy to install without any professional training.
- not dependent on the connectivity of the customers: communication protocol used is NB-IoT with Orange as provider.
- no power supply required: the device is battery-powered in order to facilitate operations. To stay consistent with our mission of simplifying operations, the battery life of the device is optimized to match the lifetime of a water meter (16 years) in order to reduce maintenance costs.

[2] https://www.youtube.com/watch?v=hZR7N43q1Vc

Figure 6. Shayp's water-measuring module.

As of today, the water consumption data is hosted on the cloud where it is processed and stored. The backbone of the cloud-based software application is the leak detection analysis. As of today, we have refined statistical and learning models to correctly determine leaks even within a building with high accuracy. However, we are looking to shift towards a trained model in order to better adapt to different types of buildings, learn about the type of leaks and even provide insightful water consumption information.

Current limitations:

- Low power consumption: to guarantee long battery life, we are limited in the payload size that we can collect. Hence data analytics algorithms are limited by the rate of data that we can send.
- Time of detection: with that data, we are capable of detecting leaks within 3 hours, which is good for many cases but not sufficient to prevent all types of damages caused by leaks.
- Accuracy of the hardware in place: even if we could use the highest data granularity, we're limited by the precision of the water meters that our device connects to. There is a wide variety of types of meters and our strength is to be compatible with many of them. The backside of that is that we have a big heterogeneity of data quality depending on the water meters in place.

As of today, Shayp mainly relies on its own hardware component, but the highest value lies in the data knowledge. This is where we want to develop our expertise even further. MIRAI focuses on this by pushing forward a new standard of edge technology and improving the quality of insights coming from the data.

2.5.2 Use-case Description

Actors: municipalities (City of Brussels), P&C insurance companies (Aviva Insurance).

Context / Setting: water monitoring & leak detection connected to water meters in buildings.

Service: monitoring water consumption, analyse data, detect leaks.

Infrastructure/equipment: Shayp device connected to the water meter.

- Current battery life – 10y
- Communication – NB-IoT
- Data sent – 120 data points/h + metadata
- Leakage detection – 3-24h big buildings, 1-3h households

Agents Involved:

Concretely, in the case of Shayp's customers, we're looking to improve our technology to address a few specific challenges:

1) Scenario 1 – As mentioned above, the network capabilities of the edge device are the component that is draining the most battery power. Hence, the obvious solution that could immediately save power on the edge and provide longer lifespan would be to send less messages to the cloud. In order to do that, we would like to implement an intelligent system that will only send messages when actual water consumption is detected, which could already prevent 30% of messages to be sent out.
2) Scenario 2 – Anomalous water usage pattern recognition requires, as of today, a minimum of 3 consecutive messages from the edge device before having enough data to confirm that there is an abnormal consumption. This is too slow to prevent damage from happening in case of important leaks. By adding an intelligent messaging system that could already tag anomalies directly at the edge, we could trigger alerts much faster.
3) Scenario 3 – Installing edge devices all over buildings creates a technical debt by essence if the firmware or the hardware versions are evolving over time. By putting bi-directional communication in place, the models used by the edge devices can be updated remotely and their capabilities improved over time.
4) Scenario 4 – In order to calibrate the edge device or in order to check if the network's water consumption is normal, there is a "calibration mode" that sends 1 message every minute for 15 minutes. This could be controlled remotely thanks to a bidirectional communication with the edge device.

2.5.3 Requirements for the MIRAI Framework

2.5.3.1 Business Requirements

ID: Shayp-BR-1
The battery lifetime of the hardware device (edge node) shall match as well as possible the lifetime of standard water meters.
Additional Comments: • Current specification of the battery: 20000mAh • Cost of the battery: 7,5 EUR • Current consumption of sending a message: 19.4mA during 3 sec • Current number of messages sent per day: 25 • Estimated lifetime of the battery: 10 years; goal: 16 years

ID: Shayp-BR-2
The solution shall provide faster anomaly detection thanks to a conjunction of work between edge devices and cloud. Edge devices should already flag anomalies as early as possible and cloud will then use that flag to confirm if the situation has to be flagged as an actual anomaly.
Additional Comments: Customers want to avoid costly leakages and water damages, so the earlier they receive an alert about a leak, the better. • Current situation: between 3 hours in best cases for household and 24 hours for institutional buildings to detect a leak • Goal: anomaly detection in less than 1 hour

2.5.3.2 Functional Requirements

ID: Shayp-FR-1
The solution shall detect leaks/anomalous consumption within the hour supported by anomaly detection on the edge in combination with the cloud.
Additional comments: • Flag anomaly on the edge & send to cloud • Increase amount of data sent to the cloud (Scenario 1) • Verify false positives on the cloud

ID: Shayp-FR-2
The solution (at the edge node) shall send data only when required based on the type of building and on the current water consumption.
Additional comments: When no water consumption, avoid sending data (given subscription on telecom, it is cheaper if sending less messages). • Update hardware for flexible sending • Update message structuring • Update data ingestion module

2.5.3.3 Non-Functional Requirements (Operational, Design, etc.)

ID: Shayp-NFR-1
The battery life of the edge node shall be increased from 10 to 16 years (as long as the water meter). (Applicable to Scenario 1.)

ID: Shayp-NFR-2
A technician installing the device shall be able to enable calibration mode resulting in sending messages every minute for 15min. (Applicable to Scenario 4.)

ID: Shayp-NFR-3
The solution should secure data on device and in transit to prevent disclosing (privacy-sensitive) water consumption data.

2.5.3.4 Technological Requirements

ID: Shayp-TR-1
The cloud shall communicate (bi-directional communication) with the edge device in order to configure, update (firmware, training set of type of building) or send action (shut valve). (Applicable to Scenario 3 & Scenario 4.)

ID: Shayp-TR-2
The solution at the edge node should be able to store & process enough local data in view of pattern recognition and initial detection of anomalous consumption.

ID: Shayp-TR-3
The solution at the edge node shall be able to compress data on device (within 512 bytes) without losing necessary information for computing useful insights on the cloud.

3 Global Framework Requirements List

This chapter lists the Global MIRAI Framework Requirements drawn from the description and requirements of the UCs identified by the partners, listed in the previous section. As described in Section 1.2, the UC requirements were first drawn independently by the associated partners, and then revised in search of commonalities, resulting in an initial version of the global requirements.

We now refer to the "MIRAI Framework" instead of the "solutions" of the previous chapter. The "solutions" can be thought of as particular instantiations of the MIRAI Framework tailored to each use-case. In this section, we wish to define global and transversal requirements.

Each Global Requirement is specified with the following fields:

- **ID and Name:** identifier of global requirement
- **Confidential:** whether requirement should be kept confidential.
- **Relevance to MIRAI vision:** whether the requirement is critical towards the objectives outlined for the MIRAI framework.
- **Work package:** work package in which the requirement will be designed/ implemented.
- **Description:** description of the global requirement.
- **Annotation:** optional field to provide additional comments.
- **UC Requirements:** UC requirements that motivate or substantiate the global requirement.
- **Relevance to UC:** an assessment of the relevance of the global requirement to all UCs.

Some Global Requirements identified in a first iteration and removed at a later occasion (due to lack of relevance) are shown in Appendix B.

3.1 Business Requirements

ID: MIRAI-BR-1	**Name: Optimize Service Efficiency through Learning/Inference at the Edge**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP2
Description	The MIRAI Framework shall use artificial intelligence/machine learning at edge nodes, deployed close to the target processes and/or equipment, to learn the target processes and optimize the efficiency of the service being offered.	
UC Requirements	- 3E-FR-2, 3E-FR-4 - Eliar-FR-1, Eliar-FR-2 - Macq-FR-3 - NOS-FR-2 - Shayp-FR-1	
Relevance to UCs	Relevant to all UCs.	

ID: MIRAI-BR-2	**Name: Availability**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP4
Description	The MIRAI Framework shall operate continuously 24/7.	
UC Requirements	- 3E-BR-5, 3E-FR-1, 3E-FR-2, 3E-FR-5 - Eliar-NFR-6 - Macq-BR-5 - NOS-FR-1 - Shayp-FR-1	

Relevance to UCs	Relevant to all UCs.

ID: MIRAI-BR-3	**Name: Minimize Communication Overhead**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP2, WP3
Description	The MIRAI Framework shall minimize the data exchanges between the framework components instantiated in each UC.	
UC Requirements	- 3E-BR-6, 3E-TR-3 - Eliar-NFR-2 - Macq-NFR-6 - Shayp-FR-2, Shayp-TR-3	
Relevance to UCs	Relevant to most UCs.	

3.2 Functional Requirements

ID: MIRAI-FR-1	**Name: Adapt Operation to Different Contexts**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP2
Description	The MIRAI Framework shall adapt the service provision to the specific setting and/or contexts in which the service is to be provided and in which edge nodes have been deployed.	
Annotations	Examples include: - NOS: adapt security solution to specific customer premises. - Eliar: adapt to specific machine types. - Macq: improve video images based on weather conditions for example. - Shayp: adapt anomaly detection to the specific type of building.	
UC Requirements	- 3E-FR-4, 3E-FR-5 - Eliar-FR-3, Eliar-FR-4 - Macq-FR-3 - NOS-FR-2 - Shayp-BR-2	
Relevance to UCs	Relevant to all UCs.	

ID: MIRAI-FR-2	**Name: Learning with Noisy and Missing Data**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP2
Description	The MIRAI Framework shall be able to carry out the learning process even in presence of noisy or missing data. This may include: performing data pre-processing tasks prior to the learning stage (e.g., removal of repeated/unnecessary samples; handling of missing data; conversion of data formats); and/or use if AI/ML algorithms/strategies that can cope with noisy, missing or unbalanced datasets.	
Annotations	Missing or noisy data, in the context of such different data types, may have different meanings. We focus on noisy, or data that is tainted by external factors. In the case of Macq's UC, objects unknown to the ML detector may be thought of as "noise".	
UC Requirements	- 3E-FR-3 - Eliar-FR-6 - Macq-BR-1 (implicit)	
Relevance to UCs	Relevant to 3 UCs.	

ID: MIRAI-FR-3	Name: Monitoring and Control of Edge Nodes by Operator	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	Medium	WP4
Description	The MIRAI Framework shall provide monitoring and control of the edge devices to the system operator (in the cloud).	
Annotation	Many UCs do not identify explicitly the need to monitor and control the edge device, but it is understood that this is necessary to support the operation of the System.	
UC Requirements	- 3E-BR-6 (implicit) - Eliar-FR-8 (implicit) - NOS-FR-5, NOS-FR-6 (implicit) - Shayp-TR-1	
Relevance to UCs	Relevant to most UCs.	

ID: MIRAI-FR-4	Name: Execute Timely Action or Feedback to Relevant Parties	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP2, WP3
Description	The MIRAI Framework shall provide regular actuation and/or feedback, or an actuation and/or feedback in response to an anomalous event, to the relevant agents (local processes/equipment, cloud-based system operator, etc.) within useful/bounded time. The deadline for an action or feedback is defined per UC.	
UC Requirements	- 3E-FR-5, 3E-BR-1, 3E-BR-2, 3E-BR-3 - Eliar-FR-5, Eliar-FR-7, Eliar-NFR-3 - Macq-NFR-2, Macq-NFR-7 - NOS-FR-3, NOS-FR-4, NOS-FR-7 - Shayp-BR-2, Shayp-FR-1	
Relevance to UCs	Relevant to all UCs.	

ID: MIRAI-FR-5	Name: Provide Data/Reports of Monitored Processes to System Operator	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	Medium	WP2, WP3
Description	The MIRAI Framework shall provide reports of the monitored processes or events to the system operator. These may refer, e.g., to statistics of operational metrics over a parameterizable period of time.	
UC Requirements	- 3E-NFR-2 - Eliar-FR-4, Eliar-FR-8, Eliar-FR-7 (event driven) - NOS-FR-5, NOS-FR-6, NOS-FR-7 (event driven) - Shayp-BR-2	
Relevance to UCs	Relevant to all UCs.	

3.3 Non-Functional Requirements

ID: MIRAI-NFR-1	Name: Cloud/Edge Complementarity for Service Provision	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP2
Description	The MIRAI Framework shall support the coordinated operation of system agents and resources at the edge nodes (e.g., local learning processes) with those at the cloud (e.g., database, other services, and/or complementary processing capabilities for learning/inference), through bi-directional communication.	

UC Requirements	- 3E-BR-6, 3E-TR-2 - Eliar-FR-4 (implicit) - NOS-NFR-2 - Shayp-FR-1, Shayp-TR-1
Relevance to UCs	Relevant to most UCs.

ID: MIRAI-NFR-2	**Name: Processing and Storage Capabilities at Edge Nodes**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP3
Description	Edge nodes should be able to carry out the necessary actions and store data locally.	
UC Requirements	Relating to all UCs (explicit mentioned in Shayp-TR2)	
Relevance to UCs	Relevant to all UCs.	

ID: MIRAI-NFR-3	**Name: Provide User Privacy and Data/Process Security**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP3
Description	The MIRAI Framework shall provide the ability to protect the privacy of users and/or other participating agents, through appropriate privacy-respecting mechanisms, and offer security of datasets and target processes when required.	
Annotations	Macq's UC focuses on monitoring of road scenes. Captured pedestrians, cyclists, drivers or passengers may not be aware that they are being monitored.	
Rationale	- 3E-NFR-1, 3E-NFR-2 - Macq-NFR-9, Macq-NFR-4 - NOS-BR-4 - Shayp-NFR-3	
Relevance to UCs	Relevant to most UCs.	

ID: MIRAI-NFR-4	**Name: Persistence of Operation of Edge Nodes**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	Medium	WP4
Description	The MIRAI Framework shall support the independent operation of the edge devices and ensure the provision of the service, even with limited capabilities, in the event of loss of communication with the remaining components.	
Rationale	- 3E-FR-6 - Eliar-NFR-1 - Macq-FR-2 - NOS-FR-8 - Shayp-TR-2	
Relevance to UCs	Relevant to all UCs.	

ID: MIRAI-NFR-5	**Name: Horizontal Scaling**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	High	WP3
Description	The MIRAI Framework shall offer mechanisms to complement and coordinate the learning and inference over multiple edge nodes. This enables supressing or mitigating needs regarding processing power, communication and/or data that a single edge node may encounter.	

Rationale	- Eliar-FR-2 - Macq-FR-2, Macq-NFR-8
Relevance to UCs	Matches vision of MIRAI.

ID: MIRAI-NFR-6	**Name: Setup Prior to Operation**	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	Medium	WP4
Description	The MIRAI Framework must consider the calibration of the sensors.	
Rationale	- Eliar-FR-1 - Macq-BR-2 - Shayp-NFR-2	
Relevance to UCs	Relevant to many UCs.	

3.4 Summary Table of UC-to-Global Req. Mapping

The following table provides an overview of the mapping between UC requirements and the Global requirements.

Global Requirements		UC requirements (UCs identified by UC owners)																	
Business		**3E**				**Eliar**			**Macq**		**NOS**			**Shayp**	
MIRAI-BR-1	Optimize Service Efficiency through Learning/Inference at the Edge	**3E-FR-2**	**3E-FR-4**			**Eliar-FR-1**	**Eliar-FR-2**		**Macq-FR-3**		**NOS-FR-2**			**Shayp-FR-1**	
MIRAI-BR-2	Availability	**3E-BR-5**	**3E-FR-1**	**3E-FR-2**	**3E-FR-5**	**Eliar-NFR-6**			**Macq-BR-5**		**NOS-FR-1**			**Shayp-FR-1**	
MIRAI-BR-3	Minimize Communication Overhead	**3E-BR-6**	**3E-TR-3**			**Eliar-NFR-2**			**Macq-NFR-6**					**Shayp-FR-2**	**Shayp-TR-3**
Functional															
MIRAI-FR-1	Adapt Operation to Different Contexts	**3E-FR-4**	**3E-FR-5**			**Eliar-FR-3**	**Eliar-FR-4**		**Macq-FR-3**		**NOS-FR-2**			**Shayp-BR-2**	
MIRAI-FR-2	Learning with Noisy and Missing Data	**3E-FR-3**				**Eliar-FR-6**			**Macq-BR-1**						
MIRAI-FR-3	Monitoring and Control of Edge Nodes by Operator	**3E-BR-6**				**Eliar-FR-8**					**NOS-FR-5**	**NOS-FR-6**		**Shayp-TR-1**	
MIRAI-FR-4	Provide Timely Feedback to Relevant Parties	**3E-FR-5**	**3E-BR-1**	**3E-BR-2**	**3E-BR-3**	**Eliar-FR-5**	**Eliar-FR-7**	**Eliar-NFR-3**	**Macq-NFR-2**	**Macq-NFR-7**	**NOS-FR-3**	**NOS-FR-4**	**NOS-FR-7**	**Shayp-BR-2**	**Shayp-FR-1**
MIRAI-FR-5	Provide Data/Reports of Monitored Processes to System Operator	**3E-NFR-2**				**Eliar-FR-4**	**Eliar-FR-8**	**Eliar-FR-7**			**NOS-FR-5**	**NOS-FR-6**	**NOS-FR-7**	**Shayp-BR-2**	
Non-Functional															
MIRAI-NFR-1	Cloud/Edge Complementarity for Service Provision	**3E-BR-6**	**3E-TR-2**			**Eliar-FR-4**					**NOS-NFR-2**			**Shayp-FR-1**	**Shayp-TR-1**
MIRAI-NFR-2	Processing and Storage Capabilities at Edge Nodes													**Shayp-TR-2**	
MIRAI-NFR-3	Provide User Privacy and Data/Process Security	**3E-NFR-1**	**3E-NFR-2**						**Macq-NFR-9**	**Macq-NFR-4**	**NOS-BR-4**			**Shayp-NFR-3**	
MIRAI-NFR-4	Persistence of Operation of Edge Nodes	**3E-FR-6**				**Eliar-NFR-1**			**Macq-FR-2**		**NOS-FR-8**			**Shayp-TR-2**	
MIRAI-NFR-5	Horizontal Scaling					**Eliar-FR-2**			**Macq-FR-2**	**Macq-NFR-8**					
MIRAI-NFR-6	Setup Prior to Operation					**Eliar-FR-1**			**Macq-BR-2**					**Shayp-NFR-2**	

4 Final Remarks

This document lists the framework level requirements (or global requirements) for the MIRAI Framework, produced under task T1.1 of project ITEA3 MIRAI. The output of this task will feed subsequent tasks of WP2 and WP3, whose purpose is to design and implement the MIRAI framework.

A revised version of this document is scheduled for M18, in which the presented requirement list will be reviewed and updated with inputs from the on-going work on the development of Machine Learning models (in WP2) and the reference architecture for the MIRAI Framework (in WP3).

Appendix A

Template prepared by the task leader and provided for partners to be filled with: (i) context, motivation, and description of use-cases (UC); and (ii) title and definition of requirements of the UCs.

ITEA 3 MIRAI project

Use-case Definition and Requirements Elicitation
[UC Name – Replace by yours]

Use-case Description

Use Case Description
Actors: [Example: Customer, Waiter]
Context / Setting: [Example: Restaurant]
Service: [Example: provide Meal]
Infrastructure/equipment: [If any]
Agents Involved: [If any]
[Add as needed]

Requirements Elicitation

Guideline 1:

Provide **The who, the what and the why** (using the elements identified in the UC description).

Example 1: Actor X shall request Service Y → Customer shall request Meal

Guideline 2:

The Easy Approach to Requirements Syntax (EARS) is a methodology for constraining the syntactic description of requirements. We suggest you try to follow it.

Examples drawn from the link above:

Generic EARS syntax:

- While <optional pre-condition>, when <optional trigger>, the <system name> shall <system response>
- Ubiquitous requirements: The <system name> shall <system response>
- Event driven requirements: When <trigger>, the <system name> shall <system response>

Etc.

Functional Requirements

Req. #1

Non-Functional Requirements (Operational, Design, etc…)

Req. #1

Technological Requirements

Req. #1

Business Requirements

Req. #1

Appendix B

Requirements initially identified as Global but ultimately discarded due to lack of relevance to a large number of UCs or to the MIRAI vision.

ID: MIRAI-BR-2	Name: Ensure Optimal Usage of other (Natural) Resources	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	Medium	WP4
Description	The framework shall aim to optimize the usage of natural resources.	
UC Requirements	- 3E-BR-1 - Shayp-BR-2	
Relevance to UCs	Relevant to 2 UCs.	

Reason for discarding: relevant to only two UCs.

ID: MIRAI-BR-5	Name: Maximize Lifetime of Edge Nodes	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	Low	WP3
Description	The framework shall maximize the lifetime of the edge nodes that are battery-powered.	
Rationale	- Shayp-BR-1, Shayp-FR-1	
Relevance to UCs	Relevant to Shayp.	

Reason for discarding: relevant to only one UC.

ID: MIRAI-FR-6	Name: Warn System Operator of Relevant Events	
Confidential	**Relevance to MIRAI vision**	**Work package**
No	Medium	WP3
Description	The MIRAI Framework shall produce warnings to the system operator when events of interest or anomalous events occur.	
Annotations	This requirement is distinguished from MIRAI-FR-4 in the sense that the warning to the operator, in this requirement, is not in the « critical path », i.e., it is not the main real-time actuation and/or feedback to be carried out in response to the identified event (comparing against, e.g., Shayp or Macq UCs).	
UC Requirements	- Eliar-FR-7 (for informative purposes) - NOS-FR-7 (for System Operator/Service Provider only)	
Relevance to UCs	Relevant to 2 UCs.	

Reason for discarding: relevant to only two UCs. While relevant, it is somewhat tangential to main vision of MIRAI (or is included in other Requirements, e.g. MIRAI-FR-4 and FR-5). This requirement was incorporated in MIRAI-FR-4 and FR-5.

Appendix C

Table listing: (i) outcomes of the first task meeting to produce an initial version of the global requirements list; and (ii) the mapping of each of the original UC requirements into one or more global requirements (after initial consolidation).

Yellow cells indicate requirements added at the time of the task meeting or later.

Note that some associations may be deprecated.

Type	UC Requirement	UC Req. ID	First proposal of global requirements (2021/03/30 meeting)		Consolidation into Global Requirements	
			Global requirement	Notes	Mapped into Global Requirement	Notes
	3E					
Business	When wholesale market prices are negative, SynaptiQ shall turn off the plants to avoid losing revenue.	3E-BR-1			Ensure Optimal Usage of other (Natural) Resources	
Business	When energy production varies throughout the day due to changing meteorological conditions, SynaptiQ shall vary flexible loads in order to maximize self-consumption of generated energy.	3E-BR-2				
Business	When short-term electricity prices fluctuate throughout the day, SynaptiQ shall charge and discharge a battery to maximize revenue.	3E-BR-3			Provide Timely Feedback to Relevant Parties	
Business	When balancing prices are high, SynaptiQ shall push settings to the local PLC to reserve a certain amount of power for balancing services, which SynaptiQ will provide as a pre-aggregator.	3E-BR-4			Real-time Monitoring and Control of Edge Nodes by Operator	
Business	SynaptiQ shall continuously calculate the optimum between Reqs. #1-4, optimizing the control of assets both on a local level (individual plant) and on a portfolio level (group of plants owned by the same entity).	3E-BR-5			Availability	
Business	The proposed cloud-edge solution will compete with pure local solutions. As a consequence, the bi-directional real-time communication to the cloud should be as lean and cost-effective as possible.	3E-BR-6	Bi-directional communication		Cloud/Edge Complementarity towards Service	
Functional	The cloud forecast shall continuously forecast production, load and prices based on market input and the production and consumption data from the plants.	3E-FR-1			Availability	
Functional	The cloud optimizer shall continuously calculate the optimal set points to the flexible assets in order to maximize revenue based on forecast production, load and prices. These set points will be compiled into a schedule for the next time period.	3E-FR-2	Optimization		Optimize Service Efficiency through Learning	
Functional	The data cleanup module shall clean up the real-time data coming from the assets to correct for missing or incorrect data.	3E-FR-3	Dataset pre-processing: Data cleanup; Handling missing data (e.g., interpolation) data homogenization		Learning with Noisy and Missing Data	
Functional	The local forecast shall predict the local production and load based on the local real-time data.	3E-FR-4			Optimize Service Efficiency through Learning	
Functional	The local optimization shall continuously adjust the schedule of the cloud optimizer as a function of the real-time data. E.g., it will react to instantaneous variations in production to avoid injecting power into the grid when possible.	3E-FR-5	Coordination between edge and cloud components		Learning Capabilities at Edge Nodes; Provide Timely Feedback to Relevant Parties	
Functional	When the edge node loses access to the cloud, the local optimizer shall execute the locally available schedule for as long as there is a global optimization and then revert to the default fall back.	3E-FR-6	Persistent operation of one or more components towards providing the service		Persistence of Operation of Edge Nodes	

Non-functional	A portfolio of distributed energy production assets, controllable from the cloud, is a high commercial and strategic risk. The risk of intrusion should be minimized.	3E-NFR-1	Security of processes		Provide User Privacy and Data/Process Security	
Non-functional	If an attack is ongoing, the System shall provide a detailed report in real time or near real time during the attack, and complete resume after it.	3E-NFR-2			Provide Data/Reports of Monitored Processes to System Operator	
Non-functional	The compression module will compress the real-time data stream at the edge node with minimum information loss in order to reduce the required bandwidth in the connection with the cloud, reduce cost, optimize performance & storage,…	3E-NFR-2	Data compression		Minimize Communication Overhead	
Technological	MFBB shall allow for implementation on different types of generic local hardware. Industrial PC, PLC, Raspberry Pi, …	3E-TR-1				
Technological	Bi-directional real-time communication should be established between the edge devices and the cloud.	3E-TR-2	Bi-directional communication		Cloud/Edge Complementarity towards Service	
		3E-FR-5	Adaptation to specific contexts	Added in the 2021/04/30 meeting	Adapt Operation to Different Contexts	
	ELIAR					
Functional	Dyeing processes consist of different type of sub-processes like bleaching, dyeing, chemical dosing, washing. Some of these sub-processes requires more precise temperature tracking, less process delay depending also on type of fabric, type of dye chemicals. According to these characteristics, priority of dyeing process and its corresponding sub-processes must be determined in a sense like HIGH, MEDIUM, LOW.	Eliar-FR-1			Optimize Service Efficiency through Learning/Inference at the Edge	
Functional	Necessary process data must be distributed among the machines: Steam priority, steam efficiency, temperature values must be distributed among the machines in order to be used tuning algorithms.	Eliar-FR-2	Bi-directional communication		Cloud/Edge Complementarity towards Service	
Functional	Heating performance of the machines must be determined Even though there is one main steam source in a dyehouse, heating performance of the machines can be differentiated between each other depending on factors like size, exchanger type, distance from the steam source, staleness, maintenance date etc. By taking into consideration these factors, heating performance of each machine must be determined to be able to design and implement aforementioned distributed control algorithms.	Eliar-FR-3	Adaptation to specific contexts		Adapt Operation to Different Contexts; Setup Prior to Operation	
Functional	Long term process data for temperature control must be saved: Temperature control takes about 70% of the duration of the dyeing process. Reference values of temperature, realized values of temperature, values of success metrics of temperature control must be saved at database of central monitoring system.	Eliar-FR-4	Report		Provide Data/Reports to System Operator	
Functional	Controller parameters must be tuned offline and real-time: Temperature control in dyeing processes is done by PID Controllers which have several parameters to tune. These parameters must be tuned offline by using long term data and real-time by using process	Eliar-FR-5		Offline tuning, followed by real-time PID parameter	Provide Timely Feedback to Relevant Parties	

	priority data that are distributed among corresponding machines.					
Functional	Solution must ignore anormal temperature values and low performance temperature control steps: If anormal temperature values are occurred solution must ignore them, also data cleaning must be done on historical data for removing low performance temperature control steps.	Eliar-FR-6	Warning: anomaly detection (?)		Learning with Noisy and Missing Data; Provide Data/Reports to System Operator	
Functional	Solution must warn the actors on insufficient steam pressure If steam pressure is generally low and solution cannot control the machines according to the given references and set point, it must warn the actors that it is impossible to control the machines.	Eliar-FR-7	Warnings		Warn System Operator of Relevant Events	
Functional	Performance analysis report: Solution must report performance of control to actor textile dyehouse machine & energy manager	Eliar-FR-8	Report		Provide Data/Reports to System Operator	
Non-functional	If network connection between operator panels is broken, process control must continue: T7701ex must continue controlling dyeing machine without the need of auto-tuning add-on. Add-on is not a must for controlling dyeing machine.	Eliar-NFR-1	Persistency (ability for edge component to continue operation independently)		Persistence of Operation of Edge Nodes	
Non-functional	Network usage must not block other systems which uses it: Auto-tuning add-on requires network communication for distributed control and data exchange. But the network is not dedicated to this add-on. Solution must not block Eliar Teleskop system and coupled machines.	Eliar-NFR-2	Minimizing data exchange		Minimize Communication Overhead	
Non-functional	Data communication period among the control panels must be at least 60 seconds: It is thought that data sharing among machines should be able to be done every 60 seconds while performing distributed control.	Eliar-NFR-3	Real-time performance - Bounded response time		Provide Timely Feedback to Relevant Parties	
Non-functional	Any actor can disable distributed temperature control for machine or process: Our solution is not a necessity for controlling the machine, any actor can disable distributed temperature control for machine or a single dyeing process.	Eliar-NFR-4			Real-time Monitoring and Control of Edge Nodes by Operator	
Non-functional	System must save necessary data on power failure which affects operator panel: If power failure occurs during temperature control, after power is on, add-on must continue running by saving necessary data for continue.	Eliar-NFR-5	Persistency (retain state when system is shutdown intentionally or accidentally)		Availability	
Non-functional	Software integration: UC solution must be run in T7701ex and some modules may need to run on Teleskop server.	Eliar-NFR-6				
Non-functional	System availability: Software must be designed to run 7/24	Eliar-NFR-7	Availability 24/7		Availability	
Technological	Network bandwidth: 1000 Mbps ethernet network must be installed.	Eliar-TR-1				
Technological	Operating System: Developed software must run on Linux OS.	Eliar-TR-2				
Business	Installed software base: Eliar control panel model must be at least T7701ex and Teleskop must be already installed.	Eliar-BR-1				
Business	Solution must be run as an add-on to the current Eliar products:	Eliar-BR-2				

	UC solution must be integrated to T7701ex and Teleskop					
	Macq					
Business	Improving the safety of: • Railway crossing; • School streets; • Complex intersections	Macq-BR-1			Learning with Noisy and Missing Data	
Business	Minimal onsite configuration needed. Although the sites are very versatile a complicated on site configuration is not desirable because of the high involved personnel cost and difficulties to train subcontractors that install the cameras.	Macq-BR-2			Setup Prior to Operation	
Business	Run on multiple versions of the hardware platform (NVIDIA).	Macq-BR-3	Multi-platform			
Functional	Detect persons in image data including status and intentions (walking, crossing tracks while barrier down,…)	Macq-FR-1			Optimize Service Efficiency through Learning/Inference at the Edge	
Functional	Efficiency of edge processing without the need to send images to the cloud / All processing should happen in the edge, in co-located cameras and/or on a ML box (same as camera but without sensors), but not in the cloud	Macq-FR-2		Related to: Coordination between edge and cloud components	Persistence of Operation of Edge Nodes	
Functional	Privacy concerns of images of VRUs	Macq-FR-3	Privacy		Provide User Privacy and Data/Process Security	
Functional	Adaptive configuration of the camera settings depending on weather, lighting, …	Macq-FR-4	Adaptation to specific contexts		Adapt Operation to Different Contexts	
Functional	Integration of privacy aspects between multiple cameras, in the case of deep learning	Macq-FR-5	Privacy		Provide User Privacy and Data/Process Security	
Non-functional	Modular solution supporting different solutions for various applications	Macq-NFR-1				
Non-functional	Real-time	Macq-NFR-2	Response in useful/bounded time		Provide Timely Feedback to Relevant Parties	
Non-functional	Explainable?	Macq-NFR-3				
Technological	Combine different images: • Black & White + near IR; • Color; • Therma; • Time of Flight	Macq-TR-1				
Technological	Possibility to combine with other non-visual technologies: • Radar; • Sound	Macq-TR-2				
Technological	Development in C++ and Python.	Macq-TR-3		Technology requirements: C++/Python		
Technological	Possibility to combine AI with traditional technologies	Macq-TR-4				
		Macq-FR-5	Reports	Added in the 2021/04/30 meeting	Provide Data/Reports to System Operator	
		Macq-FR-6	Warnings	Added in the 2021/04/30 meeting	Warn System Operator of Relevant Events	
KPI1	Increase availability when compared to a centralized approach.	Macq-BR-4			Availability	These requirements were drawn from the "UC Description/Context" section of the "Use-case Definition and Requirements Elicitation" template.

						Classification into Business, Functional and Non-Functional made by task leader.
KPI2	Guarantee that data exchange between edge/IoT and cloud devices is protected; that policies for data privacy (and, when possible, control over privacy) are applied; and that AI algorithms are executed in edge nodes in protected environment.	Macq-NFR-4			Provide User Privacy and Data/Process Security	
KPI3	Provide mechanisms to guarantee interoperability, efficient and easy integration of new edge devices with the core large-scale computing infrastructure (i.e. the cloud).	Macq-NFR-5			Cloud/Edge Complementarity for Service Provision; Real-time Monitoring and Control of Edge Nodes by Operator	
KPI4	Reduce bandwidth requirements	Macq-NFR-6			Minimize Communication Overhead	
KPI5	Sense-compute-act latency	Macq-NFR-7			Provide Timely Feedback to Relevant Parties	
KPI6	Reduction of development, deployment and operation costs for 3rd party software and embedded AI functions in edge devices.	Macq-BR-5				
KPI7	Achieve high scalability thanks to the amount of pooled resources and distributed and composable ML models (bounded by the application's architecture).	Macq-NFR-8			Horizontal Scaling	
KPI8	New services commercialized on the market within the next 3 years of the research and reaching a level of self-profitability.	Macq-BR-6				
	NOS					
Functional	Traffic monitoring always on: The System shall monitor traffic patterns 24/7 to find indicators of security threats and attacks.	NOS-FR-1	Operation 24/7		Availability; Persistence of Operation of Edge Nodes	
Functional	Smart and customized protection: The System shall learn the patterns of traffic of applications concerning IoT devices, and use the protection profile that best suits the identified patterns.	NOS-FR-2	Adaptation to specific contexts		Adapt Operation to Different Contexts; Learning with Noisy and Missing Data	
Functional	The System shall provide mitigation mechanisms against large scale attacks.	NOS-FR-3			Provide Timely Feedback to Relevant Parties	
Functional	Automated Zero Day attack mitigation: The System shall provide mitigation mechanisms against IoT devices vulnerabilities.	NOS-FR-4			Provide Timely Feedback to Relevant Parties	
Functional	If an attack is ongoing, the System shall provide a detailed report in real time or near real time during the attack, and complete resume after it. The System shall provide a global report with information about all installed CPEs to have knowledge about how many CPEs were exposed to attacks, and which was the attack profile/type.	NOS-FR-5	Produce reports		Provide Data/Reports to System Operator	
Functional	The System shall provide metrics related to vulnerabilities and attacks that have been identified and thwarted (or not).	NOS-FR-6	Metrics		Provide Data/Reports to System Operator	
Functional	The System shall provide the possibility for the Service Provider and/or Customer to be informed whenever a vulnerability and/or attack is detected.	NOS-FR-7	Produce warnings		Warn System Operator of Relevant Events	

Design	The System shall be integrated directly and operate in the Home Gateways.	NOS-NFR-1				
Design	The System may be complemented by components deployed outside the Home Gateway, namely mechanisms to support the operation of the System deployed in edge and/or cloud platforms.	NOS-NFR-2			Cloud/Edge Complementarity for Service Provision; Real-time Monitoring and Control of Edge Nodes by Operator	
Technical	The System shall use the operating system RDK.	NOS-TR-1				
		NOS-NFR-3	Privacy and security of exchanged data	Added in the 2021/04/30 meeting	Provide User Privacy and Data/Process Security	
	SHAYP					
Business	The battery lifetime of the hardware device shall match as well as possible the lifetime of standard water meters. • Current specification of the battery: XXX • Cost of the battery: 9 EUR • Current consumption of sending a message : XXX • Current number of messages sent per day: 25 • Estimated lifetime of the battery : 10 years / goal = 16 years	Shayp-BR-1	Maximizing lifetime; to be checked		Maximize lifetime of edge nodes	
Business	Faster anomaly detection thanks to a conjunction of work between edge devices and cloud. Edge devices should already flag anomalies as early as possible and cloud would then use that flag to confirm if the situation has to be flagged as an anomaly. Customers want to avoid costly leakages and water damages, so the earlier they receive an alert about a leak, the better. • Current situation: between 3 hours in best cases for household and 24 hours for institutional buildings to detect a leak • Goal : anomaly detection in less than 1 hour	Shayp-BR-2		Feedback/Specific: Anomaly detection	Provide Timely Feedback to Relevant Parties	
Business	Subscription on telecom => cheaper if sending less messages	Shayp-BR-3	Minimizing data exchange		Minimize Communication Overhead	
Functional	Detect leaks/anomalous consumption within the hour supported by anomaly detection on the edge in combination with the cloud • Flag anomaly on the edge & send to cloud • Increase amount of data sent to the cloud (UC1) • Verify false positives on the cloud	Shayp-FR-1	Response feedback		Cloud/Edge Complementarity towards Service; Warn System Operator of Relevant Events; Learning with Noisy and Missing Data; Availability	
Functional	The device shall send data only when required based on the type of building and on the current water consumption When no water consumption – avoid sending data • Update hardware for flexible sending • Update message structuring • Update data ingestion module	Shayp-FR-2	Minimizing data exchange		Provide Data/Reports to System Operator; Minimize Communication Overhead	
Non-Functional	Battery life extension (UC1) – The battery life shall be increased from 10 to 16 years (as long as the water meter)	Shayp-NFR-1	(Lifetime)		Maximize lifetime of edge nodes	
Non-Functional	Remote calibration (UC4) – A technician installing the device shall be able to enable calibration mode resulting in sending messages every minute for 15min	Shayp-NFR-2		Calibration (?)	Setup Prior to Operation	
Non-Functional	The data on device and in transit should be secured to prevent disclosing (privacy-sensitive) water consumption data.	Shayp-NFR-3	Privacy			

Technological	Bi-directional communication (UC3, UC4) – The cloud shall communicate with the edge device in order to configure, update (firmware, training set of type of building) or send action (shut valve)	Shayp-TR-1	Bi-directional communication		Cloud/Edge Complementarity towards Service; Real-time Monitoring and Control of Edge Nodes by Operator	
Technological	The device should be able to store & process enough local data in view of pattern recognition and initial detection of anomalous consumption	Shayp-TR-2	Local computation & data storage capabilities		Persistence of Operation of Edge Nodes	
Technological	Data should be compressed on device (within 512 bytes) without losing necessary information for computing useful insights on the cloud.	Shayp-TR-3	Minimizing data exchange		Minimize Communication Overhead	
			Reports/warnings	Added in the 2021/04/30 meeting; mapped onto Shayp-NFR-2		