WORKING**AGE**

Smart Working Environments for All Ages

D5.1 – IoT Platform

WP5 – IoT Platform

D5.1– IoT Platform

Project number:	826232
Project acronym:	WorkingAge
Project title:	Smart Working Environments for All Ages
Author(s):	GREEN COMMUNICATIONS (GC)
Partners contributed:	ITCL, EXUS, UCAM, POLIMI, BS, RWTH, TPZ, AUD, EENA, INTRAS, TMA
Delivery date:	M15 (April 2020)
Document date:	30/04/2020
Version:	1
Revision:	3
Deliverable type:	Report
Remarks:	
Status:	⊙ PU (Public) O PP Restricted to other programme participants (including the Commission Services) O Restricted to a group specified by the consortium (including the Commission Services) (please specify the group) O Confidential, only for members of the consortium (including the Commission Services

Document Revision Log

VERSION	REVISION	DATE	DESCRIPTION	AUTHOR
0	0	23/03/2020	First draft	GC
0	1	24/03/2020	Changes in the sensors and edge cloud sections	RWTH, GC
0	2	13/4/2020	Added content in paragraph 2	EXUS
0	3	15/4/2020	Added content in 1.4.2 and 2.2	POLIMI
0	4	16/4/2020	Added content in 2.2	AUD
0	5	16/4/2020	Added content in 1.1, 1.4.2, 2.2, 2.4.2, 3.1 and 3.2	ITCL
0	6	21/4/2020	Added content in 1.1, 1.4.2 and 2.2	ITCL
0	7	21/4/2020	Modified description of DSS (2.1)	POLIMI
1	0	22/4/2020	Update section on sensors	GC
1	1	27/4/2020	Executive summary and Conclusion	GC
1	2	30/4/2020	Partner review input, typo corrections, acronym table, update edge cloud section	BS, ITCL, POLIMI, GC
1	3	30/4/2020	Eye blinks update. Final review and formatting before submission	BS, ITCL

Acronym Table

DSS	Decision Support System
ECG	Electrocardiography
EEG	Electroencephalography
GSR	Galvanic Skin Response
IoT	Internet of Things
RH	Relative Humidity
T	Temperature
WA	WorkingAge
YOI	Mesh router of GC

Executive Summary

This deliverable aims at describing the specifications of the WA Tool System that will be deployed during project pilots. These specifications are the results of the system setup in response to the technical requirements defined in T2.4. The document will serve as basis for the setting up of the pilot operational manual D9.1.

The deliverable is organized in two parts. The first describes the hardware and software specifications of the IoT infrastructure: the sensors, mesh routers, mesh software, administrator interface and tools. The second section describes the components of the WA mobile application (place of the user interface and of the WA Decision Support System (DSS)) and the communication protocol between the WA sensors and the WA application.

Throughout the document, it is described how the generic WA Tool architecture will be adapted to each use case of the WA project.

D2.4 Technical Requirements
WA Tool System Technical Requirements

D5.1 IoT System Report
WA Tool System Specifications

D9.1 Pilot Operational Manual
WA Tool user and administrator manual

Table of Contents

Figure Index

Table Index

Introduction

As defined in D2.4 technical requirement and in the aim of providing fast, secure and resilient health and working environment monitoring services, the consortium has come to the conclusion that the WA Tool should adopt an architecture where most of the WA computation power is located close to the data source, on an Edge cloud located on company side. To answer WA mobility requirements the consortium will develop a mobile IoT infrastructure composed of wearable sensors and devices connected through an embedded wireless mesh network to monitor the participants while on the move. Connection with external servers - BS and TPZ's servers - will be provided through an Internet gateway and using secure IP tunnels.

Figure 1 introduces the generic architecture of the WA Tool. Some item may be removed from the architecture to suit the out of work and home pilot environments.

The following document provides the detailed specifications of each layer of the WA architecture (section 1) and mobile applications (section 2).
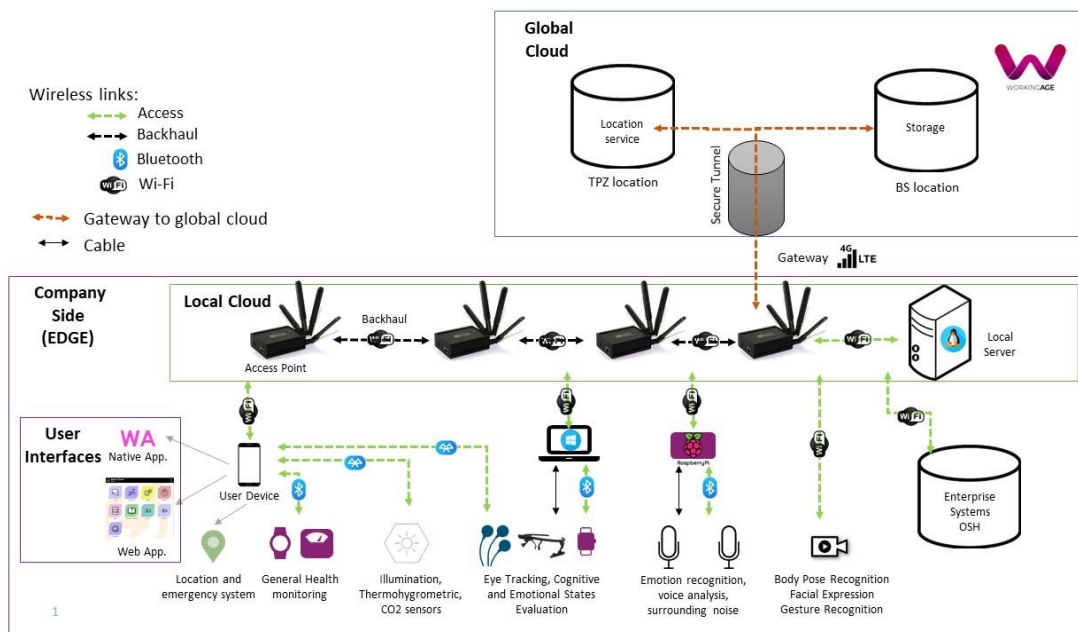

Figure 1: Architecture of the WA Tool

1 The Mobile IoT Platform

The participant will be monitored using a set of wearable sensors and devices. They will be also equipped with a smartphone and the WA native application providing the user interface. Sensors and smartphones will be connected to the WA edge cloud and to external servers thanks to a local mesh network. The sections below describe in details the specifications of each layer of the WA Tool system.

1.1 The Sensors

WA users will be equipped with a set of sensors to monitor their health and environment. The list of the WA Tool's sensors is provided in Table 1. It comprises smart bracelets, smart glasses, a headband, cameras, microphones, lux meters. CO_2/T/RH sensors and a body scale.

Table 1: List of WA Tool's Sensors and Functions:

Icon	Picture	Role	Description
		Facial Expression	Dahua IPC-HFW1320S-W
		Eye Blinking Rate	Dahua IPC-HFW1320S-W
		Body Pose estimation	Dahua IPC-HFW1320S-W
		Voice Analysis	Jabra Evolve 65e
		Noise Analysis	Self-development

		Activity Tracker	Xiaomi MiBand
		Body Scale	Xiaomi Mi Smart Scale (MiScale)
		GSR and ECG Wristband	Empatica E4
		Eye Tracker	Pupil Labs Pupil Core
		EEG Headband	Muse 2
		Mobile Phone	Xiaomi Mi9
		Environmental sensor	Self-development ITCL

All monitored persons will be equipped with the set of sensors that differs according to the use case. The next sections describe the sensor set deployed per use case.

1.1.1 At Work

At work, the participant will be monitored by the sensors showcased in Figure 2. This is an abstract of the participant's equipment that will vary according the WA use cases.
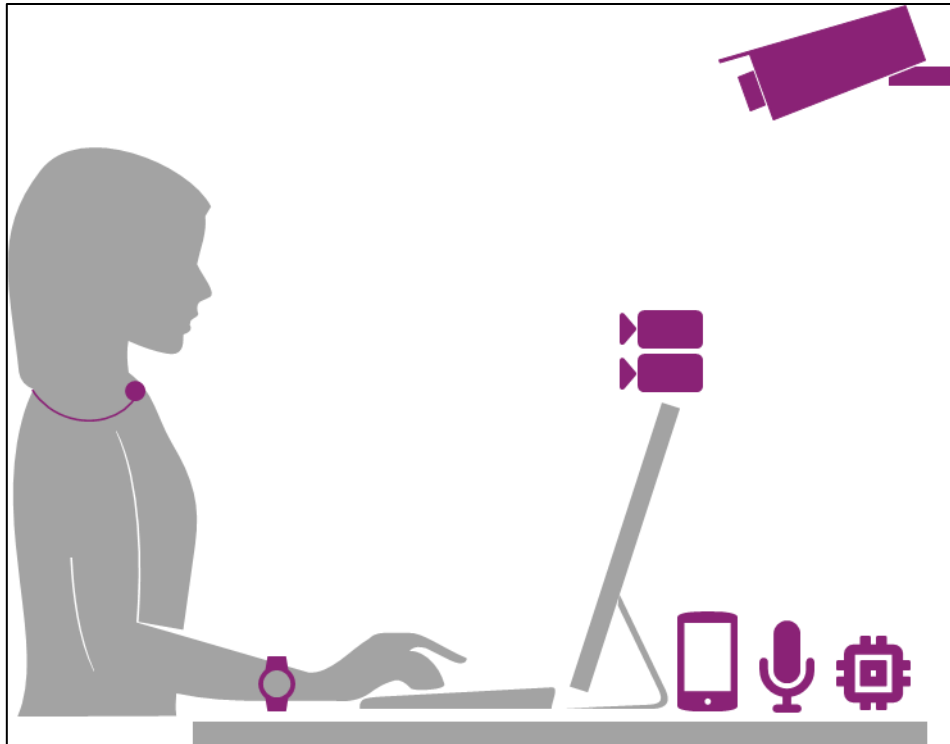
Figure 2: Participant's Sensor Equipment

Additional sensors will be provided to groups of participants (not used by all users) with some restrictions (Figure 3).

Additional sensors:

- EEG-Headband: One person per company.
- Empatica E4 Wristband: One person per company
- Eye Tracking Glasses: A few persons per company (an exact number has not yet been determined).

Restrictions:

- Eye-tracking analysis and facial affect analysis cannot be carried out together.
- Whether EEG-headband and eye-tracker can be used together is determined in the in-lab study.
- Whether (or how) Activity Tracker and GSR-Wristband can be used together is determined in the in-lab study.

Note that at the time of writing of this document, the Lab-studies were partly halted due to limited or prohibited lab access, as part of the measures during the Covid-19 pandemic.

Figure 3: Additional Sensors at Work

1.1.2 Out of Work and at Home

The users will get the possibility to use the WorkingAge system additionally at home, on a voluntary basis especially regarding the camera and microphone. Participants who consent to its use will receive a reward (e.g. the headset).

Two different scenarios are possible for using the sensors at home. Some sensors can only be used at a previously defined, fixed location, for example at a desk. These sensors can be used whenever the participant is at that location (Figure 4: right image). Some other sensors can be used on the go, users can use them whenever and wherever they want and/or consider it helpful or necessary (Figure 4: left image).
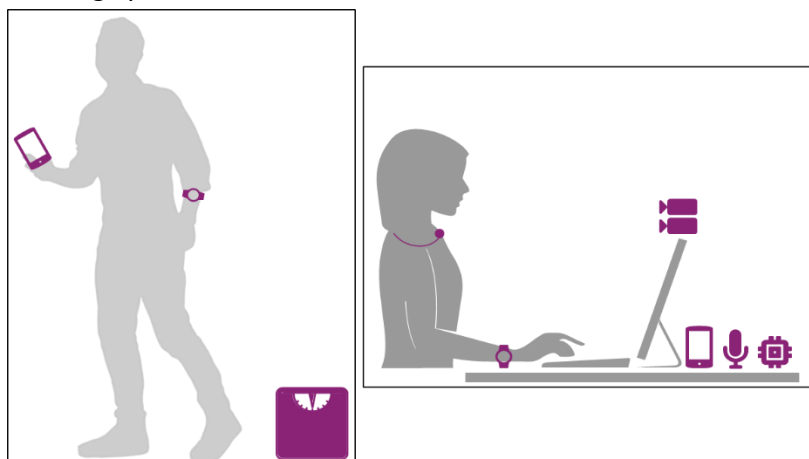
Figure 4: Sensor Set – Out of Work (left image) and at Home (right image)

Figure 4 showcases the sensors that could be used by **all users** at home. The microphone for voice analysis is connected via Bluetooth to the Raspberry PI that needs a power supply. The user can therefore only move with the Raspberry in a limited range.

Figure 5Figure 4 introduces the sensors that can only be used by **some users** at home:

- Empatica E4 – few users
- EEG headband – few users
- Body pose camera – only if possible (difficult installation)
- The microphone for voice analysis is connected via Bluetooth to the Raspberry PI that needs a power supply. The user can therefore only move around with the Raspberry in a limited range.
- The Empatica wristband is connected via Bluetooth to the Laptop. The user can therefore only move around the Laptop in a limited extent.
- The EEG headband is connected to the smartphone via Bluetooth, in addition, measurement of the EEG headband is affected by movement, the headband can be worn anywhere in resting positions, but is not suitable if movement is involved.

Figure 5: Sensor set from some users – Out of Work and at Home

1.2 The Smartphone

Each participant will be equipped with a smartphone that will host the WA native application. The WA native application main functions are described in section 2. The smartphone selected by the consortium is the Xiaomi Mi9. Smartphone key features are provided in the Figure 6.

Xiaomi Mi9 specifications:

- Dual frequency GPS with Galileo
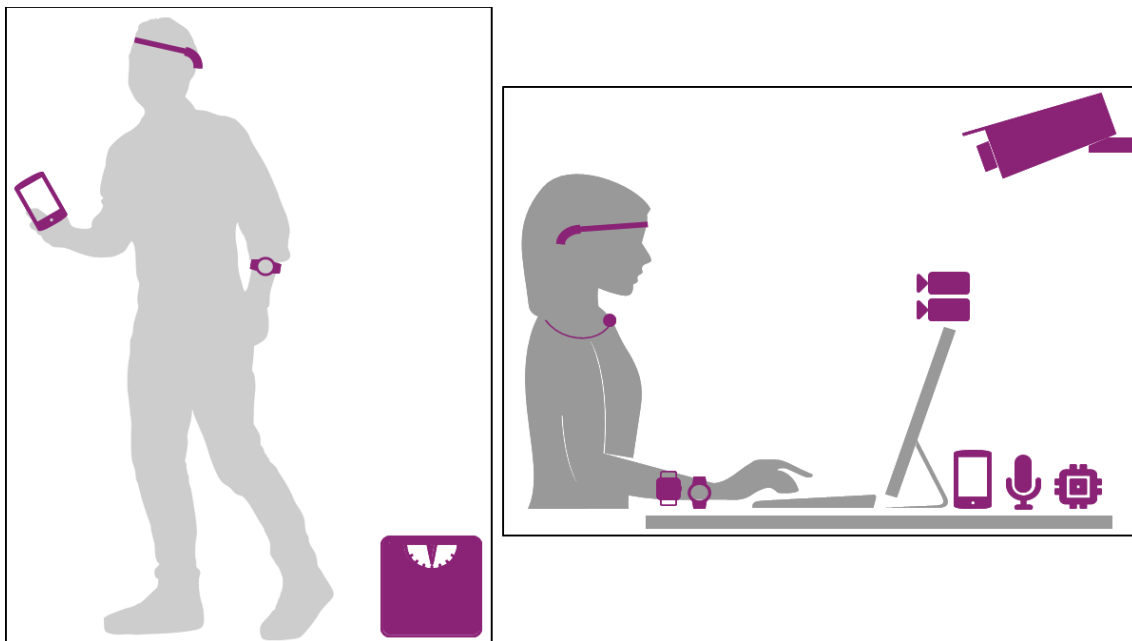- High CPU/GPU capabilities Snapdragon 855
- CPU octa-core, up to 2,84 GHz. Octa-core (1x2.84 GHz Kryo 485 & 3x2.42 GHz Kryo 485 & 4x1.78 GHz Kryo 485)
- GPU: Adreno™ 640
- Ram 6Gb
- Storage from 64GB
- Fast wireless charging 20W

Figure 6: WA Smartphone Specifications

1.3 The Mesh Network

Sensors and user devices will be connected to the edge server and external servers through a local mesh network. A mesh network consists in a set of routers called YOI that connect wirelessly to create a network and that provide a Wi-Fi or Bluetooth hotspot to connect sensors and users to the mesh network. Each router YOI comes with a GreenSoft license that provide intelligent routing, Quality of Service (QoS), mobility and edge computing capacity to host applications and services directly into the mesh network. Among the local services embedded into the mesh network are the administrator tools. The following sections describe the above-mentioned mesh network components.

1.3.1 Mesh Routers

A YOI is an embedded Linux router equipped with Green Communications' software (GreenSoft). A YOI router is equipped with 3 network interfaces: Ethernet, Wi-Fi, and either a Wi-Fi/Bluetooth or a cellular broadband modem (2G, 3G, 4G, LTE). These network interfaces can be used for 3 purposes:
- to reach another network or to provide a gateway;
- to provide an access so sensors and devices, also called mesh clients, can connect to the network (using DHCP);
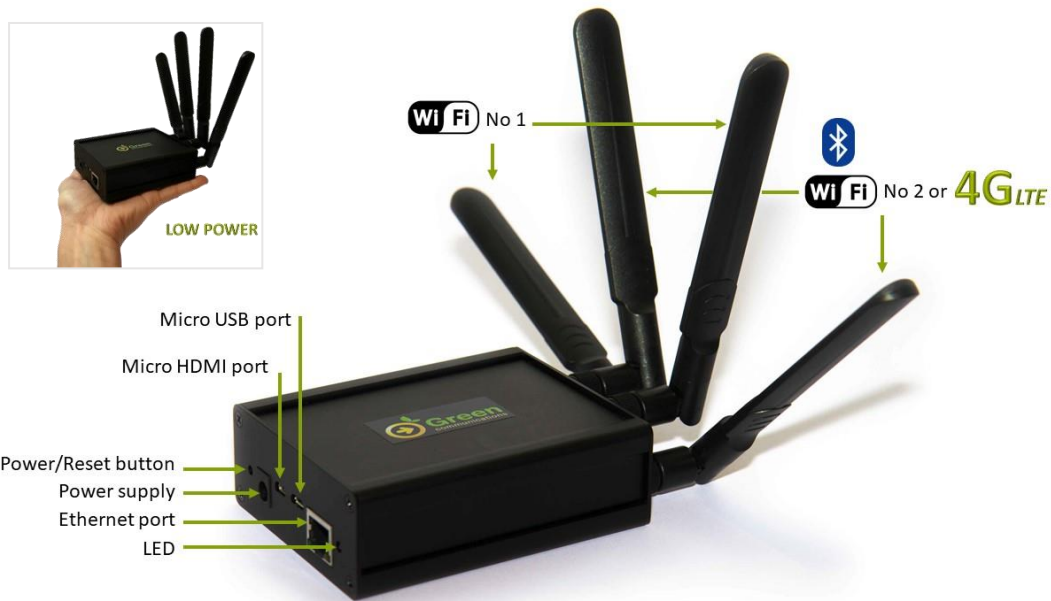- and to make a backhaul network that connects YOI routers together.

Figure 7: Mesh Router (YOI) Description

The default settings of the two types of YOI routers' deployed in the WA Tool are the following:
- YOI-BT: Wi-Fi No1 (backhaul), Wi-Fi/Bluetooth No2 (access), and Ethernet (gateway)
- YOI-4G/BT: Ethernet (access), Wi-Fi No1 (backhaul), and cellular broadband modem (gateway)

One may change the settings of an interface to create a Wi-Fi gateway, set an additional Wi-Fi access point, etc.

YOI routers feature less than 5W energy consumption so they can be battery powered. Routers are tiny enough to be embedded into a vehicle.

Table 2: The Mesh Router Specifications

Wireless	Access: Wi-Fi (a, b, g, n)/Bluetooth(4.0) Backhaul: Wi-Fi (a, b, g, n) Gateway: 4G/LTE Category 4 (LTE Bands: B1 (2100), B3 (1800), B7 (2600), B8 (900), B20 (800DD)), or Ethernet or Wi-Fi
Enclosure	IP56, 85x105x35mm
Energy consumption	<5W
Power supply	Battery (10AH provide 19h battery life) or power plug
Bandwidth	Up to 300Mbps
Weight	324g

1.3.2 The GreenSoft

Green Communication's software is the key enabler of the Wi-Fi mesh network that includes intelligent routing, quality of service (QoS), local content, apps and services. GreenSoft is a set of software components dedicated to wireless

networking. It features a wide range of applications, from low-level programs to web applications for end users. GreenSoft's low-level programs are mostly routing software for mesh networks, but also feature an SNMP module and helpers for Zeroconf networking. High-level utilities feature web applications such as a chat, a network setup app and a live network visualization tool.

Routing Software: GreenSoft's intelligent routing protocol is in charge of the following tasks:
- It detects the other devices that are part of the network.
- It estimates QoS properties for each link.
- It computes (possibly indirect) routes to other devices and sets the system's routing table up accordingly (thus ensuring that every device forwards data properly. and that any network host can reach any other host).
- When some devices forward data from the mesh network to other networks (e.g., the Internet), it ensures that all network hosts may reach these other networks.

Users Mobility: GreenSoft provides network users' mobility thanks to its handoff manager program. This is a userspace daemon that helps routers provide access points to regular Wi-Fi users. These users, though outside the core network, may associate to the access points and get regular network connectivity through the mesh network. The handoff manager ensures users can move from an access point to another without disrupting their connections. The handoff manager performs the following tasks:
- It either acts as a distributed DHCP server or as a DHCP relay. relaying DHCP requests from users to a designated DHCP server.
- It snoops on DHCP transactions and informs the network accordingly so routers can map MAC addresses to IP addresses.
- It snoops on Wi-Fi association and disassociation events, so routers can detect handoffs.
- It updates the system's routing tables accordingly and configures access point interfaces to act as a gateway to associated users. In addition, GreenSoft features an mDNS helper. This is a userspace daemon that ensures Zeroconf works. In practice, this means that devices that run the GreenSoft may advertise Zeroconf services to other devices and users; and that users may also advertise their own Zeroconf services to the network (including other users).

Local content, apps and services: the GreenSoft's local content, apps and services are described on the section 1.4 on WA Tool's edge cloud.

Performances: GreenSoft's intelligent routing is an implementation of the OLSR standard protocol for Mobile Ad hoc NETwork (MANET) developed by Green Communications (GC). These implementations aim at increasing ad hoc/mesh networks robustness, scalability and embeddability. Among these enhancements, the GreenSoft routes the information over multiple short hops with high signal quality; provides priority to MANET control messages; and

provides a robust multicast support. The GreenSoft's routing protocol has proven high performances with video conferencing over 30 Wi-Fi hops (state-of-the-art <5 hops). GreenSoft has been integrated and validated into low power routers, featuring only 5W of energy consumption (competing products >15W) enabling the system to be battery powered. GreenSoft can also be integrated as software directly into a compliant robot without reducing the system lifetime.

1.3.3 Network Size

The three pilot sites will be equipped with a set of mesh routers so as to provide sufficient network capacity to connect all the sensors and user devices during the tests period – one user being equipped with 7 to 10 sensors and one smartphone device.

By means of example, if a group of 8 participants will be monitored at the time during the long-term testing and per pilot site (details in D2.5), it represents a group of 88 connected devices. It is recommended to use one router every 15 to 20 devices. The corresponding network size would therefore be composed of 5 routers.

1.4 The Edge Cloud

In the aim of providing fast, resilient and secure service the WA Tool will host most of the WA intelligence close to the data source, at the network edge, into the WA Edge cloud.

These services will therefore be available anytime with and without internet access. They will be fast and provide high quality user experience due to the short travel of the information that is processed and stored close to the user. Data will be securely processed at its source avoiding leaks over the Internet.

The Edge Cloud of the WA tool consists in the combination of the computing power of the mesh routers and of an additional local server. The sections below describe the specifications of the Edge cloud distributed into the mesh routers also called the Green Cloud and provide a description of the additional local server.

In the WA project, the Green Cloud will host the administrator tools to manage the IoT infrastructure and the additional server will host the WA tool services' programs.

1.4.1 The Green Cloud

Mesh routers embed a distributed edge cloud, also called the Green Cloud. The Green Cloud combines mesh routers' computing capacity described in Table 3. The Green Cloud will host the administrator tools, as described in 1.6.

Table 3: Mesh Router's Computing Capacity

Computing Capacity per Mesh Router	
OS	Linux
RAM	512MB
DISK	32 GB
CPU	Cortex-A9 800 MHz Dual Core
Other	Web server Xmpp server

The Green Cloud hosts web applications such as a network setup, a network visualization tool, and collaborative services such as a chat and a file sharing system. The applications are available through a web framework (Figure 8). This framework uses client-side JavaScript and static HTTP, except for three dynamic HTTP resources:

- A resource that provides a GraphML (XML) representation of the current network. The network visualization tool uses this resource. A custom GreenSoft program provides this resource to the web server using the SCGI protocol.
- A resource that converts GET and POST HTTP requests including JSON data to SNMP GetBulk and Set requests. The network setup app uses this resource. A custom GreenSoft program provides the SNMP/JSON converter to the web server using the CGI protocol. Also note that GreenSoft features a Net-SNMP module that implements the SNMP configuration backend.
- A resource that maps XMPP traffic to HTTP using the BOSH protocol. The chat app uses this resource. Green Communications' routers (YOI) rely on ejabberd for this resource.

Figure 8: Green Cloud Web Framework

The Green Cloud is open. One can provide additional local content to users. One can also easily develop new applications to integrate to the framework.

1.4.2 Additional Local Server

Due to the large volume of data processed at the edge, more computing capacity should be provided. Therefore, the partners will add local server(s) connected to the local mesh network to host the WA services' programs.

The following scenarios will be explored:

- The first where each partner provides a local computing unit connected to the local mesh network and that will process the data incoming from its sensor. A list of additional computing units is provided in Table 4.
- The second scenario where the number of edge computing units will be reduced and some partner's programs will be merged on a same machine.

During the project, the consortium will deploy at first the edge cloud using the first scenario and will go towards reducing the number of edge computing units as per scenario 2.

Table 4: List of Additional Computing Units:

Sensor	Service	Edge Computing Unit
	Facial Expression	Linux Laptop/Server (with NVidia GPU)
	Gesture Recognition	Linux Server
	Eye Blinking Rate	Windows or Linux laptop
	Body Pose estimation	Linux Server with a NVIDIA GPU
	Voise Analysis	Raspberry PI (in common with Noise Analysis) + Linux Server
	Noise Analysis	Raspberry PI
	Activity Tracker	Mobile Phone
	Eye Tracker	Windows Laptop

	EEG Headband		Windows server
	GSR/ ECG Wristband		
	Mobile Phone	n.a.	n.a.
	Environmental sensor		Mobile Phone
	Body Scale		Mobile Phone

1.5 Connection to Remote Servers

The local Mesh network will be connected to two remote servers (to BS server and to TPZ server) through an Internet gateway and using secure IP tunnels.

1.5.1 The Gateway

One can connect the local mesh network to Internet or other networks using one of the three following modes:

- Wi-Fi gateway: One can turn the Wi-Fi interface of one mesh router so that it connects to the Wi-Fi of the facility and gets access to the Internet.
- Ethernet gateway: One can plug one router to the facility's Internet network using Ethernet.
- 4G/LTE gateway: One can use a mesh router equipped with a 4G/LTE modem to connect the local mesh network to the Internet through 4G.

A single gateway will provide an Internet access to all the routers and users of a same mesh network.

Figure 9: YOI-4G/LTE – A Mesh Router Equipped with 4G/LTE Modem

1.5.2 Connection to TPZ and BS Remote Servers Using Open VPN

See Section 1.6.4

1.6 The Administrator Tools

Specific administrator tools have been developed to enable an administrator to monitor the WA IoT infrastructure remotely. Among these services are the My Network application to visualize the state of the network, a tool to locate of the users and sensors, and a tool to connect several sites and monitor them at the time. The tools are web applications available through an administrator interface described in the section below.

1.6.1 Administrator Interface

The administrator of the WA Tool can manage the local mesh network through the web portal of the Green Cloud (Figure 8). Once logged into the Green Cloud, the administrator accesses specific applications for local network management such as: a network visualization tool, the application setup and a mesh client vCard editor (Figure 10).

Figure 10: Green Cloud Administrator Interface

1.6.2 Network Visualization tool

My Network is an application to visualize the state of the mesh network in real time. The application provides the administrator with the following set of information:

- Location: Geographical location of routers and clients on a background map (Figure 11) or logical location on an empty background (Figure 12). The router you are connected to is represented by a green disc overlay;

- <u>Mobility</u>: Real time view of mesh clients moving from one router to another (Handover).
- <u>Number of connected mesh clients per router</u>: Provided on a tag beside the router's picture;
- <u>Gateways</u>: When a router is a gateway to the Internet or to another network, it connects to either a node with a cloud or computer picture. When the router features a cellular interface, it carries an additional icon with connection type (2G, 3G or 4G) and signal strength (Figure 12);
- <u>Router's information</u>: Router's name, picture, network address and a link to make the router blink its LED, in order to localize and identify it (Figure 13);
- <u>Mesh client's information</u>: mesh client's picture, contact information, coordinates, Hostname, IP and MAC addresses and a link to the vCard Editor application to customize the mesh client's information (Figure 13);
- <u>Network link quality</u>: Signal strength in dBm is reported on each link. The application also uses a colour code to visualize the network links quality. Colour code to visualize the network links quality:
  - Ethernet: Black link
  - Excellent (signal > -50dBm): Thick red and yellow link
  - Good (-50dBm > signal > -60dBm): Red and white link
  - Average (-60dBm > signal > -70dBm): Red link
  - Bad (-70dBm > signal): Thin white link
  - Quality unavailable: Thin grey link
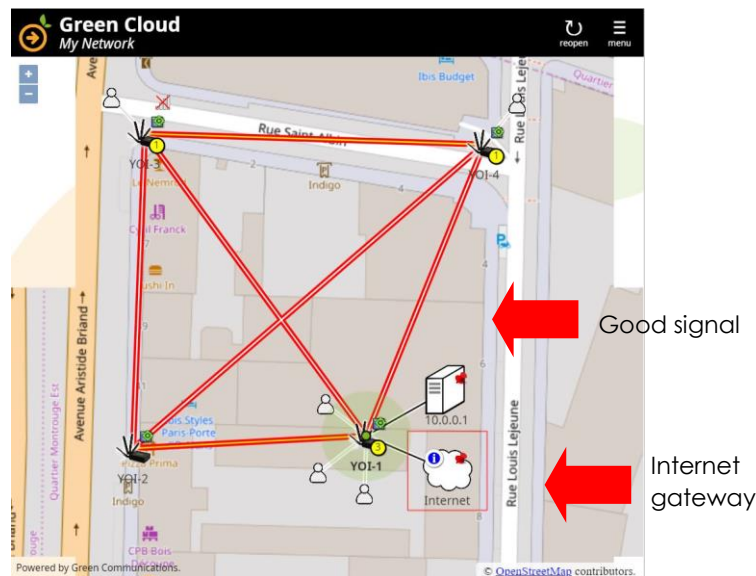
Figure 11: My Network – With Background Map
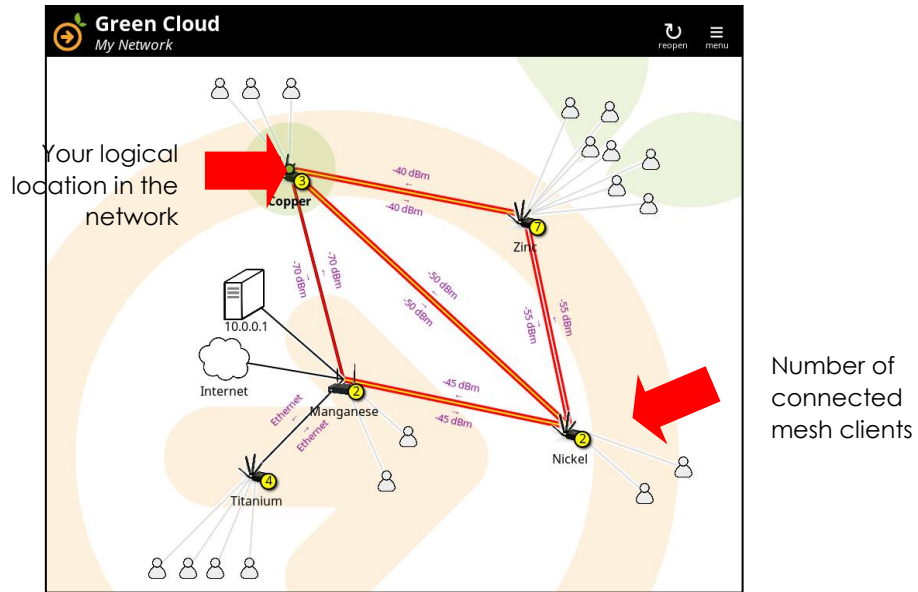
Figure 12: My Network – Without Background
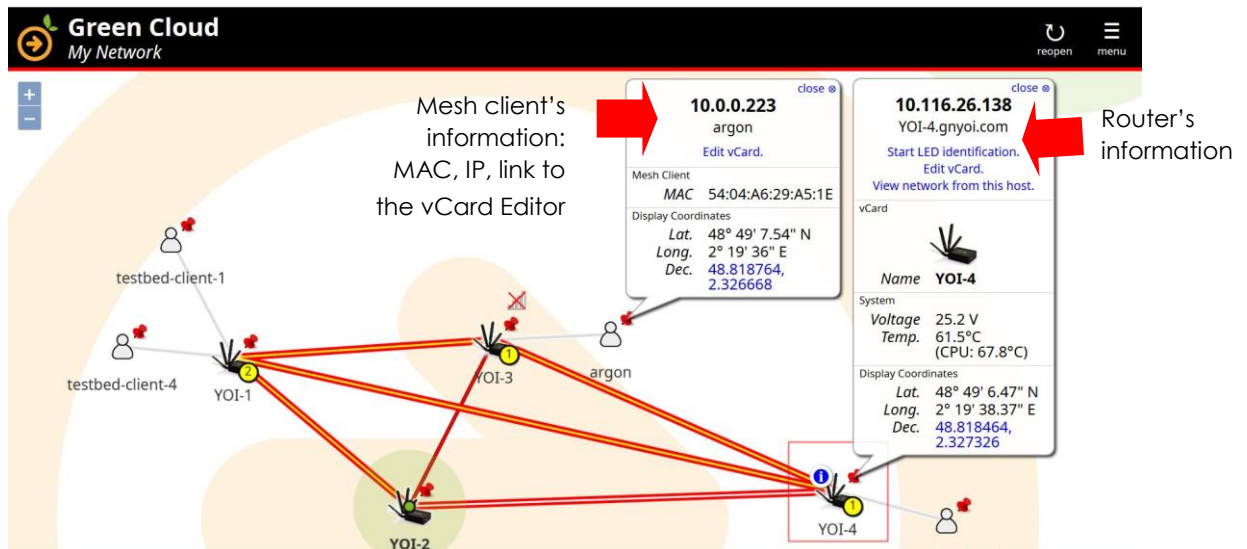
Figure 13: My Network – Routers and Mesh Clients Information

1.6.3 Mesh Client Location (User and Sensors)

One can change the settings of the application My Network in order to display the network view on a background map. The Background map is displayed automatically in My Network when a mesh client communicates its coordinates. A mesh client can share dynamically its coordinates by activating the "Share user location" function in the menu of the My Network application (Figure 14).
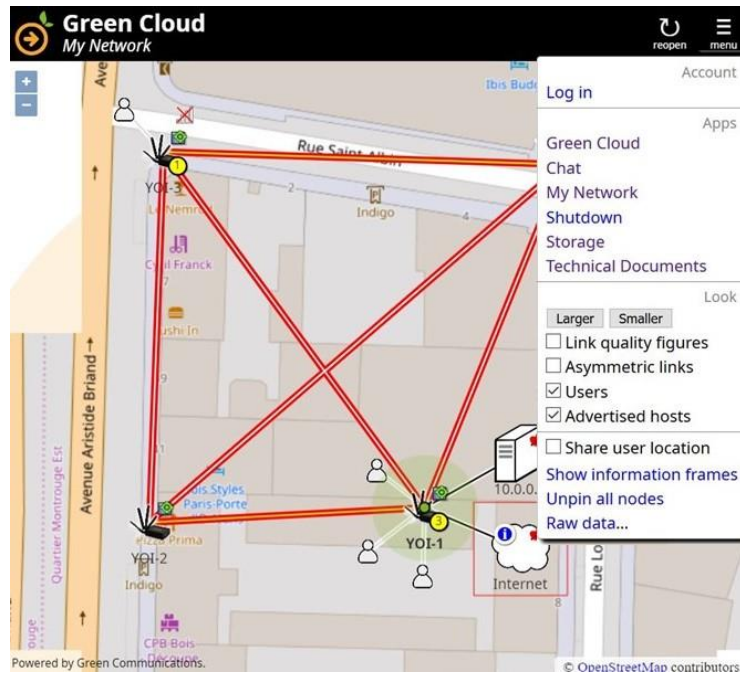
Figure 14: Mesh Client Location (Users and Sensors)

1.6.4 Connection to Remote Server and Multi Sites Management Tool

A WA administrator may like to connect its local network with remote server or monitor several sites at the time. Therefore, he can use OpenVPN to merge multiple independent mesh networks into a single global network. For instance, consider two independent networks *A* and *B*, as depicted in Figure 15. Each network is connected to the Internet, using routers A-1 and B-1. We intend to connect A and B using OpenVPN tunnels.
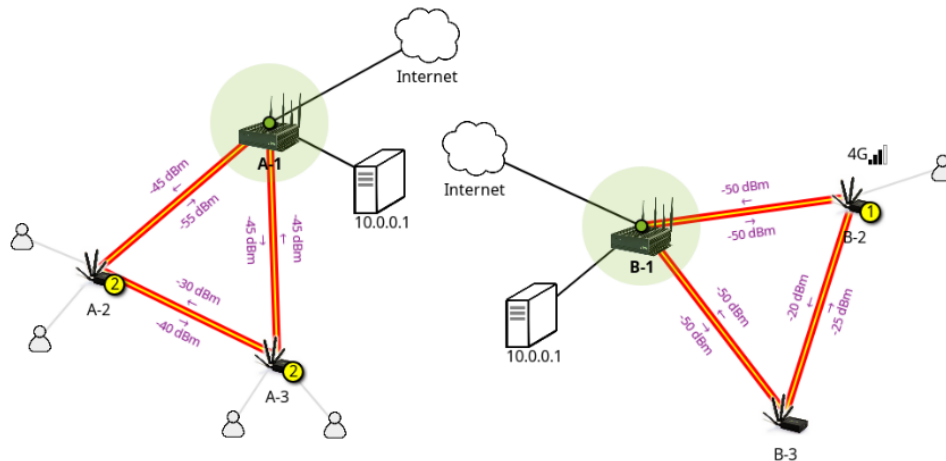
Figure 15: Two Independent Mesh Networks

One may connect both networks:

- directly via a single OpenVPN tunnel (Figure 16);
- or use a dedicated mesh router as an OpenVPN server, and then connect *A* and *B* to this server, each network using a dedicated OpenVPN tunnel to the server (Figure 17).
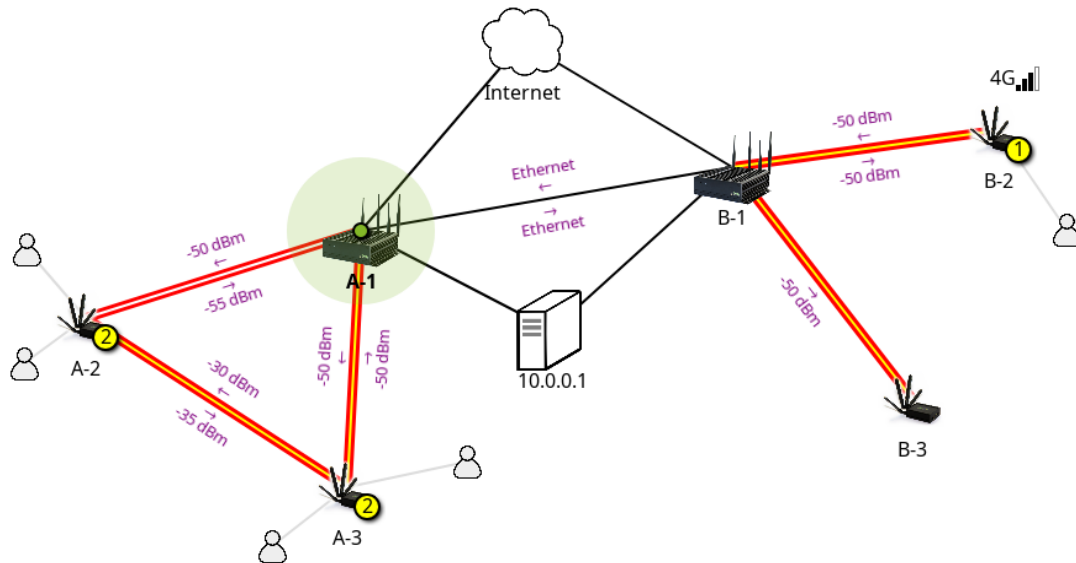
Figure 16: Networks A and B Connected Directly

In Figure 16, router A-1 connects directly to router B-1 using a single OpenVPN tunnel. Both routers depict the tunnel as a distinct Ethernet link, even though they use the Internet to reach each other. This is because with this setup, OpenVPN exposes the tunnel as a virtual Ethernet interface. Note that one cannot use a direct connection to connect more than two routers and that a direct connection would not be possible if both A-1 and B-1 were to be hidden behind NAT gateways. Also notice that each router has a limited view of the network, thus A-1 does not see the link between B-2 and B-3. This is normal and does not impair routing, as routers may only ignore links that are not essential to the routing algorithm.
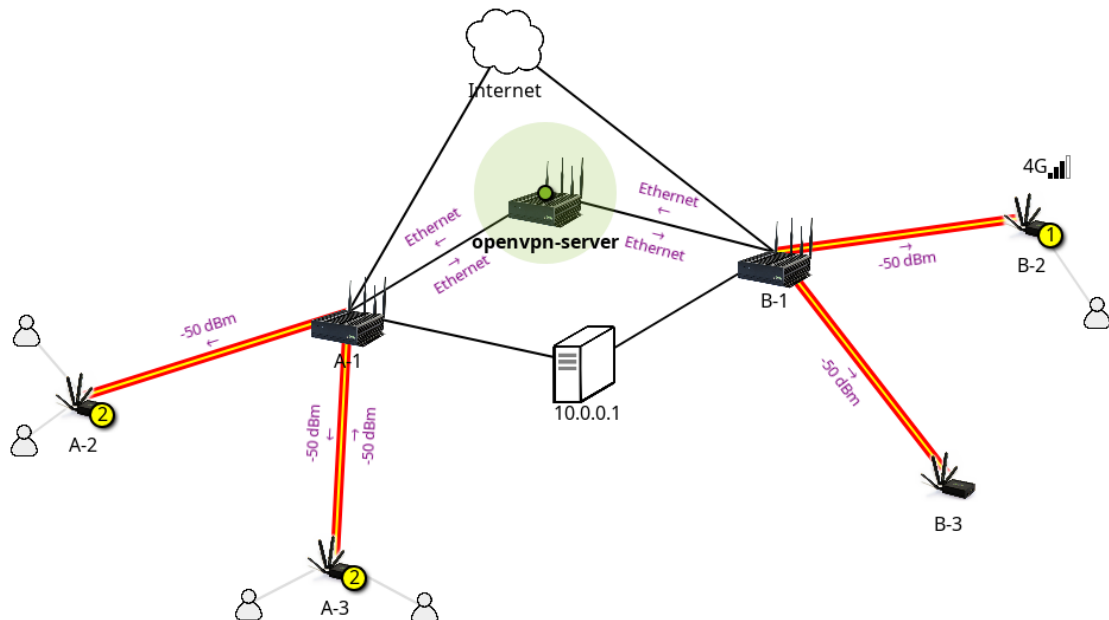
Figure 17: Networks A and B Connected via a Dedicated Server

With the setup presented in Figure 17, one dedicates a router to providing an OpenVPN server and routers A-1 and B-1 connect to this server. As long as no NAT hides the gateway (i.e., it has a reachable public IP address), one may

connect as many networks together as needed (we could plug in network C, D, etc.). Note that routers still depict OpenVPN tunnels as Ethernet links, and that the OpenVPN server ignores some links that it does not need to route packets properly (e.g., between A-2 and A-3, or B-2 and B-3).

2 The WA Mobile Application

In addition to the IoT Infrastructure, the WA tool comprises the WA mobile application. The role of the application is to carry out all the interactions with the user through a set of human computer interaction (HCI) services. The application, implemented in an Android environment, is fully compatible with the specifications of the mobile device described in paragraph 1.2 that will be used for piloting purposes. The application has been designed in full alignment with the project's user-centric principles, providing, among others, the following features:

- Customisable notifications: the users will be able to define the type of notifications they will be receiving, as well as their format and frequency.
- Emergency service: in case needed, an alert will be generated towards the user and/or the E112 service (depending on the severity of the situation and always upon the user's consent).
- Gamification: the application will contain gamification-based features to ensure its uptake by the users and also to encourage their regular and consistent feedback and use.
- Design-driven features: the app will also include a series of design-driven features, such as unique user personas and individualised preferences.
- Privacy and security: the overall WA architecture ensures that the data provided by the users is treated in a privacy and security compliant manner, in alignment with GDPR.
- Contactless interaction: thanks to the gesture-based interaction platform, the users will be able to interact with the WA Tool through gestures.

2.1 Services and Activities of the Mobile application

The WA Tool, embedded in a mobile application, consists of the following main components:

1. A Decision Support System (DSS) Component: receives high-level data from the ecosystem of sensing devices, aiming to generate rule-based recommendations. In turn, the DSS component comprises of:
   - A DSS API, which enables the rest of the Android App to use the functionalities of the DSS.
   - The main DSS module which, leveraging the ProbLog engine, makes use of the intervention rules and generates the advices.
   - A rule updater, which customises the intervention rules.
   - A persistency storage, where the DSS saves its state whenever the mobile application is closed by the Android OS.
2. The Location & Emergency Service component: in charge of spotting the geolocation of the user and to convey the emergency alerts (in a format of an 'emergency message') to the PEMEA Emergency Service Emulator on the cloud. Thus, this component consists of:

- A Position Engine: computes the user's location and identifies whether the user is located at a work, home or office environment and forwards this information to the DSS Component.
- An Emergency message generator: creates and forwards the emergency messages, originally triggered by the DSS, to the PEMEA Emergency Service Emulator.

3. A UI component: including all the user interface-related services of the mobile application and mainly the module which visualises the recommendations to the user.

4. A Registration component: meant to be used only for the registration of the users with the WA Tool.

5. An Encryption/Decryption Service: responsible for encrypting any personal data of the user that is acquired via the application before sending it to the cloud, and also to decrypt the encrypted data received.

6. A BLE service component responsible for connecting and receiving information from sensors connected directly to the smartphone: MiBand, MiScale, environmental sensors ...

The WA Mobile application design is depicted in Figure 18, whilst Figure 19 illustrates the latest integration plan with the edge cloud and the cloud.
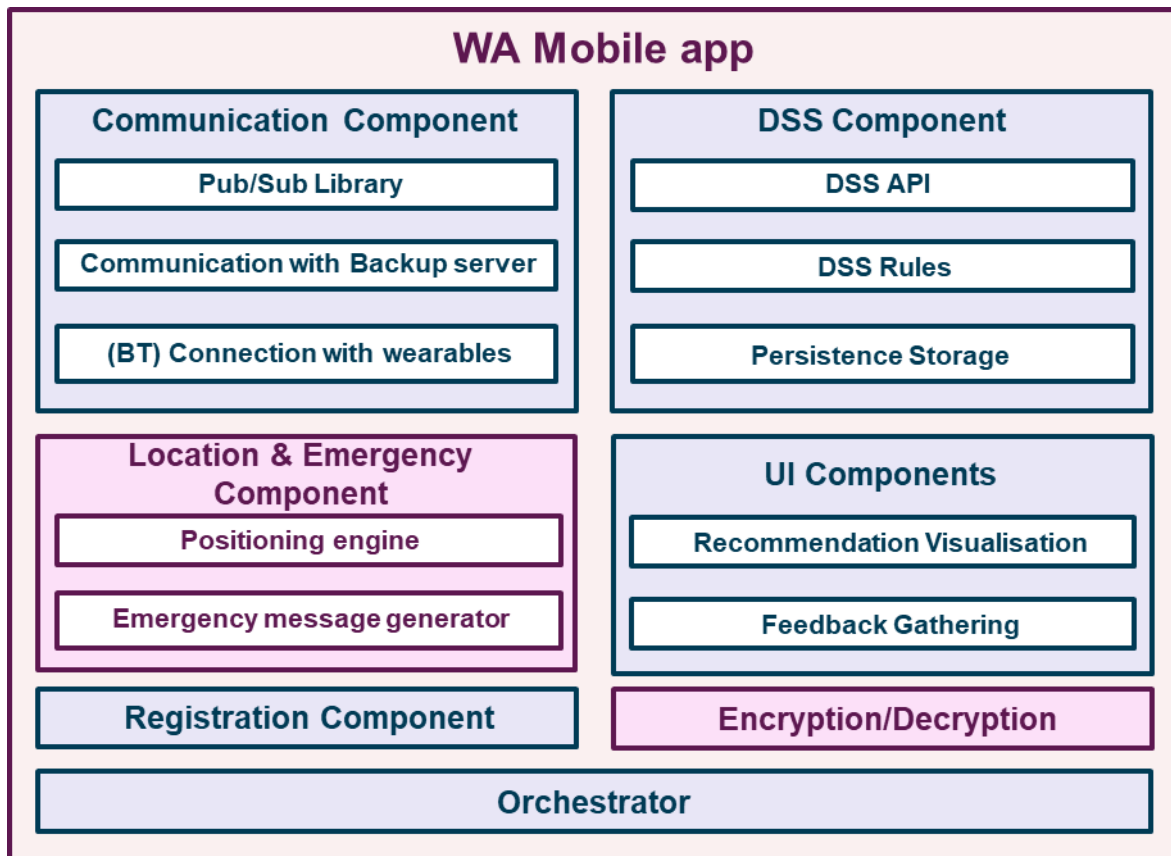

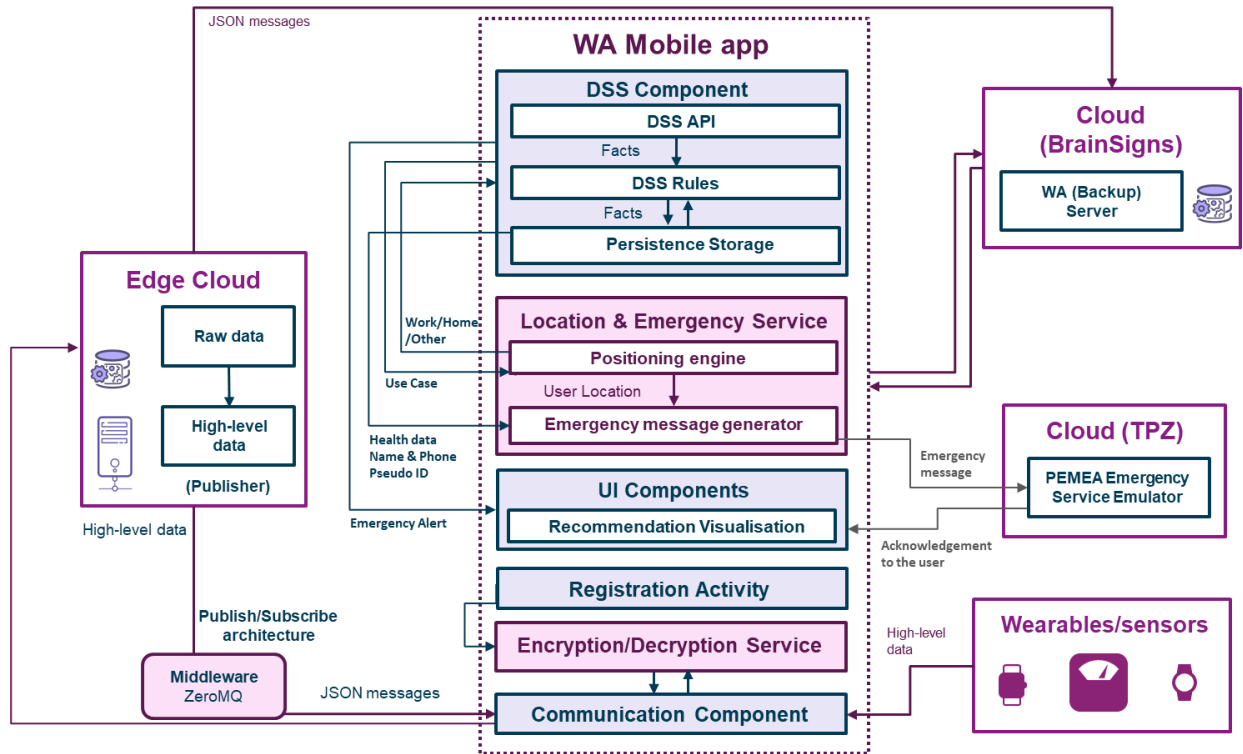*Figure 18: The Mobile app Components*

Figure 19: Mobile App Design and Integration Architecture

The UI and Registration components will be developed as 'Activities'[1], running synchronously and which can be presented to the user in one of the following ways: a) as full-screen windows, b) as floating windows (via a theme with android.R.attr#windowIsFloating set), c) as Multi-Window mode or d) embedded into other windows.

The remaining components, namely the DSS, Location & Emergency and the Encryption/Decryption services will be developed as 'Services'[2], being performed as long-running operations in the background, and not providing any user interface. These services can be called by any other application component, and they continue to run in the background even if the user switches to another application.

2.2 Sensor's Data Transmission to the Edge Cloud

In the previous section, we defined the main components of the WA mobile application and their interaction with sensors and edge cloud units. Here we will see the communications between from sensors to the edge cloud.

---

[1] https://developer.android.com/reference/kotlin/android/app/Activity

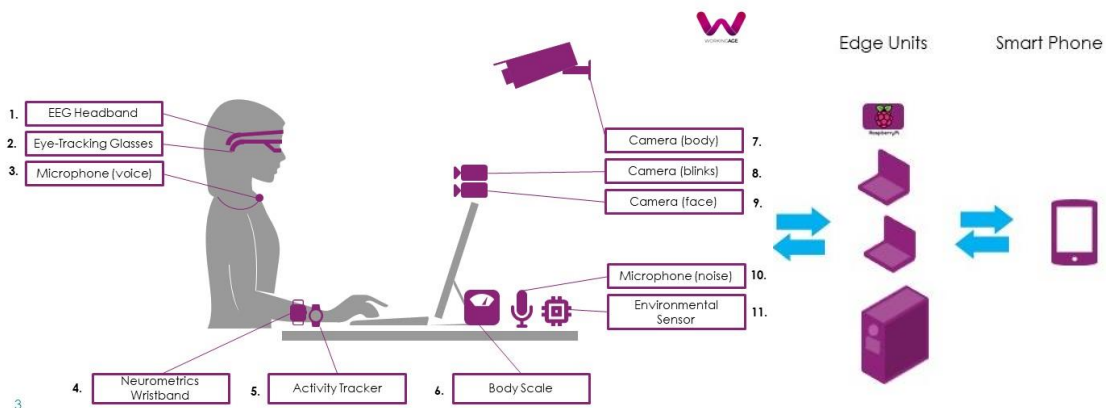[2] https://developer.android.com/guide/components/services

Figure 20: WA Sensors Communication Protocol

1. The EEG headband will connect through the BLE (Bluetooth) to the smartphone. The raw data will be sent to the Edge Cloud (Windows server) where will take place the raw data processing.

2. Eye Tracking Glasses is connected to a laptop, on which the eye tracking software and an additional strain-level application is running. The strain-level application receives the real time data stream of the eye tracker. This enables to access and evaluate the data in real time. Using the raw data, an algorithm calculates standardised strain values, and the accuracy of the measured data.

3. Microphone (voice) will connect to the Raspberry PI by means of Bluetooth. The Raspberry PI will connect to the Edge Cloud (Linux Server) via WiFi, where raw data elaboration will take place.

4. The neuromeric wristband will connect through the BLE (Bluetooth) of the Windows server of the Edge Cloud using a USB dongle[3].

5. Activity Tracker doesn't need the Edge cloud; it connects through BLE directly to the smartphone.

6. Body Scale connects directly with the Smartphone through BLE (Bluetooth)

7. Camera (body) will be connected to the Linux server by means of the WiFi network deployed.

8. Camera (eye blinks) will connect through Wi-Fi.

9. Camera (face and gesture recognition) will connect to the Linux laptop/server of the Edge Cloud via WiFi/Wired connection.

10. Microphone (noise) is connected to the Raspberry PI by means of a wire. The Raspberry PI will connect to the Smartphone via WiFi.

11. The Environmental Sensor will establish a direct connection with the Smartphone via BLE (Bluetooth Low Energy).

---

3   https://www.silabs.com/wireless/bluetooth/bluegiga-low-energy-legacy-modules/device.bled112

3 Conclusion

In this deliverable, we described in detail all the layers of the WA Tool system: the sensors, the mesh network, the edge cloud, the connexion to remote servers, the administrator tools and the WA mobile application. We also introduced the communication protocols from sensors to the WA application. We saw that the generic architecture of the IoT infrastructure will vary according the use case. The sensor set is adapted accordingly for the mobility of the user out of work and the ease to deploy at home. The number of edge computing units will also be reduced for the same reasons.

This document is the result of the reflexion performed in WP2 and of its application in WP5. The deliverable will be the base of the elaboration of the Pilot Operational Manual of WP9.