# ETSI TR 103 946 V1.1.1 (2023-10)


**Methods for Testing & Specification (MTS);**
**Security validation of IoT architecture application and conformity;**
**Case Study Experiences**

Reference
DTR/MTS-TST11Sec_IoTconf

Keywords
conformity, IoT, security, testing

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

# Contents

Intellectual Property Rights ..... 5
Foreword ..... 5
Modal verbs terminology ..... 5
1 Scope ..... 6
2 References ..... 6
2.1 Normative references ..... 6
2.2 Informative references ..... 6
3 Definition of terms, symbols and abbreviations ..... 6
3.1 Terms ..... 6
3.2 Symbols ..... 6
3.3 Abbreviations ..... 7
4 Description of a general IoT Security architecture ..... 8
5 Testing and Assurance Process for IoT Applications Using the General IoT Security Architecture ..... 8
6 Experiences with different IoT Application Domains (Case Study Samples) ..... 9
6.1 Smart Home ..... 9
6.1.1 Description and Objectives ..... 9
6.1.2 Smart Home Pilot System ..... 10
6.1.2.1 High-level Architecture ..... 10
6.1.2.2 Detailed Description ..... 12
6.1.3 Results of the Evaluation ..... 15
6.1.3.1 Setup of the Smart Home Pilot Evaluation ..... 15
6.1.3.2 Prioritized Smart Home Pilot misuse cases ..... 18
6.1.3.3 Validation results per misuse case for the Smart Home Pilot ..... 18
6.1.3.4 Conclusion for the Smart Home Pilot ..... 18
6.2 Smart Grid ..... 19
6.2.1 Prosumer Cell Pilot System ..... 19
6.2.2 Results of the Evaluation ..... 24
6.2.2.1 Setup of the Prosumer Cell Pilot Evaluation ..... 24
6.2.2.2 Prioritized Prosumer Cell pilot misuse cases ..... 25
6.2.2.3 Validation results per misuse case for the Prosumer Cell pilot ..... 25
6.2.2.4 Conclusion for the Prosumer Cell pilot ..... 25
6.3 Unmanned air systems ..... 26
6.3.1 Description and Objectives ..... 26
6.3.2 Drone Operation Pilot System ..... 26
6.3.2.1 Drone infrastructure ..... 26
6.3.2.2 Drone Pilot System Functional Overview ..... 28
6.3.3 Results of the Evaluation ..... 29
6.3.3.1 Setup of the Drone Pilot Evaluation ..... 29
6.3.3.2 Prioritized Drone pilot misuse cases ..... 31
6.3.3.3 Validation results per misuse case for the Drone pilot ..... 31
6.3.3.4 Conclusion for the Drone pilot ..... 31
6.4 Automated driving ..... 32
6.4.1 Description and Objectives ..... 32
6.4.1.1 Introduction ..... 32
6.4.1.2 Scenarios ..... 32
6.4.1.2.1 Platoon driving ..... 32
6.4.1.2.2 Platoon merging ..... 34
6.4.1.2.3 Venue ..... 36
6.4.1.3 Connected Car Infrastructure ..... 37
6.4.2 Connected Car Pilot System ..... 40
6.4.3 Results of the Evaluation ..... 40
6.4.3.1 Setup of the Connected Car Pilot Evaluation ..... 40
6.4.3.2 Prioritized Connected Car pilot misuse cases ..... 42

6.4.3.3 Validation results per misuse case for the Connected Car pilot ..... 43
6.4.3.4 Conclusion of the Connected Car pilot ..... 43
History ..... 44

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

**BLUETOOTH®** is a trademark registered and owned by Bluetooth SIG, Inc.

# Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

# Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# 1 Scope

The goal of the present document is to compile case study experiences related to the security validation and assurance for the integration and conformity of IoT applications with an existing IoT architecture in order to have a common understanding in MTS and related committees and to support trustworthiness. Industrial experiences may cover but are not restricted to the following domains: smart home, smart grid, unmanned air systems, automated driving.

# 2 References

## 2.1 Normative references

Normative references are not applicable in the present document.

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IEC 60730-1: "Automatic electrical controls - Part 1: General requirements".

[i.2] IEC 61508: "Functional safety of electrical/electronic/programmable electronic safety-related systems".

[i.3] IEC 61850: "Communication networks and systems for power utility automation".

[i.4] STANAG 4586: "Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability - AEP-84 Edition A".

[i.5] UL 991: "Tests for Safety-Related Controls Employing Solid-State Devices".

[i.6] UL 1998: "UL Standard for Safety Software in Programmable Components".

[i.7] ETSI TS 103 942: "Testing (MTS); Security Testing; IoT Security Functional Modules".

# 3 Definition of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the following terms apply:

**MODBUS:** network protocol used in the industrial manufacturing sector

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| 4G | 4th Generation (mobile networks) also known as LTE |
| 5G | 5th Generation (mobile networks) |
| AD | Attack Detection |
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| AUDRIC | AUtomated DRIving Core |
| C2 | Command and Control |
| C4I | Command, Control and Coordination Centre Infrastructure |
| CAM | Cooperative Awareness Message |
| CAN | Controller Area Network |
| CAV | Connected and Automated Vehicle |
| CERTH | CEntre for Research & Technology Hellas |
| DARIUS | Integrated Deployable SAR chain with Unmanned Systems |
| DENM | Decentralized Environmental Notification Message |
| DER | Distributed Energy Resources |
| DFD | Dataflow Diagram |
| DSRC | Dedicated Short Range Communication |
| ECU | Electronic Control Unit |
| EO/IR | Electro-Optical/Infra-Red |
| FEAM | Front-End Access Management |
| GCS | Ground Control Station |
| GGCS | Generic Ground Control Station |
| GGS | Generic Ground Station |
| GPS | Global Positioning System |
| GPU | Graphics Processing Unit |
| GSM | Global System for Mobile communication |
| ICT | Information and Communication Technology |
| ID | Identity |
| IEC | International Electrotechnical Commission |
| IMU | Inertial Measurement Unit |
| IoT | Internet of Things |
| IoTAC | Security by design IoT development and certificate framework with front-end Access Control |
| IR | Infrared |
| IT | Information Technology |
| ITI | Informatics and Telematics Institute |
| ITS | Intelligent Transportation Systems |
| JSON | JavaScript Object Notation |
| MODBUSRTU | MODBUS Remote Terminal Unit |
| MODBUSTCP | TCP-based MODBUS protocol |
| MQTT | Message Queueing Telemetry Transport |
| MTS | Methods for Testing & Specification |
| nZEB | near-Zero-Emission Building |
| OBU | On-Board Unit |
| PC | Personal Computer |
| PLC | Programmable Logic Controller |
| PMR | Personal Mobile Radio |
| PV | PhotoVoltaic |
| SAE | Society of Automotive Engineers |
| SEGOVYA-RT | SafE Generator of Vehicle trajectory using lAne information on Real-Time |
| SITL | Software-In-The-Loop |
| SME | Small and Medium Enterprise |
| STANAG | NATO Standardization Agreement |
| STRIDE | Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege |
| TCP | Tactical Command Post |
| TLS | Transport Layer Security |
| TR | Technical Report |

| | |
|---|---|
| UAV | Unmanned Aerial Vehicle (drone) |
| UDP | User Datagram Protocol |
| UI | User Interface |
| UL | Underwriters Laboratories |
| V2V | Vehicle to Vehicle |
| V2X | Vehicle to Everything |
| VPN | Virtual Private Network |
| VTOL | Vertical Take-Off and Landing |
| WC | Water Closet |
| Wi-Fi® | Wireless Fidelity |

# 4 Description of a general IoT Security architecture

Refer to [i.7], clause 4 for a description of the general IoT security architecture upon which the present document is based.

# 5 Testing and Assurance Process for IoT Applications Using the General IoT Security Architecture

Integration validation of modules is a process aimed at ensuring that the modules successfully integrate into the pilot environment and meet the required security requirements. The process involves several steps:

1) Identifying generic misuse cases relevant to the pilot (critical, high priority). These cases are grouped by processes (data collection process, storage, processing, control process, client interface).

2) Identifying pilot-specific misuse cases.

3) Identifying pilot-specific security baseline requirements addressing the generic misuse case.

4) Identifying which IoTAC modules prevent which misuse cases by implementing the security baseline requirement.

5) Checking if and how the IoTAC module is integrated into the pilot environment. To do this, the following steps are taken:

    a) Checking the architectural integration of the IoTAC modules.

    b) Checking which aspect of the security baseline requirement is implemented by the IoTAC module.

    c) Checking if the integration of the IoTAC module allows the realization of the security requirement in the context of the pilot, e.g. if the related pilot misuse case can be prevented.

The process of integrating module validation is essential in ensuring the secure integration of modules and the maintenance of the integrity and security of data and systems within the pilot environment. One of the main goals of this process is to identify and address any potential misuse cases to prevent them and guarantee the overall security of the system. To achieve this, security baseline requirements provide a set of guidelines to follow. By identifying which IoTAC modules address which misuse cases, it is possible to ensure that the appropriate measures are in place to mitigate these issues. Additionally, it is important to carefully check the integration of the IoTAC modules into the pilot environment to verify that they can effectively address the identified misuse cases and meet the security requirements.

The process of integrating module validation has two key outcomes. The first outcome is a determination of which misuse cases are covered using IoTAC modules. The second outcome is potential findings that should help the pilot's developers increase security by completely addressing their misuse cases when using the IoTAC modules.

# 6 Experiences with different IoT Application Domains (Case Study Samples)

## 6.1 Smart Home

### 6.1.1 Description and Objectives

The objective of the pilot is to validate the components and services developed by the loTAC project in the smart home application domain. The Smart House of CERTH provides an ideal environment for this purpose. In order to achieve the project's objectives, a Smart Home Pilot System over the existing infrastructure of CERTH has been defined by specifying the basic functional requirements and use-cases and identifying the most important non-functional requirements as well. A STRIDE-based threat- analysis has been executed to derive security requirements.

CERTH/ITI Smart House introduces the first house in Greece that combines enhanced construction materials and intelligent ICT solutions creating a future-proof, sustainable and active testing, validating, and evaluating environment. The house is representative of a single-family, detached residential building and is already equipped with many loT, smart home solutions that provide a lot of information about its operational characteristics. More specifically, it provides various innovative smart loT-based technologies with provided Energy, Healthcare, Big Data, Robotics and Artificial Intelligence (AI) services. The Smart House is equipped with a vast variety of sensors, actuators, smart home devices and intelligent robots. The building can operate as a microgrid by utilizing the proximity PhotoVoltaic (PV) plant and the battery unit available.

The Smart House is a single two-floor building (Figure 1). It is divided into two principal sections, the main household (living room, kitchen, bedrooms, hallways, WC, bath, etc.) and three ancillary control rooms on the left and right wings of the building. It does not have physical connection with other buildings.

(Source: IoTAC project)

**Figure 1: nZEB Smart House at CERTH/ITI's premises**

The Smart House Infrastructure provides appliances for supporting applications of highly diverse domains, as illustrated in Figure 2.

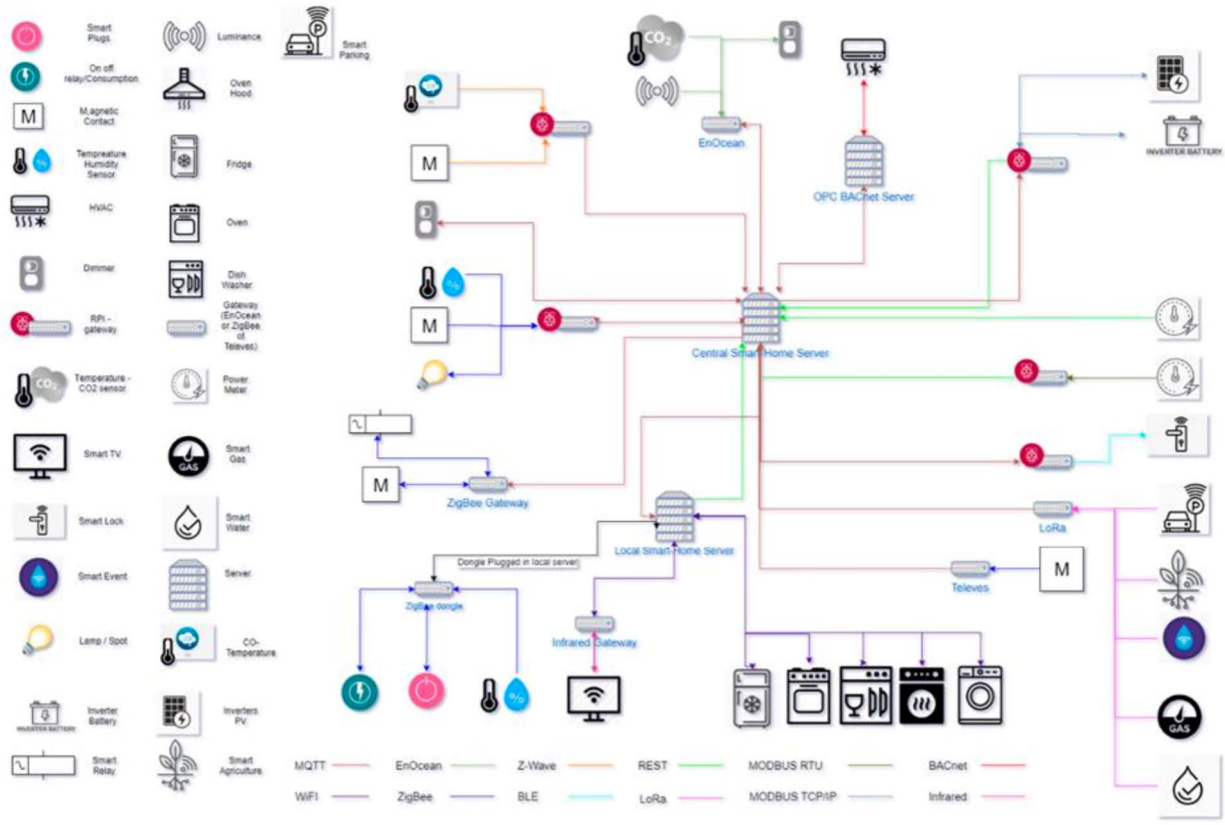



**Figure 2: Smart Home infrastructure**

Two domains that the CERTH/ITI Smart House supports, which are critical from a security viewpoint, are the Energy and Healthcare domains. Applications that belong to these domains are supported by the following infrastructure:

- Energy related equipment (e.g. smart meters, dimming and on/off actuators, environmental sensors, occupancy sensors, smart plugs, smart appliances, photovoltaics, batteries, etc.) that monitors the consumption, production and the conditions of the entire building, while automated algorithms can implement automation and/or efficiency scenarios while respecting occupant preferences.

- Health related equipment (e.g. blood pressure, glucose, oxygen levels, panic buttons, motion sensors, etc.) that monitors a variety of biometric attributes, a process that enables the extraction of valuable data (such as patterns and biometric attributes) through intelligent processing towards preventing or timely reacting to situations that could otherwise lead to harmful or even fatal outcomes.

## 6.1.2 Smart Home Pilot System

### 6.1.2.1 High-level Architecture

The Smart Home Pilot System comprises components and services related to the consumer energy and the healthcare domains. The context diagram of the system is shown in Figure 3.

The Smart Home has the ITI Smart Home Platform, which acts as a complete monitoring and control framework, just like a management system. Through the main web dashboard, the user can interact with the IoT Infrastructure of the Smart Home. More specifically, the platform provides several software applications in the form of standalone widgets, which allow the user to monitor data retrieved from different sensors through easy-to-understand visualizations, as well as to invoke actuators and activate appliances.

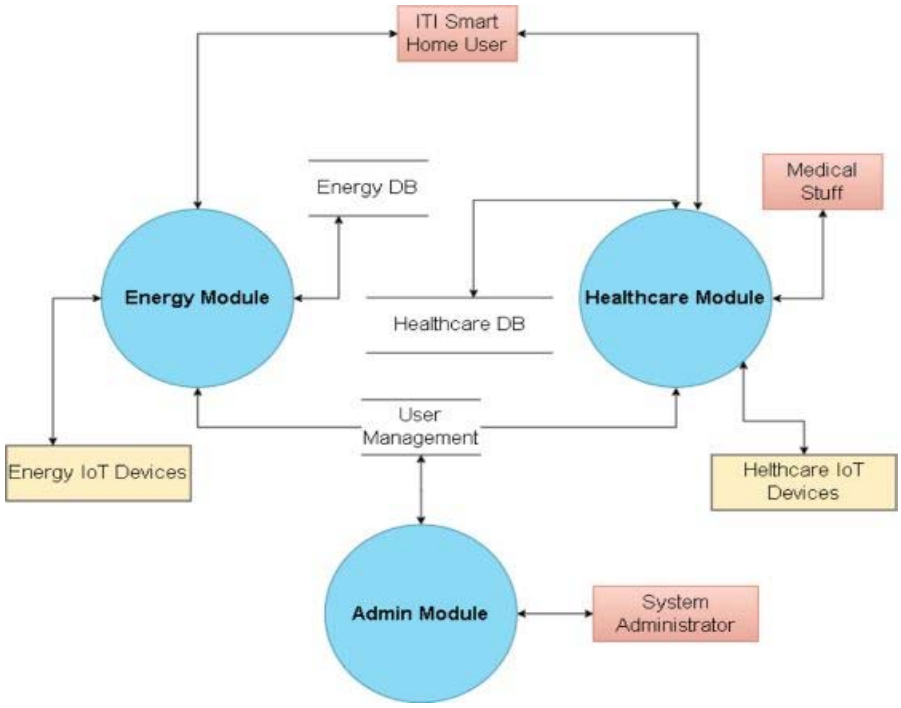



**Figure 3: ITI Smart Home Pilot System DFD Diagram (first level of decomposition)**

The main purpose of the ITI Smart Home Platform is to allow users to live in a comfortable environment while saving money by improving the energy efficiency and optimal health. This can be achieved by optimizing the day-to-day usage of the system to avoid unnecessary actions and overall to save money from their bills.

The high-level architecture of the ITI Smart Home Platform is based on the client-server approach. The User Interface (UI) consists of the web-based dashboard that allows user interaction with the underlying infrastructure. The back-end component provides the required services, data, and management of requests for the front-end functions to work. The high-level conceptual view of the CERTH ITI Smart Home Platform is shown in Figure 4.

The structure of the ITI Smart Home platform follows a centralized approach (i.e. all IoT components interact with the platform services via RESTful API interfaces). First, the data monitoring process accumulates all necessary data from sensors/actuators locally on gateways. Next, it propagates them to the respective databases (i.e. InfluxDB and MongoDB) via a dedicated RESTful API. Finally, the UI component retrieves the data to create intuitive plots and optimize the operation of the system. The API handles the data in JavaScript Object Notation (JSON) format, which is a standard and human-readable file format that is generally used for server communication. The UI of the platform is implemented with Angular, while the backend is written in Node.js.

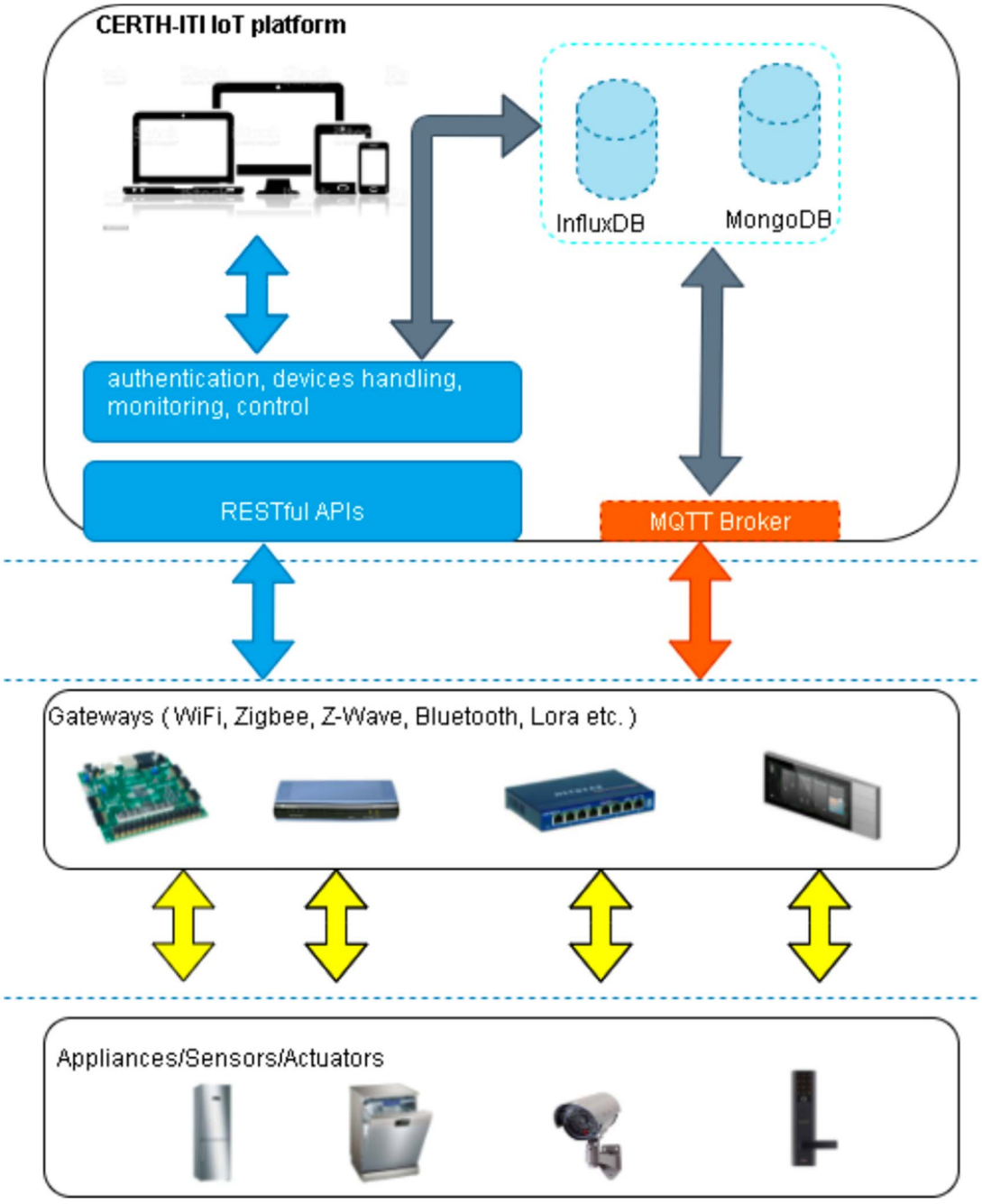
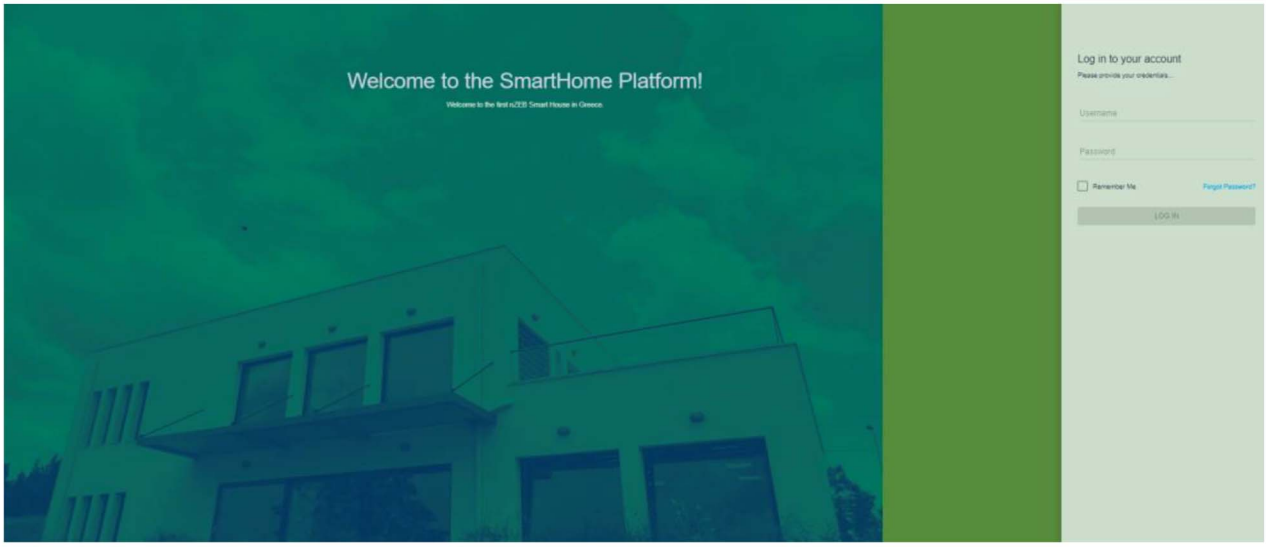



**Figure 4: ITI Smart Home Platform high-level conceptual view**

### 6.1.2.2 Detailed Description

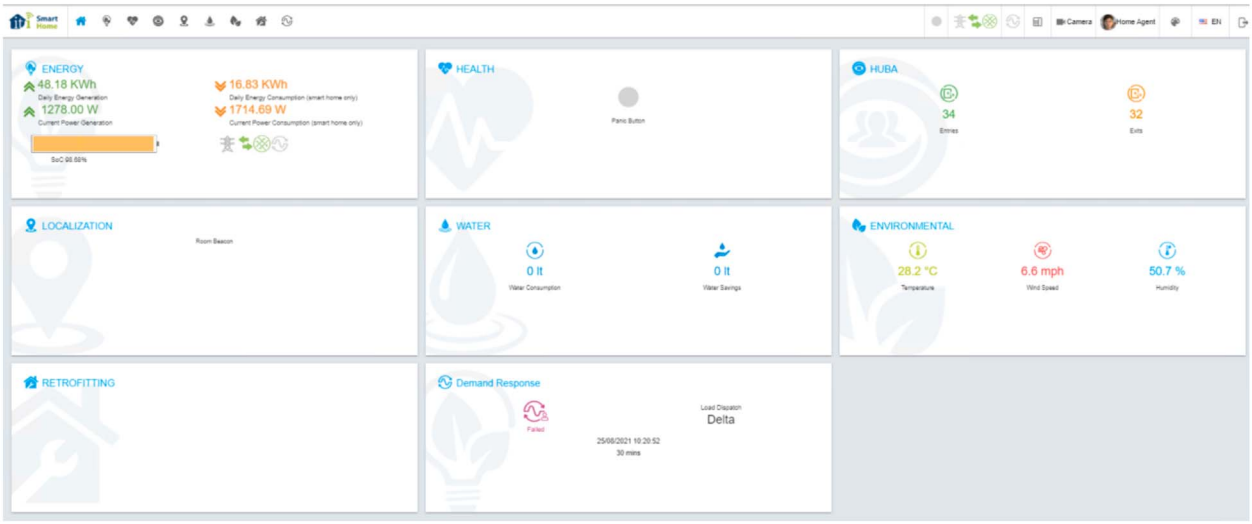
The ITI Smart Home platform requires a user authentication to ensure data security. User authentication procedure is based in several secure encryption algorithms. ITI Smart Home login page is shown in Figure 5.




(Source: IoTAC project)

**Figure 5: The ITI Smart Home platform login page**

After the mandatory login procedure, user is transferred to the ITI Smart Home Platform home page, from which user has an option to access various modules (i.e. Energy, Healthcare, Localization, Water, Environmental, Retrofitting, and Demand Response), as shown in Figure 6. As mentioned in the previous clause, for the IoTAC project Energy and Healthcare modules have been selected as the most representative ones.




(Source: IoTAC project)

**Figure 6: ITI Smart Home Platform home page**

After clicking on the Energy module, the user is transferred to the Energy panel, where he can see a summary of the various system and environment conditions. In the Microgrid tab, user can investigate various internal and external conditions as illustrated in Figure 7. On this tab, the user can monitor the building's energy consumption (Figure 8).

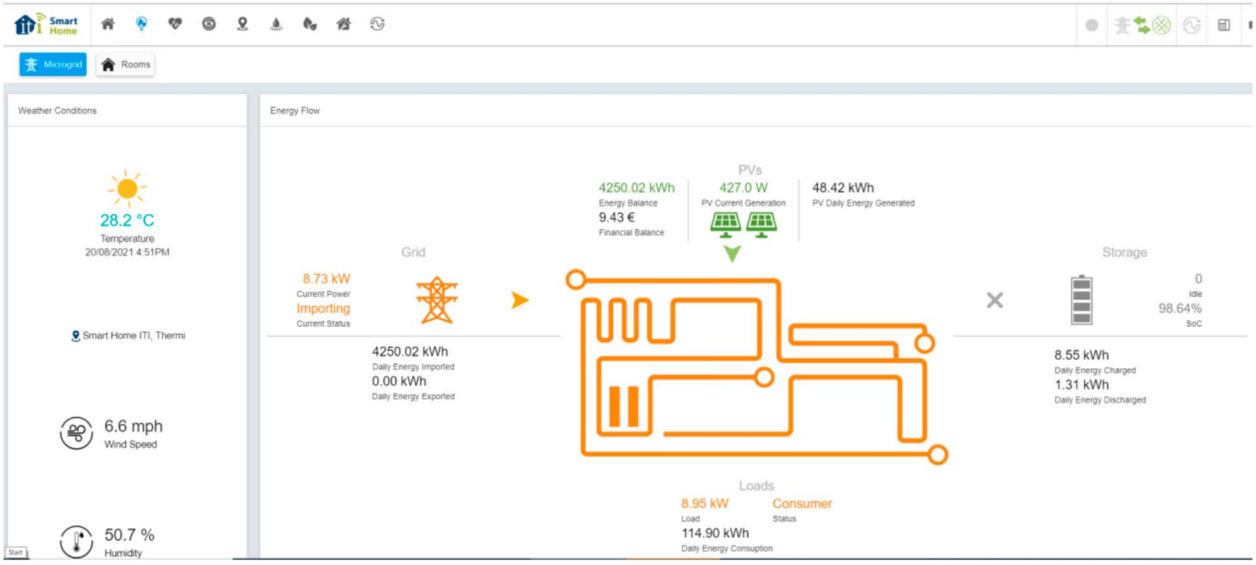



**Figure 7: Weather Conditions and Energy Flow**

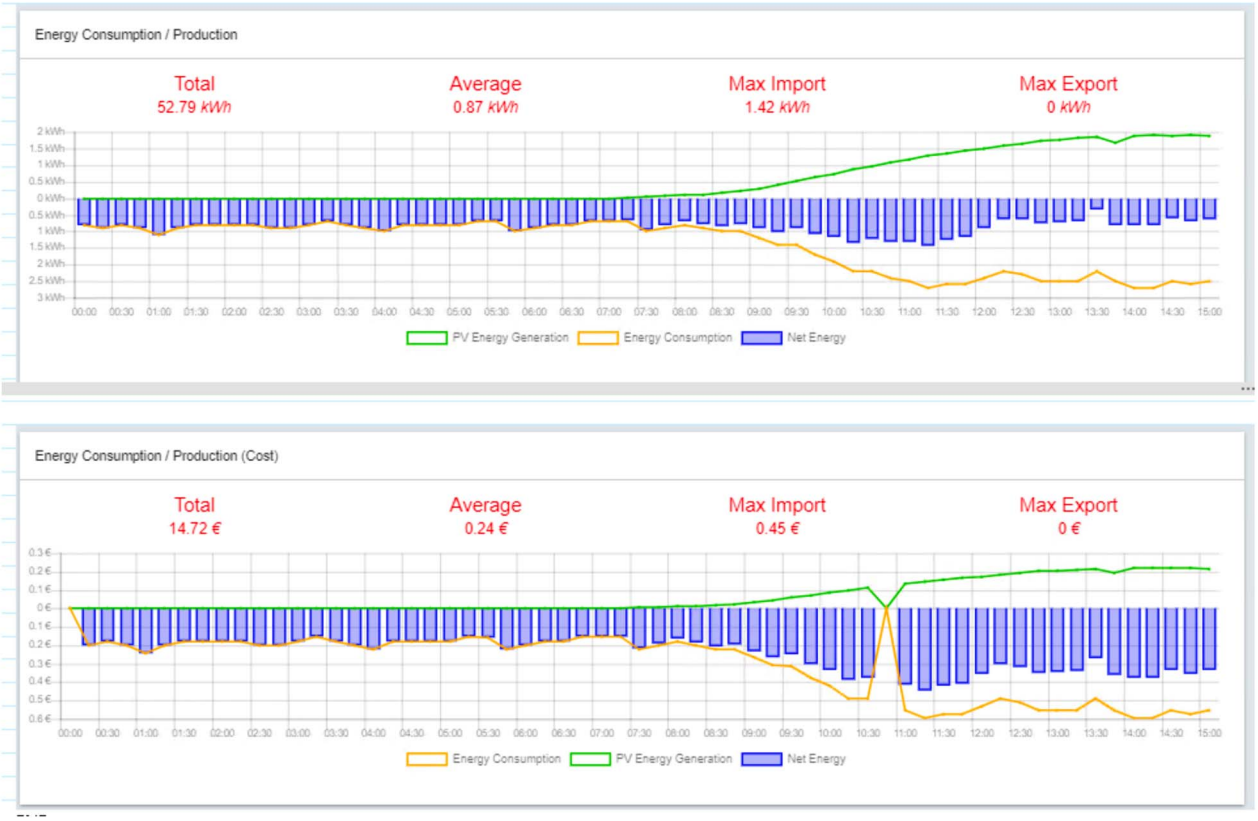



**Figure 8: Energy Consumption/Production - measurements & cost**

Besides monitoring, user has an option to invoke the following services:

- prediction (short-and long-term);
- microgrid Optimization (e.g. adaptive daily schedule, initial optimal daily schedule, daily financial balance, battery operation, etc.); and
- to monitor values of various key performance indicators (e.g. energy purchase, energy selling, reduction in overall energy demand, etc.).

After clicking on the Health module from the ITI Smart Home platform homepage, the user is transferred to the Healthcare Panel where he can see a summary of various health related parameters and conditions (Figure 9).

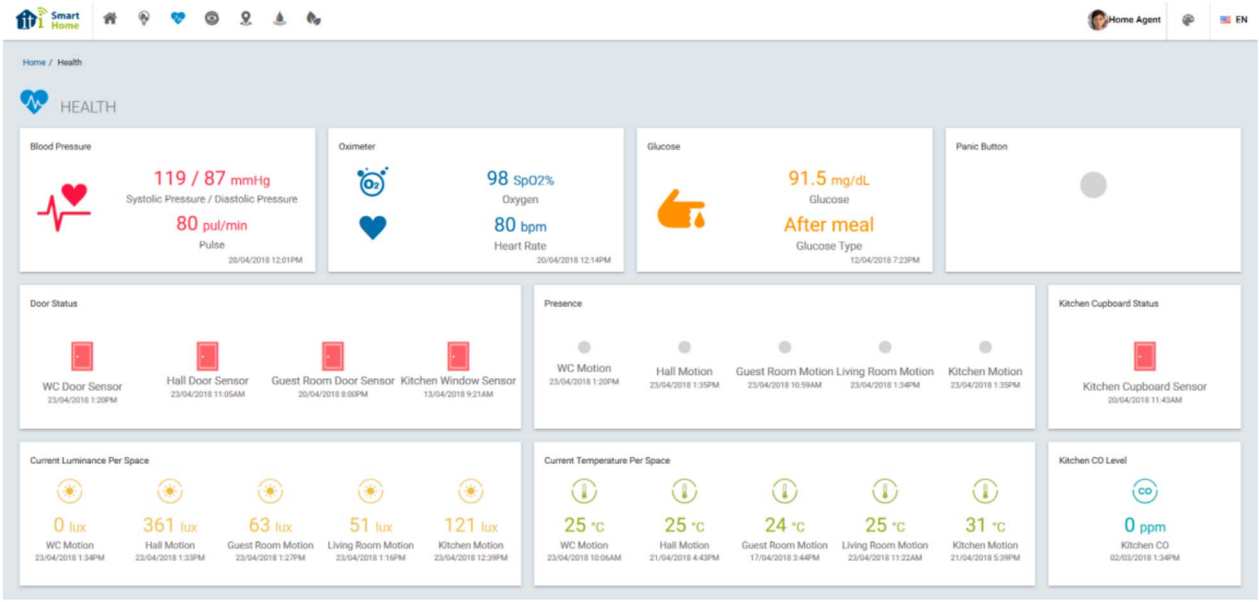



**Figure 9: ITI Smart Home Healthcare Panel**

## 6.1.3 Results of the Evaluation

### 6.1.3.1 Setup of the Smart Home Pilot Evaluation

Currently, regarding authentication and user access control on the resources of the Smart Home System, a combination of basic authentication (i.e. username and password pair) and role-based access control is used. Each user is registered and authenticated by the Smart Home System by providing a valid username and password pair. In addition, each user is assigned a role, which defines to which resources the user has access and what actions the user can perform on these resources. This scheme is considered to be adequate for some cases, but it has room for improvement.

Regarding the mechanism for reporting measurements coming from the Smart Home Assets to the Smart Home Admin, right now there is no policy established for identifying if the reported measurements are accurate or not, or more specifically, if they have been altered in a malicious way by an intruder. This has been identified as a major shortcoming since it is very important for the administrator of the Smart Home System to know that the reported measurements from the Smart Home Assets reflect the reality and that they have not been changed in any way by an attacker.

Both aforementioned security concerns can be alleviated by the deployment of IoTAC modules in the Smart Home System. More specifically, the security concern about unauthorized access to the resources of the Smart Home can be alleviated by the IoTAC FEAM (Front-End Access Management) module, which will enhance the way users are registered to the Smart Home System and how they get access to its resources. In addition, the deployment of the Attack Detection (AD) and Honeypot IoTAC modules within the Smart Home System's architecture, will introduce a mechanism for identifying the false (i.e. altered) measurements coming from the Smart Home Assets.

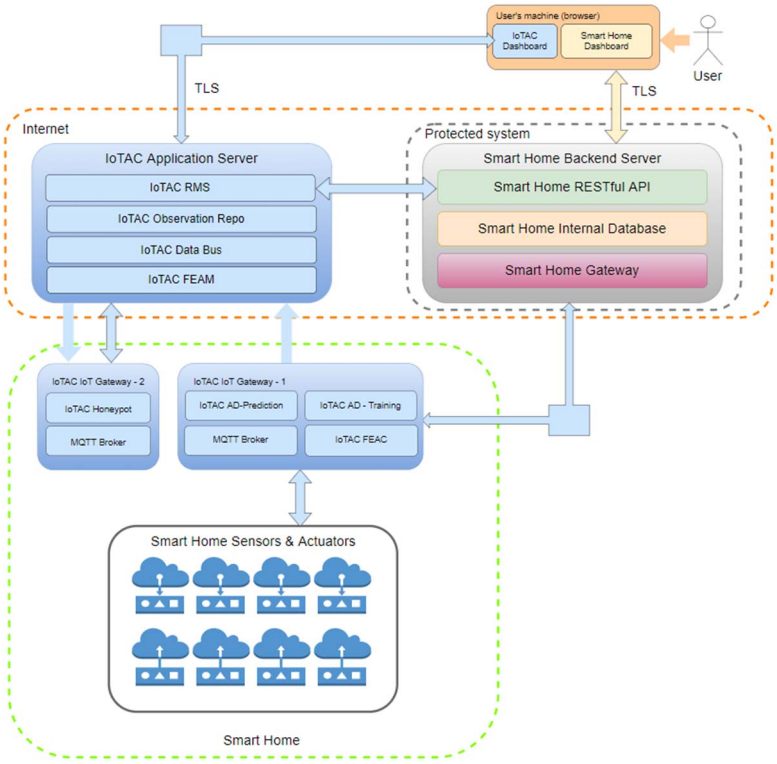



**Figure 10: Overview of the Smart Home architecture**

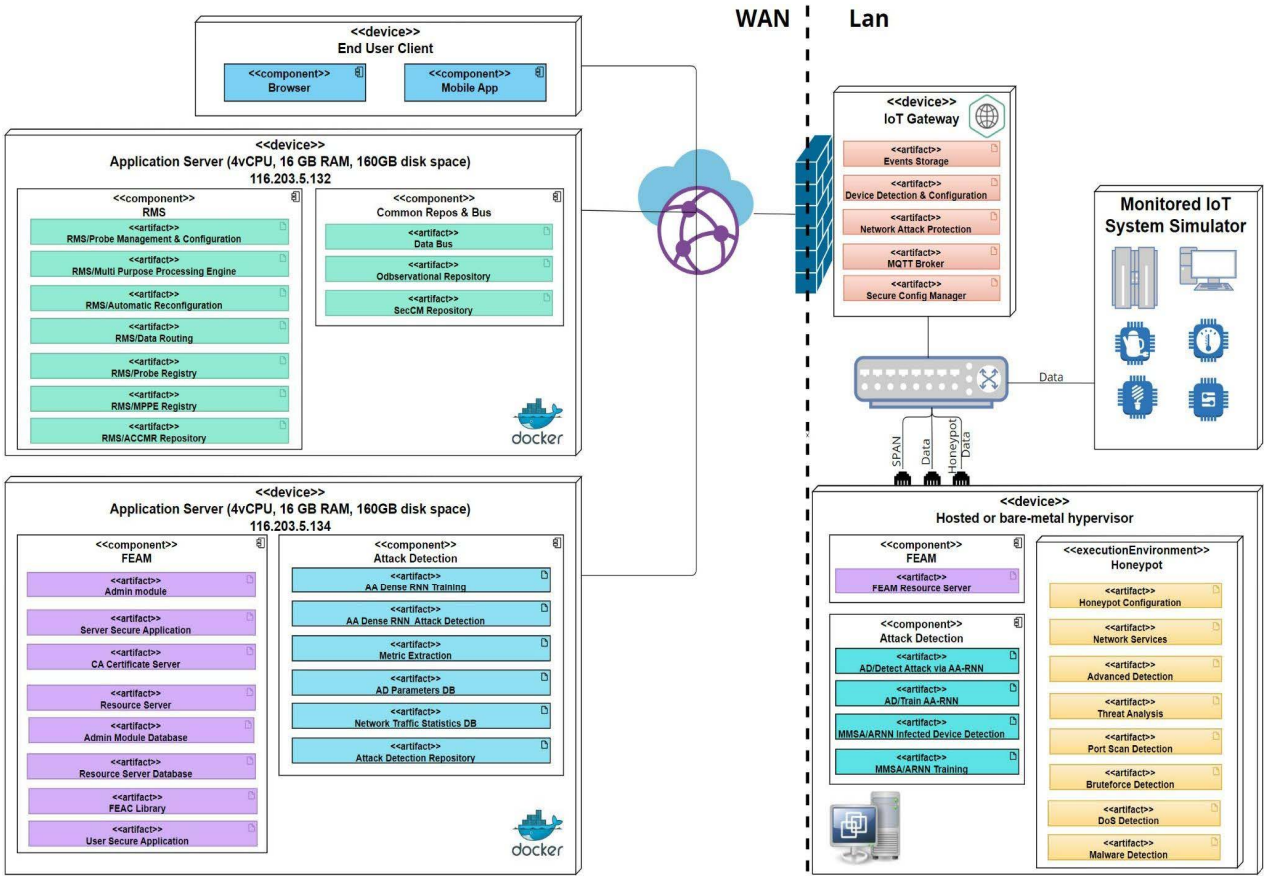



**Figure 11: A detailed overview of the logical architecture of the Smart Home Pilot**

**Table 1: Smart Home Assets**

| # | Sensor Name | Type | Description | Location | Floor | Manufacturer | Communication protocol | Can be remotely controlled | Parameter(s) |
|---|---|---|---|---|---|---|---|---|---|
| 1 | DIMM-1 | Dimmer | Measures brightness of light in a room | kitchen | 0 | Eltako Electronics | EnOcean | Y | Brightness (%) |
| 2 | DIMM-2 | Dimmer | Measures brightness of light in a room | living romm | 0 | Eltako Electronics | EnOcean | Y | Brightness (%) |
| 3 | DIMM-3 | Dimmer | Measures brightness of light in a room | guest room | 0 | Eltako Electronics | EnOcean | Y | Brightness (%) |
| 4 | DIMM-4 | Dimmer | Measures brightness of light in a room | stairs | - | Eltako Electronics | EnOcean | N | Brightness (%) |
| 5 | LUM-1 | Luminance sensor | Measures illuminance in a room | double bedroom | 1 | Eltako Electronics | EnOcean | N | Illuminance (lux) |
| 6 | LUM-2 | Luminance sensor | Measures illuminance in a room | playroom | 1 | Eltako Electronics | EnOcean | N | Illuminance (lux) |
| 7 | LUM-3 | Luminance sensor | Measures illuminance in a room | playroom | 1 | Eltako Electronics | EnOcean | N | Illuminance (lux) |
| 8 | TEM-CO2-1 | Temperature and $CO_2$ sensor | Measures temperature and $CO_2$ in a room | kitchen | 0 | Thermokon | EnOcean | N | Temperature (°C) $CO_2$ (ppm) |
| 9 | TEM-CO2-2 | Temperature and $CO_2$ sensor | Measures temperature and $CO_2$ in a room | living room | 0 | Thermokon | EnOcean | N | Temperature (°C) $CO_2$ (ppm) |
| 10 | TEM-CO2-3 | Temperature and $CO_2$ sensor | Measures temperature and $CO_2$ in a room | playroom | 1 | Thermokon | EnOcean | N | Temperature (°C) $CO_2$ (ppm) |
| 11 | TEM-HUM-1 | Temperature and humidity sensor | Measures temperature and humidity in a room | kitchen | 0 | Plugwise | Zigbee | N | Temperature (celsius) Humidity (%) |
| 12 | TEM-HUM-2 | Temperature and humidity sensor | Measures temperature and humidity in a room | living room | 0 | Plugwise | Zigbee | N | Temperature (°C) Humidity (%) |
| 13 | TEM-HUM-3 | Temperature and humidity sensor | Measures temperature and humidity in a room | guest room | 0 | Plugwise | Zigbee | N | Temperature (°C) Humidity (%) |
| 14 | TEM-HUM-4 | Temperature and humidity sensor | Measures temperature and humidity in a room | playroom | 1 | Plugwise | Zigbee | N | Temperature (°C) Humidity (%) |
| 15 | ENERGY-1 | Energy meter for Smart Home ground floor | Measures energy-related variables like power, current and voltage | whole ground floor | 0 | Gavazzi | Modbus | N | Power (W) Current (A) Voltage (V) |

(Source: IoTAC project)

#### 6.1.3.2 Prioritized Smart Home Pilot misuse cases

**Table 2: Prioritized misuse cases for the Smart Home Pilot**

| ID | Misuse case | Associated STRIDE threats | Priority |
|---|---|---|---|
| SN_EN_2 | Leaked power consumption and lighting data allows the attacker to deduce whether the occupants of the smart house are home, which is a privacy breach. | I | Medium |
| SH_EN_7 | Incorrectly controlling switches of a smart house may cause financial loss for the occupants (e.g. constant on/off commands may damage home appliances) and/or accidents (e.g. fire caused by remotely controlled oven). | S, T | High |
| SH_EN_9 | Leaked control commands allow the attacker to learn which of the publicly available billing options the occupants have chosen, which is a privacy breach. | I | Medium |
| SH_EN_11 | Incorrectly displaying power generation and/or consumption data, or price per unit data may cause occupants to mismanage their power source preferences, potentially leading to financial loss. | S, T | Medium |
| SH_EN_12 | Leaked power management configurations and/or commands set via the client interface may allow to attacker to learn e.g. absence of the occupants, which is a privacy breach. | I | Medium |

#### 6.1.3.3 Validation results per misuse case for the Smart Home Pilot

During the validation of the Smart Home Pilot an assessment of the system's architecture and security modules was conducted. The goal was to determine if the system met the necessary security requirements and was suitable for its intended use.

After conducting a document review, it was determined that the system's architecture and IoTAC modules were effective in protecting the system from potential security threats. However, during the evaluation, it was discovered that the RESTful API should be protected, MQTT should be protected (e.g. TLS) because the protocol itself does not provide any security mechanisms. In addition, the Modbus should be protected (e.g. TLS) because the protocol itself does not provide any security mechanisms as well.

It is concluded that the system's architecture is secure for its intended use, but recommendations are given to the system's operator to consider protecting the RESTful API, MQTT and Modbus as mentioned above to minimize potential security risks and to ensure the system's security level is kept high. These findings should be taken into consideration in future iterations of the system to further enhance its security.

#### 6.1.3.4 Conclusion for the Smart Home Pilot

During the validation of the Smart Home Pilot an assessment of the system's architecture and security modules was conducted. The goal was to determine if the system met the necessary security requirements and was suitable for its intended use.

After conducting a document review, it was determined that the system's architecture and IoTAC modules were effective in protecting the system from potential security threats. However, during the evaluation, it was discovered that the RESTful API should be protected, MQTT should be protected (e.g. TLS) because the protocol itself does not provide any security mechanisms. In addition, the Modbus should be protected (e.g. TLS) because the protocol itself does not provide any security mechanisms as well.

It is concluded that the system's architecture is secure for its intended use, but recommendations are given to the system's operator to consider protecting the RESTful API, MQTT and Modbus as mentioned above to minimize potential security risks and to ensure the system's security level is kept high. These findings should be taken into consideration in future iterations of the system to further enhance its security.

## 6.2 Smart Grid

### 6.2.1 Prosumer Cell Pilot System

Smart grids became important part of production and distribution of electrical energy. Their role in the safety of the service is determinative. The flat load on the grid can contribute to the optimal use of the network's capacity, which reduces the need for additional investments for extending the distribution network.

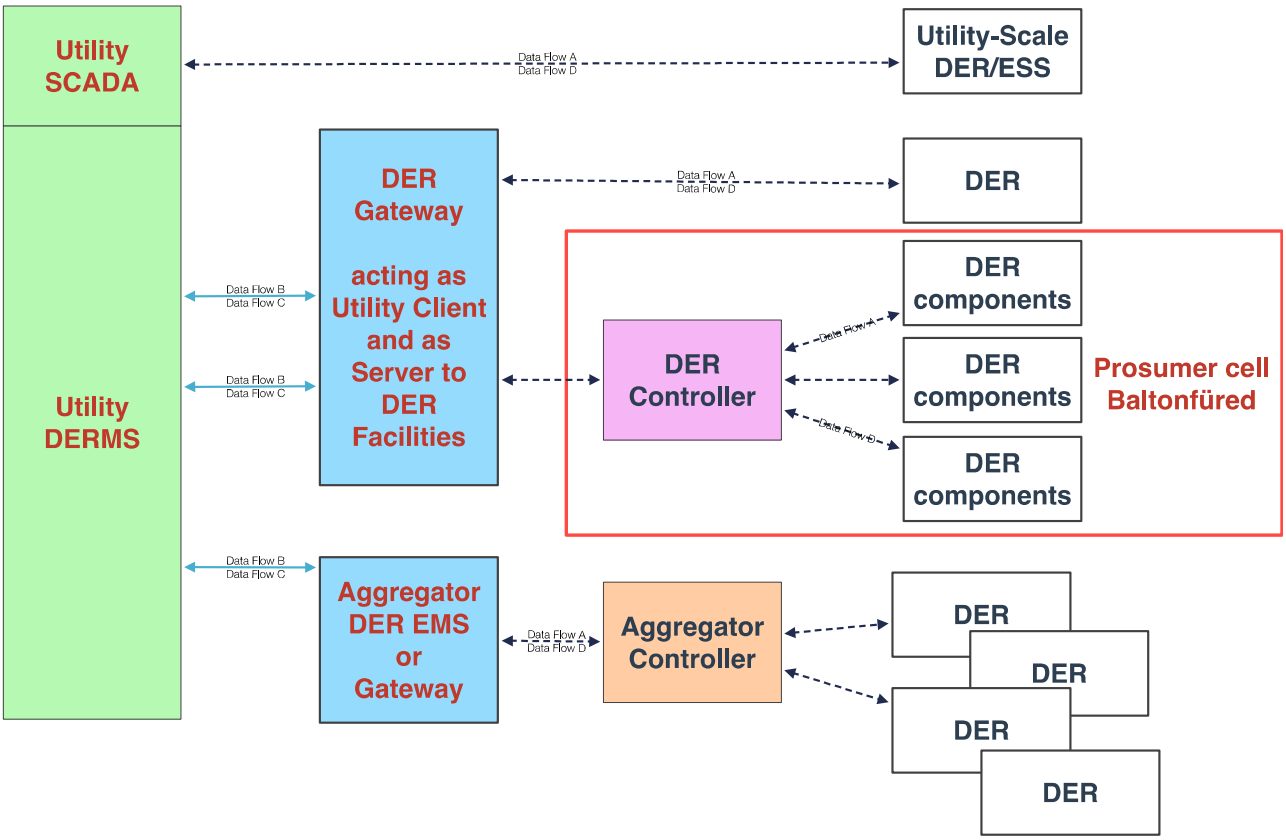
Prosumer cells are the key elements of the future smart grid. A prosumer cell is capable to behave either as producer or as customer in the grid. It usually contains small local plants (most frequently photo-voltaic modules or wind turbines), switches to change between producer consumer or off-line states, energy storage, and intelligent controller(s) with sensors and actuators.

A smart grid - as a Distributed Energy Resources (DER) system - is made up of a multitude of prosumer cells. Their activity in the grid is controlled by their user's interests. There are two main kind of users, the cell's owner and the grid operator. The cell owner and the grid operator both want to maximize their profits, but they have conflicting goals. Cell owners want to optimize the use of their own energy resources. The grid operator tries to balance the load on the grid. The coordination of their activity is based on dynamical pricing, extended with some contract-based rights for difficult or emergency situations. The cells work partly in automatic manner, partly remotely controlled by commands.

The key issue is the safe bidirectional information flow both internally between the local units of the cell and externally with the remote command interface. Commands, measured status (actual, emergency, etc.) and integrated data (long term integrated energy balance, etc.), financial information (actual price offered by the controller and by the prosumer, agreed delivery price, price for exceptional set up of energy flow direction under compulsion, etc.) are the main important components of the information flow.

The pilot will be based on a simple, single-cell experimental prosumer cell configuration installed by the manufacturer and operated by the project. The pilot's objective is to improve the security and confidence of the system by implementing the IoTAC solutions.

A relatively small, 3,5 kW peak capacity solar powered prosumer cell was constructed at the Balatonfired site. The system also has an energy storage capacity of 5 kWh. This system is connected to the local power grid. This installation will be mainly used as a development and experimental platform for DER systems, remote management of DER assets, and provide a testbed for predictive maintenance algorithms. The system will be capable to operate as part of an extended DER management system as a local DER controller with two main electric power components: the solar cell and the battery pack, according to Figure 12.




(Source: IoTAC project)

**Figure 12: DER system hierarchy**

The elements in the rectangle represent the prosumer cell under discussion. The role of Figure 12 is to show a possible hierarchical structure of a larger power grid system and the position of the cell at the bottom level of the hierarchy. Figure 12 also shows that the next obvious step for security improvement is to install a DER Gateway with security functions.

A simplified schematic of the cell is shown in Figure 13.

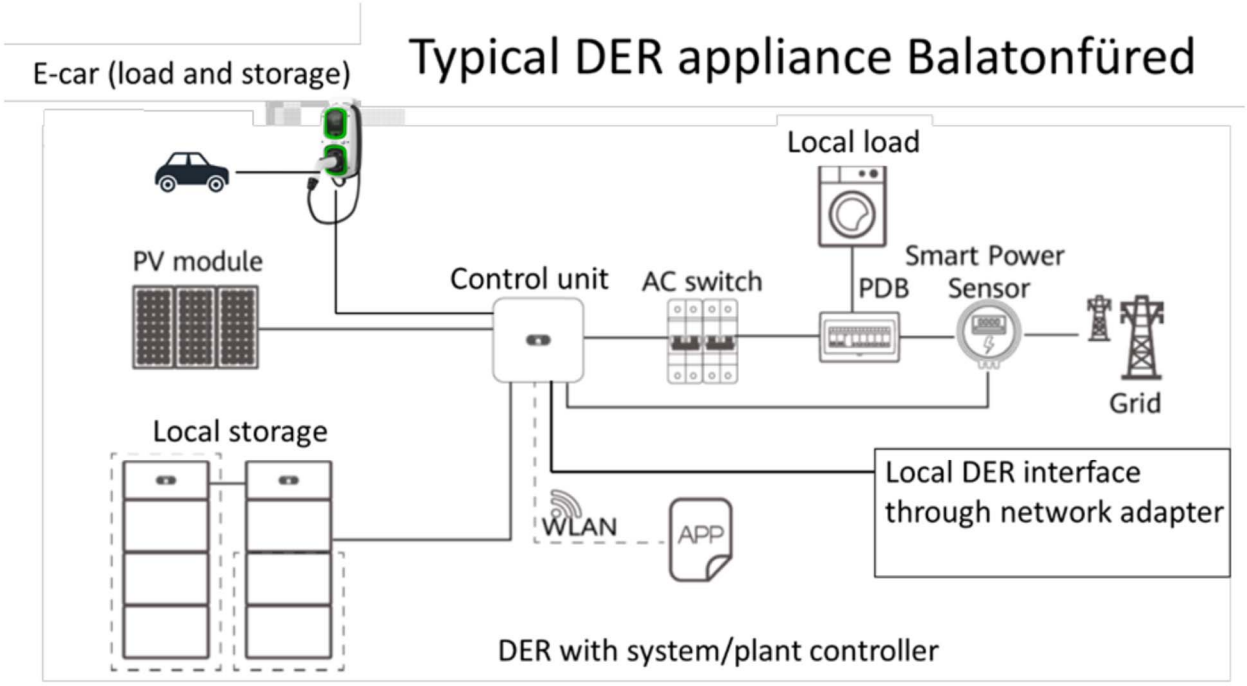



**Figure 13: Schematic of the prosumer cell**

The prosumer cell includes 9 solar panels (PV modules), a hybrid grid connected inverter, a data logger, an energy flow control device, battery back-up, an environmental monitoring unit and an e-car charger.

The control unit of the cell is an inverter combined with a Smart Logger. The battery (local storage) has a dedicated load/charge controller. Each PV module delivers the generated energy to the inverter. The e-car charge station is controlled by the cell controller. The allowed power, the time of charging, the source of the energy for charging are the most important parameters which can be adjusted by the cell's owner.

The main goal of the system is to convert energy coming from the solar panels for local consumption. If the produced energy exceeds the actual local consumption, the prosumer cell has the possibility of either storing the excess energy in the local battery or exporting it to the power grid. The decision is largely based on the cell owner's preference, however in certain situations, the cell-owner or the grid operator may prohibit exporting of energy above a certain power level (by issuing output power limitation commands).

The system works partly automatically, partly by commands given by the cell's owner or the grid operator (also called DER manager).

The energy flow direction is regulated by the smart power sensor. The local need for energy (e-car, charging of the local battery, other local load) has the highest priority. If the real-time generation of energy is not enough to serve these needs, depending on the price set-up, the generated energy will be extended by power from the battery or from the grid. If the generated energy exceeds the local need, the smart power sensors set up the energy flow towards the grid. The smart power sensor has a smart meter function too. It measures the energy flow in both directions. The accumulated values are stored with time stamps and can be queried by commands.

Communication of the internal functional units is crucial for the automatic functions. Internal connections of the components are mainly MODBUSRTU connections.

There are two main external connection links to the cell:

- Wi-Fi® through a manufacturer provided closed source application, that provides local access to data. This interface should work during the installation process. In order to improve security, the Wi-Fi® network will be disabled once setup of the cell is complete.
- Public Ethernet connection. VPN can be introduced. There is MODBUSTCP (with TLS security) communication currently implemented on the public network, but IEC 61850 [i.3] is also a requirement for remote grid Controller operation. Most of the functional units can be accessed directly also by MODBUSTCP.

The context diagram of the Prosumer Cell Pilot System is shown in Figure 14.

The system should provide at least 3 different roles with separate levels of access rights, namely, Installer, DER manager and Owner:

- The Installer is the person who sets up the system and has the highest level of access rights.
- The Owner is the person, whose interest is to operate the cell in the most efficient way from local perspective.
- The DER manager - or grid-operator - is the person (or a robot) whose interest is to operate the grid in the most efficient way from global perspective.

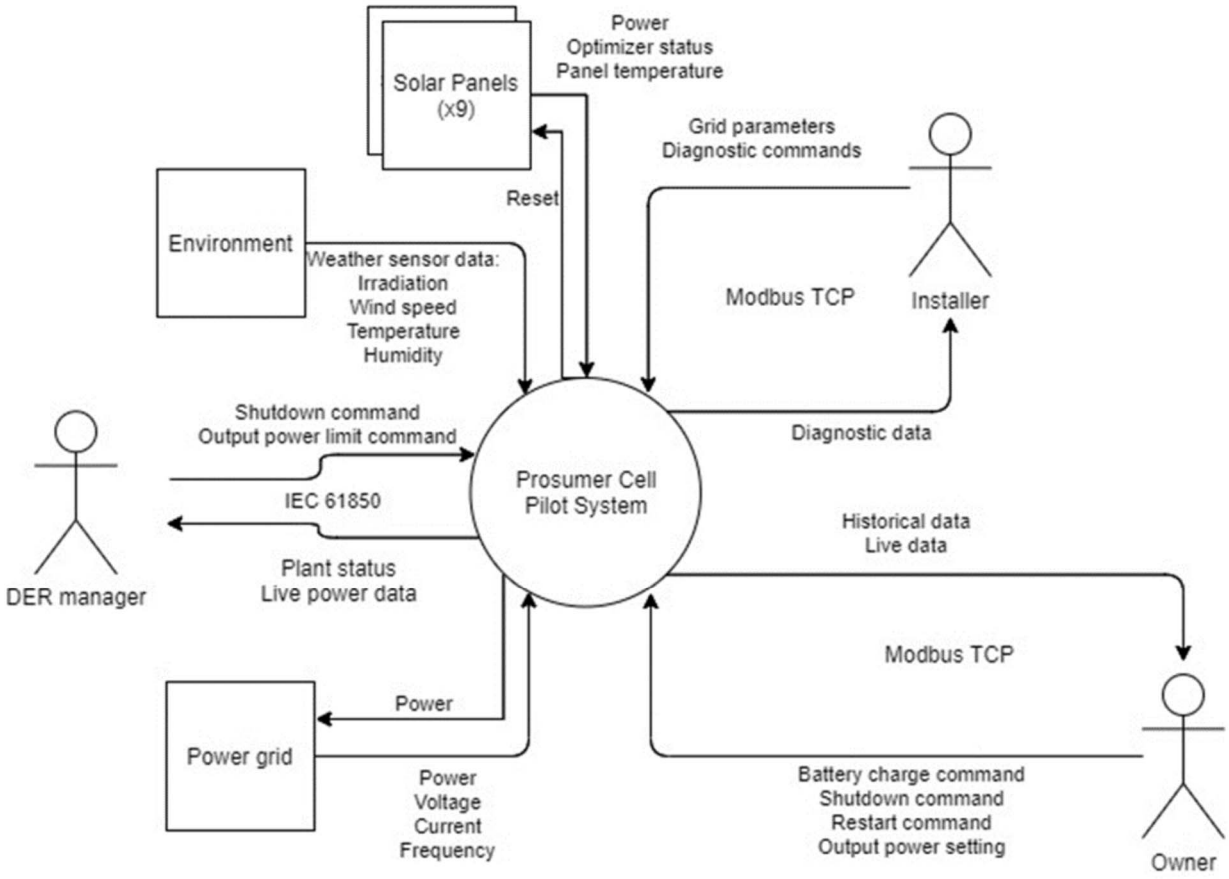



**Figure 14: Prosumer Cell Pilot System Context**

Other external connections:

- Power grid is the main physical connection for exporting or importing energy. Integrated sensors convert the actual physical parameters of the power line (voltage, frequency, current, power) to usable data format for the system.
- Solar panels (PVs) can be considered as a single external hardware unit with its own power optimizer. The unit can be reset by the system, and status information as well as panel temperature can be read.
- Environment is also monitored using different sensors like temperature, humidity, wind-speed, irradiation. These sensors are built in devices of the cell.

The component diagram of the cell is shown in Figure 15. Only the logical interfaces are represented, the physical electrical connections are only implied where they also serve as data sources (e.g. power measurement and power-line based communication).

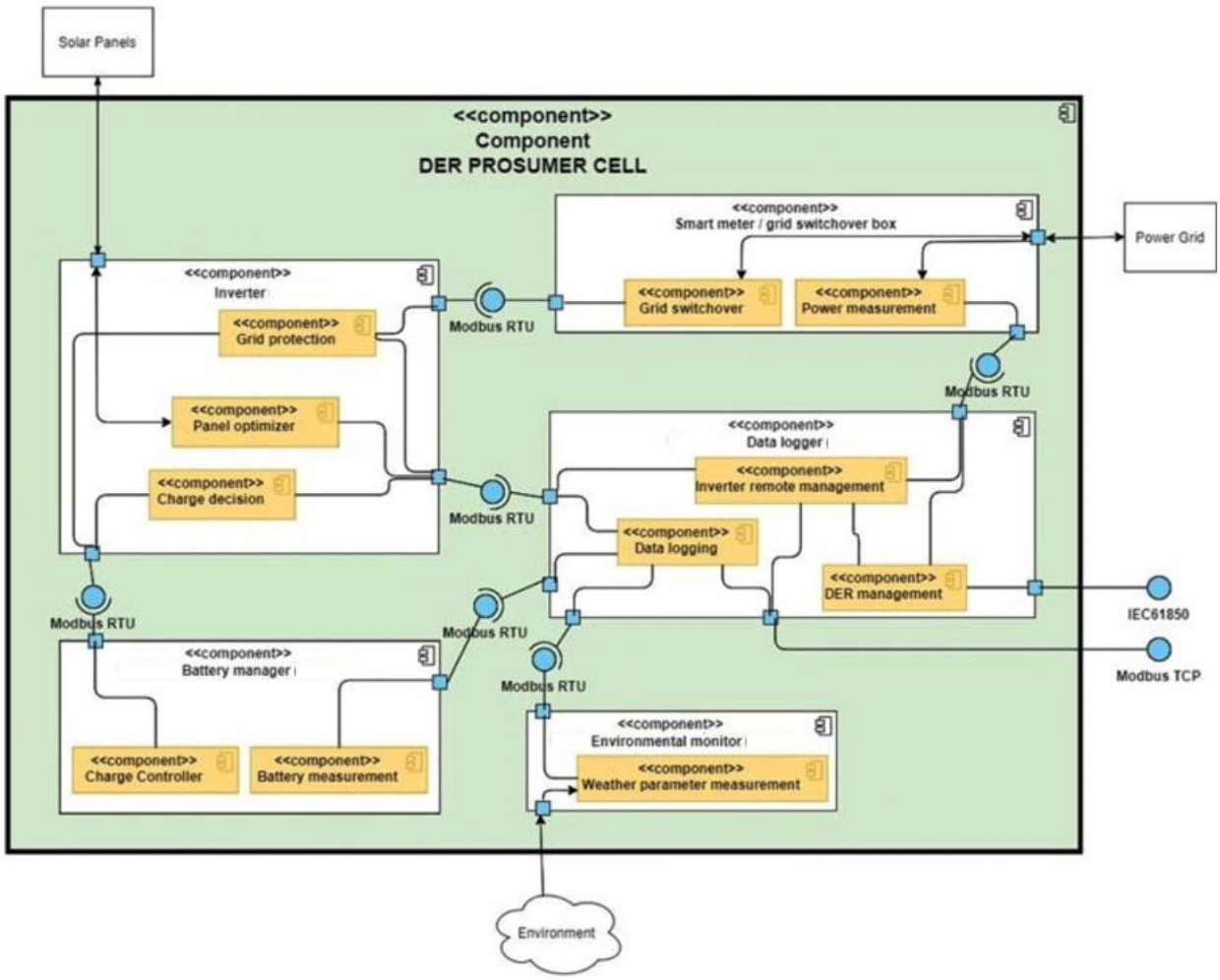



**Figure 15: Component diagram of the prosumer cell**

The control logic of the cell (built into the inverter) is realized as highly reliable software according to functional safety standards (e.g. UL 991 [i.5], UL 1998 [i.6], IEC 60730-1 [i.1] and IEC 61508 [i.2]). It controls the energy-flow directing energy in excess of current consumption to the battery or to the grid depending on the parameters set from the external interface. The data logger part of the system contains a history (for several months) of all relevant parameters and some weather-related data (irradiance, temperatures of solar panels, ambient temperature). Such history is useful e.g. for predictive maintenance purposes. This data history can also be remotely downloaded from the system.

The DER prosumer cell - as is - is a fixed component of the system, it is not subject of development. Any essential change, hardware or software upgrade can be executed only by the manufacturer. Two kinds of interfaces are available for other system components, an IEC 61850 [i.3] interface, and a MODBUS TCP interface.

The prosumer cell itself has no built in security functions. Anybody who connects to the interface can access to the whole functionality of the cell (except for the built-in safety functions). User management, authentication and the user-friendly access to the cell's functionality are presently provided by a closed secure application delivered by the manufacturer. However, the cell and this application is hardwired to the manufacturer's server and data exchange is not under the control of the cell's owner. That is the reason why a development for security improvement has been decided. The goal of the development is to replace the manufacturer's application with our own security functions (like gateway, user management, access control, secure communication, real-time protection etc.) and necessarily with our own user interfaces.

### 6.2.2 Results of the Evaluation

#### 6.2.2.1 Setup of the Prosumer Cell Pilot Evaluation

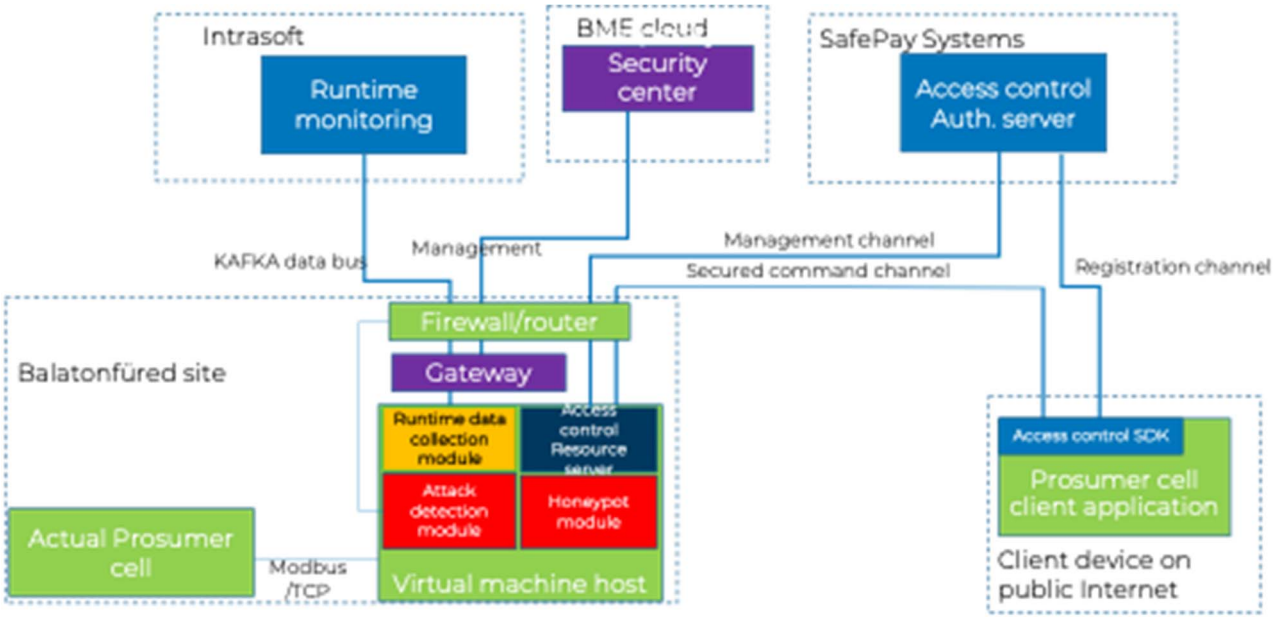



**Figure 16: Architecture of the Prosumer Cell pilot with the integrated IoTAC modules**

Pilot in the current state follows the physical and logical architecture described in Figure 16. All the modules will be included, and they already have their dedicated places, however most modules are still in the integration phase.

All physical communication is on Ethernet. The local firewall/router is only allowing the specified ports through. For the access control purposes, a dedicated port is forwarded to the access control Resource server (this is currently TCP port 12 050). Since the secure gateway cannot currently do the port forwarding, it is bypassed by the firewall. This may be mitigated in a later version. All other connections are initiated from the protected system, therefore no other ports are needed to be forwarded. The attack detection module needs a copy of all Ethernet traffic, this is done by a dedicated sniffing port on the built-in switch, and a separate Ethernet interface of the Virtual Machine host PC, which is only connected to the specific virtual machine that is to run the Attack Detection module.

Some special, battery safety related vulnerabilities are not handled by any IoTAC module, instead, they are mitigated by safety mechanisms implemented in a component of the actual prosumer cell itself (i.e. battery charger and/or inverter). Generally, the spoofing and tampering style vulnerabilities that are related to data integrity are to be handled by the Runtime Data Monitoring module as it has access to all specific data and can find and report spikes and other abnormalities of the values. Spoofing, tampering and repudiation style vulnerabilities that relate to wrong or unauthorized commands are rather handled by the Front-End Access Management module, where certain users will not have access to certain commands, or only have access to a limited time for certain commands.

#### 6.2.2.2 Prioritized Prosumer Cell pilot misuse cases

**Table 3: Prioritized misuse cases for the Prosumer Cell pilot**

| ID | Misuse case | Associated STRIDE threats | Priority |
|---|---|---|---|
| CELL_17 | Incorrectly processing energy flow data skews the operator's perception of the state of the grid, potentially causing the operator to mismanage the grid, leading to blackouts. | T | High |
| CELL_21 | Not processing energy flow data may cause the grid to be mismanaged, leading to blackouts. | D | High |
| CELL_25 | Incorrectly controlling loads at cells (e.g. on/off command for many loads at once) may put much strain on the grid, potentially leading to blackouts. | S, T | High |
| CELL_30 | Incorrectly displaying energy flow data to the grid operator may prompt the operator to mismanage the grid, potentially leading to blackouts. | S, T | High |
| CELL_41 | In case of e-car fleet charging in the prosumer cell (typical case of public transport companies) the attacker can prevent the night, charging and block the service for the next day. | S,T,D | High |
| CELL_43 | The cell owner or the grid operator may deny changing certain special parameters that should only be changed during commissioning and not in actual operation. | R | High |

#### 6.2.2.3 Validation results per misuse case for the Prosumer Cell pilot

During the validation of the Prosumer Cell pilot, an assessment of the system's architecture and IoTAC modules was conducted. The goal was to determine if the system was secure for its intended use.

After conducting a document review, it was determined that the system's architecture and IoTAC modules were effective in protecting the system from potential security threats. However, during the evaluation, it was discovered that although the used Modbus-TCP protocol was inside a protected area, it should be considered to implement security mechanisms of underlying protocols, such as TLS, as the Modbus-TCP protocol does not provide any security mechanisms. Additionally, it was found that KAFKA data bus Authentication/Authorization and encryption were not applied in the current stage, although it should be done in a production environment.

It is concluded that the system's architecture is secure enough for its intended use, but recommendations are given to the system's operator to consider implementing security mechanisms of underlying protocols and applying KAFKA data bus Authentication/Authorization and encryption in the production environment. It should be noted that these are areas for improvement to ensure the system's security level is kept high and to minimize potential security risks.

#### 6.2.2.4 Conclusion for the Prosumer Cell pilot

During the validation of the Prosumer Cell pilot, an assessment of the system's architecture and IoTAC modules was conducted. The goal was to determine if the system was secure for its intended use.

After conducting a document review, it was determined that the system's architecture and IoTAC modules were effective in protecting the system from potential security threats. However, during the evaluation, it was discovered that although the used Modbus-TCP protocol was inside a protected area, it should be considered to implement security mechanisms of underlying protocols, such as TLS, as the Modbus-TCP protocol does not provide any security mechanisms. Additionally, it was found that KAFKA data bus Authentication/Authorization and encryption were not applied in the current stage, although it should be done in a production environment.

It is concluded that the system's architecture is secure enough for its intended use, but recommendations are given to the system's operator to consider implementing security mechanisms of underlying protocols and applying KAFKA data bus Authentication/Authorization and encryption in the production environment. It should be noted that these are areas for improvement to ensure the system's security level is kept high and to minimize potential security risks.

# 6.3 Unmanned air systems

## 6.3.1 Description and Objectives

The drone pilot is operated by an European Defence and Space company, specifically by the "System House" Business Unit within this group. As such, the company is in charge of designing and developing integrated systems for their customers. These large systems integrate products and systems from the group (including airborne and space-borne platforms) and from a large panel of associated partners, including numerous SMEs.

The company also provides fully integrated modular solutions and services in order to minimize risk exposure in the areas of surveillance, Border Security, population protection, infrastructure security and responses to emergencies. They are currently developing large integrated systems for border security (blue and green borders) in Europe and all around the world. The general concept of these integrations is to integrate all the sensing platforms into one generic ground control station so as to benefit from possible collaborations between all platforms when it makes sense.

## 6.3.2 Drone Operation Pilot System

### 6.3.2.1 Drone infrastructure

The system considered in the pilot encompasses the following segments (see icons in Figure 17):

- The C4l (Command, Control and Coordination Centre Infrastructure) segment (grey): this segment consists of the Command and Control (C2) systems. The C4I segment is implemented in:
  - The Coordination Centre: a fixed control room with computers, displays and access to the infrastructure communication networks. This is the planning level of the Command and Control system.
  - The Tactical Command Post (TCP) which consists of a mobile or deployable structure (truck, shelter, tents, etc.) that is equipped with computers where the tactical functions of the C4I are implemented (i.e. tasking and current operations monitoring). The TCP can access the infrastructure communications and the wireless tactical communications. It can be composed of several elements (each agency can have its own command post that will be coordinated by the main tactical command post) and several mobile forward command posts (in trucks, cars, helicopters, planes) that operate under the control of the main command post. The TCP is in permanent communication with the C2 and information systems deployed by different agencies.
  - The execution level is equipped with terminals (laptops, PMR, etc.) that enable them to report to the C4I (tactical level).
- The Communication segment (arrows): which is generally a heterogeneous segment that groups:
  - Infrastructure communication segment (fixed + mobile) that generally supports the exchanges between coordination level and tactical level and can also be used at tactical and execution level.
  - Tactical data links (Ground-Air-Ground): wireless segment between the C4I and the unmanned systems. For the control of unmanned systems, the Tactical Data Link links generally the Ground Control Station (GCS) to the air, ground or maritime platforms. This is the uplink to control the platforms and their sensors, and the downlink to transmit the data gathered by the unmanned platforms to the GCS.
  - The wireless bubble: an ad-hoc deployable communication network set-up to provide the deployed systems and units with the necessary communication means, in areas where no network is available or where the available networks cannot guarantee the necessary availability and confidentiality.
- The Ground Control Station (GCS) segment (yellow and pink): this segment is composed of:
  - The Generic Ground Station (GGS) that will have capability of tasking any of the unmanned systems and exploiting all the data received. This is a concept supporting technical and operational interoperability as well as a real component developed within DARIUS.

- The specific Ground Control Station (GCS) associated to each unmanned system integrated to DARIUS. Each GCS is composed of 2 parts: the control module (to control the platform and the sensors) and the exploitation module (data management) to exploit the data, display them and exchange them with the C4I segment.

- The platforms are the unmanned vehicles, their navigation and communication systems and the payloads (sensors and others):
  - Unmanned Air Vehicles.
  - Ground Robots.
  - Maritime Platforms.
  - Underwater Platform: Underwater unmanned vehicle.
- The sensors (part of the platforms): typically, GSM localization module, video and IR sensors on board of ground and aerial platforms.

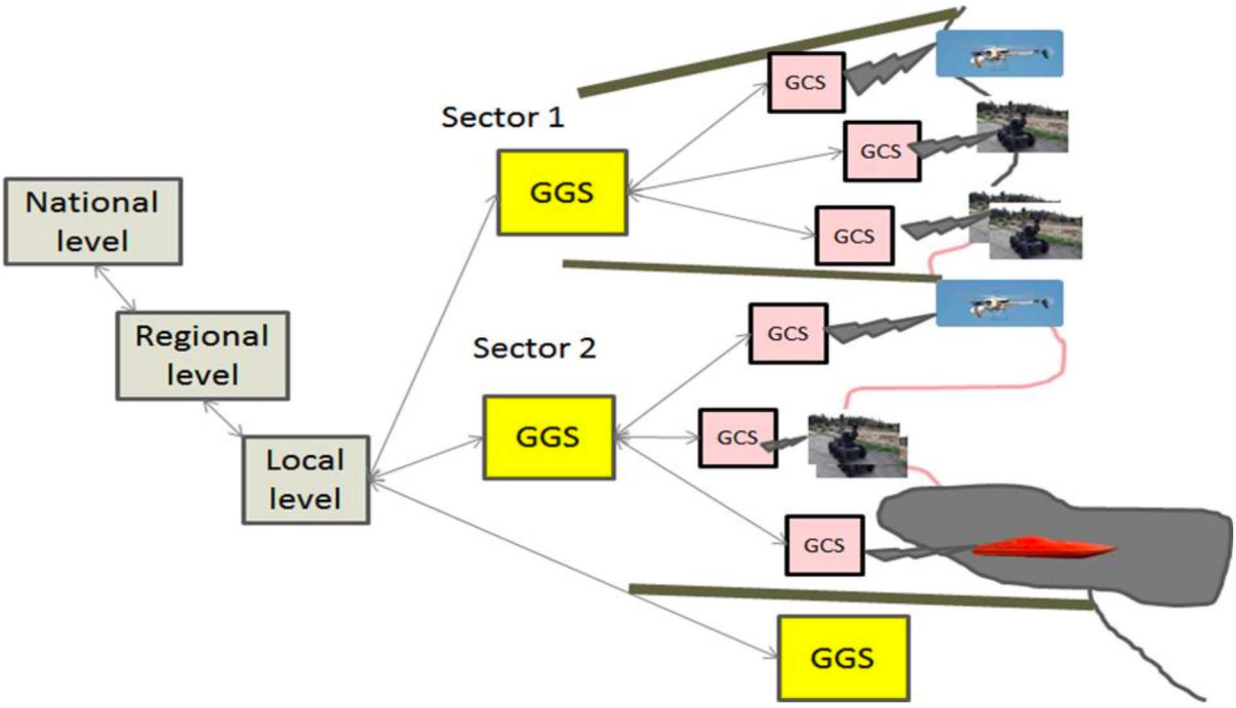



**Figure 17: Overview of the Drone Pilot infrastructure**

#### 6.3.2.2 Drone Pilot System Functional Overview

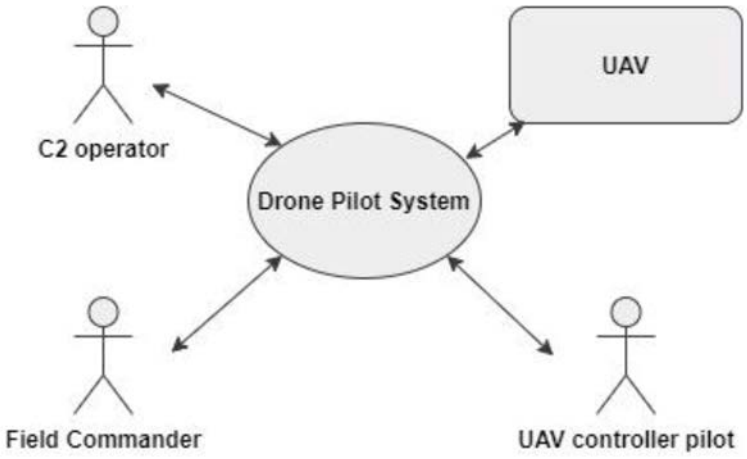



**Figure 18: Drone Pilot System Context**

The Drone Pilot System is used by border guards to monitor the border. There is a sectorial centre in charge of one portion of the border, equipped with a C2 system. The centre uses field patrols (border guards) with vehicles and/or walking. Several types of UAVs are used to help the border guards to detect humans or vehicles. Some of the UAVs are medium/long range (fixed wings) and are managed directly by the sectorial centre and others are short range (VTOLs) and are managed by the commanders in the field. Some Specific Ground Control Stations (GCSs) are therefore deployed in the field and are sometimes left unattended.

The major threats faced by the system are:

- External people taking control of the GCSs and misusing the UAVs or destroying them.
- External people taking the control of UAVs through their data links (jamming the existing data link and/or using a more powerful emitter).
- Cyber-attack against the sectorial centre.

The pilot is therefore to demonstrate how IoTAC solutions can respond to these kinds of threats. Human participants in the pilot are:

- C2 operators at sectorial centre operating the C2 and the GGS.
- Field Commanders (patrols) that operate small UAVs directly through the GCSs.
- Pilots of the UAVs.

Major behavioural scenarios:

- Operators are monitoring the UAVs missions through the respective data links (upstream and downstream). The data links are based on Wi-Fi® technology and respect the STANAG 4586 [i.4].
- Most of the UAV missions are automatic. The data link is used for safety or mission retasking. If the link is lost, there are safety protocols: the UAV takes a hippodrome pattern and waits for the data link to be re-established or (when it is too long most of the time) automatically returns to base.
- The pilots operate the GCS, and the mission controllers monitor the mission and re-task where necessary.

Major communication channels:

- Specific data link grouping uplink and downlink, based on Wi-Fi® technology. The uplink sends piloting data and sensor management orders. The downlink sends to the GCS the sensors data (video flows, pictures for the EO/IR cameras).
- There is a protocol (message formats) defined between GGS and GCSs. The communication is general wireless and depends on the radio coverage. Satcom can be used.

- The data link is very directive and there is no broadcast, so the interception from a third party is unlikely. But it has to be improved.

Valuable assets:

- C2 system.
- Sensor's data (so that malevolent people cannot know what the UAV can see).
- UAV.

The functional architecture is shown in Figure 19.

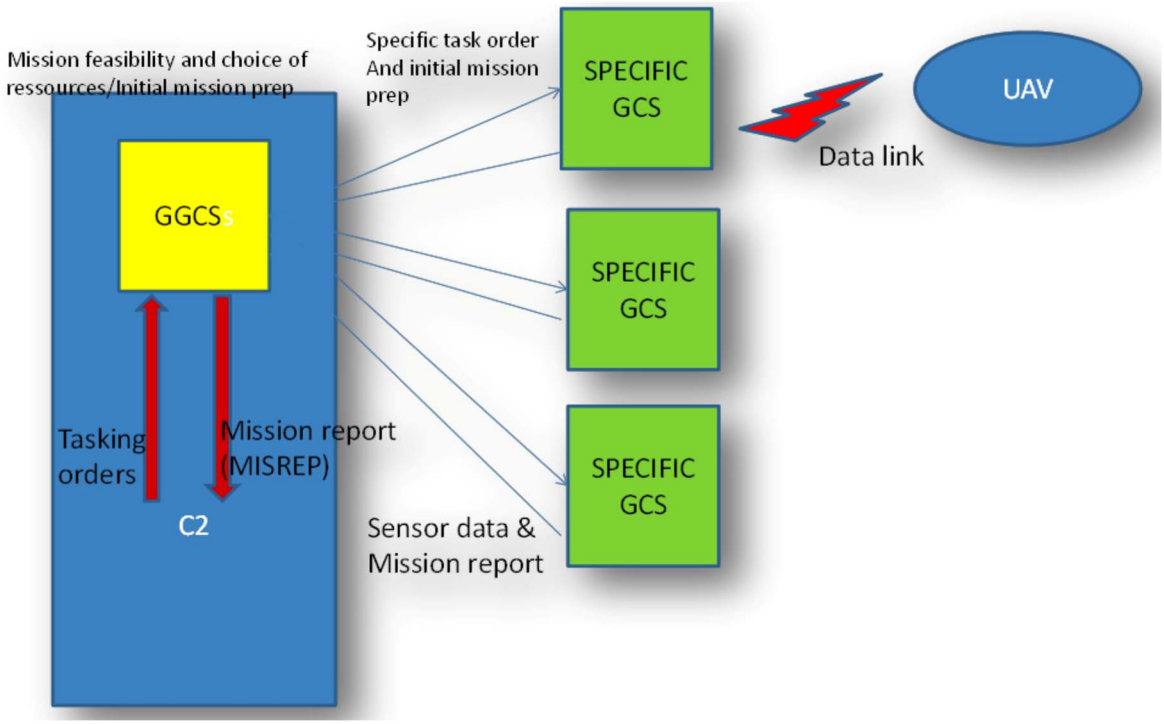



**Figure 19: The functional architecture of the Drone Pilot System**

The main components of the system are:

- The Command and Control system - C2 (or information management system in civilian systems) - that is connected to the UAVs (drone systems) through a unique interface: the Generic Ground Control Station (GGCS). Based on standard IT components.
- The Specific Ground Control Stations (GCSs) that are interfaced with the drone via a specific data link (uplink and downlink). This data link is based on Wi-Fi® technologies and has a range of typically 25 km. There is no specific protection as the data link is very directive and the beam is very narrow and extremely difficult to intercept.
- The drones are performing their missions automatically except in some cases for the take-off and landing that can be manual.

## 6.3.3 Results of the Evaluation

### 6.3.3.1 Setup of the Drone Pilot Evaluation

The Software-In-The-Loop (SITL) Simulation runs the complete system on the host machine and simulates the autopilot. It connects via local network to the simulator. The setup looks like this:

Simulator → MAVLink → SITL (see Figure 21)

The simulator is the Ground Control Station (GCS) software. In our case QGroundControl was selected - it provides full flight control and mission planning for any MAVLink enabled drone. The drone in our case is represented by the open source flight control software (Flight Controller) running in the same host computer.

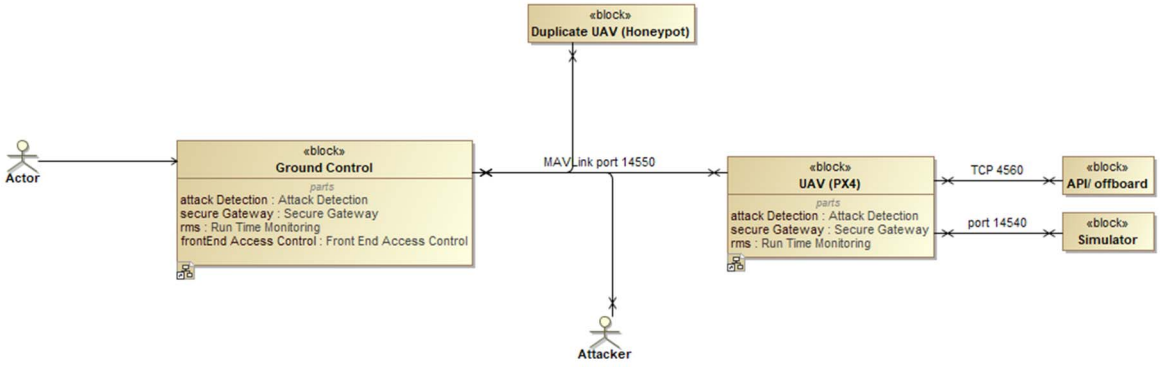



**Figure 20: Overview of the drone pilot with integrated IoTAC modules**

The Software-In-The-Loop (SITL) setup for the testbed includes three virtual machines. The three virtual machines are used as:

1) Represents UAV (open source flight control software, JMAVSim).

2) Represents Ground control station (QGroundControl).

3) Threat (Linux®).

NOTE: Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

The setup uses MAVLink communication protocol for the communication between QGroundControl and open source flight control software.

In this case mainly the UDP protocol (port 14550) is used for the GCS, and TCP (port 4560) for simulation.

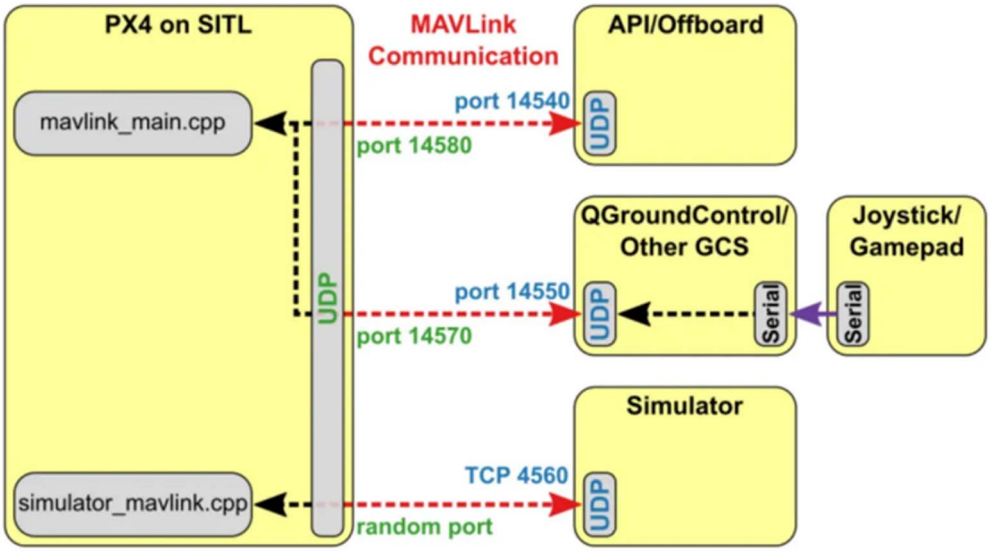



**Figure 21: Overview of the drone pilot presenting communication interfaces**

#### 6.3.3.2 Prioritized Drone pilot misuse cases

**Table 4: Prioritized misuse cases for the Drone pilot**

| ID | Misuse case | Associated STRIDE threats | Priority |
|---|---|---|---|
| DR_1 | The data collection process delivers incorrect UAV navigation data, skewing the control stations' view of where a UAV is and what it does. This may result in control stations issuing mission re-take commands. | S, T | Critical |
| DR_3 | Malicious actors can (partially) observe the video stream of one or more UAVs, and therefore can evade border control more easily. | I | Low |
| DR_4 | The data collection process delivers no UAV navigation data, blocking the control stations' view of where a UAV is. This may result in control stations continuously issuing mission re-take commands or return to base commands. | D | Critical |
| DR_5 | The data collection process delivers no video stream from a UAV, blocking a specific part of the border from the operators' view. | D | Low |
| DR_8 | Commands issued from a control station cannot be traced back to specific operators, allowing insider attackers to issue malicious commands to UAVs without consequences. | R | Low |
| DR_11 | Malicious actors can issue commands to UAVs via the client interfaces of control stations, due to, for example, insufficient authentication, which allows them to control a given set of UAVs. | E | Critical |

#### 6.3.3.3 Validation results per misuse case for the Drone pilot

During the validation of the drone pilot operation an assessment of the system's architecture integrating the IoTAC modules was conducted. The goal was to determine if the selected misuse cases were effectively mitigated and if the system was secure for its intended use.

After conducting a document review, it was determined that the system's architecture and IoTAC modules were effective in mitigating the selected misuse cases. However, during the evaluation, it was discovered that the system was using unencrypted UDP and TCP protocols, which could potentially be exploited by malicious actors. These findings should be considered in future iterations of the system to further enhance its security, especially when transferring to productive use.

It is important to note that the findings should not be considered as severe security issues, but rather areas for improvement to ensure the system's security level is kept high. It is concluded that the system's architecture is secure for its intended use, but recommendations are given to improve the identified minor issues in the upcoming iteration.

#### 6.3.3.4 Conclusion for the Drone pilot

During the validation of the drone pilot operation an assessment of the system's architecture integrating the IoTAC modules was conducted. The goal was to determine if the selected misuse cases were effectively mitigated and if the system was secure for its intended use.

After conducting a document review, it was determined that the system's architecture and IoTAC modules were effective in mitigating the selected misuse cases. However, during the evaluation, it was discovered that the system was using unencrypted UDP and TCP protocols, which could potentially be exploited by malicious actors. These findings should be considered in future iterations of the system to further enhance its security, especially when transferring to productive use.

It is important to note that the findings should not be considered as severe security issues, but rather areas for improvement to ensure the system's security level is kept high. It is concluded that the system's architecture is secure for its intended use, but recommendations are given to improve the identified minor issues in the upcoming iteration.

# 6.4 Automated driving

## 6.4.1 Description and Objectives

### 6.4.1.1 Introduction

The connected and automated vehicle pilot will provide Automated Driving scenarios, where Vehicle to Everything (V2X) data-exchange enables cooperative manoeuvres integrating decision-algorithms, at different Society of Automotive Engineers (SAE) levels of automation; and avails information exchange between the different Intelligent Transportation Systems (ITS) components.

The pilot will consist of two different scenarios: Platoon driving and Platoon Merging. These cooperative scenarios require the use of real-time low latency communication with other vehicles in order to precisely complete the manoeuvre in its correspondent route, Vehicle to Vehicle (V2V) communications based on Dedicated Short Range Communication (DSRC) will be available for all cars in the use case. This low latency communication channel poses a challenge to protect and guarantee its integrity, without incurring in significant overhead for the control of the manoeuvre.

There will be a control station also installed in the pilot system with two functions:

i) representing the road/fleet operator;

ii) controlling and monitoring the demonstration scenarios.

### 6.4.1.2 Scenarios

#### 6.4.1.2.1 Platoon driving

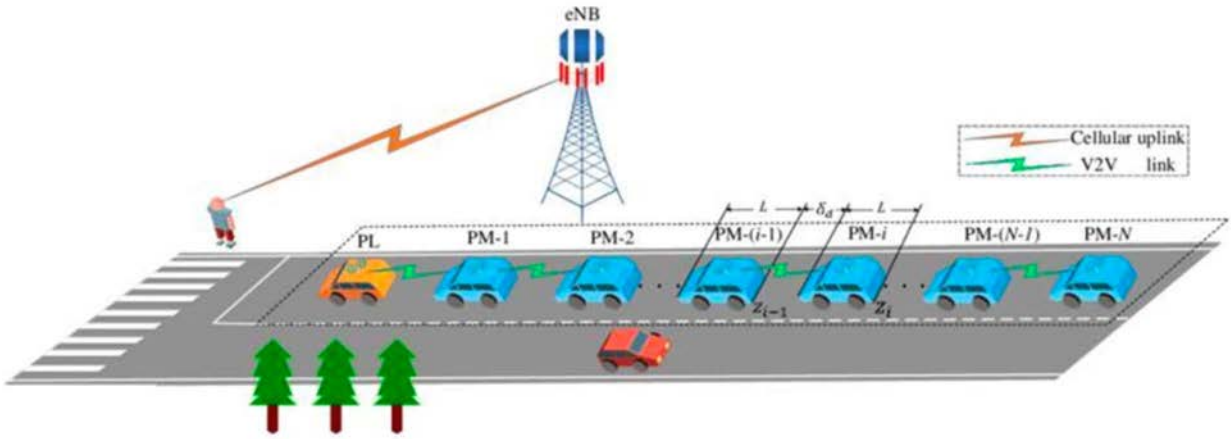



**Figure 22: Platoon driving**

Preconditions:

- All vehicles are equipped with their own architecture, being capable of communicate through V2X Communication. Vehicles are in automated mode.
- Each vehicle is reporting data to the control station through MQTT.

General Sequence:

- Each vehicle is driving towards the same destination in automated mode.
- The control station will take notice and signal a platoon to be formed, with the vehicles in the designated area.
- Each vehicle will independently transition to a platoon manoeuvre and following a leader (vehicle furthest ahead).

- At any moment the control station might disable the platooning manoeuvre in the area.
- Vehicles will communicate through V2X to negotiate the formation of a platoon. The vehicle leader, and positions of all automated vehicles will be decided as a result of this negotiation.
- Once the platoon is successfully formed, the vehicles will drive towards its destination, low level control for platooning requires constant V2X communication. The vehicles will be at all times able to communicate with all agents in the platoon.
- The manoeuvre ends once the vehicles reached the destination.

The Platoon driving state chart is shown in Figure 23.

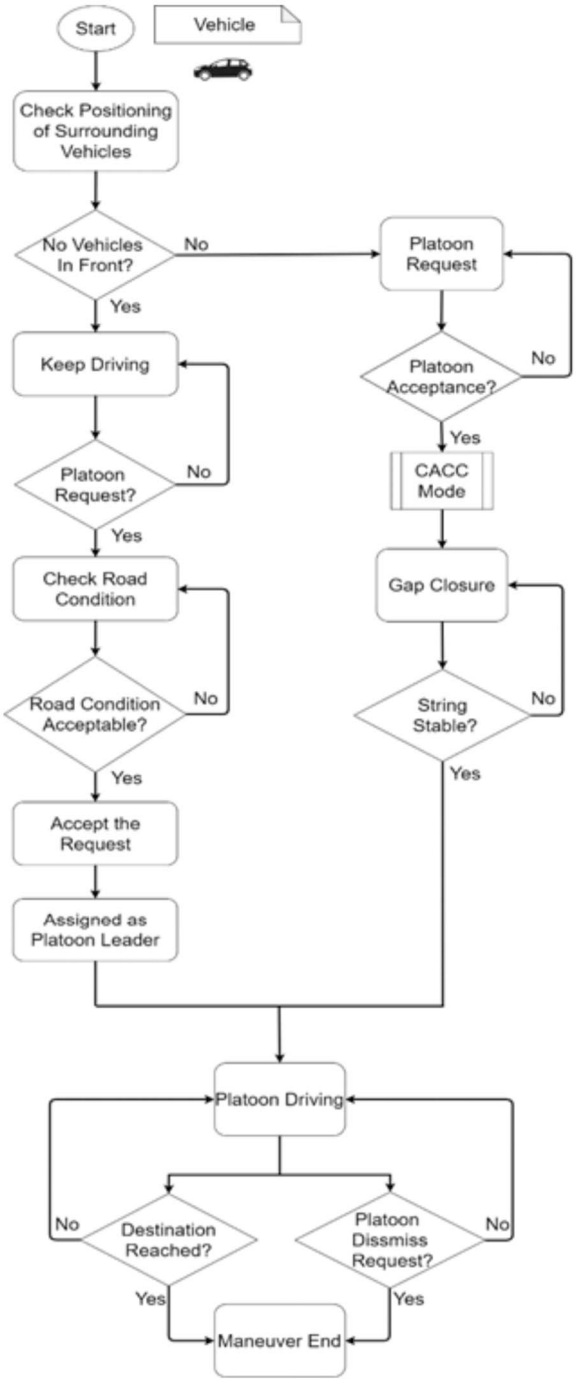



**Figure 23: Platoon driving state chart**

#### 6.4.1.2.2 Platoon merging

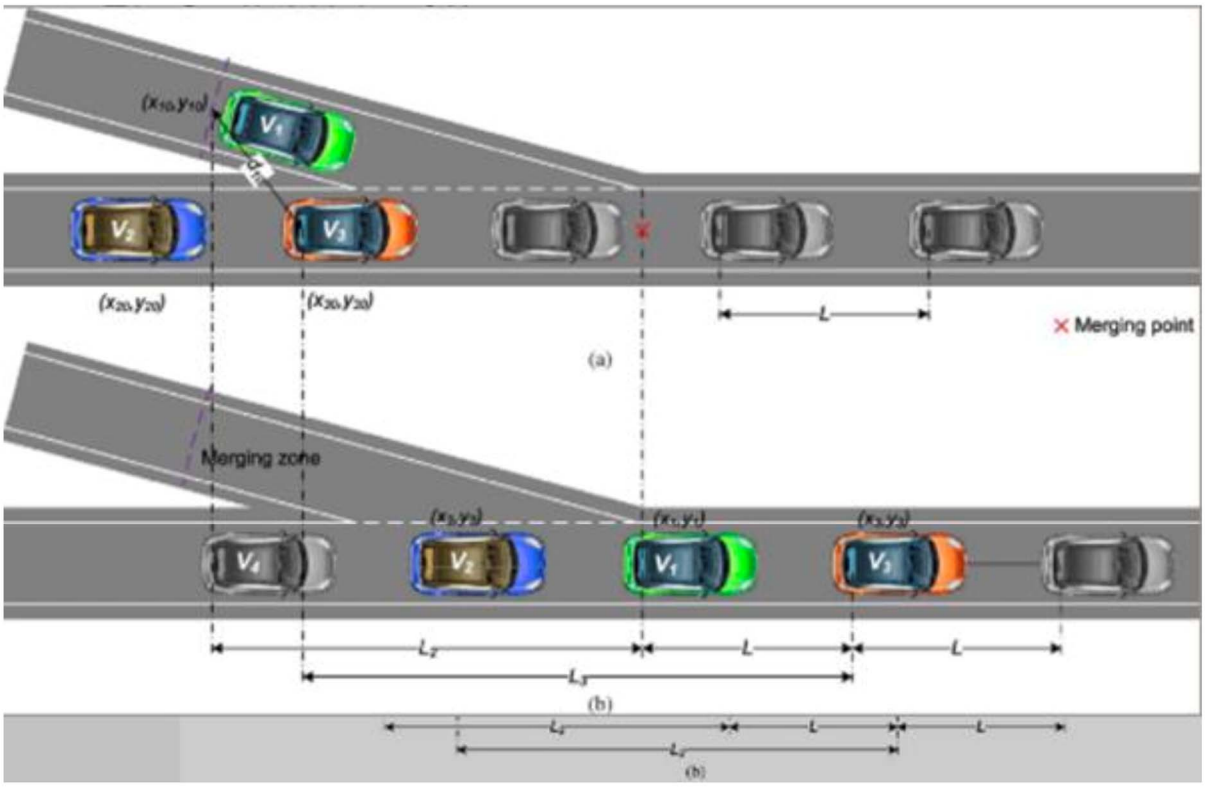



**Figure 24: Platoon merging example**

Preconditions:

- All vehicles are equipped with their own architecture, and there will be already at least one (1) platoon formed (in automated mode) and a vehicle or a second platoon (in automated mode) which requires merging into the first platoon.
- Each vehicle is reporting data to the control station through MQTT.

General Sequence:

- A first platoon is driving towards its destination, in the right lane of the road.
- A vehicle (or second platoon) in another lane reaches a merging point (roundabout, end of the lane or obstruction in the road).
- Vehicles will communicate through V2X to negotiate the formation of a single platoon.
- At any moment the control station might disable the platooning manoeuvre in the area.
- Once the platoon(s) is (are) merged, the vehicles will drive towards its destination. Low level control for platooning will requires constant V2X communication.
- The manoeuvre ends once the vehicles reached the destination.

The Platoon merging state chart is shown in Figure 25.

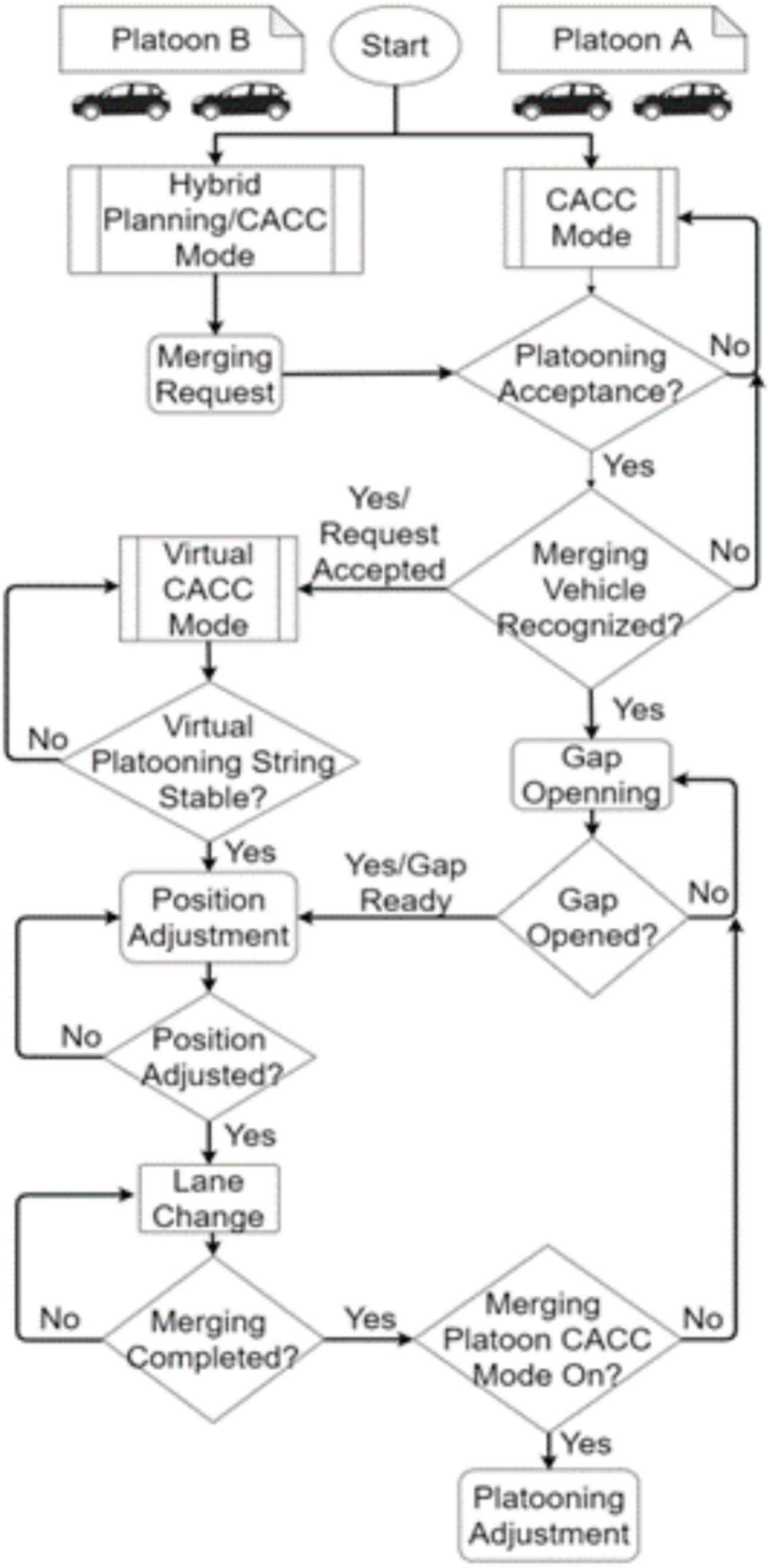
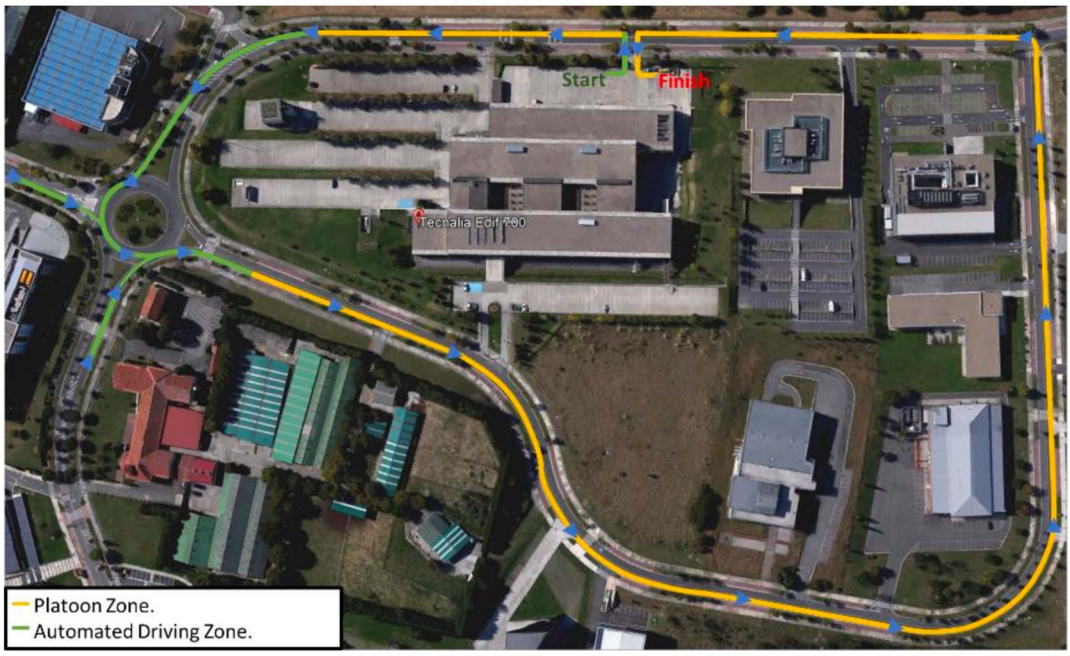



**Figure 25: Platoon merging state chart**

#### 6.4.1.2.3 Venue

The environment for the pilot tests proposed is at the Technological Park of Zamudio, Vizcaya, Spain (nearby the project partner's facilities). This scenario will allow for a realistic test and implementation of the Connected Car Pilot, with complex road segments, and multiple agents will pose a challenge to test the capabilities of the technology embedded in the vehicles.

For each use case, a zone is specified where the manoeuvre will coordinate the vehicles in order to engage, in platoon driving, or platoon merging, other zones are assumed to be driven in automated driving mode. Figure 26 and Figure 27 showcase this division in the environment for each of the scenarios proposed.




(Source: IoTAC project)

**Figure 26: Platoon driving route**


(Source: IoTAC project)

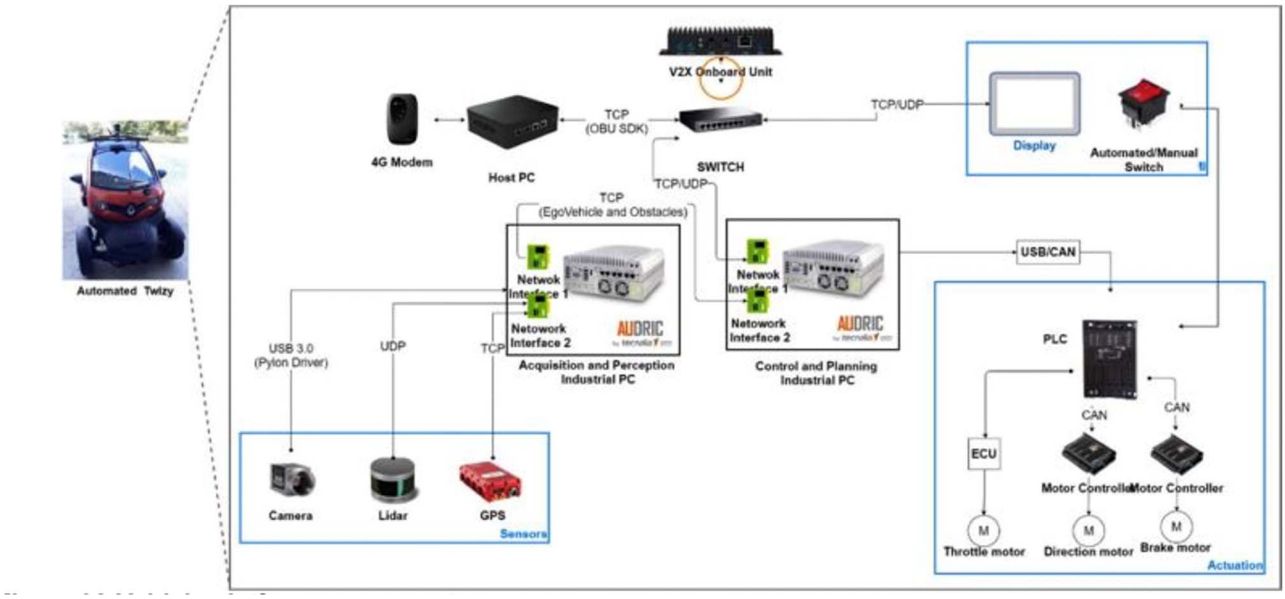
**Figure 27: Platoon merging route**

### 6.4.1.3 Connected Car Infrastructure

The infrastructure for the pilot is divided in three parts, its equipment and structure, monitoring and control framework, and finally the services provided by the pilot. The equipment required to put in place the pilot consists mainly of the vehicle platforms, and all hardware components, required for their automation, simulation, and connectivity. For the monitoring and control framework, two key systems are identified, a remote-control station, and the V2X capabilities which will enable real-time cooperation and control in cooperative manoeuvres. The general equipment and components for the platforms are showcased in Figure 28 and Figure 29.

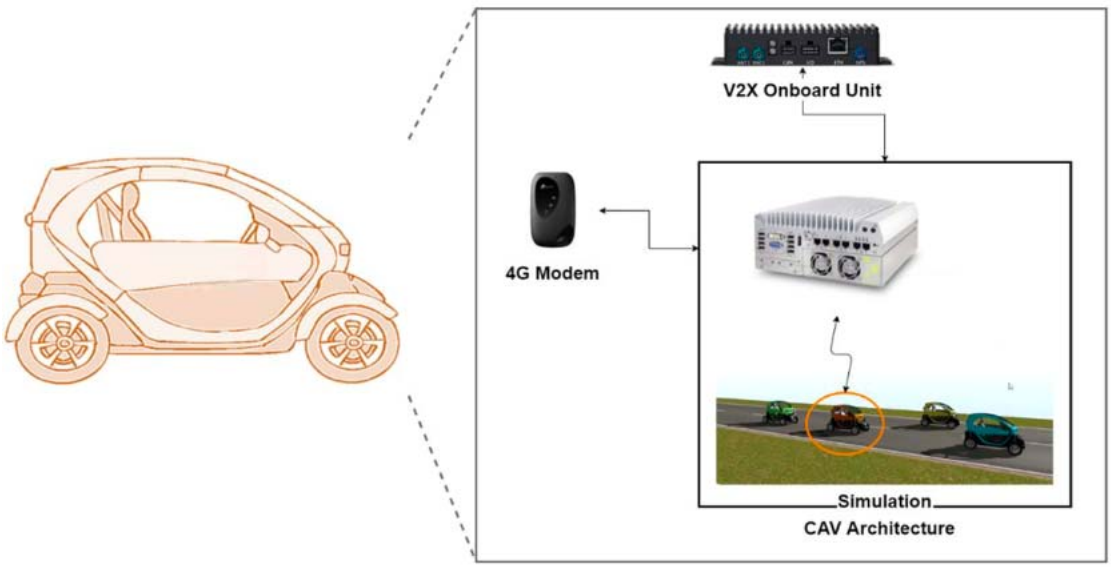
- Equipment and structure:
  - Vehicle Platform: Compact Car:
    - Control PC: AUDRIC.
    - Perception PC (with GPU): AUDRIC.
    - Router.
    - V2XOBU.
    - Host PC (for V2X and Internet Connectivity).
    - 4G/5G Modem.
    - PLC.
    - CAN Network.
    - Compact Car ECU.
    - Lidar 16 layers.
    - Front camera.
    - IMU and GPS.

        - CAN Controller and Motor (Braking).
        - CAN Controller and Motor (Steering).
        - Throttle by wire (ECU).
    - Vehicles Platforms: Simulated Compact Car using in-house simulator:
        - Simulator PC: Running Simulator and AUDRIC.
        - V2XOBU.
        - 4G/5G Modem.
- Monitoring and control framework:
    - Vehicle to Vehicle control:
        - DSRC Based Communications (V2X).
        - CAM Service.
        - DENM Service.
        - Ad-hoc Platoon messaging.
- Control Station Monitoring:
    - Server connected to the vehicle platforms:
        - MQTT Broker.
        - Monitoring positioning and state of vehicles.
        - Logging of events in the road.
        - High level decision for platoon manoeuvre (enable/disable, tweak parameters).
- Services:
    - Automated Driving.
    - Cooperative Manoeuvres:
        - Platoon Driving.
        - Platoon Merging.




(Source: IoTAC project)

**Figure 28: Vehicle platform components**




(Source: IoTAC project)

**Figure 29: Simulated Platform Components**

AUDRIC (Automated DRIving Core) is a software framework for automated driving functionalities, designed as a modular architecture that gives broad flexibility to add, change and remove components. It is composed of a master framework that connects six blocks: acquisition, perception, communication, control, decision, and actuation.

SEGOVYA-RT (SafE Generator of Vehicle trajectory using lAne information on Real-Time) is a software for real-time trajectory generation of non-holonomic ground vehicles, especially automated cars, shuttles, or buses. The software targets urban and inter-urban scenarios that mean environments with low speeds (under 50 to 60 km/h) and high reliability under different road configurations.

### 6.4.2 Connected Car Pilot System

The connected and automated car will require a series of services and functionalities in order to operate as intended. In Figure 30, a general system context with the vehicles and their interactions is proposed. For the pilot it is needed that all vehicles involved are equipped and connected with both, V2Vand 4G/5G to the internet, for MQTT interaction with the control station. In the case of V2V, each vehicle will be capable of interacting and communicate with other nearby connected vehicles, while in the MQTT case, all interaction will be handled directly through the Control Station.

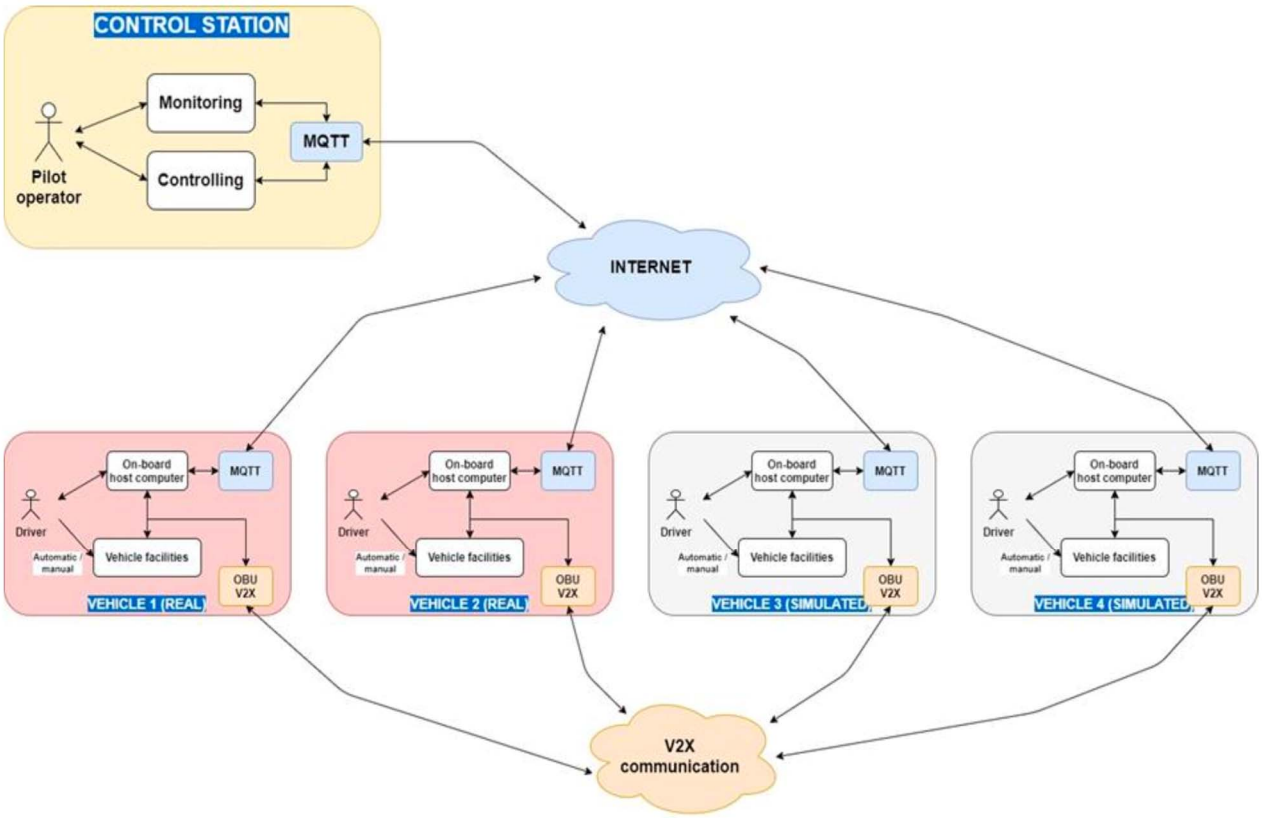



**Figure 30: Connected Car Pilot System**

### 6.4.3 Results of the Evaluation

#### 6.4.3.1 Setup of the Connected Car Pilot Evaluation

The logical architecture of the pilot is presented in Figure 31, where it can be observed the interaction between the real vehicle, and control station. The vehicles will have a driver for safety measures, the gateway and attack detection module from IoTAC. The same case applies for the Control station, which is going to have an operator to supervise the incoming vehicle data, the Front Access Management to protect the MQTT broker fort undesired connections, the Run Time Monitoring System for additional data monitoring and collection and finally the Honeypot that is placed outside of the pilot network to divert possible attacks.

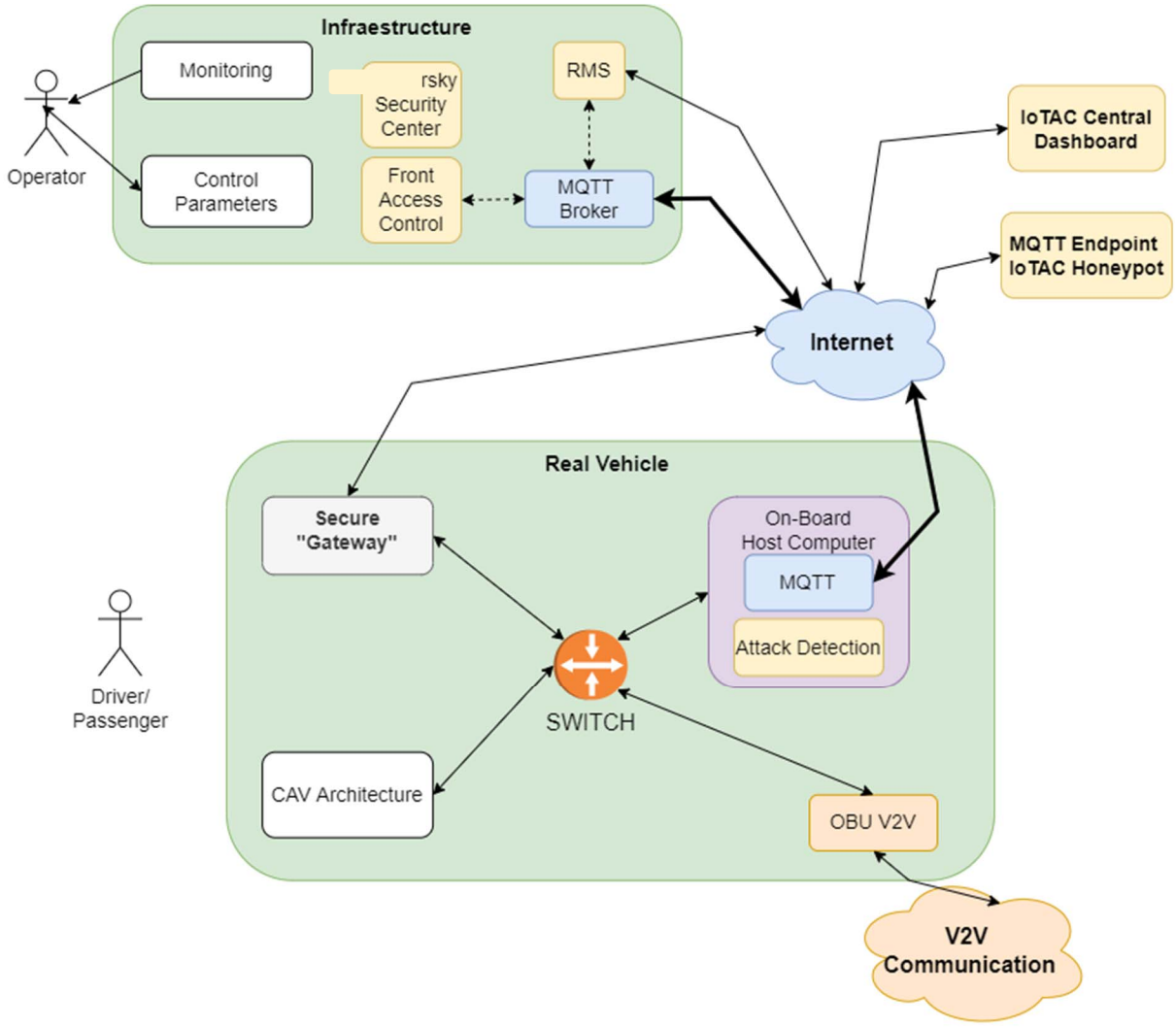



**Figure 31: Logical architecture with integrated IoTAC modules of the Connected Car pilot**

A more detailed description of the components of the vehicle and the IoTAC modules is presented in Figure 32. All the data (incoming and outcoming) pass through a switch capable of port mirroring and then to the Secure Gateway. The port that receives all the data is connected to the Host PC, which contains the IoTAC attack detection module. For internet connectivity, a 5G router is placed in front of the gateway, allowing connection from the vehicle to the Control Station, and between the security centre and the gateway. The virtual vehicles are connected to both an OBU; to exchange information with other vehicles, and the internet through MQTT to exchange information with the control station. On the other hand, the infrastructure counts with a virtual machine running the Security Centre and a control station with the IoTAC Front Access Management and Run Time Monitoring System.

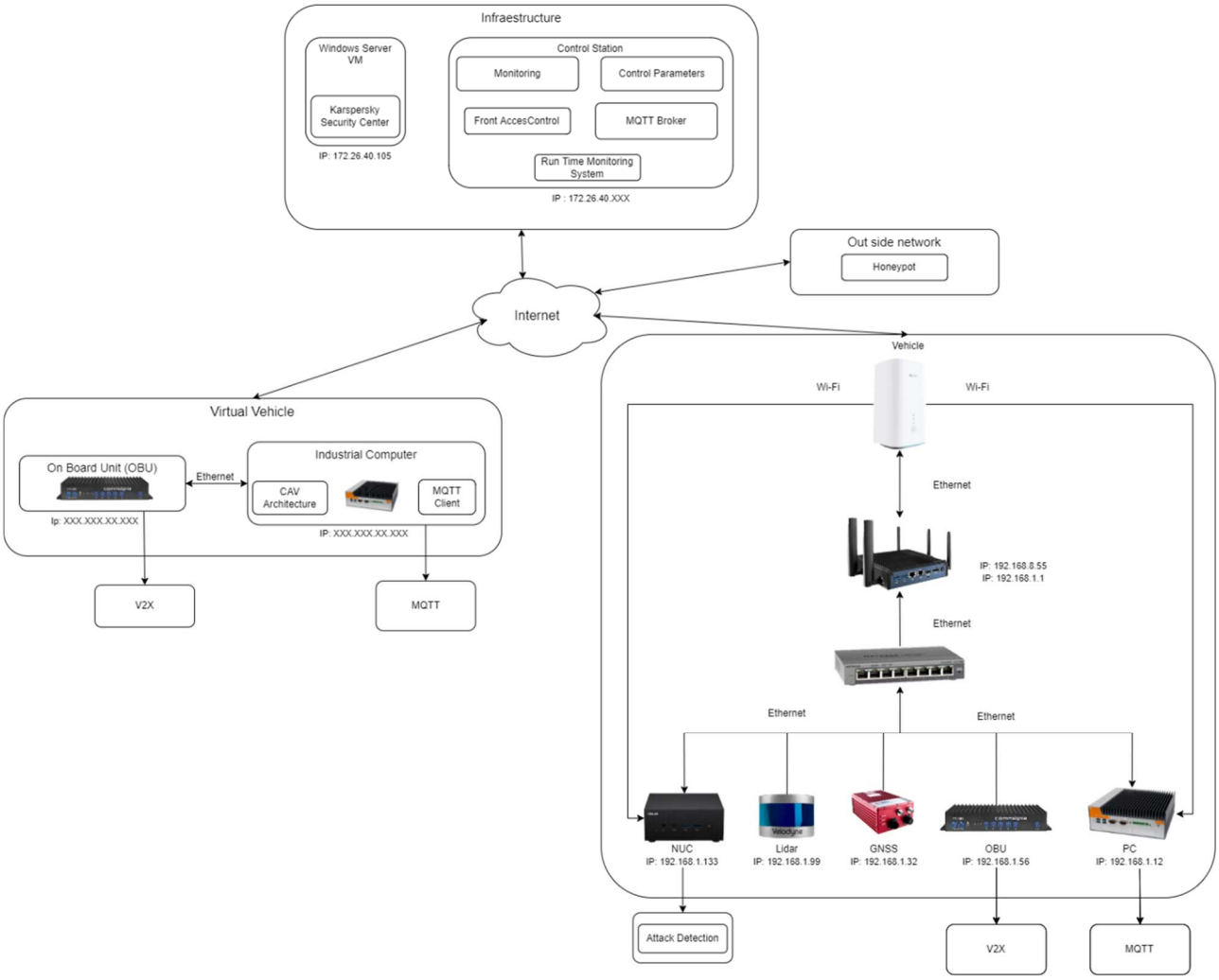



**Figure 32: Physical architecture with the integrated IoTAC modules**

### 6.4.3.2 Prioritized Connected Car pilot misuse cases

**Table 5: Prioritized misuse cases for the Connected Car pilot**

| ID | Misuse case | Associated STRIDE threats | Priority |
|---|---|---|---|
| V2X_1 | The data collection process may deliver incorrect sensors readings, skewing the CAVs perception of their position and that of other CAVs. This can result in crashes and potentially kill the passengers. | S, T | Critical |
| V2X_3 | The data collection process delivers no sensors readings, therefore, CAVs have no information about their position and that of other CAVs. This can result in crashes and potentially kill the passengers. | D | Critical |
| V2X_4 | The storage provides incorrect maps of intersections and/or roads, forcing CAVs to determine the potential directions from which merging CAVs may arrive on their own. In such scenarios, the correct functioning of sensors and actuators becomes critically important. | S, T | High |
| V2X_5 | The storage provides no maps of intersections and/or roads, forcing CAVs to determine the potential directions from which merging CAVs may arrive on their own. In such scenarios, the correct functioning of sensors and actuators becomes critically important. | D | High |
| V2X_9 | The control process act based on incorrect input data, commands, and/or implementation, potentially causing the platooning CAVs to crash. This may result in the death of passengers. | S, T | Critical |
| V2X_10 | The control process not functioning can cause platooning CAVs to crash and thus, potentially killing passengers. | D | Critical |

#### 6.4.3.3 Validation results per misuse case for the Connected Car pilot

During the validation of the Connected Car pilot, an assessment of the system's architecture and integrated IoTAC modules was conducted. The goal was to determine if the system met the necessary security requirements and was suitable for its intended use.

After conducting a document review, it was determined that the system's architecture and security modules were effective in protecting the system from potential security threats. However, during the evaluation, it was not clear whether the system have a backup resource or redundant sensors in case of wrong readings or sensor failure. Moreover, it was found that the MQTT communication service is not secured, it does not implement a security layer (e.g. TLS). In addition, the question whether the system also requires constant communication from the control centre (or what consequences would follow in case of a connection loss) was left open. Those points should be addressed in case there are missing at least when shifting to a productive use.

However, it is concluded that the system's architecture is secure enough for its intended use, but recommendations are given to the system's operator to consider implementing backup resources or redundant sensors, ensuring constant communication from the control centre, securing the MQTT communication service and implementing solutions to handle internet connectivity or signal blocking issues to ensure the system's security level is kept high and to minimize potential security risks. These findings should be taken into consideration in future iterations of the system to further enhance its security and functionality.

#### 6.4.3.4 Conclusion of the Connected Car pilot

During the validation of the Connected Car pilot, an assessment of the system's architecture and integrated IoTAC modules was conducted. The goal was to determine if the system met the necessary security requirements and was suitable for its intended use.

After conducting a document review, it was determined that the system's architecture and security modules were effective in protecting the system from potential security threats. However, during the evaluation, it was not clear whether the system have a backup resource or redundant sensors in case of wrong readings or sensor failure. Moreover, it was found that the MQTT communication service is not secured, it does not implement a security layer (e.g. TLS). In addition, the question whether the system also requires constant communication from the control centre (or what consequences would follow in case of a connection loss) was left open. Those points should be addressed in case there are missing at least when shifting to a productive use.

However, it is concluded that the system's architecture is secure enough for its intended use, but recommendations are given to the system's operator to consider implementing backup resources or redundant sensors, ensuring constant communication from the control centre, securing the MQTT communication service and implementing solutions to handle internet connectivity or signal blocking issues to ensure the system's security level is kept high and to minimize potential security risks. These findings should be taken into consideration in future iterations of the system to further enhance its security and functionality.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | October 2023 | Publication |
| | | |
| | | |
| | | |
| | | |