D6.1

Initial Pilot Use Case Requirements

WP6 – Smart Home Pilot Use Case

SIFIS-Home

Secure Interoperable Full-Stack Internet of Things for Smart Home

Due date of deliverable: 31/05/2022
Actual submission date: 31/05/2022

Responsible partner: MIND
Editor: Domenico De Guglielmo
E-mail address: dome@mind.cc

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The SIFIS-Home Project is supported by funding under the Horizon 2020 Framework Program of the European Commission SU-ICT-02-2020 GA 952652

Authors: Domenico De Guglielmo (MIND), Samuli Stenudd (RIO)
Jukka Aittakumpu (RIO)

Approved by: Valerio Frascolla (INT), Riccardo Coppola (POL)

Revision History

Version	Date	Name	Partners	Section Affected Comments
0.1	1/4/22	ToC Provided	MIND	All
0.2	10/4/22	Inserted Mind Architecture	MIND	All
0.2	12/4/22	Inserted RIO and CEN device specifications	CEN	4
0.3	25/4/22	Updated RIO architecture specification	RIO	4
0.4	10/5/22	Inserted use case requirements	MIND	6
0.5	20/5/22	Ready for review	MIND	All
1.9	28/5/22	Ready to submit	MIND, INT	All

Executive Summary

This deliverable describes the activity of requirement gathering for the SIFIS-Home pilot architecture. The deliverable reports the specification of the devices which are candidate to be used in the use case architecture, reporting thus the specification of components from MIND and RIOTS, together with considerations on how to generalize the use case to other off-the-shelves devices. Subsequently, the deliverable reports a set of requirements and their link with the requirements and use cases reported in D1.2, explaining how the pilot will serve in the validation of the functional requirements.

Table of contents

1. Introduction

This deliverable is the result of the initial work that we performed in task T6.1 and task T6.2, i.e., the WP6 tasks devoted to defining the smart home use cases of the project and providing their functional, non-functional and security requirements. The structure of the deliverable is as follows. First, we provide a detailed overview of Mind and Riots, the commercial smart home solutions provided by SIFIS-Home partners MIND and RIOTS. We describe their architectures, the devices they rely on as well as their limitations and weaknesses. Second, we report the list of different devices that we are going to use in the pilot highlighting their type (SD or NSSD). Then, we describe all the different smart home use cases that we identified. For each one of them, we highlight the list of involved devices, the non-functional and the security requirements. Finally, we report the list of tests that we plan to perform to verify that the requirements of the use cases are satisfied. Then, we conclude the deliverable.

2. MIND

Mind is a commercial solution that targets the luxury smart home market. Mind provides several features ranging from automatic lighting, temperature and irrigation control to energy consumption monitoring and control of multimedia devices. In addition, Mind allows to control the devices inside the house from a remote side and offers advanced features such as face recognition and an advanced alarm system that relies on people and object detection. Also, Mind allows its users to control the house through voice commands. Differently from the majority of smart home solutions present in the market, Mind is a distributed multi-gateway solution. In detail, Mind relies on having a number of Mind Cubes (i.e., the Mind gateway device) installed inside the house of every customer. This allows Mind to overcome the *Single Point of Failure* (SPOF) problem of classical single-gateway smart home solution. In addition, Mind has been designed in such a way that i) it does not require wires to interconnect its devices and ii) it is able to properly work even when there is no Internet connection available. Finally, all the house managing tasks are executed on the Mind cubes. Hence, Mind does not depend on cloud services to offer its main functionalities.

System architecture and limits of MIND

This section provides a detailed overview of the system architecture of Mind. First, we describe the Mind Cube, i.e., the Mind gateway, reporting its features and its hardware capabilities. Second, we provide a description of Mind Actuators. Then, we describe the network architecture of Mind and describe the different services used by Mind to provide its functionalities. Finally, we conclude the section highlighting the limitations of Mind that SIFIS-HOME components allow to overcome.

Mind Cube

Mind has been designed with the goal to provide a smart home solution that i) does not require to install wires to interconnect smart home devices, ii) has no Internet/cloud dependence to provide its functionalities and iii) provides advanced ML-based features. For being able to satisfy such requirements, Mind developed a powerful custom device, named Mind Cube, having the following characteristics:

- **Computational capabilities**
    - Nvidia Jetson TX2 SoM providing:
        - Quad-core ARM A57 CPU
        - 8GB DDR4 RAM

        - 32GB eMMC
        - NVIDIA Pascal™ GPU architecture with 256 NVIDIA CUDA cores
        - Integrated Image Signal Processor
    - **Network capabilities**
        - BRCM4354/CYW4354 WiFi Adapter
            - 802.11 ac/b/g/n 2x2 MIMO 867 Mbps
        - Texas WL1837 WiFi Adapter
            - 802.11 ac/b/g/n 2x2 MIMO 100 Mbps
        - Qualcomm Atheros QCA9882 WiFi Adapter
            - 802.11 ac/b/g/n 2x2 MIMO 867 Mbps
        - Broadcom BRCM 89610 - 1 Gbps Ethernet Controller
        - Telit LE910 4G/LTE Modem
        - Bluetooth connectivity
    - **Sensors:**
        - 2x Bosch BME680 I2C Temperature, Humidity and Pressure sensor
        - 2x Panasonic AMG8883 8x8 pixels thermal camera sensor
        - 2x Texas OPT3002 Brightness Sensor
        - 1x NGM2116 CH4 Detector (on-off output)
        - 1x TGS5141 CO Sensor (ppm output)
    - **Cameras:**
        - 2x IMX290 Ultra Low-light Full HD image sensors
    - **Lighting and user-notification devices:**
        - 2-channels LED Spotlight
        - 6x RGBW Neopixel Leds
        - Dali Master
    - **Audio**
        - 4 piezo-microphones array with beamforming capability (XMOS XVF3000 Audio processor)
        - 4/8 Ohm 2W External Speaker output

As it can be observed, Mind Cube is able to execute several tasks in parallel having a significant amount of computational power and memory available. Also, being equipped with a 256-core GPU, it can execute very complex ML tasks analysing data acquired from the microphones and the High-Definition Cameras. The Wi-Fi, Bluetooth and LTE interfaces are used to i) allow Cube-to-Cube communication, ii) communicate with the other devices of the house and iii) communicate with the Internet in case the main Internet connection experiences a failure. Mind cube allows to monitor temperature, humidity, pressure as well as brightness, CH4 and CO. Also, it can be used as a notification device using its spotlight, its led and its speaker.

Mind Actuators

Mind makes use of several Wi-Fi actuators for being able to control and monitor the energy consumption of the lights, sockets, shutters and appliances installed inside the house. The actuators are simple devices that are composed of a number of output and input channels and a Wi-Fi module (ESP8266). The actuators allow to turn on and off the appliances/light/sockets they are attached to. Also, they can measure and report the energy consumption of the attached devices. Finally, using the input channels of the actuators it is possible to detect the state of attached buttons and bistable buttons as well as the state of window and door contact sensors. The actuators can be configured to connect to any Wi-Fi network. In Mind they are connected to a Wi-Fi network created by the Mind Cubes (see below).

Mind Network architecture

Mind is a multi-gateway solution that relies on installing a number of Mind cubes inside every house, as shown in Figure 1.

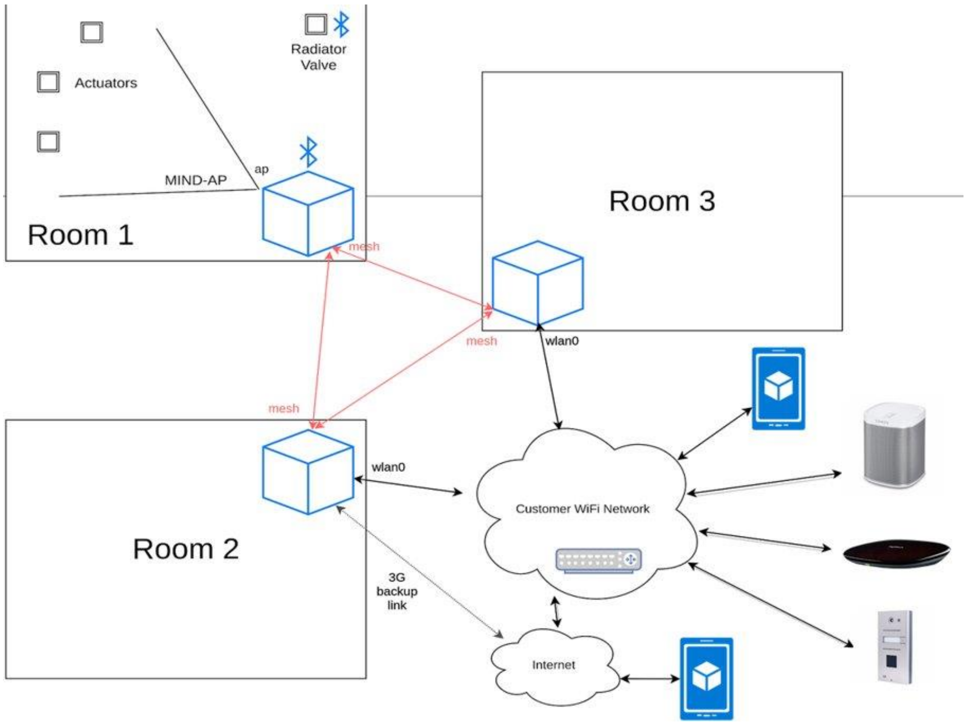

Figure 1. Mind network architecture

As it can be observed, Mind Cubes are present in the main rooms of the House and are interconnected through a Wi-Fi multi-hop mesh network (IBSS mode). Also, if available, the Cubes also connect to the customer Wi-Fi Network and communicate with the smart home devices of the customer. Finally, every Cube uses one of the available Wi-Fi interfaces, in Access Point mode, to create a dedicated Wi-Fi network to which the Wi-Fi actuators deployed in the house connect to. Please note that in case one of the Cubes experiences a failure, the actuators can connect to another Cube that is still operational and, hence, continue to provide their functionality to the user. It can be observed that every Cube is also equipped with an additional cellular modem that is used to connect to the Internet in case the main house connection to the Internet experiences problems or poor performance.

Mind services

Mind Cubes run Cube services and House services. Cube services are simple services that make use of the sensors and hardware components present on every Mind Cube. Conversely, House services are usually complex services that take care to acquire, aggregate and use information from several different Mind Cubes.

Limits of MIND

Although Mind allows new House and Cube services to be deployed in the system, currently this operation is only allowed to Mind operators, due to the concern of installing malicious or bad quality software, which might cause security and safety issues. For this reason, currently Mind is closed to third party developers, which becomes a limit for Smart Home enthusiasts that might desire a higher level of customization. Besides, the Mind framework has not been developed following a security-by-design and, although it includes basic protection mechanisms, the current framework is potentially prone to security attacks coming from the network, from the interaction with third party devices and is not resilient to device corruption.

3. Riots

Riots is a commercial IoT solution that is used in the building automation and control market. Riots is focused on apartment buildings and uses a cloud service (Riots Cloud) and several different devices to offer the following capabilities:

- Follow and control indoor conditions
- Follow and control air conditioning units
- Detect water leaks and other important states
- Connect water and electricity meters to the Internet

Riots devices are usually in spaces where their data needs to be able to be monitored or controlled around the clock. Riots Cloud makes remote monitoring and controlling possible by offering a wide range of settings including:

- Controlling devices securely anywhere, anytime
- Comprehensive, device-based history data
- User rights sharing
- Devices’ online status
- Firmware updates
- Remote device reboot
- Alerts

Riots Cloud is available as a browser and as a mobile app. The real-time analysis of the flow of data coming from the devices enables shorter reaction time in the event of possible malfunctions and situations where quick maintenance is needed. Cloud service can also harness computational AI-features to make predictions and deductions from large amounts of data. It is especially used for administrative purposes, whereas tenants of the apartment buildings where Riots automation systems have been installed use mainly the mobile app.

Riots Mobile is especially useful for the tenants since it is easy-to-use, provides the right information in real-time and can be accessed on both iOS and Android platforms. User rights can be shared to a specific apartment or space for a chosen period ranging from hours to days and months.

Making maintenance more convenient, Riots devices can be updated remotely from Riots Cloud. The current firmware version is shown as a comparison to the latest available version. If user has the correct rights, they can update the device's firmware.

Sometimes devices act up and the connection is lost. Riots Cloud provides alerts, for example, to lost internet connection making it easy to spot device failures. An option to reboot devices is offered to fix connection issues. However, this does not always guarantee the connection gets restored or fixed. It is important to consider the installation location of a device in case of a failure. The easier it is to reach the device physically, the faster it is to fix or replace the broken device.

Users can activate email and text message alerts for almost any feature (as in value). Depending on devices, these features differ slightly from each other. For example, temperature alerts can be set according to lowest and highest value and certain features can send alerts when they are switched on or off.

Riots architecture

Based on Mama and Apartment devices, Riots architecture (Image 1) relies on a wireless connection between the devices and a secure Internet connection from Mama to the Riots Cloud service. All additional devices inside an apartment are connected to its Apartment device.

Each Apartment device is independently connected to Mama which means that they do not rely on each other. If one Apartment device loses connection to Mama, others will still function as expected. If Mama loses connection to the Internet, the data will not be updated from any of the devices, but they will remain fully functional. Riots-products are compatible with the most common APIs of the industry.

Every Riots-solution can be scaled to the specific needs of each building, apartment or any other space. They can be installed freely around the space, although Mama is recommended to be installed in a technical area or close to a broadband connexion. Some devices (Mama, Apartment) do not need to be installed in sight, since they mainly act as links between other devices.

The example architecture (Image 1) showcases a typical scenario; temperature and humidity sensors (Riots Apartment) and Riots Mama connected to Riots Cloud. The scalable nature of the architecture makes it possible to add more devices and functionalities inside an apartment or space.

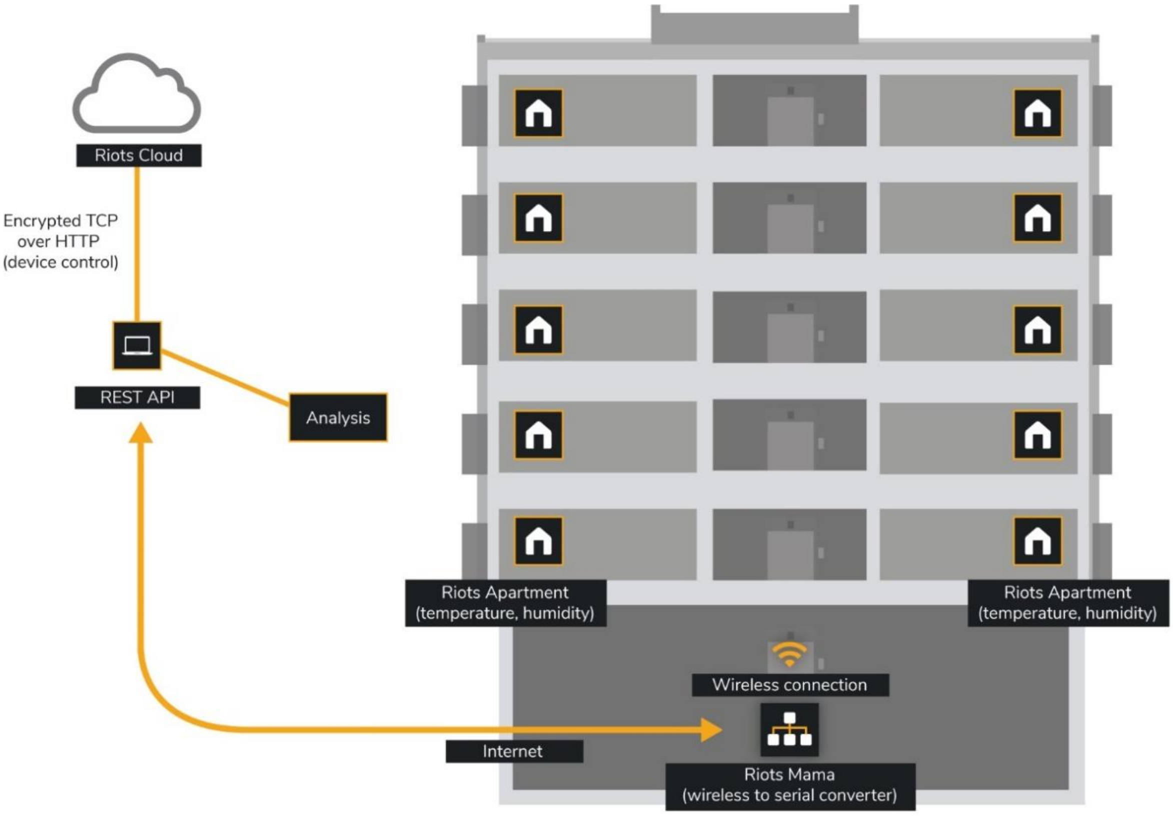
Riots Cloud
Encrypted TCP over HTTP (device control)
REST API
Analysis
Riots Apartment (temperature, humidity)
Riots Apartment (temperature, humidity)
Wireless connection
Internet
Riots Mama (wireless to serial converter)

Image 1. Riots architecture

The additional devices would be wirelessly connected to Riots Apartment which connects them online via Riots Mama. It is possible to add devices from different manufacturers within the Riots network. If a certain kind of a device is required for a certain building or space, it can be added and included in Riots Cloud for remote use. The devices do not need to rely on their corresponding IoT-platforms.

Limits of Riots architecture

The devices must however be installed within the range of the wireless connection if they are connected to each other wirelessly. Due to the subtle nature of the wireless technology used in Riots devices, there cannot be more than 10 meters between the devices. Also, certain materials (e.g., concrete) could block the connection or make it weaker and prone to errors.

Riots Mama Internet gateway

Riots Mama (Image 2) connects the local Riots-network safely and securely to Riots Cloud. Mama creates an AES128-encrypted network connection between the local Riots-network and the Riots cloud service. All the network traffic goes through Mama, which ultimately links a building and its spaces to the Internet. It is an inseparable part of every Riots solution, because it enables the spaces and buildings to be turned smart, creating a secure and efficient data transfer from cloud service to the buildings it is installed in.

Riots Mama	**Information**

Dimensions (width x height x depth)	71mm x 27mm x 71mm
Wireless range	about 10m (*)
Electricity consumption	<0.85 W
Connection	LAN
Operating temperature	+5 - +30°C

Table 1. Riots Mama

* Riots-technology is based on a slightly subtler wireless technology than mainstream applications. It utilises short-range technology which reduce the amount of wireless traffic on air.

Requirements

- Riots Mama requires a power socket and a broadband connection

Image 2. Riots Mama Internet Gateway

Riots Thermostat

Riots Thermostat (Image 3) makes room temperature control convenient using a cloud-based service, modern design and a mobile app. Device history data and current settings can be monitored and controlled in real-time using Riots Cloud on any browser or Riots Mobile app on a phone.

Main functions

- Temperature setting with easy-to-use buttons
- Shows the current setting on device screen and Riots Cloud or Riots Mobile app

The thermostat can be controlled remotely on Riots Mobile iOS and Android apps, Riots Cloud cloud-service or the wall-mounted device. Riots Thermostat connects wirelessly to the Riots Network inside an apartment. Other devices can connect to it wirelessly enabling freedom regarding their location, if they stay within the range of the wireless connection.

Riots Thermostat	**Information**
Dimensions (width x height x depth)	84mm x 84mm x 21mm
Wireless range	about 10m (*)
Temperature tolerance	± 0,2°C
Humidity tolerance	± 2% RH
Operating temperature	+5 - +30°C

Table 2. Riots Thermostat

* Riots-technology is based on a slightly subtler wireless technology than mainstream applications. It utilises short-range technology which reduce the amount of wireless traffic on air.

Image 3. Riots Thermostat

4. Devices used for the pilot

The following table reports all the devices that we intend to use for the pilot. We indicate if they are Smart Devices (SD) or Not So Smart Devices (NSSD).

Device	**Type**
Mind Cube	SD
Shelly Actuator	NSSD
Smart Doorbell	NSSD
Riots Mama	SD
Riots Thermostat	NSSD
Smartphone	SD
Raspberry PI	SD

Table 3. Devices used for the pilot

5. Smart home Use Cases

This section reports the different smart-home related use cases that we identified. For each one of them, we provide a list of devices used in such scenario, a description, non-functional requirements, security requirements and an example of each use case in action to further explain its use and features. The Use Cases are partly based on the user stories that were presented in the deliverable D1.2 “Final Architecture Requirements Report”. The non-functional and security requirements are also based on the final requirements listed in the deliverable D1.2.

Turn on/off lights using the control panel

The SIFIS-Home user wants to turn on and off lights using the SIFIS-Home control panel. The user should be able to control the lights also from a remote side.

Devices to be used

- Mind Cube, Shelly Actuator, Smartphone, Lights

Non-functional requirements of the use case

- The lights should be turned on/off in less than 3 seconds from the reception of the command.
- The interface to control the lights should be simple to use and user friendly.
- PE-07: A command should be invoked within 5 seconds from the event that triggered its execution.
- US-02: The SIFIS-Home system shall be autonomous and learn based on the users’ habits, still according to defined privacy policies.
- DE-02: The start of an interaction command should be recognized properly and correctly in more than 99% of cases.
- DE-03: The commands to execute should be recognized properly and correctly in more than 95% of cases.
- DE-09: The configuration changes should be propagated successfully to the devices in more than 99% of times.
- DE-10: The SIFIS-Home system should be able to restore the previous configurations if there are errors in applying configuration changes.
- DE-18: The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.

Security requirements of the use case

- Only allowed users should be able to use the control panel.
- Replay attacks should not be possible.
- All the exchanged messages need to be encrypted.
- SE-01: APIs for the communication with internal devices must be secured.
- SE-02: APIs for the communication with external devices must be secured.

- SE-03: Personal data stored must be encrypted.
- SE-04: The system shall protect and avoid disclosure of sensitive information.

Use case in action

- The control panel can be used from SIFIS-Home control center and remotely using a digital application.
- Add timers to make lights light on/off automatically.
- Show the status of the lights in the control panel.

Being notified if someone is at the doorbell

The SIFIS-Home system should notify the user when someone is at the doorbell. The notification should be reported in the control panel, in the mobile application and through notification devices (i.e., using a buzzer).

Devices to be used

- Mind Cube, Shelly Actuator, Smartphone, Smart Doorbell, Buzzer.

Non-functional requirements of the use case

- The user should be notified that someone is at the doorbell in less than 3 seconds.
- US-02: The SIFIS-Home system shall be autonomous and learn based on the users' habits, still according to defined privacy policies.
- DE-02: The start of an interaction command should be recognized properly and correctly in more than 99% of cases.
- DE-18: The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.

Security requirements of the use case

- Only allowed users should be able to see the notifications on the control panel.
- Only allowed users can unlock the door.
- Replay attacks should not be possible.
- SE-01: APIs for the communication with internal devices must be secured.
- SE-02: APIs for the communication with external devices must be secured.
- SE-04: The system shall protect and avoid disclosure of sensitive information.

Use case in action

- A sound is played from in-home control center with quick actions.
- Door can be unlocked from control panel.
- If user is not at home the mobile app will notify them with a sound and a notification.

- Show the status in the control panel.
- Ability to add access rights in case of deliveries.

Turn on/off lights pressing and releasing buttons

The SIFIS-Home system should turn on and off the lights of a certain room if the users press/release buttons inside the room.

Devices to be used

- Mind Cube, Shelly Actuator, Lights

Non-functional requirements of the use case

- The lights should be turned on/off in less than 1 second after pressing/releasing the buttons.
- PE-07: A command should be invoked within 5 seconds from the event that triggered its execution.
- PE-16: A command should be invoked within 5 seconds from the event that triggered its execution.
- PE-17: The current configuration of a device should be retrieved in less than 10 seconds.
- PE-21: The list of policies should be retrieved in less than 30 seconds.
- US-02: The SIFIS-Home system shall be autonomous and learn based on the users’ habits, still according to defined privacy policies.
- DE-02: The start of an interaction command should be recognized properly and correctly in more than 99% of cases.
- DE-18: The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.

Security requirements of the use case

- Replay attacks should not be possible.
- SE-01: APIs for the communication with internal devices must be secured.
- SE-02: APIs for the communication with external devices must be secured.
- SE-04: The system shall protect and avoid disclosure of sensitive information.

Use case in action

- Show the status of the lights in the control panel.

Being alerted if motion sensors detect people presence while the House is in away mode

The SIFIS-Home system should notify the user if people inside the house are detected while in Away mode.

Devices to be used

- Mind Cube, Shelly Actuator, Smartphone, Motion Sensor

Non-functional requirements of the use case

- The user should be notified that someone is inside the house in less than 3 seconds.
- PE-08: The maintainer must be able to access and watch a recording in less than one minute.
- PE-09: If requested to, the SIFIS-Home system shall contact law enforcement or private surveillance services to receive assistance in less than 30 seconds.
- PE-10: An abnormal (suspicious) behaviour caused by a malware shall be identified and notified within 60 seconds.
- US-02: The SIFIS-Home system shall be autonomous and learn based on the users' habits, still according to defined privacy policies.
- US-10: An untrained user should be able to recognise a software intrusion in less than one minute.
- DE-04: Record of intrusions must be available for a configurable time (default six months) after the recording.
- DE-05: Identity of the successfully recognized intruders must be available for a configurable time (default six months) after the recording.

Security requirements of the use case

- Only allowed users should receive the notifications.
- Restrict the rights of disabling the alarm.
- SE-03: Personal data stored must be encrypted.
- SE-19: Access to devices functionalities should be protected and controlled.
- SE-20: Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.

Use case in action

- Alert user with notification from SIFIS-Home control panel.
- Control panel shows the cause of the alert in live feed.
- Turn on/off the alert.

Being able to interact with the devices only if authorized by SIFIS

Only users of the house should be able to control the devices inside the house. Also, the users should be notified if no authorized accesses to the devices are detected.

Devices to be used

- Mind Cube, Shelly Actuator, Smartphone.

Non-functional requirements of the use case

- The user should be notified of no authorized accesses in less than 3 seconds.
- PE-14: The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.
- PE-15: The de-registration of a device should be completed in less than 30 seconds.
- PE-16: The correct configuration changes should be propagated successfully in less than 30 seconds.
- PE-17: The current configuration of a device should be retrieved in less than 10 seconds.
- PE18: The marketplace should be accessible in less than 60 seconds.
- US-11: An untrained user should be able to perform the device registration procedure in less than 5 minutes.
- US-12: An untrained user should be able to perform the device de-registration procedure in less than 5 minutes.
- DE-07: The registration of a new device should be successful in at least 99% of the cases.
- DE-08: The de-registration of a new device should be successful in at least 99% of the cases.
- DE-09: The configuration changes should be propagated successfully to the devices in more than 99% of times.

Security requirements of the use case

- Only allowed users should be able to interact with them.
- SE-19: Access to devices functionalities should be protected and controlled.
- SE-20: Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.
- SE-36: Operations related to the creation, configuration, deletion, registration and discovery of security groups shall be secured and shall be allowed only to authorized entities.

Use case in action

- A sound is played from in-home control center where the person at the door can be seen in live camera feed.
- Door can be unlocked from control panel.

Being able to control the house in case of failures

The users should be able to control the house (e.g., turn on/off lights) even if a partial number of smart devices experience a failure and when there is no Internet connectivity.

Devices to be used

- Mind Cube, Shelly Actuator, Smartphone

Non-functional requirements of the use case

- The downtime of the system in case a partial number of smart devices experience a failure should be no more than 5 minutes.
- The user should be notified of a smart device/Internet connectivity failure in less than 5 minutes.
- AV-01: The SIFIS-Home system services and devices shall be available 99% of the time
- AV-02: The SIFIS-Home system shall ensure basic services availability in case of system failures.
- DE-06: Core functionalities should be replicated on multiple devices to avoid single points of failure.
- DE-18: The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.
- RE-01: The system shall not fail more than once a week (in average).
- RE-02: The system shall not take more than one day to be repaired (in average).

Security requirements of the use case

- Only allowed users should receive the notifications.
- Restrict the rights to control based on user levels.
- SE-19: Access to devices' functionalities should be protected and controlled.
- SE-20: Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.
- SE-23: The SIFIS-Home architecture shall be resilient to network-based attacks.
- SE-24: The SIFIS-Home architecture shall be resilient to DoS attacks.
- SE-25: The SIFIS-Home architecture shall be resilient to sybil attacks.
- SE-26: The SIFIS-Home architecture shall be resilient to device compromising attacks.
- SE-27: The SIFIS-Home architecture shall be resilient to Internet connection failure.
- SE-28: The SIFIS-Home architecture shall be resilient to physical device damage or failure.
- SE-29: Devices must have unique identifiers.
- SE-30: Unless thoroughly assessed and acceptable for the specific application, communications in the networked environment shall be secured, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection.
- SE-31: It shall be possible and feasible to provide devices with the necessary key material to establish their security associations and to communicate securely, with preference for automatic procedures.
- SE-39: Devices should be able to detect ongoing (D)DoS attacks based on intensity and distribution of invalid traffic.

Use case in action

- Ability to reboot specific devices from the control panel.
- Restore factory settings remotely.
- Ability to quickly contact relevant maintenance services.

Being alerted if a software attack is detected

The SIFIS-Home system should notify the user if a software attack is detected.

Devices to be used

- Mind Cube, Smartphone

Functional requirements of the use case

- This system's purpose is to alert users if suspicious network traffic is detected, such as traffic generated by malware.
- F-19: The SIFIS-Home system shall detect, identify and disconnect infected devices.
- F-20: The SIFIS-Home system shall notify resident users and administrators when malware is detected.
- F-22: The SIFIS-Home system should allow means of verifying that the malware has not spread to other devices.

Non-functional requirements of the use case

- The user should be notified in less than 3 minutes from the detection of the software attack.
- Suspicious network traffic is detected and notified within 60 seconds.
- Alerts are created within 5 seconds after suspicious traffic is detected.
- AV-01: The SIFIS-Home system services and devices shall be available 99% of the time
- AV-03: Support should be ensured for devices to dynamically react to (D)DoS attacks, by gradually adapting their availability. This includes relying on communication intermediaries for traffic offloading during intense (D)DoS attacks.
- PE-10: An abnormal (suspicious) behaviour caused by a malware shall be identified and notified within 60 seconds.
- PE-11: The user should be informed of the presence of a malware no later than 5 seconds after the malware is recognized.
- PE-12: Self-healing algorithms should be started in less than 60 seconds if available when malware is recognized.
- PE-28: The used solutions for communication and system security shall be as much as possible lightweight to enforce in terms of performance, and especially feasible also for resource-constrained devices.
- PE-29: The performance impact due to communication and system security shall not result in

unacceptable impact on the user experience.

- PE-35: Devices should, if available, utilize low-power modes of operation to further mitigate the performance impact of ongoing (D)DoS attacks.
- US-09: An untrained user should be able to understand that an attack is ongoing in less than a minute from reading the SIFIS-Home alert or notification.
- US-11: An untrained user should be able to perform the device registration procedure in less than 5 minutes.
- DE-06: Core functionalities should be replicated on multiple devices to avoid single points of failure.

Security requirements of the use case

- Only allowed users should receive the notifications.
- SE-22: Analytics shall be able to work with anonymized data when possible.
- SE-29: Devices should be able to detect ongoing (D)DoS attacks based on intensity and distribution of invalid traffic.
- SE-09: The information about the registered devices, their characteristics and their configurations should be stored in a protected database.
- SE-13: Data confidentiality shall be ensured all the time.
- SE-14: The system should not be affected by MITM attacks.
- SE-17: Anomalous device behaviours should be identified and signalled in less than 60 seconds.
- SE-19: Access to devices' functionalities should be protected and controlled.
- SE-20: Access to critical functionalities and services of the SIFIS-Home framework shall be protected and controlled.
- SE-24: The SIFIS-Home architecture shall be resilient to DoS attacks.
- SE-29: Devices must have unique identifiers.
- SE-30: Unless thoroughly assessed and acceptable for the specific application, communications in the networked environment shall be secured, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection.
- SE-39: Devices should be able to detect ongoing (D)DoS attacks based on intensity and distribution of invalid traffic.

Use case in action

- Alert triggers a notification and plays a sound in control panel.
- Ability to turn off certain features: restrict the areas that could be harmed.
- Ability to protect wanted parts of the system with a secure password.

Being alerted if a device is generating anomalous traffic

The SIFIS-Home system should notify the user if a device is generating anomalous traffic.

Devices to be used

- Mind Cube, **TBD**

Non-functional requirements of the use case

- The user should be notified in less than 3 minutes from the detection of anomalous traffic generation.
- PE-10: An abnormal (suspicious) behaviour caused by a malware shall be identified and notified within 60 seconds.
- PE-11: The user should be informed of the presence of a malware no later than 5 seconds after the malware is recognized.
- PE-12: Self-healing algorithms should be started in less than 60 seconds if available when malware is recognized.
- US-09: An untrained user should be able to understand that an attack is ongoing in less than a minute from reading the SIFIS-Home alert or notification.

Security requirements of the use case

- Only allowed users should receive the notifications.
- Only administrative users can do administrative tasks, reducing the risk of hacked accounts to be able to cause damage or remove data/change settings.
- SE-05: The SIFIS-Home system shall prevent data alteration or deletion.
- SE-17: Anomalous device behaviours should be identified and signalled in less than 60 seconds.
- SE-29: Devices should have unique identifiers.
- SE-39: Devices should be able to detect ongoing (D)DoS attacks based on intensity and distribution of invalid traffic.
- SE-52: Personal information recognizable from audio (e.g., name, telephone number, email address, age, physical condition) must be anonymized if the analysis is outsourced to external services.

Use case in action

- Control panel shows a notification which leads to a quick action to restrict the device from others and/or the rest of the SIFIS-Home system.
- Ability to turn off certain features of the device in question (e.g., Internet connection).

Policy definition

The SIFIS-Home system should allow users to define and remove policies through the control panel.

Devices to be used

- Mind Cube, Smartphone, **TBD**

Non-functional requirements of the use case

- The policies should be active at most 3 minutes after their insertion.
- PE-19: The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.
- PE-20: The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.
- PE-21: The list of policies should be retrieved in less than 30 seconds.
- DE-12: The application of policies should always be completed successfully.
- US-16: An untrained user should be able to complete the configuration of policies for groups of devices in less than 5 minutes.
- US-17: An untrained user should be able to complete the configuration of profiles in less than 5 minutes.

Security requirements of the use case

- Only allowed users should be able to define policies.
- Policies should be divided based on user rights levels.
- SE-10: The information about policies should be stored in a protected database.
- SE-12: Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.

Use case in action

- An easy-to-use list of available policies with quick actions to turn them on and off

Policy engine: show that actions are not executed if not allowed (CNR, RIOTS)

The SIFIS-HOME system should block actions (e.g., turn on/off lights) if not allowed by the defined policies. Also, the user should be notified if an action is not carried out due to a violation of the defined policies.

Devices to be used

- Mind Cube, **TBD**

Non-functional requirements of the use case

- The policies should be active at most 3 minutes after their insertion.
- PE-19: The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.
- PE-20: The configuration of policies for groups of devices should be applied and enforced in less than 60 seconds.
- PE-22: The configuration of profiles should be applied and enforced in less than 60 seconds.

- PE-21: The list of policies should be retrieved in less than 30 seconds.
- US-16: An untrained user should be able to complete the configuration of policies for groups of devices in less than 5 minutes.
- US-17: An untrained user should be able to complete the configuration of profiles in less than 5 minutes.
- DE-12: The application of policies should always be completed successfully.

Security requirements of the use case

- Only allowed users should receive the notifications of policy violation.
- Only allowed users should be able to define policies.
- SE-10: The information about policies should be stored in a protected database.
- SE-30: Unless thoroughly assessed and acceptable for the specific application, communications in the networked environment shall be secured, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection.
- SE-36: Operations related to the creation, configuration, deletion, registration and discovery of security groups shall be secured and shall be allowed only to authorized entities.

Use case in action

- Show the blocked action clearly in control center (e.g., a pop-up dialog) and inform user why was it blocked.

Install a third-party application

The SIFIS-Home system should allow users to install/remove third-party applications. The system should indicate the *hazard* level of the third-party applications.

Devices to be used

- Mind Cube, Smartphone, **TBD**

Non-functional requirements of the use case

- The applications should be active at most 3 minutes after their installation.
- PE-19: The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.
- US-15: An untrained user should be able to complete the configuration of policies for groups of users in less than 5 minutes.
- DE-11: The installation of the selected app should be completed successfully in at least 95% of cases.

Security requirements of the use case

- Only allowed users should be able to install/remove applications.

- Restrict installation rights based on application features.
- SE-15: Software and apps shall only be installed with authorisation of the smart home administrator or resident users.
- SE-16: Users must be able to configure and allow the usage of data to the SIFIS-Home framework and third- party software.
- SE-19: Access to devices functionalities should be protected and controlled
- SE-34: Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.

Use case in action

- Should inform user about the third-party applications' features and which device features it would require an access to.

Create different users using the control panel

The SIFIS-Home system should allow the creation/removal of users for a certain house.

Devices to be used

- Mind Cube, Smartphone, **TBD**

Non-functional requirements of the use case

- The user creation process should take less than 5 minutes.
- PE-15: The de-registration of a device should be completed in less than 30 seconds.
- PE-17: The current configuration of a device should be retrieved in less than 10 seconds.
- PE-18: The marketplace should be accessible in less than 60 seconds.
- PE-19: The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.
- PE-22: The configuration of profiles should be applied and enforced in less than 60 seconds.
- PE-23: The change of current profile should be performed in less than 60 seconds.
- PE-25: The statistics about usage of profiles should be presented to the administrator in less than 30 seconds.
- US-13: An untrained user should be able to perform the configuration of devices in less than 5 minutes.
- US-17: An untrained user should be able to complete the configuration of profiles in less than 5 minutes.
- US-18: An untrained user should be able to perform a profile change in less than 30 seconds.
- DE-13: The configuration of profiles should be completed successfully in at least 99% of cases.
- DE-14: The change of current profile should be completed successfully in at least 99% of cases.

Security requirements of the use case

- SE-04: The system shall protect and avoid disclosure of sensitive information.
- SE-05: The SIFIS-Home system shall prevent data alteration or deletion.
- SE-08: Log-in information should be stored in a protected database.
- SE-11: The information about user profiles and configuration aspects should be stored in a protected database.

Use case in action

- Ability to add users by providing certain information (e.g., email, phone number).
- Ability to choose new user's rights (should not be higher user rights level than the current account).

Voice commands

The SIFIS-Home system should allow the users to control the house using voice commands.

Devices to be used

- Mind Cube, **TBD**

Non-functional requirements of the use case

- Voice commands should be executed in less than 10 seconds.
- PE-01: The user authentication shall happen in less than 2s.
- PE-02: The user recognition (identification/biometric based) shall happen in less than 5s.
- PE-03: Biometric-based authentication should be performed in less than 5 seconds
- PE-04: Activation of features based on user identity (biometric recognition) should be performed in less than 5 seconds.
- PE-05: Recognition of the start of an interaction through voice command should be performed in less than 2 seconds.
- PE-06: The interpretation of the voice commands provided by the user should be performed in less than 2 seconds.
- PE-07: A command should be invoked within 5 seconds from the event that triggered its execution.
- DE-01: The identification through biometrics should be performed correctly in more than 95% cases.
- US-09: An untrained user should be able to understand that an attack is ongoing in less than a minute from reading the SIFIS-Home alert or notification.

Security requirements of the use case

- Voice commands are not executed if the house is in away mode.
- Voice commands are not stored on the devices.
- Anonymization of the recorded commands should be performed.
- SE-07: Biometrics must be stored safely in the SIFIS-Home database.
- SE-13: Data confidentiality shall be ensured all the time.
- SE-50: The identity of the speaker should not be identifiable if the analysis is outsourced to external services.
- SE-51: The background noises in the audio streams must be anonymized if the analysis is outsourced to external devices.

Use case in action

- Ability to give voice commands from the control center.

Face recognition

A SIFIS-Home house should go from Away to In-House mode when the face of a user of the house is recognized.

Devices to be used

- Mind Cube, **TBD**

Non-functional requirements of the use case

- Face recognition should take no more than 10 seconds.
- PE-01: The user authentication shall happen in less than 2s.
- PE-02: The user recognition (identification/ biometric based) shall happen in less than 5s.
- PE-03: Biometric-based authentication should be performed in less than 5 seconds
- PE-04: Activation of features based on user identity (biometric recognition) should be performed in less than 5 seconds.
- US-08: The image-based identification through biometrics in a room (interior) or in an open space (exterior), without obstacles or face covering elements, it should be performed by the system in a radius of at least 10 meters from the device.

Security requirements of the use case

- Images are not stored on the devices.
- SE-07: Biometrics must be stored safely in the SIFIS-Home database.

- SE-13: Data confidentiality shall be ensured all the time.
- SE-31: It shall be possible and feasible to provide devices with the necessary key material to establish their security associations and to communicate securely, with preference for automatic procedures.
- SE-34: Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.

Use case in action

- Notification on the control panel when the mode has changed. Ability to switch between different modes if available.

Parental control

The SIFIS-Home system should be able to recognize the age of the users in a certain room to be able to execute parental control (e.g., turn off the TV if the current TV program is not good for children).

Devices to be used

- Mind Cube, **TBD**

Non-functional requirements of the use case

- Age estimation of users should take less than 10 seconds.

Security requirements of the use case

- Images are not stored on the devices.
- SE-07: Biometrics must be stored safely in the SIFIS-Home database.
- SE-08: Log-in information should be stored in a protected database.
- SE-15: Software and apps shall only be installed with authorisation of the smart home administrator or resident users.
- SE-31: It shall be possible and feasible to provide devices with the necessary key material to establish their security associations and to communicate securely, with preference for automatic procedures.
- SE-34: Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.

Use case in action

- Ability to add ages for user profiles if available which would make the parental control easier, faster and adds a better level of security than handling images.

Listening to 3rd party devices via SIFIS interfaces

The SIFIS-Home system should be able to communicate with other manufacturer devices via protocols

defined in earlier work packages (WP5: MQTT, WebThings)
Sensative Strips can be used to detect water leak.

Devices to be used

- Sensative Strips

Non-functional requirements of the use case

- Indication of water leak should be visible in less than 5 seconds after water leak occurred
- PE-19: The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.
- US-15: An untrained user should be able to complete the configuration of policies for groups of users in less than 5 minutes.
- DE-11: The installation of the selected app should be completed successfully in at least 95% of cases.

Security requirements of the use case

- The communication between the sensors and the system should be secure.
- SE-09: The information about registered devices, their characteristics and their configurations should be stored in a protected database.
- SE-12: Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.
- SE-17: Anomalous device behaviours should be identified and signalled in less than 60 seconds.
- SE-20: Access to devices' functionalities should be protected and controlled.
- SE-31: It shall be possible and feasible to provide devices with the necessary key material to establish their security associations and to communicate securely, with preference for automatic procedures.
- SE-34: Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.

Use case in action

- Control center should inform users with a badge or similar feature of third-party devices compared to SIFIS-Home devices.

Controlling 3rd party devices via SIFIS-Home interfaces

The SIFIS-Home system should be able to communicate with other manufacturer devices via protocols defined in earlier work packages (WP5: MQTT, WebThings). Riots Thermostat is used to control temperature of a home. Requested temperature can be changed from the control panel.

Devices to be used

- Riots Thermostat

Non-functional requirements of the use case

- Operation should happen in less than 5 second after issuing the command.
- PE-01: The user authentication shall happen in less than 2s.
- PE-02: The user recognition (identification/ biometric based) shall happen in less than 5s.
- PE-03: Biometric-based authentication should be performed in less than 5 seconds.
- PE-07: A command should be invoked within 5 seconds from the event that triggered its execution.
- PE-13: The registration of a new device should be completed in less than 30 seconds.
- PE-14: The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.
- PE-15: The de-registration of a device should be completed in less than 30 seconds.
- US-11: An untrained user should be able to perform the device registration procedure in less than 5 minutes.

Security requirements of the use case

- The communication between the actuators and the system should be secure.
- SE-12: Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.
- SE-16: Users must be able to configure and allow the usage of data to the SIFIS-Home framework and third-party software.
- SE-34: Source authentication of protected messages shall be ensured, also in a group communication setup where one-to-many messages are exchanged.

Use case in action

- Provide similar UI controls as compared to SIFIS-Home devices, but the management of third-party devices should be visually or logically separated from them.

Access privileges to physical resources

Eligible users must be able to access the physical and tactile resources in addition of their settings in SIFIS-Home app or control panel.

Devices to be used

- Mind Cube, Shelly Actuator, Smart doorbell, Riots Mama, Riots Thermostat, Smartphone, Raspberry Pi

Non-functional requirements

- PE-14: The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.

- PE-17: The current configuration of a device should be retrieved in less than 10 seconds.
- PE-20: The configuration of policies for groups of devices should be applied and enforced in less than 60 seconds.
- PE-21: The list of policies should be retrieved in less than 30 seconds.
- RE-01: The system shall not fail more than once a week (in average).
- US-01: The system shall be easy to use for users with no technical background.
- US-05 The SIFIS-Home hardware components should be easy to use for the elderly and users with no engineering background.
- US-07 Proper and easy hardware installation should be considered.
- US-11 An untrained user should be able to perform the device registration procedure in less than 5 minutes.
- DE-06 Core functionalities should be replicated on multiple devices to avoid single points of failure.
- DE-07 The registration of a new device should be successful in at least 99% of the cases.
- DE-18: The SIFIS-Home system is required to be fault tolerant, it should continue to operate, even if one or more of the nodes fail.

Security requirements of the use case

- SE-02: APIs for the communication with external devices must be secured.
- SE-09: The information about the registered devices, their characteristics and their configurations should be stored in a protected database.
- SE-19: Access to devices functionalities should be protected and controlled.
- SE-28: The SIFIS-Home architecture shall be resilient to physical device damage or failure.
- SE-40: The system shall provide a means to enforce flexible, fine-grained and reactive authorized access control for devices to access remote resources at other devices.
- SE-42: The system shall provide a means for enabling devices to get agile and possibly automatic notification, in order to signal pertaining access credentials that have been revoked while still unexpired.
- SE-49: Definition of a template for each type of device which describes the features of the specific type of device.

Use case in action

- Ensure that each device is accessible by the users who are eligible to access them.

Access device's configurations

The settings must be based on the privileges of the user account. Each account is only allowed to see and control the settings they are eligible to modify.

Devices to be used

- Mind Cube, Shelly Actuator, Smart doorbell, Riots Mama, Riots Thermostat, Smartphone

Non-functional requirements

- PE-14: The list of registered devices shall be shown by the SIFIS-Home system in less than 30 seconds.
- PE-17: The current configuration of a device should be retrieved in less than 10 seconds.
- PE-18: The marketplace should be accessible in less than 60 seconds.
- PE-20: The configuration of policies for groups of devices should be applied and enforced in less than 60 seconds.
- PE-21: The list of policies should be retrieved in less than 30 seconds.
- RE-01: The system shall not fail more than once a week (in average).
- AV-01: The SIFIS-Home system services and devices shall be available 99% of the time.
- US-01: The system shall be easy to use for users with no technical background.
- US-04: The SIFIS-Home system shall preserve consistency among all devices, related database and constraints.
- US-13: An untrained user should be able to perform the configuration of devices in less than 5 minutes.
- US-19: An untrained user should be able to access the statistics for visualizing and interpreting them in less than 5 minutes.
- DE-06: Core functionalities should be replicated on multiple devices to avoid single points of failure.
- DE-08: The de-registration of a new device should be successful in at least 99% of the cases
- DE-09: The configuration changes should be propagated successfully to the devices in more than 99% of times.
- DE-10: The SIFIS-Home system should be able to restore the previous configurations if there are errors in applying configuration changes.

Security requirements of the use case

- SE-01: APIs for the communication with internal devices must be secured.
- SE-02: APIs for the communication with external devices must be secured.
- SE-09: The information about the registered devices, their characteristics and their configurations should be stored in a protected database.
- SE-11: The information about user profiles and configuration aspects should be stored in a protected database.
- SE-13: Data confidentiality shall be ensured all the time.
- SE-19: Access to devices functionalities should be protected and controlled.

- SE-30: Unless thoroughly assessed and acceptable for the specific application, communications in the networked environment shall be secured, by ensuring confidentiality/integrity/authenticity of messages, as well as protecting from replay protection.
- SE-42: The system shall provide a means for enabling devices to get agile and possibly automatic notification, in order to signal pertaining access credentials that have been revoked while still unexpired.

Use case in action

- Provide an interface for accessing a list of devices which are available for the user and to further access their settings based on the user's rights.

Availability of services and applications

To make the user experience smooth and logical, users only need to see what they are allowed to see. Based on user rights, the more there are choices the better rights the user has. This way there are a minimal number of possible errors, considering the user knows what they are doing. Maintainers and controllers can restrict access to services and applications based on users and their profiles.

Devices to be used

- Mind Cube, Shelly Actuator, Smart doorbell, Riots Thermostat

Non-functional requirements

- PE-02: The user recognition (identification/biometric based) shall happen in less than 5s.
- PE-03: Biometric-based authentication should be performed in less than 5 seconds.
- PE-04: Activation of features based on user identity (biometric recognition) should be performed in less than 5 seconds.
- PE-07: A command should be invoked within 5 seconds from the event that triggered its execution.
- PE-18: The marketplace should be accessible in less than 60 seconds.
- PE-20: The configuration of policies for groups of devices should be applied and enforced in less than 60 seconds.
- PE-21: The list of policies should be retrieved in less than 30 seconds.
- US-14: An untrained user should be able to perform the installation of an application in less than 5 minutes.
- US-22: The list of applications running on each device should be available to MLADS.
- DE-11: The installation of the selected app should be completed successfully in at least 95% of cases.

Security requirements of the use case

- SE-09: The information about the registered devices, their characteristics and their configurations should be stored in a protected database.

- SE-11: The information about user profiles and configuration aspects should be stored in a protected database.
- SE-12: Data paths should be identified to allow data tracking and detect data leaving the smart-home perimeter, according to policies.
- SE-13: Data confidentiality shall be ensured all the time.
- SE-19: Access to devices functionalities should be protected and controlled.

Use case in action

- Provide an interface for accessing the applications and services that are available for each of the devices which the user has rights to access.
- Provide a way to add or remove user rights for specific services and applications.

6. Acceptance tests for the use cases

Following acceptance tests (Table 4) have been defined for the use cases listed in previous chapter. Each test case is tested to verify that the requirements are met.

Test ID	**Use case #**	**Test description**	**Expected result**
AT6_1	6_1 Turn on/off lights using the control panel	Turn off the lights from control panel	Lights turn off in 1 second
AT6_2	6_2	Turn on the lights from control panel	
AT6_3	Being notified if someone is at the doorbell	Show a notification on control panel	Notify user on the control panel or app.
AT6_4	Turn on/off lights pressing and releasing buttons	Turn on/off the lights on control panel and/or mobile app	Lights turn on/off in 1 second depending on their initial state.
AT6_5	Being alerted if motion sensors detect people presence while the House is in away mode	The smart home administrator must be notified as soon as an unauthorized person has accessed the smart home or a dangerous situation is detected.	The user should be notified that someone is inside the house in less than 3 seconds.
AT6_6	Being able to interact with the devices only if authorized by SIFIS	Only show devices which the user is eligible to see.	Show a list of available devices
AT6_7	Being able to control the house in case of failures	Provide control over different events of failure	The user should be notified of a smart device/Internet connectivity failure in less than 5 minutes.
AT6_8	Being alerted if a software attack is detected	The smart home administrator must be notified as soon as a software	An abnormal (suspicious) behavior caused by a malware shall be identified

		intrusion is detected in the smart home system.	and notified within 60 seconds.
AT6_9	Being alerted if a device is generating anomalous traffic	The smart home administrator must be notified as soon as a software intrusion is detected in the smart home system.	An abnormal (suspicious) behavior caused by a malware shall be identified and notified within 60 seconds.
AT6_10	Policy definition	Provide user with a list of policies and control for enabling or disabling them.	The configuration of policies for groups of users should be applied and enforced in less than 60 seconds.
AT6_11	Policy engine: show that actions are not executed if not allowed	Show an error if an action is forbidden from the user.	Only allowed users should receive the notifications of policy violation.
AT6_12	Install a third-party application	Provide ways to install a third-party app in the marketplace.	Display third-party apps in marketplace if they are compatible with SIFIS-Home.
AT6_13	Create different users using the control panel	The actor must have the possibility to create a new user profile assigning them custom privileges and the device and application allowed.	Provide settings for adding new users.
AT6_14	Voice commands	The actor can authenticate to the SIFIS-Home framework using their voice.	Provide ways to give voice commands and provide an action based on the command.
AT6_15	Voice commands	The actor can manage the smart home components through voice commands.	Provide ways to give voice commands and provide an action based on the command.
AT6_16	Face recognition	Ability to recognize a face in camera view.	Recognizes a face from camera feed or an image.
AT6_17	Parental control	Ability to restrict certain ages from certain content/devices.	Provide a setting for age limits in device and/or app settings.
AT6_18	Controlling 3rd party devices via SIFIS-Home interface	The SIFIS-Home framework must allow the installation of a third-party application that matches the smart home policies.	Provide settings for adding/removing and controlling third-party devices.
AT6_19	Access privileges to physical resources	Restrict and allow access to individual devices.	Ensure the installed devices are not available for everyone.
AT6_20	Access device’s configurations	User can only access configurations they are eligible to modify and see.	User can only reach configurations if they are allowed.
AT6_21	Availability of services and	Show services and	User can only see content

	applications	applications based on user profiles and rights.	that is relevant to them based on their profile.

Table 4. Acceptance tests of use cases.