Integrated cyber-physical security for health services

Specification of Mobile Alerting System

Deliverable 4.7

Lead Author: LINKS

Contributors: MS, CSI, ASLTO5

Deliverable classification: PU

Co-funded by the Horizon 2020 Framework Programme of the European Union

Version Control Sheet

Title	*Specification of Mobile Alerting System*
Prepared By	*LINKS*
Approved By	*Marco Gavelli*
Version Number	*1.0*
Contact	marco.gavelli@linksfoundation.com

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
0.1	5/11/2019	Initial version	MG	MG
0.2	15/11/2019	Added Mock-ups	MG	MG
0.3	25/11/2019	Merged contributions	MG	MG
0.5	2/12/2019	Final draft	MG	MG
0.7	10/12/2019	Ready for review	MG	MG
0.9	16/12/2019	Incorporated corrections and comments from reviewers EB, BN, MJN	MG	MG
1.0	17/12/2019	Final version	MG	MG

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 787002.

Table of Contents

List of Figures

List of Tables

LIST OF ACRONYMS

BTMS	Building Threat Monitoring System
CDB	Central Database
DoA	Description of Action
DXL	Data eXchange Layer
HTTPS	Hypertext Transfer Protocol over SSL
JSON	JavaScript Object Notification
JWT	JSON Web Token
Iframe	InlineFrame
IPM	Impact Propagation Module
LDAP	Lightweight Directory Access Protocol
MAS	Mobile Alerting System
MQTT	Message Queuing Telemetry Transport
REST_API	Representational State Transfer Application Program Interface
SDK	Software Development Kit
SOC	Security Operations Center

1 The SAFECARE Project

Over the last decade, the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons to impact the population. As Europeans, we know now that we must increase our awareness against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analysed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats. Health services are at the same time among the most critical infrastructures and the most vulnerable ones. They are widely relying on information systems to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this project is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It will promote new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. The project will also participate in increasing the compliance between security tools and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find customers across Europe.

2 Executive Summary

This deliverable is part of the SAFECARE work package on physical security solutions (WP4). It covers the specification of the Mobile Alerting System (MAS) for implementing an integrated alert system to improve reaction times and enrich the communication infrastructure in case of physical threats. The specification is based on the requirements detailed in the Description of Action (DoA) and on new needs emerged in the course of work in the project. The Mobile Alerting System is formed of: a server module which is interconnected with SAFECARE modules; and a mobile application running on mobile devices (smartphone and tablet).

The deliverable provides an overview of the MAS architecture and then details the server components and the Mobile Application. The server component specification describes the interactions with other SAFECARE modules, how user authentication is managed and the defined data exchanged format used. Mobile Application specification provides a description of the user interfaces, data visualization paths and mock-up of overall solution.

Finally, the deliverable considers the proposed solution in the context of the scenarios at the SAFECARE demonstrations sites.

3 Introduction

The goal of the SAFECARE project is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. Smartphone and tablets are powerful computing devices, network-connected, constantly available, and low cost, therefore they are a perfect tool for the SAFECARE system.

A building security agent with a smartphone has the ability to quickly report specific categories of security threats or alerts related to a specific failure point in a hospital (system failure, natural hazard, terrorist attack, etc.). See Figure 1

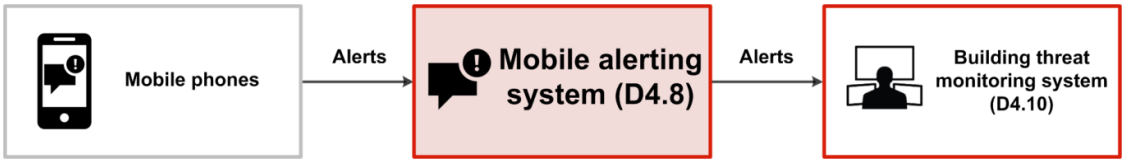

Figure 1: Mobile alerting system sending alerts

The data is securely transferred to SAFECARE modules, which will act based on the information to elaborate the best threat response. According to users' profiles (e.g. organization, role), operators will be quickly notified with the information needed to manage the incident (emergency procedures, geolocation, relevant multimedia data). See Figure 2

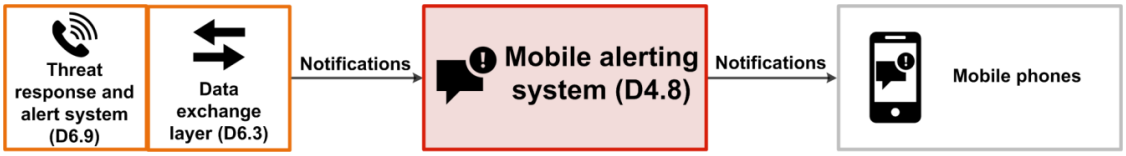

Figure 2: Mobile alerting system receiving notifications

The MAS will also offer a functionality to quickly address security issues discovered by other physical security components (e.g. Video Management System) implementing a distributed security operations center. Once a suspicious behaviour is detected by a WP4 component the alert is sent to the MAS, which notifies a building security agent to validate the alert into an incident. The validation is then transmitted to SAFECARE modules. See Figure 3

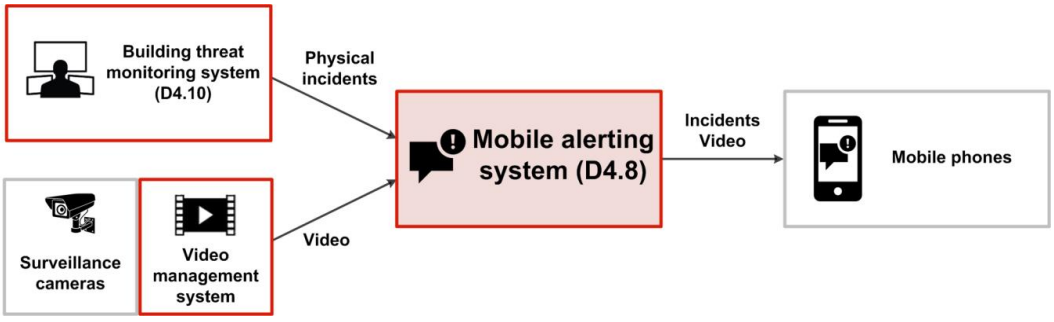

Figure 3: Mobile alerting system receiving physical incidents

The Mobile Alerting System will provide its functionalities by means of its two modules:

- the server component which interacts with the other SAFECARE modules and manages secure and authenticated connections with mobile devices
- the Mobile Application which interacts with the user and visualizes contextual information

In the next section the requirements of the system are reviewed with respect to DoA and needs emerged during the course of the project. In Section 5 a description of the information flow is provided. In Section 6, the global architecture is presented as well as each component of the MAS. In Section 7, the Mobile Application wireframes are illustrated. In Section 8, the system interconnections to the physical security systems, and the integrated cyber-physical security systems are discussed. In Section 9, is presented an analysis on how the solution can help handle the scenarios of threat described in deliverable D3.6.

4 Requirements

This sections illustrates the requirements defined for task 4.4.

4.1 DoA

From the description of T4.4 in the DoA the MAS has the following requirements:

1. Provide ability to quickly report specific categories of security threats or impacts correlated to a specific failure point, such as a hospital (e.g. system failure, natural hazard, terrorist attack...)
2. Visualize contextual information (e.g. geolocation, building, room, timestamp and any relevant multimedia data).
3. The mobile alerting system will store incidents and alerts in the central database and will also be in charge of displaying heterogeneous alerts coming from the central database.
4. Depending on users' profiles (e.g. organization, role and site affectation) specific filters will be applied in order to display only relevant alerts.
5. As a result of T2.6, close attention will be paid to privacy and ethics constraints. A specific focus will address system interoperability and data exchange standards.

Furthermore, in T6.5 a requirement to the mobile alerting system is stated as well that says: the system will be interconnected to the mobile alerting system (T4.4) as well as conventional communication means such as phone calls, SMS, emails and social networks.

4.2 Project's evolution

During the course of the project, WP4 leader requested that the following interactions would be made available to the mobile users:

1. to visualize the output of the impact propagation model (D6.4) in order to evaluate potential cascading effects;
2. to allow for manual acknowledgement of automatic alerts, to send acknowledged incidents into the central database.

Regarding the first point (1), the MAS will implement the visualization of the impact propagation model on the Mobile App and on the BTMS server using an iframe (described in the following section).

Regarding the second point (2), MAS will implement a functionality to automatically notify alerts to building security agents that will be in charge of validating them into incidents based on their judgement. The result of the validation will then be transmitted to the BTMS.

5 Information flow

In Figure 4 is depicted the sequence diagram between the SAFECARE modules when a security personnel is reporting an incident on the Mobile App.

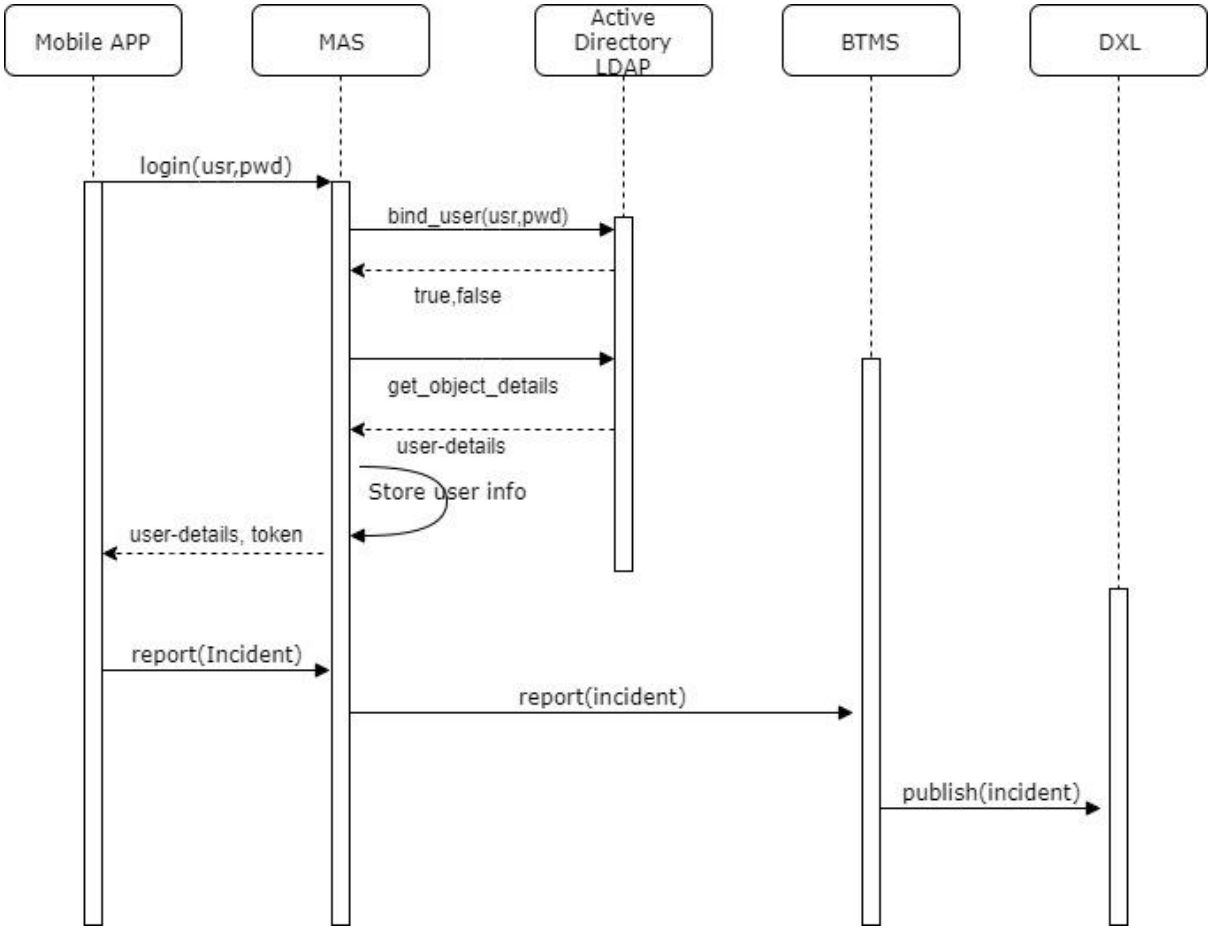

Figure 4: Mobile alerting system reporting incidents

Hereafter the interactions to report an incident are described in a sequential order:

1. User opens Mobile App and logs into the system providing his credentials.
2. Credentials are verified by an authentication server.
3. Once the user is authenticated, the MAS retrieves the user profile (email, user classification) and stores it in a local database for future use.
4. User-details, token and app data (list of hospital assets) are sent to the Mobile App
5. When a building security agent detects a threat, he opens the Mobile App, fills a form with hazard information and reports the incident to the MAS.
6. The MAS reports the incident to the BTMS.
7. The BTMS publishes the incident on the DXL.

The following sequence diagram describes the interchanges between the SAFECARE modules and the Mobile Alerting system.

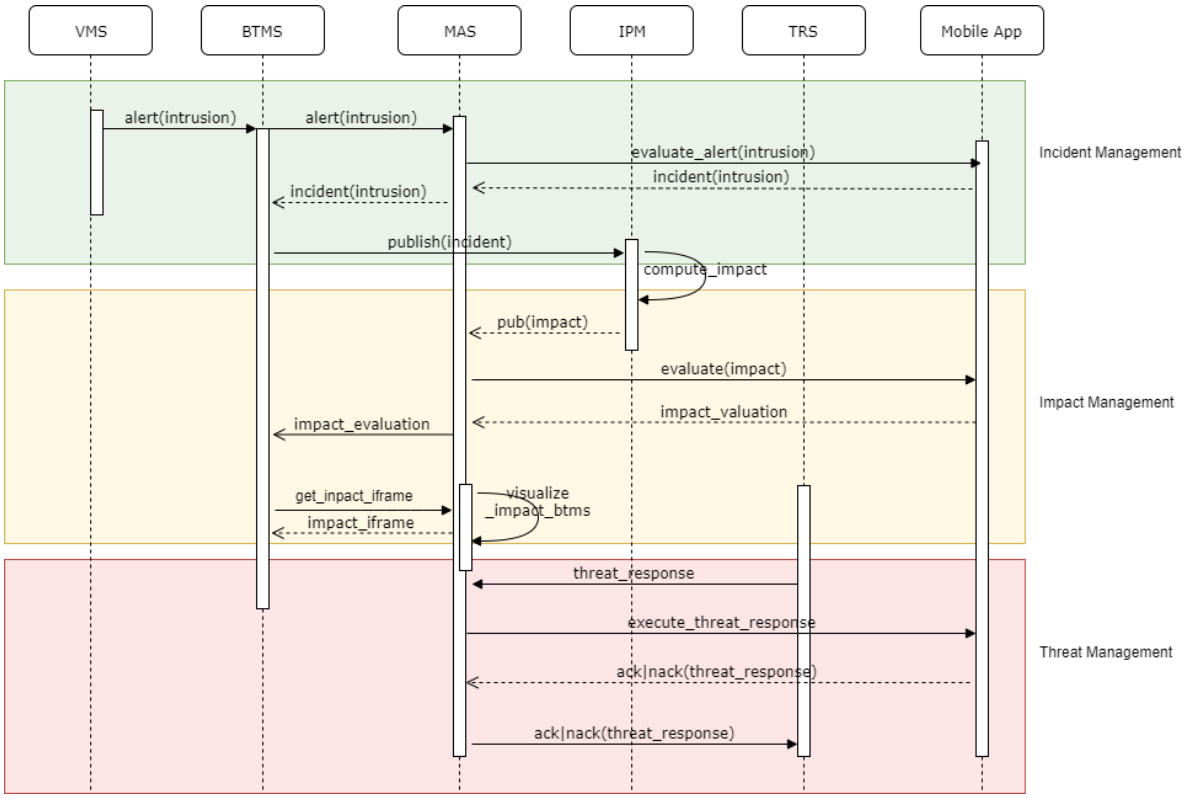

Figure 5: Mobile alerting system interactions with other SAFECARE modules

Hereafter the interactions between SAFECARE modules are described in a sequential order:

1. The VMS discovers a suspicious behaviour; it sends the alert to the BTMS for evaluation.
2. The BTMS forwards the alert to the MAS for manual acknowledgement.
3. The MAS looks at the stored user profile and extracts the SOC operator to validate the alert.
4. The MAS pushes the alert to the Mobile App.
5. The Mobile App shows the alert data (location, alert information, video) to the security operator who decides if the alert is an incident. The result of the evaluation is sent to the MAS.
6. The MAS transmits the evaluation to the BTMS.
7. In case of an incident the BTMS publish incident on the DXL.
8. The IPM receives the incident and computes the impact propagation model.
9. The IPM publishes the impact on the DXL.
10. The MAS receives the impact.
11. The MAS looks at the stored user profile and extracts the SOC operator to validate the impact.
12. The MAS pushes the impact to the Mobile App.

13. The Mobile App shows impact propagation model to building security guard. The result of the evaluation is sent to the MAS.
14. The MAS prepares an iframe[1] with the impact model visualization and notifies the BTMS.
15. The BTMS might apply fall-back strategies.
16. The TRS publishes a threat response notification containing an emergency procedure and other relevant recipients on the DXL.
17. The MAS receives the message and extracts the relevant recipient's identifiers. The identifiers are used to push the data to the corresponding mobile devices.
18. The Mobile App shows the TRS data to the building security agent, who acknowledges it if the person can execute the emergency plan. The result of the evaluation is sent to the MAS.
19. The MAS informs the TRS whether relevant recipients can or cannot execute the reaction plan.

6 Mobile Alerting System Architecture

Figure 6 depicts the architecture of the Mobile Alerting System and how the MAS is interconnected with the others SAFECARE modules. The MAS is represented by yellow blocks.

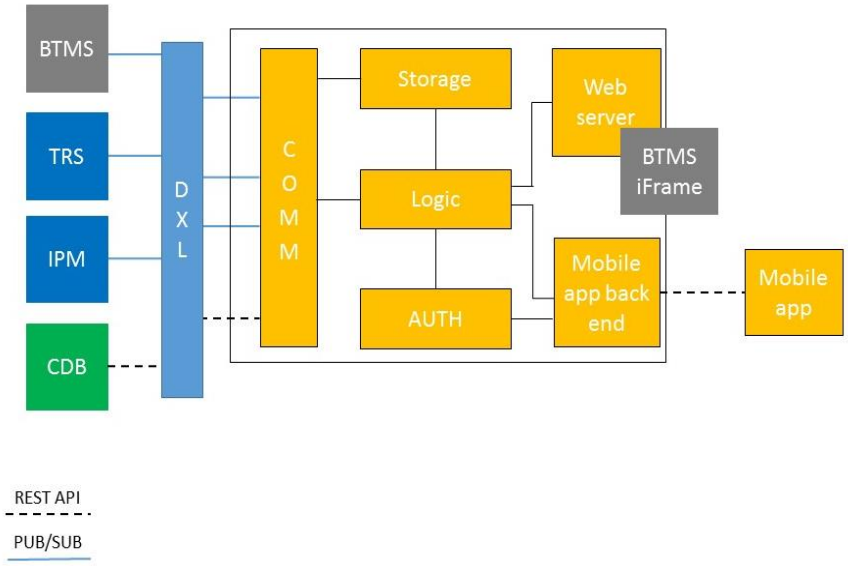

Figure 6: MAS Architecture

As per the requirements and per the SAFECARE global architectures, the MAS is connected to the Building Threat Management System, the Threat Response System, the Impact Propagation Module and the Central Database through the Data Exchange Layer. The MAS receives static data (about hospital assets and resources) from the Central Database via a REST-API, while the dynamic data (alerts, threat response, impact) is transmitted to and from the DXL via a PUB/SUB messaging pattern. The Mobile App runs on mobile devices and communicates to the MAS server via a REST-API.

The MAS server side consists of the following components:

[1] An IFrame is an HTML element that allows an external webpage to be embedded in an HTML document.

- **COMM**, which implements the communication layer between the DXL and the rest of the MAS. It is the gateway of the MAS with the "external world", enabling the communication through MQTT, subscribing and publishing to the topic of interest (Alert, Impact, Threat Response System). More information on the topics can be found in Section 8. Moreover, it also handles the connection to the Central Database, through API, retrieving the static data that will be used for visualizing the information on the Mobile App.

- **Storage** consists in a utility component which acts as a storage for all the information that needs to be kept like: User profiles, Past Events (alerts, incidents, etc.),) and Phone Identifiers (needed for the targeted notifications).

- **Auth**, which manages user authentication, integrating with the hospital authentication server. This component will be integrated with an Identity Management (e.g. Keycloak) that will proxy the authentication requests to the hospital authentication server (e.g. LDAP) exposing a more modern functionality like Token Based Authentication.

- **Logic**, is actually the actual core of the server, it will implement all the rules and constraints for handling the messages from the SAFECARE modules to the Mobile App and the messages from the Mobile App to the SAFECARE modules.

- **Web server**, is a canonical WebServer (implemented in Python) which handles the impact visualization inside the the iframe.

- **Mobile app back end**, exposes the REST-API, secured with HTTPS protocol, that will be called by the Mobile App for communicating with the SAFECARE modules. It has a strong connection with the Auth module because all the API requests will contain a token (JWT) that needs to be validated with the Identity Management. The communication between the mobile back end and the app will be done using **push notification** SDK (Firebase), giving the means to the back end to send messages containing text or other data to the Mobile App.

7 Mobile app mock-up

The section describes the graphical user interface of the Mobile Application. For each mock-up is reported the description of the implemented functionality.

7.1 Login

The Figure 7 shows how the application will look like when it is opened for the first time. It consists of a standard login form where the user enters *username* and *password*. The only difference is the dropdown menu that lets the user selects the hospital in which he works, for this project it will be ASL Torino 5 (ASLTO5), Assistance Publique-Hopitaux Marseille (APHM) and Academisch Medisch Centrum bij de Universiteit van Amsterdam (AMC).

The user will not need to login each time the user opens the application, but only the first time.

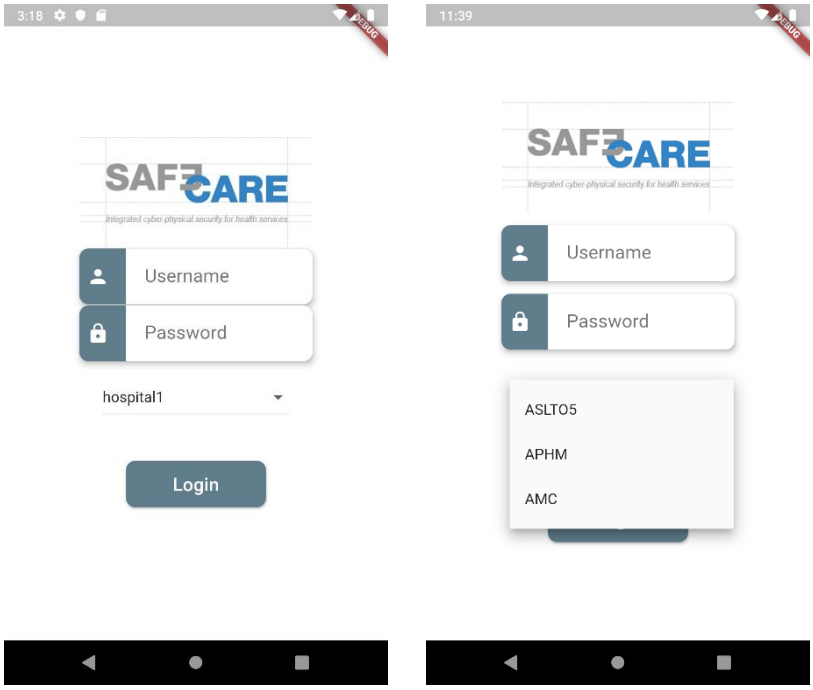

Figure 7: Login Screen

7.2 Main Screen

The two screens in **Error! Reference source not found.Error! Reference source not found.** sh ow the main page of the application, the five sections of the first screen represent the core capability of the Mobile Application:

1. Report an incident.
2. Visualize the response to a threat.
3. Manage the alerts.
4. Visualize and evaluate incidents.
5. Visualize the impacts[2].

It is also possible to see the drawer, which can be accessed by *swiping* from left-to-right, that shows the information of the logged user.

[2] At the moment of writing this deliverable it is not sure if the impacts have to been shown on the Mobile Application.

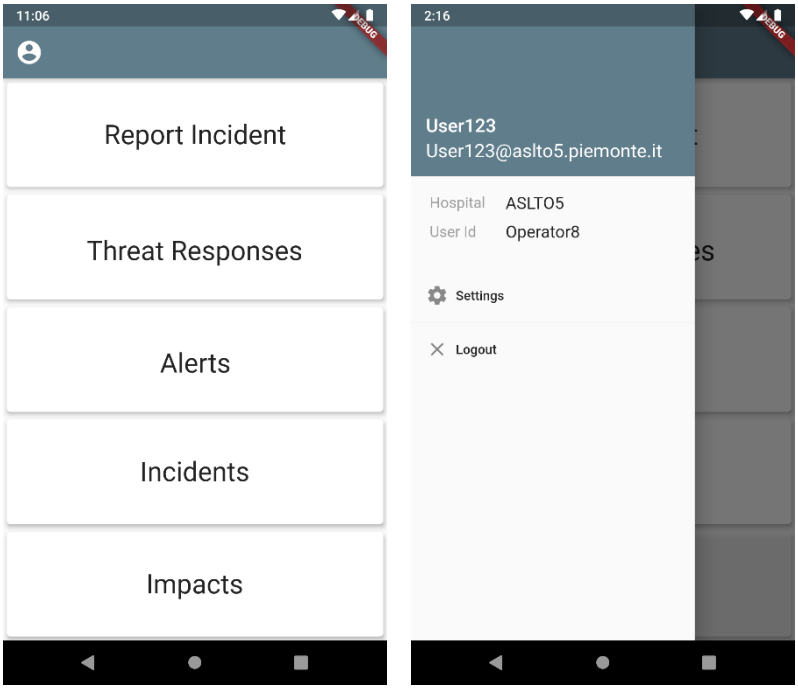

Figure 8: Main Mobile App screens

7.3 Report incident

The screens in Figure 9 shows how the interface for reporting an incident will look like. The top-left screen shows the possible incident classes. Once the appropriate one is selected, a new screen will be shown, as shown in the three other screens. The screen contains the fields that needs to be filled in order to report an incident. It is necessary to point out that depending on the chosen incident class the type of information can change. The information for each incident class as well as the incident classes themselves are to be considered as placeholders for demo purposes and they will be updated based on the future user requirements.

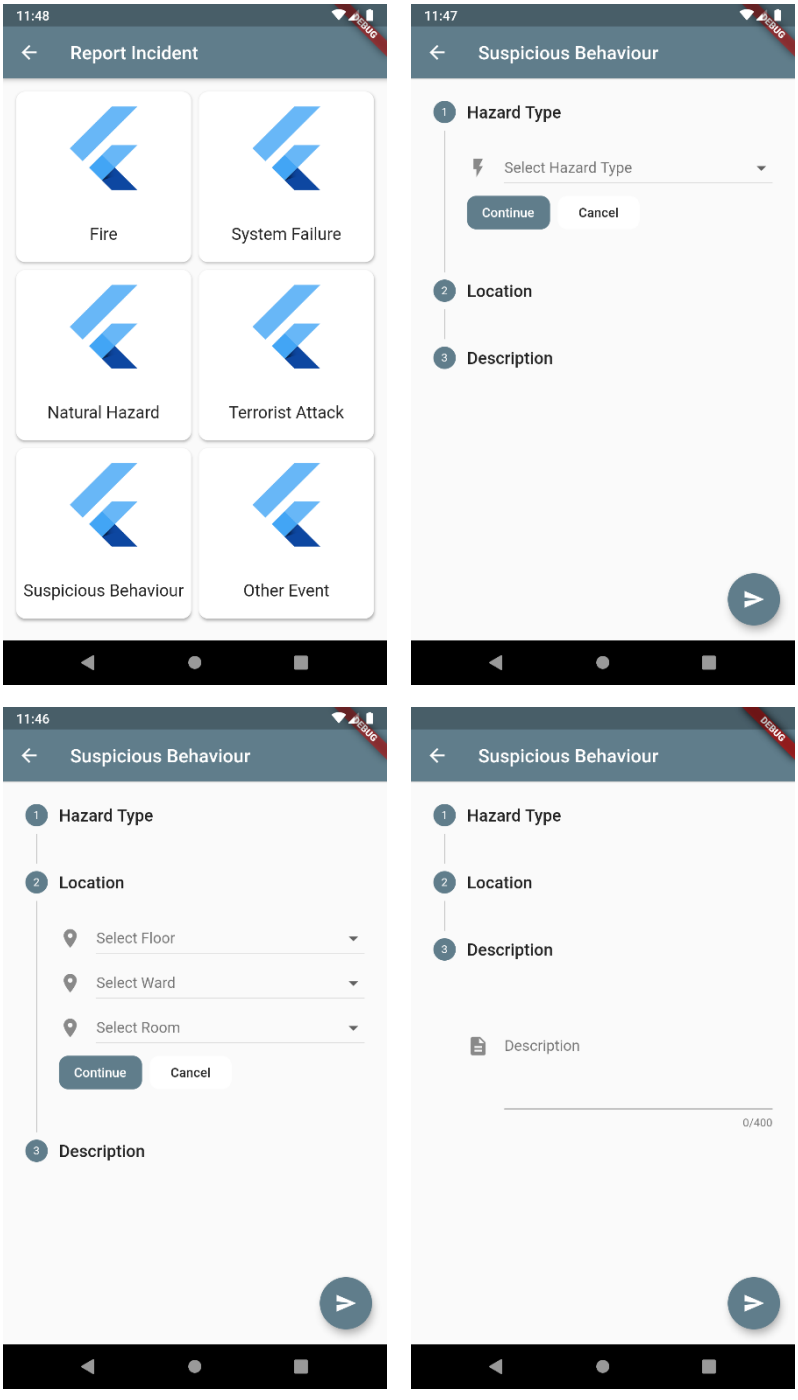

Figure 9: Report Incident

7.4 Alert evaluation

To access the Alert Evaluation screen, the user can either click on the notification displayed upon receiving a new alert (left screen of Figure 10) or by navigating to the Alerts page from the home page and selecting one of the alerts of the list (right screen of Figure 10).

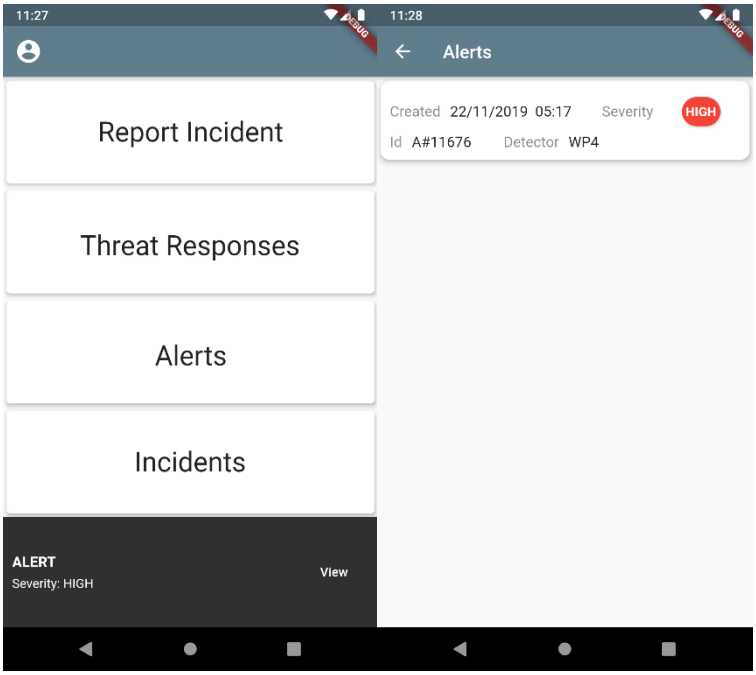

Figure 10: Alert evaluation

Inside the Alert Details Screen (Figure 11) are visualized the information (severity of the alert, component who generated it, etc.) of the alert and the events that generated it. By clicking on a single event inside the alert, detailed information (textual or video) is displayed (middle screen of Figure 11).

For each alert, at the bottom of the screen, buttons can be found to confirm, reject or pass the alert to another operator.

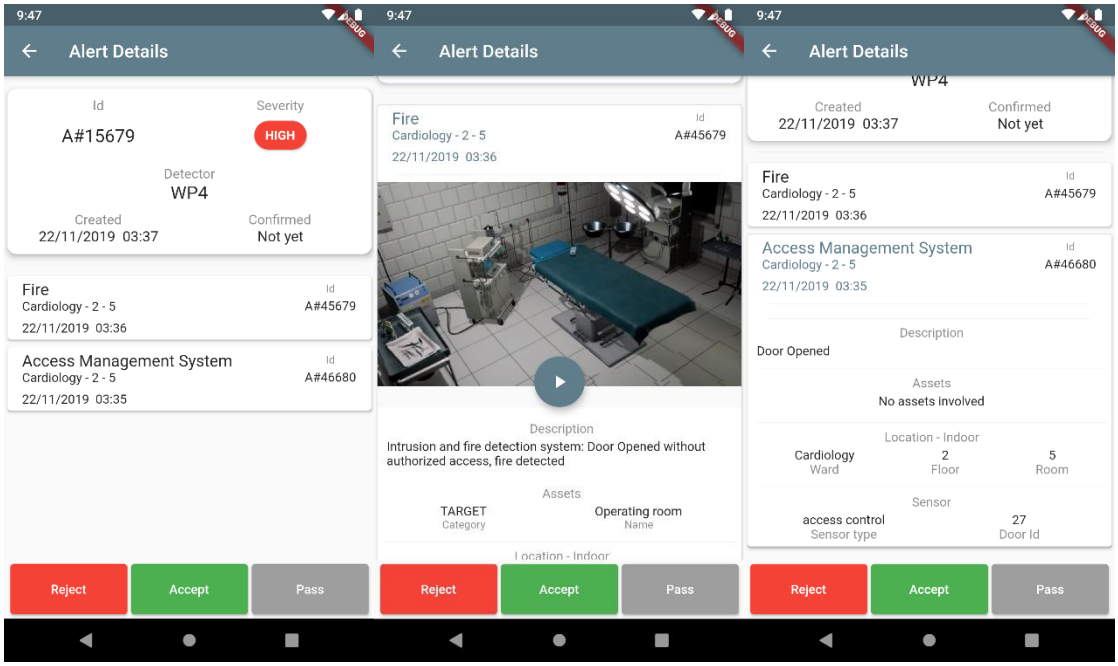

Figure 11: Alert Details Screen

7.5 Incident history

Alerts evaluated to incidents by the Mobile App users (left screen) and incidents created directly by the Mobile App users are separated into two tabs (middle screen). In the second screen is present the list of the past incidents. By clicking on one of them it is possible to have more detailed information on it (right screen). See Figure 12.

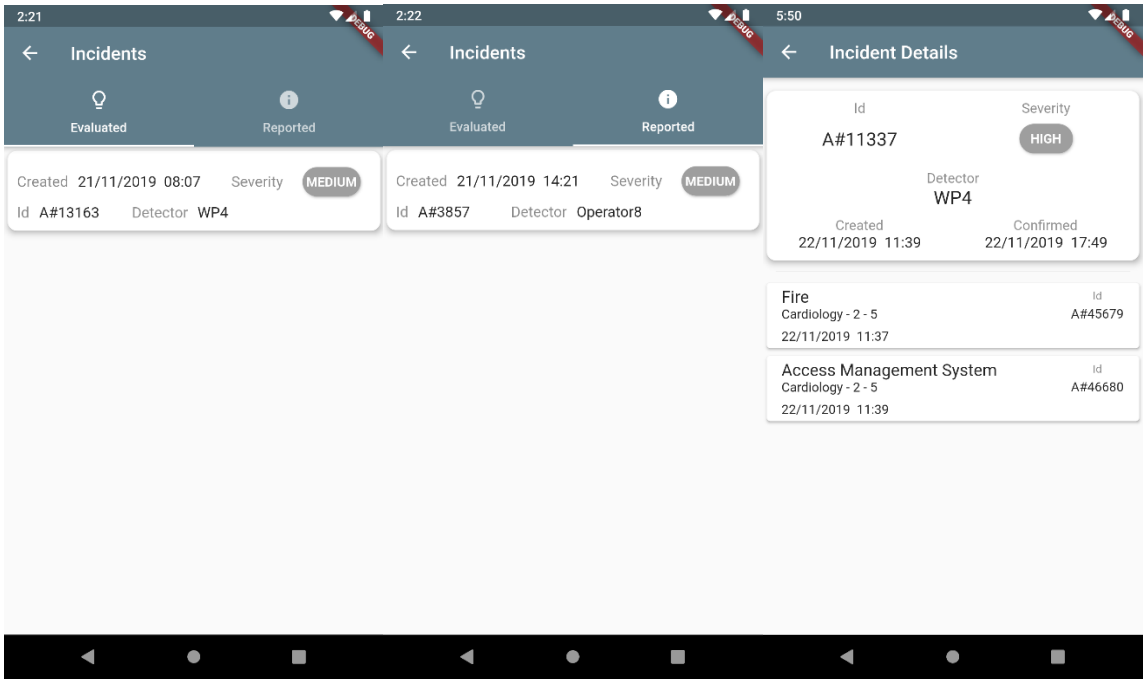

Figure 12: Incident Screens

7.6 Impact evaluation

In Figure 13 it is possible to see the details of an impact. The left screen shows all the previously reported impacts. In the middle and right screen, the details of a single impact are shown. For each impacted asset is displayed a description containing a score, which defines how likely and severe that asset is going to be impacted, as well as the other information about the asset (e.g. type, location, asset Id etc.) retrieved from the CDB.

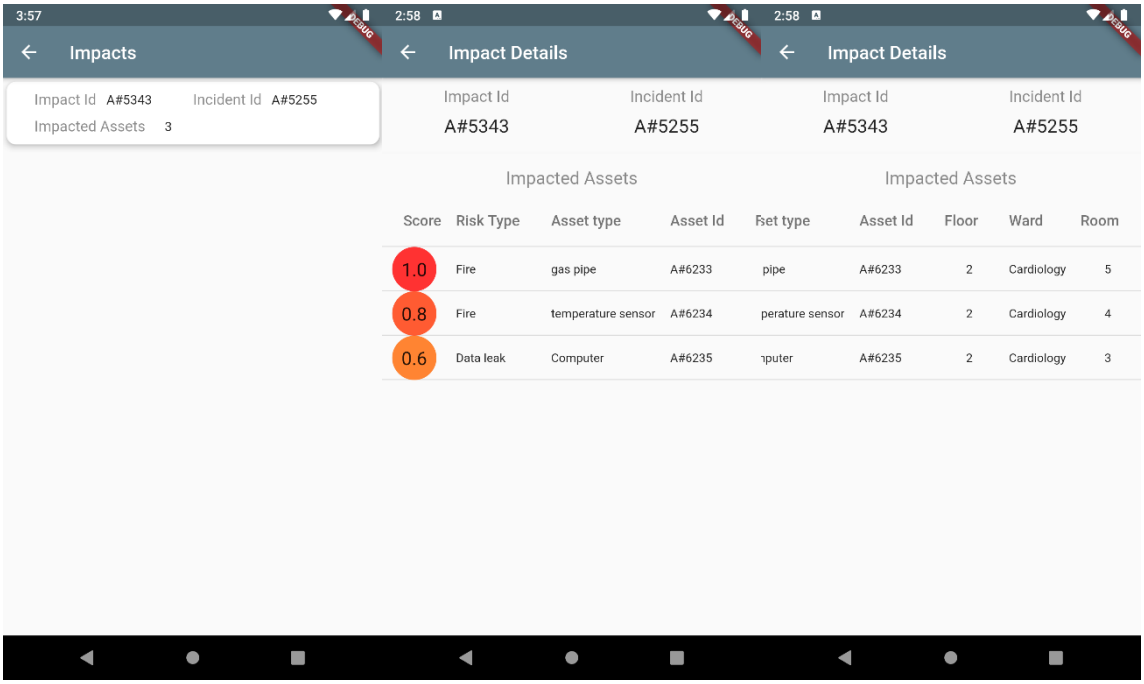

Figure 13: Impact screens

7.7 Threat response

A Threat Response can be visualized by clicking on the view button inside its notification (left screen) or by selecting it inside the Threat Responses screen (right screen).

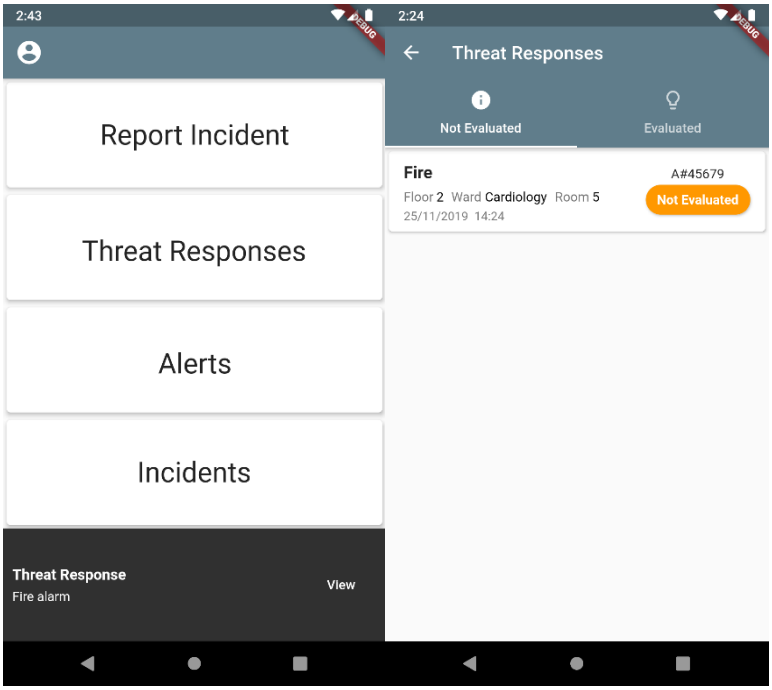

Figure 14: Threat response alert

Inside the page displaying the Threat Response are visualized the details and attached information (textual or video). The user can consult on this before accepting or rejecting the Threat Response call to action using the buttons at the bottom of the screen.

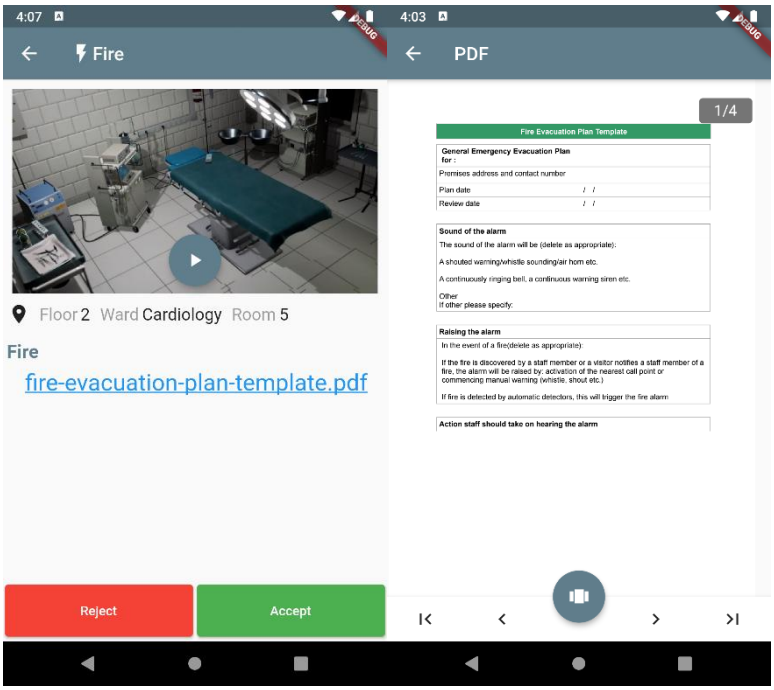

Figure 15: Threat response

8 Interactions with other SAFECARE modules

This section describes the interactions between MAS and other SAFECARE modules in terms of communication protocol and data exchanged.

8.1 DXL

DXL is used to communicate to WP6 modules: TRS, IPM and central database.

8.1.1 TRS

The MAS COMM component will use MQTT to subscribe to the topic "*SAFECARE/effect/notification"* to receive threat response notifications coming from the TRS module. The notifications are transmitted in JSON format according to D6.8 specifications.

```
{
   "ID": Some Comunication IDs and references,
   "timeout": max time to answer the message
   "recipient":{
      "user1":"user address 1",
      "delivery_method":"confirmation required",
      "delivery status":"message received",
      "message":"an example of alert message"
   }
}
```

Depending on the delivery method the TRS module could need an acknowledgement of message reception, therefore the MAS COMM will publish the ACK to topic *"SAFECARE/effect/notification_response".* The acknowledgement is transmitted in JSON format according to D6.8 specifications.

8.1.2 IPM

MAS COMM component will use MQTT to subscribe to the topic "*SAFECARE/effect/impact"* to receive threat response notifications coming from TRS module. The impacts are transmitted in JSON format according to D6.6 specifications.

```
{
   "impact_id":"XXXXXXX",
   "incident_id":"AAAAAAA",
   "assets":[{
         "asset_id":"AAAAAAA",
         "risk_type":"Fire",
         "impact_score":1
      },
      {
         "asset_id":"AAAAAAB",
         "risk_type":"Fire",
         "impact_score":0.8
      },
      {
         "asset_id":"AAAAAAC",
         "risk_type":"Data leak",
         "impact_score":0.6
      }]
}
```

8.1.3 Central database: static data

Static data, which contains information about hospital assets and locations can be retrieved through a REST-API exposed by the DXL as defined in Deliverable D6.2. Locations data and assets are related to information needed by a building security agents to report and validate an incident, they correspond to what is stored the central database but they must be human understandable.

8.2 BTMS

The MAS COMM component will use MQTT to subscribe to the topic "*SAFECARE/physec/alert*" to receive alerts notifications coming from BTMS module. The alerts are transmitted in JSON format according to D4.1 specification.

```
{
   "detector":"WP4",
   "severity":"HIGH",
   "date":"20190410T165514Z",
   "unique_identifier":"A#85647",
   "alerts":[
      {
         "id_alert_type":"XXX",
         "id_detector":"AAA",
         "date":"20190410T165514Z",
         "description":"Suspicious behaviour: loitering",
         "unique_identifier":"A#85648",
         "assets":{
            "id_asset":"XXX"
         },
         "sensor":{
            "id_asset":"XXX",
            "sensor_metadata":{
               "VideoAnalitics":{
                  "NumberOfPeople":"2",
                  "SecurityEvent":"loitering",
                  "TimeSpent":"180s",
                  "mediaPhoto":{

                  },
                  "mediaVideo":{
                     "uri":"rtsp://192/media.amp"
                  }}}}},
      {
         "id_alert_type":"YYY",
         "id_detector":"BBB",
         "date":"20190410T165514Z",
         "description":"Fire detection system: Fire alarm",
         "unique_identifier":"A#45678",
         "assets":{
            "id_asset":"YYY"
         },
         "sensor":{
            "id_asset":"YYY",
            "sensor_metadata":{
               "VideoAnalitics":{
                  "CameraId ":"a12",
                  "mediaVideo":{
                     "uri":"rtsp://192/media2.amp"
                  }}}}
   ]
}
```

The MAS COMM will publish the incidents (*evaluated* and *reported*) to topic *"SAFECARE/physec/incident".* Impact notification is transmitted to the BTMS by publishing to topic *"SAFECARE/physec/impact".*

The impact notification is transmitted in JSON format like:

```
{
   "impact_id":"XXXXXXX",
   "incident_id":"AAAAAAA",
   "iFrame_URL":"https://mas/impact?impact_id"
}
```

In Figure 16 is depicted the mock-up of the iframe. It displays the impact calculated by the Impact Propagation Module as a list of possible events that is displayed in a tabular form:

- Risk Type
- Asset (location info)
- Severity communicated with colour gradient (from yellow to red).

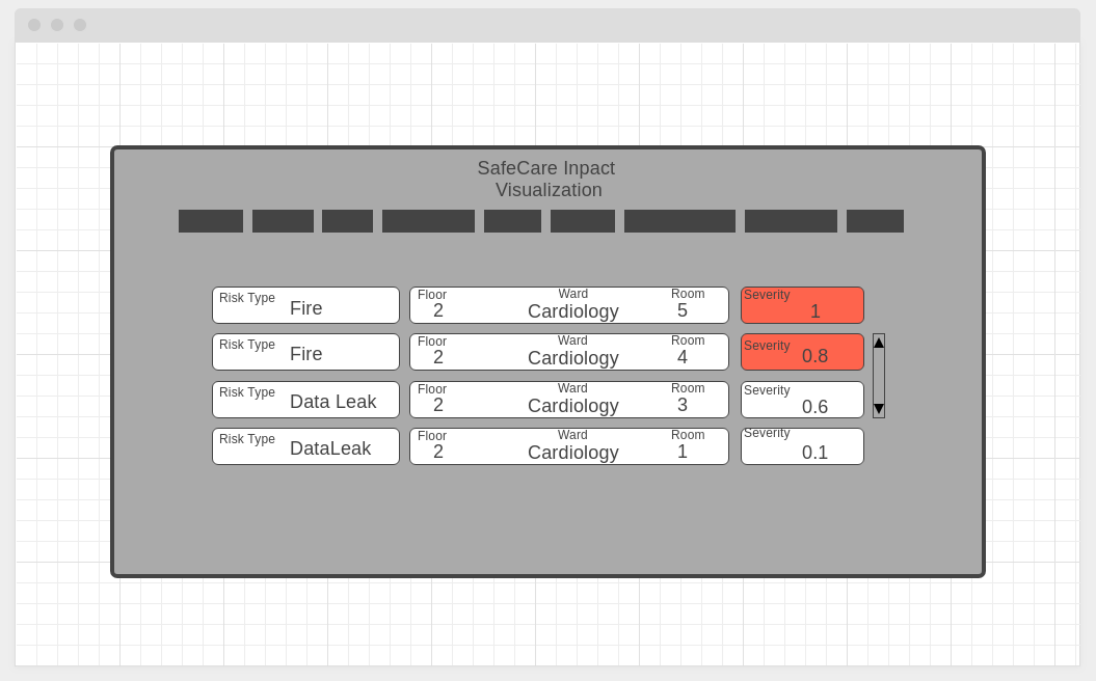

Figure 16: Impact iframe

9 End to end scenarios

This section will go through every scenario defined in Deliverable D3.6 and referenced in Deliverable D6.1, where a description and overview for all the scenarios can be found. For each of the scenarios is reported the threat attack pattern, steps of defence the MAS participate in, and the MAS tasks.

9.1 Scenario 1

The Table 1 details how MAS will collaborate to overcome an attack targeting power supply of the hospital.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker steals the key/badge of an employee. 2. The attacker gets into PLC room.	• The building threat monitoring system receives the intrusion alert by the suspicious behaviour system. • The building security agents investigate the video streams. • The building security agents confirm the alert as an "intrusion incident".	• MAS receives an alert from the BTMS for evaluation. • MAS selects the building security agent in charge of evaluation, it sends alert data to his or her mobile device with a push notification. The building security guard confirms the "intrusion incident". • MAS transmits the evaluation to the BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts. • At the reception of the computed impacts, the reaction plan, such as sending building security agents, is activated by the threat response and alert system.	• MAS receives an impact and prepares an iframe with the impact model visualization and notify the BTMS. • MAS receives a threat response notification and sends a reaction plan to the building security agents' mobile device.
3. The attacker uploads a new PLC program and locks admin access.	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS.

Table 1: scenario 1

9.2 Scenario 2

The Table 2 details how MAS will collaborate to overcome an attack to steal patient data in the hospital.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The fire triggers the fire alarm and the vapor system.	• The building threat monitoring system receives the intrusion alert from the intrusion and fire detection system. • The building security agents investigate the video streams. • The building security agents confirm the alerts (suspicious behaviour alert and fire alert) as an "fire incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "fire incident". • MAS transmits the evaluation to BTMS.
	• At the reception of the computed impacts, the reaction plan, such as sending building security agents, is activated by the threat response and alert system. • Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS.
2. The attacker breaks the door lock of the computer room and enters in computer room.	• The building threat monitoring system receives the intrusion alert from the intrusion and fire detection system. • The building security agents investigate the video streams. • The building security agents confirm the alerts (suspicious behaviour alert and intrusion alert) as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.

Table 2: scenario 2

9.3 Scenario 3

The Table 3 details how MAS will collaborate to overcome an attack targeting the population, IT systems and medical devices in the hospital, and patient data base.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker get access to a technical room.	• The building threat monitoring system receives the intrusion alert by the suspicious behaviour system. • The building security agents investigate the video streams. • The building security agents confirm the alerts (suspicious behaviour alert and fire alert) as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts. • At the reception of the computed impacts, the reaction plan, such as sending building security agents, is activated by the threat response and alert system.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS. • MAS receives threat response notification and sends reaction plan to building security agents' mobile devices.

Table 3: scenario 3

9.4 Scenario 4

The Table 4 details how MAS will collaborate to overcome an attack targeting the air-cooling system of the hospital.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker gets access to a technical room.	• The building threat monitoring system receives the intrusion alert by the suspicious behaviour system. • The building security agents investigate the environmental behaviour alert. • The building security agents confirm the alerts (suspicious behaviour alert and fire alert) as an "environmental behaviour alert".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "environmental behaviour alert". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts. • At the reception of the computed impacts, the reaction plan, such as health practitioners, is activated by the threat response and alert system.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS. • MAS receives threat response notification and sends reaction plan to health practitioners' mobile devices.

Table 4: scenario 4

9.5 Scenario 5

The Table 5 details how MAS will collaborate to overcome an attack: shooting, explosive or sabotage in critical places.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker bypasses the security control.	• The building threat monitoring system receives the intrusion alert from the intrusion and fire detection system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS.
	• At the reception of the computed impacts, the reaction plan, such as sending building security agents, is activated by the threat response and alert system.	• MAS receives threat response notification and sends reaction plan to building security agents' mobile devices.
2. The attacker plants a bomb.	• The building threat monitoring system receives the intrusion alert by the suspicious behaviour system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.

	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts. • At the reception of the computed impacts, the reaction plan, such as sending building security agents, is activated by the threat response and alert system.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS. • MAS receives threat response notification and sends reaction plan to building security agents' mobile devices.

Table 5: scenario 5

9.6 Scenario 6

The Table 6 details how MAS will collaborate to overcome an attack such as theft at hospital equipment, access to hospital network and IT systems.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker accesses to a technical room.	• The building threat monitoring system receives the intrusion alert from the intrusion and fire detection system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS.

	• At the reception of the computed impacts, the reaction plan, such as security agents, is activated by the threat response and alert system.	• MAS receives threat response notification and sends reaction plan to security agents' mobile devices.
2. The attacker opens the cabinet and unplugs the hard drive.	• The building threat monitoring system receives the intrusion alert from the intrusion and fire detection system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS.
	• At the reception of the computed impacts, the reaction plan, such as sending building security agents, is activated by the threat response and alert system.	• MAS receives threat response notification and sends reaction plan to building security agents' mobile devices.

Table 6: scenario 6

9.7 Scenario 7

The details Table 7 how MAS will collaborate to overcome an attack targeting IoT medical wearable devices (outside / inside).

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker obtains local access to a IoT medical device in hospital.	• The building threat monitoring system receives the suspicious behaviour alert from the suspicious behaviour system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "suspicious behaviour".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "suspicious behaviour". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts. • At the reception of the computed impacts, the reaction plan, such as sending building security agents, is activated by the threat response and alert system.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS. • MAS receives threat response notification and sends reaction plan to building security agents' mobile devices.

Table 7: scenario 7

9.8 Scenario 8

The Table 8 details how MAS will collaborate to overcome an attack on distributed management over distributed buildings, considering external stakeholders.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker accesses to restricted area in hospital with a badge.	• The building threat monitoring system receives the intrusion alert by the suspicious behaviour system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts. • At the reception of the computed impacts, the reaction plan, such as sending security agents, is activated by the threat response and alert system.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS. • MAS receives threat response notification and sends reaction plan to building security agents' mobile devices.
2. The attacker disrupts medical devices.	• The building threat monitoring system receives the intrusion alert by the suspicious behaviour system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.

	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS.

Table 8: scenario 8

9.9 Scenario 9

The Table 9 details how MAS will collaborate to overcome an attack blocking national crisis management.

Steps of attack	Steps of defence MAS participate in	MAS role
1. The attacker accesses to a technical room.	• The building threat monitoring system receives the intrusion alert by the suspicious behaviour system. • The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation. • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident". • MAS transmits the evaluation to BTMS.
	• Building security agents and SOC operators visualize potential cascading effects respectively on the building threat monitoring system and the cyber threat monitoring system and possibly act to prevent the threat and mitigate the impacts.	• MAS receives impact on behalf of BTMS then MAS prepares an iframe with impact model visualization and notify BTMS.
	• At the reception of the computed impacts, the reaction plan, such as sending security agents, is activated by the threat response and alert system.	• MAS receives threat response notification and sends reaction plan to building security agents' mobile devices.
2. The attacker tries to identify the WAN shelter.	• The building security agents investigate the video streams. • The building security agents confirm the alerts as an "intrusion incident".	• MAS receives an alert from BTMS for evaluation • MAS selects the building security in charge of evaluation, it sends alert data to his mobile with push notification. Building security agent confirms "intrusion incident" • MAS transmits the evaluation to BTMS.

Table 9: scenario 9

10 Conclusion

In the SAFECARE architecture, the MAS module is responsible for improving reaction times and enriching the communication infrastructure in case of physical threats. This allows the building security agents to quickly report incidents and to rapidly respond to emergencies; moreover, it offers a way to implement a distributed, affordable and always on SOC to ensures there is always a building security agent available to react to an alert. As a result, the MAS complements and extends other SAFECARE physical security modules as well as the response and alert system.

This document reports the description of specification and functionality of the MAS, in terms of architecture, description of interfaces with other SAFECARE modules; furthermore, a mock-up of the Mobile App's user interface has been designed, in order to give a first overview of the interface and the functionality.

This document represents a guideline for the development of the MAS software and for the development of the other modules that will interact with the MAS: BTMS and TRS.