SAFECARE

Integrated cyber-physical security for health services

FONDAZIONE links

PASSION FOR INNOVATION

How SAFECARE tools mitigate potential cascading effects and put in place response plans

@3S Clustering Event (Crete)

Francesco Lubrano

Michele Petruzza

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

European Commission | HORIZON 2020

SAFECARE Incident

According to the NIST (Stouffer, Falco, & Scarfone, 2011), an incident is "*an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system*"

Inside SAFECARE, an incident consists of a set of security events verified by a human operator(guard or SOC operator) and forwarded as a unique message to systems that can evaluate the potential impacts of the incident and triggers automatic alerts.

SAFECARE Global Architecture

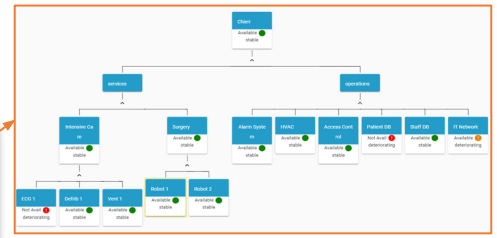
SMS
Automatic phone calls
Emails
Notification

Alerting system

Impact propagation

Central Database

HAMS



Data Exchange Layer

Building threat monitoring system

Cyber threat monitoring system

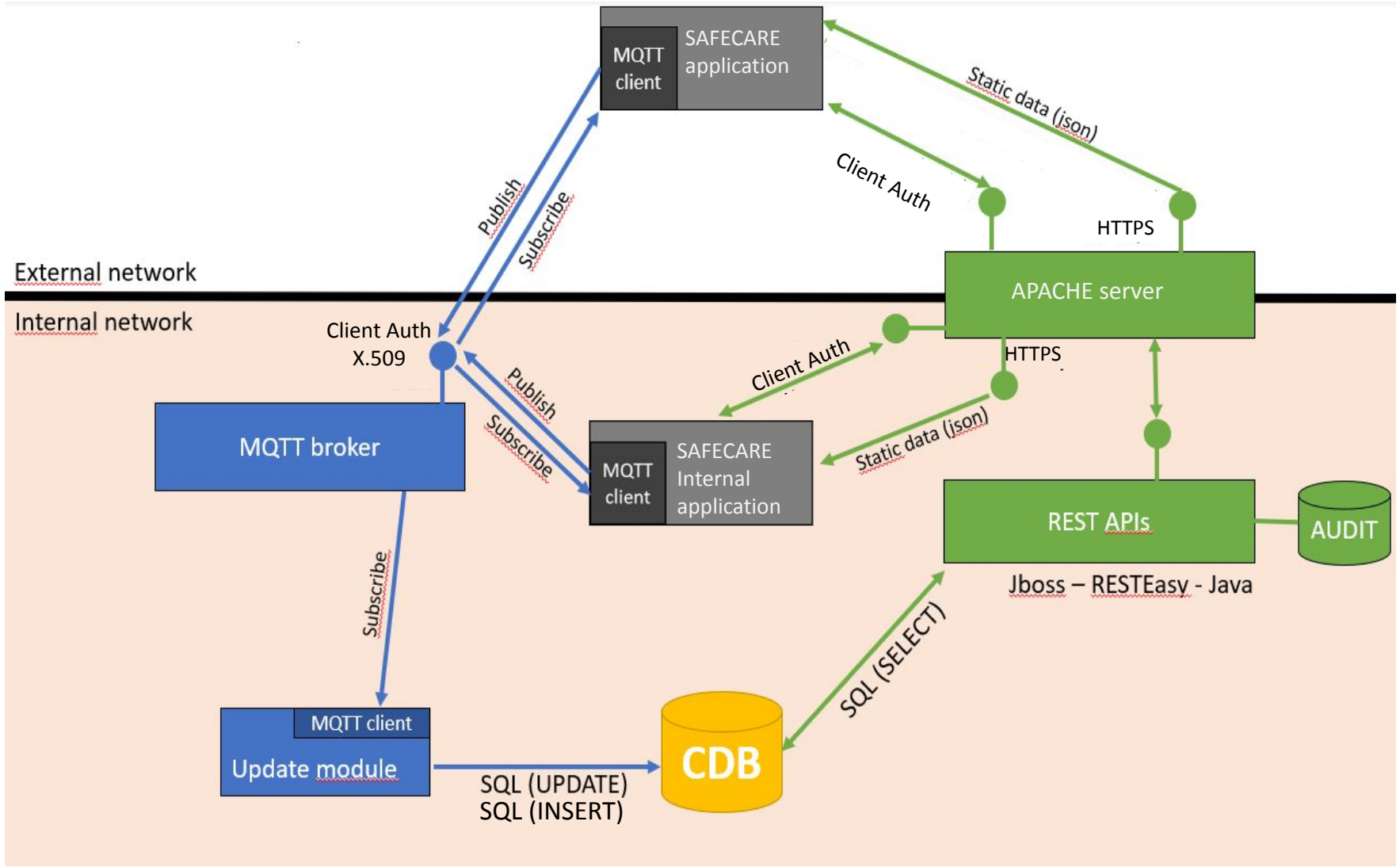
SAFECARE
Integrated cyber-physical security for health services

Data Exchange Layer & Central Database

- To provide a communication tool to allow other modules to communicate with each other and with the central database in near real time, and to provide relevant interfaces to extract data from the database

- To develop a unique database that centralises incidents coming from cyber and physical monitoring systems and stores static data (medical devices, security devices, etc.) and dynamic data(incidents, impacts, threat responses, …)

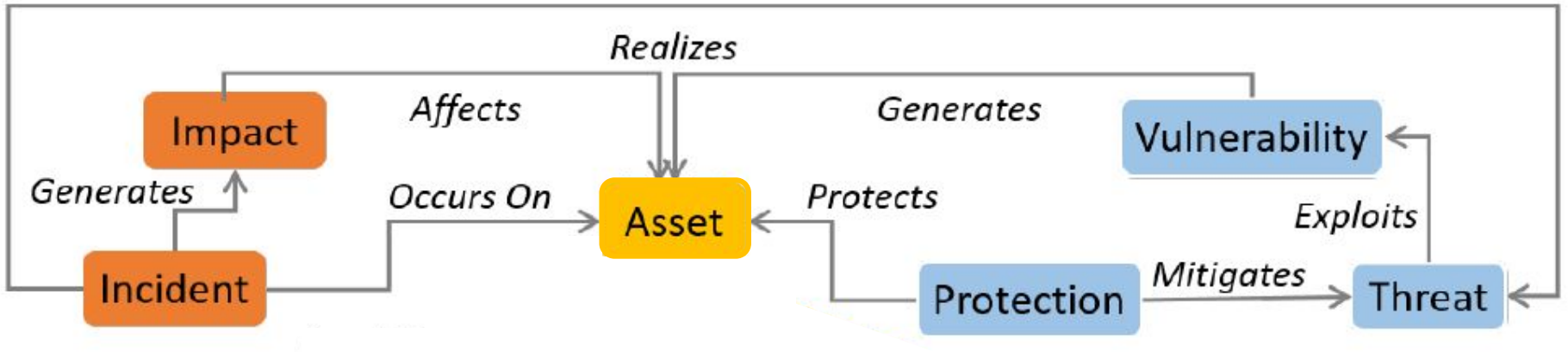
Data Exchange Layer and Central DB Internal Architecture



Impact propagation and decision support model

To allow preventing the propagation of cascading effects, formalizing the relations between physical and cyber assets and threats and anticipating potential impacts of cyber and physical incidents

- A **modular ontology** that represents the assets, their relations with other assets, as well as **incidents, protections, impacts and risks**;



Impact propagation and decision support model

To allow preventing the propagation of cascading effects, formalizing the relations between physical and cyber assets and threats and anticipating potential impacts of cyber and physical incidents

- An **impact propagation rules engine** to **infer** from the knowledge base a list of **impacted assets** and the corresponding **impact score**;

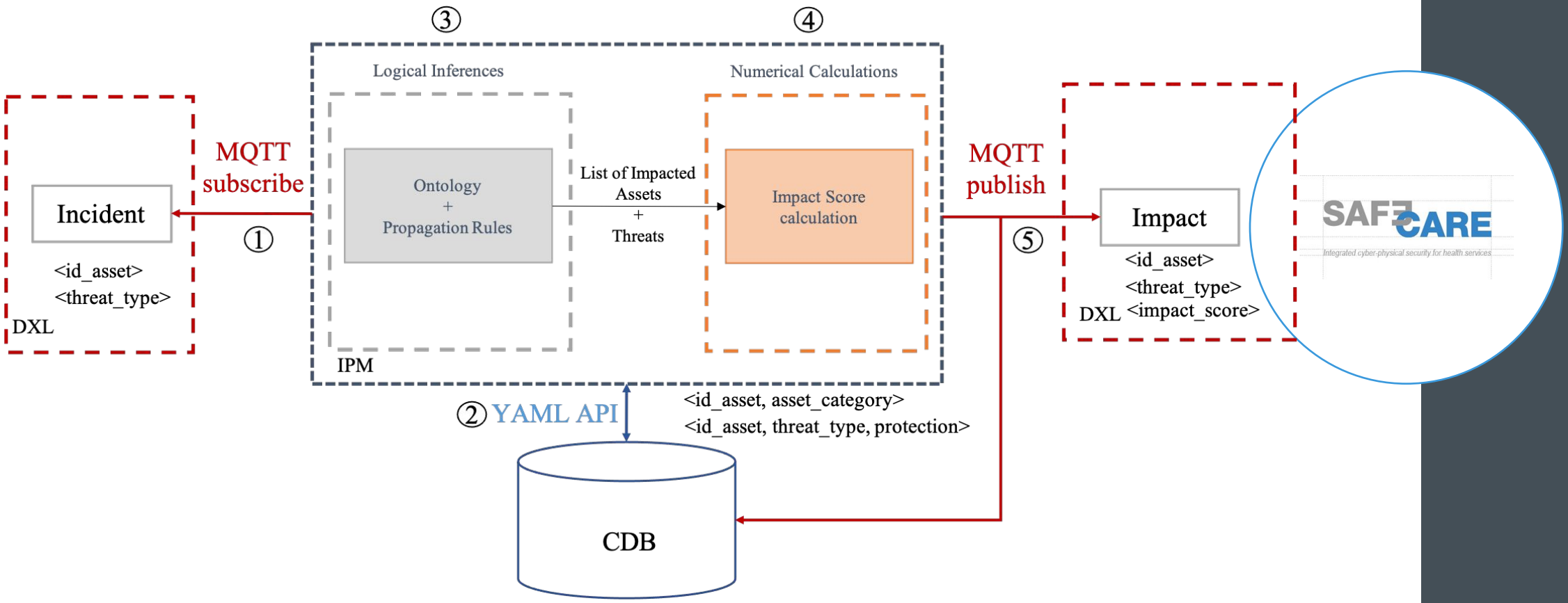
```
(?incident sco:occurs ?asset1), (?incident sco:realizes ?threat1),
(?threat1 rdf:type sco:suspicious_interaction), (?asset1 rdf:type sco:Device),
(?asset1 sco:HostsNetwork ?asset2), (?asset2 rdf:type sco:Network),
-> (?new_incident rdf:type sco:Incident), (?new_incident sco:realizes ?threat2),
(?threat2 rdf:type sco:Network_Service_Scanning),
(?new_incident sco:occurs ?asset2)
```

Impact propagation and decision support model

To allow preventing the propagation of cascading effects, formalizing the relations between physical and cyber assets and threats and anticipating potential impacts of cyber and physical incidents

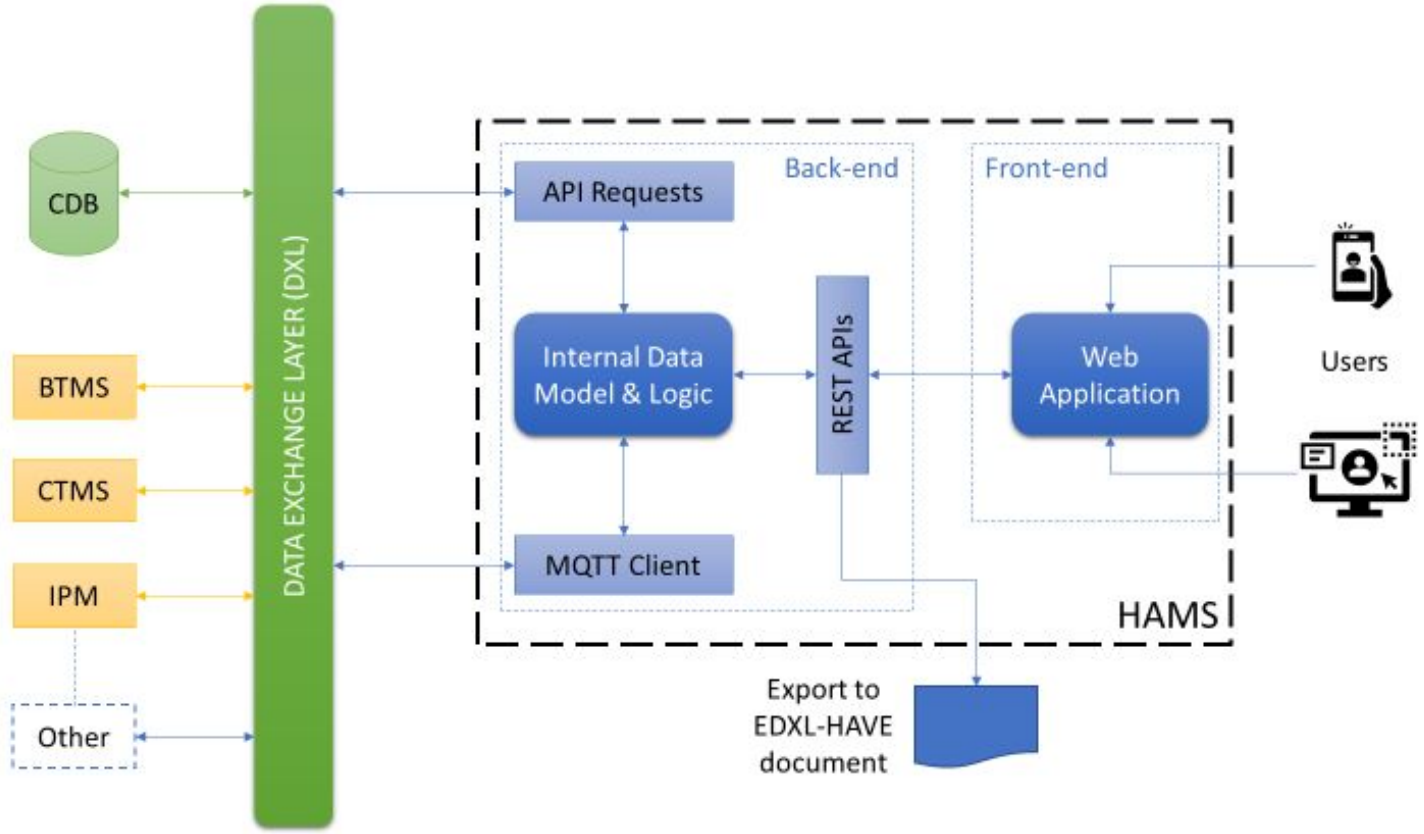
- A **methodology** to analyse threat scenarios (based on the integration of the EBIOS and Bow-Tie methodologies) to improve the set of propagation rules and test and validate the generated impacts

Impact propagation and decision support model



Hospital availability management system (HAMS)

To design and develop a system that provide hospital availability, improving the health service resilience and the data availability in case of emergency



How SAFECARE brings reaction plans to the users: TRAS & MAS

Purpose of each component:

Threat Response and Alert System

To design and develop a system that automatically process reaction plans and sends notifications and alerts to relevant recipients, improves the coordination between internal and external security practitioners and improves the response and service recovery time

Mobile Alerting System

To design and develop a system to speed up the communication between the stakeholders and the security infrastructure in case of physical threats, while also enriching the information provided to the user

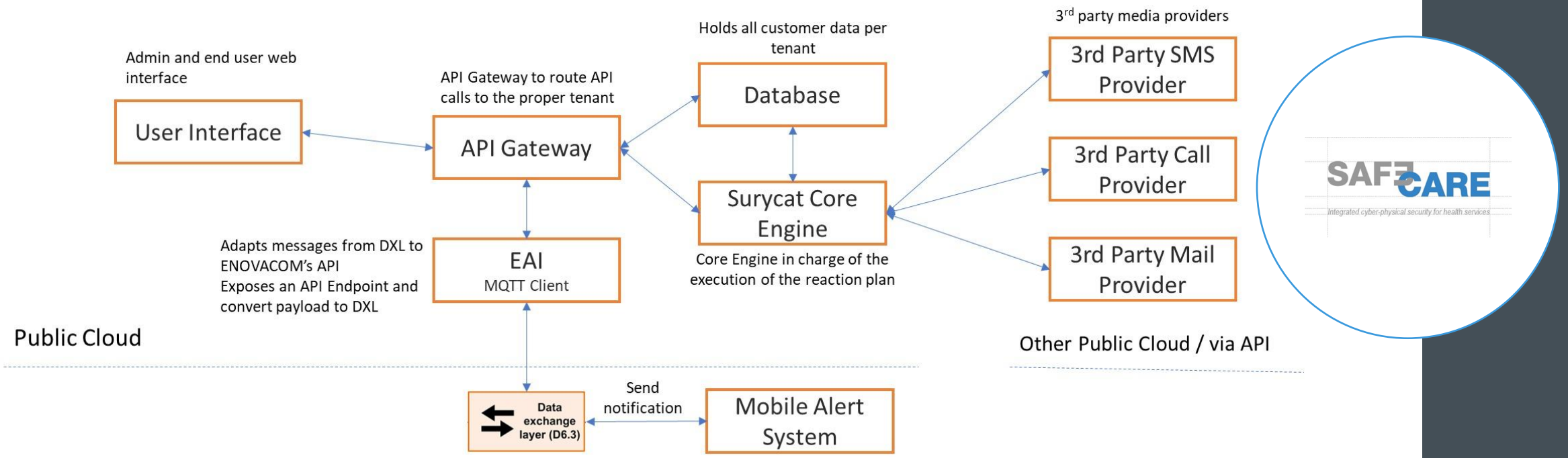
Threat Response and Alert System (TRAS)

- An automated and integrated communication platform to **provide** end users with **adaptive and efficient notifications and alerts**.
    - Thanks to these notifications the users can act with swiftness and precision based on the risk assessment of the current threat.

- Based on a **rule processing engine** that parses the impacts sent from the Impact Propagation Model module and executes all communication related to the reaction plan relative to the current threat.
    - The rules are created together with the security authorities to target the correct security practitioners (both internal and external) based on each kind of possible threat.

- Integrates current (phone call, SMS) and new (MAS) communication channels through which the threat response messages are sent to the users.

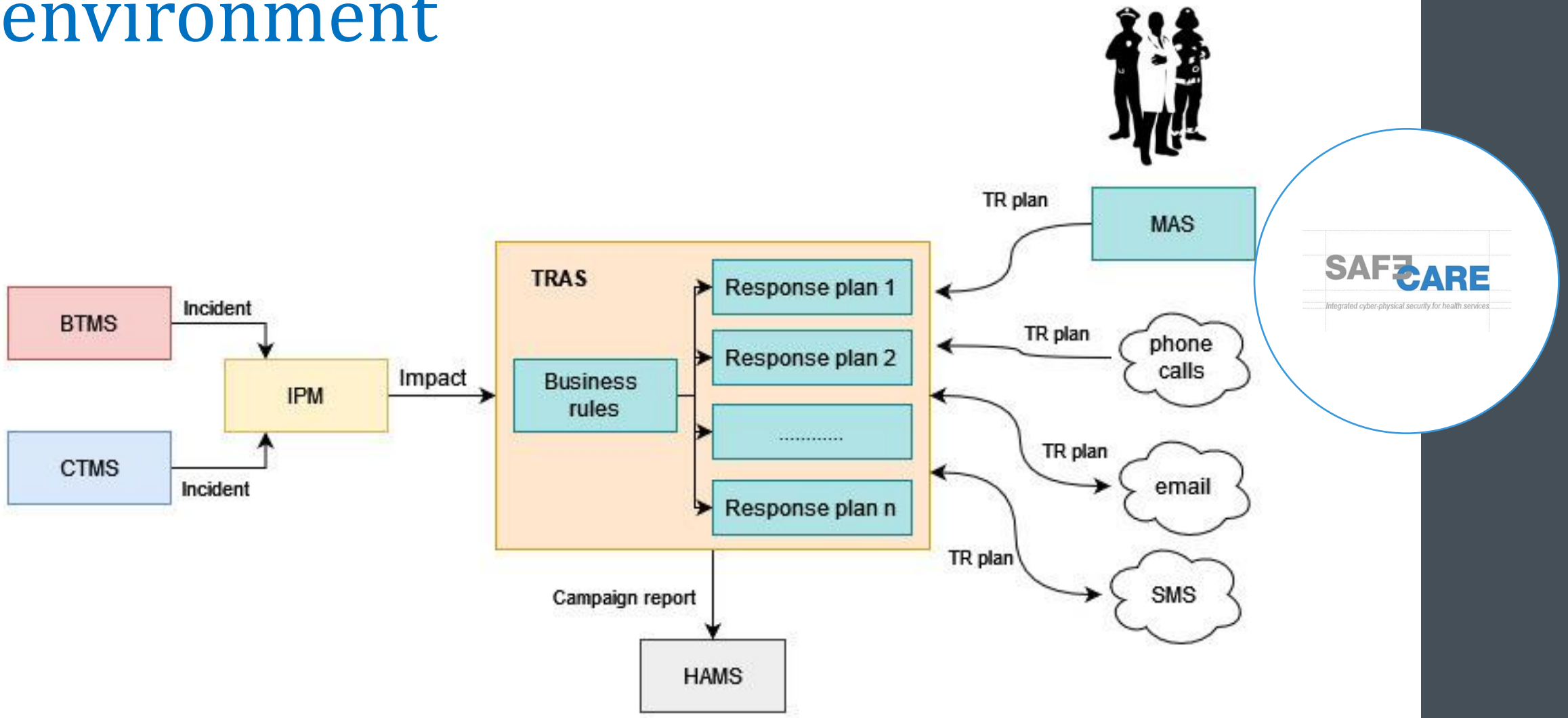
TRAS: internal architecture



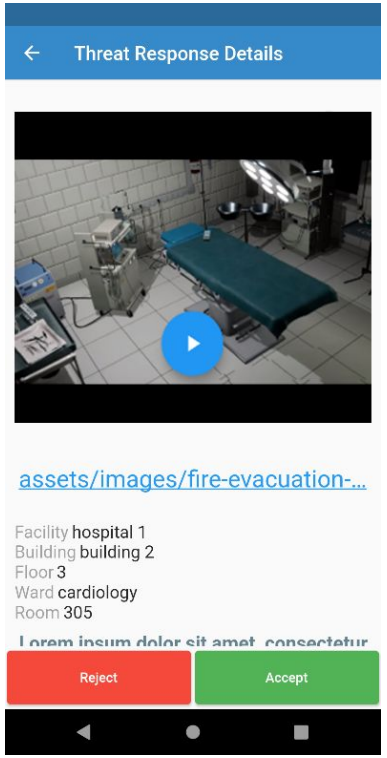
Surycat

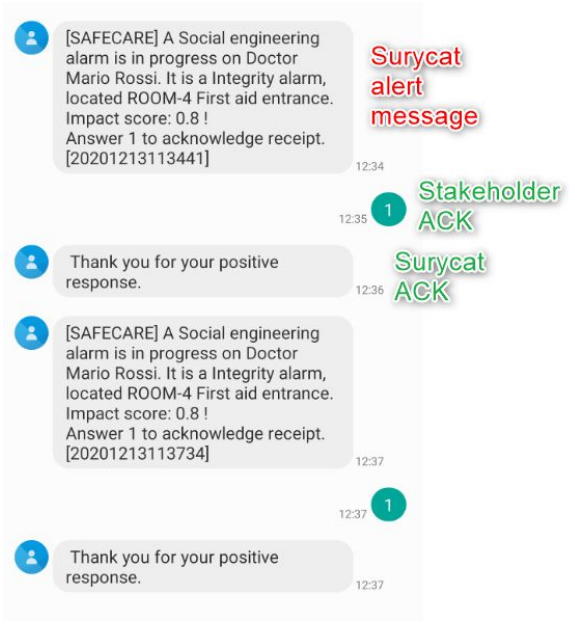
Integration Engine

TRAS: role inside the SAFECARE environment



TRAS: threat response examples





[SAFECARE] Impact score: 0.8! Social engineering, Integrity, ROOM-4 First aid entrance

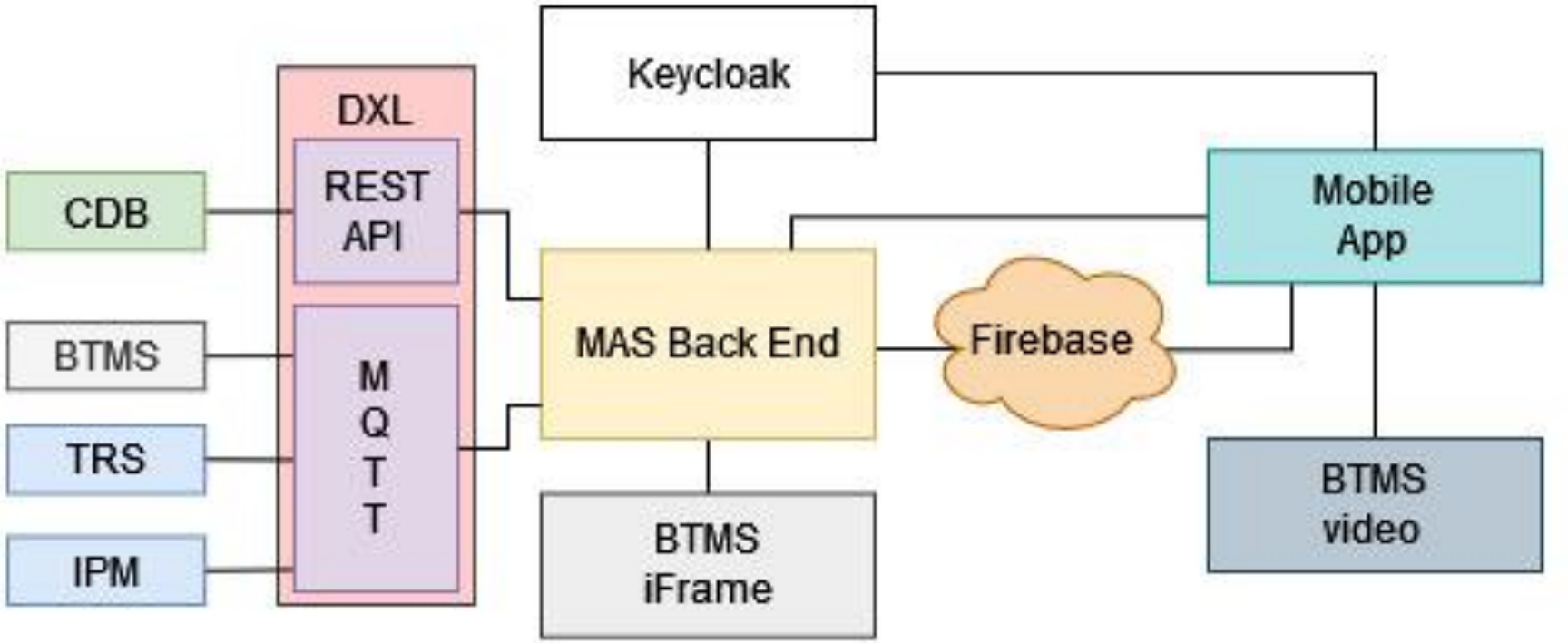
S Safecare <safecare@surycat.io>
À Guillaume Gaudel

A Social engineering alarm is in progress on Doctor Mario Rossi. It is a Integrity alarm, located ROOM-4 First aid entrance.
Impact score : 0.8 ! [{'id': '4ELp1l7p3V25i57f7tBqxk', 'name': 'Guillaume', 'phones': [{'type': 'professional', 'number':
[], 'created_at': '2020-06-15T14:20:49.921330+00:00', 'updated_at': '2020-09-30T12:47:02.267 [],
'created at': '2020-06-15T14:20:49.921330+00:00', 'updated at': '2020-09-30T12:47:02.267929+00:00',
'tags': [{'id': '6IdcrNLWMzThLCzjzcCmz9', 'name': '[DEMO] Groupe démo', 'slug': 'demo-groupe-demo',
'category': None}]}]

Mobile Alerting System (MAS)

- Provides an **integrated alerting system** to improve reaction times and enrich the communication between the users and the other modules inside the SAFECARE environment.
- It is divided into two components:
  - A **server** module (MAS back end), running inside the hospital network
  - A **mobile application** (mobile app) running on mobile devices (smartphone and tablet).
    - The mobile application, made for both Android and iOS devices, **displays the information about security events** in the hospital and **sends back the user's feedback** through the MAS back end.

MAS: structure

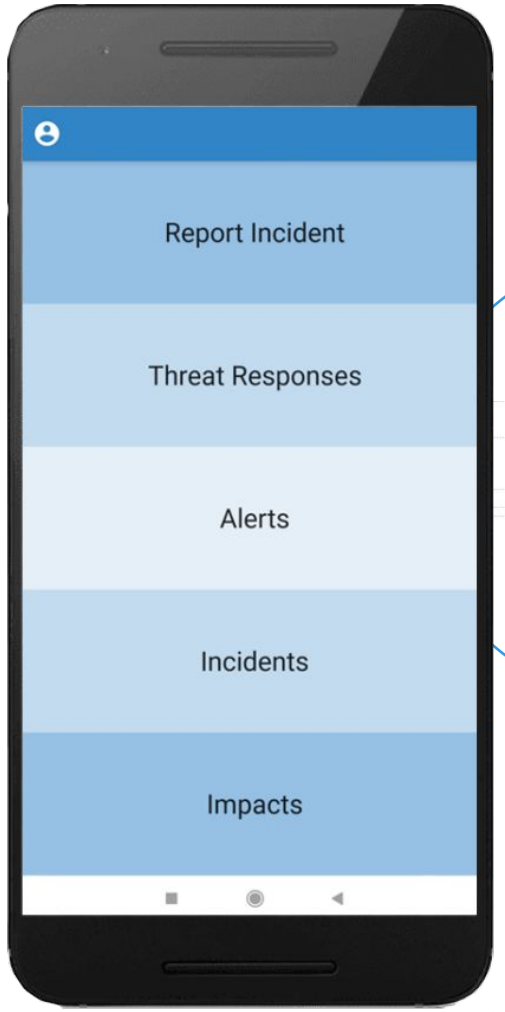


Flask KEYCLOAK Firebase Flutter

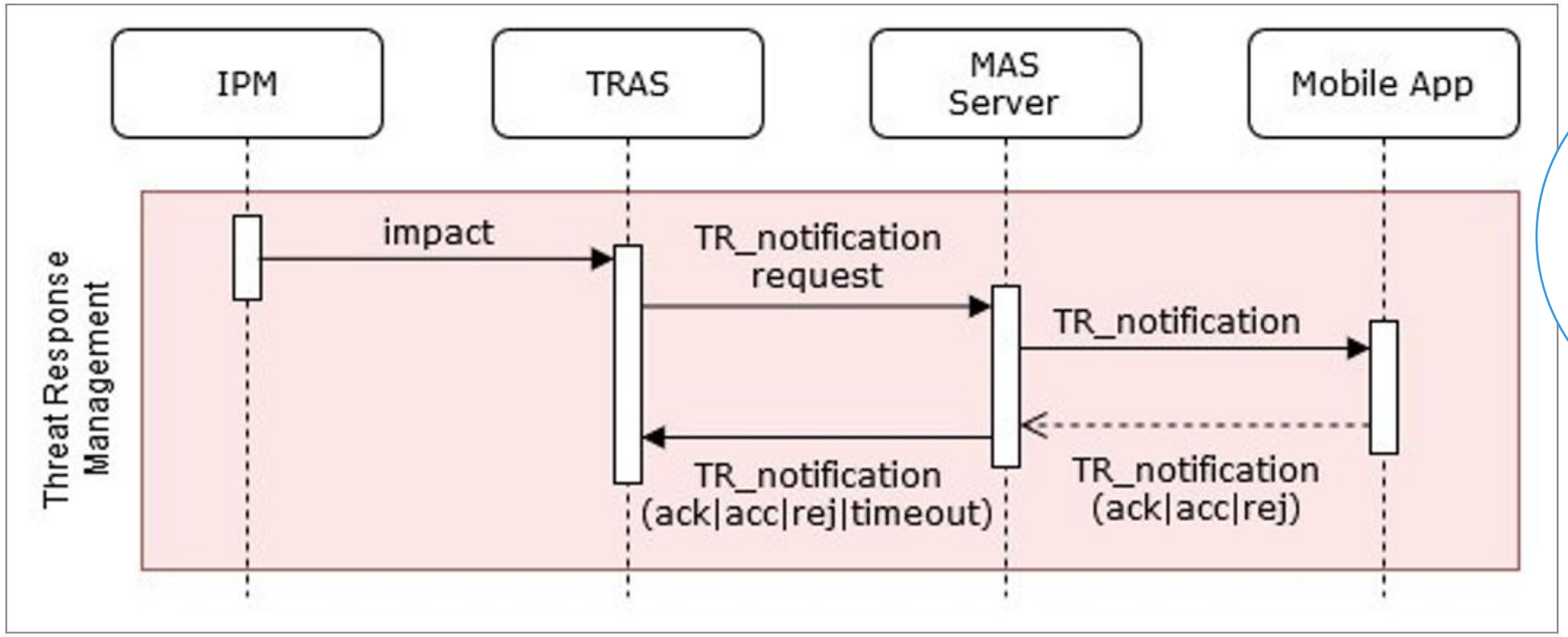
MAS: functionalities

Depending on the role of the user inside the organization the MAS offers different functionalities:

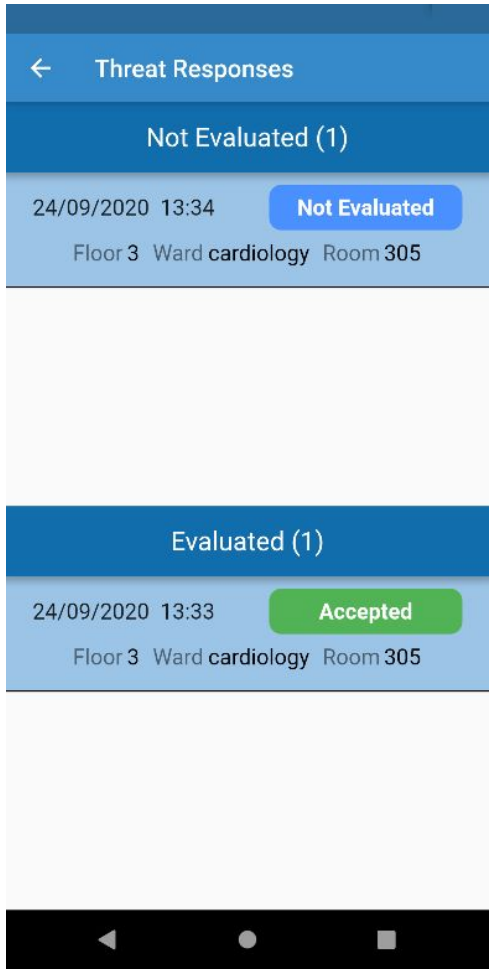
- **Receive Threat Responses** with enriched information (emergency procedures, geolocation, relevant multimedia data) needed to manage the incident.
- **Report specific categories of security threats** or incidents related to a specific failure point in a hospital (e.g. system failure, natural hazard, terrorist attack...),
- Address security incidents discovered by other physical security components (e.g. Video Management System) **implementing a distributed security operations centre**.
- Visualize impacts with detailed asset information.

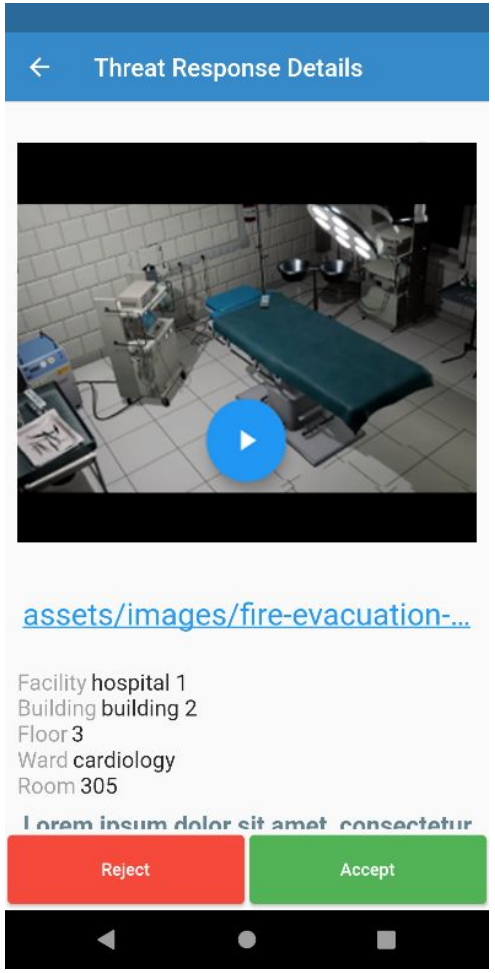


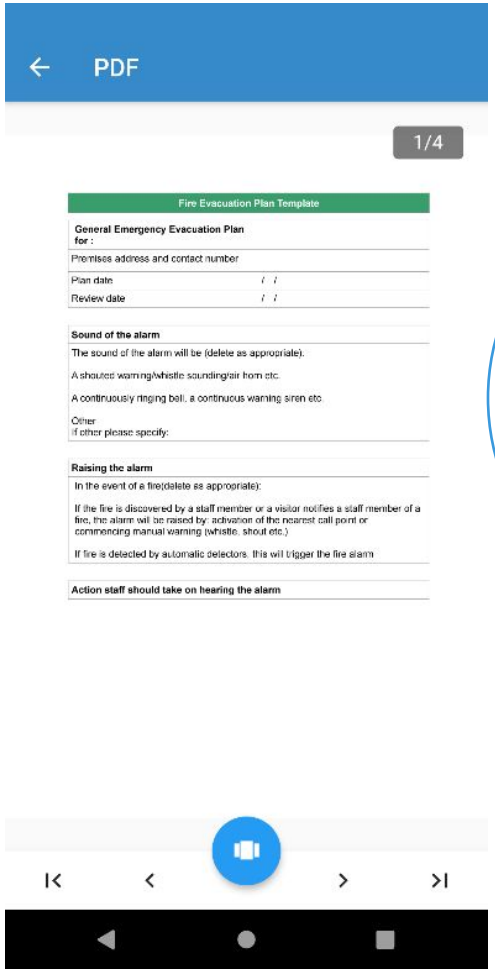
MAS: Threat Response management



MAS: Threat Response interface

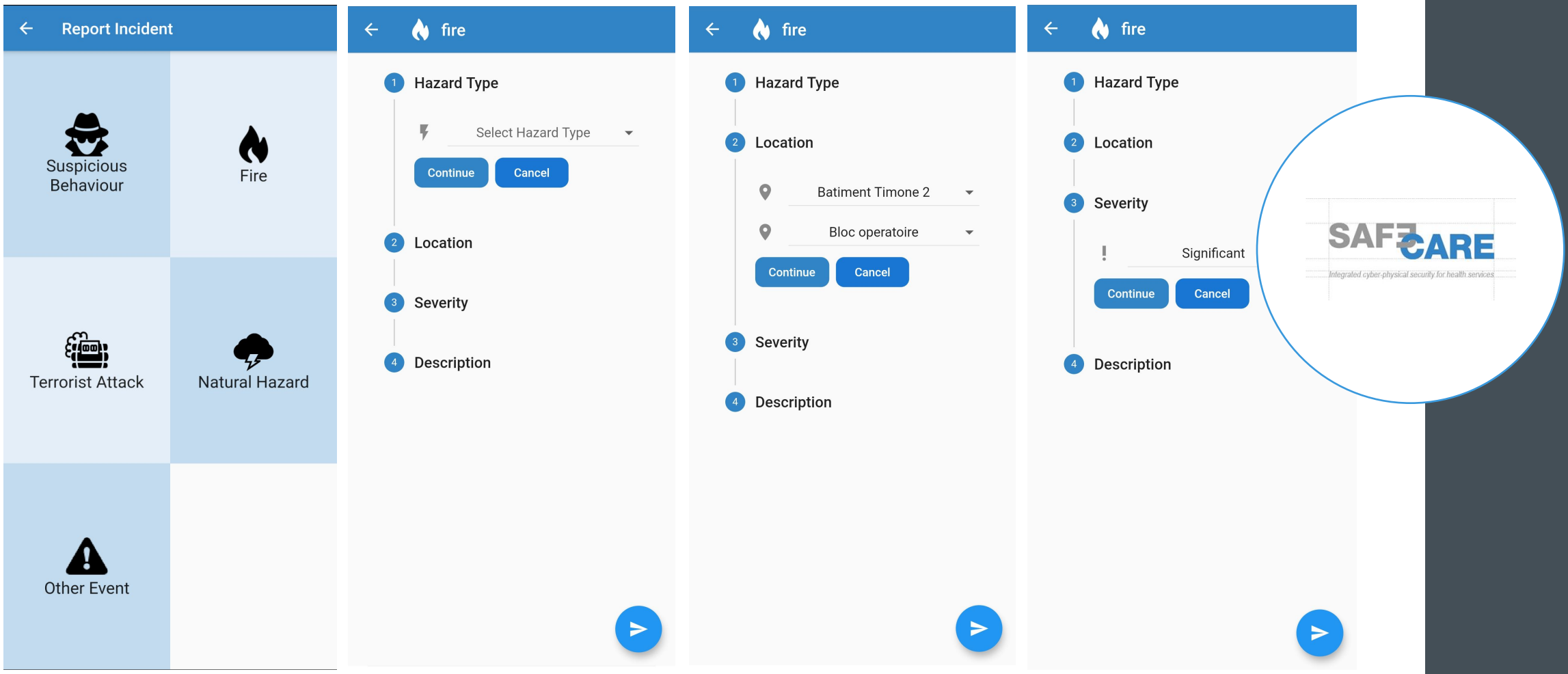




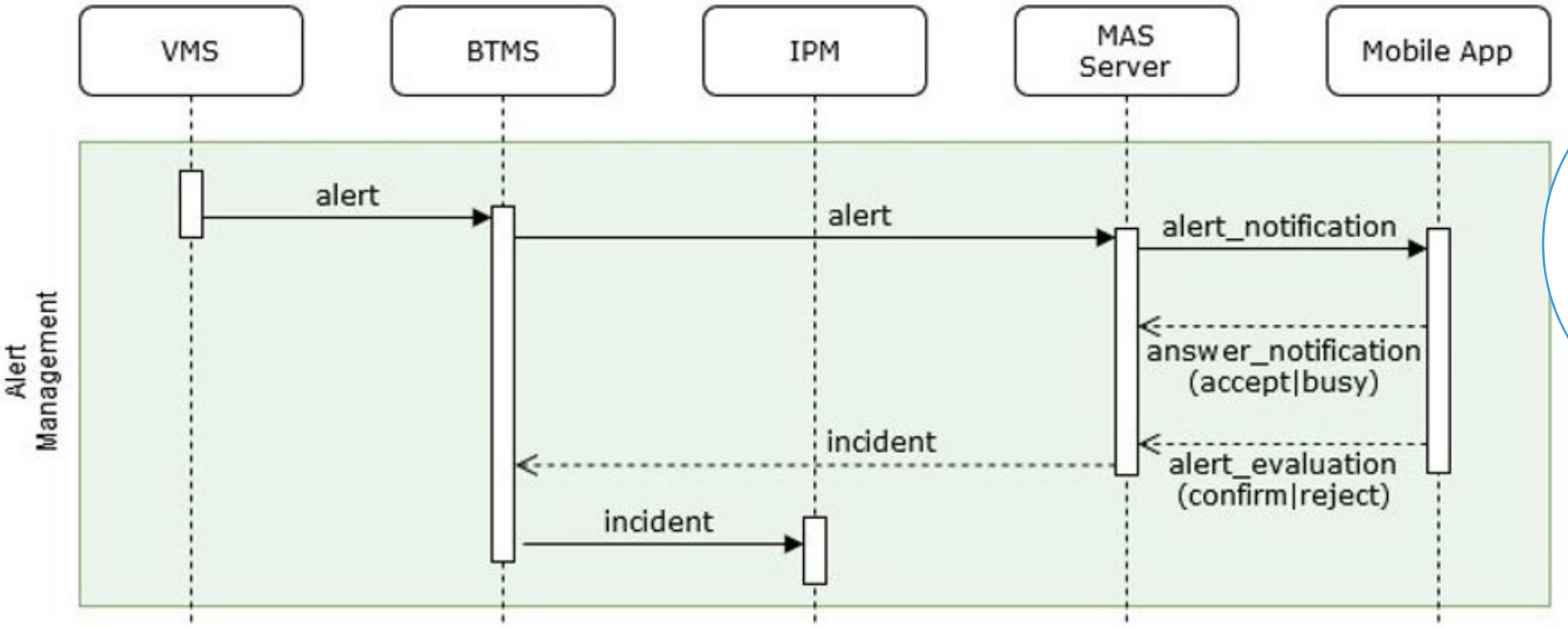


SAFECARE
Integrated cyber-physical security for health services

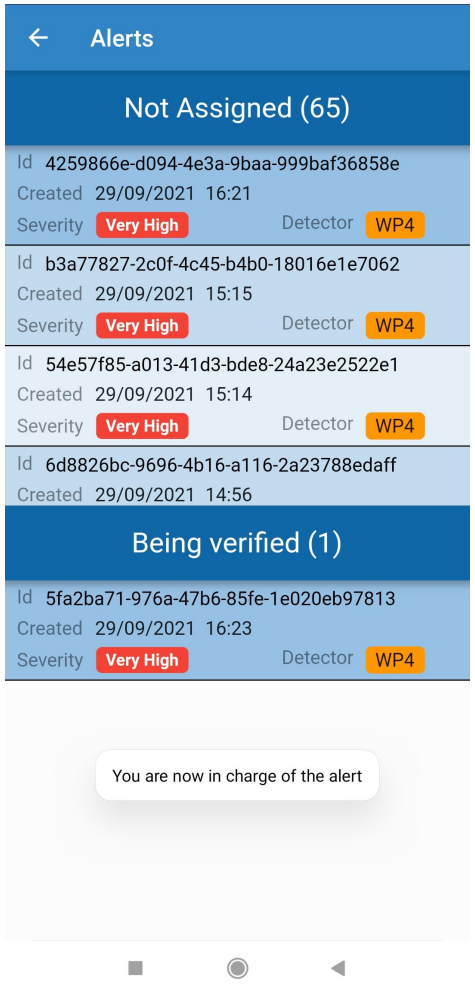
MAS: Incident reporting interface

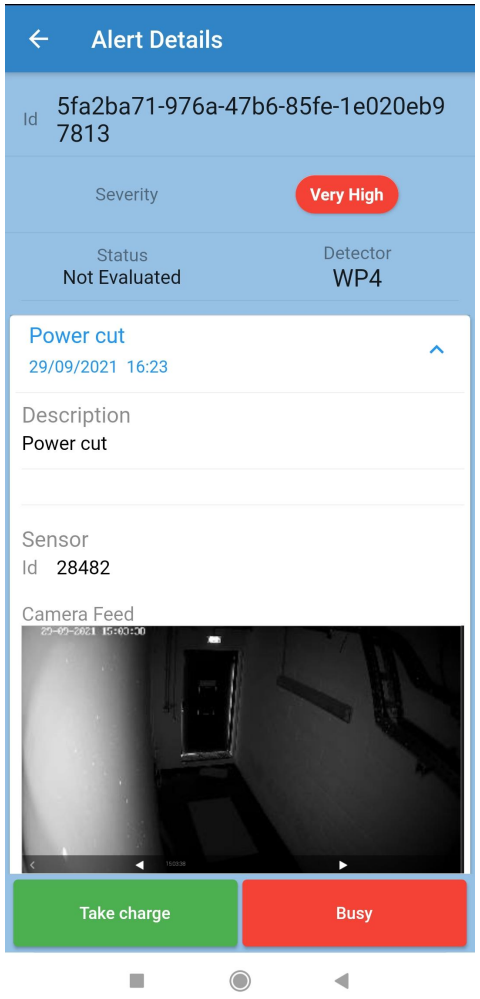


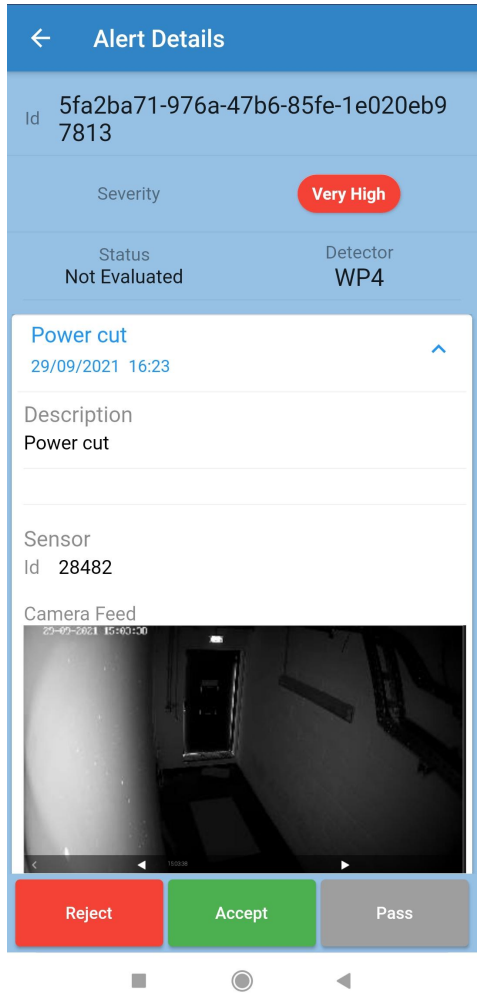
MAS: Alert management



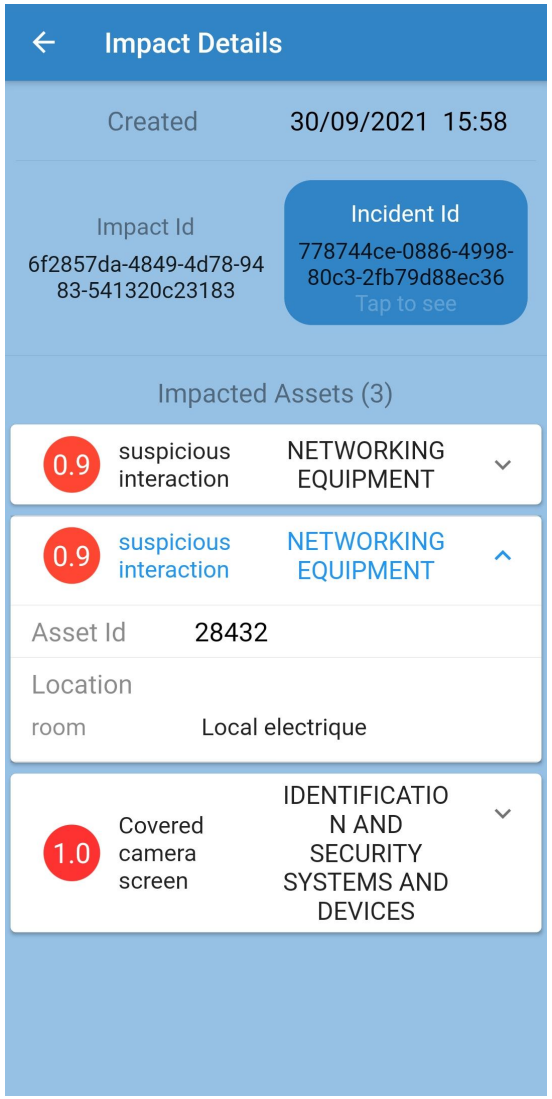
MAS: Alert interface







MAS: Impact interface



Thank you !

More details available on:

- Our website: https://www.safecare-project.eu/
- Twitter: @SafecareP
- -LinkedIn: SAFECARE Project

Francesco Lubrano
francesco.lubrano@linksfoundation.com

Michele Petruzza
michele.petruzza@linksfoundation.com