Demonstration of integrated cyber-physical security solutions in a healthcare environment

SAFECARE How to counter cyber-physical threats to Healthcare Infrastructure

Francesco Lubrano

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

Enisa Threat Landscape - 2020

_Findings

4%_ of breaches were caused by physical actions[12]

20%_ of cybersecurity incidents started or ended with a physical action[12]

5th_ most implemented malicious action on assets was physical attacks on ATMs[12]

54%_ of data breaches across all sectors included a physical attack as the main method

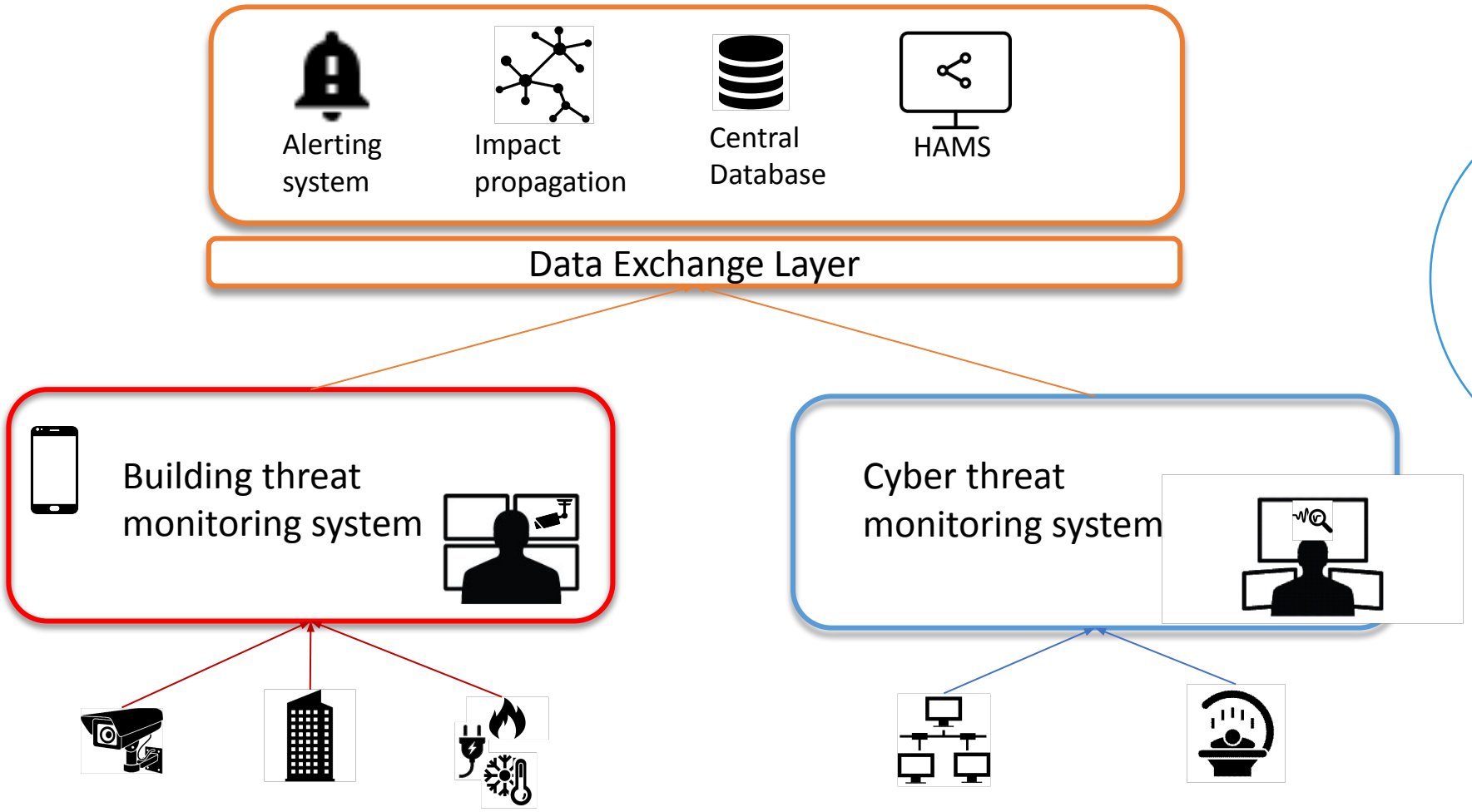
48%_ of IT managers use cloud-based video surveillance or access control[8]

72%_ of employees consider leaving sensitive information in publicly accessible areas the most serious threat to data security[14]

65%_ of over 1.000 employees surveyed reported behaving in ways and adopting practices identified as risky for physical security[15]

https://www.enisa.europa.eu/publications/physical-manipulation-damage-theft-loss

SAFECARE Global Architecture



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*"

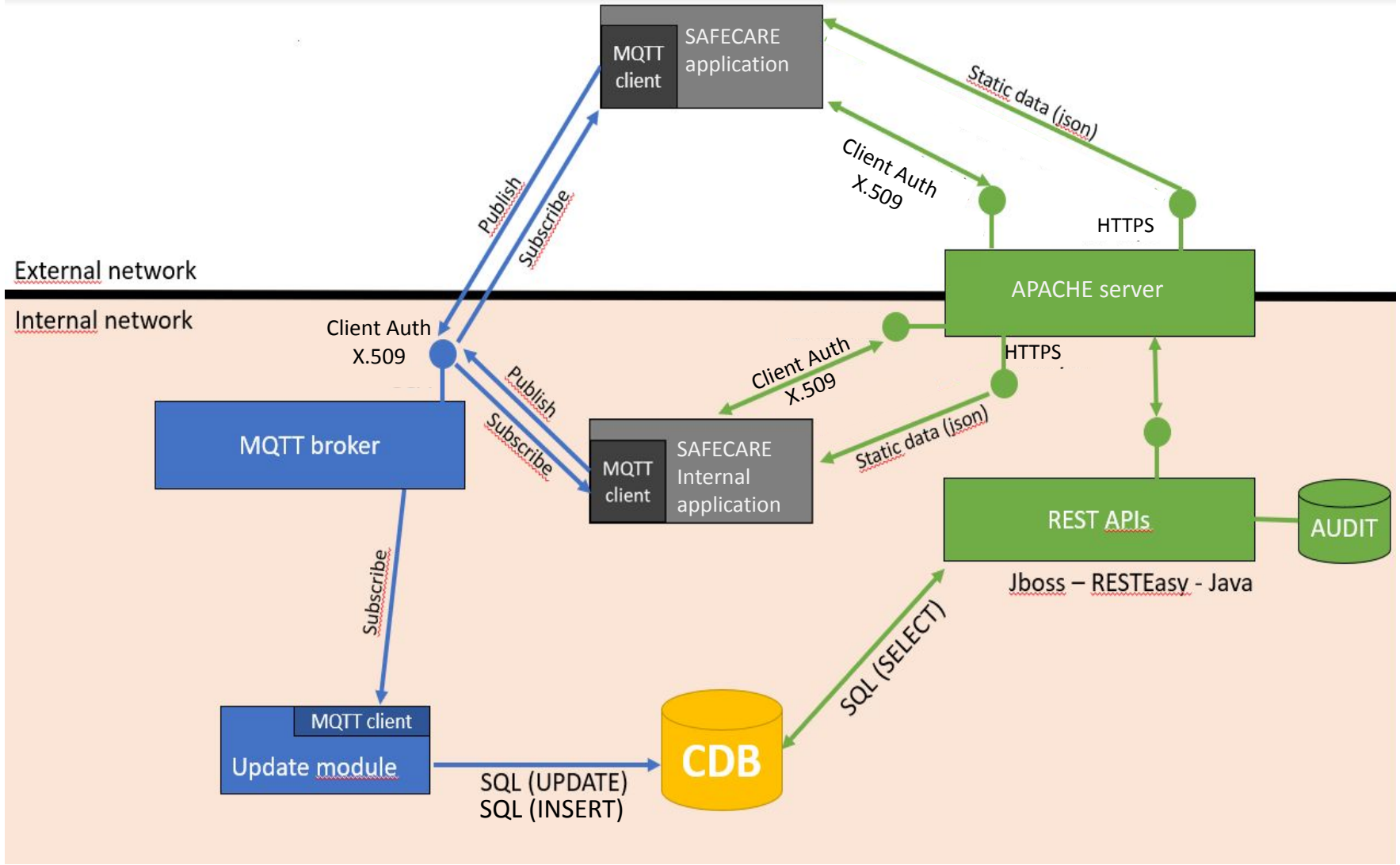
Inside SAFECARE, an incident consists of a set of security events verified by a human operator(guard or SOC operator) and forwarded as a unique message to systems that can evaluate the potential impacts of the incident and triggers automatic alerts.

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 Internal Architecture

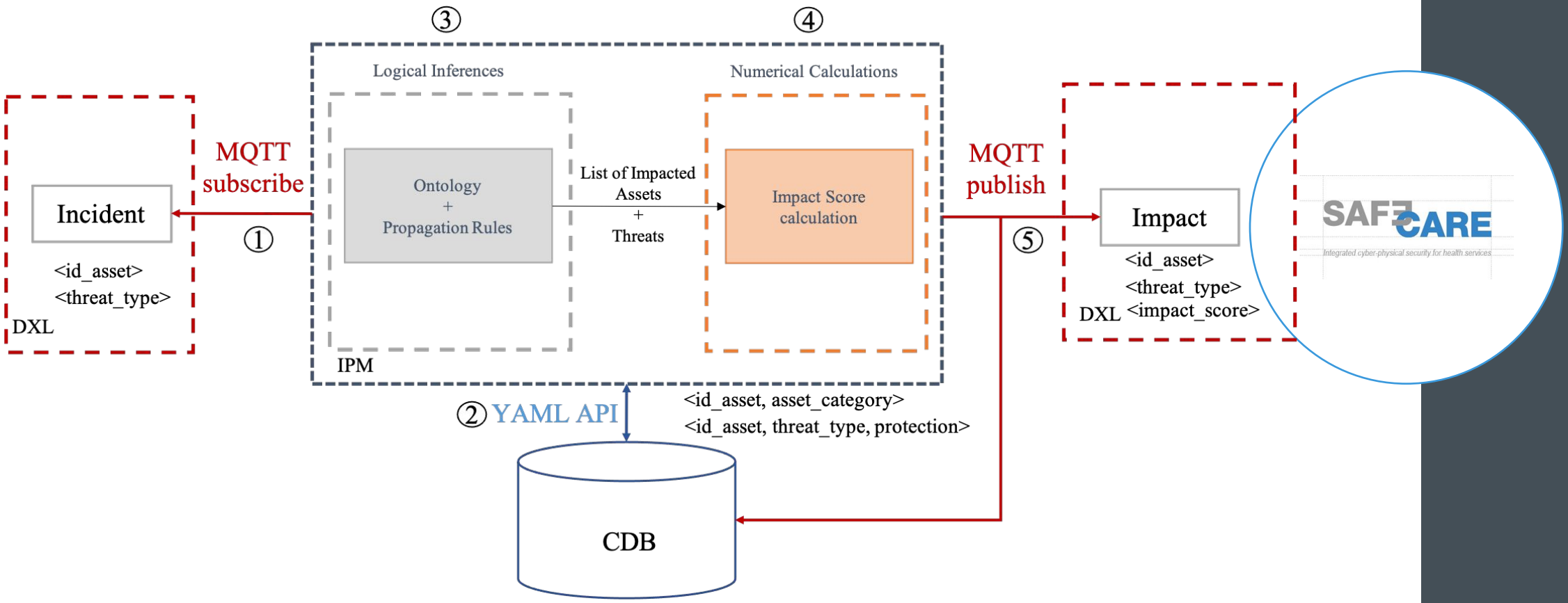


Impact propagation and decision support model

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



Threat Response and Alert System

To design and develop a system that automatically process reaction plans and send notification and alerts to relevant recipients, improve the coordination between internal and external security practitioners and contribute to improve the response time and fast service recovery

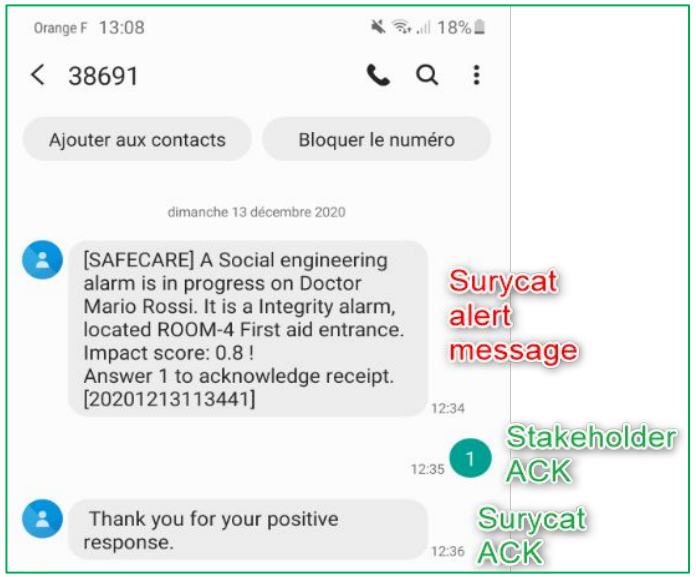
[SAFECARE] Impact score: 0.8! Social engineering, Integrity, ROOM-4 First aid entrance

Safecare <safecare@surycat.io>
À Guillaume Gaudel

Répondre | Répondre à tous | Transférer | ...

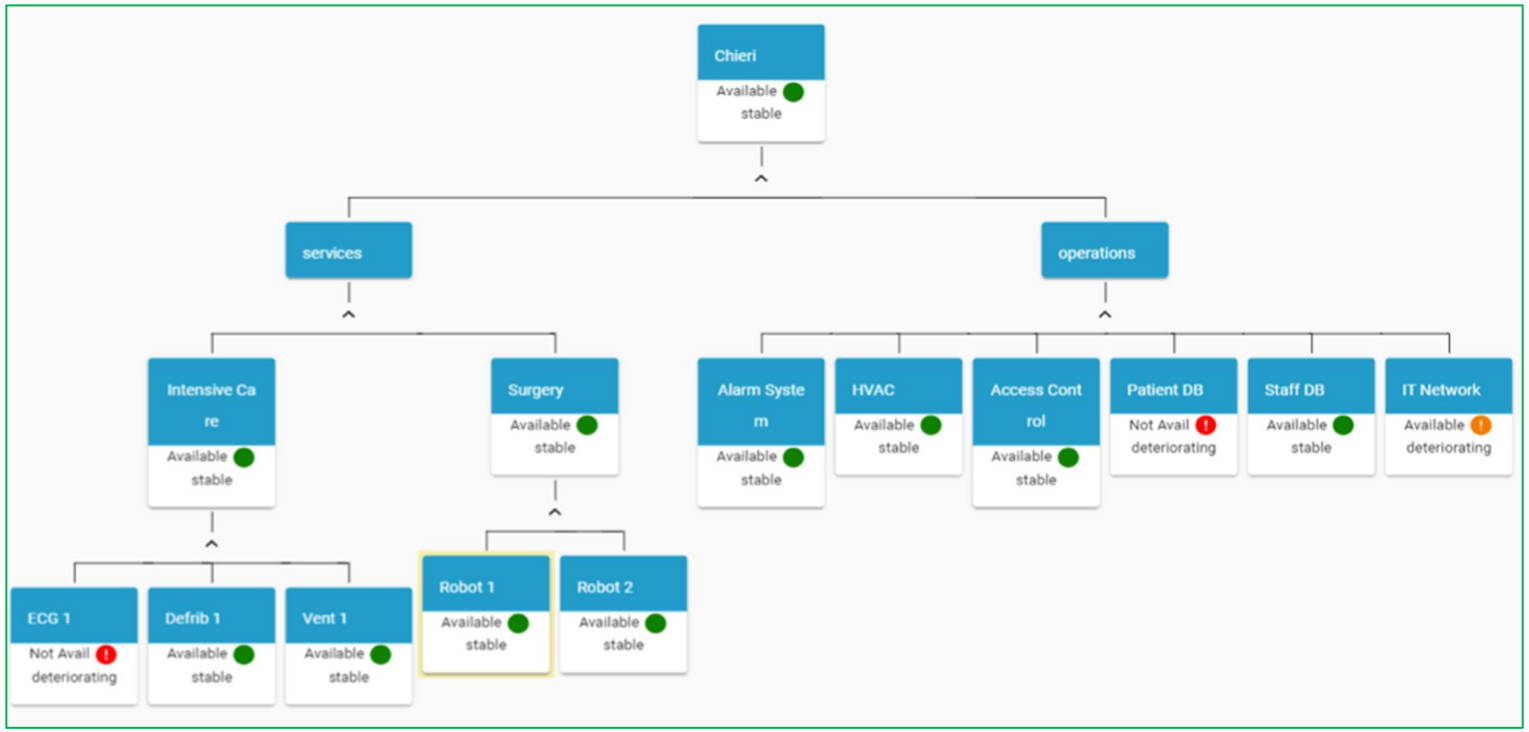
dim. 13/12/2020 12:38

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': '+33788689288'}], 'emails': [{'type': 'professional', 'address': 'ggaudel@enovacom.fr'}], 'places': [], '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}]}]

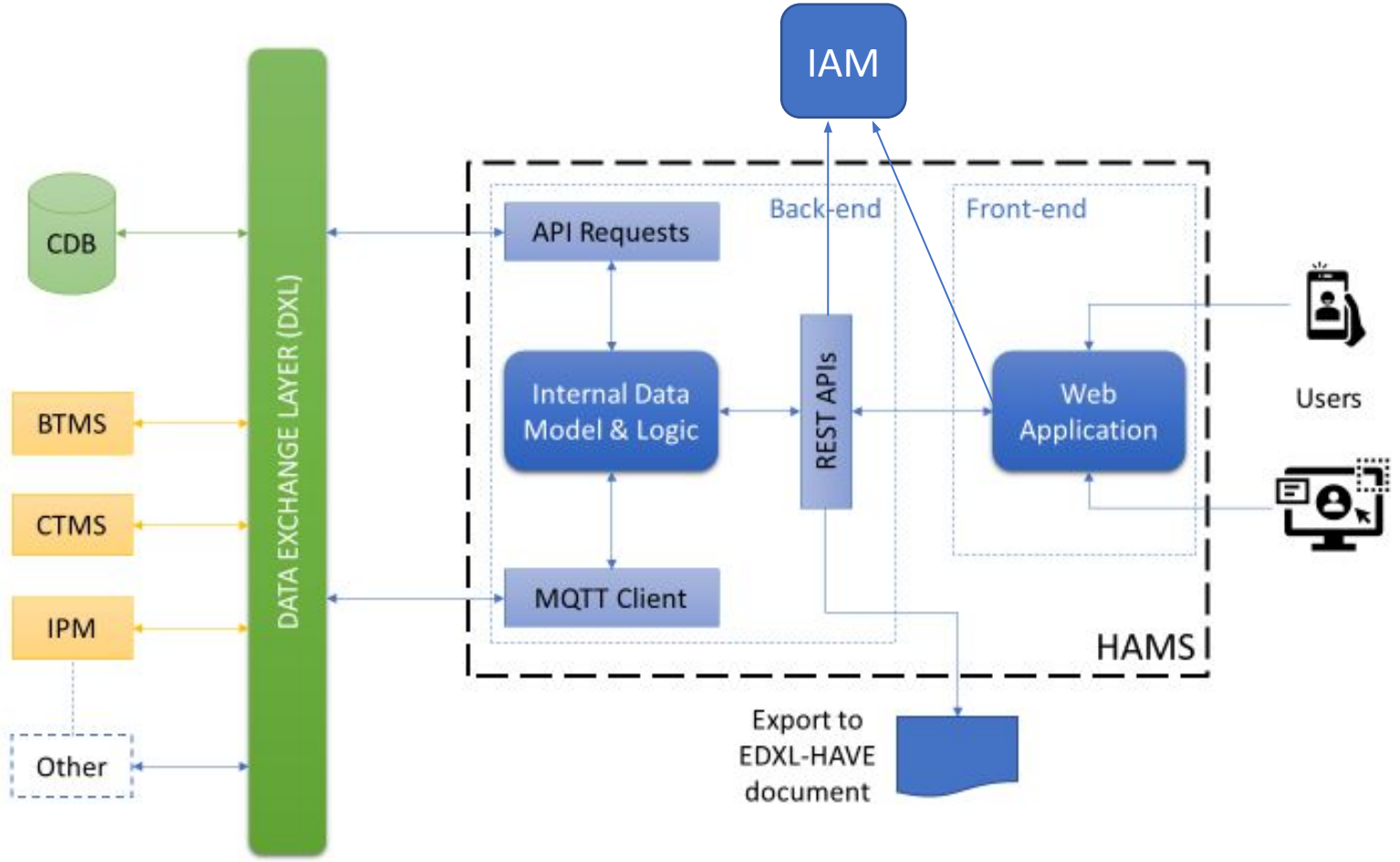


Hospital availability management system (HAMS)

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



Hospital availability management system (HAMS)

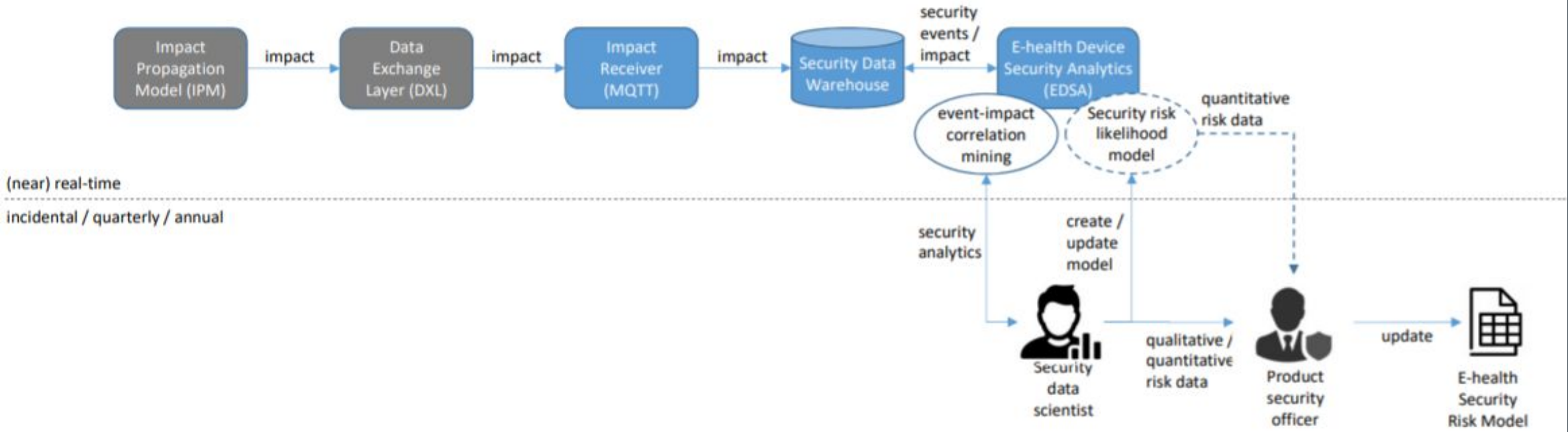


E-health security risk management model

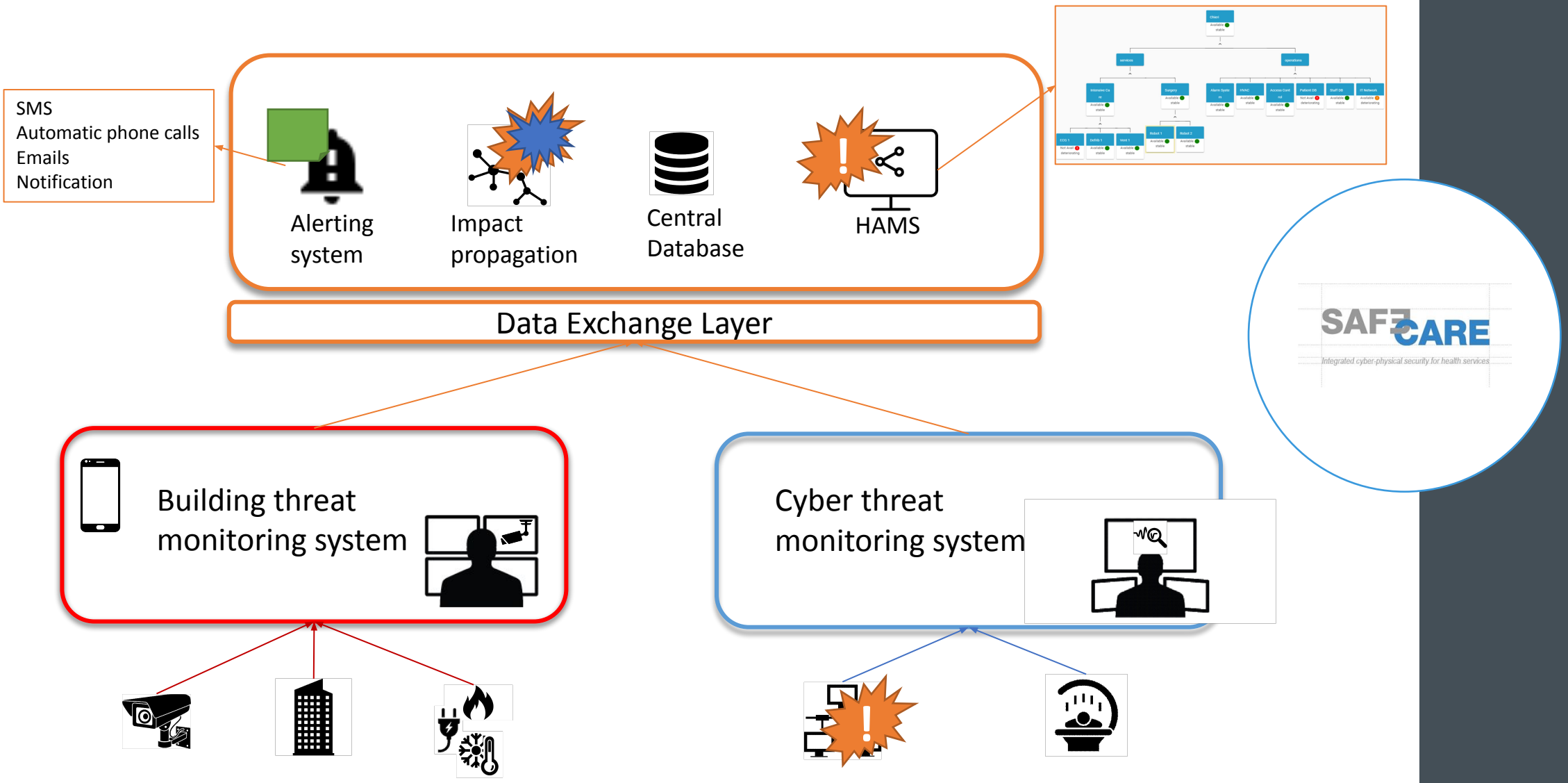
To design and develop a system that can quantify the impact of security events on medical devices and to design a risk management model

- E-health security risk management model leverage the BowTie method in combination with EBIOS to develop and update risk models for medical devices
- It is integrated with the SAFECARE system via E-health device security analytics, that can receive and correlate the impacts messages with alerts coming from e-health devices. This analysis validates the model and can result in an update of the security risk model.

E-health security risk management model



DEMO


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

Thank you !

More details available on:

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

Francesco Lubrano
francesco.lubrano@linksfoundation.com