Integrated cyber-physical security for health services

Specification of the global architecture

Deliverable 6.1

Lead Author: ACS

Contributors: LINKS, MS, CSI, CNAM, ENC, KUL, BEIA, FST, PEN, PMS

Deliverable classification: PU

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

Version Control Sheet

Title	Specification of the global architecture
Prepared By	ACS
Approved By	
Version Number	2.1
Contact	david.lancelin@airbus.com

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
1.0	30/09/2019	First complete version	DL	DL
2.0	21/10/2019	Changes according to reviewers' comments	DL	DL
2.1	25/11/2020	Updated to take into account remarks made during the first annual review	SDD	SDD

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.

Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND DEFINITIONS

BMS	Building Management System
BTMS	Building Threat Monitoring System
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CNIL	Commission Nationale de l'Informatique et des Libertés
CSIRT	Computer Security Incident Response Team
CTMS	Cyber Threat Monitoring System
DB	Database
DoS	Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EDXL	Emergency Data Exchange Language
EU	European Union
E-health	Digital health
GDPR	General Data Protection Regulation
HAMS	Hospital Availability Management System
HAVE	Hospital AVailability Exchange
HCAssets	Healthcare Critical Assests
ICS	Industrial Control Systems
IoC	Indicator of Compromise
IoT	Internet of Things
IPDSM	Impact Propagation and Decision Support Model
IT	Information Technology
JSON	JavaScript Object Notation
KG	Knowledge Graph
MISP	Malware Information Sharing Platform
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OT	Operational Technology

OWL2	Web Ontology Language
PC	Personal Computer
PIA	Privacy Impact Assessment
PLC	Programmable Logic Controller
R&D	Research and Development
RDF	Resource Description Framework
REST	Representational State Transfer
RSE	Remote Support Engineer
SCADA	Supervisory Control And Data Acquisition
SDK	Software Development Kit
SMS	Short Message Service
SOC	Security Operation Center
SPAN	Switched Port Analyzer
TAP	Terminal Access Point
TCP	Transmission Control Protocol
TDB2	Component of Apache Jena for RDF storage and query
TLS	Transport Layer Security
TRAS	Threat Response and Alert System
UDP	User Datagram Protocol
USB	Universal Serial Bus
VMS	Video Management System
W3C	World Wide Web Consortium
WP	Work Package
WP29	Article 29 Working Party
XProtect	Video Management Software developed by Milestone
Zero-day	A zero-day vulnerability is an unknown vulnerability

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 proposal 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.

Executive Summary

The objective of SAFECARE is to bring together the most advanced technologies from the physical and cyber security spheres to achieve a global optimum for systemic security and for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects. The project focuses on health service infrastructures and works towards the creation of a global protection system, which covers threat prevention, threat detection, threat response and, in case of failure, mitigation of impacts across infrastructures, populations and environment.

The architecture of SAFECARE addresses its objective through its division into three technical work packages. One work package is dedicated to the physical security systems, while another is devoted to cyber security systems. And last, the work package about the integrated cyber-physical security systems allows interconnecting the physical and cyber security spheres so that health service infrastructures can cope the combination of cyber and physical threats.

This deliverable provides an overview of the overall architecture and describes each system and its interconnections to insure consistency between the systems, so that the objective of SAFECARE can be achieved. Some communication standards are also mentioned to define guidelines for the implementation of the solutions. It is especially specified the standards for exchanging and sharing data between the threat detection systems and the threat monitoring system, between the cyber and physical security systems and the integrated cyber-physical security systems, and between different emergency systems.

Data exchange protocols, data models and data storage are depicted through the descriptions of the data exchange layer, the central database as well as ontologies and graph data model. It is defined how to share information between software components relying on referent datasets.

The privacy and data protection aspects concerning the SAFECARE solutions are highlighted with the results of the Data Protection Impact Assessments (DPIA) in order to foster trust in the processing operations that are performed within the systems of the global architecture.

Finally, a strategy of defence is disclosed to protect the hospitals of Marseille, Turin and Amsterdam against the scenarios of threats. The strategy describes the threat detection and the threat response for each scenario.

Introduction

The SAFECARE project aims at providing a global protection system that covers threat prevention, threat detection, threat response and, in case of failure, mitigation of impacts across infrastructures, populations and environment for health services infrastructures. This deliverable, which is the specification of the global architecture, provides an overview of the overall SAFECARE architecture and insures the consistency between the different technical solutions.

First, the global architecture is presented in Section 1 as well as each system part of the architecture. Then, descriptions of the systems interconnections for the physical security systems, the cyber security systems and the integrated cyber-physical security systems are provided in Section 2. Data exchange protocols, data models and data storage are addressed in Section 3. Information sharing between software components such as referent datasets and normalized assessment scales are explained in Section 4. Then, the privacy and data protection aspects regarding SAFECARE solutions are presented in Section 5. Finally, the strategy of defence for protecting target infrastructures is disclosed in Section 6.

1 Global architecture and systems

This section describes the global architecture as well as each system of the SAFECARE architecture.

1.1 Global architecture

The SAFECARE architecture can be broken down into 3 parts, as shown in Figure 1:

- Physical security solutions (Work Package 4)
- Cyber security solutions (Work Package 5)
- Integrated cyber-physical security solutions (Work Package 6)

The physical security solutions and the cyber security solutions consist of smart modules and efficient integrated technologies to respectively improve physical security and cyber security. More specifically, physical security solutions embed integrated intelligent video monitoring and interconnect building monitoring systems as well as management systems. While cyber security solutions correspond to cyber monitoring systems as well as threat detection systems related to IT, BMS and e-health systems. Both physical security solutions and cyber security solutions are interconnected thanks to the integrated cyber-physical security solutions. The integrated cyber-physical security solutions consist of intelligent modules to integrate different data sources and better take into account the combination of physical and cyber security threats.

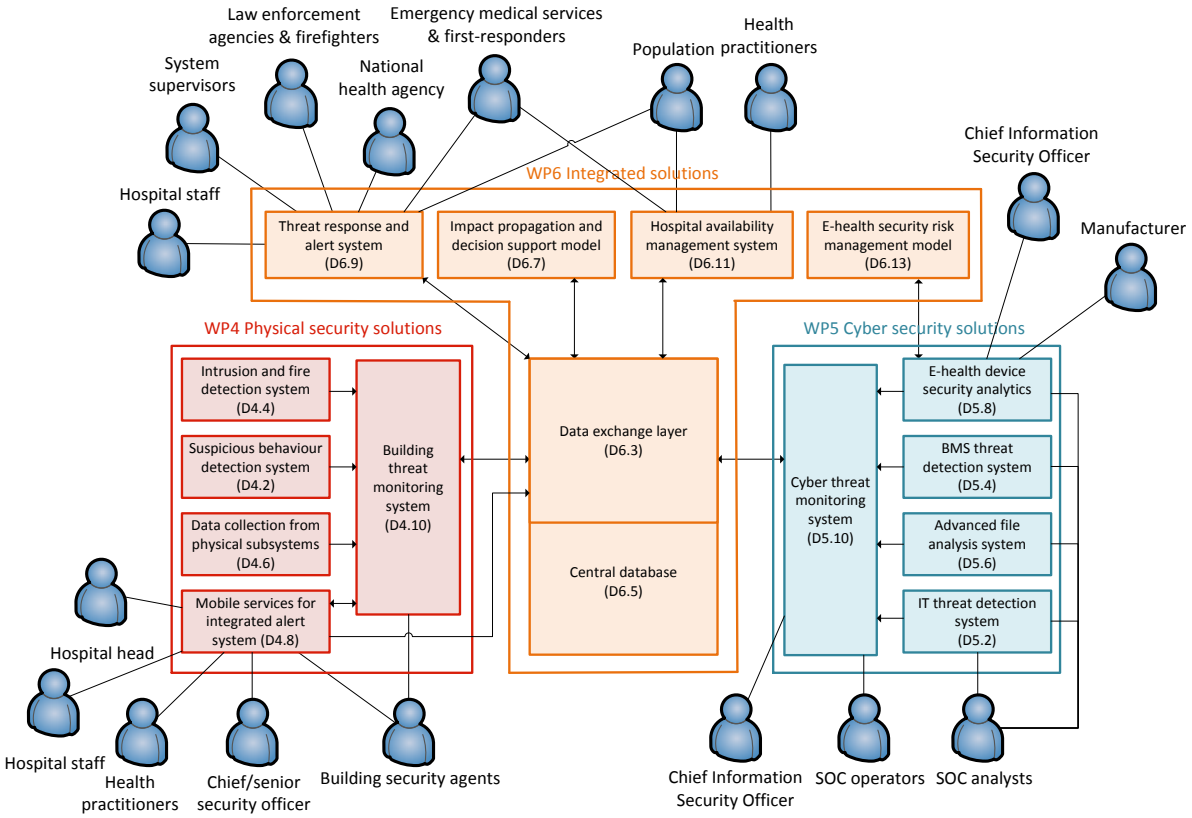

Figure 1 – Global architecture

The following systems make up the physical security solutions:

- The suspicious behaviour detection system (Deliverable 4.2) described in Section 1.2;

- The intrusion and fire detection system (Deliverable 4.4) described in Section 1.3;
- The data collection system (Deliverable 4.6) described in Section 1.4;
- The mobile alerting system (Deliverable 4.8) described in Section 1.5;
- And the building threat monitoring system (Deliverable 4.10) described in Section 1.6.

The following systems make up the cyber security solutions:

- The IT threat detection system (Deliverable 5.2) described in Section 1.7;
- The BMS threat detection system (Deliverable 5.4) described in Section 1.8;
- The advanced file analysis system (Deliverable 5.6) described in Section 1.9;
- The e-health devices security analytics (Deliverable 5.8) described in Section 1.10;
- And the cyber threat monitoring system (Deliverable 5.10) described in Section 1.11.

The following systems make up the integrated cyber-physical security solutions:

- The data exchange layer (Deliverable 6.3) described in Section 1.12;
- The central database (Deliverable 6.5) described in Section 1.13;
- The impact propagation and decision support model (Deliverable 6.7) described in Section 1.14;
- The threat response and alert system (Deliverable 6.9) described in Section 1.15;
- The hospital availability management system (Deliverable 6.11) described in Section 1.16;
- And the e-health security risk management model (Deliverable 6.13) described in Section 1.17.

1.2 Suspicious behaviour detection system

The abstract interaction of components to integrate suspicious behaviour detection is shown below:

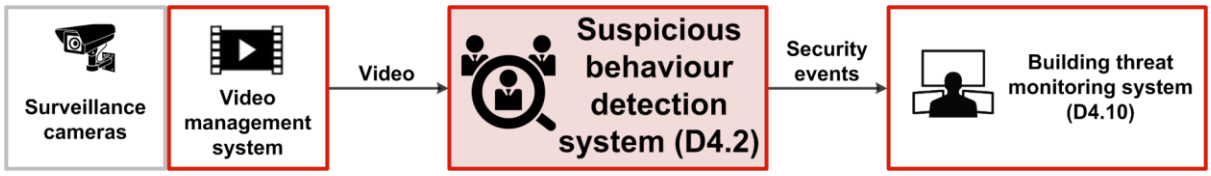

Figure 2 – Interconnections of the suspicious behaviour detection system

For the most part, suspicious behaviour will be predicted based on machine learning models over the video surveillance cameras, unlike other physical security components, which will fuse data from multiple sources.

In order to allow a flexible integration of subsystems, both reused from XProtect and developed specifically for the SAFECARE project, a more detailed interaction will be followed, as shown below in a diagram reproduced from Deliverable 4.3 on Intrusion and Fire Detection, as considered in the following subsection:

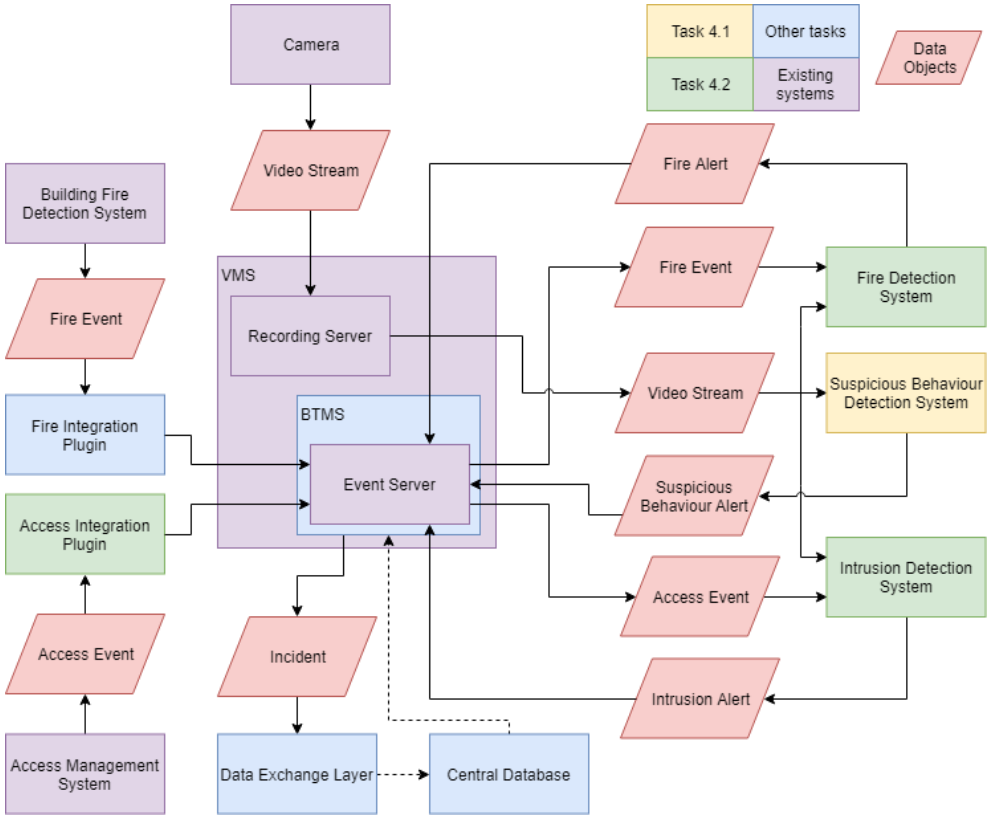

Figure 3 – Diagram of physical security systems interactions

In general the components on the right-hand side of the diagram, which may involve video analytics as in this case, carry out their prediction on the direct input streams (video streams or event streams) and produce alerts. The Building Threat Monitoring System (BTMS) may carry out further analysis in context; i.e. the suspicious behaviour detection system may raise an alert about loitering, then the BTMS judges, using further information from the central database, where the loitering is taking place (loitering is fine in Reception, more suspicious at the entrance to a controlled area).

1.3 Intrusion and fire detection system

As discussed above, physical security modules may fuse data from several sources, as is the case respectively with intrusion and with fire detection, as shown in the abstract below:

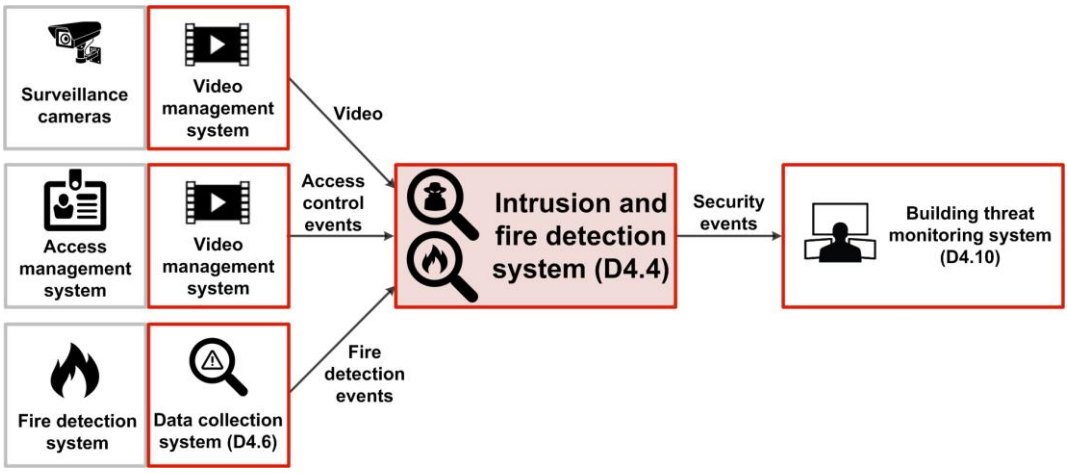

Figure 4 – Interconnections of the intrusion and fire detection system

In the diagram of Figure 3, the two systems are separated (although they're documented in one specification and produce one software deliverable) for clarity. Both camera streams and access management events, for most major vendors (see Section 2.1), are covered by existing integrations with the XProtect software. As shown above, the XProtect Event Server, on which the BTMS is based, as described in Section 1.6, will accept events from the data collection system for physical sensors for fire detection (smoke, heat, etc.) – see following subsection.

1.4 Data collection system

The system collects data from physical subsystems (such as ICS, SCADA, smart building sensors) as shown in Figure 5.

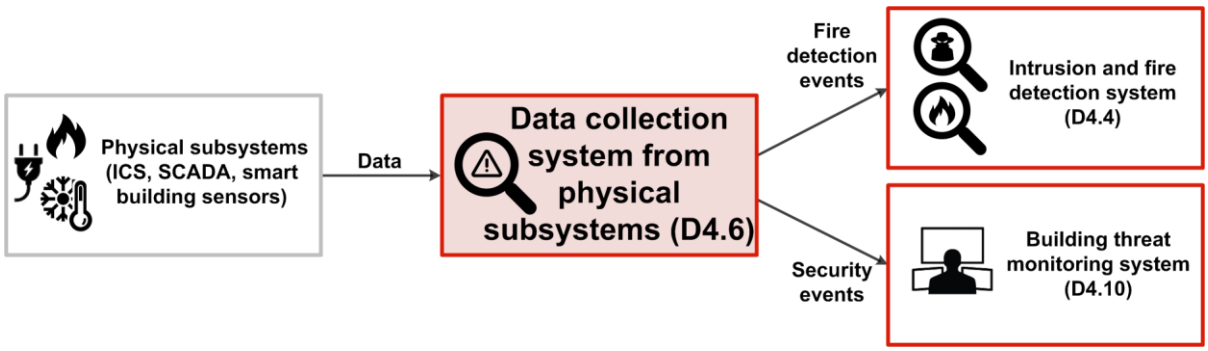

Figure 5 – Interconnections of the data collection system

The data collection system sends fire detection events to the intrusion and fire detection system.

The list of fire detection events can be the following:

- set a fire somewhere in the hospital in order to start an evacuation of the hospital;
- a bad intentioned person triggers the fire detection with a lighter in order to evacuate people;
- breaking the energy cabinet and by taking out the main power supply with fire or bombing, from the inside or outside of the hospital;

The data collection system also sends security events to the building threat monitoring system.

The list of security events can be the following:

- fraudulent use of access control key;
- tailgating;
- disrupting the power supply of the hospital (by getting access to the PLCs);
- get physical access to the hospital by distracting the receptionist and get access to the unlocked technical room;
- digital attack to cause a hardware fault;
- perform phishing attack and get physical access to the hospital change software parameters to harm patients;
- impersonate vendor to install malicious software to hurt reputation and affect patient treatment;
- taking out the air-cooling system of the hospital in order to contaminate surgery rooms, expand virus seeds and taking out data centres;
- the theft of data from hospital equipment that an insider has access to;

- stealing or replacing the IoT devices, or identifying vulnerabilities in the IoT devices to perform cyber-attacks;
- blocking information for the National Crisis Management system;
- stealing patient's data from the hospital's database;
- strategic attacks on the systems and medical devices of a hospital.

1.5 Mobile alerting system

The mobile alerting system will be used by local security agents providing the 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...), and to visualize contextual information (e.g. geolocation, building, room, timestamp and any relevant multimedia data).

The mobile alerting system will provide a means to report physical security events to security and health personnel, as illustrated in Figure 6.

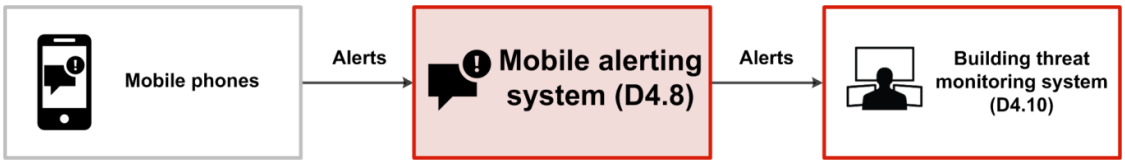

Figure 6 – Mobile alerting system sending alerts

Moreover, as shown in Figure 7, the system is able to receive physical security events by BTMS and relay those to security agents via SAFECARE Mobile application to assess if alert must be deemed as incident. The evaluation will be reported to Building threat monitoring system (BTMS).

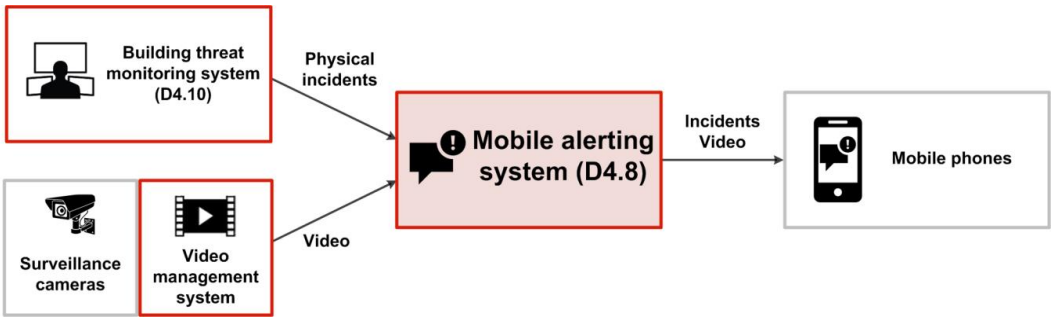

Figure 7 – Mobile alerting system receiving physical incidents

The Mobile alerting system will help BTMS to visualize the output of the impact propagation model, sending potential impacts to the supervisor in charge (hospital general manager, security chief). The impact information will be visualized within the mobile app as illustrated in Figure 8.

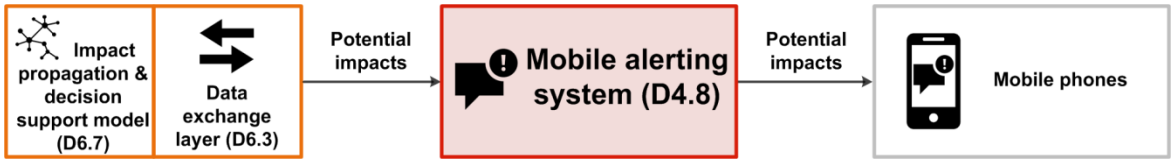

Figure 8 – Mobile alerting system receiving potential impacts

Finally, as shown in Figure 9, the system will send notifications which consist of all the information needed to manage the security threat (e.g. location, emergency procedure, video...). The notifications will be sent to all the users according to their profile.

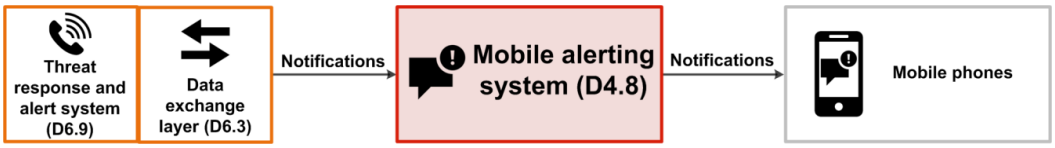

Figure 9 – Mobile alerting system receiving notifications

1.6 Building monitoring system

The Building Threat Monitoring System is the basis for interaction of the physical security components with the rest of the architecture. There are three aspects to this interaction, as explained below.

First, in order to just the alerts raised by physical security components in context (Where did the activity that led to the alert take place? What is the status of personnel – if they can be identified – engaging in the activity? Does an intrusion allow – via new/unprotected access routes – intruders access to critical assets?), the BTMS may retrieve information on assets and agents from the central database (see Figure 10):

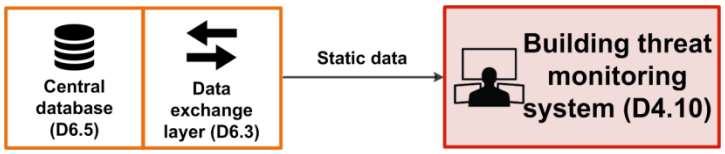

Figure 10 – Building threat monitoring system getting static data

Second, the BTMS is the central point for communicating incidents, which may be alerts or combinations of alerts and events that have been judged to need a security response, with the rest of the architecture via the data exchange layer, as shown below:

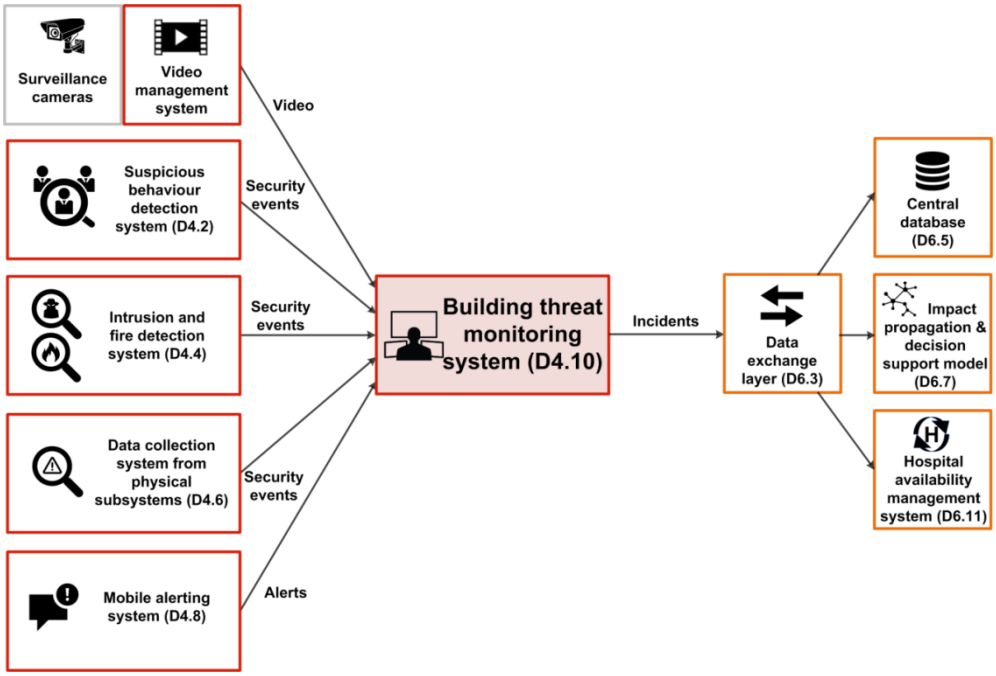

Figure 11 – Interconnections of the building threat monitoring system

Finally, the BTMS is responsible for receiving and relaying the incident handling response and decision support, according to the impact propagation model, as shown below:

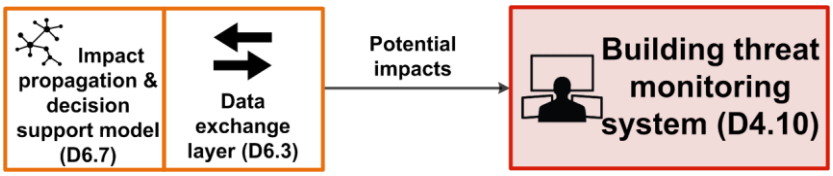

Figure 12 – Building threat monitoring system receiving potential impacts

1.7 IT threat detection system

Health services often face reconnaissance scans that look at software vulnerabilities in order to prepare cyber intrusions. Some attacks have already paralyzed hospitals, such as WannaCry in May 2017, exploiting zero-day vulnerabilities. The objective of the IT threat detection system is to detect the exploit of such vulnerabilities in critical health infrastructure by monitoring the network traffic and analyzing IT events (such as software logs) provided by the IT infrastructure.

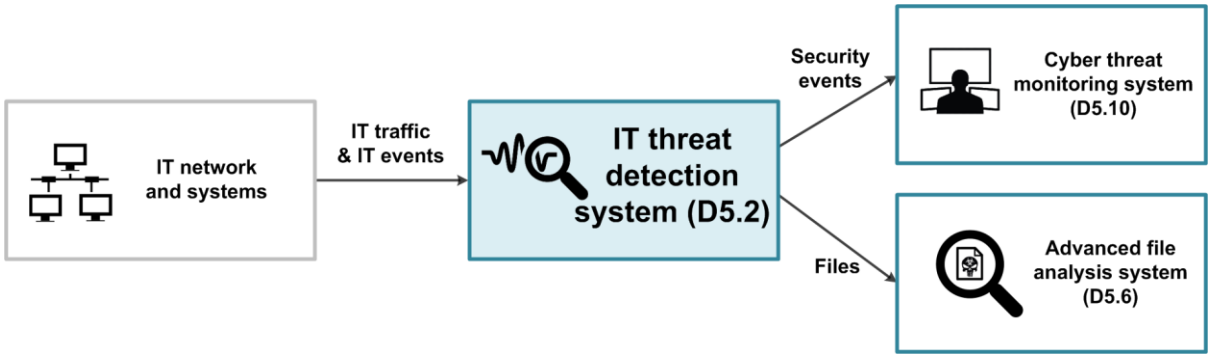

Figure 13 – Interconnections of the IT threat detection system

The IT threat detection system requires the network traffic to be duplicated in order to detect network attacks. The techniques used for this purpose are port mirroring, by connecting to the SPAN (Switched Port Analyzer) port of a network switch, or the use of network TAP (Terminal Access Point). Then, the IT threat detection system inspects the network traffic in real time by matching attack patterns, also known as signatures. The system generates security events for signature matches.

The IT threat detection system also receives IT events from the IT systems (firewalls, virtual machines, operating systems …) to detect intrusions. For example, connecting a USB stick to a computer generates IT events. The IT infrastructure of health services must be configured to send these events. IT events are generally sent via Syslog messages. Security rules are implemented within the IT threat detection system in order to generate security events from the aggregation and correlation of IT events.

Machine learning algorithms are developed and set up for the IT threat detection system within the scope of the SAFECARE project. Machine learning algorithms take IT events and generated security events as input and aim at highlighting the low level signals of advanced attacks. The machine learning algorithms also produce security events.

As shown in Figure 13, the IT threat detection system is interconnected to the cyber threat monitoring system. The latter receives the security events generated by the former.

The IT threat detection system is also interconnected to the advanced file analysis system. The former extracts files from the network traffic and automatically submits them to the latter for analysis.

1.8 BMS threat detection system

The BMS threat detection system is based on SilentDefense, one of the products in the portfolio of Forescout Technologies. SilentDefense is a passive monitoring intrusion detection system which is specifically tailored for Operational Technologies (OT) protocols used in industrial and building automation systems. SilentDefense delivers state-of-the-art device visibility and asset inventory by analyzing the traffic data for more than 130 protocols. Furthermore it integrates several threat detection engines including a library of 2100+ signature of potential dangers for the OT network. This allows to catch both known and unknown threats and greatly helps to streamline the response and mitigation processes of cyber-incidents on OT network.

For SAFECARE, this intrusion detection system is enhanced with the support of several building automation protocols as well as numerous protocols which are commonly found in the medical space, e.g. in hospitals for exchanging patient information or images. In this way both in-depth visibility and threat detection will be available also in building automation networks.

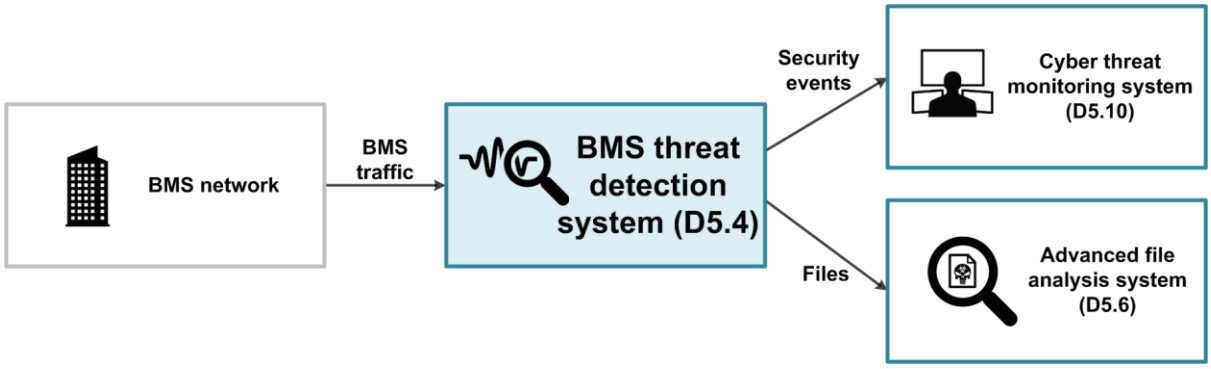

Figure 14 – Interconnections of the BMS threat detection system

As illustrated in Figure 14, the BMS threat detection system analyses the BMS network traffic. The same technics, as described below in Section 1.7, are used for replicating the traffic so that the traffic can be monitored. When threats are detected by the BMS threat detection system, the system generates security events that are sent to the cyber threat monitoring system. Within the scope of the SAFECARE project, the BMS threat detection system is improved to extract files from the network traffic and submit them to the advanced file analysis system for an in-depth analysis.

1.9 Advanced file analysis system

In health infrastructure, malwares (i.e. malicious software) can be propagated in seemingly non-suspicious health or administrative files, and in particular by attachments in e-mails. The objective of the advanced file analysis system is to detect the malwares in critical health infrastructure by performing an in-depth analysis of files.

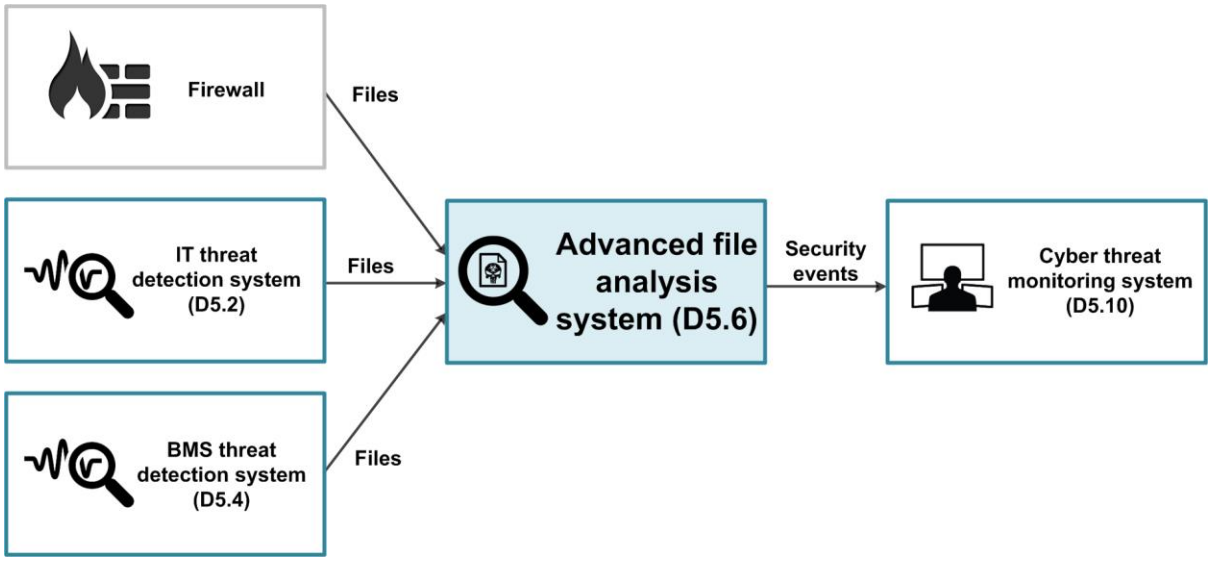

Figure 15 – Interconnections of the advanced file analysis system

The advanced file analysis system is interconnected to the IT threat detection system and the BMS threat detection system to analyse the files that transit respectively through the IT and BMS networks. To this purpose, the IT threat detection system and the BMS threat detection system submit files to the advanced file analysis system, as shown in Figure 15.

The advanced file analysis system performs a static analysis to look for malicious code into the files and a dynamic analysis to check file behaviour in a sandboxing environment. Following the analyses of a file, the advanced file analysis system produces a report that indicates a level of security risk. The main information of the report, such as the security risk level, is sent to the cyber threat monitoring system via security events.

Within the scope of the SAFECARE project, it is also experimented an interconnection with firewalls. Firewalls extract files from the network traffic and submit them to the advanced file analysis system. If a malware is detected, it allows firewalls to block the network connection with the source from which the malware originates.

1.10 E-health devices security analytics

E-Health device security analytics is a cybersecurity solution that is specialized for security monitoring, threat detection and reporting in healthcare infrastructures. The security analytics solution collects log data from medical devices, performs analytics to derive meaningful security data, and generates security insights, aggregated statistics and alerts upon detecting anomalous or suspicious security events. It aims at reducing cybersecurity risk stemming from medical devices that have been deployed at healthcare providers' sites and improving the overall security of the medical device infrastructures. Specifically, it targets to strengthen the quantitative and/or model-based approach to security risk assessment and management by creating actionable security insights.

Technically, the analytics functionality is realized through a data analytics platform that develops security models by applying data mining, machine learning and deep learning techniques on the data generated by medical devices. When these models identify potential security threats in the analyzed data, alerts are generated and sent to relevant stakeholders. The security insights and statistics resulting from these security models contribute towards improving product security risk assessment and management of connected e-health devices.

The detailed description, design specification and architecture of the e-health device security analytics solution is provided in Deliverable 5.7 "Specification of e-health device security analytics".

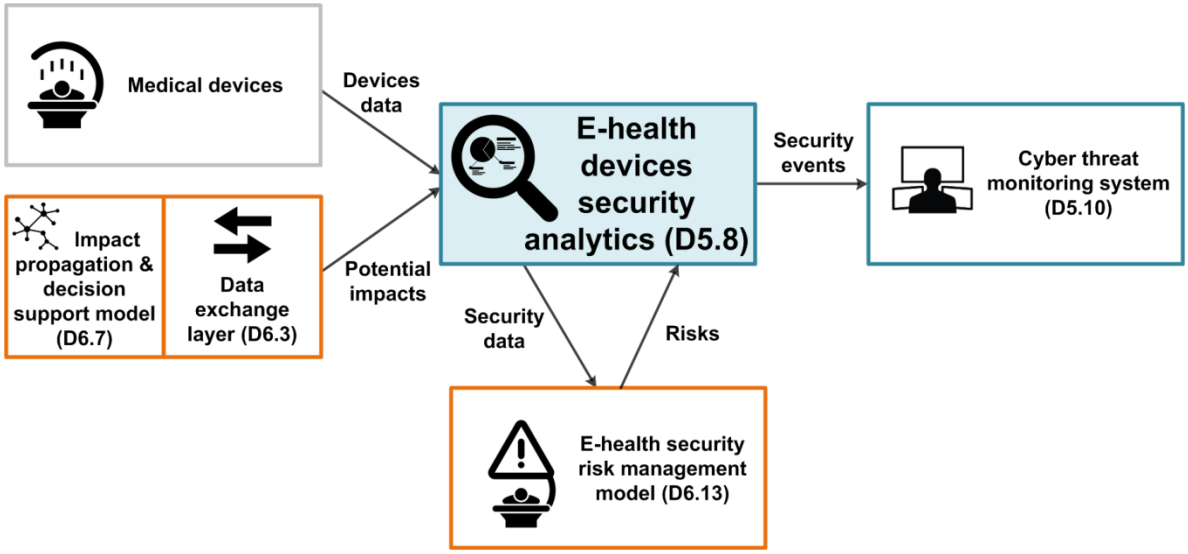

Figure 16 – Interconnections of the e-health devices security analytics

The interconnections between the e-health device security analytics solution and other components of the SAFECARE system is illustrated in Figure 16 and described below.

- **Medical devices**: The devices are manufactured by device manufacturers and deployed at healthcare providers (e.g. hospitals). The manufacturers receive log data for maintenance, monitoring and product improvement purposes. This includes security purposes. The security analytics solution acquires log data generated by the medical devices and performs analytics over this data.
- **Impact propagation model**: The security analytics solution retrieves a list of impacts resulting from the impact propagation model via the data exchange layer. These impacts could be used by the solution for post-incident analysis and to create new analytics models by leveraging the device manufacturer's development environment and its functions.
- **E-health security risk management model**: Aggregated security insights, event alerts resulting from the security analytics solution are sent to the e-health device security risk management model. The purpose of the risk management model is to assess the security risk in medical devices. Analytics results are used for improving this risk management model and also to take appropriate actions based on the type of alerts.
- **Cyber threat monitoring system**: As depicted in Figure 16 security alerts generated by the security analytics solution are sent to the cyber threat monitoring system. This system is responsible for centralizing the cyber security events from multiple security assets on a dashboard dedicated to SOC operators and other responder entities. This dashboard provides a global picture of cyber and physical security events and impacts to the SOC operators, assist them in better decision making and also improve investigation capacities by displaying relationships between "impacted" equipment and "monitoring" equipment.

1.11 Cyber threat monitoring system

The objective of the cyber threat monitoring system is to collect and centralize security events from the cyber threat detection systems, organize the information and provide user-friendly interfaces to SOC operators so that they can visualize the threats and have an overview of the impacted assets.

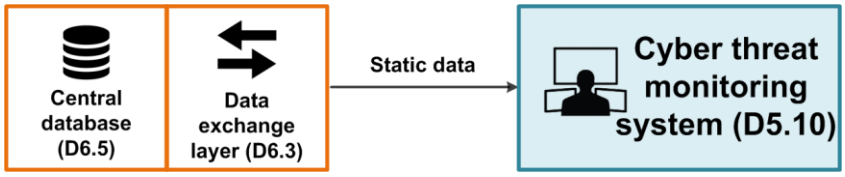

Figure 17 – Cyber threat monitoring system getting static data

In order to visualize the potential cascading effects of physical incidents on cyber assets, it is essential to have common and unique information about assets, services and sites between the building threat monitoring system, the cyber threat monitoring system and the integrated cyber-physical security solutions. This common and unique information (static data) is hosted and stored by the central database. The cyber threat monitoring system retrieves the static data from the central database through the data exchange layer, as illustrated in Figure 17.

The cyber threat monitoring system receives security events from the following systems:

- The IT threat detection system;
- The BMS threat detection system;
- The advanced file analysis system;
- And the e-health devices security analytics.

Rules are implemented within the cyber threat monitoring system to automatically generate alerts from the received security events. The cyber threat monitoring system is the entry point for SOC operators to monitor in real time all incoming cyber alerts. The system centralizes all the alerts regarding cyber threats. Then, after a first analysis phase, the SOC operators must confirm the alerts as either incidents or false-positive alerts.

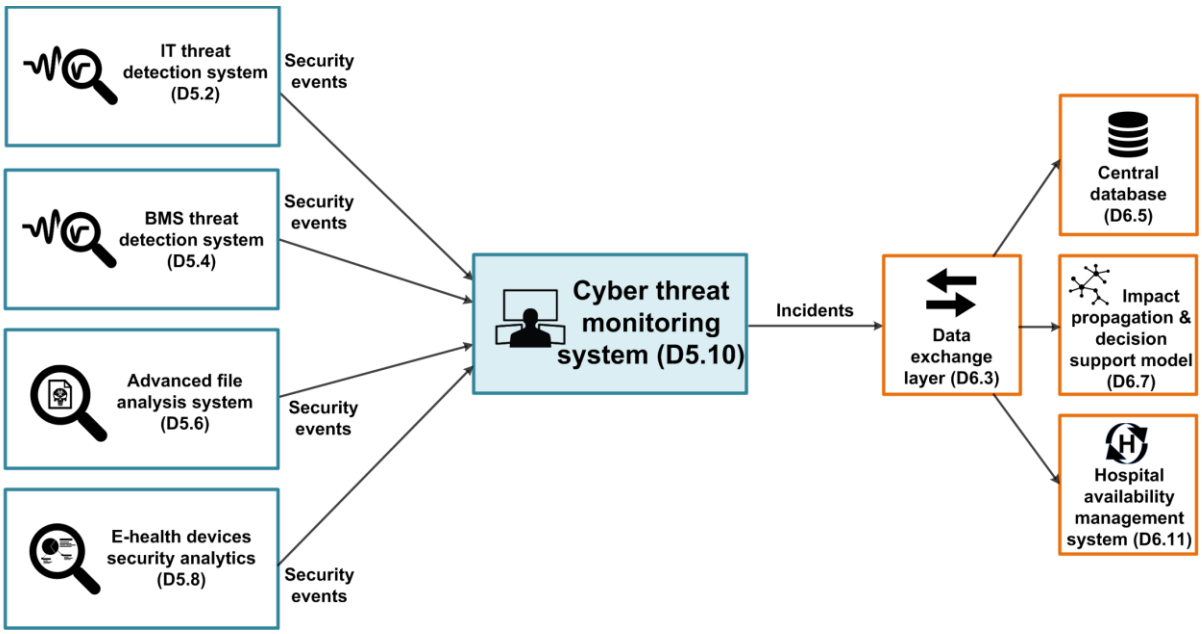

Figure 18 – Interconnections of the cyber threat monitoring system

In case of incidents, as illustrated in Figure 18, the incidents are forwarded through the data exchange layer to the following systems:

- The central database;
- The impact propagation and decision support model;
- And the hospital availability management system.

The cyber threat monitoring system receives potential impacts, which are computed from physical and cyber incidents by the impact propagation and decision support model, in order to provide SOC operators a clear understanding of potential impacted assets and services.

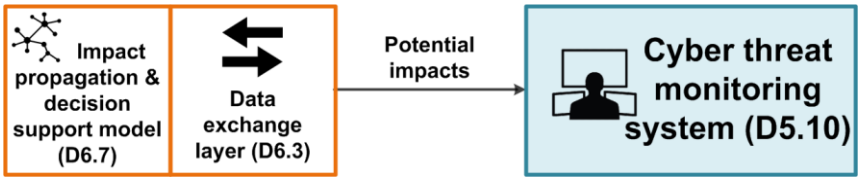

Figure 19 – Cyber threat monitoring system receiving potential impacts

As illustrated in Figure 19, the computed impacts, which are provided by the impact propagation and decision support model, allow SOC operators to visualize potential cascading effects and the cyber threat monitoring system to take into account a combination of both physical and cyber incidents.

All the SAFECARE systems among physical, cyber and integrated cyber-physical security solutions must send their security events (such as user authentication, system start/stop, updates …) to the cyber threat monitoring system.

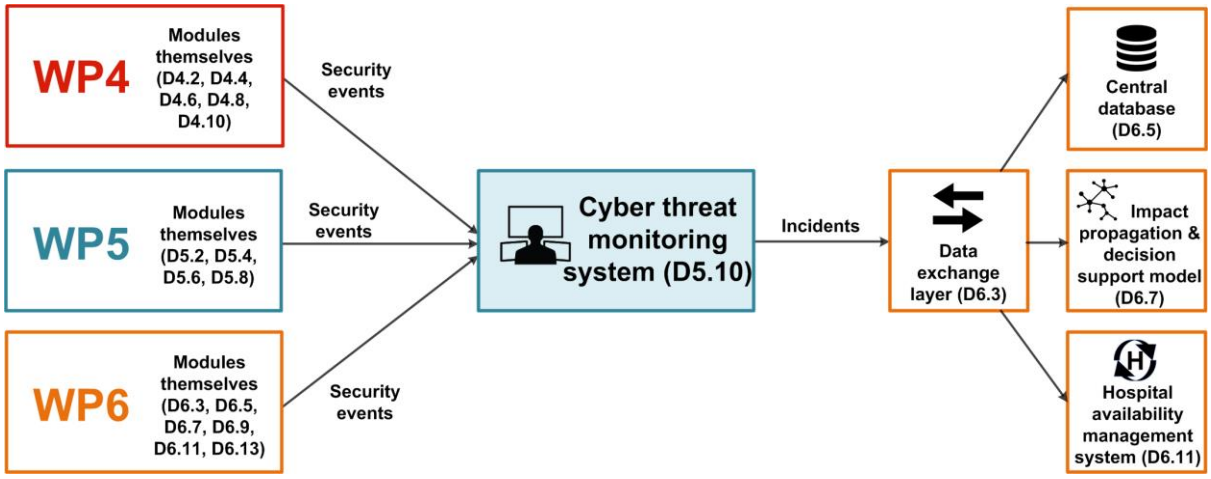

Figure 20 – Cyber monitoring of all SAFECARE modules

Therefore, as shown in Figure 20, the cyber threat monitoring system supervises the cyber security of the entire SAFECARE solution and sends incidents in case of cyber-attacks against SAFECARE modules.

1.12 Data exchange layer

The data exchange layer implements publish-subscribe mechanisms in order to trigger notifications to the other components when new physical and cyber incident (coming from the building threat monitoring system and the cyber threat monitoring system) or new impacts (coming from the impact propagation model) are sent. The data exchange layer will be

developed in order to store and extract data from the central database (e.g. web services). It will dynamically check the data format and data content before storage by checking static referential of data (e.g. list of critical assets, scale of impacts, names of rooms and buildings). The data exchange layer will allow other project components to extract added-value information on demand from the central database.

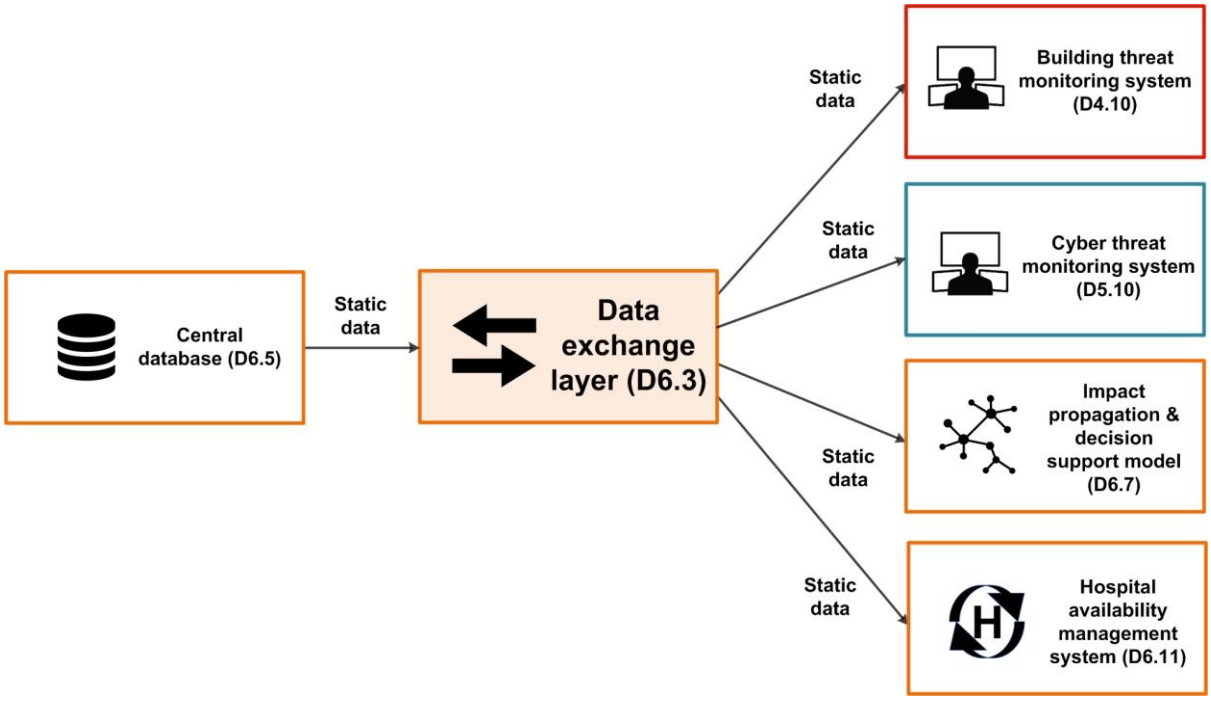

Figure 21 – Data exchange layer forwarding static data

As illustrated in Figure 21, the building threat monitoring system, the cyber threat monitoring system, the impact propagation and decision support model and the hospital availability management system get static data from the central database through the data exchange layer.

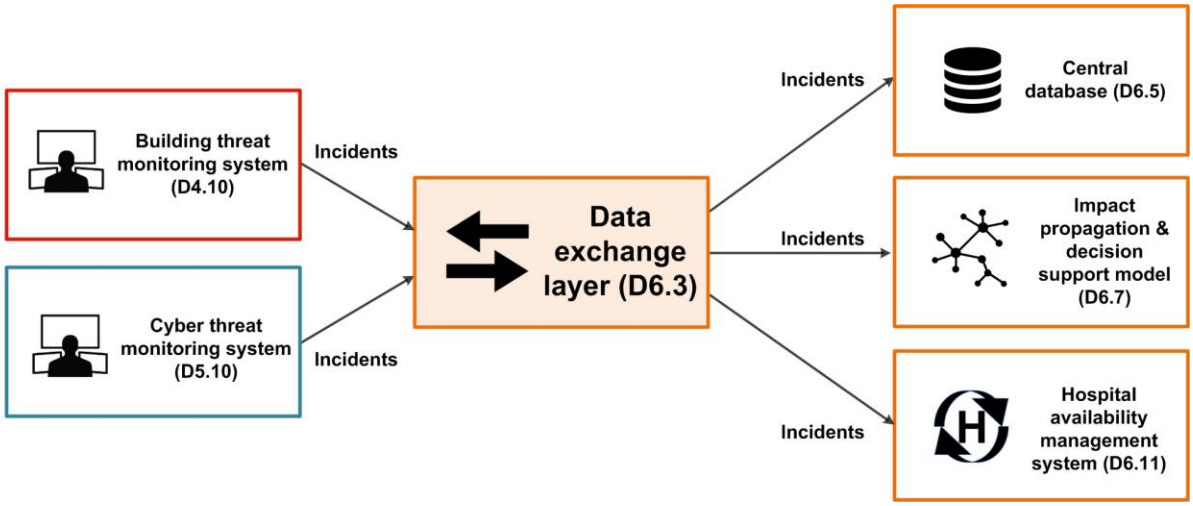

Figure 22 – Data exchange layer forwarding incidents

As illustrated in Figure 22, the data exchange layer forwards incidents from the building threat monitoring system and the cyber threat monitoring system to the central database, the impact propagation and decision support model and the hospital availability management system.

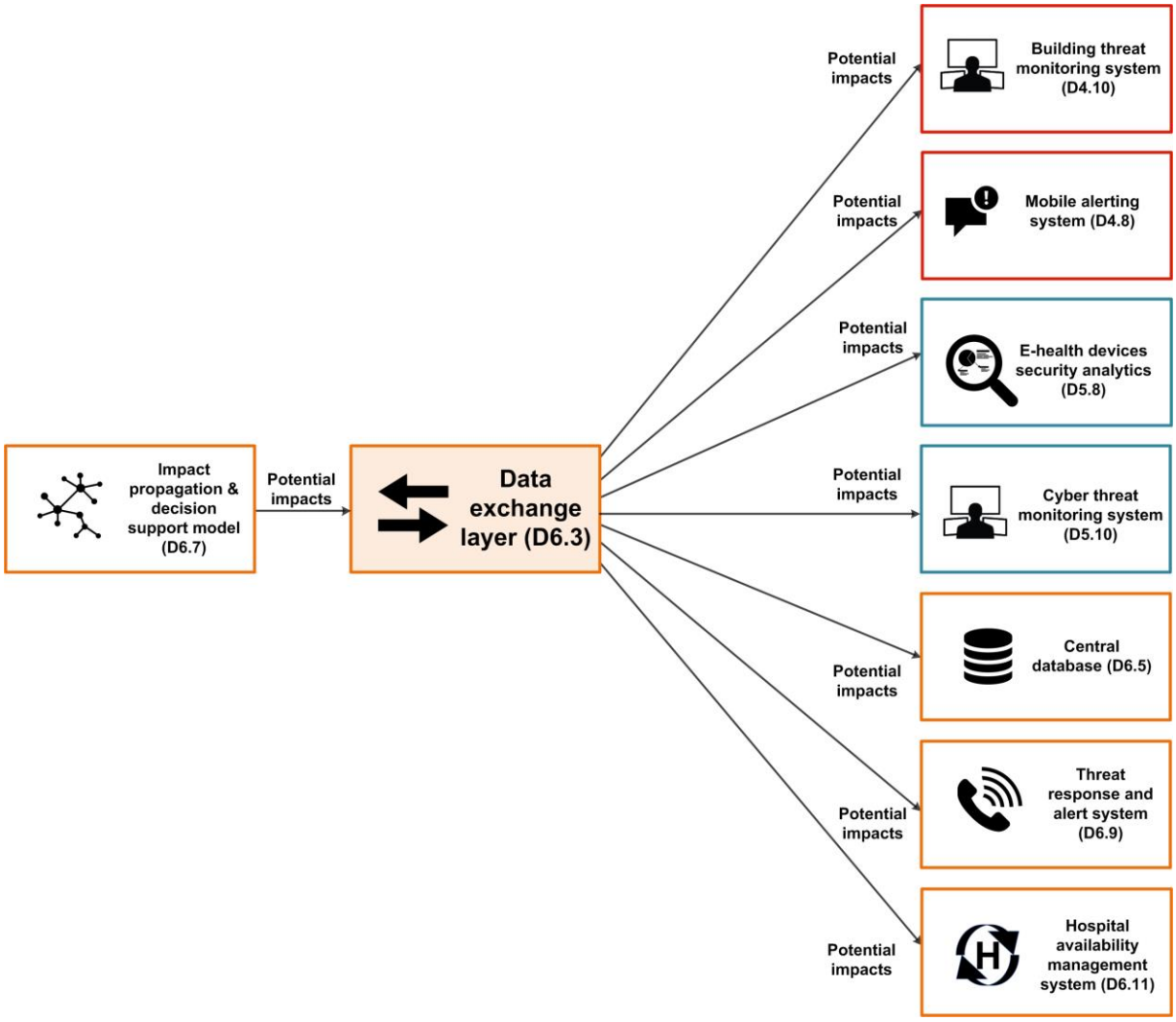

Figure 23 – Data exchange layer forwarding potential impacts

As illustrated in Figure 23, the data exchange layer forwards potential impacts from the impact propagation and decision support model to the building threat monitoring system, the mobile alerting system, the e-health devices security analytics, the cyber threat monitoring system, the central database, the threat response and alert system and the hospital availability management system.

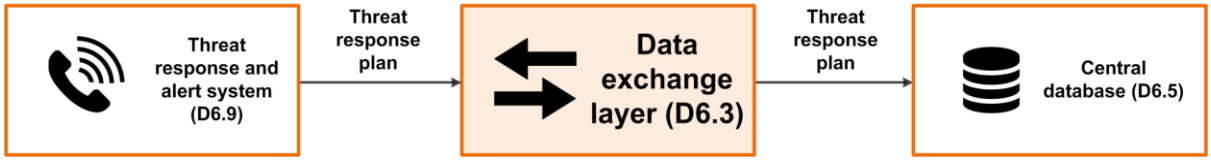

Figure 24 – Data exchange layer forwarding threat response plan

As illustrated in Figure 24, the data exchange layer forwards threat response plans from the threat response and alert system to the central database.

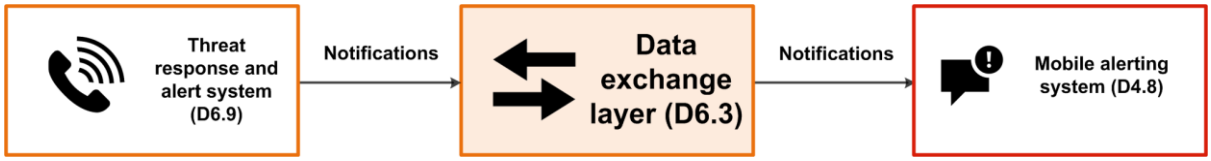

Figure 25 – Data exchange layer forwarding notifications

As illustrated in Figure 2523, the data exchange layer forwards notifications from the threat response and alert system to the mobile alerting system.

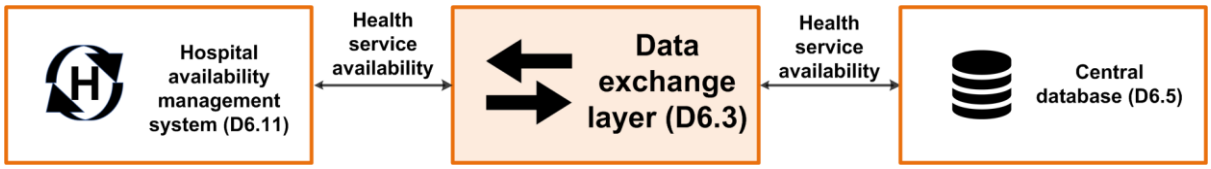

Figure 26 – Data exchange layer forwarding health service availability

As illustrated in Figure 26, the data exchange layer forwards health service availability from the hospital availability management system to the central database.

1.13 Central database

Data centralization in a single database constitutes the pillar stone in order to build added-value indicators. Cross connecting data expands the capacity to create either more consistent results or innovative results. The architecture of the database will take into account confidentiality, ethics and privacy constraints. For instance, personal data will not be mixed with equipment statuses. The central database will include a dynamic data store and a static data store, as illustrated in Figure 27 and 28.

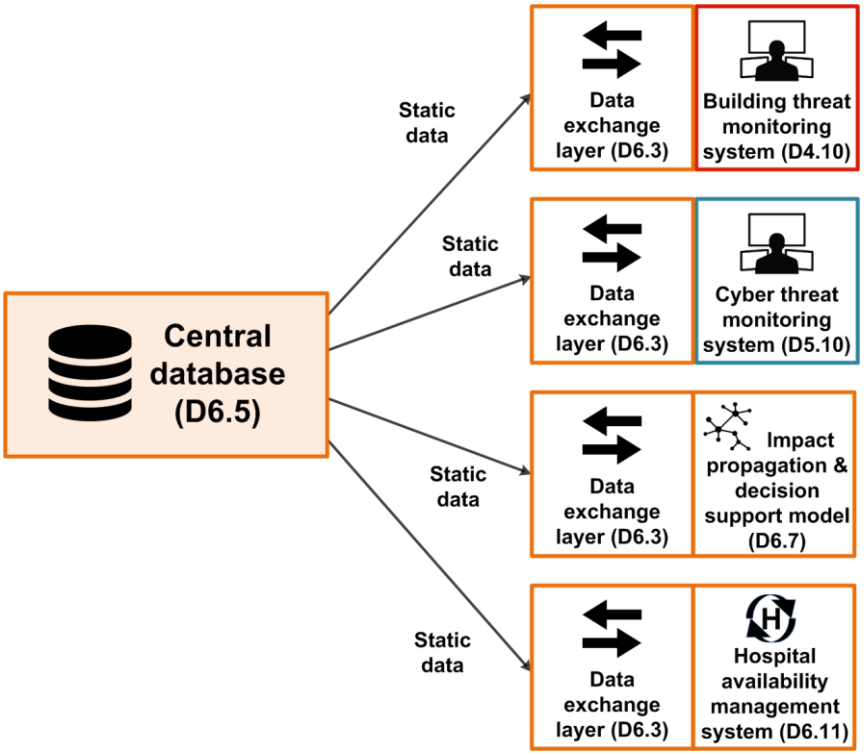

Figure 27 – Central database providing static data

The central database provides static data to the building threat monitoring system, the cyber threat monitoring system, the impact propagation and decision support model and the hospital availability management system.

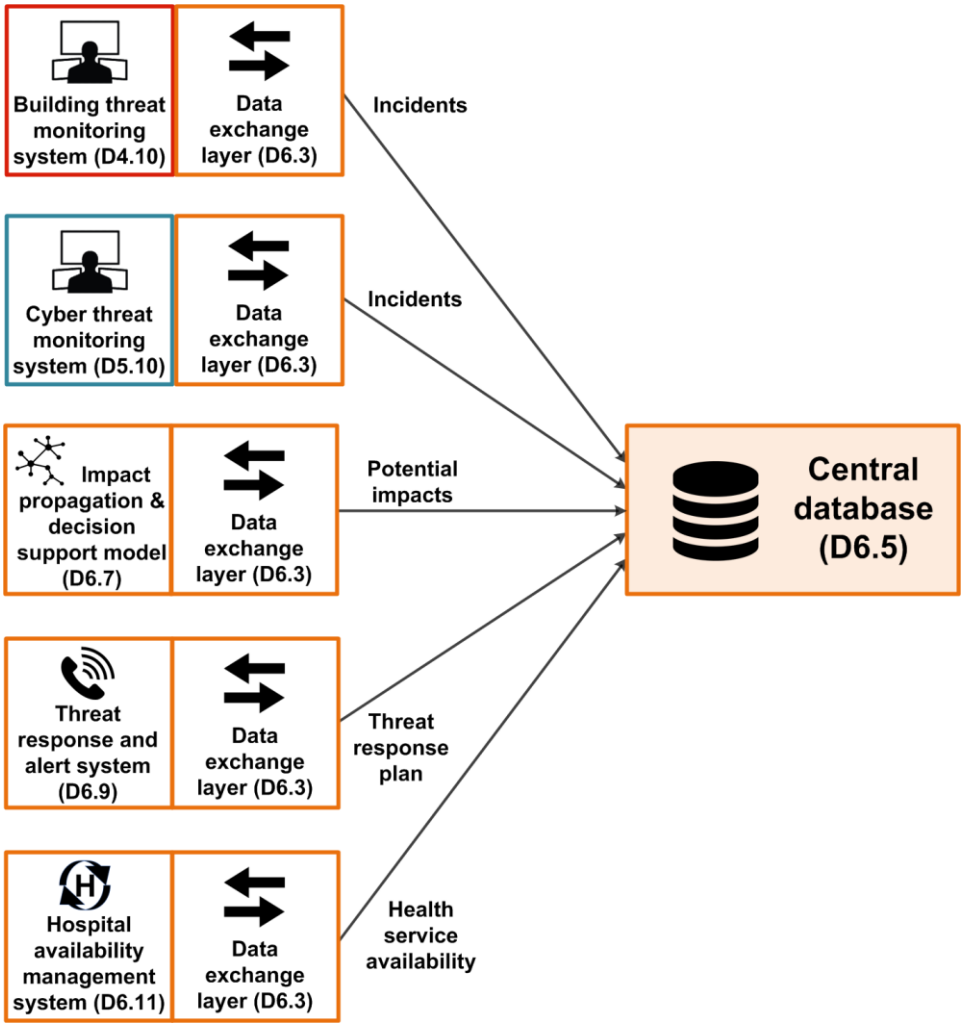

Figure 28 – Central database storing dynamic data

The building threat monitoring system, the cyber threat monitoring system, the impact propagation and decision support model, the threat response and alert system and the hospital availability management system store dynamic data into the central database.

1.14 Impact propagation model and decision support model

The objectives of the Impact propagation model and decision support model are:

- Combine physical and cyber incidents that occur on assets,
- Infer cascading effects as impacts that could potentially affect the same or related assets
- Alert other modules about the potential impacts and severity.

To be able to provide such a service, the impact propagation model operates in 2 modes, a static mode for knowledge capitalization about assets and, a dynamic mode for decision support.

To be able to reason about incidents and their potential impacts, the impact propagation model needs to hold knowledge about physical and cyber assets that are prone to attacks.

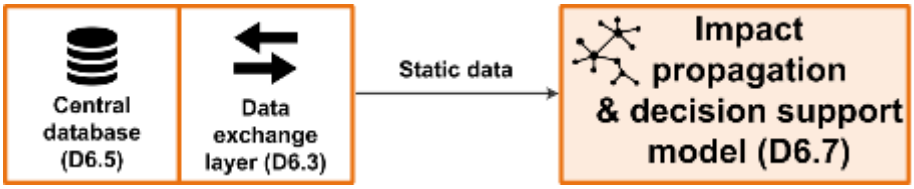

Figure 29 – Static mode communication for IPDSM

To do so, the impact propagation model relies on ontology-based formalization to represent the knowledge about the assets (see Section 3.3 for more details). As sketched in Figure 29, information about assets is sent by the structures such as hospitals and health services, to the central database to inform the system about changes affecting the assets they hold (new assets or changes on existing ones). The impact propagation model, on the other hand, regularly queries the central database, throughout the data exchanger layer to get knowledge about the assets and this is done in a static way. Moreover, the impact propagation model acquires extra knowledge about the assets from other sources such as manufacturers and vulnerabilities open databases. These inputs will increasingly enrich the knowledge graph about the assets of the system.

The ability to simulate the propagation of incidents and to anticipate risk is the cornerstone of the SAFECARE project.

As shown in Figure 30, incidents are pushed dynamically to the IPDSM through the data exchange layer. The incidents' description includes information about the attacked assets by providing their identification information, the nature and severity of the incident.

Based on the knowledge hold about the concerned assets such as known vulnerabilities and relationships with other assets, the state of the related assets resulting from previous incidents and the propagation rules, the IPDSM will compute a set of potential impacts on assets. The inferred impacts are qualified by a likelihood value that takes into account the context of the incident at hand and the impact score induced on the assets by previous incidents. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exploited or the likelihood is low if the severity of the incident is low or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

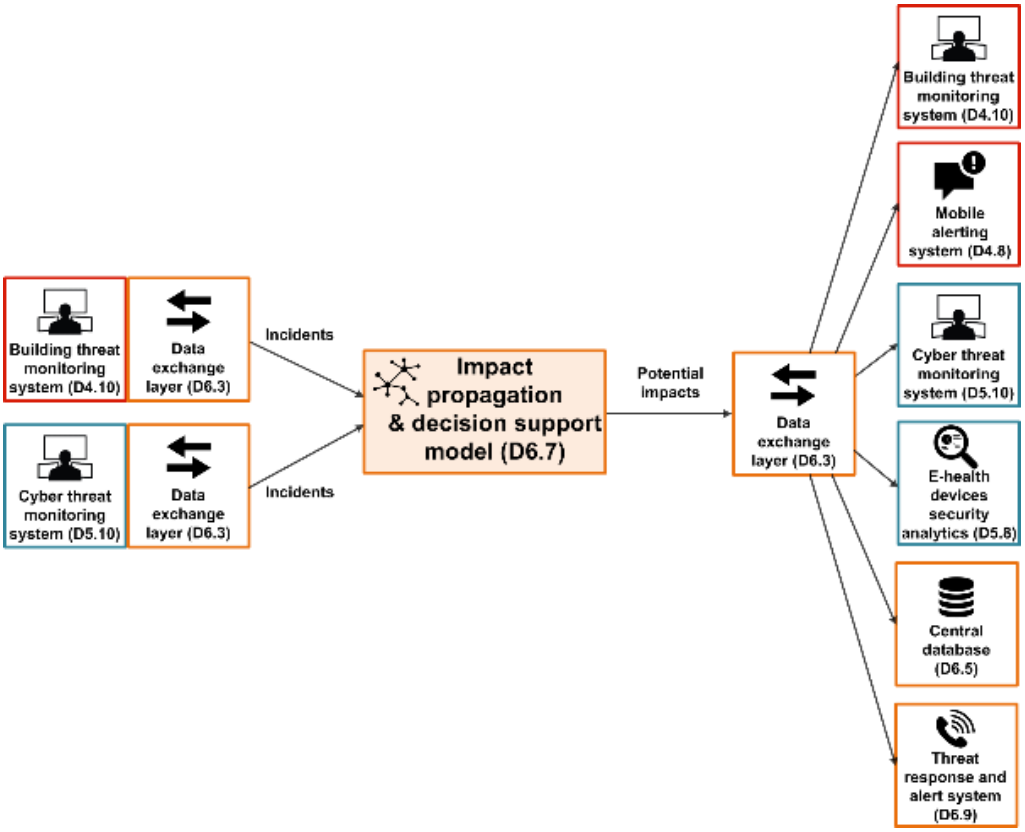

Figure 30 – Interconnections of impact propagation and decision support model

Once the impacts have been computed, they are sent through the data exchange layer to the other modules as shown in Figure 30.

The impact description details the nature of the risk encountered, the assets concerns and an evaluation of the likelihood.

1.15 Threat response and alert system

The threat response and alert system is triggered with an "impact" message from the impact propagation & decision support model, as illustrated in Figure 31.

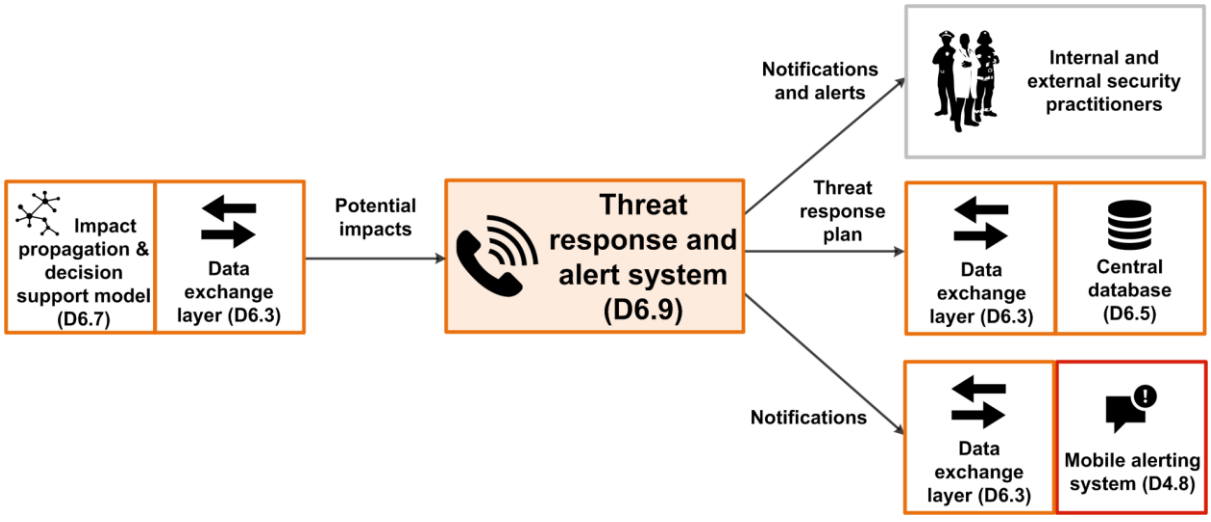

Figure 31 – Interconnections of the threat response and alert system

Each site implementation will determine the details of the response plan in terms of alerting (calls, SMS, emails, …) in front of each risk scenario taken into account and that is integrated in the impact propagation model.

This module, once excited, will parse the "impact" data retrieved from the data exchange Layer and run the corresponding response plan that will mainly consist in sending notification and alerts to internal and external practitioners.

The event that will determine when to start the response plan action could be:

- The reception of impact dataset, where the event probability goes beyond a given value (e.g. intrusion risk in room XYZ, with probability above 80%)
- The result of a manual activation by the SOC operator who is presented with the impact propagation data, and decides to start a response plan (in reaction or prevention) based on his own judgment
- As an automatic reaction to an impact propagation dataset presented to the SOC operator who didn't take any action to discard it in a given time frame for a given time set (e.g. attack risk on power supply above 70% event that hasn't been discarded / postponed by the SOC operator for 120s)

Notifications may include sending alerts to the Mobile alerting system, whose integration will be made via the data exchange layer as follows:

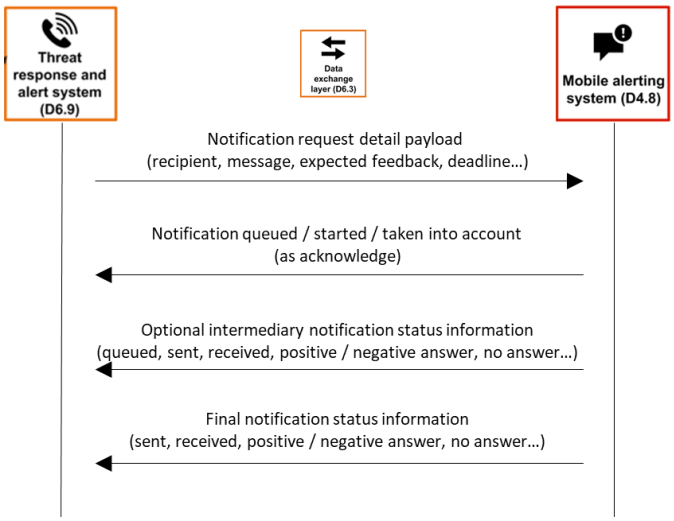

Figure 32 – Exchanges between the threat response & alert system and the mobile alerting system

The result of these notifications and alerts (e.g. notification and alert status) will be pushed back to the central database for storage and potential external retrieval, via the data exchange layer.

1.16 Hospital Availability Management System

The Hospital Availability Management System (HAMS) service will improve the resilience of health services and the communication of availability information among hospital staff and first responders.

Hospital availability will be furnished on the following elements:

- Department name and status
- Services (beds, staff, resources)

- Bed availability (counts beds Available/Baseline)
- Staff availability (counts staff Available/Baseline)
- Resource per Department (availability of Medical device)

HAMS will use the central database to get information about hospital assets and resources. The central database will store all the static data collected in the three demonstration sites of the project. Figure 33 shows how HAMS is connected to the central database: each request (query) is managed by the data exchange layer.

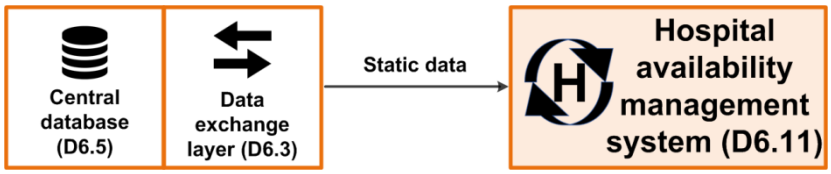

Figure 33 – Hospital availability management system getting static data

Regarding the dynamic data such as incidents and impacts, the hospital availability management system will update the availability of single assets involved both in the dashboard and in the central database. Figure 34 shows how dynamic data are received by the HAMS. HAMS will be able to report availability changes caused by both cyber and physical incidents. In addition, HAMS will be able to elaborate potential impacts in order to understand if an incident indirectly impact on an asset, compromising its availability.

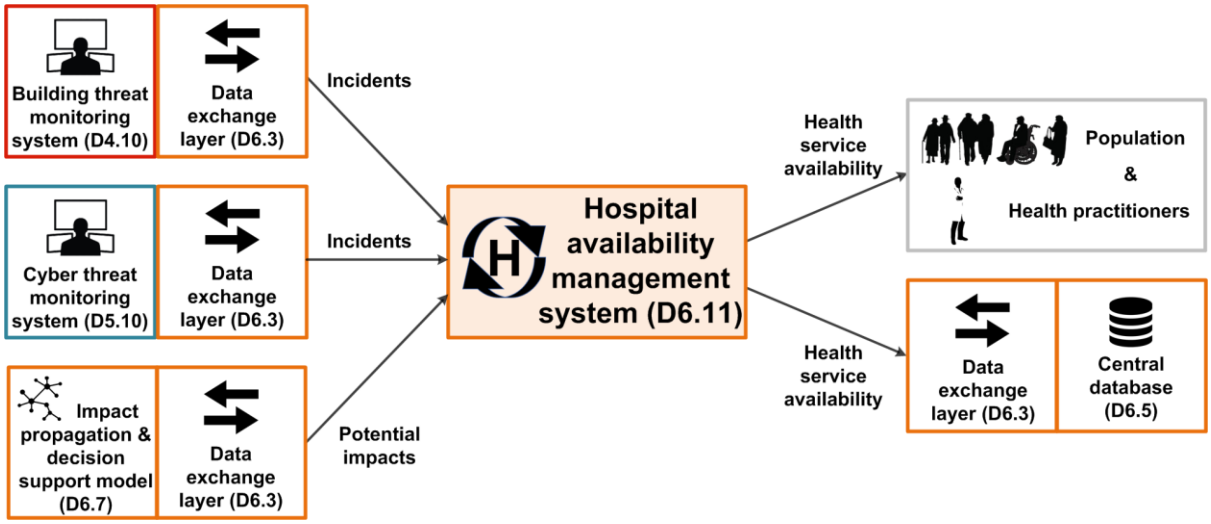

Figure 34 – Interconnections of the hospital availability management system

Further information regarding the HAMS module can be found in Deliverable 6.10.

1.17 E-health security risk management model

Embedding of security into medical device designs is, besides good engineering practice, also required in accordance with industry standards and legislations. In addition, as part of post market surveillance activities manufacturers are also required to monitor and conduct risk assessments based on applicable vulnerabilities for their products. This entails that medical device manufacturers need to evaluate information obtained from customers via customer complaints, security community via responsible disclosures as well as vulnerability notifications from suppliers/open source community for used components. The security community and medical device manufacturers perceive medical device security as an important topic and

therefore more collaborations started over the last few years including bug bounty programs, responsible disclosure processes, joint committees and more in order to improve medical device security.

When security is designed-in, the manufacturer will conduct multiple risk assessments throughout the product lifecycle besides complying with industry best practices for security (defense in-depth). In such cases, risk assessments are conducted for each change such as new product functionality, but also on lower level when an update or new third party / open source component is integrated into the product design. Risk control measures are defined and implemented based on a risk-based approach for identified (potential future) vulnerabilities. Throughout the device lifecycle applicable legislations will change as well as new vulnerabilities will be discovered which warrant product changes for uncontrolled risks or additional measures in case of controlled risks to further limit risk for similar future vulnerabilities.

Medical device logging is an important asset to determine effectiveness and usage of the embedded security controls. It provides information on device usage and its environment. This information is useful for the device manufacturer to identify potential issues and quantification of risks (likelihood/impact).

Goal of the E-health security risk management model is to create a model that will effectively quantify the impact of security events in a uniform way for medical devices using bowtie methodology. This methodology is able to visualize complex events by detailing how actors have obtained access to defined assets and what the potential risk outcome is for the related activity.

The following diagram depicts the workflow for the E-health security risk management model.

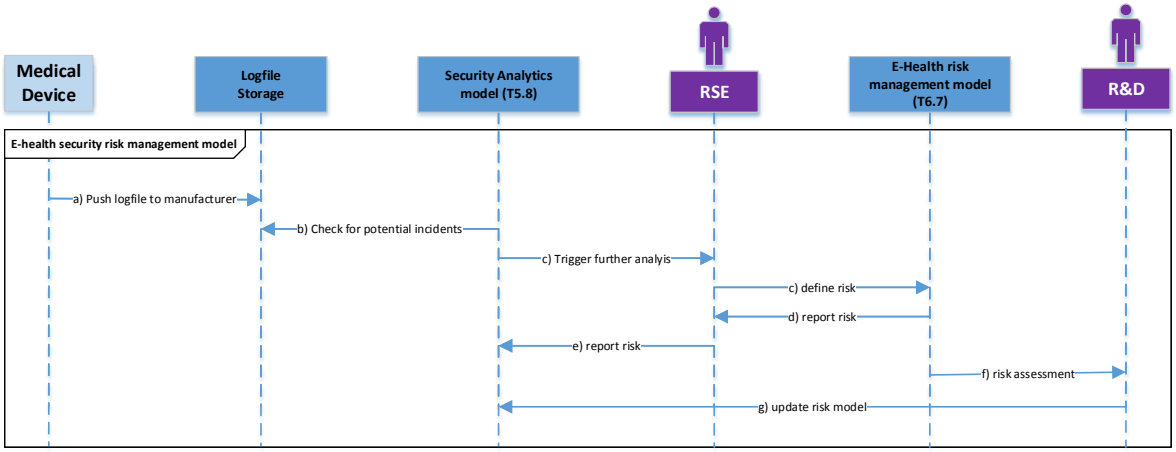

Figure 35 –Workflow of the E-health security risk management model

- Medical device collects relevant logfiles and pushes the result to the logfile storage at the medical device manufacturer using an automated process.
- Security analytics model continuously queries logfiles storage for potential hits on predefined attack patterns.
- Security analytics model notifies the Remote Support Engineer (RSE) in case of a pattern hit.
- RSE verifies the potential incident as reported by either security analytics model or customer complaints/records and uses the E-Health risk management model to determine and register the associated risk.

- RSE reports evaluated risks back to the security analytics model
- R&D uses triggers from the risk management model in post-market surveillance and as input for future developments.
- R&D defines new or updates existing patterns used by the security analytics model based on information obtained from the post market surveillance process.

External interfaces for the E-health security risk management model are limited to the 'security data' and 'risks' interface between the model and the E-health devices security analytics (D5.8), as illustrated in Figure 36.

Figure 36 – Interconnections of the e-health security risk management model

- **Security data interface**: The e-health devices security analytics tool (D5.8) uses a REST based data interface to trigger the E-health security risk management model. Data shared via this interface contains information on the threat actor, applicable security controls, event classification and impacted assets.
- **Risk interface**: After analysis of the provided data the risk model will use a callback interface to the e-health devices security analytics tool (D5.8) to report the risk level (low, medium or high). Based on the classification the analytics tool can decide to report an event to the central database.

2 Systems interconnections

This section describes systems interconnections for the physical security systems, the cyber security systems and the integrated cyber-physical security systems.

2.1 Physical security systems

The Video Management System (VMS) used in the project will be the XProtect®[1] system developed by Milestone, and already used in some partner sites. XProtect has a large integration base (8197 devices) with IP cameras (that is, cameras that communicate digital signals over computer networks) and other devices from over 150 manufacturers. Via XProtect Access, integration with a number of access control management systems is provided off-the-shelf. The XProtect Event Server is the basis on which many commercial partner solutions are build, including, for instance, with smart building / smart city sensors.

As an open platform, XProtect also provides the basis for partners and customers to build novel user interfaces via the Mobile SDK, by which video streams can be provided to mobile-based interfaces. Since SAFECARE is particularly concerned to cover also the response to incidents, user interface extensions will be carried out using this SDK, and any extensions that are necessary (e.g. to XProtect's own alarm system) will be provided.

SafeCare will build on the existing integrations provided in the XProtect family of products and thereby provide a route to exploitation of the project results.

[1] https://www.milestonesys.com/solutions/platform/video-management-software/xprotect-corporate/

2.2 Cyber security systems

The cyber supervision of health critical infrastructure must take into account not only the IT infrastructure but also the BMS infrastructure and the medical devices.

The IT infrastructure consists of IT network and IT systems (such as servers, firewalls, laptops, virtual machines …). The IT threat detection system monitors the IT network and receives the logs from the IT systems in order to detect threats targeting the IT infrastructure.

The threats that exploit the BMS network are detected by the BMS threat detection system that analyses the Operational Technologies (OT) protocols used in building automation systems (such as SCADA systems and PLC controllers).

In addition, the files, which transit on IT and OT networks, are inspected with the advanced file analysis system that provides an in-depth analysis of files. It allows to detect malwares that transit through the IT and BMS networks.

Finally medical devices forward their logs to the the e-health devices security analytics so that the e-health devices security analytics can monitor the medical devices. The e-health devices security analytics can rely on the e-health security risk management model to identify any risk with medical devices.

Thus, to detect cyber intrusions, the cyber threat monitoring system receives security events, as shown in Figure 1, from the following cyber threat detection systems:

- The IT threat detection system;
- The BMS threat detection system;
- The advanced file analysis system;
- And the e-health devices security analytics.

Based on the security events received by the cyber threat monitoring system, alerts are automatically triggered by rules. The alerts are managed within the cyber threat monitoring system and must be analyzed by SOC operators. When the incidents are confirmed by SOC operators, the incidents are sent through the data exchange layer to:

- The impact propagation and decision support model in order to compute the impacts;
- The HAMS to update the availability of health services;
- And the central database in order to store the incidents.

Once the impacts have been computed from either cyber or physical incidents, they are received by the cyber threat monitoring system so that SOC operators can visualize the potential cascading effects on cyber assets and services. The impacts are also forwarded to the e-health devices security analytics so that health practitioners can have a clear understanding of potential impacted medical devices.

2.2.1 Communication with CERTs

The cyber threat monitoring system incorporates a malware information sharing platform (MISP). It is a threat intelligence platform for sharing, storing and correlating Indicators of Compromise (IoC) of targeted attacks, threat intelligence and vulnerability information. The MISP can be connected to CERT communities as well as to other hospitals in order to share valuable knowledge about threats. Through functionalities integrated into the advance file analysis system, SOC analyst can either:

- Share information about malware encountered on the hospital network;
  The SOC analyst can choose which pieces of information to share based on information made available by the advanced file analysis system (malware hashes, malware name, analysis report);
- Search for information in the MISP database populated by communities;
  This enables SOC analysts to better understand a threat they might be facing.

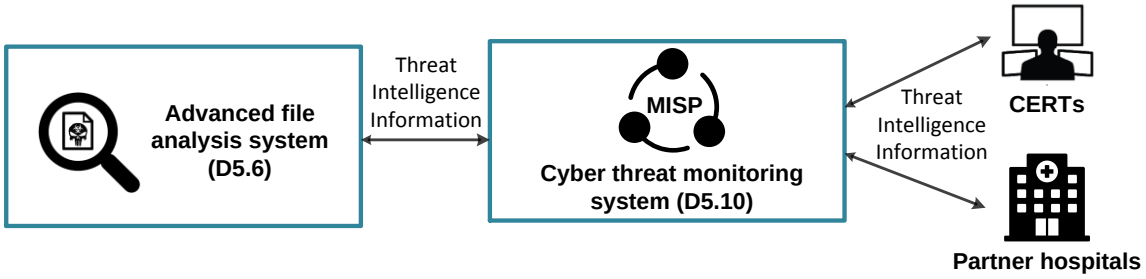

Figure 37 – Interconnection with CERTs

2.3 Cyber-physical security systems

WP6 is the work package in which the integration between cyber and physical systems takes place, through a common mechanism of communication among the involved systems. This happens through the communication between the physical and cyber monitoring systems (BTMS and CTMS) and the exchange layer and, through this, the central database.

The main concept standing below is that the integration is performed at two levels:

- data (all concentrated in a unique central database). They are both static and dynamic data.
- functions: the decisional modules may put together both physical incidents and cyber ones.

The general agreed architecture states that WP6 data exchange layer (and the central database) communicate with the BTMS of WP4 and the CTMS of WP5 through JSON messages (files). In fact, the connection between WP4 and WP6 systems is centralized through the BTMS module of WP4 which sends incidents to the data exchange layer using MQTT protocol, as well as the connection between WP5 and WP6 systems is centralized through the CTMS module of WP5, which sends incidents to the data exchange layer using MQTT protocol.

Data collection system from physical systems is managed within WP4 generating alerts and talking with BTMS module inside WP4 architecture, before any involvement of the data exchange layer. After this, BTMS generates incidents that are then sent to the data exchange layer through MQTT.

Similarly, data collection system from cyber systems is managed within WP5 generating alerts and talking with CTMS module inside WP5 architecture, before any involvement of the data exchange layer. After this, CTMS generates incidents that are then sent to the data exchange layer through MQTT.

At the same time, connection and interaction between the central level (data exchange layer and central database) with decisional modules is performed in WP6.

Decisional modules in WP6 are the following:

- the impact propagation and decision support model;
- the threat response and alert system;
- the hospital availability management system;
- the e-health security risk management model.

The data exchange layer trigger notifications to the other components when new physical and cyber incident or new impacts (or response plan, or availability situation) are sent, and it stores and extracts data from the central database; therefore, the data exchange layer allows others project components to extract added-value information on demand from the central database. The central database includes a dynamic data store and a static data store. The dynamic data store includes incidents, impacts, response, availability and impacts coming from the physical and cyber systems through the data exchange layer, as well as responses from TRAS and availability (from HAMS).

The communication among physical and cyber systems can happen as the relevant interfaces with their own software components have been defined in the project working groups.

2.4 Communication standards

This section describes the communication standards used for interconnecting the SAFECARE systems.

2.4.1 Syslog

Syslog is a standard for message logging, also known as logs. The security events generated by the cyber threat detection systems (Deliverables 5.2, 5.4, 5.6 and 5.8) are sent to the cyber threat monitoring system using Syslog messages and the Syslog protocol, either over UDP or TCP. It is also possible to transmit the security events over TLS to guarantee integrity and confidentiality. A wide variety of devices, such as printers, servers or routers across many platforms use this standard. Moreover most of software designers use the Syslog standard for system management and security auditing as well as general informational. Thus, the IT events of the IT infrastructure are also received by the IT threat detection system using this standard.

2.4.2 Standard EDXL-HAVE

Emergency Data Exchange Language (EDXL) is a group of standards adopted by OASIS to manage the entire emergency lifecycle. It is designed to exchange and share information easily between different emergency systems. EDXL Hospital AVailability Exchange (HAVE) provides information about the availability of hospitals and health networks. In particular, the information exchanged is about facility services, bed counts, capacities, operations and resources, so first responders and care facilities can have a complete view of each other's availability of health system resources. In emergencies or crises, it is important for the hospitals to share information with members of the emergency network. The capacity to exchange data regarding hospitals bed counts, status, services, and capacity allows the hospitals to manage the emergency and the emergency manager to decide better where to route patients or victims.

The principles that guided the design of the HAVE include:

- Interoperability – The HAVE message should provide an interoperable mechanism to exchange healthcare organization information among different domains and among multiple system.
- Multi-Use Format – The HAVE message must be designed such that it can be used in everyday events, during mass disasters and for incident preparedness.

- Flexibility – The design structure must be flexible such that it could be used by broad range of applications and systems to report status and availability information.

2.4.3 Publish-subscribe mechanism: MQTT protocol

The MQTT protocol is based on the principle of publishing messages and subscribing to topics. Subscribers subscribe to specific topics which are related to them and through this they receive every message published to those topics. Clients can publish messages to topics, thus making them available to all subscribers of those topics.

The MQTT protocol is implemented in the data exchange layer.

2.5 SAFECARE users

The SAFECARE system, as a global protection system of critical health infrastructures, interacts with a wide variety of individuals. In the context of a given health infrastructure (i.e. an hospital most of the time), those individuals can be divided into 4 categories:

- Hospital employees or subcontractors;
  For example: health practitioners, technical administrators, security agents…
- Civil service actors;
  For example: firefighter, police, national health agency…
- Patients;
- General population.
  For example: hospital visitors, surrounding inhabitants (potential patients).

While we all group them under the term of "SAFECARE users", the kind of interaction those individuals have with SAFECARE can be either a two-way interaction, for hospital employees/subcontractors and civil service actors, or a one-way interaction, for patients and general the population.

This section focuses on listing SAFECARE users in relation to the various subsystems it is composed of.

Table 1 gives a list and description of SAFECARE user profiles while Table 2 associates user profiles to SAFECARE subsystems.

Category	(Sub)profiles (non-exhaustive)
Hospital employees or subcontractors	
Health practitioners	Nurses Assistant nurses Doctors Externs Interns Medical imaging technicians (e.g. ultrasound technician)
Hospital staff	Hospital general manager

	Sanitary division personnel
	Reception chief
	Administrative service personnel
	Data Protection Officer
	Occupational safety and health professionals
	Crisis management team
	Biomedical team
System providers	Manufacturer
	Software editor
System maintainers	IT system administrators
	IT network administrators
	IT security administrators
	Physical devices and sensor maintainers[2]
System supervisors	*Cyber*
	SoC operators
	SoC analysts[3]
	Chief information security officer[4] (CISO)
	Physical
	Control room operators/security agents
	Chief security officer[5]
Civil service actors	
Law enforcement agencies	Local police
	National police
	Gendarmerie
Firefighters	
Emergency medical services and first-responders	Ambulances
	Operation center for emergency service with ambulances
	First aid organizations

[2] Also referred to as "system integrators"
[3] Also referred to as "Threat intelligence analysts"
[4] Also referred to as "IT Security manager"
[5] Also referred to as "Physical Security manager"

National/regional health agencies	National health agency Regional Authority – responsible for Health Service and Emergency Plan (PEIMAF = internal emergency plan for the massive influx)

Table 1 – SAFECARE user profiles

Different types of users will interact with SAFECARE depending on where it is in its life-cycle. For the installation phase, mainly system providers, maintainers and supervisors might interact with it. System maintainers will also play a main role during system maintenances.

The following table focuses on the users in interaction with SAFECARE during system operation.

System	Users	Role	Interface
Mobile service for integrated alerting system (D4.8)	Local security agents Health practitioners Hospital staff	Report a physical threat	Mobile application
	Chief/senior security officer	Evaluate physical alerts	
	Hospital general manager Sanitary division personnel Reception chief	Manage incidents impacts	
	Local security agents Health practitioners Hospital staff	Manage threat responses	
Building monitoring system (D4.10)	Local security agents	Monitor physical security (detect, display and handle alerts, visualize building information)	Desktop and web application (Milestone XProtect VMS)
IT threat detection system (D5.2)	SoC analysts	Investigate threats stemming from the IT network	Web applications (mainly Graylog and a machine learning dashboard) and command line interfaces
BMS threat detection system (D5.4)	SoC analysts	Investigate threats stemming from the BMS	Web application (Forescout

			SilentDefense)
Advanced file analysis system (D5.6)	SoC analysts	Investigate threats stemming from malicious files	Web applications (Airbus Orion Malware and MISP)
E-health devices analytics (D5.8)	SoC analysts Manufacturer service staff Manufacturer Chief information security officer	Investigate and remediate security alerts	Web applications
Cyber threat monitoring system (D5.10)	SoC operators SoC analysis Chief information security officer	Monitor cyber security (visualize threats and impacted assets, manage incident response)	Web applications (Airbus Cymerius)
Threat response and alert system[6] (D6.9)	Hospital staff System supervisors Law enforcement agencies Firefighters Emergency medical services and first-responders National health agencies General population	Receive and respond to alerts and notifications	SMS, emails, interactive voice calls, MAS
	Hospital staff	Platform management	Web application (ENOVACOM Suite V2 and ENOVACOM Surycat)
Hospital availability	General population[7]	Get informed about	Web application

[6] Workshops with each hospital will be conducted in order to identify all stakeholders and get their respective contact information.

[7] Depending on the hospital's home country customs or choice, the HAMS might not be made available to the general population in order to avoid confusion and counter productivity.

management system (D6.11)		hospital availability	
	Emergency medical services and first-responders Health practitioners	Get informed about hospital availability with relevant information about departments, services and resources available in the hospital	Web application
	Hospital staff	Update availability-related information	Web application

Table 2 – SAFECARE subsystems users

3 Data exchange protocols, data models and data storage

This section is about the data exchange layer, the central database, ontologies and graph data model.

3.1 Data exchange layer

The specification of the data exchange layer can be summarized by four main features:

- providing publish-subscribe mechanism,
- giving possibility to store and extract data from the central database,
- checking coherence of data format and data content with static data,
- other components should extract information from the central database.

Considering that the data exchange layer will provide a machine-to-machine communication mechanism, and it has to be of the kind "publish-subscribe", MQTT protocol (one of the most well known) is proposed to be adopted. Technical structure of the data exchange layer is defined in Deliverable 6.2.

3.2 Central database, table data model and data storage

According to the global architecture of the system, whose design is reported in the following, the central database of the project stores incidents, static data, and various responses/elaborations coming from the decisional modules of the project SAFECARE system (impacts, threat responses, hospital availabilities). The structure of the central database is designed as in Figure 38.

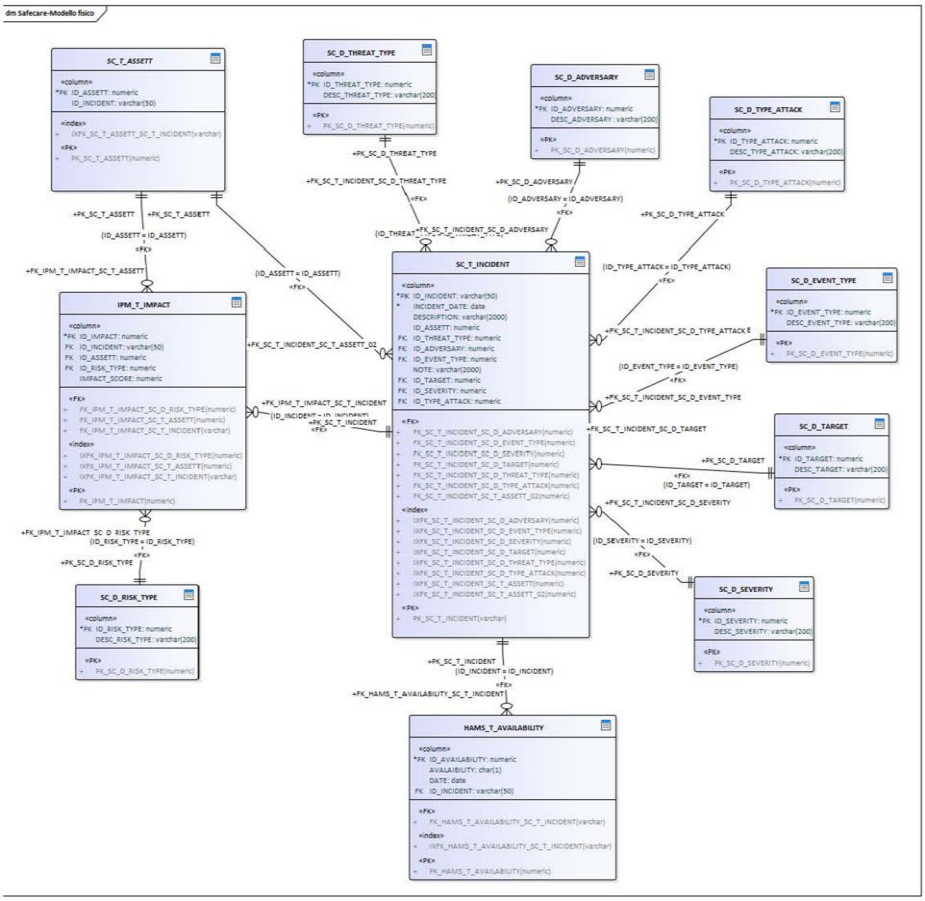

Figure 38 – Structure of the central database

Central database is proposed to be developed in PostgreSQL TM environment. Technical specifications of the central database are provided in Deliverable 6.4.

3.3 Ontologies and graph data model

This section describes the data models and data storage solutions within the Impact Propagation and Decision Support Model module. This module relies on knowledge graphs that store knowledge about assets and their interdependencies. For this, ontologies are used as they are suitable to represent semantics and enhance knowledge sharing.

As shown in Figure 39, the construction of the Knowledge Graph (KG) is based on two main stages. The first one – Ontology Construction – defines the HCAssets (Healthcare Critical Assets) ontology that describes both cyber and physical assets, their vulnerabilities and their interdependence as well as the risks and threats. The second stage – Knowledge Graph Population – provides ontology instances related to the different hospitals starting from the input "Asset.json". The resulting knowledge graph includes the HCAssets and is continually enriched with a set of instances structured regarding the concepts and the properties of the ontology.

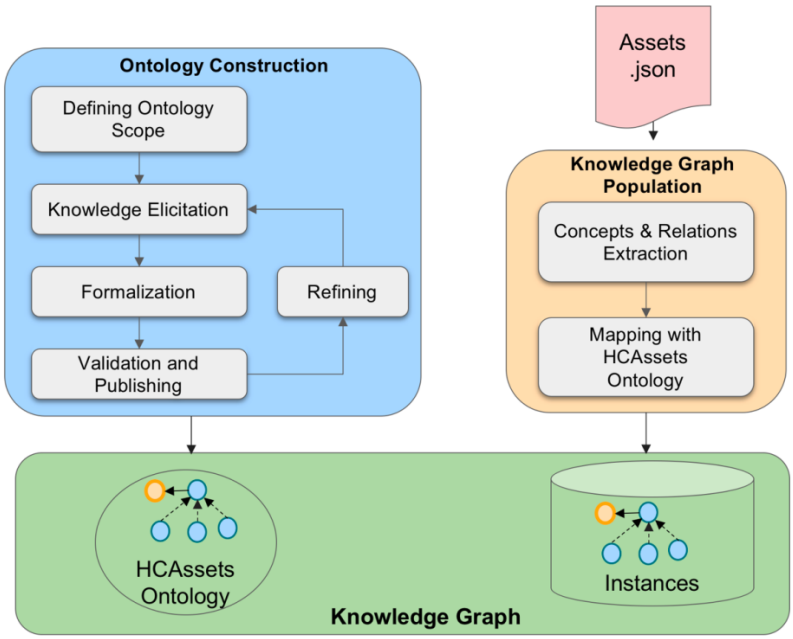

Figure 39 – Knowledge Graph Creation

3.3.1 HCAssets Ontology construction

Based on a list of critical assets provided in the Deliverable 3.1 and on discussions with different partners, the *HCAssets* ontology has been defined. This *ontology* describes, on the one hand, concepts and properties related to cyber and physical threats (e.g. alarms, vulnerabilities, incidents), and on the other hand, healthcare critical assets and their interdependencies (e.g. IT assets, human assets, medical devices). The construction of the *HCAssets* ontology followed the steps below:

- **Defining ontology scope**: In this phase, the need and purpose to create the HCAssets ontology is identified. Regarding the critical assets provided by the partners and the different threat scenarios, existing ontologies or subpart of ontologies that can be reused has been investigated. At the actual state of literature, very few work is dedicated to cyber-physical security ontologies. The challenge is to define a solution based

ontology that efficiently combines the cyber and the physical concerns and the underlying interdependencies.

- **Knowledge elicitation**: A first version of the HCAssets ontology has been defined and concerns essentially the assets description. It will be refined by means of discussions with domain experts. It is highly modular to ease its enrichment according to; (1) the threat scenarios, (2) the future incidents and their impacts, and (3) the evolution of assets and their vulnerabilities.
- **Formalization**: To formalize the different concepts and relations OWL2 standard notation has been adopted for its high expressiveness and inference capabilities. An extract of the ontology is sketched in Figure 40.

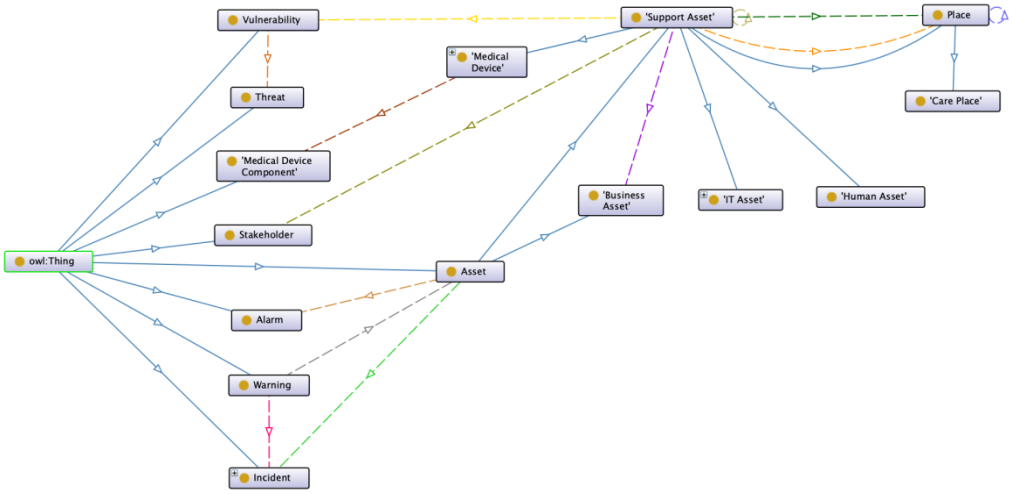

Figure 40 – HCAssets Ontology

- **Validation and publishing**: The ontology is evaluated regarding the ability of the impact propagation module to deal with the different threat scenarios. Further refinements of the ontology can arise in this phase.

3.3.2 Knowledge graph population

The process of graph population consists of instantiating the ontology concepts and relations. It includes the two following phases:

- **Concepts and relation extraction**: Using a JSON parser, the healthcare critical assets, their attributes, and their relationships are extracted from the "Assets.json" file (see Figure 39).
- **Mapping with the HCAssets ontology**: Data extracted in the first phase are mapped as instances with the HCAssets ontology concepts and properties. These instances are then stored in the knowledge graph as RDF triples.

3.3.3 The resulting knowledge graphs

The first version of the KG will be implemented as Resource Description Framework (RDF) triples which is a W3C standard used to formally describes resources and their metadata, so that they can be automatically processed. To store and query the RDF triples, it is intended to use TDB2 which is a component of Apache Jena. This native storage includes an inference subsystem that supports a range of inference engines and can be used with Apache Jena Fuseki as a high-performance RDF store on a single machine. In the future, if data processing requires a more efficient platform, it would be possible to migrate to a graph database such as Neo4j.

4 Information sharing between software components

This section describes information sharing between the SAFECARE components.

4.1 Referent datasets

Referent dataset that store data in the central database are data about incidents coming from cyber security management system (CTMS) and physical security management system (BTMS), about impact, threat response and availability coming from decisional modules, and static data provided directly by project partners into the central database.

BTMS and CTMS communicate with the central database via the data exchange layer, similarly decisional modules communicate with the central database via the data exchange layer.

4.2 Normalized assessment scales

According to NIST's report[8] there are two ways to qualify incidents and impacts namely qualitative and quantitative.

4.2.1 Qualitative assessment

Qualitative assessment uses a set of methods, principles, or rules for assessing risk based on non numerical categories or levels. The advantage is the clarity of the evaluation and the ease of interpretation. Most of existing incidents analysis tool rely on qualitative evaluation where severity is rates on a scale of three or five levels ranging from (very) Low to (very) High values. Within SAFECARE, the incidents are detected by BTMS (D4.10) and CTMS (D5.10) and are consequently rated by the solutions used for incident detection and analysis. An incident corresponds to a successful threat exercise of vulnerability. The analysis of these incidents and their severity has a direct impact on impacts propagation inference and rating.

The role of the Impact propagation and decision support model is to prioritize the impact levels associated with the compromise of critical assets based on the assessment of the sensitivity and criticality of those assets. Within SAFECARE, it is intended to provide both qualitative and quantitative impact likelihood assessment to better decision support.

4.2.2 Quantitative assessment

Quantitative assessment relies on mathematical functions that combine several parameters to compute a numerical measure to accurately evaluate the impacts' magnitude. Although it is more precise than qualitative assessment, its interpretation is more complex. The computation function definition is also difficult as it is necessary to find the relevant parameters as well as the suitable function. Within SAFECARE, this function should combine incident severity, assets interdependencies and their vulnerabilities, the cyber and physical risks interfering, the impact of previous incidents and probably new parameters that will appear as we progress in the project.

[8] JOINT TASK FORCE TRANSFORMATION INITIATIVE, et al. Guide for conducting risk assessments. National Institute of Standards and Technology, 2012.

5 Data privacy

This section is about privacy and data protection aspects regarding the SAFECARE solutions.

5.1 Overview

The privacy and data protection aspects concerning the development of the SAFECARE solutions have been illustrated in Deliverable 3.9 ('Analysis of ethics, privacy, and confidentiality constraints'). This deliverable describes the key principles and requirements laid down by the applicable privacy and data protection legislation at an EU and a national level (namely Italy, the Netherlands, and France, where the SAFECARE Pilots phases will take place). As illustrated in this document, the core piece of legislation in the EU on privacy and data protection is the General Data Protection Regulation (GDPR)[9].

The Data Protection Impact Assessment (DPIA) is a legal requirement that has been introduced by the GDPR (art 35). It has to be conducted when the processing of personal data is 'likely to result in a high risk to the rights and freedoms of natural persons'.[10] The DPIA is a process that is designed to describe the processing of personal data, to assess its necessity and proportionality. It helps to manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them.

According to guidance provided by the Article 29 Working Party[11], 'A DPIA can also be useful for assessing the data protection impact of a technology product (…) where it is likely to be used by different data controllers to carry out different processing operations. (…)'.[12] This eventuality resulted to be the case of the SAFECARE project, where, every Consortium partner resulting – according to the project Grant Agreement – to be a leading developer of a project technology/solution, has evaluated to carry out a DPIA for the same solution to be developed.

5.2 Methodology

According to art 35 GDPR, the DPIA should be carried out 'prior to the processing'. To such purpose, the Consortium partners have carried out the DPIAs within M6 of the SAFECARE project timeline and showed commitment to update the results thereof, if needed.

To reach homogeneous results, the Consortium partners have agreed to adopt a common approach with respect to tools and methodology for the execution of the DPIAs. In particular, Consortium partners have deemed to adopt the Methodology provided by the French Data Protection Authority 'CNIL' ('Commission Nationale de l'Informatique et des Libertés') and to carry out the DPIAs through the software/tool 'PIA', released by the same CNIL and rendered available on its website.[13]

---

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[10] GDPR, art 35.
[11] Article 29 Working Party (WP29) provided further interpretative guidance in its Guidelines on DPIA: see WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (2017).
[12] ibid, 8. The document states also: 'Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities'.
[13] See CNIL, 'CNIL publishes an update of its PIA Guides' (CNIL, 26 February 2018) <www.cnil.fr/en/cnil-publishes-update-its-pia-guides> accessed 1 August 2019. Version adopted: version 1.

According to the GDPR (namely, art 35(7)), a DPIA must contain: 1) a description and the purposes of the processing of personal data; 2) an evaluation of the necessity and proportionality of the processing operations in relation to the purposes; 3) an assessment of the risks to the rights and freedoms of data subjects; 3) the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR. The French Authority has affirmed that the Methodology under discussion is in line to the legal criteria set by the law and it is compatible with international standards on risk management (such as ISO 31000).

5.3 DPIAs for each SAFECARE Solution

To foster trust in the processing operations carried out in the SAFECARE project, as well as to demonstrate accountability and transparency, the Consortium partners have agreed to publish the results of the DPIAs. Such results will not be accompanied by the full DPIA assessment carried out. This choice results in line with WP29 Guidelines on DPIA, which state that the published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks.[14] Nevertheless the paragraphs that follow will provide a high-level description of the DPIAs carried out by the Consortium partners for the development of the SAFECARE solutions.

To facilitate the analysis of results, this section will explain how results are presented. Accordingly, DPIAs results are summarized in a table, providing the following details:

- Name of the technology/solution under analysis;
- 'Version and date' of every DPIA;
- 'Elements': it reports only whether the analysis of the description and purposes of the processing of personal data has occurred.[15]
- 'Risk overview': it contains (in a synthetic form) the key elements assessed in every DPIA according to the CNIL methodology, and namely:
    - the potential impacts on the data subjects' privacy if the feared event occurred;
    - the threats to personal data supporting assets that could lead to the feared events;
    - the risk sources that could cause the feared event;
    - the envisaged measures to address the risks.
- 'Risk mapping': reports the risk evaluation for the three feared events which are, as per CNIL's methodology: (i) Illegitimate access to data; (ii) Unwanted modification of data; (iii) Data disappearance. The risk evaluation is composed, as usual, by the two factors 'severity' and 'likelihood'. These may range as follows: negligible, limited, important, maximum. Graphic results ('cartography') of risk mapping are not reported in the present document – they may be found, however, in the full version of DPIAs.

Any further details about the methodology, definitions and processes concerning the execution of the DPIAs may be found on the CNIL's Methodology and Knowledge Basis documents.[16]

[14] WP29 (n2), 18.
[15] Details regarding the description and purposes of the processing operations of personal data will be left aside, for evident reasons of not repeating the content outlined elsewhere in this document. Anyway, this information is available in the DPIA documentation held by every partner.
[16] CNIL, 'Privacy Impact Assessment (PIA). Methodology' (February 2018 edition); CNIL, 'Privacy Impact Assessment (PIA). Knowledge Bases' (February 2018 edition).

5.3.1 Suspicious behaviour detection system; Intrusion and fire detection system; Building monitoring system

On the basis of the evaluations carried out by Milestone (MS), the 'suspicious behavior detection system', 'intrusion and fire detection system' and 'building monitoring system' DPIAs have been treated together under the same DPIA process. The results are summarized in the table below.

Suspicious behaviour detection system (D4.2); Intrusion and fire detection system (D4.4); Building monitoring system (D4.10)			
Version and Date	V1 – January 2019	Owner	MS
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: the restricted scope of video collected means that a data subject would only be exposed as having been present in the hospital environment (no video on medical treatment will be held). ○ **Threats**: non-compliance; improper cybersecurity; human error; malicious deletion. ○ **Sources**: cybersecurity vulnerabilities; non- or improper compliance. ○ **Measures envisaged to address the risks**: Encryption; anonymization; data minimisation; backups.		
Risk mapping	The risk evaluation carried out for the suspicious behaviour system, having regard to potential impacts, threats, sources and measures to address the risks, shows the following results for the identified feared events: - **Illegitimate access to data**: Severity = limited; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible		

Table 3 – DPIA results for D4.2, D4.4 and D4.10

5.3.2 Data collection system

The DPIA results for the 'data collection system' are summarized in the table below.

Data collection system (D4.6)			
Version and Date	V1 – January 2019	Owner	BEIA
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: disclosure of data subjects' data to unauthorized person or entity; ○ **Threats**: unauthorized access to the collected data by physical intrusion or cyber-attacks; ○ **Sources**: lack of physical or cyber-security measures; ○ **Measures envisaged to address the risks**: internally implemented risk avoidance procedures; logical access control; encryption; anonymization;		

	traceability (logging); minimizing the amount of personal data; partitioning data; archiving; operating security; website security; maintenance; paper document security; organization policy; avoiding sources of risk; protecting against non-human sources of risk; managing privacy risks; integrating privacy protection in projects; managing personal data violations; physical access control; network security; processing contracts; backups; managing workstations; clamping down on malicious software, hardware security; internally implemented risk avoidance procedures.
Risk mapping	The risk evaluation carried out for the data collection system, having regard to potential impacts, threats, sources and measures to address the risks, shows the following results for the identified feared events: - **Illegitimate access to data**: Severity = limited; Likelihood = limited - **Unwanted modification of data**: Severity = limited; Likelihood = limited - **Data disappearance**: Severity = limited; Likelihood = limited

Table 4 – DPIA results for D4.6

5.3.3 Mobile alerting system

The DPIA results for the 'mobile alerting system' are summarized in the table below.

Mobile alerting system (D4.8)			
Version and Date	V1 – December 2018	Owner	LINKS
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: show subject location. ○ **Threats**: unauthorized access to data. ○ **Sources**: internal human sources; external human sources. ○ **Measures envisaged to address the risks**: Encryption; restricting data access.		
Risk mapping	The risk evaluation carried out for the mobile alerting system, having regard to potential impacts, threats, sources and measures to address the risks, shows the following results for the identified feared events: - **Illegitimate access to data**: Severity = negligible; Likelihood = negligible		

Table 5 – DPIA results for D4.8

5.3.4 IT threat detection system

The DPIA results for the 'IT threat detection system' are summarized in the table below.

IT threat detection system (D5.2)			
Version and Date	V1 – December 2018	Owner	CCS

Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality
Risk overview	○ **Potential Impacts**: the files that are exchanged on the supervised system could be retrieved by a malicious person if he or she could access the IT threat detection system with admin rights. ○ **Threats**: unauthorized access to the IT threat detection system with admin rights by a malicious person; human error; software bug; technical failure. ○ **Sources**: human factor or error (e.g. employees); software bug. ○ **Measures envisaged to address the risks**: anonymization; data partitioning.
Risk mapping	The risk evaluation carried out for the IT threat detection system, having regard to potential impacts, threats, sources and measures to address the risks, shows the following results for the identified feared events: - **Illegitimate access to data**: Severity = limited ; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible

Table 6 – DPIA results for D5.2

5.3.5 BMS threat detection system

The DPIA results for the 'BMS threat detection system' are summarized in the table below.

BMS threat detection system (D5.4)			
Version and Date	V1 – January 2019	Owner	FST
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: leak of sensitive data; leak of network map data; decrease of cyber-protection. ○ **Threats**: network misconfiguration; cyber-attack; human error. ○ **Sources**: malicious insiders; cybercrime organization; human operator errors; human operator. ○ **Measures envisaged to address the risks**: logical access control, encryption, traceability (logging).		
Risk mapping	The risk evaluation carried out for the BMS threat detection system, having regard to potential impacts, threats, sources and measures to address the risks, shows the following results for the identified feared events: - **Illegitimate access to data**: Severity = limited; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible		

Table 7 – DPIA results for D5.4

5.3.6 Advanced file analysis system

The DPIA results for the 'advanced file analysis system' are summarized in the table below.

Advanced file analysis system (D5.6)			
Version and Date	V1 – January 2019	Owner	CCS
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: access to files of data subjects. ○ **Threats**: unauthorized access to the advanced file analysis system with admin rights; software bugs. ○ **Sources**: human factors; non-human sources. ○ **Measures envisaged to address the risks**: minimizing the amount of personal data; logical access control; traceability (logging).		
Risk mapping	The risk evaluation carried out for the advanced file analysis system, having regard to potential impacts, threats, sources and measures to address the risks, shows the following results for the identified feared events: - **Illegitimate access to data**: Severity = limited ; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible		

Table 8 – DPIA results for D5.6

5.3.7 E-health devices security analytics; E-health security risk management model

On the basis of the evaluations jointly carried out by Philips' legal entities PEN and PMS, the 'e-health device security analytics' and 'e-health security risk management model' DPIAs have been treated together under the same DPIA process. The results are summarized in the table below.

E-health device security analytics (D5.8); E-health security risk management model (D6.13)			
Version and Date	V1 – February 2019	Owner	PEN; PMS
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: very low impact; loss of device logs and maintenance history affects the device monitoring and maintenance. ○ **Threats**: breach of databases or PC of analysts by an external adversary; faulty access control mechanism at data sources that allows an unauthorized employee to access the data; transmission of data over unsecured networks; unauthorized access of the data; malware on the system where the data is processed; employee deletes dataset. ○ **Sources**: external adversary who breaches databases; external adversary		

	who infects the systems that process data; internal adversary. ○ **Measures envisaged to address the risks**: logical access control; policy; anonymization; minimizing the amount of personal data; clamping down on malicious software; backups.
Risk mapping	The risk evaluation carried out for the e-health device security analytics and the e-health security risk management model technology, having regard to potential impacts, threats, sources and measures to address the risks, shows the following results for the identified feared events: - **Illegitimate access to data**: Severity = negligible ; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible

Table 9 – DPIA results for D5.8 and D6.13

5.3.8 Cyber threat monitoring system

The DPIA results for the 'cyber threat monitoring system' are summarized in the table below.

Cyber threat monitoring system (D5.10)			
Version and Date	V1 – January 2019	Owner	CCS
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: no impact. ○ **Threats**: internal adversary; spying from specialized units or intelligence agencies. ○ **Sources**: internal human sources. ○ **Measures envisaged to address the risks**: anonymization; logical access control.		
Risk mapping	The risk evaluation carried out for the cyber threat detection system, having regard to potential impacts, threats, sources and measures to address the risks, show the following results for the identified feared events: - **Illegitimate access to data**: Severity = negligible; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible		

Table 10 – DPIA results for D5.10

5.3.9 Data exchange layer; Central database

On the basis of the evaluations executed by CSI, the 'data exchange layer' and 'central database' DPIAs have been treated together under the same DPIA process. The results are summarized in the table below.

Data exchange layer (D6.3); Central database (D6.5)			
Version and	V1 – December 2018	Owner	CSI

Date			
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: minimal, only related to e-health data; data will be backed-up at the source, so in case of tampering the restore will be possible through backups. ○ **Threats**: fraudulent access to the database; theft of credentials; internal human sources; external human sources; non-human sources; unwanted modification of data; malicious modification of data; damaging or tampering to servers. ○ **Sources**: internal human sources; external human sources; non-human sources ○ **Measures envisaged to address the risks**: anonymization; logical access control; cryptography; access logging control; traceability; backup.		
Risk mapping	The risk evaluation carried out for the data exchange layer and the central database , having regard to potential impacts, threats, sources and measures to address the risks, show the following results for the identified feared events: - **Illegitimate access to data**: Severity = negligible ; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible		

Table 11 – DPIA results for D6.3 and D6.5

5.3.10 Impact propagation model and decision support model

According to its prudent evaluations executed at M6 of the SAFECARE project timeline, the Consortium partner CNAM initially deemed not necessary to carry out a DPIA for the 'impact propagation model and decision support model'. Later on, in July 2019 CNAM finally executed a DPIA and the conclusions are summarized in the following table.

Impact propagation model and decision support system (D6.7)			
Version and Date	V1 – July 2019	Owner	CNAM
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: no impact. ○ **Threats**: Cyber or physical attack on servers with no impact as the servers and computers from CNAM side store no personal or sensitive data. ○ **Sources**: attacks on the SAFECARE project partners' sites. ○ **Measures envisaged to address the risks**: anonymization of data received from the central database, network security (physical severs isolation and logical access control).		
Risk mapping	The risk evaluation carried out for the impact propagation model and decision support system, having regard to potential impacts, threats, sources and measures to address the risks, show the following results for the identified		

	feared events: - **Illegitimate access to data**: Severity = negligible; Likelihood = negligible - **Unwanted modification of data**: Severity = negligible; Likelihood = negligible - **Data disappearance**: Severity = negligible; Likelihood = negligible

Table 12 – DPIA results for D6.7

5.3.11 Threat response and alert system

The DPIA results for the 'threat response and alert system' are summarized in the table below.

Threat response and alert system (D6.9)			
Version and Date	V1 – December 2018	Owner	ENC
Elements:	✓ Description of purposes of processing ✓ Evaluation of necessity and proportionality		
Risk overview	○ **Potential Impacts**: data leakage of personal data like email address or phone number; disorganization in security actions; alerts not sent. ○ **Threats**: cyber-attack targeting database, alerting system, telecommunication. ○ **Sources**: cyber hackers; internal users; terrorists. ○ **Measures envisaged to address the risks**: encryption, logical access control; minimizing the amount of personal data; monitoring network activity, network security, logical access control.		
Risk mapping	The risk evaluation carried out for the threat response and alert system, having regard to potential impacts, threats, sources and measures to address the risks, show the following results for the identified feared events: - **Illegitimate access to data**: Severity = limited; Likelihood = negligible - **Unwanted modification of data**: Severity = important; Likelihood = limited - **Data disappearance**: Severity = important; Likelihood = limited		

Table 13 – DPIA results for D6.9

5.3.12 Hospital Availability Management System

At M6 of the SAFECARE project timeline, the Consortium partner LINKS has estimated not necessary to carry out a DPIA for the 'Hospital Availability Management System' as the solution under analysis would not lead to an involvement of personal data.

6 Strategy of defence

This section describes how the SAFECARE solutions detect and respond to threats related to the scenarios defined in Deliverable 3.6 in order to protect the hospitals of Turin (ASLTO5), Marseille (AP-HM) and Amsterdam (AMC).

6.1 ASLTO5 protection against the scenarios of threat

The scenarios for ASLTO5 facilities are the following:

- Scenario 2: Steal patient data in the hospital.
- Scenario 5: Shooting, explosive or sabotage in critical places.
- Scenario 8: Distributed management over distributed buildings, considering external stakeholders.

6.1.1 Scenario 2

Scenario 2 corresponds to a combination of cyber and physical attacks to steal patient data in the hospital. The steps of the attacks are shown in Figure 41.

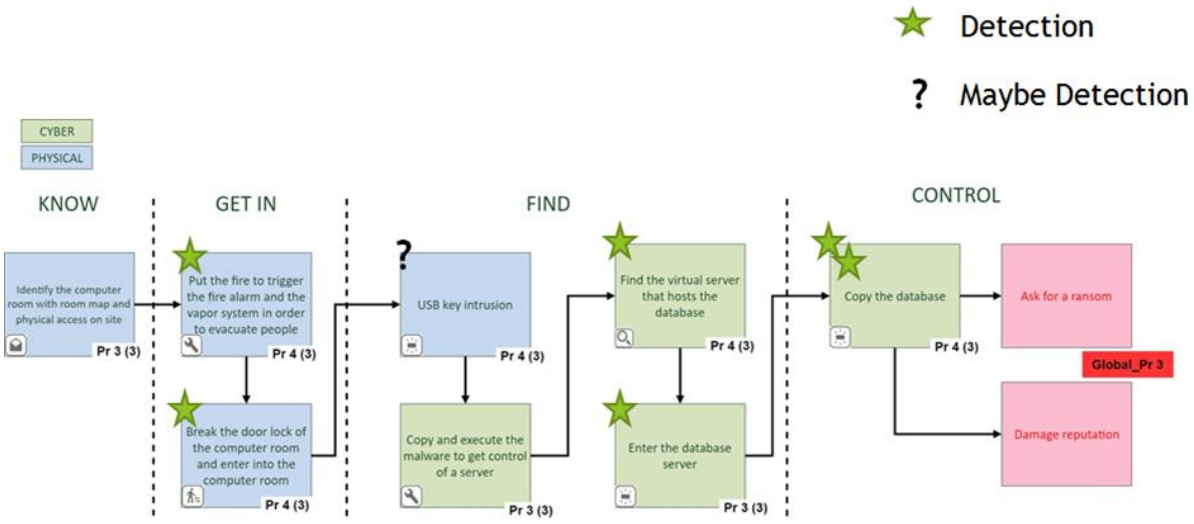

Figure 41 – Diagram of scenario 2

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- Intrusion and fire detection system (Deliverable 4.4)
- IT threat detection system (Deliverable 5.2)

The detections of the attack are illustrated with stars in Figure 41.

6.1.1.1 First detected threat

Step of the attack:

- The attacker starts putting the fire.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.

- Then, the building security agents investigate the video streams.

Next step of the attack:

- The fire triggers the fire alarm and the vapor system.

Steps of the defence:

- Detection of the fire by the intrusion and fire detection system.
- Then, the building threat monitoring system receives the fire alert from the intrusion and fire detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alerts (suspicious behavior alert and fire alert) as a "fire incident".
- Then, the "fire incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and changes the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling firefighters, 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.

6.1.1.2 Second detected threat

Step of the attack:

- The attacker breaks the door lock of the computer room and enters into the computer room.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Detection of the intrusion by the intrusion and fire detection system.
- Then, the building threat monitoring system receives the intrusion alert from the intrusion and fire detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alerts (suspicious behavior alert and intrusion alert) as an "intrusion incident".
- Then, the "intrusion incident" is sent to the data exchange layer and stored in the central database.
- The impact propagation and decision support model receives the incident and computes the potential impacts.

- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.1.1.3 Third detected threat

Step of the attack:

- The attacker searches for the database and finds the virtual server that hosts the database.

Steps of the defence:

- Detection of internal reconnaissance by the IT threat detection system.
- Then, the cyber threat monitoring system receives the internal reconnaissance alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a "cyber intrusion incident".
- Then, the "cyber intrusion incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.1.1.4 Fourth detected threat

Step of the attack:

- The attacker enters the database server.

Steps of the defence:

- Detection of unusual activities on the database server, which result from lateral movement of the attacker, by the IT threat detection system.
- Then, the cyber threat monitoring system receives the lateral movement alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators attach the alert to the previous "cyber intrusion incident".
- Then, the "cyber intrusion incident" update is sent to the data exchange layer and stored in the central database.
- The HAMS receives the update and may change the availability level of the hospital.

- The impact propagation and decision support model receives the update and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling the DPO (Data Protection Officer), 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.

6.1.1.5 Fifth detected threat

Step of the attack:

- The attacker copies and exfiltrates the database.

Steps of the defence:

- Detection of data exfiltration from the database server by the IT threat detection system.
- Then, the cyber threat monitoring system receives the data exfiltration alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators attach the alert to the previous “cyber intrusion incident”.
- Then, the “cyber intrusion incident” update is sent to the data exchange layer and stored in the central database.
- The impact propagation and decision support model receives the update and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as informing the DPO (Data Protection Officer) and national CERT of a data exfiltration, 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.

6.1.2 Scenario 5

Scenario 5 corresponds to a combination of cyber and physical attacks whose objective is shooting, explosive or sabotage in critical places (visible or invisible). The steps of the attacks are shown in Figure 42.

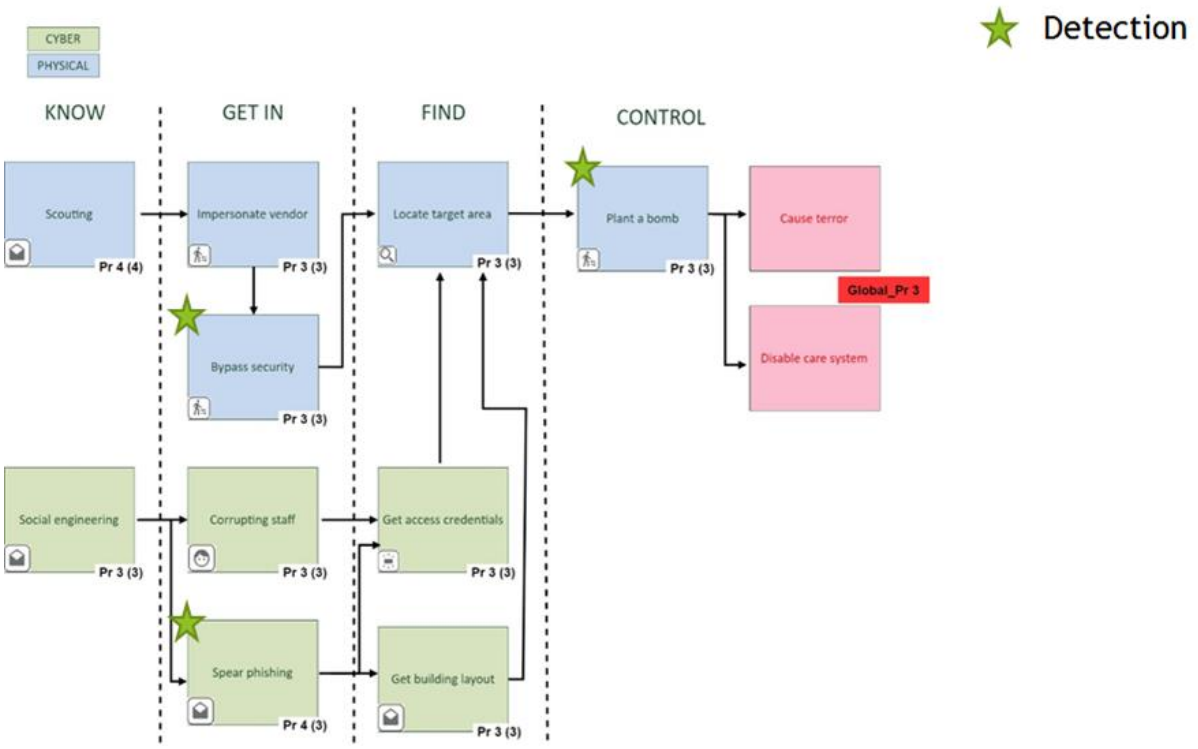

Figure 42 – Diagram of scenario 5

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- Intrusion and fire detection system (Deliverable 4.4)
- Advanced file analysis system (Deliverable 5.6)

The detections of the attack are illustrated with stars in Figure 42.

6.1.2.1 First detected threat

Step of the attack:

- The attacker sends a specific email with a malicious attachment to an internal employee.

Steps of the defence:

- Detection of the malware by the advanced file analysis system.
- Then, the cyber threat monitoring system receives the malware alert from the advanced file analysis system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a “malware incident”.
- Then, the “malware incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.

- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.1.2.2 Second detected threat

Step of the attack:

- The attacker bypasses security controls.

Steps of the defence:

- Detection of the intrusion by the intrusion and fire detection system.
- Then, the building threat monitoring system receives the intrusion alert from the intrusion and fire detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alert as an “intrusion incident”.
- Then, the “intrusion incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.1.2.3 Third detected threat

Step of the attack:

- The attacker plants a bomb.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents attach the alert to the previous “intrusion incident”.
- Then, the “intrusion incident” update is sent to the data exchange layer and stored in the central database.
- The HAMS receives the update and may change the availability level of the hospital.
- The impact propagation and decision support model receives the update and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.

- At the reception of the computed impacts, the reaction plan, such as calling the police, 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.

6.1.3 Scenario 8

Scenario 8 corresponds to a combination of cyber and physical attacks regarding distributed management over distributed buildings and considering external stakeholders (e.g., pharmacy, outpatients). The steps of the attacks are shown in Figure 43.

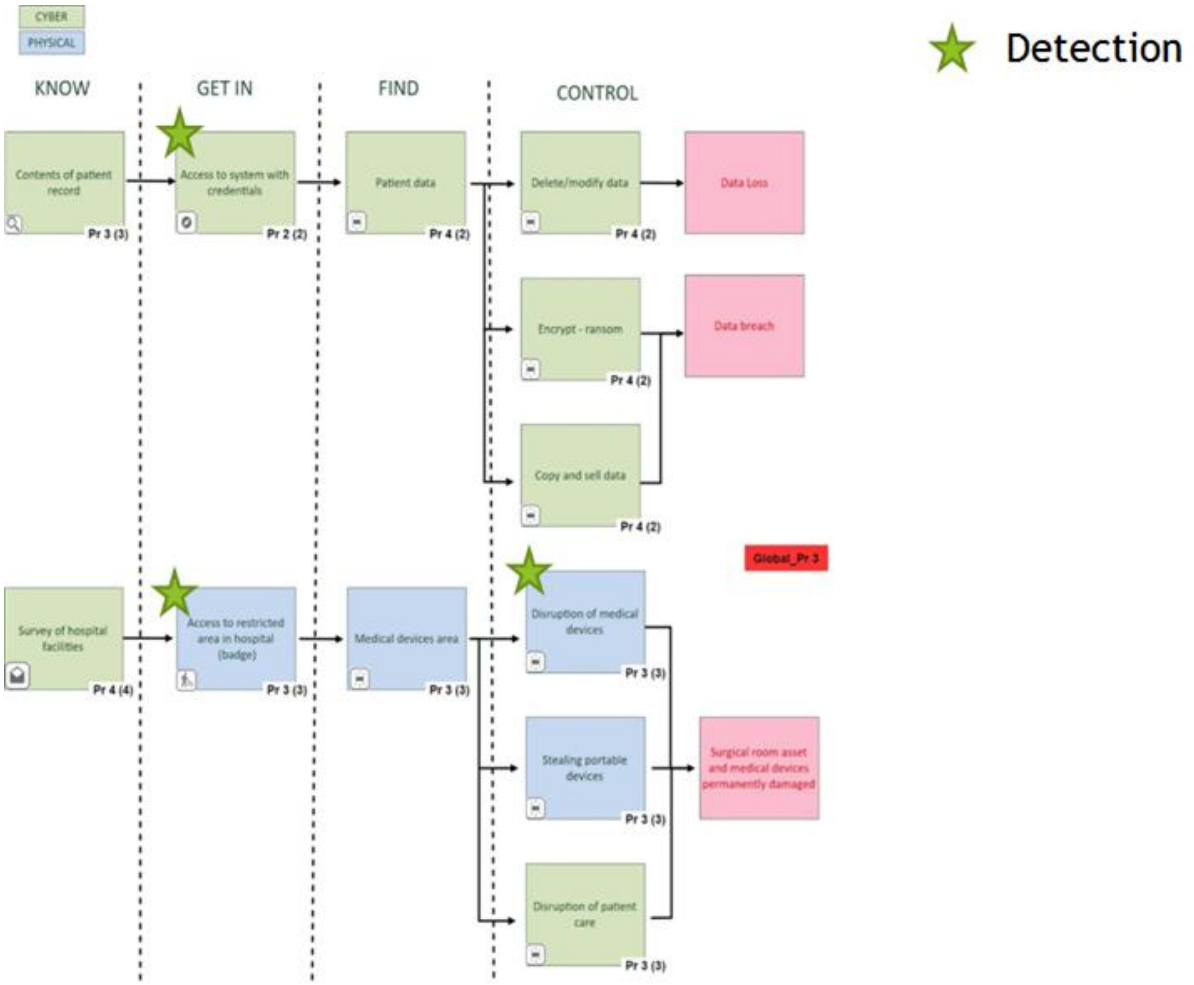

Figure 43 – Diagram of scenario 8

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- Intrusion and fire detection system (Deliverable 4.4)
- IT threat detection system (Deliverable 5.2)

The detections of the attack are illustrated with stars in Figure 43.

6.1.3.1 First detected threat

Step of the attack:

- The attacker accesses to the IT system with credentials.

Steps of the defence:

- Detection of a suspicious access by the IT threat detection system thanks to machine learning algorithms.
- Then, the cyber threat monitoring system receives the suspicious access alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a "cyber intrusion incident".
- Then, the "cyber intrusion incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.1.3.2 Second detected threat

Step of the attack:

- The attacker accesses to restricted area in hospital with a badge.

Steps of the defence:

- Detection of the intrusion by the intrusion and fire detection system.
- Then, the building threat monitoring system receives the intrusion alert from the intrusion and fire detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alert as an "intrusion incident".
- Then, the "intrusion incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.1.3.3 Third detected threat

Step of the attack:

- The attacker disrupts medical devices.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents attach the alert to the previous “intrusion incident”.
- Then, the “intrusion incident” update is sent to the data exchange layer and stored in the central database.
- The HAMS receives the update and may change the availability level of the hospital.
- The impact propagation and decision support model receives the update and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling the police, 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.

6.2 AP-HM protection against the scenarios of threat

The scenarios for AP-HM facilities are the following:

- Scenario 1: Targeting power supply of the hospital.
- Scenario 4: Targeting the air-cooling system of the hospital.
- Scenario 9: Blocking national crisis management.

6.2.1 Scenario 1

Scenario 1 corresponds to a combination of cyber and physical attacks targeting power supply of the hospital. Some steps of the attacks are shown in Figure 44.

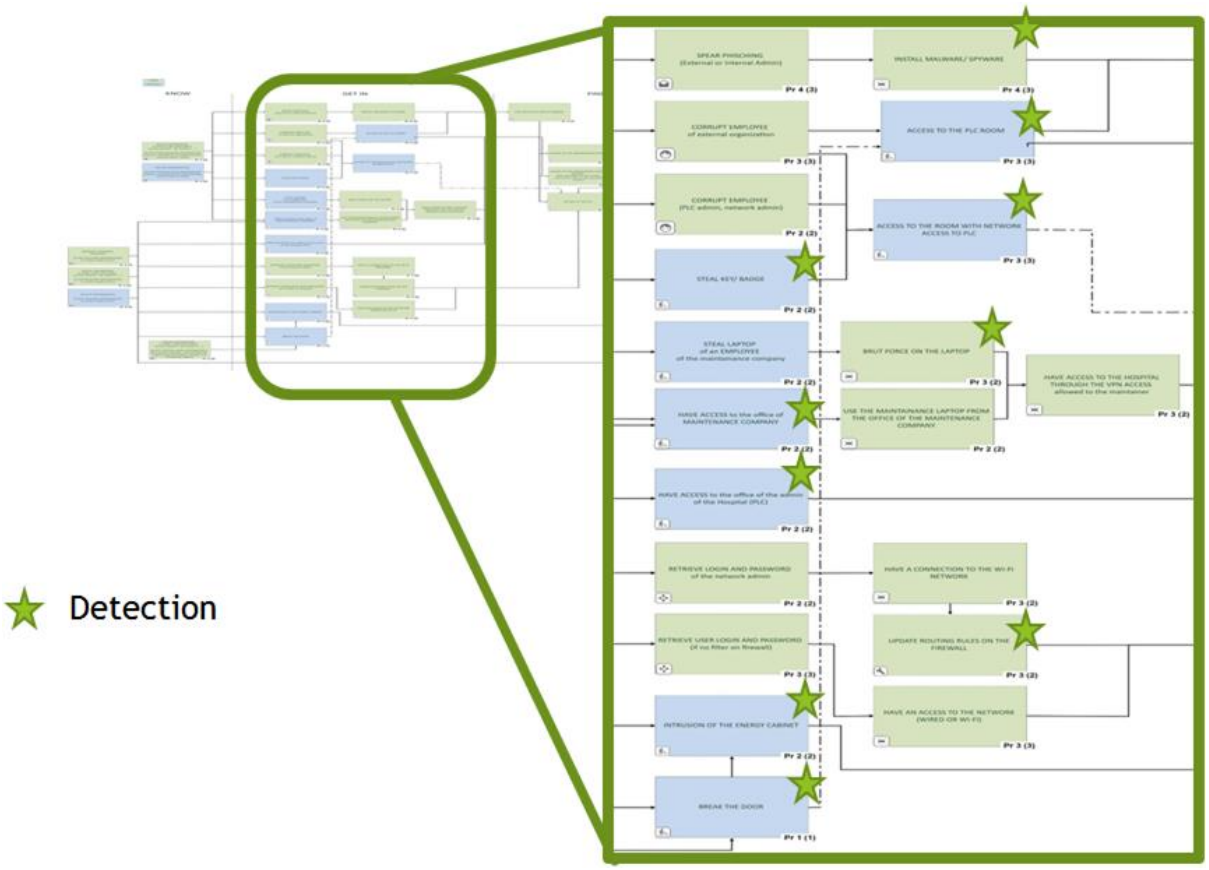

Figure 44 – Diagram of scenario 1

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- Intrusion and fire detection system (Deliverable 4.4)
- IT threat detection system (Deliverable 5.2)
- Advanced file analysis system (Deliverable 5.6)

The detections of the attack are illustrated with stars in Figure 44.

6.2.1.1 First detected threat

Step of the attack:

- The attacker sends a specific email with a malicious attachment to the PLC maintainer.

Steps of the defence:

- Detection of the malware by the advanced file analysis system.
- Then, the cyber threat monitoring system receives the malware alert from the advanced file analysis system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a “malware incident”.
- Then, the “malware incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.

- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.2.1.2 Second detected threat

Step of the attack:

- The attacker steals the key/badge of an employee.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.

6.2.1.3 Third detected threat

Step of the attack:

- The attacker gets into the PLC room.

Steps of the defence:

- Detection of the intrusion by the intrusion and fire detection system.
- Then, the building threat monitoring system receives the intrusion alert from the intrusion and fire detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alert as an “intrusion incident”.
- Then, the “intrusion incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.2.1.4 Fourth detected threat

Step of the attack:

- The attacker launches a brute-force attack on a computer.

Steps of the defence:

- Detection of the brute-force attempts by the IT threat detection system.
- Then, the cyber threat monitoring system receives the brute-force alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a "cyber intrusion incident".
- Then, the "cyber intrusion incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.2.1.5 Fifth detected threat

Step of the attack:

- The attacker uploads a new PLC program and lock admin access.

Steps of the defence:

- Detection of a security service alteration by the IT threat detection system.
- Then, the cyber threat monitoring system receives the security service alteration alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a "security service alteration incident".
- Then, the "security service alteration incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.2.2 Scenario 4

Scenario 4 corresponds to a combination of cyber and physical attacks targeting the air-cooling system of the hospital. The steps of the attacks are shown in Figure 45.

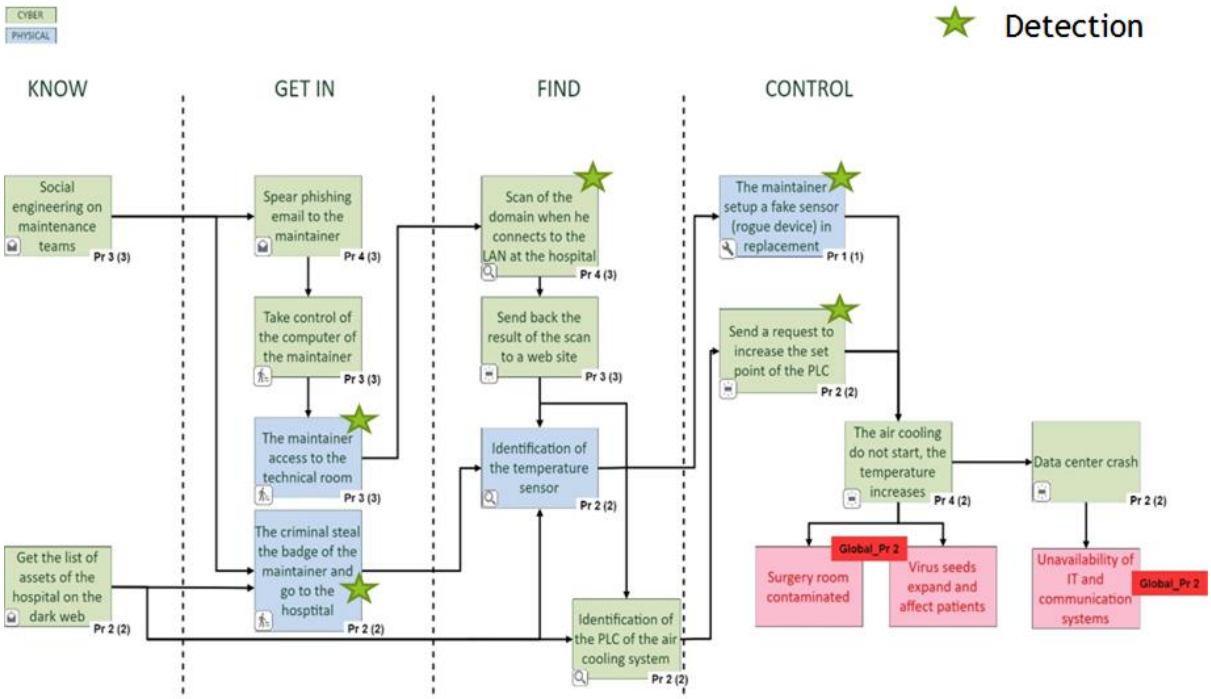

Figure 45 – Diagram of scenario 4

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Building threat monitoring system (Deliverable 4.10) with Data collection system (Deliverable 4.6)
- Advanced file analysis system (Deliverable 5.6)

The detections of the attack are illustrated with stars in Figure 45.

6.2.2.1 First detected threat

Step of the attack:

- The attacker sends a specific email with a malicious attachment to the maintainer.

Steps of the defence:

- Detection of the malware by the advanced file analysis system.
- Then, the cyber threat monitoring system receives the malware alert from the advanced file analysis system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a “malware incident”.
- Then, the “malware incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.

- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.2.2.2 Second detected threat

Step of the attack:

- The attacker stops the air cooling system, the temperature increases.

Steps of the defence:

- The data collection system gets the temperature data.
- Detection of suspicious readings by the building threat monitoring system.
- Then, the building threat monitoring system triggers an environmental behavior alert.
- Then, the building security agents investigate.
- Then, the building security agents confirm the alert as an “environmental incident”.
- Then, the “environmental incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling health practioners, 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.

6.2.3 Scenario 9

Scenario 9 corresponds to a combination of cyber and physical attacks to block national crisis management. The steps of the attacks are shown in Figure 46.

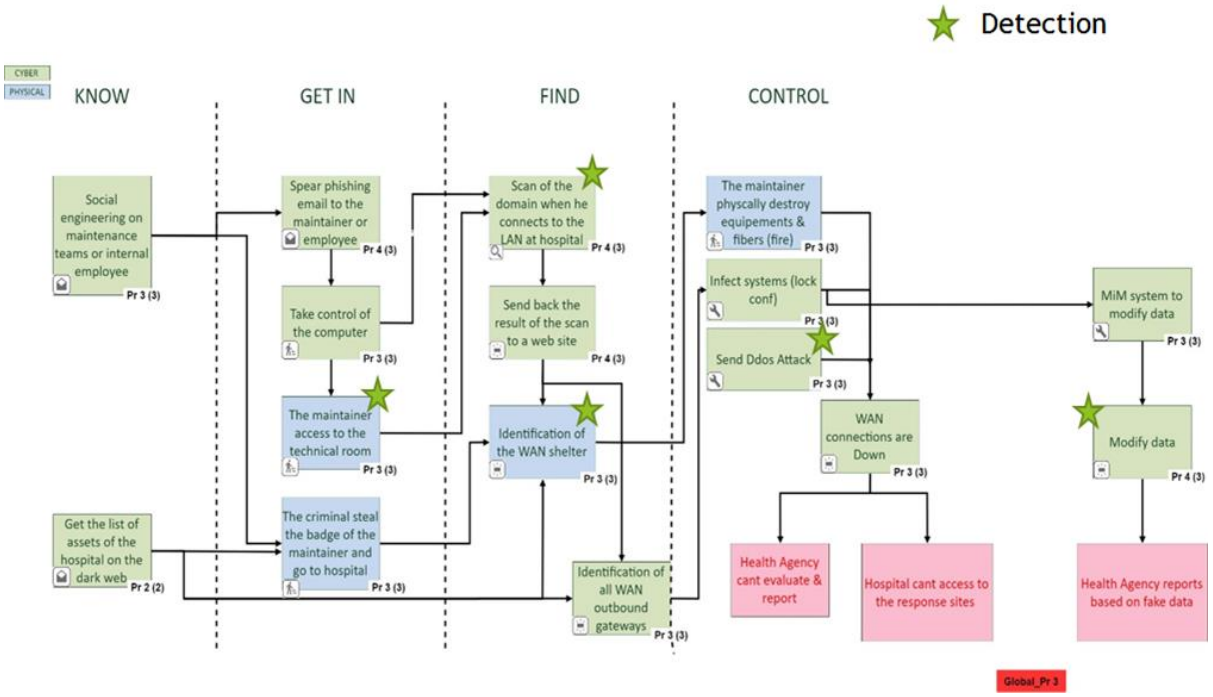

Figure 46 – Diagram of scenario 9

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- Intrusion and fire detection system (Deliverable 4.4)
- IT threat detection system (Deliverable 5.2)

The detections of the attack are illustrated with stars in Figure 46.

6.2.3.1 First detected threat

Step of the attack:

- The attacker accesses to the technical room.

Steps of the defence:

- Detection of the intrusion by the intrusion and fire detection system.
- Then, the building threat monitoring system receives the intrusion alert from the intrusion and fire detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alert as an “intrusion incident”.
- Then, the “intrusion incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.2.3.2 Second detected threat

Step of the attack:

- The attacker tries to identify the WAN shelter.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents attach the alert to the previous “intrusion incident”.
- Then, the “intrusion incident” update is sent to the data exchange layer and stored in the central database.
- The HAMS receives the update and may change the availability level of the hospital.
- The impact propagation and decision support model receives the update and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling the police, 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.

6.2.3.3 Third detected threat

Step of the attack:

- The attacker scans the network when he connects to the LAN at hospital.

Steps of the defence:

- Detection of internal reconnaissance by the IT threat detection system.
- Then, the cyber threat monitoring system receives the internal reconnaissance alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a “cyber intrusion incident”.
- Then, the “cyber intrusion incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.2.3.4 Fourth detected threat

Step of the attack:

- The attacker sends a DoS attack.

Steps of the defence:

- Detection of the network attack by the IT threat detection system.
- Then, the cyber threat monitoring system receives the DoS alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a "network incident".
- Then, the "network incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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

6.3 AMC protection against the scenarios of threat

The scenarios for AMC facilities are the following:

- Scenario 3: Targeting the population, IT systems and medical devices in the hospital, and patient data base.
- Scenario 6: Theft at hospital equipment, access to hospital network and IT systems.
- Scenario 7: Targeting IoT medical wearable devices (outside / inside).

6.3.1 Scenario 3

Scenario 3 corresponds to a combination of cyber and physical attacks targeting the population, IT systems and medical devices in the hospital, and patient data base. The steps of the attacks are shown in Figure 47.

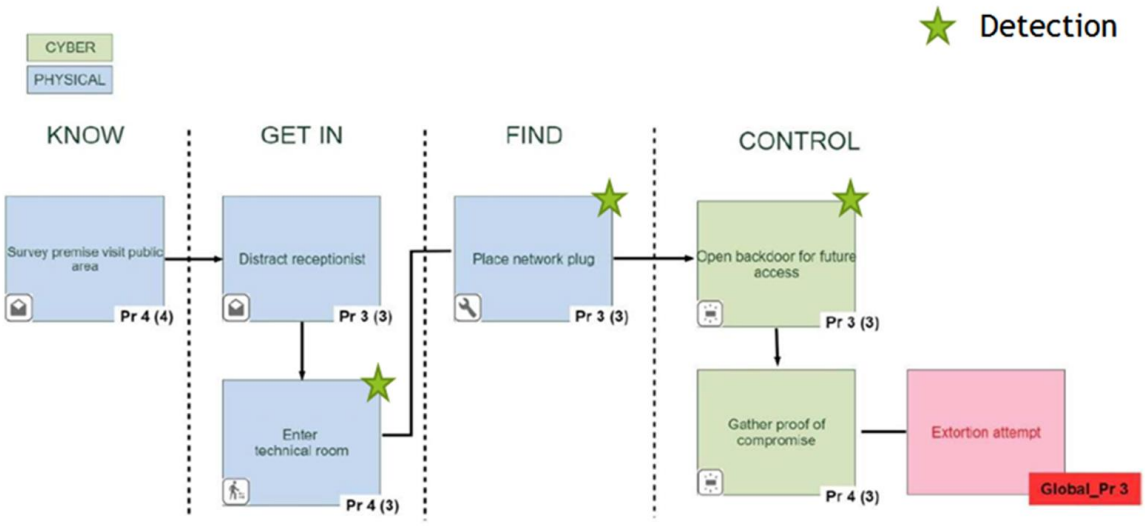

Figure 47 – Diagram of scenario 3

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- IT threat detection system (Deliverable 5.2)

The detections of the attack are illustrated with stars in Figure 47.

6.3.1.1 First detected threat

Step of the attack:

- The attacker enters the technical room.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alert as a “suspicious behaviour incident”.
- Then, the “suspicious behaviour incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.3.1.2 Second detected threat

Step of the attack:

- The attacker places a network plug.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents attach the alert to the previous “intrusion incident”.
- Then, the “intrusion incident” update is sent to the data exchange layer and stored in the central database.
- The HAMS receives the update and may change the availability level of the hospital.
- The impact propagation and decision support model receives the update and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.3.1.3 Third detected threat

Step of the attack:

- The attacker installs a backdoor for future access.

Steps of the defence:

- Detection of suspicious connections by the IT threat detection system.
- Then, the cyber threat monitoring system receives the suspicious connections alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a “cyber intrusion incident”.
- Then, the “cyber intrusion incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT), 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.

6.3.2 Scenario 6

Scenario 6 corresponds to a combination of cyber and physical attacks whose objective is a theft at hospital equipment and to access to hospital network and IT systems. The steps of the attacks are shown in Figure 48.

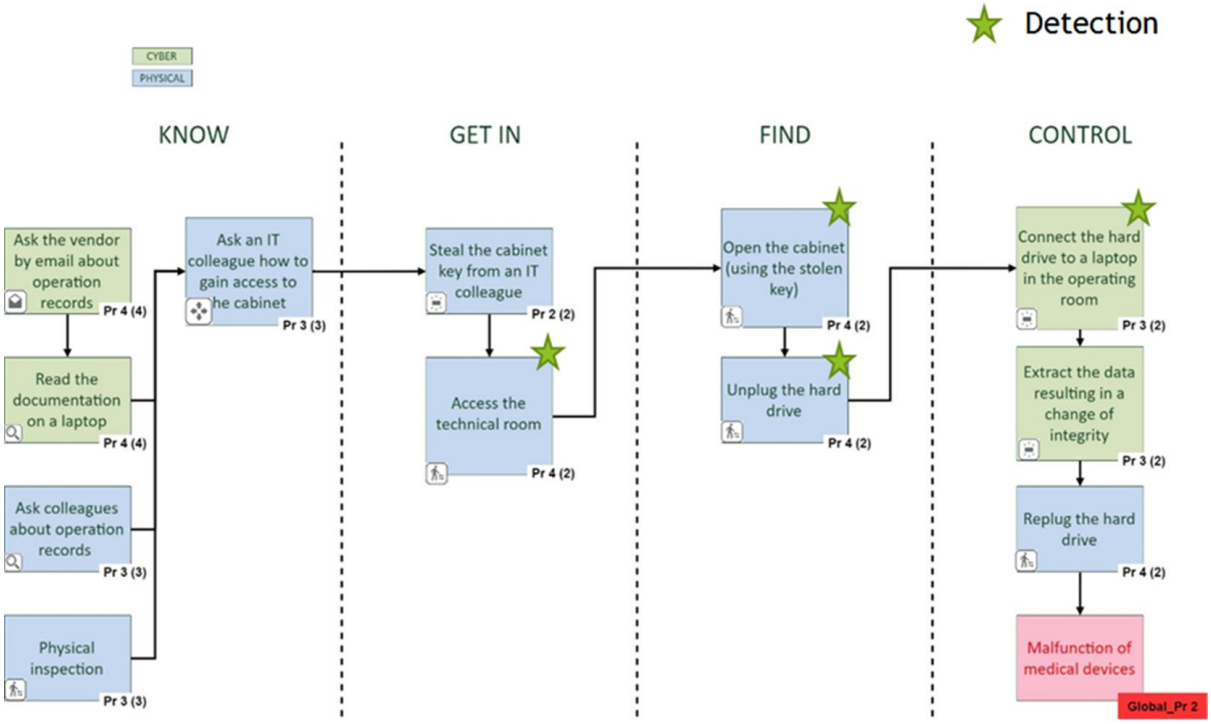

Figure 48 – Diagram of scenario 6

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- IT threat detection system (Deliverable 5.2)

The detections of the attack are illustrated with stars in Figure 48.

6.3.2.1 First detected threat

Step of the attack:

- The attacker accesses the technical room.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alert as a “suspicious behaviour incident”.
- Then, the “suspicious behaviour incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.

- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.3.2.2 Second detected threat

Step of the attack:

- The attacker opens the cabinet and unplugs the hard drive.

Steps of the defence:

- Detection of a second suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents attach the alert to the previous “suspicious behaviour incident”.
- Then, the “suspicious behaviour incident” update is sent to the data exchange layer and stored in the central database.
- The HAMS receives the update and may change the availability level of the hospital.
- The impact propagation and decision support model receives the update and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.3.2.3 Third detected threat

Step of the attack:

- The attacker connects the hard drive to a laptop in the operating room.

Steps of the defence:

- Detection of an unauthorized operation by the IT threat detection system.
- Then, the cyber threat monitoring system receives the unauthorized operation alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as an “unauthorized operation incident”.

- Then, the "unauthorized operation incident" is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling the IT security manager and 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.

6.3.3 Scenario 7

Scenario 7 corresponds to a combination of cyber and physical attacks targeting IoT medical wearable devices (outside / inside). The steps of the attacks are shown in Figure 49.

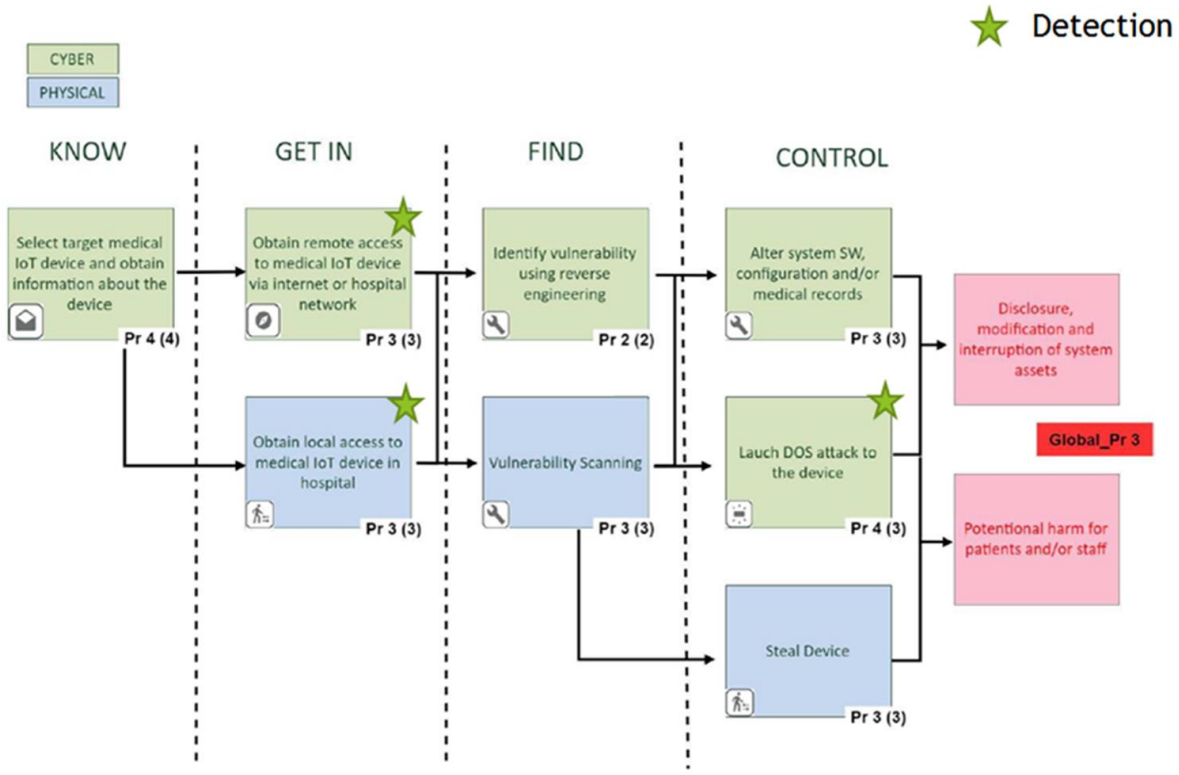

Figure 49 – Diagram of scenario 7

The cyber and physical threat detection systems, which are involved in this scenario, are the following:

- Suspicious behaviour detection system (Deliverable 4.2)
- Intrusion and fire detection system (Deliverable 4.4)
- IT threat detection system (Deliverable 5.2)
- E-Health device security analytics (Deliverable 5.8)

The detections of the attack are illustrated with stars in Figure 49.

6.3.3.1 First detected threat

Step of the attack:

- The attacker obtains local access to medical IoT device in hospital.

Steps of the defence:

- Detection of a suspicious behaviour by the suspicious behaviour detection system.
- Then, the building threat monitoring system receives the suspicious behavior alert from the suspicious behaviour detection system.
- Then, the building security agents investigate the video streams.
- Then, the building security agents confirm the alert as a “suspicious behaviour incident”.
- Then, the “suspicious behaviour incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling 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.

6.3.3.2 Second detected threat

Step of the attack:

- The attacker obtains remote access to medical IoT device via Internet or hospital network.

Steps of the defence:

- Detection of an unusual remote access by the e-health device security analytics.
- Then, the cyber threat monitoring system receives the unusual access alert from the e-health device security analytics.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as an “e-health device incident”.
- Then, the “e-health device incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling health practitioners, 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.

6.3.3.3 Third detected threat

Step of the attack:

- The attacker launches a DoS attack to the device.

Steps of the defence:

- Detection of the network attack by the IT threat detection system.
- Then, the cyber threat monitoring system receives the DoS alert from the IT threat detection system.
- Then, the SOC operators and analysts investigate the security events.
- Then, the SOC operators confirm the alert as a “network incident”.
- Then, the “network incident” is sent to the data exchange layer and stored in the central database.
- The HAMS receives the incident and may change the availability level of the hospital.
- The impact propagation and decision support model receives the incident and computes the potential impacts.
- Then the computed impacts are sent to the building threat monitoring system, the cyber threat monitoring system and the threat response and alert system.
- At the reception of the computed impacts, the reaction plan, such as calling incident response teams (CERT/CSIRT) and health practitioners, 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.

Conclusion

This specification has shown the consistency between all the systems involved in the global architecture through an overview of the overall SAFECARE solution and a description of each system and its interconnections.

Moreover the threat detection systems are able to detect the physical and cyber threats of the scenarios defined in SAFECARE Deliverable 3.6. Prevention, detection, response and mitigation capacities against threats targeting health services infrastructures are improved with the combination of all the physical and cyber threat detection systems, the threat monitoring systems and the integrated cyber-physical security systems that are part of the global architecture.

The three demonstrations that will take place at the hospital facilities in Marseille, Turin and Amsterdam will permit to test the solutions in operational conditions with security practitioners and local stakeholders. Thus, theory will be put into practice with the 9 scenarios of threats in operational conditions to confirm the optimum for systemic security brought by the SAFECARE architecture.

References

[1] https://www.milestonesys.com/solutions/platform/video-management-software/xprotect-corporate/

[2] JOINT TASK FORCE TRANSFORMATION INITIATIVE, et al. Guide for conducting risk assessments. National Institute of Standards and Technology, 2012.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

[4] GDPR, art 35.

[5] Article 29 Working Party (WP29) provided further interpretative guidance in its Guidelines on DPIA: see WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether the processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' (2017).

[6] ibid, 8. The document states also: 'Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities'.

[7] See CNIL, 'CNIL publishes an update of its PIA Guides' (CNIL, 26 February 2018) <www.cnil.fr/en/cnil-publishes-update-its-pia-guides> accessed 1 August 2019. Version adopted: version 1.

[8] WP29 (n2), 18.

[9] Details regarding the description and purposes of the processing operations of personal data will be left aside, for evident reasons of not repeating the content outlined elsewhere in this document. Anyway, this information is available in the DPIA documentation held by every partner.

[10] CNIL, 'Privacy Impact Assessment (PIA). Methodology' (February 2018 edition); CNIL, 'Privacy Impact Assessment (PIA). Knowledge Bases' (February 2018 edition).