SAFECARE

Integrated cyber-physical security for health services

White Book

Deliverable 8.4

Lead Author: EOS

Contributors: All

Deliverable classification: PU

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

Version Control Sheet

Title	*White Book*
Prepared By	*EOS*
Approved By	*FST, SPF*
Version Number	*1*
Contact	f.giacinti@eos-eu.com

Revision History:

Version	Date	Summary of Changes	Initials
0.1	21.06.2021	Initial ToC draft sent to the consortium	EOS
0.2	03.06.2021	Initial Executive Summary and deliverable's description sent to the consortium	EOS
0.3	10.06.2021	First partners' contributions	ALL
0.4	19.11.2021	Contributions from solutions providers	ALL
0.5	21.11.2021	Peer Review	FST
0.6	22.11.2021	Integration comments	EOS
0.7	24.11.2021	Peer Review	SPF
1	25.11.2021	Final Deliverable	EOS

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

Table of Contents

List of Figures

LIST OF TABLES

List of acronyms

Acronym	Definition
AFAS	Advanced File Analysis System
BMS	Building management system
BTDS	BMS threat detection system
BTMS	Building Threat Monitoring System
CDB	Central Database
CMT	Crisis Management Team
CTMS	Cyber Threat Monitoring System
DCS	Data Collection System
DLL	Dynamic link library
DoA	Description of Actions
DXL	Data Exchange Layer
D&C	Dissemination and communication
D8.4	Deliverable 8.4
EAI	Enterprise Applications Integration
EDSA	E-health Devices Security Analytics
HAMS	Hospital Availability Management System
HAZOP	HAZard and OPerability analysis
ICT	Information and Communication Technologies
IEs	Innovative elements
IFDS	Intrusion and Fire Detection System
IoT	Internet of Things
IPDSM	Impact Propagation and Decision Support Module
ISO	International Standards Organization
IT	Information technology
ITTDS	IT Threat Detection System
MAS	Mobile Alerting System
MQTT	MQ Telemetry Transport
OMW	Orion Malware

OT	Operational Technology
PLC	Programmable Logic Controller
SBDS	Suspicious Behaviour Detection System
SCADA	Supervisory Control and Data Acquisition
SOC	Security Operations Center
SPAN	Switched Port Analyzer
TAP	Terminal Access Point
TRAS	Threat Response and Alert System
UI	User Interface
VMS	Video Management System
WP	Work Package

The SAFECARE Project

Over the last decade, the European Union faced numerous threats, which gradually increased in magnitude changing the lives and habits of millions of citizens installing fear and terror. The sources of these threats and the weapons used were heterogeneous and so was the impact on population. Due to the enormous risks and the potential impact these threats may have on society, Europe is required to increase awareness among the population against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Nowadays, the lines between physical and cyber worlds cannot be viewed separately as they are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analysed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats. Health services are at the same time among the most critical infrastructures and the most vulnerable ones. They are widely relying on information systems to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this project is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It promotes 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 potential "customers" across Europe.

Executive Summary

Living in a safe and secure society is a fundamental human need. The security of critical infrastructures must be maintained so that the supply of power, water or other resources is not endangered, and that human lives are not at risk. Modern critical infrastructures are increasingly complex and they are turning into cyber-physical infrastructures because Information and Communication Technologies (ICT) are more and more important in the context of infrastructure management. Today, most of organizations are susceptible to cyber threats because they are increasingly exposed to the internet and to the external world. At the same time, most organisations are also susceptible to natural and physical attacks with strong potential impacts. Natural threats strongly depend on the location in which critical infrastructures are built (e.g. if hospitals are built in a seismic area, they are mainly interested on earthquake detection, if they are built near rivers, their attention is focused on potential floods and so on); similarly, physical threats are also strongly influenced by the culture and stress level of both patients and visitors (e.g., frequent violence) but also by the personnel (e.g. frequent theft, in terms of PC and medical equipment, and/or manmade fires). Hospitals already developed emergency defence strategies with fire-fighters and police, but this can be improved at the lens of the new geopolitical context, or using new communication technologies and media.

Within this context, the main aim of the SAFECARE project is to foster the creation of solutions for the improvement of cyber and physical security in the healthcare context, with specific regard to healthcare infrastructures. The challenge 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 comprehensive protection system, which will cover threat prevention, detection, response and, in case of failure, mitigation of impacts across infrastructures, populations and environment. Over a 39-month time frame, the SAFECARE Consortium has designed, tested, validated and demonstrated 13 innovative elements (IEs), developed in the Description of Actions (DoA), which will optimize the protection of critical infrastructures under operational conditions. These elements are interactive, cooperative and complementary, aiming at maximizing the potential use of each individual element. The consortium has also engaged with leading hospitals, national public health agencies and security Stakeholders across Europe to ensure that SAFECARE's global solution is flexible, scalable and adaptable to the operational needs of various hospitals across Europe. In this context, the aim will be to meet the requirements of newly emerging technologies and standards.

1. Introduction

The end goal of the SAFECARE project is to protect healthcare infrastructures, and eventually the safety of the patient, by fostering the creation of solutions for the improvement of cyber and physical security in the current healthcare context.

After project pilots having taken place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners in order to simulate attack scenarios in near-real conditions, this document attempts to present the SAFECARE global solution, its innovative aspects and its ways of use in a user-friendly way to facilitate its uptake after the project's end.

1.1 Deliverable 8.4

The present deliverable (D8.4) is part of the Work Package 8 (WP8), Dissemination, Communication and Exploitation, Task 8.2 - Dissemination and communication (D&C) implementation and project events, and it presents the SAFECARE global solution, its advantages from an end-user perspective, its specific components and their different ways of use in the crisis-management cycle. The aim of D8.4 is to: a) present how to use SAFECARE in crisis and risk-management processes and b) to provide a technological overview of project results.

In order to achieve its purposes, D8.4 firstly presents the different components of the SAFECARE global solution (Section 2) and the expected benefits of the future use of SAFECARE from an end-user perspective (Section 3).

Secondly, D8.4 details how to integrate the SAFECARE global solution in a hospital ecosystem (Section 4) and it presents the way each module can be used to improve the crisis-management process (Section 5).

2. The SAFECARE global solution

This section aims to present the SAFECARE global solution designed for the improvement of cyber and physical security in the healthcare context. To do this, it will present the SAFECARE global architecture and the several dedicated systems developed within the project.

2.1 The SAFECARE global architecture

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

- Physical security solutions;
- Cyber security solutions;
- Integrated cyber-physical security solutions.

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. Meanwhile, cyber security solutions correspond to cyber monitoring systems as well as threat detection systems related to information technology (IT), building management system (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 whose role is to integrate different data sources and better take into account the combination of physical and cyber security threats.

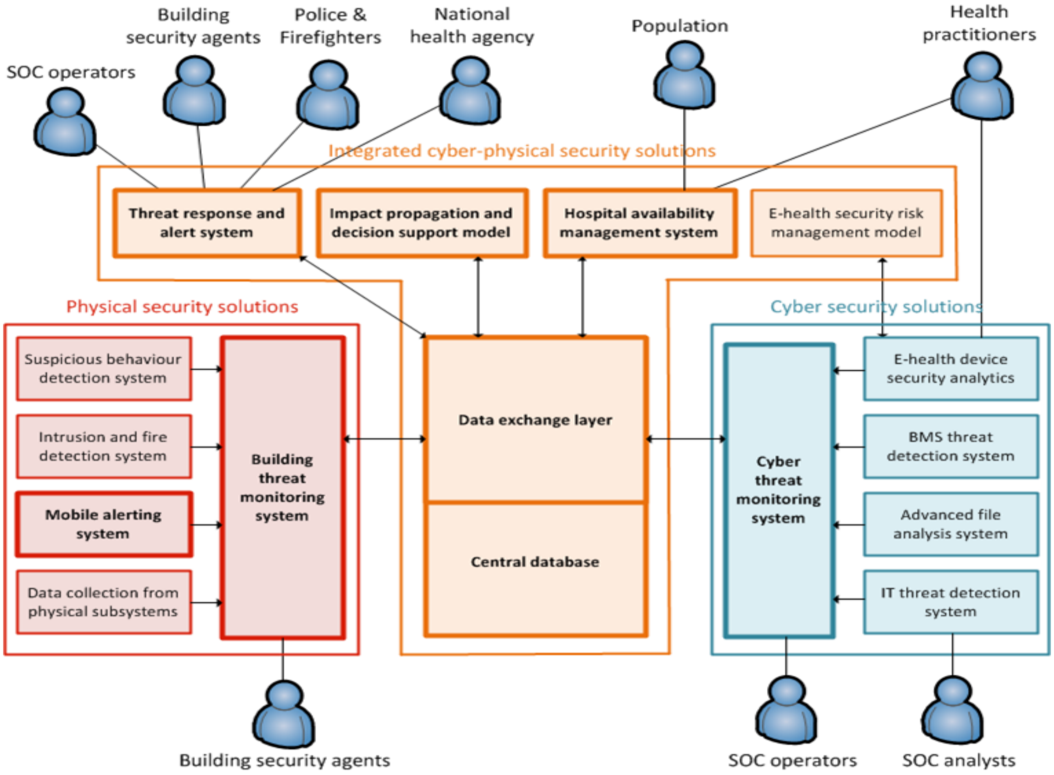

Building security agents
Police & Firefighters
National health agency
Population
Health practitioners
SOC operators
Integrated cyber-physical security solutions
Threat response and alert system
Impact propagation and decision support model
Hospital availability management system
E-health security risk management model
Physical security solutions
Cyber security solutions
Suspicious behaviour detection system
Intrusion and fire detection system
Mobile alerting system
Data collection from physical subsystems
Building threat monitoring system
Data exchange layer
Central database
Cyber threat monitoring system
E-health device security analytics
BMS threat detection system
Advanced file analysis system
IT threat detection system
Building security agents
SOC operators
SOC analysts

Figure 1: SAFECARE global architecture

2.2 The SAFECARE systems

In order to fulfil their role, each solution ensemble is composed of several dedicated systems (modules).

The physical security solutions rely on:

- The suspicious behaviour detection system (SBDS);
- The intrusion and fire detection system (IFDS);
- The data collection system (DCS);
- The mobile alerting system (MAS);
- And the building threat monitoring system (BTMS).

The cyber security solutions rely on:

- The IT threat detection system (ITTDS);
- The BMS threat detection system (BTDS);
- The advanced file analysis system (AFAS);
- The e-health devices security analytics (EDSA);
- And the cyber threat monitoring system (CTMS).

The integrated cyber-physical security solutions rely on:

- The data exchange layer (DXL);
- The central database (CDB);
- The impact propagation and decision support model (IPDSM);
- The threat response and alert system (TRAS);
- The hospital availability management system (HAMS);
- And the e-health security risk management model.

2.2.1 Suspicious behaviour detection system

The abstract interaction of components to integrate suspicious behaviour detection is shown in Figure 2:

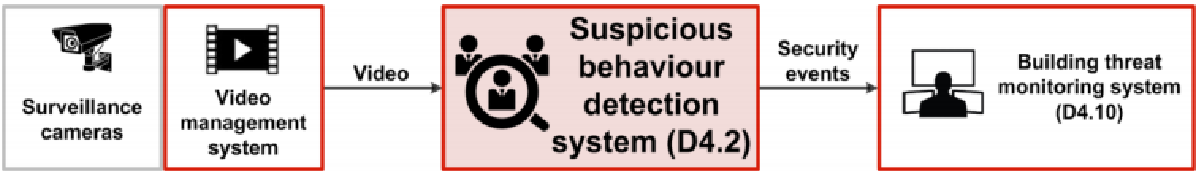

Surveillance cameras
Video management system
Video
Suspicious behaviour detection system (D4.2)
Security events
Building threat monitoring system (D4.10)

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 (XProtect Essential+ is a full-featured version of Milestone's market-leading video management software (VMS). With support for up to eight cameras and devices, XProtect Essential+ is the perfect match for smaller businesses who want basic video surveillance to protect employees and assets) 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.

In general, video analytics carry out their prediction on the direct input streams (video streams or event streams) and produce alerts. The BTMS may carry out further analysis in context; i.e. the SBDS 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).

2.2.2 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:

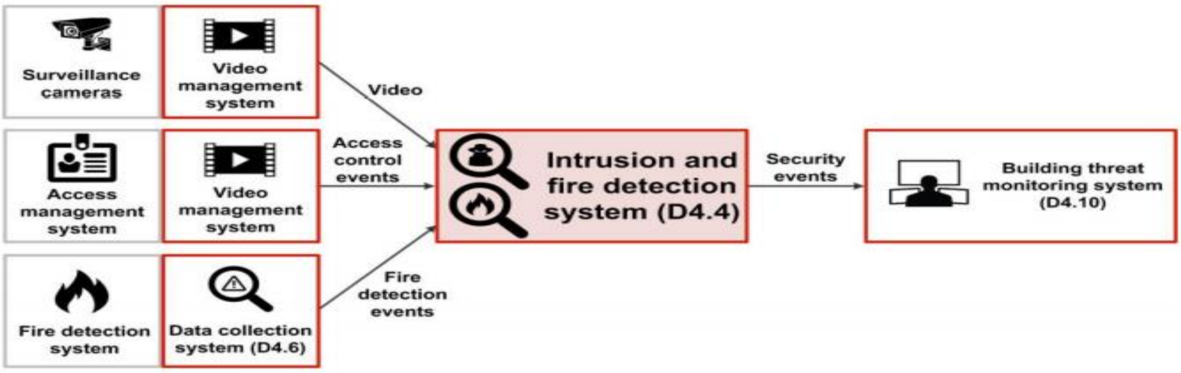


Figure 3: Interconnections of the intrusion and fire detection system

The two systems for intrusion detection and fire detection are separately implemented, although they are documented in one specification and produce one software deliverable. Both camera streams and access management events, for most major vendors, are covered by existing integrations with the XProtect software. As shown in Figure 3, the XProtect Event Server, on which the BTMS is based, will accept events from the data collection system for physical sensors for fire detection (smoke, heat, etc.) – see following subsection.

2.2.3 Data collection system

The system collects data from physical subsystems (such as ICS, SCADA, smart building sensors) as shown in Figure 4.

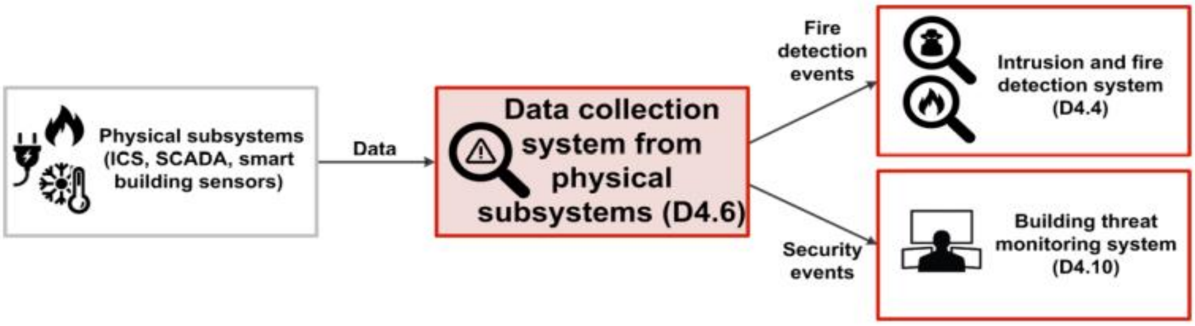

Physical subsystems (ICS, SCADA, smart building sensors)
Data
Data collection system from physical subsystems (D4.6)
Fire detection events
Security events
Intrusion and fire detection system (D4.4)
Building threat monitoring system (D4.10)

Figure 4: Interconnections of the data collection system

The DCS 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 centers;
- 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.

2.2.4 Mobile alerting system

The MAS functions as an information exchange channel between the local security agents and health personnel inside the hospital and the security modules that comprise the SAFECARE architecture. The MAS achieves its role in 4 ways:

1. It enables the users to report specific categories of security threats or impacts correlated to a specific failure point inside of a structure such as a hospital (e.g. system failure, natural hazard, terrorist attack...) as shown in Figure 5. The report by the user will contain information about the threat its type (e.g. loitering, tailgating, suspicious behaviour etc.) location, estimated severity and a brief description.

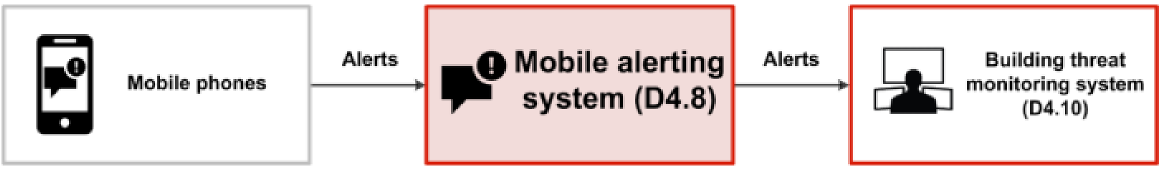

Mobile phones
Alerts
Mobile alerting system (D4.8)
Alerts
Building threat monitoring system (D4.10)

Figure 5: Mobile alerting system sending alerts

2. It enables the security operators to visualize contextual information (e.g. geolocation, building, room, video feed) on suspected threats detected by the BTMS as shown in Figure 6. The security operators will then verify the presence of the threat in person and report the outcome of the inspection to the BTMS.

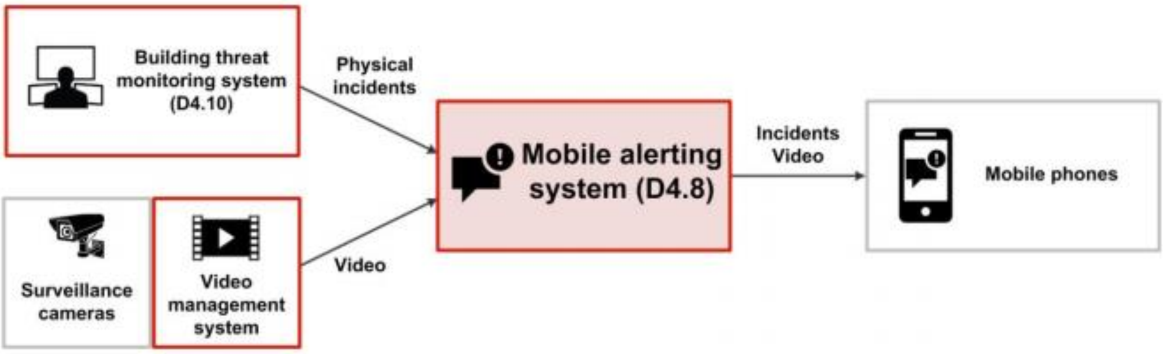


Figure 6: Mobile alerting system receiving physical incidents

3. It enables the BTMS to visualize the output of the impact propagation model by showing 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 7.

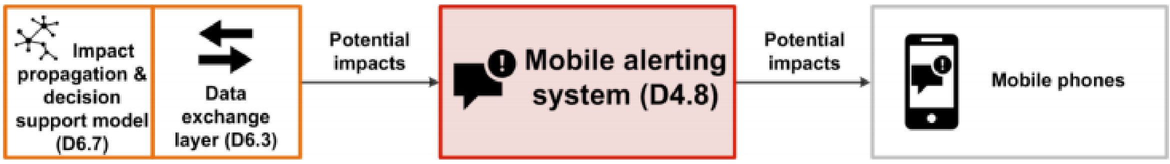

Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Mobile alerting system (D4.8)
Potential impacts
Mobile phones

Figure 7: Mobile alerting system receiving potential impacts

4. It enables the users to receive notifications containing all the information needed to manage a security threat (e.g. location, emergency procedure, video etc.) as shown in Figure 8. The notifications will be sent to the users with information specialized according to the role (e.g. security guard, health personnel, manager etc.) in their profile.

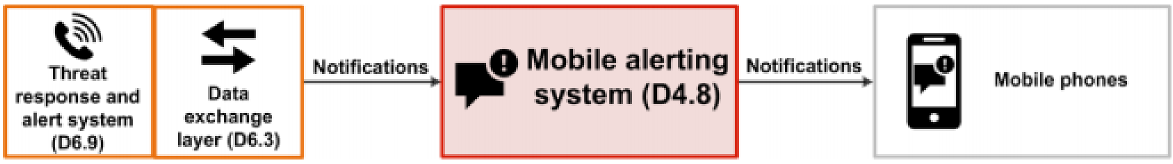

Threat response and alert system (D6.9)
Data exchange layer (D6.3)
Notifications
Mobile alerting system (D4.8)
Notifications
Mobile phones

Figure 8: Mobile alerting system receiving notifications

2.2.5 Building threat monitoring system

The BTMS 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 judge 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 CDB (see Figure 9):

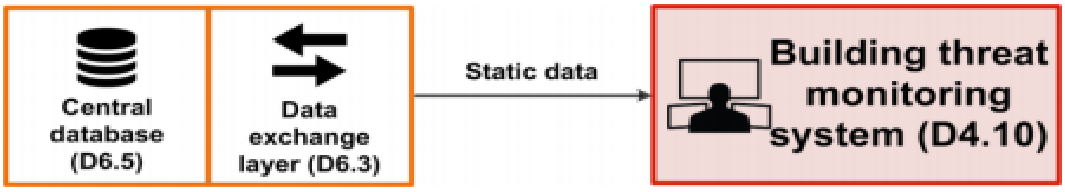

Central database (D6.5)
Data exchange layer (D6.3)
Static data
Building threat monitoring system (D4.10)

Figure 9: Building threat monitoring system getting static data

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 DXL, as shown below:

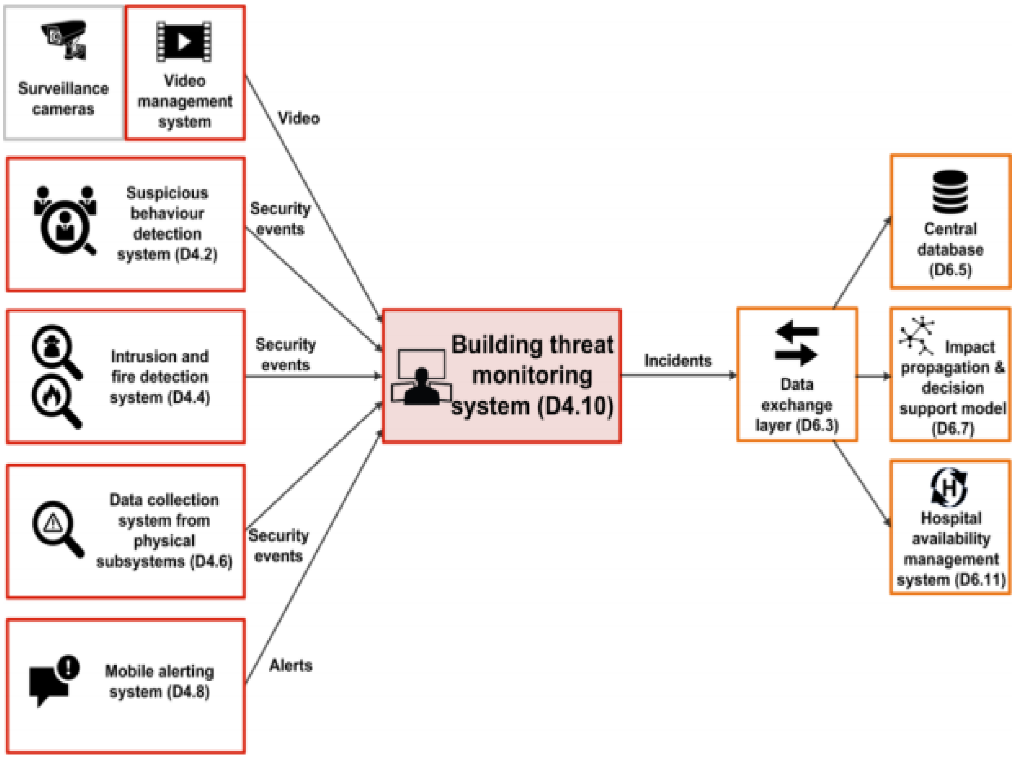

Surveillance cameras
Video management system
Video
Suspicious behaviour detection system (D4.2)
Security events
Intrusion and fire detection system (D4.4)
Security events
Data collection system from physical subsystems (D4.6)
Security events
Mobile alerting system (D4.8)
Alerts
Building threat monitoring system (D4.10)
Incidents
Data exchange layer (D6.3)
Central database (D6.5)
Impact propagation & decision support model (D6.7)
Hospital availability management system (D6.11)

Figure 10: Interconnections of the building threat monitoring system

The BTMS is also responsible for receiving and relaying the incident handling response and decision support, according to the impact propagation model, as shown in Figure 11:

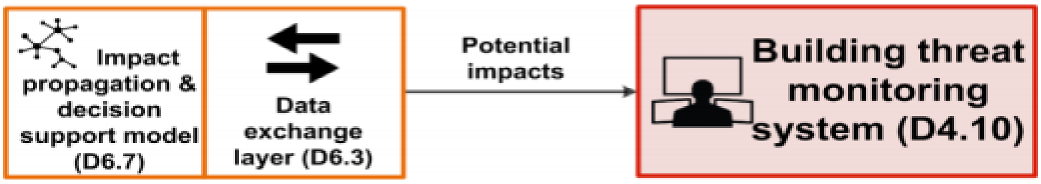
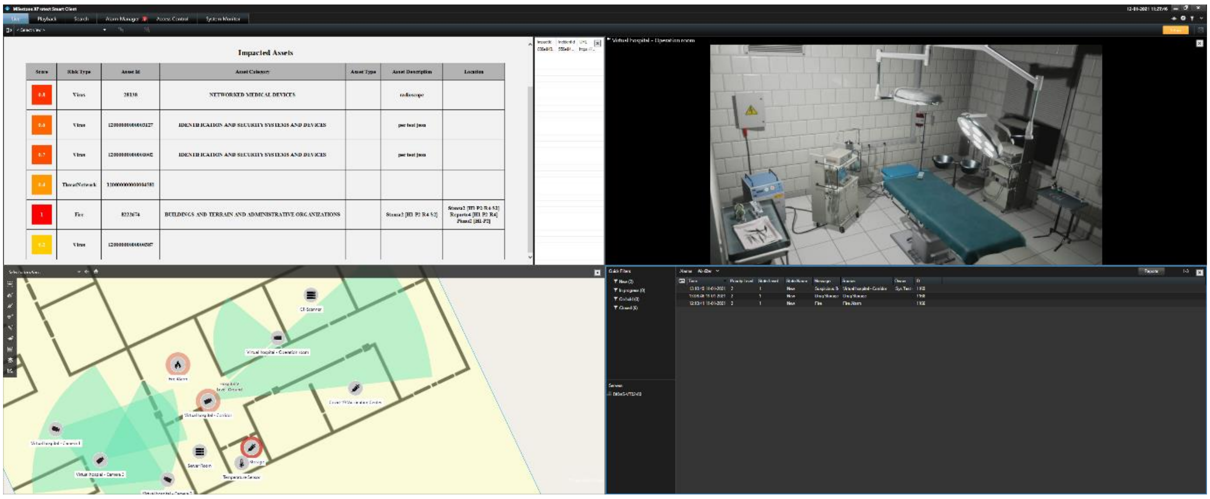

Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Building threat monitoring system (D4.10)

Figure 11: Building threat monitoring system receiving potential impacts

BTMS provides a graphical user interface based on the Milestone Stone XProtect® Smart Client for configuration, notification and user interaction (see also Section **Erreur ! Source du renvoi introuvable.**). As an example, a Smart Client view with four sub-windows is shown in Figure 12. In the top left is the impact view, generated by the MAS from the result of the IPDSM, in the top right is a camera view from inside the virtual hospital, bottom left is a building representation with cameras, assets and a sensor with active alarms shown as well, and in the bottom right is an alarm list view, with active alarms.

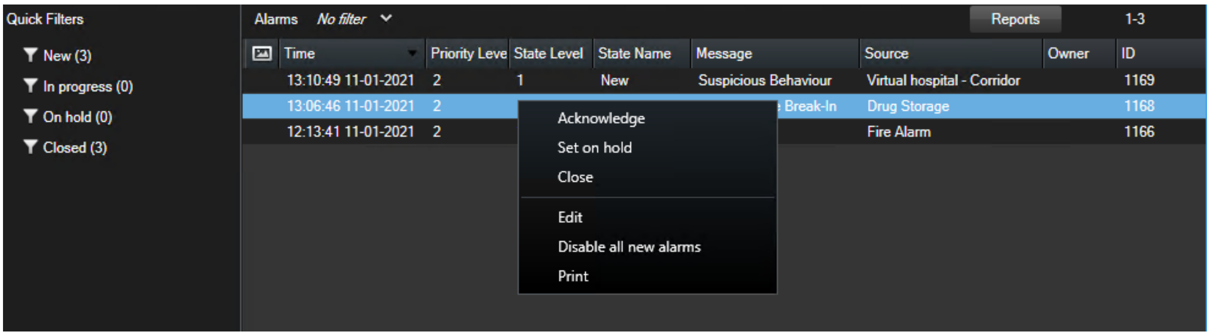

Milestone XProtect Smart Client
Live
Playback
Search
Alarm Manager
Access Control
System Monitor
Virtual hospital - Operation room
CT-Scanner
Virtual hospital - Corridor room
Fire Alarm

Impacted Assets

Score	Risk Type	Asset Id	Asset Category	Asset Type	Asset Description	Location
0.8	Virus	28138	NETWORKED MEDICAL DEVICES		radioscope	
0.8	Virus	120000000000005127	IDENTIFICATION AND SECURITY SYSTEMS AND DEVICES		per test json	
0.7	Virus	[illegible]	IDENTIFICATION AND SECURITY SYSTEMS AND DEVICES		per test json	
0.4	ThreatNetwork	110000000000004581				
1	Fire	8223674	BUILDINGS AND TERRAIN AND ADMINISTRATIVE ORGANIZATIONS		Stanza2 [H1 P2 R4 S2]	Stanza2 [H1 P2 R4 S2] Reparto4 [H1 P2 R4] Piano2 [H1 P2]
0.2	Virus	120000000000000587				

Figure 12 View with four sub-windows in the XProtect® Smart Client in BTMS. The server icon and syringe icon are under the Creative Commons Attribution 4.0 International license (https://fontawesome.com/license) or the Creative Commons CC BY (https://creativecommons.org/about/cclicenses/). The fire icon used has been created by Aisyah from the Noun Project; the thermometer icon has been created by DinosoftLabl from the Noun Project.

Figure 13 shows the user interface for alarm handling. *Acknowledge* and *Close* are used in the context of SAFECARE. Acknowledging an alarm will validate the corresponding alert into an incident, and it will change the state to *In progress.* Closing an alarm will change it to state *Closed. It* also means that the corresponding alert is not considered an incident.



Time	Priority Leve	State Level	State Name	Message	Source	Owner	ID
13:10:49 11-01-2021	2	1	New	Suspicious Behaviour	Virtual hospital - Corridor		1169
13:06:46 11-01-2021	2			Break-In	Drug Storage		1168
12:13:41 11-01-2021	2				Fire Alarm		1166

Figure 13: Options for a user to handle alarms

2.2.6 IT threat detection system

The ITTDS is a solution capable of detecting known cyber-attacks as well as suspicious behaviours that may be the work of a new unknown method for an attacker to slip into or harm the system.

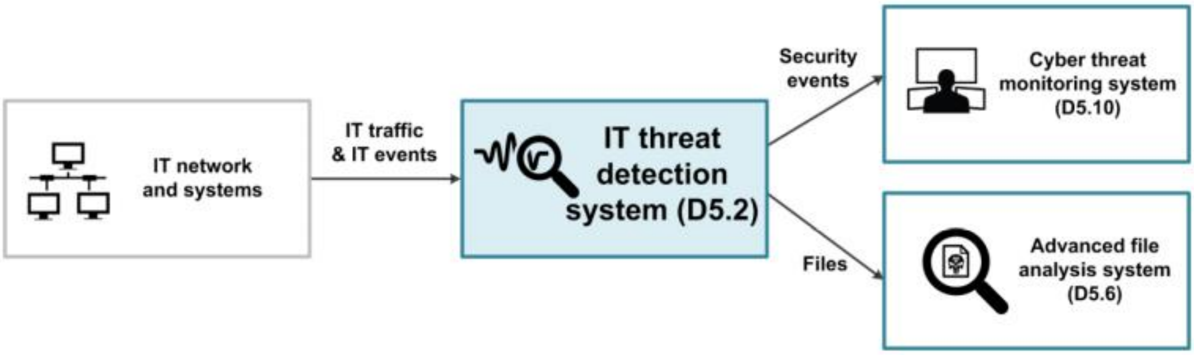

IT network and systems
IT traffic & IT events
IT threat detection system (D5.2)
Security events
Files
Cyber threat monitoring system (D5.10)
Advanced file analysis system (D5.6)

Figure 14: Interconnections of the IT threat detection system

To detect network attacks, the ITTDS requires the duplication of the network traffic as input either by using a network Terminal Access Point (TAP) or by port mirroring a switch. Thus, it is able to inspect the network traffic in near real-time by matching attack patterns, also known as signatures, to detect known cyber-attacks.

The ITTDS can also receive IT events from the IT systems. To do so, it requires configuring the IT infrastructure to send such events. Based on these events and the configuration of detection rules, the system generates security events when the IT events match the detection rules. These security events are then sent to the cyber threat monitoring system.

Machine learning algorithms are implemented and take as input the IT events as well as the replicated network traffic to detect suspicious behaviours. It produces security events highlighting low-level signals of advanced attacks.

The ITTDS also extracts files from the network traffic and automatically submits them to the advanced file analysis system.

2.2.7 BMS threat detection system

The BTDS is based on Forescout eyeInspect, which is a passive network intrusion detection system focused on Operational Technology (OT), including protocols used in industrial control systems and building automation systems.

EyeInspect delivers device visibility and asset inventory by analyzing the traffic data for hundreds of protocols. Furthermore, it integrates several threat detection engines including communication anomaly detection and a library of signatures of potential threats for the OT network. This allows catching 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 support for 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 are available also in building automation networks.

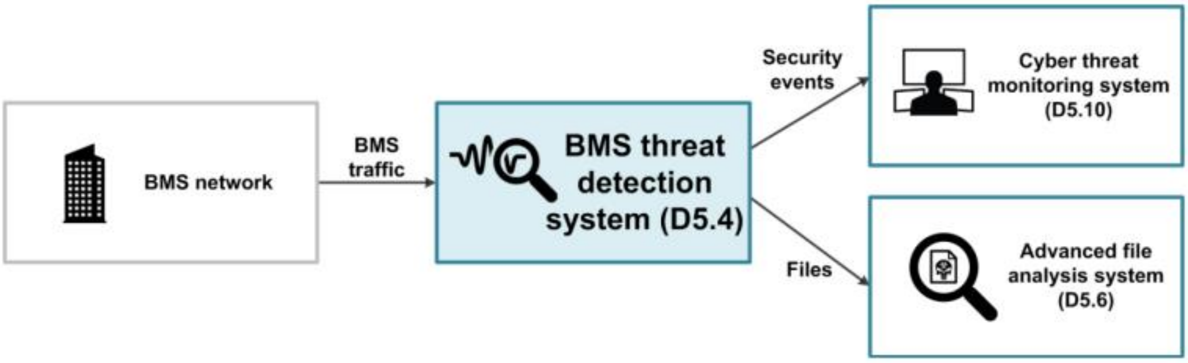

BMS network
BMS traffic
BMS threat detection system (D5.4)
Security events
Files
Cyber threat monitoring system (D5.10)
Advanced file analysis system (D5.6)

Figure 15: Interconnections of the BMS threat detection system

As illustrated in Figure 15, the BTDS analyses the BMS network traffic. The same techniques 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 BTDS is improved to extract files from the network traffic and submit them to the AFAS for an in-depth analysis.

2.2.8 Advanced file analysis system

The AFAS is a solution capable of detecting the malicious files in critical health infrastructures by performing an in-depth analysis - both statically and dynamically - of files that transit through the IT and BMS networks.

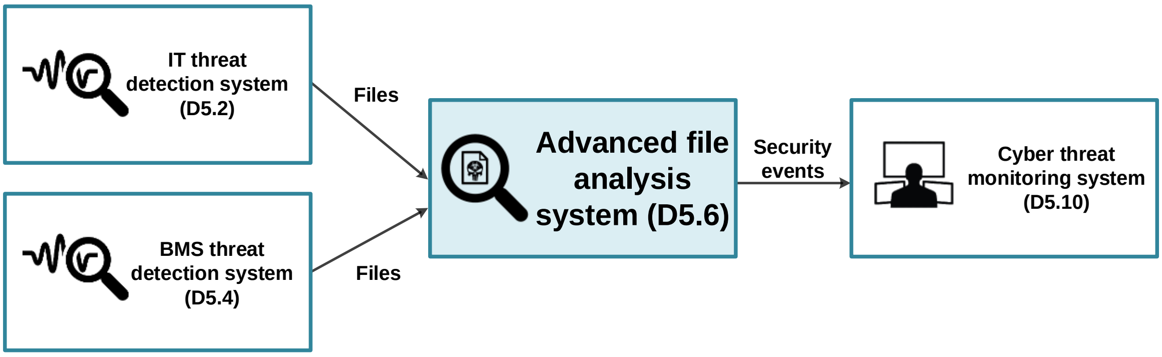

IT threat detection system (D5.2)
BMS threat detection system (D5.4)
Files
Files
Advanced file analysis system (D5.6)
Security events
Cyber threat monitoring system (D5.10)

Figure 16: Interconnections of the advanced file analysis system

It is interconnected to the ITTDS and the BTDS to receive the files that transit respectively through the IT and BMS networks and analyse them, as shown in Figure 16.

It 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 security risk level is sent to the cyber threat monitoring system through security events that also contain file metadata.

2.2.9 E-Health device security analytics

The EDSA solution offers security analytics and monitoring of medical devices and their environment. Thereby it addresses a blind spot in security monitoring in hospital environments and reducing cybersecurity risk stemming from medical devices and medical device infrastructures.

The security analytics solution extends security log data collection from medical devices, enables analytics to derive meaningful security data, and generates security insights, aggregated statistics and alerts upon detecting anomalous or suspicious security events. All of this is done in a way that does not interfere with the clinical function of the medical device.

The solution is powered by a security data warehouse and analytics platform on which security alerting models are developed and deployed. Alerting models include models to detect medical device security misconfiguration vulnerabilities and compliance issues, user behavior anomalies related to medical device use, and threats from the medical device (network) environment.

When these models identify potential security threats in the analyzed data, alerts are generated and routed to relevant parties for remediation as represented in Figure 17. Alerts related to vulnerabilities or threats in the operational environment of the medical device go to the hospital CTMS and alerts related to security controls of the medical device go to the vendor service dashboard. Furthermore, aggregated security insights are sent to the e-health device security risk management model to support data-driven and quantitative product security risk management.

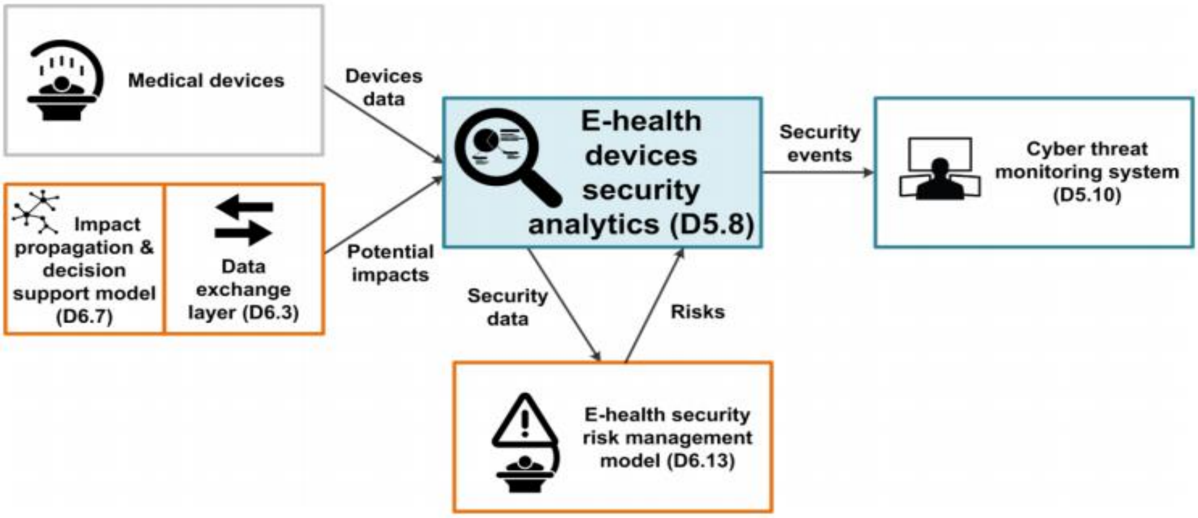

Medical devices
Devices data
E-health devices security analytics (D5.8)
Security events
Cyber threat monitoring system (D5.10)
Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Security data
Risks
E-health security risk management model (D6.13)

Figure 17: Interconnections of the e-health devices security analytics

2.2.10 Cyber threat monitoring system

The CTMS is a solution that collects and centralizes cyber security events. It displays the information in an organized way and provides user-friendly interfaces to Security Operations Center (SOC) analysts so that they can analyse and visualise threats and impacted assets.

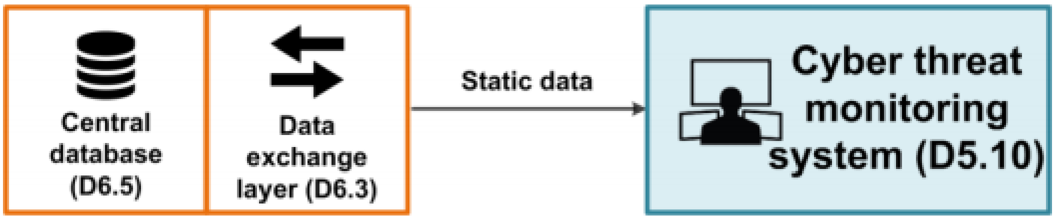

Central database (D6.5)
Data exchange layer (D6.3)
Static data
Cyber threat monitoring system (D5.10)

Figure 18: 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 CDB.

The CTMS retrieves the static data from the central database through the DXL, as illustrated in Figure 18. The CTMS receives security events from the following systems:

- The ITTDS;
- The BTDS;
- The AFAS;
- And the EDSA.

Rules are implemented within the CTMS to automatically generate alerts from the received security events. The 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, SOC operators must confirm the alerts as either incidents or false-positive alerts.

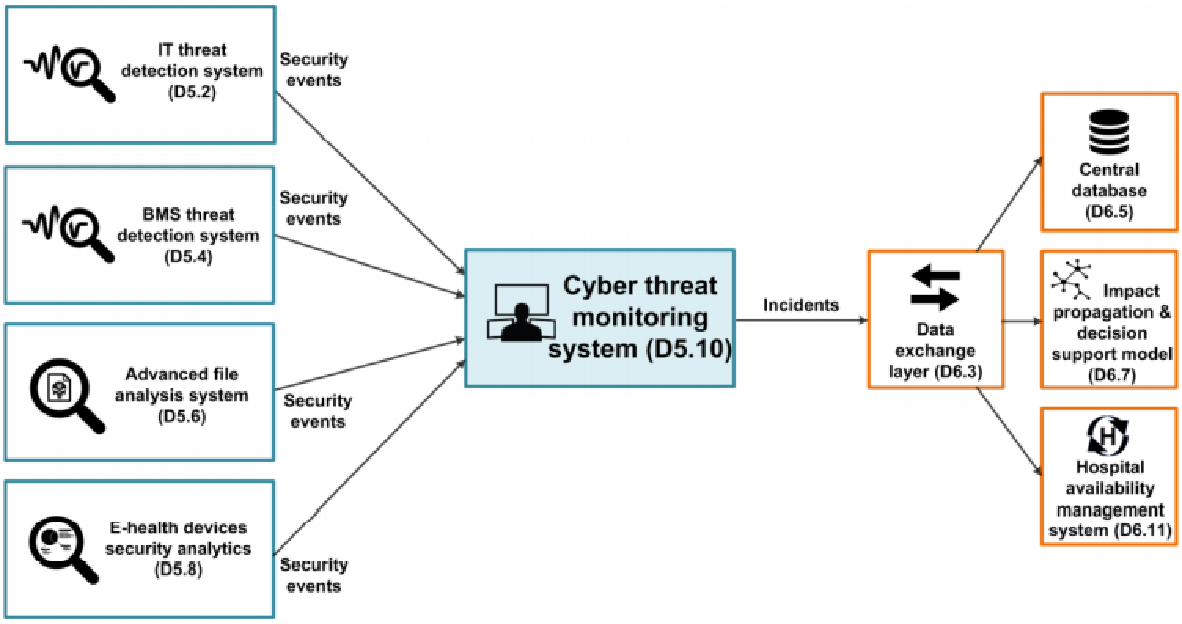

IT threat detection system (D5.2)
Security events
BMS threat detection system (D5.4)
Security events
Advanced file analysis system (D5.6)
Security events
E-health devices security analytics (D5.8)
Security events
Cyber threat monitoring system (D5.10)
Incidents
Data exchange layer (D6.3)
Central database (D6.5)
Impact propagation & decision support model (D6.7)
Hospital availability management system (D6.11)

Figure 19: Interconnections of the cyber threat monitoring system

In case of incidents, as illustrated in Figure 19, the incidents are forwarded through the DXL to the following systems:

- The CDB;
- The IPDSM;
- And the HAMS.

The CTMS also 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.

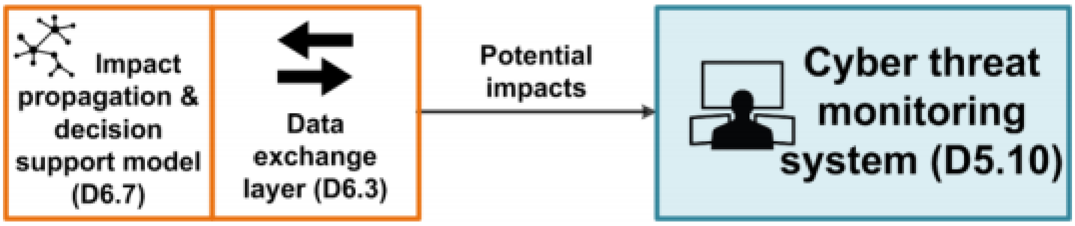

Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Cyber threat monitoring system (D5.10)

Figure 20: Cyber threat monitoring system receiving potential impacts

As illustrated in Figure 20, the computed impacts, which are provided by the IPDSM, are received by the CTMS to allow SOC operators to take into account combinations of both physical and cyber incidents and visualize potential cascading effects.

2.2.11 Data exchange layer

The DXL implements publish-subscribe mechanisms in order to trigger notifications to the other components when new physical and cyber incident (coming from the BTMS and the CTMS) or new impacts (coming from the IPDSM) are sent. The DXL was developed in order to store and extract data from the CDB (e.g. web services). It allows to 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 DXL also allows other project components to extract added-value information on demand from the CDB.

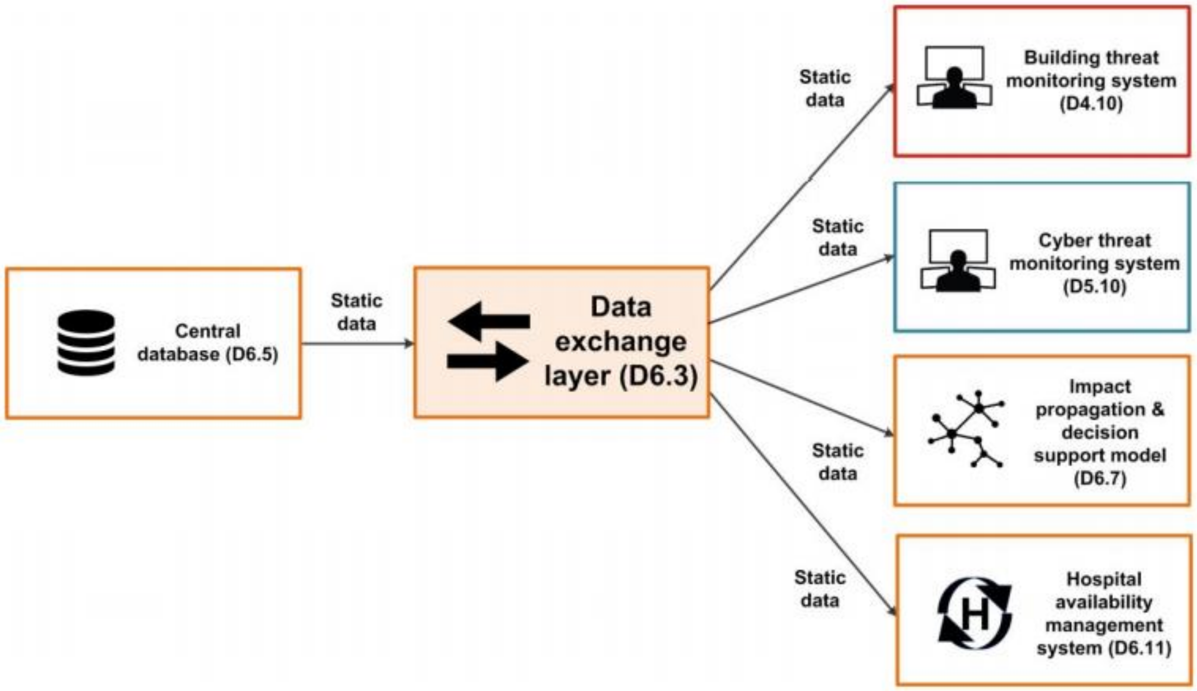

Central database (D6.5)
Static data
Data exchange layer (D6.3)
Static data
Building threat monitoring system (D4.10)
Static data
Cyber threat monitoring system (D5.10)
Static data
Impact propagation & decision support model (D6.7)
Static data
Hospital availability management system (D6.11)

Figure 21: Data exchange layer forwarding static data

As illustrated in Figure 21, the BTMS, the CTMS, the IPDSM and the HAMS get static data from the CDB through the DXL.

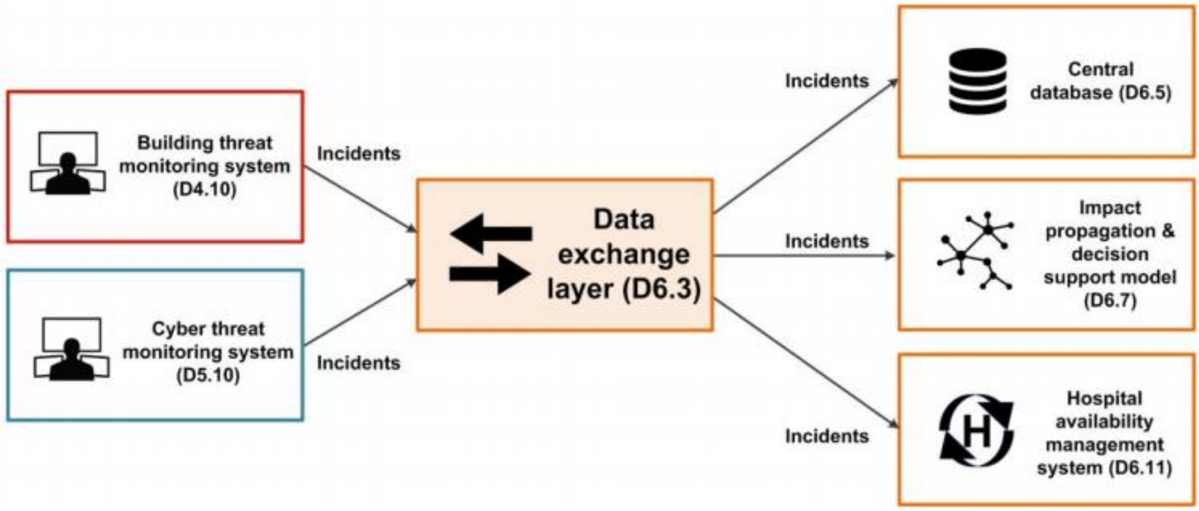

Building threat monitoring system (D4.10)
Incidents
Cyber threat monitoring system (D5.10)
Incidents
Data exchange layer (D6.3)
Incidents
Central database (D6.5)
Incidents
Impact propagation & decision support model (D6.7)
Incidents
Hospital availability management system (D6.11)

Figure 22: Data exchange layer forwarding incidents

As illustrated in Figure 22, the DXL forwards incidents from the BTMS and the CTMS to the CDB, the IPDSM and the HAMS.

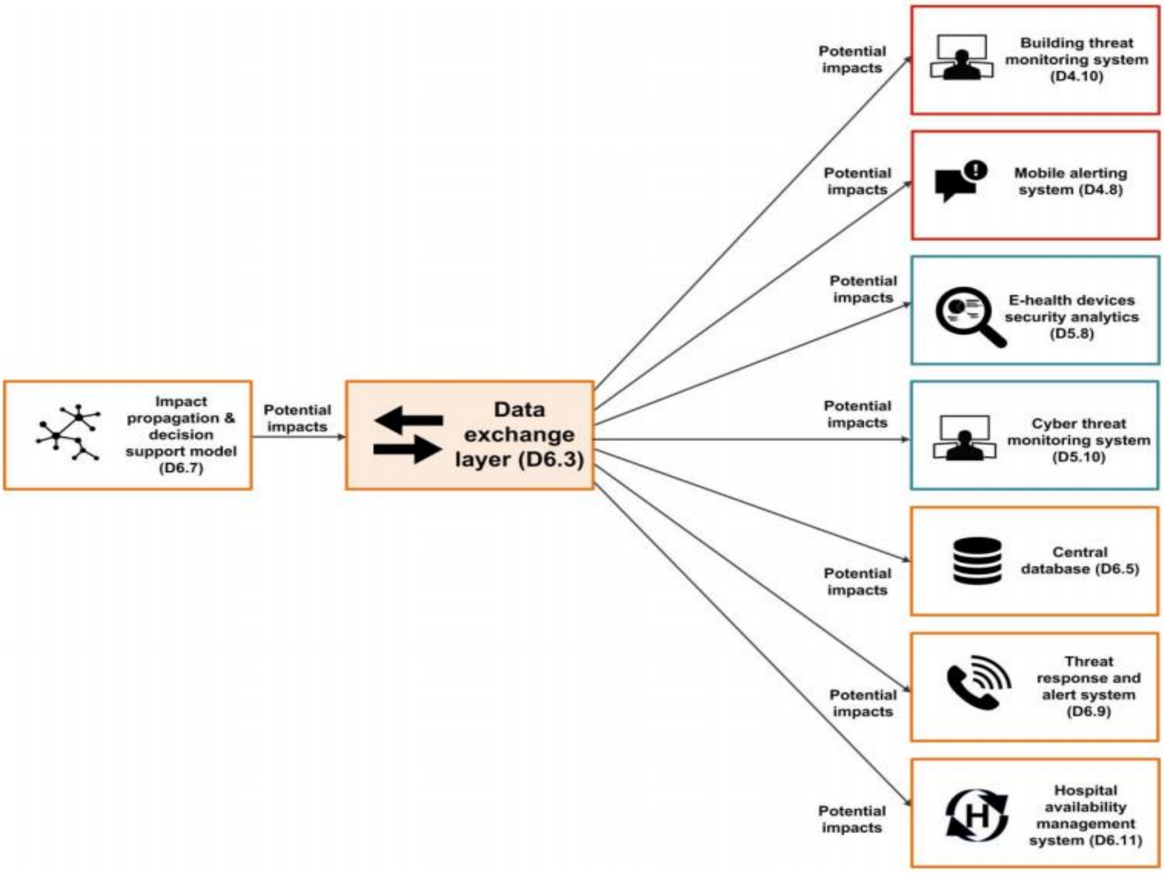

Impact propagation & decision support model (D6.7)
Potential impacts
Data exchange layer (D6.3)
Potential impacts
Building threat monitoring system (D4.10)
Potential impacts
Mobile alerting system (D4.8)
Potential impacts
E-health devices security analytics (D5.8)
Potential impacts
Cyber threat monitoring system (D5.10)
Potential impacts
Central database (D6.5)
Potential impacts
Threat response and alert system (D6.9)
Potential impacts
Hospital availability management system (D6.11)

Figure 23: Data exchange layer forwarding potential impacts

As illustrated in Figure 23, the DXL forwards potential impacts from the IPDSM to the BTMS, the MAS, the EDSA, the CTMS, the CDB, the TRAS and the HAMS.

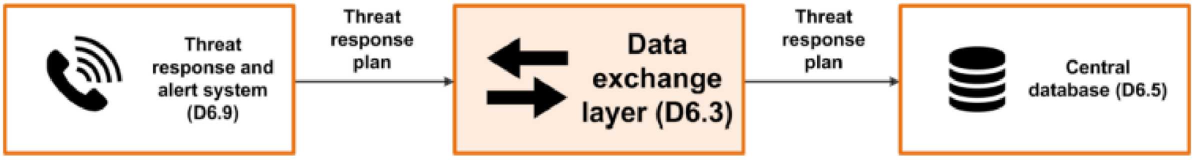

Threat response and alert system (D6.9)
Threat response plan
Data exchange layer (D6.3)
Threat response plan
Central database (D6.5)

Figure 24: Data exchange layer forwarding threat response plan

As illustrated in Figure 24, the DXL forwards threat response plans from the TRAS to the CDB.

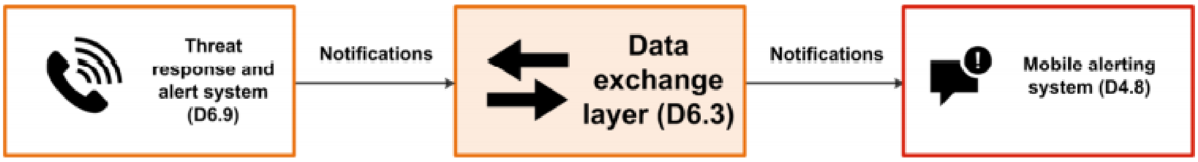

Threat response and alert system (D6.9)
Notifications
Data exchange layer (D6.3)
Notifications
Mobile alerting system (D4.8)

Figure 25: Data exchange layer forwarding notifications

As illustrated in Figure 25, the DXL forwards notifications from the TRAS to the MAS.

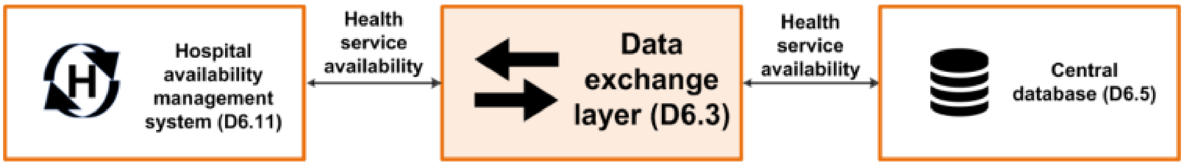

Hospital availability management system (D6.11)
Health service availability
Data exchange layer (D6.3)
Health service availability
Central database (D6.5)

Figure 26: Data exchange layer forwarding health service availability

As illustrated in Figure 26, the DXL forwards health service availability from the HAMS to the CDB.

2.2.12 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 takes into account confidentiality, ethics and privacy constraints. For instance, personal data is not be mixed with equipment statuses. The CDB includes both a static and a dynamic data store, as illustrated in Figure 27 and Figure 28.

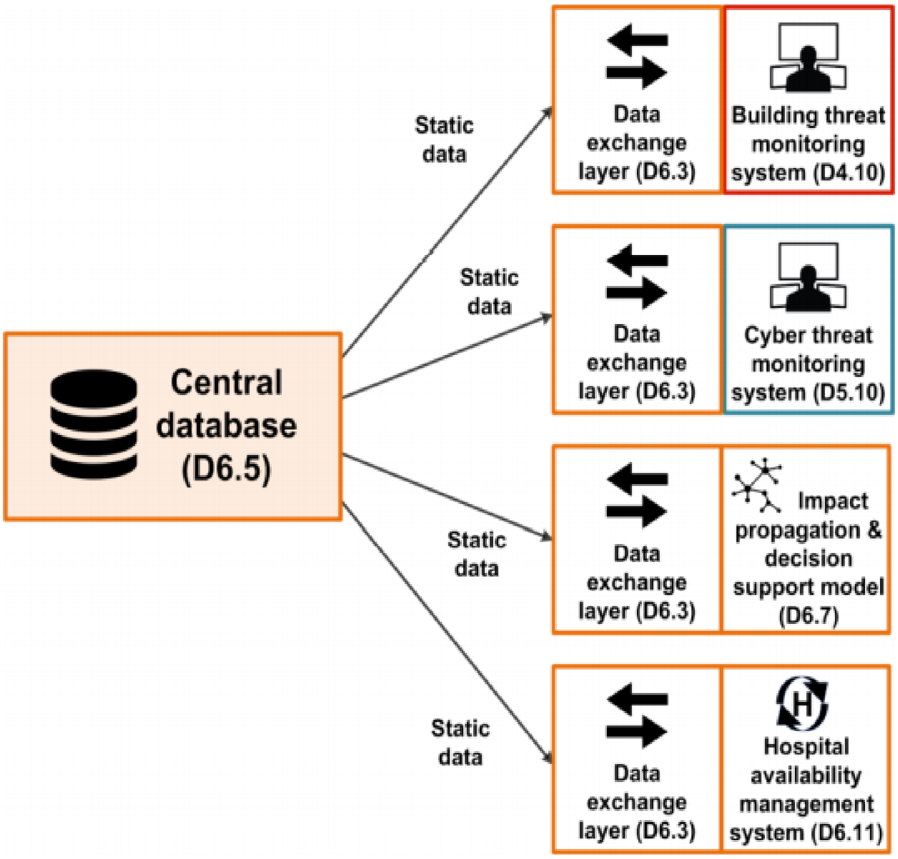

Central database (D6.5)
Static data
Static data
Static data
Static data
Data exchange layer (D6.3)
Building threat monitoring system (D4.10)
Data exchange layer (D6.3)
Cyber threat monitoring system (D5.10)
Data exchange layer (D6.3)
Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Hospital availability management system (D6.11)

Figure 27: Central database providing static data

The CDB provides static data to the BTMS, the CTMS, the IPDSM and the HAMS.

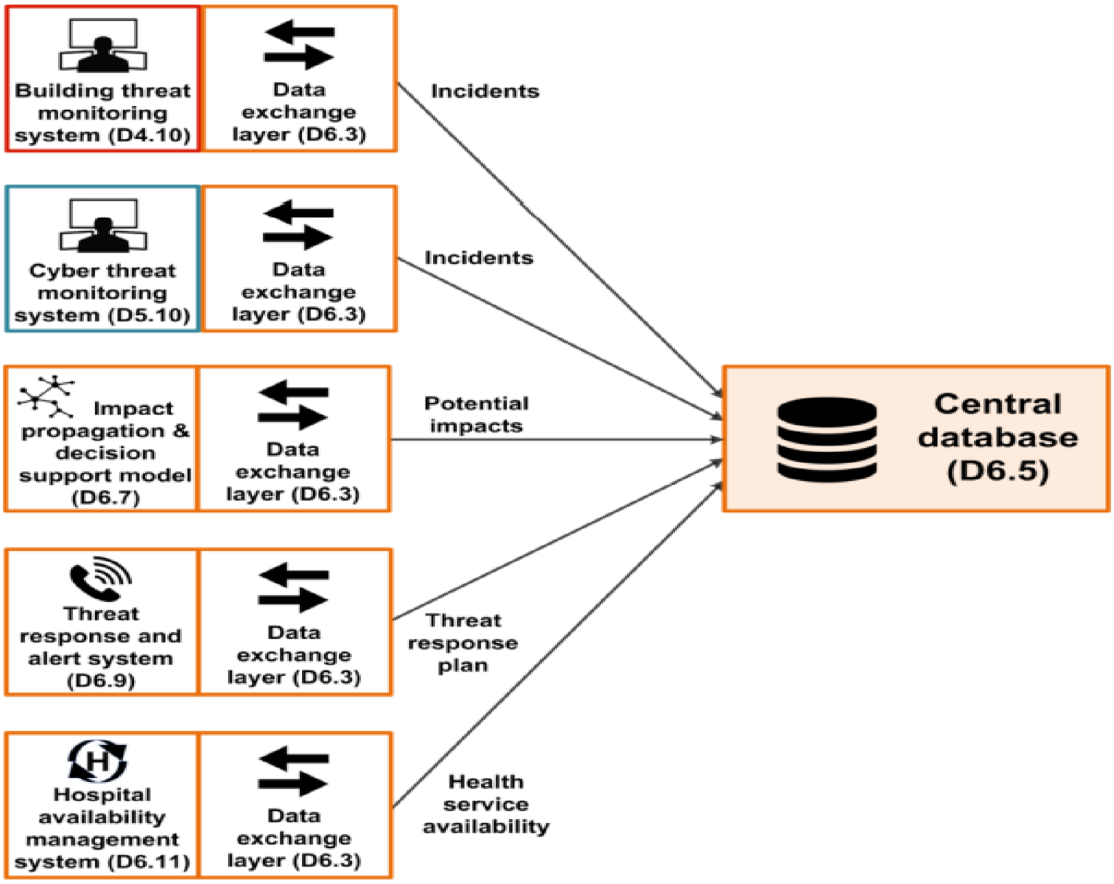

Building threat monitoring system (D4.10)
Data exchange layer (D6.3)
Incidents
Cyber threat monitoring system (D5.10)
Data exchange layer (D6.3)
Incidents
Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Central database (D6.5)
Threat response and alert system (D6.9)
Data exchange layer (D6.3)
Threat response plan
Hospital availability management system (D6.11)
Data exchange layer (D6.3)
Health service availability

Figure 28: Central database storing dynamic data

The BTMS, the CTMS, the IPDSM, the TRAS and the HAMS store dynamic data into the CDB.

2.2.13 Impact propagation and decision support model

The objectives of the IPDSM are to:

- 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 reason about incidents and their potential impacts, the IPDSM needs to hold knowledge about physical and cyber assets that are prone to attacks.

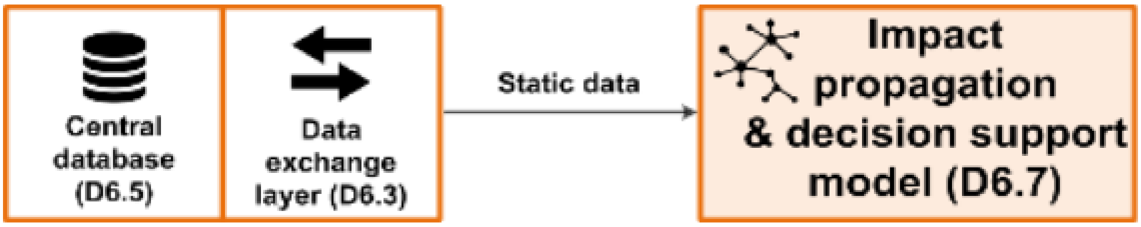

Central database (D6.5)
Data exchange layer (D6.3)
Static data
Impact propagation & decision support model (D6.7)

Figure 29: Static mode communication for IPDSM

To achieve its objective, the IPDMS embeds within it an ontology, propagation rules, a reasoner, and an impact score calculator. The ontology captures all knowledge useful for the computation of impact propagation: intrinsic and contextual knowledge about all the inventoried healthcare assets whether physical or cyber (buildings, medical devices, IT services, software, hardware, IT facilities, medical devices, etc.), their interconnections, potential attacks to which they may be prone and possible protections mitigating them.

Propagation rules capture security expert knowledge about how to infer and propagate impacts. They are subject to a continuous evolution. They are supplied to the reasoner that has in charge to compute potential impacts when an incident on an asset occurs. The severity of the potential impacts are evaluated thanks to the impact score calculator.

As illustrated in Figure 29, information about assets is sent by the structures such as hospitals and health services, to the CDB to inform the system about changes affecting the assets they hold (new assets or changes on existing ones). The IPDSM, on the other hand, regularly queries the CDB, throughout the DXL to get knowledge about the assets and this is done in a static way.

As shown in Figure 30, incidents are pushed dynamically to the IPDSM through the DXL. 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, 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.

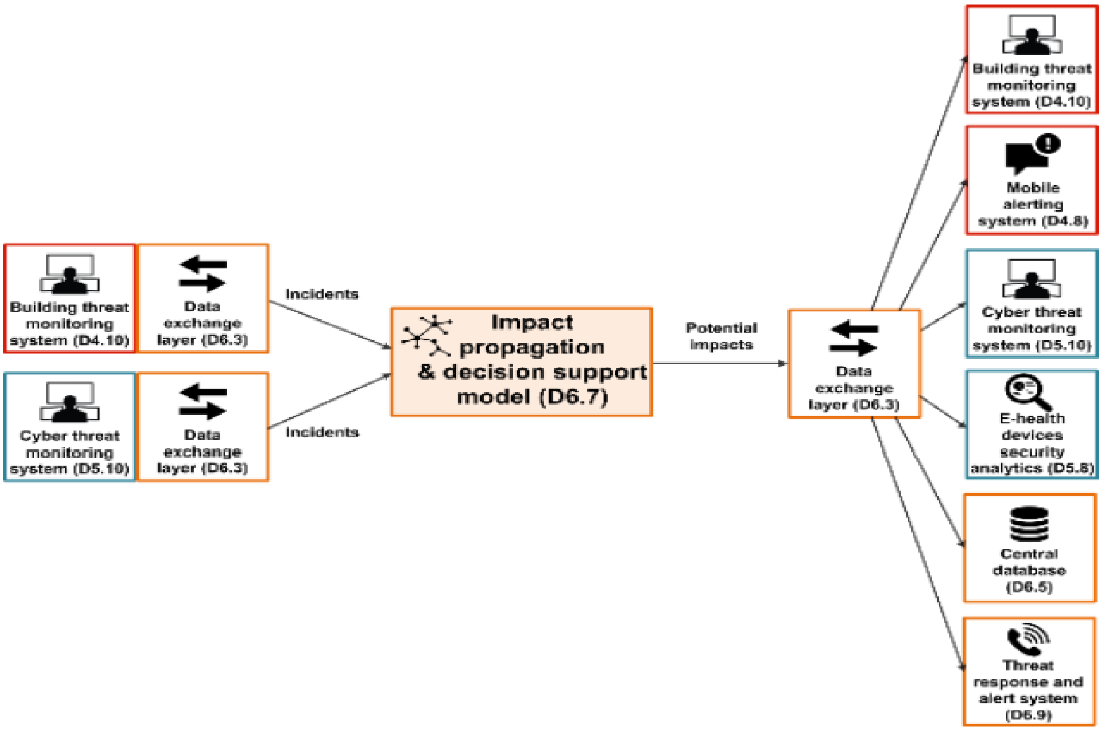

Building threat monitoring system (D4.10)
Data exchange layer (D6.3)
Cyber threat monitoring system (D5.10)
Data exchange layer (D6.3)
Incidents
Incidents
Impact propagation & decision support model (D6.7)
Potential impacts
Data exchange layer (D6.3)
Building threat monitoring system (D4.10)
Mobile alerting system (D4.8)
Cyber threat monitoring system (D5.10)
E-health devices security analytics (D5.8)
Central database (D6.5)
Threat response and alert system (D6.9)

Figure 30: Interconnections of impact propagation and decision support model

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

2.2.14 Threat response and alert system

The TRAS is in charge with sending alerts and notification upon impact reception from the IPDSM. The objective is to enable a fast response time in anticipation since the impact propagation model is using prediction. This will allow alerted stakeholder to quickly assess a situation and set in motion the appropriate action to avoid or mitigate a risk. The solution supports different media types to ensure it can reach the right stakeholder at the right time, and this includes SMS, voice call, emails as well as direct notification within the MAS.

This module is connected to the other components as detailed in Figure 31.

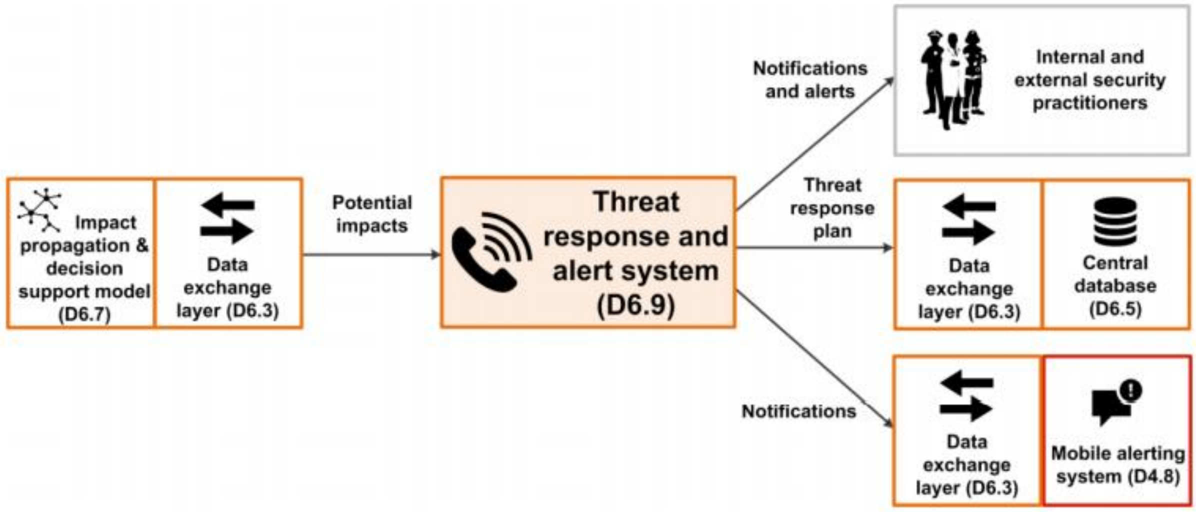

Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Threat response and alert system (D6.9)
Notifications and alerts
Internal and external security practitioners
Threat response plan
Data exchange layer (D6.3)
Central database (D6.5)
Notifications
Data exchange layer (D6.3)
Mobile alerting system (D4.8)

Figure 31: Interconnections of the threat response and alert system

The module will implement the reaction plans as specified by each user, in answer to the scenario to be taken into account.

There is not necessarily a direct correlation between scenarios and reaction plans. Users will be able to adapt the reaction plan details based on their own organization and maturity in terms of risk management organization. By receiving impacts from the IPDSM, they will be able to set their own threshold when they wish to take action, allowing a fine tuning, swift reaction to be adjusted against the risk of false alarm.

The alerting details, i.e. who has been contacted, when, and their respective answer is pushed back to the central database for further exploitation and return on operating experience.

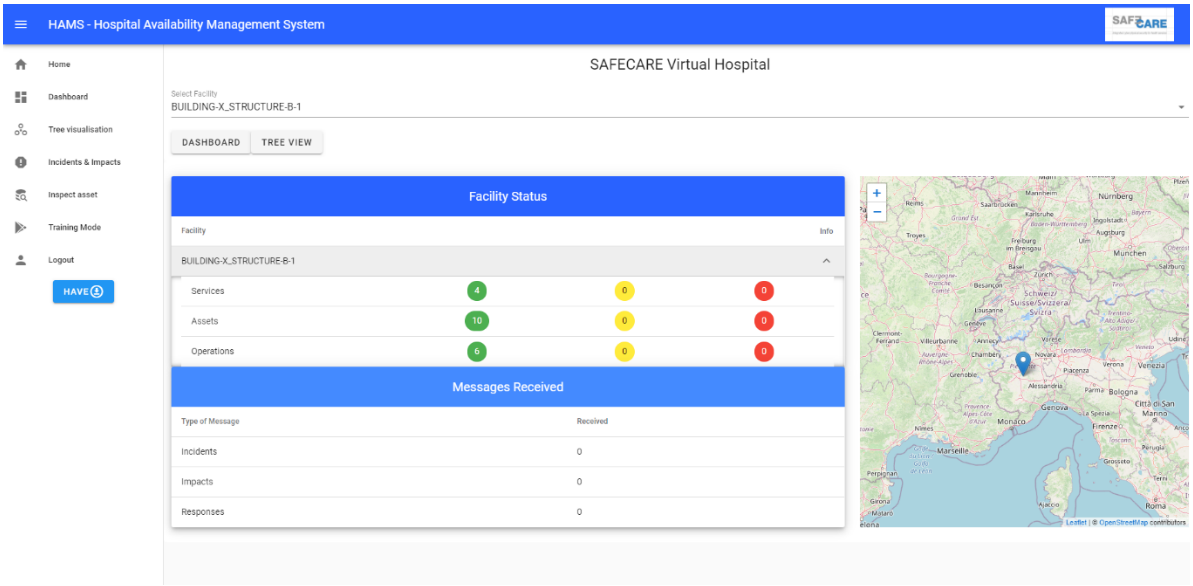
2.2.15 Hospital availability management system

The HAMS is a module of SAFECARE in charge of managing hospital status, asset and resource availability, and visualize the different messages received from the other modules. The HAMS has been designed to help emergency managers, health practitioners and security staff to manage hospital assets in case of normal operation or during emergencies or incidents. Indeed, the HAMS is able to integrate inputs from the incident detection systems to update resource and asset availability after cyber and/or physical incidents. Through the IPDSM, the SAFECARE solution is able to evaluate potential cascading effects of an incident. The HAMS can visualize these impacts through a graph-based interface, giving the opportunity to users to inspect incidents and understand which can be the potentially impacted assets.

To support the usability of such tool, the HAMS also implement a training mode, useful to learn what type of information it can provide, how data are visualized and what is the HAMS behaviour. This section reports an overview of this tool; a complete description is provided into deliverable D6.11[1].

The HAMS has been developed as a typical web application, and it is therefore composed by a server and a web interface. Starting from a facility level, the HAMS provides information about the status of services and operations. In this terminology, services include hospital departments and a list of medical devices belonging to each service. On the other side, operations include all the systems that are not related to the medical activities but essential for the hospital's correct operation. The HAMS interface is divided into four main views: homepage, dashboard, tree view and incidents & impacts view.

After the authentication page, the HAMS home page is visualized (Figure 32), providing an overview of the hospital facilities, with a summary of the availability status of the different services, assets, and operations, according to their status and color code. Furthermore, there is a table with a summary of the messages received, divided by incident, impact, and response messages.



Select Facility
BUILDING-X_STRUCTURE-B-1

Facility Status

Facility			Info
BUILDING-X_STRUCTURE-B-1			
Services	4	0	0
Assets	10	0	0
Operations	6	0	0

Messages Received

Type of Message	Received
Incidents	0
Impacts	0
Responses	0

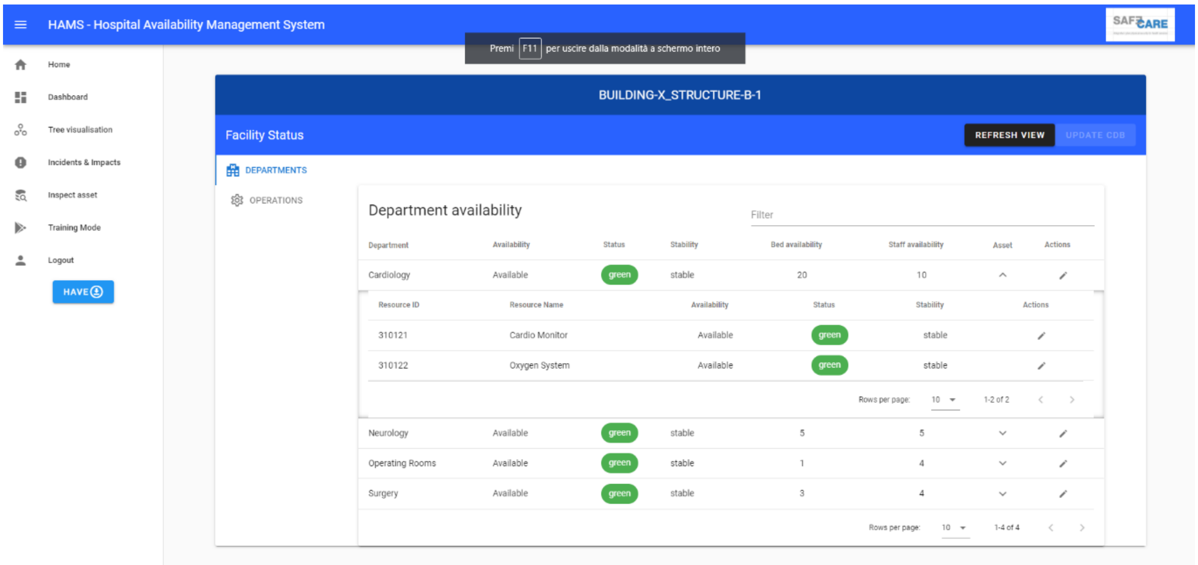
Figure 32: Homepage

The user can also select a specific facility from this page to obtain detailed information in the following Dashboard and Tree View. Upon choosing a facility, its position is shown in the map

[1] SAFECARE project D6.11: Hospital Availability Management System

widget on the page. The map can be useful in particular for hospitals that are composed of several buildings distributed in a region.

The dashboard view (Figure 33) shows the availability status of services, assets, and operations in a tabular way. Services and assets are grouped under the "Departments" tab, while operations are grouped under the "Operations" tab. Beyond availability status, the department view also shows the number of available beds and staff for each department. In both tabs, availability values can be modified manually by authorized users (for example, when an incident is closed, and the hospital original status is restored).



Department availability

Department	Availability	Status	Stability	Bed availability	Staff availability	Asset	Actions
Cardiology	Available	green	stable	20	10	^	✎
Neurology	Available	green	stable	5	5	˅	✎
Operating Rooms	Available	green	stable	1	4	˅	✎
Surgery	Available	green	stable	3	4	˅	✎

Rows per page: 10 1-4 of 4

Resource ID	Resource Name	Availability	Status	Stability	Actions
310121	Cardio Monitor	Available	green	stable	✎
310122	Oxygen System	Available	green	stable	✎

Rows per page: 10 1-2 of 2

Figure 33: Dashboard

The status of services, assets, and operations can also be displayed using a tree view (Figure 34), exploiting the intrinsic hierarchical structure of the different assets in a hospital complex. Each node of the graph reports the asset's status. For example, if a node (an asset) is involved in an incident (directly or through impact propagation) that node will be highlighted by yellow or orange color and the user, clicking on it, will see details about the last incident or impact that caused the changes in the asset status.

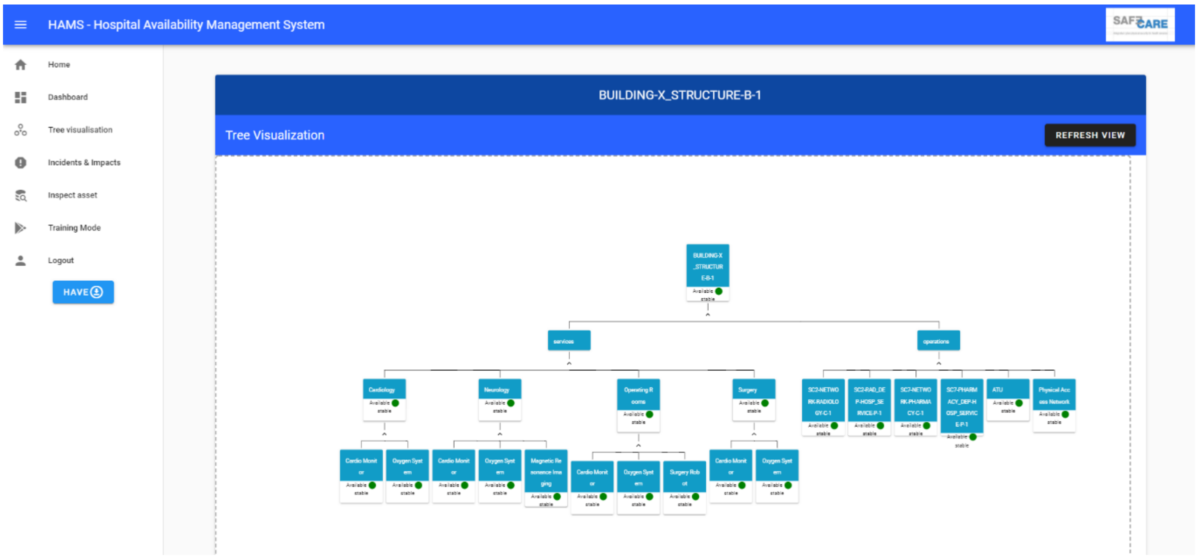


Figure 34: Tree View

When an incident occurs and the corresponding impact is generated, the SAFECARE systems send messages through the DXL. The HAMS receives these messages and populates its interfaces accordingly, updating the status of assets involved if needed.

Beside the views described above, that are asset-centric, the HAMS implement a view devoted to incident analysis. Through the incidents & impacts view, the HAMS provides detailed information about incidents, impacts and response reports. Users can visualize the main field directly and inspect whole JSON messages through a popup. Impact messages are also visualized as graphs. The graph displays assets involved and the relations among each asset, highlighting which are the assets with the highest *impact score* value. Figure 35 provides an example of a graph representation. In this case, the graph representation includes all the assets in a hospital, even if they are not impacted.

The number of assets visualized can be managed by the filter functions implemented.

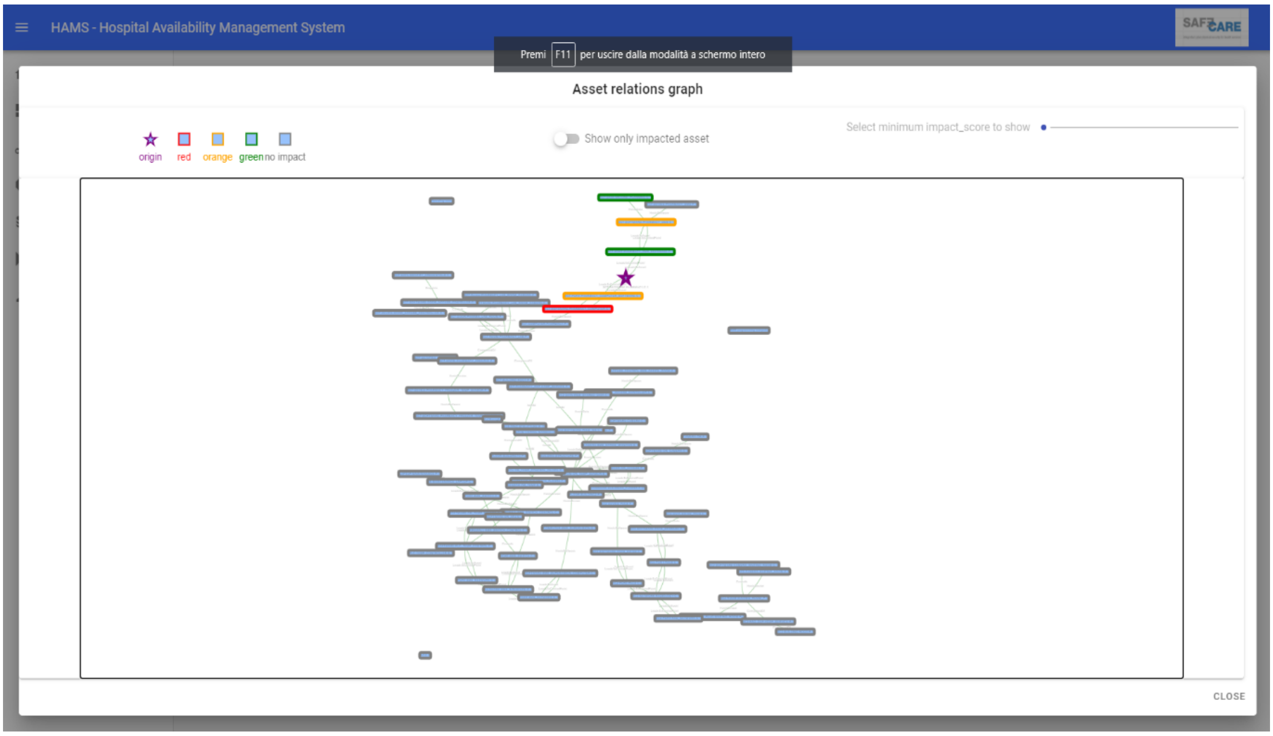
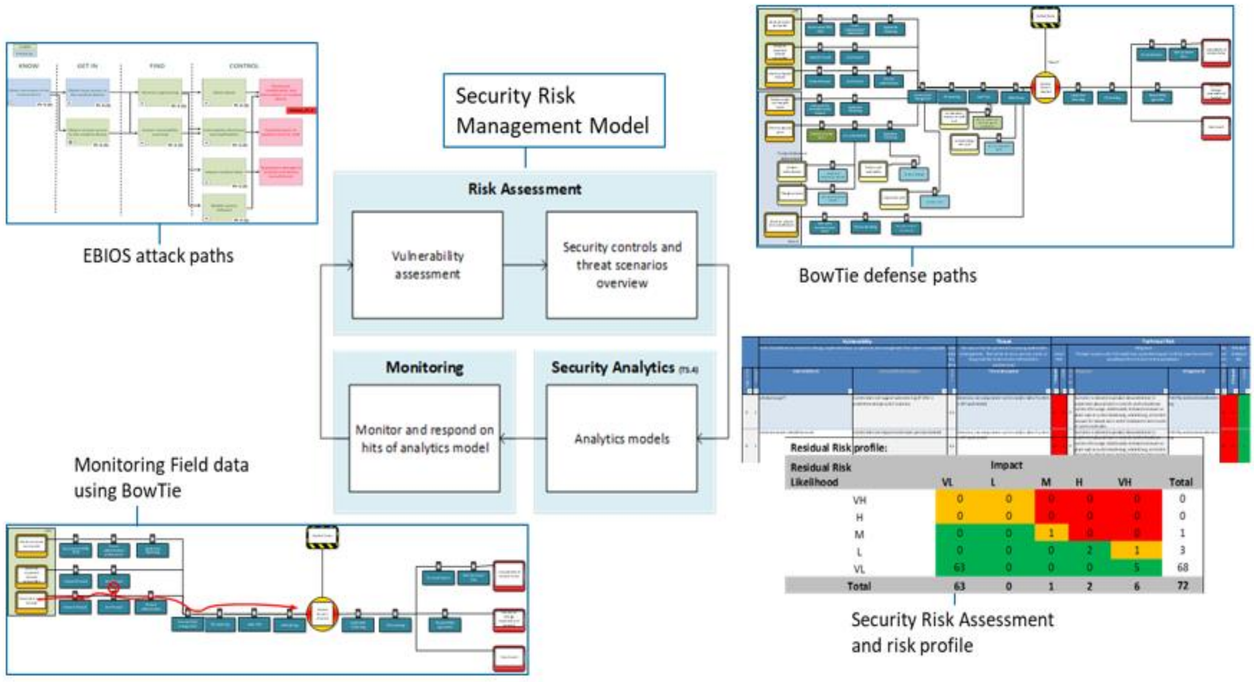

HAMS - Hospital Availability Management System
Premi F11 per uscire dalla modalità a schermo intero
Asset relations graph
origin
red
orange
green
no impact
Show only impacted asset
Select minimum impact_score to show
CLOSE

Figure 35: HAMS Impact graph

2.2.16 E-health security risk management model

The E-Health security Risk Management Model is developed to support the risk assessment process by quantifying security risks. The model can be used by health system manufactures and hospitals to identify risk sources, security events, vulnerabilities, threats and the related security controls.

The E-Health security Risk Management Model provides a stepwise iterative approach to calculate the Risk level and define risk mitigations. By combining three methodologies/tools (EBIOS, BowTie and Security Risk assessment template), different complimentary views on a health system in scope of an assessment are visualized. EBIOS shows the underpinning of the likelihood of an event the BowTie diagrams show the possible impact and related security controls with their vulnerabilities. In the Security Risk Assessment template, the risk levels are quantified by combining the likelihood and impact. This results in a security profile of the assessed health system. The Health system and the related security profile needs to be validated based on field data. The EDSA and monitoring processes are used to measure and optimize the effectiveness of the security controls of the system.


Security Risk Management Model
Risk Assessment
Vulnerability assessment
Security controls and threat scenarios overview
Monitoring
Monitor and respond on hits of analytics model
Security Analytics (T5.4)
Analytics models
EBIOS attack paths
BowTie defense paths
Monitoring Field data using BowTie
Security Risk Assessment and risk profile
KNOW
GET IN
FIND
CONTROL

Residual Risk profile:

Residual Risk Likelihood	Impact VL	L	M	H	VH	Total
VH	0	0	0	0	0	0
H	0	0	0	0	0	0
M	0	0	1	0	0	1
L	0	0	0	2	1	3
VL	63	0	0	0	5	68
Total	63	0	1	2	6	72

Figure 36: Security Risk Management Model and the supporting elements

3. End users' expected benefits from the future use of SAFECARE

The framework approach adopted to present the end users' expected benefits from the future use of SAFECARE is the SONCAS methodology. SONCAS is a French acronym standing for *Sécurité* (security), *Orgueil* (pride), *Nouveauté* (innovation), *Comfort* (comfort), Argent (money) and *Sympathie* (sympathy). Those 6 items represent the motivation categories spectrum of a customer. In other words, the motivation of a customer for solving their issue can be broken down into one or several components corresponding to those categories. Importantly, this methodology also allows extending the items representing the customer's motivation categories spectrum, as it has been done in Table 3.5 SAFECARE benefits to also include *Environnement* (environment) as a potential purchase motivation.

With the aim of presenting the end-users' expected benefits from the future use of SAFECARE, this section presents the characteristics of the SAFECARE global solution (general information, modules and scenarios that the solution will be tested), its advantages (coming from its characteristics) and its benefits (coming from its advantages). Finally, once the main benefits identified, each of them is translated into one or more purchasing motivations for the end users.

SAFECARE aims to provide a solution that will enhance threat prevention, threat detection, incident response and mitigation of impacts, as well as improve physical and cyber security in healthcare organizations, in a seamless and cost-effective way. The following Table (Table 3.1) presents the main characteristics of the SAFECARE global solution. More specifically, it is a turnkey solution, dedicated to healthcare, hospitals, and sensitive infrastructures. The core system is made of many different tools with different functionalities, it can detect mixed (cyber and physical) attacks and it is equipped with a platform which consolidates alerts and incidents.

The figure below presents the SFECARE technical characteristics.

SAFECARE technical characteristics
Detect mixed attacks (Physical and Cyber)
Solution dedicated to healthcare, hospitals, sensitive infrastructures
Turnkey solution
SaaS Mode
Compatibility with all kinds of environment
Redundant and equipped with many different alerts
Core system is made of many different tools with different functionalities
with pre-installed alerts and alarms
The solution is redundant and able to face power cut
Ability to detect thin and spread threats, with reporting tools
Detect Malwares, Ransomwares etc.

Equipped with a platform which consolidates alerts and incidents

Table 3.1 SAFECARE general information

In doing this, and as analysed in Section 2, physical, cyber and integrated solutions have been implemented in an integrated way and in Table 3.2, SAFECARE modules are presented.

SAFECARE modules
Suspicious behaviour detection system (SBDS)
Intrusion and fire detection system (IFDS)
Data collection system (DCS)
Mobile alerting system (MAS)
Building threat monitoring system (BTMS)
IT threat detection system (ITTDS)
BMS threat detection system (BMS TDS)
Advanced file analysis system (AFAS)
E health devices security analytics (EDSA)
Cyber threat monitoring system (CTMS)
Data Exchange Layer (DXL)
Central Database (CDB)
Impact Propagation and Decision Support Module (IPDSM)
Threat Response and Alert System (TRAS)
Hospital Availability Management System (HAMS)
E Health Security Risk Management Model

Table 3.2 SAFECARE modules

The SAFECARE solutions were tested, validated and demonstrated in the hospitals of Marseille, Turin and Amsterdam, based on the following cyber-physical scenarios.

SAFECARE scenarios
Prevent Cyber-physical attack targeting power supply of the hospital.
Prevent Cyber-physical attack to steal patient data in the hospital.
Prevent Cyber-physical attack targeting the population, IT systems and medical devices in the hospital, and patient data base.
Prevent Cyber-physical attack targeting the air-cooling system of the hospital.
Prevent shooting, explosive or sabotage in critical places (visible or invisible).
Theft at hospital equipment, access to hospital network and IT systems.
IOT medical wearable devices (outside / inside).
Distributed management over distributed buildings, considering external stakeholders (e.g., pharmacy, outpatients).
Physical attack against hospital staff using a gun.
Cyber-physical attack to block national crisis management.

Table 3.3 SAFECARE scenarios

Based on the characteristics of the SAFECARE global solution (general information, modules and scenarios that the solution will be tested), as presented above, the end-users participating to the project have been asked to identify its advantages, which are presented in Table 3.4.

SAFECARE advantages
Protects hospital from emerging physical and cyber threats.
Functional and long-term efficient solution.
Professional tool dedicated to health care and medical infrastructures.
Turnkey solution.
No set up additional cost, no additional equipment is required.
Adjustable and suitable for every type of health infrastructure.
Strong and resilient to attacks.
Support the detection of false vs true alert.
Can create alerts 24-7, and can automatically report alerts to targeted teams.
Efficient solution, able to switch in case of a lockdown.
Solution equipped with multi-intelligent engines, able to detect all kind of attacks that humans could not or have difficultness.
Solution that gathers and analyses all information on a single interactive and centralized platform
Solution able to create advanced calculations.
Modular solution that could be connected for example, to fires detection systems, able to listen and detect specific behaviors.
Solution that detects physical intrusions and correlates that information with anomalies coming from other information systems.
Solution that maintains up to date security and threat information, report alerts specifying the localization.
Tool that mitigates risks in several secured areas.
Tool that reports on mobiles of selected internal or external stakeholders.
Tool that is constantly updated from new threats and attacks.
Tool able to analyse, detect and distinguish malicious files, from non-malicious files.
Tool with several databases centralizing information from the different modules.
Tool that is capable to model the impacts a defect can have at a specific location, combined with another one at another specific location. The alert is graduated in terms of severity, estimated impact for the establishment.

Tool that provides information on the status and availability of the platforms (Back end & Front end).
Tool that detects and thus protects you from attacks, even when the establishment's electrical installations are powered off / threatened.
Tool that detects and thus protects you from intrusions, denial of services, attacks of all kinds to digital health databases.
Tool that detects and thus protects you from intrusions, denial of services, attacks of all kinds targeted on biomedical devices.
Tool that detects and secures attacks on critical equipment.
Tool that detects and thus limits the side effects of an explosion, sabotage that took place in a critical place.
Tool that detects and thus limits damage to attacks on equipment, access disruptions, on IS.
Tool that detects and limits damage to intrusions via "IoT".
Tool that detects and limits intrusions, theft, replacement of health products, and limits their damage.
Tool that protects, limits damage from attacks targeted on seizure cells.
Tool that enhances communication of internal and external stakeholders, through relevant information exchange on a timely, accurate and precise manner.
Tool that provides a common ground and situational awareness among internal and external stakeholders involved in crisis management process, thus enhancing the process of efficient decision making and cooperation.

Table 3.4 SAFECARE advantages

In similar lines, and based on the pre-defined advantages, the end-users identified the benefits of the SAFECARE global solution. Finally, once the main benefits identified, each of them is translated into one or more purchasing motivations for the end users, as illustrated in Table 3.5 SAFECARE benefits.

Benefits	Possible realistic capitalization and expectations at the end of the project	Expectations beyond the end of the project	Purchase motivation (SONCASE)
SAFECARE is the unique tool that protects healthcare infrastructures from modern physical and cyber-attacks. Moreover, the tool is constantly updated from new upcoming threats.	Only one solution to detect and prevent all kind of threats, updates are available against new threats.	Automatic updates and after-sale services are available for many years after purchase.	Confort, la security, pride, novelty

There is no longer the need to find separate solutions to enhance healthcare infrastructures' physical and cyber resilience. SAFECARE detects both type of threats and therefore helps to protect the infrastructure.	Infrastructure is protected against all hazards.	Infrastructure is protected against new/emerging threats, at long term.	Security, confort
The solution was developed by top-level security experts (computer scientists, statisticians, risk and security managers, healthcare professionals, first responders).	The solution is reliable and well-conceived as it is made by European Experts.	Expertise and methodologies delivered by European workforce and experts to detect centralize and cover the large panel of risks is useful, pertinent, cost-effective and will not be outdated.	Pride
The unique tool on the market to provide a turnkey solution specifically dedicated to healthcare infrastructure security.	To have a turnkey solution tailor made to healthcare infrastructures.	The solution remains the best, most famous, acknowledged and reliable solution for healthcare institutions on the market.	Confort, novelty
The tool does not require any supplementary equipment purchases. It can be integrated into the infrastructure without supplementary integration costs.	No additional cost to settle the solution.	No additional cost after the solution is settled or after a strategic move or change from the end user's company or organization.	Money, Environment
The tool can be installed on any type of infrastructure (single building, multi-building, single area, multi-area).	Adaptability and compatibility to all the infrastructure.	The investment is compatible and free of charges with end-users change orientation and long terms reorientations.	Money, environment
The solution is able to detect physical and cyber-attacks and risks not only nationally but also at the EU level	Transnational threats and attacks are covered on an EU perimeter	Transnational threats and attacks are effectively covered over the years.	Security, Money
The tool has been tested to face several different attacks. The SAFECARE solution is built "resilient" (able to face attacks on its own components)	Detection and protection from a large panel of threats and attacks. The solution is built resilient.	The solution remains resilient and efficient, even after the typology of attacks, infrastructures and technologies change.	Security
The tool counts as a unique, centralized platform. Detection engines are able to distinguish true to false-positive alerts. Therefore, the	No additional controls are required.	The solution, which integrates a centralized platform with detection engines, represents the best and most efficient tool ever.	Novelty, confort, money, environment

solution allows saving precious time.		The tool will not be completed by another mass-market solution.	
The alert and reporting tool allows internal and external stakeholders to be constantly informed on real-time threats and attack on a timely, accurate and precise manner; and communicate effectively and efficiently. Moreover, SAFECARE is updated with other infrastructures attacks, meaning that it is possible to benefit from those others attacks to protect and secure infrastructure.	Synchronized and accurate information, permanent and real-time alerts, pooled forces against threats.	The solution remains efficient in terms of synchronizations, alerts and reporting.	Security
The tool provides a common ground and a shared situational awareness picture to internal and external stakeholders. Therefore, the various stakeholders involved in the crisis management could collaborate more efficiently to the crisis resolution and could make better and more informed decisions.	Enhanced communication, cooperation and decision-making, based on real-time, precise and accurate information following standard operating procedures.	The solution remains efficient in terms of synchronizations, alerts and reporting.	Security
In the case a server fails or goes down, the connection is automatically switched to a secondary server. This enables the perfect continuity of services.	Automatic switch to a secondary server in case of a fail-down, continuity of services proved.	The continuity of services and balances (in case of a failure) is functional after years.	Security, le confort
The tools are equipped with high-level performance detection engines that are able to recognize very discreet attacks. Moreover, the detection engines are upgradable and modular.	Thin detection. Detection engines are modular (downgradable/upgradable) according to needs.	Thin detection is permanently efficient. Detection engines performance, modularity and upgradability offer remain interesting and efficient for end-users after years.	Security, confort, novelty

The tool is connected to building fire detection systems that can distinguish real from false alerts. Thus, security professionals may benefit from a supplementary tool to manage the main risks and to take the best decisions at the best time.	Synchronized with Fire Detection System, ability to manage main risks at the best time.	The solution remains the best "addons" fire detection system and fire risk management tool after years. No new law or regulation will be able, for instance, to forbid an addons system or to force to invest in a specific system or architecture.	Security, Confort
The tool is so flexible, customizable and scalable that it is able to report good alerts to security targeted internal or external teams. It allows to save precious time, but also to be real-time informed and thus to be able to manipulate and activate all the specific levers to stop the attack.	Customization and automating of reports (intern and extern). Give the information to the teams. Capacity to prepare and overwhelm a risk crisis.	Customizations of alerts, configurations, flexibility and scalability of the tool and modules remain effective after years.	Environment, Money
The tool has been conceived so that data collected are secured from rob, infiltration, listening, redirections. The end-users will benefit from a high confidentiality level on data collected.	Data collected secured from rob, infiltration, listening, redirections. High data availability, confidentiality, integrity.	Security, Confidentiality, Protectives features and methods remain efficient after years.	Security
In case of a proven attack, security practitioners are not alone facing the attack, as they may benefit from an after-sale service. A hotline and after-sale team listens to end-users and answers their questions.	Hotline and after-sale service available.	After-sale service remains available, dynamic and efficient after years.	Security, confort, money
The tool provides the end-users with real-time availability of Back-end and Front-end services. They benefit from a real control tower, and there is no longer the need to deploy specific availability tools.	Real-time Availability Service (Front end and Back end).	Real-time availability service remain effective permanently, and the best availability tool.	Confort, security
The tool is equipped with several risk mapping analysis engines, able to identify risks, their frequency, their gravity and their impact on a given infrastructure. Security	Risk mapping tool working with analysis engines.	Risk mapping engines remain efficient after years.	Security, Confort

practitioners will no longer have to deploy a risk management dedicated team.			
The tool is customizable and modular, meaning that it is possible to select various and different modules/equipment/systems necessary to protect a healthcare infrastructure.	The solution is modular and customizable. The yearly expense can be reviewed or resized every year.	Customization and modularity offer remains relevant after years.	Confort, money
The tool is able to detect attacks targeting biomedical equipment. This means protecting lives, but also the assets and the company’s reputation.	Biomedical equipment (thus high value assets and critical equipment) are protected.	The solution detects threats and attacks on biomedical equipment after years. The solution represents the best tool in detection and protection available on the market.	Security, money
The tool is able to detect attacks targeting health data. By protecting them, the end-users guarantee a high level of healthcare services and healthcare data confidentiality. This improves a company’s reputation.	Health and critical data are protected (as well as reputation).	The solution detects threats and attacks on health data after years. The solution remains the best turnkey solution to ensure and guarantee the availability, confidentiality and integrity of health data over the years.	Security, money
The tool is able to detect attacks aiming at substituting and stealing healthcare vital supply. By protecting them, the end-users ensure the quality of health cares in all circumstances and guarantee the authenticity of health products.	Healthcare vital supply, medicines, sensitive stocks, dangerous supplies are better protected.	The solution detects threats and attacks on healthcare vital supply, medicines, sensitive stocks, and dangerous supplies.	Security, money
The tool is able to adapt to new types of threats and capabilities of mitigation. In particular sensors, detection modules and the Impact Propagation Module (IPM), which represents the integration of the knowledge of practitioners and cyber and physical experts.	New types of threats are detected, it faces new attacks due to IPM Module, the cooperating sensors of which, are combined with smart and analytics engines, being able to stop the attacks.	IPM Module remains the most advanced, clever and performant tool to face new threats and attacks after years. There is no other offer on the market that could be stronger or better.	Security, environment, novelty

Table 3.5 SAFECARE benefits

4. How to integrate the SAFECARE global solution

The aim of this section is to explain how to integrate the SAFECARE global solution in an hospital ecosystem. For this, paragraph 4.1 presents the steps to be undertaken in order to integrate the SAFECARE solution in a hospital, while paragraph 4.2 details how to interface the different SAFECARE modules to the kinds of software used in the hospitals of Marseille Amsterdam for crisis and risk-management purposes.

4.1 The steps needed to integrate SAFECARE in a hospital

The following figure provides an overview of the connections between SAFECARE and the hospital's ecosystem.

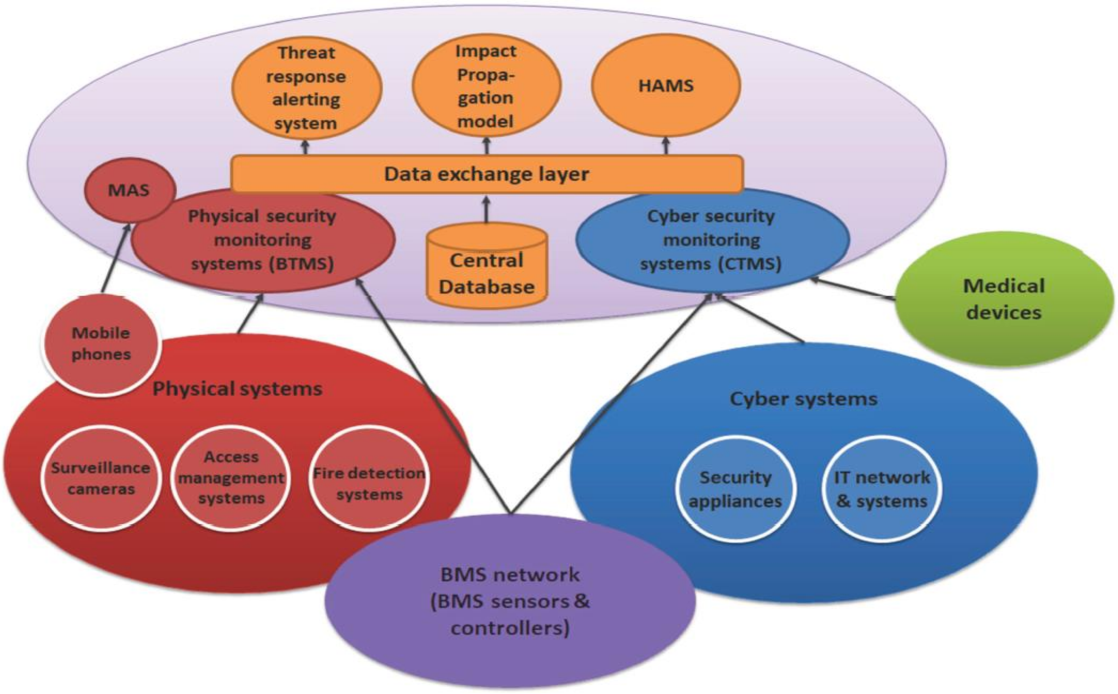

Threat response alerting system
Impact Propa-gation model
HAMS
Data exchange layer
MAS
Physical security monitoring systems (BTMS)
Central Database
Cyber security monitoring systems (CTMS)
Medical devices
Mobile phones
Physical systems
Surveillance cameras
Access management systems
Fire detection systems
Cyber systems
Security appliances
IT network & systems
BMS network (BMS sensors & controllers)

Figure 37: Connections between SAFECARE and the hospital's ecosystem

The figure below details the steps to be undertaken in order to integrate the SAFECARE global solution in a hospital ecosystem.

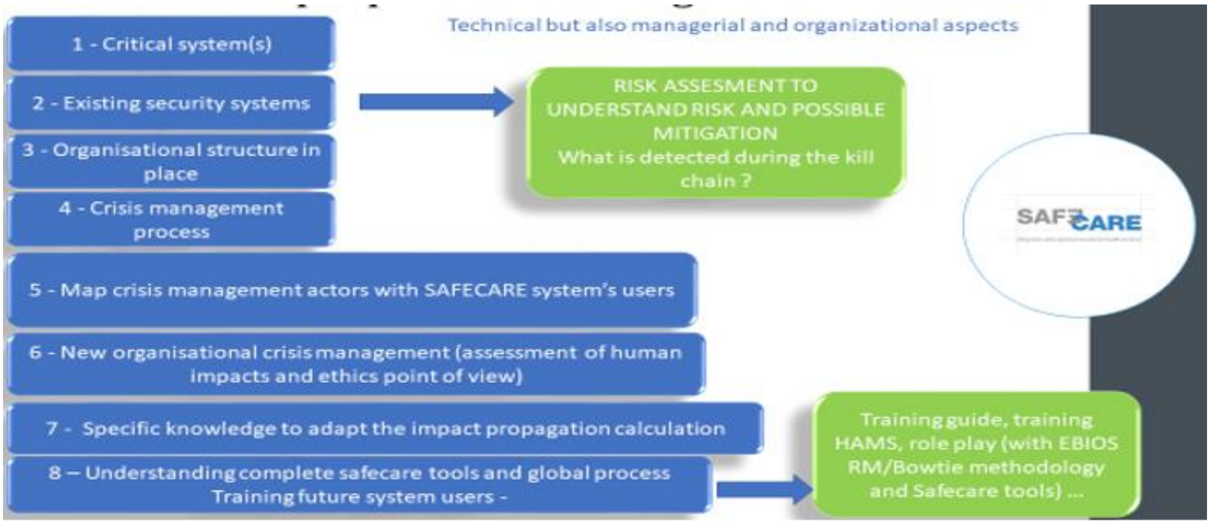

Technical but also managerial and organizational aspects
1 - Critical system(s)
2 - Existing security systems
3 - Organisational structure in place
4 - Crisis management process
RISK ASSESMENT TO UNDERSTAND RISK AND POSSIBLE MITIGATION
What is detected during the kill chain ?
SAFECARE
5 - Map crisis management actors with SAFECARE system's users
6 - New organisational crisis management (assessment of human impacts and ethics point of view)
7 - Specific knowledge to adapt the impact propagation calculation
8 – Understanding complete safecare tools and global process
Training future system users -
Training guide, training HAMS, role play (with EBIOS RM/Bowtie methodology and Safecare tools) …

Figure 38: SAFECARE integration in a hospital

These 8 steps can be summarised as follows:

1. Which **critical system(s)** are going to be integrated (number and maturity): identify and describe these systems. It is recommended to select a short list of the most critical systems in the first step.

2. As there are already mitigation measures in place, to find out which **existing security systems** (e.g. sensors, Information Systems), their characteristics (technical, communication etc.) and decide if they will (or not) be integrated to SAFECARE platform: use a method combining Ebios RM / Bowtie / tables of knowledge. Depending on the security management maturity it is also important to choose which module of SAFECARE are selected in a first step of integration.

To identify supplementary measures, it is necessary to perform a new risk assessment to find the possible risks and possible mitigation. Main questions are: what is detected during the kill chain of the risk? For each step of possible attack can we detect the attack? In these first steps we discover the use of SAFECARE that permit to improve security by identifying how to integrate modules.

3. Which **organisational structure** is in place: which security management actors are involved? Are they internal or external to the hospital? **How to integrate SAFECARE tools in their uses?**

4. Which **crisis management process** already exists in the hospital and how the aforementioned actors are involved in this process.

5. Should map **crisis management actors with SAFECARE system's users** and probably foresee new system users (e.g. for the HAMS in particular which provide a global approach of the security management including physical and cyber sides, internal or external)

6. If a **new organisational crisis management** (e.g. actors, processes etc.) is needed, it should follow the financial, organisational, human resources, etc. management. An ethic reflexion is also needed to consider ethics risks concerning impacts on human, with new data and new way to identify possible impacts, with automatic calculation of possible impacts on health care with the management of different knowledge. It is very important

to analyse and validate all automatic alerts that are an innovative component of SAFECARE but can have serious consequences. How the use of the information must be considered and the ethics impact of this new approach of the way to manage security.

7. Which **specific knowledge is needed** to adapt the impact propagation calculation. The first ontology deployed must be tuned and we have to consider the skills and the knowledge of the people in charge of management of security inside the hospital.

8. Understanding of complete SAFECARE tools and the global process of SAFECARE. The future system users should know the **description of the system** with all the integrated modules. If users don't know the system it can have an impact on security; they have to be confident in the future use. So the future system users should be **trained** on their system's uses: training guide, simulation and demo mode of HAMS module, role play (with EBIOS RM/Bowtie methodology).

4.2 Integration of the SAFECARE modules

The kinds of software used in the hospitals of Marseille and Amsterdam for crisis and risk-management purposes are the following:

- Firewall
- SIEM
- EDR
- PLC supervision
- Fire detection supervision
- Access control supervision
- Video protection supervision
- EAI (Enterprise Applications Integration)
- BMS (Building Management System).
- SIEM
- Endpoint protection
- IDS (only employed for workstation-to-internet traffic)
- Digital asset management
- Video protection supervision
- Access control management and supervision
- Network administration tools that specifically facilitate "micro-segmentation".
- Epic access supervision (involves automated classification of potentially suspicious access to health records: e.g. invocation of "break-the-glass" procedure; practitioner accessing record of person with same last name).

Based on the kinds of software presented above, this paragraph attempts to explain how the SAFECARE modules can be integrated to one (or more) of them, depending on when integration is feasible and provides sufficient benefit.

Building Threat Monitoring System (BTMS)

Fire detection supervision and access control supervision communicate with BTMS via CSI's MQ Telemetry Transport (MQTT) server. Those two systems act as publishers while BTMS is the subscriber.

Video protection supervision is managed by the Milestone Video Management System (VMS), XProtect®, installed on a Windows virtual machine provided by AP-HM. A plugin program with

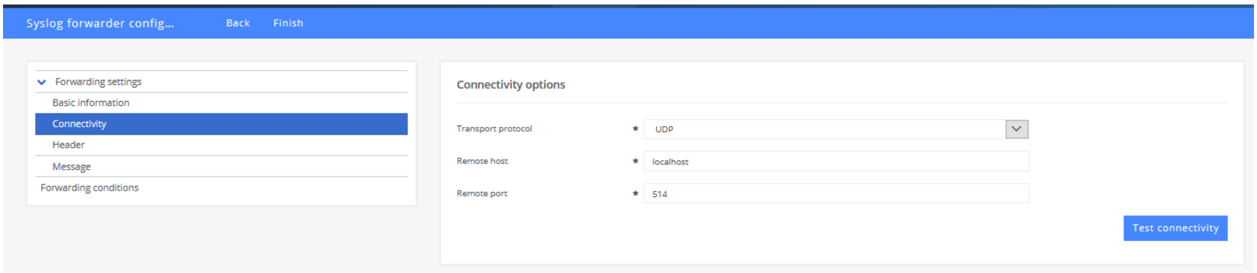
.Net Dynamic Linked Library (DLL) files and configuration files are copied to the installation folder for XProtect®.

Suspicious Behavior Detection System (SBDS) and Intrusion Fire Detection System (IFDS)

SBDS and IFDS are installed on an Ubuntu machine provided by Milestone but located at the AP-HM premises and in the same network as the Windows machine above. The IP addresses of the Ubuntu machine is configured on the XProtect user interface. SBDS/IFDS communicate with BTMS via TCP protocols. They do not communicate with other SAFECARE components.

BMS Threat Detection System (BTDS)

The BTDS can directly send information about detected threats to most SIEM systems using the Syslog protocol. Syslog forwarding can be configured as shown in Figure 38, where the destination of messages can be configured, as well as their contents.



Connectivity options

Transport protocol * UDP

Remote host * localhost

Remote port * 514

Figure 39: Configuration of the syslog forwarder

Other connections can be configured using Forescout's portfolio of solutions. Forescout provides a tool for network segmentation called eyeSegment that takes as input communication flows observed by the BTDS. Forescout also provides an Operational Technology Module for its eyeSight device visibility platform which takes asset information from the BTDS and can correlate it with information coming from cybersecurity tools via many available integrations. Those include receiving alerts and IoC matches from EDR tools (Carbon Black, Crowdstrike, FireEye, McAffee, Symantec) and designing policies for Firewall solutions (Checkpoint, Fortiner, Palo Alto).

E-Health Device Security Analytics (EDSA)

EDSA medical device security monitoring is provided as a service. The service is designed to support different integrations depending on the service and remediation type. For direct integration with the hospital, support for the industry standard Syslog protocol is foreseen. This provides an interface to integrate with hospital security software solutions such as SIEM. This facilitates the exchange of security alerts and related data to support remediation of security issues.

Depending on the type of service and alert, alerts and data will be routed to the hospital SIEM, interface with the vendor service system for vendor remediation, or interface with another system. Besides Syslog and SIEM further software adapters could be provided.

Mobile Alerting System (MAS) and Hospital Availability Management System (HAMS)

MAS & HAMS communicate via MQTT server with the other SAFECARE tools. Hospitals data are retrieved from CDB provided by CSI. Users authentication and authorization are managed by keycloak server that could be integrated with hospital directory services (e.g. Windows Active Directory).

Impact Propagation and Decision Support Model (IPDSM)

For its functioning, the IPDSM relies on up-to-date data describing the hospital's assets and the interrelationships between them. It reacts to declared and transmitted physical and / or cyber incidents and returns a potential impact list. So, if a hospital has a system that stores data on assets and their links, the IPDMS can interface with an incident detection system to provide potential impacts. It could also be interfaced with a tool for risk analysis to help the analyst in the evaluation of the risks.

IT Threat Detection System (ITTDS)

The ITTDS is composed of a network probe (Suricata) and innovative machine learning algorithms that allow the detection of different security events. These events can be sent directly to most SIEM systems using the Syslog protocol. ITTDS also contains a log management system (Graylog) that receives security events from various systems (Firewall, EDR, Endpoint protection, IDS), namely from Suricata, to correlate events and raise alerts to SIEM systems.

Advanced File Analysis System (AFAS)

The AFAS is based on Orion Malware (OMW). The AFAS use case in the framework of SAFECARE is automatic file submission from the Suricata network probe (ITTDS) and the Forescout's probe (BMS TDS) to the Orion Malware REST API. Thus, the AFAS can be integrated with IDS but also with firewalls if they are able to extract files from the network and submit them to a REST API. In addition, OMW can be configured to send the analysis result to most SIEM systems. Last, OMW can also be interfaced with other third party systems such as MISP or LDAP servers.

Cyber Threat Monitoring System (CTMS)

The CTMS can receive security alerts from most SIEM systems. In the event of an actual incident, the CTMS communicates via a MQTT server with the other SAFECARE tools. Hospitals data can be retrieved from the SAFECARE CDB. In addition, the CTMS can also be integrated with other digital asset management systems such as GLPI. In order to share incidents, the CTMS can be configured to send them to various other systems. As for receiving security events and alerts, the CTMS can also be configured to receive them from IDS or EDR.

Data Collection System (DCS)

The DCS communicates indirectly with the existing systems of the hospital as it uses the MQTT protocol to send data with security certificates to an MQTT server from which other SafeCare components can retrieve the data (such as XProtect). If any systems use a local Modbus server to store and retrieve information, using the IP address of the server, the collected information can be transmitted directly to those systems using the Modbus communication protocol.

Alternatively, the DCS can be used as an individual service, as it can provide a graphical interface (Grafana) to display information and to set up alarms triggered by certain events.

All these solutions can be utilized individually or can be used together.

E-Health Security Risk Management Model

The E-Health Security Risk Management Model for product security risk management operates in the back-office of the medical device manufacturer to support product design. Amongst others, the model takes advantage of installed base data originating from medical devices in hospitals and analytical models operating on this data, for which it interfaces with the EDSA module in SAFECARE.

The E-Health Security Risk Management Model does not directly interface with hospital security software solutions. Sharing selected data to support hospital risk management is identified as a roadmap item. The data to be shared and the interface, formats and protocols are to be defined by further industry alignment and standardization.

Central Database (CDB) and Data Exchange Layer (DXL)

CDB can be used as stand alone (used by a hospital) in order to manage hospital asset data in an integrated way or as component of SAFECARE system for management of the integration among different modules.

DXL can be used in an integrated way as component of application of SAFECARE system for management of the integration among different modules.

5. How to use the SAFECARE global solution in risk and crisis-management processes

Risk management is an increasingly valuable driver for organisations. In fact, an enterprise-wide approach to risk management allows an organisation to think about the possible impact of all types of risks on all processes, activities, stakeholders, products and services. Thus, there is a need to comprehend the risks being taken when organisations are pursuing to achieve their objectives and attain the desired level of service. Organisations need to understand the overall level of risk embedded within their processes and activities and it is important for them to acknowledge and rank their risks and identify the best critical controls to mitigate them.

5.1 Introduction to ISO 31000:2018

One of the best all-around methodologies and one of the most complete is ISO 31000 which takes into account the time continuum of operations better than any other methodology, and although it includes all of the same constituent components of other leading methodologies, it is one of the easiest to condense into a simplified yet complete risk assessment process.

ISO 31000:2018 provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual and it is not specific to any industry or sector[2].

As shown in Figure 40, the risk management process involves the application of procedures to the activities of communicating and consulting, establishing the context, risk assessment, treatment, communication and consultation, monitoring and review as well as recording and reporting.

It is also important to define the scope and context of the risk management process. The context is a combination of the external and internal environments, both viewed in relation to organisational objectives and strategies.

Then, a risk assessment should be conducted. This is composed of three sub-tasks: “risk identification”, “risk analysis” and “risk evaluation”. Initially, we need to identify sources of a particular risk, areas of impacts, and potential events including their causes and consequences. Moreover, classification of the source as internal or external should be made. We then need to identify potential consequences and factors that affect the consequences, assess the likelihood, as well as identify and evaluate the controls currently in place. After that, an evaluation of the identified risks should be performed and decisions should be made to treat or accept risks with regard to internal, legal, regulatory and external party requirements.

Moreover, management should develop and implement risk treatments to reduce residual risks to levels acceptable to key stakeholders. Finally, as part of the risk management process, risks and controls should be monitored and reviewed on a regular basis to verify that:

- assumptions about risks remain valid;

[2] https://www.monarc.lu/publications/comparison-between-monarc-and-different-risk-management-methods/#2-iso-31000

- assumptions on which the risk assessment is based, including the external and internal context, remain valid;
- expected results are being achieved;
- results of risk assessment are in line with actual experience;
- risk assessment techniques are being properly applied and;
- risk treatments are effective.

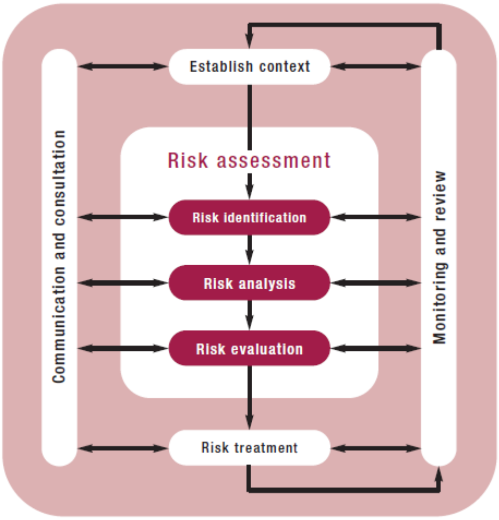


Figure 40: The Risk Management Process based on ISO 31000

5.2 IEC 31010:2019 – Risk management

Risk assessment techniques include a range of techniques to identify and understand risk and adds to ISO 31000, Risk management. These techniques are used within the risk assessment steps of identifying, analysing and evaluating risk as described in ISO31000 and more generally whenever there is a need to comprehend uncertainty and its consequences. The techniques described can be used in a wide range of situations. However, the majority originated in the technical domain. This standard assumes that the risk assessment is performed within the framework and process of risk management described in ISO 31000.

Risk assessment is the overall process of risk identification, analysis and evaluation (as analysed below). The manner in which this process is applied does not only depend on the context of the risk management process, but also on the methods and techniques used to carry out the risk assessment. The IEC 31010 classifies (as displayed in Figure 41) and analyses techniques according to their main application in assessing risk, namely: eliciting views from stakeholders, identifying risk, analysing sources and drivers of risk, analysing controls, understanding consequences, likelihood and risk, analysing dependencies and interactions, selecting between options, evaluating the significance of risk, reporting and recording.

The techniques described embody structured ways of looking at the problem in hand that have been found valuable in particular environments. The list is not expected to be complete but covers a range of commonly used techniques from a variety of sectors.

In selecting a technique the following aspects of context should therefore be considered: the context, the needs of stakeholders, any regulatory and contractual requirements, the operating environment and scenario, the importance of the decision (e.g. the consequences if a wrong decision is made), any defined decision criteria and their form, the time available before a decision must be made, information that is available or can be obtained, the complexity of the situation, as well as the expertise available or that can be obtained.

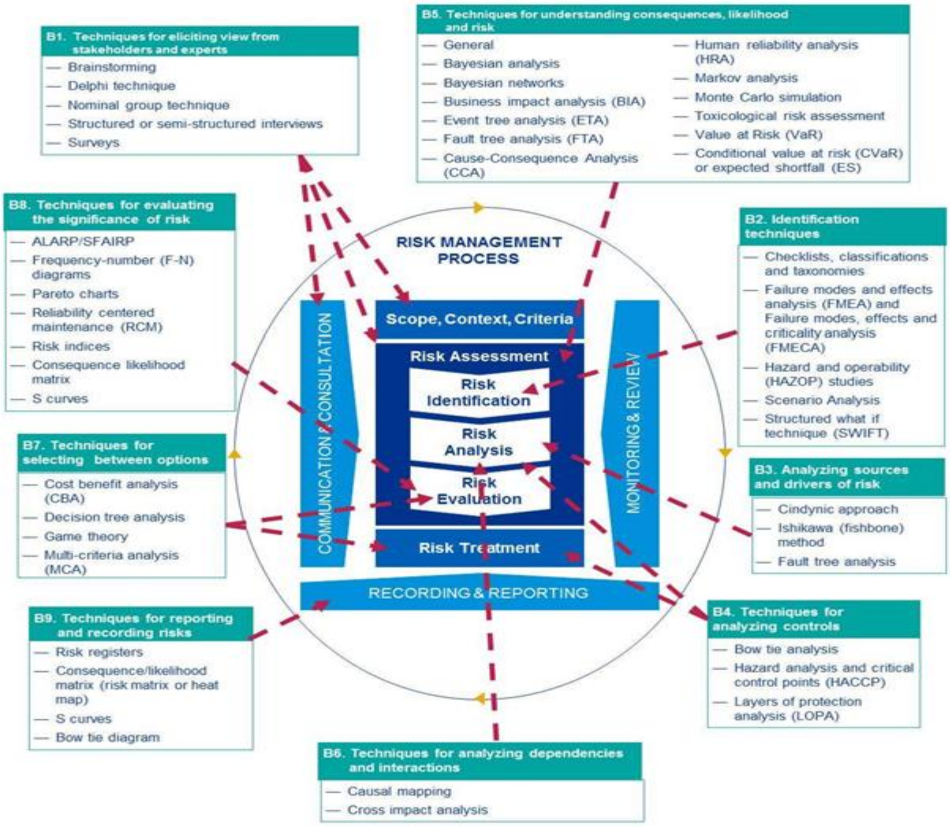

B1. Techniques for eliciting view from stakeholders and experts
— Brainstorming
— Delphi technique
— Nominal group technique
— Structured or semi-structured interviews
— Surveys
B5. Techniques for understanding consequences, likelihood and risk
— General
— Bayesian analysis
— Bayesian networks
— Business impact analysis (BIA)
— Event tree analysis (ETA)
— Fault tree analysis (FTA)
— Cause-Consequence Analysis (CCA)
— Human reliability analysis (HRA)
— Markov analysis
— Monte Carlo simulation
— Toxicological risk assessment
— Value at Risk (VaR)
— Conditional value at risk (CVaR) or expected shortfall (ES)
B8. Techniques for evaluating the significance of risk
— ALARP/SFAIRP
— Frequency-number (F-N) diagrams
— Pareto charts
— Reliability centered maintenance (RCM)
— Risk indices
— Consequence likelihood matrix
— S curves
B2. Identification techniques
— Checklists, classifications and taxonomies
— Failure modes and effects analysis (FMEA) and Failure modes, effects and criticality analysis (FMECA)
— Hazard and operability (HAZOP) studies
— Scenario Analysis
— Structured what if technique (SWIFT)
RISK MANAGEMENT PROCESS
Scope, Context, Criteria
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Risk Treatment
COMMUNICATION & CONSULTATION
MONITORING & REVIEW
RECORDING & REPORTING
B7. Techniques for selecting between options
— Cost benefit analysis (CBA)
— Decision tree analysis
— Game theory
— Multi-criteria analysis (MCA)
B3. Analyzing sources and drivers of risk
— Cindynic approach
— Ishikawa (fishbone) method
— Fault tree analysis
B9. Techniques for reporting and recording risks
— Risk registers
— Consequence/likelihood matrix (risk matrix or heat map)
— S curves
— Bow tie diagram
B4. Techniques for analyzing controls
— Bow tie analysis
— Hazard analysis and critical control points (HACCP)
— Layers of protection analysis (LOPA)
B6. Techniques for analyzing dependencies and interactions
— Causal mapping
— Cross impact analysis

Figure 41: The Risk Management Techniques of ISO 31000

5.2.1 Risk identification

Risk identification is the procedure of finding, recognizing and recording risks. The objective of risk identification is to identify what might take place or what conditions may exist that could affect the accomplishment of the objectives of the system or organization. The risk identification process consists of identifying the origins and source of the risk (hazard in the context of physical harm), events, situations or circumstances which could have a material impact upon objectives and the nature of that impact. Risk identification methods can include:

- Evidence based methods, examples of which are check-lists and reviews of historical data;
- Systematic team approaches where a team of experts follow a systematic process to

- Identify risks by means of a structured set of prompts or questions;
- Inductive reasoning techniques such as HAZOP[3];
- Brainstorming,
- Delphi methodology[4]

5.2.2 Risk analysis

Risk analysis is about creating an understanding of the risk. Risk analysis involves determining the effects and their probabilities for identified risk events, taking into account the presence (or not) and the efficiency of any existing controls. The consequences and their probabilities are then merged to determine a level of risk.

Risk analysis entails consideration of the root-causes and sources of risk, their consequences and the probability that those consequences can inflict. The methods used in analysing risks can be qualitative, semi-quantitative or quantitative. Qualitative assessment describes consequence, probability and level of risk by significance levels such as "high", "medium" and "low", may combine consequence and probability, and evaluates the subsequent level of risk against qualitative criteria. Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Quantitative analysis estimates functional values for consequences and their probabilities, and produces values of the level of risk in specific units defined when developing the context.

Inherent to the risk analysis are the steps of a) controls valuation which measures the adequacy and effectiveness of existing controls, b) consequence analysis which determines the nature and type of impact which could occur assuming that a particular event situation or circumstance has occurred, c) likelihood analysis and probability estimation based on the use of relevant historical data to identify events or situations which have occurred in the past and hence be able to extrapolate the probability of their occurrence in the future, probability forecasts using predictive techniques such as fault tree analysis and event tree analysis and also expert opinions which can be used to estimate probability.

5.2.3 Risk evaluation

Risk evaluation involves comparing the appraised levels of risk with risk criteria defined when the context was established. The aim is to determine the significance of the level and type of risk in order to inform decisions whether to treat a risk, the priorities for treatment, the treatment activities and the paths that should be followed to treat a risk.

A common approach is to divide risks into three categories:

a) an upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever it costs;

[3] HAZOP: HAZard and OPerability analysis

[4] The Delphi method is a process used to arrive at a group opinion or decision by surveying a panel of expert

b) a middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences;

c) a lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

5.3 The risk-management cycle

Despite sound risk management techniques and practices described above, some situations are unavoidable, and organizations may, at any point, face some situation that may call for crisis management. Crisis management is related to the management of unexpected events that may cause destruction or harm to an organization and its stakeholders, while risk management is the process of determining how threats would impact an organization, and how risks can be handled so as to minimize the damage to the organization.

It appears that risk management is a continuous process through which threats are emphasized and decisions are made so that solutions are in place to mitigate or avoid the risks (proactive), while crisis management is mainly reactive, occurring as the event unfolds and the risk is no longer a risk but an incident of high importance. Within the crisis management process and especially the response phase, the risk management process is continuously repeated, making risk and crisis management two processes interacting and used bilaterally when needed. Hence, when both processes are in place, an organization is able to act rapidly in times of crisis and face the least possible losses. In addition, they are able to recover from this loss quickly by ensuring that operations normalize as soon as possible.

Crisis management has been defined as "the developed capability of an organization to prepare for, anticipate, respond to and recover from crises (British Standard Institute (BSI), 2014). In the following paragraphs, the crisis management process as well as the stakeholders involved, in a healthcare setting, are presented:

Preparedness is a continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective actions that internal and external stakeholders should cooperate closely to ensure organization readiness.

Risk assessment constitutes the fundamental first step in preparedness and this means the identification and analysis of major threats, hazards and related vulnerabilities. This procedure helps organizations make decisions on equipment supply, maintenance and improvement, identification protective measures and to take quick decisions during the crisis. Having determined the risks that could impact airports and how, actions that support response process should be identified. More specifically, appropriate institutional structures, clear mandates supported by comprehensive policies, plans and legislation and the allocation of resources for all these capacities through regular budgets are also instrumental for thorough preparedness to crisis.

Response initiates when an incident is detected with a manual or automated way. Internal stakeholders should start gathering information that will be used for the initial assessment of the incident. Information gathering and assessment is a crucial and continuous step of this phase, as it highly depends not only on the source, quality, relevance of it, but also on the capacity of stakeholders involved in analyzing, interpreting, understanding and adding value to raw information. Based on the criticality of the incident, Crisis Management Team (CMT) should be informed and triggered; and CMT should determine, plan and define which response plan(s) should be activated (e.g. ambulance trafficking plan, evacuation, business continuity etc.); resources should be allocated and released and actions should be assigned and tracked. In addition, relative information (that can be used for management, informative purposes) should be communicated on-time, accurately and precisely to internal and external stakeholders, in order to manage crisis management process and protect the brand and reputation of the organization. The afore-mentioned steps could repeat, till resources return to their original use and status (demobilization) and crisis terminates.

Recovery consists of those activities that continue beyond the emergency period to restore critical community functions and begin to manage stabilization efforts. This phase starts after the response phase termination and is directly affected by decisions made as part of the response. Moreover, evidence from the incidence should be collected (in cooperation with relative stakeholders e.g. Law Enforcement Agencies, Fire Brigade etc., depending on the nature of the incident); analyzed; and an evidence report should be created. Relative information should be shared with internal external stakeholders and investigations should be assisted. Moreover, as crisis serves as a major learning opportunity for both individuals and organizations as a whole, the overall process should be reviewed and plans, procedures, tools, facilities etc. should be evaluated, to identify areas for improvement. Following the evaluation lessons learnt should be identified and recommendations/changes should be made.

Mitigation is the process related to the reduction of life and property loss by reducing the impact of crisis. It involves structural (such as change the characteristics of buildings; flood control projects, raising building elevations etc.) and non-structural measures (adopting or changing physical and cyber access control codes, training, insurance, discussion, planning etc.).

The concept of the cycle implies an ongoing process which tries to eliminate disruptions, to provide immediate assistance to affected ontologies, to reduce disaster losses and to improve the conditions of the affected communities. Usually, the crisis management cycle is triggered by an event and begins with the response to that event. As the main aim is to respond to the specific threat, crisis management programs often prioritize the preparedness and response phases, leaving limited resources to address recovery and mitigation. A systems approach to crisis management suggests a different understanding of the crisis cycle that balances resources among the four phases.

5.3.1 The SAFECARE modules throughout the crisis-management cycle

This section details in which step(s) of the crisis-management cycle presented above each SAFECARE module can be used.

Suspicious Behaviour Detection system (SBDS)

Response: This system processes videos streams from surveillance cameras in near real-time. It will trigger security alerts in case of suspicious behaviours, such as crowding, loitering in restricted areas, weapon carrying and covered faces, and report to the Buiding Threat Monitoring System.

Intrusion and Fire Detection System (IFDS)

Response: This system detects in near real-time intrusion behaviours, such as tailgating, and fire, based on video streams from surveillance cameras and other digital sensors, such as door access controls and smoke/fire alarms. It triggers security alerts and reports to the Building Threat Monitoring System.

Data Collection System (DCS)

Response: it gathers information from all the sensors, and if there are abnormal parameters received from the temperature and humidity sensors, it sends fire detection events to the intrusion and fire detection system. This way, the security alerts and reports to the Building Threat Monitoring System.

Preparedness: it detects, by analyzing sensor data, an attacker's attempt to create panic by starting a fire or by turning off the electricity. The system starts from the idea that fire events do not start randomly.

The module can be used both for real-time crisis management, when it is gathering information from all the sensors in order to detect any temperature, humidity, and power issues and for training, by running a modified script, in which the temperature is increased manually, to make the sensors think that there is a fire, for example.

Mobile Alerting System (MAS)

Preparedness: It provides access to previous security incidents and impacts.

Response:

- Enables the communication between the BTMS and the security guards to quickly verify dubious physical security threats detected by the security operators.
- Provides the security guards with the ability to report incidents
- Sends potential impacts to supervisors in charge (hospital general manager, security chief).
- Sends notifications to users with response plans to instruct personnel on the actions to take to respond to an incident.

Building Threat Monitoring System (BTMS)

Preparedness: The Milestone XProtect®, as a part of the Building Threat Monitoring System, manages the setup of security devices and placing of critical assets graphically. It helps highlight existing physical security vulnerabilities and improve the security by optimizing the setup.

Response: The building monitoring system centralises security events from the Suspicious Behaviour Detection System, Intrusion and Fire Detection System and Data Collection System and communicates with the Mobile Alerting System. It allows the user to acknowledge or reject an alert, forward an incident to the Central Database and show the impacts.

Recovery: The video and related metadata for each incident is saved by the Milestone XProtect®. The videos are used as evidence by the stakeholders. They are also used as training data for future system improvements.

IT threat detection system (ITTDS)

The IT threat detection system can be used in the following steps:

Preparedness: Provide statistics and trends of security threats based on past security alerts and exploitation of vulnerabilities. This can be useful for training and risk assessment.

Response: Detect potential threats and raise security alerts related to the IT infrastructure, providing information about the targeted hosts. The information is useful for the initial assessment of the incident during the crisis management.

Recovery: Collect the security events that allow triggering alerts and responding to the threat. The collected security events can be useful to gather evidence of the incident during the crisis management.

BMS threat detection system (BTDS)

The BMS threat detection system can be used during the following steps: **preparedness**, to help in risk assessment by highlighting existing vulnerabilities in network devices or by reviewing previous security alerts related to specific devices; and **response**, by detecting security-relevant events when they happen and providing information about source and destination hosts, protocols, type of event and other data, which allow the crisis management team to investigate and respond to an attack.

The module can be both for real-time crisis management, when gathering information and detecting security events from live network traffic, and for training, when taking as input pre-recorded network traffic that can be replayed for simulation.

Advanced file analysis system (AFAS)

Preparedness: Provide statistics and trends of security threats based on past malware detected. This can be useful for training and risk assessment.

Response: Detect malware and raise security alerts, providing a security risk level with an analysis report for each file. The report is useful for the initial assessment of the incident during the crisis management.

Recovery: Keep files corresponding to malware and can provide the footprint of malware. This is useful to gather evidence of the incident during the crisis management.

E-health Device Security Analytics (EDSA)

Preparedness: use analytics to provide statistics on security configuration, posture, threats, vulnerabilities related to medical devices to support risk management.

Response: generate alerts on security misconfigurations, threats or vulnerabilities related to medical devices with root cause and recommended action to support remediation.

Cyber threat monitoring system (CTMS)

Preparedness: Provide statistics and details on past security incidents. This can be useful for training and risk assessment.

Response: Manage security alerts to respond quickly to incidents. The tool is useful for information gathering and assessment. It can also help the crisis management team by providing relevant response plans related to the incident.

Recovery: Provide a list of compromised assets related to an incident, which is useful when compiling the evidence report.

Mitigation: Create and implement comprehensive set of reaction plan, mitigating security risks.

Data Exchange Layer (DXL)

Preparedness: Providing the service of distribution of messages among the various SAFECARE modules, it allows other modules to be involved for the preparedness purpose.

Response: Providing the service of distribution of messages among the various SAFECARE modules, it allows other modules to respond to risk management events.

Mitigation: Providing the service of distribution of messages among the various SAFECARE modules, it permits mitigating security risks.

Central Data Base (CDB)

Preparedness: Statistics generated on the basis of assets characteristics included in CDB and details on past security incidents could support the whole SAFECARE solution risk management. This can be useful also for training and risk assessment.

Response: Store and manage security alerts to respond quickly to incidents. The tool is useful for information storing and assessment of all real events happened.

Mitigation: Experience of past events duly stored and registered is a useful tool for mitigating security risks.

Impact Propagation and Decision Support Model (IPDSM)

Preparedness: Thanks to the knowledge of the internal context of the hospital capitalized on by the ontology it embeds.

Response: To determine the propagation of the impacts of an incident on the assets (as well as their evaluations) and to better react. This assumes that its ontology is correctly maintained in order to reflect the real context of the hospital.

To be efficient, this module can receive feedbacks in terms of (1) new incidents detected, (2) new mitigation solutions adopted and (3) changes about the appreciation of the value of assets. These feedbacks come from the response, recovery and mitigation steps.

Threat Response and Alert System (TRAS)

Preparedness: when used for training, it allows stakeholder to practice different simulation scenario, as part of training and continuous improvement.

Mitigation: should a risk arise, the alerting system's role is to ensure that stakeholders implement the reaction plan as soon as possible. The rest of SAFECARE module provides all the information needed to help quickly mitigate any risk. The alerting module role is to make sure stakeholder are alerted and on the bridge as quickly and as efficiently as possible.

Overall, the alerting system's role is to focus stakeholder's attention on the reaction plan to put in place, using a wide range of medias and providing as many useful information as possible. Since the alerting system is directly connected to the global architecture, it reduces delay and allows the push of relevant information to the right stakeholders.

Hospital Availability Management System (HAMS)

Preparedness: HAMS implements a dedicated view to train users with the simulation of predefined attack scenarios. In this case users will be able to i) select a scenario; ii) get relevant information about which are the steps of the attack performed, with indication about the nature of the attack (either physical or cyber); iii) inspect simulated messages, impact graph and changes in the availability of predefined hospital assets.

Response: HAMS receives both cyber and physical incidents coming from BTMS or CTMS and alerts users through a pop-up on the screen. Incidents are visualized as a list of events and users can inspect them. Same applies when impact messages are received. Impacts can be visualized as a JSON message or as a graph (see section 2.2.15). HAMS interface has been designed with end-users and security officers to be a suitable source of information during incident management.

Recovery: the core activity of HAMS is to evaluate potential changes into the availability of hospital assets when incidents occur. To this aim, HAMS provide hierarchical views of main hospital assets, one based on tables and another view based on tree representation. This allows users to have a global view about the status of each facility and asset, providing links with occurred incident.

Mitigation: the visualization of potential impacted assets through a graph-based interface allows users not only to understand what the impact of a verified incident on hospital assets could be, but also to mitigate the cascading effects. The visualization of the impact graph allows users to see the origin of the incident and how the assets are connected to it. HAMS can visualize the assets impacted and their interconnections, but it is also possible to see all the assets in a unique graph. In this way, also not impacted assets can be visualized and users can inspect how they are connected to impacted assets.

E-health security risk management model

Preparedness: to perform and structure the risk assessment required as part of this step. Results are documented and decisions can be made based on risk estimations.

Response: to define the EDSA models used for detecting & handling security incidents. Secondary response is that incidents will be gathered and analyzed to update the model as such.

Recovery: to define a recovery after incident has been detected by EDSA.

Mitigation: to create and implement comprehensive set of measures, mitigating security risks.

The figure below summarises the crisis-management steps in which each SAFECARE module can be used.

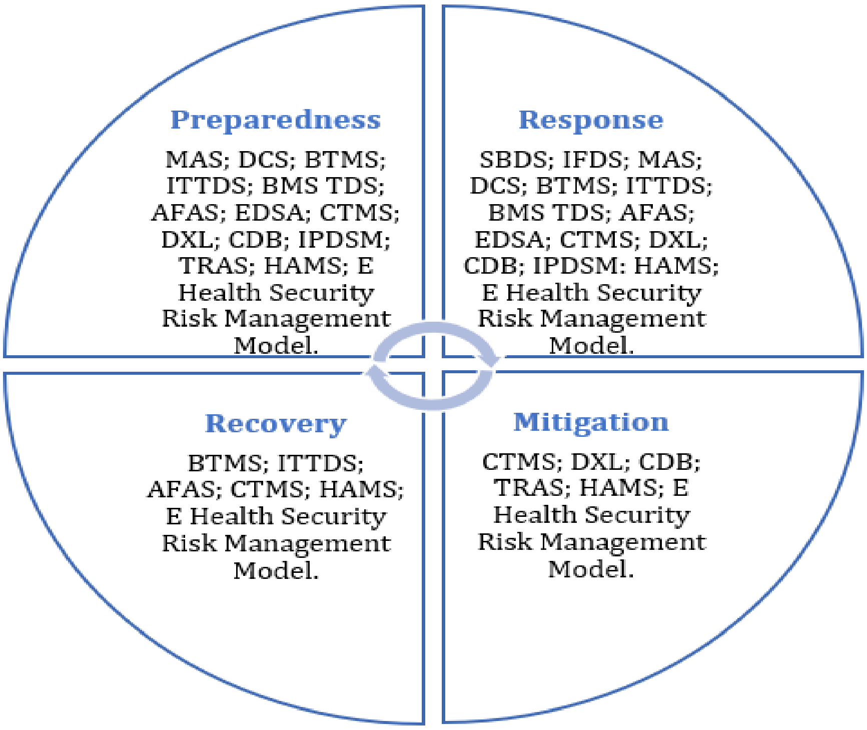

Preparedness
MAS; DCS; BTMS; ITTDS; BMS TDS; AFAS; EDSA; CTMS; DXL; CDB; IPDSM; TRAS; HAMS; E Health Security Risk Management Model.
Response
SBDS; IFDS; MAS; DCS; BTMS; ITTDS; BMS TDS; AFAS; EDSA; CTMS; DXL; CDB; IPDSM: HAMS; E Health Security Risk Management Model.
Recovery
BTMS; ITTDS; AFAS; CTMS; HAMS; E Health Security Risk Management Model.
Mitigation
CTMS; DXL; CDB; TRAS; HAMS; E Health Security Risk Management Model.

Figure 42: SAFECARE modules throughout the crisis-management cycle

Conclusion

This document aimed at presenting how to use SAFECARE in crisis and risk-management processes and to provide a technological overview of project results. In order to facilitate the uptake of the SAFECARE solution the end-users' perspective was given particular attention when presenting the SAFECARE advantages and when explaining the integration steps needed to integrate the global solution in a hospital ecosystem.

The next step will consist of making the present document accessible to the wider public in order to maximize the impact of the SAFECARE project.