SAFECARE

Integrated cyber-physical security for health services

Specification of data collection system

Deliverable 4.5

Lead Author: BEIA

Contributors: MS, CSI

Deliverable classification : PU

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

Version Control Sheet

Title	*Specification of data collection system*
Prepared By	*George Suciu, Mari-Anais Sachian, Ioana Petre, Cristiana Istrate, Denis Botezatu, Gabriel Petrescu, Loredana Chiva*
Approved By	*MS, CSI*
Version Number	*2.0*
Contact	george@beia.ro

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
V0.1	9.08.2019	Initial version	CN	
V0.2	18.10.2019	Review version	MAS, GP	
V0.3	21.10.2019	KUL review included + CCC	IP	
V0.4	24.10.2019	Few revisions according to MS review	MAS	
V0.5	30.10.2019	Final revision according the MS review	MAS, IP, GS	
V1.0	31.10.2019	Finishing touches	GS	
V2.0	5.11.2019	Finishing touches according to MS review	MAS, IP, GS	

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

Contents

List of Figures

List of Tables

1 The SAFECARE Project

Over the last decade, the European Union [1] has faced numerous threats that quickly increased in magnitude, changing the lives, the habits, and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons, to impact the population. As Europeans, we know now that we must increase our awareness against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Today, the lines between the physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet, and if not, physical intrusion might rub out the barriers. Threats cannot be analyzed solely as physical or cyber, and therefore it is critical to developing an integrated approach in order to fight against such a combination of threats. Health services are, at the same time, among the most critical infrastructures and the most vulnerable ones. They are widely relying on information systems to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this proposal is to provide solutions that will improve physical and cybersecurity in a seamless and cost-effective way. It will promote new technologies and novel approaches to enhance threat prevention, threat detection, incident response, and mitigation of impacts. The project will also participate in increasing the compliance between security tools and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin, and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find customers across Europe.

2 Executive Summary

This deliverable is part of the Work Package 4, "Physical security solution." Task 4.3 "Data collection systems from ICS, SCADA and smart building sensors," led by BEIA, have as contributors MS and CSI. The main objective of this task is to provide the technical specification for the data collection system from air cooling systems, fire detection systems, and power supply systems on the demonstration sites. In order to gather data from physical subsystems in an operation environment, it is fundamental the interfacing with the subsystems at the demonstration sites. BEIA will also implement the data exchange module for communicating with the building's monitoring system and fire detection system, enabling data collection from smart building sensors. MS will define data exchange formats to use between the data collection system, the building monitoring system, and the fire detection system, while CSI will analyze if the format of incidents coming from the BTMS developed in WP6 follows the rules defined for the data exchange.

3 Introduction

Data collection represents the most significant concern in wireless sensor networks. The main objective when it comes to gathering data is to collect large amounts of data and to diminish the data loss as a result of less memory capacity of sensor nodes. Efficient data collection methods are the key to improving the performance of sensor networks. The constant devaluation in sensors dimension and prices, but also, the diversity of sensors accessible on the market and the vast advancements in communication technology have possibly widened the impact of Wireless Sensor Networks (WSNs).

The solution provided in this deliverable firstly describes the specifications of the data collection system (D4.5) (M14) that will be integrated into M24 (D4.6). The main objective of Task 4.3 is to gather data from the sensors, transmit it to the Building Threat Monitoring System (defined in D4.9), and thereby the Data Exchange Layer (D6.2).

D4.5 presents the main ideas about the data collection systems which will be proposed in the architecture and the challenges which it will face in the project. The deliverable also presents details about the implementation of various testbed sensors that are required to be installed and used inside the hospital's rooms to collect environmental parameters, such as humidity, temperature, light, dust, movement, sound, fire, or gases. The data from the sensors will be sent afterward to the BTMS, via the Message Queuing Telemetry Transport (MQTT) protocol, and the data will be visualized in the end in the SAFECARE platform along with other events which might occur.

Section 4 presents the requirement analysis on Task 4.3 based on the DoA and the requirements established in Deliverable 3.4, merged in a single requirement table for Task 4.3. Going forth, Section 5 provides information about the solution description regarding this deliverable. Based on the previous chapter, Section 6 proposes various scenarios that describe different types of attacks that might occur in the data collection system. Furthermore, Section 7 depicts the data exchange format used for sending data to the BTMS. Section 8 has the purpose of showing and indicating what type of devices will be used for the SAFECARE laboratory room and describing the protocol which will be applied to send the data from the sensors to the BTMS. Section 9 discusses the overall integration of BTMS, while Section 10 brings to attention the legal issues when it comes to attacks against patient data. Section 11 is a briefing of solutions and demonstration sites and along with unfulfilled scenarios. Following up comes Section 12 with a presentation of the requirements mapping, and lastly, Section 13 concludes the whole deliverable D4.5 and what will be done in the future.

3.1 Vocabulary

Table 1 - Vocabulary

CSMS	Cyber Security Management System
BTMS	Building Threat Monitoring System
DDoS	Distributed Denial of Service
DNP3	Distributed Network Protocol 3.0
DoA	Description of Action
DoS	Denial of Service
ENISA	European Network and Information Security Agency
EPROM	Erasable Programmable Read Only Memory
ER	Emergency Room
GDPR	General Data Protection Regulation

HMI	Human-Machine Interface
HVAC	Heating Ventilation and Air Conditioning
IACS	Industrial Automation and Control System
ICS	Industrial Control System
ICT	Information & Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Equipment Device
IP	Internet Protocol
IR	Infra-Red
IRBC	ICT Readiness for Business Continuity
ISMS	Information Security Management System
ISO	International Organization for Standardization
LAN	Local Access Network
LED	Light-Emitting Diode
LPWA	Low Power Wide Area
LVM	Light-weight Virtual Machine
MAC	Media Access Control
MFA	Multi-Factor Authentication
MQTT	Message Queueing Telemetry Transport
NB-IoT	Narrowband-Internet of Things
PDA	Personal Digital Assistant
PHI	Protected Health Information
PII	Personally Identifiable Information
PLC	Programmable Logic Controller
PM	Particulate Matter
PP	Protection Profile
RAM	Random-Access Memory
RTU	Remote Telemetry Unit
SCADA	Supervisory Control and Data Acquisition
SKMA	SCADA Key Management Architecture
ST	Security Target
TOE	Target of Evaluation
TRL	Technology Readiness Level
TTL	Transistor-Transistor Logic
UV	Ultra Violet
VM	Virtual Machine
WAN	Wide Area Network
WSN	Wireless Sensor Network

4 Requirements

In this section are described the requirements defined for T4.3. These requirements need to be fulfilled for the final solution. The requirements are described in Deliverable 3.4 and DoA for T4.3.

4.1 Requirements from requirements analysis

In Deliverable 3.4, "Initial requirements analysis" the requirements for the project are defined. Listed (Table 2) are the requirements that directly influence the solution of the Intrusion and fire detection system for T4.3.

Table 2 – Requirements from requirements analysis

Number	Requirement title	Notes
1.	The solution should, in no way, actively compromise communication between the data collection system and the testbed sensors, or the functionalities of, medical devices and other existing infrastructure.	Threat-prevention, Threat detection,
2.	Data transferred between medical systems will likely contain sensitive patient information. When the solution performs analysis of this data for intrusion detection purposes, this is a form of personal data processing. Therefore, patient privacy should be respected by the software.	Threat-prevention, threat detection, incident response, internal processing rules
3.	Alerts shown to operators should be sufficiently informative so that they can make an informed decision on how to respond.	Incident response, interoperability
4.	Alerts for the most relevant threats with information about the likelihood of risks	Risk prevention
5.	Detect dangerous situation: - Flooding and flame; - High/low temperatures; - High voltage level supply; - Pressure, humidity; - Gases; - Movements; - IR, UV; - Sounds; - The crowd in panic.	Threat-detection, physical threats prevention

4.2 DoA requirements

From T4.3 the data collection system from ICS, SCADA, and smart building sensors description of the DoA, the following requirements of the solution are described:

- Implementation of the data collection both from SCADA systems and individual sensors

- To provide data regarding the air cooling, power supply systems, and fire detection systems
- Implementation of the data exchange module for communicating with the building's monitoring system
- Enabling data collection from smart building sensors to the BTMS

4.3 Solution requirements

Looking at the requirements from deliverable D3.4 and T4.3 and combining them, we get the following requirements that the solution must handle:

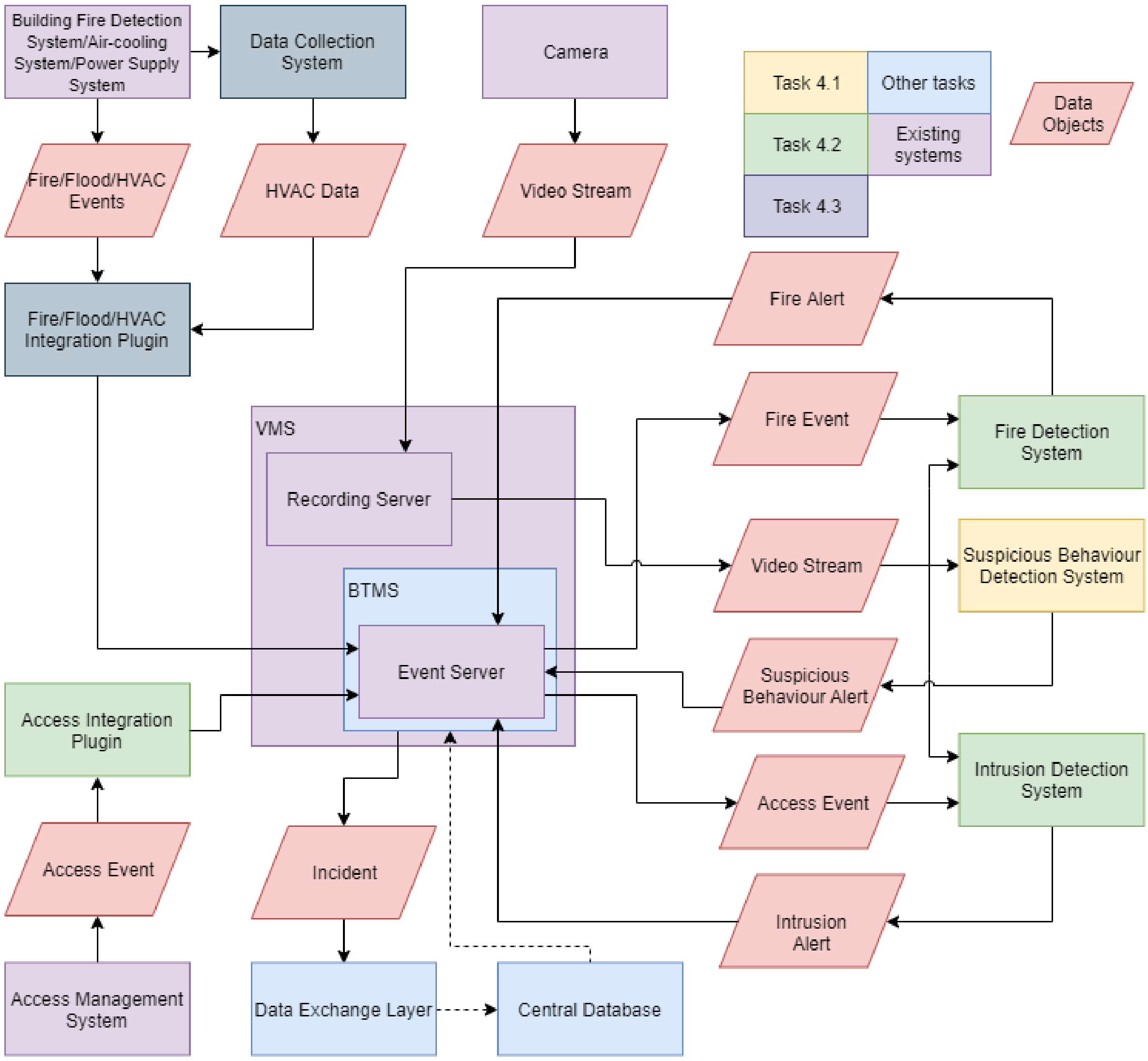
Table 3 describes the requirements for the proposed solution, as seen below.

Table 3 - Requirements for the solution

Requirement Number	Description
R1	Efficient monitoring in areas like power generation, transmission and distribution using a SCADA system
R2	Supervision and monitoring of the process cooling in the power plant's hospital to avoid dangers or risk due to a system failure
R3	Send alerts in case of detection of: - Fire; - Flood; - High/low temperature; - Humidity
R4	Supervision of the fire, power and cooling systems

Figure 1 presents how the Task 4.3 solution matches with the overall solution of the WP4. It illustrates the connection between Task 4.1 and Task 4.2 and shows how they are connected to the building systems and other tasks.

Figure 1 - Solution overview for T4.1 and T4.2 and how they connect with building systems and other tasks



5 Solution description

Based on the Solution requirements 4.3, we must use a SCADA system for monitoring the database. Requirement 2 from the solution requirements states that the system needs to be able to supervise and monitor the process cooling in the power plants of the hospital to avoid dangers or risk due to a system failure.

The SCADA system includes:

- HMI: a device that displays the process data to a human operator, and with this device, the human operator could monitor and control the process.
- Computer: a supervisory system that acquires data on the process and sends the command or control to the process.

- RTUs: connects to sensors; analyses and interprets the sensor signals to digital data and sends the data to the supervisory system.
- PLC: used as a field device.
- Various process and analytical instrumentation.

Following up, we will describe the SCADA system for the BTMS environment which will be used to transmit data to the SAFECARE platform. The SCADA is a system that works as a software and hardware architecture that is used in many ways for industry.

Some characteristics of SCADA are:

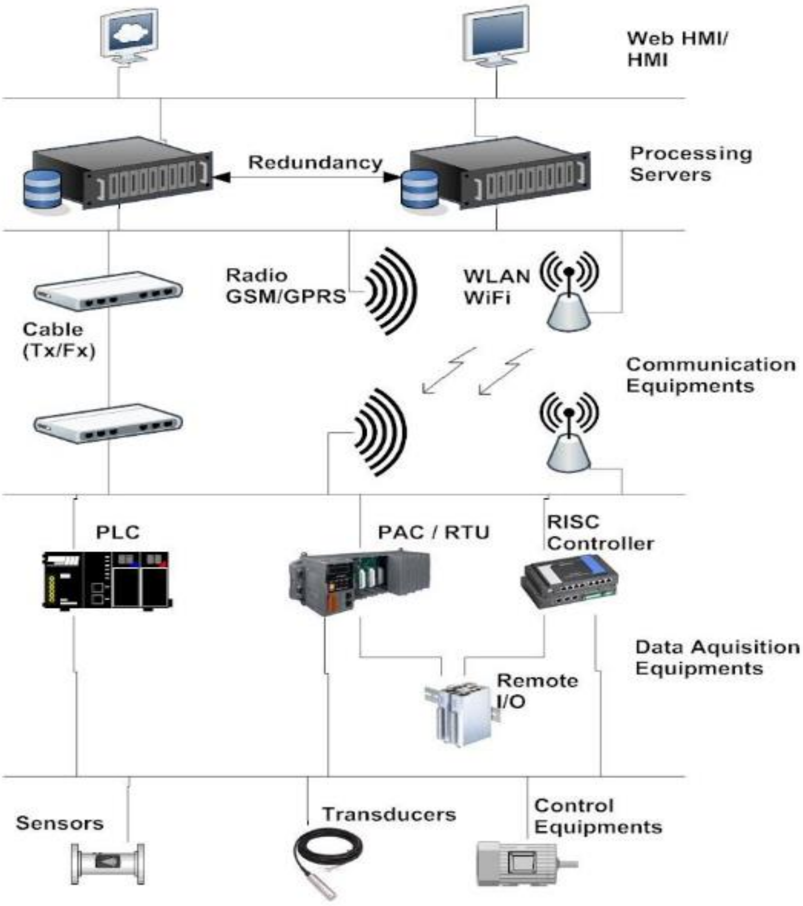
- Process real-time data, monitor, gather;
- Record specifications into a log document;
- Control mechanical procedures locally or remote areas;
- Legitimately connect with other devices, for example, sensors, valves, siphons, engines, and progressively through human-machine interface (HMI) programming.

SCADA systems are extensively used in the management of critical infrastructures. Recently, there is little understanding of protecting SCADA systems from malicious attacks. Here it is described the constraints and requirements for SCADA security and proposes a suitable architecture (SKMA) for secure SCADA communications.

A SCADA system consists of various entities communicating with each other. These entities are different in purpose and design, varying from an RTU (Remote Telemetry Unit) that collaborates with the physical environment, to an HMI that operators interact with.

In the SCADA diagram from Figure 2, there can be noticed the sensors which will be used in the project, Programmable Logic Controllers (PLCs) or Remote Terminal Units (RTUs), used for processes automation (PLC), respectively makes the connection with the supervised equipment, read the position open/closed of a relay or a valve and read measurement units (RTU). Also, HMI has the role of gathering, combining, and structuring the information from the PLC through a communication form.

Figure 2 - SCADA Architecture



- **Remote Telemetry Unit**

RTUs are devices composed of a microprocessor that controls sensors and actuators that interact with the physical environment is mentioned above in the diagram with SCADA components.

RTUs communicate with other entities in the network. This communication is two-way, with the RTUs typically allowing settings to be altered and commands to be transmitted to the sensors or actuators of an RTU.

RTUs have limited processing power and memory. RTUs are operating industry-standard protocols on 16-bit Microprocessors with 8 kilobytes of RAM (working memory) and 64 kilobytes of EPROM.

- **Master Stations**

The master station is a node that delivers supervisory control of an RTU. The master station is superior in a communication hierarchy.

The structure of a SCADA system usually consists of one central master station that communicates with a hierarchy of other nodes, including sub-master stations and RTUs.

Master stations and sub-master stations are computers with resources. These systems typically operate on commodity hardware and operating systems.

- **Human Machine Interface (HMI)**

The HMI is the device that is being used to interact with a SCADA system. HMIs for SCADA systems have been developed utilizing a full circle of client technologies, including PDAs, web browsers, and Desktop PCs.

- **Historian**

Historian is a database of historical data from the SCADA system. It is updated by the master station and can be accessed from the HMI. The Historian operates on identical hardware to the master station.

- **Communication Channels**

The network topology of a SCADA system is highly structured. The available communication channels between nodes are known in advance. In a SCADA system, there is no need to support ad-hoc communication between nodes. Nodes are joined in a managed fashion. A detailed description of the communication channels in a SCADA system is outlined below.

- **Security Requirements**

There is a specific criterion based on the investment-result ratio between the safety and comfort level provided by any suitable solution. The confidentiality, integrity, availability, and authentication levels required will be determined by knowing the concrete application, considering the environment too. It is essential to reach the balance between security levels, costs, and the possibility of installation. For example, the sensors need higher processing power for making transactions. When looking at the security of a system, the requirements can be classified in terms of:

1. **Confidentiality:** Limiting access to information or resources to people.
2. **Integrity:** Ensuring that the data has not been altered (data integrity), and the origin has not been disturbed (origin integrity or authentication). Integrity also includes user authentication.
3. **Availability:** The ability to use the information or resource desired.

6 Scenarios

This section will present cyber-physical scenarios defined in Deliverable 3.6. D3.6 presents a description of all the scenarios, along with the methodology of how the scenarios are defined, as well as the strategic and technical scenario for each of the nine scenarios.

6.1 Scenario 1

The first scenario`s main objective is to cause damage in the power supply of the hospital to precipitate and energy breakdown. The attacker can be an external person who conducts the attack to have some gain (hacker) or an employee who has malicious intentions or makes a mistake.

To get the information to carry out the attack, the attacker can utilize social engineering, internet research, etc. Social engineering refers not only to person-to-person interaction but also to network interaction using, for example, social networks (Facebook, LinkedIn, and so on), or even phishing emails.

All the information collected is used by the attacker for physical or cyber access to the PLC. This can be done through network scalation privileges or impersonating a PLC maintainer, for example. After assuming a controlling position, provoking a fire, a short circuit on the energy cabinet (physical) or uploading firmware, or even sending wrong controls to the PLC (cyber) will cause an energy breakdown for many systems, as it was intended. In the situation, the fire module sensor could be used to detect threats of this kind.

Furthermore, the criticality of this attack is very high since the deactivation of energy may cause safety and health issues: without energy, health service needs to stop partially or completely, even in critical situations.

6.2 Scenario 2

This scenario describes the physical attack of setting a fire in the hospital in order to start evacuation of the hospital and use the caused confusion for accessing the computer room. In this way, the attacker can steal the data, damage the computer room or any other hospital asset, and take advantage of these actions. In order to perform the attack, the attacker first needs to detect the computer room. After that, the attacker sets the fire and breaks in the computer room. A USB key with an installed malware will get control of the server and copy patient records. After the completion of the copying the database is finished, the attack ends.

In order to prevent such a situation, it would be adequate to place a door sensor at the entrance, so such an attack can be immediately detected, and an alert will be sent to the BTMS. In this case, the special forces can react fast and catch the intended attacker.

6.3 Scenario 3

This scenario targets the medical devices within a hospital. In this way, four technical scenarios are defined within Scenario 3. When an attacker performs an untargeted attack, the source is not defined: the access points can be services or clinical functionalities, and the attacker can be any type. The aim of the attack is extortion, sabotage or even intimidation.

6.3.1 Technical scenario A

In this scenario, the attack begins with physical access, and social engineering techniques are used to enter in the technical room. Also, the attacker opens a backdoor to allow future attacks. This attack also targets the patient, which is directly affected. The patient's trust in the healthcare facilities may be affected, which is concerning for the hospital. For this case a door sensor would be appropriate to be used for the security of the hospital room and the patients.

6.3.2 Technical scenario B

In this technical scenario, social engineering is utilized to obtain information regarding the hospital`s infrastructure. In this way, the attacker could exploit the system`s vulnerability, gain administrator privileges and cause hardware failure.

6.3.3 Technical scenario C

In this technical scenario, social engineering by phone is being used in order to get information from the employees. The attacker will try to get access to an employee’s workstation to change software parameters in order to harm patients by system misbehaviour.

6.3.4 Technical scenario D

In this technical scenario, the attacker will utilize devices in order to access the data store in the hospital`s database.

6.4 Scenario 4

This scenario describes the importance of the air-cooling system inside a hospital and presents the attack of taking out the air-cooling system of the hospital in order: to compromise surgery rooms, introduce a biological contaminant; and taking out data centers. To perform this scenario, the attacker needs to identify and access the PLC of the air-cooling system. When the air-cooling system is compromised, the temperature will increase rapidly, and a lot of assets can be compromised. For security measures, it is necessary to plant in each hospital room various air-quality sensors to check the temperature, the humidity, and certain dangerous gas concentrations to prevent the attacker from hacking the air-cooling system and the safety of the patients.

6.5 Scenario 5

This scenario describes a terrorist attack of planting a bomb in the hospital. In this way, the critical facilities of the hospital are disabled. The important accomplishment is to locate and access the place where to plant the bomb. In this case, video cameras and infrared sensors will be placed according to specific places, which might be targeted by the attacker, such as a patient's room or hospital haul to check for any bombs.

6.6 Scenario 6

This scenario describes the theft of data from hospital equipment by someone that works inside the healthcare institution and video cameras, and fingerprint sensors will be of usage for the detection of people outside of the hospital institution.

6.7 Scenario 7

In this scenario, the attacker accesses the medical device, and using reverse engineering identifies a vulnerability and exploits it. After that, the vulnerability is disclosed, a fact that damages the vendor`s reputation. The exploitation can also impact the functionality of the medical devices, which can potentially harm patients and even staff.

The two technical scenarios within this scenario describe the attack of obtaining access to an IoT device.

6.7.1 Technical scenario 1

In this scenario, the attacker can exploit the medical device in order to alter its software and cause disruptions in health systems.

6.7.2 Technical scenario 2

In this scenario, after the vulnerabilities of the medical devices are identified, the medical device system is changed, or a denial of service is launched to interrupt the health system.

6.8 Scenario 8

This scenario presents an example of an attack that occurs when badges/credentials are stolen. In this way, medical data records and restricted areas of the hospital can be accessed. The attacker will easily sell, modify or delete health records. The assets can be affected as the hospital facilities may be damaged or stolen to sabotage the medical activities.

The deletion or modification of data maybe sometimes the result of an unintentional error in the data management. Some employees can conduct a data loss, but it will have the same impact on the institution as the attack described above.

6.9 Scenario 9

This scenario describes a possible attack directly impacting the main hospital and its district may target the hospital`s network WAN connectors and interfere with this daily communication. The connections are destroyed and disabled, or the data sent to the National Agency can be modified.

7 Data Exchange Format

Data exchange [7] is a term used in data processing and stands for the forwarding of data between organizations and companies in a purpose-specific standardized form. While predominantly used in the context of electronic procedures, it is independent of the form of the data and the form of transmission. Formats and structures of the exchange data (→ exchange formats) are usually defined and standardized under the responsibility of committees, associations or other special-purpose associations.

The data collection system described in the deliverable D4.5 will use the EDXL (Emergency Data Exchange Layer), which represents a series of XML-based messaging standards that encourage emergency data sharing amongst governing entities and the full scope of emergency-related associations. Created by the OASIS International Open Standards Consortium, EDXL standardized messaging formats for interchanges between these third parties [8].

The EDXL series includes the following individual standards:

- EDXL-DE (EDXL Distribution Element);
- EDXL-HAVE (EDXL Hospital Availability Exchange);
- EDXL-RM (EDXL Resource Messaging);
- EDXL-RIM (EDXL Reference Information Model);
- EDXL-SitRep (EDXL Situation Reporting);
  EXDL-TEP (EDXL Tracking of Emergency Patients).

Data collection systems from ICS, SCADA, and smart building sensors are managed within WP4, generating alerts and talks with BTMS module inside WP4 before any involvement of data exchange layer. After this, BTMS generates incidents that are then sent to the data exchange layer through MQTT.

Table 4 describes the event types which could appear in the BTMS system.

Table 4 – Event table

Element Name	Schema Data Type	Restriction	Notes
type	string		specifies the message type: INCIDENT
ID			Unique identifier for the correlated incident
events	string		Collection of events, from 1 to many other
event-> description	string		Description of the events
event->detector	string		SAFECARE component detecting the event Specify if the event (alert/incident) is from physical or cyber domain
event-> date	dateTime	The Date Time combination must include the offset time for time zone.	Date and time at which the event occurred the first time
event-> title	string		Description of the specific event
event->severity	string		Specify the severity of the event: LOW, MINOR, MAJOR, CRITICAL
event-> type	string		Description of th event considering the EDXL specifications
event->ID	string		unique ID related to the detector

event-> assets	**string**		**Contains a list with all the assets involved in the security event**
event->assets-> category	**string**		**Asset category considering the EDXL specifications**
event->asset->name	**string**		**Asset name considering the EDXL specifications**
event-> location	**number:** **1 - indoor,** **0 - outdoor**		**Asset positioning considering the EDXL specifications**
event->location->type	**string**		**Specify the event location type: indoor or outdoor**
event->location->position	**GPS coordinates**		**GPS coordinates if the event happened outdoor**
event->sensor	**string**		**Contains information about the sensors which detected the event**
event->video analytics	**string**		**Contains data related to video analytics performed by VMS**
event->video_analytics->camera_id	**string**		**unique ID of the camera responsible for event detection**
event->video_analytics->number_of_people	**string**		**Number of people detected**
event->video_analytics->security_event	**string**		**Specifies the type of security event detected**

events->sensor_data	**string**		**Specifies the data collected from the sensor**
event->smart building	**string**		**Contains information regarding the smart building room, sensors placed in etc.**
event->smartbuilding->sensor_id	**string**		**unique ID of the smart building sensor**

8 Devices and Setups

For better integration with the entire project, various sensors are required to be installed and used inside the hospital's rooms. Numerous precious pieces of information can be gathered to create a full/bigger picture regarding different parameters in the building or the room. Data is collected from different sensors or modules directly connected to the Raspberry Pi development boards. Next, the Message Queuing Telemetry Transport (MQTT) protocol is used to send the gathered information to the Grafana platform. Grafana can support different backends that can store time-series data. One of them is InfluxDB, an open-source database specially created to store time-series data from IoT sensors, application metrics or real-time analytics. A close connection between Grafana and InfluxDB is made this way.

8.1. Test Bed Sensors

Firstly, the sensors and devices that detect various aspects regarding the room's characteristics and the connection to other rooms or lobbies are being presented. The administrators of the hospitals can see when and if a door inside a certain room is open or closed with the following sensors or devices [9]:

- Raspberry PI boards collect data from numerous sensors or devices. Then, the collected information can be sent with the MQTT protocol [10] to the Grafana platform [11], where they are processed and analyzed.
- A Magnetic Door Switch Set [12] can be connected to the development board. This piece of equipment is used to detect and record the moments when the door is open or closed.
- Surveillance cameras represent other devices that can record data. They can be mounted inside the rooms, to film the door or other important elements inside them. The recorded videos can be stored on a server for the situations when they are needed to resolve different security problems.

- An Optical Fingerprint Sensor [13] can be placed next to the door, outside the room, in plain sight of the camera. This optical fingerprint sensor can capture and compare different people's fingerprints. This is only a security measure; the sensor does not work with the Raspberry PIs, and the captured images are not sent to Grafana. It is a system used in conjunction with a matching system to enable efficient authentication for secure devices or spaces, allowing only a small number of people to enter a specific area - medical staff, administrative staff, patients, or family members. It connects the microprocessor or Transistor-Transistor Logic (TTL) communication system and sends data packets to take pictures, detect prints, hash, and searches. It can store more than 100 fingerprints with embedded Flash memory.
- A fire sensor [14] is another security feature that can be found inside a hospital room. As the name suggests, the purpose of this sensor is to detect the unfortunate case when a fire appears because of many different reasons.
- The last three entities, the surveillance cameras, fingerprint sensors, and the fire sensor can be considered to represent adequate security measures used to prevent and detect inappropriate behaviour or risky scenarios.

Secondly, the sensors and the devices that monitor the parameters inside a room are being presented. The detection principle is the same: the MQTT protocol is used to transmit to Grafana data collected from connected sensors or devices to the development boards. Information about the humidity, temperature, light, dust, movement, sound, fire, or gases can be gathered. An idea about the conditions inside of the room will be presented below, with the help of the sensors:

- A temperature sensor [15] that transmits data to Grafana is installed, having the primary purpose of detecting the ambient temperature. This is an important aspect because a constant temperature must be kept according to every patient's needs or every room requirement - a too-warm room can cause problems to a person with cardiac disorders or to server equipment.
- An IR (InfraRed) based movement sensor [16] can detect when someone enters the room or when the patient walks inside his/her space. This can be considered an additional security measure because it can log the time into Grafana.
- A dust particle sensor [17] can detect the air composition, presenting its structure. The air quality has increased importance when talking about a patient's recovery because they need to breathe purified air, without different sized PM (particulate matter). These small particles can enter a person's body and blood, causing unwanted reactions.
- A module for Adaptive Light Analog Sensor [18] can detect the natural light quantity inside a room, allowing the person inside of if to choose whether to turn off or on the artificial lights system.
- A sound sensor [19] is useful for those situations when the patient is alone in the room, and he/she screams because of the health issues it has. This way, first responders and medical staff can resolve the problem in a short period, without the risk of having a too slow intervention.

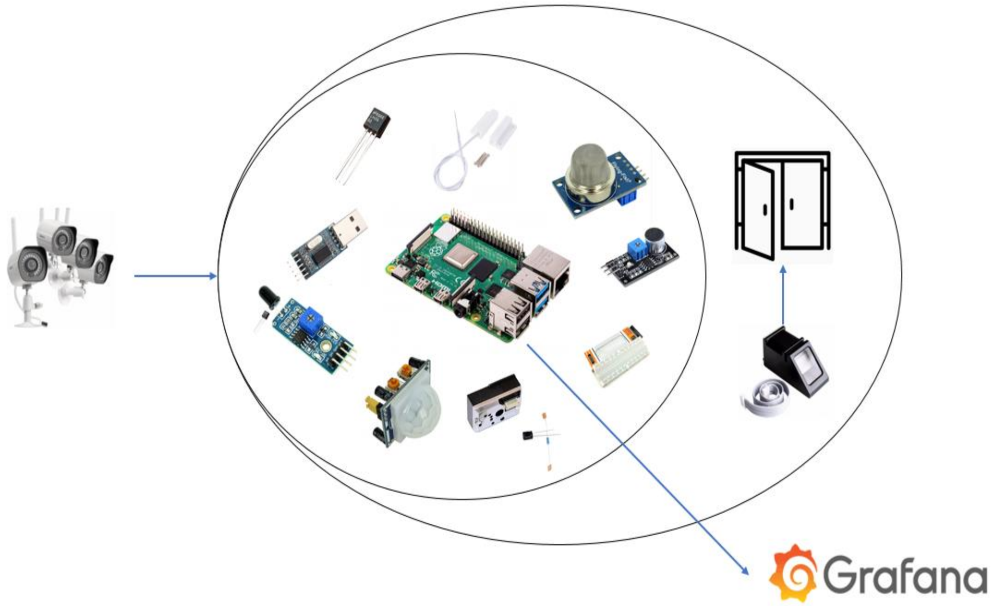
- A UV (Ultra Violet) light sensor [20] can detect and measure the intensity or power of the incident ultraviolet radiation, where the wavelength is between 280 and 390nm. The UV light has a significant importance when thinking about the sterile environment inside the hospital, and it can eliminate a big part of the pathogens inside different rooms.
- A 4G NB-IoT (Narrowband-Internet of Things) communication module [21] can be fitted on the Raspberry PI board for more available data transmission between machines. NB-IoT [22] represents a standards-based low power wide area (LPWA) technology developed in order to enable a wide range of new IoT devices and services. NB-IoT improves the power consumption of user devices, system capacity, and spectrum efficiency, especially in in-depth coverage. The battery can last more than ten years and can be supported for a wide range of use cases.

Besides the equipment as mentioned earlier, other parts are required, such as serial USB adaptors, breadboards, male-male wires, and male-female wires.

8.2. Sensor Analytics

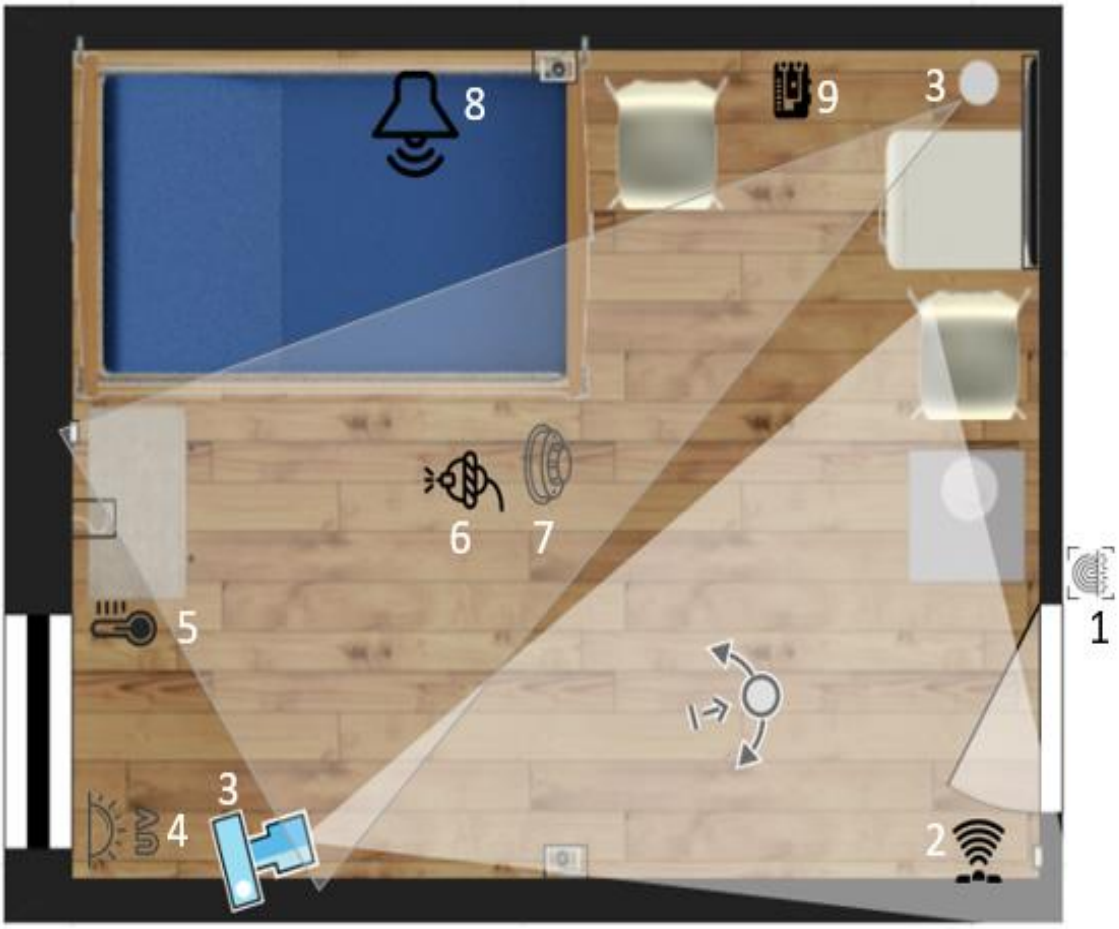
A schematic with all the sensors, as mentioned above and devices is presented in Figure 3. Some sensors are connected to the Raspberry PI boards, and the collected data is sent to Grafana. The surveillance cameras monitor the entire room, including the entrance and the fingerprint sensor, as well.

Figure 3 - The functional scheme of the system with the required sensors



The setup of the system mentioned above architecture can be seen in Figure 4. The sensors are placed into a hospital room. Each sensor is explained under the picture, in the legend.

Figure 4 - Schematic representation of sensor placement inside a hospital room



Legend:

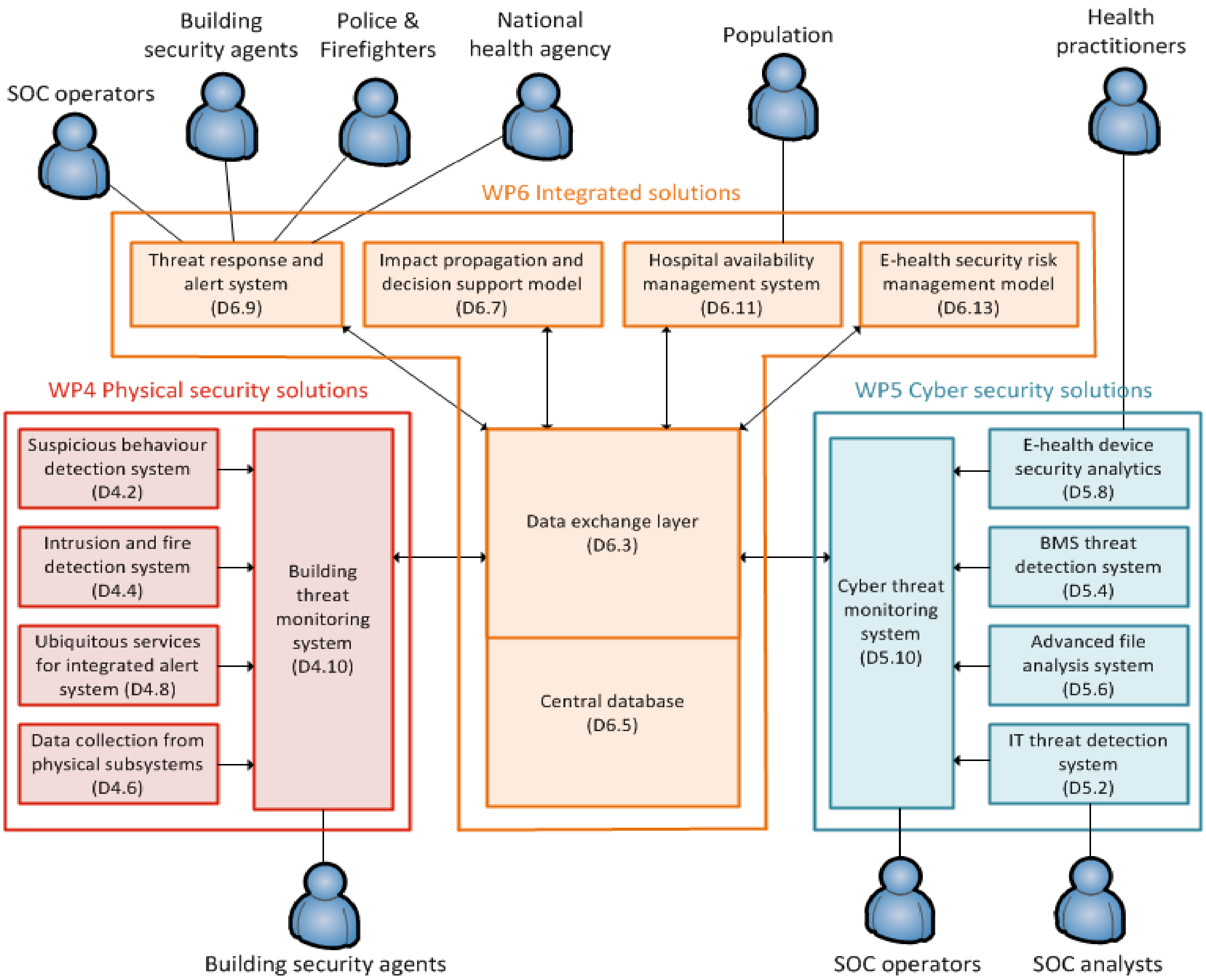
1. Fingerprint scanner sensor
2. Magnetic Door Switch and movement sensor
3. Surveillance cameras
4. UV sensor
5. Temperature sensor
6. Light sensor
7. Fire and gases sensor
8. Sound sensor
9. Raspberry PI board and other devices: 4G module, adapter

Grafana is an open-source [23] platform for visualizing running data analytics in real-time. It can be connected by using various types of databases such as Graphite, Influx DB and so on. There is also a possibility of making alerts and very detailed dashboards with all the data which must be illustrated on the platform. The main feature of the platform is for monitoring in real-time any type of data that might be needed. The testbed sensors from the SAFECARE laboratory will send data through the MQTT protocol, and afterward the metrics from the sensors will be shown on the Grafana dashboard. The database of the stored data on the platform will be InfluxDB.

9 Integration with BTMS

For the Integration of BTMS, BEIA will use the automation solutions from the Arrowhead Tools project for the transmitting of data of each sensor connecting to the Raspberry Pi. For this process automation and digitalization and automation solutions are used by addressing the engineering methodologies of Arrowhead. The Arrowhead Framework technology architecture is implemented on the basis that local clouds can consist of system of systems. Furthermore, the SCADA BTMS implementation will be described as seen in (Figure 5), the global architecture of the system.

Figure 5 - Global architecture of CCS


SOC operators
Building security agents
Police & Firefighters
National health agency
Population
Health practitioners
WP6 Integrated solutions
Threat response and alert system (D6.9)
Impact propagation and decision support model (D6.7)
Hospital availability management system (D6.11)
E-health security risk management model (D6.13)
WP4 Physical security solutions
Suspicious behaviour detection system (D4.2)
Intrusion and fire detection system (D4.4)
Ubiquitous services for integrated alert system (D4.8)
Data collection from physical subsystems (D4.6)
Building threat monitoring system (D4.10)
Data exchange layer (D6.3)
Central database (D6.5)
WP5 Cyber security solutions
Cyber threat monitoring system (D5.10)
E-health device security analytics (D5.8)
BMS threat detection system (D5.4)
Advanced file analysis system (D5.6)
IT threat detection system (D5.2)
Building security agents
SOC operators
SOC analysts

vmSCADA™ [24] is another classification of HMI contribution containing items and administrations empowered by the intensity of virtualization. VMs are motors for both Virtual Managed SCADA Systems and Virtual Managed SCADA Services. In order to interact with the HMI, the information is written to an Excel database with a script written in Python. The script continuously updates the data provided by the simulation engine to a local database. If any input tag is modified, the python script runs a new simulation and updates the local database with a set of values corresponding to the updated power system. This script can be used on multiple platforms. To manage multiple HMIs that can run various simulations at the same time, it is used discrete event-driven simulations to manage system status. Event-based discrete simulation is when separate events make changes in the system. Usually, these events are relevant to a SCADA system and are unevenly distributed over time. Some examples include a change of charge in an electrical system or the production of energy in a nuclear control center. Because there are variables that continuously change the simulation, an event is used with a scheduler in Python at the different instances of the simulation that is running. A simulation engine continuously creates scenarios dependent on HMI changes.

For the systems implemented in hospitals, SCADA data collection systems are used, and preferably the data should be integrated with a VM. One example would be the vmSCADA® which utilizes a virtual environment to provide superior features for industrial control systems by "sharing" parts of the server to what will constitute a VM. The way a virtual environment is created, and the things needed to build it can be seen in the diagram below (Figure 6), showing the experimental part. It consists of an Allen Bradley PLC, the Micrologix 1400 B Series, and four VMs. The PLC has physical ports of entry and exit. The input ports are connected with two buttons and two switches to provide digital inputs to the PLC. The output ports are connected with four different color LEDs: red, orange, green and blue.

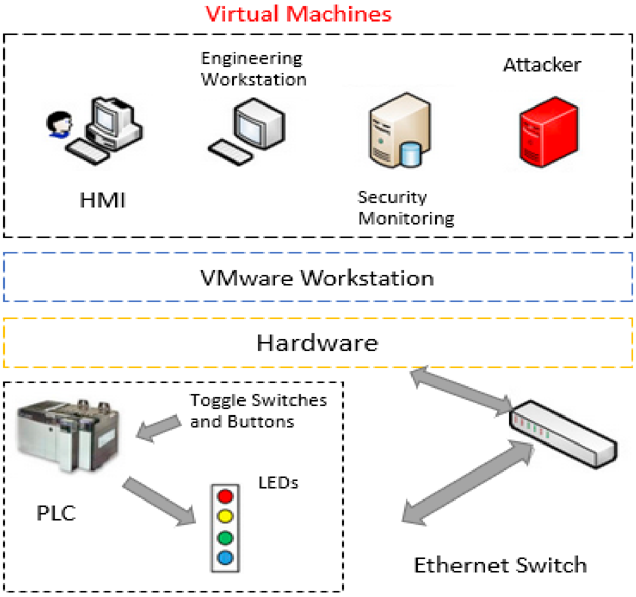
The PLC and the physical computer [25] are connected via an Ethernet switch. Two VMs are running SCADA services - human-machine interface software, and engineering workstation running ScadaAfcon. Afcon Software [26] represents a global provider for services in smart management and automation systems. The Solutions used by Afcon are the following:

- PULSE™ Smart BMS for Smart Buildings and Smart Campuses;
- PULSE™ Smart IoT;
- PULSE™ Smart City;
- PULSE™ Smart Energy;
- PULSE™ Smart Security and HLS;
- PULSE™ Smart Industrial Automation;
- PULSE™ Based Customized Solutions.

Technical features for Afcon are: Scalability, Reliability, Security and Cyber Protection, Flexible Deployment, Device Gallery, Localization, Open Platform, GIS presentation.

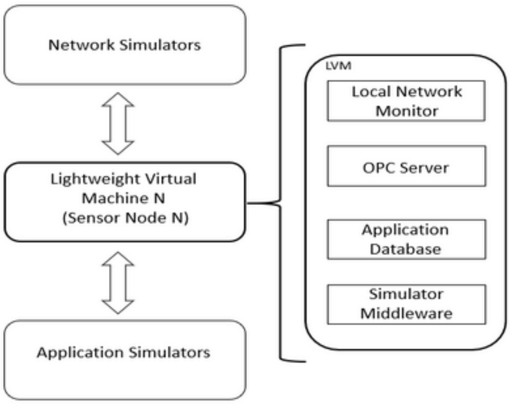
One of the VMs is for security monitoring and is running Wireshark to capture all network traffic; the last VM is a simulated attacker machine that can communicate with the PLC and send messages to transfer logic program and alter physical process state (LEDs in this case).

Figure 6 - The experimental setup for the evaluation of a VM



A light-weight virtual machine (LVM) [27] simulates the operating system of each sensor. The database contains information generated by a simulation engine, and the script changes in the simulation process depending on the messages sent from the front-end. First, the back-end architecture is described, then the front-end architecture. The network is also simulated by communication simulators, which can be connected to security analysis tools. These network analysis tools simulate how potential attackers can obtain information and compromise the SCADA system. Thus, as seen in the example below (Figure 7), in hospitals such systems would provide a high level of security of the data, which is being transmitted, as it is locally.

Figure 7 - Implementation of LVM



10 Data Availability for Test

Because of the targeted attacks against information systems and the emergence of advanced persistent threats, the invasion of patient privacy became a growing concern in the field of big data analytics. For this reason, it is crucial for healthcare organizations to manage and protect patients' personal information and address their risks and legal responsibilities regarding personal data processing. Below [28] are presented the main traditional methods for privacy-preserving in big data:

a. **De-identification** This method involves rejecting any information that may disclose patient identity. This can be done either by the removal of specific identifiers of the patient or by the patient himself by verifying that enough identifiers are deleted.

b. **HybrEx** execution mode is a model for privacy and confidentiality in cloud computing. This method allows the use of public clouds only for the organization's data considered non-sensitive and public, more precisely when the organization declares that there is no privacy risk in exporting the data and performing computation on it using public clouds. On the other hand, for an organization's sensitive and private data, the model executes its private cloud. If an application requires access to both private and public data, the application partitioning is performed so that it runs on both the private and public cloud.

c. **Identity-based anonymization** involves the process of encryption or removal of personally identifiable information from the data sets so that the identity of the person remains anonymous. The main difficulty of this method is to combine anonymization, privacy protection, and big data techniques in order to analyze the use of data while protecting the identities

The health sector collects masses of personal data in order to deliver services to patients. Although healthcare is a highly sensitive and private domain, test results are often shared widely in order to reach a diagnosis. Unfortunately, most of the time the patients do not know how their personal information is collected, who has access to it and where it is stored. To address these issues, General Data Protection Regulation (GDPR)[29], Article 1, recital 7 says that "natural persons should have control of their own personal data", which implies requirements for the processing of personal data and provides the data subject with certain rights (e.g., right to access, etc.). Also, according to Article 6, personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject [30].

Although GDPR will affect almost all industries, in the health domain the new regulations give every patient more control over their personal data and provide the patient with information on how his data is used. Under the GDPR, healthcare organizations set requirements on how their patient's personal information is collected and stored. While the changes introduced by GDPR affects mostly digital data, paper records are also affected.

Under GDPR requirements, organizations have just 72 hours to gather all related information and report data breaches to the relevant regulator. Within 72 hours after a data breach has been discovered, an organization must: carry out a thorough investigation, inform regulators and impacted individuals of the breach, identify what personal data has been impacted and how, and draft a comprehensive containment plan.

With data collected from different sources such as doctor's surgeries or specialized healthcare organizations, the data footprint of a patient is highly fragmented.

The main feature underlying the GDPR is to protect the personal and sensitive data from being used. In this way, healthcare providers will have a more comprehensive view of their patients, which could lead to a better and accurate diagnosis. Also, a reduction in costs can be achieved by making a correct diagnosis and providing the appropriate treatments.

A better structure of patient data can be hugely beneficial to healthcare professionals. The GDPR introduces a framework that determines under which conditions data can be collected and foresees that personal data is being deleted, once it is not necessary anymore.

On the healthcare professionals' side, social networks are increasingly being used to deliver patient support and care. Social platforms such as WhatsApp are regularly used by healthcare professionals in order to send and receive patient data. In this case, GDPR [31] can be breached because as patient's private information moves across the network, confidential data may reach outside the EU.

11 Scenarios and Demonstration sites

From the analysis of the scenarios in Section 7, it shows which steps of the scenarios that the solutions of Section 6 in principle can handle. This section discusses whether the available devices, set-ups or data at the demonstration sites may limit our ability to fulfill the scenarios.

From the list of devices, both camera, access control system, access management system and building fire detection system, heating systems and ventilation system available at the demonstration sites, and from the commitment to further provision pledged by the demonstration sites, no major concerns are fulfilling the analyzed scenarios.

11.1 Unfulfilled Scenarios

There are specific scenarios where attackers impersonate vendors or staff members in order to gain access to private credentials from the computers. These kinds of intrusion incidents are not covered by the system beyond using surveillance cameras, as the computers in a hospital are usually not protected. There are also plenty of times when the intruder can access the network easily because Wi-Fi passwords are written on pieces of paper and posted everywhere in the perimeter of the building.

12 Requirements Mapping

From the DoA, several mappings are described in Table 5 for physical security solutions. These requirements are the overall solutions that should contribute to the entire system. And a short discussion on each description is overviewed shortly how the data collection system from ICS, SCADA, and smart building sensors will be implemented and under what circumstances.

Table 5 -Requirements description

Requirement number	Description
R1	As described in Section 4.1, the requirement will refer to the security between the data collection system and the testbed sensors.
R2	Following up, the data sent from the medical systems requirement two will take into account the protection of patient data.
R3	The alerts will be informative and precise enough so the operator can react fast to them, and the data exchange format EDXL will be of help for the type of alert data, described in Section 7.
R4	Based on Section 6, various scenarios are described to assure the relevance of the alerts and be as suggestive enough.
R5	Section 8 illustrates the Test Bed Sensors for the SAFECARE Laboratory room, and the implemented prototype will detect dangerous situations, based on the requirement presented in Section 4.1.

13 Conclusions

Concluding what has been discussed in this deliverable, a specification of the data collection system (D4.5) was provided. The next step is to extend the system and enable integration, providing a report regarding the status of the prototype (D4.6). A smart room (laboratory) will be built with all the components of the architecture so that data collected from the sensors can be examined in a secure environment. The door sensor will be used for securing the entrance in the so-called hospital room. Other data such as motion, light, and UV readings will be examined for making the hospital room as comfortable for the patient as possible. The humidity of the air will be measured as well, and a smoke detector will be put for detecting any fire incidents.

The main purpose of a smart hospital room is to simulate various scenarios based on what issues might arise unexpectedly in a hospital room. One example would be breaches of security in the database or the data collection system or even intrusions from a third-party person who might be disguised as a doctor or even patient.

References

[1] More information about the SAFECARE project available at: https://cordis.europa.eu/project/rcn/214348/en

[2] Gorgon, W.J., Wright, A., Aiyagari, R. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *AMA Netw Open*. 2(3).

[3] Mohurle, S., Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science. 8(5).

[4] Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

[5] Drias, Z., Serhrouchni, A., Vogel, O. (2015). Analysis of cyber security for industrial control systems. 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC). doi:10.1109/ssic.2015.7245330.

[6] Rodofile, N.R., Radke, K., Foo, E. (2017). Framework for SCADA cyber-attack dataset creation. Proceedings of the Australian Computer Science Week Multiconference on - ACW'17. doi:10.1145/3014812.3014883.

[7] Ďurčeková, V.; Schwartz, L.; Hottmar, V.; Adamec, B. (2018). Detection of Attacks Causing Network Service Denial. Advances in Military Technology. 13(1), pag. 87-94.

[8] Li, B., Lu, R., Xiao, G., Bao, H., Ghorbani, A.A. (2019). Towards Insider Threats Detection in Smart Grid Communication Systems. The Institution of Engineering and Technology. 13(12), pag.1728-1736. doi:10.1049/iet-com.2018.5736.

[9] Doan, A.H., A. Halevy, A., Ives, Z. (2014). Principles of Data Integration. Saint Louis: Elsevier Science

[10] Emergency Data Exchange Layer: https://en.wikipedia.org/wiki/EDXL

[11] InfluxDB Time Series Data Monitoring with Grafana. (2019, March 11). Retrieved from https://www.influxdata.com/blog/how-to-use-grafana-with-influxdb-to-monitor-time-series-data/

[12] MQTT protocol: http://mqtt.org/

[13] Grafana platform: https://grafana.com/

[14] Magnetic door switch set: https://www.robofun.ro/magnetic-door-switch-set

[15] Optical Fingerprint Sensor: https://www.optimusdigital.ro/en/optical-sensors/1276-senzor-optic-de-amprenta.html

[16] Fire sensor: https://www.optimusdigital.ro/ro/senzori-senzori-optici/110-modul-senzor-de-flacara-.html?search_query=senzor+de+foc&results=7

[17] Temperature sensor: https://www.adelaida.ro/lm35dz-nopb-senzor-temperatura.html

[18] InfraRed Sensor: https://www.optimusdigital.ro/ro/cautare?controller=search&orderby=position&orderway=desc&search_query=Senzorul+de+mi%C8%99care+PIR+HC-SR501&submit_search=

[18] Dust particle sensor: https://www.optimusdigital.ro/ro/senzori-senzori-optici/2447-senzor-optic-de-particule-de-praf-gp2y1010au0f.html?search_query=+Senzorul+optic+de+particule+de+praf+GP2Y1014AU0F&results=1

[20] Adaptive Light Analog Sensor: https://www.optimusdigital.ro/ro/senzori/1420-modul-senzor-analogic-de-lumina-adafruit-als-pt19.html?search_query=Senzorul+de+lumina&results=49

[21] Sound sensor: https://www.robofun.ro/senzori/sunet/senzor-sunet-LM393

[22] UV Light Sensor: https://www.optimusdigital.ro/ro/senzori-senzori-optici/2944-senzor-de-lumina-uv-ml8511.html?search_query=senzor+lumina+uv&results=101

[23] Grafana: https://grafana.com/

[24] 4G NB-IoT communication module: https://www.aliexpress.com/item/32963265498.html

[25] Narrowband – Internet of Things (NB-IoT). (n.d.). Retrieved from https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/

[26] Dayal, A., Tbaileh, A., Deng, Y., & Shukla, S. (2015). Distributed VSCADA: An integrated heterogeneous framework for power system utility security modeling and simulation. 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES). doi:10.1109/mscpes.2015.7115408.

[27] Senthivel, S., Ahmed, I., & Roussev, V. (2017). SCADA network forensics of the PCCC protocol. Digital Investigation, 22, S57–S65.doi: 10.1016/j.diin.2017.06.012.

[28] Afcon: http://www.afcon-inc.com/about-us

[29] Abouelmehdi, K., Beni-Hessane, A., Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1).

[30] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88".

[31] Chassang, G., The impact of the EU general data protection regulation on scientific research, January 2017, ecancer journal 2017, 11:709 DOI: 10.3332/ecancer.2017.709.