Specification of the intrusion detection system

Deliverable 4.3

Lead Author: MS

Contributors: LINKS

Deliverable classification: PU

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

Version Control Sheet

Title	*Specification of the intrusion detection system*
Prepared By	*Milestone*
Approved By	*PEN, CSI*
Version Number	*1.0*
Contact	Barry Norton <bno@milestone.dk>

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
V0.1	16/07-2019	Initial version	MJN	
V0.2	31/07-2019	Second version	MJN	
V0.3	01/08-2019	Added Data Exchange Format	MG	
V0.4	06/08-2019	Small corrections	MJN	
V0.5	22/08-2019	Responses to reviewer's comments	BN	
V0.6	29/08-2019	Responses to reviewer's comments	MJN	
V1.0	30/08-2019	Finishing touches	MJN	

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

1 The SAFECARE Project 5
2 Executive Summary 6
3 Introduction 7
4 Vocabulary 8
5 Requirements 9
5.1 DoA requirements 9
5.2 Requirements from requirements analysis 9
Consolidated 10
5.3 solution requirements 10
6 Solution Description 12
6.1 Intrusion incidents 13
6.1.1 Fraudulent use of access control key 13
6.1.2 Tailgating 14
6.1.3 Breaking through access control by force 15
6.2 Fire incident 15
6.3 Identification capabilities 15
7 Scenarios 16
7.1 Scenario 1 16
7.2 Scenario 2 17
7.3 Scenario 3 17
7.3.1 Technical scenario A 17
7.3.2 Technical scenario B 17
7.3.3 Technical scenario C 18
7.3.4 Technical scenario D 18
7.4 Scenario 4 18
7.5 Scenario 5 18
7.6 Scenario 6 18
7.7 Scenario 7 18
7.8 Scenario 8 19
7.9 Scenario 9 19
8 Data Exchange Format 19
9 Devices and Set-ups 21
9.1 Set-up and scenarios 21

9.2 Known devices and set-ups 21
10 Integration with VMS 22
10.1 Send Data to Central Database 22
10.2 Setting up static devices 22
10.3 Access management system integration 22
10.4 Fire detection system integration 23
11 Training and Test Data 23
11.1 Video data 23
11.2 Access management system data 23
11.2.1 Fraudulent use of access control key 23
11.2.2 Tailgating 24
11.2.3 Breaking through access control by force 24
11.3 Fire detection system data 24
11.4 Training data lifecycle 24
11.5 Deployed data lifecycle 25
12 Scenarios at Demonstration Sites 25
13 Requirements Mapping 26
14 Conclusion 27
15 Appendences 28
15.1 Data exchange format example 28

List of Figures

Figure 1 – Solution overview for T4.1 T4.2 and how they connects with building systems and other tasks 13
Figure 2 - Example of devices in a set-up 21

List of Tables

Table 1 - Vocabulary 8
Table 2 – Requirements from requirements analysis 9
Table 3 – Consolidated requirements 11
Table 4 - Requirements mapping 26

1 The SAFECARE Project

Over the last decade, the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons to impact the population. As Europeans, we know now that we must increase our awareness against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analyzed 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 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

In the SAFECARE solution both physical and cyber security solutions will be made and integrated together. This deliverable is part of the physical solution and covers the specification for physical intrusion and fires, based on the combination of video analytics, access control and other physical sensors. The specification handles all the requirements originally envisioned in the DoA and handles the relevant requirements from Deliverable 3.4, except for providing flooding and a simulation mode, which Task 4.2 has no commitment to do.

For the physical intrusion system, three solutions to detect the intrusion are specified: detection of fraudulent use of access control key, tailgating and breaking through access control by force. For the fire detection system, a solution to detect fires using the surveillance cameras is proposed in two different ways; when a fire is detected, confirm that there is a fire; and, try to detect fires all the time. Solutions of the latter type are inherently limited, and their application should not be prioritised above the use of dedicated sensors in the building fire detection system. As one of the approaches to physical security, alongside others specified later in this work package, only a limited number of the scenarios can be completely covered by the means here described. In particular, Scenario 2 will be completely covered; Scenarios 1, 3, 4, 5, 7, 8 and 9 are partly covered, and Scenario 6 is unrelated. The specifications in D4.1 and D4.5 will handle other paths than those described in this deliverable.

This deliverable also contains the first draft of the data exchange layer to be used between Work Package 4 and Work Package 6. This is still at preliminary description and not the final format. It also describes how the devices will be set up, and how the access management system and building fire detection system will be integrated into the video management system.

Finally, this deliverable discusses what is required within Task 4.2 to fully analyse whether the solutions will be able to handle the scenarios at the SAFECARE demonstration sites. Given the current state of readiness within the use case sites, we document the need for a more thorough description on the devices at the demonstration sites, how these devices are set up, as well as a discussion on the need of data from the devices, as only preliminary devices lists, set-ups and data examples have been received. Despite this caution about the current lack of information, it is still not a direct concern to the solutions, if the needed information is received without much further delay.

3 Introduction

In the SAFECARE solution both physical and cyber security solutions will be made and integrated together. This deliverable is part of the physical solution and will consider physical security concerning physical intrusion and fires. In Section 5 a requirements analysis is carried out on the requirements of Task 4.2 in the DoA and the requirements stated in Deliverable 3.4, correlating the requirements of the two sources, into a single list of requirements for Task 4.2. In Section 6 a description is provided on the different solutions that is to be developed to detect physical intrusion and fires in a healthcare environment, as exemplified by the SAFECARE demonstration sites. In Section 7 is an analysis on how the solutions can help handle the attack scenarios described in Deliverable 3.6, along with an overview of which scenarios that the solutions can help handle. In Section 8 is a description on the data exchange format to be used in the data exchange layer. In Section 9 is a discussion on the devices and set-up descriptions need for the solutions, Section 10 describes how these devices will be integrated with the Video Management System (VMS), and in Section 11 is a discussion on what data is required for the solution from the devices and set-ups as well as the lifecycle of the data. Section 12 discusses the concerns on providing the solutions if the required information of the devices, set-ups and data is insufficient. In Section 13 is a requirements mapping between the requirement of Section 5 and the solutions and functions described in this deliverable.

4 Vocabulary

Table 1 - Vocabulary

Access badge	Card with electronic key used with access control readers and with info of owner printed on the badge
Access control entry point	Physical object blocking the access which can be opened to grant access
Access control key	Key used to open the access control entry point, such as a physical key, access badge, pin code and automatic biometric recognition
Access control point	A complete solution of an access control, including access control reader and access control entry point
Access control reader	Device where a person registers the access control key to get access through the access control point
Access management system	Software solution that handles all access control events from the access control devices
Alert	An event that is raised to be handled by the security personnel
Building fire detection system	Physical fire detection system in place at the demonstration sites and test site
Event	Any message sent from a system to the monitoring system (T4.5 for WP4)
Fire detection system	Fire detection system to be developed in T4.2
Incident	An alert that has been manually raised to an incident by the security personnel, with other appropriate events attached to it
PLC	Programable Logic Controller
VMS	Video management system (e.g. Milestone provide XProtect® as VMS for SAFECARE)

5 Requirements

In this section is described the requirements defined for Task T4.2. These requirements need to be fulfilled for the final solution. The requirements are described in Deliverable D3.4 and in the DoA for Task T4.2.

5.1 DoA requirements

From T4.2 the intrusion- and fire detection system description of the DoA the following requirements of the solution are described.

1. Automate detection of physical intrusion.
2. Integrate access management system and VMS.
3. Integrate fire detection system and VMS.
4. Compliance with implemented solution in simulation site.
5. Store access logs, intrusion alerts and fire alerts in central database.
6. TRL for solution is 7.
7. Improve verification and handling of fire alarms.
8. Send validated incidents to central database.

5.2 Requirements from requirements analysis

In Deliverable D3.4 "Initial requirements analysis" the requirements for the project are defined. Table 2 lists the requirements that directly influence the solution of the Intrusion and fire detection system for Task T4.2.

Table 2 – Requirements from requirements analysis

D3.4 number	Requirement title	Notes
72	Detection of floods and flame	From the DoA, we are only committed to do fire detection and not flooding detection
85, 82	Early detection – as soon as possible or virtually before	
117, 109, 77, 118, 192	Fast and accurate detection and response	
125	Intrusion detection and identification capabilities	(e.g. through CCTV equipment)
17	Operators should be able to manually tweak the configuration to reduce the number of false positives/negatives	
35, 49, 80, 99	Permit learning with already managed events	The detection solutions must either be semi-supervised or supervised machine learning solutions

5, 6	The solution should not expose the user to new security vulnerabilities, that would not be present, had the user not chosen to implement the solution	Neither new software, new hardware or additions to integration must expose new security vulnerabilities
215	For a higher detection rate, new access control/intrusion detection systems should be integrated with existing access control points on each floor depending on the criticality of the area (especially in the Department of Nuclear medicine and Blood Bank)	
18	The solution should be able to distinguish likely threats from normal usage with a reasonable degree of accuracy	Report estimated accuracy of alarm along with the alarm
24, 43, 194	For threat prevention, all the security systems described below must be integrated. • supervision of video protection • supervision of fire detection • supervision of PLC • supervision of access control	T4.2 is responsible of supervision of fire detection, access control and partly supervision of video protection.
26	A simulation mode must permit to test the existing security measures to evaluate protection and to add if necessary tools or procedures to prepare for an incident or crisis management	From the DoA, we are not committed to enabling a simulation mode. Some parts of system might enable simulation, but not all together
36	Avoid false positives	
92	Automatic recognition software for video surveillance systems	
141, 178, 214	Controlled environment through biometric methods, accessible only to authorized personnel	
233	High level of maturity is mandatory for a high acceptance level	
93.1	Integrated approach of detection systems, with increased effectiveness from the integration	

5.3 Consolidated solution requirements

Consolidating the above requirements from D3.4 and from T4.2, we derive the following requirements. The requirements are presented in Table 3.

Table 3 – Consolidated requirements

Requirement number	Description
R1	Automatic detection of physical intrusion • A biometric method must be used
R2	Use access management system together with VMS to improve intrusion detection
R3	Identification capabilities of people involved in the incident
R4	Automatic detection of fires
R5	Use fire detection system together with VMS to improve verification and handling of fire alarms
R6	Have a technology readiness level of at least 7
R7	Send validated incidents, intrusion alerts, fire alerts and access logs to the central database
R8	Comply with implemented solution in simulation site
R9	Be fast, accurate and detect as soon as possible: • The solutions must be designed to try to detect the incident even before it has actual occurred; • The solutions must respond in almost real time; • The solutions must be able to detect the incident just after it has occurred; • The solutions must have high accuracy, avoid false positives and report accuracy
R10	Allow operators to manually tweak the configuration
R11	Use semi-supervised or supervised learning
R12	Not expose new security vulnerabilities compared to not using the solution

6 Solution Description

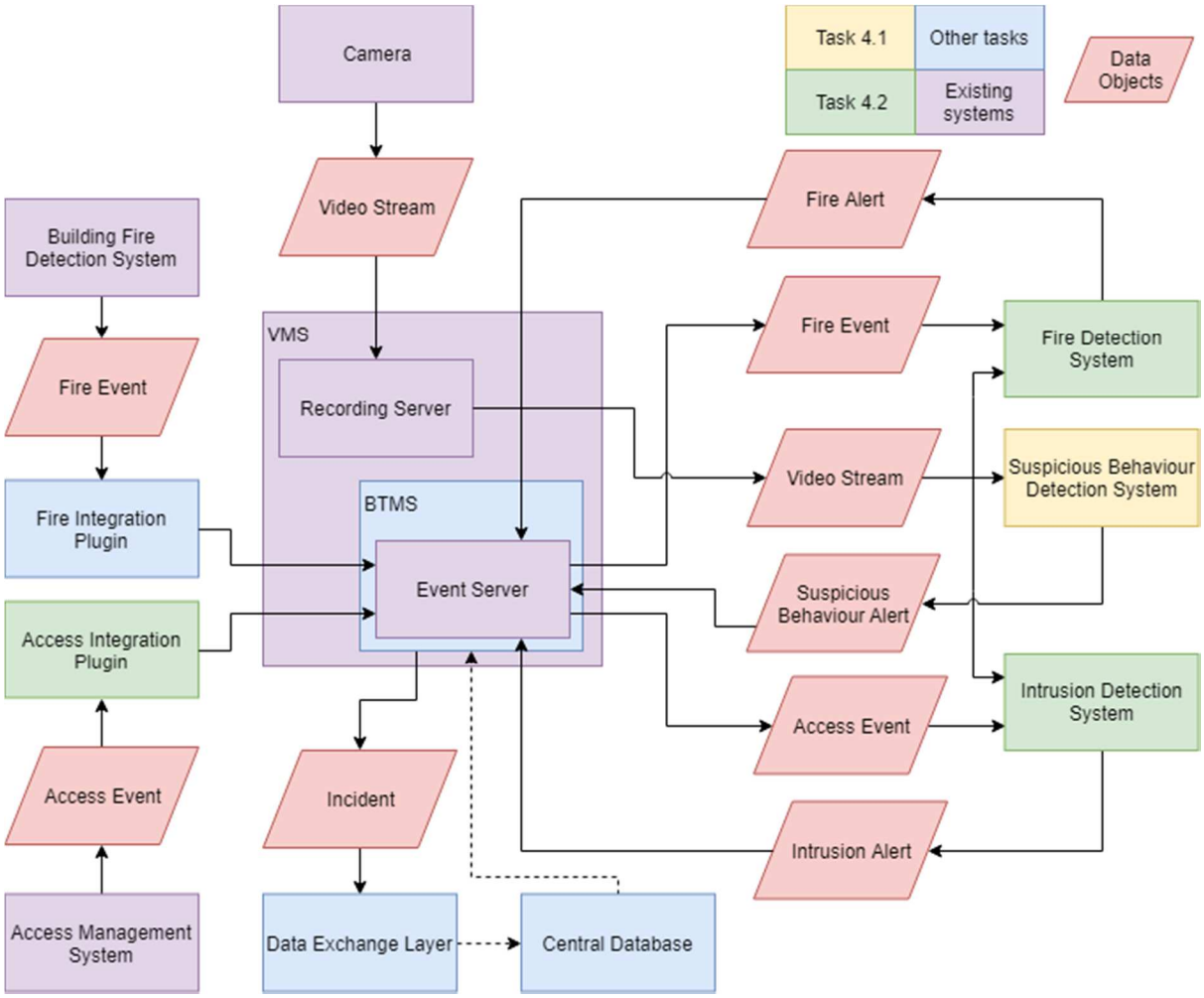
In this section there follows an informal description of the different types of incidents the system will handle. A short description is made for each of the incidents, followed by how the system will try to handle the incident, how the video management system integrates with the access management system and the building fire detection system as well as what difficulties, limitations and requirements there is for the system to handle the incidents. A description of how the system and the VMS will handle the identification of people will also be described.

From the solution requirements Section 5.3 Requirements R1 and R4 states that we need to be able to automatically detect intrusion and fires and Requirements R2 and R5 state that the access management system and fire detection must be integrated together with the VMS. The system will handle three different kind of intrusions: fraudulent use of access control key (which will be the biometric method); tailgating; and, by breaking through the access control by force and the solution will be able to detect fires in general. Requirement R3 from the solution requirements state, that the system needs to be able to identify people involved in the incident, which will not be handled directly by each of the solutions, but a limited solution will be handled by integrating with the VMS.

Requirements R6, R9, R10, R11 and R12 cannot be fulfilled until the main functionality of the component has been implemented, so are not explicitly dealt with in this specification.

In Figure 1 is visualised an overview of how the solution will be integrated with the other components relevant to Task 4.2. The diagram shows that the fire detection system and intrusion detection system, described later in this section, will receive the video streams from the recording server and the fire and access control events from event server, and send new alerts via the event server, which is the central part of the BTMS. Also discussed in Section 10.1, the diagram shows that the BTMS will be responsible for sending the incidents through the data exchange layer. The diagram also shows that the access management integration will be done in this task, and this is described in Section 10.3.

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



6.1 Intrusion incidents

The intrusion detection system should be able to detect three different kinds of intrusions. Fraudulent use of access control key, tailgating and breaking through access control by force. For the intrusions the intrusion detection system will try to detect the intrusion before the access control entry point has been passed if the set-up allows it.

6.1.1 Fraudulent use of access control key

Fraudulent use of an access control key is the act of using a key which you were not granted or by using a fake version of an access control key. As there are many forms of keys to an access control point, the required difficulty of getting hold of or faking the key depends a lot on the type of key that is used. For example, you may need access to the management system to obtain or change a pin code, and it is very hard to steal biometrics, while it can be fairly easy to steal a physical key.

The intrusion detection system will try to detect fraudulent use of access control key when someone registers their access control key to pass an access control point. The intrusion detection will try to detect the person using the access control key and confirm that the holder of the key is also the one who has been granted the key. This system must handle different cases, although some of the cases might not be feasible to do, so the system will try to handle some of the cases that is reasonable for the scenarios. These could be:

- Physical key / Pin code: In general, is it hard to keep track of who has a physical key or who knows the pin code and keep a photo database of people who has been granted that specific key, and therefore hard to detect fraudulent use. For an access control point with few users, with a corresponding photo for each one, it can be possible to detect fraudulent use, but this must be updated if code is shared.
- Access Badge (Electronic key): It is easy to have a corresponding photo to a unique badge, so trying to detect if the person using a badge is the same as the one having been granted the badge is possible.
- Access Badge (Showing badge): Detecting fraudulent use when showing badge to receptionist or security personnel at access control is almost impossible, as the system is most likely unable to get a view of the badge and it is the personnel's responsibility to confirm the identity.
- Automatic biometric recognition: Would mean that the system would detect other biometrics from a person, compared to the automatic biometric recognition system.

This solution has some different limitations and requirements for the different types of access control key used, but there are some general ones as well:

- Requires camera coverage of both access control reader and entry point
- Can produce warning if someone is lending out the key to a fellow employee
- Is unable to handle cases like guest access badges
- Physical key / Pin code: A photo database must be updated when new people are granted access
- Physical key / Pin code / Access Badge: Photo database should be updated occasionally if people changes to much
- Physical key / Pin code / Access Badge: For identification of people, more than one image is preferred, especially from different angles and set-ups

6.1.2 Tailgating

Tailgating is the act of getting through an access control point without having the required key to get through by following behind someone else who validly went through the entry system. Tailgating can take many forms and can in principle both be for people and cars and the different kinds of tailgating might work for different entry systems.

When someone registers their access control key at the access control reader and passes through an access control point, the solution will try to detect the person using the access control key, and then try to detect if anyone is tailgating for a short period of time at the access control point using the cameras covering the access control point, whether it is casual walking behind the person, grabbing the door just before it closes or blocking the gate.

This solution has some limitations and requirements which might not make it an optimal solution for every entry point. These are limitations and requirements are:

- Requires camera coverage of both access control reader and entry point
- Can produce a lot of warnings if employee typical move through together
- Can provide warnings only after the access control point has been breached

6.1.3 Breaking through access control by force

Forcingly breaching access control is the act of getting to a restricted area through an access control entry point without registering a key at the access control reader. The way of breaching the access control entry point depends on the type. Breaching a locked solid door is different than breaching a low gate or a security guard at an entrance.

The solution will at all time use the video feed covering the access control point to detect if anyone passes the access control entry point without registering the key at access control reader. The solution will also try to detect if someone is trying to pass the access control point by force in order to alarm the security personnel before an intrusion have occurred.

This solution needs to handle a lot of different types of entry points which results in some difficulties in detecting breaching of an access control. The difficulties and requirements are:

- Requires camera coverage of the entry point
- Can be hard to generalise a solution with many types of access control entry points

6.2 Fire incident

A situation with fire and smoke is not necessarily an attack but it could be an innocent accident. Any unintended fire, such as a candle with a flame, intended fire and smoke is considered as a situation with fire or smoke. This solution can be made two work in two different ways. Either by trying to confirm a fire alarm or by trying to detect fires everywhere, all the time. Requirement R5 state that the fire solution must improve verification and handling of fire alarms, thus only requiring to confirm fire alarms.

The solution to confirm fire alarms will wait for the buildings fire detection system to report any alarm. When an alarm is received, the solution will try to detect any fire and smoke at the location of the alarm, in order to confirm the alarm, and to provide video streams of the fire to the security personnel.

The solution to detect any fire and smoke at all time, will use all cameras available and try to detect a fire or smoke on all of them at all time. This can be able to warn about a fire before the buildings fire detection system detects a fire. This solution is prone to limitations and therefore should be viewed as a secondary source of information to the sensor-based solution, not as a primary signal.

- Can only help to confirm fire and smoke, if the fire and smoke is under camera coverage
- Detecting fire at all time, requires complete camera coverage of the entire building
- Can be hard to determine if the fire has been started on purpose
- Cameras at deployment can influence performance as a camera with thermal capabilities can detect fires with better accuracy

6.3 Identification capabilities

In order to identify people involved in accidents, the video management system needs to have information and images already stored of the people that need to be identified. For the fraudulent use of access control badges, the information needed for identification of staff with access badges is provided, making it possible to identify staff being involved in an incident, but not third parties (patients, visitors, intruders, etc.).

The VMS will be able to enable, although not a requirement from the DoA, D3.4 motivates that, identification capabilities for people using access control systems and people involved in incidents. The VMS will be able to enable reidentification capabilities of people captured in a video stream in other video streams stored in the VMS.

7 Scenarios

This section will go through every scenario defined in Deliverable D3.6, where a description and overview for all the scenarios can be found along with the methodology of how the scenarios are defined as well as the strategic and technical scenario for each scenario. For each of the scenarios a short description will be provided, the physical steps of the technical scenario the intrusion and fire detection solution can raise an intrusion or fire alert for and how these solutions should be able to help handle the step. The solutions defined in this deliverable concern only detection of incidents regarding steps with the classification "Intrusion or physical trap", although not necessarily all steps with that classification. For a full picture of how the SAFECARE solution for physical security will cover these scenarios the reader should also consider D4.1 and D4.3.

Overview

When considering at the attacks described in the scenarios, we look at whether the intrusion and fire detection system has a chance of detecting the intrusion, and thereby help stopping the attack.

For scenario 2, the intrusion and fire detection system should be able to detect an intrusion or fire for all path of the scenario.

For scenario 1, 3, 4, 5, 7, 8 and 9, the intrusion and fire detection system should be able to detect at least one intrusion or fire for each scenario, but there is way the attack can be performed around the system.

For scenario 6, the intrusion and fire detection systems are unable to detect any form of intrusion or fire.

1	2	3	4	5	6	7	8	9

Each of these judgements will be considered in more detail in the following subsections.

7.1 Scenario 1

This scenario describes the attack of disrupting the power supply of the hospital. The scenario describes the attacks of taking out the internal power supply by getting access to the Programable Logic Controller (PLC), by physically breaking the energy cabinet and by taking out the main power supply with fire or bombing, either from the inside or outside of the hospital. These attacks can of course be combined to make a stronger attack. For this technical scenario we will look at preventing the attack at the four "Get In" steps:

1. **Access to the room with network access to PLC:** For this step there is three possible connections, and this system is only able to handle the step if coming from step "Steal key/badge". Assuming this, the fraudulent use of access key solution can handle the intrusion.

2. **Break the door:** This step occurs before the "Intrusion of the energy cabinet" and the "Access to PLC room" steps and the breaking through access control by force solution will handle the intrusion.
3. **Intrusion of the energy cabinet:** This step already has a previous connection of "Break the door". Depending on the set-up the fraudulent use of access control key and tailgating solutions can handle the intrusion if not coming from the "Break the door" step, although tailgating would have to be specialised to handle the case of someone using the cabinet after someone who did not close the cabinet door properly.
4. **Have access to the office of the admin of the hospital:** For this step we assume that the office is behind some kind of access control point and then any of the fraudulent use of access key, tailgating and breaking through access control by force solution can come into use depending on the intrusion attempt. If the office is not behind an access control point, then this system cannot detect the intrusion.

7.2 Scenario 2

This scenario describes the physical attack of setting a fire somewhere in the hospital in order to start an evacuation of the hospital and use the resulting confusion and potential automatic unlocking of doors for escape routes to get unhindered access to a computer- or server room. For this scenario we will look at preventing the attack at the two "Get In" steps of the technical scenario:

1. **Put the fire to trigger the fire alarm:** The fire and smoke solution will try to handle this step.
2. **Break the door lock of the computer room:** For this step the intrusion will be handled by breaking through access control by force.

7.3 Scenario 3

This scenario describes the strategic scenario of targeting the medical devices in the hospital. Four technical scenarios are defined for this scenario; get physical access to gather proof of compromise at the hospital, digital attack to cause a hardware fault, do phishing attack and get physical access to the hospital change software parameters to harm patients, and impersonate vendor to install malicious software to hurt reputation and affect patient treatment.

7.3.1 Technical scenario A

In this technical scenario the attacker, or attackers, will try to get physical access to the hospital by distracting the receptionist and get access to the unlocked technical room. For this scenario we will analyse the intermediate step between the "Get In" steps of "Distract receptionist" and "Enter (unlocked) technical room" of "Passing the distracted receptionist". As there is no fraudulent use of access control key, no force being used and no tailgating, none of the solutions can handle this intrusion. Either another solution must be made to handle this intrusion or rely on the suspicious behaviour of Deliverable 4.1 to handle this intrusion.

7.3.2 Technical scenario B

In this technical scenario the attacker carries out a digital attack to change the software, in order to cause a hardware fault. In none of the steps will any of the solutions be able to detect physical intrusion or fire to prevent the attack from happening.

7.3.3 Technical scenario C

In this technical scenario the attacker will try to get access to an employee's workstation to change software parameters in order to harm patients by system misbehaviour. For this scenario we will look at preventing the attack at the "Get In" steps:

1. **"Break into department at night":** The intrusion solutions of the system assume a set-up at access control points, so as long as the break in happens at an access control point, then the breaking through access control by force solution can handle the intrusion. If the intrusion happens at another place, the intrusion detection solution is not set up to handle it.
2. **"Enter employee office":** Assuming that the employee office has an access control point, then breaking through access control by force can handle the intrusion.

7.3.4 Technical scenario D

In this technical scenario the attacker will impersonate a vendor and request access from the hospital staff to get access to the maintenance interface, even though this can be considered physical intrusion there is no way this solution can detect it as the attacker is granted access to the target.

7.4 Scenario 4

This scenario describes the attack of taking out the air-cooling system of the hospital in order to contaminate surgery rooms, expand virus seeds and taking out data centres. In the technical scenario we can prevent the attack in the "Get In" step "The criminal steals the badge of the maintainer and go to the hospital". When the attacker tries to enter the hospital the fraudulent use of access control key can handle the intrusion.

7.5 Scenario 5

This scenario describes a terrorist attack of planting a bomb in the hospital. The technical scenario defines two paths to get there, a physical about impersonating a vendor and trying to bypass the security and a digital to get access to credentials. For this technical scenario we will look at preventing the attack at the "Get In" step "Bypass Security" for the physical solution. In order to bypass the security, the attacker can both try to tailgate, steal an access control key to fraudulent use this or break through the access control by force. So, all the systems intrusion solution will try to handle this step.

7.6 Scenario 6

This scenario describes the theft of data from hospital equipment that an insider has access to. There is no physical intrusion and no fire to detect for this scenario, so there is no solution to prevent this attack.

7.7 Scenario 7

This scenario describes the attack of getting access to an IoT device at the hospital to harm the hospital, its patients or the device manufacturer by either stealing or replacing the IoT device or identifying vulnerabilities in the IoT devices to perform cyber-attacks. In this scenario two technical scenarios are described. In the first technical scenario the attacker is a security researcher who is assumed to have been granted access to the IoT device, so there is no intrusion and no fire to detect for this technical scenario. In the second technical scenario the attacker is an outsider who will try to get access to the IoT device to either scan for vulnerabilities, steal or replace the device. In this technical scenario we can prevent the attack in the "Get In" step "Obtain

local access to medical IoT device in hospital". If the medical IoT device is behind an access control point, the attacker can both try to tailgate, steal an access control key to fraudulent use this or break through the access control by force. So, all the systems intrusion solution will try to handle this step.

7.8 Scenario 8

This scenario describes the attack if the badge or account of a doctor or pharmacist has been stolen. This scenario has two technical scenarios where Technical scenario A has two paths. The first path in technical scenario A and the entire technical scenario B is completely a cyber-attack, so there is no physical solution to prevent these two. The second path in Technical scenario A describes the attacker getting access to the hospital with a stolen employee badge to get access to medical devices to either steal them or disrupt the usage. For this path we will look at preventing the attack at the "Get In" step "Access to restricted area in hospital (badge)". As the attacker is trying to get access to the hospital using a stolen badge, the fraudulent use of access control key solution will try to handle the intrusion.

7.9 Scenario 9

This scenario describes the attack of blocking information for the National Crisis Management system. In this scenario we can prevent the attack in the "Get In" step "The criminal steals the badge of the maintainer and got to hospital". When the attacker tries to enter the hospital the fraudulent use of access control key can handle the intrusion.

8 Data Exchange Format

Requirement R7, see Section 5.3, states that the systems must send incidents, alerts and access logs to the central database. This Section describes the format that will be used to send the incidents alerts and logs to the central database. For this, JSON (JavaSCript Object Notification) has been chosen as data exchange format for the messages to be send through the data exchange layer to the central database. JSON format provides maximum system interoperability in SAFECARE project, in fact it will be used also in WP5 and WP6. The format is lightweight and easy to understand by humans and by machines. In the appendix Section 15.1 is an example of the data exchange format with an incident containing two events, where one is classified as an alert.

Starting from the scenarios described in the previous sections a list of names/values has been compiled to capture the required data in the JSON format. The format will be extended and changed as the work package progresses, but the following provide a basis on which to begin.

Key	Value description
detector	Specify if the event (alert/incident) is from physical or cyber domain
created_timestamp	
confirmed_timestamp	
severity	Specify the severity of the event: LOW, MINOR, MAJOR, CRITICAL
start_date	

type	Specify message type: INCIDENT
unique_identifier	Unique identifier for the correlated incident
events	Collection of event 1 to many
event->description	Human readable description of the event
event->detector	SAFECARE component detecting the event
event->date	Time at which the event was detected for the first time.
Event->title	Description of the event
event->type	Description of the event according to data exchange layer specification (EVENT, ALERT)
event->unique_identifier	Unique identifier related to the detector
event->assets	The structure contains the data related to assets involved in the security event
event->asset->category	Description of the asset category according to data exchange layer specification
event->asset->name	Description of the asset name according to data exchange layer specification
event->location	Description of the asset position according to data exchange layer specification
event->location->type	Specify if indoor (1) or outdoor (0)
event->location->position	In case of outdoor the structure contains GPS coordinates, in case of indoor it contains position as specified in central database
event->sensor	Structure containing information related to the Sensor which detected the event.
event->video_analytics	Structure containing data related to video analytics performed by VMS
event->video_analytic->camera_id	Camera responsible for the event detection, matching a camera in central database
event->video_analytic->number_of_people	Number of people detected
event->video_analytic->security_event	Type of security event detected
event->camera	T.B.D
event->media_video	URL pointing to event captured video
event->badge_owner	Example of additional attribute

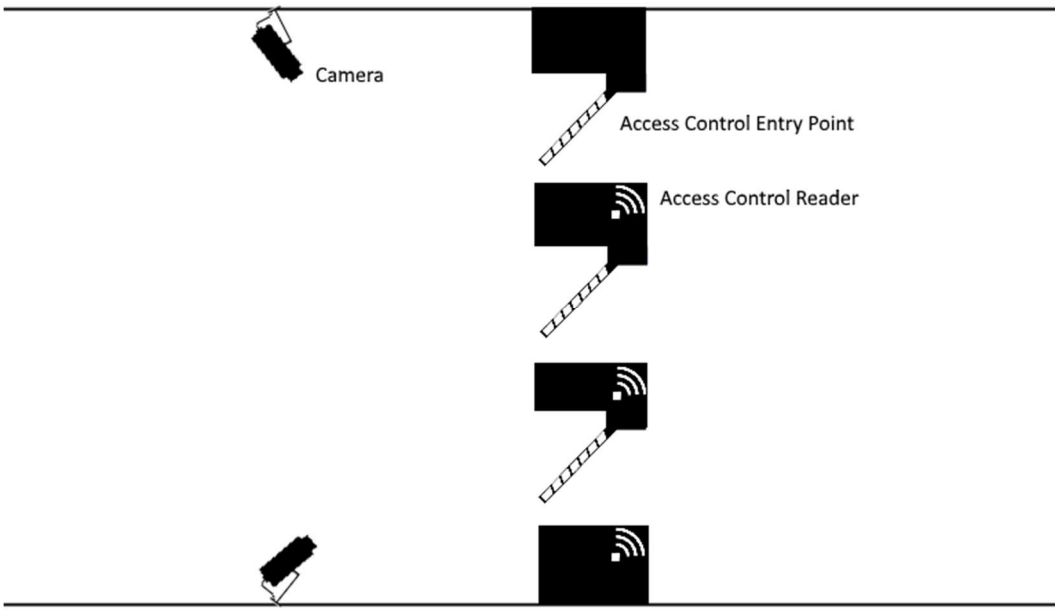
9 Devices and Set-ups

Requirement R8, see Section 5.3, state that the solution needs to comply with the implemented solution at the demonstration sites. In order to develop a solution that complies with the implemented solution at the simulation sites, it is required that demonstration sites provide information about their devices and set-ups before the solution is made.

9.1 Set-up and scenarios

In order to show that the solutions defined in Section 6 can handle the scenarios defined in D3.6 and analysis in Section 7 for the specific demonstration sites, we need to know what devices are available at each demonstration site, and how the data from the devices can be correlated together. In Figure 2 is an example of a set-up with multiple camera, access control entry points and access control readers which could be used as the set-up for Scenario 4 described in Section 7.4 and Scenario 5 described in Section 7.5.

Figure 2 - Example of devices in a set-up



9.2 Known devices and set-ups

Devices and preliminary examples of set-up at the demonstration sites have been provided, but these cannot be described further due to the confidentiality level of this deliverable, but set-ups will be described in detail in D4.4 with the implemented solution. For the initial design of the solutions described in Section 6 the provided examples satisfies, but for the final implementation specific and detailed examples of the demonstration sites set-ups are need to develop the optimal solution.

10 Integration with VMS

Requirements R2 and R5, see Section 5.3, state that the access management system and fire detection must be integrated together with the VMS to improve the intrusion detection and handling and verification of the fire alarms. For the system the Milestone XProtect® VMS[1] will be used, along with its current features and SDKs. There follows an overview of how this integration will be made.

- Transferring incidents, etc. to the central database.
- Setting up static devices.
- Receiving access control events.
- Enable video recording from events using rules.
- Receiving fire detection events.

These steps are considered in more detail in the following subsections.

10.1 Send Data to Central Database

Requirement R7 states that the solution must send incidents, alerts, events and access logs to the central database. The alerts, events and access logs will be stored inside the incidents as described in Section 8. Deliverable 4.10 will concern a XProtect® plugin that will handle the transmission of the incidents, with the alerts and events, for Task 4.2 to the data exchange layer.

10.2 Setting up static devices

For T4.2, static devices are the cameras, the detectors in the buildings fire detection system and the access control entry points and readers of the access management system. These devices are all devices that will be set up once and most likely never be moved, only removed at one point in time, which happens in larger reconfiguration of the security of the hospital.

For normal installation of the XProtect® VMS, all the devices are set up manually, and reconfigured manually if needed directly into the VMS. If all the set-up data for the devices are stored in the central database, a plugin can be made to set-up all devices associated with the physical security solutions. As it has yet to be determined whether the set-up data for the static devices will be stored in the central database, before the VMS is configured. This deliverable will leave open both ways to achieve this.

10.3 Access management system integration

A XProtect® plugin, using XProtect® Access[2], will be developed to handle the integration with the access management systems of the demonstration sites and at the test site. This plugin will handle the reception of all events from the access management system and all access control points associated to it, as well as providing information from the access management systems database and controlling the devices and configuration of the access management system.

Through the XProtect® Event Server[3] it is possible to create rules on events received by devices, including devices connected to the access management system. By integrating the access management system into the VMS, it will be able to control the appropriate cameras needed for

[1] https://www.milestonesys.com/solutions/platform/video-management-software/xprotect-corporate/
[2] https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/access/
[3] https://www.milestonesys.com/globalassets/techcomm/2018-r2/advvms/english-united-states/index.htm?toc.htm?10684.htm

the access management point and start the analytics needed to analyse the appropriate video stream. Doing this will help providing the needed information to the security personnel responsible for handling the alerts, and it will help threat response by correlating the events received together with the alerts into the incidents that is being sent to the central database.

10.4 Fire detection system integration

A XProtect® plugin will be developed to provide an API for the building fire detection systems of the demonstration sites and the test site. The specification of the integration of the building fire detection system will be specified in D4.5 and the integration of the building fire detection system will be done in D4.6. The API will enable reception of all events needed from the specifications of D4.5.

Through the XProtect® Event Server it is possible to create rules on events received by building fire detection system. By integrating the building fire detection system into the VMS, it will be able to control the appropriate cameras needed in case of a fire and start the analytics needed to analyse the appropriate video stream to confirm the fire. Doing this will help the security personnel confirm that a fire has occurred, and it will help threat response by correlating the events received together with the alerts into the incidents that is being sent to the central database.

11 Training and Test Data

It is an explicit and well-understood requirement of the use of machine learning that training of models for the solutions, require a large amount of relevant data. When the solutions have been deployed, they need the same kind of data to perform. For this data to be as relevant as possible, the training data will be delivered by the demonstration sites to optimise the training for operational use. Data examples of different situations are also needed to implement the solutions in the best way possible.

11.1 Video data

For the solutions described in Section 6.1 a significant quantity of video data is needed from all cameras involved in the set-ups for the scenarios for the demonstration sites which is described in Section 9.1. The video data must also cover all events described in the following section, and the video data must be correlated with the access management system data described in the following section. For the solution described in Section 6.2 some video data is needed for some corridors and rooms at the demonstration sites, and if available, video data with smoke or fire could prove helpful.

11.2 Access management system data

For the solutions described in Section 6.1 examples of the information received by the access management system is needed. For all events examples received by physical devices, information on location of device is needed, and if possible, in which set-up it is part of.

11.2.1 Fraudulent use of access control key

The fraudulent use of access control key incident solution described in Section 6.1.1 needs to know where the events are coming from, what access control key is being used, how the access control point is being used and who is associated with the access control key. For this, the following data examples are at least needed for the solution:

1. Events on both correct and erroneous use of access control point;
2. Location of access control reader being interacted with;
3. Information stored about the person associated to the access control key used.

The training data provided storing information about the person should be anonymised before provided for training, so no personal or identifiable data about owners of access control keys leave the demonstration sites.

11.2.2 Tailgating

The tailgating incident solution described in Section 6.1.2 needs to know where the events are coming from and how the access control point is being used. For this, the following data examples are at least needed for the solution:

1. Events on both correct and erroneous use of access control point;
2. Location of access control point being used.

11.2.3 Breaking through access control by force

The breaking through access control by force solution described in Section 6.1.3 needs to know where the events are coming from and how the access control point is being used, as well as any event on damages done to the access control point. For this, the following data examples are at least needed for the solution:

1. Events on damage done to access control point;
2. Events on both correct and erroneous use of access control point;
3. Location of access control point being used.

11.3 Fire detection system data

For the solution described in Section 6.2 examples are needed for all types of fire and smoke sensors available in the system from the building fire detection system. For this Deliverable, examples of fire and smoke sensor events have not been provided yet. If available, examples of events received by the sensors containing the following information is needed as the more information that can be integrated, the better solution can be made.

1. Status of fire and smoke sensors such as:
    - All good state: No smoke or fire detection;
    - Warning states: Low level smoke of heat detected, without setting of the alarm;
    - Alert state: Smoke or fire detected.
2. Type detected e.g. Smoke, gas, fire, etc.
3. Information on location of sensor.

11.4 Training data lifecycle

In order to handle identifiable data received by the demonstration sites, data sharing agreements are being drafted between the demonstration sites as data controllers and the data processors of this work package. Training data received by the demonstration sites will be handled and deleted following the data agreement that is being made or deleted when the data is no longer necessary to use for the purpose of the processing, as according to GDPR Article 5 (e). Internal sharing of the data within the organisation will have to be on a need-to-know basis.

11.5 Deployed data lifecycle

All data retrieved from the cameras, the access management system and the building fire detection system, as well as the output of the solutions of Task T4.2 will all be handled by the VMS. The VMS that Milestone will provide, XProtect® Corporate 2019 R2, has received the European Privacy Seal's GDPR-ready certification, and can be configured to apply the data handling policies chosen in this project.

12 Scenarios at 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 fulfil the scenarios.

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

As the set-ups and the data examples of demonstration sites have not been provided yet, it cannot be determined whether any of these factors will have an impact on fulfilling the analysed scenarios, although there has been shown some commitment from the demonstration sites to alter the set-ups if this should become an issue.

Regarding data examples, an issue that could arise would be if the data privacy concerns constrain the data that will be available for training. If this should be the case, some more general-purpose datasets will have to be used, in order to try to fulfil the requirements of the project.

13 Requirements Mapping

In Table 1 is presented the mapping between the consolidated requirements with the existing functionalities in the VMS and new functionalities to be made. For each requirement is a short description on how it is fulfilled, and which section describes it further.

Table 4 - Requirements mapping

Requirement number	Description
R1	As described in Section 6.1, the solution will handle three kinds of physical intrusion: Fraudulent use of access control key; tailgating; and breaking through access control by force. In Section 6.1.1 is a description on how a biometric will be used
R2	Section 10.3 is a description on how the integration of the access management system will be done with the VMS
R3	In Section 6.3 is a description on how the VMS will enable identification capabilities of people
R4	Discussed in Section 6.2 is how the solution will handle detection of fires
R5	Section 10.4 is a description on how the integration of the building fire detection system will be done with the VMS
R6	As discussed in Section 6, having a technology readiness level of at least 7 will be fulfilled as part of the implementation and will be done in of D4.4
R7	The validated incidents, alerts and access logs will be stored as described in Section 8 and the actual transmission will be done in D4.10 as described in Section 10.1
R8	In Section 9 is the discussion on how the solution will comply with the implemented solutions
R9	As discussed in Section 6, this will be fulfilled as part of the implementation and will be done in of D4.4
R10	As discussed in Section 6, this will be fulfilled as part of the implementation and will be done in of D4.4
R11	As discussed in Section 6, this will be fulfilled as part of the implementation and will be done in of D4.4
R12	As discussed in Section 6, this will be fulfilled as part of the implementation and will be done in of D4.4

14 Conclusion

In this deliverable it was concluded that solutions needed to handle the physical intrusion and fire attacks in the scenarios described in D3.6, can be handled by the intrusion solutions, detection of fraudulent use of access control key, tailgating and forcingly breaking through access control points and by detecting fire on video streams. It is also concluded that the provision of protection for critical assets in a healthcare environment can indeed be improved by the integration of the relevant buildings' fire detection systems and access management systems with the video management system and with techniques for video analytics with the capabilities specified herein. This deliverable concludes that for Deliverable 4.4, more information on devices and set-ups, as well as a significant amount of data is needed from the demonstration sites to implement the solutions in the best way possible. In the end it is concluded that Task 4.2 will help fulfil the overall objectives for Work Package 4.

15 Appendences

15.1 Data exchange format example

The following is an entirely fictitious example of a message (the facilities and assets mentioned do not reflect a real use case environment).


```
{
  "detector":"WP4",
  "created_timestamp":"20190410T165514Z",
  "confirmed_timestamp ":"20190410T165514Z",
  "severity":"MEDIUM",
  "start_date":"20190410T165514Z",
  "type": "INCIDENT",
  "unique_identifier":"A#45678",
  "events":[
    {
      "description":"Unauthorised Access",
      "detector":"IFDS t 4.2",
      "date":"20190410T165514Z",
      "title":"Intrusion and fire detection system: Door Opened without authorized access",
      "type":"ALERT",
      "unique_identifier":"A#45679",
      "assets":[
        {
          "category":"TARGET",
          "name":"Power room"
        }
      ],
      "location":{
        "type":0,
        "position":{
          "ward":"main building ",
          "floor":"basement",
          "room":"power room"
        }
      },
      "sensor":{
        "type": "access control",
        "door_id": "27"
      },
      "video_analytics":{
        "camera_id": "128",
        "number_of_people": "1",
        "security_event" : "UnauthorisedAccess"
      },
      "camera":{

      },

      "media_video":{
        "uri":"rtsp://192.168.1.1:554/axis-media/media2.amp"
      }
    },
    {
      "detector":"Access Management System",
      "date":"20190410T165512Z",
      "title":"Door Opened",
      "type":"EVENT",
      "unique_identifier":"A#46679",
      "location":{
        "type":0,
```

```
            "position":{
               "ward":"main building ",
               "floor":"basement",
               "room":"power room"
            }
         },
         "sensor":{
            "type": "access control",
            "door_id": "27"
         },
         "badge_owner":{
            "badge_id":"A#142789",
            "name":"John Doe"
         }
      }
   ]
}
```