SAFECARE

Integrated cyber-physical security for health services

Initial Dissemination and Communication Report

Deliverable 8.2

Lead Author: EOS

Contributors: All Partners

Deliverable classification: PU

Co-funded by the Horizon 2020 Framework Programme of the

Version Control Sheet

Title	*Initial Dissemination and Communication Report*
Prepared By	*James Philpot – Elodie Reuge*
Approved By	
Version Number	*Version 1*
Contact	Elodie.reuge@eos-eu.com

Revision History:

Version	Date	Summary of Changes	Initials
V0.1	20.09.2019	Initial draft sent to the reviewers	ER - JP
V0.2	25.09.2019	Comments from the reviewers	VM-IG
V0.3	26.09.2019	Comments taken into consideration	ER-JP
V1	26.09.2019	Final version sent for submission	ER-JP

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

Contents

List of Figures

List of Tables

List of acronyms

Acronym	Definition
ATP	Advanced Persistent Threats
BMS	Building Management system
CIP	Critical Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
D&C	Dissemination & Communication
DG	Directorate Generals
DoA	Document of Action
DoW	Description of Work
DPIA	Data Protection Impact Assessment
EC	European Commission
ECSO	European Cyber Security Organisation
EOS	European Organisation for Security
EU	European Union
ERA	Emergency Response Agency
EPCIP	European Program for Critical Infrastructure Protection
FG	Focus Group
GA	Grant Agreement
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IT	Information Technology
IAP2	International Association of Public Participation
IE	Innovation Elements
IoT	Internet of Things
KPIs	Key Performance Indicators
LEA	Law Enforcement Agency
PLC	Programmable Logic Controllers
QM	Quality Manager
SOC	Security Operations Center

WP	Work Package
WPL	Work Package Leader

The SAFECARE Project

Over the last decade, the European Union faced numerous threats, which gradually increased in magnitude changing the lives and habits of millions of citizens installing fear and terror. The sources of these threats and the weapons used were heterogeneous and so was the impact on population. As Europeans, the consortium knows that it must increase awareness since these attacks can affect and destabilize Critical Infrastructures (CI) depending on. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analysed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats. Health services are at the same time among the most Critical Infrastructures and the most vulnerable ones.

They are widely relying on Information Systems (IS) to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this project is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It promotes new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. The project will also participate in increasing the compliance between security tools and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find potential “customers” across Europe.

Executive Summary

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

Over a 36-month time frame, the SAFECARE Consortium will design, test, validate and demonstrate 13 innovative elements, developed in the Description of Actions (DoA), which will optimise the protection of critical infrastructures under operational conditions. These elements are interactive, cooperative and complementary, aiming at maximizing the potential use of each individual element. The consortium will also engage with leading hospitals, national public health agencies and security Stakeholders across Europe to ensure that SAFECARE's global solution is flexible, scalable and adaptable to the operational needs of various hospitals across Europe. In this context, the aim will be to meet the requirements of newly-emerging technologies and standards.

The Dissemination and Communication Strategy (D8.1) is introducing the overall engagement approach that SAFECARE already follows and will keep respecting until the end of the project, providing the foundations and the perspectives of the D&C.

One of the main purposes of the deliverable is to ensure that: (a) project outputs and outcomes are widely and rightly disseminated to the suitable target audiences and at the right time, through intelligible tools and channels and (b) stakeholders that can contribute to project outputs' development, evaluation, uptake and exploitation should be identified and encouraged, from the beginning, to proactively interact with the consortium partners on a regular and systematic basis.

First, the Dissemination & Communication Strategy considers the engagement process as a whole. The overall concept is presented below and details about the objectives for engaging with the sensitive healthcare environment will also be shared (Section 2). Moreover, the engagement process has to be considered at different levels, with many stakeholders and through several mechanisms. A description of the targeted stakeholders and a definition of the key messages that should be shared with them, as well as the identification of the currently available tools used to create an appropriate interaction with them is developed (Section 3, 4 and 5). A justification on right timing to use them and the purpose of tools' use is also provided. Hence, Section 6 describes a set of measures that should be followed in order to successfully engage the process. This document has to be seen as a reference point to evaluate the impact of the communication and dissemination activities to be carried out until September 2021. It will be updated and adjusted according to SAFECARE's progress, reflecting the lessons learnt during the implementation of the project. Finally, Section 7 provides details on the monitoring tools and mechanisms that have been put in place to measure the impact of the Dissemination and Communication activities carried out, and to enable the early identification of possible deviation occurring within the Project.

1. Introduction

To achieve the sensitive and ambitious objectives of SAFECARE, a comprehensive stakeholder engagement approach was considered as the key point of the SAFECARE D&C Strategy. This approach was meant to also fully understand the objectives, and ensure that the Dissemination and Communication activities will occur at the right time.

The D&C Strategy had as its main goal the perfect understanding of SAFECARE's objectives and outputs by different internal and external stakeholders. It laid the foundation of an appropriate implementation of the engagement process in a meaningful way, defined the appropriate messages for the right stakeholders, selected adequate tools and used suitable channels, respecting the appropriate timing. The Initial Dissemination and Communication Report (D8.2) provides the reader with an update of the Dissemination and Communication Strategy after 10 months of implementation.

An explanation of what is expected from D8.2 is provided in point 1.1 and the detailed content of each section of the deliverable is presented in 1.2 Methodology.

1.1 Deliverable 8.2

According to the DoA, EOS will deliver a report about the results of the Dissemination and Communication campaign in place since November 2018.

The deliverable will analyze the relevance of the activities implemented during the first year, previously identified as end-users and practitioners in the CIP and the security industry, standardization bodies, policy and decision makers as well as the Cyber Security PPP and other relevant networks. The key messages and means used to approach the stakeholders will be methodically examined in order to measure their impact.

1.2 Methodology

The goal of D8.2 is to present the main achievements of 10 first months of SAFECARE in terms of Dissemination and Communication used in the project to increase the engagement of the relevant stakeholders. The effective implementation of the Dissemination and Communication activities has been proved to be key for the successful project implementation. As explained in the D&C Strategy, the activities focused on two major points the promotion and the increase in terms of visibility of the relevant activities of SAFECARE; and the encouragement of the participatory engagement with key stakeholder groups to enhance the project's impact and ensure the adoption of its main outcomes.

As D8.1 has to be seen as an evolving document to be continuously updated and populated throughout the project duration, reflecting the entire consortium point of view, D8.2 (and D8.3 at a later stage) aims at reflecting the activities and results achieved by SAFECARE and informing about the adjustment of the strategy. The Initial Dissemination and Communication deliverable will report on the measures, evaluation tools and mechanisms applied in SAFECARE, benefiting from a dedicated monitoring.

In section 2, an overview of the Dissemination and Communication activities put in place since September 2018 is provided. Section 3 identifies and defines the Monitoring and evaluation of the D&C activities and means. In Section 4, the Dissemination and Communication plan starting from M13 and to be applied until M36, will be presented.

2. Dissemination and Communication activities put in place since M3

2.1 Dissemination strategy: main means

The online and offline dissemination means were put in place to serve common objectives:

- Creating awareness
- Engaging, with stakeholders already identified in the Dissemination and Communication Strategy.

Several channels and tools were used as well as the right timing to use them.

The purpose of the following section is to provide an overview of the several channels and tools used (and the right timing to use them) for the past 10 months.

2.1.1 Online means

The SAFECARE Project Website

Having a clear impact in terms of Dissemination and Communication, the establishment of a website was considered as crucial and had to be put in place as quick as possible. This was done in October 2018 (M2).

SAFECARE's website can be accessed at the following address: www.safecare-project.eu. The website is modern, using latest state-of-the art functionalities offered by WordPress and presents the same graphical identity as the communication tools used within the project.

Moreover, it is also optimized for the search engines and ISEP, in charge of providing the website structure, and was supposed to include a Google analytics code to monitor users, activities and provenance which are very useful to monitor the KPI (see section 3). Unfortunately, this analytics was not put in place during the first year[1].

The website serves as both promotional and information tool. On a regular basis, the content of the website was meant to be updated to share the most relevant news, upcoming events (sponsored or attended by SAFECARE), as well as the project outcomes and main achievements. The website was also supposed to store and manage project resources. At this stage of the project, EOS faced some issues in updating the website. These are the following:

- Non-user-friendly aspect of the WordPress version, which makes each update very complicated
- The lack of uniform styling across the website, diminishing its ability to function as a D&C tool
- Non-publication of the PU deliverables before their official approval by the EC
- Lack of sharing information from SAFECARE Partners to EOS (despite the various calls of EOS)

[1] The issue has been realized once EOS asked ISEP for the Google Analytics.

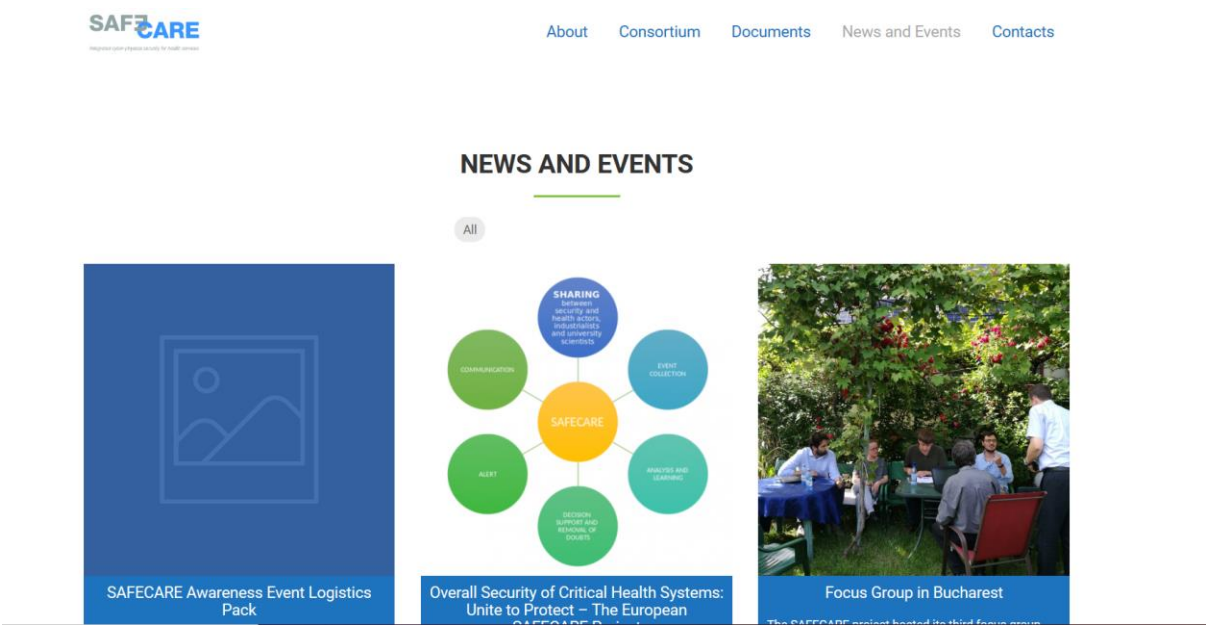


Figure 1: News and Event Page of SAFECARE website

Online Media Strategy and diverse publications

Considering that the main objective of the dissemination strategy is to build and increase the project's awareness across the critical health infrastructure ecosystem (and strengthening the general public's understanding), the promotion of SAFECARE outputs to the online media (which can be general and specialized) is the second crucial point of the dissemination strategy.

As the first year of SAFECARE did not have any proper results to share, it was used to internally establish the list of online media (including local, national, regional and international, general and specialized media). The second and the third year will be used to share key findings with the media, as planned.

Indeed, publishing in scientific journals and conferences will give the opportunity to the consortium to target dedicated scientific communities. The awareness about SAFECARE and the cooperation between SAFECARE and the scientific community will be reinforced, ensuring that another type of peer will be reviewing SAFECARE's scientific approach.

The list of relevant media to contact can be found in Annex XX

Network of stakeholders

A list of relevant stakeholders was established by SAFECARE partners to help to directly be in touch with them about the project's outputs. This list is XX long (see Annex XX)

2.1.2 Offline means

Public deliverables

As a sensitive project, SAFECARE will deliver a certain amount of classified and EU restricted deliverables. Based on that, it is even more crucial to proceed with the proper dissemination of the Public deliverables (33 PU deliverables will be written and submitted during the project lifetime). These documents are crucial, as they contain detailed descriptions of the results. After their official submission and approval by the EC, they are open to CORDIS (the EC portal) and to the project's website, making them accessible to a wide audience. The first review meeting will

be held in November 2019 (M15) and the deliverables to be submitted during the first year are yet still not accepted. Thus, they are not yet available online.

External channels

SAFECARE's activities (and not yet results) have been shared on several external websites for awareness purposes. The most commonly used channels are the following:

- SAFECARE's partners websites and social networks (see in annexes)
- Websites of related H2020 (or EC funded in general) projects targeting Critical Infrastructure in general or Critical Infrastructure in particular

Figure 2: BEIA consulting Twitter page reporting on SAFECARE

Figure 3: STEPWISE Project retweeted about the Awareness event

On top of that, SAFECARE's partners should contribute on a regular basis to targeted blogs with articles, notes and events in their fields of expertise. To facilitate such publications, a point of contact in charge of the media relations has been put in place for each partner. The list of the contact points is shared in Annex 5.

Strategy on Mass Media

A strategy on Mass Media was put in place with the idea to support the consortium in the organization of two main types of events (awareness events and commercial events).The Mass media campaign has been linked to the social media strategy (which has been developed in D8.1). In D8.1 each event had a proper timeline in terms of Communication. At M13, the consortium only tested the strategy for the first Awareness event and applied the following:

1st Awareness event, which took place in Leuven but organized by EOS on the 18th of September, which is the partner in charge with the support of the consortium:

M9: Promotional Tools are ready. Invitation letters are created and sent as well as logistics pack EOS decided to share the promotional tools as early as possible (sticking to the initial deadline), because of the summer break.

M10-13: Information about the AE provided on SAFECARE website and opening of registration (EOS is responsible) and Start of the Social Campaign. From M10 onwards, EOS opened the

registration process, regularly shared information on SAFECARE website, started the Social Media Campaign and asked SAFECARE Partners to proceed the same way.

M11: Press Release announcing the event was sent (EOS is responsible) to the consortium in order for them to distribute it with their network. It appears that this action could have been taken earlier, as it was sent in the summer period.

M14: Press Release summarizing the main outputs will be sent (EOS is responsible)

It is crucial to start the process as early as possible, taking into consideration the calendar issues (summer break and a very busy September).

2.1.3 Dissemination via events

It was already clear that a proper distinction would have to be made between events organized in the frame of SAFECARE and those related to its objectives, called external events.

At M13, SAFECARE has organized only 1 Awareness event (still 1 Awareness and 2 Commercial Events to come until August 2021), as per DoA.

Figure 4: Olivier Théveneau from APHM, coordinator of the project, kicking off the awareness event

Despite the fact that the event was attended by 38 people, was well organised, the presentations were well received and the consortium received a positive feedback, only 5 external people attended it, as:

- The impossibility to fund the travels and accommodations of external people;

- The event might have taken place too early in the project, without a lot of results to showcase, which leads to a very formal agenda.
- Several other large events were taking place at the same time such as the Digital Excellence Forum, which meant that other stakeholders were unable to be present.

Third Party events

SAFECARE has been presented to several third Party events:

Presentations of SAFECARE:

- 19/10/2018: Presentation of SAFECARE at the Conference *Forum biomedical "l'Avenir de l'e-santé"*, Marseille (France) by APHM
- 11/2018: Presentation of SAFECARE at the *European Cyber Week (ECW)*, Rennes (France) by CCS
- 6/12/2018: Presentation of SAFECARE at the SAYSO 2nd Public Workshop, Brussels (Belgium), by EOS and KEMEA
- 23/01/2019: Presentation of SAFECARE at the *International Security forum (FIC)*, in Lille (France) by APHM
- 25-24/02/2019: Presentation of SAFECARE at the *Milestone Integration Platform Symposium (MIPS)*, Nashville (US), by Milestone
- 18/03/2019: Presentation of SAFECARE at the *Evènement national H2020 Sécurité des Infrastructures Critiques*, Paris (France), by APHM and CCS
- 25-27/03/2019: Presentation of SAFECARE at MIPS EMEA, Copenhagen (Denmark) by Milestone
- 2-5/04/2019: Presentation of SAFECARE at MIPS APAC, Bali (Indonesia) by Milestone
- 10/07/2019: Presentation of SAFECARE at the *Cybersecurity for Health Workshop*, Brussels (Belgium), by KEMEA
- 17/09/2019: Presentation of SAFECARE at the Community of Users, Brussels (Belgium) by APHM

Networking sessions:

- 24-25/10/2018: Networking for SAFECARE at the "*Internet of things security conference"*, in The Haag (The Netherlands), by BEIA
- 24/10/2018: Networking for SAFECARE at the *"European Brokerage Event on resilience from Disaster"*, Paris (France), by BEIA
- 5-6/12/2018: Networking at the Security Research Event, Brussels (Belgium) by EOS and ISEP
- 21-23/05/2019: Networking for SAFECARE at the Paris Healthcare Week (France) by Enovacom
- 18/09/2019: Presentation of and Networking for SAFECARE at the *SAFECARE Awareness Event,* Leuven (Belgium) by the entire consortium

2.1.4 Interactions with relevant projects

From the start of the project, SAFECARE has been in touch with several projects:

- SAYSO, for the workshop of which SAFECARE was invited to be presented
- SPHINX, for the workshop of which SAFECARE was invited to be presented

- FINSEC, for the workshop of which SAFECARE has been invited to be presented but could unfortunately not join
- Both FINSEC and SPHINX were presented during the SAFECARE first Awareness event
- Invited several other European projects to present at the awareness event and to maintain contacts for dissemination purposes: SAURON, DEFENDER, ASCEPLIOS, ANASTACIA and STOP-IT
- In discussions with FINSEC and DEFENDER to co-author a book discussing the technical aspects of the project and the results that will be public

Figure 5: Dr. Habtamu Abie, from FINSEC explaining their work on the security of financial infrastructure at the SAFECARE Awareness Event.

- SATIE project with which SAFECARE will start a strong collaboration
- IMPRESS project (FP7 and completed), from which SAFECARE used its network for dissemination purposes

Figure 6: Olivier Théveneau, from APHM, meeting Tim Stelken-Kobsch from DLR (Coordinator of the SATIE project)

- SAFECARE is also part of the H2020 synergy strategy which aims to increase the collaboration between relevant projects, in the field of cybersecurity in the health sector and promote dissemination amongst stakeholders in the field.

2.2 Communication means

The terms "Communication" was already defined in D8.1, underlining the importance of having a proper strategy. The following means were put in place during the first year of the project.

2.2.1 Visual materials

The SAFECARE visual identity has always been the trademark of the project and is defined by the project's logo (created at the time of the submission) and by the document templates (provided at M1 by EOS as SAFECARE quality manager).

Building upon the visual identity, a promotional package has been designed by EOS and was available for use at M3:

- Two SAFECARE roll-up banners to be used during project events and events SAFECARE will participate in[2] (EOS also provided a roll-up template for the Partners to be printed by themselves)

[2] It has been decided to produce one banner at M3 and one banner at M6. The reason is to include first pictures of the SAFECARE Consortium meetings or of partners presenting SAFECARE during external events.

- Flyers in English, French and Italian, both in soft and hard copies, to be disseminated during events in general and to shared online, to raise awareness about SAFECARE
- A standard PowerPoint presentation of SAFECARE, describing a detailed overview about the approach and objective, to be used and adapted if needed during events.
- Standard presentation to be adapted by each partner depending on the scope of their intervention

2.2.2 SAFECARE Website

As explained above, a website is accessible by a wide audience, through several means: mobile phones, computers or tablets. It diffuses and shares information about SAFECARE in general.

Despite that SAFECARE website was intended to serve as the main dissemination and communication tool, it appeared not to be so friendly. EOS faced some issues in updating its content.

2.2.3 SAFECARE social network and social media strategy

Understanding the crucial need of having an efficient Social network and social media strategy, several channels have been created for SAFECARE:

A **LinkedIn Group,** called SAFECARE Project has been initially set up. Due to the restrictive access of the Group, it was then decided to change it into **LinkedIn Page** (in May 2019) to have a more open access. The page is managed by EOS with the inputs of the consortium. Despite several reminders, not all the partners have followed the migration and the Page has only 18 followers (against 57 for the group).

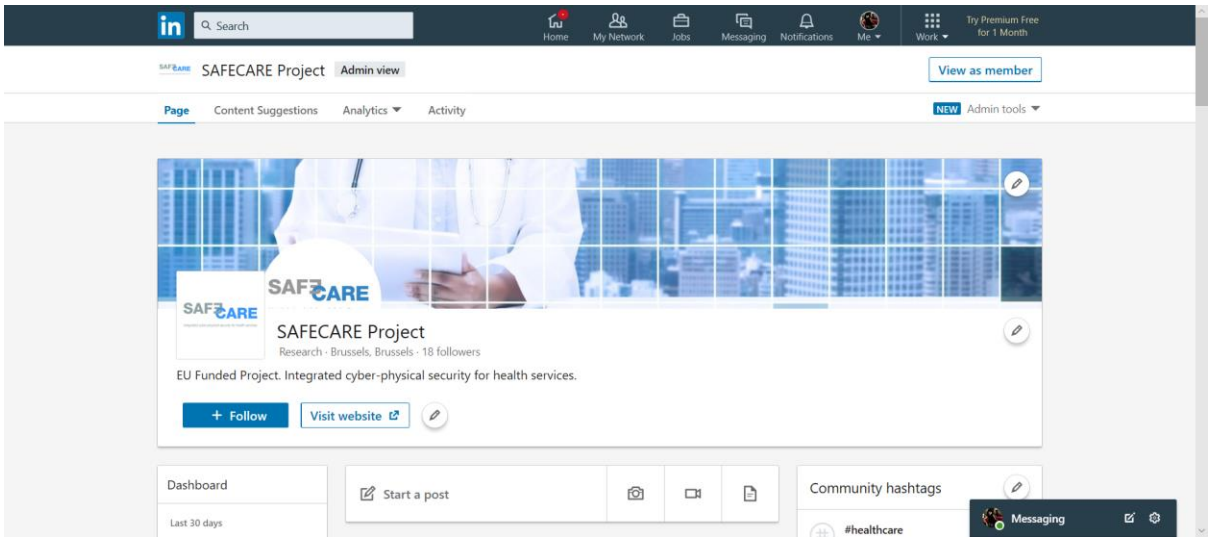


Figure 7: Screenshot of the LinkedIn Group

A **Twitter Account**, @SafecareP, was also created in November 2018 (M3). So far the account, counts 174 followers and posted 157 tweets and retweets, announcing important events or sharing interesting articles related to the scope of SAFECARE.

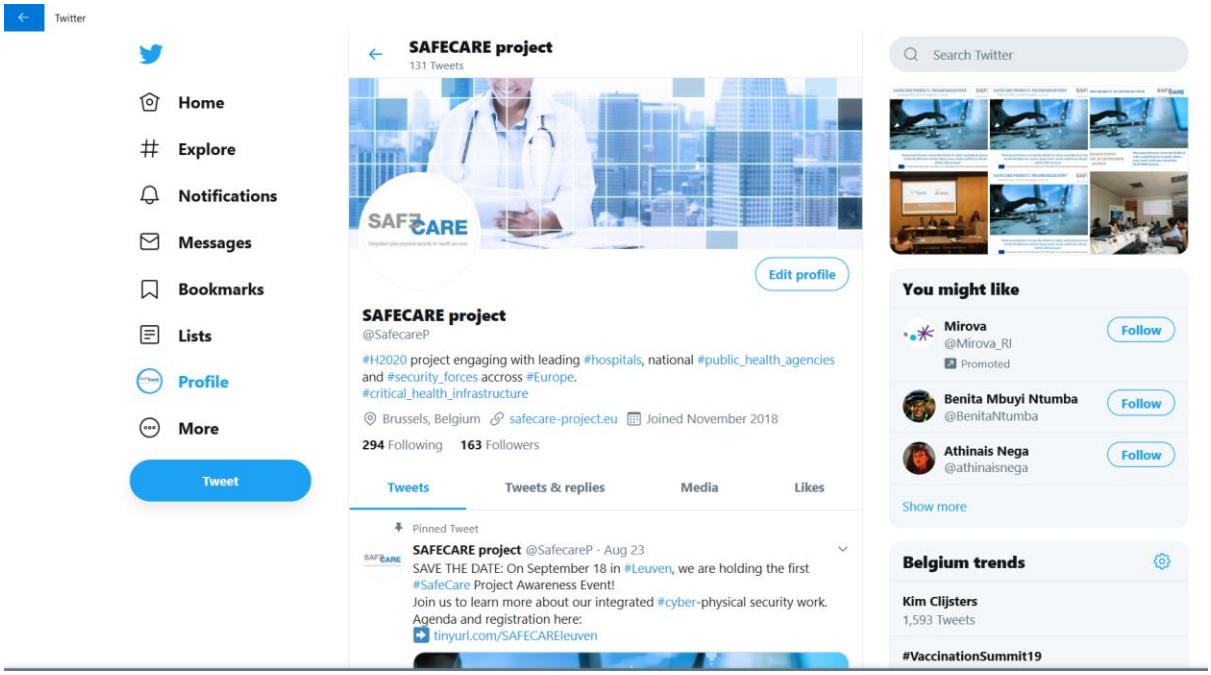


Figure 8: Screenshot of the Twitter Account @SafecareP

The platforms **LinkedIn** and **Twitter** are used to promote project events, by specific posts before the event (Twitter and LinkedIn), during the event (mostly Twitter on real time) and after the event (Twitter and LinkedIn).

2.2.4 Newsletters

Every six months, SAFECARE newsletter is shared to partners, presenting project's achievements and upcoming activities from the past and following six months respectively. Following the requirements established in D8.1, two newsletters have been shared so far, one at M7 and a second one, with an improved format, at M12 found in Annexes. The purpose of the newsletter is also to be shared through each partner's network to reach a wide audience.

2.3 SAFECARE communication policy

As explained in D8.1, SAFECARE consortium promotes the project, its objectives and results, by sharing targeted messages to a wide audience. This is done according to a strategic and previously well-defined way. Partners will be asked to communicate with interested stakeholders with the final objective being to serve SAFECARE's interests.

The communication activities are listed in this deliverable and include the following:

- The third party event, for which each presentation to be done was approved by EOS and APHM and,
- The promotional materials, pre-approved by the entire consortium and produced by EOS.

Before any communication activities (articles, production of promotional materials, contribution to third party events), SAFECARE Partners will have to get in touch and coordinate with EOS, which is the entity leading the WP8 (the Work Package on Dissemination, Exploitation and standardization) but also the Project Technical Coordinator. In case a communication activity is expected to have a major impact in terms of media, EOS and AP-HM will need to inform the European Commission.

3. Monitoring and Evaluation of the D&C activities during the first year

Key Performance Indicators had been defined at M3 and need to be constantly reviewed and adapted. Table 3 shows initial targets and the actual results obtained; and defines the D&C KPIs for the next period. Table 4 will establish the updated KPIs till M35

Table 1: Initial KPIs

KPIs		Target at M13			Measure from last year	Analysis
		Level of performance				
Dissemination and Communication tools	Definition of the indicator	Poor	Good	Excellent		
Project[3] Website	Number of visits per month	Less than 180 per month Less than 1800 at M13	180-375 per month 1800-3750 at M13	More than 375 per month More than 3750 at M13	2202 at M13	Good performance: In line with the objectives set in D8.1.
	Page views per month	Less than 250 per month Less than 2750 at M13	250-400 per month 2750-4000 at M13	More than 400 per month More than 4000 at M13	N/A	N/A
	Average time spent on website	Less than 45 seconds	45 seconds -2min	More than 2min	N/A	N/A
	Number of posts published	Less than 3 per month Less than 30 at M13	3-6 per month 30-60 at M13	More than 6 per month More than 60 at M13	N/A	N/A
	Number of posts relayed on partner's internal websites	Less than 250 at M13	250- 450 at M13	More than 450 at M13	N/A	N/A
	Number of downloads of project reports[4]	Less than 15 at M13	15-50 at M13	More than 50 at M13	N/A	N/A
Social Media Strategy	Subscribers of the LinkedIn Group	Less than 150 at M13	150-250 at M13	More than 250 at M13	57 (LinkedIn Group) + 46 (LinkedIn Page)	Poor: A strategy must be put in place to gain more followers and raise interaction with them.
	Number of discussion groups on LinkedIn	Less than 5 at M13	5-10 at M13	More than 10 at M13	14 (LinkedIn Group) + 10 (LinkedIn page)	Excellent performance: Only a few partners posted on LinkedIn. The strategy needs to be refined but the KIPs are line with the objectives of D8.1.
	Number of Twitter followers	Less than 250 at M13	250-450 at M13	More than 450 at M13	174	Poor performance: The strategy needs to be refined.
	Number of tweets only	Less than 165	165-330	More than 330	156[5]	Poor performance: additional efforts need to be put
	Number of retweets	Less than 66	66-154	More than 154	98	Good performance. In line of the objectives of D8.1.

[3] Important is to say that the website was put online at M3. The data collected reflects only 10 months of the project and not 11.
[4] The report will be uploaded on the website after their approval
[5] Important is to say that the twitter account has been launched at M3 (November 2018)

	Number of tweets liked per month	Less than 10	10-25	More than 25	29.5	Excellent performance. In line with the objectives of D8.1.
Biannual Newsletter	Number of Newsletters published	Less than 1	1-2	More than 2	2	Good Performance. In line with the objectives of D8.1.
	Number of clicks to open newsletter (for each newsletter)	Less than 100	100-200	More than 200	N/A	Metrics not available as Mailchimp not used
	Number of subscriptions obtained after each Newsletter release	Less than 13	13-28	More than 28	N/A	Metrics not available as Mailchimp not used
	Size of the dissemination list	Less than 200	200-400	More than 400	238[6]	Good performance
Media campaign, including publications in scientific journals, e-Newsletters and other media	Number of scientific papers submitted	Less than 5	5-10	More than 10	N/A	A lot of the work is ongoing. Concrete results/products will be shared up to year 2.
	Number of external websites, e-Newsletters, journals used for dissemination of project outcomes/outputs	Less than 15	15-30	More than 30	N/A	
	Number of Media partnerships concluded	Less than 3	3-6	More than 6	N/A	
Contributions to external events	Number of external events in which SAFECARE participates	0-1 per month Less than 10 at M13	1-2 per month 10-20 at M13	More than 2 per month More than 20 at M13	13	Good performance. In line with the objectives of D8.1.
	Number of abstracts/papers submitted and selected	Less than 6 at M13	6-18 at M13	More than 18 at M13	9	Good performance. In line with the objectives of D8.1.
	Copies of the brochure/factsheet distributed	Less than 300 at M13	300-800 at M13	More than 800 at M13	400	Good performance. In line with the objectives of D8.1.
Focus Group	Number of Focus Groups organised	2	2	2	4	Good performance: two more Focus Groups were organized due to the need expressed by the partners. In line with the objectives of D8.1.
	Number of Tweets during the events	Less than 5	5-10	More than 10	7	Good performance. In line with the objectives of D8.1.
	Number of online articles making reference to Focus Groups	Less than 2	2-7	More than 7	2	Bucharest and Brussels reported on.

6 Only SAFECARE Mailing lists and EOS mailing list have been counted

Awareness Event (M13 in Leuven)	Number of participants Countries of origin	Less than 30 Less than 4 countries	30-50 From 4-6 countries	More than 50 More than 6 countries	38 11 different countries	Between good and very good: the number of participants needs to be increased while the diversity in the country they come from is fine
	M&E questionnaire (response return %)	20%	20%-30%	More than 30%	20-30%	Good performance but can be improved
	Number of Tweets during the event	Less than 6	6-12	More than 12	14	Excellent performance
	Number of online articles making reference to the awareness event	Less than 5	5-10	More than 10	0	Poor performance
	Number of hits on the event page	Less than 100	100-200	More than 200	604	Event hosted on Eventbrite, analysis taken from there.
Liaison activities and synergies	Number of relevant projects/initiatives identified and contacted/invited at project events	Less than 8	8-20	More than 20	4	Poor: The idea was here to really get in touch with projects and initiatives directly related to SAFECARE.
	Number of relevant organisations/communities/experts identified and contacted/invited at project events	Less than 20	20-50	More than 50	48	Good performance: (contacts to be seen in Annex XX). In line with the objectives of D8.1.
	Number of MoU signed and/or concrete collaboration activities initiated with related initiatives/projects	Less than 10	10-20	More than 20	3.	Poor performance: the strategy needs to be refined. Need to formalize SAFECARE contribution to dissemination projects.
	Number of cooperation activities (common events and other clustering activities)	Less than 1	2-5	More than 5	2	Good performance: SAFECARE needs to follow its initial move
Link to the Community of Users	Number of SAFECARE presentations made during plenary meetings and thematic workshops	1 every three events	1 every two events + organisation of 1 external cooperation workshop	1 per event + organisation of more than 1 external cooperation workshop	1 presentation out of three events since September 2018	Poor performance: The KPIS need to be revised
Impact towards Policy Makers	Number of bilateral meetings with Policy makers	0-1 at M13	2-4 at M13	More than 4 at M13	1	Poor Performance: only during the CoU. KPIs need to be revised

	Presentations made during events gathering policy makers	Less than 2 at M13	2-5 at M13	More than 5 at M13	3	Good Performance: in line with the KPIs
Promotional material	Number of brochures produced	500 brochures at M13	650 brochures at M13	800 brochures at M13	500	Poor performance: It is to say that EOS also produced the French and Italian version to be printed by the partners
	Number of brochures distributed	400 brochures at M13	600 brochures at M13	750 brochures at M13	500	Between poor and good performance: KPIS to be revised

Table 2: Updated KPIs

KPIs		**Target at M35**		
		Level of performance		
Dissemination and Communication tools	**Definition of the indicator**	**Poor**	**Good**	**Excellent**
Project Website	Number of visits per month	Less than 180 per month	180-270 per month	More than 270 per month
	Page views per month	Less than 250 per month	250-400 per month	More than 400 per month
	Average time spent on website	Less than 45 seconds	45 seconds -2min	More than 2min
	Number of posts published	Less than 3 per month	3-6 per month	More than 6 per month
Social Media Strategy	Subscribers of the LinkedIn Group	Less than 100 at M35	100-200 at M35	More than 200 at M35
	Number of discussion groups on LinkedIn	Less than 15 at M35	15-25 at M35	More than 25 at M35
	Number of Twitter followers	Less than 300 at M35	300-450 at M35	More than 450 at M35
	Number of tweets per month	Less than 12	12-25	More than 25
	Number of retweets per month	Less than 6	6-14	More than 14
	Number of tweets liked per month	Less than 10	10-25	More than 25
Biannual Newsletter	Number of Newsletters published	Less than 1	1-2	More than 2
	Size of the dissemination list	Less than 200	200-400	More than 400
Contributions to external events	Number of external events in which SAFECARE participates	0-1 per month	1-2 per month	More than 2 per month
	Number of presentations given	Less than 18 at M35	18-54 at M35	More than 54 at M35

	Copies of the brochure/factsheet distributed	Less than 900 at M35	900-1600 at M35	More than 1600 at M35
Focus Group	Number of Focus Groups organised	6 at M35	6 at M35	6 at M35
	Number of Tweets during the events	Less than 5	5-10	More than 10
Awareness Event (M21 in Athens)	Number of participants Countries of origin	Less than 30 Less than 4 countries	30-50 From 4-6 countries	More than 50 More than 6 countries
	M&E questionnaire (response return %)	20%	20%-30%	More than 30%
	Number of Tweets during the event	Less than 6	6-12	More than 12
Liaison activities and synergies	Number of relevant projects/initiatives identified and contacted/invited at project events	Less than 10 at M35	10-16 at M35	More than 16 at M35
	Number of relevant organisations/communities /experts identified and contacted/invited	Less than 30 at m35	20-50 at M35	More than 50 at M35
	Number of cooperation activities (common events and other clustering activities)	Less than 2 at M35	2-7 at M35	More than 7 at M35
Link to the Community of Users	Number of SAFECARE presentations made during plenary meetings and thematic workshops	1 every six events	1 every four events + organisation of 1 external cooperation workshop	1 every two events + organisation of more than 1 external cooperation workshop
Impact towards Policy Makers	Number of bilateral meetings with Policy makers	Less than 2 at M35	2-4 at M35	More than 4 at M35
	Presentations made during events gathering policy makers	Less than 4 at M35	4-6 at M35	More than 6 at M35
Promotional material	Number of brochures produced	1000 brochures at M35	1300 brochures at M35	1600 brochures at M35
	Number of brochures distributed	800 brochures at M35	1200 brochures at M35	1500 brochures at M35

4. Dissemination and Communication Plan from M13 to M35

4.1 Dissemination strategy: main means

The idea of updating the Dissemination and Communication Plan is to keep serving the objectives mentioned in the section 2, and first put in place during the first year of the project:

- *Creating and maintaining awareness*
- *Engaging, with stakeholders already identified in the Dissemination and Communication Strategy.*

The purpose of the following section is to provide the updated plan of the several channels and tools used (and the right timing to use them) from M13 onwards until the end of the project.

4.1.1 Online means

The SAFECARE Project Website

As clearly established, the website is one of the main tools in terms of Dissemination and Communication.

Several weaknesses have been identified and will be corrected during the last phase of SAFECARE. The google analytics is now put in place and will give the opportunity to analyze the relevant data. The PU deliverables will be put online after their acceptance by the EC. Regarding the non-friendly aspect of the WordPress version, EOS will be working to redesign the website so that it is more user-friendly and presents a better tool for communications.

Finally, the partners have been asked to be more proactive in sharing information or articles. EOS has established a weekly reminder sent every Tuesday at 11.00 to remind them this.

Online Media Strategy and diverse publications

With the list of online media being established and the first public results about to be shared, the Online Media strategy will finally be applied. From M13 to M16, the consortium will start contacting media and present SAFECARE in general. This being done, publications of articles from January 2020 onward could start.

Network of stakeholders

The consortium will use the list of relevant stakeholders established by the partners to help to directly be in touch with them and share the first results as soon as they are available.

4.1.2 Offline means

External channels

SAFECARE's activities and results will keep being shared on several external websites for awareness purposes.

The most commonly used channels are the following:

- SAFECARE's partners websites and social networks (see in annexes)
- Websites of related H2020 (or EC funded in general) projects targeting Critical Infrastructure in general or Critical Infrastructure in particular

As experienced in the first phase, voluntary contribution is not working well within the consortium. Besides its reminder every Tuesday, EOS will also establish a table to be put online to keep track on the partners that contributed and a specific reminder will be sent to the point of contacts on that purpose.

Strategy on Mass Media

The timeline regarding the Awareness event taking place in Athens at M21, the Commercial Event in Elancourt at M34 and the Commercial Event in Brussels at M35 will remain the same with the one provided in D8.1.

4.1.3 Dissemination via events

SAFECARE partners are very proactive in attending events and workshops on behalf of SAFECARE. The updated list of external events can be found in Annex 1.

4.1.4 Interactions with relevant projects

With the first results of the project arriving, SAFECARE will become more attractive for other projects. The idea here is not to expand but to find really accurate projects with whom interact, as it is already the case.

Thanks to its several partners, SAFECARE has a lot of opportunities to share experience with other EU funded project. Its prospection will continue next year, by probably joining the next STEPWISE workshop.

4.2 Communication means

4.2.1 Visual materials

Being the trademark of SAFECARE, the visual materials will be produced all along the project.

Building upon the visual identity, a promotional package has been designed by EOS and was available for use at M3:

- SAFECARE roll-up banners design has been to the partners and can be printed anytime. EOS also proposed to the partners to print some. Only CCS responded to the request.
- Flyers in English, French and Italian, both in soft and hard copies, to be disseminated during events in general and to shared online, to raise awareness about SAFECARE are available and printed upon request by EOS
- The standard PowerPoint presentation of SAFECARE and the Standard presentation to be adapted by each partner are both regularly updated, according to any changes in the consortium

4.2.2 SAFECARE social network and social media strategy

Understanding the crucial need of having an efficient Social network and social media strategy, several channels have been created for SAFECARE:

LinkedIn: the major challenge here is to bring more followers to the **LinkedIn Page**. First, the followers of the former **LinkedIn group** need to join the page. Then, as a page is more visible than a group, the partners will be asked to contribute on a regular basis (upon request of the Tuesday reminder).

The same strategy of asking the partners 's contributions on a regular basis will apply to **Twitter**,

4.2.3 Newsletters

The process of the newsletter is working quite well and won't be changed for the rest of the project.

4.3 SAFECARE communication policy

The communication policy of SAFECARE will remain the same with the one explained in D8.1.

Annexes

Annex 1: List of external events

INTERNATIONAL / EUROPEAN External Publications			
Name of the event	**Description**	**Date**	**Location**
Community of Users (CoU	The Community of Users provides a platform to share information across member states and brings together the latest policy and research developments in a way that is easy to access. It encourages the exchange of information and practices to support those responsible for countering the various threats Europe faces. How is this going to be achieved? A forum of information exchanges represents the first level of interactions at EU level among research, policy, industry, and practitioners active in EU-funded security research.	Every three months	Brussels, Belgium
The 14th International Conference on Critical Information Infrastructure Security	CRITIS 2019 aims at bringing together researchers, professionals from academia, critical (information) infrastructure operators, industry, defense sector and governmental organisations working in the field of the security of critical (information) infrastructure systems.	23-25/09/2019	Linköping, Sweden
Critical Infrastructure Protection & Resilience Europe (CIPRE)	Critical Infrastructure Protection and Resilience Europe brinsg together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe. The conference looks at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.	14-16/10/2019	Milan, Italy
3rd ENISA - Europol IoT Security Conference	https://www.enisa.europa.eu/events/3rd-europol-enisa-iot-security-conference	24-25/10/2019	Athens, Greece
Mediterranean Security Event 2019 (MSE)	The objective is to bring together innovative R&D security projects, practitioners network, industry and academia in order to facilitate interaction	29-31/10/2019	Heraklion, Greece

	and synergy among R&D activity and the networks of practitioners as users of European Research.		
Security Research Event 2019 (SRE)	The SRE is the annual conference where industry, public authorities and knowledge institutions come together to discuss the state of play and future challenges for security research in Europe, and where a selection of EU funded security-related projects are displayed in a large exhibition area.	6-7/11/2019	Helsinki, Finland
Smart city expo world congress 2020	The Smart City Expo World Congress is the leading event for cities, the place where the future of cities is discussed and the most inspiring ideas for exploring our urban future are brought to stage. Since its first edition in 2011, it has succeeded in becoming a referential global meeting point for governments, companies, social entrepreneurs and research centers in order to strengthen capacities, increase collaboration and share inspiration for supporting the improved development of our cities.	19-21/11/2019	Barcelona, Spain
European Cyber Week	The European Cyber Week is a European event, organized in Rennes by the "Pôle d'excellence cyber" and its partners. The program of this 3rd edition includes technical conferences, business meetings and high-level events, addressing civilian and military stakes, around the thematic of "artificial intelligence and cybersecurity", and its applications in the area of health, media and defense. This event welcomes a large audience of cybersecurity experts: business executives, researchers, institutional bodies, investors and students.	19-21/11/2019	Rennes, France
Black Hat Europe 2019	Black Hat provides attendees with the very latest in research, development, and trends in Information Security. Here the brightest professionals and researchers in the industry will come together for a total of four days—two or four days of deeply technical hands-on Trainings, followed by two days of the latest research and vulnerability disclosures in the Briefings.	2-5/12/2019	London, UK
European, Mediterranean and Middle Eastern	European, Mediterranean and Middle Eastern Conference on Information Systems (EMCIS) is an annual research event addressing the IS discipline with	9-10/12/2019	Dubaï, UAE

Conference on Information Systems (EMCIC)	regional as well as global perspective. EMCIS has successfully helped bringing together researchers from around the world in a friendly atmosphere conducted to free exchange of innovative ideas. EMCIS was founded in 2004 by Brunel University research Group ISEing and it is an annual event. A number of respected collaborations were made with different local universities across the destinations chosen each year and EMCIS still proves to attract many further partnerships.		
15th International Conference on Information Assurance and Security (IAS)	The 15th International Conference on Information Assurance and Security (IAS) aims to bring together researchers, practitioners, developers, and policy makers involved in multiple disciplines of information security and assurance to exchange ideas and to learn the latest development in this important field.	11-12/12/2019	Bhopal, India
International Cybersecurity Forum (FIC 2020)	The international cybersecurity forum is a platform aiming at promoting a pan-european vision of cybersecurity as well as to strengthen the fight against cybercrime. In order to do so, the FIC relies on : The trade show, to share knowledge and ideas, recruit new employees and maintain contacts The forum, to discuss and debate with experts, to gather ideas and to share professional lessons The Observatory, to continue exchanging views and information after the FIC, to explore topics in greater depth and to consolidate our network of experts and like minded throughout the year	28-29/01/2020	Lille, France
13th International Conference on Health Informatics – HEALTHINF 2020	The purpose of the International Conference on Health Informatics is to bring together researchers and practitioners interested in the application of information and communication technologies (ICT) to healthcare and medicine in general and to the support of persons with special needs in particular. Databases, networking, graphical interfaces, data mining, machine learning, intelligent decision support systems and specialized programming languages are just a few of the technologies and research areas currently contributing to medical	24-26/02/2020	Valletta, Malta

	informatics. Mobility and ubiquity in healthcare systems, physiological and behavioral modeling, standardization of technologies and procedures, certification, privacy and security are some of the issues that medical informatics professionals and the ICT industry and research community in general are addressing in order to further promote ICT in healthcare. In the case of medical rehabilitation and assistive technology, research in and applications of ICT have contributed greatly to the enhancement of quality of life and full integration of all citizens into society.		
14th IFIP Working Group 11.10 on Critical Infrastructure Protection	The IFIP Working Group 11.10 on Critical Infrastructure Protection is an active international community of researchers, infrastructure operators and policy-makers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in information infrastructure protection. Following the success of the last 13 conferences, the 14th Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will again provide a forum for presenting original, unpublished research results and innovative ideas related to all aspects of critical infrastructure protection. Papers and panel proposals are solicited. Submissions will be refereed by members of Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection. Papers and panel submissions will be selected based on their technical merit and relevance to IFIP WG 11.10.	16-18/03/2020	Arlington, USA
Paris Healthcare Week	Over three days, around 900 exhibitors (OEMs, software publishers, suppliers, e-health entrepreneurs, medical device manufacturers, architects, carers, institutional representatives, etc.) meet with over 28,000 visitors, including CEOs, CIOs, heads of purchasing, care staff in hospitals and private practice, experts, decision-makers and healthcare professionals involved in management, digitalisation, equipment and construction for healthcare facilities.	26-28/05/2020	Paris, France
IoT Week 2020	IoT Week is a one-of-a-kind 5 day conference where leaders from the worlds	1-5/06/2020	Dublin, France

	of business, techn and science shed light on the future of technology and its impact on business and life.		
CEBIT 2020	Europe's Leading Digital Event - Business, leads and ideas: The triad of exhibits, conference and networking event provides a 360-degree view of digitization. For companies, administration and society CEBIT is the most important event of its kind in Europe.	June 2020	Hannover, Germany
SEC 2020 - 35th International Conference on ICT Systems Security and Privacy Protection - IFIP SEC 2020	The IFIP SEC conferences aim to bring together primarily researchers, but also practitioners from academia, industry and governmental institutions to elaborate and discuss IT Security and Privacy Challenges that societies are facing today and will be facing in the future.	25-28/05/2020	Maribor, Slovenia
International Conference on Informatics Management and Technology in Healthcare	The International Conference on Informatics, Management and Technology in Healthcare will cover topics like biomedical informatics, clinical informatics, standards, social and legal issues, health information management, knowledge management, and diagnostic technologies for medical decision support.	3-5/07/2020	Athens, Greece
18th World Congress on Medical and Health informatics	https://medinfo2021.org/	21-25/08/2021	Sydney, Australia

Annex 2 – List of the relevant stakeholders (without email address)

Network of Stakeholders			
Partners in charge	**Practioners contacted**	**Organisation**	**Advisory Board member**
N/A	XX[7]	Streamwide	YES
N/A	XX	InnovationSprint	YES
N/A	XX	FH Burgenland	YES
N/A	XX	Eurecat	YES
N/A	XX	MISIS	YES
N/A	XX	SRG Consulting	YES
N/A	XX	CHSJ	YES
N/A	XX	ECSO	YES
N/A	XX	ECTEG	YES
N/A	XX	SGSP	YES
N/A	XX	SPF	YES
N/A	XX	APHP	YES
N/A	XX	CHU Lyon	YES
N/A	XX	AIRBUS	YES
N/A	XX	DMU	YES
N/A	XX	EVNH	YES
N/A	XX		YES
EOS	XX	G4S	NO
EOS	XX	Italian Ministry of Interior - Department of Public Security	NO
EOS	XX	General Inspectorate of Romanian Police	NO
EOS	XX	UK Home Office - Centre for Applied Science and Technology	NO
EOS	XX	Judiciary Policy of Portugal	NO
EOS	XX	Italian Carabinieri	NO
EOS	XX	Police department Ministry of Interior of Lithuania	NO
EOS	XX	Polish Platform for Homeland Security	NO
EOS	XX	Lithuanian Cybercrime Center of Excellence for Training, Research and Education	NO
EOS	XX	National Institute for Criminologie	NO
EOS	XX	Belgian Crisis Center	NO
EOS	XX	Spanish Police	NO
EOS	XX	Italian Red Cross	NO
EOS	XX	Finnish Police	NO

[7] The names of the Practitioners has been hidden for data protection purposes

SPHINX Project	XX	VILabs	NO
SPHINX Project	XX	ViLabs	NO
ASCEPLIOS Project	XX	Suite5	NO
ASCEPLIOS Project	XX	Suite5	NO
ASCEPLIOS Project	XX	Suite5	NO
FINSEC Project	XX	GFT	NO
DEFENDER Project	XX	Engineering	NO
STOPIT Project	XX	IWW	NO
KEMEA	XX	Hygeia hospital Greece	NO
KEMEA	XX	KAT General Hospital, Greece	NO
KEMEA	XX	KAT General Hospital, Greece	NO
KEMEA	XX	Asklipieio Voulas Hospital, Greece	NO
KEMEA	XX	Hellenic Telecommunications Organisation S.A.,	NO
KEMEA	XX	University of the Peloponnese	NO
KEMEA	XX	University of Nicosia	NO
KEMEA	XX	Harokopio University	NO
KEMEA	XX	Harokopio University	NO
KEMEA	XX	G.Papanikolaou Hospital	NO
KEMEA	XX	3rd Health Region	NO
KEMEA	XX	3rd Health Region	NO
KEMEA	XX	G.Papanikolaou Hospital	NO
KEMEA	XX	4th Health Region	NO
KEMEA	XX	4th Health Region	NO
KEMEA	XX	Serres General Hospital	NO
KEMEA	XX	Ippokrateio General Hospital of Thessaloniki	NO
BEIA	XX	University Politehnica of Bucharest	NO
BEIA	XX	Carol I National Defense University, Bucharest	NO
BEIA	XX	Carol I National Defense University, Bucharest	NO

Annex 3 – List of relevant media

List of relevant publication	
Name of the publication	**Contact**
International Journal of Emergency Management	XX[8]
Get Resilient	XX
International Firefighter Magazine	XX
Asia Pacific Fire Magazine	XX
The European	XX
EU Horizon Magazine	XX
European Data Quaterly	XX
Security Europe	XX
Euractiv	XX
Politico	XX
New Europe	XX
Crisis Prevention	XX
Emergency Services Times	XX
FIRE	XX
Ambulance news	XX
TIEMS Newsletter	XX
France	
Civique Revue, ENSP	XX
Preventique	XX
Face au Risque	XX
Global Security Mag	XX
Defense et Sécurité Internationale	XX
Sécurité et défense Magazine	XX
Protection Sécurité Magazine	XX
Germany	
THW Journal	XX
Krisenmagazin	XX
Denmark	
Videnskab	XX

[8] The names of the Practitioners have been hidden for data protection purposes

Annex 4 – Updated Dissemination and Communication Points of Contact

D&C Points of contact				
Partners	**Names**	**Email**	**Any Communication department?**	**Email**
APHM	Caroline Peragut	Caroline.peragut@ap-hm.fr	N/A	N/A
CCS	David Lancelin	David.lancelin@airbus.com	Yes	Ambra.canale@airbus.com
UG	Sandra Lemanski	sandra.lemanski@uni-greifswald.de	Yes	Samuel.Schalck@airbus.com
ENC	Melanie Dufrou	mdufrou@enovacom.fr	Yes	information@enovacom.fr
SPF	Valérie Derrey	Valerie.DERREY@santepubliquefrance.fr	N/A	N/A
ISEP	Isabel Parça	Icp@isped.ipp.pt	Yes	GCI@isep.ipp.pt
CNAM	Samira Si-Said Cherfi	samira.cherfi@cnam.fr	N/A	N/A
KUL	Elisabetta Biasin Daniela Bresic Ilaria Buri	elisabetta.biasin@kuleuven.be Daniela.bresic@kuleuven.be ilaria.buri@kuleuven.be	N/A	N/A
LINKS	Cristiana D'Alberto	dalberto@ismb.it	N/A	N/A
CSI	Manuela Sarchioni	Manuela.sarchioni@csi.it	Yes	Maurizio.gomboli@csi.it
ASLT05	Paolo Petrucci	petrucci.paolo@aslto5.piemonte.it	N/A	N/A

EOS	Elodie Reuge	Elodie.reuge@eos-eu.com	Yes	James.Philpot@eos-eu.com
AMC	Henk Marquering	h.a.marquering@amc.uva.nl	N/A	N/A
MS	Barry Norton	BNO@milestone.dk	Yes	MSW@milestone.dk
FST	Mario Dragada	Mario.dragada@forescout.com	N/A	N/A
PEN/PMS	Brinda Hampiholi	brinda.hampiholi@philips.com	N/A	N/A
FMI / Civipol	Marie Fontaine	fontaine.m@civipol.fr	N/A	N/A
KEMEA	Ilias Gkotis Vasiliki Mantzana	i.gkotsis@kemea-research.gr v.mantzana@kemea-research.gr	N/A	N/A
BEIA	George Suciu	George@beia.ro	Yes	marketing@beia.ro
SGSP	Tadeusz Keson Piotr Kolmann	tkeson@sgsp.edu.pl pkolmann@sgsp.edu.pl	Yes	mglowka@sgsp.edu.pl

Annex 5 - Newsletter 1

Integrated cyber-physical security for health services

SAFECARE NEWSLETTER

Please find below short updates of SAFECARE's latest developments, discussions, reports and interesting upcoming events.

Management team in a nutshell

The SAFECARE (SAFEguard of Critical heAlth infrastructuRE) project was officially launched in September 2018. After more than 6 months of activity our project has come to life and our teams have rapidly gotten to know and work with each other thanks to our kickoff meeting and to our on-going focus group workshops.
Due to the technical and organizational complexities involved in our project, communications between all project members has been the key to our success thus far.

I would like to acknowledge and thank the dedication of all participants who have contributed in the crucial tasks involved in the building of the overall project (and deliverables). Although there is still a long way to go, I am happy to report that we are actively moving forward very quickly. The project management must therefore remain highly responsive to the needs of each task force in order to maintain and enhance the quality of our exchanges and innovations.

This initial phase of the project has allowed us to establish a management and organizational system composed of the 8 Work Packages leaders among whom 3 of them assist me in coordinating: Isabel Praça (ISEP) as Scientific Coordinator, Louis Jallet (CSS) as Technical Coordinator and Elodie Reuge (EOS) as Communications and Organizational Coordinator. This team offered major support in the preparation of the overall project from its inception.

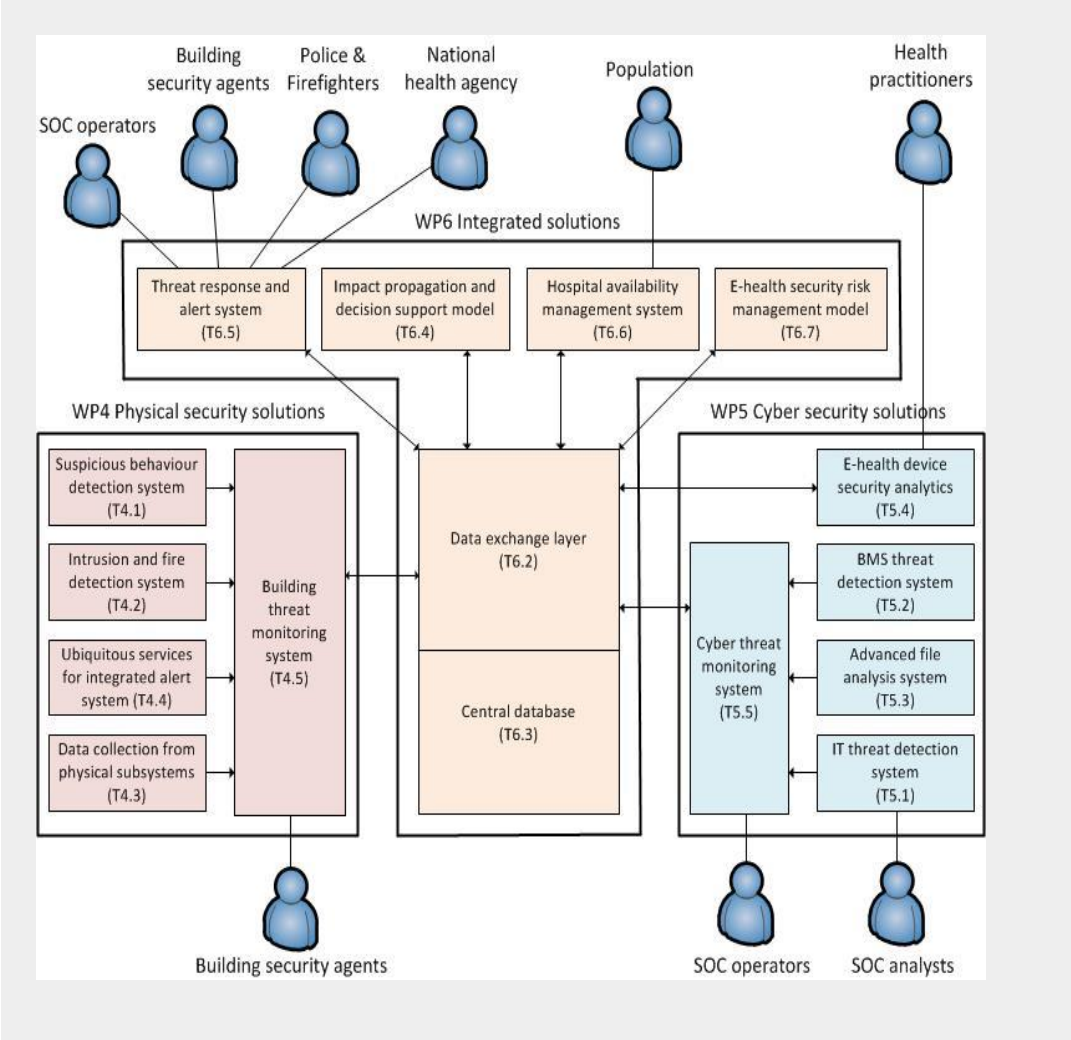
SafeCare coordinator

Philippe Tourron

Project Status

Below is an illustration of the main outcomes of SAFECARE for each Work package. The list of Work Packages and the Global architecture and interconnections are described in the following figures as a reminder.

WP Number	WP Title	Lead beneficiary	Start month	End month
WP1	Ethic requirements	1- AP-HM	1	36
WP2	Project Management	1 – AP-HM	1	36
WP3	Risk assessment and requirements	6 – ISEP	1	36
WP4	Physical security solutions	14 - Milestone	6	26
WP5	Cyber security solutions	2- CCS	6	26
WP6	Integrated cyber-physical security solutions	9 – ISMB	6	26
WP7	Tests and demonstrations	10 – CSI	18	33
WP8	Dissemination, exploitation and standardization	12 – EOS	1	36



Work Package 1

The WP on Ethics requirements was requested by the European Commission in the development phase, before signing the Grant Agreement. With such themes related to the healthcare, it is legitimate and fundamental to raise questions relating to ethics while at the same time, carrying out a risk analysis on privacy for the patients. It aims to consolidate information into deliverables originally planned for another WPs (including consents, responding to GDPR concerns). The consortium has been able to produce the first 3 deliverables of this period. Nevertheless, the partners will have to improve the coordination between themselves in order to facilitate the work to be done under the WP1. The first approach to the analysis of privacy has been made. The latter is to be completed over the following months in order to take into account the particularities of the tool under construction within the framework of the SAFECARE project. Significant work on authorizations has been done by the entire consortium but the final approval before demonstration on-site still needs to be obtained. The next deliverable will be the annual report of the Ethics board which is to be prepared by all the partners.

Work Package 2

The Work Package dedicated to Project Management organizes WP Leaders meetings every two weeks to review the status of each WP. At this time, the difficulties and the possible needs for arbitration by the coordinator are reported. In general, it is mainly a question of allowing each WP Leader to access the necessary information in order to best organize the planning of her/his WP and to define interfaces with other WPs. These meetings allow the organization to submit the deliverables as per DoA at the right level of quality and in keeping with the deadlines. They also contribute in the planning of the focus groups and events. 2 deliverables were completed on time (The initial Quality plan and the Financial Report). Some difficulties were experienced for the Financial Report, in terms of recovering the needed information. This point will be taken into consideration for the next financial deliverables.

Work Package 3

WP3 deals with risk analysis and requirements. This WP started working on the first day of project execution with the Kick-off of tasks 3.1 (Identification of critical assets in health infrastructure), 3.3 (Requirement analysis) and 3.6 (Study of ethical and privacy constraints related to the health environment). Up to now, work about critical assets, requirements analysis, SoA of security and know vulnerabilities and ethics, privacy and confidentiality constraints has been delivered. All these tasks are crucial to achieving the SAFECARE project goal to provide solutions that will improve physical and cyber security to prevent attacks, to promote incident responses and mitigate the impacts.

Work Package 4

WP4 concerns physical security solutions and kicked off in February 2019. Current tasks address the specification of functionalities for suspicious behavior detection, intrusion and fire detection, and the mobile service for integrated alerting. The process of collecting information of current provision of, and historical data, from cameras, fire detection devices and access control system is being carried out. The participants are also working on mapping out how the systems will interact, both within the physical security systems scope, and within the larger integration (WP6), in collaboration with WP5 on cybersecurity. A task on the building threat monitoring system, which is the basis of interaction with the rest of the architecture, will start in April 2019, and data collection from ICS, SCADA and smart building sensors will start in May 2019.

Work Package 5

The WP5 about Cyber security solutions has officially started in February 2019 during the Focus Group in Turin in January 2019.
The task T5.4 started in February 2019, with the objectives to provide a device security analytics solution. The task is led by Philips and its main contributors are CSI, Enovacom, AMC, Airbus and KU Leuven. First a specification of the e-health devices security analytics will be delivered, then the prototype will be achieved.
All other WP5 tasks will start in May 2019

Work Package 6

The WP6 about Integrated cyber-physical security solutions has just started at M6. The contributors of this WP will meet every 2 weeks for periodic calls in order to contribute to the development and achievement of the main objectives of this WP as the realization of :

- The central database
- A communication system between modules developed in other WPs
- Models for impact propagation and cascading effects
- Software modules for improving the availability and security of health services

Work Package 7

N/A (The WP7 about Tests and demonstrations will start at M18)

Work Package 8

The WP8 (Dissemination, exploitation and standardization D8.1) started at M1. The first deliverable of the project, the Dissemination and Communication strategy, has been submitted at M3 (and will be updated at M13). The implementation of the strategy will be carried out under the T8.2 and several activities are already in place :

- Web presence (SAFECARE Website)
- Social media presence (SAFECARE Project LinkedIn and SAFECARE Twitter)
- Material design for flyers
- Events participation (see below)
- Events organization (such as the Focus Groups and the first awareness event)
- Newsletters

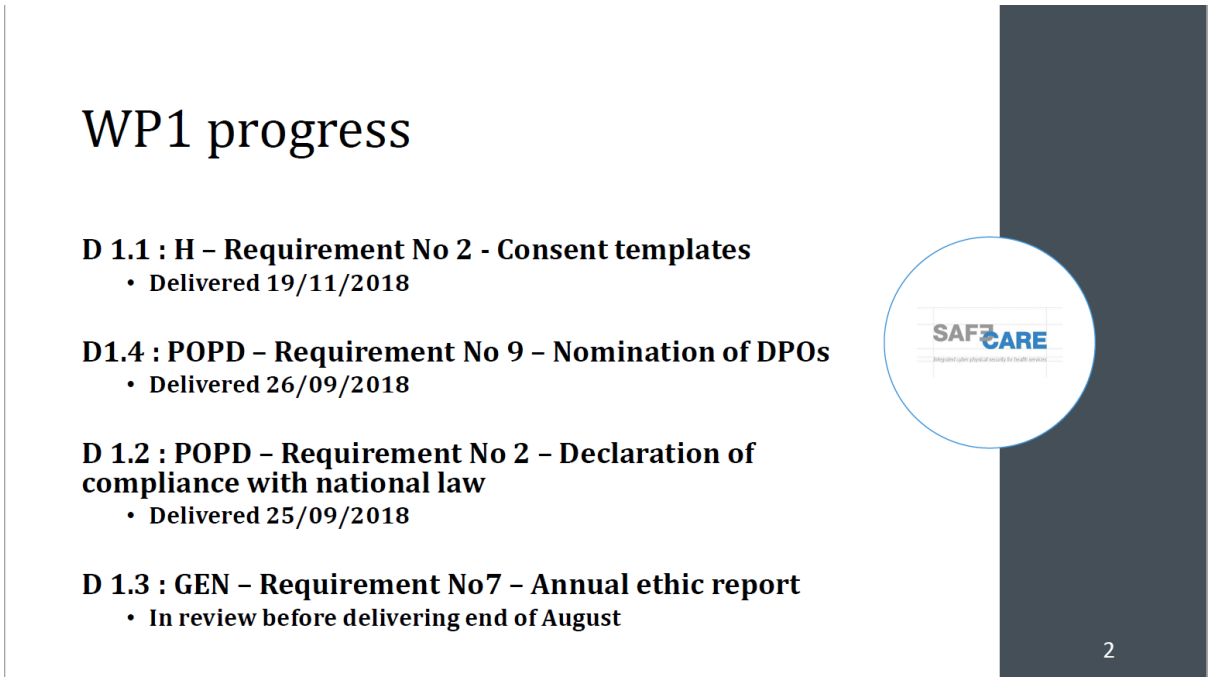
Past and Upcoming Events

- 19/10/2018 : Presentation of SAFECARE at the conference *Forum biomedical « l'Avenir de l'e-sante »,* in Marseille (France) by AP-HM
- 24-25/10/2018 : Networking for SAFECARE at the *,Internet of things security conference*, in The Haag (The Netherlands) by BEIA
- 24/10/2018 : Networking for SAFECARE at the *European Brokerage Event on Resilience from disaster*, in Paris (France) by BEIA
- 11/2018: Presentation of SAFECARE at the *European Cyber Week (ECW),* in Rennes (France) by Airbus
- 14/11/2018: Networking for SAFECARE at the *4th eHealth Security Workshop,* in Rotterdam (The Netherlands) by ISEP

- 5-6/12/2018: Networking at the *Security Research Event,* in Brussels (Belgium) by EOS and ISEP
- 6/12/2018 : Presentation of SAFECARE at the SAYSO 2nd Public Workshop, in Brussels (Belgium) by EOS and KEMEA
- 15-16/01/2019: First Focus Group, in Marseille (France) with all the partners
- 23/01/2019 : Presentation of SAFECARE at the *International Security forum (FIC) :* « Are SCADAs and cyber-physical systems 'unsecure' by design ? » in Lille (France) by AP-HM (Please see the link of the conference)
- 29-30/01/2019 : Second Focus Group, in Turin (Italy) with all the partners
- 25-24/02/2019 : Presentation of SAFECARE at the *Milestone Integration Platform Sysmposium* (MIPS), in Nashville (US) by Milestone
- 18/03/2019: Presentation of SAFECARE at the *Evènement national H2020 Sécurité des Infrastructures Critiques* in Paris (France) by AP-HM and Airbus
- 25-27/03/2019 : Presentation of SAFECARE at MIPS EMEA, Copenhagen, (Denmark) by Milestone
- 2-5/04/2019: Presentation of SAFECARE at MIPS APAC, in Bali (Indonesia) by Milestone

Twitter Website

Annex 6 - Newsletter 2



Next steps

D 1.3 : GEN – Requirement No 7 – Annual ethic report Y1

- **To be delivered M12**

D 1.5 : GEN – Requirement No10 – Annual ethic report Y2

- **To be delivered M 24**

D 1.6 : GEN – Requirement No11 – Annual ethic report Y3

- **To be delivered M 36**

3

SAFECARE

Integrated cyber-physical security for health services

AP-HM

Assistance Publique Hôpitaux de Marseille

WP2 Project Management

Olivier Théveneau

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

European Commission | HORIZON 2020

WP2 progress

T 2.1 Technical and scientific coordination

(Technical Coordination : CCS Airbus)

(Scientific Coordination : ISEP)

- **By weekly conference call with Work Package Leaders**
- **Preparation of annual progress report D2.1 M12**

T2.2 Administrative and financial tasks

- **Templates for biannual financial report**
- **Upload of first report on cumulative expenditures**

T2.3 Quality documents and deliverables management

- **Quality plan by EOS**
- **Designation of reviewers for all deliverables**

2

Next steps

T 2.1 Technical and scientific coordination

(Technical Coordination : CCS Airbus)

(Scientific Coordination : ISEP)

- **Continuation of by weekly conference call with Work Package Leaders**
- **Review and upload of final version of annual progress report (D2.1 M12)**

T2.2 Administrative and financial tasks

- **Consolidation of financial reports to prepare annual progress report**

T2.3 Quality documents and deliverables management

- **Follow up of effectiveness of review process**

3

SAFECARE
Integrated cyber-physical security for health services

isep Instituto Superior de Engenharia do Porto

WP3 Risk assessment and requirements

Isabel Praça (ISEP)

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

European Commission | HORIZON 2020

WP3 progress (since February 2019)

- **T3.2. State-of-the-art analysis and known vulnerabilities (M3-M12)**
  - A first draft of D2.2, that includes a list of physical and cyber vulnerabilities, how they might impact the likelihood of attacks and their effects, and the state-of-the-art analysis about security controls in health infrastructures, was delivered in M6.
- **T3.3. Requirements analysis (M1-M12)**
  - Initial requirements analysis in terms of physical security solutions, cyber security solutions, crisis management, communication and coordination strategies (D3.4) was delivered on M6.
  - Lexicon about crisis management applicable to cyber security and physical security was also delivered in M6 as an annex of D3.4.
- **T3.4. Definition of the cyber-physical scenarios of threat (M3-M9)**
  - Identification and formalization of the relevant use-cases and complex attack scenarios against critical health infrastructures. The resulting report (D3.6) was delivered in M9.
- **T3.5. Cyber-physical risk assessment and impact analysis (M9-M35)**
  - Kick-off of the task..
- **T3.6. Ethics, data privacy, data confidentiality, European and national regulations (M1-M36)**
  - Analysis of ethical, privacy and confidentiality constraints. The resulting report (D3.9) was delivered in M6.

SAFECARE

2

Next steps (by August 2019)

- **T3.2. State-of-the-art analysis and known vulnerabilities (M3-M12)**
  - An updated version of D3.2 will be delivered in M12 (D3.3).
- **T3.3. Requirements analysis (M1-M12)**
  - A Final requirements analysis that needs to include functional requirements with regards to threat prevention, threat detection, incident response processes and impacts mitigation will be delivered in M12 (D3.5).
- **T3.5. Cyber-physical risk assessment and impact analysis (M9-M35)**
  - Risk assessment and impact analysis of health will be developed, in the light of the implemented prototypes (D6.2) and demonstration results (D6.4). It will be delivered in M11.
- **T3.6. Ethics, data privacy, data confidentiality, European and national regulations (M1-M36)**
  - A second report about the implementation of ethical, privacy and confidentiality (D3.10) will be produced (to be delivered at M27).

3

SAFECARE
Integrated cyber-physical security for health services

milestone

WP4 – Physical security solutions

Barry Norton (Milestone)

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

European Commission | HORIZON 2020

WP4 progress (since February 2019)

- T4.1 – Suspicious behaviour system (Started in February 2019):
  - Requirements capture complete and definition of solution nearing completion
  - Research on current video provision in use case sites progressing
  - Definition of test bed hardware demonstrator for video underway
- T4.2 – Intrusion and fire detection system (Started in February 2019):
  - Requirements capture complete and definition of solutions nearing completion
  - Access control management system at ASLTO5 and AP-HM has been determined
  - Definition of test bed hardware demonstrator for access control underway
- T4.3 – Data collection system from ICS, SCADA… (Started May 2019):
  - Requirements capture and solution definition underway
  - Research on fire mgt. sensors at hospitals has been determined, and others underway
  - Definition of test bed hardware demonstrator for sensors undeway
- T4.4 – Mobile service for integrated alerting system (Started Feb 2019):
  - Requirements collection complete and definition of system architecture underway
  - First mockups of Safecare app produced
  - Proposal of data exchange format (JSON and EDXL)
- T4.5 – Building monitoring system (Started in April 2019):
  - Alignment of planned functionality with global architecture and mobile service underway

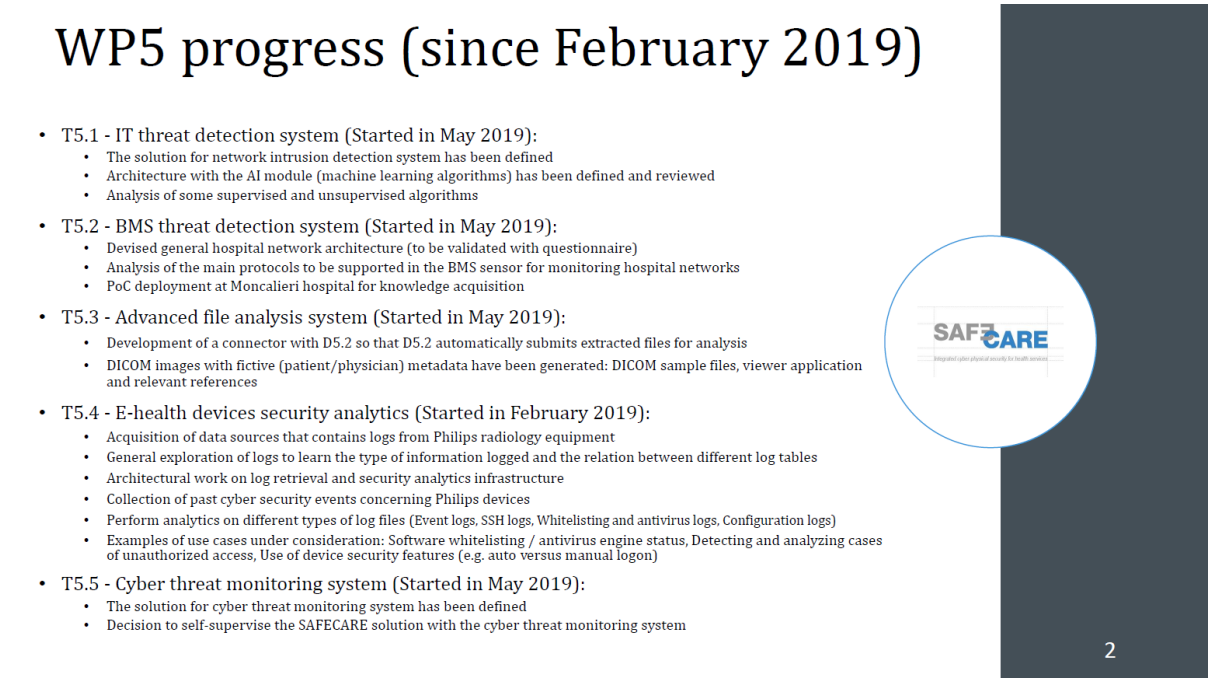
2

Next steps (by August 2019)

- T4.1 - Suspicious behaviour system:
  - Finalisation of specification (on track)
  - First prototype of test bed configuration
- T4.2 - Intrusion and fire detection system:
  - Publication of specification (on track)
  - First prototype of test bed configuration
- T4.3 - Data collection system from ICS, SCADA and smart building sensors:
  - Finalisation of specification (on track)
  - First prototype of test bed configuration
- T4.4 - Mobile service for integrated alerting system:
  - Architecture finalization
  - Direct connection to data exchange layer or through BTMS
  - Safecare App as mobile SOC for BTMS
  - Data exchange finalization
  - Safecare app mockup
- T4.5 - Building monitoring system:
  - Scope of functionality, with respect to data exchanged and UI provided, refined

3


SAFECARE
Integrated cyber-physical security for health services
AIRBUS
WP5 - Cyber security solutions
David Lancelin (AIRBUS)
SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002
European Commission | HORIZON 2020


WP5 progress (since February 2019)
• T5.1 - IT threat detection system (Started in May 2019):
• The solution for network intrusion detection system has been defined
• Architecture with the AI module (machine learning algorithms) has been defined and reviewed
• Analysis of some supervised and unsupervised algorithms
• T5.2 - BMS threat detection system (Started in May 2019):
• Devised general hospital network architecture (to be validated with questionnaire)
• Analysis of the main protocols to be supported in the BMS sensor for monitoring hospital networks
• PoC deployment at Moncalieri hospital for knowledge acquisition
• T5.3 - Advanced file analysis system (Started in May 2019):
• Development of a connector with D5.2 so that D5.2 automatically submits extracted files for analysis
• DICOM images with fictive (patient/physician) metadata have been generated: DICOM sample files, viewer application and relevant references
• T5.4 - E-health devices security analytics (Started in February 2019):
• Acquisition of data sources that contains logs from Philips radiology equipment
• General exploration of logs to learn the type of information logged and the relation between different log tables
• Architectural work on log retrieval and security analytics infrastructure
• Collection of past cyber security events concerning Philips devices
• Perform analytics on different types of log files (Event logs, SSH logs, Whitelisting and antivirus logs, Configuration logs)
• Examples of use cases under consideration: Software whitelisting / antivirus engine status, Detecting and analyzing cases of unauthorized access, Use of device security features (e.g. auto versus manual logon)
• T5.5 - Cyber threat monitoring system (Started in May 2019):
• The solution for cyber threat monitoring system has been defined
• Decision to self-supervise the SAFECARE solution with the cyber threat monitoring system
SAFECARE
2

Next steps (by August 2019)

- T5.1 - IT threat detection system:
  - Integration of the AI architecture on Airbus CyberRange (simulation platform)
  - Collect information on the target infrastructures (hospital network architecture)
- T5.2 - BMS threat detection system:
  - Validation of the hospital network architecture
  - Support for main protocols used in medical space within the BMS sensor: HL7, DICOM
  - Model threats pivoting from building network (PLCs) to medical networks
- T5.3 - Advanced file analysis system:
  - Test phase of the developed connector regarding performance
  - Specification of the advanced file analysis system (D5.5)
- T5.4 - E-health devices security analytics:
  - Specification of the E-health devices security analytics (D5.7)
  - Analyze different types of attack patterns in the medical device logs
  - Assign likelihood and severity for the detected events
- T5.5 - Cyber threat monitoring system:
  - Integration of the solution on Airbus CyberRange (simulation platform)

3

SAFECARE
Integrated cyber-physical security for health services

LINKS
ISMB

WP6 Integrated cyber-physical security solutions

Francesco Lubrano (LINKS foundation)

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

European Commission | HORIZON 2020

WP6 progress (since February 2019)

- **T6.1 Specification of the global architecture (M9-M16)**
  - The global architecture schema has been defined. It reports all the interconnections and message flows among SAFECARE modules
  - Relevant terms have been defined:
    - Security events, are detected by cyber or physical security modules and are automatically evaluated in order to understand if they can be considered as alerts
    - Alerts, are shown to human operators (e.g. SOC) that can check if they are true alerts or false positives
    - Incidents, are human-verified alerts that are sent to decisional modules (WP6) to be stored and elaborated
- **T6.2 Data exchange layer (M6-M24)**
  - MQTT has been chosen as the protocol to implement publish-subscribe mechanism
  - The data exchange layer is the only one module that can directly interact with the central database
- **T6.3 Central database (M6-M24)**
  - Main elements that will be stored in the central database have been defined
- **T6.4 Impact propagation model and decision support model (M6-M25)**
  - Requirements and functionalities of this module have been generally defined as well as its internal architecture
- **T6.6 Hospital Availability Management System (HAMS) (M9-M25)**
  - Functionalities of the HAMS have been defined
  - EDXL-HAVE standard has been studied and analysed
  - A first draft of the user interface has already commented by ASLTO5

2

Next steps (by August 2019)

- **T6.1 Specification of the global architecture**
  - Initial definition of the data models for the main elements in the architecture (assets, incidents, impacts, etc.)
- **T6.2 Data exchange layer**
  - Initial definition of relevant APIs in order to allows software modules to get data from the central database
- **T6.3 Central database**
  - Definition of the elements that will be stored in the central database according to requirements of the other tasks

T6.4 Impact propagation model and decision support model

  - First output example of the impact propagation model
  - Draft of the ontology that will be general enough to be used for all the defined scenarios
- **T6.6 Hospital Availability Management System (HAMS)**
  - Specification of the HAMS that will include the description of the user interface

3

WP8 – Communications and Dissemination

James Philpot (EOS)

SAFECARE has received funding as part of the "Secure societies – Protecting freedom and security of Europe and its citizens" challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

WP8 progress (since February 2019)

- T8.1 - Dissemination and Communication Strategy
  - Strategy delivered M3
  - Promotion material created and disseminated at events. Copies available online for partners to print their own.
  - Material being translated into multiple languages (French and Italian initially)
- T8.2 – Dissemination and communication, implementation and project events
  - Work is active and ongoing on the task through the three main communications channels: Website, Twitter and LinkedIn. Lack of content at the moment but that will change as results start arriving and more events take place
  - Event promotion has started for Leuven – Save the Date has been created.

2

Next steps (by September 2019)

- T8.1 - Dissemination and Communication Strategy
  - Will continue to update channels and promote project online. Will work to adapt deliverables and event reports to be shared online when possible.
- T8.2 – Dissemination and communication, implementation and project events
  - Awareness event in Leuven (M13). Will bring together project members, stakeholders and other practitioners to promote the project and seek synergies. Agenda is currently being finalised with contributions by project partners. More promotion material will be created once the agenda is set.
  - Press Release to accompany event as well as invitation letters.
  - Report of Dissemination Results (M13)
  - Newsletter (M12)

3

Thank you !

4